Customer Owned Switch Requirements for ProConnect

Summary

This document outlines the requirements for providing Consolidated's ProConnect service using a customer provided switching infrastructure. The requirements listed below should be considered minimum requirements to deliver ProConnect services over customer equipment.

Customer agrees that it is responsible for the installation, management and troubleshooting of the customer provided LAN switch used for ProConnect service.

ProConnect voice traffic (phones and other devices) must connect through a voice VLAN. The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. When the switch is connected to an IP phone, the phone sends voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values.

Switch Requirements

The customer's network must fully meet all LAN requirements. Individual requirements are outlined below:

- The customer's existing switching infrastructure must support:
  - Power over Ethernet (802.11af), ensuring the switch has sufficient power for all connected devices.
    - *PoE is preferred. Power bricks may be used with the phones in lieu of PoE switches.*
  - VLANs and VLAN Trunking (802.1q – Voice LANs)
  - Ethernet Quality of Service (802.1p)
  - Link Layer Discovery Protocol – Media Endpoint (LLDP-MED) (802.1AB)
- The customer must implement Consolidated's Voice VLAN across all switches (Consolidated recommends standardizing on VLAN 46).
- The customer must hand VoIP and public data to Consolidated's equipment over an 802.1q trunk interface.
- Consolidated recommends all Voice VLAN traffic is prioritized over all other LAN traffic. The customer must provide LLDP-MED for the Voice VLAN.
- **The customer must identify and make the changes to their switching infrastructure to support all items above or identify an external contact who will do so at the customer's expense.**

LAN Addressing Requirements

- Preferred network: 192.168.0.0 /24
- Standard exclusions: 192.168.0.0 thru 192.168.0.20
  192.168.0.230 thru 192.168.0.255 (this upper exclusion is what Consolidated uses for its switch management)
  Option would be to use a 10.x.x.x network to prevent overlap within an existing network.
- Requirements for the port facing the Consolidated SBC (generally an Adtran device):
  - Switch port Mode: Access
  - Switch port access VLAN is the same as the global voice VLAN (i.e. VLAN 46)
  - Some switches will also require that the native VLAN be the same as the access/voice VLAN on this port also (this appears to be a requirement on Cisco switches).
  - Some switches require that the voice VLAN also be an explicitly called out 'allowed' VLAN.

LAN Cabling Requirements

- Must meet 100BASE-TX standards.
  - (e.g.) Cabling must be copper and must be category 5 or better.
- All cables must be properly terminated to RJ-45 connectors.
- Cables must run directly from the receiving Ethernet jack to the switch/telephony closet without splices and without passing through another hub, switch, or repeater.
- Ethernet wiring must be separated from sources of EMI (electromagnetic interference).
  - (e.g.) It should not run parallel to electrical wiring, should not cross florescent light fixtures or air conditioning units.
- All cables must have both endpoints identified and labeled.
  - (e.g.) Ethernet jacks must be labeled and have a corresponding label on the cable or patch panel in the switch room/telephony closet.
- All cabling must be indoors or properly shielded in a conduit.
- No Ethernet cable should be longer than 100 meters (328.1 feet) in length.

ProConnect remote site installations

"BYOB" – Bring your own Bandwidth

Consolidated's ProConnect service is a managed hosted voice solution that requires Consolidated to have access to the customer's hosted phones and voice switches (where appropriate) for troubleshooting and support. To have access to the hosted phones and switches, Consolidated will place an Adtran edge Session Border Controller (eSBC) at the customer's location at Consolidated's expense. The customer must provide rack space and power for the eSBC. See below for details.

ProConnect remote site (BYOB) phone install minimum configuration requirements:

- **There cannot be a firewall between the telephone's voice traffic and the internet.** The Consolidated edge session border controller (eSBC) will act as the voice firewall and is configured to allow for VoIP traffic.
    - Separate VLANs should be configured on the customer's LAN for VoIP and internet traffic. The VoIP traffic must bypass the customers firewall and route directly to Consolidated's eSBC.
    - **SIP ALG** must be **disabled** on the customer's LAN and internet provider's router for the VoIP traffic. *Failure to disable SIP ALG will result in phantom calls.*
    - Hosted phones require the following destination ports:
        - TCP/443 for configuration management, directory searches and XSI commands.
        - UDP/TCP Port 53 for DNS queries
        - UDP/5060 for SIP Signaling
        - UDP/10000 thru 41999 for RTP for physical phones
        - UDP/8000-8099 for Audio RTP and 8100-8199 for Video RTP if using Webex
    - If no eSBC is installed (Single office / home office only – maximum of 2 phones), phones must be configured by Consolidated to utilize zero touch provisioning (ZTP) and cannot be configured on the local switching LAN to using any DHCP Options as this will conflict with ZTP.
        - Polycom – Option 66
        - Cisco – Option 150 or Option 66
- Sufficient bandwidth must be provided downstream and upstream for the voice traffic. VoIP traffic must be prioritized appropriately. Typically, a minimum of 100 kbps should be allocated per voice call path for phones without video. 612 kbps is recommended when using video with the Poly or Cisco phones. A dedicated voice circuit is strongly recommended.
- Phones must be connected to the network LAN switches via RJ45 Cat5 connections. If using a Poly or Cisco phone on Wi-Fi connections, it is the customer's responsibility to configure the Wi-Fi. Consolidated will not support Wi-Fi connections unless Consolidated is also providing the Wi-Fi service.
- Switches must be able to provide PoE with sufficient power (dependent on the phone model) for the phones or an external power supply (not PoE) must be used to power the phones.

SIP Trunking & IP-PRI remote site (BYOB) installations

Consolidated's SIP Trunking and IP PRI service is a managed hosted voice solution that requires Consolidated to have access to the customer's network equipment (where appropriate) for troubleshooting and support. To have access to the equipment, Consolidated may place an edge Session Border Controller (eSBC) at the customer's location at Consolidated's expense. The customer must provide rack space and power for the eSBC. See below for details.

SIP Trunking or IP PRI remote site (BYOB) install minimum configuration requirements:

- Off-network platforms are supported best effort. Consolidated cannot guarantee that there will be VoIP QoS on another provider's internet connection.
- **There cannot be a firewall between the telephone's voice traffic and the internet.** The Consolidated edge session border controller (eSBC) will act as the voice firewall and is configured to allow for VoIP traffic.
    - Separate VLANs should be configured on the customer's LAN for VoIP and internet traffic. The VoIP traffic must bypass the customers firewall and route directly to Consolidated's eSBC.
    - **SIP ALG** must be **disabled** on the customer's LAN and provider's router for the VoIP traffic. *Failure to disable SIP ALG will result in phantom calls.*
- Sufficient bandwidth must be provided downstream and upstream for the voice traffic. VoIP traffic must be prioritized appropriately. Typically, a minimum of 100 kbps should be allocated per voice call path. A dedicated voice circuit is strongly recommended.

Internet Connectivity Requirements

ProConnect, SIP, or IP-PRI BYOB

Consolidated may place an edge Session Border Controller (eSBC) at the customer's premises.

- A dedicated voice circuit with NO data traffic is recommended for the best voice quality. A dedicated voice circuit eliminates the potential of data traffic overusing the bandwidth capacity.
- Customer to provide space and power for the eSBC at no charge to Consolidated.
- Customer to provide Consolidated with a **public facing static IP** for the eSBC to connect to the internet.
- The eSBC must connect to the customer's internet circuit directly and not pass through a firewall.
- Customers must ensure that **SIP ALG** is **disabled** in the firewall, router, and PCs for the network that carries the data or voice traffic.

Off-network phones, platforms, or switches are supported on a "best efforts" basis. Consolidated cannot guarantee that phones will register or there will be VoIP QoS on another provider's internet connection. Failure to place the Consolidated eSBC at the customer site will limit, and may preclude, Consolidated's ability to troubleshoot any voice quality issues. As such, there will be no service quality guarantees without an eSBC.

Customer Vendor Requirement

- **Consolidated will not provide management of customer owned equipment**. Customer must provide IT Staff or Data Vendor who can configure and maintain their equipment.
- **The IT Staff or Data Vendor must be available during service cutover**.

Consolidated will not configure customer owned equipment or LAN. For customer owned networks, Consolidated recommends using a networking specialist, an internal resource, value added reseller, or IT vendor who can understand and configure the LAN for VoIP applications.

Webex Desktop & Mobile Clients

The Webex Desktop and Mobile[1] (iPhone and Android) applications utilize the customer's data network. The following configuration settings must be made within the customer's data firewall. If the firewall is filtering on domain, the **voicecci.net** and **consolidated.net** domains must be whitelisted.

For Device Management, XSI, etc., Webex clients need to reach the following on the Consolidated network:

TCP 443	xsp.consolidated.net	209.107.242.177
		64.126.0.98
	xsp-w4b.consolidated.net	72.251.167.3

For Webex softphone services, the following IPs and ports must be opened in the firewall:

State	SIP	RTP
CA	66.60.166.11 UDP/5060, TCP/5075	66.60.166.10 UDP/10000 to 41999
IL	208.124.104.235 UDP/5060, TCP/5075	208.124.104.234 UDP/10000 to 41999
ME	71.161.127.203 UDP/5060, TCP/5075	71.161.127.202 UDP/10000 to 41999
MN	216.70.4.24 UDP/5060, TCP/5075	216.70.4.23 UDP/10000 to 41999
PA	209.195.142.11 UDP/5060, TCP/5075	209.195.142.10 UDP/10000 to 41999
TX	207.70.173.248 UDP/5060, TCP/5075	207.70.173.247 UDP/10000 to 41999

In addition to the settings above, Cisco provides additional details on configuring the local network for two-way voice calls to be successful.

https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Services

[1] ***Note**: **The Webex soft client for tablets (Android and iPad) only supports VoIP voice calls. Cellular voice calls are not available on tablet devices.***

Teams Desktop & Mobile Clients

The Teams Desktop and Mobile[2] (iPhone and Android) applications will utilize the customer's data network; therefore, the following configuration settings must be made within the customer's data firewall. If the firewall is filtering on domain, the **voicecci.net** and **consolidated.net** domains must be whitelisted.

For Device Management, XSI, etc., Teams clients need to reach the following on the Consolidated network:

TCP 443	xsp.consolidated.net	209.107.242.177
		64.126.0.98
	xsp-w4b.consolidated.net	72.251.167.3

For Teams softphone services, the following IPs and ports must be opened in the firewall:

State	SIP	RTP
CA	66.60.166.11 UDP/5060, TCP/5075	66.60.166.10 UDP/10000 to 41999
IL	208.124.104.235 UDP/5060, TCP/5075	208.124.104.234 UDP/10000 to 41999
ME	71.161.127.203 UDP/5060, TCP/5075	71.161.127.202 UDP/10000 to 41999
MN	216.70.4.24 UDP/5060, TCP/5075	216.70.4.23 UDP/10000 to 41999
PA	209.195.142.11 UDP/5060, TCP/5075	209.195.142.10 UDP/10000 to 41999
TX	207.70.173.248 UDP/5060, TCP/5075	207.70.173.247 UDP/10000 to 41999

In addition to the settings above, Microsoft provides additional details on configuring the local network in order for two-way voice calls to be successful.

https://learn.microsoft.com/en-us/microsoftteams/business-voice/get-ready-internet

[2] ***Note**: **The Teams softclient for tablets (Android and iPad) only supports VoIP voice calls. Cellular voice calls are not available on tablet devices.***