



## Application Note

# Network Requirements for the Onsight Mobile Video Collaboration System V5.0



Librestream

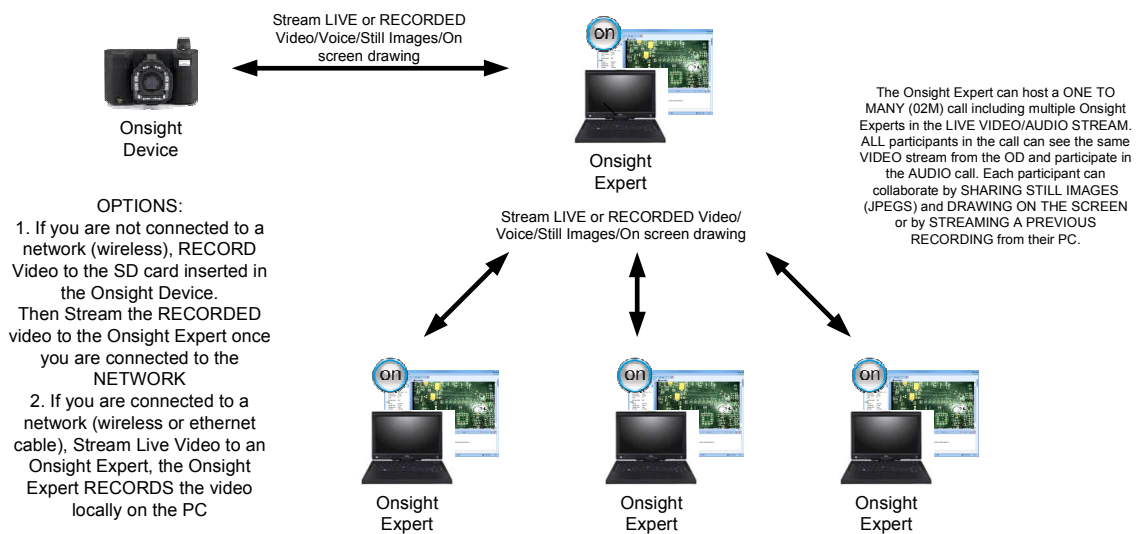
<b>1</b>	<b>NETWORK REQUIREMENTS FOR ONSIGHT MOBILE VIDEO COLLABORATION SYSTEM AND HOSTED SIP SERVICE.....</b>	<b>3</b>
1.1	Overview.....	3
1.2	Direct IP Calling .....	3
1.3	Endpoint Registration to SIP Server .....	5
<b>2</b>	<b>ONSIGHT: NETWORK PROTOCOLS AND PORTS .....</b>	<b>7</b>
2.1	Network Protocols and Ports Table .....	7
<b>3</b>	<b>FIREWALL REQUIREMENTS – ALLOWING SIP TRAFFIC .....</b>	<b>8</b>
3.1	Firewall Diagram.....	9
3.2	Sample Firewall Configuration .....	10
<b>4</b>	<b>ONSIGHT ENDPOINT SIP SERVER CALLS THROUGH FIREWALLS .....</b>	<b>11</b>
4.1	Session Initiation Protocol – Communication Exchange.....	11
<b>5</b>	<b>ONSIGHT TEAMLINK HTTP TUNNELING SERVER .....</b>	<b>12</b>
5.1	TeamLink Encapsulation.....	12
5.2	Firewall Detect.....	12
<b>6</b>	<b>POTENTIAL ISSUES: .....</b>	<b>13</b>
6.1	TeamLink Firewall Detect Limitations.....	13
6.2	Cisco SIP Aware .....	13
<b>7</b>	<b>SIP SERVICE CHECK LIST .....</b>	<b>14</b>

# 1 Network Requirements for Onsight Mobile Video Collaboration System and Hosted SIP Service

## 1.1 Overview

This document provides a description of the network requirements for the Onsight Mobile Video Collaboration system on a Local Area Network and on the Public Internet.

The Onsight Mobile Collaboration System uses Session Initiation Protocol (SIP) to establish an audio and video communication session between endpoints. Communication can occur directly between the Onsight Endpoints when they are on the same LAN or it can occur via a SIP Proxy Server when they exist on different networks.



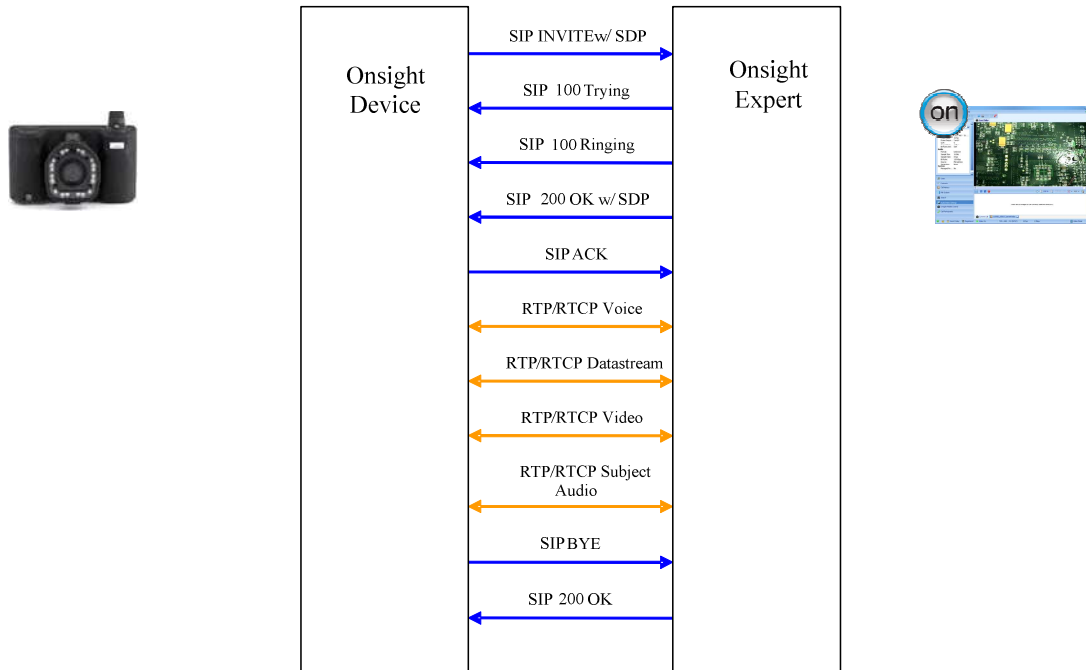
NOTE: The Onsight Expert can only stream RECORDED Video to the Onsight Device. The Onsight Device can stream LIVE or RECORDED Video to the Onsight Expert.

## 1.2 Direct IP Calling

When both Onsight endpoints exist on the same LAN they can communicate directly using the IP address of each Onsight endpoint as the **contact address** to route traffic between each other. Table 4.1 describes the source ports for the SIP and UDP traffic involved in an Onsight Collaboration session.

TCP port 5060 is used for the SIP Protocol and UDP ports 6000 – 6200 are used for Media (audio, video, and data).

## Direct IP Address Call



The Onsite Expert will attempt to open the following Source ports on the PC to initiate sending traffic to the Onsite Device:

### Source Ports for SIP, RTP, RTCP\*

SIP (TCP): random

Video (RTP/RTCP): 6000/6001

Subject audio (RTP/RTCP): 6002/6003

Voice (RTP/RTCP): 6004/6005

Data (RTP): 6006

*\*Each RTP stream has an RTCP stream associated with it, e.g. video happens over RTP 6000, and its associated RTCP stream is over 6001. RTCP provides statistics on the RTP stream.*

However, if these ports are already in use on a PC the Onsite Expert Software will increment the source port until it finds a free one to a maximum of 6200. So the possible range of UDP source ports is 6000 - 6200 on the Onsite Expert.

The Onsite Device will always use these source ports (6000/6001, 6002/6003, 6004/6005, 6006) because it is a closed system.

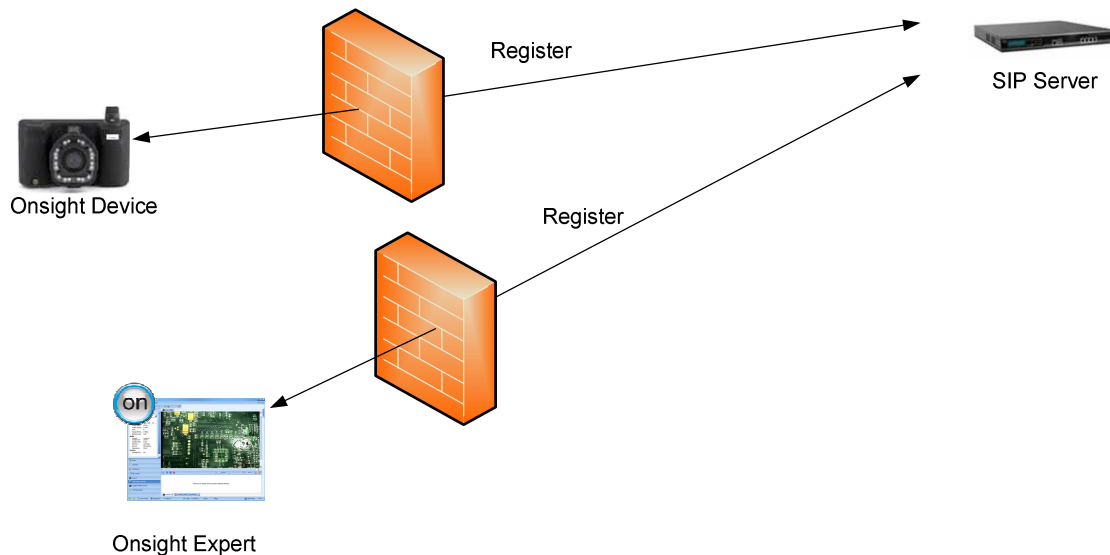
### Destination Ports when using Direct IP Calls:

The destination ports are usually the same so that the video stream's source port is 6000 and it is sending to destination port 6000 on the Onsite Device. (They're both on the same LAN and

communication directly with each other.) The SIP destination port is always 5060 or 5061 (for SIP-TLS).

### 1.3 Endpoint Registration to SIP Server

Firewall/NAT traversal is required to establish a session when the endpoints are not located on the same LAN. This is accomplished by using a SIP Server. Each endpoint registers to the SIP Server which is typically located outside of the Firewall. The SIP Server acts as a proxy and directs SIP messaging and data traffic between the endpoints. Each endpoint is assigned a unique Uniform Resource Identifier (URI) by the SIP Server which is used as the **contact address** for the endpoint. Its format is user@sipdomain.com.



When the Onsite endpoints are registered to the SIP Server, both the Onsite Device and the Onsite Expert can initiate calls by calling the **contact address** (URI) of the other endpoint.

The Onsite Expert Software will attempt to open the following Source ports on the PC to initiate sending traffic to the SIP Server:

#### Source Ports for SIP, RTP, RTCP\*

SIP (TCP): random  
Video (RTP/RTCP): 6000/6001  
Subject audio (RTP/RTCP): 6002/6003  
Voice (RTP/RTCP): 6004/6005  
Data (RTP): 6006

*\*Each RTP stream has an RTCP stream associated with it, e.g. video happens over RTP 6000, and its associated RTCP stream is over 6001. RTCP provides statistics on the RTP stream.*

However, if these ports are already in use on a PC the Onsite Expert Software will increment the source port until it finds a free one to a maximum of 6200. So the possible range of UDP source ports is 6000 - 6200 on the Onsite Expert.

The Onsite Device will always use these source ports (6000/6001, 6002/6003, 6004/6005, 6006) because it is a closed system and nothing else is going to be using them.

Destination Ports when using a SIP SERVER:

When using a SIP Server the destination ports are in the range configured on the SIP Server for the RTP and RTCP traffic, this is because the SIP Server has directed the Onsite Expert to send to these ports. These ports must be opened on the Firewall.

Both the RTP and RTCP are in the range that has been configured on the SIP Server, this range is determined by the SIP Server Administrator and is based on the number of concurrent calls that need to be supported. Note that SIP traffic is still sent to the destination ports of 5060 or 5061.

From the Onsite Experts point of view, it is only sending and receiving traffic to the SIP Server.

## 2 Onsight: Network Protocols and Ports

### 2.1 Network Protocols and Ports Table

This table describes the protocols and ports used by the Onsight Mobile Collaboration System for SIP messaging and data transfer between Onsight Endpoints. For the SIP protocol the source port on the originating endpoint is random, the destination port is TCP 5060. The calling endpoint will try to open the UDP ports as listed in the following table. If a UDP port is already in use on the system the Onsight endpoint will increment the UDP port by one until it finds an open port. The port number will increment until a maximum of 6200. The UDP Media traffic will always be in the port range of 6000 to 6200 when both endpoints exist on the same LAN. (Note that for each RTP stream there is an associated RTCP stream with the exception of the Data stream.)

When two endpoints are using a SIP Server to communicate the UDP destination ports will be in the range dictated by the SIP Server configuration, however the UDP source ports should be in the 6000 to 6200 range. (Note that Firewall/NAT will change source ports as the traffic exits the Local network and is sent over the internet.)

Category	Protocol	SRC Port(s)	Notes	Detail <sup>3,8</sup>	
<b>SIP Signaling</b>	TCP <sup>5</sup>	Random <sup>7</sup>	Used for calls that do not use a SIP proxy server	PC/Device sends SIP/TCP pkts out with SRC=x and DST=5060	PC/Device receives SIP/TCP pkts with SRC=5060 and DST=x
<b>SIP Signaling</b>	TCP	Random <sup>7</sup>	SIP proxy server based calls	PC/Device sends SIP/TCP pkts out with SRC=x and DST=5060	PC/Device receives SIP/TCP pkts with SRC=5060 and DST=x
<b>Video</b>	RTP	6000/6001 <sup>2</sup>		PC/Device sends RTP/RTCP/UDP pkts out with SRC=6000-6001 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6000-6001
<b>Subject Audio</b>	RTP	6002/6003 <sup>2</sup>		PC/Device sends RTP/RTCP/UDP pkts out with SRC=6002-6003 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6002-6003
<b>Voice</b>	RTP	6004/6005 <sup>2,1</sup>	Two-way voice	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6004-6005 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6004-6005
<b>Data</b>	RTP <sup>4</sup>	6006 <sup>2,6</sup>	Status, control, data, etc.	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6006 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6006

1. Device OS 2.34 (and lower) used random ports. PC Application 2.5.1 (and lower) used random ports.
2. The SRC ports shown are the first choice when a call is established. If a requested port is in use on the PC, the port number will increment (to a limit of 6200) until an available port is located. The Device will not have conflicts and will use the ports shown.

3. 'x' are random ports determined during SIP negotiation.
4. Device OS 2.xx used UDP. PC Application 2.x.x used UDP.
5. Optionally configurable as UDP.
6. Device OS 3.76 (and lower) used port 8888. PC Application 3.1.2 (and lower) used port 8888.
7. Send DST port is 5060, or 5061 if TLS is enabled.
8. 'y' are ports determined by the SIP proxy server during call negotiation usually from a limited range configured by the SIP proxy server administrator.

### 3 Firewall Requirements – Allowing SIP Traffic

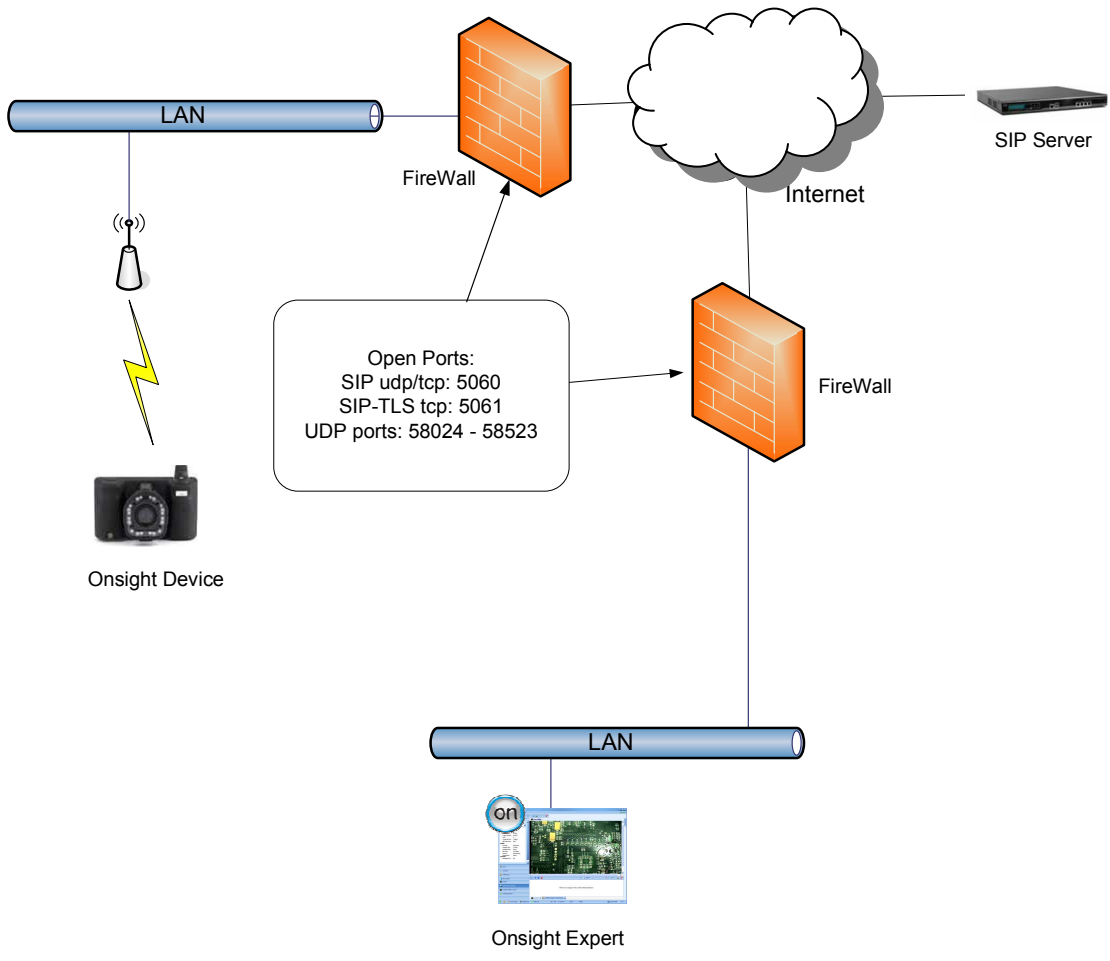
The following ports must be opened to allow SIP and Media traffic to the SIP Server:

- SIP TCP/UDP: 5060 (The Onsite endpoints use SIP TCP 5060 by default but the option to use SIP UDP 5060 is provided.)
- SIP-TLS TCP 5061 (Optional, but required if using TLS encryption for SIP messaging on the SIP Server. SIP-TLS provides encrypted SIP messages and requires the installation of certificates on the Onsite endpoints.)
- UDP Media Ports (see NOTE 1). The range of media ports allows the following RTP/RTCP streams:
  - Video
  - Voice
  - Subject Audio
  - Data

**NOTE 1:**

- Each connection between the Onsite Device and Onsite Expert endpoints will require 16 UDP ports, 8 for each endpoint: 4 RTP and 4 RTCP.
- The SIP Server passes RTP (video/audio/subject audio/data) streams and their associated RTCP streams over the UDP Media Ports. Each stream sends and receives on the same port number.
- The range of UDP ports that must be opened for Media traffic is dependent on the configuration of the SIP Server. The SIP Server dictates which UDP ports will be used during a session by an endpoint.
- See Section 4.1 for a diagram showing the SIP, RTP and RTCP stream flow.

### 3.1 Firewall Diagram



### 3.2 Sample Firewall Configuration

The following sample configuration allows 3 specific IP addresses to send (and receive) SIP (TCP and UDP) messages and data (UDP) to the hosted Librestream SIP server at IP address 64.4.89.118 (siphost.librestream.com). The firewall could also be configured to allow any internal IP address to send/receive on the required ports.

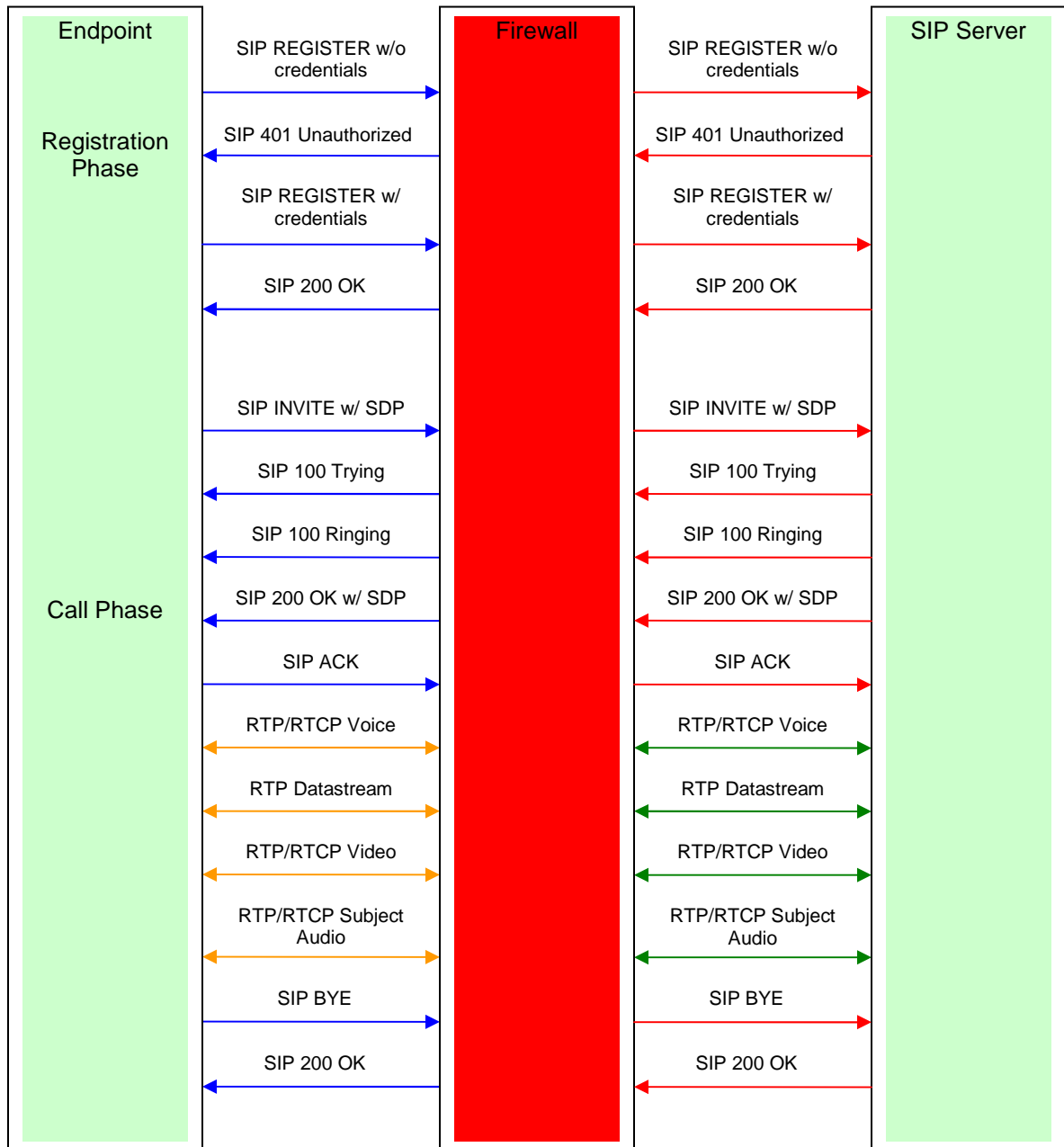
<b>ACTION</b>	<b>Source IP Address</b>	<b>Destination</b>	<b>IP Type</b>	<b>Protocol / Port #</b>
<i>Permit or Deny</i>	<i>IP Address, Hostname that INITIATES</i>	<i>IP Address, Hostname</i>	<i>UDP or TCP</i>	<i>Media Port Range</i>
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060

## 4 Onsite Endpoint SIP Server calls through Firewalls

The Onsite endpoints (Onsite mobile device or Onsite Expert) must register with the SIP Server. Any calls between the Onsite Endpoints are managed by the SIP Server.

Note: There is an option on some SIP Servers to allow two endpoints located behind the same Firewall/NAT to send data directly between each other, but normally all data traffic is routed through the SIP Server.

### 4.1 Session Initiation Protocol – Communication Exchange

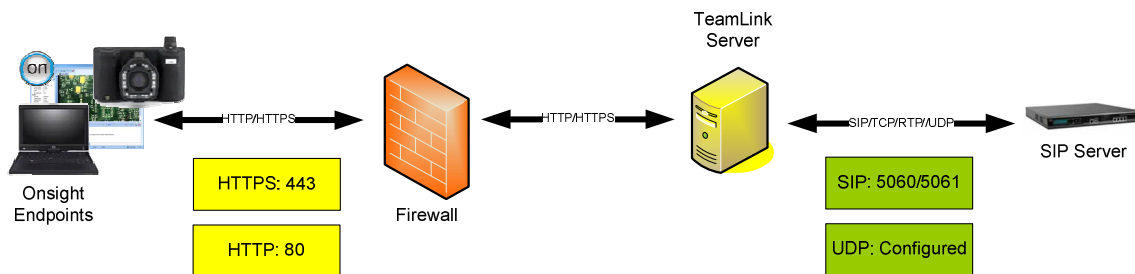


## 5 Onsite TeamLink HTTP Tunneling Server

In situations where it is not possible or practical to open the required SIP and UDP ports on the Firewall, TeamLink can be used to tunnel all SIP and Media traffic encapsulated in HTTP/S packets to an TeamLink Server. The TeamLink Server will proxy all traffic to the SIP Server on behalf of the Onsite Endpoint behind the Firewall. The advantage of this method is that TeamLink uses existing open ports on the Firewall, TCP 80 for HTTP and TCP 443 for HTTPS.

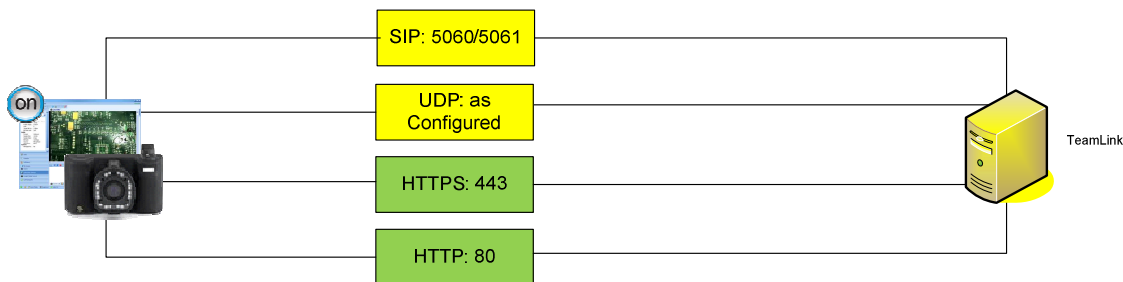
### 5.1 TeamLink Encapsulation

When using TeamLink the Onsite Endpoint will encapsulate SIP (TCP) and Media (RTP/RTCP/UDP) traffic in either HTTP or HTTPS protocol packets. The TeamLink Server receives these packets and strips off the HTTP/HTTPS encapsulation before forwarding them to the SIP Server. The SIP Server will send responses to the TeamLink Server. TeamLink encapsulates the packets before sending them back to the Onsite Endpoint.



### 5.2 Firewall Detect

Firewall Detect is an Onsite System feature that tests the open ports on the Firewall and determines the best method for SIP Registration. If SIP ports are open the Onsite Endpoint will SIP register directly to the SIP Server, if SIP ports are closed the Onsite Endpoint will use TeamLink to SIP register by proxy, using TeamLink, to the SIP Server.



\*Firewall Detection Settings: The tested range of SIP (TCP), HTTP, HTTPS and UDP ports can be configured within the Onsite Endpoint. The UDP range must match the SIP Server's UDP Media range configuration.

## 6 Potential Issues:

### 6.1 TeamLink Firewall Detect Limitations

The firewall detection implementation of TeamLink and the OE/OD clients have these known issues:

1. TeamLink won't detect firewalls that have already been configured to work with unknown SIP Servers which may result in the use of HTTP/HTTPS tunneling when it is not required. This is because the SIP ports are tested using the TeamLink Server as the destination. If the Firewall blocks SIP to TeamLink but allows it to another unknown SIP Server this will be reported as 'SIP blocked'. (Note: the term 'unknown SIP Server' is meant only to indicate that TeamLink is unaware of the SIP Server in terms of Firewall Detect.)
2. TeamLink won't detect VCS Expressway/Control pairs and depending on configuration, SIP calls may fail.
3. CUCM is not supported and would not work without an alternative firewall traversal mechanism.

CASE 1: An existing customer already has firewall rules to allow SIP/UDP to a certain SIP Server. If there are no similar rules on the firewall defined for the TeamLink, the firewall detection algorithms on the OD/OE will report that SIP is not available and use tunneling by default. Recommendation is that existing and new customers should apply firewall rules for SIP/UDP for both the TeamLink and the existing SIP Server; *otherwise they should disable the TeamLink configuration when inside the firewall.*

CASE2: A customer has a VCS Expressway and VCS Control pair. In this case the TeamLink may report that SIP is not available when behind the firewall and tunneling may not work if the SIP settings are pointing to the VCS Control. Customers in this configuration already have to re-point the SIP settings to the VCS Express or VCS Control when they cross from one side of the firewall to the other. *It is recommended that you disable the TeamLink configuration when behind the firewall and enable the TeamLink configuration when on the outside of the firewall.*

CASE3: Customers with Cisco Unified Communications Manager (CUCM). The CUCM installations we've seen do not have any firewall/NAT traversal mechanisms and are generally always behind the firewall. In this case, since the TeamLink is in the cloud, it cannot contact the CUCM and will not be able to tunnel.

### 6.2 Cisco SIP Aware

Cisco Routers have a SIP aware feature that is enabled by default. It rewrites header information in the SIP packets with respect to source addressing for the SIP packet, which confuses the SIP Server and must be turned OFF in order for the SIP Server communication to work correctly.

**To turn OFF Cisco SIP aware:**

- show fixup sip 5060
- no fixup protocol sip 5060

Or

- no ip nat service sip udp port 5060
- no ip nat service sip tcp port 5060

Alternatively, the Onsite endpoints can be configured to use SIP-TLS for the Authentication transport. This requires a certificate to be installed on the endpoints. SIP-TLS encrypts the SIP messaging headers and therefore the headers are ignored by the SIP aware feature of the Cisco router.

## 7 SIP Service Check List

- Firewall ports have been configured
- Onsite devices are connected to the network (WiFi or Ethernet)
- Endpoints have been configured with SIP Account information
- SIP server address
  - URI
  - User name and password
  - Authentication Transport Setting
- Install Certificates (if necessary, for SIP-TLS)
- If required, TeamLink has been enabled.
- TeamLink accounts have been configured
  - Server, Path, User ID, Password
  - HTTP Port, HTTPS Port

For further information regarding SIP Registration Setup consult the Onsite Device and Onsite Expert User Manuals.