Networking Primer

Table of Contents

Introduction ..................................................................................................................... 4
Ethernet ........................................................................................................................... 4
Hub .............................................................................................................................. 4
Switch ......................................................................................................................... 4
Firewall ....................................................................................................................... 5
Router .......................................................................................................................... 5
Multifunction Router .................................................................................................. 5
Wireless ........................................................................................................................... 7
Access Point .............................................................................................................. 7
Wireless Router .......................................................................................................... 7
Wireless Network Security ......................................................................................... 7
Broadband ....................................................................................................................... 9
DSL ............................................................................................................................. 9
Cable ........................................................................................................................... 9
Wireless ....................................................................................................................... 9
Satellite ....................................................................................................................... 9
In2 Network .................................................................................................................. 10
Internet Protocols ........................................................................................................ 11
DHCP ........................................................................................................................ 11
DNS ............................................................................................................................ 11
IP ............................................................................................................................... 11
TCP ........................................................................................................................... 11
UDP ........................................................................................................................... 11
HTTP ........................................................................................................................ 11
CCP ........................................................................................................................... 11
Remote Access and Firewalls ....................................................................................... 12
Virtual Private Network ............................................................................................ 12
Remote Control ......................................................................................................... 12
Port Forwarding ......................................................................................................... 12
Appendix A ................................................................................................................... 13
Ethernet Wiring Specification .................................................................................... 13
Introduction

This Networking Primer is designed to introduce some of the basic concepts and review the basics of Ethernet networking. This guide is not a substitute for training and experience in networking.

The In2 Networks control system is based on standard Ethernet networking hardware and protocols. These standards promote interoperability between networking devices from many different manufacturers and vendors. In2 Networks leverages the standards of Ethernet and IP to make home theater control affordable, easy to install, and compatible with hardware and software from many different companies.

This guide reviews important networking topics including Ethernet, Wireless, Broadband, and Internet Protocols

Ethernet

Since the rise of the Internet age, Ethernet has displaced many different wired networking topologies to become the de-facto standard network for personal computers worldwide.

The most current form of Ethernet uses Category 5 (or CAT-5e) cable, which is very inexpensive and readily available. Ethernet equipment is available in several different speeds, and all use the same cable.

<table>
<thead>
<tr>
<th>Ethernet</th>
<th>Speed</th>
<th>Maximum Length</th>
<th>Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Base-T</td>
<td>10 Mbits/second</td>
<td>100 Meters</td>
<td>CAT5</td>
</tr>
<tr>
<td>100Base-T</td>
<td>100 Mbits/second</td>
<td>100 Meters</td>
<td>CAT5e</td>
</tr>
<tr>
<td>1000Base-T</td>
<td>1000 Mbits/second</td>
<td>100 Meters</td>
<td>CAT5e</td>
</tr>
</tbody>
</table>

Hub

Ethernet requires home run wiring from each network device (or computer) to a central concentrator, or a hub. An Ethernet hub passes the electrical signals from each network device to all the other devices connected to the hub.

Switch

A Switch performs the same basic function as a hub, providing ports for several Ethernet devices. A switch differs from a hub, because the switch actually buffers the data before passing it along to the other ports. A switch reduces collisions, which occurs when two packets are sent at the same time and neither one makes it. Switches also allow devices of different speeds to be connected to the same network.
Firewall
A Firewall is a device that blocks all requests from an outside network, and allows all requests from an inside network. There are many different firewall configurations, that restrict access from inside as well as outside. The purpose of a firewall is to protect the inside network from outside attacks.

Router
A router is a device designed to connect two networks together. The most common router function is to link a private network (like an in-home network) to the Internet. Routers typically include an IP address server (DHCP Server) to lease IP addresses to the devices on the network. In home networks, routers lease private addresses to all the computers and Ethernet devices on the network. Private addresses are IP addresses starting with 192.168.x.x or 10.x.x.x, and these addresses are valid on any home or corporate network, but are not valid on the Internet. The router gets a valid Internet address and routes data to all the devices on the network with private addresses.

Multifunction Router
The most common router used in home networks is actually a multifunction router. This device is a router, with a built in DHCP server, a built-in Ethernet switch (usually 4 ports), a built-in Firewall, and usually a built-in wireless access point. Some multifunction routers also include a VPN.

The multifunction router is the least expensive and simplest way to create a secure home network that is easy to access and easy to maintain and configure.

Figure 1 shows a simple PC network configured for broadband Internet access. This exact configuration can be used without the broadband modem for a simple local network of more than one PC.
Figure 1 - Basic Home PC Network
Wireless

Wireless networks are gaining popularity because they solve many of the problems associated with network cabling, and they have finally become affordable and reliable.

There are several different forms of wireless products that are compatible with Ethernet networks, but the most common are:

<table>
<thead>
<tr>
<th>Wireless</th>
<th>Maximum Speed</th>
<th>Typical Range</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>52 Mbits/second</td>
<td>100 Feet</td>
<td>5GHz band, expensive</td>
</tr>
<tr>
<td>802.11b</td>
<td>11 Mbits/second</td>
<td>100 Feet</td>
<td>2.5GHz band</td>
</tr>
<tr>
<td>802.11g</td>
<td>52 Mbits/second</td>
<td>100 Feet</td>
<td>2.5GHz, compatible with b</td>
</tr>
</tbody>
</table>

With all wireless products, the environment has a great impact on the speed and reliability of the communication. 802.11 based wireless connections reduce the speed when the link quality is poor, so even 802.11g equipment can slow down to a 1Mb/sec connection.

Many things affect the link quality, including distance from the access point, clutter and obstructions in the path of the signal (outdoor is better than indoor), and electrical interference. A wireless site survey may be necessary to optimize a wireless network.

Access Point

A wireless access point is a device that connects wireless devices to a wired Ethernet network. Access points must be configured for the desired wireless channel and security settings. An access point may need to obtain an IP address from a router. A wireless router is recommended over a separate router and access point for ease of installation and support.

Wireless Router

A wireless router is simply an access point and a router in a single package. These are commonly paired with a 4 port switch, and represent the simplest and most cost-effective unit for home networks with wireless access.

Wireless Network Security

Wireless networks provide many benefits to the consumer, but also carry security risk. The walls of the home may keep out trespassers, but they don’t protect the network data when wireless networks are used. Any wireless home network should be configured to use WEP (Wireless Encryption Protocol) and a secure key to reduce theft of network access or data.
Figure 2 shows a basic home network with wired and wireless computers. This configuration can also be used without the broadband modem for a local network of wired and wireless computers.
Broadband
There are many options for residential internet access. The In2 Networks control system does not require a broadband connection, but Internet access does unlock several important features, including Firmware updates, maintenance alerts, and remote diagnostics. In2 Networks products are compatible with most Ethernet based broadband equipment.

DSL
DSL (Digital Subscriber Line) modulates the network traffic over a phone line. DSL requires equipment at the CO (Central Office), and availability is limited based on the distance to the CO, and other factors. DSL is typically an always on connection, and the phone line can be used while the network is in use. Filters are required on the phones for the best voice and data quality.

Cable
Cable modems send network traffic through the cable television network. Cable modems also require equipment at the cable office, and are not available in some areas.

Wireless
Wireless broadband connections are available in many different varieties, and use several different technologies, including 802.11. Wireless networks are limited by range and terrain.

Satellite
Satellite based broadband connections send network data from the internet over the satellite link. Upload data is typically sent via modem over a telephone line.
**In2 Network**

In2 networks follow all the same networking rules as the computers on a local network. The nodes need an IP address, and use an Ethernet port just like the computers on the network. The nodes plug into Ethernet ports on a switch or router, and obtain an IP address from the router (DHCP server).

Figure 3 shows an In2 network coexisting with computers on a typical home network.
**Internet Protocols**

There are thousands of different protocols used over the Internet. Each protocol has a specific purpose, and most require other protocols to work correctly (like TCP and UDP). This is a review of some of the basic protocols used by typical home networking equipment.

**DHCP**
Dynamic Host Configuration Protocol (DHCP) is used to lease IP addresses to network devices. The simplest way to set IP addresses in all devices on the network is to enable DHCP on the router.

**DNS**
Domain Name Service (DNS) is used to assign a name to an IP address. DNS causes a request like `www.in2nets.com` to resolve to the IP address of the In2 Networks server.

**IP**
Internet Protocol (IP) is the low level protocol used to route all packets on the Internet. IP sends a data packet to an IP address. The data payload contains other protocols and data.

**TCP**
Transport Control Protocol (TCP) is a connection protocol that makes it easy to send files and data more than 1400 bytes in length. TCP handles missed packets and retries. Most other Internet protocols run on top of TCP or UDP.

**UDP**
Universal Datagram Protocol (UDP) is a packet protocol that handles packet data.

**HTTP**
HyperTerminal Transfer Protocol (HTTP) is used to transfer files over TCP/IP. Web servers use HTTP to serve web pages to clients on the network.

**CCP**
Connect and Control Protocol (CCP) is the protocol the In2 devices use to communicate with each other and with the tablet.
Remote Access and Firewalls

There are several different ways to access devices in the home from the Internet. Each of these access methods has a benefits and drawbacks. Each method is discussed below.

Virtual Private Network
A Virtual Private Network (VPN) is a very secure way to allow access to all the devices in the home network. This is the way corporate networks are configured to allow employees to access corporate resources on the road in a secure way. The VPN is typically a hardware device setup in the corporate DMZ outside the firewall, or it can be a function of the router itself.

Software on the client’s PC makes a secure connection to the VPN server. Once authenticated, the VPN server tunnels network traffic from the client PC to the network behind the firewall – granting access to all nodes in the network, as well as all PCs, printers and servers on the network.

VPNs are very secure, but require software on the client (remote) PC, and can be difficult to setup and configure.

Remote Control
There are several software packages that allow remote access to a PC in the home, including: PC Anywhere, GoToMyPC, VNC, and LogMeIn. These products and services allow you to take control of a PC in the home, granting access to everything in the home network from a virtual PC.

Remote control software is typically easy to setup and secure. The drawback is that these products require a PC to be running all the time within the home.

Port Forwarding
Port forwarding is a setting on the router that allows requests from outside the home to be forwarded to a device in the home. Some consumers and installers are uncomfortable with this solution because it “opens a hole” in the firewall, which can reduce the overall security of the home system.

Port forwarding for remote access entails routing external packets directed to a port (http port 80 for example) to an IP device on the internal network. The device web page is returned as if there were no router or firewall in-between.

Since version 2.1.40 all ICMs include a password protected control page that can be accessed remotely from a forwarded port on the router. Two ports must be forwarded for remote access to work correctly: Port 80 (http) and port 50001 (tcp feedback port). The default password for remote access is “default”, and only one external address is granted access at a time.
Appendix A

Ethernet Wiring Specification

Standard Ethernet cables follow the T568B wiring specification. A straight through Ethernet cable is used for all Ethernet device connections except hub to hub uplink connections. Straight through cables are wired with both ends terminated with the T568B color code. T568B is also used with CAT-5 cables that are punched down to a 110-block wiring patch panel. 66-block telephone patch panels do not meet the specification for Ethernet wiring, and should not be used for Ethernet termination.

### T568B Wiring Specification

<table>
<thead>
<tr>
<th>Pin</th>
<th>Color</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/Orange</td>
<td>Transmit +</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td>Transmit -</td>
</tr>
<tr>
<td>3</td>
<td>White/Green</td>
<td>Receive +</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>White/Blue</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>Receive -</td>
</tr>
<tr>
<td>7</td>
<td>White/Brown</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td></td>
</tr>
</tbody>
</table>

The T568A wiring specification is used to make crossover cables. One end of the cable is terminated using the T568A color code, and the other end of the cable is terminated using the T568B specification.

### T568A Wiring Specification

<table>
<thead>
<tr>
<th>Pin</th>
<th>Color</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/Green</td>
<td>Transmit +</td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>Transmit -</td>
</tr>
<tr>
<td>3</td>
<td>White/Orange</td>
<td>Receive +</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>White/Blue</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Orange</td>
<td>Receive -</td>
</tr>
<tr>
<td>7</td>
<td>White/Brown</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td></td>
</tr>
</tbody>
</table>