Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting

Release 21.0
Issue 2
July 2025

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H

(HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Part 1: Overview

Chapter 1: Introduction

Introduction

Purpose

This document describes how to administer, and troubleshoot connections between Avaya Call Management System (CMS) and Avaya Aura® Communication Manager.

Change history

The following table outlines the key changes in this document for Release 21.x:

Issue	Date	Summary of changes
2	November 2024	General refresh.
1	January 2020	Revised outdated information throughout the document.

Chapter 2: Compatibility

Communication Manager and CMS release compatibility

Different releases of CMS software are certified to interface with the following Communication Manager software releases.

Communication Manager release	CMS release								
	16.x	17.x	18.0	18.1	19.0	19.1	19.2	20.0	21.0
7.x	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8.x	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
8.1.2+ Secure	No	No	No	No	No	Yes	Yes	Yes	Yes
10.x	No	No	No	No	No	No	No	No	Yes

For CMS Release 19.1 and later with Communication Manager Release 8.1.2 and later, the messaging link between the two systems are now encrypted.

Part 2: Connecting the link

Chapter 3: Connect the link

Connecting the link

You can connect a CMS server to a Communication Manager system using TCP/IP over a local area network (LAN).

This connection enables the CMS software to receive, store, and format the ACD information it receives from one or more Communication Manager systems.

The CMS software cannot communicate with the Communication Manager system if the ACD feature, CMS, or the Communication Manager system hardware is not properly administered. For more information, see Administering the Communication Manager system link on page 33.

Local vs remote connections

You can use a local or remote connection between the Communication Manager system and the CMS server. These connections are defined as follows:

- **Local**

  Connections use facilities local to the Communication Manager system, such as a direct connection over a LAN.

- **Remote**

  Connection is over a wide area network (WAN).

Multiple ACDs (multiple Communication Manager systems)

One CMS server can collect data from up to eight different Communication Manager systems. From the CMS server point of view, each Communication Manager system represents one ACD. Each Communication Manager system requires a link to the CMS server that is collecting data from the Communication Manager system.

High availability option

The High Availability option provides dual links between the Communication Manager system and two separate CMS servers. You must connect a link from one ethernet port on the Communication Manager system to one CMS server, and a second link on the Communication Manager system to another CMS server.

Planning for Communication Manager system links

When setting up a Communication Manager system link using TCP/IP over a LAN, planning information must be gathered before you begin. Some of the information needed includes:

- How is the connection being made from the CMS server to the Communication Manager system?
  - Private LAN, no connectivity to customer LAN (uses private LAN addresses).
    - Most robust and reliable, no dependency on customer's network.
    - A dedicated LAN port on the CMS server provides the Communication Manager system link.
    - The primary LAN port is used for other connectivity using a different subnet from the Communication Manager system link.
    - If desired, a second ethernet port can be used to provide additional isolation for the CMS link.
    - A dedicated LAN hub to connect the links.
  - Customer LAN with private segment.
    - Uses a network switch or router to provide a private network or network segment.
    - Minimal dependency on customer's network.
    - A dedicated LAN port on the CMS server provides the Communication Manager system link.
    - The primary LAN port is used for other connectivity using a different subnet from the Communication Manager system link.
    - Customer must provide equipment and administer network for private segment.
    - Customer LAN administrator must be present during setup.
  - Direct connection to Customer LAN, without private segment.
    - 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 the customer LAN is used, the following information is needed from the customer:
  - Customer network physical connectivity:
    - Location of network access point (hub, router, and so on).
    - Distance between the ethernet port on the Communication Manager system and the network access point (328 ft, 100 m maximum).
    - Wiring to access point, existing or new, Category 5 minimum required.

- Customer network administration:
  - IP address of Communication Manager system ethernet ports, CMS server, and gateways.
  - Node names of Communication Manager system ethernet ports, CMS server, and gateways.
  - Subnet masks for all LAN segments containing Communication Manager system ethernet ports or adjuncts.
  - Gateway IP address for all LAN segments containing Communication Manager system ethernet ports, adjuncts, or routers.
  - Are all endpoints (Communication Manager system ethernet ports and adjuncts) on the same local LAN segment?
  - Network routes.

  Network administration information needs to be mapped into specific administration fields.

- Sanity check of information obtained from customer:
  - If Communication Manager system and adjuncts are on different LAN subnets (recommended), gateway IP addresses are different.
  - If Communication Managersystem and adjuncts (CMS or messaging system) are on the same LAN subnet (not recommended):
    - Gateway IP address (if present) and subnet mask information is valid.
    - All IP addresses contain the same subnet address.

Chapter 4: CM connection over a LAN

Communication Manager system connections over a LAN

Any Communication Manager system can use either the TN799DP C-LAN circuit pack or a processor ethernet port on the Communication Manager system to interface to a CMS server using a LAN. This connection can be made in the following ways:

- Connecting with a crossover cable
- Connecting with a LAN hub or a network switch (recommended configuration)
- Connecting over a customer LAN

Connecting one or more ACDs using a LAN

Any Communication Manager system equipped with a TN799DP C-LAN circuit pack or a processor ethernet port can interface to a CMS server using a LAN. CMS servers are equipped with at least two ethernet ports for network connections.

- The connection to the Communication Manager system must be dedicated to a second ethernet port which is provided on a PCI or SBus card in the CMS server.
- The primary built-in ethernet port can be used for printers, CMS Supervisor.

Avaya recommends that these two network connections be on different subnets.

Detailed parts lists and cabling diagrams are shown later in this document for each Communication Manager system that supports a LAN connection.

Ethernet ports on the Communication Manager system

The Communication Manager system provides an ethernet port using either the TN799DP C-LAN circuit pack or the processor ethernet port. For connectivity purposes, it does not matter which ethernet port is used, but the correct port must be administered on the Communication Manager system.

Ethernet ports on a CMS server

CMS servers are equipped with at least two ethernet ports for network connections.

- The connection to the Communication Manager system must be dedicated to a second ethernet port which is provided on a PCI or SBus card in the CMS server.

- The primary built-in ethernet port can be used for printers and CMS Supervisor. Avaya suggests that these two network connections be on different subnets.

Important:

- If possible, ensure that the Communication Manager connection is isolated

Data transfer speed

All TN799DP C-LAN circuit packs support 10 Mbps ethernet connections. The TN799DP and later supports 10 and 100 Mbps ethernet connections as long as all the connecting equipment supports that speed. If you use 10 Mbps hubs between the Communication Manager system and the CMS, the speed of the connection will be 10 Mbps.

The processor ethernet port on the S8xxx servers support 10 Mbps and 100 Mbps, autosensing.

The TN799DP C-LAN circuit pack also uses the IP Media Processor adapter (Material ID 848525887) to provide an ethernet modular jack connection on the Communication Manager system backplane. This adapter must be used to attain 100 Mbps connections.

The LAN speed of 1 Gbps is also supported to both processor ethernet and C-LAN.

Chapter 5: Sample configurations

Sample configurations

The CMS server can connect to a Communication Manager system in a number of ways using a LAN. This section shows some examples of how this can be done. Though several sample configurations are shown, there will be variations not shown here. All but the most basic configurations require planning by the customer and account team.

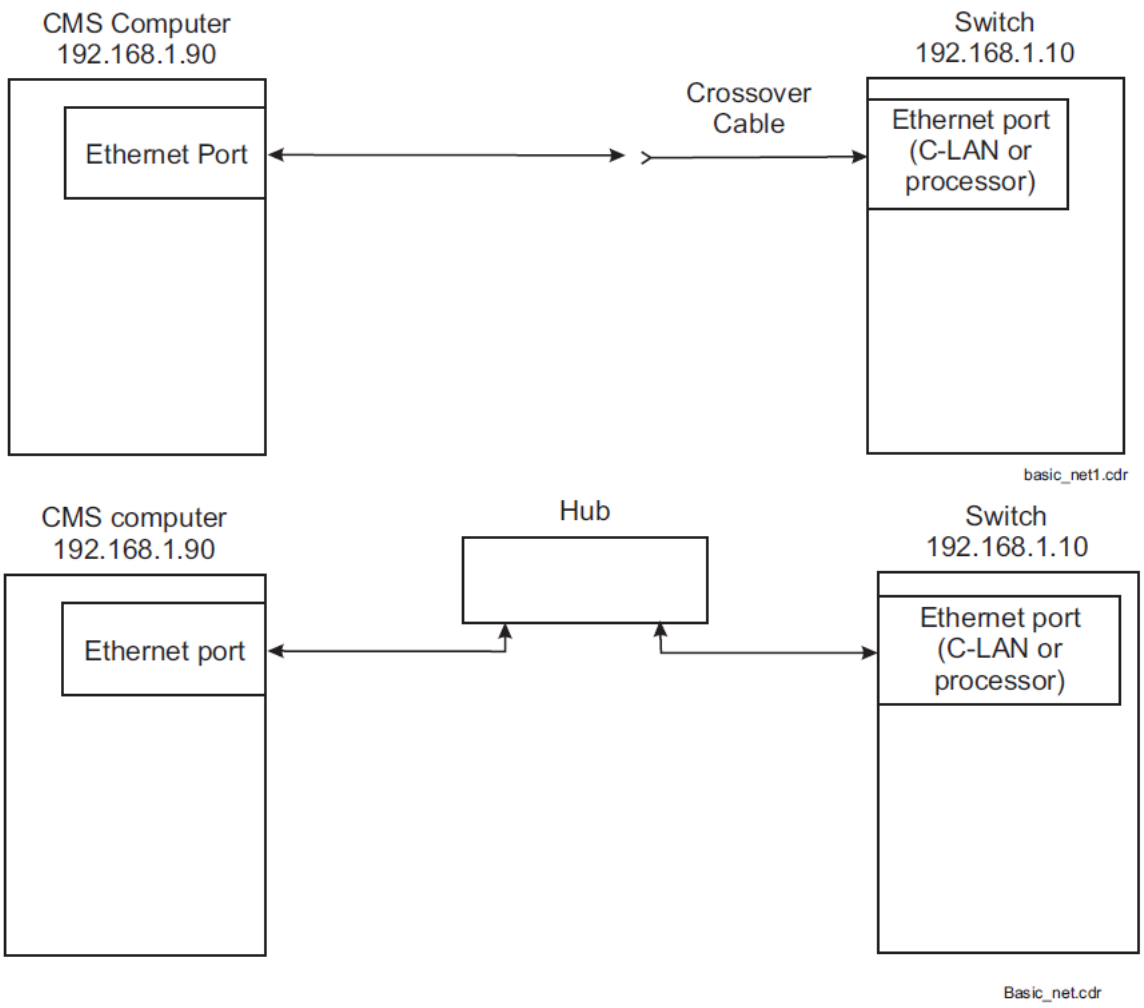
Note:

Note that the IP addressing shown in these examples reflects a basic recommended scheme that can be used if the customer does not have their own addressing requirements.

Basic configuration

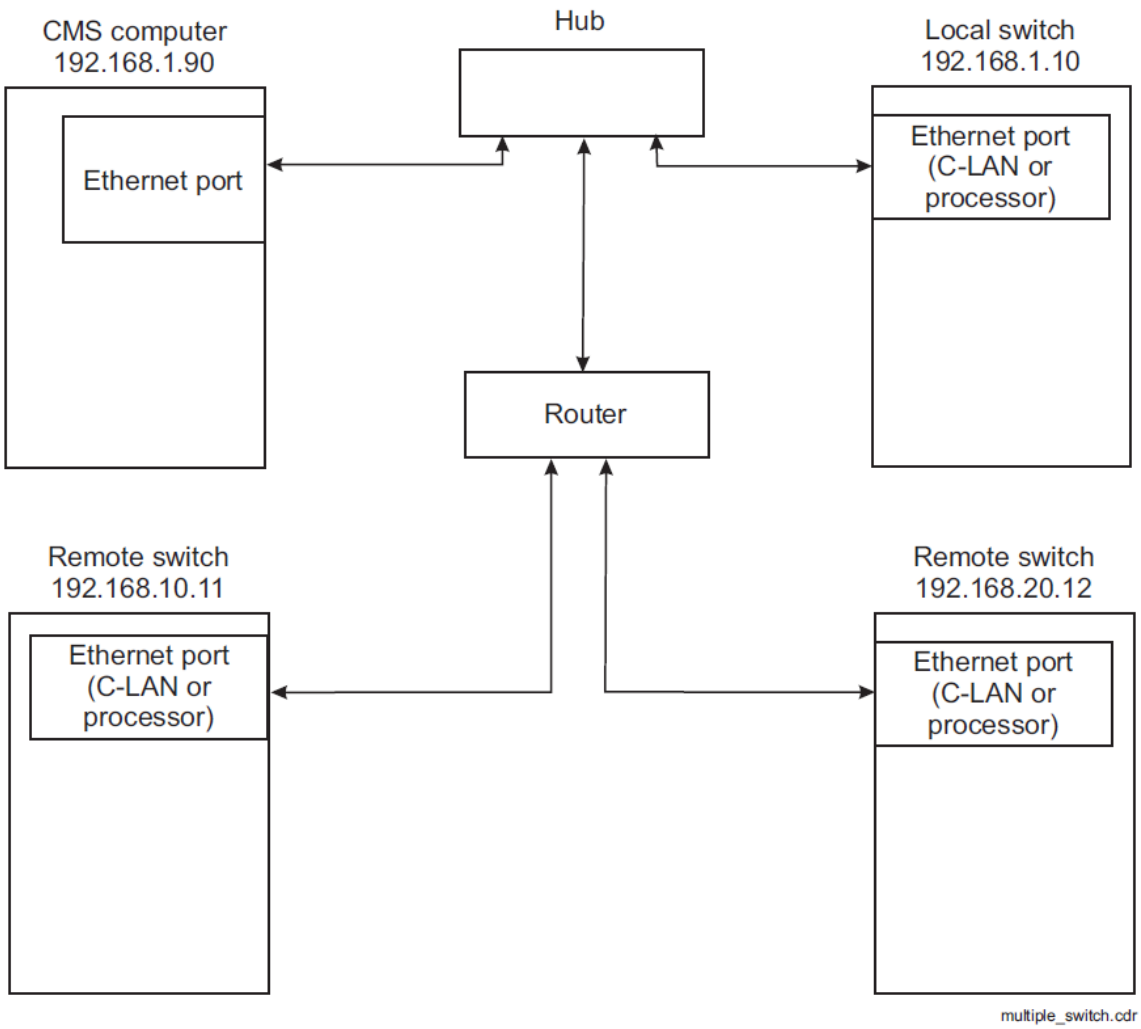
In the most basic configuration, you can create a LAN between a CMS server and a Communication Manager system using either a crossover cable or a dedicated hub. This setup provides isolation from the customer data network, keeping all Communication Manager system-to-CMS messaging traffic on a dedicated private network. The CMS server is directly connected to the Communication Manager system, and neither is part of another network.

This configuration is adequate if there is no printer or CMS Supervisor traffic.



Multiple ACDs

The CMS server can collect data from more than one Communication Manager system. The following figure shows how several ACDs (local or remote) would connect to a CMS server over a LAN. This example isolates the Communication Manager to CMS traffic from any other network traffic.

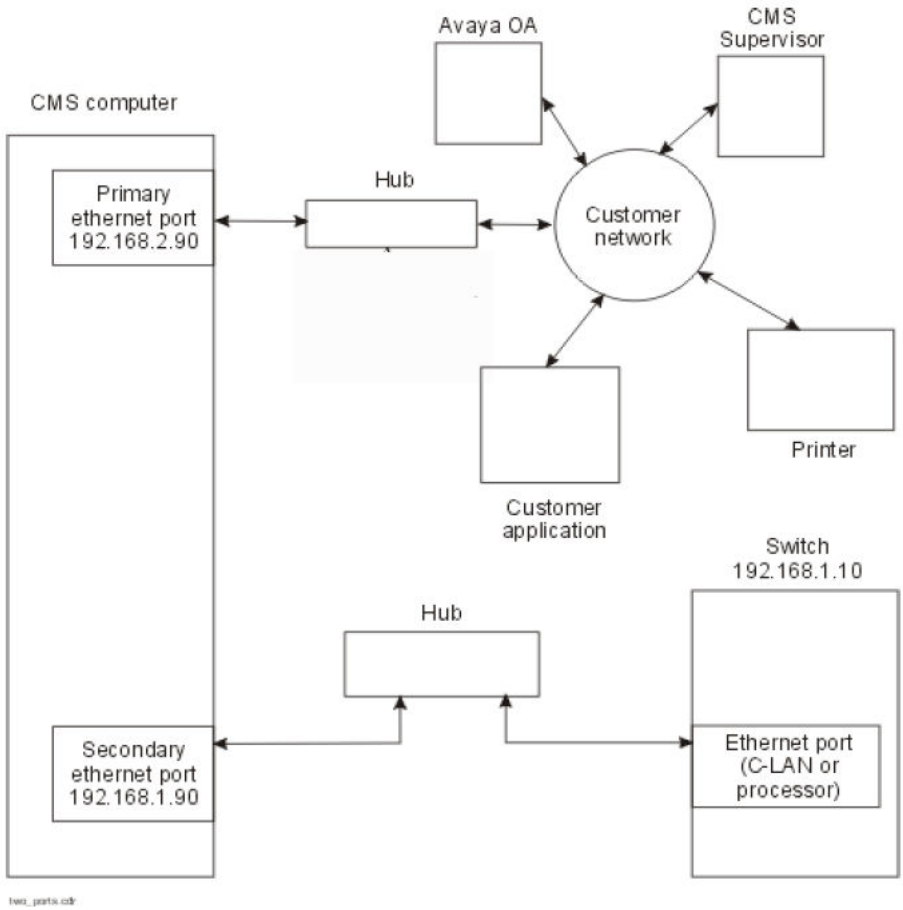


Two ethernet ports on CMS server

If the CMS server is using a LAN for both Communication Manager system link traffic and connections to CMS Supervisor and other network applications, the CMS server should be equipped with two ethernet ports.

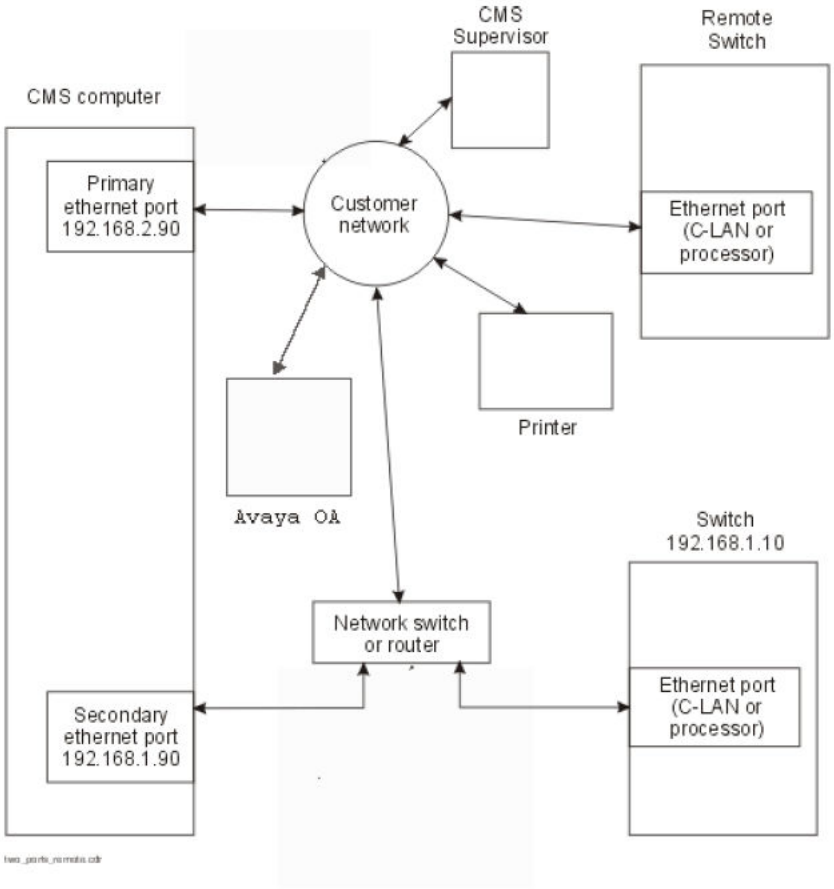
In this configuration, the primary ethernet port is used for all non-Communication Manager system applications. The secondary ethernet port is dedicated for carrying Communication Manager system link traffic. This link can be connected using either a LAN hub or a crossover cable.

Each ethernet port must be administered on different networks, so Communication Manager system-to-CMS traffic does not mix with other traffic.



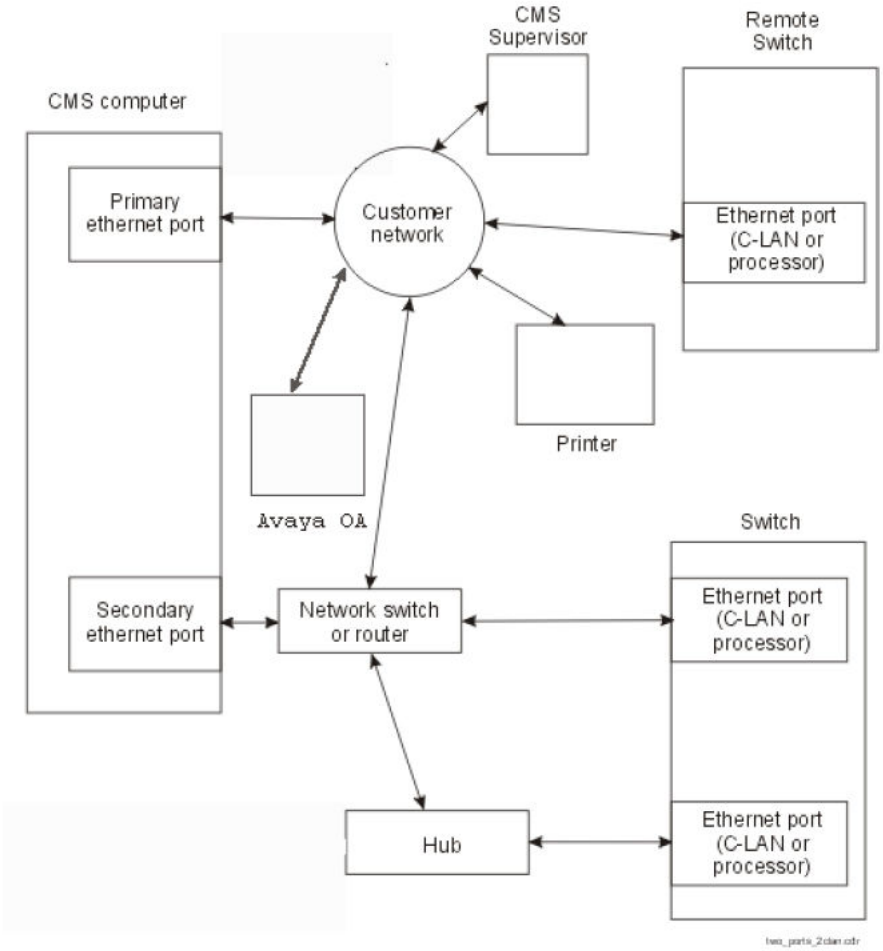
Remote Communication Manager system on the customer network

A remote Communication Manager system can also be connected through the customer network, using a router and a network switch to isolate the Communication Manager system link traffic from the Message Manager traffic and the other customer network traffic.



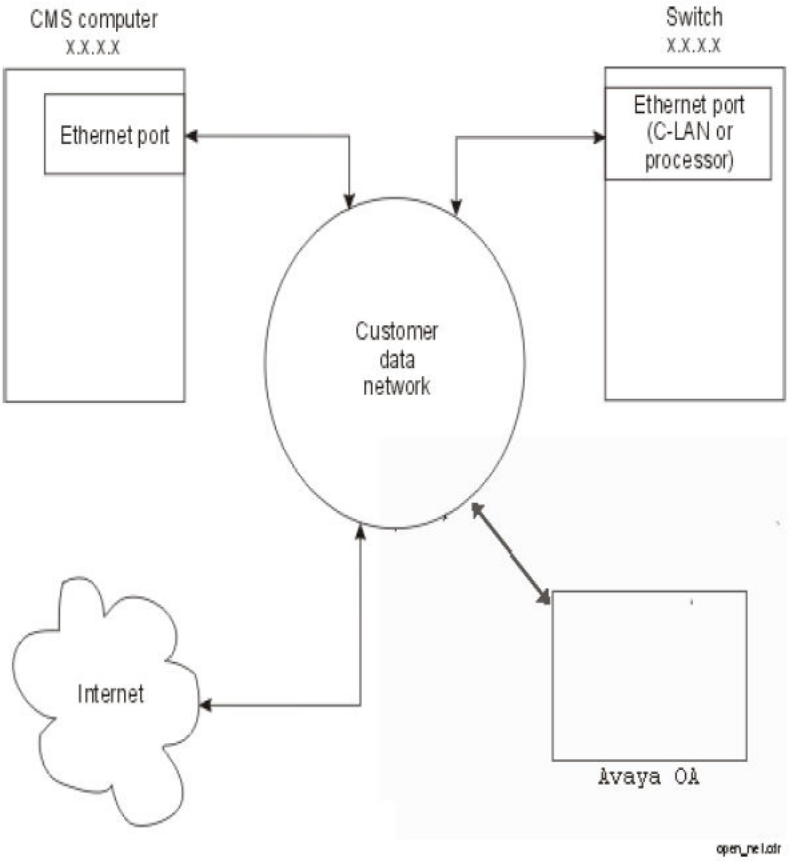
Two ethernet ports option

This configuration shows the best way to isolate the CMS links to the Communication Manager system. This configuration uses two ethernet ports on the Communication Manager system. A router must be used to send traffic from the customer network to the remote Communication Manager system that connects to the CMS server. For true link isolation, this is the best option available.



Public network

In a public network where the customer is connected to the Internet, the default IP addressing cannot be used. For Communication Manager system to CMS traffic, this setup is the least desirable way to set up a Communication Manager system link because of potential message loss on a network that has too much traffic.


CMS computer
x.x.x.x
Ethernet port
Switch
x.x.x.x
Ethernet port
(C-LAN or
processor)
Customer
data
network
Internet
Avaya OA

Chapter 6: Connecting with a crossover cable

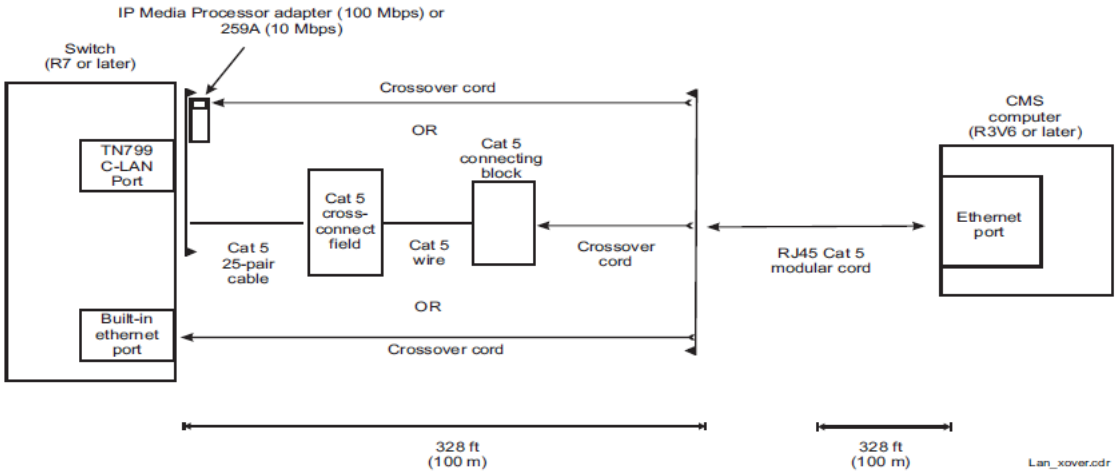
Connecting with a crossover cable

The direct LAN connection is the most basic method to connect the Communication Manager system to the CMS server.

Distance limits

The distance limit for a direct LAN connection is 328 feet (100 meters).

Cabling diagram - LAN via crossover cable



Cabling procedure

About this task

To connect the Communication Manager system to a CMS server using a crossover cable.

Procedure

1. Do one of the following:
   - Attach an adapter (259A, 258B, or 356A) to the backplane connector of the TN799DP C-LAN circuit pack and then attach the plug end of the crossover cable to the adapter. Use jack #1 on the 258B or 356A adapters.

     Connect the ethernet port of a TN799DP C-LAN circuit pack to a Category 5 connecting block using Category 5 cross-connect wiring and then attach the plug end of the crossover cable to the connecting block.
2. Connect one end of an RJ45 Category 5 modular cord to the receptacle end of the crossover cable.
3. Connect the other end of the modular cord to an ethernet port on the CMS server.

Chapter 7: Connecting with a LAN hub or router

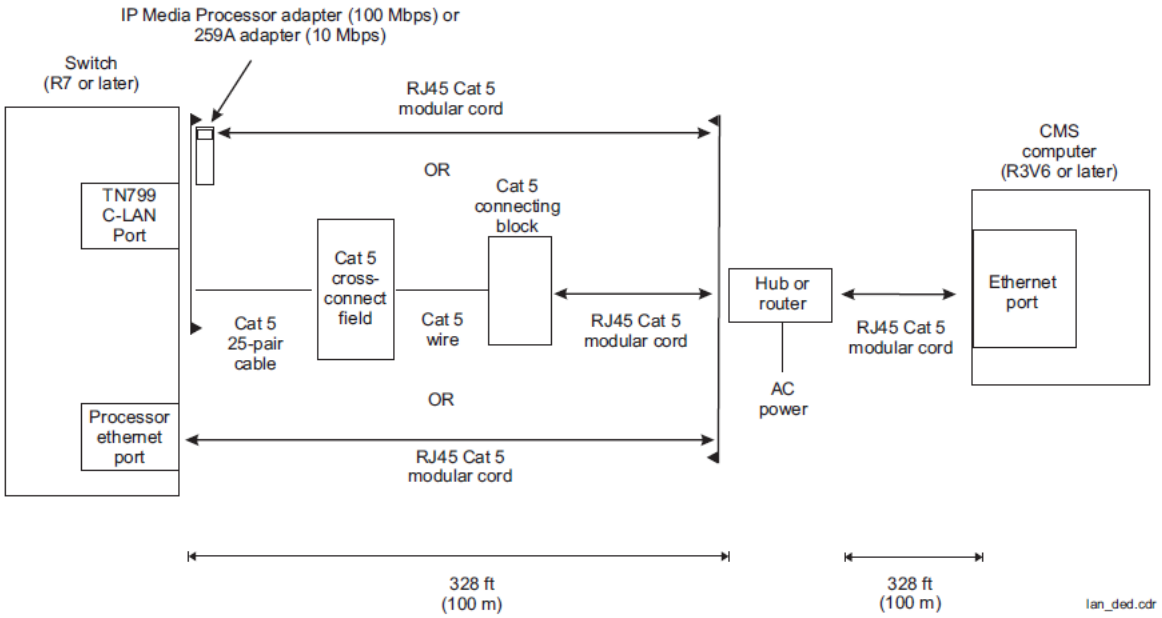
Connecting with a LAN hub or router

The LAN hub or router connection is the recommended method to connect the Communication Manager system to the CMS server. The hub or router can be used to connect to more than one Communication Manager system (multiple ACDs), and to connect to NTS units.

Distance limits

The distance limit for a single hub or router LAN connection is 328 feet (100 meters) from the Communication Manager system to the hub or router, and another 328 feet (100 meters) from the hub or router to the CMS server. If the distance between the Communication Manager system and the CMS server is more than 328 feet (100 meters), you can daisy-chain up to four separate hubs or routers.

Cabling Diagram - LAN via hub or router



Cabling procedure

About this task

To connect the Communication Manager system to a CMS server using a LAN hub.

Procedure

1. Do one of the following depending on your hardware configuration:
   - Attach an adapter (IP Media Processor or 259A) to the backplane connector of the TN799DP C-LAN circuit pack. Attach one end of an RJ45 Category 5 modular cord to the adapter.
   - Connect the ethernet port of a TN799DP C-LAN circuit pack to a Category 5 connecting block using Category 5 cross-connect wiring. Attach one end of an RJ45 Category 5 modular cord to the connecting block.
   - Attach one end of an RJ45 Category 5 modular cord to the processor ethernet port on the Communication Manager system. On the S8100 Server, the processor ethernet port is found on the processor interface cable assembly of the TN2314 processor circuit pack.
   - Attach one end of an RJ45 Category 5 modular cord to either the EXT1 or EXT2 ethernet port on a G700 Media Gateway. A G700 Media Gateway can be controlled by either an S8300 Server or an S87xx Server.
2. Connect the other end of the modular cord to a port on the LAN hub or router.

3. Connect another RJ45 Category 5 modular cord to a different port on the LAN hub or router.
4. Connect the other end of the modular cord to an ethernet port on the CMS server.
5. Connect and apply power to the LAN hub or router.

Chapter 8: Connecting over a customer LAN

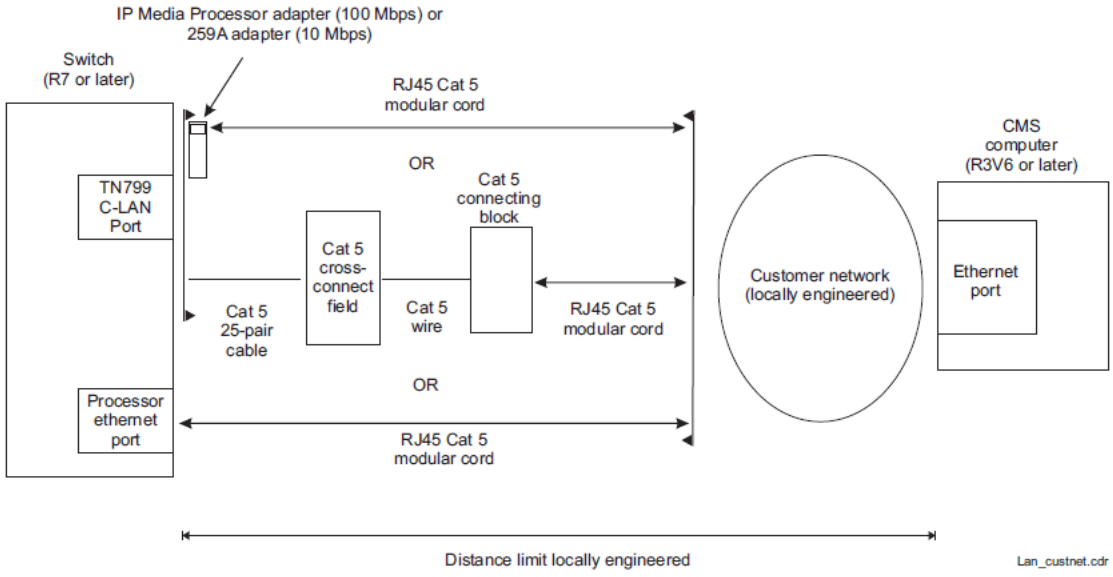
Connecting over a customer LAN

Using a customer network is another method to connect a Communication Manager system to the CMS server. This method is not recommended except in special cases. The LAN hub or router method should be used for most installations.

Distance limits

The distance limit using a customer network must be locally engineered.

Cabling diagram - customer LAN



Cabling procedure

About this task

To connect the Communication Manager system to a CMS server using a customer LAN.

Procedure

1. Do one of the following depending on your hardware configuration:
   - Attach an adapter (IP Media Processor or 259A) to the backplane connector of the TN799DP C-LAN circuit pack. Attach one end of an RJ45 Category 5 modular cord to the adapter.
   - Connect the ethernet port of a TN799DP C-LAN circuit pack to a Category 5 connecting block using Category 5 cross-connect wiring. Attach one end of an RJ45 Category 5 modular cord to the connecting block.
   - Attach one end of an RJ45 Category 5 modular cord to the processor ethernet port on the Communication Manager system. On the S8100 Server, the processor ethernet port is found on the processor interface cable assembly of the TN2314 processor circuit pack.
   - Attach one end of an RJ45 Category 5 modular cord to either the EXT1 or EXT2 ethernet port on a G700 Media Gateway. A G700 Media Gateway can be controlled by either an S8300 Server or an S87xx Server.
2. Connect the other end of the modular cord to a port on the customer data network.
3. Connect from the customer data network to an ethernet port the CMS server.

Chapter 9: Dual IP

Dual IP address

Before using this chapter, ensure that the Dual IP package is installed.

Using the Dual IP address feature, you can switch over to a secondary IP for an ESS/LSP survivable CMS when the connection to the primary Communication Manager system fails. CMS remains connected to the ESS/LSP until the connection is lost, either through a manual link reset or other interventions.

To support survivability in distributed Communication Manager environments, CMS establishes connections with ESS/LSP nodes. Only one secondary IP/host address for one alternate connection is allowed per ACD.

To use the Dual IP feature, you must use the Processor Ethernet (PE) ports instead of the C-LAN ports. Using CMS, you can arrange an alternate IP address to the survivable satellite ESS/LSP in addition to the primary link to the main Communication Manager system for each ACD. CMS establishes a link to either the primary the Communication Manager system or the secondary ESS by connecting to the primary IP address, and then to the secondary IP address when the primary IP address fails to register.

Functional specifications

The functional specifications of the Dual IP feature are as follows:

- After installing the Dual IP package, you can configure an optional secondary IP address in CMS to connect to a survivable Communication Manager system. The secondary IP address can be a hostname or an actual IP address and port number. Do the configuration during the **`cmssvc setup`**, **`cmssvc swsetup`**, and **`cmsadm acd_create`** commands for each ACD.
- If you do not install the Dual IP package, the administration options for the second IP address are not displayed. The option for one IP address for the link to Communication Manager is displayed.
- When establishing a TCP/IP connection to Communication Manager, CMS tries to connect to the primary IP address five times, waiting 30 seconds between each attempt. If unable to connect, CMS tries the Survivable Communication Manager IP address, if assigned, two times, waiting 30 seconds between each attempt.
  - If connection to the Survivable Communication Manager IP address also fails, CMS tries connecting to the primary IP address five times, waiting 30 seconds between each attempt until one of the connections starts functioning.

  - If the main link fails at any time, the entire connection cycle is attempted again until a connection is established with the main Communication Manager or ESS/LSP.
- After the TCP/IP connection is established with the Communication Manager system, CMS requests data. Therefore, a delay occurs before CMS starts processing data, which is normal for link establishment.
- If the link is fully established through the secondary IP, an informational message is recorded in the CMS elog file.
- A new link indicator is used by the clients to show the alternative connection status.
- After Communication Manager fragmentation is resolved, when the primary Communication Manager system gains control again and the ESS is not in control, the ESS eventually drops the link as it becomes inactive. When the link drops, CMS tries to re-establish the connection to the primary link.
  - If you switch back to the primary Communication Manager before the ESS is inactive, manually turn data collection off and back on.

Feature implementation scenarios

The user scenario and the steps implemented by the feature to handle this user scenario are as follows:

1. The primary Communication Manager is inactive and the call processing fails over to the secondary ESS.
   - CMS detects the TCP/IP link problem to the main Communication Manager system and tries to reconnect.
   - After five attempts to connect to the primary Communication Manager system,CMS tries the secondary link. When the TCP/IP connection is established, CMS starts receiving call center traffic data.
2. When the primary Communication Manager system is backed up and ESS releases control of all the resources, the ESS node drops the link.
   - CMS detects a problem with the TCP/IP link to the Survivable Communication Manager system.
   - CMS tries the primary link. When the TCP/IP connection is established, CMS starts receiving call center traffic data.

Scenarios that require manual intervention

Network failure to both the primary Communication Manager and secondary ESS.

- When CMS attempts to establish connections to the primary and secondary IP addresses in a sequence, CMS might connect to the secondary ESS before the main Communication Manager network is available. Manual intervention might be required to correct the situation depending on the nature of the network outage and which Communication Manager system (main or secondary) is operational.

Status message descriptions

CMS Supervisor displays icons and messages that give the status of the link to the ACD. In the PC Client, the windows display the following status indicators:

Indicator	Definition
^	The primary link is active.
v	TCP/IP connection to the primary link is inactive.
-	TCP/IP connection to the primary link is slow or not responding.
*	TCP/IP connection is connected to the Survivable Communication Manager.

Note:

When CMS is connected to the Survivable Communication Manager system, the Connection field in the Connection Status window displays the message “Secondary”.

Data collection exceptions

The system sends the following data collection exceptions when the link is active:

- ACD %s: data collection started.
- ACD %s: data collection started - new translations.

When the primary Communication Manager system starts collecting data, exceptions are generated. When the secondary Communication Manager system starts collecting data, one of the following new exceptions is generated:

- ACD %s: data collection to the Survivable Communication Manager started.
- ACD %s: data collection to the Survivable Communication Manager started - new translations.

Part 3: Administration

Administering the Communication Manager system link

These sections provides procedures to administer the link to a Communication Manager system.

Chapter 10: Administering the link on CMS

Administering the link on CMS

You must set up the Communication Manager system link on CMS using the swsetup option of the `cmssvc` command. This procedure is documented in *Deploying Avaya Call Management System* and *Maintaining and Troubleshooting Avaya Call Management System*.

To set up the Communication Manager system link:

1. Using the `cmssvc` command, turn off CMS.
2. Using the `cmssvc` command, access the **swsetup** option. When you access this option, you are queried for the following information:
   - ACD switch name and model
   - Local and remote port

     The local and remote port assignments must be symmetrical between the Communication Manager system and the CMS. The standard CMS provisioning procedure is to set the local and remote port assignments equal to the Communication Manager system processor channel used for the link. For example, if you use processor channel 10, set the local and remote port to 10.
   - Transport method used to connect to the Communication Manager system (TCP/IP). For TCP/IP, the IP address or host name, and TCP port (the default is 5001).
3. If the CMS server has two ethernet ports, it is possible that the system might attempt to route packets from one interface to another. To prevent this, edit the `/etc/rc2.d/S98cms_ndd` file and add the following line to the end of the file:

   ```
   ndd -set /dev/ip ip_forwarding 0
   ```

   If the file already has this line, do not make any changes.

Chapter 11: Administering CMS and CM release options

Administering the CMS and Communication Manager system release options

Use the following sections to verify release and version information before configuring the ACD link.

Related links

Verifying the software version on page 35
Verifying the call center release on page 36
Setting the reporting adjunct release on page 36

Verifying the software version

Use the System Parameters Customer Options form to verify the software version. If the software version is not correct, apply a new license file that has the correct version.

```
display system-parameters customer-options Page 1 of 12
OPTIONAL FEATURES
G3 Version: V8 Software Package: Enterprise
Location: 2 System ID (SID): 1
Platform: 28 Module ID (MID): 1
USED
Platform Maximum Ports: 71000 3147
Maximum Stations: 41000 142
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 14
Maximum Off-PBX Telephones - OPS: 41000 15
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 2
(NOTE: You must logoff & login to effect the permission changes.)
```

Option	Description
G3 Version	Enter the appropriate software release of the Communication Manager system. If you set this field to an earlier release number, you will not have access to the latest features. Apply a new license file that has the correct version. The G3 Version must be set to V8 or later to use the High Availability option.

Related links

Administering the CMS and Communication Manager system release options on page 35

Verifying the call center release

Use the first Call Center Optional Features page of the System Parameters Customer Options form to set the Call Center Release. If the release number is not correct, apply a new license file that has the correct version.

```
display system-parameters customer-options Page 7 of 12
CALL CENTER OPTIONAL FEATURES
Call Center Release: 7.0
ACD? y Reason Codes? y
BCMS (Basic)? y Service Level Maximizer? n
BCMS/VuStats Service Level? y Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y Service Observing (Remote/By FAC)? y
Business Advocate? n Service Observing (VDNs)? y
Call Work Codes? y Timed ACW? y
DTMF Feedback Signals For VRU? y Vectoring (Basic)? y
Dynamic Advocate? n Vectoring (Prompting)? y
Expert Agent Selection (EAS)? y Vectoring (G3V4 Enhanced)? y
EAS-PHD? y Vectoring (3.0 Enhanced)? y
Forced ACD Calls? n Vectoring (ANI/II-Digits Routing)? y
Least Occupied Agent? y Vectoring (G3V4 Advanced Routing)? y
Lookahead Interflow (LAI)? y Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y Vectoring (Best Service Routing)? y
Multiple Call Handling (Forced)? y Vectoring (Holidays)? y
PASTE (Display PBX Data on Phone)? y Vectoring (Variables)? y
(NOTE: You must logoff & login to effect the permission changes.)
```

Option	Description
Call Center Release	Enter a Call Center Release number that matches the set of Call Center features you want to use. If you set this field to something other than your current Call Center load, you will not have access to the latest Call Center features. Apply a new license file that has the correct version.

Related links

Administering the CMS and Communication Manager system release options on page 35

Setting the reporting adjunct release

Use the following page of the System Parameters Features form to set the Reporting Adjunct Release. Depending on the Communication Manager system software release, this field will be found on different pages.

```
change system-parameters features Page 12 of 19
FEATURE-RELATED SYSTEM PARAMETERS
AGENT AND CALL SELECTION
MIA Across Splits or Skills? n
ACW Agents Considered Idle? n
AUX Agents Considered Idle (MIA)? n
AUX Agent Remains in LOA Queue? n
Call Selection Measurement: current-wait-time
Service Level Supervisor Call Selection Override? n
Auto Reserve Agents: none
Block Hang-up by Logged-in Auto-Answer Agents? y
CALL MANAGEMENT SYSTEM
```

```
REPORTING ADJUNCT RELEASE (determines protocol used by appl link)
CMS (appl mis): R18.1
AAPC/IQ (appl ccr): 5.2.6+
BCMS/VuStats LoginIDs? y
BCMS/VuStats Measurement Interval: half-hour
BCMS/VuStats Abandon Call Timer (seconds):
Validate BCMS/VuStats Login IDs? y
Clear VuStats Shift Data: at-midnight
Remove Inactive BCMS/VuStats Agents? n
```

Option	Description
Reporting Adjunct Release	The field that determines the protocol used by the appl link. The CMS (appl mis) and IQ (appl ccr) parameters determine the Switch Protocol Interpreter (SPI) language protocol used for the CMS (mis) and Avaya IQ (ccr) links. You must administer the mis and ccr links on the Processor Channel Assignment screen. You can assign a maximum of two links for each type of parameter. For example, you can assign two mis links and two ccr links. If you activate Special Application SA9090, you can administer three to four links as application type mis. • If you administer three links as appl type mis, you can administer only one Avaya IQ interface ccr link. • If you administer all four links as appl type mis, you cannot administer the ccr links because the total number of mis and ccr links is four.
CMS (appl mis)	The option to select the CMS release to which you are connecting. You can leave the field blank to indicate that CMS is not connected to the system. This option is the default.
IQ (appl ccr)	The option to select a release of Avaya IQ. You must administer **Expert Agent Selection** (EAS) and **Universal Call ID** (UCID) before establishing a connection with Avaya IQ. Connection to the second Avaya IQ using ccr2 link is optional. You can leave the field blank to indicate that Avaya IQ is not connected to the system. This option is the default.

Related links

[Administering the CMS and Communication Manager system release options](#) on page 35

Chapter 12: Administering data collection options

Administering data collection options

In addition to administering the Communication Manager system link described in this document, you must also administer and understand the following data collection options:

- Enable CMS measuring for hunt groups, trunk groups, and VDNs.
- Assign measured extensions and multiple splits or skills.
- Measured trunks versus unmeasured facilities.
- Interactions with CMS measurements and IP trunk groups.

Chapter 13: Adminstering a C-LAN connection

Administering a C-LAN connection

Use the procedures in this section to administer a TCP/IP connection to a C-LAN circuit pack. This section contains examples of the administration forms with detailed explanations for the required fields. Use the forms in the order shown.

Form	Purpose
`change system-parameter maintenance`	Adding a second packet interface
`add data-module`	Adding an ethernet data module
`change node-names ip`	Adding node names and IP addresses
`change ip-interfaces`	Adding a C-LAN IP interface
`change communication-interface processor-channels`	Adding the processor interface channels
`add ip-route`	Adding IP routes (if needed)

Related links

Adding a second packet interface on page 39
Adding node names and IP addresses on page 40
Adding a C-LAN IP interface on page 41
Adding an ethernet data module on page 42
Adding the processor interface channels on page 43
Adding IP routing on page 44

Adding a second packet interface

Use the Maintenance-Related System Parameters form to add a second packet interface.

```
change system-parameter maintenance Page 2 of 3
MAINTENANCE-RELATED SYSTEM PARAMETERS
MINIMUM MAINTENANCE THRESHOLDS ( Before Notification )
TTRs: 4 CPTRs: 1 Call Classifier Ports: 0
MMIs: 0 VCs: 0
TERMINATING TRUNK TRANSMISSION TEST ( Extension )
Test Type 100: Test Type 102: Test Type 105:
ISDN MAINTENANCE
ISDN-PRI Test Call Extension: 30999 ISDN-BRI Service SPID:
DS1 MAINTENANCE
```

```
DS0 Loop-Around Test Call Extension:
SPE OPTIONAL BOARDS
Packet Intf1? y Packet Intf2? y
Bus Bridge: 01A03 Inter-Board Link Timeslots Pt0: 6 Pt1: 1 Pt2: 1
```

Option	Description
Packet Intf2	Enter y to add a second packet interface.
Bus Bridge	Enter the equipment location of the C-LAN circuit pack that does the bus bridge functionality when the packet bus is activated. This must be administered for the C-LAN 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 Communication Manager system 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.

Related links

Administering a C-LAN connection on page 39

Adding node names and IP addresses

Use the Node Names form to assign the name and IP address of the CMS server and any Communication Manager systems that are networked with the CMS server. With the High Availability option, you will assign two Communication Manager system node names and two CMS server node names.

```
change node-names ip Page 1 of 1
IP NODE NAMES
Name IP Address Name IP Address
3net 192.168.3 .0 . . .
cmshost 192.168.1 .90 . . .
cmshost2 192.168.3 .90 . . .
default 0 .0 .0 .0 . . .
gateway 192.168.1 .211 . . .
gateway2 192.168.4 .211 . . .
switchhost 192.168.1 .10 . . .
switchhost2 192.168.4 .10 . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
( 8 of 8 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Option	Description
Name	Enter the hostname of the CMS server, any Communication Manager systems that are networked with the CMS server, 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 read-only and is not used for this application. For consistency, use the CMS server hostname as defined during the CMS Setup procedure. 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 server.
IP Address	Enter the IP address of the CMS server, the Communication Manager systems, 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.

Related links

[Administering a C-LAN connection](#) on page 39

Adding a C-LAN IP interface

Use the IP Interfaces form to assign a C-LAN circuit pack as an IP interface. For HA, assign two separate C-LAN IP interfaces.

```
change ip-interface proc Page 1 of 2
IP INTERFACES
Type: PROCR
Target socket load: 19660
Enable Interface? y Allow H.323 Endpoints? y
Allow H.248 Gateways? y
Network Region: 1 Gatekeeper Priority: 5
IPV4 PARAMETERS
Node Name: procr IP Address: 10.133.68.220
Subnet Mask: /24
```

Caution:

- If the IP interface is already administered, do not change the administration. Changing the administration could cause failure with IP telephones and other adjunct links.

Option	Description
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 read-only field that shows the designation number of the circuit pack installed in the specified slot.
Node Name	Enter the Communication Manager system node name assigned on the Node Names form. 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 LAN.
Gateway Address	Enter the address of a network node that will serve as the default gateway for the IP interface. For a subnet, the gateway address of the router is required. If the Communication Manager system and CMS server are on the same subnet, no gateway is required. 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.
VLAN	Enter `y` for a virtual LAN, `n` for a standard LAN.
Number of CLAN Sockets Before Warning	Enter the number of C-LAN sockets available before the system issues a warning.
Auto	Enter `y` for auto-negotiation, or `n` for manual speed and duplex settings.
Speed	Set the speed to either `10Mbps` or `100Mbps`.
Duplex	Enter either `full` or `half`.

Related links

[Administering a C-LAN connection](#) on page 39

Adding an ethernet data module

Use the Data Module form to assign the Ethernet port of the C-LAN circuit pack.

```
add data-module 2000 Page 1 of 1
DATA MODULE
Data Extension: 2000 Name: ethernet data module
Type: ethernet
Port: 01A0317
Link: 8
Network uses 1’s for Broadcast Address? y
```

Option	Description
Data Extension	Enter an unassigned extension number.

Table continues…

Option	Description
Type	Enter ethernet.
Port	Enter the equipment location of the C-LAN circuit pack (TN799DP). 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.
Network uses 1's for Broadcast Address	This sets the host portion of the IP address to 0s or 1s. The default is yes (all 1s). Use the default if the private network contains only Avaya Communication Manager systems and adjuncts. Enter `n` only if the network includes non-Avaya switches that use the 0s method of forming broadcast addresses.

Related links

[Administering a C-LAN connection](#) on page 39

Adding the processor interface channels

Use the Processor Channel form to assign the processor channel attributes. For HA, 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 2 2
3: n 0
4: n 0
5: n 0
6: n 0
7: n 0
8: n 0
9: n 0
10: n 0
11: n 0
12: n 0
13: n 0
14: n 0
15: n 0
16: n 0
```

Option	Description
Proc Chan	Select a processor channel for this link.
Enable	Enter `y`.
Appl	Enter `mis`.
Gtwy To	Leave blank for the local CMS to Communication Manager system link.
Mode	Enter `s` for server.

Table continues…

Option	Description
Interface Link	Enter `p` for the processor ethernet port.
Interface Chan	Enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup. For more information, see the CMS installation documentation.
Destination Node	Enter the node name of the CMS server as assigned on the Node Names form. In these examples, `cmshost` is used.
Destination Port	Use the default of 0.
Session Local/ Session Remote	The local and remote port assignments must be symmetrical between the Communication Manager system and the CMS. The standard CMS provisioning procedure is to set the local and remote port assignments equal to the Communication Manager system processor channel used for this link. For example, if you use processor channel 10, set the local and remote port to 10.
Mach ID	Not used for CMS.

Related links

[Administering a C-LAN connection](#) on page 39
[Administering the Communication Manager ethernet port](#) on page 46

Adding IP routing

Use the IP Routing form to set up the IP routes from the Communication Manager system to the CMS server. This is required when either:

- The Communication Manager system and the CMS server are on different subnets.
- When a Gateway Address is not administered for the C-LAN IP interface.

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
Network Bits: 24 Subnet Mask: 255.255.0 .0
Gateway: gateway2
Board: 01C02
Metric: 0
Route Type: Network
```

Option	Description
Route Number	If you are going through a router, you must set up IP route 1 from the Communication Manager system to the router and set up IP route 2 from the Communication Manager system to the CMS server. 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 server or a router, depending on your configuration.

Table continues…

Option	Description
Network Bits (R1.1 and later)	Enter a value from 0-30.
Subnet Mask (R1.1 and later)	Enter a subnet mask.
Gateway	Enter the node name of the gateway by which the destination node is reached for this route. For example, if there were one or more routers between the C-LAN port and the final destination node (the CMS server), the gateway would be the node name of the first router.
C-LAN Board	Enter the equipment location of the C-LAN circuit pack that provides this route. It is possible to have more than one C-LAN circuit pack, but most configurations will only have one C-LAN.
Metric	Specifies the complexity of this IP route. Enter `0` if there are no intermediate nodes between the C-LAN port and the ethernet port on the CMS server. A metric value of 1 is used only on a Communication Manager system that has more than one C-LAN circuit pack installed.

Related links

[Administering a C-LAN connection](#) on page 39

Chapter 14: Administering a processor ethernet port

Administering the Communication Manager ethernet port

Use the procedures in this section to configure a TCP/IP connection over a LAN when connected to a processor ethernet port.

Related links

[Administering a processor ethernet port connection](#) on page 46
[Displaying the processor ethernet port](#) on page 47
[Adding node names and IP addresses](#) on page 47
[Adding the processor interface channels](#) on page 43

Administering a processor ethernet port connection

If the processor ethernet port is not enabled, you must apply a new license file to the Communication Manager system.

```
display system-parameters customer-options Page 5 of 11
OPTIONAL FEATURES
Multinational Locations? n Station and Trunk MSP? n
Multiple Level Precedence & Preemption? n Station as Virtual Extension? n
Multiple Locations? n
System Management Data Transfer? n
Personal Station Access (PSA)? n Tenant Partitioning? n
Posted Messages? y Terminal Trans. Init. (TTI)? n
PNC Duplication? n Time of Day Routing? n
Port Network Support? n Uniform Dialing Plan? y
Usage Allocation Enhancements? y
Processor and System MSP? n TN2501 VAL Maximum Capacity? y
Private Networking? y
Processor Ethernet? y Wideband Switching? n
Wireless? n
Remote Office? n
Restrict Call Forward Off Net? y
Secondary Data Module? y
(NOTE: You must logoff & login to effect the permission changes.)
```

Option	Description
Processor Ethernet	Verify that the processor ethernet port is enabled.

Related links

[Administering the Communication Manager ethernet port](#) on page 46

Displaying the processor ethernet port

Use the IP Interfaces form to display the IP address to the processor ethernet port. Use this form to verify that the IP interface has been administered.

```
display ip-interface procr
IP INTERFACES
Type: PROCR
Node Name: procr
IP Address: 192.9 .22 .245
Subnet Mask: 255.255.255.0
Enable Ethernet Port? y
Network Region: 1
```

Caution:

In most cases, the IP interface is already administered. Changing the configuration may cause failures IP telephone and other adjunct links.

Related links

Administering the Communication Manager ethernet port on page 46

Adding node names and IP addresses

Use the Node Names form to assign the name and IP address of the CMS server and any gateways that are networked with the CMS server. For HA, assign two CMS server node names.

```
change node-names ip Page 1 of 1
IP NODE NAMES
Name IP Address Name IP Address
3net 192.168.3 .0 . . .
cmshost 192.168.1 .90 . . .
cmshost2 192.168.3 .90 . . .
default 0 .0 .0 .0 . . .
gateway 192.168.1 .211 . . .
gateway2 192.168.4 .211 . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
( 8 of 8 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Option	Description
Name	Enter the host name of the CMS server and any gateway hosts used in the network. The processor ethernet port is displayed on this form, but cannot be changed. The node names can be entered in any order. Names are displayed in alphabetical order the next time the form is displayed. The default node name entry is read-only and is not used for this application. These names are also used for the IP interfaces, data module, IP routing, and other forms. If you change the node name in this form, it is automatically updated in 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 server.
IP Address	Enter the IP address of the CMS server 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.

Related links

[Administering the Communication Manager ethernet port](#) on page 46

Adding the processor interface channels

Use the Processor Channel form to assign the processor channel attributes. For HA, 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 2 2
3: n 0
4: n 0
5: n 0
6: n 0
7: n 0
8: n 0
9: n 0
10: n 0
11: n 0
12: n 0
13: n 0
14: n 0
15: n 0
16: n 0
```

Option	Description
Proc Chan	Select a processor channel for this link.

Table continues…

Option	Description
Enable	Enter `y`.
Appl	Enter `mis`.
Gtwy To	Leave blank for the local CMS to Communication Manager system link.
Mode	Enter `s` for server.
Interface Link	Enter `p` for the processor ethernet port.
Interface Chan	Enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup. For more information, see the CMS installation documentation.
Destination Node	Enter the node name of the CMS server as assigned on the Node Names form. In these examples, `cmshost` is used.
Destination Port	Use the default of 0.
Session Local/ Session Remote	The local and remote port assignments must be symmetrical between the Communication Manager system and the CMS. The standard CMS provisioning procedure is to set the local and remote port assignments equal to the Communication Manager system processor channel used for this link. For example, if you use processor channel 10, set the local and remote port to 10.
Mach ID	Not used for CMS.

Related links

[Administering a C-LAN connection](#) on page 39
[Administering the Communication Manager ethernet port](#) on page 46

Chapter 15: Administering a survivable backup CMS

Administering a Survivable Backup CMS

Use the Survivable Processor form to associate a survivable backup CMS for either:

- a C-LAN port on a specific ESS server,
- a processor ethernet port on a specific ESS or LSP server

The Survivable Processor form is administered on the main server. The translations are sent to the ESS server or LSP during a file sync. After the file sync, the information on Page 2 is used by the LSP or the ESS server to connect to the CMS.

On Page 1 of the form, everything but the Network Region is pre-populated based on what was already administered on the Node Name form and the System Parameters ESS form.

```
add survivable-processor ESS1 Page 1 of 4
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET
Node Name: ESS1
IP Address: 192.0.9.0
ID: 30
Type: LSP
Network Region: 1
```

Option	Description
Network Region	Enter the network region in which the LSP or ESS server resides.

Use Page 2 of the Survivable Processor form to administer the CMS that is connected to a C-LAN or processor ethernet interface.

```
add survivable-processor ESS1 Page 2 of 4
SURVIVABLE PROCESSOR - PROCESSOR CHANNELS
Proc Interface Destination Session
Chan Enable Appl. Mode Link/Chan Node Port Local/Remote
1: y mis s p 5001 cmshost 0 7 7
2: n 0
3: n 0
4: n 0
5: n 0
6: n 0
7: n 0
8: n 0
9: n 0
10: n 0
11: n 0
12: n 0
```

```
13: n 0
14: n 0
15: n 0
16: n 0
Field
```

Option	Description
Proc Chan	Displays the processor channel for this link.
Enable	Enter one of the following values in this field: • Enter `n` if this processor channel is disabled on the LSP or the ESS server. • Enter `i` (inherit) if this link is to be inherited by the LSP or ESS server. You can use the inherit option in the following cases: - The main server connects to the adjuncts using a C-LAN and you want the ESS server to use the same connectivity. - The main server connects to the adjuncts using the main server's PE interface and you want the LSP or ESS server to connect to the adjunct using its PE interface. • Enter an `o` to override the processor channel information sent in the file sync from the main server. The override option causes the near-end address of the link to change to a `p` when the translations are sent from the main server to the LSP or the ESS server. Generally, you would want the override option when an adjunct connects to the main server using a C-LAN and you want the adjunct to connect to the LSP or the ESS server's processor ethernet interface. When you enter an `o` in the enable field, you can enter the processor channel information for the LSP or the ESS server in the remaining fields.
Appl	Displays `mis`.
Mode	Enter `s` for server.
Interface Link	Enter `p` when the physical link is the processor ethernet interface on an LSP or ESS. Enter the C-LAN link number when the physical link is a C-LAN on an ESS.
Interface Chan	Enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup.
Destination Node	Enter the node name of the CMS server as assigned on the Node Names form. In these examples, `cmshost` is used.
Destination Port	Use the default of 0.
Session Local/ Session Remote	The local and remote port assignments must be symmetrical between the Communication Manager system and the CMS. For example, if you use processor channel 10, set the local and remote port to 10.

Chapter 16: Admin second IP

Administering and configuring the secondary IP address

When you configure CMS, you must administer a secondary IP address on an existing or new ACD. Use the following commands to administer the connections between CMS and Communication Manager:

- To set up the initial system configuration, add all ACDs to the system, and configure the maximum number of entities to ACDs.

  - `cmssvc: 5) setup`:

- To change the existing Communication Manager system information on CMS.

  - `cmssvc: 7) swsetup`:

- To add a new ACD to CMS.

  - `cmsadm: 1) acd_create`:

For information about how to use these commands, see *Maintaining and Troubleshooting Avaya Call Management System*.

Related links

Secondary connection configuration on page 52
Secondary connection configuration display on page 53

Secondary connection configuration

After you administer the primary connection, you can change the default port number. The default port number specifies the port number assigned to the primary connection.

The system does not prompt the session layer, virtual local ports, and virtual remote ports for the Survivable Communication Manager system. The secondary connection uses the values that are set for the primary connection. For example:

```
Does this switch have a secondary host name or IP address? (y/n): (default: y) y
Enter secondary switch host name or IP Address: 1.2.3.5 4
Enter secondary switch TCP port number (5001-5999): (default: 5004) 5004
```

Related links

Administering and configuring the secondary IP address on page 52

Secondary connection configuration display

If you have administered the secondary connection, the `cmssvc swinfo` command displays the secondary connection.

For example:

```
Switch administration for acd 1:Switch name: denvercm6
Switch model: Communication Mgr 10.x
Vectoring: y
Expert Agent Selection: y
Central office disconnect supervision: y
Local port: 1
Remote port: 1
Link: TCP/IP 1.2.3.4 5004
Secondary Link: TCP/IP 1.2.3.5 5004
```

Related links

Administering and configuring the secondary IP address on page 52

Part 4: Testing

Chapter 17: CM Testing

Communication Manager system tests

TCP/IP link troubleshooting can be done from Communication Manager system and from CMS server. This section describes tests you can run from Communication Manager.

When selecting the CMS adjunct release, make sure that the features you want to use are compatible with the Communication Manager and CMS release.

Related links

CM system test: ping ip-address on page 55
CM system test: ping node-name on page 56
CM system test: netstat on page 56
CM system test: status processor-channels on page 56
CM system test: status link on page 56
CM system test: status data-module on page 57
CM system test: status sys-link on page 57
CM system test: status packet on page 57
CM system test: trace-route on page 57
CM system test: list measurements on page 58

CM system test: ping ip-address

This command sends a test message to the specified IP address to request a remote echo. The results will be either pass or fail, and will show how long the test took to complete. The packet length defaults to 64 bytes, with a maximum of 1500 bytes.

```
ping ip-address X.X.X.X board CCs [packet-length YYYY repeat ZZZ]
```

Where:

- `X.X.X.X` is the IP address of the CMS server.
- `CCs` is the equipment location of the `C-LAN` circuit pack.
- `YYYY` is the size of the test packet.
- `ZZZ` is the number of times the test will be repeated.

Related links

Communication Manager system tests on page 55

CM system test: ping node-name

This command sends a test message to the specified node name to request a remote echo. The results will be either pass or fail, and will show how long the test took to complete. The packet length defaults to 64 bytes, with a maximum of 1500 bytes.

```
ping node-name XXX board CCs [packet-length YYYY repeat ZZZ]
```

Where:

- `XXX` is the node name of the CMS server.
- `CCs` is the equipment location of the C-LAN circuit pack.
- `YYYY` is the size of the test packet.
- `ZZZ` is the number of times the test will be repeated.

Related links

Communication Manager system tests on page 55

CM system test: netstat

Using the system administration terminal on the Communication Manager system, you can use the following commands to test the TCP/IP link:

This command displays the destination IP address, gateway IP address, C-LAN circuit pack used for the route, and the interface for the route:

```
netstat ip-route
```

Related links

Communication Manager system tests on page 55

CM system test: status processor-channels

This command displays the current status of the processor channel used for the TCP/IP link, and the last time and reason that the channel went down:

```
status processor-channels X
```

Where:

- `X` is the processor channel used for the TCP/IP link.

Related links

Communication Manager system tests on page 55

CM system test: status link

This command displays the status for the TCP/IP link. Page 1 of the test shows whether the link is connected and is in service. Page 3 of the test shows whether the link is up or down. If the link is not up, there is a problem in translations or connectivity.

```
status link X
```

Where:

- `X` is the TCP/IP link number.

Related links

Communication Manager system tests on page 55

CM system test: status data-module

This command displays the status for the ethernet data module. This shows which port is connected and if the port is in service.

```
status data-module XXXX
```

Where:

- `XXXX` is the extension number of the ethernet data module.

Related links

Communication Manager system tests on page 55

CM system test: status sys-link

This command displays the status data for a specific system link. Each system link can be listed using the list `sys-link` command. The status includes the type and operational state of the link, the associated processor channel (if any), active alarms and path status, and a list of all hardware components that make up the link path.

```
status sys-link CCsc
```

Where:

- `CCsc` is the cabinet, carrier, slot, and circuit of the system link in question.

Related links

Communication Manager system tests on page 55

CM system test: status packet

This command displays the packet interface status.

```
status packet
```

Related links

Communication Manager system tests on page 55

CM system test: trace-route

This command works using the TN799B C-LAN circuit pack. This command displays the hops traversed from source to destination, along with the IP addresses of the hop points and final destination, and the observed round-trip delay from the source to each hop point. If no reply is received from a hop point, the IP address is blank.

```
trace-route [ip-address X.X.X.X] [node-name nodename] board CCs
```

Where:

- `X.X.X.X` is the IP address of the CMS server.
- `nodename` is the node name of the CMS server.
- `CCs` is the cabinet, carrier, and slot number of the C-LAN circuit pack.

Related links

Communication Manager system tests on page 55

CM system test: list measurements

This command displays Cyclic Redundancy Check and collision counts for the past 24 hours in 15-minute intervals. N/A is displayed if the data cannot be retrieved for any interval.

```
list measurements clan ethernet CCsc
```

Where:

- `CCsc` is the cabinet, carrier, slot, and circuit number of the ethernet port on the C-LAN circuit pack.

Related links

Communication Manager system tests on page 55

Chapter 18: CMS Testing

CMS tests

TCP/IP link troubleshooting can be done from Communication Manager system and from CMS server. This section describes tests you can run from Communication Manager.ping XXX

Related links

CMS tests: netstat on page 59
CMS tests: ping x.x.x.x on page 59
CMS tests: ping XXX on page 59
CMS tests: traceroute on page 60
CMS tests: snoop on page 60
CMS tests: spray hostname on page 60
CMS tests: link status on page 60

CMS tests: netstat

This command displays general network status information.

```
netstat
```

Related links

CMS tests on page 59

CMS tests: ping x.x.x.x

In this command, `X.X.X.X` is the IP address of the Communication Manager system.

```
ping X.X.X.X
```

This command sends a test message to the specified IP address to request a remote echo. The results will be either alive or no answer.

Related links

CMS tests on page 59

CMS tests: ping XXX

In this command,`XXX` is the node name of the Communication Manager system.

```
ping XXX
```

This command sends a test message to the specified node name to request a remote echo. The results will be alive, no answer, or unknown host.

Related links

CMS tests on page 59

CMS tests: traceroute

In this command, `X.X.X.X` is the IP address of the Communication Manager system

```
traceroute X.X.X.X
```

This command traces the route that an IP packet follows from the CMS server to the Communication Manager system. There are more options to the command other than the IP address. Check the manual page for traceroute for more options.

Related links

CMS tests on page 59

CMS tests: snoop

This command allows you to capture and inspect network packets.

```
snoop
```

Related links

CMS tests on page 59

CMS tests: spray hostname

This command sends a stream of packets to a selected host, reports how many were received, and the transfer rate.

```
spray hostname
```

In this command, hostname is the name of the Communication Manager system.

Related links

CMS tests on page 59

CMS tests: link status

This CMS command displays status information for the Communication Manager system links.

```
/usr/sbin/ndd /dev/tcp tcp_smallest_anon_port
tcp_largest_anon_port
```

This command allows you to display the possible range of talk ports randomly assigned by the CMS when communicating with the Communication Manager system. These ports are called ephemeral ports.

You should also check the `/etc/hosts and /etc/defaultrouter` files to verify that the IP addresses and host names are accurate.

Related links

CMS tests on page 59

Appendix A: Resources

Documentation

CMS and CMS Supervisor documents

Title	Description	Audience
Overview		
Avaya Call Management System Overview and Specification	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	All users
Installation and maintenance		
Deploying Avaya Call Management System	Describes how to install and configure CMS in a virtualized VMware or KVM environment.	Implementation engineers, administrators
Deploying Avaya Call Management System in an Infrastructure as a Service Environment	Describes how to deploy CMS in an Amazon Web Services or Google Cloud Platform environment.	Implementation engineers, administrators
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Administrators, support personnel
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS.	Administrators, installation personnel, support personnel
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Administrators, installation personnel, software specialists involved with HA
Using Avaya Call Management System High Availability and Admin-Sync	Describes how to install and maintain your CMS High Availability (HA) system.	Administrators, support personnel
Upgrading		

Table continues…

Title	Description	Audience
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release. This document is focused on full software or platform upgrades.	System administrators, implementation engineers
Avaya Call Management System Base Load Upgrade	Describes how to perform a simplified base load upgrade. You can perform a base load upgrade within a CMS release or for other approved scenarios. Not all releases support base load upgrades.	System administrators, implementation engineers
Administration		
Administering Avaya Call Management System	Provides instructions on administering a call center using CMS Supervisor.	Avaya support personnel, Administrators
Avaya Call Management System Call History Interface	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators, supervisors
Using ODBC and JDBC with Avaya Call Management System	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators, support personnel
Avaya Call Management System Database Items and Calculations	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, support personnel
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, report designers
Avaya Call Management System Security	Describes how to implement security features in CMS.	Administrators, support personnel
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Implementation engineers, system administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Supervisors, administrators
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Supervisors, administrators

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server	All users

Table continues…

Title	Description	Audience
Installing the Avaya Solutions Platform 130 Series	Describes how to install Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel
Maintaining and Troubleshooting Avaya Solutions Platform 130 Series	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Index

N

P

R

S

T

V

W