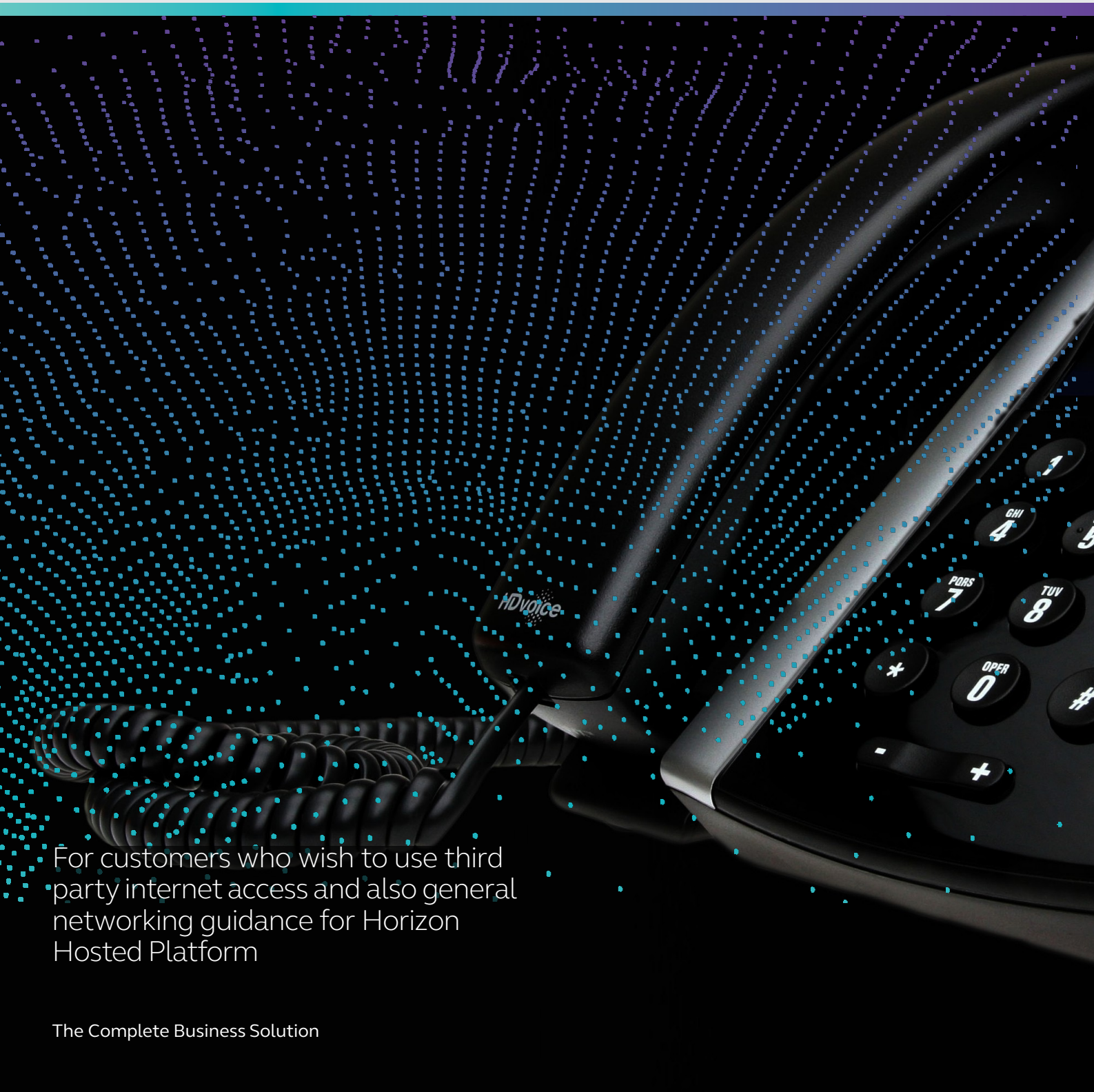
VOICE
MOBILE
DATA
IT

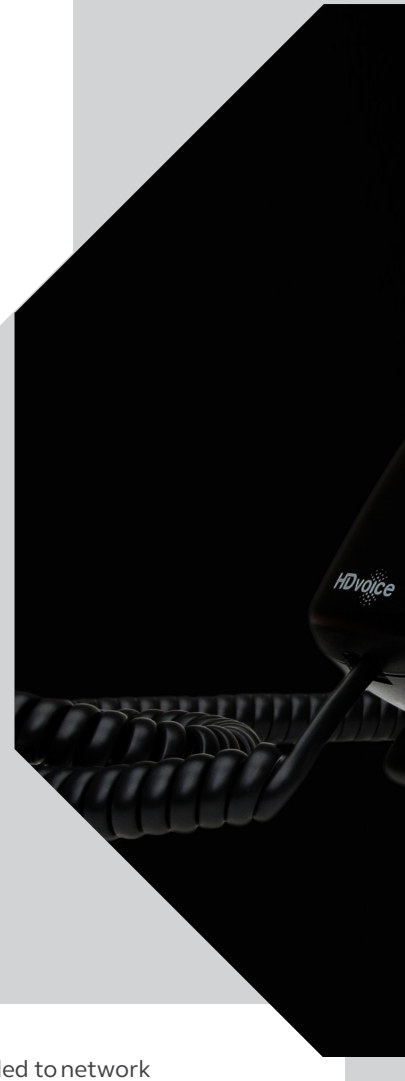
Horizon Network Configuration Guidelines

V6.0



For customers who wish to use third party internet access and also general networking guidance for Horizon Hosted Platform

The Complete Business Solution



Version	Date	Author	Reason
5.0	30/05/2019	Vicki Rishbeth	New SBC infrastructure added to network
6.0	21/04/2020	Vicki Rishbeth	updated SRV rules and UDP timeout values

1.0 Introduction

While Focus Group always prefer to install our own dedicated and on-net bandwidth and LAN for our VOIP products we recognise that some customers have existing data services they make like to use.

The purpose of this document is to define the access requirements for two scenarios when on-net access is not used as the delivery method for Horizon traffic to an end user site. The two scenarios are:

1. Delivered over Internet Access by a supplier other than the Horizon platform provider (Gamma Telecom)

2. Delivered via a Private Access/Interconnect to the Horizon Platform provider (Gamma Telecom)

Horizon is designed to work using public IP addressing for access. This provides more than just the provision of speech and signalling protocols but also access to other publicly available services which Horizon uses.

If a customer wishes to utilise another data provider or ISP, they need to ensure that the access can meet the following requirements and functionality. Failure to meet the access requirements below will result in quality and setup/support issues.

VOICE
MOBILE
DATA
IT

2.0 Public Access via Internet

2.1. Access Control

Customers must ensure that the following IP addresses and ports (both directions) are available and not blocked by firewalls. If these ports are not opened (i.e. a customer or network based firewall is blocking them), or IP addresses allowed, Horizon will not function correctly.

DNS records utilised by Horizon are provided. These are informational only for most deployments as DNS will be learned from records populated on Gamma's authoritative public DNS servers. Customers who maintain private DNS servers may need to populate the DNS records in their servers.

Focus recommends that only trusted IPs are allowed to send and receive traffic via port 5060 and 5080.

Domain Name	Record Type	IP Address	Ports	Function
xsp.unlimitedhorizon.co.uk	A	88.215.61.171 88.215.61.173 88.215.61.177 88.215.61.178	TCP 80, 443	Device provisioning, including soft clients and software downloads.
dms.mypabx.co.uk	A	88.215.60.165 88.215.60.167	TCP 80, 443	Soft client provisioning and software downloads
xsi.unlimitedhorizon.co.uk	A	88.215.60.155 88.215.60.156 88.215.60.166 88.215.60.168 88.215.50.193 88.215.50.194	TCP 443	Soft clients, Integrator, TAPI
xsip1.unlimitedhorizon.co.uk	A	88.215.60.156		
xsit1.unlimitedhorizon.co.uk	A	88.215.60.155		
xsip2.unlimitedhorizon.co.uk	A	88.215.60.166		
xsit2.unlimitedhorizon.co.uk	A	88.215.60.168		
N/A	A	127.0.0.1	TCP 21050	TCP 21050

VOICE
MOBILE
DATA
IT

Domain Name	Record Type	IP Address	Ports	Function
clients.unlimitedhorizon.co.uk **URLS** **https://clients.unlimitedhorizon.co.uk/receptionist** **https://clients.unlimitedhorizon.co.uk/callcentre**	A	88.215.60.162 88.215.60.163	TCP 443	Receptionist, Call Centre Clients
clientp.unlimitedhorizon.co.uk **clientt.unlimitedhorizon.co.uk**	A	88.215.60.162 88.215.60.163	TCP 443	Receptionist, Call Centre Clients
im.unlimitedhorizon.co.uk	A	88.215.60.163	TCP 5222	Instant messaging and presence (for softphone clients)
www.gointegrator.com	A	104.24.108.175 104.24.108.175	TCP 443, 80	Integrator
ntp.business-access.co.uk	A	88.215.61.81 88.215.63.145	UDP 123	NTP for time/date display
europe.pool.ntp.org	A	178.79.162.34 78.47.138.42 148.251.127.15 46.165.212.205		NTP for time/date display Polycom
ldap.unlimitedhorizon.co.uk	A	88.215.60.129 88.215.60.132	TCP 389, 636	Corporate Directory Service

VOICE
MOBILE
DATA
IT

2.2 Voice and Video Traffic

Voice and video traffic from all Horizon IP phones and soft-clients route via Horizon Access SBCs as defined below. Occasionally new Horizon Access SBCs will be added to the list and the change will be communicated via regular channels.

IP Address	Protocol and Ports	Function
88.215.63.171	UDP 5060, TCP 5080	SBC SIP signalling
88.215.63.21		
88.215.58.1		
88.215.55.33		
88.215.54.1		
88.215.58.129		
88.215.58.161		
88.215.48.0/25		
88.215.58.2	UDP 10000-60000	SBC RTP Traffic
88.215.63.172		
88.215.54.2		
88.215.55.34		
88.215.62.22		
88.215.58.130		
88.215.58.162		
88.215.48.0/25		

VOICE
MOBILE
DATA
IT

2.3 SBC Discovery

DNS SRV records are used to provide high availability service for Horizon IP phones and soft-clients. DNS SRV records resolve to two or more DNS A-records, which in turn resolve to IP addresses of Horizon Access SBCs. This mechanism provides each Horizon device with multiple SBCs to send or receive calls.

Domain Name	Record Type	Service Name	Portocol	Port	Function
sipX.unlimitedhorizon.co.uk ***Example*** ***_sip._udp.sip1.unlimitedhorizon.co.uk*** ***_sip._udp.sip9.unlimitedhorizon.co.uk***	SRV	SIP	UDP	5060	SRV Records for Horizon Voice Signalling Traffic
siptX.unlimitedhorizon.co.uk ***Example*** ***_sip._tcp.sipt3.unlimitedhorizon.co.uk***	SRV	SIP	TCP	5080	SRV record for SIP ALG bypass
siptX.unlimitedhorizon.co.uk ***Example*** ***_sip._udp.sipt3.unlimitedhorizon.co.uk***	SRV	SIP	UDP	5080	SRV record for SIP ALG bypass
mobile-sipX.unlimitedhorizon.co.uk ***Example*** ***_sip._tcp.mobile-sip1.unlimitedhorizon.co.uk***	SRV	SIP	TCP	5080	SRV Records for Horizon Mobile Client Voice Signalling Traffic
nodex.sip.unlimitedhorizon.co.uk ***Example*** ***node4.sip.unlimitedhorizon.co.uk***	A	N/A	N/A	N/A	A Records for Horizon Voice Signalling Traffic

2.4 UDP Fragmentation During Horizon Communications.

In some instances, the size of the UDP packets transmitted between the Horizon platform and customer handsets will exceed the default 1500-byte payload, when this happens packet fragmentation will occur. It is the responsibility of the customer to ensure that any in path CPE is able to support UDP fragmentation. It is also advised that a check is made to confirm that any further applications/functions running on the CPE do not interfere with the reassembly of fragmented UDP packets.

VOICE
MOBILE
DATA
IT

If UDP fragmentation is not allowed on CPE network devices the following features may not function correctly.

- BLF (Busy Lamp Field)
- Feature Synchronisation (DND, Call Forward Busy, Call Forward Always & Call Forward Unreachable/No Answer)
- Incoming calls to Horizon devices after a series of call forwards within the same Horizon Company

2.5 SIP ALG

SIP Application Layer Gateway (ALG) is common in many of today's routers and in most cases enabled by default on enterprise, business and home broadband routers. Its primary use is to prevent problems associated to the router's firewalls by inspecting VOIP traffic packets, and if necessary modifying them to allow connection to the required protocols or ports.

On many business and home class routers Active SIP ALG will cause a mixture of problems by adjusting or terminating Horizon traffic packets in such a manner that they are corrupted and cause issues with the service, manifesting in a range of intermittent issues such as; one-way audio, dropped calls, problems transferring calls, handset dropping registration and making or receiving internal calls.

SIP ALGs should be disabled on all CPE routers, we will not accept any faults or issues raised against Horizon if a SIP ALG is enabled.

For instructions on disabling this feature please refer to the specific router user guide.

2.6 Desktop Client SIP ALG Bypass

Summary

For deployments featuring Horizon Desktop Client, on Windows and Mac OS, please ensure that firewalls allow access to Gamma SBCs on TCP port 5080 in addition to UDP port 5050.

Description

Prior to January 2019 the Horizon Desktop Client used the standard UDP port 5060 to exchange signalling traffic with Horizon Access SBCs.

Due to its portability Horizon Desktop Client is often used in remote access situations, at home or on public internet connections where SIP ALG may be present and it is outside the user's control to disable it.

From January 2019 Horizon Desktop client will use new DNS SRV records as defined in the SBC Discovery section of this document. These records route SIP traffic to the Horizon Access SBCs via TCP 5080 first choice. TCP 5080 is a non-standard port for SIP traffic so SIP ALGs will not inspect and alter the traffic.

If the client cannot reach the Horizon SBCs on TCP 5080 it will reattempt on the standard UDP 5060 route, so existing deployments behind restrictive firewalls will continue to make and receive calls.

For optimal performance it is strongly recommended that access to Horizon SBCs via TCP 5080 is allowed.

7. Keep-Alives

Handsets are pre-configured to send UDP keep-alive messages towards the Horizon platform every 45 seconds using the SIP port. These messages keep the firewall pin-holes open which ensures the success of incoming calls.

8. UDT NAT Timeout

Set UDP NAT Timeout > 572 seconds.

Some routers have been reported to close NAT pinholes despite Horizon phones sending keep-alives every 45 seconds. To protect against this occurring it is recommended that UDP NAT Timeout on the router is set higher than the SIP registration refresh interval for Horizon phones. That is higher than 572 seconds.

9. NAT Port Translation

For Horizon handsets to register correctly, if using a router that requires setting up Dynamic Port Address Translation - Port Multiplexing option must be selected.

10. DNS

A public DNS service must be available to the Horizon handsets so that the domain names can be resolved to the associated IP addresses. SRV and A record types are used by the Horizon service. As best practice resilience of DNS needs to be considered hence both a primary and secondary DNS service should be configured as part of any deployment.

Gamma's DNS servers are detailed below, please note these can only be used with Gamma access.

Primary DNS Server	Secondary DNS Server
88.215.61.255	88.215.63.255

3.0 Horizon Collaborate

Customers who are deploying Unified Communications features with the Horizon Collaborate enhancement can use the IP address and port information for Horizon Collaborate servers to configure firewalls. DNS SRV records for server discovery are also provided for those managing private DNS solutions.

VOICE
MOBILE
DATA
IT

Failure to provide access to these servers will cause issue for features like Instant Messaging, Presence, MyRoom sessions and Screen Sharing.

3.1 Horizon Collaborate Access Control

Collaborate Guest Client URLs are dynamically generated by the Collaborate My Room owner for sharing with Conference Guests.

Domain Name	Record Type	IP Address	Ports	Function
uss01.unlimitedhorizon.co.uk uss02.unlimitedhorizon.co.uk uss03.unlimitedhorizon.co.uk	A	88.215.50.145 88.215.50.146 88.215.50.147	TCP 8443 TCP 443	Collaborate Sharing Server
ums01.unlimitedhorizon.co.uk ums02.unlimitedhorizon.co.uk ums03.unlimitedhorizon.co.uk ums04.unlimitedhorizon.co.uk	A	88.215.50.129 88.215.50.130 88.215.50.133 88.215.50.134	TCP 5222, TCP 5269, TCP 443, TCP 5280-5281, TCP 1081-1082	Collaborate Instant messaging and Presence server. For IMP, File exchange and Mobile gateway
wrsh01.unlimitedhorizon.co.uk wrsj01.unlimitedhorizon.co.uk wrst01.unlimitedhorizon.co.uk	A	88.215.50.162 88.215.50.161 88.215.50.163	TCP 8060, TCP 8070, UDP 1024-3024, UDP 3478, TCP 443	Collaborate WebRTC server signalling, media and STUN port
clients.mypabx.co.uk 1	A	88.215.50.241 88.215.50.242	TCP 443	Collaborate White-label Guest Client
clients.unlimitedhorizon.co.uk 1	A	88.215.60.162 88.215.60.163	TCP 443	Collaborate Guest Client Landing page
ums01.im.unlimitedhorizon.co.uk ums02.im.unlimitedhorizon.co.uk ums03.im02.unlimitedhorizon.co.uk ums04.im02.unlimitedhorizon.co.uk	A	88.215.50.131 88.215.50.132 88.215.50.135 88.215.50.136	TCP 443	Collaborate Guest Client Access

1 Collaborate Guest Client URLs are dynamically generated by the Collaborate My Room owner for sharing with Conference Guests.

VOICE
MOBILE
DATA
IT

3.2 Horizon Collaborate DNS SRV Records

The below DNS SRV records are used to support high-availability services in Horizon Collaborate.

Domain Name	Record Type	Service Name	Protocol	Port	Function
uss.unlimitedhorizon.co.uk *Example* *_uss-client._tcp.uss.unlimitedhorizon.co.uk*	SRV	uss-client	TCP	8443	Horizon Collaborate sharing server
umsc01.unlimitedhorizon.co.uk *Example* *_xmpp-client._tcp.umsc01.unlimitedhorizon.co.uk* umsc02.unlimitedhorizon.co.uk *Example* *_xmpp-client._tcp.umsc02.unlimitedhorizon.co.uk*	SRV	xmpp-client	TCP	5222	Horizon Collaborate Instant Messaging and Presence Server
muc.umsc01.unlimitedhorizon.co.uk *Example* *_xmpp- server._tcp.muc.umsc01.unlimitedhorizon.co.uk* muc.umsc02.unlimitedhorizon.co.uk Example _xmpp-server._tcp.muc.umsc02.unlimitedhorizon.co.uk	SRV	xmpp-server	TCP	5269	
umsc01.unlimitedhorizon.co.uk *Example* *_gateway- client._tcp.umsc01.unlimitedhorizon.co.uk* umsc02.unlimitedhorizon.co.uk *Example* *_gateway-client._tcp.umsc02.unlimitedhorizon.co.uk*	SRV	gateway-client	TCP	443	

3.3 Horizon Collaborate Video Bandwidth

Horizon Collaborate Desktop and Mobile soft-clients implement Dynamic Video Bitrate where the video quality will reduce when packet loss is detected between two video devices in a call. The feature aims to provide a stable and responsive video session when the bandwidth available for the call is constrained. It works by both video devices exchanging RTCP (Real-time Control Protocol) messages providing feedback if network conditions are poor and video frames are lost in transit. RTCP is sent to the same Horizon Access SBCs and port range as normal media (RTP) traffic so no changes to customer firewalls should be required to support the feature.

The range of video bandwidth transmitted by Horizon Collaborate Clients is 128kbps to 2048 kbps depending on network conditions. For deployments where bandwidth is known to be limited it is possible to limit the video bandwidth transmitted by the Horizon Desktop Client in the Audio/Video Settings Menu.

VOICE
MOBILE
DATA
IT

4.0 The LAN

4.1 Support For VLANS

Both Cisco and Polycom phones provided as part of the Horizon service have CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discover Protocol) enabled as default on delivery. These protocols, CDP (Cisco proprietary), and LLDP including LLDP-MED (vendor neutral), are link layer protocols used by network devices for advertising their identities and capabilities in order to assist with management of the local area network environment, specifically VLAN segregation.

If you wish to support either of these functions for VLAN configuration/ selection on the LAN, then you should enable the desired function on the network equipment and disable the alternative option. For example, if you wish to support CDP for a particular end user you should make sure LLDP is not configured as a live option on their network equipment and that CDP is enabled as a live option.

When using LLDP or CDP the Horizon phones will support and use any VLAN ID configured on the switching infrastructure (as part of the LLDP and CDP configuration) for both Voice and Data. If the customer wishes to daisy chain laptops or PC's using the switch port on the Horizon phones, any traffic from this port will be entered into the data VLAN.

Example VLAN set up (using CDP/LLP)

Example Data VLAN: 20

Example Voice VLAN: 30

What we do not support:

Fixed VLAN ID's

Static VLAN assignment either directly from the phone or from the core network.

We cannot enable only one of the VLAN options (either CDP or LLDP). Both will always be enabled on Horizon phones and it is the customer's responsibility to enable/disable the required function on their network.

Please be aware Softphone Clients, ATA's and Wireless handsets (Dect) do not currently support VLAN.

VOICE
MOBILE
DATA
IT

5.0 Firmware Upgrades

Horizon handsets are pre-configured to check for configuration and firmware updates every evening between 00:00 and 05:00.

Horizon handsets will only download new configuration or firmware files when they detect that a change has been made. Configuration files are typically ~70Kb or less, but firmware files are larger ranging between 3.5 to 57.5MB. Network administrators should consider these file downloads with regards to the bandwidth available on the access circuits the Horizon service runs over.

Device Type	Firmware File size
Cisco 122	10.0 MB
Cisco 232	11.3 MB
Cisco 501	4.2 MB
Cisco 502	4.2 MB
Cisco 504	4.2 MB
Cisco 509	4.2 MB
Cisco 525	11.6 MB
Cisco MPP 8841	105 MB
Cisco MPP 8851	105 MB
Cisco MPP 8861	105 MB
Polycom 331	3.5 MB
Polycom 335	3.5 MB
Polycom 450	4.1 MB
Polycom 650	3.5 MB
Polycom 5000	3.7 MB
Polycom 7000	11.3 MB
Polycom VVX 150	34.8 MB
Polycom VVX 201	33.4 MB
Polycom VVX 250	46.2 MB
Polycom VVX 310	51.1 MB
Polycom VVX 411	51.1 MB
Polycom VVX 450	46.2 MB
Polycom VVX 500	58.9 MB
Polycom VVX 600	57.5 MB
Polycom Trio 8500	294.3 MB
Polycom Trio 8800	294.3 MB
Yealink W52P	9.2 MB

VOICE
MOBILE
DATA
IT

6.0 Mobile Clients Customer Firewall Requirements (R22+)

Since August 2017 Horizon Mobile Clients use cloud messaging systems from Apple and Google to receive incoming call notifications. In 2019 instant messages will be sent to Mobile Clients in the same way.

When an incoming call is received by a user who is logged into the Horizon Mobile Client on Android or iOS (R22+) Horizon servers will send a notification to Apple or Google's servers. Apple or Google will forward the notification to the device and the app will wake up, alert for an incoming call and will setup the voice call with the Horizon servers if the call is answered.

Any Horizon Mobile Clients (R22+) operating behind firewalls must therefore allow access to Apple and Google push notification servers at the IP addresses and via the ports below.

These rules are derived from advice from Google and Apple. They specify wide ranges of IP addresses as their push notification servers scale to millions of requests so new servers may be commissioned at new IP addresses in their ranges with no way to provide prior notice.

For the Mobile client to receive push notifications from Apple or Google servers, when running on a phone behind a firewall access must be allowed to Apple and Google servers on the following ports:

Apple
TCP: 443, 5223

Google
TCP: 443, 5228, 5229, and 5230

The connections are outbound originated only, from the phone to the cloud messaging server. The phone will keep the connection alive and setup a new connection when required.

Apple and Google may commission new servers, at new IP addresses at any time to manage the load across the systems. As a result it is not possible to provide customers with a list of IP addresses to configure the firewall with. Push Notification servers are discovered using DNS requests but these are managed to Operating System processes so, again, it is not possible to state a list of hostnames that could be entered into a firewall that can allow traffic based on configured FQDNs.

Apple provide a straight-forward solution, their servers will appear somewhere in their class A subnet: 17.0.0.0/8

Google however, only state that the IPs will appear in their ASN 15169. This contains hundreds of IP subnets which would be impractical to input into a firewall. Focus have summarised the subnets to a more manageable list. This list is subject to change by Google and Focus will not be notified so use of it is at the maintainers own risk.

VOICE
MOBILE
DATA
IT

IP Address	Protocol and Ports	Function
8.0.0.0/10	TCP 443, 5228, 5229, 5230	Push Notifications for Horizon Mobile Client – Android
23.224.0.0/11		
35.128.0.0/9		These ranges, and the servers behind them are operated by Google. Horizon Mobile clients R22 and up use Google's Firebase Cloud Messaging service to deliver notifications: https://firebase.google.com/docs/cloud-messaging/
64.0.0.0/4		
104.0.0.0/5		
128.0.0.0/3		
162.216.0.0/13		
185.0.0.0/8		
172.96.0.0/12		
172.192.0.0/10		
173.192.0.0/10		
192.104.160.0/23		
192.158.28.0/22		
192.178.0.0/15		
199.192.0.0/11		
207.223.160.0/20		
208.0.0.0/4		
17.0.0.0/8	TCP 443, 5223	Push Notifications for Horizon Mobile Client – iOS. These ranges, and the servers behind them are operated by Apple. Horizon Mobile clients R22 and up use Apple's Push Notification service to deliver notifications: https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html

VOICE
MOBILE
DATA
IT

7.0 Handsets

- The phones require a DHCP address, hence must have access to a DHCP server.
- (Fixed static IP's are not supported).
- NAT must be used and enabled for DHCP pool supplied to phones.

7.1 Phone RTP Port Ranges

Horizon phones will send/receive RTP from the following port ranges:

Device	RTP Port Max	RTP Port Max
Mobile client (Android/iOS) Audio	8500	8599
Mobile client (Android/iOS) Video	8600	8699
Desktop client (Windows/Mac) Audio	8500	8599
Desktop client (Windows/Mac) Video	8600	8699
Polycom_xxx	2222	2268
Yealink_xxx	16384	16538
Cisco_122		16482
Cisco_232		
Cisco_501		16538
Cisco_502		
Cisco_504		
Cisco_509		
Cisco_525		16482

VOICE
MOBILE
DATA
IT