Remote H.323 Extensions

For Release 8.0+, the configuration of remote H.323 extensions is supported without needing those extensions to be running special VPN firmware. This option is intended for use in the following scenario:

- The customer LAN has a public IP address which is forwarded to the IP Office system. That address is used as the call server address by the H.323 remote extensions.
- The user has a H.323 phone behind a domestic router. It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, it will be able to receive RTP/RTCP from that same IP address and port. If this is not the case, the configuration of the user's router to support that is not covered by this documentation.
- Other scenarios can be configured. For example, one of the IP Office's LAN interfaces can be connected to the public internet.

Supported Telephones
Currently remote H.323 extension operation is only supported with 9600 Series phones already supported by the IP Office system.

License Requirements
For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either Teleworker or Power User user profiles. On Server Edition systems remote workers can only be configured for users licensed and set to the Power User user profile.

Customer Network Configuration
The corporate LAN hosting the IP Office system requires a public IP address that is routed to the LAN interface of the IP Office system configured for remote H.323 extension support.

STUN from the IP Office system to the Internet is used to determine the type of NAT being applied to traffic between the system and the Internet. Any routers and other firewall devices between the H.323 phone location and the IP Office system must allow the following traffic.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>1719</td>
<td>UDP port 1719 traffic to the IP Office system must be allowed. This is used for H225 RAS processes such as gatekeeper discovery, registration, keepalive, etc. If this port is not open the phone will not be able to register with the IP Office system.</td>
</tr>
<tr>
<td>TCP</td>
<td>1720</td>
<td>TCP port 1720 traffic must be allowed. This is used for H225 (call signalling).</td>
</tr>
<tr>
<td>RTP</td>
<td>Various</td>
<td>The ports in the range specified by the system's RTP Port Number Range (Remote Extn) settings must be allowed.</td>
</tr>
<tr>
<td>RTCP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Network Configuration
It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, it will be able to receive RTP/RTCP from that same IP address and port. If this is not the case, the configuration of the user's router to support that is not covered by this documentation.

System Configuration
This is a summary of the system configuration changes necessary. Additional details and information for H.323 telephone installation are included in the H.323 IP Telephone Installation manual. This section assumes that you are already familiar with IP Office system and H.323 IP telephone installation.

1. Licensing
For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either Teleworker or Power User user profiles. On Server Edition systems remote workers can only be configured for users licensed and set to the Power User user profile.

2. System Configuration
The following needs to be configured on the IP Office system LAN interface to which the public IP address is routed.

a. Select System | LAN1/LAN2 | VoIP. Check that the H.323 Gatekeeper Enable setting is selected.

b. Due to the additional user and extension settings needed for remote H.323 extension configuration, we assume that the extension and user records for the remote H.323 extensions and users are added manually.
c. Select H.323 Remote Extn Enable.

d. Set the RTP Port Number Range (Remote Extn) range to encompass the port range that should be used for remote H.323 extension RTP and RTCP traffic. The range setup must provide at least 2 ports per extension being supported.

  • Note: When the system is configured on an open internet connection, the standard RTP port range is used for all H.323 calls including remote workers. In such a case the RTP Port Number Range is used.

3. Network Topology Configuration

STUN can be used to determine the type of NAT/firewall processes being applied to traffic between between the IP Office system and the Internet.

a. Select the Network Topology tab. Set the STUN Server IP Address to a known STUN server. Click OK. The Run STUN button should now be enabled. Click it and wait while the STUN process is run. The results discovered by the process will be indicated by ! icons next to the fields.

b. If STUN reports the Firewall/NAT Type as one of the following, the network must be reconfigured if possible as these types are not supported for remote H.323 extensions: Static Port Block, Symmetric NAT or Open Internet.

4. H.323 Extension Configuration

H.323 remote extensions use non default settings and so cannot be setup directly using auto-create.

a. Within Manager, add a new H.323 extension or edit an existing extension.

b. On the Extn tab, set the Base Extension number.

c. On the VoIP tab, select Allow Remote Extn.

d. The other settings are as standard for an Avaya H.323 telephone.

  • The IP Address field can be used to restrict the the source IP address that can used by the Remote Worker. However, it should not used in the case where there is more than one phone behind the domestic router.

  • Regardless of direct media configuration, direct media is not used for remote H.323 extensions.

5. User Configuration

For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either Teleworker or Power User user profiles.

a. In the user configuration, select Enable Remote Worker.

  • If the user’s Extension Number matches the Base Extension setting of an IP extension, the Allow Remote Extn setting of that extension is automatically changed to match the user’s Enable Remote Worker setting and vice versa.

Phone Configuration

The phones do not require any special firmware. Therefore they should first be installed as normal internal extensions, during which they will load the firmware provided by the IP Office system.

Once this process has been completed, the address settings of the phone should be cleared and the call server address set to the public address to be used by remote H.323 extensions.

It is assumed that at the remote location, the phone will obtain other address information by DHCP from the user’s router. If that is not the case, the other address setting for the phone will need to be statically administered to match addresses suitable for the user’s home network.

Performance figures, data and operation quoted in this document are typical and must be specifically confirmed in writing by Avaya before they become applicable to any particular order or contract. The company reserves the right to make alterations or amendments at its own discretion. The publication of information in this document does not imply freedom from patent or any other protective rights of Avaya or others.

All trademarks identified by (R) or TM are registered trademarks or trademarks respectively of Avaya Inc. All other trademarks are the property of their respective owners.