**Network Measurement and Monitoring Tools**

**Introduction**

Network measurements are essential to keep a network running efficiently, for detecting bottlenecks/system faults and for forecasting future network requirements. Dealing with performance problems or faults (hardware and software) is relatively easy providing the network's usual performance is well documented. Likely bottlenecks, which can degrade performance, include: CPUs (too slow), memory (not enough), disk controllers, and network cards/media.

Monitoring performance is a necessary part of preventive maintenance for your computer network. Through monitoring, you obtain performance data that is useful in diagnosing system problems and in planning for the growth in demand for system resources. You can monitor server and network performance with a variety of utility programmes available with most operating systems or use specialized test instruments such as field testers for diagnosing cabling problems and sophisticated monitoring and management tools for network performance analysis.

With the increasing importance of wireless networks and real time communications like VoIP, specialist tools or add-ons to existing ones have been developed to help with the additional monitoring and measurement demands of these technologies.

**Cable Measurement and Field test instruments**

Cabling is the basic building block for most networks but gets the least attention even though without it a network will not function at all. Cable installers need to be up to date on the latest cabling installation and conformance techniques to make sure that the work meets international standards.

**Twisted Pair cable testing**

Cat5 UTP copper is the dominant choice for today’s LANs for speeds up 1Gbps. Various tests may need to be carried out depending on type of installation (home or commercial premises). At the basic level continuity checker or multimeters are used to test end-to-end connections.

Verification field testers also provide wire map measurements to verify that the plug/socket connections (crossovers etc.) are correct and there are no obvious wiring mistakes. Some testers (e.g. the Fluke Microscanner) have TDR (Time Domain Reflectometer) capabilities for measuring cable length to verify that it doesn’t exceed the specified maximum (e.g. 100m for 100BaseT). TDRs measure length based on propagation delay (Tp) and the nominal velocity of propagation (NVP) expressed as a fraction of the speed of light (c=3x108 m/s).

Length = NVP x Tp metres

N.B. *max channel length for Cat 5e UTP =100m (PC to Hub), but the length of fixed cable (socket to socket should be 90m max to allow for patch leads)*

For accurate measurements of length field testers must be calibrated for the cable type used since insulation and cable twists can have an effect on Tp.

Certification of new cable plants is done to ensure that they meet the demands of new applications. Cable performance certification requires a more advanced field tester such as the Fluke Omniscanner which able to measure other cable parameters such as propagation delay, attenuation loss, crosstalk etc. at a range of frequencies to meet the standard which the installation is to conform to (e.g. TIA 568A for Cat5e).

****

Figure 1 Cable testers

**Optical Fibre cable testing**

There are a variety of tools available for testing fibre cable. White light sources are used to check continuity, laser based devices are used to detect breaks, loss test kits to measure attenuation, optical TDRs for length measurements and certification tools to measure parameters for compliance with standards. (e.g. the Fluke Optifiber certifying OTDR is an integrated tool which can measure most fibre cable parameters, diagnose problems and test for standards compliance).

**System Monitoring and Diagnostic Tools (Windows)**

Windows (7/2008/12) provides several utilities for monitoring network performance and diagnosing problems and faults:

**Event Viewer**

The Event Viewer allows you to view the events in the computer log to help locate problems. Using the event logs in Event Viewer, you can gather information about hardware, software, and system problems, and you can monitor Windows security events.

Windows records events in three kinds of logs:

***Application log***

The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The program developer decides which events to record.

***System log***

The system log contains events logged by the Windows system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows.

***Security log***

The security log can record security events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

Event Viewer displays these types of events:

**Error**

A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged.

**Warning**

An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged.

**Information**

An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.

**Audit**

A security access attempt. For example, a user's successful attempt to log on the system will be logged as a Success Audit event.

**Performance Console**

The primary monitoring tools in Windows are in the *Performance console.* These are *System Monitor*, and *Performance Logs and Alerts*. They can be configured to show a wide range of network related events in graphical form to help diagnose performance problems.

***System Monitor***

With System Monitor, you can measure the performance of your own computer or other computers on a network:

* Collect and view real-time performance data on a local computer or from several remote computers.
* View data collected either currently or previously in a counter log.
* Present data in a printable graph, histogram, or report view, see Figure 2
* Incorporate System Monitor functionality into Microsoft Word or other applications in the Microsoft Office suite by means of Automation.
* Create HTML pages from performance views.
* Create reusable monitoring configurations that can be installed on other computers using Microsoft Management Console.

With System Monitor, you can collect and view extensive data about the usage of hardware resources and the activity of system services on computers you administer. You can define the data you want the graph to collect in various ways and collect data from your local computer or from other computers on the network where you have permission.

To select the data to be collected, you specify performance objects; performance counters, and object instances.

Some objects provide data on system resources (such as memory); others provide data on the operation of applications (for example, system services or applications running on your computer).

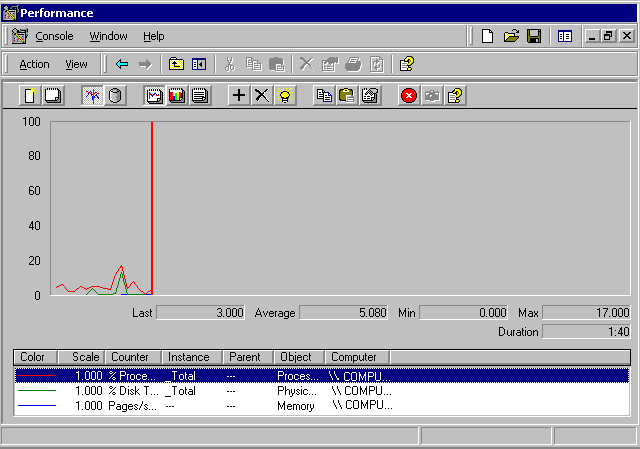


Figure 2 System monitor (chart display)

N.B. *You can further extend use of System Monitor by incorporating its functionality into Microsoft Word or other Microsoft applications by means of Automation.*

***Performance Logs and Alerts***

With Performance Logs and Alerts you can collect performance data automatically from local or remote computers. You can view logged counter data using *System Monitor* or export the data to spreadsheet programs or databases for analysis and report generation, see Figure 3.

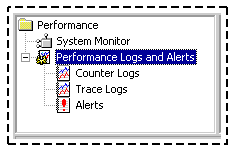


Figure 3 Performance console logs and alerts

Similar to System Monitor, Performance Logs and Alerts supports defining performance objects, performance counters, and object instances, and setting sampling intervals for monitoring data about hardware resources and system services.

Performance Logs and Alerts also offer other options related to recording performance data.

**Task Manager**

Task Manager offers an immediate overview of system activity and performance that can be used for troubleshooting and bottleneck analysis.

Task Manager lacks the logging and alert capabilities of the Performance although the data displayed by Task Manager comes from the same source. Task Manager does not have access to the breadth of information available from all installed counters but provides some extra capabilities not available with the Performance console such as a list of running processes and applications and measures of their performance, see Figure 4.

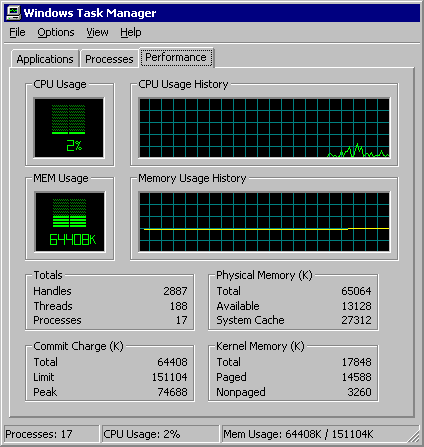


Figure 4 Task manager performance tab

**Network Monitor** (included with Windows Server, but an Win 7 version is also available)

Network monitor is a network performance/protocol analyzer – *see later for basic operation of this type of tool.*

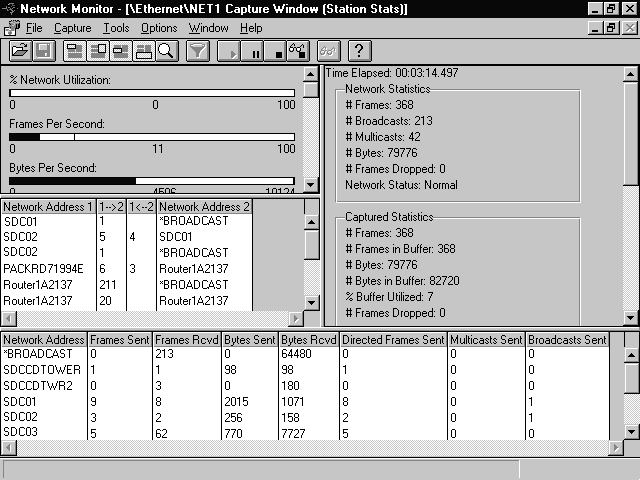
****You would use Network Monitor to capture and display the frames or packets on the local network interface and associated traffic statistics, see Figure 5.

Figure 5 Network Monitor statistics

Windows 2008/12 Server receives from a local area network (LAN). You can use Network Monitor to detect and troubleshoot networking problems that the local computer might experience. For example, you might use Network Monitor to diagnose hardware and software problems when the server computer cannot communicate with other computers. Packets captured by Network Monitor can be saved for later analysis.

Network application developers can use Network Monitor to monitor and debug network applications as they are developed.

N.B. *Microsoft Systems Management Server includes a full version of Network Monitor. In addition to the functionality in Windows Network Monitor, Systems Management Server Network Monitor can capture frames sent to and from all computers in a network segment, i.e. it can operate in promiscuous mode.*

**TCP/IP and NetBIOS utilities**

Table1 lists the diagnostic utilities included with Microsoft Windows TCP/IP. All are useful to identify and resolve TCP/IP networking problems.

When you troubleshoot a TCP/IP networking problem, begin by checking the TCP/IP configuration on the computer that is experiencing the problem and then go on to test the connectivity with other network computers. For a more complete description of using these tools see the laboratory reference guide: *useutils\_05.doc.*

|  |  |
| --- | --- |
| **Utility** | **Used to** |

|  |  |
| --- | --- |
| Arp | View the ARP (Address Resolution Protocol) cache on the interface of the local computer to detect invalid entries. |
| Hostname | Display the host name of the computer. |
| Ipconfig | Display current TCP/IP network configuration values, and update or release Dynamic Host Configuration Protocol (DHCP) allocated leases, and display, register, or flush Domain Name System (DNS) names. |
| Nbtstat | Check the state of current NetBIOS over TCP/IP connections, update the NetBIOS name cache, and determine the registered names and scope ID. |
| Netstat | Display statistics for current TCP/IP connections. |
| Netdiag | Check all aspects of the network connection. |
| Nslookup | Check records, domain host aliases, domain host services, and operating system information by querying Internet domain name servers. |
| Pathping | Trace a path to a remote system and report packet losses at each router along the way. |
| Ping | Send ICMP Echo Requests to verify that TCP/IP is configured correctly and that a remote TCP/IP system is available. |
| Route | Display the IP routing table, and add or delete IP routes. |
| Tracert | Trace a path to a remote system. |

Table 1 TCP/IP Diagnostic Utilities

N.B. *Netdiag is a Windows utility that helps isolate networking and connectivity problems by performing a series of tests to determine the state of your network client and whether it is functional. These tests and the key network status information they expose give network administrators and support personnel a more direct means of identifying and isolating network problems. Netdiag diagnoses network problems by checking all aspects of a host computer’s network configuration and connections. Beyond troubleshooting TCP/IP issues, it also examines a host computer’s IPX and NetWare configurations.*

**Network performance measurement tools**

Ping can be used to rudimentary performance tests, but there are many other open source and third part testing tools from network test specialists such Ixia.

IxChariot is used for network performance testing. Many websites also offer broadband testing tools.

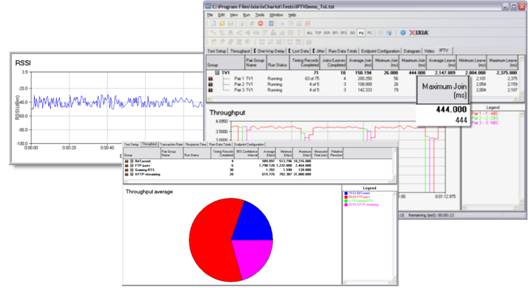


Figure 6 IxChariot GUI and Qcheck

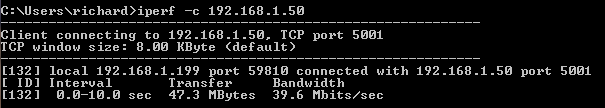
Ixia also offer a very useful tool called Q-Check for free that allows you to measure network delays and throughput and will be used extensively in the labs.

For a response time test, Qcheck returns the minimum, maximum and average number of seconds it took to complete a transaction. For a throughput test, Qcheck returns the amount of data per second that was successfully sent between the two endpoints. For a streaming test, Qcheck returns the rate at which the streaming data was received by the second endpoint and the amount of packet loss that occurred. For a traceroute test, Qcheck returns the number of hops, average hop latency, and the address and names of the host at each hop

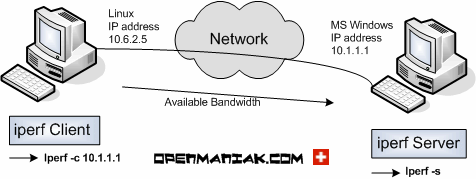
There are many free broadband testing tools that you can download or run on-line. The Global Broadband Speedtest site at speedtest.net is particularly useful for measuring latency and upload and download speeds. Other sites also provide tests of VoIP capability for your broadband link.

**iPerf**

**iPerf** is a command line network testing tool. It can create TCP and UDP data streams and measure the throughput of a network link.

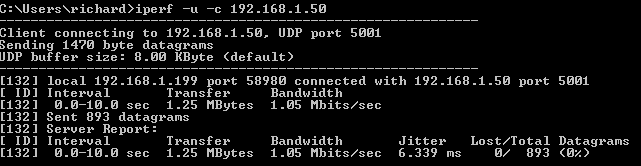
****

It employs a client and server functionality, to measure the throughput between the two ends, either unidirectonally or bidirectionally.

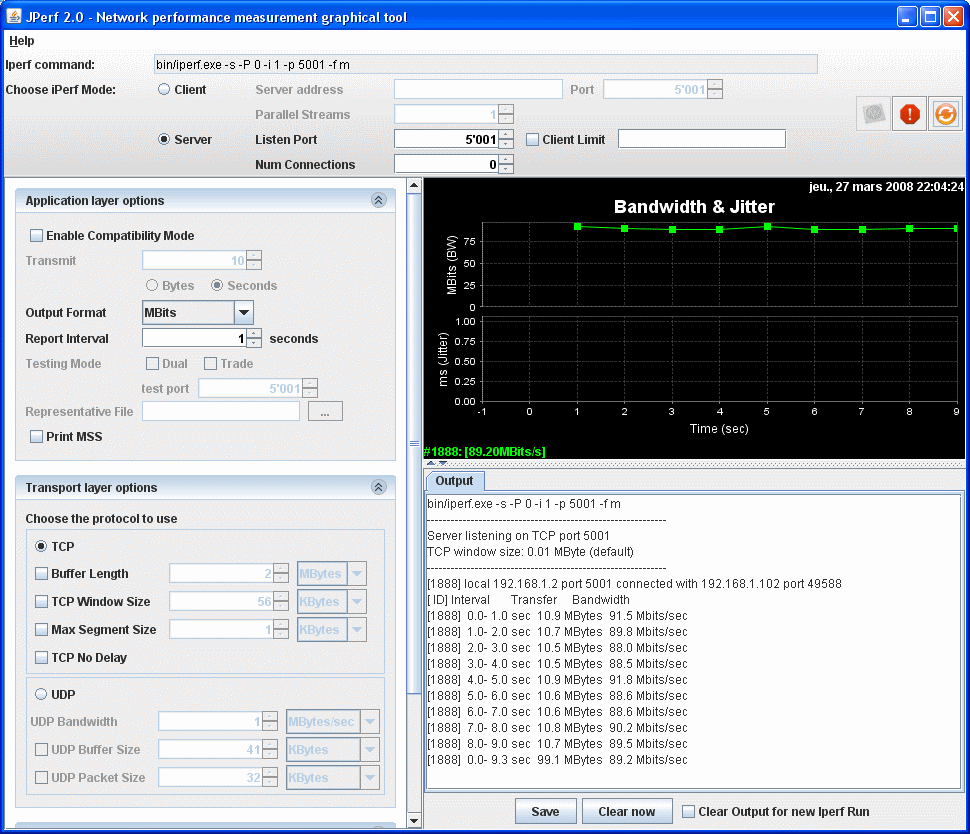


iPerf was developed to simplify TCP performance tuning by making it easy to measure maximum throughput and bandwidth.

When used with UDP, iPerf can also measure datagram loss and jitter. iPerf can be run over any kind of IP network, including local Ethernet LANs, Internet access links, and Wi-Fi networks.



There is a GUI front end available called jPerf that allows results to be displayed as graphs and charts.



**SNMP**

TCP/IP networks use a standard management protocol called Simple Network Management Protocol (SNMP) developed as a solution for network management on TCP/IP networks.

Computers and other network devices can be configured with an SNMP agent. After you configure the SNMP agent, the management variables can be accessed and set from a central SNMP Network Management Station.

Figure 7 shows a model for network management. The network consists of several devices that have a management agent running in them. Some of the device parameters are specific to the device that is managed. For instance, router devices will have parameters that describe the routing table. All devices can be expected to have some common parameters such as the name of device, how long the device has been active (up time), and so on. The agents can be managed by a special device called the Network Management Station (NMS).

The NMS can issue specific requests to a device for information about its network parameters. The agent for the device will receive these requests, and send back the requested information. The NMS, upon receiving the reply, knows the value of the requested parameters. It can use this information to deduce information on the state of the device and whether the device requires attention.

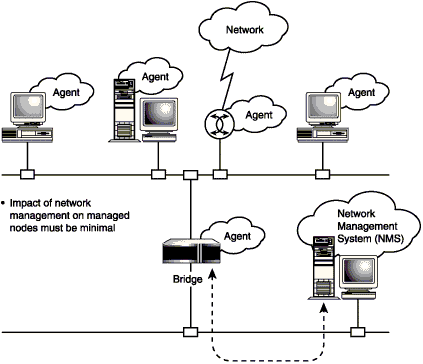


Figure 7 SNMP

**RMON**

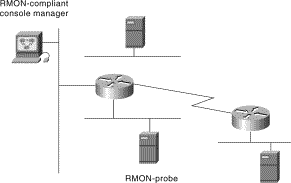
****

Figure 8 RMON

Remote Monitoring is used by remote monitoring agents to analyze network performance. RMON is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. RMON provides comprehensive network-fault diagnosis, planning, and performance-tuning information. Figure 8 illustrates an RMON probe capable of monitoring an Ethernet segment and transmitting statistical information back to an RMON-compliant console.

**Network Monitors, Analyzers, Sniffers and Probes**

***Network Monitoring and Analysis*** tools are used by network administrators, security professionals and hackers. They are available from several vendors either as fully integrated hardware devices or software packages designed to run on notebook or desktop computers equipped with promiscuous mode LAN adapters. They are similar to the Windows Network Monitor programme, but have many more features to help you track down network problems, analyze traffic and forecast future network requirements. Fluke produce advanced portable Network analyzers such as Optview, see Figure 9.



Figure 9 Fluke Optiview

There are several different types of analyzers that can be broadly grouped into LAN and WAN analyzers. Some perform both functions. A WAN analyzer will capture data on PPP links, frame relay links, ATM links, and others. It uses special interface cards to read the frames off the WAN. Additionally, WAN analyzers are typically connected to the wide area network with a "Y" connector to facilitate capture while allowing traffic to flow normally.

LAN analyzers capture and display information from LANs, including Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI). These analyzers are connected to the LAN segment by means of a hub or a switch.

**Wireshark** (the earlier *version of Wireshark was called Ethereal)* is the popular open source package that has extensive network protocol analyzer functionality. Figure 10 shows Wireshark's decode screen - also see Appendix1 for more on Wireshark.

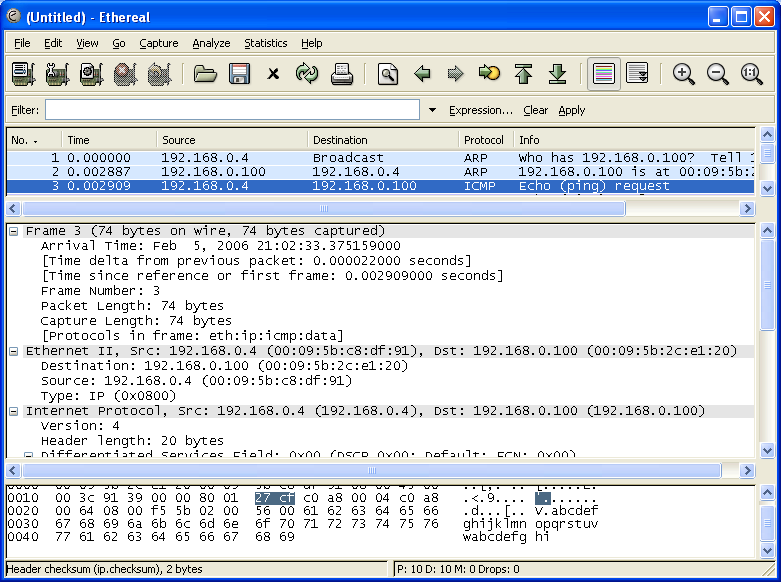


Figure 10 Wireshark Decodes screen

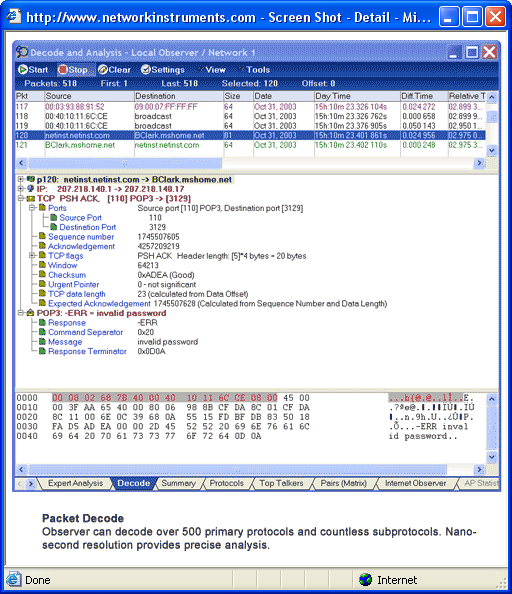


Figure 11 Observer Packet capture/decode and protocol analysis

Network Instruments *Observer* (see Figure 11) and Network Associates *Sniffer* are two popular commercial software based LAN analyzers that have a full range of monitoring and diagnostic features.

Features include data capture, traffic generation, protocol analysis, network utilization baseline testing and trending (to monitor on going traffic patterns). Analyzers let you filter traffic based on host or destination addresses, so they can capture the traffic that one conversation between two machines generates or filter by protocol type.

Some of the more advanced systems also include (‘What If analysis’) expert systems to help with capacity planning. Finally, it is common for analyzers to be able to read and display the formats of other analyzer products.

N.B*. Traffic Generators are a feature of most analyzer packages. They allow you to do active network measurements by creating packets of suitable length for various protocols to inject onto the network in order to analyze performance under different loads. See Observer quickstart guide for more details about Observer.*

***Network probes*** make use of RMON to analyze network traffic at the network and application layers. They provide much of the same detailed network information that analyzers generate, but they can't provide single-packet analysis. Probes are best at monitoring a network's health over time.

Probes are available which run as a service on other network PCs to allow data to be gathered from remote network segments by Network analyzers such as Observer.

**Basic LAN Protocol Analyzer Operation**

The operation of a protocol analyzer is quite simple as shown in Figure 11.

It receives a copy of each packet by operating in promiscuous mode that captures all packets at the interface, not just broadcasts or packets addressed to the analyzer adaptor.



Figure 11 Basic Protocol Analyzer Operation

The packets may then be filtered (optional) and time stamped before being stored in the packet capture buffer. You can then post filter out the stuff you are not interested in before the results are displayed in a format showing the breakdown of each packet to describe each part of the header information in detail. The packets can then be saved and retrieved for further analysis.

Two types of protocol analyser:

Stand-alone: single console tool used to capture/analyse local segment/subnet

Distributed: central console + remote probes to send data back across segment/subnet boundaries

**Wireless Network Monitoring and Measurement Tools**

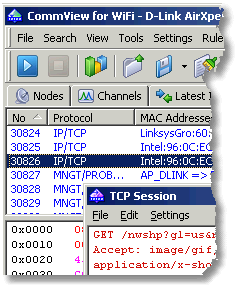
Wireshark and Observer can be used to capture and analyze IEEE 802.11 wireless network traffic when using a computer with suitable wireless LAN adapter that can operate in monitor mode. Several vendors also offer more specialist WLAN tools such as Airopeek (now called OmniPeek) and Airmagnet or the lower cost CommView for [](http://www.tamos.com/products/commwifi/)WiFi shown in Figure 12.



Figure 12 Airmagnet CommView for WiFi

There are also many LINUX security distributions such as BackTrack3 or Kali Linux which include a host of tools for monitoring and analyzing wireless networks.

Other tools such as NetStumbler shown in Figure 13 are employed to detect, enumerate and measure WLAN networks and used by administrators for site survey and security audit or hackers for Wardriving.

Spectrum analysers are invaluable for detecting and analyzing RF signals noise and interference. WiSpy for instance shown in Figure 14 is a low cost 2.4GHz spectrum analyzer in the form of a USB adapter and software.

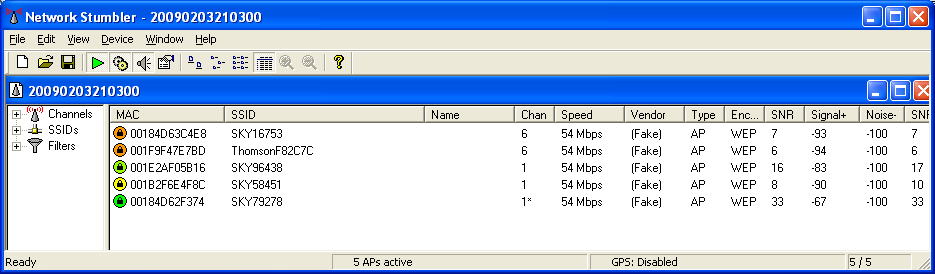


Figure 13 Netstumbler

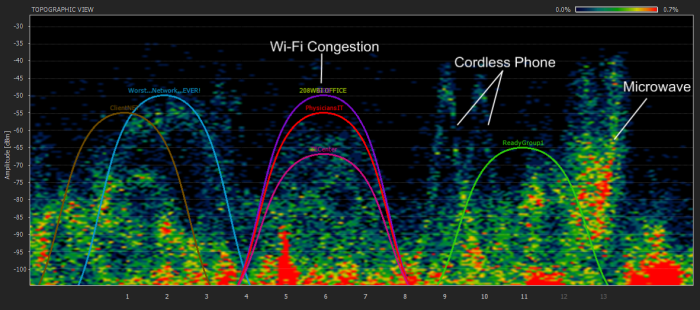


Figure 14 WiSpy

**Management Suites**

Intel LANdesk and HP OpenView are very sophisticated Network management packages designed to help administer large networks. They can be used to automate the mundane tasks of network management such as hardware and software inventory and licence metering SNMP and RMON are used to gather statistics about network operation. Built in network monitor/analyzer and probe capability allow network traffic to be monitored remotely from a central management console to assist with network maintenance.

**Real Time Quality Measurement tools**

Quality of Service (QoS) measurements is essential in measuring the real time performance of networks. Observer, Wireshark and some of the other network analysers now have expert analysis features that can measure the metrics from which QoS assessments can be made. Observer VoIP Expert for instance shown in Figure 15 will decode RTP traffic and format the results for latency, jitter and packet loss to provide graphical information and overall MOS scores or R-Factor.



Figure 15 Observer VoIP expert

**Simulators, Emulators and Network Modelling**

On small networks, you can use network monitoring to diagnose problems or predict the network's reaction to new hardware or software. However, as networks grow, their numerous devices and connections make understanding the network impossible. Too many conversations among too many devices via too many network routes occur simultaneously for you to accurately predict how one application's traffic will affect another part of the network. To diagnose problems or test new applications on a complex network, you need to simulate the network-- use a simulation program, or simulator, to build a software model of key network elements and test how well the model functions with various traffic loads or network designs.

To simulate your production network, you need to construct a reasonable representation of the network's topology, including the physical devices and logical parameters that comprise the network. You need to determine how much traffic is on your network during the period you want to emulate. You must specify a question you want the simulation to answer. And finally, you need to run the model through a simulator.

*Comnet* and *OPNET* (see Figure 16)are two commercial packages, which allow networks to be simulated either to assist with the research and design of new networks or to model an existing network and help predict the effect of changes on network performance (change simulation or What if Analysis).

Open source simulator programmes such as NS2/NS3 and OMNeT++ are also available.

NISTNET is an emulator programme that is useful for internetwork testing. It turns a Linux computer into a router with variable performance metrics. Jitter, latency, bandwidth and packet loss can be altered to test the effects on performance.

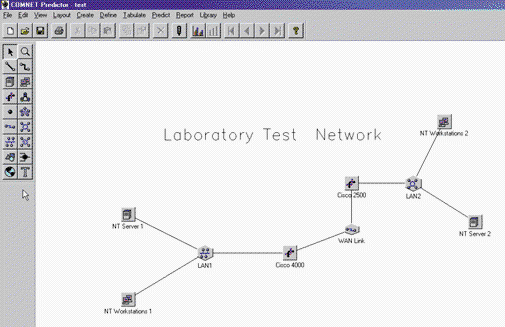
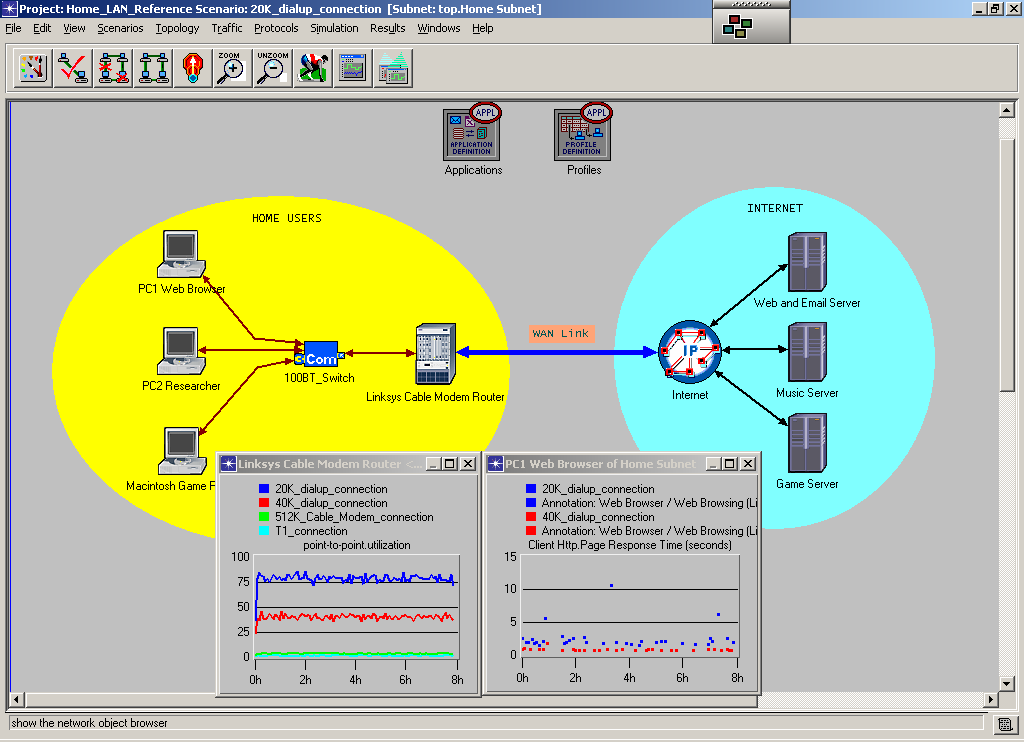


Figure 16 OPNET and COMNET simulators

**Appendix 1 Using Wireshark**

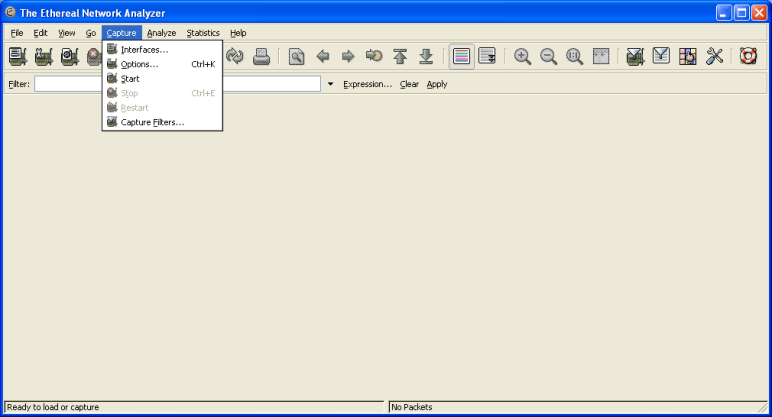
Wireshark is a GUI network protocol analyzer and TShark is the command line version. It can examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark can assemble all the packets in a TCP conversation and show you the ASCII (or EBCDIC, or hex) data in that conversation. Display filters in Wireshark are very powerful; more fields are filterable in Wireshark than in other protocol analyzers. Data can be captured from a live network connection or read from a capture file.

* Wireshark can read capture files from tcpdump (libpcap), Network Instruments Observer, NAI's Sniffer™ and Sniffer™ Pro (compressed and uncompressed), Sun snoop and atmsnoop, AIX's iptrace, Microsoft's Network Monitor, Novell's LANalyzer, Cisco Secure IDS iplog etc.
* Live data can be read from Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, Classical IP over ATM.
* Output can be saved or printed as plain text or PostScript®.

**Using Wireshark to analyze Ping Packets**

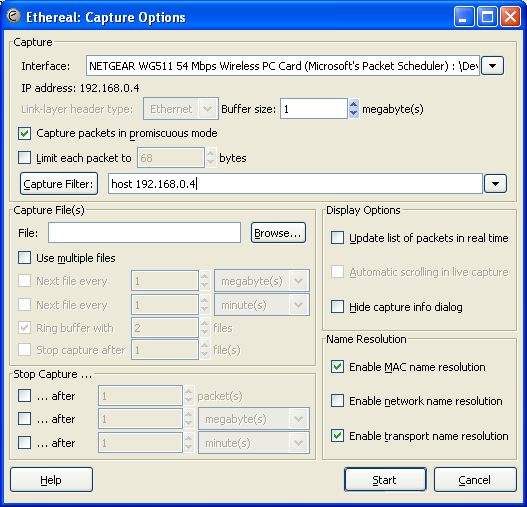
Like most other analyzers, there are three windows that display summary, detail, and hexadecimal data after the information has been captured or has been read from a previously captured file. Various preferences and display options can be set according to requirements. For example you could select the interface to capture on and just accept all the standard defaults and capture a file or you could apply a pre filter to restrict which packets are captured. If you issue a Ping command to an IP address (because a name is not being entered as the target no name resolution or a DNS lookup does not have to be performed). The two nodes that are involved in the ping operation are on the same LAN segment; therefore, the only other protocol that may come into play is ARP.If the node that issues the Ping command does not have the MAC address of the target node in its ARP cache, an ARP will first be broadcast to determine the target's hardware address. Remember, a Ping command is actually an Internet Control Message Protocol (ICMP) Echo Request and is followed by an ICMP Echo Reply.

To start a capture, we select **Capture** in the pull-down menu and choose**Start** as shown on the Start Capture Screen diagram.



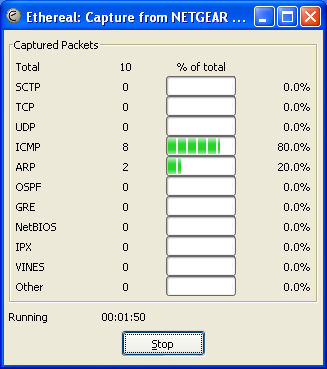
Start Capture Screen

Additional parameters, such as a capture filter can also be set e.g. to restrict capture to a particular interface 192.168.0.4 as in Capture Filter Screen diagram.



Capture Filter Screen

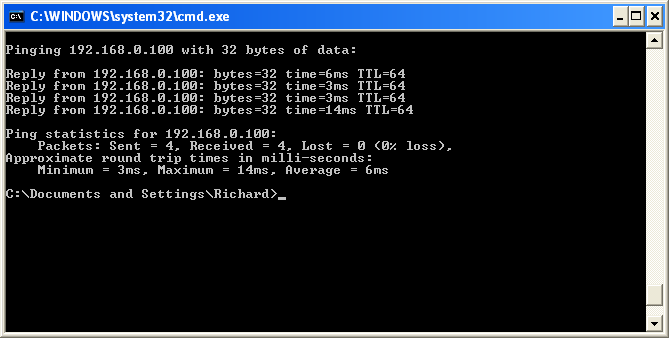
After the user chooses **Start,** another smaller window pops up showing statistics on some common protocols or you can update the display in real time.



Protocol Screen

The **STOP** button will stop the capture.

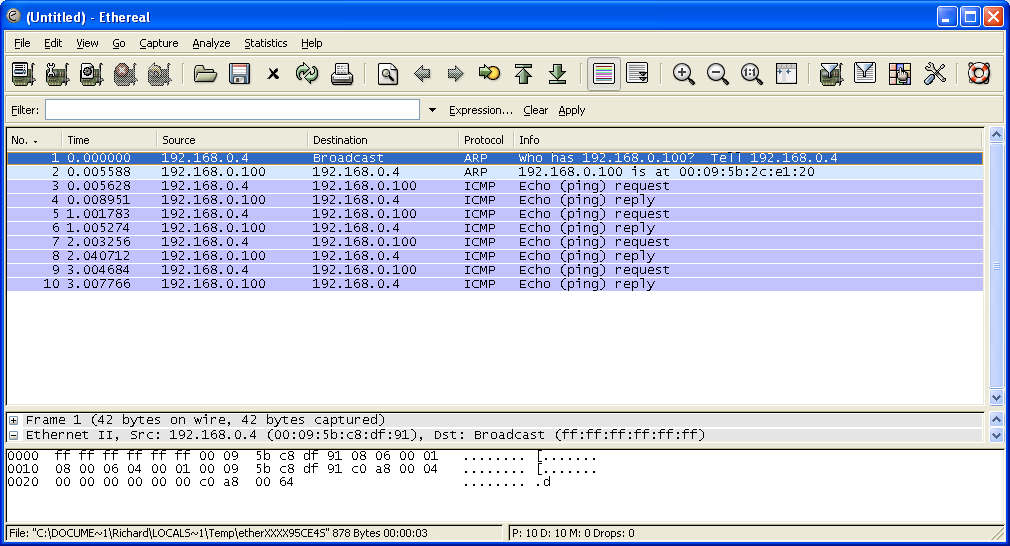
The analyzer will begin to capture traffic. Remember because we set a capture filter only traffic on the 192.168.0.4 interface will be captured even though the analyzer sees all the traffic when operating in promiscuous mode. The node that is issuing the Ping command is at IP address 192.168.0.4, and the target node's address is 192.168.0.100. The response to the Ping command is shown on the Command Prompt Screen diagram.



Command Prompt Screen

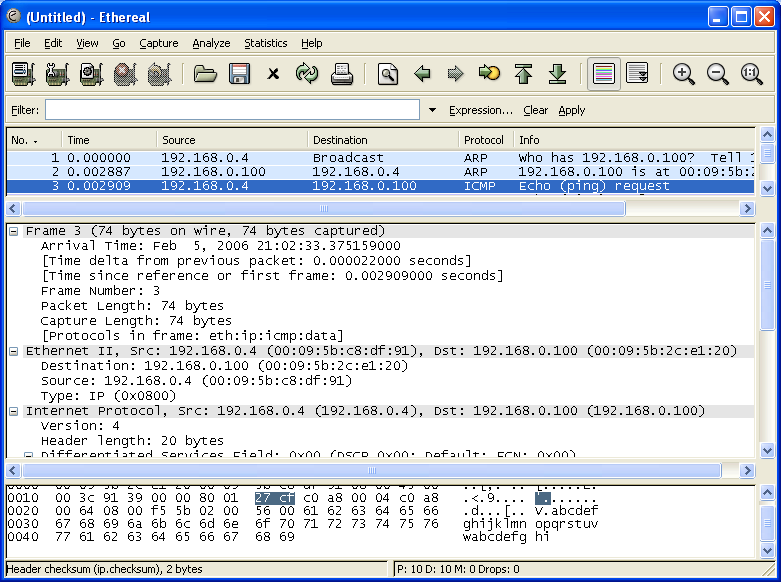
After the trace has been captured, the **Stop** button will stop the trace, and a small window will pop up indicating the trace is being processed (loading). This loading window may remain on the screen for quite some time (well over a minute) on longer traces, so be patient. When the trace has been processed, the information illustrated on the Captured Ping Trace Screen diagram is displayed.

The summary window shows 10 frames were captured consisting of an ARP request and response to determine the MAC address of 192.168.0.100 and the request/reply pairs of a Ping command issued from address 192.168.0.4.



Captured Ping Trace Screen

The Detail window shows headings for Frame 1, Ethernet II, and Address Resolution Protocol (broadcast) etc. Each one has a plus sign (+) next to it indicating there is additional information to display when the entries are expanded. To expand an entry, click on the **+** sign. Another way to expand everything is to go up to the Display pull-down menu and select **Expand All**. When this is done, all levels (protocols) will be shown. After choosing the **Expand All** option, a window will be displayed like the one on the Show All Trees Screen Diagram.



Show All Trees Screen

The Detail window may be scrolled to observe all the protocols. Notice there is a vertical scroll bar in all three windows indicating additional information. In addition, windows can be resized by placing the cursor on the dividing bar between the windows and dragging it up or down. If you don't see the bar moving as you drag it, don't be dismayed, just drag it to the desired position and you will see the result when you release.

##### Display Filters: To display certain information to the exclusion of other information, a display filter can easily be set. You can set a filter from a file that you have already saved or you can enter a filter parameter directly into the Filter window at the bottom of the screen. The information concerning display filter syntax can be found in the Wireshark manual page (man page) which is accessible from the home page of http://www.Wireshark.org. Fields can be compared against values. The comparison operators can be expressed either through C-language type symbols (!=), or short abbreviations (ne):

= =, eq Equal

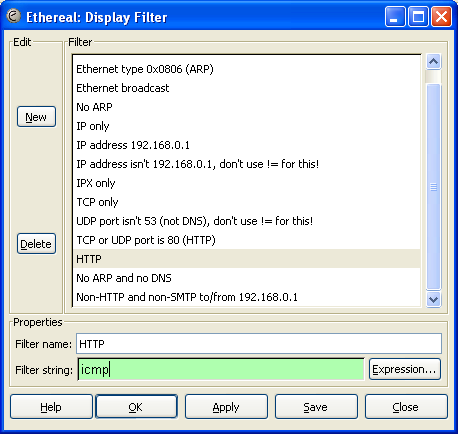
!= , ne Not equal

>, gt Greater than

<, lt Less Than

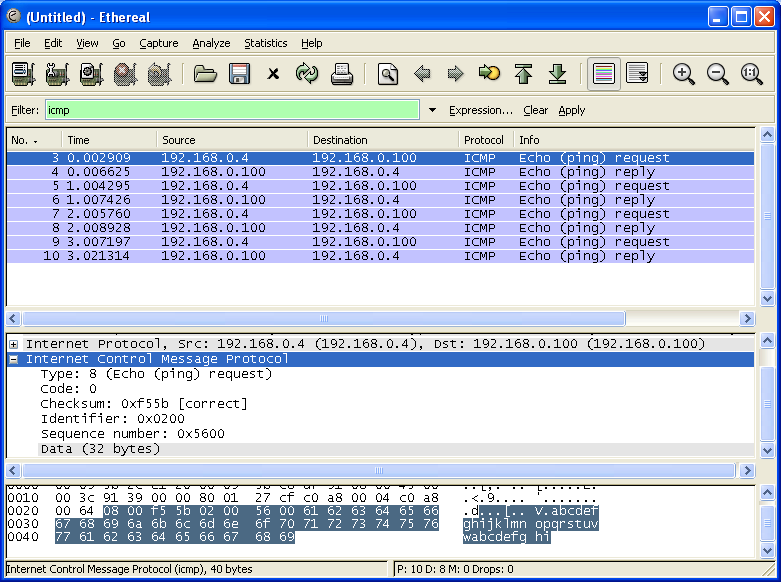
>=, ge Greater than or Equal to

<=, le Less than or Equal to



Edit/Apply Display Filter Screen

The names of the individual fields in each protocol can be found in the Wireshark main page. There is another (simpler) way of discovering a field name. Suppose we want to display all the captured records that are ICMP messages. If you go to the Detail window and highlight the ICMP field in the IP header you will see a screen that looks like this:



ICMP Display Filter Screen

Notice the Protocol field highlighted and the name of the field. If we enter this IP field name in the filter window at the lower left of the screen, only ICMP protocol packets will be displayed. This is illustrated on the ICMP Display Filter Screen Diagram. Observe that the ARP records (1 and 2) are no longer displayed, but all records (3 through 10) containing the ICMP protocol identifier in the IP header Protocol fields are displayed.

N.B. *Download the latest version of Wireshark for free from* *http://www.wireshark.org and install it on your home PC if you have one. Then you can have a go at the Exercises. Documentation is also available 'on line' or for download as a PDF file and/or read Ch4 and Ch5 of the ‘Wireshark and Ethereal Network Analyser Toolkit’ book.*

**Exercises**

**Exercise 1 Wireshark Filters**

You can learn a lot about network protocols by decoding and analysing packet captures. You must first, however, learn to filter out the traffic that you are not interested in. Create filters that will only show the packets indicated in both capture and display formats:

1. Ethernet broadcasts destination
2. Source MAC address 00-40-96-AD-28-6E
3. IP address 192.168.1.1
4. IP source address 192.168.1.1 and IP destination address 192.168.2.2
5. Web traffic using TCP port 80
6. Ping echo response packets

**Exercise 2 A simple Wireshark Flow Graph**

Download the **ICMPtest.cap** file from your Blackboard site and open it in Wireshark.

Filter for ICMP packets then format the results to show the packet interchange using the Flowgraph feature found under the Statistics tab of Wireshark.

**Exercise 3 Analyse TCP flow to determine Telnet passwords**

1. Download the **telnet.cap** file from your Blackboard site and open it in Wireshark.
2. Filter for Telnet packets then format the results to show the packet interchange using the Follow TCP feature found under the Analysis tab of Wireshark.
3. Notice the echoplexing used by the Telnet protocol and locate the password

**Exercise 4 Analyse a VoIP voice conversation with Wireshark**

Download the **VoIPtest.cap** file from your Blackboard site and open it in Wireshark.

Filter for SIP and display the Flowgraph

Use the VoIP Calls analysis tool found under the statistics tab to:

1. Display the Flowgraph of the overall voice call
2. Replay the conversation in each direction using the player facility.

**Exercise 5 Observer network analyzer**

1. Download the latest version (17) and use it in demo mode to investigate the operation and features it offers.
2. Compare the protocol analyser features of Observer and Wireshark