Avaya Aura® Communication Manager Survivability Options

Release 10.2.x
Issue 2
April 2025

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 in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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 websites 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 Avaya hardware and software. Please refer to your agreement with Avaya 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 website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document provides procedures to install and configure survivable core server.

Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the End of sale G650 document published on the Avaya Support website.

Intended audience

This document is for the following audiences:

- Technical support representatives
- Authorized Business Partners

Change history

Issue	Date	Summary of changes
2	April 2025	Updated the following section: • Survivability Overview on page 9
1	November 2024	Initial release R10.2

Chapter 2: Survivability Overview

The Survivable remote server (formerly called Local Survivable Processor [LSP]) and the Survivable core server (formerly called Enterprise Survivable Server [ESS]) are survivable options available with Avaya Aura® Communication Manager.

- Survivable Remote Server: When communication to the Primary Controller (main server) is lost, the survivable remote server option allows the IP telephones and one or more gateways to register with a Survivable remote server. if the **Local Survivable Server (LSP)** is selected on the Server Role page of System Management Interface (SMI), the survivable remote server takes control of gateways that has its address in the Media Gateway Controller (MGC) list. You must manually administer the MGC list. The IP telephones use an Alternate Gateway List (AGL) for gateway addresses. These addresses are automatically generated by Communication Manager and sent to the IP telephones upon registration. To understand the difference between a Survivable remote server and a Survivable core server see *Processor Ethernet overview*.
- Survivable Core Server: When communication to the Primary Controller (main server) is lost, the survivable core server option allows the IP telephones and one or more gateways to register with a Survivable core server. If the **Enterprise survivable server (ESS)** is selected on the Server Role page of System Management Interface (SMI), the survivable core server takes control of gateways that has its address in the MGC list. You can manually administer the MGC list. The IP telephones use an Alternate Gateway List (AGL) for gateway addresses. These addresses are automatically generated by Communication Manager and sent to the IP telephones upon registration. The Survivable core server option provides survivability to an Avaya configuration by allowing survivable servers to be placed in various locations in the customer's network.

  An ESS activates when the main Communication Manager encounters an error. The ESS functions as a backup for the main Communication Manager. To configure the **Survivable License Grace Period (in days)** field, the administrator navigates to the **Survivable Processor** screen on the main Communication Manager server and enters the preferred grace period. The valid values for this field are 30, 60, 90, and 180 days, and the default value is 30 days.

For more information about the supported servers and supported gateways, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Related links

Processor Ethernet overview on page 13
C-LAN access for survivable core server registration
Survivable core server requirements on page 15

Survivable core server failover examples on page 16
Survivable core server on page 11
C-LAN access for survivable core server registration
Survivable core server requirements on page 15
Survivable core server failover examples on page 16
Processor Ethernet overview on page 13
C-LAN access for survivable core server registration
Survivable core server requirements on page 15
Survivable core server failover examples on page 16

Survivable remote and core servers

Survivable remote server

In a survivable remote environment, each gateway is manually configured with a list of call controllers during initialization and each IP endpoint can be manually configured with a list of call controllers during initialization or the Call controller settings can be downloaded to the endpoints. If for any reason, the communication between a gateway and its primary controller stops, the gateways and the IP endpoints register with a call controller on its list. If the survivable remote server is in the list of call controllers, the gateway and the IP endpoint registers with the survivable remote server. The gateway registers with the survivable remote server first before the IP telephone registers with the survivable remote server.

The Media Gateway Controller list can have Processor Ethernet addresses of main or survivable servers or Avaya Session Border Controller for Enterprise addresses prefixed with Session Border Controller for Enterprise in an Edge Friendly configuration. The list can contain up to 4 IP addresses/FQDNs.

The Processor Ethernet (PE) interface on a survivable remote server is used for:

- Connectivity to three adjuncts: Call Detail Recording (CDR), Application Enablement Services (AES), and Call Management System (CMS).
- H.323 and H.248 registration.

For more information on Processor Ethernet, see Processor Ethernet overview on page 13.

You can have both survivable core servers and survivable remote servers in a survivable core server configuration.

In an Edge Topology, a survivable remote server can be deployed within a cloud-connected branch office or within a distinct sub network behind a Network Address Translation (NAT) device. In this mode, the survivable remote establishes a connection to the main Communication Manager through a single WebSocket tunnel, which also facilitates remote access. If the remote branch office becomes isolated, the Local Survivable Processor (LSP) assumes control of call

functionalities, operating as a Local Survivable Server similar to the setup in the enterprise (non-Edge) topology. For further details, see *Administering Avaya Aura® Communication Manager*.

Related links

Processor Ethernet overview on page 13

Survivable core server

In a survivable core server environment, the media gateway contains a priority list of survivable core servers. If for any reason, the communication between the media gateway and the main server is lost, the media gateway requests service from the highest ranking survivable core server on its list. The survivable core server accepts the request and assumes control of the media gateway.

The survivable core server provides the same functionality and the same capacity as the main server.

A single survivable core server can use the Processor Ethernet interface to connect to CDR, AESVCS, and CMS. Duplex servers can use the Processor Ethernet interface to connect to CDR and Avaya Aura® Messaging.

Communication Manager Release 6.0 and later has the following capabilities:

- Processor Ethernet (PE) is supported on simplex and duplex servers for the connection of H.323 devices, Gateways, SIP trunks, and most adjuncts.
- When Processor Ethernet is used on duplex servers, it must be assigned to an IP address, **Active Server IP address**, that is shared between the servers. This address is known in networking terminology as an IP-alias. The active server is the only server that will respond on the IP-alias.

The Communication Manager templates are available in following two categories:

1. Communication Manager survivable core server contains the following templates:
   - Duplex
   - Simplex
2. Communication Manager survivable remote server contains the following templates:
   - Simplex Survivable Remote
   - Embedded Survivable Remote

The following table provides information on template types that can be used as a survivable remote or core server for Communication Manager.

Table 1: Survivable remote or core server template types

Template type	S8300	R640
Duplex	__	Y

Table continues…

Template type	S8300	R640
Simplex	__	Y
Embedded	Y	__
Simplex Survivable Remote	__	Y
Embedded Survivable Remote	Y	__

The survivable core server option provides survivability to an Avaya configuration by allowing survivable servers to be placed in various locations in the customers network.

In a survivable core environment, there is only one main server. The main server can be a single server, or a duplicated server. If the main server is a single server, all the survivable core servers in the configuration must also be a single server.

Through careful planning and consideration, the servers are placed in various locations in the network of the customer (see *Survivable Core Server design and planning*). Each survivable core server is administered on the main server. During administration, values are assigned to the survivable core server. After administration, system translations are synchronized between the main server and the survivable core server. Once the survivable core server receives the translations, it assigns its values to every media gateway in the configuration. This is true for all servers except those administered as a Local Only server. Local Only servers connect to media gateways in their same community. For more information on administering the values for survivable core server, see *Survivable core server administration*.

The media gateways in the configuration contain a list (called a priority list) of survivable core servers. The main server is always the highest ranking server on an media gateways's priority list. The media gateway prioritizes the survivable core servers on its list using the administered values assigned by the survivable core server. The priority list is dynamic. Changes to the media gateways's priority list may be caused by a change in the assigned value of a survivable core server, a server with a higher value bumping a server with a lower value off the list, or loss of communication with a survivable core server.

Related links

Survivable core server administration on page 52
Survivable Core Server design and planning on page 28

Primary search timer

The media gateway may be requesting service from a survivable core server after the media gateway loses communication with the main (primary) server. The interval from the loss of communication to the time the media gateway requests service of a survivable core server is called the primary search time out interval. During this interval the media gateway only tries to reconnect to the primary server. The value for the primary search timer is administrable from 1 to 59 minutes, with a default 1 minute. For more information on the primary search timer see, *Administering Avaya Aura® Communication Manager*.

Related links

Checking the administration on the main server on page 57

Failover to a survivable core server

Existing Communication Manager recovery mechanisms still occur prior to a failover of a Media Gateway to a survivable core server.

Response to a failover	Description
The Main fails for duplicated servers.	• Failure of the active server causes a server interchange. The Media Gateway is still under control of the main server. • Failure of both servers causes loss of communication to the Media Gateway. The Media Gateways primary search timer activates.
The Main fails for a single or simplex server.	Failure of the main server causes loss of communication to the Media Gateway. The Media Gateways primary search timer activates.

Related links

Survivable core server administration on page 52

Processor Ethernet overview

Processor Ethernet (PE) is used for IP connectivity.

Note:

Communication Manager IP endpoints can register either to PE . PE resides on the Communication Manager server . Communication Manager can have one PE.

When configuring Communication Manager on a server, the PE interface is assigned to an IP Address on the control network or corporate LAN. Communication Manager establishes a logical connection between the Communication Manager software and the physical port (NIC) for the PE interface.

The PE interface is enabled by default in the license file. The feature keyword FEAT_PRETH must be checked to **ON** in the license file for PE to work.

A survivable server enables the PE interface automatically. On a survivable remote server, the **H.248** and the **H.323** fields default to a `yes` on the IP Interface Procr screen, to allow the registration of H.248 gateways and H.323 endpoints using the PE interface.

The gateway and H.323 endpoint registration on a survivable core server is allowed if you administer the **Enable PE for H.248 Gateways** and **Enable PE for H.323 Endpoints** fields on the Survivable Processor screen on the main server. Therefore the **H.248** and the **H.323** fields on the IP Interface Procr screen of the survivable core server display the values that you administered.

Important:

Both survivable core and remote servers require the use of the PE interface to register to the main server. Do not disable the PE interface.

Processor Ethernet functionality

The following table shows how the Processor Ethernet (PE) functionality works on main servers and survivable core servers. For more information on how to administer the PE interface, see *Administering page one of the Survivable Processor screen*.

Table 2: Use of Processor Ethernet interface on main servers and survivable core servers

Possible functions of the PE interface	Main server	Survivable core server
Registration	The main server accepts registration messages from a survivable core or remote server through the PE interface.	The use of the PE interface for registration to the main is automatically enabled by the Communication Manager software. The PE interface needs to be configured on the System Management Interface.
Adjunct connectivity	All adjuncts are administered on the IP Services screen on the main server. • You can use the PE interface on a simplex server to connect to three supported adjuncts, AESVCS, CMS, and CDR. • You can use the Process Ethernet interface on a duplex main server to connect to CMS. You can use the PE interface on a duplex server to connect to CDR, Messaging (all that support IP connectivity) [1].	The way adjuncts connect to a survivable core server is administered on the Survivable Processor screen on the main server.
Gateway registration	Administration to allow H.248 registration on the PE interface of a main server is performed on the IP Interfaces screen.	Administration to allow H.248 registration on the PE interface of a survivable core server is performed on the Survivable Processor screen.

Related links

Administering page one of the Survivable Processor screen on page 53

Support for Processor Ethernet on a survivable core server

A survivable core server supports the connection of IP devices to the Processor Ethernet interface.

A survivable core server uses its Processor Ethernet interface to support IP devices such as Branch Gateways, H.323 Media Gateways, Adjuncts, IP telephones, IP trunks, and SIP trunks.

[1] If you connect the gateways to PE on the main server because there are no C-LANs in the system, the gateways should have the PE of the survivable core server as the first entry in the survivable server portion of their MGC list. If C-LANs are present, the MGC list includes C-LAN addresses in the primary portion of their MGC list

A survivable core server provides the equivalent benefit of a survivable remote server. A survivable core server creates a duplicate server, providing additional redundancy to the survivability of the server.

Processor Ethernet requirements

- For Processor Ethernet on duplex servers, assign the Processor Ethernet interface to the Processor Ethernet Active Server IP Address (IP-alias).
- The Network Interface Card (NIC) assigned to the Processor Ethernet interface must be on a Local Area Network (LAN) connected to the main server.
- If the survivable server registers to the Processor Ethernet on the main server, the Processor Ethernet on the main server must have IP connectivity to the LAN. However, the LAN must be assigned to the NIC used for Processor Ethernet on the survivable core server.
- Processor Ethernet on duplex servers works effectively when the gateways and IP telephones are on the latest firmware release.

Optimal performance requirements

- To ensure optimal server performance while using Processor Ethernet on duplex servers, use the following IP telephone models:
  - 9610, 9620, 9630, 9640, and 9650 telephones with firmware 3.0 or later.
  - 96xx models that support Time to Service (TTS).
  - 4601+, 4602SW+, 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW Broadcom telephones with firmware R 2.9 SP1 or later provides the 46xx telephones. 46xx telephones are not in the same subnet as the servers.
  - J129, J139, J159, and J189

    All other IP telephone models re-register during server interchange. The 46xx telephones re-register if they are in the same subnet as the servers.
- When utilizing Processor Ethernet (PE) on duplicated servers, assign PE to an active server IP address shared between the servers.
- To check for the latest available versions of communication devices, go to the Avaya Support website at http://avaya.com/support and click **DOWNLOADS & DOCUMENTS**. Select the required product and check the available versions.

Survivable core server requirements

The requirements are as follows:

- The main server and each survivable core server must be running Communication Manager Release 8.1 or later.

  For more information about the supported servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*.
- The license file for the main server covers the survivable core server.

- An IP network that provides connectivity for all Media Gateways and servers.

Survivable core server failover examples

This section contains examples that are fabricated to illustrate survivable core server functionality. The examples illustrate LAN/WAN and server failures in different configurations.

Example one: Main servers fail

In example one (see Figure 1: S8300E, R640 Server with survivable core servers in normal operation), the duplicated server is acting as the main server in a survivable core server environment. Two survivable core servers have been positioned in the network. Through administration on the main server, another duplicated server is selected as the primary backup or 1st alternative to the main server. A third duplicated server pair is acting as a secondary backup or 2nd alternative in case the 1st alternative fails or there is WAN fragmentation. For example one, the intent of the survivable core server configuration is to keep all Media Gateways under the control of a single server.

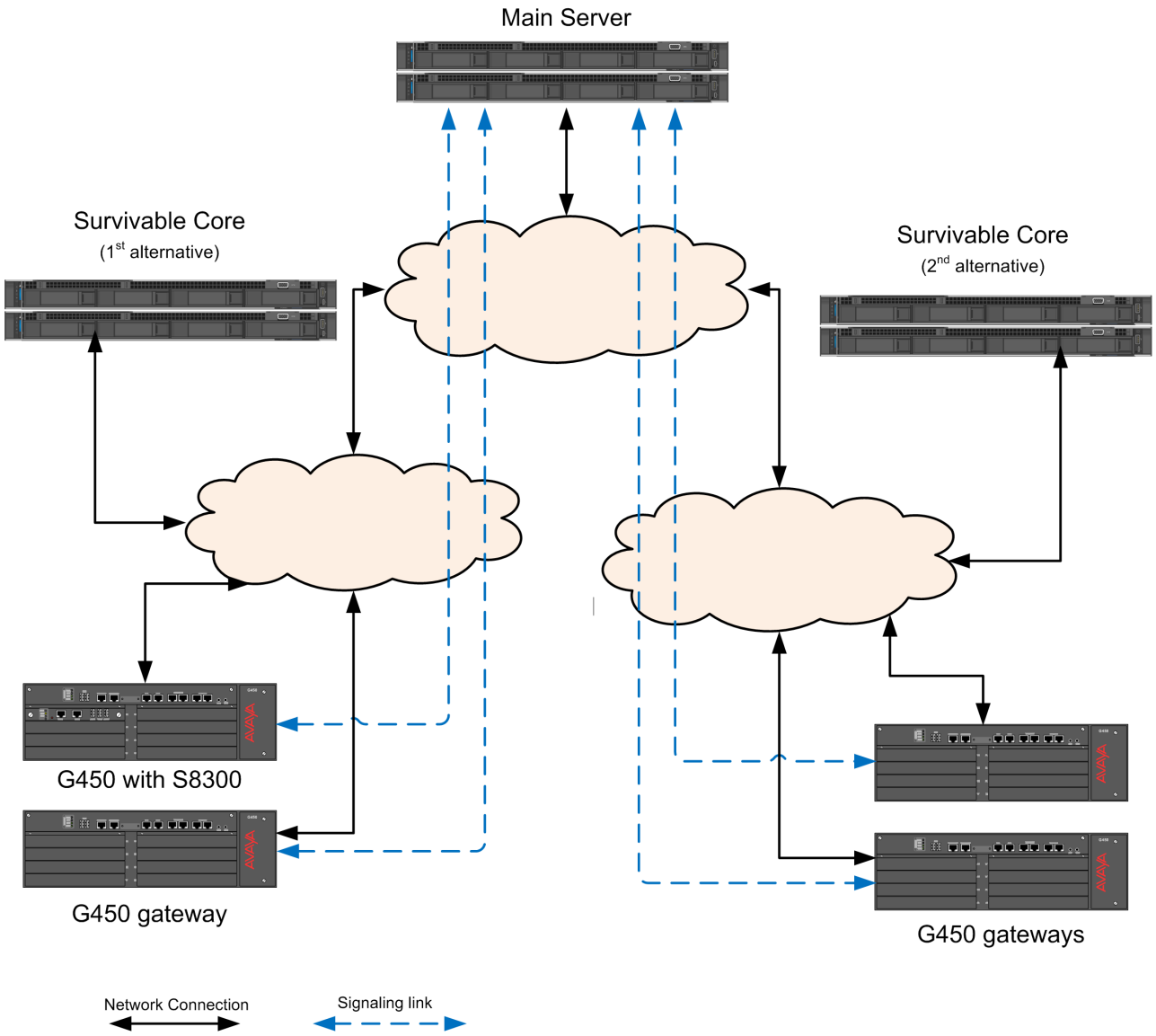

Figure 1: Servers with survivable core servers in normal operation

A catastrophic failure occurs on the main servers (see *Figure 2: Catastrophic main server failure*). The Media Gateway can no longer communicate with the main server. The primary search timer activates.

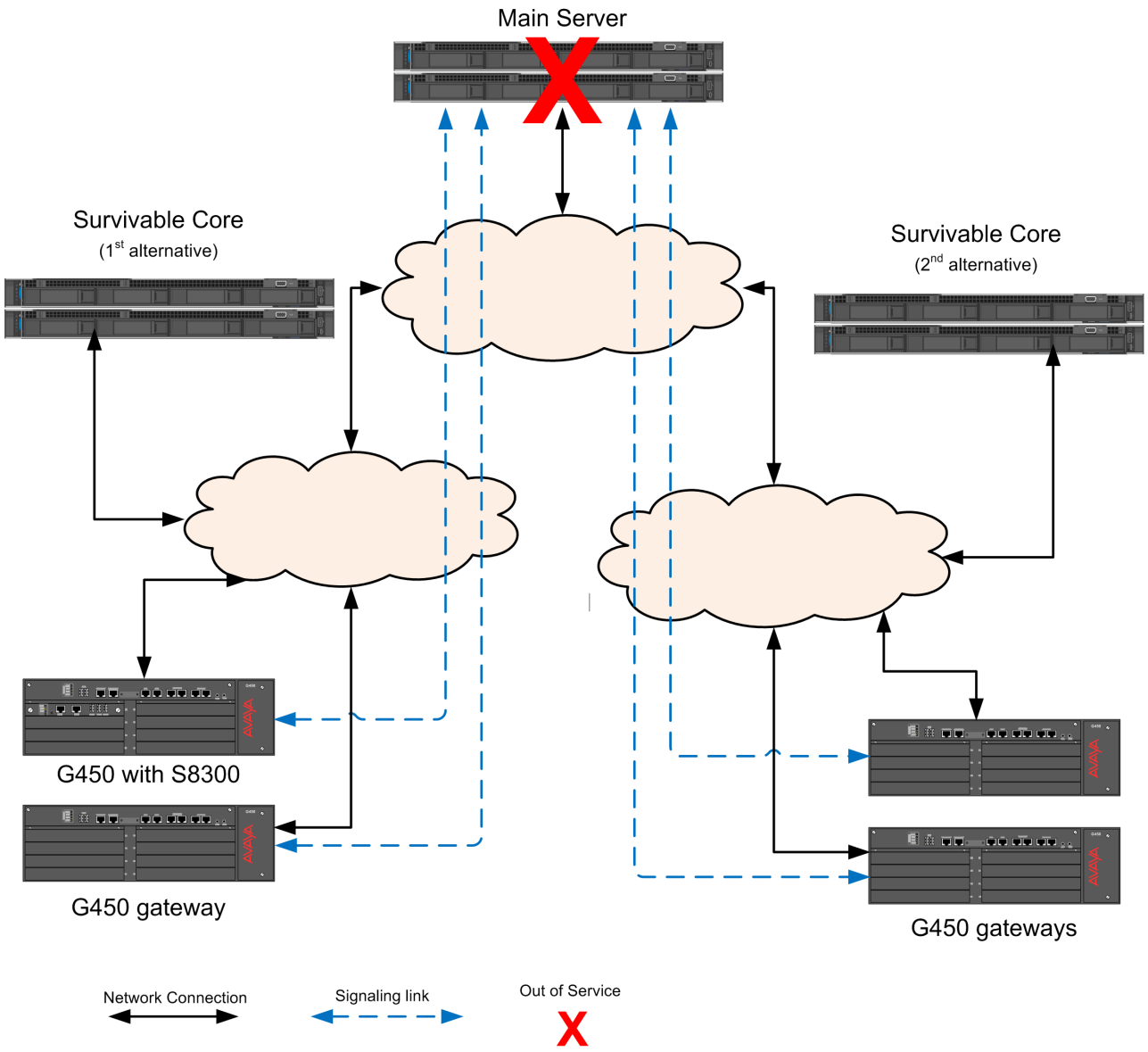

Figure 2: Catastrophic main server failure

The administered values of the survivable core servers are assigned to the Media Gateways in the 'mgc list' configuration, the order in the list defines the search order. Based on the values in the mgc list of the survivable core servers, the Media Gateway placed the 1st alternative survivable core server higher on its priority list then the 2nd alternative survivable core server.

When the primary search timer expires (see *Figure 3: main servers fail- survivable core server recovery of failure*), the Media Gateways request service from the highest survivable core server on its list (1st alternative). The 1st alternative survivable core server acknowledges the request and takes control of the Media Gateway.

The primary search timer is configured on the G4xx gateways CLI using the set reset-times primary-search. The default value is 1 minute and the configurable range is 1-59 minutes.

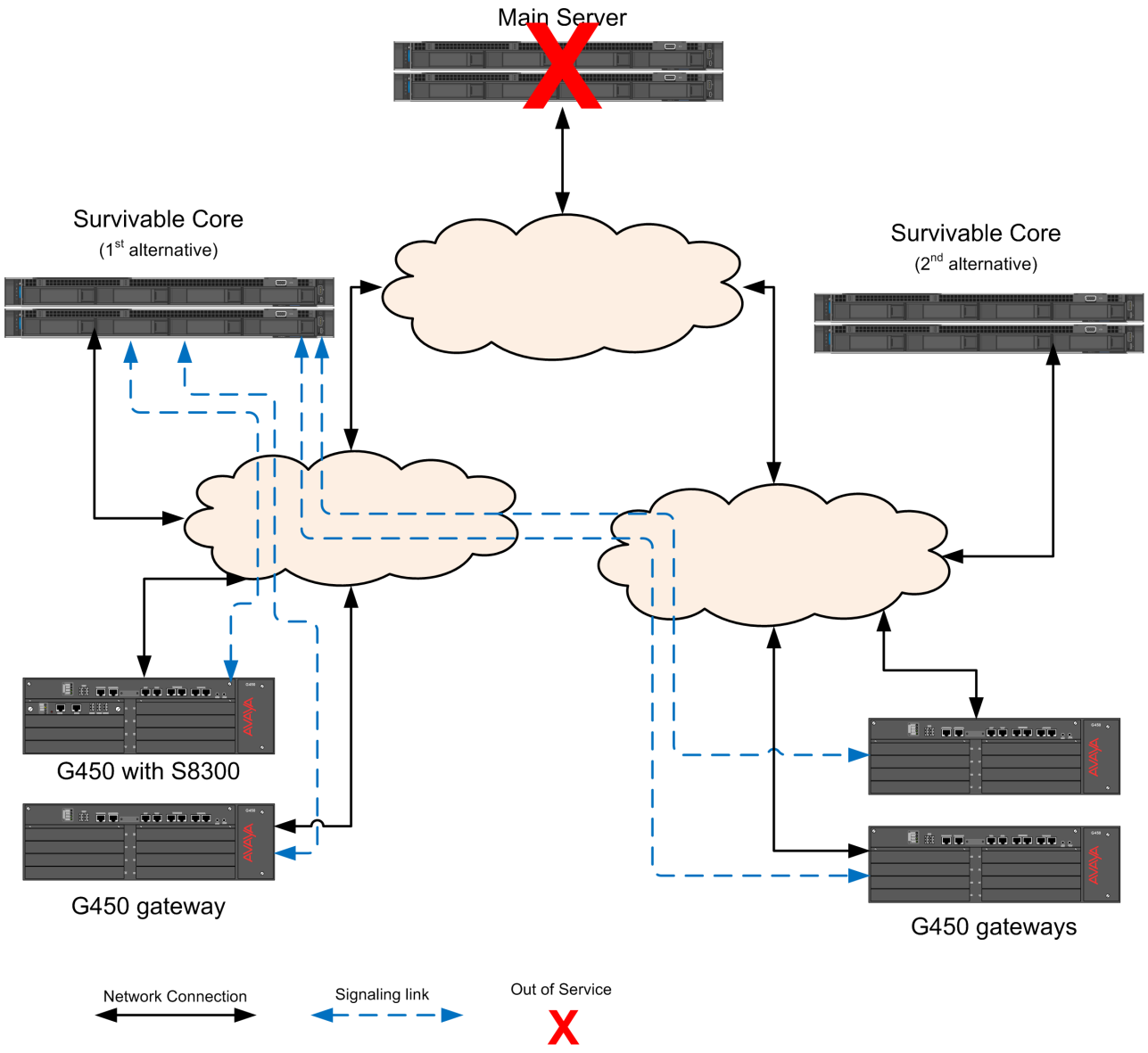

Figure 3: main servers fail- survivable core server recovery of failure

Example two: Network failure

Example two uses the same configuration used in example one. The S8300E Server is the main server, with two S8300E survivable core servers (first alternative and second alternative). Due to a catastrophic failure the main server is out-of-service. All Media Gateways are now controlled by the 1st alternative survivable core server.

Up to this point this is the same scenario as example one. Now, the customer experiences a network outage resulting in fragmentation of the network (see *Figure 4: Network fragmentation failure*). Media Gateways three and four can communicate with the second alternative survivable

core server but can no longer communicate with the main server or the first alternative survivable core server. Media Gateways one and two can still communicate with the first alternative survivable core server but can no longer communicate with the second alternative survivable core server.

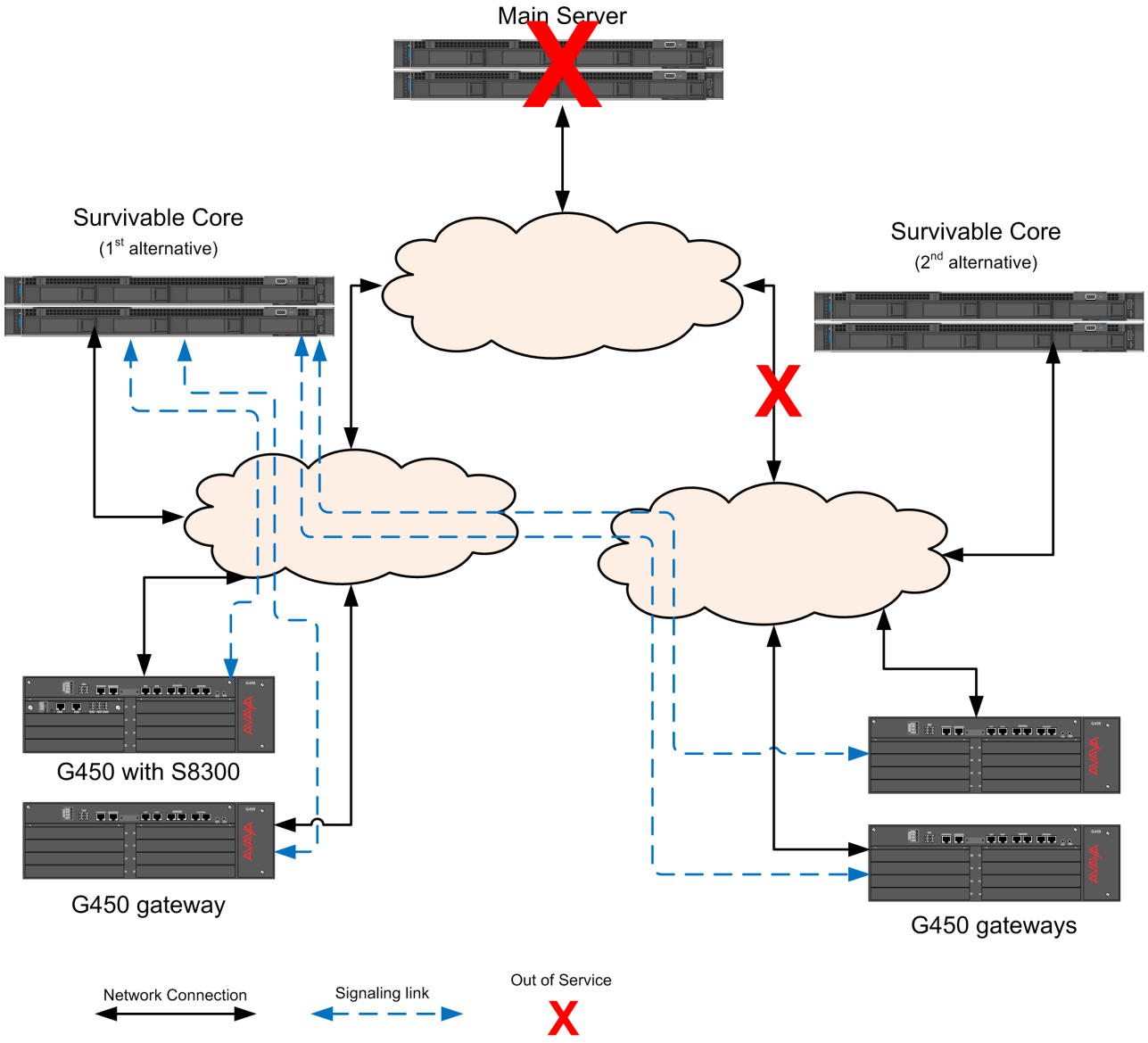

Figure 4: Network fragmentation failure

Because the Media Gateways three and four are no longer able to communicate with the main server or the 1st alternative server, they adjust their priority list and move the 2nd alternative server to the top of the list. The 2nd alternative server acknowledges the request and assumes control of gateways three and four (see *Figure 5: Network failure - Survivable core server recovery*). Note that Media Gateways one and two did not experience any service outage from the failure.

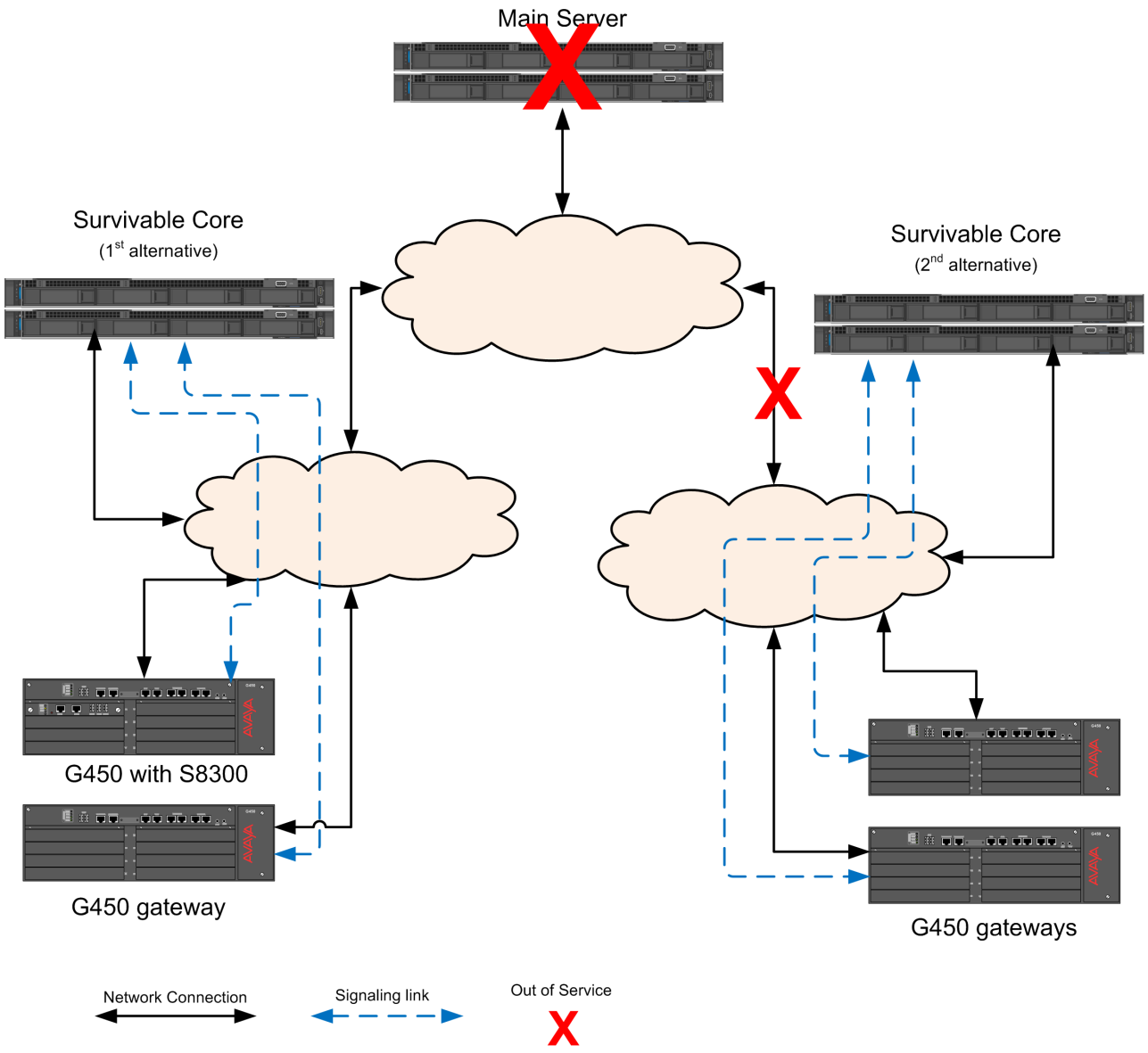

Figure 5: Network failure - Survivable core server recovery

The users in gateways one through four experience the following:

- During the primary search timer interval:
  - Stable calls remain up in the state they were in before the outage occurred. The stable calls do not have access to any features such as hold, conference, etc. The state of the stable call cannot be changed.
  - Users attempting to originate a telephone call, do not get dial tone.
  - Incoming calls to the system receive a fast busy (reorder tone) or an announcement from the facility provider saying all trunks are busy.

- After the primary search timer expires:
  - For the users on an IP connected telephone call, the shuffled IP calls stay up. Once the call terminates, the user of the IP telephone cannot make another call until the IP telephone re-registers with a gatekeeper.
  - Calls on DCP or analog telephones terminate.

The customer is now in the process of recovering from both the network failure and the main server failure (see *Figure 6: Network fragmentation recovery*). As the network failure is fixed, the Media Gateways three and four can now communicate with the first server. The gateways do not automatically return to the control of the first secondary server. The gateways always try to return to the main (primary) controller. The return to main is defined by the “recovery rule” configured for each gateway in the “add/change media-gateway” form. The return to main can be set for a certain time of day/day of week, when there are no calls in progress or can be configured to be immediate. The return to the primary can be also set to manual using ‘no rule’ in that case the gateways return to main only when the administrator issue an **`enable mg-return`** command.

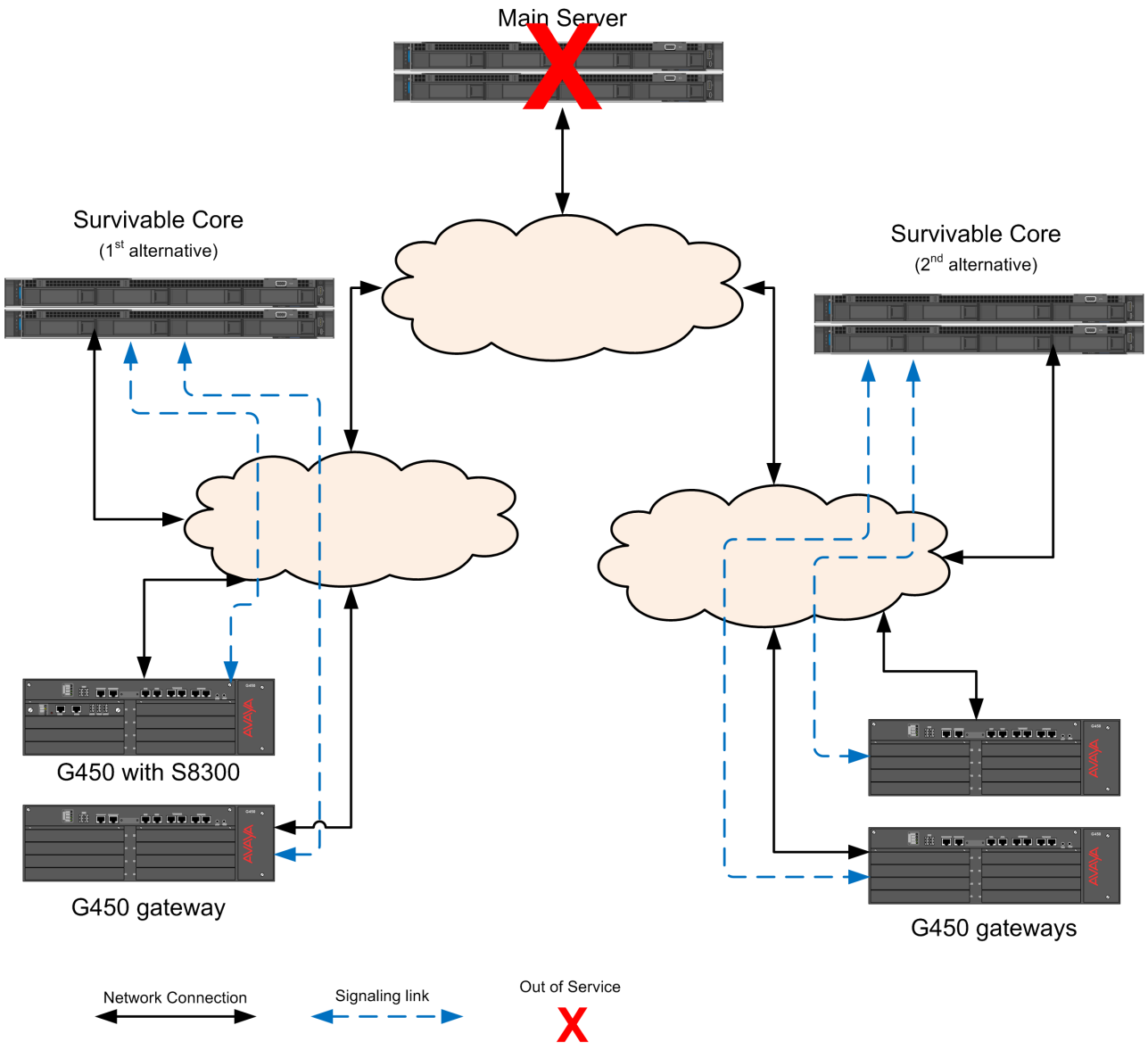

Figure 6: Network fragmentation recovery

The main server is now restored (see *Figure 7: Main server recovery*). The Media Gateways can now communicate with the main server and each survivable server. The main server is always the highest priority on any Media Gateway priority list.

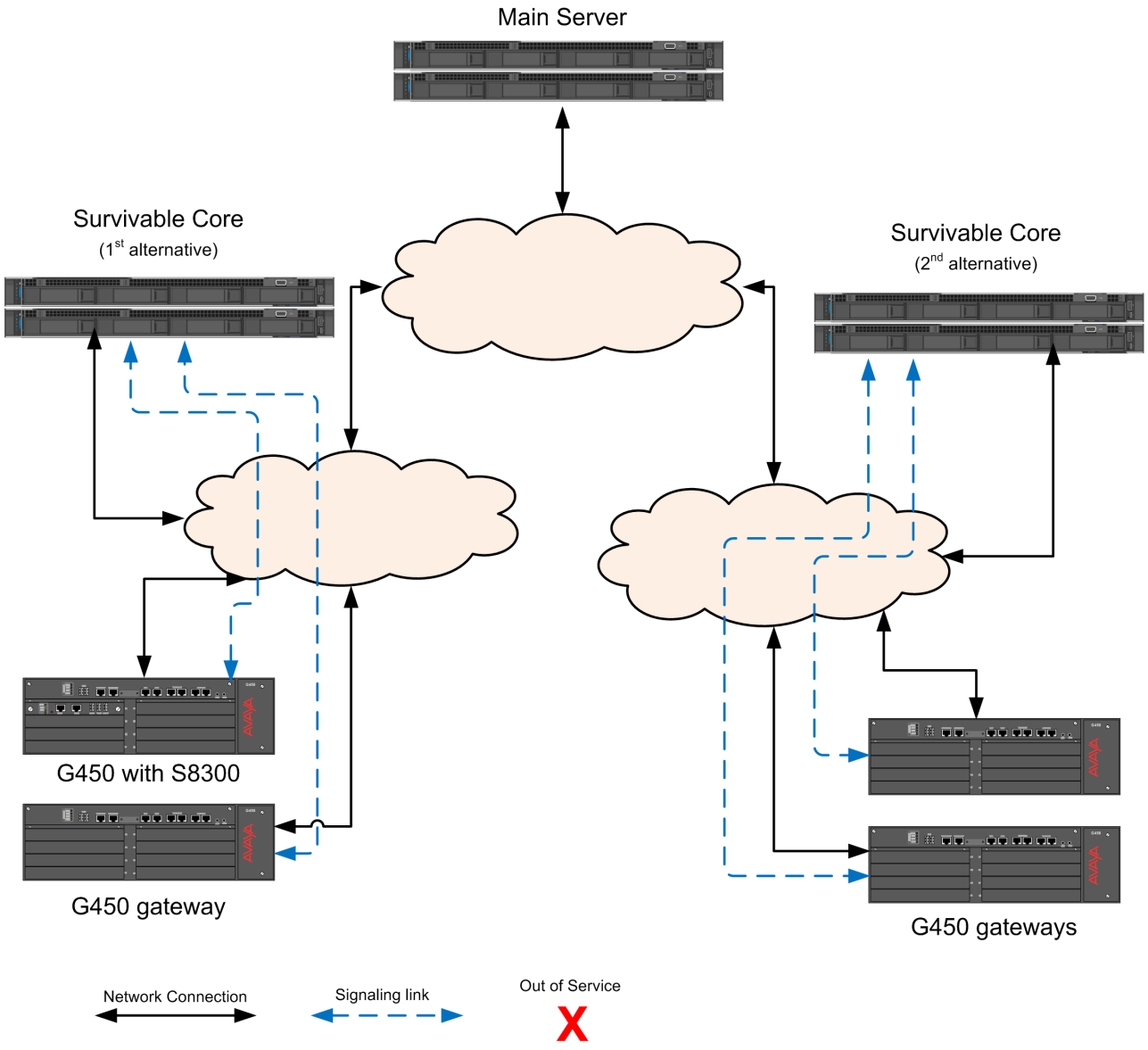

Figure 7: Main server recovery

The return to main is defined by the recovery rule configured for each gateway in the add/change media-gateway form. The return to main can be set for a certain time of day/day of week, when there are no calls in progress or can be configured to be immediate. The return to the primary can be also set to manual using no rule in that case the gateways return to main only when the administrator issue an **`enable mg-return`** command.

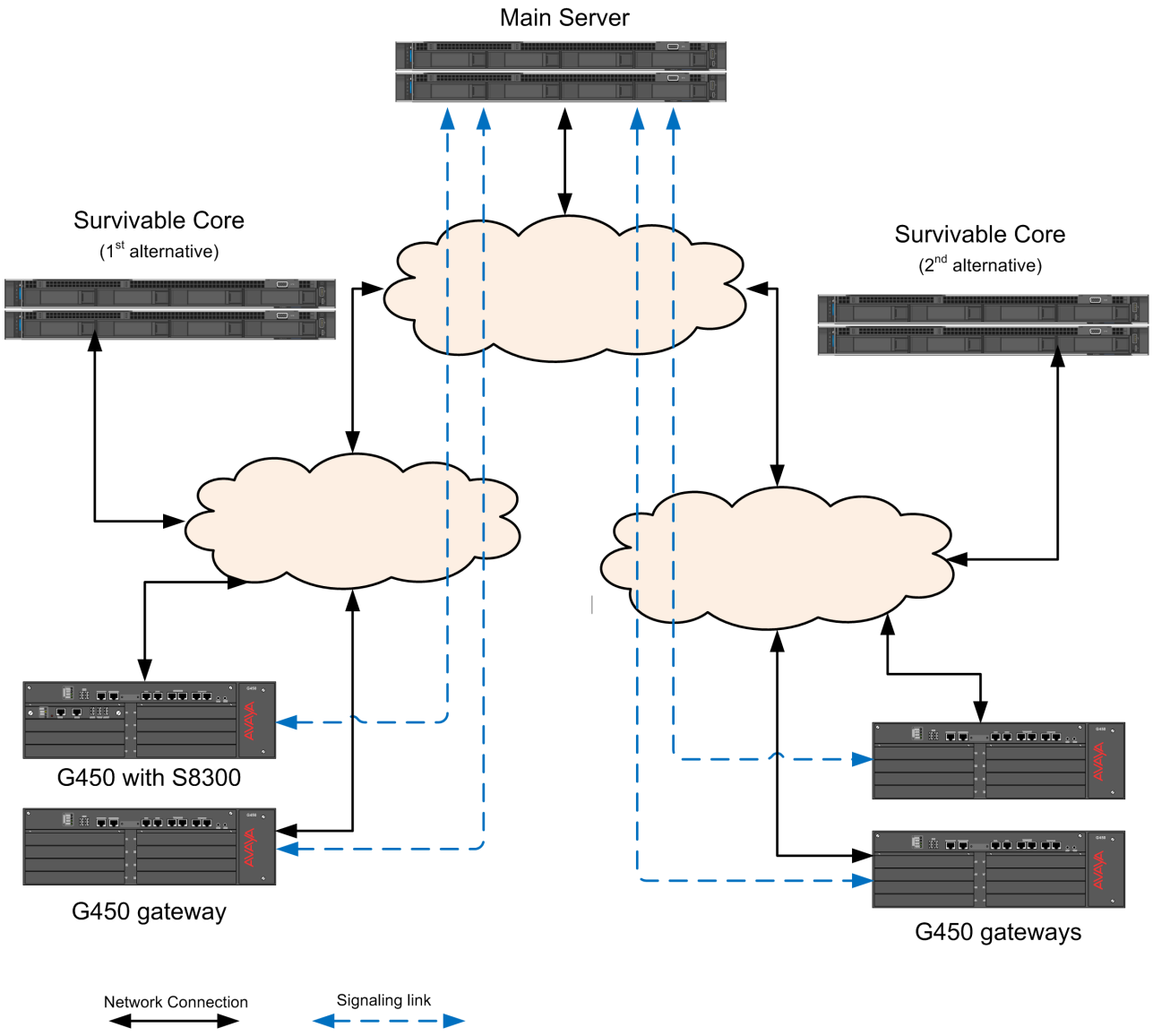

Figure 8: Survivable remote server working in a survivable core server environment - normal operation

Related links

[Checking the administration on the main server](#) on page 57
[Survivable core server administration](#) on page 52

Example three: A survivable remote server working in a survivable core server environment

Two survivable core servers are administered and the LSP in the S8300 is administered last in the secondary list in gateways 1 and 2. When the branch becomes isolated the gateways cannot connect to the primary server or the secondary core servers and therefore connect to the last

server in the list, the S8300 in the same branch, see *Figure 8: Survivable remote server working in a survivable core server environment - normal operation*.

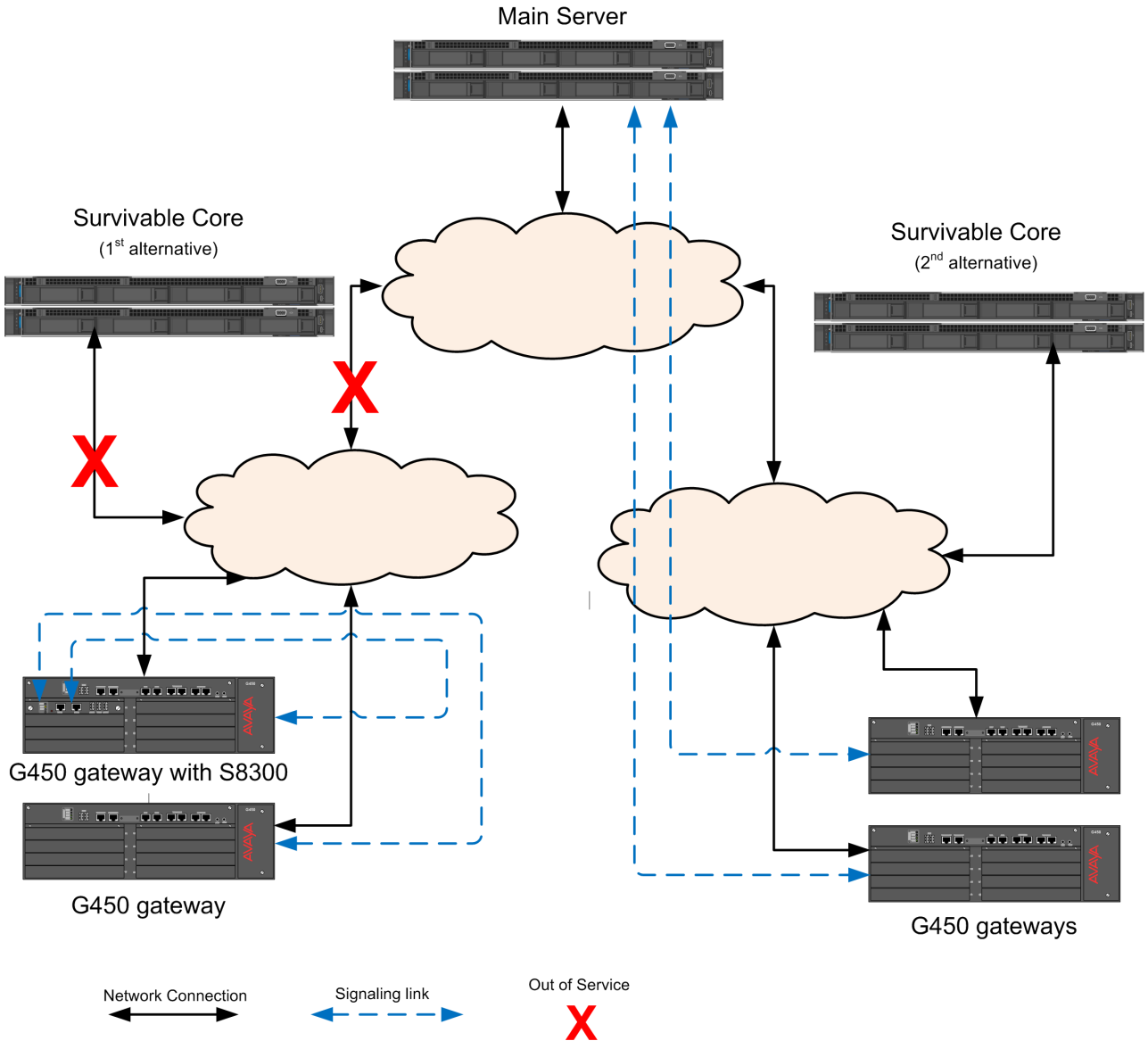

Figure 9: Survivable remote server working in a survivable core server environment - normal operation

The gateway has a Primary Search Timer, which is used when attempting to contact the main server. If the gateway loses its registration with the main server, it will attempt to re-register with the main server for that time. The default value is one minute but it can be administered to be as high as 30 minutes. If registration to main server is unsuccessful, the gateway will attempt to register with a server in the backup server portion of the Media Gateway Controller (MGC) list. The gateway will try each server in turn and, if there are no responses from any of the servers, gateway will go to the top of the MGC list and try each server in turn until a server responds.

The problem that caused the outage has been fixed (see *Figure 10: Survivable remote working in a survivable core environment - fall-back to the main server*).

If a media gateway recovery rule has been assigned, the media gateway will register with the main server when the recovery rules parameters have been met. If a recovery rule has not been assigned or if you want the gateway to immediately return, run the **`enable mg-return`** command. A manual reset of the gateway or the survivable remote server is not required.

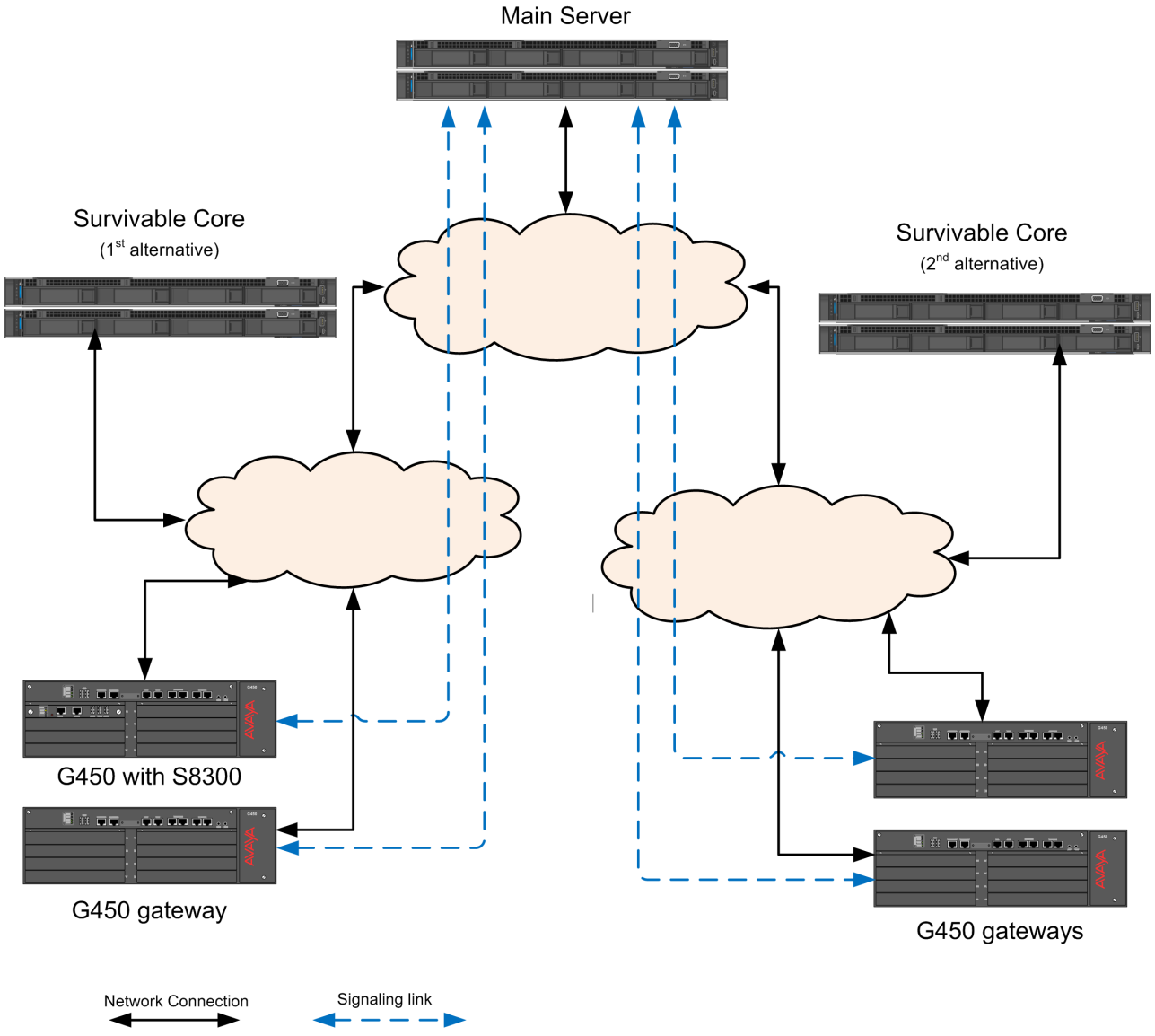

Figure 10: Survivable remote working in a survivable core environment - fall-back to the main server

Related links

[Feature considerations](#) on page 35
[Primary Search Timer](#) on page 35

Chapter 3: Survivable Core Server design and planning

This section describes the design strategies, terminologies, and various other aspects of survivable core server during the design and planning phase.

For more information on the supported server, see “Supported servers” section.

For more information about the process and procedures for upgrading Communication Manager , see *Upgrading Avaya Aura® Communication Manager*.

Survivable core server design strategy

During the design and planning phase of a survivable core server implementation, it is important to understand the goal of the customer for survivability, including prioritization. This is done by determining the strategy of Survivable core server support for the Media gateways in the system. Goals for deploying and administering the survivable core servers are:

- Avoiding fragmentation of the system: The survivable core server controls as much of the system as possible.
- Avoiding overload of network resources with excessive call traffic: Each survivable core server controls only limited portions of the system. Multiple survivable core servers may be needed to support the number of Media gateways. In this way, a survivable core server can potentially assume control of a single Media gateways or a group of Media gateways while the WAN traffic is unaffected or even reduced.

During the initial design and whenever additional capacity is added, the priorities listed above should be taken into account. Once a plan is developed to allow a survivable core server to take control of all or part of the configuration, priority parameters are administered for the survivable core server implementing the strategy.

After an overall strategy is selected, determine the placement of the survivable core servers in the network. Determine the administered values and communities for each survivable core server. For more information about administered values and communities, see *Survivable core server administration*.

Related links

Survivable core server administration on page 52

Survivable core server terminology

The following list contains terms that are used in a survivable core server environment. Become familiar with these terms before you plan, configure, and administer Survivable core server.

- Main server and survivable core server: The primary controller is referred to as the main server and the survivable server as a survivable core server.
- Cluster: You will see the term cluster in the SAT screens that are used for Survivable core server. A cluster can be either a simplex server or a duplex pair of servers. If the cluster is a pair of duplex servers you will see both servers referred to as one cluster. In some cases you will see both terms of survivable core server and cluster used in this book.
- Cluster Identifier (CLID): Each module receives a module identifier (MID) when a license file is created. The MID is referred to as the CLID in Survivable core server. A CLID uniquely identifies a single cluster so that each server in a duplex pair can have the same CLID.
- System Identifier (SID): Communication Manager has a default system ID of 1. You can configure the System ID on the Server Role page. The system ID is common across the main server and all survivable servers. Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form.
- Server Identifier (SVID): Each server in a survivable core server environment is administered with a unique SVID. That means each server in a duplex pair has a different SVID. You can number the servers sequentially or leave gaps in the numbering.
- Server Ordinal (SVOR): Each server in a survivable core server environment has a SVOR. The SVOR identifies the server within a cluster. The A-side server in a duplex pair always has ordinal one and the B-side server always has ordinal two. The SVOR is set automatically when the server is configured.
- IP-alias address: When Processor Ethernet is used on duplicated servers, it must be assigned to an IP address that is shared between the servers. This address is known in the industry as an IP-alias. The active server is the only server that will respond on the IP-alias address.

Survivable core server prerequisites

- You must gather the information in the *Survivable core server worksheet*.

  Note:

  For a more complete list of addresses, see *Survivable core server installation checklist*.

  The IP addresses in the worksheet are used when configuring the main server and each survivable core server. For more information on configuring and administering the main server and the survivable core server, see *Survivable core server administration*.
- Each survivable core server must share the license file of the main server. For security purposes, PLDS requires that each license file have a MAC address.

Related links

Survivable core server worksheet on page 30
Survivable core server installation checklist on page 41
Survivable core server administration on page 52

Survivable core server worksheet

Field	Value	Note
Main server IP address		
Survivable core servers IP address		
Default gateways IP address		
NIC cards IP address		
Subnet masks IP address		
Server ID		
Module Identification Number (MID)		

Server ID

The system administrator assigns a *unique* Server Identification number (SVID) to each server. The SVID must be in the range of one to 256. With duplicated servers, each server in a server pair requires a different SVID. Each SVID must be unique within the enterprise. The administrator can assign the SVID sequentially or allow gaps in the numbering such as 10, 20, 30, etc.

Module Identification Number (MID)

The Communication Manager main server has a default module ID of 1. You can configure the Module ID on the Server Role page. Each survivable server has a unique module ID of 2 or greater.

The module ID must be unique for the main server and all survivable servers. The MID is administered as the Cluster Identification Number (CLID) in the Survivable Processor screen.

Network port considerations

The main server, survivable remote servers, and each survivable core server use specific ports across a customer's network for registration and translation distribution. You can modify the firewall settings from the command line using the **`firewall`** command with *suser* level access.

Note:

Use ports 80 and 443 to access the System Management Interface (SMI). Use the port 5022 for the secured System Access Terminal (SAT).

Use the information in the following table to determine the ports that must be open in the customer's network in a survivable core server environment.

Table 3: Open ports

Port	Used by	Description
22	ssh/sftp	
68	DHCP	
514	This port is used in Communication Manager 1.3 to download translations.	
1719 (UDP port)	The survivable core server to register to the main server.	A survivable core server registers with the main server using port 1719.
1024 and above	Processor Ethernet	TCP outgoing
1039	PTLS encrypted H.248	
2944	H.248 over TLS	
2945	H.248 over TCP	
5000 to 9999	Processor Ethernet	TCP incoming
21874 (TCP port)	The main server to download translations to the survivable core server.	A main server uses port 21874 to download translations to the survivable core server and the survivable remote server(s).

Related links

C-LAN access for survivable core server registration

Main server and survivable core server differences

For the most part, capabilities of the main server and the survivable core server are the same if both are of the same platform type. There are some important differences between the main server and the survivable core server that should be taken into consideration when planning and designing a survivable core server configuration:

- License file: The license file of the main server must have ESS Administration enabled and Enterprise Survivable Server disabled.
- Translations: You can change translations on a survivable core server but you cannot save them. A file sync from the main server to the survivable core server will over-write translations performed on the survivable core server.
- Administrative value: The value of the main server is always the highest ranking value on an Media Gateway's priority list. The value for the main server cannot be administered. However, the value of each survivable core server is administrable. For more information on administration, see *Survivable core server administration*.
- Survivable core server capacity: When used as a survivable core server, the survivable server match the capacity of the main server that is used as a main server.

For more information about system capacities, see *Avaya Aura® Communication Manager System Capacities Table* .

- Processor Ethernet: Processor Ethernet can be used on both the simplex main server and the simplex survivable core server. On the simplex main server the Processor Ethernet interface can be used for adjunct connectivity, H.323 endpoint registration, and gateway registration. The Processor Ethernet interface can be used for support of H.323 devices and gateways and adjunct connectivity if you administer relevant fields on the Survivable Processor screen.

  For more information on how the Processor Ethernet functionality works on main servers and survivable core servers, see *Processor Ethernet functionality*.

Related links

Survivable core server administration on page 52
Processor Ethernet functionality on page 14

Trunking considerations

Use this section to understand trunking considerations in a survivable core server environment.

ISDN PRI non facility associated signaling

Customers can have up to 479 B channels with one D channel. In North America a backup D channel is offered. The backup D channel is located on channel 24 of a second DS1 interface. While both DS1 interfaces are connected to the same Central Office, only one is used for signaling at a time.

In the event of a failover, if a different survivable core server controls the primary and the backup D channels, each survivable core server will think the D channel it does not control is out of service and will try to bring the D channel that it controls into service. The Service Provider will only use one of the D channels for signaling. When the D channel is not in service, the associated B channels of the DS1 will be out of service.

Guidelines for using ISDN PRI non facility associated signaling

Use the following guidelines when using ISDN PRI non facility associated signaling in a survivable core server environment.

- Whenever possible place both D-channels in one media gateway.
- If it is not possible to place both D-channels in one media gateway, place the D-channels within media gateways where:
- The media gateways are most likely to failover to the same survivable core server.
- Enable “Force Phones and Gateways to Active Survivable Servers?” feature on “change system-parameters ip-options” screen.

E911

An E-911 call or other emergency call handling can only be routed if the trunk facility is under the control of the same survivable core server as the person originating the call.

Inter-Gateway Alternate Routing

Inter-Gateway Alternate Routing (IGAR) provides an alternate inter-region routing mechanism that is used when the IP network cannot, or should not, carry bearer. IGAR preserves the internal makeup of a call, so the call's use of non-IP bearer facilities is transparent to the end user. IGAR can be triggered by Call Access Control via Bandwidth Limitation (CAC-BL), or can be forced to use an alternate route. IGAR can use Public Switched Telephone Network (PSTN) facilities, or private switched facilities to carry the inter-region audio bearer.

After failover, if a survivable core server controls media gateways or gateways in one or more network regions where IGAR is administered, IGAR continues to work. However, if media gateways or gateways across different network regions are controlled by separate survivable core servers, calls between these systems are not seen as internal calls and therefore, IGAR does not apply.

For example, a survivable core server customer with eight media gateways administers each media gateway in a separate network region (one through eight). IGAR is administered between all eight regions. A network fragmentation failure occurs. Media gateways one through four failover to survivable core server one. Media gateways five through eight failover to Local Only survivable core servers. survivable core server one uses IGAR to establish inter-media gateway bearer between media gateways one through four. Each Local Only survivable core server controls one media gateway (five through eight). IGAR does not apply for the Local Only servers.

Personal Central Office Line

A Personal Central Office Line (PCOL) consists of a Central Office trunk that terminates on a telephone or in a PCOL group shared by a number of telephones. During a failover, PCOL calls can only be handled if the trunk and the station administered with it are under control of the same survivable core server.

Separation of Bearer and Signaling

Separation of Bearer and Signaling (SBS) provides a low-cost, virtual private network over IP trunks. During a failover, SBS calls will fail unless the C-LAN for the signaling call and the bearer trunks are under the control of the same survivable core server. Alternate routes may be used if under the control of the same survivable core server as the originator.

Data Networking

In an Avaya solution, IP connectivity is required for call control between simplex or duplex Servers. There can be a single call control connection or duplicated call control connections on a public or private network.

For more information about control networks, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

H.323 considerations when using survivable core server

Because H.323 trunk usage can exhaust memory pool and can prevent H.323 stations from registering, Communication Manager 6.0 and later provides a way to control where H.323 trunks are used. When the **Group Type** field is `h.323` and **Near-end Node Name** is `procr` on the Signaling Group screen, an additional page, Limit Signaling Group Usage, is added to allow control of H.323 trunk usage.

```
change signaling-group 3                                        Page   2 of   6
                        LIMIT SIGNALING GROUP USAGE
                        Enable on the main Processor(s)? y
          Enable on Survivable Processors (ESS and LSP): selected
                             Selected Survivable Processor Node Names
                              1:
                              2:
                              3:
                              4:
                              5:
                              6:
                              7:
                              8:
```

To allow usage of H.323 trunks only on the main server, set **Enable on the main Processor(s)** to `y`.

To specify usage of H.323 trunks on survivable core and remote servers, set **Enable on Survivable Processors (ESS and LSP)** to `all`, `ess-all`, `none`, or `selected` as per your network requirements. The **Selected Survivable Processor Node Name** field appears only if you enter `selected` in the **Enable on Survivable Processors (ESS and LSP)** field.

Timing considerations

Depending on your configuration, there are a number of timers that are used during a failover. After the failover, conflict with the timers may produce a configuration that you did not want or anticipate.

Primary Search Timer

For information about primary search timer, see *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Feature limitations during gateway outage

Since there is no communication possible between the gateway and the IP endpoint during a link outage, button depressions are not recognized, feature access codes do not work, and any other types of call handling ceases. In essence, the server cannot react to any stimuli until the H.323 signaling link is restored.

Feature considerations

Depending on the reason for the failure, some Communication Manager features may not work as administered. If the failure is on the main server but the network is still intact, you may not see any changes to features, such as call forwarding, hunt groups, and call coverage. If the network fragments, the same features may or may not work as intended.

Note:

Features may act differently depending on the release of Communication Manager.

This section highlights how a failover would affect the Communication Manager features.

Announcements

Announcements are available to callers when the announcement is under the control of the survivable core server.

Attendant Console

When a Media Gateway fails-over to a survivable core server any attendant console in that media gateway will come into service in the Night Service mode. Calls can be taken from the attendant console after the console is taken out of Night Service. Only the trunks under the control of the servicing survivable core server will be affected by the deactivation of the Night Service mode. The survivable core server assumes that any console that it cannot control is out of service.

Best Service Routing

Best Service routing polling works if the facility used for routing the polling call is under the control of that survivable core server.

Call Classification

Call Classification works only if there are one or more Call Classification resources under the control of the survivable core server.

Call Coverage

Calls may follow a call coverage path only if the route is under the control of the same survivable core server. If the covered party is not under the control of the survivable core server, the covering call will go immediately to coverage.

Call Vectoring

Routing a call using Call Vectoring is successful only if the route-to-endpoints are under the control of the survivable core server. This is true whether the endpoint is another station, adjunct, or route in a routing pattern.

Centralized Attendant Service

For a Centralized Attendant Service (CAS), main system calls from a branch will be processed if the Media Gateways under the control of the survivable core server contain the incoming trunks and attendant consoles.

For a CAS Branch, calls are routed as if Night Service mode was activated. Calls are routed only if the trunks to the CAS Main are under control of the survivable core server controlling the media gateway where attendant seeking calls arrive for service.

Crisis Alert

Crisis alerting calls can only be routed to endpoints under the control of the survivable core server that controls the originator.

CVLAN links

The survivable core server will only have access to CVLAN links in Media Gateways under its control.

Dial Plan Transparency

The Dial Plan Transparency feature preserves dialing patterns of users when a gateway registers with a Survivable Remote Server (SRS) or Media Gateway and requests service from a Survivable Core Server (SCS).

When a gateway registers with a Survivable Remote Server, the Dial Plan Transparency feature routes calls over the Public Switched Telephone Network (PSTN) to connect endpoints that no longer connect over the corporate IP network.

Dial Plan Transparency does not work when two gateways are in the same network region.

For more information about administering Dial Plan Transparency, see:

- *Avaya Aura® Communication Manager Feature Description and Implementation*
- *Administering Network Connectivity on Avaya Aura® Communication Manager*
- *Administering Avaya Aura® Communication Manager*

Facility Busy Indication

Facility Busy Indicators can only track the endpoints that are under the control of the same survivable core server as the endpoint with the facility busy indicator button or display.

Hunt Groups

Hunt Group calls can be directed to hunt group members in the Media Gateways under the control of that survivable core server.

Leave Word Calling

When a survivable core server takes control of a Media Gateway, all previous Leave Word Calling messages are lost. The same is true when control is returned to the main server.

Music on Hold

The survivable core server can provide Music on Hold only if the music source is in control of the survivable core server. Calls to a survivable core server without a music source hear silence.

Adjunct considerations

When a failover occurs, a survivable core server may or may not have connectivity to various adjuncts.

This section highlights how a failover would affect the following adjuncts:

- Call Detail Recording
- Call Management System
- Extension to Cellular
- Property Management System
- Voice Mail
- Voice Response System

Note:

You can connect three adjuncts to the Processor Ethernet interface of a survivable remote server or an simplex survivable core server. The three adjuncts are Call Management System

(CMS), Call Detail Recording (CDR), and Application Enablement Services (AE Services). You can connect the CDR, CMS, and Messaging adjuncts to the Processor Ethernet interface of a duplex server. For more information on the Processor Ethernet interface, see *Processor Ethernet overview*.

Related links

[Processor Ethernet overview](#) on page 13
[Call Management System](#) on page 39
[Extension to Cellular](#) on page 39
[Property Management System](#) on page 39
[Voice Mail](#) on page 40
[Voice Response System](#) on page 40

Call Detail Recording

Traditional Call Detail Recording

A Call Detail Recording (CDR) unit can connect to a survivable core server through the server's Processor Ethernet interface. The Processor Ethernet interface for each CDR is specified in translations. In the event a failure and fragmentation occurs, call details for completed calls are collected. The server with Processor Ethernet or the server controlling one through which the CDR data is sent, will attempt to deliver the records to the CDR output device. If the network is intact to the device, the call records will be delivered. If the server knows that the CDR device is not connected, it will store the records in a buffer. When the system restores and the main server can once again communicate with the CDR device, any records buffered by the main server will download to the CDR output link. Other records that were not delivered to the CDR adjuncts and buffered in a survivable core server will be unrecoverable, as the survivable core server will perform a restart.

Survivable CDR

The Survivable CDR feature is used to store CDR records to a server's hard disk. For survivable core and remote servers, the Survivable CDR feature is used to store the CDR records generated from calls that occur when a survivable remote server or survivable core server is controlling one or more gateways or media gateways. For a man server, the Survivable CDR feature provides the ability to store CDR records on the server's hard disk.

When the Survivable CDR feature is enabled, the CDR records are saved in a special directory named /var/home/ftp/CDR on the server's hard disk. The CDR adjunct retrieves the Survivable CDR data files by logging into the server and copying the files to its own storage device. The CDR adjunct uses a special login that is restricted to only accessing the directory where the CDR records are stored. After all the files are successfully copied, the CDR adjunct deletes the files from the server's hard disk and processes the CDR records in the same manner that it does today.

Note:

This feature is available on main servers and survivable core servers that are Communication Manager Releases 5.0 and later only. The feature is available on survivable remote server platforms running Communication Manager 4.0 and later.

The CDR adjunct must poll each main, survivable remote server, and survivable core server regularly to see if there are any new data files to be collected. This is required even when a survivable remote server or survivable core server is not controlling a gateway because the CDR adjunct has no way of knowing if a survivable remote server or survivable core server is active.

The Survivable CDR feature uses the same CDR data file formats that are available with legacy CDR.

For more information about Survivable CDR, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Call Management System

Call Management System (CMS) connects to the server through the servers Processor Ethernet (PE) interface. During server failover, a survivable core server communicates with CMS through the PE interface of the survivable core server. Here, the survivable core server sends the events to Call Management System. When the control network fails, CMS fails, resulting in the data loss.

Important:

An explanation of how the survivable core server and the survivable remote server interact with CMS does not apply to the High Availability (HA) offer. Using HA, CMS configuration for a survivable core server or a survivable remote server involves specific constraints and limitations.

To understand the limitations, contact Avaya Communication Solutions and Integration (CSI) at http://csi.avaya.com.

Extension to Cellular

Extension to Cellular users will have access to the Extension to Cellular service only if their endpoint is also under the control of the same survivable core server that controls the Extension to Cellular.

Property Management System

Property Management System (PMS) interfaces to the server through a Procr. If the network is fragments, only Procr, under control of a survivable core server, will be able to pass entered or event data to the PMS.

Voice Mail

In the event of a failover, the survivable core server will only be able to deliver covered and diverted called parties to voice messaging systems that are connected to the same controlled system segment as the calling party.

A user of a voice mail system will only get a message waiting indication if their messaging server is in the same controlled segment as their station. The only way a voice mail user will be able to retrieve messages is through a dial connection or tool, such as Message Manager, to connect to the voice mail system.

Voice Response System

The voice response system is connected by ports to a Media Gateway. The Media Gateway is under the control of the main server. In the event of a failure resulting in a fragmented system, the voice response system will be able to execute any instructions that can be handled by call processing in the Media Gateway under the control of the same server. Other requests will be denied.

Chapter 4: Survivable Core Server installation

The survivable core server installation includes the following:

- Survivable core server installation checklist
- Survivable core server license files
- Server configuration worksheet
- Survivable core server administration
- Translations

Because Communication Manager Release 8.1 require replacing the existing server with the supported server, these servers require a hardware upgrade as part of the process. For more information about the supported servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Caution:

A survivable core server and the main server must be running compatible Communication Manager software loads. Before starting a survivable core server installation, check the compatibility of the software loads using the *Latest Communication Manager Software & Firmware Compatibility Matrix*. The matrix can be found in the download section at http://support.avaya.com.

Survivable core server installation checklist

This section provides a checklist for two types of survivable core server installations:

- Installing a survivable core server with existing servers
- Installing a survivable core server with new servers

Installing a survivable core server

About this task

A Survivable core server installation requires the following high-level steps.

Procedure

1. Design the system, and determine the survivable core server administration factors. For more information about how to design and plan the system, see Survivable Core Server design and planning on page 28.
2. Install or upgrade Communication Manager on each survivable core server.
   a. Start and stop the server.
   b. Configure the server. (Server configuration worksheets on page 50)
3. Install or upgrade Communication Manager on the main server.
   a. Install the license and authentication file. (Survivable core server license files on page 47)
   b. Restart the server.
   c. Configure the server. (Server configuration worksheets on page 50)
4. Administer survivable core server. (Survivable core server administration on page 52)
5. Verify that the survivable core servers can register to the main server. (Checking the administration on the main server on page 57)
6. Perform acceptance testing. (Survivable core server acceptance testing on page 78)

Checklist for installing survivable core server with existing server

Use the information in the following as a reference when installing survivable core server with existing servers.

	Task	Information	Documentation
#	General preparation		
1.	Obtain license and authentication files for all servers in the network.	Obtain a PLDS license and an authentication file for the main server.	License and authentication files are generated using PLDS.
	Survivable core servers		
4.	Upgrade each server to later version of Communication Manager.	All survivable core servers must be upgraded to the current release of Communication Manager before upgrading the main server.	For instructions on how to upgrade a server to a Communication Manager Release 5.2 or later, see *Upgrading Avaya Aura® Communication Manager*.
5.	Configure the survivable core server.	Use the server System Management Interface to configure the server	

Table continues…

	Task	Information	Documentation
6.	Restart the server.	Verify that the survivable core server administration feature is turned on.	To verify that the survivable core server Administration and Enterprise Survivable Server feature is turned on, see Checking the license file on page 49.
7.	Attach the survivable core server to the network and verify communication with the customer's LAN interface.	The IP address of the Procr that you entered when configuring the survivable core server is used when the survivable core server registers with the main server for the first time and it may be used for subsequent registrations. On the survivable core server, run the **ping** command with the IP address of the Procr.	
8.	Verify the communication to the main server over the IP network.	On the survivable core server, use the **ping** command with the IP address of the main server.	
	Main Server		
9.	Upgrade the server.	Upgrade the main server to later version of Communication Manager. A main server should never run a release of Communication Manager that is later than that of the survivable core server. If the existing server is running an earlier release of Communication Manager, upgrade to the latest version.	To use the standard process to upgrade the main server to Communication Manager, see *Upgrading Avaya Aura® Communication Manager*.
10.	Configure the main server.	Use the System Management Interface of the server to configure the main server.	To configure a server for Survivable core server that is already running Communication Manager Release 5.2 or later, see Converting the existing survivable core server to main server on page 62.
11.	Restart the server.	Verify that the survivable core server administration feature is turned on.	To verify that the survivable core server Administration feature is turned on, see Checking the license file on page 49.

Table continues…

	Task	Information	Documentation
12.	Verify open ports in the customer's network.	Certain ports must be open for survivable core server to work properly.	To obtain a list of ports that must be open for survivable core server, see Network port considerations on page 30.
13.	Verify LAN/WAN connectivity.	For each of the survivable core servers, run the **ping** command on the main server with the IP address of the survivable core server.	
14.	Administer Survivable core server.	On the main server, administer each survivable core server, media gateway communities, and no service timer.	To administer the main server see Survivable core server administration on page 52.
15.	Verify that each survivable core server registers with the main server.	Use the **status ess clusters** command to verify survivable core server registration. A configured survivable core server automatically registers with the main server when the survivable core server administration completes. After registration, the survivable core server receives a translation download from the main server. The survivable core server resets to load the translations and then re-registers with the main server.	For more information on the **status ess clusters** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.
16.	Distribute the translations to the survivable core servers.	To synchronize translations between the main and newly added survivable core server for the first time, run the **save translations all** or the **save translations ess** command.	For more information, see Translations on page 59.
17.	Acceptance testing.	Test the survivable core server configuration.	For more information on testing a survivable core server configuration, see Survivable core server acceptance testing on page 78.

Checklist for installing survivable core server with new servers

Use the information in the following table as a reference when installing survivable sore server with new servers.

	Task	Information	Documentation
1.	Main servers: Obtain the PLDS license and the authentication files.	Obtain PLDS license files and authentication files for the main server. A MAC address for the main server is needed for the license file.	License files are generated using PLDS.
3.	Survivable Core Server: Install the hardware, , and load Communication Manager.	.	To install the server hardware, see the supported server documentation. To install the IP connectivity hardware, see Adding New Hardware for Avaya Servers and Gateways.
4.	Survivable Core Server: Configure the survivable core server.	**Note:** You must set the time of the survivable core server to the same time zone as the main server even if the survivable core server is physically located in a different time zone.	For more information on the Configure ESS window, see Server configuration worksheets on page 50.
5.	Survivable Core Server: Install the license.	Only a license file with a MID of 1 (m1) should be loaded on a main server. Only a license file with a MID greater than 1 (m2 or greater) should be loaded on a survivable core server.	To verify that the survivable core server Administration and Enterprise Survivable Server feature is turned on, see Survivable core server license files on page 47.
6.	Survivable Core Server: Verify that the survivable core server can communicate with the customer's LAN interface.	An IP address of a Procr was entered when you configured the survivable core server. The Procr is used when the survivable core server registers with the main server for the first time and may be used for subsequent registrations. On the survivable core server, use the **`ping`** command followed by the IP address of the Procr or Processor Ethernet.	

Table continues…

	Task	Information	Documentation
7.	Survivable Core Server: Verify that the survivable core server can communicate with the main server over the IP network.	On the survivable core server, use the **ping** command followed by the IP address of the main server.	
8.	Main server: Install the hardware, System Platform, and install Communication Manager.	In a survivable core server environment, you must use static IP addresses for the Media Gateways in the configuration.	To install the server hardware, see the supported server documentation.
9.	Main server: Install the license and authentication file.	Verify that the survivable core server Administration feature is turned on.	To verify that the survivable core server Administration feature is turned on, see Checking the license file on page 49.
10.	Main server: Verify LAN/WAN connectivity.	On the main server, use the **ping** command followed by the IP address of the survivable core server for each of the survivable core servers.	
11.	Main server: Verify open ports in customer's network.	Certain ports must be open for survivable core server to work properly.	To obtain a list of ports that must be open for survivable core server, see Network port considerations on page 30.
12.	Main server: Administer Survivable Core Server.		To administer Survivable Core Server on the main server, see Survivable core server administration on page 52.
13.	Main server: Verify survivable core server registration.	Use the **status ess clusters** command to verify survivable core server registration with the main server.	For more information on the **status ess clusters** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.
14.	Acceptance testing	Test the survivable core server configuration.	For more information on how to test a configuration, see Survivable core server acceptance testing on page 78.
15.	Main server: Distribute the translations to the survivable core server.	To synchronize translations between the main and the survivable core server, run the **save translations all** or the **save translations ess** command.	For more information on the **save translations** command, see Translations on page 59.

Survivable core server license files

This section provides information on PLDS license files for survivable core servers. It does not contain information on how to load a license file on an Avaya server. For license file installation, refer to the installation documentation of the product you are installing.

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager Release 6.0 and later. PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.

License file for survivable servers

Install the license file on the Communication Manager main server. Survivable servers do not require a license file.

The license file on the Communication Manager main server controls licensing for survivable servers. The Maximum Survivable Processors (VALUE_CM_SP) feature in the license file specifies the number of survivable servers you can administer on the Communication Manager main server. This number comes from the number of maximum Enterprise Survivable Server (ESS) stations (VALUE_CM_ESS_STA) and maximum Local Survivable Server (LSP) stations (VALUE_CM_LSP_STA) activated in the license file. Each survivable server administered on the main server consumes one of the Maximum Survivable Processors feature capacities.

Station licenses for survivable servers

Station licenses for Communication Manager Enterprise Edition include station licenses for survivable servers.

Note:

The Communication Manager interfaces and license file refer to Survivable Core Servers as Enterprise Survivable Servers (ESSs) and refer to Survivable Remote Servers as Local Survivable Processors (LSPs).

Standard Edition customers must purchase a sufficient number of survivable server station licenses to cover the number of stations that will be supported on Survivable Core Servers or Survivable Remote Servers. Each Survivable Remote Server requires an LSP station license for each user of the server. Each Survivable Core Server requires an ESS station license for each station license on the main server.

The number of ESS station licenses and LSP station licenses that the customer activates is included in the license file. The number of activated survivable server station licenses is used to determine the number of Survivable Core Servers and Survivable Remote Servers that are needed to support the licensed stations. The appropriate number of Survivable Core Servers and Survivable Remote Servers, as determined by the number of survivable server station licenses that are activated, is specified in the Maximum Survivable Processors (VALUE_CM_SP) feature in the license file.

If the number of survivable server users on the system exceeds the number of survivable server station licenses, the customer must activate or purchase additional survivable server station licenses.

License files

Avaya requires a separate license file for every Avaya simplex server and every Avaya duplex pair of servers. License files are created using the Product Licensing and Delivery System (PLDS).

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 and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

When you place an order for a PLDS-licensed software product such as Communication Manager, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

This section provides an understanding the following:

- How the Module IDs and Cluster IDs, System Identification numbers, and MAC address affects a survivable core server:
- How to verify the license status:

Module IDs and Cluster IDs

The Communication Manager main server has a default module ID of 1. You can configure the Module ID on the Server Role page. Each survivable server has a unique module ID of 2 or greater.

The module ID must be unique for the main server and all survivable servers. The MID is administered as the Cluster Identification Number (CLID) in the Survivable Processor screen.

Each module receives a module identifier (MID) when a license file is created. The MID is referred to as the CLID in Survivable core servers. A CLID uniquely identifies a single cluster so that each server in a duplex pair can have the same CLID.

For the survivable core server to register with the main server, the MID of the survivable core server must match its administered CLID. The CLID is administered in the Survivable processor screen. For more information about how to administer a survivable core server using the Survivable processor screen, see *Survivable core server administration*.

Related links

Survivable core server administration on page 52

System Identification numbers

Communication Manager has a default system ID of 1. You can configure the System ID on the Server Role page. The system ID is common across the main server and all survivable servers.

Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form.

MAC Address

To activate the license file in PLDS, you must provide the WebLM host ID. The WebLM host ID is the MAC address of the server and is obtained from the WebLM Web interface.

Checking the license file

Procedure

After you load the license file on the server, run the following Linux commands on a survivable core server to ensure that you have the feature bits set correctly:

- **`Statuslicense -v -f FEAT_ESS`**: Verify FEAT_ESS (ESS administration feature) is locked on.
- **`Statuslicense -v -f FEAT_ESS_SRV`**: Verify that FEAT_ESS_SRV (Enterprise Survivable Server feature) is locked on.

Important:

After loading a license file on a server, you must stop and start the survivable core server using the following Linux commands:

- **`stop -af`** or **`stop -caf`**
- **`start -a`** or **`start -ca`**

Feature Keywords

The SAP order for a survivable core server system contains material codes for feature settings that appear in the license file. The material codes in a license file are identified as Keywords.

PLDS uses the following Keywords:

- FEAT_ESS (Survivable Core Server feature administration): FEAT_ESS must be turned **on** to use the survivable core server. For the main server, you can set it on the System Management Interface (SMI) page.
- FEAT_ESS_SRV (Survivable Core Server): FEAT_ESS_SRV must be **off** for the main server and **on** for the survivable core servers. This is done automatically when the server is configured as a main server or Survivable core server.

The FEAT_ESS and FEAT_ESS_SRV Keywords are both type I. Type I features have an on/off or yes/no value. Both ESS Feature Keywords are turned off by default.

Verifying the license status

About this task

To verify the license status, access the System Management Interface remotely through the corporate LAN connection or directly from a laptop connected to the server through the services port.

Procedure

1. Log in to the Communication Manager System Management Interface (SMI).
2. Click **Administration** > **Licensing**.
3. In the left navigation pane, click **License Status**.

   The License Status page displays the license mode and error information.

Server configuration worksheets

Collect the following network settings, network configuration, duplication parameters, and add login information before configuring the main server and each survivable core server.

After the survivable core server is configured it attempts to register with the main server. If the survivable core server is unable to register with the main server within 10 minutes after being configured, an alarm is generated. The survivable core server continues its attempt to register with the main server until registration is successful.

Note:

A survivable core server cannot register with the main server until it has been administered. Administration for a survivable core server is done on the main server. For instructions on how to administer the survivable core server, see *Survivable core server administration*.

Note:

The survivable core server cannot control an Media Gateway prior to receiving the initial translation download from the main server. A configured survivable core server automatically receives translations from the main server after it is administered.

Related links

Survivable core server administration on page 52
Network settings on page 51
Network configuration settings on page 51
Duplication parameters on page 51
Add Login on page 52

Network settings

Field	Value	Note
Communication Manager virtual machine IP address		
Communication Manager virtual machine hostname		

Network configuration settings

Field	Value	Note
Hostname		
Alias hostname		
Server ID (between 1 and 256)		
DNS domain		
Search domain list		
Primary DNS		
Secondary DNS (Optional)		
Tertiary DNS (Optional)		
Default gateway		
IP address for IP configuration of eth0		
Subnet mask for IP configuration of eth0		
Alias IP address for eth0		Is required only for duplication.
IP address for IP configuration of eth1		
Subnet mask for IP configuration of eth1		
Alias IP address for eth1		

Duplication parameters

You need to specify these parameters only in case of duplication and pertain to the standby server.

Field	Value	Note
Hostname		
Corporate LAN/PE IP address		
Duplication IP		
Server ID (between 1 and 256 and different from that of primary server)		
PE interchange priority		
IP address for PE health check		

Add Login

Field	Value	Note
Privileged administrator user ID		
Privileged administrator password		
Login shell script		
Home directory		

Survivable core server administration

Survivable Core Server administration is performed on the SAT of the main server using the Survivable Processor screen. The screen contains seven pages:

- Administer up to 63 survivable core servers on pages one through five.
- Administer the no service timer and schedule the Auto Return feature on page seven.

In Communication Manager, use the Survivable Processor screen to administer node names for survivable core servers.

Pre-requisites for administering a survivable core server on the main server

About this task

For details of the screen, see the Survivable Processor screen. On the main server, use the following steps to translate each survivable core server.

Procedure

1. On the main server, type `change survivable processor n`, where *n* is the node name of the survivable core server.
2. Administer the required fields for each survivable core server:
3. On page 1 of the Survivable Processor screen, identify survivable remote servers and survivable core servers and control use of the Processor Ethernet interface.
4. On page 2 of the Survivable Processor screen, administer CMS.

   If you have a CMS connecting to the Processor Ethernet interface of the server that you identified in page 1.
5. On page 3 of the Survivable Processor screen, administer AES.

   If you have an AES, a CDR that connects to the Processor Ethernet interface of the survivable remote server or survivable core server that you identified in page one.

The system displays page 4 of the Survivable Processor screen only if CDR is administered..

Related links

Assigning community for Port Network

Survivable Processor screen

For more information about administering the Survivable Processor screen, see *Avaya Aura® Communication Manager Screen Reference*.

Administering page one of the Survivable Processor screen

About this task

The fields and values that display on this screen depend on the **Type** value. If you are adding a survivable core server, when you change **Type** to either `simplex-ess` or `duplex-ess`, the screen is refreshed.

Procedure

1. Run the **`add survivable-processor`** command to gain access to the Survivable Processor screen.
2. Enter the survivable processor type. The default values are lsp, simplex-ess, or duplex-ess.
3. Enter the network region in which the Processor Ethernet interface of the survivable remote or core server resides (valid values 1 to 250).
4. Enter the Cluster ID (the Module ID from the Communication Manager license file) for the survivable core server.

   The Cluster ID corresponds to the Module ID from the license file of the survivable core server. Valid values are 1 through 999 and blank.
5. Displays the name used to identify this server. You can enter node names through the IP Node Names screen.

   If the survivable processor is duplicated, there are three node names, one each for the duplicated server pair and one for the server that is active at a given point of time. The IP address of the active server is known as the IP-Alias address.
6. Displays the IP address that corresponds to the node name you entered.

   There are three IP addresses, one for each node name if the survivable processor is a duplex server.
7. Enter `y` to allow the Processor Ethernet interface of the survivable core server to be used for H.323 devices such as telephones.

   If you enter `n`, the survivable core server Node Name may not display in the Alternate Gatekeeper (Survivable Server) List on the IP Network Regions screen. If you enter `y` and you administer the survivable core server node name on the IP Network Regions screen, the AGL list for IP endpoints will include the survivable core server Processor Ethernet.

When you run the **display ip-interface procr** command on the survivable core server, the **Allow H.323 Endpoints** field in that screen displays the value that you enter.

8. Enter `y` to allow the Processor Ethernet interface of the survivable core server to be used for gateways. When you run the **display ip-interface procr** command on the survivable core server, the **Allow H.248 Gateways** field in that screen displays the value that you enter.
9. The **Active Server Node Name** field is displayed only for duplex servers. The node name entered at the command line is displayed.
10. The **Active Server IP Address** field is displayed only for duplex servers. The IP address corresponding to the node name entered at the command line is displayed.
11. Server A ID corresponds to the Server ID configured using the Network Configuration page under **Server Configuration** on the System Management Interface of the survivable core server. The administration on the main server and the configuration on the survivable core server must match for the survivable core server to register to the main server. Valid values are 1 through 256 and blank.
12. For survivable remote server or simplex survivable core server, the node name is displayed in the **Server A Node Name** field. For duplex servers, enter the node name for Server A.
13. The IP address corresponding to the node name for Server A is displayed in the **Server A IP Address** field.
14. For duplex servers, the node name of Server B is displayed in the **Server B ID** field.
15. For duplex servers, enter the node name for Server B in the **Server B Node Name** field.
16. For duplex servers, the IP address corresponding to the node name for Server B is displayed in the **Server B IP Address** field.

Administering page two of Survivable Processor screen

About this task

Use page two of the Survivable Processor screen if you have a CMS connecting to the Processor Ethernet interface of the server that you identified in page one. If the CMS was administered in the Survivable Processor - Processor Channels screen the system will automatically display on page two of the Survivable Processor screen. You cannot add an adjunct in this screen. The adjunct must be administered in the Survivable Processor - Processor Channels screen first.

Procedure

1. The **Proc Channel** field displays the processor channel used for this link when it was administered in the Survivable Processor - Processor Channels screen.
2. Enter one of the following values in the **Enable** field:
   - Enter `n` (no) if this processor channel is disabled on the survivable remote server or the survivable core server.
   - Enter `I` (inherit) if this link is to be inherited by the survivable remote server or survivable core server. You must use the inherit option in the following scenario, where the main

server connects to the adjuncts using the main servers Processor Ethernet interface and you want the survivable remote server or survivable core server to connect to the adjunct using their Processor Ethernet interface.

- Enter ○ (over-ride) to over-ride the processor channel information sent in the file sync from the main server. The over-ride option causes the near-end (server's end of the link) address of the link to change to a **p** when the translations are sent from the main server to the survivable remote server or the survivable core server. Generally you would want the over-ride option when an adjunct connects to the main server and you want the adjunct to connect to the survivable remote server or the Processor Ethernet interface of the survivable core server.

  When you enter ○ in the **Enable** field, you can enter the processor-channel information for the survivable remote server or the survivable core server in the remaining fields.

3. The **Appl** field identifies the server application type/adjunct connection used on this channel.
4. The **Mode** field identifies if the IP session is passive (client) or active (server). Valid entries are c for client, s for server, or blank.
5. The **Interface Link** field identifies the physical link carrying this processor (virtual) channel. Yap' in this field indicates that the physical link is the Processor Ethernet interface.
6. For TCP/IP, interface channel numbers are in the range of 5000-64500. The value 5001 is recommended for CMS.
7. The **Destination Node** field identifies the adjunct at the far end of this link. Enter an adjunct name or leave this field blank for services local to this server.
8. The **Destination Port** field identifies the port number of the destination. The number 0 means any port can be used. Valid entries are 0 and 5000 through 64500.
9. In the **Session Local and Session Remote** field the Local and Remote Session is an integer from 1 to 384.

   For each connection, the Local Session number on this switch must equal to the Remote Session number on the remote switch and vise versa. It is allowed, and sometimes convenient, to use the same number for the Local and Remote Session numbers for two or more connections.

Administering Page three of the Survivable Processor screen

About this task

Use page three if you have an Application Enablement Services (AES), a CDR that connects to the Processor Ethernet interface of the survivable remote server or survivable core server that you identified in page one, or Survivable CDR. If the AES or the CDR is administered on the IP Services screen, the system automatically displays on page three of the Survivable Processor screen. You cannot add an adjunct using this screen. The adjunct must be administered in the ip-services screen first.

Note:

For more information on Survivable CDR, see *Survivable CDR*. For more information on how to administer Survivable CDR, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Procedure

1. The **Service Type** field identifies the server application type/adjunct connection used on this channel.

   Valid entries include the following: CDR1, CDR2, and AESVCS.

2. Enter one of the following values in the **Enabled** field:

   - Enter `n` (no) if this ip-services link is disabled on the survivable remote server or the survivable core server.
   - Enter `i` (inherit) if this link is to be inherited by the survivable remote server or survivable core server. Generally you would use the inherit option in the following scenario, where the main server connects to the adjuncts using the main servers Processor Ethernet interface and you want the survivable remote server or survivable core server to connect to the adjunct using their Processor Ethernet interface.
   - Enter `o` (over-ride) to over-ride the processor channel information sent in the file sync from the main server. The over-ride option causes the near-end (servers end of the link) address of the link to change to **p** when the translations are sent from the main server to the survivable remote server or the survivable core server. Generally you would want the over-ride
   - Enter `y` to enable Survivable CDR for this survivable remote server or survivable core server.

     When the **Service Type** field is set to `CDR1` or `CDR2` and the **Store to Dsk** field is set to `y`, all CDR data for the specific survivable remote server or survivable core server being administered will be sent to the hard disk rather than output to an IP link. Survivable remote server or survivable core server will only store CDR records to hard disk when the survivable remote server or survivable core server is controlling a gateway or media gateway.

3. The **Local Node** field contains the node name as defined on the Node Names screen.
4. The **Local Port** field contains the originating port number. For client applications such as CDR, this field defaults to 0.
5. The **Remote Node** field specifies the name at the far end of the link for the CDR. The remote node should not be defined as a link on the **IP Interface**or Data Module screen. The **Remote Node** field does not apply for AESs.
6. The **Remote Port** field specifies the port number of the destination. Valid entries range from 5000 to 65500 for CDR or AESs. The remote port number must match the port administered on the CDR or AESs server.

Note:

There can only be one AESs entered for each Processor Ethernet interface.

Note:

The System-Parameters CDR screen is removed on the survivable remote server or the translations of the survivable core server when `no` is entered in the **Enabled** field on the page three of the Survivable Processor screen.

Related links

Survivable CDR on page 38

Administering Page four of the Survivable Processor screen

About this task

The system displays this page only if CDR is administered on page three. Use page four to enter the session layer timers for the CDR. You can enter information in the fields on page four only if you set the **Enabled** field on page three to `o` (over-ride). If the **Enabled** field on page three is set to either `n` or `i` the fields on page four are display-only.

Procedure

1. The **Service Type** field displays the service type.
2. The **Reliable Protocol** field is used to indicate whether you want to use a reliable protocol over this link. Valid entries include y or n.
3. Enter the number of seconds, from 1 to 255, that the system will wait to send another packet from the time a packet is sent until a response or acknowledgement is received from the far end.
4. Enter the number of times Communication Manager tries to establish a connection with the far-end adjunct. Valid entries are from 1 to 5.
5. Enter the amount of seconds that the link can be idle before Communication Manager sends a connectivity message to ensure the link is still up.
6. The **Session Protocol Data Unit** counter indicates the number of times Communication Manager transmits a unit of protocol data before generating an error.
7. Enter the amount of time, from 1 to 255 seconds, that the link can be idle before Communication Manager sends a connectivity message to ensure the link is still up.

Checking the administration on the main server

Procedure

1. Type the **`status ess clusters`** command, and verify the following:
   a. The **Cluster ID** field for the main server is always 1.

b. The **Active Server ID** field is the Server ID that was entered for this server in the Set Server Identities web page during configuration. For duplex servers, the **Active Server ID** is active for the pair of servers.

c. The **Registered** field is `y`. If there is `n` in this column, the survivable core server is not registered and no data will display in the **Translation Updated** or **Software Version** columns. It may take several minutes for the survivable core server to register to the main server. For more information about how to troubleshoot the survivable core server registration, see *Troubleshooting*.

- The **Translations Updated** column:

  For Cluster ID 1 (the main server): The **Translations Updated** column correlates with the time of the last successful **`save translation`** command.

  For all other Cluster IDs: The **Translations Updated** column correlates with the date and time of the last successful translation download from the main server.

- The **Software Version** field indicates later versions of Communication Manager.

  For an example of the output of the **`status ess clusters`** command, see the following figure.

```
status ess clusters

Cluster ID   2           ESS CLUSTER INFORMATION

                      Active
  Cluster             Server               Translations        Software
    ID     Enabled?     ID   Registered?     Updated           Version

    2        y          2        y       21:29 7/12/2011   R016x.02.0.815.0
```

Figure 11: ESS Cluster information

Note:

The survivable core server software version will not appear until the survivable core server registers with the main server for the first time.

2. Type the **`display survivable processor node name`** command, and verify that the screen displays the values that you administered.

Related links

[Troubleshooting](#) on page 71
[Verifying the survivable core server translations](#) on page 71
[Verifying the survivable core server configuration](#) on page 72
[Registration](#) on page 72
[Troubleshooting the survivable core server](#) on page 72
[Monitoring registration requests example](#) on page 74
[IPSI is not connected to a server](#)
[Troubleshooting the IPSI connection](#)

Translations

Translations are saved on the main server by executing the **save translations** command. You cannot save translations on a survivable core server. When logging into a survivable core server you receive a message stating that this server is a survivable core server and translations cannot be saved.

The main server keeps one complete copy of translations plus the differences between that copy and one previous copy. Each copy has an associated day and time (timestamp). If the translation timestamp of the survivable core server matches the timestamp of the main server's current translations, no translation download occurs. If the timestamp of the survivable core server matches the timestamp of the main server's previous copy, the main server sends only the differences to the survivable core server. If the timestamp of the survivable core server does not match either of the main server's copies, then the main server sends the entire translation download to the survivable core server.

Translations are distributed from the main server to the survivable core server by executing the **save translations ess** or **save translations all** command. Executing this command requires network resources and should be performed when impact to the network is minimal. The survivable core server resets after it receives the translation download. The registration to the main server drops until the reset completes.

Saving translations, including sending the translations to the survivable core servers, can be performed during routine Communication Manager maintenance. Communication Manager scheduled maintenance is administered using the **system-parameters maintenance** command. For an example of the Maintenance-Related System Parameters screen, see the following figure.

```
display system-parameters maintenance                          Page   1 of   3
                  MAINTENANCE-RELATED SYSTEM PARAMETERS

OPERATIONS SUPPORT PARAMETERS
     CPE Alarm Activation Level: none

SCHEDULED MAINTENANCE
                                          Start Time: 22 : 00
                                           Stop Time: 06 : 00
                                    Save Translation: daily
 Update LSP and ESS Servers When Saving Translations: y
                           Command Time-out (minutes): 120
                         Control Channel Interchange: no
                      System Clocks/IPSI Interchange: no

SYSTEM RESETS
            Reset System SAT Command Warning Message? n
```

Figure 12: system-parameters maintenance

Verifying that the survivable core server has received the translations on the main server

Procedure

1. Run the **`status ess cluster`** command. The **Translations Updated** column contains the day and time (timestamp) of the last successful translation download to each survivable core server.
2. Run the **`save translations`** command. The **Translations Updated** column may take several minutes to update, depending on the size of the translations and network congestion.

Chapter 5: Survivable core server conversions

During the evolution of an enterprise communication network, it may be necessary to convert a standard server to a Survivable Core Server (ESS) or main server, a main server to a survivable core server, or a survivable core server to a main server.

The conversion procedures detail the specific steps required for the survivable core server feature only. Other steps (such as upgrading, re-mastering, or completely configuring a server) are found in standard documents that are referenced in this book.

For more information about conversions, see *Converting Avaya Servers and Gateways*.

Important:

The license file that is required for a conversion from a main server to a survivable core server or a survivable core server to a main server requires a special conversion process that must be performed by Avaya IT or by AGS.

Survivable core server conversion requirements

The requirements are as follows:

- For any conversion, the survivable core server should always be addressed before the main server. When a survivable core server is not controlling a Media Gateway, it can be converted without disrupting service.
- If possible, disconnect survivable core servers from the LAN/WAN until the main server is operational. Then connect the survivable core servers to the LAN/WAN and allow them to register with the main server.
- Two main servers should never be active on the LAN/WAN at the same time. When converting a server to a main server, care should be taken to disconnect or power down an existing main server before the new main server comes online.
- When converting servers, survivable core server to main server, or main server to survivable core server, a new license file is required. There are no exceptions and no way to turn on the required features without a new license file.
- The main server requires a MAC address to generate a license file in PLDS.
- All conversion options, including the main server (non survivable core server to main server, survivable core server to main server, and main server to survivable core server) is service

affecting. When Media Gateway are controlled by a new server (main server or survivable core server), they perform a restart which resets every Media module in the Media Gateway.

Converting the existing survivable core server to main server

About this task

Use this procedure to convert an existing survivable core server to a main server. For example, when two or more systems are being combined into one system, an existing Avaya server could be converted to a main server while other servers could be converted to survivable core servers.

Caution:

This procedure is service affecting. As the new main server is coming online, the Media Gateway that are being controlled by other servers will eventually switch to the new main server. This requires that the Media Gateway perform a reset. If a survivable core server exists, it may be advantageous to switch all Media Gateway to the survivable core server prior to the conversion.

Procedure

1. Back up the translations on the server to be converted. If the existing main server is still in operation, perform a complete backup. If the existing main server is not in operation, determine the location of the last known good backup.
2. Verify that the server to be converted is disconnected from the LAN/WAN.

   Caution:

   Two main servers cannot be connected to the LAN/WAN at the same time.
3. Connect the laptop to the services port on the server that you are converting.
4. Confirm that the server to be converted is running the latest version of Communication Manager.
   a. On the System Management Interface, click **Administration** > **Server (Maintenance)**.

      The Server Administration Interface is displayed.
   b. Click `Software Version` under **Server**.

      If the server is not running on the latest version of Communication Manager, upgrade the server.
5. If the server is a duplex pair, busy out the standby server.

6. Execute this step for S8300E active servers. In the System Management Interface, under **Server Configuration**, click the **Network Configuration** option.
   a. Enter a unique Server ID (SVID) in the **Server ID** field. A single SVID is required for a single server and two unique SVIDs are required for a duplicated server pair. This ID must be between 1 and 256. Usually the main servers are set to SVID 1 and 2.Gaps in the numbering are allowed (10, 20, 30, . . .) but servers may also be consecutively numbered.
      - Click **Continue**, and verify the IP Addresses.
   b. Under the **Server Configuration**, click the **Server Role** option from the left margin.
      - Select the main server.
7. For duplicated servers, perform the same configuration activities as step 6 for the standby server.
8. Install a new license file with the appropriate settings for the main server.

   The new license file should have the following attributes:

   - **Enterprise Survivable Server** set to `n`
   - **ESS Administration** set to `y`
   - A Module ID (MID) of 1: The MID is referred to as the Cluster ID (CLID) by the survivable core server feature. This value is set by the license file and cannot be administered in Communication Manager. Each server in a duplex pair (OEMR XL R640) has the same CLID. A main server always has the MID of 1.

     The MID appears in the license file name after the letter m. In an example where the main server license file name is s66579v5m1-060214-20295.lic, the MID would be 1.
   - A System ID (SID): The SID is unique to the system configuration. The main server and all survivable core servers will have the same SID.
9. Configuring the server causes a reset to be executed. It is not sufficient to notify all of the non Communication Manager processes of the new server configuration including the Cluster ID.
10. From the active server command line interface, run the following commands to notify all processes of the new parameters:
    - **`stop -caf`**
    - **`start -ca`**
11. For duplicated servers, release the busy out of the standby server using the **`Release Server`** command on the System Management Interface.
12. Wait for the license file to be file synced from the active server to the standby. This can be verified by using the Linux command **`statuslicense-v`** repeatedly until the Module ID is updated.

13. Once the Module ID is updated, run the following commands from the command line to inform all processes of the new server configuration and Module ID.interface:
    - **stop -caf**
    - **start -ca**
14. Be sure that the translations from the main server match the translations for the newly converted main server. Use the **display survivable-processor** command to check the main translations. If the translations do not match, adjust as necessary using the **Network Configuration** command from the System Management Interface (see step 6).
15. Remove the old ESS translations from the newly converted main server using the **remove survivable-processor nodename** command, where **nodename** is the old ESS node name.

    If this is not done the new main server will alarm when the former survivable core server fails to register. For more information on administering ESS, see *Survivable core server administration*.
16. After the former ESS translations have been removed, it is necessary to notify all Communication Manager processes that the old Cluster ID no longer exists. Use the following commands to notify the Communication Manager processes:
    - **save trans all**
    - **reset sys 4**
17. Use the **list survivable-processor**, **display survivable-processor nodename**,command to verify that the correct translations are present for all the survivable core servers.
18. Disconnect, if connected, the old main server from the LAN/WAN.
19. Connect the new main server to the LAN/WAN.
20. At any existing survivable core server, verify that the new main server or server pair are connected to the LAN/WAN.
21. Using the System Management Interface, on each **ESS** and **LSP** specify:

    The IP address(es) of the new main server.

    Changing the address of the main server on the survivable core server does not require a **reset system 4**, nor does it do one automatically.

    For more information on how to configure the server, see *Server configuration worksheets*.
22. Verify that each of the survivable core servers and survivable remote servers register with the main server and that the translations are updated.

    Using the **status ess clusters** command, verify that the main server (this server) is shown and that all survivable core servers register and their translations are updated.

Periodically repeat the **status ess clusters** or **list survivable-processor** command until all survivable core servers register and are updated.

Note:

An active main server knows its own state and that of any survivable core servers that have registered with it. For some period of time (minutes), after all servers are installed and configured, there may be a discrepancy between the state displayed by the main server and the survivable core servers.

23. If a **save trans all** command was not performed in step 16 then do so now. At the main server, execute the **save translation all** command to synchronize translations between the new main server, the survivable remote servers, and the survivable core servers.
24. If a **reset system 4** command was not performed in 16, then do so now. From the main server, execute the **reset system 4** command.

Related links

License files on page 48
Survivable core server administration on page 52
Pre-requisites for administering a survivable core server on the main server on page 52
Survivable Processor screen on page 53
Administering page one of the Survivable Processor screen on page 53
Administering page two of Survivable Processor screen on page 54
Administering Page three of the Survivable Processor screen on page 55
Administering Page four of the Survivable Processor screen on page 57
Assigning community for Port Network
Checking the administration on the main server on page 57
Server configuration worksheets on page 50
Network settings on page 51
Network configuration settings on page 51
Duplication parameters on page 51
Add Login on page 52

Converting the existing server to survivable core server

About this task

This procedure is used when you have an existing server that you are converting to a survivable core server.

Procedure

1. Back up the translations on the server to be converted.

If the existing server is still in operation, perform a complete backup. If the existing main server is not in operation, determine the location of the last known good backup.

2. Verify that the server to be converted is disconnected from the LAN/WAN.

   Caution:

   Be careful to never have two main servers connected to the LAN/WAN at the same time.

3. Connect the laptop to the services port on the server.
4. Confirm that the server to be converted is running the latest version of Communication Manager.
   a. On the System Management Interface, click **Administration** > **Server (Maintenance)**.

      The Server Administration Interface is displayed.

   b. Click **`Software Version`** under **Server**.

      If the server is not running on the latest version of Communication Manager, upgrade the server. For the procedure to upgrade the server, see *Upgrading Avaya Aura® Communication Manager*.
5. If the server is a duplex pair busy out the standby server.
6. Perform this step for simplex and active servers of duplex pair. In the System Management Interface, click **Server Configuration** > **Network Configuration**.
7. For duplex servers, perform the same configuration activities as step 6 for the standby server.
   a. Enter a unique Server ID (SVID) in the **Server ID** field.

      A single SVID is required for a simplex server and two unique SVIDs are required for a duplex server pair. This ID must be between 1 and 256. Usually the main servers are set to SVID 1 and 2. Gaps in the numbering are allowed (10, 20, 30, . . .) but servers may also be consecutively numbered.

      - Click **Continue**, and verify the IP Addresses.

   b. Go to **Server Configuration** and click the **Server Role** option.

      - Select the main server.
8. Configuring the server causes a reset to be executed. It is not sufficient to notify all of the non Communication Manager processes of the new server configuration including the Cluster ID.
9. From the active server command line interface use the command line interface to run the following commands to inform all processes of the new server configuration and Module ID.:
   a. **`stop -caf`**

b. **start -ca**

10. For the duplex servers, release the busy out of the standby server using the **Release Server** command on the System Management Interface.

    Use the command line interface to perform the following commands to inform all processes of the new server configuration and Module ID:

    a. **stop -caf**

    b. **start -ca**

11. Verify that the main server has the latest translations available.
12. Translate the new survivable core server on the main server: From the main server execute the **change survivable-processor** command.

    For more information on administering the survivable core server, see *Survivable core server administration*.

13. Connect the new survivable core server to the LAN/WAN.
14. Verify that the survivable core servers register with the main server and that the translations are updated on the survivable core server.

    Use the **status ess clusters** command to verify that the main (this server) is shown and that all the survivable core servers register and translations are updated. Periodically repeat the **status ess clusters** command until all the survivable core servers are registered and updated.

    Note:

    A active main server knows its own state and that of any survivable core server that registers with it. For some period of time (minutes), after all servers are installed and configured, there may be a discrepancy between the state displayed by the main server and the survivable core servers.

15. To synchronize translations between the main server, the survivable remote servers, and the survivable core server, run **save translation all** on the main server.

Related links

Survivable core server administration on page 52
Pre-requisites for administering a survivable core server on the main server on page 52
Survivable Processor screen on page 53
Administering page one of the Survivable Processor screen on page 53
Administering page two of Survivable Processor screen on page 54
Administering Page three of the Survivable Processor screen on page 55
Administering Page four of the Survivable Processor screen on page 57
Assigning community for Port Network
Checking the administration on the main server on page 57

Chapter 6: Survivable core server management

This section describes various nuances that one should be aware of when a survivable core server controls one or more Media Gateways.

Translations administration

All administration is performed on the main server. The main server can only distribute translations to a survivable core server if the survivable core server is registered with the main server. The survivable core server registers with the main server through Processor Ethernet. Translations can be administered on a survivable core server but they cannot be saved.

Determining when the last translation is download from the main server

About this task

The main server sends translations to the survivable core server when you:

- Run a **`save translations all`** or a **`save translations ess`** command.
- Select the Update survivable remote server and survivable core servers when saving translations option during routine maintenance.

Procedure

1. Run the **`status ess clusters`** command.
2. Check the value of the **Translations Updated** (timestamp) column associated with the cluster ID of the survivable core server.

```
status ess clusters

Cluster ID  1          ESS CLUSTER INFORMATION

                     Active
  Cluster            Server               Translations        Software
    ID     Enabled?    ID   Registered?     Updated            Version

   2        y          2         y        21:29 7/12/2011   R016x.02.0.815.0
   3        y          91        y        21:29 7/12/2011   R016x.02.0.815.0
```

Figure 13: Status ess clusters

User enabled telephone features

User enabled telephone features, such as Call Forwarding and Send All Calls, will be preserved after a failover to a survivable core server, if the administered features were captured when translations were saved and the translations were distributed to the survivable core server prior to the failover.

When a survivable core server controls a Media Gateway, user enabled telephone features will not be preserved when the system falls back to the main server. The user enabled features cannot be saved to translations on a survivable core server and the main server will have no knowledge of the settings.

Alarms

The main server generates alarms when it no longer controls a gateway. The following is a partial list of the types of alarms the main server may generate:

- A major alarm for every gateway no longer under the main server’s control.
- A platform alarm if the main server failed because of a hardware issue.
- A minor alarm if gateways are not registered to the main server.

The following is a partial list of the types of alarms generated by the survivable core server when it obtains control of a media gateway:

- An alarm is generated when the survivable core server controls gateways and IP endpoints.

Update the main server

Before bringing a main server back on-line, check the main server's software to make sure it matches the software version running on the survivable core server. Verify the software version on the Web interface of the survivable core server. Verify the software version on the main server. Update the software on the main server (if necessary).

After a fall-back to the main server

The survivable core server performs a reset system 4 when it no longer controls a Media Gateway. The **`reset system 4`** command is used to clear alarms, busyouts and allow any pending translations to be loaded.

Note:

It is possible to perform a file sync (translation download) from the main server to the survivable core server while the survivable core server is controlling one or more Media Gateway. The translations are received by the survivable core server but are not loaded as long as the survivable core server controls a Media Gateways. Once the survivable core server no longer controls a Media Gateway, the survivable core server resets and loads the new translations.

Chapter 7: Troubleshooting

There may be times when you need to troubleshoot a survivable core server implementation. To determine what is causing a fault it is important to understand the following:

- The layout and topology of the network
- Where survivable core servers are located on the network
- How you want the design to work during the failure

You can obtain this information from the implementation team or the customer.

By looking at the translation of a particular Survivable core server installation, you can make reasonable predictions as to how the installation will react to server failure and/or a network failure. However, keep in mind that the way the various components are configured and translated may not reflect the original intent of the network design.

Verifying the survivable core server translations

Procedure

Use the following commands to verify the survivable core server translations:

- **`list survivable-processor`** (executed on the main server) displays all translated survivable core servers.
- **`status ess clusters`** displays the following information:
  - Which clusters are enabled
  - When translations were last updated
  - What software release the main server and survivable core servers are running

    The survivable core servers can be on a later release than the main server but the main server should never be on a later release than the survivable core servers. The software release should only be different when upgrades are being performed. Always upgrade the survivable core servers first and then the main server.

Verifying the survivable core server configuration

Procedure

Use the following System Management Interface screens to verify the survivable core server configuration:

- Network Configuration specifies whether the server is a main server or a survivable core server. If it is a survivable core server specify an address for a Processor Ethernet and the main server.
- Network Configuration sets the Server IDs of the individual servers.

Registration

Use this section for information on how to troubleshoot registration problems.

Survivable core server is not registered with the main server

A survivable core server registers with the main server. Under normal conditions a survivable core server may not register with the main server if the survivable core server is resetting. The survivable core server resets when it receives a new translation file or when it is first enabled. This should be a temporary condition.

See *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers* for errors related to survivable core server registration. Error 257 should be logged when a survivable core server is administered on the main server but is not registered.

Troubleshooting the survivable core server

Procedure

1. On the main server, run the **`display survivable-processor essName`** to verify that the survivable core server is properly administered.

   A survivable core server must be administered on the main server before it can register with the main server. Record the administered values to use when you troubleshoot.

2. On the main server, run the **`display events`** command with a **category** of **denial** to display the denial events related to survivable core server. The survivable core server registration denial events are in the 36xx range.

   For descriptions of the survivable core server denial events, see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*.

3. On the main server, run the **`list trace ras ip-address`** command to monitor registration requests from the survivable core server.

   This command displays registration requests from the survivable core server and the associated response from the main server.

Note:

Under normal operation, a Keep Alive (KA) message is periodically sent from the survivable core server to the main server. This should not be confused with a registration failure.

4. On the survivable core server, run the **`ping nnn.nnn.nnn.nnn`** command to verify connectivity between the survivable core server and main servers, where **`nnn.nnn.nnn.nnn`** is the IP address of the Procr in the main server that the survivable core server is trying to register with.

   Caution:

   n the next steps be careful to use the **`Close Window`** button to cancel out of the Network Configuration page to avoid a reboot of the survivable core server. Do not update the system.

   To determine which IP address the survivable core server is attempting to register with use the **`Server Configuration`** command from the System Management Interface on the survivable core server to display the Configure ESS page.

5. Firewalls or other security measures may preclude the main server and survivable core server from communicating. Verify that the following ports are open:
   - Port 1719 Registration between the survivable core server and the main server.
   - Port 21874 Filesync (rsync) is open between the main server and survivable core server.
6. On the survivable core server, run the Server Configuration pages of the System Management Interface to verify the following:
   a. On the Network Configuration page, verify that the correct Server ID (SVID) is entered. This should be a unique value for each server. The SVID can be between 1 and 256. Gaps in the SVIDs are allowed but the servers may also be consecutively numbered. Each server in the system, duplex or simplex, main server or survivable core server, requires a unique SVID.
   b. On the Configure ESS page, verify that the correct platform type (duplex or simplex) is selected and the correct Processor Ethernet and main server's IP addresses are entered. The survivable core server uses these addresses to establish a connection and register with the main server (see step 1).
   c. On the Status Summary page, verify that the Cluster ID and the individual server IDs are correct.

      Note:

      The individual server IDs should be the same as the ones that were entered on the Network Configuration page of the Server configuration procedure.
7. On the survivable core server, run the **`display system-parameters customer-options`** command. Verify the administration of the following fields:
   a. The **ESS Administration** field is set to `y`

b. The **Enterprise Survivable Server** field is set to `y`

Tip:

The customer options can only be set with the Avaya license file. If the fields above are incorrect obtain a new license file with the correct data.

8. From the System Management Interface, under **Administration** > **Server (Maintenance)**, click **License File**, and verify that the license mode is **normal**.
9. On the survivable core server, run the **`status ess clusters`** command to verify that a translation file has been sent to this survivable core server.

   The translation file is only sent after the survivable core server successfully registers. If a translation file has never been sent, this is an indication of either serious network connectivity issues, Communication Manager administration, and/or configuration errors.

Monitoring registration requests example

About this task

This example shows how you would use the **`list trace ras ip-address x.x.x.x`** command to monitor registration requests from a survivable core server and the associated response from the main server.

Procedure

1. Run the **`display survivable-processor`** command from the main server and make note of the IP addresses of the main Server and the survivable core servers.

```
display survivable-processor ESS                              Page   1 of 3

                             SURVIVABLE PROCESSOR

Type: simplex-ess      Cluster ID/MID: 2  Processor Ethernet Network Region: 1
                            Community: 1      Enable PE for H.323 Endpoints? n
                                              Enable PE for H.248 Gateways? n

SERVER A
    Server ID: 2
 V4 Node Name: ESS              Address: 10.13.6.123
 V6 Node Name:                  Address:


PORT NETWORK PARAMETERS
                  Community Size: all      System Preferred: y
                  Priority Score: 1         Local Preferred: n
                                                 Local Only: n
```

Figure 14: Troubleshooting - display survivable processor example

2. From the survivable core server that is to be monitored, use the System Management Interface and the Server Configuration screen to display the Configure ESS page and make note of the IP address that is configured as the primary address of the main server.

3. From the main server, enter the **`list trace ras ip-address x.x.x.x`** command for the IP address that is to be monitored.

   In this example, the IP address of the survivable core server (135.9.78.143) was entered.

   The first message exchange is from the survivable core server sending a Registration Request (RRQ) to the main server. The main server responds with a Registration Confirmation (RCF). The survivable core server and main server continue a conversation where the survivable core server sends a Keep-Alive message (KARRQ) and the main server confirms it (RCF).

```
list trace ras ip-address 135.9.78.143                          Page   1

                                LIST TRACE

time            data

11:01:02   rcv RRQ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
11:01:02   snd RCF endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext

11:03:02   rcv KARRQ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
11:03:02   snd RCF endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext

11:04:02   rcv KARRQ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
11:04:02   snd RCF endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext

11:05:02   rcv KARRQ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
11:05:02   snd RCF endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
11:06:02   rcv KARRQ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
11:06:02   snd RCF endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
11:07:02   rcv KARRQ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
```

Figure 15: Troubleshooting - list trace ras command example - main server

4. Fom the survivable core server, run the trace command. Use the IP address obtained from the Configure ESS page with the **`list trace ras`** command.

   The same ESS/main message exchange takes place. From this perspective the survivable core server sends a Registration Request (these appear as KARRQ messages at the main server) and the main server responds with Registration Confirmation (RCF) messages.

```
list trace ras ip-address 135.9.72.168                          Page   1

                                LIST TRACE

time            data

11:01:02   snd RRQ endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
11:01:02   rcv RCF endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext

11:03:02   snd RRQ endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
11:03:02   rcv RCF endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext

11:04:02   snd RRQ endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
11:04:02   rcv RCF endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext

11:05:02   snd RRQ endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
11:05:02   rcv RCF endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
11:06:02   snd RRQ endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
11:06:02   rcv RCF endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
```

Figure 16: Troubleshooting - list trace ras command example - ESS

5. Suppose that the survivable core server is incorrectly administered on the main server.

   In this example, the survivable core server is configured to have Server ID 98 using **Network Configuration** on the Server Configuration page. However, the survivable core server also has Server ID 97 administered on the main server using the SAT command **`change survivable-processor`**.

   From the main server, the data shown in the following figure displays using the **`list trace ras`** command.

```
list trace ras ip-address 135.9.78.143                          Page   1

                                LIST TRACE

time            data

12:47:42   rcv RRQ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
12:47:42   denial event 3600: IP RRJ-ESS not admin endpt 135.9.78.143 data0:0x0
12:47:42   snd RRJ endpt 135.9.78.143:1719 switch 135.9.72.168:1719 ext
```

Figure 17: Troubleshooting - mis-administration - main server perspective

Notice that on the main server a denial event occurs when the survivable core server attempts to register. Denial events are displayed using the **`display events`** command. Briefly, the denial events associated with survivable core server are:

- 3600: IP RRJ-ESS not admin: The survivable core server attempting to register does not match any of the administered survivable core servers in translations.
- 3601: IP RRJ-ESS obj not init: The FEAT_ESS feature bit is not turned on in the license file.
- 3602: IP RRJ-ESS bad SID sent: The survivable core server sent a SID that does not match that of the main server. The SID is set by the license file.

Using the **list trace ras** command on the survivable core server, the server displays the data as shown in the following figure.

```
list trace ras ip-address 135.9.72.168                          Page   1

                                LIST TRACE

time            data

12:47:42   snd RRQ endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
12:47:42   rcv RRJ endpt 135.9.72.168:1719 switch 135.9.78.143:1719 ext
```

Figure 18: Troubleshooting - mis-administration - ESS perspective

Notice that the survivable core server sends a Registration Request (RRQ) but only receives a Registration Rejection (RRJ) from the main server.

Chapter 8: Survivable Core Server Acceptance Testing

Survivable core server acceptance testing

Acceptance testing is used to test the design and administration of the survivable core server configuration.

Testing transfer of control from main server to survivable core server

About this task

You can expect the following events to occur:

- All the tested Media Gateways re-register to the survivable core when coming into service on it.
- The registration process may take several minutes.

Caution:

This test is service affecting. When a survivable core server or main server assumes control of a media gateway, the media gateway re-registers. At this point the call goes in connection preservation and any more feature activations on this call ends up in dropping it.

Use this procedure to test the ability of a survivable core server to take control of one or more Media Gateways. Use the following steps to execute this test.

Procedure

1. Identify the Media Gateways that are being tested.
2. Identify the survivable core server that is being tested. The survivable core server must be connected to the Media Gateways identified in step 1.

Testing transfer of control from survivable core server to main server

About this task

You can expect the following event to occur:

- The survivable core server loses control of all media gateways and media servers under its control as the gateways and media-servers move back to main.

This test takes several minutes.

Use this procedure to test the ability of the main server to assume control of the media gateways and media servers that are currently under control of the survivable core server. Perform the following steps to execute this test.

Procedure

1. Verify that the mg-recovery-rule and ms-recovery-rule is set to manual.
2. Verify that the survivable core server is in control of the media-gateways and media servers being tested by executing the **`list media-gateway`** and **`list media-server`** command from the main server. The status of the port networks being tested is shown as **rd**.
3. On the main server, execute the SAT command, **`enable mg-return all`** and **`enable ms-return all`**.

   Caution:

   This test is service affecting.

Verifying the acceptance criteria

About this task

Check that the selected media gateways and media-servers are now under control of the main server by performing the following steps

1. On the main server, run the **`list media-gateway`** command, and verify the following:
   - All media gateways are listed.
   - The status of all media gateways is shown as **up**.
2. On the survivable core server, run the **`list media-gateway`** command, and verify the following:
   - All media gateways are listed.
   - The status of all media gateways is shown as **down**.
3. Place a telephone call between two media gateways that are being tested. If only one media gateway was tested, skip to step 4. Verify that you have a two way talk path.
4. Place a telephone call between two media gateways that were not selected for this test. Verify that you have a two way talk path.

5. Place a telephone call between a media gateway being tested and one that is not being tested. Verify that you have a two way talk path.

Disabling a survivable core server from the main server

About this task

You can expect the following events to occur:

- Communication Manager resets on the selected survivable core server.
- Once the survivable core server resets, it re-registers with the main server.
- The status of the survivable core server changes from unregistered to registered. The change in the status of the survivable core server takes several minutes and will not happen immediately.

Use this procedure to test the ability to disable a survivable core server from the main server. Perform the following step to execute this test.

Procedure

On the main server, execute the **`disable ess cluster <cluster ID>`** command.

Verifying the acceptance criteria

Procedure

1. On the main server:

   After the survivable core server comes back up from the reset and re-registers with the main server, execute the **`status ess clusters`** command from the main server SAT. Verify that:

   - The enabled state under the **Enabled** column, shows `n`.
   - The registration state under the **Registered** column shows `y`.

2. On the survivable core server:

   Execute the **`status ess clusters`** command. Verify that:

   - The enabled state under the **Enabled** column, shows `n`.
   - The registration state under the **Registered** column shows `y`.

Enabling a survivable core server from the main server

About this task

You can expect the following events to occur:

- Communication Manager resets on the survivable core server being tested.
- Once the survivable core server resets it re-registers with the main server.
- The survivable core server receives a translation download from the main server and resets again.
- After the reset, the survivable core server re-registers with the main server.

Use this procedure to test the ability to enable a survivable core server from the main server. Perform the following step to execute this test.

Procedure

On the main server, execute the **`enable ess cluster <cluster ID>`** command.

Verifying the acceptance criteria

Procedure

1. On the main server:

   After the survivable core server comes back up from the reset and re-registers with the main server, execute the **`status ess clusters`** command from the main server SAT. Verify that:

   - The enabled state under the **Enabled** column shows `y`.

2. On the survivable core server:

   Execute the **`status ess clusters`** command. Verify that:

   - The enabled state under the **Enabled** column shows `y`.

Chapter 9: Resources

Communication Manager documentation

The following table lists the documents related to Communication Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Overview and Specification	Provides an overview of the features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Security Design	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
LED Descriptions for Avaya Aura® Communication Manager Hardware Components	Describes the LED for hardware components of Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware requirements for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Survivability Options	Describes the system survivability options for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Core Solution Description	Provides a high level description for the solution.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides procedures to maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues…

Title	Description	Audience
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides commands to monitor, test, and maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Alarms, Events, and Logs Reference	Provides procedures to monitor, test, and maintain Avaya servers and describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager SNMP Administration and Reference	Describes SNMP administration for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Avaya Aura® Communication Manager Server Options	Describes server options for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Data Privacy Guidelines	Describes how to administer Communication Manager to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager on a software-only environment and Amazon Web Service, Microsoft Azure, and Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

Title	Description	Audience
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Screen Reference	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that specific customers request for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.

- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Glossary

CLID	Cluster Identification number. In a survivable core server environment, the Module Identification number (MID) found in the license file is referred to as the CLID. The CLID identifies a unique cluster. Each server in a duplex pair has the same CLID.
Community	A virtual group consisting of one survivable core server and one or more media gateways.
Main server	The primary server that usually controls the system. The main server may be simplex or duplex servers.
MID	Module Identification number: Refers to a simplex server and a duplex pair of servers, within the same Avaya system, as a module. Each module is assigned a unique Module Identification number (MID). In the case where there is a duplex pair of servers, each processor within the pair has the same license file. In a survivable core server environment, the MID and the CLID are the same value.
MO	Maintenance object
P	
Preference	An ESS can be administered with one of three preference settings. The preference settings are System Preferred, Local Preferred, and Local Only.
Priority score	See Priority value.
Priority value	An administered value entered in the Survivable Processor screen. The priority value is used to distinguish between survivable core servers with the same preference settings and survivable core servers with no preference settings. For this document, the term priority value and priority score is interchangeable.
S	
SAP	Avaya’s ordering system for products and services.
SSO	Single Sign-On: An Avaya corporate mechanism requiring a single login to allow users access to certain websites.

Survivable Core Server	The Avaya option that provides survivability by allowing survivable servers to be placed in various locations in the customer's network. The server that is ready to respond to an IPSI's request for service if all other recovery mechanisms fail. The survivable core server may be simplex or duplex servers.
Survivable Remote Server	An Avaya server that may accept gateway and/or endpoint registrations in case of a server or network failure.
SVID	Server Identification number: A unique identification number assigned by the customer to the server when the server is configured.
SVOR	Server Ordinal: This value identifies a server within its server pair. This value is set automatically when the server is configured. The A-side server in a duplex pair always has the ordinal of one. The B-side server in a duplex pair always has the ordinal of two. Simplex servers always have the ordinal of one.

Index

H

I

K

L

M

N

P

S

T

U

V

W