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

Release 19.2
Issue 1
March 2021

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 mediums which may include product information, 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. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You 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 SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO,YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/licenseinfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, and 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

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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.265 (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 for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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).

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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.

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 Inc.

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.

Contents

Chapter 1: Introduction

Purpose

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

Intended audience

This document is intended for:

- Avaya support personnel
- Contact center administrators

This document assumes a minimum level of technical knowledge on the part of its readers. It assumes, for example, that a reader knows how to use the Communication Manager system administration interfaces and how to connect Communication Manager system hardware.

Chapter 2: Communication Manager system and CMS release compatibility

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

Communication Manager release	CMS software release						
	R16.x	R17.x	R18.0	R18.1	19.0	19.1	19.2
Communication Manager 6.x	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Communication Manager 7.x	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Communication Manager 8.x	No	No	No	Yes	Yes	Yes	Yes
Communication Manager 8.1.2+ Secure	No	No	No	No	No	Yes	Yes

Important:
With CMS Release 19.1 and later and Communication Manager Release 8.1.2 and later, the messaging link between the two systems are now encrypted. For more information, see *Avaya Call Management System Overview and Specification*, *Deploying Avaya Call Management System*, and *Maintaining and Troubleshooting Avaya Call Management System*.

Chapter 3: Connecting the link

This section explains how to connect a CMS server to a Communication Manager system using TCP/IP over a local area network (LAN).

This section includes the following topics:

Overview

The connection between a CMS server and a Communication Manager system allows the CMS software on the computer to receive, store, and format the Automatic Call Distribution (ACD) information it receives from one or more Communication Manager systems.

A technician should be on-site to make the connection from the CMS server to the Communication Manager system and, if necessary, to administer the Communication Manager system for the ACD feature and CMS. The CMS software will not communicate with the Communication Manager system if the ACD feature, CMS, or the Communication Manager system hardware is not properly administered. See Administering the Communication Manager system link on page 37 for more information.

This section includes the following topics:

Local vs remote connections

This section shows both local and remote connections between the Communication Manager system and the CMS server. For clarification, these connections are defined as follows:

- Local - The connections between the Communication Manager system and the CMS server use facilities local to the Communication Manager system, such as a direct connection over a LAN.
- Remote - The connections between the Communication Manager system and the CMS server are 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. If the customer has purchased the High Availability option, you must connect a link from one ethernet port on the Communication Manager system to one CMS server, and a second link from a different ethernet port on the Communication Manager system to another CMS server.

Note:
For the S8300 Server, you cannot have dedicated links to each CMS server; if you want true duplication, you must use a different solution.

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. In particular, you must take into account if the LAN connection includes both a connection to the CMS server and an Avaya Operational Analyst (OA) system. 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 (the built-in ethernet port) is used for other connectivity (printers, terminals, Avaya CMS Supervisor and Avaya OA) 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 (the built-in ethernet port) is used for other connectivity (printers, terminals, Avaya CMS Supervisor and Avaya OA) 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 connect 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 Manager system 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

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

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

This section includes the following topics:

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, and connections to Avaya OA. 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, CMS Supervisor, and connections to Avaya OA. Avaya recommends that these two network connections be on different subnets.

Important:
It is recommended that, if possible, the Communication Manager system connection be isolated to a dedicated LAN port without any other network connections.

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.

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.

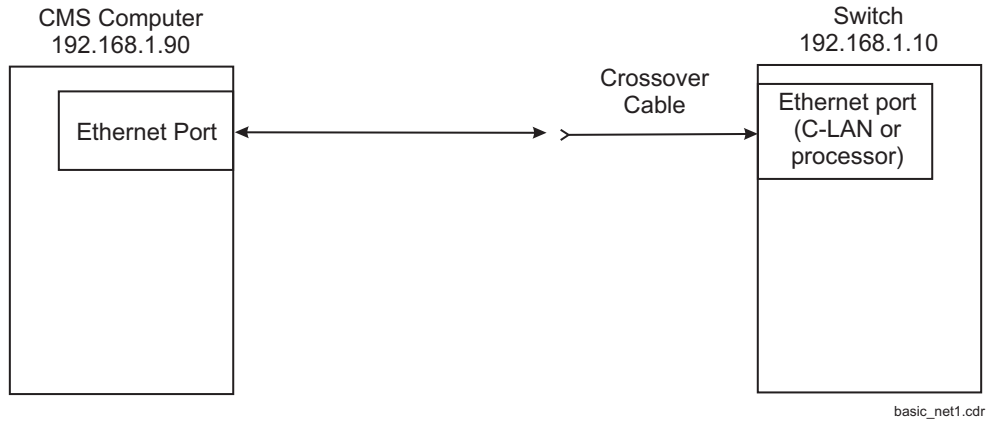
Note:
Please note that the IP addressing shown in these examples reflects a basic recommended scheme that can be used if the customer does not have their own addressing requirements.

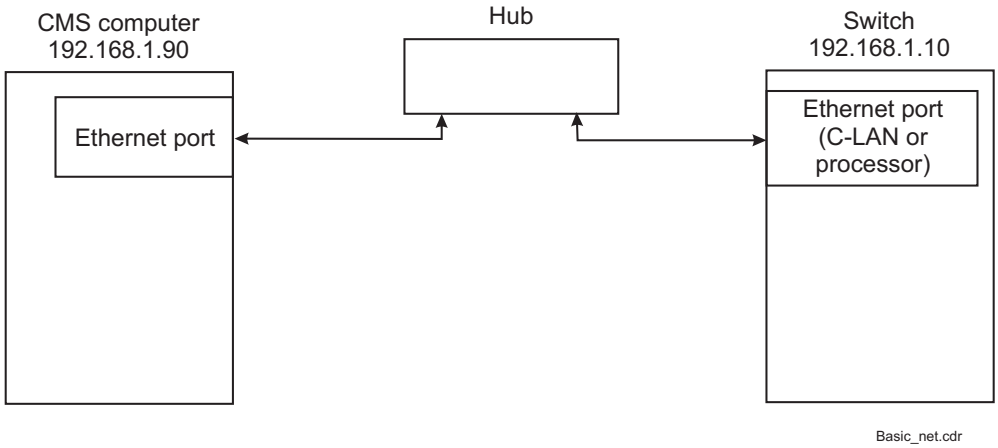
This section includes the following topics:

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.

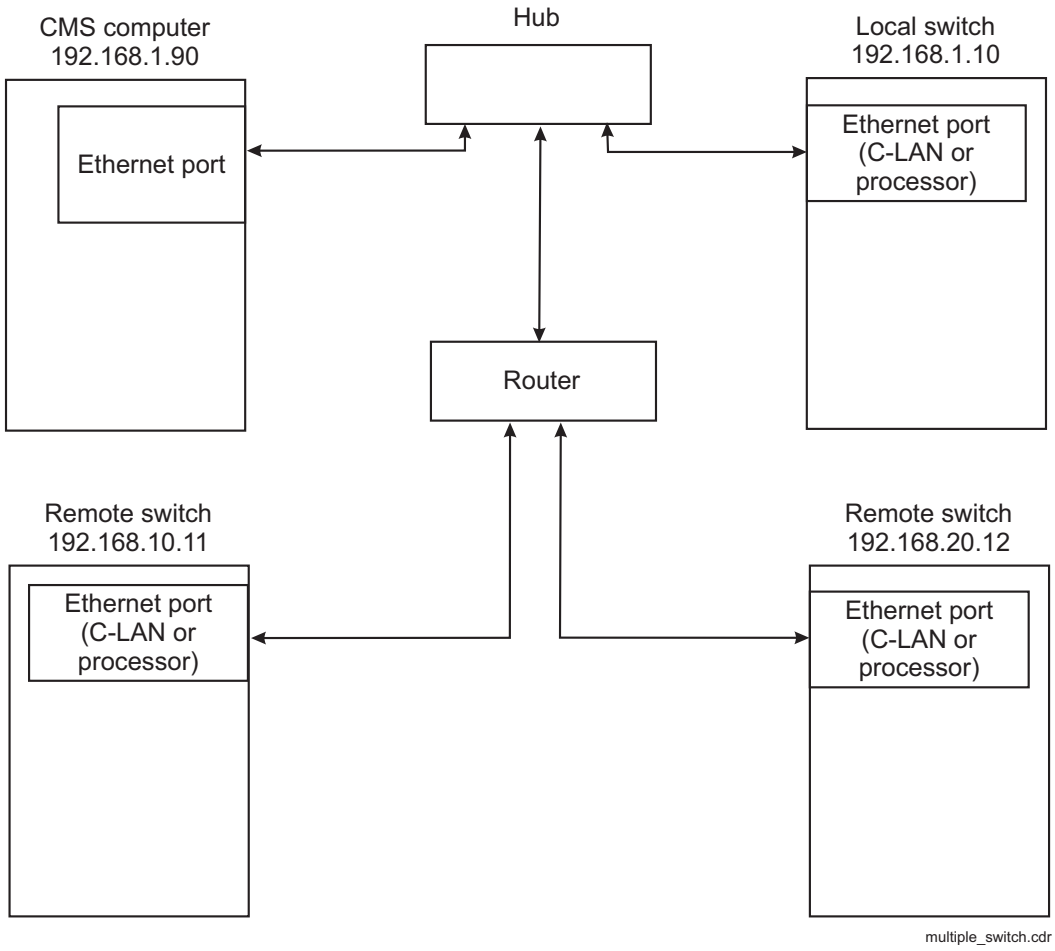
This configuration is adequate if there is no printer or CMS Supervisor traffic.





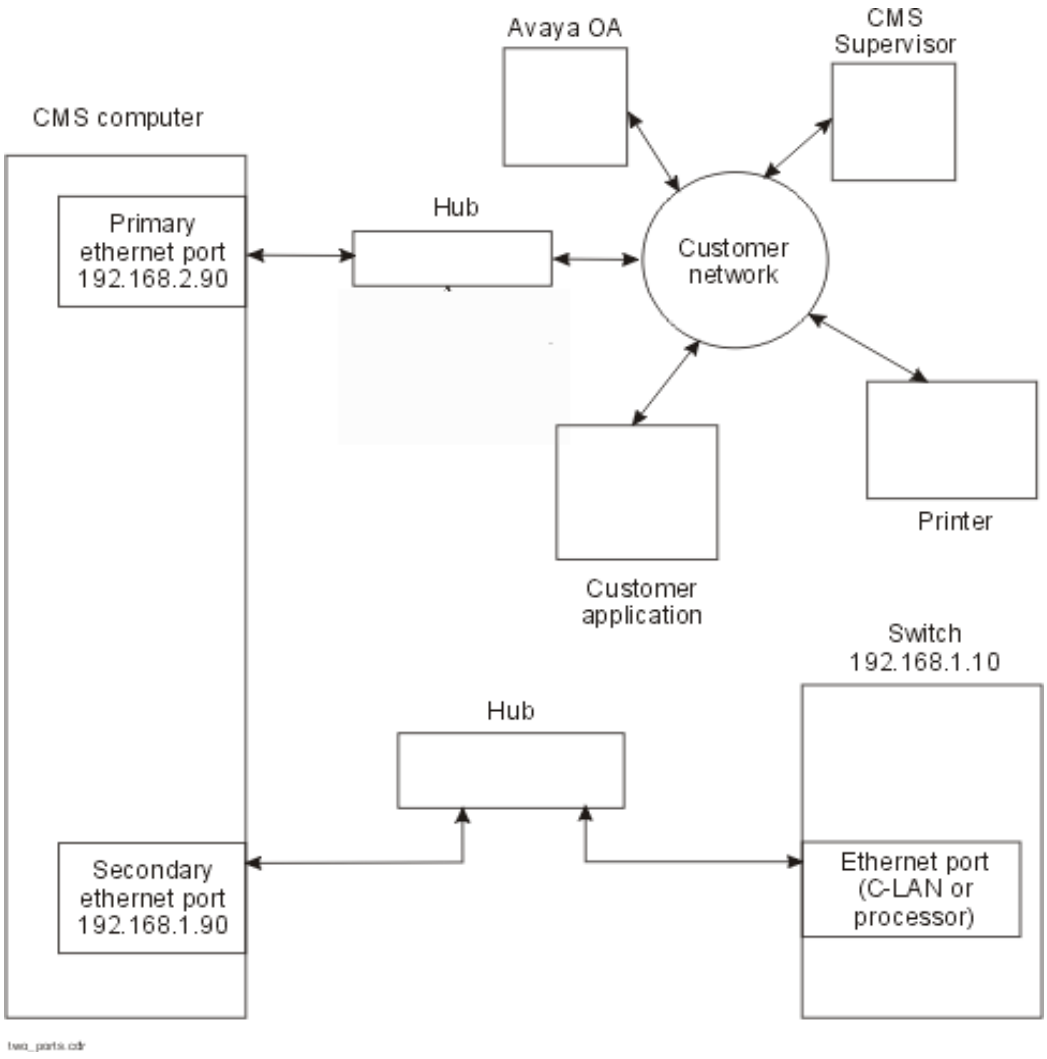
Multiple ACDs (Communication Manager system)

A 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 system-to-CMS traffic from any other network traffic.



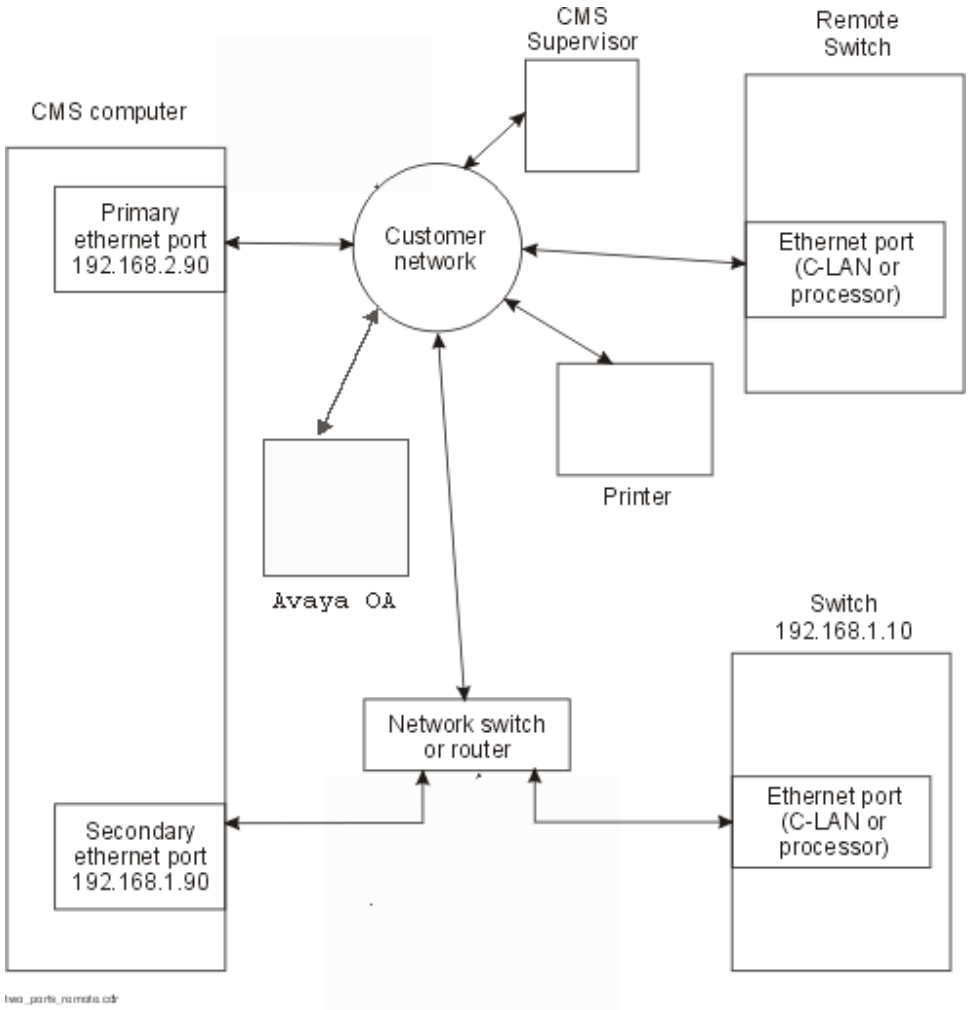
Two ethernet ports on CMS server

If the CMS server is using a LAN for both Communication Manager system link traffic and connections to CMS Supervisor, Avaya OA, 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.



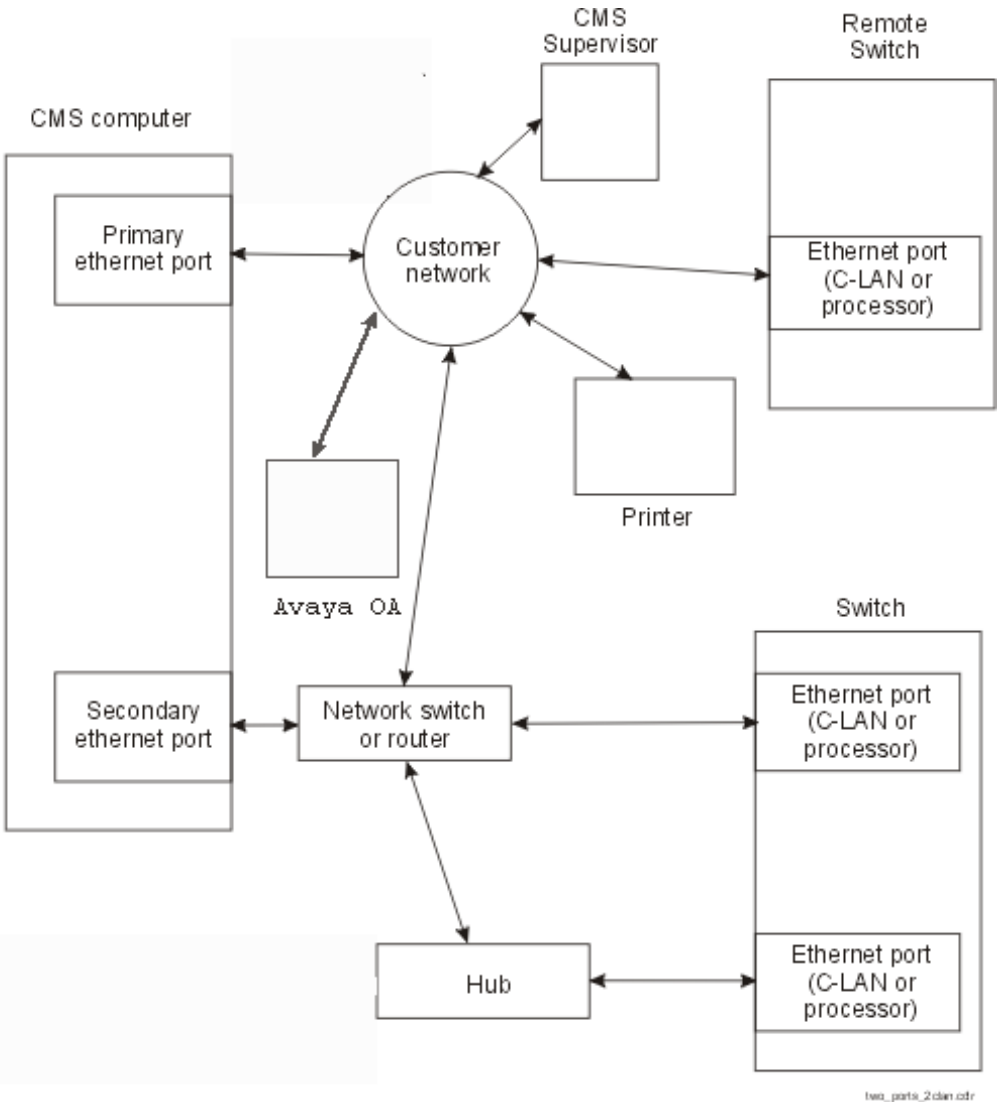
Remote Communication Manager system on the customer network

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.



High availability option

The High Availability option uses dual links from one Communication Manager system to different CMS servers. This option helps ensure that CMS data is not lost if one of the links loses connectivity or if one of the CMS servers goes down.

You can achieve the High Availability option by using separate IP addresses on separate C-LAN cards or Ethernet ports on the Communication Manager system.

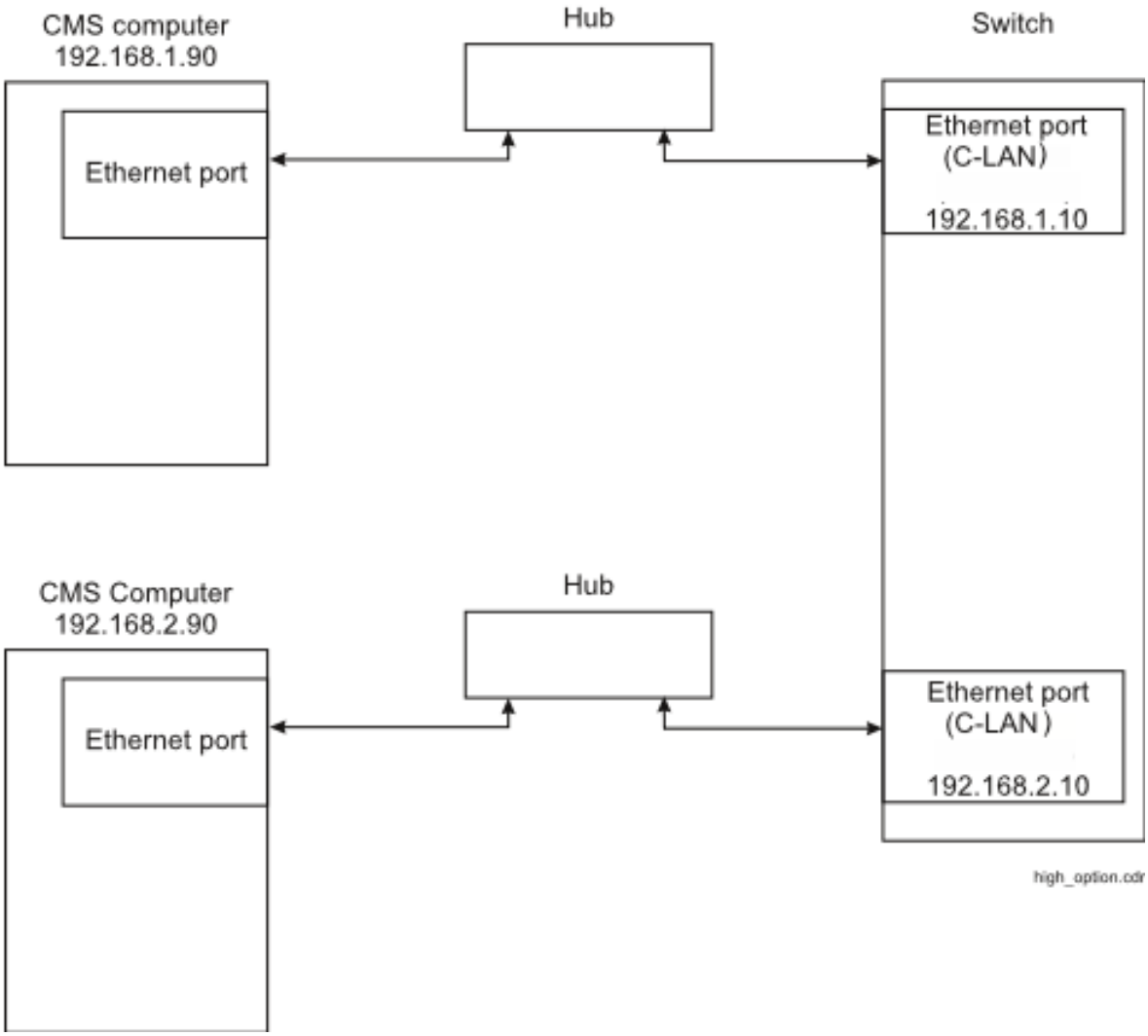
Duplicated Processor Ethernet Communication Manager system port connections are supported, thus removing the need for C-LAN cards on the Communication Manager system. The connection to the Processor Ethernet (PE) applies to High Availability, Survivable CMS and Dual Role CMS. These are all Avaya Professional Services offers.

To configure a solution using the PE interface and any of these offers, contact Avaya Professional Services.

The following figure shows a typical High Availability C-LAN configuration. Though not shown here, you can use a second Ethernet port on the CMS server to isolate the printer and CMS Supervisor traffic.

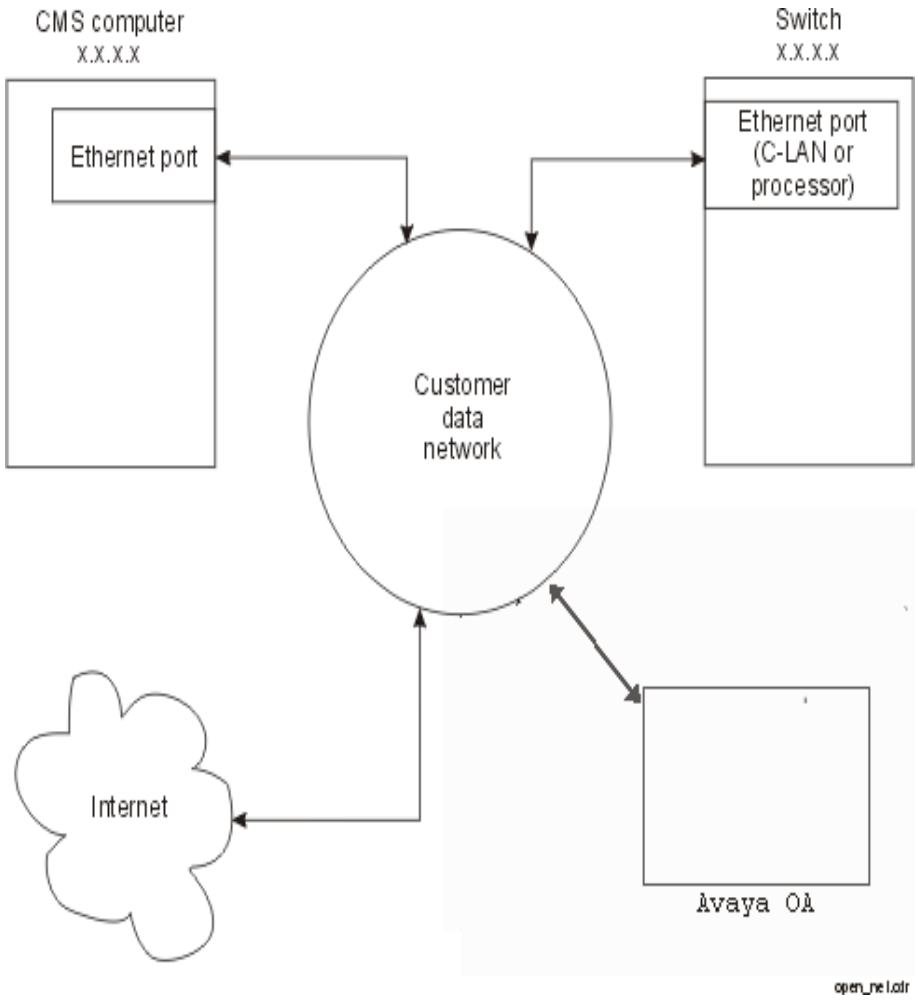
Note:

For the S8300 Server, you cannot have dedicated links to each CMS server. If you want true duplication, you must use a different solution.


CMS computer
192.168.1.90
Ethernet port
Hub
Switch
Ethernet port
(C-LAN)
192.168.1.10
CMS Computer
192.168.2.90
Ethernet port
Hub
Ethernet port
(C-LAN)
192.168.2.10
high_option.cdr

Public network

In a public network where the customer is connected to the Internet, the default IP addressing cannot be used. You must administer IP addressing based on the customer requirements. 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.



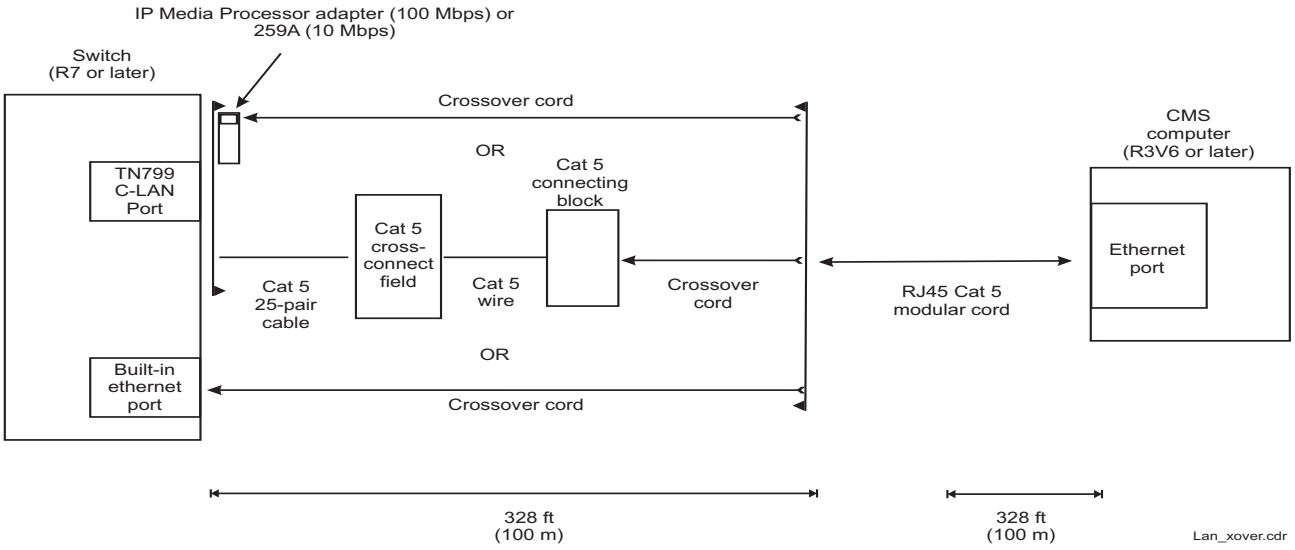
Connecting with a crossover cable

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

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

1. Do one of the following:
   - Attach an adapter (259A, 258B, or 356A) to the backplane connector of the TN799DP C-LAN circuit pack, 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, 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.

Connecting with a LAN hub or router

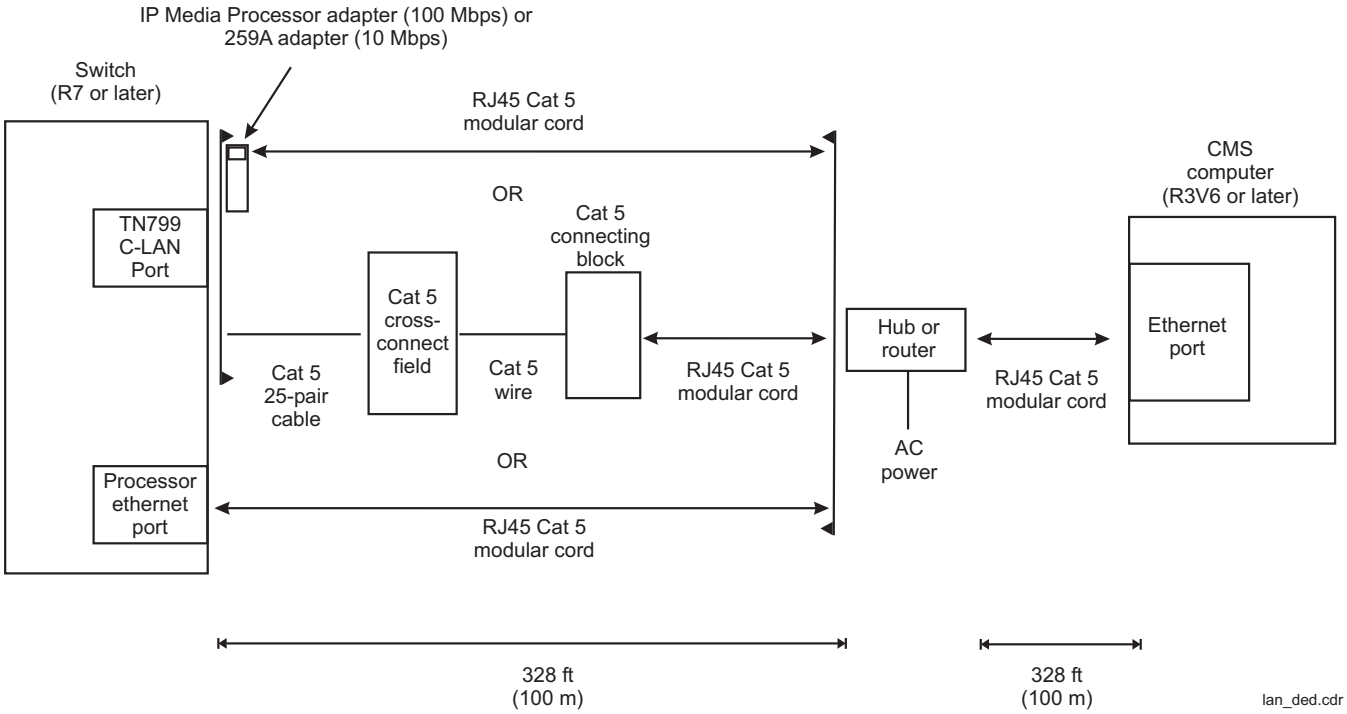
The LAN hub or router connection is the recommended method to connect the Communication Manager system to the CMS server. The hub or router can be used to connect to more than one Communication Manager system (multiple ACDs), and to connect to NTS units.

This section includes the following topics:

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

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

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.

Connecting over a customer LAN

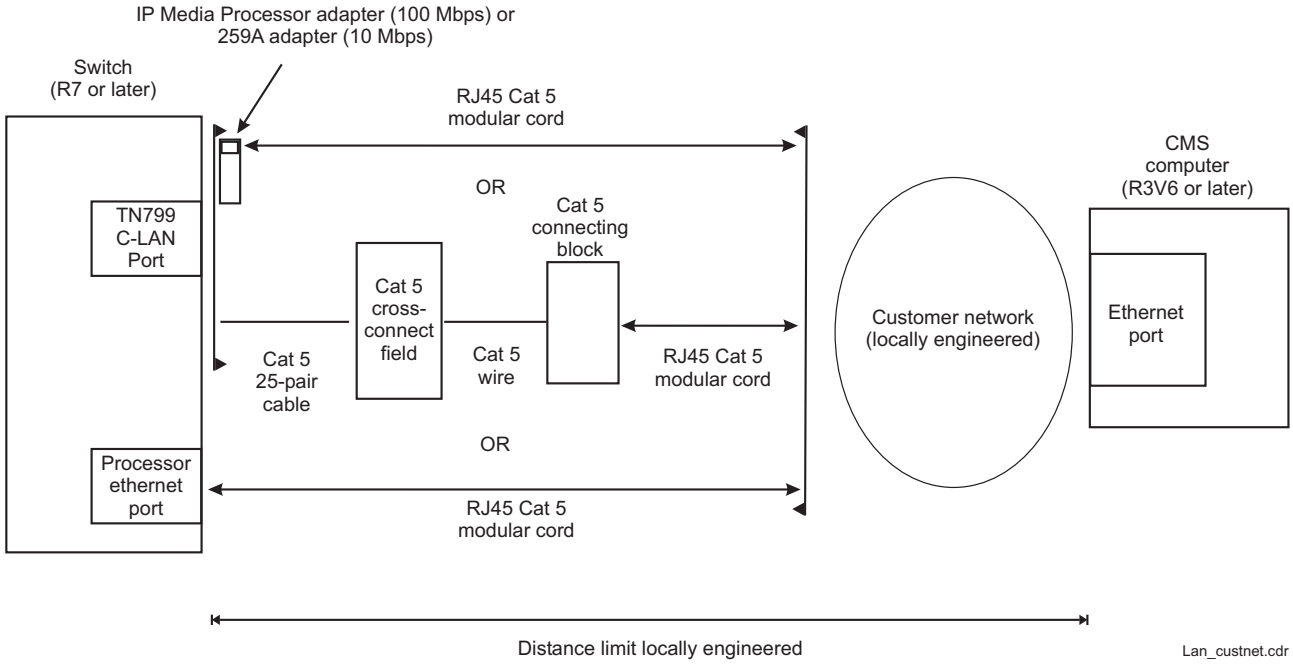
Using a customer network is another method to connect a Communication Manager system to the CMS server. This method is not recommended except in special cases. The LAN hub or router method should be used for most installations.

This section includes the following topics:

Distance limits

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

Cabling diagram - customer LAN



Cabling procedure

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

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 4: Dual IP address

This section describes the Dual IP feature. You must install the Dual IP package to use the feature.

Overview

Using the Dual IP address feature, you can switch over to a secondary IP for an ESS/LSP survivable Communication Manager system 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 CLAN 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 host name or an actual IP address and port number. Do the configuration during the **`cmssvc setup`**, **`cmssvc swsetup`**, and **`cmsadm acd_create`** commands for each Automatic Call Distribution (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 CMS is 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 either the primary or Survivable Communication Manager system, CMS requests for the pump-up 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 a customer switches back to the primary Communication Manager before the ESS is inactive, manually turn the data collection off and back on. CMS tries to re-establish the link through the primary link.

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 is failed over to the secondary ESS.
   - CMS detects the TCP/IP link problem to the main Communication Manager system and tries to re-connect.
   - After five attempts to connect to the primary Communication Manager system, CMS tries the secondary link and is able to establish the TCP/IP connection.
   - CMS pumps up from the secondary link and starts to receive 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 and is able to establish the TCP/IP connection.
- CMS pumps up from the primary link and starts to receive 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 (Communication Manager system). 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 for Automatic Call Distribution (ACD), 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 exception is generated:

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

All exceptions are displayed on the following screens:

- Exception
- Real-time Exception Log and Exception
- Historical Reports
- Other Exceptions
- Data Collection

Chapter 5: Administering the Communication Manager system link

This section provides the procedures to administer the link to a Communication Manager system.

This section includes the following topics:

Administering the link on CMS

In addition to the Communication Manager system administration presented in this section, you must also 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:
   - Communication Manager system name
   - Communication Manager system 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).
- Communication Manager system host name

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, quit out of the file and make no changes.

Administering the CMS and Communication Manager system release options

This section contains release option administration that must be done before you administer the Communication Manager system to CMS server link. The following administration must be done:

- Verifying the software version on page 39
- Verifying the call center release on page 40
- Setting the reporting adjunct release on page 41

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.)
```

Field	Definition
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.

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.)
```

Field	Definition
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.

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
```

Field	Definition
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 maximum two links of 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.

Field	Definition
CMS (appl mis)	The option to select the release of CMS to which you are connecting. The options are: ● **R16.1/R16.x/R17.0**: These releases apply to CMS 16.1, 16.2, 16.3, or 17.0. ● **R18**: This release applies to CMS 18.0.x. ● **R18.1**: This release applies to CMS 18.1.x. ● **R19.0**: This release applies to CMS 19.0.x. ● **R19.1+**: This release applies to CMS 19.1 and later, which uses a secure encrypted link to Communication Manager Release 8.1.2 and later. Connection to the second CMS using mis2 link is optional. 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. The options are: ● 5.1/5.2: Apply to 5.1.x, 5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, and 5.2.5. ● 5.2.6+: Applies to 5.2.6 and 5.3.x. 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.

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

For more details about these data collection options, see “Forms and fields used to enable CMS measurements” in *Administering Avaya Aura™ Call Center Features.*

Administering a TCP/IP connection

The administration for a TCP/IP connection over a LAN is different if you are using a C-LAN circuit pack or if you are using a processor ethernet port as described in Ethernet ports on the Communication Manager system on page 18.

This section includes the following topics:

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)

Note:

If the customer has purchased the High Availability option, you must administer a link from one ethernet port on the Communication Manager system to one CMS server, and a second link from a different ethernet port on the Communication Manager system to another CMS server.

This section includes the following topics:

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
```

Field	Definition
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 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**.

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
```

Field	Definition
Name	Enter the host name 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 display-only and is not used for this application. For consistency, use the CMS server host name as defined during the CMS Setup procedure. See your CMS installation document 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 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.

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 will assign two separate C-LAN IP interfaces.

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.

```
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
```

Field	Definition
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 Communication Manager system node name assigned on 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 LAN.

Field	Definition
Gateway Address	Enter the address of a network node that will serve as the default gateway for the IP interface. If the application goes to points off the subnet, the gateway address of the router is required. If the Communication Manager system and CMS server are on the same subnet, a gateway is not 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** if this is on a virtual LAN or **n** for a standard LAN.
Number of CLAN Sockets Before Warning	Enter the number of CLAN sockets available before the system issues a warning.
Auto	Enter **y** for auto-negotiation or **n** for manual speed and duplex settings.
Speed	Enter either **10Mbps** or **100Mbps**.
Duplex	Enter either **full** or **half**.

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
```

Field	Definition
Data Extension	Enter an unassigned extension number.
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.

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       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
```

Field	Definition
Proc Chan	Select a processor channel for this link. The standard CMS provisioning procedure is to use channel 1.
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 the TCP/IP link number used on the ethernet data module form.
Interface Chan	Enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup. See your CMS software installation document for more information.
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**.

Field	Definition
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.

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:

- The Communication Manager system and the CMS server are on different subnets, or
- 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
```

Field	Definition
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.
Network Bits (R1.1 and later)	Enter a value from 0-30.
Subnet Mask (R1.1 and later)	Enter a subnet mask.

Field	Definition
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 of 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 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. See *Administration for Network Connectivity* for more information about using this field.

Administering a processor ethernet port connection

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

Field	Definition
Processor Ethernet	Verify that the processor ethernet port is enabled.

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.

CAUTION:
In most cases, the IP interface is already administered. Do not change the administration. Changing the administration could cause failure with IP telephones and other adjunct links.

```
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
```

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. With the High Availability option, you will 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
```

Field	Definition
Name	Enter the host name of the CMS server and any gateway hosts used in the network. The processor ethernet port can be displayed on this form, but cannot be changed. 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 server host name as defined during the CMS Setup procedure. See your CMS installation document 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 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.

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    p   5001  cmshost         0       1     1
  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	Definition
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.
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. See your CMS installation document for more information.
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**.

Field	Definition
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.

Administering a Survivable Backup CMS

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

- a CLAN port on a specific ESS server,
- or 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.

Note:
For more information about the Survivable CMS offer, contact Avaya Professional Services.

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
```

Field	Definition
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 CLAN 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	Definition
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. Generally, you would use the inherit option in the following cases: – The main server connects to the adjuncts using a CLAN 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 it's PE interface. ● Enter an **o** (override) to override the processor channel information sent in the file sync from the main server. The override option causes the near-end (server's end of the link) address of the link to change to a **p** when the translations are sent from the main server to the LSP or the ESS server. Generally, you would want the override option when an adjunct connects to the main server using a CLAN 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**.

Field	Definition
Mode	Enter **s** for server.
Interface Link	Enter **p** in this field when the physical link is the processor ethernet interface on an LSP or ESS. Enter the CLAN link number when the physical link is a CLAN on an ESS.
Interface Chan	Enter the TCP channel number (5000-64500). The default for CMS is 5001 and is defined during CMS setup. See your CMS installation document for more information.
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**.

Chapter 6: Administering and configuring the secondary IP address

When you configure CMS, you must administer a secondary IP address on an existing Automatic Call Distribution (ACD) or a new ACD.

Use the following commands to administer the connections between CMS and Communication Manager:

- `cmssvc: 5) setup`: To set up the initial system configuration, add all ACDs to the system, and configure the maximum number of entities to ACDs.

  Note:
  Running this command is mandatory to install a dual IP package.

- `cmssvc: 7) swsetup`: To change the existing Communication Manager system information on CMS.
- `cmsadm: 1) acd_create`: To add a new ACD to CMS.

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

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
```

Secondary connection configuration display

The **`cmssvc swinfo`** command displays the secondary connection if you have administered the secondary connection. For example:

```
Switch administration for acd 1:Switch name: denvercm6
```

```
Switch model: Communication Mgr 6.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
```

Chapter 7: Troubleshooting link connections

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

The information in this section includes:

Communication Manager system administration

Check all Communication Manager system administration. See the following sections:

- Administering the Communication Manager system link on page 37
- Verifying the software version on page 39
- Setting the reporting adjunct release on page 41.

When selecting the CMS adjunct release, make sure that the features you want to use are compatible with the Communication Manager and Call Center Release. For example, if you want to use features specific to Communication Manager 8.0, the Reporting Adjunct Release on the Communication Manager system should be set to at least R18.1, the ACD on the CMS must be administered as Communication Manager 8.0, and the CMS installed must be at least r18.1yy.y.

Communication Manager system tests

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

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, and ***ZZZ*** is the number of times the test will be repeated)

The packet length and repeat options are available with Communication Manager Release 8 or later. 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 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, and ***ZZZ*** is the number of times the test will be repeated)

The packet length and repeat options are available with Communication Manager Release 8 or later. 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.

netstat ip-route

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

status processor-channels *X*

(where ***X*** is the processor channel used for the TCP/IP link)

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 link *X*

(where ***X*** is the TCP/IP link number)

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 data-module *XXXX*

(where ***XXXX*** is the extension number of the ethernet 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 sys-link *CCsc*

(where ***CCsc*** is the cabinet, carrier, slot, and circuit of the system link in question)

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 packet

This command displays the packet interface status.

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, and ***CCs*** is the cabinet, carrier, and slot number of the C-LAN circuit pack)

This command works for Communication Manager Release 8 or later 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.

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)

This command works for Communication Manager Release 8 or later. 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.

Additional references

See the Communication Manager system maintenance documents for more details on these test commands.

CMS tests

Using the system console on the CMS server, you can use the following commands to test the TCP/IP link. More information about the commands can be found by printing out the manual pages (**man *command***).

netstat

This command displays general network status information.

ping *X.X.X.X*

(where ***X.X.X.X*** is the IP address of the Communication Manager system)

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.

ping *XXX*

(where ***XXX*** is the node name of the Communication Manager system)

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.

traceroute *X.X.X.X*

(where ***X.X.X.X*** is the IP address of the Communication Manager system)

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.

snoop

This command allows you to capture and inspect network packets.

spray *hostname*

(where ***hostname*** is the name of the Communication Manager system)

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

Maintenance > Connection Status (from CMS Main Menu)

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.

Chapter 8: 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.	Sales engineers, Administrators
Product Privacy Statement for Avaya Call Management System	Describes how personal data is stored and processed by CMS.	Administrators
Design		
Avaya Customer Experience Virtualized Environment Solution Description	Describes the Avaya Customer Experience Virtualized Environment market solution from a holistic perspective that focuses on the functional view of the solution architecture.	Sales engineers
Installation, upgrades, maintenance, and troubleshooting		
Deploying Avaya Call Management System	Describes how to plan, deploy, and configure CMS on new VMware-based installations.	Avaya support personnel
Deploying Avaya Call Management System on Amazon Web Services	Describes how to plan, deploy, and configure CMS on new Amazon Web Services installations.	Avaya support personnel
Port Matrix for Avaya Call Management System	Lists the ports and connections used by CMS.	Avaya support personnel

Title	Description	Audience
Avaya Call Management System Dell® PowerEdge™ R630 and R730 Hardware Installation, Maintenance and Troubleshooting	Describes how to install, maintain, and troubleshoot Dell® servers used with CMS.	Avaya support personnel
Avaya Call Management System HPE DL20 G9 and DL380 G9 Hardware Installation, Maintenance, and Troubleshooting	Describes how to install, maintain, and troubleshoot HPE servers used with CMS.	Avaya support personnel
Planning for Avaya Call Management System Upgrades	Describes the procedures customers must plan for before and after upgrading to a new CMS release.	Administrators
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release.	Avaya support personnel
Avaya Call Management System Base Load Upgrade	Describes the procedures to upgrade from one base load (for example, 19.1.0.0) to another base load (for example, 19.1.0.1). Not all releases support base load upgrades.	Avaya support personnel, Administrators
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Avaya support personnel, Administrators
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Communication Manager systems used by CMS.	Avaya support personnel, Administrators
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Avaya support personnel, Administrators
User guides		
Using Avaya Call Management System High Availability	Describes how to use and maintain a CMS HA system.	Avaya support personnel, Administrators
Using Avaya Call Management System LAN Backup	Describes how to back up your CMS data using a LAN connection to a remote server.	Administrators
Using Avaya Call Management System High Availability	Describes how to install and maintain your CMS High Availability (HA) system.	Avaya support personnel, Administrators

Title	Description	Audience
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
Administration		
Administering Avaya Call Management System	Provides instructions on administering a contact 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
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, Report designers
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, Operations personnel, Report designers
Avaya Call Management System Security	Describes how to implement security features in CMS.	Avaya support personnel, Administrators.
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Avaya support personnel, Administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Administrators, Operations personnel
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Administrators, Operations personnel, Report designers

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server.	IT Management, sales and deployment engineers, solution architects, support personnel
Installing the Avaya Solutions Platform 130 Appliance	Describes how to install Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel
Maintaining and Troubleshooting Avaya Solutions Platform 130 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Describes procedures to use the iDRAC9 tools on the Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel

WebLM Documents

Title	Description	Audience
Deploying standalone Avaya WebLM in Virtual Appliance	Deploy the application in virtual appliance environment by using Solution Deployment Manager.	Implementation personnel
Deploying standalone Avaya WebLM in Virtualized Environment	Deploy the application in virtualized environment.	Implementation personnel
Deploying standalone Avaya WebLM in Infrastructure as a Service Environment	Deploy the application on cloud services.	Implementation personnel
Deploying standalone Avaya WebLM in Software-Only Environment	Deploy the application in software-only environment.	Implementation personnel
Upgrading standalone Avaya WebLM	Upgrade the application.	Implementation personnel
Administering standalone Avaya WebLM	Administer the system.	System administrators

VMware Documents

VMware component or operation	Document description	Document URL
vSphere Virtual Machine Administration	Provides information on managing virtual machines in the VMware vSphere Web Client for vSphere 6.0 or later. This document also provides information of the following: • Deploying OVF templates • Configuring virtual machine hardware and options • Managing Virtual Machines	https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-55238059-912E-411F-A0E9-A7A536972A91.html
vSphere Web Client	Provides information on how through a browser vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.	https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vcenterhost.doc/GUID-A618EF76-638A-49DA-991D-B93C5AC0E2B1.html

Note:

If the document description (link) are no longer active, consult VMware for documents associated with the component or operation.

Related links

Finding documents on the Avaya Support website on page 77

Accessing the port matrix document on page 78

Avaya Documentation Portal navigation on page 78

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. Click **Support by Product** > **Documents**.

4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click the document to open it in your browser or download the document.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, select one or more of the following categories:
   - Application & Technical Notes
   - Design, Development & System Mgt

   The system displays the Port Matrix document.
7. Click the document to open it in your browser or download the document.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com/.

Important:
For documents that are not available on the Avaya Documentation Center, click **More Sites > Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content in one of the following ways:
  - Type a keyword in **Search**, and click **Filters** to search for content by product or release.
  - From **Products & Solutions**, select a solution and product and then select the appropriate document from the list.
- Sort documents on the search results page by last updated and relevance.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs**.

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon.

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable Include in email notification to receive alerts in email.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:
Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

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.

Procedure

- 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 **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All**, and select **Video** in the **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 key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the list of videos available for the topic. 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.

Related links

Using the Avaya InSite Knowledge Base on page 80

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. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press **Enter**.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Glossary

Automatic Call Distribution (ACD)	A Communication Manager system feature. ACD is software that channels high-volume incoming call traffic to agent groups (splits or skills). Also an agent state where the extension is engaged in an ACD call, with the agent either talking to the caller or the call waiting on hold.
CMS	Call Management System (CMS). A software product used by business customers that have a Communication Manager system and receive a large volume of telephone calls that are processed through the Automatic Call Distribution (ACD) feature of the Communication Manager system.
Split	A group of extensions that receive special-purpose calls in an efficient, cost-effective manner. Normally, calls to a split arrive over one or a few trunk groups.
Switch	A private switch system providing voice-only or voice and data communications services (including access to public and private networks) for a group of terminals within a customer premises.
TSC	Technical Service Center. The Avaya organization that provides technical support for Avaya products.
Transmission Control Protocol/ Internet Protocol (TCP/IP)	A communications protocol that provides interworking between dissimilar systems. It is the de facto standard for computer systems.

Index