The ABCs of Ethernet Troubleshooting, Part 2 — Digging Deeper

The previous *ABCs of Ethernet Troubleshooting* paper (http://www.ctrlink.com/pdf/abc2.pdf) discussed mostly physical and Data Link layer network issues. If problems persist after applying the suggestions in that document, other diagnostic efforts can be taken.

Tools such as protocol analyzers can be used to help diagnose network problems. Protocol analysis is the process of capturing Ethernet frames and analyzing the data in these frames. There are many tools and applications that can help you do this. We like to use one called *Ethereal*. This open-source application is available for free at www.ethereal.com. To use this application on a Windows® computer, you must first install *WinPcap*. Then you can install *Ethereal*. On the latest download of *Ethereal* for Windows, *WinPcap* is installed automatically.

Before using a protocol analyzer such as *Ethereal*, make sure your IT department allows this. Some IT departments may not allow the use of protocol analyzers, especially if they are using hubs in their network infrastructure.

It is our goal to provide you with enough information here to allow you to use a protocol analyzer to help diagnose common network problems. After capturing traffic with *Ethereal*, you can select **Statistics** -> **Protocol Hierarchy** and *Ethereal* will show you the percentage and number of messages received of a specific type. If one type of message is consuming a large amount of bandwidth you can then examine these messages to determine the offending device and then adjust the configuration of this device or contact the device supplier.

Once you have a protocol analyzer application, you can begin to capture frames from your network. Even if you do not fully understand TCP/IP or the protocols used by your vendor's equipment, protocol analyzers such as *Ethereal* can decode many of the messages for you and help diagnose problems. Each captured frame is decoded and explained for you.

It is handy to understand some of the OSI model or TCP/IP model when viewing Ethernet frames. In the previous *ABCs of Ethernet Troubleshooting* we discussed mostly physical and Data Link solutions to problems. Ironically, when we say "digging deeper", we actually mean going higher into the OSI or TCP/IP model. When using a protocol analyzer, higher level issues (such as those at the network or transport layer) can be examined. An Ethernet frame can be composed of information for many layers of communication.

OSI Model	TCP/IP Model
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transportation Layer	Transport Layer (TCP/UDP)
Network Layer	Internet Layer (IP)
Data Link Layer	Network Access Layer
Physical Layer	

When you view a webpage, for example, an Ethernet frame is sent to you that contains an Ethernet source and destination. This is part of the Data Link layer (OSI model) or the Network Access layer (TCP/IP model). The frame also has an IP address source and destination that are part of the Network layer (OSI model) or the Internet layer (TCP/IP model). There is also a TCP section that belongs to the Transport layer. And there is an HTTP (Hypertext Transfer Protocol) section from the Application layer.

Protocol analyzers such as *Ethereal* will decode each captured Ethernet frame and show you the data from the various layers within each captured frame.

Receiving Data

If you are using switches in your network, your computer can monitor all the traffic you send or receive — including broadcast messages. Normally you will not be able to see what other computers are sending or receiving (except for broadcast messages). To see directed messages between other devices, you must have a switch that supports port mirroring. This feature allows you to select the ports you wish to monitor and copy this traffic to a designated port on the switch. This feature is available on our EISX8M, EICP8M and all managed EISB products.

Contemporary Control Systems, Inc. • *2431 Curtiss Street* • *Downers Grove, Illinois 60515* • *USA*
Telephone *1-630-963-7070* **Fax** *1-630-963-0109* **E-mail** *info@ccontrols.com* **Web** *www.ccontrols.com, www.CTRLink.com*

Contemporary Controls Ltd • *Sovereign Court Two* • *University of Warwick Science Park* • *Sir William Lyons Road* • *Coventry CV4 7EZ UK*
Telephone *+44 (0)24 7641 3786* **Fax** *+44 (0)24 7641 3923* **E-mail** *info@ccontrols.co.uk* **Web** *www.ccontrols.co.uk*

Request/Response

Most Ethernet traffic contains a request from one device to another. The request frame is followed by one or many response frames. Some Ethernet communication also supports producer/consumer messaging using multicast messages (such as EtherNet/IP).

TCP/IP

Most protocols that communicate over Ethernet use TCP/IP as the basis of their communication. There are some legacy communications which utilize IPX/SPX or NetBEUI, but most Ethernet communications today use TCP/IP. Thus, it is helpful to understand some TCP/IP basics. When TCP/IP communications occur, they utilize either TCP or UDP messaging. TCP is a *connected* protocol. That is, two devices create a *virtual* connection and then exchange data. UDP is *connectionless*. One device can send another device a UDP message at any time. UDP is the only protocol that supports IP multicast messaging.

Just as the Data Link layer has Ethernet or MAC addresses to identify the sender and the recipient, the IP layer has *IP addresses* and the Transport layer has *port numbers* to identify the service on each device responsible for sending the data and which service is supposed to receive the data. For example, when viewing a webpage your computer sends a request to port 80 of the server that hosts the webpage you wish to view. The destination port of an Ethernet request generally tells you which Application layer protocol is being used. Protocol analyzers such as *Ethereal* will tell you which protocol is being used if they support this protocol. *Ethereal* currently supports over 700 protocols.

ARP

When two Ethernet devices communicate, they do not really use IP addresses to send each other messages. First, each device looks at its ARP cache which contains a list of IP addresses and corresponding Ethernet (MAC) addresses. If the cache has no entry for the IP address in question, the device sends an ARP broadcast that basically asks if anyone knows the Ethernet address for the IP address in question. When the device receives a response to its ARP request, it transmits an IP message. Without this ARP response, the device cannot transmit its IP message. For example, if you try to ping a computer on your network, your computer will first look at its ARP cache.

TCP Connection

When viewing TCP Ethernet frames, you generally see the connection request then the connection response. After the connection is made, data can be transferred. The connection request, connection response and TCP data are all *TCP* frames. When the connection is requested, the TCP message has its SYN flag set. The other device will respond with its SYN and ACK flags set (OK) or it's SYN and RST flags set (Not OK). If the response is OK, then data can be transferred. To end the TCP connection, an FIN flag is set in the message.

TCP Protocols

You may find many TCP protocols flowing through your network. *HTTP* provides webpages to your browser. *TELNET* allows computer systems to interact in a command mode. *SMTP* is for exchanging email. *FTP* is used to send/receive files. *Modbus/TCP* uses TCP to send/receive I/O data between devices.

UDP

UDP is a protocol that does not require a connection. One device can send another device a UDP message at any time. This is attractive if the Application layer protocol already handles connections. A lot of industrial protocols were initially written for very low-end communication systems and therefore do a lot of work themselves, such as creating connections, handling acknowledgements, handling re-transmissions, etc. They basically use TCP/IP to just carry their industrial protocol messages. UDP can also be used for multicast messaging. *EtherNet/IP* uses UDP multicasts for its implicit communications. UDP can also be used for broadcast messages.

UDP Protocols

There are many UDP protocols such as *SNMP*, *DNS*, *DHCP*, *Windows Browser Service*, *VoIP*, etc.

IP Protocols

IP Protocols (or Internet layer protocols) are used, usually, as control messages between TCP/IP devices. These include *STP* (Spanning Tree Protocol) control messages, *ICMP* (Internet Control Management Protocol) messages (one type is used for ping), *IGMP* (Internet Group Management Protocol) messages, etc. These are to be expected. However, if their frequency is very high, there may be an issue. STP control messages generally appear once every two seconds and are used on networks to provide redundancy.

PING

PING (Packet InterNet Grouper) is really an ICMP echo request and the response is really an ICMP echo reply. Ping is used to confirm that a device is at a specific IP address. Pings are used by some network monitoring tools to keep track of devices on the network. Pings are also used by some network worms to gain control of computers. Be aware of which computer is originating the pings — and if they occur on a frequent basis, make sure the originator is a device which should be sending pings.

IPX/SPX

Some networks use IPX/SPX communication between their devices. IPX/SPX is similar to TCP/IP, but they are not compatible. Some Windows boxes automatically enable IPX/SPX communications. Supporting more protocols is normally not a problem. However, IPX/SPX devices typically use *SAP* (Service Advertising Protocol) to announce their presence to the network on a periodic basis. If you are not using IPX/SPX in your communications, this can create unneeded network traffic that can easily be removed from the network by disabling IPX/SPX support in your Windows computers and your printers.

BROWSE/NetBIOS/NBNS

Windows computers use *NetBIOS* protocol (over TCP/IP) to make themselves known to the network and as a simple network naming system (like DNS). *NetBIOS* is used for the *Browser* service and for *WINS* (Windows Internet Naming Service) as a way for Windows devices to find each other on the network and to share data. This typically is used for file sharing and Windows networking. These messages are broadcasts and occur on a frequent basis.

HTTP

HTTP (HyperText Transport Protocol) is used to carry HTML webpages from webservers and browsers such as *Internet Explorer* use it to request and receive webpages.

High Frequency of Messaging

Many of the above protocols will most likely appear on your network. However, if their usage is too frequent there could be a configuration issue with one of your devices or a network worm or virus may have infected one of your Windows computers. You may want to capture Ethernet traffic when everything is working fine and then this can be used for comparison if problems occur. This can help you distinguish between normal traffic (when everything is working fine) and abnormal traffic.

Unusual Network Uses

When watching network traffic you may find unusual uses of your network bandwidth. The Internet has spawned many interesting ways of using TCP/IP and, when used over an office network, this may not cause a problem. However, this may not be the case for control networks. We have heard of a whole control system being taken down by one technician who listened to Internet Radio during his break. These new protocols may be decodable by *Ethereal*. *MSN* instant messenger (IM) uses a protocol called *MSNMS* which can be decoded by *Ethereal*.

Internet Radio applications such as *Windows Media Player* uses *HTTP* or *RTSP* to transfer music from various radio stations over the Internet. *RTSP* may be used by other audio/video entities on your network such as video cameras.

An application known as *BitTorrent* is used to share files among its users. It can move lots of data through your network. It uses TCP to transfer its data. It normally uses port 6881 — but if another port is used, protocol analyzers may have trouble identifying this traffic.

Broadcast, Multicast and Directed Messages

You need to be aware of the type of Ethernet messages traveling through your network. Ethernet messages can be broadcast, multicast or directed messages.* Excessive broadcast or multicast traffic (with unmanaged switches) can burden network devices that must review unwanted messages in software before discarding them. This could potentially overwhelm a device. Directed messages are usually not as threatening — however, you must consider where these messages are going. If they are all directed to one device then this device can be overwhelmed. If they all travel through a backbone then the backbone can become overwhelmed.

* Broadcasts are received by everyone. Multicasts are received by everyone in an *unmanaged* network — but if using *managed* switches and IGMP snooping, only subscribing devices receive multicasts.

The Future

The Internet is constantly changing and so are the protocols based on TCP/IP. Protocol analyzers such as *Ethereal* are also being updated with support for an ever-growing number of protocols. In the future you may see newer protocols than are mentioned here. When the protocol analyzer gives you a protocol name for a captured message you are unfamiliar with you can search the Internet for information on it and perhaps find others experiencing the same problems.