Configuring Avaya™ Communication Manager for the Avaya™ S8300 Media Server and Avaya™ G700 Media Gateway to support Avaya™ IP Softphones and Avaya™ IP Telephones behind D-Link and Linksys Broadband Routers with and without VPN Clients
- Issue 1.0

Abstract

These Application Notes present sample configurations to support multiple Avaya IP endpoints behind D-Link and Linksys Broadband Routers, with and without VPN clients. Cisco VPN clients with a Cisco VPN 3000 Concentrator and Avaya VPN clients with an Avaya VSU 5000 Gateway were verified in these Application Notes.
1. Introduction

Avaya Communication Manager can discover Network Address translated (NATed) IP endpoints through the registration process, after which it instructs them to use their NATed IP addresses for registration, call signaling and media control.

These Application Notes present a sample configuration to support multiple IP endpoints behind the D-Link and Linksys Broadband Routers as shown in Figure 1, 2 and 3. An Avaya S8300 Media Server with a G700 Media Gateway is located in the Main Office and two SOHO 1 and 2 (small offices home office) are located remotely. SOHO 1 and 2 use D-Link and Linksys Broadband Routers to access the Main Office respectively. In Figure 1, the S8300 Media Server is on the public data network, therefore, the IP endpoints behind these routers can access to the S8300 Media Server without using a VPN tunnel. In Figure 2 and 3, the S8300 Media Server is on the Intranet (private) network and the remote PCs must communicate with the Intranet in the Main Office through VPN clients. The Cisco VPN 3000 Concentrator is used in Figure 2 and the Avaya VSU 5000 is used in Figure 3.

The D-Link and Linksys Broadband Routers are configured with one WAN (public) IP address to support all the devices on their private networks by network address port translation (NAPT).
Figure 2: Avaya IP Softphones with Cisco VPN Clients

Figure 3: Avaya IP Softphones with Avaya VPN Clients
2. Software and Hardware Validated

This configuration was based on the following software versions:

<table>
<thead>
<tr>
<th>Hardware Component</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya™ S8300 Media Servers</td>
<td>R011X.02.110.4</td>
</tr>
<tr>
<td>Avaya™ IP 4612 telephone</td>
<td>1.72</td>
</tr>
<tr>
<td>Avaya™ IP Softphone</td>
<td>4.1.38</td>
</tr>
<tr>
<td>Avaya™ VPN Manager</td>
<td>3.2.14</td>
</tr>
<tr>
<td>Avaya™ VSU 5000</td>
<td>3.2.17</td>
</tr>
<tr>
<td>Avaya VPNremote® client</td>
<td>4.1.09</td>
</tr>
<tr>
<td>Cisco 3000 concentrator</td>
<td>3.6.3</td>
</tr>
<tr>
<td>Cisco 3000 client</td>
<td>3.6.3</td>
</tr>
<tr>
<td>D-Link DI-704P</td>
<td>2.6.1 build 2</td>
</tr>
<tr>
<td>Linksys BEFSR41</td>
<td>1.44.2</td>
</tr>
</tbody>
</table>

3. Considerations

3.1. Considerations for NATed Endpoints in Figure 1

a. Multiple IP Softphones can be supported behind the D-Link or Linksys routers. When multiple IP Softphones are configured with different port ranges, these port ranges can be configured as service ports on the D-Link or Linksys so that they are not changed across the D-Link or Linksys router. A local IP address must be configured to the WAN IP address for the IP Softphones behind the Linksys router (See Section 4.3.1).
b. Only one IP telephone can be supported behind the D-Link router. The reason is that the IP telephones within the same network region use the same source layer 4 (TCP or UDP) port or port range for registration and signaling.
c. The Linksys router cannot support any IP telephones. The reason is that the IP telephone cannot configure the local IP address as the IP Softphone does.
d. Direct IP-IP Audio Connections in section 4.1 must be set to “No” for remote IP network region 2 when the IP endpoints behind the same Linksys router need to communicate with each other (IP Softphones 3 and 4 in Figure 1). There is no such limitation for the D-Link router, i.e. direct IP-IP Audio Connection can be set to either yes or no.
e. The D-Link router needs to be rebooted for new changes to take effect. Sometimes, it is necessary to restart the IP Softphone application for successful registrations.

3.2. Considerations for VPN Clients in Figures 2 and 3

The following observation apply to Cisco and Avaya VSU related VPN configurations:

a. For the D-Link and Linksys routers, multiple VPN clients can be supported. Regular NAPTeed devices may not support multiple VPN clients behind them. D-Link and
Linkssys can support ISAKMP (Internet Security Association and Key Management Protocol) not only based on UDP port 500, but also based on ISAKMP initiator cookies.
b. When a client VPN is up, all the application layer information including layer 4 and above is encapsulated into the VPN header, D-Link and Linksys only process the VPN header using NAPT and do not touch the application layer. Therefore, there is no NAPTed issue for the IP Softphones.
c. IPSec over UDP encapsulation must be configured in order to support multiple VPN clients behind the D-Link or Linksys router. If UDP encapsulation is used for the IPSec tunnel, there is no need to enable IPSec pass-through on the D-Link or Linksys router. In order to support IPSec over UDP encapsulation, it must be enabled on the Cisco VPN 3000 Concentrator and the Cisco VPN client or Avaya VPNremote Client.
d. The ‘change ip-network-map’ command in Communication Manager can be used to put the remote IP Softphone into a separate network region based on the IP address pool (10.10.10.1-254 in the example).

Cisco VPN related considerations:

a. For the Cisco VPN clients, the IP Softphone is a NATed device. The NATed IP address is the IP address obtained from the client IP address Pool (10.10.10.1-254 in the example).
b. When Split Tunneling Policy is configured to ether tunnel everything or only tunnel networks in a list that includes the client IP address pool, two remote clients can communicate with each other. Therefore, Direct IP-IP Audio Connections can be configured to “yes” for the remote network region so that the two IP Softphones can communicate with each other through Direct IP-IP.
c. If Split Tunnel Policy is configured to only tunnel networks in a list that does not include the client IP address pool, two remote clients cannot communicate directly with each other. Therefore, Direct IP-IP Audio Connections must be configured to “No” for the remote IP network region (Network region 2 in the example) so that the two IP Softphones can communicate with each other through IP-TDM.

Avaya VPN related considerations:

a. For Avaya VPNremote clients, the IP Softphone is a non-NATed device and the IP address is the address from the client IP address Pool.
b. Two VPN remote clients are not allowed to communicate with each other (even if the client IP address pool is included in the IP group) on the VSU. Direct IP-IP Audio Connections must be configured to “No” for the remote IP network region (Network region 2 in the example) so that two IP Softphones can communicate with each other through IP-TDM.

4. Device Configurations In Figure 1

A D-Link or Linksys Router must be configured so that any layer 4 ports used by the Avaya IP endpoints do not change across the router. The following layer 4 ports are used by Avaya IP telephones:
Registration: UDP 49300
Signaling: TCP range 1500 to 6500
Media (RTP): Obtained from ip-network-region configuration on S8300 Media Server
(See section 4.1)

Layer 4 ports used by Avaya IP Softphones are manually configured on the login screen:
**Setting/Advanced** (See section 4.2.1 and 4.3.1). IP Softphones use these ports for registration,
signaling, and media, and will ignore the port range obtained from the ip-network-region
configuration on the MultiVantage Server during the registration process.

### 4.1. Avaya S8300 Media Server Configuration

**Figure 4** shows the related Avaya S8300 Media Server configuration in **Figure 1**.
Based on the configuration in **Figure 4**, all the remote IP endpoints are put into default network
region 2, considering the remote public IP addresses are unknown. The local IP endpoints are
put into network region 1 by using the ‘change ip-network-map’ command. Remote IP endpoints
are configured to communicate with the other IP endpoints using the G.729 (IP Codec-set 2) to
save bandwidth. The remote IP telephones will use UDP port range 8000 to 9001 configured in
IP-network-region 2 for media connections.

---

#### display ip-interfaces

<table>
<thead>
<tr>
<th>Enable</th>
<th>Eth Pt</th>
<th>Type</th>
<th>Slot</th>
<th>Code Sfx</th>
<th>Node Name</th>
<th>Subnet Mask</th>
<th>Gateway Address</th>
<th>Rgn</th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>PROCR</td>
<td></td>
<td>10</td>
<td>.4 .4 .78</td>
<td>255.255.255.0</td>
<td>10 .4 .4 .1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### change ip-network-region 2

<table>
<thead>
<tr>
<th>Region: 2</th>
<th>IP Network Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Audio Parameters</td>
<td>Direct IP-IP Audio Connections?</td>
</tr>
<tr>
<td>Codec Set: 2</td>
<td>IP Audio Hairpinning?</td>
</tr>
<tr>
<td>Location: UDP Port Range</td>
<td>RTCP Enabled?</td>
</tr>
<tr>
<td>Min: 8000</td>
<td>RTCP Monitor Server Parameters</td>
</tr>
<tr>
<td>Max: 9001</td>
<td>Use Default Server Parameters?</td>
</tr>
</tbody>
</table>

DiffServ/TOS Parameters

| Call Control PHB Value: 34 |
| VoIP Media PHB Value: 46 |
| BBE PHB Value: 43 |
| 802.1p/Q Enabled? | N |

---
change ip-network-region 2

Inter Network Region Connection Management
Region (Group Of 32)
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 001-032 2 2

change ip-network-map

IP ADDRESS MAPPING
Subnet
From IP Address (To IP Address or Mask) Region
10.4.4.0 10.4.4.254 1
...

change ip-codec-set 2

IP Codec Set
Codec Set: 2
Codec Silence Frames Packet
Audio Suppression Per Pkt Size (ms)
1: G.729 n 2 20
2:

Figure 4: S8300 Media Server Configuration

4.2. D-Link and related IP endpoints configuration

It is recommended to configure static IP addresses for the IP telephone and the PCs with IP Softphones (As shown in Figure 1: SOHO 1), because these IP addresses must be known for the virtual server/service ports configuration on the D-Link router. The Non-IP Softphone PCs can be configured as DHCP Clients.

4.2.1. IP Softphone 1 and 2 Configuration

Figure 5 and 6 show IP Softphone 1 and 2 configuration through Login/Setting/Advanced. IP Softphone 1 will use source layer 4 (TCP and UDP) port range 1025 to 1124 for RAS, signaling and media and IP Softphone 2 will use different source layer 4 (TCP and UDP) port range 7025 to 7124 for RAS, signaling and media.

Note: A WAN IP address can be configured as local IP address.
Figure 5: IP Softphone 1 Configuration

Figure 6: IP Softphone 2 Configuration
4.2.2. D-Link Configuration

**Figure 7** shows WAN Configuration through Home/WAN with a WAN IP address 192.168.5.30 and Gateway: 192.168.5.1

**Figure 8** shows LAN Configuration through Home/LAN. A DHCP server is enabled on the D-Link with the IP pool address range 192.168.0.100 to 192.168.0.199. The IP telephone should use the static IP addresses, which are not in the DHCP IP pool range. 192.168.0.200 to 202 are used for the IP telephone and IP Softphones.

**Figure 9** shows the Virtual Server Configuration through Advanced/Virtual Server. IP Softphone 1 with IP address 192.168.0.200 is configured with service port range 1025 to 1124, IP telephone 1 with IP address 192.168.0.201 is configured with service port 49300 (RAS), 1500 to 6500 (Signaling) and 8000 to 9001 (Media). IP Softphone 2 with IP address 192.168.0.202 is configured with service port range 7025 to 7124.

Note: There should be no overlap for service ports. These service ports associated with the IP endpoints apply to both TCP and UDP and are not changed through the D-Link.
Figure 8: LAN Configuration for D-Link

Figure 9: Virtual Server Configuration for D-Link Router
4.3. Linksys and related IP endpoints Configuration

It is recommended to configure static IP addresses for the IP telephone and the PCs with IP Softphones (as shown in Figure 1: SOHO 2), because these IP addresses must be known for port range forwarding configuration on the Linksys router. The Non-IP Softphone PCs can be configured as DHCP Clients.

4.3.1. IP Softphone 3 and 4 configurations

Similar to the section 4.2.1, IP Softphone 3 and 4 are configured to use different source layer 4 port ranges (port range 1025 to 1124 for IP Softphone 3 in Figure 10 and 7025 to 7124 for IP Softphone 4 in Figure 11). Note that these port ranges must not be overlapped.

Note: For successful registration, local IP address must be configured to the WAN IP address: 192.168.6.30.

Figure 10: IP Softphone 3 Configuration
4.3.2. Linksys Configuration

**Figure 12** shows setup configuration for WAN and LAN. WAN IP address: 192.168.6.30; WAN Gateway: 192.168.6.1; LAN IP address: 192.168.0.1.

**Figure 13** shows DHCP configuration. The DHCP server uses an IP pool address from 192.168.0.2 to 192.168.0.51 (50 IP addresses) for the Non-IP Softphone PCs installed. IP Softphone 3 and 4 use static IP addresses 192.168.0.200 and 192.168.0.202, which are not in the DHCP IP address pool.

**Figure 14** shows Port Range Forwarding Configuration. IP Softphone 3 with IP address 192.168.0.200 is configured with service port range 1025 to 1124 (TCP and UDP). IP Softphone 4 with IP address 192.168.0.202 is configured with service port range 7025 to 7124 (TCP and UDP). Make sure that protocol TCP and UDP are selected and enabled.
Figure 12: Setup Configuration on WAN and LAN for Linksys Router

Figure 13: DHCP Configuration for Linksys Router
5. Device Configurations In Figures 2 and 3
See Section 8 for general Cisco and Avaya VPN client configuration references.

5.1. Avaya S8300 Media Server Configuration
Figure 15 shows the related Avaya S8300 Media Server configuration. The local IP endpoints are put into the default network region 1 and the remote IP Softphones are put into network region 2 by the ‘change ip-network-map’ command based on the client IP address pool. The remote IP endpoints are configured to communicate with the other IP endpoints using G.729 (IP Codec-set 2) to save bandwidth.
```
display ip-interfaces

IP INTERFACES

<table>
<thead>
<tr>
<th>Enable</th>
<th>Eth Pt Type</th>
<th>Slot</th>
<th>Code</th>
<th>Sfx</th>
<th>Node Name</th>
<th>Subnet Mask</th>
<th>Gateway Address</th>
<th>Rgn</th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>PROCR</td>
<td>10</td>
<td>.4</td>
<td>.4</td>
<td>.78</td>
<td>255.255.255.0</td>
<td>10.4.4.1</td>
<td>1</td>
</tr>
<tr>
<td>n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

change ip-network-map

IP ADDRESS MAPPING

<table>
<thead>
<tr>
<th>From IP Address</th>
<th>(To IP Address or Mask)</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.0</td>
<td>10.10.10.255</td>
<td>24</td>
</tr>
</tbody>
</table>

change ip-network-region 2

IP Network Region

Region: 2
Name:

Audio Parameters
Codec Set: 2
Location:
UDP Port Range
Min: 2048
Max: 3028

DiffServ/TOS Parameters
Call Control PHB Value: 34
VoIP Media PHB Value: 46
BBE PHB Value: 43

802.1p/Q Enabled? N

change ip-network-region 2

Inter Network Region Connection Management

Region (Group Of 32)
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 2 3 4 5 6 7 8 9 0 1 2
001-032 2 2
033-064
```
change ip-codec-set 2

IP Codec Set

Codec Set: 2

Audio Codec: 2
Silence Suppression Per Pkt Size(ms)
1: G.729 n 2 20

Figure 15: S8300 Media Server Configuration for VPN Clients

5.2. Cisco VPN 3000 Concentrator Configuration

Figure 16 shows Basic Group Configuration for Client Configuration through Configuration> User Management>Base Group>Client Config. Make sure that IPSec over UDP is checked. Split Tunneling Policy is configured to tunnel everything for strong security in Figure 16. If Split Tunneling Policy is configured to only tunnel network in a list, include the client IP address pool in the list. Network List can be configured through Configuration>Policy Manage>Traffic Management>Network Lists>Add. Figure 17 shows a network list named “Intranet” configuration and the list includes private IP network 10.4.4.0/24 and client IP Pool 10.10.10.0/24.
Figure 16: Base Group Client Configuration for Cisco VPN 3000 Concentrator
5.3. Cisco VPN Client Configuration

Figure 18 shows how to enable IPSec over UDP encapsulation for a Cisco VPN Client. **Transparent tunneling** and **Allow IPSec over UDP** must be enabled on the Cisco VPN Client.
5.4. Avaya VPNremote Client Configuration

Figure 19 shows how to enable IPSec over UDP Encapsulation for an Avaya VPN remote client through Advanced/Preferences. Enable UDP encapsulation must be checked on the Avaya remote client. Note: There is no configuration needed on the Avaya VSU.

![Figure 19: Avaya VPNremote Configuration for IPSec over UDP](image)

6. Verification Steps

The verification includes two parts:

1. Verify that the IP endpoints can register to the S8300 Media Server successfully. Use the command ‘status station <phone number>’ to verify that IP endpoints register to the S8300 Media Server with correct IP addresses. For the scenario without VPN, IP endpoints should register to the S8300 Media Server with the public IP address. For the scenario with VPN, IP endpoints should register to the S8300 Media Server with IP addresses obtained from the IP address pool.
2. Verify that phone calls can get through for remote IP endpoints with correct IP addresses among Main Office, SOHO 1 and 2 with the command ‘status station <phone number>’.

7. Conclusion
As illustrated in these Application Notes, Avaya Communication Manager Software can discover NATed endpoints. D-Link and Linksys Broadband routers can be configured to support multiple IP endpoints for SOHO with and without IPSec tunnels. For the scenario without VPNs (Figure 1), different configuration considerations apply, depending on the router used.

8. References

Refer to [http://support.avaya.com/japple/css/japple?PAGE=avaya.css.CSSLvl1&temp.groupID=125617](http://support.avaya.com/japple/css/japple?PAGE=avaya.css.CSSLvl1&temp.groupID=125617) for Avaya VPNmanager® and VPNremote Client Configuration.