

## 6.0—Network Health, Monitoring, & System Maintenance

---

*By Mark Mullins. Reprinted with permission from the Industrial Ethernet Book, [www.ethernet.industrial-networking.com](http://www.ethernet.industrial-networking.com), ©2001 GGH Marketing Communications and Fluke Networks.*

### 6.1 What is it that makes a network run well?

Fluke Networks has profiled dozens of networks worldwide in an effort to determine the answer. In our research, the best run-networks had thirtyfive times less downtime, resulting in annual savings of over \$227,000. Not surprisingly, users of these networks were the most satisfied of all groups studied. One surprising conclusion is that the number of support staff per end-user of these well-run networks was actually lower than that of the poorly-performing networks.

So how does a network support group enter this desirable group? In studying this question, Fluke Networks uncovered seven “best practices” of well-run networks. They are:

- Management Involvement
- Preparation & Planning
- Problem Prevention
- Early Problem Detection
- Quick Problem Isolation and Resolution
- Invest in Tools and Training
- Quality Improvement Approach

Having the right tools for monitoring, documenting, and troubleshooting your network helps with nearly all of these areas. Let’s look at each of these three functions and discuss the tools for each.

#### Monitoring

Monitoring your network is essential to find problems before they become serious, and just to have a general idea of what is going on in your network. When monitoring, there are a number of key questions you’ll need the answer to:

- Who’s talking to whom?

- What are they talking about?
- Are there problems out there?

The most important tools are protocol analyzers, embedded **RMON** (Remote **MON**itoring) agents, and external RMON agents.

*Protocol analyzers* allow the network engineer to capture traffic passing by on the network, and then decode that traffic in order to understand the traffic. For example, single frame may contain IP addressing information, TCP flow control, and HTTP commands. The analyzer needs to be able to decode each of the protocols so that the user is not presented with a bunch of unintelligible hexadecimal. Billions of such frames may travel over a network in the course of a day, so the analyzer needs to be set up to filter, that is to capture only certain types or sources of frames, as well as trigger, or start capturing traffic after a certain type of frame is detected.

Low cost analyzers have trouble keeping up with fast or busy networks, while higher-priced ones offer more memory, and specialized hardware to keep up with even gigabit ethernet. Higher priced ones also decode more protocols, and offer expert analysis of traffic to find problems faster.

Embedded agents are found in most of today's switches and routers, and collect information on activities in each interface of the device. This information is stored in a Management Information Base (MIB), and can be accessed by devices using Simple Network Management Protocol (SNMP). External RMON agents do much the same thing, except that they offer much greater depth of information, and they have to be purchased (where embedded RMON is usually a no-cost feature).

In terms of depth, embedded RMON agents generally offer only a very-high level overview of what's happening on the network interface: utilization statistics (how 'busy' the interface is), and error counts. Some embedded RMON agents can also generate alarms when certain thresholds are exceeded. External agents, on the other hand, generally offer much greater detail, such as which devices are using the port, and the ability to capture traffic, like a protocol analyzer.

Most newer external agents support RMON2, which adds the ability to track application-layer traffic. This is important in determining who is really using bandwidth. A quick comparison of the detail yielded by the

three approaches is instructive. An Embedded RMON agent would tell you that Ethernet Interface 42 is very busy. An external RMON probe could tell you that a certain PC is sending a lot of traffic to the router. An RMON2 probe could tell you that 'Bob's PC' is sending HTTP traffic to the Web site `hotjobs.com. Obviously, RMON2 provides much more detail. And, not surprisingly, that detail comes at a cost.

## Monitoring Switched Networks

The main issue with external probes and protocol analyzers is where to put them. Before the advent of switched Ethernet, a probe placed anywhere on the network could see all the traffic on the network and provide total visibility. Today, switched networks provide higher performance and faster response, and are recommended for industrial networks. Unfortunately, switched networks only send traffic to the intended recipient, so special allowances must be made so that the probe can monitor the relevant part of the network.

One of the simplest methods is to use port mirroring. By appropriate commands to the switch, it can be configured to copy traffic at one interface to another one where the probe is connected. The advantages of this method are the fact that it allows you to monitor whichever port you want. The disadvantage is that while monitoring that port, you have no idea what's happening on any other port. In addition, port mirroring will generally forward only good frames, and often, it's the bad ones you're looking for. Finally, if the switch is very busy it may not send all the frames to the mirror port - so that one critical frame causing the problem might be missed.



**Tip 21** – For more thorough monitoring, a tap may be installed into critical links. This is simply a hardware device that allows the probe to see all the traffic on the link. Unlike mirroring, taps never miss a frame or an error. However, they have to be installed on every port that must be monitored. And like mirroring, they give visibility into only one link at a time.

To get complete vision when monitoring a switched network, a combination of approaches must be used. Embedded agents can be monitored to get an overview of what's happening on every interface in the network. External RMON2 agents can be installed with taps to provide constant monitoring of key links, such as those between switches, to servers, and wide area networks. Additional RMON agents can be con-

nected to switches and connected as needed using port mirroring to monitor problem ports found with the embedded agents.

## Documenting



**Tip 22 – Documenting your network is essential for two reasons.** First, when it becomes necessary to upgrade or expand your network, you'll need an idea of where to start.

Second, knowing the normal state of your network is essential when it's time to troubleshoot. If a doctor didn't know what a normal temperature or blood pressure is, those measurements would be meaningless. Each network has its own normal operating condition, so it's important to know what yours looks like—before a problem arises.

A good example of this is a network at an automotive plant in Michigan, where Fluke Networks was offering training on network documenting. This customer had recently upgraded its network and was extremely pleased with how well it was operating. In the course of the class, we documented a number of interesting characteristics of this network — over 1,100 stations in one collision domain, over 400 errored frames in two hours, sustained peak utilization over 70%, and an average of 2% collisions. Any of these would be considered serious problems in most networks, but this was 'normal' for them. If they ever experience a problem they need only look for what changed, rather than waste time tracking down unrelated issues.

Documenting is the process of recording the state of your network. The two main questions are, "what's out there", and "how is it performing". By keeping records provided through monitoring systems, a good idea of normal performance can be obtained. Some additional documenting tools can be valuable.

The first of these can be called SNMP/Ping Monitors. These discover the devices in the network and then gather SNMP information from these devices. They also offer some powerful documenting features. Microsoft Visio, for example finds the devices and then provides a complete network diagram at a very reasonable price. Fluke Networks' Network Inspector provides a wide variety of reports, and can plot SNMP statistics for up to a 24 hour period. Other reporting packages are available from Concord Communications, InfoVista, and Visual Networks.

## Troubleshooting

When something goes wrong, it is usually important that it get fixed as fast as possible. Many of the tools noted above can help with the troubleshooting process. In fact, if everyone installed everything noted above, and never let any users or applications near the network, there wouldn't be much need for specialized troubleshooting tools. For the real world, however, a number of specialized tools are available to solve problems fast.

The most common of these is the Protocol Analyzer, loaded onto a laptop computer. While indepth analysis capabilities allows this to tackle the most challenging of network problems, the complex set-up and limited vision in switched networks make them a troubleshooting tool of last resort.

The next most common tool is the *cable tester*, which can help track down the most common cause of network problems—cabling. Basic and advanced types are available. Basic testers will find broken cables, shorts, and split pairs. A split pair occurs when two channels constituting a transmit plus and transmit minus are not connected to a pair that is twisted together. The result can be transmission errors or even a complete breakdown in communications. Many low cost testers cannot find this problem—use of these is not recommended. Some basic testers can display the distance to the fault, which can greatly speed troubleshooting.



**Tip 23 – Advanced cable testers not only find these common problems, but can also determine the performance level of the cable.** In the days of 10-Mb Ethernet, almost any

cable could handle the requirements. Higher-speed networks, at 100-Mb and gigabit speeds, place significantly higher demands on the cabling and more advanced tools are needed to determine if the cable is up to the task. These advanced testers measure parameters such as crosstalk and return loss and can certify the performance of cabling for high speed networks. They also cost about four times what a basic tester costs! If cable performance is verified with an advanced tester at installation, most sites need only the basic tester for daily troubleshooting. However, as higher performance networks become more common, the need for advanced testers will grow accordingly.

A new class of tester, the Integrated Network Analyzer, offers the fastest approach to network troubleshooting. These devices incorporate the

most commonly used capabilities of protocol analyzers and cable testers to provide a complete solution for troubleshooting. Portability and ease of operation are two key features. Some also offer advanced features such as the ability to discover devices on the network (like SNMP/Ping Monitors) and SNMP queries of network devices.

*Mark Mullins is Marketing Manager for Enterprise Systems at Fluke Networks in Everett, Washington, USA. He holds a Bachelor's in Computer Science and an MBA from the University of Washington. He has been with Fluke for 21 years, and was one of the founders of Fluke Networks.*

## 6.1 Popular PC-Based Ethernet Utilities, Software, and Tools

PC-based network sniffers operate on a PC that links to an Ethernet LAN via a hub (not a switch) and collect data as it goes by. They break down and organize Ethernet frames and/or TCP/IP packets so you can make sense of what's happening on your network. Use them to identify chattering nodes, corrupted data, and mysterious sources of network traffic.

If your TCP/IP sessions “hang up,” a sniffer might tell you which device sent the last packet and which one failed to respond. Similarly, if devices are responding slowly, time stamps will show you which system is waiting and which system is responding slowly. The sniffer can monitor broadcast or multicast storms and packet errors. By recording and displaying the traffic on the Ethernet wire, or a filtered segment of the traffic, you will pinpoint problems and intelligently improve network performance.

**Table 6-1 – Netboy Suite from WhiteHat**

Package:	Netboy Suite from WhiteHat <a href="http://www.whitehatinc.com/nttools/netboy/">http://www.whitehatinc.com/nttools/netboy/</a>
Platform(s):	Windows
Description:	<p>Netboy is composed of three software programs: EtherBoy, PacketBoy, and WebBoy.</p> <p>EtherBoy displays all traffic on your LAN and identifies all devices on your LAN including potential security threats. You can define custom protocols, display real-time traffic statistics and protocol breakdowns on individual hosts, monitor individual hosts and links, and customize alarm triggers.</p> <p>PacketBoy is a packet analyzer/decoder package capable of decoding many of the commonly used LAN protocols. Protocols that can be decoded include TCP/IP, IPX (Novell Netware), Appletalk, Banyan, and DECNET protocol suites. Multiple captures can be loaded and saved to disk.</p> <p>WebBoy is an Internet/intranet monitoring package. It provides statistics on standard Web traffic including URLs accessed, cache hit ratios, Internet protocols, and user-defined protocols.</p>

**Table 6-2 – Sniffer Basic from Network Associates**

Package:	Sniffer Basic from Network Associates <a href="http://www.sniffer.com/products/sniffer-basic/">http://www.sniffer.com/products/sniffer-basic/</a>
Platform(s):	Windows
Description:	Very configurable, allows you to write protocol decoder modules for custom protocols; good user interface. Generates real-time traffic statistics, with alarms.

**Table 6-3 – EtherPeek by the AG Group**

Package:	EtherPeek by The AG Group <a href="http://www.wildpackets.com/products/etherpeek/">http://www.wildpackets.com/products/etherpeek/</a>
Platform(s):	Windows and Macintosh
Description:	Similar to Sniffer Basic; includes support and runs on more platforms.

**Table 6-4 – Network Spy by Code Maniac**

Package:	Network Spy by Code Maniac <a href="http://www.network-spy.com/netspy.php">http://www.network-spy.com/netspy.php</a>
Platform(s):	Windows
Licensing:	Shareware
Description:	This is a basic graphical sniffer. The shareware version will capture for 30 seconds at a time, and must be restarted after each capture session. Interesting features: The network load graph is more typical of higher-end packages for network administrators. Also included when you become a registered user: Internet Maniac, which does Ping, Traceroute, Port Scan, etc. when you register Network Spy.

**Table 6-5 – The Gobbler by Tirza van Rijn**

Package:	The Gobbler by Tirza van Rijn, University of Delft, The Netherlands <a href="http://www.umich.edu/~archive/msdos/communications/wattcp/delft/gobbler.zip">http://www.umich.edu/~archive/msdos/communications/wattcp/delft/gobbler.zip</a>
Platform(s):	DOS
User interface:	Text graphics
Licensing:	Freeware with source code available.
Description:	A highly regarded freeware DOS Ethernet sniffer. Decodes the Ethernet, IP, TCP, and UDP layers and low-level protocols like ARP and ICMP. The interface is easy to maneuver.

**Table 6-6 – Analyzer, WinDump, and WinPCap**

Package:	Analyzer, WinDump, and WinPCap by Piero Viano, Paolo Politano, and Loris Degioanni <a href="http://netgroup-serv.polito.it/analyzer/">http://netgroup-serv.polito.it/analyzer/</a>
Platform(s):	Windows
Licensing:	Freeware
Description:	Analyzer is a user interface built on top of WinPCap ( <a href="http://netgroup-serv.polito.it/winpcap/">http://netgroup-serv.polito.it/winpcap/</a> ), which is a Windows port of Libpcap. They have also ported tcpdump ( <a href="http://tangentsoft.net/wskfaq/resources/#tcpdump">http://tangentsoft.net/wskfaq/resources/#tcpdump</a> ) to a Windows program called WinDump ( <a href="http://netgroup-serv.polito.it/windump/install/">http://netgroup-serv.polito.it/windump/install/</a> ). The features and usability of the interface are very good. Documentation is in Italian.

**Table 6-7 – Ethereal**

Package:	Ethereal <a href="http://www.ethereal.com">http://www.ethereal.com</a>
Platform(s):	UNIX, Windows
Licensing:	GPL
Description:	<p>Ethereal is a free network protocol analyzer for UNIX and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.</p> <p>Ethereal can remotely debug network problems: use Telnet to access a UNIX server at a remote site, upload a copy of Ethereal, record network traffic and save it to a file, retrieve the file, and view it with Ethereal. It may save you a plane ticket to some remote location.</p>

**Table 6-8 – SPY by Christian Lorenz**

Package:	SPY by Christian Lorenz <a href="http://www.gromeck.de/Spy/">http://www.gromeck.de/Spy/</a>
Platform(s):	UNIX
Price:	Free for noncommercial usage, approx. \$430 for single license
Description:	<p>SPY is a LAN Protocol Analyzer running on UNIX platforms. It has a built-in capture facility for all attached network interfaces. This capture facility supports Ethernet, FDDI, SLIP/CSLIP, PPP, and PLIP.</p> <p>SPY also provides a user capture interface (UCI), which can be used to feed SPY with data packets from your own program. Of course, captured data can be stored to files in binary format for later analysis.</p> <p>The capture facility provides prefilters on the MAC and IP layer (this does not mean that SPY supports only IP networks). These prefilters allow the reduction of network traffic to relevant data on the basis of addresses (sending and/or receiving hosts) or encapsulated protocols.</p>

**Table 6-9 – Atelier Web Security Port Scanner**

Package:	Atelier Web Security Port Scanner by Atelier <a href="http://www.atelierweb.com/pscan/">http://www.atelierweb.com/pscan/</a>
Platform(s):	Windows
Licensing:	Shareware
Description:	<p>A port scanner probes your PC for open ports that may be used by external applications and thus present security threats. It has an Internet Assigned Numbers Authority (IANA) Ports Database, a useful function that tells what purpose the port is registered for, who registered it, and what other uses it's known to have. It also tells you which program is listening on a port. The user interface is very good.</p>