



## **VIDEO COMMUNICATIONS SERVICE NETWORK TECHNICAL GUIDE**



**ENDPOINT SOLUTIONS, LLC**  
**T-973-696-0115**  
**C-201-247-4032**  
**DLENTO@ENDPOINTSOLUTIONS.NET**  
**WWW.ENDPOINTSOLUTIONS.NET**

**THE FUTURE IS NOW - GET CONNECTED TODAY!**

## **Table of Contents**

Introduction .....	3
What is H.323 .....	4
Networking and H.323 .....	5
Endpoint set up .....	6
Security Concerns .....	7

# Introduction

The object of this document is to provide the client with an overview of various setup configurations that will be encountered. This document will not cover all possible scenarios, however, with basic knowledge of the Endpoint Videophone and networking, the majority of installs will be relatively simple.

This document will also briefly touch on Networking Technology and the H.323 protocol on which the Endpoint unit is based, enabling technical personnel to better understand the dynamics of videoconferencing and to become more proficient in Endpoint set up and troubleshooting.

# What is H.323?

H.323 is a standard recommended by the ITU (International Telecommunication Union) that defines real-time multimedia communications and conferencing over packet based networks, including LANs, WANs, and the Internet, which may not provide a guaranteed Quality of Service.

The H.323 Recommendation encompasses several standards such as H.323, H.225.0 and H.245. For more information on the inner workings of the H.323 protocol go to <http://www.h323forum.org/>

There are four basic elements involved in videoconferencing implementation. These are endpoints, gatekeepers, gateways and multipoint control units (MCUs). Although all are not necessarily used or required, they enhance the overall functionality of video over IP.

**Terminals:** H.323 endpoints (Endpoint) that support real time multimedia communications.

**Gatekeepers:** The “traffic cops” of an H.323 network. The gatekeeper is responsible for address translation, admission control, bandwidth control, call control signal processing, call authorization and call management.

**Gateways:** Are an optional component of video conferencing that allow dissimilar networks, such as IP to ISDN, to communicate. The gateway performs the translation needed for signaling, audio and video codices, setup and termination.

**MCUs:** also known as Bridges, provide the ability to bring together three or more endpoints in a conference. All endpoints participating in the conference establish a connection with the MCU. In multiparty bridging the MCU has the ability to control aspects of the audio and video, initiate or receive calls, ad hoc conferencing or scheduled events.

# Networking and H.323

**Network:** A group of interconnected computers capable of exchanging information. A network can be as few as several personal computers on a LAN or as large as the Internet, a worldwide network of computers.

Endpoint works utilizing the customers' LAN (Local Area Network) and their existing broadband connection to the Internet. TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. The IP portion handles the address part of each packet so that it gets to the right destination.

For our purposes there are two types of IP addresses, PUBLIC and PRIVATE. A computer on the Internet is identified by its IP address. In order to avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Computers on private TCP/IP LANs however do not need public addresses, since they do not need to be accessed by the public. For this reason, the NIC has reserved certain addresses that will never be registered publicly. These are known as private IP addresses, and are found in the following ranges:

From 10.0.0.0 to 10.255.255.255  
From 172.16.0.0 to 172.31.255.255  
From 192.168.0.0 to 192.168.255.255

Most networks today utilize these private addresses.

Public address ranges:

From 1.0.0.0 to 126.255.255.255  
From 128.0.0.0 to 191.255.255.255  
From 192.0.0.0 to 223.255.255.255

There are certain inherent difficulties with H.323 communicating over a network. Unlike most TCP/IP applications, H.323 uses DYNAMIC PORTS instead of STATIC PORTS. That means that each H.323 connection is somewhat different than the last. For instance, the HTTP web site application uses port 80. H.323 can use any of over 60,000 different ports. Putting a web server behind a firewall means opening a single small hole. Putting an H.323 device behind a firewall means opening over 60,000 ports, not something the IT people will look kindly on.

Another trait of H.323 is to stuff the source IP address of the endpoint into the UDP payload. When using private IP addressing the far end host tries to respond to the private address which is dropped by the outgoing router and the call fails.

\* The Endpoint has a built-in solution to this problem. In the NETWORK field of the Endpoint CONFIGURATION screen there is an option, "Being called by above IP", when using a PUBLIC IP address this option is set to YES and the UDP payload is not altered. When using a PRIVATE address this option is set to NO. By setting this option to NO a program in the Endpoint determines the PUBLIC address and inserts it into the UDP payload. Now when the far endpoint responds, the packets are properly routed.

## Endpoint Set Up

The Endpoint can be set up in several ways depending on how the broadband is being delivered, which network devices are in use, and whether public or private addressing is being implemented on the LAN.

Due to the nature of H.323 the Endpoint needs to appear open to the internet.

The simplest solution is to connect the Endpoint to the router/cable/DSL modem either directly or through a switch and assign it a PUBLIC IP address or if the ISP's equipment is set up for DHCP then allow the Endpoint to dynamically assign itself a PUBLIC address.

In the case of some DSL providers, such as Verizon which uses PPPoE (Point to Point Protocol over Ethernet), a username and password must be configured in the Endpoint in the ADVANCED setup screen under PPPoE.

The majority of users however need to connect multiple devices to the internet and are usually given only one PUBLIC IP address. To remedy this, a user can request additional IP address space from their ISP or connect a router such as Netgear, Dlink etc. to the cable/DSL modem. The router will then utilize NAT (network address translation) by translating the external PUBLIC address to multiple internal private IP addresses. Remember the Endpoint IP address must appear PUBLIC to work. To do this the broadband router must support a DMZ. A DMZ forwards ALL ports to the DMZ host. This also means that a DMZ overrides all other port forwarding commands set up in your router and it will only work for

ONE host. To have more than one Endpoint on a LAN you will need as many public addresses. First, assign the Endpoint a STATIC IP address in your network. Then set that new IP address in the router's DMZ. All routers will handle this differently so refer to your router manufactures documentation for proper configuration.

## Security Concerns

Endpoint is built on a proprietary OS which has not incorporated programs such as telnet, SNMP, etc. There is no way to remotely manage the unit and so the ability to log into and hop off of the endpoint is not present. This should alleviate the concerns of IT administrators when placing the Endpoint in the DMZ or between the outside broadband connection and the firewall. In case of the latter the LAN is still protected by the firewall.