Avaya™ CMS

R3V11

High Availability Connectivity, Upgrade and Administration

585-215-514
Comcode 700203300
Issue 1.0
May 2002
Compas ID 89409

Notice

Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

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 working on your company's behalf). Be aware that there may 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 support or assistance, call Technical Service Center Toll Fraud Intervention Hotline at +1 800 643 2353.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of your company's telecommunications equipment) by some party.

Your company's “telecommunications equipment” includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, “networked equipment”).

An “outside party” is anyone who is not a corporate employee, agent, subcontractor, or working on your company's behalf. Whereas, a “malicious party” is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Your Responsibility for Your Company’s Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure your:

- Avaya-provided telecommunications systems and their interfaces
- Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Federal Communications Commission Statement

Part 15: Class A Statement. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

European Union Declaration of Conformity

Avaya Business Communications Systems declares that equipment specified in this document conforms to the referenced European Union (EU) Directives and Harmonized Standards listed below:

EMC Directive 89/336/EEC

Low Voltage Directive 73/23/EEC

CE The “CE” mark affixed to the equipment means that it conforms to the above Directives.

Trademarks

Enterprise, Solaris, SPARCserver, Sun, SunSwift, Sun Blade 100, and Ultra are trademarks or registered trademarks of Sun Microsystems, Inc.

INFORMIX is a registered trademark of Informix Software, Inc.

MultiVantage is a trademark of Avaya, Inc.

DEFINITY is a registered trademark of Avaya, Inc.

All other product names mentioned herein are the trademarks of their respective owners.

Ordering Information

Call:	US Voice:	1 800 457 1235
	US Fax:	1 800 457 1764
	non-US Voice:	+1 410 568 3680
	non-US Fax:	+1 410 891 0207

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA

Order: Document No. 585-215-514, Issue 1.0,
May 2002

You can be placed on a Standing Order list for this and other documents you may need. Standing Order will enable you to automatically receive updated versions of individual documents or document sets, billed to account information that you provide. For more information on Standing Orders, or to be put on a list to receive future issues of this document, please contact the Avaya Publications Center.

Avaya National Customer Care Center

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-242-2121.

Avaya Web Page

http://www.avaya.com

Acknowledgment

This document was written by the CRM Development group.

Avaya CMS R3V11
High Availability Connectivity, Upgrade and Administration

Contents

Introduction

Connecting HA servers to the switch

Upgrading CMS to the High Availability option

Administering the switch for CMS HA systems

Introduction

Overview

The Avaya Call Management System (CMS) High Availability (HA) option is a system of hardware and software features designed to reduce potential loss of call center data.

The CMS HA system includes features associated with the Automatic Call Distribution (ACD) feature of Avaya, Inc. DEFINITY or MultiVantage switches operating in conjunction with the CMS software application. The CMS HA system consists of the following major features:

- Dual Automatic Call Distribution (ACD) links on the switch
- A paired set of CMS servers, each separately connected to one of the dual ACD links, and through which simultaneous and identical sets of call data are received
- Separate network subnet connections for paired ACD-CMS combinations

HA system redundancy of critical hardware components greatly reduces possible data loss due to single point-of-failure sources. HA also minimizes data loss which might otherwise occur during CMS software upgrades or as a result of software/database corruption problems.

ACD data is simultaneously routed to two CMS servers through paired C-LAN circuit cards on the switch over separate TCP/IP over Ethernet subnets.

The CMS servers installed in HA systems are designated as the “primary” and “secondary” servers. The primary server is distinguished from the secondary server by the following differences:

- If the customer has a license for Internet Call Center, it is installed only on the primary server
- Most CMS administration changes are entered only on the primary server. Any changes that are made on the primary server are subsequently transferred to the secondary server by either copying a full maintenance backup or manually making the changes on the secondary server.
- If the customer has the External Call History package, it should be installed on both servers. If the customer has customized report solutions implemented by Avaya, Inc. CRM Professional Services Organization (PSO), External Call History should be active on both servers. Otherwise, it should be active on only the primary server.

Other than the configuration and operational differences listed above, the primary and secondary servers function in a highly similar manner and collect identical data streams through their respective ACD links. Should either server fail or need to be brought down for maintenance, the remaining unit is fully capable of carrying the full CMS activity load without interruption.

Supported switches

The CMS HA option is supported on the following Avaya switches:

- R8csi
- R8si
- R8r
- R9.*x*
- R10.*x*
- ProLogix R3
- R11.*x*

Supported CMS platform combinations

CMS HA is supported on the following platform combinations:

- Sun Ultra 5 - Sun Ultra 5
- Sun Enterprise 3000 - Sun Enterprise 3000
- Sun Enterprise 3500 - Sun Enterprise 3000
- Sun Enterprise 3500 - Sun Enterprise 3500
- Sun Blade 100 - Sun Ultra 5
- Sun Blade 100 - Sun Blade 100

Note:

Use the following recommendations for HA configurations with different Sun platforms:

- For HA configurations in which Enterprise 3000 and 3500 servers are combined, the 3500 server should be designated as the primary HA server.

- For HA configurations in which Ultra 5 and Ultra 5 Einstein servers are combined, the Einstein server should be designated as the primary server.
- For HA configurations in which Sun Blade 100 and Ultra 5 servers are combined, the Sun Blade 100 server should be designated as the primary server.

Required and optional software

A complete set of CMS R3V11 software package CDs (with the exceptions listed below) is provided for the second server at no additional charge.

For primary and secondary servers deployed in HA systems, the following exceptions to the standard CMS R3V11 software configurations apply:

- X.25 software is not supported as the final connection link between the switch and the HA servers (X.25 can be used to connect remote switches to an on site switch).
- Internet Call Center is never installed on the secondary server.
- If one or more network terminal servers are linked to the primary server and NTS installation is required for the secondary server, then the Bay Networks Annex R10.0B software package provided for the primary server can also be installed on the secondary server.
- If the optional INFORMIX® ISQL software package is installed on the primary server, a second licensed copy of the software must also be purchased by the customer for use on the secondary server.
- If the optional Openlink Open Database Connectivity (ODBC) software package is installed on the primary server, a second licensed copy of the software must also be purchased by the customer for use on the secondary server.

Special upgrade considerations

When an installed CMS HA system is subject to a software upgrade (or when one of the servers is restored to service after a system failure), the alternate server continues to collect data without interruption. Since manual synchronization between the primary and secondary servers is a key maintenance objective for HA systems, CMS upgrades should proceed in a manner that restores synchronization of the servers with the least time and effort, while minimizing data loss as much as possible.

If the CMS server has any custom features, such as Custom Reporting, custom interfaces, LAN printers, token ring, and so forth, PSO must be contacted before the upgrade process is initiated.

For further details of the CMS upgrade process, see Chapter 3, Upgrading CMS to the High Availability option on page 25.

General roles and responsibilities

This document is written for Avaya, Inc. on-site technicians, Technical Service Center (TSC) personnel, software specialists, and customer administrators. The following table lists the major tasks for each switch type, the location of the procedure in the book, and who is responsible for performing each task.

Chapter	Task	Technician	TSC	Software Specialist	Customer
2	Connecting the switch	X			
3	Administering CMS			X	X
4	Administering the switch			X	X
N/A	Troubleshooting switch connections	X	X		

For information about troubleshooting switch connections, see *Call Management Systems Switch Connections and Administration,* 585-215-876.

Customer-specific roles and responsibilities

Customers are solely responsible for several tasks required to support the CMS HA option. The following table lists tasks for which the customer is solely responsible.

Task
Retention of CMS documentation and software
For those administration changes that are non-transferable via backup tape, revision on each HA server
Nightly full maintenance backups on the primary server
Nightly full maintenance restores on the secondary server
Monthly (or more frequent) CMSADM backups
Checking log records to verify success of backup

Reasons for re-issue

This is the first issue of this document.

Avaya CMS helplines

⚠ **Important:**

Inform support personnel that your CMS system is configured for the High Availability service option.

If a problem arises that requires assistance, use the support information and help lines presented below.

Frequently asked questions (FAQs)

For answers to common problems, CMS customers and Avaya technicians can access the CMS technical support FAQ at:

http://www.avaya.com

Click on **Support**, then **Call Center/CRM Solutions**, then **CentreVu Call Management System**, and then **FAQ**.

Please check this information before you call in a trouble ticket. It could save you time and money.

Customer support for the United States

Customers can report problems and generate trouble tickets by calling:

1-800-242-2121

The customer is prompted to identify the type of problem (that is, Automatic Call Distribution, hardware, or Avaya CMS) and is connected to the appropriate service organization.

Technician support for the United States

Avaya technicians can receive help by calling:

1-800-248-1234

Customer and technician support outside the United States

For customer and technician support outside the United States, see the Avaya web site:

http://www.avaya.com

Click on **Support**, then click on **Escalation Lists US and International**. For escalation telephone numbers outside the United States, click on **Global Escalation List**.

Connecting HA servers to the switch

Overview

Connecting HA servers to the switch describes connectivity requirements and recommendations specific to CMS High Availability (HA) systems. For more information on supported switches, see, Supported switches on page 8.

The connectivity configurations described in this chapter represent the optimal link setups for HA systems. Other switch-to-server connectivity configurations are not described. For information about other switch-to-server connections, see *Call Management System Switch Connections and Administration,* 585-215-876.

Server switch-over options

The primary purpose of the CMS High Availability offer is to ensure an uninterrupted data stream between the switch and the CMS system on which the data is stored. Some customers may also desire continuous access to their CMS data. Following a major failure event on their primary HA server, customers have the option to switch over to their secondary server for purposes of CMS data monitoring and reporting. A server switch-over should be performed only when the anticipated down time for the primary server is expected to be significant.

Customers must choose between the following switch-over options:

1. **No switch-over**

   Customers who do not require continuous access to their CMS data can choose not to switch over to the secondary server after the primary server experiences a major failure event. When the primary server goes down, uninterrupted collection of call data continues on the secondary server, but the customer is not able to access that data until the primary server is restored.

2. **Manual server switch-overs**

   If uninterrupted access to CMS data is desired, a manual server switch-over must be performed. At a minimum, manual switch-over entails re-administration of CMS Supervisor clients by their individual users in order to redirect the Supervisor clients from the primary to secondary server.

   Depending on the nature of the customer network, additional measures may be required, such as re-administration or addition of NTS servers, physical reconnection of peripheral devices, and so forth. Customers considering the manual switch-over option should consult with their TSO and/or PSO representatives in order to discuss logistical issues associated with manual server switch-overs.

Basic configuration rules

CMS HA servers do not have to be physically located in the same building, or even in the same city.

CMS HA computers can collect data from up to eight different ACDs. Mixed ACD links, in which the server is connected to both single ACD links and HA dual links, is not supported. Mixed ACD links could potentially result in significant call data loss and fill system error logs with meaningless data.

Link connections are implemented only by the TCP/IP over ethernet LAN communications protocol. Connections must run over LAN facilities local to the switch.

Each CMS HA server should be connected to a separate UPS on a separate protected power circuit.

ACD traffic is routed through dual control C-LAN circuit packs on the switch. The switch must be administered to enable the dual C-LAN cards; for details about the administration of dual ACD links on HA systems, see Administering the switch for CMS HA systems on page 61.

Finally, note that the parts requirements and physical connection schemes described in this chapter are applicable to each switch-to-server link installed on the HA system, regardless of the total number of links connected to the server.

Connecting blocks

In this chapter, references are made to 103A connecting blocks, which have one RJ45 connector per block. If needed, you can substitute the 104A connecting block, which has two RJ45 connectors per block. The wiring for both connecting blocks are identical.

Planning for LAN switch links

When setting up a switch link over a LAN, information must be gathered before you begin. In particular, you must take into account whether the LAN connection includes both a connection to CMS and to Intuity™ AUDIX® with Message Manager. You must coordinate the setup of the Intuity system with the switch and the CMS. Some of the required information includes the following:

- How is the connection being made from the CMS computer to the switch?

  a. Private LAN, no connectivity to customer LAN (uses private LAN addresses)

     — Preferred option, most robust and reliable, no dependency on customer's network.

     — A secondary, dedicated LAN port on the CMS computer provides the switch link; the primary LAN port is used for other purposes (printers, terminals, Avaya CMS Supervisor, Intuity Message Manager).

     — If desired, a second C-LAN circuit pack can be used to provide additional isolation for the CMS link.

     — Crossover cable (with flipped transmit/receive leads) is used so a hub is not required.

     — Hub can be used instead of crossover cable to extend distances.

  b. Customer LAN with private segment

     — Uses a network switch or router to provide a private network or network segment

     — Minimal dependency on customer's network

     — A secondary, dedicated LAN port on the CMS computer provides the switch link; the primary LAN port is used for other purposes (printers, terminals, Avaya CMS Supervisor)

     — Customer must provide equipment and administer network for private segment

     — Customer LAN administrator must be present during setup.

  c. Direct connect to Customer LAN, without private segment

     — Least preferred option

     — Complete dependency on performance and reliability of customer's LAN

     — Allows remote location of endpoints when customer LAN connectivity is convenient

     — Customer LAN administrator must be present during setup

- If option b or c is chosen, the following information is needed from the customer:
  1. Customer network physical connectivity:
     - — Location of 10BaseT network access point (hub, router, and so on)
     - — Distance between C-LAN and network access point (328 ft, 100 m maximum)
     - — Wiring to access point, existing or new (Category 5 minimum required)
  2. Customer network administration:
     - — IP address of C-LANs, CMS computer, Intuity, and gateways
     - — Node names of C-LANs, CMS computer, Intuity, and gateways
     - — Subnet masks for all LAN segments containing C-LANs or adjuncts
     - — Gateway IP address for all LAN segments containing C-LANs, adjuncts, or routers
     - — Are all endpoints (C-LANs and adjuncts) on the same local LAN segment?
     - — Network routes
     - — Network administration information needs to be mapped into specific administration fields.
- Sanity check of information obtained from customer:
  1. If C-LAN and adjuncts (CMS or Intuity) are on the same LAN segment:
     - — Gateway IP address (if present) and subnet mask information is valid
     - — All IP addresses contain the same subnet address
  2. If C-LAN and adjuncts are on different LAN segments, gateway IP addresses are different

Without the above information the technician may not be able to complete the installation. Installations that require the technicians to return because information was not available incur additional charges.

Connecting to the switch

Overview

The recommended link setup for HA systems consists of a private LAN connection between switch and server, with no connectivity to other customer LAN segments. This arrangement optimizes performance of ACD traffic over the link and eliminates potential points of failure extraneous to the needs of switch-to-server communication. However, this configuration may not be feasible for some CMS customers who adopt the HA option.

LAN connectivity options

There are two basic ways to make the LAN connection between the switch and the server:

- Connecting with a 10Base-T hub and cables

  The recommended method to connect the switch-to-server link uses a 10Base-T hub and unshielded twisted pair UTP Category 5 cabling to directly connect switch and server over a private LAN.

- Connecting with a crossover cable

  Direct switch-to-server connectivity can be accomplished using a crossover cable with flipped transmit/receive leads. Although this method has the advantage of ensuring that the LAN connection is private, because a hub is not included in the configuration, it is not recommended for HA systems.

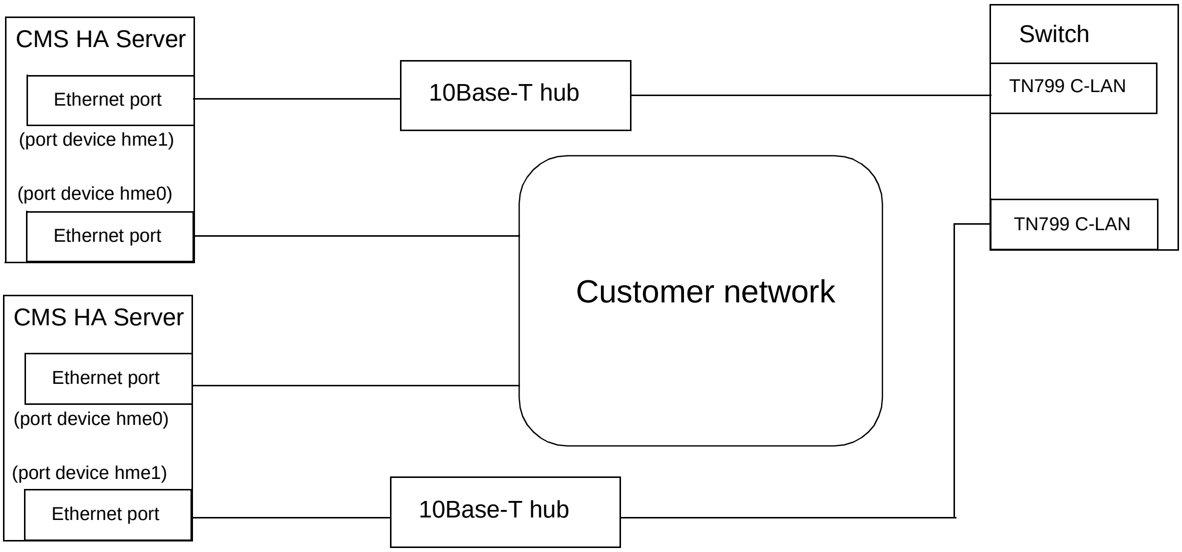
If the customer requires a link connection by means of crossover cables or other methods not described above, general descriptions and requirements for alternate connectivity setups are described in *Call Management System Switch Connection and Administration,* 585-215-876.

Ethernet ports on a CMS server

Ideally, a second ethernet card should be installed on each CMS HA server. If two ethernet ports are available, the standard provisioning procedure is to use the first (built-in) ethernet port for connectivity to the customer LAN or public network. The second ethernet card (Fast-SCSI Buffered Ethernet (FSBE) or SunSwift™ ethernet) should be dedicated solely to the switch link.

A depiction of an ideal HA system configuration for a single-ACD system is displayed in the following figure.

Local switch configuration diagram



Note:

Existing customer network configurations are likely to require a LAN setup that is different from the idealized configuration shown above, especially when multiple ACDs are connected to the CMS server. For information about alternate LAN configurations, see *Call Management System Switch Connections and Administration,* 585-215-876.

Connecting with a 10Base-T hub

Connecting through a 10Base-T hub LAN connection is the recommended method for connecting the switch to the CMS computer.

Hubs used to connect servers to multiple dual link ACDs must have sufficient ports for all of the incoming ACD links as well as the connection from the hub to the HA server. Thus, an 8-port hub supports a maximum of seven ACDs. If eight ACDs links are required or planned, use a 16-port hub to make the connection to the switch.

Distance limits

The maximum allowable length for a single segment of Cat 5 cable is 100 meters (328 feet). A maximum of four hubs can be used in series to connect cable segments; so, the distance between a local switch and server must not exceed a maximum distance of 500 meters (1,640 feet).

However, when multiple ACDs are in use, few, if any, switches are likely to be installed in the same physical location as the CMS servers. In most cases, connections to the switches (both local and remote) are made through a private network maintained by the customer.

Parts list

The following parts list includes the basic hardware required to connect each dual ACD link to a CMS HA server according to the recommended connectivity configuration. For multiple dual link connections, greater quantities of some components may be required.

Quantity (per CMS server)	Description	Comcode[1]
1	TN799 C-LAN port	N/A
1	259A adapter, or 258B adapter, or 356A adapter, or Category 5 cross-connect hardware and connecting block	102631413 103923025 104158829 N/A
2	RJ45 UTP Category 5 modular cord: 5 feet, 1.5 meters 10 feet, 3 meters 15 feet, 4.5 meters 25 feet, 7.6 meters 50 feet, 15.2 meters 100 feet, 30.5 meters 200 feet, 61 meters 300 feet, 91 meters	 107748063 107748105 107748188 107742322 107742330 107748238 107748246 107748253
1	CenterCOM 10Base-T LAN hub	407086735

[1] Parts for which no comcode is displayed must be obtained by the customer prior to the scheduled upgrade.

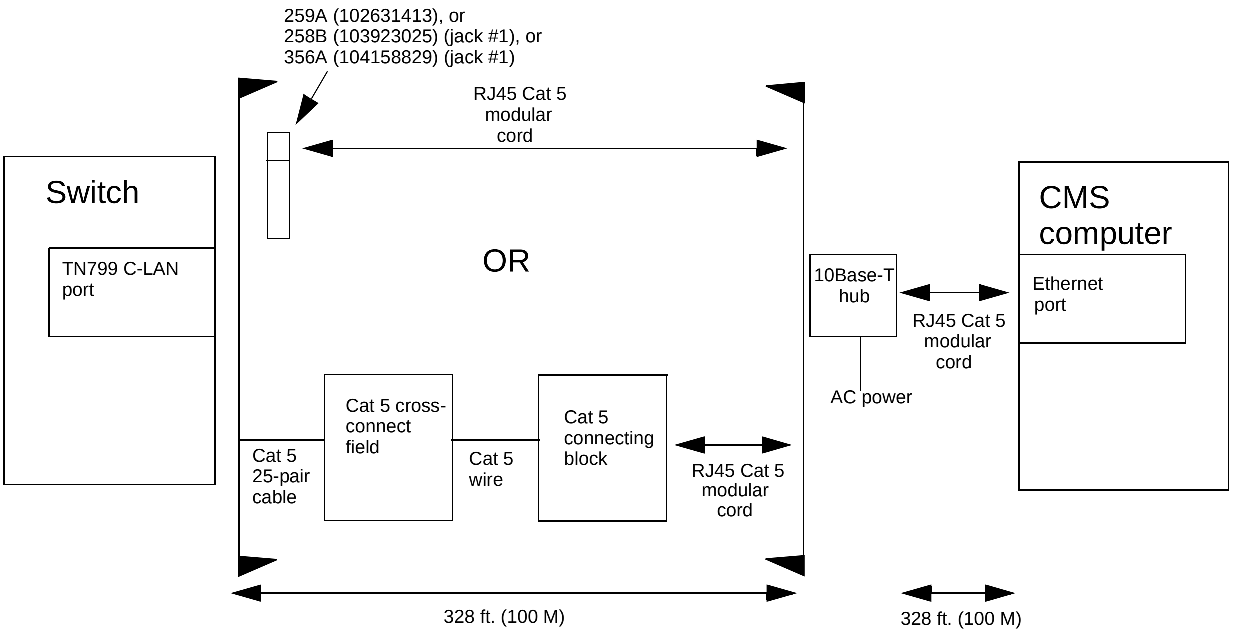
Setting up the cabling

You must set up the cabling to make the connection between a dual ACD link and the HA server. For more information, see the Cabling diagram - LAN via 10Base-T hub on page 23.

To set up the cabling:

1. Do one of the following:
   - Attach an adapter (259A, 258B, or 356A) to the backplane connector of the TN799 C-LAN circuit pack, then attach one end of an RJ45 Category 5 modular cord to the adapter. Use jack #1 on the 258B or 356A adapters.
   - Connect the ethernet port of a TN799 C-LAN circuit pack to a Category 5 connecting block using Category 5 cross-connect wiring; then attach one end of an RJ45 Category 5 modular cord to the connecting block.
2. Connect the other end of the modular cord to a port on the 10Base-T hub.
3. Connect another RJ45 Category 5 modular cord to a different port on the 10Base-T hub.
4. Connect the other end of the modular cord to an ethernet port on the CMS computer.
5. Connect and apply power to the 10Base-T hub.

Cabling diagram - LAN via 10Base-T hub



Upgrading CMS to the High Availability option

Overview

Upgrading CMS to the High Availability option describes Avaya Call Management System (CMS) upgrade procedures used to combine a new CMS server with an existing CMS system in order to create a CMS High Availability (HA) system.

The CMS servers used in an HA system must have the same CMS version and base load number. If the original server has a different CMS version from the new server being added to the system, upgrade of the original server must be performed by means of a Avaya CMS Upgrade Express (CUE) upgrade.

HA upgrade scenarios

Two CMS servers to be incorporated into an HA system must have the same CMS version and base load number for the CMS software. In many the new HA systems will consist of an existing CMS installation combined with a newly purchased CMS server.

Note:

In the procedures that follow, the two CMS servers incorporated into the system are referred to as follows:

- The CMS server that is already installed on site is referred to as the “original server”
- The server purchased by the customer to enable the HA option is referred to as the “new HA server”.

In terms of the installed CMS software, one of the following conditions will be true at the beginning of the upgrade:

1. The CMS servers have the same CMS version and base load
2. The original server has the same CMS version as the version installed on the new HA server, but the base loads are different
3. The original server has an earlier version of CMS than the version installed on the new HA server

If conditions 1 or 2 are in effect, the upgrade process is significantly simplified, since:

- The switch can be administered for the correct CMS version and the dual ACD links prior to the arrival of the new HA server on site (the unused C-LAN link is busied out until the new HA server is installed)
- The original server either does not require a software upgrade or needs only a base load upgrade to match the installation on the new HA server.

In either case, when a new HA server is added to a system in which the original server is already installed with the correct CMS version, achievement of a synchronized system requires minimal or no software installation, followed by one or two maintenance backups and restores between the two servers. The servers are never truly synchronized because of operational differences between the primary and secondary servers.

When an original server is already installed with the correct CMS version, logistics associated with creation of a new HA system are greatly simplified. Therefore, this document describes only that upgrade scenario in which a full CMS version upgrade is required.

In contrast, when the original server is installed with a pre-R3V11 version of the CMS software, the HA upgrade process entails a specific sequence of installation and administration activities, as well as various maintenance backups, data migrations, and data restores. These activities must be executed in an ordered sequence intended to minimize system downtime and overall provisioning effort. The procedures required to perform an HA upgrade under this scenario are presented in the following sections.

Overview of the HA upgrade process

The steps required to perform an HA upgrade when the original server requires a full CMS version upgrade, are summarized below and depicted in the Schematic depiction of the HA Upgrade procedure when a full CMS version upgrade is required: on page 29.

To upgrade HA:

> ⚠ **Important:**
>
> Steps 1 through 4 below should be performed approximately 24 hours before the HA upgrade process is initiated.

1. Upgrade the switches to Release 8.1 or later and administer the switches to run with the current (pre-R3V11) version of CMS installed on the original server.
2. Since backup tapes will be exchanged between the two servers, verify that the tape drive on the original server is compatible with the tape drive on the new HA server.

   Example:

   If a Sun Enterprise 3500 server is purchased for incorporation with an existing Enterprise 3000 server, the tape drive on the 3000 system must be replaced with a new DDS-4 tape drive. *Old tapes should be discarded so that they are not mistakenly used in the new tape drive.*

   Note:

   If replacement of the tape drive on the original server is required, Provisioning will dispatch a Sun technician. If the call center operates on a 24/7 basis, this activity will incur some loss of CMS data.

3. Coordinate with the customer to:

   a. Determine which CMS server will be designated as the primary server and which will be designated as the secondary server (for details, see Supported CMS platform combinations on page 8)

   b. Establish a cut-off time on the day of the HA upgrade, after which CMS users will not make changes to the system administration until the upgrade is complete.

4. Perform a CMS full maintenance backup and a CMSADM backup on the original server approximately 24 hours before the HA upgrade begins.
5. On the day of the upgrade, the Avaya technician arrives on site and performs a backup of system and ACD-specific admin data on the original server.

   Note:

   At this point in the upgrade process, CMS users must not attempt to make administrative changes on the system until the HA upgrade is completed.

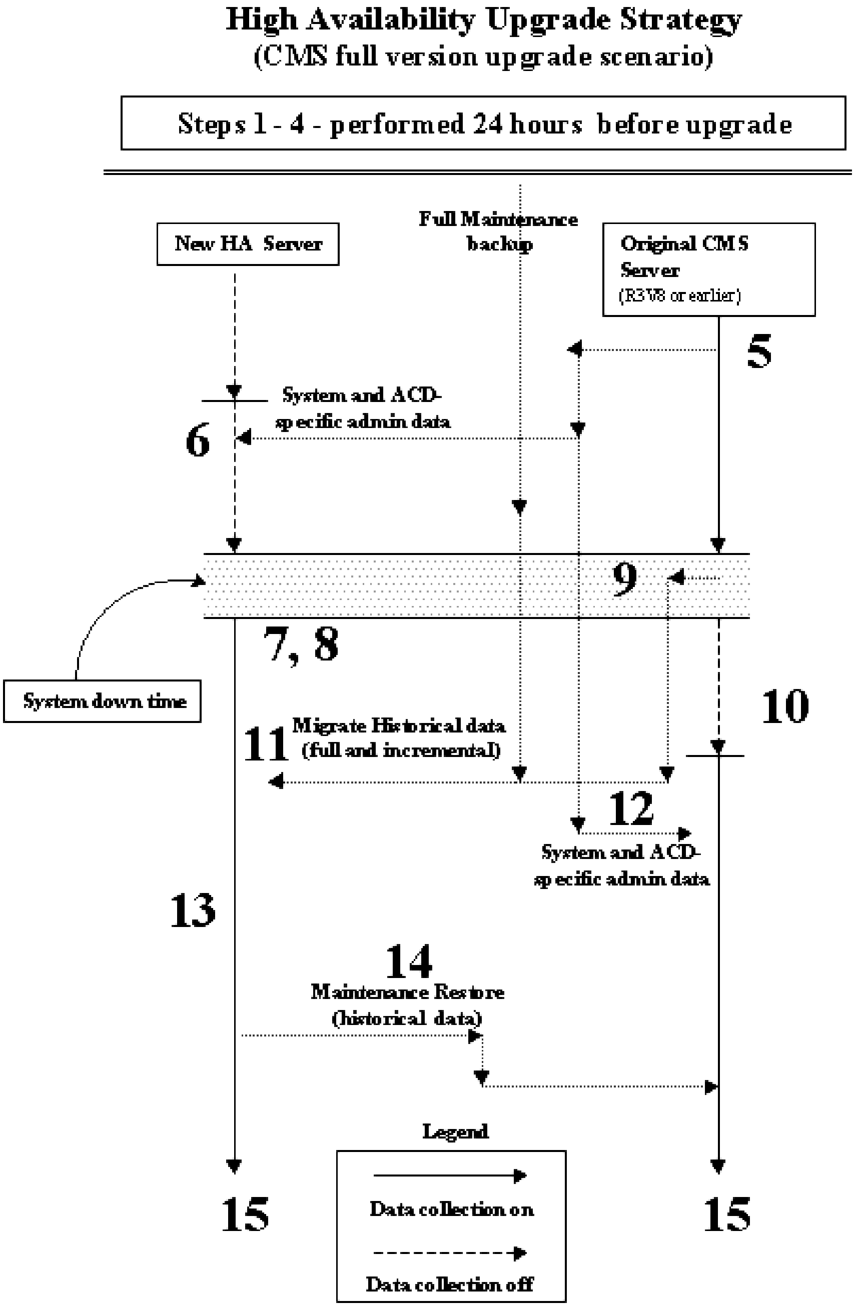
6. The technician installs and configures the new HA server. The technician puts CMS into single user mode and the backup tape (created in Step 5) is used to migrate the system administration data and agent/call center admin data onto the new HA server.
7. After the most recent intrahour interval archive completes on the original server, busy out all ACD links at their respective switches and re-administer them for CMS R3V11 and dual ACD links. When the switches are re-administered, release the busy out for the links.
8. As soon as the switch is re-administered and the ACD links for the new HA server come up, verify that CMS data collection on the new HA server is active for all ACDs.
9. Perform an incremental maintenance backup on the original server (historical data only), then power it down. Do all other required pre-upgrade procedures which are necessary prior to starting the Avaya CMS Upgrade Express (CUE) upgrade. Refer to the platform-specific instruction booklet included in the CUE upgrade kit. Then perform the rest of the CUE upgrade.
10. After the CUE upgrade is complete and the new CMS software has been set up, restart CMS data collection on the original server. Verify that data is collected from all ACDs.
11. Migrate the CMS historical data from the incremental maintenance backup (Step 9) to the new HA server. When the migration completes, replace the incremental tape with the original full maintenance tape (Step 4) and migrate all of the remaining historical data to the new HA server.
12. Use the CMS system administration and ACD-specific admin data backup tape (Step 5) to migrate that data back onto the newly upgraded original CMS server.
13. Run a full maintenance backup on the new HA server.
14. Restore the historical data from the full maintenance backup tape (created in the preceding step) onto the original server.

    The two servers now share the same initial set of administrative data. *CMS users can now resume or begin making administrative changes to whichever CMS system is designated as the primary server.*
15. Run CMSADM backups on both servers.

The CMS HA upgrade process is now complete. Customers should initiate a regular maintenance schedule.

For more information, see *Avaya CMS R3V11 High Availability User Guide,* 585-215-714.

Schematic depiction of the HA Upgrade procedure when a full CMS version upgrade is required:


High Availability Upgrade Strategy
(CMS full version upgrade scenario)
Steps 1 - 4 - performed 24 hours before upgrade
New HA Server
Full Maintenance backup
Original CMS Server (R3V8 or earlier)
5
6
System and ACD-specific admin data
9
7, 8
System down time
10
11
Migrate Historical data (full and incremental)
12
System and ACD-specific admin data
13
14
Maintenance Restore (historical data)
15
15
Legend
Data collection on
Data collection off

Verifying the tape drive on the server currently in service

This procedure is required only for HA systems when:

- An E3000 server, currently in service and equipped with a 14-GB tape drive, is combined with a new E3500 platform equipped with a Mammoth drive
- An E3500 server, currently in service and equipped with a Mammoth tape drive, is combined with a new E3500 platform equipped with a DDS-4 drive
- An Ultra 5 server, currently in service and equipped with an SLR5 tape drive, is combined with a new Ultra 5 equipped with a DDS-4 drive
- An Ultra 5 server, currently in service and equipped with an SLR5 tape drive, is combined with a new Sun Blade 100 equipped with a DDS-4 drive

Note:

New systems are currently offered with the DDS-4 tape drive; the Mammoth tape drive has been discontinued, but is shown here to support existing systems. If a new system with a DDS-4 tape drive is combined with an existing system with a Mammoth tape drive, you will need to replace the Mammoth tape drive with a DDS-4 tape drive.

For HA systems in which a new Enterprise 3500 platform is installed in combination with an Enterprise 3000 that is already in service, the tape drive on the 3000 must be replaced with a DDS-4 drive.

For HA systems in which a new Enterprise 3500 platform is installed in combination with an existing Enterprise 3500 that is equipped with a Mammoth tape drive, the tape drive on the existing 3500 must be replaced by a new DDS-4 drive

For Ultra 5 - Ultra 5 or Ultra 5 - Sun Blade 100 combinations in which a new platform is installed in combination with an older Ultra 5 that is equipped with an original SLR5 tape drive, the SLR5 drive must be replaced with a new DDS-4 drive.

The tape drive replacement, which is performed by a Sun technician, must be completed before the HA upgrade process is initiated.

⚠ **WARNING:**

After the original tape drive on an Enterprise 3000 has been replaced, the customer must discard any old tapes which were previously in use with the old drive. *Re-use of old tapes on the replacement drive will damage the tape device.*

Verifying the Mammoth tape drive

New systems are currently offered with the DDS-4 tape drive; the Mammoth tape drive was discontinued, but is shown here to support existing systems.

If replacement of the tape device is required for an existing Enterprise 3000 system prior to beginning an upgrade to the High Availability option, use this procedure to confirm that the old tape drive is replaced by a new Mammoth drive:

1. Insert an 8mm 170m AME tape cartridge in the tape drive and enter:

   `mt -f /dev/rmt/0 status`

   If the drive has been replaced, the system responds:

```
Mammoth EXB-8900 8mm Helical Scan tape drive:
   sense key(0x0)= No Additional Sense   residual= 0   retries= 0
   file no= 0   block no= 0
```

Verifying the DDS-4 Ultra 5 tape drive

If replacement of the tape device is required for an existing Ultra 5 system prior to beginning an upgrade to the High Availability option, use this procedure to confirm that the old tape drive has been replaced by a new DDS-4 drive:

1. Insert a 150mm 20GB DAT cartridge in the tape drive and enter:

   `mt -f /dev/rmt/0 status`

   If the drive has been replaced, the system responds:

```
Vendor ’HP   ’ Product ’C5683A   ’ tape drive:

sense key(0x0)= No Additional Sense
residual= 0  retries= 0  file no= 0  block no= 0
```

Verifying a DDS-4 E3500 tape drive

If replacement of the tape device is required for an existing E3500 system prior to beginning an upgrade to the High Availability option, use this procedure to confirm that the old tape drive has been replaced by a new DDS-4 drive:

1. Obtain a 150mm 20GB DAT cartridge, verify that it fits correctly in the E3500 tape drive, and insert it into the drive.
2. Enter:

   `mt -f /dev/rmt/0 status`

   If the drive has been replaced, the system responds:

```
Vendor ’HP   ’ Product ’C5683A   ’ tape drive:

sense key(0x0)= No Additional Sense
residual= 0  retries= 0  file no= 0  block no= 0
```

Performing a CMSADM backup

A CMSADM file system backup saves all system files (excluding CMS call data) and is used to restore the system in the event of an upgrade failure. A CMS ADM backup must be performed within 24 hours of the start of the HA upgrade process. CMSADM backups must also be performed on both servers immediately after the completion of the HA upgrade.

Overview

The CMSADM file system backup includes the following:

- Solaris system files and programs
- CMS programs
- Non-CMS customer data placed on the computer (in addition to the CMS data).

Prerequisites

- Verify that at least three tapes are available for use during the upgrade process.
- Before starting the backup procedures described in this section, log in as root, and enter **`lp /etc/vfstab`**. The output from the printer is necessary when doing a system restore. Bundle the printout of the **/etc/vfstab** file with the system backup tapes for future reference.

  Note:

  The CMS server must be administered to support a printer before the **vfstab** file can be printed out.

Procedure

To perform a CMSADM backup:

1. Log in as **root** and enter:

   `cmsadm`

   The **Avaya Call Management System Administration Menu** is displayed:

2. Enter the number associated with the `backup` option.

3. Depending on the configuration of your system, go to a or b, below.
   a. If only one tape drive is available on the system, the program responds:

```
Please insert the first cartridge tape into <device name>.
Press ENTER when ready or Del to quit:^?
```

   b. If more than one tape drive is available for use by the system, the program will display output similar to the following example:

```
Select the tape drive:
  1) Exabyte EXB-8900 8mm Helical Scan tape drive: /dev/rmt/0
  2) Exabyte EXB-8500 8mm Helical Scan tape drive: /dev/rmt/1
Enter choice (1-2):
```

4. Enter a tape drive selection from the displayed list. The program displays:

```
Please insert the first cartridge tape into <device name>.
Press ENTER when ready or Del to quit:^?
```

Note:

If only one tape drive is available, the output shown above is not displayed.

5. Press **Enter**.

   The backup process begins. If more than one tape is required, the program displays the following message:

```
End of medium on "output".
Please remove the current tape, number it, insert tape number x, and
press Enter
```

   If you see the message displayed above, insert the next tape and allow it to rewind. When it is properly positioned, press **Enter**.

6. When the backup is complete, the program response varies according to the number of tapes used for the backup:

- If the number of tapes required is one, the system responds:

```
xxxxxxx blocks
Tape Verification
xxxxxxx blocks
WARNING:  A CMS Full Maintenance Backup in addition to this cmsadm
backup must be done to have a complete backup of the system.  . . . .

Please label the backup tape(s) with the date and the current CMS
version (r3vXxx.x)
```

- If the number of tapes required is more than one, the system responds:

```
xxxxxxx blocks
Tape Verification
Insert the first tape
Press Return to proceed :
```

If you see the second message, insert the first tape used in the backup and press **Enter**. Wait for the tape drive light-emitting diode (LED) to stop blinking before you remove the tape.

When prompted, repeat this process for any additional tapes generated by the backup process. When the final tape is verified, the program displays the output shown above in Step 6.

7. Save the tapes and the *vfstab* printout until a backup restore is performed.

CAUTION:

Label all tapes with the tape number and the date of the backup. Set the tape write-protect switch to read-only.

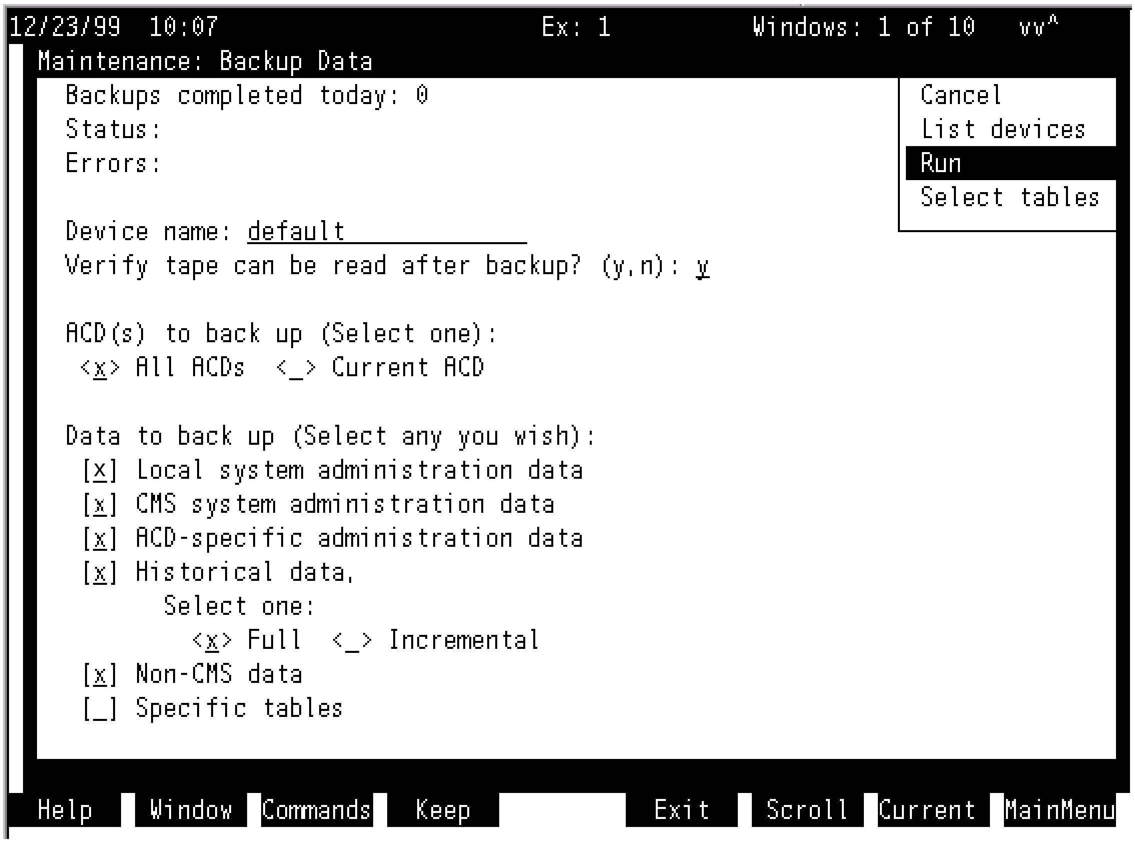
Performing a full maintenance backup

Before an existing CMS server is incorporated into a new HA system, the customer must perform a CMS full maintenance backup within 24 hours of starting the HA upgrade process.

To perform a full maintenance backup:

1. Log in as a CMS user and select **Maintenance** > **Back Up Data** option from the main menu.

   The **Back Up Data** window is displayed.



```
12/23/99  10:07                      Ex: 1          Windows: 1 of 10   vv^
  Maintenance: Backup Data
    Backups completed today: 0                                   Cancel
    Status:                                                      List devices
    Errors:                                                      Run
                                                                 Select tables
    Device name: default____________
    Verify tape can be read after backup? (y,n): y

    ACD(s) to back up (Select one):
     <x> All ACDs  <_> Current ACD

    Data to back up (Select any you wish):
     [x] Local system administration data
     [x] CMS system administration data
     [x] ACD-specific administration data
     [x] Historical data,
           Select one:
             <x> Full  <_> Incremental
     [x] Non-CMS data
     [_] Specific tables

  Help   Window  Commands   Keep          Exit   Scroll  Current  MainMenu
```

2. To accept the default backup options, press **Enter** to activate the action list in the upper right corner of the window.
3. Select the `Run` option and press **Enter**.

Performing a maintenance backup (administration data only)

When the CMS technician arrives on site, the technician performs an initial maintenance backup on the original server. This backup should include only CMS system administration data, ACD-specific admin data, and non-CMS data.

Note:

Once this backup is started, CMS users must not make any new administrative changes to the system until the upgrade process is finished.

Procedure

To perform a maintenance backup of the administration data:

1. From the CMS main menu, select **Maintenance** > **Back Up Data**.

   The **Back Up Data** window is displayed.

2. Select the following data backup options:

   - CMS System Administration data
   - ACD-specific admin data
   - Non-CMS data

   Exclude **Historical data** from this backup

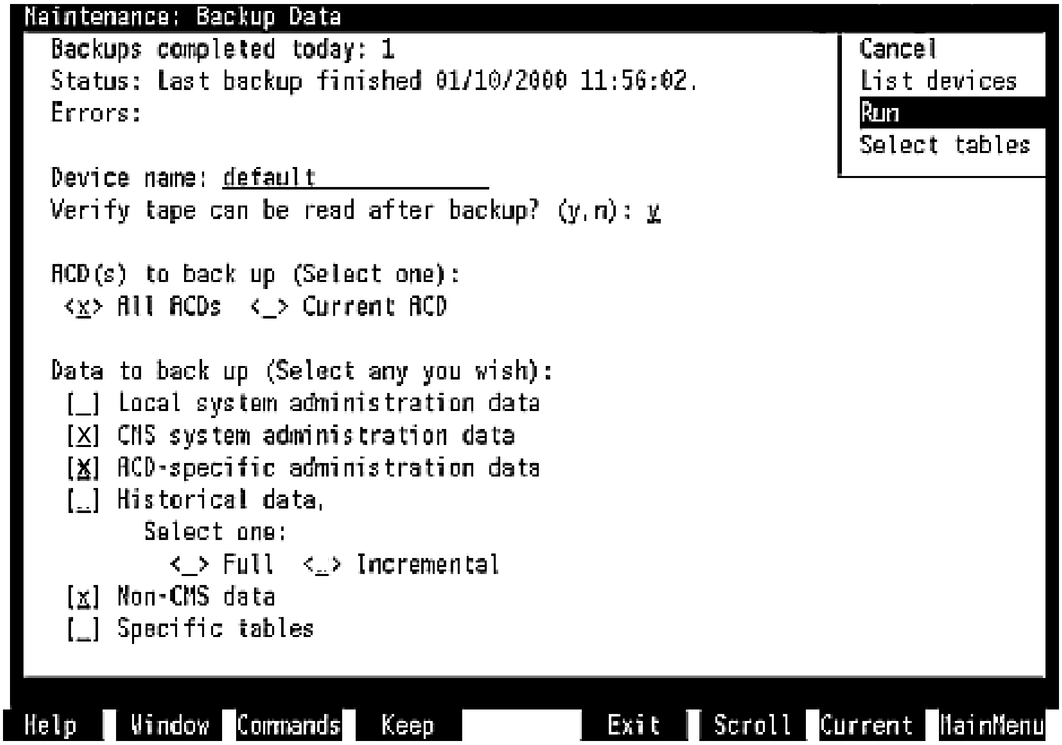
3. Press **Enter** to move the active cursor to the action list in the upper right corner of the window.

4. Select **Run** and press **Enter**.

⚠ **CAUTION:**

> The HA upgrade entails the use of multiple backup tapes. Be careful to label these tapes appropriately; use of the wrong tape during a migration or restore may result in failure to achieve an initial state of synchronization between the two HA servers.

The correct backup option selections are shown in the following example:



```
Maintenance: Backup Data
  Backups completed today: 1
  Status: Last backup finished 01/10/2000 11:56:02.
  Errors:

  Device name: default
  Verify tape can be read after backup? (y,n): y

  ACD(s) to back up (Select one):
   <x> All ACDs  <_> Current ACD

  Data to back up (Select any you wish):
   [_] Local system administration data
   [X] CMS system administration data
   [X] ACD-specific administration data
   [_] Historical data,
          Select one:
            <_> Full  <_> Incremental
   [x] Non-CMS data
   [_] Specific tables
```

After you have selected the appropriate options for the backup, press **Enter** to activate the action list in the upper right corner of the window. Move the cursor to the **Run** option and press **Enter** to start the backup.

5. To verify that the backup completed without errors:

   a. Open a terminal window and enter:

      `cms/bin/br_check`

      The system responds:

```
Enter device type [q for qtape, f for floppy]:
```

b. Enter: **q**

The system responds:

```
Enter device path:
```

c. Enter the device path for the tape drive.

Example:

```
/dev/rmt/0c
```

The system displays a list of ACD(s) backed up on the volume and prompts:

```
Enter l to list the tables or v to also verify the volume:
```

d. Enter: **l**

The system displays a list of the database tables included on the backup.

Setting up CMS on an HA server

Overview

Setting up CMS on an HA server refers to procedures which apply to both the new HA server and the original server (after it has undergone a CUE upgrade).

TSC personnel verify authorizations, set up data storage parameters, and set up the CMS application remotely. On-site technicians should call the TSC to coordinate this process.

Most of the procedures listed in this section refer to the following document:

Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide, 585-215-115.

Verify that this document is available before beginning these procedures.

Note:

Although this section repeatedly refers to the above-referenced document for descriptions of the actual procedures, some of the procedure listings provided below contain information that is specific to HA systems. Therefore, each of the procedures below should be reviewed for HA-specific information before you refer to the associated procedures described in the CMS software installation maintenance and troubleshooting document.

Prerequisites

The TSC should verify that the on-site technicians have:

- Connected the console to the CMS computer.
- Connected the CMS computer to the TSC Remote Maintenance Center (remote console).
- Connected additional terminals and printers to the NTS ports.
- Connected the link between the CMS computer and the switch.

Note:

If the hardware link or the Automatic Call Distribution (ACD) feature and CMS are not properly administered, the CMS software cannot communicate with the switch. For switch administration procedures, see Administering the switch for CMS HA systems on page 61**.**

- Connected the NTS and the CMS computer to the network hub unit. For more information, see:
  - *Call Management System Sun Enterprise 3000 and SPARCserver Computers Hardware Maintenance and Troubleshooting*, 585-214-016
  - *CMS Sun Enterprise 3500 Computer Hardware Installation Maintenance and Troubleshooting*, 585-215-873
  - *CMS Sun Ultra 5 Computer Hardware Installation Maintenance and Troubleshooting*, 585-215-871

Setting CMS authorizations

Before setting up CMS, TSC personnel need to set authorizations for CMS features purchased by the customer. Authorizations apply to all administered ACDs.

For the procedure used to set up CMS authorizations, see "Setting up CMS authorizations" in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Setting up data storage parameters

Overview

TSC personnel modify specific data storage parameters on the CMS computer so that the CMS application can operate properly. The **storage.def** file contains these data storage parameters, which are installed with a set of standard default values.

Review the default data storage values for each authorized ACD. The default values are found on the line immediately below each storage parameter, and many of them can be can be edited to meet the needs of individual customers. Use the values determined by the Account Executive, System Consultant, and Design Center based on the customer configuration.

Note:

For a new HA system being added to an existing CMS installation, data storage values should be identical to the values installed on the original server at the customer site.

Procedure

For the procedure used to set up data storage parameters, see "Setting up CMS data storage parameters" in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Setting up a LAN for switch connections

Overview

Setting up a LAN for switch connections contains information about setting up a LAN connection between the CMS computer and one or more HA-enabled switches. This type of connection is used only with switch Release 8.1 or later. The LAN connections described herein are based on the configuration recommended for HA systems, which includes two ethernet ports for each server and which assumes that private LAN subnets are used for the switch-to-server connections.

To set up a LAN connection to an HA-enabled switch, you must coordinate the administration done on the CMS computer with the administration done on the switch and, if required, within the customer's own data network.

Prerequisites

Before you begin this procedure:

- Verify that you are logged in as root user.
- CMS must be turned off.
- All file systems must be mounted.

Procedure

For the procedure used to set up data storage parameters, see "Setting up a LAN for switch connections" in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Setting Up the CMS application

Prerequisites

Before you begin this procedure:

- Verify that you are logged in as root user.
- CMS must be turned off.
- All file systems must be mounted.

Procedure

For the procedure used to set up data storage parameters, see “Setting up a LAN for switch connections” in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Installing feature packages

These procedures are used to install the following feature packages:

- Forecasting
- External Call History (ECH).

Running ECH in the HA environment

When a CMS customer is using ECH in an HA environment, the ECH software should be installed on both the primary and secondary servers. The recommended practice for running ECH on the HA servers depends on the customer-specific factors:

- If the customer is using ECH in support of customized reporting features implemented by the Avaya Professional Services Organization (PSO), ECH should be active on both the primary and secondary features.
- If the customer is not using ECH in support of customized reporting features implemented by PSO, the ECH software should be active on the primary server and turned off on the secondary server.

Customers can install these CMS feature packages if they have been authorized during CMS setup.

Procedure

For Feature Package installation procedures, see “Installing Feature Packages” *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Setting up the remote console

Overview

Redirecting the remote console port allows the TSC to dial in and perform remote maintenance. Remote access is required for both the primary and secondary servers.

Designating remote console ports on an HA system

Since the X.25 communications protocol is not supported on HA systems, either port can be used for the remote console. However, it is recommended that the standard provisioning conventions be used. For more information, see the following table:

Hardware platform	Port A	Port B
Sun Enterprise 3000 Sun Enterprise 3500	Remote console	Switch link (optional)
Sun Blade 100	Remote console[1]	N/A
Sun Ultra 5	Switch link (optional)	Remote console

[1] Port A is used exclusively for the remote console on a Sun Blade 100 system.

Procedure

For procedures used to administer and test the remote console port on the back of the CMS computer, see “Setting up the remote console” and “Redirecting the remote console port to the modem” in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Setting up the Alarm Origination Manager

Overview

The setup of the AOM config files is usually performed by the database group when a new system is administered for AOM. A product ID number must be obtained from the CMS database administration group. CMS technical support personnel contact the database group at 800-248-1111, ext. 07425 and provide them with the customer IL number.

If the AOM system administration information for the server is already established by the database group, and a product ID is available, the config file setup can be performed manually by provisioning personnel.

Procedure

For a description of the AOM config file set up, see “Setting up the alarm origination manager” in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Setting up the NTS

For information about setting up the NTS, see “Setting up the NTS” in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Creating an alternate boot device for mirrored systems

This procedure creates an alternate boot device. This procedure is required only for Enterprise 3000 or Enterprise 3500 platforms configured as mirrored systems.

For a description of the procedure used to create the alternate boot device, see “Creating an Alternate Boot Device for Mirrored Systems” in *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Migrating CMS system administration data to the new server

This procedure uses the maintenance backup tape which was created during the procedure described in Performing a maintenance backup (administration data only) on page 37. The backup was created on the original server in order to migrate administration data onto the new HA server.

Since the immediate objective is to bring the new HA server to an operational state as quickly as possible, CMS Historical data is not migrated onto the new HA server until later in the upgrade process.

> ⚠ **CAUTION:**
>
> The backup used in this procedure includes only CMS system administration data, ACD-specific admin data, and non-CMS data. Do not use the Full Maintenance backup tape created in Performing a full maintenance backup on page 36 for this migration.

Procedure

For all versions of CMS Release 3, migrate the system administration data via the **R3 Migrate Data** window.

> ⚠ **WARNING:**
>
> Attempting to migrate system administration data more than once may cause catastrophic errors from which recovery is difficult. Before a re-migration of system administration data can be performed, you must turn off CMS and perform a second setup of the CMS software.

To migrate CMS system administration data to the new server:

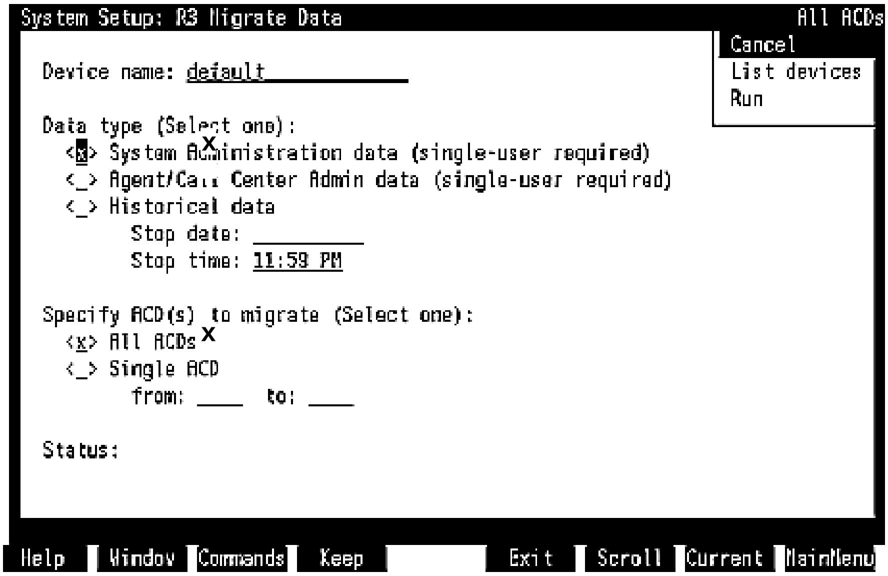
1. Log in to CMS.

   The CMS main menu is displayed.

2. From the CMS main menu, select **System Setup** > **CMS State**
3. Select **Single User Mode**.
4. Insert the backup tape that contains the latest version of the admin data into the tape drive on the new HA server.
5. Select **System Setup** > **R3 Migrate Data** from the CMS main menu.

   The **System Setup: R3 Migrate Data** window is displayed.

6. Specify **System Administration data** as the migration data types, and specify **All ACDs** for migration, as shown in the following example:



```
System Setup: R3 Migrate Data                                  All ACDs
                                                           Cancel
  Device name: default____________                         List devices
                                                           Run
  Data type (Select one):
    <x> System Administration data (single-user required)
    <_> Agent/Call Center Admin data (single-user required)
    <_> Historical data
          Stop date: ________
          Stop time: 11:59 PM

  Specify ACD(s) to migrate (Select one):
    <x> All ACDs
    <_> Single ACD
          from: ____   to: ____

  Status:

 Help  Window Commands  Keep          Exit  Scroll Current MainMenu
```

7. Press **Enter** to access the action list in the top right corner of the window.

8. Select **Run** and press **Enter**.

   The **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.

9. Repeat the procedure, this time selecting **Agent/Call Center Admin data** as the data type to be migrated.

   Again, the **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.

   Note:

   Printer administration must be done on the new HA server before Step 10 can be performed.

10. To print out the customer migration log, enter:

    `lp /cms/migrate/r3mig.log`

For help interpreting the log and its messages, U.S. customers can contact CMS technical support at 1-800-242-2121; international customers should contact their Avaya distributors or customer representatives.

The services migration log is in **/cms/maint/r3mig/mig.log**

Checking the archive interval

When you are ready to upgrade the CMS software on the original server, wait for the current archive interval to complete before busying out the link. This avoids unnecessary loss of call data.

To check the archive interval status:

1. Log in as a CMS user and select **Maintenance** from the CMS Main Menu.

   The **Maintenance** options window is displayed.

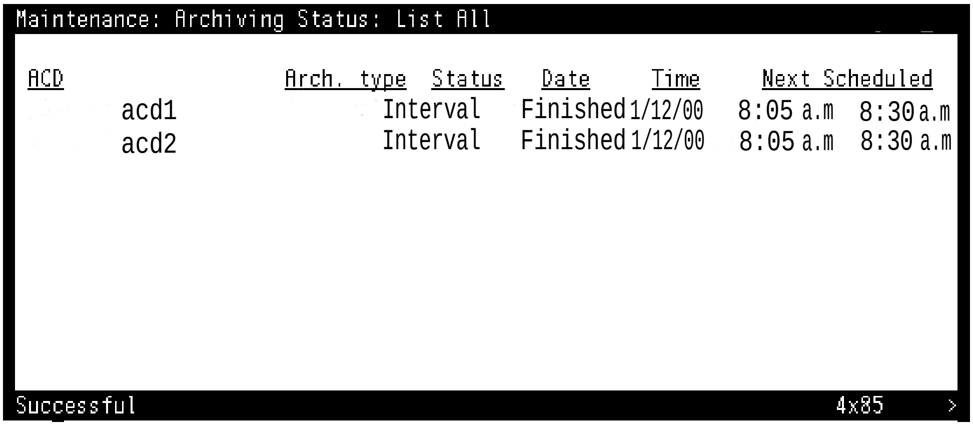
2. Cursor down to the **Archiving Status** option and press **Enter**.

   The **Maintenance: Archiving Status** window is displayed.

3. Cursor down to the **Archiving type** list and use the spacebar to deselect the **Daily, Weekly** and **Monthly** options.

4. Press **Enter** to activate the action box in the top right corner of the window; press **Enter** again to select the **List all** option.

   The **Maintenance: Archiving Status: List all** window is displayed.



```
Maintenance: Archiving Status: List All

ACD                   Arch. type  Status    Date     Time       Next Scheduled
       acd1             Interval   Finished 1/12/00  8:05 a.m   8:30 a.m
       acd2             Interval   Finished 1/12/00  8:05 a.m   8:30 a.m

Successful                                                   4x85      >
```

5. Note the figures in the **Time** column. If the elapsed time since the last archive completion is not more than a few minutes, proceed with the link busy out. If more than a few minutes has elapsed since the last archive completion, wait for the next archive interval to complete before busying out the link.

Administering the switch

After links to the original server are busied out at the switch, the switch is re-administered for the new CMS version and the HA dual C-LAN option.

For details of switch administration for HA systems, see Administering the switch for CMS HA systems on page 61.

After you have re-administered the switch, bring up the links and start data collection on the new HA server. At this point in the HA upgrade process, both CMS systems are offline and call data is not collected. Therefore, you should complete administration of the switch for the new CMS version and HA dual links, followed by startup of data collection on the new HA server, as quickly as possible.

Note:

Be sure to verify that data collection is active on all ACD links before you begin the next procedure.

The services migration log is in **/cms/maint/r3mig/mig.log** The log may contain information inappropriate for the customer.

Performing an incremental maintenance backup

Perform an incremental maintenance backup (historical data only) on the original server. Begin the server upgrade immediately after the backup is complete.

Procedure

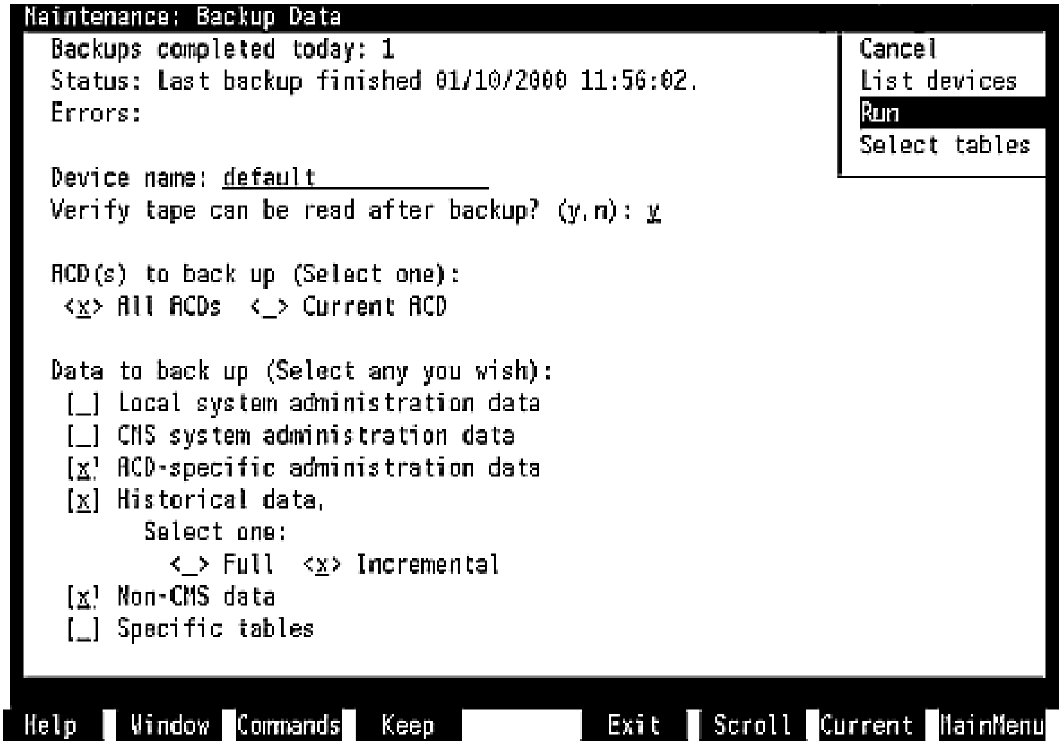
To perform an incremental maintenance backup:

1. From the CMS main menu, select the **Maintenance** > **Back Up Data**.

   The Back Up Data window is displayed.

2. Select only the **Historical data** > **incremental** data type to be copied onto the backup.

   The correct backup option selections are shown in the following example:



```
Maintenance: Backup Data
  Backups completed today: 1
  Status: Last backup finished 01/10/2000 11:56:02.
  Errors:

  Device name: default
  Verify tape can be read after backup? (y,n): y

  ACD(s) to back up (Select one):
   <x> All ACDs  <_> Current ACD

  Data to back up (Select any you wish):
   [_] Local system administration data
   [_] CMS system administration data
   [x] ACD-specific administration data
   [x] Historical data,
         Select one:
           <_> Full  <x> Incremental
   [x] Non-CMS data
   [_] Specific tables
```

3. After you have selected the appropriate options for the backup, press **Enter** to activate the action list in the upper right corner of the window. Select the **Run** option and press **Enter** to start the backup.

Upgrade the original CMS server

As soon as the incremental backup (for more information, see Performing an incremental maintenance backup on page 52) is successfully completed on the original server, the original server can be powered down, the CUE upgrade is performed, and all necessary software authorization, setup, and configuration steps are also performed. For details, see Setting up CMS on an HA server on page 40.

By the time the upgrade of the original server is complete and data collection is turned on, the new HA server should be fully operational.

The final steps in the HA upgrade process, which includes two separate data migrations, a final full maintenance backup and restore, and the creation of CMSADM backups for each of the HA servers, are described in the following procedures.

Migrating CMS historical data to the new HA server

After the switch is re-administered for the upgraded CMS version, the HA dual C-LAN option is enabled and CMS data collection is started on the new HA server, CMS historical data can be migrated to the new HA server.

Procedure

This procedure migrates CMS historical data from the second incremental maintenance backup (see Performing an incremental maintenance backup on page 52) to the new HA server.

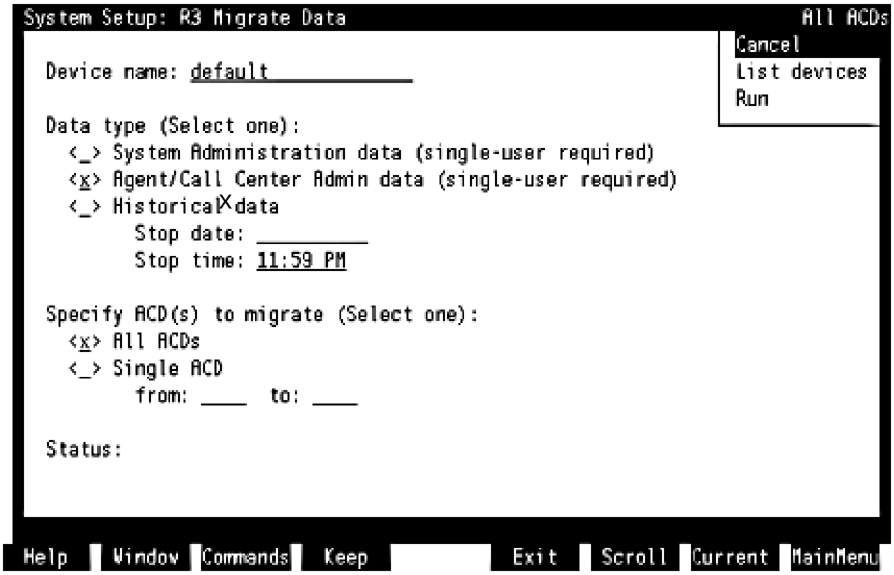
To migrate CMS historical data to the new HA server:

> ⚠ **WARNING:**
>
> Attempting to migrate CMS data more than once may cause catastrophic errors from which recovery is difficult. Before a re-migration of data can be performed, CMS must be turned off and a second setup of the CMS software must be performed.

1. Insert the incremental maintenance backup tape that contains incremental historical data into the tape drive on the new HA server.
2. Select **System Setup** > **R3 Migrate Data** from the CMS main menu.

   The **System Setup: R3 Migrate Data** window is displayed.

3. Select **Historical data** as the data type, and **specify All ACDs** for migration, as shown in the following example:



```
System Setup: R3 Migrate Data                                        All ACDs

 Device name: default

 Data type (Select one):
   <_> System Administration data (single-user required)
   <x> Agent/Call Center Admin data (single-user required)
   <_> HistoricalXdata
          Stop date:
          Stop time: 11:59 PM

 Specify ACD(s) to migrate (Select one):
   <x> All ACDs
   <_> Single ACD
          from: ____   to: ____

 Status:
```

4. Press **Enter** to activate the action list in the top right corner of the window.
5. Select **Run** and press **Enter**.
6. The **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.
7. When the migration is finished, remove the incremental tape from the drive and insert the original full maintenance backup tape (see Performing a full maintenance backup on page 36) and repeat Steps 2 through 6.

   Note:

   Printer administration must be done on the new HA server before Step 8 can be performed.

8. To print out the customer migration log, enter:

   ```
   lp /cms/migrate/r3mig.log
   ```

   For help interpreting the log and its messages, U.S. customers can contact CMS technical support at 1-800-242-2121; international customers should contact their Avaya distributors or customer representatives.

   The services migration log is found in **/cms/maint/r3mig/mig.log**

Migrating administration data back to the original server

After the original server is upgraded to the same CMS version and base load as the new HA server, the original administration data, which was copied to tape in the first maintenance backup (Performing a maintenance backup (administration data only) on page 37) is migrated back onto the system. After this procedure is performed, the two servers should share identical sets of administration data.

⚠ **WARNING:**

Attempting to migrate CMS data more than once may cause catastrophic errors from which recovery is difficult. Before a re-migration of data can be performed, you must turn off CMS and a second setup of the CMS software must be performed.

Migrate the administration data

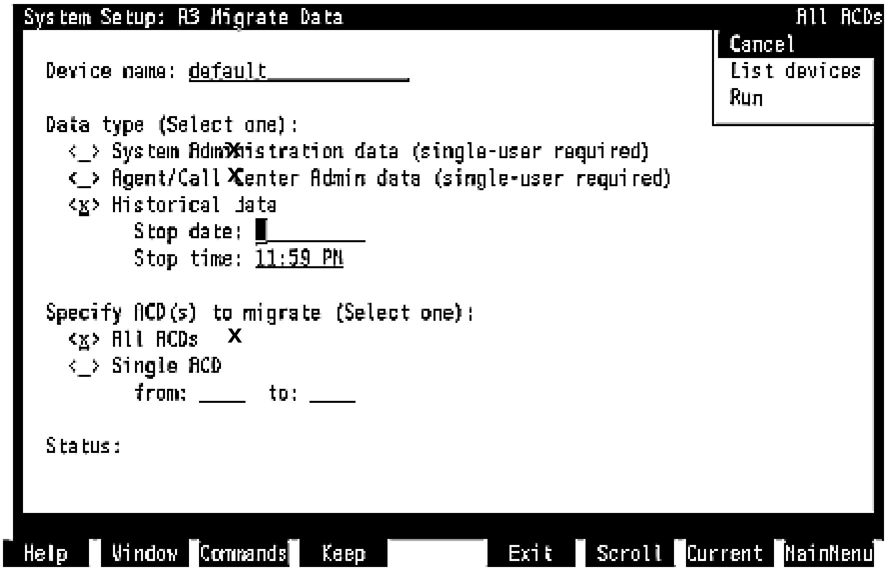
To migrate the administration data:

1. Insert the initial maintenance backup tape back into the tape drive of the original server.
2. Log in as a CMS user.

   The CMS main menu is displayed.
3. Select **System Setup** > **CMS State** from the CMS main menu and select **Single User Mode**.
4. Select **System Setup** > **R3 Migrate Data** from the CMS main menu.

   The **System Setup: R3 Migrate Data** window is displayed.

5. Select **CMS administration data** and **Agent/Call center admin data** as data types and specify **All ACDs** for migration, as shown in the following example:



```
System Setup: R3 Migrate Data                                    All ACDs

 Device name: default____________

 Data type (Select one):
   <_> System AdmXnistration data (single-user required)
   <_> Agent/Call Xenter Admin data (single-user required)
   <x> Historical data
         Stop date: █________
         Stop time: 11:59 PM

 Specify ACD(s) to migrate (Select one):
   <x> All ACDs   X
   <_> Single ACD
         from: ____   to: ____

 Status:
```

6. After you verify that the correct options are selected, press **Enter** to activate the action list in the top right corner of the window.
7. Select **Run** and press **Enter**.

   The **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.
8. Select **System Setup** > **CMS State** from the CMS main menu
9. Select **Multi User Mode**.
10. Verify that data collection is on for all ACD links.
11. To print out the customer migration log, enter:

    ```
    lp /cms/migrate/r3mig.log
    ```

    For help interpreting the log, U.S. customers can contact CMS technical support at 1-800-242-2121; international customers should contact their Avaya distributors or customer representatives.

    The services migration log is stored in **/cms/maint/r3mig/mig.log**

Performing a new full maintenance backup and restore

These procedures create a full maintenance backup on the new HA server. The backup is then used to restore CMS historical data back onto the original server.

Performing the full maintenance backup on the new HA server

The required full maintenance backup copies all system data to tape. For details, see Performing a full maintenance backup on page 36.

Note:

Assuming that the new HA server is used as the HA primary server, this backup represents the first tape to be archived for the new HA system. The other backup tapes used during the provisioning process may now be reused for nightly maintenance backups.

Restoring historical data to the original server

This procedure copies historical data from the full maintenance backup.

Procedure

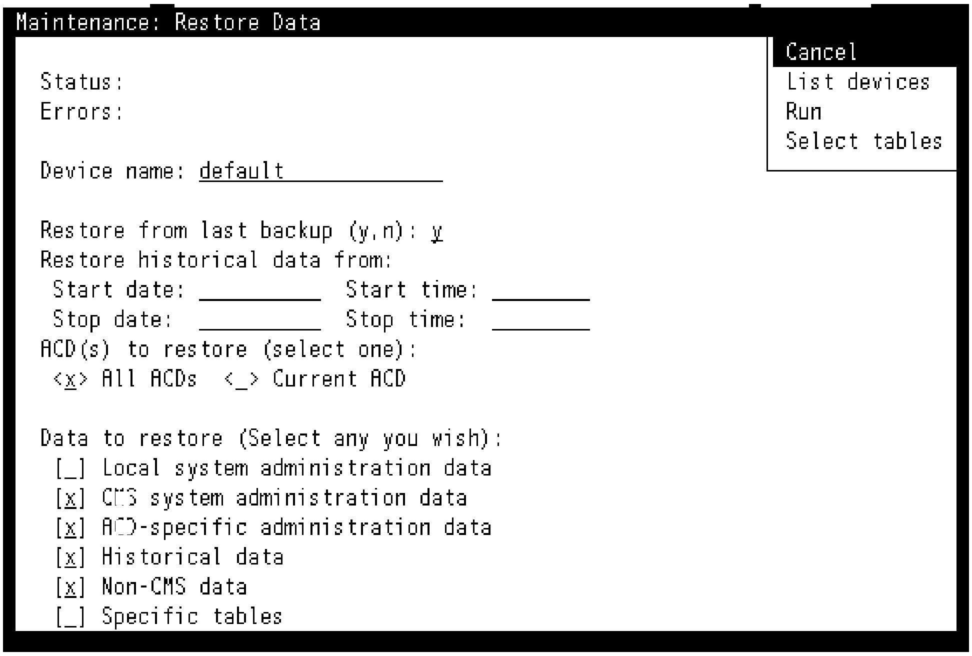
To restore data to the original server:

1. Insert the full maintenance backup tape created on the new HA server into the tape drive on the original server.
2. Log in as a CMS user.

   The **CMS Main Menu** is displayed.
3. From the main menu, select **Maintenance** > **Restore Data**.

   The **Maintenance: Restore Data** window is displayed.

4. In the **Data to Restore** fields, select the **Historical data** and **Non-CMS data** options, as illustrated in the following figure:



```
Maintenance: Restore Data

Status:
Errors:

Device name: default

Restore from last backup (y,n): y
Restore historical data from:
 Start date: __________  Start time: ________
 Stop date:  __________  Stop time:  ________
ACD(s) to restore (select one):
 <x> All ACDs  <_> Current ACD

Data to restore (Select any you wish):
 [_] Local system administration data
 [x] CMS system administration data
 [x] ACD-specific administration data
 [x] Historical data
 [x] Non-CMS data
 [_] Specific tables
```

5. After you verify that the correct restore options are selected, press **Enter** to move the active cursor to the action box in the top right corner of the window.

6. Select the **Run** option and press **Enter**.

   If the customer does not have any custom report tables set up by the PSO, the **Maintenance: Restore Data** window will display the following message when the restore is run:

   ```
   Errors: Initialization errors. See Error Log.
   ```

   To view the error log, select **Maintenance** > **Error Log** from the CMS menu. The relevant log message reads as follows:

   ```
   Restore process startup failed. Cannot restore non-CMS data
   because there are not tables in the database for that group.
   ```

   These error messages can be ignored.

CMSADM backups on the HA servers

When both servers are fully operative, CMSADM backups must be performed as soon as possible on each server. The CMSADM file system backup saves all system files (excluding CMS call data). You must store these backups in a safe place so they can be used to restore the system after a major system failure.

For a description of the CMSADM backup procedure, see Performing a CMSADM backup on page 33.

Administering the switch for CMS HA systems

Overview

Before a Avaya Call Management System (CMS) high availability (HA) system can collect and process Automatic Call Distribution (ACD) data from the switch, you must administer a special hardware interface on the switch. Each switch can use a number of different interfaces to communicate to a CMS computer.

The switch administration procedures described in *Administering the switch for CMS HA systems* apply to all Avaya switches supported by CMS Release 3 Version 11 that are capable of supporting 2 C-LAN boards.

For additional information about switch administration, see the appropriate switch administration documents.

Multiple ACDs on HA systems

For the High Availability option, you must connect a link from one C-LAN circuit pack to one CMS computer, and a second link from a different C-LAN circuit pack to another CMS computer.

In addition to having the correct CMS version and base load, the switch must be:

- Optioned with a switch version of V8 or later
- Call Center Release 8.1 or later
- Adjunct CMS Release of R3V8 or later, as specified below in Determining switch/CMS compatibility on page 62

The two CMS computers used in a dual server HA system can collect identical data from up to eight switches. When viewed from the perspective of the CMS server, each switch represents one ACD. For HA systems, all switches connect to the servers via TCP/IP. The switch administration procedures shown in *Administering the switch for CMS HA systems* are applicable whether you are setting up one switch or as many as eight switches; each switch requires a link to the CMS computer.

Setting up version and release values

Setting up version and release values contains switch administration activities that must be done for all G3 switches (si, r, and csi) before you administer the switch-to-CMS computer link.

Overview

Administrative procedures related to setting up version and release values include:

- Setting the G3 version on the **System-parameters customer-options** screen
- Setting the call center release on the **System-parameters customer-options** screen
- Setting up the adjunct CMS release on the **System-parameters features** screen

In addition, some basic CMS link administration is described in this section.

Note:

The screens in this section are for reference only. The screens you see may vary, depending on the type of switch and the configuration.

Determining switch/CMS compatibility

Use the following *Switch/CMS compatibility table* to set the G3 version, call center release, adjunct CMS release, and CMS setup switch type based on the release of the switch. You can set the G3 version, call center release, or adjunct CMS release to an earlier version, but you will not have all of the features that are available with the most recent release.

Switch/CMS compatibility table

Switch release	Switch administration			CMS administration
	G3 version	Call center release	Adjunct CMS release	CMS setup switch model
R8.x	V8	8.1 or later	R3V8	DEFINITY-R8
R9.x	V9	9.1 or later	R3V8/R3V9	DEFINITY-R9
R10.x	V10	9.1 or later	R3V9	DEFINITY-R9
R11.x	V11	11 or later	R3V11	MultiVantage-R11

Setting the switch version

Use `Page 1` of the **System-parameters customer-options** screen and the Switch/CMS compatibility table on page 62 to set the switch version.

To enable the HA option:

1. In the `G3 version` field, enter the software release of the switch.

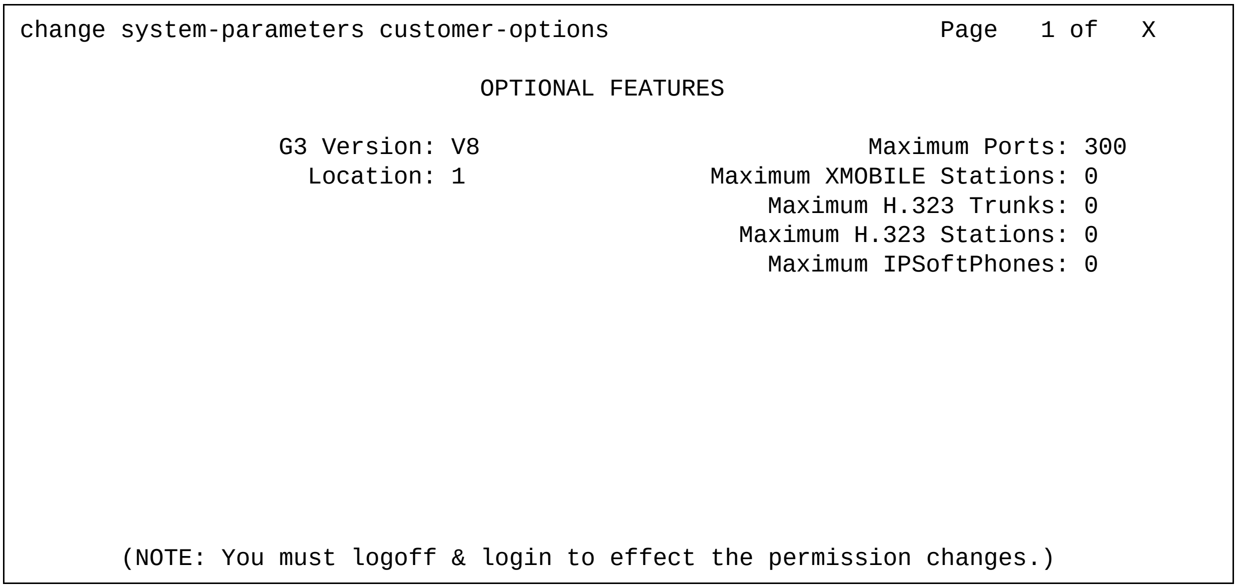
Important:

This entry must be **V8** or later.

Note:

If you set this field to a release number that is earlier than the switch release, you will not have access to the latest switch features.

Example:



```
change system-parameters customer-options                       Page   1 of   X

                                OPTIONAL FEATURES

                  G3 Version: V8                           Maximum Ports: 300
                    Location: 1                 Maximum XMOBILE Stations: 0
                                                    Maximum H.323 Trunks: 0
                                                  Maximum H.323 Stations: 0
                                                    Maximum IPSoftPhones: 0










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

Setting the call center release

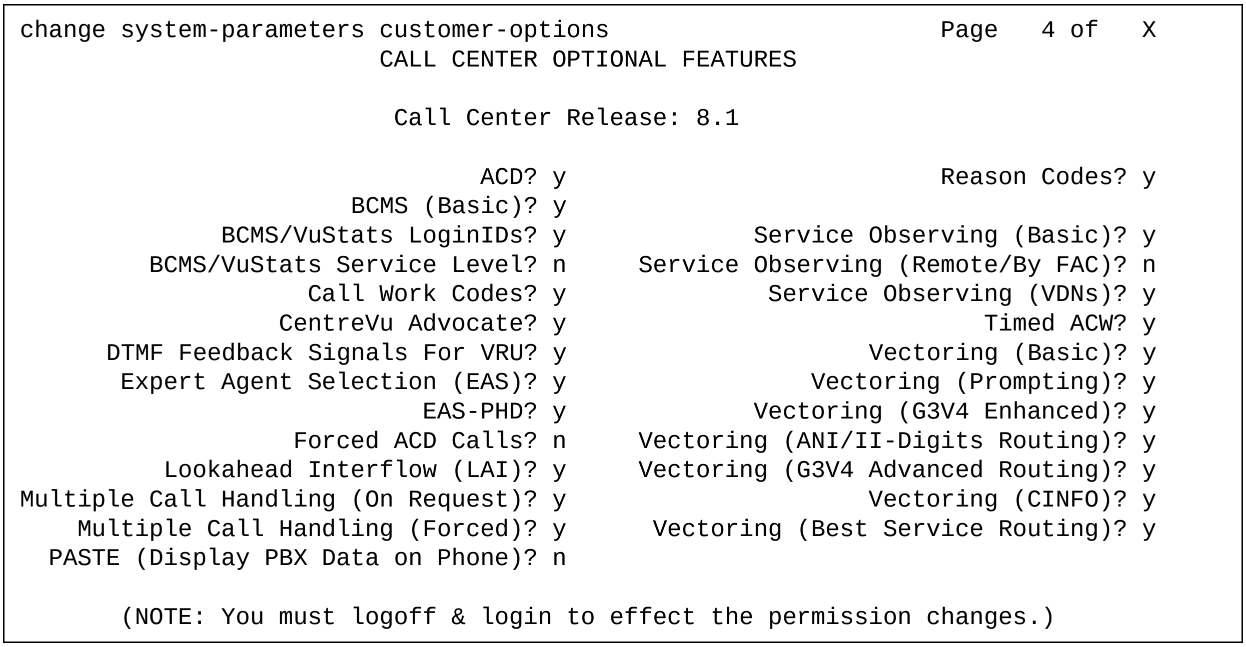
Use the **System-parameters customer-options** screen and the Switch/CMS compatibility table on page 62 to set the call center release. The `Call Center Release` field is a new field introduced with R8.

1. In the `Call Center Release` field, enter the call center release value.

Important:

The call center release must be set to **`8.1`** or later in order to use the High Availability option.

Example:



```
change system-parameters customer-options                       Page   4 of   X
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 8.1

                                ACD? y                          Reason Codes? y
                       BCMS (Basic)? y
              BCMS/VuStats LoginIDs? y             Service Observing (Basic)? y
         BCMS/VuStats Service Level? n     Service Observing (Remote/By FAC)? n
                    Call Work Codes? y              Service Observing (VDNs)? y
                  CentreVu Advocate? y                             Timed ACW? y
      DTMF Feedback Signals For VRU? y                     Vectoring (Basic)? y
       Expert Agent Selection (EAS)? y                 Vectoring (Prompting)? y
                            EAS-PHD? y             Vectoring (G3V4 Enhanced)? y
                   Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
          Lookahead Interflow (LAI)? y     Vectoring (G3V4 Advanced Routing)? y
Multiple Call Handling (On Request)? y                     Vectoring (CINFO)? y
    Multiple Call Handling (Forced)? y      Vectoring (Best Service Routing)? y
  PASTE (Display PBX Data on Phone)? n

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

Setting the adjunct CMS release

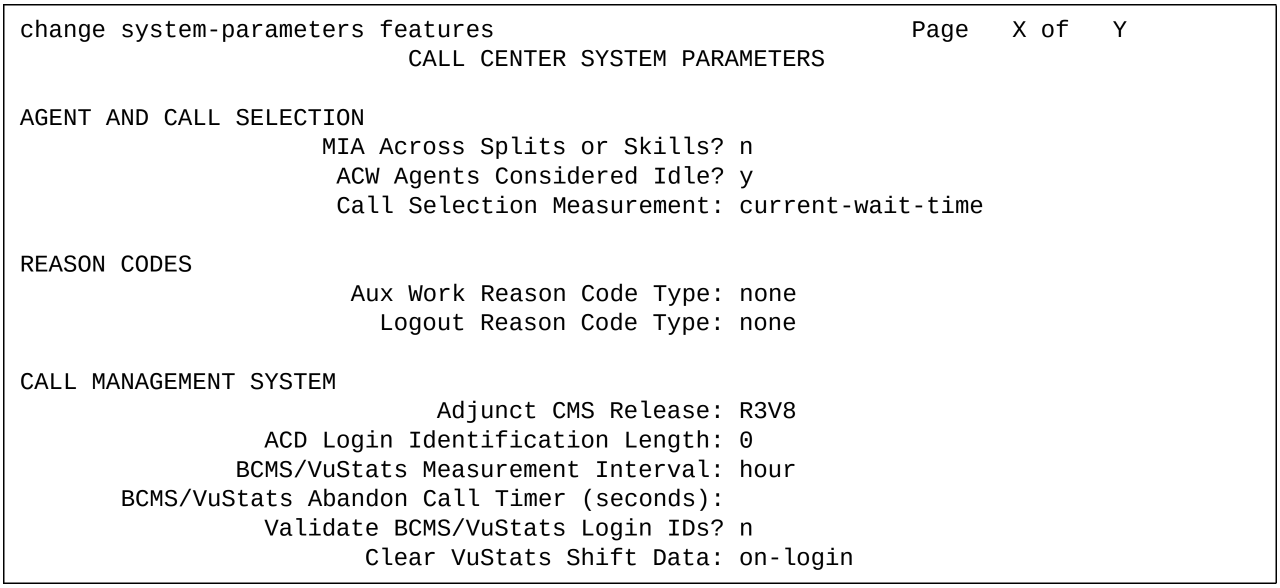
Use the **System-parameters features** screen and the Switch/CMS compatibility table on page 62 to set the adjunct CMS release. Depending on the switch release, the `Adjunct CMS Release` field can be found on different pages in the **System-parameters features** screen.

1. In the `Adjunct CMS Release` field, enter the CMS release.

   ⚠ **Important:**

   The adjunct CMS release must be set to `R3V8` or later in order to use the High Availability option.

Example:



```
change system-parameters features                               Page   X of   Y
                           CALL CENTER SYSTEM PARAMETERS

AGENT AND CALL SELECTION
                     MIA Across Splits or Skills? n
                      ACW Agents Considered Idle? y
                      Call Selection Measurement: current-wait-time

REASON CODES
                       Aux Work Reason Code Type: none
                         Logout Reason Code Type: none

CALL MANAGEMENT SYSTEM
                             Adjunct CMS Release: R3V8
                 ACD Login Identification Length: 0
               BCMS/VuStats Measurement Interval: hour
       BCMS/VuStats Abandon Call Timer (seconds):
                 Validate BCMS/VuStats Login IDs? n
                        Clear VuStats Shift Data: on-login
```

Setting up the link on the CMS computer

You must obtain the following information before setting up the CMS link:

- Switch name
- Switch model (release)
- Whether Vectoring is enabled on the switch (if authorized)
- Whether Expert Agent Selection (EAS) is enabled on the switch (if authorized)
- Whether the Central Office have disconnect supervision
- Local and remote port

  Note:

  The local and remote port assignments must be symmetrical between the switch and the CMS. The standard CMS provisioning procedure is to set the local and remote port assignments equal to the switch processor channel used for the link. For example, if you use processor channel 10, set the local and remote ports to 10.
- IP address or hostname
- TCP port

In addition to the switch administration presented in *Administering the switch for CMS HA systems*, you must also set up the switch link on the CMS computer using the `setup` or `swsetup` options of the **`cmssvc`** command.

See *Avaya CMS Release 3 Version 11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115.

Administering the switch

Overview

Administering the switch contains the procedures required to establish a communications link between the CMS computer and the switch.

Administering the LAN connection

Use the procedures in this section to administer the LAN connection to the switch. *Administering the LAN connection* contains examples of pertinent switch administration screens, with detailed explanations for the required fields. Use the screens in the order shown in the following *Switch administration screen table*.

Switch administration screen table

Form	Purpose
change node-names (Release 8 switch) change node-name IP (Release 9 switch) change node-name IP (Release 11 switch)	Adding node names and IP addresses
change ip-interfaces	Adding a C-LAN IP interface
add data-module	Adding an ethernet data module
change communication-interface processor-channels	Adding the processor interface channels
add ip-route	Adding IP routes (if needed)

Note:

To enable the HA option, you must administer a link from one C-LAN circuit pack to one CMS computer, and a second link from a different C-LAN circuit pack to another CMS computer.

Adding a second packet interface

⚠ **Important:**

This procedure is required only for G3csi switches.

Use the **Maintenance-Related System Parameters** screen to add a second packet interface to the G3csi switch. This is required for CMS computer connectivity.

1. In the `Packet Intf2` field, enter **`y`** to add a second packet interface.
2. In the `Bus Bridge` field, enter the equipment location of the CLAN circuit pack that does the bus bridge functionality when the packet bus is activated. This must be administered for the CLAN to work.

   Note:

   In the `Inter-Board Link Timeslots` field, the total number of timeslots allocated cannot be greater than 11.

3. In the `Inter-Board Link Timeslot Pt0` field, enter the number of timeslots (1-9) used by this port. Port 0 carries the bulk of messaging traffic between the switch and the CMS. The default of **`6`** should be adequate, but can be increased (if needed) to improve traffic flow.
4. In the `Inter-Board Link Timeslot Pt1` field, enter the number of timeslots (1-3) used by this port. Port 1 is a low traffic port and should always be set to **`1`**.
5. In the `Inter-Board Link Timeslot Pt2` field, enter the number of timeslots (1-3) used by this port. Port 2 is a low traffic port and should always be set to **`1`**.

Example:

```
change system-parameter maintenance                            Page 2 of X
                         MAINTENANCE-RELATED SYSTEM PARAMETERS

MINIMUM MAINTENANCE THRESHOLDS ( Before Notification )
        TTRs: 4        CPTRs: 1        Call Classifier Ports:
        MMIs: 0          VCs:

TERMINATING TRUNK TRANSMISSION TEST (Extension)
  Test Type 100:        Test Type 102:         Test Type 105:

ISDN MAINTENANCE
   ISDN-PRI TEST CALL Extension:         ISDN BRI Service SPID:

DS1 MAINTENANCE
   DSO Loop-Around Test Call Extension:

LOSS PLAN (Leave Blank if no Extra Loss is Required)
   Minimum Number of Parties in a Conference Before Adding Extra Loss:

SPE OPTIONAL BOARDS
              Packet Intf1? y     Packet Intf2? y
   Bus Bridge: 01A03   Inter-Board Link Timeslots  Pt0: 6  Pt1: 1  Pt2: 1
```

Adding node names and IP addresses

For the HA option, assign two switch node names and two CMS computer node names. Use the **Node Names** screen pages to assign the name and IP address of the CMS computers and all switches networked with the CMS computer.

1. In the `Name` field, enter the host name of the CMS computer, any switches that are networked with the CMS computer, and any gateway hosts used in the network. The node names can be entered in any order. The names are displayed in alphabetical order the next time the form is displayed. The `default` node name entry is display-only and is not used for this application.

   For consistency, use the CMS computer's host name as defined during the CMS Setup procedure. See the appropriate CMS software installation maintenance and troubleshooting book for more information.

   These names are also used in the IP interfaces, data module, IP routing, and other forms. If you change the node name in this form, it is automatically updated on the other forms.

   Note:

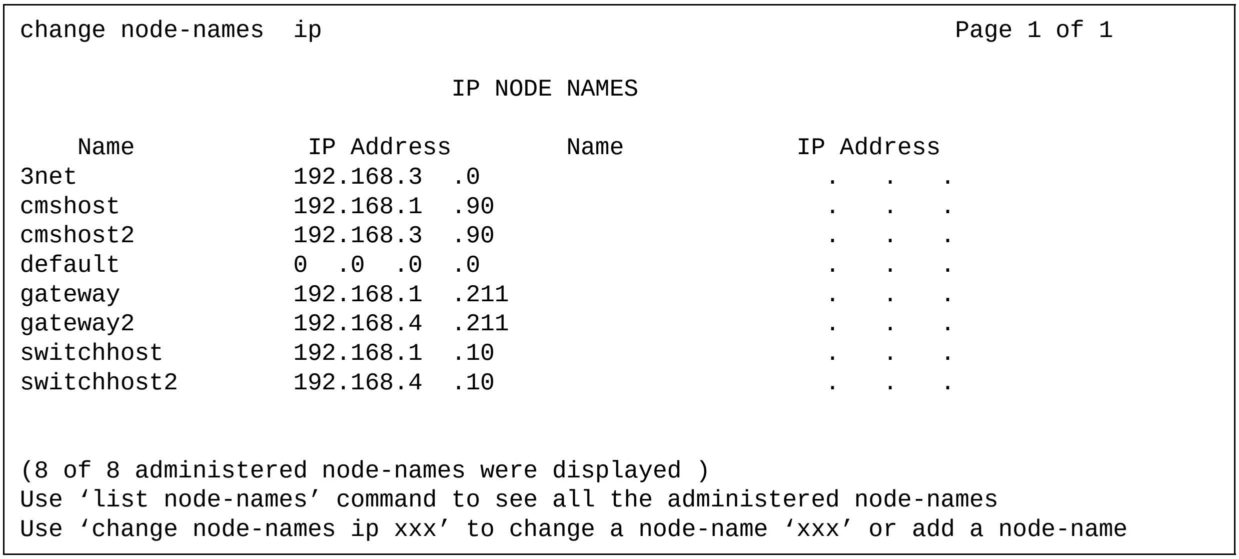
   Do not use special characters in the node name. Special characters are not allowed in the **/etc/hosts** file on the CMS computer.

2. In the `IP Address` field, enter the IP address of the CMS computer, the switches, and any required gateways.

   ⚠ **CAUTION:**

   Plan out the network before you assign any IP addresses. Any future changes that require a change to IP addresses will cause a service disruption.

Example:



```
change node-names  ip                                                  Page 1 of 1

                              IP NODE NAMES

    Name              IP Address        Name              IP Address
3net               192.168.3  .0                            .   .   .
cmshost            192.168.1  .90                           .   .   .
cmshost2           192.168.3  .90                           .   .   .
default            0  .0  .0  .0                            .   .   .
gateway            192.168.1  .211                          .   .   .
gateway2           192.168.4  .211                          .   .   .
switchhost         192.168.1  .10                           .   .   .
switchhost2        192.168.4  .10                           .   .   .


(8 of 8 administered node-names were displayed )
Use ‘list node-names’ command to see all the administered node-names
Use ‘change node-names ip xxx’ to change a node-name ‘xxx’ or add a node-name
```

Note:

On R8 switches, `Page 1` of the **Node Names** screen is reserved for Intuity™ administration.

Adding a C-LAN IP interface

Use the **IP Interfaces** screen to assign a C-LAN circuit pack as an IP interface. With the High Availability option, you must assign two separate C-LAN IP interfaces.

1. In the `Network regions are interconnected` field, enter **n**. This application is not used for C-LAN.
2. In the `Enabled` field, enter `y` to enable the C-LAN IP interface. After initial administration, you must disable the interface before you make any changes.
3. In the `Type` field, enter **`C-LAN`**

4. In the Slot field, enter the equipment location of the C-LAN circuit pack.

   Note:

   The Code/Sfx field is a display-only field that shows the designation number of the circuit pack installed in the specified slot.

5. In the Node Name field, enter the switch node name you assigned on the **Node Names** screen.

   For example, enter **switchhost**. The same node name cannot be assigned to two different IP interfaces.

6. In the Subnet Mask field, use the default entry or check with the LAN administrator on site if connecting through the customer's LAN.

   Note:

   The Subnet Mask field identifies which portion of an IP address is a network address and which is a host identifier.

7. In the Gateway Address field, enter the address of a network node that will serve as the default gateway for the IP interface.

   - If the application goes to points off the subnet, a gateway address of the router is required.
   - If the switch and the CMS server are on the same subnet, a gateway address is not required.
   - If ethernet only is used, and a gateway address is administered, no IP routes are required.

8. In the Net Rgn field, enter **1** for a C-LAN IP interface.

Example:

```
change ip-interfaces                                          Page 1 of 1

 Network regions are interconnected? n
 En-                                                                Net
abled Type   Slot  Code Sfx Node Name       Subnet Mask     Gateway Address Rgn
  y   C-LAN  01A03 TN799B   switchhost      255.255.255.0   192.168.1  .254 1
  y   C-LAN  01C02 TN799B   switchhost2     255.255.255.0   192.168.4  .254 1
  n                                         255.255.255.0      .   .   .
  n                                         255.255.255.0      .   .   .
  n                                         255.255.255.0      .   .   .
  n                                         255.255.255.0      .   .   .
  n                                         255.255.255.0      .   .   .
```

Adding an ethernet data module

Use the **Data Module** screen to assign an ethernet data module for each of the C-LANs used for CMS HA (this is a different version of the form than that used for DEFINITY R7). With the High Availability option, you assign two ethernet data modules.

1. In the `Data Extension` field, enter an unassigned extension number.
2. In the `Type` field, enter: **`ethernet`**
3. In the `Port` field, enter the equipment location of the C-LAN circuit pack (TN799). For the ethernet link, always use circuit 17 (for example, 01A0317).
4. In the `Link` field, enter a TCP/IP link number (1-25 for csi/si, 1-33 for r). This entry is also used on the processor channel screen.
5. In the `Name` field, enter a name for the data module. This name will display when you list the assigned data modules.

   Note:

   The `BCC` field is a display-only field.
6. In the `Network uses 1’s for Broadcast Address` field, choose one of the following actions:

   Note:

   the `Network uses 1’s for Broadcast Address` field is used to set the host portion of the IP address to 0’s or 1’s.

   - The default is **y** (all 1’s). Use the default if the private network contains only Avaya switches and adjuncts.
   - Enter **n** only if the network includes non-Avaya switches that use the 0’s method of forming broadcast addresses.

Example:

```
add data-module 2000                                            Page   1 of   1
                                DATA MODULE

  Data Extension: 2000            Name: ethernet data module         BCC: 2
            Type: ethernet
            Port: 01A0317
            Link: 8




Network uses 1’s for Broadcast Address? y
```

Adding the processor interface channels

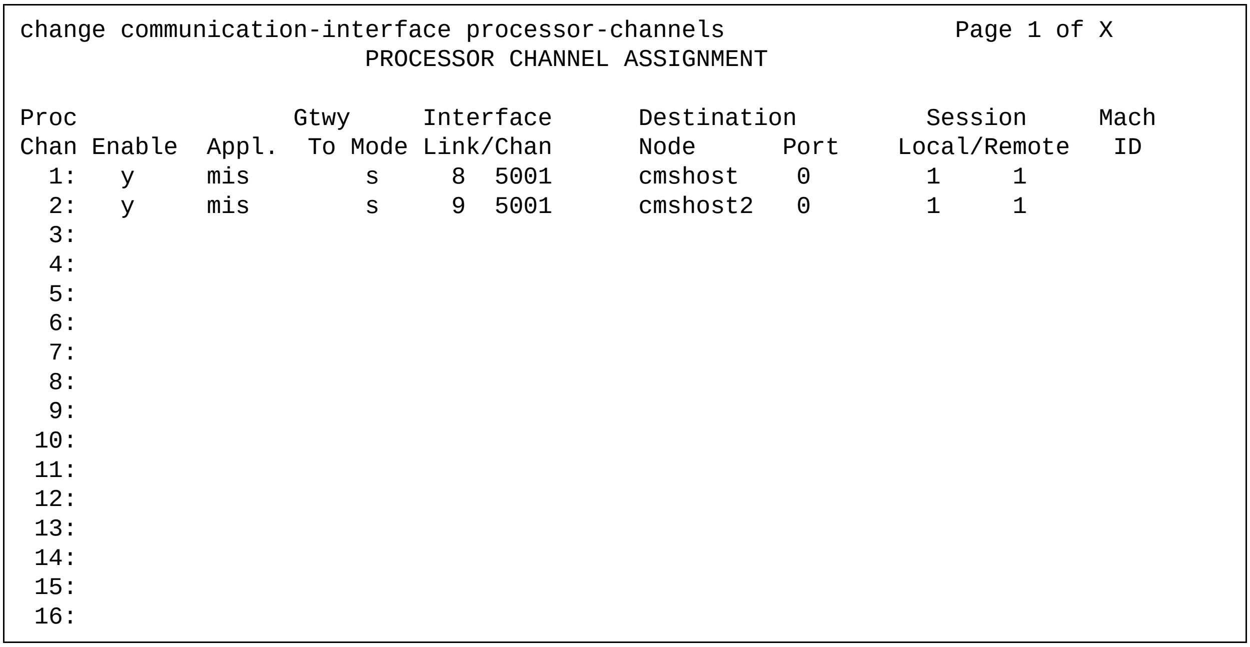
Use the **Processor-channels** screen to assign the processor channel attributes. With the High Availability option, you will assign two separate processor channels.

1. In the `Proc Chan` field, select a processor channel for this link. The standard CMS provisioning procedure is to use channel 1 on a G3r switch, and to use channel 10 on a G3csi or G3si switch.
2. In the `Enable` field, enter: **`y`**
3. In the `Appl` field, enter: **`mis`**

   Note:

   The `Gtwy To` field is not used for CMS.
4. In the `Mode` field, enter **`s`** for server.
5. In the `Interface Link` field, enter the TCP/IP link number used on the ethernet data module form.
6. In the `Interface Chan` field, enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup.
7. In the `Destination Node` field, enter the node name of the CMS computer as assigned on the **Node Names** screen. In the example below, `cmshost` is used.
8. In the `Destination Port` field, use the default of **`0`**
9. In the `Session Local/Session Remote` field, the local and remote port assignments must be symmetrical between the switch and the CMS server. The standard CMS provisioning practice is to set the local and remote port assignments equal to the processor channel assignment. For example, if you use processor channel 10, also set the local and remote ports to 10.
10. The `Mach ID` field is not used for CMS.

Example:



```
change communication-interface processor-channels               Page 1 of X
                        PROCESSOR CHANNEL ASSIGNMENT

Proc               Gtwy     Interface      Destination         Session     Mach
Chan Enable  Appl.  To Mode Link/Chan      Node      Port    Local/Remote   ID
  1:   y     mis        s     8  5001      cmshost    0         1     1
  2:   y     mis        s     9  5001      cmshost2   0         1     1
  3:
  4:
  5:
  6:
  7:
  8:
  9:
 10:
 11:
 12:
 13:
 14:
 15:
 16:
```

Adding IP routing

Use the IP Routing form to set up the IP route(s) from the switch to the CMS computer. This is required when:

- The switch and the CMS computer are on different subnets, or
- When a Gateway Address is not administered for the C-LAN IP interface.

Note:

LAN configurations that require IP routing are not recommended for use with the HA option.

To add IP routing:

1. In the `Route Number` field, choose one of the following actions:
   - If the link between the switch and the CMS computer is a dedicated link through a hub, you only need to assign one IP route.
   - If you are going through a router, you must set up IP route 1 from the switch to the router, and then set up IP route 2 from the switch to the CMS computer.

   The example below shows a simple IP route.
2. In the `Destination Node` field, enter the node name for the CMS computer or a router, depending on your configuration.

   Note:

   The `Destination Node` field represents the node name of the destination for this route.
3. In the `Gateway` field, enter the node name of the gateway by which the destination node is reached for this route. This is either the local C-LAN port or the first intermediate node between the C-LAN port and the final destination.

   For example, if there were one or more routers between the C-LAN port and the final destination node (the CMS computer), the gateway would be the node name of the first router.
4. In the `C-LAN Board` field, enter the equipment location of the CLAN circuit pack that provides this route. It is possible to have more than one C-LAN circuit pack, but most configurations will have only one C-LAN.

5. In the `Metric` field, choose one of the following actions:

   - Enter **`0`** if there are no intermediate nodes between the switch C-LAN port and the ethernet port on the CMS computer.
   - Enter **`1`** only on a switch that has more than one C-LAN circuit pack installed.

   Note:

   The `Metric` field specifies the complexity of this IP route. See *Administration for Network Connectivity* for more information about using this field.

6. In the `Route Type` field (R8 switches, only), perform one of the following actions:

   - Use a `Host` route to get to a specific IP address.
   - Use a `Network` route to get to a subnet.

   Note:

   The `Route Type` field specifies whether the route is host or network (default).

Example:

The following example shows an IP route. This route shows how you get from a gateway (for example, a router) to a network.

```
add ip-route 1                                          Page   1 of   1
                             IP ROUTING

    Route Number: 1
Destination Node: 3net
         Gateway: gateway2
     C-LAN Board: 01C02
          Metric: 0
      Route Type: Network
```

Index