UCx Local Area Network (LAN) Deployment Guide

Introduction

The installation of your new UCx service will go more smoothly if you have a solid knowledge and understanding of your IP infrastructure. To ensure a successful UCx deployment, you must inspect and properly configure each network service and component which makes up your Local Area Network (LAN). This guide will help you, the network administrator, to identify those network services and components which you should consider.

Top 10 UCx Deployment Challenges

Although the majority of our UCx installations are uneventful, sometimes unforeseen problems can arise. Here is a "Top 10" list of the challenges our customers may face during a UCx deployment. This short list illustrates how important it is for you to review your network topology. Throughout this guide, you'll learn how to set up your network to keep these problems from impacting your UCx service.

#	**Problem**	**Symptom**
10	Incorrect firewall settings	One-way audio
9	DHCP address pool exhausted	Unable to obtain an IP address
8	Uncertified Cat5 cable	Static heard on calls
7	Un-terminated Cat5 network jack	Unable to plug in phone
6	Incorrect QOS settings	Garbled voice during large downloads
5	Firewall license restrictions	Unable to place call or register
4	IP address conflict	DHCP address statically configured on PC
3	Incorrect amplified headset settings	Static/echo heard on all calls
2	Incorrect FTP server settings	Failure to register
1	Speed/Duplex mismatches	Voice audio fades in/out

IP Addressing

UCx phones are nothing more than specialized computers which process analog speech to Voice over IP (VoIP). A UCx phone deployment of 30 phones is similar to deploying 30 additional computers on your network: each UCx device requires an IP address. By default, UCx phones will request an IP address assignment using DHCP.

DHCP

Most of our customers use DHCP to assign IP addresses to their UCx phones. The phone will request a DHCP lease upon boot-up and will follow the lease timeout set by the DHCP server. The UCx phones require a minimum DHCP configuration to operate normally. The following are required to provide the phones with a working network configuration:

Option 3 – Router
Option 4 – Time Server
Option 5 – DNS Servers
Option 15 – DNS Domain Name

DHCP Reservations

You may statically assign IP addresses to each UCx phone by using a DHCP reservation. This is a good idea if you want to assign all VoIP devices specific IP addresses of the DHCP scope (192.168.1.0/24 is the DHCP scope, but 192.168.1.128-196 contains the DHCP reservations for all VoIP devices). You can

configure DHCP reservations on your DHCP server by assigning an IP address within the DHCP scope to the MAC address of the phone. The MAC address of a UCx phone is also the serial number.

Statically Assigned IP Address
If you cannot support IP address assignment via DHCP, you have the option to statically assign IP address information on each UCx phone. If you need to take this route, please contact us to request an instructional guide.

Option 66 – Boot Server
If you use Option 66 or "Boot Server" on your network, you'll need a special configuration on each phone to ignore this DHCP option. Our customers typically use Option 66 when they have thin clients or WYSE terminals deployed on their network. Option 66 is used to identify a server which DHCP clients can obtain configuration and/or application information from. By default, UCx phones will attempt to use the Option 66 Boot Server; this will cause the phones to fail their initial setup. If you use Option 66, notify your Account Executive during the ordering process so the phones will be configured to disregard the Option 66 setting.

DNS
Today's network devices and phones are configured with an FQDN address, instead of an IP address, which identifies who the device should communicate with. DNS is used to resolve these FQDNs to IP addresses (sometimes more than one) to provide failover functionality in the event of an outage. You are required to provide your phones with adequate resources to resolve DNS in a timely fashion. Two DNS servers should be provided through the use of DHCP.

LAN Cabling
You should ensure your network is wired with at least certified Cat5 wiring and adaptors. Cat5 terminations (4 pairs) is the minimum required to support Power over Ethernet (PoE). Some legacy networks are wired with Cat3 (2 pair), which will support a 10BaseT and possibly VoIP at 10MB, but will not support PoE or speeds greater than 10MB. Each UCx phone location must have a readily accessible network jack to accept an RJ-45 male adaptor.

A Gigabit speed network will require at least Cat5E wiring and adaptors. Cat6 wiring is required for 10GIG networks and greater.

Configuration Management
We have deployed two different platforms to manage device configuration: DMS and FTP. DMS is used for all new UCx customers moving forward. FTP is used by existing UCx customers who have not yet converted to DMS.

UCx phones are required to access our configuration management servers periodically. During the startup process, the phones will download configurations and software. Going forward, the phones will periodically upload log files used to assist in troubleshooting. The phones will also push localized changes made by the end user.

If Internet access will not be available to the phones from your network, you must notify your Account Executive during the ordering process to identify the network limitations. A secured gateway IP address may be configured to allow the phones to access the public server through an MPLS WAN IP address.

DMS Server
We use a new secured public DMS set of servers which supports HTTP/HTTPS/TFTP/FTP protocols. The protocol used depends on the device and how it is configured to access the server. During the

shipping process, UCx phones are programmed and tested to access DMS to retrieve their configurations.

Each phone on your network must be able to HTTP/HTTPS file transfer (TCP/80 & TCP/443) with voice.dsci-net.com and voice2.dsci-net.com; each FQND can resolve to multiple servers. If you use our MPLS product, you should make arrangements to ensure the phones are not restricted from accessing the HTTP/HTTPS servers using your Internet gateway.

FTP Server

We use a secured public FTP server to maintain UCx configuration files. Each phone is provisioned to login to the FTP server using a username and password which is unique to your company. Once logged into the FTP server, the phone will have access to download newer software, applications, and configuration files. The phone also uses the FTP server to upload user customizations and log files to assist with troubleshooting.

Each phone on your network must be able to FTP file transfer (TCP/20 & TCP/21) with ftp.dsci-net.com. If you use our MPLS product, you should make arrangements to ensure the phones are not restricted from accessing the FTP server using your Internet gateway.

Powering Phones

Each UCx phone is powered using one of two methods: with an AC power supply, or through a Power over Ethernet (PoE) enabled network.

An AC power supply provides the phone with power from a nearby wall outlet. Phones which use a power supply are dependent upon the power supply to operate.

PoE is typically made available to the phone by a PoE enabled network switch or through a PoE injector cable. You may wish to consider the use of PoE to centrally manage the power required to support your UCx deployment.

We highly recommend Uninterrupted Power Supplies (UPS) for all of your network and VoIP devices. UPSs will protect your network investments and provide business continuity during a power outage. In the event of a power outage, distributed PoE devices may be centrally supported by UPS protected PoE network switches. The UPS can be sized to supply power to the network switches and phones throughout the outage. You should verify that your DMARC equipment (firewalls and routers) is also UPS protected.

As each Polycom phone model consumes a different amount of power, you should ensure your PoE enabled switches have the capacity to support the number of phones you wish to deploy. Some switch manufacturers enable PoE on each switch port but restrict the total power available to all ports. Power requirements for Polycom phones are included in Polycom Technical Bulletin TB48152 – Polycom Power Consumption.

Polycom phones support both PoE standards: Cisco and IEEE 802.3af. Optional PoE adaptor cables are required for the Polycom 300/301 and 500/501 phones to use switch-based PoE. Polycom 601 phones are not supported on Cisco switches.

If you would like to deploy ATAs (analog terminal adapters) to support analog phones over a VoIP network, you are required to provide a power source near where the ATA will be placed. Our ATAs do not currently support PoE.

Quality of Service (QoS)

QOS is a feature supported on most managed network switches and routers to ensure priority is given to specific network traffic. For a successful UCx deployment, voice traffic must be identified, classified, and given priority through bottleneck segments.

Polycom UCx phones will mark all VoIP traffic with an IP Precedence bit of 5 by default. All non-VoIP traffic from the phone or from the PC port on the back of the phone will be marked with an IP Precedence bit of 3. You can configure your LAN switches to look at the Precedence bit, and give the highest priority to traffic marked with a 5.

Once network traffic reaches our Managed Router, we will reclassify all traffic based on the destination network. All traffic going to our outbound proxy will be marked with an IP Precedence bit of 5, all other traffic will be marked with a 3.

We use strict priority queuing on our managed routers. This means that traffic marked with a 5 is given the highest priority over a T1, or NxT1 solution across our backbone. Likewise, VoIP traffic destined for your network is reclassified based on the source network. Any traffic originating from our outbound proxy is given strict priority queuing over your T1 or NxT1 solution.

Priority queuing is configured to give up to 85% of the outbound bandwidth to VoIP traffic. If there is limited VoIP traffic at any time, all unused bandwidth is available for normal data traffic. We do not use Committed Access Rate (CAR) or Rate-Limits. These technologies effectively dedicate a portion of bandwidth to a specific traffic type.

Bring Your Own Broadband (BYOB)

If you are “bringing your own” broadband based Internet service, the biggest difference is the availability of QOS. We can apply QOS on both sides to ensure phone calls receive the highest priority over web and email.

Here are some basic command-prompt tests you can perform to help identify bottlenecks which can affect any type of traffic (including VoIP).

Find Local IP Address

Use *ipconfig* to show the network interfaces that have been assigned IP addresses. We recommend that you do all testing from a LAN connection. When in doubt, disable any wireless connections to ensure the rest of the test is accurate.

Ping Local IP Address

Use *ping* to verify IP connectivity to your Local Area Connection. The results of this test should indicate a time of <1ms and no packet loss (“Lost = 0 (0% loss)”). There are a few options to *ping* which you may find to be useful:

Ping -t ipaddress	Continuously ping the host until the user hits CTRL+C
Ping -n NUMBER ipaddress	Ping the host the NUMBER of times or until CTRL+C
Ping -l NUMBER ipaddress	Ping the host with a buffer the size of NUMBER

Ping Default Gateway

Use *ping* on the IP address of the Default Gateway, which can be found in the *ipconfig* command executed above. The Default Gateway is typically a router or firewall used to access the Local Area Network. This tests your connection to the router, and ensures that local wiring is not causing any problems. The results of this test should indicate a time of <1ms and no packet loss.

Trace Route
Use *tracert* to show the network path taken to reach the UCx service. You can test against the following two endpoints: 204.11.148.254 (Charlestown, MA) or 209.104.247.254 (Waltham, MA). The traceroute shows how long it takes to reach each point of the path. Traceroute by default will resolve IP addresses. This is very useful to identify the carriers which the traceroute traverses. If you see a sudden increase in network latency from one hop to another, it most likely indicates a congested network link between two routers.

Ping Path
The *pingpath* tool combines *ping* and *tracert* together, although the output is a little more cumbersome. You can use pingpath to do extended testing, which may show link failures better. You can test against the following two endpoints: 204.11.148.254 (Charlestown, MA) and 209.104.247.254 (Waltham, MA). Reviewing the results should show no packet loss. The final RTT should be less than 100ms to support VoIP. The final number of hops should be less than 25.

We strongly encourage you to run these tests multiple times, during different hours of different days. If there is a particular time you know your network is usually very busy, make sure you run the tests then.

If you have a BYOB connection, you are bound to the configuration requirements within this document. Be aware that there are benefits no longer available to you, as we cannot control QOS and bandwidth dedication over the Internet.

Network Capacity
You should ensure that you will have adequate network capacity to support the number of simultaneous phone calls desired, as well as the bandwidth over your LAN. Capacity is typically only a factor when ordering T1s, but you should also pay attention to the LAN.

Our converged products allow for VoIP and data to traverse a shared T1 configured with QOS. As VoIP and Internet traffic are considered data, T1 channelization is not required, so there is no requirement to isolate 64K channels to data and 64K channels to VoIP.

We have selected G.722 HD as the primary VoIP codec, as it offers high-definition fidelity and consumes 80 kilobits of bandwidth in each direction. Alternatively, when G.722 is not available, the phones can use G.729; this codec offers compression to reduce bandwidth requirements to 40 kilobits of bandwidth in each direction.

If you order a T1 from us which is configured with QOS, you can expect to have 16 G.722 calls, 30 G.729 calls, or 22 G.711 calls simultaneously without degradation.

Depending on the type of traffic which traverses your LAN and the speed of switch interconnections, you should monitor your switch ports to ensure uplink interfaces have enough capacity to support VoIP.

Network Topology
There are a few general rules regarding network topology that you should be aware of. Consider each of these important factors when you are determining if a network is VoIP capable.

Uplink ports are those ports which interconnect network devices together. Uplink ports should always be statically set for speed and duplex to ensure auto negotiation is never a cause of a speed/duplex mismatch. Devices which only support 10baseT are acceptable as long as they can be set for full duplex. Speed/Duplex mismatches account for 90% of VoIP call quality issues.

Hubs are not supported with UCx deployments and must be replaced with switches (preferably managed switches). Hubs broadcast traffic by design and will ultimately cause network congestion, which will degrade call quality. Hubs are typically unmanaged, which means there is no way to hard code speed/duplex settings.

Network switches should be deployed in a tree (or hub/spoke) topology instead of a cascade topology. This will ensure that all network traffic originating from one switch has the same number of Ethernet hops to reach the network gateway as any other switch. Take care to avoid any Ethernet device from being more than three hops away from a network gateway.

Spanning-Tree portfast (on Cisco switches) and Spanning-Tree edgeport (on Adtran switches) should be enabled on each port a phone will be connected to. These commands allow the network port to turn on quickly and begin passing traffic faster than normal. Since the UCx phones boot fairly quickly, if the network port does not unblock fast enough, the phone may try to obtain a DHCP lease prior to being able to pass network traffic. The phone will display an "Unable to obtain IP Address" error if this happens.

NOTE: Spanning-Tree portfast / edgeport commands should not be enabled on uplink ports, nor ports used for mutli-link connections which may create a network loop.

Downlink ports are considered switch ports which phones plug into. Downlink ports should be configured for auto speed and auto duplex. Polycom phones currently support a maximum speed of 100 Mb. A PC plugged into the back of the Polycom phone should also be set for auto speed and auto duplex. This will ensure proper network negotiation during bootup.

Sites with multiple gateways require special attention if you want all network traffic to go to one router and all VoIP traffic to go through another router. For these deployments, it is desirable to give the shortest path to the most critical traffic. You can accomplish this by using the router closest to the VoIP network as the default route for the LAN, then let that router direct the less critical traffic to the WAN router or out the Internet router. Other customers who support a WAN and an Internet connection at a single site typically use this to strip off VoIP to us and then route everything else over the WAN.

Analog Terminal Adaptors (ATAs)

ATAs are devices which convert SIP-based phone service into an analog signal which can be used to support existing fax machines, cordless phones, or any other legacy phone technology.

Types of ATA

We can use many types of ATAs to support your analog services. The main difference between the various devices is the number of analog ports each device supports and the handoff to your network. Here are two types of ATAs we use today:

Grandstream HT503 supports:

- DHCP Client
- 2FXS analog ports
- 2 RJ-11 ports

Grandstream GXW-42XX supports:

- 16, 24, 36 and 48 FXS analog ports
- Amphenol connector(s) and RJ-11 Ports for 16, 24 & 36 port models
- Amphenol connectors for 48 port model

Adtran TA900 series supports:

- Full AOS Router
- 4-24 FXS analog ports
- 4 FXO analog ports
- Up to 4 RJ-11 ports
- Up to 2 RJ-45 Ethernet ports
- Amphenol connector, requires a cable and 66 Block for punch-down termination

Choosing an ATA

The ATA selection process is based on your physical building layout and how your phone plant is run. If you have existing phones wired back to a central closet, you may have the ATA installed in the closet. You may require two separate ATAs if you have fax machines on opposite sides of the building. If you need a large number of analog ports you may have the ATAs stacked on top of each other, to provide multiples of 48 lines.

Remote Access

Unlike Polycom phones, we do not centrally manage ATAs. This means the ATA is pre-configured and installed on your premises. Once it's installed, we will require remote access to make configuration changes and to troubleshoot any issues you may report in the future.

You are required to provide network connectivity and power to each ATA. You are also required to provide us with remote network access for the purposes of remotely managing the ATA configurations. To achieve remote access, ATAs should be:

1. Static IP addressed or assigned a DHCP reservation
2. Firewalls must have a static port mapping created to each ATA

A single public IP address may be mapped to up to 65,000 ATAs. Here is an example of how the public IP address 204.1.2.3 may be mapped to 3 internal ATAs:

Public IP	Public Port	Private IP	Private Port
204.1.2.3	TCP/8001	192.168.1.1	TCP/80
204.1.2.3	TCP/8002	192.168.1.2	TCP/80
204.1.2.3	TCP/8003	192.168.1.3	TCP/80

The firewall port mapping is critical to allow us remote technical access to troubleshoot each ATA. Remote access is required before we will dispatch a Field Technician to continue troubleshooting an issue. Charges will apply if you do not provide remote access and a Field Dispatch is required.

Supported Security Devices

You are ultimately responsible for the security of your network. The introduction of our UCx service adds additional intricacies to your network which require careful consideration.

Most of our customers use private IP address assignments on their LAN and use Network Address Translation (NAT) or Port Address Translation (PAT) on a router or firewall. Manufacturers are adding features and functionalities to their devices which may hinder the proper operation of the VoIP deployment.

Our support site includes a list of security devices supported with UCx. These devices have been tested and proven to work with UCx deployments. This site also includes a list of security devices that we do not

support. In addition to the unsupported devices on the list, we do not support any devices or software which have reached their end-of-life. Once you have removed or replaced an unsupported device, we will begin troubleshooting the problem if it persists.

Connection Timeouts
We use an ACME Packet Session Border Controller behind your security device to maintain a pinhole connection through the firewall. If someone makes an inbound call to one of your phones, the ACME sends the call through the opened port to the phone. If the firewall closes the port prematurely, the call will die at the firewall and the phone will never ring.

License Considerations
Since each UCx phone consumes an IP address, you must ensure you have adequate licensing if your firewall restricts the number of connections or hosts it will support. For example: If your firewall has a 10 user license, and there are 3 UCx phones and 8 computers, the site requires a total of 11 licenses through the firewall. Firewalls will typically block one IP address until connections from another are closed.

Configuration Notes
The following section will help you facilitate the appropriate changes prior to your new UCx deployment.

We deploy our UCx service in such a way to reduce the amount of time you must spend configuring your security devices. Typically, a network is UCx ready if it supports a security device (router or firewall) which performs basic NAT. General network connectivity must be established prior to installing phones on your LAN. This means that NAT/PAT should be functional and provide basic Internet browsing prior to installing the phones.

If you have locked down your network using IP Access Lists (ACL) or firewall policies, you should verify the following ports are not restricted from making outbound connections from your LAN. You should not need to make any inbound allotments for the proper functionality of the UCx service.

Common Session Border Controllers

SBCs – 204.11.148.40, 209.104.255.30, 209.104.247.240
- SIP TCP/5060 outbound
- SIP UDP/5060 outbound
- RTP UDP/60000-65536

SIP1.we.ucx.telepacific.com – 65.98.131.70, 209.104.248.70 (Dynamic SRV Record)
- SIP TCP/5060 outbound
- SIP UDP/5060 outbound
- RTP UDP/60000-65536

SIP1.mw.ucx.telepacific.com – 65.98.131.70, 209.104.248.70 (Dynamic SRV Record)
- SIP TCP/5060 outbound
- SIP UDP/5060 outbound
- RTP UDP/60000-65536

SIP1.sw.ucx.telepacific.com – 65.98.131.80, 209.104.248.80 (Dynamic SRV Record)
- SIP TCP/5060 outbound
- SIP UDP/5060 outbound
- RTP UDP/60000-65536

SIP1.se.ucx.telepacific.com – 65.98.131.81, 209.104.248.81 (Dynamic SRV Record)
- SIP TCP/5060 outbound
- SIP UDP/5060 outbound
- RTP UDP/60000-65536

SIP1.ne.ucx.telepacific.com – 65.98.131.81, 209.104.248.81 (Dynamic SRV Record)
SIP TCP/5060 outbound
SIP UDP/5060 outbound
RTP UDP/60000-65536
Media Session Controllers – 65.98.131.83, 65.98.131.84, 209.104.248.83, 209.104.248.84
SIP TCP/5060 outbound
SIP UDP/5060 outbound
RTP UDP/60000-65536

Common UCx Services

FTP.dsci-net.com – 204.11.148.130
FTP TCP/20-21 outbound
TIME.dsci-net.com – 204.11.148.0/24
NTP TCP/123 outbound
XSP-WEB1.dsci-net.com – 209.104.248.110
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
FTP TCP/20-21 outbound
XSP-WEB2.dsci-net.com – 66.81.108.110
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
FTP TCP/20-21 outbound
XSP-CC1.dsci-net.com – 209.104.248.111
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
XSP-CC2.dsci-net.com – 66.81.108.111
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
XSP-REC1.dsci-net.com – 209.104.248.112
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
XSP-REC2.dsci-net.com – 66.81.108.112
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
XSP-XSI1.dsci-net.com – 209.104.248.113
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
XSP-XSI2.dsci-net.com – 66.81.108.113
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
UMS1.dsci-net.com – 204.11.148.44
XMPP TCP/5222 outbound
XMPP TCP/1081 outbound
HTTPS TCP/443 outbound
UMS2.dsci-net.com – 204.11.148.143
XMPP TCP/5222 outbound
XMPP TCP/1081 outbound
HTTPS TCP/443 outbound
USS1.dsci-net.com – 204.11.148.49
HTTPS TCP/8443 outbound
USS2.dsci-net.com – 204.11.148.145

HTTPS TCP/8443 outbound

WRS-R1.dsci-net.com – 209.104.248.118
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound

WRS-R2.dsci-net.com – 66.81.108.118
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound

WRS-NR1.dsci-net.com – 209.104.248.117
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound

WRS-NR2.dsci-net.com – 66.81.108.117
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound

XSP-WEB5.ucx.telepacific.com – 65.98.131.90
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
FTP TCP/20-21 outbound

XSP-WEB6.ucx.telepacific.com – 66.81.108.90
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
FTP TCP/20-21 outbound

XSP-CC5.ucx.telepacific.com – 65.98.131.91
HTTP TCP/80 outbound
HTTPS TCP/443 outbound

XSP-CC6.ucx.telepacific.com – 66.81.108.91
HTTP TCP/80 outbound
HTTPS TCP/443 outbound

XSP-REC5.ucx.telepacific.com – 65.98.131.92
HTTP TCP/80 outbound
HTTPS TCP/443 outbound

XSP-REC6.ucx.telepacific.com – 66.81.108.92
HTTP TCP/80 outbound
HTTPS TCP/443 outbound

XSP-XSI5.ucx.telepacific.com – 65.98.131.93
HTTP TCP/80 outbound
HTTPS TCP/443 outbound

XSP-XSI6.ucx.telepacific.com – 66.81.108.93
HTTP TCP/80 outbound
HTTPS TCP/443 outbound

UMS3.ucx.telepacific.com – 65.98.131.94
XMPP TCP/5222 outbound
XMPP TCP/1081 outbound
HTTPS TCP/443 outbound

UMS4.ucx.telepacific.com – 66.81.108.94
XMPP TCP/5222 outbound
XMPP TCP/1081 outbound
HTTPS TCP/443 outbound

USS3.ucx.telepacific.com – 65.98.131.95

HTTPS TCP/8443 outbound
USS4.ucx.telepacific.com – 66.81.108.95
HTTPS TCP/8443 outbound to
WRS-R3.ucx.telepacific.com – 65.98.131.98
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound
WRS-R4.ucx.telepacific.com – 66.81.108.98
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound
WRS-NR3.ucx.telepacific.com – 65.98.131.97
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound
WRS-NR4.ucx.telepacific.com – 66.81.108.97
HTTP TCP/80 outbound
HTTPS TCP/443 outbound
STUN TCP/3478 outbound

Auxiliary Services

WEBMEET.dscicorp.com – 72.44.196.198
HTTPS TCP/443 outbound
CounterPath Bria
HTTP TCP/80 outbound to bria.dsci-net.com (currently 209.104.229.128)
HTTPS TCP/443 outbound to secure.counterpath.com (currently 69.90.51.170)

Manufacturers are adding features to their security devices which alter VoIP traffic as it traverses the firewall. These devices attempt to mask the internal IP information required by the ACME Packet to properly communicate with the UCx phone. For this reason, we require you to disable all VoIP application awareness features configurable on the firewall. Failure to do so will cause one-way audio issues and call route failures.

Cisco PIX Firewalls
Cisco's Fixup performs application layer modifications which are not desirable for UCx. There are two global Fixup commands which you must disable to allow the SIP protocol to traverse the security device unchanged.

All other commands, including session timers, should be left at their default. Note that if a "clear xlate" is performed, UCx phones will cease to function correctly until they are rebooted or re-register.

```
Config t
    no fixup protocol sip 5060
    no fixup protocol sip udp 5060
```

Cisco ASA Firewalls
Like Cisco's PIX Firewall, the ASA version needs to have SIP ALG services disabled.
To determine whether the Cisco PIX or Cisco ASA security appliance is configured to support inspection of sip packets, log in to the device and issue the CLI command show service-policy | include sip. If the

output contains the text Inspect: sip and some statistics, then the device has SIP inspection enabled. The following example shows a Cisco ASA with SIP inspection enabled:

```
asa#show service-policy | include sip
    Inspect: sip, packet 123612, drop 23, reset-drop 0
```

```
Config t
    policy-map global_policy
        class inspection_default
            no inspect sip
```

Cisco IOS Routers (Using NAT/PAT)
We recommend that IP Reflexive ACLs are enabled to ensure valid two-way communication is not restricted. Reflexive ACLs will allow dynamic port mappings for SIP and RTP to occur when using PAT.

Newer IOSs have a NAT service which performs packet modification (much like fixup for Cisco firewalls) which needs to be disabled. Note that if a "clear ip nat translation *" is performed, UCx phones will cease to function correctly until they are rebooted or re-register.

```
Config t
    No ip nat service sip udp port 5060
```

IP Inspect is part of Cisco's firewall feature set and is not supported.

Adtran Total Access (Using NAT/PAT)
Adtran routers which have "ip firewall" enabled should have the following two global configuration entries disabled:

```
Config t
    no ip firewall alg h323
    no ip firewall alg sip
```

Juniper Netscreen 5-GT
The Netscreens have a Denial of Service (DoS) feature for UDP traffic which should be disabled. If this feature triggers, VoIP traffic will be blocked, causing call termination. We have tested and certified Netscreen v5.3.0r1.0 (Firewall+VPN) as a supported security device.

```
Security Mode:  trust-untrust
ALG SIP:  DISABLED
UDP Flood Protection:  DISABLED
```

SonicWall SonicOS
The following SonicWall settings should be set to allow UCx phones to properly communicate through the firewall.

```
Enable Consistent NAT:  DISABLED
Enable SIP Transformations:  DISABLED
Enable H.323 Transformations:  DISABLED
```

FortiGate Firewalls
The following FortiGate Firewall Session Helper must be removed to disable the firewall's ability to manipulate SIP traffic.

```
show sys session-helper
        #find the SIP helper ID #
config sys session-help
        #delete #
end
```

We will add more hardware configuration notes as we certify additional equipment.