RingCentral

RingCentral Network Requirements and Recommendations

Extended Version

Table of contents

RingCentral Network Requirements and Recommendations

1. Introduction

The purpose of this document is to provide RingCentral customers with customer site network requirements and recommendations to ensure that the RingCentral unified communications solution operates properly. These requirements include constraints for network capacity, quality of service, firewall configuration, and unsupported devices and configurations. Chapter 3 introduces the RingCentral Unified Communications Reference Architecture, which can be used to understand the context of the network requirements stated in later chapters.

2. Acronyms

The following acronyms are used in this document:

- **ACL** - Access Control List
- **ALG** - Application Layer Gateway
- **BLA** - Busy Lamp Appearance
- **BW** - Bandwidth
- **BWH-Data** - Headroom bandwidth for data traffic
- **BWH-Video** - Headroom bandwidth for video traffic
- **BWH-VoIP** - Headroom bandwidth for VoIP traffic
- **BWM-Data** - Maximum bandwidth needed for data traffic
- **BWM-Video** - Maximum bandwidth needed for video traffic
- **BWM-VoIP** - Maximum bandwidth needed for VoIP traffic
- **BWR-Data** - Bandwidth required for data traffic plus headroom for future growth
- **BWR-Total** - The aggregate bandwidth required for VoIP, video, and data traffic
- **BWR-Video** - Bandwidth required for video traffic plus headroom for future growth
- **BWR-VoIP** - Bandwidth required for VoIP traffic plus headroom for future growth
- **DHCP** - Dynamic Host Configuration Protocol
- **DMZ** - Demilitarized Zone
- **DPI** - Deep Packet Inspection
- **DSCP** - Differentiated Services Code Point
- **DSL** - Digital Subscriber Line
- **EF** - Expedited Forwarding
- **GW** - Gateway
- **HD** - High Definition
- **HQ** - High Quality
- **IP** - Internet Protocol
- **ISP** - Internet Service Provider
- **ISP-WAN-CAP** - Capacity required on the ISP WAN link for data plus VoIP traffic
- **ICMP** - Internet Control Message Protocol
- **ITSP** - Internet Telephony Service Provider
- **LAN** - Local Area Network
- **M-Video** - Expected maximum number of video calls
- **M-VoIP** - Expected maximum number of VoIP calls
- **ms** - Milliseconds
- **NTP** - Network Time Protocol
- **PoE** - Power over Ethernet

- **PSTN** - Public Switched Telephone Network
- **QoS** - Quality of Service
- **RTP** - Real-time Protocol
- **SIP** - Session Initiation Protocol
- **SPI** - Stateful Packet Inspection
- **TCP** - Transport Control Protocol

- **UDP** - User Datagram Protocol
- **VLAN** - Virtual LAN
- **VoIP** - Voice over IP
- **VQ** - Voice Quality
- **WAN** - Wide-Area Network
- **WiFi** - Set of standards for wireless communication

3. Unified Communications Reference Architecture

Figure 1 provides the Unified Communications Reference Architecture for RingCentral. The top of the diagram indicates the call control function, a media server function, and carrier telephony interfaces. This functionality is implemented in two data centers. No details are provided of this functionality because they are not important for the customer-site requirements stated in this document. The figure provides representative sample designs of customer sites.

The functionality in the Reference Architecture is color coded as follows:

- RingCentral provided functionality including call controller, voice and video media servers, and carrier interfaces are illustrated in orange. Note that customers sometimes retain existing desk phones, in which case it cannot be designated as RingCentral provided.

- Customer functionality is blue.

A customer network may include one or more of the following functional components:

- **Firewall:** Allows TCP and UDP port control, Access Control List (ACL) or port triggering (opening of ports for the time needed to exchange information with a remote server). The firewall includes a Wide-Area Network Interface that may be of Ethernet, DSL, or cable modem type.

- **Router:** Provides routing (advertisements of IP networks), packet forwarding, ping and traceroute ICMP support and may support packet prioritization, bandwidth management, and Smart Packet Inspection.

- **Ethernet Switch:** Performs Ethernet frame switching, and may support configuration of VLANs, control of Ethernet ports, Power over Ethernet (PoE), and Green Ethernet.

- **Desktop Telephone:** The phones perform two main functions:

  - Call Control: Registration, call set up, call control, and call tear down, and user interface call progress indications and call-handling features.

  - Voice Processing: Analog-to-digital and digital-to-analog conversion, sidetone injection, voice framing, jitter buffering, echo cancellation, speaker and microphone functionality.

- **Computer:** May be serialized with the phone and run the RingCentral Phone™ desktop app, RingCentral Meetings™, or many other types of RingCentral API plug-ins (Google, Salesforce®, Zendesk®, etc.).
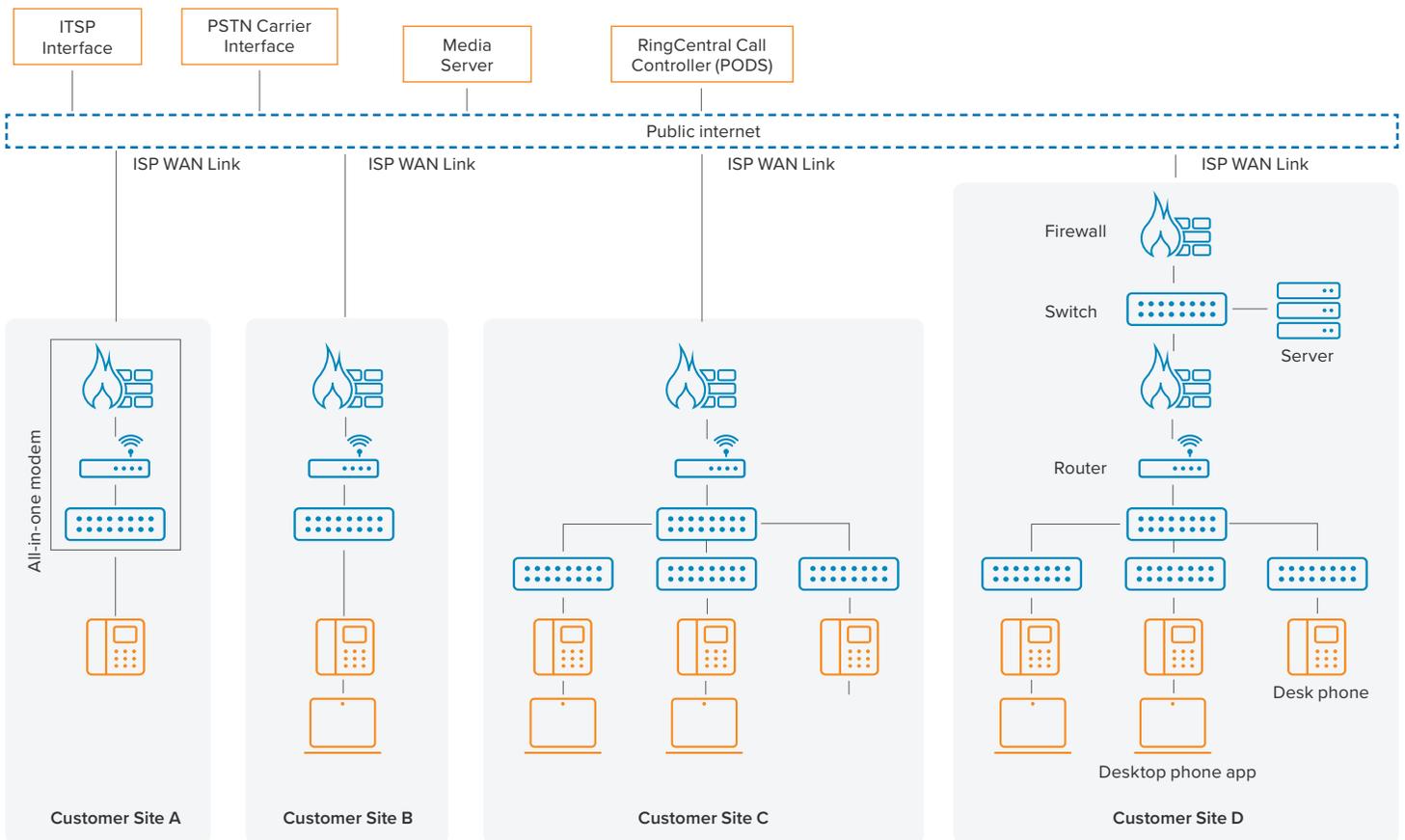
Figure 1. RingCentral Unified Communications Reference Architecture

Implementation variations that may occur at customer sites are:

- One or multiple ISP WAN links (not illustrated in the figure).

- One or more firewalls may be present, e.g., to demarcate a DMZ.

- The Wide Area Network interface, firewall, router, and switch may be implemented as:

  - Individual devices. This implementation is used at larger enterprise sites.

  - Integrated into fewer or even into a single modem device. In the latter case it is referred to as an all-in-one modem, as a (DSL or cable) modem, or as a "router." All-in-one modems are typically only used at small customer sites.

- One or more levels of routers or Ethernet switches may be present. This is typically the case at large enterprise sites.

- Sites may have desk phones, softphones, application integrated dialers (e.g., for Google Chrome™) or a combination thereof depending on user needs.

- Computers running RingCentral applications may or may not be serialized with desk phones.

A full-featured all-in-one modem device has a (DSL or cable) network interface, and router and firewall capabilities. Such a device may connect to the customer network switch. It may also be configured to operate in bypass mode. In bypass mode, a separate firewall and router located behind the modem are provided to provide more advanced firewalling and routing capabilities.

In general, customer network implementations are site dependent. For example, large offices will have a more advanced firewalling, routing, and switching architecture than small branch-office sites. Also, the number and type of phone is more likely to vary at larger sites.

Voice and video calls can be made between phones at a single customer site via the internet, between phones at different customer sites via the internet, involve a Media Server (e.g., for conference calls or to store/retrieve voice mail), or calls may connect to an ITSP or PSTN gateway. The Call Controller registers the phones and handles call orchestration between the various components. To support these types of calls:

- Call control connectivity must exist between the local VoIP LAN at the customer site, the internet, and the RingCentral Call Controller®.

- Media path connectivity must exist between the VoIP LAN at the customer site, the internet, the Media Server, and to the ITSP and PSTN gateway.

4. Required and Recommended Devices and Configurations

RingCentral requires that the customer network supports a minimal set of features to ensure a high-quality VoIP service.

4.1 Tested Routers

A set of WAN routers has been validated to work properly with the RingCentral VoIP service. The list of routers that have been tested can be found at ringcentral.com/support/qos-router.html. It is recommended to use these routers.

Other firewalls and routers have not been tested in an end-to-end RingCentral VoIP solution and may or may not work properly.

4.2 Traffic Prioritization

RingCentral desk phones use Differential Services Expedited Forwarding, EF[46], marking for VoIP and video signaling and media packets. In this way, routers in a customer network prioritize these types of traffic over data traffic.

For reliable media traffic transport, all customer network IP routers must support and enable QoS: routers need to be configured such that VoIP and video traffic is handled with Expedited Forwarding (EF) DSCP 46.

More specifically, to ensure proper call connectivity, and voice and video quality, QoS traffic prioritization must be configured for both inbound and outbound traffic of the following types:

- Signaling SIP/UDP
- Media RTP/UDP
- Media Secured SRTP/UDP

This must be configured for the port ranges indicated in all firewall port tables in section 6.1.

4.3 Bandwidth Management

If routers support bandwidth management, then it is advised to enable this feature and set the bandwidth dedicated for VoIP traffic to the number stated in chapter 7.

4.4 VLANs

If VLANs are supported by network switches, then it is recommended (but not required) to define a VLAN specifically for VoIP and video traffic to logically separate these types of traffic from data traffic. This simplifies management of the unified communications infrastructure.

5. Unsupported Devices and Configurations

Some types of device, device configurations, and network configurations are not supported by the RingCentral unified

communications solution, as they are known to cause continuous or intermittent voice quality issues.

5.1 Unsupported Devices and Configurations

RingCentral does not support use of any of the following devices and network configurations to provide VoIP service:

- Load Balancers routing VoIP traffic concurrently across more multiple WAN links
- WAN Accelerators

Use of load balancers can cause out-of-order packet arrival, which can result in intermittent or continuous voice quality issues. WAN

Use of load balancers can cause out-of-order packet arrival, which can result in intermittent or continuous voice quality issues. WAN accelerators use compression and data duplication to reduce generated traffic. For VoIP, this can lead to packet loss and extra jitter.

5.2 Device Configurations – section completely redone

Some types of device, device configurations, and network configurations are not supported by the RingCentral VoIP solution, as they are known to cause continuous or intermittent voice quality issues.

Unsupported Devices and Configurations: RingCentral does not support the use of any of the following devices or network configurations to provide VoIP or video service:

- Load Balancers routing VoIP traffic concurrently across more multiple WAN links

- WAN Accelerators

Device Configurations: For proper support of the RingCentral unified communications services, the following device settings may need to be disabled on routers, firewalls, and Ethernet switches:

- Router and Firewalls:

    - Session Initiation Protocol Application Layer Gateway (SIP ALG)

    - Deep Packet Inspection (DPI)

    - Stateful Packet Inspection (SPI)

    - WAN Acceleration

    - SIP Transformation on SonicWall Security Appliance

- Ethernet switches: Green Ethernet for power saving

Disabling the router and firewall functionality can be restricted to the RingCentral addresses provided in the next section.

Note that the enabling these device settings may result in intermittent call problems related to phone and call connectivity

6. Firewall Access

To allow call control and media path connectivity, outbound and inbound firewall ports must be opened between the internal customer network and the ISP WAN for the following applications:

- Telephone provisioning and registration

- Call control (SIP signaling)

- RTP media

- Auxiliary services (NTP and Directory Services)

6.1 Firewall Ports

The table below indicates the source port and destination port numbers that are, besides a source IP address, entered in signaling, media, and auxiliary traffic packets by the RingCentral phone and applications residing in the private network. The designation 'random' means that the source port is randomly selected by the host.

The type of phone to which the table pertains is indicated at the bottom of each table. There are no separate ports necessary for Busy Lamp Appearance. BLA uses the signaling ports and uses standard SIP NOTIFY packets. It will use whatever ports all the other messages are using (INVITE, BYE, REGISTER, etc.).

For the next considerations, it is assumed that a firewall with Network Address Translation functionality resides at the interface between the private network and ISP-WAN. The notions of inbound and outbound are defined relative to a local private network.

The source (IP address, port number) pair will be translated by the NAT function into a public source (IP address, port number) pair. To allow traffic to be passed from the private network to the ISP-WAN, if not opened by default, the firewall needs to open a set of outbound ports matching the destination ports indicated in the last column of the table.

In a stateful firewall, no inbound ports need to be opened because they are automatically opened upon a reply to outbound traffic. NAT entry expiration timeout must be set to larger than 5 minutes since telephones re-register every 5 minutes and between registrations keep-alive messages need to be transferred from RingCentral call servers to telephones.

For security reasons, it is advised to avoid use of non-stateful firewalls.

Traffic Type	Protocols	Source Port Number	Destination Port Number
Provisioning	HTTP/TCP and HTTPS/TCP	random	80 and 443
Signaling[1]	SIP/UDP	5060–6000	5090
Signaling	SIP/TCP	5060–6000	5090
Signaling - Secured	SIP/TLS/TCP	5060–6000	5096
Media	RTP/UDP	16384–16482	20000–39999
Media - Secured	SRTP/UDP	16384–16482	40000–49999
Network Time Service	NTP/UDP	random	123
LDAP Directory Service	LDAP-SSL/TCP	random	636

Table 1. Desk Phone

Traffic Type	Protocols	Source Port Number	Destination Port Number
Provisioning	HTTP/TCP and HTTPS/TCP	random	80 and 443
Signaling (deprecated)	SIP/UDP	5060-5099	5091
Signaling	SIP/TCP	random	5091
Signaling - Secured	SIP/TLS/TCP (was SRTP)	random	5097
Media	RTP/UDP	8000–8200	50000–59999
Media - Secured	SRTP/UDP	4000–5000, 20000–60000	60000–64999
LDAP Directory Service	LDAP-SSL/TCP	random	636

Table 2. RingCentral Phone Desktop Application

Traffic Type	Protocols	Source Port Number	Destination Port Number
Signaling and (secured) Media (WebRTC)	HTTP/TLS/TCP, STUN/UDP	5060, 6182, 8080, 8083[2]	5060, 6182, 8080, 8083

Table 3. WebRTC Plugins

Traffic Type	Protocols	Source Port Number	Destination Port Number
Provisioning	HTTP/TCP and HTTPS/TCP	80 and 443	80 and 443
Signaling	SIP/UDP	5060	5090–5091
Signaling	SIP/TCP	random	5090–5091
Signaling - Secured	SIP/TLS/TCP	random	5097
Media	RTP/UDP	4000–5000, 20000–60000	50000–59999
Media - Secured	SRTP/UDP	4000–5000, 20000–60000	60000–64999
Mobile App Data Sync with RingCentral backend for e.g., call log info, presence, and voicemails	HTTPS	random	443
LDAP Directory Service	LDAP/TCP	random	636

Table 4. RingCentral Phone Mobile Application (on Wi-Fi and Cellular Network)

Traffic Type	Protocols	Source Port Number	Destination Port Number
Provisioning/Signaling	HTTP/TCP and HTTPS/TCP	random	443, 8801, 8802
Signaling - Secured	SIP/TLS/TCP (was SRTP)	random	5097
Media	SIP/UDP	random	5091, 8801, STUN: 3478–3479

Table 5. RingCentral Meetings

1. Any third-party device set to "Other" in Admin Web (provisioning tool accessible to RingCentral only) will default to use UDP signaling

6.2 Access Control Lists

Routers and firewalls usually supports an Access Control List (ACL) which can be configured to allow or deny inbound traffic based on source/destination IP address or port numbers produced by remote

- For inbound traffic, the ACL must be set to the following RingCentral originating source IP address ranges:

  — 104.245.56.0/21

  — 185.23.248.0/22

  — 199.68.212.0/22

  — 199.255.120.0/22

  — 103.44.68.0/24

applications. The following inbound ACL rules may be configured in order to disable certain firewall feature such as Deep Packet Inspection (DPI):

- Use of "any / any" ACL rules must be avoided to prevent opening too many ports.

Notes:

- CIDR notation /21 corresponds to a netmask of 255.255.248.0

- CIDR notation /22 corresponds to a netmask of 255.255.252.0

- CIDR notation /24 corresponds to a netmask of 255.255.255.0

7. Bandwidth and LAN/WAN Link Capacity Determination

Several artifacts need to be collected to be able to calculate the bandwidth needed for VoIP, Video over IP, and data traffic at a given customer site. The results of the calculation can be used to determine the capacity needed for the LAN links and the ISP WAN link.

7.1 VoIP Traffic Bandwidth

The following procedure can be used to determine the required VoIP bandwidth across the ISP WAN link and LAN links:

1. Determine the maximum number of simultaneous calls, M-VoIP, at the customer site. This number may be smaller than the number of telephones deployed at the customer site. Solutions used with call centers will result in a higher maximum number of simultaneous calls compared to remote office operation and may be equal to the number of deployed telephones phones. The M-VoIP number can be obtained in various ways depending on whether the VoIP solution superseded a previous (non-)VoIP solution and on the specific use of the solution:

   - **Replaced Legacy** Telephony Solution: In this case, a previous telephony solution (PBX, Centrex, or other vendor's VoIP solution) was present before the RingCentral system was installed. The maximum number of simultaneous calls BWMVoIP can be determined if call logs are still available.

- **Completely New VoIP Solution**: In this case, no history information is available to determine the number of voice calls that will be made from/to the site and the RingCentral solution has not been operational long enough to determine the maximum number of simultaneous calls. Determine the number or hard/soft phones that will be deployed at the site by interviewing the customer or obtaining the information from the Network Information spreadsheet filled out by the customer. A representative percentage of this number should give the expected maximum number of simultaneous calls that will be made to/from the site.

- Operational RingCentral Solution: In this case, the RingCentral VoIP solution has been operational (ideally) for several weeks. Determine from the RingCentral Admin Web application or the RingCentral Service Web interface call log the maximum number of simultaneous calls BWM-VoIP that occur at the site by examining the call logs over a representative number of business days.

2. Take into account that the RingCentral Phone mobile app may be used as well. Mobile apps can be used in two ways:

    •   On the customer's Wi-Fi network. In this case, it will affect the required ISP WAN link capacity. Therefore, the maximum number of mobile applications using Wi-Fi needs to be known and be included in M-VoIP.

    •   On public mobile phone network. With this option, the customer network bandwidth calculation on the customer network is not directly affected.

3. Calculate the bandwidth for each call direction, BWM-VoIP, based on the maximum number of simultaneous calls as:

    BWM-VoIP = **M-VoIP x 100 kbit/s**

    The 100 kbit/s bandwidth includes signaling and media traffic.

7.2 Video Traffic Bandwidth

RingCentral Meeting users may use different communication options:

•   Two-party sessions or group sessions involving at least three parties.

•   If a user does not join the audio portion of a RingCentral Meetings session but calls in via a separate phone connection, then no audio is transferred (transmitted/received) on the user's PC. However, video is still transferred.

The bandwidth used for the RingCentral Meetings application depends on the communication mode:

•   The total audio bandwidth used is similar for a phone (100 kbit/s) or PC joining (60 kbit/s) a RingCentral Meeting session. The differences are due to the used audio codecs. For bandwidth calculations, 100 kbit/s should be used for transmit and received direction (see also group audio conferencing below).

•   Group audio conferencing:

    —   Transmit: 100 kbit/s

    —   Receive: 100 kbit/s

•   Two-party HQ video calls:

    —   Transmit: 600kbit/s

    —   Receive: 600kbit/s

•   Two-party HD video calls:

    —   Transmit: 2 Mbit/s

    —   Receive: 2 Mbit/s

4. To accommodate future growth of the user population at the customer site, add some headroom (BWH-VoIP) for VoIP calls. It is useful to configure some headroom to prevent frequent changes in either Bandwidth Management or the ISP interface capacity required. Use a factor of 10% of the number of simultaneous calls in cases where the expected growth is unknown.

5. The required bandwidth in each direction, BWR-VoIP, to carry VoIP traffic on a customer network on each LAN link and the WAN link, is given by:

    BWR-VoIP = **BWM-VoIP** + **BWH-VoIP**

•   Group HQ video calls:

    —   Transmit: 600kbit/s

    —   Receive: 2 Mbit/s

The following procedure can be used to determine the required Video over IP bandwidth across the ISP WAN link:

1. 1Determine the maximum number of simultaneous video calls, M-Video, at the customer site. This number may be smaller than the number of users at the customer site.

2. Calculate the bandwidth for each call direction, BWM-Video, based on the maximum number of simultaneous calls as:

    BWM-video = **M-video x 2.1 Mbit/s**

    The 2.1 Mbit/s bandwidth used in the calculation assumes that all users used HD video and that a separate audio connection is used for audio.

3. To accommodate future growth of the user population at the customer site, add some headroom (BWH-Video) for video calls

    Use a factor of 10% of the number of simultaneous calls in cases where the expected growth is unknown.

4. The required bandwidth in each direction, BWR-Video, to carry video traffic on a customer network on each LAN link and the WAN link, is given by:

    BWR-Video = **BWM-Video** + **BWH-Video**

7.3 Data Traffic Bandwidth

The following procedure can be applied to determine the bandwidth for data traffic on each LAN/WAN link used to carry VoIP traffic:

- Measure the current maximum amount of data traffic bandwidth, BWM-Data, on the physical links that are also traversed by VoIP and video traffic.

- Add some extra bandwidth headroom (BWH-Data) to ensure that future growth of data traffic is accommodated.

- The possible data traffic bandwidth on a given LAN/WAN link is:

  BWR-Data = BWM-Data + BWH-Data

7.4 Total Required Bandwidth

The total required bandwidth on LAN links and WAN link is equal to

BWR-Total = BWR-VoIP + BWR-Video = BWR-Data

Note that this number may vary per link.

7.5 LAN and WAN Link Capacity

Using the calculated total bandwidth, BWR-Total, the required capacity, ISP-WAN-CAP on the ISP WAN link at a customer site can be determined. If the required bandwidth for BWR-Total, is smaller than the capacity provided by the ISP, then it is clear that the ISP WAN link capacity must be increased to at least the BWR-Total to provide enough bandwidth to support all traffic. If not enough capacity is available, then additional capacity needs to be purchased by the customer from the ISP.

A similar capacity assessment procedure can be used to determine the required capacity for any LAN link inside the customer network which carries VoIP, video and data traffic.

7.6 References

For more information on the RingCentral unified communications solutions, please consult: success.ringcentral.com/RCSupportPortalGuidesVideos

---

For more information, please contact a sales representative. Visit ringcentral.com or call 855-774-2510.

RingCentral, Inc. (NYSE:RNG) is a leading provider of global enterprise cloud communications and collaboration solutions. More flexible and cost-effective than legacy on-premises systems, RingCentral empowers today's mobile and distributed workforce to communicate, collaborate, and connect from anywhere, on any device. RingCentral unifies voice, video, team messaging and collaboration, conferencing, online meetings, and integrated contact center solutions. RingCentral's open platform integrates with leading business apps and enables customers to easily customize business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

RingCentral®

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com