Avaya Aura® Communication Manager Survivability Options

03-603633
Issue 2
Release 6.2
July 2012

© 2012 Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Website: http://support.avaya.com. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya.

Licenses

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

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

License types

- Designated System(s) License (DS):
  End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU):
  End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU):
  End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User" means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (for example, webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR):
  Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (See Third-party Components for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Website: http://support.avaya.com.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura™ are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S.and other countries.

Downloading documentation

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

Contact Avaya Support

See the Avaya Support Web site: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support Web site: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

About this document 9
Overview 9
Audience 9
Downloading this book and updates from the web 9
Downloading this document 9
Related resources 10
Avaya Mentor videos 10
Support 10
Technical assistance 11
Within the US. 11
International 11
Trademarks. 11
Sending comments 11

Chapter 1: Survivability Overview 13
Avaya survivability 13
Survivable remote and core servers 13
Survivable remote server 14
Survivable core server 14
Survivable core server overview 15
No service timer 16
Failover to a survivable core server 16
Processor Ethernet overview 19
Support for Processor Ethernet and Port Networks on a survivable core server 21
Firmware for optimal performance 21
C-LAN access for survivable core server registration 22
Survivable core server requirements. 23
Survivable core server failover examples 24
Example one: Main servers fail 24
Example two: Network failure. 28
Example three: A survivable remote server working in a survivable core server environment 35

Chapter 2: Survivable Core Server design and planning 43
Survivable core server design strategy 43
Survivable core server terminology 44
Survivable core server prerequisites. 45
Network port considerations 46
Main server and survivable core server differences 47

Trunking considerations 48
ISDN PRI non facility associated signaling 48
Guidelines for ISDN PRI non facility associated signaling 48
E911. 49
Inter-Gateway Alternate Routing 49
Personal Central Office Line 49
Separation of Bearer and Signaling 50
Data Networking 50
H.323 considerations when using survivable core server 50
IPSI priority list. 51
Assigning priority to an IPSI 54
Changes to a priority list 54
Examples of how the priority list works 56
Timing considerations. 60
Survivable core server no service timer 60
Primary Search Timer 60
Feature limitations during gateway outage 60
PN Cold Reset Delay timer 61
Feature considerations 61
Announcements 62
Attendant Console 62
Best Service Routing 62
Call Classification 62
Call Coverage 62
Call Vectoring 62
Centralized Attendant Service 63
Crisis Alert 63
CVLAN links 63
Dial Plan Transparency 63
Facility Busy Indication 64
Hunt Groups 64
Leave Word Calling 64
Music on Hold 64
Adjunct considerations 64
Call Detail Recording 65
Traditional Call Detail Recording 65
Survivable CDR 65
Call Management System 66
Extension to Cellular 66
Property Management System 67

Voice Mail 67
Voice Response System 67

Chapter 3: Survivable Core Server installation 69
Survivable core server installation checklist 70
Overview 70
Installing survivable core server with existing servers 71
Installing survivable core server with new servers 75
Survivable core server license files 79
Licensing survivable servers 79
Station licenses for survivable servers 80
License files 80
Module IDs and Cluster IDs 81
System Identification numbers 81
MAC Address 82
Checking the license file 82
Feature Keywords 82
Verifying the license status 83
Server Configuration 83
After the survivable core server is configured 85
Administering survivable core server 86
Administering a survivable core server on the main server 86
Important upgrade information 86
Pre-requisites 86
Survivable Processor screen 87
Administering page one of the Survivable Processor screen 87
Administering page two of Survivable Processor screen. 89
Administering Page three of the Survivable Processor screen 90
Administering Page four of the Survivable Processor screen 91
Assigning Community for Port Networks screen 92
After administering the survivable core servers 93
Checking the administration on the main server 93
Translations 96

Chapter 4: Survivable core server conversions 99
Basic guidelines for conversions 99
Existing survivable core server to main server 100
Existing server to survivable core server 103

Chapter 5: Running in survivable core server mode 107
Administering and saving translations. 107
User enabled telephone features 108
Alarming 108
Unplanned fall-back or failover 109
Unplanned fall-back to the main server 109
Unplanned failover to another survivable core server 110
Updating the main server 110
After a fall-back to the main server 110

Chapter 6: Troubleshooting. 113
Registration 114
Survivable core server is not registered with the main server 114
list trace ras command example 116
IPSI is not connected to a server 119

Chapter 7: Survivable core server acceptance testing 121
Testing transfer of control from main server to survivable core server 121
What to expect 121
Acceptance criteria 122
Testing transfer of control from survivable core server to main server 122
What to expect 123
Acceptance criteria 123
Disable a survivable core server from the main server 124
What to expect 124
Acceptance criteria 124
Enable a survivable core server from the main server 125
What to expect 125
Acceptance criteria 125

Glossary 127

Index 129

About this document

Overview

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

Audience

This document is for the following audiences:

- Technical support representatives
- Authorized Business Partners

Downloading this book and updates from the web

You can download the latest version of this document from the Avaya Support website http://support.avaya.com. You must have access to the Internet and a copy of Adobe Reader installed on your personal computer.

Avaya makes all possible efforts to ensure that the information in this book is complete and accurate. However, information can change after we publish this document. Therefore, the Avaya Support website might also contain new product information and updates to the information in this document. You can also download these updates from the Avaya Support website.

Downloading this document

To download the latest version of this document:

1. Access the Avaya Support website at http://support.avaya.com.
2. In the **SEARCH AVAYA SUPPORT** text box, type the document number 555-245-112 and click the arrow button.
3. In the resulting list, locate the latest version of this document.

4. Click the document title to view the document in PDF Format.

Related resources

- *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431
- *Upgrading to Avaya Aura® Communication Manager*, 03-603560
- *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504
- *Implementing Avaya Aura® Communication Manager*, 03-603558
- *Installing the Avaya S8800 Server for Avaya Aura® Communication Manager*, 03-603444
- *Adding New Hardware for Avaya Servers and Gateways*, 555-245-112

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at http://support.avaya.com, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya Technical Consulting and System Support (TC-SS) at 1-800-225-7585.
- Maintenance and warranty technical support, call the Avaya National Customer Care Support Line at 1-800-242-2121.
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353.

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Sending comments

Avaya welcomes your comments on this book. You can send your comments to: *infodev@avaya.com*.

In comment, mention the name and number of this document, *Avaya Aura® Communication Manager Survivability Options*, 03-603633.

Chapter 1: Survivability Overview

Avaya survivability

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. The Survivable remote server does not manage the Internet Protocol Server Interface (IPSI). Therefore, port networks are not controlled by the survivable remote server. 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 port networks and 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. For more information, see Survivable core server overview.

Survivable remote and core servers

This section explains the differences between a survivable remote and a survivable core server.

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 of Main or survivable servers and Control Local Area Networks (C-LANs) known as TN799 in the list. All the C-LANs (TN799) represent a single call controller, although it could be the main server or a survivable Core Server. However, if processor ethernet is used for registration, then only one server controller address is in the main server part of the media controller list.

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.

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

Survivable core server

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

The survivable core server provides the same functionality and the same capacity as the main server. Through the IPSI circuit pack in the port network, the survivable core server can provide service to a gateway. The survivable core server can also provide service to each gateway through C-LAN connections in the port networks.

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.

- The capabilities of survivable core servers are enhanced to support connection of IP devices to the Processor Ethernet interface as well as to C-LAN interfaces located in the port networks.
- 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

Table 1 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	S8300D	S8510	S8800/HP DL360 G7/Dell R610
Duplex	__	__	Y
Simplex	__	Y	Y
Simplex Survivable Remote	__	Y	Y
Embedded Survivable Remote	Y	__	__

Survivable core server overview

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. The survivable core servers are given administered values that are assigned to each IP Server Interface (IPSI) in the configuration. The IPSI places the survivable core server on a priority list based on the administered values. If for any reason, the IPSI can no longer communicate with the main server, the IPSI requests service from the next highest priority survivable core server on its list. The survivable core server accepts the request and assumes control of the IPSI controlled port 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.
For more information on server template types, see Table 1: Survivable remote or core server template types.

Through careful planning and consideration, the servers are placed in various locations in the customer's network (Chapter 2: 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 IPSI in the configuration. This is true for all servers except those administered as a Local Only server. Local Only servers connect to IPSIs in their same community only. For more information on administering the values for survivable core server, see Administering survivable core server.

The IPSIs 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 IPSI's priority list. The IPSI 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 IPSI'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.

No service timer

During survivable core server administration, a value is entered for the no service timer. The value administered for the no service timer determines the amount of time the IPSI waits to request service from another server. The IPSI may be requesting service from a survivable core server after the IPSI loses communication with the main server or the controlling survivable core server. The interval from the activation of the no service timer to the time the IPSI requests service of a survivable core server is called the no service time out interval. The value for the no service timer is administrable from 2 to 15 minutes, with a default of five minutes. For more information on the no service timer, see After administering the survivable core servers.

Note:

The IPSI's no service timer starts when the IPSI loses service because it does not have socket connections to the main server and it is no longer being scanned.

Failover to a survivable core server

Existing Communication Manager recovery mechanisms still occur prior to a failover of a port network to a survivable core server. For example, if a main server loses control of a majority of

port networks it may attempt to switch to its survivable server. This would happen before an IPSI requests service from a survivable core server. The response to a typical failover is:

- The Main fails:
  - Duplicated servers:
    a. Failure of the active server causes a server interchange. The IPSI is still under control of the main server.
    b. Failure of both servers causes loss of communication to the IPSI. The IPSIs no service timer activates.
  - Single server:
    a. Failure of the main server causes loss of communication to the IPSI. The IPSIs no service timer activates.
- The IPSI:
  - Duplicated IPSI:
    a. Loss of communication between the active IPSI and the main server causes the IPSI to interchange.
    b. Loss of communication between both IPSIs and the main server causes the IPSIs no service timer to activate.
  - Single IPSI:
    a. Loss of communication between the IPSI and the main server causes the IPSIs no service timer to activate.
- During the no service time out interval, other existing failure recovery mechanisms continue to be exercised.
  - If the server that last controlled the IPSI reconnects with the IPSI before the no service timer expires, the IPSI will immediately request service from that server.
- If the no service timer expires, the IPSI requests service from the highest ranking survivable core server on its priority list.

As part of a failover, the survivable core server resets the port networks that it now controls. The port network performs a restart. During a restart:

- Every call is dropped.
- Administrative sessions are dropped.
- Every application and system link is dropped and re-established.
- Non-translation feature data, such as Automatic Wakeup calls, are lost and must be re-entered.
- Every login, including remote access and system port logins, is dropped.
- Every hardware component is reset except:
  - Active TN2312 IPSI in any port network

  - DS1 clocks
- Every busied-out maintenance object is released and can be re-busied.
- Circuit packs are re-initialized and translations are verified.
- For a critical-reliability system (duplicated PNC), a global refresh of the standby PNC is performed after the reset.

Depending on the type of failure and how the survivable core servers are configured, an individual survivable core server can accept control of all the port networks, several of the port networks, a single port network, or no port networks. When a LAN or WAN failure occurs in configurations where port networks are widely dispersed, multiple survivable core servers may be required to collectively accept control with each survivable core server controlling some portion of the set of port networks. When a survivable core server accepts control, survivable core server communicates directly with each port network through its IPSI circuit pack.

Once the issue that caused the failover is resolved, you can put the control of an IPSI port network back to the main server. The main server can assume control of port networks all at once or one at a time. The following command options allow the port networks to return to the main server:

- All at once:
  - **Auto Return**: The **Auto Return** field in the **System-Parameters Port Networks** screen provides three options, **no**, **yes**, and **scheduled**. Two of the options, **yes** and **scheduled**, allow the port networks to return to the main server all at once:
    - **Scheduled**: You can schedule a day and a time for the return of all the IPSI port networks to the control of the main server. This option is administered on the main server up to seven days before the requested fall-back occurs. For more information, see Administering survivable core server.
    - **Yes**: The port networks automatically return to the control of the main server if a **yes** is entered in the **Auto Return** field. In the **IPSI Connect Up time** field, enter the amount of time from 3 to 120 minutes. If the IPSI and the main server stay connected for the duration of the time administered in the **IPSI Connect Up time** field, the port networks automatically fall-back to the control of the main server. For more information, see Administering survivable core server.
  - **`get forced-takeover ipserver-interface all`**: The **`get forced-takeover ipserver-interface`** SAT command with the **`all`** parameter, allows a survivable core server or main server to manually take control of all the IPSI port networks at once. This command must be issued from the survivable core server or the main server that intends to take control of the port network(s). For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431.
- One at a time:
  - **`get forced-takeover ipserver-interface port-network [1-64]`**: The **`get forced-takeover ipserver-interface port-network`** SAT command followed by the port network number, provides the capability for a survivable core server or main

server to manually take control of one IPSI port network. The command must be issued from the survivable core server or the main server that intends to take control of the port network. For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431.

Note:

When the main server resumes control of a port network, the port network performs a restart.

Processor Ethernet overview

Processor Ethernet (PE) is used for IP connectivity. You use C-LAN and Processor Ethernet in one configuration. The introduction of Processor Ethernet does not change the use or the functionality of the C-LAN.

Note:

Communication Manager IP endpoints can register either to PE or to CLAN ip-interfaces. PE resides on Communication Manager server and CLAN resides on any of the port network. Communication Manager can have one PE and multiple CLANs. PE and CLAN ip-interfaces are associated with the ip-network-regions.

When configuring Communication Manager on a server, the Processor Ethernet 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 Processor Ethernet interface.

The Processor Ethernet interface is enabled by default in the license file. The feature keyword FEAT_PRETH must be checked to *ON* in the license file for Processor Ethernet 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 Processor Ethernet 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 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 Processor Ethernet interface to register to the main server. Do not disable the Processor Ethernet interface.

The following table shows how the Processor Ethernet functionality works on main servers and survivable core servers.

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 Processor Ethernet interface.	The use of the Processor Ethernet interface for registration to the main is automatically enabled by the Communication Manager software. The Processor Ethernet interface needs to be configured on the System Management Interface.
Gateway registration	Administration to allow H.248 registration on the Processor Ethernet interface of a main server is performed on the **IP Interfaces** screen.	Administration to allow H.248 registration on the Processor Ethernet interface of a survivable core server is performed on the **Survivable Processor** screen.
H.323 endpoint registration	Administration to allow H.323 registration of the Processor Ethernet interface of a main server is performed on the **IP Interfaces** screen.	Administration to allow H.323 registration on the Processor Ethernet interface of a survivable core server is performed on the **Survivable Processor** screen.
Adjunct connectivity	All adjuncts are administered on the **IP Services** screen on the main server. ● You can use the Processor Ethernet 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 Processor Ethernet 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.

1. If you connect the gateways to Processor Ethernet on the main server because there are no C-LANs in the system, the gateways should have the Processor Ethernet 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.

For more information on how to administer the Processor Ethernet interface, see Administering page one of the Survivable Processor screen.

Support for Processor Ethernet and Port Networks on a survivable core server

Survivable core servers support connection of IP devices to the Processor Ethernet interface as well as to C-LAN interfaces located in the port networks.

A survivable core server uses its Processor Ethernet interface to support IP devices such as Branch Gateways, H.323 Media Gateways, IP Adjuncts, IP telephones, IP trunks, and SIP trunks. The survivable core server optionally controls port networks (G650 Media Gateways) through IPSI at the same time. When there are no port networks in the configuration, survivable core server may provide the equivalent benefit of a survivable remote server. The survivable core server can be duplicated, providing additional redundancy to the survivability of the system.

For Processor Ethernet on duplex servers to work, you must assign the Processor Ethernet interface to the PE Active Server IP Address (IP-alias) and not the server unique address. The NIC assigned to the Processor Ethernet interface must be on a LAN connected to the main server.

- If the survivable server registers to the C-LAN on the main server, the C-LAN must have IP connectivity to the LAN assigned to the NIC used for Processor Ethernet on the survivable core 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 assigned to the NIC used for Processor Ethernet on the survivable core server.

Firmware for optimal performance

Processor Ethernet on duplex servers works effectively only when the gateways and IP telephones are on the most current release of firmware.

Avaya recommends that you use the following IP telephone models to ensure optimal system performance when you use Processor Ethernet on duplex servers.

- 9610, 9620, 9630, 9640, and 9650 telephones with firmware 3.0 or later; any future 96xx models that support Time to Service (TTS) will work optimally.

- 4601+, 4602SW+, 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW Broadcom telephones with firmware R 2.9 SP1 or later, provided the 46xx telephones are not in the same subnet as the servers.

All other IP telephone models will re-register in case of server interchange. The 46xx telephones will re-register if they are in the same subnet as the servers.

When PE is used on duplicated 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.

To ensure that you have the most current versions of communication devices, go to the Avaya Support website, http://avaya.com/support. Click **DOWNLOADS & DOCUMENTS** and select the product.

C-LAN access for survivable core server registration

During the survivable core server configuration, an IP address of a C-LAN is used. The survivable core server uses this configured C-LAN IP address during the initial registration with the main server.

Plan carefully when using a C-LAN in a survivable core server configuration. The C-LAN should be local to the survivable core server or of high availability to the survivable core server. During the initial registration to the main server, the survivable core server does not contain translations and therefore has no knowledge of other C-LAN circuit packs in the configuration. If the survivable core server cannot communicate with the configured C-LAN circuit pack it will be unable to register with the main server.

When a survivable core server registers with the main server through the C-LAN, the main server validates the survivable core server Module ID, System ID, platform type, and IP address with that of the administered values. Only the active server of a duplicated server pair registers with the main server. Once registered, the survivable core server uses the same C-LAN connection it used to register to send Keep-Alive messages to the main server.

Important:
The C-LAN must be set to allow H.323 endpoints on the **IP Interfaces** screen for a survivable core server to register to the main server.

The survivable core server re-registers with the main server when:

- Translations are received from the main server: The survivable core server performs a reset after receiving translations from the main server. During the reset the survivable core server stops sending Keep-Alive messages.

  Once translations are loaded on the survivable core server, the survivable core server re-registers with the main server. The survivable core server attempts to use the C-LAN in its configuration for the registration process.

  If a C-LAN is used in the configuration and communication with the configured C-LAN is not available, the survivable core server selects a C-LAN from its list of available C-LANs. The survivable core server re-registers to the main server through the available C-LAN and, after registration, uses the C-LAN to send Keep-Alive messages to the main server.

  Note:

  If a survivable core server is still registered with the main server while controlling port networks, the survivable core server can receive translation downloads from the main server. In this case, the survivable core server accepts the translation download but does not reset until it no longer controls a port network.

- The C-LAN reboots or fails: If the C-LAN that the survivable core server used to register to the main server reboots or fails, the Keep-Alive messages from the survivable core server to the main server stops. The main server shows the status of the survivable core server as unregistered in the ESS Cluster Information screen. The survivable core server attempts to communicate with the lost C-LAN. If attempts to communicate with the lost C-LAN fails, the survivable core server selects another C-LAN from its list of C-LANs.
- The port network containing the C-LAN reboots or fails: If the port network containing the C-LAN that is used by the survivable core server to register to the main server reboots or fails, the Keep-Alive messages from the survivable core server to the main server stops. The main server shows the status of the survivable core server as unregistered in the ESS Cluster Information screen. The survivable core server attempts to re-connect to the C-LAN. It the attempts fail, the survivable core server selects another C-LAN from its list of C-LANs.
- The Network experiences problems: If network problems prohibit communication between the survivable core server and the C-LAN, the Keep-Alive messages between the survivable core server and the main server terminates. The main server shows the survivable core server as unregistered in the ESS Cluster Information screen. If multiple C-LANs are used in this configuration, the survivable core server selects another C-LAN from its list and attempts to re-register with the main server using the new C-LAN.

Survivable core server requirements

A survivable core server configuration requires the following:

- The main server and each survivable core server must be running Communication Manager Release 6.0 or later.
- The main server can be an S8510 Server or an S8800 Server or an HP ProLiant DL360 G7 1U (HP DL360 G7) Server or a Dell™ PowerEdge™ R610 (Dell R610) Server. If the main server is an S8510 server, all survivable core servers must be S8510 servers. The capacities of the set of port networks a survivable core server can control must not exceed the published capacities of the survivable core server. For more information on system capacities, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.
- Minimum vintage IPSI firmware: To identify the firmware needed for an IPSI in a survivable core environment, see the Minimum Firmware/Hardware Vintages document at http://support.avaya.com.
- The license file for the main server covers the survivable core server.
- An IP network that provides connectivity for all IPSIs and servers.
- For duplicated IPSI control, the S8510 server must be equipped with a dual NIC card.

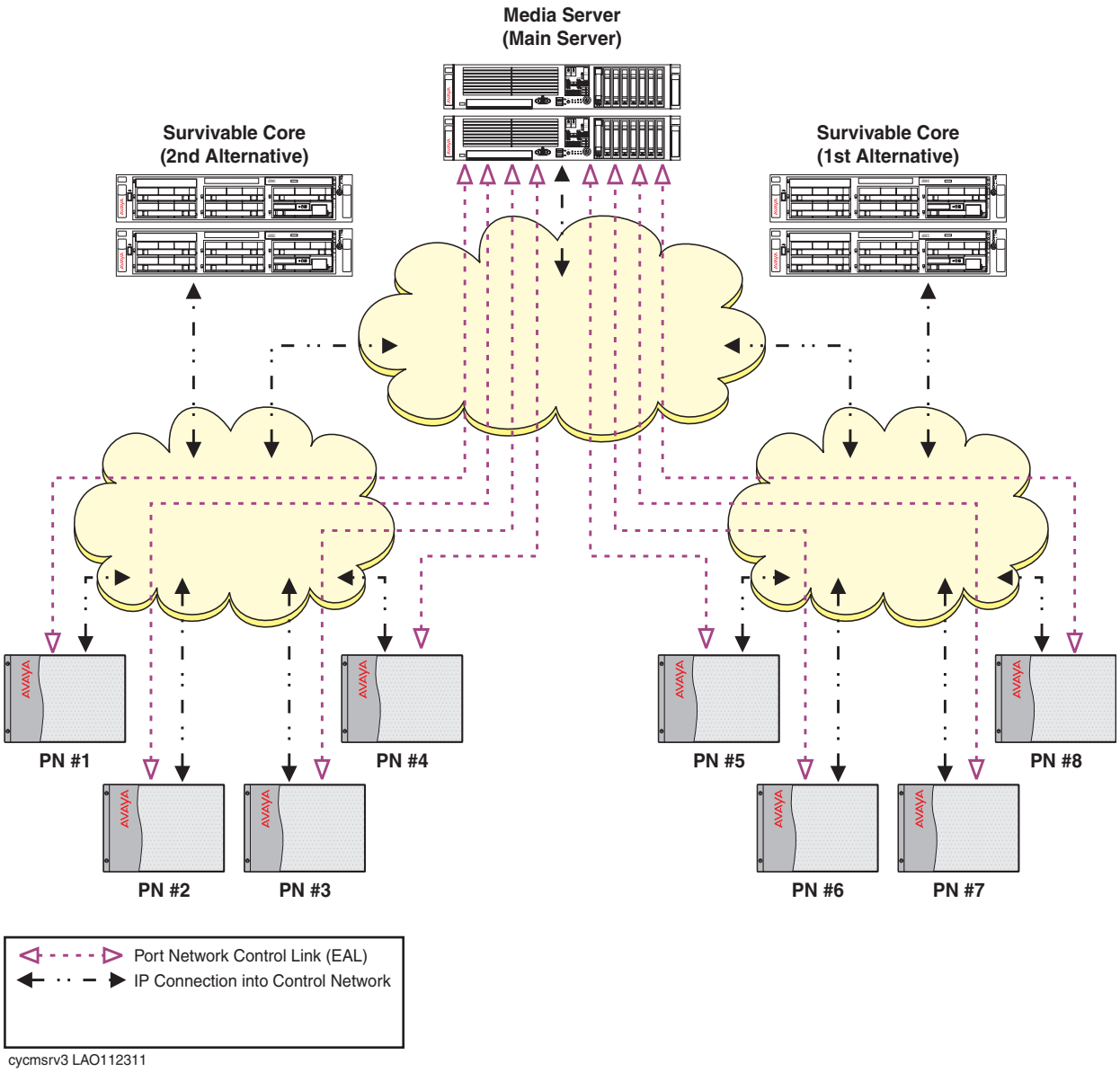
Survivable core server failover examples

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

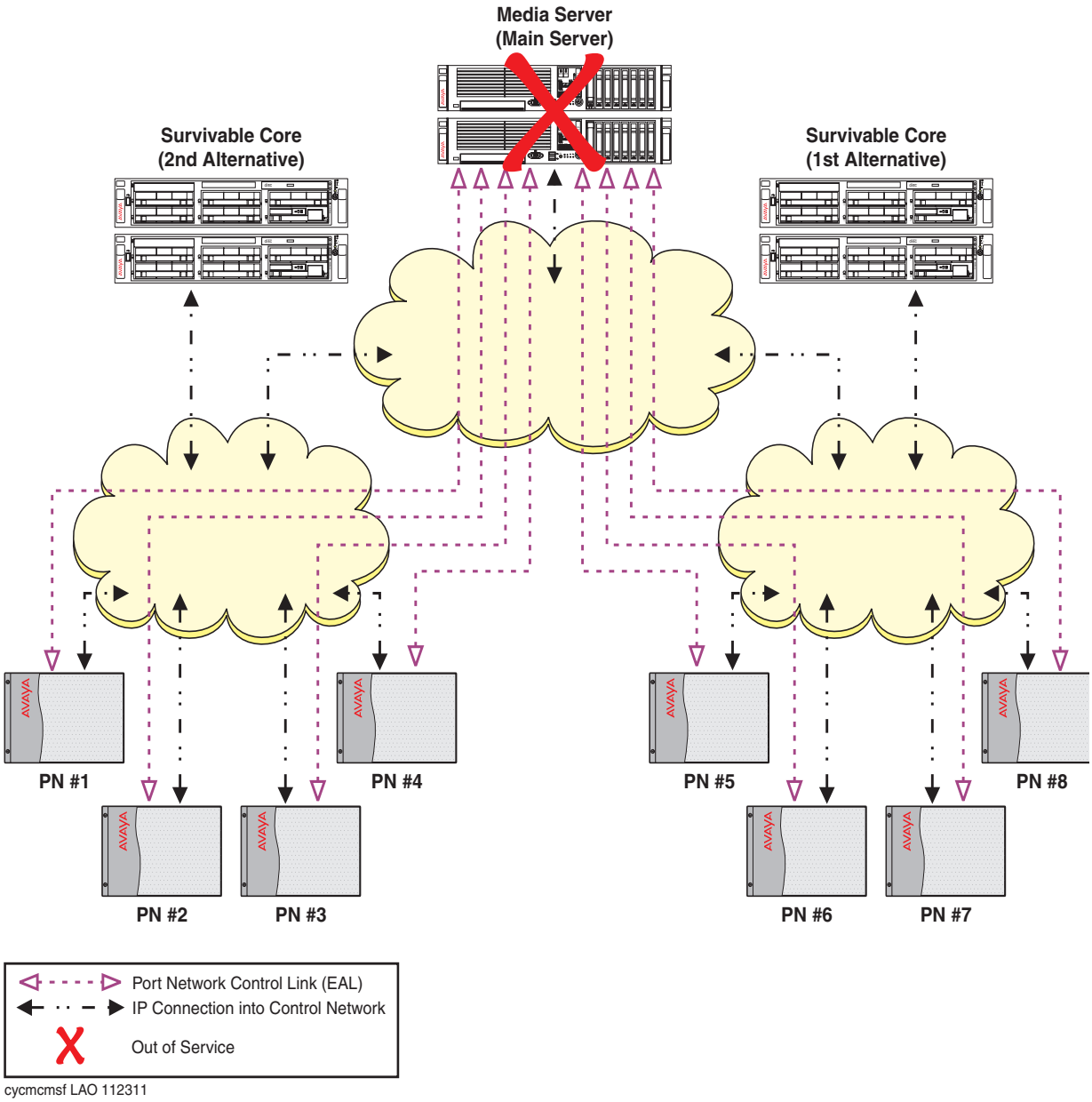
In example one (Figure 1), the duplicated server is acting as the main server in a survivable core server environment. Two survivable core servers have been positioned in the network. Through administration on the main server, another duplicated server is selected as the primary backup or 1st alternative 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 port networks under the control of a single server.

Figure 1: S8800 Server with survivable core servers in normal operation



A catastrophic failure occurs on the main servers (Figure 2). The IPSI in each port network can no longer communicate with the main server. The no service timer activates.

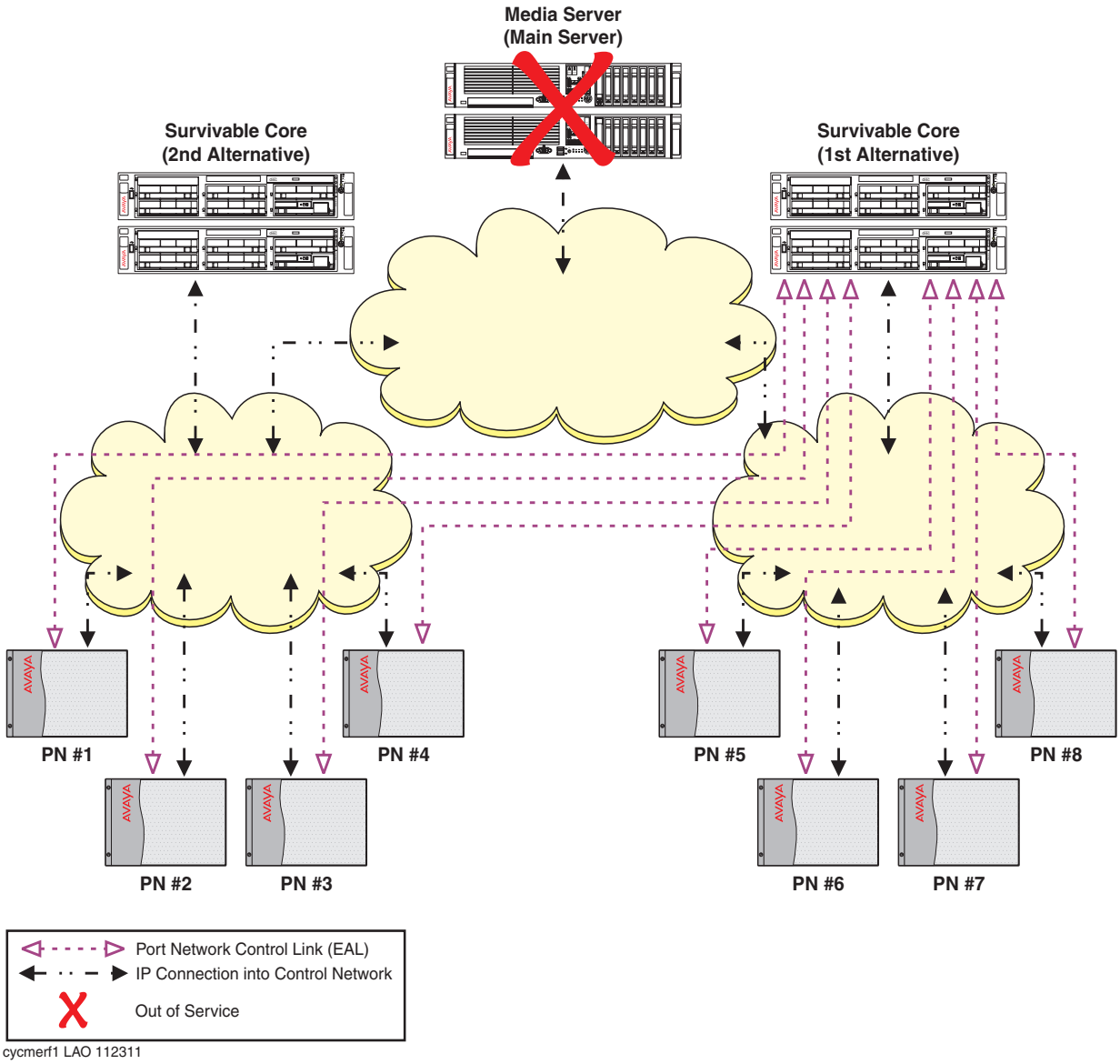
Figure 2: Catastrophic main server failure



When survivable core server was administered on the main server, the 1st alternative server received higher values than the 2nd alternative server. The administered values of the survivable core servers are assigned to the IPSIs in the configuration. Based on the values of the survivable core servers, the IPSI placed the 1st alternative survivable core server higher on its priority list then the 2nd alternative survivable core server.

The no service timer expires (Figure 3), the IPSIs 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 IPSI controlled port networks.

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

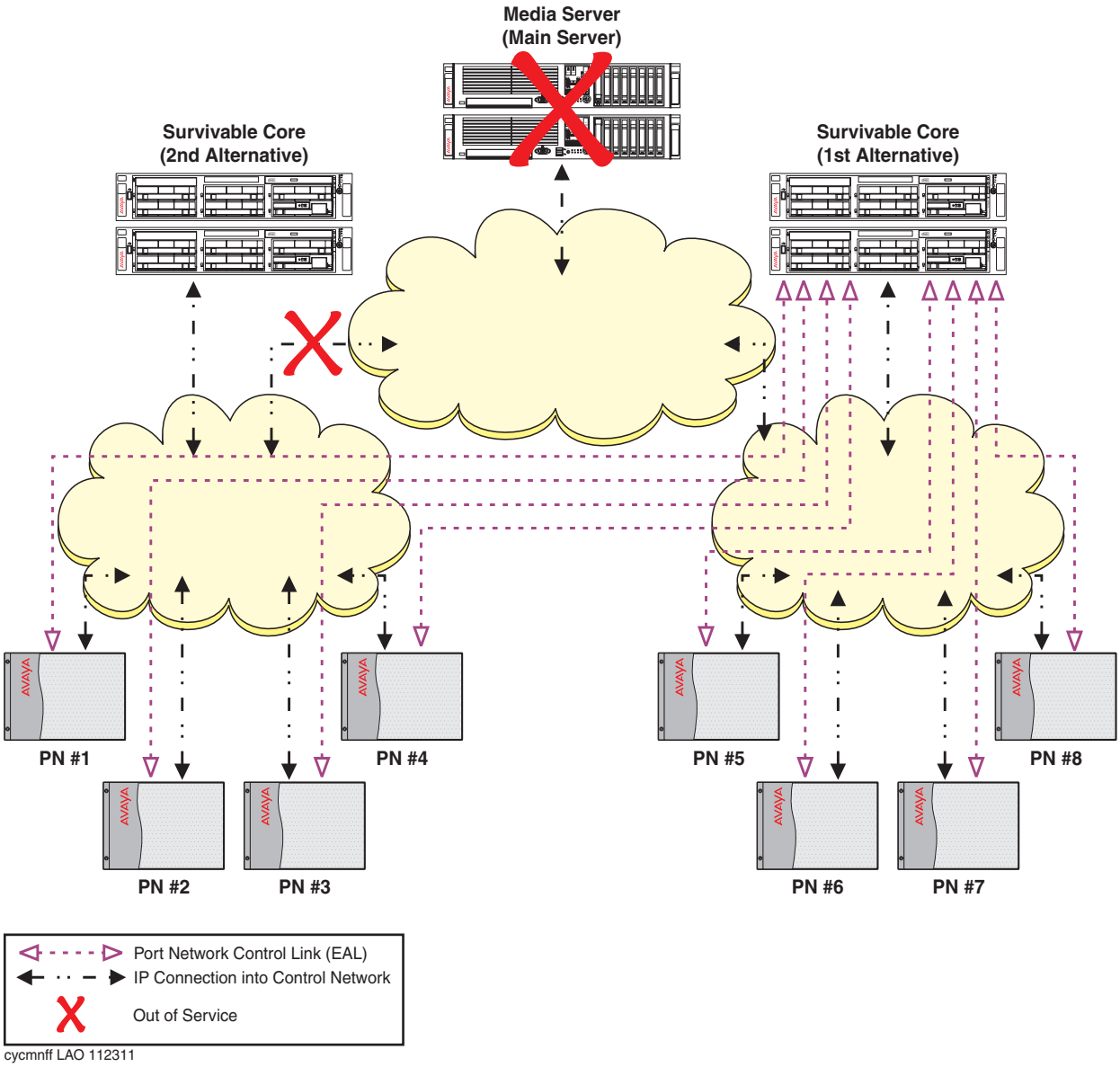


Example two: Network failure

Example two uses the same configuration used in example one. The S8800 Server is the main server, with two S8800 survivable core servers (1st alternative and 2nd alternative). Due to a catastrophic failure the main server is out-of-service. All port networks are now controlled by the 1st alternative survivable core server.

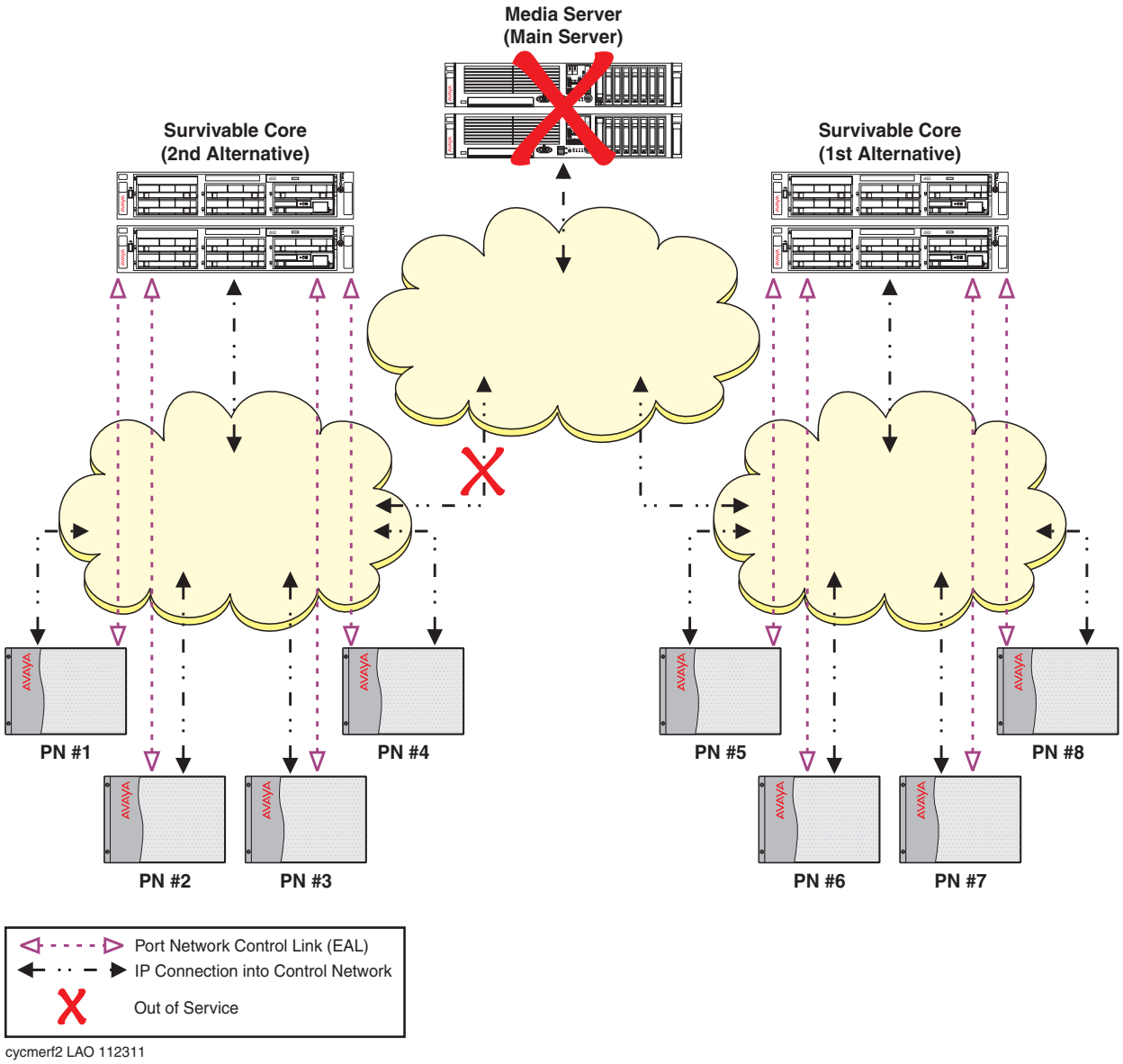
Up to this point this is the same scenario as example one. Now, the customer experiences a network outage resulting in fragmentation of the network (Figure 4). Port networks one through four can communicate with the 2nd alternative survivable core server but can no longer communicate with the main server or the 1st alternative survivable core server. Port networks five through eight can still communicate with the 1st alternative survivable core server but can no longer communicate with the 2nd alternative survivable core server.

Figure 4: Network fragmentation failure



Because the IPSIs in port networks one through four are not 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 no service timer activates for port networks one through four. When the no service timer expires, the IPSIs in port networks one through four request service from the 2nd alternative server. The 2nd alternative server acknowledges the request and assumes control of port networks one through four (Figure 5). Note that port networks five through eight did not experience any service outage from the failure.

Figure 5: Network failure - Survivable core server recovery



The users in port networks one through four experience the following:

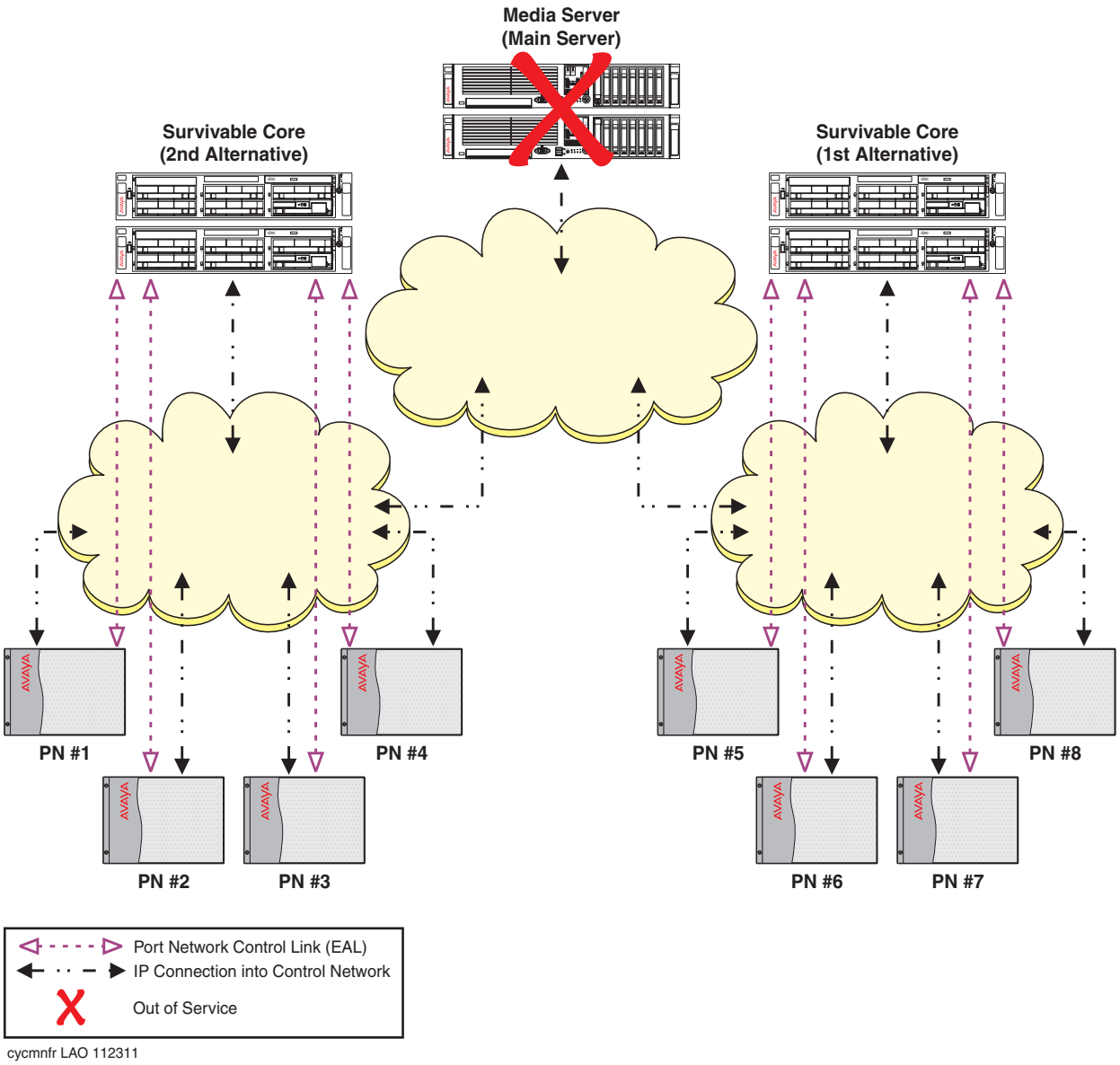
- During the no service timer interval:
  - Stable calls remain up in the state they were in before the outage occurred. The stable calls do not have access to any features such as hold, conference, etc. The state of the stable call cannot be changed.
  - Users attempting to originate a telephone call, 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 circuits are busy.

- After the no service 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.

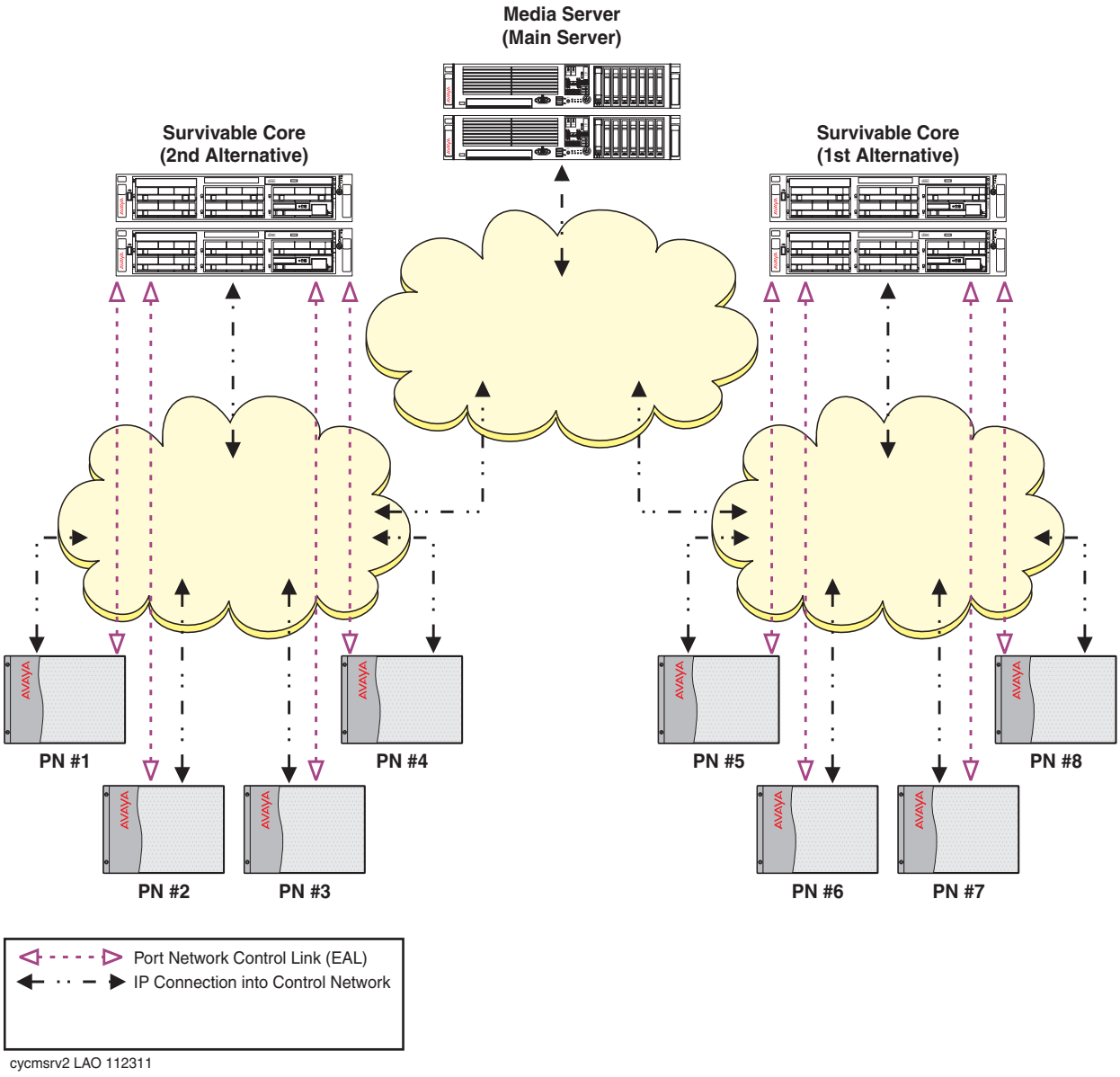
The customer is now in the process of recovering from both the network failure and the main server failure (Figure 6). As the network failure is fixed, the IPSIs in port networks one through four can now communicate with the 1st alternative server. The IPSI priority list adjusts to reflect the 1st alternative as the highest priority server. Even though the IPSI priority list now shows the 1st alternative server as its highest priority survivable server, the port networks do not automatically return to the control of the 1st alternative server. Moving the port networks requires manual intervention using the **`get forced-takeover ipserver-interface`** command or scheduling the Auto Return functionality. For more information on the **`get forced-takeover ipserver-interface`** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431. For more information on the Auto Return functionality, see After administering the survivable core servers.

Figure 6: Network fragmentation recovery



The main server is now restored (Figure 7). The IPSIs in the port networks can now communicate with the main server and each survivable server. The main server is always the highest priority on any IPSI priority list.

Figure 7: Main server recovery

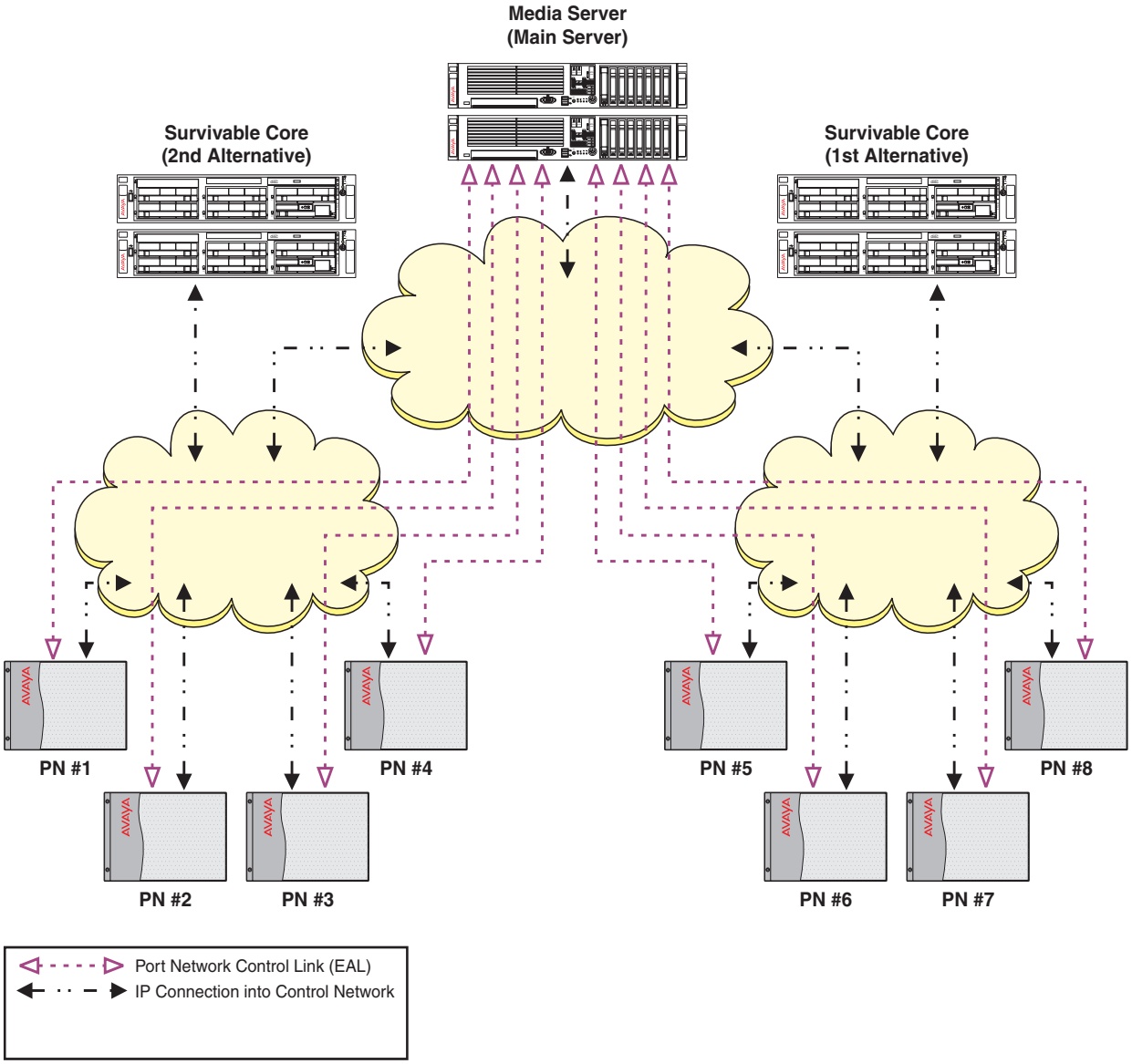


The customer is now ready to have the main server control the configuration (Figure 8). Moving the port networks back to the control of the main server can be accomplished by one of the following:

- Moving each port network individually using the **`get forced-takeover ipserver-interface port-network [N]`** (where N is the number of the port network) command.

- Moving all port networks at one time using the `get forced-takeover ipserver-interface all` command.
- Administering the Auto Return capability on the main server (Administering survivable core server).

Figure 8: Fall-back to main server



cycmsrv3 LAO112311

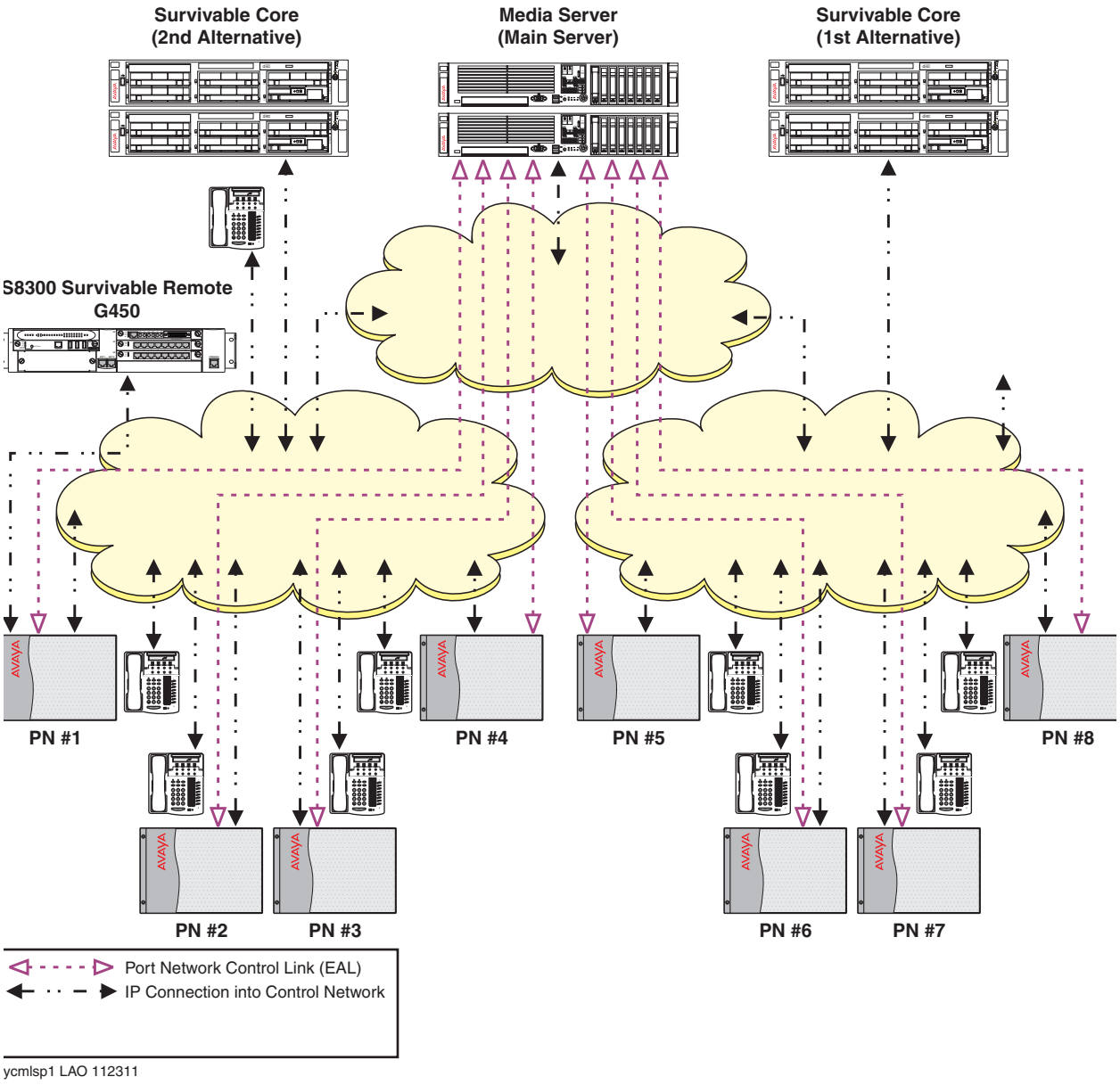
Example three: A survivable remote server working in a survivable core server environment

In example nine (Figure 9), there is an S8300 survivable remote server residing in a G450 Branch Gateway. Main server communicates with the G450 through a C-LAN circuit pack to which G450 is registered.

Two survivable core servers are administered. The 1st alternative survivable core server has the highest priority and is the first survivable core server the IPSI requests service from if it can no longer communicate with the main server. If the IPSI can’t communicate with either the main server or the 1st alternative survivable core server, it will request service from the 2nd alternative survivable core server.

The goal of this configuration is to have all port networks and gateways under the control of one survivable core server.

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



ycmlsp1 LAO 112311

In a survivable core environment, a no service timer activates when the IPSI can no longer communicate with the main server or the controlling survivable core server. The no service timer is administrable and can be set from three to 15 minutes.

Because of a catastrophic main server failure, port networks one through eight can no longer communicate with the main server. The no service timer activates. After the no service time out

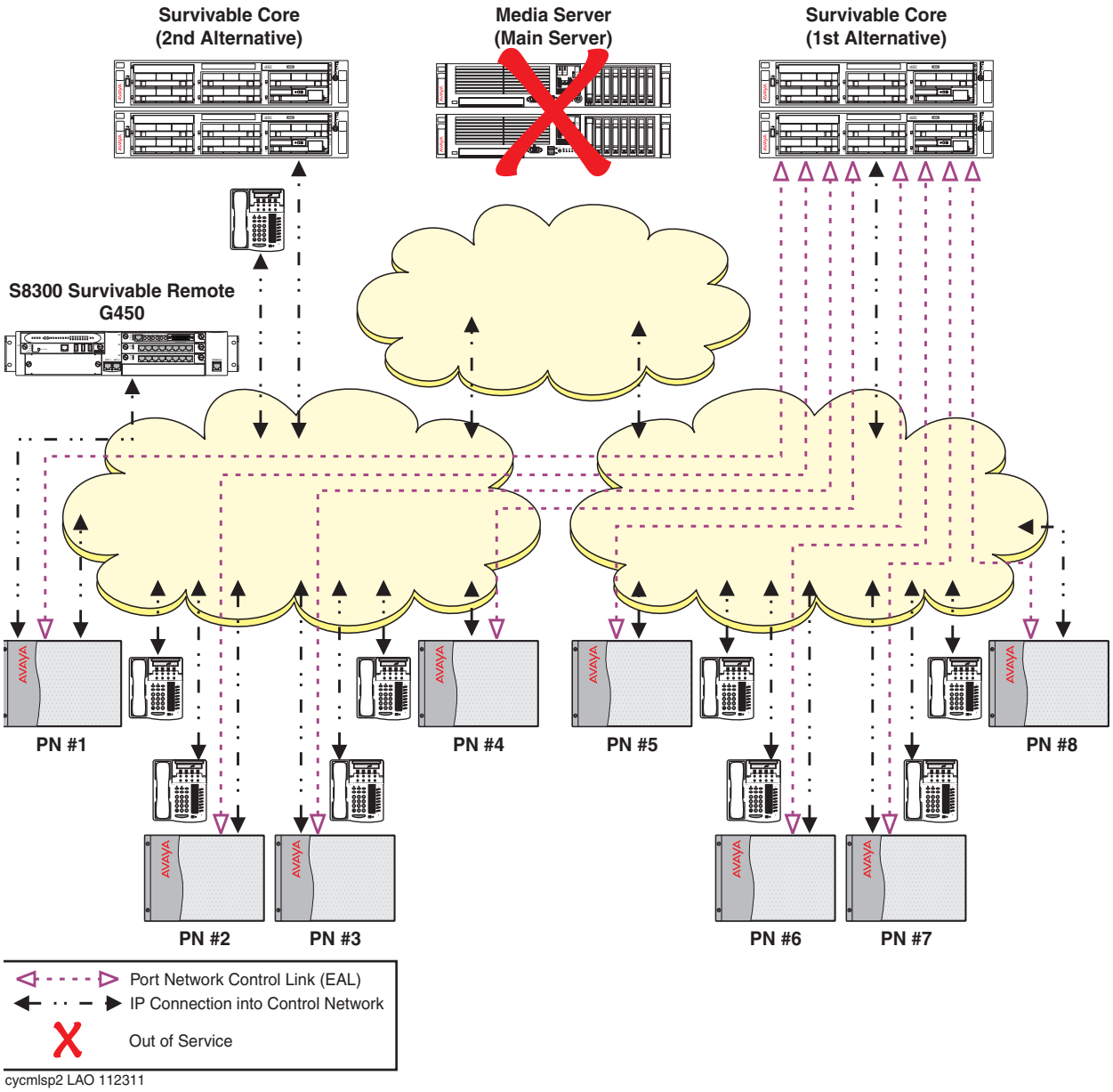
interval expires, the IPSIs in port networks one through eight request service of the 1st alternative survivable core server.

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.

If the gateway registers with a C-LAN, which would be in the main server portion of the MGC list, the port networks IPSI might be registered with the survivable core. However the gateway does not know that and treats it as a main server.

In Figure 10 the gateway was able to register with the survivable core server through the C-LAN in port network one to the 1st alternative survivable core server before the Primary Search Timer expired. For more information on Primary Search Timer, see Primary Search Timer.

Figure 10: Survivable remote server working in a survivable core server environment - ESS timer before Primary Search Timer

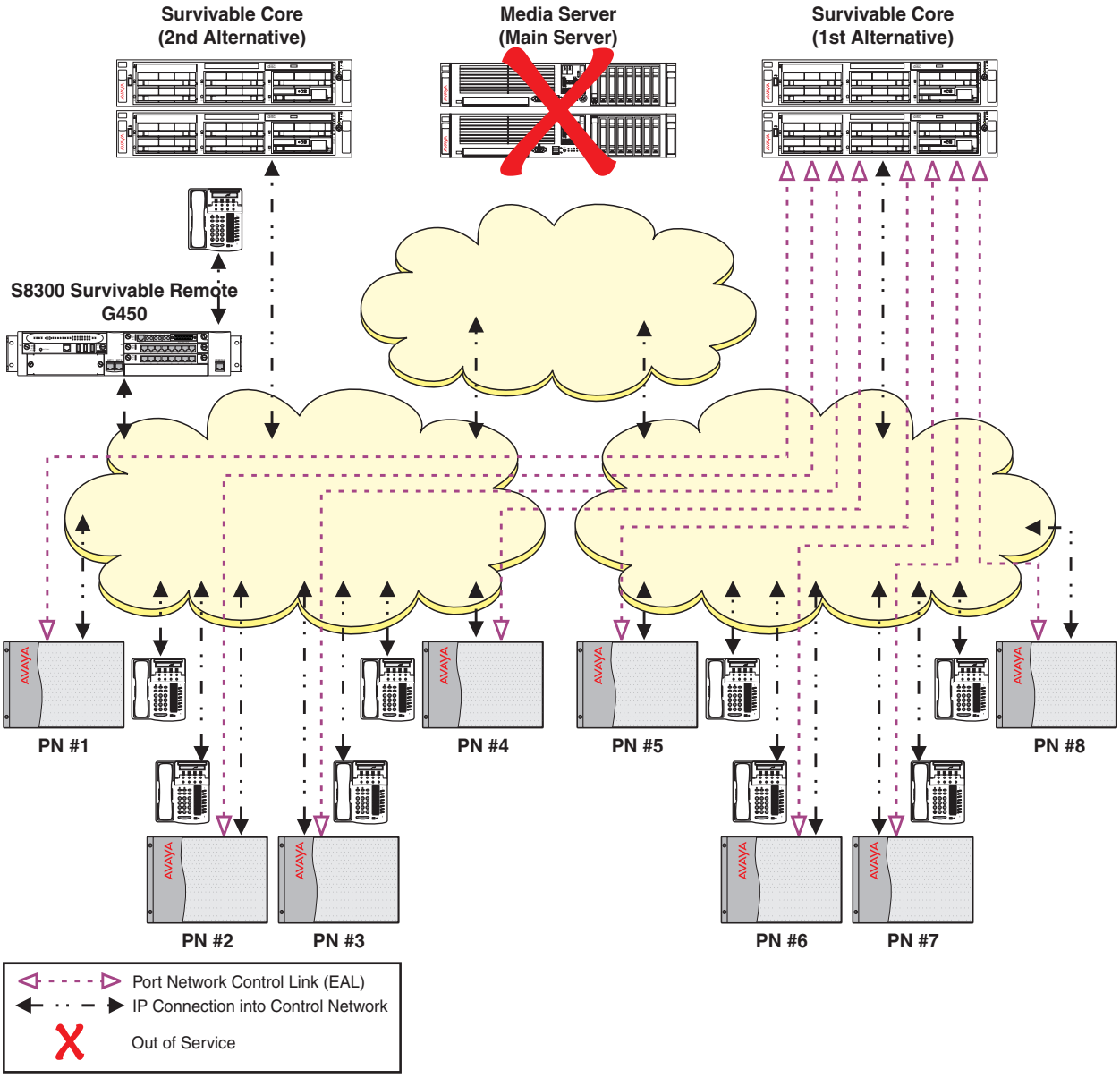


Using a different scenario, in Figure 11 the Primary Search Timer expired before the survivable core server no service timer. The IP telephones and the G450 Branch Gateway connects to the survivable remote server. The no service timer expires and the IPSIs in port networks one through eight request service from the survivable core server.

The system is now fragmented between two controlling servers.

- Some functionality provided by adjuncts may be missing for users registered with the survivable remote server. For more information on adjuncts, see Feature considerations.
- Users registered with the survivable remote server may not be able to make normal station-to-station calls to port networks controlled by the survivable core server.

Figure 11: Survivable remote server working in a survivable core server environment - Primary Search Timer before survivable core server timer



cycmlsp3 LAO 112311

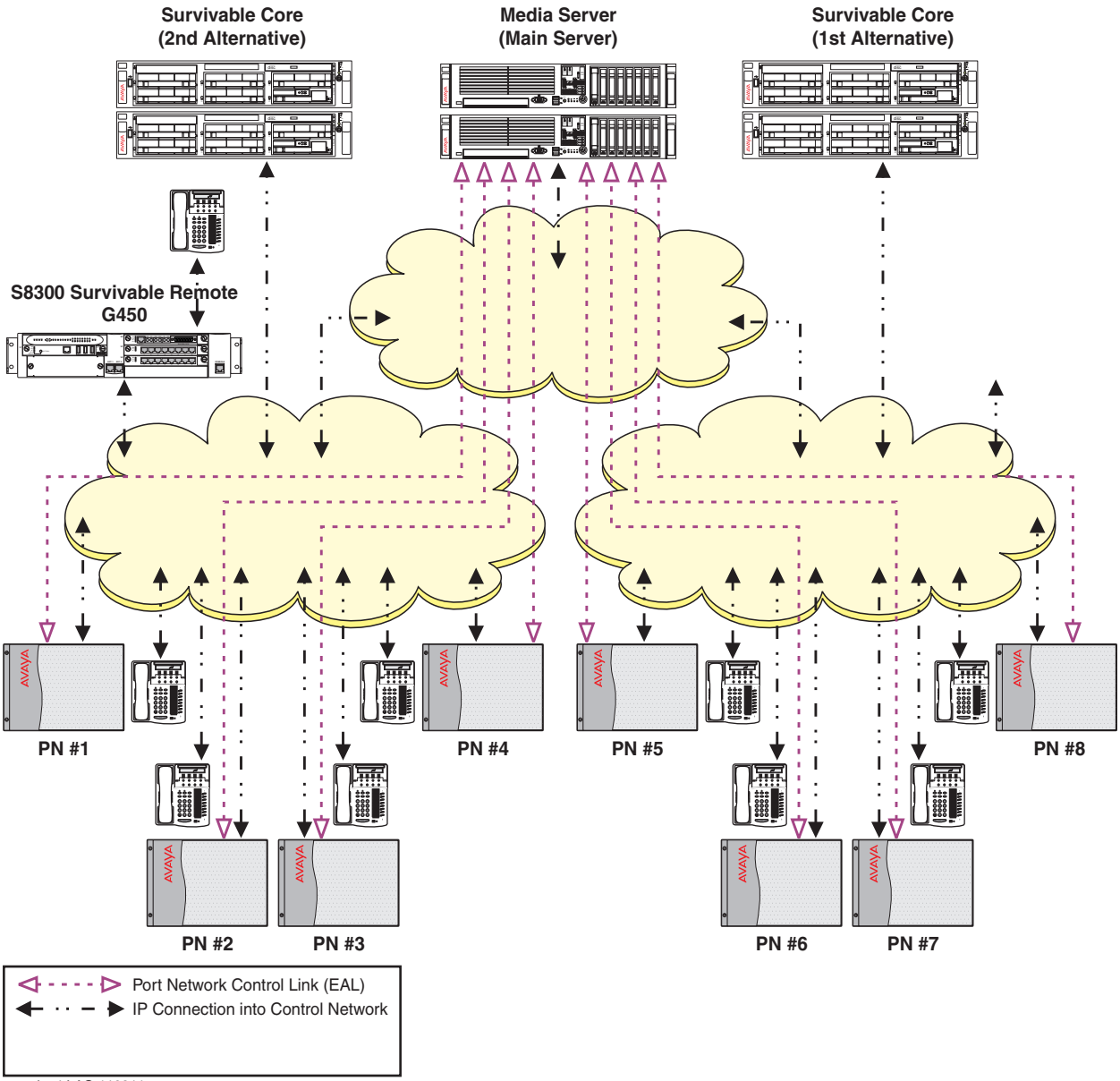
The problem that caused the main server outage has been fixed (Figure 12). All port networks can now communicate with the main server. Using the Auto Return functionality, the administrator scheduled the return of all port networks to the main server.

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.

Note:

This only applies for gateways that are registered to the survivable remote server as illustrated in Figure 12.

Figure 12: Survivable remote working in a survivable core environment - fall-back to the main server



cycmlsp4 LAO 112311

Chapter 2: Survivable Core Server design and planning

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

Upgrading to Release 6.0 and later (Release 6.x) is different than previous releases upgrades because Release 6.x of Communication Manager is an application that resides on a virtual server. The underlying framework is called System Platform, and Communication Manager is a template that runs on System Platform.

Because Communication Manager Release 6.x, runs on only five servers, most upgrades require replacing the existing server with an Avaya S8800 Server (standalone) or Avaya S8300D Server (embedded) or HP ProLiant DL360 G7 1U (HP DL360 G7) Server or Dell™ PowerEdge™ R610 (Dell R610) Server. Although Release 6.x runs on an Avaya S8510 server and an Avaya S8800 Server, it is no longer being sold. However, S8510 and S8800 Servers are still supported. Communication Manager Release 4.0.5 or Release 5.2.1 or Release 6.0.1, can be upgraded to Release 6.x on the Avaya S8300D Server, Avaya S8510 Server, Avaya S8800 Server, HP DL360 G7 Server, and Dell R610 Server. The S8510 and S8800 servers require a hardware upgrade as part of the process.

Note:

Before upgrading to Release 6.x, all servers must be either on Release 4.0.5 or Release 5.2.1. Any servers that are not on Release 4.0.5 or Release 5.2.1 must be upgraded to Release 4.0.5 or Release 5.2.1 before upgrading to Release 6.x.

For more information about the process and procedures for upgrading Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.x, see *Upgrading to Avaya Aura® Communication Manager*, 03-603560.

Survivable core server design strategy

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

1. Avoiding fragmentation of the system: The survivable core server controls as much of the system as possible.
2. 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 port networks. In this way, a survivable core server can

potentially assume control of a single port network or a group of port networks 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 further details on administered values and communities, see Administering a survivable core server on the main server.

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: In this book, 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

Detailed planning for survivable core server is mandatory. Certain information must be gathered to facilitate the implementation of this feature:

- **IP address(es)**: Obtain the following IP addresses:
  - Main server
  - Survivable core server(s)
  - C-LAN circuit pack(s)
  - Default gateway(s)
  - Control network
  - NIC card(s)
  - IPSI(s)
  - Subnet mask(s)

  Note:

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

  The IP addresses listed above 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 Administering survivable core server.

- **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.
- **License files**: Each survivable core server shares the main server's license file. For security purposes, PLDS requires that each license file have a MAC address.
- **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 Table 3 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
20	ftp data	
21	ftp	
22	ssh/sftp	
23	telnet server	
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. For more information on survivable core server registration, see C-LAN access for survivable core server registration.
1024 and above	Processor Ethernet	TCP outgoing
1956	Command server - IPSI	
2312	Telnet firmware monitor	
5000 to 9999	Processor Ethernet	TCP incoming
5010	IPSI/Server control channel	
		1 of 2

Table 3: Open ports (continued)

Port	Used by	Description
5011	IPSI/Server IPSI version channel	
5012	IPSI/Server serial number channel	
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).
		2 of 2

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* turned on and *Enterprise Survivable Server* turned off.
- **Translations**: You can change translations on a survivable core server but you *cannot* save them. This is true even if the survivable core server is providing service to an IPSI. 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 IPSI'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 Administering survivable core server.
- **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 detailed information on system capacities, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.
- **Control Network duplication**: When used as a survivable core server, the single server can support one or more port networks with single IPSI or duplicated IPSI.
- **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 Use of Processor Ethernet interface on main servers and survivable core servers.

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 ISDN PRI non facility associated signaling

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

1. Whenever possible place both D-channels in one port network.
2. If it is not possible to place both D-channels in one port network, place the D-channels within port networks where:
   - The port network has an IPSI.
   - The port networks are most likely to failover to the same survivable core server.
3. After failover, if the D-channels are being serviced by two different survivable core servers:
   - Perform the `get forced-takeover ipserver-interface` command if the network conditions allow bringing both port networks under the same survivable core server.
   - Busy-out one D-channel to prevent thrashing with the Central Office if network fragmentation will not allow one survivable core server to provide service to the port

networks containing both D-channels. On the SAT of the server, use the **`busyout port x`** (where X is the location of the port) to busy-out the D-channel.

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 port networks or gateways in one or more network regions where IGAR is administered, IGAR continues to work. However, if port networks 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 port networks administers each port network in a separate network region (one through eight). IGAR is administered between all eight regions. A network fragmentation failure occurs. Port networks one through four failover to survivable core server one. Port networks five through eight failover to Local Only survivable core servers. survivable core server one uses IGAR to establish inter-port network bearer between port networks one through four. Each Local Only survivable core server controls one port network (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 and an IPSI. There can be a single call control connection or duplicated call control connections on a public or private network.

For more information on control networks, see *Administering Network Connectivity on Avaya Aura® Communication Manager* at http://support.avaya.com.

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** 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** fields display only if you enter **selected**.

IPSI priority list

The IPSI uses its priority list to determine available survivable core servers to failover to in the event of communication loss to the main server. The IPSI places the survivable core server on the priority list as each survivable core server assigns its values to the IPSI.

A survivable core server receives its values when it is administered on the main server using the **`survivable processor`** command. See Figure 13 for an example of the **Survivable Processor** screen.

Figure 13: Administering 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
```

Each IPSI maintains its own priority list of eight clusters (servers) in order of highest priority. The list contains one main server and seven survivable core server clusters. A maximum of 63 survivable core server clusters can be administered in one survivable core server configuration. A survivable core server cluster can be a simplex or a duplex pair of servers. If an IPSI receives an assigned value from a survivable core server cluster and its priority list is full, the ISPI checks the value of the displayed cluster against the values of the survivable core server clusters on the list.

If the assigned value of the survivable core server cluster:

- Is greater than one of the survivable core server clusters already on the list, the survivable core server cluster that is already on the list is removed and the newly assigned survivable core server cluster is added.
- Is less than the survivable core server clusters that are already on the list, the survivable core server cluster is not added to the list and the list remains the same. The rejected survivable core server cluster continues to assign to the IPSI until the IPSI accepts the survivable core server cluster on the list.

Note:

The **`status ess port-networks`** command is used to display the status of all the port networks known to the server on which the command is run. For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431.

Based on the administered community of a particular IPSI port network, each IPSI may have a different list of available survivable core server clusters. Since the main server defaults to the highest priority in a system, the main server holds the highest position on any IPSI's list. The value for the main cluster is not administrable and can never be changed.

In the **Survivable Processor** screen, each survivable core server is administered with one of two preference settings, System Preferred (**Sys Prf** field) and Local Preferred (**Loc Prf** field). A survivable core server administered with either the System Preferred or the Local Preferred preference can assign to all the IPSIs in the configuration. The preference setting (System Preferred/Local Preferred), along with a community (**Comm** field) and a priority value (**Pri Scr** field), determines the server's priority on the IPSI's list.

The System Preferred preference has the highest *administered* value, followed by the Local Preferred preference, and then a survivable core server with no preference setting. The value for the Local Preferred preference is only used by the IPSIs within the same community as the survivable core server. When the survivable core server with a Local Preferred preference assigns to an IPSI outside of its community, the preference value is the same as a survivable core server with no preference.

Local Only works differently than preferences. While the System Preferred preference, the Local Preferred preference, and the survivable core server with no preference can connect to IPSIs in all communities, a survivable core server with Local Only administered can only connect to IPSIs within its community. If there are multiple Local Only servers within one community, either the priority value or setting the Local Preferred preference, can be used to rank one Local Only server above the other on the IPSI's list.

A survivable core server administered with both the Local Only and the Local Preferred preference will:

- Act like a Local Only server and only connect to IPSIs within its community.
- Have the preference value of a Local Preferred server.

Important:
It is important to note that the administration of Local Only, does not affect the priority of a survivable core server but does limit which IPSI list contains the Local Only server.

A priority value, entered in the **Pri Scr** column, is used to distinguish between survivable core servers with the same preference settings, survivable core servers with no preference setting, or survivable core servers that are not in the same community as the IPSI.

See Table 4 for a list of survivable core servers relative priorities in order from highest to lowest value.

Table 4: Survivable core server relative priority

Administered survivable core server type	Priority value impact
System Preferred server	System Preferred servers have a higher value than any other Local Preferred server *independent* of community or administered priority value. If multiple System Preferred servers are administered, the server with the highest administered priority value has the top priority on an IPSI's list.
Local Preferred servers in the same community	After the System Preferred preference, the Local Preferred preference has the second highest value within an IPSI community. If multiple Local Preferred servers are administered, the server with the highest administered priority value has the top priority on an IPSI's list.
Local Preferred and Local Only server in the same community	A survivable core server administered with both the Local Preferred preference and Local Only has the value of a Local Preferred server but can only connect to IPSIs within its community.
Local Preferred server outside its administered community	The Local Preferred preference has no value outside its administered community. When outside the administered community, the value of the Local Preferred server is based solely on its priority value.
Local Only server	A Local Only server only assigns to the IPSI within its community. The value of a Local Only server is based solely on its priority value. If a Local Preferred server (outside its administered community), or a survivable core server with no preference, assigns to an IPSI in the same community as a Local Only server, the priority score of each server would determine its ranking on the IPSI's priority list.
	1 of 2

Table 4: Survivable core server relative priority (continued)

Administered survivable core server type	Priority value impact
No preference server	The value of a survivable core server administered with no preference is based solely on its priority value. It is possible to administer all survivable core servers with no preferences. In this case, all survivable core servers would start out with the same value and a priority value would be used to rank the importance of the survivable core servers independent of communities.
	2 of 2

For more information on how to administer a survivable core server, see Administering a survivable core server on the main server.

Note:

In the case where there are two survivable core servers administered with the same type and the same priority score, the survivable core server with the lowest server ID will be ranked highest on the IPSI's list.

Assigning priority to an IPSI

A survivable core server assigns its priority to an IPSI:

- Every time it disconnects and reconnects to the main server. A survivable core server disconnects and reconnects to the main server after it receives translations from the main server, during a network outages, etc.
- When its priority changes.
- At periodic intervals if it is rejected by the IPSI.

Changes to a priority list

The IPSI priority list is dynamic and may change when:

- Communication is lost between a survivable core server and the IPSI: The survivable core server resets after receiving translations from the main server. When the survivable core server resets, communication between the survivable core server and the IPSI is lost. The IPSI adjusts its priority list, removing the survivable core server from the list. When the survivable core server re-establishes communication with the IPSI, the survivable core server will regain its proper order on the list.

- A survivable core server cluster is deleted: The survivable core server cluster was removed from translations.
- A survivable core server cluster with a higher value than a survivable core server cluster on the list assigns its value to the IPSI. In this case the survivable core server cluster with the lowest value is removed from the list and the newly assigned survivable core server cluster is added.

  Note:

  In a special case where the lowest priority cluster is controlling an IPSI port network, the second lowest priority cluster is rejected instead of the lowest priority cluster.

- **A survivable core server priority changes**: If the priority of the survivable core server cluster changes in the main server's translations:
  - The new translations are synchronized with the survivable core server cluster
  - The survivable core server cluster resets

  Note:

  A survivable core server cluster in control of an IPSI, will not reset when it receives new translations. The survivable core server cluster performs a reset to bring in the new translations after it is *no* longer in control of an IPSI.

  - The survivable core server cluster assigns its new priority to the IPSI.

You can view the IPSI's priority list by executing the **`status ess port-networks`** command on the main server's SAT. The IPSI's priority list can be found under the **Connected Cluster** heading. The list is in priority order, from left to right, using the Cluster ID of the survivable core server. The Cluster ID is always the same as the Module ID found in the license file and is used to identify the server. For example, in Figure 14 the priority list for the IPSI in port network two is, 50, 10, 99, 90, 80, 70, and then 30. For more information on **`ess port-networks`** field details, see Administering survivable core server.

Figure 14: status ess port-networks

```
status ess port-networks

Cluster ID 2             ESS PORT NETWORK INFORMATION

                  Port IPSI   Pri/  Pri/    Cntl Connected
   Com  Intf Intf Ntwk Gtway  Sec   Sec     Clus Clus(ter)
PN Num  Loc  Type Ste  Loc    Loc   State     ID IDs

 1  1   1A01  IPSI up   1A01  1A01  actv-aa    1   1
                              1B01  standby    1   1

 2  1   26A01 IPSI up   26A01 26A01 actv-aa    1   1
                              26B01 standby    1   1
```

Examples of how the priority list works

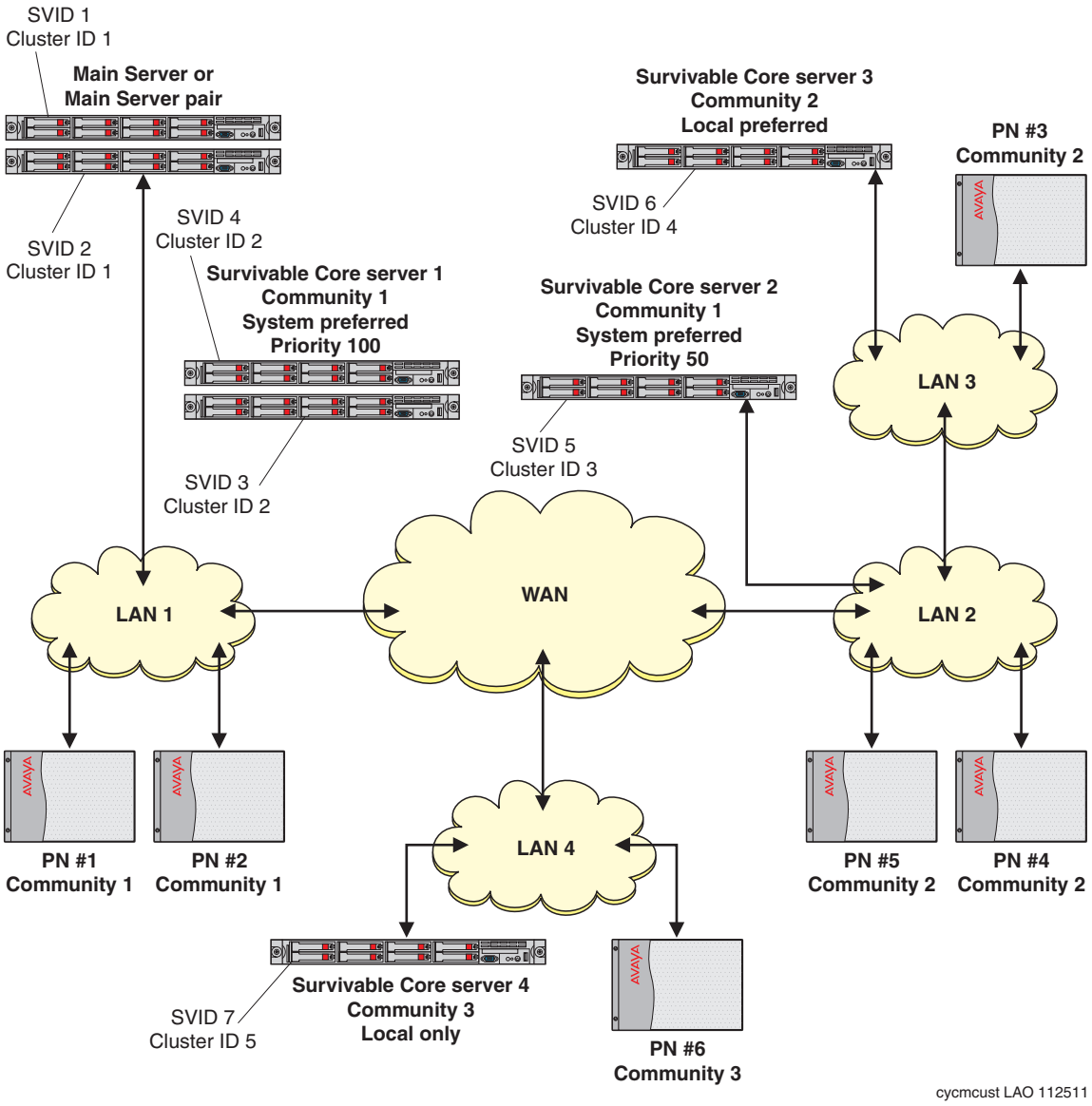
The following example demonstrates how the IPSI priority list is used during failover scenarios.

In this example, an IP connected system has five IPSI connected port networks and four survivable core servers. During the planning phase, the administrator decided that:

- The primary goal was to keep as much of the system in-tact as possible. To achieve that objective, two survivable core servers (survivable core server one and survivable core server two) were placed in the network. Both survivable core servers backup the main server if the main server fails, or if communication from the port networks to the main server fails.
- If the WAN fails where port networks two, four, five, and six, can no longer communicate with the main server or survivable core server one:
  - The main server will control port networks one and two.
  - survivable core server two will control port networks three, four, five, and six.
- If LAN three fails where port network three can no longer communicate to LAN two, survivable core server three will control port network three.
- If the WAN fails where port network six can no longer communicate with servers outside its community, than a survivable core server four (the Local Only server) will control port network six.

See Figure 15 for the customer's configuration with the priority scoring of each survivable core server.

Figure 15: Customer's configuration



To administer survivable core server, it is helpful to start with a data collection worksheet, as shown in Table 5:

Table 5: Survivable core server worksheet

Server Preference	Cluster ID	Platform Type	SVID	IP Address	Priority Score	Community	IPSI List in Com 1	IPSI List in Com 2	IPSI List in Com 3
System Preferred (highest value preference)	2	Duplex Server	3 4	192.9.13.10 192.9.13.11	100	1	1 2 3	1 2 3	1 2 3 4
	3	Simplex Server	5	192.9.44.11	50	1			
Local Preferred (second highest value preference in its community)	4	Simplex Server	6	192.9.33.22		2			
No Preference (no value)									
Local Only (only assigns to IPSIs in its own community)	5	Simplex Server	7	192.8.55.7		3			

Using the parameters outlined in Table 5, the priority of the survivable core server, during no-fault conditions, on the IPSI priority list will be:

- Both survivable core server one and survivable core server two are administered with a System Preferred preference. The System Preferred preference has the highest value of any preference. Further ranking within the System Preferred preference is achieved by adding a priority score. The priority score of 100 placed survivable core server one above survivable core server two in the ranking within the System Preferred preference. The IPSI priority list in any community will show survivable core server one as the first priority server, followed by survivable core server two.
- survivable core server three is administered as Local Preferred for community two. The Local Preferred preference is the second highest preference after System Preferred for port networks within its community. For port networks outside its community, the Local Preferred preference holds no value and would be the same as a survivable core server with no preference. When configurations have multiple Local Preferred servers, additional ranking can be achieved by using a Priority Score.

  In this example, survivable core server three would be the third choice for port network three, port network four, and port network five, which are all in community two. survivable core server three would also be the third choice for port network one and port network two.
- survivable core server four is administered as a Local Only server for community three. A Local Only server only displays on the IPSI's priority list if that IPSI is in its community. That means, survivable core server four only displays on the IPSI's list in community three and will never display on the IPSI priority list for any other IPSI not in community three.

In this example, the following failover scenarios in Table 6 might occur:

Table 6: Failover scenarios for IP connected example

Failure type	failover description
Main server fails	survivable core server one is the highest ranking survivable core server on the IPSI priority list. All port networks failover to survivable core server one.
Both main server and survivable core server1 fails	survivable core server two is second highest ranking survivable core server on the IPSI priority list. All port networks failover to survivable core server two.
WAN connection fails	The main server continues to control port networks one and two. The main server and survivable core server one can no longer communicate with the IPSIs in port networks three, four, five, and six and are removed from the IPSI's priority lists. The IPSIs in PN three, four, and five request service from the highest survivable core server on their priority list (survivable core server two). survivable core server four is the only survivable core server available to port network six if the WAN is not available.

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. This section provides information on the following:

- Survivable core server no service timer
- Primary Search Timer
- Feature limitations during gateway outage

Survivable core server no service timer

During survivable core server administration, a value is entered for the no service timer. The value of the no service timer determines the amount of time the IPSI will wait after it loses communication with the main server or controlling survivable core server, before requesting service from the highest ranked survivable core server on its priority list. All stable calls remain in a stable condition when the no service timer activates. The time from when the no service timer actives, to the time the IPSI requests service of a survivable core server, is called the no service time out interval. If the communication to the main server is restored before the no service time out interval expires, normal system recovery occurs.

The value for the no service timer is administrable from two to 15 minutes, with a default of five minutes. For more information on the no service timer, see Assigning Community for Port Networks screen.

Primary Search Timer

For more information on Primary Search Timer, see *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300432.

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.

PN Cold Reset Delay timer

The value for the PN Cold Reset Delay timer is administrable from 60 to 120 seconds, with a default of 60 seconds. This timer sets the time in seconds after which the PN cold reset occurs. For more information on the PN Cold Reset Delay timer, see After administering the survivable core servers.

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, call coverage, etc. 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 following Communication Manager features:

- Announcements
- Attendant Console
- Best Service Routing
- Call Classification
- Call Coverage
- Call Vectoring
- Centralized Attendant Service
- Crisis Alert
- CVLAN links
- Dial Plan Transparency
- Facility Busy Indication
- Hunt Groups
- Leave Word Calling
- Music on Hold

Announcements

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

Attendant Console

When a port network fails-over to a survivable core server any attendant console in that port network 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 (BSR) polling works if the facility used for routing the polling call is under the control of that survivable core server.

Call Classification

Call Classification will work 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 port networks 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 port network 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 port networks under its control.

Dial Plan Transparency

When a port network requests service from a survivable core server, or when a gateway registers with a survivable remote server, the Dial Plan Transparency feature routes calls that cannot be routed over the IP network over the public network, enabling the continued use of dialing patterns.

Dial Plan Transparency does not work when two port networks or gateways are in the same network region but failover to different survivable core servers.

For more information on Dial Plan Transparency, see:

- *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205
- *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504
- *Administering Avaya Aura® Communication Manager*, 03-300509

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 port networks under the control of that survivable core server.

Leave Word Calling

When a survivable core server takes control of a port network, 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.

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 or the Control Local Area Network (C-LAN). The Processor Ethernet interface or the C-LAN 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 or both of the C-LANs 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. The buffer size of the output link is the same as the S8800 Server buffer. 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 port networks. 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 5.0 and later releases only. It 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 or a port network 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 on Survivable CDR, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Call Management System

Call Management System (CMS) connects to the server through a C-LAN or through the server's Processor Ethernet (PE) interface. In the event of a failover, a survivable core server may control the port network that contains the C-LAN or may be able to communicate with the CMS through the Processor Ethernet interface of the survivable core server. In this case only the events that are under control of that survivable core server will be sent to the CMS. All other related system data will be lost. This occurs in the event of a fragmented system resulting from a control network failure.

Important:

The explanation of how the survivable core server and the survivable remote server interacts with CMS does not necessarily apply to the High Availability (HA) offer. There are special constraints and limitations when using the HA CMS configuration for a survivable core server or a survivable remote server. Customers should seek guidance from CSI to understand these limitations.

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 C-LAN. If the network is fragmented, only the port network with that C-LAN, 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 port network. The port network 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 port network under the control of the same server. Other requests will be denied.

Chapter 3: Survivable Core Server installation

The survivable core server installation chapter contains the following:

- Survivable core server installation checklist
- Survivable core server license files
- Server Configuration
- Administering survivable core server
- Translations

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.

Upgrading to Release 6.0 and later (Release 6.x) is different than previous releases upgrades because Release 6.x of Communication Manager is an application that resides on a virtual server. The underlying framework is called System Platform, and Communication Manager is a template that runs on System Platform.

Because Communication Manager Release 6.x, runs on only five servers, most upgrades require replacing the existing server with an Avaya S8800 Server (standalone) or Avaya S8300D Server (embedded) or HP ProLiant DL360 G7 1U (HP DL360 G7) Server or Dell™ PowerEdge™ R610 (Dell R610) Server. Although Release 6.x runs on an Avaya S8510 server and an Avaya S8800 Server, it is no longer being sold and, therefore, is not a target server. Communication Manager Release 4.0.5 or Release 5.2.1 or Release 6.0.1, can be upgraded to Release 6.x on the Avaya S8300D Server, Avaya S8510 Server, Avaya S8800 Server, HP DL360 G7 Server, and Dell R610 Server. The S8510, S8800, HP DL360 G7, and Dell R610 servers require a hardware upgrade as part of the process.

Note:

Before upgrading to Release 6.x, all servers must be either on Release 4.0.5 or Release 5.2.1. Any servers that are not on Release 4.0.5 or Release 5.2.1 must be upgraded to Release 4.0.5 or Release 5.2.1 before upgrading to Release 6.x.

For more information about the process and procedures for upgrading Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.x, see *Upgrading to Avaya Aura® Communication Manager*, 03-603560.

Survivable core server installation checklist

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

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

Overview

In general, a survivable core server installation requires the following high-level steps:

1. Design the system and determine the survivable core server administration factors. For more information on how to design and plan the system, see Survivable Core Server design and planning.
2. Install/upgrade Communication Manager on each survivable core server.
   - Start and stop the server (After loading a license file on a server, you must stop and start the survivable core server using the following Linux commands:)
   - Configure the server (Server Configuration)
3. Install/upgrade Communication Manager on the main server.
   - Install the license and authentication file (Survivable core server license files)
   - Restart the server
   - Configure the server (Server Configuration)
4. Administer survivable core server (Administering survivable core server)
5. Verify that the survivable core servers can register to the main server (Checking the administration on the main server)
6. Acceptance testing (Survivable core server acceptance testing)

Installing survivable core server with existing servers

Use the information in Table 7 as a reference when installing survivable core server with existing servers.

For more information, see *Implementing Avaya Aura® Communication Manager*, 03-603558.

Table 7: 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.
2. Upgrade the IPSI firmware.	Check the Minimum Firmware/ Hardware Vintage document for the correct IPSI firmware needed in a survivable core server environment. If you do not have the correct firmware, upgrade the firmware before continuing. If this system has duplicated IPSIs make sure the firmware on the duplicated IPSI pair is common.	To identify the firmware needed for an IPSI in a survivable core server environment see the Minimum Firmware/Hardware Vintages document found at http://support.avaya.com. A link to download IPSI firmware can be found at http://support.avaya.com. For instructions on how to perform the firmware upgrade, see *Upgrading Avaya Aura® Communication Manager*, 03-603445.
3. Survivable core server with IP-PNC.	No changes are needed for an IP connect environment.	
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*, 03-603445.
		1 of 4

Table 7: Installing survivable core server with existing servers

Task	Information	Documentation
5. Configure the survivable core server.	Use the server System Management Interface to configure the server.	For instructions, see *Implementing Avaya Aura® Communication Manager*, 03-603558.
6. Restart the server.	After loading the license file, stop the survivable core server using the following Linux command: **`? stop -af`** or **`stop -caf`** Then restart the survivable core server using the following Linux command: **`? start -a`** or **`start -ca`** 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 Survivable core server license files.
7. Attach the survivable core server to the network and verify communication with the customer's LAN interface.	The IP address of the C-LAN 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, use the **`ping`** command followed by the IP address of the C-LAN.	
8. Verify the communication to 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.	
Main Server		
		2 of 4

Table 7: Installing survivable core server with existing servers

Task	Information	Documentation
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*, 03-603445.
10. Configure the main server.	The server's System Management Interface is used 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 Existing survivable core server to main server.

11. Restart the server.	After loading the license file, stop the survivable core server using the following Linux command:
	`? stop -af` or `stop -caf`
	
	Then restart the survivable core server using the following Linux command:
	`? start -a` or `start -ca`
	
	Verify that the survivable core server administration feature is turned on.
		To verify that the survivable core server Administration feature is turned on, see Survivable core server license files.

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.
		3 of 4

Table 7: Installing survivable core server with existing servers

Task	Information	Documentation
13. Verify LAN/WAN connectivity.	Verify communication between each survivable core server and the main server over the LAN/ WAN. On the main server, use the **`ping`** command followed by the IP address of the survivable core server.	
14. Administer Survivable core server.	On the main server, administer each survivable core server, port network communities, and no service timer.	To administer the main server see Administering survivable core server.
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*, 03-300431.
16. Distribute the translations to the survivable core servers.	Run the **`save translations all`** or **`save translations ess`** command to synchronize translations between the main and newly added survivable core server for the first time.	For more information on the **`save translations`** command, see Translations.
17. Acceptance testing.	Avaya recommends testing the survivable core server configuration.	For more information on testing a survivable core server configuration, see Survivable core server acceptance testing.
		4 of 4

Installing survivable core server with new servers

Use the information in Table 8 as a reference when installing survivable sore server with new servers.

Table 8: Installing survivable core 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.
2. **IPSI**: Upgrade the IPSI firmware.	Check the Minimum Firmware/Hardware Vintage document for the correct IPSI firmware needed in a survivable core server environment. If you do not have the correct firmware, upgrade the IPSI firmware before continuing. If this system has duplicated IPSIs make sure the firmware on the duplicated IPSI pair is common.	To identify the firmware needed for an IPSI in a survivable core server environment see the Minimum Firmware/ Hardware Vintages document found on the http://support.avaya.com website. A link to download IPSI firmware can be found on the support.avaya.com website. For instructions on how to perform the firmware upgrade see *Upgrading Avaya Aura® Communication Manager on Avaya S8xxx Servers* (03-602885).
		1 of 5

Table 8: Installing survivable core server with new servers (continued)

Task	Information	Documentation
3. **Survivable Core Server**: Install the hardware, System Platform, and load Communication Manager.	.	To install the server hardware, see *Installing the Avaya S8800 Server for Avaya Aura® Communication Manager*, 03-603444. To install the IP connectivity hardware, see *Adding New Hardware for Avaya Servers and Gateways*, 555-245-112. To install Communication Manager, see *Implementing Avaya Aura® Communication Manager*, 03-603558.
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.
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.
		2 of 5

Table 8: Installing survivable core server with new servers (continued)

Task	Information	Documentation
6. **Survivable Core Server**: Verify that the survivable core server can communicate with the customer's LAN interface.	An IP address of a C-LAN was entered when you configured the survivable core server. The C-LAN is used when the survivable core server registers with the main server for the first time and may be used for subsequent registrations. To verify that the survivable core server can communicate with the customer's LAN interface use the following instruction: ● On the survivable core server, use the **`ping`** command followed by the IP address of the C-LAN or Processor Ethernet.	
7. **Survivable Core Server**: Verify that the survivable core server can communicate with the main server over the IP network.	To verify that the survivable core server can communicate with the main server: 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 IPSIs in the configuration.	To install the server hardware, see *Installing the Avaya S8800 Server for Avaya Aura® Communication Manager*, 03-603444. To install Communication Manager, see *Implementing Avaya Aura® Communication Manager*, 03-603558.
		3 of 5

Table 8: Installing survivable core server with new servers (continued)

Task	Information	Documentation
9. **Main server**: Install the license and authentication file.	After installing the license file, stop the main server using the following Linux command: ● `stop -af` or `stop -caf` Then restart the main server using the following Linux command: ● `start -a` or `start -ca` Verify that the survivable core server Administration feature is turned on.	To install the license and authentication file, see *Implementing Avaya Aura® Communication Manager*, 03-603558. To verify that the survivable core server Administration feature is turned on, see Survivable core server license files.
10. **Main server**: Verify LAN/WAN connectivity.	Verify communication between each survivable core server and the main server over the LAN/WAN. To verify that the main server can communicate with all servers on the LAN/WAN: On the main server, use the `ping` command followed by the IP address of the survivable core server.	
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.
12. **Main server**: Administer Survivable Core Server.		To administer Survivable Core Server on the main server, see Administering survivable core server.
		4 of 5

Table 8: Installing survivable core server with new servers (continued)

Task	Information	Documentation
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*, 03-300431.
14. Acceptance testing	Avaya recommends testing the survivable core server configuration.	For more information on how to test a configuration, see Survivable core server acceptance testing.
15. **Main server**: Distribute the translations to the survivable core server.	If changes are made to translations, they must be distributed to the survivable core server by executing the **`save translations all`** or **`save translations ess`** command.	For more information on the **`save translations`** command, see Translations.
		5 of 5

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.

Earlier versions of Communication Manager, except Midsize Business Template Communication Manager Release 5.2.1, will continue to use the Remote Feature Activation (RFA) online tool for license files.

Licensing survivable servers

For Communication Manager Release 6.0 and later, license files are installed only on the Communication Manager main server. License files are not installed on survivable servers. 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 that can be administered on the main server. This number is based on the number of Maximum ESS Stations (VALUE_CM_ESS_STA) and Maximum LSP Stations (VALUE_CM_LSP_STA) that are activated in the license file. Each survivable server that is administered on the main server consumes one of the Maximum Survivable Processors feature capacity.

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).

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

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 of how:

- Certain aspects of license file affect a survivable core server:
  - Module IDs and Cluster IDs
  - System Identification numbers
  - MAC Address
- Verifying the license status:
  - Verifying 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 on how to administer a survivable core server using the **Survivable processor** screen, see Administering a survivable core server on the main server.

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.

For more information on accessing the WebLM from the System Platform Web Console, see *Implementing Avaya Aura® Communication Manager*, 03-603558.

Checking the license file

After you load the license file on the server you can 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. For Communication Manager Release 6.0 and later, 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. In Communication Manager Release 3.0 and later releases, both ESS Feature Keywords are turned off by default.

Verifying the license status

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.

1. Start and log in to the Communication Manager System Management Interface (SMI).
2. In the menu bar, click **Administration** > **Licensing**.
3. In the navigation pane, click **License Status**.

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

Server Configuration

This section provides instructions on how to configure the server in a survivable core server configuration.

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

Table 9: Network Settings

	Value	Note
Communication Manager virtual machine IP address		

Table 10: Network Configuration Settings

Field	Value	Note
Hostname		
Alias hostname		
Server ID (between 1 and 256)		

Field	Value	Note
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		

Note:

The parameters in the table Table 11 needs to be specified only in case of duplication and pertain to the standby server.

Table 11: Duplication Parameters

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

Field	Value	Note
PE interchange priority		
IP address for PE health check		

Table 12: Add Login

	Value	Note
Privileged administrator user ID		
Login shell script		

For more information about installation and configuration steps, see *Implementing Avaya Aura® Communication Manager*, 03-603558 at http://support.avaya.com.

After the survivable core server is configured

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 Administering a survivable core server on the main server.

Note:

The survivable core server cannot control an IPSI 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.

Administering survivable core server

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 port network communities on page six.
- Administer the no service timer and schedule the Auto Return feature on page seven.

Each section of the **Survivable Processor** screen is described in more detail in this chapter.

Administering a survivable core server on the main server

Important upgrade information

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

Pre-requisites

On the main server, use the following steps to translate each survivable core server:

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:

   Page 1: Identify survivable remote servers and survivable core servers and control use of the Processor Ethernet interface.

   Page 2: Administer CMS, if you have a CMS connecting to the Processor Ethernet interface of the server that you identified in page one.

   Page 3: 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.

   Page 4: Displays only if CDR is administered on page three.

   For details of the screen, see Survivable Processor screen

3. Run the **`change system-parameters port-networks`** command to administer the **Community Assignments for Port Networks** screen and the **Port Network Recovery Rules** screen.

   Page 1: Administer the community assignments for port networks, as described in Assigning Community for Port Networks screen.

   Page 2: Schedule the **Auto Return** feature and to set the no service timer.

Survivable Processor screen

Run the **`add survivable-processor`** command to use the **Survivable Processor** screen to administer survivable remote servers and survivable core servers to control use of the Processor Ethernet interface.

For more information to administer the Survivable Processor screen, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

Administering page one of the Survivable Processor screen

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 the Type to either **simplex-ess** or **duplex-ess**, the screen is refreshed.

1. Enter the survivable processor type. Default values are **lsp, simplex-ess,** or **duplex-ess**.
2. Enter the network region in which the Processor Ethernet interface of the survivable remote or core server resides (valid values 1 to 250).
3. 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** thru **999** and **blank**.
4. 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.
5. 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.
6. Assign a survivable core server to a community
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** thru **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.
17. **Community Size** field is set to **all**.
18. Select the System Preferred option when the goal is to keep as much of the system network intact as possible, allowing one survivable core server to replace the Main server. If this field is set to **y**, then **Local Preferred** and **Local Only** default to **n** and cannot be changed. If this field is **n**, then **Local Preferred** and **Local Only** can be either **y** or **n**. Default is **y**.
19. Enter the Priority Score for this survivable core server. Valid values are 1 thru 100. Default is 1.
20. Select the Local Preferred option when you want the survivable core server to accept the request for service from IPSIs co-located in the same geographical region, WAN/LAN segment, district, or business unit. Default is **n**.
21. Select the Local Only option when you want the survivable core server to accept the request for service from an IPSI, only if the IPSIs is located in the same community as the survivable core server. Default is **n**.

Administering page two of Survivable Processor screen

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 it 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.

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 a *n* (no) if this processor channel is disabled on the survivable remote server or the survivable core server.
   - Enter an *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 cases:
     - The main server connects to the adjuncts using a C-LAN and you want the survivable core server to use the same connectivity.
     - 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 an *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 (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 using a C-LAN 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 an *o* 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. Otherwise the C-LAN link number is used.
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 one 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

Use page three if you have an Application Enablement Services (AESs), 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 it 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.

Important:
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*, 555-245-205.

1. The **Service Type** field identifies the server application type/adjunct connection used on this channel. Valid entries include CDR1 or CDR2, and AESVCS.
2. Enter one of the following values in this field:
   - Enter a *n* (no) if this ip-services link is disabled on the survivable remote server or the survivable core server.
   - Enter an *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 cases:
     - The main server connects to the adjuncts using a C-LAN and you want the survivable core server to use the same connectivity.
     - 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 an *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 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
3. Enter a *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 yes, 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 port network.

Note:

More administration is required for the Survivable CDR feature to work. For complete Survivable CDR information, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

4. The **Local Node** field contains the node name as defined on the **Node Names** screen.
5. The **Local Port** field contains the originating port number. For client applications such as CDR, this field defaults to a zero.
6. The **Remote Node** 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.
7. 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 a **no** is entered in the **Enable** field on the page three of the **Survivable Processor** screen.

Administering Page four of the Survivable Processor screen

Page four displays 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 a *n* or an *i* the fields on page four are display-only.

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, one 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 one to five.
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, one to 255 seconds, that the link can be idle before Communication Manager sends a connectivity message to ensure the link is still up.

Assigning Community for Port Networks screen

For more information to administer the Port Networks screen, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

1. Run the **`change system-parameters port-networks`** command to administer the **Community Assignments for Port Networks** screen and the **Port Network Recovery Rules** screen.
2. In the **Community Assignments for Port Networks** screen, enter the community assignments for each port network.

   Note:

   Assigning port networks to a community associates the port network with a survivable core server administered with the Local Preferred or as a Local Only server. A survivable core server is assigned a community on page one of the **Community Assignments for Port Networks** screen. To have the survivable core server and the port networks in the same community, the community number of the survivable core server and the community number for each port network must match.
3. In the **Port Network Recovery Rules** screen schedule the **Auto Return** feature and set the no service timer:
4. The **Auto Return** feature is used to administer one of the following options:

   No: When the value is set to no, the port networks cannot automatically return to the control of the main server. No additional fields display when the value is set to no.

   Schedule: Enter schedule to schedule a day and time to return the port networks to the control of the main server. When the value is set to scheduled, the day and time fields display. The schedule can be set up to seven days prior to its activation.

   Day: Enter the day of the week.

   Time: Enter the time of day in a 24 hour (military) format.

   Yes: When the value is set to yes the IPSI Connect up time field displays. When Auto Return is set to yes the port networks can automatically return to the main server after the value set in the IPSI Connect up time expires.

   IPSI Connect up time: Enter the number of minutes that the IPSI will wait to return to the main server after communication with the main server is restored. Valid values for this field are three minutes to 120 minutes.

5. In the **No Service Time Out Interval** field enter the time, in minutes, that the IPSIs will wait before requesting service from the highest survivable core server on its priority list. Valid values for this field are two to 15 minutes. The default value is 5 minutes.
6. In the **PN Cold Reset Delay Timer** field specify the time in seconds after which the PN cold reset occurs. Valid values are **60** thru **120**. The default value is 60 second.

After administering the survivable core servers

After you run the **`change survivable processor`** and **`change system-parameters port-networks`** commands and submit the forms:

- Each configured survivable core server registers with the main server.
- The main server sends the survivable core server a copy of the translations.
- The survivable core server receives the translations, resets, and re-registers with the main server.

The process listed above is automatic. After the survivable core server receives the initial translation download, any translation changes are sent to the survivable core server by executing the **`save translations all`**, or **`save translations ess`** command. For more information on translation, see Translations.

Checking the administration on the main server

To check the administration on the main server, type the following commands using the SAT:

1. **`status ess clusters`**

   Verify that:

   a. The Cluster ID 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 a *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 on how to troubleshoot the survivable core server registration, see Troubleshooting.

   - The **Translations Updated** column:

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

b. 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 Figure 16.

Figure 16: ESS Cluster information

```
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
```

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. **`display survivable processor`** ***`node name`***

   Verify that the screen displays the values that you administered.

For an example of the output of the **`display survivable processor`** command, see Figure 17.

Figure 17: survivable Processor screen

```
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
```

3. **`status ess port-networks`**

   Verify that:

   - All port networks are shown. This report may span several pages.
   - All port networks come into service as indicated in the **Port Ntwk Ste** column.

For an example of the output of the **`status ess port-networks`** command, see Figure 18.

Figure 18: status ess port-networks

```
status ess port-networks

Cluster ID 2             ESS PORT NETWORK INFORMATION

                  Port IPSI   Pri/  Pri/    Cntl Connected
   Com  Intf Intf Ntwk Gtway  Sec   Sec     Clus Clus(ter)
PN Num  Loc  Type Ste  Loc    Loc   State     ID IDs

 1  1   1A01  IPSI up   1A01  1A01  actv-aa    1   1
                             1B01  standby    1   1

 2  1   26A01 IPSI up   26A01 26A01 actv-aa    1   1
                             26B01 standby    1   1
```

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 Figure 19.

Figure 19: system-parameters maintenance

```
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
```

To verify that the survivable core server has received the translations on the main server:

1. Execute 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. Execute the **`save translations`** command.

   The **Translations Updated** column may take several minutes to update, depending on the size of the translations and network congestion.

   For an example of the **`status ess cluster`** command, see Figure 16.

Chapter 4: 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 in this chapter 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.

The following conversions are detailed in this book:

- Existing survivable core server to main server
- Existing server to survivable core server

  For more information on conversions, see *Converting Avaya Servers and Branch Gateways*, 03-602884.

  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.

Basic guidelines for conversions

Read the following information before performing one of the conversion procedures listed in this chapter:

- For any conversion, the survivable core server should always be addressed before the main server. When a survivable core server is not controlling a port network, 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 port networks are controlled by a new server (main server or survivable core server), they perform a restart which resets every board in the port network.
- IP server interface (IPSI) circuit packs may require a firmware upgrade to be compatible with the survivable core server feature. For compatibility information, see the *Minimum Firmware/Hardware Vintages* document at http://support.avaya.com.

Existing survivable core server to main server

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 port networks that are being controlled by other servers will eventually switch to the new main server. This requires that the port networks perform a reset. If a survivable core server exists, it may be advantageous to switch all port networks to the survivable core server prior to the conversion.

Use the following steps to convert an existing server to a main server:

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 S8300D and S8800 active servers.
   In the System Management Interface, under the **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 **a 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. For more information on license files, see License files. This license file could use the same IPSI serial number that the previous license file used unless the server is physically moved and another IPSI is now logically closer.

   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 (S8800) will have 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. While this is normal, it is not sufficient to notify all of the non Communication Manager processes of the new server configuration including the Cluster ID.
   From the active server command line interface, use the following commands to notify all processes of the new parameters:

   `stop -caf`

   Then execute:

   `start -ca`

10. For duplicated servers, release the busy out of the standby server using the **Release Server** command on the System Management Interface.
    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. Once the Module ID is updated, execute the following commands from the command line interface:
    `stop -caf`

    Then execute:

    `start -ca`

    to inform all processes of the new server configuration and Module ID.
11. Be sure that the translations from the main server match the translations for the newly converted main server. Use the **`display survivable-processor`** and **`display system-parameters port-networks`** commands 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).
12. 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 Administering a survivable core server on the main server.
13. 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 SAT commands to notify the Communication Manager processes:
    `save trans all`

    Then execute:

    `reset sys 4`
14. Use the **`list survivable-processor`**, **`display survivable-processor`** ***`nodename`***, and **`display system-parameters port-networks`** commands to verify that the correct translations are present for all the survivable core servers.
15. Disconnect, if connected, the old main server from the LAN/WAN.
16. Connect the new main server to the LAN/WAN.
17. At any existing survivable core server, verify that the new main server or server pair are connected to the LAN/WAN.
18. Using the System Management Interface, on each **ESS** and **LSP** specify:

    a. The IP address of the C-LAN controlled by the new main server.

b. 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.

19. Verify that each of the survivable core servers and survivable remote servers register with the main server and that the translations are updated.

    a. 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.

20. If a **`save trans all`** command was **not** performed in step 13 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.

21. If a **`reset system 4`** command was **not** performed in 13, then do so now. From the main server, execute the **`reset system 4`** command.

Existing server to survivable core server

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

Use the following steps to convert an existing server to a survivable core server:

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*, 03-603445.
5. If the server is a duplex pair busy out the standby server.
6. Execute this step for simplex and active servers of duplex pair.
   In the System Management Interface, go to **Server Configuration** and click the **Network Configuration** option.
   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 from the left margin.
      - Select **a main server.**
7. For duplex servers, perform the same configuration activities as step 6 for the standby server.
8. Configuring the server causes a reset to be executed. While this is normal, it is not sufficient to notify all of the non Communication Manager processes of the new server configuration including the Cluster ID.
   From the active server command line interface use the command line interface to perform the following commands:

   ```
   stop -caf
   ```

   Then execute:

   ```
   start -ca
   ```

   to inform all processes of the new server configuration and Module ID.

   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:
`stop -caf`

Then execute:

`start -ca`
to inform all processes of the new server configuration and Module ID.

9. Verify that the main server has the latest translations available.
10. 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 Administering a survivable core server on the main server.
11. Connect the new survivable core server to the LAN/WAN.
12. Verify that the survivable core servers register with the main server and that the translations are updated on the survivable core server.
    a. 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.
13. To synchronize translations between the main server, the survivable remote servers, and the survivable core server, execute **`save translation all`** on the main server.

Chapter 5: Running in survivable core server mode

This chapter describes various nuances that one should be aware of when a survivable core server controls one or more port networks.

Administering and saving translations

All administration is performed on the main server. Distribution of the translations to the survivable core server happens when the **`save translations ess`** or **`save translations all`** command is executed 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 a C-LAN circuit pack or through Processor Ethernet. Translations can be administered on a survivable core server but they cannot be saved.

To determine when the last translation download from the main server to the survivable core server occurred, type **`status ess clusters`** from the server's SAT. Check the **Translations Updated** (timestamp) column associated with the cluster ID of the survivable core server (Figure 20). The main server sends translations to the survivable core server:

- Every time a **`save translations all`** or **`save translations ess`** command is executed.
- During routine maintenance, if the **Update survivable remote server and survivable core servers when saving translations** option is checked.

Figure 20: Status ess clusters

```
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
```

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

Alarming

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

- A major alarm for every port network that is no longer under the main server's control.
- 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.

If the survivable core server is not in control of a port network, it generates platform alarms only. Once in control of a port network, the survivable core server generates Communication Manager alarms.

A survivable core server alarms when it can no longer communicate with an IPSI unless the survivable core server was rejected by the IPSI.

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

- A major alarm is generated when the survivable core server controls a port network. For more information, see *Maintenance Alarms for Avaya Aura® Communication Manager, Gateways and Servers*, 03-300430.
- An alarm is generated when the survivable core server controls gateways and IP endpoints.

Unplanned fall-back or failover

In some cases an unplanned fall-back to the main server or an unplanned failover to another survivable core server is possible. It is important to understand the circumstances surrounding these situations to prevent unwanted configurations and fragmentation.

Unplanned fall-back to the main server

The no service timer activates when an IPSI cannot communicate with the main server or the controlling survivable core server. The no service timer is administered using the **system-parameters port networks** command.

If the fall-back to the main server was premature, the **`get forced-takeover ipserver-interface`** command can be used to pull the port net works back to the control of the previous survivable core server. For more information on the **`get forced-takeover ipserver-interface`** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431.

CAUTION:

The **`get forced-takeover ipserver-interface`** command is service effecting.

In an environment where there are multiple survivable core servers, you can ensure that the port networks, controlled by the survivable core server do not fall-back to the main server by:

- Executing the **`disable ess`** command. This command allows a survivable core server or main server to be disabled (taken out of service). A survivable core server or main server may be disabled only if it is not in control of any port networks. A disabled survivable core server or main server will not connect to an IPSI.

  This command may be executed from either a main server or a survivable core server. A survivable core server may only disable its own cluster ID. When the command is run from the main server, any and all cluster IDs may be disabled, including the main server itself.

  For more information on the **`disable ess`** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431.

- Disconnecting the control network from the main server. By disconnecting the control network the main server cannot access an IPSI.

  CAUTION:

  Disabling or isolating the main server is not recommended when there is only one survivable core server in the configuration. In this case, disabling the main server would cause a system outage if the survivable core server fails or if communication between the survivable core server and the port networks was lost.

Unplanned failover to another survivable core server

A system that failed over to a single survivable core server could experience unwanted fragmentation if the IPSI can no longer communicate with the main server but can communicate with multiple survivable core servers. For example, due to a temporary network outage one or more IPSIs in a configuration can no longer communicate with the controlling survivable core server. In this situation the no service timer activates. If the no service timer expires before the temporary network outage is restored, the IPSI requests service from the next highest survivable core server on its priority list. In the resulting configuration, the port network that was experiencing the temporary network outage is now controlled by a different survivable core server than the rest of the port networks.

If the failover to another survivable core server causes unwanted fragmentation, the **`get forced-takeover ipserver-interface`** command can be used to pull the port networks back to the previous survivable core server. For more information on the **`get forcd-takeover ipserver-interface`** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers,* 03-300431.

CAUTION:

The **`get forced-takeover ipserver-interface`** command is service effecting.

Updating 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 port network. The reset system 4 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 port networks. The translations are received by the survivable core server but are not loaded as long as the survivable core server controls a port network. Once the survivable core server no longer controls a port network, the survivable core server resets and loads the new translations.

Chapter 6: 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.

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:
  - 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.
- The **`status ess port-networks`** command displays which Cluster ID is controlling each port network and which survivable core server the port networks (IPSIs) have on their priority lists.

The following System Management Interface commands can be used 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 C-LAN or 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* (03-300431) 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.

On the main server, use the following list of commands to troubleshoot a survivable core server that is not registering with the main server:

1. Use 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. Use the SAT **`ping ip-address board <location> nnn.nnn.nnn.nnn`** command to verify connectivity between the main server and the survivable core server. Where, **`<location>`** is the location of the C-LAN circuit pack the survivable core server is trying to use to register with and ***`nnn.nnn.nnn.nnn`*** is the IP address of the survivable core server.
3. Use 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. See *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers* (03-300430) for descriptions of the survivable core server denial events.
4. Use 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.

From the survivable core server that is not registering with the main server, use the following commands to troubleshoot:

CAUTION:

In 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.

1. Use the Linux **`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 C-LAN in the main server that the survivable core server is trying to register with. 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.
2. 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.
3. Use the **Server Configuration** pages of the System Management Interface to verify the following:
   - 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.
   - On the **Configure ESS** page, verify that the correct platform type (duplex or simplex) is selected and the correct C-LAN or 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).
   - 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.
4. On the SAT, execute the **`display system-parameters customer-options`** command. Verify the administration of the following fields:
   - The **ESS Administration** field is set to **y**
   - 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.

5. From the System Management Interface:
   - Under **Administration > Server (Maintenance)**, click **License File** and verify that the license mode is **normal**.
6. Use the SAT command **`status ess clusters`** 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.

list trace ras command example

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.

1. To begin, find the IP addresses of the systems involved by executing the **`display survivable-processor`** command from the main server. Note the IP addresses of the main Server and the survivable core servers. For an example, see Figure 21.

Figure 21: Troubleshooting - display survivable processor example

```
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
```

From the survivable core server that is to be monitored, use the System Management Interface and the **Server Configuration** command to display the **Configure ESS** page. Note the IP Address that is configured as the main server's primary address.

2. Execute the trace command from the main server.

   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). For an example of the **`list trace ras`** command, see Figure 22.

Figure 22: Troubleshooting - list trace ras command example - main server

```
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
```

3. Execute the trace command from the survivable core server.

   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 (Figure 23).

Figure 23: Troubleshooting - list trace ras command example - ESS

```
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
```

4. Now, suppose 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 Figure 24 displays using the **`list trace ras`** command.

Figure 24: Troubleshooting - mis-administration - main server perspective

```
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
```

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 Figure 25.

Figure 25: Troubleshooting - mis-administration - ESS perspective

```
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
```

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

IPSI is not connected to a server

On the main server, use the **`status ess port-networks`** command to verify the servers a particular IPSI has established a connection with. Under normal operation (no network or server failures) a IPSI will establish connections to all survivable core servers but only the eight servers that have the highest priority are shown when the **`status ess port-networks`** command is executed.

The servers are listed under the **Connected Clus(ter) IDs** field in the order in which the IPSI will request service. The main server, if there is a connection to it, always has the highest priority.

See *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers* (03-300431) for errors related to survivable core server socket connections to IPSIs. Error 513 should be logged if a socket connection can not be established between an enabled survivable core server and an IPSI.

If the IPSI is not connected to the server, use the following steps to try and determine the cause:

1. On the main server's System Management Interface, use the **IPSI Version** command to verify that all IPSIs have the current hardware and firmware. See the Minimum Firmware/ Hardware Vintages document found at: http://support.avaya.com.

2. From the System Management Interface pages of the survivable core server that is not connecting, initiate a **PING** to the administered IPSIs to verify connectivity between the survivable core server and IPSIs.
3. Firewalls or other security measures may preclude the server and IPSI from communicating. Verify that these ports are open through the network between the server and the IPSI:
   - 5010 IPSI/Server control channel
   - 5011 IPSI/Server IPSI version channel
   - 5012 IPSI/Server serial number channel
4. Use the SAT command **status ess port-networks** to identify the Cluster IDs of the survivable core servers a port network (IPSI) is connected to. This command may be executed at either a main server or a survivable core server. With a fragmented network it may be necessary to execute this command at each server in the system configuration to acquire a complete view of the IPSI connectivity.
   Figure 26 shows an example of an IPSI (the standby IPSI in PN 2) that does not have a connection established with the server.

Figure 26: status ess port-networks example

```
status ess port-networks

Cluster ID 2             ESS PORT NETWORK INFORMATION

                  Port IPSI   Pri/  Pri/    Cntl Connected
   Com  Intf Intf Ntwk Gtway  Sec   Sec     Clus Clus(ter)
PN Num  Loc  Type Ste  Loc    Loc   State     ID IDs

 1  1   1A01  IPSI up   1A01  1A01  actv-aa    1   1
                              1B01  standby    1   1

 2  1   26A01 IPSI up   26A01 26A01 actv-aa    1   1
                              26B01 standby    1   1
```

5. Resolve network fragmentation and outage issues using your local practice.
6. Use the SAT command **status ess port-network** to verify that all port networks (IPSIs) are communicating with servers.

Chapter 7: Survivable core server acceptance testing

Acceptance testing is used to test the design and administration of the survivable core server configuration. To check the survivable core server configuration, it is recommended that you use the **`status ess port-networks`** and **`status ess clusters`** command on a regular bases.

Testing transfer of control from main server to survivable core server

CAUTION:

This test is service affecting. When a survivable core server or main server assumes control of a port network, the port network restarts. During the restart, all established calls on the port network are torn down except shuffled calls between IP endpoints. Shuffled IP calls do not have access to features during port network resets.

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

1. Identify the port networks that are being tested.
2. Identify the survivable core server that is being tested. The survivable core server must be connected to the port networks identified in step 1. To verify that the survivable core server is connected to the port network(s), execute a **`status ess port-networks`** command from either the main server or the survivable core server. The CLID of the survivable core server must appear in the list of connected *Clusters IDs* for the port networks.
3. On the survivable core server, execute the **`get forced-takeover ipserver-interface N`** command (where N is the number of the first port network).
4. On the survivable core server, repeat the **`get forced-takeover ipserver-interface N`** command for every port network identified in step 1.

What to expect

You can expect the following events to occur:

- All the tested port networks go through a restart when coming into service on the survivable core server.
- The restart may take several minutes.

Acceptance criteria

Check that the selected port networks are under the control of the survivable core server that is being tested by performing the following steps:

1. On the main server:
   a. Execute **`status ess port-networks`** command from the SAT. Verify the following:
      - All the port networks display on the list.
      - The status of the selected port networks are shown as **down**. The status of all the other port networks that are not being tested are shown as **up.**
2. On the survivable core server:
   a. Execute a **`status ess port-networks`** command from the SAT. Verify the following:
      - All port networks are displayed on the list.
      - The status of the selected port networks are shown as **up**. The status of all other port networks not being tested are shown as **down.**
3. Place a telephone call between the port networks being tested. If only one port network was selected, place a telephone call within that port network
4. Place a telephone call between the port networks not selected for this test.
5. Place a telephone call between the port networks that are being tested and the port networks not selected for this test. Verify that you receive a fast busy. Note that calls to Extension to Cellular endpoints may go to coverage instead of returning a fast busy.

Testing transfer of control from survivable core server to main server

Use this procedure to test the ability of the main server to assume control of the port networks that are currently under control of the survivable core server. Perform the following steps to execute this test:

1. Verify that the survivable core server is in control of the port networks being tested by executing the **`status ess port-networks`** command from the main server. The status of the port networks being tested is shown as **down**.

2. On the main server, execute the SAT command, **`get forced-takeover ipserver-interface all`**.

   CAUTION:
   This test is service affecting.

What to expect

You can expect the following events to occur:

- The survivable core server loses control of all port networks under its control as the port networks restart.
- Survivable core server reboots on the main server.
- This test takes several minutes.

Acceptance criteria

Check that the selected port networks are now under control of the main server by performing the following steps:

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

Disable a survivable core server from the main server

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:

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

   Note:

   You cannot disable a survivable core server that is controlling an IPSI. For more information on the **`disable ess cluster`** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers,* 03-300431.

What to expect

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.

Acceptance criteria

Verify that the selected survivable core server is now disabled by performing the following steps:

1. On the main server:
   a. 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:
   a. 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**

b. Execute the **`status ess port-networks`** command:

- The port network connection under the **Port Ntwk Ste** column shows **down.**

Enable a survivable core server from 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:

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

What to expect

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.

Acceptance criteria

Verify that the survivable core server being tested is now enabled by performing the following steps:

1. On the main server:

   a. 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:

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

   - The enabled state under the **Enabled?** column shows **y**

Glossary

C

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.

Cluster A cluster is a server or set of servers which share a call state. The cluster can be the singular case (S8510 Servers) or the duplex case (S8800 Servers). This definition implies that a server within a cluster can be interchanged if it is duplicated.

Community A virtual group consisting of one survivable core server and one or more port networks.

M

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 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.

Priority score See Priority value.

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.
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.
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.

Index

A

Adjunct considerations 64
Administering and saving translations 107
Administering Survivable Core Server 86
Administration 107
Administrative value 47
Announcements 62
Attendant Console 62
Auto Return 92
Avaya survivability 13
Avoiding overload of network resources 43
Avoiding system fragmentation 43

B

Best Service Routing 62

C

Call Classification 62
Call Coverage 62
Call Detail Recording 65
Call Management System 66
Call Vectoring 62
Centralized Attendant Service 63
Check the administration 93
C-LAN access for survivable core server registration . 22
CLID 87
Cluster ID 81
Conversions 99
Crisis Alert 63
CSS considerations 50
CVLAN links 63

D

Data Networking 50
D-channel 48
Design 43
Design strategy 43
Dial Plan Transparency 63

E

E911 49
EC500 66
Enterprise Survivable Server (Survivable Core Server)
  Troubleshooting
    Survivable Core Server not registered 114
Examples
  Network failure 28
Examples of how the priority list works 56

F

Facility Busy Indication 64
Failover to a Survivable core server 16
Feature considerations 61
Feature Keywords 82
Fiber-PNC configuration 60
Figures
  Catastrophic main server failure 26
  Fall-back to the main server 34
  Main server recovery 33
  Main servers fail 24
  Main servers fail - Survivable core server recovery of failure 27
  Network failure - Survivable core server recovery . 30
  Network fragmentation failure 29
  Network fragmentation recovery 32
  Port Network Recovery Rules screen 93
  S8800 Server with Survivable core servers in normal operation 25
  Status ess clusters 94
  system-parameters maintenance 96

G

G250 60

H

Hunt Groups 64

I

Important considerations 43
IP Endpoints 60
IPSI version 24
ISDN PRI guidelines 48
ISDN PRI Non Facility associated signaling 48

L

Leave Word Calling 64
License file 47, 79

License files 80
Licenses files 45

M

Main server and Survivable core server differences . 47
MID 45
Module ID 81
Module Identification Number 45
Music on Hold 64

N

Network port considerations 46
No service time out interval 93
No service timer 16

O

Obtaining a RFA license file 82
Overview
High-level 15

P

PCOL 49
Planning 43
Port network communities 92
Port network fall-back 18
Ports 46
Prerequisites 45
priority list 56
Processor Ethernet
overview 19
support with C-LANs 21
Property Management System 67

R

Registration 22
Running in Survivable core server mode. 107
Administering and saving translations 107
Alarming 108
save translations ess 107
Unplanned fall-back or failover. 109
Updating the main server 110
User enabled telephone features 108

S

Save translations 96
Saving translations. 107
SBS. 50
Serial numbers 82
Server ID 45
SID 81
Survivable CDR 65
Survivable Core Server
Conversions 99
Existing server to Survivable Core Server . . 103
Existing Survivable Core Server to main server 100
Failover to a Survivable Core Server 16
Survivable Core Server Design and Planning . . . 43
Survivable Core Server design strategy 43
Troubleshooting
Survivable Core Server not registered 114
Survivable core server
Capacity 47
Conversions
Existing server to Survivable Core Server . . 103
Conversions, basic guidelines 99
Prerequisites 45
Sequence of events for a failover 17
Troubleshooting
IPSI not connected 119
troubleshooting
IPSI not connected 119
Survivable Core Server (Survivable core server)
Conversions 99
Survivable core server (Survivable core server)
Conversions
Existing Survivable Core Server to main server 100
Survivable core server failover examples
Main server fails. 24
Network failure 28
Survivable core server license file 79
Survivable core server re-registers with main server . 23
Survivable Processor screen 87
Survivable remote and core 19
SVID 45
Synchronization 49
System Identification numbers. 81

T

Tables
Installing Survivable core server with new servers . 75
Timing considerations. 60
Translations 47, 96
Trunking considerations. 48

U

Unplanned failover to another Survivable core server .110
get forced-takeover ipserver-interface. 110
Unplanned fallback to the Main server
system-parameters port networks 109
Unplanned fall-back to the main server. 109
Unplanned fallback to the main server

get forced-takeover ipserver-interface 109
Updating the main server 110

V

Voice Mail (Audix, Intuity, Octel) 67
Voice Response Systems (Conversant) 67