
Japan

National private networking support

Provides support for Japanese private ISDN networks. The Japanese private network ISDN protocol is different from the standard ISDN protocol. The switch supports extensions to the ISDN protocol for switches using the Japanese country code.

Katakana character set

Communication Manager supports the katakana character set (Japan). This nine-point character font was designed to display katakana characters in the user interface as well as in switch-generated messages.

Russia

Central Office support on G700 Media Gateway

Communication Manager supports central office (CO) trunks in Russia using the G700 Media Gateway.

ISDN/DATS network support

This feature supports ISDN/DATS trunk networks when the tone generated field is set to 15 (Russia) on the system-parameters country-options screen. It modifies the overlap sending delay and ISDN T302 and T304 timers to support the Russian trunk network.

Multi-Frequency Packet signaling

Multi-Frequency Packet (MFP) address signaling is provided in Russia on outgoing CO trunks. Calling party number and dialed number information is sent on outgoing links between local and toll switches. Russian MFP is set on each trunk group on the **type** field on the trunk screen.

Note:

Russian MFP does not apply to PCOL trunks.

E&M signaling - continuous and pulsed

Continuous and pulsed E&M signaling is a modification to the E&M signaling used in the United States. Continuous E&M signaling is intended for use in Brazil, but can also be used in Hungary. Pulsed E&M signaling is intended for use in Brazil.

Multinational Locations

For customers who operate in more than one country, the Multinational Locations feature provides the ability to use a single Enterprise Communication Server (ECS) across multiple countries with:

- ┆ telephones
- ┆ port networks
- ┆ remote offices
- ┆ media gateways

The Multinational Locations feature allows the following Communication Manager features to work across international borders:

- ┆ A & Mu law companding
- ┆ Call Progress Tone Generation
- ┆ Loss Plan
- ┆ Analog line board parameters
- ┆ Call Detail Recording
- ┆ R2-MFC (multifrequency signaling) trunks

The Multinational Locations feature works across all Linux platforms supported by Communication Manager release 2.1 or higher.

The S8300, S8500, and S87XX Servers each supports 25 location parameter sets. You can administer one parameter set for each country that you support, for a maximum of 25 countries.

Note:

Since the S8100 Server supports only 1 location, and since the Multinational Locations feature depends on multiple locations, the Multinational Locations feature is not supported on the S8100 platform.

Analog line board parameters per location

You can administer the following analog line board parameters for each location:

- | Analog Ringing Cadence
- | Analog Line Transmission
- | Flashhook Interval Upper Bound
- | Flashhook Interval Lower Bound
- | Forward Disconnect Timer (msec)
- | Analog line tests use the same parameters

Analog line circuit packs use these parameters, according to the location parameters of the circuit pack.

Companding for DCP telephones and circuit packs per location

You can administer the Companding Mode for each remote office, media gateway, and the rest of the system that is circuit switched.

- | When a Digital Communications Protocol (DCP) telephone comes into service, Communication Manager downloads the correct companding mode for the location of the telephone.
- | When a circuit pack comes into service, Communication Manager downloads the administered companding mode for the Avaya 8XXX Server, remote office, or media gateway that is supporting that circuit pack.

Location ID in Call Detail Record records

You can administer the following CDR parameters in the custom CDR format for both the source and destination:

- | location
- | time zone
- | country

Loss plans per location

For each location, you can administer Digital Loss & Tone Loss, DCP terminal loss parameters, and administrator-entered customizations.

When inserting loss for a multilocation intrasystem call, Communication Manager treats the call as if IP tie trunks are connecting the different parties. When an audio stream is converted from time-division multiplexing (TDM) to Internet Protocol (IP), the system adjusts the audio stream. The system adjusts the audio stream by the IP media processor board of the sending location, to an ISO standard level for voice over IP. The system then adjusts the audio stream by the media processor of the receiving location to match the TDM levels for that location.

This board level adjustment is not done for DS1 remoted expansion port networks (EPNs). Use DS1 remoted EPNs between countries only if the countries have similar voice transmit levels.

Multifrequency signaling per trunk group

Prior to Communication Manager release 2.1, you administer R2-Multifrequency Coded (MFC) signaling parameters per system. With Communication Manager release 2.1 and higher, you administer R2-MFC signaling parameters per trunk group.

R2-Multifrequency Coded signaling trunk groups use one of 8 sets of MFC signaling parameters according to the MFC signaling code administered for that trunk group.

Tone generation per location

You can administer tone generation characteristics and administrator-entered customizations per location. You can administer the server so that, when a telephone or trunk needs to play a Communication Manager ECS-generated tone, the software plays a tone into the call using the tone characteristics of the location of the listening endpoint, or of another endpoint on the call.

Public network call priority

Provides call retention, forced disconnect, intrusion, mode-of-release control, and re-ring to switches on public networks. Different countries frequently refer to these capabilities by different names.

World class tone detection

World class tone detection enables Communication Manager to identify and handle different types of call progress tones, depending on the system administration. You can use the tone detector and identification to display on data terminal dialing and to decide when to send digits on trunk calls through abbreviated dialing, ARS, AAR, and data terminal dialing.

XOIP Tone Detection Bypass

The X over IP Tone Detection Bypass feature (where X = modem, fax, TTY-TDD, etc.) serves customers using older or non-standard external equipment such as modems, fax, TTY devices which are not easily recognized by VoIP resources within Communication Manager. By identifying this external equipment through administration, VoIP firmware determines whether to immediately attempt to put a call in pass-through mode, or allow the system to handle it normally.

Chapter 9: Message integration

Avaya Aura™ Communication Manager Messaging

The CM Messaging application enhances communications and information exchange within enterprises, helping customers be more successful with call answering and messaging. The CM Messaging application enables customers to see messages on their PCs, add a voice mail component to an e-mail, and listen to e-mail using voice mail. The distributed architecture in CM Messaging is designed for reliability and survivability and is centrally managed for simplicity, efficiency and quick response to help ensure business recovery.

The Communication Manager license includes the CM Messaging application with up to 500 mailboxes. CM Messaging enforces licensing for mailboxes in excess of 500.

CM Messaging supports digital (TCP/IP) networking protocol. More extensive networking can be provided with the Avaya Interchange.

All the administrative features for CM Messaging are available on the Messaging Administration Web interface. Using the Web interface, the administrator can perform a system backup and restore of all administered data—announcements, recorded names, greetings—and approximately 50 hours of messages over the local area network (LAN). The screens are easier to understand and more intuitive, which reduces installation time and lessens the need for training and experience. The CM Messaging system uses smart defaults rather than requiring every field to be addressed.

Enhanced security features, such as disallowing voice PINS related to mailbox number, aging of voice mail PINS, locking of voice mails after invalid PIN attempts, duration of voice mail locking, default voice mail PIN length and so on.

Upgrade CM Messaging from release 3.x, 4.x, 5.x to release 5.2.

For more information on the CM Messaging messaging application, see the *Avaya Aura™ Communication Manager Messaging* Application Documentation CD collection on the Avaya Support web site.

CM Messaging application

While many voice messaging systems require separate equipment and connections, the CM Messaging application installs on the Communication Manager application to support advanced voice messaging capabilities without the need for an adjunct processor. The messaging capability on servers that support CM Messaging system are:

- ┆ Support for S8500C Server with up to 5,000 mailboxes
- ┆ Support for S8510 Server with up to 6,000 mailboxes

Message integration

- | Support for S8300 Server with up to 450 mailboxes
- | Support for S8400 Server with up to 900 mailboxes

Whenever you call the CM Messaging system, you interact with it by entering commands through your telephone touch-tone keypad. You simply specify the desired activity, and follow the voice prompts for the desired task.

Special voice-processing features include voice mail, call answering, outcalling, multi-level automated attendant, and bulletin board. The following is a summary of CM Messaging capabilities:

- | *Enhanced List application* provides the ability to deliver messages to large numbers of recipients.
- | *Lockout Notification Mailbox* is a mailbox that you can create to send out locked login notification to a local mailbox.
- | *Calling Party Number*, when turned on in the Messaging Administration Web interface, gets you up to 39 digits of the message sender's number when you listen to the message header from Telephone User Interface, or when you use a IMAP4/POP3 client to retrieve the call answer message. However, you need to administer Communication Manager to get up to 39 digits of the calling party.
- | Support for * in the dial string.
- | *Outcall scheduling* for a subscriber is based on a subscribers time zone and not on the system time zone.
- | Depending on the *Privacy Enhancement Type* set, the messaging system blocks a private message and a user sees a warning or alert message when retrieving a private message from a IMAP4/POP3 client. The language of alerting message depends on Message Locale defined for that user.
- | *Enhanced no cover 0* does not follow the coverage path for the covering extension. However, you can press (*T) to transfer the call to another extension.
- | *Messaging Capacity calculator* helps to determine the number of call answer ports required to administer the system.
- | Configure an *external SMTP relay host* using an IP host name to deliver an email that is not addressed for delivery to a locally known CM Messaging system or an Intuity Audix LX system that supports Internet Messaging. The external host is responsible to deliver the email to its correct destination.
- | Configure a server with CM Messaging application installed on it as a *Centralized Messaging Server* (CMS).
- | *Shared extensions* provide personal mailboxes for each person sharing a telephone.
- | *Multiple personal greetings* allows you to prepare a pool of up to nine personal greetings to save time and provide more personal customer service. Separate messages can indicate that you are on the telephone, away from the desk, on vacation, etc. You can assign different messages to internal, external, or after-hours calls.

- | *Priority messaging* places important messages ahead of others. Internal and external callers can mark the message as priority.
- | *Outcalling* automatically dials a prearranged telephone number or pager when you have messages in your voice mailbox.
- | *Priority outcalling* automatically dials a prearranged telephone number or pager when you have *priority* messages in your voice mailbox.
- | *Broadcasting* allows you to send a single message to multiple recipients or to all users on the system.
- | *System broadcast* allows you to send broadcast messages as regular voice messages, or as messages that recipients hear as they log in.
- | *CM Messaging directory* allows you to look up the extension number of any other user by entering their name on the telephone keypad.
- | *Personal directory* allows you to create a list of nicknames for quick access to telephone numbers.
- | *Call answering for nonresident subscribers* provides voice mailboxes for users who do not have an extension number on the system.
- | *Full mailbox answer mode* informs callers whenever messages cannot be left because there is no room in a subscriber mailbox.
- | *Name record by subscriber* lets you record your own name on the system.
- | *Automatic message scan* can play all new messages in part or in their entirety without requiring you to press additional buttons, which is particularly useful when you are getting messages from your mobile telephone.
- | *Sending restrictions by community* enables you to limit the communities of callers who can communicate using CM Messaging voice messaging.
- | *Group lists* allows you to create mailing lists of up to 250 people to use for broadcasting messages.
- | *Message forwarding* allows you to forward messages with or without attached comments.
- | *Name addressing* allows you to address messages by name if you do not know the extension.
- | *Private messaging* is a special coding feature that prevents recipients from forwarding messages.
- | *Leave word calling* allows you to press a button on your telephone in order to leave a standard “call me” message on any extension.
- | *Multiple language support* allows you to install up to nine languages on the system, from a superset of 30 available languages.
- | *Enhanced message handling* gives you the flexibility for handling messages. Two of these features are *optional advance/rewind* that lets you advance through and rewind individual

messages, and *undelete messages* that lets you retrieve any messages that you may have accidentally deleted.

- | *Fax messaging* allows you to handle faxes as easily as you handle voice mail. You can send, receive, store, scan, delete, skip, or forward faxes. This feature is fully integrated with voice messaging, so you can attach faxes to voice messages, for example. You can also create special mailboxes for each of your fax machines. These mailboxes accept fax telephone calls when the fax machine is busy and then deliver the fax to the fax machine when the fax machine is available.
- | *Turn off CM Messaging call answering* allows you to turn off call answering in order to conserve system resources. You can create a message that tells callers they cannot leave a message, giving them another number to call, for example.
- | *Pre-addressing* allows you to address a message before recording it.
- | *Integrated messaging* allows you access and manage incoming voice, fax, and e-mail messages and file attachments from your personal computer or your telephone. A voice message appears in your e-mail mailbox, for example, and vice versa. You can also set options to have just the message headers appear in the alternate mailbox. You can also create a voice or fax message by telephone and send it to an e-mail recipient.
- | *Text-to-speech* allows you listen to a voice rendering of text messages sent from a supported e-mail system and/or message manager.
- | *Print text* allows you to print messages sent from a supported e-mail system and/or message manager.
- | *Enhanced addressing* allows you to send a message to up to 1500 recipients.
- | *Transfer restrictions* allow you to control toll fraud by restricting transfers going through the voice messaging system.
- | *Internet messaging* allows you to exchange messages (voice and text) with any e-mail address via the World Wide Web.
- | *International availability*.

Record on messaging

Users can record conversations by pressing a single button using the Telephone User Interface. This feature uses AUDIX as the recording device.

Note:

It is important that anyone who wants to activate this feature should study and understand your local laws regarding the recording of calls *before* activating this feature.

A feature button named `audix-rec` is used for this feature. The button is available for all stations that have administrable feature buttons. When administered, the button also requires a hunt group extension number (for the CM Messaging extension number) along with it.

Note:

Attendant consoles do not have this button.

To record a conversation when a call is in process, press the `audix-rec` button. When you push the button, the LED light for the feature button begins to flash. After about 4~6 seconds, internal users who are participating in the call will notice that the telephone display changes to `CONFERENCE`. The LED light on the telephone that initiated the recording is steadily illuminated. This indicates that the AUDIX recording facility is ready and begins to record the conversation.

The internal users on the same switch with the display equipment can notice that the number of parties in the call increases by 1. At this point, depending on the administration, a ready indication tone will play to all the parties in the call, the initiator only, or none of the parties.

After enough information has been recorded, the initiator can then stop the recording by pressing the `audix-rec` button a second time when the LED light is illuminated. The feature button LED light on the initiator telephone goes out. The internal users with the display equipment can again notice that the number of parties in the call decreases by 1. The call remains active.

The `Interval For Applying Periodic Alerting Tone` field is used to allow the switch administrator to choose an interval to play an alerting tone to all the parties on the call during recording. Values are 0 to 60, and the default is 15. This means, if the default value is used, that all parties on the call hear an alerting tone every 15 seconds that indicates the conversation is being recorded. If the value for the field is 0, then no periodic tone is played during recording.

Audible message waiting

Audible message waiting places a stutter at the beginning of the dial tone when a telephone user picks up the telephone. The stutter dial tone indicates that the user has a message waiting. This feature is particularly useful for visually impaired people who may not be able to see a message light. It is often used with telephones that have no message waiting lights.

Audible message waiting may not be available in countries that restrict the characteristics of dial tones provided to users.

Leave Word Calling

Leave Word Calling (LWC) allows internal system users to leave a short preprogrammed message for other internal users. The preprogrammed message usually is the word "call," the caller name, extension, and the time of the call. When the message is stored, the message lamp on the called telephone automatically lights.

LWC messages can be retrieved using a telephone display, voice message retrieval, or telephone user interface. Messages may be retrieved in English, French, Italian, Spanish, or a user-defined language.

Leave Word Calling - QSIG/DCS

The Leave Word Calling (LWC) feature is extended to enterprise networks with QSIG as the private network protocol, as well as those with DCS.

For enterprise networks that are mixed or in transition from DCS to QSIG, interworking of the LWC feature between the protocols can be provided. LWC also works within a single non-networked switch.

Note:

A DCS+ signaling group is needed, but can only be used in networks with 4-digit or 5-digit dial plans.

Manual message waiting

This feature allows multi-appearance telephone users to light the status lamp associated with the manual message waiting button at another multi-appearance telephone. They do this by simply pressing a button on their own telephone. This feature can be administered only to pairs of telephones such as a secretary and an executive. The secretary might press the button to signal to the executive that a call needs answering or someone has arrived for an appointment. The executive might use the button to indicate that he or she should not be disturbed.

Centralized voice mail (Tenovis)

A Tenovis C3000 Voice Mail server that was connected through a Tenovis system to a Avaya AuraTM Communication Manager server, could not light the Message Waiting Indicator lamps when messages were left for Avaya AuraTM Communication Manager users. Now, when connecting a Centralized Voice Mail to the I55, it is possible to switch the message indication for Avaya AuraTM Communication Manager subscribers in a QSIG Corporate Network.

Message retrieval

With the message waiting lamp on their telephones, employees always know when they have messages. Messages can be retrieved in a variety of ways. These message retrieval options can be assigned to individual users.

You can also use Message Manager PC software to retrieve messages.

Message Sequence Tracer enhancements

In the past, it had been difficult to trace messages through the Message Sequence Tracer (MST) tool pertaining to a particular socket because there was no tag in each message distinguishing it from other sockets.

New message formats for outgoing and incoming data now include the socket number/identifier. These new formats use new Type identifiers of 05 and 06. A pair of new formats 07 and 08 have also been created for outgoing and incoming socket control messages on the PROCR ip-interface.

By creating new format types for these new formats, the task of decoding these messages is easier.

The following enhancement was made to the Message Sequence Tracer (MST):

- 1 Signaling messages between Avaya AuraTM Communication Manager and the TN799 CLAN can now be traced for better diagnostics during network outages.
 - Add processor TN799 CLAN socket information to the MST trace in order to help developers debug socket problems.
 - Enhance MST to include the socket number in socket data.
 - Add TN799 CLAN board ID to CLAN MST IP socket trace messages.

Octel integration

Avaya AuraTM Communication Manager integrates with the entire line of Octel messaging systems including the Octel 200/300 message server, and the Octel 250/350 message server.

QSIG/DCS voice mail interworking

QSIG/DCS voice mail interworking is an enhancement to the QSIG feature. It integrates DCS and QSIG centralized voice mail using the DCS+/QSIG gateway. Switches labeled DCS+/QSIG integrate multi-vendor PBXs into a single voice messaging system. QSIG/DCS voice mail interworking works on G3r, G3si, and G3csi. It provides network flexibility, DCS functionality without a dedicated T1.

Multiple QSIG voice mail hunt groups

Avaya AuraTM Communication Manager provides for ten message center hunt groups to support QSIG integrated messaging. This feature allows customers to spread users in a single Avaya AuraTM Communication Manager system over multiple messaging systems. This allows users to move among Avaya AuraTM Communication Manager systems while retaining their same voice mailbox. Users do not lose voice messages.

This feature also enhances customer usability of Avaya messaging systems in the enterprise by allowing not only for growth, but the ability to migrate end users on a single Avaya AuraTM Communication Manager system.

Voice mail retrieval button

Avaya Communication Manager supports the voice mail retrieval feature as a fixed feature button on the 2420 DCP and the 4602 telephone.

A field, “voice-mail Number: _____” appears on the **Station** screen for stations of type 2420 and 4602. The allowed values for this field are identical to the values allowed for an autodial feature button number. The field is a fixed field allowing entry of up to 16 digits that are auto-dialed to access the user's voice mail system.

- 1 If the number field is blank, the voice mail retrieval button is treated like the “Transfer to Voice Mail” button.

If the number field is not blank, the voice mail retrieval button is treated like an autodial button.

Voice message retrieval

Voice message retrieval allows telephone users, remote access users, and attendants to retrieve leave word calling and call coverage voice messages. You can use voice message

retrieval to retrieve your own messages or messages for another user. However, you can only retrieve messages for another user:

- ▮ from a telephone or attendant console in the coverage path
- ▮ from an administered system-wide message retriever
- ▮ if you are a remote-access user and you know the extension and associated security code

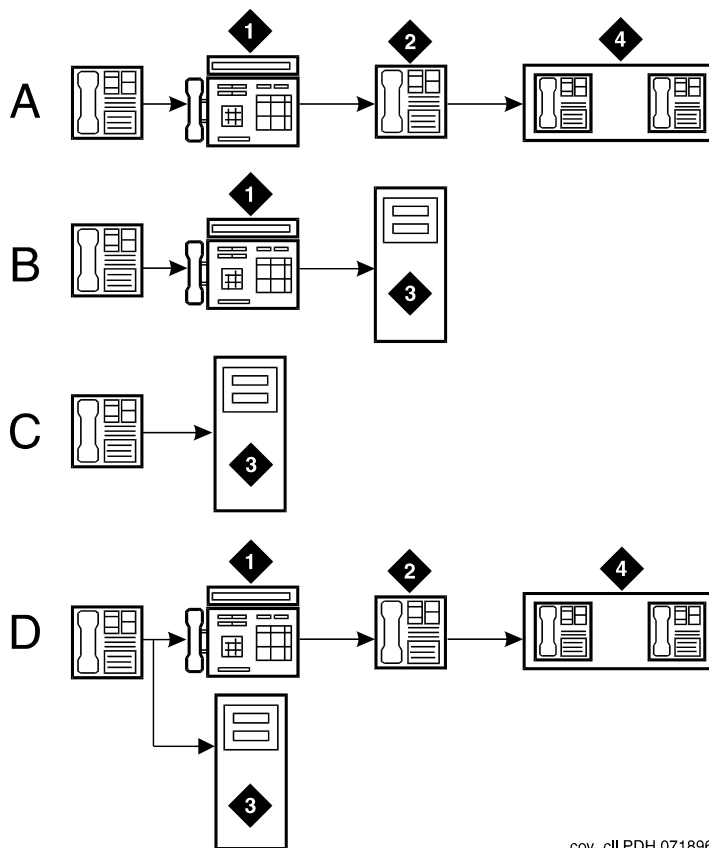
The system restricts unauthorized users from retrieving messages.

Voice messaging and call coverage

Often a CM Messaging system is set up as the last point on a call-coverage path, as shown in [Figure 3: Typical call coverage options](#) on page 112. A secretary or colleague who answers a redirected call intended for you can also transfer the caller to your CM Messaging mailbox. The caller may prefer to leave voice-mail for you if the message is personal, lengthy, or technical.

Many other options are available. For example, a caller can redirect a call from the CM Messaging system to an attendant. Or the caller can transfer to another extension instead of leaving a message. You can even have the CM Messaging automated attendant answer all calls to the company and send calls to various extensions. In this case, callers are instructed to enter keypad commands to direct the call.

Figure 3: Typical call coverage options



cov_cll PDH 071896

Figure notes:

- | | |
|-----------------------------------------------------|----------------------------------------|
| A External call: active, busy, do not answer | 1. Secretary |
| B Internal call: cover all | 2. Clerk |
| C Internal call: active, busy, do not answer | 3. CM Messaging voice messaging |
| D Internal call: send all calls | 4. Message center group |

Chapter 10: Mobility

IP telephones or IP Softphones allow you to access the features of Communication Manager without having to be tied to one location. One of the major benefits of IP telephones is that you can move the telephones around on a LAN just by unplugging them and plugging them in somewhere else. One of the main benefits of IP softphones is that you can load them on a laptop PC, and then use the PC's modem to connect them to the switch from almost anywhere.

For more information, see [Avaya IP Softphone](#) on page 83.

Administration Without Hardware

This feature allows you to administer telephones that are not yet physically present on the system. This feature works the same as administration with hardware: when stations are moved, user-activated features such as call forwarding and send all calls are preserved and functional. This greatly facilitates the speed of setting up and making changes to the telephones on the system.

Automatic Customer Telephone Rearrangement

Automatic Customer Telephone Rearrangement (ACTR) allows a telephone to be unplugged from one location and moved to a different location without additional switch administration. The switch automatically associates the extension to the new port.

ACTR works with the 2420 DCP telephone, the 6400 serialized telephones, and newer DCP telephones. The 6400 serialized telephone is stamped with the word “serialized” on the faceplate for easy identification. The 6400 serialized telephone memory electronically stores its own part ID (comcode) and serial number. ACTR uses the stored information and associates the telephone with new port when the telephone is moved.

ACTR makes it easy to identify and move telephones.

Avaya Wireless Telephone Solutions

Avaya Wireless Telephone Solutions (AWTS) is fully integrated with Communication Manager, and allows a user full access to Communication Manager features from a mobile telephone.

Note:

Avaya Wireless Telephone Solutions (AWTS) replaces the DEFINITY Wireless Business System (DWBS).

Avaya Extension to Cellular

The Avaya Extension to Cellular feature provides the expansion of mobile services, including one-number availability, increased user capacities, flexibility across facilities and hardware, more control over unauthorized usage, enhanced enable/disable capability, increased serviceability, and support of IP trunk facilities.

Avaya Extension to Cellular and off-PBX stations (OPS) provides users with the capability to have one administered telephone that supports Communication Manager features for both an office telephone and one outside telephone. Extension to cellular/OPS allows users to receive and place office calls anywhere, any time. People calling into an office telephone can reach users even if they are not in the office. Users could receive the call on their cell telephone, for example.

This added flexibility also allows them to use certain Communication Manager features from a telephone that is outside the telephone network.

Previous versions of Extension to Cellular allowed for office calls to be extended to the cell telephone of a user. Also, calls from the cell telephone would appear as if the call originated from the user office telephone when calling another telephone on the same call server. Certain features within Communication Manager are available from the cell telephone. These features are still available.

In previous versions of Extension to Cellular, cell telephones had to be administered as XMOBILE stations. This is no longer necessary with Communication Manager Release 2.0.

If you had administered Extension to Cellular in earlier releases of Communication Manager, you do not have to change the administration to continue using Extension to Cellular features. It still works. However, users would not have the full range of features that are now possible with Extension to Cellular/OPS.

You can gain multi-country switch access by administering multiple sets of Feature Name Extension (FNE). You can have one Communication Manager system with different gateways in multiple locations. Each gateway can have its own FNE set.

In addition, Communication Manager supports the ability for Public Fixed Mobile Convergence (PBFMC) calls appear to be on the same location as a user's desk set and not the gateway that supports incoming trunks. The same location based dialing rules can be used to ensure that the same ARS and route patterns are used for calls in the same location.

Communication Manager also supports the use of the Confirmed Answer option for cellular voice mail avoidance for any OPTIM application, including EC500. With Confirmed Answer, upon answering the phone, the user hears the dial tone. The user must then press one of the digits on the cellular phone's keypad. Until the system receives a digit, the system does not treat the call as answered.

There are several uses for Confirmed Answer:

- 1 In some businesses with the use of EC500 (such as for after hours support), it is critical that a call be treated as answered only if a person answers the call. In such a scenario, Confirmed Answer is the only reliable voice mail avoidance method.
- 1 Since Confirmed Answer is the most reliable form of cellular voice mail avoidance, some users may be willing to use the feature with PBFMC. An added benefit of the feature is that the dial-tone is a signal to the user that this is a business call, not a personal call.

Communication Manager provides the following Extension to Cellular features:

- 1 Conditional Call Extending (controls which type of calls to extend when EC 500 is enabled)
- 1 Shared Voice Connections (allows two voice calls to share a single trunk connection between the cell phone and the PBX)
- 1 Sharing Mappings among CM PBXs (allows the station name and station mapping information to be across multiple Communication Managers)
- 1 SPFMC OPTIM Application (enables support for dual-mode cell phones)
- 1 One-X Mobile Server and Application Support (allows use of one-X server to configure and control a set of features; each extension can support four one-X applications)

Off-PBX station

The off-PBX station (OPS) application type is used to administer of a SIP telephone. OPS cannot be disabled using the Extension to Cellular enable/disable feature button.

Note:

A 4602 SIP telephone must register with the SIP proxy regardless of whether OPS is administered.

The Extension to Cellular/OPS application allows for many of the parameters used for the original Extension to Cellular application to be ported onto one of several DCP and IP station types. From a call processing perspective, Extension to Cellular/OPS is in fact dealing with a multi-function telephone, whereas the previous Extension to Cellular implementation utilized one or two XMOBILE stations that behaved like analog station types.

The Extension to Cellular/OPS application has its own documentation set. For a complete list of Extension to Cellular/OPS documentation, see your Avaya representative.

E911 ELIN for IP wired extensions

This feature automates the process of assigning an emergency location information number (ELIN) through an IP subnetwork ("subnet") during a 911 call. The ELIN is then sent over either CAMA or ISDN PRI trunks to the emergency services network when 911 is dialed. This feature properly identifies locations of wired IP telephones that call an emergency number from anywhere on a campus or location.

Note:

This feature depends upon the customer having subnets that correspond to geographical areas.

This feature works for both types of IP endpoints:

- ┆ H.323
- ┆ SIP

A caller who needs emergency assistance dials a Universal Emergency Number - for example, 911 in the United States, 000 in Australia, and 112 in the European community. The call routes through a local Central Office, through an emergency tandem office, to the appropriate Public Safety Answer Point (PSAP). The PSAP answers the call.

A typical tandem office can route the call to a PSAP within at most four surrounding areas. (In the US, that translates to four surrounding area codes.) If the PSAP that receives the call is not the correct one to handle the emergency, the PSAP might be able to transfer the call to the correct PSAP. Such transfers can only occur between geographically adjacent or nearby PSAPs.

Each PSAP usually covers one city or one rural county. At the PSAP, emergency operators determine the nature of the emergency and contact the appropriate agency: police, fire, ambulance, etc. A single PSAP is usually responsible for an area covering several independent police and fire departments in the United States.

With Enhanced 911 (E911), the system might send to the emergency services network the Calling Party Number (CPN) with the call over Centralized Automatic Message Accounting (CAMA) trunks or through the Calling Number IE over ISDN trunks. A system at the PSAP uses the CPN to look up the documented street address location of the caller from the Automatic Location Information (ALI) database. The ALI database is usually owned and managed by Local Exchange Carriers. Many enterprise customers choose to contract with a third party to update the ALI database for them.

This depends on the assumption that a CPN always corresponds to the street address that the system owner arranged to have administered into the ALI database. This assumption is not always true.

- l Users who have H.323 IP telephones can move them without notifying the system administrator.
- l Users who have SIP IP telephones can use the same extension number simultaneously at several different telephones.

Without this feature, if these users dial 911, the emergency response personnel might go to the wrong physical location. With this feature, the emergency response personnel can now go to the correct physical location. In addition, emergency response personnel can now go to the correct physical location if a 911 emergency call comes from a bridged call appearance.

E911 device location for IP telephones

Communication Manager works with an E911 Manager device from RedSky Technologies. This third-party E911 Manager provides a flexible, complete, and automated E911 management system for customers who want to implement voice over IP (VoIP) telephony. The E911 Manager from RedSky Technologies works with Communication Manager release 2.1 and beyond to keep the Automatic Location Information (ALI) record for each extension correct. The E911 Manager also provides notification whenever someone moves an IP endpoint to a new subnet.

Personal Station Access

The Personal Station Access (PSA) feature allows you to transfer your telephone station preferences and permissions to any other compatible telephone. This includes the definition of telephone buttons, abbreviated dial lists, and class of service, and class of restrictions permissions.

PSA has several telecommuting applications. For example, several telecommuting employees can share the same office on different days of the week. The employees can easily and remotely make the shared telephone “theirs” for the day.

PSA association and dissociation are enhanced by Hot Desking. For more information, see [Hot Desking Enhancement](#) on page 209.

Do not answer reason code

The Personal Station Access (PSA) feature uses Administration Without Hardware (AWOH), a feature that allows the system administrator to assign a telephone without specifying a physical port. For example, use “X” as the port. If a telephone is disassociated, it means that it is not currently mapped to a particular physical telephone, such as a digital telephone. If a caller dials

into an extension that is currently disassociated, they are provided a message that indicates “Don’t answer” instead of “Busy”.

Name/number permanent display

When a person uses PSA to associate their extension with a station, a display appears on the station indicating their name and extension number. This information is displayed until the user disassociates their extension from the station using the PSA-disassociate feature access code.

Seamless Converged Communication Across Networks

The SCCAN (Seamless Converged Communication Across Networks) program consists of the joint collaboration of three companies, Motorola, Proxim, and Avaya. The purpose of SCCAN is to create and deploy a converged cellular Wireless Local Area Network (WLAN), and Internet Protocol (IP) Telephony services that delivers new levels of communications mobility and network connectivity.

The SCCAN system consists of new products including:

- ┆ A Wi-Fi/cellular dual-system telephone from Motorola (sometimes referred to as the Subscriber Unit)
- ┆ Session Initiation Protocol (SIP)-enabled IP Telephony software from Avaya (most often referred to as Communication Manager SIP Trunking)
- ┆ IPSec security client from Avaya (VPNRemote) that runs on the Motorola handset
- ┆ Light Access Points (LAPs) that are developed by Proxim

SIP Visiting User

The SIP Visiting User (SIP VU) feature enables users with the 9620 or 9630 SIP telephone to log in to any SIP telephone in the enterprise and receive their own individualized services, including menus, contacts, and buddy lists. When a SIP Visiting User makes an emergency call, the call is routed to the local emergency personnel closest to the visited site, not the user’s home site.

The SIP Visiting User feature relies on specialized firmware on the telephone, and also requires SIP VU administration.

SIP Visiting Users can be roaming or non-roaming.

- 1 Non-roaming visiting user - If a visiting user is non-roaming, the user is logged into a visiting phone that is served by the user's usual SIP Enablement Services (SES) home server. For example, a non-roaming visiting user logs into a phone that is in the office adjacent to their primary phone. No special connections need to be made to serve up the contacts, permissions, and buddy list the non-roaming visiting user expects.
- 1 Roaming visiting user - If a visiting user is roaming, the visiting user is logged into a phone that uses a SES home server that is different from the visiting user's home SES. During registration, the roamed-to SES home server retrieves the user's credentials from the SES data service as the means to enable roaming for that user. This causes the user's home SES to flag the user as roaming.

Terminal Translation Initialization

Communication Manager provides Terminal Translation Initialization (TTI), a feature that works with Administration Without Hardware (AWOH). TTI associates the terminal translation data with a specific port location through the entry of a special feature-access code, a TTI security code, and an extension number from a terminal that is connected to a wired (but untranslated) jack.

TransTalk 9000 digital wireless system

The TransTalk 9000 is a single-zone or dual-zone, in-building wireless system that provides a mobility solution on Communication Manager-based systems. It delivers the benefits and accessibility of a wireless telephone with all the power and functionality of a wired desk telephone.

X-station mobility

X-station mobility allows remote users to access switch features. That is, X-station mobility allows certain OEM wireless telephones remoted over a PRI trunk interface to be controlled by Communication Manager as if the telephones were directly connected to the switch.

The telephones are administered to be of the type XMOBILE and have additional administration information on the **Station** screen that assigns the capabilities of a remote station to the associated PRI trunk group. The wireless telephones thus have access to such features as call-associated display, bridging, message waiting, call redirection, and so forth.

Mobility

X-station mobility is currently used for non-cellular wireless offers (DECT and PHS) in EMEA and APAC regions, and the Extension to Cellular offer globally.

Chapter 11: Port network and gateway connectivity

Asynchronous Transfer Mode

The Asynchronous Transfer Mode (ATM) switch is a replacement option for the CSS or the direct-connect switch. Several Avaya ATM switch types can provide Communication Manager port network connectivity. Non-Avaya ATM switches that comply with the ATM standards set by the European Union can also provide Communication Manager port network connectivity.

Port Network Connectivity

ATM Port Network Connectivity (ATM-PNC) provides an alternative to the Center Stage Switch (CSS) configurations for connecting the Processor Port Network (PPN) to one or more Expansion Port Networks (EPN). ATM-PNC replaces the CSS in a DEFINITY R8r and later network with an ATM switch or network. ATM-PNC is available with all three Communication Manager reliability options - standard, high, and critical. In addition, it offers ATM-PNC duplication.

ATM-PNC integrates delivery of voice, video, and data via ATM over a converged large bandwidth network, providing reduced infrastructure cost and improved network manageability. ATM-PNC uses standards-based open interfaces that can be provisioned with either new or existing systems running Communication Manager.

Port Network Connectivity over WAN

ATM-PNC over a public Wide Area Network (WAN) represents an environment where the customer uses a service provider's ATM network between privately-owned ATM switches. The customer does not control the ATM switches in the network, including traffic policing policies and product quality.

Using a public WAN, Permanent Virtual Paths (PVP) may be set up between customer-owned ATM switches similar to the dedicated circuits in a private WAN. However, ATM cell processing occurs in a public WAN so the customer is dependent on ATM switches owned and managed by the service provider.

Switched Virtual Circuits (SVC) use the ATM protocol to transmit voice-like applications over ATM networks. The advantage of the SVC solution is that Communication Manager can dynamically signal the ATM network to provide more bandwidth as needed to handle peaks in the call traffic. If the ATM network cannot handle the additional traffic, calls will be denied.

Circuit switched

Center Stage Switch

Communication Manager supports CSS as a method to interface between the PPN and EPNs using circuit switched technology to carry the voice traffic.

Center Stage Switch separation

Avaya 8XXX Servers in an Avaya MCC1, SCC1, or G650 Media Gateway configuration, with four or more Port Networks (PN), use a Center Stage Switch (CSS) to interconnect the PNs.

The Center Stage Switch (CSS) separation feature allows for the physical separation of redundant Avaya 8XXX Servers, and their corresponding CSS, to improve their survivability. Avaya 8XXX Servers and the CSS can be separated up to 6.2 miles (10 km), providing backup and survivability for a communications network in one or more remote locations.

Internet Protocol

H.248 media gateway control

Communication Manager uses standards based H.248 to perform call control to Avaya media gateways such as the G700. H.248 defines a framework of call control signaling between the intelligent Avaya 8XXX Servers and multiple “unintelligent” media gateways.

Inter-Gateway Alternate Routing

For single-server systems that use the IP-WAN to connect bearer between port networks or media gateways, Inter-Gateway Alternate Routing (IGAR) provides a means of alternately using the public switched telephone network (PSTN) when the IP-WAN is incapable of carrying the bearer connection. IGAR may request that bearer connections be provided by the PSTN under the following conditions:

- ┆ The number of calls allocated or bandwidth allocated via Call Admission Control-Bandwidth Limits (CAC-BL) has been reached
- ┆ VoIP RTP resource exhaustion in a MG/PN is encountered
- ┆ A codec set is not specified between a network region pair
- ┆ Forced redirection between a pair of network regions is configured

IGAR takes advantage of existing public and private network facilities provisioned in a network region. Most trunks in use today can be used for IGAR. Examples of the better trunk facilities for use by IGAR are:

- ┆ Public or Private ISDN PRI/BRI
- ┆ R2MFC

IGAR provides enhanced Quality of Service (QoS) to large distributed single-server configurations.

Network Region Wizard

For large distributed single-server systems that have multiple network regions, the Network Region Wizard (NRW) simplifies and expedites the provisioning of multiple IP network regions, including Call Admission Control using Bandwidth Limits (CAC-BL) and Inter-Gateway Alternate Routing (IGAR).

IP Port Network Connectivity

Communication Manager allows Control Channel Message Set (CCMS) messages to be packetized over IP LAN and WAN connections to control multiple port networks.

Improved Port Network Recovery from Control Network Outages

The IP-connected port networks experience disproportionately long outages from short network disruptions. The Improved Port Network Recovery feature provides customers using IP connected Port Networks with less downtime in the face of IP network failures.

The feature lessens the impact of network failures by:

- 1 Improving TCP recovery times that increase the IPSI-CM connection bounce coverage time from the current 6-8 seconds range for the actual network outage to roughly 10 seconds. Results vary based on traffic rates.
- 1 Modifying the IPSI recovery action after a network outage to be a warm interrupt rather than a IPSI application reset (hardware interrupt)). This prevents H.323 IP telephones from having to re-register and/or have their connections regenerated. This minimizes recovery time from network outages in the range of 15-60 seconds.

This feature also monitors the IPSI-CM connection and helps in identifying and troubleshooting network related problems.

Link Recovery

IP calls must have an H.248 link between the Avaya G700 Media Gateway and the call controller. The H.248 link between an Avaya server running Communication Manager and the Avaya media gateway provides the signaling protocol for:

- 1 Call setup
- 1 Call control (user actions such as Hold, Conference, or Transfer)
- 1 Call tear-down

If the link fails for any reason, the Link Recovery feature preserves any existing calls and attempts to re-establish the original link. If the gateway cannot reconnect to the original server, then Link Recovery automatically attempts to connect with alternate TN799DP (CLAN) circuit packs within the original server configuration or to a Local Spare Processor (LSP).

Link Recovery does not attempt to recover or overcome any network failure that created the link outage. Link Recovery also does not diagnose or repair the network failure that caused the link outage.

Since there is no communication possible between the Media Gateway and call controller during a link outage, button depressions are not recognized, feature access does not work, and neither does any other type of call handling. In essence, the system is unresponsive to any stimuli until the H.248 link is restored. This might be the only indication that a Link Recovery is in process.

CAUTION:

If an administrator attempts to add a telephone to a gateway while that gateway is in Link Recovery, that station is not put into service when the gateway comes back. If this happens, perform a **busyout/release** command on that telephone when the gateway comes back into service.

Feature highlights:

- ┆ Call signaling channel failures are detected at a fast rate (in the order of 30 seconds, by default).
- ┆ The endpoint has an awareness about the primary and the alternate gatekeepers for the purpose of faster and less disruptive recovery from signaling channel failures.
- ┆ The endpoint attempts to re-establish the signaling channels with the primary gatekeeper while preserving an existing call.
- ┆ An IP endpoint's registration (while it is recovering from a signaling failure) can be accepted while preserving that endpoint's existing call(s).
- ┆ The customer can administer the endpoint recovery parameters (such as timers and gatekeepers).

In order for IP endpoints to take advantage of this feature, the firmware or application software must be updated with the new algorithm that supports the resiliency feature. IP endpoints include IP telephones and IP softphones. However, since the feature provides backward compatibility, it is not mandatory that existing IP endpoints be upgraded.

Separation of Bearer and Signaling

The Separation of Bearer and Signaling (SBS) feature provides a low cost virtual private network with high voice quality for customers who cannot afford private leased lines. SBS provides a DCS+ VPN replacement for those customers needing Dial Plan Expansion (DPE) functionality.

Note:

DCS does not work with six-digit or seven-digit dial plans. Although QSIG does work with six-digit and seven-digit dial plans, QSIG does not work over VPNs.

The SBS feature supports:

- ┆ QSIG private networking signaling over a low cost IP network
- ┆ Voice (bearer) calls over public switched network
- ┆ Association between QSIG feature signaling information and each voice call

You must always use AAR/ARS/UDP to originate an SBS call. You cannot use a Trunk Access Code / Dial Access Code to originate an SBS call.

Proper administration and configuration is required for SBS calls to work correctly. This includes:

- ┆ Fields in the **System-Parameters Features** screen, a field on the **Trunk Group** screen, and a **Station** type called an **SBS Extension** (an extension number without hardware assigned to it that is used to associate the separate bearer and signaling calls).

Port network and gateway connectivity

- | Customers must allocate a sufficient number of SBS extensions based on expected SBS traffic volume. The same applies to SBS trunk group members.
- | Each administered SBS extension must correspond to a DID/DDI number obtained from a local service provider.

Note:

Obtaining a DID/DDI number for each SBS extension is not necessary if the Feature Plus Pseudo DID feature is available.

- | In remote office configurations or other remote gateway configurations with limited direct network access, these DID/DDI numbers should be obtained from a service provider that is local to the controlling gateway server, not local to the remote office/gateway. This eliminates excessive traffic through the remote office/gateway to its controlling gateway server.
- | The **ISDN Public-Unknown Numbering** screen must be correctly administered to map every SBS extension to the corresponding national public network complete number (that is, the DID/DDI number). This screen is used to develop the complete number even if the incoming SBS trunk group numbering format is administered for private numbering.

Chapter 12: Trunk connectivity

Asynchronous Transfer Mode

See [Asynchronous Transfer Mode](#) on page 121.

Circuit Emulation Service

ATM-circuit emulation service (ATM-CES) lets Communication Manager emulate ISDN-PRI trunks on an ATM facility. These virtual trunks can serve as integrated access, tandem, or tie trunks.

ATM-CES trunk emulation maximizes port network capacities by consolidating trunking. For example, the CES interface can define up to eight virtual circuits for tie-line connectivity, consolidating onto one circuit card network connectivity that usually requires multiple circuit packs.

CMS measurement of ATM

See [CMS measurement of ATM](#) on page 63.

Circuit switched

DS1 trunk service

Bit-oriented signaling that multiplexes 24 channels into a single 1.544-Mbps stream. DS1 can be used for voice or voice-grade data and for data-transmission protocols. E1 trunk service is bit-oriented signaling that multiplexes 32 channels into a single 2.048-Mbps stream. Both DS1 and E1 provide a digital interface for trunk groups. Digital Service 1 (DS1) trunks can be used to provide T1 or ISDN Primary Rate Interface (PRI) service.

Echo cancellation - with UDS1 circuit pack

The universal DS-1 (UDS1) circuit pack (TN464GP/TN2464BP) available for all Communication Manager platforms has echo cancellation circuitry. The echo cancellation capability of the circuit pack is intended only for channels supporting voice communication. It is not desirable to provide echo cancellation over channels supporting data communication.

The TN464GP/TN2464BP is intended for Communication Manager customers who are likely to encounter echo over circuits connected to the public network. The occurrence of echo is likely if Communication Manager is configured for complex services such as ATM or IP. In addition, echo is likely to occur if Communication Manager interfaces to local service providers who do not routinely install echo cancellation equipment in all their circuits.

E1

Communication Manager also supports E1 connections. T1/E1 access and conversion allows simultaneous connection to both T1 (1.544 Mbps) and E1 (2.048 Mbps) facilities (using separate circuit packs).

T1

When planning your networking requirements, one of the options you should consider is multiplexing over digital services 1 (DS1) facilities.

Separate licensing for TDM stations and TDM trunks

Prior to release 2.0, Communication Manager was sold by licensed ports that included stations and trunks. The system displayed the total of licensed ports in the **Maximum Ports** field on the **Optional Features** screen.

For Communication Manager, Avaya sells licenses for stations, but not for trunks. Currently, the **Maximum Ports** field on the **Optional Features** screen is used for licensing ports, which include both trunks and stations.

In Communication Manager, a separate field, **Maximum Stations**, is created on the **Optional Features** screen to track station licenses only. This helps customers easily identify the number of station licenses on the system.

Internet Protocol

H.323 trunk

A TN802B in MedPro mode or a TN2302AP IP interface enables H.323 trunk service using IP connectivity between two systems running Communication Manager. The H.323 trunk groups can be configured as system-specific tie trunks, generic tie trunks, or direct-inward-dial (DID) public trunks. In addition, the H.323 trunks support ISDN features such as QSIG and BSR.

Improved button downloads

The improved button download to IP endpoints feature greatly reduces the time needed for button labels to be sent to the IP telephone upon a new registration. This feature also reduces the traffic being sent to the IP telephones when button labels have not changed on a reregistration.

The Avaya H.323-based IP telephones request whether they need feature button information when they send the RRQ message to the Communication Manager server during registrations or re-registrations. If the IP telephones request the button information, or if Communication Manager is aware of an administration change that occurred to change button information, Communication Manager then downloads that button information (including the labels) in the RCF message back to the telephone. This process does not rely on background maintenance sending down the labels in CCMS messages, or on NSM messages after registration. If the IP telephones did not request the button information (due to a re-registration), and no recent administration changes in the button information had occurred, Communication Manager does not include any button information in the RCF message. The IP telephones use the labels they already have in memory.

Increased trunk capacity

Communication Manager trunk capacities, which include all IP and TDM trunk types, are increased from 8,000 to 12,000 for any single Communication Manager server within a configuration. With an Avaya S8730 or S8720 server in an XL configuration, Communication Manager trunk capacities support 12,000 trunks, multiplied by the number of Communication Manager servers. The maximum trunk capacity is 96,000 (12,000 trunks x 8 Communication Manager servers). For information on trunk capacities, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

IP loss groups

A primary reason to accomplish a loss plan for voice communication systems is the desire to have the received speech and tone loudness at a comfortable listening level. This should be accomplished so that users can listen to each other without being concerned who or where the remote party is, or what kind of telephone equipment each may be using.

A connection with an end-to-end loss (called an Overall Loudness Rating) of 10 dB - which approximates a normal conversation between a talker and listener spaced one meter apart - provides a high degree of satisfaction for the majority of users. Therefore, voice communication standards for end-to-end loss are based on this number.

Communication Manager has now defined two additional loss groups for IP telephony. The purpose of these two loss groups is to set speech and tone loudness separately for IP connections. These loss groups use country-specific gateway loss plans.

The two IP loss groups are:

- ┆ Loss Group 18: IPtrunk - loss group for IP trunks (IP Carrier Medium)
- ┆ Loss group 19: IPphone - loss group for IP terminals (IP ports)

On an upgrade, if the default for an IP station loss plan is 2, and the IP trunk loss plan is 13, Communication Manager changes the defaults to 19 and 18 respectively.

IP trunks

IP trunk groups may be defined as virtual private network tie lines between systems or ITS-E servers running Communication Manager. Each IP trunk circuit pack provides a basic 12-port package that can be expanded up to a total of 30 ports. The number of ports that are defined will correspond to the total number of simultaneous calls transmitted over the IP trunk interface.

The benefits of IP trunk include a reduction in long distance voice and fax expenses, facilitating global communications, providing a full function network with data and voice convergence and optimizing networks by using the available network resources.

IP trunking is a good choice for basic, corporate voice and fax communications, where cost is a major concern. IP trunk calls travel over a company intranet rather than the public telephone network. So, for the most common types of internal corporate communications, IP trunks offer considerable savings.

IP trunking is usually not a good choice for applications where calls have to be routed to multiple destinations (as in most conferencing applications) or to a voice messaging system. IP trunk calls are compressed to save network bandwidth. Repeated compression and decompression results in a loss of data at each stage and degrades the final quality of the signal.

The maximum number of compression cycles acceptable on a call is three, and three compression cycles can compromise voice quality. Normal corporate voice or fax calls typically go through fewer than three compression cycles. However, multipoint conference calls and most voice messaging systems add too many compression cycles for acceptable quality.

IP trunk fallback to PSTN

The PSTN fallback of IP trunks feature refers to bypassing, or skipping over, IP trunks when IP network conditions make the voice quality of IP trunks unacceptable. The skipping over of IP trunks allows existing route patterns to look at secondary trunk groups for outgoing calls. When these secondary trunk groups are not IP, the PSTN fallback feature applies. The key to the existing implementation is the evaluation of the current network condition.

Evaluation data is obtained from ICMP PING packets that are generated from the TN2302/TN2602 media processor circuit packs. Reports are generated from the circuit packs that aggregate many individual ICMP PING requests.

The existing family of H.248 media gateways (G250, G350, and G700) do not provide this functionality. In systems which do not contain TN media processors, or where those media processors don't have access to the network regions that are reachable by H.248 gateways, there is no PSTN fallback capability for IP trunks in the event of network degradation.

The PSTN fallback for IP trunks feature for H.248 media gateways resolves this problem.

IP trunk link bounce

H.323 trunk link bounce provides customers with fewer call failures in the event of an IP network failure or disruption. This feature lessens the impact of IP network failures and disruptions by postponing corrective action after an H.323 signaling link failure. When a failure is detected, Communication Manager initiates a timer to allow time for the network to recover. If the network does recover within that period, calls are allowed to continue without interruption.

Session Initiation Protocol

Session Initiation Protocol (SIP) is a signalling protocol used for establishing sessions in an IP network.

SIP has a separate set of documentation. For more information on SIP, click the **documentation** link from the <http://www.avaya.com> Web site.

SIP trunks

SIP trunking functionality allows a Linux server to function as a POTS gateway between traditional legacy endpoints (stations and trunks) and SIP endpoints. It also provides SIP to SIP routing. In the routing scenario, the server supports call routing similar to what a SIP proxy would provide.

SIP links can be secured using TLS to encrypt signaling, and use Digest Authentication to perform validation. When using TLS, the Media Encryption feature is also available to encrypt audio channels.

SIP trunking functionality:

- 1 Provides access to less expensive local and long distance telephone services, plus other hosted services from SIP service providers
- 1 Provides presence and availability information to members of the enterprise and authorized consumers outside the enterprise, including other enterprises and service providers
- 1 Facilitates SIP-enabled converged communications applications within the enterprise, such as the Seamless Service Experience.

Allowing encryption of signaling and audio channel provides the customer with the option to provide a secure communications infrastructure. See [Signaling encryption for SIP trunks](#) on page 206.

Auxiliary trunks

Auxiliary trunks connect devices in auxiliary cabinets with Communication Manager. Some of the features that are supported with this type of trunk are recorded announcements, telephone dictation service, malicious call trace, and loudspeaker paging.

Advanced Private Line Termination

Provides access to and termination from CO (Central Office)-based private networks; namely, Common Control Switching Arrangements (**CCSA**) and Enhanced Private Switched Communications Service (**EPSCS**).

APLT trunks are physically the same as those used for analog tie trunks, where the trunk signaling is compatible with **EPSCS** and **CCSA** network switches. The outgoing **APLT** trunk repeats any number of digits to the private network as dialed. **APLT** trunks can tandem through the **PBX** from **EPSCS** network only; **CCSA** networks require an Attendant to complete the call.

Central Office

Central Office (CO) trunks connect Communication Manager to the local central office for incoming and outgoing calls.

Central Office support on G700 Media Gateway - Russia

See [Central Office support on G700 Media Gateway](#) on page 97.

Digital multiplexed interface

The digital multiplexed interface feature supports two signaling techniques: bit-oriented signaling and message-oriented signaling for direct connection to host computers.

Digital multiplexed interface offers two major advantages:

- ┆ digital multiplexed interface delivers a standard, single-port interface for linking host computers internally and externally through a T1 carrier.
- ┆ Since it is compatible with ISDN standards and is licensed to numerous equipment manufacturers, digital multiplexed interface promotes multi-vendor connectivity.

Communication Manager supports two versions of digital multiplexed interface, each differing in the way information is carried over the 24th channel:

- ┆ Bit-oriented signaling
- ┆ Message-oriented signaling

Bit-oriented signalling

Digital multiplexed interface bit-oriented signalling carries framing and alarm data and signalling information for connections to host computers and other vendor equipment.

Message-oriented signalling

Digital multiplexed interface message-oriented signalling, fully compatible with ISDN-PRI, uses the same message-oriented signalling format - link access procedure on the D-channel - as ISDN-PRI for control and signalling. These signalling capabilities extend the advantages of

digital multiplexed interface message-oriented signalling multiplexed communications to the public ISDN network.

Direct Inward Dialing

Direct Inward Dialing (DID) trunks connect Communication Manager to the local central office for incoming calls dialed directly to stations without attendant assistance.

Direct Inward/Outward Dialing

Traditionally, Central Office (CO) trunks and Direct Inward Dialing (DID) trunks interface an attendant console with a central office. A CO trunk services outgoing calls and accepts incoming calls that are terminated at the attendant. A Direct Inward/Outward Dialing (DIOD) trunk is used for calls that need to be terminated without an attendant interaction.

E&M signaling - continuous and pulsed

See [E&M signaling - continuous and pulsed](#) on page 98.

E911 CAMA trunk group

This screen administers the Centralized Automatic Message Accounting (CAMA) trunks and provides Caller Emergency Service Identification (CESID) information to the local enhanced 911 system through the local central office.

Foreign Exchange

Foreign Exchange (FX) trunks connect Communication Manager to a Central Office other than to the local office.

ISDN trunks

Gives you access to a variety of public and private network services and facilities. The ISDN standard consists of layers 1, 2, and 3 of the Open System Interconnect (**OSI**) model. Systems running Communication Manager can be connected to an ISDN using standard frame formats: Basic Rate Interface (BRI) and the Primary Rate Interface (PRI).

An **ISDN** provides end-to-end digital connectivity and uses a high-speed interface that provides service-independent access to switched services. Through internationally accepted standard interfaces, an **ISDN** provides circuit or packet-switched connectivity within a network and can link to other **ISDN** supported interfaces to provide national and international digital connectivity.

Automatic Termination Endpoint Identifier

The user side will support automatic TEI assignment by the network. Both fixed and automatic TEI assignment will be supported on the network side.

Call-by-call service selection

Enables a single ISDN-PRI trunk group to carry calls to a variety of services, rather than requiring each trunk group to be dedicated to a specific service. It allows you to set up various voice and data services and features for a particular call.

ETSI functionality

The full set of ETSI public-network and private-network ISDN features is officially supported. This includes Look-Ahead Interflow (LAI), look-ahead routing, and usage allocation.

Also included is all QSIG supplementary services, such as:

- | Name identification
- | Call diversion (including rerouting)
- | Call transfer
- | Path replacement

ETSI functionality does not include:

- | DCS
- | Non-facility associated signaling

Trunk connectivity

- ┆ D-channel backup
- ┆ Wideband signaling

ETSI completion of calls

The auto-callback feature known as ETSI Completion of Calls to Busy Subscriber (CCBS) and on No Reply (CCNR) works over the DSS1 network. An analog phone activates this feature by dialing the FAC. A multi-appearance voice terminal can use either the FAC or programmed buttons. By pressing an idle Automatic Callback button, a caller can activate either the SS-CCBS when the called station is busy, or the SS-CCNR when the called station does not answer.

The originating caller receives a callback when:

- ┆ The busy station becomes available after the user hangs up.
- ┆ An unanswered station becomes available after it is used for another call and then hangs up.

The call-back feature expires after a period of 40 minutes.

Facility and non-facility associated signaling

Facility and non-facility associated signaling allows an **ISDN-PRI DS1/E1** interface D-channel to carry signaling information for B-channels (voice or data). D-Channel Backup can also be administered to increase system reliability.

Feature plus

Feature plus enables those users without DID service to direct dial users on a remote PBX through the public network. ISDN feature plus eliminates the need for attendant intervention for those without DID capabilities.

ISDN-Basic Rate Interface

Enables connection of the system to equipment or endpoints that support an Integrated Services Digital Network (ISDN) by using a standard format called the Basic Rate Interface (BRI). This feature is a 192-Kbps interface that carries two 64-Kbps B-channels and one 16-Kbps D-channel.

ISDN is a global access standard that uses a layered protocol. It eliminates the need for multiple, separate access arrangements for voice, data, facsimile, and video services and

networks. Using the same pair of wires that carry simple telephone calls, ISDN can deliver voice, data, and video services in a digital format.

The ISDN-BRI Trunk circuit pack allows Communication Manager to support the T interface and the S/T interface as defined by ISDN standards (ITU-T recommendation I.411). The circuit pack provides eight ports to the network and supports two B channels and one D channel.

The ISDN-BRI Trunk provides the following advantages:

- ┆ Provides an inexpensive way to connect to ISDN services provided by the network provider
- ┆ Meets almost all ETSI Country protocol requirements
- ┆ Supports essential (not supplementary) ISDN services

BRI trunks support public-network access outside the U.S. on point-to-midpoint connections, with the restriction that Communication Manager must not be configured in a passive bus arrangement with other BRI endpoints. ISDN-BRI trunks can be used as inter-PBX tie lines using the QSIG peer protocol. See [Figure 4: Communication Manager and ISDN](#) on page 138.

Figure 4: Communication Manager and ISDN

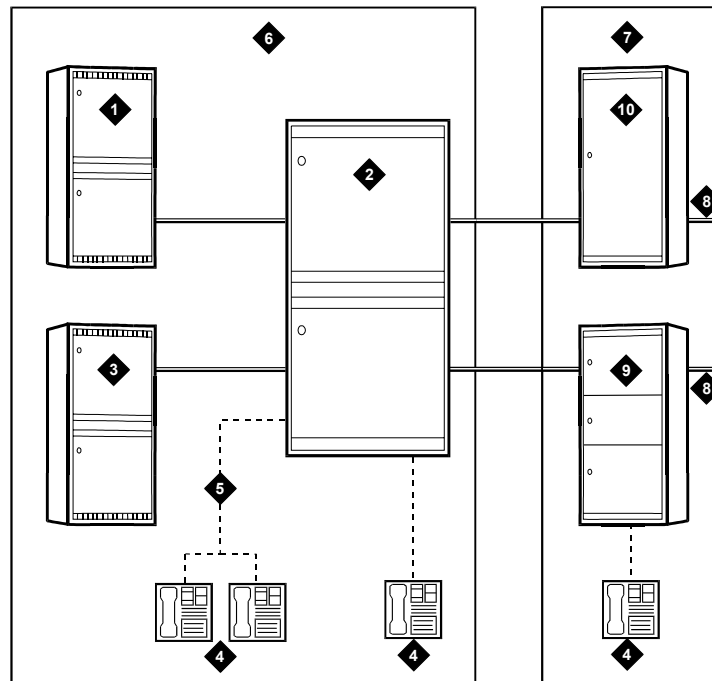


Figure notes:

- | | |
|-----------------------------------------|-----------------------------------------------|
| 1. System running Communication Manager | 6. Private ISDN (can be carried over ATM-CES) |
| 2. System running Communication Manager | 7. Public ISDN (can be carried over ATM-CES) |
| 3. System running Communication Manager | 8. Public and private networks |
| 4. Basic rate interface telephone | 9. Central office switch |
| 5. Passive bus | 10. Tandem switch |

Multiple subscriber number - limited

The ISDN standard MSN feature lets customers assign multiple extension to a single BRI endpoint. The MSN feature works with BRI endpoints that allow the channel ID IE to be encoded as “preferred.”

NT interface on TN556C

Communication Manager supports the NT (network) side of the T interface using the TN556C circuit pack. This gives the switch full tie trunk capability using BRI trunks. Communication Manager supports leased BRI connections through the public network, with a TN2185 on each end of the leased connection. Communication Manager will not, however, allow customers to administer both endpoints and trunks on the same TN556C circuit pack.

Presentation restriction

Restricts the display of calling/connected numbers over ISDN trunks. ISDN trunk groups can be administered to control the display of calling/connected numbers. Each trunk group can be administered to display “presentation restricted,” “number no available due to networking,” or an administered text string instead of the calling/connected number.

Wideband switching

Provides the ability to dedicate two or more **ISDN** B-channels or **DSO** endpoints for applications that require large bandwidth. Certain applications, such as video conferencing and high-speed data transmission, require extra bandwidth and it becomes necessary to put several ISDN-PRI narrowband channels into one wideband channel to accommodate the needs of these applications.

This feature supports both European and North American standards.

Multi-Frequency Packet signaling - Russia

See [Multi-Frequency Packet signaling](#) on page 97.

National private networking support - Japan

See [National private networking support](#).

Personal Central Office Line

Provides a dedicated trunk circuit between multi-appearance telephones and a CO or other switch via the network.

Release Link Trunks

Release Link Trunks (RLT) are used between switch locations to provide centralized attendant service or automatic call distribution group availability.

Remote access trunks

Tie trunks

Tie trunks carry communications between Communication Manager and other switches in a private network. Several types of trunks can be used, depending on the type of private network you establish.

Timed automatic disconnect for outgoing trunk calls

This feature provides the capability to automatically disconnect an outgoing trunk call after an administrable amount of time. The amount of time that can elapse before the trunk is dropped can be specified, and can vary between 2 and 999 minutes. If the timer field is blank (the default value), the feature is disabled and the trunk will not be automatically disconnected.

Timed call disconnection applies to all outgoing trunk calls initiated by a party belonging to a specified Class of Restriction (COR).

The outgoing trunk disconnect timer only affects outgoing public network trunks (CO, DIOD, FX, WATS, and ISDN public-network).

Note:

The outgoing trunk disconnect timer should be administered to a value large enough to provide users with adequate response time.

The outgoing trunk disconnect timer does not apply to outgoing trunk calls that are emergency or service calls. Specifically, the outgoing trunk disconnect timer does not apply to calls with ARS call types `alrt`, `emer`, `nsvc`, `op`, `svcl`, `svfl`, `svct`, or `svft`.

The outgoing trunk disconnect timer starts after the outgoing trunk call is answered. The outgoing trunk call is considered answered if:

- ┆ the network provides an answer supervision line signal
- ┆ an ISDN CONNect message is received
- ┆ the Answer Supervision Timeout timer expires
- ┆ the call classifier classifies the call as answered
- ┆ the Outgoing End of Dial Timer expires

Prior to disconnecting the trunk, warning tones are applied to all parties on the call. The first warning tone occurs when one minute remains on the call. The second warning tone occurs when 30 seconds remain on the call.

Wide Area Telecommunications Service

Wide Area Telecommunications Service (WATS) trunks allow you to place long-distance outgoing voice-grade calls to telephones in defined service areas. The calls are priced according to distance in the service area, length of the call, time of day, and the day of the week.

Chapter 13: Public Networking and connectivity

Caller ID on analog trunks

Caller ID on analog trunks allows the system to accept calling name information from a Local Exchange Carrier (LEC) network that supports the Bellcore calling name specification. The system can send calling name information in the format if Bellcore calling name ID is administered.

Caller ID on digital trunks

In the United States, the telephone of a user displays calling party information (if the telephone is a display telephone). Name and calling number are available from the US central offices.

This feature may be used in countries that comply with either US. The display of name and number will work with all Communication Manager digital telephones (DCP and BRI) equipped with a 40-character or a 32-character alphanumeric display.

DS1 trunk service

See [DS1 trunk service](#) on page 127.

Echo cancellation - with UDS1 circuit pack

See [Echo cancellation - with UDS1 circuit pack](#) on page 128.

E1

See [E1](#) on page 128.

T1

See [T1](#) on page 128.

Flexible billing

See [Flexible billing](#) on page 48.

Local exchange trunks

Local exchange trunks connect Communication Manager to a central office. The following local exchange trunks are some of the types available.

800-service trunks

800-service trunks let your business pay the charges for inbound long-distance calls so that callers can reach you toll-free.

Central Office trunks

See [Central Office](#) on page 133.

Digital Service 1 trunks

See [DS1 trunk service](#) on page 127.

Direct Inward Dialing trunks

See [Direct Inward Dialing](#) on page 134.

Direct Inward/Outward Dialing trunks

See [Direct Inward/Outward Dialing](#) on page 134.

Foreign Exchange trunks

See [Foreign Exchange](#) on page 134.

Wide Area Telecommunications Service

See [Wide Area Telecommunications Service](#) on page 141.

QSIG Supplementary Service - Advice of Charge

The QSIG Supplementary Service - Advice of Charge (SS-AOC) provides the capability to extend the public network charging information, provided by service providers in various countries, into users in a private network. This is done by transiting the charge information from a gateway enterprise system to the end user's enterprise system and desktop display.

This support is for both the AOC-D (charging information during the call), and the AOC-E (charging information at the end of the call).

Chapter 14: Intelligent networking

Avaya VoIP Monitoring Manager

See [Avaya VoIP Monitoring Manager](#) on page 217.

Distributed Communications System protocol

The Distributed Communications System (DCS) protocol allows you to configure two or more switches as if they were a single, large system. DCS provides attendant and voice-terminal features between these switch locations. DCS simplifies dialing procedures and allows transparent use of some of the Communication Manager features. (Feature transparency means that features are available to all users on DCS regardless of the switch location.) For more information, also see [Centralized Attendant Service](#) on page 43 and [Inter-PBX attendant calls](#) on page 39.

Attendant with DCS

Direct trunk group selection

See [Direct trunk group selection](#) on page 39.

Display

See [Display](#) on page 43.

DCS automatic circuit assurance

See [DCS automatic circuit assurance](#) on page 222.

DCS over ISDN-PRI D-channel

Enhances DCS by allowing access to the public network for DCS connections between DCS switch nodes. With this feature (also known as DCS Plus or DCS+), DCS features are no longer restricted to private facilities. The ISDN-PRI B-channel is used for voice communications, and the ISDN-PRI D-channel is used to transport DCS control information.

DCS protocol - Italy

See [Distributed Communications Systems protocol](#) on page 96.

DCS with reroute

Allows a DCS call to be rerouted over a different path if the switch finds a better quality and lower cost route. This feature allows for rerouting the call after a transfer or rerouting during a call. DCS with reroute is similar to the rerouting capabilities used with QSIG.

QSIG/DCS voice mail interworking

See [QSIG/DCS voice mail interworking](#) on page 110.

Electronic Tandem Network

In an Electronic Tandem Network (ETN) - also known as Private Network Access (PNA) - Communication Manager provides a variety of features on a network-wide basis. It allows calls to other systems in a private network. These calls do not use the public network. Instead, they are routed over your dedicated facilities.

Automatic alternate conditional routing

You can control the routing of particular calls using conditional routing. For example, you can limit the number of communications satellite hops (communications satellite links used as trunks) in any end-to-end private network routing pattern. Limiting the number of satellite hops may be desirable for controlling transmission quality or call delay in both voice and data calls.

Trunk signaling and error recovery

The reliability of electronic tandem network calls is improved by allowing a trunk call to be retried on another circuit when signaling failures occur.

- ▮ **tandem switch:** A switch within an ETN that provides the logic to determine the best route for a network call, possibly modifies the digits outputted, and allows or denies certain calls to certain users.
- ▮ **tandem through:** The switched connection of an incoming trunk to an outgoing trunk without human intervention.
- ▮ **Tandem Tie-Trunk Network (TTTN):** A private network that interconnects several customer switching systems.

See also [Port network and gateway connectivity](#) on page 121.

Extension number portability

When employees move within the network, they can retain their extension numbers. The ability to keep extension numbers, and even electronic tandem network and direct inward dialed numbers, when moving to other locations within the company eliminates missed calls and saves valuable time.

Internet Protocol

The capabilities and applications of Communication Manager are extended using IP. Communication Manager IP supports audio/voice over a LAN or WAN, and it ensures that remote workers have access to communication system features from their PCs. Communication Manager also provides standards based control between Avaya 8XXX Server and media gateways allowing communications infrastructure to be distributed to the edge of the network.

The Communication Manager IP engine offers features that enables users to increase the quality of voice communications. The Quality of Service (QoS) feature enables users to administer and download the differentiated services type-of-service value to optimize voice quality. The QoS feature reduces latency by implementing buffers in the audio-processing board, and assists some routers in prioritizing audio traffic.

Communication Manager IP also includes hairpin and IP-IP direct connections, two features that make voice communications more efficient. These features increase the efficiency of voice communications by reducing both per port costs and IP bandwidth usage.

IP solutions supports trunks, IP communications devices, IP port networks, and IP control for media gateways. IP solutions is implemented using various IP-media processor circuit packs inside the servers or the Avaya media gateways. The IP media processors provides H.323 trunk connections and H.323 voice processing for IP telephones. The features that use the IP media processor also require the CLAN circuit pack or native processor ethernet connectivity.

The IP LAN can also connect through VPN and WAN facilities to extend the customer IP network across geographically disparate locations. Distributed communication services (DCS+), or QSIG services, can extend feature transparency, centralized voice mail, centralized attendant service, call center applications, and enhanced call routing across IP trunks.

Note:

To maximize voice quality using IP, you must consider both your hardware and network configurations. For example, with IP softphones, you can send the audio over traditional circuit switch lines, providing high quality voice, or over IP using LAN connections. The IP network must be a switched ethernet infrastructure and have the appropriate engineering to accommodate bandwidth, latency and packet loss requirements to effectively provide for real-time voice over IP traffic.

Alternate gatekeeper and registration addresses

When an IP endpoint (including softphones, IP telephones, and Avaya R300) registers with the switch, the switch sends back an IP registration address. The switch sends a different IP address for each registration according to a cyclic algorithm.

If registration with the original CLAN circuit pack IP address is successful, the switch sends back the IP addresses of all the CLAN circuit packs in one network region, not including interconnected regions. These CLAN addresses are called gatekeeper addresses. These addresses can also be used if the call signaling on the original CLAN circuit pack fails.

Note:

On switches using the LAN region based on IP Address feature, it is likely that the network region number assigned to an IP telephone would be different from the network region number of the TN799 that the telephone is registering through. That difference would mean the list of TN799 addresses in the same network region as the IP telephone would be empty. The alternate gatekeeper feature would send a blank list to the IP telephone.

To prevent that from happening, an IP terminal registers with Communication Manager. Communication Manager then sends to the endpoint the IP addresses of the CLANs in the same region as the terminal, followed by network regions interconnected with the network region of the terminal.

If the network connection to one CLAN circuit pack fails, the IP endpoint re-registers with a different CLAN. Alternate gatekeeper and registration addresses, and CLAN circuit pack load sharing, spread IP endpoint registration across more than one CLAN circuit pack, increasing performance and reliability.

Classless Interdomain Routing

Classless Interdomain Routing (CIDR) is a redefinition of the subnet mask, allowing for the aggregation of contiguous classful networks under a single network definition. This allows for more efficient routing table management when administering IP address on Communication Manager.

Multiple network regions per CLAN

Multiple network regions per CLAN enables a single CLAN to provide registration and call control to IP endpoints in multiple network regions. Communication Manager implements this approach by allowing IP addresses to be mapped to network regions in a mapping screen, instead of just to a CLAN. When an IP telephone registers, the switch determines the telephone's network region number based on the telephone's IP address.

Multiple location support for network regions

Multiple location support for network regions allows remote Avaya media gateways connected to a central Avaya 8XXX Server to retain:

- ┆ Local user time
- ┆ Local ARS public analysis tables for local trunking
- ┆ Automatic daylight savings time
- ┆ Local touch tone receivers for IP communications devices, such as Avaya IP telephones.

Communication Manager allows administrators to map locations to IP network regions.

Daylight Savings Time rules change

Communication Manager is updated to comply with the new Daylight Saving Time (DST) in the U.S. DST is extended beginning in 2007. DST now starts the second Sunday of March, and ends on the first Sunday of November.

Network regions

Network regions provide the administrative foundation on which Communication Manager features are allocated to IP endpoints. A network region is a collection of IP endpoints and switch IP interfaces interconnected by an IP network.

Endpoints that share network regions typically represent users with common interests. For example, a customer might have two separate small campuses in a large metropolitan area, interconnected by a WAN, and both served by the same server running Communication Manager. Communication Manager allows the customer to define a network region for each campus, and associate each of their CLAN and IP media processor circuit packs with these regions.

Processor Ethernet

The Processor Ethernet interface is one way of connecting VoIP and IP-based devices to Communication Manager. The Processor Ethernet label is the representation of the computer's native ethernet interface inside of the Communication Manager application.

An Enterprise Survivable Server (ESS) and a Local Survivable Processor (LSP) registers with the main server when it is first configured, and every time it receives a file sync from the main server. You do not have to administer the Processor Ethernet interface for registration purposes. The system software enables the use of the Processor Ethernet interface on servers configured as an LSP or and ESS server.



CAUTION:

Do not disable the Processor Ethernet interface on an LSP or an ESS server. Disabling the Processor Ethernet interface disables the LSP or ESS server's ability to register with the main server. The LSP or ESS server will not work if the Processor Ethernet interface is disabled.

You can administer the server where IP endpoints may register through:

- | The Processor Ethernet interface only
- | CLAN interfaces only (requires the configuration to have CLANs)
- | Either the Processor Ethernet interface or specified CLAN interfaces (requires the configuration to have CLANs) That is, both interfaces must be able to be enabled at the same time with some endpoints registering through the Processor Ethernet interface and some through CLANs.

Adjuncts

The following adjuncts are supported for connectivity to the Processor Ethernet interface:

LSP or Simplex ESS

- | CMS
- | CDR
- | Application Enablement Services (AES)

Duplex ESS

- ┆ CDR
- ┆ Messaging
- ┆ SIP Enablement Services (SES)

An adjunct link is established between the LSP or the ESS server. Administration that allows dedicated and shared connections between the adjuncts and the servers must allow for the link to remain active at all times. When the LSP or ESS server is not active, the adjunct does not receive data from that server.

For information on how to administer the adjunct link, see the adjunct documentation that is specific to your adjunct.

Merge of IP Connect and Multiconnect configurations

Communication Manager uses the System Management Interface to configure Avaya 8XXX Servers. You can now choose how to configure each Ethernet Network Interfaces (NIC) based on their network and policies. This feature applies to all Linux-based Communication Manager servers that have more than two Ethernet Network Interfaces (NICs).

A customer can assign the following functions to any server NIC:

- ┆ Enterprise LAN
- ┆ Duplication LAN (duplicated servers only)
- ┆ Control Network A
- ┆ Control Network B (duplicated control networks only)
- ┆ Services Laptop

This feature eliminates all reference to, and the distinction between, S87XX Multi-Connect and IP Connect. Eliminated, too, are all restrictions and rules on Ethernet port assignment except:

- ┆ No other functions may be assigned to the NIC used for the Services Laptop.
- ┆ The duplication LAN must use a gigabit NIC. Avaya highly recommends that no other functions be assigned to the NIC used for duplication.

H.248 and H.323 registration

The system uses the Processor Ethernet interface to register H.248 gateways and H.323 endpoints. In Communication Manager, Processor Ethernet is supported on simplex and duplex servers for connection of H.323 devices, H.248 gateways, SIP trunks, and most adjuncts.

S8500 Servers

With the increased functionality of the Processor Ethernet interface, the role of the S8500 Server has been expanded. This expansion includes an S8500 configured as an LSP, and an S8500 configured as a main server in an IP configuration with no port networks.

Quality of Service

By employing a variety of Quality of Service (QoS) features, Communication Manager provides the best possible end-to-end audio experience when all or part of the audio path is carried over packet facilities. “Best” in this context is defined by the customer as represented by the system administrator, and represents a trade-off between audio reproduction quality, audio path delay (latency), audio loss, and network resource consumption.

802.1p/Q

IEEE standard 802.1Q and 802.1p provide the means to specify both a Virtual LAN (VLAN) and a frame priority at layer 2 for use by LAN hubs, or bridges, that can do routing based on MAC addresses. 802.1p/Q provides for 8 levels of priority (3 bits) and a large number (12 bits) of VLAN identifiers. The VLAN identifier at layer 2 permits segregation of traffic to reduce traffic on individual links. Because 802.1p operates at the MAC layer, its presence may vary from LAN segment to LAN segment within a single network region. Flexibility requires that 802.1p/Q options be administered individually for each network interface.

Camp-on/Busy-out

A camp-on/busy-out command is commonly used by system technicians to busy-out system resources that need maintenance or repair. Without it, all active calls using those resources are indiscriminately dropped if the resource is physically removed from the system. This disruptive action causes problems for customers, especially when a large number of calls are torn down.

The Camp-on/Busy-out feature for Prowler, MedPRO, and Cruiser adds the ability to remove idle VoIP resources from the system pool of available VoIP resources.

Note:

This feature is not supported by the G700 or G350 Media Gateway platforms.

The Camp-on/Busy-out feature enables the user to select the media processor to be busied-out while the media processor is still in service. After a call ends that was using resources within the specified media processor, the idled resource is removed from the system pool of available resources. Once all of the media processor resources are in a “busy-out” state, the associated board can be removed from the system without disrupting active calls.

Call Admission Control bandwidth management

In order to ensure Quality of Service for Voice over IP calls, there is a need to limit overall VoIP traffic on WAN links. The Call Admission Control (CAC) Bandwidth Management feature of Communication Manager allows the customer to specify a VoIP bandwidth limit between any pair of IP network regions. The feature then denies calls that need to be carried over the WAN link that exceed that bandwidth limit.

CLAN load balancing

CLAN load balancing is the process of registering IP endpoints to CLAN circuit packs (TN799x). Load balancing occurs among CLANs within a network region.

IP endpoint registration among CLAN circuit packs is done through an algorithm. This algorithm tracks the number of sockets being used per TN799x circuit pack, and registers IP endpoints to the TN799x with the most available (unused) sockets. This algorithm applies to H.248, H.323 signaling groups, H.323 stations, and SIP endpoints. Sockets used by adjuncts are not included in the socket count.

Codecs

A codec (coder/decoder) provides the means by which audio is compressed. A codec is typically used in VoIP. Some of the codecs supported by Communication Manager include G.711, G.722, G.723, and G.729.

Differentiated services

With the Differentiated Services (DiffServ) option, the system administrator can administer (by region) and download, to the TN2302AP, the DiffServ Type-Of-Service (TOS) value. This allows data networking equipment to prioritize the audio stream at the IP level to promote voice quality. DiffServ makes use of the TOS octet in the existing IP version 4 header. As such, it may be set by information senders and used by IP (layer 3) routers within the network.

Dynamic jitter buffers

Propagation delay and jitter is caused when a human's voice is sampled, encoded, and packetized for transport over the IP network, but is received and decoded at different rates. Jitter buffers are used to buffer the audio output to smooth the conversions. Communication Manager provides dynamic jitter buffers to balance both delay of conversation and rapid bursts that may occur.

Integration with Cajun rules

Cajun rules provide a central repository for QoS parameters and allows comprehensive QoS management across routers, switches, and endpoints. QoS parameters and policies are

assigned according to network regions on a network region and are distributed through enterprise directory gateway to Communication Manager and to routers and switching devices.

IP overload control

This enhancement more effectively manages processor occupancy overload situations. The enhancement applies selected overload mechanisms at a lower occupancy threshold in an effort to avoid more serious symptoms experienced at higher occupancy levels.

The IP overload control enhancement:

- ┆ fortifies the system against bursts of registration traffic
- ┆ provides a mechanism to alert the far-end to abstain from issuing registrations for some specified period of time
- ┆ records the event to maintain a history of potential performance problems
- ┆ optimizes the maximum number of simultaneous registrations the server can handle based on the available memory and CPU cycles
- ┆ reduces the frequency that a server might go into overload due to network problems

IPSI administration enhancements

The TN2312BP IP server Interface (IPSI) administration enhancements enable you to administer and manage Quality of Service (QoS) and Ethernet interface settings parameters using the SAT interface. You can administer and manage certain IPSI related parameters such as the gateway IP address and subnet mask. QoS settings are standardized to communicate between the IPSI and the Communication Manager. Communication Manager generates a warning alarm if it finds any discrepancies in Quality of Service (QoS) and Ethernet interface settings parameters. The IPSI administration inter-operates with Communication Manager by using the pre-existing QoS and administration interface.

Note:

The initial IPSI settings must still be administered using the command line interface.

QoS for call control

Communication Manager allows QoS for the signaling packets coming from gatekeepers such as the CLAN by employing the same standards based DiffServ and 802.1p/Q schemes as with audio channels. QoS services further improve the users VoIP audio experience.

QoS for VoIP

Communication Manager implements QoS through the selection of audio codec such as G.711, G.723 and G.729, and by requesting network prioritization through the layer 3 differentiated

services (DiffServ) scheme, as well as the layer 2 IEEE 802.1p/Q prioritization. Diffserv and 802.1p/Q are supported on voice packets coming to/from the gateway, all the way down to the endpoints such as IP telephones. Dynamic jitter buffers are also used.

QoS to endpoints

Users can set operating parameters to optimize the audio performance, or quality of service (QoS), on calls made over your IP network. These parameters include the audio codec, network priority through DiffServ capability, and the IEEE 802.1p/Q MAC-layer prioritization and segregation.

Default QoS parameters are downloaded to the IP telephone R1.5 and the IP softphone R3 when the values are not provided by the endpoint installer or the user. Certain options can be set locally by the endpoints or through the gatekeeper. The endpoints receive the parameters when the endpoints register, and once they are registered, whenever the administered values of the QoS parameters are modified.

Resource Reservation Protocol

Resource Reservation Protocol (RSVP) is a QoS signaling protocol. RSVP provides a means of specifying the requirements of IP packet flow, and determining if the intervening network can provide the resources to protect that flow through a process called “admission control.”

RSVP protection of VoIP audio streams on WANs and other links that are susceptible to congestion can safeguard the quality of VoIP calls already in progress.

- 1 IP telephones or gateways request the network routers to reserve bandwidth.
- 1 The routers act upon the request to allocate bandwidth according to the QoS request.
- 1 When the bandwidth is reserved, the call is protected against other network traffic in a loaded or congested network, thereby ensuring good voice quality.

Administrators can now configure RSVP settings in Communication Manager. When the `RSVP enable` field in the **IP Network Region** screen is set to **y**, the `RSVP Reservation Parameters` field appears.

Sending and receiving faxes over IP

Starting with Communication Manager release 2.1, users can send and receive faxes over the voice over IP (VoIP) and modem over IP (MoIP) networks. The firmware that is resident on the TN2302AP circuit packs (Hardware Vintage 10 or later), the MM760 Media Module, the G700 Media Gateway, and the G350 Media Gateway, actually performs the processing necessary to allow proper handling of faxes over an IP network.

Modem over IP

The modem over IP (MoIP) feature allows for transport of data over a 64kbps unrestricted clear channel. Starting with Communication Manager release 3.0, when a clear channel data call is originated, the system communicates to the media processor or VoIP engine to allow a 64kbps clear channel to be opened for transport.

Relay mode

In relay mode, the firmware detects fax tones and uses the appropriate modulation protocols (V.xx) to terminate or originate the fax so that the fax can be carried over the IP network. To reduce bandwidth over the IP network, the system encodes the modulated analog signal from the fax, and uses a relay coder/decoder. This process improves the reliability of transmission. Also, because the data packets for faxes in relay mode are sent almost exclusively in one direction, from the sending endpoint to the receiving endpoint, bandwidth use is reduced.

Relay mode works only if the receiving fax endpoint and the sending fax endpoint both communicate through Avaya 8XXX Servers. This transport of fax signals occurs at a 9600 bps rate (though this rate may vary with the version of firmware). This mode may be used for fax calls to and from Communication Manager R2.0 systems.

Pass through mode

Alternatively, you can choose to have fax signals sent in “pass through” mode. Pass through mode means the fax signals are transported using G.711-like encoding and are delivered to the receiving fax endpoint as IP signals. This capability provides higher quality transmission in the circumstance where endpoints in the network are all synchronized to the same clock source. Pass through mode works only if the receiving fax endpoint and the sending fax endpoint both communicate through Avaya 8XXX Servers.

The transport speed is up to the equivalent of circuit-switched calls and supports G3 and Super G3 fax rates, up to and including 33.6 kbps.



CAUTION:

If users are using Super G3 fax machines as well as modems, do not assign these fax machines to a network region with an IP Codec set that is modem-enabled as well as fax-enabled. If its Codec set is enabled for both modem and fax signaling, a Super G3 fax machine incorrectly tries to use the modem transmission instead of the fax transmission.

Therefore, assign modem endpoints to a network region that uses a modem-enabled IP Codec set, and assign the Super G3 fax machines to a network region that uses a fax-enabled IP Codec set.

You can assign packet redundancy in both pass through and relay mode, which means the media gateways use RFC 2198 packet redundancy to improve packet delivery and robustness of fax transport over the network.

Pass through mode uses more network bandwidth than relay mode. Redundancy increases bandwidth usage even more.

Encryption

You can encrypt fax pass through calls using either Avaya Encryption Algorithm (AEA) or Advanced Encryption Standard (AES). You can encrypt fax relay calls with AEA only. For more information about encryption, see [Security, privacy, and safety](#) on page 197.

T.38 faxes over the Internet

The users can send and receive faxes over the VoIP network using the T.38 standard for relay. The firmware resident on the TN2302AP circuit packs (Hardware Vintage 10 or later), the MM760 Media Module, the G700 Media Gateway, and the G350 Media Gateway actually performs the processing necessary to allow proper handling of faxes over an IP network. This transport of fax signals occurs at a 9600 bps rate.

The T.38 fax capability allows users to send faxes to and receive faxes from endpoints that are connected to non-Avaya systems. This capability is standards-based and uses IP trunks and H.323 signaling to allow communication with non-Avaya systems. Additionally, the T.38 fax capability uses the UDP protocol.

Note:

Fax endpoints served by two different Avaya 8XXX Servers can also send T.38 faxes to each other if both systems are enabled for T.38 fax. In this case, the servers also use IP trunks.

However, if the T.38 fax sending and receiving endpoints are on port networks or media gateways that are registered to the same server, the gateways or port networks revert to Avaya fax relay mode. Avaya fax relay mode is more efficient than T.38 from a bandwidth perspective.

Both the sending and receiving systems must announce support of T.38 fax data applications during the H.245 capabilities exchange. Avaya systems announce support of T.38 fax if the capability is administered on the Codec Set screen for the region and a T.38-capable media processor was chosen for the voice channel. In addition, for a successful fax transmission, both systems should support the H.245 null capability exchange (shuffling) in order to avoid multiple IP hops in the connection.

Note:

The T.38 fax capability does not support TCP.

You can assign packet redundancy to T.38 standard faxes to improve packet delivery and robustness of fax transport over the network.

Pass through mode

You cannot send faxes in pass through mode with the T.38 standard.

Shuffling and hairpinning

Shuffling and hairpinning can improve traffic handling performance and improve voice quality by more efficiently using both Communication Manager switching fabric by allocating, when possible, available IP network resources.

“Shuffling” means rerouting the audio channel connecting two IP endpoints. After shuffling, the audio which previously was carried in a mixed connection of IP signaling and TDM bus signaling, goes directly through the LAN or WAN between the two IP endpoints. Shuffling also can mean reversing this process if an endpoint requests a resource to support a feature, such as conferencing that requires the TDM bus.

“Hairpinning” means rerouting the audio channel connecting two IP endpoints so that the bearer (audio) packets are routed through the TN2302AP IP Media Processor board in IP format, without having to go through the IP to TDM conversion or traverse the TDM bus.

G.722 shuffling over H.323/SIP trunks

During a typical phone call that goes over the PSTN, it is sometimes difficult to distinguish certain letter sounds, such as “f” and “s” or “t” and “d.” The reason for this is that most of the speech energy that allows humans to distinguish consonants occurs above 3,000 Hz. The best digital PSTN phone call doesn’t pass any energy above 3,300 Hz.

High-fidelity audio (sometimes called wideband audio) passes audio frequencies of up to 7,000 Hz. Research has shown that conversations over these higher frequencies dramatically improve intelligibility and reduce listener fatigue. They also make it much easier to understand accented speech.

G.722 is an audio coding system (50 to 7,000 Hz) that can be used in a variety of higher quality speech applications. This feature supports endpoints capable of handling G.722 codecs, but it is specifically intended for the Avaya 96xx H.323 telephones and G.722-capable conference bridge endpoints.

NAT with shuffling

Communication Manager allows IP endpoints to shuffle if they are behind a Network Address Translation (NAT) device in an IP network.

Note:

Network Address Translation (NAT) is a method to address the shortage of IP V4 addresses by allowing globally register IP addresses to be reused by native networks. A NAT device translates between translated and native IP addresses.

Communication Manager supports IP direct calls (a call that has been shuffled) between two IP endpoints that are translated through a NAT device.

This enhancement works with static one-to-one NAT. It does not facilitate Port Address Translation (PAT), also known as Network Address Port Translation (NAPT). This enhancement does not work with many-to-one NAT.

TTY

People with hearing or speech disabilities often rely on a device known as a TTY in order to communicate on telephone systems. The term “TTY” is an abbreviation for Teletypewriter. The term “TDD” (Telecommunication Device for the Deaf) is also frequently used. The term TTY is generally preferred, however, because many people who use these devices are not deaf.

TTY devices typically resemble small laptop computers, except that there is a one- or two-line alphanumeric display in place of the computer screen.

Connection to the telephone network is generally through an acoustic coupler into which the user places the telephone's handset, or through an analog RJ-11 tip/ring connections.

Reliable transmission of TTY signals is supported by Communication Manager. This complies with the requirements and guidelines outlined in United States accessibility-related laws. Those laws include:

- ┆ Titles II, III, and IV of the Americans with Disabilities Act (ADA) of 1990.
- ┆ Sections 251 and 255 of the Telecommunications Act of 1996.
- ┆ Section 508 of the Workforce Investment Act of 1998.

Communication Manager TTY support is currently restricted to TTY devices that use the:

- ┆ US English standard TTY protocol, specified by ANSI/TIA/EIA 825 as: “A 45.45 Baud FSK modem.”
- ┆ UK English standard TTY protocol, Baudot 50.

Important characteristics of this standard are:

- ┆ TTYs are silent when not transmitting. Unlike fax machines and computer modems, TTYs have no “handshake” procedure at the start of a call, nor do they have a carrier tone during the call. This approach has the advantage of permitting TTY tones, DTMF, and voice to be intermixed on the same call.

Note:

A large percentage of people who use TTY devices intermix voice and typed TTY data on the same call. The most common usage is by people who are hard of hearing, but nevertheless able to speak clearly. These people often prefer to receive text on their TTY device and then speak in response. This process is referred to as Voice Carry Over (VCO).

- 1 Operation is “half duplex.” TTY users must take turns transmitting and typically cannot interrupt each other. If two people try to type at the same time, their TTY devices might show no text at all or show text that is unrecognizable. Also, there is no automatic mechanism that lets TTY users know when a character they have correctly typed has been received incorrectly.
- 1 Each TTY character consists of a sequence of seven individual tones. The first tone is always a “start tone” at 1800 Hz. This is followed by a series of five tones, at either 1400 or 1800 Hz, which specify the character. The final tone in the sequence is always a “stop tone” at 1400 Hz. The stop tone is a border that separates this character from the next.

The following types of systems support TTY communication:

- 1 Analog telephones and trunks
- 1 Digital telephones and trunks
- 1 VoIP gateways
- 1 Messaging systems
- 1 Automated attendant systems
- 1 IVR systems
- 1 Wireless systems in which a TTY-compatible coder is used

As long as the user's TTY device supports the following, Communication Manager allows:

- 1 Voice and TTY tones to be intermixed on the same call.
- 1 DTMF and TTY (with or without voice) to be intermixed on the same call. This allows TTY users to access DTMF-based voice mail, auto-attendant, and IVR systems.
- 1 The use of acoustically coupled and “direct connect” (RJ-11) TTY devices.

TTY over analog and digital trunks

Communication Manager supports TTY calls within a gateway or port network between two analog telephones. TTY calls from a gateway or port network over analog trunks or digital trunks is also supported.

TTY over Avaya IP trunks

Communication Manager supports calls over IP trunks, as well as Inter-Gateway Calls (IGC).

Note:

For this feature to work, both the sender (near end) and the receiver (far end) of a TTY call must each be connected to Avaya IP trunks. This feature does not work if either telephone is an IP telephone.

TTY relay mode

In relay mode, the system:

- ▮ detects TTY characters
- ▮ transports a representation of the characters over the IP network
- ▮ regenerates TTY characters/tones for delivery to the TTY device

This transport of TTY supports US English TTY (Baudot 45.45) and UK English TTY (Baudot 50). TTY uses RFC 2833 or RFC 2198 style packets to transport TTY characters.

Depending on the presence of TTY characters on a call, the transmission toggles between voice mode and TTY mode. The system uses up to 16 kbps of bandwidth when sending TTY characters, and normal bandwidth of the audio codec for voice mode. This mode may be used for TTY calls to and from Communication Manager R2.0 systems.

In relay mode, you can also assign packet redundancy. Packet redundancy means the media gateways send duplicated TTY packets to ensure and improve quality over the network.

TTY pass through mode

Alternatively, you can choose to have TTY signals sent in pass through mode. With pass through mode enabled, when the system detects TTY characters, the system uses G.711 encoding to transport the TTY signals end-to-end over the IP network. G.711 encoding pass through mode means the TTY signals are changed to digital format, and are delivered to the receiving endpoint after unencoding the digital signals.

Pass through mode provides higher quality transmission when endpoints in the network are all synchronized to the same clock source.

In pass through mode, you can also assign packet redundancy. Packet redundancy means the media gateways send duplicated TTY packets to ensure and improve quality over the network.

Pass through mode uses more network bandwidth than relay mode. Pass through TTY uses 87-110 kbps, depending on the packet size, whereas TTY relay uses, at most, the bandwidth of the configured audio codec. Redundancy increases bandwidth usage even more.

Variable length ping

Provides an enhancement to the ping command included in R7.1. This enhancement specifies a longer packet to be sent by ping and shows if a router or host has a problem fragmenting or integrating transferred packets.

Variable Length Subnet Mask

Variable Length Subnet Mask (VSLM) is a redefinition of the subnet mask, allowing for a more efficient allocation of IP addresses within a traditional classful block when administering IP address on Communication Manager.

QSIG

Auto callback - QSIG Call Completion

Auto Callback covers auto callback within a private corporate network only through QSIG. Auto Callback provides an administrable option on the Trunk Group screen to allow users to specify the method of signaling connection the system uses while waiting for a busy station to become idle.

Basic

QSIG provides compliance to the International Standardization Organization (ISO) ISDN-PRI private-networking specifications. QSIG is defined by ISO as the worldwide standard for private networks. QSIG features are supported on BRI trunks.

QSIG is the generic name for a family of signaling protocols. The Q-reference point or interface is the logical point where signaling is passed between 2 peer entities in a private network. QSIG signaling can provide feature transparency in a single-vendor or multi-vendor environment.

QSIG provides call-related supplementary services. These are services **that go** beyond voice or data connectivity and number transport and display. Examples of supplementary services include name identification, call forwarding (diversion), and call transfer.

Call completion

Call completion utilizes the QSIG platform enhancement call independent signaling connections and is functionally equivalent to the Distributed Communications System (DCS) feature: auto-callback. The call completion feature includes a connection release method. The connection release method clears the Temporary Signaling Connection (TSC) after each phase of call-independent signaling and establishes a new TSC for each subsequent phase.

Call forwarding (diversion)

QSIG call forwarding (diversion) is based on the Communication Manager call forwarding feature. It extends the feature transparency aspects of call forwarding over a QSIG trunk:

- ┆ If QSIG call forwarding is activated, all calls are diverted immediately.
- ┆ If QSIG call forwarding with busy/do not answer is activated and a station is busy, a call is diverted immediately.
- ┆ If QSIG call forwarding with busy/do not answer is activated and a station is idle but the call is not answered, a call is diverted after a specified number of rings.

These features are activated either by dialing a Feature Access Code (FAC) or by pressing a button.

Call Independent Signaling Connections

Call Independent Signaling Connections (CISC) are used to pass QSIG supplementary service information that is independent of an active call between two QSIG compliant nodes. Implementation is based on the ISO standard for CISC. It is possible to determine the status of a QSIG TSC by using the “status signaling group” command on the SAT.

Call offer

This feature, on request from the calling-user (or on behalf of that user), enables a call to:

- 1 Be offered to a busy called-user
- 1 Wait for a busy called-user to accept the call when the necessary resources have become available

Call transfer

QSIG call transfer differs from the standard Communication Manager transfer feature in that additional call information is available for the connected parties after the transfer completes. However, the information is only sent for QSIG trunks. If one call is local to the transferring switch, that user receives the name of the party at the far end.

Name display on unsupervised transfer

Station A calls station B, and is then transferred to station C. Station B has established a connection through QSIG to station A, and an enquire connection (intern or through QSIG) to station C.

Station B transfers station C to station A. The name of station C (not answered enquire call) is sent after call transfer to station A when the **Send Name** field on the **Trunk Group** screen is set to **y** at the QSIG trunk side to the primary PINX. So the name of the transferred-to station C appears on the display of the station A in the primary connection immediately after the call transfer.

Called name ID

The QSIG called name feature presents the name of the called party on the display of the calling party while the call is ringing. It then reverts to “connected name” when answered.

Centralized Attendant Service

Provides you with the capability to have all your attendants in one location, serving users in multiple locations. QSIG CAS does not utilize separate Release Link Trunks (RLT). This feature will not restrict calls from going out over non-QSIG trunks; however, the full functionality of the QSIG CAS will not be available.

Attendant display of Class of Restriction

While on a call, the attendant can press a “COR display” button to see the class of restriction of the user. The attendant will not block the transfer of the restricted line to the user. This feature is used for informational purposes only.

Attendant return call

If a call that is transferred by the attendant goes unanswered for a specified period of time, the call is returned to the attendant. Preferably the call will transfer back to the attendant who transferred the call.

Priority queue

QSIG MSI will pass more information to the main PBX. This information enables calls coming in from a QSIG CAS branch to be placed in the appropriate place in the queue, as if the call originated on the main PBX.

RLT emulation through a PRI

ISDN QSIG trunks will route calls from the branch PBX to the main PBX. You no longer have to specify a dedicated RLT network. The QSIG path replacement takes care of the trunk optimization. You have the flexibility to route calls to the main PBX.

Communication Manager/Octel QSIG integration

Communication Manager enables integration of Octel messaging servers through QSIG. See [Octel integration](#) on page 109.

Complex private numbering plan support

Additional flexibility is provided for private-network numbering in support of customers' private networks.

Leave Word Calling

See [Leave Word Calling](#) on page 107.

Manufacturer-Specific Information

QSIG handles non-standardized information that is specific to a particular PBX or network. This information is known as Manufacturer Specific Information (MSI). A manufacturer can define manufacturer-specific supplementary services operations after it has:

- 1 Applied to a sponsoring and issuing organization (ECMA or European Computer Manufacturers Association in this case)
- 1 Been assigned an organization identifier. This organization identifier is used as the root of the manufacturer-specific service-operation value.

All MSI operation values should be unique to that manufacturer.

Manufacturer-specific supplementary services can be created using specific operations encoded with the identifier of the manufacturer. Communication Manager supports non-QSIG applications that transport information across QSIG networks in MSI. Applications have the same functionality over QSIG networks that they have over non-QSIG networks. Applications that use MSI include Centralized Attendant Service, Transfer to AUDIX, Best Service Routing, and QSIG VALU.

Message Waiting Indication

The system indicates that a guest telephone has received one or more messages in their voice mailbox. An automatic message waiting lamp light at the telephone of the called party.

Name and number identification

Allows a **switch** to send and receive the calling number, calling name, connected number, and connected name. Additional parameters that control the display of the connected name and number are administered on the **Feature-Related System-Parameters** screen. QSIG Name and Number Identification displays up to 15 characters for the calling and connected name and up to 15 digits for the calling and connected number across ISDN-PRI interfaces.

Path replacement with path retention

With this feature, a call between switches in a private network can be replaced with new connections while the call is active. This feature is invoked when a call is transferred and improvements may be made in costs.

For example, after a call is transferred, the two parties on the transferred call can be connected directly and the unnecessary trunks are dropped off the call. The routing administered at the endpoints may allow for a more cost-effective connection.

Earlier versions of DEFINITY could not route a call over the original trunk when path replacement was turned on. Path Replacement features Path Retention, which allows Communication Manager to use the original trunk group path when the routing analysis performed by the switch shows the original trunk group to be the best route.

QSIG/DCS voice mail interworking

QSIG/DCS Voice Mail Interworking is an enhancement to the current QSIG feature. It integrates DCS and QSIG Centralized Voicemail through the DCS+/QSIG gateway. Switches labeled DCS+/QSIG integrate multi-vendor PBXs into a single voice messaging system. QSIG/DCS Voice Mail Interworking works on G3r, G3si, and G3csi. It provides network flexibility, DCS functionality without a dedicated T1.

Reroute after diversion to voice mail

Supports path optimization for calls that are diverted to a QSIG voice mail hunt group. That is, the switch moves the call to the shortest route between the caller and the voice mail system. For example, if user A on switch A calls user B on switch B and the call goes to a voice mail system attached to switch C, then the call is using up two trunks: A-B and B-C. If there is a trunk that directly connects switches A and C, this feature will drop the A-B and B-C connection and set up a new call from switch A to switch C, thus saving one trunk. The reroute happens automatically; the user never knows that the extra trunk was dropped.

Stand-alone path replacement

Path Replacement is the process of routing an established call over a more efficient path, after which the old call is torn down leaving those resources free. Path Replacement offers potential savings by routing calls more efficiently, saving resources and trunk usage.

Path replacement can exist as a stand-alone feature, or occur in the following additional cases:

- 1 Call Forwarding by Forward Switching supplementary service, including the case where Call Diversion by Rerouting fails, and Call Forwarding is accomplished via forward switching
- 1 Gateway scenarios where Communication Manager, serving as an incoming or outgoing gateway, invokes PR to optimize the path between the gateways
- 1 Calls in queue/vector processing even though no true user is on the call yet
- 1 QSIG Lookahead Interflow call, Best Service Route call, or adjunct route

Supplementary services and rerouting

The QSIG standard defines Supplementary Services as those service beyond voice or data connectivity and number transport and display. Examples include call forwarding, transfer and call hold.

VALU

Call coverage

This feature provides similar call coverage as DCS call coverage and Call Coverage Remote Off Net (C-CRON). The call will come back if covered over QSIG. The functionality will only be complete when all the switches are running under Communication Manager and using QSIG VALU. The covered-to party can still receive distinct alerting.

Call coverage and CAS

When a trunk has both CAS and VALU Call Coverage activated, the coverage display information is provided on calls that cover from a branch PBX to the main PBX. Path replacement will be attempted after coverage.

Distinctive alerting

Provides distinctive ringing, internal and external, to the remote called party when the call is routed over the QSIG network.

Uniform Dial Plan

A unique four- or five-digit number assigned to each station on the network. Uniform numbering gives each station a unique number (location code plus extension) that can be used at any location in the electronic tandem network to access that station. Communication Manager enhances the standard UDP with the unrestricted 5-digit Uniform Dial Plan, which allows up to five digits to be parsed for call routing.

Dial Plan Expansion

With Communication Manager release 4.0, you can expand your dial plan to a maximum of 13 digits. This affects telephones, data modules, login IDs, and vectors.

Administrators have the flexibility to administer dial plans between 3 and 13 digits in length. Communication Manager supports mixed digit lengths in the same dial plan within a location and across a network of locations.

Customers upgrading to Communication Manager 4.0 can choose to migrate to the expanded 13-digit dial plan. Customers who choose not to migrate may convert their dial plans at a later date.

Distributed Communications System (DCS) protocol is limited to a dial plan of 3-5 digits. If your dial plan requires 6 or 7 digits, QSIG, which is the generic name for a family of signaling protocols, is required.

Note:

Some features cannot expand to 13 digits. For a complete description of the Dial Plan Expansion feature, see the following documents:

- 1 *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.
- 1 *Administering Avaya Aura™ Communication Manager*, 03-300509.

Multi-location dial plans

When a customer migrates from a multiple voice server QSIG/DCS network to a single voice server whose gateways are distributed across a data network, it may initially seem as if some dial plan functions are no longer available.

This feature preserves dial plan uniqueness for extensions and attendants that were provided in a multiple QSIG/DCS network, but were lost when customers migrated to a single distributed network. This feature provides dial plan capabilities similar to those provided before the migration, including:

- ┆ extension uniqueness
- ┆ announcement per location
- ┆ local attendant access
- ┆ local ARS code administration

A major reason to migrate customers from a multiple QSIG/DCS environment to a single S87XX network is to provide a greater set of features and help reduce costs. Migrating to a single network reduces the number of systems a customer has to maintain. That in turn lowers administration costs - one switch to administer instead of multiple switches, one dial plan to maintain, and so on. With a single distributed network solution, some features no longer work transparently across multiple locations.

For example, in a department store with many locations, each location might have had its own switch with a QSIG/DCS network. That way, the same extension could be used to represent a unique department in all stores. For example, extension 123 might be the luggage department in all stores. If the customer migrates to a single distributed network, this functionality is not available without this feature.

In addition, an S87XX solution does not assure that a call that is routed to an attendant would terminate at the local attendant. Let us use an example of a public school district that previously was networked with a switch at each school. If the school district migrates to an S87XX network, dialing the attendant access code at your school may not route your call to the local attendant.

Instead of having to dial a complete extension, the multi-location dial plan feature allows a user to dial a shorted version of the extension. For example, a customer can continue to dial 4567 instead of having to dial 123-4567. Communication Manager takes the location prefix and adds those digits to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the **Dial Plan Parameters** screen.

Note:

You can use the Per-Location Dial Plan feature to allow different branches to have different short extensions, so that the extensions do not conflict across branches.

Punctuation on station displays

On digital telephone displays, Communication Manager can display punctuation to make reading a longer extension easier.

Punctuation marks that are allowed include:

- ı hyphen (for example, xxx-xxxx)
- ı period (for example, xxx.xxxxx)
- ı space (for example, xx xx xx)

Formats for displaying numbers with punctuation are on the **Dial Plan Parameters** screen.

For more information on the **Dial Plan Parameters** screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Extended trunk access

Used with Uniform Dial Plan, allows the system to send any unrecognized number (such as an extension not administered locally) to another system for analysis and routing. Such unrecognized numbers can be Facility Access Codes, Trunk Access Codes, or extensions that are not in the Uniform Dial Plan table. Non-Uniform Dial Plan numbers are administered on either the First Digit Table (on the **Dial Plan Record** screen) or the Second Digit Table. They are not administered on the Extended Trunk Access Call Screening Table. Extended Trunk Access helps you make full use of automatic routing and Uniform Dial Plan.

Extension Number Portability - When employees move within the network, they can retain their extension numbers. The ability to keep extension numbers, and even Electronic Tandem Network and Direct Inward Dialed numbers, when moving to other locations within the company eliminates missed calls and saves valuable time.

Chapter 15: Data interfaces

Administered connections

Automatically establishes an end-to-end connection between two access or data endpoints based on administered attributes. This feature provides capabilities such as alarm notification, including an administrable alarm type and threshold; automatic restoration of connections established over a Software-Defined Data Network; ISDN-PRI trunk group [service may be referred to as ISDN-PRI (AC/AE) Service]; scheduled as well as continuous connections; and administrable-retry interval for failed connection attempts.

Data call setup

Enables the setting up of data calls using a variety of methods, such as: keyboard dialing, telephone dialing, Hayes command dialing, permanent switched connections, administered connections, automatic calling unit interface, and Hot Line dialing. Data Call Setup is provided for both DCP and ISDN-BRI telephones.

Data hot line

Provides for automatic placement of a data call when the originator hangs up. Data Hot Line may be used for security purposes. This feature offers fast and accurate call placement to commonly called data endpoints. Data terminal users who constantly call the same number can use Data Hot Line to automatically place the call when they hang up the telephone.

Data privacy

Data Privacy protects analog data calls from being disturbed by any overriding or ringing features of the system. Data Privacy is activated when you dial an activation code at the beginning of the call.

Data restriction

Protects analog data calls from being disturbed by any overriding or ringing features of the system. It is administered at the system level to selected analog and multi-appearance telephones and trunk groups.

Default dialing

Provides data terminal users who dial a specific number the majority of the time a very simple method of dialing that number. This feature enhances Data Terminal (Keyboard) Dialing by allowing a data terminal user to place a data call to a pre-administered destination in several different ways, depending on the type of data module. Data Terminal Dialing and Alphanumeric Dialing are unaffected.

IP asynchronous links

IP asynchronous links enable Communication Manager to transfer existing asynchronous adjunct connectivity to an Ethernet (TCP/IP) environment. IP asynchronous links support switch server applications, as well as client applications. Systems running Communication Manager can connect to System Management applications such as the Avaya Visibility Suite over the LAN. Call Detail Recording (CDR) devices, Property Management System (PMS) and printers can be connected using asynchronous TCP/IP links.

IP asynchronous links:

- 1 Reduce the cost of connecting to systems running Communication Manager for various adjuncts
- 1 Allow for an open architecture to transport information and increases the speed at which data is transferred
- 1 Allow customers to manage applications from on-site or remote locations
- 1 Allow several system management applications to run on a single PC, thereby reducing hardware requirements
- 1 Guarantee data delivery through a reliable session-layer protocol
- 1 Support the existing serial hardware investment of a customer through use of Network Terminal Servers

Multimedia application server interface

The Multimedia Application Server Interface provides a link between Communication Manager and one or more Multimedia Communications eXchange nodes. A Multimedia Communications eXchange is a stand-alone multimedia call processor produced by Avaya. This link to Communication Manager enhances the capabilities of each Multimedia Communications eXchange system by enabling it to share some of the Communication Manager features. In particular, the interface provides the following advantages:

- 1 Call Detail Recording (CDR). The capture of call detail records so you can analyze the call patterns and usage of multimedia calls just as Communication Manager administrators analyze normal calls.
- 1 Automatic Alternate Routing/Automatic Route Selection (AAR/ARS). The intelligent selection of the most cost-effective routing for calls, based on available resources and your carrier preference. The system may select public trunks via DEFINITY Multimedia eXchange (MMCX).
- 1 Voice Mail Integration. You can access your EMBEDDED AUDIX or CM Messaging voice messaging system from a Multimedia Communication eXchange (MMCX).

Multimedia calling

Multimedia calls are initiated with voice and video only. Once a call is established, one of the parties may initiate an associated data conference to include all of the parties on the call who are capable of supporting data. The data conference is controlled by an adjunct device called an Expansion Services Module (ESM).

Multimedia call early answer on vectors and stations

Early Answer is a feature applied to multimedia calls in conjunction with conversion to voice. Early Answer:

- 1 Answers the data call
- 1 Establishes the multimedia protocol prior to completion of a converted call
- 1 Ensures that a voice path to/from the originator is available when the (voice) call is answered

For an incoming call, Early Answer answers the dynamic service-link calls when the destination endpoint answers, unless Early Answer is specified during routing or termination processing.

Note:

The “destination voice endpoint” might be an outgoing voice trunk if the destination voice station is forwarded or covered off-premises.

Multimedia Call Handling

Multimedia Call Handling (MMCH) enables you to control voice, video, and data transmissions using your telephone set. The feature buttons on a multi-function telephone enable you to conduct video conferences, and forward, cover, hold, or park multimedia calls much as you would a standard voice call. You can also share PC applications so that you and colleagues can collaborate while working from remote sites. See [Figure 5: Multimedia Call Handling \(MMCH\)](#) on page 178.

Figure 5: Multimedia Call Handling (MMCH)

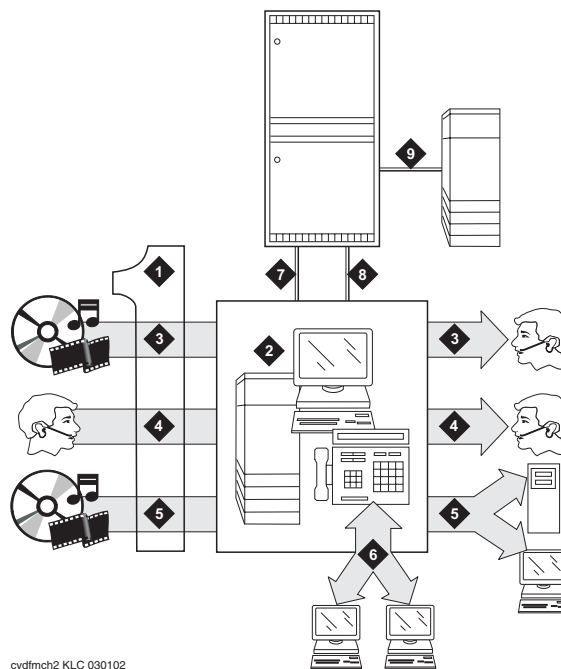


Figure notes:

- | | |
|-----------------------------------|----------------------------|
| 1. One number access | 5. Call redirection |
| 2. Multimedia call complex | 6. Multimedia conferencing |
| 3. Multimedia to voice conversion | 7. BRI data connection |
| 4. Standard voice call handling | 8. DCP voice connection |
| | 9. ESM data collaboration |
-

Multimedia call redirection to multimedia endpoint

A dual port multimedia station may be a destination of call redirection features such as call coverage, forwarding, and station hunting. The station can receive and accept full multimedia calls or data calls converted to multimedia.

Multimedia data conferencing (T.120) through ESM

The data conference is controlled by an adjunct device called an Expansion Services Module (ESM). The Expansion Services Module is used to terminate T.120 protocols [including Generalized Conference Call (GCC), a protocol standard for data conference control] and provide data conference control and data distribution. The MultiMedia Interface circuit pack, TN787, is used to rate adapt T.120 data to/from the ESM.

Multimedia hold, conference, transfer, and drop

Station users have the ability to activate hold, conference, transfer, or drop on multimedia calls. Multimedia endpoints and voice-only stations may participate in the same conference.

Multimedia multiple-port networks

Communication Manager supports the equivalent of 580 Basic mode complexes operating at 6CCS traffic level. All enhanced mode complexes operate with soft-mode service links since the use of hard-mode service links reduces capacities. G3si limits are 1/3 to 1/2 of the G3r limits, depending on memory limitations and port network limitations.

Pass advice of charge information to world class BRI endpoints

Provides Advice of Charge (AOC) information to World Class BRI (WCBRI) endpoints. On a call using a WCBRI endpoint, AOC information will be displayed on the endpoint after the call has completed and the far end has hung up.

Chapter 16: Call routing

Alternate facility restriction levels

Allows Communication Manager to adjust facility restriction levels or authorization codes for lines or trunks. Each line or trunk is normally assigned a facility restriction level. With this feature, Alternate Facility Restriction Levels are also assigned. Attendants can change to the alternates, thus changing access to lines and trunks. You might want to use this feature to disable most long-distance calling at night, for example, to prevent unauthorized staff from making long-distance calls.



CAUTION:

This feature may change the AAR and ARS routing preferences. Using it on tandem and tie-trunk applications affects entire networks. Calls that are part of a cross-country private network may be blocked.

Automatic routing features

Communication Manager provides a variety of automatic routing features for public and private networks. Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) are the foundation for these automatic-routing features. They route calls based on the preferred (normally the least expensive) route available at the time the call is placed. Generally, AAR routes calls over a private network and ARS routes calls using the public network numbering plan. However, both AAR and ARS support public and private networks. You can use the other features listed in this section when you use AAR and ARS.

Automatic Alternate Routing

Automatic Alternate Routing (AAR) allows private network calls to originate and terminate at one or many locations without accessing the public network. When you dial an access code and telephone number, **AAR** selects the most desirable route for the call and performs digit conversion as necessary. If the first choice route is unavailable, another route is chosen automatically.

The numbers you call using AAR are normally private-network numbers. However, you can call a public-network number, a service code, an **international** number, operator access code, or an operator-assisted dialing number. With **AAR** and Subnet Trunking, you have a convenient way

to place **international** calls to frequently-called foreign cities. Such calls route as far as possible over the private network, and then access the public network. This saves toll charges and allows you to use your private network as much as possible. In a multi-location system, you can administer AAR on a per-location basis.

Automatic Route Selection

Automatic Route Selection (ARS) selects carriers automatically and routes calls inexpensively over the public network. When there are one or more long-distance carriers and Wide Area Telecommunications Service (**WATS**) provided, Communication Manager selects the most preferred route for the call. Long-distance carrier-code dialing is not required on routes selected by the system. You assign long-distance carrier-codes and Communication Manager translates them. The system inserts codes as needed to guarantee automatic-carrier selection. **ARS** can route calls to a variety of types-of-numbers and access a variety of types of trunk groups. In a multi-location system, you can administer ARS on a per-location basis.

ARS/AAR dialing without FAC

The Automatic Route Selection (ARS) version of this feature allows users to place calls by dialing the full public-network numbers without first having to dial a Feature Access Code (FAC), such as the number “9” to access an outside line. The system recognizes the call as an ARS call and uses the ARS digit analysis and digit conversion tables to manipulate the digits to route the call.

The Automatic Alternate Routing (AAR) version of this feature is similar except that the call is routed as an AAR call and therefore uses the AAR digit analysis and digit conversion tables.

AAR/ARS overlap sending

Communication Manager supports overlap sending for AAR and ARS calls that are routed over ISDN-PRI trunk groups. ISDN-PRI call-address information is sent one digit at a time instead of in one block. In countries with complex public-network numbering plans, this allows for a significant decrease in call setup time. When overlap receiving is enabled, this is especially significant for tandem calls.

AAR/ARS partitioning

Allows **AAR** and **ARS** to be partitioned into 8 user groups within a single system and provides individual routing treatment for each of these user groups.

User groups share the same Partition Group Number, which indicates the choice of routing tables that are used on a particular call. Each Class of Restriction (COR) is assigned a specific **Partition Group Number** or Time of Day specification. Different **classes of restriction** may be assigned the same **Partition Group Number**.

AAR/ARS partitioning

Allows **AAR** and **ARS** to be partitioned into 8 user groups within a single system and provides individual routing treatment for each of these user groups.

Enbloc Dialing and Call Type Digit Analysis

The Enbloc Dialing and Call Type Digit Analysis feature allows users to automatically place outgoing calls based on the telephone number information in the telephone's call log, without the user having to modify the telephone number.

Enbloc Dialing is the ability of Communication Manager software to receive in one message all of the digits necessary to set up a call, or any time the terminal makes a request rather than receiving digits one at a time.

Call Type Digit Analysis is the ability for Communication Manager to decide how to route a call based on all of the digits in a telephone number in a call log. The system administrator maintains the **Call Type Digit Analysis Table**, which is similar to AAR and ARS Routing Tables. A phone signals for Call Type Digit Analysis when the user places a call from the phone's call log or from the contacts or corporate directory. The telephone sends to Communication Manager the information stored in the call log, or from the list of contacts or the corporate directory. Communication Manager uses the **Call Type Digit Analysis Table** to analyze the stored number, determines a corresponding dialable number, and makes the call.

The Enbloc Dialing and Call Type Digit Analysis feature is available with Communication Manager. It works in conjunction with Avaya terminals (proprietary signaling protocol): DCP phones, H.323 and SIP terminals (96xx H.323 phones, Avaya one-X Mobile Edition for S60 3rd Edition Dual-Mode SIP phones).

Generalized route selection

Provides voice and data call-routing capabilities. You use it to select not only the least-cost routing, but also optimal routing over the appropriate facilities. It enhances **AAR** and **ARS** by providing additional parameters in the routing decision and maximizing the chance of using the right facility to route the call. Also, if an endpoint incompatibility exists, it provides a conversion resource (such as a modem from a modem pool) to attempt to match the right facility with the right endpoint.

Look-ahead routing

Provides an efficient way to use trunking facilities. It allows you to continue to try to reroute an outgoing ISDN-PRI call that is not completing. When Communication Manager receives a cause value that indicates congestion, Look-Ahead Routing tells the system what to do next. For each routing preference, you can indicate if the next routing-preference should be attempted or if the current routing-preference should be attempted again.

Node number routing

Allows you to specify the route pattern associated with each node in a private network. It is a required capability for Extension Number Portability and is used in conjunction with Automatic Route Selection, AAR and ARS Partitioning, Private Networking, and Uniform Dial Plan. **Uniform Dial Plan** extensions can be routed to a specified node using its associated pattern. Node Number Routing allows a **Uniform Dial Plan** route pattern based on node numbers or on location codes. On the **AAR** and **ARS** Digit Analysis Tables, you also can specify a Node Number instead of a Route Pattern.

Time of day routing

Provides the most economical routing of **ARS** and **AAR** calls. This routing is based on the time of day and day of the week that each call is made. Up to 8 TOD routing plans may be administered, each scheduled to change up to 6 times a day for each day in the week. This allows you to take advantage of lower calling rates during specific times of the day and week. In addition, companies with locations in different time zones can use different locations that have lower rates at different times of the day or week. This feature is also used to change patterns during the times an office is closed in order to reduce or eliminate unauthorized calls.

Multiple location support

Multiple Location Support enables local user time, local ARS Public Analysis Tables for local trunking, automatic Daylight Savings Time, and enhances shared resource algorithms (touch tone receivers) when Remote Expansion Port Networks (EPNs), ATM Port Networks, and Avaya Media Gateways are remoted off of a central server at a different location.

Multiple location support for network regions

See [Multiple location support for network regions](#) on page 151.

Traveling class marks

Traveling Class Marks are a mechanism for passing the facility restriction level of a caller from one Electronic Tandem Network switch to another. Traveling Class Marks allow privilege checking to be passed across switches through the Electronic Tandem Network.

Answer detection

For purposes of Call-Detail Recording (CDR), it is important to know when the called party answers a call. Communication Manager provides three ways to determine whether the called party has answered an outgoing call.

Answer supervision by time-out

You set a timer for each trunk group. If the caller is off-hook when the timer expires, Communication Manager assumes that the call has been answered. This is the least accurate method. Calls that are shorter than the timer duration do not generate call records, and calls that ring for a long time produce call records whether they are answered or not.

Call-classifier board

A call-classifier board detects tones and voice-frequency signals on the line and determines whether a call has been answered.

Network answer supervision

The Central Office (CO) sends back a signal to indicate that the far end has answered. If a call has traveled over a private network before reaching the CO, the signal is transmitted back over

Call routing

the private network to the originating system. This method is extremely accurate, but is not available in the United States over CO, FX, or WATS trunks.

Chapter 17: Reliability and survivability

Alternate gatekeeper

The alternate gatekeeper enhancement can provide survivability between Communication Manager and IP communications devices such as IP Telephones and IP Softphone. This is accomplished by providing alternate gatekeepers (CLAN) in the event of network or gatekeeper failure and by load balancing endpoint traffic among multiple gatekeepers. It is important to recognize that calls will drop during that interval while the communication is re-established to the switch.

The Alternate Gatekeeper List (AGL) feature allows administrators to specify the number of IP interfaces for each connected network region that are allowed for phones within a specific network region.

Auto fallback to primary for H.248 gateways

This feature automatically returns a fragmented network, where a number of H.248 media gateways are being serviced by one or more Local Survivable Processors (LSP), to the primary Avaya 8XXX Server. This feature is targeted to H.248 media gateways only.

This feature allows the administrator to define any of the following rules for migration:

- 1 Whether or not the media gateways, serviced by LSPs, should automatically migrate to the primary media gateway.
- 1 Whether or not the media gateway should migrate immediately when possible, regardless of active call count.
- 1 Whether or not the media gateway should only migrate if the active call count is 0.
- 1 Whether or not the media gateway should only be allowed to migrate within a window of opportunity, by providing day of the week and time intervals per day. This option does not take call count into consideration.
- 1 Whether or not the media gateway should be migrated within a window of opportunity by providing day of the week and time of day, or immediately if the call count reaches 0. Both rules are active at the same time.

Internally, the primary call controller gives priority to registration requests from those media gateways that are currently not being serviced by an LSP. This priority is not administrable.

Connection preserving failover/failback for H.248 media gateways

The Connection Preserving Migration (CPM) feature preserves existing bearer (voice) connections while an H.248 media gateway migrates from one Communication Manager server to another. Migration might be caused by a network or server failure.

Only stable calls are preserved. Call that are not preserved are:

- ┆ Unstable calls. An unstable is any call where the call talk path between parties has not been established, or is not currently established. Some examples are:
 - Calls with dial tone
 - Calls in dialing stage
 - Calls in ringing stage
 - Calls listening to announcements
 - Calls listening to music
 - Calls on hold (soft, hard)
 - Calls in ACD queues
 - Calls in vector processing
- ┆ IP trunks, both SIP and H.323
- ┆ ISDN-BRI telephones
- ┆ ISDN-BRI trunks

Users on connection-preserved calls cannot use such features as Hold, Conference, or Transfer.

Connection preserving upgrades for duplex servers

The connection preserving upgrades for duplex servers feature provides connection preservation on upgrades of duplex servers for:

- ┆ connections involving IP telephones
- ┆ connections involving TDM connections on port networks
- ┆ connections on H.248 gateways
- ┆ IP connections between port networks and media gateways

Stable calls are preserved. Unstable calls are dropped.

Enterprise Survivable Servers

The Enterprise Survivable Server (ESS) provide survivability by allowing backup servers to be placed in various locations in the customer network. The backup servers supply service to port networks in the case where the Avaya 8XXX Server pair fails, or connectivity to the main server or server pair is lost.

In an ESS environment, there can only be one main server, either one S85XX Server, or one pair of S87XX servers. If the main server is an S85XX Server, all ESSs in the configuration must also be S85XX Servers. During normal operation, the main server communicates with and controls all the port networks. The main server contains a license file that identifies the server as the main server and activates the ESS functionality.

The S8400 server can be used as an ESS in Communication Manager Release 5.2 and later. For more information, see *Using Avaya Enterprise Survivable Servers (ESS)*, 03-300428.

Automatic return to primary server

When ESS is in control due to a network fragmentation or catastrophic main server failure, the return to the primary (main) server is predicated by three options:

- ┆ scheduled
- ┆ manual
- ┆ automatic

There is a timer that is associated with the auto return to primary feature. The customer sets the timer before the auto return to primary feature is activated to prevent recovery to the main server before the network is stable.

Dial Plan Transparency for LSP and ESS

The Dial Plan Transparency feature preserves users' dialing patterns if a media gateway registers with a local survivable processor (LSP), or when a port network registers with an Enterprise Survivable Server (ESS).

When a media gateway registers with a local survivable processor (LSP), or when a port network registers with an Enterprise Survivable Server (ESS), the Dial Plan Transparency feature routes calls over the public network when they cannot be routed over the IP network.

Note:

This feature lets users continue their dialing patterns when LSP or ESS fragments exist, but it does not guarantee feature transparency for the calls. In most cases, only basic trunk features are available to the calling and called parties.

IP bearer duplication using the TN2602AP circuit pack

The TN2602AP IP Media Resource 320 circuit pack provides high-capacity voice over Internet protocol (VoIP) audio access to the switch for local stations and outside trunks. The IP Media Resource 320 provides audio processing for the following types of calls:

- ┆ TDM-to-IP
- ┆ IP-to-TDM
- ┆ IP-to-IP

The TN2602AP IP Media Resource 320 circuit pack has two capacity options, both of which are determined by the license file installed on Communication Manager:

- ┆ 320 voice channels, considered the standard IP Media Resource 320
- ┆ 80 voice channels, considered the low-density IP Media Resource 320

Only two TN2602AP circuit packs are allowed per port network.

Note:

The TN2602AP IP Media Resource 320 is not supported in CMC1 and G600 Media Gateways. For more information about the TN2602AP circuit pack, see *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

Load balancing

Up to two TN2602AP circuit packs may be installed in a single port network for load balancing. The TN2602AP circuit pack is also compatible with and can share load balancing with the TN2302 and TN802B IP Media Processor circuit packs. Actual capacity may be affected by a variety of factors, including the codec used for a call and fax support.

Bearer signal duplication

Two TN2602AP circuit packs may be installed in a single port network for bearer signal duplication. In this configuration, one TN2602AP is an active IP media processor and one is a standby IP media processor. If the active media processor, or connections to it, fail, active connections failover to the standby media processor and remain active. This duplication prevents active calls in progress from being dropped in case of failure.

For bearer duplication, both TN2602AP circuit packs must be Hardware Version 2, and must have firmware version 211 or higher.

Note:

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.

**Important:**

If you change from load balanced to duplicated TN2602s, existing calls retain the real IP address on the TN2602AP circuit pack. New calls are associated with the virtual IP address of the TN2602AP circuit pack. If an interchange occurs during this time, existing calls that are associated with the real IP address will drop.

Reduced channels with duplicated TN2602AP circuit packs

If a pair of TN2602AP circuit packs, previously used for load balancing, are re-administered to be used for bearer duplication, only the voice channels of the active circuit pack can be used. For example,

- 1 If you have two TN2602 AP circuit packs in a load balancing configuration, each with 80 voice channels, and you re-administer the circuit packs to be in bearer duplication mode, you have 80, not 160, channels available.
- 1 If you have two TN2602 AP circuit packs in a load balancing configuration, each with 320 voice channels, and you re-administer the circuit packs to be in bearer duplication mode, you will have 320, not the maximum 484, channels available.
- 1 When two TN2602AP circuit packs, each with 320 voice channels, are used for load balancing within a port network, the total number of voice channels available is 484, not 640. The reason is that 484 is the maximum number of time slots available for connections within a port network.

IP endpoint Time-to-Service

The IP endpoint Time-to-Service (TTS) feature improves a customer's IP endpoint time to service, especially in cases where the system has a lot of IP endpoints trying to register or re-register. With this feature, the system considers that IP endpoints are in-service immediately after they register.

Local Survivable Processor

A Local Survivable Processor (LSP) is an Internal Call Controller (ICC) with an integral G700 Media Gateway, in which the ICC is administered to behave as a spare processor rather than as the main processor. The standby Avaya S87XX Server runs in duplex mode with the main server ready to take control in the event of a outage with no loss of communication.

An LSP is a configuration used to provide redundancy of the Avaya call processing application. Usually, a media module serves as the ICC for the system, but it can also serve as a redundant processor for call processing. In the LSP configuration, the processor serves as an alternate controller/gatekeeper for IP entities, such as IP telephones and media gateways. These IP entities use the LSP when they lose connectivity to their primary controller.

In the event that the communication link is broken between the remote Avaya G700 Media Gateway and the primary call controller (either an Avaya S8300 Server or an Avaya S87XX Server), the LSP provides service for the Avaya IP telephones and Avaya G700 Media Gateways that were controlled by the primary call controller.

How the Avaya G700 Gateways and IP endpoints change control from the primary to the LSP is driven by the endpoints themselves, using a list of call controllers. During initialization, each IP endpoint and Avaya G700 Gateway receives a list of call controllers. The IP endpoints ask each call controller in the list for service until one responds with a positive reply. If the link to that call controller fails at some later time, the endpoint will try to receive service from the other call controllers in the list, including the LSP.

The LSP provides service to all Avaya G700 Gateways and IP endpoints that can sometimes register with it. When the primary call controller is prepared to provide service, the LSP is reset. This informs the IP endpoints to try their call controller list again, and returns to the primary call controller for service.

The LSP provides redundancy in a variety of configurations, and can be located anywhere in a network of Avaya G700 Gateways.

For LSP capacities, refer to the capacities table. See [Capacities](#) on page 26 for instructions how to view the capacities table.

Note:

You cannot use Upgrade Tool or Avaya Installation Wizard (AIW) for the upgrade procedures to Communication Manager Release 5.2 or later.

Handling of split registrations

Split registrations occur when resources on one network region are registered to different servers. For example, after an outage activates Local Survivable Processors (LSPs), telephones in a network region register to the main server or Enterprise Survivable Server (ESS), while the gateways in that network region are registered with an LSP. The telephones registered with the main server are isolated from their trunk resources. You can manage split registrations by:

- 1 Setting the **Migrate H.248 MG to primary** field on the **system-parameters mg-recovery-rule** screen to **Immediately**.
- 1 Forcing telephones and gateways to register with the main server or the LSP. Split registrations occurring between a main server and LSPs or between an ESS and LSPs are managed by this feature. This feature does not handle split registration between a main server and an ESS.

Multiple network regions per CLAN

See [Multiple network regions per CLAN](#) on page 151.

Power failure transfer

Provides service to and from the local telephone company central office (CO), including wide area telecommunications system, during a power failure. This allows you to make or answer important or emergency calls during a power failure. This feature is also called emergency transfer.

Standard Local Survivability

Standard Local Survivability (SLS) provides a local Avaya G250/G350 Media Gateway and Juniper J4350/J6350 gateways with a limited subset of Communication Manager functionality when there is no IP-routed WAN link available to the main server or when the main server is unavailable.

SLS provides:

- ┆ Calling capability among analog, DCP, and IP telephones
- ┆ ISDN BRI/PRI trunk interfaces supported on the G250-DS1, G250-BRI, G350, and Juniper J4350/J6350 gateways
- ┆ Non-ISDN digital DS1 trunk interfaces supported on the G250-DS1, G350 and Juniper J4350/J6350 gateways
- ┆ Outbound dialing through the local PSTN (local trunk gateway) from analog, DCP, and IP telephones
- ┆ Inbound calls from each trunk to pre-configured local analog or IP telephones that have registered
- ┆ Direct Inward Dialing (SLS)
- ┆ Multiple call appearances
- ┆ Hold (SLS) and Call Transfer (SLS) functions
- ┆ Contact closure feature
- ┆ Local call progress tones (dial tone, busy, etc.)
- ┆ Emergency Transfer in survivable mode on the media gateway hardware in cases of power loss
- ┆ Auto Fallback to Primary Server
- ┆ IP station registration
- ┆ Expanded dial extension numbering for a maximum of 13 digits

Survivable Remote EPN

The Survivable Remote Expansion Port Network (SREPN) allows a DEFINITY ECS (R6r or later) EPN to provide service to the customer when the link to the main processor fails or is severed or when the processor or CSS fails. When the links to the system are restored and stable, the logic switch is manually reset and the EPN is reconnected to the links from the

switch. There are both command and manual resets. The resets can be done remotely at the SAT or manually at the equipment.

The SREPN must be administered separately (not as a duplicated PPN) to function in a disaster recovery scenario. It does not function as a survivable remote EPN without the administration (stations, trunks, features) to support its operation.

Note:

SREPN is not compatible with ATM port network connectivity (ATM-PNC).

Chapter 18: Security, privacy, and safety

System administrator

Authentication, Authorization, and Accounting Services

Authentication, Authorization and Accounting (AAA) Services allow customers to store and maintain administrator account information on a central server. Communication Manager supports account information being stored on an external AAA server or locally on the Communication Manager server itself. Both types of accounts may be used at the same time.

AAA Service interactions with Communication Manager use the Pluggable Authentication Module (PAM) and Name-Switch Service (NSS) features of Linux, which are provided on Linux-based Communication Manager servers.

External AAA support is a Linux process that is separate from Communication Manager, is not controlled by a license file, and is freely available to the customer. Customers can use the same AAA server for Communication Manager as is used by other servers on their network.

Access security gateway

Access security gateway (ASG) is an authentication interface used to secure the system administration and maintenance ports and/or logins on the system. Access security gateway employs a challenge/response protocol to confirm the validity of a user and reduce the opportunity for unauthorized access.

Successful authentication is accomplished when the feature communicates with a compatible key. The challenge/response negotiation is initiated once an RS-232 session is established and a valid system login ID has been supplied by a user. The authentication transaction consists of a challenge, issued by the system and based on the login ID supplied by the user, followed by receipt of the expected response, which is supplied by the user.

Branch gateway enhancements

Access security gateway authentication allows Avaya's Services organization to remotely login to Avaya 8XXX Servers that are under service agreement. To enhance customer support in branch offices, ASG is enhanced to allow authentication capabilities to the G350/G250 gateway product line.

Alternate facility restriction levels

This feature allows Communication Manager to adjust facility restriction levels or authorization codes for lines or trunks. Each line or trunk is normally assigned a facility restriction level. With this feature, alternate facility restriction levels are also assigned. Attendants can change to the alternates, thus changing access to lines and trunks.

You might want to use this feature to disable most long-distance calling at night, for example, to prevent unauthorized staff from making long-distance calls.



CAUTION:

This feature may change the AAR and ARS routing preferences. Using it on tandem and tie-trunk applications affects entire networks. Calls that are part of a cross-country private network may be blocked.

Alternate operations support system alarm number

This feature allows you to establish a second number for Communication Manager to call when an alarm event occurs. This feature is useful for alerting a second support organization, such as INADS or OneVision.

Privacy - attendant lockout

See [Attendant lockout - privacy](#) on page 39.

Authorization codes - 13 digits

Authorization codes extend calling-privilege control and enhance security for remote-access callers. Authorization codes can be up to 13 digits in length.

Avaya site administration authorization codes may be used to:

- 1 Override facility restriction levels assigned to originating stations or trunks
- 1 Restrict individual incoming tie trunks and remote-access trunks from accessing outgoing trunks
- 1 Track CDR calls for cost-allocation purposes
- 1 Provide additional security control

Call restrictions

By dialing an access code, administrators and attendants have the ability to restrict users from making or receiving certain types of calls. There are five restrictions:

- 1 Outward. User cannot place external calls.
- 1 Station-to-station. User cannot place or receive internal calls.
- 1 Termination. User cannot receive any calls (except priority calls).
- 1 Toll. User cannot place toll calls but can place local calls.
- 1 Total. User can neither place nor receive any calls.

Class of Restriction

Defines many different classes of call origination and termination privileges. Communication Manager may have no restrictions, only a single COR, or may have as many classes of restrictions as necessary to effect the desired restrictions. Many different types of classes of restriction can be assigned to many types of facilities on the switch. For example, you can use a calling-party COR to prevent callers from accessing the public network.

Block collect call

See [Block collect call](#) on page 96.

Customer-provided equipment alarm

Provides you with an indication that a system alarm has occurred and that the system has attempted to contact a service organization. A device that you provide, such a lamp or a bell, is used to indicate the alarm situation. You can administer the level of alarm about which you want to be notified.

Data privacy

See [Data privacy](#) on page 175.

Data restriction

See [Data restriction](#) on page 176.

Encryption algorithm for bearer channels

Communication Manager supports the Advanced Encryption Standard (AES) format of signal encryption for IP telephony. This encryption algorithm is in addition to the Avaya proprietary encryption protocol, the Avaya Encryption Algorithm (AEA).

AES encryption is a cryptographic algorithm developed by the U.S. Government to protect unclassified information. Communication Manager uses AES with 128 bit keys in counter mode (AES-128-CTR).

Administration is supported to select a combination of no encryption, AEA encryption, and/or AES encryption on a per codec set basis.

SRTP media encryption

SRTP is a media encryption standard. An end-to-end SRTP implementation includes the following media processing platforms:

- ┆ SIP telephones (SRTP video encryption for SIP is not covered)
- ┆ TN2602AP circuit pack
- ┆ MM760 media module in a G700 Media Gateway
- ┆ G700 VoIP on-board element
- ┆ G450 VoIP element
- ┆ G350 VoIP element
- ┆ G250 VoIP element

Note:

All of these platforms, except for SIP telephones, also support AES and AEA media encryption.

Enhanced security logging

Enhanced security logging increases the granularity of logging of user activity, and provides a single place of customer choosing, external server or Linux syslog, to store the security logs. Along with centralized authentication, enhanced security logging consolidates several existing Communication Manager security log files, and routes the files to an industry standard external log server or the internal Linux syslog.

Enhanced security logging adds these additional security events:

- | Successful and failed admin login
- | Logout
- | Successful and failed endpoint authentication
- | DOS attacks
- | SAT administration changes, including data describing the exact change

Note:

To take advantage of centralized authentication, the customer must have an industry standard RADIUS, Microsoft ActiveDirectory, or LDAP external server. These are not supplied by Avaya.

Facility restriction levels and traveling class marks

Allows certain calls to specific users, while denying the same calls to other users. For example, certain users may be allowed to use Central Office (CO) trunks to other corporate locations while other users may be restricted to less expensive private-network lines. **You can administer up to eight** levels of restriction for users of AAR and ARS.

H.248 link encryption

To provide privacy for media streams carried over IP networks, the H.248 signaling channel between the Avaya 8XXX Server (media gateway controller) and the media gateways is encrypted. This signaling channel is used to distribute the media session keys to the media gateways, and may carry user-dialed authorization codes and passwords.

This feature protects our customer investments by encrypting the signaling channel between the H.248 gateway and server. This feature also protects the media encryption key, PINs, and account codes between the media gateway and the media gateway controller.

Encryption of the H.248 link to any given media gateway may be enabled or disabled through the **Media Gateway** screen. However, the encryption protocol cannot be disabled.

Malicious call trace

Allows you to trace malicious calls. You define a group of terminal users who can notify others in the group when they receive a malicious call. These users can then retrieve information related to the call. Using this information, you can identify the malicious call source or provide information to personnel at an adjacent system to complete the trace. It also allows you to record the malicious call, as well as trace a malicious call over ETSI PRI.

Malicious call trace logging

Malicious call trace logging allows a PC to receive information from Communication Manager to log malicious calls.

Mask station name and number for internal calls

Communication Manager blocks the calling party name and number for internal calls. This feature includes the following capabilities:

- 1 Called party does not see the name or number of the calling party.
- 1 Display of the incoming call is administrable on a system level. For example, customers may administer the display to show “Restricted Call.”
- 1 Blocking of the calling party name and number is administrable on a Class of Restriction (COR) basis, as well as on a call basis (through the CPN Block button).
- 1 The calling party name and number information is available to CDR, vectors, and/or AE Services.

Media encryption

Media Encryption is the encryption of the audio (voice) portion of a Voice Over IP (VoIP) call. Media Encryption can be used to provide enhanced privacy for VoIP communications that involve exchange of sensitive information. Media Encryption is provided between Avaya media gateways and Avaya 8XXX Servers.

Digitally encrypting the audio (voice) portion of a VoIP call can reduce the risk of electronic eavesdropping. IP packet monitors, sometimes called sniffers, are to VoIP calls what wiretaps are to circuit-switched (TDM) calls. One exception is that an IP packet monitor can watch for and capture unencrypted IP packets, and can play back the conversation in real-time or store it for later playback.

Communication Manager encrypts IP packets before they traverse the IP network. An encrypted conversation sounds like white noise or static when played through an IP monitor. End users do not know that a call is encrypted because there are:

- 1 No visual or audible indicators to indicate that the call is encrypted.
- 1 No appreciable voice quality differences between encrypted calls and non-encrypted calls.

SECURITY ALERT:

Be sure that you understand these important media encryption limitations:

- Any call that involves a circuit-switched (TDM) endpoint, such as a DCP or analog telephone, is vulnerable to conventional wire-tapping techniques.
- Any call that involves an IP endpoint or gateway that does not support encryption can be a potential target for IP monitoring. A common example of this is are IP trunks to 3rd-party vendor switches.
- Any party that is not encrypting an IP conference call exposes all parties on the IP call between the unencrypted party and its supporting media processor to monitoring, even though the other IP links are encrypting.

For a list of the supported hardware, software, and firmware requirements for Media Encryption, and a list of the equipment that is not supported, see *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

License file requirements

Media Encryption does not work unless the server has a valid License File with Media Encryption enabled. To determine whether Media Encryption is enabled in the current License File:

1. Type `display system-parameters customer-options` a. Press **Enter**.
The system displays the **Optional Features** screen.
2. Press **Next** until you see the **Media Encryption Over IP** field ([Figure 6: Optional Features screen](#) on page 204).
3. Ensure that the `Media Encryption Over IP` field is set to **y**.

Figure 6: Optional Features screen

```

display system-parameters customer-options                                Page 4 of 11
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                         IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                             ISDN Feature Plus? n
    Enhanced EC500? y                                         ISDN/SIP Network Call Redirection? n
Enterprise Survivable Server? n                                         ISDN-BRI Trunks? y
  Enterprise Wide Licensing? n                                         ISDN-PRI? y
    ESS Administration? n                                         Local Survivable Processor? n
      Extended Cvg/Fwd Admin? y                                         Malicious Call Trace? n
External Device Alarm Admin? n                                         Media Encryption Over IP? y
Five Port Networks Max Per MCC? n   Mode Code for Centralized Voice Mail? n
  Flexible Billing? n
Forced Entry of Account Codes? n                                         Multifrequency Signaling? y
  Global Call Classification? n                                         Multimedia Call Handling (Basic)? y
    Hospitality (Basic)? y                                         Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? n   Multimedia IP SIP Trunking? y
  IP Trunks? y

IP Attendant Consoles? y
(NOTE: You must logoff & login to effect the permission changes.)

```

PIN Checking for Private Calls

This feature restricts users from making private calls (internal or external) by forcing them to enter a Personal Identification Number (PIN) code after dialing a PIN feature access code and only when the PIN is valid, the user can dial the destination digits to make a call. The PIN code used for the call is reported in Call Detail Record (CDR) output with a special character **P**. SIP telephones do not support PIN checking.

Restriction - controlled

Allows an attendant or telephone user, with console permission, to activate and deactivate for an individual telephone or a group of telephones, the following restrictions:

- | outward
- | total
- | station-to-station
- | termination restrictions

Secure shell and secure FTP

The Telnet protocol allows remote access to a network device console that is based on login and password authentication. Beginning with Communication Manager release 3.0, Secure Shell (SSH) provides this capability over an encrypted channel. Similarly, Secure FTP (SFTP) is an encrypted version of the FTP protocol that allows remote file transfers. SSH/SFTP provides a secure alternative for file transfer of firmware download files and voice announcements, as well as secure remote server access.

The **enable filexfer** command enables SSH and SFTP for both the TN799DP Control LAN (CLAN) circuit pack, and the TN2501AP Voice Announcement over LAN (VAL) circuit pack.

The Telnet, FTP, SSH, and SFTP enabling capabilities on the TN2312A/BP IP Server Interface (IPSI) circuit pack continue to be handled through the Communication Manager System Management Interface and the Communication Manager Linux bash shell.

Security of IP telephone config files

This feature supports the inclusion of a digital certificate and the use of TLS to allow an IP telephone to authenticate the server for the download of configuration files. This enables IP telephones to ensure that configuration parameters come only from an authenticated source. Configuration files that are delivered through this mechanism can deliver message digest values for the authentication of software code files delivered through a non-secure connection.

Security of IP telephone registration/H.323 signaling channel

Note:

Please check with your Avaya Sales Representative or your Avaya Authorized Business Partner for availability of this feature.

This feature provides a secure mechanism for an H.323 endpoint and a Communication Manager gatekeeper to mutually authenticate themselves and the contents of the messages that they exchange during IP registration, admission, and status (RAS). This authentication is based on the simple 3-to-8 digit PIN administered for each extension.

Execution of Encrypted Key Exchange (EKE) procedures during RAS results in the negotiation of a strong secret that is shared between the endpoint and the gatekeeper. This strong secret is used to derive a set of secrets which are used to digitally sign all RAS and call signaling messages, and to encrypt selected elements of call signaling messages, media session keys and CCMS messages. If one or the other parties does not possess the correct PIN, the computed shared secrets will, in fact, be different. Message authentication fails, and the parties refuse to communicate.

In summary, these procedures permit:

- 1 The endpoint and the gatekeeper to authenticate each other;

- 1 The endpoint and the gatekeeper to sign/authenticate each message sent;
- 1 Privacy for selected elements of call signaling, including media session encryption keys and dialed digits.
- 1 Security of the endpoint/gatekeeper communication even if an observer obtains the user's PIN.
- 1 Security of past or future communications even if one session is penetrated by an attacker with knowledge of the PIN. (This is known as “perfect forward secrecy”.)
- 1 Reuse of the negotiated strong secret (identified by a unique session ID) to secure new signaling links between parties for re-registration or trunking.

Security Violation Notification

Security Violation Notification (SVN) allows you to set security-related parameters and to receive notification when the limits that you have established are violated. You can run reports related to both valid and invalid access attempts. You can also disable a login ID or remote access authorization that is associated with a security violation.

Signaling encryption for SIP trunks

Signaling encryption for SIP trunks protects customer investments by encrypting the voice channel over SIP trunks. Signaling encryption for SIP trunks is accomplished by using TLS and protects customer investments by encrypting signaling data and instant messages.

Station security codes

To provide additional security around the customer options the “init” login has been provided with additional security for the purpose of establishing an authentication procedure for attempts to remotely log into the system.

Tripwire security

Tripwire is a security program provided on all Linux-based Avaya 8XXX Servers. The list of files that Tripwire monitors needs to be determined during design when all administration and configuration files have been identified.

If there are any detected security violations, Tripwire reports its findings through the security log. These events generate an alarm.

Note:

Tripwire normally reports security violations through e-mail. However, by reporting events to the security log, security violations can be immediately acted upon.

End user

Backup alerting

Notifies backup attendants that the primary attendant cannot pick up a call. It provides both audible and visual alerting to backup stations when the attendant queue reaches its queue warning level. When the queue drops below the queue warning level, alerting stops. Audible alerting also occurs when the attendant console is in night mode, regardless of the attendant queue size.

Barrier codes

A barrier code is a security code that is used with remote access to prevent unauthorized access to your system. To increase your system security, use a 7-digit barrier code with remote access barrier code aging. A barrier code automatically expires if an expiration date or number of accesses has exceeded the limits you set. If both a time interval and access limits are administered for a barrier code, the barrier code expires when one of the conditions is satisfied.

Note:

Barrier codes are not tracked by call detail recording (CDR). Barrier codes are incoming access codes, whereas, authorization codes are primarily outgoing access codes.

Calling/Connected Party Number restriction

Per call CPN restriction

Users may indicate calling number privacy information. For ISDN calls, the CPN presentation indicator is encoded accordingly. For non-ISDN calls going to a public network that supports the CPN restriction feature, the network specific feature activation code gets passed to the network for interpretation and activation of the desired feature.

If per call CPN restriction is activated for an outgoing call, it will override any per line CPN restriction administration for the calling station, and will override any ISDN trunk group administration for sending calling number.

Per line CPN restriction

Users may block the calling party number when originating calls. For ISDN calls, the CPN presentation indicator is encoded accordingly. For non-ISDN calls, going to a public network that supports the CPN restriction feature, the network specific feature activation code gets passed to the network for interpretation and activation.

If per line CPN restriction is administered for a station, it will override any ISDN trunk group administration for sending calling party number.

Crisis alerts to a digital numeric pager

Crisis alert can also send notification of an emergency call to a digital pager. In this case, it sends a message of 7-digits to 22-digits to the pager and displays a crisis alert code, an extension and room number, and a main number (if one is entered). The person paged thus knows the origin of the emergency call and can direct emergency-service response to the appropriate location.

To use crisis alert with a digital pager, the system is administered so that at least one digital set has a CRSS-ALRT button and the `Alert Pager` field is set to `y`. Any station with a CRSS-ALRT button and a pager receives the correct alert.

Crisis alerts to a digital station

Crisis alert uses both audible and visual alerting to notify administered digital display stations when an emergency call is made. Audible alerting sounds like an ambulance siren. Visual alerting flashes the CRSS-ALRT button lamp and displays the name and extension, or room, of the caller. The crisis alert display of the origin of the emergency call enables the attendant or other user to direct emergency-service response to the caller.

When crisis alerting is active, the station is placed in position-busy mode so that other incoming calls can not interfere with the emergency call notification. The station can still originate calls to allow notification of other personnel.

If an emergency call is made while another crisis alert is still active, the incoming call will be placed in the queue. If the system is administered so that all users must respond, then every user must respond to every call, in which case the calls are not necessarily queued in the order in which they were made. If the system is administered so that only one user must respond, the first crisis alert remains active at the telephone where it was acknowledged. Subsequent calls are queued to the next available station in the order in which they were made.

Crisis alerts to an attendant console

Crisis alert uses both audible and visual alerting to notify attendant consoles when an emergency call is made. Audible alerting sounds like an ambulance siren. Visual alerting flashes the CRSS-ALRT button lamp and displays the name and extension, or room, of the caller. The crisis alert display of the origin of the emergency call enables the attendant or other user to direct emergency-service response to the caller. Though often used in the hospitality industry, it can be set up to work with any standard attendant console.

When crisis alerting is active, the console is placed in position-busy mode so that other incoming calls can not interfere with the emergency call notification. The console can still originate calls to allow notification of other personnel. Once a crisis alert call has arrived at a console, the console user must press the position-busy button to unbusy the console, and press the crisis-alert button to deactivate audible and visual alerting.

If an emergency call is made while another crisis alert is still active, the incoming call will be placed in the queue. If the system is administered so that all users must respond, then every user must respond to every call, in which case the calls are not necessarily queued in the order in which they were made. If the system is administered so that only one user must respond, the first crisis alert remains active at the telephone where it was acknowledged. Subsequent calls are queued to the next available station in the order in which they were made.

Emergency access to the attendant

Provides for emergency calls to be placed to an attendant. These calls can be placed automatically by the system or can be dialed by system users. Emergency access calls can receive priority handling by the attendant.

E911 CAMA trunk group

See [E911 CAMA trunk group](#) on page 134.

Hot Desking Enhancement

Hot Desking is a generic term for features that allow end users to lock and unlock their telephones or to move fully customized station profiles to another compatible telephone.

Hot Desking enhances the existing features:

- ┆ IP Login/Logoff
- ┆ PSA Association/Dissociation
- ┆ Station Lock and Time of Day Station Lock

Parts of the enhancement require firmware changes for the telephones. Only the 96xx-series H.323 IP telephones with the appropriate firmware change support the full range of HDE.

Privacy - auto exclusion

When the class of service (COS) is set for the automatic exclusion option, the feature is activated when you take your telephone off-hook. The feature can be deactivated when you push the exclusion button before dialing a call or during a call. An excluded call that is on hold can be taken off hold by any telephone that has a bridged appearance of the telephone that put the call on hold.

Privacy - manual exclusion

Allows multi-appearance telephone users to keep other users with appearances of the same extension number from bridging onto an existing call. Exclusion is activated by pressing the exclusion button on a per-call basis.

Restriction - controlled

See [Restriction - controlled](#) on page 204.

Station lock

Station lock allows users to lock their telephones to prevent unauthorized outgoing calls. Users can block outgoing calls and still receive incoming calls. This feature is activated by pressing a telephone button or dialing a feature access code (FAC), along with a station security code (SSC).

Station lock allows users to block all outgoing calls, except for emergency calls, on all telephones, unless the telephone is pre-administered. An example of a pre-administered telephone is a telephone that is administered to block all outgoing calls except for emergency calls. Telephones can be remotely locked and unlocked.

While the Hot Desking Enhancement (HDE) feature is active and a station is locked, the following restrictions apply:

- ┆ No access to telephone capabilities (applies to 96xx H.323 IP telephones with firmware changes)
- ┆ No access to Call log
- ┆ No access to Avaya menu

- | No access to Contact list
- | No access to USB
- | No access to Redial button
- | No bridging on EC500 calls
- | No access to bridged appearances

Additionally, if Hot Desking Enhancement is enabled, some telephone capabilities and some Communication Manager capabilities are locked.

Station lock by Time of Day

The Time of Day (TOD) Station Lock feature allows a customer to lock and unlock one or more stations using a TOD schedule.

For more information, see [Time of day](#) on page 240.

Note:

Station Lock by TOD cannot override a station that has been manually locked. The Station Lock by TOD feature cannot release the manually locked station when the schedule allows the release. If a user unlocks the station that was locked by the TOD Station Lock feature, the station stays unlocked until the next TOD lock interval.

Chapter 19: System management

Communication Manager system management provides the administrator powerful tools to maintain their communication solutions and to drive down the total cost of ownership.

Administration change notification

Administration change notification enables Communication Manager to communicate with the Avaya Directory Enabled Management (DEM) client. This feature enables the client to have real-time, integrated, directory-based, read/write access to Communication Manager administration data based on rules defined by the customer. Administration change notification enables the client to subscribe to notifications of changes to administration data in Communication Manager. It thus provides real-time updates whenever administration changes occur in a particular object (for example, a station).

Administration Without Hardware

See [Administration Without Hardware](#) on page 113.

Alternate facility restriction levels

This feature allows Communication Manager to adjust facility restriction levels or authorization codes for lines or trunks. Each line or trunk is normally assigned a facility restriction level. With this feature, alternate facility restriction levels are also assigned. Attendants can change to the alternates, thus changing access to lines and trunks. You might want to use this feature to disable most long-distance calling at night, for example, to prevent unauthorized staff from making long-distance calls.



CAUTION:

This feature may change the AAR and ARS routing preferences. Using it on tandem and tie-trunk applications affects entire networks. Calls that are part of a cross-country private network may be blocked.

Announcements

Use the Announcements feature to administer announcements that play for callers to your business. For example, you can inform callers that the call cannot be completed as dialed, the call is in a queue, or that all lines are busy. An announcement is often used in conjunction with music. Announcements can be *integrated* or *external*.

- ┆ Integrated announcements reside on a circuit pack in the carrier.
- ┆ External announcements are stored on an adjunct, and are played back from the adjunct equipment.

Authorization codes - 13 digits

See [Authorization codes - 13 digits](#) on page 198.

Automatic circuit assurance

Assists in identifying possible trunk problems. Communication Manager maintains a record of the performance of individual trunks and automatically calls a designated user when a possible failure is detected. This feature provides better service through early detection of faulty trunks and consequently reduces out-of-service time.

Automatic transmission measurement system

Measures voice and data trunk facilities for satisfactory transmission performance. The measurement report contains data on trunk signal loss, noise, signaling return loss, and echo return loss. Acceptable performance, the scheduling of tests, and report contents are administrable.

Avaya Directory Enabled Management

Avaya Directory Enabled Management (DEM) provides real-time, integrated, directory-based read/write access to Avaya 8XXX Servers and INTUITY AUDIX messaging servers. It streamlines workflow and information management in an electronic environment using converged networks.

DEM creates a meta-directory for converged voice and data networks. It synchronizes directory information with data from Communication Manager and INTUITY devices, and stores the information in an LDAP-compliant directory service, for example, eDirectory from Novell, or active directory from Microsoft. Directory-enabled applications can then use the DEM to implement workflow processes that automate various system management functions and speed business operations.

Avaya Integrated Management

Avaya Integrated Management is a systems management software suite that contains applications to manage a converged voice and data network. The applications include:

- | network management
- | fault management
- | performance management
- | configuration management
- | directory management
- | policy management functionality

Communication Manager configuration manager

Avaya configuration manager provides centralized management of distributed network and campus environments, using a single point of entry and graphical Web-based interface for configuration and administration of multiple Avaya 8XXX Servers.

Communication Manager fault/performance manager

Communication Manager fault/performance manager integrates with Avaya multiservice network manager to provide a system view of your converged network. Fault manager displays a hierarchical view of devices and their status, allowing you to view and isolate alarms and errors. Performance manager provides a comprehensive set of performance reports for trending and isolation of performance issues.

Avaya site administration

Avaya site administration is a Microsoft Windows-based graphical user interface for making changes, adding or moving users, and performing basic traffic analysis.

Voice Announcement over LAN manager

Avaya Voice Announcement over LAN (VAL) Manager is part of the Avaya Integrated Management suite of products. It enables you to the use of a LAN to transfer recorded announcements to Avaya 8XXX Servers.

Announcements can be stored in **.wav** files, which can be sent to a voice announcement over LAN board without conversion. The voice announcement over LAN manager also provides a repository to backup and restore announcement files, and simplifies administration. With voice announcement over LAN manager, you can view the current status of announcements, easily add, change, and remove announcements, and copy and backup announcement files from Avaya 8XXX Servers to the voice announcement over LAN manager and back, through the LAN.

Increased announcement support

Communication Manager release 4.0 increases support for announcements, but only on the XL systems, for example, S8720XL servers. A new license file is required to increase the number of VAL boards in a customer's configuration, even if a customer upgrades to an S8720XL.

- 1 Support for TN2501 (VAL) boards within a single Communication Manager configuration is increased from 10 to 128.
- 1 The number of touch tone receivers (TTRs) in a system is increased from 1,200 to 8,000. This does not apply to H.248 gateways since H.248 gateways use a separate TTR resource.
- 1 The total number of supported announcements is increased from 3,000 to 9,000. This applies to VAL boards (TN2501) and the vVALs. As a result of this increase, the way in which announcements are administered is also modified.

- 1 The number of announcement files that are supported on the TN2501 circuit pack is increased from 256 to 1024. This increase is supported on non-XL systems.

Note:

While the TN750 circuit packs still exist, they are no longer supported. In other words, full functionality is not available on LINUX systems. If used, they are included in the 128 total announcement boards in the system.

In Communication Manager Release 5.2, the G450 H.248 gateway allocates announcement time slots dynamically as needed. The Avaya G450 introduces a removable external compact flash that supports the backup and restore of 1024 announcement files (up to 4 hours of storage). This requires a memory upgrade to 512MB from the base 256MB.

Avaya VoIP Monitoring Manager

Avaya VoIP monitoring manager (VMON) provides the ability to monitor voice over IP (VoIP) network quality. This web-based application receives QoS statistics from Avaya IP end points and displays the data via graphs and reports, so administrators can isolate voice quality problems and send traps when poor voice quality is detected.

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol version 3 (LDAPv3) is an industry compliant protocol for accessing online directory services. A directory is like a database, but tends to contain more description information. Communication Manager integrates with LDAP datastores through the use of the administration change notification feature and Avaya directory enabled management client application to provide real-time, integrated, directory-based read/write access to Communication Manager and INTUITY AUDIX messaging servers.

Barrier codes

See [Barrier codes](#) on page 207.

Bulletin board

Provides a place on the switch where you can post information and receive messages from other switch users, including Avaya personnel. Anyone with appropriate permissions can use

the bulletin board for everyday messages. In addition, Avaya personnel can leave high-priority messages that are displayed on the first ten lines of the bulletin board.

Busy verification of telephones and trunks

Allows attendants and users of multi-appearance telephones to make test calls to trunks, telephones, and hunt groups to check the status of an apparently busy resource. With this feature, an attendant or multifunction telephone user can distinguish between a telephone that is truly busy and one that only appears busy because of some problem. You can also use the feature to quickly identify faulty trunks.

Call charge information

Provides two ways to know the approximate charge for calls made on outgoing trunks:

- 1 Advice of Charge, for ISDN trunks

Advice of Charge (AOC) collects charge information from the public network for each outgoing call. Charge advice is a number representing the cost of a call; it is recorded as either a charging or currency unit.

- 1 Periodic pulse metering, for non-ISDN trunks

Periodic Pulse Metering (PPM) accumulates pulses transmitted from the public network at periodic intervals during an outgoing trunk call. At the end of the call, the number of pulses collected is the basis for determining charges.

Call-charge information helps you to account for the cost of outgoing calls without waiting for the next bill from your network provider. This is especially important in countries where telephone bills are not itemized. You can also use this information to let employees know the cost of their telephone calls, and so encourage them to help manage your company telecommunications expenses.

Note:

This feature is not offered by the public network in some countries, including the United States.

In addition, the pass advice of charge to BRI endpoints feature will transparently pass AOC information that has been received from PRI networks to WCBRI endpoints.

Call Detail Recording

Records detailed call information on incoming and outgoing calls for the purpose of call accounting, and sends this call information to a Call Detail Recording (CDR) output device. You can specify the trunk groups and extensions for which you want records to be kept as well as the type of information to be recorded. You can keep track of both internal and external calls. This application contains a wide variety of administrable options and capabilities.

Call Detail Recording display of physical extension

For Expert Agent Selection (EAS) agent-originated calls, if the `Record Agent ID on Outgoing?` field on the **CDR System Parameters** screen is set to **y** (the default value), then the agent ID is used for outgoing calls.

If the `Record Agent ID on Outgoing?` field on the **CDR System Parameters** screen is set to **n**, the physical extension is used.

Legacy CDR and Survivable CDR

You can have Legacy, or Conventional CDR or Survivable CDR for your system. Both methods provide the identical call accounting information and support the same CDR formats.

In a Legacy CDR environment, Communication Manager generates all CDR records to the active server and then exports the records to a CDR adjunct (using IP links) for further processing. In these systems, the CDR adjunct functions in a “listen only” mode receiving the records sent by Communication Manager. This type of CDR processing was used exclusively in Communication Manager up through Release 3.X. In a Legacy CDR environment, the system cannot collect CDR records when link between main, LSP and/or ESS and CDR adjunct is down (this is generally the case when a LSP or ESS is active). It also requires the IP link between Communication Manager and the CDR adjunct to be up at all times.

Communication Manager introduced a new method of data collection called Survivable CDR. Survivable CDR allows CDR data records to be stored on the local hard drive of Communication Manager, if desired. The CDR adjunct then periodically polls each the Communication Manager server and collects the CDR data files from the servers. The Survivable CDR is supported on all Communication Manager platforms, that is, on the main, LSPs, and ESS. Survivable CDR allows CDR data to be transferred in an encrypted manner from the Communication Manager server to the CDR adjunct using the Secure File Transfer Protocol (SFTP). Note that Survivable CDR requires updated CDR adjuncts. CDR records are stored and transferred in batches, rather than one record at a time as with Legacy CDR.

Call restrictions

By dialing an access code, administrators and attendants have the ability to restrict users from making or receiving certain types of calls. There are five restrictions:

- ┆ Outward. The user cannot place external calls.
- ┆ Station-to-station. The user cannot place or receive internal calls.
- ┆ Termination. The user cannot receive any calls (except priority calls).
- ┆ Toll. The user cannot place toll calls but can place local calls.
- ┆ Total. The user can neither place nor receive any calls.

Calling party/billing number

Allows the system to transmit calling party number/billing number (CPN/BN) information to an ISDN-PRI trunk group. The CPN is the calling party telephone number. BN is the calling party billing number. The CPN/BN may contain international country codes. It is used with an adjunct application.

Class of Restriction

See [Class of Restriction](#) on page 199.

Class of Service

Defines whether or not telephone users have permission to access features and functions. You can administer a station to have access to up to 16 Classes of Service. In Communication Manager, you can also administer Classes of Service on a per-tenant basis if you use partitioning in your system. You can administer up to 100 COS groups, each with 16 Classes of Service. This can be useful in controlling service to the stations and attendant of different tenants.

Examples of features and functions controlled by Class of Service:

- ┆ Automatic callback

- | Call forwarding
- | Data privacy
- | Priority calling
- | Restrict call forwarding off-net
- | Call forward busy/do not answer
- | Extended forwarding and busy/do not answer
- | Personal station access
- | Trunk-to-trunk transfer restriction override
- | Off-hook alert
- | Console permission
- | Client room

Classless Interdomain Routing

See [Classless Interdomain Routing](#) on page 151.

Concurrent user sessions

In order to increase the efficiency of administration and maintenance functions, the Communication Manager accommodates multiple concurrent administration and maintenance user sessions. Three or more devices (management terminals or operation support systems) can be connected to the switch to perform administration and/or maintenance tasks simultaneously.

Communication Manager supports eight concurrent administration and maintenance users. Five can perform concurrent administration, and three can perform concurrent maintenance. The eight concurrent sessions can be in any combination of local and remote connections.

Customer-provided equipment alarm

See [Customer-provided equipment alarm](#) on page 199.

Customer telephone activation

Enables customers to install their own telephones, eliminating the need for a service technician to do the installation. This feature is based on the TTI feature and allows the customer to associate a physical telephone with a station translations switch.

CTA is a streamlined version of TTI; it has a fixed feature-access code but does not require a security code. In addition, CTA allows only for “merging” of telephones with station translations, whereas TTI allows for both “merging” and “unmerging” of telephones with station translations.

CTA applies only to DCP and analog touch-tone, circuit-switched telephones.

DCS automatic circuit assurance

Allows a user or attendant at one node to activate or deactivate automatic circuit assurance referral calls for the entire DCS network. This transparency allows the referral calls to originate at a node other than the node that detects the problem.

External device alarming

Allows you to assign analog ports to alarm interfaces for external devices. You can specify a port location, information to identify the external device, and the alarm level to report when a contact closure occurs.

Facility busy indication

Allows users of multi-appearance telephones to see which lines, trunk groups, terminating extension groups, hunt groups, or paging zones (called resources or facilities) are busy. When the lamp associated with the resource is lit, the resource is busy.

You can store extension numbers, trunk group access codes, and loudspeaker paging access codes in a facility busy indication button. The facility busy indication button provides direct access to any of the facilities.

Facility restriction levels and traveling class marks

Allows certain calls to specific users, while denying the same calls to other users. For example, certain users may be allowed to use central office (CO) trunks to other corporate locations while other users may be restricted to less expensive private-network lines. **You can administer up to eight** levels of restriction for users of AAR and ARS.

Facility test calls

Allows telephone users to make test calls to access specific trunks, dual tone multifrequency receivers, time slots, and system tones. The user dials an access code and makes the test call to make sure the facility is operating properly. Security measures are included to prevent unauthorized use.

Firmware download

The firmware download feature allows you to download an image from a remote or local source into the system running Communication Manager, and use that image to reprogram the application code of a port circuit pack. This feature makes updating firmware more cost effective. This feature also reduces the expense of servicing the system port circuit packs because it eliminates the need for a technician to be involved when a board is updated. Firmware download is achieved using the TN799C CLAN interface.

Note:

Circuit packs that can be updated with the firmware download feature have a “P” at the end of their TN number.

Five EPN maximum in MCC1 Media Gateways

Note:

This feature is for MCC1 Media Gateways when used with an S87XX Server or DEFINITY® Server R configurations only.

This optional software feature allows customers that require high calling traffic capacities to have from two to five expansion port networks (EPN) in a single MCC1 Media Gateway. Only two port networks (PN) are generally available unless a specialized cable was purchased from Avaya and work-arounds were performed in software administration to make additional carriers function as EPNs.

When this feature is activated, Communication Manager enables administration of up to five carriers as EPNs and no custom cables are necessary. This means that the full bandwidth of the TDM bus is available to each carrier while still enabling the customer to have the footprint of an MCC1 Media Gateway. This is especially appealing to call centers without IPSI/PNC duplication, where systems can be quite large and heavily utilized.

The hardware limitation of the MCC1 Media Gateway is five port carriers. All five can be expansion port carriers, although traffic considerations may dictate some number less than that which is optimum. For example, a customer may choose to have three EPN carriers and two standard port carriers.

There is only one maintenance board, which is placed in carrier A. This is the only maintenance board in the cabinet.

Note:

Only two PNs are physically supported in S87XX Server IPSI-enabled systems when high/critical reliability options are desired. Only two PNs are physically supported in DEFINITY Server R systems when critical/ATM Network Duplication reliability is desired.

For more information on this feature, see your local Avaya representative.

Information and reports

1 Attendant position report

The attendant position report lists the following:

- Attendant usage
- Number of calls answered
- Total time the attendant was available to answer a new call
- Average holding time on calls answered

1 Avaya Software Compatibility Audit (ASCA) tool

The Avaya Software Compatibility Audit (ASCA) tool allows a customer to:

- Run a report on the software and firmware versions that are active on their system
- Compare their software and firmware versions with the latest Avaya releases, and indicating the suggested upgrades

1 Blockage study report

1 Call coverage reports

The call coverage report displays measurements of the distribution of traffic offered to call-coverage groups. Separate reports for all calls and external calls are supplied.

1 Coverage points report

The coverage points report differs based on whether all calls or external calls is selected. For each coverage point in the group, the number of calls offered, abandoned while at that coverage point, and overflowing to the next coverage point are listed.

1 Display ARP reports

1 Emergency and journal reports

The emergency and journal report is based on information from all crisis alerts.

1 Hunt group measurements report

1 IP reports

System management

1 Packet error history report

Provides a 24-hour history of important packet level statistics that indirectly indicate some LAN performance characteristics. The 24-hour history gives the ability to look back at these measures if the trouble cleared.

1 Port network and link usage report

1 Processor occupancy report

The processor occupancy report provides summary information on how heavily the processor is loaded.

1 Recent change history report

Allows the system manager to view or print a history report of the most recent administration and maintenance changes on the switch. This report may be used for diagnostic or information purposes.

1 Refresh route reports

1 Summary report

The summary report provides a performance summary of your system running Communication Manager.

1 Tandem traffic report

The tandem traffic report provides information on facilities that serve tandem traffic.

1 Tracelog

The Tracelog, among other things, lists:

- all IP endpoint registrations
- all IP endpoint unregistrations
- all Ethernet interfaces coming into service
- all Ethernet interfaces coming out of service

These events are tagged as a new log type.

1 Traffic reports

Traffic reports show measurements in the format of switch-based reports for local or remote access, and can be collected for subsequent analysis and reporting by adjuncts and operation support systems using the operation support system interface protocol.

1 IP traffic measurements reports

These reports show DSP activity on IP port networks and IP media processors for specific regions and time periods. DSP measurements are also available for H.248 gateways.

1 Voice/Network Statistics reports

The voice/network statistics reports show hourly and summary level measurement data on packet loss, jitter, round trip delay, and data calls.

- 1 Trunk group detailed measurements

Enhanced logging of user actions

Enhanced logging in Communication Manager servers increases logging of user actions. The following major enhancements are included:

- 1 Modifying the Communication Manager software to log administrator activity in the System Administration Terminal (SAT) to the Linux syslog.
- 1 Providing the ability for the system administrator to define what SAT activity is logged and at what level, including the ability to log changed values both prior to and following a change.
- 1 Enhancing logging of web pages.
- 1 Ensuring that all non-debugging logs use **syslog** and that logs can be sent to a network **syslog** server of the customer's choosing.

Parsing capabilities for the history report

The history report provides details about every data command. You can use parsing options to limit the data returned in this report. The following table identifies the parsing options that are available.

Note:

You can display these options by entering the command `list history`, then clicking **HELP** or pressing **F5**.

| Option | Description |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| date | Specify the month (MM) or day (MM/DD) for which to display history data. |
| time | Specify the hour (HH) or minute (HH:MM) for which to display history data. |
| login | Specify the login for which you wish to display history data. |
| action | Specify the command action (the first word of the command string) for which you wish to display history data. You can view the list of available command actions by clicking HELP or pressing F5 at the command line. |
| 1 of 2 | |

| Option | Description |
|-----------|---------------------------------------------------------------------------|
| object | Specify the command object for which you wish to display history data. |
| qualifier | Specify the command qualifier for which you wish to display history data. |
| 2 of 2 | |

To limit the data displayed in the history report, enter the command **list history** followed by a space and the appropriate parser and, if applicable, format. Only the data for the specified parsers will appear in the report.

You can include multiple parsers, but only a single instance of any parser (for example, you may parse for **date**, **time**, and **login**, but not for **date**, **time**, and two different **logins**).

IP asynchronous links

See [IP asynchronous links](#) on page 176.

Malicious call trace

The New Malicious Call Identification (MCID) feature enables your server to signal to an ETSI ISDN network when the network should record the source of an incoming call. For more information, See [Malicious call trace](#) on page 202.

Malicious call trace logging

See [Malicious call trace logging](#) on page 202.

Music-on-hold

Automatically provides music, silence, or tone to a caller. Music lets the caller know that the connection is still valid.

Local music-on-hold

The music on hold feature is supported on the G700 Media Gateway with Communication Manager. The music source is connected to a port on the MM711 Analog Media Module. Local music-on-hold is part of the call center functionality on the S8300 Server.

Local music-on-hold allows one music source. To use multiple music sources on a G700 Media Gateway, you must use multiple ports on the MM771 Analog Media Module, one for each music source.

For more information, see *Installation for Adjuncts and Peripherals for Avaya Aura™ Communication Manager*. Also see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Multiple music sources

On an MCC1, SCC1, CMC1, or G600 Media Gateway, this feature allows the customer to provide multiple distinct music sources for use with the call vectoring features, calls placed on hold, calls awaiting pickup, and so on. By purchasing the multiple music-on-hold (also called tenant partitioning) feature, you can have up to 100 music sources.

Many different music options can be administered to accommodate different tenants. See [Tenant partitioning](#) on page 230.

Restriction - controlled

Allows an attendant or telephone user, with console permission, to activate and deactivate for an individual telephone or a group of telephones, the following restrictions:

- | outward
- | total
- | station-to-station
- | termination restrictions

Scheduling

Functional scheduling in Communication Manager allows you to specify the time a command will be executed or to specify that it should be executed on a periodic basis. Only commands that do not require user interaction after being entered on the command line (such as list, display, test) can be scheduled.

Security Violation Notification

See [Security Violation Notification](#) on page 206.

Station security codes

See [Station security codes](#) on page 206.

Tenant partitioning

Allows partitioning of the system in order to lease the system services and features to multiple tenants. This provides attractive services and revenue for “virtual” landlords. It provides the robust features of a large system at affordable rates to small business tenants. Depending on the platform, or server, you are using, Communication Manager supports multiple partitions and attendant groups.

Multiple attendant groups can be assigned to each partition. Stations, hunt groups, and other endpoints assigned to a Class of Service (COS) can be partitioned. Network routing pattern preferences also support the assigned tenant partitioning. Tenant partitioning also allows you to assign a unique music source for each tenant partition for customers who are put on hold.

See [Music-on-hold](#) on page 228.

Terminal Translation Initialization

See [Terminal Translation Initialization](#) on page 119.

Time of day clock synchronization through a LAN source

Customers need accurate and common time of day time source across multiple switches in a network. This is especially important when customers are using a central Avaya Call Management System (CMS) to report events coming from multiple servers running Communication Manager.

The time of day clock synchronization through a LAN source feature is implemented on two different platforms:

- 1 Linux
- 1 UNIX

Linux platforms

Communication Manager that is running on Linux-based Avaya 8XXX Servers synchronizes time directly from a LAN source.

UNIX platforms

Communication Manager running on DEFINITY servers which use an Oryx/Pecos operating system (proprietary UNIX-based OS) receives a command from Avaya site administration to adjust the time. Avaya site administration is synchronized to the LAN PC's clock.

Trunk group circuits

Trunks provide the communications links between Communication Manager and other switches, including central office switches and other premises switches. Trunks that perform the same function are grouped together and administered as trunk groups. Trunks interface with Communication Manager through port circuit packs.

Variable length ping

See [Variable length ping](#) on page 163.

Variable Length Subnet Mask

See [Variable Length Subnet Mask](#) on page 164.

Chapter 20: Telecommuting and remote office

Coverage of calls redirected off-net

Coverage of calls redirected off-net (CCRON) allows calls that have been redirected to locations outside of the switch to return to the switch for further processing.

For example, an employee that telecommutes can have two coverage paths. One coverage path is used when the employee is in the office and the other coverage path is used when the employee is working from home. The coverage path used from home takes a call to the employee work telephone, and covers the call to the employee home telephone. If the employee does not answer the call or is busy on another call, the call is redirected back to the switch for further processing, such as coverage to voice mail.

Remote call coverage and call forwarding off-net allow calls to be redirected to a remote location. This allows you to have calls placed to your on-site office redirected to your home office. You can administer the system to either monitor calls and bring them back for additional processing if not answered or to leave calls at the remote (off-net) location.

Extended user administration of redirected calls (telecommuting access)

Extended user administration of redirected calls (also called telecommuting access) allows you to change the lead call coverage path or forwarding extension from any on-site or off-site location. Thus you can change the path or extension from your home office, for example.

IP Softphone and IP Agent - RoadWarrior mode

See [IP Softphone and IP Agent - RoadWarrior mode](#) on page 84.

IP Softphone and IP Agent - Shared Control mode

See [IP Softphone and IP Agent - Shared Control mode](#) on page 84.

IP Softphone and IP Agent - Telecommuter mode

See [IP Softphone and IP Agent - Telecommuter mode](#) on page 84.

IP Softphone

See [Avaya IP Softphone](#) on page 83.

Off-premises station

A trunk-data module connects off-premises private-line trunk facilities and Communication Manager. The trunk-data module converts between the RS-232C and the DCP, and can connect to DDD modems as the DCP member of a modem pool.

See [Call redirection](#) on page 240 and [Call vectoring](#) on page 59.

Remote access

Permits authorized callers from remote locations to access the system via the public network and then use its features and services. There are a variety of ways of accessing the feature. After gaining access, you hear a system dial tone, and, for system security, may be required to dial a barrier code.

Chapter 21: Telephony

Abbreviated Dialing

Abbreviated Dialing (AD) provides lists of stored numbers you can use to:

- ▮ Place local, long-distance, and international calls
- ▮ Activate features
- ▮ Access remote computer equipment

You simply dial the list number and the one-digit, two-digit, or three-digit number associated with the telephone number you want. The number is then automatically dialed by the system. A frequently called number can be stored on an abbreviated dialing button that you need only press once to make the call.

Abbreviated dialing labeling

An administrator can type personalized labels for the Abbreviated Dialing (AD) System List entries. Users of the 2420 DCP telephone, as well as the 4600-series, 6400-series, and 8400-series display telephone sets, can administer labels for the AD softkey buttons. These personalized labels appear on the menu display.

These personalized labels can be administered in the standard supported languages (English, French, Italian, Spanish, and a user-defined language). If a personalized label has not been administered for the AD system list entry, the feature button label that is downloaded to the telephone is **ADnn**, where **nn** is the abbreviated dialing number.

Note:

This enhancement applies only to the AD system list.

Abbreviated dialing on-hook programming

On-hook programming allows users of the 2420 DCP telephone, as well as the 4600-series, 6400-series, and 8400-series telephone sets with enabled speakers, to access the programming mode without going off-hook during available call appearances. Signaling changes from DTMF to the S-channel, allowing the use of a longer (60 seconds) time-out period. Signaling will remain DTMF and the current time-out period of 10 seconds will still apply to non-display telephone sets.

ABCD tone support

The support of signaling messages for generating DTMF tones for the characters A, B, C, and D is added to the H.248 gateway family. These tones are generated on both line-side and trunk-side interfaces on the H.248 gateways for purpose of supporting signaling for our voice adjunct applications. These applications currently include:

- ┆ Voice Response Units (VRU) for Call Center
- ┆ Call-me, Find-me, auto-attendant transfer, blind-transfer features for Modular Messaging
- ┆ MLPP (Multi-Level Precedence & Preemption) feature for military/government applications

Active dialing

6400-series and 4600-series telephone sets have a dialing option where the set will send S-channel button codes when the user presses a number on the dial pad when on-hook.

Administrable timeout on call timer

Enhances the call timer feature on the 6400-series telephones. The call timer feature measures the duration of a call, starting a timer when the call is answered and stopping the timer when the call is dropped.

Previously, the call timer feature displayed the duration of the call for only five seconds after the call was dropped. The administrable timeout on call timer feature allows the user to specify how long to display the duration of the call.

Alphanumeric dialing

See [Alphanumeric dialing](#) on page 89.

Automatic Call Back

Automatic Call Back (ACB) allows users who placed a call to a busy or unanswered telephone on an internal or public network to be called back automatically when the called telephone becomes available.

When a user activates automatic callback, the system monitors the called telephone. When the called telephone becomes available to receive a call, the system originates the automatic callback call. The originating party receives priority ringing. The calling party then lifts the handset and the called party receives the same ringing provided on the original call.

Automatic Call Back allows queuing of called parties. This feature works on analog, DCP, IP (H.323), and SIP telephones.

Automatic Call Back for analog telephones

When a person, using an analog telephone, places a call and the line is busy, an announcement prompts the caller to enter the digit 1 to activate ACB, or to enter the digit 2 to route the call to a hunt group extension.

Automatic hold

Allows attendants and multi-function telephone users to alternate easily between two or more calls. For example, with automatic hold, selection of a second call automatically puts the active call (if any) on hold and makes the second call active. This feature can be activated on a system-wide basis only. When automatic hold is not activated, the selection of the second call drops the first call.

Avaya video telephony solution

The Avaya Video Telephony Solution enables Communication Manager to merge a set of enterprise features with Polycom's video conferencing adjuncts. It unifies Voice over IP with video, Web applications, Avaya's video enabled IP softphone, third-party gatekeepers, and other H.323 endpoints.

The following components are part of the Avaya Video Telephony Solution feature:

Telephony

- 1 Polycom VSX3000, VSX7000 and VSX8000 conferencing systems with Release 8.03 or later
- 1 Polycom V500 video calling systems
- 1 Polycom RMX 2000 video bridge is supported. For more specific information on the RMX 2000 product, see: <http://www.polycom.com/usa/en/products/products.html>
- 1 Polycom MGC video conferencing bridge platforms with Release 8.0.1 are supported, but with some limitations. Release 7.5 of the MGC is not supported.
- 1 Third-party gatekeepers, including Polycom Path Navigator

You also need a system running Communication Manager Release 3.1.3 or later, and Avaya IP Softphone Release 5.2 with video integrator.

For more information, see *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Bellcore calling name ID

Allows the system to accept calling name information from a Local Exchange Carrier (LEC) network that supports the Bellcore calling name specification. The system can send calling name information in the format if Bellcore calling name ID is administered. The following caller ID protocols are supported.

- 1 Bellcore (default) - US protocol (Bellcore transmission protocol with 212 modem protocol)
- 1 V23-Bell - Bahrain protocol (Bellcore transmission protocol with V.23 modem protocol).

Bridged call appearance - multi-appearance telephone

Allows calls made to or from a primary telephone extension to be handled from more than one telephone. A bridged call appearance is set up by administering a primary extension and the button number associated with it on a multi-lamp button on another telephone. This feature is most often used by secretaries or assistants who answer or handle calls to the primary extension (an executive, for example).

When the primary extension receives a call, the bridged call appearance flashes or rings on all telephones administered with this feature. The call can be answered by anyone having a telephone with this feature and handled as if the primary extension user was answering it. The maximum number of bridged appearances is 64.

Bridged call appearance - single-line telephone

Allows single-line telephones users to have a bridged appearance on a multi-appearance telephone.

Call coverage

Call coverage provides automatic redirection of calls that meet specified criteria to alternate answering positions in a call coverage path. A coverage path can include any of the following:

- ┆ a telephone
- ┆ an attendant group
- ┆ a Uniform Call Distribution (UCD) hunt group
- ┆ a Direct Department Calling (DDC) hunt group
- ┆ an Automatic Call Distribution (ACD) hunt group
- ┆ a voice messaging system
- ┆ a Coverage Answer Group (CAG) established to answer redirected calls

Alphanumeric field designation

In addition to numeric designations for key system lists and groups of related information, the system administrator can specify alphanumeric designations, 0-15 characters in length, for the following:

- ┆ abbreviated dial lists
- ┆ abbreviated dial groups
- ┆ call pickup groups
- ┆ call routing patterns

Changeable coverage paths

Changeable coverage paths allows the end user to modify the coverage points by using a feature access code (FAC).

Directory

The directory feature allows users with display-equipped telephones to access the system database, use the touch-tone buttons to enter a name, and retrieve an extension number from the integrated directory. The directory contains the names and extensions assigned to all telephones on the system. The directory feature can also handle Russian names.

The integrated directory enables speed dial for both internal and external numbers while decreasing the number of dedicated buttons for speed dial. It also provides for a common directory across all endpoints. The integrated directory is linked to an external Lightweight Directory Access Protocol (LDAP) directory.

Enhanced coverage and ringback for logged off IP/PSA/TTI stations

A field on the **system-parameter customer-options** screen, called **Don't Answer Criteria For Logged Off IP/PSA/TTI Stations?**, allows a customer to choose how to handle non-registered stations. Possible entries for this field are **y** or **n**.

- ┆ If this field is set to **n**, call forwarding follows the busy criteria.
- ┆ If this field is set to **y**, call forwarding follows the don't answer criteria.

Time of day

This feature allows a user to have multiple coverage paths depending on the time of day, and day of the week.

Call redirection

Call forward busy/do not answer

Allows calls to be forwarded when the called extension is busy or when the call is not answered after an administrable interval. If the extension is busy, the call forwards immediately. If the extension is not busy, the incoming call rings the called extension, then forwards only if it remains unanswered longer than the administered interval.

Call forwarding all calls

Allows calls to be forwarded to an internal extension, external (off-net) number, an attendant, or an attendant group. You can include an access code or special characters, like pause characters, in the forwarding destination.

Call forwarding enhancements

Enhancements to the Call Forward feature give users the following capabilities:

- 1 Designate different preferred destinations for calls that originate from internal and external callers
- 1 Separate call forwarding/busy don't answer calls
- 1 Three different ways to forward incoming calls
 - Enhanced call forwarding unconditional (ECFU)
 - Enhanced call forward busy (ECFB)
 - Enhanced Feature no reply (ECFNR)

Chained call forwarding

This feature allows calls to be forwarded up to 10 hops (each calling station is considered to be one hop), the default value being 3 hops. Chained call forwarding allows mixed use of standard Call forwarding and Enhanced call forwarding. You can use the coverage path of the last forward-to station in the chain for coverage after forwarding.

Enhanced Redirection Notification

The activation of redirection features at a user's station is indicated through visual display or through a special dial tone (if the station is not equipped with a display). This feature works on DCP and IP (H.323) telephones, but not on SIP telephones and attendant consoles.

Call forwarding override

Allows the user at the forwarded-to extension to override call forwarding and either initiate a call or transfer a call back to the forwarded-from extension.

Send All Calls and Call Forwarding Override

The Send All Calls and Call Forwarding (SAC/CF) Override feature overrides active rerouting. This feature overrides these active rerouting settings:

- ┆ Send All Calls (SAC)
- ┆ Call Forwarding (CF) all
- ┆ Enhanced Call Forwarding (ECF) unconditional

The SAC/CF override feature depends on call initiation. On enabling SAC/CF override, the call may:

- ┆ Execute override - ring called station
- ┆ Cancel the override
- ┆ Display a message and wait for further input

Call redirection intervals

Avaya AuraTM Communication Manager allows the system administrator to specify the number of times that a call rings at each call coverage point before the call proceeds to the next coverage point.

Call Log enhancements

The Log Forwarded Call operation creates missed call log entries for calls that are redirected by Call Forward All, Send All Calls, or Goto Cover. You have the option to decide whether to log calls forwarded to another party on the forwarding telephone as missed calls or not. Call Forward, Enhanced Call Forward, Coverage and the interactions around these [Send All Calls (SAC) button, Goto Cover button, Do Not Disturb (DND)] are covered.

Call park

Allows you to put a call on hold and then retrieve a call from any other telephone on the system. This is helpful when you are on a call and need to go to another location for information. It also allows you to answer a call from any telephone after being paged by a telephone user or an attendant.

Call pickup

Along with directed call pickup, allows you to answer calls for other telephones within your specified call pickup group. Directed call pickup allows you to pick up any call on the system. With this feature, you do not have to leave your telephone to answer a call for a nearby telephone. You simply dial an access code or press a call pickup button.

Enhanced Call Pickup Alerting

Call Pickup Alerting provides display of calling and called party information for all members of the pickup group and administrable alerting options. This feature works on DCP and IP (H.323) telephones but not on SIP telephones.

Group call pickup

Allows you to dial a feature access code (FAC) and a pickup group number to answer a call from a different group. For example, marketing would be able to pickup calls in the sales group when the sales group is unavailable. This feature is ideal for offices that are not divided by partitions and generally have the departments on the same floor.

Caller ID on analog trunks

See [Caller ID on analog trunks](#) on page 143.

Caller ID on digital trunks

See [Caller ID on digital trunks](#) on page 143.

Circular station hunt group

See [Circular station hunt group](#) on page 62.

Conferencing

See [Conferencing](#) on page 73.

Consult

Allows a covering user, after answering a call received through call coverage, to call the called party for private consultation. Consult can be used to let a covering user ask the principal if they want to speak with the calling party.

Coverage callback

Allows a covering user to leave a message for the called party to call back the person who called.

Coverage incoming call identification

Allows multi-appearance telephones users without a display in a coverage answer group to identify an incoming call to that group.

Disconnecting unanswered calls

Disconnects unanswered outgoing calls after a predetermined amount of time. When any of the following timers expire during an outgoing local, toll, or international call attempt, the switch disconnects the call and applies busy tone, which may or may not be followed by howler tone:

- ┆ Pre-dialing and interdigit timer
- ┆ Outgoing seizure acknowledge timer
- ┆ Answer supervision timer
- ┆ 60-, 90-, and 120-second no-answer disconnect timers, based on ARS call type

- 1 120-second timer used for calls without a call type, such as calls to trunk access codes

Distinctive ringing

Rings or activates alerting on your telephone in such a way that you are aware of the type of incoming call before answering it. This feature operates in a Distributed Communications System (DCS) environment the same as it does within a single system. In Communication Manager, you can also administer distinctive ringing on a per-tenant basis if you use partitioning in your system.

By default, internal calls are identified by a 1-burst ringing pattern, external calls by a 2-burst ringing pattern, and priority calls by a 3-burst ringing pattern. You can administer these patterns.

Maintain external ring tone after internal transfer

When a call from outside the Avaya Aura™ Communication Manager system is transferred internally from one Avaya Aura™ Communication Manager station to another, ringing that indicates that the original call is from an external source is maintained. In other words, the transferred-to telephone rings to indicate an external call.

Edit dialing

Edit Dialing feature allows an end-user to pre-dial a number when the telephone is on-hook. During the pre-dial phase the user can edit the digits of a dialed number. The number is dialed when the user goes off-hook (lifts handset or presses the speaker button) or presses the send soft key. Edit Dialing is supported by Spice telephones, which are telephones from the 96xx Series with the protocol version H.323 (9620 Lite, 9620 Color, 9650 Color). To use this feature, the software version must be Spice 3.0 or later. SIP telephones are not supported by this feature.

Emergency calls from unnamed IP endpoints

With the Emergency calls from unnamed IP endpoints feature, an IP telephone can register without an extension number. The Emergency calls from unnamed IP endpoints feature places the IP telephone into Terminal Translation Initialization (TTI) service. Users can dial a feature

access code (FAC) to either associate an extension number with a telephone, or to dissociate an extension number from a telephone.

If Avaya AuraTM Communication Manager is appropriately administered, a user can use an IP telephone that is in TTI service to make emergency or other calls.

The Emergency Calls from Unnamed IP Endpoints feature requires IP telephone software R2.3 or later. IP telephone software R2.3 or later requires TN799C hardware vintage 3 or later circuit packs. TN799C hardware vintage 1 and 2 circuit packs do not work with IP telephone software R2.3. All versions of TN799DP circuit packs are compatible with IP telephone software R2.3. Therefore, the Emergency Calls from Unnamed IP Endpoints feature requires TN799DP or TN799C hardware vintage 3 or later circuit packs.

Enhanced abbreviated dialing

Supplements abbreviated dialing by providing one enhanced number per system. Enhanced number lists can contain any number or dial access code. System administrators designate privileges for group number lists, system number lists and enhanced number lists. With privileged lists, users can access otherwise restricted numbers (for example, telephones without long-distance access can be programmed to access specified long-distance numbers).

The Avaya 8XXX Server supports 20,000 entries within the enhanced abbreviated dialing system list. This second enhanced abbreviated dialing list doubles the capacity to from 10,000 entries to 20,000 entries.

Future increases to the enhanced abbreviated dialing list can be performed easily by increasing the number of lists. Increasing the number of lists increases the overall capacity by multiples of 10,000 entries.

Enhanced telephone display

The enhanced telephone display feature allows you to choose the character set that you want to see in Avaya AuraTM Communication Manager softkeys and display telephones. In addition to the standard Roman character set, you can choose either the Katakana or characters used for most European languages.

Enterprise Mobility User

Use the Enterprise Mobility User (EMU) feature to associate the features and permissions of the primary telephone of a user to a telephone of the same type anywhere within the customer enterprise. With EMU, the Class of Restriction (COR) and Class of Service (COS) permissions of the primary telephone are not associated with other telephones in the system.

Note:

Any telephone that is not the primary telephone is referred to as the visited telephone. Any server that is not the home server of the primary telephone is referred to as the visited server.

The following list outlines the requirements for the EMU feature:

- 1 QSIG must be the private networking protocol in the network of Communication Manager systems. This requirement also includes QSIG MWI.
- 1 Communication Manager software must be running on the home server and all visited servers.
- 1 All servers must be on a Linux platform. EMU is not supported on DEFINITY servers.
- 1 The visited telephone must be the same model type as the primary telephone to enable a optimal transfer of the image of the primary telephone. If the visited telephone is not the same model type, only the call appearance (**call-appr**) buttons and the message waiting light are transferred.
- 1 All endpoints must be self-designating terminals.
- 1 Uniform Dial Plan (UDP).

Calls made from a visited telephone can be processed by either the home server or the visited server. Which server processes the call depends on how the user originates the call. The home server processes any calls that are a result of a user depressing one of the buttons that were downloaded to the visited telephone. The visited server processes any calls that are placed on the visited telephone using the dial pad.

Enterprise Mobility User enhancements

Enhancements are made to the Enterprise Mobility User (EMU) feature for release 4.0:

- 1 Enable EMU while mobile within a single Avaya AuraTM Communication Manager server domain.
- 1 Permit visited station's principal user to use Extension to Cellular OPTIM application during a registered EMU period at that station.

You can administer the amount of time that must elapse before a visitor can log in as EMU after making emergency calls from an EMU-activated station.

Enterprise Wide Licensing

Enterprise Wide Licensing (EWL) is a technology within Avaya Aura™ Communication Manager release 3.0 and a Avaya Aura™ Communication Manager license file. EWL is used to partially support a developing offer known as Enhanced Software License Program (ESLP). ESLP gives customers the ability to bulk purchase and then share license capacities across multiple locations.

Note:

Launch of the ESLP offer will be announced at a later date.

Go to cover

Allows users who call another internal extension to send the call directly to coverage.

Hold

Allows you to disconnect from a call temporarily, use your telephone for other call purposes, and then return to the original call.

Intercom - automatic answer

Automatic answer intercom calls (auto answer ICOM) allows a user to answer an intercom call within the intercom group without pressing the intercom button. Auto answer ICOM works with digital, BRI, and hybrid telephones with built-in speaker, headphones, or adjunct speakerphone.

Internal automatic answer

Allows specific telephones to answer incoming internal calls automatically. This feature is intended for use with telephones that have speakerphones or headsets. You simply press an internal automatic answer feature button, and calls are automatically answered when the

telephone is idle. Internal and Distributed Communications System (DCS) calls can be answered using automatic answer, but only attendants can use automatic answer to answer external calls directed to the attendant.

Last number dialed

Allows you to automatically redial the last number dialed. The system saves the first 24-digits of the last number dialed, whether the call attempt was manually dialed or dialed using abbreviated dialing. When you press the last number dialed button or dial the last number dialed feature access code, the system places the call again.

Local call timer automatic start/stop

Automatically starts the local timer of a 6400-series telephone when a call is received. The timer is stopped automatically when a call is ended. When a call is placed on hold the timer continues to run, but is not displayed. When the call comes off hold, the total elapsed call-time displays.

Long hold recall

Visual and audible warnings are sent to the telephone where a call has been on hold past a specified period of time. Both visual and audible warnings are used if the telephone is on-hook. If the telephone is off-hook, a "priority ring" is used. This is an optional feature at the system level.

Manual originating line service

Connects single-line telephone users to the attendant automatically when the user lifts the handset. The attendant number is stored in an abbreviated dialing list. When the telephone user lifts the handset, the system automatically routes the call to the attendant using the hot line service feature.

Misoperation handling

Defines how calls are handled when a misoperation occurs. A misoperation is when calls are left on hold when the controlling station goes on hook.

For example, a misoperation can occur under either of the following conditions:

- 1 If you hang up prior to completing a feature operation (in some cases, hanging up completes the operation, as in call transfer). If, for example, you place a call on hold, begin to transfer the call, dial an invalid extension number, and then hang up, that is a misoperation.
- 1 When the system enters night service while attendant consoles have calls on hold.

The system administrator can alter the standard misoperation handling to ensure that an external caller is not left on hold indefinitely, or dropped by the system after a misoperation with no way to reach someone for help.

Note:

This feature is required only in France and Italy, but it can be used at any location where the feature has been turned on.

Multiappearance preselection and preference

Provides options for placing or answering calls on selected call appearances.

- 1 Ringing appearance *preference* automatically connects you to the incoming ringing call when the user picks up the handset.
- 1 *Idle appearance preference* automatically connects you to an idle appearance.
- 1 *Preselection* allows the user to manually select an appearance. Preselection is used, for example, when you want to reconnect with a held call or activate a feature.

Preselection can be used with a feature button. For example, if you press an abbreviated dialing button, the call appearance is automatically selected and, if you pick up the handset within five seconds, the call is automatically placed. The preselection option overrides both of the other preference options.

Multiple level precedence and preemption

Multiple level precedence and preemption (MLPP) is an optional group of features that provide users the ability to interface to and operate in a Defense Switched Network (DSN). The DSN is a highly secure and standards-based communication system of the US Government Department of Defense (DoD).

**CAUTION:**

MLPP is currently designed to meet only DoD GSCR requirements for connection to a DSN by federal, state, or local government agencies. As such, MLPP is not currently designed for use in commercial enterprise environments. Activation of this feature in any other kind of network environment could result in unexpected and unwanted feature operations.

The MLPP features allow users to request priority processing of their calls during critical situations. The MLPP features include:

- | [Announcements for precedence calling](#)
- | [Dual homing](#)
- | [End office access line hunting](#)
- | [Line load control](#)
- | [Precedence call waiting](#)
- | [Precedence calling](#)
- | [Precedence routing](#)
- | [Preemption](#)
- | [Worldwide numbering and dialing plan](#)

Announcements for precedence calling

In certain situations, precedence calls are blocked because of unavailable resources or improper use. When this occurs, recorded announcements are used to identify what went wrong. The announcements used for MLPP include:

- | Blocked precedence call
- | Unauthorized precedence level attempted
- | Service interruption prevented call completion
- | Busy, not equipped for preemption or precedence call waiting
- | Vacant code

Dual homing

Dual homing allows a user to dial a telephone number and, if the initial route is unavailable, have the call route to its destination over alternate facilities.

End office access line hunting

End office access line hunting automatically hunts for an idle trunk over end office access lines, based on the precedence level of the call.

Line load control

Line load control is a feature that restricts a predefined set of station users from originating calls during a crisis or emergency. Through administration, users are assigned to a line load control level based on their relative importance. When an emergency occurs, the administrator manually enables the feature to restrict calling by users of lower importance. When the emergency is over, the administrator manually disables the feature.

For example, if a situation occurs that threatens national defense, station users in the defense department will not be restricted from originating calls, but stations in other departments, such as the accounting department, will be restricted. When the crisis is over, the system can be returned to normal operation by the administrator.

Precedence call waiting

After a precedence call is routed, the called party may already be busy on another call. Precedence call waiting allows the caller to “camp on” to the line of the called party and wait for the user to answer the call. The caller hears a special ringback tone and the called party hears a call waiting tone.

Depending on the type of telephone being used, the called party can put the current call on hold and answer the call, or the called party must hang up on their current call to answer the incoming call.

Precedence calling

Precedence calling is the centerpiece of the MLPP features. Precedence calling allows users, on a call-by-call basis, to select a level of priority for each call based on their need and

importance (rank). The call receives higher-priority routing, whether the call is local or going around the world.

Users may access five levels of precedence when placing calls:

- 1 Flash Override (the highest precedence level)
- 1 Flash
- 1 Immediate
- 1 Priority
- 1 Routine (the default, and lowest precedence level)

Each station user is administered with a maximum precedence level. The more important or higher in rank of the user, the higher the precedence level. Users cannot originate calls at precedence levels higher than their maximum administered level. Non-MLPP calls are treated as routine level precedence calls.

Precedence routing

When precedence calls are destined for other switches in a private network, the precedence routing feature is used to route the calls. The precedence routing feature routes calls based on three main criteria:

- 1 Routing based on the destination number
- 1 Routing based on the precedence level
- 1 Routing based on the time of day

These routing criteria are administrable and can be changed as required. Two related features are dual homing and end office access line hunting.

Preemption

Preemption works with the precedence routing feature to further extend the call routing capabilities of the MLPP features. Preemption, when allowed through administration, can actually tear down an existing lower priority call in order to complete a more important precedence call. Even non-MLPP calls are treated as routine level precedence calls and can be preempted.

When this occurs, the callers on the existing call hear a tone indicating that the call is about to be preempted. The callers have three seconds to end the call before the call is automatically disconnected. After the existing call is disconnected, the new call is placed using preempted facility.

Worldwide numbering and dialing plan

The worldwide numbering and dialing plan (WNDP) feature allows Avaya Aura™ Communication Manager to conform to the standard numbering system established by the Defense Communications Agency (DCA). WNDP defines its own format for the precedence dialing. The capability to operate with this numbering plan must be incorporated into all new switches introduced into the Defense Switched Network (DSN).

Night service

There are five night service features:

- 1 Hunt group night service allows an attendant or a split supervisor to assign a hunt group or split to night service mode. All calls for the hunt group then are redirected to the hunt group designated night service extension. When a user activates hunt group night service, the associated button lamp lights.
- 1 Night console service directs all calls for primary and daytime attendant consoles to a night console. When a user activates night console service, the night service button for each attendant lights and all attendant-seeking calls (and calls waiting) in the queue are directed to the night console. To activate and deactivate this feature, the attendant typically presses the night button on the principal attendant console or designated console.
- 1 Night station service directs incoming calls for the attendant to designated extensions. Attendants can activate night station service by pressing the night button on the principle console if there is not an active night console. If the night station is busy, calls (including emergency attendant calls) receive a busy tone. They do not queue for the attendant.
- 1 Trunk answer from any station allows telephone users to answer all incoming calls to the attendant when the attendant is not on duty and when other telephones have not been designated to answer the calls. The incoming call activates a gong, bell, or chime and a voice-terminal user dials an access code to answer the call.
- 1 Trunk group night service allows an attendant or a designated telephone user to individually assign a trunk group or all trunk groups to the night service mode. Specific trunk groups individually assigned to the service are in Individual trunk night service mode. Calls coming into these trunk groups are redirected to designated night service extensions. Incoming calls on other trunk groups are processed normally.

Enhanced night service

Avaya Aura™ Communication Manager informs a voice mail system (VMS) that it is in night service, allowing the VMS to perform different actions and call handling for out-of-hours

operation. For example, the VMS may be administered to provide recorded announcements after hours. The enhancement is made to the mode code voice mail interface.

License modes

The three modes of license operation for your system are:

- 1 [License-normal mode](#)
- 1 [License-error mode](#)
- 1 [No-license mode](#)

License-normal mode

The license-normal mode is the desired mode of operation of a stable system. During this mode of operation, a license is properly installed, the license contains a serial number that matches the processors, the license is not expired, and feature usage does not exceed limits.

License-error mode

The license-error mode is a warning mode. During this mode, call processing is supported, the system declares a major alarm, and a 6-day countdown timer is running. If this timer is allowed to expire, the no-license mode is invoked.

The license-error mode is entered as a result of one of the following conditions:

- 1 The serial number of the active processor does not match the license file.
- 1 The standby processor cannot be contacted or the serial number of the standby processor does not match the serial numbers in the license.
- 1 The license has expired.
- 1 Feature usage exceeds limits. For example, there are more ports translated than permitted by the port limit in the license.
- 1 A WAN spare or survivable remote processor enters License-Error mode when it is providing primary service.
- 1 A switch has initialized after a software upgrade and a new license has not yet been installed.

The license-error mode is cleared by correcting the error that caused the system to enter into license-error mode, or by installing a valid license that is consistent with the configuration of the switch.

Limit the number of concurrent calls

A typical Avaya AuraTM Communication Manager digital or IP station has three call appearances.

- ┆ The first two call appearances are for receiving incoming calls.
- ┆ The last call appearance is reserved for call origination or receiving priority calls if the first two call appearances are active.

When the Limit the Number of Concurrent Calls (LNCC) configuration is administered, the LNCC feature allows the station user to limit the number of concurrent calls to one call.

LNCC uses a feature access code or a programmed button. A visual display or audio feedback is provided that indicates if LNCC is active.

A call to a station that is LNCC-busy is treated like a call to a normal busy station. The call follows the call coverage path for status busy if administered or hunts to the hunt-to station if administered.

No-license mode

The no-license mode is a state in which all new call originations, except alarm calls and calls to an administered emergency number, are denied. All incoming calls, except calls to an administered number, are also denied.

The no-license mode state is entered as the result of one of the following reasons:

- ┆ No license is installed in the system.
- ┆ The License-Error timer has expired.
- ┆ A survivable remote processor detects a port board in its port network other than an Expansion Interface board.
- ┆ A reset system 3 preserve-license command is executed and the offer category in translation does not match the offer category in the license.

Starting with Avaya AuraTM Communication Manager release 2.1, no-license mode not only protects customers from loss of call processing, but also provides software copy protection. The result of no-license mode is an error message on telephone displays, and blocked system administration.

No-license mode is cleared by correcting the error that caused the system to enter into no-license mode, or by installing a valid license that is consistent with the configuration of the system.

Personalized ringing

Allows users of certain telephones to uniquely identify their own calls. Each user can choose one of a number of possible ringing patterns. The eight ringing patterns are tone sequences consisting of different combinations of three tones. With this feature, users working closely in the same area can each specify a different ringing pattern in order to better identify their own calls.

Posted messages

In most situations, after a few rings when no one answers a call, the calling party usually hears an announcement saying that the called party is not available and to please leave a message. At this point, the calling party has no clue when the called party would return the call.

The posted messages feature provides Avaya Aura™ Communication Manager users with the capability of indicating the reason of their unavailability to calling parties. The system provides 30 messages for a user to choose from, such as “on vacation,” or “at lunch.” Of the 30 messages, 15 messages are fixed system messages, and the remaining 15 messages are administrable (custom messages). After a user has chosen one of the messages and thus activated the feature, the message is immediately sent to calling parties who have terminal displays.

The system provides two ways to activate/deactivate this feature: using button pushes and feature access codes. The system allows users to use the feature access codes from their own display telephone, from another station/attendant, or from a remote access trunk.

Priority calling

Allows you to ring another telephone with a distinctive signal that tells the called party the incoming call requires immediate attention. The called party can then handle the call accordingly. You activate priority calling by dialing a priority calling access code or pressing a feature button, followed by the extension number. You can use priority calling only if your telephone has been administered with the required class of service.

Pull transfer

Allows *either* the party who was originally called, *or* the party to whom the held call will be transferred, to complete the transfer. This is a convenient way to connect a party with someone better qualified to handle the call. Attendant assistance is not required and the call does not have to be redialed. It interfaces with satellite workstations through TGU/TGE trunks and is always available for calls that use TGU/TGE trunks.

Recall signaling

Recall signaling allows the user of an analog station to place a call on hold, use the telephone for other call purposes, and then return to the original call.

Recorded telephone dictation access

Allows telephone users, including remote access and incoming tie trunk users, to access dictation equipment. The dictation equipment is accessed by dialing an access code or extension number. The start/stop function can be voice or dial controlled. Other functions such as initial activation and playback are controlled by additional dial codes.

Reset shift call

If a called number is busy and does not have coverage, or the called number and the coverage are both busy, you have an opportunity to replace the last digit that was entered. This allows you to call another extension without having to hang up and redial. Reset shift call is a feature that is active for station to station (internal) calls and for private network calls. The private network trunks must signal busy using out-of-band signaling.

Ringback queuing

Places calls in an ordered queue (first in, first out) when all trunks are busy. The telephone user who is trying to make a call is automatically called back when a trunk becomes available, and hears a distinctive three-burst signal when called back.

Ringer cutoff

Allows the user of a multi-appearance telephone to turn audible ringing signals on and off. Visual alerting is not affected by this feature. When this feature is enabled, only priority (three-burst) ring, redirect notification, intercom ring, and manual signaling ring at the telephone. Internal and external calls do not ring.

Ringing - abbreviated and delayed

Allows you to manually or automatically assign one of four ring types to each call appearance on a telephone. Whatever treatment you assign to a call appearance is automatically assigned to each of its bridged call appearances.

Ringing options

Provides multi-appearance telephone users with different ringing patterns. This feature primarily affects audible ringing for calls directed to telephones that are off hook, or calls directed to idle and active CALLMASTER telephones.

Send all calls

Allows users to temporarily direct all incoming calls to coverage regardless of the assigned call-coverage redirection criteria. Covering users can temporarily remove their telephones from the coverage path. The feature is activated and deactivated via a button or access code.

Special dial tone

Provides the ability to play a special dial tone whenever an analog set is not able to receive calls. When such conditions as call forward all calls, call forward busy/no answer, send all calls, or do not disturb are activated on a telephone set, a special dial tone lets you know that you cannot receive any calls.

Station hunting

Routes calls made to a busy extension to another extension. To use station hunting, you create a station hunting chain that governs the order in which a call routes from one extension to the next when the called extension is busy. Each extension in the chain links *to* only one subsequent extension. However, an extension may be linked *from* any number of extensions.

Station hunt before coverage

This feature changes the interaction that occurs between station hunting and call coverage. Station hunt before coverage causes a call going to a busy station to go through a station hunting process before going to coverage. If all the stations in the hunt group are busy, the call will go to the coverage path.

Station self display

Station self display shows the extension number of the telephone set when a user either dials the feature access code while off-hook, or depresses the **INSPECT** button when on-hook. The dialed number will be displayed once the user starts to dial. This feature is helpful to people who move from one desk to another while they are working. This feature is also used by maintenance personnel to ensure that an extension number is correctly administered.

Station used as a virtual extension

Allows a customer to assign multiple, individual, virtual extensions to one physical telephone. The physical telephone must be analog and on the local switch. The administrator can set each virtual extension with a unique ring pattern to identify the extension for which the incoming call is intended. For example, an administrator could assign three virtual extensions, each with a unique ring pattern, to a single telephone shared by three roommates in a college dormitory. This feature affects incoming calls only; all outgoing calls are associated with the physical extension.

Support for the Hewlett Packard DL380G2 server

Avaya Aura™ Communication Manager is supported on Hewlett Packard (HP) DL380G2 servers in an S87XX IP-PNC system configuration (an S87XX Server with a G600 Media Gateway).

Team button

The Team Button feature monitors members of a team of stations. A team is a virtual set of stations. Members of a team can be any station type with multiple call appearance displays and administrable feature buttons. Analog stations, BRI stations, SIP telephones, X-ports, and X-mobiles are allowed as valid monitored stations, but not as monitoring stations. Attendant consoles are not allowed as monitoring stations or monitored stations. The assignment of a Team Button on a station brings it automatically into the virtual team.

The team button, using its speed dial function, can override a rerouting caused by active Send All Calls (SAC), Call Forwarding (CFWD) all, or Enhanced Call Forward (ECF) unconditional.

When the team button is pressed on the monitoring station and the monitored station has a direct rerouting active (SAC, CFWD all, ECF unconditional), the call may do any of the following, depending upon administration:

- 1 Be rerouted
- 1 Ring the monitored station
- 1 Display a message asking the caller whether to ring the monitored station or reroute the call

The number of team buttons per station is 31. However, the maximum number stations that can monitor any one station is 15. Certain enhancements are made to team button display and

execution functions. For more information, see *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Telephone display

Provides multi-appearance telephone users with updated call and message information. This information is displayed on a display-equipped telephone. The information displayed depends upon the display mode selected by the user. Information that allows personalized call answering is available on many calls.

Users may select any of the following as the display message language: English (default), French, Italian, or Spanish. In addition, messages can be administered on the system in a fifth language. The language for display messages is selected by each user.

ISO 8859-1 encoding compatibility

ISO 8859-1 encoding compatibility enables Avaya Aura™ Communication Manager to support correct display of names in languages that use the Latin1 set of symbols (also referred to as extended ASCII). Latin1 covers most West European languages, including:

- ┆ French (fr)
- ┆ Spanish (es)
- ┆ Catalan (ca)
- ┆ Basque (eu)
- ┆ Portuguese (pt)
- ┆ Italian (it)
- ┆ Albanian (sq)
- ┆ Rhaeto-Romanic (rm)
- ┆ Dutch (nl)
- ┆ German (de)
- ┆ Danish (da)
- ┆ Swedish (sv)
- ┆ Norwegian (no)
- ┆ Finnish (fi)
- ┆ Faroese (fo)
- ┆ Icelandic (is)

- | Irish (ga)
- | Scottish (gd)
- | English (en)

Telephone self administration

The telephone self administration capability allows you to program feature buttons on the telephone yourself.

Temporary bridged appearance

Allows multi-appearance telephone users in a terminating extension group or personal central office line group to bridge onto an existing group call. If a call has been answered using the call pickup feature, the originally called party can bridge onto the call. This feature also allows a called party to bridge onto a call that redirects to coverage before the called party can answer it.

Terminating extension group

Allows an incoming call to ring (either audible or silent alerting) as many as four telephones at the same time. Any user in the group can answer the call. Any telephone can be administered as a group member. Only a multi-appearance telephone can be assigned a feature button with an associated status lamp, however.

The feature button allows the user to select a terminating extension group call appearance for answering or bridging onto an existing call but not for call origination. For example, a department in a large store might have three telephones. Anyone in the department can answer the call. The salesperson most qualified to answer the call can bridge onto the call.

Any telephone can be assigned as a TEG member; however, only a multi-appearance telephone can be assigned a TEG button with associated status lamp. The TEG button allows the telephone user to select a TEG call appearance for answering or for bridging onto an existing call. The TEG members are assigned on an extension number basis. Call reception restrictions applicable to the group are specified by the group class of restriction (COR). The group COR takes precedence over an individual member's COR. When a Terminating Extension Group (TEG) receives an incoming call, TEG's primary Class of Restrictions (COR) should be considered for the calling/called restrictions. The members could all be termination

restricted but still receive calls if the group is not restricted. For the Terminating Extension Group screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Time of day routing

Provides the most economical routing of **ARS** and **AAR** calls. This routing is based on the time of day and day of the week that each call is made. Up to eight TOD routing plans may be administered, each scheduled to change up to six times a day for each day in the week.

This allows you to take advantage of lower calling rates during specific times of the day and week. In addition, companies with locations in different time zones can use different locations that have lower rates at different times of the day or week. This feature is also used to change patterns during the times an office is closed in order to reduce or eliminate unauthorized calls.

Timed call disconnection for outgoing trunk calls

This feature provides the capability to automatically disconnect an outgoing trunk call after an administrable amount of time. Warning tones are applied to all parties on the call prior to the disconnection.

The amount of time that can elapse before the trunk is dropped can be specified, and can vary between 2-999 minutes. If the timer field is blank, which is the default value, then the feature is disabled and the trunk will not be automatically disconnected.

Timed call disconnection applies to all outgoing trunk calls initiated by a party belonging to a specified Class of Restriction (COR).

Prior to disconnecting the trunk, warning tones are applied to all parties on the call. The first warning tone occurs when one minute is remaining on the call. The second warning tone occurs when 30 seconds are remaining on the call.

Transfer

Allows telephone users to transfer trunk or internal calls to other telephones within the system without attendant assistance. This feature provides a convenient way to connect a party with someone better qualified to handle the call.

Abort transfer

Allows a user to abort a transfer attempt by pressing a non-idle line appearance. The call being transferred would be taken off a transfer-type hold and be put on a traditional hold. The transfer will also be aborted when you hang up (going on-hook), unless transfer upon hang-up is activated on the switch. This is an optional feature at the system level.

Transfer - outgoing trunk to outgoing trunk

Allows a user or attendant to initiate two or more outgoing trunk calls and then transfer the trunks together. The transfer operation removes the original user from the connection and conferences the outgoing trunks. Alternatively, the controlling party can establish a conference call with the outgoing trunks and then drop out of the conference, leaving only the outgoing trunks on the conference. This is an optional enhancement to trunk-to-trunk transfer and requires careful administration and use. DCS trunk turnaround may be a safer alternative to this feature.

Transfer recall

Returns the unanswered transfer calls back to the person who transferred the call. Transfer recall uses a priority alerting signal, and the display on the telephone shows “rt”, which indicates a returned call from a failed transfer operation.

Transfer upon hang-up

Provides you with the ability to transfer a call by hanging up instead of having to press the transfer button a second time. You would press the transfer button, dial the number the call is being transferred to and then hang up. This is an optional feature at the system level. You will still be able to transfer a call by pressing the transfer button a second time.

Trunk-to-trunk transfer

Allows the attendant or telephone user to connect an incoming trunk call to an outgoing trunk call. This feature is particularly useful when a caller outside the system calls a user or attendant and requests a transfer to another outside number. For example, a worker, away on business, can call in and have the call transferred elsewhere. The system assures that incoming central office (CO) trunks without disconnect supervision are not transferred to outgoing trunks or other incoming central office trunks without disconnect supervision.

Trunk flash

Trunk flash allows a feature or function button on a multifunction telephone or attendant console to be assigned as a flash button. Pressing this button while connected to a trunk (which must have been administered to allow trunk flash) causes the system to send a flash signal out over the connected trunk.

Trunk flash enables multifunction telephones to access central office customized services that are provided by the central office to which the system running Avaya Aura™ Communication Manager is connected. **These** services are electronic features, such as conference and transfer, that are accessed by a sequence of flash signal and dial signals from the system station on an active trunk call.

The trunk flash feature can help to reduce the number of trunk lines connected to the system. “Digit 1 as flash” as used in Italy, and the United Kingdom will not serve as the flash button in this application.

Index

Numerical

| | |
|-------------------------------|---------------------|
| 2B-channel transfer | 67 |
| 800-service trunks | 144 |
| 802.1p/Q | 154 |

A

| | |
|-------------------------------------------------------------------------------------|---------------------|
| AAA, <i>see</i> Authentication, Authorization, and Accounting Services (AAA) | |
| AAR, <i>see</i> Automatic Alternate Routing (AAR) | |
| AAR/ARS, <i>see</i> Automatic Alternate Routing/Automatic Route Selection (AAR/ARS) | |
| AAS, <i>see</i> Auto-Available Split (AAS) | |
| abandoned call | 51 |
| abandoned call search | 51 |
| Abbreviated Dialing (AD) | 235 |
| labeling | 235 |
| on-hook programming. | 235 |
| ABCD tone support | 236 |
| abort conference on hangup | 73 |
| abort transfer | 265 |
| ACB, <i>see</i> Automatic Call Back (ACB) | |
| access security gateway (ASG). | 197 |
| accessing the attendant | 37 |
| ACD, <i>see</i> Automatic Call Distribution (ACD) | |
| active dialing | 236 |
| ACTR, <i>see</i> Automatic Customer Telephone Rearrangement (ACTR) | |
| ACW, <i>see</i> After Call Work (ACW) | |
| AD, <i>see</i> Abbreviated Dialing (AD) | |
| add/remove skills | 64 |
| adjunct route support for network call redirection | 47 |
| adjunct routing. | 52 |
| Adjunct Switch Application Interface (ASAI) | 34 |
| adjunct route support for network call redirection | 47 |
| co-resident DEFININTY LAN Gateway (DLG) | 48 |
| Direct Agent Announcement (DAA) | 48 |
| flexible billing. | 48 |
| pending work mode change | 49 |
| trunk group identification | 49 |
| User-to-User Information (UUI) | 49 |
| administered connections | 175 |
| administrable language displays | 95 |
| administrable loss plan | 95 |
| administrable time-out on call timer | 236 |
| administration | |
| automatic routing | 181 |
| call management | 54 |
| change notification | 213 |
| duplicate agent login ID | 64 |
| agent-loginID skill pair increase. | 64 |

| | |
|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| monitoring calls | 44 |
| property management | 92 |
| site | 216 |
| Administration Without Hardware (AWOH) 113 , 117 , 119 , 213 | |
| admission control. | 157 |
| Advanced Encryption Standard (AES) | 159 , 200 |
| encryption algorithm for bearer channels | 200 |
| Advanced Private Line Termination (APLT). | 132 |
| advanced vector routing. | 59 |
| Advice of Charge (AOC) | 218 |
| AE Services, <i>see</i> Application Enablement Services (AE Services) | |
| AEA, <i>see</i> Avaya Encryption Algorithm (AEA) | |
| AES, <i>see</i> Advanced Encryption Standard (AES) | |
| After Call Work (ACW) | 62 |
| ALI, <i>see</i> Automatic Location Information (ALI) | |
| alphanumeric dialing | 89 , 236 |
| alternate facility restriction levels | 181 , 198 , 213 |
| alternate gatekeeper and registration addresses | 150 |
| alternate operations support system alarm | 198 |
| analog | |
| CAMA - E911 trunk group | 209 |
| TTY over analog trunks | 162 |
| ANI, <i>see</i> Automatic Number Identification (ANI) | |
| announcements | 214 |
| increased support | 216 |
| multiple music sources. | 229 |
| Voice Announcement over LAN (VAL) Manager | 216 |
| announcements for precedence calling | 251 |
| answer detection | 185 |
| answer supervision by time-out | 185 |
| AOC, <i>see</i> Advice of Charge (AOC) | |
| API, <i>see</i> Application Programming Interface (API) | |
| APLT, <i>see</i> Advanced Private Line Termination (APLT) | |
| Application Enablement Services (AE Services) | 31 |
| bundled server option | 32 |
| software-only option | 31 |
| Application Programming Interface (API). | 31 |
| Adjunct Switch Application Interface (ASAI) | 34 |
| device and media control API | 33 |
| JTAPI | 34 |
| TSAPI | 34 |
| Application Server Interface (ASI) | 78 , 177 |
| approximate charge for calls | 218 |
| ARS, <i>see</i> Automatic Route Selection (ARS) | |
| ASA, <i>see</i> Average Speed of Answer (ASA) routing | |
| ASAI, <i>see</i> Adjunct Switch Application Interface (ASAI) | |
| ASCA, <i>see</i> Avaya Software Compatibility Audit (ASCA) tool | |
| ASCII character set. | 92 |
| ASI, <i>see</i> Application Server Interface (ASI) | |

Index

- asynchronous links. [176](#), [228](#)
- Asynchronous Transfer Mode (ATM) [121](#), [127](#)
 - Circuit Emulation Service (ATM-CES) [127](#)
 - Port Network Connectivity (ATM-PNC) [121](#)
 - over WAN. [121](#)
- ATM-CES, *see* Asynchronous Transfer Mode (ATM), Circuit Emulation Service (ATM-CES)
- ATM-PNC, *see* Asynchronous Transfer Mode (ATM), Port Network Connectivity (PNC)
- attendant
 - auto manual splitting [44](#)
 - auto start. [44](#)
 - automated [40](#)
 - backup. [38](#)
 - backup alerting [40](#)
 - call handling [39](#)
 - call waiting [40](#)
 - calling of inward restricted stations. [40](#)
 - conferencing [41](#)
 - control of trunk group access [44](#)
 - crisis alert [45](#)
 - dial access to. [37](#)
 - direct extension selection [45](#)
 - display of Class of Restriction (COR). [167](#)
 - do not split [44](#)
 - functions using Distributed Communications System (DCS) protocol [38](#), [147](#)
 - control of trunk group access. [38](#)
 - direct trunk group selection. [39](#), [45](#), [147](#)
 - display [43](#), [147](#)
 - inter-PBX attendant calls. [39](#)
 - increased consoles [43](#)
 - individual access to [37](#)
 - intrusion [39](#)
 - listed directory number [41](#)
 - lockout - privacy [39](#)
 - override of diversion features [41](#)
 - position report [225](#)
 - priority queue. [42](#)
 - QSIG Centralized Attendant Service (CAS). [167](#)
 - recall. [37](#)
 - release loop operation [42](#)
 - return call [167](#)
 - room status [38](#), [89](#)
 - serial calling [42](#)
 - split swap [39](#)
 - timed reminder [42](#)
 - trunk group busy/warning indicators [46](#)
 - trunk identification [46](#)
 - vectoring [40](#)
 - Visually Impaired Attendant Service (VIAS). [46](#)
- audible message waiting [107](#)
- AUDIX
 - record on messaging [106](#)
- Authentication, Authorization, and Accounting Services (AAA) [197](#)
- authorization codes - 13 digits [198](#), [214](#)
- auto answer ICOM [248](#)
- auto callback - QSIG call completion. [164](#)
- auto fallback to primary for H.248 gateways [187](#)
- auto manual splitting [44](#)
- auto reserve agents [55](#)
- auto start. [44](#)
- Auto-Available Split (AAS) [52](#)
- auto-in work mode [52](#)
- automated attendant [40](#)
- automatic alternate conditional routing [148](#)
- Automatic Alternate Routing (AAR) [181](#)
- Automatic Alternate Routing/Automatic Route Selection (AAR/ARS) [78](#)
 - dialing without FAC [182](#)
 - overlap sending [182](#)
 - partitioning [182](#), [183](#)
- automatic answer
 - intercom [248](#)
 - internal [248](#)
- Automatic Call Back (ACB) [237](#)
 - for analog telephones [237](#)
- Automatic Call Distribution (ACD) [50](#), [52](#), [57](#), [239](#)
- automatic circuit assurance [147](#), [214](#), [222](#)
- Automatic Customer Telephone Rearrangement (ACTR) [113](#)
- automatic hold [237](#)
- Automatic Location Information (ALI). [116](#), [117](#)
- Automatic Number Identification (ANI) [49](#), [52](#)
 - Incoming Automatic Number Identification [52](#)
 - Outgoing Automatic Number Identification [53](#)
- Automatic Route Selection (ARS) [182](#)
- automatic routing features. [181](#)
- automatic selection of Direct Inward Dialing (DID) numbers [89](#)
- automatic transmission measurement system [214](#)
- automatic wakeup [89](#)
- auxiliary trunks [132](#)
- Avaya business advocate [55](#)
 - enhancements
 - auto reserve agents [55](#)
 - call selection override per skill. [55](#)
 - dynamic percentage adjustment. [55](#)
 - dynamic queue position. [55](#)
 - dynamic threshold adjustment. [55](#)
 - Least Occupied Agent (LOA) [65](#)
 - logged-in advocate agent counting [55](#)
 - percent allocation distribution [56](#)
 - reserve agent time in queue activation. [56](#)
 - VuStats. [71](#)
- Avaya call center
 - basic [56](#)
 - deluxe [56](#)
 - elite [56](#)
 - features supported on the Avaya G700 Media Gateway [56](#)
- Avaya Call Management System (CMS) [57](#), [231](#)

- dual links to CMS [63](#)
- measurement of ATM [63](#), [127](#)
- site statistics for remote port networks [70](#)
- Avaya computer telephony [47](#)
- Avaya Directory Enabled Management (DEM) [215](#)
- Avaya Encryption Algorithm (AEA) [159](#), [200](#)
- Avaya Extension to Cellular [114](#)
- off-PBX station (OPS) [115](#)
- Avaya Installation Wizard [26](#)
- Avaya Integrated Management [215](#), [216](#)
- Avaya IP agent [83](#)
- Avaya IP Softphone [83](#)
- for pocket PC [84](#)
- Avaya one-X Communicator [85](#)
- Avaya one-X Portal as software-only phone [85](#)
- Avaya SIP softphone [86](#)
- Avaya site administration [216](#)
- Avaya SoftConsole [86](#)
- RoadWarrior mode [86](#)
- Telecommuter mode [87](#)
- Avaya Software Compatibility Audit (ASCA) tool [225](#)
- Avaya video telephony solution [237](#)
- Avaya virtual routing [57](#)
- Avaya VoIP Monitoring Manager (VMON) [147](#), [217](#)
- Avaya Wireless Telephone Solutions (AWTS) [114](#)
- Average Speed of Answer (ASA) routing [59](#)
- AWOH, *see* Administration Without Hardware (AWOH)
- AWTS, *see* Avaya Wireless Telephone Solutions (AWTS)

B

- backup alerting [40](#), [207](#)
- barrier codes [207](#), [217](#)
- Basic Call Management System (BCMS) [54](#)
- reports [54](#)
- Basic Rate Interface (BRI) [135](#)
- BCD, *see* Binary Coded Decimal (BCD)
- BCMS, *see* Basic Call Management System (BCMS)
- Bellcore calling name ID [95](#), [143](#), [238](#)
- Best Service Routing (BSR) [59](#)
- polling over IP without B channel [59](#)
- Binary Coded Decimal (BCD) [92](#)
- block CMS Move Agent events [49](#)
- block collect call [96](#), [199](#)
- blockage study report [225](#)
- BRI, *see* Basic Rate Interface (BRI)
- bridged call appearance
 - multi-appearance telephone [238](#)
 - single-line telephone [239](#)
- BSR, *see* Best Service Routing (BSR)
- bulletin board [104](#), [217](#)
- busy tone disconnect [96](#)
- busy verification of telephones and trunks [218](#)

C

- CAC, *see* Call Admission Control (CAC)

- CAG, *see* Coverage Answer Group (CAG)
- Cajun rules [155](#)
- call accounting
 - Xiox [93](#)
- Call Admission Control (CAC) bandwidth management [155](#)
- Call Admission Control using Bandwidth Limits (CAC-BL) [123](#)
- call-by-call service selection [135](#)
- call center [47](#)
- messaging [60](#)
- release control [58](#)
- call charge information [218](#)
- call-classifier board [185](#)
- call completion [164](#)
- call control [156](#)
- call coverage [111](#), [170](#), [239](#)
- alphanumeric field designation [239](#)
- and CAS [170](#)
- changeable coverage paths [239](#)
- enhanced coverage and ringback for logged off IP/PSA/TTI terminals [240](#)
- redirection intervals [242](#)
- report [225](#)
- time of day [240](#)
- Call Coverage Remote Off Net (C-CRON) [170](#)
- Call Detail Recording (CDR) [78](#), [176](#), [177](#), [219](#)
- display of physical extension [219](#)
- call distribution based on skill [65](#)
- call forwarding
 - all calls [241](#)
 - busy/do not answer [240](#)
 - diversion [165](#)
 - override [241](#)
- call handling [39](#)
- Call Independent Signaling Connections (CISC) [166](#)
- Call Management System (CMS)
 - measurement of ATM [63](#), [127](#)
- call offer [166](#)
- Call Offer, *see* attendant, intrusion
- call park [242](#)
- call pickup [243](#)
- group call pickup [243](#)
- call prompting
 - call center messaging [60](#)
 - data collection [58](#)
 - Data In/Voice Answer (DIVA) [58](#)
- call redirection intervals [242](#)
- call redirection to multimedia endpoint [79](#)
- call restrictions [199](#), [220](#)
- call routing [181](#)
- call selection override per skill [55](#)
- call transfer [166](#)
- call vectoring [59](#)
- advanced vector routing [59](#)
- Average Speed of Answer (ASA) routing [59](#)
- Class of Restriction (COR) for VDN [61](#)

Index

| | |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Expected Wait Time (EWT) | 60 |
| holiday vectoring | 60 |
| call waiting | 40 |
| Call Work Codes (CWC) | 62 |
| called name ID | 166 |
| Caller Emergency Service Identification (CESID). . . | 134 |
| Caller ID (ICLID) | |
| on analog trunks | 143 , 243 |
| on digital trunks. | 143 , 243 |
| Caller Information Forwarding (CINFO) | 62 |
| calling of inward restricted stations | 40 |
| calling party/billing number | 220 |
| calls | |
| charging for service | 218 |
| disconnecting. | 244 |
| monitoring | 44 |
| placing | 44 |
| redirecting | 240 |
| routing capabilities | 183 |
| CAMA, see Centralized Automatic Message Accounting (CAMA) | |
| camp-on/busy-out | 154 |
| capacities | 26 |
| CAS, see Centralized Attendant Service (CAS) | |
| CCMS, see Control Channel Message Set (CCMS) | |
| C-CRON, see Call Coverage Remote Off Net (C-CRON) | |
| CCSA, see Common Control Switching Arrangements (CCSA) | |
| CDR, see Call Detail Recording (CDR) | |
| Center Stage Switch (CSS). | 121 , 122 |
| separation of | 122 |
| Central Office (CO) | 133 , 144 |
| support on G700 Media Gateway - Russia . . . | 97 , 133 |
| Centralized Attendant Service (CAS) | 43 , 167 |
| Centralized Automatic Message Accounting (CAMA) 134 , 209 | |
| Centralized voice mail (Tenovis) | 108 |
| CES, see Circuit Emulation Service (CES) | |
| CESID, see Caller Emergency Service Identification (CESID) | |
| changeable coverage paths | 239 |
| check-in/check-out | 90 |
| CIDR, see Classless Interdomain Routing (CIDR) | |
| CINFO see Caller Information Forwarding (CINFO) | |
| Circuit Emulation Service (CES) | 127 |
| circuit switched | 122 , 127 |
| circular station hunt group | 62 , 243 |
| CISC, see Call Independent Signaling Connections (CISC) | |
| CLAN, see Control LAN (CLAN) | |
| Class of Restriction (COR) | 61 , 140 , 167 , 199 , 220 , 264 |
| attendant display | 167 |
| for VDN | 61 |
| Class of Service (COS). | 220 , 230 |
| Classless Interdomain Routing (CIDR) | 151 , 221 |
| CMS, see Call Management System (CMS) | |
| CO, see Central Office (CO) | |
| code calling access | 79 |
| codecs. | 155 |
| Common Control Switching Arrangements (CCSA) . . | 132 |
| communication device support | 83 |
| Communication Manager | 25 , 215 |
| fault/performance manager | 216 |
| Octel QSIG integration. | 167 |
| overview | 25 |
| PC console | 85 |
| Communication Manager Messaging | 103 |
| Completion of Calls on No Reply (CCNR) | 136 |
| Completion of Calls to Busy Subscriber (CCBS) . . | 136 |
| Complex private numbering plan support. | 167 |
| Computer Telephony Integration (CTI) | 47 , 62 |
| concurrent user sessions | 222 |
| conference/transfer display prompts | 74 |
| conference/transfer toggle/swap | 74 |
| conferencing | 73 , 244 |
| abort conference on hangup | 73 |
| automatic answer intercom. | 80 |
| automatic intercom | 80 |
| code calling access | 79 |
| conference/transfer display prompts | 74 |
| dial intercom | 80 |
| expanded meet-me | 75 |
| group listen | 74 |
| group paging | 80 |
| hold/unhold | 74 |
| loudspeaker paging access | 81 |
| manual signaling | 81 |
| meet-me | 75 |
| multimedia | 79 , 179 |
| no dial tone | 75 |
| no hold conference | 75 |
| select line appearance. | 76 |
| selective party display and drop | 76 |
| six party | 73 |
| three party | 73 |
| transfer toggle/swap | 74 |
| whisper page | 81 |
| with attendant | 41 |
| configuration manager | 215 |
| Connected Party Number (CPN). | 49 , 207 |
| restriction per call | 207 |
| restriction per line | 208 |
| connection preserving failover/failback for H.248 media gateways | 188 |
| Connection Preserving Migration (CPM) | 188 |
| connection preserving upgrades for duplex servers . | 188 |
| console | |
| Avaya SoftConsole | 86 , 87 |
| PC | 85 |
| consult. | 244 |
| Control Channel Message Set (CCMS) | 123 |
| Control LAN (CLAN) | |
| load balancing | 155 |

- multiple network regions [151](#), [193](#)
- control of trunk group access [38](#)
- COR, *see* Class of Restriction (COR)
- Co-residency with SIP [29](#)
- co-resident DEFINITY LAN Gateway (DLG) [48](#)
- COS, *see* Class of Service (COS)
- Coverage Answer Group (CAG) [239](#)
- coverage callback [244](#)
- coverage incoming call identification [244](#)
- coverage points report [225](#)
- CPM, *see* Connection Preserving Migration (CPM)
- CPN, *see* Connected Party Number (CPN)
- crisis alert
 - to a digital numeric pager [208](#)
 - to a digital station [208](#)
 - to an attendant console [45](#), [209](#)
- CSS, *see* Center Stage Switch (CSS)
- CTI, *see* Computer Telephony Integration (CTI)
- customer selection of VIP DID numbers [90](#)
- Customer Telephone Activation [222](#)
- customer-provided equipment alarm [199](#), [222](#)
- CVLAN [32](#)
- CWC, *see* Call Work Codes (CWC)

D

- DAA, *see* Direct Agent Announcement (DAA)
- daily wakeup [90](#)
- data call setup [175](#)
- data calls [89](#)
- data collection [58](#)
- data conference [77](#), [79](#), [177](#), [179](#)
- data conferencing (T.120) via ESM [79](#), [179](#)
- data hot line [175](#)
- Data In/Voice Answer (DIVA) [58](#)
- data interfaces [175](#)
 - administered connections [175](#)
 - data call setup [175](#)
 - data hot line [175](#)
 - data privacy [175](#)
 - data restriction [176](#)
 - default dialing [176](#)
- multimedia
 - Application Server Interface (ASI). [177](#)
 - call early answer on vectors and stations [177](#)
 - call redirection to multimedia endpoint [179](#)
 - calling [177](#)
 - hold, conference, transfer, and drop [179](#)
 - Multimedia Call Handling (MMCH) [178](#)
 - multiple-port networks [179](#)
- pass advice of charge information to world class BRI endpoints [179](#)
- data privacy [175](#), [199](#)
- data restriction [176](#), [200](#)
- Daylight Savings Time rules change [151](#)
- DCS+, *see* Distributed Communications System plus (DCS+)

- DCS, *see* Distributed Communications System (DCS) protocol
- DDC, *see* Direct Department Calling (DDC)
- default dialing [176](#)
- defense switched network (DSN) [251](#)
- DEFINITY LAN Gateway (DLG) [34](#)
- DEFINITY Wireless Business System (DWBS) [114](#)
- deluxe paging [81](#)
- DEM, *see* Avaya Directory Enabled Management (DEM)
- destination voice endpoint. [78](#), [178](#)
- device and media control API [33](#)
- dial access to attendant [37](#)
- Dial Plan Expansion (DPE) [125](#), [171](#)
- Dial Plan Transparency for LSP and ESS [189](#)
- dial-by-name [90](#)
- Dialed Number Identification Service (DNIS) [63](#)
- DID, *see* Direct Inward Dialing (DID)
- differentiated services (DiffServ) [155](#)
 - type-of-service value [149](#)
- Digital Communications Protocol (DCP) [99](#)
- digital interfaces [135](#)
 - Digital Service 1 (DS1) trunks [127](#), [143](#)
 - E1 [128](#), [143](#)
 - T1 [128](#), [144](#)
 - TTY over digital trunks [162](#)
- digital multiplexed interface [133](#)
 - bit-oriented signalling [133](#)
 - message-oriented signalling [133](#)
- Digital Service 1 (DS1) trunks [127](#), [143](#), [144](#)
- digital telephones
 - 2420 DCP
 - voice mail retrieval button. [110](#)
- DIOD, *see* Direct Inward/Outward Dialing (DIOD)
- Direct Agent Announcement (DAA) [48](#)
- direct agent calling [63](#)
- Direct Department Calling (DDC) [239](#)
- direct extension selection [45](#)
- direct extension selectors (DXS). [43](#)
- Direct Inward Dialing (DID) [134](#), [144](#)
 - automatic number selection [89](#)
- Direct Inward/Outward Dialing (DIOD) [134](#), [145](#)
- direct trunk group selection [39](#), [45](#), [147](#)
- directory [240](#)
- disconnecting unanswered calls [244](#)
- display [43](#), [147](#)
 - and drop conferencing [76](#)
 - ARP report [225](#)
 - VDN for route-to DAC [61](#)
- distinctive alerting [170](#)
- distinctive ringing [245](#)
 - maintain external ring tone after internal transfer [245](#)
- Distributed Communications System (DCS) protocol [147](#), [164](#), [171](#), [245](#), [249](#)
 - attendant functions [38](#), [147](#)
 - control of trunk group access [38](#)
 - direct trunk group selection [39](#), [147](#)

Index

- display [43](#), [147](#)
- inter-PBX attendant calls [39](#)
- automatic circuit assurance [147](#), [222](#)
- Italy [96](#), [148](#)
- over ISDN-PRI D-channel [148](#)
- with reroute [148](#)
- Distributed Communications System plus (DCS+) . . . [148](#)
- DIVA, *see* Data In/Voice Answer (DIVA)
- DLG, *see* co-resident DEFINITY LAN Gateway (DLG)
- DLG, *see* DEFINITY LAN Gateway (DLG)
- DNIS, *see* Dialed Number Identification Service (DNIS)
- do not answer reason code [117](#)
- do not disturb [91](#)
- do not split [44](#)
- DPE, *see* Dial Plan Expansion (DPE)
- DS1, *see* Digital Service 1 (DS1)
- DSN, *see* defense switched network (DSN)
- dual homing [252](#)
- dual links to CMS [63](#)
- dual wakeup [91](#)
- duplicate agent login ID administration [64](#)
- agent-loginID skill pair increase [64](#)
- DWBS, *see* DEFINITY Wireless Business System (DWBS)
- DXS, *see* direct extension selectors (DXS)
- dynamic jitter buffers [155](#)
- dynamic percentage adjustment [55](#)
- dynamic queue position [55](#)
- dynamic threshold adjustment [55](#)

E

- E&M signaling - continuous and pulsed [98](#), [134](#)
- E1 digital interface [128](#), [143](#)
- E911 [134](#), [209](#)
- E911 device location for IP telephones [117](#)
- E911 ELIN for IP wired extensions [116](#)
- EAS, *see* Expert Agent Selection (EAS)
- EC500, *see* Avaya Extension to Cellular
- echo cancellation circuit pack [128](#), [143](#)
- ECS, *see* Enterprise Communication Server (ECS)
- ECT, *see* ETSI Explicit Call Transfer (ECT) signaling
- EIW, *see* Electronic pre-Installation Worksheet (EIW)
- Electronic pre-Installation Worksheet (EIW) [27](#)
- Electronic Tandem Network (ETN) [148](#)
- automatic alternate conditional routing [148](#)
- extension number portability [149](#)
- traveling class marks [185](#)
- trunk signaling and error recovery [149](#)
- emergency access to the attendant [209](#)
- emergency and journal report [225](#)
- emergency calls [116](#), [134](#), [209](#)
- emergency calls from unnamed IP endpoints [245](#)
- emergency transfer [193](#)
- EMU, *see* Enterprise Mobility User (EMU)
- Enbloc Dialing and Call Type Digit Analysis [183](#)
- encryption algorithm for bearer channels [200](#)

- end office access line hunting [252](#)
- enhanced abbreviated dialing [246](#)
- enhanced coverage and ringback for logged off IP/PSA/TTI terminals [240](#)
- enhanced information forwarding [57](#)
- enhanced logging of user actions [227](#)
- enhanced night service [254](#)
- Enhanced Private Switched Communications Service (EPSCS) [132](#)
- enhanced security logging [201](#)
- Enhanced Software License Program (ESLP) [248](#)
- enhanced telephone display [246](#)
- Enterprise Communication Server (ECS). [98](#)
- Enterprise Mobility User (EMU) [247](#)
- enhancements [247](#)
- Enterprise Survivable Servers (ESS). [189](#)
- Enterprise Wide Licensing (EWL) [248](#)
- EPN, *see* Expansion Port Network (EPN)
- EPSCS, *see* Enhanced Private Switched Communications Service (EPSCS)
- ESLP, *see* Enhanced Software License Program (ESLP)
- ESM, *see* Expansion Services Module (ESM)
- ESS, *see* Enterprise Survivable Servers (ESS)
- ETN, *see* Electronic Tandem Network (ETN)
- ETSI Explicit Call Transfer (ECT) signaling [67](#)
- ETSI functionality [135](#)
- ETSI Completion of Calls to Busy Subscriber (CCBS) and on No Reply (CCNR). [136](#)
- European Union [121](#)
- EWL, *see* Enterprise Wide Licensing (EWL)
- EWT, *see* Expected Wait Time (EWT)
- expanded meet-me conferencing [75](#)
- Expansion Port Network (EPN) [121](#)
- Expansion Services Module (ESM) [77](#), [79](#), [177](#), [179](#)
- Expected Wait Time (EWT) [60](#)
- Expert Agent Selection (EAS) [48](#), [50](#), [64](#)
- add/remove skills [64](#)
- call distribution based on skill [65](#)
- queue to best ISDN support [65](#)
- extended trunk access [173](#)
- extension number portability [149](#)
- external device alarming [223](#)

F

- FAC, *see* Feature Access Code (FAC)
- facility and non-facility associated signaling [136](#)
- facility busy indication [223](#)
- facility restriction levels and traveling class marks [201](#), [223](#)
- facility test calls [223](#)
- far end mute, *see* selective conference mute
- faxes, sending and receiving over IP [157](#)
- Feature Access Code (FAC) [165](#)
- feature plus [136](#)
- FIFO, *see* First In/First Out (FIFO)
- firmware download [224](#)
- First In/First Out (FIFO) [57](#)

five EPN maximum in MCC1 Media Gateways [224](#)
flexible billing [48](#), [144](#)
Foreign Exchange (FX). [134](#), [145](#)
FX, *see* Foreign Exchange (FX)

G

Gateway Installation Wizard (GIW) [28](#)
Generalized Conference Call (GCC) [79](#), [179](#)
generalized route selection [183](#)
GIW, *see* Gateway Installation Wizard (GIW)
go to cover [248](#)
group call pickup. [243](#)
group listen [74](#)
group paging [80](#)

H

H.248 link encryption. [201](#)
H.248 media gateway control [122](#)
H.323 trunk [129](#)
hairpinning [160](#)
historical reports [54](#)
history report
 parsing capabilities [227](#)
hold [248](#)
hold, conference, transfer, and drop. [79](#)
hold/unhold conference [74](#)
holiday vectoring. [60](#)
hospitality [89](#)
hot line service [249](#)
housekeeping status [91](#)
HP DL380G2 server, support for [261](#)
hunt group measurements report [225](#)
hunt groups [50](#)
 circular station [62](#)
 circular station hunting [243](#)

I

ICC, *see* Internal Call Controller (ICC)
ICLID, *see* Caller ID
IGAR, *see* inter-gateway alternate routing (IGAR)
IGC, *see* Inter-Gateway Calls (IGC)
increased attendant consoles [43](#)
increased text field length for feature buttons - DCP [87](#)
individual attendant access [37](#)
individual operator access [37](#)
integrated directory [240](#)
Integrated Services Digital Network (ISDN)
 automatic Termination Endpoint Identifier (TEI) [135](#)
 Basic Rate Interface (ISDN-BRI). [136](#)
 call-by-call service selection [135](#)
 ETSI functionality [135](#)
 facility and non-facility associated signaling. [136](#)
 feature plus [136](#)
 Multiple Subscriber Number (MSN) [138](#)
 NT interface on TN556C [139](#)
 presentation restriction. [139](#)
 queue to best ISDN support [65](#)
 trunks [135](#)
 wideband switching [139](#)
integration with Cajun rules [155](#)
intelligent networking [147](#)
intercom
 automatic [80](#)
 automatic answer [80](#), [248](#)
 dial [80](#)
inter-gateway alternate routing (IGAR) [123](#)
Inter-Gateway Calls (IGC). [162](#)
internal automatic answer [248](#)
Internal Call Controller (ICC) [27](#), [192](#)
international digital connectivity [135](#)
International Standardization Organization (ISO) [164](#)
Internet Protocol (IP) [122](#), [129](#), [149](#)
 asynchronous links [176](#), [228](#)
 Avaya Softphone [83](#), [234](#)
 for pocket PC [84](#)
 H.323 trunk [129](#)
 improved button downloads [129](#)
 increased trunk capacity [129](#)
 loss groups [130](#)
 Port Network Connectivity (PNC) [123](#)
 report. [225](#)
 sending and receiving faxes [157](#)
 T.38 faxes over the Internet [159](#)
 trunks [130](#)
 fallback to PSTN [131](#)
 link bounce [131](#)
 TTY over Avaya IP trunks [162](#)
 TTY pass through mode [163](#)
 TTY relay mode [163](#)
inter-PBX attendant calls [39](#)
Interruptible Aux work. [52](#)
intrusion [39](#)
IP bearer duplication using the TN2602AP circuit pack [190](#)
 bearer signal duplication [191](#)
 load balancing [190](#)
 reduced channels with duplication [191](#)
IP endpoint Time-to-Service (TTS). [192](#)
IP overload control [156](#)
IP packet monitors [202](#)
IP Softphone and IP Agent
 RoadWarrior mode [84](#), [233](#)
 Shared Control mode [84](#), [234](#)
 Telecommuter mode. [84](#), [234](#)
ISDN, *see* Integrated Services Digital Network (ISDN)
ISDN-BRI, *see* Integrated Services Digital Network (ISDN),
 Basic Rate Interface (ISDN-BRI)
ISO 8859-1 encoding compatibility. [262](#)
ISO, *see* International Standardization Organization (ISO)
Italian Distributed Communications System (DCS) protocol
 [96](#), [148](#)

Index

J

Japanese national private networking support . . . [97](#), [139](#)
Java Telephony Application Programming Interface (JTAPI) [34](#)
JTAPI, *see* Java Telephony Application Programming Interface (JTAPI)

K

katakana characters [97](#)

L

LAI, *see* Look-Ahead Interflow (LAI)
last number dialed [249](#)
LDAP *see* Lightweight Directory Access Protocol (LDAP)
Least Occupied Agent (LOA) [65](#)
Leave Word Calling (LWC) [107](#), [168](#)
 QSIG/DCS [108](#)
LEC, *see* Local Exchange Carrier (LEC)
license modes [255](#)
 license-error mode [255](#)
 license-normal mode [255](#)
 no-license mode [256](#)
Lightweight Directory Access Protocol (LDAP) [217](#)
Limit Number of Concurrent Calls (LNCC) [256](#)
line load control [252](#)
link recovery [124](#)
Linux platforms
 time of day clock synchronization [231](#)
listed directory number [41](#)
Listen-only FAC for service observing [69](#)
LNCC, *see* Limit Number of Concurrent Calls (LNCC)
LOA, *see* Least Occupied Agent (LOA)
local call timer automatic start/stop [249](#)
Local Exchange Carrier (LEC) [95](#), [143](#), [238](#)
local exchange trunks [144](#)
 800-service [144](#)
 Central Office (CO) [133](#), [144](#)
 Digital Service 1 (DS1) [144](#)
 Direct Inward Dialing (DID) [144](#)
 Direct Inward/Outward Dialing (DIOD) [145](#)
 Foreign Exchange (FX) [145](#)
 Wide Area Telecommunications Service (WATS) [145](#)
local feedback for queued ACD calls [53](#)
local music-on-hold [229](#)
Local Survivable Processor (LSP) [27](#), [192](#)
localization [95](#)
locally sourced announcements and music [66](#)
logged-in advocate agent counting [55](#)
long hold recall [249](#)
Look-Ahead Interflow (LAI) [57](#), [135](#)
 enhanced information forwarding [57](#)
look-ahead routing [135](#), [184](#)
loss groups for IP [130](#)
loudspeaker paging access [81](#)
LSP, *see* Local Survivable Processor (LSP)

LWC, *see* Leave Word Calling (LWC)

M

maintain external ring tone after internal transfer . . . [245](#)
making calls [44](#)
malicious call trace [202](#), [228](#)
 logging [202](#), [228](#)
 over ETSI PRI [202](#)
management
 calls [54](#)
 property [92](#)
manual message waiting [108](#)
manual originating line service [249](#)
manual signaling [81](#)
Manufacturer-Specific Information (MSI) [65](#), [168](#)
mask station name and number for internal calls . . . [202](#)
media encryption [202](#)
meet-me conferencing [75](#)
merge of IP Connect and Multiconnect configurations [153](#)
message integration [103](#)
Message Sequence Tracer (MST) [109](#)
Message Waiting Indication (MWI) [168](#)
messages
 audible message waiting [107](#)
 manual message waiting [108](#)
 retrieval [109](#)
MFP, *see* Multi-Frequency Packet (MFP) signaling - Russia
misoperation handling [250](#)
MLPP, *see* multiple level precedence and preemption (MLPP)
MMCH, *see* Multimedia Call Handling (MMCH)
MMCX, *see* Multimedia Communications Exchange (MMCX)
mobility [113](#)
modem over IP (MoIP) [158](#)
MoIP, *see* modem over IP (MoIP)
monitoring calls [44](#)
MSI, *see* Manufacturer-Specific Information (MSI)
MSN, *see* Multiple Subscriber Number (MSN)
MST, *see* Message Sequence Tracer (MST)
multiappearance preselection and preference [250](#)
Multi-Frequency Packet (MFP) signaling - Russia [97](#), [139](#)
multi-location dial plans [171](#)
multimedia, *see* multimedia calling
Multimedia Call Handling (MMCH) [78](#), [178](#)
multimedia calling
 Application Server Interface (ASI) [78](#), [177](#)
 call early answer on vectors and stations . . . [78](#), [177](#)
 call redirection to multimedia endpoint . . . [79](#), [179](#)
 data conferencing [77](#)
 (T.120) via ESM [79](#), [179](#)
 Expansion Services Module (ESM) [77](#), [79](#), [177](#), [179](#)
 hold, conference, transfer, and drop [79](#), [179](#)
 multiple-port networks [179](#)
 queuing with voice announcement [79](#)
 voice and video [77](#)
Multimedia Communications Exchange (MMCX) . . . [78](#)

| | |
|------------------------------------------------------------------------|-------------------------------------------|
| Multinational Locations | 98 |
| analog line board parameters per location | 99 |
| companding for DCP telephones and circuit packs per location | 99 |
| location ID in Call Detail Record (CDR) records | 99 |
| loss plans per location | 100 |
| multifrequency signaling per trunk group | 100 |
| multiple call handling (forced) | 65 |
| multiple level precedence and preemption (MLPP) | 251 |
| announcements for precedence calling | 251 |
| dual homing | 252 |
| end office access line hunting | 252 |
| line load control | 252 |
| precedence call waiting | 252 |
| precedence calling | 252 |
| precedence routing | 253 |
| preemption | 253 |
| worldwide numbering and dialing plan (WNDP) | 254 |
| multiple location support | 184 |
| for network regions | 151 , 185 |
| multiple music sources | 229 |
| multiple music/audio sources | 66 |
| multiple network regions per CLAN | 151 , 193 |
| multiple split queuing | 66 , 67 |
| Multiple Subscriber Number (MSN) | 138 |
| Multi-Tech gateway support | 29 |
| music-on-hold | 228 |
| MWI, see Message Waiting Indication (MWI) | |

N

| | |
|-------------------------------------------------------|-------------------------------------------|
| name and number identification | 168 |
| name display on unsupervised transfer | 166 |
| name/number permanent display | 118 |
| names registration | 91 |
| NAPT, see Network Address Port Translation (NAPT) | |
| NAT, see Network Address Translation (NAT) | |
| national private networking support - Japan | 97 , 139 |
| NCR, see Network Call Redirection (NCR) | |
| Network Address Port Translation (NAPT) | 161 |
| Network Address Translation (NAT) | 160 |
| with shuffling | 160 |
| network answer supervision | 185 |
| Network Call Redirection (NCR) | 47 , 66 |
| 2B-channel transfer | 67 |
| Network Region Wizard (NRW) | 123 |
| network regions | 151 |
| multiple location support for | 151 , 185 |
| network services | 135 |
| night service | 254 |
| enhanced | 254 |
| no dial tone conferencing | 75 |
| no hold conference | 75 |
| node number routing | 184 |
| NRW, see Network Region Wizard (NRW) | |
| NT interface on TN556C | 139 |

O

| | |
|--------------------------------------------------------|-------------------------------------------|
| Octel integration | 109 , 167 |
| off-PBX station (OPS) | 115 |
| off-premises station | 234 |
| on-hook programming | 235 |
| Open System Interconnect (OSI) | 135 |
| operator dial access | 37 |
| OPS, see off-PBX station (OPS) | |
| optional software | 26 |
| Options to clear display of collected digits | 62 |
| OSI, see Open System Interconnect (OSI) | |
| Overall Loudness Rating | 130 |
| override of diversion features | 41 |
| overview of Communication Manager | 25 |

P

| | |
|--------------------------------------------------------------------------|---------------------|
| packet error history report | 226 |
| paging access | |
| loudspeaker | 81 |
| parsing capabilities of the history report | 227 |
| pass advice of charge information to world class BRI endpoints | 179 |
| pass advice of charge to BRI endpoints | 218 |
| PASTE, see PC Application Software Translation Exchange (PASTE) | |
| PAT, see Port Address Translation (PAT) | |
| path replacement with path retention | 169 |
| PC Application Software Translation Exchange (PASTE) 67 | |
| PCOL, see Personal Central Office Line (PCOL) | |
| PE, see Processor Ethernet (PE) | |
| pending work mode change | 49 |
| per call CPN restriction | 207 |
| per line CPN restriction | 208 |
| percent allocation distribution | 56 |
| Percentage allocation routing | 60 |
| Periodic Pulse Metering (PPM) | 218 |
| Permanent Virtual Paths (PVP) | 121 |
| Personal Central Office Line (PCOL) | 140 |
| Personal Station Access (PSA) | 117 |
| name/number permanent display | 118 |
| personalized ringing | 257 |
| placing calls | 44 |
| PMS, see Property Management System (PMS) | |
| PNA, see Private Network Access (PNA) | |
| PNC, see port network connectivity (PNC) | |
| Port Address Translation (PAT) | 161 |
| port network and gateway connectivity | 121 |
| port network and link usage report | 226 |
| Port Network Connectivity (PNC) | |
| Asynchronous Transfer Mode (ATM) | 121 |
| over WAN | 121 |
| Internet Protocol (IP) | 123 |
| posted messages | 257 |
| power failure transfer | 193 |
| PPM, see Periodic Pulse Metering (PPM) | |

Index

- PPN, *see* Processor Port Network (PPN)
- precedence call waiting [252](#)
- precedence calling [252](#)
- precedence routing [253](#)
- preemption [253](#)
- presentation restriction [139](#)
- PRI, *see* Primary Rate Interface (PRI)
- Primary Rate Interface (PRI) [127](#), [135](#)
- priority calling [257](#)
- priority queue [42](#), [167](#)
- privacy
 - attendant lockout [39](#), [198](#)
 - auto exclusion [210](#)
 - manual exclusion [210](#)
- Private Network Access (PNA) [148](#)
- Processor Ethernet (PE) [152](#)
 - adjuncts [152](#)
 - H.248 and H.323 registration [153](#)
 - S8500 Media Servers [154](#)
- processor occupancy report [226](#)
- Processor Port Network (PPN) [121](#)
- Property Management System (PMS) [90](#), [176](#)
 - digit to insert/delete [92](#)
 - interface [92](#)
- PSA, *see* Personal Station Access (PSA)
- PSTN, *see* Public Switched Telephone Network (PSTN)
- public network call priority [100](#)
- public networking and connectivity [143](#)
- Public Switched Telephone Network (PSTN). [66](#)
- pull transfer [258](#)
- PVP, *see* Permanent Virtual Paths (PVP)
- Q**
 - QoS, *see* Quality of Service (QoS)
 - QSIG [135](#)
 - basic. [164](#)
 - call completion [164](#)
 - call forwarding (diversion) [165](#)
 - Call Independent Signaling Connections (CISC) [166](#)
 - call offer [166](#)
 - call transfer. [166](#)
 - called name ID [166](#)
 - Centralized Attendant Service (CAS). [167](#)
 - attendant return call [167](#)
 - priority queue [167](#)
 - RLT emulation through a PRI. [167](#)
 - Class of Restriction (COR), attendant display. [167](#)
 - Communication Manager/Octel integration [167](#)
 - Leave Word Calling (LWC) [108](#)
 - Manufacturer-Specific Information (MSI) [168](#)
 - Message Waiting Indication (MWI) [168](#)
 - name and number identification [168](#)
 - overview [164](#)
 - path replacement with path retention. [169](#)
 - reroute after diversion to voice mail [169](#)
 - stand-alone path replacement [169](#)
 - supplementary services and rerouting [170](#)
 - support for Unicode [88](#)
 - VALU. [170](#)
 - call coverage [170](#)
 - call coverage and CAS [170](#)
 - distinctive alerting [170](#)
 - QSIG Supplementary Service - Advice of Charge (SS-AOC) [145](#)
 - QSIG/DCS
 - Leave Word Calling (LWC). [108](#)
 - voice mail interworking. [110](#), [148](#), [169](#)
 - Quality of Service (QoS) [149](#), [154](#)
 - 802.1p/Q [154](#)
 - call control [156](#)
 - codecs [155](#)
 - differentiated services (DiffServ) [155](#)
 - dynamic jitter buffers [155](#)
 - for VoIP. [156](#)
 - integration with Cajun rules [155](#)
 - RSVP [157](#)
 - shuffling and hairpinning [160](#)
 - to endpoints. [157](#)
 - variable length ping [163](#)
 - Variable Length Subnet Mask (VLSM) [164](#)
 - queue status indications [54](#)
 - queue to best ISDN support [65](#)
 - queuing
 - multiple split. [66](#)
 - with voice announcement [79](#)
- R**
 - real-time reports [54](#)
 - reason codes. [68](#)
 - recall [37](#)
 - recall signaling [258](#)
 - recalling the attendant [37](#)
 - recent change history report. [226](#)
 - record on messaging [106](#)
 - recorded telephone dictation access [258](#)
 - redirection of calls [240](#)
 - call forward busy/do not answer [240](#)
 - call forwarding all calls. [241](#)
 - call forwarding override [241](#)
 - call redirection intervals [242](#)
 - on no answer [68](#)
 - RedSky Technologies, *see* E911 device location for IP telephones
 - refresh route report [226](#)
 - Release Link Trunks (RLT) [140](#), [167](#)
 - emulation through a PRI [167](#)
 - release loop operation [42](#)
 - reliability and survivability [187](#)
 - remote access trunks [140](#), [234](#)
 - remote logout of agent [68](#)
 - reports [225](#)

- attendant position [225](#)
- blockage study [225](#)
- call coverage [225](#)
- coverage points [225](#)
- display ARP [225](#)
- emergency and journal [225](#)
- historical [54](#)
 - parsing capabilities of [227](#)
- hunt group measurements. [225](#)
- Internet Protocol (IP) [225](#)
- management [54](#)
- packet error history [226](#)
- port network and link usage [226](#)
- processor occupancy [226](#)
- real-time [54](#)
- recent change history [226](#)
- refresh route [226](#)
- summary [226](#)
- tandem traffic. [226](#)
- traffic [226](#)
- trunk group detailed measurement. [227](#)
- reroute after diversion to voice mail [169](#)
- reserve agent time in queue activation [56](#)
- reset shift call [258](#)
- Resource Reservation Protocol (RSVP) [157](#)
- restriction - controlled [204](#), [210](#), [229](#)
- ringback queuing [259](#)
- ringer cutoff [259](#)
- ringing
 - abbreviated and delayed [259](#)
 - distinctive [245](#)
 - options. [259](#)
 - personalized [257](#)
- RLT, see Release Link Trunks (RLT)
- room numbers dialing plan [92](#)
- room status [38](#), [89](#)
- routing features [181](#)
- RSVP, see Resource Reservation Protocol (RSVP)
- Russian CO support on G700 Media Gateway [97](#), [133](#)
- Russian Multi-Frequency Packet (MFP) signaling [97](#), [139](#)
- S**
- satellite hops [148](#)
- SBS, see Separation of Bearer and Signaling (SBS)
- scheduling. [230](#)
- secure shell and secure FTP (SSH/SFTP). [205](#)
- security of IP telephone config files [205](#)
- security of IP telephone registration/H.323 signaling channel [205](#)
- Security Violation Notification (SVN) [206](#), [230](#)
- security, privacy, and safety [197](#)
 - end user [207](#)
 - backup alerting [207](#)
 - barrier codes [207](#)
 - crisis alert to a digital numeric pager [208](#)
 - crisis alert to a digital station [208](#)
 - crisis alert to an attendant console [209](#)
 - emergency access to the attendant [209](#)
 - per call CPN restriction [207](#)
 - per line CPN restriction [208](#)
 - privacy, auto exclusion [210](#)
 - privacy, manual exclusion. [210](#)
 - restriction - controlled. [210](#)
 - station lock [210](#)
 - station lock by Time of Day [211](#)
- system administrator [197](#)
 - access security gateway (ASG) [197](#)
 - alternate facility restriction levels [198](#)
 - alternate operations support system alarm [198](#)
 - call restrictions [199](#)
 - Class of Restriction (COR) [199](#)
 - customer-provided equipment alarm. [199](#)
 - data privacy [199](#)
 - data restriction [200](#)
 - encryption algorithm for bearer channels. [200](#)
 - facility restriction levels and traveling class marks [201](#)
 - H.248 link encryption [201](#)
 - malicious call trace [202](#)
 - mask station name and number for internal calls [202](#)
 - media encryption [202](#)
 - privacy - attendant lockout [198](#)
 - restriction - controlled. [204](#)
 - Security Violation Notification (SVN). [206](#)
 - signaling encryption for SIP trunks [206](#)
 - SRTP media encryption [200](#)
 - station security codes [206](#)
 - tripwire security [206](#)
- select line appearance conferencing [76](#)
- selective conference mute [42](#), [77](#)
- selective conference party display and drop [76](#)
- self-administered telephones [263](#)
- send all calls [259](#)
- separate licensing for TDM telephones and TDM trunks [128](#)
- Separation of Bearer and Signaling (SBS) [125](#)
- serial calling [42](#)
- service observing. [68](#)
 - by COR. [69](#)
 - of VDNs [69](#)
 - remote [69](#)
 - vector-initiated [70](#)
- Session Initiation Protocol (SIP)
 - SIP Visiting User [118](#)
- Session Initiation Protocol (SIP) [116](#), [131](#), [155](#)
 - trunks [132](#)
- shuffling [160](#)
 - and NAT devices [160](#)
- signaling encryption for SIP trunks. [206](#)
- single-digit dialing and mixed station numbering [92](#)
- SIP, see Session Initiation Protocol (SIP)
- site statistics for remote port networks [70](#)
- six party conferencing. [73](#)

Index

- skill [64](#)
- SLS, *see* Standard Local Survivability (SLS)
- SMS, *see* system management service (SMS)
- sniffers [202](#)
- special dial tone [260](#)
- SREPN, *see* Survivable Remote Expansion Port Network (SREPN)
- SRTP media encryption [200](#)
- SS-AOC, *see* QSIG Supplementary Service - Advice of Charge (SS-AOC)
- SSH/SFTP, *see* secure shell and secure FTP (SSH/SFTP)
- stand-alone path replacement [169](#)
- Standard Local Survivability (SLS) [194](#)
- station hunt before coverage [260](#)
- station hunting [260](#)
- station lock [210](#)
- station lock by Time of Day [211](#)
- station security codes [206](#), [230](#)
- station self display [260](#)
- station used as a virtual extension [261](#)
- suite check-in [93](#)
- summary report [226](#)
- supplementary services and rerouting [170](#)
- supplementary services, definition of [164](#)
- support for the HP DL380G2 server [261](#)
- Survivable Remote Expansion Port Network (SREPN) [194](#)
- SVC, *see* Switched Virtual Circuits (SVC)
- SVN, *see* Security Violation Notification (SVN)
- switch
 - Asynchronous Transfer Mode (ATM) [121](#), [127](#)
 - CSS (direct connect) [121](#)
- Switched Virtual Circuits (SVC) [121](#)
- system management [213](#)
- system management service (SMS) [32](#)
- T**
- T.120 protocols [79](#), [179](#)
- T.38 faxes over the Internet. [159](#)
- T1 digital interface [128](#), [144](#)
- tandem switch [149](#)
- tandem through [149](#)
- Tandem Tie-Trunk Network (TTTN) [149](#)
- tandem traffic report [226](#)
- TDD, *see* Telecommunication Devices for the Deaf (TDD); *see also* TTY
- team button [261](#)
- TEI, *see* Termination Endpoint Identifier (TEI)
- Telecommunication Devices for the Deaf (TDD) [161](#)
- telecommuting access [233](#)
- telecommuting and remote office [233](#)
- telephone display [262](#)
 - ISO 8859-1 encoding compatibility [262](#)
- telephones
 - announcements [214](#)
 - digital
 - 2420 DCP. [110](#)
 - self-administration [263](#)
 - telephony [235](#)
 - telephony service (TS) [32](#)
 - Telephony Services Application Programming Interface (TSAPI) [34](#)
 - temporary bridged appearance [263](#)
 - Temporary Signaling Connection (TSC) [164](#)
 - tenant partitioning [229](#), [230](#)
 - Terminal Translation Initialization (TTI). [119](#), [231](#)
 - terminating extension group [263](#)
 - Termination Endpoint Identifier (TEI), automatic [135](#)
 - three party conferencing [73](#)
 - tie trunks [140](#)
 - time of day [240](#)
 - time of day clock synchronization
 - Linux platforms [231](#)
 - UNIX platforms [231](#)
 - via LAN source [231](#)
 - time of day routing [184](#), [264](#)
 - timed automatic disconnect for outgoing trunk calls [140](#)
 - timed call disconnection for outgoing trunk calls [264](#)
 - timed reminders [42](#)
 - TN464GP/TN2464BP universal DS-1 circuit pack. [128](#)
 - TN556C circuit pack [139](#)
 - TN787 [79](#), [179](#)
 - TOS, *see* Type-Of-Service (TOS)
 - traffic report [226](#)
 - transfer
 - abort [265](#)
 - outgoing trunk to outgoing trunk [265](#)
 - recall [265](#)
 - trunk-to-trunk [265](#)
 - upon hang-up [265](#)
 - TransTalk 9000 digital wireless system. [119](#)
 - traveling class marks [185](#)
 - tripwire security. [206](#)
 - trunk call disconnection [140](#), [264](#)
 - trunk connectivity [127](#)
 - trunk flash [266](#)
 - trunk group
 - attendant control of access. [44](#)
 - busy/warning indicators to attendant [46](#)
 - circuits [231](#)
 - detailed measurement report. [227](#)
 - identification [49](#)
 - trunk identification by attendant [46](#)
 - trunk signaling and error recovery [149](#)
 - trunks
 - analog
 - Caller ID (ICLID) [143](#), [243](#)
 - auxiliary [132](#)
 - Advanced Private Line Termination (APLT) [132](#)
 - echo cancellation. [128](#), [143](#)
 - digital. [133](#)
 - Caller ID (ICLID) [143](#), [243](#)
 - Digital Service 1 (DS1). [127](#), [143](#)

Direct Inward Dialing (DID) [134](#)
 Direct Inward/Outward Dialing (DIOD) [134](#)
 Foreign Exchange (FX) [134](#)
 group circuits [231](#)
 H.323 [129](#)
 Internet Protocol (IP) [130](#)
 ISDN [135](#)
 local exchange [144](#)
 800-service [144](#)
 Central Office (CO) [133](#), [144](#)
 Digital Service 1 (DS1) [144](#)
 Direct Inward Dialing (DID) [144](#)
 Direct Inward/Outward Dialing (DIOD) [145](#)
 Foreign Exchange (FX) [145](#)
 Wide Area Telecommunications Service (WATS) [145](#)
 Personal Central Office Line (PCOL) [140](#)
 Release Link (RLT) [140](#), [167](#)
 remote access [140](#), [234](#)
 tandem [148](#)
 tie [140](#)
 Wide Area Telecommunications Service (WATS) . [141](#)
 trunk-to-trunk transfer [265](#)
 TS, see telephony service (TS)
 TSAPI, see Telephony Services Application Programming Interface (TSAPI)
 TSC, see Temporary Signaling Connection (TSC)
 TTI, see Terminal Translation Initialization (TTI)
 TTS, see IP endpoint Time-to-Service (TTS)
 TTTN, see Tandem Tie-Trunk Network (TTTN)
 TTY [161](#)
 over analog and digital trunks [162](#)
 over Avaya IP trunks [162](#)
 pass through mode [163](#)
 relay mode [163](#)
 Type-Of-Service (TOS) [155](#)

U

UCD, see Uniform Call Distribution (UCD)
 UDP, see Uniform Dial Plan (UDP)
 UDS1 circuit pack with echo cancellation [128](#), [143](#)
 Unicode support [87](#)
 QSIG [88](#)
 Uniform Call Distribution (UCD) [239](#)
 Uniform Dial Plan (UDP) [171](#)
 UNIX platforms
 time of day clock synchronization [231](#)
 usage allocation [135](#)
 user service [33](#)
 User-to-User Information (UUI)
 over the public network [70](#)
 propagation [49](#)
 UUI, see User-to-User Information (UUI)

V

variable length ping [163](#), [232](#)
 Variable Length Subnet Mask (VLSM) [164](#), [232](#)

VCO, see Voice Carry Over (VCO)
 VDN, see Vector Directory Number (VDN)
 vector commands [59](#)
 Vector Directory Number (VDN) [60](#), [64](#), [68](#)
 display VDN for route-to DAC [61](#)
 in a coverage path [61](#)
 observing on agent answer [70](#)
 of origin announcement [61](#)
 override for ASAI messages [50](#)
 return destination [61](#)
 vectoring [59](#)
 attendant [40](#)
 holiday [60](#)
 vector-initiated service observing [70](#)
 VIAS, see Visually Impaired Attendant Service (VIAS)
 video [177](#)
 VIP wakeup [93](#)
 Virtual LAN (VLAN) [154](#)
 Visually Impaired Attendant Service (VIAS) [46](#)
 VLSM, see Variable Length Subnet Mask (VLSM)
 VMON, see VoIP Monitoring Manager (VMON)
 Voice Announcement over LAN (VAL) Manager . . . [216](#)
 Voice Carry Over (VCO) [161](#)
 voice mail integration [78](#)
 voice mail interworking [169](#)
 QSIG/DCS [110](#), [148](#)
 voice mail retrieval button [110](#)
 voice mail system (VMS) [254](#)
 voice message retrieval [110](#)
 voice messaging and call coverage [111](#)
 Voice Response Integration (VRI) [71](#)
 VoIP Monitoring Manager (VMON) [147](#), [217](#)
 VRI, see Voice Response Integration (VRI)
 VuStats [71](#)
 login IDs [71](#)
 service level [71](#)

W

wakeup
 activation via confirmation tones [93](#)
 automatic [89](#)
 daily [90](#)
 dual [91](#)
 VIP [93](#)
 WATS, see Wide Area Telecommunications Service (WATS)
 Web services [32](#)
 whisper page [81](#)
 Wide Area Telecommunications Service (WATS) [141](#), [145](#), [182](#)
 wideband switching [139](#)
 wireless
 X-station mobility [119](#)
 WNDP, see worldwide numbering and dialing plan (WNDP)
 world class tone detection [101](#)
 worldwide numbering and dialing plan (WNDP) . . . [254](#)

Index

X

Xiox call accounting [93](#)
XOIP Tone Detection Bypass [101](#)
X-station mobility [119](#)