Avaya Network Routing 2.0

Overview

Document ID 585-810-001
Issue 2.0
April 2004
Compas ID 100003

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites and does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the following Web site:

http://www.avaya.com/support

Preventing toll fraud

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

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call 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 Web site:

http://www.avaya.com/support

Providing telecommunications security

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

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

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

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

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

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

Your responsibility for your company's telecommunications security

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

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

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

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

Trademarks

Avaya and MultiVantage are trademarks of Avaya Inc.

DEFINITY is a registered trademark of Avaya Inc.

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

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-344-9670 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Avaya Network Routing 2.0
Overview

Contents

Preface

This document describes the Avaya Network Routing 2.0 solutions and the hardware required for the solution. This document was written for all audiences.

Reasons for reissue

Issue 2.0 of this document includes the changes to support Avaya Network Routing 2.0.

Organization

This document includes the following:

Related documents

See the following documents for more information about Network Routing and related features:

Title	Number
Avaya Network Routing 2.0 Documentation Library	585-810-601
Avaya Network Routing 2.0 Overview	585-810-001
Avaya Network Routing 2.0 Installation and Configuration	585-810-101
Avaya MultiVantage Call Center Software Call Vectoring and Expert Agent Selection (EAS) Guide	555-230-714
Avaya MultiVantage Call Center Software Guide to ACD Call Centers	555-230-716
Avaya Communication Manager Call Center Call Vectoring and Expert Agent Selection (EAS) Guide	555-245-783
Avaya Communication Manager Guide to ACD Call Centers	555-245-784

Network Routing solution

Avaya Network Routing enables customers in a multi-communication server network to better control call routing across their network by integrating inter-exchange carrier (IXC) networks and the Automatic Call Distribution (ACD) feature. Network Routing analyzes each incoming call, determines which communication server can best service the call before the call leaves the IXC network, and routes the call from the network to the appropriate communication server. This equalizes the work load for agents and the expected wait time for customers.

This section includes the following topics:

- Description and functional components on page 8
- Benefits on page 12
- Sample call flow on page 13
- Capacities and performance on page 15

Description and functional components

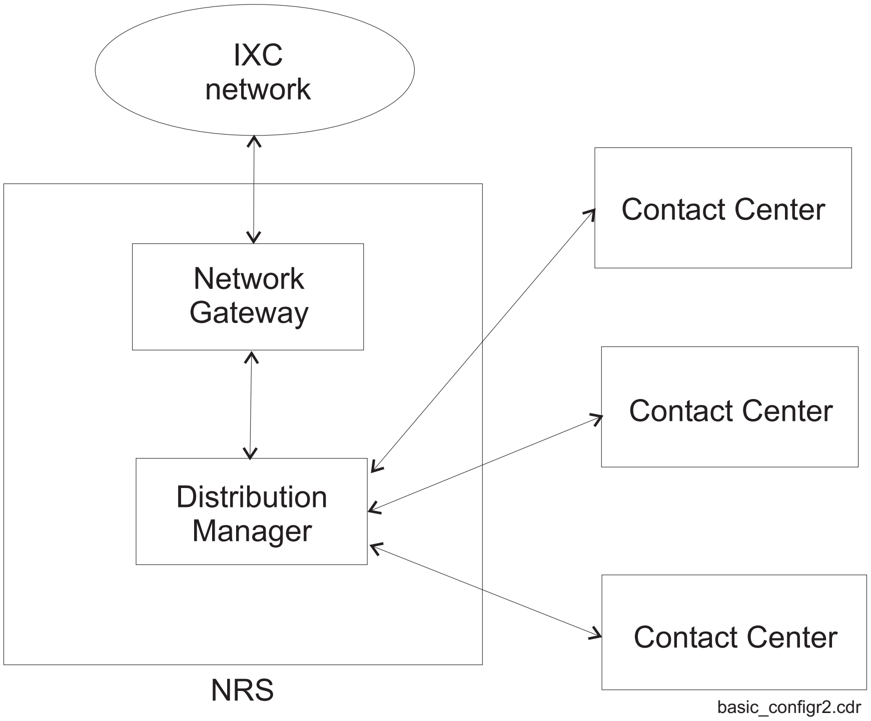
When calls destined for a Contact Center (CC) that uses Network Routing originate in an IXC network, the processing of that call is temporarily suspended while a route request query is sent to the Distribution Manager by way of a Network Gateway, both of which reside on the network routing server (NRS).

As route requests arrive at the Distribution Manager, the Distribution Manager uses its information to determine the most appropriate resource to process the incoming call. Once this has been determined, the Distribution Manager generates a route response that is sent back to the network to route the call to the optimum destination communication server.

As soon as the network receives the route response, it resumes call processing, using the routing information provided by the Distribution Manager. This entire process takes place in a fraction of a second, making the delay imperceptible to the caller.

As shown in the following figure, the Network Routing solution consists of the following functional components:

- Network routing server (NRS) on page 9
- Network Gateway on page 9
- Distribution Manager on page 10
- Contact Centers on page 11



basic_configr2.cdr

Network routing server (NRS)

The NRS is the physical server where the Network Gateway and Distribution Manager reside. See Network routing server (NRS) on page 18 for more information about NRS requirements.

Network Gateway

The Network Gateway functions as a protocol gateway for the Distribution Manager. The Network Gateways are "signaling only" servers and do not terminate bearer traffic. They provide customer specific call routing details that are returned to the IXC and the IXC routes the call as directed.

The type of gateway is dependent on the IXC service provider. The following Network Gateways are supported for Network Routing 2.0:

- AT&T ICP Network Gateway on page 9
- MCI CAP Network Gateway on page 10
- Sprint EnhanCED SiteRP Network Gateway on page 10

⚠ **Important:**
A Network Routing configuration can only support one IXC service provider. You cannot mix two or more IXC service providers in one configuration.

Future releases of Network Routing may support other IXC service providers.

Before configuring a Network Gateway for AT&T or MCI, customers must decide if they want to operate with an active NRS and a hot spare or to run in a load-sharing mode. Sprint will load balance between the two NRSs if they are both in-service.

AT&T ICP Network Gateway

The AT&T Intelligent Call Processing (ICP) Network Gateway, which resides on the NRS, terminates SS7 signaling received from the network and converts this to the "native" Extensible Markup Language (XML) encoded Interface for Network Application Programming (INAP) protocol used by the Distribution Manager. When the interface into the network is SS7-based, an SS7 Network Gateway server is required.

Incoming SS7 messages from the network are converted to their XML-encoded INAP equivalent so that the Distribution Manager can process the messages. Outgoing XML Application Programming Interface (API) messages are converted by the Network Gateway into an SS7 format recognized by the AT&T network.

The Network Gateway interfaces to and is compliant with the AT&T ICP service, TR54022 (1997), an AT&T Data Communications Reference.

MCI CAP Network Gateway

The MCI Customer Access Point (CAP) Network Gateway, which resides on the NRS, interfaces between the MCI toll-free network and the Network Routing Distribution Manager. The CAP Network Gateway receives a route request message from the MCI network and converts the message to the "native" XML encoded INAP protocol used by the Distribution Manager. Outgoing XML API messages are converted by the CAP Network Gateway into a format recognized by the MCI network.

The Network Gateway interfaces to and is compliant with the *WorldCom Gateway to CAP Interface* dated November 7, 2002, Release 1.0, Version 0.9.

Sprint EnhanCED SiteRP Network Gateway

The Sprint EnhanCED SiteRP Network Gateway, which resides on the NRS, interfaces between the Sprint Service Control Points (SCPs) and the Network Routing Distribution Manager.

The SiteRP Network Gateway receives a route request message from the Sprint SCP network and converts the message from the X.25 protocol utilized by the Sprint EnhanCED SiteRP service to the "native" XML encoded INAP protocol used by the Distribution Manager. Outgoing XML API messages are converted by the SiteRP Network Gateway into the X.25 format recognized by the Sprint network.

The SiteRP Network Gateway interfaces to and is compliant with the Sprint EnhanCED SiteRP Interface Specification, date of issue 5/14/01, revision 1.53.

Distribution Manager

The Distribution Manager uses the Virtual Routing software of CC communication servers to obtain Expected Wait Time (EWT) and Average Advance Time (AAT) information for a particular communication server skill or service. After storing this information and adjusting the EWT (now the AEWT) for each call routed, the Distribution Manager maintains a real-time optimum routing “picture” of the CC.

AAT is a function of the number of working agents and the call holding time. AAT equals the Average Hold Time (AHT) divided by the number of agents. The AHT used to compute AAT uses an "exponential average" that increasingly depreciates older data in favor of newer data. AAT can also be derived by the average time between calls coming off of the wait queue.

EWT is one plus the number of calls in queue times the AAT. Each time a route request is made to the Distribution Manager, it will look at the Adjusted EWTs (AEWT) for the CCs in its Network Application and pick the CC with the smallest AEWT. By using AAT, the AEWT will be increased by the value of AAT for each call that is routed to a queue.

Since AAT reflects how many agents are working, sites that have fewer agents will have a larger AAT. For customers who shut down sites, the BSR polling vector could return a large EWT (by considering a queue with no logged in agents) at a certain time or when there are less than *X* agents staffed.

The Distribution Manager uses the XML API to communicate with a Network Gateway to receive route requests and reply with route responses that contains the routing number that is best available to service a call.

A Java applet provides administration, configuration, and monitoring of the Distribution Manager using Microsoft Internet Explorer 5 or later or Netscape Navigator 6.2 or later. Multiple users, administered with read or read/write permissions, can access the Distribution Manager to make changes or view system performance.

Contact Centers

Contact Centers (CC) have an approved Avaya communication server that polls the CC communication servers to obtain Expected Wait Time (EWT) and Average Advance Time (AAT) information for a particular communication server skill or service. After storing this information and adjusting the EWT (now the AEWT) for each call routed, the Distribution Manager maintains a real-time optimum routing "picture" of the CC.

Polling groups and network applications for splits or skills on a CC can be distributed across local port networks or remote expansion port networks (EPNs).

For Network Routing 2.0, Avaya Communication Manager 1.3.1 (load 218.6 or later) and Avaya Communication Manager 2.0 (load 533 or later) are supported on CC communication servers.

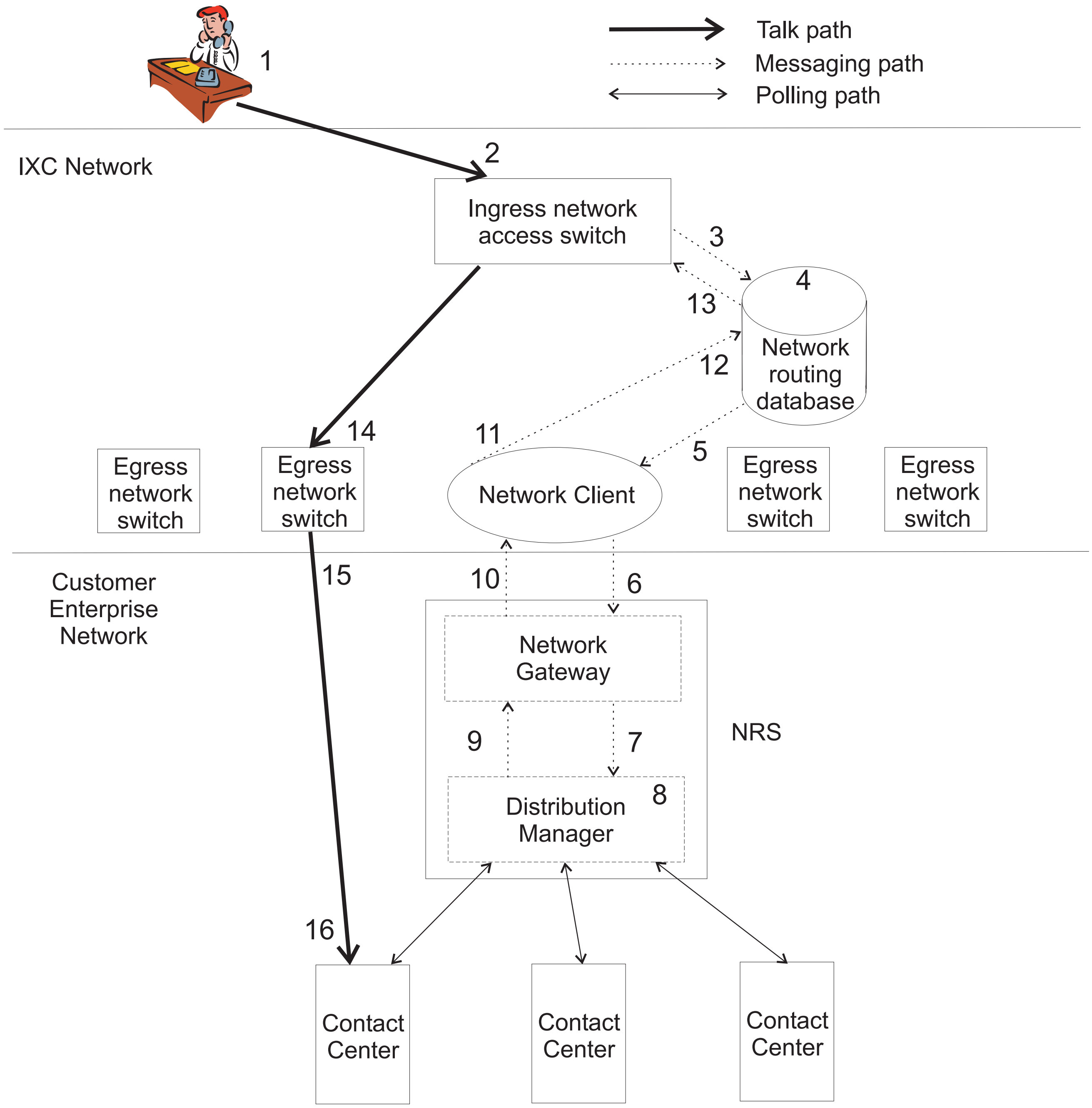
Benefits

Network Routing provides the following benefits:

- Balances the load across multi-site CCs
- Equalizes caller wait-time
- Operates as one virtual CC to gain efficiencies across multiple sites that you normally get only in single, centralized centers in the areas of customer service, staffing, and hours of operation
- Reduces potential abandons at sites with no available agents when other sites do have available agents
- Minimizes operational risk by distributing critical CC resources across multiple geographic locations
- Provides potentially cost effective routing strategies for voice calls using PSTN offered services
- Reduces agent staff while maintaining a high level of service
- Provides real-time, enterprise-wide monitoring to ensure continuous operation and efficient utilization of resources
- Directs voice traffic to desired locations and resources based on caller information
- Routes customer requests among a network of CCs to balance heavy volumes in emergency situations
- Predetermines disaster recovery strategies and application scenarios

Sample call flow

The following figure and notes show a sample Network Routing call flow:



1. A customer dials a telephone number, typically a toll-free number.
2. The call reaches the IXC ingress (originating) network access switch.
3. The originating network access switch queries the IXC network routing database to determine where to route the call (a route request).
4. The IXC network routing database determines that the first-choice route is to query a provisioned customer routing database (for example, an SS7/ICP link or a DAP).
5. The IXC network routing database makes a "route-tag request" of the provisioned Network Control Point (NCP), Remote Data Gateway (RDG), or Service Control Point (SCP).
6. The NCP/RDG/SCP passes the route request to the Network Gateway on the NRS.
7. The Network Gateway, using XML, sends a route request to the Distribution Manager.
8. The Distribution Manager queries the polling database to determine the current best site to service the incoming call.

   To build the polling database, the Distribution Manager calls a reply-best vector on each communication server in the Network Application. The EWT and AAT are returned in the UUI data of the disconnect using a QSIG trunk group.
9. The Distribution Manager sends the routing tag to the Network Gateway.
10. The Network Gateway responds to the route request from the NCP/RDG/SCP with the routing tag.
11. The NCP/RDG/SCP replies to the IXC network routing database with the routing tag.
12. The IXC network routing database consults its provisioning tables and translates the routing tag to an IXC-specific proprietary number called a Routing Telephone Number (RTN).
13. The IXC network routing database responds to the originating network switch route request with the RTN.
14. The IXC originating switch routes the voice call to the proper egress (terminating) switch.
15. The IXC terminating switch delivers the call to the selected CC communication server.
16. The CC communication server receives the call and begins normal vector call processing.

Capacities and performance

Network Routing supports the following capacity and performance characteristics:

- The NRS can poll up to 16 CCs.
- The NRS can have up to 100 polling groups for each CC (splits or skills monitored on each CC).
- The NRS can have up to 1,000 network applications (groups of VDNs/toll-free numbers to which calls are distributed).
- The NRS can process up to 150,000 requests per hour to a Network Gateway.
- The NRS can process up to 60,000 polling requests per hour to the CCs. Since only one poll per second is done to the CC, performance of the CC is minimally impacted. If a polling group contains multiple VDNs on the same CC, and there are many of these polling groups, CC occupancy may be impacted.
- Network Routing has a throughput requirement for the CLAN circuit pack of one message per second. The CLAN link can be shared with other applications except for the Computer Telephony Interface (CTI) application.
- The NRS has a time-out rate of less than 0.01% with the IXC network. If timeouts occur, a default call routing number is selected by the IXC. The timeout for a route response after an NCP/RDG/SCP route request is 500 ms. If timeouts occur to the CCs, a default call routing tag is selected by the Distribution Manager.
- The NRS can support up to 10 simultaneous administrative sessions.

⚠ **Important:**

The performance of the NRS polling is directly dependent on the efficiency of the customer network. That is, if the customer network is engineered to operate properly with minimal traffic delays, the NRS will be able to process polling in an efficient manner. Conversely, if the customer network is not engineered properly and does not handle traffic efficiently, the NRS will not be able to process polling in an efficient manner.

Network Routing component requirements and configurations

This chapter provides a detailed description of the components that support Network Routing. These components include:

- Network routing server (NRS) on page 18
- Contact Center communication servers on page 19
- Sample configurations on page 19

Network routing server (NRS)

The NRS has the following characteristics:

- IBM 345 computer (or approved equivalent), dual 2.0 GHz Xeon CPUs (minimum), 768 MB RAM (minimum)
- Redundant disk drives (18 GB minimum) set up as RAID 1
- Redundant power supplies
- Interface cards:
  - T1-SS7 Multiple Protocol Access Card (MPAC) for AT&T (installed on-site and requires a full-length PCI slot)
  - Dual Network Interface Card (NIC) for MCI (preinstalled at the factory)
  - X.25 interface card for Sprint (installed on-site)
- Red Hat Linux Professional - Version 8.0 (minimum) operating system, the Apache Httpd daemon, and Java support (preinstalled at the factory)
- IBM Informix Dynamic Server - Workgroup Edition, Version 9.40 (preinstalled at the factory)
- Distribution Manager and Network Gateway applications, which provide the Web-based Java interface for administration, configuration, and maintenance (preinstalled at the factory)

Note:

A monitor, keyboard, and mouse are required. These must be provided by the customer. The monitor, keyboard, and mouse can be shared with other servers using a KVM switch.

NRS administration and configuration access

A Java applet on the NRS provides administration, configuration, and monitoring of the Distribution Manager application. You must use Microsoft Internet Explorer 5 or later or Netscape Navigator 6.2 or later and Java plugin 1.4.0 or later. Multiple users (a maximum of 10), administered with read or read/write permissions, can access the Distribution Manager to make changes or view system performance.

Avaya recommends that a minimum of 256 Kbps data access is available between NRSs, NRSs and administrators, and NRSs and CCs. Network delays should be less than 300 ms.

Contact Center communication servers

The CC communication servers require the following software, hardware, and features to support Network Routing:

- Avaya Communication Manager 1.3.1 (load 218.6 or later) and Avaya Communication Manager 2.0 (load 533 or later)
- Virtual Routing is required on all communication servers
- IP trunking required on all communication servers
- CLAN circuit packs (minimum vintage D) required on all communication servers

Sample configurations

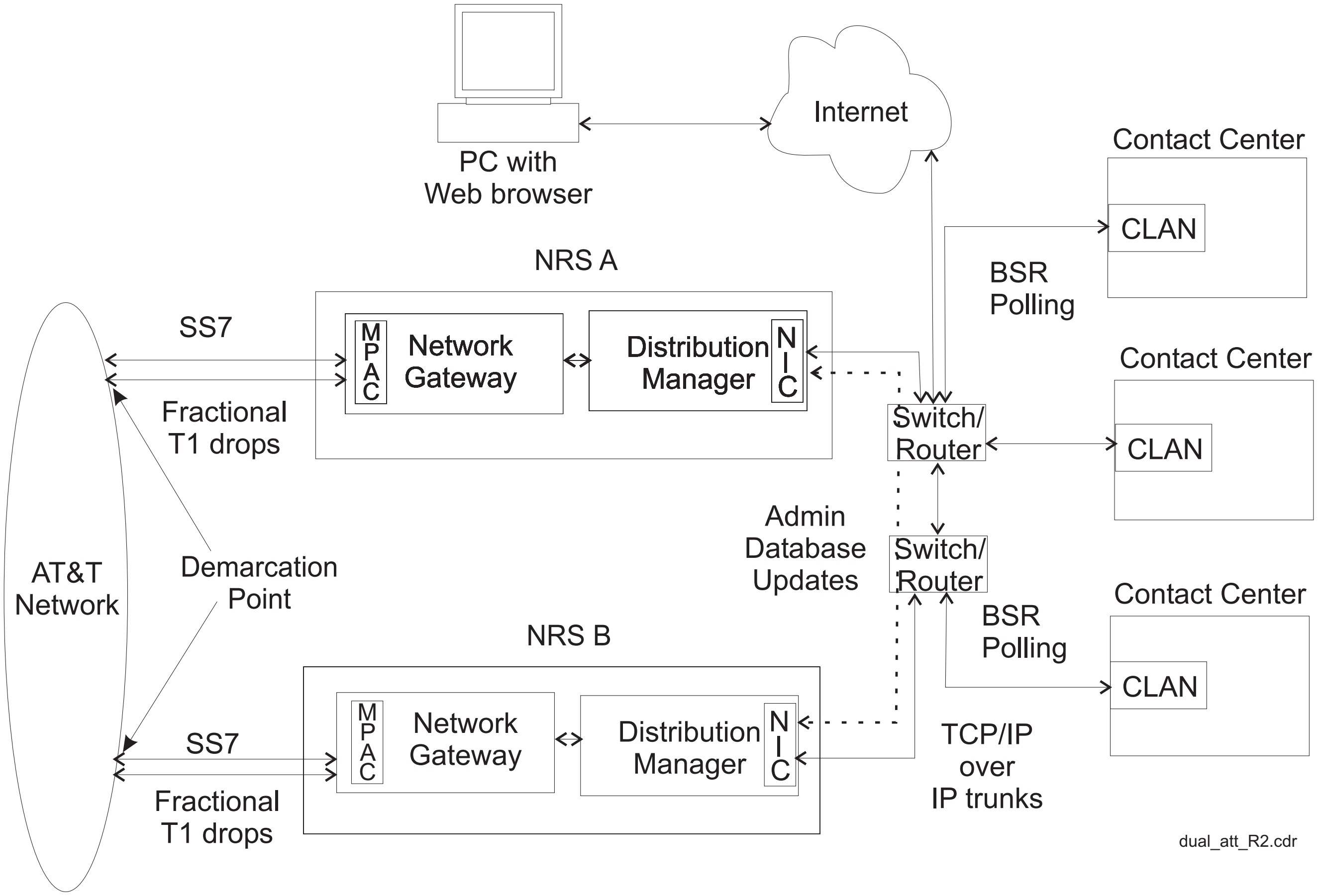
Network Routing requires two NRSs to support a dual simplex configuration for high availability. Avaya recommends that each server be installed in a different physical location to improve availability and reliability. The Distribution Manager on one NRS updates the Distribution Manager administrative database on the other NRS over the TCP/IP network, and updates can go in both directions depending on where changes are being applied.

This section includes the following topics:

- Sample configuration for AT&T on page 20
- Sample configuration for MCI on page 21
- Sample configuration for Sprint on page 22

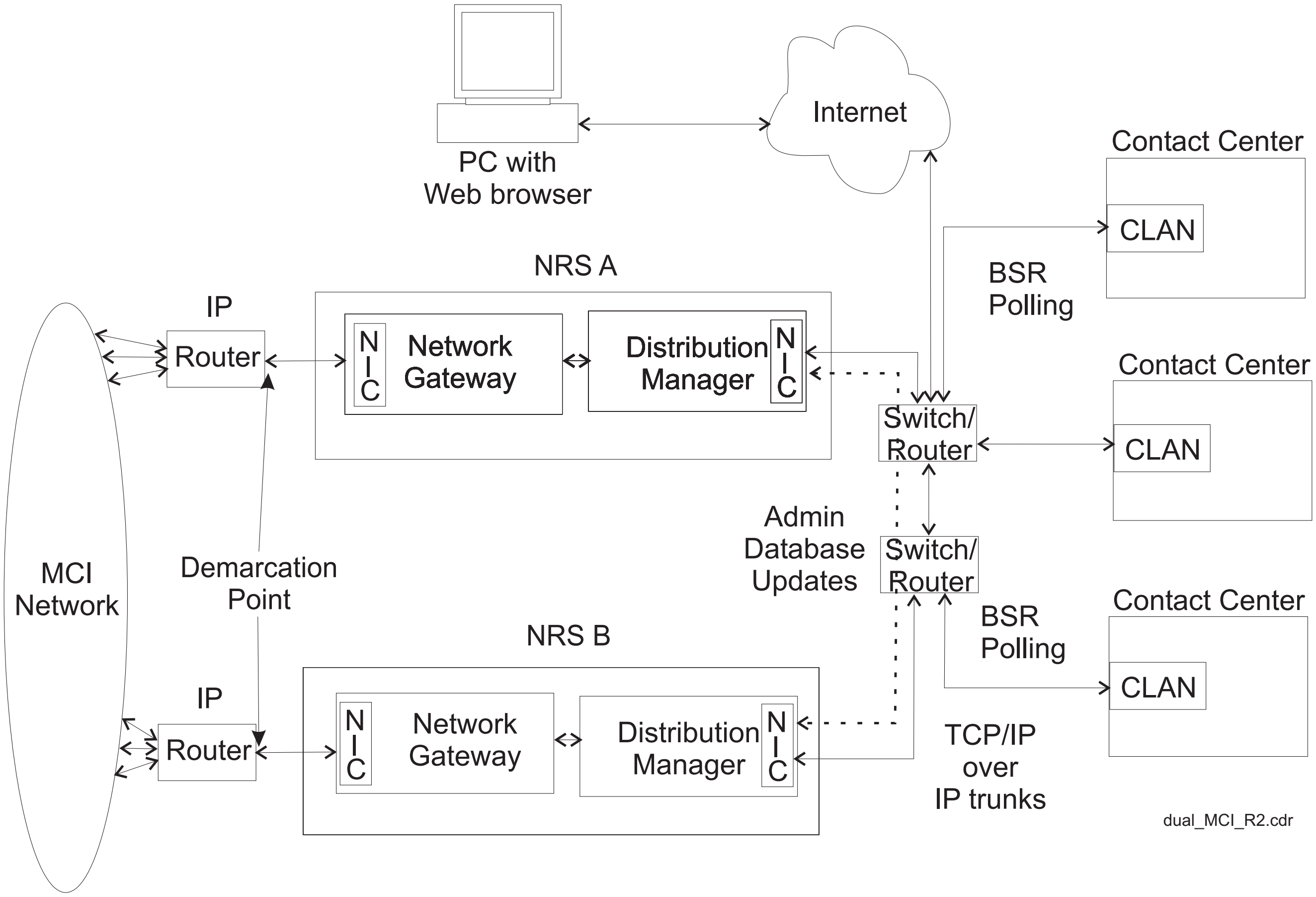
Sample configuration for AT&T

The following figure shows connectivity with the AT&T network. The PC shown in the diagram is used to access the NRS for configuring and monitoring the system.



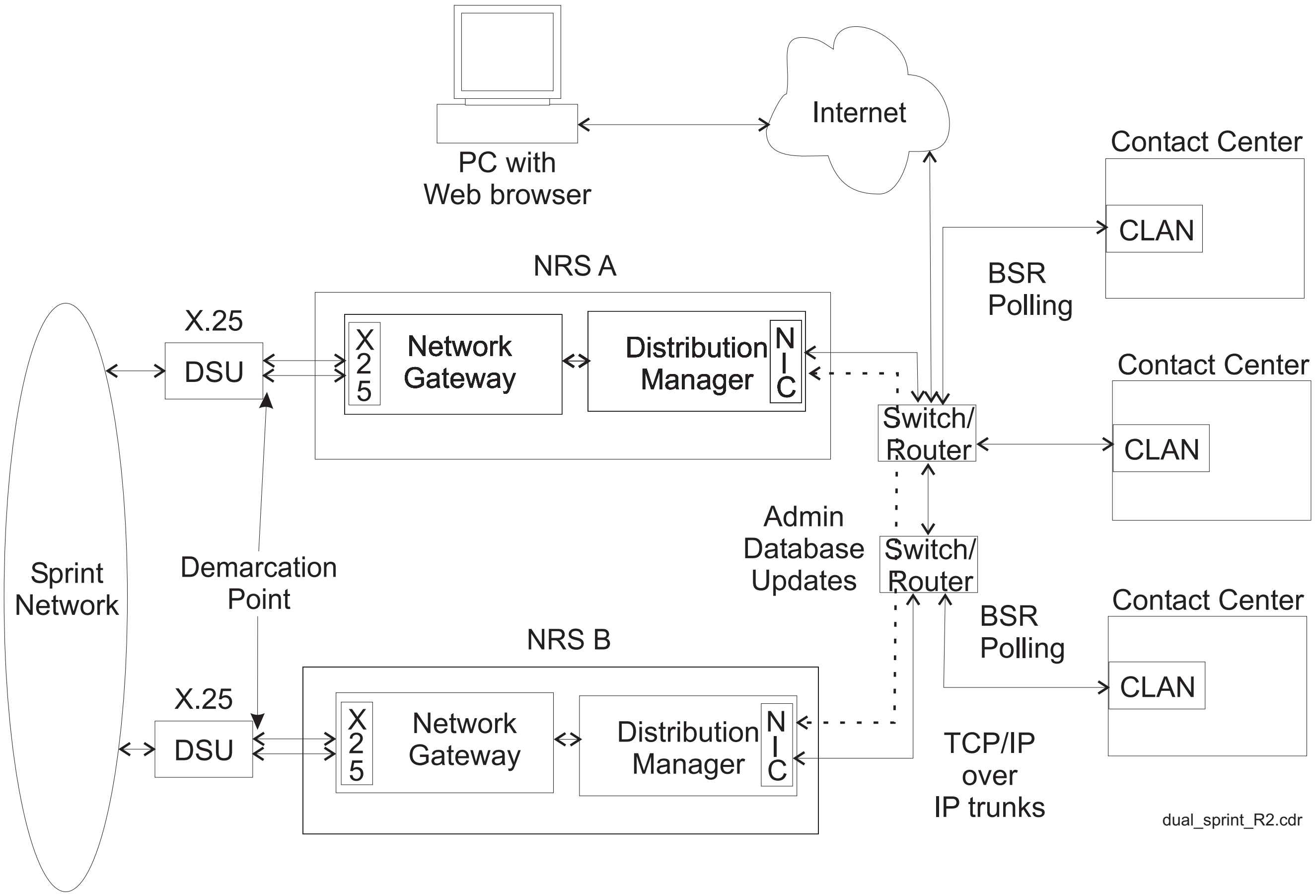
Sample configuration for MCI

The following figure shows connectivity with the MCI network. The PC shown in the diagram is used to access the NRS for configuring and monitoring the system.



Sample configuration for Sprint

The following figure shows connectivity with the Sprint network. The PC shown in the diagram is used to access the NRS for configuring and monitoring the system.



Glossary

API
Application Programming Interface

Automatic Call Distribution (ACD)
A feature of Avaya communication servers that delivers incoming calls to agents based on administered distribution methods.

Best Service Routing (BSR)
A feature on Avaya communication servers that uses Call Vectoring to route ACD calls to the split, skill, or call center best able to service each call. BSR is used to integrate call center resources across a network of communication servers. Network Routing uses the capabilities of BSR to extend best call routing.

CAP
Customer Access Point

CC
Contact Center. This is an overarching term that represents the communication server equipment used in a customer’s Network Routing configuration. The communication servers in a Network Routing configuration report polling status to the NRS.

communication server
A communication server is a switch in the Network Routing configuration that is polled by the NRS.

Distribution Manager
The Distribution Manager is a Web-based application that stores configuration and performance data to determine the best site available to route a call. It responds to call routing requests from the carrier network through the Network Gateway.

Failsafe routing
Default call routing. Failsafe routing schemes are used by both the IXC network routing database and by the Distribution Manager polling channel database.

ICP
Intelligent Call Processing

An advanced toll-free service application that supports cooperative call processing features between the AT&T network and a customer premises database (such as the Distribution Manager call routing database).

INAP
Interface for Network Application Programming

IXC
Inter-exchange Carrier

NCP
Network Control Point

A database in the AT&T network that normally controls call routing, but is suspended to use Network Routing.

Network application
Groups of VDNs (toll-free numbers) to which calls are distributed.

Network Gateway
The Network Gateway interfaces between the IXC and the Distribution Manager with an XML API to help determine the best available destination to route a call.

Polling group
Splits or skills monitored on each CC.

PSTN
Public Switched Telephone Network

RDG
Remote Data Gateway

A database in the MCI network that normally controls call routing, but is suspended to use Network Routing.

RP
Routing Processor

The RP is the customer premise interface to the Sprint EnhanCED SiteRP service. This provides the interface to the Sprint SCPs and the customer specific routing information. The Sprint RP for Avaya is our Sprint EnhanCED SiteRP Network Gateway.

RTN
Routing Telephone Number

SCP
Service Control Point

An enhanced toll free service that supports cooperative call processing features between the Sprint network and customer Routing Processors (RPs), such as the Sprint EnhanCED SiteRP Network Gateway.

Signaling System Seven (SS7)
A standard call control protocol used by IXC service providers.

XML
Extensible Markup Language

Index