AT&T Collaborate^{SM}

Customer Configuration Guide

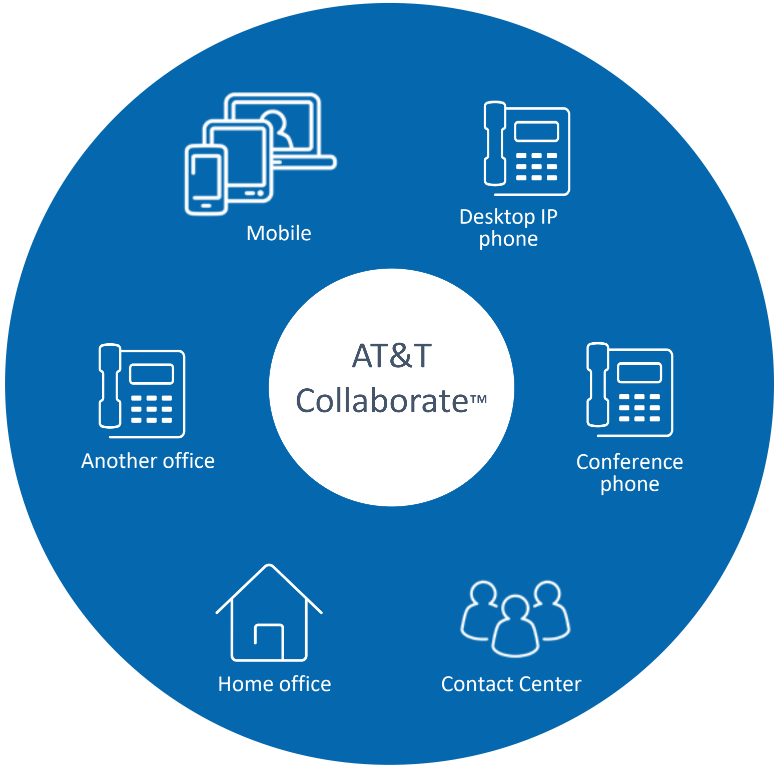
June 2019

AT&T Business

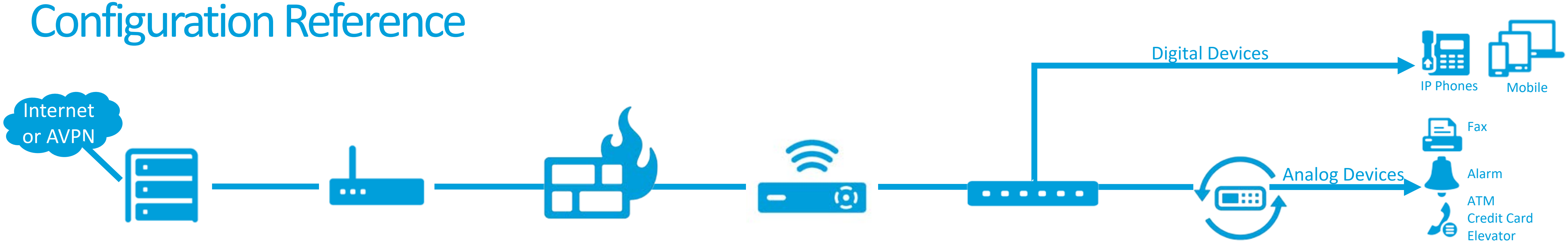
Content

Welcome to the AT&T Collaborate Service, this guide will cover the site configurations that need to be configured to work with AT&T Collaborate to deliver quality voice calls.

1. Access connection
2. Routers and Firewalls
3. Voice Prioritization and Local Area Network (LAN) switches
4. End user devices



Configuration Reference



Access	Router	Firewall	Voice Prioritization	LAN Switch	Analog Terminal Adaptors (ATAs)	End Devices
Adequate internet/ AVPN (AT&T Virtual Private Network) ***bandwidth*** is needed to support the number of simultaneous calls	Router needs to be configured to allow ***appropriate routes*** to communicate with AT&T Collaborate	Firewall needs to be ***configured*** to work with AT&T Collaborate and Network Assessment Tool (NAT)	Check if there is voice prioritization on the transport service. Voice Prioritization Device* can be added to offer ***better quality***	Ensure the network has adequate: ***1) LAN ports*** for wired devices. ***2) Bandwidth and coverage*** for wireless devices.	***ATAs* are required*** for AT&T Collaborate to use with all analog devices (e.g. fax, elevator, alarm, credit card and ATM lines)	Account for all end user devices* and ensure all are ***compatible*** to use with AT&T Collaborate. (See Certified Equipment List)
1	2	2	3	3	4	4

Additional information can be found in the section listed in this guide.

Note:
*Equipment is available to purchase with AT&T, please see Certified Equipment List
Content is organized according to a sample configuration. Please review all information to ensure requirements are met for your specific configuration.

1 Access Connection

I. Overview

- The customer connects to the service using any internet service provider connection (including internet service provided by AT&T) or AT&T VPN service.
- Adequate Internet/AVPN bandwidth is needed to support the number of simultaneous calls.
- If you're unsure if your network has enough bandwidth, please contact your Sales respective representative for your bandwidth requirements.

II. Network Assessment Tool

- A Network Assessment tool helps to measure the network performance at the customer's site and provides feedback to confirm its network is VoIP ready. It must be run from a personal computer/device connected across the same LAN at the site where the service will be used, (see page 7 & 8 for firewall port configuration).

III. Setup

- In many instances the customer owns and manages the router on their premise used to connect to the facility. Both BGP (Border Gateway Protocol) and static routes can be used to connect the customer managed router.
- Any and all network interfaces for the internet connection will be supported for AT&T Collaborate.

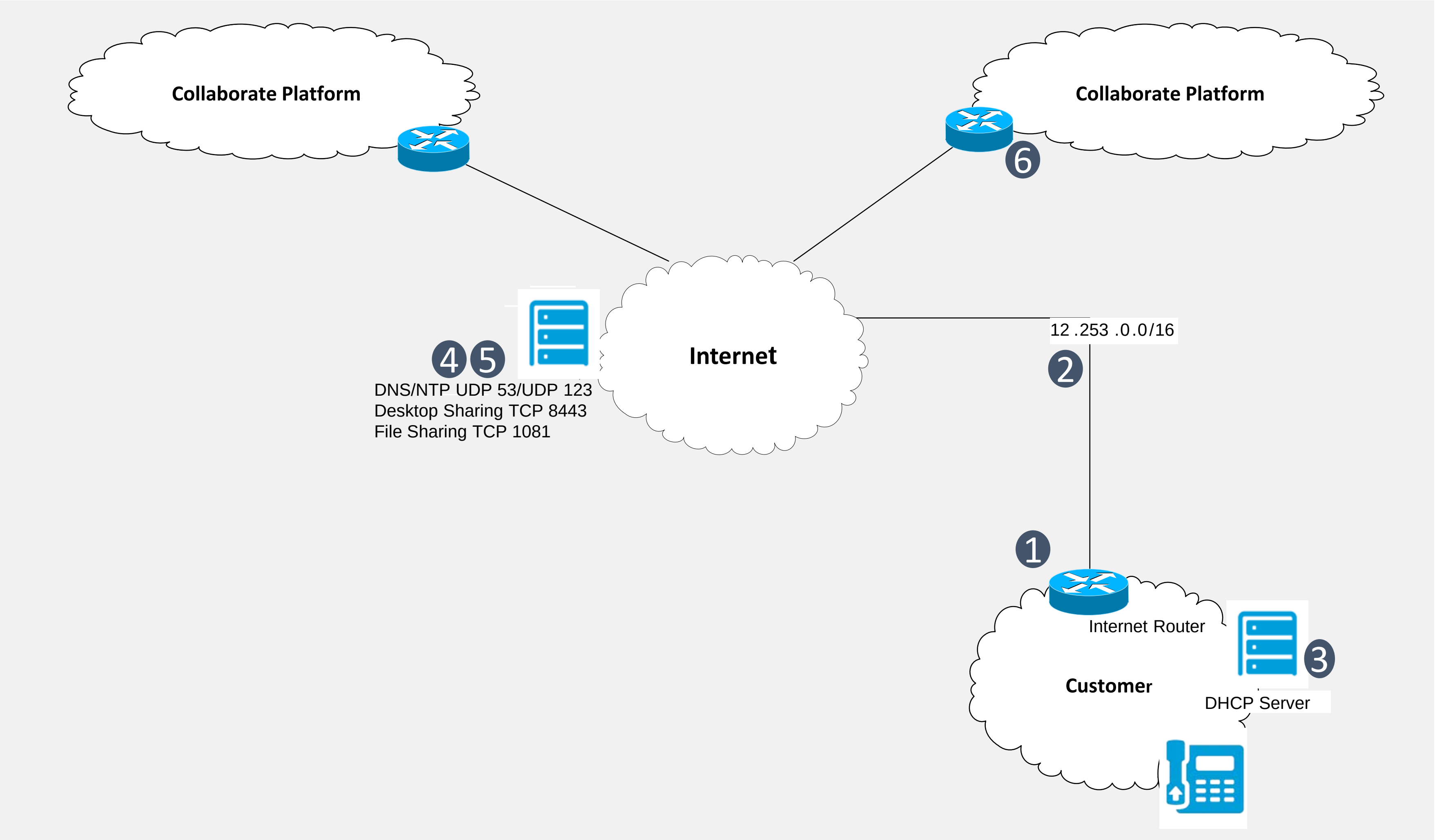
IV. Quality of Service (QoS)

- Class of service is a method to prioritize the VoIP traffic higher than other data. It is recommended for the transport equipment to support Quality of Service (QoS) capabilities for voice traffic since other data traffic may impact the quality of voice calls.
- If the access is AT&T provided, customer will have access to whichever CoS packages/profiles are supported as part of the access service. It is recommended that AT&T Collaborate subscribers utilize multimedia high or multimedia standard packages/profiles. Please contact your respective Sales representative with any questions. An order needs to be issued on the transport service to make appropriate changes.

V. Multiple access connections

If multiple access connections are being used in conjunction with a load balancer, all the VoIP traffic must be sent over a single access connection.

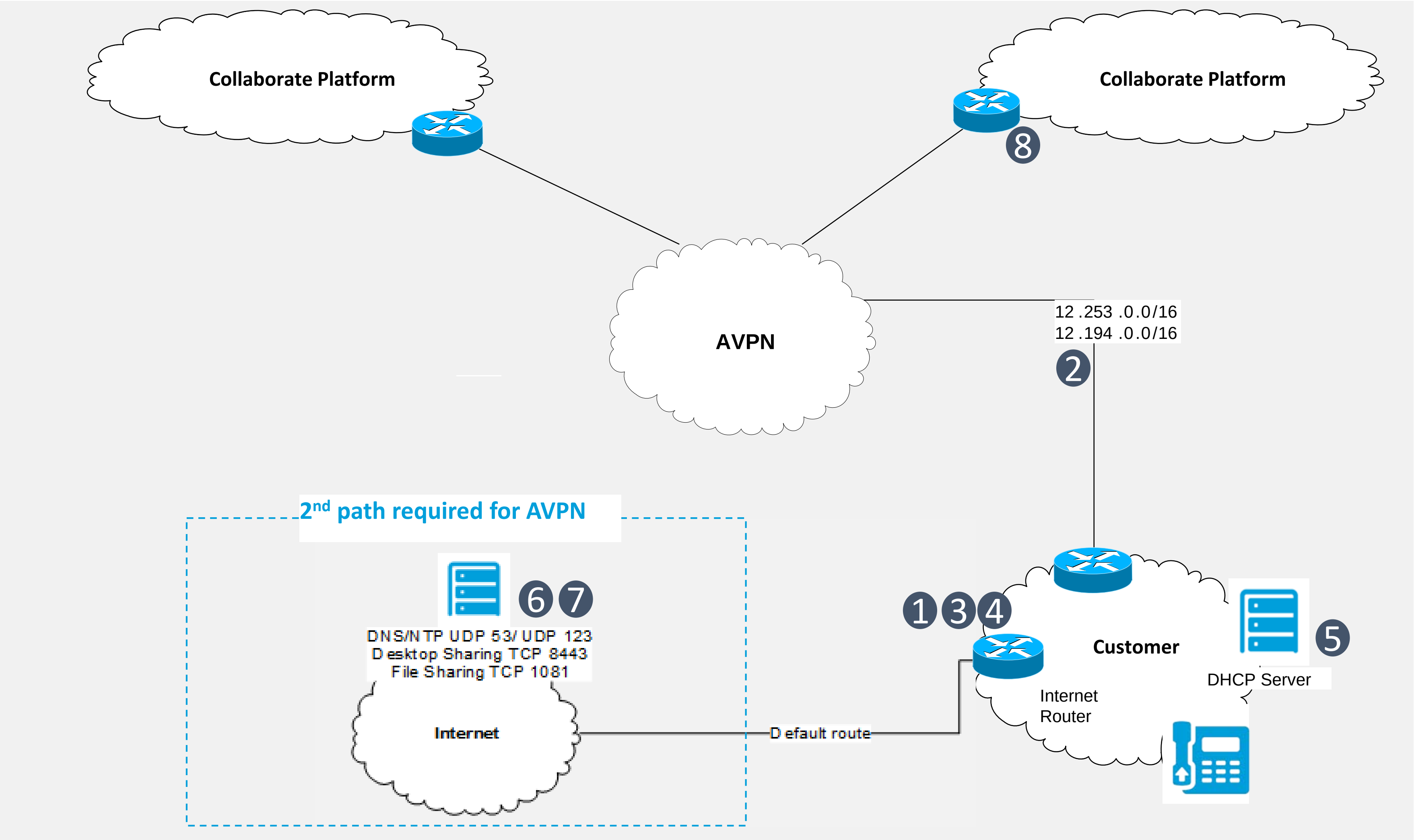
1 Internet Access



Configuration:

1. NAT Tool IP's 144.160.20.0/24 & 144.160.229.0/24
2. Router will provide subnets from within 12.253.0.0/16
3. Onsite DHCP server – Tells phone IP address of DNS and NTP servers
4. Phone queries DNS for Collaborate servers
5. Phone queries NTP server for time sync
6. Phone downloads proper config and registers

1 AT&T Virtual Private Network (AVPN) Access



Configuration:

1. NAT Test Tool IP's 144.160.20.0/24 & 144.160.229.0/24
2. AVPN router will provide six subnets from within 12.253.0.0/16 and 12.194.0.0/16
3. Default route must point to the Internet
4. Desktop sharing and file transfers are routed out to the Internet
5. Onsite DHCP server – Tells phone IP address of DNS and NTP servers
6. Phone queries DNS for Collaborate servers
7. Phone queries NTP server for time sync
8. Phone downloads proper config and registers

2 Routers and Firewalls

I. Overview

- A firewall is a necessary element for general network security and to avoid potential interference with the Collaborate service by only allowing SIP traffic from the AT&T elements that the customer initiated communication with. However, it is possible that there may be firewalls or other local area configuration parameters that will interfere with connectivity to the AT&T network.

  ⚠ In general, to avoid several potential issues it is highly recommended that the secure communications option (TLS/SRTP) be set in the Administrator Portal for any devices that support it.
- Refer to Appendix 1 for information on how to configure an AT&T Digital Internet (ADI) router with Collaborate service.
- The secure communications option must be used in cases where an ADI router is used.
- The only exceptions to enabling TLS/SRTP is that these protocols cannot be used with customers implementing the voice survivability option using EdgeMarc devices for a specific location or customers using AVPN transport.
- Your firewall should be configured with:
  - Stateful packet inspection enabled. Your router must allow inbound SIP signaling only from the AT&T Session Border Controllers to which it is registers
  - Configure a strong administrator password and disable remote access (should apply to firewalls and routers)

II. Criteria

- If the secure communications option is not used for all devices, then the following criteria must be met for the service to work properly.
  - The SIP ALG (Application Layer Gateway) must be disabled.
  - The UDP timeout must be set to greater than 180 seconds.
  - Fragmentation Support – The local network service provider and customer equipment must support the fragmentation requirements below.
    1. For outgoing packets from a phone where the payload is greater than 1450 bytes, fragment the packet to something smaller than 1450 in each packet's payload.
    2. For fragmented packets incoming to the CPE, accept packets with payloads of 1450 bytes or less.
- If the customer desires to limit the outgoing traffic to the specific destinations required for AT&T Collaborate, the rules can be set up with the source address as "inside" and the destination IPV4 addresses as:
  - 12.253.0.0/16
  - 12.194.0.0/16 (for AVPN access only)
  - 144.160.20.0/24 (for the Network Assessment Tool)
  - 144.160.229.0/24 (for the Network Assessment Tool)

III. Rules or Access-Lists

If there is an access-list used on the internet serial interface of the customer managed router, then allow the ports used for signaling and voice payload protocols that are shown in the table on page 8.

2 Routers and Firewalls

- For reference, the following table provides details of the signaling and voice payload protocols that will be used for the Collaborate service. If restrictive security policies are in place, these must be allowed in the firewall rules.
- For specific information, consult your firewall vendor documentation. Additionally, many vendor websites provide easy to follow, step-by-step instructions.

Protocol	Ports
HTTPs/TLS	TCP 443 TCP 7543 TCP 8543 TCP 9543
HTTP	TCP 80
SIP signaling	TCP/UDP 5060 TCP/UDP 5061 TCP/UDP 5075 TCP/UDP 5076
RTP/SRTP media	UDP 16384-49152
NTP	UDP 123
DNS	UDP 53
XMPP (IM&P)	TCP 5222
HTTPS (Sharing)	TCP 8443
BroadWorks Assistant	TCP 2208-2209
XMPP (File Transfer Proxy)	TCP 1081
Network Assessment Testing	TCP/UDP 20000 TCP/UDP 20001 UDP 8090

3 Voice Prioritization and LAN Switches

I. Overview

- Check if voice prioritization is current on transport service. Voice Prioritization Device offers better voice quality.
- Each wired device needs a port. Ensure there are enough LAN ports for all the devices on the Customer site.
- For any devices connecting via wireless connectivity (e.g. Wi-Fi) on the LAN, the Customer or the Customer's LAN Provider has the responsibility to ensure the LAN environment can support the additional load of the voice, video, communication traffic generated by the AT&T Collaborate service along with all other business traffic as this is a shared communication method.
- If AT&T Collaborate service has performance issues due to the LAN infrastructure, it will be Customer's responsibility to resolve these LAN issues directly or with the support of Customer's LAN provider.
- It is Customer's responsibility to ensure the connection is secure if the Customer is using a Wi-Fi / shared connection for any of the AT&T Collaborate traffic.

II. Quality of service (QOS) considerations

- Voice VLANs are recommended for a better customer experience, especially if you have more than 50 devices at the location.
- The voice traffic is competing with other data traffic. In general, most VoIP deployments use some kind of Quality of Service/Class of Service (CoS) methodology to provide priority to the voice traffic over the data traffic. Internet routers (that the Customer equipment connects to) are configured with CoS options to provide priority to the voice signaling and media traffic destined to the CPE.
- The Customer router should be configured to provide 90% of the traffic for real time handling (DSCP markings of 46 for SIP and 46 for RTP packets). AT&T recommends configuring routers and switches to give priority to voice traffic to help ensure a better experience when using AT&T Collaborate. The standard port for SIP is 5060 and RTP ports are 16384-49152. (see the firewall rules for a complete port list).

4 End Users Devices

I. Certified equipment

Certified equipment are available to purchase directly from AT&T, or from other sources. Purchasing from AT&T has the benefit that the device will be pre-configured, where possible. Customer provided equipment must be from the certified list. The list indicates which devices can be purchased from AT&T

II. IP Addressing

Customer accessing AT&T collaborate via the internet must have registered addressing. If end users are using private addressing, the addresses must be NATed to public addresses before the traffic is sent to the AT&T network.

III. DNS (Domain Name System)

Access to a public DNS server is required for devices to work with the AT&T Collaborate service (even if the customer is using AT&T VPN service to reach the service). The SIP phone will be configured with FQDNs (Fully Qualified Domain Names) to access AT&T's network. The SIP phone queries the DNS to resolve the FQDNs to configure their devices and perform registration.

IV. NTP (Network Time Protocol)

Access to an NTP server is required to provide time for the phones. By default the phones will need to reach the Internet (0.us.pool.ntp.org) for time, unless another source is specified via DHCP (Dynamic Host Configuration Protocol) option 42.

V. Phone Configuration

- Phones purchased from AT&T for the AT&T Collaborate service will be pre-configured.
- When the user brings a device not purchased from AT&T or being reused from some other service, the user needs to configure the phone following instructions provided.

VI. Analog Terminal Adaptors (ATA)

ATAs are required for AT&T Collaborate to use with all analog devices (e.g. fax, elevator, alarm, credit card and ATM lines)

VII. DHCP (Dynamic Host Configuration Protocol)

CPE will perform DHCP for the IP phones and data devices on the LAN.

VIII. Codec Selection

The default codec used for all SIP phones on Collaborate is G.722. If bandwidth issues exist, a codec having lower voice quality such as G.729 can be used to reduce bandwidth requirements. This is set per device in the Admin portal.

4 Cisco IP Phone Configuration

NOTE: Only Cisco 3PCC (3rd Party Call Control) models will work on AT&T Collaborate. Look in the Product Information menu of the phone for the **Product name** and **Software version** fields. The **Product name** must show “3PCC” and the **Software version** will need to be 11-x or higher for the device to work on AT&T Collaborate. If these criteria are met, then the instructions below can be used to configure the device to work on AT&T Collaborate. In devices that will not work, under Settings->Phone Information it will show “Model Number” and “Active Load.”

Step I: Reset the phone to factory configuration (only required if phone was previously used for another service)

1. Turn the phone on, but don’t connect it to the network or internet.
2. Press the phone’s **Applications** button (⚙).
3. Scroll to “**Device Administration**” and press “**Select**” soft key.
4. Scroll to “**Factory Reset**” and press “**Select**” soft key.
5. Press “**OK**” soft key.
6. Phone reboots to factory defaults.
7. In “**Set password**” screen, press “**Skip**” soft key.

Step II: Configure the phone

1. Connect the phone to the network.
2. Press the phone’s **Applications** button (⚙).
3. Scroll to “**Device Administration**” and press “**Select**” soft key.
4. Scroll to “**Profile rule**” and press “**Select**” soft key.
5. Enter the value: **https://devicemgt.hcomm.att.net/dms/def/$PSN.xml**
   - Use 1 button to get to characters ‘.’ and ’/’
   - Use # button to get to ‘$’

6.Press “**Resync**” soft key.

- ⚠ Phone may reboot during this resync process.

4 Polycom IP Phone Configuration

Note that SoundPoint and SoundStation phones can only be used on Collaborate if they have manufacturer signed security certificates (2010 or newer phones). This can be checked via the phone menu by selecting Menu->Status->Platform and then scrolling down. Usable phones will show - **Device Certificate: Factory Installed**

Step I: Reset the phone to factory configuration (only required if phone was previously used for another service) . Note that if the SoundPoint /Soundstation phone is not up to firmware level UCS 4.0 or if the Admin password is unknown, the special instructions in page 13 must be used.

1. Turn the phone on, but don't connect it to the network or Internet.
2. Press the phone's **Menu** button.
3. Scroll to **Settings**, and then press the **Select** soft key.
4. Scroll to **Advanced**, and then press the **Select** soft key.
5. Enter the administrator password (default **456**), then press the **Enter** soft key.
6. When **Admin Settings** appears, press the **Select** soft key.
7. Scroll to **Reset to Defaults**, and then press the Select soft key.
8. Scroll to **Reset to Factory**, and then press the Select soft key.
9. Press the Yes soft key.

Step II: Set up the phone for configuration DHCP Options

1. Turn the phone on, but don't connect it to the network or Internet.
2. Press the phone's **Menu** button.
3. Scroll to **Settings**, and then press the **Select** soft key.
4. Scroll to **Advanced**, and then press the **Select** soft key.
5. Enter the administrator password (default **456**), then press the **Enter** soft key.
6. When **Admin Settings** appears, press the **Select** soft key.
7. When **Network Configuration** appears, press the **Select** soft key.
8. When **Prov. Server** appears, press the **Select** soft key.
9. When **DHCP Menu** appears, press the **Select** soft key.
10. Scroll to **Boot Server**, and then press the **Edit** soft key.
11. Change to **Static**. Scroll through the options by pressing the **<** or **>** buttons (on phone models without these, press the up or down arrow keys or press the **Change** soft key). When **Static** appears in the **Boot Server** field, press the **OK** soft key.
12. Press the **Exit** or **Back** soft key to return to **Prov. Server** menu.

Step III: Complete the process

1. Scroll to **Server Type**, and then press the **Edit** soft key.
2. Scroll through the protocol options and select **HTTPS**, and then press the **OK** soft key. To locate **HTTPS**, press the **<** or **>** buttons (on phone models without these, press the up or down arrow keys or the **Change** soft key).
3. Scroll to **Server Address**, and then press the **Edit** soft key.
4. Enter this value: **https://devicemgt.hcomm.att.net/dms/def**

- Note that characters you enter overwrite existing characters.
- Verify that the mode shown on the screen is **a**. If not, press the **Edit** soft key and select **a**.
- Enter a period (**.**) or colon (:) by pressing the star (*****) or pound (#) key.
- Enter a slash (**/**) by pressing the pound (**#**) key until the slash (**/**) appears.
- Backspace is the **x** key or the **<<** softkey depending on model.

4 Polycom IP Phone Configuration

Step III: Complete the process (continues)

5. When you've entered the correct value (shown in step 4), press the **OK** soft key.

6. Scroll to **Tag SN to UA**, and change the value to **Enabled,** if not already set to that value (this ensures the MAC address of the device is sent to enable retrieval of configuration files).

7. Press the **Exit** or **Back** soft key to return to the **Network Configuration** menu.

8. Press the **Exit** or **Back** soft key to return to the **Network Admin Settings** menu.

9. Connect the phone to the network.

10. To save your changes, scroll to **Save Config**, and then press the **Select** soft key. To discard your changes, select **exit without saving**. Note that you must save or your changes will be lost. Also note that the wording of these choices may vary on different models.

11. The phone automatically reboots several times. Be patient. The phone may sit without any indication of activity for one or two minutes between reboots

12. f the phone is not working properly, may need to reboot several times.

If the SoundPoint/SoundStation device is on a firmware version lower than UCS 4.0, then follow the steps given on Step I & II (page 12) and use step III shown below.

Step III

1. Scroll to **Server Type**, and then press the **Edit** soft key.

2. Scroll through the protocol options and select **HTTP**, and then press the **OK** soft key. To locate **HTTP**, press the **<** or **>** buttons (on phone models without these, press the up or down arrow keys or the **Change** soft key).

3. Scroll to **Server Address**, and then press the **Edit** soft key.

4. **Enter this value: http://upgrade.hcomm.att.net**
   - Note that characters you enter overwrite existing characters.
   - Verify that the mode shown on the screen is **a**. If not, press the **Edit** soft key and select **a**.
   - Enter a period (**.**) by pressing the star (*****) key.
   - Enter a slash (**/**) by pressing the pound (**#**) key until the slash (**/**) appears.

5. When you've entered the correct value (shown in step 4), press the **OK** soft key.

6. Scroll to **Tag SN to UA**, and change the value to **Enabled,** if not already set to that value (this ensures the MAC address of the device is sent to enable retrieval of configuration files).

7. Press the **Exit** or **Back** soft key to return to the **Network Configuration** menu

4 Polycom IP Phone Configuration

8. Press the **Exit** or **Back** soft key to return to the **Network Admin Settings** menu.

9. Connect the phone to the network.

10. To save your changes, scroll to **Save Config**, and then press the **Select** soft key. To discard your changes, select **exit without saving**. Note that you must save or your changes will be lost. Also note that the wording of these choices may vary on different models.

- The phone automatically reboots several times. Be patient. The phone may sit without any indication of activity for one or two minutes between reboots
- If the phone is not working properly, may need to reboot several times.

⚠ If for some reason the server in step 4 is inaccessible, then a process with an extra step is required.

1. Use http://sildevicemgt.hcomm.att.net/dms/def in Step III, 4 (page 13).

2. After that download completes, then follow steps II and III (page 12, 13.) Change the protocol to https and using the server address provided in steps II and III.

Password Reset

To reset the Administrator Password for a Polycom VOIP Phone, please do the following:

Reboot the phone to get the countdown screen then use step 1 below. Note: If the phone is running 3.30 or above, press cancel to get the phone to the countdown screen.

1.On boot up during the initial countdown sequence, press and hold 4, 6, 8,* on the dial pad

a) Note: On the IP6000 phone only press and hold 6, 8, * on the dial pad

b) Note: On the IP3xx, IP450, and IP7000 phones only press and hold 1, 3, 5, 7 on the dial pad

c) Note: On the VVX3xx, VVX4xx, VVX500, and VVX600, press and hold 1, 3, 5 on the dial pad

2. Once this command is accepted the phone will ask for an admin password

3. Use the phone's MAC address as the admin password using lower case for any letters in the MAC address (No colons and the alpha characters must be entered as lowercase letters)

4. The phone will now reboot.

4 Yealink IP Phone Configuration

Step I: Reset the phone to factory configuration (only required if phone was previously used for another service)

T40P/T42S/T58V

1. Turn the phone on.
2. Press the phone's **Menu** soft key.
3. Scroll to **Settings**, and then press the **Enter** soft key.
4. Scroll to **Advanced Settings**, and then press the **Enter** soft key.
5. Enter the administrator password (default **admin**), and then press the **OK** soft key.
6. Scroll to **Reset Config**, and then press the **Enter** soft key.
7. Scroll to **Reset to Factory**, and then press the **Enter** soft key.
8. Press the **OK** soft key.
9. The phone immediately resets to factory defaults and the phone reboots.

T46G/T46S

1. Turn the phone on.
2. Press the phone's **Menu** soft key.
3. Scroll to **Advanced**, and then press the **Enter** soft key.
4. Enter the administrator password (default **admin**), and then press the **OK** soft key.
5. Scroll to **Reset Config**, and then press the **Enter** soft key.
6. Scroll to **Reset to Factory**, and then press the **Reset** soft key.
7. Press the **OK** soft key.
8. The phone immediately resets to factory defaults and the phone reboots.

W56P

1. Turn the phone on with handset connected with base station.
2. Press handset's **OK** button.
3. Scroll to **Settings** and then press the **OK** button.
4. Scroll to **System Settings**, and then press the **OK** button.
5. Scroll to **Base Reset**, and then press the **OK** button.
6. Enter the PIN code(default **0000**), and then press the **OK** button.
7. The base immediately resets to factory defaults and the base reboots.

Step II: Configure the phone

T46G/T40P/T46S/T42S/T58V

1. Enter the Administrator password (default **Admin**) as shown on the left side of this slide and then press the **OK** soft key.
2. Scroll to **Auto Provision** and then press the **Enter** soft key.
3. Scroll to **URL** and enter this value: **https://devicemgt.hcomm.att.net/dms/def**
   - Verify that the mode shown on the screen is **abc**. If not, press the second soft key until it appears.
   - Enter a period (**.**) or slash (**/**) by pressing the star (*****) key until it appears.
4. When you've entered the correct value (shown in step 3), press the **Save** soft key.
5. Press **OK** soft key.

4 Yealink IP phone Configuration

Step II: Configure the phone (continued…)

W56P

1. Wait for Base unit to finish initializing (3 green lights). Press handset's **OK** button.

2. Scroll to **Status** and then press the **OK** button.

3. Scroll to **Base** and the press the **OK** button.

4. Make a note of the IP address shown on **IPv4** section.

5. Access the Web interface of the phones from a PC via http://(IP address shown in step 4).

6. Enter the administrator username/password (default admin/admin), and then click **Confirm**.

7. Go to **Settings->Auto Provision** menu.

8. Enter this value: **https://devicemgt.hcomm.att.net/dms/def** in **Server URL** text box.

9. Click **Confirm** button at the bottom of the page.

10. Click **Autoprovision Now** button at the bottom of the page and then click **OK** button.

Appendix

Appendix 1 - Cisco router configuration example for ADI router

The following ADI router has been tested with AT&T Collaborate: Cisco 3945E/K9

The Customer may require that the ADI router to support a new or existing LAN interface and also may also require the ADI router to support DHCP Server configuration. The following example is for LAN DHCP Server scope on the ADI router, the Collaborate IP Phones will connect on the same LAN interface and ip subnet on the ADI router. In this example the IP phones will be assigned 10.128.X.X/ ip address range and the ADI router LAN interface/subinterface will be assigned 10.128.1.1/24 as the default-router in the DHCP scope.

Router configuration:

```
ip dhcp pool NET10_Collaborate_IP_Phones
network 10.128.1.0 255.255.255.0
default-router 10.128.1.1
option 42 ip X.X.X.X  = NTP server IP address
dns-server Z.Z.Z.Z
```

The Collaborate services requires the use of public ip addresses, the following example shows how to configure the ADI router to translate the Customer’s private LAN interface to the public WAN interface ip address PAT example

```
ip access-list extended LAN
 permit ip 10.128.0.0 0.0.0.15 any

Int S0/0/0
  ip nat outside
Int gi0/0
 ip nat inside

Ip access-list extended LAN
 permit ip 10.128.0.0 0.0.0.15 any
ip nat inside source list LAN interface Serial0/0/0 overload
```

Access control list:

Outbound ACL Update if needed

```
  Permit ip any 12.253.0.0 0.0.255.255 < Collaborate SBG Subnet >
```

Inbound ACL

```
  Permit ip 12.253.0.0 0.0.255.255 any
  permit tcp any established
  permit udp host X.X.X.X any eq 123
  permit udp host Z.Z.Z.Z any eq 53
```

Appendix 1 - Cisco router configuration example for ADI router (continued)

Based on the specific COS configuration supported on the ADI router either the named or numbered ACLs must be updated to include the Customer's Collaborate IP Phone subnet and the Collaborate SBG to classify all voice and signaling traffic with DSCP marking EF. The Collaborate IP Phone subnet address should be used in the access-list for media. Following is an example numbered access-list for RTP media for Collaborate IP Phones with COS1 profile.

Router configuration:

```
class-map match-any COS1_TRAFFIC
  description Real-Time traffic
 match access-group 181
 match access-group 185
 match ip dscp ef

access-list 181 permit udp host 12.253.0.0 any range 16384 32767
```

Collaborate requires Encrypted signaling and uses Transmission Control Protocol **(TCP)** on port **5061** rather than User Datagram Protocol (UDP) on port 5060. Therefore, the COS1 configuration ACL need to be adjusted to correctly place SIP signaling in COS1.

The following example changes are required for access-list 185.

```
access-list 185 permit tcp host 12.253.0.0 any eq 5061
```

** Any access-list 185 statements for port 5060 can be removed **only** after all of the Customer's IP FlexReach TNs have been migrated to the Collaborate service.

AT&T Business