Implementing the Avaya B5800 Branch Gateway

Release 6.1
18-603853
Issue 5
November 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya is a registered trademark of Avaya Inc.

Aura is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Overview

The Avaya B5800 Branch Gateway is a single-platform solution with multiple deployment options that enable seamless, user-centric access to Avaya Aura® Messaging, Avaya Aura® Conferencing, Avaya Aura® Presence services and much more. It's complimentary to any existing networking solution, adding communications and collaboration functionality in a “thin” device designed for branch use. Supporting either distributed, centralized, or mixed network deployments, the B5800 Branch Gateway is adaptable to meet the needs of specific features and applications of individual employees in each branch location. The result is a smooth migration between architectures. In addition to centralized SIP endpoints, the B5800 Branch Gateway can concurrently support other IP and TDM endpoints for a community of centralized and distributed users on the same platform. Ideal for customers wanting applications deployed in customer data centers and/or in the branch itself, the B5800 Branch Gateway enables the branch to cost effectively deliver the range of communication tools without complex infrastructure and administration.

Branch user deployment models

B5800 Branch Gateway can be deployed in the Distributed, Centralized or Mixed Branch user models.

- **Distributed Branch user model** — In this model, call processing for the branch phones is provided locally. Non-IP phones are connected to B5800 Branch Gateway and IP and SIP video endpoints are administered with B5800 Branch Gateway as their controller. Access to and from the rest of the Avaya Aura® network is via the B5800 Branch Gateway system's Avaya Aura® Session Manager link across the enterprise WAN. This connection allows for VoIP connectivity to other B5800 Branch Gateway systems, to centralized trunking and to centralized applications such as conferencing and Modular Messaging.
- **Centralized Branch user model** — Certain 9600 Avaya SIP phones can use the B5800 Branch Gateway as a survivability gateway (see Supported telephones on page 21 for more information). In normal operation, these phones register directly to the Avaya Aura®Session Manager in the enterprise core and get services from core applications such as the Communication Manager Feature Server. The local B5800 Branch Gateway can still be accessed as a SIP gateway connected to the core Avaya Aura®Session Manager to provide access to local PSTN trunks and services when required. If WAN connectivity to the Avaya Aura®Session Manager is lost, the SIP phones automatically register with and get services from the B5800 Branch Gateway. When connection to the Avaya Aura®Session Manager is available again, failback occurs where the SIP phones return to being controlled by Avaya Aura® Session Manager.
- **Mixed Branch user model** — Each B5800 Branch Gateway system can support extensions using the Centralized Branch user model and extensions using the Distributed

Branch user model at the same time. The extensions supported in the Centralized Branch user model are SIP extensions only.

Centralized solution

The B5800 Branch Gateway can be deployed as a Distributed branch, a Centralized branch, or a Mixed branch. Both Distributed and Centralized branches can benefit from centralization. In Distributed branch deployments, the option to leverage centralized PSTN trunking and centralized applications such as voice mail and conferencing is provided. In Centralized branch deployments, in addition to the above, phone registration and call processing is also centralized.

The centralized solution is based primarily on the central Avaya Aura® infrastructure at the enterprise core. During normal operation, the centralized users located in the branches receive their service from the core, like users in the main office do. The phones register directly to the Avaya Aura®Session Manager in the enterprise core, get their features from the central Communication Manager Feature Server (CM-FS) or Communication Manager Evolution Server (CM-ES), and utilize the Avaya Aura® applications.

The local B5800 Branch Gateway can be accessed as a SIP gateway connected to the core Avaya Aura®Session Manager to provide access to local PSTN trunks and services when required. In addition, if WAN connectivity to the Avaya Aura®Session Manager is lost, the centralized SIP phones automatically failover and register with the B5800 Branch Gateway which provides them with basic telephony survivability. When connection to the Avaya Aura®Session Manager is available again, failback occurs where the SIP phones return to being controlled by Avaya Aura®Session Manager.

In the centralized solution, the users must be administered on the Avaya Aura®Session Manager and the core Communication Manager, as well as on the local B5800 Branch Gateway. The centralized users' extension numbers must be defined according to the enterprise numbering plan of the Avaya Aura® Session Manager. In addition to general administration of the Avaya Aura®Session Manager and the core Communication Manager, special consideration must be given to the design and configuration of branch location-dependent functionality in the Session Manager and optionally also in the core Communication Manager. It is also important to verify the readiness of the underlying IP network since in the centralized solution, VoIP is transported over the WAN.

PSTN trunking configurations

With the ability to administer call control at both the B5800 Branch Gateway and the Avaya Aura®Session Manager, there are many ways you can optimize external PSTN trunk usage. The B5800 Branch Gateway is a full PABX and by default uses its own PSTN trunks. However

it can be configured to make and receive external calls via the central Avaya Aura®Session Manager. A combination of these methods can be used for PSTN calls based on the call type (local, national, international), time of day or even individual user. See Branch PSTN call routing examples on page 325 for more information.

Voicemail support options

B5800 Branch Gateway supports a range of options for voicemail services to the branch's native users. It supports embedded voicemail for native branch users and auto attendants for external PSTN trunks. This can be changed to using a local Voicemail Pro voicemail server or to using the central Modular Messaging server. In the later mode the B5800 Branch Gateway can still use the local Embedded Voicemail for announcements to waiting callers and for auto attendants.

Centralized management

The Network Management offer is a suite of software applications that enable centralized management of the B5800 Branch Gateway system. It provides a single access interface to manage multiple branch locations. The suite of applications include:

- Avaya Network Management Console — allows you to view the devices in the network.
- Manager — allows you to view and edit individual branches in the B5800 Branch Gateway system.
- Avaya Provisioning and Installation Manager — allows you to provision and install large numbers of B5800 Branch Gateway devices simultaneously through the use of templates and bulk provisioning to a group of devices.

Note:

- When using Network Management to create a hardware template, Manager provides the **IP500v2** and **ABG B5800** control units as options. Be sure to select **ABG B5800**. IP500v2 is not supported in branch mode.
- The B5800 Branch Gateway system is referred to as IP Office in the Network Management applications.

If you do not have the Network Management applications installed on a server in your network, you can use Manager to administer each branch in the system. Manager is an off-line editor. This means that it receives a copy of the current branch configuration. Changes are made to the copy and then sent back to the branch for those changes to become active.

Note:

If you are going to use Network Management for centralized management of the B5800 Branch Gateway system, Network Management (NM) 6.0, NM 6.0 SP2, plus an additional B5800 Branch Gateway patch hosted on the Avaya support web site must be installed and configured.

For more information about Network Management, see the *Avaya Integrated Management 6.0 Network Management Configuration* guide which is available on the Avaya support web site.

Remote access to Network Management

You are able to use Avaya Aura® Session Manager Release 6.x, cut-through capability to access Network Management. The System Manager cut-through allows the provisioning of the Network Management IP address with a unique menu name within the System Manager GUI. Although System Manager and Network Management must be installed on two separate servers, there is a single access interface for administration and management of the B5800 Branch Gateway. For more information, see Creating a System Manager link to Network Management on page 161.

In addition to System Manager cut-through, you are able to remotely access Network Management using a Secure Access Link (SAL) Gateway. A standalone SAL Gateway is installed in the enterprise headquarters and allows remote management of individual branches in the B5800 Branch Gateway system. See Standalone SAL Gateway for remote service on page 215 for more information.

Licensing

B5800 Branch Gateway is a licensed solution. Branch licenses are issued and validated against the Feature Key serial number of the System SD card used by that branch. That number is printed after the **FK** prefix on the System SD card and is also shown in the branch system configuration. This means that licenses issued for one branch cannot be used in the configuration of another branch. In the Manager application, this number appears in the **PLDS Host ID** field on the System page when you select **System > System**.

The B5800 Branch Gateway licenses are as follows:

- Avaya Branch Gateway System Software license
- Station licenses
- Embedded Messaging Ports license
- Voicemail Pro Messaging Ports license
- SIP Trunk Sessions license
- Additional channels licenses
    - Additional T1 Channels license

    - Additional E1 Channels license
- 120-day trial license

B5800 Branch Gateway uses the Avaya Product Licensing and Delivery System (PLDS) to manage license entitlements. See **Chapter 11: Managing license files with PLDS** for more information.

The B5800 Branch Gateway licenses are described below.

Avaya Branch Gateway System Software license

This license is required for operation of the B5800 Branch Gateway system. This license does not include any implicit entitlements and therefore is not sufficient by itself for branch operation without additional Station and/or SIP Trunk Session licences.

Station licenses

All users on a B5800 Branch Gateway system must be licensed by the addition of Station licenses. There are two types of Station licenses:

- **Native Station licenses** — are required for all configured users with analog, digital, H.323 or DECT extensions and for all users with SIP extensions set as native (or local) (that is, extensions operating in the Distributed Branch user model).
- **Survivable Station licenses** — are required for all configured users with SIP extensions set as survivable (or centralized) (that is, extensions operating in the Centralized branch user model, normally connecting to the Avaya Aura® core and connecting to the B5800 Branch Gateway is survivable mode during rainy-day).

Warning:

Unlicensed extensions will display **No License Available** but will be able to make emergency calls, i.e. calls that match B5800 Branch Gateway Dial Emergency short codes.

Embedded Messaging Ports license

This license is required if you are using the B5800 Branch Gateway voicemail option, Embedded voicemail or using the B5800 Branch Gateway Embedded Auto-Attendant and Announcements with a central voicemail option. Up to 6 ports can be licensed. At least one Embedded Messaging Port license must be purchased to enable this service.

Voicemail Pro Messaging Ports license

This license is required if you are using the B5800 Branch Gateway voicemail option, Voicemail Pro. Up to 40 ports can be licensed. At least one Voicemail Pro Messaging Port license must be purchased to enable this service.

Note:

An Embedded Messaging Ports license and a Voicemail Pro Messaging Ports license cannot be used together on the same system.

SIP Trunk Sessions license

This license refers to the total number of concurrent sessions allowed on all SIP connections to the B5800 Branch Gateway. The maximum number of SIP trunk sessions is 128. SIP trunks

provide the SIP connections between Avaya Aura®Session Manager and B5800 Branch Gateway.

Additional channels licenses

The PRI Universal (PRI-U) trunk card can be used in the B5800 Branch Gateway system. The PRI-U ports can be configured to support E1, E1R2, or T1 line types. Each port supports 8 B channels which do not require a license. Additional B channels beyond these 8 require a license. There are two additional channels licenses that define the number of additional channels (above the default 8):

- **Additional T1 Channels license** — This license is for additional T1 trunks.
- **Additional E1 Channels license** — This license is for additional E1 or E1R2 trunks.

For trunk types on which channels can be set as in service, the licenses are consumed by those channels which are configured as being in service. Manager will block attempts to configure PRI channels as in service if they exceed the 8 per port allowed by default on that card and if there are no Additional T1 Channels or Additional E1 Channels licenses available.

120-day trial license

This license provides a 120-day trial period during which you have access to the features, functions, and capabilities available in B5800 Branch Gateway. After the expiration of the 120-day trial license, the 30-day grace period is activated. At the end of the 30-day grace period, if no other license is installed or available, system administration is blocked.

License modes

The B5800 Branch Gateway system can be in one of three license modes — License Normal Mode, License Error Mode, and License Restricted Mode. The license mode, as well as any license errors, are displayed in Manager. When the B5800 Branch Gateway system is in License Error Mode, a 30-day grace period is provided during which time the system is fully functional. If the B5800 Branch Gateway system is in License Error Mode, all license errors must be fixed, either by installing a valid license file with the appropriate licenses or by changing the configuration so that it does not exceed any licensed capacities. If the B5800 Branch Gateway system is in License Error Mode and not all license errors are fixed within the 30-day grace period, the system will go into License Restricted Mode in which system administration is blocked except for fixing the license errors.

System components

The B5800 Branch Gateway system is comprised of the following hardware components.

- **Control unit** — The control unit stores the system configuration and performs the routing and switching for telephone calls and data traffic. It includes 4 slots for optional base cards to support trunk and phone extension ports. The slots are numbered 1 to 4 from left to

right. They can be used in any order; however, if the capacity for a particular type of card is exceeded, the card in the right-most slot will be disabled.

- **SD card** — The B5800 Branch Gateway SD card is a uniquely numbered dongle used to validate license keys entered into the B5800 Branch Gateway system configuration to enable features. It also provides embedded voicemail support and storage for system software files. The card fits into a slot in the rear of the control unit.
- **Base cards** — The control unit has slots for up to 4 base cards. The base cards are used to add analog extension ports, digital extension ports, and voice compression channels. Each base card includes an integral front panel with ports for cable connections. The following base cards are supported:
  - **Digital station base card** — This card provides 8 digital station (DS) ports for the connection of Avaya digital phones other than IP phones. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection. A maximum of 3 digital station base cards are allowed per control unit.
  - **Analog phone base card** — This card is available in two variants, supporting either 2 or 8 analog phone ports. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection. A maximum of 4 analog phone base cards are allowed per control unit. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.
  - **VCM base card** — This card is available in variants supporting either 32 or 64 Voice Compression Channels (VCM) for use with VoIP calls. A maximum of 2 VCM base cards are allowed per control unit. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection.
  - **4–port expansion base card** — This card adds an additional 4 expansion ports for external expansion modules. The card is supplied with four 2m yellow interconnect cables. This card does not accept any trunk daughter cards. A maximum of 1 4–port expansion base card is allowed per control unit (right-hand slot 4 only). See External expansion modules on page 20 for a list of the supported external expansion modules.
  - **BRI combination card** — This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 2 BRI trunk ports (9-10, 4 channels). The card also includes 10 VCM channels. This card has a pre-installed BRI trunk daughter card. A maximum of 2 BRI combination cards of any type are allowed per control unit.
  - **ATM combination card** — This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 4 analog trunk ports (9-12). The card also includes 10 VCM channels. This card has a pre-installed analog trunk daughter card. A maximum of 2 ATM combination cards of any type are allowed per control unit. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.

- **Trunk daughter cards** — Most base cards can be fitted with a trunk daughter card to support the connection of trunks to the base card. The following trunk daughter cards are supported:
  - **Analog trunk card** — This card allows the base card to support 4 analog loop-start trunks. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12. A maximum of 4 analog trunk cards are allowed per control unit.
  - **BRI trunk card** — This card allows the base card to support up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. The card is available in 2 port (4 channels) and 4 port (8 channels) variants. A maximum of 4 BRI trunk cards are allowed per control unit. For S-Bus connection, the card can be switched from To trunk mode to So mode. This mode requires additional terminating resistors and an ISDN crossover cable connection.
  - **PRI trunk card** — This card allows the base card to support up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. A maximum of 4 PRI trunk cards are allowed per control unit. The B5800 Branch Gateway system supports 8 unlicensed B-channels on each IP500 PRI-U port fitted. Additional B-channels, up to the capacity of ports installed and PRI mode selected require Universal PRI (Additional Channels) licenses added to the configuration. These additional channels consume the licenses based on which additional channels are configured as in-service from port 9 of slot 1 upwards. D-channels are not affected by licensing.
- **Combination cards** — Combination cards are pre-paired base and trunk daughter cards. They provide 6 digital station ports, 2 analog phone ports, 10 VCM channels and either 4 analog trunk ports or 4 BRI channels (2 ports). The trunk daughter card cannot be removed or replaced with another type of trunk daughter card.
- **External expansion modules** — External expansion modules are used to add additional analog and digital ports. If the control unit is fitted with a 4–port expansion base card, then up to 12 external expansion modules are supported. The following external expansion modules are supported:
  - **Analog trunk module** — This module rovides an additional 16 analog ports for connection of analog trunks. It supports both loop-start and ground-start trunks.
  - **BRI So8 module** — This module provides 8 ETSI BRI-So ports for the connection of ISDN devices. This module is not intended to support BRI trunks.
  - **Digital station module** — This module provides, depending on variant, an additional 16 or 30 DS ports for supported Avaya digital phones.
  - **Phone module** — This module provides, depending on variant, an additional 16 or 30 phone ports for analog phones.

- **Power supplies** — The control unit has an internal power supply unit. Each external expansion module is supplied with an external power supply unit. Additional power supply units may also be required for IP phones and some phone add-ons.
- **Power cords** — Depending on the locale, different power cords need to be ordered for each control unit, external expansion module, and any phones or devices using external power supply units.
- **Mounting kits** — The control unit can be used free-standing, with external expansion modules stacked above it. With optional rack mounting kits, the control unit and external expansion modules can also be rack mounted. Alternatively, with an optional wall mounting kit the control unit can be wall mounted. However, the control unit cannot support any external expansion modules when wall mounted.
- **Surge protectors and barrier boxes** — Where the installation includes extensions in other buildings, additional protective equipment is required. This equipment may also be required in areas where the lightning risk is high.
- **Phones** — B5800 Branch Gateway systems support a variety of Avaya digital and IP phones plus analog phones.
- **Application DVDs** — The B5800 Branch Gateway applications can be ordered on a number of DVDs. In addition they can be downloaded from the B5800 Branch Gateway section of the Avaya support web site (http://support.avaya.com).

Supported telephones

Telephone	Native extensions	Survivable extensions
Analog	✔	
1403	✔	
1408	✔	
1416	✔	
1603	✔	
1603SW	✔	
1608	✔	
1616	✔	
1603SW-I	✔	
1608-I	✔	
1616-I	✔	

Telephone	Native extensions	Survivable extensions
BM32 (DSS)	✔[1]	
2402D	✔	
2410D	✔	
2420	✔	
3641 wireless	✔	
3645 wireless	✔	
3720 DECT R4	✔	
3725 DECT R4	✔	
4602IP	✔	
4602SW	✔	
4610IP	✔	
4610SW	✔	
4621	✔	
4625	✔	
5402	✔	
5410	✔	
5420	✔	
EU24 (DSS)	✔[1]	
5601	✔	
5602IP	✔	
5602SW	✔	
5610IP	✔	
5610SW	✔	
5620	✔	
5621	✔	
EU24BL (DSS)	✔[1]	
9620L	✔[2]	✔[3]
9620C	✔[2]	✔[3]
9630G	✔[2]	✔[3]
9640	✔[2]	✔[3]
9640G	✔[2]	✔[3]

Telephone	Native extensions	Survivable extensions
9650	✔[2]	✔[3]
9650C	✔[2]	✔[3]
SMM24	✔[1]	
9608		✔ [4]
9611G		✔ [4]
9621G		✔[4]
9641G		✔[4]
BM12	✔[1]	
Avaya 1010/1020/1030/1040 video conferencing units	✔	
Standards-compliant 3rd-party SIP audio and video endpoints	✔	

[1] When connected to their respective telephones

[2] With H.323 firmware

[3] With SIP 2.6 firmware

[4] With SIP 6.0 firmware

Software applications

The B5800 Branch Gateway software applications are provided on DVDs. They can also be downloaded from Network Management.

- **User applications** — The following applications are supported for use by native users on an B5800 Branch Gateway system.
  - **Embedded Voicemail**: supports basic voicemail mailbox operation, simple auto-attendants and hunt group announcements. It is provided on the Avaya SD card. This voicemail option requires a license. See Licensing on page 16 for more information.
  - **Voicemail Pro**: is a complete voicemail solution and provides Interactive Voice Response (IVR) and call recording capabilities. Voicemail Pro runs on a server PC connected to the B5800 Branch Gateway system. This voicemail option requires a license. See Licensing on page 16 for more information.

- **SoftConsole**: is intended for telephone system operators or receptionists. It displays details of calls and allows them to quickly see the status of the callers required destination and transfer the call. The SoftConsole user is able to access a range of details about the status of users and groups on the B5800 Branch Gateway system. Up to 4 simultaneous SoftConsole users can be configured. This application does not require a license.

- **Installer/maintainer applications** — The following B5800 Branch Gateway applications are used to program and maintain an B5800 Branch Gateway system. These applications do not require a license.
  - **Manager**: a configuration application used to access all parts of the B5800 Branch Gateway configuration. Different levels of access can be defined to control which parts of the configuration the Manager user can view and alter. Manager is also used to upgrade the software files used by an B5800 Branch Gateway system.
  - **System Status Application**: a monitoring application used to inspect the current status of B5800 Branch Gateway lines and extensions and to view records of recent alarms and events. It runs as a Java application.
  - **System Monitor**: shows a trace of all activity on the B5800 Branch Gateway system in detail. Interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. B5800 Branch Gateway installers and maintainers must run System Monitor when Avaya requests copies of System Monitor traces to resolve support issues.
  - **SNMP MIBs**: Not an application as such, the SNMP MIB files can be used by 3rd-party SNMP applications to monitor the B5800 Branch Gateway system.

Supported country locales

When a new or defaulted system's configuration is first opened in Manager, the value set in the **Locale** field (**System** > **System** > **Locale**) should always be checked and changed if necessary. The system's locale sets factors such as the default ringing patterns and caller display settings. The locale also controls the language that a voicemail server will use for prompts.

The following table indicates locale settings supported for different functions. Note that this does not necessarily indicate support, availability or approval for B5800 Branch Gateway within that country.

Locale	Language	Telephony	Phone Display	Applications		Voicemail	
				Manager	Soft Console	Embedded Voicemail	Voicemail Pro
Argentina	**Latin Spanish**	✓	✓	✓	✓	✓	✓

Locale	Language	Telephony	Phone Display	Applications		Voicemail	
				Manager	Soft Console	Embedded Voicemail	Voicemail Pro
Australia	UK English	✓	✓	✓	✓	✓	✓
Belgium	Dutch	✓	✓	✓	✓	✓	✓
Belgium	French	✓	✓	✓	✓	✓	✓
Brazil	Brazilian	✓	✓	✓	✓	✓	✓
Canada	Canadian French	✓	✓	-	-	✓	✓
Chile	Latin Spanish	✓	✓	✓	✓	✓	✓
China	Mandarin	✓	-	-	✓	✓	✓
Colombia	Latin Spanish	✓	✓	✓	✓	✓	✓
Denmark	Danish	✓	✓	-	✓	✓	✓
Finland	Suomi	✓	✓	-	✓	✓	✓
France	French	✓	✓	✓	✓	✓	✓
Germany	German	✓	✓	✓	✓	✓	✓
Greece	Greek	✓	-	-	-	-	✓
Hong Kong	Cantonese	✓	-	-	-	-	✓
Hungary	Hungarian	-	-	-	-	-	✓
Iceland	Icelandic	✓	-	-	-	-	-
India	UK English	✓	-	✓	✓	✓	✓
Italy	Italian	✓	✓	✓	✓	✓	✓
Korea	Korean	✓	-	-	✓	✓	✓
Mexico	Latin Spanish	✓	✓	✓	✓	✓	✓
Netherlands	Dutch	✓	✓	✓	✓	✓	✓
New Zealand	UK English	✓	✓	✓	✓	✓	✓
Norway	Norwegian	✓	✓	-	✓	✓	✓

Locale	Language	Telephony	Phone Display	Applications		Voicemail	
				Manager	Soft Console	Embedded Voicemail	Voicemail Pro
Peru	**Latin Spanish**	✓	✓	✓	✓	✓	✓
Poland	**Polish**	✓	-				

- **Locale:** The country represented by the locale.
- **Language:** The voicemail prompt language used for that locale.
- **Telephony:** The B5800 Branch Gateway provides default telephony settings matching the normal expected defaults for the locale.
- **Phone Display:** Indicates that display messages from the B5800 Branch Gateway to Avaya phones can be sent using the appropriate language for that locale. Note that the user locale can be used to override the system locale for these messages. Note also that some phones support their own language selection options for menus displayed by the phone's own software.
- **Manager:** Indicates that the B5800 Branch Gateway Manager application can run in the specific locale language. Manager uses the best match it has (French, German, Brazilian, Dutch, Italian, Mexican Spanish or US English) for the regional location setting of the PC on which it is running, otherwise it defaults to UK English. If required the language used within the Manager screens can be overridden.
- **Voicemail:** These columns indicate for which locales the different B5800 Branch Gateway voicemail servers can provide the appropriate language prompts. In all cases, the system locale can be overridden by setting a different user locale.
  - **Embedded Voicemail:** Indicates that the locale is recognized by Embedded Voicemail and appropriate language prompts are then used. If an unsupported locale is used, Embedded Voicemail will attempt the best match using the first two characters of the locale.
  - **Voicemail Pro:** Indicates that the locale is recognized by Voicemail Pro and appropriate language prompts are then used. For an unsupported locale if used, or one for which the necessary prompts are not available, Voicemail Pro will attempt the best match using a sequence of alternate locales. For example French Canadian falls back to French, then US English and finally UK English. Note that the languages available are selectable during Voicemail Pro installation.

Training

Avaya University provides a wide range of training courses for B5800 Branch Gateway and its associated applications. This includes courses necessary for B5800 Branch Gateway resellers to become Avaya Authorized Channel Partners and for individuals to achieve B5800 Branch Gateway certification.

Details of courses can be found on the Avaya University web site (http://www.avaya-learning.com). The site can be used to check course availability and to book courses. It also includes on-line courses and on-line course assessments. The site requires users to setup a user name and password in order to track their personal training record.

For a list of recommended courses available for the B5800 Branch Gateway, see Recommended courses for Avaya B5800 Branch Gateway training on page 335.

Web sites

Information to support B5800 Branch Gateway can be found on a number of web sites.

- Avaya (http://www.avaya.com)

  The official web site for Avaya. The front page also provides access to individual Avaya web sites for different countries.

- Avaya Enterprise Portal (http://partner.avaya.com)

  This is the official web site for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the site portal can be individually customized for what products and information types you wish to see and to be notified about by email.

- Avaya Support (http://support.avaya.com)

  Contains documentation and other support materials for Avaya products.

- Avaya University (http://www.avaya-learning.com)

  This site provides access to the full range of Avaya training courses. That includes both on-line courses, course assessments and access to details of classroom based courses. The site requires users to register in order to provide the user with access to details of their training record.

- Avaya Community (http://www.aucommunity.com)

  This is the official discussion forum for Avaya product users. However it does not include any separate area for discussion of B5800 Branch Gateway issues.

Documentation

Ensure that you have read this manual before starting the installation. Also read the installation documentation for any other equipment and applications being installed as part of the B5800 Branch Gateway system.

Documents you may need to consult are as follows:

- Administering Avaya Aura® Session Manager, document number 03-603324
- Avaya Integrated Management Release 6.0 Network Management Configuration
- Avaya Integrated Management Release 6.0 Network Management Installation and Upgrade
- Avaya Integrated Management Release 6.0 Network Management Console User Guide
- IP Office Manager, document number 15-601011
- IP Office Release 6.1 Embedded Voicemail Installation, document number 15-601067
- Provisioning and Installation Manager for IP Office help system (available in the application)
- Avaya B5800 Branch Gateway Solution Overview, document number 18-603903

Revision history

Issue	Date	Summary of changes
2, 3, and 4		In issues 2, 3, and 4, the following sections were added: • Centralized solution • 96x1 phones SIP firmware download in B5800 Branch Gateway centralized branch deployments • Centralized deployment example call flows • Avaya port matrix for B5800 Branch Gateway and SIP phones • Additional glossary terms
5	2/3/2012	Release 6.1 does not support the 9608, 9621G, and 9641G H.323 telephones in the Distributed Branch user model. In the Supported Telephones table in Chapter 1, the check mark in the **Native extensions** column for these telephones has been removed. These telephones *are* supported as survivable extensions with SIP 6.0 firmware.

Chapter 2: Planning

Before you begin installing and configuring the B5800 Branch Gateway system, you should already have determined the implementation issues listed in the table below.

You have determined...	See	✔
The branch user model you are deploying.	Branch user deployment models on page 13	
The dial plan you are configuring for the system and each branch.	Dial plan considerations on page 30	
The B5800 Branch Gateway licenses required for this installation.	Licensing on page 16	
How you are going to route outgoing PSTN calls.	Branch PSTN call routing considerations on page 32	
The voicemail solution you are going to deploy.	Voicemail considerations on page 31	
The method you will use to configure and manage the branches in the system.	B5800 Branch Gateway configuration methods on page 32	

Prerequisites

The following applications and servers must be installed and configured before the B5800 Branch Gateway system is installed.

- Avaya Aura® Session Manager must be installed and configured at the headquarters location.
- Avaya Aura® Communication Manager must be installed and configured as a feature server at the headquarters location.
- If you are going to use Network Management for centralized management of the B5800 Branch Gateway system, Network Management (NM) 6.0, NM 6.0 SP2, plus an additional B5800 Branch Gateway patch hosted on the Avaya support web site must be installed and configured.
- A stand-alone Secure Access Link (SAL) gateway must be deployed.

Note:
System Platform's virtual SAL gateway is not supported.

Dial plan considerations

A uniform dial plan greatly simplifies configuration, management and phone calls within the network branch sites. For example, if each branch has similar roles such as reception, manager and warehouse - using the same extension number for each role and a unique prefix for each branch allows calls between sites with little need for directory lookups. It also means a standard configuration can be used at branches; simplifying installation, user training and maintenance.

For our examples we have used the following dial plan for each branch site:

- **3-digit branch prefixes beginning with 8** — A 3-digit branch prefix in the range 800 to 899. This allows us up to 100 branches yet keeps call routing simple. Any dialing at a branch that being with an 8 can be assumed to be a call to a branch number and can be routed to the Avaya Aura® Session Manager for routing to the correct branch.
- **3-digit extension numbers beginning with 2** — 3-digit extension numbers for all native extensions and hunt groups starting from 200. This is the default numbering used by B5800 Branch Gateway.

Centralized survivable extensions may have very different numbering. However, even here, adopting elements of the uniform dial plan will simplify management and usage. For the survivable extensions in our examples we have used a dial plan that has 6-digit extension numbers of which the first 3 digits are equal to the branch prefix. This allows users that migrate from the Distributed Branch user model to the Centralized Branch user model to keep their same numbers. The numbers for the survivable extensions can also be different and don't necessarily have to share common first digits.

Dial plan example

To describe a dial plan example, we have created Acme Travel, a travel agency with a growing number of branches. Each branch follows the same pattern, with extensions for a branch manager and a small team of travel consultants in a sales group.

Given the nature of the business, branch users need to make national and international calls. The company has taken advantage of a bulk call contracts from it headquarters site so wants such calls routed via the headquarters site wherever possible. In addition, the branch staff want to keep their branch phone numbers.

- 3-digit branch numbers beginning with 8, ie. 800 to 899.
- 3-digit native extension numbers beginning with 2, ie. 200 to 299.

- 6-digit survivable extension numbers of which the first 3 digits are equal to the branch prefix e.g. 811250.
- Dial 9 prefix for outgoing PSTN calls.
- National and international calls allowed but routed via the headquarters site's PSTN trunks.
- Where a national call matches a branch location, it should be routed to the PSTN via that branch.
- Local calls allowed from each branch using its own PSTN trunks.
- Modular Messaging at the headquarters site provides voicemail services to all employees.
- The LAN on each branch has a unique IP address, 192.168.42.1, 192.168.44.1 and so on.
- A number of survivability features are required:
- National calls via the branch's PSTN trunks when the branch data connection to the headquarters site is not available or at maximum capacity.
- Modular Messaging fallback via PSTN.

This example assumes that all the branches were initially setup with the default North American locale. For B5800 Branch Gateway that means that a dial 9 prefix is used for external calls. For calls in other locales or between branches in different locals, the example will need to be adjusted to ensure that the resulting number received at the remote branch will be routed to an external PSTN trunk and is suitable for external dialing.

Voicemail considerations

The B5800 Branch Gateway system uses its Embedded Voicemail by default. However, a number of other voicemail options are supported.

- **Embedded Voicemail** — Embedded Voicemail uses the system SD card in the B5800 Branch Gateway system control unit for storage of prompts and messages. Embedded Voicemail supports mailboxes for all local extension numbers, announcements to waiting callers, and auto attendants (up to 40) for external calls. Its capacity is limited to 15 hours of recorded messages, prompts and announcements. At least one Embedded Messaging Port license must be purchased to enable this service.
- **Voicemail Pro** — Voicemail Pro runs on a server PC connected to the B5800 Branch Gateway system and provides a wide range of features. Voicemail Pro is the only option that supports manual call recording for the B5800 Branch Gateway system users. It also supports automatic call recording for the B5800 Branch Gateway system. At least one Voicemail Pro license must be purchased to enable this service.
- **Modular Messaging** — The B5800 Branch Gateway system can be configured to use Modular Messaging as its voicemail server. When Modular Messaging is used as the

central voicemail system, at each branch you have the option to still use the local Embedded Voicemail for auto attendant operation and for announcements to waiting calls. See Configuring Modular Messaging on page 164 for more information. Note that for this configuration, Embedded Voicemail licenses are required.

For more information about licensing, see Licensing on page 16.

Branch PSTN call routing considerations

Each B5800 Branch Gateway system can support its own external PSTN trunks. When deployed in an Avaya Aura® network, you have considerable flexibility over where outgoing PSTN calls should emerge from the network and similarly where incoming calls should be routed.

For examples of some of the options available, see Branch PSTN call routing examples on page 325. The examples demonstrate the following options:

- Centralized call control on page 325 — External calls at a branch site can be rerouted to be dialed out at another site. This can be done for reasons of call cost and call control. For example, the central site may have a bulk call tariff for national and international calls that would benefit all branches.
- Branch PSTN Override on page 328 — Having configured the branch to send outgoing external calls to the Avaya Aura® Session Manager for onward routing, there may be cases where a specific number should still be routed via the branches own PSTN trunks.
- PSTN Fallback on page 330 — The B5800 Branch Gateway can be configured to allow some calls that would normally use the Avaya Aura® Session Manager line to be routed via the PSTN when the Avaya Aura® Session Manager line is not available.

The various methods used in the these examples can be combined to match the customer's needs. However the main aim should be as follows:

- To keep the branch configuration as generic as possible, i.e. to use the same PSTN call control in all branch configurations. This simplifies maintenance of multiple branches.
- To centralize as much of the PSTN call control in the Avaya Aura® Session Manager as possible. Again this simplifies maintenance and control.

B5800 Branch Gateway configuration methods

There are two ways to configure and manage the branches in your B5800 Branch Gateway system – locally using Manager or centrally using Network Management.

The Network Management offer is a suite of software applications that enable centralized management of the B5800 Branch Gateway system. It provides a single access interface to manage multiple branch locations. The suite of applications include:

- Avaya Network Management Console — allows you to view the devices in the network.
- Manager — allows you to view and edit individual branches in the B5800 Branch Gateway system.
- Avaya Provisioning and Installation Manager — allows you to provision and install large numbers of B5800 Branch Gateway devices simultaneously through the use of templates and bulk provisioning to a group of devices.

Note:

- When using Network Management to create a hardware template, Manager provides the **IP500v2** and **ABG B5800** control units as options. Be sure to select **ABG B5800**. IP500v2 is not supported in branch mode.
- The B5800 Branch Gateway system is referred to as IP Office in the Network Management applications.

If you do not have the Network Management applications installed on a server in your network, you can use Manager to administer each branch in the system. Manager is an off-line editor. This means that it receives a copy of the current branch configuration. Changes are made to the copy and then sent back to the branch for those changes to become active.

Note:

If you are going to use Network Management for centralized management of the B5800 Branch Gateway system, Network Management (NM) 6.0, NM 6.0 SP2, plus an additional B5800 Branch Gateway patch hosted on the Avaya support web site must be installed and configured.

For more information about Network Management, see the *Avaya Integrated Management 6.0 Network Management Configuration* guide which is available on the Avaya support web site.

Network assessment for VoIP requirements

B5800 Branch Gateway is a converged telephony system, that is it combines aspects of traditional PABX telephone systems and IP data and telephony systems. This works at various levels.

- Individual phone users can control the operation of their phone through applications running on their PC.
- Data traffic can be routed from the LAN interface to a telephony trunk interface, for example a dial-up ISP connection.
- Voice traffic can be routed across internal and external data links. This option is referred to as voice over IP (VoIP).

The VoIP mode of operation can include IP trunks between customer systems and or H.323 IP telephones for users. In either case the following factors must be considered:

- The B5800 Branch Gateway control unit must be fitted with voice compression channels (see Voice compression channels on page 38). These channels are used whenever an IP device (trunk or extension) needs to communicate with a non-IP device (trunk or extension) or a device that uses a different codec.
- A network assessment is a mandatory requirement for all systems using VoIP. For support issues with VoIP, Avaya may request access to the network assessment results and may refuse support if those are not available or satisfactory.

A network assessment includes a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.
- The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support H.323, DHCP, TFTP and jitter buffers in H.323 applications.
- An outline of the expected network assessment targets is:

Test	Minimum Assessment Target
Latency	Less than 150ms
Packet Loss	Less than 3%
Duration	Monitor statistics once every minute for a full week

Chapter 3: Installation requirements

This chapter provides information about power supplies, cables, grounding and environmental and space requirements for installing the B5800 Branch Gateway control unit and external expansion modules. The B5800 Branch Gateway control unit can be mounted on the wall if no external expansion units are included in the installation. If the installation includes external expansion modules, the control unit and external expansion modules can be mounted into a standard 19-inch rack system.

Power supply backup (UPS)

The use of an Uninterrupted Power Supply (UPS) with any telephone system is strongly recommended. Even at sites that rarely lose electrical power, that power may occasionally have to be switched off for maintenance of other equipment. In addition, most UPSs also provide an element of power conditioning, reducing spikes and surges.

The capacity of UPS systems and the total equipment load the UPS is expected to support are usually quoted in VA. Where equipment load is quoted in Watts, multiply by 1.4 to get the VA load.

The calculation of how much UPS capacity is required depends on several choices.

- **What equipment to place on the UPS?** Remember to include server PCs such as the voicemail. It is recommended that the total load on a new UPS is never greater than 75% capacity, thus allowing for future equipment.
- **How many minutes of UPS support is required?** Actual UPS runtime is variable, it depends on what percentage of the UPSs capacity the total equipment load represents. For example, a 1000VA capacity UPS may only support a 1000VA (100%) load for 5 minutes. This relationship is not linear, the same UPS would support a 500VA (50%) load for 16 minutes. Therefore the lower the percentage of capacity used, the increasingly longer the UPS runtime, typically up to 8 hours maximum. Remember also that for most UPS's the ratio of discharge to full recharge time is 1:10.
- **How many output sockets does the UPS provide?** Multiple UPS units may be required to ensure that every item of supported equipment has its own supply socket.

The web site http://www.avayaups.com provides a calculator into which you can enter the equipment you want supported on a UPS. It will then display various UPS options. The site uses VA values for typical B5800 Branch Gateway systems. However, if more specific values are required for a particular system, the table below can be used to enter values.

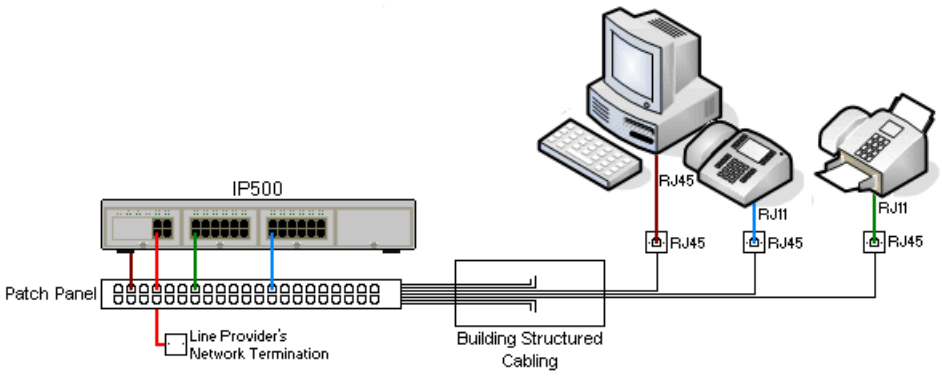
Typical B5800 Branch Gateway System	VA
B5800 Branch Gateway system	230
Individual Equipment	**VA**
Analog 16 module	88
Digital Station 16 module	34
Digital Station 30 module	42
WAN3 module	17
So8 module	34

The 1151D2 power supply unit for Avaya H.323 IP phones includes a backup battery. This typically provides 15 minutes backup at maximum load (20 Watts) and up to 8 hours at light load (2 Watts).

Cables

The B5800 Branch Gateway system is designed primarily for use within an RJ45 structured cabling system using CAT3 unshielded twisted-pair (UTP) cabling and RJ45 sockets.

A structured cabling system is one where cables are run from a central RJ45 patch panel in the communications/data room to individual RJ45 sockets at user locations. All wires in each cable between the patch panel and the desk socket are connected straight through. This arrangement allows devices connected at the patch panel to be swapped to match the type of device that needs to be connected at the user socket. For example, making one user socket a phone port and another user socket a computer LAN port, without requiring any rewiring of the cables between the patch panel and the user location.



- **Traditional IDC punchdown wiring installations** — Where necessary, the far end RJ45 plug can be stripped from B5800 Branch Gateway cables and wired into traditional wiring

systems using punch-block connectors. This type of installation should be performed by an experienced wiring technician.

- **Trunk connections** — The majority of B5800 Branch Gateway trunk ports use RJ45 connectors for acceptance of an RJ45-to-RJ45 cable. However, connection at the line provider's end may require use of a different plug type in order to match the line providers equipment.
- **RJ11 phone connectors** — Many phones use RJ11 sockets and are supplied with RJ11-to-RJ11 cables. RJ11 plugs can be inserted into RJ45 sockets and in many case the connection will work. However this is not recommended or supported as the connection lock is not truly positive and may become disconnected. An RJ45-to-RJ11 cable is available for these connections.

Standard B5800 Branch Gateway cables

The following are Avaya standard cables available for use with B5800 Branch Gateway systems. The maximum length is applicable if the standard Avaya cable is replaced with an alternate cable.

Cable	Description	Standard Length	Maximum Length
9-way DTE cable	Connects to control unit RS232 DTE port. 9-way D-type plug to 9-way D-type socket.	2m/6'6"	2m/6'6"
Structured cabling DS line cable	Connects from RJ45 sockets to RJ11 socketed DS and analog phones.	4m/13'2"	–
BRI/PRI trunk cable	Connects BRI/PRI trunk ports to the line provider's network termination point. RJ45 to RJ45. Red.	3m/9'10"	–
Expansion interconnect cable	Connects the control unit to expansion modules (except WAN3 modules). RJ45 to RJ45. Blue.	1m/3'3"	1m/3'3"
LAN cable	Connects from B5800 Branch Gateway LAN ports toB5800 Branch Gateway devices. RJ45 to RJ45. Grey.	3m/9'10"	100m/328'
V.24 WAN cable	37-way D-type plug to 25-way D-type plug.	3m/9'10"	5m/16'5"
V.35 WAN cable	37-way D-type plug to 34-way MRAC plug.	3m/9'10"	5m/16'5"
X.21 WAN cable	37-way D-type plug to 15-way D-type plug.	3m/9'10"	5m/16'5"

Grounding

Use of ground connections reduces the likelihood of problems in most telephony and data systems. This is especially important in buildings where multiple items of equipment are interconnected using long cable runs, for example phone and data networks.

All control units and external expansion modules must be connected to a functional ground. Where the unit is connected to a power outlet using a power cord with an earth lead, the power outlet must be connected to a protective earth.

In some cases, such as ground start trunks, in addition to being a protective measure this is a functional requirement for the equipment to operate. In other cases it may be a locale regulatory requirement and or a necessary protective step, for example areas of high lightning risk.

For more information about grounding including the location of the ground points on the control unit and external expansion modules, see Grounding on page 65.

Wall and rack mounting

The B5800 Branch Gateway control unit is designed to be freestanding. When external expansion modules are used, the control unit and expansion modules are intended to be stacked. With optional mounting kits, the system can be wall or rack mounted. See Wall mounting on page 59 and Rack mounting on page 61 for more information.

Voice compression channels

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. For B5800 Branch Gateway systems this conversion is done by voice compression channels. These support the common IP audio codecs G711, G723 and G729a.

For the B5800 Branch Gateway control unit, channels can be added using VCM base cards, BRI combination cards, and ATM combination cards. See System components on page 18 for more information about these cards.

The voice compression channels are used as follows:

Call type	Voice compression channel usage
IP device to non-IP device	These calls require a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.
IP device to IP device	Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions: • Short code confirmation, ARS camp on and account code entry tones require a voice compression channel. • Devices using G723 require a voice compression channel for all tones except call waiting. When a call is connected: • If the IP devices use the same audio codec no voice compression channel is used. • If the devices use differing audio codecs, a voice compression channel is required for each.
Non-IP device to non-IP device	No voice compression channels are required.
Music on Hold	This is provided from the B5800 Branch Gateway TDM bus and therefore requires a voice compression channel when played to an IP device.
Conference resources and IP devices	Conferencing resources are managed by the conference chip which is on the B5800 Branch Gateway TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion, call recording and silent monitoring.
Page calls to IP dDevice	B5800 Branch Gateway only uses G729a for page calls, therefore only requiring one channel but also only supporting pages to G729a capable devices.
Voicemail services and IP devices	Calls to the B5800 Branch Gateway voicemail servers are treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
T38 fax calls	In order to use T38 fax connection, B5800 Branch Gateway performs fax tone detection if the analog extension connected to the fax machine is set as “Standard telephone.” If the fax machine does not include an attached handset that is used to make/receive voice calls, then the Equipment Classification of an analog extension connected to the fax machine can be set to **Fax Machine**, which will result in T38 fax connection without fax tone detection and respective signaling renegotiation. Additionally, a new short code feature, Dial Fax, is available.

Measuring channel usage

The B5800 Branch Gateway System Status Application can be used to display voice compression channel usage. Within the **Resources** section it displays the number of channels in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

For the VCM cards, the level of channel usage is also indicated by the LEDs (1 to 8) on the front of the VCM card.

Emergency and power failure ports

B5800 Branch Gateway systems can provide 2 types of analog extension power failure ports as described in the following table.

Type	Description	Provided By:
Switching power failure ports	During normal B5800 Branch Gateway operation these ports can be used for normal analog phone connection. During power failure the port is directly connected to an analog trunk port.	• **Analog phone 8 card** When an analog phone 8 base card is fitted with an analog trunk daughter card, during power failure extension port 8 is connected to analog trunk port 12. • **ATM combination card** On this card, during power failure, extension port 8 is connected to analog trunk port 12.
Emergency only power failure ports	During normal B5800 Branch Gateway operation these ports cannot be used. During power failure the port is directly connected to an analog trunk port.	• **Analog trunk daughter card** Regardless of the card hosting it, during power failure pins 4 and 5 of port 12 are connected to pins 7 and 8.

In all cases these only work with loop-start analog trunks. Any phones connected to these ports should be clearly labeled as power fail extensions in accordance with the appropriate national and local regulatory requirements.

Environmental requirements

The planned location must meet the following requirements. If being installed into a rack system, these are requirements for within the rack:

- Temperature: 0°C to 40°C / 32°F to 104°F.
- Humidity: 10% to 95% non-condensing.
- Check there are no flammable materials in the area.
- Check there is no possibility of flooding.
- Check that no other machinery or equipment needs to be moved first.
- Check that it is not an excessively dusty atmosphere.
- Check that the area is unlikely to suffer rapid changes in temperature and humidity.
- Check for the proximity of strong magnetic fields, sources of radio frequency and other electrical interference.
- Check there are no corrosive chemicals or gasses.
- Check there is no excessive vibration or potential of excessive vibration, especially of any mounting surface.
- Check that where telephones are installed in another building, that the appropriate protectors and protective grounds are fitted (see Out of Building Telephone Installation on page 66).
- Check there is suitable lighting for installation, system programming and future maintenance.
- Check that there is sufficient working space for installation and future maintenance.
- Ensure that likely activities near the system will not cause any problems, e.g. access to and maintenance of any other equipment in the area.
- Where ventilation holes are present on any of the B5800 Branch Gateway units, those holes should not be covered or blocked.
- The surface must be flat horizontal for free-standing or rack mounted installations.

Wall mounting: In additional to the requirements above, the following are applicable to control units that are mounted on the wall.

- Units must only be mounted onto permanent wall surfaces.
- The surface must be vertical and flat.
- Orientation of the unit must be as shown in the section on IP500 Wall Mounting on page 59.
- The appropriate Avaya wall mounting kits must be used.

Note:

See Important safety instructions when using your telephone equipment on page 275 for basic safety precautions to follow when using your telephone equipment.

Space requirements

The B5800 Branch Gateway control unit and external expansion modules are designed to be installed either in a free-standing stack or into a 19-inch rack system. Rack installation requires a rack mounting kit for each control unit and expansion module. See Rack mounting on page 61 for more information. If there are no external expansion modules used in the installation, the control unit can be wall mounted using a wall mounting kit. See Wall mounting on page 59 for more information.

- **Cable clearance**

  Clearance must be provided at the front and rear of all modules for cable access and feature key dongle connection. Allow a minimum clearance of 90mm (3.5 inches).

- **Additional clearance**

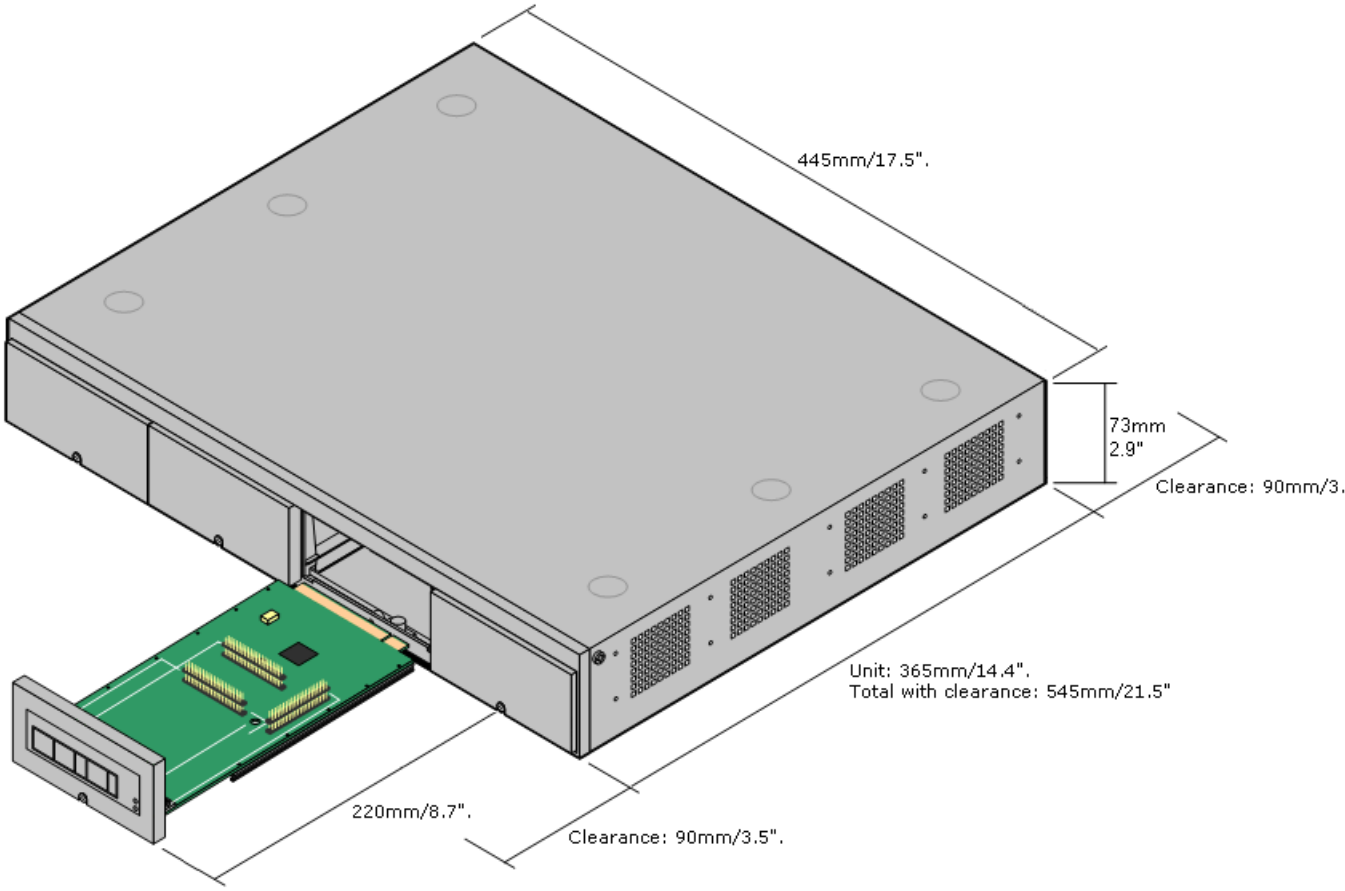
  Care should be taken to ensure that the positioning of the modules does not interrupt air flow and other environmental requirements. The control unit has ventilation slots at the side that must not be blocked. See Environmental requirements on page 41 and Rack space requirements on page 44 for more information.

- **Cable access**

  Power cords must not be attached to the building surface or run through walls, ceilings, floors and similar openings. Installation measures must be taken to prevent physical damage to the power supply cord, including proper routing of the power supply cord and provision of a socket outlet near the fixed equipment or positioning of the equipment near a socket outlet.

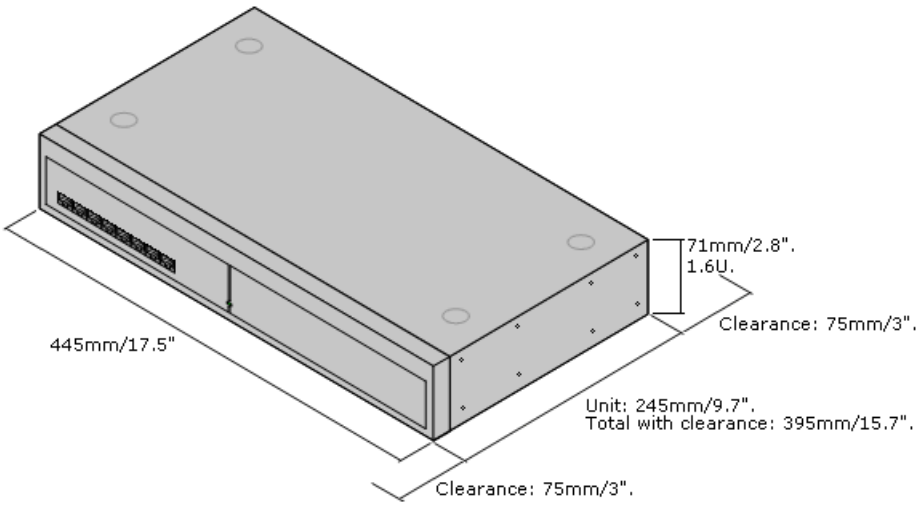
Control unit

When wall mounted, a clearance of 500mm is required on all sides. The ventilation slots on the rear and sides should not be covered or blocked.



External expansion modules

The dimensions below are applicable to all external expansion modules.



Wall mounting space requirements

The control unit can be wall mounted if not using any external expansion modules. A wall mounting kit is required in addition to 4.5mm fixings suitable for the wall type. A clearance of 500mm around the control unit is required. See Wall mounting on page 59 for more information.

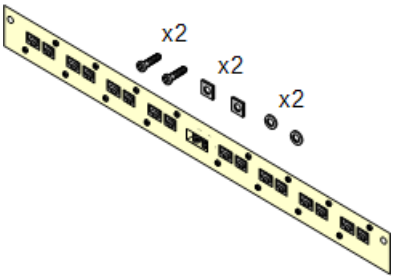
Rack space requirements

The B5800 Branch Gateway control unit and external expansion modules can be rack mounted into standard 19-inch rack systems. Each unit requires a 2U slot space within the rack. Rack mounting requires a rack mounting kit for each control unit and external expansion module. See Rack mounting on page 61 for more information about the rack mounting kit.

Where B5800 Branch Gateway systems are being rack mounted, the effect of conditions within the rack cabinet must be considered. For example the rack temperature may be above the room temperature and airflow within the rack will be restricted. The environmental requirements for the individual control unit and expansion modules are still applicable inside the rack cabinet.

Barrier box rack mounting kit

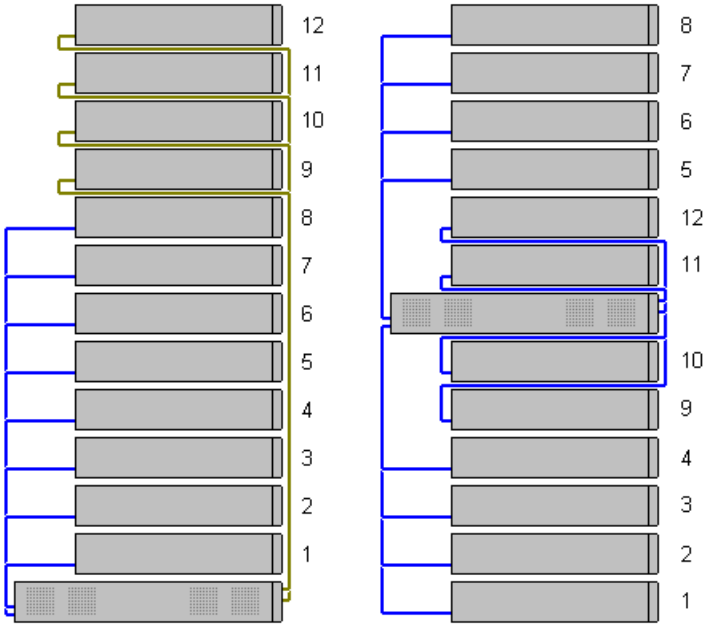
The barrier box rack mounting kit must be used for out-of-building analog phone extensions. This bracket allows up to 8 barrier boxes to be rack mounted and simplifies the number of connections to the protective ground point in the rack. This kit must be used when more than 3 barrier boxes are in use and supports a maximum of 16 barrier boxes for a single external expansion module.



Rack module positioning

The integral expansion ports on a control unit are located on the rear of the unit. An additional 4 expansion ports can be added to the front of the control unit by installing a 4-port expansion card.

- Each external expansion module is supplied with a blue 1 meter (3'3") expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on a 4-port expansion card, a yellow 2-meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. Four yellow cables are supplied with the 4-port expansion card.



Chapter 4: Hardware and software installation

All hardware components should be turned off while they are installed and connected. Once the installation is complete, the system is turned on. The control unit will then upgrade all of the connected components, including phones, to the appropriate level of firmware. In addition, when the system is turned on, it should not be connected to the customer's data network. This ensures that the control unit will default to known default IP address settings (unless you have pre-loaded the System SD card with a configuration file with different settings).

Installation checklist

Use this checklist to monitor your progress as you install a B5800 Branch Gateway system.

#	Description	Section	✔
1	Review the prerequisites.	See Prerequisites on page 29.	
2	Review the Installation requirements.	See Installation requirements on page 35.	
3	Review the required tools and equipment.	See Tools and equipment required on page 48.	
4	Unpack the equipment.	See Unpacking equipment on page 49.	
5	If you want to pre-configure the system, there are several tasks you can perform to configure the SD card before it is installed in the control unit.	See SD card preparation on page 50.	
6	Prepare the base and trunk cards and install them in the control unit.	See Base and trunk card installation on page 53.	
7	Do one of the following: • Install the control unit on the wall. • Install the control unit in a rack.	See one of the following: • Wall mounting on page 59. • Rack mounting on page 61.	

#	Description	Section	✔
8	Connect the external expansion modules.	See External expansion modules on page 63.	
9	Connect the control unit and external expansion modules to a functional ground.	See Grounding on page 65.	
10	Install the B5800 Branch Gateway administration applications on the installer PC.	See Installing the administration applications on page 72.	
11	Connect the PC to the control unit.	See Installer PC connection on page 73.	
12	Apply power to the system.	See Applying power to the system on page 75.	
13	Start the Manager application.	See Starting Manager on page 78.	
14	Change the default IP address settings to match the customer requirements.	See Changing the IP address settings on page 81.	
15	Connect the control unit to the network.	See Connecting the control unit to the network on page 82.	
16	Change the system's security settings.	See Changing the security settings on page 82.	
17	Change the remote user password.	See Changing the remote user password on page 83.	
18	Connect the phones.	See Connecting phones on page 84.	
19	Download the SIP firmware for the 96x1 SIP phones.	See 96x1 phones SIP firmware download in B5800 Branch Gateway centralized branch deployments on page 84.	

Tools and equipment required

Following is a general summary of the tools required. Additional tools and equipment are required for wall and/or rack mounting and to fashion ground cable connections suitable to local requirements.

- **Tools required**
  - 5mm Flat-blade screwdriver
  - Crosshead screwdriver
  - Anti-static wrist strap and ground point

- RJ45-RJ45 ethernet LAN cable
- M4 cross-head screwdriver
- Tools suitable for crimping a cable spade
- If wall mounting, drills and tools for wall mounting fixtures

- **Additional parts required**

  In addition to orderable system equipment, the following items are required.

  - 14AWG solid copper wire for ground connection of control units and expansion modules
  - Cable sleeve matching local regulator requirements for ground wires. Typically green for a functional ground and green/yellow for a protective ground.
  - If wall mounting, additional 4.5mm diameter fixtures and fittings suitable for the wall type
  - Cable ties and labels for tidying and identifying cables

- **PC requirements**

  - Windows PC with the administration software installed. See PC requirements on page 72.
  - SD card reader

Unpacking equipment

About this task

Use the following procedure when unpacking any equipment supplied by Avaya or an Avaya reseller or distributor. Have the equipment order checklist available as you unpack the equipment to ensure you have all parts and equipment ordered.

Procedure

1. **Check for package damage**

   Before unpacking any equipment, check for any signs of damage that may have occurred during transit. If any damage exists bring it to the attention of the carrier.

2. **Check the correct parts have been delivered**

   Check all cartons against the packing slip and ensure that you have the correct items. Report any errors or omissions to the equipment supplier.

3. **Retain all packaging and documentation**

   While unpacking the equipment, retain all the packaging material. Fault returns are accepted only if repackaged in the original packaging. If performing a staged installation, the original packaging will also assist when repacking equipment to be moved to the final install site.

4. **Ensure that anti-static protection measures areobserved**

   Ensure that anti-static protection measures are observed at all times when handling equipment with exposed electrical circuit boards.

5. **Check all parts**

   Visually inspect each item and check that all the necessary documentation and accessory items have been included. Report any errors or omissions to the dealer who supplied the equipment.

6. **Check all documentation**

   Ensure that you read and retain any documentation included with the equipment.

SD card preparation

B5800 Branch Gateway control units are supplied with no installed firmware or configuration. When first powered up, the control unit loads and installs the necessary firmware from the B5800 Branch Gateway System SD card that has been installed in the control unit. A default configuration is then created that matches the cards installed in the control unit and external expansion modules attached.

You can perform the following tasks prior to installing the B5800 Branch Gateway System SD card in order to pre-configure the system.

- See Upgrade the Card Firmware on page 50
- See Creating a configuration file on page 51.
- See Adding a configuration file on page 52.
- See Adding music-on-hold files on page 52.
- See Add a 9600 Screen Saver Image File on page 53.

For more information about SD cards, see SD Card Management on page 253.

Upgrading the card firmware

About this task

This process creates the folder structure on the SD card and copies the firmware files from those installed with Manager onto the SD card. This includes the binary files for the B5800 Branch Gateway system and any external expansion modules and phones. It also includes the prompt files for embedded voicemail operation.

This process can be used to upgrade an existing SD card to match the file set installed with Manager. The card installed in the System SD slot must be an Avaya SD Feature Key card. The card must be correctly formatted.

If the card contains any dynamic system files, for example SMDR records, they are temporarily backed up by Manager and then restored after the card is recreated.

Procedure

1. Insert the SD card into a card reader on the Manager PC.

   Note:
   Do not remove the SD card. Removing the SD card will interrupt the upgrade.
2. Using Manager, select **File** > **Advanced** > **Recreate IP Office SD Card**.
3. Select **Avaya Branch Gateway**.
4. Browse to the card location and click **OK**.
   Manager starts creating folders on the SD card and copying the required files into those folders. This process takes approximately 15 minutes. Do not remove the SD card until the Manager status bar at the bottom shows a **Ready** message.

Creating a configuration file

About this task

Manager can be used to create a new configuration file without connecting to a B5800 Branch Gateway system. This allows the creation of a configuration prior to installing the system. The configuration file can be loaded on the System SD card before the card is installed. The configuration file specifies the system's location, trunk cards, control unit, and expansion modules.

- The configuration created must match the physical equipment in the B5800 Branch Gateway system for which the configuration will be loaded. If they do not match, the system may reset and experience other problems.
- The configuration creation tool includes all control units, external expansion modules and trunk cards supported by B5800 Branch Gateway. It is your responsibility to confirm the B5800 Branch Gateway equipment that is supported in your location.

Procedure

1. Start Manager with no configuration loaded into Manager.
2. Click on **Create an Offline Configuration** in the simplified view.
3. Select the type of configuration that you want to create.
4. When completed, click **OK**.
   Manager will create and load the configuration.
5. Edit the configuration to match the customer requirements.
   This can include importing information from prepared CSV files.

Note:

For information about CSV files, see the Help available in the Manager application. From Manager, select **Help > Contents**. In the Manager Help window, in the left navigation pane, expand **IP Office Configuration Mode** and then expand **Editing Configuration Settings**. Then click **Importing and Exporting Settings**.

6. When completed, select **File** > **Save Configuration As**.

Adding a configuration file

About this task

Use this procedure to add a configuration file on the System SD card. That configuration file will then be used when the B5800 Branch Gateway system is started.

Procedure

1. Create an offline configuration that matches the customer requirements and the equipment that will be installed in the B5800 Branch Gateway system. See Creating a configuration file on page 51.
2. Rename the configuration file **config.cfg**.
3. Using a card reader, copy the file into the **/system/primary** folder on the System SD memory card.

Adding music-on-hold files

About this task

By default B5800 Branch Gateway uses internal music-on-hold by uploading a music file. You can load a file onto the System SD card prior to installing it in the control unit

The file must be of the following format and must be called **holdmusic.wav**.

Property	Value
File Type	WAV
Bit Rate	128kbps
Audio sample size	16 bit
Channels	1 (mono)
Audio Sample Rate	8 kHz

Property	Value
Audio Format	PCM
Length	Up to 90 seconds.

Procedure

1. Rename the music file **holdmusic.wav**.
2. Using a card reader, copy the file into the **/system/primary** folder on the System SD memory card.
3. If the B5800 Branch Gateway system is configured for additional music-on-hold files (up to 3 additional files), copy those files to the same location.

   The name of the additional files must match those specified in the B5800 Branch Gateway system configuration.

9600 series phones screen saver file

When idle, 9600 Series phones can timeout and display a screen saver image. A file, **96xxiposs.jpg**, is present on the cards by default.

You can replace this file with your own branded file. The file should be smaller than the screen size on 9600 Series phones in order for the image to move around the screen.

Base and trunk card installation

The base cards and trunk daughter cards should be fitted before power is applied to the control unit. Ensure that cards are inserted in the order that matches the planned or pre-built configuration. In general, the following applies to card installation:

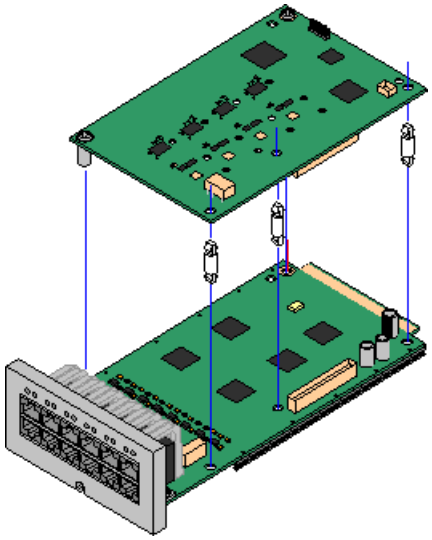
- Cards can be fitted in any order into any available slots. The only exception is the 4-port expansion card which can only be installed in right-hand slot 4.
- It is recommended that cards are fitted from left to right.
- There are restrictions to the number of supported cards of some types. When a limit is exceed, the right-most card of that type will not function.
- Ensure that you use the labels supplied to identify the card fitted into the control unit.

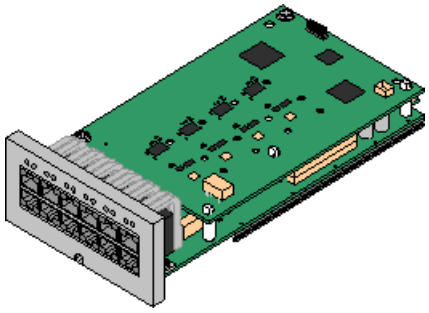
Warning:

- Correct anti-static protection steps should be taken before handling circuit boards.
- Cards must never be added or removed from the control unit while it has power connected.

Trunk daughter card preparation

Trunk daughter cards can be fitted to any base card except the legacy card carrier. For combination cards, the trunk daughter card is pre-installed and cannot be changed.





Warning:

Correct anti-static protection steps should be taken while handling circuit boards.

Parts and equipment required

- Base card (except the legacy card carrier)
- Trunk daughter card
- 3 stand-off pillars (these are supplied with the trunk daughter card)

Tools required

- 5mm Flat-blade screwdriver
- Anti-static wrist strap and ground point

Installing a trunk daughter card

Procedure

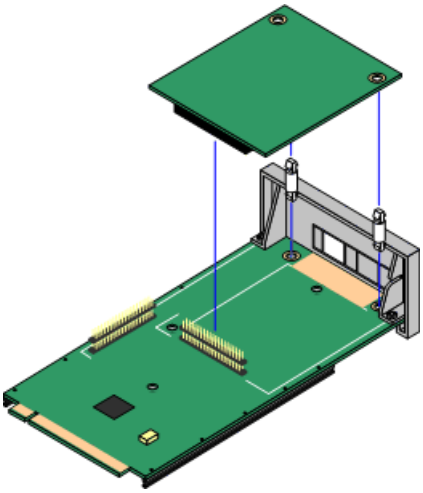
1. Check that correct cards have been supplied.
2. Ensure that you are wearing an anti-static wrist strap connected to a suitable ground point.
3. On the base card, identify the position of the 3 holes for the plastic pillars for the trunk daughter card.

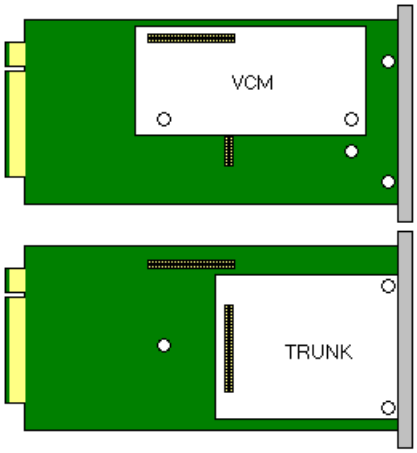
   These are along the same edge as the card connector.
4. Fit the stand-off pillars to the base card.
5. If there is a clip-on metal shield over the connector block on the base card, remove it.
6. Using minimal force and checking that the pins are correctly located, push the trunk card onto its connector block and the stand-off pillars.
7. Check that the card connector has snapped into position.
8. Using the washers and screws provided, secure the metal stand-off pillars to the base card.
9. From the set of labels that are supplied with the trunk daughter card, fit the appropriate label to the front of the base card.

Legacy carrier card preparation

A legacy carrier card can be used to fit VCM cards into the B5800 Branch Gateway control unit. Up to 2 legacy carrier cards can be inserted. The following trunk and VCM cards are supported. Cards not listed are not supported.

• PRI T1 • Dual PRI T1 • PRI 30 E1 (1.4) • Dual PRI E1	• PRI 30 E1R2 RJ45 • Dual PRI E1R2 RJ45 • BRI-8 (UNI) • ANLG 4 UNI (US only)	• VCM 4 • VCM 8 • VCM 16 • VCM 24 • VCM 30





Warning:

Correct anti-static protection steps should be taken while handling circuit boards.

Parts and equipment required

- Legacy carrier card
- VCM card

- 2 plastic stand-off pillars per card
- Trunk cards are supplied with a replacement blanking plate which is not required.

Tools required

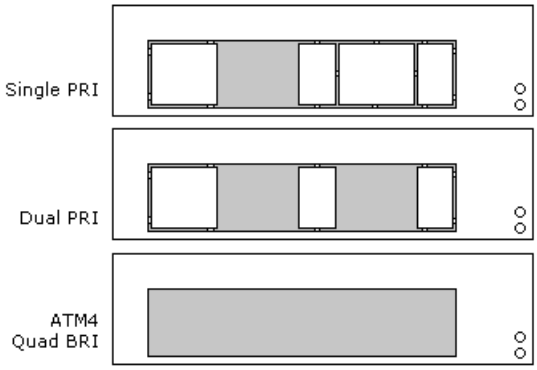
- 5mm Flat-blade screwdriver
- Anti-static wrist strap and ground point

Installing a legacy carrier card

Procedure

1. Check that correct cards have been supplied.
2. Ensure that you are wearing an anti-static wrist strap connected to a suitable ground point.
3. On the carrier card identify the position of the jumper block and stand-off pillar holes for the IP400 card.

   The peg holes are labeled as VCM or TRUNK.
4. If fitting an IP400 trunk card, identify which of the plastic snap-off panels on the front of the carrier card need to be removed to allow the trunk cable connections.



5. Carefully remove those panels.
6. Fit the stand-off pillars to the legacy carrier card.
7. Using minimal force and checking that the pins are correctly located, push the IP400 card onto its jumper and the stand-off pillars.

Base card insertion

Having prepared each base card by adding the trunk daughter cards or legacy carrier cards, the base card can be inserted into the control unit.

Warning:

- Correct anti-static protection steps should be taken before handling circuit boards.
- Cards must never be added or removed from the control unit while it has power connected.

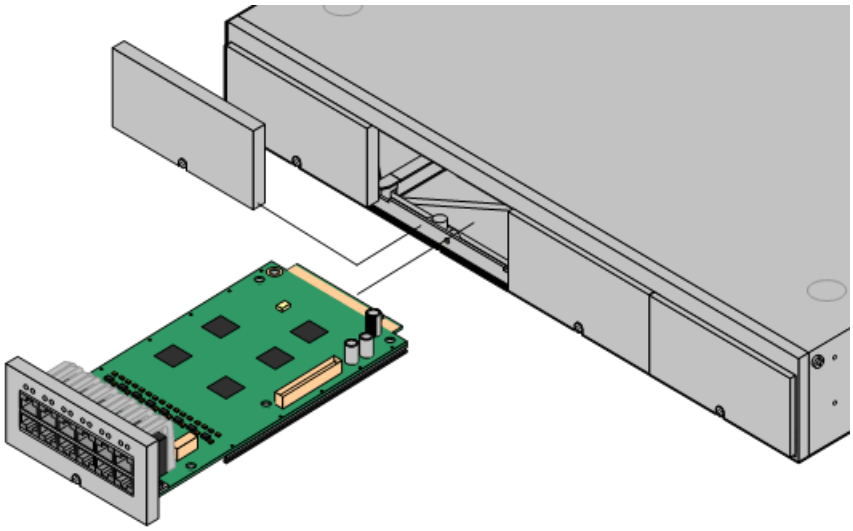
- **Tools required**
  - 5mm Flat-blade screwdriver
  - Anti-static wrist strap and ground point

Installing a base card

Procedure

1. Check that there is no power to the control unit.
2. Using a flat-bladed screwdriver, remove the cover from the slot on the front of the control unit that will be used for each card being installed.

   This cover is no longer required but should be retained until installation has been completed.



3. Allowing the card to rest against the bottom of the slot, begin sliding it into the control unit.
4. When half inserted, check that the card rails have engaged with the slot edges by trying to gently rotate it. If the card rotates, remove it and begin inserting it again.

   The card should slide in freely until almost fully inserted.

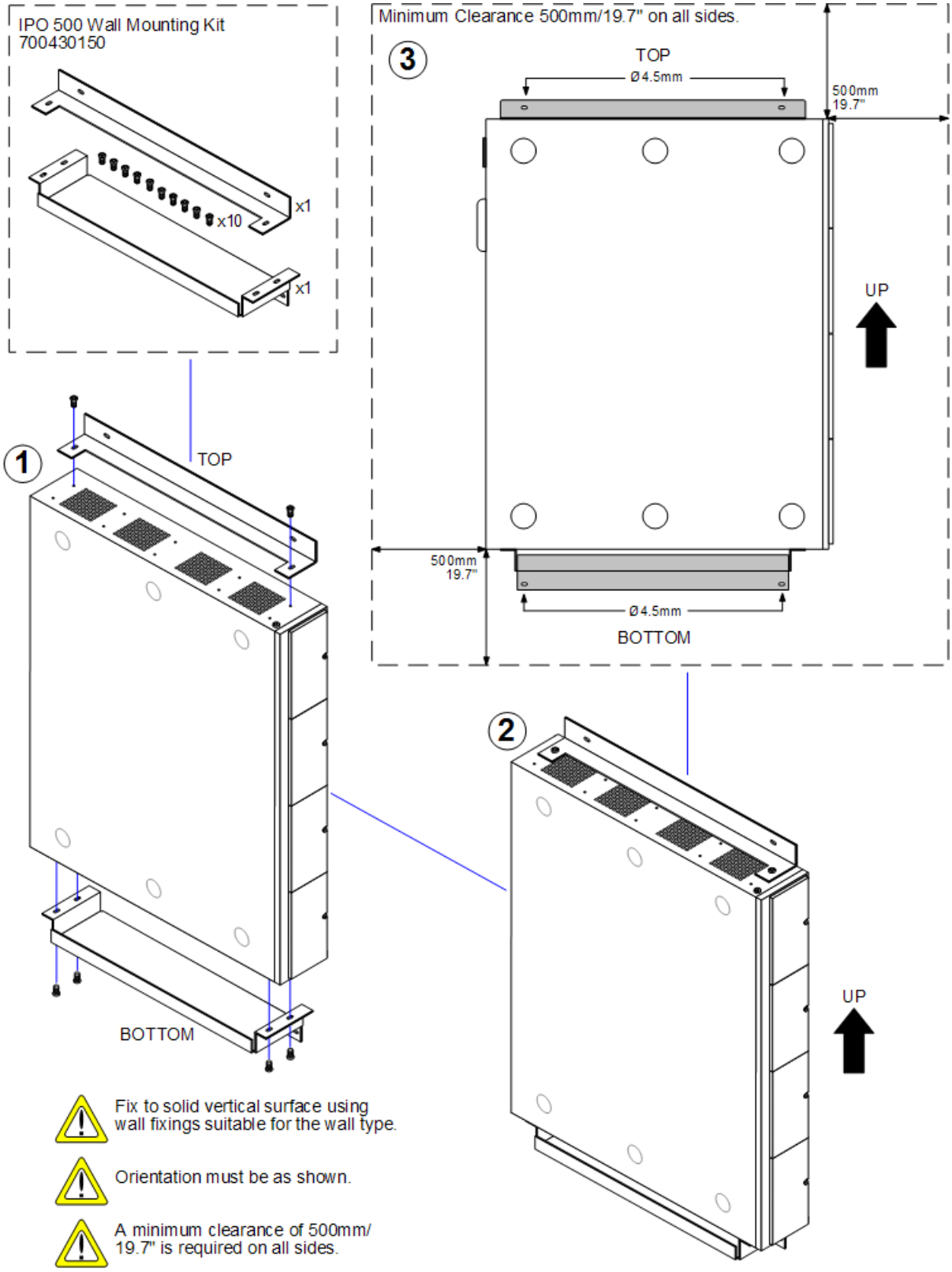
5. At this point apply pressure at the base of the front of the card to complete insertion.
6. Using a flat-bladed screwdriver secure the card.

Wall mounting

B5800 Branch Gateway control units can be wall mounted. This requires a wall mounting kit plus additional 4.5mm fixtures and fittings suitable for the wall type. The wall mounting kit includes two brackets, one top and one bottom.

In addition to the existing environmental requirements on page 41, the following requirements apply when wall mounting a unit:

- The wall surface must be vertical, flat and vibration free.
- The brackets must be used as shown, with the deeper tray-like bracket used at the bottom of the wall mounted control unit.
- Only the screws (M3 x 6mm) provided with the mounting kit should be used to attach the brackets to the control unit.


IPO 500 Wall Mounting Kit
700430150
x1
x10
x1
Minimum Clearance 500mm/19.7" on all sides.
3
TOP
Ø4.5mm
500mm
19.7"
UP
500mm
19.7"
Ø4.5mm
BOTTOM
1
TOP
BOTTOM
2
UP
Fix to solid vertical surface using wall fixings suitable for the wall type.
Orientation must be as shown.
A minimum clearance of 500mm/ 19.7" is required on all sides.

Rack mounting

The B5800 Branch Gateway control unit and external expansion units can be rack mounted into 19-inch rack systems. This requires a rack mounting kit for each unit.

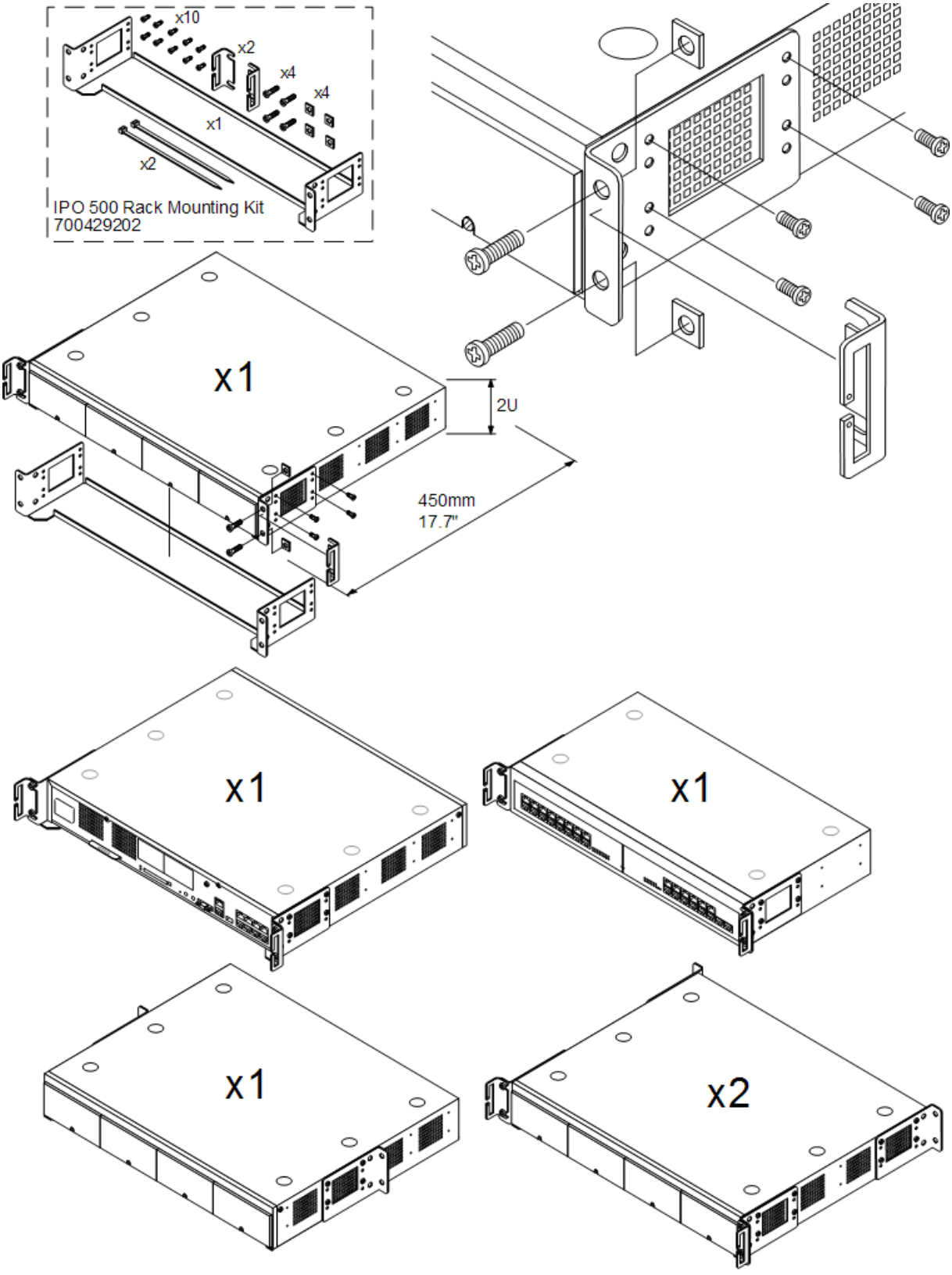
The rack mounting kit includes:

- A rack mounting bracket and screws for attachment of the bracket to the unit
- Nuts and bolts for rack attachment
- Brackets and cable ties for cable tidying

Environmental requirements

In addition to the environmental requirements on page 41, the following factors must be considered when rack mounting a unit:

- Rack positioning — Ensure compliance with the rack manufacturers safety instructions. For example check that the rack legs have been lowered and fixing brackets have been used to stop toppling.
- Elevated operating ambient — If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
    - Operating temperature: 0°C (32°F) to 40°C (104°F).
    - Operating humidity: 10% to 95% non-condensing.
- Reduced air flow — Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. Proper ventilation must be maintained. The side ventilation slots on the control unit should not be covered or blocked.
- Mechanical loading — Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit overloading — Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable earthing — Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).



- **Important:**

  Only the screws (M3 x 6mm) provided with the mounting kit should used to attach the

brackets to the control unit. As indicated in the diagram, the rack mounting bracket can be used in several positions on the unit.

External expansion modules

External expansion modules should be connected to the control unit before power is applied to the control unit. Ensure that modules are attached in the order that matches the planned or pre-built configuration.

External expansion modules connect to the control unit using an expansion interconnect cable. Each module is supplied with an expansion interconnect cable and a power supply unit. An appropriate local specific power cord for the power supply unit must be ordered separately.

- Each external expansion module is supplied with a blue 1 meter (3'3") expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on a 4-port expansion card, a yellow 2-meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. Four yellow cables are supplied with the 4-port expansion card.

Installation requirements

- Installation space either on or under the control unit
- Switched power outlet socket
- Available EXPANSION port on the control unit
- Functional grounding requirements — connection of a functional ground is:
    - recommend for all modules
    - mandatory for analog trunk modules
- Protective grounding requirements — connection of a protective ground via surge protection equipment is:
    - mandatory for analog trunk modules in the Republic of South Africa
    - mandatory for digital station and phone modules connected to out-of-building extensions
    - mandatory for digital station V2 and phone V2 modules

Tools required

- Manager PC
- Tools for rack mounting (optional)

Parts and equipment required

- External expansion module — each module is supplied with a suitable external power supply unit and a 1m blue interconnect cable. 2m yellow interconnect cables are supplied with the 4-Port expansion card and should only be used with that card.
- Power cord for the power supply unit
- Rack mounting kit (optional)
- Cable labeling tags

Connecting external expansion modules

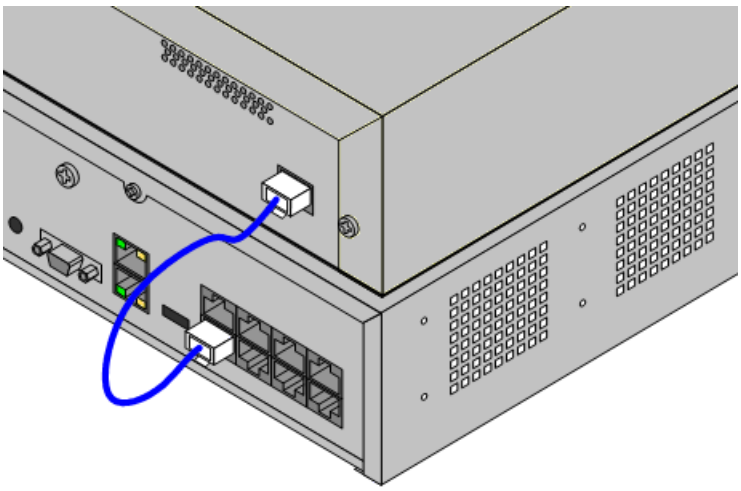
About this task

Note:

External expansion modules should not be attached to a control unit that has power.

Procedure

1. If the system is being installed in a rack, attach the rack mounting kit to the expansion module. See Rack mounting on page 61.
2. Attach the external expansion module's power supply but do not switch power on.
3. Connect the expansion interconnect cable from the module's EXPANSION port to the EXPANSION port on the control unit. Make careful note of the port used and include this detail on the cable label and any other system records.



Grounding

Use of ground connections reduces the likelihood of problems in most telephony and data systems. This is especially important in buildings where multiple items of equipment are interconnected using long cable runs, for example phone and data networks.

All control units and external expansion modules must be connected to a functional ground. Where the unit is connected to a power outlet using a power cord with an earth lead, the power outlet must be connected to a protective earth.

In some cases, such as ground start trunks, in addition to being a protective measure this is a functional requirement for the equipment to operate. In other cases it may be a locale regulatory requirement and or a necessary protective step, for example areas of high lightning risk.

Warning:

During installation do not assume that ground points are correctly connected to ground. Test ground points before relying on them to ground connected equipment.

Additional protective equipment

In addition to grounding, additional protective equipment is required in the following situations.

- On any digital station or phones external expansion module connected to an extension located in another building. See Out of Building Telephone Installations on page 66.
- In the Republic of South Africa, on all analog trunk external expansion modules (ATM16) and on any control units containing an analog trunk cards (ATM4/ATM4U).

Tools required

- M4 cross-head screwdriver
- Tools suitable for crimping a cable spade

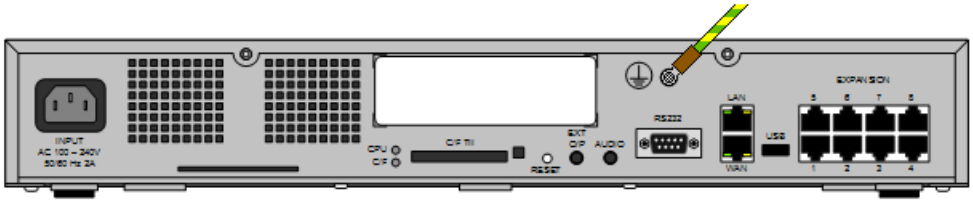
Parts and equipment required

- 14AWG solid copper wire for ground connection
- Cable sleeve matching local regulator requirements. Typically green for a functional ground and green/yellow for a protective ground.

The ground point on control units and expansion modules are marked with a ⏚ or ⏚ symbol. Ground connections to these points should use a 14 AWG solid wire with either a green sleeve for a functional ground or green and yellow sleeve for a protective ground.

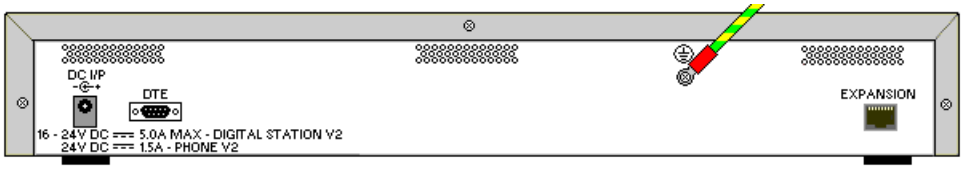
B5800 Branch Gateway control unit

On control units the ground point is located above the RS232 DTE port.



External expansion modules

On expansion modules, the ground point is a 4mm screw located towards the right on the rear of the module.



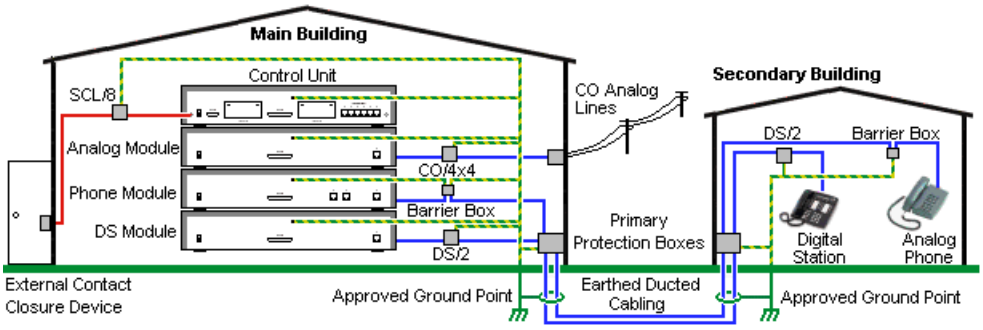
On some older modules, the dedicated ground point screw is not present. In those cases, the top-center cover fixing screw (3mm) can be used as an alternative ground connection point. A toothed washer should be added to ensure good contact.

Out-of-building connections/lightning protection

The following are the only supported scenarios in which wired extensions and devices outside the main building can be connected to the B5800 Branch Gateway system. In these scenarios, additional protection in the form of protective grounding and surge protectors must be fitted.

Warning:

The fitting of additional protection does not remove the risk of damage. It merely reduces the chances of damage.



- Cables of different types, for example trunk lines, phone extensions, ground and power connections, should be kept separate.
- All cabling between buildings should be enclosed in grounded ducting. Ideally this ducting should be buried.
- A Primary Protection Box must be provided at the point where the cables enter the building. This should be three point protection (tip, ring and ground). Typically this would be gas tube protection provided by the local telephone company. The ground wire must be thick enough to handle all the lines being affected by indirect strike at the same time.

Connection type	Protection device type	Requirement
DS phone extensions External expansion module DS ports only.	**ITWLinx towerMAX DS/2** Supports up to 4 connections. (This device was previously referred to as the Avaya 146E.)	• Connection from the expansion module to the phone must be via a surge protector at each end and via the primary protection point in each building. • The expansion module, control unit, and IROB devices must be connected to the protective ground point in their building. • The between building connection must be via earthed ducting, preferable underground. The cable must not be exposed externally at any point.
Analog phone extensions Phones external expansion module (POT or Phone) ports only.	**Barrier box** Supports a single connection. Maximum of 16 on any expansion module.	
Analog trunks	**ITWLinx towerMAX CO/4x4** Supports up to 4 two-wire lines. (This device was previously referred to as the Avaya 146C.)	For installations in the Republic of South Africa, the fitting of surge protection on analog trunks is a requirement. For other locations where the risk of lightning strikes is felt to be high, additional protection of incoming analog trunks is recommended.

Connection type	Protection device type	Requirement
External output switch	**ITWLinx towerMAX SCL/8** (This device was previously referred to as the Avaya 146G.)	Connections from an Ext O/P port to an external relay device must be via a surge protector.

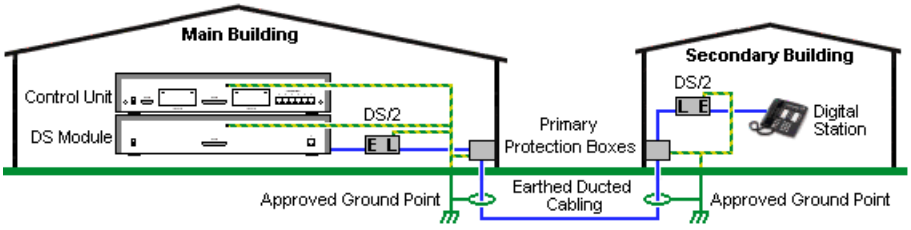
The towerMAX range of devices are supplied by ITWLinx (http://www.itwlinx.com).

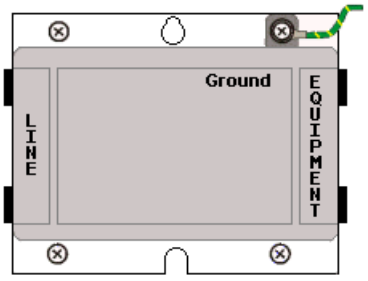
DS phone IROB installation

When digital phone extensions are required in another building, additional In-Range Out-Of-Building (IROB) protective equipment must be used. For phones connected to B5800 Branch Gateway DS ports, the supported device supplied by ITWLinx is a towerMAX DS/2 module. This IROB device was previously referred to by Avaya as the 146E IROB.

The protection device should be installed as per the instructions supplied with the device. The ground points on the control unit and the DS modules must be connected to a protective ground using 18AWG wire with a green and yellow sleeve.

Typically the IROBs 2 RJ45 EQUIPMENT ports are straight through connected to the 2 RJ45 LINE ports. This allows existing RJ45 structured cabling, using pins 4 and 5, to be used without rewiring for up to two DS connections. However each of these ports can be used to connect a second extension using pins 3 and 6.



LINE		Signal		EQUIPMENT	
RJ45 8 1	1	Not used		1	RJ45 8 1
	2	Not used		2	
	3	Ring II (Optional)		3	
	4	Ring I		4	
	5	Tip I		5	
	6	Tip II (Optional)		6	
	7	Not used		7	
	8	Not used		8	

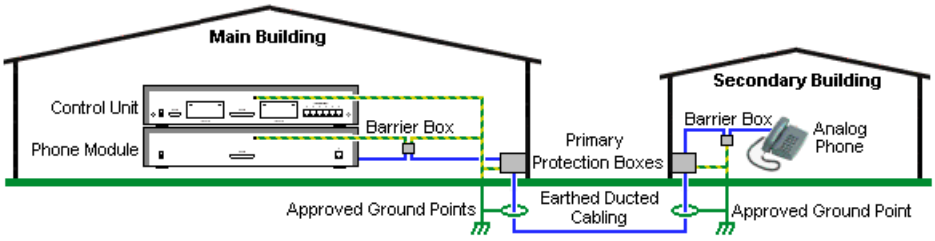
Analog phone barrier boxes

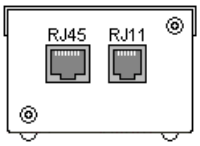
Where analog phone extensions are required in another building, phone barrier boxes and protective earth connections must be used .

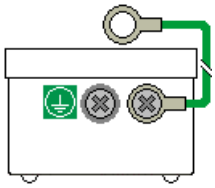
Warning:

PHONE (POT) ports on the front of control units must not be used for extensions that are external to the main building.

- The correct B5800 Branch Gateway barrier boxes must be used. These modules have been designed specifically for the signalling voltages used by the B5800 Branch Gateway system:
  - Only the B5800 Branch Gateway phone barrier box should be used with phone V1 modules.
  - Only the B5800 Branch Gateway phone barrier box V2 should be used with phone V2 modules.
  - No other type of analog phone barrier box should be used.
  - Where more than 3 barrier boxes are required in a building, they must be rack mounted using a barrier box rack mounting kit. See Rack mounting barrier boxes on page 70.
  - A maximum of 16 barrier boxes can be used with any phone module.
  - The phone barrier box does not connect the ringing capacitor in phone V1 modules.



Main Building	Barrier Box	Secondary Building
• **RJ11** — Connect to PHONE (POT) port on the Phone module using cable supplied with the barrier box. • **RJ45** — Connect to the secondary building barrier box via primary protection in both buildings.		• **RJ11** — Connect to analog phone. Cable not supplied. • **RJ45** — From main building via primary protection in both buildings.

Main Building	Barrier Box	Secondary Building
• **Center screw** — Connect to main building protective ground (or ground terminal of Barrier Box Rack Mounting Kit). Use 18AWG (minimum) wire with a green and yellow sleeve. • **Right-hand screw** — Connect to ground point on Phone module using ground cable supplied with barrier box.		• **Center screw** — Connect to main building protective ground. Use 18AWG (minimum) wire with a green and yellow sleeve. • **Right-hand screw** — Not used.

The following wires must be kept apart, that is, the wires cannot be routed in the same bundle:

- Earth leads from the barrier box to the phone modules.
- Internal wires, for example extension leads going directly to the phone modules.
- Wires from external telephone going directly to the barrier boxes.

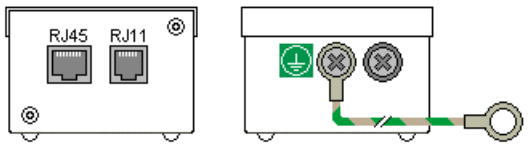
Rack mounting barrier boxes

About this task

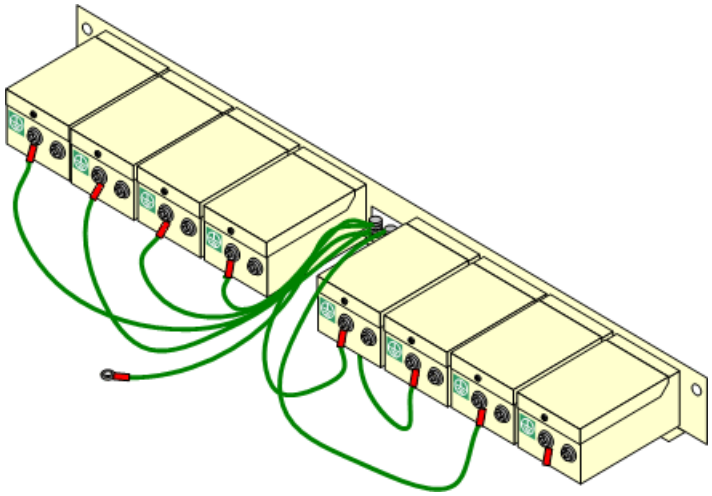
Where more than 3 phone barrier boxes are used they must be rack mounted. The Barrier Box Rack Mounting Kit (SAP Code 700293905) supports up to 8 phone barrier boxes.

Procedure

1. Unscrew the two screws arranged diagonally at the front of each barrier box and use these same screws to reattach the barrier box to the rack mounting strip.
2. Each barrier box is supplied with a solid green ground wire connected to its functional ground screw. Remove and discard this wire.
3. Connect a green/yellow ground wire to the protective earth screw in the center of the point on the back of the barrier box.



4. The rack mounting strip has threaded M4 earthing pillars. Connect the other end of the barrier box ground wire, using M4 washers and nuts, to the earthing pillar on that side of the rack mounting strip.



5. Using 14AWG wire with green and yellow sleeve, connect one of the earthing pillars to the buildings protective earth.
6. Using 14AWG wire with green and yellow sleeve, connect the other earthing pillar to the phone module.
7. Ensure that the following wires are not routed together in the same bundle:
    - Earth lead from the barrier box to the phone module.
    - Internal wires, e.g. wires going directly to the phone module.
    - Wires from external telephone going directly to the barrier boxes.

Administration software suite

The B5800 Branch Gateway administration software applications are installed on the installation PC. They are used by installers and maintainers to configure, manage, and monitor the B5800 Branch Gateway system.

The B5800 Branch Gateway administration applications are:

- **Manager**

  B5800 Branch Gateway Manager is used to access all parts of the B5800 Branch Gateway configuration. Different levels of access can be defined to control which parts of the configuration the Manager user can view and alter. Manager is also used to upgrade the system software files.

- **System Status**

  The B5800 Branch Gateway System Status application is a monitoring and reporting tool that provides a wide range of information about the current status of the system. It can report the available resources and components within the system and details of calls in

progress. Details of the number of alarms are recorded and the time and date of the most recent alarms.

- **System Monitor**

  The B5800 Branch Gateway System Monitor application is a tool that shows details of all activity on the B5800 Branch Gateway system. Because of the level of detail, interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. Installers and maintainers must understand how to run System Monitor when necessary as Avaya may request copies of System Monitor traces to resolve support issues.

PC requirements

The minimum Microsoft® Windows® PC requirements for the B5800 Branch Gateway system tools are provided in the following table. If other applications are to be installed on the PC then those individual requirements should also be met.

Requirement	Minimum	Recommended
Processor	600MHz Pentium or AMD Opteron, AMD Athlon64, AMD Athlon XP.	800MHz Pentium or AMD Opteron, AMD Athlon64, AMD Athlon XP.
RAM	128MB	256MB
HD Space	1GB - 800MB for .NET2, 200MB for Manager.	1.4GB - 800MB for .NET2, 600MB for the full B5800 Branch Gateway Admin suite.
Display	800 x 600 - 256 Colors	1024 x 768 - 16-bit High Color
Operating System	Supported on Windows® XP Pro, Windows® Vista, Windows® 7, Windows® 2003 and Windows® 2008. • 32-bit and 64-bit versions are supported. • Vista support is only on Business, Enterprise and Ultimate versions. • Windows 7 support is only on Professional, Enterprise and Ultimate versions.	

Installing the administration applications

Procedure

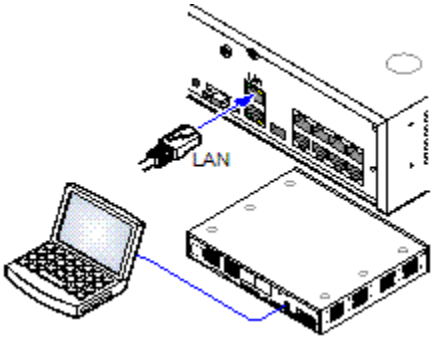
1. Insert the B5800 Branch Gateway Administrator Applications DVD.

2. Select B5800 Branch Gateway Administration Suite.
3. Double-click on **setup.exe**.
4. Select the language you want to use for the installation process.
   This does not affect the language used by Manager when running.
5. Click **Next**.
6. Select who should be able to run the Administration Suite applications.
7. Click **Next**.
8. If required, select the destination to which the applications should be installed.
   It is recommended that you accept the default destination.
9. Click **Next**.
   The Custom Setup window appears.
10. Select the applications that you want to install. At a minimum select **System Monitor** and **Manager**.
    When you select an application, a description of the application appears. Click on the ▾ next to each application to change the installation selection.
11. Click **Next**.
12. Click **Install**.
    Installation of Windows .Net2 components may be required. If dialogs for this appear, follow the prompts to install .Net.
13. If requested, reboot the PC.

Installer PC connection

During installation it is recommended that the B5800 Branch Gateway control unit be started without it being connected to any network. That ensures that the B5800 Branch Gateway defaults to a known set of IP address settings.

The B5800 Branch Gateway control unit is connected to the PC with a standard RJ45–RJ45 LAN cable.



Connecting the PC directly to the control unit

About this task

The default address for a B5800 Branch Gateway control unit LAN port is 192.168.42.1/255.255.255.0. Use this procedure to change the TCP/IP properties for the LAN port on the PC and directly connect the PC to the control unit.

Procedure

1. Change the TCP/IP properties of the LAN port on the PC to the following:
   - Fixed IP address: 192.168.42.203
   - Subnet mask: 255.255.255.0
   - Default gateway: 192.168.42.1

   Note:
   While setting the PC to be a DHCP client could be used, this is not recommended for performing more advanced functions such as firmware upgrades.
2. Connect the LAN cable from the PC LAN port to the LAN or LAN1 port on the control unit.
3. Check that the orange LED lamp on the control unit LAN port is on.

   The green LED may also be flickering. This indicates traffic across the LAN connection.
4. To test the connection before running Manager or the System Status application, do the following:
   a) Select **Start** > **Run**.
   b) Enter `cmd`.
   c) In the command window that appears, enter `ping 192.168.42.1`.

      The results should show a number of ping replies from the B5800 Branch Gateway . This confirms basic communication between the Manager PC and the B5800 Branch Gateway .

d) If there are no ping replies, enter `ipconfig`.

The results should list the IP address settings of the Manager PC as required above.

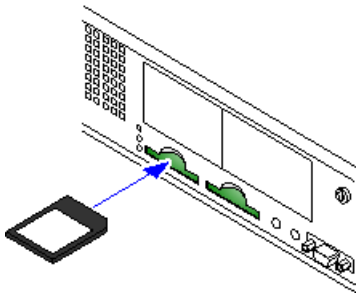
e) If the IP address settings of the Manager PC are displayed, enter `exit` and check the cable connection.

Applying power to the system

Procedure

1. With the power off on the control unit, insert the B5800 Branch Gateway System SD card into the **System SD** slot on the rear of the control unit.

   Ensure that you have the correct card. The B5800 Branch Gateway System SD card is required for branch operation. The card is labeled **System SD BRANCH GW**.



2. Apply power to the external expansion modules.

   The power outlet used must include a switch and in cases where the power cord includes an earth lead, that outlet must have a protective earth connection.

3. Apply power to the control unit.

   The power outlet used must include a switch and the power outlet must have a protective earth connection.

   When power is applied to the control unit, the following occurs:

   - The control unit begins loading firmware from the System SD card with which it will upgrade itself and the components installed in the control unit. This process takes approximately a minute. The end of this process is indicated by LED1 on each base card flashing every 5 seconds and LED9 on each base card fitted with a trunk daughter card flashing every 5 seconds.
   - The control unit will then begin upgrading the external expansion modules. This is indicated by the red center LED on each module flashing red. The process is completed when the LED changes to steady green.

- If a configuration file is already present on the System SD card, it is loaded by the B5800 Branch Gateway. If not, the B5800 Branch Gateway creates a default configuration based on the components of the system and copies that configuration onto the System SD card.

You are now able to use Manager to access the B5800 Branch Gateway configuration.

Control unit LEDs startup sequence

The LEDs on the rear of the control unit go through the following sequence during a normal start up. Note that the times are approximate only.

LED	4s	4s	12s	5s	2s	5s	5s	10s	10s	Finished
CPU	Orng	Grn	Grn	Grn Red	Grn	Grn	Grn	Grn	Grn	Grn
System SD	Orng	Off	Grn	Grn	Grn	Off	Grn	Grn	Grn Flash	Grn
Optional SD (if present)	Orng	Off	Grn	Grn	Grn	Off	Off	Grn	Grn	Grn

Orng = Orange Grn = Green

On the front of the control unit, LED1 on any IP500 base cards fitted is used as follows. LED9 is also used for any trunk daughter cards fitted.

LED	30s	30s	Finished
Optional SD	Red	Red	Red
		Fast Flash	Flash every 5 seconds

About the LEDs

Control unit LEDs

LED	Description
Optional SD	• Off = card shutdown

LED	Description
System SD	• Green on = card present • Green flashing = card in use • Orange steady = reset imminent • Red flashing = card initializing or shutting down • Red fast flashing = card full • Red steady = card failure/wrong type
CPU	• Alternate red/green = starting up • Green on = okay • Red on = no software • Flashing Red = error/shutdown

Base card LEDs

Base Card	LEDs 1 to 8 Usage
All cards	LED1 is used for base card status: • Red on = error • Red slow flash = initializing • Red flash every 5 seconds = card okay • Red fast flash = system shutdown
Analog phone	No status LEDs are used for analog phone extensions.
Digital station	Green on = phone detected
VCM	LEDs 1 to 8 are unlabelled. They are used to indicate voice compression channel usage. Each LED lit represents 12.5% of the available voice compression channel capacity in use (total card capacity rather than licensed capacity).
4-port expansion	LEDs 1 to 8 are used for the expansion ports on the rear of the control unit. LEDs 9 to 12 are used for the card's own expansion ports. • Green on = expansion module present • Red flashing = initializing • Red on = error • Orange regular flash = base card okay
Combination	LEDs 1 to 6 Green on = phone detected

Trunk daughter card LEDs

Trunk Daughter Card	LEDs 9 to 12 Usage
All cards	LED 9 is used for daughter card status: • Red on = error • Red slow flash = initializing • Red flash every 5 seconds = card okay • Red fast flash = system shutdown
Analog trunk	• Green on =card fitted • Green flashing = trunk in use
BRI trunk	• Off = no trunk present • Green on = trunk present • Green flashing = trunk in use
PRI trunk	• Off = no trunk present • Green on = trunk present • Green flashing = trunk in use • Red/green fast flash (port 9) or greenfast flash (port 10) = alarm indication signal (AIS) from the trunk remote end • Red with green blink (port 9) or green blink (port 10): port in loopback mode (set through System Monitor)

External expansion module LEDs

External expansion module	
All modules	• Green on = module okay • Red flashing = module starting up • Red on = error

Starting Manager

About this task

B5800 Branch Gateway Manager is used to access all parts of the B5800 Branch Gateway configuration. Different levels of access can be defined to control which parts of the

configuration the Manager user can view and alter. Manager is also used to upgrade the system software files.

Procedure

1. Select **Start** > **Programs** > **IP Office** > **Manager**.
   If the PC has firewall software installed, you may be prompted as to whether you want to allow this program to access the network.
2. If a prompt appears requesting permission to allow this program to access the network, select **Yes** or **OK**.
3. From the menu bar, select **File** > **Open Configuration**.
   The Select IP Office window appears. After a few seconds, the control unit should be listed. The default name used for a newly installed control unit is its MAC address. If the control unit is not found, the address used for the search can be changed.
4. If the control unit is not found, change the address for which to search as follows:
   a) In the **Unit/Broadcast Address** field, enter or select the required address.
   b) Click **Refresh** to perform a new search.
5. Click the check box next to the system and then click **OK**.
   The name and password request is displayed.
6. Enter the name and password.
   The name and password must match one of those setup through the security settings. The default name and password for full configuration settings access is **Administrator** and **Administrator**.

Default configuration

Unless you loaded a configuration file onto the System SD card, the B5800 Branch Gateway system will be configured with default settings when the system is started.

Following are the basic default configuration settings for a B5800 Branch Gateway system.

Network Settings	LAN1	LAN2/WAN
IP address	192.168.42.1	192.168.43.1
IP mask	255.255.255.0	255.255.255.0
DHCP mode	server	server
Number of DHCP IP addresses	200	200

- **Extensions and users** — A user is automatically created for each physical extension port detected in the system. Users are assigned extension numbers starting from 201. User names take the form Extn201, Extn202, etc.
- **Hunt group** — A single hunt group 200 called Main is created and the first 10 users are placed into that hunt group as members.
- **Incoming call routes** — Two default incoming call routes are created. Voice calls are routed to the hunt group Main. Data calls are routed to the RAS user DialIn.
- **Default short codes** — A-Law or U-Law variant operation is determined by the Feature Key installed in the control unit. Depending on the variant, different short codes and trunk settings are added to the default configuration.
- **A-Law or Mu-Law** — Pulse Code Modulation (PCM) is a method for encoding voice as data. In telephony, two methods of PCM encoding are widely used, A-law and Mu-law (also called U-law). Typically Mu-law is used in North America and a few other locations while A-law is used by the rest of the world. As well as setting the correct PCM encoding for the region, the A-Law or Mu-Law setting of a B5800 Branch Gateway system when it is first started affects a wide range of regional defaults relating to line settings and other values. The encoding default is set by the type of Feature Key installed when the system is first started.

Default DHCP/IP address settings

When a defaulted or new B5800 Branch Gateway control unit is switched on, it requests IP address information from a DHCP server on the network. This operation will occur whether the LAN cable is plugged in or not. The process below is done separately for both the LAN port (LAN1 in the configuration) and the WAN port (LAN2 in the configuration) on the back of the control unit.

- The B5800 Branch Gateway makes a DHCP request for what IP address information it should use.
- If a DHCP server responds within approximately 10 seconds, the control unit defaults to being a DHCP client and uses the IP address information supplied by the DHCP server.

  Note:

  For this installation, we have not yet connected the control unit to the network so a DHCP server will not respond.

- If a DHCP server does not respond, the control unit defaults to being the DHCP server for the LAN using the following settings:
  - For its LAN1 it allocates the IP address 192.168.42.1 and IP Mask 255.255.255.0. It supports 200 DHCP clients using the addresses range 192.168.42.2 and 192.168.42.201, the IP Mask 255.255.255.0 and default gateway address 192.168.42.1 (the control unit LAN1 address).
  - For its LAN2 if supported, it allocates the IP address 192.168.43.1 and IP Mask 255.255.255.0.
  - Note that the B5800 Branch Gateway does not check that these addresses are valid and or available on the network.

Important:

Once the control unit has obtained IP address and DHCP mode settings, it retains those settings even if rebooted without a configuration file present on the System SD card. To fully remove the existing IP address and DHCP mode setting the B5800 Branch Gateway must be defaulted using Manager.

Changing the IP address settings

About this task

Use this procedure to change the system name, IP address, IP mask, or DHCP settings of the B5800 Branch Gateway system. By default the B5800 Branch Gateway system name is set to match its MAC address. The system name can be changed to something more distinctive. For more information about the system default settings, see Default configuration on page 79. Note that if you change the IP address settings, you must restart the system.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. On the **System** tab, in the **Name** field, enter a distinctive name for this B5800 Branch Gateway system.
4. Click **OK**.
5. Click the **LAN1** tab.
6. On the **LAN Settings** sub-tab, do the following:
   a) Change the IP Address to match the customer requirements.
   b) Change IP Mask to match the customer requirements.
   c) Change DHCP Mode setting to match the customer requirements.

   These settings are used for the **LAN** port on the back of the control unit.
7. Click **OK**.
8. Click the **LAN2** tab.
9. On the **LAN Settings** sub-tab, do the following:
   a) Change the IP Address to match the customer requirements.
   b) Change IP Mask to match the customer requirements.
   c) Change DHCP Mode setting to match the customer requirements.

   These settings are used for the **WAN** port on the back of the control unit.
10. Click **OK**.
11. Select **File > Save Configuration**.

12. Reboot the system.

Connecting the control unit to the network

About this task

Once you have changed the B5800 Branch Gateway system default settings to those that match the customer requirements, you can connect the B5800 Branch Gateway control unit to the customer's network.

Procedure

1. Disconnect the LAN cable from the installer PC.
2. Connect the LAN cable to the customer network.
3. If you want to use the administration PC for on-going administration, connect the PC to the customer network.

Default passwords

Do not change any other settings than those described below until you have read and understood the Security Mode section of the IP Office Manager document. See Section 3.3 “The Security Mode Interface” in the IP Office Manager document for more information.

A B5800 Branch Gateway system's security settings can be set back to default if necessary. See “Resetting an IP Office's Security Settings” in Section 3.5 “Editing Security Settings” in the IP Office Manager document for more information.

Changing the security settings

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File** > **Advanced** > **Security Settings**.
3. In the Select IP Office window, click the check box for the appropriate system.
4. Click **OK**.

5. In the Security Service User Login window, enter a user name and password of an account that has security configuration access to the B5800 Branch Gateway system.

   The defaults are **security** and **securitypwd**.

6. In the left navigation pane, click **System**.
7. Click the **Unsecured Interfaces** tab.

   The password in the **System Password** field is used by Manager for remote software upgrade of the B5800 Branch Gateway system. The default password is **password**.

8. Next to the **System Password** field, click the **Change** button.
9. Enter a new password and click **OK**.
10. Click **OK**.
11. Click on **Service Users**.
    The list shows the service user accounts that can access the system configuration. The default service users Administrator, Manager and Operator each use the same value (Administrator, Manager and Operator) as their password.
12. For each of these service users:
    a) Click on the service user name.
    b) In the **Service User Details** tab, click on **Change** and enter a new password.
    c) Click **OK**.
    d) Click **OK**.
13. Click on **General**.

    The general security settings are displayed in the main display area.

14. Next to the **Password** field, click on **Change** and enter a new password for the security administrator.
15. Click on **File** > **Configuration** to exit security configuration mode and return to the B5800 Branch Gateway configuration.

Changing the remote user password

About this task

The B5800 Branch Gateway configuration contains a user whose password is used as the default for remote dial-in access to the B5800 Branch Gateway network. Use this procedure to change this user's password.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.

2. In the left navigation pane, click **User**.
3. In the user list, click **RemoteManager**.
4. On the **User** tab, do the following:
   a) In the Password field, enter a new password for the user.
   b) In the Confirm Password field, enter the new password again.
5. Click **OK**.
6. Select **File > Save Configuration**.

Connecting phones

Procedure

1. Connect the analog phones to the phone ports.
2. Ensure that the analog phones that are connected to power failure ports are clearly labeled as such.
3. Connect the Avaya digital phones to the appropriate DS ports.
   When the control unit is started, after loading its own firmware and the firmware for its external expansion modules, it will upload the appropriate firmware to the digital phones.

   Avaya H323 phones do not need to be connected at this stage. They will go through a firmware upgrade process when connected to an B5800 Branch Gateway system that is already running. Refer to the H323 IP Phone Installation Manual.

96x1 phones SIP firmware download in B5800 Branch Gateway centralized branch deployments

When Avaya SIP phones are deployed in the centralized branch deployment model, the primary method for phone firmware download is centralized as well. In this mode the phones get their settings file and firmware file from a central HTTP server.

However, if this method cannot be used, for example, due to WAN bandwidth concerns, an alternative method may be used leveraging the B5800 Branch Gateway located in the branch where the phones are located.

This section describes the process for 96x1 Series Phone SIP firmware download using the B5800 Branch Gateway. The procedure required to replace the H.323 version of the firmware to the SIP version is not covered here.

B5800 Branch Gateway support for SIP phone firmware download

This capability is made available in the B5800 Branch Gateway Release 6.1 SP2. Note that a hidden B5800 system configuration parameter (the B5800 NoUser Source Number 'ENABLE_SIP_FIRMWARE_DOWNLOAD') needs to be configured.

Enabling the DHCP server on the B5800 Branch Gateway

About this task

Before upgrading the phones, a DHCP server has to be set up to provide the correct HTTP server address to the phones. The preferred approach is for the DHCP server to be enabled on each B5800 Branch Gateway. Perform this procedure on each B5800 Branch Gateway.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway.
2. In the left navigation pane, click **System**.
3. Click the **LAN** tab.
4. In the **LAN Settings** tab, under **DHCP Mode**, click **Server**.
5. Click the **Advanced** button.
6. Click the **Apply to Avaya IP Phones only** check box to select this option.

About using external DHCP servers

As an alternative to enabling the DHCP server on each B5800 Branch Gateway, external DHCP servers can be used if preferred. In this case, the DHCP server must be configured to provide the IP address of each B5800 Branch Gateway as the HTTP server address in the Site-Specific Option of the DHCP response to the phone.

The SIP phone configuration file 46xxsettings.txt has to be edited and then loaded to the B5800 Branch Gateway. This should be done as part of installation and does not have to be repeated when upgrading to a new phone SIP firmware.

- SIP_CONTROLLER_LIST has to have the appropriate Avaya Aura® Session Manager IP address as a primary SIP server.
- See Survivability settings on page 198 for the settings file parameters that are relevant to B5800 Branch Gateway centralized branch deployment.
- HTTPSRVR IP address may have to be set to point to the B5800 Branch Gateway (if this is not what is already provided to the phone via DHCP).

The SIP phone firmware load of the required version has to be obtained. It comes as a zip file containing multiple files (tar, xml, txt).

Loading the SIP phone firmware to the B5800 Branch Gateway SD card

About this task

The SIP phone firmware must be loaded onto the B5800 Branch Gateway SD card. The entire content of the zip file should be copied to the B5800 Branch Gateway. In particular, be sure to load the phone upgrade file 96x1Supgrade.txt containing the correct name of the new firmware files.

Loading the files to the B5800 Branch Gateway can be done using B5800 Branch Gateway Manager, either locally in the branch or remotely where B5800 Branch Gateway Manager connects from the NOC to the different branches and loads the files to each branch at a time. The unzipped files have to be on the machine running B5800 Branch Gateway Manager.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway.
2. Select **File > Advanced > Embedded File Management**.
3. Copy the files onto the B5800 Branch Gateway SD card in the System/Primary folder.

Loading the SIP phone configuration file to the B5800 Branch Gateway SD card

About this task

The SIP phone configuration file (46xxsettings.txt) must be loaded onto the B5800 Branch Gateway SD card. Loading the files to the B5800 Branch Gateway can be done using B5800 Branch Gateway Manager. Note that this file does not have to be modified and loaded to the B5800 Branch Gateway again each time a new firmware for the SIP phone is available.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway.
2. Select **File > Advanced > Embedded File Management**.
3. Copy the configuration file onto the B5800 Branch Gateway SD card.

About rebooting the phones

The phones must be rebooted to start the firmware download from the B5800 Branch Gateway. You can reboot the phones remotely from the Avaya Aura® System Manager in the NOC or by power cycling the phones.

Rebooting the phones from Avaya Aura® System Manager

About this task

When upgrading from phones running firmware versions prior to R6.0 SP2, upgrade up to 10 phones in each branch at once. Once these phones finish, another set of up to 10 phones can be rebooted to start the upgrade. If more than 10 phones try to download their firmware from B5800 Branch Gateway at once, there is a risk that the download will not be successful on some of phones. If this occurs, the phones that failed to download successfully should be rebooted to try again.

When upgrading from phones running firmware versions R6.0 SP2 and later, simultaneous upgrade of groups of up to 50 phones is supported.

Note:

This procedure must be performed in sunny day conditions when the phones are registered to Session Manager.

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.
2. Select **System Status > User Registrations**.
3. Use the **Advanced Search Criteria** option to find the phones to be upgraded.

   Using the **Location** search criteria and specifying the branch location may provide a convenient way to display all phones in a given branch, assuming **Location** is administered in System Manager for all users. Alternatively, other criteria can be used, including choosing the **Address** search criteria and specifying the leading digits that are common to and unique to the users in that branch, or choosing the **IP Address** search criteria and specifying the subnet IP address of the branch

4. In the list of users that is displayed, select the check box (on the left of each row) for the users to be rebooted.

   Note:
   Multiple users can be selected by checking the boxes of multiple entries on the list. For best results of the firmware download process, check multiple (up to 10) users from the list to reboot them together in one action.

5. Click the **Reboot** button (located next to **AST Devices Notification** above the list of users).
   System Manager will notify Session Manager that will instruct each of the selected phones to reboot. After the reboot, the phone will get in DHCP the address of the local B5800 Branch Gateway in its branch as HTTP server, and will get its configuration files (upgrade and settings files) and then download its firmware file from the B5800 Branch Gateway. After the download completes successfully, the phone will automatically restart using the new firmware.

6. Confirm that the firmware upgraded correctly by choosing one of the following methods:

   - From the phone craft menu, do the following:

     1. Press the **Mute** button.
     2. Enter the password, `CRAFT# (27238#)`
     3. Scroll to the **View** option.

   - From the phone user menu, do the following:

     1. Select **Home > Network Information > IP Parameters**.
     2. Scroll right 4 pages.

   - Use a MIB browser to read the following two MIB items from the Avaya 96x1 SIP Phone MIB:

     - endptAPPINUSE
     - endptRFSINUSE

     The MIB items from the Avaya 96x1 SIP Phone MIB are on the Avaya support site at https://support.avaya.com/css/appmanager/css/support/Downloads/P0553/SIP%206.0.x/C2010 111895427550_1#files).

7. If the firmware download was not successful on a given phone, reboot the phone again.

Rebooting the phones by power cycling the phones

About this task

This procedure can be performed in sunny day or rainy day conditions. The phones do not need to be registered to Session Manager.

Procedure

To power cycle the phone, remove power to the phone, wait about one minute, then reapply power.

Chapter 5: Administration software suite

The B5800 Branch Gateway administration software applications are installed on the installation PC. They are used by installers and maintainers to configure, manage, and monitor the B5800 Branch Gateway system.

The B5800 Branch Gateway administration applications are:

- **Manager**

  B5800 Branch Gateway Manager is used to access all parts of the B5800 Branch Gateway configuration. Different levels of access can be defined to control which parts of the configuration the Manager user can view and alter. Manager is also used to upgrade the system software files.

- **System Status**

  The B5800 Branch Gateway System Status application is a monitoring and reporting tool that provides a wide range of information about the current status of the system. It can report the available resources and components within the system and details of calls in progress. Details of the number of alarms are recorded and the time and date of the most recent alarms.

- **System Monitor**

  The B5800 Branch Gateway System Monitor application is a tool that shows details of all activity on the B5800 Branch Gateway system. Because of the level of detail, interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. Installers and maintainers must understand how to run System Monitor when necessary as Avaya may request copies of System Monitor traces to resolve support issues.

Starting System Status

About this task

The B5800 Branch Gateway System Status application is a monitoring and reporting tool that provides a wide range of information about the current status of the system. It can report the available resources and components within the system and details of calls in progress. Details of the number of alarms are recorded and the time and date of the most recent alarms.

Procedure

1. To start the System Status application, choose one of the following:
   - On the PC where System Status has been installed, select **Start** > **Programs** > **IP Office** > **System Status**.

- If Manager is also installed and is running, select **File** > **Advanced** > **System Status**.
- Start a web browser and enter the IP address of the control unit. Then select the System Status Application link.

The Logon window appears.

2. In the Logon window, enter the details of the B5800 Branch Gateway system to which you want it to connect as follows:
   a) In the **Control Unit IP Address** drop-down box, select the appropriate address, or enter the IP address of the control unit.
   b) In the **Services Base TCP Port** field, enter the Services Base TCP Port setting that was set in the system's security settings. The default is 50804
   c) In the **Local IP Address** field, enter the appropriate local IP address. If the PC has more than one IP address assigned to its network card or multiple network cards, the address to use can be selected if necessary.
   d) In the **User Name** field, enter a user name that has been configured for System Status access in the B5800 Branch Gateway security settings.
   e) In the **Password** field, enter the appropriate password.
   f) Check the **Auto Reconnect** check box if you want System Status to attempt to reconnect using the same settings if connection to the B5800 Branch Gateway is lost.
3. Click **Logon**.

Starting System Monitor

About this task

The B5800 Branch Gateway System Monitor application is a tool that shows details of all activity on the B5800 Branch Gateway system. Because of the level of detail, interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. Installers and maintainers must understand how to run System Monitor when necessary as Avaya may request copies of System Monitor traces to resolve support issues.

Procedure

1. Select **Start** > **Programs** > **IP Office** > **Monitor**.
   If System Monitor has been run before it will attempt to connect with the system which it monitored previously.
2. To monitor a different system, select **File** > **Select Unit**.
   The Select System to Monitor window appears.

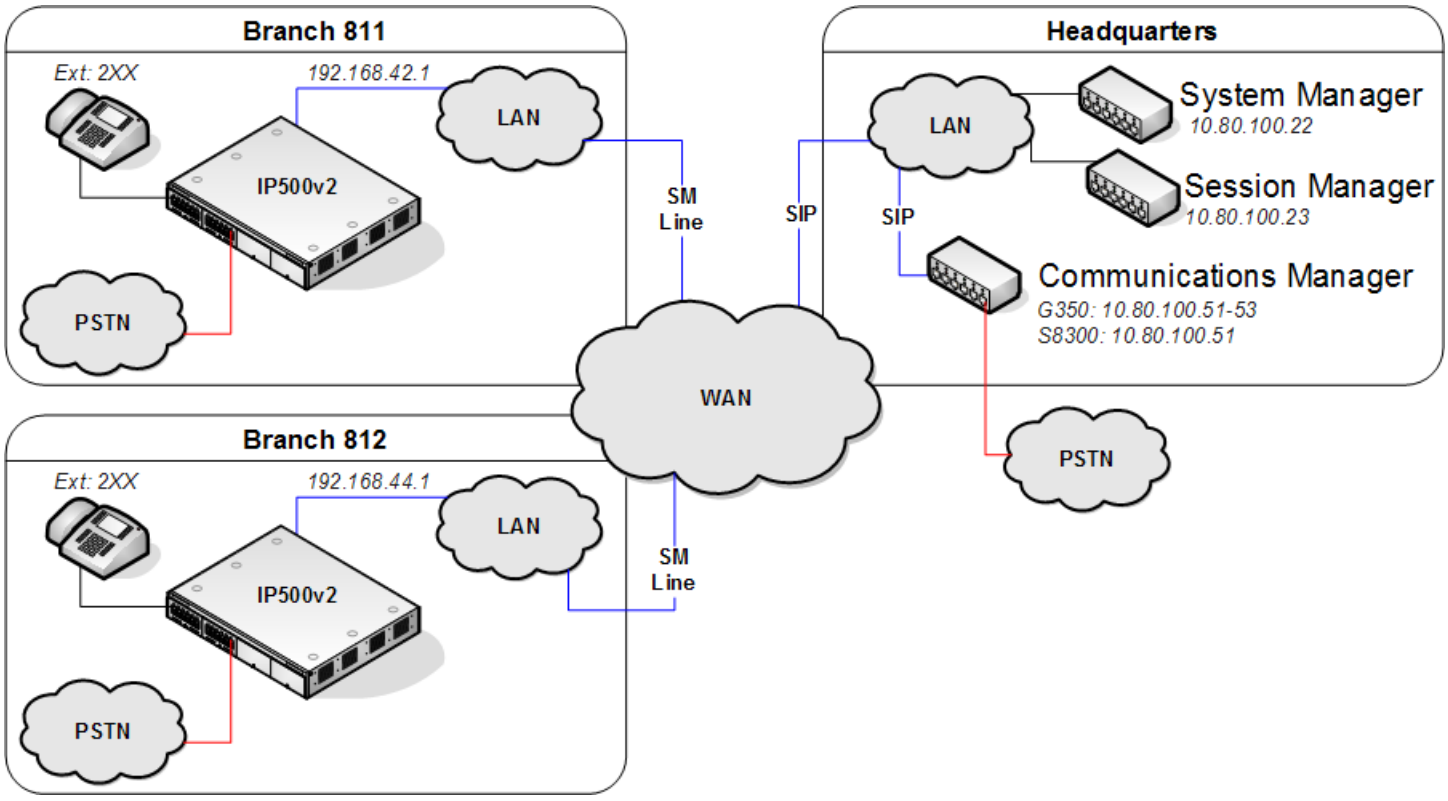
3. In the Control Unit IP Address drop-down box, select the IP address of the control unit you want to monitor.
4. In the Password field, enter the appropriate password.

   Note:

   You are able to set a System Monitor password using Manager. If the B5800 Branch Gateway does not have a System Monitor password set, System Monitor uses the B5800 Branch Gateway System password. The System Monitor password and System password are both set within the B5800 Branch Gateway system security settings.
5. For Control Unit Type, select **IP Office**.
6. Click **OK**.

Chapter 6: Initial configuration for a Centralized Branch

This chapter provides initial configuration tasks required for each B5800 Branch Gateway branch deployed in the Centralized Branch user model.



In the scenario where no survivable extensions are present and the same hardware is used at each branch, the branches can use the same configuration except for branch prefix and IP address.

Communication Manager vs Communication Manager Feature Server

When an B5800 Branch Gateway is not hosting any survivable extensions, the Communication Manager at the headquarters location is acting just as a trunk gateway for the branches and not also as a Communication Manager Feature Server for survivable extensions.

Centralized Branch configuration checklist

Use this checklist to monitor your progress as you configure a B5800 Branch Gateway system deployed as Centralized Branch.

#	Description	Section	✔
1	Launch Network Management and start Network Management Console to discover devices in your network. **Note:** This step applies only if you are using Network Management to configure the system.	See “Chapter 3: Discovering the Voice Network” in *Avaya Integrated Management Release 6.0 Network Management Configuration*.	
2	Activate license files and deliver the license files to the branches.	See Activating license files on page 98.	
3	If you are not going to use Network Management to configure the branch, disable the Network Management administration feature for the branch.	See Disabling the Network Management administration feature for the branch on page 103.	
4	Disable unused trunks.	See Disabling unused trunks on page 104.	
5	Set a trunk clock quality setting.	See Setting a trunk clock quality setting on page 106.	
6	Set trunk prefixes.	See Setting the trunk prefixes on page 106.	
7	Enable SIP trunk support.	See Enabling SIP trunk support on page 109.	
8	Set the branch prefix and local number length for the extension numbering.	See Setting the branch prefix and local number length for extension numbering on page 110.	
9	Change the default codec selection.	See Changing the default codec selection on page 112.	
10	Change the maximum SIP sessions.	See Changing the maximum SIP sessions on page 113.	
11	Add a Session Manager line.	See Adding an Avaya Aura Session Manager line on page 114.	

#	Description	Section	✔
12	Add a second Session Manager line for redundancy.	See Avaya Aura Session Manager line redundancy on page 118.	
13	Set up outgoing call routing.	• See Setting up outgoing call routing on page 120. • For information on routing back to the branch for fallback alternate routes, see Branch PSTN call routing examples on page 325.	
14	Configure Modular Messaging as the voicemail system the branch will use. Survivable extensions cannot use Embedded Voicemail or Voicemail Pro.	See Voicemail operation on page 163.	
	Note: Numbers 15 through 23 are performed from Avaya Aura®Session Manager. B5800 Branch Gateway supports Session Manager 6.1 and 6.0 and procedures for both versions are provided.		
15	View a list of the SIP domains.	• For Session Manager 6.1, see Viewing the SIP domains on page 150. • For Session Manager 6.0, see Viewing the SIP domains on page 156.	
16	Create a location.	• For Session Manager 6.1, see Creating locations on page 150. • For Session Manager 6.0, see Creating locations on page 156.	
17	Create a digit adaptation.	• For Session Manager 6.1, see Creating adaptations on page 151. • For Session Manager 6.0, see Creating adaptations on page 157.	
18	Create a SIP entity.	• For Session Manager 6.1, see Creating SIP entities on page 151. • For Session Manager 6.0, see Creating SIP entities on page 157.	
19	Create an entity link.	• For Session Manager 6.1, see Creating entity links on page 152. • For Session Manager 6.0, see Creating entity links on page 158	

#	Description	Section	✔
20	Create a time range.	For Session Manager 6.1 or 6.0, see Creating time ranges on page 153.	
21	Create a routing policy.	• For Session Manager 6.1, see Creating routing policies on page 153. • For Session Manager 6.0, see Creating routing policies on page 159	
22	Create a dial pattern.	• For Session Manager 6.1, see Creating dial patterns on page 154. • For Session Manager 6.0, see Creating dial patterns on page 160	
23	If you are going to use Network Management to configure the branch, you can create a System Manager cut-through link to Network Management.	For Session Manager 6.1 or 6.0, see Creating a System Manager link to Network Management on page 161.	
24	Administer extensions	See Extension administration on page 173.	

Activating license files

About this task

B5800 Branch Gateway uses the Avaya Product Licensing and Delivery System (PLDS) to manage license entitlements. When you access PLDS and activate a license file, you are given the opportunity to save the license file to the local PC. Once saved on the local PC, you can send the license file to the branch in two ways — either through Provisioning and Installation Manager (PIM) or Manager. If using PIM, you load the license file to PIM and then create a job to send the license file to the B5800 Branch Gateway device. If using Manager, you select a locally saved license file and then upload the license file to the B5800 Branch Gateway device.

PIM provides a bulk provisioning feature where you can use a mapping file that contains a list of comma separated key value pairs of B5800 Branch Gateway IP addresses and license file names, one pair for each branch, to send licenses to multiple branches simultaneously. The license file names are based on the Feature Key (FK) serial number on the SD cards. See Creating a mapping file on page 102 for more information.

Note:

B5800 Branch Gateway supports a 30-day grace period during which time the system is fully functional if a license error is detected or if a license file cannot be obtained, for example due to loss of WAN connectivity.

Procedure

1. See Activating license entitlements on page 209 to generate the licenses.
2. Depending upon which method you want to use to deliver the activated license files to each branch, see one of the following:
   - See Using Manager to deliver license files to the branches on page 99.
   - See Using Provisioning and Installation Manager to deliver license files to the branches on page 100.

Using Manager to deliver license files to the branches

Before you begin

License files have been activated. See Activating license entitlements on page 209.

About this task

You can use Manager to distribute activated license files to B5800 Branch Gateway sites. This procedure explains how to distribute the license files to a single branch at a time.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, select **PLDS License**.
3. Right-click **PLDS License** and select **Send license file to IP Office**.
4. In the Upload Files window, select the PLDS license xml file.
   Manager copies the license file to the B5800 Branch Gateway SD card where it is validated and stored for persistent use.
5. Select **File > Close Configuration**.
6. To view the license, select **File > Open Configuration**.

Deleting the PLDS license file from the branch

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, select **PLDS License**.
3. Right-click **PLDS License** and select **Delete PLDS License file from Avaya Branch Gateway**.

4. Select **File > Close Configuration**.

Using Provisioning and Installation Manager to deliver license files to the branches

Before you begin

License files have been activated. See Activating license entitlements on page 209.

About this task

Use this procedure to load the license files to Provisioning and Installation Manager (PIM) and then create a job to send the license files to the B5800 Branch Gateway branches. You can send license files to a single branch or to multiple branches simultaneously. You can also schedule when you want the job to run.

Procedure

1. From the Avaya Integrated Management Launch Products page, click **Provisioning and Installation Manager for IP Office**.
2. From the Provisioning and Installation Manager main window, select **Administration > Licenses** in the left panel.
3. Click **Add**.
4. In the PIM – Upload License file window, click the **Browse** button and select the .xml license file.
5. Click the **Upload file** button.
   The license file is uploaded to PIM and appears in the License Files List.

   Note:

   The license file is now stored in the Network Management server file system under \Program Files\Avaya\Network Management\CSV\IPOLicenses. PIM renamed the license file name to the format <*host ID of the SD card*>_HID.xml, for example **111306312781_HID.xml**. The host ID is the Feature Key (FK) serial number printed on the SD card. PIM renames the license file to one that identifies the respective device. If you have multiple license files, once you upload all the license files, you can create a mapping file for bulk distribution. See Creating a mapping file on page 102 for more information.
6. To send the license file to the branch, from the Provisioning and Installation Manager main window, click **Import Licenses** at the top of the window.
   The Import Licenses Job Wizard appears.
7. On the General page, do the following:
   a) In the **Job Name** field, enter a name for this job.
   b) In the **Notes** field, enter notes about this job.

8. Click **Next**.
9. On the Import Licenses Wizard page, choose one of the following:
   - To select a mapping file, click the **Select Mapping File** option button and then click **Browse** to locate the mapping file.

     Note:
     Mapping files are used for bulk provisioning. See Creating a mapping file on page 102 for more information.
   - To select a device and license file from a list, do the following:
     1. Click the **Select Devices from list** option button.
     2. Click the check box for the device.
     3. From the corresponding drop-down box, select the license file name that matches the FK serial number printed on the SD card for the device.

     The IP address of the device is shown as well as the name of the license file associated with the device. The license file name is created from the host ID of the SD card and is in the format <*host ID of the SD card*>_HID.xml, for example **111306312781_HID.xml**. The host ID is the Feature Key (FK) serial number printed on the SD card.

     Note:
     Even if the license file name was changed at an earlier point, for example to make it shorter, the license file name that appears here is derived from the host ID of the SD card, not the file name as it was renamed.
10. Click **Next**.
11. On the Check Mapping List page, review the list and then click **Next**.
12. On the Schedule page, choose one of the following
    - Click the **Run now** option button to import the license files to the devices now.
    - Click the **Run the job on** option button to run the job at a specified date and time. Then do the following:
      1. Click the date/time icon and select the date and time you want the job to run.
      2. In Time Zone drop-down box, select the appropriate time zone.
    - Click the **I'll schedule the job later** option button to schedule the job later.
13. Click **Next**.
14. On the Job Options page, do the following:

a) Click the **Full execution** option button.
b) Click the **Ignore Warnings** check box to deselect it so that warnings are not ignored during validation.

15. Click **Next**.
16. Review the summary, and then click **Next**.
17. Click **Finish**.
    The License Wizard closes. When the job is run, either now or on the date and time you specified, the license file(s) are pushed down to the designated devices using TFTP.
18. To view the status of a completed job, on the License Files List page, in the left navigation pane, select **Jobs > Completed**.
    The jobs that have completed are listed on the Completed Jobs page.

Creating a mapping file

About this task

If you have activated multiple license files in PLDS, you can create a mapping file that contains a list of comma separated key value pairs of B5800 Branch Gateway IP addresses and license file names, one pair for each branch. A mapping file is useful for bulk provisioning. When you distribute the license files to the branches, you have the opportunity to select the mapping file you created. Alternatively, you are also able to select devices from a list. See Using Provisioning and Installation Manager to deliver license files to the branches on page 100 for more information.

You can create a mapping file in advance by opening a text file and typing the device IP address and corresponding license file name for each device. The license file name is the Feature Key (FK) serial number printed on the SD card designated for that device. You would type the IP address/license file name for each device to which you want to send a license.

Alternatively, you can create the mapping file once the license files are imported into Provisioning and Installation Manager. Once imported, the license files are stored in the Network Management server file system under \Program Files\Avaya\Network Management \CSV\IPOLicenses. This method allows for less errors in the mapping file because you are able to copy the device IP address/license file name from the Network Management folder.

Procedure

1. Open a generic CSV text file.
2. Enter the B5800 Branch Gateway IP address and corresponding license file name in the following format: < *IP address of the device*>,< *License file name* >.

Note:

The license file name is comprised of the host ID of the SD card followed by _**HID.xml**, for example **111306312781_HID.xml**. The host ID is the Feature Key (FK) serial number printed on the SD card.

3. Repeat step 2 for each IP address/license file pair.

   Sample mapping file:

```
148.147.206.251,111306312781_HID.xml
148.147.206.160,111310198782_HID.xml
148.147.175.145,111313365847_HID.xml
```

4. Save the file.

Disabling the Network Management administration feature for the branch

About this task

If you want to administer the branch through Manager and not through Network Management, you must disable the Network Management administration feature for the branch.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File** > **Advanced** > **Security Settings**.
3. In the Select IP Office window, click the check box for the appropriate system.
4. Click **OK**.
5. In the Security Service User Login window, enter a user name and password of an account that has security configuration access to the B5800 Branch Gateway system.

   The defaults are **security** and **securitypwd**.
6. In the Security Settings pane, select **Services**.
7. In the Services pane, select **Configuration**.
8. In the Service Details pane, click the check box for **Under ENM Administration** to deselect this option.

   Note:

   When Network Management is installed, this check box is checked by default and you are not able to administer the branch through Manager. To be able to use Manager to administer the branch, this check box must be unchecked.

9. Click **OK**.
10. Select **File > Save Configuration**.

Disabling unused trunks

About this task

Each B5800 Branch Gateway trunk card provides a fixed number of trunk ports with digital trunk ports supporting a fixed number of digital channels. By default th B5800 Branch Gateway configuration will have settings for all the possible trunks and channels.

In cases where the number of trunks or trunk channels in use is lower than the number supported by the trunk card, the unused trunks and channel must be disabled.

Important:
Failure to do this will cause problems with outgoing calls.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. For each line, set those lines or channels that are not connected or not being used as **Out of Service**.
   The location of the relevant setting varies for each trunk type.
4. For **Analog Trunks**, set the **Trunk Type** to **Out of Service**.
5. For **BRI, E1 PRI, S0 and QSIG Trunks**, set the channels quantities to match the actual subscribed channels.
6. For **T1, T1 PRI and E1R2 Trunks**, select the Channels tab. Then do the following:

a) Select those channels that are not used and click **Edit**.

- For T1 set the **Type** to **Out of Service**
- For T1 PRI set the **Admin** field to **Out of Service**.
- For E1R2 trunks set the **Line Signalling Type** to **Out of Service**.

7. Select **File > Save Configuration**.

Digital trunk clock source

About this task

Digital trunks require the telephone system at each end of the trunk to share a clock signal to ensure synchronization of call signalling. The B5800 Branch Gateway can obtain and use the clock signal from any of its digital trunks. Typically the clock signal provided by a digital trunk from the central office exchange is used as this will be the most accurate and reliable clock source.

To do this, the **Clock Quality** setting on each line in the B5800 Branch Gateway configuration is set to one of the following:

- **Network**

  If available, the clock signal from this trunk should be used as the B5800 Branch Gateway clock source for call synchronization. If several trunk sources are set as Network, the B5800 Branch Gateway will default to using one as detailed below.

- **Fallback**

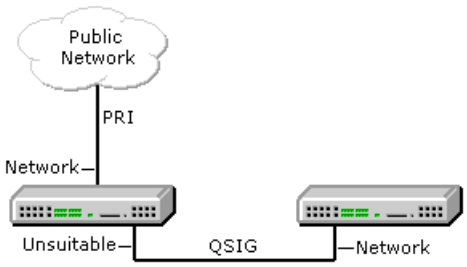
  If available, the clock signal from this trunk can be used as the clock source if none of the trunks set as Network are providing a clock source.

- **Unsuitable**

  The clock source from this trunk will never be used as the B5800 Branch Gateway clock source.

If no clock source is available the B5800 Branch Gateway can use its own internal clock if necessary.

In the example below the first B5800 Branch Gateway is set to use the public network trunk as its clock source and ignoring the possible clock source from the QSIG trunk. The other B5800 Branch Gateway system is using the clock signal received from the first B5800 Branch Gateway on its QSIG trunk as its clock source. Thus both systems are using the same clock source and that clock source is the public network exchange.



When multiple trunks with the same setting are providing clock signals, trunks are used in the order of slots 1 to 4 and then by port on each slot.

The current clock source being used by an B5800 Branch Gateway system is shown on the Resources page within the B5800 Branch Gateway System Status Application.

Setting a trunk clock quality setting

About this task

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. For each digital line, do the following:
   a) Select the line.
   b) On the **Line** tab, select whether that trunk should provide the clock source for the network or whether the trunk is unsuitable.

   Note:
   For E1R2 trunks the **Clock Quality** setting is on the **Advanced** tab
4. Ensure that only one trunk is set to **Network**. This should preferably be a direct digital trunk to the central office exchange.
5. Set one other trunk to **Fallback** in case the selected network trunk connection is lost.

   Note:
   If possible this should be a trunk from a different provider since that reduces the chances of both sources failing at the same time.
6. Ensure that all other digital trunks are set as **Unsuitable**.
7. Select **File > Save Configuration**.

Setting the trunk prefixes

About this task

Where a prefix has been implemented for outgoing calls, that same prefix needs to be added to trunk settings. The prefix is then used as follows:

- On incoming calls the prefix is added to any incoming ICLID received with the call. That allows the ICLID to be used by B5800 Branch Gateway phones and applications to make return calls.
- On outgoing calls, the short codes used to route the call to a trunk must remove the dialing prefix.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. For each line enter the prefix. The location of the relevant setting varies for each trunk type.
    - For analog trunks, select the **Line Settings** tab and enter the prefix in the **Prefix** field.
    - For T1 and T1 PRI trunks, select the **PRI 24 Line** tab and enter the prefix in the **Prefix** field.
    - For BRI, E1 PRI, S0 and QSIG trunks, select the **PRI Line** tab and enter the appropriate prefix in the following fields:
        - Prefix
        - National Prefix
        - International Prefix
4. Select **File > Save Configuration**.

SIP trunk prefixes

The prefix fields Prefix, National Prefix, Country Code and International Prefix are available with the SIP line settings. These fields are used in the following order:

1. If an incoming number (called or calling) starts with the + symbol, the + is replaced with the International Prefix.
2. If the Country Code has been set and an incoming number begins with that Country Code or with the International Prefix and Country Code, they are replaced with the National Prefix.
3. If the Country Code has been set and the incoming number does not start with the National Prefix or International Prefix, the International Prefix is added.
4. If the incoming number does not begin with either the National Prefix or International Prefix, then the Prefix is added.

For example, if the SIP line is configured with the following prefixes, the numbers are processed as described in the table below.

- Line Prefix: 9
- National Prefix: 90

- International Prefix: 900
- Country Code: 44

Number Received	Processing	Resulting Number
+441707362200	Following rule 1 above, the + is replaced with the International Prefix (900), resulting in 900441707362200. The number now matches the International Prefix (900) and Country Code (44). Following rule 2 above they are replaced with the National Prefix (90).	901707362200
00441707362200	Following rule 2 above the International Prefix (900) and the Country Code (44) are replaced with the National Prefix (90).	90107362200
441707362200	Following rule 2 above, the Country Code (44) is replaced with the National Prefix (90).	901707362200
6494770557	Following rule 3 above the International Prefix (900) is added.	9006494770557

Administering a Session Manager line for each branch

This section provides the procedures required to configure a Session Manager line between each branch site and the headquarters site.

This section also describes how the B5800 Branch Gateway uses a configured Session Manager line to handle incoming and outgoing calls to and from the branch and explains how a second Session Manager line can be configured for Session Manager line redundancy.

- See Enabling SIP trunk support on page 109. Use this procedure to configure the IP Office LAN interface which will be used for the Session Manager line connection to the Avaya Aura® Session Manager.
- See Setting the branch prefix and local number length for extension numbering on page 110. Use this procedure to set the prefix number for the B5800 Branch Gateway and the required extension length.

- See Changing the default codec selection on page 112. Use this procedure to set the preferred order for codec negotiation. This can be done as a system default and also for each individual SIP and Avaya Aura® Session Manager line.
- See Adding an Avaya Aura Session Manager line on page 114. Use this procedure to create a Session Manager line for calls to the Avaya Aura® Session Manager.
- See Setting up outgoing call routing on page 120. Use this procedure to create short codes for routing calls to the Avaya Aura® Session Manager line when the required destination or resource is on another branch of the Avaya Aura® network.
- See How the B5800 Branch Gateway uses a configured Session Manager line on page 121.
- See Avaya Aura Session Manager line redundancy on page 118.

Enabling SIP trunk support

About this task

Before adding any SIP trunks, includingAvaya Aura® Session Manager lines, the B5800 Branch Gateway system must be configured for SIP trunk operation. The system has 2 LAN interfaces, LAN1 and LAN2 (the physical ports are labeled LAN and WAN respectively). Either can be used for the Avaya Aura® Session Manager line operation.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **LAN1** or **LAN2** tab as appropriate depending on which branch site LAN interface will be used for the data connection to the Avaya Aura® network.
4. Confirm that the IP address and IP Mask fields are set correctly for the site.
5. Click the **VoIP** tab.
6. Select the **SIP Trunks Enable** option. This is required for Avaya Aura® Session Manager trunk support.

   Note:

   The **SIP Registrar Enable** setting and settings in the **SIP Registrar** tab relate to SIP extension support and therefore do not affect Avaya Aura® Session Manager lines. The settings in the **Network Topology** tab relate to external SIP trunks. Those settings are not used by Avaya Aura® Session Manager lines, which use open internet across the customer WAN.

7. Click **OK**.
8. Select **File > Save Configuration**.
   The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Setting the branch prefix and local number length for extension numbering

About this task

Each B5800 Branch Gateway system in the network should have a unique branch number. That number is added as a prefix to the caller's extension number for calls routed to the Avaya Aura® Session Manager.

The prefix is also used in the Avaya Aura® Session Manager configuration to create unique dial patterns for routing calls to the appropriate B5800 Branch Gateway.

By default B5800 Branch Gateway systems use 3-digit extension numbering starting from 200. The existing allocated numbers can be changed in bulk using the **Tools > Extension Renumber** option. This will add or remove a set value from all existing extension numbers in the configuration.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **System** tab.
4. Set the following fields as appropriate:
   - Branch Prefix
   - Local Number Length
   - Proactive
   - Reactive

   These 4 fields are the key settings for B5800 Branch Gateway operation. See System tab field descriptions on page 111 for more information.
5. Click **OK**.
6. Select **File > Save Configuration**.
   The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

System tab field descriptions

Name	Range or Default	Description
Branch Prefix	Range = 0 to 999999999	This number is used to identify the B5800 Branch Gateway system within the Avaya Aura® network. The branch prefix of each B5800 Branch Gateway system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. On calls routed via an Avaya Aura®Session Manager line, the branch prefix is added to the caller's extension number.
Local Number Length	Range = Blank (Off) or 3 to 9	This field sets the default length for extension numbers for extensions, users, and hunt groups added to the B5800 Branch Gateway configuration. Entry of an extension number of a different length will cause an error warning by Manager. The combined **Branch Prefix** and **Local Number Length** should not exceed 15 digits.
Proactive	Default = 60 seconds	The B5800 Branch Gateway sends regular SIP OPTION messages to the Avaya Aura®Session Manager line in order to check the status of the line. This setting controls the frequency of the messages when the Avaya Aura®Session Manager line is currently in service. Note that centralized extensions use their own settings.
Reactive	Default = 60 seconds	The B5800 Branch Gateway sends regular SIP OPTION messages to the Avaya Aura®Session Manager line

Name	Range or Default	Description
		in order to check the status of line. This setting controls the frequency of the messages when the Avaya Aura®Session Manager line is currently out of service. Note that centralized extensions use their own settings.

Changing the default codec selection

About this task

By default, all B5800 Branch Gateway IP trunks and extensions use automatic codec negotiation. The default negotiation order is G729(a) 8K CS-ACELP, G711 U-Law 64K, G711 A-Law 64K and G723.1 6K3 MP-MLQ.

If bandwidth between the B5800 Branch Gateway and Avaya Aura® sites is sufficient, we recommend that you change the first default preference to one of the G711 codecs. Note that the specific setting for individual branch trunks and extensions can be set to override the system setting if necessary.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **Telephony** tab.
4. Click the **Telephony** sub-tab.
5. In the **Automatic Codec Preference** drop-down box, select the appropriate setting.
   The **Automatic Codec Preference** setting is used to indicate the preferred codec order for trunks and extensions that are using automatic codec negotiation. See Automatic codec preference settings on page 113 for more information.
6. Click **OK**.
7. Select **File > Save Configuration**.

The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Automatic codec preference settings

Setting	Selected Preference	2nd Preference	3rd Preference	4th Preference
G.729	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K	G723.1 6K3 MP-MLQ
G.723	G723.1 6K3 MP-MLQ	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K
G.711 U-Law	G711 U-Law 64K	G711 A-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ
G.711 A-Law	G711 A-Law 64K	G711 U-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ

Changing the maximum SIP sessions

About this task

The Maximum SIP Sessions setting limits the number of concurrent sessions allowed across all SIP trunks (public exchange and Session Manager). This setting must not exceed the number of SIP trunk sessions licensed in PLDS. If the PLDS license file is already installed, the Maximum SIP Trunk Sessions licensed for the system is identified on the PLDS screen when you select **PLDS License** on the left navigation pane. If the PLDS license file is not yet installed, you must still set this feature. This will determine the Avaya Branch Gateway operation and system capacities during the 30-day grace period that is in effect when the system is in License Error Mode because the license is not yet installed. Once the PLDS license is installed, the Maximum SIP Session setting should be changed to match what appears on the PLDS screen. This will change the License Mode setting that appears on the PLDS screen to Normal Mode.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **Telephony** tab.
4. Click the **Telephony** sub-tab.
5. In the **Maximum SIP Sessions** drop-down box, select the number that matches the Maximum SIP Trunk Sessions licensed for the system.

To see the Maximum SIP Trunk Sessions licensed for the system, in the left navigation pane, select **PLDS License**.

6. Click **OK**.
7. Select **File > Save Configuration**.

Adding an Avaya Aura® Session Manager line

About this task

Use this procedure to add an Avaya Aura®Session Manager line to the B5800 Branch Gateway system configuration. If multiple Avaya Aura®Session Managers are available at the headquarters site, an additional Avaya Aura® Session Manager line can be added for Session Manager line redundancy. See Avaya Aura Session Manager line redundancy on page 118 for more information.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. Click the **New** icon and select **SM Line**.
4. Configure the line settings as appropriate. See Session Manager tab field descriptions on page 115 for more information.
5. Click **OK**.
6. Click the **VoIP** tab.
7. Click the **Allow Direct Media Path** check box to select this option.
8. Click the **Re-Invite Supported** check box to select this option.
9. Configure the remaining fields as appropriate. See VoIP tab field descriptions on page 116 for more information.
10. Click **OK**.
11. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Session Manager tab field descriptions

Name	Description
Line Number	This value is automatically assigned by B5800 Branch Gateway and should be unique for each line added to the configuration.
In Service	The default setting is enabled. This option can be used to manually take the Session Manager line out of service. It does not reflect or set the actual state of the line.
SM Domain Name	This name should match a SIP domain defined in the Session Manager system's SIP Domains table. Unless there are reasons to do otherwise, all the B5800 Branch Gateway systems in the Avaya Aura® network can share the same domain. **Note:** See Viewing the SIP domains on page 150 for a list of SIP domains defined in Session Manager.
SM Address	Enter the IP address of the Session Manager that the line should use in the Avaya Aura® network. The same Session Manager should be used for the matching Entity Link entry in the Avaya Aura® configuration.
Inactivity timeout (seconds)	The default setting is 0. Keep the default setting to maintain a persistent connection with Session Manager.
Outgoing Group ID	The default setting is 99999. This value is not changeable. However note the value as it is used in B5800 Branch Gateway short codes used to route calls to the Session Manager.
Prefix	This field is blank by default. This prefix will be added to any source number received with incoming calls.
Max Calls	The default setting is 10. This value sets the number of simultaneous calls allowed between B5800 Branch Gateway and Session Manager using this connection. Each call uses one of the available licenses that are shared by all SIP trunks configured in the system.

Name	Description
Network Configuration	These settings are fixed to **TCP** using send and receive ports **5060**.

VoIP tab field descriptions

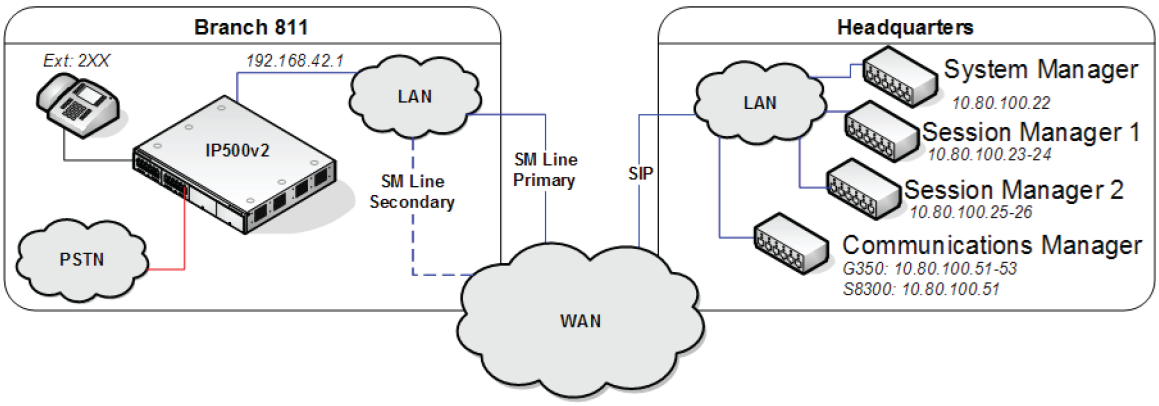
Name	Range or Default	Description
Compression Mode	Default = Automatic Select	These settings are used to select the code negotiation order. • The default, **Automatic Select**, sets the line to use the codec order selected on the System > Telephony form. • The optionis in the drop-down list box are used to select which code should come first in the selection order of G729(a) 8K CS-ACELP > G711 U-Law 64K > G711 A-Law 64K > G723.1 6K3 MP-MLQ. Note that if one of the G711 options is selected as the first choice codec, the other G711 option is used as the second choice codec. • The **Advanced** option can be used to manually configure the codec preference order and specify which codecs are used.
Call Initiation Timeout	Default = 4 seconds	The B5800 Branch Gateway sends regular OPTION messages to each Avaya Aura®Session Manager line in order to check the lines in or out of service status. If a response is not received within this timeout, the line is treated as being out of service.

Name	Range or Default	Description
DTMF Support	Default = RFC2833	This setting is used to select the method by which DTMF key presses are signaled to the remote end. The supported options are **In Band**, **RFC2833** or **Info**.
VoIP Silence Suppression	Default = Off	When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods.
Fax Transport Support	Default = Off	This option is only selectable if the option **Re-Invite Supported** is also selected. If enabled, the B5800 Branch Gateway is able to support the sending and receiving of faxes via the Avaya Aura® Session Manager line using the T38 protocol. The settings for T38 are set on the T38 Fax tab.
Allow Direct Media Path	Default = On	This setting controls whether connected calls must remain routed via the B5800 Branch Gateway or can be routed alternately if possible within the network structure. • If enabled, connected calls can take routes other than through the B5800 Branch Gateway. This removes the need for a voice compression channel. • If disabled or not supported at one end of the call, the call is routed via the B5800 Branch Gateway. However RTP relay support allows calls between devices using the same audio codec to not require a voice compression channel.
Re-Invite Supported	Default = On	When enabled, Re-Invite can be used during a session to

Name	Range or Default	Description
		change the characteristics of the session, for example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk.
Use Offerer's Preferred Codec	Default = Off	Normally for SIP calls, the codec preference of the answering end is used. This option can be used to override that behavior and use the codec preferences offered by the caller.

Avaya Aura® Session Manager line redundancy

In an Avaya Aura® network that includes multiple Avaya Aura® Session Managers for redundancy, the B5800 Branch Gateway system can be configured with a secondary Avaya Aura® Session Manager line. If for any reason the B5800 Branch Gateway system's primary Avaya Aura® Session Manager line goes out of service, the system will automatically attempt to use the secondary Avaya Aura® Session Manager line.



Note:

Determining which Session Manager line is the primary line and which is the secondary line is not an option that can be configured.

During normal operation, the Avaya Aura® Session Manager line added to the B5800 Branch Gateway configuration first is used as its primary Avaya Aura® Session Manager line for all calls to the Avaya Aura® network. Incoming calls can be received on either line at all times.

The B5800 Branch Gateway system sends regular OPTION messages to both Avaya Aura® Session Manager lines in order to check their in-service or out-of-service status. If the current line in use changes to out of service and the other line is in service, the B5800 Branch Gateway will switch to using the other line. However it will not automatically switch back if the previous line returns back to in service. The B5800 Branch Gateway system will only switch lines when the line currently in use changes to out of service.

If all available channels of the current Avaya Aura®Session Manager line are in use, the B5800 Branch Gateway will not overflow calls to the other Avaya Aura®Session Manager line. However, if PSTN trunk fallback has been configured, the other Avaya Aura®Session Manager line will be used. See PSTN trunk fallback on page 330 for more information.

Avaya Aura®Session Manager line service status checks

The B5800 Branch Gateway system sends regular OPTION messages to any Avaya Aura® Session Manager lines in its configuration. The Proactive and Reactive settings on the B5800 Branch Gateway system's System tab set how often the OPTION messages are sent in seconds. The Proactive setting is used for an Avaya Aura® Session Manager line currently thought to be in service. The Reactive setting is used for an Avaya Aura® Session Manager line currently thought to be out of service.

- If a response is received and is not a 408, 500, 503 or 504 response, the Avaya Aura® Session Manager line is treated as in service; otherwise the line is treated as being out of service.
- If no response is received within the set Call Initiation Timeout setting on the Avaya Aura® Session Manager line's VoIP tab the line is treated as being out of service.
- If the line is out of service, and call comes from the trunk, the trunks status is changed back to in service.
- If the line is in service, a call may fail due to either being unable to deliver the message or receive a 100 response within a configured timeout. The line will not go out of service because this may be a temporary failure due to a busy system.
- In addition each Avaya Aura® Session Manager line can be manually set to in or out of service using the In Service option on the Avaya Aura® Session Manager line's Session Manager tab.

Centralized extensions

In scenarios where there are multiple Avaya Aura®Session Managers, centralized extensions can be configured to use these for survivability in addition to using the local B5800 Branch Gateway system. This is preferable as the additional Avaya Aura® Session Manager will be able to provide full feature support. In this scenario, the backup Avaya Aura®Session Manager used by the centralized extensions should be the same one as used for the secondary Avaya Aura® Session Manager line.

Secondary Avaya Aura® Session Manager line configuration

The secondary Avaya Aura® Session Manager line is configured in the same way as the primary Avaya Aura®Session Manager line. The only difference required is to set the **SM Address** field to the address of the alternate Avaya Aura®Session Manager from the one being used by the primary Avaya Aura® Session Manager line.

Setting up outgoing call routing

About this task

For calls from extensions on the B5800 Branch Gateway system to other numbers within the network, system short codes are used to route the calls to the Avaya Aura® Session Manager line. The Avaya Aura® Session Manager then performs the routing to determine where the call should go.

Note:

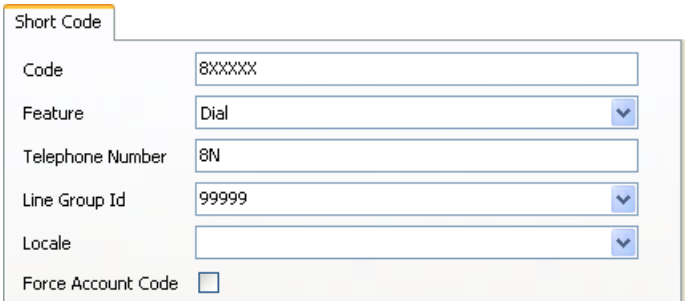
See Branch PSTN call routing examples on page 325 for information on routing back to the branch for fallback alternate routes.

Ideally the number of such system short codes should be kept to a minimum and the same short codes used on all branches in order to ease maintenance. This is where using a uniform dial plan for all branches helps, as explained in Dial plan considerations on page 30. For our example, the uniform dial plan allows the same single short code to be used at all branches.

See the Manager context-based help for more information on creating short codes.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Short Code**.
3. Click the **New** icon and select **Short Code**.



4. Configure the settings as appropriate. See Short Code tab field descriptions on page 121 for more information.

   Note:

   To view more information about the system short codes, press F1. In particular, see the description of the **Dial** short code.

5. Click **OK**.
6. Select **File > Save Configuration**.

Short Code tab field descriptions

Name	Description
Code	Enter the number dialed by users that should be matched to this short code. Use **X** wildcards for any single digit.
Feature	Leave this field set as **Dial**.
Telephone Number	Set this field to match a number that should be passed to the Avaya Aura® Session Manager for routing against its dialing pattern matches. The **N** wildcard can be used to match any wildcards in the **Code**. **Note:** Add SS to the entry in this field to have the caller ID passed to the Session Manager line. For example, if you are entering 8N in the Telephone Number field, enter 8NSS.
Line Group Id	Set the **Line Group ID** to match the **Outgoing Group** settings used in the SM lines URI setting.
Local	Features that transfer the caller to Voicemail Pro can indicate the language locale required for prompts. This is subject to the language being supported and installed on the voicemail server. The default is blank.
Force Account Code	When selected, for short codes that result in the dialing of a number, the user is prompted to enter a valid account code before the call is allowed to continue. The default is **Off**.

How the B5800 Branch Gateway uses a configured Session Manager line

Once configured and in operation, the Avaya Aura® Session Manager line is used as follows.

Outgoing calls from a branch

In the Distributed branch user model, if the outgoing call begins with the branch's own prefix, the prefix is removed and the call is targeted locally to the matching native user or hunt group

extension number. If there is no matching extension number, the call is targeted to any matching system short code.

Incoming calls to a branch

Incoming calls on an Avaya Aura®Session Manager line are treated as being internal calls and do not go through the B5800 Branch Gateway system's Incoming Call Route settings.

- If the destination of the incoming call on the Avaya Aura® Session Manager line starts with the system's branch prefix, the prefix is removed. The call is then targeted to the matching native user or hunt group extension number. If there is no matching extension number, the call is targeted to any matching system short code.
- If the destination of the incoming call on the Avaya Aura® Session Manager line does not start with the system's branch prefix, the whole number is checked for a match against system short codes.

Line status detection

The B5800 Branch Gateway system sends regular OPTION messages to any Avaya Aura® Session Manager lines in its configuration. The Proactive and Reactive settings on the B5800 Branch Gateway system's **System** tab set how often the OPTION messages are sent in seconds. The Proactive setting is used for an Avaya Aura® Session Manager line currently thought to be in service. The Reactive setting is used for an Avaya Aura® Session Manager line currently thought to be out of service.

- If a response is received and is not a 408, 500, 503 or 504 response, the Avaya Aura® Session Manager line is treated as in service; otherwise the line is treated as being out of service.
- If the line is out of service, and call comes from the trunk, the trunks status is changed back to in service.
- If the line is in service, a call may fail due to either being unable to deliver the message or receive a 100 response within a configured timeout. The line will not go out of service because this may be a temporary failure due to a busy system.
- In addition each Avaya Aura® Session Manager line can be manually set to in or out of service using the In Service option on the Avaya Aura® Session Manager line's **Session Manager** tab.

Chapter 7: Initial configuration for a Distributed Branch

This chapter provides initial configuration tasks required for each B5800 Branch Gateway branch deployed in the Distributed Branch user model.

Distributed Branch configuration checklist

Use this checklist to monitor your progress as you configure a B5800 Branch Gateway system deployed as Distributed Branch.

#	Description	Section	✔
1	Launch Network Management and start Network Management Console to discover devices in your network. **Note:** This step applies only if you are using Network Management to configure the system.	See "Chapter 3: Discovering the Voice Network" in *Avaya Integrated Management Release 6.0 Network Management Configuration*.	
2	Activate license files and deliver the license files to the branches.	See Activating license files on page 125.	
3	If you are not going to use Network Management to configure the branch, disable the Network Management administration feature for the branch.	See Disabling the Network Management administration feature for the branch on page 130.	
4	Disable unused trunks.	See Disabling unused trunks on page 131.	
5	Set a trunk clock quality setting.	See Setting a trunk clock quality setting on page 133.	
6	Set trunk prefixes.	See Setting the trunk prefixes on page 134.	
7	Enable SIP trunk support.	See Enabling SIP trunk support on page 136.	

#	Description	Section	✔
8	Set the branch prefix and local number length for the extension numbering.	See Setting the branch prefix and local number length for extension numbering on page 137.	
9	Change the default codec selection.	See Changing the default codec selection on page 139.	
10	Change the maximum SIP sessions.	See Changing the maximum SIP sessions on page 140.	
11	Add a Session Manager line.	See Adding an Avaya Aura Session Manager line on page 141.	
12	Set up outgoing call routing.	• Setting up outgoing call routing on page 145. • For information on routing back to the branch for fallback alternate routes, see Branch PSTN call routing examples on page 325.	
13	Configure the type of voicemail system the branch will use.	See Voicemail operation on page 163.	
	Note: Numbers 14 through 22 are performed from Avaya Aura®Session Manager. B5800 Branch Gateway supports Session Manager 6.1 and 6.0 and procedures for both versions are provided.		
14	View a list of the SIP domains.	• For Session Manager 6.1, see Viewing the SIP domains on page 150. • For Session Manager 6.0, see Viewing the SIP domains on page 156.	
15	Create a location.	• For Session Manager 6.1, see Creating locations on page 150. • For Session Manager 6.0, see Creating locations on page 156.	
16	Create a digit adaptation.	• For Session Manager 6.1, see Creating adaptations on page 151. • For Session Manager 6.0, see Creating adaptations on page 157.	
17	Create a SIP entity.	• For Session Manager 6.1, see Creating SIP entities on page 151. • For Session Manager 6.0, see Creating SIP entities on page 157.	

#	Description	Section	✔
18	Create an entity link.	• For Session Manager 6.1, see Creating entity links on page 152. • For Session Manager 6.0, see Creating entity links on page 158	
19	Create a time range.	For Session Manager 6.1 or 6.0, see Creating time ranges on page 153.	
20	Create a routing policy.	• For Session Manager 6.1, see Creating routing policies on page 153. • For Session Manager 6.0, see Creating routing policies on page 159	
21	Create a dial pattern.	• For Session Manager 6.1, see Creating dial patterns on page 154. • For Session Manager 6.0, see Creating dial patterns on page 160	
22	If you are going to use Network Management to configure the branch, you can create a System Manager cut-through link to Network Management.	For Session Manager 6.1 or 6.0, see Creating a System Manager link to Network Management on page 161.	
23	Administer extensions	See Extension administration on page 173.	

Activating license files

About this task

B5800 Branch Gateway uses the Avaya Product Licensing and Delivery System (PLDS) to manage license entitlements. When you access PLDS and activate a license file, you are given the opportunity to save the license file to the local PC. Once saved on the local PC, you can send the license file to the branch in two ways — either through Provisioning and Installation Manager (PIM) or Manager. If using PIM, you load the license file to PIM and then create a job to send the license file to the B5800 Branch Gateway device. If using Manager, you select a locally saved license file and then upload the license file to the B5800 Branch Gateway device.

PIM provides a bulk provisioning feature where you can use a mapping file that contains a list of comma separated key value pairs of B5800 Branch Gateway IP addresses and license file names, one pair for each branch, to send licenses to multiple branches simultaneously. The

license file names are based on the Feature Key (FK) serial number on the SD cards. See Creating a mapping file on page 129 for more information.

Note:

B5800 Branch Gateway supports a 30-day grace period during which time the system is fully functional if a license error is detected or if a license file cannot be obtained, for example due to loss of WAN connectivity.

Procedure

1. See Activating license entitlements on page 209 to generate the licenses.
2. Depending upon which method you want to use to deliver the activated license files to each branch, see one of the following:
   - See Using Manager to deliver license files to the branches on page 126.
   - See Using Provisioning and Installation Manager to deliver license files to the branches on page 127.

Using Manager to deliver license files to the branches

Before you begin

License files have been activated. See Activating license entitlements on page 209.

About this task

You can use Manager to distribute activated license files to B5800 Branch Gateway sites. This procedure explains how to distribute the license files to a single branch at a time.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, select **PLDS License**.
3. Right-click **PLDS License** and select **Send license file to IP Office**.
4. In the Upload Files window, select the PLDS license xml file.
   Manager copies the license file to the B5800 Branch Gateway SD card where it is validated and stored for persistent use.
5. Select **File > Close Configuration**.
6. To view the license, select **File > Open Configuration**.

Deleting the PLDS license file from the branch

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, select **PLDS License**.
3. Right-click **PLDS License** and select **Delete PLDS License file from Avaya Branch Gateway**.
4. Select **File > Close Configuration**.

Using Provisioning and Installation Manager to deliver license files to the branches

Before you begin

License files have been activated. See Activating license entitlements on page 209.

About this task

Use this procedure to load the license files to Provisioning and Installation Manager (PIM) and then create a job to send the license files to the B5800 Branch Gateway branches. You can send license files to a single branch or to multiple branches simultaneously. You can also schedule when you want the job to run.

Procedure

1. From the Avaya Integrated Management Launch Products page, click **Provisioning and Installation Manager for IP Office**.
2. From the Provisioning and Installation Manager main window, select **Administration > Licenses** in the left panel.
3. Click **Add**.
4. In the PIM – Upload License file window, click the **Browse** button and select the .xml license file.
5. Click the **Upload file** button.
   The license file is uploaded to PIM and appears in the License Files List.

   Note:

   The license file is now stored in the Network Management server file system under \Program Files\Avaya\Network Management\CSV\IPOLicenses. PIM renamed the license file name to the format <*host ID of the SD card*>_HID.xml, for example **111306312781_HID.xml**. The host ID is the Feature Key (FK) serial number printed on the SD card. PIM renames the license file to one that identifies the respective device. If you have multiple license files, once you upload all the

license files, you can create a mapping file for bulk distribution. See Creating a mapping file on page 129 for more information.

6. To send the license file to the branch, from the Provisioning and Installation Manager main window, click **Import Licenses** at the top of the window.
   The Import Licenses Job Wizard appears.
7. On the General page, do the following:
   a) In the **Job Name** field, enter a name for this job.
   b) In the **Notes** field, enter notes about this job.
8. Click **Next**.
9. On the Import Licenses Wizard page, choose one of the following:
   - To select a mapping file, click the **Select Mapping File** option button and then click **Browse** to locate the mapping file.

     Note:
     Mapping files are used for bulk provisioning. See Creating a mapping file on page 129 for more information.
   - To select a device and license file from a list, do the following:
     1. Click the **Select Devices from list** option button.
     2. Click the check box for the device.
     3. From the corresponding drop-down box, select the license file name that matches the FK serial number printed on the SD card for the device.

     The IP address of the device is shown as well as the name of the license file associated with the device. The license file name is created from the host ID of the SD card and is in the format <*host ID of the SD card*>_HID.xml, for example **111306312781_HID.xml**. The host ID is the Feature Key (FK) serial number printed on the SD card.

     Note:
     Even if the license file name was changed at an earlier point, for example to make it shorter, the license file name that appears here is derived from the host ID of the SD card, not the file name as it was renamed.
10. Click **Next**.
11. On the Check Mapping List page, review the list and then click **Next**.
12. On the Schedule page, choose one of the following
    - Click the **Run now** option button to import the license files to the devices now.
    - Click the **Run the job on** option button to run the job at a specified date and time. Then do the following:

1. Click the date/time icon and select the date and time you want the job to run.
2. In Time Zone drop-down box, select the appropriate time zone.

- Click the **I'll schedule the job later** option button to schedule the job later.

13. Click **Next**.
14. On the Job Options page, do the following:
    a) Click the **Full execution** option button.
    b) Click the **Ignore Warnings** check box to deselect it so that warnings are not ignored during validation.
15. Click **Next**.
16. Review the summary, and then click **Next**.
17. Click **Finish**.
    The License Wizard closes. When the job is run, either now or on the date and time you specified, the license file(s) are pushed down to the designated devices using TFTP.
18. To view the status of a completed job, on the License Files List page, in the left navigation pane, select **Jobs > Completed**.
    The jobs that have completed are listed on the Completed Jobs page.

Creating a mapping file

About this task

If you have activated multiple license files in PLDS, you can create a mapping file that contains a list of comma separated key value pairs of B5800 Branch Gateway IP addresses and license file names, one pair for each branch. A mapping file is useful for bulk provisioning. When you distribute the license files to the branches, you have the opportunity to select the mapping file you created. Alternatively, you are also able to select devices from a list. See Using Provisioning and Installation Manager to deliver license files to the branches on page 127 for more information.

You can create a mapping file in advance by opening a text file and typing the device IP address and corresponding license file name for each device. The license file name is the Feature Key (FK) serial number printed on the SD card designated for that device. You would type the IP address/license file name for each device to which you want to send a license.

Alternatively, you can create the mapping file once the license files are imported into Provisioning and Installation Manager. Once imported, the license files are stored in the Network Management server file system under \Program Files\Avaya\Network Management \CSV\IPOLicenses. This method allows for less errors in the mapping file because you are able to copy the device IP address/license file name from the Network Management folder.

Procedure

1. Open a generic CSV text file.
2. Enter the B5800 Branch Gateway IP address and corresponding license file name in the following format: < *IP address of the device*>,< *License file name* >.

   Note:

   The license file name is comprised of the host ID of the SD card followed by _**HID.xml**, for example **111306312781_HID.xml**. The host ID is the Feature Key (FK) serial number printed on the SD card.
3. Repeat step 2 for each IP address/license file pair.

   Sample mapping file:

   ```
   148.147.206.251,111306312781_HID.xml
   148.147.206.160,111310198782_HID.xml
   148.147.175.145,111313365847_HID.xml
   ```
4. Save the file.

Disabling the Network Management administration feature for the branch

About this task

If you want to administer the branch through Manager and not through Network Management, you must disable the Network Management administration feature for the branch.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File** > **Advanced** > **Security Settings**.
3. In the Select IP Office window, click the check box for the appropriate system.
4. Click **OK**.
5. In the Security Service User Login window, enter a user name and password of an account that has security configuration access to the B5800 Branch Gateway system.

   The defaults are **security** and **securitypwd**.
6. In the Security Settings pane, select **Services**.
7. In the Services pane, select **Configuration**.
8. In the Service Details pane, click the check box for **Under ENM Administration** to deselect this option.

Note:

When Network Management is installed, this check box is checked by default and you are not able to administer the branch through Manager. To be able to use Manager to administer the branch, this check box must be unchecked.

9. Click **OK**.
10. Select **File > Save Configuration**.

Disabling unused trunks

About this task

Each B5800 Branch Gateway trunk card provides a fixed number of trunk ports with digital trunk ports supporting a fixed number of digital channels. By default th B5800 Branch Gateway configuration will have settings for all the possible trunks and channels.

In cases where the number of trunks or trunk channels in use is lower than the number supported by the trunk card, the unused trunks and channel must be disabled.

Important:

Failure to do this will cause problems with outgoing calls.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. For each line, set those lines or channels that are not connected or not being used as **Out of Service**.

   The location of the relevant setting varies for each trunk type.
4. For **Analog Trunks**, set the **Trunk Type** to **Out of Service**.
5. For **BRI, E1 PRI, S0 and QSIG Trunks**, set the channels quantities to match the actual subscribed channels.
6. For **T1, T1 PRI and E1R2 Trunks**, select the Channels tab. Then do the following:

a) Select those channels that are not used and click **Edit**.

- For T1 set the **Type** to **Out of Service**
- For T1 PRI set the **Admin** field to **Out of Service**.
- For E1R2 trunks set the **Line Signalling Type** to **Out of Service**.

7. Select **File > Save Configuration**.

Digital trunk clock source

About this task

Digital trunks require the telephone system at each end of the trunk to share a clock signal to ensure synchronization of call signalling. The B5800 Branch Gateway can obtain and use the clock signal from any of its digital trunks. Typically the clock signal provided by a digital trunk from the central office exchange is used as this will be the most accurate and reliable clock source.

To do this, the **Clock Quality** setting on each line in the B5800 Branch Gateway configuration is set to one of the following:

- **Network**

  If available, the clock signal from this trunk should be used as the B5800 Branch Gateway clock source for call synchronization. If several trunk sources are set as Network, the B5800 Branch Gateway will default to using one as detailed below.

- **Fallback**

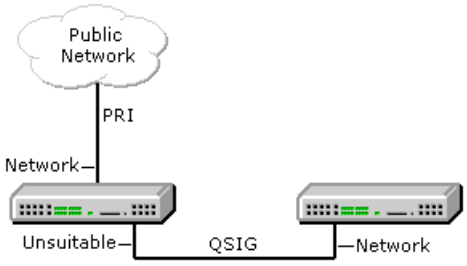
  If available, the clock signal from this trunk can be used as the clock source if none of the trunks set as Network are providing a clock source.

- **Unsuitable**

  The clock source from this trunk will never be used as the B5800 Branch Gateway clock source.

If no clock source is available the B5800 Branch Gateway can use its own internal clock if necessary.

In the example below the first B5800 Branch Gateway is set to use the public network trunk as its clock source and ignoring the possible clock source from the QSIG trunk. The other B5800 Branch Gateway system is using the clock signal received from the first B5800 Branch Gateway on its QSIG trunk as its clock source. Thus both systems are using the same clock source and that clock source is the public network exchange.



When multiple trunks with the same setting are providing clock signals, trunks are used in the order of slots 1 to 4 and then by port on each slot.

The current clock source being used by an B5800 Branch Gateway system is shown on the Resources page within the B5800 Branch Gateway System Status Application.

Setting a trunk clock quality setting

About this task

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. For each digital line, do the following:
   a) Select the line.
   b) On the **Line** tab, select whether that trunk should provide the clock source for the network or whether the trunk is unsuitable.

   Note:
   For E1R2 trunks the **Clock Quality** setting is on the **Advanced** tab
4. Ensure that only one trunk is set to **Network**. This should preferably be a direct digital trunk to the central office exchange.
5. Set one other trunk to **Fallback** in case the selected network trunk connection is lost.

   Note:
   If possible this should be a trunk from a different provider since that reduces the chances of both sources failing at the same time.
6. Ensure that all other digital trunks are set as **Unsuitable**.
7. Select **File > Save Configuration**.

Setting the trunk prefixes

About this task

Where a prefix has been implemented for outgoing calls, that same prefix needs to be added to trunk settings. The prefix is then used as follows:

- On incoming calls the prefix is added to any incoming ICLID received with the call. That allows the ICLID to be used by B5800 Branch Gateway phones and applications to make return calls.
- On outgoing calls, the short codes used to route the call to a trunk must remove the dialing prefix.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. For each line enter the prefix. The location of the relevant setting varies for each trunk type.
    - For analog trunks, select the **Line Settings** tab and enter the prefix in the **Prefix** field.
    - For T1 and T1 PRI trunks, select the **PRI 24 Line** tab and enter the prefix in the **Prefix** field.
    - For BRI, E1 PRI, S0 and QSIG trunks, select the **PRI Line** tab and enter the appropriate prefix in the following fields:
        - Prefix
        - National Prefix
        - International Prefix
4. Select **File > Save Configuration**.

SIP trunk prefixes

The prefix fields Prefix, National Prefix, Country Code and International Prefix are available with the SIP line settings. These fields are used in the following order:

1. If an incoming number (called or calling) starts with the + symbol, the + is replaced with the International Prefix.
2. If the Country Code has been set and an incoming number begins with that Country Code or with the International Prefix and Country Code, they are replaced with the National Prefix.
3. If the Country Code has been set and the incoming number does not start with the National Prefix or International Prefix, the International Prefix is added.
4. If the incoming number does not begin with either the National Prefix or International Prefix, then the Prefix is added.

For example, if the SIP line is configured with the following prefixes, the numbers are processed as described in the table below.

- Line Prefix: 9
- National Prefix: 90
- International Prefix: 900
- Country Code: 44

Number Received	Processing	Resulting Number
+441707362200	Following rule 1 above, the + is replaced with the International Prefix (900), resulting in 900441707362200. The number now matches the International Prefix (900) and Country Code (44). Following rule 2 above they are replaced with the National Prefix (90).	901707362200
00441707362200	Following rule 2 above the International Prefix (900) and the Country Code (44) are replaced with the National Prefix (90).	90107362200
441707362200	Following rule 2 above, the Country Code (44) is replaced with the National Prefix (90).	901707362200
6494770557	Following rule 3 above the International Prefix (900) is added.	9006494770557

Administering a Session Manager line for each branch

This section provides the procedures required to configure a Session Manager line between each branch site and the headquarters site.

This section also describes how the B5800 Branch Gateway uses a configured Session Manager line to handle incoming and outgoing calls to and from the branch and explains how a second Session Manager line can be configured for Session Manager line redundancy.

- See Enabling SIP trunk support on page 136. Use this procedure to configure the IP Office LAN interface which will be used for the Session Manager line connection to the Avaya Aura® Session Manager.
- See Setting the branch prefix and local number length for extension numbering on page 137. Use this procedure to set the prefix number for the B5800 Branch Gateway and the required extension length.
- See Changing the default codec selection on page 139. Use this procedure to set the preferred order for codec negotiation. This can be done as a system default and also for each individual SIP and Avaya Aura® Session Manager line.
- See Adding an Avaya Aura Session Manager line on page 141. Use this procedure to create a Session Manager line for calls to the Avaya Aura® Session Manager.
- See Setting up outgoing call routing on page 145. Use this procedure to create short codes for routing calls to the Avaya Aura® Session Manager line when the required destination or resource is on another branch of the Avaya Aura® network.
- See How the B5800 Branch Gateway uses a configured Session Manager line on page 147.

Enabling SIP trunk support

About this task

Before adding any SIP trunks, includingAvaya Aura® Session Manager lines, the B5800 Branch Gateway system must be configured for SIP trunk operation. The system has 2 LAN interfaces, LAN1 and LAN2 (the physical ports are labeled LAN and WAN respectively). Either can be used for the Avaya Aura® Session Manager line operation.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **LAN1** or **LAN2** tab as appropriate depending on which branch site LAN interface will be used for the data connection to the Avaya Aura® network.
4. Confirm that the IP address and IP Mask fields are set correctly for the site.
5. Click the **VoIP** tab.
6. Select the **SIP Trunks Enable** option. This is required for Avaya Aura® Session Manager trunk support.

   Note:

   The **SIP Registrar Enable** setting and settings in the **SIP Registrar** tab relate to SIP extension support and therefore do not affect Avaya Aura® Session Manager lines. The settings in the **Network Topology** tab relate to external SIP trunks. Those settings are not used by Avaya Aura® Session Manager lines, which use open internet across the customer WAN.
7. Click **OK**.
8. Select **File > Save Configuration**.
   The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Setting the branch prefix and local number length for extension numbering

About this task

Each B5800 Branch Gateway system in the network should have a unique branch number. That number is added as a prefix to the caller's extension number for calls routed to the Avaya Aura® Session Manager.

The prefix is also used in the Avaya Aura® Session Manager configuration to create unique dial patterns for routing calls to the appropriate B5800 Branch Gateway.

By default B5800 Branch Gateway systems use 3-digit extension numbering starting from 200. The existing allocated numbers can be changed in bulk using the **Tools > Extension Renumber** option. This will add or remove a set value from all existing extension numbers in the configuration.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.

3. Click the **System** tab.
4. Set the following fields as appropriate:
   - Branch Prefix
   - Local Number Length
   - Proactive
   - Reactive

   These 4 fields are the key settings for B5800 Branch Gateway operation. See System tab field descriptions on page 111 for more information.
5. Click **OK**.
6. Select **File > Save Configuration**.
   The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

System tab field descriptions

Name	Range or Default	Description
Branch Prefix	Range = 0 to 999999999	This number is used to identify the B5800 Branch Gateway system within the Avaya Aura® network. The branch prefix of each B5800 Branch Gateway system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. On calls routed via an Avaya Aura®Session Manager line, the branch prefix is added to the caller's extension number.
Local Number Length	Range = Blank (Off) or 3 to 9	This field sets the default length for extension numbers for extensions, users, and hunt groups added to the B5800 Branch Gateway configuration. Entry of an extension number of a different length will cause an error warning by Manager. The combined **Branch Prefix** and **Local Number**

Name	Range or Default	Description
		Length should not exceed 15 digits.
Proactive	Default = 60 seconds	The B5800 Branch Gateway sends regular SIP OPTION messages to the Avaya Aura®Session Manager line in order to check the status of the line. This setting controls the frequency of the messages when the Avaya Aura®Session Manager line is currently in service. Note that centralized extensions use their own settings.
Reactive	Default = 60 seconds	The B5800 Branch Gateway sends regular SIP OPTION messages to the Avaya Aura®Session Manager line in order to check the status of line. This setting controls the frequency of the messages when the Avaya Aura®Session Manager line is currently out of service. Note that centralized extensions use their own settings.

Changing the default codec selection

About this task

By default, all B5800 Branch Gateway IP trunks and extensions use automatic codec negotiation. The default negotiation order is G729(a) 8K CS-ACELP, G711 U-Law 64K, G711 A-Law 64K and G723.1 6K3 MP-MLQ.

If bandwidth between the B5800 Branch Gateway and Avaya Aura® sites is sufficient, we recommend that you change the first default preference to one of the G711 codecs. Note that the specific setting for individual branch trunks and extensions can be set to override the system setting if necessary.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **Telephony** tab.
4. Click the **Telephony** sub-tab.
5. In the **Automatic Codec Preference** drop-down box, select the appropriate setting.
   The **Automatic Codec Preference** setting is used to indicate the preferred codec order for trunks and extensions that are using automatic codec negotiation. See Automatic codec preference settings on page 113 for more information.
6. Click **OK**.
7. Select **File > Save Configuration**.
   The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Automatic codec preference settings

Setting	Selected Preference	2nd Preference	3rd Preference	4th Preference
G.729	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K	G723.1 6K3 MP-MLQ
G.723	G723.1 6K3 MP-MLQ	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K
G.711 U-Law	G711 U-Law 64K	G711 A-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ
G.711 A-Law	G711 A-Law 64K	G711 U-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ

Changing the maximum SIP sessions

About this task

The Maximum SIP Sessions setting limits the number of concurrent sessions allowed across all SIP trunks (public exchange and Session Manager). This setting must not exceed the number of SIP trunk sessions licensed in PLDS. If the PLDS license file is already installed, the Maximum SIP Trunk Sessions licensed for the system is identified on the PLDS screen when you select **PLDS License** on the left navigation pane. If the PLDS license file is not yet installed, you must still set this feature. This will determine the Avaya Branch Gateway

operation and system capacities during the 30-day grace period that is in effect when the system is in License Error Mode because the license is not yet installed. Once the PLDS license is installed, the Maximum SIP Session setting should be changed to match what appears on the PLDS screen. This will change the License Mode setting that appears on the PLDS screen to Normal Mode.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **Telephony** tab.
4. Click the **Telephony** sub-tab.
5. In the **Maximum SIP Sessions** drop-down box, select the number that matches the Maximum SIP Trunk Sessions licensed for the system.

   To see the Maximum SIP Trunk Sessions licensed for the system, in the left navigation pane, select **PLDS License**.
6. Click **OK**.
7. Select **File > Save Configuration**.

Adding an Avaya Aura® Session Manager line

About this task

Use this procedure to add an Avaya Aura®Session Manager line to the B5800 Branch Gateway system configuration. If multiple Avaya Aura®Session Managers are available at the headquarters site, an additional Avaya Aura® Session Manager line can be added for Session Manager line redundancy. See Avaya Aura Session Manager line redundancy on page 118 for more information.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Line**.
3. Click **New** and select **SM Line**.
4. Configure the line settings as appropriate. See Session Manager tab field descriptions on page 115 for more information.

5. Click **OK**.
6. Click the **VoIP** tab.
7. Click the **Allow Direct Media Path** check box to select this option.
8. Click the **Re-Invite Supported** check box to select this option.
9. Configure the remaining fields as appropriate. See VoIP tab field descriptions on page 116 for more information.
10. Click **OK**.
11. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Session Manager tab field descriptions

Name	Description
Line Number	This value is automatically assigned by B5800 Branch Gateway and should be unique for each line added to the configuration.
In Service	The default setting is enabled. This option can be used to manually take the Session Manager line out of service. It does not reflect or set the actual state of the line.
SM Domain Name	This name should match a SIP domain defined in the Session Manager system's SIP Domains table. Unless there are reasons to do otherwise, all the B5800 Branch Gateway systems in the Avaya Aura® network can share the same domain. **Note:** See Viewing the SIP domains on page 150 for a list of SIP domains defined in Session Manager.
SM Address	Enter the IP address of the Session Manager that the line should use in the Avaya Aura® network. The same Session Manager should be used for the matching Entity Link entry in the Avaya Aura® configuration.

Name	Description
Inactivity timeout (seconds)	The default setting is 0. Keep the default setting to maintain a persistent connection with Session Manager.
Outgoing Group ID	The default setting is 99999. This value is not changeable. However note the value as it is used in B5800 Branch Gateway short codes used to route calls to the Session Manager.
Prefix	This field is blank by default. This prefix will be added to any source number received with incoming calls.
Max Calls	The default setting is 10. This value sets the number of simultaneous calls allowed between B5800 Branch Gateway and Session Manager using this connection. Each call uses one of the available licenses that are shared by all SIP trunks configured in the system.
Network Configuration	These settings are fixed to **TCP** using send and receive ports **5060**.

VoIP tab field descriptions

Name	Range or Default	Description
Compression Mode	Default = Automatic Select	These settings are used to select the code negotiation order. • The default, **Automatic Select**, sets the line to use the codec order selected on the System > Telephony form. • The optionis in the drop-down list box are used to select which code should come first in the selection order of G729(a) 8K CS-ACELP > G711 U-Law 64K > G711 A-Law 64K > G723.1 6K3 MP-MLQ. Note that if one of the G711 options is selected as the first choice codec, the other

Name	Range or Default	Description
		G711 option is used as the second choice codec. • The **Advanced** option can be used to manually configure the codec preference order and specify which codecs are used.
Call Initiation Timeout	Default = 4 seconds	The B5800 Branch Gateway sends regular OPTION messages to each Avaya Aura®Session Manager line in order to check the lines in or out of service status. If a response is not received within this timeout, the line is treated as being out of service.
DTMF Support	Default = RFC2833	This setting is used to select the method by which DTMF key presses are signaled to the remote end. The supported options are **In Band**, **RFC2833** or **Info**.
VoIP Silence Suppression	Default = Off	When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods.
Fax Transport Support	Default = Off	This option is only selectable if the option **Re-Invite Supported** is also selected. If enabled, the B5800 Branch Gateway is able to support the sending and receiving of faxes via the Avaya Aura® Session Manager line using the T38 protocol. The settings for T38 are set on the T38 Fax tab.
Allow Direct Media Path	Default = On	This setting controls whether connected calls must remain routed via the B5800 Branch Gateway or can be routed

Name	Range or Default	Description
		alternately if possible within the network structure. • If enabled, connected calls can take routes other than through the B5800 Branch Gateway. This removes the need for a voice compression channel. • If disabled or not supported at one end of the call, the call is routed via the B5800 Branch Gateway. However RTP relay support allows calls between devices using the same audio codec to not require a voice compression channel.
Re-Invite Supported	Default = On	When enabled, Re-Invite can be used during a session to change the characteristics of the session, for example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk.
Use Offerer's Preferred Codec	Default = Off	Normally for SIP calls, the codec preference of the answering end is used. This option can be used to override that behavior and use the codec preferences offered by the caller.

Setting up outgoing call routing

About this task

For calls from extensions on the B5800 Branch Gateway system to other numbers within the network, system short codes are used to route the calls to the Avaya Aura® Session Manager line. The Avaya Aura® Session Manager then performs the routing to determine where the call should go.

Note:

See Branch PSTN call routing examples on page 325 for information on routing back to the branch for fallback alternate routes.

Ideally the number of such system short codes should be kept to a minimum and the same short codes used on all branches in order to ease maintenance. This is where using a uniform dial plan for all branches helps, as explained in Dial plan considerations on page 30. For our example, the uniform dial plan allows the same single short code to be used at all branches.

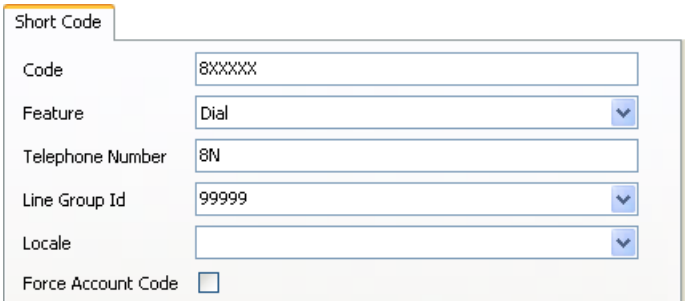
See the Manager context-based help for more information on creating short codes.

Note:

In the Distributed branch user model, when a short code match occurs and the telephone number to be sent to the Avaya Aura® Session Manager line begins with the B5800 Branch Gateway system's own branch prefix, the prefix is removed and the call is re-targeted locally on the B5800 Branch Gateway system.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Short Code**.
3. Click the **New** icon and select **Short Code**.



4. Configure the settings as appropriate. See Short Code tab field descriptions on page 121 for more information.

   Note:

   To view more information about the system short codes, press F1. In particular, see the description of the **Dial** short code.

5. Click **OK**.
6. Select **File > Save Configuration**.

Short Code tab field descriptions

Name	Description
Code	Enter the number dialed by users that should be matched to this short code. Use **X** wildcards for any single digit.
Feature	Leave this field set as **Dial**.
Telephone Number	Set this field to match a number that should be passed to the Avaya Aura® Session Manager for routing against its dialing pattern matches. The **N** wildcard can be used to match any wildcards in the **Code**. **Note:** Add SS to the entry in this field to have the caller ID passed to the Session Manager line. For example, if you are entering 8N in the Telephone Number field, enter 8NSS.
Line Group Id	Set the **Line Group ID** to match the **Outgoing Group** settings used in the SM lines URI setting.
Local	Features that transfer the caller to Voicemail Pro can indicate the language locale required for prompts. This is subject to the language being supported and installed on the voicemail server. The default is blank.
Force Account Code	When selected, for short codes that result in the dialing of a number, the user is prompted to enter a valid account code before the call is allowed to continue. The default is **Off**.

How the B5800 Branch Gateway uses a configured Session Manager line

Once configured and in operation, the Avaya Aura® Session Manager line is used as follows.

Outgoing calls from a branch

In the Distributed branch user model, if the outgoing call begins with the branch's own prefix, the prefix is removed and the call is targeted locally to the matching native user or hunt group

extension number. If there is no matching extension number, the call is targeted to any matching system short code.

Incoming calls to a branch

Incoming calls on an Avaya Aura®Session Manager line are treated as being internal calls and do not go through the B5800 Branch Gateway system's Incoming Call Route settings.

- If the destination of the incoming call on the Avaya Aura® Session Manager line starts with the system's branch prefix, the prefix is removed. The call is then targeted to the matching native user or hunt group extension number. If there is no matching extension number, the call is targeted to any matching system short code.
- If the destination of the incoming call on the Avaya Aura® Session Manager line does not start with the system's branch prefix, the whole number is checked for a match against system short codes.

Line status detection

The B5800 Branch Gateway system sends regular OPTION messages to any Avaya Aura® Session Manager lines in its configuration. The Proactive and Reactive settings on the B5800 Branch Gateway system's **System** tab set how often the OPTION messages are sent in seconds. The Proactive setting is used for an Avaya Aura® Session Manager line currently thought to be in service. The Reactive setting is used for an Avaya Aura® Session Manager line currently thought to be out of service.

- If a response is received and is not a 408, 500, 503 or 504 response, the Avaya Aura® Session Manager line is treated as in service; otherwise the line is treated as being out of service.
- If the line is out of service, and call comes from the trunk, the trunks status is changed back to in service.
- If the line is in service, a call may fail due to either being unable to deliver the message or receive a 100 response within a configured timeout. The line will not go out of service because this may be a temporary failure due to a busy system.
- In addition each Avaya Aura® Session Manager line can be manually set to in or out of service using the In Service option on the Avaya Aura® Session Manager line's **Session Manager** tab.

Chapter 8: Session Manager Configuration

The Session Manager procedures in this chapter are for configuring Session Manager for the B5800 Branch Gateway. The B5800 Branch Gateway supports Session Manager 6.1 and Session Manager 6.0. Depending on the Session Manager version you are using, see one of the following sections:

- Session Manager 6.1 on page 149
- Session Manager 6.0 on page 155

For more information about these Session Manager procedures, see “Chapter 5: Managing Session Manager routing” in *Administering Avaya Aura® Session Manager*, document number 03–603324.

Also provided in this chapter is a procedure to create a cut-through link from System Manager to Network Management. See Creating a System Manager link to Network Management on page 161 for more information.

Session Manager 6.1

The topics in this section provide procedures for configuring Session Manager 6.1 to support calls to and from B5800 Branch Gateway systems. Perform the following procedures:

1. View the SIP domains for which the Session Manager provides call management. Multiple domains can be listed. See Viewing the SIP domains on page 150.
2. Identify logical and/or physical locations where SIP entities reside. IP address patterns can be used to define different locations within the Avaya Aura® network, for example the IP address range of each B5800 Branch Gateway system. The creation of locations allows features such as bandwidth management to be applied to connections from those locations. See Creating locations on page 150.
3. Create a set of digit adaptations in order to ensure correct routing. If the digits to or from a branch need alteration in order to be routed correctly at either end, this can be done using a table of digit adaptations. Each SIP entity (branch) is associated with its own set of digit adaptations. See Creating adaptations on page 151.
4. Add each B5800 Branch Gateway system to the list of SIP entities that send calls to and from the Avaya Aura® network. See Creating SIP entities on page 151.
5. Add an entity link for each SIP entity including each B5800 Branch Gateway. An entity link must be added to define the ports and transport method used for connections between the SIP entity and the Session Manager. See Creating entity links on page 152.

6. Create time ranges to control when different routing policies are used. See Creating time ranges on page 153.
7. Add a routing policy. A routing policy consists of a selected SIP entity as its destination and a number of time ranges that define when the policy can be used. See Creating routing policies on page 153.
8. Add dial patterns. Dial patterns are used to match digits received to a destination. Each dial pattern has an associated routing policy that defines the target entity for matched calls and when the match should be used. See Creating dial patterns on page 154.

Note:

You must complete fields marked with an asterisk. Fields not marked with an asterisk are optional.

Viewing the SIP domains

The domain for which the Session Manager is authoritative was added when Session Manager was initially configured for the B5800 Branch Gateway system. The domain name set in the B5800 Branch Gateway system's Session Manager line configuration (see Adding an Avaya Aura Session Manager line on page 114) should match one of the entries that is listed on the Domain Management page.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Domains**.

   The SIP domains are listed on the Domain Management page.

Creating locations

Locations are used to identify logical and/or physical locations where SIP entities reside. The location entries in Session Manager allow bandwidth management and call control to be applied for connections to and from those locations.

Typically locations are added for each B5800 Branch Gateway branch site.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Locations**.
3. On the Location page, click **New** to add a new location.
4. On the Location Details page, in the **Name** field, enter a name to identify the location.
5. In the **Notes** field, enter notes about the location, as appropriate.

6. In the **Managed Bandwidth Units** field, accept the default setting.
7. In the **Total Bandwidth** field, accept the default setting, blank
8. In the **Default Audio Bandwidth** field, accept the default setting.
9. In the **Location Pattern** section, click **Add** to add a location pattern.
10. In the **IP Address Pattern** field, enter an IP address pattern that matches the IP LAN address range.

    The * character can be used as a match-all wildcard. For example, the pattern 192.168.42.* matches all addresses in the range 192.168.42.1 to 192.168.42.255.
11. In the **Notes** field, enter notes about this location pattern, as appropriate.
12. Click **Commit**.

Creating adaptations

Occasionally calls to or from the branch may require digit conversion in order to ensure correct routing. For example, reinserting an external dialing prefix. This is done using a set of digit conversions stored by the digit adaptation associated with the SIP entity.

Adaptations are optional and are deployment specific. For more information, see “Adaptations” in “Chapter 5: Managing Session Manager routing” in *Administering Avaya Aura®Session Manager*, document number 03–603324.

Creating SIP entities

A SIP entity is required for each branch system. This is in addition to the SIP entities that should already exist for Session Manager and Communication Manager Feature Server or Communication Manager.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **SIP Entities**.
3. On the SIP Entities page, click **New** to create a new SIP Entity.
4. On the SIP Entity Details page, in the **Name** field, enter the name of the SIP entity.
5. In the **FQDN or IP Address** field, enter the IP address of the B5800 Branch Gateway system LAN interface configured for the Session Manager line operation.
6. In the **Type** drop-down box, select **Survivability Server**.

7. In the **Notes** field, enter a description to help identify this SIP entity, as appropriate.
8. In the **Adaptation** drop-down box, select the adaptation that contains the digit conversions to apply to calls to and from the location.
9. In the **Location** drop-down box, select the location that matches the location you configured in Creating locations on page 150.
10. In the **Time Zone** drop-down box, select the time zone for the location.
11. For the **Override Port & Transport with DNS SRV** check box, accept the default setting, unchecked.
12. In the **SIP Timer B/F (in seconds)** field, accept the default setting, 4.

    Note:
    If you see that calls are abnormally terminated, you should increase this number.
13. In the **Credential Name** field, accept the default setting, blank.
14. In the **Call Detail Recording** field, accept the default setting.
15. In the **SIP Link Monitoring** drop-down box, accept the default, **Use Session Manager Configuration**.
16. Under **Port**, click **Add**.
17. In the **Port** field, enter `TCP`.
18. In the **Protocol** drop-down box, select **5060**.

    The port and protocol will be pushed to the phones along with the B5800 Branch Gateway IP address when this SIP entity is selected as the survivability server for the user (see Step 8e in Adding stations to Session Manager on page 185). This will be the port and protocol that the phones will use to connect to the B5800 Branch Gateway in rainy-day.
19. Click **Commit**.

Creating entity links

For each SIP entity communicating with the Avaya Aura® Session Manager, an entity link needs to be configured. That includes one for each B5800 Branch Gateway.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Entity Links**.
3. On the Entity Links page, click **New**.
4. In the **Name** field, enter a name to describe this link.

5. In the **SIP Entity 1** drop-down box, select the name of the Session Manager system that is at one end of the link.

   SIP Entity 1 must always be a Session Manager instance. For a Session Manager line from a B5800 Branch Gateway system, this should match the Session Manager set as the **SM Address** in the Session Manager line's configuration.

6. In the **Protocol** drop-down box, select **TCP**.

   When TCP is selected, the **Port** field is automatically set as **5060**. This is the port to which the SIP Entity 2 sends SIP requests.

7. In the **SIP Entity 2** drop-down box, select the name of the B5800 Branch Gateway system that is at the other end of the link.

   When you selected TCP in the previous step, the **Port** field was automatically set as **5060**.

8. Select the **Trusted** check box.

   This check box must be checked. If it is not checked, calls from the associated SIP Entity 2 will be denied by Session Manager.

9. In the **Notes** field, enter notes regarding this entity link, as appropriate.
10. Click **Commit**.

Creating time ranges

Additional time ranges can be created and used with a routing policy to define when the routing policy is active. For most B5800 Branch Gateway implementations, you do not need to define additional time ranges. If you need to add or adjust a time range, see "Creating Time Ranges" in *Administering Avaya Aura Session Manager*, document number 03-603324.

Creating routing policies

A routing policy is a collection of multiple time ranges and a destination SIP entity. For each dial pattern configured to route calls received by the Session Manager, the routing policy associated with that dial pattern defines when and where matching calls are directed.

Separate routing policies are required for each B5800 Branch Gateway entity to which the Session Manager routes calls. No routing policy is required for Communication Manager Feature Server systems.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Routing Policies**.
3. On the Routing Policies page, click **New** to create a new routing policy.

4. On the Routing Policies Details page, in the **Name** field, enter a name to describe this routing policy.
5. For the **Disabled** check box, accept the default, unchecked.
6. In the **Notes** field, enter notes about this routing policy, as appropriate.
7. In the **SIP Entity as Destination** section, do the following:
    a. Click **Select**.
    b. On the SIP Entity List page, select the SIP entity to which the routing policy applies.
    c. Click **Select**.
8. Skip the **Time of Day** section, **Dial Patterns** section, and **Regular Expressions** section. You do not need to configure these settings.
9. Click **Commit**.

Creating dial patterns

A dial pattern is defined to direct calls prefixed with the branch prefix to each branch.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Dial Patterns**.
3. On the Dial Patterns page, click **New** to create a new dial pattern.
4. On the Dial Pattern Details page, in the **Pattern** field, enter the branch prefix.

    This is the dialed number or number prefix that the dial pattern is intended to match.
5. In the **Min** field, enter the minimum length (1 to 36) of the dialed number that the pattern should match. For example, if the branch prefix is 3 digits and the extension number length is 4 digits, you would enter 7.
6. In the **Max** field, enter the maximum length (1 to 36) of the dialed number that the pattern should match. For example, if you set this to the same value as the **Min** value, the dial pattern will match only internal calls.
7. For the **Emergency Call** check box, leave the check box set to the default setting, unchecked.
8. In the **SIP Domain** drop-down box, select the appropriate SIP domains that should be matched, or select **All** to allow calls from all SIP domains to be routed.
9. In the **Notes** field, enter notes to describe this dial pattern, as appropriate.
10. In the **Originating Locations and Routing Policies** section, click **Add**.
11. In the **Originating Location** section, click the check box for **Apply The Selected Routing Policies to All Originating Locations**.

12. In the **Routing Policies** section, click the check box for the routing policy that was created for the branch.
13. Click **Select**.
14. If you need to specify that calls from certain locations be denied, do the following:
    a. In the **Denied Originating Locations** section, click **Add**.
    b. Do one of the following:
        • Click the **Apply to All Originating Locations** check box.
        • Click the check box(es) for the locations that should be denied.
    c. Click **Select**.
15. On the Dial Patterns Detail page, click **Commit**.

Session Manager 6.0

The topics in this section provide procedures for configuring Session Manager 6.0 to support calls to and from B5800 Branch Gateway systems. Perform the following procedures:

1. View the SIP domains for which the Session Manager provides call management. Multiple domains can be listed. See Viewing the SIP domains on page 156.
2. Identify logical and/or physical locations where SIP entities reside. IP address patterns can be used to define different locations within the Avaya Aura® network, for example the IP address range of each B5800 Branch Gateway system. The creation of locations allows features such as bandwidth management to be applied to connections from those locations. See Creating locations on page 156.
3. Create a set of digit adaptations in order to ensure correct routing. If the digits to or from a branch need alteration in order to be routed correctly at either end, this can be done using a table of digit adaptations. Each SIP entity (branch) is associated with its own set of digit adaptations. See Creating adaptations on page 157.
4. Add each B5800 Branch Gateway system to the list of SIP entities that send calls to and from the Avaya Aura® network. See Creating SIP entities on page 157.
5. Add an entity link for each SIP entity including each B5800 Branch Gateway. An entity link must be added to define the ports and transport method used for connections between the SIP entity and the Session Manager. See Creating entity links on page 158.
6. Create time ranges to control when different routing policies are used. See Creating time ranges on page 153.

7. Add a routing policy. A routing policy consists of a selected SIP entity as its destination and a number of time ranges that define when the policy can be used. See Creating routing policies on page 159.
8. Add dial patterns. Dial patterns are used to match digits received to a destination. Each dial pattern has an associated routing policy that defines the target entity for matched calls and when the match should be used. See Creating dial patterns on page 160.

Note:

You must complete fields marked with an asterisk. Fields not marked with an asterisk are optional.

Viewing the SIP domains

The domain for which the Session Manager is authoritative was added when Session Manager was initially configured for the B5800 Branch Gateway system. The domain name set in the B5800 Branch Gateway system's Session Manager line configuration (see Adding an Avaya Aura Session Manager line on page 114) should match one of the entries that is listed on the Domain Management page.

1. On the System Manager console, in the left navigation pane, select **Routing > Domains**.

   The SIP domains are listed on the Domain Management page.

Creating locations

Locations are used to identify logical and/or physical locations where SIP entities reside. The location entries in Session Manager allow bandwidth management and call control to be applied for connections to and from those locations.

Typically locations are added for each B5800 Branch Gateway branch site.

1. On the System Manager console, in the left navigation pane, select **Routing > Locations**.
2. On the Location page, click **New** to add a new location.
3. On the Location Details page, in the **Name** field, enter a name to identify the location.
4. In the **Notes** field, enter notes about the location, as appropriate.
5. In the **Managed Bandwidth** field, accept the default setting, blank.
6. In the **Average Bandwidth per call** field, accept the default setting.
7. In the **Location Pattern** section, click **Add** to add a location pattern.

8. In the **IP Address Pattern** field, enter an IP address pattern that matches the IP LAN address range.

   The * character can be used as a match-all wildcard. For example, the pattern 192.168.42.* matches all addresses in the range 192.168.42.1 to 192.168.42.255.

9. In the **Notes** field, enter notes about this location pattern, as appropriate.
10. Click **Commit**.

Creating adaptations

Occasionally calls to or from the branch may require digit conversion in order to ensure correct routing. For example, reinserting an external dialing prefix. This is done using a set of digit conversions stored by the digit adaptation associated with the SIP entity.

Adaptations are optional and are deployment specific. For more information, see “Adaptations” in “Chapter 5: Managing Session Manager routing” in *Administering Avaya Aura®Session Manager*, document number 03–603324.

Creating SIP entities

A SIP entity is required for each branch system. This is in addition to the SIP entities that should already exist for Session Manager and Communication Manager Feature Server or Communication Manager.

1. On the System Manager console, in the left navigation pane, select **Routing > SIP Entities**.
2. On the SIP Entities page, click **New** to create a new SIP Entity.
3. On the SIP Entity Details page, in the **Name** field, enter the name of the SIP entity.
4. In the **FQDN or IP Address** field, enter the IP address of the B5800 Branch Gateway system LAN interface configured for the Session Manager line operation.
5. In the **Type** drop-down box, select **SIP Trunk**.
6. In the **Notes** field, enter a description to help identify this SIP entity, as appropriate.
7. In the **Adaptation** drop-down box, select the adaptation that contains the digit conversions to apply to calls to and from the location.
8. In the **Location** drop-down box, select the location that matches the location you configured in Creating locations on page 150.

9. In the **Time Zone** drop-down box, select the time zone for the location.
10. For the **Override Port & Transport with DNS SRV** check box, accept the default setting, unchecked.
11. In the **SIP Timer B/F (in seconds)** field, accept the default setting, 4.

    Note:
    If you see that calls are abnormally terminated, you should increase this number.
12. In the **Credential Name** field, accept the default setting, blank.
13. In the **Call Detail Recording** field, accept the default setting.
14. In the **SIP Link Monitoring** drop-down box, accept the default, **Use Session Manager Configuration**.
15. Click **Commit**.

Creating entity links

For each SIP entity communicating with the Avaya Aura® Session Manager, an entity link needs to be configured. That includes one for each B5800 Branch Gateway.

1. On the System Manager console, in the left navigation pane, select **Routing > Entity Links**.
2. On the Entity Links page, click **New**.
3. In the **Name** field, enter a name to describe this link.
4. In the **SIP Entity 1** drop-down box, select the name of the Session Manager system that is at one end of the link.

   SIP Entity 1 must always be a Session Manager instance. For a Session Manager line from a B5800 Branch Gateway system, this should match the Session Manager set as the **SM Address** in the Session Manager line's configuration.
5. In the **Protocol** drop-down box, select **TCP**.

   When TCP is selected, the **Port** field is automatically set as **5060**. This is the port to which the SIP Entity 2 sends SIP requests.
6. In the **SIP Entity 2** drop-down box, select the name of the B5800 Branch Gateway system that is at the other end of the link.

   When you selected TCP in the previous step, the **Port** field was automatically set as **5060**.
7. Select the **Trusted** check box.

This check box must be checked. If it is not checked, calls from the associated SIP Entity 2 will be denied by Session Manager.

8. In the **Notes** field, enter notes regarding this entity link, as appropriate.
9. Click **Commit**.

Creating time ranges

Additional time ranges can be created and used with a routing policy to define when the routing policy is active. For most B5800 Branch Gateway implementations, you do not need to define additional time ranges. If you need to add or adjust a time range, see “Creating Time Ranges” in *Administering Avaya Aura Session Manager*, document number 03-603324.

Creating routing policies

A routing policy is a collection of multiple time ranges and a destination SIP entity. For each dial pattern configured to route calls received by the Session Manager, the routing policy associated with that dial pattern defines when and where matching calls are directed.

Separate routing policies are required for each B5800 Branch Gateway entity to which the Session Manager routes calls. No routing policy is required for Communication Manager Feature Server systems.

1. On the System Manager console, in the left navigation pane, select **Routing > Routing Policies**.
2. On the Routing Policies page, click **New** to create a new routing policy.
3. On the Routing Policies Details page, in the **Name** field, enter a name to describe this routing policy.
4. For the **Disabled** check box, accept the default, unchecked.
5. In the **Notes** field, enter notes about this routing policy, as appropriate.
6. In the **SIP Entity as Destination** section, do the following:
    a. Click **Select**.
    b. On the SIP Entity List page, select the SIP entity to which the routing policy applies.
    c. Click **Select**.
7. Skip the **Time of Day** section, **Dial Patterns** section, and **Regular Expressions** section. You do not need to configure these settings.
8. Click **Commit**.

Creating dial patterns

A dial pattern is defined to direct calls prefixed with the branch prefix to each branch.

1. On the System Manager console, in the left navigation pane, select **Routing > Dial Patterns**.
2. On the Dial Patterns page, click **New** to create a new dial pattern.
3. On the Dial Pattern Details page, in the **Pattern** field, enter the branch prefix.

   This is the dialed number or number prefix that the dial pattern is intended to match.
4. In the **Min** field, enter the minimum length (1 to 36) of the dialed number that the pattern should match. For example, if the branch prefix is 3 digits and the extension number length is 4 digits, you would enter 7.
5. In the **Max** field, enter the maximum length (1 to 36) of the dialed number that the pattern should match. For example, if you set this to the same value as the **Min** value, the dial pattern will match only internal calls.
6. For the **Emergency Call** check box, leave the check box set to the default setting, unchecked.
7. In the **SIP Domain** drop-down box, select the appropriate SIP domains that should be matched, or select **All** to allow calls from all SIP domains to be routed.
8. In the **Notes** field, enter notes to describe this dial pattern, as appropriate.
9. In the **Originating Locations and Routing Policies** section, click **Add**.
10. In the **Originating Location** section, click the check box for **Apply The Selected Routing Policies to All Originating Locations**.
11. In the **Routing Policies** section, click the check box for the routing policy that was created for the branch.
12. Click **Select**.
13. If you need to specify that calls from certain locations be denied, do the following:
    a. In the **Denied Originating Locations** section, click **Add**.
    b. Do one of the following:
       - Click the **Apply to All Originating Locations** check box.
       - Click the check box(es) for the locations that should be denied.
    c. Click **Select**.
14. On the Dial Patterns Detail page, click **Commit**.

Creating a System Manager link to Network Management

About this task

You are able to use Avaya Aura® Session Manager Release 6.x, cut-through capability to access Network Management. The System Manager cut-through allows the provisioning of the Network Management IP address with a unique menu name within the System Manager GUI. Although System Manager and Network Management must be installed on two separate servers, there is a single access interface for administration and management of the B5800 Branch Gateway.

Procedure

1. Depending on the version of Session Manager you are using, do one of the following:
   - For Session Manager 6.1, on the System Manager console, under **Elements**, select **Application Management**. Then, in the left navigation pane, click **Other Applications**.
   - For Session Manager 6.0, on the System Manager console, on the left navigation pane, select **Elements > Application Management > Other Applications**.
2. On the Manage Elements page, click **New**.
3. On the New Other Applications Instance page, in the **Application** section, do the following:
   a) In the **Name** field, enter a name for this cut-through link.
   b) In the **Type** drop-down box, accept the default, **Other Applications**.

      Note:
      The content in this field is hard-coded and not selectable.
   c) In the **Description** field, enter a description of this cut-through link.
   d) In the **Node** field, enter the IP address of the Network Management server.
4. Expand the **Access Point** section, and do the following:

   Note:
   In Session Manager 6.0, the **Access Point** section appears after the **Port** section.

   a) Click **New**.
   b) In the **Name** field, enter the name of the access point.
   c) In the **Access Point Type** drop-down box, select **EMURL**.
   d) In the **Protocol** drop-down box, select the appropriate protocol.
   e) In the **Host** field, enter the IP address of the Network Management server.

f) In the **Port** field, enter 443.
g) In the **URI** field, enter `/cgi-bin/launch_products.pl`.
h) In the **Order** field, enter the order in which the access points are accessed.
i) In the **Description** field, enter a description of this access point.
j) Click **Save**.

5. Expand the **Port** section, and do the following:

a) Click **New**.
b) In the **Name** field, enter the name of the port.
c) In the **Protocol** drop-down box, select the appropriate protocol.
d) In the **Port** field, enter 443.
e) In the **Description** field, enter a description about the port.
f) Click **Save**.

6. Click **Commit**.

Chapter 9: Voicemail operation

The B5800 Branch Gateway system uses its Embedded Voicemail by default. However, a number of other voicemail options are supported.

- **Embedded Voicemail** — Embedded Voicemail uses the system SD card in the B5800 Branch Gateway system control unit for storage of prompts and messages. Embedded Voicemail supports mailboxes for all local extension numbers, announcements to waiting callers, and auto attendants (up to 40) for external calls. Its capacity is limited to 15 hours of recorded messages, prompts and announcements. At least one Embedded Messaging Port license must be purchased to enable this service.
- **Voicemail Pro** — Voicemail Pro runs on a server PC connected to the B5800 Branch Gateway system and provides a wide range of features. Voicemail Pro is the only option that supports manual call recording for the B5800 Branch Gateway system users. It also supports automatic call recording for the B5800 Branch Gateway system. At least one Voicemail Pro license must be purchased to enable this service.
- **Modular Messaging** — The B5800 Branch Gateway system can be configured to use Modular Messaging as its voicemail server. When Modular Messaging is used as the central voicemail system, at each branch you have the option to still use the local Embedded Voicemail for auto attendant operation and for announcements to waiting calls. See Configuring Modular Messaging on page 164 for more information. Note that for this configuration, Embedded Voicemail licenses are required.

For more information about licensing, see Licensing on page 16.

Feature	Embedded Voicemail	Voicemail Pro	Modular Messaging
Maximum Simultaneous Users	6	40	Depends on the number of licensed Session Manager line channels.
Capacity	15 hours	1MB per minute disk space.	–
Auto Attendants	Yes (40)	Yes (unlimited)	Yes*
Call Recording	No	Yes	No
Announcements	Yes	Yes	Yes*
Visual Voicemail	Yes	Yes	Yes

*Provided using the local Embedded Voicemail.

Configuring Modular Messaging

About this task

The B5800 Branch Gateway system can be configured to use Modular Messaging as its voicemail server.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Modular Messaging over SIP**.

   Note:
   Fields applicable to this mode of voicemail support remain enabled.
5. Check the **Use embedded for AA and Announcements** check box to enable the local B5800 Branch Gateway system features for Embedded Voicemail auto attendants and announcements. The announcements are those that the callers hear when the call in on hold.

   Note:
   You must also enable the announcements. Do this by selecting the check box for **Announcements On** which appears when you select **Hunt Group > Announcements** tab.
6. In the **MM Number** field, enter the extension number configured for mailbox access to the Modular Messaging system. Note that this number is automatically routed via the active Avaya Aura®Session Manager line. It does not need to be routed through the normal branch call routing.
7. In the **MM PSTN Number** field, enter the PSTN number to which you want to reroute attempts to access mailboxes when the Avaya Aura®Session Manager line(s) are out of service. (This field is optional.)

   This number needs to be a valid DID number from the branch to the Modular Messaging system. When calls to access voicemail are routed by this method, the caller will be prompted by Modular Messaging to indicate the action they are performing (leaving or collecting messages) and the target mailbox.

   Depending on the call routing being used by the branch system for external PSTN calls, you may need to do additional configuration to ensure that this number is routed via a branch PSTN trunk. See Modular Messaging PSTN Fallback on page 165 for more information.

8. In the **Maximum Record Time** field, use the up and down arrows to set the maximum recording length in seconds for recorded announcement and auto attendant prompts.

   Note:

   You can set a number in this field only if **Use embedded for AA and Announcements** is checked.

9. Click **OK**.
10. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Modular Messaging PSTN Fallback

When the branch is configured to use Modular Messaging for its voicemail services, that configuration includes setting an internal Modular Messaging number (800700 for the following example) for calls to Modular Messaging which are automatically routed via the Session Manager line.

An additional Modular Messaging PSTN number can also be configured for use when the Session Manager line is not in service (915553800701 for the following example). However, it may also require additional configuration to ensure that this number is correctly routed to a branch PSTN trunk. That could be done using a system short code, but doing it in the ARS form keeps all the branch PSTN call routing in one place for ease of maintenance.

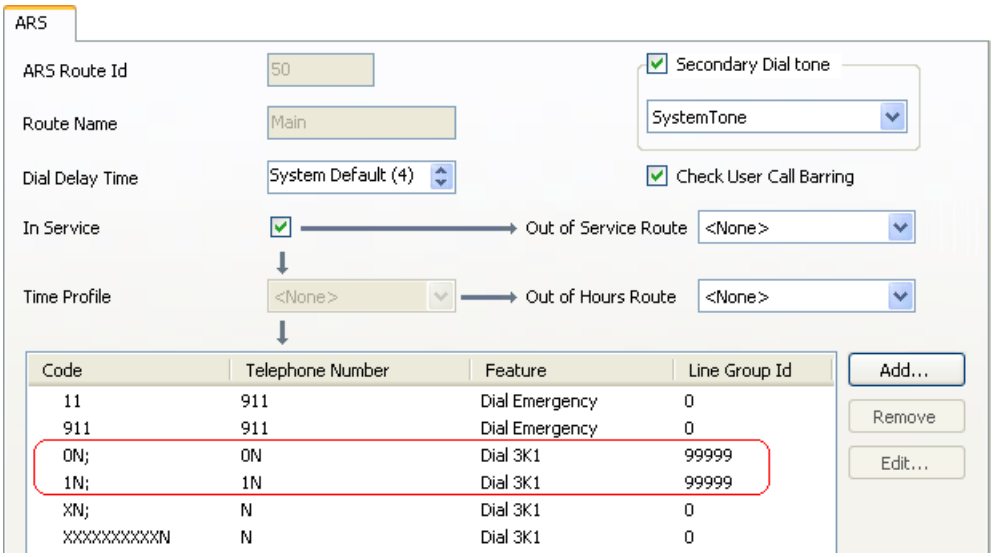
Adding an overriding short code

About this task

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **ARS**.

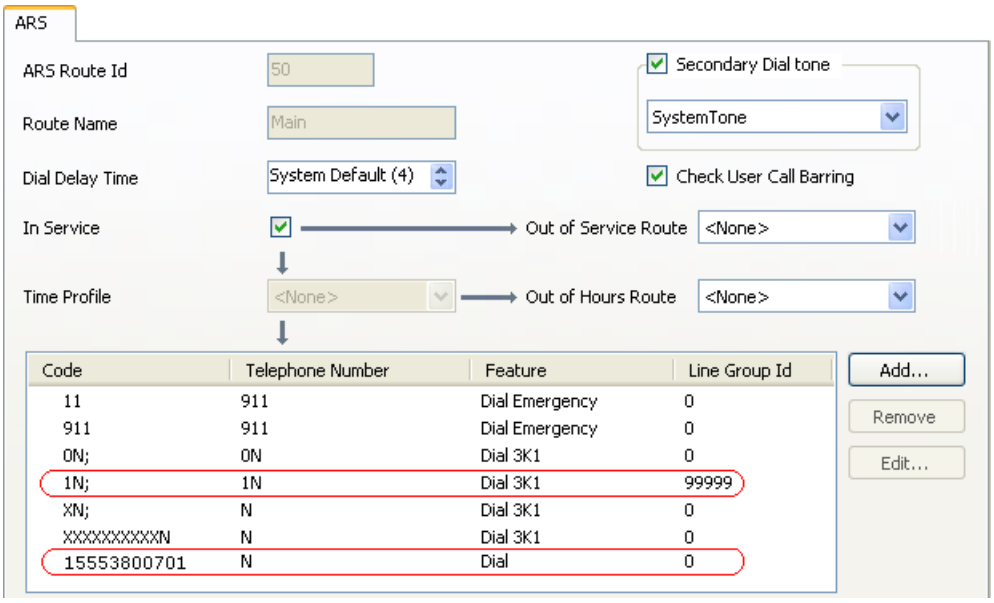
3. Click **50: Main**.



Within the ARS form, the default **1N;** short code is the one used for national calls. It would match the MM PSTN Number and attempt to route it to the SM Line which we know is out of service if the MM PSTN Number is being used for calls to voicemail. We can change the routing by adding a specific short code for the MM PSTN Number.

4. To add a short code, click the **Add...** button.
5. Make the changes as follows:
   a) In the **Code** field, set this to match the external PSTN number for Modular Messaging without the external dialing prefix.
   b) In the **Feature** drop-down box, select **Dial3K1**.
   c) In the **Telephone Number** field, set this to **N** to match the whole number in the **Code** field.
   d) In the **Line Group Id** drop-down box, select the line group ID being used for the branch's PSTN trunks. The default is 0.
6. Click **OK**.
   The ARS now has two short codes that will potentially match external national calls. However, one is a more exact match for certain calls and therefore will be applied

to those calls.



7. Click **OK**.
8. Select **File > Save Configuration**.

Embedded Voicemail for auto attendants and announcements

If Modular Messaging is used as the central voicemail system, you are able to still use the local Embedded Voicemail for auto attendant operation and for announcements to waiting calls. The procedures required to configure the auto attendant are provided in this section.

For more information about Embedded Voicemail, see *IP Office Release 6.1 Embedded Voicemail Installation*, document number 15-601067. Also refer to the Manager on-line help.

Creating an auto attendant

About this task

Note:

If you are going to use time profiles in the auto attendant, the time profile has to be created before creating the auto attendant. For more information, see the Manager on-line help.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, right-click **Auto Attendant** and select **New**.
3. In the **Auto Attendant** tab, do the following:
   a) In the **Name** field, enter the name of the auto attendant. The name can be up to 15 characters in length.

      External calls can be routed to the auto attendant by entering AA:*Name* in the destination field of an Incoming Call Route.
   b) In the **Maximum Inactivity** field, use the up and down arrows to select a number. The default is 8.

      This field sets how long after playing the prompts the auto attendant should wait for a valid key press. If exceeded, the caller is either transferred to the fallback extension set within the Incoming Call Route used for their call or the caller is disconnected.
   c) Accept the default setting, **on**, for **Enable Local Recording**.

      If set to **off** (unchecked) the use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings.
   d) The number in the **AA Number** field is assigned by the B5800 Branch Gateway system and cannot be changed. It is used in conjunction with short codes to access the auto attendant service or to record auto attendant greetings.
   e) For the **Direct Dial-By-Number** check box, select one of the following:

      - Select the check box if you want the key press for the action to be included in any following digits dialed by the caller for extension matching. For example, if 2 is set in the actions to Dial by Number, a caller can dial 201 for extension 201.
      - Do not select the check box (the default setting) if you do not want the key press for the action to be included in any following digits dialed by the caller for extension matching. For example, if 2 is set in the actions to Dial by Number, a caller must dial 2 and then 201 for extension 201.

   f) In the **Dial By Name Match Order** drop-down box, depending on how you want the names to appear for the Dial by Name function, select one of the following:

      - Select **First then Last**.
      - Select **Last then First**.

   g) Complete the **Morning**, **Afternoon**, **Evening**, and **Menu Options** fields as appropriate.

      Each auto attendant can consist of three distinct time periods, defined by associated time profiles. A greeting can be recorded for each period. The

appropriate greeting is played to callers and followed by the Menu Options greeting which should list the available actions.

- **Time Profile** — defines each period of auto attendant operation. When there are overlaps or gaps between time profiles, precedence is given in the order morning, afternoon and then evening.
- **Recording Name** — appears next to the short code used for manually recording auto attendant prompts. It is only used if using pre-recorded .wav files as greetings rather than manually recording greetings using the indicated short codes. If used, note that the field is case sensitive and uses the name embedded within the .wav file header rather than the actual file name. The utility for converting .wav files to the correct format is provided with Manager and can be launched by selecting **File > Advanced > LVM Greeting Utility**. Files then need to be manually transferred to the embedded voicemail memory card.
- **Shortcode** — indicates the system short codes automatically created to allow recording of the time profile greetings and the menu options prompt.

4. Click the **Actions** tab to define the actions available to callers depending on which DTMF key they press. Do the following:
   a) To define the auto attendant action when the **0** key is pressed, click the row that begins with **0**.
   b) Click **Edit**.
   c) In the **Action** drop-down box, select the appropriate action.

      Note:
      See the Manager on-line help for a description of each action.
   d) In the **Destination** drop-down box, select the appropriate destination.
   e) Click **OK**.
   f) Repeat steps a through e for each key that requires a definition for this auto attendant.
5. Click **OK** to save the auto attendant.

   Note:
   Short codes are automatically created for the auto attendant and the codes can be viewed in the **Auto Attendant** tab.
6. Select **File > Save Configuration** to save the changes back to the B5800 Branch Gateway system.
7. Following the system reboot, you can record prompts for the auto attendant using the short codes created. For more information, see Recording prompts on page 170.

Recording prompts

About this task

When a new auto attendant is created, a number of short codes are automatically added to the system short codes table. The short codes allow the recording of the various auto attendant prompts. The appropriate number to dial is indicated against each greeting on the **Auto Attendant** tab in Manager.

The telephone number part takes the form **"AA:*Name.x*"** where ***N*** is the auto attendant number and ***x*** is **1** for the morning greeting, **2** for the afternoon greeting, **3** for the evening greeting, and **4** for the menu options prompt.

When using any of these short codes, you hear the options:

- **1** to hear the current prompt.
- **2** to record a new prompt.
- **3** to save the new prompt.

Note:

- To prevent abuse of these default short codes, they can be deleted or changed. They can also be removed from the system short codes section and rebuilt in the user short codes of a trusted user. Alternately, disabling the Enabling Local Recording option stops the use of short codes to record the auto attendant greetings.
- Using the Dial feature, the short codes can be assigned to a programmable button. This allows quick access and recording of any prompts that change frequently.

Recording announcements

About this task

There are no default queue announcements for user and hunt groups. The maximum length for announcements is 10 minutes.

There are two default short codes that enable you to record announcements. The default short codes are:

- ***91N; / N".1" / Record Message**

  Used to record an announcement 1. For example, to record announcement 1 for a hunt group on extension 300 dial ***91300#** and follow the instructions to record the new announcement.

- ***92N; / N".2" / Record Message**

  Used to record an announcement 2. For example, to record announcement 2 for a hunt group on extension 300 dial *92300# and follow the instructions to record the announcement.

Transferring recordings to the system SD card

About this task

Use this procedure to manually copy the pre-recorded prompts and announcements onto the system SD card.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File > Advanced > Embedded File Management**.
3. Drag and drop the recording into the folder **dynamic\lvmail\AAG** on the system SD card.

Chapter 10: Extension administration

This chapter provides the procedures to administer native and survivable extensions. When the B5800 Branch Gateway is deployed in the Distributed Branch user model, the extensions are referred to as native extensions. When the B5800 Branch Gateway is deployed in the Centralized Branch user model, the extensions are referred to as survivable extensions. Each B5800 Branch Gateway system can support extensions using the Centralized Branch user model and extensions using the Distributed Branch user model at the same time. This is referred to as the Mixed Branch user model. So there can be both survivable extensions and native extensions configured for a system. For more information about the branch user deployment models, see Branch user deployment models on page 13.

To administer extensions, see:

Native extensions

Native extensions can support different types of telephones. For a list of supported telephones, see Supported telephones on page 21. Voicemail for native extensions is provided at the local branch, from Embedded Voicemail, Voicemail Pro, or Modular Messaging. For more information about voicemail, see Voicemail operation on page 163.

Native extension configuration checklist

Use this checklist to monitor your progress as you administer native extensions.

#	Description	Section	✔
1	Enable SIP extension support on the branch.	See Enabling branch SIP extension support on page 174.	
2	Add SIP extensions and users to the branch.	See Adding extensions and users to the B5800 Branch Gateway on page 176.	

Enabling branch SIP extension support

About this task

Before adding any SIP extensions, the B5800 Branch Gateway system must be enabled for SIP extension support. Use this procedure to configure the B5800 Branch Gateway to support the addition of SIP extensions.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **LAN1** or **LAN2** tab, depending on which branch site LAN interface will be used for the SIP extensions.
4. Make a note of the IP Address and IP Mask details as these will be required during the SIP extension configuration.
5. Click the **VoIP** tab.
6. Check the **SIP Registrar Enable** check box. This is necessary for support of SIP extensions directly by the branch or when providing survivability support for Avaya Aura® SIP extensions.
7. Click **OK**.
8. Click the **SIP Registrar** tab.
9. Confirm the **Auto-create Extn/User** check box is checked.

   For native extensions, this setting should be enabled.
10. Configure the remaining fields on this tab as appropriate. See SIP Registrar tab field descriptions on page 175 for more information.
11. Click **OK**.
12. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

SIP Registrar tab field descriptions

Name	Default	Description
Domain Name	Default = Blank	This is the local SIP registrar domain name that will be needed by SIP devices in order to register with the B5800 Branch Gateway. If this field is left blank, registration is against the LAN IP address. For our examples we have been using a domain, **example.com**.
Layer 4 Protocol	Default = Both TCP & UDP	This is the transport protocol for SIP traffic between the B5800 Branch Gateway and SIP extension devices.
TCP Port	Default = 5060	This is the SIP port if using TCP.
UDP Port	Default = 5060	This is the SIP port if using UDP.
Challenge Expiry Time (sec)	Default = 10	The challenge expiry time is used during SIP extension registration. When a device registers, the SIP Registrar will send a challenge back to the device and waits for an appropriate response. If the response is not received within this timeout the registration is failed.
Auto-create Extn/User	Default = On	• For survivable extensions, it is strongly recommended that this setting is disabled. SIP extensions should only be allowed to register with the B5800 Branch Gateway system if they match existing extension and user entries in the configuration. If a centralized (survivable) extension is allowed to

Name	Default	Description
		auto create matching entries, the extension's **Extension Mode** setting defaults to **Local** (native) which is incorrect for a centralized (survivable) extension. • For local (native) extensions, this setting can be enabled.

Adding extensions and users to the B5800 Branch Gateway

About this task

For each native extension, matching extension and user entries must be added to the B5800 Branch Gateway configuration. The required information is the extension number, the user name and the user password. These values must match those used by the extension user when logging into the B5800 Branch Gateway system during normal operation. Sufficient Enterprise Branch User licenses must exist for the native extensions to register when required.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Extension**.
3. Click the **New** icon and select the appropriate extension type.
4. Click the **Extn** tab.
5. Configure the fields as appropriate. See Extn tab field descriptions on page 178 for more information.
6. Click **OK**.
7. In the left navigation pane, click **User**.
8. Click the **New** icon and select **User**.
9. Click the **User** tab.
10. In the **Name** field, enter the same user name used for the native extension login to B5800 Branch Gateway.
11. In the **Extension** field, enter the Base Extension setting used for the SIP extension entry.

Note:

The full range of B5800 Branch Gateway user settings can be configured for a native extension. However the key settings are the **Name** and **Extension** fields.

12. Click **OK**.
13. Click the **Telephony** tab.
14. Click the **Call Settings** tab.
15. Click the **Call Waiting On** check box to select this option. This setting is required to allow features such as transferring calls.
16. Click **OK**.
17. To administer Embedded Voicemail or Voicemail Pro settings, click the **Voicemail** tab and do the following:
    a) In the **Voicemail Code** field, enter a code (1 to 15 digits) used by the voicemail server to validate access to this mailbox.

       If remote access is attempted to a mailbox that does not have a voicemail code set, the prompt "remote access is not configured on this mailbox" is played.
    b) In the **Confirm Voicemail Code** field, enter the code again.
    c) If you want to enable the voicemail email service, in the **Voicemail email** field, enter the user or group email address. Then select one of the following:
       - If you want to turn this feature off at this time, click the **Off** button.
       - If you want a copy of the message emailed to the email address, click the **Copy** button.

         Each time a new voicemail message is received in the voicemail mailbox, a copy of the message is attached to an email and sent to the email address.
       - If you want the message emailed to the email address, click the **Forward** button.

         Each time a new voicemail message is received in the voicemail mailbox, that message is attached to an email and sent to the email address. No copy of the voicemail message is retained in the voicemail mailbox and there is no message waiting indication.
       - If you want a simple email sent to the email address, click the **Alert** button.

         Each time a new voicemail message is received in the voicemail mailbox, a simple email message is sent to the email address. This is an email message announcing details of the voicemail message but without a copy of the voicemail message attached.
    d) Ensure that the **Voicemail On** option is selected.

       When on, the mailbox is used by the B5800 Branch Gateway system to answer the user's unanswered calls or calls when the user's extension is busy. Note

that if you do not select this feature, the user's mailbox is not disabled. Messages can still be forward to their mailbox and recordings can be placed in it. The mailbox can also still be accessed to collect messages.

e) If you want users retrieving messages to automatically hear the prompt "For help at any time press 8" , check the **Voicemail Help** check box.

If switched off, users can still press **8** for help.

f) If, when a new message is received, you want the voicemail server to call the user's extension to attempt to deliver the message each time the telephone is hung up, check the **Voicemail Ringback** check box.

Voicemail will not ring the extension more than once every 30 seconds.

g) To enable the user to use any of the Voicemail Pro UMS services to access the voicemail messages, check the **USM Web Services** check box

This option can be enabled only for users whose profile is set to Teleworker, Office Worker or Power User.

h) Click **OK**.

Note:

For more information about the fields in the Voicemail tab, see the Manager online help.

18. Select **File > Save Configuration**.

Extn tab field descriptions

Name	Default	Description
Extension Id		The physical ID of the extension port. Except for IP extensions, this setting is allocated by the system and is not configurable.
Base Extension	N/A	This should match the extension number used by the centralized extension during normal operation.
Caller Display Type	Default = On	Controls the presentation of caller display information for analog extensions. For digital and IP extensions, this value is fixed as **On**.
Reset Volume After Calls	Default = Off	If selected, resets the phone's handset volume after each call.

Name	Default	Description
Device Type	Default = Unknown SIP device	This is an information field only. If the configuration has been loaded from a system with SIP extensions currently registered, the current type of SIP phone is listed if recognized.
Module		This field indicates the external expansion module on which the port is located. **BP** indicates an analog phone extension port on the base or control unit. **BD** indicates a digital station (DS) port on the control unit. **BD** and **BP** is also followed by the slot number. VoIP extensions report as **0**.
Port		This field indicates the port number on the module indicated in the Module field. VoIP extensions report as **0**.
Disable Speakerphone	Default = Off	When selected, disables the fixed **SPEAKER** button if present on the phone using this extension port. Only supported on Avaya phones. An audible beep is sounded when a disabled **SPEAKER** button is pressed. Incoming calls such as pages and intercom calls are still connected but the speech path is not audible until the user goes off-hook using the handset or headset. Similarly calls made or answered using other buttons on the phone are not audible unless the user goes off-hook using the handset or headset. Currently connected calls are not affected by changes to this setting
Force Authorization	Default = On	If enabled, SIP devices are required to register with the B5800 Branch Gateway

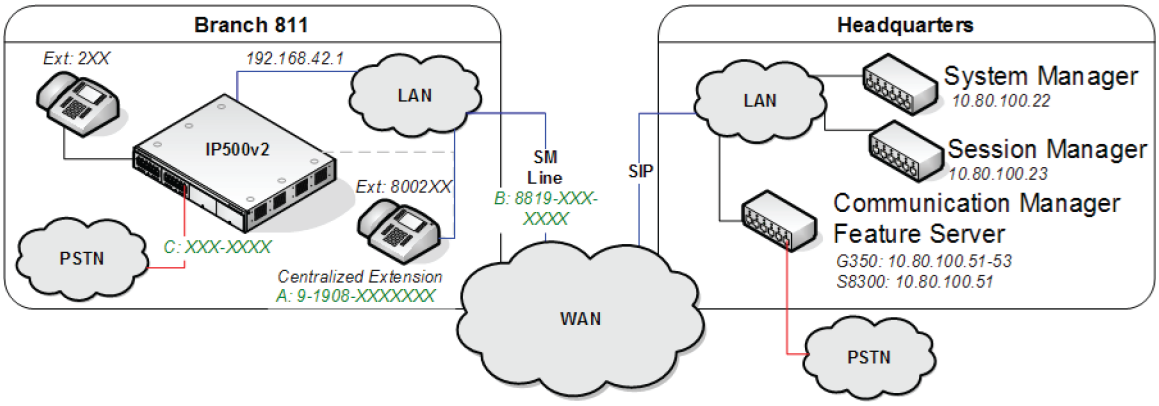
Name	Default	Description
		system using the Name and Login Code configured for the user within the B5800 Branch Gateway configuration. For centralized extensions this should be set to On.
Extension Mode	Default = Local	• For survivable extensions, this must be set to **Centralized**. • For native extensions, this must be set to **Local**.
DID Numbers	Default = Blank	• This field does not apply to native extensions. When configuring a native extension, leave this field blank. • When configuring a survivable extension (also referred to as a centralized extensions), this field is optional for systems where there is a clear mapping of DID numbers to extension number, for example DID 01555364123 and extension 884123. Another usage is if the phone registers with extension number using branch prefix, but expects to be dialed using short format. This relies on the behavior that when Session Manager lines are out of service, if the branch has a call (internal or external) targeted to the Session Manager line, it tries to first target any matching centralized extension DID and then any centralized extension number before checking any alternative routes configured.

Survivable extensions

Survivable extensions support SIP phones only. For a list of supported telephones, see Supported telephones on page 21. Voicemail for survivable extensions is provided by Modular Messaging. When Modular Messaging is used as the central voicemail system, at each branch you have the option to still use the local Embedded Voicemail for auto attendant operation and for announcements to waiting calls. For more information about voicemail, see Voicemail operation on page 163.

SIP extensions can be registered to the Communication Manager Feature Server at the central headquarters site but be physically located at the B5800 Branch Gateway site. This mode of operation is called survivable extension mode.

The survivable extensions can be configured to use the local B5800 Branch Gateway site to make and receive calls when connection to the Avaya Aura® network is not available. When this happens the B5800 Branch Gateway is acting as a survivable gateway for the extensions. This can be in addition to trying to register with an alternate Avaya Aura® Session Manager.



Limitations

- **WARNING** — Survivable phones (also referred to as centralized phones) are not provisioned from the B5800 Branch Gateway system. Centralized phones should be configured to obtain their setting and firmware files from a source other than the B5800 Branch Gateway system, unless you use the procedure described in 96x1 phones SIP firmware download in B5800 Branch Gateway centralized branch deployments on page 84.
- **Manual Configuration** — For survivability operation, survivable extensions must be added to the branch configuration manually. Auto creation of the required extension and user configuration entries should not be used.
- **Telephony Feature Restrictions** — When registered with the B5800 Branch Gateway system in survivability mode, the range of telephony features available to the centralized phone will be limited compared to the features provided to the phone normally by the Communication Manager Feature Server or Evolution Server.

The B5800 Branch Gateway supports Session Manager 6.1 and Session Manager 6.0. Depending on the Session Manager version you are using, see one of the following sections:

- Session Manager 6.1 configuration required for survivable extension support on page 185
- Session Manager 6.0 configuration required for survivable extension support on page 188

Survivable extension configuration checklist

Use this checklist to monitor your progress as you administer survivable extensions.

#	Description	Section	✔
1	Add a user on Session Manager for each survivable extension.	Depending on the version of Session Manager you are using, see one of the following: • Session Manager 6.1 configuration required for survivable extension support on page 185. • Session Manager 6.0 configuration required for survivable extension support on page 188.	
2	Enable SIP extension support on the branch.	See Enabling branch SIP extension support on page 192.	
3	Add SIP extensions and users to the branch.	See Adding SIP extensions and users to the B5800 Branch Gateway on page 194.	

Survivability operation

During normal operation, survivable extensions register with the Communication Manager Feature Server at headquarters. However, they can also be configured to automatically failover to their local B5800 Branch Gateway system for survivable telephony services when the connection to the Avaya Aura® Session Manager is lost for any reason.

Each survivable extension phone monitors its own connectivity to the Avaya Aura® Session Manager (and secondary Avaya Aura® Session Manager if configured). If it detects loss of connectivity, it automatically registers with the B5800 Branch Gateway and switches to survivability operation. There will be a short unavailability of services while failing over.

The survivable phones in the branch will typically be able to make and receive calls processed by the B5800 Branch Gateway approximately 2 minutes after a WAN failure. When the phone

detects that connection to the Avaya Aura® Session Manager is available again, it dynamically registers with it and switches back to normal operation.

Important:

Branch Survivability Settings. Survivable extensions entering survivability mode with the branch will occur in parallel with the branch loosing whatever centralized call control and trunk services it was configured to receive from the Avaya Aura® Session Manager. Therefore the calls and call routing applied to both native and survivable extensions may be limited. See PSTN Trunk Fallback on page 330.

Internal calls

Though physically located at a branch, during normal operation a survivable extension's calls are routed by the Avaya Aura® Session Manager and Communication Manager Feature Server rather than the B5800 Branch Gateway. Therefore there are some considerations for the routing of calls between native and survivable extensions.

The table below summarizes the possible scenarios for calls between native and survivable extensions:

Extension Type		Dialed Number	Notes
Call from...	Call to...		
Native	Native	2XX	Dial the extension number as shown on the target extension. The call routing is done by the local branch. The call is sent to the matching native extension number. If no match is found then it is checked against system and user short codes. No additional configuration is required.
		8XXXX	Dial the extension number as shown but with the branch prefix added. The configuration shown in the section Initial configuration for a Centralized Branch on page 95 covers the routing necessary for inter-branch calls. If the call begins with the branch's own prefix, the prefix is removed by the branch and the remaining number is treated the same as the scenario above. If the call begins with another branch's prefix, the routing to the appropriate branch is done by the Avaya Aura® Session Manager.

Extension Type		Dialed Number	Notes
Survivable	Survivable	8XXXX	Dial the extension number as shown on the target extension. The call routing is done by the Avaya Aura® Session Manager and Communication Manager Feature Server. No additional configuration is required.
Native	Survivable	8XXXX	Dial the extension number as shown on the target extension. Because for our examples, the survivable extension numbers begin with the same 8 prefix as the branches, the branch routes the call to the Avaya Aura® Session Manager where it matches the target survivable extension.
Survivable	Native	2XX	A survivable extension user dials the extension number of a native extension as shown on that native extension. Without additional configuration, the call will not route as the Avaya Aura® Session Manager cannot determine which branch is intended. In that situation, the survivable extension user needs to always include the branch prefix of the intended native extension. See Creating locations on page 150 and Creating adaptations on page 151 for more information. If, as recommended, the survivable extension has been installed with an IP address that puts it at the same location as the branch, then calls from the survivable extension go through the digit adaptation setup for that location. In that scenario we can specify a digit conversion that adds the branch prefix to any 2XX dialing received. Such calls would then be routed back to the branch.
		8XXXX	The configuration shown in the sectionInitial configuration for a Centralized Branch on page 95 will route the call to the correct branch where it will be matched to the native extension numbers.

Session Manager 6.1 configuration required for survivable extension support

The topics in this section provide the Session Manager 6.1 procedures required to configure survivable extension mode.

Note:

In the Session Manager application, you must complete fields marked with an asterisk. Fields not marked with an asterisk are optional.

Adding stations to Session Manager

The survivable extension can now be added to Session Manager. The details are automatically synchronized with the Communication Manager Feature Server.

1. On the System Manager console, under **Users**, click **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, in the Identity section, do the following:
    a. In the **Last Name** field, enter the user's last name.

    Note:

    Since you are adding a station in this procedure and not a user, depending on how the branches and stations in your system are named and organized, you could enter a location name in this field, for example `Chicago 25`. Then in the next field, **First Name**, you could enter a location within that branch, for example `cashier`.

    b. In the **First Name** field, enter the user's first name.
    c. In the **Middle Name** field, enter the user's middle name.
    d. In the **Description** field, enter a description of this user profile.
    e. In the **Login Name** field, enter the extension user login in the format, username@domainname.com or extension@domainname.com. For example, nsmith@avaya.com or 5002432@avaya.com.

    For survivability mode operation with a B5800 Branch Gateway system, the user name without the domain name should match the user name configured in the branch system.

    f. In the **Authentication Type** drop-down box, accept the default setting, **Basic**.

g. In the **Password** field, enter the password required to log into System Manager for personal web configuration.
h. In the **Confirm Password** field, enter the password again.
i. In the **Localized Display Name** field, enter the name to be used as the calling party.
j. In the **Endpoint Display Name** field, enter the user's full name.
k. In the **Honorific** field, enter the user's title if applicable.
l. In the **Language Preference** drop-down box, select the appropriate language.
m. In the **Time Zone** drop-down box, select the user's time zone.

5. To add a postal address for this user, expand the Address section and do the following:
   a. Click **New**.
   b. On the Add Address page, in the **Name** field, enter the user's name.
   c. In the **Address Type** drop-down box, select **Office** or **Home**, as appropriate.
   d. In the **Building** field, enter the building name.
   e. In the **Room** field, enter the room number.
   f. In the **Street** field, enter the street name.
   g. In the **Locality** field, enter the appropriate locale.
   h. In the **State or Province** field, enter the state or province, as appropriate.
   i. In the **Country** drop-down box, select the country.
   j. Click **Add**.
6. Click the **Communication Profile** tab to expand that section, and accept the default values for the **Name** field and **Default** check box.
7. Expand the **Communication Address** section, and do the following:
   a. Click **New**.
   b. In the **Type** drop-down box, select **Avaya SIP**.
   c. In the **Fully Qualified Address** field, enter the extension and select the domain from the drop-down box.
   d. Click **Add** to add the record.
8. Expand the **Session Manager Profile** section, and do the following:

a. In the **Primary Session Manager** drop-down box, select the Session Manager instance that should be used as the home server for the currently displayed communication profile.

b. In the **Secondary Session Manager** drop-down box, Session Manager instance that should be used as the backup server for the currently displayed communication profile.

c. In the **Origination Application Sequence** drop-down box, select the Communication Manager Feature Server or Evolution Server.

d. In the **Termination Application Sequence** drop-down box, select the Communication Manager Feature Server or Evolution Server.

e. In the **Survivability Server** drop-down box, do one of the following:

- If you are running System Manager R6.1 SP1 or later, select the B5800 Branch Gateway that is in this user's branch.
- If you are running System Manager R6.1 without a service pack update, accept the default setting, **none**.

Note:

With System Manager R6.1 prior to SP1, you do not designate the B5800 Branch Gateway in this field. The B5800 Branch Gateway address must be provided to the telephones through the settings file. See Survivability settings on page 198 for more information.

f. In the **Home Location** drop-down box, select the location that should be used as the home location for the currently displayed communication profile.

9. Expand the **Endpoint Profile** section, and do the following:

a. In the **System** drop-down box, select the appropriate Communication Manager entity.

b. In the **Profile Type** drop-down box, select the default setting, **Endpoint**.

c. Check the **Use Existing Endpoints** check box to select this option.

d. In the **Extension** field, enter the extension number.

e. In the **Template** drop-down box, select an appropriate template matching the telephone type as configured on Communication Manager.

f. In the **Set Type** field, accept the default.

g. In the **Security Code** field, enter the security code.

h. In the **Port** field, click on the search icon to select a port.

i. In the **Voice Mail Number** field, enter the number used to access the voicemail system.

j. Check the **Delete Endpoint on Unassign of Endpoint from User or on Delete Users** check box to select this option.

Note:

You do not need to configure the Messaging Profile section for B5800 Branch Gateway at this time.

10. Click **Commit**.
11. Repeat this procedure to add each survivable extension.

Viewing Session Manager registered users

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.
2. In the left navigation pane, click **System Status > User Registrations**. The list of registered users appears.
3. To see the complete registration status of an individual user, click **Show** in the Details column for the user you want to view.

Session Manager 6.0 configuration required for survivable extension support

The topics in this section provide the Session Manager 6.0 procedures required to configure survivable extension mode.

Note:

In the Session Manager application, you must complete fields marked with an asterisk. Fields not marked with an asterisk are optional.

Adding stations to Session Manager

The survivable extension can now be added to Session Manager. The details are automatically synchronized with the Communication Manager Feature Server.

1. On the System Manager console, in the left navigation pane, select **Users > Manage Users**.
2. On the User Management page, click **New**.
3. On the New User Profile page, in the General section, do the following:
    a. In the **Last Name** field, enter the user's last name.

    Note:

    Since you are adding a station in this procedure and not a user, depending on how the branches and stations in your system are named and organized, you could enter a location name in this field, for example `Chicago 25`. Then in the next field, **First Name**, you could enter a location within that branch, for example `cashier`.

    b. In the **First Name** field, enter the user's first name.
    c. In the **Middle Name** field, enter the user's middle name.
    d. In the **Description** field, enter a description of this user profile.
4. In the Identity section, do the following:
    a. In the **Login Name** field, enter the extension user login in the format, username@domainname.com or extension@domainname.com. For example, nsmith@avaya.com or 5002432@avaya.com.

    For survivability mode operation with a B5800 Branch Gateway system, the user name without the domain name should match the user name configured in the branch system.

    b. In the **Authentication Type** drop-down box, accept the default setting, **Basic**.
    c. In the **Password** field, enter the password required to log into System Manager for personal web configuration.
    d. In the **Confirm Password** field, enter the password again.
    e. In the **Shared Communication Profile** field, enter the appropriate password.
    f. In the **Confirm Password** field, enter the password again.
    g. In the **Localized Display Name** field, enter the name to be used as the calling party.
    h. In the **Endpoint Display Name** field, enter the user's full name.
    i. In the **Honorific** field, enter the user's title, if applicable.
    j. In the **Language Preference** drop-down box, select the appropriate language.
    k. In the **Time Zone** drop-down box, select the user's time zone.

5. To add a postal address for this user, in the Address section, do the following:
    a. Click **New**.
    b. On the Add Address page, in the **Name** field, enter the user's name.
    c. In the **Address Type** drop-down box, select **Office** or **Home**, as appropriate.
    d. In the **Building** field, enter the building name.
    e. In the **Room** field, enter the room number.
    f. In the **Street** field, enter the street name.
    g. In the **Locality** field, enter the appropriate locale.
    h. In the **State or Province** field, enter the state or province, as appropriate.
    i. In the **Country** drop-down box, select the country.
    j. Click **Add**.
6. Expand the **Communication Profile** section , and accept the default values for the **Name** field and **Default** check box.
7. Expand the **Communication Address** section, and do the following:
    a. Click **New**.
    b. In the **Type** drop-down box, select **Avaya SIP**.
    c. In the **Fully Qualified Address** field, enter the extension and select the domain from the drop-down box.
    d. Click **Add** to add the record.
8. Expand the **Session Manager Profile** section, and do the following:
    a. In the **Primary Session Manager** drop-down box, select the Session Manager instance that should be used as the home server for the currently displayed communication profile.
    b. In the **Secondary Session Manager** drop-down box, Session Manager instance that should be used as the backup server for the currently displayed communication profile.
    c. In the **Origination Application Sequence** drop-down box, select an application sequence that will be invoked when calls are routed from this user.
    d. In the **Termination Application Sequence** drop-down box, select the Communication Manager Feature Server or evolution server.
    e. In the **Survivability Server** drop-down box, accept the default setting, **none**.

Note:

Do not designate the B5800 Branch Gateway in this field. The B5800 Branch Gateway address must be provided to the telephones through the settings file. See Survivability settings on page 198 for more information.

Note that when running System Manager R6.1 SP1 or later, you are able to select **B5800** in this field. See Adding stations to Session Manager on page 185 for more information.

f. In the **Home Location** drop-down box, select the location that should be used as the home location for the currently displayed communication profile.

9. Expand the **Endpoint Profile** section, and do the following:

   a. In the **System** drop-down box, select the appropriate Communication Manager entity.
   b. Check the **Use Existing Endpoints** check box to select this option.
   c. In the **Extension** field, enter the extension number.
   d. In the **Template** drop-down box, select an appropriate template matching the telephone type as configured on Communication Manager.
   e. In the **Set Type** field, accept the default.
   f. In the **Security Code** field, enter the security code.
   g. In the **Port** field, click on the search icon to select a port.
   h. In the **Voice Mail Number** field, enter the number used to access the voicemail system.
   i. Check the **Delete Endpoint on Unassign of Endpoint from User** check box to select this option.

Note:

You do not need to configure the Messaging Profile section for B5800 Branch Gateway at this time.

10. Click **Commit**.
11. Repeat this procedure to add each survivable extension.

Viewing Session Manager registered users

Procedure

1. On the System Manager console, in the left navigation pane, select **Elements > Session Manager > System Status > User Registrations**.

The list of registered users appears.

2. To see the complete registration status of an individual user, click the check box for the user you want to view.

Enabling branch SIP extension support

About this task

Before adding any SIP extensions, the B5800 Branch Gateway system must be enabled for SIP extension support. Use this procedure to configure the B5800 Branch Gateway to support the addition of SIP extensions.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **LAN1** or **LAN2** tab, depending on which branch site LAN interface will be used for the SIP extensions.
4. Make a note of the IP Address and IP Mask details as these will be required during the SIP extension configuration.
5. Click the **VoIP** tab.
6. Check the **SIP Registrar Enable** check box. This is necessary for support of SIP extensions directly by the branch or when providing survivability support for Avaya Aura® SIP extensions.
7. Click **OK**.
8. Click the **SIP Registrar** tab.
9. Click the **Auto-create Extn/User** check box so that it is not checked (the default setting is enabled).

   This setting must be disabled. SIP extensions should only be allowed to register with the Avaya Branch Gateway B5800 system if they match existing extension and user entries in the configuration. If a centralized extension (also referred to as a survivable extension) is allowed to auto create matching entries, the extension's Extension Mode setting defaults to Local (also referred to as a native extension) which is incorrect for a centralized extension.
10. Configure the remaining fields on this tab as appropriate. See SIP Registrar tab field descriptions on page 175 for more information.

11. Click **OK**.
12. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

SIP Registrar tab field descriptions

Name	Default	Description
Domain Name	Default = Blank	This is the local SIP registrar domain name that will be needed by SIP devices in order to register with the B5800 Branch Gateway. If this field is left blank, registration is against the LAN IP address. For our examples we have been using a domain, **example.com**.
Layer 4 Protocol	Default = Both TCP & UDP	This is the transport protocol for SIP traffic between the B5800 Branch Gateway and SIP extension devices.
TCP Port	Default = 5060	This is the SIP port if using TCP.
UDP Port	Default = 5060	This is the SIP port if using UDP.
Challenge Expiry Time (sec)	Default = 10	The challenge expiry time is used during SIP extension registration. When a device registers, the SIP Registrar will send a challenge back to the device and waits for an appropriate response. If the response is not received within this timeout the registration is failed.
Auto-create Extn/User	Default = On	• For survivable extensions, it is strongly recommended that this setting is disabled. SIP extensions should only be allowed to register with

Name	Default	Description
		the B5800 Branch Gateway system if they match existing extension and user entries in the configuration. If a centralized (survivable) extension is allowed to auto create matching entries, the extension's **Extension Mode** setting defaults to **Local** (native) which is incorrect for a centralized (survivable) extension. • For local (native) extensions, this setting can be enabled.

Adding SIP extensions and users to the B5800 Branch Gateway

About this task

For each survivable extension, matching extension and user entries must be added to the B5800 Branch Gateway configuration. The required information is the extension number, the user name, and the user password. These values must match those used by the extension user when logging into the B5800 Branch Gateway system during normal operation. Sufficient Enterprise Branch User licenses must exist for the survivable extensions to register when required.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **Extension**.
3. Click the **New** icon and select **SIP Extension**.
4. Click the **Extn** tab.
5. Configure the fields as appropriate. See Extn tab field descriptions on page 178 for more information.
6. Click **OK**.
7. In the left navigation pane, click **User**.
8. Click the **New** icon and select **User**.
9. Click the **User** tab.

10. In the **Name** field, enter the same user name used for the survivable extension login to B5800 Branch Gateway.
11. In the **Extension** field, enter the Base Extension setting used for the SIP extension entry.

    Note:
    The full range of B5800 Branch Gateway user settings can be configured for the centralized user while they are operating in survivability mode. However the key settings are the **Name** and **Extension** fields.
12. Click **OK**.
13. Click the **Telephony** tab.
14. Click the **Call Settings** tab.
15. Ensure that the **Call Waiting On** option is selected. This setting is required to allow features such as transferring calls.
16. Click **OK**.
17. Click the **Supervisor Settings** tab.
18. Ensure the **Login Code** matches the **Shared Communication Profile Password** set for the centralized extension user in Avaya Aura®Session Manager. See Adding stations to Session Manager on page 185 for more information.
19. Click **OK**.
20. Select **File > Save Configuration**.

Extn tab field descriptions

Name	Default	Description
Extension Id		The physical ID of the extension port. Except for IP extensions, this setting is allocated by the system and is not configurable.
Base Extension	N/A	This should match the extension number used by the centralized extension during normal operation.
Caller Display Type	Default = On	Controls the presentation of caller display information for analog extensions. For

Name	Default	Description
		digital and IP extensions, this value is fixed as **On**.
Reset Volume After Calls	Default = Off	If selected, resets the phone's handset volume after each call.
Device Type	Default = Unknown SIP device	This is an information field only. If the configuration has been loaded from a system with SIP extensions currently registered, the current type of SIP phone is listed if recognized.
Module		This field indicates the external expansion module on which the port is located. **BP** indicates an analog phone extension port on the base or control unit. **BD** indicates a digital station (DS) port on the control unit. **BD** and **BP** is also followed by the slot number. VoIP extensions report as **0**.
Port		This field indicates the port number on the module indicated in the Module field. VoIP extensions report as **0**.
Disable Speakerphone	Default = Off	When selected, disables the fixed **SPEAKER** button if present on the phone using this extension port. Only supported on Avaya phones. An audible beep is sounded when a disabled **SPEAKER** button is pressed. Incoming calls such as pages and intercom calls are still connected but the speech path is not audible until the user goes off-hook using the handset or headset. Similarly calls made or answered using other buttons on the phone are not audible unless the user goes off-hook using the handset or headset.

Name	Default	Description
		Currently connected calls are not affected by changes to this setting
Force Authorization	Default = On	If enabled, SIP devices are required to register with the B5800 Branch Gateway system using the Name and Login Code configured for the user within the B5800 Branch Gateway configuration. For centralized extensions this should be set to On.
Extension Mode	Default = Local	• For survivable extensions, this must be set to **Centralized**. • For native extensions, this must be set to **Local**.
DID Numbers	Default = Blank	• This field does not apply to native extensions. When configuring a native extension, leave this field blank. • When configuring a survivable extension (also referred to as a centralized extensions), this field is optional for systems where there is a clear mapping of DID numbers to extension number, for example DID 01555364123 and extension 884123. Another usage is if the phone registers with extension number using branch prefix, but expects to be dialed using short format. This relies on the behavior that when Session Manager lines are out of service, if the branch has a call (internal or external) targeted to the Session Manager line, it tries to first

Name	Default	Description
		target any matching centralized extension DID and then any centralized extension number before checking any alternative routes configured.

Survivability settings

The settings used by each survivable extension are set through System Manager, as described in Step 8e in Adding stations to Session Manager on page 185 and through the 46xxsettings.txt file loaded by each survivable extension when it is started. The 46xxsettings.txt file includes survivability settings. Since the settings may be slightly different for each branch site, the 46xxsettings.txt file used by each branch site may be different, potentially making it difficult to use a single file server for all survivable extensions. However this can be solved by using a single file with GROUP options. See Using the group parameters on page 201 for more information.

When there is a single Avaya Aura® Session Manager, the 9600 Series SIP phones perform alternate registration with either the Avaya Aura® Session Manager when available or the survivable B5800 Branch Gateway. This is done by setting the SIMULTANEOUS_REGISTRATIONS parameter to 1.

When operating in a network deployment that includes Avaya Aura® Session Manager redundancy, the phones can do simultaneous registration with both Avaya Aura® Session Managers. This is done by setting the SIPREGPROXYPOLICY parameter to simultaneous and the SIMULTANEOUS_REGISTRATIONS parameter to 2 (the number of Avaya Aura® Session Managers). Simultaneous registration is supported between Avaya Aura® Session Managers but not between an Avaya Aura® Session Manager and a B5800 Branch Gateway.

Note:

The SIMULTANEOUS_REGISTRATIONS parameter in the SIP endpoint settings file must be set to match the number of Avaya Aura®Session Managers. That is, the value has to be 1 if there is only one Session Manager and B5800 Branch Gateway is the phones' second controller, and the value has to be 2 if there are two Session Managers and B5800 Branch Gateway is the phones' third controller.

The following are the key 46xxsettings.txt file settings which affect survivability operation.

- **CONTROLLER_SEARCH_INTERVAL**

  Time in seconds that the phone waits to complete the maintenance check for monitored controllers. Range 4 to 3600 seconds. Default 4 seconds.

- **DIALPLAN**

During survivable mode, when registered to the B5800 Branch Gateway system, the phone is not able to obtain dial plan information from the Avaya Aura® Session Manager as it would normally expect. This DIALPLAN strings can be used to set what numbers are dialed immediately when matched without waiting for any dialing timeout. Multiple entries can be used, separated by | characters. For example, on a typical B5800 Branch Gateway system, the following might be used. The first entry matches local extension numbers. The next two entries match numbers for other branches. The final entry matches US national number dialing:

```
SET DIALPLAN [2]xx|[8]xxxxx|[6]xxxxxx|9Z1xxxxxxxxxx
```

- **DISCOVER_AVAYA_ENVIRONMENT**

  This setting is used by the phone to set whether is should request if the controller to which it has registered supports AST (Advanced SIP Telephony). B5800 Branch Gateway systems do not support AST. However, since survivable phones connect in normal mode to Avaya Aura® Session Manager, the setting DISCOVER_AVAYA_ENVIRONMENT 1 can be used.

- **ENABLE_REMOVE_PSTN_ACCESS_PREFIX**

  Enables the removal of the PSTN access prefix from collected dial strings when the phone is registered with a non-AST controller such as B5800 Branch Gateway. Enabling this parameter (1) when the phone is communicating with an AST-capable controller has no effect. The default is 0 (do not remove prefix).

- **FAILBACK_POLICY**

  This setting controls how the phone checks for return to its primary server when available. The following values are used:

  - **admin** (SET FAILBACK_POLICY admin)

    The phone waits for administrative interventions. This option should not be used with B5800 Branch Gateway.

  - **auto** (SET FAILBACK POLICY auto)

    The phone periodically checks the availability of the primary controller and dynamically fails back. This is the default setting.

- **FAST_RESPONSE_TIMEOUT**

  This timer terminates SIP INVITE transactions if no SIP response is received within the specified number of seconds after sending the request. This is useful when a phone goes off-hook after connectivity to the centralized SIP Server is lost, but before the phone has detected the connectivity loss. After the SIP INVITE is terminated, the phone immediately transitions to Survivable Mode. Default 4 seconds.

- **MSGNUM**

  This sets the number dialed when the **Message** button is pressed and the phone is in normal centralized mode. For example, the extension number for the Modular Messaging system.

- **PSTN_VM_NUM**

  This sets the number dialed when the **Message** button is pressed and the phone is in survivable mode. For example, a DID number for the Modular Messaging system.

- **RECOVERYREGISTERWAIT**

  This is the monitoring interval used by the phone when no available controller was detected by a previous monitoring check. The phone waits for a response from each controller in the SIP_CONTROLLER_LIST with the CONTROLLER_SEARCH_INTERVAL setting. The actual interval used is between 50% to 90% of the setting. Range 10 to 36000 seconds. Default 60 seconds.

- **REGISTERWAIT**

  This is the monitoring interval used by the phone when it has a currently selected active controller. The phone waits for a response from each controller in the SIP_CONTROLLER_LIST with the CONTROLLER_SEARCH_INTERVAL setting. Range 30 to 86400 second. Default 300 seconds.

- **SIMULTANEOUS_REGISTRATIONS**

  If the SIPREGPROXYPOLICY is set to simultaneous, the extension can remain registered with multiple available controllers, though only the highest priority controller is set as the active controller. This must be set to match the number of available Avaya Aura® Session Managers.

- **SIP_CONTROLLER_LIST**

  This setting should contain a priority ordered list of SIP servers that the phone should use. Each entry should contain the server IP address, port and transport method (TCP or UDP). The multiple entries should be separated by a comma.

  - The list should contain the primary Avaya Aura® Session Manager as the first entry then the B5800 Branch Gateway. If there is an additional Avaya Aura® Session Manager being used for redundancy (see “SecondaryAvaya Aura® Session Manager line configuration in Avaya Aura Session Manager line redundancy on page 118) it should be included before the B5800 Branch Gateway entry.
  - The string below would set the phone's primary SIP controller to the Avaya Aura® Session Manager and the secondary controller to an B5800 Branch Gateway used in the basic configuration example:

    ```
    SET SIP_CONTROLLER_LIST 10.80.100.23:5060;transport=tls,
    35.1.1.51:5060;transport=tcp
    ```

    Warning:

    If the port and transport are not specified for a controller, the default values of 5061 and TLS are used. Note that B5800 Branch Gateway currently only supports TCP and or UDP.

- **SIPDOMAIN**

The enterprise SIP domain. This must match a domain set in the Avaya Aura® domains settings.

- **SIPREGPROXYPOLICY**

  This setting controls how the list of SIP controllers specified above are monitored and used. The settings are:

  - **alternate** (SET SIPREGPROXYPOLICY alternate) Remain registered with only the active controller. This is the default setting.
  - **simultaneous** (SET SIPREGPROXYPOLICY simulataneous) Remain registered with the number of controllers set by the SIMULTANEOUS_REGISTRATIONS setting, selecting from the highest available controllers.

Using the group parameters

With a single central file server to distribute settings files and firmware to the survivable extensions, it is not practical to have to repeatedly edit the 46xxsettings file. However, using the GROUP option allows the file to contain settings that are different for each branch.

1. Install and register the survivable extensions but with no survivable server settings, ie. only the Avaya Aura® Session Manager server listed in the SIP_CONTROLLER_LIST entry. For example SET SIP_CONTROLLER_LIST 10.80.100.23;transport=tcp.
2. Now replace that entry with section similar to the following. Each entry sets a new value for SIP_CONTROLLER_LIST for each branch which includes both the Avaya Aura® Session Manager and the branch's B5800 Branch Gateway system. Note that group numbers can only be a maximum of 3 digits.

   ```
   ...IF $GROUP SEQ 811 goto GROUP811IF $GROUP SEQ 812 goto GROUP812goto END
   # GROUP811
   ```

   ```
   SET SIP_CONTROLLER_LIST 10.80.100.23:5060;transport=tcp,
   35.1.1.51:5060;transport=tcpgoto END
   # GROUP812
   ```

   ```
   SET SIP_CONTROLLER_LIST 10.80.100.23:5060;transport=tcp,
   35.1.1.52:5060;transport=tcpgoto END
   # END## Common settings come after thisSET SIPREGPROXYPOLICY alternateSET
   FAILBACK POLICY auto...
   ```

3. At each survivable extension, with the extension idle have the user or a site administrator dial **Mute 47687** (**Mute GROUP**). When prompted enter the appropriate group number for the branch and press #.
4. The phone will fetch the new 46xxsettings.txt file.

SIP controller monitoring

It is important to understand that both the B5800 Branch Gateway system and the survivable extensions perform monitoring of the Avaya Aura® Session Manager availability.

- The monitoring done by each survivable extension is used to determine when it should failover to another SIP controller.
- The B5800 Branch Gateway system's monitoring is used to determine when the B5800 Branch Gateway system should allow survivable extensions to register with it.

The sections below summarize this monitoring in more detail.

B5800 Branch Gateway system line monitoring

The B5800 Branch Gateway system sends regular OPTION messages to any Avaya Aura® Session Manager lines in its configuration. The Proactive and Reactive settings on the B5800 Branch Gateway system's System tab set how often the OPTION messages are sent in seconds. The Proactive setting is used for an Avaya Aura® Session Manager line currently thought to be in service. The Reactive setting is used for an Avaya Aura® Session Manager line currently thought to be out of service.

- If a response is received and is not a 408, 500, 503 or 504 response, the Avaya Aura® Session Manager line is treated as in service; otherwise the line is treated as being out of service.
- If no response is received within the set Call Initiation Timeout setting on the Avaya Aura® Session Manager line's VoIP tab the line is treated as being out of service.
- If the line is out of service, and call comes from the trunk, the trunks status is changed back to in service.
- If the line is in service, a call may fail due to either being unable to deliver the message or receive a 100 response within a configured timeout. The line will not go out of service because this may be a temporary failure due to a busy system.
- In addition each Avaya Aura® Session Manager line can be manually set to in or out of service using the In Service option on the Avaya Aura® Session Manager line's Session Manager tab.

Centralized 9600 extension SIP controller monitoring and selection

Each survivable extension performs monitoring to determine which SIP controllers are available and, from the results, which controller to use as its active controller. It does this as follows:

- Using the list of SIP controllers, the extension send a SIP REGISTER (Adding bindings) message to each controller. The controller list is set by the SIP_CONTROLLER_LIST which lists controllers in priority order from highest priority first.
- The phone waits for a response from each controller within a set time. That time is set by the CONTROLLER_SEARCH_INTERVAL setting (default 4 seconds).
- The controller is considered available if a 200 OK response is received from it within the timer interval. Once a controller has been marked as available, the phone unregisters

from it. B5800 Branch Gateway only responds to this request if its Avaya Aura® Session Manager lines are out of service.

  - If the phone does not have a current controller, it will register with the highest ranked available controller.
  - If a higher ranked controller then the extension's current active controller is available, it will switch its active controller to the higher ranked available controller. This only applies if the FAILBACK_POLICY is set to auto.
  - While operating with its selected controller, the phone will continue monitoring the available controllers. It does this at regular intervals set by the REGISTERWAIT setting (default 300 seconds).
  - If no response is received from any controller, the extension retries monitoring. It does this at random intervals between 50 to 90% of the RECOVERYREGISTERWAIT setting (default 60 seconds).

- A survivable extension can register with available extensions as follows. Whichever method is used, only the highest ranking controller is set as its active controller.
  - Register with only the active controller. This is selected by the SIPREGPROXYPOLICY being set to alternate.
  - Register with several controllers. This is selected by the SIPREGPROXYPOLICY being set to simultaneous. The extension will register to the number of controllers specified by the SIMULTANEOUS_REGISTRATIONS setting.
- A survivable extension will not failover to another SIP controller while it has a connected call in progress. However, it will not be able to make or receive any additional calls while in this state. Once the existing call is completed, the extension will failover to the other SIP controller.
- In addition to the regular monitor checks, the extension will perform a monitoring check when any of the following events occur:
  - It does not receive a response to an INVITE it send to its active controller within a set time. The time is set by the FAST_RESPONSE_TIMEOUT settings (default 4 seconds).
  - It receives a TCP keep-alive failure or other socket error.
  - If prompted by an administrator.
  - If it receives an INVITE from a controller other than its active controller.

9600 extension operation

Features available during failover

The following apply while an extension is in the process of failover to another SIP controller. Typically the failover process will be completed within 2 minutes.

- The phone will display the survivability warning icon. In addition:
  - If the extension is idle, it displays the message **Link recovery. Limited phone service. Calls may be lost**.
  - If the user has a call in progress which continues, the survivability warning icon is displayed along with the message **Limited phone service**. The only call control available is End Call. The phone will not failover until the call is ended.
  - If the message **Acquiring Service..**. is displayed it indicates that the extension could not detect any available SIP controller. It will not failover until an available controller is detected.
- During the failover:
  - No new calls can be made or received.
  - Held calls are lost during failover.
  - Transfers are lost during failover.

Features available during survival mode

The following section only covers features when using the B5800 Branch Gateway system for survival mode.

- Call appearances can be used to make and receive calls as normal.
- Dialing that matches local B5800 Branch Gateway extension numbers will be routed as normal.
- All other numbers will be processed by the B5800 Branch Gateway and routed using its call control settings, for example calls with the external dialing prefix.
- The dial plan used by the extension is that specified by the 46xxsettings.txt file.
- Hold and transfer are supported.
- AST features (FNUs and Bridged call appearances) are unavailable and not displayed on the phone menus. Some features can be invoked on B5800 Branch Gateway by dialing appropriate short codes.
- Unsupported features are not displayed.

- The message waiting indicator does not work and is switched off.
- Voicemail may still be available using the **PSTN_VM_NUM** number configured in the survivability settings.
- One-button voicemail access will be available if the central voice mail system continues to operate and will make a PSTN call to the voice mail system. Depends on correct provisioning.
- Local telephone features will be available: audio selection (speaker / headset / handset), mute.
- Local phone applications will be available: local call redial, Call Logs, Volume Control, local contacts, speed-dials, auto-dials, WML browser (WML Browser is dependent on network access to WML server!) but cannot be changed.
- Contact or Autodial Favorite Features are displayed on the Phone Screen.
- Presence is not supported.
- The only Avaya A-Menu options available are Brightness and Contrast.
- Craft changes may be made and are saved locally on the phone.

Feature	Normal operation	Survivability mode with B5800 Branch Gateway
Make call	Yes	Yes
Receive call	Yes	Yes
Multiple call Appearances	Yes	Yes
Call hold	Yes	Yes
Consultative hold	Yes	Yes
Ad hoc conferencing	Yes, up to six parties	Yes, three-party Also up to 64-party Meet-Me conferencing supported
Voice mail coverage & access	Yes	Yes over PSTN. No MWI
Attended call transfer	Yes	Yes
Unattended call transfer	Yes	Yes
Call forward (all/ busy/ no answer)	Yes	Yes*
CDRs	Yes	SMDR records stored on B5800 Branch Gateway for retrieval upon WAN recovery
Music on hold	Yes	Yes
Hunt groups	Yes	No

Feature	Normal operation	Survivability mode with B5800 Branch Gateway
Call Management	Yes (CM COR)	Yes (Some restrictions can be configured in the B5800 Branch Gateway either at the system level or for the user.)
Calling party block/ unblock	Yes	Yes*
Call park	Yes	Yes*
Call unpark	Yes	Yes*
Call pickup	Yes	Yes*
Directed call pickup	Yes	Yes*
Extended call pickup	Yes	Yes*
Priority call	Yes	Yes*
Auto callback	Yes	Yes*
Malicious call trace	Yes	No
Malicious call trace cancel	Yes	No
EC500	Yes	Calls arriving at core Communication Manager will still be sent to cell phone. Calls arriving at a branch site can be sent to cell phone if Mobile Twinning feature is set. Extend active call and EC500 on/off not available in 96xx phone UI
Transfer to voicemail	Yes	No
Bridge line and call appearances	Yes	No
Hold recall	Yes	Yes
Transfer recall	Yes	Yes
Busy Indicator	Yes	No

* Not available through the phone menus. However, similar features are supported by B5800 Branch Gateway and can be invoked by the survivable phone by dialing the appropriate B5800 Branch Gateway feature access codes (i.e. short codes). If the default B5800 Branch Gateway short code for the feature ends with a #, then it has to be changed in the B5800 Branch Gateway configuration to a short code that does not end with a # and can be dialed by the 9600 Series SIP phones.

Chapter 11: Managing license files with PLDS

Overview

The Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements. Using PLDS, you can perform operations such as license activations, license upgrades, and license moves.

When you place an order for a PLDS-licensed software product, the license entitlements on the order are automatically created in PLDS. In addition to these license entitlements, you can also have your licences activated in Avaya PLDS. You must provide the host ID of each B5800 Branch Gateway in your network to generate a license for each branch. The host ID is the Feature Key Serial Number printed on the B5800 Branch Gateway System SD card.

- PLDS lets you activate license entitlements to create license files.
- When you purchase a licensed Avaya software product you get an e-mail notification from PLDS.
- This e-mail includes a LAC.
- You can use the LAC to quickly find and activate the newly purchased license entitlements in PLDS.
- License activation requires you to specify the host ID of the B5800 Branch Gateway for inclusion in the license file.
- You can also use other search methods in PLDS to find the license entitlements you wish to activate.
- PLDS also allows you to change license activations and deliver updated license files.

Examples:

- Adding more license entitlements to an existing activation
- Upgrading a license file to a new major release
- Moving license entitlement activations between branches
- Regenerating a license file with an new host ID

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site (https://plds.avaya.com).
   You will be redirected to the Single sign-on (SSO) Web site.
2. Log in to SSO using your SSO ID and Password.
   You will be redirected to the PLDS registration page.
3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Link ID, send an e-mail to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License Authorization Code (LAC)
4. Click **Submit**.
   Avaya will send you the PLDS access confirmation within one business day.

About license activation

What is license activation?

License activation is a process of activating license entitlements by specifying the host ID of each B5800 Branch Gateway. The process includes generating the license file.

When license entitlements are activated, PLDS generates Activation Records containing the activation information and License/Key.

Types of license activation

Types of activation include:

- Regular activation: where license entitlements are activated to generate Activation Records.
- Upgrade activation, which involves either:
  - Activating license entitlements that have been marked as upgradeable. When you activate these license entitlements, you can generate License/Key for either the current version or the old version.
  - Activating upgrade license entitlements, which are purchased to upgrade other existing license entitlements. When users activate these license entitlements, they select the license entitlements to upgrade.

Activating license entitlements

Before you begin

Host ID of each B5800 Branch Gateway.

About this task

Use the License Activation Code (LAC) to activate one or more license entitlements. You may choose to activate all of the licenses or specify the number of licenses that you want to activate from the quantity available. Upon successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification e-mail message to the customer that is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the B5800 Branch Gateway system. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification e-mail message. You need to install the license file on each B5800 Branch Gateway to use the licenses.

Procedure

1. Type http://plds.avaya.com in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an e-mail message.

   Note:

   If you do not have an e-mail message with your LAC, follow the steps in the Searching for Entitlements section and make a note of the appropriate LAC from the LAC column.

Note:

The Quick Activation automatically assumes that you want to activate all license entitlements on LAC and gives the option to remove line items and enter the amount of each license to activate (full or partial amount).

4. Enter the B5800 Branch Gateway information.
5. Click **Next** to validate the registration detail.
6. Enter the B5800 Branch Gateway information.

   This is the Feature Key Serial Number printed on the System SD card. You must add dashes between pairs of digits to provide the number in MAC address format (nn-nn-nn-nn-nn-nn). You can also get the Host ID from Manager.
7. Enter the number of licenses you want to activate.
8. Review the Avaya License Agreement and accept the agreement if you agree.
9. Perform the following steps to send an activation notification e-mail message:
   a) In the **E-mail to** field, enter e-mail addresses for any additional activation notification recipients.
   b) Enter any comments or special instructions in the **Comments** field.
   c) Click **Finish**.
10. Click **View Activation Records**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. A single license file will be generated for each branch. From the **License/Key** tab, you can view and download the license file to your local PC. See Activating license files on page 98 for information on how to upload the license files to the Network Management server for distribution to each branch using Provisioning and Installation Manager (PIM) or upload the license files to each branch using the Manager application.

Searching for license entitlements

About this task

Use this functionality to search for an entitlement by using any one or all of the following search criteria:

- Company name
- Group name

- Group ID
- License activation code

In addition to these search criteria, PLDS also provides other additional advanced search criteria for searching license entitlements.

Note:

Avaya associate or Avaya Partners can only search license entitlements by company name.

Procedure

1. Type http://plds.avaya.com in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Assets** > **View Entitlements**.

   The system displays Search Entitlements page.
4. If you want to search license entitlements by company name, enter the company name in the **%Company: field**. If you would like to see a complete list of possible companies before searching for their corresponding entitlements, do the following:

   a) Click the **magnifying glass** icon.
   b) Enter the name or several characters of the name and a wildcard (%) character.
   c) Click **Search Companies**.
   d) Select the desired company name from the list of options.

   Tip:

   You can use a wildcard (%) character if you do not know the exact name of the company you are searching for. For example, if you enter Av%, the system searches for all the company names starting with the letter Av. You can enter a wildcard character (%) at any position in the search criteria.
5. If you want to search license entitlements by group name, enter the appropriate information in the **%Group name:** or **%Group ID:** fields.

   Group Names or IDs are specific to Functional Locations and Sold-To's that define the actual location of equipment and software.

   Tip:

   You can use a wildcard (%) character if you do not know the exact name of the group you are searching for. For example, if you enter Gr%, the system searches for all the groups starting with the characters Gr. You can enter a wildcard character (%) at any position in the search criteria.
6. If you want to search license entitlements by LAC, enter the specific LAC in the **%LAC:** field.

Tip:

You can use a wildcard (%) character if you do not know the exact LAC you are searching for. For example, if you enter AS0%, the system searches for all the LACs starting with AS0. You can enter a wildcard character (%) at any position in the search criteria.

You will receive LACs in an e-mail if you have supplied the e-mail address to your sales order. If you do not have this code, you will need to search using one of the other search criteria.

7. If you want to search license entitlements by application, product and/or license status, select the appropriate application, product, and/or status from the field.
8. Click **Search Entitlements**.

Result

All corresponding entitlement records appear at the bottom of the page.

Regenerate License files

Use this functionality to regenerate the license file on a selected B5800 Branch Gateway. During the regeneration process, you can only modify host ID information.

Regenerating a license file

Procedure

1. Type http://plds.avaya.com in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Activation** > **Regeneration** from the Home page.
4. Search License Activations to Regenerate.

   You can search the activation records by the Company name, B5800 Branch Gateway system, Group name or ID using the Search Activation Records functionality.
5. Click **Regenerate** from the appropriate record.
6. Validate the Registration Detail and click **Next**.
7. Validate the items that will regenerate and click **Next**.
8. Accept the Avaya Legal Agreement.

9. Perform the following steps to send an activation notification e-mail message:
   a) In the **E-mail to** field, enter e-mail addresses for any additional activation notification recipients.
   b) Enter any comments or special instructions in the **Comments** field.
   c) Click **Finish**.
10. Click **View Activation Records**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. A single license file will be generated for each branch. From the **License/Key** tab, you can view and download the license file to your local PC. See Activating license files on page 98 for information on how to upload the license files to the Network Management server for distribution to each branch using Provisioning and Installation Manager (PIM) or upload the license files to each branch using the Manager application.

Chapter 12: Standalone SAL Gateway for remote service

Avaya Global Services (AGS) uses the Secure Access Link (SAL) Gateway to provide remote delivery of service to the B5800 Branch Gateway. The supported configuration requires a standalone SAL gateway that is deployed in the enterprise headquarters/data center and using the B5800 Branch Gateway administration applications — Manager, System Status, and System Monitor. See Administration software suite on page 71 for a description of these applications. In order to use SAL to remotely launch the administration tools in the customer environment, the administration tools must be installed on the customer's Network Management server or VMPRO server.

SAL Gateway R2.0 software must be installed on a customer-provided server in the enterprise at a central location that allows for network connectivity to each deployed branch. The SAL Gateway manages the B5800 Branch Gateways in multiple branches, relaying alarms from the B5800 Branch Gateways back to Avaya, and proxying connection requests for support engineers. The SAL solution is fully customer controlled through the deployment and use of the optional SAL policy server.

Note:

System Platform's Virtual SAL Gateway (VSALGW) is not supported in managing each individual branch. The VSALGW is only officially supported by Avaya in management of system platform “on-board” devices such as System Platform, Session Manager and System Manager. Each B5800 Branch Gateway branch is considered an “off-board” device.

Use of SAL to access the B5800 Branch Gateway management tools and Network Management applications

You are able to access the B5800 Branch Gateway management tools and Network Management applications through SAL.

- **Manager**

  Manager is an administration tool used to configure and upgrade the B5800 Branch Gateway system. When the Avaya Network Management suite is not installed on a server in the customer network, you can use Manager to administer each branch individually. You are able to use SAL to access the Manager application for local or remote configuration management of the B5800 Branch Gateway system.

Note:

For B5800 Branch Gateway upgrades, you must access Manager that is installed on a PC or Network Management server that resides within the customer network.

- **System Status Application**

  The System Status Application is an administration tool used to monitor the current status of individual branches in the B5800 Branch Gateway system. You are able to use SAL to access the System Status Application that is installed locally or remotely.

- **System Monitor** (Tier3/4 tool only)

  System Monitor is an administration tool that provides detailed traces of all activity on the B5800 Branch Gateway system.

  Note:

  You are able to use SAL to access the System Monitor application that is installed on a PC or Network Management server that resides within the customer network.

- **Avaya Network Management**

  The Avaya Network Management offer is a suite of software applications that enable centralized management of the B5800 Branch Gateway system. It provides a single access interface to manage multiple branch locations. You are able to use SAL to access the Network Management server through Remote Desktop Connection (RDC) or through the HTTP web-access client option where you are able to remotely administer and manage the branches.

For more information about the B5800 Branch Gateway management tools and Network Management applications, see Centralized management on page 15 and Administration software suite on page 71.

SAL Gateway installation and registration

To install SAL Gateway, see Chapter 2 in *Secure Access Link 2.0, SAL Gateway Implementation Guide*, document number 144813, which is available on the Avaya support Web site http://support.avaya.com. The *Secure Access Link 2.0 Software Gateway* download is also available on the Avaya support Web site.

Registering a product with Avaya is a process that uniquely identifies the device so that Avaya can service it. A SAL Gateway registration form is provided with your software download. See Universal Install/SAL Registration Request Form on page 218 for more information. To register the SAL Gateway, complete Step 1 on the form and send it to salreg@avaya.com. The following information is requested in Step 1:

- Your company name
- Avaya Sold-to Number (customer number)
- Your contact information, so that Avaya can contact you if there are questions

Avaya uses this information to register your gateway. When the registration is complete, Avaya will send you an e-mail that provides the following information:

- The Solution Element ID and Product ID numbers
- A list of the devices currently registered at this location
- A list of other locations for your company

Note:

Optional: If you want to get Solution Element IDs (SEID) from other locations, complete the Step 2 tab of the registration sheet and send it to salreg@avaya.com using the link included on the sheet. Avaya will send you a list of SEIDs from the locations you selected.

B5800 Branch Gateway registration and SAL Gateway on-boarding

Each B5800 Branch Gateway deployed must be registered with Avaya. To add managed devices to your SAL Gateway using the Solution Element IDs (SEID) provided to you during SAL Gateway registration described above, see “Configuring a Managed Element” in Chapter 4 in the *Secure Access Link 2.0, SAL Gateway Implementation Guide*, document number 144813, which is available on the Avaya support Web site.

When you have added all your managed devices, complete Step 2 of the SAL Gateway registration form for each managed device you added to your SAL Gateway and send the form to salreg@avaya.com. When this form is received, the Avaya registration team makes the appropriate changes to allow access to your managed devices through the SAL Gateway. Avaya will then confirm via an e-mail notification that remote access to your product has been enabled through your SAL Gateway.

B5800 Branch Gateway SAL-based alarming

The SAL Gateway supports alarming for the B5800 Branch Gateway managed device. You must change the alarm destination on your B5800 Branch Gateway managed device so that alarms are routed to your centralized SAL Gateway. See SNMP on page 236 for more information. During the registration and on-boarding process of each branch, the Avaya registration team also tests alarming through the SAL Gateway and back into Avaya alarm receivers.

Universal Install/SAL Registration Request Form

You can download this form from the Avaya support web site as follows:

1. Go to the Avaya support Web site http://support.avaya.com.
2. Select **More Resources** > **Equipment Registration**.
3. Under **Non-Regional (Product) Specific Documentation**, select **Universal Install/SAL Registration Request Form**.
4. Complete the registration form as instructed.

Chapter 13: Additional installation and system procedures

The following topics are provided in this chapter:

System shutdown

B5800 Branch Gateway systems can be shut down in order to perform maintenance. The shut down can be either indefinite or for a set period of time after which the B5800 Branch Gateway will automatically reboot. During the shut down process, the current configuration in the control unit's RAM memory is copied to the System SD card.

Warning:

- A shutdown must always be used to switch off the system. Simply removing the power cord or switching off the power input may cause errors.
- This is not a polite shutdown, any users calls and services in operation will be stopped. Once shutdown, the system cannot be used to make or receive any calls until restarted.

- The shutdown process takes up to a minute to complete. When shutdown, the CPU LED and the base card LEDs 1 and 9 (if trunk daughter card fitted) will flash red rapidly. The memory card LEDs are extinguished. Do not remove power from the system or remove any of the memory cards until the system is in the this state.
- To restart a system when shutdown indefinitely, or to restart a system before the timed restart, switch power to the system off and on again.

Shutting down the system using Manager

Procedure

1. Start Manager.
2. Select **File** > **Advanced** > **System Shutdown**.
   The Select IP Office window appears.
3. Select the B5800 Branch Gateway system you want to shut down.
   The System Shutdown Mode window appears.
4. Do one of the following:
   - To shut down the system for an indefinite period of time, select **Indefinite**.

     To restart the system you must switch the power off and then on.
   - To shut down the system for a specific period of time, select **Timed** and then specify the duration in hours and minutes.

     The system will automatically reboot after the set time has elapsed.
5. Click **OK**.

Shutting down the system using the System Status application

Procedure

1. Start System Status and access the system status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Shutdown System**.
4. Select the time duration for the shutdown or indefinite.

Shutting down the system using a system phone

About this task

To shut down the system using a system phone, you must be administered as a System Phone user. You can shut down the system using a 1400, 1600, or 9600 series phone (excluding XX01, XX02, and XX03 models). Unlike Manager, a system phone user cannot select an indefinite shutdown. A system phone user can set a timed shut down of between 5 minutes and 24 hours. Your Login Code is used to restrict access to some system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **System Shutdown**.
4. Select a time period for the shutdown. It must be in between 5 minutes and 24 hours.
5. Select **Done** and then **Confirm** to begin the shutdown.

Shutting down the system using the AUX button

Procedure

On the control unit, press the **AUX** button for more than 5 seconds.
The control unit will shutdown with the restart timer set to 10 minutes.

Rebooting the system

About this task

You can use Manager to reboot an B5800 Branch Gateway system.

Procedure

1. Start Manager.
2. Select **File** > **Advanced** > **Reboot**.
3. In the Select IP Office window, select the B5800 Branch Gateway system.

4. Enter your user name and password.
5. In the Reboot window, do one of the following:
   - Select **Immediate** to reboot the system immediately.
   - Select **When Free** to reboot the system when there are no calls in progress. This selection can be combined with the **Call Barring** options.
   - Select **Timed** and then specify a time in hours and minutes.

     This reboots the system the same as When Free but first waits for a specific time. After the specified time, the system waits for there to be no calls in progress and then reboots. This selection can be combined with the **Call Barring** options.

     Note:
     If the time is after midnight, the system's normal daily backup is canceled.
6. In the **Call Barring** section, select **Incoming Calls** and/or **Outgoing Calls**. These settings are used when the reboot mode is **When Free**. They bar the sending or receiving of any new calls.
7. Click **OK**.

About changing components

Except for memory cards, cards and external expansions modules must only be removed and added to an B5800 Branch Gateway system when the system is turned off. See Memory card removal on page 270 and System shutdown on page 219 for more information.

Note that for extension ports, by default both an extension entry and a user entry are configured in the system. Extension entries can be deleted without deleting the corresponding user entry. This allows retention of the user settings and association of the user with a different extension by changing that extension's Base Extension number to match the user's Extension ID.

In the following procedures, the term component refers to a card fitted into the control unit or an external expansion module.

Replacing a component with one of the same type

About this task

If you are replacing a component with one of the same type and capacity, no configuration changes are required.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 219.
2. Remove the card or external expansion module.

   Note:
   The card slot or expansion port used as the replacement must be installed in the same position.
3. Install the replacement using the appropriate procedure for the type of component. See Base and trunk card installation on page 53 or Connecting external expansion modules on page 64 for more information.
4. Restart the B5800 Branch Gateway system.

Replacing a component with one of higher capacity

About this task

If you are replacing a component with one of the same type but with higher capacity, when restarted the B5800 Branch Gateway system will automatically create configuration entries for the new trunks or extensions/users.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 219.
2. Remove the card or external expansion module.

   Note:
   The card slot or expansion port used as the replacement must be installed in the same position.
3. Install the replacement using the appropriate procedure for the type of component. See Base and trunk card installation on page 53 or Connecting external expansion modules on page 64 for more information.
4. Restart the B5800 Branch Gateway system.
5. Use Manager to configure the new trunks or extension/users.

Replacing a component with one of lower capacity

About this task

If you are replacing a component with one of the same type but with lower capacity, when restarted the B5800 Branch Gateway system configuration must be edited to remove redundant entries.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 219.
2. Remove the card or external expansion module.

   Note:

   The card slot or expansion port used as the replacement must be installed in the same position.
3. Install the replacement using the appropriate procedure for the type of component. See Base and trunk card installation on page 53 or Connecting external expansion modules on page 64 for more information.
4. Restart the B5800 Branch Gateway system.
5. Use Manager to delete the trunks or extensions/users in the configuration that are no longer supported by the replacement component.

Replacing a component with one of a different type

About this task

If you are replacing a component with one of a different type, you must perform two procedures; one to permanently remove the component and then one to add the component.

Procedure

1. Remove the existing component. See Permanently removing a component on page 225.

   Note:

   Be sure to reboot the system and edit the configuration after you remove the component.
2. Install the new component. See Adding a new component on page 225.

Adding a new component

About this task

If you are adding a new component to an available slot or port, when restarted the B5800 Branch Gateway system will automatically create configuration entries for the new trunks or extensions/users.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 219.
2. Install the new component using the appropriate procedure for the type of component. See Base and trunk card installation on page 53 or Connecting external expansion modules on page 64 for more information.
3. Restart the B5800 Branch Gateway system.
4. Use Manager to configure the new trunks or extension/users.

Permanently removing a component

About this task

If you are permanently removing a component, when restarted the B5800 Branch Gateway system configuration must be edited to remove redundant entries.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 219.
2. Remove the card or external expansion module.
3. Restart the B5800 Branch Gateway system.
4. Use Manager to delete the trunks or extensions/users in the configuration that relate to the component removed.
5. In the **Control Unit** section of the configuration, delete the entry for the component that is no longer present in the system.

Swapping extension users

About this task

This procedure explains how to swap extensions for two users. This example refers to User A and User B which represent any two users for whom you want to swap extensions.

Procedure

1. Load the B5800 Branch Gateway configuration.
2. Select **Extension**.
3. In the **Extension** section of the window, select the extension for User A.
4. In the **Base Extension** field, change the extension to User B's extension.

   Note:

   If Manager is set to validate edits, a warning appears that says this change conflicts with the existing Base Extension setting of another extension. Ignore the warning at this stage. Click **OK**.
5. In the **Extension** section of the window, select the extension for User B.
6. In the **Base Extension** field, change the extension to User A's extension.
7. Save the configuration back to the B5800 Branch Gateway system.
8. At each of the extensions, dial the log out short code set on the B5800 Branch Gateway system. The default is ***36**.
9. If either user is configured for **Forced Login**, they will have to complete the login process at their new extension using their Login Code.

About changing extension numbers

The default configuration for a new B5800 Branch Gateway system numbers each extension in sequence, going by module and port order, starting from 201. An extension entry is created in the configuration and also an associated user entry. A similar process occurs when a new extension expansion module is detected.

Important:

Extension versus User: It is important to understand that "extension number" is a user setting that belongs to and moves with the user. For example, a user can login at any phone and that phone then temporarily assumes the user's extension number and settings until they log off. The **Base Extension** value set for extensions in the B5800 Branch Gateway

configuration indicates the default associated user of the extension. It is not the extension number of that port.

Renumbering all extensions and users

About this task

Use this procedure to shift all user extension numbers up or down by a set amount. Any settings linked to those numbers are adjusted including extension Base Extension settings. It does not affect hunt group extension numbers.

Warning:

This procedure alters extension settings and therefore requires a system reboot when the configuration is sent to the B5800 Branch Gateway.

Procedure

1. Select **Tools** > **Extension Renumber**.
2. In the Renumber window, in the **Value** field, enter the amount by which you want to shift the current extension numbering of extensions and users.
3. Click **Add** or **Subtract** as appropriate.
4. Click **OK**.
5. Send the configuration back to the B5800 Branch Gateway and select the appropriate settings for the reboot.

Changing a user's extension number

Procedure

1. Select **User**.
2. Select the relevant user.
3. On the **User** tab, in the **Extension** field, change the extension number to the new number.
4. Click on another field.

   If an error warning appears it is most likely due to a conflict with an existing use of that extension number. Do one of the following:

   - Click **Cancel** to return the user to their original extension number.
   - If you are planning to change the other extension number, click **OK** and then edit the other entry.

Manager automatically propagates the number change to any hunt groups, incoming call routes, user buttons, bridged appearance buttons and call coverage appearance buttons associated with the user's original extension number.

If the user has an extension with which they are associated by being the extension's **Base Extension** setting, that setting is not automatically updated. If the user should still be associated with that extension by default, the extension must be updated manually to match the user's new extension number.

5. To update the user's Base Extension setting, select **Extension**.
6. On the **Extn** tab, in the **Base Extension** field, change the base extension number to match the user extension who should now be associated with that extension port by default.
7. Click **OK**.

Note:
If a validation error message appears due to a user being associated with two extensions, ignore the message until all the user moves have been completed.

8. Repeat steps 2 through 7 for each user whose extension number you need to change.
9. Click ✓ to revalidate the configuration and check that there are no conflicts between users and associated extensions.
10. Send the configuration back to the B5800 Branch Gateway and select appropriate settings for the reboot.

B5800 Branch Gateway software upgrade

The B5800 Branch Gateway Manager includes B5800 Branch Gateway software files for control units, external expansion modules and phones appropriate to the system's software level. The B5800 Branch Gateway system can be upgraded in two ways:

- Using the B5800 Branch Gateway Manager upgrade wizard. See Using the upgrade wizard on page 230.
- Using the System SD card. See System upgrade using the System SD card on page 267.

Note:
Check the latest B5800 Branch Gateway Technical Bulletin for the B5800 Branch Gateway software release before proceeding any further. It may contain information relating to

changes that occurred after this document was completed. Bulletins are available from http://support.avaya.com

- **Multiple Managers** — If more than one copy of Manager is running it is possible for the B5800 Branch Gateway system to request BIN files from a different Manager from the one that started the upgrade process. Ensure that only one copy of Manager is running when upgrading an B5800 Branch Gateway system.
- Other B5800 Branch Gateway applications — Upgrading the core software of the B5800 Branch Gateway control unit may require upgrades to associated software. Typically B5800 Branch Gateway is compatible with the previous release of most B5800 Branch Gateway applications, however for each B5800 Branch Gateway core software release there may be exceptions. See the Technical Bulletin for the B5800 Branch Gateway core software release for more information.

Creating a backup of the system configuration

About this task

Before performing an upgrade, ensure you have a current backup of the B5800 Branch Gateway system configuration. If you do not, use this procedure to create a backup of the system configuration.

Procedure

1. Start Manager.
2. Select **File > Open Configuration**.
3. In the Select B5800 Branch Gateway window, select the appropriate system.
4. Click **OK**.
5. Enter the name and password for a service user account on that system.
6. Click **OK**.
   A BOOTP entry for the system is created in Manager. This also confirms communication between the Manager PC and the B5800 Branch Gateway system.
7. Select **File** > **Save Configuration As...** and save a copy of the configuration file onto the PC.

Using the upgrade wizard

About this task

Before using the upgrade wizard, be sure you have a current backup of the system configuration. See Creating a backup of the system configuration on page 229 for more information.

Procedure

1. Start Manager.
2. Select **File** > **Advanced** > **Upgrade**.
   The UpgradeWiz scans for B5800 Branch Gateway modules using the address specified in the **Unit/Broadcast Address** field.
3. If the expected control units are not shown, adjust the address in the **Unit/Broadcast Address** field, and click **Refresh**.

   The current version of each B5800 Branch Gateway .bin file held in the control units memory is displayed. This is regardless of whether that .bin file is currently being used by any module in the system.

   In the **Available** column, Manager lists the versions of software it has available. If Manager detects that there is a higher version available, the check box for that row is automatically selected.
4. Click the check box for the modules you want to upgrade.
5. Click the check box for **Validate**.

   When this option is selected, the upgrade wizard checks the amount of free RAM memory available in the control unit to temporarily store the new bin files. If insufficient memory is available, you will be prompted whether to continue with an off-line upgrade or cancel upgrading. If offline is selected, the system is rebooted into offline mode. It may be necessary to use the **Refresh** option within the upgrade wizard to reconnect following the reboot. Validate upgrade can then be attempted again to check the amount of available RAM memory for transfer of bin files. If the memory is still insufficient, the option is offered to either do an unvalidated upgrade or cancel.

   During a validated upgrade, the bin files required are transferred to the system and stored in temporary memory. The backup system files and upload system files actions are performed. Once all file transfers are completed, the upgrade wizard promps whether it is okay to proceed with the upgrade process. Select **Yes** to continue. Each module being upgraded will delete its existing core software, restart and load the new software file that was transferred. This process may take several minutes for each unit.
6. Select the following options as appropriate:

- Click the check box for **Backup System Files** if, before upgrading to the new software, you want the current files in the System SD cards **/primary** folder copied to a **/backup** folder.
- Click the check box for **Upload System Files** if you want the full set of software files that Manager has to be copied to the **/primary** folder on the System SD card. In addition to control unit and module software this will include phone software files. Following the reboot, the phone will upgrade using those files if necessary.
- Click the check box for **Restart IP Phones** if you want all Avaya IP phones to be restarted following the upgrade and reboot. This will cause them to recheck whether the firmware they currently have loaded matches that on their configured file server. Use this option if the B5800 Branch Gateway system is the file server and the upgrade included new IP phone firmware.

7. Click **Upgrade**.
   The system password for each system is requested.
8. Enter the system password and click **OK**.

External output port (EXT O/P)

The B5800 Branch Gateway control unit is equipped with an external output port. The port is marked as EXT O/P and is located on the back of the control unit adjacent to the power supply input socket.

The port can be used to control up to two external devices such as door entry relay switches. The usual application for these switches is to activate relays on door entry systems. However, as long as the criteria for maximum current, voltage and if necessary protection are met, the switches can be used for other applications.

The switches can be switched closed, open or pulsed (closed for 5 seconds and then open). This can be done in a number of ways:

- Using B5800 Branch Gateway short codes.
- Through the Door Release option in B5800 Branch Gateway SoftConsole.
- Via the Open Door action in Voicemail Pro.

Default short codes: The following are the default short codes in the B5800 Branch Gateway configuration for external output switch operation. They use the short code features Relay On (closed), Relay Off (open) and Relay Pulse.

State	Switch 1	Switch 2
Closed	*39	*42

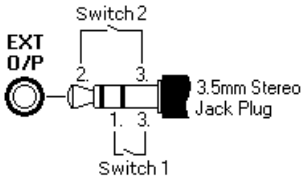
State	Switch 1	Switch 2
Open	*40	*43
Pulse	*41	*44

EXT O/P connections

EXT O/P ports use a standard 3.5mm stereo jack plug for connection. The B5800 Branch Gateway is able to open (high resistance), close (low resistance) or pulse (close for 5 seconds and then open) two switches within the port. Either switch can be operated separately. These switches are intended for activation of external relays in systems such as door opening systems.

Caution:

In installations where this port is connected to a device external to the building, connection must be via a towerMAX SCL/8 Surge Protector and a protective ground connection must be provided on the B5800 Branch Gateway control unit.

EXT O/P	Pin	Description
	1	Switch 1
	2	Switch 2
	3	0 Volts (Ground/Chassis)

- Switching Capacity: 0.7A
- Maximum Voltage: 55V d.c
- On state resistance: 0.7 ohms
- Short circuit current: 1A
- Reverse circuit current capacity: 1.4A
- Ensure that pins 1 and 2 are always at a positive voltage with respect to pin 3

3.5mm stereo audio jack plugs are frequently sold as pre-wired sealed modules. It may be necessary to use a multi-meter to determine the wiring connections from an available plug. Typically 3 (common to both relays) is the cable screen.

Example of BRI So8 module configuration

The ports on a BRI So8 module can be used for the connection of ISDN devices. Following are examples of how to configure a port on the BRI So8 module for an ISDN terminal and for video conferencing.

Example 1: ISDN terminal

About this task

In this example, calls on DID 123456 are routed to the first port of the So8 expansion module. That port has been configured as Line Group ID 701.

Procedure

1. Configure an incoming call routing. The destination is a short code that directs the call to the line group ID that contains the SO lines.

   The Bearer Capability has been set to **Any** to allow data and voice via this route.

   - Line Group ID: 0
   - Incoming Number: 123456
   - Destination: 123456
   - Bearer Capability: Any

2. Create a system short code. This is the destination used in the incoming call route.

   - Short Code: 123456
   - Telephone Number: 123456
   - Line Group ID: 701
   - Feature: Dial

3. Send the configuration to the control unit.
   Any call coming into the main system on DID 123456 will now be passed directly to the first port.

4. If you wish to assign DIDs from your main pool to individual ports and avoid network charges when dialing between them, try variations on the following:

   a) You have DID ranges, for example: 7325551000 to 7325551099. You wish to assign 7325551000-19 to port 1 and 7325551020-20 to port 2 etc.

b) Configure incoming call route. The # is used here instead of "n" to avoid problems with "Main". The minus sign means the number is processed from the left and so will wait for the whole number.
   - Line Group ID: 701
   - Incoming Number: -100x
   - Destination: #

c) Repeat for Line Group ID 702 etc.

d) Create short codes, for example:
   - Short Code: 100x
   - Telephone Number:
   - Line Group ID: 701
   - Feature: Dial

S0 calls dialed without the area code are handled locally without network charges. Calls with area calls will go via the network.

Example 2: video conference

About this task

In this example, calls are routed to a Polycom Viewstation module connected to a S0 port of the B5800 Branch Gateway system.

The following settings were used on 4 incoming data channels of a PRI line:

- Line Number: 5
- Channel Allocation: 23 -> 1
- Switch Type: 5ESS
- Line Sub Type: PRI
- Provider: AT&T
- Channels: 1-4
- Incoming Line Group: 95
- Outgoing Line Group: 95
- Direction: Bothway
- Bearer: Data
- Service: Accunet (this is a important)
- Admin: In Service

To route an incoming video call on the PRI lines configured above to an So8 module requires the following:

Procedure

1. Create a dial short code that has the SO port as its destination line group. For this example the following is used:
   - Short Code: 1500
   - Number:
   - Feature: Dial
   - Line Group: 601 (the So8 port number)
2. Create an incoming call routing that routes the appropriate calls to that short code. For this example the following is used:
   - Line Group: 95 (identifies calls using the PRI lines configured above)
   - Destination: 1500 (the short code created above)
   - Bearer: Any
3. To allow the video device on the S0 port to make outgoing calls to the PRI lines also requires a short code. For this example the following is used:
   - Code: 91N;
   - Number: N
   - Feature: Dial
   - Line Group: 95

   Polycom Video module settings

   The Polycom modules used in the previous example were the Viewstation 128, Viewstation 256 and Viewstation MP.

   The Polycom module must have software that supports 'Standard ETSI ISDN' (European ISDN) and have its ISDN Switch Protocol setting set to 'Standard ETSI Euro-ISDN'

   The following were the settings used during testing:

Characteristics	Admin/Software and Hardware/ Software
• Polycom View Station 512 MP • NTSC UIS Interface • View Station PVS 1419	• Software: 7.0.1 • Network Interface: S/T Interface • ISDN Version: IEUS v18:a00320
Admin/General Setup	**Admin/Video Network/ISDN Video Network**

Characteristics	Admin/Software and Hardware/ Software
• Country: USA • Language: English (USA) • Auto Answer: Yes • AllowDial: Yes • Allow User Setup: Yes • Maximum Time on Call: 480	• Country Code: 1 • Area Code: 732 • Number A: blank • Number B: blank • ISDN Switch Protocol: Standard ETSI Euro-ISDN
User Setup	**Admin/Video Network/IMUX**
• Auto Answer: Yes • PIP: Auto • Far Control of Near Camera: Yes • MP Mode: Auto	• Numbers: blank • SPID: blank • Audio Quality: 168KB/s • Advanced Dialing: Dial Channels in Parallel
System Information	**Admin/Software and Hardware/ Hardware**
• Release: 7.0.1 • Model: VS: 512	• Camera: NTSC • Video Comm Interface: ISDN_Quad_BRI • Network Interface Type: S/T Interface
Admin/Video Network	**Admin/Video Network/Call Preference**
• MultiPoint Setup: Auto	• ISDN Video Calls (H:320): Yes

SNMP

SNMP (Simple Network Management Protocol) is a standard network protocol that allows the monitoring and management of data devices across a network. An SNMP agent can be built into network devices such as routers and hubs. An SNMP manager application, for example CastleRock or HP OpenView, can then communicate with those devices.

B5800 Branch Gateway supports SNMP communication. This communication can be:

- **Polling:** Some SNMP applications (called "managers") send out polling messages to the network. They then record the responses of any SNMP enabled devices (called "agents").

This allows the application to create a network map and to raise an alarm when devices previously present do not respond.

- Most SNMP manager applications can also do simple IP address polling to locate non-SNMP enabled devices. However this method of polling does not identify the device type or other information.
- SNMP polling including details about the responding device. For example an B5800 Branch Gateway control unit's response includes the control unit type, level of software, routing table information, up time, etc.

- **Traps:** When certain events occur, a devices SNMP agent can send details of the event to the SNMP manager. This is called an SNMP trap. These appear in the event log of the SNMP manager. Most SNMP managers can be configured to give additional alerts in response to particular traps.
- **Management:** Some SNMP agents support device management and configuration changes through the SNMP manager interface. This is not supported by B5800 Branch Gateway.

B5800 Branch Gateway SNMP operation has been tested against Castle Rock SNMPc-EE 5.1.6c and HP OpenView Network Node Manager 6.41.

What information is available via SNMP

As described above, SNMP information can either be polled by the SNMP application or received as the result of the B5800 Branch Gateway sending SNMP trap information.

While the MIB files should not be edited, they can be read using a text editor and contain descriptions of all the various information objects that can be polled or sent and the information that each object will include. For a list of the MIB files, see Installing the B5800 Branch Gateway MIB files on page 237. The NOTIFICATION-TYPE objects are those used for SNMP traps. The other types of objects are those that can be polled.

Installing the B5800 Branch Gateway MIB files

To allow full communication between an SNMP agent and an SNMP manager, the SNMP manager must load MIB files (Management Information Base) specific to the SNMP agent device and the features it supports. These MIB files contain details of the information the agent can provide and the traps that it can send.

The MIB files for B5800 Branch Gateway operation are included on the B5800 Branch Gateway DVD in the folder **\AdminCD\smnp_mibs**. The actual files required and the method of loading depend on the SNMP manager application being used. The details below cover the two SNMP manager applications supported.

HP OpenView Network Node Manager

Procedure

1. Copy the following MIB files to the application's MIB folder.

MIB File	Source
rfc2737-entity-mib.mib	snmp_mibs\standard folder on OpenView Install CD.
avayagen-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.
ipo-prod-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.
ipo-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.
inet-address-mib.mib	\AdminCD\snmp_mibs\Standard folder on B5800 Branch Gateway Admin DVD.
rfc2213-integrated-services-mib.mib	\AdminCD\snmp_mibs\standard folder on OpenView Install CD.
diffserv-dscp-tc.mib	\AdminCD\snmp_mibs\Standard folder on B5800 Branch Gateway Admin DVD.
diffserv-mib-hpov.mib	\AdminCD\snmp_mibs\Standard folder on B5800 Branch Gateway Admin DVD.
ipo-phones-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.

2. Start the OpenView Network Node Manager console.
3. Select **Options** and then Load/Unload MIBs: SNMP.
4. Select **Load** and select all the MIB files listed above.
5. Select **Compile**.

Castlerock SNMPc 5.1.6c and earlier

Procedure

1. Copy the following MIB files to the application's MIB folder. This folder is typically C:\Program Files\SNMPc Network Manager\mibfiles.

MIB file	Source
ENTITY-MIB	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
AVAYAGEN-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.
IPO-PROD-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.
IPO-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.
INET-ADDRESS-MIB.mib	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
INTEGRATED-SERVICES-MIB	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
DIFFSERV-DSCP-TC.mib	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
DIFFSERV-MIB.mib	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
IPO-PHONES-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.

2. In SMNPc select **Config > MIB Database**.
3. Select **Add** and select the MIB files listed above in the order listed.

Castlerock SNMPc V5.0.1

Procedure

1. Copy all of the B5800 Branch Gateway MIBs and standard MIBs from the B5800 Branch Gateway Administrator Applications DVD to the SNMPc mibfiles directory.
2. In the SNMPc mibfiles directory open the files STANDARD.mib and SNMPv2-SMI.mib in Notepad.

3. In the SNMPv2-SMI.mib file find the definition of zeroDotZero and copy this to the clipboard.
4. In the STANDARD.MIB file find the SNMPv2-SMI section and paste in the definition of zeroDotZero from the clipboard before the end of this section (just before the END statement).
5. Save the modified STANDARD.MIB file.
6. Add the MIB file SNMP-FRAMEWORK-MIB.mib to the MIB database.
7. Add all the MIB files in the order listed.
8. Compile the MIBs ready for use.

Note:

The IPO-PHONES-MIB.mib relies upon the DIFFSERV-MIB.mib for the definition of the textual convention of IndexInteger. The DIFFSERV-MIB needs the definition of the textual convention zeroDotZero which is normally defined in SNMPv2-SMI.mib. However including SNMPv2-SMI.mib in the MIB file compilation list results in errors due to conflicts with what appear to be internal definitions within SNMPc and the SNMPv2-SMI section in its STANDARD.mib file. Therefore to resolve the issue the required definition of zeroDotZero must be placed in the SNMPv2-SMI section in SNMPc's STANDARD.mib file.

Enabling SNMP and polling support

About this task

In order for the B5800 Branch Gateway control unit to be discovered and polled by an SNMP manager, its SNMP agent must be enabled and placed in the same read community as the SNMP manager.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **System Events** tab.
4. Select **SNMP Enabled**.
5. In the **SNMP Port** field, enter the UDP port number used by the SNMP agent to listen for and respond to SNMP traffic.

   The default is 161.
6. In the **Community (Read-only)** field, enter the community to which the device belongs for read access.

   This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to

establish communication and then changed (at both the SNMP agent and manager ends) for security.

7. Click **OK**.
8. Select **File > Save Configuration** to send the configuration back to the B5800 Branch Gateway and then select **reboot**.
   After the reboot, the SNMP manager will be able to discover the control unit. The discovery includes the control unit type and the current level of core software.

Enabling SNMP trap sending

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **System Events** tab.
4. In the **Configuration** sub-tab, in the **SNMP Agent** section, ensure the **SNMP Enabled** check box is selected.
5. In the **Community (read-only)** field, enter the SNMP community name to which the system belongs.

   This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
6. In the **SNMP Port** field, accept the default.
7. In the **Device ID** field, enter the alarm ID or PID of the registered system.

   Note:

   This enables product alarming back to Avaya via the Secure Access Link (SAL). The unique alarm ID is included in the var-bind of all SNMP trap notifications sent by the system. The alarm ID, or PID, is parsed out of the alarm and used for automatic case creation by matching the registered system's customer record with the alarm event.
8. In the **Contact** field, enter contact information as appropriate.
9. In the **Location** field, enter location information as appropriate.
10. Click the **Alarm** tab.
11. Click **Add**.
12. In the **New Alarm** section, do the following:

    a) Click the **Trap** option button.

b) In the **IP Address** field, enter the IP address of the PC running the SNMP manager application.
c) In the **Port** field, enter the port on which the trap messages should be sent.
This is the UDP port on which the B5800 Branch Gateway sends SNMP trap messages. The default is 162.
d) In the **Community** field, enter the community that will be used by the agent and the SNMP manager.

13. In the **Events** section, click the check boxes for the events you want to send.
See the Manager on-line help for a description of the events.
14. Click **OK**.
15. Select **File > Save Configuration** to send the configuration back to the B5800 Branch Gateway and then select **reboot**.

DTE port maintenance

The DTE port on the back of control unit is not normally used when configuring an B5800 Branch Gateway system. However, in extreme cases, the DTE port can be used to default the system's configuration or to erase the core software if necessary.

Warning:
The procedures in this section should only be performed if absolutely necessary to return a system back to working order. In all cases, you must have a backup copy of the system configuration before you perform these procedures. See Creating a backup of the system configuration on page 229.

The DTE ports on B5800 Branch Gateway expansion modules are not used for any maintenance or diagnostics.

RS232 DTE port settings

The RS232 DTE ports are located on the rear of all control units and external expansion modules. The DTE ports on external expansion modules are not used. The RS232 DTE ports on the control units can be used for system maintenance and connection of serial terminal adaptors.

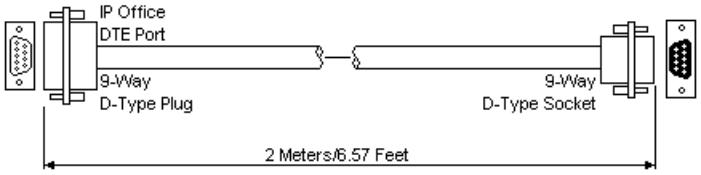
An asynchronous terminal program such as HyperTerminal is also required. Configure this for operation via a PC serial port, as follows:

Bits per second	38,400	**Parity**	None	**Flow Control**	None

Data bits	8	**Stop Bits**	1	**Settings** > **Emulation**	TTY

DTE cables

These cables are used for system maintenance and diagnostics under Avaya guidance. They can also be used for connection of RS232 serial terminal adaptor equipment to the control unit. This cable is a "Straight through DB9 female to DB9 male serial cable."



9-Way RS232 DTE Port	Signal	PC/Terminal Adaptor
3	⬅Receive data	3
2	➡Transmit Data	2
7	⬅RTS (Request To Send)	7
8	➡CTS (Clear To Send)	8
6	➡DSR (Data Set Ready)	6
5	●Ground	5
1	➡DCD (Data Carrier Detect)	1
4	⬅DTR (Data Terminal Ready)	4
9	➡RI (Ring Indicator)	9

About erasing the configuration

The following procedures erase the B5800 Branch Gateway configuration stored in the control unit. This includes both the current configuration being used in RAM memory and the backup configuration stored in non-volatile memory. Following this, the B5800 Branch Gateway will restart with a default configuration.

These procedures should be performed from a PC with a fixed IP address, directly connected to the B5800 Branch Gateway control unit and with the B5800 Branch Gateway system disconnected from any network. The control unit IP address will default to 192.168.42.1.

Important:

Do not perform any of these processes unless absolutely necessary. The configuration settings can be returned to the default settings using Manager by selecting **File** > **Advanced** > **Erase Configuration** command.

Erasing the configuration via debug

About this task

This procedure erases the system's configuration settings but does not alter the security settings. It is easier to use than the boot loader method. Before you perform this procedure, be sure you have a current backup of the system configuration. See Creating a backup of the system configuration on page 229 for more information.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.
2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 242. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Enter `AT` (upper case).

   An `OK` response appears.
4. Enter `AT-DEBUG`.

   The time and date and then the `Hello>` prompt appears to show the system is ready to accept commands.
5. To erase the current configuration in RAM memory, enter `eraseconfig`.

   The `Hello>` prompt reappears.
6. To erase the backup configuration stored in non-volatile Flash memory enter **erasenvconfig**.

   The `Hello>` prompt reappears.
7. To reboot the system, enter `reboot`.

   The system reboots and restarts with a defaulted configuration.
8. Close the terminal program session.
9. Use Manager to edit and then upload an old configuration file or receive and edit the system's now defaulted configuration.

Erasing the configuration and security settings via the boot loader

About this task

This procedure erases the system's configuration settings and the security settings and resets them to the default settings. Before you perform this procedure, be sure you have a current

backup of the system configuration. See Creating a backup of the system configuration on page 229 for more information.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.
2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 242. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Arrange the program windows so that the terminal program and Manager TFTP log are visible at the same time.
4. Switch off power to the control unit.
5. Power on the control unit and press the escape key every second until you get a loader message. An example of this message is:

   ```
   P12 Loader 2.4

   CPU Revision 0x0900
   ```
6. Enter `AT` (upper case).

   An `OK` response appears. If `OK` does not appear, check the settings of your terminal program.
7. To erase the alarm log, enter `AT-X1`.
8. To erase the backup configuration stored in non-volatile memory, enter `AT-X2`.
   An `OK` response appears.
9. To erase the current configuration in RAM memory, enter `AT-X3`
   A series of `OK` responses appear.
10. Switch power to the control unit off and then back on.

    Messages appear as the control unit performs the start-up tasks.
11. Close the terminal program session.
12. Use Manager to edit and then upload an old configuration file or receive and edit the system's now defaulted configuration.

Resetting the security settings to the default settings

About this task

This procedure resets the systems security settings back to the default settings but does not alter the configuration settings.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.
2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 242. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Enter AT (upper case).

   An OK response appears. If OK does not appear, check the settings of your terminal program.
4. Enter AT-SECURITYRESETALL.
   You are prompted to confirm the control unit's MAC address.
5. Enter the MAC address.
   An OK response appears.
6. Close the terminal program session.
7. Use Manager to edit the system's now defaulted security settings.

Resetting the configuration and security settings to the default settings via the boot loader

About this task

This procedure erases the system's configuration settings and the security settings and resets them to the default settings. Before you perform this procedure, be sure you have a current backup of the system configuration. See Creating a backup of the system configuration on page 229 for more information.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.

2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 242. Within a HyperTerminal session, the current settings are summarized across the base of the screen.

3. Arrange the program windows so that the terminal program and Manager TFTP log are visible at the same time.
4. Switch off power to the control unit.
5. Power on the control unit and press the escape key every second until you get a loader message. An example of this message is:

   ```
   P12 Loader 2.4
   CPU Revision 0x0900
   ```

6. Enter AT (upper case).

   An OK response appears. If OK does not appear, check the settings of your terminal program.

7. To erase the backup configuration stored in non-volatile memory, enter AT-X2.
   An OK response appears.
8. To erase the current configuration in RAM memory, enter AT-X3
   A series of OK responses appear.
9. Switch power to the control unit off and then back on.

   Messages appear as the control unit performs the start-up tasks.

10. Close the terminal program session.
11. Use Manager to edit and then upload an old configuration file or receive and edit the system's now defaulted configuration.

About erasing the operational firmware

When the firmware loaded by the control unit is erased, the control unit begins making BOOTP requests for a replacement firmware file. Manager can act as a BOOTP server and respond to the control units request with the appropriate file from those installed with Manager.

When the firmware loaded by the B5800 Branch Gateway control unit is erased, the control unit will first look for replacement firmware on the System SD card before falling back to using a BOOTP request to Manager.

The procedure should be performed from a PC with a fixed IP address, directly connected to the B5800 Branch Gateway control unit and with the B5800 Branch Gateway system disconnected from any network. During the process, the control unit's IP address may default

to a value in the 192.168.42.1 to 192.168.42.10 range. If this occurs it may be necessary to amend the BOOTP entry in Manager to match the address the system is using.

Important:

- Do not erase the core software unless absolutely necessary. The B5800 Branch Gateway software can normally be upgraded using Manager. See B5800 Branch Gateway software upgrade on page 228 for more information.
- These procedures erase the operational software. Before performing these procedures, you must know the MAC and IP addresses of the system, plus have a system backup and the correct .bin file for the control unit type and level of software.
- The presence of any firewall blocking TFTP and or BOOTP will cause these procedures to fail.

Erasing the core software via debug

Procedure

1. Start Manager.
2. In the **BOOTP** entries, check that there is an entry that matches the MAC address, IP address and .bin file used by the system. An entry is normally automatically created when a configuration has been loaded from the B5800 Branch Gateway system.
3. If an entry is not present, do the following:
   a) Create a new entry manually. The MAC address and IP address can be found in the control unit settings in the configuration file.
   b) Close Manager.
   c) Restart Manager.
4. Under **File** > **Preferences** ensure that Manager is set to 255.255.255.255. Also check that **Enable BootP Server** is checked.
5. Select **View** > **TFTPLog**.
6. Check that the required .bin file is present in Manager's working directory.
7. Attach the serial cable between the PC and the DTE port on the control unit.
8. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 242. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
9. Enter AT (upper case).

An `OK` response appears.

10. Enter `AT-DEBUG`.

    The time and date and then the `Hello>` prompt appears to show the system is ready to accept commands.

11. To erase the current configuration in RAM memory enter `upgrade`.
    The B5800 Branch Gateway system erases the current software and then sends out a BOOTP request on the network for new software. Manager responds and starts transferring the software using TFTP.

Erasing the core software via the boot loader

Procedure

1. Start Manager.
2. In the **BOOTP** entries, check that there is an entry that matches the MAC address, IP address and .bin file used by the system. An entry is normally automatically created when a configuration has been loaded from the B5800 Branch Gateway system.
3. If an entry is not present, do the following:
   a) Create a new entry manually. The MAC address and IP address can be found in the control unit settings in the configuration file.
   b) Close Manager.
   c) Restart Manager.
4. Under **File** > **Preferences** ensure that Manager is set to 255.255.255.255. Also check that **Enable BootP Server** is checked.
5. Select **View** > **TFTPLog**.
6. Check that the required .bin file is present in Manager's working directory.
7. Attach the serial cable between the PC and the DTE port on the control unit.
8. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 242. Within a HyperTerminal session, the current settings are summarized across the base of the screen.

9. Arrange the program windows so that the terminal program and Manager TFTP log are visible at the same time.
10. Switch off power to the control unit.

11. Power on the control unit and press the escape key every second until you get a loader message. An example of this message is:

    ```
    P12 Loader 2.4

    CPU Revision 0x0900
    ```

12. Enter `AT` (upper case).

    An `OK` response appears. If `OK` does not appear, check the settings of your terminal program.

13. Enter `AT-X`.
    Multi-Sector Erase response appears. The control unit then requests the .bin file that is stored on the System SD card.

14. If the files do not appear to be transferring, check that the IP address shown in the TFTP log matches the BOOTP entry. Adjust the BOOTP entry if necessary.
    When the file transfers are completed, the system reboots.

Reset button

The **Reset** button is on the control unit. Pressing the button while the control unit is starting up will pause the start up until the button is released. The effect of pressing the button during normal operation will depend on how long the button is pressed and is indicated by the CPU LED.

Press Duration (seconds)	CPU LED	Action	Summary
0 to 5	Off	None	None
5 to 10	Orange	Reboot when free	Reboot when free with new incoming/outgoing call barring. A reboot using the reset button is recorded in the audit trail.
10 to 30	Flashing orange	Erase configuration/ immediate reboot	Erase the configuration, alarm log and audit trail. Immediate reboot without waiting for active calls to end. See About erasing the configuration on page 243 for more information.
30 to 40	Red	Erase all	Erase configuration, alarm log and core software. See About erasing the operational firmware on page 247 for more information.

Press Duration (seconds)	CPU LED	Action	Summary
Over 40	Flashing green	None	None

AUX button

The **AUX** button is on the control unit. If the AUX button is pressed during a restart of the control unit, the control unit skips booting from the /primary folder on the System SD card. If the AUX button is pressed for more than 5 seconds when a system is running, the control unit will shutdown for 10 minutes.

Creating a WAN link

About this task

This procedure is a high level procedure for creating a data link from Site A to Site B via the WAN ports. For this example the IP address is 192.168.43.1.

Procedure

1. At Site A, on IP address 192.168.43, create a normal service.

   The service name can be any text and is used to identify this particular service. The account name and password entered for the service are presented to the remote end, therefore must match the user name and password configured at Site B. The Encrypted Password option can only be used if the remote end also supports CHAP.

2. Create a user.

   Under the **Dial In** tab, select **Dial In On**. This User account is used to authenticate the connection from the Site B. Note that if the service and user have the same name these two configuration forms are automatically linked and become an Intranet service. The user password is displayed at the bottom of the Service tab as the Incoming Password.

3. Setup RAS.

   If CHAP is to be used on this link, then the Encrypted Password option must be checked in the service and in the RAS service. The name of the RAS service must match the name of the service at Site B. Note that if the RAS settings are given the same name as the service and user they are automatically linked and become a WAN service. Ensure that the Encrypted Password option is not checked when using a WAN service.

4. Edit the WAN port.

   Do not create a new WAN port. The WAN port is automatically detected. If a WAN port is not displayed, connect the WAN cable, reboot the control unit and receive the configuration. The WAN port configuration form should now be added.

5. Create an IP Route.

   In the **IP address** field enter the network address of the remote end — *not* the IP address of the control unit. Under **Destination** select the service created above.

6. At Site B, on IP address 192.168.43, repeat steps 1 through 5 but alter the details to create a route from Site B to Site A.

Chapter 14: SD card management

There are two SD card slots on the control unit. They are labeled **System SD** and **Optional SD**.

System SD card slot

- An Avaya System SD card must be present in this slot at all times. This card holds copies of the B5800 Branch Gateway firmware and configuration and is used as the control units non-volatile memory.
- Each System SD card has a unique Feature Key serial number which is used for generating and validating licenses entered into the B5800 Branch Gateway configuration.
- The card stores the prompts for Embedded Voicemail operation and acts as the message store for embedded voicemail messages.
- Prior to any planned shutdown or restart of the B5800 Branch Gateway system, the current configuration running in the system's RAM memory is copied to the primary folder on the System SD card and to the systems non-volatile memory.
- Following a restart, the software in the primary folder is loaded by the control unit. If the required software is not present or valid, a sequence of fallback options is used, see Booting from the SD Cards on page 256 for more information.
- Following a restart, the configuration file, if present, in the primary folder is loaded by the control unit. If no file is present the system will check for a file in its internal non-volatile memory. If no copy is found it will generate a default configuration file. See Booting from the SD Cards on page 256 for more information.
- Once each day (approximately between 00:00 and 00:30) the B5800 Branch Gateway will copy the current configuration running in its RAM memory to the primary folder on the card.
- Configuration changes made using Manager are first written to the copy of the configuration file on the card and then merged with the configuration running in the system's RAM memory.
- The write lock setting on cards in the System SD card slot is ignored.

Optional SD card slot

- A card does not have to be present in this slot for normal B5800 Branch Gateway operation. The slot can be used for various maintenance actions.
- A card with updated B5800 Branch Gateway software or configuration can be inserted into the Optional SD card slot and those files are then transferred to the System SD card in order to upgrade the B5800 Branch Gateway system.
- The full contents of the System SD card can be copied to the Optional SD card while the B5800 Branch Gateway system is running.
- The write lock setting on cards in the Optional SD card slot is honored.

Warning:

Memory cards should always be shut down before being removed when the system is running. Though the card slot LEDs indicate when data is being written to a card, lack of flashing LEDs is not a sufficient safeguard. Shutting down the card will disable embedded voicemail if being used. If the System SD card is removed, features licensed by the card's Feature Key serial number will continue operating for up to 2 hours.

Card maintenance

Using Manager, the System Status application, or a phone configured as a system phone, you can perform the following procedure on the SD cards.

Procedure	Description	Manager	System Status	System Phone	Minutes
Backing up the primary folder using Manager on page 260	Copy the files in the primary folder on the System SD card to the/backup folder on the card.	✓	✓	✓	6
Restoring from the backup folder using Manager on page 262	Copy the files in the backup folder on the System SD card to the primary folder on the card and restart the B5800 Branch Gateway system.	✓	✓	✓	6
Backing up to the Optional SD card using Manager on page 264	Copy all the files on the System SD card to the Optional SD card.	✓	✓	✓	90
Upgrading using an Optional SD card on page 269	Copy the configuration file in the primary folder on the Optional SD card to the primary folder on the System SD card and then restart the B5800 Branch Gateway system.	✓	–	–	15
Upgrading remotely using Manager on page 268	Upload a set of B5800 Branch Gateway software and embedded voicemail prompts to the System SD card.	✓	–	–	40
Viewing the card contents on page 260	View the folders and files on the control unit memory cards.	✓	–	–	–
The following procedures can be performed on cards in an SD card reader on a PC running Manager.					
Formatting an SD card on page 258	Reformat a card for B5800 Branch Gateway use without removing the Feature Key serial number.	✓	✓	–	1

Procedure	Description	Manager	System Status	System Phone	Minutes
	Caution: This process will erase all existing files on the card.				
Recreate on page 257	Create the folder structure on a memory card and copy a set of B5800 Branch Gateway software files into those folders.	✓	–	–	15

Card specification

Non-Avaya cards can be used in the Optional SD card slot as long as they match or exceed the following standard:

SDHC 4GB minimum Class 2+. Single partition FAT32 format.

SD card folders

The System SD card contains the following folders:

- **primary** — contains the firmware files for the control unit, external expansion modules and supported phones. The folder can also contain music on hold files and license key files. This is the main set of files used by the B5800 Branch Gateway system when booting up. It also contains the stored copy of the B5800 Branch Gateway configuration.
- **backup** — contains a copy of the primary folder at some previous point. A backup copy of the primary contents to this folder can be invoked manually (using Manager or SSA) or as part of the B5800 Branch Gateway software upgrade using Manager.
- **lvmail** — a sub-folder that is used to store individual user and group mailbox messages, name recordings and announcements used by Embedded Voicemail. The storage capacity for Embedded Voicemail is limited to 15 hours regardless of the capacity of the card. Mailbox messages and greetings are stored in a sub-folder of the /dynamic folder.
- **AAG** — a sub-folder that is used to store embedded voicemail auto-attendant greetings.
- **doc** — contains initial installation documentation for B5800 Branch Gateway .
- **dynamic** — contains files used by the B5800 Branch Gateway and retained through a reboot of the B5800 Branch Gateway system.
- **temp** — contains temporary files used by the B5800 Branch Gateway and not retained through a reboot of the B5800 Branch Gateway system.

The Optional SD card can contain a similar set of folders as the System SD card. The Optional SD card folders are used as an additional backup or they can be used as the source for upgrading the contents of the System SD card.

Booting from the SD cards

When being powered up, the control unit looks for a valid .bin binary file to load. It does this using the possible source below in the order shown, skipping to the next source if the file is not present or is not valid.

1. System SD card primary folder.
2. The control unit's own internal non-volatile memory. Once a system has been installed, it uses its non-volatile memory to keep copies of the configuration and system binary files it is using. These can be used to restore operation during a system reboot. Note that though a system can boot from non-volatile memory, a System SD card must still be present for correct system operation.
3. System SD card backup folder.
4. Optional SD card primary folder.
5. Optional SD card backup folder.
6. If no file is found, the control unit will fallback to making BOOTP requests to the network. Manager can respond to the BOOTP request. See About erasing the operational firmware on page 247 for more information.

Once a valid .bin file is found, the control unit loads that firmware. The source from which the control unit binary file was loaded is then used to load further files.

Configuration file loading

After the system firmware files are installed, a configuration file must be installed on the control unit.

- If the control unit booted using binary files from an SD card location, it looks for a valid configuration file in the same location.
  - If a configuration file is present and valid, it is loaded.
  - If a configuration file is present but is not valid, load the configuration copy in its non-volatile memory if present. Otherwise, the control unit will have a default configuration.
  - If a configuration file is not present, use the non-volatile memory copy unless the reboot is as a result of a default system command.
- If the control unit booted using binary files from its non-volatile memory, it will also load the configuration copy from that location.
  - It will indicate a boot alarm (see **Boot alarms** below).
  - It will attempt to restore the firmware file in the System SD card /primary folder using the copy in its non-volatile memory.

- The normal boot-up process of upgrading expansion module firmware does not occur. If the **File** > **Advanced** > **Upgrade** command is used, only external expansion modules actually present in the system are listed for upgrade.

Post boot operation

During normal operation, configuration and binary files sent to the System SD card /primary folder using Manager are also written to the non-volatile memory.

If the system has booted from its non-volatile memory due to an SD card problem, it is still possible to upgrade the .bin file using the B5800 Branch Gateway upgrade wizard. See B5800 Branch Gateway software upgrade on page 228 for more information.

Boot alarms

The following apply if the control unit boots up using software other than that in its System SD primary folder:

- An alarm will be shown in the System Status application. It will also generate an alarm if the card in any slot is not compatible. These alarms are also output as SNMP, Syslog or email alarms.
- The Manager **Select IP Office** window will display an ⚠ icon indicating that the system is running using software other than from the System SD card's primary folder.
- The configuration can be read but will be read only. Attempting to send a configuration to the system will cause the error message `Failed to save configuration data. (Internal error)`.

Bypassing the System SD card primary folder

The control unit can be forced to bypass the System SD card's primary folder and non-volatile memory when starting. This is done by pressing the **AUX** button while applying power to the control unit. This may be necessary if, following an upgrade of the B5800 Branch Gateway system, it is determined that a roll back to the previously backed up firmware and configuration is required. Using the **AUX** button should restore system operation using the backup folder files while the installer then restores the contents of the primary folder to a previous release.

About creating an B5800 Branch Gateway SD card

The procedures in this section are for B5800 Branch Gateway SD cards for use in the System SD card slot. They can also be applied to non-Avaya SD cards for use in the Optional SD card slot. For the System SD card slot, only Avaya SD cards with a Feature Key should be used.

The card must be in the following format:

SDHC 4GB minimum Class 2+. Single partition FAT32 format.

⚠ Warning:

Avaya supplied SD cards should not be formatted using any other method than the format commands within Manager and the System Status application. Formatting the cards using

any other method will remove the feature key used for B5800 Branch Gateway licensing from the card.

These procedures are run on an SD card inserted in a card reader on the Manager PC. That card can then be used in the System SD card slot of a new system or in the Optional SD card slot of an existing system to upgrade that system.

Formatting an SD card

About this task

Avaya SD cards should only be formatted using the format options provided within the B5800 Branch Gateway applications.

Warning:

This procedure will erase any existing files and folders on the card.

Procedure

1. Start Manager.
2. Insert the SD card into a reader slot on the Manager PC.
3. Select **File** > **Advanced** > **Format IP Office SD Card**.
4. Select one of the following:
   - **IP Office A-Law**
   - **IP Office U-Law**

   Choose the label that matches the file set you will be placing on the card. This step designates the card label that appears when viewing the card details. It does not affect the actual formatting.
5. Browse to the card location and click **OK**.
   The status bar at the bottom of Manager displays the progress of the formatting process.
6. When the formatting is complete, load the B5800 Branch Gateway folders and files onto the card from the Manager PC. See Recreating an SD card on page 259.

Formatting a System SD card using the System Status application

Procedure

1. Start the System Status application and access the System Status output.

2. In the navigation panel, select **System > Memory Cards > System SD**.
3. Click on the **Format** button at the bottom of the screen.
   The card is reformatted. All files and folders on the card will be deleted. This process takes a few seconds.

Recreating an SD card

About this task

This procedure creates the folder structure on the SD card and copies the required firmware files from those installed with Manager onto the SD card. This includes the binary files for the system, any external expansion modules, and phones. It also includes the prompt files for embedded voicemail operation.

This procedure can be used to upgrade an existing SD card to match the file set installed with Manager. For the card to be used in the System SD card slot, the card must be an Avaya SD Feature Key card. The card must be correctly formatted. See Formatting an SD card on page 258.

If the card contains any dynamic system files, for example SMDR records, they are temporarily backed up by Manager and then restored after the card is recreated. This procedure takes approximately 15 minutes.

Procedure

1. Insert the SD card into a card reader on the Manager PC.

   Note:
   Do not remove the SD card. Removing the SD card will interrupt the upgrade.
2. Using Manager, select **File** > **Advanced** > **Recreate IP Office SD Card**.
3. Select one of the following:

   - **IP Office A-Law**
   - **IP Office U-Law**

   This selection determines how the system operates when defaulted with the SD card installed in the System SD card slot.
4. Browse to the card location and click **OK**.
   Manager starts creating folders on the SD card and copying the required files into those folders. This process takes approximately 15 minutes. Do not remove the SD card until the Manager status bar at the bottom shows a **Ready** message.

Viewing the card contents

About this task

Using Manager you can view the folders and files on the System SD card and the Optional SD card.

Procedure

1. Start Manager.
2. Select **File > Embedded File Management**.
3. From the Select IP Office window, select the B5800 Branch Gateway system you want to view.
   The file contents of the memory cards are displayed.

About backing up the System SD card

There are two levels of backup that can be performed.

- **Backup the System SD card primary folder** — The contents of the primary folder on the System SD card are copied to the backup folder on the System SD. This can be performed remotely.
- **Backup all files on the System SD card** — The contents of the primary folder, backup folder, and embedded voicemail files including message files on the System SD card are copied to the Optional SD card. This can be performed remotely. However, the contents can only be copied back manually using a card reader.

Note:

The backup, restore, and copy operations will not be performed if the destination card has insufficient space for the files being copied.

Backing up the primary folder using Manager

About this task

This procedure copies the contents of the primary folder on the System SD card to the backup folder on the System SD card. Files with matching file names are replaced. This procedure takes approximately 6 minutes.

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Backup System Files**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.

Backing up the primary folder using the System Status application

Procedure

1. Start the System Status application and access the B5800 Branch Gateway status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Backup System Files**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.

Backing up the primary folder using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **System Backup**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.

About restoring from the backup folder

When you restore from the backup folder, you copy the contents of the backup folder on the System SD card to the primary folder on the System SD card. Files with matching file names are replaced.

Warning:

This procedure will cause the B5800 Branch Gateway system to be restarted, disconnecting any current calls and services in progress.

Restoring from the backup folder using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Restore System Files**.
   The contents of the backup folder on the System SD card are copied to the primary folder on the System SD card. The process takes approximately 6 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring from the backup folder using the System Status application

Procedure

1. Start the System Status application and access the B5800 Branch Gateway status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Restore System Files**.
   The contents of the backup folder on the System SD card are copied to the primary folder on the System SD card. The process takes approximately 6 minutes. When

the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring from the backup folder using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **System Restore**.
   The contents of the backup folder on the System SD card are copied to the primary folder on the System SD card. The process takes approximately 6 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

About backing up to the Optional SD card

Backing up to the Optional SD card copies all files on the System SD card to the Optional SD card. This includes contents of the primary folder, backup folder, and embedded voicemail files including message files. Matching files and folders on the Optional SD card are overwritten.

Any files already copied that change while this process is running are not recopied. Any new files added (for example voicemail messages) while the process is running may not be copied.

Backing up to the Optional SD card takes at least 90 minutes and may take much longer depending on the amount of data to be copied. For example, it will take longer if embedded voicemail is being used by the B5800 Branch Gateway system to take messages.

Backing up to the Optional SD card using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Copy System Card**.
   The contents of the System SD card are copied to the Optional SD card. This takes at least 90 minutes and can take much longer.

Backing up to the Optional SD card using the System Status application

Procedure

1. Start the System Status application and access the B5800 Branch Gateway status output.
2. In the navigation panel select **System**.
3. Select **Memory Cards**.
4. Select **System Card**.
5. At the bottom of the screen select **Copy System Card**.
   The contents of the System SD card are copied to the Optional SD card. This takes at least 90 minutes and can take much longer.

Backing up to the Optional SD card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.

2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **Copy**.
   The contents of the System SD card are copied to the Optional SD card. This takes at least 90 minutes and can take much longer.

About restoring from the Optional SD card

The files in the primary folder on the Optional SD card can be copied to the primary folder on the System SD card. Files with matching file names are replaced.

There are two levels of restore that can be performed:

- **Restoring only configuration files from the Optional SD card** — Only the configuration file config.cfg and the licenses file keys.txt are copied from the Optional SD card to the System SD card.
- **Restoring only software files from the Optional SD card** — All files in the primary folder *except* the configuration file config.cfg and licenses file keys.txt are coped from the Optional SD card to the System SD card. This process does not restore embedded voicmail prompts. This process takes approximately 5 minutes.

Being able to restore just the software files allows software files to be copied from an Optional SD card without affecting the existing configuration of that system.

Warning:

This procedure will cause the B5800 Branch Gateway system to be restarted, disconnecting any current calls and services in progress.

Restoring a configuration file from the Optional SD card using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File > Upgrade Configuration**.
   The configuration file config.cfg and licenses file keys.txt in the primary folder on the Optional SD card are copied to the primary folder on the System SD card. This

takes a few seconds. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring a configuration file from the Optional SD card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **Upgrade Config**.
   The configuration file config.cfg and licenses file keys.txt in the primary folder on the Optional SD card are copied to the primary folder on the System SD card. This takes a few seconds. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring software files from the Optional SD card using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File > Upgrade Binaries**.
   All files in the primary folder on the Optional SC card except the configuration file config.cfg and licenses file keys.txt are copied to the primary folder on the System SD card. This takes approximately 5 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring software files from the Optional SD card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **Upgrade Binaries**.
   All files in the primary folder on the Optional SC card except the configuration file config.cfg and licenses file keys.txt are copied to the primary folder on the System SD card. This takes approximately 5 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

System upgrade using the System SD card

In addition to using the upgrade wizard (see Using the upgrade wizard on page 230), control units can be upgraded by loading the required firmware files onto the System SD card and rebooting the system. There are several ways to load the required firmware onto the System SD card as described in the table below.

Note:

- Check the latest B5800 Branch Gateway Technical Bulletin for the B5800 Branch Gateway software release before proceeding any further. It may contain information relating to changes that occurred after this document was completed. Bulletins are available from http://support.avaya.com
- Some upgrades may require entry of upgrade licenses.

Warning:

This procedure will cause the system to be restarted, disconnecting any current calls and services in progress.

Method	Description	Location	Software Files	Embedded Voicemail Prompts
Using Manager on page 268	Using Manager, the contents of the card are compared to the files that Manager has available and are upgraded if necessary.	**Local or Remote**	✓	✓
System SD Card Upgrade on page 269	In this method, the System SD card is shut down and removed from the control unit. The card's contents are upgraded using Manager.	**Local**	✓	✓
Upgrade from Optional SD Card on page 269	This method uses an SD card loaded with the required version of B5800 Branch Gateway software. The card is inserted into the control unit and then Manager, System Status or a system phone is used to transfer the software to the System SD card.	**Local**	✓	–

Upgrading remotely using Manager

About this task

This procedure copies all system files not present or of a different version compared to those already present on the System SD card.

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Backup System Files**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.
5. Select **File** > **Upload System Files**.
   Manager uploads the system files to the primary folder on the System SD card. This includes B5800 Branch Gateway software files and embedded voicemail prompt

files. Depending on the files that need to be updated, this can take up to40 minutes.

Upgrading the SD card locally

About this task

You can upgrade the SD card locally if you have physical access to the control unit. This method should be used with a timed reboot, allowing the card upgrade to be done during normal operation hours followed by a reboot outside of normal operation hours. See Rebooting the system on page 221 for more information.

If the card is being used for embedded voicemail, that service is not available while the card is shutdown. Licensed features however will continue running for up to 2 hours while the card is shutdown.

Procedure

1. Shutdown the System SD card and remove it from the control unit. See Memory card removal on page 270 for more information.
2. Create the SD card. See About creating an B5800 Branch Gateway SD card on page 257.
   This procedure overwrites the software files on the card with the files available in Manager. It will not affect any other files, for example the configuration file. This process takes approximately 15 minutes.
3. Reinsert the card into the System SD card slot on the control unit.
4. Using Manager, select **File** > **Advanced** > **Reboot**.
5. In the Select IP Office window, select the appropriate system and click **OK**.
6. Select the type of reboot you want to perform and click **OK**.
   When the system reboots, the software files are loaded in the primary folder of the System SD card.

Upgrading using an Optional SD card

About this task

This method allows an Optional SD card to be used as the source from which the System SD card is upgraded. It only upgrades the software files, it does not update embedded voicemail prompts.

Procedure

1. Insert the SD card into a card reader on the Manager PC.

   Note:
   Do not remove the SD card. Removing the SD card will interrupt the upgrade.
2. Using Manager, select **File** > **Advanced** > **Recreate IP Office SD Card**.
3. Select one of the following:
   - **IP Office A-Law**
   - **IP Office U-Law**

   This selection determines how the system operates when defaulted with the SD card installed in the System SD card slot.
4. Browse to the card location and click **OK**.
   Manager starts creating folders on the SD card and copying the required files into those folders. This process takes approximately 15 minutes. Do not remove the SD card until the Manager status bar at the bottom shows a **Ready** message.
5. Insert the card into the Optional SD card slot on the control unit.
6. Use one of the following procedures to copy the software from the Optional SD card to the System SD card:
   - See Restoring software files from the Optional SD card using Manager on page 266.
   - See Restoring software files from the Optional SD card using a system phone on page 267.

Memory card removal

Warning:
Memory cards should always be shut down before being removed when the system is running. Though the card slot LEDs indicate when data is being written to a card, lack of flashing LEDs is not a sufficient safeguard. Shutting down the card will disable embedded voicemail if being used. If the System SD card is removed, features licensed by the card's Feature Key serial number will continue operating for up to 2 hours.

Card services can be restarted by either reinserting the card or using a Start Up command.

Shutting down a memory card using Manager

Procedure

1. Start Manager.
2. Select **File** > **Advanced** > **Memory Card Commands** > **Shutdown**.
3. In the Select IP Office window, select the system containing the memory card.
4. Click **OK**.
5. At the back of the control unit, confirm that the appropriate memory card LED is off.
6. Remove the card.

Shutting down a memory card using a system phone

About this task

To shut down a memory card using a system phone, you must be administered as a System Phone user. You can shut down a memory card using a 1400, 1600, or 9600 series phone (excluding XX01, XX02, and XX03 models). Your Login Code is used to restrict access to some system administration functions on the phone.

Procedure

1. Select **Features > Phone User > System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. Select **Memory Card**.
4. Select **System** for the System SD card or **Option** for the Optional SD card.
5. Select **Shutdown**.
6. At the back of the control unit, confirm that the appropriate memory card LED is off.
7. Remove the card.

Shutting down a memory card using System Status

Procedure

1. Start System Status and access the status output.
2. In the navigation panel select **System**.
3. Select **Memory Cards**.
4. Select either **System Card** or **Optional Card**.
5. At the bottom of the screen select **Shutdown**.
6. At the back of the control unit, confirm that the appropriate memory card LED is off.
7. Remove the card.

Card startup

Reinserting a memory card into a system that is already switched on will automatically restart card operation. However, if the card has been shutdown but not removed, it can be restarted using Manager without requiring a reboot.

Starting up a card using Manager

Procedure

1. Start Manager.
2. Select **File > Advanced > Memory Card Commands > Startup**.
3. From the Select IP Office window, select the system containing the memory card.
4. Click **OK**.

Starting up a card using the System Status application

Procedure

1. Start the System Status application and access the B5800 Branch Gateway status output.
2. In the navigation panel select **System**.
3. Select **Memory Cards**.
4. Select either **System Card** or **Optional Card**.
5. At the bottom of the window, select **Start Up**.

Starting up a card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Choose one of the following:
   - Select **System** for the System SD card
   - Select **Option** for the Optional SD card.
5. Select **Startup**.

Chapter 15: Safety and regulatory information

Safety statements

The B5800 Branch Gateway modules are intended to be installed by Service Personnel and it is the responsibility of the Service Personnel to ensure that all subsidiary interconnected equipment is wired correctly and also meet the safety requirements of IEC60950 or UL60950 where applicable.

- CE
  The CE mark affixed to this equipment means that the module complies with the 1999/5/EC (R&TTE), 89/336/EEC (EMC) and 72/23EEC (LVD) Directives.
- The Declarations of Conformity (DoC) for the B5800 Branch Gateway products are available on the B5800 Branch Gateway Application DVD.
- **Warning:**
  This warning symbol is found on the base of B5800 Branch Gateway modules.
- Refer to Trunk Interface Modules on page 277 for information concerning which trunk interface module variants are fitted in which country.

In Finland, Norway and Sweden a protective earthing conductor must be attached to the protective earth point on the rear of the servers. See Grounding on page 65 for more information. In addition, the server must be located in a restricted access location where equipotential bonding has been applied, for example, in a telecommunication center.

Important safety instructions when using your telephone equipment

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual.

Lithium batteries

A lithium battery is fitted to the real time clock on the control unit motherboard.

Warning:

The Lithium battery must only be replaced by Avaya personnel or authorized representatives. There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Lightening protection/hazard symbols

Lightning protectors — The buildings lightning protectors must be verified as follow:

1. Check the lightning protectors at the trunk cable entry point to the building housing the B5800 Branch Gateway system , paying special attention to the lightning protection grounding. Report any problems, in writing, to the telephone company.
2. Equipment that is designed to be connected using internal wiring is typically not lightning protected. Hence, B5800 Branch Gateway extension cabling must not leave the building. For installations where telephones and/or other standard (tip/ring) devices are installed in another building then lightning protection is required, see Out of Building Telephone Installations on page 66.

Hazard Symbol — The shock hazard symbol is intended to alert personnel to electrical hazard or equipment damage. The following precautions must also be observed when installing telephone equipment:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Always use caution when working with telephone lines.

Trunk interface modules

To ensure the validation of the approvals, only the following types of trunk interface cards must be fitted in the B5800 Branch Gateway control unit.

USA/Canada							
Product	**Quad BRI**	**PRI E1**		**PRI T1**		**ATM4**	**WAN**
		Single	**Dual**	**Single**	**Dual**		
Control unit	✗	✗	✗	✓	✓	✓	✗

Rest of World							
Product	**Quad BRI**	**PRI E1/E1R2**		**PRI T1**		**ATM4**	**WAN**
		Single	**Dual**	**Single**	**Dual**		
Control unit	✓	✓	✓	✗	✗	✓	✗

Note:
E1R2 trunks are only supported in CALA and Korea.

Port safety classification

The B5800 Branch Gateway systems have the following ports which are classified as follows:

Port Name	Port Description	Port Classification
PRI port	PRI ISDN connection (NET)	TNV (Operating within the limits of SELV)
BRI ports	BRI ISDN connection (NET)	TNV (Operating within the limits of SELV)
Analog ports	Two wire analog trunk	TNV3
Power fail ports	Two wire analog trunk	TNV3
DTE port	Async Data connection.	SELV
Analog telephone ports	Telephone Extension ports	TNV2
Digital telephone ports	Telephone Extension ports	SELV
WAN port	WAN connection (NET).	SELV
LAN ports	10/100 BaseT attachment to LAN.	SELV

Port Name	Port Description	Port Classification
Expansion ports	Expansion Module connector.	SELV
Audio port	Connector for Music on Hold.	SELV
External control port	Connector for Controlling Ancillary circuits.	SELV
DC input port	Connector for DC input power.	SELV

Interconnection circuits shall be selected to provide continued conformance with the requirements of EN 609050:1992/A3:1995 clause 2.3 for SELV circuits and with the requirements of clause 6 for TNV circuits, after connections between equipment.

EMC cautions

889/336/ EEC (EMC Directive) CISPR 22:1993 including A1 + A2, AS/NZ 3548:1995 (ROW)

Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

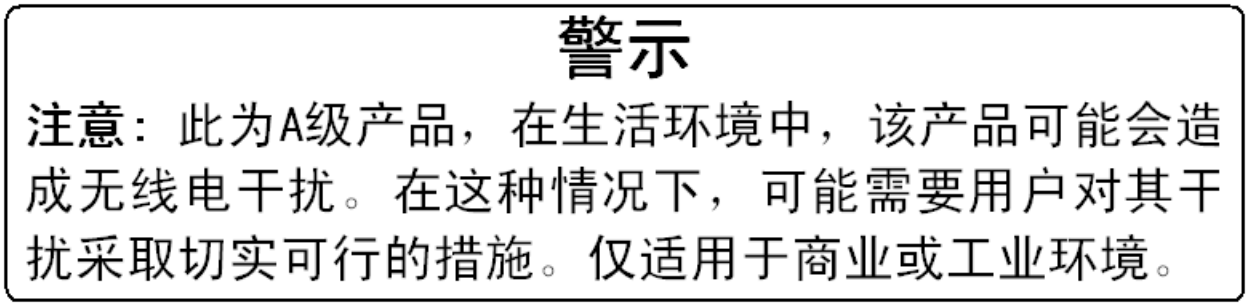
Federal communications commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

Canadian department of communications (DOC)

"NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment."

EMC caution for china



Regulatory Instructions for Use

Australia

BRI interface

During the configuration, ensure "000" emergency number is not barred, by performing the following:

- Short Code: 000
- Telephone No: 000;
- Function: DialEmergency

Connections to TS013, the following bearer capabilities shall not be used: 7kHz Audio, Video, Restricted Digital Information.

If unknown type of number is used in calling party number, the network will use the default CLI.

The system must be configured for Point to Multi point connection to comply with Austel requirements for connecting to TS013 circuits.

As the B5800 Branch Gateway does not support emergency dialing after loss of power, the following warning notice should be recognized:

Warning:
This equipment will be inoperable when main power fails.

PRI interface

During the configuration, ensure "000" emergency number is not barred, by performing the following:

- Short Code: 000
- Telephone No: 000;
- Function: DialEmergency

Canada

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met.

It does not imply that Industry Canada approved the equipment.

"NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 1. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five."

China

AVAYA

700433220
February 2007

所有在中华人民共和国境内进口或销售的电子信息产品必须附上本文件

Include this document with all Electronic Information Products imported or sold in the People's Republic of China

部件名称 (Part Name)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	○	○	○
电路模块 (Circuit Modules)	×	○	○	○	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	×	○	○	○	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
电路开关/断路器 (Circuit Switch/Breakers)	○	○	○	○	○	○
电源组件 (Power Assemblies)	×	○	○	○	○	○
显示器 (LCD, Monitor)	○	○	○	○	○	○
玻璃 (Glass)	○	○	○	○	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363 2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363 2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363 2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363 2006 standard.

本表显示，所附的亚美亚电子信息产品中，从生产日期起，可能包含这些物质。注意：所附产品可能包含或不含以上所列的某些组件。
This table shows where these substances may be found in Avaya's electronic information products, as of the date of manufacture of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非有另外特别的标注,此标志将作为所附产品及零部件的环保使用期标志. 某些产品会有一个不同的环保使用期(例如,电话机)并贴在其产品上.此环保使用期限只适用于产品在产品手册中所规定的条件下使用

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain products have a different EFUP (for example, telephones) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

European Union

- 999 and 112 calls must not be barred. Doing so will invalidate the approval.
- All connections at the MDF shall be identifiable by suitable labeling.
- The CE mark displayed on B5800 Branch Gateway equipment indicates the systems compliance with the EMC, LVD, and R&TTE Directives and common technical regulations for Primary Rate and Basic Rate ISDN.
- All ports for the connection of other non-telecommunications apparatus have a Safety Extra Low Voltage (SELV) safety status.

New Zealand

The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.

FCC notification

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of connection

Connection of this equipment to the telephone network is shown in the following table.

Port	FIC	SOC	USOC Jack	REN
IPO500 PRI 1U, IPO500 PRI2U, IP400 PRI-T1	04DU9.BN, 04DU9.DN, 04DU9.IKN, 04DU9.ISN	6.0Y	RJ48C	NA
IPO500 ATM4U IP400 ATM4U	OL13A, OL13B, OL13C, 02AC2, 02LA2, 02LB2, 02LC2, 02LR2, 02LS2	9.0Y	RJ45S	0.1B
IPO500 ATM16	OL13A, OL13B, OL13C, 02AC2, 02GS2, 02LA2, 02LB2, 02LC2, 02LR2, 02LF2 02GS2, 02LS2	9.0Y	RJ45S	0.1B

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Equipment with Direct Inward Dialing (DID)

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC’s rules.

Proper answer supervision is when:

- This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
    - Answered by the called station
    - Answered by the attendant

- Routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
- Routed to a dial prompt

- This equipment returns answer supervision signals on all DID calls forwarded back to the PSTN. Permissible exceptions are:
  - A call is unanswered.
  - A busy tone is received.
  - A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic dialers

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll restriction and least cost routing equipment

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

FCC part 68 supplier's declarations of conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Compliance with FCC rules

Transmit and receive gain settings for PRI/T1 and analog ports

The Gain settings are password controlled for use by qualified installation personnel only and must not be made available to the end user. The default gain settings of 0dB ensures compliance with FCC part 68 section 68.308(b)(5) and TIA/EIA-IS-968 Section 4.5.2.5. "Through transmission amplification from ports for the connection of separately registered equipment or from other network connection ports". Gain setting adjustment by unqualified

personnel may result in violation of the FCC rules. Qualified personnel may adjust gain settings above these levels only where:

- Measurement is made to ensure that the power levels sent to line at each network interface connected does not exceed the maximum levels specified in FCC part 68 section 68.308(b) and TIA/EIA-IS-968 Section 4.5 for that specific interface type.
- Where gain adjustment away from the default values are made, precautions should be taken to ensure that the connection of terminal equipment is controlled by qualified installation personnel.
- To conform with the Receive Objective Loudness Rating at distances greater than 2.7km from the central office, on analog trunks a receive gain of 1.5dB must be set.

Appendix A: Centralized deployment example call flows

This appendix provides examples of call flows for a system that is configured in a centralized deployment.

Routing concepts

In the example network deployment provided in this appendix, all calls that are routed within Avaya Aura® Session Manager are converted to E.164. The primary function for this is to support Tail-End-Hop-Off (TEHO).

E.164

E.164 is a numbering format that is recommendation by the International Telecommunications Union - Telecommunications (ITU-T). E.164 can have a maximum of 15 digits and is preceded by a +.

- Maximum of 15 digits (not including the preceding +).
- First part is a 1 to 3-digit country code.
- Second part is a national destination code.
- Last part is the subscriber number.
- Second and last parts are collectively known as the national number.

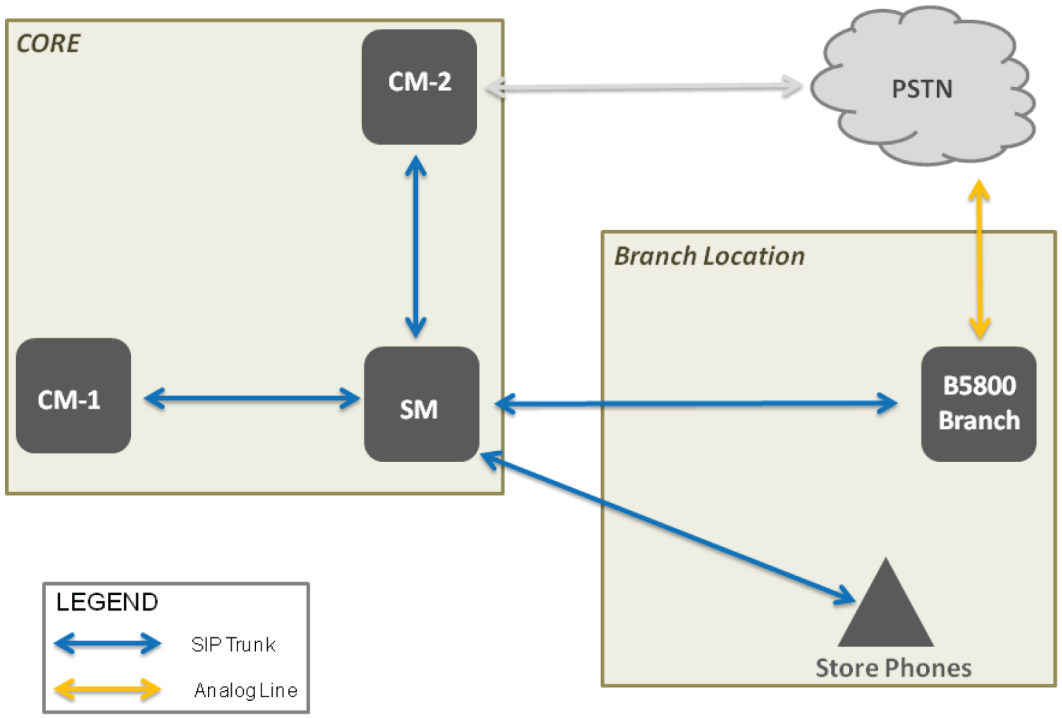
Tail-End-Hop-Off (TEHO)

TEHO is the process of routing a call through a private network to the closest node of the destination call, and then routing over the public network as a local call.

Call flows

The B5800 Branch Gateway centralized solution revolves around SIP endpoints at a branch location that registers to a Session Manager. Local trunking is provided through the B5800 Branch Gateway at the branch location. When connectivity to the Session Manager is lost, the SIP endpoints failover and register to the B5800 Branch Gateway for connectivity.

Solution overview



The Solution overview illustrates the store network.

- **CM-1** represents a Communication Manager used for features for the store phones.
- **CM-2** represents the primary Communication Manager used for corporate endpoints and PSTN trunking.
- **SM** represents all Session Managers.

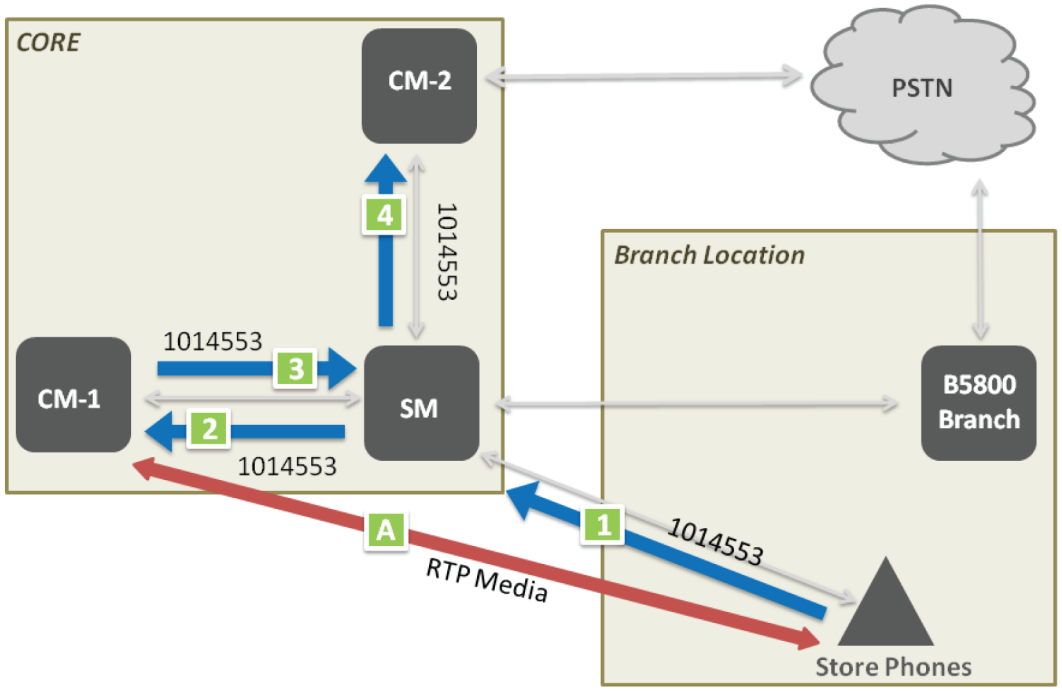
There must be at least:

- 1 or more Communication Managers
- 1 or more Session Managers
- 1 or more B5800 Branch Gateways
- SIP endpoints at each branch location

Sunny day

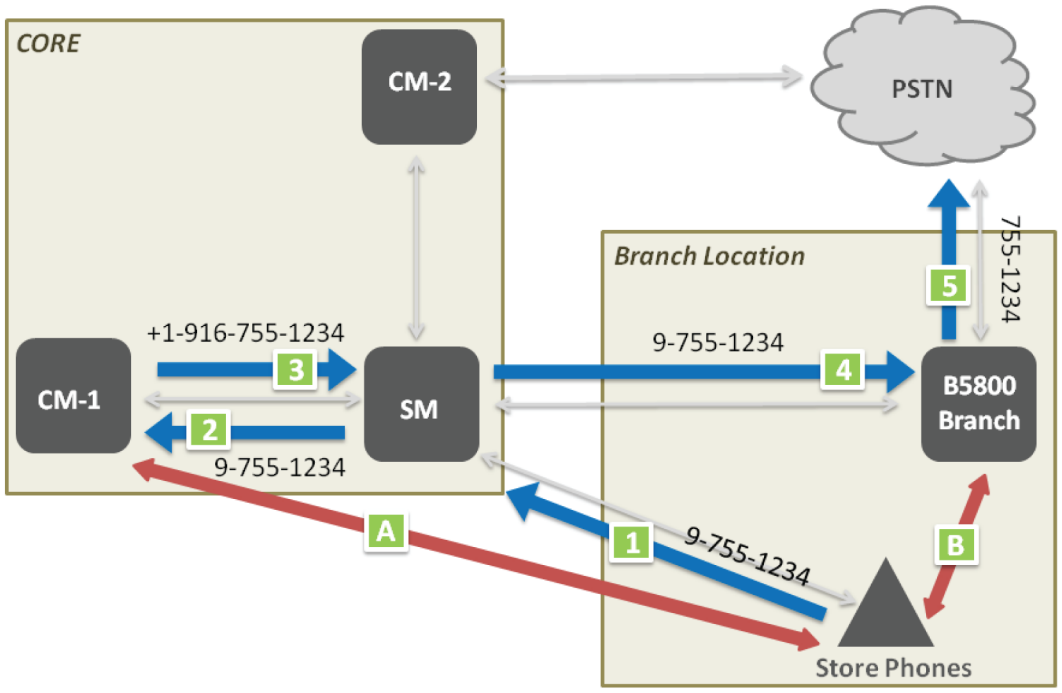
The first set of call flows are for sunny day. This is when all SIP endpoints have full connectivity across the WAN back to the core and are registered to the Session Manager. All SIP trunks are in service.

Internal call



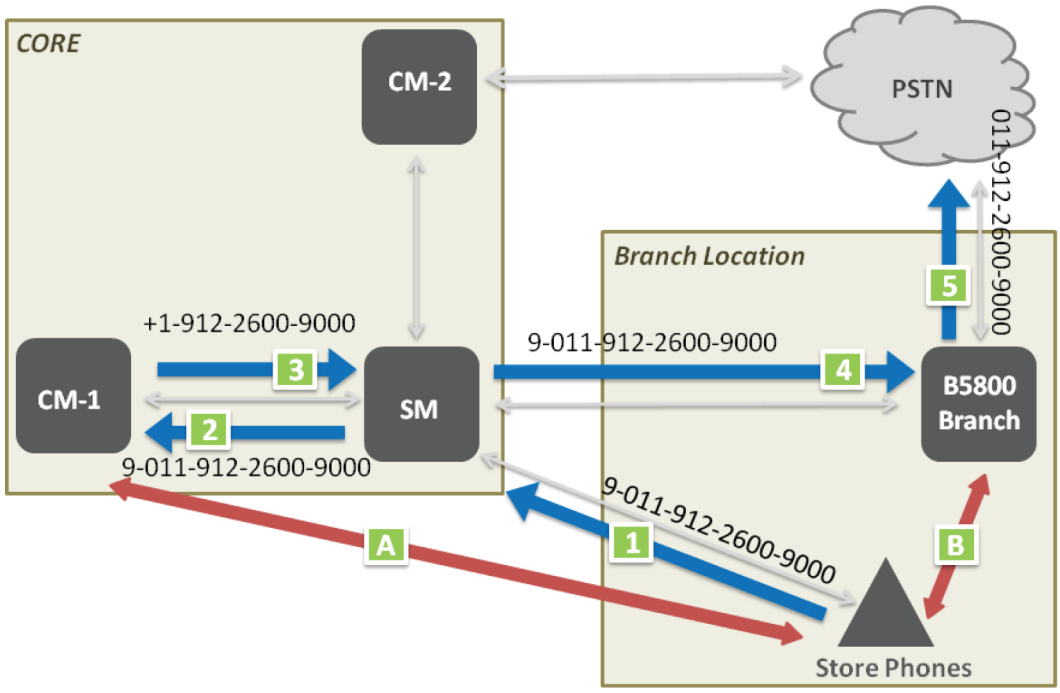
1	**Store Phone** originates call to a corporate station 1014553.
2	**SM** sends 1014553 to CM for origination processing.
3	**CM** identifies call as internal and routes 1014553 back to **SM**.
4	**SM** sends call to destination phone 1014553 at destination **CM**. This call flow is similar for calls within the same branch or calls to other branches with the exception that the calls terminate at the destined branch.
A	RTP Media stream is initially between the **Store Phone** and a **CM-1** media gateway. This will shuffle between the **Store Phone** and **CM-2** or another endpoint once established.

Local PSTN dialing



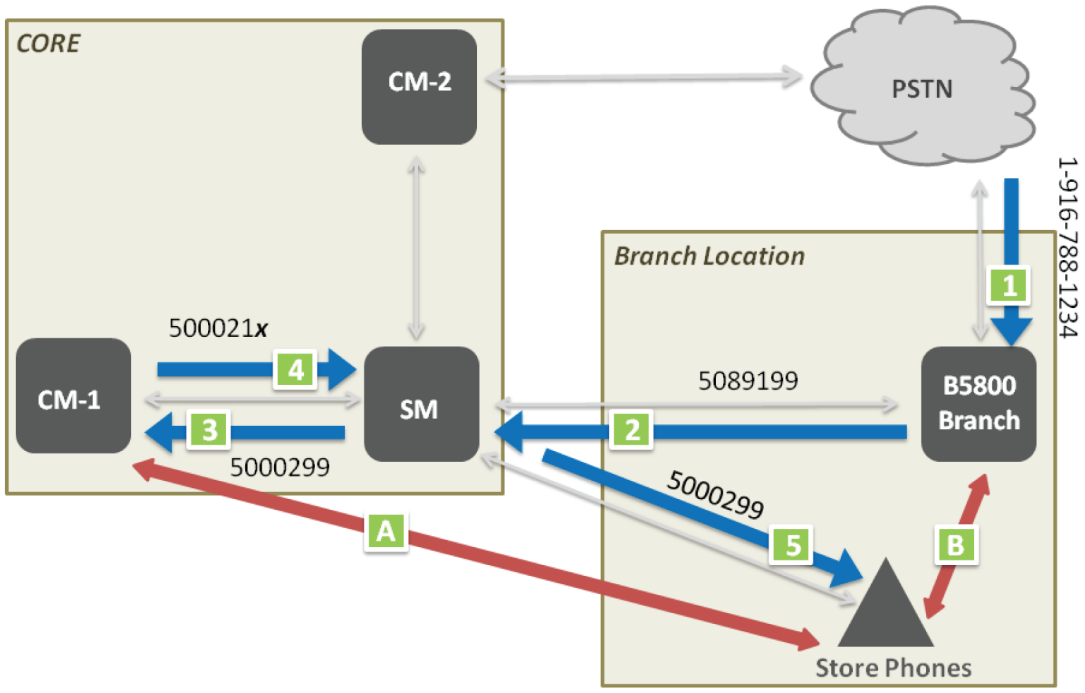
1	**Store Phone** calls local extension 9-755-1234.
2	**SM** sends 9-755-1234 to **CM** for origination call processing.
3	**CM** translates the call into E.164 based on callers' location and sends +1-916-755-1234 to **SM**.
4	**SM** adapts the call for the local carrier and sends 9-755-1234 back to original branch. Session Manager could use the E.164 formatted number to do TEHO routing at this step.
5	**B5800 Branch** sends 755-1234 to the **PSTN**.
A	RTP Media stream is initially between the **Store Phone** and **CM-1** media gateway.
B	Once the call is established, the RTP Media stream will shuffle between the **Store Phone** and the **B5800 Branch**.

Long distance and international



1	**Store Phone** calls long distance number 9-011-912-2600-9000.
2	**SM** sends 9-011-912-2600-9000 to **CM** for origination call processing.
3	**CM** translates the call into E.164 based on callers' location and sends +1-912-2600-9000 to **SM**.
4	**SM** adapts the call for the local carrier and sends 9-011-912-2600-9000 back to original branch. Session Manager could use the E.164 formatted number to do TEHO routing at this step.
5	**B5800 Branch** sends 011-912-2600-9000 to the CO.
A	RTP Media stream is initially between the **Store Phone** and **CM-1** media gateway.
B	Once the call is established, the RTP Media stream will shuffle between the **Store Phone** and the **B5800 Branch**.

Incoming call



1	Customer dials store extension 1-916-788-1234 (the branch phone number).
2	**B5800 Branch** sends call to VDN 5000299 on **CM** via **SM**. Routing to a VDN allows reporting of branch calls.
3	**SM** matches call with a Route Pattern and sends to **CM**.
4	**CM** routes call to x-ported station that is bridged to all branch endpoints. (X-ported refers to AWOH (Admin With Out Hardware) stations that are administered as an endpoint without any physical hardware.)
5	**SM** sends call to all endpoints at the branch.
A	RTP Media stream is initially between the **Store Phone** and **CM-1** media gateway.
B	Once the call is established, the RTP Media stream will shuffle between the **Store Phone** and the **B5800 Branch**.

Rainy day

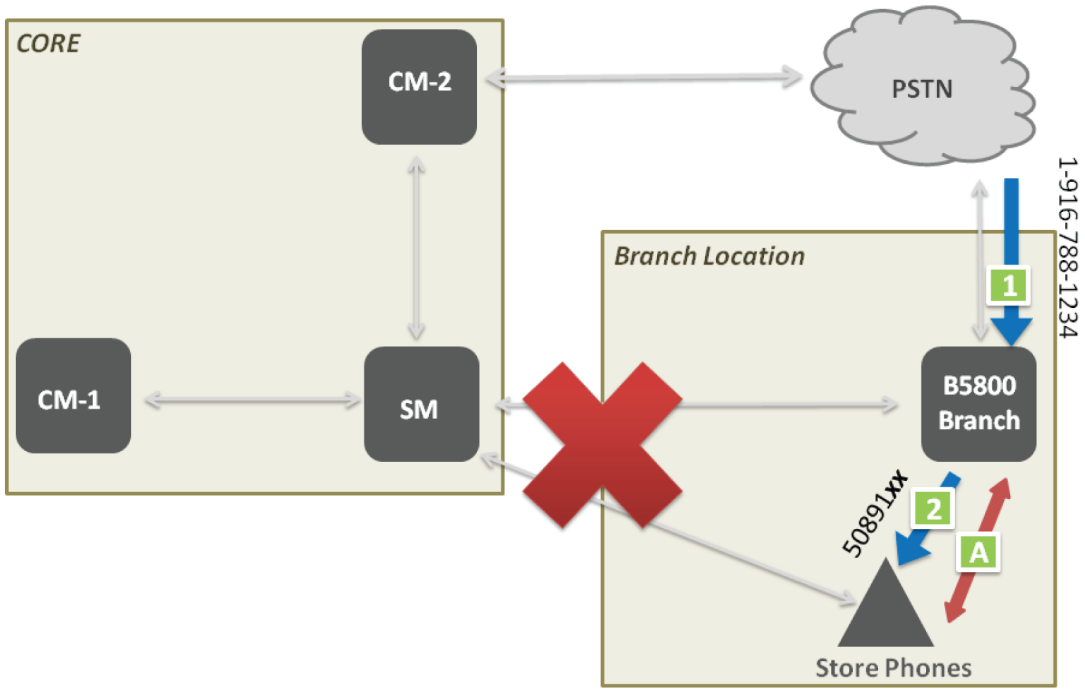
The next set of call flows are for rainy day. In a rainy day scenario, the SIP phones will failover to the B5800 Branch Gateway in standalone mode. The standalone mode operates with a

reduced SIP feature set which does not support all sunny day features. In a rainy day inbound call scenario, the process would be as follows: an inbound call will ring on all phones until that call is answered. Because bridged line appearances are not supported as a rainy day feature, once that call is answered, the call will only appear on the active station, and all other stations will show idle. Note that all idle phones will continue to be available to make or answer incoming calls from the local PSTN or make and receive calls from within the store.

Moving an answered call from one phone to another requires a transfer. Only internal store and PSTN dialing is supported, and any non-PSTN extensions to extension dialing will not be routed. To dial any external number in rainy day, users will need to dial 9 followed by the complete 7 or 10 digit number.

Additionally, due to the dial plan convention adopted, any store to store calling, or calls from corporate locations, are only supported through the PSTN to the main CO lines provisioned. Without any additional programming, all 7 digit dialing from the corporate location or other retail store to a store operating in rainy day will receive a ‘wave-off’ tone. In order to mitigate this behavior the recommendation is to provide each station with a point of coverage that directs the calling party to primary DID for store where the extension resides.

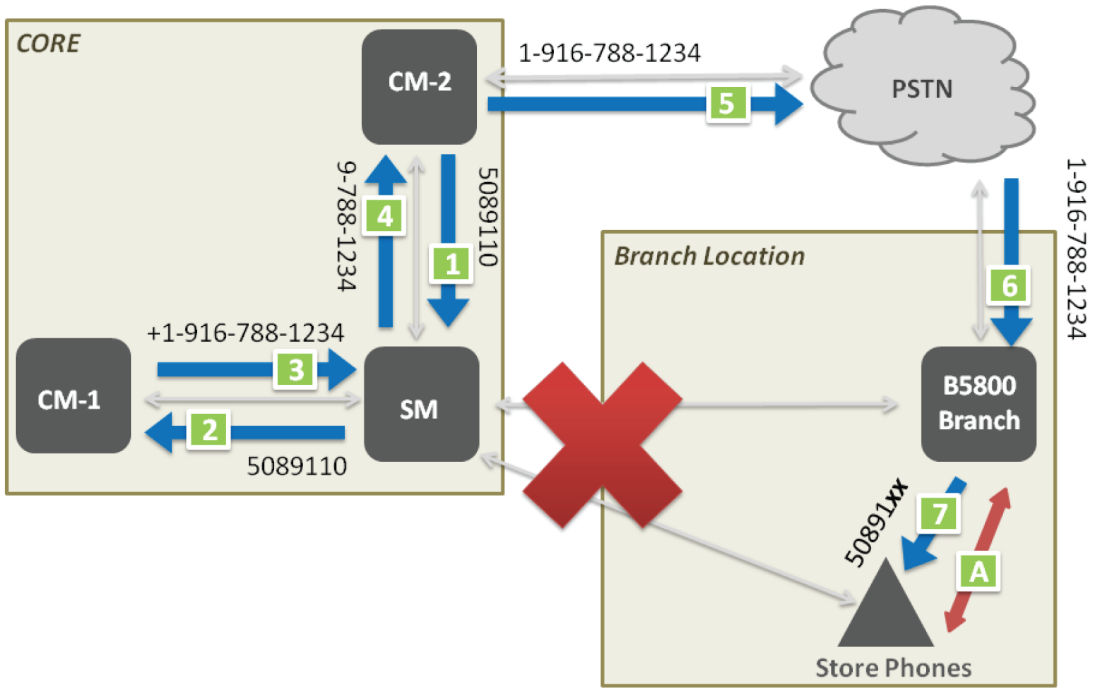
Incoming call — failover, inbound call



1	Customer dials store extension 1-916-788-1234.

2	**B5800 Branch** sends the call directly to all registered SIP stations in the hunt group.
A	RTP Media is established between the **Store Phone** and the **B5800 Branch**.

Incoming call from corporate – coverage



1	Corporate user dials branch extension 5089110
2	**SM** routes call to **CM-1** for origination call processing.
3	**CM-1** and **SM** identify that branch is unreachable. **CM-1** routes call to coverage path for 5089110. In this case the remote coverage path would be the E.164 formatted DID of the store +1-916-788-1234.
4	**SM** sends the call back to the originating **CM-2**. **SM** adapts the call to a format that is routable at the local **CM-2**.
5	**CM-2** sends the call to the PSTN.
6	Call is routed through the PSTN to the store through the local CO.
7	**B5800 Branch** routes the call to a hunt group. This hunt group in turn sends the call to all registered SIP stations at the branch.

A	RTP Media stream is established between the **Store Phone** and the **B5800 Branch**.

Appendix B: Avaya port matrix for B5800 Branch Gateway and SIP phones

This appendix provides example ingress and egress ports for B5800 Branch Gateway and SIP phones.

What are ports and how are they used?

TCP and UDP use ports (defined at http://www.iana.org/assignments/port-numbers) to route traffic arriving at a particular IP device to the correct upper layer application. These ports are logical descriptors (numbers) that help devices multiplex and de-multiplex information streams. Consider your desktop PC. Multiple applications may be simultaneously receiving information. In this example, email may use destination TCP port 25, a browser may use destination TCP port 80 and a telnet session may use destination TCP port 23. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streams inside the PC. Furthermore, each of the mini-streams is directed to the correct high-level application because the port numbers identify which application each data mini-stream belongs. Every IP device has incoming (Ingress) and outgoing (Egress) data streams.

Ports are used in TCP and UDP to name the ends of logical connections which carry data flows. TCP and UDP streams have an IP address and port number for both source and destination IP devices. The pairing of an IP address and a port number is called a socket (discussed later). Therefore, each data stream is uniquely identified with two sockets. Source and destination sockets must be known by the source before a data stream can be sent to the destination. Some destination ports are “open” to receive data streams and are called “listening” ports. Listening ports actively wait for a source (client) to make contact to a destination (server) using a specific port that has a known protocol associate with that port number. HTTPS, as an example, is assigned port number 443. When a destination IP device is contacted by a source device using port 443, the destination uses the HTTPS protocol for that data stream conversation.

Port type ranges

Port numbers are divided into the following three ranges:

- Well known ports are those numbered from 0 through 1023.
- Registered ports are those numbered from 1024 through 49151
- Dynamic ports are those numbered from 49152 through 65535

The well known and registered ports are assigned by IANA (Internet Assigned Numbers Authority) and are found at http://www.iana.org/assignments/port-numbers.

Well known ports

For the purpose of providing services to unknown clients, a service listen port is defined. This port is used by the server process as its listen port. Common services often use listen ports in the well known port range. A well known port is normally active meaning that it is “listening” for any traffic destined for a specific application. For example, well known port 23 on a server is actively waiting for a data source to contact the server IP address using this port number to establish a Telnet session. Well known port 25 is waiting for an email session, etc. These ports are tied to a well understood application and range from 0 to 1023.

In UNIX and Linux operating systems, only root may open or close a well known port. Well known ports are also commonly referred to as privileged ports.

Registered ports

Unlike well known ports, these ports are not restricted to the root user. Less common services register ports in this range. Avaya uses ports in this range for call control. Some, but not all, ports used by Avaya in this range include: 1719/1720 for H.323, 5060/5061 for SIP, 2944 for H.248 and others. The registered port range is 1024 – 49151. Even though a port is registered with an application name, industry often uses these ports for different applications. Conflicts can occur in an enterprise when a port with one meaning is used by two servers with different meanings.

Dynamic ports

Dynamic ports, sometimes called private ports, are available to use for any general purpose. This means there are no meanings associated with these ports (similar to RFC 1918 IP Address Usage). These are the safest ports to use because no application types are linked to these ports. The dynamic port range is 49152 – 65535.

Sockets

A socket is the pairing of an IP address with a port number. An example would be 192.168.5.17:3009, where 3009 is the socket number associated with the IP address. A data flow, or conversation, requires two sockets – one at the source device and one at the destination device. The data flow then has two sockets with a total of four logical elements. Each data flow must be unique. If one of the four elements is unique, the data flow is unique. The following three data flows are uniquely identified by socket number and/or IP address.

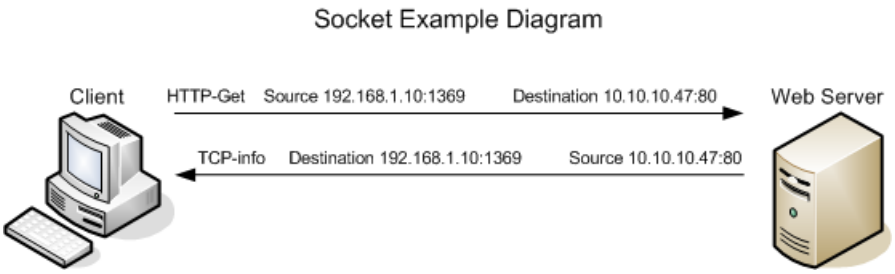
- Date flow 1: 172.16.16.14:1234 — 10.1.2.3:2345
- Date flow 2: 172.16.16.14:1235 — 10.1.2.3:2345
- Date flow 3: 172.16.16.14:1234 — 10.1.2.4:2345

Data flow 1 has two different port numbers and two different IP addresses and is a valid and typical socket pair.

Data flow 2 has the same IP addresses and the same port number on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique.

Therefore, if one IP address octet changes, or one port number changes, the data flow is unique.

Socket example showing ingress and egress data flows from a PC to a web server



Notice the client egress stream includes the client's source IP and socket (1369) and the destination IP and socket (80). The ingress stream has the source and destination information reversed because the ingress is coming from the server.

Firewall types

There are three basic firewall types described below.

Packet filtering

Packet Filtering is the most basic form of the firewalls. Each packet that arrives or leaves the network has its header fields examined against criterion to either drop the packet or let it through. Routers configured with Access Control Lists (ACL) use packet filtering. An example of packet filtering is preventing any source device on the Engineering subnet to telnet into any device in the Accounting subnet.

Application level gateways

Application level gateways (ALG) act as a proxy, preventing a direct connection between the foreign device and the internal destination device. ALGs filter each individual packet rather than blindly copying bytes. ALGs can also send alerts via email, alarms or other methods and keep log files to track significant events.

Hybrid

Hybrid firewalls are dynamic systems, tracking each connection traversing all interfaces of the firewall and making sure they are valid. In addition to looking at headers, the content of the

packet, up through the application layer, is examined. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Stateful inspection firewalls close off ports until the connection to the specific port is requested. This is an enhancement to security against port scanning. Port scanning is the act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Firewall policies

The goals of firewall policies are to monitor, authorize and log data flows and events. They also restrict access using IP addresses, port numbers and application types and sub-types. This appendix focuses on identifying the port numbers used by Avaya products so effective firewall policies can be created without disrupting business communications or opening unnecessary access into the network.

Knowing that the source column in the port usage tables provided below is the socket initiator is key in building some types of firewall policies. Some firewalls can be configured to automatically create a return path through the firewall if the initiating source is allowed through. This option removes the need to enter two firewall rules, one for each stream direction, but can also raise security concerns.

Another feature of some firewalls is to create an umbrella policy that allows access for many independent data flows using a common higher layer attribute. Finally, many firewall policies can be avoided by placing endpoints and the servers that serve those endpoints in the same firewall zone.

TFTP port usage

B5800 Branch Gateway upgrade wizard and VM Pro all use TFTP for commands and data transfer. B5800 Branch Gateway implements a version of the TFTP Transfer Identifier mechanism (TID) defined by RFC 1350.

The general mechanism is each has a TFTP listener on port 69, any received command (READ request) is responded to with a TFTP response (WRITE request) to port 69. Any subsequent data transfer uses the source ports from both request and response.

B5800 Branch Gateway Manager (upgrade wizard)	**B5800 Branch Gateway**
TFTP Read, src port 2421, dst port 69 >	
	< TFTP Write, src port 4153, dst port 69

	< TFTP Data packet (1..n), src port 4153, dst port 2421
TFTP Acks (1..n), src port 2421, dst port 4153	

Ingress ports for B5800 Branch Gateway and SIP phones

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
1	22	TCP/ SSH	No	Open	Admin terminal or SAL Gateway	Yes	System mgmt requiring shell access – Remote maintenance.
2	69	UDP/ TFTP	No	Open	NM/ Manager	Yes	B5800 Branch Gateway status, configuration data, program data. See Port type ranges on page 297 for ranges.
3	80	TCP/ HTTP	No	Open	NM/ Manager	Yes	Web client access, Inter B5800 Directory Exchange (optional).
4	123	UDP/ NTP	No	Open	NTP Server	Yes	NTP (RFC4330) Service.
5	161-C	UDP/ SNMP	Yes	Closed	Admin terminal or NMS	Yes	Read-only access to MIB entries.
6	5060	TCP/SIP	No	Open		Yes	SIP Signaling.
7	49152 – 53247-C	UDP/ RTP-RTCP	Yes	Open	IP Phones, RTCP Collector	Yes	Dynamically allocated ports used during VoIP calls for RTP and RTCP traffic. The port range can be adjusted through the System > Gatekeeper tab.
8	50802	TCP/ Who Is?	Yes	Open	B5800 Manager	Yes	TCP Discovery.

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
9	50805-C	TCP/ HTTP B5800 config access	No	Open	B5800 Manager	Yes	B5800 Configuration Service – Secured. See optional 50804.
10	50808-C	TCP/ HTTP B5800 Sys Status Access	No	Open	B5800 Manager	Yes	B5800 System Status Access.
11	50813-C	TCP/ HTTP B5800 Sec Settings Access	No	Open	B5800 Manager	Yes	B5800 Security Settings Access – Secured. See optional 50812.
OPTIONAL							
I-A	68	UDP/ DHCP-Cli	Yes	Open	DHCP-Srv	Yes	If configured, B5800 obtains its' IP address from a remote server.
I-B	443	TCP/ HTTP	No	Open	Dect R4	Yes	File transfer Web client access.
I-C	1718	TCP/ H323-Disc	No	Open	Branch Trunk	No	Offering H.323 service to IP phones.
I-D	1719	TCP/ RAS	No	Open	IP Phones	No	Offering H.323 service to IP phones.
I-E	5061	TCP/ TLS	Yes	Closed	Session Manager	Yes	Encrypted SIP signaling.
I-F	50796	UDP/ Partner App	Yes	Closed	Phone Mgr	Yes	Control of telephones from Phone Manager, Soft Console.
I-G	50804-C	TCP/ HTTPS B5800 Config Access	No	Open	B5800 Manager	Yes	B5800 Configuration Service – Unsecured. See 50805.
I-H	50812-C	TCP/ HTTP	No	Open	B5800 Manager	Yes	B5800 Security Settings Access –

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
		B5800 Sec Settings Access					Unsecured. See 50813.

For a description of the column headings, see Table column heading definitions on page 305.

Egress ports for B5800 Branch Gateway and SIP phones

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
1	53	UDP/ DNS	No	Open	DNS Server	Yes	DNS service to resolve URL and IP addresses.
2	69	UDP/ TFTP	No	Open	Manager	Yes	B5800 Branch Gateway status, configuration data, program data. See Port type ranges on page 297 for ranges.
3	123	UDP/ NTP	No	Open	NTP Server	Yes	NTP (RFC4330) Service.
4	162	UDP/ SNMP	Yes	Closed	Trap Receiver	Yes	Trap generation from B5800 Branch Gateway.
5	389	TCP/ LDAP	Yes	Closed	LDAP Server	Yes	Import of directory information from LDAP database.
6	500	UDP/ IKE	Yes	Closed	Security device	Yes	Form IPSec associations with remote security devices. Requires license.

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
7	514	UDP/ Syslog-Cli	Yes	Open	Syslog Server	No, but could be	Log files transmitted from IP phones to server.
8	5005-C	RTCP	Yes	Open	NMS	Yes	RTCP collector (HP-Openview, AIM, etc.).
9	5060	TCP/SIP	No	Open		Yes	SIP signaling.
10	49152 – 53247-C	UDP/ RTP-RTCP	Yes	Open	IP Phones, RTCP Collector	Yes	Dynamically allocated ports used during VoIP calls for RTP and RTCP traffic. The port range can be adjusted through the System > Gatekeeper tab.
11	50794	UDP/ TCP/ Monitor	No	Open	Manager	Yes	Event, trace and diagnostic outputs.
OPTIONAL							
E-1	25	TCP/ SMTP	Yes	Open	Mail Server	Depends	
E-2	37	UDP/ Time	Yes	Closed	Manager	Yes	TIME (RFC868) Service supported by Manager and VMPro. Requested by B5800 Branch Gateway. This service is an option to NTP – port 123.
E-3	67	UDP/ DHCP-Srv	Yes		IP Clients	No	DHCP service to IP phones, PCs and other clients.
E-4	1720	TCP/ H323	Yes	Open	H323 Server	No	Offering H.323 service to IP phones.
E-5	5061	TCP/ TLS	Yes	Closed	Session Manager	Yes	Encrypted SIP signaling.

For a description of the column headings, see Table column heading definitions on page 305.

Table column heading definitions

Column heading	Description
Dest Port	Destination port — this is the layer-4 port number to which the connection request is sent. Valid values include 0 – 65535.
Network/App Protocol	Network/application protocol — this is the name associated with the layer-4 protocol and layers-5-7 application.
En or Dis?	Optionally Enabled or Disabled? — this field indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid values are Yes or No. • No means the default port state cannot be changed (that is, enable or disabled). • Yes means the default port state can be changed (that is, enabled or disabled).
Default Port State	Default Port State — a port is either open, closed, filtered or N/A. • Open ports will respond to queries. • Closed ports may or may not respond to queries and are only listed when they can be optionally enabled. • Filtered ports can be open or closed. Filtered UDP ports will not respond to queries. Filtered TCP will respond to queries, but will not allow connectivity. • N/A is used for the egress default port state since these are not listening ports on the product.
Remote Device	Remote Device — this is the remote device that is initiating a connection request (Ingress Connections) or receiving a connection request (Egress Connections).
Ext to Branch?	External to Branch? — this indicates whether traffic to this layer-4 port is needed between the branch and other sites, requiring this port to be open on firewalls, if any, between the branch and the rest of the customer's network. Note that this depends on the customer's deployment. Valid Values are: • Yes (meaning typically needed) • No (meaning not expected to be needed) • Depends (on customer deployment)

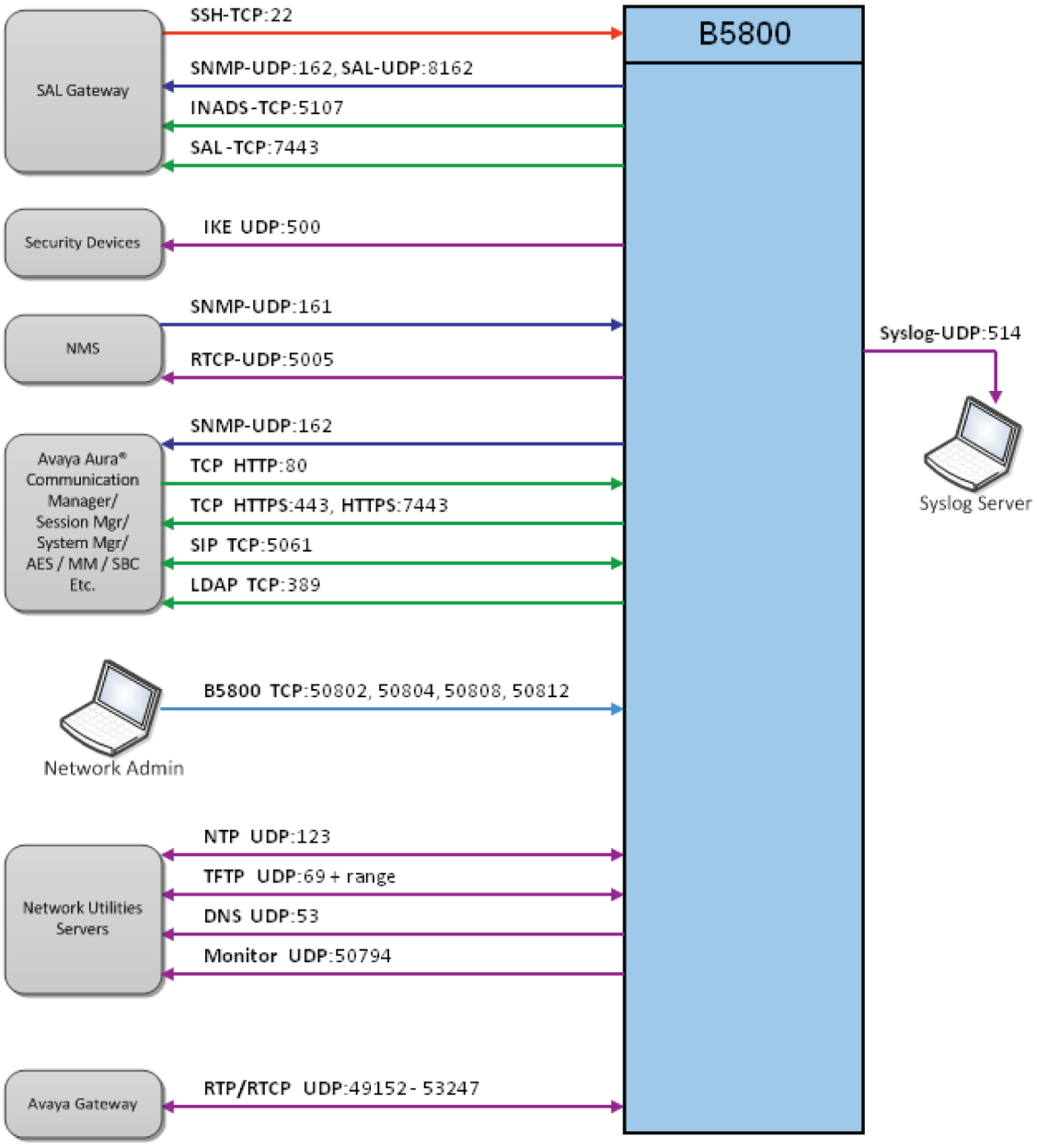
Notes:

- Email will not flow through the B5800 Branch Gateway in this example. See optional section for port 25.
- An off-site DHCP server is used to supply IP addresses to phones and PCs. Otherwise, add ports 67 and 68 in optional sections.
- The B5800 Branch Gateway IP address will be manually configured and not need a DHCP server.
- TFTP service begins using port 69, but eventually uses the source ports from both sides.
- Ports 80804 and 80812 are unsecure communications but have optional port 80805 and 80813 as secure options.
- For B5800 Branch Gateway R6.1, the TFTP/UDP port selection is an issue; B5800 Branch Gateway Manager, ENM, and SysMonitor do not constrain the selection of TFTP/UDP source port.

  B5800 Branch Gateway R6.2 improves this TFTP port issue greatly in a number of ways:

  - System Manager does not use TFTP.
  - SysMonitor and B5800 Branch Gateway Manager have configurable TFTP/UDP port ranges.
- HTTPS is used for DECT R4 administration.

Port usage diagram



In this diagram, direction of the arrow depicts call initiation. Data traffic will typically be 2-way.

Appendix C: B5800 Branch Gateway call flows

Calls from local extensions (i.e. deployed in Distributed branch model)

1. Local phone to local phone

   Local phone A → B5800 Branch Gateway → local phone B

2. Local phone to PSTN (using local trunking)

   Local phone → B5800 Branch Gateway → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP Trunk) → PSTN

3. Local phone to PSTN (using centralized trunking)

   Local phone → B5800 Branch Gateway → Session Manager→ central gateway/SBC → PSTN

4. Local phone to headquarters or other enterprise site

   Local phone → B5800 Branch Gateway → Session Manager → target phone's controller → target phone

Calls to local extensions (i.e. deployed in Distributed branch model)

1. From PSTN to local extension via IP Office auto-attendant (branch auto-attendant LDN is associated with local B5800 Branch Gateway trunk)

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → B5800 Branch Gateway auto-attendant → caller enters extension number → local phone

2. From PSTN direct to Local phone's DID (LDN is associated with local B5800 Branch Gateway trunk)

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → B5800 Branch Gateway → local phone

3. From headquarters (or other enterprise site) to local phone's enterprise number

   Originating phone → originating phone's controller → Session Manager → B5800 Branch Gateway → local phone

4. From headquarters (or other enterprise site) to local extension via IP Office auto-attendant

   Originating phone → originating phone's controller → Session Manager → B5800 Branch Gateway → B5800 Branch Gateway auto-attendant → caller enters extension number → local phone

Calls from Centralized phones in normal mode (aka sunny day)

1. Centralized phone A to centralized phone B in the same branch

Centralized phone A → Avaya Aura core servers (including Session Manager and CM-FS) → centralized phone B

Note:

The B5800 Branch Gateway is not involved in handling the call in this scenario.

The call flow descriptions in this document are intended to clarify the call flow between the branch and the core with focus on B5800 Branch Gateway involvement. For brevity, they do not elaborate on the processing of the call within the core, among the different elements of the Avaya Aura® server infrastructure at the enterprise core. For example, a more complete depiction of the call flow for this scenario would be:

Centralized phone A → Session Manager → origination-side processing by the CM-FS responsible for user of phone A → Session Manager → termination-side processing by the CM-FS responsible for user of phone B → Session Manager → centralized phone B

This depiction of the call flow includes the core Avaya Aura® Communication Manager acting as the feature server for the centralized user. The Communication Manager Feature Servers (CM-FSs) for user A and user B may be the same CM server or two different CM servers, depending on the provisioning of the users on the core CM servers. Furthermore, additional application servers may be sequenced in the call flow by Session Manager if additional core sequenced applications are deployed by the enterprise. See the Avaya Aura® Session Manager documentation for more information regarding the operation of the CM-FS with Session Manager, and regarding Session Manager application sequencing.

2. Centralized phone to local phone (dialing local phone's enterprise number)

   Centralized phone → Session Manager → CM-FS → Session Manager → B5800 Branch Gateway → local phone

3. Centralized phone to PSTN (using local trunking)

   Centralized phone → Session Manager → CM-FS → Session Manager → B5800 Branch Gateway → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → PSTN

4. Centralized phone to PSTN (using centralized trunking)

   Centralized phone → Session Manager → CM-FS → Session Manager → central gateway/SBC → PSTN

   Note:

   The B5800 Branch Gateway is not involved in handling the call in this scenario.

5. Centralized phone to headquarters or other enterprise site

   Centralized phone → Session Manager → CM-FS → Session Manager → target phone's controller (if target phone does not register directly to SM) → target phone

   Note:

   The B5800 Branch Gateway is not involved in handling the call in this scenario.

Calls to Centralized phones in normal mode (aka sunny day)

1. From PSTN to centralized phone's DID (LDN is associated with local B5800 Branch Gateway trunk)

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → B5800 Branch Gateway → Session Manager → CM-FS → Session Manager → centralized phone

2. From PSTN to centralized phone via B5800 Branch Gateway auto-attendant (branch auto-attendant LDN is associated with local B5800 Branch Gateway trunk)

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP Trunk) → B5800 Branch Gateway auto-attendant → caller enters extension number → B5800 Branch Gateway modifies extension number to user's enterprise number → Session Manager → CM-FS → Session Manager → centralized phone

3. From PSTN to centralized phone's DID (if LDN is ported to centralized trunks at the core)

   PSTN → central gateway/SBC → Session Manager → CM-FS → Session Manager → centralized phone

   Note:
   The B5800 Branch Gateway is not involved in handling the call in this scenario.

4. From branch local phone to centralized phone (dialing phone's enterprise number)

   Local phone → B5800 Branch Gateway → Session Manager → CM-FS → Session Manager → centralized phone

5. From headquarters (or other enterprise site) to centralized phone's enterprise number

   Originating phone → originating phone's controller → Session Manager → CM-FS → Session Manager → centralized phone

   Note:
   The B5800 Branch Gateway is not involved in handling the call in this scenario.

Calls from Centralized phones in survivability mode (aka rainy day)

1. Centralized phone A to Centralized phone B in the same branch

   Centralized phone A → B5800 Branch Gateway → centralized phone B

   Note:
   In rainy-day the centralized phones register to survivability service on the B5800 Branch Gateway in the branch.

2. Centralized phone to local phone (dialing either local phone's enterprise number or short extension)

   Centralized phone → B5800 Branch Gateway → local phone

3. Centralized phone to PSTN

Centralized phone → B5800 Branch Gateway → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → PSTN

4. Centralized phone to headquarters or other enterprise site

   B5800 Branch Gateway can be administered to send such calls over the PSTN. See below.

Calls to Centralized phones in survivability mode (aka rainy day)

1. From PSTN to centralized phone's DID

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → B5800 Branch Gateway → centralized phone

   Note:
   In rainy-day the centralized phones register to survivability service on B5800 Branch Gateway in the branch.

2. From PSTN to centralized phone via B5800 Branch Gateway auto-attendant

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → B5800 Branch Gateway auto-attendant → caller enters extension number → centralized phone

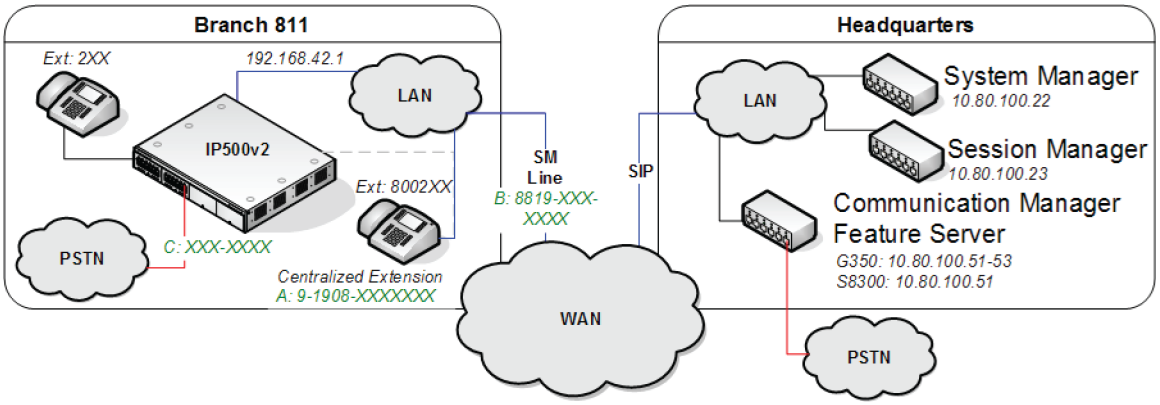
3. From branch local phone to centralized phone (dialing either local phone's enterprise number or short extension)

   Local phone → B5800 Branch Gateway → centralized phone

Appendix D: PSTN example call flow

During normal operation, calls made by a survivable extension are received by the Avaya Aura®Session Manager and passed to the extension's Communication Manager Feature Server. The Communication Manager Feature Server then sends the call back to the Avaya Aura®Session Manager for routing elsewhere in the Avaya Aura® network.

In this example, a survivable extension at branch 811 dials an external number in local area code 908. This happens to be local to branch 811, so we want Avaya Aura®Session Manager and Communication Manager Feature Server to route the call to that branch to be dialed as a local PSTN call.



For this example, the call routing is as follows:

1. The survivable extension co-located at branch 811 dials 9-1908-555-1111 (A).
2. This sends a SIP INVITE to the Avaya Aura® Session Manager. The B5800 Branch Gateway system at branch 811 is not involved.
3. The Avaya Aura® Session Manager identifies that the call is from an extension that matches an assigned Communication Manager Feature Server extension and so forwards the SIP INVITE to the Communication Manager Feature Server.
4. The Communication Manager Feature Server receives the SIP INVITE from Avaya Aura® Session Manager on a SIP trunk group number (for this example 42).
5. The Communication Manager Feature Server identifies the IP address of the extensions as an IP address mapped to IP Network Region 11 and Location 11.
6. The leading 9 in the dialed digit string matches the ARS Access Code. The 9 is removed from the dialed digit string.
7. The ARS Digit Analysis Table for Location 11 is queried for a match on the remaining digits 19085551111.
8. A match on 1908 is found, specifying Route Pattern 11.

9. Route Pattern 11 routes the call to SIP Trunk Group Number 32. This connects the Communication Manager Feature Server to the Avaya Aura®Session Manager and is specifically configured for routing local PSTN calls to branches.
10. The Communication Manager Feature Server sends a new SIP INVITE to Avaya Aura®Session Manager over SIP Trunk Group Number 32 with the dialed digits of 19085551111.
11. Avaya Aura® Session Manager finds a configured Dial Pattern that matches the dialed number 19085551111 with associated Routing Policy that routes the call to the B5800 Branch Gateway at branch 811.
12. The digit adaptation for calls going from Avaya Aura® Session Manager to that branch include a digit conversion that transforms 1908-XXX-XXXX into a local PSTN call 8119-XXX-XXXX.
13. Avaya Aura® Session Manager forwards the SIP INVITE with dialed digits string 8119-555-1111 to the branch.
14. The B5800 Branch Gateway internally routes the call to one of its PSTN trunks.

Communication Manager configuration required for survivable extension support

The topics in this section provide the Communication Manager procedures required to configure survivable extension mode. They are provided here as a reference for the Communication Manager configuration required to implement the PSTN call flow described in PSTN example call flow on page 313.

The procedures are provided using the Communication Manager SAT commands. However, you can use a different administrative interface, such as System Manager, to perform this configuration.

Verifying Communication Manager licenses

The license file installed on the Communication Manager system controls the maximum capacities permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

1. Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features required for this scenario.
2. Enter the **display system-parameters customer-options** command.
3. Navigate to Page 2 and compare the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column to verify that there is sufficient remaining capacity for SIP trunks.

The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

Configuring trunk-to-trunk transfer

Use this procedure to configure Communication Manager to allow trunk-to-trunk transfers.

1. Enter the **change system-parameters features** command.
2. In the **Trunk-to-Trunk Transfer** field, enter the appropriate number.

Note:

If the **Trunk-to-Trunk Transfer** field is set to **all**, this will enable all trunk-to-trunk transfers on a system-wide basis.

Note that this feature poses significant security risk, and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using **Class Of Restriction** or **Class Of Service** levels.

Configuring IP node names

Use this procedure to add Avaya Aura®Session Manager as an IP node.

1. Enter the **change node-names ip** command.
2. In the **Name** field, enter a name for this IP node.
3. In the **IP Address** field, enter the IP address of the Avaya Aura® Session Manager's Security Module (SM-100) interface.

Configuring IP codec set

If necessary, configure an IP codec set for use with SIP calls.

1. Enter the **change ip-codec-set n** command, where **n** is the codec set number to be used.
2. In the **Audio Codec** field, enter the desired audio codec type.
3. Retain the default values for the remaining fields.

Configuring IP network regions

An IP address map can be used for network region assignment. The network region assignment can be used to vary behaviors within and between regions. Typically, though this can be varied, each location will match an IP region and vice versa.

The following screen illustrates a subset of the IP network map used for this example configuration. Branch 811 has IP addresses in 192.168.42.0/24 assigned to network region 11.

```
display ip-network-map                                          Page   1 of  63
                              IP ADDRESS MAPPING

                                                  Subnet Network      Emergency
 IP Address                                       Bits   Region  VLAN Location Ext
 ------------------------------------------------ ------ ------- ---- -------------
 FROM: 10.1.2.0                                   /24    1       n
   TO: 10.1.2.255
 FROM: 10.32.1.0                                  /24    1       n
   TO: 10.32.1.255
 FROM: 10.32.2.0                                  /24    1       n
   TO: 10.32.2.255
 FROM: 192.168.42.0                               /24    11      n
   TO: 192.168.42.255
```

The following screens illustrate important aspects of the settings for each IP Network Region. The IP Network Region for each branch is mapped to the matching location . The values used for Branch 812 in IP Network Region 12 are shown below.

```
display ip-network-region 12                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 11
Location: 11        Authoratative Domain: example.com
    Name: Branch 811
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
```

- The **Authoritative Domain** matches the SIP domain configured in the Avaya Aura®Session Manager and the B5800 Branch Gateway.
- The **Codec Set** for intra-region calls is set to the codec set created for SIP calls.
- The **Intra region IP-IP Direct Audio** and **Inter region IP-IP Direct Audio** parameters are set to **yes** to allow direct media paths within and between regions. This minimizes the use of media resources in the Media Gateway.

The connectivity between network regions is specified under the Inter Network Region Connection Management heading, beginning on Page 3. Codec set 1 is specified for connections between network region 11 and network region 1.

```
display ipnetwork-region 12                                    Page   3 of  19

 Source Region: 11    Inter Network Region Connection Management      I       M
                                                                     G  A     e
 dst codec direct  WAN-BW-Limits   Video      Intervening      Dyn     A  G     a
 rgn  set   WAN  Units   Total Norm  Prio Shr Regions          CAC     R  L     s
 1    1     y    NoLimit                                             n all
 2
 3
 4
 5
 6
 7
 8
 9
10
11    1                                                              all
12    1                                                              all
```

The ip-network-region form for Network Region 1 needs to be similarly configured. Network region 1 is for phones and servers as well as Session Manager at the central location.

SIP signaling group and trunk group

For this example configuration two SIP signaling groups and two associated trunk groups are used between Communication Manager and Avaya Aura® Session Manager in the example configuration.

The primary SIP trunk group and its associated signaling group are used for regular call signaling and media transport to/from SIP phones registered to Avaya Aura® Session Manager including survivable extensions at the branches. The secondary SIP trunk group and its associated signaling group are used for routing calls from branch phones to native (non-toll) PSTN destinations.

Note that a single trunk group could be used for both purposes. However, the use of two trunk groups provides added flexibility to change trunk parameters independently. Tracing call legs within Communication Manager is also simplified.

Configuring SIP signaling groups

For Communication Manager to act as a Communication Manager Feature Server supporting survivable extensions, an IMS enabled SIP trunk to Avaya Aura®Session Manager is required.

1. Enter the **add signaling-group n** command, where **n** is an available signaling group number.
2. Enter the following values for the specified fields and retain the default values for all remaining fields.
    a. In the **Group Type** field, enter `sip`.
    b. In the **Transport Method** field, enter `tls`.
    c. In the **IMS Enabled?** field, enter `y`.
    d. In the **Near-end Node Name** field, enter the IP node name added for the Communication Manager Feature Server.
    e. In the **Far-end Node Name** field, enter the IP node name added for the Avaya Aura®Session Manager.
    f. In the **Near-end Listen Port** field, enter `5061`.
    g. In the **Far-end Listen Port** field, enter `5061`.
    h. In the **Far-end Network Region** field, enter the IP network region number assigned to the Avaya Aura®Session Manager.
    i. In the **Far-end Domain** field, enter the SIP domain name.
    j. In the **DTMF over IP** field, enter **rtp-payload**.

The screen below shows signaling group 42 which is used in the example configuration as the primary signaling group.

```
add signaling-group 42
                                SIGNALING GROUP

Group Number: 42                Group Type: sip
                          Transport Method: tls
 IMS Enabled? y


  Near-end Node Name: cm                      Far-end Node Name: sm1
Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1
                                               Far-end Domain: example.com

                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
```

The screen below shows signaling group 32 which is used in the example configuration as the “Secondary” signaling group to be associated with trunk group 32 for routing local PSTN calls from branch phones to Avaya Aura® Session Manager. Note that all the settings for this signaling group are identical to those for signaling group 42 except the following:

- The **Transport Method** is set to **tcp** (the port numbers will change automatically to **5060**).
- **IMS Enabled?** is set to **n**.

```
add signaling-group 32
                                SIGNALING GROUP

Group Number: 32              Group Type: sip
                        Transport Method: tcp
 IMS Enabled? n


  Near-end Node Name: cm                    Far-end Node Name: sm1
Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                       Far-end Network Region: 1
                                            Far-end Domain: example.com

                                                 Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                      RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload                 Direct IP-IP Audio Connections? y
```

Configuring SIP trunk groups

Next, SIP trunk groups need to be added.

1. Enter the **add trunk-group n** command, where **n** is an available trunk group number to add to SIP trunk groups.
2. Enter the following values for the specified fields, and retain the default values for the remaining fields.
    a. In the **Group Type** field, enter `sip`.
    b. In the **Group Name** field, enter a description for the trunk group.
    c. In the **TAC** field, enter an available trunk access code as per the dial plan.
    d. In the **Service Type** field, enter `tie`.
    e. In the **Signaling Group** field, enter the signaling group number .
    f. In the **Number of Members** field, enter the number that is equal to the maximum number of concurrent calls supported.

```
add trunk-group 42                                          Page   1 of   21
                                TRUNK GROUP

Group Number: 42                Group Type: sip                CDR Reports: y
  Group Name: SIP endpoints               COR: 1          TN: 1       TAC: *142
   Direction: two-way         Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n

                                                    Signaling Group: 42
                                                  Number of Members: 20
```

Navigate to Page 3, and enter **private** for the **Numbering Format** field as shown below. Use default values for all other fields.

```
add trunk-group 42                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n                Measured: none
                                                        Maintenance Tests? y

                  Numbering Format: private
                                                   UUI Treatment: service-provider

                                                    Replace Restricted Numbers? n
                                                   Replace Unavailable Numbers? n
```

The trunk group 32 used for routing local PSTN calls from branch phones is similarly configured.

Configuring route patterns

Configure a route pattern to correspond to each of the two newly added SIP trunk groups.

1. Enter the **change route-pattern n** command, where **n** is an available route pattern.
2. Enter the following values for the specified fields, and retain the default values for the remaining fields.
    a. In the **Pattern Name** field, enter a descriptive name for the route pattern.
    b. In the **Grp No** field, enter the trunk group number configured in Configuring SIP trunk groups on page 319.
    c. In the **FRL** field, enter the Facility Restriction Level that allows access to this trunk, **0** being least restrictive.

Configuring private numbering

1. Enter the **change private-numbering 0** command to define the calling party number to be sent
2. Add an entry for the Configuring SIP trunk groups on page 319.

In the example shown below, all calls originating from a 3-digit extension beginning with 2 and routed across any trunk group (shown by the **Trk Grp(s)** setting being blank) will result in a 3-digit calling number. The calling party number will be in the SIP **From** header.

```
change private-numbering 0                                      Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext            Trk         Private         Total
Len Code           Grp(s)      Prefix          Len
 3  4                                         3      Total Administered: 1
                                                        Maximum Entries: 540
```

Configuring AAR

1. Enter the **change aar analysis** command to add an entry for the extension range corresponding to the branch survivable extensions
2. Enter the following values for the specified fields, and retain the default values for the remaining fields.
    a. In the **Dialed String** field, enter the dialed prefix digits to match on.
    b. In the **Total Min** field, enter the minimum number of digits.
    c. In the **Total Max** field, enter the maximum number of digits.
    d. In the **Route Pattern** field, enter the route pattern number configured for these extensions.
    e. In the **Call Type** field, set this to **aar**.

```
change aar analysis 4                                           Page   1 of   2
                            AAR DIGIT ANALYSUS TABLE
                                  Location: all               Percent Full:   2

         Dialed           Total     Route   Call     Node     ANI
         String          Min  Max  Pattern  Type     Num      Reqd
    4                    3    3     42      aar              n
    49998                5    5     32      aar              n
    50000                5    5     1       aar              n
```

ARS Access Code

The example configuration designates **9** as the ARS Access Code. This is shown below on Page 1 of the **change feature-access-codes** form. Calls with a leading 9 will be directed to the ARS routing table.

```
change feature-access-codes                                    Page   1 of   8
                                FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *56
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
      Auto Route Selection (ARS) - Access Code: 9    Access Code 2:
                  Automatic Callback Activation: *57   Deactivation: *58
```

Location specific ARS digit analysis

Location based analysis is used before global analysis. Using it we could apply rules that only apply to calls from survivable extensions at location 11. For example, the pattern below routes calls prefixed 1908 from location 11 back to the Avaya Aura® Session Manager using Route Pattern 32 on page 320 when a match occurs.

The **change ars analysis location x y** command is used to make location specific routing entries where the **x** is the location number and the **y** is the dialed digit string to match on.

```
change ars analysis location 11 1908                           Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                  Location:  11              Percent Full:   2

          Dialed           Total      Route      Call    Node   ANI
          String          Min  Max   Pattern     Type    Num    Reqd
    1908                  11   11    32          natl           n
```

However for our example, we want to route any dialing prefixed with 1908, regardless of location, which we can do in the Global ARS Digit Analysis on page 322.

Global ARS Digit Analysis

For this example we want all outgoing external calls prefixed with 1908 to be routed back to the Avaya Aura® Session Manager, regardless of the location of the survivable extension making the call.

The **change ars analysis y** command is used to make global routing entries where the **y** is the dialed digit string to match. A match on this table can occur if there is no match on the ARS Location Specific ARS Analysis on page 322.

The global ARS table as used in the example configuration is shown below. Long distance calls, 1 + 10 digits, will match the Dialed String of 1 with 11 digits and select Route Pattern 3 on page 320.

Route Pattern 3 is configured to use a Trunk Group that connects to the Communication Manager Feature Server at the headquarters location for PSTN calls to and from that site.

```
display ars analysis 1                                      Page   1 of   2
                          ARS DIGIT ANALYSIS TABLE
                                Location:  all            Percent Full:    2

          Dialed            Total     Route    Call    Node    ANI
          String           Min  Max  Pattern  Type    Num     Reqd
     1                     11   11    3        hnpa            n
     101xxxx0              8    8     deny     op              n
     101xxxx0              18   18    deny     op              n
     1908                  11   11    32       natl            n
```

Appendix E: Branch PSTN call routing examples

Each B5800 Branch Gateway system can support its own external PSTN trunks. When deployed in an Avaya Aura® network, you have considerable flexibility over where outgoing PSTN calls should emerge from the network and similarly where incoming calls should be routed.

The following examples demonstrate some of the options available:

- Centralized call control on page 325 — External calls at a branch site can be rerouted to be dialed out at another site. This can be done for reasons of call cost and call control. For example, the central site may have a bulk call tariff for national and international calls that would benefit all branches.
- Branch PSTN Override on page 328 — Having configured the branch to send outgoing external calls to the Avaya Aura® Session Manager for onward routing, there may be cases where a specific number should still be routed via the branches own PSTN trunks.
- PSTN Fallback on page 330 — The B5800 Branch Gateway can be configured to allow some calls that would normally use the Avaya Aura® Session Manager line to be routed via the PSTN when the Avaya Aura® Session Manager line is not available.

The various methods used in these examples can be combined to match the customer's needs. However the main aim should be as follows:

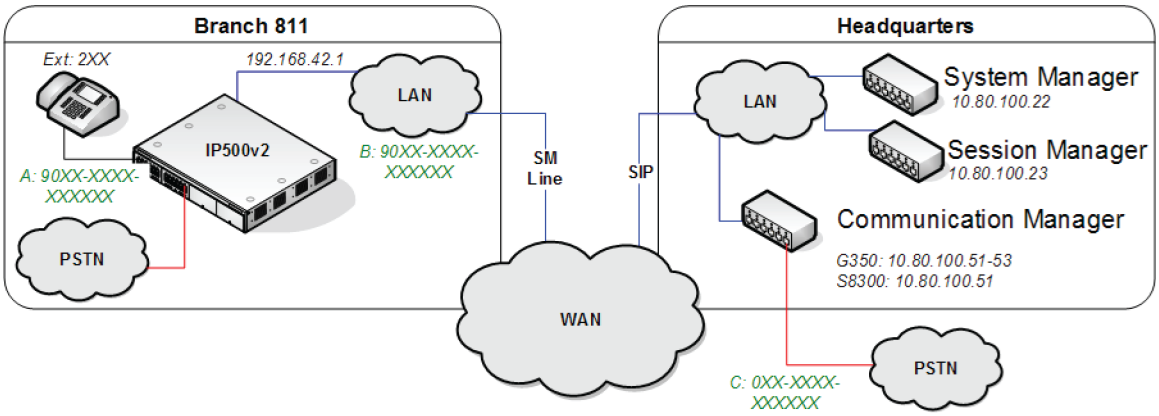
- To keep the branch configuration as generic as possible, i.e. to use the same PSTN call control in all branch configurations. This simplifies maintenance of multiple branches.
- To centralize as much of the PSTN call control in the Avaya Aura® Session Manager as possible. Again this simplifies maintenance and control.

Centralized call control

External calls at a branch site can be rerouted to be dialed out at another site, typically the headquarters site. This can be done for reasons of call cost and control and to reduce the external PSTN capacity required at the individual branch sites.

In this example we route all national and international calls to the headquarters site. The Avaya Aura® Session Manager there routes the calls out via PSTN services at that site. Note, however, that the Avaya Aura® Session Manager could alternately use the trunks at a branch for some calls. For example, if the national call is to an area code that is local to a particular branch, the call could be routed to that branch for dialing on its PSTN trunks.

In this example, the company wants all national and international calls made at the branch to be routed to use the headquarter site's PSTN trunks. This is in order to benefit from a bulk cost reduction available for calls from that site.



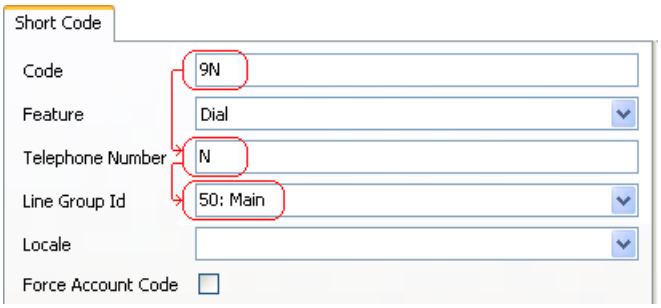
This example assumes that all the branches were initially setup with the default North American locale. For B5800 Branch Gateway that means that a dial 9 prefix is used for external calls. For calls in other locales or between branches in different locals, the example will need to be adjusted to ensure that the resulting number received at the remote branch will be routed to an external PSTN trunk and is suitable for external dialing.

Routing B5800 Branch Gateway calls

About this task

At each B5800 Branch Gateway, we need to ensure that calls starting with 90, the external and then international number prefixes, are routed to the branch's Avaya Aura® Session Manager line rather than direct to an external PSTN line.

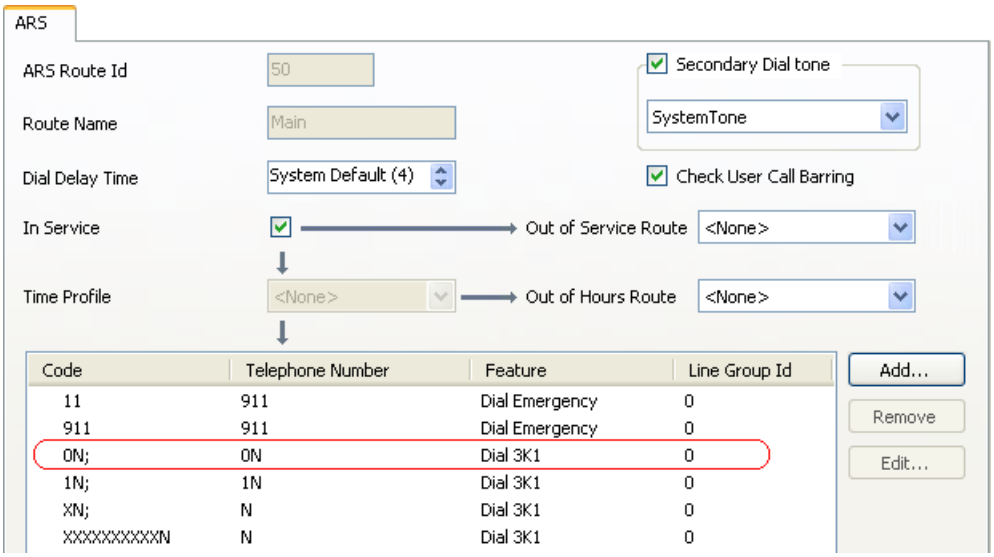
In the B5800 Branch Gateway system configuration, the default system short code **9N** is used to match calls prefixed with a 9. The short code removes the 9 prefix and routes the call to the branch's ARS form **50: Main**.



Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **ARS**.

3. Click **50: Main**.



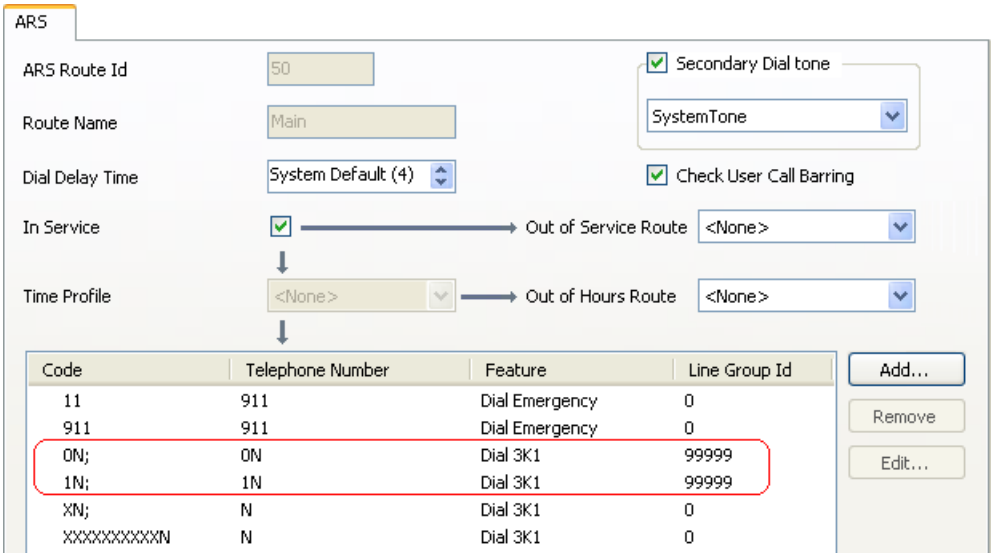
   Within the ARS window, the default **0N;** short code that matches international numbers currently routes those calls to any available trunk in line group 0.

4. To edit the short code, click the short code.
5. Click the **Edit...** button.
6. Make the following changes:

   a) In the **Code** field, leave this set to **0N;**.
   b) In the **Feature** field, change this to **Dial**.
   c) In the **Telephone Number** field, change this to **90N**.

      The **9** has been added back as it matches the dial pattern typically used at the Avaya Aura® site for matching a call that needs routing to the PSTN.
   d) In the **Line Group ID** field, change this to match the Avaya Aura® Session Manager line Outgoing Group ID. The default is **99999**.

7. Click **OK**.
8. Repeat Steps 4 through 7 for the **1N;** short code which is used for national calls. The branch system's default ARS form is now set to route all national and international calls to the Session Manager line and thus to the Avaya Aura® Session Manager.



9. Click **OK**.
10. Select **File > Save Configuration**.

Branch PSTN override

In the example provided in Centralized call control on page 325, we configured the branch system so that all national and international calls go to the headquarters site for routing to the PSTN. There may occasionally be scenarios where a particular number needs to override this and be dialed via the branch system's own PSTN trunks.

One example is the Modular Messaging PSTN number that can be configured for access to voicemail when the branch's Avaya Aura® Session Manager line is out of service. Another might be to provide a maintenance number to the headquarters site to report suspected loss of the Avaya Aura® Session Manager line connection.

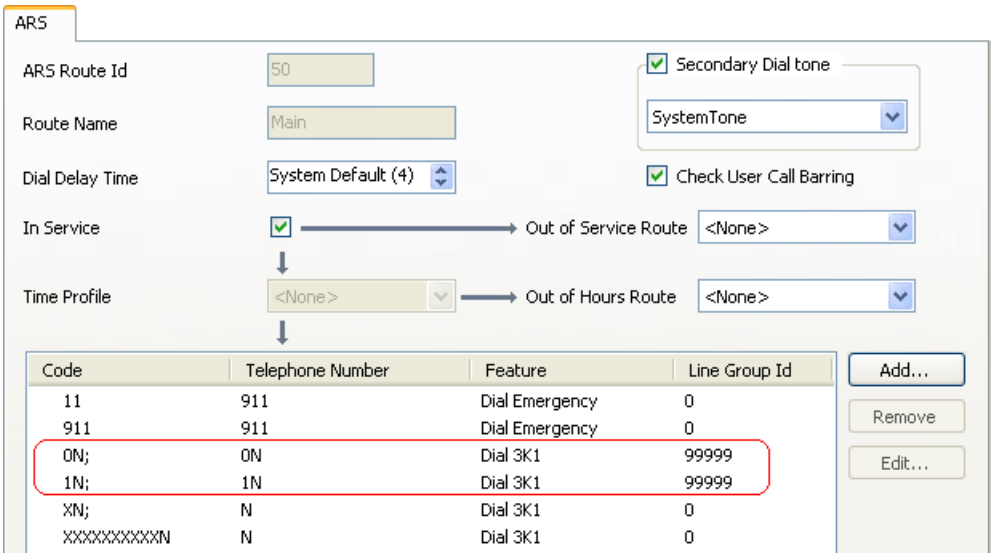
Adding an overriding short code

About this task

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **ARS**.

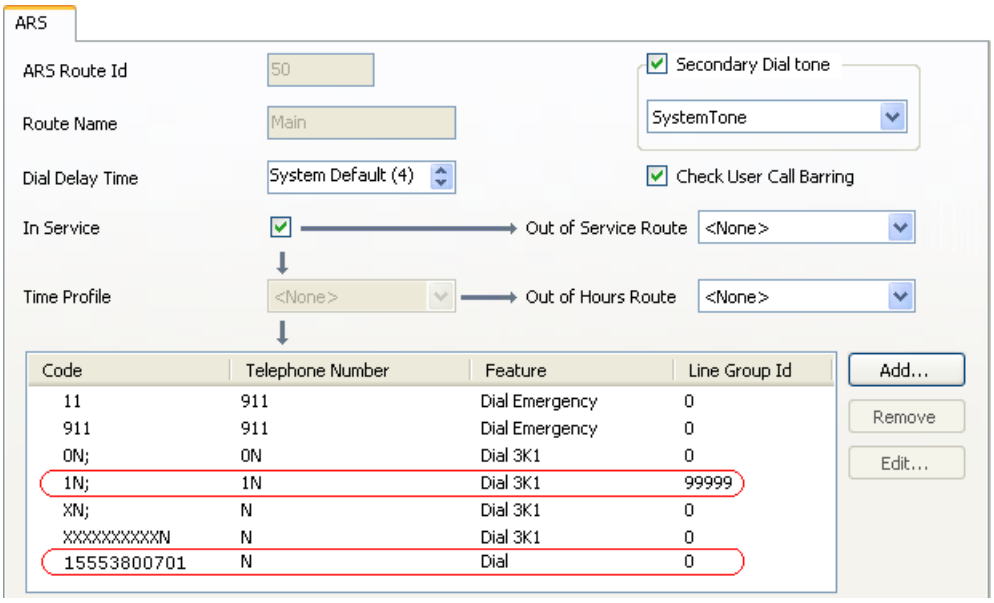
3. Click **50: Main**.



Within the ARS form, the default **1N;** short code is the one used for national calls. It would match the MM PSTN Number and attempt to route it to the SM Line which we know is out of service if the MM PSTN Number is being used for calls to voicemail. We can change the routing by adding a specific short code for the MM PSTN Number.

4. To add a short code, click the **Add...** button.
5. Make the changes as follows:
   a) In the **Code** field, set this to match the external PSTN number for Modular Messaging without the external dialing prefix.
   b) In the **Feature** drop-down box, select **Dial3K1**.
   c) In the **Telephone Number** field, set this to **N** to match the whole number in the **Code** field.
   d) In the **Line Group Id** drop-down box, select the line group ID being used for the branch's PSTN trunks. The default is 0.
6. Click **OK**.
   The ARS now has two short codes that will potentially match external national calls. However, one is a more exact match for certain calls and therefore will be applied

to those calls.



7. Click **OK**.
8. Select **File > Save Configuration**.

PSTN trunk fallback

In branch scenarios where centralized call control and trunking (see Centralized call control on page 325) has been configured for certain calls, loss of the Avaya Aura®Session Manager line connection will impact making those calls. For instance, in our example where all branch national and international calls are routed via the headquarters site, loss of the Avaya Aura® Session Manager line will leave the branch users only able to make local calls (that includes any centralized extension users at the site who may be operating in survival mode).

Since loss of the Avaya Aura® Session Manager line should only be an infrequent and temporary condition, some restriction during that state may be acceptable. However the following options can be used to allow continued branch operation:

- If the headquarters site has multiple Avaya Aura®Session Managers for redundancy, each branch can also be configured with multiple Avaya Aura® Session Manager lines. See Avaya Aura Session Manager line redundancy on page 118 for more information.
- As in our example business, centralized call control has not been applied to all branch local calls. Therefore local calls are still available without any additional configuration for the loss of the Avaya Aura® Session Manager line connection.
- Since loss of the Avaya Aura® Session Manager line should be infrequent and temporary, the loss of some services may be tolerable until the Avaya Aura® Session Manager line

issue is resolved. However, even if that is the case, it may be recommended to configure a headquarters PSTN number that can be dialed to report the Avaya Aura® Session Manager line issue. See Branch PSTN override on page 328 for more information.

- Provide PSTN trunk fallback within the branch configuration. See Configuring PSTN trunk fallback on page 331. Note however that PSTN fallback will also occur when the number of external calls exceeds the available SIP trunk licenses.

Note:

If you want to have long distance routing on local trunks, be sure that the appropriate trunks have been ordered from the local provider. Do not create a route for international phone calls if you do not have that service.

Configuring PSTN trunk fallback

About this task

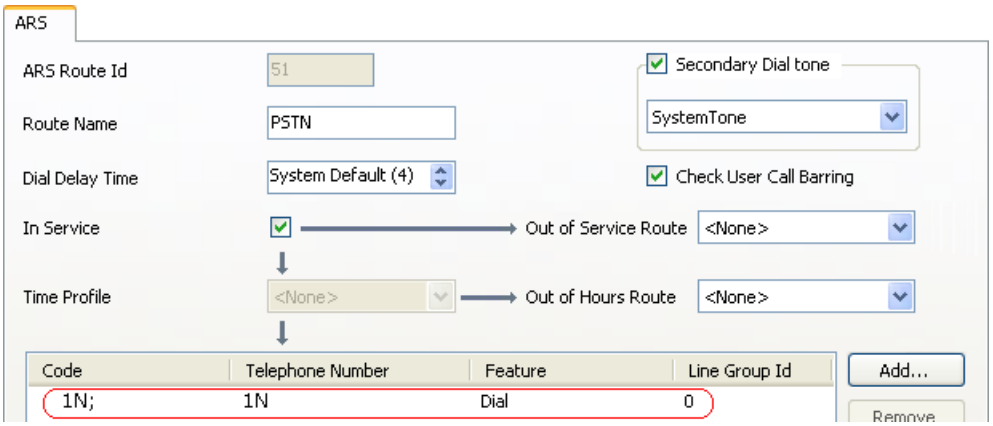
Use this procedure to provide PSTN trunk fallback with the branch configuration.

Procedure

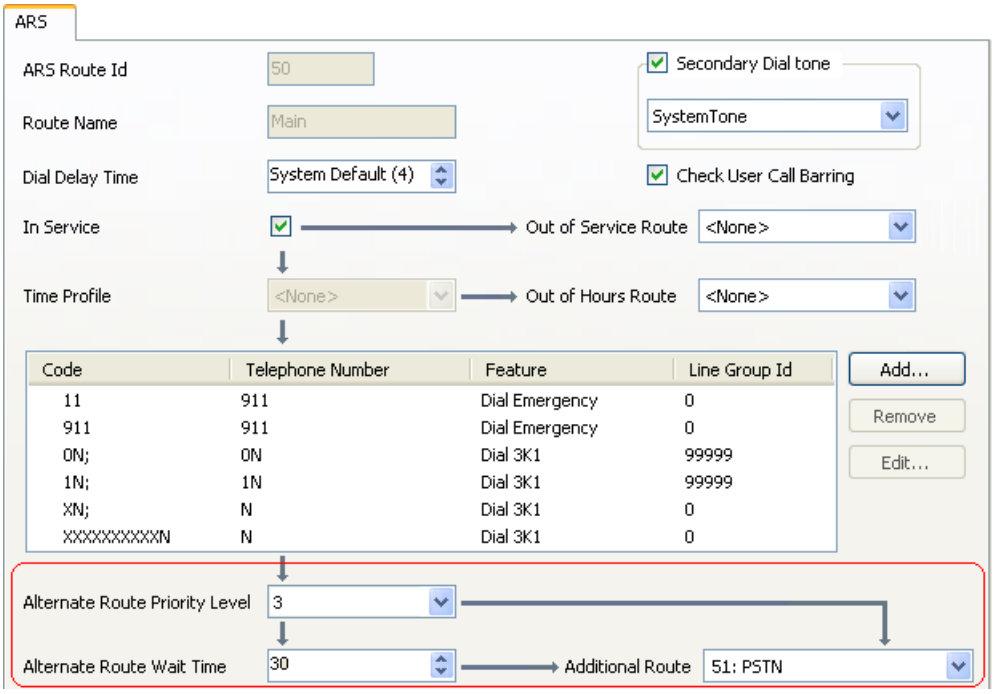
1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **ARS**.
3. Click the **New** icon and select **ARS**.
4. Enter a **Route Name**, for example **PSTN**.
5. To add a short code click the **Add...** button.

   A short code is required that will send the national calls to the branch's own PSTN. Enter the normal defaults for such a short code as follows:
6. Make the changes as follows:
   a) In the **Code** field, enter **1N;**. For this example, **1N;** will match any national number dialing.
   b) In the **Feature** field, leave the entry set as **Dial3K1**.
   c) In the **Telephone Number** field, enter **1N**. For this example **1N** will match the number dialed by the user after the dial 9 prefix.
   d) In the **Line Group Id** drop-down box, select the line group used for the B5800 Branch Gateway system's external trunks. The default is 0.

7. Click **OK**.



8. Click **OK**.
9. Double click on the existing default ARS that was reconfigured to send all branch national and international calls to the Avaya Aura® Session Manager line.



10. In the **Additional Route** drop-down box , select the PSTN ARS form just created above.

    The form is now set such that, if the Avaya Aura® Session Manager line is not available (out of service or all licensed channels busy) calls can be checked for a dialing match in the PSTN ARS form. This works as follows:

    - The **Alternate Route Priority Level** controls which users are able to use the alternate route immediately, ie. those user's whose priority is equal or higher than this setting. The default priority for users is **5**.

- The **Alternate Route Wait Time** is used for caller's whose priority is not sufficient to use the alternate route immediately. The default setting is 30 seconds. However, you may want to adjust this setting to one that meets your requirements.
- Since the only short code match in the alternate route in our example is for national calls, international calls will continue to wait for the Avaya Aura® Session Manager line.

11. Select **File > Save Configuration**.

Appendix F: Recommended courses for Avaya B5800 Branch Gateway training

Avaya B5800 Branch Gateway

Table 1: APSS – SMEC

Type	Code	Course title	Delivery	Duration (hours)	First offering
Existing	ASC00121 WEN	Selling IP Office	eLearning	4	Now
New	ASC00126 OEN	Selling IP Office - Update Release 6.1	eLearning	0.5	October

Table 2: ACIS – IP Office

Type	Code	Course title	Delivery	Duration (hours)	First offering
New	ATU02142 WEN	IP Office Technical Delta Release 6.1 (inclusive Release 6)	eLearning	1.5	Nov
Existing	AVA00916 WEN	IP Office Hardware and Data Components	eLearning	6	Now
Existing	ATA01225I EN	IP Office 6.1 Implementation Workshop	ILT	40	Now
Update to vILT	ATC01225 VEN	IP Office 6.1 Implementation Workshop	vILT	40	Jan
New	6401.1	Avaya IP Office Implementation Exam (ACIS)	Exam	2	Nov

Unified Communications

Table 3: ACIS – Session Manager and System Manager

Type	Code	Course title	Delivery	Duration (hours)	First offering
Update	ATU00180OE	System Manager General Overview	eLearning	1	Dec 6
Update	ATU00171OEN	Session Manager General Overview	eLearning	2	Dec 6
Update	ATU00183OEN	System Manager Technical Overview	eLearning	1	Dec 6
Update	ATU00170OEN	Session Manager Technical Overview	eLearning	2	Dec 6
Update	ATC00175OEN	Session Manager Rack and Stack	eLearning	.5	Dec 6
New #	ATA02641OEN	System Manager Installation and Setup 6.1	eLearning	.5	Dec 6
New #	ATA02446OEN	Session Manager Installation and Initial Setup 6.1	eLearning	2	Dec 6
New #	ATA02446OEN	Survivable Remote Session Manager Installation & Initial Setup 6.1	eLearning	.5	Dec 6
Update	ATC00182OEN	Getting Started with System Manager	eLearning	1	Dec 6
Update	ATC00184VEN	System Manager Administering User Profile & Operator Accounts	vILT	3	Dec 6
Update	ATI00176VE	Session Manager Network Routing Policy Administration	vILT	6	Dec 6
New	ATA01517VEN	Session Manager Instance Administration	vILT	2	Dec 6
New	ATA02444VEN	Session Manager User Administration	vILT	3	Dec 6

Type	Code	Course title	Delivery	Duration (hours)	First offering
New	ATI02445VEN	Session Manager, CM and other Feature Server Administration	vILT	5	Dec 6
Update	ATC01840VEN	Survivable Remote Session Manager Administration 6.1	eLearning	2	Dec 6
Update	ATC01842OEN	CM and System Manager	eLearning	2	Dec 6
New	ATA02540VEN	Advanced System Manager Administration	eLearning	3	Dec 6
New	ATU02643OEN	System Manager 6.1: Delta General Overview	eLearning	.5	Dec 6
New	ATU01515OEN	Session Manager 6.1: Delta General Overview	eLearning	1	Dec 6
New	ATI02642OEN	System Manager 6.1: Delta Technical Overview	eLearning	1	Dec 6
New	ATI01516OEN	Session Manager 6.1: Delta Technical Overview	eLearning	1	Dec 6

Table 4: ACIS – Communication Manager and CM Messaging 6.0

Type	Code	Course title	Delivery	Duration (hours)	First offering
New	ATI02348IEN	Avaya Aura™ Communication Manager Implementation	vILT/ILT	30	Nov
New	ATI01731VEN	Avaya Aura™ Communication Manager Messaging – Embedded Implementation	vILT	12	Nov
New	6002.1	Avaya Aura™ Communication Manager and Communication Manager Messaging ACIS Exam	Exam	1	Nov

Glossary

Centralized Branch user model

This term describes aB5800 Branch Gateway deployment model where certain 9600 Avaya SIP phones can use the B5800 Branch Gateway as a survivability gateway. In normal operation, these phones register directly to the Avaya Aura®Session Manager in the enterprise core and get services from core applications such as the Communication Manager Feature Server or Evolution Server. The local B5800 Branch Gateway can still be accessed as a SIP gateway connected to the core Avaya Aura®Session Manager to provide access to local PSTN trunks and services when required. If WAN connectivity to the Avaya Aura®Session Manager is lost, the SIP phones automatically register with and get services from the B5800 Branch Gateway. When connection to the Avaya Aura®Session Manager is available again, failback occurs where the SIP phones return to being controlled by Avaya Aura®Session Manager

Centralized extension

See Survivable extension.

Centralized management

This term is used to describe a central management system that delivers a set of shared management services and provides a single access interface to administer multiple branch locations and multiple distributed or centralized B5800 Branch Gateway users.

Centralized trunking

This term describes routing outgoing external calls from the branch sites to the central site in order to utilize the central sites PSTN trunks. The same applies for distributing incoming PSTN calls from the central site to the appropriate branches.

Distributed Branch user model

This term describes a B5800 Branch Gateway deployment model where call processing for the branch phones is provided locally. Non-IP phones are connected to B5800 Branch Gateway and IP and certain SIP endpoints (not including the Avaya 9600 SIP phones) can be administered with B5800 Branch Gateway as their controller. Access to and from the rest of the Avaya Aura® network is via the B5800 Branch Gateway system's Avaya Aura®Session Manager link across the enterprise WAN. This connection allows for VoIP connectivity to other B5800 Branch Gateway systems, to centralized trunking and to centralized applications such as conferencing and Modular Messaging.

Distributed trunking

This term describes the scenario where each branch retains and uses its own PSTN trunks for incoming and outgoing external calls.

Failback	This term is used for the situation where a centralized extension that is working with a survivability call controller detects that its normal call controller is available again. The extension will go through a process of failback to its normal call controller.
Failover	This term is used for the situations where a centralized extension's preferred call controller is no longer available. The extension will go through a process of failover to the first available of its configured alternate call controllers which then provides survivability services to the extension.
Local extension	See Native extension.
Local management	This term is used to describe managing a B5800 Branch Gateway device using the local B5800 Branch Gateway Manager application.
Mixed Branch user model	This term describes a B5800 Branch Gateway deployment model where each B5800 Branch Gateway system can support extensions using the Centralized Branch user model and extensions using the Distributed Branch user model at the same time. The extensions supported in the Centralized Branch user model are SIP extensions only. This user model has also been referred to as a Concurrent Branch user model.
Mixed mode trunking	The flexibility of Avaya Aura® Session Manager is such that both centralized and distributed trunking can be used. For example, routing all national and international calls via centralized trunking at the headquarters site while still allowing local calls via the branch sites.
Native extension	This term is used to describe extensions that get their call services from the branch site and operate in the Distributed Branch user model. A native extension is also referred to as a local extension.
Rainy day	This term refers to a loss of network connectivity from the branch to the core data center. All endpoints are registered to the local B5800 Branch Gateway. See Survivability.
Sunny day	This term refers to full network connectivity from the branch to the core data center. SIP endpoints are registered to the Avaya Aura®Session Manager.
Survivable extension	This term is used to describe an extension which, though physically located at a branch site, receives its' telephony services from the central or headquarters site and operate in the Centralized Branch user model. A survivable extension is also called a centralized extension.
Survivability	This term describes centralized extensions when working after failover. The range of functions available to the phones in this state depend largely on those configured for them on the branch system and will not

	match those available from the headquarters system during normal operation. See Rainy day.
Tail-End-Hop-Off	Part of mixed mode trunking, this describes scenarios where certain calls at other branches or the headquarters site are routed to the PSTN of another branch.