

Vocera IP Port Reference Guide

Notice

Stryker Corporation or its divisions or other corporate affiliated entities own, use or have applied for the following trademarks or service marks: Stryker, Vocera. All other trademarks are trademarks of their respective owners or holders. The absence of a product or service name or logo from this list does not constitute a waiver of Stryker's trademark or other intellectual property rights concerning that name or logo. Copyright © 2025 Stryker.

Last modified: 2025-02-21 11:24

ED-IPP-Production-Docs build 21

Contents

- Introduction to the Vocera IP Port Reference Guide.....4
- About This Vocera IP Port Reference Guide..... 4
- Intended Audience for the Vocera IP Port Reference Guide..... 4
- Vocera Analytics IP Ports..... 5
- Vocera Edge IP Ports.....6
- Vocera Engage 5.x IP Ports.....10
- Vocera Engage 7.x IP Ports.....14
- Vocera Engage 7.x External IP Ports..... 14
- Vocera Engage 7.x Internal IP Ports..... 17
- Vocera Messaging Platform IP Ports..... 22
- Vocera Platform IP Ports.....25
- Vocera Platform External IP Ports..... 25
- Vocera Platform Internal IP Ports.....28
- Vocera Voice Server IP Ports.....37
- Glossary..... 44

Introduction to the Vocera IP Port Reference Guide

The section summarizes the information covered in the Vocera IP Port Reference Guide, the intended audience, and the related documentation that you can refer to.

About This Vocera IP Port Reference Guide

The primary communication platforms provided by Vocera require you to open specific IP ports to allow each server and its clients to communicate with each other.

Table Conventions

The port information in this guide is presented in a table format. Following are the columns with description available in each table. For terms and definitions, see [Glossary](#) on page 44.

Column Name	Column Description
Port	The internal or external port number. It is sorted in an ascending order within each table. For port numbers given in a range, the starting number in the range is used for sorting.
Protocol	The underlying transport protocols used to establish communications are: • TCP • UDP Other protocols include SIP, RTP, REST, STMP, IMAP, POP3, EWS, HTTP/2, GRPC, and MRCPv2.
Source	The local process or application.
Destination	The remote process or application.
Direction	The direction of communication flowing through the port. It includes: • Inbound (traffic coming into the network) • Outbound (traffic going out of the network) • Bidirectional (inbound and outbound)
Notes	Any additional information related to the port, protocol, or the processes involved in the communication.

Intended Audience for the Vocera IP Port Reference Guide

This guide is intended primarily for network administrators.

Vocera Analytics IP Ports

The IP port usage information required for Vocera Analytics is provided in a table format.

Keep the following ports open for effective communications between the source and destination processes.

Vocera Analytics Server Ports

Port	Protocol	Source	Destination	Direction	Notes
3306	TCP	MySQL	Visualization server, Reporting server	Inbound	
4040	TCP	VA Server	Spark	Bidirectional	
7778	TCP	VA Server	VMP Flume agent	Bidirectional	
7779	TCP	VA Server	Engage Flume agent	Bidirectional	
8443	TCP	VA Server	Reporting service	Bidirectional	
9445	TCP	Voice Server	Browser	Inbound	The source is a remote agent.

Vocera Edge IP Ports

The IP port usage information required for Vocera Edge is provided in a table format.

Vocera Edge Servers

The Vocera Edge System servers do not require any outbound access to the Internet and all management, monitoring, and support access is managed over an IP specific site-to-site VPN tunnel.

If the organization wants users to be able to access the Vocera Edge System from outside the hospital network for cases such as BYOD mobile device users and/or Web Messenger, then outbound access can be configured just for those two application use cases. In these cases, Vocera Edge Solutions recommends the use of Multi-Factor Authentication (MFA). Device Authorization is available solely in the Vocera Edge system; however, integration with an MFA provider such as SecureAuth, ADFS, or Microsoft Azure AD using SAML 2.0 is recommended.

Vocera Edge Mobile Devices Running the Vocera Edge Mobile Application

While not required, Vocera Edge Solutions does recommend that several ports be allowed for outbound access to the internet in order to provide the most robust application experience. The ports that should be opened for outbound internet access allow Vocera Edge Solutions to provide functionality required by Apple Push Notification Services (APNS). The Vocera Edge mobile application uses APNS to provide notifications to devices that may be in a sleep state and to ensure that the mobile application automatically relaunches if the application crashes. The following ports should be open to the Internet to take full advantage of APNS functionality:

- TCP port 5223 to communicate with APNS
- TCP port 443 or 2197 to send notifications to APNS
- TCP port 443 is required during Apple device activation, and afterwards for fallback (on Wi-Fi only) if devices cannot reach APNS on port 5223

In addition, if your facility is using Mobile Device Management (MDM), additional ports may be required to allow the mobile devices access to check into cloud-hosted MDM services. Ports are specific to your MDM vendor.



Note: To activate and configure software scanning functionality, devices must be able to externally access <https://license.intermec.com> on TCP port 443. This access is only necessary during the initial configuration of the device and is not required beyond initial activation.

Ports

Each managed server is configured with an active firewall. Certain ports are required to be open through the VPN tunnel, while others need to be accessible to the client or internal users.

- [Interface Ports](#) on page 7
- [SQL Database Server Ports](#) on page 7
- [Customer/Edge Access Ports](#) on page 7
- [Edge Management Ports \(Customer to Edge\)](#) on page 7

- [Edge Management Ports \(Edge to Customer\)](#) on page 8
- [Cluster Ports](#) on page 8
- [Client Ports \(iOS and Android\)](#) on page 9

Interface Ports

Port	Protocol	Description
8131	GRPC	Voice Server outbound connection to Edge
8877	TCP	Interface Engine
8878	TCP	Interface Engine

SQL Database Server Ports

Access to SQL Database Server VIP from the Edge servers and across VPN.

Port	Protocol	Description
1433	TCP	MSSQL or custom port

Customer/Edge Access Ports

Port	Protocol	Description
137	TCP/UDP	File Sharing
138	TCP/UDP	File Sharing
443	TCP	Apache: Training Server Reset
4443	TCP	NGINX Proxy Pass: Load Balancer setup for BYOD external, if needed (NGINX > Tomcat)
5060	UDP	Voice Server (FreeSwitch): Load Balancer setup for external voice, if needed
5222*	TCP	Messaging: Load Balancer setup for external messaging, if needed (XMPP/Openfire)
7443	TPC	Web Messenger (BOSH): Load Balancer setup for Web Messaging external, if needed (XMPP/Openfire)
8091	TCP	Analytics Jasper (Tomcat)
8443*	TCP	PSS Web Applications: Load Balancer setup for Apps (NGINX > Tomcat)
10443	TCP	Messaging Attachments: Load Balancer setup for external messaging if needed (XMPP/Openfire)
16384–32767	UDP	VoIP RTP Port Range

Load Balancer should be configured to either send pass through traffic to port 8443 or proxy protocol traffic to port 4443.

* For application and messaging access outside of the hospital network, these ports must be accessible.

Edge Management Ports (Customer to Edge)

Accessible from customer servers to Edge across Support VPN.

Port	Protocol	Description
25	TCP	SMTP/Mail
53	TCP/UDP	DNS
80	TCP	Software Updates
123	UDP	NTP
389	TCP/UDP	Active Directory
445	TCP	Active Directory
464	TCP	Active Directory
636	TCP	Active Directory (LDAPS)
3268	TCP	Active Directory

Edge Management Ports (Edge to Customer)

Accessible to customer servers from Edge across Support VPN.

Port	Protocol	Description
22	TCP	SSH
631	TCP/UDP	CUPS Printer Server
2443	TCP	NGINX Admin Page
5601	TCP	Kibana
8090	TCP	Analytics Talend (Tomcat)
9000	TCP	Kafka Manager
9091	TCP	Openfire Admin Console
9300	TCP	Elastic Search
10050	TCP	Zabbix
10051	TCP	Zabbix
44444	TCP	Tomcat debug

Cluster Ports

Accessible between servers in a cluster.

Port	Protocol	Description
22	TCP	SSH
2181	TCP	ZooKeeper
5044	TCP	Logstash
5071	TCP	Hazelcast Clustering
5222*	TCP	Messaging
8200	TCP	Vault IO
8201	TCP	Vault IO Cluster
8443*	TCP	Edge Web Applications
9093	TCP	Kafka

Port	Protocol	Description
30865	TCP	csync2: used to sync printer configuration for CUPS

* For application and messaging access outside of the hospital network, these ports must be accessible.

Client Ports (iOS and Android)

Port	Protocol	Description
5060	UDP	VoIP Communications
5066	SIP	SIP Client Listening
5151	TCP	Unified Messaging and Alerting for Edge Integration with Vocera Voice and Vocera Engage
5222*	TCP	Messaging
8443*	TCP	Edge Web Applications
16384–32767	UDP	VoIP RTP Port Range

* For application and messaging access outside of the hospital network, these ports must be accessible.

Vocera Engage 5.x IP Ports

The IP port usage information required for Vocera Engage 5.x Versions is provided in a table format.

Keep the following ports open for effective communications between the source and destination processes:

- [Engage 5.x Ports](#) on page 10
- [Internal Network Ports](#) on page 11
- [Inbound Engage Middleware Module Ports](#) on page 13

Engage 5.x Ports

Port	Protocol	Source	Destination	Notes
22	TCP	Engage Middleware Module	svc.ext-inc.com	• Remote Support. • The destination IP address is 199.180.201.227
443	TCP	Engage Middleware Module	svc.ext-inc.com	• Provisioning. • APNS certificate retrieval. • The destination IP address is 199.180.201.227
443	TCP	Engage Middleware Module	yum.ext-inc.com	• Repository access for installing Ubuntu and Engage Middleware Module software updates. • The destination IP address is 199.180.201.238
443	TCP	Engage Mobile	Engage Mobile	• Workflow page access for Android and Engage Mobile App, iOS devices using a reverse proxy in a DMZ. • Traffic from any address to Engage Middleware Module on port 443 must be open unless a reverse proxy is used.
443	TCP	Engage Middleware Module (all networks)	Reverse proxy	• Workflow page access for Android and Engage Mobile App, iOS devices using a reverse proxy in a DMZ. • Traffic from any address to the proxy on port 443 must be open. • Using a reverse proxy also has an internal requirement for the proxy to access Engage Middleware Module.

Port	Protocol	Source	Destination	Notes
443	TCP	External browser access (all networks)	Engage Middleware Module	- When workflow page access for browsers outside the network is desired not using a reverse proxy. - Traffic from any address to Engage Middleware Module on port 443 must be open unless a reverse proxy is used.
443	TCP	External browser access (all networks)	Reverse proxy	- When workflow page access for browsers outside the network is desired not using a reverse proxy. - Traffic from any address to Engage Middleware Module on port 443 must be open unless a reverse proxy is used.
2196	TCP	Engage Middleware Module	feedback.push.17.0.0.0/8	- XMPP feature - Retrieve list of failed devices from Apple Push Notification Service (APNS) Outbound, to Apple.
5222	TCP	Engage Mobile iOS	Engage Middleware Module	- XMPP feature - Client to server XMPP traffic use the well known port 5222.
5222	TCP	Engage Mobile iOS	Edge> Engage Middleware Module	- XMPP feature - External XMPP traffic communicates with Engage Middleware Module through the Edge XMPP proxy on port 5222.
5223	TCP	Engage Mobile App, iOS device	.push.apple.17.0.0.0/8	- XMPP feature - Receive push notifications on Engage Mobile App, iOS device. - According to Apple, the iOS device is using Wi-Fi, port 5223 must be open outbound and inbound to the Wi-Fi. - If all devices are using 4G port 5223 is not required.
5269	TCP	Federated XMPP Server	Engage Middleware Module	- XMPP feature - Federated server communication uses port 5269. Federation can be initiated in either direction. - This does not need to be opened externally if only federating with servers on the internal network.
5269	TCP	Engage Middleware Module	Federated XMPP Server	- XMPP feature - Federated server communication uses port 5269. Federation can be initiated in either direction. - This does not need to be opened externally if only federating with servers on the internal network.

Internal Network Ports

Port	Protocol	Source	Destination	Notes
22	TCP	Any SSH client	Engage Middleware Module	SSH access.

Port	Protocol	Source	Destination	Notes
25	TCP	SMTP Client	Engage Middleware Module	- Incoming e-mail feature - Inbound SMTP messages for the incoming e-mail interface.
25	TCP	Engage Middleware Module	SMTP	- Outgoing e-mail feature - Outbound SMTP messages from the outgoing e-mail interface.
80	TCP	Any HTTP client	Engage Middleware Module	Admin Console and workflow access through HTTP.
80	TCP	Cisco or SpectraLink Phones	Engage Middleware Module	Workflow access from mobile devices.
161	UDP	SNMP Client	Engage Middleware Module	- SNMP feature. - Query Engage Middleware Module for SNMP parameters.
161	UDP	Engage Middleware Module	SNMP Manager	- SNMP feature. - Send SNMP traps for audit events.
389	TCP	Engage Middleware Module	LDAP Server	- LDAP feature. - LDAP default configuration for Active Directory.
443	TCP	Reverse proxy	Engage Middleware Module	Reverse proxy access to Engage Middleware Module when a proxy is used in a DMZ for external smart phone or external browsers.
443	TCP	Any HTTP client	Engage Middleware Module	Admin Console and workflow access through HTTPS.
1322	TCP	Engage Middleware Module	Unite Connectivity Manager (UCM)	- Ascom feature. - Push interactive messages to Ascom devices.
2000	UDP	Carescape Network	Engage Middleware Module	Carescape Time synchronization.
2021	TCP	Engage Middleware Module	DigiBox	- TAP / Serial Devices. - Default non-secure DigiBox port.
6661	TCP	HL7 (LLP)	Engage Middleware Module	- Inbound HL7 messages. - This is the default port configured in Mirth. This might be changed or additional connections added. - Any additional connections require opening the ports.
7000	UDP	Carescape Network	Engage Middleware Module	- Carescape feature. - Device discovery. - Alarm Messages.

Port	Protocol	Source	Destination	Notes
8443	TCP	Mirth Client	Engage Middleware Module	Mirth administration once client is downloaded.
8888	TCP	Any HTTP client	Engage Middleware Module	HTTP access to Mirth client download and login.
12000	TCP	Navicare Server	Engage Middleware Module	- Navicare feature. - Inbound Hill-Rom Navicare messages.
27015	TCP	Engage Middleware Module	Vocera Server	- Vocera feature. - Communicate with Vocera server.
5000-5004	TCP	UCM	Engage Middleware Module	- Ascom feature. - UCM responses to message delivery.

Inbound Engage Middleware Module Ports

Port	Protocol	Notes
22	TCP	SSH access.
80	TCP	HTTP access.
161	TCP	SNMP.
443	TCP	HTTP access.
6661	TCP	Default HL7 port.
8443	TCP	Mirth HTTPS administrative access.
8888	TCP	Mirth HTTP client access.

Vocera Engage 7.x IP Ports

The IP port usage information required for Vocera Engage is provided in a table format.

The table for external and internal port information includes required and optional port information for Vocera Engage and adapters, and integrations with Vocera Voice.

You must access the Vocera Engage Web Console with a Fully Qualified Domain Name (FQDN). Facilities using Transport Layer Security (TLS) should install a trusted certificate with a matching FQDN.

Vocera Engage 7.x External IP Ports

Keep the following ports open for effective communications between the source and destination processes.

Firewall Requirements

The following table describes the firewall requirements which should be configured to successfully install, update, and support Vocera Engage and its operating system.

Port	Protocol	Source	Destination	Notes
22	TCP	Vocera Engage	gw.tools.vocera.com	- Remote Support and Proactive Monitoring - Establish SSH tunnel via port 22 to pass the traffic - The Destination IP addresses are: 34.198.242.61, 54.82.202.24, 52.2.127.189, 54.144.178.22
22	TCP	Vocera Engage	as1.vocera.com	- Outbound communication with the destination server, as1.vocera.com, for sending logs - Destination IP address is 38.108.178.34
443	TCP	Vocera Engage	api.tools.vocera.com	- Remote support - Establish control connection (WebSocket) - Upload and download files (HTTPs) - The destination IP addresses are: 44.195.218.130, 54.90.102.113 and 54.210.212.191
443	TCP	Vocera Engage	box.vocera.com	- Software Update. - Repository access for installing Redhat and Vocera software updates. - The Destination IP address is subject to change. Or for legacy installations, the destination is yum.ext-inc.com and the IP address is 38.99.68.43

Port	Protocol	Source	Destination	Notes
443	TCP	Vocera Engage	portal.tools.v	- Remote Support, Provisioning, and APNS Certificate retrieval - The destination IP addresses are: 75.2.62.171, 99.83.128.202, 75.2.104.130, 99.83.136.195
443/80	TCP	Active Standby	Standby Active	- Node trust feature - Health Checks

Additional Firewall Requirements for Vocera Engage Version 7.0

The following table describes the firewall requirements which should be configured to successfully install, update, and support Vocera Engage 7.0 and its operating system.

Port	Protocol	Source	Destination	Notes
22	TCP	Vocera Engage	svc.ext-inc.com	- Connectivity to svc.ext-inc.com is required for Vocera Engage 7.0 only. For Engage 7.1+, disregard this entry. - Remote Support - Destination IP address is: 54.165.208.197
443	TCP	Vocera Engage	svc.ext-inc.com	- Connectivity to svc.ext-inc.com is required for Vocera Engage 7.0 only. For Engage 7.1+, disregard this entry. - Provisioning (licensing). - APNS certificate retrieval. - The destination IP address is 54.165.208.197

Optional External Ports

The following table lists optional external ports that may be needed depending on the configured software and desired functionality.

Port	Protocol	Source	Destination	Notes
123	UDP	Vocera Engage	NTP Server	Ensure connection to the NTP server of the user's choice to mitigate time synchronization issues that could adversely impact time-sensitive functionality.  Note: The NTP server is listed as an optional external port for implementations where no internal NTP server is available.
443	TCP	Vocera Engage	APNS	- XMPP feature. - The destination is api.push.apple.com. Apple requests that firewalls allow all outbound connections in the subnet range of 17.0.0.0/8. - Send notifications for data and calls through the Apple Push Notification Service (APNS).
443	TCP	Vocera Engage	Google's ASN of 15169	- XMPP feature. - Send notifications for data and calls through Firebase Cloud Messaging (FCM) See Firebase firewall configuration and AS15169 Google LLC.

Port	Protocol	Source	Destination	Notes
443	TCP	External browser access (all networks)	Customer-owned DMZ network appliance Firewall pinhole-Vocera Engage Port forwarder-Vocera Engage	- When workflow page access for browsers outside the network is desired using a customer-owned network appliance in a DMZ, traffic from any address to the proxy on port 443 must be open. - Using a Customer-owned DMZ network appliance is required for external Vocera Vina users. - For more information, see Off-Premise Support for Vocera Vina in the Vocera Platform Administration Guide.
443	TCP	Vocera Engage	www.amion.com	- Amion Adapter feature. - Download Amion schedule updates from the Amion cloud service.
443	TCP	Vocera Engage	api.qgenda.com	- Ogenda Adapter feature. - Download Ogenda schedule updates from the Ogenda cloud service.
443	TCP	Vocera Engage	s3.suki.ai	Enhanced Voice/Suki
5222	TCP	Vina	Customer-owned DMZ network appliance Firewall pinhole-Vocera Engage Port forwarder-Vocera Engage	- XMPP feature. - External XMPP traffic communicates with Vocera Engage through the customer-owned DMZ network appliance. - For more information, see Off-Premise Support for Vocera Vina in the Vocera Platform Administration Guide.
5223	TCP	Vina (iOS only)	APNS	- XMPP feature. - The destination is api.push.apple.com. Apple requests that firewalls allow all outbound connections in the subnet range of 17.0.0.0/8. The APNS servers use load balancing, so your devices do not always connect to the same public IP address for notifications. It is best to let your device access these ports on the entire 17.0.0.0/8 address block assigned to Apple. If you can't allow access to the entire 17.0.0.0/8 address block refer to https://support.apple.com/en-us/HT203609 - The installer can choose a different port when configuring the adapter. - Receive push notifications on iOS device. According to Apple, the iOS device is using Wi-Fi, port 5223 must be open outbound to the Wi-Fi.
5228, 5229, 5230	TCP	Vina (Android only)	Firebase, Google's ASN of 15169	- XMPP feature. - Receive push notifications on Android device. See Firebase firewall configuration and AS15169 Google LLC.

Vocera Engage 7.x Internal IP Ports

We recommend that you keep the following ports open to ensure effective communication between the source and destination.

- [Clustering Ports](#) on page 17
- [Adapter Ports](#) on page 18
- [Vocera Analytics Ports](#) on page 20

It is assumed that the following sources or destinations are on the internal network. If a listed item has a source or destination outside the internal network, then it must also be opened in the external firewall.

Engage Ports

Port	Protocol	Source	Destination	Notes
11102	TCP	Artemis Jolokia	Artemis Jolokia	This port establishes connections within the cluster (both private IPs and the VIP) and the ephemeral port range. It is not part of Artemis clustering but used to monitor the health of message queues and has other management capabilities. It is also used for sending audit events from certain components/scripts without using GlassFish.
22	TCP	Any SSH client	Vocera Engage	• SSH access. • Command line administration.
25	TCP	Vocera Engage	SMTP Server	• SMTP feature. • Send SMTP messages for audit events.
80	TCP	Cisco or SpectraLink Phones	Vocera Engage	• Workflow access from mobile devices.
123	UDP	Vocera Engage	NTP Server	Ensure connection to the NTP server of the user's choice to mitigate time synchronization issues that could adversely impact time-sensitive functionality.
139	UDP	Vocera Engage	Client shared drive	Supports automatic transfer of the system backup files to another location for storage using Server Message Block (SMB) protocol .
161	UDP	SNMP Client	Vocera Engage	• SNMP feature. • Query Vocera Engage for SNMP parameters.
161	UDP	Vocera Engage	SNMP Manager	• SNMP feature. • Send SNMP traps for audit events.
443	TCP	Any HTTPS client	Vocera Engage	• Vocera Engage Web Console and workflow access through HTTPS.
445	UDP	Vocera Engage	Client shared drive	Supports newer version of SMB protocol.

Clustering Ports

IP packets of type 112 must be allowed for VRRP (Virtual Router Redundancy Protocol).

Port	Protocol	Source	Destination	Notes
1099	JMX/RMI	Active	Standby	Used for monitoring the health of the Artemis queues when Artemis is active on the standby node in Vocera Engage 7.1.0 and above.
1100	JMX/RMI	Active	Standby	Used for monitoring the health of the Artemis queues when Artemis is active on the standby node in Vocera Engage 7.1.0 and above.
22	TCP	Active	Standby	• Rsync over SSH. • Filesystem replication.
5432	TCP	Standby	Active	• Postgres feature. • Database replication.
5433	TCP	Standby	Active	• Postgres feature. • Database replication.
61616	TCP	Active Standby	Standby Active	• Apache Artemis feature. • JMS broker clustering.
61617	TCP	Active Standby	Standby Active	• Apache Artemis feature. • JMS broker replication.

Adapter Ports

The following port usage depends on the configured integrations.

Port	Protocol	Source	Destination	Notes
25	TCP	SMTP Client	Vocera Engage	• Email (incoming) feature. • These are the default values. The installer can choose a different port when configuring the adapter. • Inbound SMTP messages for the Incoming Email interface
25	TCP	Vocera Engage	SMTP Server	• Email (outgoing) feature. • These are the default values. The installer can choose a different port when configuring the adapter. • Outbound SMTP messages from the Outgoing Email interface.
80	TCP	Multiple inbound integrations	Vocera Engage	• Available for inbound adapter integration \ support for HTTP when HTTPS is not supported.
80	TCP	Vocera Engage	Multiple outbound integrations	• Available for outbound adapter integration \ support for HTTP when HTTPS is not supported.
80	TCP	Cisco or SpectraLink Phones	Vocera Engage	• Workflow access from mobile devices.
389	TCP	Vocera Engage	LDAP Server	• LDAP feature. • Authentication and user synchronization through LDAP.

Port	Protocol	Source	Destination	Notes
443	TCP	Multiple inbound integrations	Vocera Engage	Inbound adapter integrations that support HTTPS. For example, ResponderSync, Hill-Rom Clinical API, SOAP Publisher.
443	TCP	Vocera Engage	Multiple outbound integrations	Outbound adapter integrations that support HTTPS. For example, ResponderSync, Hill-Rom Clinical API, SOAP Publisher.
443	TCP	Any HTTPS client	Vocera Engage	Vocera Engage Web Console and workflow access through HTTPS.
636	TCP	Vocera Engage	LDAP Server	- LDAP feature. - Authentication and user synchronization through LDAP over SSL.
1322	TCP	Vocera Engage	Unite Connectivity Manager (UCM)	- Ascom Unite Connectivity Manager (UCM) feature. - Push interactive messages to Ascom devices.
2000	UDP	Carescape Network	Vocera Engage	- Carescape feature. - These are the default port values. The installer can choose a different port when configuring the adapter. - Time synchronization.
5000-5004	TCP	UCM	Vocera Engage	- Ascom feature. - These are the default port values. The installer can choose a different port when configuring the adapter. - UCM responses to message delivery.
5005	TCP	VMI Client	Vocera Engage	- Vocera Messaging Interface (VMI) feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Inbound VMI integrations.
5005/5251	TCP	Vocera Adapter	Voice Server	The Vocera Adapter is also referred to as Outgoing VMI.
5007	TCP	VMI Client	Vocera Engage	- Vocera Messaging Interface (VMI) feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Inbound VMI integrations using TLS.
5050	TCP	EarlySense Gateway	Vocera Engage	These are the default values. The installer can choose a different port when configuring the adapter.
5222	TCP	Vina	Vocera Engage	- XMPP feature. - Client to server XMPP traffic for all data, messaging, presence.
5251	TCP	VAI Data	Vocera Engage	- Voice Group Sync feature. - Communication of Vocera Administration Interface (VAI) data; used for polls, and to import Groups and Users.
6661-6664	TCP	HL7	Vocera Engage	HL7 (ADT) feature.

Port	Protocol	Source	Destination	Notes
				- These are the default values. The installer can choose a different port or add more ports when configuring the adapter. - Inbound HL7 ADT messages through LLP.
7000,8000-8010	TCP	HL7	Vocera Engage	- HL7 (Alarms) feature. - These are the default values. The installer can choose a different port or add more ports when configuring the adapter. - Inbound HL7 Philips, Capsule or IHE compliant Alarm messages through LLP.
7001	UDP	Carescape Network	Vocera Engage	- Carescape feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Monitor Alarm Messages.
8131	gRPC	Vocera Engage	Vocera Edge	- PresenceSync feature. - Required for Engage 7.1+. - This port is used to keep the Presence between Engage and Edge in sync.
9443	HTTPS	Vocera Engage	Vocera Engage	- Austco feature. - Request to register a subscription.
9443	WSS	Vocera Engage	Austco	- Austco feature. - Persistent connection to receive Austco alerts.
12000	TCP	Navicare Server	Vocera Engage	- Navicare feature. - Inbound Hill-Rom Navicare messages.
70001	UDP	Carescape Network	Vocera Engage	- Carescape feature. - Device discovery.

Vocera Analytics Ports

Port	Protocol	Source	Destination	Direction	Notes
3306	TCP	Vocera Platform Cluster Nodes	(Listening) Maria DB	Inbound	Vocera Platform Adapter Connects to Maria DB
4040	TCP	VA Server	Spark UI	Inbound	
7778	TCP	VA Server (VMP Flume agent)	Spark	Bidirectional	
7779	TCP	VA Server (Engage Flume agent)	Spark	Bidirectional	
7780	TCP	Voice Server (VS Flume Agent)	Spark	Bidirectional	
8443	TCP	VA Server (Reporting service)	Reporting service	Inbound	This is a default or user-defined port.

Port	Protocol	Source	Destination	Direction	Notes
9445	TCP	Voice Server (Remote Agent)	Browser	Inbound	

Vocera Messaging Platform IP Ports

The IP port usage information required for Vocera Messaging Platform is provided in a table format.

Keep the following ports open for effective communications between the source and destination processes.

- [VMP Server Ports](#) on page 22
- [Apple iOS Device Messaging Ports](#) on page 22
- [Firebase Cloud Messaging \(FCM\) Ports For Android Devices](#) on page 23
- [MS Graph Ports](#) on page 23
- [Simple Network Paging Protocol \(SNPP\) Gateways Using The Default Ports](#) on page 23
- [Wireless Communications Transfer Protocol \(WCTP\) Gateways Using Default Ports](#) on page 23
- [Vocera Secure Texting Ports](#) on page 23
- [Engage Server Using Default Ports](#) on page 23
- [Email Ports](#) on page 23
- [Vocera Collaboration Suite \(On-premises\) Ports](#) on page 24
- [Vocera Collaboration Suite \(Off-premises\) Ports](#) on page 24

VMP Server Ports

Port	Protocol	Source	Destination	Direction	Notes
80, 443	TCP	VMP Web Console Users' computers	VMP Server	Outbound	• SSL ports.
389, 636	TCP	VMP Server	Microsoft AD Server	Outbound	• SSL ports.
1433	TCP	VMP Server	Microsoft SQL Server	Outbound	
5008	TCP	VMP Server	VCG Server	Bidirectional	• For versions of VMP earlier than version 5.5, the Use VCG for VCS client connection management option must be set in the VMP Administrator.

Apple iOS Device Messaging Ports

Port	Protocol	Source	Destination	Direction	Notes
443	HTTP/2	VMP Server	APNS	Outbound	• The Apple Push Notification Service (APNS) destination is <code>api.push.apple.com</code>

Port	Protocol	Source	Destination	Direction	Notes
5223	TCP	Apple iOS devices using Wi-Fi connection	APNS	Outbound	- Apple iOS devices can use port 443 as a fallback if this port is not working. - The Apple Push Notification Service (APNS) destination is <code>gateway.push.apple.com</code>

Firestore Cloud Messaging (FCM) Ports For Android Devices

Port	Protocol	Source	Destination	Direction	Notes
443	TCP	VMP Server	FCM	Outbound	The Firestore Cloud Messaging (FCM) destination is <code>fcm.googleapis.com</code>.
5228-5230	TCP	Android devices using Wi-Fi connection	FCM	Outbound	- Your firewall must accept outgoing connections to all IP addresses contained in the IP blocks listed in Google's ASN of 15169. - Android devices running version 4.3 or later can use port 443 as a fallback if the other three ports are not working.

MS Graph Ports

Port	Protocol	Source	Destination	Direction	Notes
443	TCP	VMP Server	MS Graph	Outbound	The MS Graph URL is <code>https://graph.microsoft.com/</code>.

Simple Network Paging Protocol (SNPP) Gateways Using The Default Ports

Port	Protocol	Source	Destination	Direction	Notes
444	TCP	VMP Server	SNPP Gateway	Outbound	

Wireless Communications Transfer Protocol (WCTP) Gateways Using Default Ports

Port	Protocol	Source	Destination	Direction	Notes
80, 443	TCP	VMP Server	WCTP Gateway	Bidirectional	

Vocera Secure Texting Ports

Port	Protocol	Source	Destination	Direction	Notes
443	TCP	VMP Server	VST Server	Bidirectional	

Engage Server Using Default Ports

Port	Protocol	Source	Destination	Direction	Notes
80, 443	REST	VMP Server	Engage server	Outbound	

Email Ports

Port	Protocol	Source	Destination	Direction	Notes
25, 465	SMTP	VMP Server	SMTP	Bidirectional	This port is for secure SMTP.
80, 443	EWS	VMP Server	EWS	Bidirectional	This port is for secure Exchange Web Services (EWS).

Port	Protocol	Source	Destination	Direction	Notes
110	POP3	VMP Server	POP3	Bidirectional	
143, 993	IMAP	VMP Server	IMAP	Bidirectional	This port is for secure IMAP.

Vocera Collaboration Suite (On-premises) Ports

Port	Protocol	Source	Destination	Direction	Notes
80, 443	TCP	VCS	Vocera Voice Server Ping/Comet connection	Bidirectional	- In versions of VMP earlier than version 5.5, this is used if the Use VCG for VCS client connection management and Enable Enhanced Voice Server NIO Tomcat Feature option are not set in the VMP Administrator. - In version 5.5 and later of VMP, this is not used.
443	TCP	VCS	VMP	Bidirectional	
5060	TCP (see Notes)	VCS	VCG	Bidirectional	- SIP ports. - Type: Signaling. - For versions of VMP earlier than version 5.5, the protocol is UDP if the Use VCG for VCS client connection management option is not set. - For VMP version 5.5 and later, the protocol is UDP if: - You are using Vocera Voice Server 5.5 or later, and - You are using VCS 3.8 or later on a device running Apple iOS 13.3 or later or any Android operating system.
5888-5889	UDP	VCS	VCG	Bidirectional	- VOMO ports. - Type: Signaling.
7700-8467	UDP	VCS	VCG	Bidirectional	- iPhone ports. - Type: Audio.
7700-8467, 32768-65536	UDP	VCS	VCG	Bidirectional	- Android ports. - Type: Audio.
8080	TCP	VCS	Vocera Voice Server Ping/Comet connection	Bidirectional	- In versions of VMP earlier than version 5.5, this is used if the Enable Enhanced Voice Server NIO Tomcat Feature option is set in the VMP Administrator and if the Use VCG for VCS client connection management option is not set in the VMP Administrator. - In version 5.5 and later of VMP, this is not used.

Vocera Collaboration Suite (Off-premises) Ports

Port	Protocol	Source	Destination	Direction	Notes
443	TCP	VCS	VMP	Bidirectional	

Vocera Platform IP Ports

The IP port usage information required for Vocera Platform is provided in a table format.

The table for external and internal port information includes required and optional port information for Vocera Platform, Adapters, Voice Service, Vocera SIP Telephony Gateway, Vocera Badges, and Vocera Vina.

You must access the Vocera Platform Web Console with a Fully Qualified Domain Name (FQDN). Facilities using Transport Layer Security (TLS) should install a trusted certificate with a matching FQDN.

Vocera Platform External IP Ports

Keep the following ports open for effective communications between the source and destination processes.

- [Firewall Requirements](#) on page 25
- [Optional External Ports](#) on page 26

Firewall Requirements

The following table describes the firewall requirements which should be configured to successfully install, update, and support the Vocera Platform and its operating system.

Port	Protocol	Source	Destination	Notes
22	TCP	Vocera Platform	gw.tools.vocera.com	• Remote Support and Proactive Monitoring • Establish SSH tunnel via port 22 to pass the traffic • The Destination IP addresses are: 34.198.242.61, 54.82.202.24, 52.2.127.189, 54.144.178.22
22	TCP	Vocera Platform	svc.ext-inc.com	• Remote Support • Destination IP address is: 54.165.208.197 • Connectivity to svc.ext-inc.com is required for Vocera Platform 6.6.0 and under. For Platform 6.6.1 and above, disregard this entry.
22	TCP	Vocera Platform	asl.vocera.com	• Outbound communication with the destination server, asl.vocera.com, for sending logs • Destination IP address is 38.108.178.34
443	TCP	Vocera Platform	api.tools.vocera.com	• Remote support • Establish control connection (WebSocket) • Upload and download files (HTTPs) • The destination IP addresses are: 44.195.218.130, 54.90.102.113 and 54.210.212.191

Port	Protocol	Source	Destination	Notes
443	TCP	Vocera Platform	svc.ext-inc.com	- Provisioning (licensing). - APNS certificate retrieval. - The destination IP address is 54.165.208.197 - Connectivity to svc.ext-inc.com is required for Vocera Platform 6.6.0 and under. For Platform 6.6.1 and above, disregard this entry.
443	TCP	Vocera Platform	box.voceracomr	- Software Update. - Repository access for installing Red Hat and Vocera software updates. - The Destination IP address is subject to change. Or for legacy installations, the destination is yum.ext-inc.com and the IP address is 38.99.68.43
443	TCP	Vocera Platform	portal.tools.v	- Remote Support, Provisioning, and APNS Certificate retrieval - The destination IP addresses are: 75.2.62.171, 99.83.128.202, 75.2.104.130, 99.83.136.195
443/80	TCP	Active Standby	Standby Active	- Node trust feature - Health Checks

Optional External Ports

The following table lists optional external ports that may be needed depending on the configured software and desired functionality.

Port	Protocol	Source	Destination	Notes
123	UDP	Vocera Platform	NTP Server	Ensure connection to the NTP server of the user's choice to mitigate time synchronization issues that could adversely impact time-sensitive functionality.  Note: The NTP server is listed as an optional external port for implementations where no internal NTP server is available.
443	TCP	Vocera Platform	APNS	- XMPP feature. - The destination is <code>api.push.apple.com</code>. Apple requests that firewalls allow all outbound connections in the subnet range of 17.0.0.0/8. - Send notifications for data and calls through the Apple Push Notification Service (APNS).
443	TCP	Vocera Platform	Google's ASN of 15169	- XMPP feature. - Send notifications for data and calls through Firebase Cloud Messaging (FCM) See Firebase firewall configuration and AS15169 Google LLC.

Port	Protocol	Source	Destination	Notes
443	TCP	External browser access (all networks)	Customer-owned DMZ network appliance Firewall pinhole-Vocera Platform Port forwarder-Vocera Platform	- When workflow page access for browsers outside the network is desired using a customer-owned network appliance in a DMZ, traffic from any address to the proxy on port 443 must be open. - Customer-owned DMZ network appliance is required for external Vocera Vina users - For more information, see Off-Premise Support for Vocera Vina in the Vocera Platform Administration Guide.
443	TCP	Vocera Platform	www.amion.com	- Amion Adapter feature. - Download Amion schedule updates from the Amion cloud service.
443	TCP	Vocera Platform	api.qgenda.com	- Qgenda Adapter feature. - Download Qgenda schedule updates from the Qgenda cloud service.
443	TCP	Vocera Platform	s3.suki.ai	Enhanced Voice/Suki
5222	TCP	Vina	Customer-owned DMZ network appliance Firewall pinhole-Vocera Platform Port forwarder-Vocera Platform	- XMPP feature. - External XMPP traffic communicates with Vocera Platform through the customer-owned DMZ network appliance . - For more information, see Off-Premise Support for Vocera Vina in the Vocera Platform Administration Guide.
5223	TCP	Vina (iOS only)	APNS	- XMPP feature. - The destination is api.push.apple.com. Apple requests that firewalls allow all outbound connections in the subnet range of 17.0.0.0/8. The APNS servers use load balancing, so your devices do not always connect to the same public IP address for notifications. It is best to let your device access these ports on the entire 17.0.0.0/8 address block assigned to Apple. If you can't allow access to the entire 17.0.0.0/8 address block refer to https://support.apple.com/en-us/HT203609 - The installer can choose a different port when configuring the adapter. - Receive push notifications on iOS device. According to Apple, the iOS device is using Wi-Fi, port 5223 must be open outbound to the Wi-Fi.
5228, 5229, 5230	TCP	Vina (Android only)	Firebase, Google's ASN of 15169	- XMPP feature. - Receive push notifications on Android device. See Firebase firewall configuration and AS15169 Google LLC.

Vocera Platform Internal IP Ports

We recommend that you keep the following ports open to ensure effective communication between the source and destination.

- [Platform Ports](#) on page 28
- [Clustering Ports](#) on page 29
- [Adapter Ports](#) on page 29
- [Voice Service Ports](#) on page 32
- [SIP Telephony Gateway Ports](#) on page 33
- [Badge Ports](#) on page 34
- [Smartbadge Ports](#) on page 34
- [Vina Ports](#) on page 35
- [Vocera Analytics Ports](#) on page 35
- [Enhanced Voice](#) on page 35

It is assumed that the following sources or destinations are on the internal network. If a listed item has a source or destination outside the internal network, then it must also be opened in the external firewall.



Important: By default, the signaling gateway ports are dynamically assigned to allow clients to connect. If your organization's firewall set up blocks clients to connect with the signaling gateway's randomly selected ports, you can specify a value for signaling gateway ports (TCP and UDP) in the `interface.properties.user` file. Contact Vocera Technical Support to implement any customizations to the `interface.properties.user` file.

Platform Ports

Port	Protocol	Source	Destination	Notes
11102	TCP	Artemis Jolokia	Artemis Jolokia	This port establishes connections within the cluster (both private IPs and the VIP) and the ephemeral port range. It is not part of Artemis clustering but used to monitor the health of message queues and has other management capabilities. It is also used for sending audit events from certain components/scripts without using GlassFish.
22	TCP	Any SSH client	Vocera Platform	• SSH access. • Command line administration.
25	TCP	Vocera Platform	SMTP Server	• SMTP feature. • Send SMTP messages for audit events.
80	TCP	Cisco or SpectraLink Phones	Vocera Platform	• Workflow access from mobile devices.
123	UDP	Vocera Platform	NTP Server	Ensure connection to the NTP server of the user's choice to mitigate time synchronization issues that could adversely impact time-sensitive functionality.
139	UDP	Vocera Platform	Client shared drive	Supports automatic transfer of the system backup files to another location for storage using Server Message Block (SMB) protocol .
161	UDP	SNMP Client	Vocera Platform	• SNMP feature. • Query Vocera Platform for SNMP parameters.

Port	Protocol	Source	Destination	Notes
161	UDP	Vocera Platform	SNMP Manager	- SNMP feature. - Send SNMP traps for audit events.
443	TCP	Any HTTPS client	Vocera Platform	Web Console and workflow access through HTTPS.
445	UDP	Vocera Platform	Client shared drive	Supports newer version of SMB protocol.
4848	TCP	Glassfish Administration	Vocera Platform	Glassfish service uses this port to connect to the client instance.

Clustering Ports

IP packets of type 112 must be allowed for VRRP (Virtual Router Redundancy Protocol).

Port	Protocol	Source	Destination	Notes
1099	JMX/RMI	Active	Standby	Used for monitoring the health of the Artemis queues when Artemis is active on the standby node in Vocera Platform 6.6.1 and above.
1100	JMX/RMI	Active	Standby	Used for monitoring the health of the Artemis queues when Artemis is active on the standby node in Vocera Platform 6.6.1 and above.
22	TCP	Active	Standby	- Rsync over SSH. - Filesystem replication.
5432	TCP	Standby	Active	- Postgres feature. - Database replication.
5433	TCP	Standby	Active	- Postgres feature. - Database replication.
61616	TCP	Active Standby	Standby Active	- Apache Artemis feature. - JMS broker clustering.
61617	TCP	Active Standby	Standby Active	- Apache Artemis feature. - JMS broker replication.

Adapter Ports

The following port usage depends on the configured integrations.

Port	Protocol	Source	Destination	Notes
25	TCP	SMTP Client	Vocera Platform	- Email (incoming) feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Inbound SMTP messages for the Incoming Email interface
25	TCP	Vocera Platform	SMTP Server	- Email (outgoing) feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Outbound SMTP messages from the Outgoing Email interface.

Port	Protocol	Source	Destination	Notes
80	TCP	Multiple inbound integrations	Vocera Platform	Available for inbound adapter integration \ support for HTTP when HTTPS is not supported.
80	TCP	Vocera Platform	Multiple outbound integrations	Available for outbound adapter integration \ support for HTTP when HTTPS is not supported.
80	TCP	Cisco or SpectraLink Phones	Vocera Platform	Workflow access from mobile devices.
389	TCP	Vocera Platform	LDAP Server	- LDAP feature. - Authentication and user synchronization through LDAP.
443	TCP	Multiple inbound integrations	Vocera Platform	Inbound adapter integrations that support HTTPS. For example, ResponderSync, Hill-Rom Clinical API, SOAP Publisher.
443	TCP	Vocera Platform	Multiple outbound integrations	Outbound adapter integrations that support HTTPS. For example, ResponderSync, Hill-Rom Clinical API, SOAP Publisher.
443	TCP	Any HTTPS client	Vocera Platform	Web Console and workflow access through HTTPS.
636	TCP	Vocera Platform	LDAP Server	- LDAP feature. - Authentication and user synchronization through LDAP over SSL.
1322	TCP	Vocera Platform	Unite Connectivity Manager (UCM)	- Ascom Unite Connectivity Manager (UCM) feature. - Push interactive messages to Ascom devices.
2000	UDP	Carescape Network	Vocera Platform	- Carescape feature. - These are the default port values. The installer can choose a different port when configuring the adapter. - Time synchronization.
5000-5004	TCP	UCM	Vocera Platform	- Ascom feature. - These are the default port values. The installer can choose a different port when configuring the adapter. - UCM responses to message delivery.
5005	TCP	VMI Client	Vocera Platform	- Vocera Messaging Interface (VMI) feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Inbound VMI integrations.
5007	TCP	VMI Client	Vocera Platform	- Vocera Messaging Interface (VMI) feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Inbound VMI integrations using TLS.

Port	Protocol	Source	Destination	Notes
5050	TCP	EarlySense Gateway	Vocera Platform	These are the default values. The installer can choose a different port when configuring the adapter.
5222	TCP	Vina	Vocera Platform	- XMPP feature. - Client to server XMPP traffic for all data, messaging, presence.
5251	TCP	VAI Data	Vocera Platform	- Voice Group Sync feature. - Communication of Vocera Administration Interface (VAI) data; used for polls, and to import Groups and Users.
6661-6664	TCP	HL7	Vocera Platform	- HL7 (ADT) feature. - These are the default values. The installer can choose a different port or add more ports when configuring the adapter. - Inbound HL7 ADT messages through LLP.
7000,8000-8010	TCP	HL7	Vocera Platform	- HL7 (Alarms) feature. - These are the default values. The installer can choose a different port or add more ports when configuring the adapter. - Inbound HL7 Philips, Capsule or IHE compliant Alarm messages through LLP.
7001	UDP	Carescape Network	Vocera Platform	- Carescape feature. - These are the default values. The installer can choose a different port when configuring the adapter. - Monitor Alarm Messages.
7676	HTTP	OpenMQ	Vocera Platform	Port is used by client connections.
8080	HTTP	Vocera Platform	Vocera Platform	- Used by Tomcat. - Used also for telecom ports.
8443	HTTP	Vocera Platform	Vocera Platform	- Used by Tomcat. - Used for telecom and internet ports.
9443	HTTPS	Vocera Platform	Vocera Platform	- Austco feature. - Request to register a subscription.
9443	WSS	Vocera Platform	Austco	- Austco feature. - Persistent connection to receive Austco alerts.
12000	TCP	Navicare Server	Vocera Platform	- Navicare feature. - Inbound Hill-Rom Navicare messages.
70001	UDP	Carescape Network	Vocera Platform	- Carescape feature. - Device discovery.

Voice Service Ports

Port	Protocol	Source	Destination	Direction	Notes
5001	TCP	Vocera SIP Telephony Gateway	Vocera Server	Outbound	Type: Signaling  Note: The 5001 port is only used when connecting external Windows VSTG to the Vocera Platform nodes.
5002	UDP	Badge	Vocera Server	Bidirectional	Type: Signaling
5062	UDP	Nuance Speech Server	Voice Server	Bidirectional	- Type: Signaling - Not opened on firewall
5200	UDP	Badge	Badge / Voice Server / Vocera SIP Telephony Gateway	Bidirectional	Type: Audio
5400	UDP	Badge/Badge Properties Editor (BPE)	Badge Log Collector	Bidirectional	Type: Signaling
5500	UDP	Smartbadge	Vocera Server	Outbound	- Type: Secure Signaling - Signaling between the Vocera Server and Vocera Smartbadge using the underlying TLS/SSL protocol.
7200-7263	UDP	Badge	Vocera Server	Inbound	Type: Audio Recording
7892 - 9100	UDP	Vocera Server	Badge/VSTG	Outbound	For Vocera Platform 6.5 and below: - Type: Audio - Only even-numbered ports are used. The range is configurable in the NSSserver.cfg file available at \opt\vocera\nuance\config
7500 - 8220	UDP	Vocera Server	Badge/VSTG	Outbound	For Vocera Platform 6.6 and above: - Type: Audio - Only even-numbered ports are used. The range is configurable in the NSSserver.cfg file available at \opt\vocera\nuance\config
5251	TCP	Vocera Server Cluster	(Listening)	Inbound	Type: Signaling
5555-5556	UDP	Badge	Vconfig	Bidirectional	Type: Vocera Configuration Utility (Vconfig), Signaling during Discovery
5555-5556	TCP	Badge	Vconfig	Bidirectional	Type: Vconfig (Vch) Signaling during Discovery
7023	TCP	Nuance Watcher Telnet Client	(Listening)	Inbound	

Port	Protocol	Source	Destination	Direction	Notes
6666-6669, 7890, 8919	TCP	Nuance Watcher	(Listening)	Inbound	
9919	UDP	Nuance Watcher	(Listening)	Inbound	
27000	TCP	Nuance License Manager	(Listening)	Inbound	
5059, 5058	TCP	Nuance Speech Server	(Listening)	Inbound	This source allows UDP connections.  Important: Do not use a port from the ephemeral range (32768-60999) as an incoming/outgoing adapter port as it can cause a collision/outage.
8200	TCP	Nuance Recognition Server	(Listening)	Inbound	The source is <code>nuance-server.exe</code>.
32768-60999	TCP	Vina (iOS only)	Signaling Gateway	Bidirectional	
32768-60999	UDP	Vina (Android only)	Signaling Gateway	Bidirectional	 Important: Do not use a port from the ephemeral range (32768-60999) as an incoming/outgoing adapter port as it can cause a collision/outage.
32768-60999	UDP/TCP	Nuance Voice Service	Voice Server	Bidirectional	 Important: Do not use a port from the ephemeral range (32768-60999) as an incoming/outgoing adapter port as it can cause a collision/outage.

SIP Telephony Gateway Ports

Port	Protocol	Source	Destination	Direction	Notes
4000-4049, 9200-9399	UDP	IP PBX	Vocera SIP Telephony Gateway	Bidirectional	Type: Audio (RTP/RTCP)
5060	UDP	IP PBX	Vocera SIP Telephony Gateway	Bidirectional	Type: Signaling
5300-5555	UDP	Vocera Platform	Vocera SIP Telephony Gateway Audio	Bidirectional	Only even-numbered ports are used. The range is configurable in the <code>NSSserver.cfg</code> file available at <code>\vocera\nuance\SpeechServer\config</code>
Any free port	UDP	Vocera Platform	Vocera SIP Telephony Gateway	Bidirectional	Type: Signaling

Badge Ports

Port	Protocol	Source	Destination	Direction	Notes
5002	UDP	Badge	Vocera Server	Bidirectional	• Type: Signaling
5200	UDP	Badge	Badge / Voice Server / Vocera SIP Telephony Gateway	Bidirectional	• Type: Audio
5400	UDP	Badge	Badge Log Collector	Outbound	Badge Log Collector service updates firmware build and badge properties.
5555-5556	UDP	Badge	Badge Log Collector	Bidirectional	• Type: Signaling
5555-5556	UDP	Badge	Vconfig	Bidirectional	• Type: Vconfig (Vch) Signaling during Discovery
5555-5556	TCP	Badge	Vconfig	Bidirectional	• Type: Vconfig (Vch) Signaling during Discovery

Smartbadge Ports

Port	Protocol	Source	Destination	Direction	Notes
5002	UDP	Smartbadge	Vocera Server	Bidirectional	• Type: Signaling
5200	UDP	Badge	Badge / Voice Server / Vocera SIP Telephony Gateway	Bidirectional	• Type: Audio
5222	TCP	Smartbadge	Vocera Platform	Bidirectional	• XMPP feature • Client to server XMPP traffic for all data, messaging, presence.
5400	UDP	Smartbadge	Badge Log Collector	Outbound	Badge Log Collector service updates firmware build and badge properties.
5555-5556	UDP	Smartbadge	Badge Log Collector	Bidirectional	• Type: Signaling
5555-5556	UDP	Smartbadge	Vconfig	Bidirectional	• Type: Vconfig (Vch) Signaling during Discovery
5555-5556	TCP	Smartbadge	Vconfig	Bidirectional	• Type: Vconfig (Vch) Signaling during Discovery
32768-60999	UDP	Smartbadge	Vocera Platform	Bidirectional	• Signaling Gateway feature. • Call signaling and notifications.

Vina Ports

Port	Protocol	Source	Destination	Notes
5222	TCP	Vina	Vocera Platform Vocera Edge Firewall pinhole Port forwarding	- XMPP feature - Client to server XMPP traffic for all data, messaging, presence. - Communication with Edge proxy or other customer configured port 5222 access will off-premise.
5800-5899	UDP	Vina	Vina	- RTP feature - Client to client VoIP.
32768-60999	TCP	Vina (iOS only)	Vocera Platform	- Signaling Gateway feature - Call signaling and notifications.
32768-60999	UDP	Vina (Android only)	Vocera Platform	- Signaling Gateway feature. - Call signaling and notifications.

Vocera Analytics Ports

Port	Protocol	Source	Destination	Direction	Notes
3306	TCP	Vocera Platform Cluster Nodes	(Listening) Maria DB	Inbound	Vocera Platform Adapter Connects to Maria DB
4040	TCP	VA Server	Spark UI	Inbound	
7778	TCP	VA Server (VMP Flume agent)	Spark	Bidirectional	
7779	TCP	VA Server (Engage Flume agent)	Spark	Bidirectional	
7780	TCP	Voice Server (VS Flume Agent)	Spark	Bidirectional	
8443	TCP	VA Server (Reporting service)	Reporting service	Inbound	This is a default or user-defined port.
9445	TCP	Voice Server (Remote Agent)	Browser	Inbound	

Enhanced Voice

The following table lists the ports that must be opened for the Enhanced Voice feature.

Port	Protocol	Source	Destination	Direction	Notes
443	TCP / HTTP/2 / GRPC	Voice Service	Cloud Recognition Service	Outbound	
6080	TCP / HTTP	Operational/Monitoring	Automatic Speech Recognition (ASR) Broker	Inbound	
6102-6822	UDP / RTP	Badge	ASR Broker	Bidirectional	For Vocera Platform 6.5 and below: The range includes only even-numbered ports.
8250-8970	UDP / RTP	Badge	ASR Broker	Bidirectional	For Vocera Platform 6.6 and above: The range includes only even-numbered ports.

Vocera Voice Server IP Ports

The IP port usage information required for Vocera Voice Server is provided in a table format.

Keep the following ports open for effective communications between the source and destination processes.

- [Vocera Voice Server Ports](#) on page 37
- [Vocera SIP Telephony Gateway Ports](#) on page 39
- [Vocera Client Gateway Ports](#) on page 40
- [Vocera Report Server Ports](#) on page 40
- [Badge Ports](#) on page 41
- [Vocera Collaboration Suite Ports](#) on page 41
- [WLAN Ports Used by Vocera Clients](#) on page 42
- [Vocera Analytics Ports](#) on page 42
- [Vocera Auto Sending Logs Ports](#) on page 43
- [ASR Broker Ports](#) on page 43



Important: By default, the signaling gateway ports are dynamically assigned to allow clients to connect. If your organization's firewall set up blocks clients from connecting with the signaling gateway's randomly selected ports, you can specify a value for signaling gateway ports (TCP, UDP, and DTLS) in the `application.properties` file. You can find this file in the following directory: `{vocera_drive}/vocera/signalinggateway`. Contact Vocera Technical Support to implement any customizations to the `application.properties` file.

Vocera Voice Server Ports

Port	Protocol	Source	Destination	Direction	Notes
80, 443	TCP	Browser	Apache Signaling	Bidirectional	• Type: Signaling • These are SSL ports.
8443	TCP	Tomcat HTTP Connector	Browser	Inbound	• The server is listening on the port.
3306	TCP	Database	Listening	Inbound	• Type: Signaling • The source is MySQL.
5001	TCP	Vocera SIP Telephony Gateway	Vocera Server	Outbound	• Type: Signaling
5002	UDP	Badge	Vocera Server	Bidirectional	• Type: Signaling
5003	TCP	RSIP	Vocera Server	Bidirectional	• Type: Signaling

Port	Protocol	Source	Destination	Direction	Notes
5005	TCP	Vocera Server	VMI	Bidirectional	- Type: Connection - The source includes VMI clients.
5006	TCP	VCG	Vocera Server	Outbound	Type: Signaling
5007	TCP	Vocera Server	VMI	Bidirectional	The destination includes VMI Clients (TLS).
5060, 5061, 5062	TCP	Nuance Speech Server	Listening	Inbound	- Nuance is on the listening mode. - Voice server sends MRCP requests to these ports.
5060, 5062	TCP	Nuance Speech Server	Listening	Inbound	The source allows UDP connections.
5251	TCP	Vocera Server	VAI Clients	Bidirectional	The source is Vocera Administration Interface.
5251	TCP	Vocera Server	Vocera Report Server	Bidirectional	Type: Signaling
5251	TCP	Vocera Server Cluster	Listening	Inbound	Type: Signaling
5252	TCP/TLS	Badge	Voice Server	Inbound	Secure Badge Log Collector signaling
5253	TCP/TLS	Vocera Server Cluster	Listening	Inbound	Type: Secure Signaling
5254	TCP/TLS	Vocera SIP Telephony Gateway	Vocera Server	Outbound	Type: Secure Signaling
5255	TCP/TLS	Vocera Client Gateway	Vocera Server	Outbound	Type: Secure Signaling
5400	UDP	Badge	Updater	Bidirectional	Type: Signaling
5500	UDP	Smartbadge	Vocera Server	Outbound	For Vocera Voice Server 5.9 and below. - Type: Secure Signaling - Signaling between the Vocera Server and Vocera Smartbadge using the underlying TLS/SSL protocol.
49152-65535	TCP/UDP/DTLS	Smartbadge/Edge Mobile	Vocera Server	Bidirectional	For Vocera Voice Server 5.10. - Secure Call Signaling and Notifications between Vocera Edge, Android Client, and Smartbadge. - Secure DTLS Signaling between the Vocera Server and Vocera Smartbadge. - Signaling between the Vocera Server and Vocera Edge iOS Client.
5555, 5556	TCP / UDP	Badge	Vconfig	Bidirectional	- Type: Vconfig (Vch) - Signaling during Discovery

Port	Protocol	Source	Destination	Direction	Notes
7023	TCP	Nuance Watcher Telnet Client	Listening	Inbound	
7200-7263	UDP	Badge	Vocera Server	Inbound	• Type: Audio Recording
7500 - 8700	UDP	Vocera Server	Badge/VCG/ VSTG	Outbound	• Type: Audio • Only even-numbered ports are used. The range is configurable in the NSSserver.cfg file available at \vocera\nuance\SpeechServer\config.
7777	TCP	Nuance Resource Manager	Listening	Inbound	• The source is used only when multiple recognition servers are configured.
7780	TCP	VA Flume agent	Vocera Analytics	Bidirectional	
7890	UDP	Nuance Watcher	Listening	Inbound	
8005	TCP	Apache Tomcat	Listening	Inbound	
8009	TCP	Apache Tomcat Connector	Listening	Inbound	
8011	TCP	BPE	Localhost (127.0.0.1)	Bidirectional	
8080	TCP	Apache Tomcat HTTP Connector	Listening	Inbound	
8200	TCP	Nuance Recognition Server	Listening	Inbound	• The source is nuance-server.exe.
8202, 8204, 8206	TCP	Nuance Recognition Server	Listening	Inbound	• The source is nuance-server.exe. • Each additional port used only when dual, triple, or quad recognition servers are configured.
9091	TCP	Administratio Console	Vocera Server	Bidirectional	
9445	TCP	VA Service Monitor	Vocera Analytics	Bidirectional	
27000	TCP	Nuance License Manager	Listening	Inbound	

Vocera SIP Telephony Gateway Ports

Port	Protocol	Source	Destination	Direction	Notes
5060	UDP	IP PBX	Vocera SIP Telephony Gateway	Bidirectional	• Type: Signaling.

Port	Protocol	Source	Destination	Direction	Notes
5300-5555	UDP	Vocera Server	Vocera SIP Telephony Gateway	Bidirectional	- Type: Audio. - Only even-numbered ports are used. The range is configurable in the NSSserver.cfg file available at \vocera\Nuance\SpeechServer\config.
8700 - 9467	UDP	IP PBX	Vocera SIP Telephony Gateway	Bidirectional	- Type: Audio (RTP/RTCP). - The number of ports used is based on the number of lines configured. The maximum number of lines is 256 with 2 ports (RTP and RTCP) for each, or 512 total. The server multiplies 512 by 1.5 to reserve additional ports in case some ports are already in use, resulting in 768 ports. The base port for this range is configurable.
Any free port	UDP	Vocera Server	Vocera SIP Telephony Gateway	Bidirectional	Type: Signaling.

Vocera Client Gateway Ports

Port	Protocol	Source	Destination	Direction	Notes
5200-6300	TCP	Smartphone	VCG	Bidirectional	- Type: Signaling. - If the Use VCG client connection management option is set, the protocol is TCP. Otherwise, it is UDP.
5200-6300	UDP	Badge	VCG	Bidirectional	- Type: audio. - The number of ports used is based on the number of lines configured.
6300-6555	UDP	Vocera SIP Telephony Gateway	VCG	Bidirectional	- Type: audio. - The number of ports used is based on the number of lines configured.
7700-8467	UDP	Smartphone	VCG	Bidirectional	- Type: Audio - The destination uses RTP/RTCP. - The number of ports used is based on the number of lines configured.
Any free port	TCP	Vocera Server	VCG	Bidirectional	Type: Signaling

Vocera Report Server Ports

Port	Protocol	Source	Destination	Direction	Notes
80	TCP	Report Results	(Listening)	Inbound	
3306	TCP	Database	(Listening)	Inbound	The source is MySQL.
5251	TCP	Vocera Server	Vocera Report Server	Bidirectional	Type: Signaling.
8080	TCP	Report Console	Apache Tomcat	Bidirectional	The source is Vocera Report console opened in a browser.

Port	Protocol	Source	Destination	Direction	Notes
9090	TCP	Report Console	Vocera Report Server	Bidirectional	

Badge Ports

Port	Protocol	Source	Destination	Direction	Notes
5000	HTTP	Workstations	Badge	Outbound	C1000/V5000 Onboard Diagnostic Portal
5002	UDP	Badge	Voice Server	Bidirectional	Type: Signaling.
5200	UDP	Badge	Voice Server, VSTG, and VCG	Bidirectional	Type: audio
5400	UDP	Badge	Voice Server	Outbound	Badge Updater Service
5500	UDP	Badge	Voice Server	Outbound	For Vocera Voice Server 5.9 and below. - Type: Secure Signaling - Signaling between the Vocera Server and Vocera Smartbadge using the underlying TLS/SSL protocol.
49152-65535	UDP/DTLS	Badge	Vocera Server	Bidirectional	For Vocera Voice Server 5.10. - Secure Call Signaling and Notifications. - Secure DTLS Signaling between the Vocera Server and Vocera Smartbadge.
5555	TCP/UDP	Badge	Vocera Server	Bidirectional	Badge Log Collector Signaling
5556	TCP/UDP	Badge	Vocera Server	Bidirectional	Badge Log Collector Data
443	TCP/UDP	Badge	Voice Server	Outbound	Signaling and Message Data

Vocera Collaboration Suite Ports

Port	Protocol	Source	Destination	Direction	Notes
80, 443	TCP	VCS Push Notification	(Listening)	Inbound	SSL ports.
5060-5080	TCP	iPhone and Android Smartphone	VCG	Bidirectional	- SIP ports. - Type: Signaling. - If the Use VCG client connection management option is set, the protocol is TCP. Otherwise, it is UDP.
7700-8467	UDP	iPhone or Android Audio	(Listening)	Inbound	Type: audio.
7700-8467, 32768-65536	UDP	Android Audio	(Listening)	Inbound	Type: audio.

WLAN Ports Used by Vocera Clients Ports

Port	Protocol	Source	Destination	Direction	Notes
80, 8080	TCP	VCS	VMP	Inbound	- Type: Data signaling - These ports are for NIO. - The source is for Android and iPhone.
5002	UDP	Badge	Vocera Server	Bidirectional	Type: Signaling
5005	TCP	VMI	Vocera Server	Bidirectional	- Type: Connection - The source includes VMI clients.
5060, 5888, 5889	UDP	VCS	Vocera Client Gateway	Bidirectional	- Type: Signaling - The source is for Android and iPhone.
5200	UDP	Badge	Badge / Voice Server / Vocera SIP Telephony Gateway	Bidirectional	Type: Audio
5251	TCP	VAI	Vocera Server	Bidirectional	- Type: Connection - The source includes VAI clients including Staff Assignment
5300-5555	UDP	Badge	Vocera SIP Telephony Gateway	Inbound	Type: Audio
5400	UDP	Badge	Updater	Bidirectional	Type: Signaling
5555, 5556	UDP	Badge	Voice Server	Bidirectional	Type: Discovery
5555, 5556	TCP	Badge	Voice Server	Bidirectional	- Type: Connection - Ensure that you allow packets from TCP port 5556 to be received on any available port on the Vocera Voice Server.
6300-6555	UDP	Badge	Vocera Communicatic Gateway	Inbound	- Type: Audio - The base port for this range is configurable.
7500-8700	UDP	Badge	Voice Server	Inbound	Type: Audio
8080	TCP	VCS	Vocera Server	Inbound	- Type: Signaling - The source is for Android and iPhone.
32768-65536	UDP	VCS	Vocera Devices	Bidirectional	- Type: Audio - The source is for Android.

Vocera Analytics Ports

Port	Protocol	Source	Destination	Direction	Notes
3306	TCP	Database	(Listening)	Inbound	- Type: Signaling - The source is Maria DB Signaling.
4040	TCP	VA Server	Spark UI	Inbound	
7778	TCP	VA Server	Spark	Bidirectional	The source is a VMP Flume agent.

Port	Protocol	Source	Destination	Direction	Notes
7779	TCP	VA Server	Spark	Bidirectional	• The source is a Engage Flume agent.
7780	TCP	Voice Server	Spark	Bidirectional	• The source is a VS Flume agent.
9445	TCP	Voice Server	(Listening)	Inbound	• The source is a remote agent.
8443	TCP	VA Server	(Listening)	Inbound	• This port is default or user defined. • The source is a reporting service.

Vocera Auto Sending Logs Ports

Port	Protocol	Source	Destination	Direction	Notes
22	TCP	Vocera Server	Vocera ASL Server	Bidirectional	• Each Vocera server is bidirectionally communicating with the destination server, asl.vocera.com: • Inbound direction for ASL update • Outbound direction for sending logs

ASR Broker Ports

Port	Protocol	Source	Destination	Direction	Notes
443	TCP / HTTP/2 / GRPC	ASR Broker	GCP Services	Outbound	
5060	UDP / SIP	ASR Broker	Nuance	Bidirectional	
6060	UDP / SIP	Voice Server	ASR Broker	Bidirectional	
6060	TCP / MRCPv2	Voice Server	ASR Broker	Inbound	
6075	TCP / MRCPv2	ASR Broker	Nuance	Inbound	
6080	TCP / HTTP	Operational/ Monitoring	ASR Broker	Inbound	
6100-6499	UDP / RTP	Badge	ASR Broker	Bidirectional	For Vocera Voice Server 5.7 and below. • The range, 6100-6499 includes only even-numbered ports.
8250-8970	UDP / RTP	Badge	ASR Broker	Bidirectional	For Vocera Voice Server 5.8 and above. • The upper range value is not inclusive. So if upper value is 8700, it means we can go to port 8699.
0/*	TCP / HTTP	ASR Broker	Voice Server	Inbound	• The source is Grizzly HTTP Server.
0/*	UDP / RTP	ASR Broker	Nuance	Bidirectional	

Glossary

A list of networking terms related to IP ports and usage sorted in alphabetical order.

Bidirectional Network Connection

A bidirectional network connection is a connection on which a **source** and **destination** can transmit and receive data and not both at the same time.

See **Unidirectional Network Connection** on page 48

Destination Port

The destination **port number** is the number for the communication associated with the destination application or process on the remote host. The source and destination port numbers are available in the header of each segment or datagram. The datagram is delivered to the process identified by the destination port number.

For example, port 80 refers to HTTP or web service. The client specifies port 80 for the server to know that the request is for web services.

Dynamic Ports

The dynamic ports numbers are in the range between 49152 and 65535. These ports cannot be registered through **IANA** or by any other means. This port range is used for private or customized services, for temporary purposes, and for automatic allocation of ephemeral ports. The dynamic ports are also known as private ports.

See **Port Number** on page 46

EWS

Exchange Web Services (EWS)

It is a protocol introduced by Microsoft for Exchange that was intended for desktop email clients such as Microsoft Outlook. It is a cross-platform API that enables applications to access mailbox items such as email messages, meetings, and contacts from Exchange Online, Exchange Online as part of Office 365, or on-premises versions of Exchange starting with Exchange Server 2007.

See **Network Protocol** on page 45

HTTP

Hypertext Transfer Protocol (HTTP)

It is an application protocol for distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web.

As a request-response protocol, HTTP gives users a way to interact with web resources such as HTML files by transmitting hypertext messages between clients and servers. HTTP clients generally use Transmission Control Protocol (**TCP**) connections to communicate with servers.

See [Network Protocol](#) on page 45

IANA

Internet Assigned Numbers Authority (IANA)

The IANA is a standards body that is responsible for global coordination of the Internet Protocol addressing systems, as well as the Autonomous System Numbers used for routing Internet traffic. Currently, it is a function of [ICANN](#).

ICANN

Internet Corporation for Assigned Names and Numbers (ICANN)

As the operator of Internet Assigned Numbers Authority ([IANA](#)) functions, ICANN allocates IP address blocks to the Regional Internet Registries (RIRs). The RIRs allocate smaller IP address blocks to ISPs and other network operators.

IMAP

Internet Message Access Protocol (IMAP)

It is a standard protocol to access email on a remote server from a local client. It uses the underlying [transport layer protocols](#) to establish host-to-host communication services for applications. It is used to send and receive emails through a remote mail server. IMAP is cross-platform and used to synchronize your email across all devices. The [well-known port](#) address for IMAP is 143.

See [Network Protocol](#) on page 45

IP Address

An IP address (Internet Protocol address) is an identifier for a computer or device on a [TCP/IP](#) network. It is used to identify devices connected to a network. There are currently two different versions of IP addresses in use—IPv4 and IPv6.

Networks using the TCP/IP protocol route messages based on the IP address of the [destination](#).

See [Public IP Address](#) on page 46 and [Private IP Address](#) on page 46

Network Protocol

It is a standard set of rules that governs the communications between computers on a network. Network protocols incorporate all the processes requirement and constraints of initiating and accomplishing communication between computers, routers, servers, and other network enabled devices.

A protocol stack is the complete set of protocol layers that work together to provide networking capabilities. The following are the networking protocols categories defined by the OSI (Open Systems Interconnection) Reference Model:

- **Physical and Data Link layer protocols** define network hardware characteristics, establish communication between devices at a hardware level, and handle data transfers across the network.
- **Network or Internet layer protocols** manage data addressing and delivery between networks, initiate data transfers, and route them over the Internet.
- **Transport layer protocols** manage data transfer and define how packets are sent, received (in sequence), and confirmed.
- **Application, Presentation, and Session layer protocols** contain commands for specific applications, manage connections and terminations, and maintain the form of data sent and received.

POP3

Post office Protocol (POP)

POP3 is designed for receiving incoming E-mails.

See [Network Protocol](#) on page 45

Port Number

The port numbers are in the range between 1 and 65535. The Internet Assigned Numbers Authority ([IANA](#)) assigns port numbers. See [Port Number Registry](#).

A port is an endpoint to a logical connection. A computer-to-computer connection needs a port number to identify what type of port it is. Administrators need to keep the ports open on firewalls and routers to allow the associated protocol into or out of the network. For example, an administrator keeps the port **80** open in order to allow HTTP traffic.

There are three types of ports:

- [Well-known ports](#) (0-1023)
- [Registered ports](#) (1024-49151)
- [Dynamic ports](#) (49152-65535)

Private IP Address

The Private IP Addresses are assigned to hosts that:

- do not require access to hosts in other enterprises or the Internet at large
- do need access to a limited set of outside services (like E-mail, FTP, netnews, remote login) which can be handled by mediating gateways (like application layer gateways)

The Internet Assigned Numbers Authority ([IANA](#)) has reserved the following three blocks of the [IP address](#) space for private internets:

- 24-bit block: Begins with 10.
Example: 10.0.0.0 through 10.255.255.255
- 20-bit block: Begins with 172.16. through 172.31.
Example: 172.31.255.255
- 16-bit block: Begins with 192.168.
Example: 192.168.255.255

Public IP Address

The Public IP Addresses are assigned to hosts that need network layer access outside the enterprise.

See [IP Address](#) on page 45

Registered Ports

The registered ports are assigned by [IANA](#) and on most systems can be used by ordinary user processes or programs executed by ordinary users. The registered ports numbers are also known as user ports and in the range between 1024 and 49151.

Registered ports are temporary ports, usually used by clients, and varies each time a service is used. The port is then abandoned and can be used by other services.

See [Port Number](#) on page 46

RTP

Real-Time Transport Protocol (RTP)

RTP is used to deliver streaming audio and video media over the internet, thereby enabling the Voice Over Internet Protocol (VoIP). RTP is generally used with a signaling protocol, such as SIP, which sets up connections across the network. RTP applications can use the Transmission Control Protocol ([TCP](#)), but most use the User Datagram protocol ([UDP](#)) instead because UDP allows for faster delivery of data.

While RTP allows for real-time data transfer, RTCP provides out-of-band statistics and control information for any given RTP session. It does not actually transport any media data, but rather helps with quality control.

See [Network Protocol](#) on page 45

SIP

Session Initiation Protocol (SIP)

It is a signaling protocol that enables the Voice Over Internet Protocol (VoIP) by defining the messages sent between endpoints and managing the actual elements of a call. SIP supports voice calls, video conferencing, instant messaging, and media distribution.

SIP is just one method of deploying VoIP; its primary benefit is the fact that it provides a direct connection between private or local telephone systems (private branch exchanges, or PBX) and the public telephone network. This way, individuals and businesses do not need a legacy telephone line to connect. Other VoIP deployment methods include the Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), and Session Description Protocol (SDP).

See [Network Protocol](#) on page 45

SMTP

Simple Mail Transfer Protocol (SMTP)

SMTP is used to send and receive email. It is sometimes paired with [IMAP](#) or [POP3](#) (for example, by a user-level application), which handles the retrieval of messages, while SMTP primarily sends messages to a server for forwarding.

SMTP can both send and receive mail, but it is bad at queuing incoming messages, hence the common delegation to other protocols. Proprietary systems like Gmail have their own mail transfer protocols when using their own servers, but they still use good old SMTP to email beyond that.

See [Network Protocol](#) on page 45

Socket

The source and destination ports are placed within the segment. The segments are then encapsulated within an IP packet. The IP packet contains the IP address of the source and destination. The combination of the source and destination IP addresses and the source and destination port numbers is known as a socket. During the lifespan of the socket, the port number on the source and destination will not change.

The socket is used to identify the server and service being requested by the client. Everyday thousands of hosts communicate with millions of different servers. Those communications are identified by the sockets.

It is the combination of the transport layer port number, and the network layer IP address of the host, that uniquely identifies an application process running on an individual host device. This combination is called a socket. A socket pair, consisting of the source and destination IP addresses and port numbers, is also unique and identifies the specific conversation between the two hosts.

Source Port

The source port number is the number for the communication associated with the originating application or process on the local host. The source and destination port numbers are available in the header of each segment or datagram. The datagram is delivered to the process identified by the source port number.

The source port number is randomly generated by the sender to identify a conversation between two applications or processes. Multiple conversations can occur simultaneously; an application or process can send multiple HTTP service requests to a web server at the same time. The conversations are separated and tracked based on the source port numbers.

TCP/IP

Transmission Control Protocol (TCP)

The TCP/IP is the suite of communications protocols that are highly reliable and used to connect hosts in the network. TCP works with the Internet Protocol and guarantees the delivery of data packets and duplicate protection.

Transport Layer Protocols

The transport layer is concerned with efficient and reliable transportation of the data packets from one network to another. The transport layer protocols establish end-to-end communication between the source and destination hosts. These protocols verify that the packets arrive in sequence without errors and swap acknowledgements of data reception or lost packets.

The data packets sent over a network are re-assembled into the proper order at the receiving end. A message goes back to the originating network to resend data packets or to confirm reception of all the packets. At the transport layer level, TCP and UDP are the two protocols used. TCP, paired with IP, is by far the most popular protocol.

UDP

User Datagram Protocol (UDP)

It is a stateless and lightweight transport protocol. The pieces of communication in UDP are called datagrams. These datagrams are sent by the transport layer protocol. Neither the client nor the server is obligated to keep track of the state of the communication session.

The user datagram protocol is transaction-oriented. It does not guarantee the delivery and duplicate protection like **TCP**.

See **Network Protocol** on page 45

Unidirectional Network Connection

A unidirectional network connection is a connection on which a source or destination can do **one** of the following (and not both):

- only transmit data (and unable to receive)
- only receive data (and unable to send)

A **source** can transmit data to one or more **destinations**, but the destinations cannot transmit data back to the source because it is unable to receive. The **Inbound** and **Outbound** directions denote the direction of the traffic moving between networks. However, it is relative to whichever network you are referencing to.

- **Inbound** direction refers to data traffic coming **into** the network.
- **Outbound** direction refers to data traffic going **out of** the network.

VRRP

Virtual Router Redundancy Protocol (VRRP)

This protocol specifies an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN. It allows several routers on a multiple access link to utilize the same virtual IP address. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

The protocol number assigned by the IANA for VRRP is 112 (decimal).

Well-known Ports

The well-known ports are assigned by [IANA](#) and cover the range of [port numbers](#) between 0 and 1023. On many systems, they can only be used by system (or root) processes or by programs executed by privileged users. The well-known ports are also known as system ports.

The well-known ports are the Internet services that have been assigned a specific port. For instance, SMTP is assigned port 25. Servers listen on the network for requests at the well-known ports.

See [Port Number](#) on page 46