AVAYA communication

CentreVu® Call Management System

Release 3 Version 9
High Availability Connectivity, Upgrade and Administration

585-215-106
Comcode 700016702
Issue 1.0
April 2001

Notice

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

Intellectual property related to this product (including trademarks) and registered to Lucent Technologies Inc. has been transferred or licensed to Avaya Inc.

Any reference within the text to Lucent Technologies Inc. or Lucent should be interpreted as references to Avaya Inc. The exception is cross references to books published prior to April 1, 2001, which may retain their original Lucent titles.

Avaya Inc. formed as a result of Lucent's planned restructuring, designs builds and delivers voice, converged voice and data, customer relationship management, messaging, multi-service networking and structured cabling products and services. Avaya Labs is the research and development arm for the company.

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 assistance or support, call the Technical Service Center's 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.

Canadian Department of Communications (DOC) Interference Information

This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the radio interference regulations of the Canadian Department of Communications.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le ministére des Communications du Canada.

Trademarks

CentreVu is a registered trademarks of Avaya and Lucent Technologies.

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

INFORMIX is a registered trademark of Informix Software, Inc.

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

Avaya National Customer Care Center

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

European Union Declaration of Conformity

The "CE" mark affixed to the equipment described in this book indicates that the equipment conforms to the following European Union (EU) Directives:

- Electromagnetic Compatibility (89/336/EEC)
- Low Voltage (73/23/EEC)
- Telecommunications Terminal Equipment (TTE) i-CTR3 BRI and i-CTR4 PRI

For more information on standards compliance, contact your local distributor.

Avaya Web Page

http://www.avaya.com

Acknowledgment

This document was developed by the Avaya University CRM Information Development group.

CentreVu® Call Management System
High Availability Connectivity, Upgrade and Administration

Table of Contents

Chapter 1 Introduction

Overview 1-1
Supported Definity switches 1-2
Supported CMS platform combinations 1-2
Required and optional software 1-3
Special upgrade considerations 1-4
General roles and responsibilities 1-4
Customer-specific roles and responsibilities 1-5
CentreVu CMS helplines 1-6
Customer support for U.S. and Canada 1-6
Customer and technician support outside of U.S. and Canada 1-6
Technician support for U.S. and Canada. 1-6

Chapter 2 Connecting HA servers to the switch

Overview 2-1
Server switch-over options. 2-1
Basic configuration rules 2-2
Connecting blocks 2-3
Planning for LAN switch links 2-3
Connecting to the Definity switch 2-6
Overview 2-6
LAN connectivity options. 2-6
Ethernet ports on a CMS server 2-7

Chapter 3 Upgrading CMS to the HA option

Overview 3-1
HA upgrade scenarios 3-1
Overview of the HA upgrade process 3-2
Verifying the tape drive on the server currently in service 3-6
E3000 tape verification procedure 3-7
Ultra 5 tape verification procedure 3-7
E3500 tape verification procedure 3-8
Performing a CMSADM backup 3-8
Overview 3-8
Prerequisites 3-9
Procedure 3-9
Performing a Full Maintenance backup 3-12
Performing a maintenance backup (Administration Data only) 3-13
Procedure 3-13
Setting Up CMS on an HA server 3-15

Overview 3-15
Prerequisites 3-16
Setting CMS authorizations 3-16
Setting Up data storage parameters 3-17
Setting Up a LAN for switch connections 3-18
Setting Up the CMS application 3-18
Installing feature packages 3-19
Setting up the remote console 3-19
Overview 3-19
Designating remote console ports on an HA system 3-20
Procedure. 3-20
Setting Up the Alarm Origination Manager 3-20
Overview 3-20
Procedure 3-20
Setting up the NTS 3-21
Creating an alternate boot device for mirrored systems 3-21
Migrating CMS system administration data to the new server . . . 3-22
Procedure 3-22
Checking the archive interval 3-24
Administering the switch 3-25
Performing an Incremental Maintenance backup 3-25
Procedure 3-25
Upgrade the original CMS server 3-26
Migrating CMS Historical Data to the new HA server 3-27
Migrating Administration Data back to the original server. . . . 3-28
Migrate the Administration Data 3-29
Performing a new Full Maintenance backup and restore 3-30
Performing the Full Maintenance backup on the new HA server . . . 3-30
Restoring historical data to the original server. 3-30
Procedure. 3-31
Performing CMSADM backups on the HA servers 3-32

Chapter 4 Administering the switch for CMS HA systems

Overview 4-1
Multiple ACDs (switches) on HA systems. 4-2
Setting up version and release values 4-2
Overview 4-2
Determining switch/CMS compatibility 4-3
Setting the switch version 4-3
Setting the call center release 4-4
Setting the adjunct CMS release 4-5
Setting up the link on the CMS computer 4-6
Administering the Definity switch 4-6
Overview 4-6
Administering the LAN connection 4-7

Index **IN-1**

Introduction

Overview

The CentreVu® 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® 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 Definity 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 CentreVu Internet Call Center, it is installed only on the primary server
- Most CMS administration changes are entered only on the primary server. Any changes made on the primary server are subsequently transferred to the secondary server by means of 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 only on 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 Definity switches

The CMS HA option is supported on the following Definity ECS (R8.1 or later) switches:

- Definity ECS R8csi
- Definity ECS R8si
- Definity ECS R8r
- ProLogix R3

Supported CMS platform combinations

CMS HA is supported on the following platform combinations:

- Sun Ultra 5 - Ultra 5
- Sun Enterprise 3000 - Enterprise 3000
- Sun Enterprise 3500 - Enterprise 3000
- Sun Enterprise 3500 - Enterprise 3500

NOTE:

- for HA systems in which Enterprise 3000 and 3500 servers are combined, it is recommended that the 3500 server be designated as the primary HA server
- for HA systems in which Ultra 5 and Ultra 5 Einstein servers are combined, the Einstein server should be designated as the primary server

Required and optional software

A complete set of CMS R3V9 software package CDs (with the exceptions listed below) is provided for the second server at no additional charge. For a complete list of required and optional software packages for CMS R3V9, see Chapter 1 in: “CentreVu Call Management System Software Installation, Maintenance and Troubleshooting (585-215-956)”.

For primary and secondary servers deployed in HA systems, the following exceptions to the standard CMS R3V9 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 onsite switch)
- CentreVu 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.

[*] *INFORMIX* is a registered trademark of Informix Software, Inc.

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 event), 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 servers synchronization with the least time and effort, while minimizing data loss as much as possible.

If the customer CMS server has any custom features, such as Custom Reporting, custom interfaces, LAN printers, token ring, etc., 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 HA option” .

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 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 CentreVu 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 in order to support a CMS HA installation.

Task
Retention of CMS documentation and software
For those administration changes which 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

CentreVu CMS helplines

If an installation problem arises that requires assistance, customers or Avaya, Inc. technicians can call the numbers provided below.

Customers should inform Support personnel that their CMS system is configured for the High Availability service option.

Customer support for U.S. and Canada

http://support.avaya.com or 1-800-242-2121

Customers can access the CMS internet support web site and access the Online Expert to get answers to common problems, obtain copies of CMS document and create service requests.

By calling the 1-800 number, the customer reports the problem and generates a trouble ticket so that the problem can be worked by the services organization. The customer is prompted to identify the type of problem (ACD, hardware, or CentreVu CMS) and is connected to the appropriate service organization.

Customer and technician support outside of U.S. and Canada

For customer and technician support outside of the U.S. and Canada, contact your Avaya, Inc. representative or distributor for more information.

Technician support for U.S. and Canada

1-800-248-1234

Avaya Inc. technicians can receive help during installations by using this number.

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. This information is applicable to the following Definity switches (Release 8.1 or later):

- Generic 3si (G3si)
- Generic 3r (G3r)
- Generic 3csi (G3csi)
- ProLogix Release 3 (G3csi)

The connectivity configurations described in this chapter represent the optimal link setups for HA systems. Other switch-to-server connectivity configurations are not described herein. For information about other switch-to-server connections, see *CentreVu 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 Definity ECS and the CMS system on which the data is stored. However, 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 will continue on the secondary server, but the customer will not be 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 editing of host configuration files on the secondary server and re-administration of CMS supervisor clients by their individual users in order to redirect them 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, etc. 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 must be physically located in the same building, and ideally, should be directly adjacent to each other in order to facilitate ease of maintenance.

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 Definity 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 4-1.

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, irrespective 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, planning information must be gathered before you begin. In particular, you must take into account if the LAN connection includes both a connection to CMS and 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, CentreVu Supervisor, Intuity Message Manager)

     — If desired, a second Definity 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, CentreVu 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:

  a. 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.

  b. 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:

  a. 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

  b. 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 Definity 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 many, if not most, CMS customers who adopt the HA option.

LAN connectivity options

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

- **Connecting with a 10Base-T hub and Cat 5 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, since a hub is not included in the configuration, it is not recommended for HA systems.

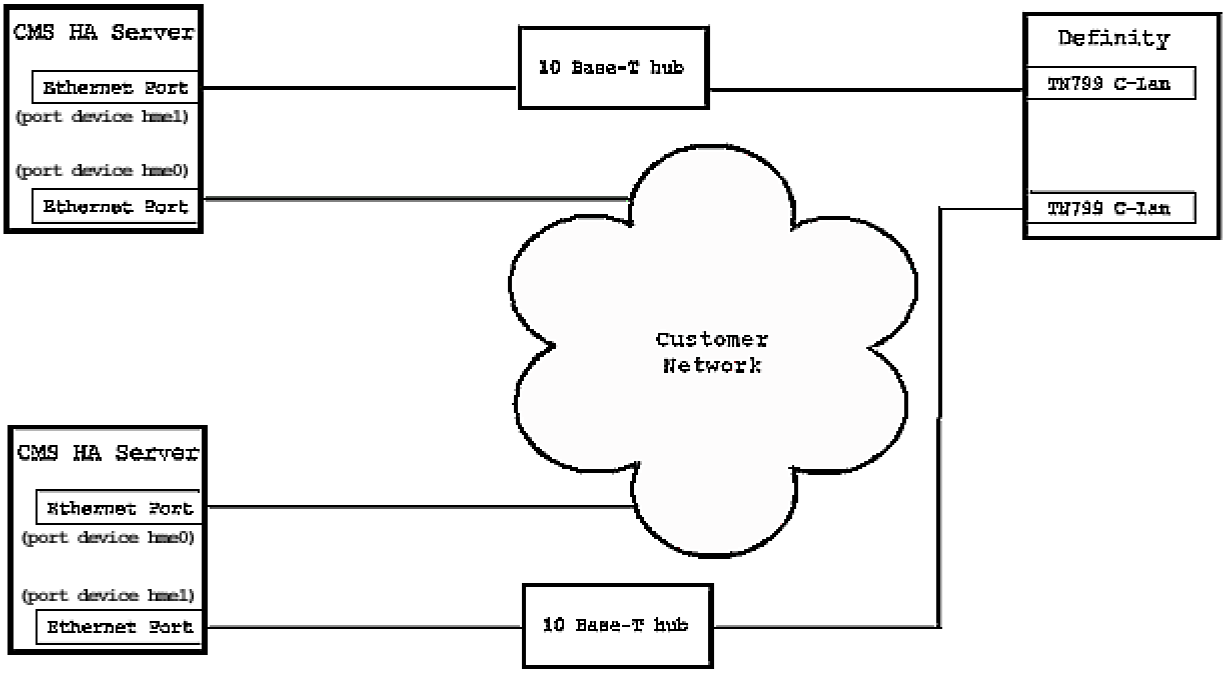
If the customer requires a link connection by means of crossover cables or other methods not described above, general descriptions and requirements for alternate connectivity setups are described in *CentreVu Call Management System Switch Connection and Administration* (585-215-876).

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



NOTE:

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

*·*SunSwift* is a trademark of Sun Microsystems, Inc.

Connecting with a 10Base-T hub

Connecting through a 10Base-T hub LAN connection is the recommended method to connect 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 included in future upgrade plans), 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. Therefore, 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 typically made through a private network maintained by the customer.

Parts list

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

Quantity (per CMS server)	Description	Comcode*
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

Quantity (per CMS server)	Description	Comcode*
2	**RJ45 UTP Category 5 modular cord:**	
	5 feet, 1.5 meters	107748063
	10 feet, 3 meters	107748105
	15 feet, 4.5 meters	107748188
	25 feet, 7.6 meters	107742322
	50 feet, 15.2 meters	107742330
	100 feet, 30.5 meters	107748238
	200 feet, 61 meters	107748246
	300 feet, 91 meters	107748253
1	CenterCOM 10Base-T LAN Hub	407086735

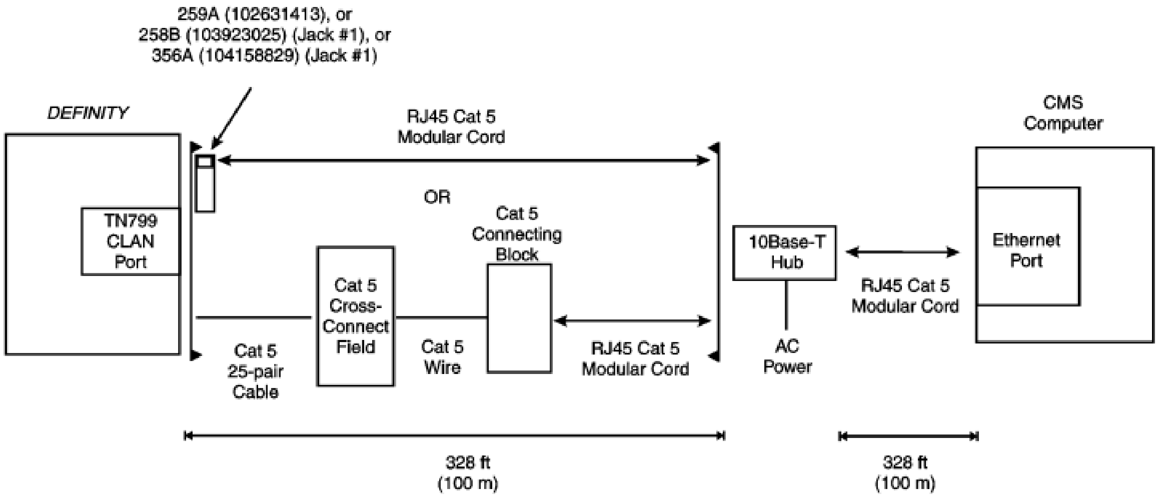
*Parts for which no comcode is displayed must be obtained by the customer prior to the scheduled upgrade.

Cabling procedure

This procedure describes the step required to make the connection between a dual ACD link and the HA server. For more information, refer to the “Cabling diagram - LAN via 10Base-T hub” on Page 2-10.

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 HA option

Overview

“Upgrading CMS to the High Availability Option” describes CentreVu 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 CentreVu Upgrade Express (CVUE) 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, if not most cases, 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 onsite 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:

a. the CMS servers have the same CMS version and base load

b.the original server has the same CMS version as that installed on the new HA server, but the base loads are different

c. the original server has an earlier version of CMS than that installed on the new HA server

If either case a) or b) are in effect, the upgrade process is significantly simplified, since:

- the Definity switch can be administered for the correct CMS version and the dual ACD links prior to the arrival of the new HA server onsite (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 only needs 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 due to 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-R3V9 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 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 accompanying figure on Page 3-5.

NOTE:

Steps 1 through 4 (below) should be performed approximately 24 hours before the HA upgrade process is initiated.

1. Upgrade the Definity Switches to Release 8.1 (or later) and administer the switches to run with the current (pre-R3V9) 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. For 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 Exabyte Mammoth 20-40 Gbyte 8mm (EXB-8900) 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. For 24/7 call center operations, 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 1-2)
   b. establish a cut-off time on the day of the HA upgrade, after which time CMS users will not make changes to the system administration until the upgrade is completed.
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 onsite 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 new HA server is installed, configured, CMS is put 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.

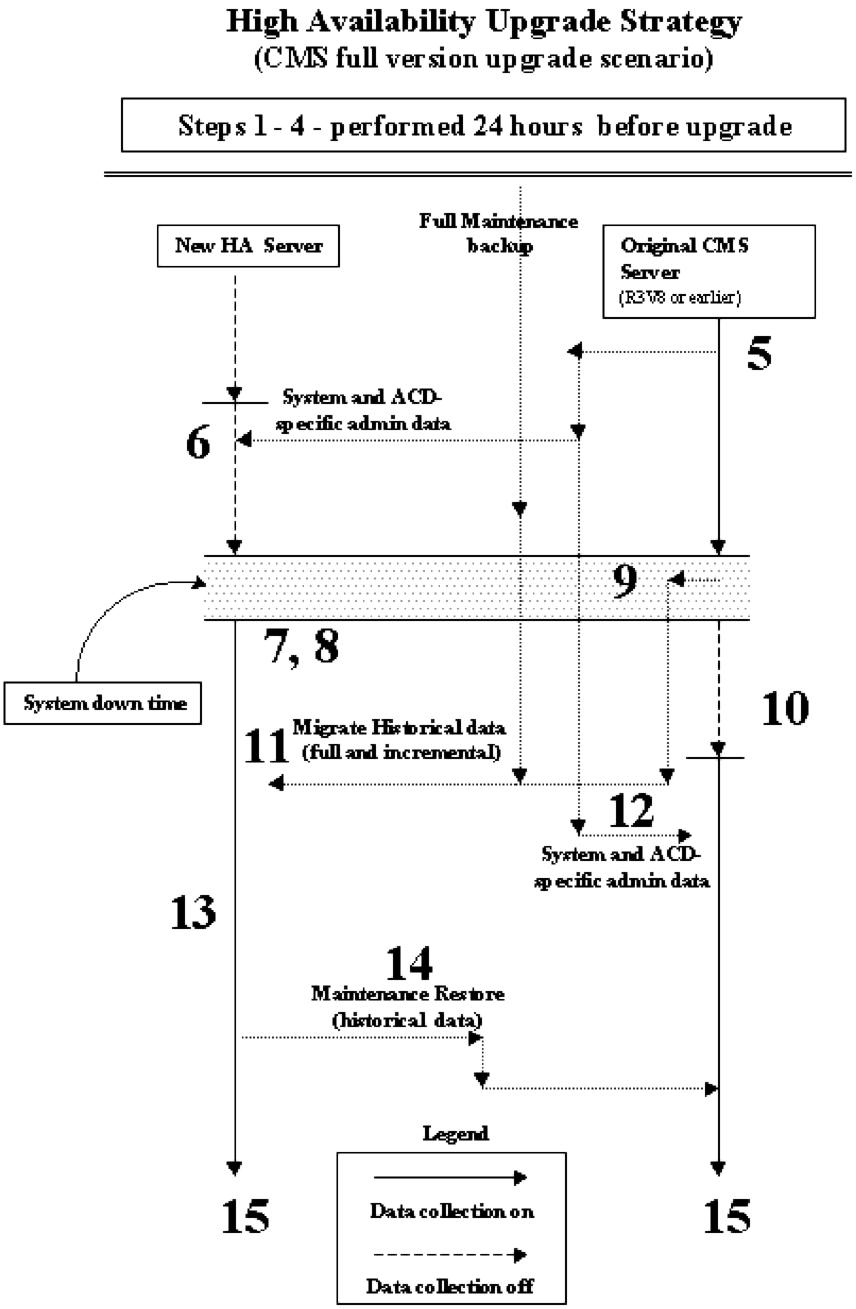
**Sun* is a registered trademark of Sun Microsystems, Inc.

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 R3V9 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 CentreVu Upgrade Express (CVUE) upgrade. Refer to the platform-specific instruction booklet included in the CVUE upgrade kit. Then perform the rest of the CVUE upgrade.
10. After the CVUE 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 preceeding 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 *CentreVu Call Management System R3V9 High Availability User Guide* (585-215-705).

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
System and ACD-specific admin data
6
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)
Legend
Data collection on
Data collection off
15
15

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

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 an Exabyte Mammoth 20-40 Gbyte 8mm drive (EXB-8900).

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, one of the following conditions must be true in order to ensure tape drive compatability:

- The tape drive on the existing 3500 must be replaced by a new DDS-4 drive (if the new E3500 is equipped with a DDS-4 drive)
- The new 3500 must be equipped with a Mammoth tape drive in order to be compatible with the Mammoth drive on the existing 3500

For Ultra 5 - Ultra 5 combinations in which a new Ultra 5 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 DDS4 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.

E3000 tape verification procedure

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
   ```

Ultra 5 tape verification procedure

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 is 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
   ```

E3500 tape verification procedure

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 is 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 3 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 tape(s) for future reference.

NOTE:

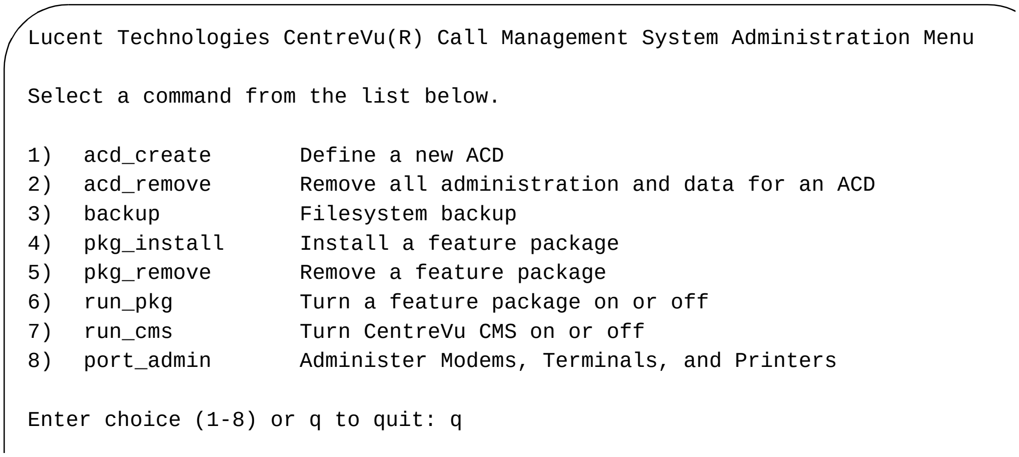
The CMS server must be administered to support a printer before the `vfstab` file can be printed out.

Procedure

1. Log in as root and enter:

   `cmsadm`

   The CMS Administration menu appears:



```
Lucent Technologies CentreVu(R) Call Management System Administration Menu

Select a command from the list below.

1)  acd_create       Define a new ACD
2)  acd_remove       Remove all administration and data for an ACD
3)  backup           Filesystem backup
4)  pkg_install      Install a feature package
5)  pkg_remove       Remove a feature package
6)  run_pkg          Turn a feature package on or off
7)  run_cms          Turn CentreVu CMS on or off
8)  port_admin       Administer Modems, Terminals, and Printers

Enter choice (1-8) or q to quit: q
```

2. Enter `3` to select the `backup` option. Depending on the configuration of your system, go to step 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-8500 8mm Helical Scan>
  2) <Archive QIC-150>
Enter choice (1-2):
```

3. Enter a tape drive selection from the displayed list. The program responds:

```
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.

4. 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 receive the message displayed above, insert the next tape and allow it to rewind. When it is properly positioned, press Enter.

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

   a.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)
```

   b. 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 receive the message displayed above, 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 5 a.

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

CAUTION:

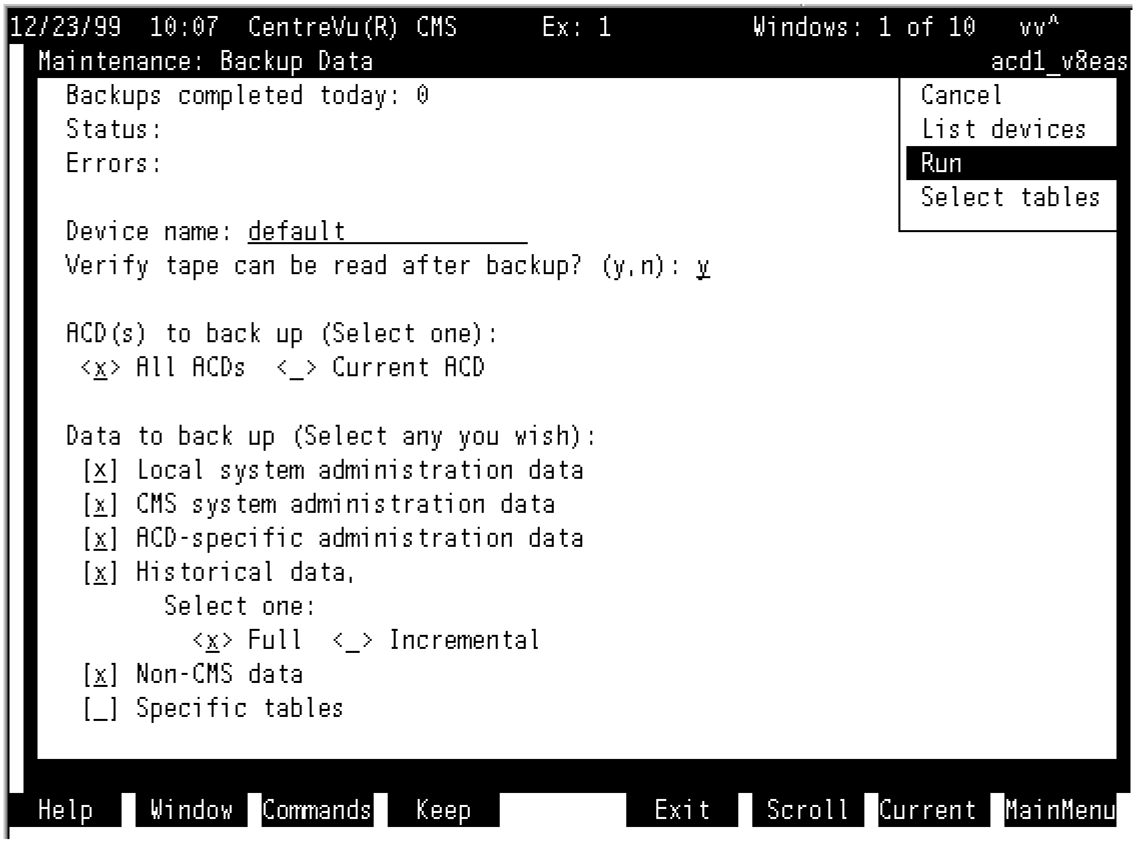
Label all tapes with the tape number and the date of the backup. Set the tape write-protect switch to read-only.

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.

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

   The Back Up Data window is displayed.



```
12/23/99  10:07  CentreVu(R) CMS      Ex: 1          Windows: 1 of 10   vv^
 Maintenance: Backup Data                                             acd1_v8eas
   Backups completed today: 0
   Status:
   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):
    [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
```

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

Performing a maintenance backup (Administration Data only)

When the CMS technician arrives onsite, they perform 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

1. From the CMS main menu, select the `Maintenance - Back Up Data option.`

   The Back Up Data window is displayed. Select the following data backup options:

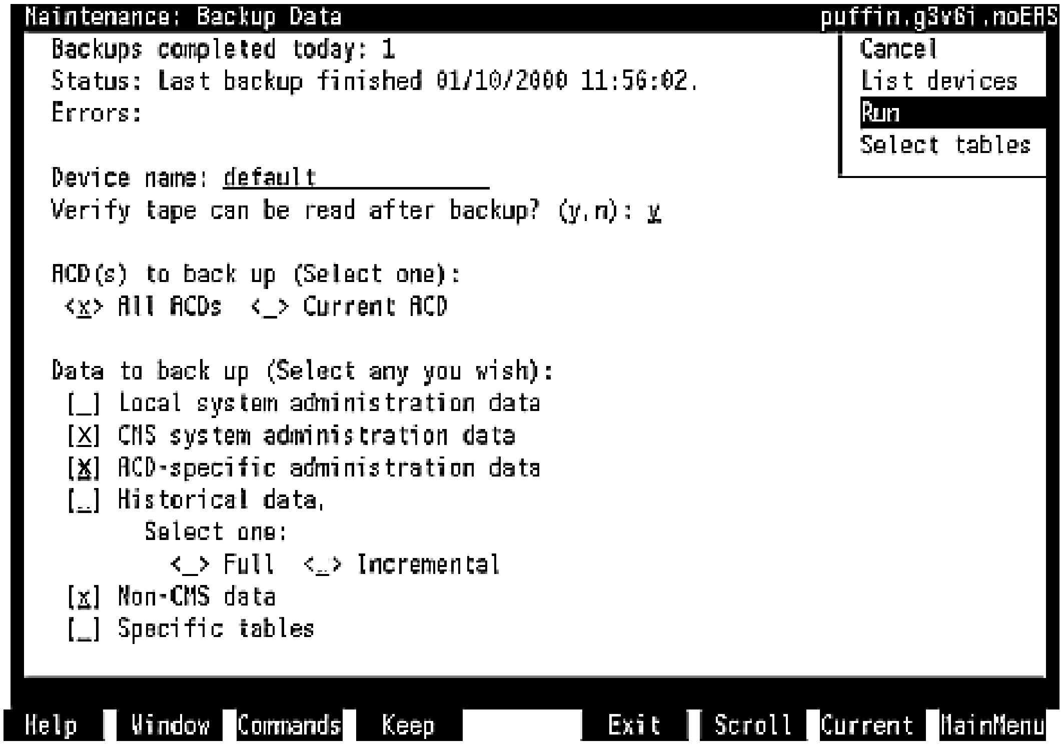
   - CMS System Administration data
   - ACD-specific admin data
   - Non-CMS data

   Exclude `Historical data` from this backup
2. Press the Enter key to move the active cursor to the action list in the upper right corner of the window active.
3. Select the `Run` option 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                                  puffin.g3v6i.noEAS
 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 access the action list in the upper right corner of the window, cursor to the `Run` option and press enter to start the backup.

4. Use the following procedure 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, for 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

This section refers to procedures which apply to both the new HA server purchased by the customer and the original server (after it has undergone a CVUE 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 reference the following document:

“CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

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 sections provided 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 completed the following tasks:

- 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 4-1**.**

- Connected the NTS and the CMS computer to the network hub unit. For more information, see:
  - — *CentreVu CMS R3V6 Sun Enterprise 3000 Computer Connectivity Diagram* (585-215-865)
  - — *CentreVu CMS Sun Enterprise 3500 Computer Hardware Installation Maintenance and Troubleshooting* (585-215-873)
  - — *CentreVu CMS Sun Ultra 5 Computer Hardware Installation Maintenance and Troubleshooting* (585-215-871).

Setting CMS authorizations

Overview

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

Procedure

For the procedure used to set up CMS authorizations, see "Setting up CMS authorizations, in Chapter 2 , "CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting" (585-215-956).

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 Chapter 2 of “CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

Setting Up a LAN for switch connections

Overview

This section contains information about setting up a LAN connection between the CMS computer and one or more HA-enabled Definity switches. This type of connection is used only with Definity ECS 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 also 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

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

Procedures

For the procedure used to set up data storage parameters, see "Setting up a LAN for switch connections", in Chapter 2 of "CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting" (585-215-956).

Setting Up the CMS application

Prerequisites

- 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 Chapter 2 of "CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting" (585-215-956).

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.

Procedures

For Feature Package installation procedures, see “Installing Feature Packages”, in Chapter 2 of “CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

Setting up the remote console

Overview

Redirecting the remote console port allows the TSC to dial in and do 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, the standard provisioning convention is to use Port A for Enterprise 3000 and 3500 platforms and Port B for Ultra 5 platforms.

Hardware Platform	Port A	Port B
Enterprise 3000 Enterprise 3500	Remote Console	Not used
Ultra 5	Not used	Remote Console

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 Chapter 2 of “CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

Setting Up the Alarm Origination Manager

Overview

The setup for 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 for some reason 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 Chapter 2 of “CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

Setting up the NTS

For information about setting up the NTS, see “Setting up the NTS”, in Chapter 2 of “CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

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 Chapter 2 of “CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

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 3-13. 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 3-12 for this migration.

Procedure

For all versions of CMS Release 3, the system administration data is migrated 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, CMS must be turned off and a second setup of the CMS software must be performed.

1. Log in to CMS.

   The CMS main menu is displayed.

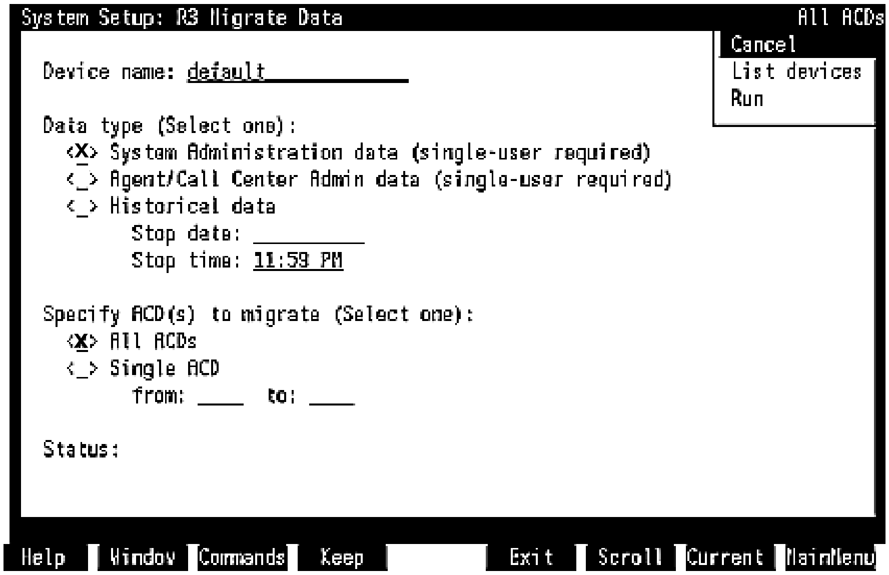
2. Select `System Setup - CMS State` from the CMS main menu and select the **`Single User`** `Mode` option

3. Insert the backup tape that contains the latest version of the admin data into the tape drive on the new HA server.

4. Select the `System Setup` -> `R3 Migrate Data` option from the CMS main menu.

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

5. 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

 Device name: default

 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:
```

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

7. Select the `Run` option and press Enter.

   The `Status:` field reports the progress of the migration. When the migration ends, `Status:` indicates the success or failure of the run.

8. 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. When the migration ends, `Status:` indicates the success or failure of the run.

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

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

NOTE:

Printer administration must be done on the new HA server before this step can be performed.

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 the `Maintenance` option from the CMS Main Menu.

   The `Maintenance` options window is displayed.

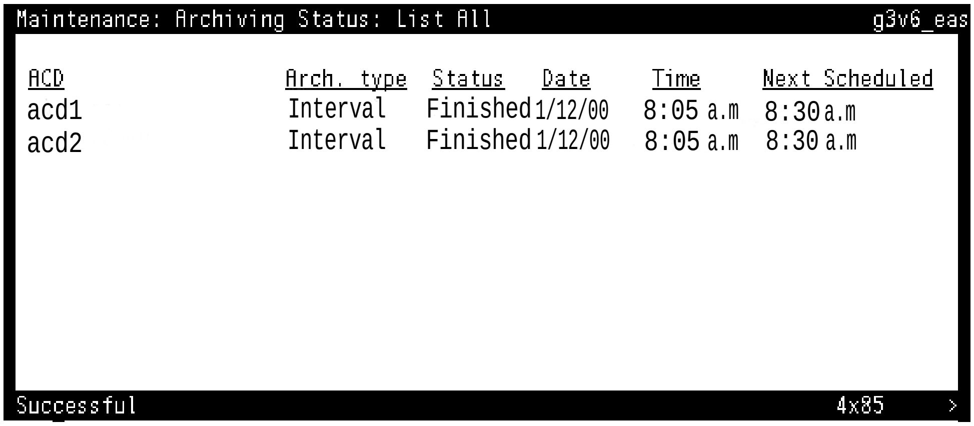
2. Cursor down to the `Archiving Status` option and press Enter.

   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 move the active cursor to 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                                  g3v6_eas

 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. Alternately, 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 Definity 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 4-1.

After the switch is re-administered, 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, administration of the switch for the new CMS version and HA dual links, followed by startup of data collection on the new HA server, should be completed as quickly as possible.

NOTE:

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

Performing an Incremental Maintenance backup

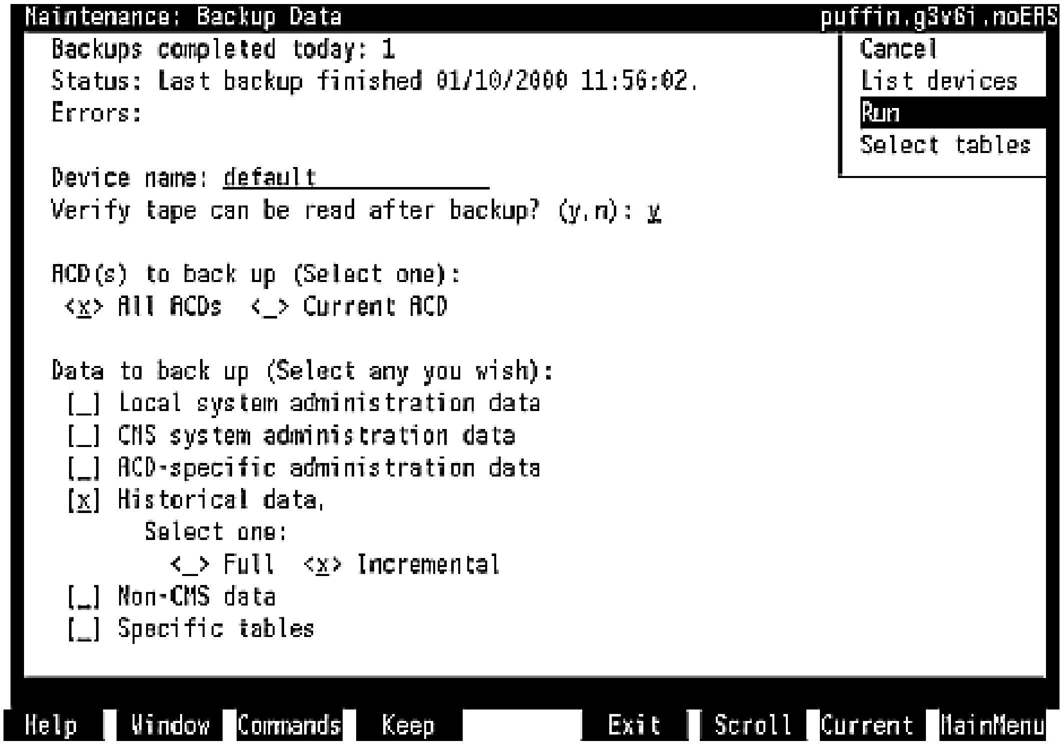
Perform an incremental maintenance backup (historical data only) on the original server. Begin the server upgrade immediately after the backup completes.

Procedure

1. From the CMS main menu, select the `Maintenance - Back Up Data option.`

   The Back Up Data window is displayed. Only select 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                                   puffin.g3v6i.noEAS
  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
   [_] ACD-specific administration data
   [x] Historical data.
         Select one:
           <_> Full  <x> Incremental
   [_] Non-CMS data
   [_] Specific tables
```

2. After you have selected the appropriate options for the backup, press enter to access the action list in the upper right corner of the window, cursor to the Run option and press enter to start the backup.

Upgrade the original CMS server

As soon as the incremental backup (preceding procedure) is successfully completed on the original server, the original server can be powered down, the CVUE 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 3-15.

By the time the upgrade of the original server is completed and data collection is turned on, the new HA server should already 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

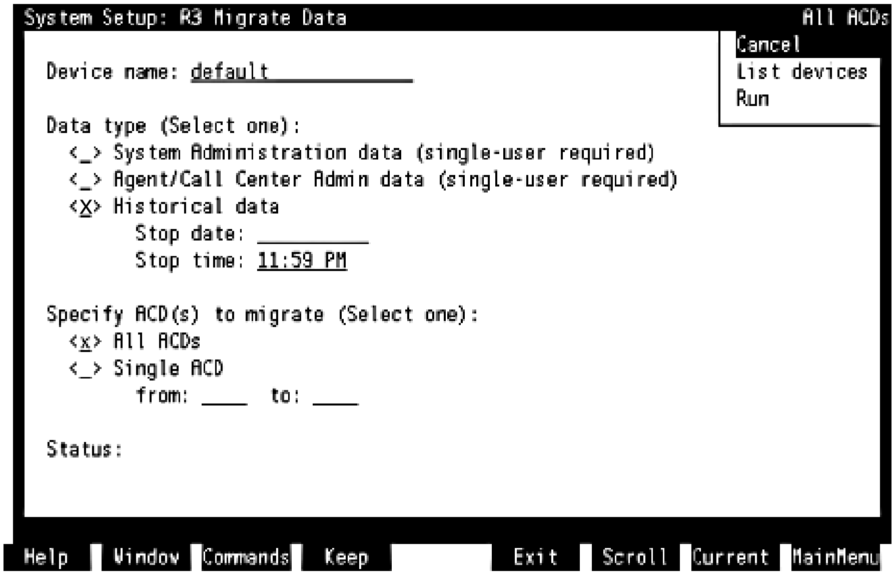
This procedure migrates CMS historical data from the second incremental maintenance backup ("Performing an Incremental Maintenance backup" on Page 3-25) onto the new HA server.

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. Install the incremental maintenance backup tape (which contains incremental historical data) into the tape drive on the new HA server.
2. Select the `System Setup` -> `R3 Migrate Data` option 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)
   <_> Agent/Call Center 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
   <_> Single ACD
         from: ____  to: ____

 Status:
```

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

5. Select the `Run` option and press Enter.
6. The `Status:` field reports the progress of the migration. When the migration ends, `Status:` indicates the success or failure of the run.
7. When the migration is finished, remove the incremental tape from the drive and insert the original full maintenance backup (“Performing a Full Maintenance backup” on Page 3-12) and repeat steps 2 through 6.
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.

NOTE:

Printer administration must be done on the new HA server before this step can be performed.

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 3-13) 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, CMS must be turned off and a second setup of the CMS software must be performed.

Migrate the Administration Data

Insert the initial maintenance backup tape back into the tape drive of the original server.

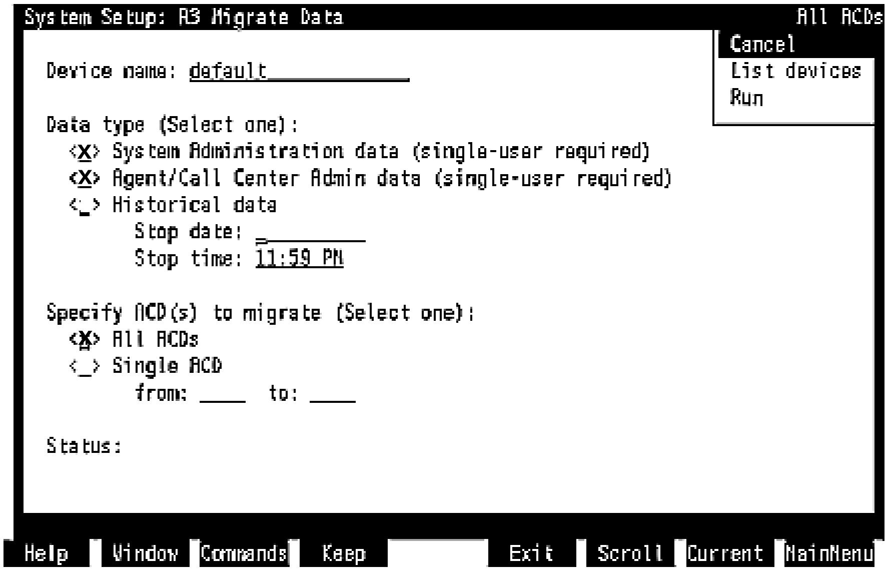
1. Log in as a CMS user.

   The CMS main menu is displayed.

2. Select `System Setup - CMS State` from the CMS main menu and select the **`Single User`** `Mode` option.

3. Select the `System Setup` -> `R3 Migrate Data` option from the CMS main menu.

   The `System Setup: R3 Migrate Data` window is displayed. 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):
    <X> System Administration data (single-user required)
    <X> 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:
```

4. After you verify that the correct options are selected, press enter to access the action list in the top right corner of the window.

5. Select the `Run` option and press Enter. The `Status:` field reports the progress of the migration. When the migration ends, `Status:` indicates the success or failure of the run.

6. Select `System Setup - CMS State` from the CMS main menu and select the **`Multi User`** `Mode` option.

7. Verify that data collection is on for all ACD links.

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 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 3-12.

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

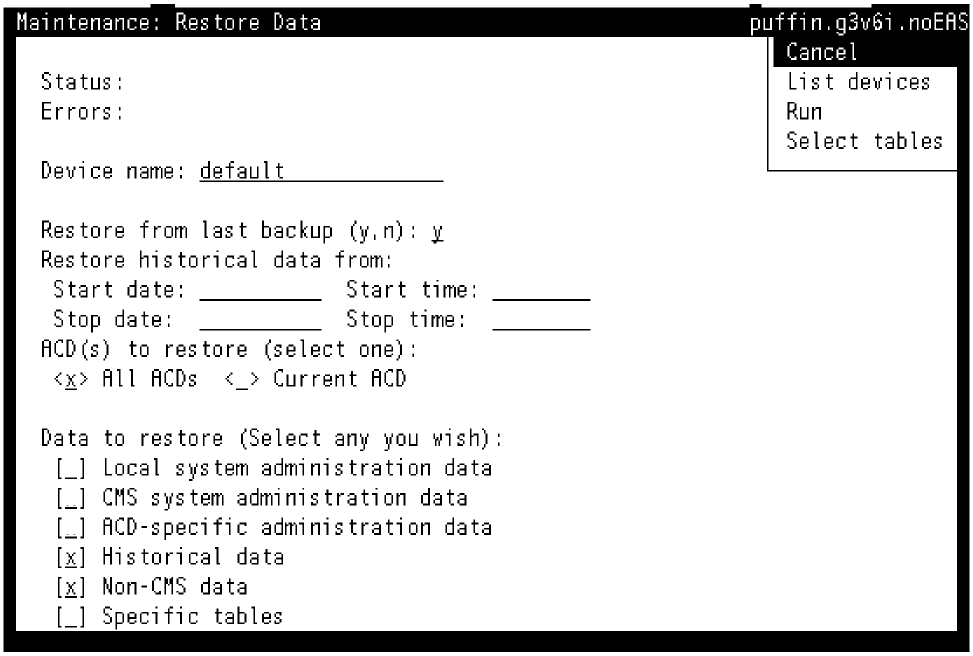
This procedure copies historical data from the Full Maintenance backup created in the preceeding procedure.

Procedure

1. Insert the Full Maintenance Backup 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. In the Data to Restore fields, select the `Historical data` and `Non-CMS data` options, as illustrated in the following figure:



```
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
 [_] CMS system administration data
 [_] ACD-specific administration data
 [x] Historical data
 [x] Non-CMS data
 [_] Specific tables
```

4. 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, 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 should read 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.

Performing CMSADM backups on the HA servers

Once both servers are fully operative, CMSADM backups must be performed on each server as soon as possible. The CMSADM file system backup saves all system files (excluding CMS call data). These backups must be stored 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 3-8.

Administering the switch for CMS HA systems

Overview

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

The switch administration procedures described in this chapter apply to the following Definity switches:

- Generic 3si (G3si)
- Generic 3r (G3r)
- Generic 3csi (G3csi)

For additional information about switch administration, refer to the appropriate Definity administration documents.

Multiple ACDs (switches) on HA systems

If the customer has purchased 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 Definity switch must be optioned with a switch version of V8 or later, Call Center Release 8.1 or later, and Adjunct CMS Release of R3V8 or later, as specified below in “Determining switch/CMS compatibility” on Page 4-3.

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 this chapter are applicable whether you are setting up one switch or eight switches; each switch requires a link to the CMS computer.

Setting up version and release values

This section 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 setting up version and release values include:

- setting the G3 Version on the System Parameters Customer Options form
- setting the Call Center Release on the System Parameters Customer Options form
- setting up the Adjunct CMS Release on the System Parameters Features form.

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

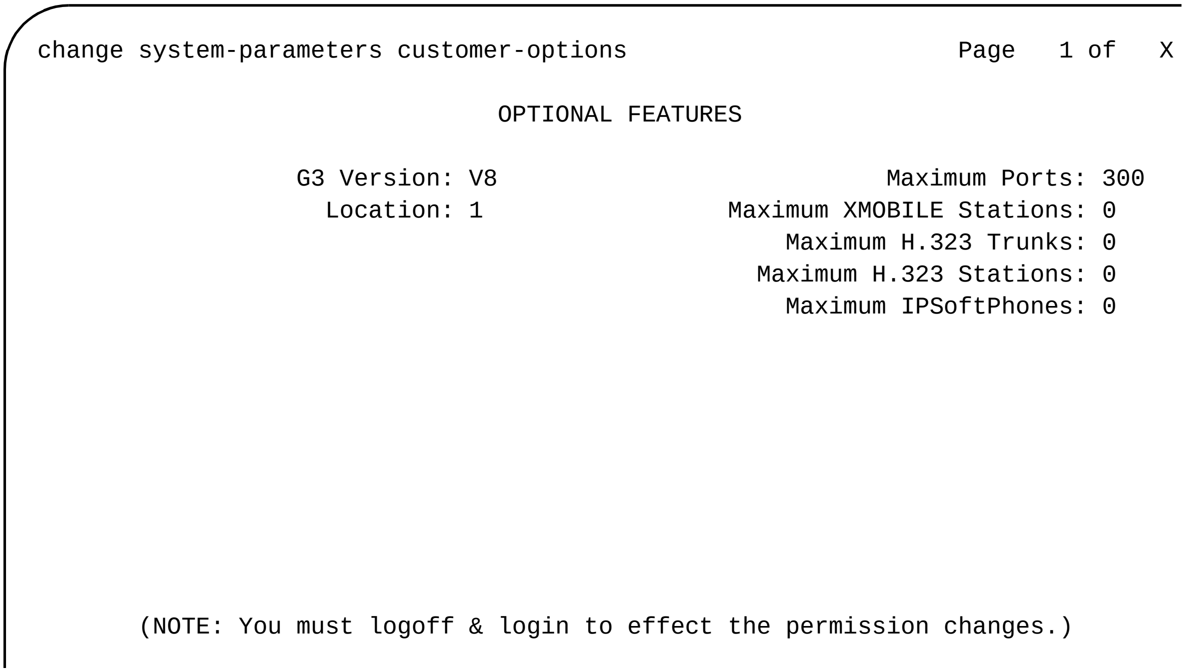
Determining switch/CMS compatibility

The following table reflects how you should 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 access to all of the features of the most recent release.

Switch Release	Definity 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

Setting the switch version

Use Page 1 of the System Parameters Customer Options form to set the switch version.

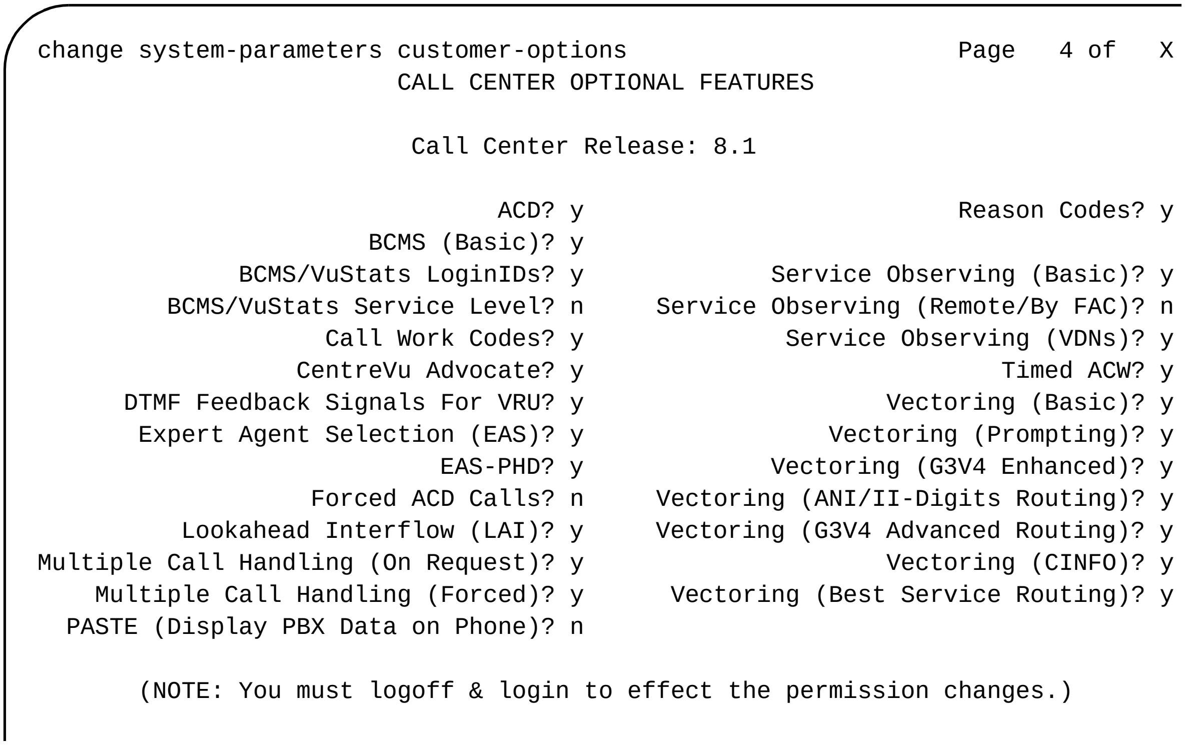


```
change system-parameters customer-options                       Page   1 of   X

                                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.)
```

Field	Definition
G3 Version	To enable the HA option, enter V8 or later, depending on the software release of the switch. If you set this field to an earlier release number, you will not have access to the latest switch features.

Setting the call center release

Use Page 4 of the System Parameters Customer Options form to set the Call Center Release. This is a new field introduced with R8.

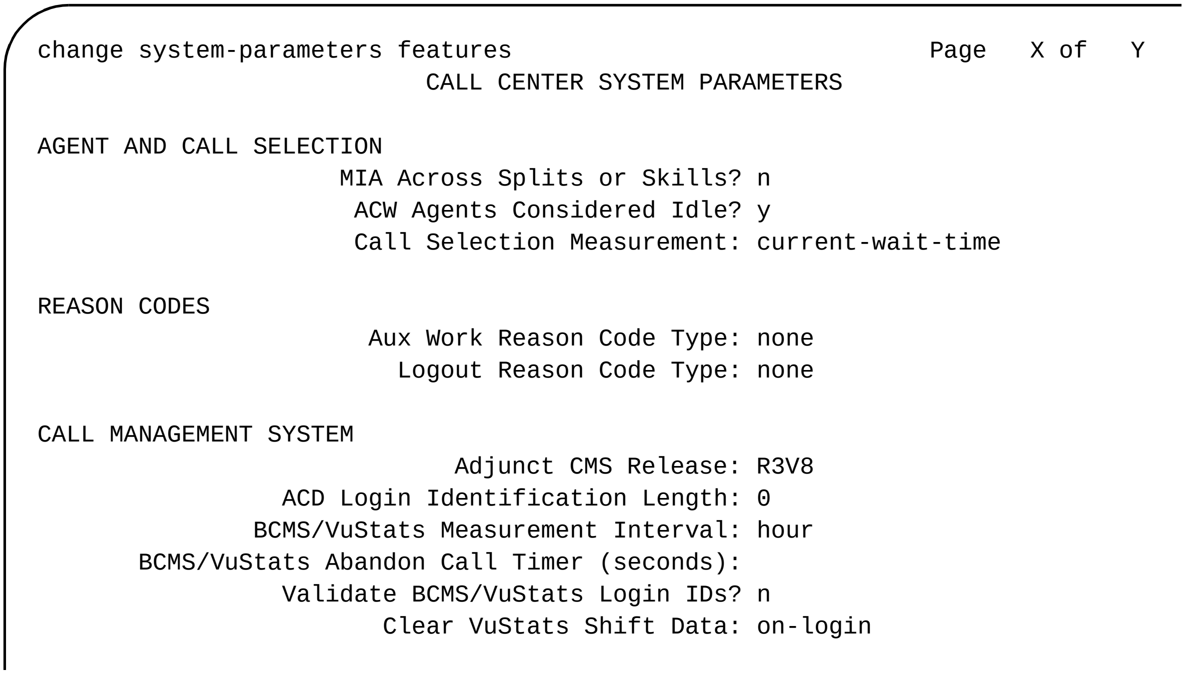


```
change system-parameters customer-options                      Page   4 of   X
                         CALL CENTER OPTIONAL FEATURES

                          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.)
```

Field	Definition
Call Center Release	The Call Center Release must be set to 8.1 (or later) to use the High Availability option.

Setting the adjunct CMS release

Use the System Parameters Features form to set the Adjunct CMS Release. Depending on switch release, this field can be found on different pages.



```
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
```

Field	Definition
Adjunct CMS Release	The Adjunct CMS Release must be set to R3V8 or later to use the High Availability option.

Setting up the link on the CMS computer

The following information must be obtained to set up the CMS link:

- switch name
- switch model (release)
- is Vectoring enabled on the switch (if authorized)?
- is Expert Agent Selection (EAS) enabled on the switch (if authorized)?
- does 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, also set the local and remote ports to 10.

- the IP address or hostname, and TCP port

In addition to the switch administration presented in this chapter, you must also set up the switch link on the CMS computer using the `setup` or `swsetup` options of the `cmssvc` command. See “CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance and Troubleshooting” (585-215-956).

Administering the Definity switch

Overview

This section 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. This section contains examples of the switch administration forms, with detailed explanations for the required fields. Use the forms in the order shown.

Form	Purpose
change node-names (Release 8 switch) change node-name IP (Release 9 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

This procedure is required only for Definity G3csi switches.

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

```
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
```

Field	Definition
Packet Intf2	Enter y to add a second packet interface.
Bus Bridge	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.
Inter-Board Link Timeslots — The total number of timeslots allocated cannot be greater than 11.	
Inter-Board Link Timeslot Pt0	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.

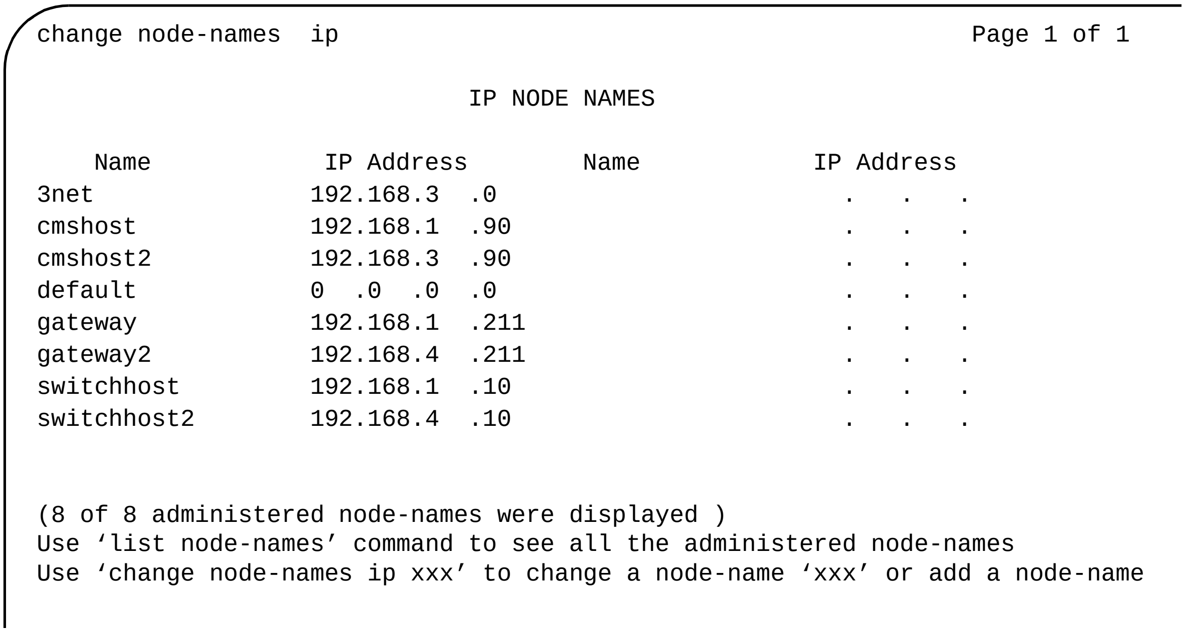
Field	Definition
Inter-Board Link Timeslot Pt1	Enter the number of timeslots (1-3) used by this port. Port 1 is a low traffic port and should always be set to `1`.
Inter-Board Link Timeslot Pt2	Enter the number of timeslots (1-3) used by this port. Port 2 is a low traffic port and should always be set to `1`.

Adding Node Names and IP Addresses

For the HA option, assign two switch node names and two CMS computer node names. Use Pages 2 through 6 of the Node Names form to assign the name and IP address of the CMS computers and all switches networked with the CMS computer.

NOTE:

Page 1 of the Node Names form is reserved for Intuity™ administration.

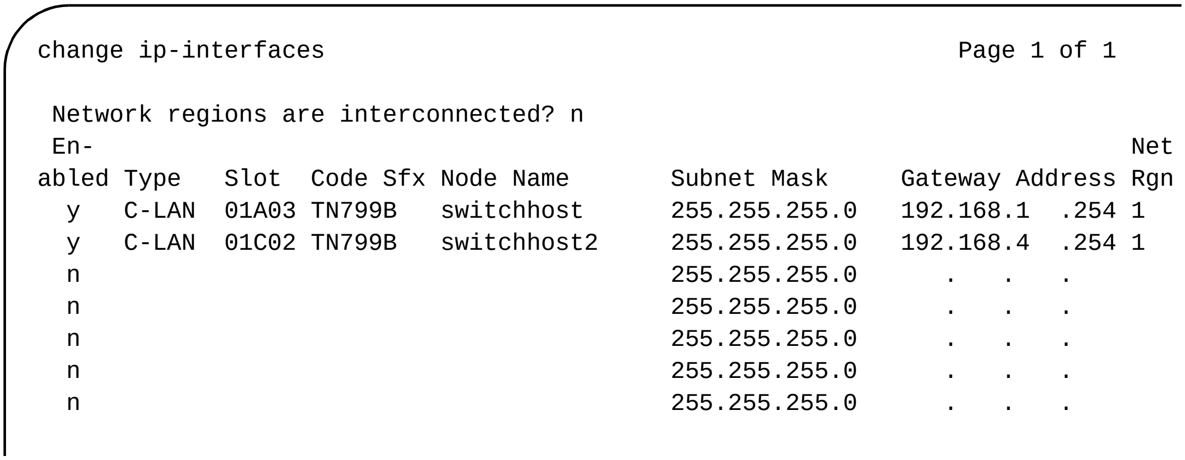


```
change node-names  ip                                            Page 1 of 1

                              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
```

Field	Definition
Name	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 CentreVu *CMS Software Installation and Setup* 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.
IP Address	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.

Adding a C-LAN IP Interface

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



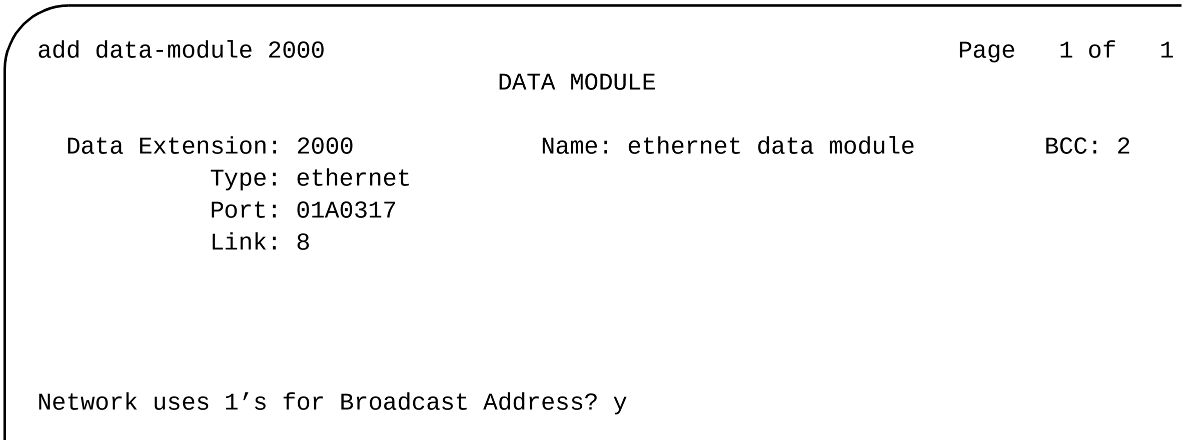
```
change ip-interfaces                                                Page 1 of 1

 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      .   .   .
```

Field	Definition
Network regions are interconnected	Enter n. This application is not used for C-LAN.
Enabled	Enter y to enable the C-LAN IP interface. After initial administration, you must disable the interface before you make any changes.
Type	Enter C-LAN.
Slot	Enter the equipment location of the C-LAN circuit pack.
Code/Sfx	This is a display-only field that shows the designation number of the circuit pack installed in the specified slot.
Node Name	Enter the switch node name assigned on Pages 2 through 6 of the Node Names form. In this example, enter switchhost. The same node name cannot be assigned to two different IP interfaces.
Subnet Mask	Identifies which portion of an IP address is a network address and which is a host identifier. Use the default entry, or check with the LAN administrator on site if connecting through the customer’s LAN.

Field	Definition
Gateway Address	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.
Net Rgn	For a C-LAN IP interface, use `1`.

Adding an ethernet data module

Use the Data Module form to assign an ethernet data module (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.



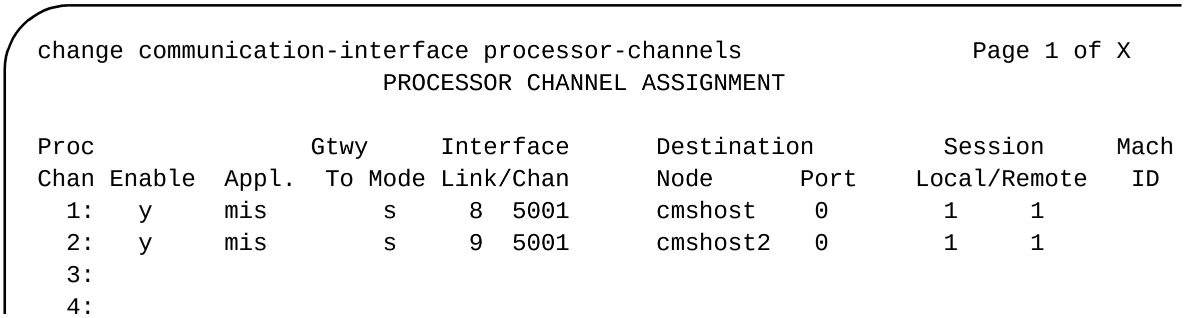
```
add data-module 2000                                              Page   1 of   1
                                DATA MODULE

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




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

Field	Definition
Data Extension	Enter an unassigned extension number.
Type	Enter `ethernet`.

Field	Definition
Port	Enter the equipment location of the C-LAN circuit pack (TN799). For the ethernet link, always use circuit 17 (for example, 01A0317).
Link	Enter a TCP/IP link number (1-25 for csi/si, 1-33 for r). This entry is also used on the Processor Channel form.
Name	Enter a name for the data module. This name will display when you list the assigned data modules.
BCC	A display-only field.
Network uses 1’s for Broadcast Address	This sets the host portion of the IP address to 0’s or 1’s. The default is yes (all 1’s). Use the default if the private network contains only Definity switches and adjuncts. Enter n only if the network includes non-Definity switches that use the 0’s method of forming broadcast addresses.

Adding the processor interface channels

Use the Processor Channel form to assign the processor channel attributes. With the High Availability option, you will assign two separate processor channels.



```
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:
```

Field	Definition
Proc Chan	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 G3esi or G3si switch.

Field	Definition
Enable	Enter `y`.
Appl	Enter `mis`.
Gtwy To	Not used for CMS.
Mode	Enter `s` for server.
Interface Link	Enter the TCP/IP link number used on the ethernet data module form.
Interface Chan	Enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup.
Destination Node	Enter the node name of the CMS computer as assigned on the Node Names form. In these examples, `cmshost` is used.
Destination Port	Use the default of `0`.
Session Local/ Session Remote	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.
Mach ID	Not used for CMS.

Adding IP Routing

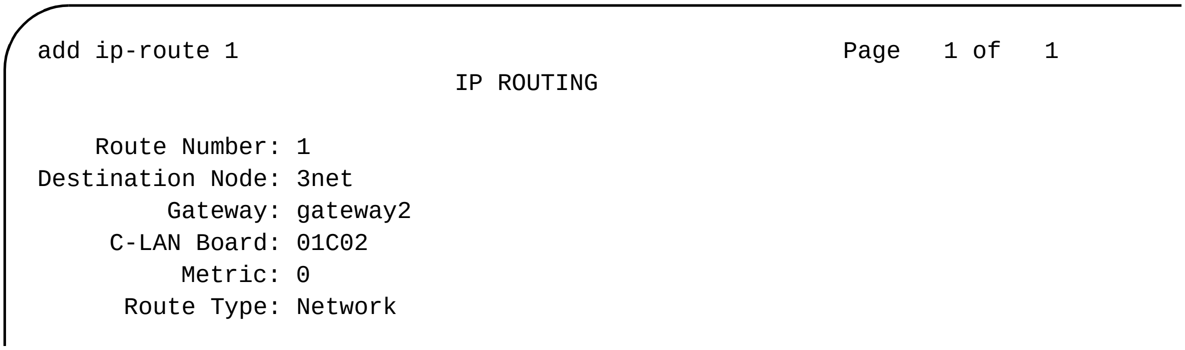
Use the IP Routing form to set up the IP route(s) from the switch to the CMS computer. This is required when:

- 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.

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
```

Field	Definition
Route Number	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 above shows a simple IP route.
Destination Node	This field represents the node name of the destination for this route. You would typically enter the node name for the CMS computer or a router, depending on your configuration.
Gateway	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.
C-LAN Board	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.

Field	Definition
Metric	Specifies the complexity of this IP route. Enter `0` if there are no intermediate nodes between the switch C-LAN port and the ethernet port on the CMS computer. A metric value of `1` is used only on a switch that has more than one C-LAN circuit pack installed. See *Definity ECS Administration for Network Connectivity* for more information about using this field.
Route Type (R8 switches, only)	Specifies whether the route is host or network (default). Use a Host route to get to a specific IP address. Use a Network route to get to a subnet.

Index

A

ACDs, multiple 4-2
administer
  switch LAN .3-18
  TCP/IP 3-18
administering
  LAN 4-7
Alarm Origination Manager, setup. 3-20
archive interval, checking 3-24

B

backup
  Admin data 3-13
  Full Maintenance 3-12
  incremental maintenance. 3-25
backup, CMSADM. 3-8
  prerequisites 3-9

C

cabling, ACD to CMS server. 2-9
CMS
  application setup 3-18
  authorizations, setting 3-16
  data storage parameters 3-17
  feature packages 3-19
  setting up on HA servers 3-15
configuration rules. 2-2
connecting
  single ACDusing serial ports 2-6
  to Definity switch 2-6
connecting Blocks 2-3
connecting blocks 2-3
Customer Support 1-6

D

Definity, switch administration. 4-6
distance limits
  Cat 5 cable 2-8

E

ethernet ports 2-7

F

FSBE. 2-7

H

Helplines, technical support 1-6
High Availability, defined. 2-1

L

LAN
  overview. 3-18
LAN connections
  hardware 2-8
LAN connectivity options. 2-6

M

migration
  administration data 3-28
  CMS historical data 3-27
  CMS system admin data 3-22
mirrored systems, alternate boot device 3-21

N

NTS
  administration 3-21
  setup 3-21

P

platforms
  combinations supported by High Availability . .1-2
  supported HA combinations. 1-2
ports, ethernet
  on CMS computers 2-7
primary server
  defined 1-1
  installed software 1-1

R

remote console
  designating ports 3-20
  setting up the software 3-19
restore, historical data 3-30
roles and responsibilities
  customer 1-5
  technical support personnel. 1-4

S

secondary server
- defined 1-1
- installed software 1-1

set Up
- remote Console 3-19
- switch LAN 3-18

set up
- TCP/IP. 3-18

software
- required and optional 1-3

software installation
- setting up remote Console 3-19

SunSwift 2-7

support 1-6

switch
- administration 3-25
- link. 3-18
- TCP/IP. 3-18

switch links
- connectivity options 2-6
- planning 2-3

switches
- support for High Availability 1-2
- supported releases 2-1

switch-over
- options. 2-1

system administration data, migrating 3-22

T

tape drive, verification. 3-6
- Enterprise 3000 3-7
- Ultra 5 3-7

TCP/IP 3-18

Technician Support 1-6

U

upgrade
- overview 3-2
- scenarios. 3-1

upgrades
- special considerations 1-4