

***Evaluation of the Direct
Packet STNS Firewall
Traversal Solution***



Evaluation of the Direct Packet STNS Firewall Traversal Solution

October 2007



Table of Contents

<i>Executive Summary</i>	1
<i>Introduction</i>	2
<i>Evaluation Results</i>	3
<i>Test Environment</i>	5
<i>Baseline (Failure) Testing</i>	6
<i>STNS Installation</i>	7
<i>STNS Evaluation</i>	12
Part 1 – Dial-Out Testing	12
Part 2 – H.239 Testing	13
Part 3 – IP to IP Gateway Testing.....	14
Part 4 – Video Auto Attendant (AA) Testing	14
Part 5 – HTTP / Web Proxy Testing	15
<i>Summary of Test Results</i>	17
<i>About Wainhouse Research</i>	20
About the Author(s)	20
<i>About Direct Packet Research</i>	20
<i>Appendix A – Network Diagram</i>	21
<i>Appendix B – Equipment Information</i>	22
Additional Equipment Notes.....	23
<i>Appendix C – Test Call Results</i>	24

List of Figures

Figure 1: Evaluation Results - Overall Ratings	3
Figure 2: Evaluation Results – Radar Charts	3
Figure 3: Equipment Used within the Test Environment.....	5
Figure 4: Typical Session Border Controller Deployment	7
Figure 5: Direct Packet Appliance Systems Used During the Evaluation	8
Figure 6: FE - Listening for Back End Units	9
Figure 7: BE - Confirming Connection to the FE.....	9
Figure 8: BE - List of Endpoints Registered.....	10
Figure 9: BE - Systems Authorized to Traverse the Firewall	10
Figure 10: FE - View of All Registered Devices in the Environment	11
Figure 11: FE - Video Auto Attendant Permissions	15

Executive Summary

In August 2007, Wainhouse Research (WR) conducted a thorough evaluation of Direct Packet Research's Secure Traversal Navigation Solution (STNS), an appliance-based solution that enables videoconferencing sessions to be conducted through enterprise firewalls.

To facilitate this testing, WR set up four (4) discrete local area network spaces, similar to those found within the typical enterprise, in our Atlanta test lab. Three of the networks were "private," utilizing hardware-based firewalls and private IP address spaces (ex. 192.x.x.x), and the fourth was "public" and did not include a firewall. We then installed a total of nine video systems and three video bridges / MCUs from leading manufacturers including Polycom, Tandberg, LifeSize, Sony, Aethra, and others.

Prior to installing the STNS solution, only "local" video calls within the same network space were possible. Without exception, ALL video calls between the different networks failed (either the systems were unable to connect, or video / audio transmission failed). After installing the STNS solution, a relatively straight-forward process that did NOT require modifications to the network configuration or firewall rules, we were able to successfully conduct video calls between all test systems and MCUs.

After installing STNS within the test environment, video calls between the different networks and firewalls worked perfectly.

The key take-away from this evaluation is that the STNS solution allowed us to conduct video calls between devices (endpoints, MCUs) from different vendors installed in different network spaces, without having to sacrifice the call experience (bandwidth, video / audio protocols, video resolution, encryption, etc.) or modify firewall configurations.

This document contains detailed information about the test environment, setup, procedures, and results.

Introduction

Traditionally, the majority of videoconferencing sessions were conducted internally, involving primarily internally-deployed conferencing systems. However, the enhanced reliability and performance of IP-based videoconferencing has generated newfound trust for videoconferencing within the enterprise, and has fueled increased interest in videoconferencing with external entities (clients, prospects, partners, affiliates, etc.).

Unfortunately, the systems and methods (firewalls, NAT, etc.) used to protect IP networks from unauthorized access block the communication paths needed for inter-enterprise videoconferencing. For this reason, most of the external video sessions conducted today use ISDN, which means that the meeting participants do not typically enjoy the best possible reliability and performance for their video sessions. How ironic that demand generated largely by the benefits of IP is usually fulfilled using ISDN. Fortunately, there are solutions on the market today that allow organizations to conduct IP-based videoconferencing sessions with those outside their private network without sacrificing network security.

This document details the results of a WR evaluation of the Direct Packet Secure Traversal Navigation Solution; an SBC-type firewall traversal solution that utilizes appliances installed both behind and outside the firewall to allow for secure videoconferencing between private and public networks.

IMPORTANT NOTES

- 1) For the purposes of this document, we suggest the following definitions:
 - An “internal” videoconferencing session is a video call involving video systems or devices installed within the enterprise facilities, using the enterprise’s private data network (LAN / WAN), and operating behind the enterprise’s firewall and network security systems.
 - An “external” videoconferencing session is call including at least one video system or device located outside the enterprise’s private data network / firewalls. The external system(s) may be installed on the public Internet or on private data networks and behind the firewalls of other entities.
 - A network space is one of the four distinct network environments, each with its own IP address subnet, created for this evaluation.
- 2) Although the discussions within this document focus primarily on “external” videoconferencing sessions, the same principles apply for “internal” videoconferencing sessions involving sites with discrete IP networks. For example, a health care consortium might include ten different hospitals, each utilizing a private network. For the purposes of this paper, calls between those hospitals would be considered “external.”
- 3) The cost associated with this third-party evaluation was covered by Direct Packet Research.

Evaluation Results

Based on our testing and evaluation, WR gave the evaluated solution ratings from one to five in each category (where five is the best possible score) as shown below.

Recognizing that each enterprise will have different needs and priorities, we have included a weighting factor that WR believes represents the need of many enterprises. WR recommends that enterprises considering an investment of this type should recalculate the averages below using weighting factors appropriate for their environment.

Ratings: Higher = Better	WR Weighting Factor	Direct Packet STNS Solution
Install / Configure	2	4.0
User Interface	3	4.0
Connectivity	5	4.5
Interoperability	5	4.5
Feature Set	4	4.0
Security	5	4.5
Cost (Small Deployment)	3	2.8
Cost (Large Deployment)	2	1.8
Un-Weighted Average		4.3 / 3.8
Weighted Average		4.3 / 4.0

Figure 1: Evaluation Results - Overall Ratings

Since WR does not believe that cost alone will be a significant decision-making factor for most organizations seeking to deploy this type of solution, WR calculated two different ratings. The first (4.3 for STNS) includes only performance related ratings (install, UI, connectivity, interoperability, feature set, and security). The second includes both performance and cost-related ratings.

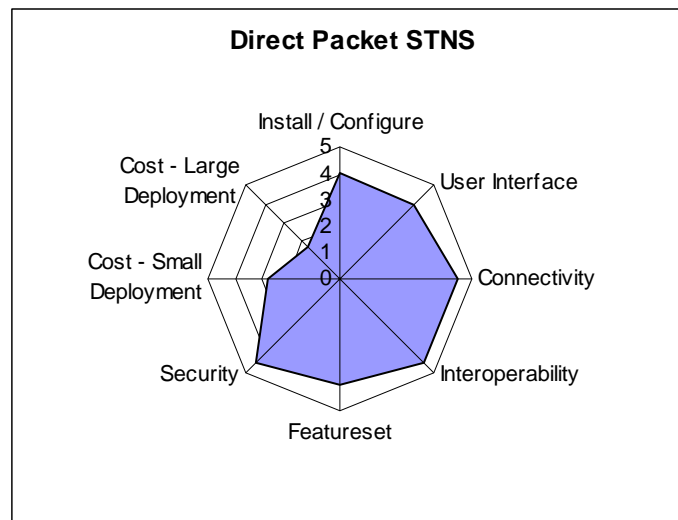


Figure 2: Evaluation Results – Radar Charts

As shown above, the Direct Packet STNS solution excelled in the areas that WR deems most critical for NAT / firewall traversal solutions including connectivity, interoperability, feature set, and security.

Install / Configure – Reflects a variety of install / configuration related items including the time required, overall difficulty and complexity, and the need for additional software or specialized technical knowledge.

User Interface – Reflects WR’s opinion of the system user interface including the UI’s organization and structure, responsiveness, general utility and usability, and our assessment of the learning curve associated with using the UI.

Connectivity – For the purposes of this report, “connectivity” is an indication of whether the solution forced any connectivity compromises between the test devices. In other words, did the solution impact the connections in terms of support / use of different connection speeds, video / audio protocols, video resolution, H.239, encryption, or other items?

Interoperability – Reflects the system’s ability to support devices (endpoints, MCUs, etc.) from different manufacturers, whether the system functions better with one vendor’s devices compared to another, and if the system requires other devices to function.

Feature Set - Provides an indication of whether the system provides additional “advanced” features beyond the standard NAT / firewall traversal functionality. Possible advanced features include H.460 support, an embedded gatekeeper, IP to IP gateway, IP to ISDN gateway, video auto attendant, NAT server, etc.

Security – Reflects the security features / capabilities included within the solution including a) UI security (logins / passwords / access levels) and b) NAT / firewall traversal security (# of ports that must be opened on the firewall in order to allow traversal traffic, whether the data streams themselves are encrypted, security in place to control which devices can leverage the traversal solution, etc.).

Cost (Small and Large Deployment) – Provides an indication of the relative costs (compared with competing offerings) associated with the deployment of this NAT / firewall traversal for a typical small and large enterprise as described in the table below.

	Small Deployment	Large Deployment
# of Large Offices (12 video systems per office)	0	5
# of Small Offices (3 video systems per office)	4	20
# of SOHO users (1 system per location)	2	10

As a part of the cost comparison exercise, WR considered a variety of factors including the need for appliances or PCs in each location, the total number and bandwidth of traversal calls that can be conducted simultaneously, and whether or not all traversal traffic would be routed through a central device / location.

Test Environment

The STNS testing was conducted in August 2007 in WR's Atlanta test lab. The goal of this exercise was to assess the functionality and performance of this firewall traversal solution in the following areas:

- Ease of Installation / Configuration
- Usability / System Management
- Reliability and Performance
- Features and Functions
- Interoperability with leading video systems, video bridges, and enterprise firewalls

To facilitate this testing, WR set up four (4) discrete network spaces, similar to those found within the typical enterprise, in our Atlanta test lab. Three of the network spaces (Corporate HQ, Branch Office, and SOHO) were "private," utilizing hardware-based firewalls and private IP address spaces (ex. 192.x.x.x). The fourth network space was "public" and did not include a firewall.

We then installed a total of nine video systems, three video bridges and three network firewalls / NAT devices from leading manufacturers into the various network spaces as shown in the table below.

	Corporate HQ	Branch Office	SOHO	Public Space
IP Addresses	192.168.70.x	192.168.60.x	192.168.1.x	10.0.0.x
Video Endpoints	LifeSize Room Polycom VSX7000 Tandberg 1700MXP	Polycom VSX3000 Sony G-50 Tandberg 880MXP	Polycom HDX9004* Tandberg-1000* * Only 1 at a time	Aethra X3 Polycom ViewStation
Video Bridge	Codian MCU4200	Tandberg MPS-200	None	Polycom MGC-50
Firewall / NAT Device	Cisco PIX	Microsoft ISA	LinkSys BEFSX41	None
Direct Packet Device	BE-100	BE-10	REO	FE-200

Figure 3: Equipment Used within the Test Environment

As shown in the table above, each of the four network spaces also included a Direct Packet STNS appliance (see figure 5 below for information about each Direct Packet device).

For additional information, please review the following:

- 1) Appendix A - Network Diagram for a network topology diagram of the test environment.
- 2) Appendix B - Equipment Information about the devices used within the evaluation

Baseline (Failure) Testing

To establish a functionality baseline BEFORE the implementation of the Direct Packet STNS solution, WR installed all video endpoints, MCUs, and firewalls as shown in the diagram above. We then attempted a series of calls between endpoints and MCUs within the same network zone and between different network zones.

Part 1 - No Gatekeeper

Prior to installing the STNS appliances, there were no active gatekeepers within the test environment. For this reason, calls were placed using each system's IP address.

As expected, ALL video calls between devices (systems and MCUs) within the same network space were successful. However, ALL video calls between the different networks spaces failed (either the systems were unable to connect due to network errors, or the video / audio transmission failed).

These test calls confirmed two key items:

- i) The basic functionality of all video devices (endpoints and MCUs) within the test environment.
- ii) That the firewalls / NAT devices within the test environment were blocking video between the different network spaces.

Part 2 – Including Gatekeeper

For the second part of the baseline testing, WR connected the STNS devices within each network space (detailed information about the STNS installation and configuration will be provided later in this document) and registered each device (endpoint and MCU) to its local STNS gatekeeper. Note that for this portion of the testing, we activated only the STNS gatekeeper capability, and specifically did NOT activate the firewall traversal functionality.

Once all systems were registered to their local gatekeeper (confirmed both on the video devices directly and via the STNS user interface), we repeated the above test calls using each system's E.164 alias instead of its IP address. Once again, ALL video calls between devices in the same network space were successful, but calls between the different network spaces failed.

This round of testing verified two items:

- i) The basic functionality of the STNS gatekeeper
- ii) That using a gatekeeper does NOT allow video calls to traverse firewalls and NAT devices.

STNS Installation

The STNS solution follows the basic deployment architecture of SBC-type solutions as follows (and shown below):

- Session Border Controllers (SBCs) are installed in accessible network spaces.
- Session Border Clients are installed locally within each network space containing devices in need of firewall traversal assistance.
- The clients reach out through the firewall(s) and register with the SBC and establish permanent connections (or streams) between the client and the SBC to be used for firewall traversal.

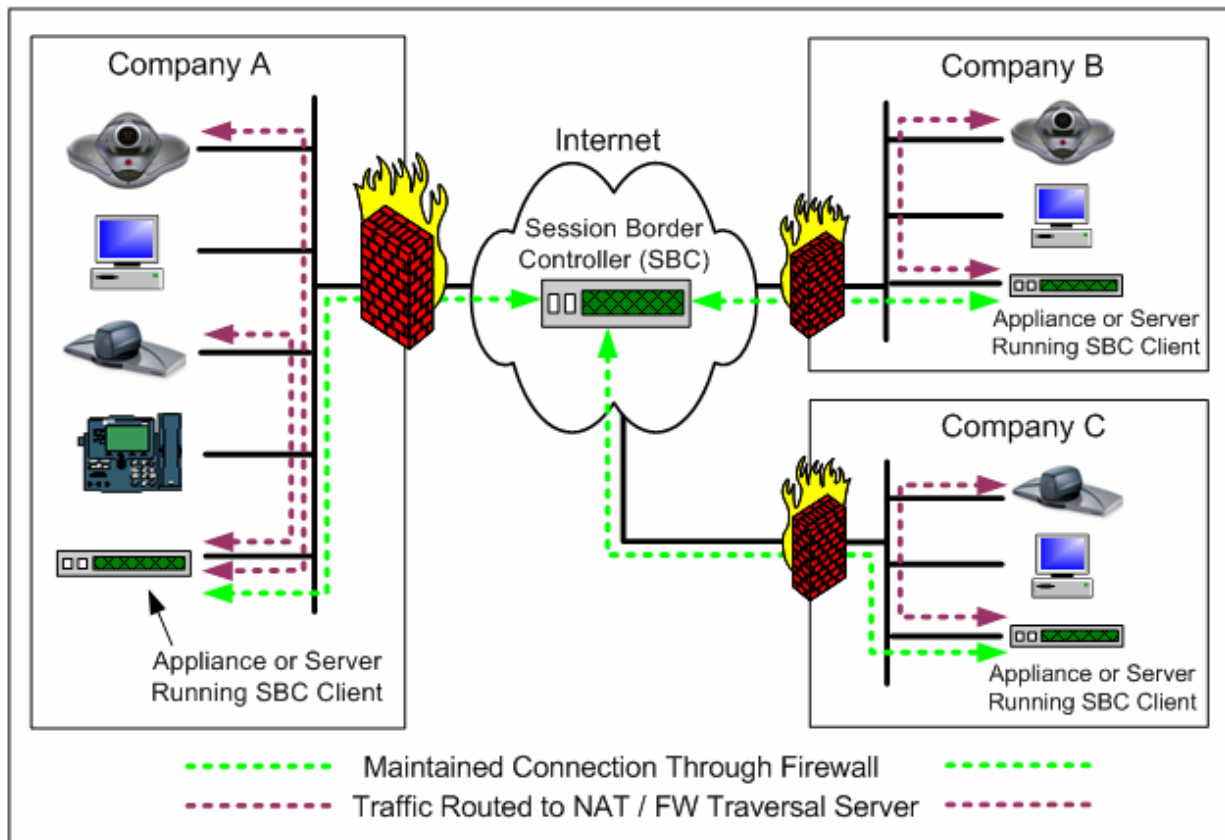


Figure 4: Typical Session Border Controller Deployment

In the Direct Packet STNS environment, the session border controllers are called Front End units (FEs) and the session border clients are called Back End units (BEs). All STNS enterprise products are rack-mountable appliances (either 1 RU or 2 RU high depending upon the model), and include several Ethernet ports (typically Gigabit ports) on the front or back of the unit. Each unit also includes a front panel LCD display which shows the device's current IP address.

Within our evaluation, we used the following STNS devices (which represent only a portion of the overall STNS product offering):

Model	Type	Capacity / Capability	List Price (US \$)
FE-200	Front End Controller	200 Back-End or Endpoint Registrations	\$31,990
BE-100	Back End Controller	100 Endpoint Registrations	\$14,990
BE-10	Back End Controller	10 Endpoint Registrations	\$4,990
REO	Back End Controller	1 Endpoint Registration	\$1,050

Figure 5: Direct Packet Appliance Systems Used During the Evaluation

Note that the STNS units used within the test environment were selected for illustration purposes only and were not “right-sized” for the test environment. For example, although we used an FE-200 during the testing, an FE-10 (list price \$9,990) could have met our capacity requirements for half the price.

Installing / Configuring the Front-End Unit

When the Direct Packet solution is in place, all firewall traversal traffic will flow through the FE units. As such, the FEs must be installed in network spaces that can be accessed by other STNS devices (and public endpoints in need of firewall traversal support) within the environment.

For most enterprises, the above means that the FEs will be installed in the network demilitarized zone (DMZ) or on the public Internet. For our evaluation, we installed an FE-200 in the “public” network. Installing the FE-200 took only a few minutes and involved the following steps:

- 1) Connecting a cross-over network cable between our notebook PC and the second Ethernet port on the FE. The second Ethernet port is a dedicated service port with a static IP address (set at the factory) that allows network administrators to easily monitor and configure the FE.
- 2) Setting our notebook PC to an IP address in the same subnet as the FE’s service port
- 3) Opening a browser window pointed at the IP address of the FE’s service port
- 4) Logging into the FE using the administrator login credentials
- 5) Accessing the Network menu on the user interface and setting the FE’s basic network information (system name, IP address, subnet mask, gateway, etc.).
- 6) Accessing the Networking / Enterprise Front End menu and clicking the “Start Listening” button to instruct the FE to accept connections from remote Back End units (see below).

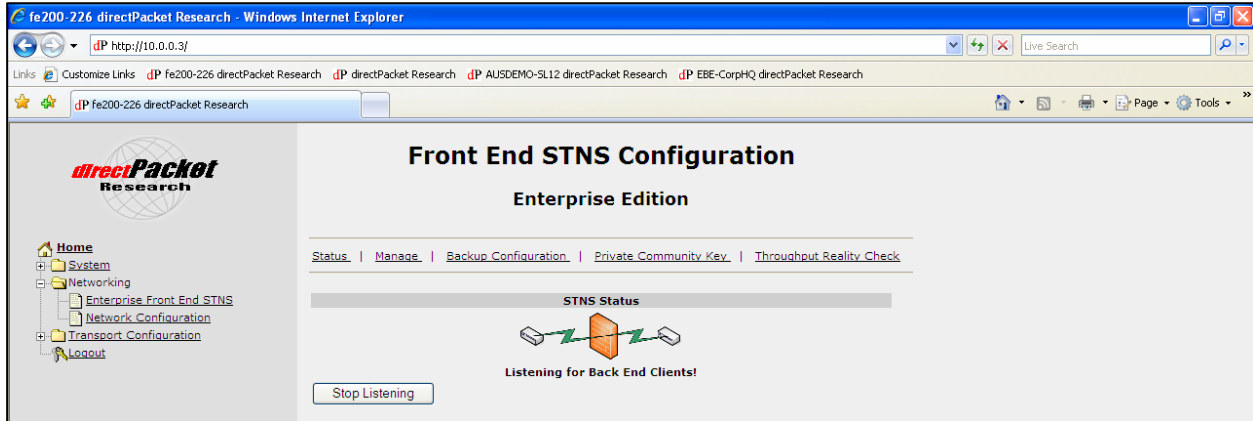


Figure 6: FE - Listening for Back End Units

Although there are additional options that users may wish to set within the UI (ex. restricting which Back End units and outside endpoints are allowed to register with the FE, restricting which IP addresses can be used for remotely managing the FE, creating additional users / accounts, etc.), the above basic steps were all we needed within our test environment.

Installing the Back-End Units

Once the FE was installed, we installed each back end unit by following steps 1 through 5 from the FE installation above. We then performed the following additional steps to configure / activate the gatekeeper functionality and create the traversal stream between each BE and the FE-100.

- 1) Accessing the Transport Configuration menu and entering the IP address of the FE.
- 2) Clicking the Connect button and waiting a few minutes for the system to confirm that a successful connection has been established between the BE and the FE (as shown below).

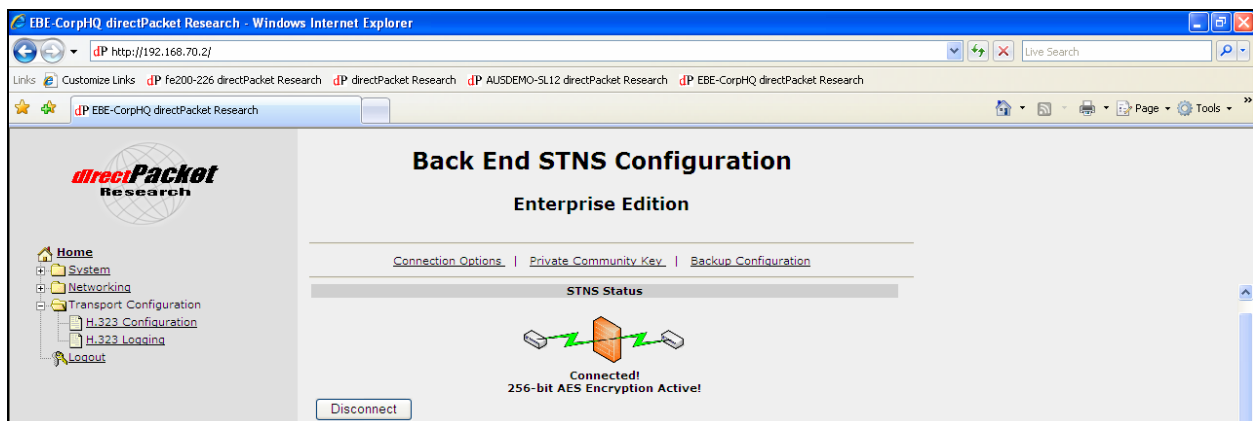
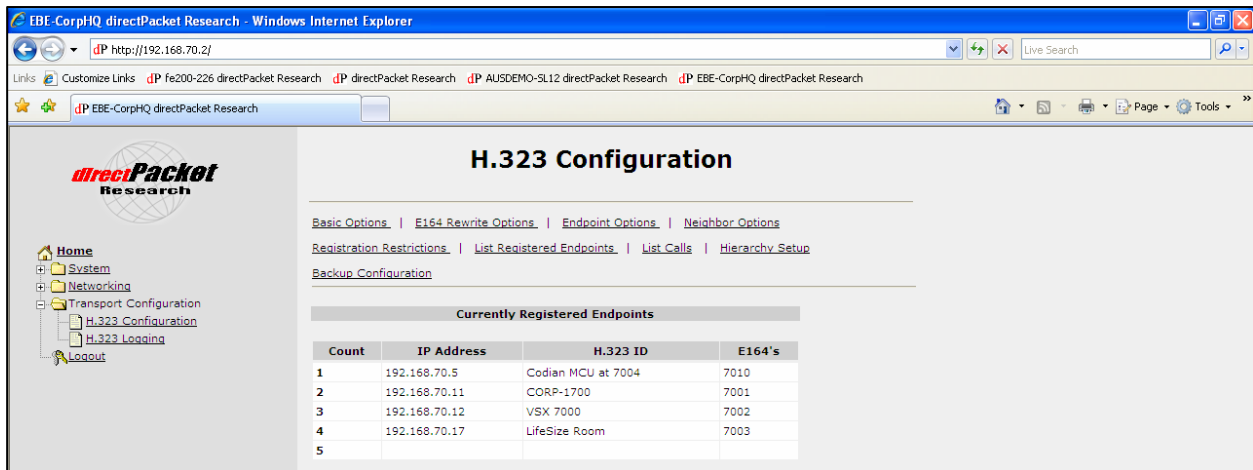


Figure 7: BE - Confirming Connection to the FE

c) Registering the Video Systems / Devices

Since we did not have any other gatekeepers in the test environment, we had to configure each device to register with the STNS gatekeeper; a process which took roughly 20 minutes for us to complete. Environments with existing gatekeepers would simply have to neighbor their gatekeepers with the STNS gatekeeper and would not have to modify the gatekeeper settings of each video device. We then accessed the Transport Configuration / H.323 Configuration / List Registered Endpoints section of each BE's UI to view the registered endpoints (see below).



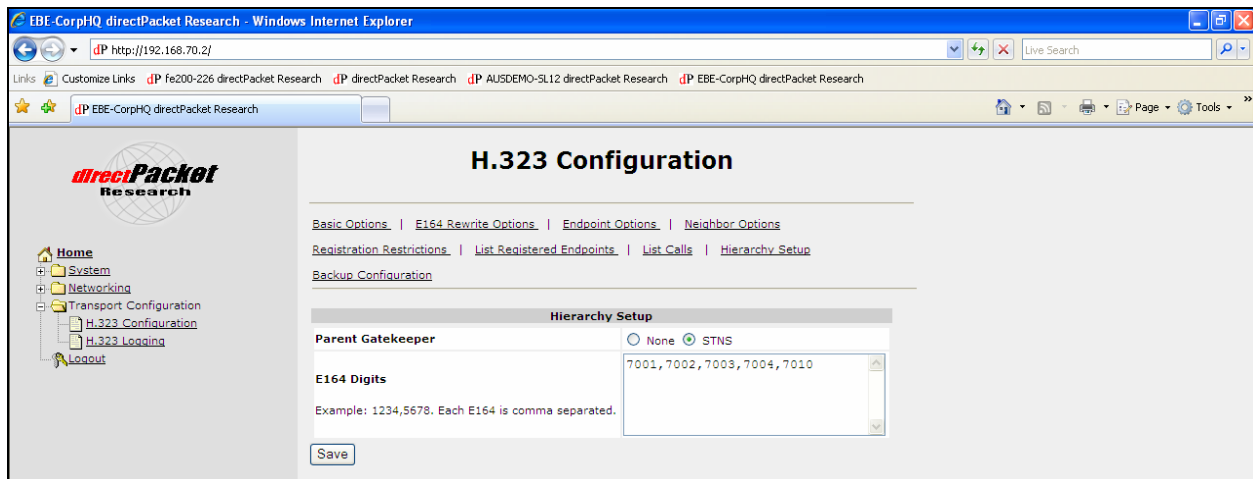
The screenshot shows the 'H.323 Configuration' page in a web browser. The page title is 'H.323 Configuration'. There are several navigation tabs: 'Basic Options', 'E164 Rewrite Options', 'Endpoint Options', 'Neighbor Options', 'Registration Restrictions', 'List Registered Endpoints', 'List Calls', and 'Hierarchy Setup'. The 'List Registered Endpoints' tab is selected. Below the navigation tabs is a table titled 'Currently Registered Endpoints'.

Count	IP Address	H.323 ID	E164's
1	192.168.70.5	Codian MCU at 7004	7010
2	192.168.70.11	CORP-1700	7001
3	192.168.70.12	VSX 7000	7002
4	192.168.70.17	LifeSize Room	7003
5			

Figure 8: BE - List of Endpoints Registered

d) Enabling Firewall Traversal

STNS allows administrators to specify within each Back End unit which systems / devices are allowed to traverse the firewall and call video systems in other network spaces (by default, none are allowed). Administrators can either enter the E.164 aliases of each system into an "allowed" list (see screenshot below in which devices 7001, 7002, 7003, 7004, and 7010 are authorized) or use an "Auto Configure" feature that automatically grants traversal rights to any device currently registered to the BE unit.



The screenshot shows the 'H.323 Configuration' page in a web browser. The page title is 'H.323 Configuration'. There are several navigation tabs: 'Basic Options', 'E164 Rewrite Options', 'Endpoint Options', 'Neighbor Options', 'Registration Restrictions', 'List Registered Endpoints', 'List Calls', and 'Hierarchy Setup'. The 'Hierarchy Setup' tab is selected. Below the navigation tabs is a form titled 'Hierarchy Setup'.

Hierarchy Setup

Parent Gatekeeper: None STNS

E164 Digits: 7001,7002,7003,7004,7010

Example: 1234,5678. Each E164 is comma separated.

Save

Figure 9: BE - Systems Authorized to Traverse the Firewall

Finally, we visited the FE-200's Transport Configuration / H.323 Configuration screen to confirm the overall installation. As shown below, the FE-200 was able to "see" all three BE units (and the devices registered to each of them), and the two endpoints and one MCU in the public network registered directly to the FE. This confirmed communication throughout our test environment.

The screenshot shows the 'H.323 Configuration' page in a web browser. The page title is 'H.323 Configuration' and it includes navigation links for 'Basic Options', 'E164 Rewrite Options', 'Endpoint Options', and 'Neighbor Options'. Below these are links for 'Registration Restrictions', 'List Registered Endpoints', 'List Calls', and 'Hierarchy Setup'. A 'Backup Configuration' link is also present. The main content area displays a table titled 'Currently Registered Endpoints' with the following data:

Count	IP Address	H.323 ID	E164's
1	10.0.0.11	Old512	502
2	10.0.0.21		505 100
3	STNS Back End Unit	EBE-CorpHQ	7001 7002 7003 7004 7010
4	STNS Back End Unit	AUSDEMO-SL12	2020 2022 2024 2025 2026 2027 2028 2029 303 304 305 6001 6010 99999 9999999
5	STNS Back End Unit	REO-WH-YAURQ	101
6	10.0.0.10	VegaX3	501
7			

Figure 10: FE - View of All Registered Devices in the Environment

Time / Expertise Required

It took roughly 15 minutes to install and configure the FE-200, and 10 minutes to install each back end unit. Including registering each endpoint with the STNS gatekeeper, the total installation took roughly an hour to complete. WR believes that given a short tutorial on the SBC / STNS architecture, the basic installation and configuration of this solution could be completed by almost any network administrator.

STNS Evaluation

Part 1 – Dial-Out Testing

For this part of the evaluation, WR conducted a round-robin of more than 50 calls between the systems and devices in the test environment. The calls were chosen such that each device's ability to place and receive calls to systems in its own and in the other network spaces was tested.

For detailed call information, please see calls HQ-1 to HQ-23, Branch-1 to Branch-20, SOHO-1 to SOHO-11, and Public-1 to Public-18 in the Test Call Results in the Appendix.

Test Results:

- 1) ALL calls placed to devices within the same network zone were successful (as was the case before the STNS system was installed)
- 2) ALL calls placed to devices within a different network zone were successful. Note that these calls consistently failed prior to the installation of the STNS solution (see the Baseline Testing section for details).
- 3) All devices, whether local (within the same network segment) or external (in a different network segment), were addressable by their E.164 aliases. It was NOT necessary to use IP addresses or different dialing commands (prefixes, suffixes, extensions, etc.) at any time.
- 4) The use of the STNS firewall traversal solution appeared to have no effect on the video connection in terms of:
 - a. Interoperability between vendors
 - b. Bandwidth / call speed
 - c. Call quality / experience
 - d. Encryption support
 - e. Video protocols available / used
 - f. Video resolutions available / used
 - g. Audio protocols available / used
 - h. Other capabilities (ex. ability to use DTMF or FECC to select meetings on MCUs)

***The STNS solution resolved the
NAT / firewall issues within our test
environment seamlessly.***

In other words, the STNS solution resolved the firewall / NAT issues in the environment seamlessly and without adversely impacting the overall call quality and user experience.

Part 2 – H.239 Testing

As an add-on to the general connectivity testing in Part 1 above, WR tested the support for H.239 / dual stream signals with the test environment.

1) HQ Testing

This test was conducted after connecting and documenting calls HQ13 – HQ21 (all endpoints connected to the Codian 4200 MCU) and using the Tandberg 1700MXP (in the CorpHQ network) connected to an XGA signal as the H.239 signal source.

The following endpoints were able to successfully receive the H.239 signal in native resolution:

Corp HQ Network: Tandberg 1700MXP, Polycom VSX-7000, LifeSize Room
Branch Network: Polycom VSX-3000, Tandberg 880MXP, Sony G-50
Public Network: Aethra V3

The remaining endpoints (Tandberg 1000 and Polycom ViewStation) do not support H.239.

2) Branch Testing

This test was conducted after connecting and documenting calls Branch12 – 20 (all endpoints connected to the Tandberg MPS MCU) using the Tandberg 1700MXP (in the CorpHQ network) connected to an XGA signal as the H.239 signal source.

The following endpoints were able to successfully receive the H.239 signal in native resolution:

Corp HQ Network: Tandberg 1700MXP, Polycom VSX-7000, LifeSize Room
Branch Network: Polycom VSX-3000, Tandberg 880MXP, Sony G-50
Public Network: Aethra V3

The remaining endpoints (Tandberg 1000 and Polycom ViewStation) do not support H.239.

3) SOHO Testing

To facilitate the H.239 testing to the SOHO network, WR replaced the Tandberg 1000 (which did not have the H.239 option installed) in the SOHO network with a Polycom HDX-9000. After call SOHO-11 was connected and documented, WR added the H.239 signal source (the Tandberg 1700MXP in the CorpHQ network) to the meeting on the Codian MCU and activated H.239.

The result was that the Polycom HDX in the SOHO network was able to participate in the H.239 call and receive the H.239 signal in native resolution.

According to our test results, the STNS solution fully supports H.239 / dual stream video during firewall traversal calls.

4) Public Testing

This test was conducted after connecting and documenting calls Public-10 – 20 (all endpoints connected to the Polycom MGC-50 MCU) using the Tandberg 1700MXP (in the CorpHQ network) connected to an XGA signal as the H.239 signal source.

The following endpoints were able to successfully receive the H.239 signal in native resolution:

Corp HQ Network:	Tandberg 1700MXP (source), Polycom VSX-7000
Branch Network:	Polycom VSX-3000, Tandberg 880MXP

The remaining endpoints (Tandberg 1000, Polycom ViewStation, and LifeSize Room) either do not support H.239 or could not participate in an H.239 session hosted by the Polycom MGC-50 (due to interoperability issues unrelated to this evaluation).

Part 3 – IP to IP Gateway Testing

This part of the evaluation tested the ability to dial out to public endpoints that are NOT registered to the enterprise gatekeepers. In the STNS environment, calls to external non-registered endpoints require the use of the “@” symbol before the IP address (ex. a call to @10.0.0.50 is a call to an external endpoint with IP address 10.10.0.50).

For this testing, WR moved two of the test endpoints (the Polycom VSX-7000 and the Tandberg 880MXP) to the public network and did NOT allow them to register to the STNS gatekeeper. From a networking perspective, these endpoints now appeared to the STNS system as external endpoints. For detailed call information, please see calls Misc-1 through Misc-10 in the Test Call Results in the Appendix.

Test Results - As shown, calls from each of the four network segments to the “external” endpoints worked perfectly, confirming the STNS gateway’s support for various call speeds, encryption, video and audio protocols, and resolutions.

Part 4 – Video Auto Attendant (AA) Testing

This part of the evaluation tested a feature called the Video Auto Attendant that allows external (unregistered) devices to reach internal devices by dialing and connecting to the Front End unit and entering the destination device’s E.164 address using DTMF tones.

By default, Auto Attendant is disabled throughout the environment. To allow internal devices to be reached via the Auto Attendant, administrators enter the E.164 addresses of those devices into the Transport Configuration / Video Auto Attendant screen on the FE unit. In the screenshot below, 10 different systems (101, 7001, 6001, etc.) can be reached via the Auto Attendant. Administrators also have the option of adding all known extensions (all systems that have registered with the system in the past) to the list of allowed Auto Attendant extensions.

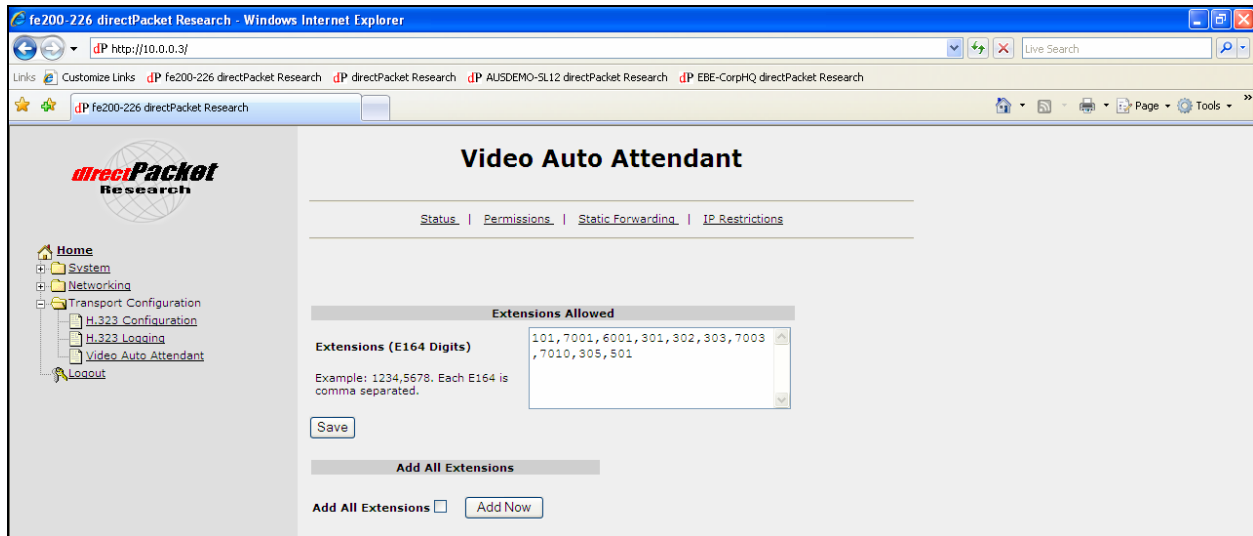


Figure 11: FE - Video Auto Attendant Permissions

The Auto Attendant function supports only basic connectivity (H.323, 384 kbps max, H.263 video and G.711 audio only). Although encryption is supported during Auto Attendant calls, H.239 is not.

As shown in the test call results (see calls Misc-11 through Misc-25 in the Test Call Results in the Appendix), the results of the Video Auto Attendant testing were mixed. Specifically, while the majority of Video Auto Attendant calls worked as advertised, calls involving any Tandberg system using Tandberg's F6.0 software (current as of this writing) failed. WR then downgraded the software version of the Tandberg endpoints to version F5.3, which resolved the problem. According to Direct Packet (but not verified by Tandberg or tested by WR), software version F6.1 resolves this issue.

Overall, and aside from the Tandberg issue, the Video Auto Attendant worked as advertised. However, with its current limitations in bandwidth and protocol support, the utility of this feature is limited. Given a capability overhaul, the Video Auto Attendant feature could be a VERY useful value-add offered by the STNS solution.

Part 5 – HTTP / Web Proxy Testing

Some organizations use proxies to limit access to the Internet, to control the usage of specific services or protocols, or to track user behavior. For example, a proxy might be used to block access to inappropriate websites or monitor and track web activity. Because the STNS solutions uses SSLv3 on port 443 by default, the ability to communicate and authenticate with HTTP / web proxies is an additional value-add offered by this platform.

To evaluate this functionality, WR activated the integrated web proxy function on the Microsoft ISA firewall to test the STNS system's ability to function in conjunction with an Internet proxy. We then activated proxy support via the Transport Configuration menu on the BE supporting the Branch network.

Proxy Test #1 - Authentication with Base 64 Encoding

For this test, WR activated the web proxy service on the Microsoft ISA firewall using Base 64 encoded authentication. After entering the proper password into the proxy settings of the BE, we then placed a number of test calls within the branch network and between the branch network and other network zones.

Test Results - In all cases, the test calls worked properly.

Proxy Test #2 - Authentication with IWA (Integrated Windows Authentication) / NTLM

For the second part of the proxy test, we re-configured the ISA proxy to require IWA / NTLM authentication. We then updated the settings on the BE unit supporting the Branch Network and placed additional test calls within the branch network and between the branch network and other network zones.

Test Results - In all cases, the test calls worked properly.

The above test results confirm that STNS is able to provide NAT / firewall traversal services successfully, even for environments using web proxies (with Base64 or IWA / NTLM authentication requirements).

It is worth pointing out that although supported by STNS, because of the potential for increased latency, as a general rule the use of HTTP / web proxies to manage real-time traffic (ex. video conferencing, VoIP traffic) is not recommended.

Summary of Test Results

Overall, Direct Packet's STNS solution performed exceptionally well during our testing and provided seamless NAT / Firewall traversal within our test environment.

Primary Strengths:

1) Exceptional Interoperability

STNS works with any standards-based videoconferencing system / device able to register to a system gatekeeper. Our testing verified interoperability with Polycom, Tandberg (minor issue noted – see above), LifeSize, Sony, and Aethra. Also, the solution works with both current and legacy devices.

2) Use of a Single Network Port

By design, H.323 videoconferencing requires access to a range of more than 65,000 dynamic network ports. The recently ratified H.460 standard decreases the number of required network ports to four. STNS, however, requires only a single network port.

3) Use of a Typically "Open" Network Port

Understandably, network administrators are reluctant to compromise security by opening ports on the firewall. Not only does STNS utilize only a single network port, by default it uses port 443; a port typically open on most firewalls to allow secure HTTP / Internet traffic. This means that in many cases, STNS can be installed without the need to open any additional firewall ports.

It is also worth pointing out that as a part of sending traffic through port 443, STNS actually encapsulates the call traffic (audio, video, data, etc.) into an encrypted SSL v3 stream. This conversion to SSL provides several benefits including a) an additional level of security, b) decreased burden on the firewall since firewalls know to not perform deep packet inspection on SSL traffic, and c) improved control through the use of TCP (a data transmission protocol that provides flow control and error correction) instead of the UDP protocol.

4) Transparent Operation

STNS does not interfere with the capabilities exchange or protocols / resolutions used by the participating video systems. This evaluation confirmed support for encryption and the following protocols / resolutions during traversal calls:

Video Protocols - H.263, H.264

Video Resolutions - QCIF, CIF / SIF, 288p, 400p, 448p, 2SIF, 4CIF / 4SIF, VGA

Audio Protocols – G.722, Siren-14, AAC-LC, AAC-LD

5) Auto Attendant

Although not heavily touted by Direct Packet and in need of some enhancement, WR believes that STNS's Video Auto Attendant function is actually a diamond in the rough as it allows external endpoints to call internal video systems without having to register on the enterprise gatekeepers.

Other Strengths:

- Appliance-Based Architecture
- Exceptional System Security - user-based permissioning, ability to limit remote access, system for creating security keys for authorizing BE to FE streams, etc.
- Fail-Safe Operation - if power is lost, the BE units re-connect to the FE automatically
- Multiple Ethernet Ports - allows the use of FE and BE units on several networks simultaneously
- Dedicated Service Port
- Eliminates Need for H.460 Support in Devices – allows use of legacy devices in the environment without having to install a dedicated gatekeeper.
- Very Strong Reliability
- Straight-Forward User Interface
- IP to IP Gateway
- Support for Web Proxy Environments

Primary Weaknesses:

1) Appliance Required in Each Network Zone

To provide firewall traversal services, STNS requires the installation of a dedicated appliance behind the firewall in each location. For enterprises with only a few systems in need of traversal support, this method can be expensive (although STNS devices supporting as few as a single endpoint / device are available). Alternative methods used by competitors, each with pros and cons, include:

- a) Using gatekeepers in each network location (can be expensive for small deployments)
- b) Requiring H.460 support across the enterprise (may require equipment upgrades)

2) No Support for H.460

In fairness, lack of compliance with the H.460 standard is both a strength and a weakness. A big part of the power of this offering (single port functionality, exceptional interoperability, support for both current and legacy devices, etc.) stems from its deviation from the H.460 standards. However, H.460 clients are embedded in many current-generation video systems, which can decrease the cost of traversing the firewall in some situations. In addition, H.460 is an international standard for H.323 NAT / firewall traversal and is often included in many RFIs and RFPs.

Other Weaknesses:

- Auto Attendant Limitations – speeds, protocols supported, etc.
- Limited Bandwidth Support on the REO (single-endpoint BE unit)
- Limited On-Screen Help – a minor point since the system is somewhat self-explanatory
- Time required to initially establish streams between the BE and FE can be up to 120 seconds. This has no impact on the video calls themselves, but was longer than expected (fortunately this is not something administrators must do on a regular basis)

The WR Wish List:

- Enhanced Video Auto Attendant functionality (support for H.264, higher bandwidth, etc.)
- Support for notifications (emails, text messages) as new BE units register on an FE
- Easier access to some commands / capabilities. For example, the “turn gatekeeper on” function on a BE unit is accessible only after one saves the network configuration settings. Ideally the interface would include a “turn gatekeeper on / off” button.
- Expanded front-panel LCD functionality. Currently, the front panel LCD only shows the IP address of the system. WR suggests adding front-panel control buttons and the ability to activate / de-activate functions, view statistics (# of devices connected, status of BE / FE stream, etc.).

About Wainhouse Research

Wainhouse Research (www.wainhouse.com) is an independent market research firm that focuses on critical issues in rich media communications and conferencing. The company conducts multi-client and custom research studies, consults with end users on key implementation issues, publishes white papers and market statistics, and delivers public and private seminars as well as speaker presentations at industry group meetings. Wainhouse Research publishes Conferencing Markets & Strategies, a three-volume study that details the current market trends and major vendor strategies in the multimedia networking infrastructure, endpoints, and services markets, as well as a variety of segment reports, the free newsletter The Wainhouse Research Bulletin, and the PLATINUM (www.wrplatinum.com) content website.

About the Author(s)

Ira M. Weinstein is a Senior Analyst and Partner at Wainhouse Research, and a 15-year veteran of the conferencing, collaboration and audio-visual industries. Prior to joining Wainhouse Research, Ira was the VP of Marketing and Business Development at IVCi, managed a technology consulting company, and ran the global conferencing department for a Fortune 50 investment bank. Ira's current focus includes IP video conferencing, network service providers, global management systems, scheduling and automation platforms, ROI and technology justification programs, and audio-visual integration. Mr. Weinstein holds a B.S. in Engineering from Lehigh University and can be reached at iweinstein@wainhouse.com.

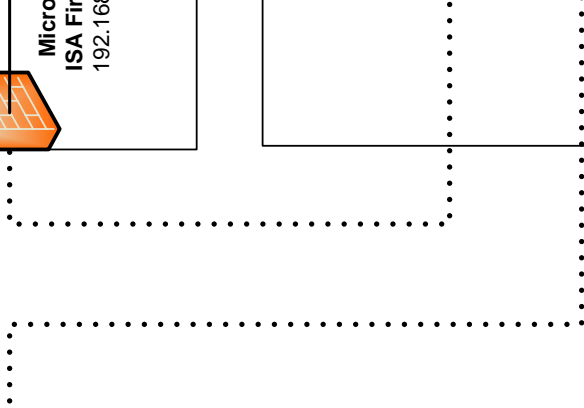
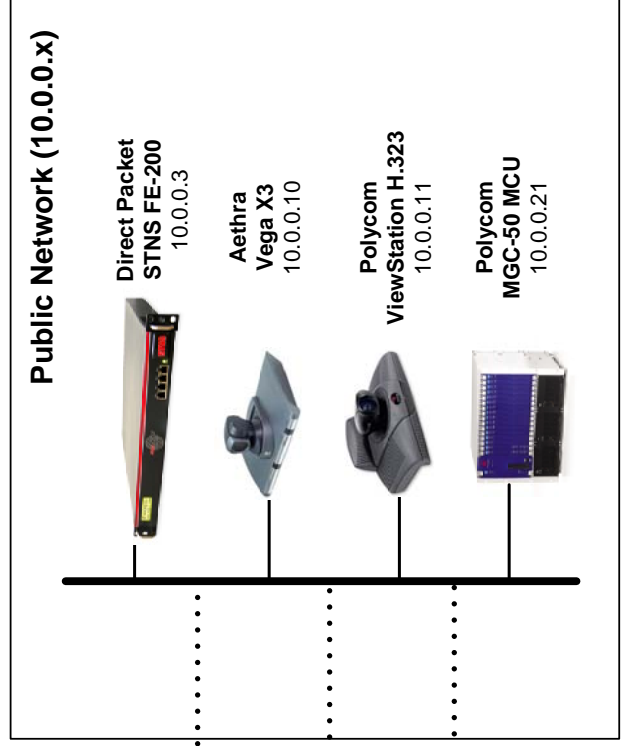
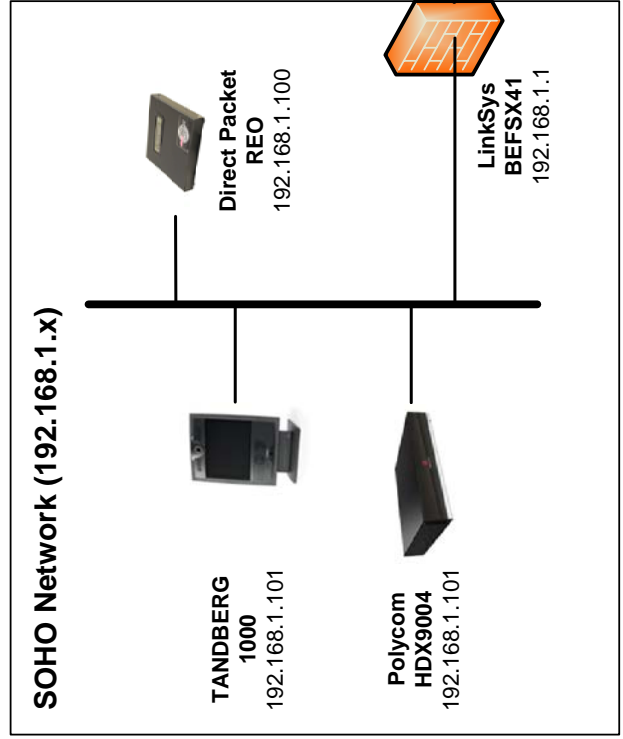
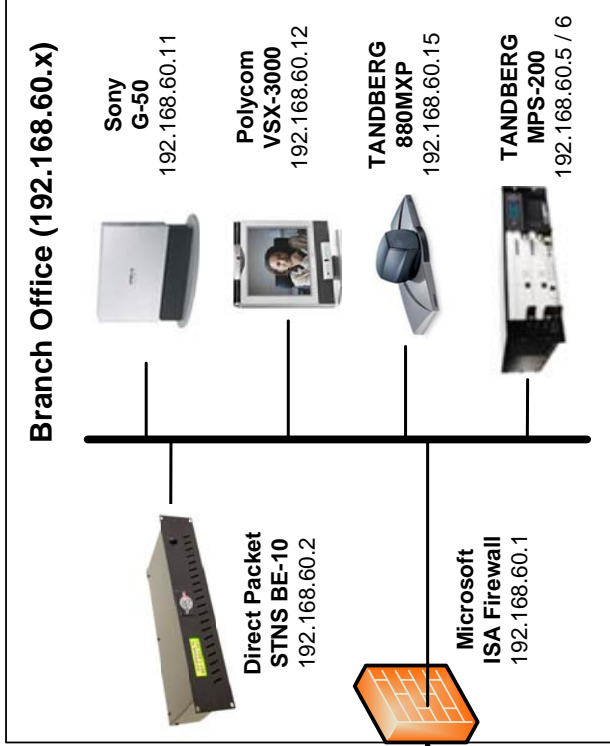
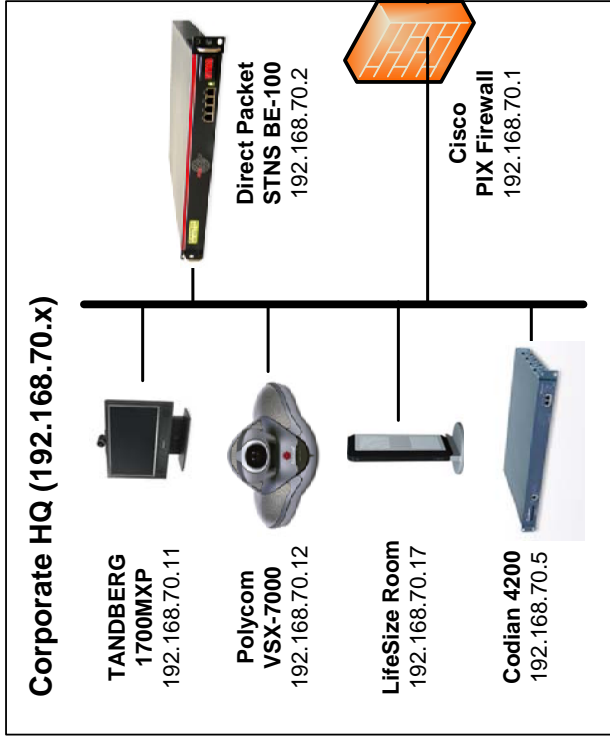
About Direct Packet Research

Direct Packet Research develops IP voice and video communication technology emphasizing security and interoperability.

Our feature-rich infrastructure products excel in multi-vendor environments providing our customers the greatest protection from obsolescence, unsurpassed flexibility, and a low total solution cost. Our dedication to endpoint and network room compatibility has driven success in healthcare, education, enterprise and government sectors including security-critical networks within the Federal Government, Department of Defense contractors and high-security research institutions.

Direct Packet Research is a privately held company based in Dallas, Texas. More information is available at www.directpacket.com.

Appendix A – Network Diagram



Appendix B – Equipment Information

The tables below provide addition information about the devices used during the evaluation.

1) Corporate HQ Network Space

(IP Range: 192.168.70.X, Subnet 255.255.255.0, Gateway 192.168.70.1)

Manufacturer	Model	E.164 Alias	IP Address	Software Rev.
Polycom	VSX-7000	7002	192.168.70.12	8.7
LifeSize	Room	7003	192.168.70.17	LS_RM1_2.6.3(2)
Tandberg	1700MXP	7001	192.168.70.11	F6.0 NTSC, Security
Codian	MCU 4200	7010	192.168.70.5	2.1 (1.3)
Direct Packet	BE-100		192.168.70.2	
Cisco	PIX Firewall		192.168.70.1	

2) Branch / Divisional Network Space

(IP Range: 192.168.60.X, Subnet 255.255.255.0, Gateway 192.168.60.1)

Manufacturer	Model	E.164 Alias	IP Address	Software Rev.
Sony	G-50	305	192.168.60.11	Host: 02.5 / DSP 03.56
Polycom	VSX-3000	303	192.168.60.12	8.7
Tandberg	880-MXP	304	192.168.60.15	F6.0 NTSC, Security
Direct Packet	BE-10		192.168.60.2	
Microsoft	ISA Firewall		192.168.60.1	

3) SOHO Network Space

(IP Range: 192.168.1.X, Subnet 255.255.255.0, Gateway 192.168.1.1)

Manufacturer	Model	E.164 Alias	IP Address	Software Rev.
TANDBERG*	1000	101	192.168.1.102	E5.3 NTSC
Polycom *	HDX-9000	101	192.168.1.102	1.0.2 – 354
Direct Packet	REO		192.168.1.100	
LinkSys	BEFSX41		192.168.1.1	

* Only 1 of the above endpoints was connected in the SOHO network at a time.

4) Public Network Space

(IP Range: 10.0.0.X, Subnet 255.255.255.0, Gateway 10.0.0.254)

Manufacturer	Model	E.164 Alias	IP Address	Software Rev.
Aethra	X3	501	10.0.0.10	10.02.0014
Polycom	ViewStation H.323	502	10.0.0.11	7.5.4
Polycom	MGC-50	505 / 100	10.0.0.121	8.0.0.27
Direct Packet	FE-200		10.0.0.3	

Additional Equipment Notes

1) Polycom ViewStation

This evaluation included three generations of Polycom video systems; the HDX line, the VSX line, and the original ViewStation line. The ViewStation used for this testing supported a maximum of 768 kbps of IP bandwidth, and did NOT support H.264, H.239, or encryption.

2) Tandberg 1000

This evaluation also included three generations of Tandberg video systems; the HD-capable line, the original MXP line, and the non-MXP line. The Tandberg 1000 used for this testing did NOT support H.239 (although the device is capable of supporting this feature, the option code was not installed).

3) Codian 4200 MCU

Throughout the testing, the Codian MCU was set for balanced motion / sharpness. As a result, many of the connections from the MCU to the endpoints used 4CIF resolution.

4) Tandberg MPS-200 MCU

The MPS does NOT support an “encrypt if possible” mode. For this reason, and because the MPS is unable to establish encrypted connections to some of the endpoints within the environment, encryption was disabled for all MPS test calls.

5) Direct Packet REO

Intended to support the basic needs of a home-user or SOHO environment, the REO supports call speeds of up to 384 kbps only. For this reason, calls to / from the SOHO network were always placed at (or below) this 384 kbps limit.

6) Microsoft ISA Firewall

Due to processor limitations on the host server utilized, the Microsoft ISA firewall used during this evaluation was capable of supporting a throughput of approximately 1 Mbps.

7) Firewalls

All 3 firewalls (Cisco PIX, Microsoft ISA, Linksys BEFSX41) were set to allow only “establish / related” HTTP (port 80) and HTTPS / SSL (port 443) traffic. For example, the Cisco PIX access list included only two rules: 1) https any out (443) and 2) www any out (80). These settings were chosen to ensure that the security in the test environment was at least as restrictive as the typical enterprise.

8) Gatekeeper

For this evaluation, we had each of the endpoints and MCUs register to the gatekeeper embedded in the Direct Packet device within its local network. This allowed the use of E.164 dialing throughout the environment without the need to install 3rd party gatekeepers. Organizations deploying these solutions have two options; 1) register their devices directly to the gatekeepers within the Direct Packet appliances (tested within this evaluation), or 2) use 3rd party gatekeepers (available from Polycom, Radvision, Tandberg, etc.) and neighbor those gatekeepers to the locally deployed Direct Packet device(s).

Appendix C – Test Call Results

The sheets that follow include detailed information about the test calls performed by Wainhouse Research during the evaluation of the Direct Packet STNS firewall traversal solution.

Direct Packet STNS Call Testing

Call Configuration			Traversal?	Call Request		Call Results		Actual Outgoing Stats			Actual Incoming Stats		
Call #	From	To		BW	Encrypt	BW	Encrypt	V Protocol	Resol	A Protocol	V Protocol	Resol	A Protocol
Dial-Out Testing from the Corporate HQ Network													
HQ-1	CorpHQ - TANDBERG 1700 MXP (7001)	CorpHQ - Polycom VSX-7000 (7002)	No	384	Yes	384	Yes	H.264	CIF (352x288)	G.722	H.264	SIF (352x240)	G.722
HQ-2	CorpHQ - TANDBERG 1700 MXP (7001)	CorpHQ - LifeSize Room (7003)	No	768	Yes	768	Yes	H.264	448p (576x448)	G.722	H.264	w400p (720x400)	G.722
HQ-3	CorpHQ - Polycom VSX-7000 (7002)	CorpHQ - LifeSize Room (7003)	No	1M	Yes	1M	Yes	H.263	CIF (352x288)	Siren-14	H.263	CIF (352x288)	Siren-14
HQ-4	CorpHQ - TANDBERG 1700 MXP (7001)	Branch - Sony G-50 (305)	Yes	768	Yes	768	Yes	H.264	CIF (352x288)	G.722	H.264	CIF (352x288)	G.722
HQ-5	CorpHQ - Polycom VSX-7000 (7002)	Branch - Sony G-50 (305)	Yes	512	Yes	512	Yes	H.264	SIF (352x240)	G.722	H.263	CIF (352x288)	G.722
HQ-6	CorpHQ - LifeSize Room (7003)	Branch - TANDBERG 880-MXP (304)	Yes	384	Yes	384	Yes	H.264	w400p (720x400)	G.722	H.264	400p (528x400)	G.722
HQ-7	CorpHQ - Polycom VSX-7000 (7002)	Branch - TANDBERG 880-MXP (304)	Yes	1M	Yes	1M	Yes	H.263+	CIF (352x288)	G.722	H.263+	SIF (352x240)	G.722
HQ-8	CorpHQ - LifeSize Room (7003)	Branch - Polycom VSX-3000 (303)	Yes	768	Yes	768	Yes	H.264	SIF (352x240)	Siren-14	H.264	SIF (352x240)	Siren-14
HQ-9	CorpHQ - LifeSize Room (7003)	SOHO - TANDBERG 1000 (101)	Yes	384	Yes	384	Yes	H.264	QCIF (176x144)	G.722	H.264	CIF (352x288)	G.722
HQ-10	CorpHQ - TANDBERG 1700 MXP (7001)	Public - Aethra Vega X3 (501)	Yes	1152	Yes	1152	Yes	H.263+	CIF (352x288)	AAC-LD	H.263+	SIF (352x240)	AAC-LD
HQ-11	CorpHQ - Polycom VSX-7000 (7002)	Public - Polycom ViewStation (502)	Yes	512	No	512	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
HQ-12	CorpHQ - LifeSize Room (7003)	Public - Polycom ViewStation (502)	Yes	768	No	768	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
HQ-13	CorpHQ - Codian MCU 4200 (7010)	CorpHQ - TANDBERG 1700 MXP (7001)	No	2M	Yes	2M	Yes	H.263+	w4CIF (1024x576)	AAC-LD	H.264	w448p (768x448)	AAC-LD
HQ-14	CorpHQ - Codian MCU 4200 (7010)	CorpHQ - Polycom VSX-7000 (7002)	No	2M	Yes	2M	Yes	H.263+	4CIF (704x576)	Siren-14	H.263+	CIF (352x288)	Siren-14
HQ-15	CorpHQ - Codian MCU 4200 (7010)	CorpHQ - LifeSize Room (7003)	No	2M	Yes	2M	Yes	H.263+	720p (1280x720)	Siren-14	H.264	624x352	Siren-14
HQ-16	CorpHQ - Codian MCU 4200 (7010)	Branch - Polycom VSX-3000 (303)	Yes	384	Yes	384	Yes	H.263+	4CIF (704x576)	Siren-14	H.264	SIF (352x240)	Siren-14
HQ-17	CorpHQ - Codian MCU 4200 (7010)	Branch - TANDBERG 880-MXP (304)	Yes	384	Yes	384	Yes	H.263+	w288p (512x288)	AAC-LD	H.264	SIF (352x240)	AAC-LD
HQ-18	CorpHQ - Codian MCU 4200 (7010)	Branch - Sony G-50 (305)	Yes	384	Yes	384	Yes	H.263	4CIF (704x576)	AAC-LC	H.264	CIF (352x288)	AAC-LC
HQ-19	CorpHQ - Codian MCU 4200 (7010)	SOHO - TANDBERG 1000 (101)	Yes	384	Yes	384	Yes	H.263	VGA (640x480)	G.722	H.264	SIF (352x240)	G.722
HQ-20	CorpHQ - Codian MCU 4200 (7010)	Public - Aethra Vega X3 (501)	Yes	2M	Yes	2M	Yes	H.263+	4CIF (704x576)	G.722	H.263+	SIF (352x240)	G.722
HQ-21	CorpHQ - Codian MCU 4200 (7010)	Public - Polycom ViewStation (502)	Yes	768	No	768	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
HQ-22	CorpHQ - Polycom VSX-7000 (7002)	SOHO - Polycom HDX-9000 (101)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722.1C	H.264	SIF (352x240)	G.722.1C
HQ-23	CorpHQ - LifeSize Room (7003)	SOHO - Polycom HDX-9000 (101)	Yes	384	Yes	384	Yes	H.264	4SIF (704x480)	G.722.1C	H.264	VGA (640x480)	G.722.1C

NOTES:

To verify dial-in capability to the Codian 4200 MCU located in the Corp HP network, for calls HQ-13 through HQ-21, each endpoint was disconnected from the MPT call and then dialed back in to the MCU directly.

In the case of the Codian 4200 MCU, each endpoint dialed the E.164 ID of the multi-point meeting.

Although the detailed call statistics were not documented, bi-directional video and audio were tested and no issues were noted.

Direct Packet STNS Call Testing

Call Configuration			Traversal?	Call Request		Call Results		Actual Outgoing Stats			Actual Incoming Stats		
Call #	From	To		BW	Encrypt	BW	Encrypt	V Protocol	Resol	A Protocol	V Protocol	Resol	A Protocol
Dial-Out Testing from the Branch Network													
Branch-1	Branch - Polycom VSX-3000 (303)	Branch - TANDBERG 880-MXP (304)	No	1152	Yes	1152	Yes	H.263	CIF (352x288)	G.722	H.263	SIF (352x240)	G.722
Branch-2	Branch - Polycom VSX-3000 (303)	Branch - Sony G-50 (305)	No	768	Yes	768	Yes	H.264	SIF (352x240)	G.722	H.263	CIF (352x288)	G.722
Branch-3	Branch - TANDBERG 880-MXP (304)	Branch - Sony G-50 (305)	No	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	CIF (352x288)	G.722
Branch-4	Branch - Polycom VSX-3000 (303)	CorpHQ - TANDBERG 1700 MXP (7001)	Yes	512	Yes	512	Yes	H.264	SIF (352x240)	G.722	H.264	4CIF (704x576)	G.722
Branch-5	Branch - TANDBERG 880-MXP (304)	CorpHQ - Polycom VSX-7000 (7002)	Yes	768	Yes	768	Yes	H.263+	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
Branch-6	Branch - Sony G-50 (305)	CorpHQ - LifeSize Room (7003)	Yes	1M	Yes	1M	Yes	H.264	CIF (352x288)	G.722	H.264	CIF (352x288)	G.722
Branch-7	Branch - Polycom VSX-3000 (303)	Soho - TANDBERG 1000 (101)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
Branch-8	Branch - Sony G-50 (305)	Soho - TANDBERG 1000 (101)	Yes	256	Yes	256	Yes	H.263	4CIF (704x576)	G.722	H.264	SIF (352x240)	G.722
Branch-9	Branch - TANDBERG 880-MXP (304)	Public - Aethra Vega X3 (501)	Yes	512	Yes	512	Yes	H.264	SIF (352x240)	AAC-LD	H.264	SIF (352x240)	AAC-LD
Branch-10	Branch - Sony G-50 (305)	Public - Polycom ViewStation (502)	Yes	768	No	768	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Branch-11	Branch - Polycom VSX-3000 (303)	Public - Aethra Vega X3 (501)	Yes	1M	Yes	1M	Yes	H.263	SIF (352x240)	G.722	H.263	SIF (352x240)	G.722
Branch-12	Branch - TANDBERG MPS 200 (6010)	Branch - Polycom VSX-3000 (303)	No	768	No	768	No	H.263	4CIF (704x576)	G.722	H.263	SIF (352x240)	G.722
Branch-13	Branch - TANDBERG MPS 200 (6010)	Branch - TANDBERG 880-MXP (304)	No	2M	No	768	No	H.263	4CIF (704x576)	AAC-LD	H.263+	SIF (352x240)	AAC-LD
Branch-14	Branch - TANDBERG MPS 200 (6010)	Branch - Sony G-50 (305)	No	2M	No	768	No	H.263	4CIF (704x576)	G.722	H.263+	CIF (352x288)	G.722
Branch-15	Branch - TANDBERG MPS 200 (6010)	CorpHQ - TANDBERG 1700 MXP (7001)	No	384	No	384	No	H.263	4CIF (704x576)	AAC-LD	H.263+	CIF (352x288)	AAC-LD
Branch-16	Branch - TANDBERG MPS 200 (6010)	Soho - TANDBERG 1000 (101)	No	384	No	384	No	H.263	4CIF (704x576)	G.722	H.263+	SIF (352x240)	G.722
Branch-17	Branch - TANDBERG MPS 200 (6010)	Public - Aethra Vega X3 (501)	No	384	No	384	No	H.263	4CIF (704x576)	AAC-LD	H.263+	SIF (352x240)	AAC-LD
Branch-18	Branch - TANDBERG MPS 200 (6010)	Public - Polycom ViewStation (502)	No	128	No	128	No	H.263	QCIF (176x144)	G.728	H.263	CIF (352x288)	G.728
Branch-19	Branch - TANDBERG MPS 200 (6010)	CorpHQ - LifeSize Room (7003)	No	256	No	256	No	H.263	4CIF (704x576)	G.722	H.263	CIF (352x288)	G.722
Branch-20	Branch - TANDBERG MPS 200 (6010)	CorpHQ - Polycom VSX-7000 (7002)	No	256	No	256	No	H.263	QCIF (176x144)	G.722	H.263	SIF (352x240)	G.722.1

NOTES:

To verify dial-in capability to the MPS-200 MCU located in the Branch network, for calls Branch-12 through Branch-20, each endpoint was disconnected from the MPT call and then dialed back in to MCU directly.

In the case of the TANDBERG MPS-200 MCU, each endpoint dialed the E.164 ID of the multi-point meeting.

Although the detailed call statistics were not documented, bi-directional video and audio were tested and no issues were noted.

Direct Packet STNS Call Testing

Call Configuration			Traversal?	Call Request		Call Results		Actual Outgoing Stats			Actual Incoming Stats		
Call #	From	To		BW	Encrypt	BW	Encrypt	V Protocol	Resol	A Protocol	V Protocol	Resol	A Protocol

Dial-Out Testing from the SOHO Network with the TANDBERG 1000

SOHO-1	SOHO - TANDBERG 1000 (101)	CorpHQ - TANDBERG 1700 MXP (7001)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.263+	QCIF (176x144)	G.722
SOHO-2	SOHO - TANDBERG 1000 (101)	CorpHQ - Polycom VSX-7000 (7002)	Yes	256	Yes	256	Yes	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722.1
SOHO-3	SOHO - TANDBERG 1000 (101)	CorpHQ - LifeSize Room (7003)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	QCIF (176x144)	G.722
SOHO-4	SOHO - TANDBERG 1000 (101)	Branch - Polycom VSX-3000 (303)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
SOHO-5	SOHO - TANDBERG 1000 (101)	Branch - TANDBERG 880-MXP (304)	Yes	256	Yes	256	Yes	H.264	SIF (352x240)	G.722	H.263+	SIF (352x240)	G.722
SOHO-6	SOHO - TANDBERG 1000 (101)	Branch - Sony G-50 (305)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	CIF (352x288)	G.722
SOHO-7	SOHO - TANDBERG 1000 (101)	Public - Aethra Vega X3 (501)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
SOHO-8	SOHO - TANDBERG 1000 (101)	Public - Polycom ViewStation (502)	Yes	384	No	384	No	H.23	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722

Dial-Out Testing from the SOHO Network with the Polycom HDX-9000 installed to confirm H.239 functionality

SOHO-9	SOHO - Polycom HDX-9000 (101)	CorpHQ - Polycom VSX-7000 (7002)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722.1C	H.264	SIF (352x240)	G.722.1C
SOHO-10	SOHO - Polycom HDX-9000 (101)	CorpHQ - TANDBERG 1700 MXP (7001)	Yes	384	Yes	384	Yes	H.264	2SIF (704x240)	G.722	H.264	w288p (512x288)	G.722
SOHO-11	SOHO - Polycom HDX-9000 (101)	CorpHQ - Codian MCU 4200 (7010)	Yes	384	Yes	384	Yes	H.264	2SIF (704x240)	G.722.1C	H.264	w288p (512x288)	Siren-14

Direct Packet STNS Call Testing

Call Configuration			Traversal?	Call Request		Call Results		Actual Outgoing Stats			Actual Incoming Stats		
Call #	From	To		BW	Encrypt	BW	Encrypt	V Protocol	Resol	A Protocol	V Protocol	Resol	A Protocol
Dial-Out Testing from the Public Network													
Public-1	Public - Aethra Vega X3 (501)	Public - Polycom ViewStation (502)	No	768	No	768	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-2	Public - Aethra Vega X3 (501)	CorpHQ - TANDBERG 1700 MXP (7001)	Yes	768	Yes	768	Yes	H.264	SIF (352x240)	AAC-LD	H.264	CIF (352x288)	AAC-LD
Public-3	Public - Polycom ViewStation (502)	CorpHQ - Polycom VSX-7000 (7002)	Yes	384	No	384	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-4	Public - Aethra Vega X3 (501)	CorpHQ - LifeSize Room (7003)	Yes	1152	Yes	1152	No	H.263	SIF (352x240)	G.722	H.263	SIF (352x240)	G.722
Public-5	Public - Aethra Vega X3 (501)	Branch - Polycom VSX-3000 (303)	Yes	512	Yes	512	No	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
Public-6	Public - Polycom ViewStation (502)	Branch - TANDBERG 880-MXP (304)	Yes	384	No	384	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-7	Public - Aethra Vega X3 (501)	Branch - Sony G-50 (305)	Yes	768	Yes	768	Yes	H.264	CIF (352x288)	G.722	H.264	CIF (352x288)	G.722
Public-8	Public - Aethra Vega X3 (501)	Soho - TANDBERG 1000 (101)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
Public-9	Public - Polycom ViewStation (502)	Soho - TANDBERG 1000 (101)	Yes	256	No	256	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-10	Public - Polycom MGC-50 (100 / 505)	Public - Aethra Vega X3 (501)	No	1024	Yes	1024	Yes	H.263	4CIF (704x576)	G.722	H.263	CIF (352x288)	G.722
Public-11	Public - Polycom MGC-50 (100 / 505)	Public - Polycom ViewStation (502)	No	768	No	768	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-12	Public - Polycom MGC-50 (100 / 505)	Soho - TANDBERG 1000 (101)	Yes	384	Yes	384	Yes	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-13	Public - Polycom MGC-50 (100 / 505)	Branch - Polycom VSX-3000 (303)	Yes	768	Yes	768	Yes	H.263	4CIF (704x576)	Siren-14	H.263	CIF (352x288)	Siren-14
Public-14	Public - Polycom MGC-50 (100 / 505)	Branch - TANDBERG 880-MXP (304)	Yes	512	Yes	512	Yes	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-15	Public - Polycom MGC-50 (100 / 505)	Branch - Sony G-50 (305)	Yes	512	Yes	512	Yes	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Public-16	Public - Polycom MGC-50 (100 / 505)	CorpHQ - TANDBERG 1700 MXP (7001)	Yes	768	Yes	768	Yes	H.263	4CIF (704x576)	G.722	H.263	4CIF (704x576)	G.722
Public-17	Public - Polycom MGC-50 (100 / 505)	CorpHQ - Polycom VSX-7000 (7002)	Yes	768	Yes	768	Yes	H.263	4CIF (704x576)	Siren-14	H.263	CIF (352x288)	Siren-14
Public-18	Public - Polycom MGC-50 (100 / 505)	CorpHQ - LifeSize Room (7003)	Yes	768	Yes	768	No	H.263	4CIF (704x576)	G.722	H.263	CIF (352x288)	G.722

NOTES:

To verify dial-in capability to the Polycom MGC MCU located in the Public network, for calls Public-10 through Public-18, each endpoint was disconnected from the MPT call and then dialed back in to the MCU.

In the case of the Polycom MGC-50, each endpoint dialed into the Polycom's Entry Queue and then selected the proper meeting using DTMF tones.

Although the detailed call statistics were not documented, bi-directional video and audio were tested and no issues were noted.

Direct Packet STNS Call Testing

Call Configuration			Traversal?	Call Request		Call Results		Actual Outgoing Stats			Actual Incoming Stats		
Call #	From	To		BW	Encrypt	BW	Encrypt	V Protocol	Resol	A Protocol	V Protocol	Resol	A Protocol
IP to IP Gateway Testing (to verify the ability to dial out to public endpoints by IP address)													
Misc-1	CorpHQ - TANDBERG 1700 MXP (7001)	Public - Polycom VSX-7000 (@10.0.0.50)	Yes	768	Yes	768	Yes	H.264	CIF (352x288)	G.722	H.264	SIF (352x240)	G.722
Misc-2	CorpHQ - TANDBERG 1700 MXP (7001)	Public - TANDBERG 880-MXP (@10.0.0.51)	Yes	384	Yes	384	Yes	H.264	w288p (512x288)	AAC-LD	H.264	w400p (720x400)	AAC-LD
Misc-3	Branch - Polycom VSX-3000 (303)	Public - Polycom VSX-7000 (@10.0.0.50)	Yes	1024	Yes	1024	Yes	H.263	SIF (352x240)	Siren14-96k	H.263	SIF (352x240)	Siren14-96k
Misc-4	Branch - Polycom VSX-3000 (303)	Public - TANDBERG 880-MXP (@10.0.0.51)	Yes	512	Yes	512	Yes	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
Misc-5	Soho - TANDBERG 1000 (101)	Public - Polycom VSX-7000 (@10.0.0.50)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.264	SIF (352x240)	G.722
Misc-6	Soho - TANDBERG 1000 (101)	Public - TANDBERG 880-MXP (@10.0.0.51)	Yes	384	Yes	384	Yes	H.264	SIF (352x240)	G.722	H.253+	SIF (352x240)	G.722
Misc-7	Public - Aethra Vega X3 (501)	Public - Polycom VSX-7000 (@10.0.0.50)	No	1152	Yes	1024	Yes	H.263	SIF (352x240)	G.722	H.263	SIF (352x240)	G.722
Misc-8	Public - Polycom ViewStation (502)	Public - TANDBERG 880-MXP (@10.0.0.51)	No	768	No	768	No	H.263	CIF (352x288)	G.722	H.263	CIF (352x288)	G.722
Misc-9	CorpHQ - Codian MCU 4200 (7010)	Public - Polycom VSX-7000 (@10.0.0.50)	Yes	2M	Yes	2M	Yes	H.263+	CIF (352x288)	Siren14	H.263+	CIF (352x288)	G.722.1C
Misc-10	CorpHQ - Codian MCU 4200 (7010)	Public - TANDBERG 880-MXP (@10.0.0.51)	Yes	1152	Yes	1152	Yes	H.263+	CIF (352x288)	AAC-LD	H.264	w400p (720x400)	AAC-LD

Video Auto Attendant (AA) Testing - with the TANDBERG 1700MXP and TANDBERG 880MXP systems running SW version F6.0

Misc-11	Public - Polycom VSX-7000 (@10.0.0.50)	CorpHQ - TANDBERG 1700 MXP (7001)	Y - Via AA	FAILED		Tandberg unit made only a 64k connection to the AA (no video transmitted)							
Misc-12	Public - Polycom VSX-7000 (@10.0.0.50)	CorpHQ - LifeSize Room (7003)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711
Misc-13	Public - Polycom VSX-7000 (@10.0.0.50)	Branch - Polycom VSX-3000 (303)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711
Misc-14	Public - Polycom VSX-7000 (@10.0.0.50)	Branch - Sony G-50 (305)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711
Misc-15	Public - Polycom VSX-7000 (@10.0.0.50)	Soho - TANDBERG 1000 (101)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711
Misc-16	Public - Polycom VSX-7000 (@10.0.0.50)	CorpHQ - Codian MCU 4200 (7010)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711
Misc-17	Public - TANDBERG 880-MXP (@10.0.0.51)	CorpHQ - LifeSize Room (7003)	Y - Via AA	FAILED		Tandberg unit made only a 64k connection to the AA (no video transmitted)							
Misc-18	Public - TANDBERG 880-MXP (@10.0.0.51)	Branch - Polycom VSX-3000 (303)	Y - Via AA	FAILED		Tandberg unit made only a 64k connection to the AA (no video transmitted)							
Misc-19	Public - TANDBERG 880-MXP (@10.0.0.51)	Soho - TANDBERG 1000 (101)	Y - Via AA	FAILED		Tandberg unit made only a 64k connection to the AA (no video transmitted)							
Misc-20	Public - TANDBERG 880-MXP (@10.0.0.51)	CorpHQ - Codian MCU 4200 (7010)	Y - Via AA	FAILED		Tandberg unit made only a 64k connection to the AA (no video transmitted)							

Re-Test of the Video Auto Attendant (AA) Testing - with the TANDBERG 1700MXP and TANDBERG 880MXP systems downgraded to SW version F5.3

Misc-21	Public - Polycom VSX-7000 (@10.0.0.50)	CorpHQ - TANDBERG 1700 MXP (7001)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711
Misc-22	Public - TANDBERG 880-MXP (@10.0.0.51)	Branch - Polycom VSX-3000 (303)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711
Misc-23	Public - TANDBERG 880-MXP (@10.0.0.51)	SOHO - Polycom HDX-9000 (101)	Y - Via AA	384	Yes	384	No	H.263	CIF (352x288)	G.711	H.263	CIF (352x288)	G.711

NOTES:

- 1) The issues noted in calls Misc-17 through Misc-20 were resolved by downgrading the TANDBERG software to version F5. WR has been told that TANDBERG F6.1 Beta software (not yet released) resolves this issue.
- 2) Call Misc-23 - WR noted issues (64k connection rate, no video in or out) the 2nd time the TANDBERG 880-MXP tried to connect to the Auto Attendant. This was resolved by rebooting the TANDBERG 880-MXP system.
- 3) Call Misc-23 - The TANDBERG 880-MXP received a very low resolution (QCIF or lower) video image despite the call stats showing the resolution to be CIF. WR does not believe this is related to the Direct Packet STNS solution.