SETUP FOR POLYCOM HDX on the Learning Network of Vermont (LNV)

<u>Network Preparation:</u>

The LNV uses the H.460 firewall traversal standard of H.323. This means that ***all connections to and from the Polycom are outgoing connections***, even if they are incoming calls. There is no need to open incoming ports on the firewall, no need to set up 1-to-1 NAT, and no need to set up dedicated public IP addresses.

Most networks are "ready-to-go," and the Polycom can be placed on the network just as you would place any workstation that can access the Internet.

Specifically, the Polycom needs to be able to make **outgoing, stateful connections** using both **TCP and UDP.** Again, most networks are set up this way by default.

To summarize:

- Polycom can have a static IP address or use DHCP – it's up to you.
- Polycom must be able to make outgoing, stateful connections over TCP and UDP
- No need to explicitly open incoming ports
- No 1-to-1 NAT

<u>Firewalls:</u>

Because the LNV uses H.460 traversal, the firewall **must not** utilize any application inspection for H.323. A few firewalls come with such inspection enabled by default, and this inspection must be disabled. **Disabling H.323 application inspection will not decrease security**.

The application inspection we most often encounter are on these firewalls:

SonicWall

H.323 Transformations are enabled by default and **must be disabled.**

Cisco ASA/PIX

inspect h323 RAS and **inspect h323 h225** are enabled in the default configuration and **must be disabled** (In older versions of IOS, these used to be called **h323 RAS fixup** and **h323 h225 fixup**.)

Polycom Configuration:

The following instructions cover the *basic* configuration necessary to operate the Polycom HDX on the LNV. The options available on the HDX are extensive and cover many areas not addressed here, such as call speed, what you see on the screen, etc.

We recommend using the **web interface** to configure the Polycom. Using any web browser located on the same network as the Polycom, enter the Polycom's local IP address as the web address. The Polycom's current IP address is listed on the "Place A Call" screen (press "Home" on the remote control).

You must know the admin password to make config changes on the Polycom. The systems installed by NCS on the LNV use the password **12345**. If yours is different, we won't know it. (As a last resort, a Polycom can be reset to its factory configuration, erasing all passwords but those built in. It requires a lot of work to bring the Polycom back to its working configuration, so we don't recommend it lightly.)

1. Check LAN Settings
    a. **Admin Settings → LAN Properties**
    b. The IP Address can be set manually or automatically (DHCP). The choice is yours, and we do not need to know if you change your IP address.
    c. If you need to know the Polycom's MAC address for your DHCP server, you can find it on the left-hand side of the web interface at **Tools → System Information**
    d. When you click **Update** on the LAN Properties page, the Polycom will reboot
2. H.323 Configuration
    a. **Admin Settings → Network → IP Network → H.323 Settings**
        i. Enable IP H.323:   [**checked**]
        ii. Display H.323 Extension [**checked**]
        iii. H.323 Name: [**as assigned**]
        iv. H.323 Extension (e.164) [**as assigned**]
        v. Use Gatekeeper   **Specify**
        vi. Gatekeeper IP Address   **159.105.0.73**
    b. **Admin Settings → Network → IP Network → Gateway**
        i. (**Leave as-is**)
    c. **Admin Settings → Network → IP Network → SIP Settings**
        i. Enable SIP   [**unchecked**]
    d. **Admin Settings → Network → IP Network → Quality of Service**
        i. (**leave as-is**)
    e. **Admin Settings → Network → IP Network → Firewall**
        i. Fixed Ports   [**unchecked**]
        ii. Enable H.460 Firewall Traversal [**checked**]
        iii. NAT Configuration   **Off**

    DON'T FORGET TO CLICK UPDATE!

Testing

1. First, look at the "Place A Call" screen to see if there are any Alerts. There should be no Alerts (however, an Alert for a bad Time Server will not affect anything negatively. You can fix this by entering a known good time server in the configuration)
2. If all looks good, call **1800**. This is the LNV Bridge menu, and you should see the meeting entry screen. If the call connects well, hang up and try the next test.
3. Call **5851999.** This is the Northeast Computer Systems, Inc., LNV Polycom. It is on 24X7 for testing. It does not have a person attending it, but during business hours, someone will come by and tell you if your image and sound are good, and and test calling you back if you wish.
4. If you encounter problems, and for further testing, contact LNV Tech Support.