Lucent Technologies
Bell Labs Innovations

CentreVu® Call Management System

Release 3 Version 8

High Availability Connectivity, Upgrade and Administration

585-215-105
Comcode 108678319
Issue 1
June 2000

Copyright© 2000 Lucent Technologies
All Rights Reserved
Printed in U.S.A.

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.

Your Responsibility for Your System's Security

Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system and, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your system manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The system manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use.

Lucent Technologies Fraud Intervention

If you *suspect that you are being victimized* by toll fraud and you need technical support or assistance, call Technical Service Center Toll Fraud Intervention Hotline at 1-800-643-2353.

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 and *DEFINITY* are registered trademarks of Lucent Technologies.

Sun, Sun Microsystems, SunOS, the *Sun* logo, *Solaris, Solstice, Solstice DiskSuite*, *Enterprise,* and *Ultra* are trademarks or registered trademarks of Sun Microsystems, Inc.

Exatape is a trademark of Exabyte Corporation.

INFORMIX is a registered trademark of Informix Software, Inc.

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

Ordering Information

Call: Lucent Technologies Publications Center
Voice: 1-800-457-1235
International Voice: +1-317-361-5353
Fax: 1-800-457-1764
International Fax: +1-317-361-5355

Write: Lucent Technologies Publications Center
P.O. Box 4100
Crawfordsville, IN 47933
U.S.A.

Order: CentreVu CMS R3V8 High Availability Connectivity, Upgrade and Administration
Document No. 585-215-105
Comcode 108678319
Issue 1, June 2000

For additional documents, refer to the section entitled "Related Documents" in the Preface.

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

Lucent Technologies National Customer Care Center

Lucent Technologies 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.

Document Support Telephone Number

Lucent Technologies provides telephone numbers for you to use to report errors or to ask questions about the information in this document. The support telephone numbers are:
Voice: 1-888-584-6366 and
International Voice: +1-317-322-6848.

European Union Declaration of Conformity

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

EMC Directive	89/336/EEC
Low Voltage Directive	73/23/EEC

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

Heritage Statement

Lucent Technologies—formed as a result of AT&T's planned restructuring—designs, builds, and delivers a wide range of public and private networks, communication systems and software, consumer and business telephone systems, and microelectronics components. The world-renowned Bell Laboratories is the research and development arm for the company.

Comments

To comment on this document, return the comment card at the front of the document.

Acknowledgment

This document was developed by the Lucent Technologies Information Development Organization for Global Learning Solutions.

CentreVu® Call Management System
Release 3 Version 8
High Availability Connectivity, Upgrade and Administration

Table of Contents

Introduction 1-1
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

Connecting HA Servers to the Switch 2-1
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. 2-5
Overview 2-5
LAN Connectivity Options 2-5
Ethernet Ports on a CMS Computer. 2-5

Upgrading CMS to the High Availability Option 3-1
Overview 3-1
HA Upgrade Scenarios 3-1
Overview of the HA Upgrade Procedure 3-3
Verifying the Tape Drive on an Enterprise 3000 Server 3-6
Tape Verification Procedure 3-6
Performing a CMSADM Backup 3-7
Overview 3-7
Prerequisites 3-7
Procedure 3-8
Performing a Full Maintenance Backup 3-11
Performing a Maintenance Backup (Administration Data Only) . . . 3-12
Procedure 3-12
Setting Up CMS on an HA Server 3-14
Overview 3-14
Prerequisites 3-14
Setting Authorizations 3-15
Setting Up Data Storage Parameters 3-21
Setting Up a LAN for Switch Connections 3-24
Setting Up the CMS Application 3-27
Installing Feature Packages. 3-46
Installing the Forecasting Package 3-46
Installing the External Call History Package 3-50
Setting Up the Remote Console 3-56
Overview 3-56
Platform Considerations 3-56
Administering the Remote Console Port 3-56
Redirecting the Remote Console Port to the Modem 3-57
Setting Up the Alarm Originator 3-59
Setting Up the NTS 3-59
Configuring the NTS. 3-59
Creating an Alternate Boot Device for Mirrored Systems 3-64
Migrating CMS System Administration Data to the New Server . . . 3-64
Procedure 3-64

Checking the Archive Interval 3-66
Administering the Switch 3-67
Performing an Incremental Maintenance Backup. 3-67
Procedure 3-67
Upgrade the Original CMS Server 3-68
Migrating CMS Historical Data to the New HA Server 3-69
Migrating Administration Data Back Onto the Original Server . . . 3-70
Migrate the Administration Data 3-70
Performing a New Full Maintenance Backup and Restore 3-72
Performing the Full Maintenance backup on the new HA server . 3-72
Restoring historical data to the original server 3-72
Procedure 3-72
Performing CMSADM Backups on the HA Servers 3-74

Administering the Switch for CMS High Availability Systems 4-1
Overview 4-1
Multiple ACDs (Switches) on HA Systems 4-1
Setting Up Version and Release Values 4-2
Overview 4-2
Determining Switch/CMS Compatibility 4-2
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. 4-7
Overview 4-7
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 Lucent Technologies *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 recieved
- separate network subnet connections for paired ACD-CMS combinations

HA system redundancy of critical hardware components greatly reduces the possibility of 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 and system administration software on dual-CLAN enabled Definity switches is configured to allow simultaneous communication via dual ACD links. Each link connects to a separate CMS server. ACD data transmission is routed through paired C-LAN circuit cards on the switch and traverses separate TCP/IP over Ethernet subnets to a CMS server (X.25 protocol is not supported on HA systems).

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 should be installed only on the primary server
- most (but not all) CMS administration changes should be 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, for some administrative tasks, 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 Lucent Technologies 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 be brought down for maintenance, the remaining unit is fully capable of carrying the full CMS activity load without interuption.

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* R8

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

*_Ultra_ is a trademark of Sun Microsystems, Inc.
†_Enterprise_ is a trademark of Sun Microsystems, Inc.

Required and Optional Software

The HA option is supported only for CMS servers using CMS software version R3V8, or later. With a few exceptions (noted below), software configurations for the HA primary and secondary servers are identical, and also correspond to the standard (non-HA) CMS software configuration. Also (with the exceptions listed below) a complete set of CMS R3V8 software packages is provided for the second server on CD media at no additional charge. For a complete list of required and optional software packages for CMS R3V8, see Chapter 1 in "*CentreVu Call Management System Software Installation and Setup* (585-210-941)".

For primary and secondary servers deployed in HA systems, the following exceptions to the standard CMS R3V8 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 HA systems).

General Roles and Responsibilities

This document is written for Lucent Technologies 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. User responsibilities are described in detail in “CentreVu Call Management System Release 3 Version 8 High Availability User Guide” (585-210-931).

Task
Retention of CMS documentation and software
For those administration changes which are non-transferrable 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 Lucent Technologies technicians can call the numbers shown 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.lucent.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 Lucent Technologies representative or distributor for more information.

Technician Support for U.S. and Canada

1-800-248-1234

Lucent Technologies 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* Release 8.1 switches:

- 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. **Customized software switch-over**

   If the HA primary and secondary servers connect to CMS clients and other peripherals, such as NTS servers, printers, etc. over the same network subnet, LAN traffic on this “user” network can be automatically redirected from the primary to the secondary server by means of customized scripting tools. The scripts, which are set up by PSO, create an alias for the IP address of the primary server on the secondary server.

3. **Manual server switch-overs**

   If the customer is unable to connect the two HA servers to the “user” network via a common network subnet, the custom software switch-over solution offered by the PSO can not be implemented. Therefore, if the customer still desires uninterrupted access to their CMS data, the server switch-over must be performed manually.

   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 duplication) of NTS servers, physical reconnection of peripheral devices, etc. Customers considering the manual switch-over option must be strongly encouraged to 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 (standard CMS) ACD links and HA dual links, is not supported. If implemented, mixed ACD links could potentially result in significant call data loss, and could also fill up system error logs with meaningless data.

Link connections are implemented only by the TCP/IP over ethernet LAN communications protocol, and 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 High Availability 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. You should also take into account if the Intuity™ AUDIX® product will be part of the LAN. You must coordinate the setup of that system with the switch and the CMS. Some of the information needed includes:

- 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):
     — Recommended option for HA systems, most robust and reliable, no dependency on customer's network
     — Hubs are used to make the connections; up to four hubs can be used to extend distances
     — Crossover cable can be used instead of hubs (with flipped transmit/receive leads)
  b. Customer LAN with private segment:
     — Uses switch or router to provide a private collision domain
     — Minimal dependency on customer's network
     — 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 questions:

— 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 questions:

— IP address of C-LANs, adjuncts, and gateways

— Node names of C-LANs, adjuncts, 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 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 information described above, the Lucent Technologies technician will be unable to complete the installation.

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. This method has the advantage of ensuring that the LAN connection is private, since a hub is not included in the configuration, but is not recommended for HA systems.

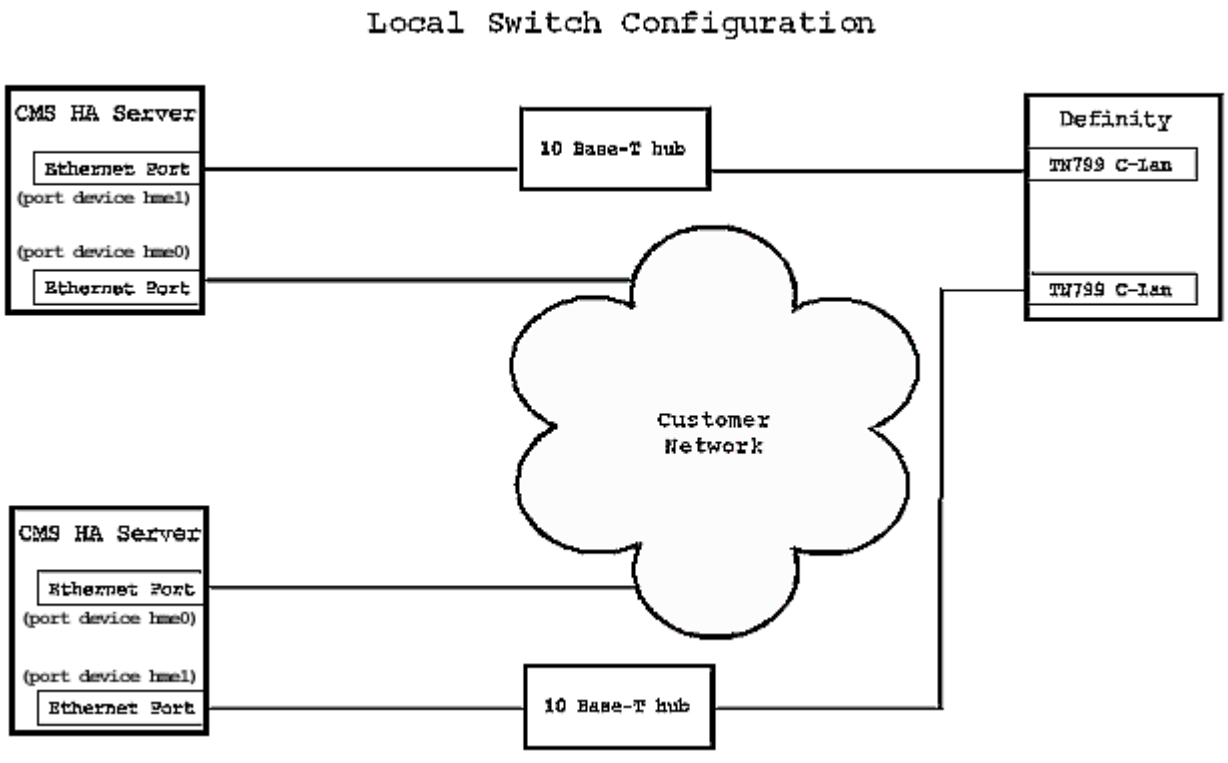
If the customer requires a link connection by means of crossover cables or other methods not described above, general descriptions and requirements for alternate connectivity setups are described in *CentreVu Call Management System Switch Connection and Administration* (585-215-876).

Ethernet Ports on a CMS Computer

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.

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

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



Note:

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

Connecting with a 10Base-T Hub

Connecting through a 10Base-T hub LAN connection is the recommended method 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	102631413
	258B adapter, or	103923025
	356A adapter, or	104158829
	Category 5 cross-connect hardware and connecting block	N/A
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

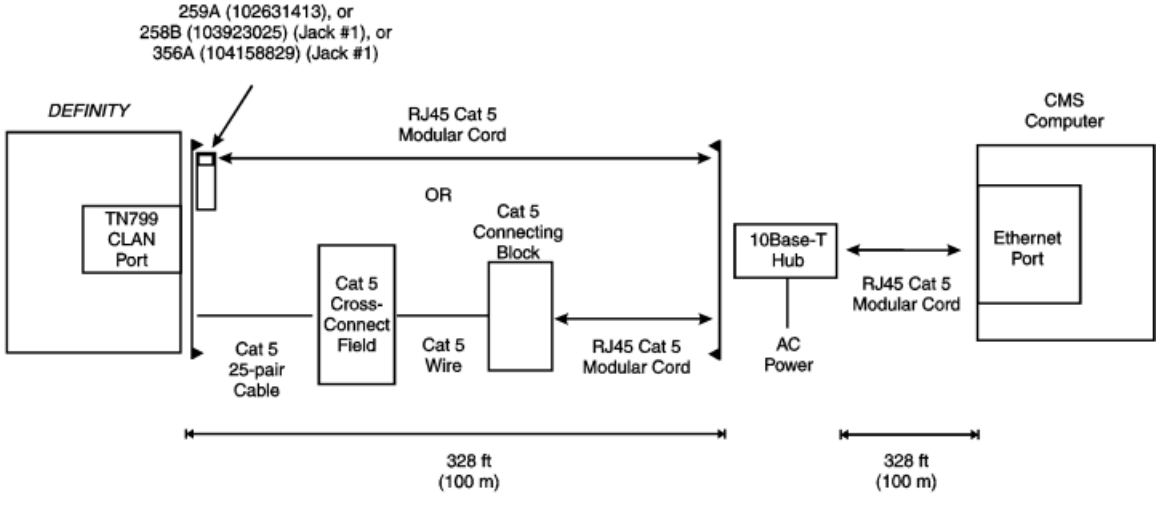
*Parts for which no comcode is displayed must be obtained by the customer prior to the scheduled upgrade.

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 2-8.

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

Cabling Diagram - LAN via 10Base-T Hub



Upgrading CMS to the High Availability Option

Overview

Upgrading CMS to the High Availability Option describes CentreVu Call Management System (CMS) upgrade procedures required to add a new CMS server to 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 through a Lucent Speed Centre facility.

HA Upgrade Scenarios

Two CMS servers to be incorporated into an HA system must be installed with the same version (R3V8 or later) and base load of 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). **Due to the simplified logistics associated with creation of a new HA system when the original server is already installed with the correct CMS version, this document does not describe upgrade scenarios in which a full CMS version upgrade is not required.**

In contrast, when the original server is installed with a pre-R3V8 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 that minimizes system downtime and the 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 Procedure

The steps required to perform an HA upgrade when the original server requires a full CMS version upgrade are described below and depicted in the accompanying figurePage 2-5.

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-R3V8) 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.

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

5. On the day of the upgrade, the Lucent 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.

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 R3V8 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 to install the new drives from the Speed Centre.

10. After the Speed Centre disks are installed 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.

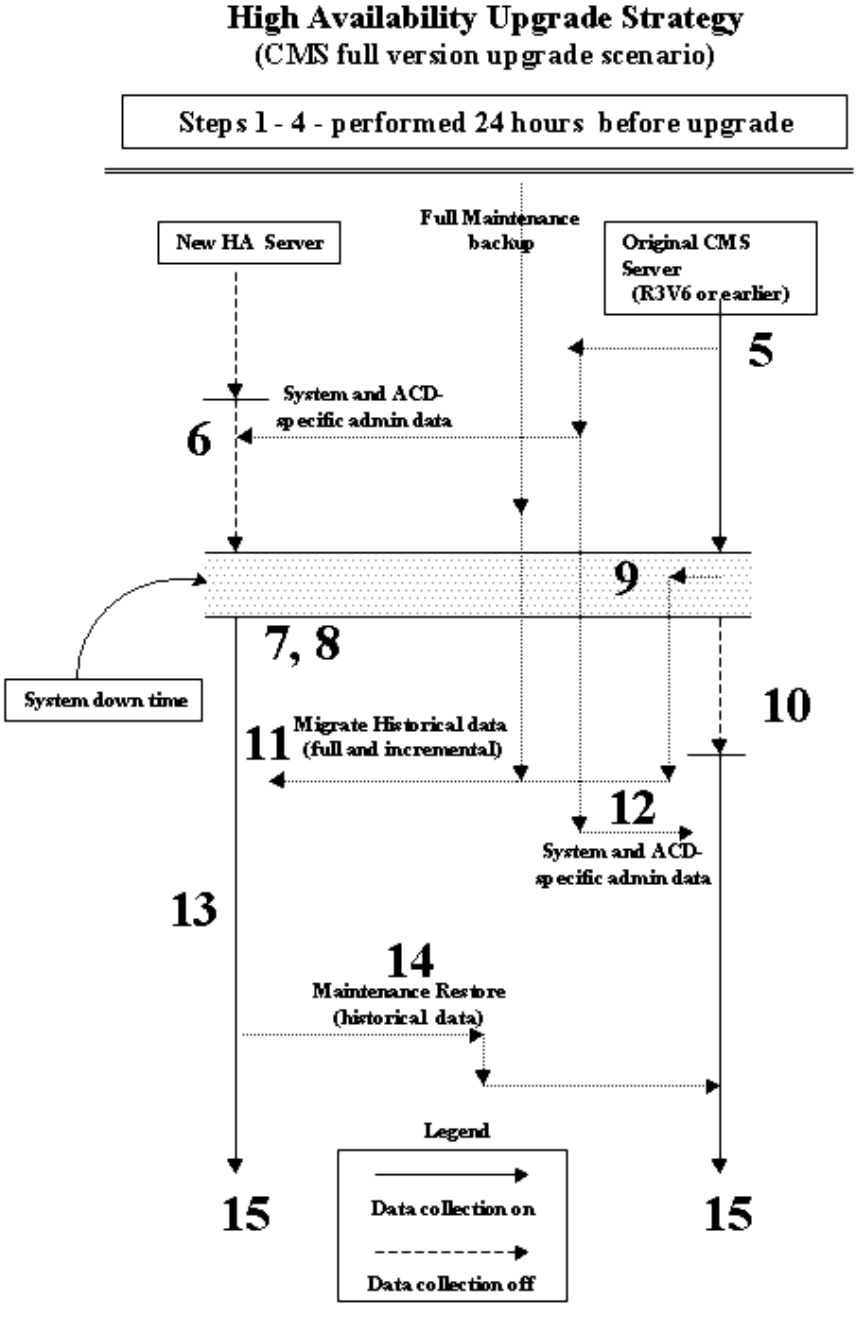
14. Restore the historical data from the full maintenance backup tape (created in the preceeding step) onto the original server.

    The two servers now share the same initial set of administrative data; **CMS users can now resume (or start) 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 R3V8 High Availability User Guide*" (585-210-931).

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



Verifying the Tape Drive on an Enterprise 3000 Server

This procedure is required only for Ha systems which use an E3000 - E3500 platform combination for the primary and secondary servers.

WARNING!

After the original tape drive on an Enterprise 3000 is replaced with an Exabyte Mammoth 20-40 Gbyte 8 mm drive, the customer must discard any old tapes which were formerly used with the old drive. Reuse of old tapes on the replacement drive will result in damage to the tape device.

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).

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

Tape Verification Procedure

If a tape device change-out was required, perform the following steps to confirm that the old tape drive was replaced:

Insert an 8mm 170m AME tape cartridge in the tape drive on the Enterprise 3000 server 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
```

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 perfomed 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 (r3v8xx.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 4a.

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.

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:

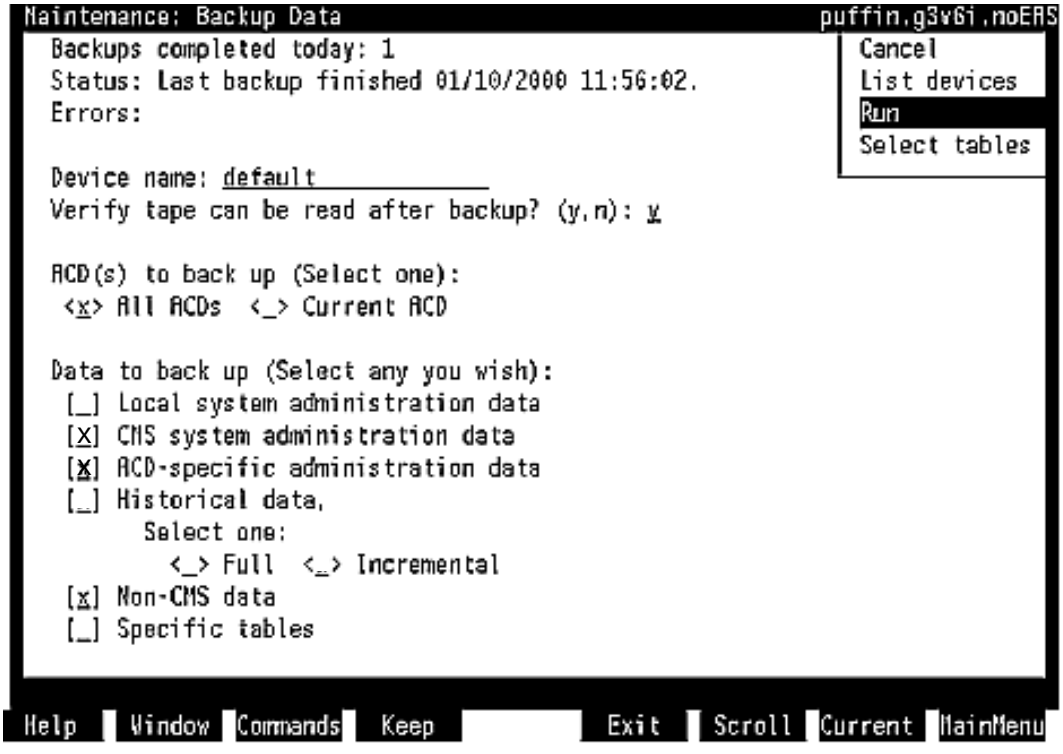
   - CMS System Administration data
   - ACD-specific admin data
   - Non-CMS data

   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:



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 been upgraded with new disk drives supplied by a Lucent Speed Centre facility).

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.

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's 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 High Availability Systems" on Page 4-1.

- Connected the NTS and the CMS computer to the network hub unit. See *CentreVu® CMS R3V6 Sun® Enterprise™ 3000 Computer Connectivity Diagram* (585-215-865), *CentreVu® CMS Sun® Enterprise™ 3500 Computer Hardware Connectivity Diagram* (585-215-877), or *CentreVu® CMS Sun® Ultra™ 5 Computer Connectivity Diagram* (585-215-872).

Setting 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.

You can use the `auth_set` option in the CMS Services menu (`cmssvc`) to do the following:

- Set the purchased version of CMS
- Authorize the following packages and features, if authorized by the customer:
  - Forecasting
  - Vectoring
  - Graphics
  - External Call History
  - Expert Agent Selection (EAS)
  - External Application
  - Vector Directory Numbers (VDNs)
  - *CentreVu* Supervisor
  - *CentreVu* Report Designer.
- Change the number of agents, ACDs, or Supervisor logins.

Procedure

1. Access the CMS Services menu by entering the following command:

   `cmssvc`

   The program responds:

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

Select a command from the list below.
  1) auth_display Display feature authorizations
  2) auth_set     Authorize capabilities/capacities
  3) run_cms      Turn CentreVu CMS on or off
  4) setup        Set up the initial configuration
  5) swinfo       Display switch information
  6) swsetup      Change switch information
  7) patch_inst   Install a single CMS patch from
  8) patch_rmv    Backout an installed CMS patch
  9) load_all     Install all CMS patches found on CD
 10) back_all     Backout all installed CMS patches from machine
Enter choice (1-10) or q to quit:
```

2. Enter `2` to select the `auth_set` option. The program responds:

```
Password:
```

3. Enter the cms services password. This password is available only to authorized personnel.

   NOTE:

   Some of the following questions may not appear if the authorization cannot be changed at this time.

   The program responds:

```
Is this an upgrade? (y/n):
```

   NOTE:

   This question occurs the first time you run `auth_set` on the system.

If this is not an upgrade and you enter n, the program responds:

```
Purchased version is R3V8. Is this correct? (y/n):
```

4. Enter y.

   NOTE:

   The program uses the above information to populate the "Purchased CMS Release" field of the *System Setup:Switch Setup* screen.

   The program continues with the following questions:

```
Authorize installation of forecasting package? (y/n):(default: n)
```

5. Enter y if the customer purchased Forecasting; otherwise, press Enter. The program responds:

```
Authorize installation of vectoring package? (y/n): (default: n)
```

6. Enter y if the customer purchased vectoring; otherwise, press Enter. The program responds:

```
Authorize use of graphics feature? (y/n): (default: n)
```

7. Enter y if the customer purchased Graphics; otherwise, press Enter. The program responds:

```
Authorize use of external call history feature? (y/n): (default: n)
```

8. Enter y if the customer purchased the External Call History feature; otherwise, press Enter. The program responds (if the vectoring package is authorized):

```
Authorize use of expert agent selection feature? (y/n): (default: n)
```

9. Enter y if the customer purchased the Expert Agent Selection feature; otherwise, press Enter. The program responds:

```
Authorize use of external application feature? (y/n):
(default: n)
```

10. Enter y if the customer purchased the External Application feature; otherwise, press Enter. The program responds:

```
Authorize use of more than 2000 VDNs (yes turns off VDN
permission checking)? (y/n): (default: n)
```

11. Enter y if the customer needs to use more than 2000 VDNs; otherwise, press Enter. The program responds:

```
Enter the number of simultaneous Lucent Technologies CentreVu(R)
Supervisor logins the customer has purchased
(2-250): (default: X)
```

12. Enter the number of simultaneous logins purchased. The program responds:

```
Has the customer purchased Lucent Technologies CentreVu(R)
Report Designer? (y/n): (default: n)
```

13. Enter y if the customer purchased report designer; otherwise, press Enter. The program responds:

```
Enter the maximum number of split/skill members that can be
administered (1-10000): (default: 1)
```

14. Enter the maximum possible number of split or skill members that the customer might use based on the switch agent size purchased.

    For R3V8, “split or skill members” are defined as the number of CMS-measured agent-split and agent-skill combinations logged in at the same time. Each split an agent logs into is an agent-split combination. Each skill assigned to an agent while logged in is an agent-skill combination. The recommended numbers for Expert Agent Selection (EAS) and non-EAS systems are shown in the following table.

Switch Agent Size Range Purchased	Number of Split or Skill Members	
	Non-EAS	EAS
0-12	100	500
0-25	100	500
0-50	200	1000
0-75	300	1500
0-100	400	2000
0-200	800	4000
0-300	1200	6000
0-400	1600	8000
0-500	2000	10000
0-600	2400	10000
0-max. agents	10000	10000

NOTE:

The minimum size configuration for CMS is 0-25; that is the reason groups 0-12 and 0-25 have the same provisioning. You should also note that the customer will be able to limit the split or skill random access memory (RAM) allocation to the size actually needed for the current configuration of agents and splits or skills. That is accomplished by the “Total split/skill members summed over all splits/skills” field, which is accessed through the `setup` option of the `cmssvc` command.

The program responds:

```
Enter the maximum number of ACDs that can be installed (1-8):
(default: 1)
```

15. Enter the number of ACDs the customer purchased.

    The prompt displays and all authorizations have been set.

16. Verify that authorizations were set by entering the following:

    `tail /cms/install/logdir/admin.log`

    The `admin.log` file contains information relating to CMS administration procedures. The file should display the following message:

```
Capabilities/capacities authorized <date/time>
```

    You can also verify the authorizations by using the `auth_display` option of the `cmssvc` command.

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

Procedure

1. To change to the CMS installation directory, enter:

   ```
   cd /cms/install/cms_install
   ```

2. Enter:

   ```
   vi storage.def
   ```

   NOTE:

   If you delete or damage the `storage.def` file, you can find a copy of this file (`storage.skl`) in the same directory.

3. The default storage parameters are listed (immediately below each of the defined storage paremeters) in the order in which they appear in the storage.def file.

   - # Intrahour interval (15, 30, 60 minutes):

     30

   - # Week start day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday):

     Sunday

   - # Week end day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday):

     Saturday

- # Daily start time (regular time):

  12:00 AM
- # Daily stop time (data will be collected for seconds of last minute):

  11:59 PM
- # Number of agent login/logout records (0-999999):

  10000
- # Number of agent trace records:

  10000
- # Number of call records (0-5000 internal or 0-99999 external):

  0
- # Number of exceptions records (1-2000):

  250
- # Days of intrahour for splits (1-62):

  31
- # Days of daily splits (1-1825):

  387
- # Weeks of weekly splits (1-520):

  53
- # Months of monthly splits (1-120):

  13
- # Days of intrahour for agents (1-62):

  31
- # Days of daily agents (1-1825):

  387
- # Weeks of weekly agents (1-520):

  53
- # Months of monthly agents (1-120):

  13
- # Days of intrahour for trunk groups (1-62):

  31
- # Days of daily trunk groups (1-1825):

  387

- # Weeks of weekly trunk groups (1-520):

  53
- # Months of monthly trunk groups (1-120):

  13
- # Days of intrahour for trunks (1-62):

  31
- # Days of daily trunks (1-1825):

  387
- # Weeks of weekly trunks (1-520):

  0
- # Months of monthly trunks (1-120):

  53
- # Days of intrahour for call work codes (1-62):

  0
- # Days of daily call work codes (1-1825):

  0
- # Weeks of weekly call work codes (1-520):

  0
- # Months of monthly call work codes (1-120):

  0
- # Days of intrahour for vectors (1-62):

  31
- # Days of daily vectors (1-1825):

  387
- # Weeks of weekly vectors (1-520):

  53
- # Months of monthly vectors (1-120):

  13
- # Days of intrahour for VDNs (1-62):

  31

- # Days of daily VDNs (1-1825):

  387
- # Weeks of weekly VDNs (1-520):

  53
- # Months of monthly VDNs (1-120):

  13

4. After entering the appropriate values, enter:

   `:wq`

After the CMS application is running, the system administrator can change the data storage parameters using the Data Storage Allocation window and the Storage Intervals window in the CMS System Setup menu. For more information about changing ACD data storage parameters, see the CMS System Setup chapter in *CentreVu® CMS R3V8 Administration* (585-210-910).

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.*
- CMS must be turned off.
- All file systems must be mounted.

Procedures

To set up a network connection to an HA-enabled switch and other CMS computer peripherals, the following steps are performed:

- Edit the /etc/hosts file.
- Set up a second network interface.
- Edit the /etc/defaultrouter file.

Editing the `/etc/hosts` File

1. To save a backup copy of the file, enter:

   ```
   cp /etc/hosts /etc/hosts.old
   ```

2. To edit the `/etc/hosts` file, enter:

   ```
   vi /etc/hosts
   ```

3. Add a new line in this file for each ACD/switch that will connect to this computer using TCP/IP. Lines must also be added for any NTS devices installed on the system.

   ```
   192.168.2.1      cms
   192.168.2.101    cmsterm1
   192.168.2.102    cmsterm2
   192.168.1.2      cms_1
   192.168.1.11     switch1
   192.168.1.12     switch2
   ```

   This example shows the recommended default IP addressing scheme for the two ethernet ports installed on the server. The hostname “cms_1” represents the second network interface, which is on the same private subnet carrying the link to the switches. This example also shows the first ethernet port conncecting to two NTS servers (cmsterm1 and cmsterm2).

4. Press the Esc key to leave the edit mode.

5. Enter `:wq` to save and quit the existing file.

6. To edit the hostname files associated with the second network hostname created in `/etc/hosts`, enter one of the following:

   - On an *Enterprise* 3000 or *Enterprise* 3500 with a second FSBE card, enter the following:

     ```
     vi /etc/hostname.le0
     ```

   - On an *Enterprise* 3000, *Enterprise* 3500, or *Ultra* 5 with a second *SunSwift* card, enter the following:

     ```
     vi /etc/hostname.hme1
     ```

7. Add a line to this new file with the host name you added to the `/etc/hosts` file. For example:

```
cms_1
```

8. Press the Esc key to leave the edit mode.

9. Enter `:wq` to write and quit editing the file.

Editing the `/etc/defaultrouter` File

If the connection between the first network interface on the CMS computer connects through a customer network, you will have to set up a default network router.

1. To create a default router file, enter:

   ```
   vi /etc/defaultrouter
   ```

2. Add a line to this new file with the IP address for the default system router on the customer's network. This address must be obtained from the customer. For example:

```
192.168.1.254
```

3. Press the Esc key to leave the edit mode.

4. Enter `:wq` to write and quit editing the file

Turn Off IP Forwarding

To eliminate a potential security risk associated with the IP Forwarding function, enter:

```
touch /etc/notrouter
```

Setting Up the CMS Application

Overview

Use the procedures in this section to set up the CMS application.

Prerequisites

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

Setup Methods

You can set up the CMS feature package using one of two methods:

a. **Interactively from a terminal** — Using the interactive option, the program prompts you for the necessary information to set up the CMS application (for example, system type, number of agents, trunks, vectors, VDNs, and so on).

To set up the CMS application using this option, see "Setting Up CMS Interactively from a Terminal" in this chapter.

b. ***UNIX**** **System flat file** — Using the flat file option, you edit a *UNIX* System flat file containing the necessary information (for example, system type, number of agents, trunks, vectors, VDNs, and so on) to set up the CMS application. When you execute the program, it runs in the background and uses the *UNIX* System flat file data to set up the CMS application. To set up the CMS application using this option, see "Setting Up CMS Using a UNIX Flat File" in this chapter.

**UNIX* is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Setting Up CMS Interactively from a Terminal

Overview:

Using the interactive option, the program prompts you for the necessary information.

Procedure:

1. If you are not sure of the device path, do the following:
   a. Insert a tape into the tape drive.
   b. In another xterm window, enter the following commands:
      - `mt -f /dev/rmt/1c status`
      - `mt -f /dev/rmt/0c status`

   The correct device path will show information similar to the following example:

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

2. Access the CMS Services menu by entering the following:

   `cmssvc`

   The program responds:

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

Select a command from the list below.
  1) auth_display Display feature authorizations
  2) auth_set     Authorize capabilities/capacities
  3) run_cms      Turn CentreVu CMS on or off
  4) setup        Set up the initial configuration
  5) swinfo       Display switch information
  6) swsetup      Change switch information
  7) patch_inst   Install a single CMS patch from CD
  8) patch_rmv    Backout an installed CMS patch
  9) load_all     Install all CMS patches found on CD
 10) back_all     Backout all installed CMS patches from machine
Enter choice (1-10) or q to quit:
```

3. Enter `4` to select the `setup` option.

NOTE:

If system setup has already been done, the program responds:

```
Warning!!! Setup has already been performed.
Running this command will remove all CMS data in the database.
Do you wish to proceed and re-configure CMS? (y/n): (default: n)
```

4. Enter `y` to continue with the setup, or enter `n` to exit setup. If you enter `y`, the program responds:

```
Select the language for this server:

All languages are ISO Latin except Japanese. Selection of the
server language assumes that existing customer data is
compatible. (Upgrade from any ISO Latin language to any ISO
Latin language or from Japanese to Japanese is supported).

1) English
2) Dutch
3) French
4) German
5) Italian
6) Portuguese
7) Spanish
8) Japanese
Enter choice (1-8): (default: 1)
```

5. Enter the number for the language used on this system. If setup has been done previously, the customer CMS data is now initialized. When finished, the program responds:

```
Enter a name for this UNIX system (up to 256 characters):
(default: XXXXXX)
```

6. Press enter to accept the default.

   The program responds:

```
Select the type of backup device you are using
   1) SCSI QIC-150 cartridge tape - 150MB tape
   2) 40.0 Gbyte 8mm tape
   3) 14.0 Gbyte 8mm tape
   4) 5.0 Gbyte 8mm tape
   5) SCSI QIC-2.5 cartridge tape - 2.5GB tape
   6) SCSI 4-8 SLR cartridge tape - 4GB tape (8GB compressed)
Enter choice (1-6):
```

7. Enter the number to specify the type of cartridge tape you are using as the backup device. The program responds:

```
Enter the default backup device path:
(default: /dev/rmt/0c)
```

   Enter the default backup device path.

   The correct device path will show information similar to the following example:

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

8. After you enter the correct device path, the program responds:

```
Enter number of ACDs being administered (1-8):
```

9. Enter the number of ACDs to be administered. This number may be less than the number of ACDs authorized. The program responds:

```
Information for ACD 1

Enter switch name (up to 20 characters):
```

10. Enter the name for the switch associated with ACD 1. The program responds:

```
Select the model of switch for this ACD
  1) Definity-G3V2
  2) Definity-G3V3
  3) Definity-G3V4
  4) Definity-G3V5
  5) Definity-R6/R7
  6) Definity-R8

Enter choice (1-6):
```

11. Enter the option number associated with switch model associated with this ACD. For the initial release of the HA option, Definity-R8 is the only viable option.

    If the switch supports vectoring and vectoring is authorized, the following message appears; otherwise, go to Step 14:

```
Is Vectoring enabled on the switch? (y/n):
```

12. Enter y if vectoring is enabled on this switch; otherwise, enter n. The following message appears if vectoring is enabled, the switch supports EAS, and EAS is authorized. If the message does not appear, go to Step 14.

```
Is Expert Agent Selection enabled on the switch? (y/n):
```

13. Enter y if EAS is enabled on this switch; otherwise, enter n. The program responds:

```
Does the Central Office have disconnect supervision?
(y/n): (default: y)
```

14. Enter `y` if the CMS is located in the U.S., then go to Step 16. If you answer `n`, the program responds:

```
ACD calls shorter than the Phantom Abandon Call Timer value
will be counted as abandoned.
Enter the Phantom Abandon Call Timer value in seconds
(1-10): (default:10)
```

15. Enter the Phantom Abandon Call Timer value.

    NOTE:

    The Phantom Abandon Call Timer value can be changed through the `cmssvc` menu using the `swsetup` option.

    The program responds:

```
Enter the local port assigned to switch. (1-64):
```

    NOTE:

    The standard CMS provisioning procedure is to set the local and remote port assignments equal to the switch processor channel assignment. For example, the remote and local port assignments for switch processor channel 2 would both be set to a value of 2.

16. Enter the local port or channel number on the switch. The program responds:

```
Enter the remote port assigned to switch (1-64):
```

17. Enter the remote port or channel number on the switch.

    You must now select how the CMS platform is connected to the *Definity* switch for message transport. The program responds:

```
Select the transport to the switch
   1) X.25
   2) TCP/IP
Enter choice (1-2):
```

    Enter 2 to select TCP/IP.

18. The program responds:

```
Enter Definity ECS host name or IP Address:
```

19. Enter the host name of the *Definity* ECS (not the IP address) that is connected to this ACD. If you enter a host name that has not been added to the computer's `/etc/hosts` file, the program responds:

```
Switch_name has not been administered in a DNS or
/etc/hosts file. The DNS or /etc/hosts file must be
corrected or the link to the switch will not work.
```

    See the switch LAN setup on "Editing the /etc/hosts File" on Page 3-25 for more information about setting up the hosts file. The program continues:

```
Enter Definity ECS TCP port number (5001-5999):
(default: 5001)
```

20. Press Enter to use the default TCP port number 5001. This number must match the port number administered on the *Definity* switch.

    The program responds:

```
Number of splits/skills (0-XXX):
```

21. Enter the number of splits/skills in this ACD.

    The program responds:

```
Total split/skill members, summed over all splits/skills
(0-XXXX):
```

22. Enter the maximum number of split/skill members that will be logged into this ACD simultaneously, considering shift overlap.

    - For non-EAS, sum all agent-split combinations, counting each split an agent will log into (maximum is 4) as a split member.
    - For EAS, sum all agent-skill combinations that will be logged in at the same time, counting the maximum number of skills the supervisors expect to assign to each agent (up to 20) during a shift.

    If it is not possible to sum the number of splits/skills for each agent, you can determine the capacity needed by multiplying the total number of agents by the average number of splits/skills per agent. The program responds:

```
Number of shifts (1-4):
```

23. Enter the number of shifts.

    The program responds:

```
Enter the start time for shift 1 (hh:mmXM):
```

24. Enter the start time for shift `1`; for example, `08:00am`. The program responds:

```
Enter the stop time for shift 1 (hh:mmXM)
:
```

25. Enter the stop time for shift 1; for example, `05:00pm`.

    The program responds:

```
Number of agents logged into all splits/skills during
shift 1 (0-XXX):
```

26. Enter the number of agents logged in during the shift.

    NOTE:

    Steps 24 through 26 repeat for the number of shifts entered in Step 23.

    When all shifts have been set up, the program responds:

```
Number of trunk groups (0-XXX):
```

27. Enter the number of trunk groups associated with this ACD. The program responds:

```
Number of trunks (0-XXXX):
```

28. Enter the number of trunks associated with this ACD. The program responds:

```
Number of unmeasured facilities (0-XXXX):
```

29. Enter the number of unmeasured trunk facilities associated with this ACD. If the switch supports call work codes, the program responds:

```
Number of call work codes (X-XXXX):
```

30. Enter the number of call work codes. If this is the ACD being set up, the program responds:

```
Updating database
.................
```

After a few minutes, if vectoring is enabled on the switch (that is, if a y was entered in Step 12), the program responds:

```
Enter number of vectors (0-XXXX):
```

31. Enter the number of vectors. The program responds:

```
Enter number of VDNs (0-XXXX):
```

32. Enter the number of VDNs.

The program repeats Steps 10 through 31 for each ACD entered in Step 9. After you define the last ACD, the program continues:

```
Updating database.

Computing space requirements and file system space
availability.

Setup completed successfully.
```

If the setup determines that you do not have enough file space, you will get the following warning message:

```
Failed to find sufficient file space for CMS data.

WARNING: You do not currently have sufficient file space
for your existing CMS data. At this point you should turn
on CMS, go to the “Data Storage Allocation” screen, and
verify/modify the administration, or go to the “Free Space
Allocation” screen and verify your existing free space.

Setup completed with warnings.
```

If the setup was successful, then you will see the following message:

```
Setup completed successfuly
```

33. Verify that the installation completed successfully by entering the following:

    `tail /cms/install/logdir/admin.log`

    All failure messages are logged in this file. The CMS software is successfully set up when you see a message similar to the following:

```
File systems/space available:
   /cms      12994480

File systems/current blocks free:
   /cms      12994480
/cms: VDN,TKGRP,VECTOR,TRUNK,AGENT_LOG_REC,
AGENT_TRACE_REC,SPLIT,AGENT,EXCEPTIONS_REC,WORKCODE
Number of calls to fill_fs():12
Setup completed successfully <data/time>
```

    You may edit this file and add comments about the packages that were installed or authorized.

If you need to install additional CMS-related feature packages (Forecasting or External Call History), go to “Installing Feature Packages” on Page 3-46.

If you are not installing any other feature packages, perform the following steps to turn on CMS:

1. Access the CMS Services menu by entering `cmssvc`. The menu appears.
2. Enter `3` to select the `run_cms` option.
3. Enter `1` to turn on CMS.

Setting Up CMS Using a *UNIX* Flat File

Setting up the CMS feature package using a *UNIX* flat file consists of editing a copy of the `cms.inst.skl` file and starting the install program.

NOTE:

This procedure is not necessary if you already performed the CMS setup interactively.

Editing the File:

1. Enter:

   cmssvc

   The CMS services menu is displayed.
2. Enter `the number for the run_cms` option.

   The `Turn on/turn off` CMS menu is displayed.
3. Enter `2` to turn off CMS.
4. To change to the CMS installation directory, enter:

   cd /cms/install/cms_install
5. Make a copy of the CMS installation file by entering the following:

   cp cms.inst.skl cms.install
6. Change permissions on the copied CMS installation file by entering the following:

   chmod 644 cms.install
7. Edit the copied CMS installation file by entering the following:

   vi cms.install

   The file contains a series of questions and value ranges for the ACD/switch configuration. The following pages show a sample file with example values in bold.

   NOTE:

   When selecting a switch model in the file, refer to the table on Page 2-31.

```
# Enter a name for this UNIX system (up to 256 characters):
cms3
# Select the type of backup device you are using
#    1) SCSI QIC-150 cartridge tape - 150MB tape
#    2) 40.0 Gbyte 8mm tape
#    3) 14.0 Gbyte 8mm tape
#    4) 5.0 Gbyte 8mm tape
#    5) SCSI QIC-2.5 cartridge tape - 2.5GB tape
#    6) SCSI 4-8 SLR cartridge tape - 4GB tape 8GB compressed)
# Enter choice (1-6):
5
# Default backup device paths based on device type:
# Device                            Default backup path
# SCSI QIC-150 cartridge tape - 150MB tape  /dev/rmt/0
# 40.0 Gbyte 8mm tape                       /dev/rmt/0c
# 14.0 Gbyte 8mm tape                       /dev/rmt/0c
# 5.0 Gbyte 8mm tape                        /dev/rmt/0
# SCSI QIC-2.5 cartridge tape - 2.5GB tape  /dev/rmt/0c
# SCSI 4-8 SLR cartridge tape - 4GB tape (8GB compressed)
/dev/rmt/0c
# Enter the default backup device path:
/dev/rmt/0c
# Enter number of ACDs being administered (1-8):
3
# The following information is required per ACD:
# Information for ACD 1:
# Enter switch name (up to 20 characters):
# Select the model of switch for this ACD
#    1) Definity-G3V2
#    2) Definity-G3V3
#    3) Definity-G3V4
#    4) Definity-G3V5
#    5) Definity-R6/R7
#    6) Definity-R8
# Enter choice (1-6):
6
# Is Vectoring enabled on the switch? (y/n):
y
# Is Expert Agent Selection enabled on the switch? (y/n):
y
# Does the Central Office have disconnect supervision? (y/n):
y
# If the Central Office has disconnect supervision, enter 0.
# Otherwise, ACD calls shorter than the Phantom Abandon |
# Call Timer value will be counted as abandoned.
# Enter the Phantom Abandon Call Timer value in seconds (0-10):
0
# Enter the local port assigned to switch (1-64):
1
# Enter the remote port assigned to switch (1-64):
1
```

```
# TCP/IP transport is only available with DEFINITY R7 and
# later switch models.
# Select the transport to the switch
#    1) X.25
#    2) TCP/IP
# Enter choice (1-2):
2
# Skip the next question if you did not enter choice 1.
# These are used for X.25 connections only.
# Select the device used for x.25 connectivity to the switch
#    1) Serial port A
#    2) Serial port B
#    3) HSI link 0
#    4) HSI link 1
#    5) HSI link 2
#    6) HSI link 3
#    7) HSI link 4
#    8) HSI link 5
#    9) HSI link 6
#   10) HSI link 7
#   11) Software loopback link 0
#   12) Software loopback link 1
# Enter choice (1-12):

# Skip the next question if you did not enter choices 11 - 12.
# These are used for testing only. If you select one of these,
# you will not be able to collect data from your ACD.
# Are you sure you want to do this? (y/n):

# Skip the next two questions if you did not enter choice 2
# (TCP/IP). These are used for TCP/IP connections only.
# If a host name is entered, the host name must be administered
#in a DNS or /etc/hosts file or the link to the switch
# will not work.
# Enter DEFINITY host name or IP Address:
192.168.2.2
# Enter DEFINITY TCP port number (5001-5999):
5001
# Maximum number of splits/skills based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4     255
# Definity-G3V5/Definity-R6/R7                  600
# Definity-R8                                   999
# Number of splits/skills (0-Maximum):
# Maximum number of split/skill members based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4    5200
# Definity-G3V5/Definity-R6/R7/Definity-R8    10000
# Total split/skill members, summed over all
# splits/skills (0-Maximum):
1000
```

```
# Number of shifts (1-4):
1
# Enter the start time for shift 1 (hh:mmXM):
08:00AM
# Enter the stop time for shift 1 (hh:mmXM):
05:00PM
# Number of agents logged into all splits/skills during
# shift 1 (1-Maximum):
100
# Enter the start time for shift 2 (hh:mmXM):

# Enter the stop time for shift 2 (hh:mmXM):

# Number of agents logged into all splits/skills during
# shift 2 (1-Maximum):

# Enter the start time for shift 3 (hh:mmXM):

# Enter the stop time for shift 3 (hh:mmXM):

# Number of agents logged into all splits/skills during
# shift 3 (1-Maximum):

# Enter the start time for shift 4 (hh:mmXM):

# Enter the stop time for shift 4 (hh:mmXM):

# Number of agents logged into all splits/skills during
# shift 4 (1-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4     666
# Definity-G3V5/Definity-R6/R7/Definity-R8      666
# Number of trunk groups (0-Maximum):
20
# Maximum number of trunks based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4    4000
# Definity-G3V5/Definity-R6/R7/Definity-R8     4000
# Number of trunks (0-Maximum):
100
```

```
#Number of unmeasured facilities (0 to (Maximum trunks - Number of trunks)):
10
# Minimum number of call work codes based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4       1
# Definity-G3V5/Definity-R6/R7/Definity-R8        1
# Maximum number of call work codes based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4    1999
# Definity-G3V5/Definity-R6/R7/Definity-R8     1999
# Number of call work codes (Minimum-Maximum):
100
# Maximum number of vectors based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4     512
# Definity-G3V5/Definity-R6/R7                  512
# Definity-R8                                   999
# Enter number of vectors (0-Maximum):
20
# Maximum number of VDNs based on switch type:
# Release(s)                                  Value
# Definity-G3V2/Definity-G3V3/Definity-G3V4    2000
# Definity-G3V5                                2000
# Definity-R6/R7                               8000
# Definity-R8                                 20000
# Enter number of VDNs (0-Maximum):
10



# Information for ACD 2:
```

(The file repeats the preceding statements for ACDs 2 through 8; enter data for only the required number of ACDs.)

8. Enter the appropriate values for your configuration. As shown in bold in the examples, the entries must be added on the blank lines after each question.

   CAUTION:

   Use the computer's host name for the UNIX system name. The computer's host name was assigned during the factory installation.

   After you have entered all the appropriate values, enter `:wq` to write and quit the file.

Running Setup with a Flat File

1. Enter `cd` to change to the root directory.
2. Access the CMS Services menu by entering:

   `cmssvc`

   The program responds:

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

Select a command from the list below.
  1) auth_display Display feature authorizations
  2) auth_set     Authorize capabilities/capacities
  3) run_cms      Turn CentreVu CMS on or off
  4) setup        Set up the initial configuration
  5) swinfo       Display switch information
  6) swsetup      Change switch information
  7) patch_inst   Install a single CMS patch from CD
  8) patch_rmv    Backout an installed CMS patch
  9) load_all     Install all CMS patches found on CD
 10) back_all     Backout all installed CMS patches from machine
Enter choice (1-10) or q to quit:
```

3. Enter `4` to select the `setup` option. If setup has been done previously, the program responds:

```
Warning!!! Setup has already been performed.
Running this command will remove all CMS data in the database.
Do you wish to proceed and re-configure CMS? (y/n): (default: n)
```

4. Enter y. The program responds:

```
Select the language for this server:

All languages are ISO Latin except Japanese. Selection of the
server language assumes that existing customer data is
compatible. (Upgrade from any ISO Latin language to any ISO
Latin language or from Japanese to Japanese is supported).

1) English
2) Dutch
3) French
4) German
5) Italian
6) Portuguese
7) Spanish
8) Japanese
Enter choice (1-8): (default: 1)
```

5. Enter the number for the language used on this system. The program responds:

```
The input will be read from
  1) the terminal
  2) a flat file
Enter choice (1-2):
```

6. Enter `2` to select the `flat file` option. The program responds:

```
*** The rest of this command is running in the background ***
```

7. Verify that the installation completed successfully by entering the following:

   `tail -f /cms/install/logdir/admin.log`

   The `-f` option in the `tail` command updates the console as messages are written to the `admin.log` file. All failure messages are logged in this file. The CMS software is successfully set up when you see a message similar to the following:

```
File systems/space available:
   /cms      12994480

File systems/current blocks free:
   /cms      12994480
/cms: VDN,TKGRP,VECTOR,TRUNK,AGENT_LOG_REC,
AGENT_TRACE_REC,SPLIT,AGENT,EXCEPTIONS_REC,WORKCODE,
CALL_REC,
Number of calls to fill_fs():12
Setup completed successfully <data/time>
```

   You may edit this file and add comments about the packages that were installed or authorized.

8. Press the Delete key to break out of the `tail -f` command.

If you need to install additional CMS-related feature packages (Forecasting or External Call History), go to "Installing Feature Packages" on Page 3-46.

If you are not installing any other feature packages, do the following to turn on CMS:

1. Access the CMS Services menu by entering `cmssvc`.

   The menu appears.

2. Enter `3` to select the `run_cms` option.

3. Enter `1` to turn on CMS.

   CMS turns on.

Installing Feature Packages

Use the procedures in this section to install the following feature packages:

- Forecasting
- External Call History (ECH).

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

Installing the Forecasting Package

Overview

Use the procedure in this section to install the Forecasting feature package.

Prerequisites

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

Procedure

1. Access the CMS Services menu by entering the following command:

   `cmssvc`

   The program responds:

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

Select a command from the list below.
  1) auth_display Display feature authorizations
  2) auth_set     Authorize capabilities/capacities
  3) run_cms      Turn CentreVu CMS on or off
  4) setup        Set up the initial configuration
  5) swinfo       Display switch information
  6) swsetup      Change switch information
  7) patch_inst   Install a single CMS patch from CD
  8) patch_rmv    Backout an installed CMS patch
  9) load_all     Install all CMS patches found on CD
 10) back_all     Backout all installed CMS patches from machine
Enter choice (1-10) or q to quit:
```

2. Enter `1` to select the `auth_display` option. The system lists the current authorizations (for example):

```
                                Version purchased:   R3V8
                              Capability/Capacity    Authorization
                              -------------------    -------------
                                        vectoring    authorized
                                      forecasting    authorized
                                         graphics    authorized
                                external call history  authorized
                               expert agent selection  authorized
                                 external application  authorized
                          More than 2000 VDNs measured  authorized
              Lucent Technologies CentreVu(R) Supervisor  authorized
         Lucent Technologies CentreVu(R) Report Designer  authorized
                   Maximum number of split/skill members  10000
                                Maximum number of ACDs  2
                  Simultaneous CentreVu Supervisor logins  250
```

3. Verify that the system is authorized to install the Forecasting package.

   NOTE:

   If Forecasting is not authorized but should be, go to "Setting Authorizations" on Page 3-15.

4. Access the CMS Administration menu by entering:

   `cmsadm`

   The program responds:

```
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:
```

5. Select the `pkg_install` option. The program responds:

```
The CMS Features that can be installed are
  1) forecasting
  2) external call history
Enter choice (1-2) or q to quit:
```

NOTE:

The `pkg_install` option menu displays only those feature packages that are authorized but not yet installed.

6. Enter the number that corresponds to the Forecasting package. The program responds:

```
Creating database tables
.......
```

When creation of the Forecasting database tables is completed, the program responds:

```
Computing space requirements and file system space
availability.

Forecasting package installed.
```

If the program determines that you do not have enough file space, you will get the following warning message:

```
Failed to find sufficient file space for CMS data.

WARNING: You do not currently have sufficient file space
for your existing CMS data. At this point you should turn
on CMS, go to the “Data Storage Allocation” screen, and
verify/modify the administration, or go to the “Free
Allocation” screen and verify your existing free space.

Forecasting package installed with warnings.
```

7. Verify that the installation completed successfully by entering the following:

   ```
   tail /cms/install/logdir/admin.log
   ```

   The Forecasting package is successfully installed when you see this message:

   ```
   Forecasting package installed (date/time )
   ```

   You may edit this file in order to add comments about the packages that were installed or authorized.

If you need to install External Call History, go to "Installing the External Call History Package" on Page 3-50. If you do not need to install External Call History, do the following to turn on CMS:

1. Access the CMS Services menu by entering `cmssvc`.

   The menu appears.

2. Enter `3` to select the `run_cms` option.

3. Enter `1` to turn on CMS.

   CMS turns on.

Installing the External Call History Package

Overview

Use these procedures to install the External Call History (ECH) feature package.

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 Lucent 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

Prerequisites

- The customer must have a separate computer for the storage and reporting of call records.
- Both the storage machine and the CMS machine must be administered in *UNIX*-to-*UNIX* copy (UUCP).
- If the storage machine is not running the *UNIX* system, use a DOS version of UUCP.
- Verify that you are logged in as *root.*
- The computer must be in run-level 3 (check this with the command `who -r`).
- All file systems must be mounted.
- CMS must be turned off.

NOTE:

Once the External Call History package is installed, you will no longer be able to access any call record data from CMS. For more information about administering the UUCP link port on an NTS, see *CentreVu® CMS R3V8 External Call History Interface* (585-210-912).

Procedure

1. Access the CMS Services menu by entering:

   `cmssvc`

   The program responds:

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

Select a command from the list below.
  1) auth_display Display feature authorizations
  2) auth_set     Authorize capabilities/capacities
  3) run_cms      Turn CentreVu CMS on or off
  4) setup        Set up the initial configuration
  5) swinfo       Display switch information
  6) swsetup      Change switch information
  7) patch_inst   Install a single CMS patch from CD
  8) patch_rmv    Backout an installed CMS patch
  9) load_all     Install all CMS patches found on CD
 10) back_all     Backout all installed CMS patches from machine
Enter choice (1-10) or q to quit:
```

2. Enter `1` to select the `auth_display` option. The program responds by displaying the current authorizations (for example):

```
                              Version purchased:   R3VX

                           Capability/Capacity   Authorization
                           -------------------   -------------
                                     vectoring   authorized
                                   forecasting   installed
                                      graphics   authorized
                            external call history   authorized
                           expert agent selection   authorized
                             external application   authorized
                    More than 2000 VDNs measured   authorized
        Lucent Technologies CentreVu(R) Supervisor   authorized
    Lucent Technologies CentreVu(R) Report Designer   authorized
              Maximum number of split/skill members   10000
                            Maximum number of ACDs   2
            Simultaneous CentreVu Supervisor logins   250
```

3. Verify that the system is authorized for the External Call History package.

   NOTE:

   If External Call History is not authorized but should be, go to "Setting Authorizations" on Page 3-15 (this procedure can only be performed by CMS provisioning personnel).

4. Access the CMS Administration menu by entering:

   `cmsadm`

   The program responds:

```
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:
```

5. Select the `pkg_install` option. The program responds:

```
The CMS Features that can be installed are
  1) forecasting
  2) external call history
Enter choice (1-2) or q to quit:
```

NOTE:

The system displays only feature packages that are authorized but not yet installed.

6. Enter the number that corresponds to the External Call History package (in this example, 2). The program responds:

```
Enter name of computer to which to send call records
(up to 256 characters):
```

7. Enter the name of the computer where call records will be collected. The program responds:

```
Enter full path of the program to transmit the external
call history files: (default: /cms/dc/chr/uucp_copy)
```

8. Press Enter. The program responds:

```
Enter full path of the program to check the external call
history file transmission: (default:
/cms/dc/chr/uucp_check)
```

9. Press Enter. The program responds:

```
Enter password for nuucp login on computer (up to 8
characters)
```

10. Enter the password for `nuucp` of the receiving computer that was administered in `uucp`. The program responds:

```
Enter CMS port for connection to computer (s_pdevxxx):
```

11. Enter the CMS port administered for the Call History Reporting machine. This port can either be on one of the 64-port NTS patch panels or on one of the 8- or 16-port NTSs. For more information on administering the ports on the NTS, see *CentreVu® CMS Terminals, Printers, and Modems* (585-215-874). The program responds:

```
Select a speed for this connection
1) 19200
2) 38400
Enter choice (1-2):
```

12. Enter the speed that the connection between the CMS and Call History Reporting machine will be using. The program responds:

```
Number of call segments to buffer for ACD xxxxx (0-99999):
```

13. Enter the number of call records to be held in the buffer if the Call History machine cannot accept the data. (This step reserves disk space; therefore, sufficient disk space must be available.)

    NOTE:

    This step is repeated for each administered ACD.

    The program responds:

```
Computing space requirements and file system space
availability.

External Call History package installed.
```

    If the setup determines that you do not have enough file space, you will get the following warning message:

```
Failed to find sufficient file space for CMS data.

WARNING: You do not currently have sufficient file space
for your existing CMS data. At this point you should turn
on CMS, go to the “Data Storage Allocation” screen, and
verify/modify the administration, or go to the “Free
Allocation” screen and verify your existing free space.

External call history package installed with warnings.
```

14. Verify that the installation completed successfully by entering:

    `tail /cms/install/logdir/admin.log`

    If the External Call History package is installed successfully, the program responds:

    ```
    External Call History package installed (date/time )
    ```

    You may edit this file in order to add comments about the packages that were installed or authorized.

If you need to install Forecasting, go to "Installing the Forecasting Package" on Page 3-46.

If you are not installing any other feature packages, do the following to turn on CMS:

1. Access the CMS Services menu by entering `cmssvc`.

   The menu appears.

2. Enter `3` to select the `run_cms` option.

3. Enter `1` to turn on CMS.

   CMS turns on.

Setting Up the Remote Console

Overview

This section describes how to redirect the remote console port on the new HA server using the *Solaris* software package. Remote access is required for both the primary and secondary servers. Redirecting the console allows the TSC to dial in and do remote maintenance.

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

Platform Considerations

- All platforms.

Administering the Remote Console Port

To administer the remote console port on the back of the CMS computer, do the following:

1. Remove the current port administration by entering:

   `/cms/install/bin/abcadm -r ttyX`

   (where X is “a” or “b”)

   The program responds:

```
ttyX is currently set to be incoming

Are you sure you want to change it? [y,n,?]
```

2. Enter y. The program responds:

```
ttyX administration removed
```

3. Enter the following to administer the remote console port:

   ```
   /cms/install/bin/abcadm -i -b 9600 ttyX
   ```

   (where X is “a” or “b”)

   The program responds:

```
ttyX set to incoming port 9600 baud
#
```

The remote console port has been administered.

Redirecting the Remote Console Port to the Modem

Use the remote console port functions on a CMS computer by:

- redirecting the console from the local console to the remote console
- redirecting the console back to the local console

1. Dial in from the remote console to the remote console modem on the CMS computer and log in as *root*.

2. Remove the port monitor by entering:

   ```
   /cms/install/bin/abcadm -r ttyX
   ```

   (where X is “a” or “b”)

   The program responds:

```
ttyX is currently set to be incoming

Are you sure you want to change it? [y,n,?]
```

3. Enter y. The program responds:

```
ttyX administration removed
```

4. Redirect the console to the remote console port by entering the following:

   ```
   /cms/install/bin/abcadm -c -b 9600 ttyX
   ```

   The program responds:

```
This change requires a reboot to take affect

Are you ready to reboot? [y,n,?]
```

5. Enter y. The system will automatically reboot, and the remote console port will come up as the console.

   As the system reboots, shut down messages appear on the local console. When the system starts to come back up, the local console should go blank and the system boot diagnostics should appear on the remote console. When the system is restarted, a login prompt should appear on the remote console.

6. Log in to the remote console as root.

   CAUTION:

   If you enter Control-D from the remote console to exit the system without first redirecting control back to the local console, you may lock yourself from using the console locally or remotely.

7. Redirect the console back to the local console by entering:

   ```
   /cms/install/bin/abcadm -c local
   ```

   The program responds:

```
Console set to local

This change requires a reboot to take affect

Are you ready to reboot? [y,n,?]
```

8. Enter y. The system automatically reboots and the remote console port comes up as a regular dial-in port with the `login:` prompt displayed.

   As the system reboots, the shutting-down messages appears on the remote console. When the system starts to come back up, the system boot diagnostics should appear on the local console. After the system reboots, a login prompt should appear on the local console.

9. Log into the local console as *root*.

   The console has been redirected from the remote console to the local console.

Setting Up the Alarm Originator

For information on setting up the alarm origination manager on the HA servers, see “CentreVu CMS R3V8 Alarm Origination Manager (585-215-884).

Setting Up the NTS

For information about setting up the NTS, see “Setting up the NTS”, in Chapter 2 of “CentreVu Call Management System R3V8 Software Installation and Setup” (585-210-941).

Configuring the NTS

This procedure is performed on NTS devices when:

- the NTS is newly installed, or
- the NTS requires reconfiguration during a manual HA server switch-over after the HA server to which the NTS was initially connected has experienced a failure event

1. Connect a dumb terminal to the Console Port on the rear of the NTS using the console cable and adapter that came with the NTS. On the 8- and 16-port NTSs, the Console Port is port **#1**.

   You will need the following for the 8- and 16-port units:

   - Console Cable
   - Adapter - comcode 407361823
   - Null Modem - comcode 407122043.

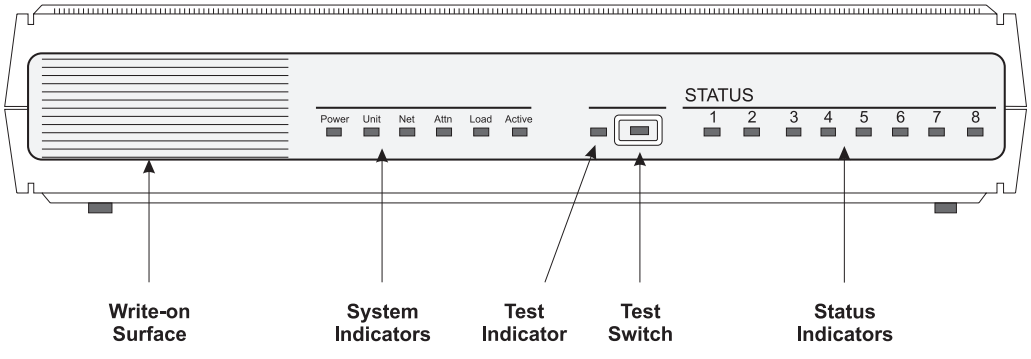
You will need the following for the 64-port unit:

- Console Cable
- Adapter - part number 06-988-260-20.

NOTE:

The terminal options should be set to 9600 bps, 8 bits, no parity or space parity, and a stop bit.

2. Turn on the NTS, and within 15 seconds push the Test Switch on the front of the NTS (see the following figure).



3. The NTS goes through its hardware diagnostics, and the following prompt should appear:

```
Monitor::
```

4. Enter the `erase` command.

NOTE:

There are two types of information that can be erased:

- `EEPROM (configuration information)`
- `FLASH (self-boot image).`

If only one type of information is present, the program begins to erase it. If there are two types of information, the program prompts you to select the information you want to erase. Erase both the EEPROM and the FLASH information.

The program responds:

```
Erase
   1) EEPROM (i.e., Configuration Information)
   2) FLASH (i.e., Self Boot Image)
Enter 1 or 2::
```

5. Enter `1` to erase EEPROM. The program responds:

```
Erase all non-volatile EEPROM memory? (y/n) [n]::
```

6. Enter `y`. The program responds:

```
Erasing xxxx bytes of non-volatile memory. Please wait....
.............................
Erased xxxx bytes of non-volatile memory complete.
Monitor::
```

7. Repeat Steps 4 through 6, but select `2` (FLASH) to erase the FLASH information.

8. After you have completed the `erase` command, enter `addr`. The program responds:

```
Enter Internet address [<uninitialized>]::
```

9. Enter the IP address for this NTS. The program responds:

```
     Internet address : xxx.xxx.xxx.xxx

Enter Subnet mask [255.255.255.0]::
```

10. Enter the appropriate Subnet mask, or press Enter to accept the default. The program responds:

```
     Subnet mask: xxx.xxx.xxx.xxx

Enter preferred load host Internet address [<any host>]::
```

11. Enter the IP address of the CMS computer. The program responds:

```
     Preferred load host address xxx.xxx.xxx.xxx

Enter Broadcast address [0.0.0.0]::
```

12. Press Enter to accept the default broadcast message address. The program responds:

```
Enter Preferred dump address [0.0.0.0]::)
```

13. Enter the IP address of the CMS computer. The program responds:

```
     Preferred dump address: xxx.xxx.xxx.xxx

Select type of IP packet encapsulation (ieee802/ethernet)
[<ethernet>] ::
```

14. Press Enter to accept the default IP packet encapsulation. The program returns to the `monitor::` prompt if you have a 64-port NTS. Continue with Step 16.

    The program responds with the following question if you have an 8- or 16-port NTS:

```
     Type of IP packet encapsulation: <ethernet>

Load Broadcast Y/N [Y]::
```

15. Enter `N`. The program returns to the `monitor::` prompt.

16. Enter the `boot` command at the monitor prompt to reinitialize the NTS with the new parameters. The program responds:

```
Enter boot file name [oper.42.enet]::
```

NOTE:

The boot file name differs depending on the type of NTS. For the 8- and 16-port NTS, the boot file name is:

`[(ip) “oper.52.enet”,(mop)“OPER_52_ENET.SYS”]`

For the 64- port NTS, the boot file name is:

`oper.42.enet`

17. Press Enter to accept the default boot file name. The program responds:

```
     Requesting boot file “oper.42.enet”.
     Unanswered requests shown as ‘?’,
                              transmission errors as ‘*’.

     Booting file: oper.42.enet from 192.168.2.1

     Loading image from 192.168.2.1
.....................
```

The periods (dots) continue to appear as the NTS is initialized and set up.

NOTE:

If the program displays “SELF” instead of the IP address (192.168.2.1 is the factory default; your IP address may be different), it means that you did not erase EEPROM. Go back to Step 4 to erase EEPROM.

When the initialization finishes, the program responds:

```
annex::
```

18. Disconnect the dumb terminal from the NTS.

The NTS has been administered.

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 R3V8 Software Installation and Setup” (585-210-941).

Migrating CMS System Administration Data to the New Server

This procedure uses the maintenance backup tape (“Performing a Maintenance Backup (Administration Data Only)” on Page 3-12), which was created on the original server, 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!
Do not use the Full Maintenance backup tape created in “Performing a Full Maintenance Backup” on Page 3-11 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.

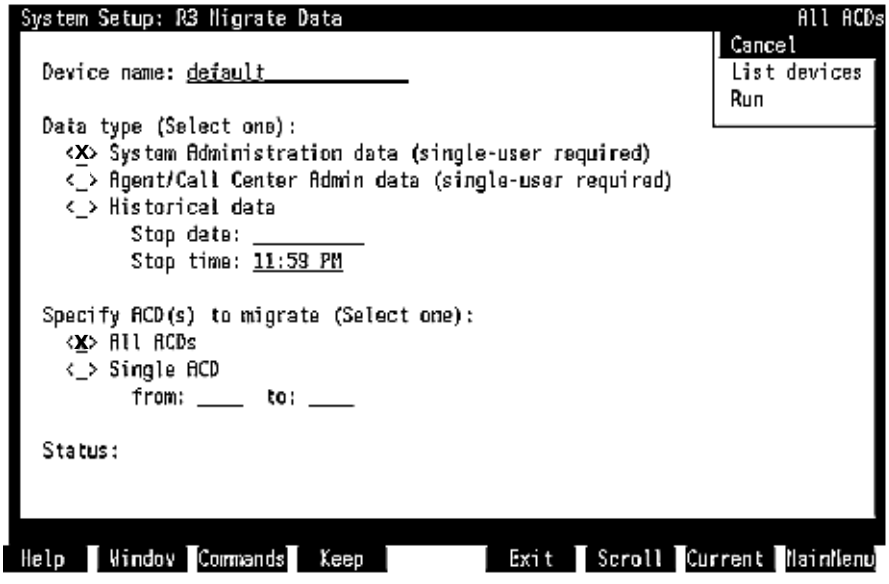
2. Select `System Setup - CMS State` from the CMS main menu and select the **`Single User`** `Mode` option

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 the migration data types, and specify `All ACDs` for migration, as shown in the following example:



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 telephone the Lucent National Customer Care Center at 1-800-242-2121; international customers should contact their Lucent 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.

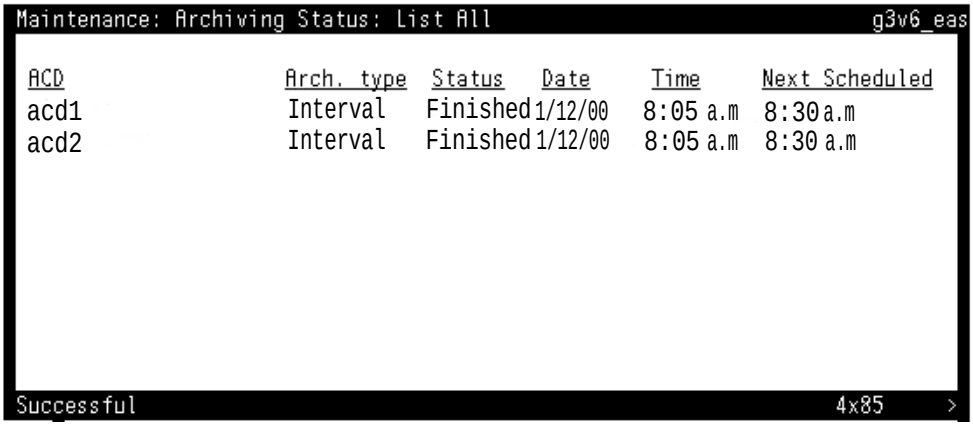
2. Cursor down to the `Archiving Status` option and press Enter.

   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.



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 R3V8 and the HA dual C-LAN option.

For details of switch admininistration for HA systems, see "Administering the Switch for CMS High Availability 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 R3V8 and HA dual links and 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

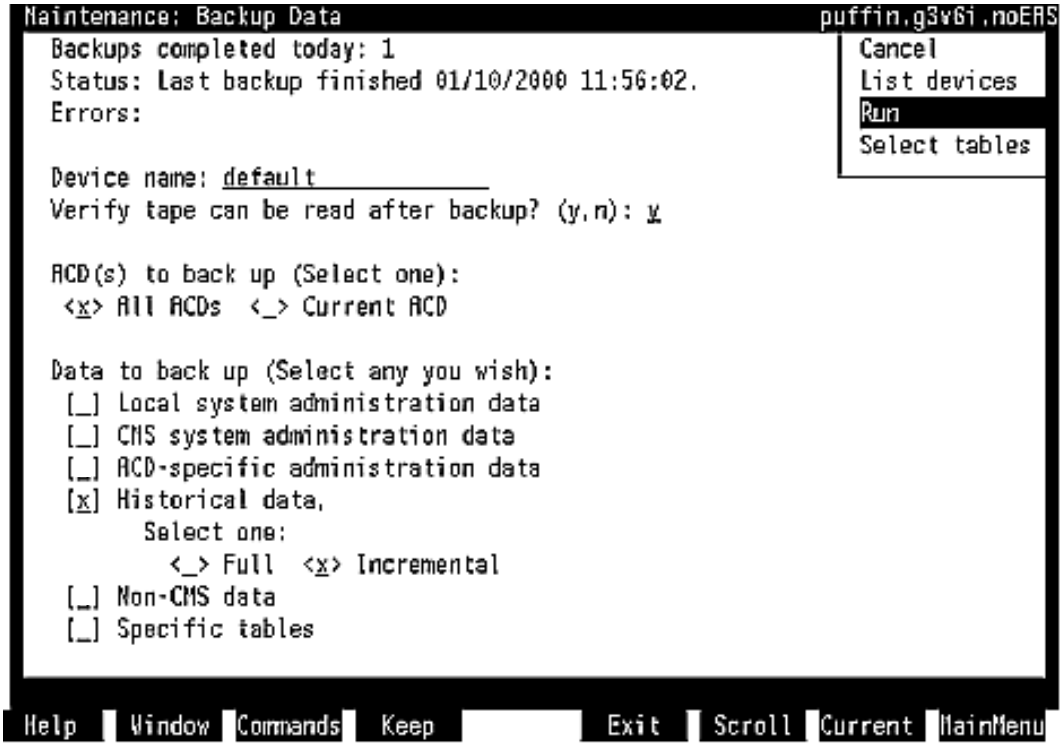
Perform an incremental maintenance backup (historical data only) on the original server. Begin the server upgrade immediately after the backup completes.

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:



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 (preceeding procedure) is successfully completed on the original server, the original server can be powered down, the system hard drives are swapped out with the new drives provided by the Speed Centre and all necessary software authorization, setup, and configuration steps are performed. For details, see “Setting Up CMS on an HA Server” on Page 3-14.

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 R3V8 and the HA dual C-LAN option and CMS data collection is started on the new HA server, migrate CMS historical data to the new HA server.

Procedure

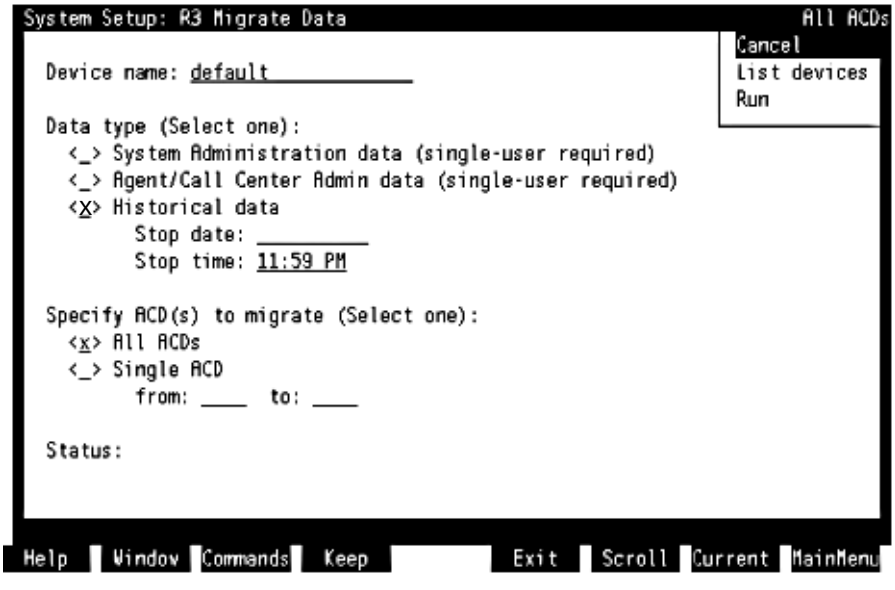
This procedure migrates CMS historical data from the second incremental maintenance backup ("Performing an Incremental Maintenance Backup" on Page 3-67) onto the new HA server.

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 the data type, and `specify All ACDs` for migration, as shown in the following example:



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 3-11) 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 telephone the Lucent National Customer Care Center at 1-800-242-2121; international customers should contact their Lucent 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 Onto 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 3-12) 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

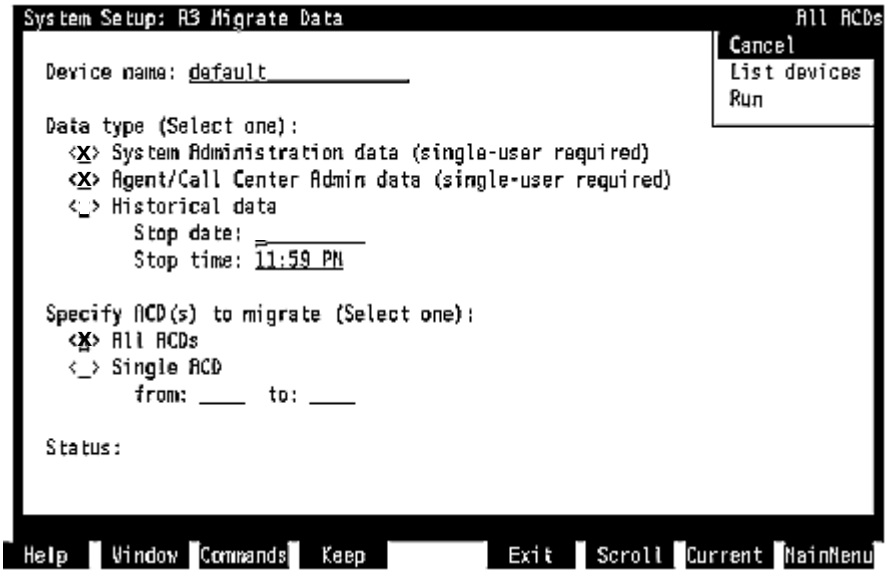
Insert the initial maintenance backup tape back into the tape drive of the original server.

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:



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 telephone the Lucent National Customer Care Center at 1-800-242-2121; international customers should contact their Lucent 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 3-11.

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.

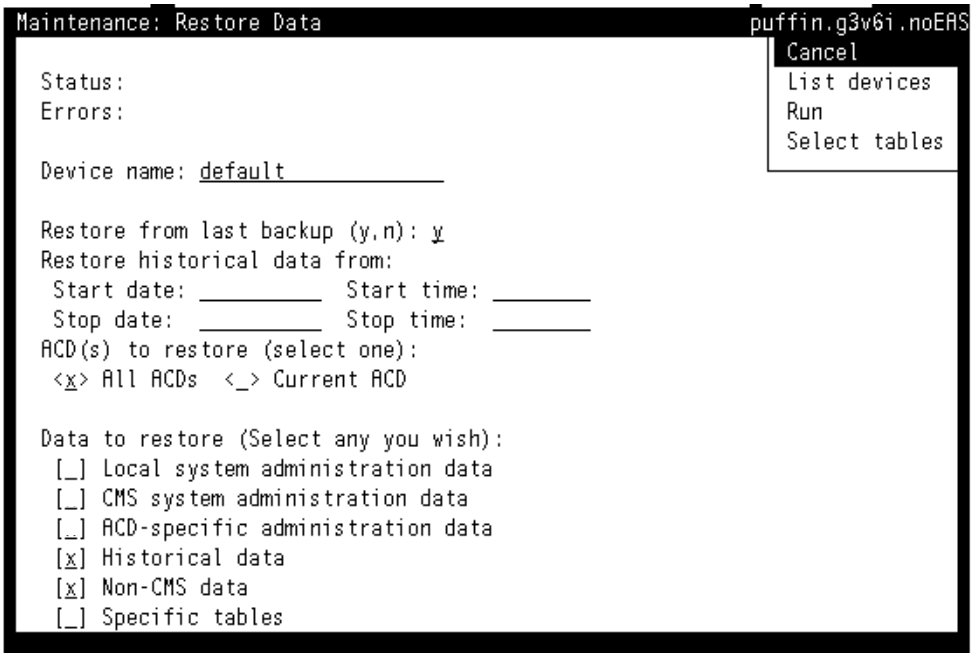
Procedure

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:



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.

Note:

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 3-7.

Administering the Switch for CMS High Availability 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 switch 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 R3V8 load, the *Definity* switch must be optioned with a switch version of V8, Call Center Release of 8.1, and Adjunct CMS Release of R3V8, as specified below in "Determining Switch/CMS Compatibility" on Page 4-2.

The two CMS computers used in a dual server HA system can collect identical data from up to eight switches. From the perspective of the CMS computer, 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	R3V8	Definity-R8

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

  The local and remote port assignments must be symmetrical between the switch and the CMS. For example, if the CMS local port is 1 and the remote port is 10, the switch local port must be 10 and the remote port must be 1.
- the hostname or IP address, and TCP port

Note:

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. This procedure is documented in *CentreVu® CMS Software Installation and Setup (585-210-941)*.

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	Adding node names and IP addresses
change ip-interfaces	Adding a C-LAN IP interface
add data-module (this form has been changed in R8)	Adding an ethernet data module
change communication-interface processor-channels	Adding the processor interface channels
add ip-route (this form has been changed in R8)	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.
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                                          Page 2 of 6

                              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                       .   .   .
```

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.

NOTE:

This form is new for *DEFINITY* R8 and later. Several of the fields on this form were previously on the Data Module form in *DEFINITY* R7.

```
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.
Gateway Address	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 if not required. If required, enter the address of a network node that will serve as the default gateway for the IP interface. ~~If using ethernet only, 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`.
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. Use the first channel available.
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. For this series of examples, link `8` was used.
Interface Chan	Enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup (see 19 Page 2-33).
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	Although not strictly required, the standard CMS provisioning practice is to set the local and remote port assignments equal to the processor channel assignment for each connection.
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.
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	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

Administer
- NTS . . . 3-59
- Remote Console Port . . . 3-56
- Switch LAN . . . 3-24
- TCP/IP . . . 3-24

Administering
- Generic 3si Switch . . . 4-7
- LAN
  - Generic 3si . . . 4-7

Administration Log . . . 3-20
Authorizations
- EAS . . . 3-15
- External Call History . . . 3-15
- Feature Packages . . . 3-15
- Forecasting . . . 3-15
- Graphics . . . 3-15
- Set . . . 3-15

C

CMS
- Setup . . . 3-27
  - Interactively from a Terminal . . . 3-28
  - Using *UNIX* System Flat File . . . 3-38

Connecting
- Generic 3si Switch . . . 2-5
- Single ACD Using Serial Ports . . . 2-5

Connecting Blocks . . . 2-3
Customer Support . . . 1-6

D

Data Storage Parameters . . . 3-21
Default Router . . . 3-26
DEFINITY . . . 2-1
distance limits
- Cat 5 cable . . . 2-7

E

EAS . . . 3-15
Editing /etc/defaultrouter File . . . 3-26
Editing /etc/hosts File . . . 3-25
ethernet ports . . . 2-5
External Call History
- Authorize . . . 3-15
- Install . . . 3-50

F

Feature Authorizations . . . 3-15
Feature Packages . . . 3-50
- External Call History . . . 3-50
- Forecasting . . . 3-46
- Graphics . . . 3-15
- Set Authorizations . . . 3-15

Flat File
- CMS Setup . . . 3-38
- Example of . . . 3-39, 3-42

Forecasting
- Authorize . . . 3-15
- Install . . . 3-46

FSBE . . . 2-5

G

Generic 3si
- Administering
  - LAN . . . 4-7

Graphics . . . 3-15

H

Helplines . . . 1-6
High Availability Option . . . 4-2
High Availability, defined . . . 2-1
Hosts File . . . 3-25

I

Install
- External Call History . . . 3-50
- Feature Packages . . . 3-46, 3-50
- Forecasting . . . 3-46

L

LAN
- Administration
  - Generic 3si . . . 4-7
- Overview . . . 3-24

LAN connections
- hardware . . . 2-7

LAN connectivity options . . . 2-5

M

migration
- system administration data . . . 3-64

Multiple ACDs (Switches) . . . 4-1

N

NTS
Administer 3-59

P

Platforms
combinations supported by High Availability . . . 1-2
primary server
defined 1-1
installed software 1-1

R

Redirect Remote Console Port 3-56
Remote Console
Administer the Port 3-56
Redirecting the Port 3-56
Setting Up the Software 3-56
Test 3-57
Responsibilities 1-4
Roles 1-4

S

secondary server
defined 1-1
installed software 1-1
Set
Authorizations 3-15
Set Up
CMS 3-27
Interactively from a Terminal 3-28
Using a *UNIX* System Flat File 3-38
Data Storage Parameters 3-21
NTS 3-59
Remote Console 3-56
Switch LAN 3-24
TCP/IP 3-24
Setup Methods
Interactively from a Terminal 3-28
Using a UNIX System Flat File 3-38
Software
required and optional 1-3
Software Installation
Feature Packages 3-46
Setting Up Remote Console 3-56
storage.def file 3-21
SunSwift 2-5
Support 1-6
Switch
Link 3-24
TCP/IP 3-24
Switches
support for High Availability 1-2
supported releases 2-1
system administration data, migrating 3-64

T

TCP/IP 3-24
Technician Support 1-6

V

vector.def file 3-21