

**DELIVERING ON THE
PROMISE OF EASY TO
USE, SECURE, AND
INEXPENSIVE VIDEO
CONFERENCING IN AN IP
ENVIRONMENT**

Solving the Challenges Created by Firewalls
and Network Address Translation in a
Videoconferencing Environment

**A Frost & Sullivan Whitepaper Sponsored by
Polycom**

TABLE OF CONTENTS

TABLE OF CONTENTS

Abstract	3
Introduction	3
Challenges Faced by Users and Implementers of Videoconferencing Solution	4
Firewalls and NAT Traversal	4
Business-to-Business (B2B) Communications	7
Endpoint Protection	7
Organizational Politics	8
Solutions to Videoconferencing Challenges	8
H.460	8
FIPS 140-2 and Endpoint Protection	9
Dedicated VPNs	10
The Polycom Solution	10
The Hybrid Solution	11
Ease of Use and Connectivity	12
Traffic Management and QoS	13
Endpoint Security	14
Conclusion	14

ABSTRACT

Internet Protocol (IP) Video Conferencing can provide companies substantial operational efficiencies and cost savings. Although IP video conferencing is desirable from a cost perspective challenges to implementation exist including NAT traversal, endpoint connectivity and traffic management. Additional connectivity challenges such as differing security policies and differing vendor standards have caused concern and delay for many videoconferencing deployments. This whitepaper evaluates the challenges of deploying IP video conferencing in a secure and easy to use manner. The paper presents solutions to those problems and explains how the Polycom V²IU™ delivers those solutions.

INTRODUCTION

Businesses today are facing unique communication challenges. The workplace is a dynamic and constantly changing environment. Along with rapidly evolving product lines, work teams are becoming more dispersed due to factors such as globalization, increased competition, and pricing pressures. As a result, the DNA of today's workforce is substantially different. There is an increasing need for traditional workers as well as for remote employees and work teams to stay connected and able to communicate regardless of location, device, or network.

The perception of videoconferencing has received some of its initial negative sentiments from experiences of older technology. While traditional videoconferencing was as good as the technology of the time would allow, there are new advancements available to provide a higher quality visual and audio experience. Even though videoconferencing has been adopted by many organizations over the last 20 years, it has still not hit critical mass. Much of the responsibility for the slow rate of adoption has been high expectations and low results.

Frost & Sullivan has seen a significant paradigm shift in the videoconferencing market. Since 2004, growth in this market has been steadily increasing for a number of reasons. Much of this revival is attributed to the increasing availability of capital expenditure due to stable economic growth. Globalization and the need for dispersed workgroups to collaborate continues to increase and with it, the interest in videoconferencing has increased. Another important driver for this market is the move to an IP based infrastructure and the success of technologies like Voice Over IP (VOIP). As videoconferencing vendors prove the ease of integrating their technology into the corporate infrastructure, videoconferencing will become a much more interesting business communication tool.

Frost & Sullivan has also seen videoconferencing fall into the same trap as other markets such as Supervisory Control And Data Acquisition (SCADA) systems and financial networks. When a technology is deployed on a dedicated network connection with limited accessibility, there is little concern for security. The technology is inherently secure because of its deployment. As seen in technologies like VOIP, there is a new set of

security challenges once technology moves out onto the same infrastructure as all the other data devices and is visible to the global Internet.

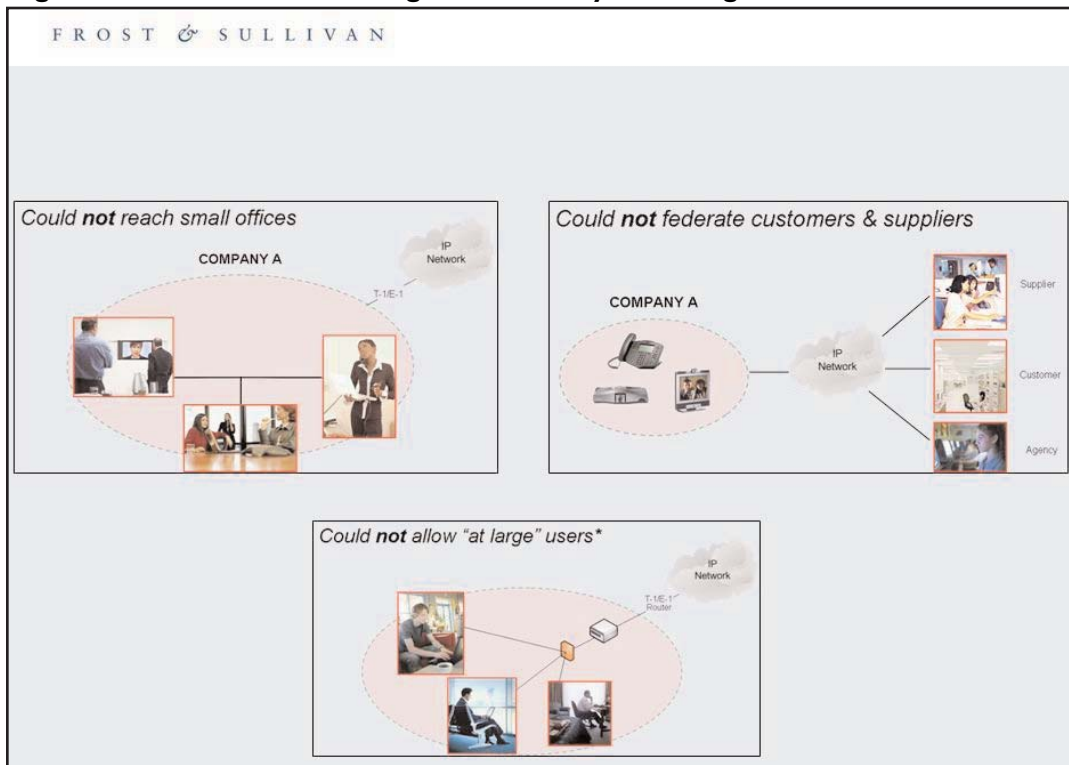
This paper will discuss many of the challenges that videoconferencing technology faces in regards creating easy-to-use, secure IP videoconferencing. Each challenge will be described in detail, and various methods of solving each challenge will also be presented.

CHALLENGES FACED BY USERS AND IMPLEMENTERS OF VIDEOCONFERENCING SOLUTION

Firewalls and NAT Traversal

The increase in IP network availability, capacity, and capabilities has encouraged the enterprise to leverage their investment in IP networking across all applications. One of the primary problems with IP based videoconferencing and security relates to traversing the corporate firewall. As stated before videoconferencing grew out of a point-to-point environment and adaptation to an IP infrastructure presents a number of challenges. As illustrated by Figure 1, deployment has been a challenge due to the various communication scenarios that exist between a company's sites, its partners and its users.

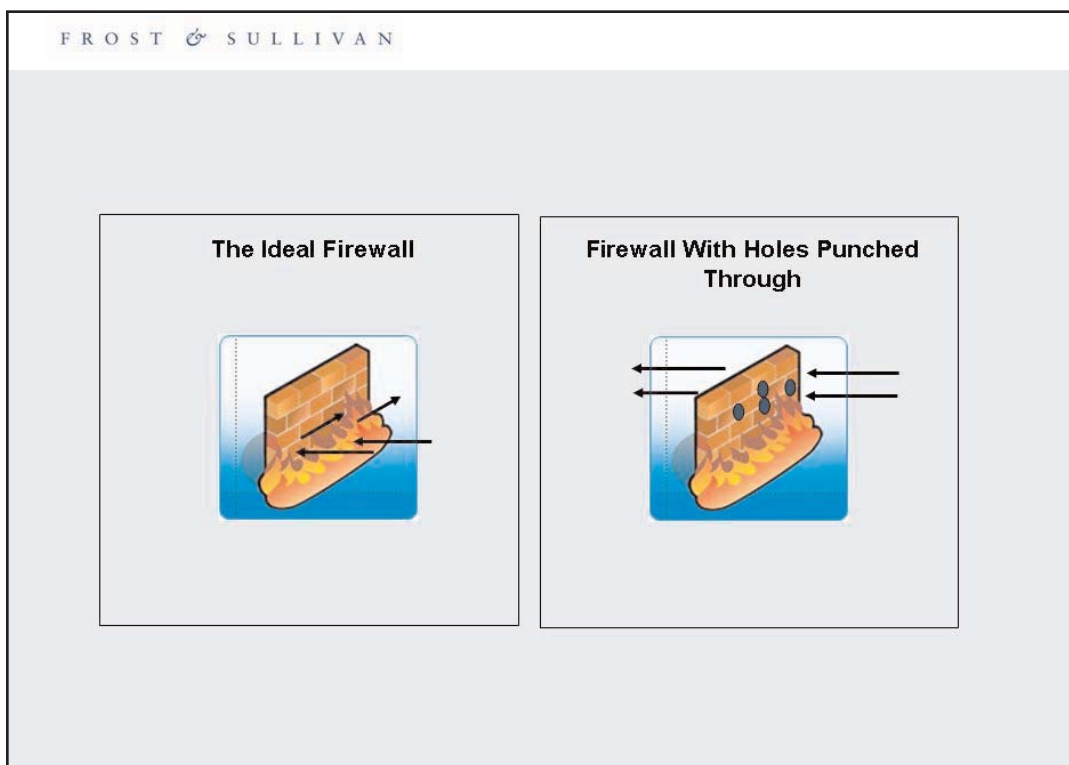
Figure 1 - Video Conferencing Connectivity Challenges



Firewalls are designed to keep certain types of traffic out of a network and are usually deployed in strategic points in the network infrastructure, primarily between the public Internet and the corporate network, between branch offices and the corporate network or even between segments of the corporate network. Firewall rules are set based on specific needs of the network it is protecting. For example, many corporations do not allow telnet traffic to pass through the firewall. In that case, the firewall would inspect all traffic coming in or out of the network and drop all traffic that is telnet.

Unfortunately, it is very difficult in today's connected environment to implement a firewall that completely separates networks. Most firewalls have some holes left open to allow some traffic through. Port 80, the default port for HTML or Web traffic, is the most common port left open in firewall implementations. However, the more ports that are opened, the higher the probability that Trojans and other unwanted software could pass through. Figure 2 shows the difference between a "perfect" firewall, and a the firewall as deployed in most organizations today.

Figure 2 - Comparison of Ideal vs. Typical Firewall



Many videoconferencing systems use the H.323 protocol for communication. Unfortunately, H.323 was not designed with security in mind and requires the opening of a large number of ports in order to function. Table I shows H.323 port usage. This is an administrative nightmare and has a great deal of security implications relating to policies and real security risks.

Table I - H.323 Port Usage

Port	Type	Description
80	Static TCP	HTTP Interface (optional)
389	Static TCP	ILS v2.0 Registration (LDAP)
1002	Static TCP	Win 2000 ILS Registration
1503	Static TCP	T.120
1718	Static TCP	Gatekeeper Discovery
1719	Static TCP	Gatekeeper RAS
1720	Static TCP	H.323 Call Setup
1731	Static TCP	Audio Call Control
8080	Static TCP	HTTP Server Push (optional)
1024 - 65535	Dynamic TCP	H.245 (Call Parameters)
1024 - 65535	Dynamic UDP	RTP (Video Stream Data)
1024 - 65535	Dynamic UDP	RTP (Audio Stream Data)
1024 - 65535	Dynamic UDP	RTCP (Control Information)

There is a push for increased security in the network and opening all the ports for H.323 would also open the network to abuse by Trojan applications, peer-to-peer applications such as Kazaa and Denial of Service (DOS) attacks. Most security administrators are working hard to limit the number of open ports and are forcing users to go to great lengths to justify opening new ports.

Network Address Translation (NAT) creates another major hurdle for IP videoconferencing. NAT is a popular method for allowing a one-to-many relationship of IP addresses in a corporate network. NAT keeps track of requests from machines inside a network to websites outside the network. To the outside world, all requests appear to come from one IP address, the public address. As information comes back, NAT handles the translation from the one public facing address back into the internal addressing scheme. NAT provides many advantages to the corporate network.

NAT was originally designed to help reduce the size of the address space that organizations needed on their network. As the Internet was becoming popular, it was quickly realized that there were not enough available addresses for the number of devices needing access. NAT was developed in a way that the NAT device was responsible for translating traffic from the internal, private address space to the external space. By performing the translation at the border to the public network, one address can be used for a multitude of machines.

NAT also hides the footprint of the network. Because all communication occurs through the NAT device, the network endpoints are obscured. This alone provides a level of security to the network as it is difficult for prying eyes to know how many hosts exist on a network, much less the types of devices located there. Another security consideration is that since the connection to the endpoint must be initiated from inside the network and cannot come from the outside, it is impossible to connect into the network uninvited. This security provided by NAT causes a headache for videoconferencing over IP. Many IP video conferencing systems use IP addresses for dialing. Network address translation makes this more complicated as a videoconferencing endpoint inside the network will have a different internal IP address than it would appear to have from outside the firewall.

Business-to-Business (B2B) Communications

One of the most convincing reasons for businesses to adopt videoconferencing is to reduce the travel required to and from various locations for meetings. While globalization continues, the interaction between businesses in different parts of the world continues to increase.

Videoconferencing is an attractive solution for communication when dealing with entities halfway across the world. However, in the traditional point-to-point model of IP videoconferencing, communication is only possible between businesses that have similarly configured videoconferencing equipment and firewall rules. This procedure often requires extensive coordination between a variety of groups inside each organization. To a layperson, it can be very confusing and frustrating when videoconferencing equipment will not connect for apparently no reason. The normal user does not understand esoteric networking protocols, ports, IP addresses and more. They are likely to turn to their network administrator who may not even have the right or knowledge to change settings on the firewall.

While the H.460 and related protocols go a long way to address these problems, many organizations are unaware of the advantages of adopting a platform that allows any business to have the ability to securely engage in a videoconference. Most organizations have not addressed the challenge of B2B communications and are underutilizing their videoconferencing infrastructure.

Endpoint Protection

Every Internet user is familiar with SPAM or junk e-mail. Most users understand that their PC must have antivirus and other anti-malware software to be safe. More sophisticated users are also aware that attacks can be launched against web sites to deny their availability to legitimate users. What most users do not realize is that VoIP telephony and videoconferencing will be subject to growing attacks in the form of denial of service attacks and automated or unsolicited audio and video calls.

Enterprises are realizing more and more the importance of protecting the endpoint not only from attacks, but also from eavesdropping and snooping. With the amount of regulations going into effect it is imperative that vendors incorporate the same protections being implemented in other data devices.

Some organizations have realized the value of IP videoconferencing and in order to maximize its ease of use have logically placed the videoconferencing endpoints outside the firewall. This practice avoids all the issues associated with H.323, NAT and ports, but opens the videoconferencing endpoint to attack and misuse.

Organizational Politics

In many organizations the group that is driving the implementation of an IP videoconferencing solution is not always the same group responsible for securing that solution on the network. Frost & Sullivan has seen this challenge arise in other segments of the security market as the security team and the application support teams often have differing goals and responsibilities.

As stated previously, the inordinately large number of allowed ports required for a standard H.323 deployment is considered unreasonable for many organizations and many security administrators would have serious concerns with opening the organization up to that kind of risk due to increasing the threat to the organization. Deployments would likely be at least stalled if not cancelled due to the security implications of implementing IP videoconferencing.

Another problem related to organization politics concerns connectivity between businesses. The internal security policies of one organization can be complicated enough, but when dealing with the intricacies and security policies of multiple companies that may be pursuing an IP videoconferencing solution, these challenges increase exponentially.

SOLUTIONS TO VIDEOCONFERENCING CHALLENGES

While there are a number of challenges to videoconferencing, it is not to say that progress has not been made in the industry. There are a number of innovative solutions developing in the industry that are paving the way for videoconferencing to grow and expand its reach into more organizations.

H.460

Based on the inherent challenges associated with implementing H.323 networks and overcoming the firewall/NAT traversal problems, the International Telecommunications Union (ITU) has recently ratified a new set of standards to resolve this issue. The standard H.460 was designed as a long-term solution to be adopted by vendors addressing NAT-Firewall traversals between various vendor videoconferencing equipment and diverse organization more efficient.

Until recently, each organization was able to implement their own solution for NAT/firewall traversal, however, in order to communicate over H.323 inter-company there was no standard to overcome this obstacle. H.460 removes this barrier enabling interoperability for IP communications between companies. The standard provides two categories of solutions dealing with signaling (H.460.17 and 18) and media (H.460.19)

There are typically two elements required in deploying H.460. The first is a client software residing behind the firewall, which will either be located inside the videoconferencing endpoint or alternately a gatekeeper to handle non-compliant endpoints. The second requirement is the session border controller (SBC).

The H.460.17 and .18 deals with signaling. The H.460.18 solution does not utilize tunneling, but as an alternative attempts to follow basic H.323 messages by perpetually hunting in order to open pinholes from the internal network to the external one. Without using the H.460.18 solution, which permits the gatekeeper to open a connection, the external Company A could not communicate with internal Company B, because the firewall would obstruct its attempt to setup a call. Consequently, the gatekeeper, on the behalf of the external endpoint, is instead required to signal the internal Company B to open the connection. For this reason, the extra signaling was added and necessitates calls always being routed through the gatekeeper.

H.460.19 extends H.323 by defining the NAT/firewall mechanism for media. In addition, H.460.19 provides a solution for opening RTP and RTCP pinholes and a method for maintaining them using a keep-alive mechanism.

This new protocol means NATs and firewalls will no longer be a barrier for multimedia communications between organizations. IP videoconferencing and telephony users will be able to communicate with suppliers, customers, and partners using inexpensive and reliable IP networks, even in multi-vendor configurations. The rapid development and acceptance of this new protocol shows strong industry cooperation to solve this problem for users. The firewall issue is improved significantly because administrators can open a limited number of ports for the SBC and are no longer required to open a huge range of ports to the outside world.

FIPS 140-2 and Endpoint Protection

On a dedicated line, endpoint protection and the potential for eavesdropping is not the problem it is on the open Internet. Protocols such as H.323 may do a good job at protecting the actual traffic. However, many videoconferencing systems use more traditional protocols such as HTTP, and TFTP for updates and management functions. Without proper safeguards and encryption on those channels, the system could still be susceptible to attacks, theft of service, or eavesdropping.

FIPS 140-2 provides a third-party-verified security standard with a federal-government heritage that ensures corporations' data security and can help them meet the

IT-compliance requirements of the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act, and other federal mandates.

FIPS 140-2-certified products go through a detailed review and testing, including direct code review, by a NIST-approved agency to ensure the trustworthiness of the implementation's cryptographic algorithms, loading methods, operating systems, documentation, operating software and hardware.

Some of the protections provided by FIPS 140-2 certification may seem subtle or related only to the cryptographic module itself. There are other changes as part of FIPS 140-2 that are very noticeable. For example, very few services or ports are actually active and those that are active are secured. A FIPS 140-2 compliant device would be running SFTP and HTTPS as opposed to the cleartext versions of those protocols.

Dedicated VPNs

Some organizations have begun using Virtual Private Networks (VPNs) to simulate dedicated ISDN lines and to provide an extra layer of security. There are many additional challenges associated with using this approach that need to be considered.

The primary challenge that comes from using VPN as a solution is the limited connectivity that comes from that solution. VPNs are strictly a point-to-point solution, and while this might be acceptable for a single branch, the usability is severely limited. There are also issues concerning password and key management for every connection that is set up. Each VPN connection point needs to have either the credentials maintained, causing extra administrative overhead.

Another challenge with VPN technology is the extra overhead that is generated by encryption. As stated earlier, videoconferencing is a technology that is very susceptible to latency. The encryption necessary for a VPN tunnel is significant, and only adds to the already high bandwidth requirements for videoconferencing.

THE POLYCOM SOLUTION

Frost & Sullivan has been studying the videoconferencing market and believes that Polycom has developed a solution that addresses many of the security and usability challenges in the market today. The V²IU™ supports a number of connectivity and security features that facilitate easy and secure videoconferencing both within the organization and with external partners. Table 2 gives a description of benefits addressed by the V²IU™ features.

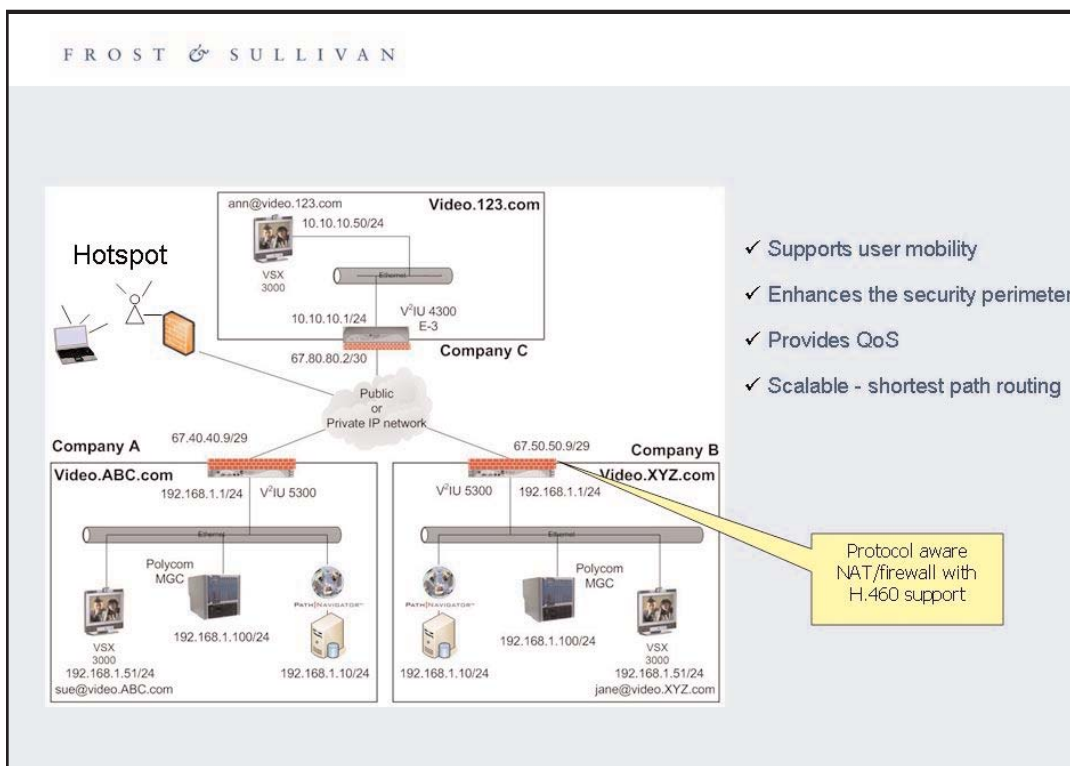
Table 2 - Customer Pain Points Addressed by the Polycom V²IU™

Customer Pain Point	V ² IU™ Features	Benefits
Opening an excessive range of ports in the firewall makes the firewall ineffective.	Application layer gateway / Stateful Packet Inspection Firewall	Stateful security for video devices- ports are only open when needed.
Dialing by IP is counter intuitive and very difficult to use	E-Mail dialing	Conferencing is easy...simply call "<name>@company.com"
Normal IP traffic, by its nature, is plagued by problems of dropped packets, latency, out of order packets, and other problems.	Traffic management	High quality video conferencing, CAC, Traffic Shaping
Management protocols and sessions are susceptible to sniffing and being captured	Endpoint Security	FIPS 140 certification provides an extra layer of protection.

The Hybrid Solution

As illustrated in Figure 3, the Polycom V²IU™ is a H.460 aware, stateful packet inspection firewall designed to protect against a variety of attacks against the system. There are other solutions on the market that are NAT aware or act as gateways. However, a NAT traversal solution is ineffective if it does not inspect the traffic coming into the corporate network. In a pure H.460 solution, traffic is tunneled directly to the endpoint. In theory a hacker could use a videoconferencing tunnel to bypass the corporate firewall and attack other corporate assets via videoconference endpoints. By inspecting the traffic, the V²IU™ can prevent a variety of inappropriate access and sophisticated attacks.

Figure 3 - The Hybrid Solution



It would not be realistic to expect organizations to perform forklift upgrades to their existing firewall infrastructure. The V²IU™ offers the very important feature of being able to run in parallel with existing firewalls. Additionally, by being application aware, the V²IU™ can act as a gateway and only open the ports that are absolutely necessary for communication.

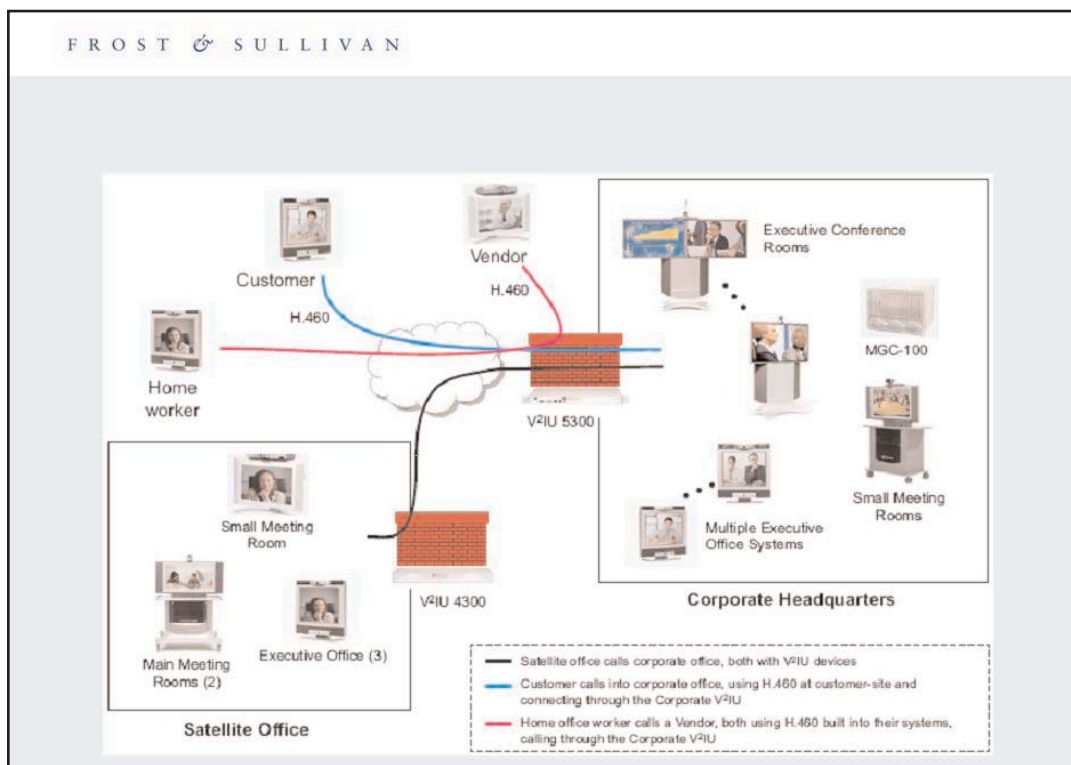
Ease of Use and Connectivity

The V²IU™ fully supports the H.460 suite of protocols, allowing an unprecedented level of connectivity between not only branch offices, but outside businesses as well. Users can initiate a video conference simply by "dialing" the user by email address. This provides an ease of use that is very attractive to customers.

Another advantage of the V²IU™ is its ability to interoperate with partners who have solutions from other vendors. Some vendors their solution at both end of the connection, but by supporting H.460, the V²IU™ allows other vendors to communicate with the V²IU™.

As shown in Figure 4, the V²IU™ allows all users, ranging from employees at branch offices, remote workers, clients, and vendors to connect securely to an organization.

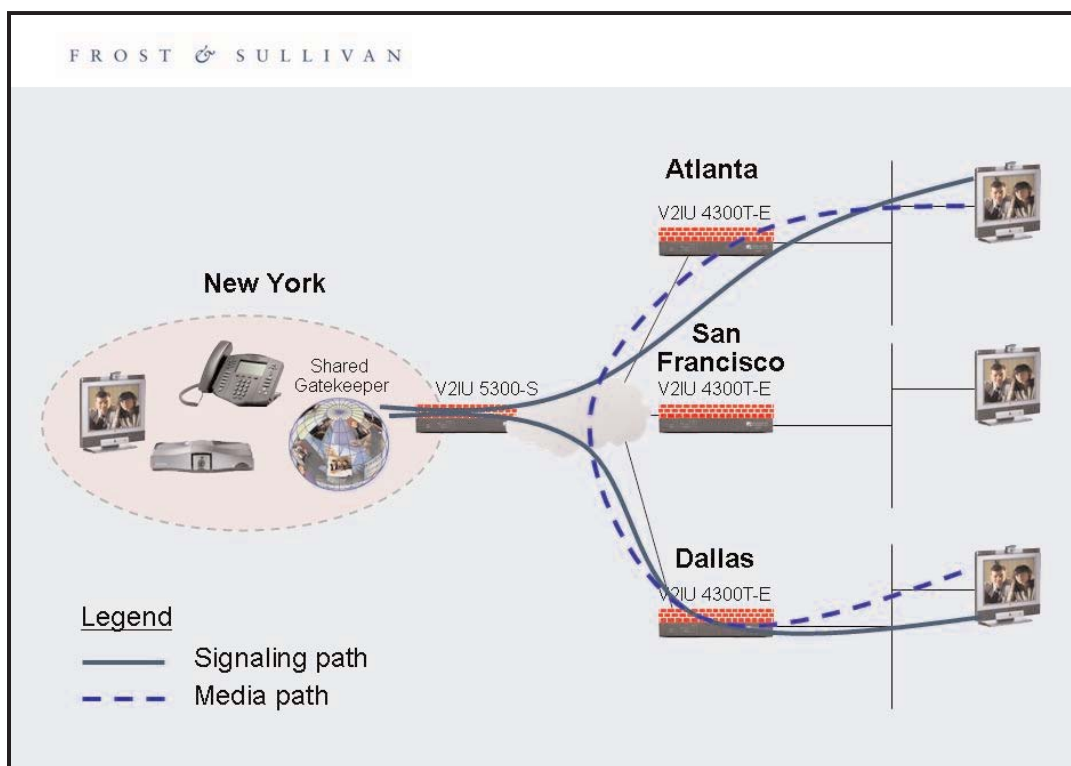
Figure 4 - Connectivity to a Variety of Endpoints



Traffic Management and QoS

The V²IU™ provides extensive traffic management and QoS capabilities in addition to a very scalable solution. The V²IU™ also offers Route Media Shortest Path which provides advantages to organizations with geographically disperse endpoints. As illustrated in Figure 5, connections are initiated from branch offices in a variety of different locations and the V²IU™ will automatically determine the shortest path to take to the endpoint. This means that an organization using a V²IU™ solution at each branch office would see a bandwidth usage improvement as the V²IU™s would automatically determine the best path to take, significantly reducing latency. Some solutions on the market require all traffic to be routed through a centralized gateway. This can create lots of additional latency and increases the potential for lost or out of order packets. With the V²IU™ solution, the device determines the most reliable and fastest route from the source to its destination.

Figure 5 - Polycom Route Optimization and Traffic Management Solution



Endpoint Security

The upcoming software release of the V²IU™ (scheduled for May 2006) is currently being certified as FIPS 140-2, ensuring the first government level certified device for all calls. Without encryption, any user sniffing the network could pull user names and passwords directly off the line. A malicious user could then manipulate the videoconferencing gateway. By running encrypted protocols, the V²IU™ helps to ensure that only authorized users can access the management and updating features of the device.

Polycom plans to continue certification of the V²IU™ as needed.

CONCLUSION

First generation videoconferencing products worked well in homogenous, dedicated environments, but stumbled when deployed across heterogeneous public networks. Consequently, today's videoconferencing landscape requires preparation and thought surrounding connectivity in particular securing the network environment.

Preparing and implementing a secure environment, brings piece of mind to all parts of the organization. This enables the end users the freedom to use videoconferencing as a critical business communication tool, allowing them to connect where and when they need to at a moments notice. In addition, network administrators can feel confident that their data is safe and secure from intruders.

Understanding the challenges and evaluating the solutions is the biggest hurdle to overcome when implementing an IP videoconferencing solution. Polycom, with its strong emphasis on security, connectivity, and ease of use has addressed three of the most prevalent challenges in the videoconferencing world. Frost & Sullivan believes that customers can use the V²IU™ to maximize productivity of employees, partners and vendors by providing a truly collaborative environment

CONTACT US

Bangalore

Bangkok

Beijing

Buenos Aires

Cape Town

Chennai

Delhi

Dubai

Frankfurt

Kuala Lumpur

London

Mexico City

Mumbai

New York

Oxford

Palo Alto

Paris

San Antonio

Sao Paulo

Seoul

Shanghai

Singapore

Sydney

Tokyo

Toronto

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your organization, and thereafter it may not be recopied, reproduced or otherwise redistributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.

For information regarding permission, write:

Frost & Sullivan
2400 Geng Rd., Suite 201
Palo Alto, CA 94303-3331, USA