Using the Avaya Enterprise Survivable Servers (ESS)

03-300428
Issue 5.0
May 2009

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full support information, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03-600758.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not 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. Customer and/or 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. 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 through the following Web site: http://www.avaya.com/support.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

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 fraud intervention

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

http://www.avaya.com/support

Avaya support

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

Contents

Chapter 1: ESS Overview

Avaya survivability

Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS) are survivability options available with Communication Manager.

- **LSP**: When communication to the Primary Controller (main server) is lost, the LSP option allows the IP telephones and one or more media gateways to register with an LSP. The Avaya S8300 and Avaya S8500-Series servers can be used as LSPs. To understand the difference between an LSP and an ESS see LSP and ESS on page 13. The LSP option is available from Communication Manager Release 1.x onwards.
- **ESS**: The ESS option provides survivability to an Avaya configuration by allowing backup servers to be placed in various locations in the customer's network. For more information, see High-Level ESS Overview. The ESS option is available from Communication Manager Release 3.0 onwards.

  Note:

  Before Communication Manager Releases 3.0, Avaya offered the following survivability options:

- **Survivable Remote Processor (SRP)**: In an SRP option, DEFINITY server SI provided continued service for a single fiber-Port Network Connected Center Stage Switch (fiber-PNC CSS) port network.
- **ATM WAN Spare Processor (WSP)**: In a WSP option, multiple DEFINITY server R processor port networks provided continued service for systems with ATM port network connectivity.
- **Manual Backup Server (MBS)**: The MBS option used an S8700-Series or an S8500-Series server to backup the main server. The takeover of the port networks by the backup server and the recovery back to the main server were manual processes and required customer intervention. This was an interim offer, made available until the ESS offer was released.

High-Level ESS Overview

The ESS option provides survivability to an Avaya configuration by allowing backup servers to be placed in various locations in the customer's network. The backup servers (ESS servers) are given administered values that are advertised to each IP Server Interface (IPSI) in the configuration. The IPSI places the ESS 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 ESS server on its list. The ESS Server accepts the request and assumes control of the IPSI controlled port network.

Detailed ESS Overview

In an ESS environment, there is only one main server. The main server can be a single server (S8500-Series server), or a duplicated server (S8700-Series server). If the main server is an S8500-Series server, all the ESS servers in the configuration must also be S8500-Series servers or an S8400 Server. For more information on server types that can be an ESS server or an LSP, see Table 1: LSP or ESS server types for Release 5.2 on page 15.

Note:

The S8500A Server and the S8700 Server cannot run Communication Manager 5.0 and later releases.

Through careful planning and consideration, the S8700-Series servers and/or S8500-Series servers are placed in various locations in the customer's network (Chapter 2: ESS Design and Planning on page 61). Each ESS server is administered on the main server. During administration, values are assigned to the ESS server. After administration, system translations are synchronized between the main server and the ESS server. Once the ESS server receives the translations, it advertises 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 advertise to IPSIs in their same community only. For more information on administering the values for ESS, see Administering ESS on page 130.

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

No service timer

During ESS 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. The IPSI may be requesting service from an ESS server after the IPSI loses communication with the main server or the controlling ESS server. The interval from the activation of the no service timer to the time the IPSI requests service of an ESS server is called the no service time out interval. The value for the no service timer is administrable from three to 15 minutes, with a default of five minutes. For more information on the no service timer, see Port Network Recovery Rules screen on page 141.

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 an ESS server

Existing Communication Manager recovery mechanisms still occur prior to a failover of a port network to an ESS server. For example, if a main server loses control of a majority of port networks it may attempt to switch to its standby server. This would happen before an IPSI requests service from an ESS 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 a loss of communication to the IPSI. The IPSI's no service timer activates.
  - Single server:
    a. Failure of the main server causes loss of communication to the IPSIs. The IPSI's 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 IPSI's no service timer to activate.
  - Single IPSI:
    a. Loss of communication between the IPSI and the main server causes the IPSI's no service timer to activate.

  Note:

  When an IPSI fails in an ATM environment, control fails over to an IPSI in another port network without loss of service.

  When an IPSI fails in a CSS environment, the port network is out of service.
- 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 ESS server on its priority list.

As part of a failover, the ESS 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
  - Active EI in a non-IPSI connected PN
  - SNIs
  - SNCs
  - DS1 clocks
- Every busied-out MO 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 ESS servers are configured, an individual ESS 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 ESS servers may be required to collectively accept control with each ESS server controlling some portion of the set of port networks.

When an ESS server accepts control, it communicates directly with each MCC1, CMC1, SCC1, G600, or G650 Media Gateway through the gateway's IPSI circuit pack. The ESS server can also control non-IPSI controlled port networks through an ATM Expansion Interface circuit pack. The ESS server communicates indirectly with each media gateway through Control-LAN (C-LAN) connections in the port networks.

Once the issue that caused the failover is resolved, you can put the control of an IPSI port networks 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 ESS on page 130.
- **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 three 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 ESS on page 130.

- **`get forced-takeover ipserver-interface all`**: The **`get forced-takeover ipserver-interface`** SAT command with the **`all`** parameter, allows an ESS server or main server to manually take control of all the IPSI port networks at once. This command must be issued from the ESS 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, Media 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 an ESS server or main server to manually take control of one IPSI port network. The command must be issued from the ESS 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, Media Gateways and Servers*, 03-300431.

Note:

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

LSP and ESS

Both an LSP and an ESS server are considered survivable servers. This section explains the differences between an LSP and an ESS server.

LSP

Each IP endpoint and each media gateway is manually configured with a list of call controllers during initialization. If for any reason, the communication between a media gateway and its primary controller stops, the media gateways and the IP endpoints register with a call controller on its list. If the LSP is in the list of call controllers, the media gateway and the IP endpoint registers with the LSP. The media gateway registers with the LSP first before the IP telephone registers with the LSP. The LSP does not control port networks or the media gateways.

The Processor Ethernet (PE) interface on an LSP can be used for:

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

For more information on Processor Ethernet, see Processor Ethernet overview on page 16.

You can have both ESS servers and LSPs in an ESS configuration.

ESS server

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

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

A single ESS server can use the Processor Ethernet interface to connect to CDR, AESVCS, and CMS. Duplex ESS servers can use the Processor Ethernet interface to connect to CDR, Messaging, and SIP Enablement Server (SES).

Communication Manager Release 5.2 provides the following enhancements:

- Processor Ethernet (PE) is supported on duplex servers for the connection of H.323 devices, H.248 Media Gateways, SIP trunks, and most adjuncts.
- The capabilities of Enterprise Survivable Servers (ESS servers) are enhanced to support connection of IP devices to the Processor Ethernet interface as well as to C-LAN interfaces located in Avaya G650 (port network) Media Gateways.
- 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.

Table 1 provides information on server types that can be used as an LSP or an ESS server for Communication Manager Release 5.2.

Table 1: LSP or ESS server types for Release 5.2

LSP or ESS server							
Main Server	**S8300B**	**S8300 C, D**	**S8400 A[1], B**	**S8510/ S8500 B, C**	**S8720**	**S8720 XL**	**S8730**
S8300B	LSP						
S8300C		LSP					
S8300D		LSP					
S8400	LSP	LSP					
S8500 B, C	LSP	LSP	ESS	LSP or ESS			
S8510	LSP	LSP	ESS	LSP or ESS			
S8710	LSP	LSP	ESS	LSP or ESS	ESS		
S8720	LSP	LSP	ESS	LSP or ESS	ESS		
S8720 XL		LSP	ESS	LSP or ESS		ESS	ESS
S8730		LSP	ESS	LSP or ESS		ESS	ESS

1. If you are using an S8400A server as an ESS, you must install a Memory Upgrade Kit (material code 218452).

Important:

The S8500A Server and the S8700 Server are not supported on Communication Manager 5.x and later releases.

Processor Ethernet overview

Starting with Communication Manager Release 3.1, Processor Ethernet (PE) can be used for IP connectivity. You can 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.

During the configuration of a server, the Processor Ethernet interface is assigned to an interface such as a control network or a corporate LAN. The selected interface determines which physical port the Processor Ethernet uses on the server. Communication Manager establishes a logical connection between the Communication Manager software and the physical port (NIC) for the Processor Ethernet interface. No additional hardware is needed.

Note:

The Processor Ethernet interface is supported on S8720 and S8730 servers for endpoint, gateway, or adjunct connectivity in Communication Manager Release 5.2 and later. If you have an S8710 server anywhere in your network, you cannot enable Processor Ethernet on any S87xx server without first upgrading the S8710 server to an S8720 or S8730 server.

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.

The Processor Ethernet administration is performed on the main server. The ESS receives the translations from the main server when a **`save translations all`** or **`save translations ess`** command is executed on the main server.

An LSP or an ESS server enables the Processor Ethernet interface automatically. On an LSP, 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.

In Communication Manager release 5.2 and later, H.248 Media Gateway and H.323 endpoint registration on an ESS 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 ESS server display the values that you administered.

Important:

Both the ESS server and the LSP require the use of the Processor Ethernet interface to register to the main server. Do not disable the Processor Ethernet interface on an ESS server or an LSP.

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

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

Possible functions of the PE interface	Main server	ESS server
Registration	The main server accepts registration messages from an ESS server or an LSP through the Processor Ethernet interface only if H.323 is enabled on the main server's 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.
H.248 media 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 an ESS 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 an ESS 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 Processor Ethernet interface on a duplex server to connect to CDR, Messaging (all that support IP connectivity), and SIP Enablement Server (SES)[1].	The way adjuncts connect to an ESS is administered on the **Survivable Processor** screen on the main server.

1. If you connect SIP Enablement Server (SES) to Processor Ethernet on the main server, SES will work on the main server but will not switch to an ESS in the event of the main server failure because SES supports only a single IP address for Communication Manager. If failover to ESS is required, connect SES through C-LANs.

For more information on how to administer the Processor Ethernet interface, see Page one of the Survivable Processor screen on page 132.

Support for Processor Ethernet and Port Networks on an ESS server

In Communication Manager Release 5.2 and later, the capabilities of ESS servers are enhanced to support connection of IP devices to the Processor Ethernet interface as well as to C-LAN interfaces located in G650 (port network) gateways.

An Enterprise Survivable Server (ESS) can use its Processor Ethernet interface to support IP devices such as H.248 Media Gateways, H.323 Media Gateways, IP Adjuncts, IP telephones, IP trunks, and SIP trunks. The ESS can optionally control port networks (G650 Media Gateways) through IPSI at the same time. When there are no port networks in the configuration, ESS may provide the equivalent benefit of an LSP. The ESS 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 LSP or ESS 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 ESS.
- If the LSP or ESS 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 ESS.

Firmware for optimal performance

Processor Ethernet on duplex servers works effectively only when the H.248 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 TTS (Time to Service) 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.

To ensure that you have the most current versions, go to the Avaya Support web site, http://avaya.com/support. Click **Downloads** and select the product.

C-LAN access for ESS registration

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

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

When an ESS server registers with the main server through the C-LAN, the main server validates the ESS Module ID, System ID, platform type, and IP address with that of the administered values. Only the active server of an S8700-Series server pair registers with the main server. Once registered, the ESS 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 an ESS server to register to the main server.

The ESS server re-registers with the main server when:

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

  Once translations are loaded on the ESS server, the ESS server re-registers with the main server. The ESS 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 ESS server selects a C-LAN from its list of available C-LANs. The ESS 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 an ESS server is still registered with the main server while controlling port networks, the ESS server can receive translation downloads from the main server. In this case, the ESS 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 ESS server used to register to the main server reboots or fails, the Keep-Alive messages from the ESS server to the main server stops. The main server shows the status of the ESS server as unregistered in the **`status ess cluster`** window. The ESS server attempts to communicate with the lost C-LAN. If attempts to communicate with the lost C-LAN fails, the ESS 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 ESS server to register to the main server reboots or fails, the Keep-Alive messages from the ESS server to the main server stops. The main server shows the status of the ESS server as unregistered in the **`status ess cluster`** window. The ESS server attempts to re-connect to the C-LAN. It the attempts fail, the ESS server selects another C-LAN from its list of C-LANs.
- The Network experiences problems: If network problems prohibit communication between the ESS server and the C-LAN, the Keep-Alive messages between the ESS server and the main server terminates. The main server shows the ESS server as unregistered in the **`status ess cluster`** window. If multiple C-LANs are used in this configuration, the ESS server selects another C-LAN from its list and attempts to re-register with the main server using the new C-LAN.

ESS requirements

An ESS configuration requires the following:

- The main server and each ESS server must be running Communication Manager Release 3.0 or later.
- The main server can either be an S8500-Series server, or an S8700-Series server. If the main server is an S8500-Series server, all ESS servers must be S8500-Series servers or S8400 Server. The S8400 ESS server is available only in Communication Manager Release 5.2 and later and has some limitations and special requirements, as described in S8400 as an ESS server on page 21. The capacities of the port network in which the ESS server resides must not exceed the published capacities of the ESS server. For detailed 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 an ESS environment, see the Minimum Firmware/Hardware Vintages document at http://support.avaya.com.
- A separate license file for the main server and each ESS server: Each license file must contain a unique serial number of a reference IPSI, a unique MID and a common SID.
- An IP network that provides connectivity for all IPSIs and servers.
- In a CSS environment:
  a. You must have an IPSI and an IP Media Processor circuit pack for each survivable CSS port network. In an ESS environment, a survivable port network is one that is designed to failover to an ESS server when communication to the main server is lost.
  b. In addition, you must have one or more TN570D circuit packs in each port network that contains an IPSI. If the TN570 circuit pack is not a TN570D, you must upgrade the circuit pack.

Note:

A port network that is not survivable (the port network does not have an IPSI and will not failover to an ESS server), can use the TN570B version 7 or later. For example, remote location A is the only location within the system designed to failover to an ESS server. In this case, all the port networks within location A need a TN570D expansion interface. Other non-survivable locations within the system can use the TN570B version 7 expansion interface.

- For duplicated IPSI control, the S8500-Series server must be equipped with a dual NIC card.

S8400 as an ESS server

Important:

Before you start implementing an S8400A Server as an ESS server, you must purchase and install a Memory Upgrade Kit (material code 218452).

S8400 ESS server limitations

- An S8400 ESS server functions only in a *local only* mode and can only be installed in a G600, G650, or CMC1 Media Gateway.
- An S8400 ESS server cannot be used as a survivability option for an S8400 main server.
- An S8400 main server can support Communication Manager Messaging (CMM) service. However, the CMM administration is blocked in an S8400 ESS server.
- An S8400 main server can support up to five H.248 Media Gateways using either a TN799 C-LAN circuit pack or Processor Ethernet. An S8400 ESS server can support H.248 Media Gateways using a TN799 C-LAN circuit pack. Processor Ethernet is also supported in this configuration if you administer Processor Ethernet to support H.248 Media Gateways using the **Survivable Processor** screen.
- An S8400 ESS server only supports IP-PNCs (port network connectivity), not fiber-PNCs.

S8400 ESS server hardware requirements

The TN8400 circuit pack requirements must be one of the following:

- TN8400AP with 1 GB DRAM and a 4 GB SSD (the material code for the TN8400AP upgrade kit is 218452)
- TN8400BP

When S8400 is used as an ESS server, the TN8412AP Server IP Interface (SIPI) circuit pack is not supported. If the S8400 ESS server is installed in a G650 media gateway, the IP Server Interface (IPSI) that it supports must be a TN2312BP IPSI or later. TN799 C-LAN circuit pack or Processor Ethernet is required if H.248 Media Gateways are to be supported by an S8400 ESS server.

ESS failover examples

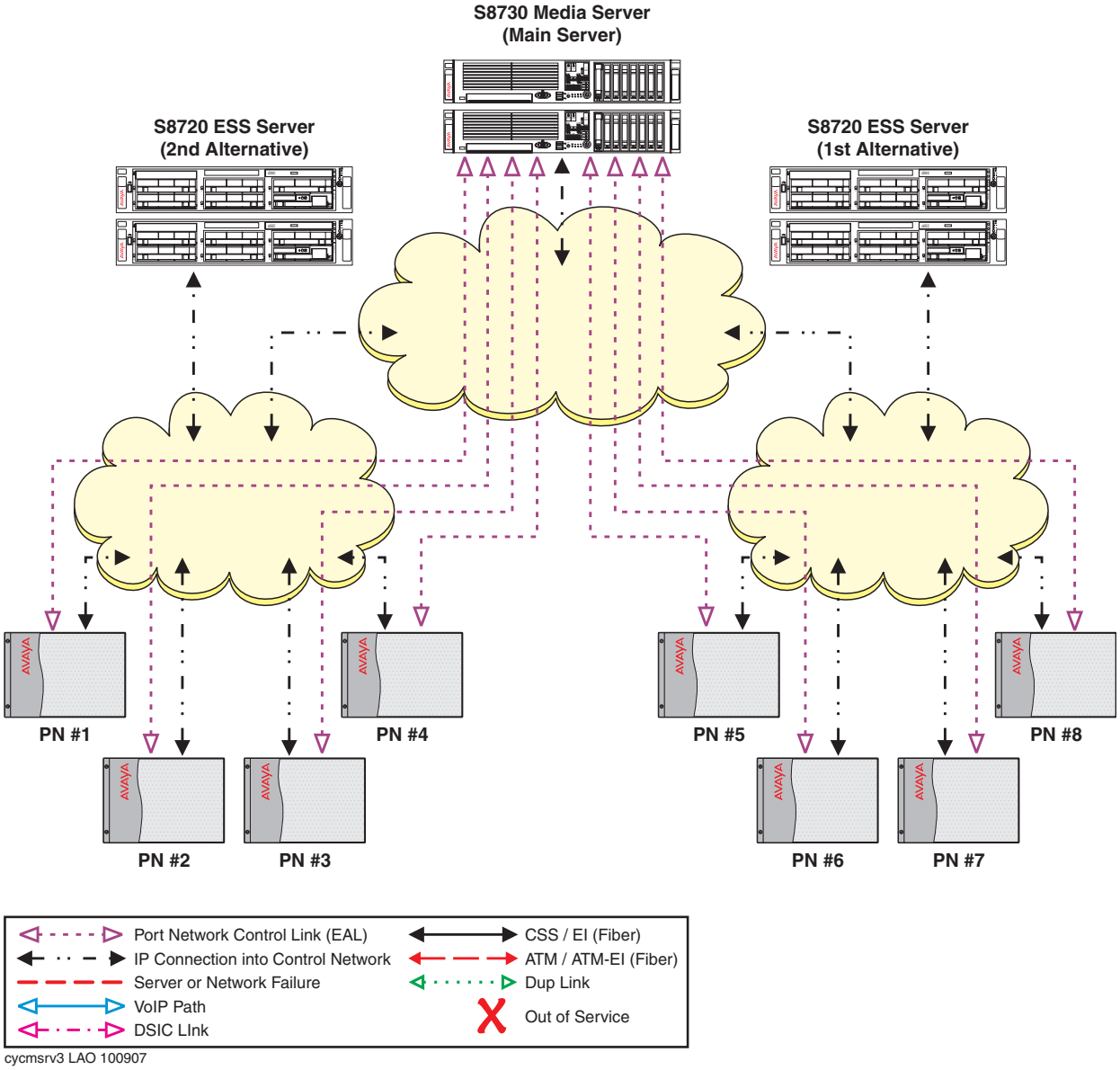
This section contains examples that are fabricated to illustrate ESS functionality. The examples illustrate LAN/WAN and server failures in different configurations.

Example one: Main servers fail

Important:
Communication Manager Release 5.x and later is not supported on the S8700 Server and the S8500A server.

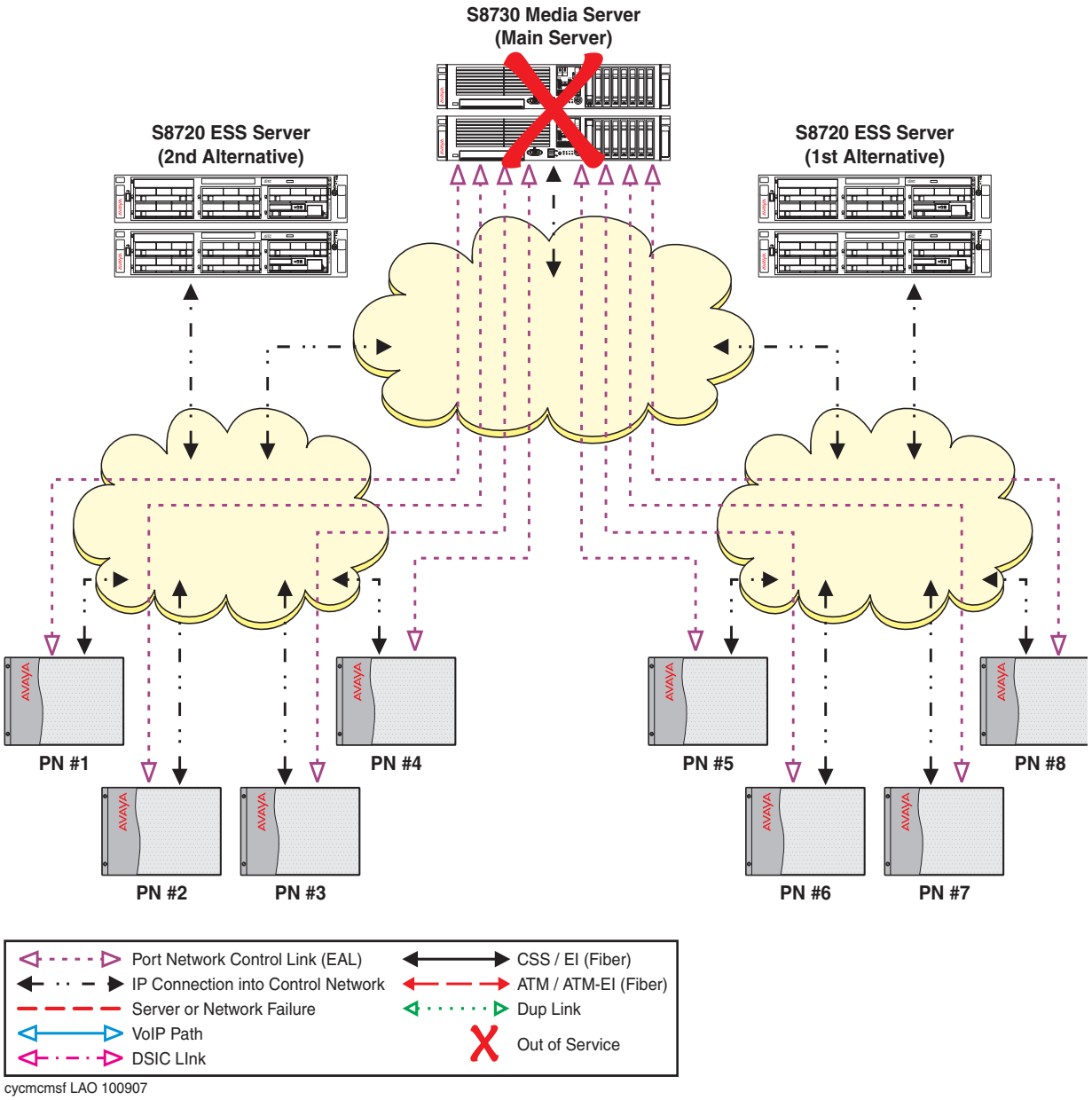
In example one (Figure 1), the S8730 Server is acting as the main server in an ESS environment. Two ESS servers have been positioned in the network. Through administration on the main server, an S8720 Server is selected as the primary backup or 1st alternative to the main server. An S8720 Server is acting 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 ESS configuration is to keep all port networks under the control of a single server.

Figure 1: S8730 Server with ESS servers in normal operation



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

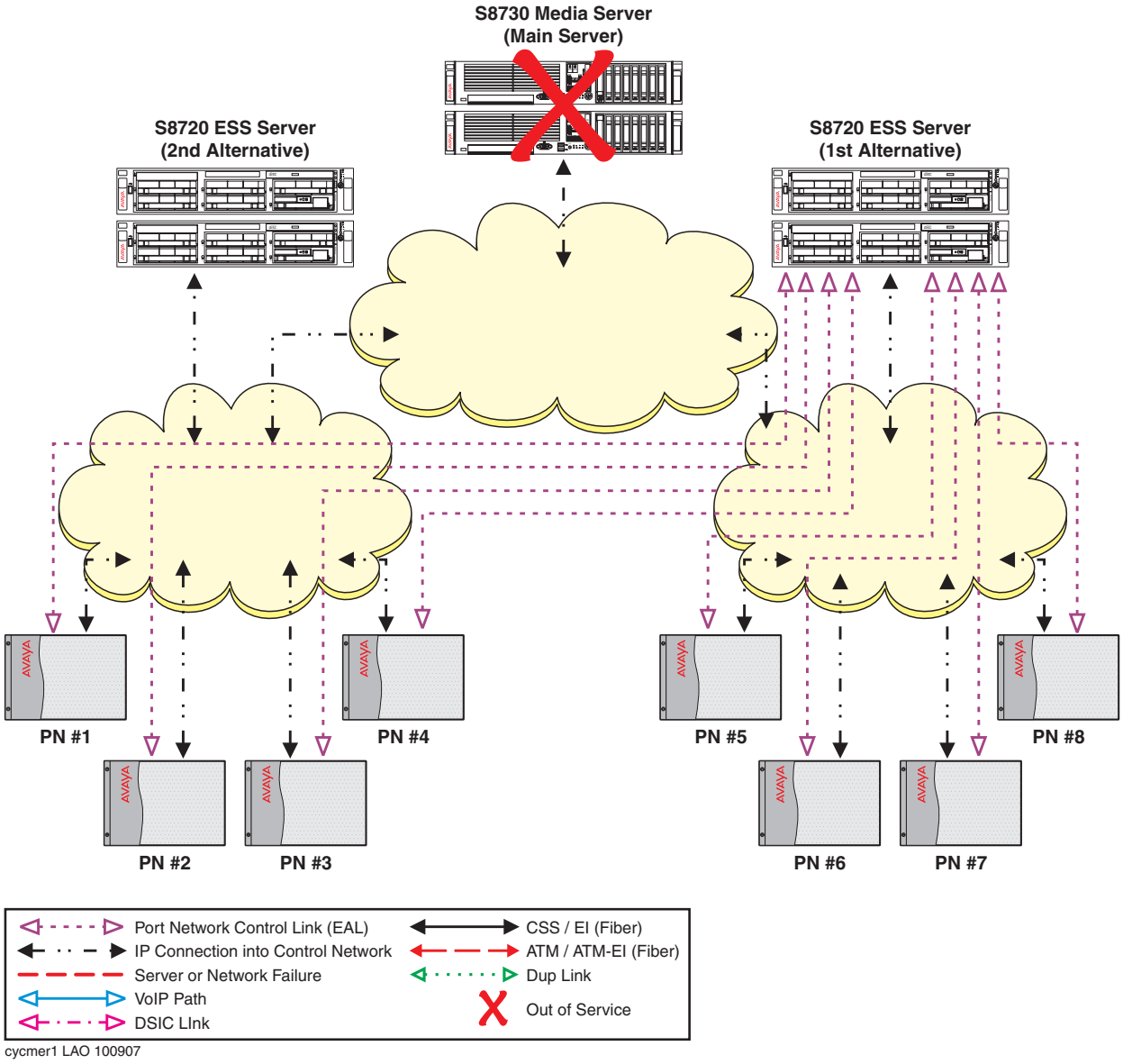
Figure 2: Catastrophic main server failure



When ESS server was administered on the main server, the 1st alternative S8720 Server received higher values than the 2nd alternative S8720 Server. The administered values of the ESS servers are advertised to the IPSIs in the configuration. Based on the values of the ESS servers, the IPSI placed the 1st alternative ESS server higher on its priority list then the 2nd alternative ESS server.

The no service timer expires (Figure 3), the IPSIs request service from the highest ESS server on its list (1st alternative). The 1st alternative ESS server acknowledges the request and takes control of the IPSI controlled port networks.

Figure 3: main servers fail- ESS server recovery of failure



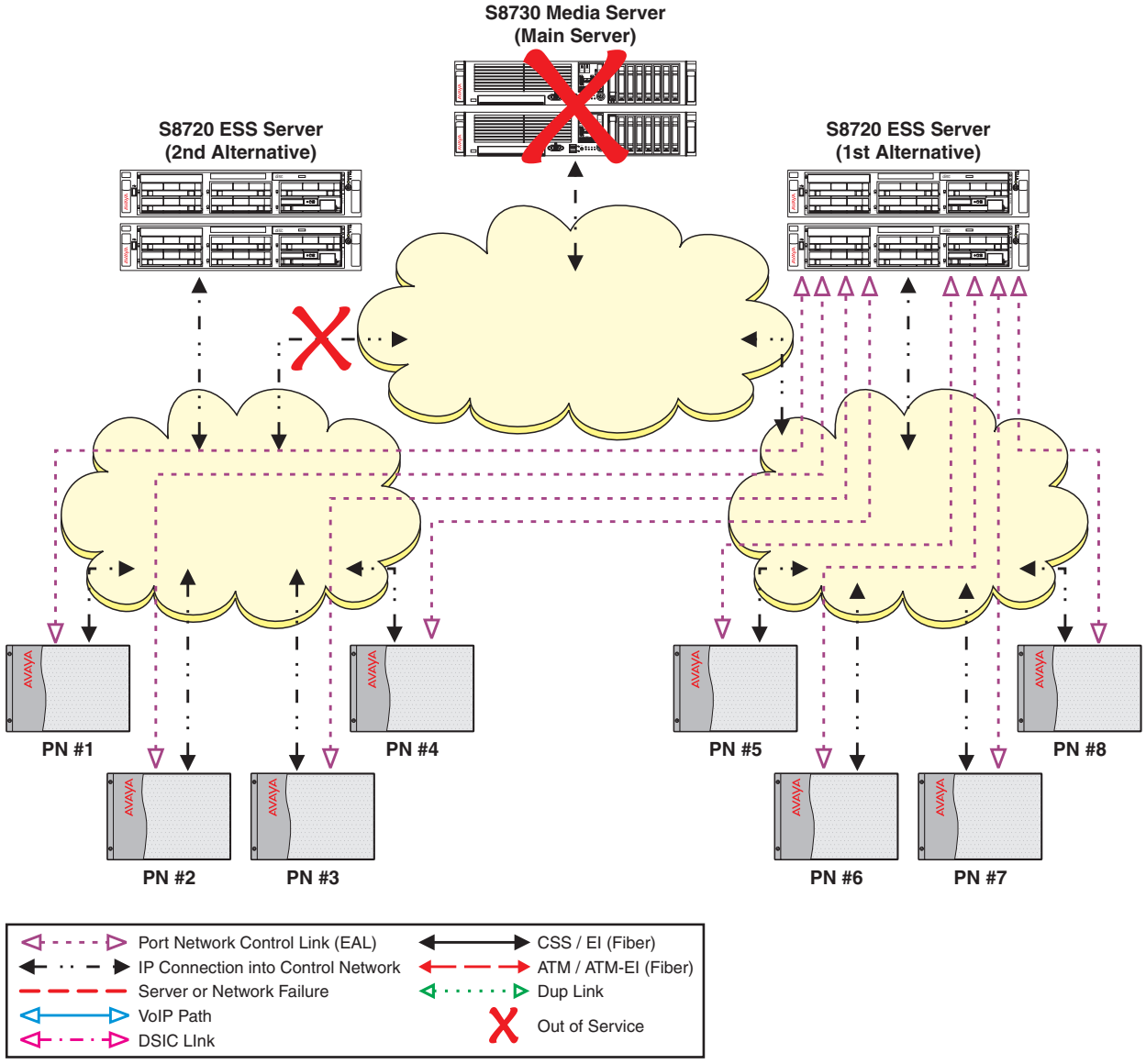
Example two: Network failure

Important:
Communication Manager Release 5.x and later is not supported on the S8700 Server and the S8500A server.

Example two uses the same configuration used in example one. The S8730 Server is the main server, with two S8720 ESS 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 ESS 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 ESS server but can no longer communicate with the main server or the 1st alternative ESS server. Port networks five through eight can still communicate with the 1st alternative ESS server but can no longer communicate with the 2nd alternative ESS server.

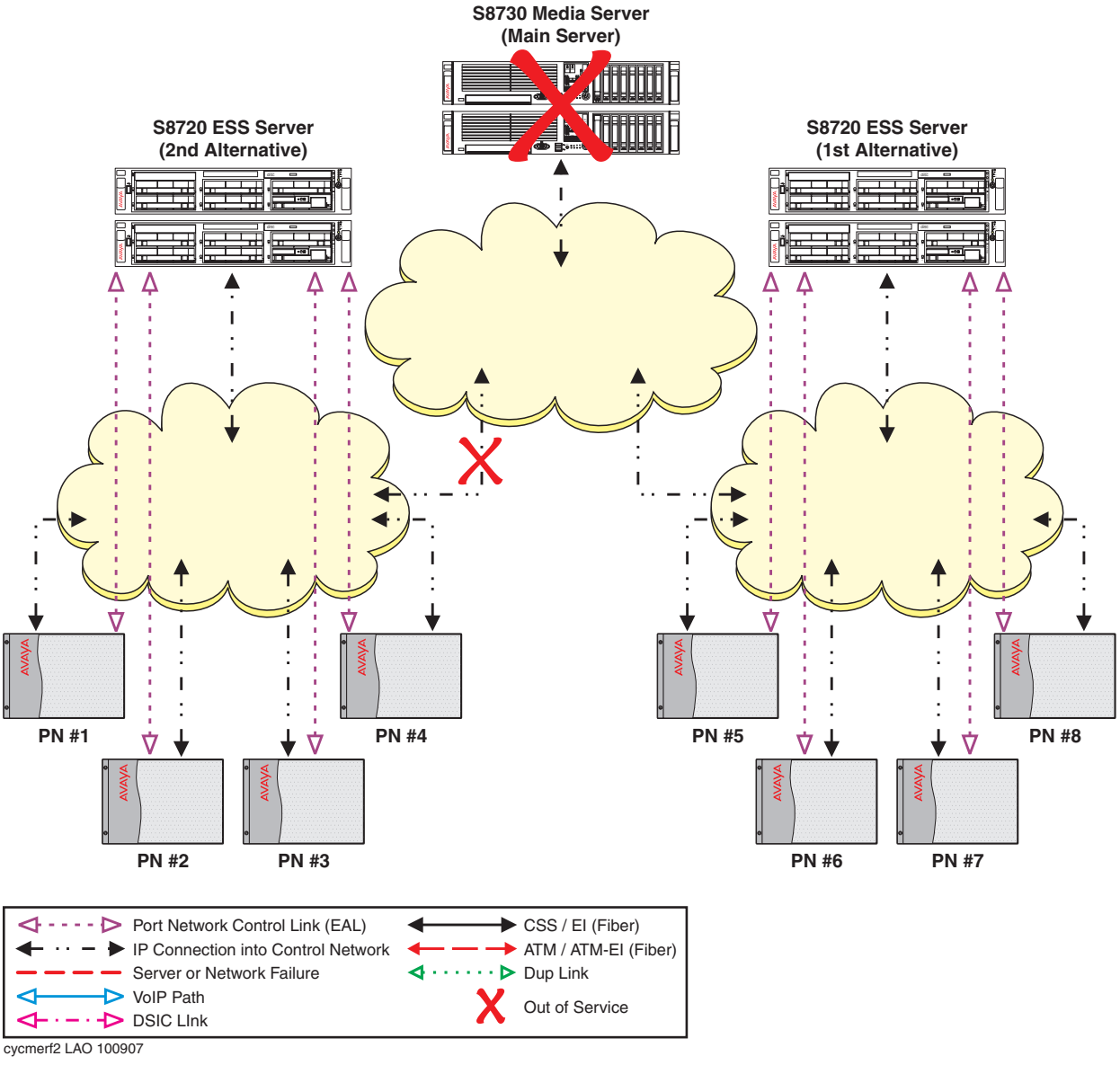
Figure 4: Network fragmentation failure



cycmnff LAO 100907

Because the IPSIs in port networks one through four are not longer able to communicate with the main server or the 1st alternative ESS server, they adjust their priority list and move the 2nd alternative ESS 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 ESS server. The 2nd alternative S8720 ESS 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 - ESS recovery

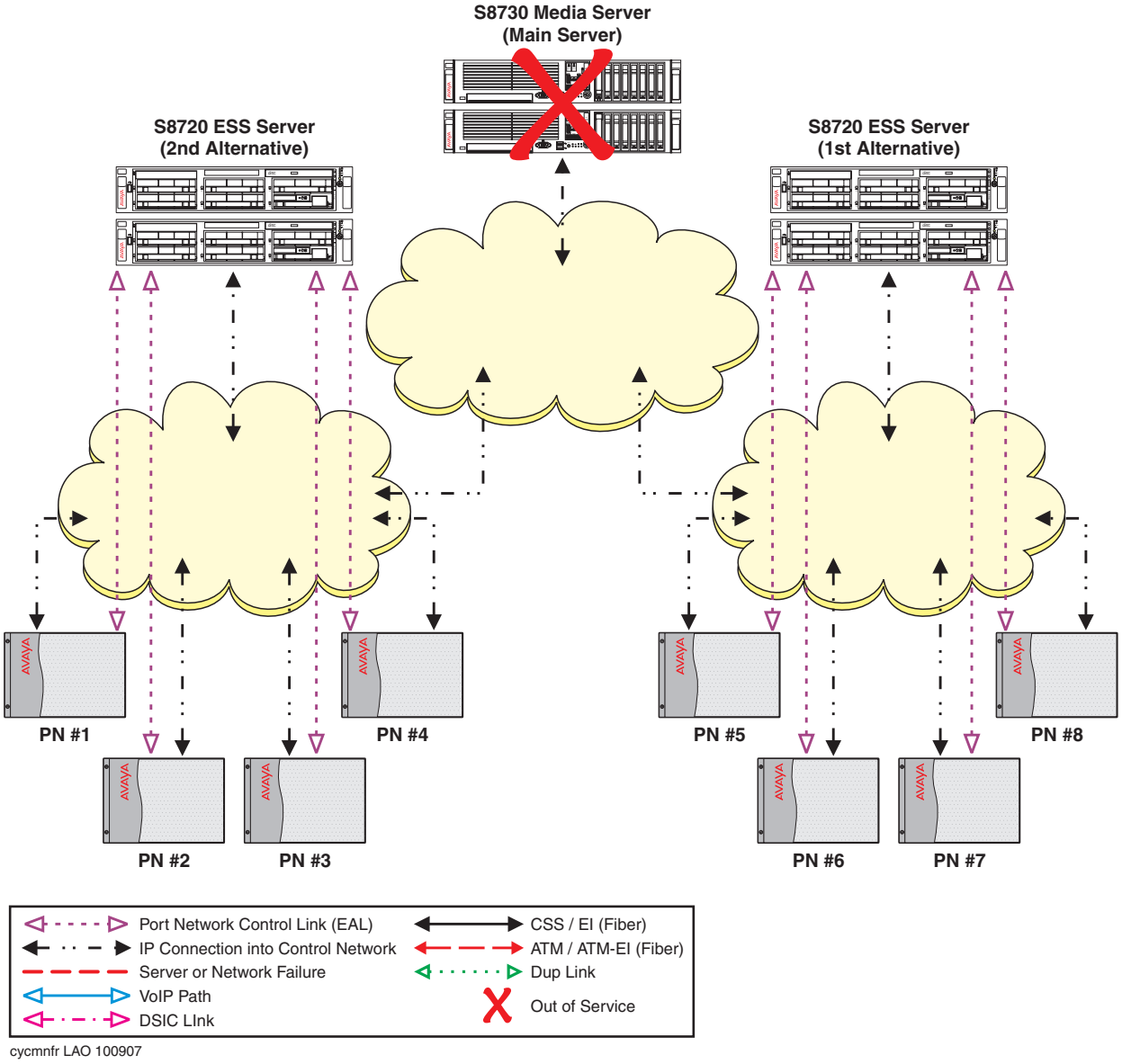


The users in port networks one through four experience the following:

- 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.

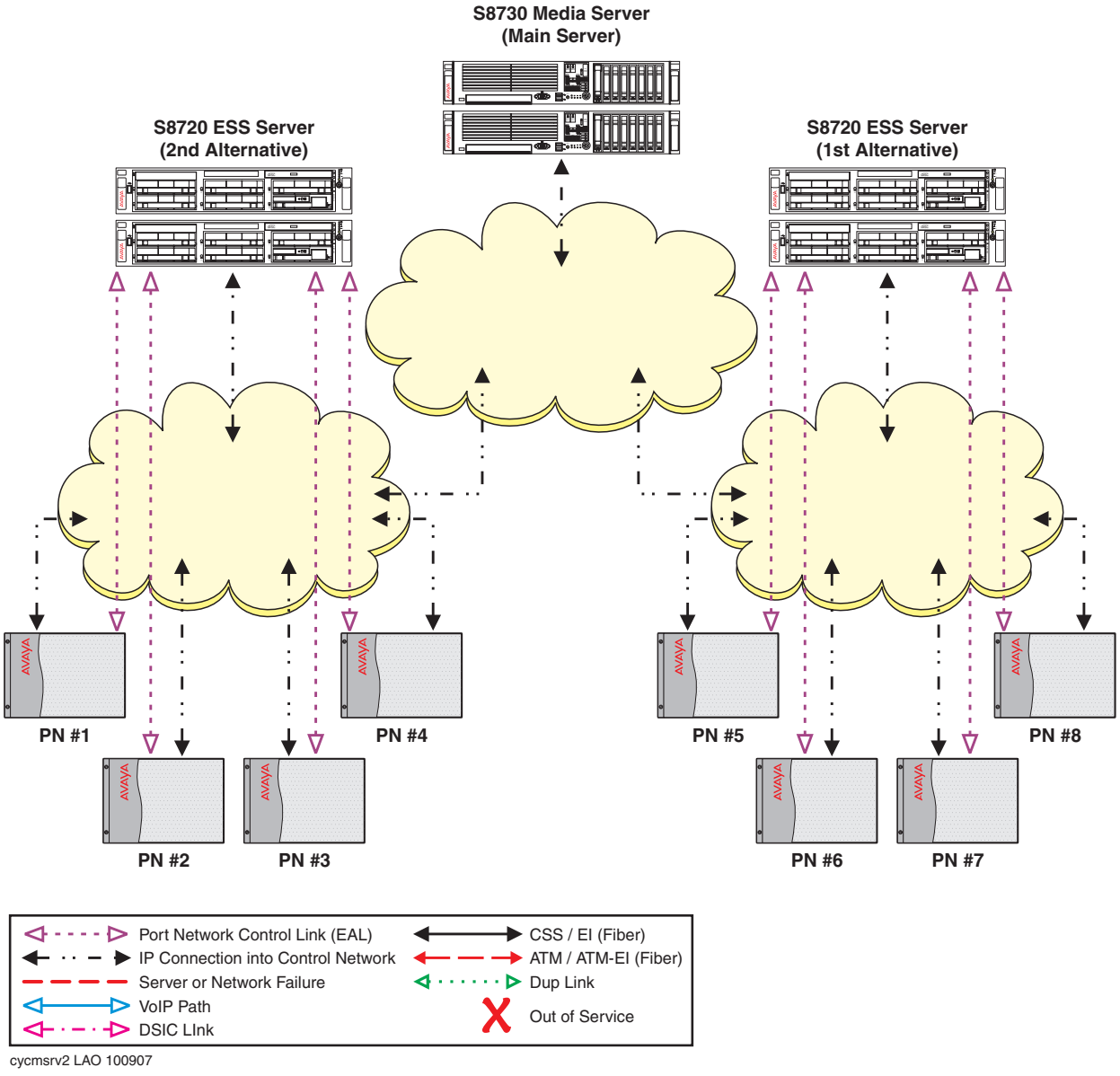
The customer is now in the process of recovering from both the network failure and the main server failure (Figure 6). As the network failure is fixed, the IPSIs in port networks one through four can now communicate with the 1st alternative ESS server. The IPSI priority list adjusts to reflect the 1st alternative as the highest priority ESS server. Even though the IPSI priority list now shows the 1st alternative server as its highest priority ESS 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 ipsi-interface`** command or scheduling the Auto Return functionality. For information on the **`get forced-takeover ipsi-interface`** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. For information on the Auto Return functionality, see **`Port Network Recovery Rules screen`** on page 141.

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 ESS server. The main server is always the highest priority on any IPSI priority list.

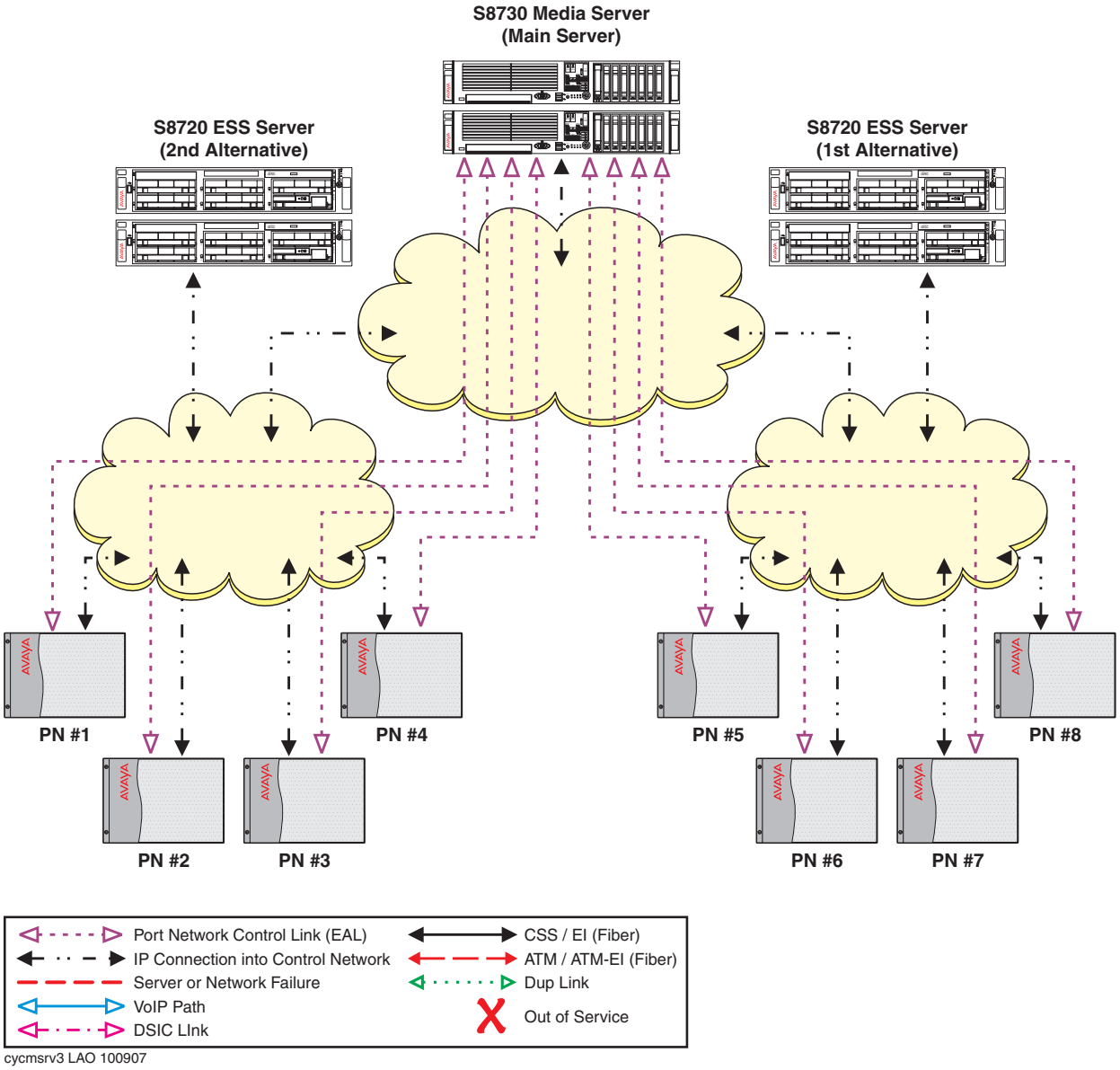
Figure 7: Main server recovery



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 ipsi-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 ipsi-interface all`** command.
- Administering the Auto Return capability on the main server (Administering ESS on page 130).

Figure 8: Fall-back to main server



cycmsrv3 LAO 100907

Example three: Combined IP connected port networks with CSS or ATM connected port networks

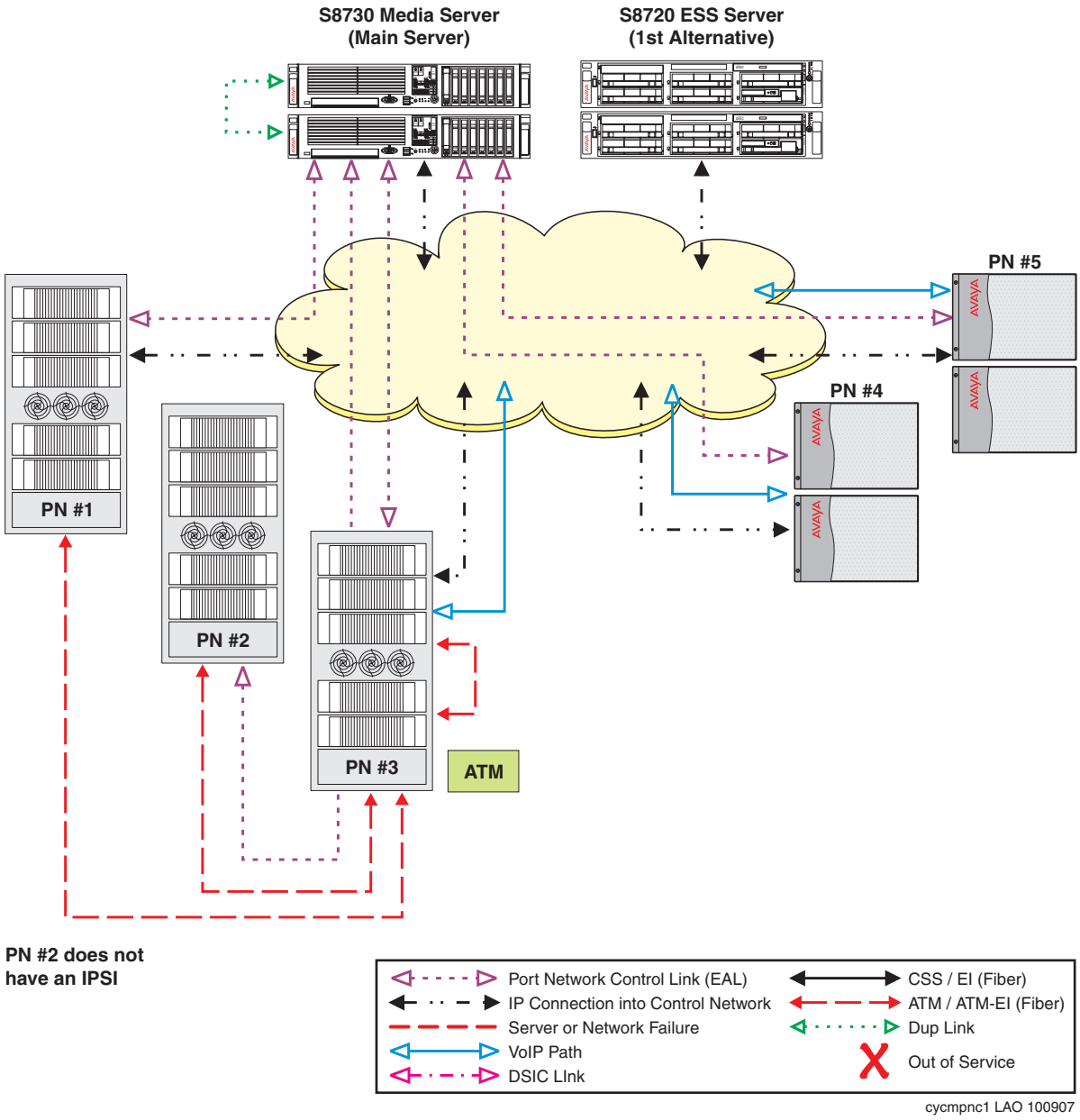
Important:
Communication Manager Release 5.x and later is not supported on the S8700 Server and the S8500A server.

Starting with Communication Manager Release 3.0, mixed configurations that combine IP-PNC with CSS-connected or ATM-connected port networks are supported. Additionally, servers can support both single control networks and duplicated control networks in the same configuration as well as single bearer networks and duplicated bearer networks. Simultaneous single and duplicated control/bearer connectivity cannot be achieved in traditional CSS and ATM connected port networks.

In example three (Figure 9), the customer has an environment where:

- Port networks one through three are part of a Center Stage Switch (CSS).
  - Port network two connects to the main server through port network three.
  - IPSIs are installed in port network one and three.
- Port networks four and five use IP connect.

Figure 9: Mixed port networks in normal operation

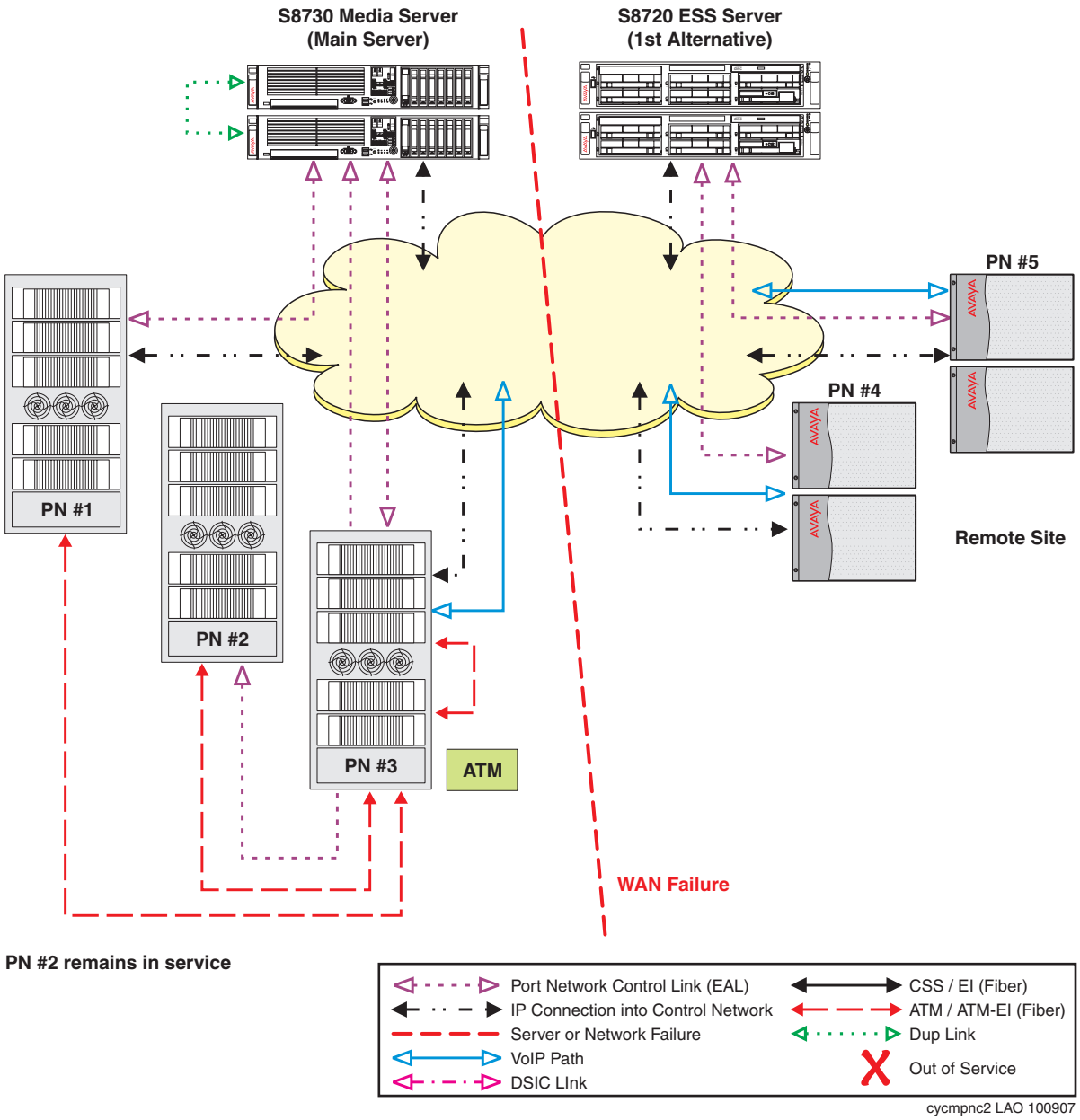


A WAN failure occurs (Figure 10). Port networks four and five can no longer communicate with the main server but can still communicate with the 1st alternative ESS server. The no service timer activates for IPSIs in port networks four and five. After the no service timer expires, the IPSIs in port networks four and five request service from the 1st alternative ESS server. The 1st alternative ESS server assumes control of port networks four and five. Port networks one, two, and three remain under the control of the main server and do not experience any service interruptions.

The system is now fragmented between two controlling servers. The following occurs:

- Some functionality provided by adjuncts may be missing for users in port networks four and five. For more information on adjuncts, see Feature considerations on page 85.
- Users on each side of the fragmentation cannot make normal station-to-station calls to port networks on the other side of the fragmentation.

Figure 10: Mixed port network after failover



Example four: ESS with Center Stage Switch (CSS)

ESS requires that all survivable port networks in a CSS environment, connect to the network using an IP Media Processor circuit pack. The following information must be considered for an ESS in a CSS environment:

- To be survivable, ESS requires that all port networks within a CSS environment must have the ability to transition to IP bearer. To transition to IP bearer the designated survivable port networks must have an IPSI for control and IP Media Processor circuit pack for bearer communication.
- All IPSI connected port networks must have a TN570D Expansion Interface.
  - In an ESS environment, aTN570D is required when it resides in a port network that also contains IPSIs and the port network will failover to an ESS server.

  Note:

  Port networks that do not have IPSIs, and therefore are not survivable, can use the TN570B version seven or later.
- While the former MBS option utilized the CSS during a failover, the ESS server never controls the CSS.

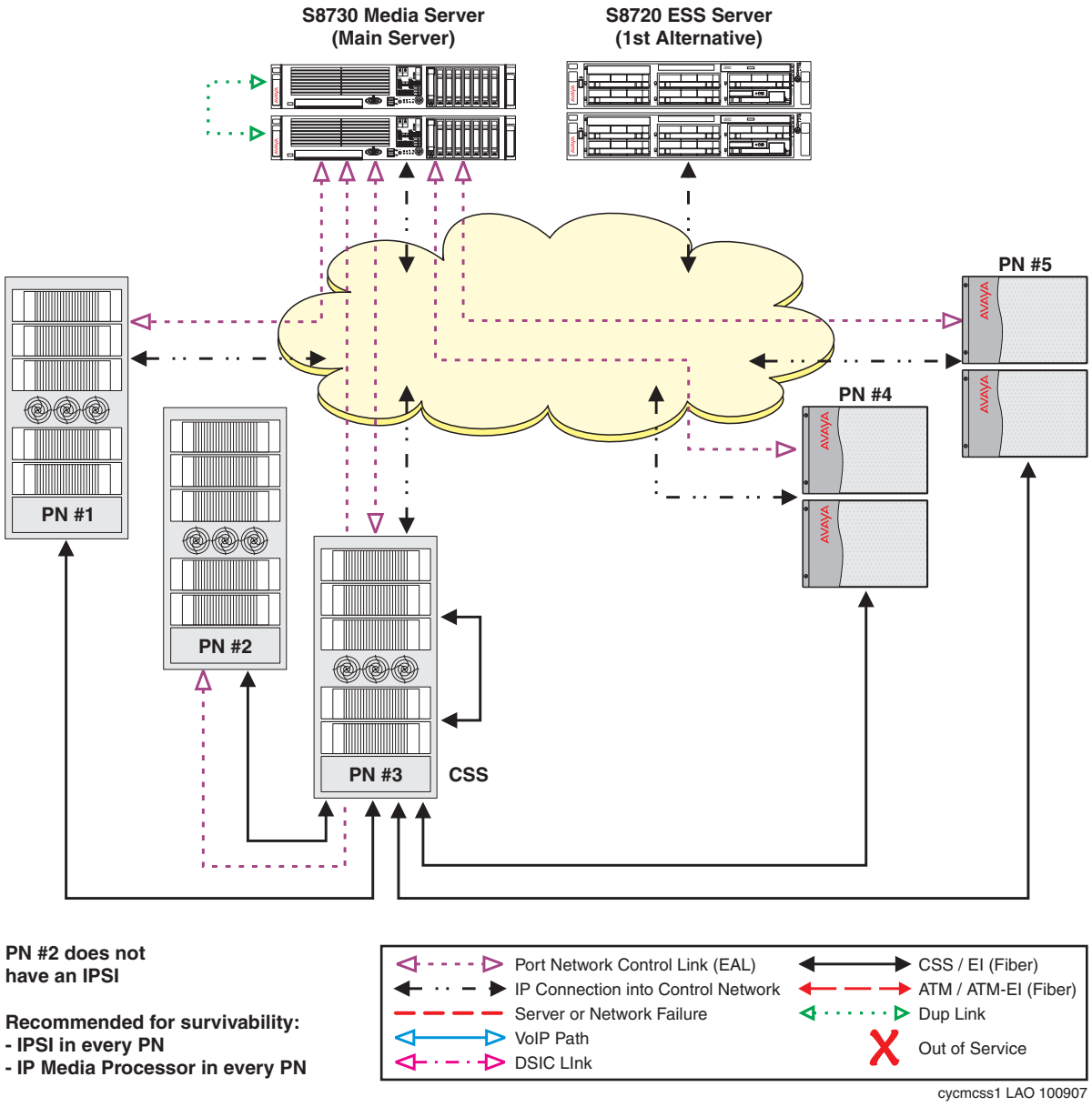
  Important:

  When an CSS system fails over to an ESS server, the port network connectivity transitions to IP-PNC.

In example 4 (Figure 11), the S8730 main server provides service to IPSI connected port networks one, three, four, and five. Port network two communicates with the main servers through its EI circuit pack, the CSS, and the IPSI circuit pack in port network three.

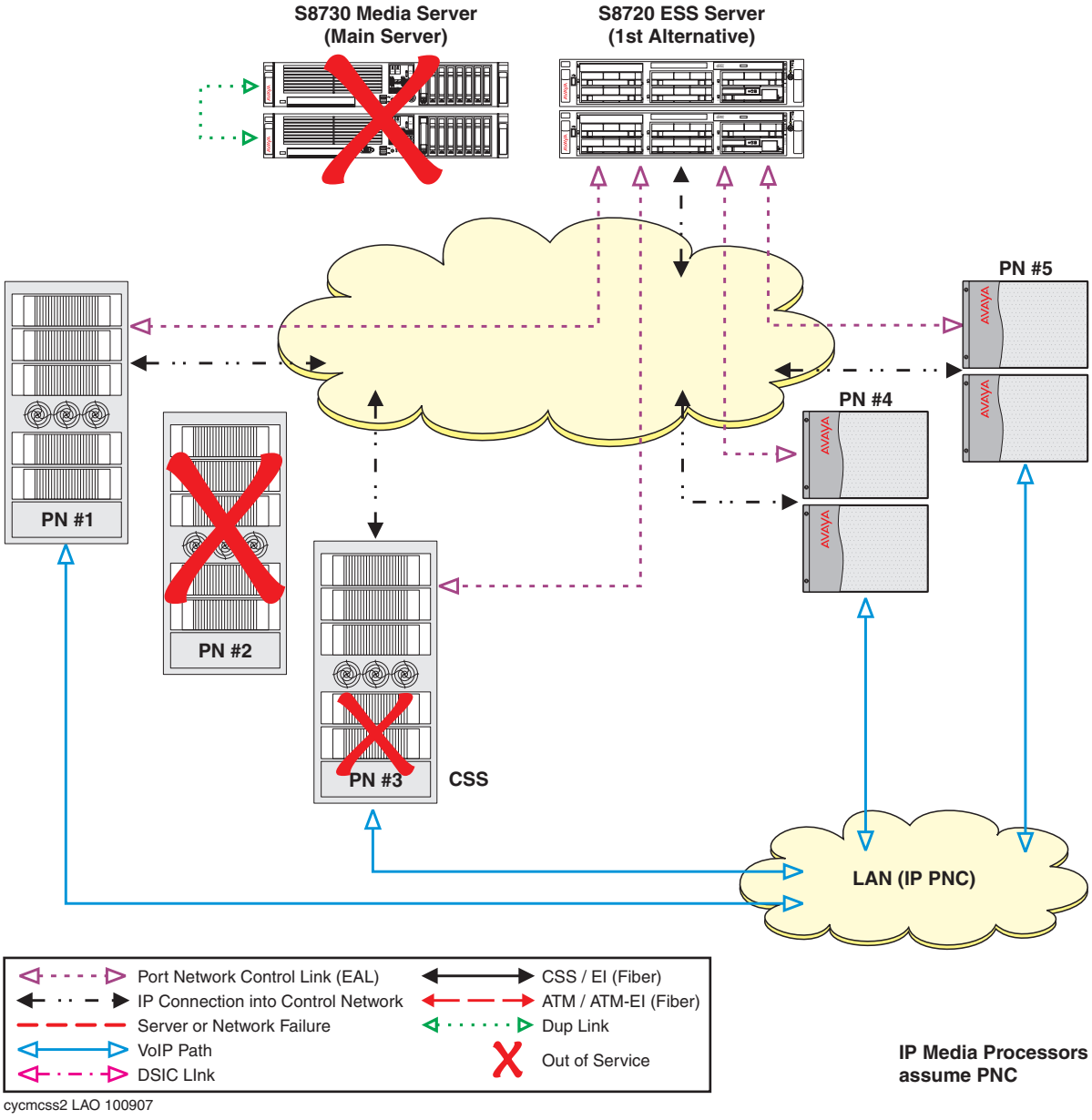
There is only one ESS server in this example.

Figure 11: Normal operation CSS with single ESS



A catastrophic failure occurs on the S8730 main server (Figure 12). The port networks can no longer communicate with the main server. The IPSIs in port networks one, three, four, and five, request service from the S8720 ESS server after the no service timer expires. ESS does not utilize CSS, therefore port network two and the CCS located in port network three is out-of-service.

Figure 12: CSS after failover with single ESS server



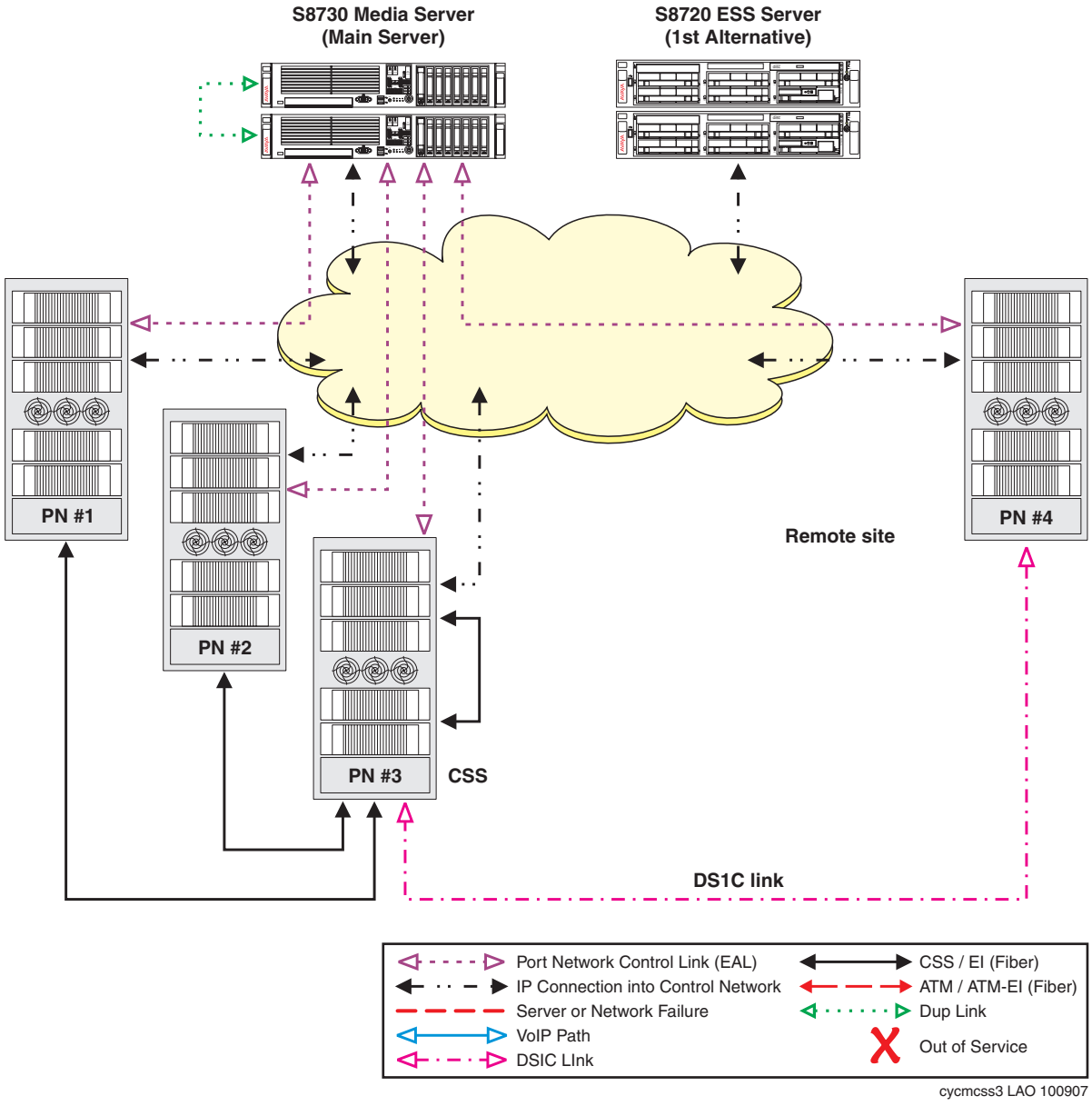
Example five: CSS with DS1C

Important:

Communication Manager Release 5.x and later is not supported on S8700 Servers and S8500A servers.

In example five, port network four is remotely connected to the CSS using a DS1C. Port network four is equipped with Public Switched Telephone Network resources. There is an IPSI in each port network.

Figure 13: CSS with DS1C - normal operation



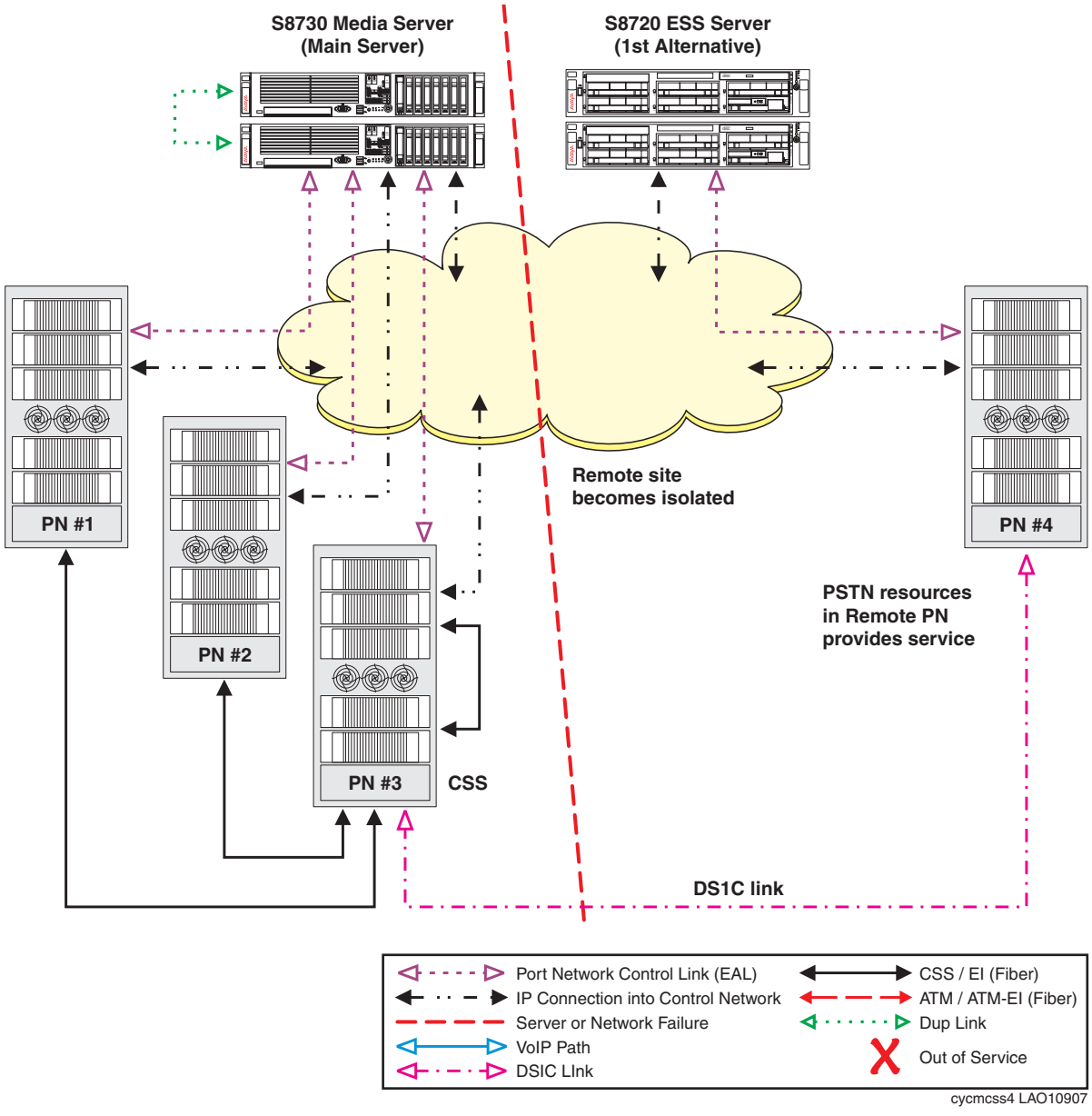
A network problem occurs where port network four is isolated from the CSS and the DS1C link (Figure 14).

Note:

If only the DS1C link was lost, port network four would not transition to the ESS server. Communication between the DS1C location and the main location would be disrupted since there is no bearer path.

After the no service time out interval expires, the IPSI in port network four requests service from the S8720 ESS server. The Public Switched Telephone Network resources enable local and long distance calling.

Figure 14: CSS with DS1C - remote takeover



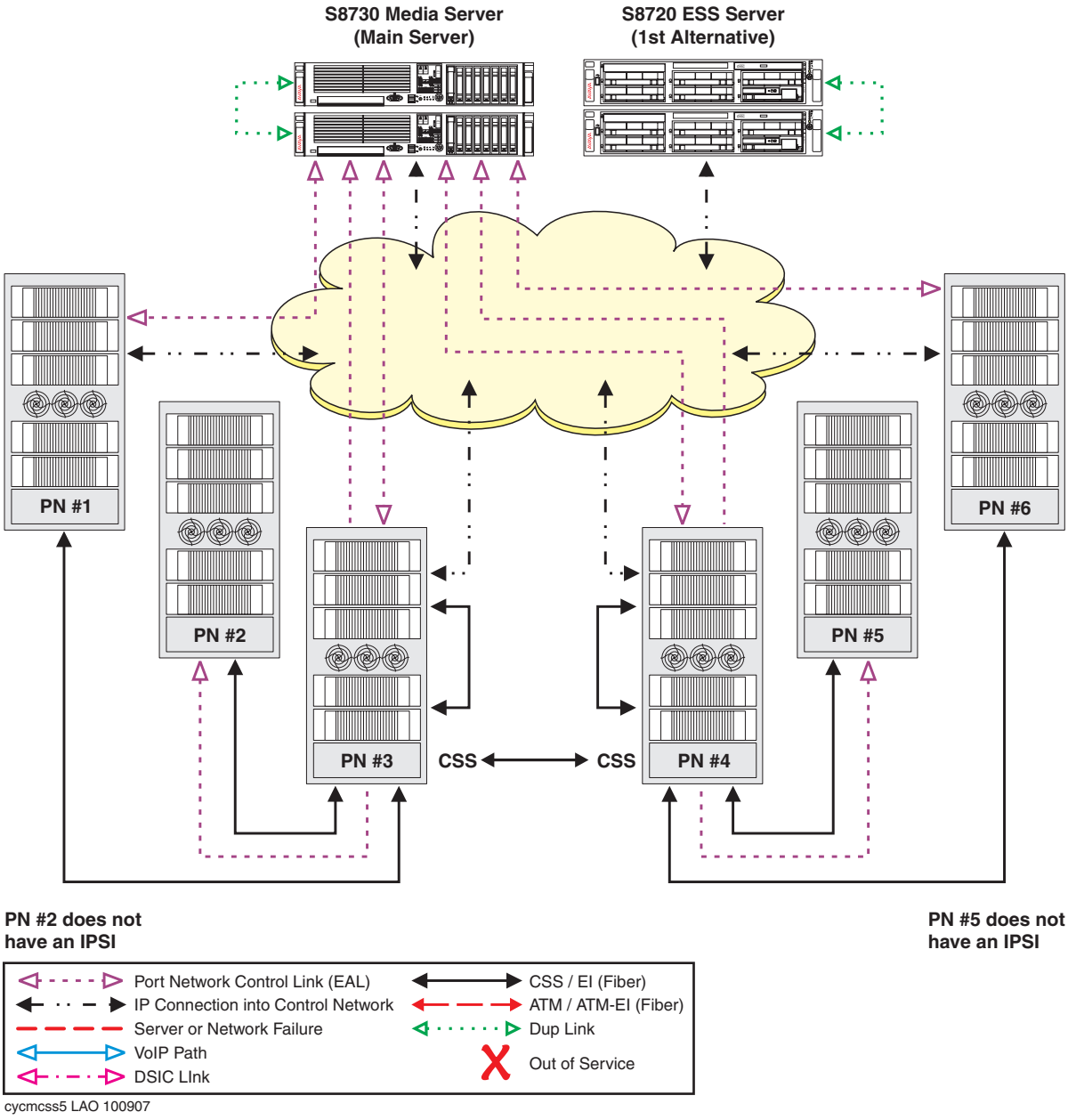
Example six: CSS with multiple nodes

Important:

Communication Manager Release 5.x and later is not supported on S8700 Servers and S8500A servers.

In example six, there is a multiple node CSS controlled by the S8730 main server. Port network two is connected to the CSS node in port network three. Port network five is connected to the CSS node in port network four. There are no IPSIs in either port network two or port network five (Figure 15).

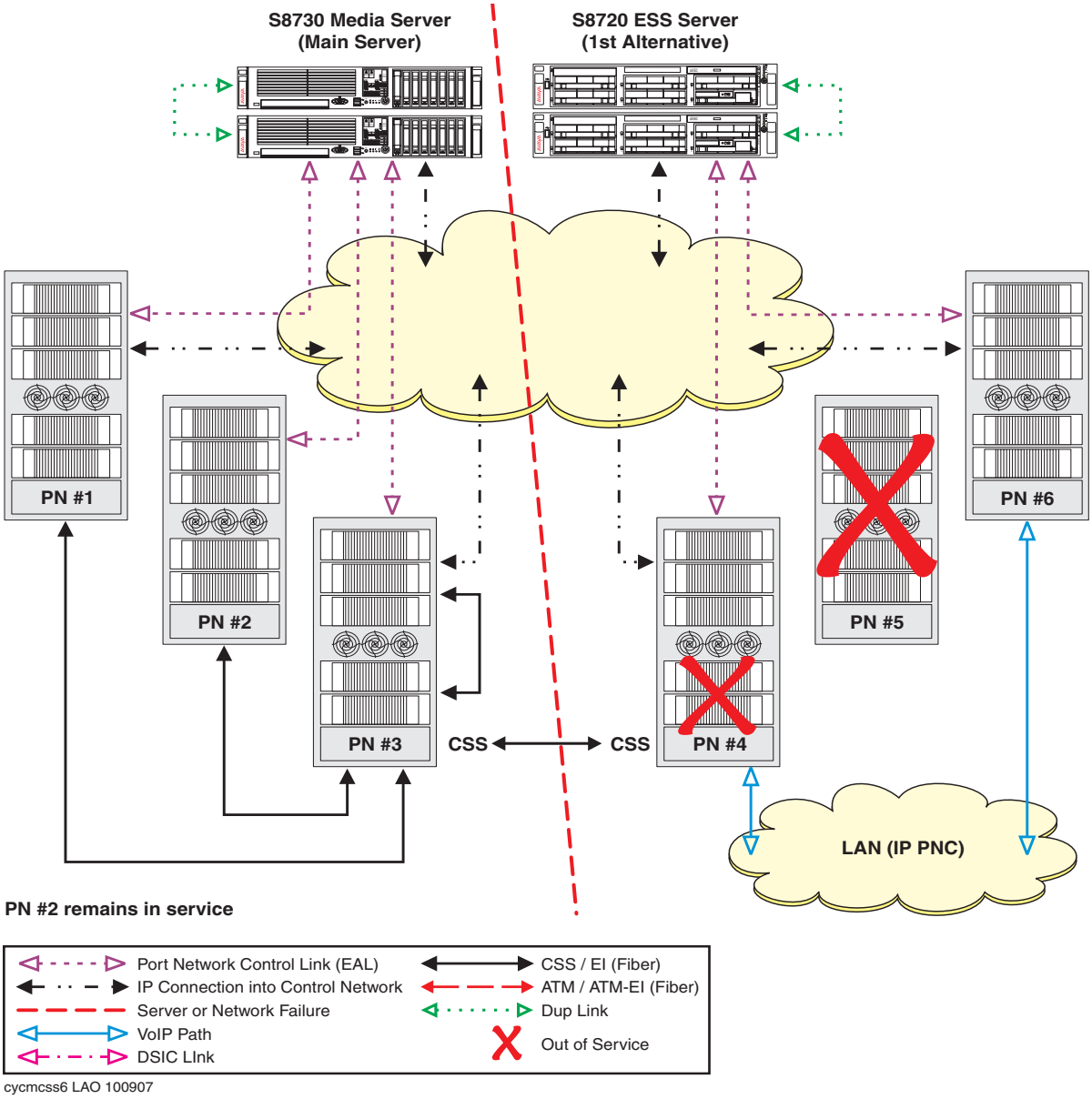
Figure 15: CSS with multiple nodes in normal operation



A network outage occurs that stops communication from the main server to port networks four through six (Figure 16). The main server continues to provide service to port networks one through three. The no service timer activates for port networks four and six. After the no service timer expires, the IPSI in port network four and port network six requests and receives service from the S8720 ESS server. The ESS server cannot take control of the CSS node in port network four. The CSS node in port network four is not utilized. Port network five is also not

utilized as it does not have an IPSI and can no longer communicate with the CSS node in port network four. Port networks one, two, and three, are not affected by the outage.

Figure 16: CSS with multiple nodes - failover



cycmcss6 LAO 100907

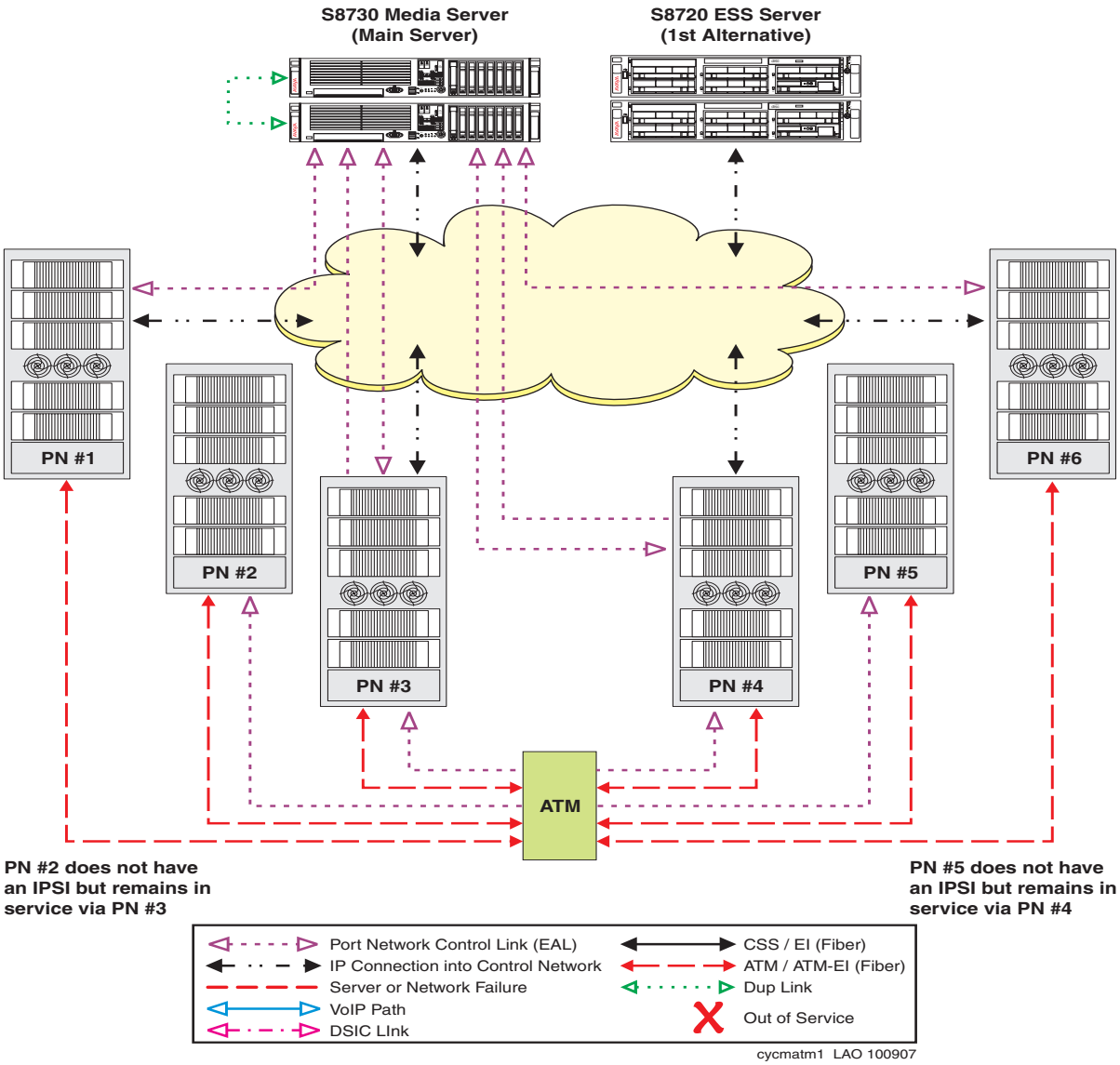
Example seven: ESS with ATM

Important:
Communication Manager Release 5.x and later is not supported on S8700 Servers and S8500A servers.

For port networks that do not have an IPSI but are controlled by the main server through ATM connections, an ESS server similarly communicates indirectly through an IPSI controlled port network, and then through an ATM connection (TN2305B or TN2306B ATM Expansion Interface circuit pack).

In example seven (Figure 17), there is a single ESS server in an ATM configuration. The S8730 is the main server with an S8720 Server as the ESS server. IPSIs are installed in all port networks except port network two and port network five.

Figure 17: ATM with a single ESS server in normal operation



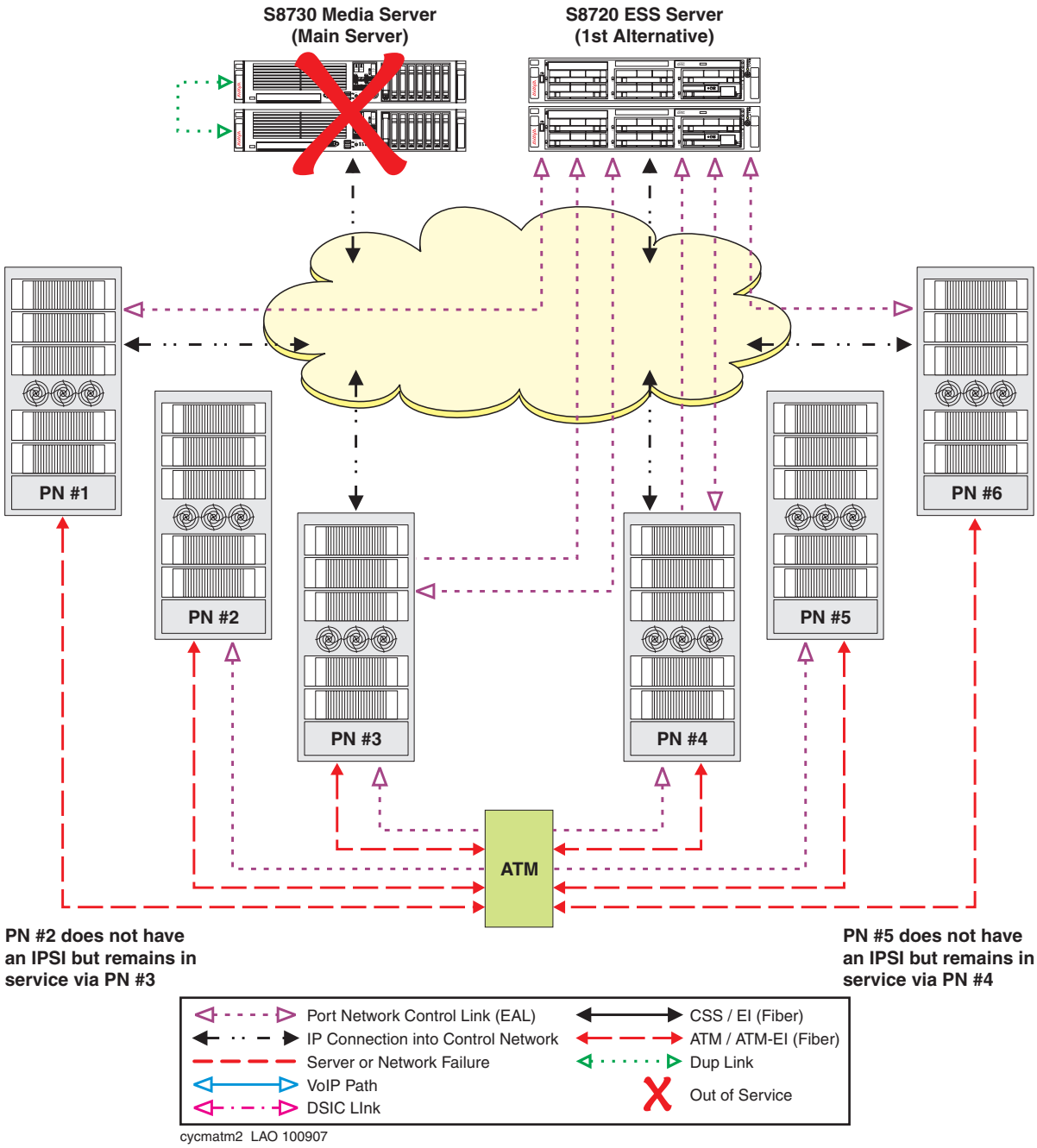
ATM - single ESS takeover examples

In the first takeover example (Figure 18), a catastrophic failure happens to the S8730 main server. The IPSIs request service of the S8720 ESS server after the no service timer expires. The S8720 ESS server assumes control of port networks one, three, four, and five. Once the S8720 ESS server assumes control of the port network, it attempts to take over all other port networks in the system through the ATM Expansion Interface (EI) board (TN2305B or TN2306B). Since there isn't a server that is controlling port network two and port network five, the attempt by the S8720 ESS server to control port network two and port network five through the ATM EI is successful.

Important:

Port networks in an ATM environment do not transition to IP during a failover to an ESS server.

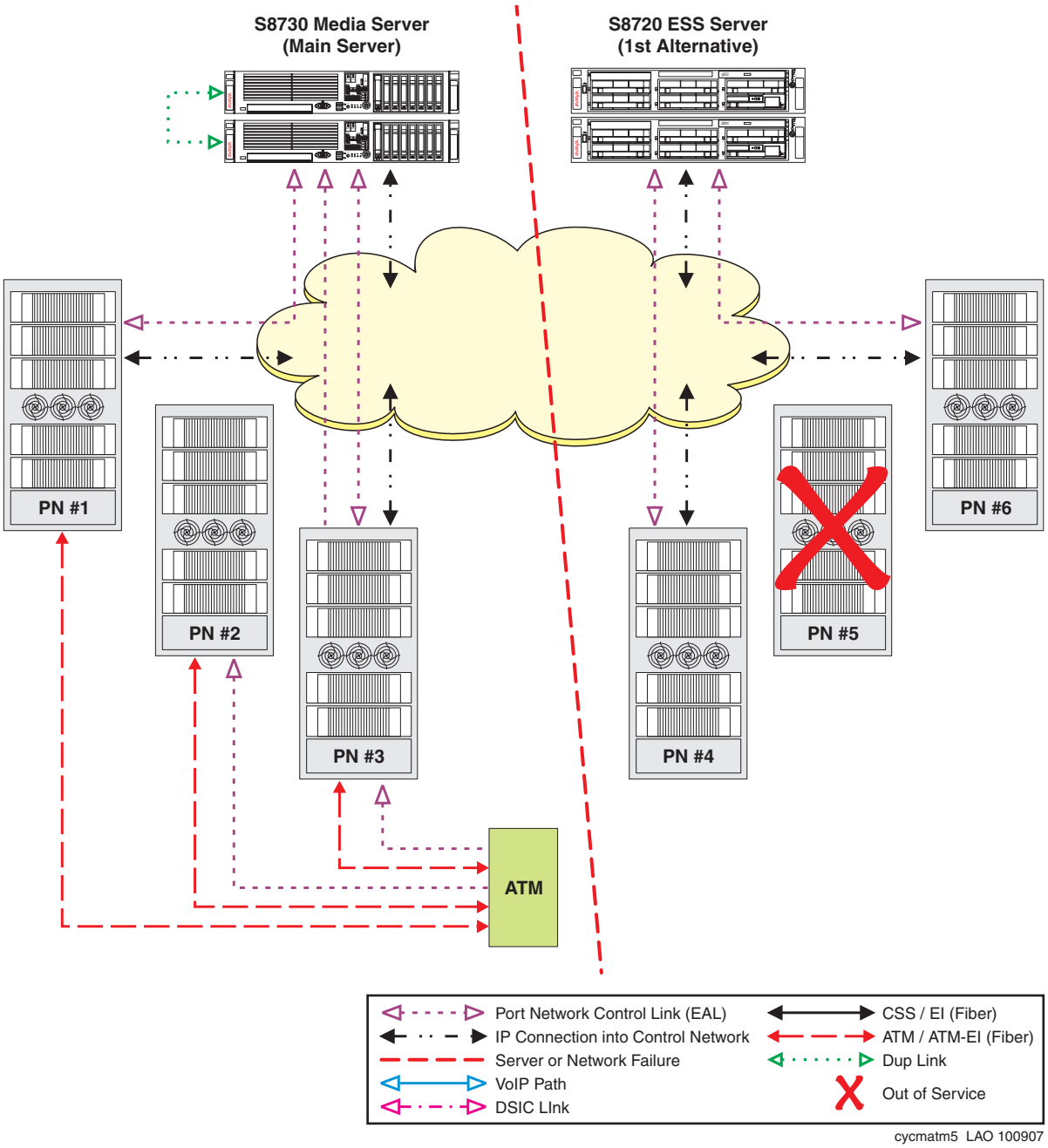
Figure 18: ATM - single ESS server first takeover scenario



In the second takeover example (Figure 19), the customer experiences a network failure. Communication between the main server and port networks one through three has not been affected by the outage. The IPSIs in port network four and port network five can no longer communicate with the main server. The no service timer activates. When the no service timer expires the IPSIs in port networks four and five request service from the S8720 ESS server.

In order for an ESS server to control a port network without an IPSI, such as PN5, the ESS server must first control a port network with an IPSI. Once the ESS server controls a port network with an IPSI the ESS server may then attempts to communicate with and possibly control a non-IPSI port network through the ATM network. The S8720 ESS server cannot communicate with the ATM switch and therefore cannot take control of port network five through the ATM connection (EI board).

Figure 19: ATM - Single ESS sever second takeover scenario



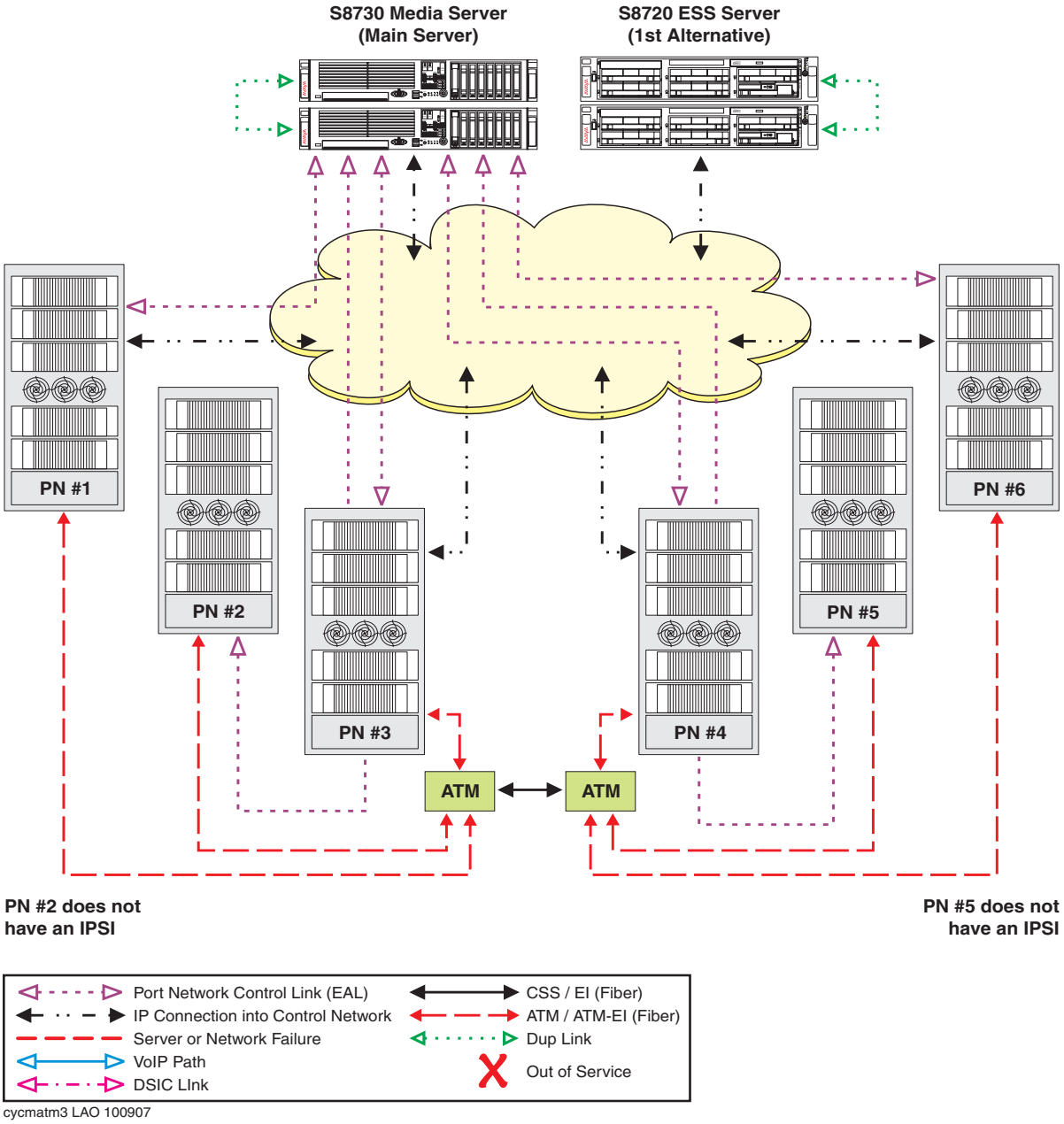
Example eight: Distributed ATM Switches

Important:

Communication Manager Release 5.x and later is not supported on S8700 Servers and S8500A servers.

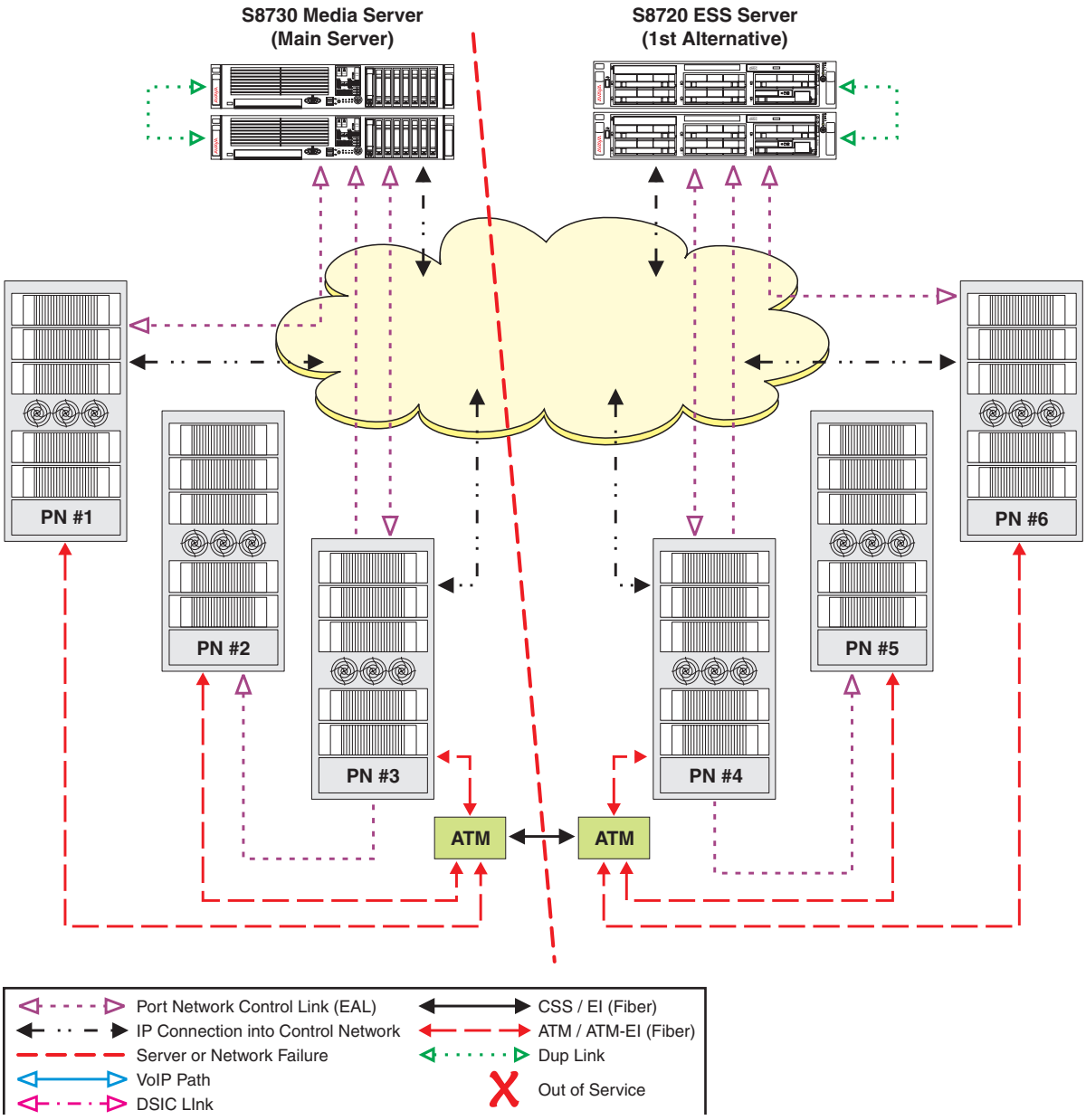
In example eight there is a single ESS server with multiple ATM nodes. Port network two does not have an IPSI and connects using an ATM Expansion Interface (EI) board to the ATM node on the left side of Figure 20. Port network five does not have an IPSI and connects using an ATM EI board, to the ATM node on the right side of Figure 20.

Figure 20: ATM, single ESS server, multiple nodes in normal operation



A network outage occurs that fragments the two ATM and IP networks (Figure 21). The main server continues to provide service to port networks one through three without a service interruption. The IPSIs in port networks four and six requests service of the S8720 ESS server after the no service timer expires. The S8720 ESS server assumes control of port network four first. Once in control on port network four, the ESS server assumes control of port network five through the EI board.

Figure 21: ATM, single ESS server, multiple nodes in a takeover scenario



The users in port networks one through three can make station-to-station calls to each other but cannot make station-to-station calls to users in port networks four through six. The reverse is also true, where users in port networks four through six cannot make calls to users in port networks one through three.

Example nine: LSPs working in an ESS environment

Important:

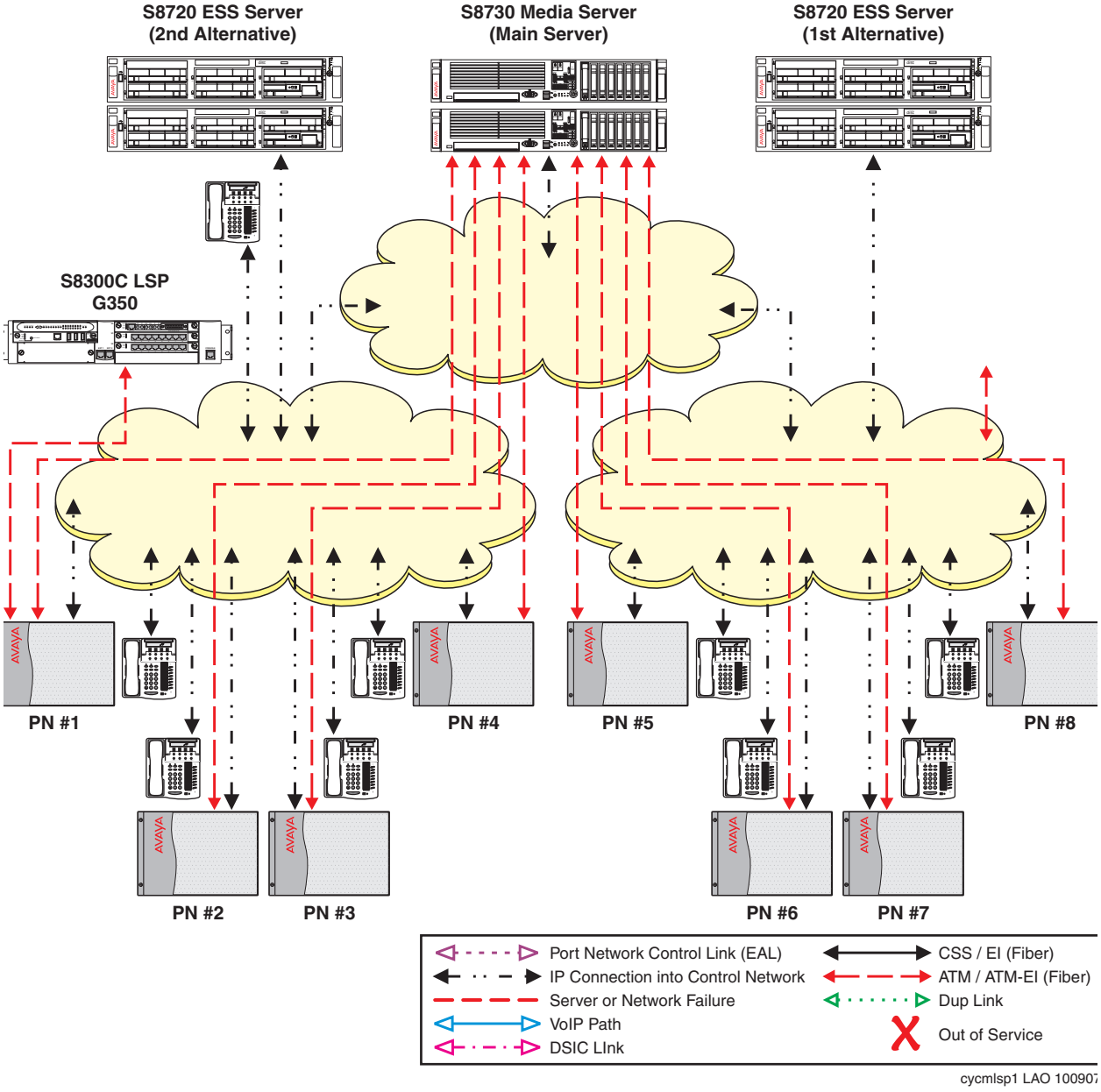
Communication Manager Release 5.x and later is not supported on S8700 Servers and S8500A servers.

In example nine (Figure 22), there is an S8300 LSP residing in a G350 Media Gateway. In a normal operation the main server communicates with the G350 through a C-LAN circuit pack in port network one.

Two ESS servers are administered. The 1st alternative S8720 ESS server has the highest priority and is the first ESS 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 ESS server, it will request service from the 2nd alternative S8720 ESS server.

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

Figure 22: LSP working in an ESS environment - normal operation



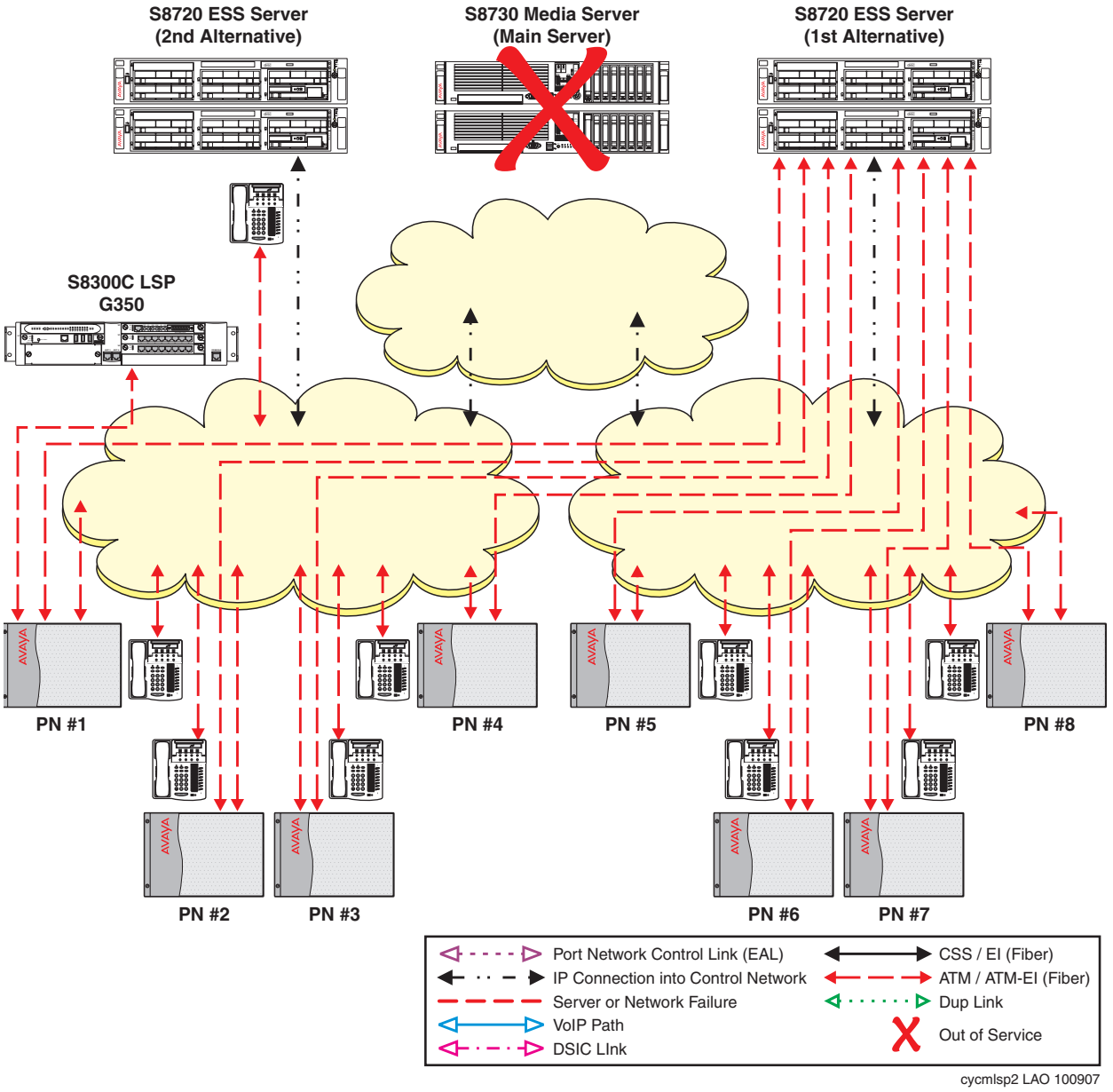
In an ESS environment, a no service timer activates when the IPSI can no longer communicate with the main server or the controlling ESS server. The no service timer is administrable and can be set from three to 15 minutes.

The media gateway has a recovery variable timer design that incorporates three separate timers. The timers monitor the period of time that the server or gateway spends in a specific Link Recovery processes. If the timers expires before the ESS no service timer, the G350 Media Gateway and IP telephones automatically attempt to connect with an alternate C-LAN circuit pack within the original server's configuration or to an LSP.

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 ESS server.

In Figure 23 the Link Recovery was able to re-establish the link through the C-LAN circuit pack in port network one to the 1st alternative ESS server before the Link Recovery timers expired. For more information on Link Recovery, see Link Recovery on page 84.

Figure 23: LSP working in an ESS environment - ESS timer before Link Recovery timer

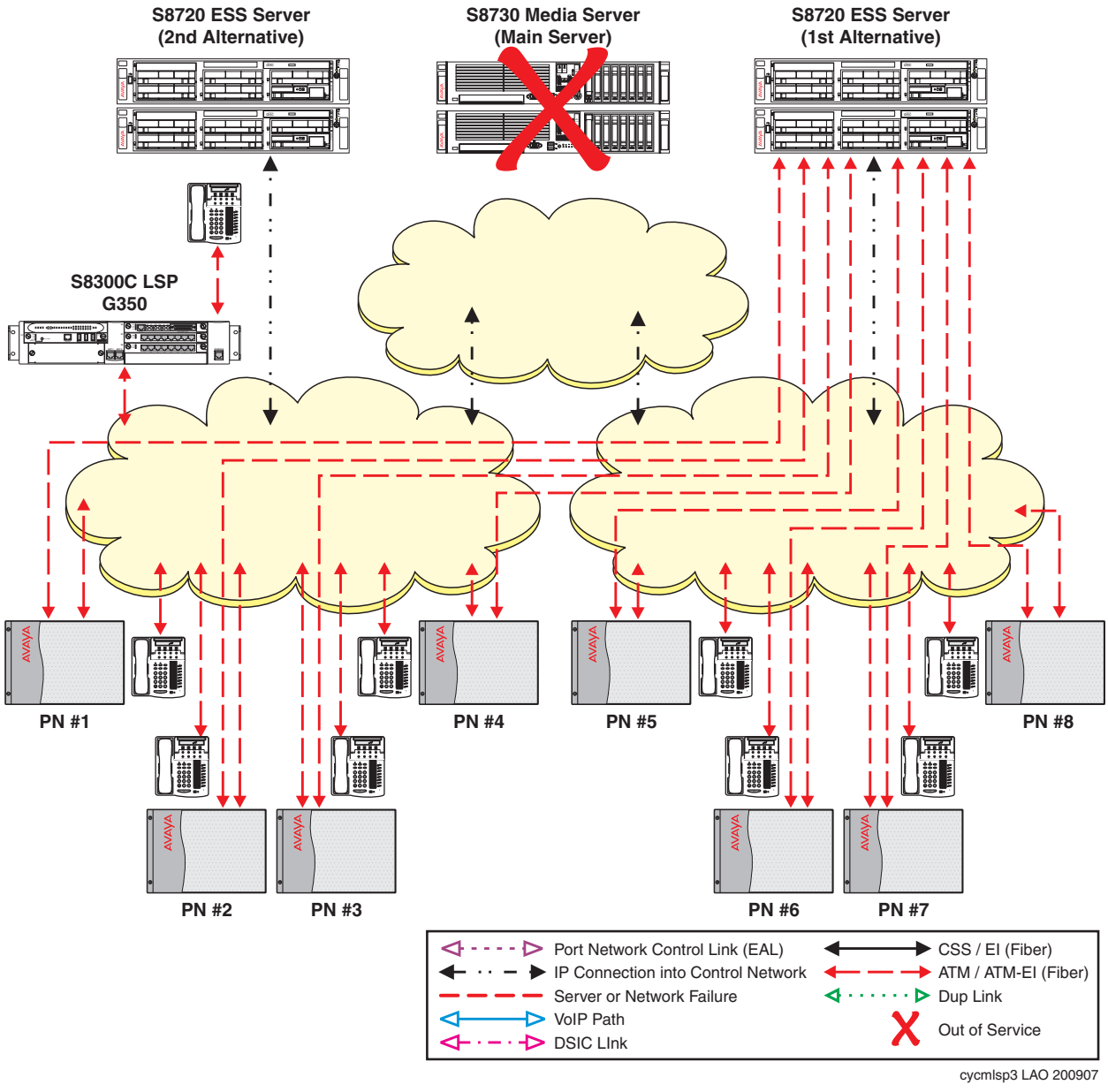


Using a different scenario, in Figure 24 the Link Recovery timer expired before the ESS no service timer. The IP telephones and the G350 Media Gateway connects to an alternate gatekeeper (the LSP). The no service timer expires and the IPSIs in port networks one through eight request service from the 1st alternative ESS server.

The system is now fragmented between two controlling servers.

- Some functionality provided by adjuncts may be missing for users registered with the LSP. For more information on adjuncts, see Feature considerations on page 85.
- Users registered with the LSP may not be able to make normal station-to-station calls to port networks controlled by the 1st alternative ESS server.

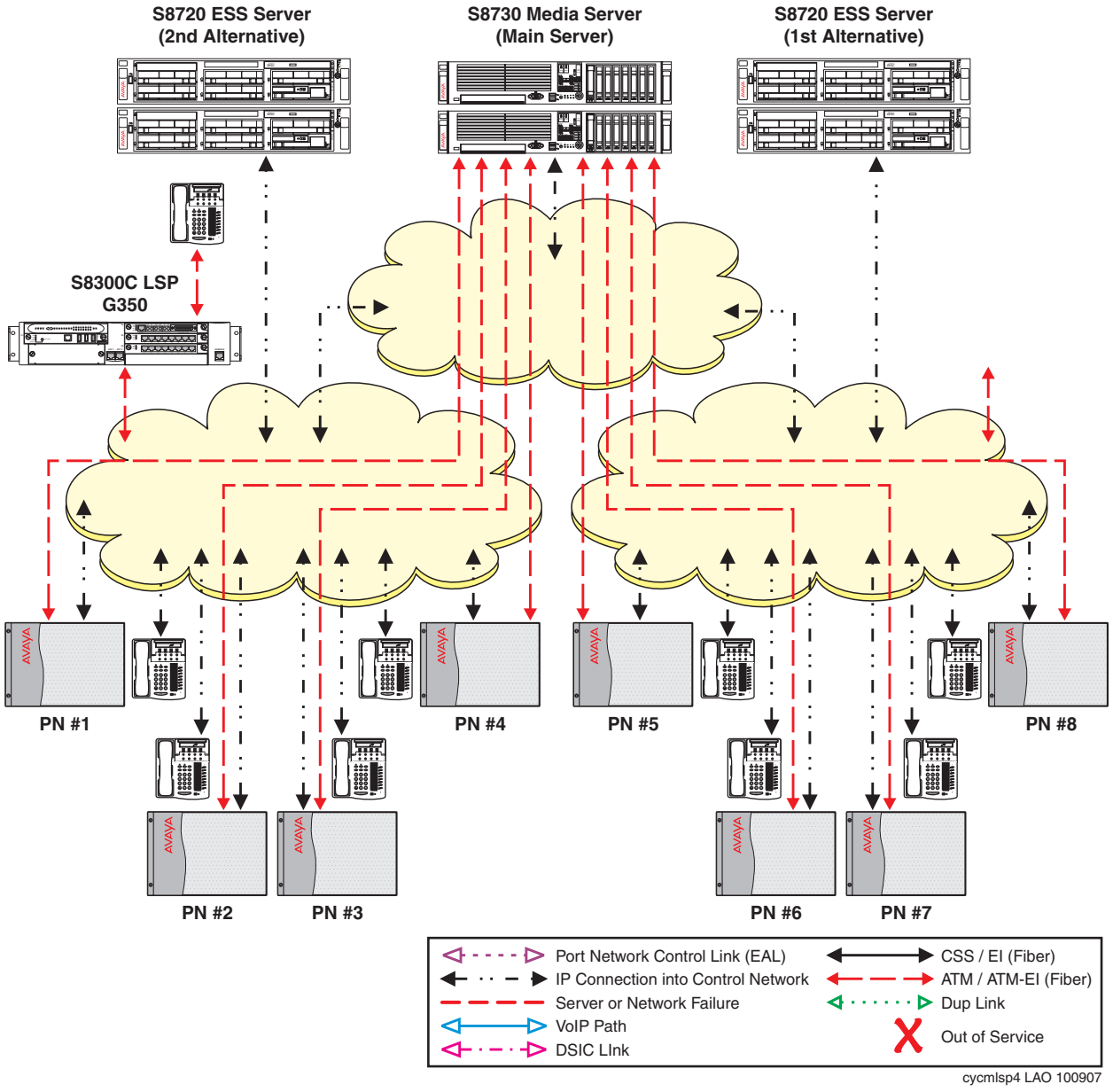
Figure 24: LSP working in an ESS environment - Link Recovery timer before ESS timer



The problem that caused the main server outage has been fixed (Figure 25). 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 the Auto Fallback to Primary feature (Communication Manager Release 3.0 or later) is being used, the G350 automatically re-registers with the main server when it becomes available. If the Auto Primary feature is not being used (Figure 25), a manual reset must be performed on the G350.

Figure 25: LSP working in an ESS environment - fall-back to the main server



Chapter 2: ESS Design and Planning

CAUTION:

Read this caution if you are ***upgrading*** a main server with one or more LSPs or ESS servers from Communication Manager Release 1.3.2 to Release 5.x.

As part of the standard upgrade process, an LSP or an ESS server must upgrade before the main server. However, if the LSP or ESS server upgrades from Release 1.3.2 to Release 5.x, it will not get a filesync from the main server until the main server upgrades from Release 1.3.2 to Release 5.x. In the timeframe after the LSP and ESS server upgrade and before the main sever upgrade, the LSP and ESS server will continue to use the last translations it received before the upgrade.

In some customer environments, an LSP or ESS server running out-of-date translations might be undesirable. For example, if the main server remains on Release 1.3.2 for an extended period of time after the upgrade of an LSP or ESS server to Release 5.x, the risk is higher that the translations on the LSP or ESS server may become seriously out-of-date. In this example, the customer may choose to upgrade to Release 4.x instead of Release 5.x.

Important:

When you upgrade a duplex ESS from an earlier release of Communication Manager to Release 5.2 or later, the duplex ESS uses the PE Active Server IP address (IP-alias). The upgraded duplex ESS uses the PE Active Server IP address that is shared by the duplex ESS pair.
In a situation when the duplex ESS is upgraded and is running Release 5.2 or later and the main server pair is not yet upgraded and is still running release 5.1.x or prior, the main server has no concept that the duplex ESS has a PE Active Server IP Address. In this interim state, special consideration must be given to the administration for the duplex ESS.

Information on how to upgrade a main or ESS server can be found in *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

ESS design strategy

During the design and planning phase of an ESS implementation, it is important to understand the customer’s goal for survivability, including prioritization. This is done by determining the

strategy of ESS support for the port networks in the system. Goals for deploying and administering the ESS servers are:

1. Avoiding fragmentation of the system: The ESS server controls as much of the system as possible.
2. Avoiding overload of network resources with excessive call traffic: Each ESS server controls only limited portions of the system. Multiple ESS servers may be needed to support the number of port networks. In this way, an ESS 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 an ESS server to take control of all or part of the configuration, priority parameters are administered for the ESS server implementing the strategy.

After an overall strategy is selected, determine the placement of the ESS servers in the network. Determine the administered values and communities for each ESS server. For further details on administered values and communities, see Administering an ESS server on the main server on page 131.

ESS terminology

The following list contains terms that are used in an ESS environment. Become familiar with these terms before you plan, configure, and administer ESS.

- Main server and ESS server: In this book, the primary controller is referred to as the main server and the backup server as an ESS server.
- Cluster: You will see the term cluster in the SAT screens that are used for ESS. 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 ESS 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 ESS. A CLID uniquely identifies a single cluster so that each server in a duplex pair can have the same CLID.
- System Identifier (SID): A SID is assigned by RFA when a license file is created. The value of the SID is the same for *all* the severs in an ESS configuration.
- Server Identifier (SVID): Each server in an ESS 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 an ESS 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.

ESS prerequisites

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

- **IP address(es)**: Obtain the following IP address(es):
  - Main server
  - ESS 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 ESS Installation Checklist on page 94.

  The IP addresses listed above are used when configuring the main server and each ESS server. For more information on configuring and administering the main server and the ESS server, see Administering ESS on page 130.
- **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 99. Each server in a server pair (S8700-Series Servers) 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**: The main server and each ESS server requires its own license file. For security purposes, RFA requires that each license file have a unique serial number. Prior to ESS, the serial number of a single reference IPSI was used for the entire enterprise. For an ESS implementation, each license file for an ESS server and a main server must have

a unique serial number from a *separate* reference IPSI. For more information on ESS license files, see ESS server license files on page 113.

- **Module Identification Number (MID)**: This is a unique value assigned by RFA and found in the license file. The MID is administered as the Cluster Identification Number (CLID) in the **Survivable Processor** screen.

  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. In an example where the ESS server license file is s66579v4m2-060214-19431.lic, the MID would be 2.

  CAUTION:

  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 an ESS server.

Network port considerations

The main server, LSPs, and each ESS server use specific ports across a customer's network for registration and translation distribution. Use the information in Table 3 to determine the ports that must be open in the customer's network in an ESS 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 ESS server to register to the main server.	An ESS server registers with the main server using port 1719. For more information on ESS server registration, see C-LAN access for ESS registration on page 19.
		1 of 2

Table 3: Open ports (continued)

Port	Used by:	Description
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	
5011	IPSI/Server IPSI version channel	
5012	IPSI/Server serial number channel	
21873 (TCP port)	The main server running Communication Manager 2.0 to download translations to the LSP(s).	Prior to an upgrade to Communication Manager 3.0 or later, a server running Communication Manager 2.x uses port 21873 to download translations to the LSP(s). Once the upgrade to 3.0 is complete and all servers are running versions of Communication Manager 3.0 or later, the main server uses port 21874 to download translations and port 21873 will no longer be needed.
21874 (TCP port)	The main server to download translations to the ESS server.	A main server uses port 21874 to download translations to the ESS server and the LSP(s) on Communication Manager 3.0 and later loads.
		2 of 2

Main server and ESS server differences

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

- The license file: The license file of the main server must have *ESS Administration* turned on and *Enterprise Survivable Server* turned off. The license file for an ESS server must

have both *ESS Administration* and *Enterprise Survivable Server* turned on. For more information on license files, see ESS server license files on page 113.

- Translations: You can change translations on an ESS server but you *cannot* save them. This is true even if the ESS server is providing service to an IPSI. A file sync from the main server to the ESS server will over-write translations performed on the ESS server.
- Center Stage Switch (CSS): An ESS server can never take control of an CSS.
- 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 ESS server is administrable. For information on administration, see Administering ESS on page 130.
- ESS server capacity:

  For detailed information on system capacities, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

  - When used as an ESS server, the S8500-Series Server and the S8700-Series server match the capacity of the S8700-Series server that is used as a main server.
  - When used as an ESS server, the S8400 Server matches the capacity of the S8400 Server that is used as a main server.
- Control Network duplication:
  - When used as an ESS server, the S8500-Series server can support one or more port networks with single IPSI or duplicated IPSI.
  - When used as an ESS server, the S8400 server can control one port network with single IPSI or duplicated IPSI.
- Processor Ethernet: Processor Ethernet can be used on both the simplex main server and the simplex ESS server. On the simplex main server the Processor Ethernet interface can be used for adjunct connectivity, H.323 endpoint registration, and H.248 gateway registration. In Communication Manager Release 5.2 and later, the Processor Ethernet interface can be used for support of H.323 devices and H.248 gateways and adjunct connectivity if you administer relevant fields on the **Survivable Processor** screen.

  For information on how the Processor Ethernet functionality works on main servers and ESS servers, see Use of Processor Ethernet interface on main servers and ESS servers on page 17.

Trunking considerations

Use this section to understand trunking considerations in an ESS 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 ESS server controls the primary and the backup D channels, each ESS 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 an ESS 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 ESS server.
3. After failover, if the D-channels are being serviced by two different ESS servers:
   - Perform the **`get forced-takeover ipserver-interface`** command if the network conditions allow bringing both port networks under the same ESS server.
   - Busy-out one D-channel to prevent thrashing with the Central Office if network fragmentation will not allow one ESS 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.

Synchronization

In an IP connected environment, each port network may have its own primary and secondary external source that provide synchronization for the DS1. Synchronization is not supported across IP networks.

In a CSS or ATM-PNC environment, there is only one primary and secondary synchronization source for all DS1s in the CSS/ATM-PNC port networks. If a DS1 loses the primary and secondary synchronization source, it uses the Tone Clock in the port network where it resides. Use of Tone Clock synchronization may result in audible artifacts due to slips.

H.320 Video applications require synchronization. In the event that the H.320 Video application loses synchronization, the call would be expected to drop.

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 ESS server as the person originating the call.

Inter-Gateway Alternate Routing (IGAR)

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

For example, an ESS 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 ESS server one. Port networks five through eight failover to Local Only ESS servers. ESS server one uses IGAR to establish inter-port network bearer between port networks one through four. Each Local Only ESS server controls one port network (five through eight). IGAR does not apply for the Local Only servers.

All port networks within a CSS must be in network region one. When an ESS server obtains control of port network from the CSS, all port networks remain in network region one. IGAR does not apply within the same network region.

Personal Central Office Line (PCOL)

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 ESS server.

Separation of Bearer and Signaling (SBS)

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 ESS server. Alternate routes may be used if under the control of the same ESS server as the originator.

Network addressing considerations

When implementing ESS, it is necessary that all Network Control Elements such as the main server, ESS servers, and IPSIs, be assigned static IP addresses. When a customer is converting to an ESS environment, and normally receives IP addresses from a DHCP server, the Network Control Elements must be given static IP addresses before adding ESS.

For information on assigning static IP addresses see:

- *Installing and Configuring the Avaya S8400 Server* (03-300678)
- *Installing and Configuring the Avaya S8500-Series Server* (03-300143), or
- *Installing and Configuring the Avaya S8700-Series Server* (03-300145).

Both documents can be found at http://support.avaya.com.

Data Networking

In an Avaya solution, IP connectivity is required for call control between an Avaya S8500-Series or S8700-Series Servers and a reference IPSI. There can be a single call control connection called Control Network A (CNA) or duplicated call control connections called CNA and CNB. CNA and CNB can be on either a public or private network.

A third call control connection called Control Network C (CNC) allows control to be passed through the customer LAN interface. Using CNC allows customers, with local private control networks (CNA and CNB), to also use their enterprise (public) network to support remote IPSI controlled port networks.

Note:

To use CNC in an ESS environment, you must enable CNC on all servers in an ESS configuration.

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

CSS considerations when using ESS

In an ESS environment, all Expansion Interface (EI) boards must be a D version (TN570D) when the EI board resides in a survivable port network that contains IPSIs.

Note:

A TN570B vintage 7 or later expansion interface can be used if the CSS port network is not survivable (will not failover to an ESS server).

An ESS server cannot take control of a CSS, but can control a CSS connected port network where an IPSI and an IP Media Processor reside. When an IPSI in a CSS port network requests service from an ESS server, the port network enters into an IP-PNC mode.

The following is true for CSS in an ESS environment:

- In the event of a main server failure, the CSS is out-of-service. This is true because the CSS is enabled only for the main server and disabled for all other servers.
- The number and vintage of the IP Media Processor resource will have an impact on the traffic volume for the failed-over port network. Traffic engineering should consider the use of multiple IP Media Processors to allow for adequate call volume of failed-over port networks.
- An ESS server can provide service to an IPSI in a mixed port network configuration such as:
  - CSS and IP-PNC
  - ATM-PNC and IP-PNC

Note:

CSS and ATM-PNC mixed configurations are not supported.

ATM considerations when using ESS

In an ATM environment, all ATM Expansion Interface (EI) boards must be either the TN2305B or the TN2306B. An ESS server can control ATM port networks without an IPSI by communicating indirectly through an IPSI controlled port network, and then through the TN2305B or TN2306B ATM EI board.

Port networks in an ATM environment do not transition to IP during a failover to an ESS server.

H.323 considerations when using ESS

Because H.323 trunk usage can exhaust memory pool and can prevent H.323 stations from registering, Communication Manager 5.2 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 ESS servers and LSPs, 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 appear only if you enter **selected**.

IPSI Priority List

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

An ESS server receives its values when it is administered on the main server using the **`survivable processor`** command. See Figure 26 for an example of the **Survivable Processor** screen.

Figure 26: Administering the ESS servers

```
display survivable-processor sv-ess13                          Page   1 of   4
                    SURVIVABLE PROCESSOR

Type: simplex-ess      Cluster ID: 13    Processor Ethernet Network Region: 1
                        Community: 20        Enable PE for H.323 Endpoints? n
                                              Enable PE for H.248 Gateways? n


SERVER A
          Server ID: 13
          Node Name: sv-ess13
         IP Address: 172.24.206.29



PORT NETWORK PARAMETERS
                  Community Size: all      System Preferred: n
                  Priority Score: 1         Local Preferred: y
                                                 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 ESS clusters. A maximum of 63 ESS clusters can be administered in one ESS configuration. An ESS cluster can be a simplex or a duplex pair of servers. If an IPSI receives an advertised value from an ESS cluster and its priority list is full, the ISPI checks the value of the advertised cluster against the values of the ESS clusters on the list. If the advertised value of the ESS cluster:

- Is greater than one of the ESS clusters already on the list, the ESS cluster that is already on the list is removed and the newly advertised ESS cluster is added.
- Is less than the ESS clusters that are already on the list, the ESS cluster is not added to the list and the list remains the same. The rejected ESS cluster continues to advertise to the IPSI until the IPSI accepts the ESS 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, Media 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 ESS 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 ESS server is administered with one of two preference settings, System Preferred (**Sys Prf** field) and Local Preferred (**Loc Prf** field). An ESS server administered with either the System Preferred or the Local Preferred preference can advertise 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 an ESS server with no preference setting. The value for the Local Preferred preference is only used by the IPSIs within the same community as the ESS server. When the ESS server with a Local Preferred preference advertises to an IPSI outside of its community, the preference value is the same as an ESS server with no preference.

Local Only works differently than preferences. While the System Preferred preference, the Local Preferred preference, and the ESS server with no preference can advertise to IPSIs in all communities, an ESS server with Local Only administered can only advertise 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. An ESS server administered with both the Local Only and the Local Preferred preference will:

- Act like a Local Only server and only advertise 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 an ESS 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 ESS servers with the same preference settings, ESS servers with no preference setting, or ESS servers that are not in the same community as the IPSI.

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

Table 4: ESS relative priority

Administered ESS 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.
	1 of 2

Table 4: ESS relative priority (continued)

Administered ESS server type	Priority value impact
Local Preferred and Local Only server in the same community	An ESS server administered with both the Local Preferred preference and Local Only has the value of a Local Preferred server but can only advertise 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 advertises 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 an ESS server with no preference, advertises 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.
No preference server	The value of an ESS server administered with no preference is based solely on its priority value. It is possible to administer all ESS servers with no preferences. In this case, all ESS servers would start out with the same value and a priority value would be used to rank the importance of the ESS servers independent of communities.
	2 of 2

For information on how to administer an ESS server, see Administering an ESS server on the main server on page 131.

Note:

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

Advertising priority to an IPSI

An ESS server advertises its priority to an IPSI:

- Every time it disconnects and reconnects to the main server. An ESS 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 an ESS server and the IPSI: The ESS server resets after receiving translations from the main server. When the ESS server resets, communication between the ESS server and the IPSI is lost. The IPSI adjusts its priority list, removing the ESS server from the list. When the ESS server re-establishes communication with the IPSI, the ESS server will regain its proper order on the list.
- An ESS cluster is deleted: The ESS cluster was removed from translations.
- An ESS cluster with a higher value than an ESS cluster on the list advertises its value to the IPSI. In this case the ESS cluster with the lowest value is removed from the list and the newly advertised ESS 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.

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

  Note:

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

  - The ESS cluster advertises 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 ESS 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 27 the priority list for the IPSI in port network two is, 50, 10, 99, 90, 80, 70, and then 30. For **`ess port-networks`** field details, see Administering ESS on page 130.

Figure 27: status ess port-networks

```
status ess port-networks                                          Page   1

Cluster ID 50            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  25           down       11A01 active     1   1  50  10  99 100  90  80  70

 2  26           down        2AXX active     1   1  50  10  99  90  80  70  30
                             2B01 standby    1   1  50  10  99  90  80  70  30

 3  26           down        2E02 active     1   1  50  10  99  90  80  70  30
                             2D01 standby    1   1  50  10  99  90  80  70  30

 4  26           down        3AXX active     1   1  50  10  99  90  80  70  30
                             3B01 standby    1   1  50  10  99  90  80  70  30

 5  26           down        3E02 active     1   1  50  10  99  90  80  70  30
                             3D01 standby    1   1  50  10  99  90  80  70  30
```

Examples of how the priority list works

The following examples demonstrate how the IPSI priority list is used during failover scenarios.

IP connected port networks

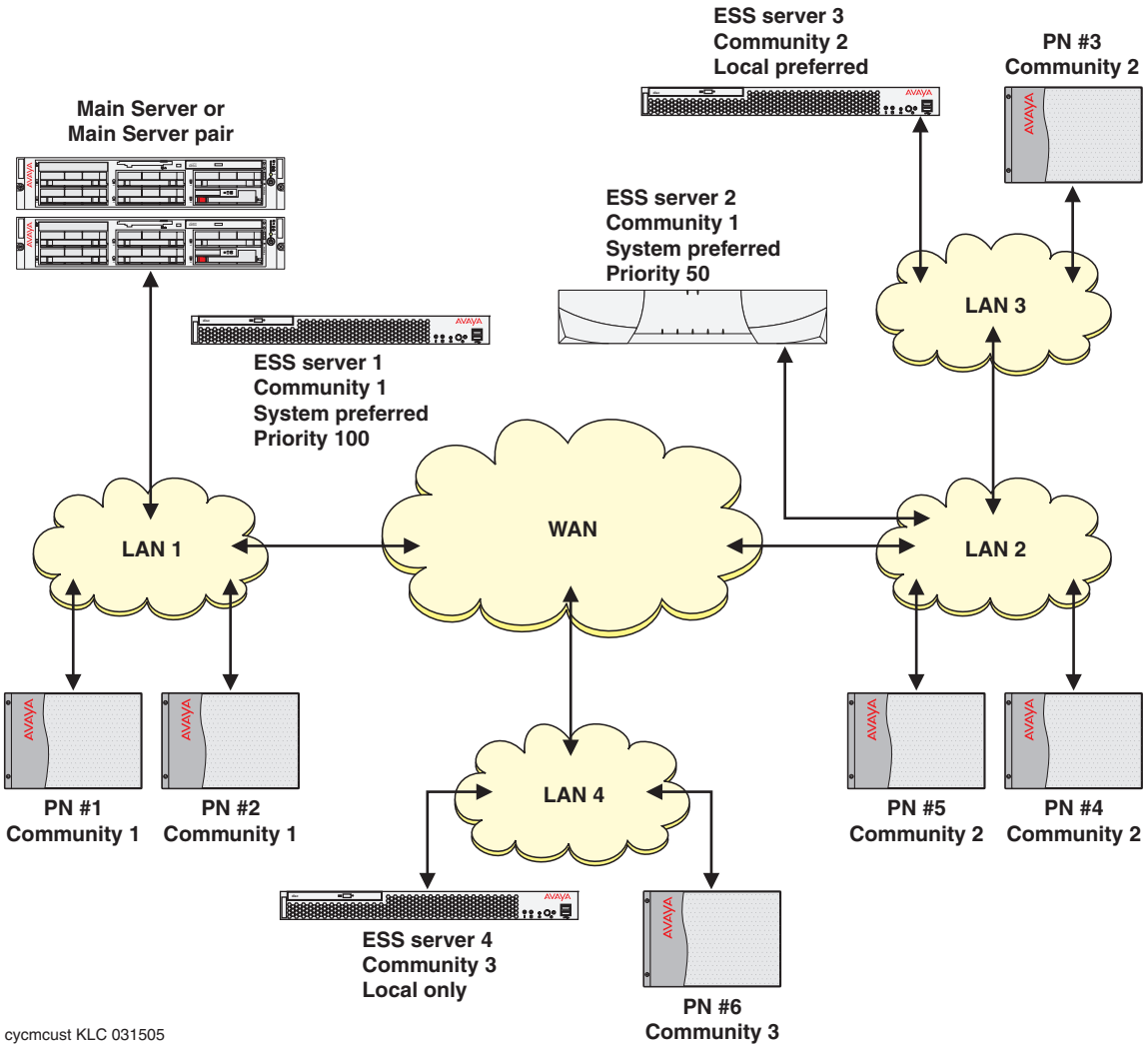
In this example, an IP connected system has five IPSI connected port networks and four ESS servers. During the planning phase, the administrator decided that:

- The primary goal was to keep as much of the system in-tact as possible. In order to achieve that objective, two ESS servers (ESS server one and ESS server two) were placed in the network. Both ESS 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 ESS server one:
  - The main server will control port networks one and two.
  - ESS 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, ESS 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 ESS server four (the Local Only server) will control port network six.

See Figure 28 for the customer's configuration with the priority scoring of each ESS server.

Figure 28: Customer's configuration



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

Table 5: ESS 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	S8700 -Series Server	1 2	192.9.13.10 192.9.13.11	100	1	1 2 3	1 2 3	1 2 3 4
	3	S8500 -Series Server	3	192.9.44.11	50	1			
Local Preferred (second highest value preference in its community)	4	S8500 -Series Server	4	192.9.33.22		2			
No Preference (no value)									
Local Only (only advertises to IPSIs in its own community)	5	S8500 -Series Server	5	192.8.55.7		3			

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

- Both ESS server one and ESS 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 ESS server one above ESS server two in the ranking within the System Preferred preference. The IPSI priority list in any community will show ESS server one as the first priority server, followed by ESS server two.
- ESS 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 an ESS server with no preference. When configurations have multiple Local Preferred servers, additional ranking can be achieved by using a Priority Score.

  In this example, ESS server three would be the third choice for port network three, port network four, and port network five, which are all in community two. ESS server three would also be the third choice for port network one and port network two.
- ESS server four is administered as a Local Only server for community three. A Local Only server only appears on the IPSI's priority list if that IPSI is in its community. That means, ESS server four only appears on the IPSI's list in community three and will never appear 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

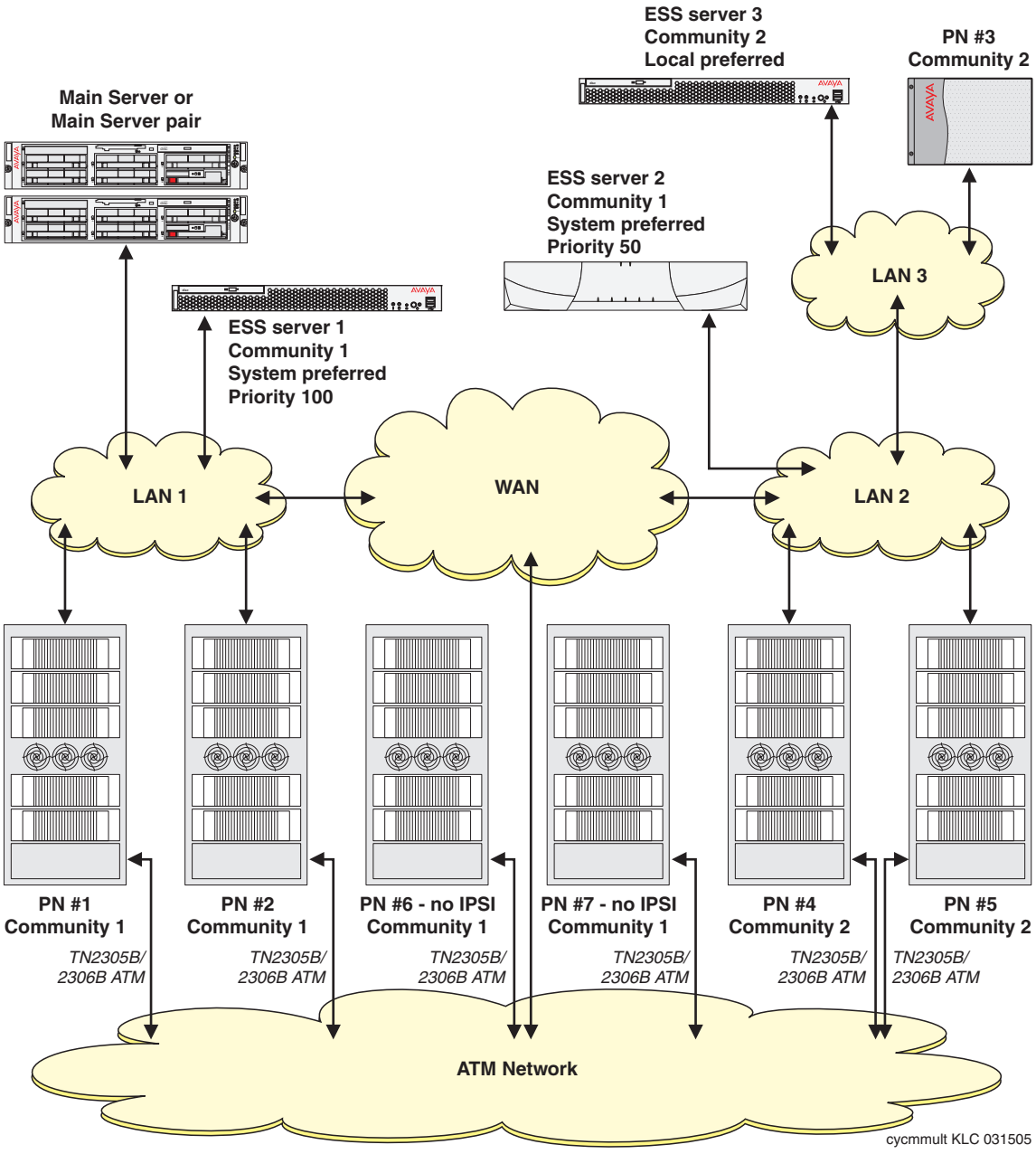
Failure type	failover description
Main server fails	ESS server one is the highest ranking ESS server on the IPSI priority list. All port networks failover to ESS server one.
Both main server and ESS1 fails	ESS server two is second highest ranking ESS server on the IPSI priority list. All port networks failover to ESS server two.
WAN connection fails	The main server continues to control port networks one and two. The main server and ESS 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 ESS server on their priority list (ESS server two). ESS server four is the only ESS server available to port network six if the WAN is not available.

Fiber-PNC configuration using ATM PNC

In this example, the fiber-PNC configuration has seven port networks and three ESS servers. As in the previous IP connected configuration example, the administrator wants the system to stay as much in-tact as possible after a failover. Should IPSI communication to the main server fail, the administrator wants ESS server one to provide service to the entire system. If the IPSIs loses communication with ESS server one, then ESS server two will take over the entire system. Port networks six and seven connect to the main server over the ATM network and do not have a direct IPSI connectivity to the main server.

See Figure 29 for the customer's ATM PNC configuration with the priority scoring of each ESS server:

Figure 29: ATM PNC configuration



See Table 7 for an example data collection worksheet for Figure 29.

Table 7: fiber-PNC using ATM PNC data collection sheet

Server Preference	Cluster ID	Platform Type	SVID	IP Address	Priority Score	Community	IPSI List in Com 1	IPSI List in Com 2
System Preferred	2	S8700 -Series Server	1 2	192.9.13.10 192.9.13.11	100	1	1 2 3	1 2 3
	3	S8500 -Series Server	3	192.9.44.11	50	1		
Local Preferred	4	S8500 -Series Server	4	192.9.33.22		2		
No Preference								
Local Only								

In this example all the IPSIs have the same priority lists. There are no IPSIs in PN6 and PN7 and therefore no priority list associated with those port networks.

In the case of an IP Network failure, if PN6 and PN7 cannot communicate with the main server, they will fall under control of one of the other ESS servers. In order for an ESS server to control a port network without an IPSI, such as PN6 or PN7, the ESS server must first control a port network with an IPSI. Once the ESS server controls a port network with an IPSI the ESS server can then attempt to communicate with, and possibly control, a non-IPSI port network through

the ATM network. An ESS server is always more likely to take control of a non-IPSI port network if it is providing service to an IPSI in that community.

In this example, the failover scenarios in Table 8 might occur:

Table 8: Fiber-PNC using ATM PNC

Failure type	failover description
Main server fails	ESS server1 is the highest ranked ESS server on the IPSI priority list. All port networks failover to ESS server1 including those without an IPSI.
Both main server and ESS1 fails	ESS2 is second highest ranked ESS server on the IPSI priority list. All port networks failover to ESS2.
Control network fails	The main server continues to control PN1, PN2, PN6, and PN7. In addition, the main server assume control of PN4 and PN5 through the ATM network. ESS2 controls PN3.
Main server fails, WAN connection fails, and ESS1 fails	PN3, PN4, and PN5 failover to ESS2 as it is now the first ESS server on their priority lists. ESS2 is not available to PN1 and PN2 over the WAN but ESS2 can support PN1 and PN2 through the connections to the ATM network.
Main server fails first and then control network fails	PN1 and PN2 request service from ESS1. PN3, PN4, and PN5 request service from ESS2. ESS1 will be the first to try to take control of PN6 and PN7 through the ATM network. This however, is timing dependent. There is some possibility that ESS2 might control PN6 and PN7 instead.

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:

ESS no service timer

During ESS 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 ESS server, before requesting service from the highest ranked ESS 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 an ESS 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 three to 15 minutes, with a default of five minutes. For more information on the no service timer, see Port Network Recovery Rules screen on page 141.

Link Recovery

For detailed information on Link Recovery, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media 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 Port Network Recovery Rules screen on page 141.

Feature considerations

Note:

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

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.

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

Announcements

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

Attendant Console

When a port network fails-over to an ESS 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 ESS server will be affected by the deactivation of the Night Service mode. The ESS server assumes that any console that it cannot control is out of service.

Best Service Routing (BSR)

BSR polling works if the facility used for routing the polling call is under the control of that ESS server.

Call Classification

Call Classification will work only if there are one or more Call Classification resources under the control of the ESS server.

Call Coverage

Calls may follow a call coverage path only if the route is under the control of the same ESS server. If the covered party is not under the control of the ESS 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 ESS server. This is true whether the endpoint is another station, adjunct, or route in a routing pattern.

Centralized Attendant Service (CAS)

For a CAS Main system calls from a Branch will be processed if the port networks under the control of the ESS 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 ESS 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 ESS server that controls the originator.

CVLAN links

The ESS server will only have access to CVLAN links in port networks under its control.

Dial Plan Transparency

When a port network requests service from an ESS server, or when a gateway registers with an LSP, 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 will not work when two port networks or gateways are in the same network region but failover to different ESS servers. However, given the nature of network failures, it would be unexpected for port networks and gateways in the same network region to failover to different ESS servers. This type of failure is more likely with fiber-PNC connected port networks because all fiber-PNC connected port networks must be assigned to network region 1. Customers wanting Dial Plan Transparency for port networks connected with fiber-PNC must migrate the port networks to IP-PNC.

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 ESS 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 ESS server.

Leave Word Calling

When an ESS 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 ESS server can provide Music on Hold only if the music source is in control of the ESS server. Calls to an ESS server without a music source hear silence.

Adjunct considerations

When a failover occurs, an ESS server may or may not have connectivity to various adjuncts.

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

- Call Detail Recording (CDR) on page 89
- Call Management System (CMS) on page 90
- Extension to Cellular on page 90
- Property Management System (PMS) on page 90
- Voice Mail (Audix, Intuity, Octel, Modular Messaging) on page 90
- Voice Response Systems (Conversant) on page 91

Note:

Starting with Communication Manager Release 3.1, you can connect three adjuncts to the Processor Ethernet interface of an LSP or an simplex ESS server. The three adjuncts are Call Management System (CMS), Call Detail Recording (CDR), and Application Enablement Services (AE Services). Starting with Communication Manager Release 5.2, you can connect the CDR, Messaging, and SIP Enablement Server (SES) adjuncts to the Processor Ethernet interface of a duplex ESS server. For more information on the Processor Ethernet interface, see Processor Ethernet overview on page 16.

Call Detail Recording (CDR)

Traditional CDR

A CDR unit can connect to an ESS server through the server's Processor Ethernet interface or the 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 S8700 Server buffer. Other records that were not delivered to the CDR adjuncts and buffered in an ESS server will be unrecoverable, as the ESS server will perform a restart.

Survivable CDR

The Survivable CDR feature is used to store CDR records to a server's hard disk. For ESS servers and LSPs, the Survivable CDR feature is used to store the CDR records generated from calls that occur when an LSP or ESS 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 ESS servers that are Communication Manager 5.0 and later releases only. It is available on LSP platforms running Communication Manager 4.0 and later.

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

The Survivable CDR feature utilizes 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 (CMS)

CMS connects to the server through a C-LAN or through the server's Processor Ethernet (PE) interface. In the event of a failover, an ESS 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 ESS server. In this case only the events that are under control of that ESS 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 ESS server and the LSP 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 an ESS server or an LSP. 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 ESS server that controls the Extension to Cellular.

Property Management System (PMS)

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 an ESS server, will be able to pass entered or event data to the PMS.

Voice Mail (Audix, Intuity, Octel, Modular Messaging)

In the event of a failover, the ESS 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 Systems (Conversant)

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: ESS Installation

The ESS installation chapter contains the following:

CAUTION:

An ESS server and the main server must be running compatible Communication Manager software loads. Before starting an ESS 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.

CAUTION:

Read this caution if you are ***upgrading*** a main server with one or more LSPs or ESS servers from Communication Manager Release 1.3.2 to Release 5.x.

As part of the standard upgrade process, an LSP or an ESS server must upgrade before the main server. However, if the LSP or ESS server upgrades from Release 1.3.2 to Release 5.x, it will not get a filesync from the main server until the main server upgrades from Release 1.3.2 to Release 5.x. In the timeframe after the LSP and ESS server upgrade and before the main sever upgrade, the LSP and ESS server will continue to use the last translations they received before the upgrade.

In some customer environments, an LSP or ESS server running out-of-date translations might be undesirable. For example, if the main server remains on Release 1.3.2 for an extended period of time after the upgrade of an LSP or ESS server to Release 5.x, the risk is higher that the translations on the LSP or ESS server may become seriously out-of-date. In this example, the customer may choose to upgrade to Release 4.x instead of Release 5.x.

When you upgrade a duplex ESS from an earlier release of Communication Manager to Release 5.2 or later, the duplex ESS uses the PE Active Server IP address (IP-alias). The upgraded duplex ESS uses the PE Active Server IP address that is shared by the duplex ESS pair.

In a situation when the duplex ESS is upgraded and is running Release 5.2 or later and the main server pair is not yet upgraded and is still running release 5.1.x or prior, the main server has no concept that the duplex ESS has a PE Active Server IP

Address. In this interim state, special consideration must be given to the administration for the duplex ESS.

Information on how to upgrade a main or ESS can be found in *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

ESS Installation Checklist

This section provides a checklist for two types of ESS installations:

- Installing ESS with existing servers on page 95
- Installing ESS With New Servers on page 105

Overview

In general, an ESS installation requires the following high-level steps:

1. Design the system and determine the ESS administration factors. For information on how to design and plan the system, see ESS Design and Planning on page 61.
2. Install/upgrade Communication Manager 3.0 or later on each ESS server.
   - Install the license and authentication file (ESS server license files on page 113)
   - Start and stop the server (After loading a license file on a server, you must stop and start the ESS server using the following Linux commands: on page 117)
   - Configure the server (Configuring the Servers on page 120)
3. Install/upgrade Communication Manager Release 3.0 or later on the main server.
   - Install the license and authentication file (ESS server license files on page 113)
   - Restart the server
   - Configure the server (Configuring the Servers on page 120)
4. Administer ESS (Administering ESS on page 130)
5. Verify that the ESS servers can register to the main server (Check the administration on the main server on page 142)
6. Acceptance testing (Enterprise Survivable Server Acceptance Testing on page 181)

Installing ESS with existing servers

Use the information in Table 9 as a reference when installing ESS with existing servers.

Table 9: Installing ESS with existing servers

Task	Information	Documentation
General preparation		
1. Obtain license and authentication files for *all* servers in the network.	Obtain an RFA license and an authentication file for *each* ESS server and the main server. A unique IPSI serial number reference is needed for *each* license file. All enterprise servers must run Avaya Communication Release 3.0 or later. If you upgrade from one major version to another (such as 4.0 to 5.2), you need a new license file for each upgrading server.	License and authentication files are generated using at the RFA web site, at http://rfa.avaya.com. For information on how to use RFA, see *Avaya Remote Feature Activation (RFA) User Guide* at http://support.avaya.com.
2. Upgrade the IPSI firmware.	Check the Minimum Firmware/ Hardware Vintage document for the correct IPSI firmware needed in an ESS 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 an ESS 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 on Avaya S8xxx Servers* (03-602885).
		1 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
3a. ESS with Direct-PNC.	The ESS is not supported in a Direct Connect environment. The Direct Connect environment must be converted to an IP connect environment.	To convert a Direct Connect system to an IP Connect system, see *Converting Avaya Servers and Media Gateways* (03-602884).
3b. ESS with IP-PNC.	No changes are needed for an IP connect environment.	
3c. ESS with CSS-port network connectivity (PNC).	Install an IP Media Processor and an IPSI circuit pack in every survivable port network. In all IPSI controlled port networks, verify that the TN570D circuit pack is used. The S8400 ESS is not supported in CSS-PNC environment.	
3d. ESS with ATM-PNC.	All ATM PNC and CES circuit packs must be either TN2306B or TN2305B circuit packs. If the ATM is local to the port networks, a five to one IPSI port ratio is allowed for each survivable port network. If the ATM is remote to the port networks, an IPSI is required in each survivable port network.	
4. ESS with mixed port network connectivity (PNC).	Install an IP Media Processor and an IPSI circuit pack in every survivable port network.	
5. Change the dynamic IP address to a static IP address.	In an ESS environment, all IPSIs *must* have a static IP address.	To change the IPSI from a dynamic IP address to a static IP address, see *Installing and Configuring the Avaya S8400 Server* (03-300678), *Installing and Configuring the Avaya S8500-Series Server* (03-300143), or *Installing and Configuring the Avaya S8700-Series Server* (03-300145)
ESS servers		
		2 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
5a. (Extra Large Configurations with S8500-Series ESS servers only) Upgrade RAM.	If you are using an S8500-Series Server as an ESS server behind an Extra Large Configuration main server you must upgrade the S8500-Series server from 512 MB DRAM to 1 GB DRAM.	For instructions on how to upgrade a server to a Communication Manager 5.2 or later, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
5b. (S8400 ESS only) If required, obtain a carrier for the TN8400BP circuit pack.	A TN8400BP circuit pack can be installed only in a G650, G600, or CMC1 Media Gateway.	For instructions, see *Adding New Hardware for Avaya Servers and Gateways* (03-300684).
5c. (S8400 ESS only) Install the TN8400BP circuit pack in the G650, G600, or CMC1 Media Gateway.	Install a TN8400BP circuit pack. To prevent it from affecting service, ensure that the TN8400 circuit pack is isolated from the network during installation.	
6. Upgrade each ESS server to Avaya Communication Release 5.2.	All ESS servers must be upgraded to Avaya Communication Release 5.2 before upgrading the main server.	For instructions on how to upgrade a server to a Communication Manager 5.2 or later, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
7. (S8400 ESS only) Install Communication Manager and remaster the S8400 SSD and hard drive.	Install Communication Manager 5.2. You must remaster the SSD and hard drive before configuring the S8400 Server as an ESS server.	For instructions, see *Installing and Configuring the Avaya S8400 Server* (03-300678). For instructions on how to run the **`remaster`** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431). For remastering, you must have a USB CD/DVD drive attached to the S8400 Server.
		3 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
8. Configure the ESS server.	Use the server System Management Interface to configure the server. From the top navigation bar, click **Installation > Configure Server** and follow the online help instructions.	For instructions, see *Installing and Configuring the Avaya S8400 Server* (03-300678), *Installing and Configuring the Avaya S8500-Series Server* (03-300143), or *Installing and Configuring the Avaya S8700-Series Server* (03-300145)
		4 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
9. As needed, install license & authentication files on the ESS servers.	If you are upgrading the server from one major release to another (such as 4.0 to 5.2), a new license is required. Ensure that you are *not* loading the license file for the main server on an ESS server by checking the MID associated with the license file. The MID appears in the license file name after the letter m. Example: If you did *not* rename the license files, and the main server license file name is *s66579v5m1-060214-20295.lic*, the MID would be 1. If the ESS server license file is *s66579v5m2-060214-20295.lic*, the MID would be 2. 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 should be loaded on an ESS server.	For information on how to install the license files, see *Installing and Configuring the Avaya S8400 Server (03-300678), Installing and Configuring the Avaya S8500-Series Server* (03-300143), or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
10. Restart the server.	After loading the license file, stop the ESS server using the following Linux command: **`? stop -af`** or **`stop -caf`** Then restart the ESS server using the following Linux command: **`? start -a`** or **`start -ca`** Verify that the ESS server administration feature is turned on.	To verify that the ESS server Administration and Enterprise Survivable Server feature is turned on, see ESS server license files on page 113

Table 9: Installing ESS with existing servers

Task	Information	Documentation
11. Attach the ESS 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 ESS server is used when the ESS server registers with the main server for the first time and it may be used for subsequent registrations. On the ESS server, use the **ping** command followed by the IP address of the C-LAN.	For information on how to use the **ping** command, see *Installing and Configuring the Avaya S8400 Server (03-300678), Installing and Configuring the Avaya S8500-Series Server* (03-300143), or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
12. Verify the communication to the main server over the IP network.	On the ESS server, use the **ping** command followed by the IP address of the main server.	
Main Server		
		6 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
13. Upgrade the server.	Upgrade the main server to Communication Manager 5.2 or later. A main server should *never* run a release of Communication Manager that is later than that of the ESS server. If the existing server is running a Communication Manager release prior to 5.2, upgrade to Communication Manager 5.2 using the standard procedures. If the existing server is a main server with a manual backup server (MBS), do not upgrade to Communication Manager 5.2 or later. Instead, remaster the server using Communication Manager 5.2 or later software. If the existing server was used as an MBS, do not upgrade to Communication Manager 5.2 or later. Instead, remaster the server using Communication Manager 5.2 or later software.	To use the standard process to upgrade the main server to Communication Manager 5.2 or later, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
14. Configure the main server.	The server's System Management Interface is used to configure the main server. From the top navigation bar, click **Installation > Configure Server** and follow the online help instructions. If the server was remastered using Communication Manager 5.2 or later, use the Avaya wizard to configure the server.	To configure a server for ESS that is already running Communication Manager 5.2 or later, see Existing ESS server to main server on page 148. To configure the server using the Avaya wizard, see *Installing and Configuring the Avaya S8400 Server (03-300678), Installing and Configuring the Avaya S8500-Series Server* (03-300143), or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
		7 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
15. Install the RFA license and authentication file.	A new license for the main server (with ESS Administration feature enabled) is required if the main server has never had an ESS server. A new license is required if the server upgrade was from one major release to another. If required, load the RFA license and authentication file. Ensure that you are *not* loading the license file of an ESS server on the main server by checking the MID associated with the license file. The MID appears in the license file name after the letter m. Example: If you did *not* rename the license files, and the main server license file name is s66579v5m1-060214-20295.lic, the MID would be 1. If the ESS server license file is s66579v5m2-060214-19431.lic, the MID would be 2. 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 an ESS server.	To install the license and authentication file see *Installing and Configuring the Avaya S8400 Server (03-300678), Installing and Configuring the Avaya S8500-Series Server* (03-300143), or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
		8 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
16. Restart the server.	After loading the license file, stop the ESS server using the following Linux command: **`? stop -af`** or **`stop -caf`** Then restart the ESS server using the following Linux command: **`? start -a`** or **`start -ca`** Verify that the ESS server administration feature is turned on.	To verify that the ESS Administration feature is turned on, see ESS server license files on page 113.
17. Verify open ports in the customer's network.	This step may be necessary if the customer has firewalls. If the customer does not have firewalls, you can skip this step. Certain ports must be open for ESS server to work properly.	To obtain a list of ports that must be open for ESS server, see Network port considerations on page 64.
18. Verify LAN/WAN connectivity.	Verify communication between each ESS server and the main server over the LAN/WAN. On the main server, use the **`ping`** command followed by the IP address of the ESS server.	For information on how to use the **`ping`** command, *Installing and Configuring the Avaya S8400 Server (03-300678), Installing and Configuring the Avaya S8500-Series Server* (03-300143), or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
19. Administer ESS.	On the main server, administer each ESS server, port network communities, and no service timer.	To administer the main server see Administering ESS on page 130.
		9 of 10

Table 9: Installing ESS with existing servers

Task	Information	Documentation
20. Verify that each ESS server registers with the main server.	Use the **status ess clusters** command to verify ESS registration. A configured ESS server automatically registers with the main server when the ESS administration completes. After registration, the ESS receives a translation download from the main server. The ESS server resets to load the translations and then re-registers with the main server.	For information on the **status ess clusters** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Gateways and Servers* (03-300431).
21. Distribute the translations to the ESS servers.	Run the **save translations all** or **save translations ess** command to synchronize translations between the main and newly added S8400 ESS server for the first time.	For more information on the **save translations** command, see Saving translations on page 144.
22. Acceptance testing.	Avaya recommends testing the ESS configuration.	For information on testing an ESS configuration, see Enterprise Survivable Server Acceptance Testing on page 181.
		10 of 10

Installing ESS With New Servers

Use the information in Table 10 as a reference when installing ESS with new servers.

Table 10: Installing ESS with new servers

Task	Information	Documentation
1. **All servers**: Obtain the RFA license and the authentication files.	Obtain RFA license files and authentication files for *each* ESS server and the main server. A serial number of a different reference IPSI is needed for *each* license file.	License and authentication files are generated using RFA at http://rfa.avaya.com. For information on how to use RFA, see *Avaya Remote Feature Activation (RFA) User Guide*, at http://support.avaya.com.
2. **IPSI**: Upgrade the IPSI firmware.	Check the Minimum Firmware/Hardware Vintage document for the correct IPSI firmware needed in an ESS 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 an ESS environment see the Minimum Firmware/ Hardware Vintages document found on the http://support.avaya.com web site. A link to download IPSI firmware can be found on the support.avaya.com web site. For instructions on how to perform the firmware upgrade see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
3. **Extra Large Configurations** with S8500-Series servers only.	If you are using an S8500-Series Server as an ESS server behind an Extra Large Configuration main server you must upgrade the S8500-Series Server from 512 MB od DRAM to 1 GB DRAM.	For instructions on how to upgrade the S8500-Series Server to 1 GB DRAM, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
		1 of 9

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
4. **ESS**: Install the hardware and load Communication Manager 5.2 or later software.	.	To install the server hardware, see one of the following documents: • *Quick Start for Hardware Installation: Avaya S8400 Media Server in an Avaya G650 Media Gateway (03-300705)* • *Quick Start for Hardware Installation: Avaya S8500 Server* (555-245-701) • *Quick Start for Hardware Installation: Avaya S8700-Series Server* (555-245-703) To install the IP connectivity hardware, see *Adding New Hardware for Avaya Servers and Gateways* (555-245-112). To load Communication Manager, see one of the following documents: • *Installing and Configuring the Avaya S8400 Server (03-300678)* • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Server* (03-300145)
		2 of 9

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
5. **ESS**: Set the time.	It is important to set the time on the ESS server before loading the license file.	To set the time, see one of the following documents: • *Installing and Configuring the Avaya S8400 Server* (03-300678) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Server* (03-300145)
6. **ESS**: Configure the ESS server.	On a new installation, the Avaya wizard is used. Configuration for ESS server is included in the Avaya wizard. **Note**: You must set the time of the ESS server to the same time zone as the main server even if the ESS server is physically located in a different time zone.	For information on how to use the Avaya wizard, see one of the following documents: • *Installing and Configuring the Avaya S8700-Series Server* (03-300145) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8400 Server* (03-300678) For information on the Configure ESS window, see Configuring the Servers on page 120.
		3 of 9

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
7. **ESS**: Install the license and authentication files.	Install an RFA license file and an authentication file on *each* ESS server. Ensure that you are *not* loading the main license file on an ESS server by checking the MID associated with the license file. 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. In an example where the ESS server license file is s66579v4m2-060214-19431.lic, the MID would be 2. 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 an ESS server. After loading the license file, stop the ESS server using the following Linux command: • **`stop -af`** or **`stop -caf`** Then restart the ESS server using the following Linux command: • **`start -a`** or **`start -ca`** Verify that the ESS Administration and Enterprise Survivable Server feature is turned on.	To install the license and authentication file, see one of the following documents: • *Installing and Configuring the Avaya S8400 Server* (03-300678) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Server* (03-300145) To verify that the ESS Administration and Enterprise Survivable Server feature is turned on, see ESS server license files on page 113.

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
8. **ESS**: Verify that the ESS server can communicate with the customer's LAN interface,	An IP address of a C-LAN was entered when you configured the ESS server. The C-LAN is used when the ESS server registers with the main server for the first time and may be used for subsequent registrations. To verify that the ESS server can communicate with the customer's LAN interface use the following instruction: • On the ESS server, use the **`ping`** command followed by the IP address of the C-LAN or Processor Ethernet.	For information on how to use the **`ping`** command, see one of the following documents: • *Installing and Configuring the Avaya S8700-Series Server* (03-300145) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8400 Server* (03-300678)
9. **ESS**: Verify that the ESS server can communicate with the main server over the IP network.	To verify that the ESS server can communicate with the main server: On the ESS server, use the **`ping`** command followed by the IP address of the main server.	For information on how to use the **`ping`** command, see one of the following documents: • *Installing and Configuring the Avaya S8700-Series Server* (03-300145) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8400 Server* (03-300678)
		5 of 9

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
10. **Main server**: Install the main server hardware and load Communication Manager 5.2 or later.	In an ESS environment, you must use static IP addresses for the IPSIs in the configuration.	To install the server hardware, see one of the following documents: • *Quick Start for Hardware Installation: Avaya S8400 Media Server in an Avaya G650 Media Gateway* (03-300705) • *Quick Start for Hardware Installation: Avaya S8500 Server* (555-245-701) • *Quick Start for Hardware Installation: Avaya S8700-Series Server* (555-245-703) To load Communication Manager, see one of the following documents: • *Installing and Configuring the Avaya S8400 Server* (03-300678) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Server* (03-300145)
		6 of 9

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
11. **Main server**: Install the license and authentication file.	Ensure that you are *not* loading the license file for an ESS server on the main server by checking the MID in the license file. 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. In an example where the ESS server license file is s66579v4m2-060214-19431.lic, the MID would be 2. 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 an ESS server. After loading 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 ESS Administration feature is turned on.	To install the license and authentication file, see one of the following documents: • *Installing and Configuring the Avaya S8400 Server* (03-300678) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Server* (03-300145) To verify that the ESS Administration feature is turned on, see ESS server license files on page 113.
		7 of 9

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
12. **Main server**: Verify LAN/WAN connectivity.	Verify communication between each ESS 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 ESS server.	For information on how to use the **`ping`** command, see one of the following documents: • *Installing and Configuring the Avaya S8700-Series Server* (03-300145) • *Installing and Configuring the Avaya S8500-Series Server* (03-300143) • *Installing and Configuring the Avaya S8400 Server* (03-300678)
13. **Main server**: Verify open ports in customer's network.	This step may be necessary if the customer has firewalls. If the customer does not have firewalls, you can skip this step. Certain ports must be open for ESS server to work properly.	To obtain a list of ports that must be open for ESS server, see Network port considerations on page 64.
14. **Main server**: Administer ESS.		To administer ESS on the main server, see Administering ESS on page 130.
15. **Main server**: Verify ESS registration.	Use the **`status ess clusters`** command to verify ESS registration with the main server.	For information on the **`status ess clusters`** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Gateways and Servers* (03-300431).
		8 of 9

Table 10: Installing ESS with new servers (continued)

Task	Information	Documentation
16. Acceptance testing	Avaya recommends testing the ESS configuration.	For information on how to test a configuration, see Enterprise Survivable Server Acceptance Testing on page 181.
17. **Main server**: Distribute the translations to the ESS server.	If changes are made to translations, they must be distributed to the ESS server by executing the **`save translations all`** or **`save translations ess`** command.	For more information on the **`save translations`** command, see Saving translations on page 144.
		9 of 9

ESS server license files

This chapter provides information on RFA license files for ESS 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. For information on the S8700-Series servers or the S8500-Series server see one of the following documents:

- For the S8700-Series servers refer to *Installing and Configuring the Avaya S8700-Series Server* (03-300145) at http://support.avaya.com.
- For the S8500 Servers refer to *Installing and Configuring the Avaya S8500-Series Server* (03-300143) at http://support.avaya.com.

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 Remote Feature Activation (RFA) application found at the RFA web site, http://rfa.avaya.com.

This section provides an understanding of how:

- Certain aspects of an RFA license file impacts ESS:
  - Module IDs and Cluster IDs on page 114
  - System Identification numbers (SID) on page 115

- Serial numbers on page 115
- IPSI maintenance replacement on page 116

- To turn on the ESS functionality using the license file:
  - Activating ESS through the RFA license file on page 116
- To obtain a RFA license file:
  - Obtaining a RFA license on page 117
- License-error mode and No-License error modes impacts an ESS server:
  - License error modes with ESS servers on page 118
- To obtain a license file when replacing a main server or an ESS server:
  - License files for replacement servers on page 119

Module IDs and Cluster IDs

The Remote Feature Activation (RFA) application assigns a Module Identification number (MID) to each simplex server and every duplex pair of servers.The MID is contained in the license file and cannot be changed.

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. In an example where the ESS server license file is s66579v4m2-060214-19431.lic, the MID would be 2.

CAUTION:

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 an ESS server.

RFA assigns a maximum of 250 MIDs for each system. The MID for the main server is always one. The remaining 249 MIDs are assigned to each ESS server, and LSP, in sequence.

For the ESS server to register with the main server, the MID of the ESS server must match its administered CLID. The CLID is administered in the **Survivable processor** screen. For more information on how to administer ESS using the **Survivable processor** screen, see Administering an ESS server on the main server on page 131.

System Identification numbers (SID)

When a license file is created in RFA, the system is assigned a System Identification number (SID). Each SID is a unique number that can be used to identify and locate the System Record within RFA. Once a SID is created in RFA the value never changes. Any changes to the RFA information contained in a SID is reflected in a change in the SID's version number.

In an ESS environment, the main server and every ESS server has the same SID.

See Table 11 for an overview of RFA naming conventions and how they pertain to ESS.

Note:

In ESS terminology, there is a SID and a Server ID (SVID). The SID is assigned by RFA and cannot be changed. The Server ID (SVID) is a number selected by the administrator that is assigned to the server when the server is configured. For more information on administering the SVID, see Configuring the Servers on page 120.

Table 11: RFA naming convention

RFA Name	ESS Name	Notes
Module ID (MID)	Cluster ID (CLID)	This value is generated by RFA and is unique for each ESS server and main server.
System ID (SID)	System ID (SID)	This value is generated by RFA and will be the same for the main server and each ESS server.

Serial numbers

RFA requires a unique serial number for each license file. In an ESS environment, the serial number for the reference Internet Protocol Server Interface (IPSI) is used. Each ESS server requires its own license file with an associated unique IPSI serial number. This implies that there cannot be more ESS servers than there are IPSI circuit packs in the system. However, for high availability systems, that have duplex IPSIs, both IPSIs in a port network may be used to generate license files.

You can find the serial numbers for all the IPSIs in the system by:

- Executing the **`statuslicense -v`** Linux command. An asterisk (*) denotes the reference IPSI in the list.
- Clicking **License File** from the server's maintenance Web interface. An asterisk (*) denotes the reference IPSI on the list.

IPSI maintenance replacement

As stated earlier, each server in an ESS configuration must contain a license file with a unique IPSI serial number. When multiple IPSIs in a configuration are being used as reference IPSIs, additional care is needed when replacing an IPSI for maintenance.

Note:

For each server, you can determine the serial number of the IPSI that is being used as a reference IPSI by clicking **`License File`** under the Security heading of the server's maintenance Web interface.

If a reference IPSI is changed out, a new RFA license file must be generated using the RFA Swap-Out functionality.

Activating ESS through the RFA license file

The license file is used to activate the ESS feature. It is important to understand what needs to be enabled in the license file for a main server and an ESS server.

Feature Keywords

The SAP order for an ESS system contains material codes for feature settings that appear in the license file. The material codes in a license file are identified as Keywords. RFA uses the following Keywords for ESS:

- FEAT_ESS (ESS feature administration): This feature is turned **on** for both the main server and the ESS server.
- FEAT_ESS_SRV (Enterprise Survivable Server): This feature is turned **off** for the main server and **on** for the ESS 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.

Checking the license file

After you load the license file on the server you can run the following Linux commands on an ESS 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 ESS server using the following Linux commands:

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

Obtaining a RFA license

What you need

You will need the following information to create license files for the main server and each ESS server in RFA:

- Single Sign On (SSO) login
- Serial numbers for each reference IPSI

  Note:

  Each ESS server must be licensed to a **unique** reference IPSI.
- SAP order numbers
- Serial number of the media gateway, if a LSP is being used
- Customer information
- Delivery method: E-mail address if this file is delivered using email
  - RFA provides two methods of delivery, e-mail and computer download.

Creating the license file

For detailed instructions on how to create a license file using the Remote Feature Activation (RFA) application, see the *Avaya Remote Feature Activation (RFA) User Guide* located at http://support.avaya.com.

Important:

You must be registered and authenticated for the Communication Manager product family to create a license file in RFA:

- Registered: You have been given an SSO login and are identified in the RFA database.
- Authenticated: Your coach or your BusinessPartner manager has approved your access to RFA.

License error modes with ESS servers

An ESS server runs in License-Normal mode when it does not control an IPSI. Once the ESS server controls an IPSI, the ESS server runs in License-Error mode. The ESS server continues to run in License-Error mode until it no longer controls an IPSI, or until the 30 day timer expires and it enters into a No-License mode.

A main server runs in License-Normal mode when it has a valid license file and can communicate with its reference IPSI. During a failover, the license mode on the main server can change when:

- **It has been in-service for more than 35 minutes and can no longer communicate with its configured reference IPSI**: The main server enters into License-Error mode if it can no longer communicate with its reference IPSI. This condition is possible during a failover if, due to network fragmentation, the reference IPSI resides in a port network that is now being controlled by an ESS server.

  The lack of communication between the main server and the reference IPSI is detected by the License File audit or by the **`test license`** command. Once the server has determined that the reference IPSI is missing, it takes approximately two to three hours for the main server to enter into License-Error mode. Once in License-Error mode administration commands are blocked. The License-Error condition remains on the main server even after communication with the reference IPSI is established until:

  - The license audit runs (this may take up to one hour).
  - A **`test license`** command is executed on the main server's SAT and is completed successfully.

- **The main server was out-of-service and upon reboot, cannot communicate with its reference ISPI**: Thirty minutes after any system restart, Communication Manager starts the first License File audit by attempting to retrieve the previous license file state. If the previous state cannot be retrieved because of errors, such as, 'Reference IPSI Not

Responding', then the system enters into No-License mode. In No-License mode administration is denied. Once communication with the reference IPSI is re-established, the main server enters into License-Normal mode when:

- The license audit runs (this may take up to one hour).
- A **`test license`** command is executed on the main server's SAT and is completed successfully.

License files for replacement servers

A new RFA license file is required in the following scenarios:

- The main server has a non-recoverable error and is replaced by an ESS server:
  - The license files for a main server and an ESS server are different. The license file for an ESS server has both the FEAT_ESS and FEAT_ESS_SRV keywords turned on. The FEAT_ESS keyword identifies this server as an ESS server. To change the ESS server to a main server, you must obtain a new RFA license file with the FEAT_ESS_SRV keyword turned off and the FEAT_ESS keyword turned on.

An existing RFA license must be installed in the following scenario:

- The ESS server or main server has a non-recoverable error and must be replaced with another server of the same type.
  - If the same reference IPSI is used for the new server, you do not have to generate a new RFA license file.The existing RFA license file can be used.

The Extra Large main server

The Extra Large configuration is offered on two servers, the S8720 Server and the S8730 Server. The S8730 Server is offered in an Extra Large configuration only while the S8720 server is offered in two configurations, Standard Capacities and Extra Large.

Both the S8720 Server and the S8730 Server can be configured as software duplication or hardware duplication. If the server is configured as hardware duplication the DAL2 duplication memory card is used. The DAL2 has increased memory (512MB) over the existing DAL1 (256MB).

Not all server types can be used as an ESS server when the main server is configured as Extra Large. Use Table 1: LSP or ESS server types for Release 5.2 on page 15 for information on supported server configurations

Note:

If the main server is configured as Extra Large, the ESS server must also be configured as Extra Large.

Configuring the Servers

This section provides instructions on how to configure the server in an ESS configuration.

Collect the data

Collect the following information before configuring the main server and each ESS server:

- IP address for this server.
- Host name for this server
- Function assignment and configuration information for each operational ethernet interface.
- IP addresses of UPS units.
- DNS configuration (if used).
- DHCP server configuration (if used).
- Configuration data for static network routes (if used).
- Network Time Server configuration data.
- Modem return route data from Avaya Services (if Avaya Services supports this server).
- Configure Remote Maintenance Board (RMB) (only used in S8400 and S8500-Series servers).

  Note:

  DHCP is not supported in an ESS environment.

- **Priority and preference settings of each ESS server**: For more information on setting the priority for each ESS server, see IPSI Priority List on page 71.

Before you start

Complete the following steps before configuring the main server and each ESS server:

1. Communication Manager release 3.0 or later must be installed on each server.
   - **An ESS server**: An ESS server can run a release of Communication Manager that is ***later*** than that of the main server.
     - To ensure that translation downloads occur properly, upgrade an ESS server and any LSPs *before* upgrading the main server.

   Important:

   Do not connect the ESS server to the LAN until you have configured it.

2. Install the required patches.
3. Upgrade the firmware on the IPSIs: To identify the firmware needed for an IPSI in an ESS environment see the Minimum Firmware/Hardware Vintages document located at http://support.avaya.com
4. A new license file with ESS enabled installed on each server: The license file enables the ESS feature and sets the platform type. A license file with ESS enabled must be loaded on each server in the enterprise. After loading the license file execute the **`display system-parameters customer-options`** command.

   Check the following:

   a. The main server and each ESS server**:** Each server is assigned a platform number in the license file. The platform number appears on the first page of the **Optional Features** screen. For an example of page one of this screen, see Figure 30.

Figure 30: System-parameters customer-options platform type

```
display system-parameters customer-options                    Page   1 of  11
                              OPTIONAL FEATURES

    G3 Version: V15                            Software Package: Standard
      Location: 1                           RFA System ID (SID): 1
      Platform: 15                          RFA Module ID (MID): 50

                                                        USED
                                Platform Maximum Ports: 48000 16581
                                      Maximum Stations: 36000 12795
                                Maximum XMOBILE Stations: 0     0
                    Maximum Off-PBX Telephones - EC500: 4     3
                    Maximum Off-PBX Telephones -   OPS: 2     0
                    Maximum Off-PBX Telephones - PBFMC: 0     0
                    Maximum Off-PBX Telephones - PVFMC: 0     0
                    Maximum Off-PBX Telephones - SCCAN: 2     0




       (NOTE: You must logoff & login to effect the permission changes.)
```

Use Table 12 to verify that the platform type is correct for your server type.

Table 12: Platform numbers and server types

Platform number	Server type
6	S8700-Series servers
12	S8500-Series, S8510 main server
14	S8700-Series ESS server
15	S8500-Series ESS server
24	S8400 ESS server

b. There are two features for ESS, **Enterprise Survivable Server** and **ESS Administration**. The ESS features can be found on page 4 of the **Optional Features** screen.

- Main server: Verify the **ESS Administration** field is set to yes while the **Enterprise Survivable Server** field is set to **no**.

- Each ESS server: Verify that both the **Enterprise Survivable Server** and **ESS Administration** fields are set to **yes**.

For an example of page 4 of the **Optional Features** screen for an ESS server, see Figure 31.

Figure 31: System-parameters customer-options - page 4 - ESS server

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

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

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

Important:

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

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

Configuring the main server and each ESS server

Important:

On duplex servers, you must run Configure Server on each server in the server pair.

Use the following steps to configure the main server and each ESS server:

Note:

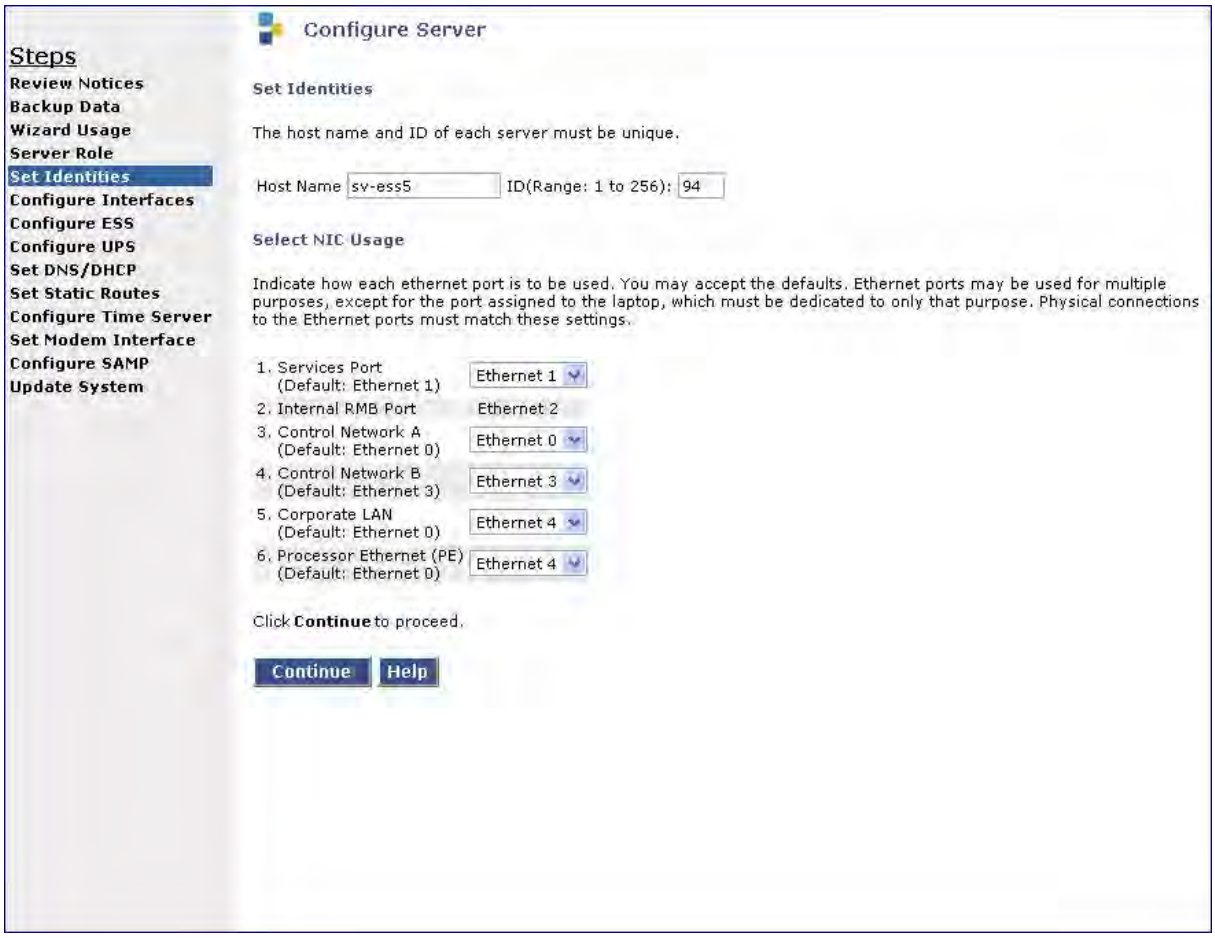
This chapter outlines the fields that are important when administering a main server in an ESS environment, or a server used as an ESS server in an ESS environment. It does not contain detailed information on how to load and configure the Avaya S8xxx servers. For documentation information, see ESS Installation Checklist on page 94.

Important:

You must set the time of the ESS server to the same time and time zone as the main server even if the ESS server is physically located in a different time zone.

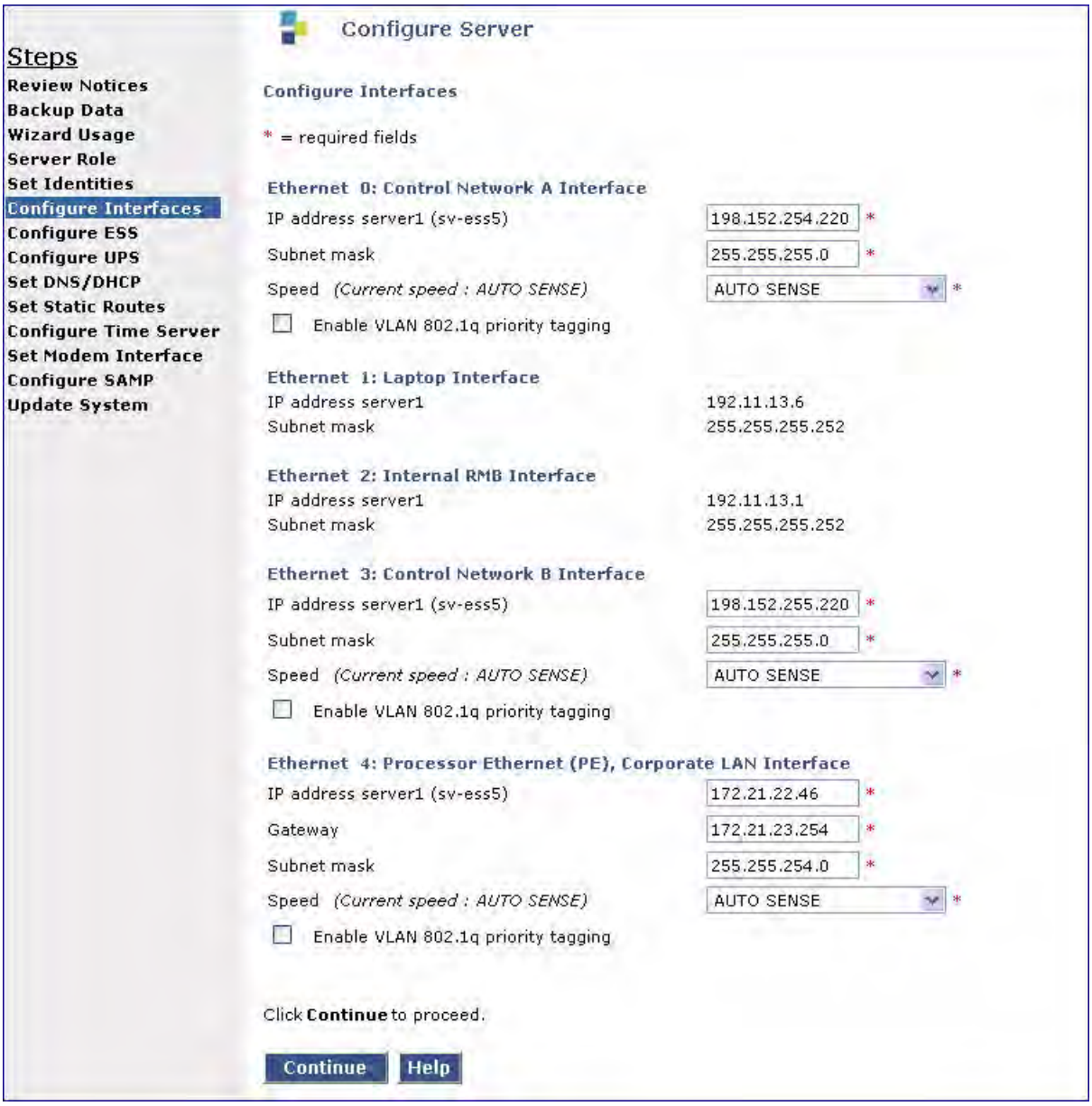
1. Log on the server's System Management Interface:
   a. Open a supported Web browser.
   b. In the **Address** field, enter http://*IPaddress*, where *IPaddress* is the IP address of the server that you want to access. Alternatively, enter the fully qualified domain name of the server.
   c. Log in as dadmin or craft.
   d. Click **Yes** to suppress alarm origination.
2. Click **Installation > Configure Server**.
3. On the **Review Notices** page, click **Continue**.
4. If the server is the active server of a duplicated pair, the system displays a warning. Click **Continue**.
5. On the **Back Up Data** page, perform one of the following actions:
   a. If you do not want to back up your data, click **Continue**.
   b. If you want to back up your data, click **Administration > Server (Maintenance)** on the System Management Interface. Click **Backup Now**. After the backup is complete, continue with the remaining steps of this procedure.
6. On the **Specify how you want to use the wizard page**, select one of the following:
   - Configure all services using the wizard
   - Configure individual services
   - (only for duplex servers) Copy configuration information from the duplicated server
7. On the **Specify Server Role** page, specify whether the server is a main server, ESS server, or an LSP.
8. On the **Set Identities** page (Figure 32), specify the server ID, serial number, duplication technology details, and network interface card usage details as applicable to your server type. For more information, see Set Identities page parameters on page 127.

Figure 32: Set Identities page



9. On the **Configure Interfaces** page (Figure 33), specify the IP addresses for network interfaces and special parameters for Processor Ethernet as applicable to your server type. For more information, see Configure Interfaces page parameters on page 128.

Figure 33: Configure Interfaces page



10. On the **Configure ESS** page (Figure 34), specify the interfaces on the main server(s) that this ESS server will use for registration and file synchronization. For more information, see Configure ESS page parameters on page 129.

Figure 34: Configure ESS page

11. Complete the remaining steps to configure the server.
12. Reset the server after configuring the server.
13. Connect the configured ESS server to the LAN.

Set Identities page parameters

ID: Each server within the enterprise is assigned a unique server ID (SVID). Gaps in the SVIDs are allowed. Each server in the system, duplex or simplex, main server or ESS server, requires a unique SVID. You assign a unique SVID to each server. The SVID must be in the range of 1 to 99. Each server in a server pair (S8700-Series servers) requires a different SVID. You can assign the SVID sequentially or allow gaps in the numbering such as 10, 20, 30, etc.

You will enter the Server ID in the **Survivable Processor** screen when you administer ESS. You cannot enter duplicate server IDs in this screen.

Server Number: This field appears only for duplex servers. When servers are duplicated, one server is assigned server number 1 and the other number 2. The server assigned

number 1 will be is preferred in server interchange decisions when the state of health of the two servers is equal.

Server Duplication: If this server is duplicated, the ability to select the type of duplication technology is provided. If a hardware duplication circuit pack is present, the ability to select hardware duplication is provided. If this circuit pack is not present, then only software duplication is shown and the only choice is to select encryption of the duplication link or not.

Note: Selecting encryption reduces the capacity of the server by approximately 25%.

Select NIC Usage: This section lists the functions that are supported on this server and allows those functions to be associated with a particular network interface. The possible functions are:

- Laptop Interface: The laptop function must be assigned to a NIC by itself. The laptop interface is not restricted by firewall rules and is designed for local connection of a services laptop.
- Duplication Link: The duplication link is the link that is used to shadow memory contents from the active server to the standby server in a duplicated pair. This link must be assigned to a gigabit Ethernet interface and must be assigned to a NIC by itself.
- Control Network A and Control Network B: These are the links that are used to communicate with the IP Serial Interfaces (IPSI) in a G650 gateway. If there is only one IPSI in each G650, then only control network A is assigned. If there are two IPSIs in each G650, then both control network A and control network B are assigned.
- Enterprise LAN: The enterprise LAN is the primary interface for system administration.
- Processor Ethernet: The Processor Ethernet or Processor Ethernet interface is a special interface that is used like or in place of a C-LAN interface. IP telephones, trunks and certain adjuncts may connect to the Processor Ethernet interface. *The Processor Ethernet interface must be assigned to the same NIC as the enterprise LAN*.

Note:

Only those functions supported on this server are shown on the **Set Identities** page.

Configure Interfaces page parameters

This page is used to configure IP addresses for the network interfaces that were assigned in the Set Identities page and to configure special parameters for the Processor Ethernet (PE) interface on duplex servers. A red asterisk (*) marks a field that is a required entry.

When entering values in this page the following must be noted:

- The NIC used for the laptop interface is automatically assigned fixed values that cannot be changed.
- When entering information for duplex servers, enter IP addresses consistent with how these servers were assigned server numbers on the Set Identities page.

- The address assigned to the active server on duplex servers is what the industry knows as an IP-alias. The active server in a duplex pair of Communication Manager servers will respond on this address; the standby server in the pair will not. If a server interchange occurs, the server that becomes the active server will re-associate its MAC address with the active server IP address. It is very important to assign the *same* IP address to the active server entry on both servers in a duplex pair of servers. The NIC being assigned an active server address will have two IP addresses associated with it, a server unique address assigned as IP address server1 or IP address server2 and an alias address assigned as the IP address active server. A pair of duplex servers will then require three IP addresses, one unique to each server and a third for the alias. All three addresses must be on the same subnet.
- The terms IP address, (default) gateway, subnet mask, speed, and VLAN tagging are used in the standard industry manner.
- Verify with the network administrator that the LAN hardware supports 802.1q priority tagging. If supported, select **VLAN 802.1q priority tagging**.

Processor Ethernet (PE) Parameters

Two special parameters appear when Processor Ethernet is assigned on a duplex pair of servers. These parameters control how the health of the Processor Ethernet interface affects server interchange decisions and how the system determines whether the Processor Ethernet interface is working or not (PE state of health).

PE Interchange Priority

Assign the Processor Ethernet a simple relative priority as compared to IPSIs in configurations that use both Processor Ethernet and IPSIs. The priority levels are as follows:

- **PE = HIGH** Favor the server with the best PE SOH when PE SOH is different between servers.
- **PE = LOW** Favor the server with the best IPSI connectivity when IPSI SOH is different between servers.
- **PE = EQUAL** Count the Processor Ethernet interface as one IPSI and favor the server with the best connectivity count.
- **PE = IGNORE** Do not consider the Processor Ethernet in server interchange decisions.

IP Address for PE Health Check

Enter the IP address to enable the server to determine whether its Processor Ethernet interface is working or not. The network gateway router is the default address. Any device on the network that will respond can also be used.

Configure ESS page parameters

- Enter the C-LAN or Processor Ethernet IP address that will be used when the ESS server registers with the main server. For more information, see C-LAN access for ESS registration on page 19.

- Enter the IP address(es) for the main server. This IP address(es) will be used for synchronizing the translation file between the main server and the ESS server.
- Optionally, you can enter the alternate address for file synchronization.
- **Configure Memory**: Select the type of memory used by the server. The ESS server must be configured as Extra Large if the main server is configured as Extra Large. The S8720 main server can be configured with either Extra Large or Standard memory. The S8730 main server is always configured as Extra Large.

After the ESS server is configured

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

Note:

An ESS server cannot register with the main server until it has been administered. Administration for an ESS server is done on the main server. For instructions on how to administer the ESS server, see Administering an ESS server on the main server on page 131.

Note:

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

Administering ESS

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

- Administer up to 63 ESS 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 an ESS server on the main server

Important upgrade information

In Communication Manager Release 5.2, use the **Survivable Processor** screen to administer node names for servers. Starting with Communication Manager Release 3.1, node-names were used in place of the IP addresses for the ESS servers. When *upgrading* an ESS configuration, the following events occur automatically:

- The system automatically creates a node-name for each administered ESS server. The node-name is combination of:
  - The string 'ESSCid' followed by the cluster ID of the ESS server.
  - The string 'Sid' followed by the ID of the ESS server.

    For example, if the ESS server had an IP address of 111.222.333.123, a cluster ID of 4, and a server ID of 2, the node-name automatically assigned to the server would be, ESSCid004Sid002. This node-name would have the IP address of 111.222.333.123.
- A survivable-processor entry is created for each ESS server.

Pre-requisites

Verify the MID: Use the **`statuslicense -v`** Linux command if you do not know the MID for the ESS server. The MID displays in the **RFA Module ID** field. 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. In an example where the ESS server license file is s66579v4m2-060214-19431.lic, the MID would be 2.

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 an ESS server.

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

1. On the main server, type **`change survivable processor`** ***n*** where ***n*** is the node name of the ESS server.
2. Administer the required fields for each ESS server:

   Page 1: Identify LSPs and ESS 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 AE Services, if you have an AE Services, a CDR that connects to the Processor Ethernet interface of the LSP or ESS server that you identified in page one.

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

   For details of the screen, see Survivable Processor screen on page 132

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 Community Assignments for Port Networks screen on page 139.

   Page 2: Schedule the **Auto Return** feature and to set the no service timer, as described in Port Network Recovery Rules screen on page 140.

Survivable Processor screen

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

Page one of the Survivable Processor screen

The first page of this screen initially appears as shown in Figure 35. The other fields and values that appear on this screen depend on the **Type** value. If you are adding an ESS server, when you change the Type to either **simplex-ess** or **duplex-ess**, the screen gets refreshed, as shown in Figure 36 and Figure 37.

Figure 35: Survivable Processor screen- adding an LSP

```
add survivable-processor punsrvrl                              Page   1 of   4
                    SURVIVABLE PROCESSOR

Type: lsp                                 Processor Ethernet Network Region:


          Node Name: lsp-4
         IP Address: 135.9.9.4
```

Figure 36: Survivable Processor screen- adding a simplex ESS server

```
add survivable-processor punsrvrs                                Page   1 of   4
                    SURVIVABLE PROCESSOR

Type: simplex-ess      Cluster ID:       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:
          Node Name: ess-smp
         IP Address: 135.9.9.4




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

Figure 37: Survivable Processor screen- adding a duplex ESS server

```
add survivable-processor punsrvrd                                Page   1 of   4
                    SURVIVABLE PROCESSOR

Type: duplex-ess       Cluster ID:       Processor Ethernet Network Region: 1
                        Community: 1         Enable PE for H.323 Endpoints? n
ACTIVE SERVER                                 Enable PE for H.248 Gateways? n
          Node Name: ess-d
         IP Address: 135.9.9.4
SERVER A
          Server ID:
          Node Name:
         IP Address:
SERVER B
          Server ID:
          Node Name:
         IP Address:

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

- **Type**: Enter the survivable processor type, **lsp, simplex-ess,** or **duplex-ess**.
- **Processor Ethernet Network Region**: Enter the network region in which the Processor Ethernet interface of the LSP or ESS resides (valid values 1 to 250).
- **CLID**: Enter the Cluster ID (the Module ID from the Communication Manager license file) for the ESS server. The Cluster ID corresponds to the Module ID from the license file of the ESS server. Valid values are **1** thru **999** and **blank**.
- **Node Name**: (display-only) shows the name used to identify this server. You 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.
- **IP Address**: (display-only) shows 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 ESS.
- **Community**: A community is a virtual group consisting of an ESS server and one or more Port Networks. Assigning an ESS server to a community associates the ESS server with the IPSI(s) in the Port Network(s) for that community. The IPSI(s) are assigned to communities on the **System Parameters Port Network** screen. The association effects how the ESS server is prioritized for the IPSI in that community, if the ESS server is administered with a **Local Preferred** or **Local Only** preference. The Community number for an S8400 ESS server must be set to 2 or greater and must be unique.

Note:

It is possible to administer an ESS server as having no preferences and just a priority score. If all ESS servers were administered in this fashion, the IPSI would prioritize each ESS server based on its priority score only.

- **Enable PE for H.323 Endpoints?**: Enter **y** to allow the Processor Ethernet interface of the ESS server to be used for H.323 devices such as phones. If you enter **n**, the ESS Node Name may not appear in the Alternate Gatekeeper (Backup Server) List on the **IP Network Regions** screen. If you enter **y** and you administer the ESS node name on the **IP Network Regions** screen, the AGL list for IP endpoints will include the ESS Processor Ethernet.

  When you run the **`display ip-interface procr`** command on the ESS server, the **Allow H.323 Endpoints?** field in that screen displays the value that you enter.
- **Enable PE for H.248 Gateways?**: Enter **y** to allow the Processor Ethernet interface of the ESS server to be used for gateways. When you run the **`display ip-interface procr`** command on the ESS server, the **Allow H.248 Gateways?** field in that screen displays the value that you enter.
- **Active Server Node Name**: (display only) This field is displayed only for duplex ESS servers. The node name entered at the command line is displayed.

- **Active Server IP Address**: (display only) This field is displayed only for duplex ESS servers. The IP address corresponding to the node name entered at the command line is displayed.
- **Server A ID**: Server A ID corresponds to the Server ID configured using the **Set Identities** page under **Configure Server** on the System Management Interface of the ESS server. The administration on the main server and the configuration on the ESS server must match for the ESS server to register to the main server. Valid values are **1** thru **256** and **blank**.
- **Server A Node Name**: (display only) For LSP or simplex ESS server, the node name is displayed. For duplex ESS servers, enter the node name for Server A.
- **Server A IP Address**: (display only) The IP address corresponding to the node name for Server A is displayed.
- **Server B ID**: (display only) For duplex ESS servers, the node name of Server B is displayed.
- **Server B Node Name**: For duplex ESS servers, enter the node name for Server B.
- **Server B IP Address**: (display only) For duplex ESS servers, the IP address corresponding to the node name for Server B is displayed.
- **Community Size**: Default is **all**. For an S8400 ESS server, the value must be **Sngl_PN**.
- **System Preferred**: Use this option when the goal is to keep as much of the system network intact as possible, allowing one ESS 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**.

  For S8400 ESS server, this defaults to **n** and cannot be changed.
- **Priority Score**: Enter the Priority Score for this ESS server. Valid values are 1 thru 100. Default is 1.
- **Local Preferred**: Use this option when you want the ESS 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**. When the Community size is set to **Sngl_PN** (for an S8400 ESS server) this field defaults to **n** and cannot be changed.
- **Local Only**: Use this option when you want the ESS server to accept the request for service from an IPSI, only if the IPSIs is located in the same community as the ESS server. Default is **n**. For S8400 ESS server, this defaults to **y** and cannot be changed.

Page two of the 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 appear 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.

Figure 38: Survivable Processor screen page two

```
change survivable-processor sv-ess13                          Page   2 of   4
                  SURVIVABLE PROCESSOR - PROCESSOR CHANNELS

Proc                          Interface        Destination        Session
Chan Enable   Appl.      Mode Link/Chan      Node          Port  Local/Remote
 1     i      mis         s    1   5001   CMS_lebeau      0      1     1
```

- **Proc Channel**: This display only field shows the processor channel used for this link when it was administered in the **Survivable Processor - Processor Channels** screen.
- **Enable**: Enter one of the following values in this field:
  - Enter a 'n' (no) if this processor channel is disabled on the LSP or the ESS server.
  - Enter an 'i' (inherit) if this link is to be inherited by the LSP or ESS 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 ESS server to use the same connectivity.
    - The main server connects to the adjuncts using the main server's Processor Ethernet interface and you want the LSP or ESS 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 LSP or the ESS 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 LSP or the Processor Ethernet interface of the ESS server.

    When you enter an 'o' in the enable field, you can enter the processor-channel information for the LSP or the ESS server in the remaining fields.
- **Appl**: This display-only field identifies the server application type/adjunct connection used on this channel.
- **Mode**: This field identifies if the IP session is passive (client) or active (server). Valid entries are 'c' for client, 's' for server, or blank.
- **Interface Link**: This 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.

- **Interface Channel**: For TCP/IP, interface channel numbers are in the range of 5000-64500. The value 5001 is recommended for CMS.
- **Destination Node**: This 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.
- **Destination Port**: This 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.
- **Session Local and Session Remote**: The Local and Remote Session is an intriguer 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.

Page three of the Survivable Processor screen

Use page three if you have an AE Services, a CDR that connects to the Processor Ethernet interface of the LSP or ESS server that you identified in page one, or Survivable CDR. If the AE Services or the CDR is administered on the **IP Services** screen it automatically appears 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 on page 89. For more information on how to administer Survivable CDR, see *Avaya Aura™ Communication Manager Feature Description and Implementation* (555-245-205).

Figure 39: Survivable Processor screen page three

```
change survivable-processor sv-ess13                          Page   3 of   4
                  SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local             Local    Remote            Remote
  Type              to dsk  Node              Port     Node              Port
  CDR1        C       n     gert_clan1        0        cdr_1             9003
  CDR2        i       n     gert_clan1        0        cdr_rsp           9000
  AESVCS      i       n     gert_clan2        8765
  AESVCS      i       n     gert_clan6        8765
```

- **Service Type**: This display only field identifies the server application type/adjunct connection used on this channel. Valid entries include CDR1 or CDR2, and AESVCS.
- **Enabled**: Enter one of the following values in this field:
  - Enter a 'n' (no) if this ip-services link is disabled on the LSP or the ESS server.
  - Enter an 'i' (inherit) if this link is to be inherited by the LSP or ESS 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 ESS server to use the same connectivity.
- The main server connects to the adjuncts using the main server's Processor Ethernet interface and you want the LSP or ESS 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 LSP or the ESS server. Generally you would want the over-ride

- **Store to Dsk:** Enter a 'y' to enable Survivable CDR for this LSP or ESS 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 LSP or ESS server being administered will be sent to the hard disk rather than output to an IP link. LSP or ESS server will only store CDR records to hard disk when the LSP or ESS 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).

- **Local Node:** This field contains the node name as defined on the **Node Names** screen.
- **Local Port:** This field contains the originating port number. For client applications such as CDR, this field defaults to a zero.
- **Remote Node:** Specify 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. This field does not apply for AE Services.
- **Remote Port**: Specify the port number of the destination. Valid entries range from 5000 to 65500 for CDR or AE Services. The remote port number must match the port administered on the CDR or AE Services server.

Note:

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

Note:

The **System-Parameters CDR** screen is removed on the LSP or the translations of the ESS server when a **no** is entered in the **enable** field on the page three of the **Survivable Processor** screen.

Page four of the Survivable Processor screen

Page four appears 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.

Figure 40: Survivable Processor screen page four

```
change survivable-processor sv-ess13                          Page   4 of   4
         SURVIVABLE PROCESSOR - IP-SERVICES - Session Layer Timers

 Service     Reliable  Packet Resp   Session Connect  SPDU  Connectivity
  Type       Protocol     Timer       Message Cntr    Cntr     Time

  CDR1         n          30               3          3         60
  CDR2         n          30               3          3         60
```

- **Service Type**: This display-only field shows the service type.
- **Reliable Protocol**: This field is used to indicate whether you want to use a reliable protocol over this link. Valid entries include ’y’ or ’n’.
- **Packet Response Timer**: 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.
- **Session Message**: Enter the number of times Communication Manager tries to establish a connection with the far-end adjunct. Valid entries are one to five.
- **Connect Cntr**: 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.
- **SPDU Cntr**: This Session Protocol Data Unit counter indicates the number of times Communication Manager transmits a unit of protocol data before generating an error.
- **Connectivity Timer**: 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.

Community Assignments for Port Networks screen

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 one of the screen is used to enter the community assignments for each port network. Assigning port networks to a community associates the port network with an ESS server administered with the Local Preferred or as a Local Only server. An ESS server is assigned a community on page one of the **Community Assignments for Port Networks** screen. To have the ESS server and the port networks in the same community, the community number of the ESS server and the community number for each port network must match. For an example of the screen, see Figure 41.

Note:

The community number associated with a S8400 ESS must be 2 or greater and the S8400 ESS can be associated with only one port network.

Figure 41: Community Assignments for Port Networks screen - page 1

```
change system-parameters port-networks                          Page   1 of   2

               COMMUNITY ASSIGNMENTS FOR PORT NETWORKS


 PN Community     PN Community     PN Community     PN Community     PN Community
 ------------     ------------     ------------     ------------     ------------
  1: 10            14: 1            27: 1            40: 1            53: 1
  2: 1             15: 1            28: 1            41: 1            54: 1
  3: 1             16: 1            29: 1            42: 1            55: 1
  4: 1             17: 1            30: 1            43: 1            56: 1
  5: 1             18: 1            31: 1            44: 1            57: 1
  6: 1             19: 1            32: 1            45: 1            58: 1
  7: 1             20: 1            33: 1            46: 1            59: 1
  8: 1             21: 1            34: 1            47: 1            60: 1
  9: 1             22: 1            35: 1            48: 1            61: 1
 10: 1             23: 1            36: 1            49: 1            62: 1
 11: 1             24: 1            37: 1            50: 1            63: 1
 12: 1             25: 1            38: 1            51: 1            64: 10
 13: 1             26: 10           39: 1            52: 1
```

Port Network Recovery Rules screen

Page two of the screen is used to schedule the **Auto Return** feature and to set the no service timer: See Figure 42.

- **Auto Return**: The **Auto Return** functionality 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 appear 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 appear. 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 appears. 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.

- **No Service Time Out Interval** (default 5 minutes): Enter the time, in minutes, that the IPSIs will wait before requesting service from the highest ESS server on its priority list. Valid values for this field are three to 15 minutes.
- **PN Cold Reset Delay Timer** (default 60 sec): Time in seconds after which the PN cold reset occurs. Valid values are **60** thru **120**.

Figure 42: Port Network Recovery Rules screen

```
change system-parameters port-networks                          Page   2 of   2


                  PORT NETWORK RECOVERY RULES


 FAILOVER PARAMETERS                      FALLBACK PARAMETERS

 No Service Time Out Interval (min): 5             Auto Return: no

    PN Cold Reset Delay Timer (sec): 60
```

After administering the ESS servers

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

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

The process listed above is automatic. After the ESS server receives the initial translation download, any translation changes are sent to the ESS server by executing the **save translations all**, or **save translations ess** command (Saving translations on page 144).

Check 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** field in the title line has the same value as the MID in the license file. To verify the Cluster ID for each server, use the Linux command, **`statuslicense -v`**. The Cluster ID is the same as the RFA Module ID. 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 ESS server is not registered and no data will appear in the **Translation Updated** or **Software Version** columns. It may take several minutes for the ESS server to register to the main server. To troubleshoot the ESS registration, see Troubleshooting on page 171.

   - 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 Communication Manager 3.0 or later.

   For an example of the output of the **`status ess clusters`** command, see Figure 43.

Figure 43: ESS Cluster information

```
status ess clusters

Cluster ID   1             ESS CLUSTER INFORMATION

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

     1        y         2        y       23:30 3/19/2009   R015x.02.0.947.1
    13     unknown               n
```

Note:

The ESS software version will not appear until the ESS 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 44.

Figure 44: survivable Processor screen

```
display survivable-processor sv-ess13                          Page   1 of   4
                    SURVIVABLE PROCESSOR

Type: simplex-ess      Cluster ID: 13    Processor Ethernet Network Region: 1
                        Community: 20        Enable PE for H.323 Endpoints? n
                                              Enable PE for H.248 Gateways? n


SERVER A
          Server ID: 13
          Node Name: sv-ess13
         IP Address: 172.24.206.29




PORT NETWORK PARAMETERS
                  Community Size: all      System Preferred: n
                  Priority Score: 1         Local Preferred: y
                                                 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 by the 'up' in the **Port Ntwk Ste** column.

For an example of the output of the **status ess port-networks** command, see Figure 45.

Figure 45: status ess port-networks

```
status ess port-networks

Cluster ID 1             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  10  1A01 IPSI up    1A01  1A01 actv-aa    1   1
                            1B01 standby    1   1

26  10 26A01 IPSI up   26A01 26A01 actv-aa    1   1
                           26B01 standby    1   1

64  10 64A01 IPSI up   64A01 64A01 actv-aa    1   1
                           64B01 standby    1   1
```

Saving translations

Translations are saved on the main server by executing the **save translations** command. You cannot save translations on an ESS server. When logging into an ESS server you receive a message stating that this server is an ESS 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 ESS server matches the timestamp of the main server's current translations, no translation download occurs. If the timestamp of the ESS server matches the timestamp of the main server's previous copy, the main server sends only the differences to the ESS server. If the timestamp of the ESS server does not match either of the main server's copies, then the main server sends the entire translation download to the ESS server.

Translations are distributed from the main server to the ESS 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 ESS 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 ESS 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 46.

Figure 46: 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: 23 : 20
                                           Stop Time: 06 : 20
                                    Save Translation: daily
 Update LSP and ESS Servers When Saving Translations: y
                           Command Time-out (minutes):
                          Control Channel Interchange: no
                       System Clocks/IPSI Interchange: no
```

On the main server verify that the ESS server has received the translations by executing the **status ess cluster** command. The **Translations Updated** column contains the day and time (timestamp) of the last successful translation download to each ESS server. After the **save translations** command executes, 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 43.

Chapter 4: Enterprise Survivable Server Conversions

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

The conversion procedures in this chapter detail the specific steps required for the ESS 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 ESS server to main server on page 148
- Existing server to ESS server on page 152
- Manual Backup Server to ESS server on page 163

Important:

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

Important:

Communication Manager Release 5.x and later is not supported on S8700 Servers and S8500A servers.

Note:

The ESS server to Manual Backup Server conversion is not supported.

Basic guidelines for conversions

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

- For any conversion, the ESS should always be addressed before the main server. When an ESS server is not controlling a port network, it can be converted without disrupting service.
- If possible, disconnect ESS servers from the LAN/WAN until the main server is operational. Then connect the ESS 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, ESS server to main server, or main server to ESS 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.
- Each main server and ESS server requires a unique IPSI serial number in order to generate a license file in RFA. This means that you cannot have more servers requiring licenses (i.e. main server plus all ESS servers) than there are physical IPSI circuit packs in the system. With high availability (duplex IPSI) systems both active and standby IPSI serial numbers may be used to generate individual license files.
- All conversion options, including the main server (non ESS server to main server, ESS server to main server, and main server to ESS server) is service affecting. When port networks are controlled by a new server (main server or ESS 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 ESS feature. For compatibility information, see the *Minimum Firmware/Hardware Vintages* document at http://support.avaya.com .

Existing ESS server to main server

Important:

The S8700 Server and the S8500A server cannot run Communication Manager Release 5.x and later releases. You cannot convert an S8700 Server or an S8500A server from an ESS server to a main server running Communication Manager Release 5.x or later.

Note:

Manual Backup Servers and the Enterprise Survivable Server functionality can not be implemented on the same system.

Note:

Do not use this procedure to convert a Manual Backup Server to a main server. To convert a Manual Backup server to a main server, see Manual Backup Server to ESS server on page 163.

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 an ESS server exists, it may be advantageous to switch all port networks to the ESS server prior to the conversion.

Use this procedure to convert an existing ESS 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 ESS servers.

Important:

If a server is being converted to replace a previously existing main server it must be of the same server type as the original. An S8500-Series ESS server cannot be converted to a main server if the main server was an S8720.

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 Communication Manager 3.0 or later software.

   a. On the System Management Interface, click **Administration > Server (Maintenance)**.

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

      If the server is not running Communication Manager 3.0 or later software, upgrade the server. For the procedure to upgrade the server, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
5. If the server is a duplex pair (S8700-Series) busy out the standby server.
6. Execute this step for S8500-Series and S8700-Series active servers.
   From the System Management Interface, click **Installation > Configure Server**. Select the **Configure individual services** option.

   a. Choose **Set Identities**:

      - Enter a unique Server ID (SVID) in the **ID** field. A single SVID is required for a S8500-Series Server and two unique SVIDs are required for a S8700-Series Server pair. This ID must be between 1 and 99. 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. Choose **Server Role** from the left margin.

- Select **a main server.**

7. For S8700-Series 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 on page 113. 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 ESS feature. This value is set by the license file and cannot be administered in Communication Manager. Each server in a duplex pair (S8700-Series) 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.

     CAUTION:

     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 an ESS server.

   - A System ID (SID): The SID is unique to the system configuration. The main server and all ESS servers will have the same SID.
9. Configuring the server using the System Management Interface 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 S8700-Series 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 **Configure Server** 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 ESS server fails to register. For information on administering ESS, see Administering an ESS server on the main server on page 131.
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 ESS 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 ESS 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 server** 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 ESS server does not require a **reset system 4**, nor does it do one automatically.

    For more information on how to configure the server, see Configuring the main server and each ESS server on page 123.

19. Verify that each of the ESS servers and LSPs 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 ESS servers register and the their translations are updated. Periodically repeat the **status ess clusters** or **list survivable-processor** command until all ESS servers register and are updated.

    Note:

    An active main server knows its own state and that of any ESS 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 ESS 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 LSPs, and the ESS 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 ESS server

Important:

The S8700 Server and the S8500A server cannot run Communication Manager Release 5.x and later releases. You cannot convert an S8700 Server or an S8500A server to an ESS server running Communication Manager Release 5.x or later. An ESS server must run the same or an earlier release than that of the main server.

Note:

Manual Backup Servers and the Enterprise Survivable Server functionality can not be implemented on the same system.

Note:

Do not use this procedure to convert a Manual Backup Server to an ESS server. For the procedure to convert a Manual Backup Server, see Manual Backup Server to ESS server on page 163.

This procedure is used when you have an existing server that you are converting to an ESS server. For example, when an existing S8700 Server pair is being replaced by an S8710 Server pair, the S8700 Servers could be converted to an ESS server.

Use the following steps to convert an existing server to an ESS 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 Communication Manager 3.0 or later software.

   a. On the System Management Interface, click **Administration > Server (Maintenance)**.

      If the server is not running Communication Manager 3.0 or later software, upgrade the server. For the procedure to upgrade the server, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
5. If the server is a duplex pair (S8700-Series), busy out the standby server.
6. Execute this step for S8500-Series and S8700-Series active servers:
   Run the **Configure Server** command from the System Management Interface. Select the **Configure Individual Services** method.

   a. Choose **Set Identities**:

      - Enter a unique Server ID (SVID) in the **ID** field. A single SVID is required for a S8500-Series Server and two unique SVIDs are required for a S8700-Series Server pair. This ID must be between 1 and 99. 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. Choose **Configure ESS** from the left margin.

   c. Enter the IP address of a C-LAN or Processor Ethernet that is controlled by the main server and the IP address for each of the main server (or main servers, if duplicated).
7. For the S8700-Series Servers, perform the same configuration activities as step 6 for the standby server.
8. Install a new license file with the appropriate settings for an ESS server. For more information on ESS license files, see License files on page 113. This license file should probably 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 ***y***
- **ESS Administration** set to ***Y***
- A Module ID (MID) greater than 1: A MID is also referred to as the Cluster ID (CLID) by the ESS feature. This value is set by the license file and cannot be administered in Communication Manager. Each server in a duplex pair (S8700-Series) will have the same CLID.

  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.

Note:

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 an ESS server.

- A System ID (SID): The SID is unique to the system configuration. The main server and all ESS servers will have the same SID.

9. Configuring the server via the System Management Interface 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 S8700-Series 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 file sync 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, 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.
10. Verify that the main server has the latest translations available.
11. Translate the new ESS server on the main server: From the main server execute the command. For more information on administering the ESS, see Administering an ESS server on the main server on page 131.

12. Connect the new ESS server to the LAN/WAN.
13. Verify that the ESS servers register with the main server and that the translations are updated on the ESS server.
    a. Use the **status ess clusters** command to verify that the main (this server) is shown and that all the ESS servers register and translations are updated. Periodically repeat the **status ess clusters** command until all the ESS servers are registered and updated.

    Note:

    A active main server knows its own state and that of any ESS 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 ESS servers.
14. To synchronize translations between the main server, the LSPs, and the ESS server, execute **save translation all** on the main server.

Existing S8400 main server to S8400 ESS server

You can migrate from a S8400 main server-based system to an IP-connected port network controlled by an S8500 or S8700-Series Server with S8400 as an ESS server, as follows:

Task	Information	Documentation
General preparation		
1. Save existing translations from the existing S8400 main server.	Backup the translations on the S8400 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. The translations on the existing main S8400 Server would not be used after it is converted to an ESS server, but they would be used if it is again configured as a main server. You *can* also backup the existing S8500 or S8700-Series Server.	For information on running the **save translations** command, see Saving translations on page 144.
		1 of 9

Task	Information	Documentation
2. Note all administered data that will be needed.	Design the system and determine the ESS administration factors to support the port network on the new S8500 or S8700-Series system. Additional C-LANs might be required for IP endpoint registration purposes. You can administer only the **Priority** for an S8400 ESS server because the other factors default to local only. You might need to make factor changes to the existing non-S8400 ESS clusters to allow for the new S8400 ESS server to be added to the IPSI priority cluster lists.	For information on how to design and plan the system, see ESS Design and Planning on page 61.
New S8500 or S8700-Series Main network		
3. Disconnect the new S8500 or S8700-Series main server from the network.		
		2 of 9

Task	Information	Documentation
4. Upgrade the new S8500 or S8700-Series main server.	Upgrade the main server to Communication Manager 5.2 or later. A main server should *never* run a release of Communication Manager that is later than that of the ESS server. If the existing server is running a Communication Manager release prior to 5.2, upgrade to Communication Manager 5.2 using the standard procedures. If the existing server is a main server with a manual backup server (MBS), do not upgrade to Communication Manager 5.2 or later. Instead, remaster the server using Communication Manager 5.2 or later software. If the existing server was used as an MBS, do not upgrade to Communication Manager 5.2 or later. Instead, remaster the server using Communication Manager 5.2 or later software.	To use the standard process to upgrade the main server to Communication Manager 5.2 or later, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
5. Configure the main server.	The server's System Management Interface is used to configure the main server.	To configure a server for ESS that is already running Communication Manager 5.2 or later, see Configuring the Servers on page 120. To configure the server using the Avaya wizard, see *Installing and Configuring the Avaya S8400 Server* (03-300678).
		3 of 9

Task	Information	Documentation
6. install the RFA license and authentication file.	A new license for the main server (with ESS Administration feature enabled) is required. A new license is required if the server upgrade was from one major release to another. If required, load the RFA license and authentication file. Ensure that you are *not* loading the license file of an ESS server on the main server by checking the MID associated with the license file. The MID appears in the license file name after the letter m. Example: If you did *not* rename the license files, and the main server license file name is s66579v5m1-060214-20295.lic, the MID would be 1. If the ESS license file is s66579v5m2-060214-19431.lic, the MID would be 2. 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 an ESS server. Verify that the ESS administration feature is turned on.	To install the license and authentication file see *Installing and Configuring the Avaya S8400 Server* (03-300678). To verify that the ESS Administration feature is turned on, see Administering ESS on page 130.
7. Copy the translations from the S8400 Server to be converted to this new main server.	Run the **`save translations all`** or **`save translations ess`** command.	For more information on the **`save translations`** command, see Saving translations on page 144.
		4 of 9

Task	Information	Documentation
8. Restart the main server.	After loading the license file, restart the server using the following Linux commands: **`? stop -af or stop -caf`** **`? start -a or start -ca`** **Warning:** Do *not* connect this server to the network *before* you disconnect the S8400 to be converted from the network, because two main servers must *not* be connected to the LAN/WAN at the same time.	
9. Install an IPSI circuit pack on the S8400 to be converted.	Remove the existing TN8412 Server IP Interface (SIPI) circuit pack and replace it with a TN2312BP IP Server Interface (IPSI) or later.	For instructions, see *Adding New Hardware for Avaya Servers and Gateways* (03-300684).
10. Turn off power to the S8400 server.	Disconnect the server to be converted from the LAN/WAN.	
11. Turn on power to the S8500 or S8700-Series main server.		
12. Verify that the new S8500 or S8700-Series main server is running correctly and in control of the network.		To verify that the ESS Administration feature is turned on, see Administering ESS on page 130.
S8400 ESS server		
13. Disconnect the S8400 from the network.		
14. Turn on power to the S8400 server.		
		5 of 9

Task	Information	Documentation
15. As a safety measure, remove the translations from this server to prevent interference with the new main server.		
16. If required, obtain a carrier for the TN8400BP circuit pack.	A TN8400BP circuit pack can be installed only in a G650, G600, or CMC1 Media Gateway.	For instructions, see *Adding New Hardware for Avaya Servers and Gateways* (03-300684).
17. Install a circuit pack in the network.	Do one of the following: ● Replace the TN8400AP circuit pack with a TN8400BP circuit pack. ● Upgrade the TN8400AP circuit pack using the upgrade kit (memory and SSD) In both cases, use the same slot that was originally used for the TN8400AP circuit pack. Usually, this is slot 1 or 2, depending on the carrier. Disconnect the Ethernet cable that connects the backplane I/O adapter of the TN8400 circuit pack to the TN8412AP Server IP Interface (SIPI) circuit pack. Connect the backplane I/O adapter of the TN8400 circuit pack to the network that leads to the new S8500 or S8700-Series Server.	
18. If H.248 gateways are to be supported by the ESS server, install a TN799 C-LAN circuit pack, if required.	The endpoints and H.248 gateways (if any) require a C-LAN or Processor Ethernet interface that they can register to.	For instructions, see *Adding New Hardware for Avaya Servers and Gateways* (03-300684).
		6 of 9

Task	Information	Documentation
19. Upgrade each ESS server to Communication Manager 5.2 or later.	Each ESS server must be running Communication Manager 5.2 or later. Upgrade each ESS server *before* upgrading the main server. If the existing server is running a Communication Manager release prior to 5.2, upgrade using the standard procedures.	For instructions on how to upgrade a server to a Communication Manager 5.2 or later, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
20. Remaster the S8400 SSD and hard drive.	You must remaster the SSD and hard drive before configuring the S8400 Server as an ESS server.	For instructions on how to run the **`remaster`** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431). For remastering, you must have a USB CD/DVD drive attached to the S8400 Server.
21. Configure the ESS server.	Use the Avaya wizard to configure the server. • Add a new node name for the S8400 ESS server. • Add S8400 as an ESS server. • Add the TN8400 to the system. For information about administering the ESS, see Administering and saving translations on page 167.	To configure the server using the Avaya wizard, see *Installing and Configuring the Avaya S8400 Server* (03-300678).
		7 of 9

Task	Information	Documentation
22. Install the required ESS license file and restart the server.	Ensure that you are *not* loading the license file for the main server on an ESS server by checking the MID associated with the license file. The MID appears in the license file name after the letter m. Example: If you did *not* rename the license files, and the main server license file name is *s66579v5m1-060214-20295.lic*, the MID would be 1. If the ESS server license file is *s66579v5m2-060214-20295.lic*, the MID would be 2. 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 should be loaded on an ESS server. After loading the license file, stop the ESS server using the restart button on the web page or by using following Linux commands: **`? stop -af or stop -caf`** **`? start -a or start -ca`**	To install the license and authentication file, see *Installing and Configuring the Avaya S8400 Server* (03-300678).
23. Attach the S8400 ESS server to the network and verify communication with the customer's LAN interface.	Connect the backplane I/O adapter of the ESS server to the network that leads to the S8500 or S8700-Series Server. The IP address of the C-LAN that you entered when configuring the ESS server is used when the ESS server registers with the main server for the first time and it may be used for subsequent registrations. Use the following instruction to verify that the ESS server can communicate with the customer's LAN interface: • On the ESS server, use the **`ping`** command followed by the IP address of the C-LAN.	For information on how to use the **`ping`** command, see *Installing and Configuring the Avaya S8500-Series Server* (03-300143) or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
		8 of 9

Task	Information	Documentation
24. Verify the communication to the main server over the IP network.	Use the following instruction to verify that the ESS server can communicate with the customer's IP network: • On the ESS server, use the **`ping`** command followed by the IP address of the main server.	
25. Verify connectivity from the TN2312BP circuit pack to the new S8500 or S8700-Series Server		For information on how to use the **`ping`** command, see *Installing and Configuring the Avaya S8500-Series Server* (03-300143) or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
26. From the new main server, administer the endpoints, trunks, and dial plans.	All of the endpoints, trunks, and dial plans that were originally administered on the S8400 main server will have to be administered on the new S8500 or S8700-Series main server.	
		9 of 9

Manual Backup Server to ESS server

Important:

The S8700 Server and the S8500A server cannot run Communication Manager Release 5.x and later releases. You cannot convert an S8700 Server or an S8500A server to an ESS server running Communication Manager Release 5.x or later. An ESS server must run the same or an earlier release than that of the main server.

If Manual Backup Servers (MBS) are installed at some locations, they will need to be converted to ESS servers. You cannot use MBS and ESS together in the same configuration. There is only one manual backup server pair installed for each installation.

CAUTION:

Some MBS installations perform manual file transfers (ftp) between the main server and MBS servers and a manual restore to keep the MBS up-to-date. This practice must be stopped once the conversion to ESS server is completed. The synchronization of translation data for an ESS server is automatic. Manual file transfers to the ESS server will cause errors.

Use the following steps to make the conversion from a manual backup server to an ESS server. These steps are general in nature. Refer to the specific referenced documents for more detail.

1. Upgrade the existing Main S8700-Series Servers to Communication Manager 3.0 or later. See *Upgrading Software and Firmware - Avaya S8500 Server* (555-245-111), or *Upgrading Software and Firmware - Avaya S8700 Server* (555-245-115).
2. On the main server install a new license file with the appropriate settings for a main server. For more information on license files, see License files on page 113.

   The new license file should have the following attributes:

   - **Enterprise Survivable Server** set to **n**
   - **ESS Administration** set to ***y***
   - A unique Module ID (MID): The MID is referred to as the Cluster ID (CLID) by the ESS feature. The MID of a main server is always 1 (CLID 1). This value is set by the license file and cannot be administered in Communication Manager. Each server in a duplex pair (S8700/S8710) will have the same MID (CLID).

     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.

   Note:

   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 an ESS server.

   - A System ID (SID): The SID is unique to the system configuration. The main server and each ESS server will have the same SID.
3. On the main server, administer the ESS server in translations. For more information on administering an ESS, see Administering an ESS server on the main server on page 131. The **`change survivable processor`** and **`change system-parameters port-networks`** commands are used to administer the ESS server.
4. Disconnect the Manual Backup Server from the WAN/LAN.
5. Re-master the Manual Backup Server with Communication Manager 3.0 or later.

CAUTION:

This is information is very important: A Manual Backup Server must be re-mastered. ***Do not*** upgrade a Manual Backup Server. ***Do not*** reinstall the Manual Backup Server scripts or the Manual Backup Server cron tasks on the main server or the ESS server.

To re-master a MBS server running a 1.x load, use the steps outlined in *Upgrading, Migrating, and Converting Servers and Gateways* located at http:\\support.avaya.com.

To re-master a MBS server running a 2.x load, re-master using the Communication Manager CD. Refer to *Installing and Configuring the Avaya-S8700 Series Server* (03-300145), located at http:\\support.avaya.com.

6. Configure the ESS server using the System Management Interface per standard procedures. See *Installing and Configuring the Avaya S8400 Server* (03-300678)*, Installing and Configuring the Avaya S8500-Series Server* (03-300143) or *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
   The specific web pages and fields that are unique to ESS server are:
   - **Set Identities** page:

     Enter a unique Server ID (SVID) in the **ID** field. A single SVID is required for a S8500-Series Server and two unique SVID are required for a S8700-Series Server pair. This ID must be between 1 and 99.
     Gaps in the numbering are allowed (10, 20, 30,. . .) but servers may also be consecutively numbered.
   - **Configure ESS** page:

     Specify the interfaces on the main server(s) that this ESS server will use for registration and file synchronization. These will be IP address of the C-LAN or Processor Ethernet interfaces for one or more main servers.

     Select one of the following **Configure Memory** options:
     - **Standard**
     - **Extra large**
7. Install a new license file with the appropriate settings for an ESS server. For more information on license files, see License files on page 113.

   The license file should have the following attributes:
   - **Enterprise Survivable Server** set to **y**
   - **ESS Administration** set to ***y***
   - A unique Module ID (MID): The MID is referred to as the Cluster ID (CLID) by the ESS feature. The MID is set by the license file and cannot be administered in Communication Manager. Each server in a duplex pair (S8700/S8710) will have the same MID (CLID).

     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.

Note:

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 an ESS server.

- A System ID (SID): The SID is unique to the system configuration. The main server and each ESS server will have the same SID.

8. Install a new authentication file.
9. Configuring the server using the System Management Interface 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 and 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. Re-connect the new ESS server to the LAN/WAN.
11. On the main server, verify that the new ESS server registers and that translations are updated by executing the following command:

    - **`status ess clusters`**

      Periodically repeat this command until each server registers.

    Note:

    An ESS server only knows its own state. For some period of time (minutes) after an ESS server boots up and connects to the network there may be a discrepancy between the state displayed by the main server and the ESS server.

Chapter 5: Running In ESS Mode

This chapter describes various nuances that one should be aware of when an ESS 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 ESS 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 an ESS server if the ESS server is registered with the main server. The ESS server registers with the main server through a C-LAN circuit pack or through Processor Ethernet. Translations can be administered on an ESS server but they cannot be saved.

To determine when the last translation download from the main server to the ESS server occurred, type **status ess clusters** from the server's SAT. Check the **Translations Updated** (timestamp) column associated with the cluster ID of the ESS server (Figure 47). The main server sends translations to the ESS server:

- Every time a **save translations all** or **save translations ess** command is executed.
- During routine maintenance, if the 'Update LSP and ESS servers when saving translations' option is checked.

Figure 47: Status ess clusters

```
status ess clusters

Cluster ID  1          ESS CLUSTER INFORMATION

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

   1        y          1         y        23:31 3/24/2009   R015x.02.0.947.1
  10        y         91         y        23:31 3/24/2009   R015x.02.0.947.1
  20        y         97         y        23:31 3/24/2009   R015x.02.0.947.1
  30        y         96         y        23:31 3/24/2009   R015x.02.0.947.1
  40        y         95         y        23:31 3/24/2009   R015x.02.0.947.1
  50        y         94         y        23:31 3/24/2009   R015x.02.0.947.1
```

User Enabled telephone features

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

When an ESS 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 an ESS 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 minor alarm for every ATM Expansion Interface board that is no longer communicating with the main server.
- A minor alarm for every CSS Expansion Interface board that is no longer communicating with the main server.
- A platform alarm if the main server failed because of a hardware issue.

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

An ESS server alarms when it can no longer communicate with an IPSI unless the ESS server was rejected by the IPSI.

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

- A major alarm is generated when the ESS 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 ESS server enters into a License-Error mode. An ESS server runs in License-Error mode until it no longer controls a port network or until the 30 day timer expires and it enters into a No-License mode.
- An alarm is generated when the ESS server enters into No-License mode.
- An alarm is generated when the ESS 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 ESS 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 ESS 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 ESS server. For more information on the **`get forced-takeover ipserver-interface`** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431).

CAUTION:

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

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

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

  This command may be executed from either a main server or an ESS server. An ESS 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, Media 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 only there is only one ESS server in the configuration. In this case, disabling the main server would cause a system outage if the ESS server fails or if communication between the ESS server and the port networks was lost.

Unplanned failover to another ESS server

A system that failed over to a single ESS server could experience unwanted fragmentation if the IPSI can no longer communicate with the main server but can communicate with multiple ESS servers. For example, due to a temporary network outage one or more IPSIs in a configuration can no longer communicate with the controlling ESS 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 ESS 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 ESS server than the rest of the port networks.

If the failover to another ESS server causes unwanted fragmentation, the **`get forced-takeover ipserver-interface`** command can be used to pull the port networks back to the previous ESS server. For more information on the **`get forcd-takeover ipserver-interface`** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media 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 ESS server. Verify the software version on the Web interface of the ESS 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 ESS 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 ESS server while the ESS server is controlling one or more port networks. The translations are received by the ESS server but are not loaded as long as the ESS server controls a port network. Once the ESS server no longer controls a port network, the ESS server resets and loads the new translations.

Chapter 6: Troubleshooting

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

- The layout and topology of the network
- Where ESS 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 ESS 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 ESS translations:

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

  The ESS servers can be on a later release than the main server but the main server should never be on a later release than the ESS servers. The software release should only be different when upgrades are being performed. Always upgrade the ESS servers first and then the main server.
- The **`status ess port-networks`** command displays which Cluster ID is controlling each port network and which ESS server the port networks (IPSIs) have on their priority lists.

The following System Management Interface commands can be used to verify the ESS configuration:

- **Configure Server > Configure ESS** specifies whether the server is a main server or an ESS server. If it is an ESS server specify an address for a C-LAN or Processor Ethernet and the main server.
- **Configure Server > Set Identities** sets the Server IDs of the individual servers.

Registration

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

ESS server is not registered with the main server

An ESS server registers with the main server. Under normal conditions an ESS server may not register with the main server if the ESS server is resetting. The ESS 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, Media Gateways and Servers* (03-300431) for errors related to ESS registration. Error 257 should be logged when an ESS server is administered on the main server but is not registered.

On the main server, use the following list of commands to troubleshoot an ESS server that is not registering with the main server:

1. Use the **`display survivable-processor essName`** to verify that the ESS server is properly administered. An ESS 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 ESS server. Where, **`<location>`** is the location of the C-LAN circuit pack the ESS server is trying to use to register with and ***`nnn.nnn.nnn.nnn`*** is the IP address of the ESS server.
3. Use the **`display events`** command with a **category** of **denial** to display the denial events related to ESS. The ESS registration denial events are in the 36xx range. See *Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300430) for descriptions of the ESS denial events.
4. Use the **`list trace ras ip-address`** command to monitor registration requests from the ESS server. This command displays registration requests from the ESS server and the associated response from the main server.

   Note:

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

From the ESS 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 **Configure Server** page to avoid a reboot of the ESS server. Do not Update the system.

1. Use the Linux **ping *nnn.nnn.nnn.nnn*** command to verify connectivity between the ESS server and main servers. Where ***nnn.nnn.nnn.nnn*** is the IP address of the C-LAN in the main server that the ESS server is trying to register with. To determine which IP address the ESS server is attempting to register with use the **Configure Server** command from the System Management Interface on the ESS server to display the **Configure ESS** page.
2. Firewalls or other security measures may preclude the main server and ESS server from communicating. Verify that the following ports are open:
   - Port 1719 Registration between the ESS server and the main server.
   - Port 21874 Filesync (rsync) is open between the main server and ESS server.
3. Use the **Configure Server** pages of the System Management Interface to verify the following:
   - On the **Set Identities** 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 99. 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 ESS server, requires a unique SVID.
   - On the **Configure ESS** page, verify that the correct platform type (8700-Series or 8500-Series) is selected and the correct C-LAN or Processor Ethernet and main server's IP addresses are entered. The ESS 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 **Set Identities** page of the Configure Server 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 ESS server. The translation file is only sent after the ESS 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 an ESS 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 ESS servers. For an example, see Figure 48.

Figure 48: Troubleshooting - display survivable processor example

```
display survivable-processor sv-ess13                          Page   1 of   4
                    SURVIVABLE PROCESSOR

Type: simplex-ess      Cluster ID: 13    Processor Ethernet Network Region: 1
                        Community: 20        Enable PE for H.323 Endpoints? n
                                              Enable PE for H.248 Gateways? n


SERVER A
          Server ID: 13
          Node Name: sv-ess13
         IP Address: 172.24.206.29




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

From the ESS server that is to be monitored, use the System Management Interface and the **Configure Server** command to display the **Configure ESS** page. Note the IP Address that is configured as the main server's primary address. For an example, see Figure 49.

Figure 49: Troubleshooting - Configure ESS example

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 ESS server (135.9.78.143) was entered.

   The first message exchange is from the ESS server sending a Registration Request (RRQ) to the main server. The main server responds with a Registration Confirmation (RCF). The ESS server and main server continue a conversation where the ESS 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 50.

Figure 50: 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 ESS 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 ESS 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 51).

Figure 51: 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 ESS server is incorrectly administered on the main server. In this example, the ESS server is configured to have Server ID 98 using **Configure Identities** on the **Configure Server** page. However, the ESS 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 52 displays using the **list trace ras** command.

Figure 52: 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 ESS server attempts to register. Denial events are displayed using the **display events** command. Briefly, the denial events associated with ESS server are:

- 3600: IP RRJ-ESS not admin: The ESS server attempting to register does not match any of the administered ESS 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 ESS 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 ESS server, the server displays the data as shown in Figure 53.

Figure 53: 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 ESS 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 ESS 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, Media Gateways and Servers* (03-300431) for errors related to ESS server socket connections to IPSIs. Error 513 should be logged if a socket connection can not be established between an enabled ESS 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 ESS server that is not connecting, initiate a **PING** to the administered IPSIs to verify connectivity between the ESS 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 ESS servers a port network (IPSI) is connected to. This command may be executed at either a main server or an ESS 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 54 shows an example of an IPSI (the standby IPSI in PN 2) that does not have a connection established with the server.

Figure 54: status ess port-networks example

```
status ess port-networks

Cluster ID 1             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  1B01 IPSI up    1B01  1AXX standby  1   1   44  64  13  9   200 100 500
                            1B01 actv-aa  1   1   44  64  13  9   200 100 500

 2   1  2AXX IPSI up    2AXX  2AXX actv-aa  1   1   44  64  13  9   200 100 500
                            2B01 standby  *   *   44  64  13  9   200 100 500

 3   2  3AXX IPSI up    3AXX  3AXX actv-aa  1   1   44  64  13  100 500 850 9
                            3B01 standby  1   1   44  64  13  100 500 850 9

 4   2  4A01 IPSI up    4A01  4A01 actv-aa  1   1   44  64  13   100 500 850 9
                            4B01 standby  1   1   44  64  13  100 500 850 9

 5   1  5A01 EI   up    3AXX
```

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: Enterprise Survivable Server Acceptance Testing

Acceptance testing is used to test the design and administration of the ESS configuration. To check the ESS 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 ESS server

CAUTION:

This test is service affecting. When an ESS 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 an ESS 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 ESS server that is being tested. The ESS server must be connected to the port networks identified in step 1. To verify that the ESS server is connected to the port network(s), execute a **status ess port-networks** command from either the main server or the ESS server. The CLID of the ESS server must appear in the list of connected 'Clusters IDs' for the port networks.
3. On the ESS server, execute the **get forced-takeover ipserver-interface N** command (where N is the number of the first port network).
4. On the ESS server, repeat the **get forced-takeover ipserver-inerface 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 ESS server.
- The restart may take several minutes.

Acceptance criteria

Check that the selected port networks are under the control of the ESS 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 ESS 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 ESS 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 ESS server. Perform the following steps to execute this test:

1. Verify that the ESS 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 ESS server loses control of all port networks under its control as the port networks restart.
- Communication Manager 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 ESS 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 an ESS server from the main server

Use this procedure to test the ability to disable an ESS 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 an ESS server that is controlling an IPSI. For more information on the **`disable ess cluster`** command, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers,* 03-300431.

What to expect

You can expect the following events to occur:

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

Acceptance criteria

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

1. On the main server:
   a. After the ESS 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 ESS 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 an ESS server from the main server

Use this procedure to test the ability to enable an ESS 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 ESS server being tested.
- Once the ESS server resets it re-registers with the main server.
- The ESS server receives a translation download from the main server and resets again.
- After the reset, the ESS server re-registers with the main server.

Acceptance criteria

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

1. On the main server:
   a. After the ESS 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 ESS server:
   a. Execute the **`status ess clusters`** command. Verify that:
      - The enabled state under the **Enabled?** column shows **y**

Glossary

A

ATM Asynchronous Transfer Mode. An industry standard for moving data. In an ESS environment, ATM refers to the scheme used to connect port networks together.

C

CLID Cluster Identification number. In an ESS 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. The MID/CLID is set by the RFA license file and cannot be changed.

Cluster A cluster is a server or set of servers which share a call state. The cluster can be the singular case (S8500-Series Servers) or the duplex case (S8700-Series Servers). This definition implies that a server within a cluster can be interchanged if it is duplicated.

Community A virtual group consisting of one ESS and one or more port networks.

E

ESS Enterprise Survivable Servers: The Avaya option that provides survivability by allowing backup servers to be placed in various locations in the customer's network.

ESS The server that are ready to respond to an IPSI's request for service if all other recovery mechanisms fail. The ESS may be simplex (S8500-Series Servers), or duplex (S8700-Series Servers). The S8700 Server and the S8500A Server cannot run Communication Manager 5.x and later releases.

L

LSP Local Survivable Processor: An Avaya server that may accept media gateway and/or endpoint registrations incase of a server or network failure.

M

Main server The primary server that usually control the system. The main server may be simplex (S8500-Series Servers), or duplex (S8700-Series Servers). The S8700 and the S8500A server cannot run Communication Manager 5.x and later releases.

MID Module Identification number: RFA 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.The MID is assigned by RFA and cannot be changed. In an ESS 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 ESS servers with the same preference settings and ESS servers with no preference settings. For this document, the term priority value and priority score is interchangeable.

Priority score See Priority value.

R

RFA Remote Feature Activation: The web-based application used to generate license and authentication files.

S

SAP Avaya’s ordering system for products and services.

Serial numbers A serial number of the Avaya hardware is used to create a valid license file. The hardware serial number and the serial number within the license file must match.

SSO Single Sign-On: An Avaya corporate mechanism requiring a single login to allow users access to certain web sites.

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.

System Record A number used by RFA to identify the system within the RFA database.

Index

F

G

H

I

L

M

N

O

P

R

S

T

U

V