stryker

Vocera Messaging Platform IP Port Reference Guide

Notice

Last modified: 2024-02-14 04:08

IPP-Production-Docs build 237

Contents

Introduction

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 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.

The IP Port Reference guide is available for the following Vocera products and each guide provides a comprehensive list of the port requirements required for the product:

- Vocera Analytics
- Vocera Engage
- Vocera Messaging Platform
- Vocera Platform
- Vocera Voice Server

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 9.

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

This guide is intended primarily for network administrators.

Related Information

Here is a list of recommended Vocera products and reference documentation that support the information in this guide.

Vocera Product Documentation

- Vocera Analytics documentation
- Vocera Messaging Platform documentation
- Vocera Platform documentation
- Vocera Voice Server documentation

IP Port Reference Guides for Vocera Products

- Vocera Analytics IP Port Reference Guide
- Vocera Engage IP Port Reference Guide
- Vocera Messaging Platform IP Port Reference Guide
- Vocera Platform IP Port Reference Guide
- Vocera Voice Server IP Port Reference Guide

Additional Information

- Internet Assigned Numbers Authority

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

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 `api.push.apple.com`

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 `gateway.push.apple.com`

Firebase Cloud Messaging (FCM) Ports For Android Devices

Port	Protocol	Source	Destination	Direction	Notes
443	TCP	VMP Server	FCM	Outbound	• The Firebase Cloud Messaging (FCM) destination is `fcm.googleapis.com`.
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 `https://graph.microsoft.com/`.

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	

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 13

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 11

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 10

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 10

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 10

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 11 and Private IP Address on page 11

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 10

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 10

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 11

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 10

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 10

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 10

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 10

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 11