IHE Eye Care Connectathon 2016 - Network Information

Introduction

This document explains the network configuration you will need to understand for the October 2016 IHE Eye Care Connectathon. This document describes both public IP addresses and private addresses.

Wireless

There will be a wireless network provided on-site. This is used for access to the internet for email and light internet browsing, and is not used for testing. The login/password to the wireless network will be provided when you arrive in at the RSNA Headquarters.

Testing Network -- Physical Connections

At the Connectathon, each vendor system will be given one network drop from the network group. **If you need more connections, you should bring a hub for fanout**. You are responsible for supplying your own network cables if you need more than one. We strongly suggest you bring a hub even if you think you have only one computer. Bring an extra hub if you have space in your luggage; they come in handy.

Eye Care Connectathon 2016

Systems in the Eye Care Connectathon will use private address space described below. Your system should be configured to use an IP address in the private space listed below. The manager of your event (Felhofer) will assign IP address(es) to your test system.

Subnet	10.242.0.0/24
Address range	10.242.0.20 – 10.242.0.100 (Eye Care equipment)
Gateway	10.242.0.1
Subnet Mask	255.255.255.0
DNS (for connectathon)	10.242.0.1 / 128.104.254.254 / 204.246.1.20
DHCP	Yes, for laptops for email, etc. Not for test systems in the connectathon unless they are just client PCs that are invisible to test partners

Network Reminders

1. For each test system you have, bring written instructions that tell your staff how to change the network settings, including:
    a. Your IP address
    b. Default gateway
    c. Subnet mask
    d. DNS server

    e. NTP server
    f. The root/administrator password
2. If your systems have software firewalls, know how to configure those to open/close ports. This is not always obvious on Unix systems.
3. If you use a VPN to connect back to your corporate network, ask the corporate IT staff to document what ports need to be open to enable the VPN. Do not tell us "We use the Cisco VPN." The network guys will need to know what ports to open; they don't necessarily use the same VPN software that you use. Bring a written a copy as you won't have email access until this works.
4. We suggest you bring dumb hubs to provide fanout. If you want to bring an Ethernet switch and/or firewall, do not configure to use NAT. We are already giving you private IP addresses; if you decide to use NAT that will only require one more level of debugging.
5. Bring extra cables. If you have space, throw in an extra hub.
6. Know how to tell the difference between:
    a. My Ethernet wire fell out of the hub or my system.
    b. I cannot ping/communicate with a partner on my hub.
    c. I cannot ping the default gateway
    d. I cannot make a network connection to a peer application of another vendor.
    e. I can make a connection, but my application does not work.
    f. I put a message in a delivery queue, and it has not yet arrived at the receiver.
7. Do not just pick what you think is an empty IP address. Your company may not have been assigned consecutive addresses. If you need another IP address, ask Lynn Felhofer.

Network Sharing Rules

The wireless network and the testing network are shared resources for all participants. These rules help to ensure the network supports our testing goals:

1. All systems are required to have active and up to date anti-virus software. Relevant operating system security patches should be installed. Ports that are not needed by other participants should be blocked by a software or hardware firewall at your table
2. The items listed below are not allowed during the hours of 07:30 and 17:00 each day.
    a. Streaming video is not allowed. That includes Skype video sessions.
    b. Streaming audio is not allowed. Skype calls (audio only) are allowed.
    c. Peer-to-peer file sharing (Limewire, BitTorrent, etc) is not allowed.
    d. Downloading large files (unless they are work related)
    e. Attaching your own wireless equipment to the network is not allowed. You shall use the wireless network provided by the RSNA onsite.
    f. Keep personal internet usage to email and light web surfing.