



User's Guide_{v2.4}

COPYRIGHT

Information in this document is subject to change without notice and does not represent a commitment on the part of eEye Digital Security. The software described in this document is subject to the license agreement that is included with Retina, in whole or in part, in print, or in any other storage and retrieval system is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means for any purpose other the purchaser's personal use without express written permission of eEye Digital Security.

Iris™ is a trademark of eEye Digital Security.

Microsoft Excel is a registered trademark of Microsoft Corporation.

Windows NT is a registered trademark of Microsoft Corporation

Windows 2000 is a registered trademark of Microsoft Corporation

Copyright © 1998-2001 eEye Digital Security, All rights reserved.

Table of Contents



Introducing Iris	1
Monitoring Network Activity.....	1
Decoding and Reconstructing Captured Data	1
Session reassembly	1
Detecting Connection Attempts.....	1
Configuring Capture Sessions Through the Use of Filters.....	2
Logging Activity	2
Displaying Network Statistics	3
Post-processing capture data	3
Installing Iris	5
System Requirements.....	5
Planning Your Installation.....	5
Installing Iris	6
Uninstalling Iris	7
Starting Iris	7
Terminating the license	7
Using Iris to Monitor Network Activity	8
Starting Iris	8
Configuring Iris	9
Using schedules	14
Optimizing Iris.....	15
Using the Packet Interface	15
Using Iris to Troubleshoot Your Network	21
Using Iris to search traffic for words.....	22
Decoding and Reconstructing Captured Data	23
Decoding and Reconstructing Captured Data	23
Setting Decode Options	24

The Decode Menu	25
Viewing Host Activity.....	25
Viewing Sessions.....	26
Viewing Session Data.....	27
Detecting Connection Attempts.....	29
Guard Settings	29
Guard Alerting.....	31
Creating Filters	32
Using the Address Book in Filters.....	32
Hardware Filter	32
Layer 2,3 Filter	34
Words Filter.....	36
MAC Address Filter.....	38
IP Address Filter	39
Ports Filter.....	40
Advanced Filter	42
Logging Activity	43
Enable Capture Logging	43
Enable Decode Logging	45
Enable Guard Logging.....	46
Importing Iris Log Files to a Spreadsheet.....	47
Displaying Network Statistics	48
Configuring Graphs.....	48
Displaying the Protocol Distribution Graph.....	49
Displaying the Top Hosts Graph.....	51
Displaying the Size Distribution Graph	53
Displaying the Bandwidth Graph	55
Creating Traffic Reports.....	58
Using Command Line Arguments	60
Appendix A-Frequently Asked Questions	61

Appendix B – Networking Overview	63
Network basics	63
Ethernet	65
Sniffer Theory	66
Appendix C Introduction to TCP/IP	67
Introduction	67
The Four Layers of TCP/IP	67
TCP/IP Networking Protocols	69
Appendix D–Glossary	79
Index	96

Introducing Iris



Iris is a network management tool designed to help IT personnel proactively monitor their organization's network.

Monitoring Network Activity

A next-generation network protocol analyzer or “sniffer,” Iris provides a graphical user interface (GUI) to allow network administrators to capture and retrace the steps of any network user. By monitoring both incoming and outgoing network traffic, Iris functions as a complete systems management watchdog.

Decoding and Reconstructing Captured Data

In addition to the expected sniffing functions, Iris lets you reconstruct data and display all content that was captured. In decode mode, captured data is reassembled in a way that allows you to view each session as if you were the actual session owner. Many common protocols can be reconstructed in this manner.

Session reassembly

TCP is a connection-oriented protocol. This means that in a normal TCP session, such as downloading a web page, a certain sequence that must be followed to create a connection, and then to destroy that connection. TCP is also session based, meaning that once a connection is established, it remains established and can send data until it goes through a proscribed close sequence.

Traditional sniffers offer you a view of all packets representing a TCP sequence. You can look at each packet in the session in sequence and a knowledgeable administrator can determine what was happening in a TCP session.

Iris takes this one step further. A reassembled HTTP session is fed into a decoder that allows it to be displayed as a fully rendered web page. This allows Iris to not only show you the packet that created the session, but a realistic view of the actual contents of data sent within that session.

Detecting Connection Attempts

Iris's Guard feature watches for a specific connection sequence when a TCP session begins and reports it if it meets the connection criteria set in the filter. This allows you to watch specific connections to and from any machine, and be alerted if Iris sees a connection from an IP or TCP port that Iris has been configured to watch for. You can also enable sound so that you receive an audio alert when an unauthorized connection is attempted.

Configuring Capture Sessions Through the Use of Filters

You can create custom filters so that Iris only retrieves traffic you are interested in.

On an average network, there is a lot of data going across that is not relevant to anything you are looking for. Iris allows you to focus on relevant data through the use of packet filtering. Packet filtering also provides the added benefit of decreasing the amount of work Iris must do to achieve specific results.

Creating filters requires that you understand a little about the underlying protocol. We recommend you start with general filtering rules and continue to refine them until you get the exact data you are looking for.

For example, if you are only interested in seeing which web pages a specific end user is browsing, you can set a filter that only captures data for users accessing TCP port 80, the traditional HTTP/web port. This limits the traffic you sniff to web traffic (or other port 80 traffic). This is good, but you will still see all web traffic that all users on that segment generated. To see only web traffic from a single user, a secondary filter must also be applied. In this case, the secondary filter would be an IP address, since this would be unique to the specific user.

Packet filters can be simple, like the one described above, or very complex. Iris implements a wide array of packet filtering techniques, allowing you to filter on almost any part of a packet.

You can create filters based on:

- Hardware Layer
- Protocol Layer
- Key words
- MAC address
- IP address
- Source and destination port
- Custom data and size of the packets

This feature is extremely useful in a networking environment in which there is a high volume of network traffic.

Logging Activity

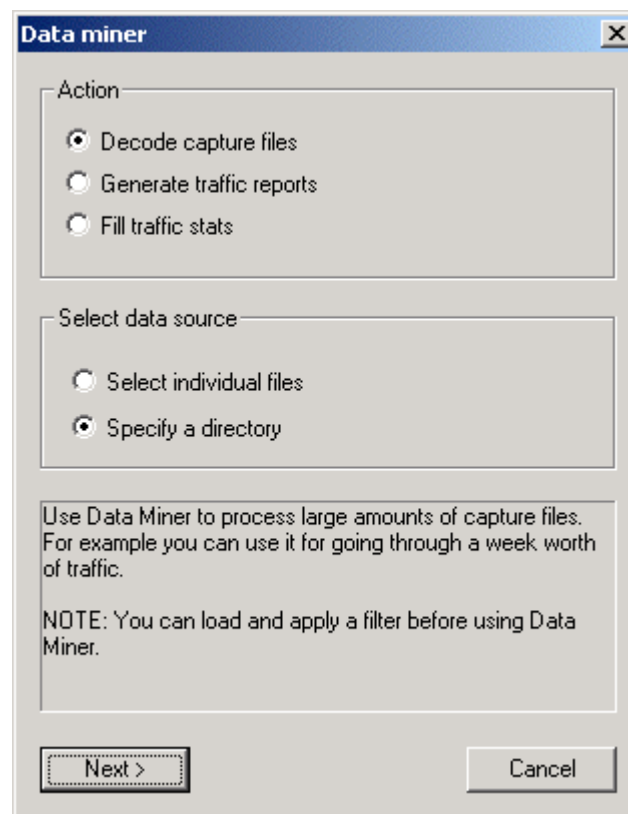
It is easy to configure logging so that only the desired content is saved. Logging options are available for both Capture and Decode Modes. This allows you to catalog and save the data Iris has retrieved off of your network in a simple and efficient manner. You can even have Iris automatically organize the data by day and month.

Displaying Network Statistics

You can display network statistics according to Protocol, Top Hosts and Size Distribution.

Post-processing capture data

Data Miner (File menu -> Data Miner) has been designed for post processing a large number of capture files created by Iris or any other sniffer.



Action

Decode capture files

When this Action is selected, Iris will reconstruct all TCP sessions contained in processed files. Packets will not be loaded in memory, therefore Iris will be able to decode a big amount of captured traffic. Before using this feature, be sure you have enough free space on the partition where Iris is installed. Iris will require the same amount of free space as the one occupied by the capture files being processed.

Generate traffic reports

When this Action is selected, Iris will process all selected files without loading the packets and without reconstructing the sessions. In this case Iris will not require free space as it will not create temporary files. However, with this option you can create only traffic reports.

Fill traffic stats

Use this option to extract statistical traffic information from a large number of capture files. Upon completion, Size Distribution, Protocol Distribution and Top N hosts statistics will be displayed. Packets will not be loaded, sessions will not be reconstructed and traffic reports can be generated using this option.

Select data source

Select individual files

After clicking Next>, select the files (using Ctrl key) which to be processed.

Specify a directory

After clicking Next>, select the folder which to be processed and specify if to be processed recursively or not.

Installing Iris



Before installing Iris, be sure you have at least the minimum system requirements and have read the section on “Planning Your Installation.”

System Requirements

System Requirements:

- Windows 95/98/NT/2000
- Internet Explorer 4.x AND comctl32.dll version 5.00 or higher.
OR
Internet Explorer 5.x.
- **Minimum system**
Pentium 166, 32MB RAM, 1GB HDD
- **Recommended**
Pentium 400, 128MB, 10 GB HDD

Additional Recommendations:

Latest service packs and patches for Operating System, Internet Explorer, NDIS compliant drivers and supported Ethernet cards.

Planning Your Installation

“Sniffing” entails putting the node’s Ethernet card into promiscuous mode so that it can see all packets destined for all nodes on the segment. By understanding your network configuration, you can install Iris for optimal performance.

COMCTL32.DLL

Iris requires comctl32.dll version 5.00 or higher to be installed on your system. It is usually installed by Microsoft Internet Explorer 5.0 or higher, but can be installed separately from an update package available from: <ftp://ftp.microsoft.com/developr/platformsdk/april2000/x86/redist/comctl32/50comupd.exe>.

Where to Install Iris on Your Network

Some general rules to consider before you install Iris:

- **Install Iris at the Edge:** The closer you can install Iris to the edge of your network, the more information it will be able to see. For example, many networks have routers on their edge, connected directly to a switch that provides internal network connectivity. In this case, since the router is the edge, a good place to install Iris is between the router and the switch.

- **Switches break sniffers:** Switches create multiple segments. Iris can only view traffic on the segment it is installed on. If you use switches directly to end users, those end users are immune to “sniffing”. There are some switches, however, that have special ports that do receive all traffic destined for all ports. This is typically called a shunt or management port. Switches with this feature will allow you to use this port to sniff all (or some) ports on the switch.
- **Firewalls and Iris:** A firewall acts as an active security gateway on your network by disallowing certain types of network traffic. Like a router, a firewall is often at the edge of your network. Iris can be used to make certain that your firewalls are acting, as they should. Placing Iris both in front and behind a firewall will provide you with the ability to view traffic on either side of your protected gateway.
- **Hubs are Iris friendly:** Hubs allow Iris to see traffic on all nodes serviced by the hub. Having a small multi-port hub (3 ports should suffice) can even make sniffing in a switched environment practical. With a 3-port hub, you can install Iris at any point along your network, allowing you greater access. One port on the hub is for the sniffer, and the other two are for connecting to the switch and end user.

Installing Iris

Installing from the CD-ROM

1. Insert the CD-ROM and follow the instructions on the screen.
2. If Auto Play is disabled on your CD-ROM drive, you will need to navigate to the CD-ROM drive through Windows Explorer or My Computer and double-click on the Iris200.exe file.

Installing from the Run Dialog

From Windows,

1. Click Start > Run.
2. Type **X:\iris.exe** where X:\ is the letter designation of your CD ROM drive.
3. Follow the on-screen instructions.

Uninstalling Iris

From Windows,

1. Click **Start > Settings > Control Panel**.
2. Click **Add/Remove Programs**.
3. Follow the on-screen instructions to remove Iris from your system.

Starting Iris

From Windows,

1. Click **Start > Program Files > Iris > Iris**.

Terminating the license

(Note: This feature does not exist in the Evaluation Version)

Generally licenses terminate automatically if they have been issued only for a period of time, however there may be instances where it is necessary to terminate a license manually.

When you should terminate the license:

1. If you upgrade the computer on which Iris is installed on.
2. If you plan to use Iris on another computer. Because Iris is bound to the system where it has been licensed, if you want to move it to another system you **MUST** terminate the license from the first computer.

For example, you may wish to change a hardware component. In such cases you must request the eEye Digital Security to generate a new License Key for your software but before doing this, the publisher must verify that the original license has been terminated. This can be accomplished by providing the termination code to eEye Digital Security.

Procedure for Terminating a License

- Click the Help menu and select License Management... menu.
- Select Terminate License option, click Next and then confirm the action.
- When you have confirmed that the product should be terminated, the Termination Code is displayed. Make a note of this so that it can be verified by the eEye Digital Security. The code is also saved in a file (termination.txt) file in Iris's installation folder.
- When the product is re-installed, it will display a different reference code. Email at sales@eeye.com the termination code, the reason for termination and the new reference code.
- eEye Digital Security will issue a new License Key.

Using Iris to Monitor Network Activity



Starting Iris

Iris's default settings have been carefully chosen for efficient and simple usage. Every time you install Iris you will start with the default settings.

From Windows,

Click Start > Program Files > Iris.

Click Capture > Start (shortcut Ctrl-A).

You will immediately see the packets flowing in the Capture view.

1. Click Start Capture

2. Packets will appear here

3. Click Decode Buffer

No.	MAC s...	MAC d...	Frame	Protocol	Addr. IP src
39	00:06...	00:06:...	IP	TCP-> NETBIOS-SSN	192.168.1.
40	00:06...	00:06:...	IP	TCP-> NETBIOS-SSN	192.168.1.
41	00:06...	00:06:...	IP	TCP-> NETBIOS-SSN	192.168.1.
				TCP-> NETBIOS-SSN	192.168.1.
				TCP-> NETBIOS-SSN	192.168.1.
44	00:06...	00:06:...	IP	TCP-> NETBIOS-SSN	192.168.1.

0000 FF FF FF FF FF FF 08 00 46 07 F5
0010 00 4E 65 C8 00 00 80 11 50 69 CC
0020 01 FF 00 89 00 89 00 3A 24 2D F4
0030 00 00 00 00 00 00 20 45 50 45 47
0040 44 45 46 43 41 43 41 43 41 43 41
0050 41 43 41 43 41 43 41 43 41 43 41

In this window it will be decoded the content of packet edit
see its position in packet editor window.

CPU: 0% 44/100 IP: 192.168.1.9 MAC: 00:06:

Configuring Iris

There are a variety of settings you can configure to make sure Iris is capturing exactly the data you want.

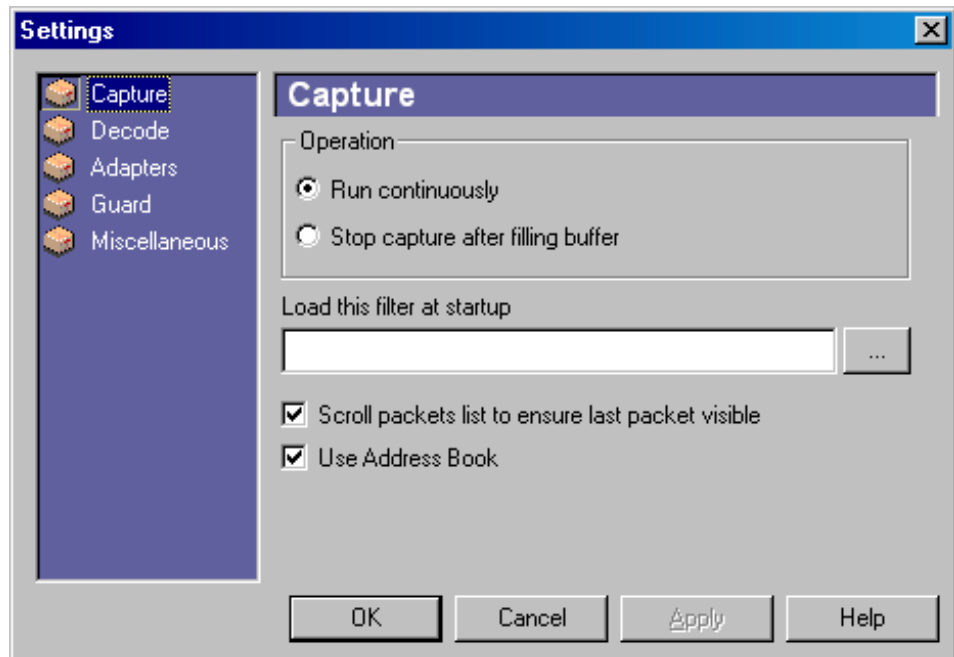
To open the Settings Window,

Click Tools > Settings.

Select the module you want to configure.

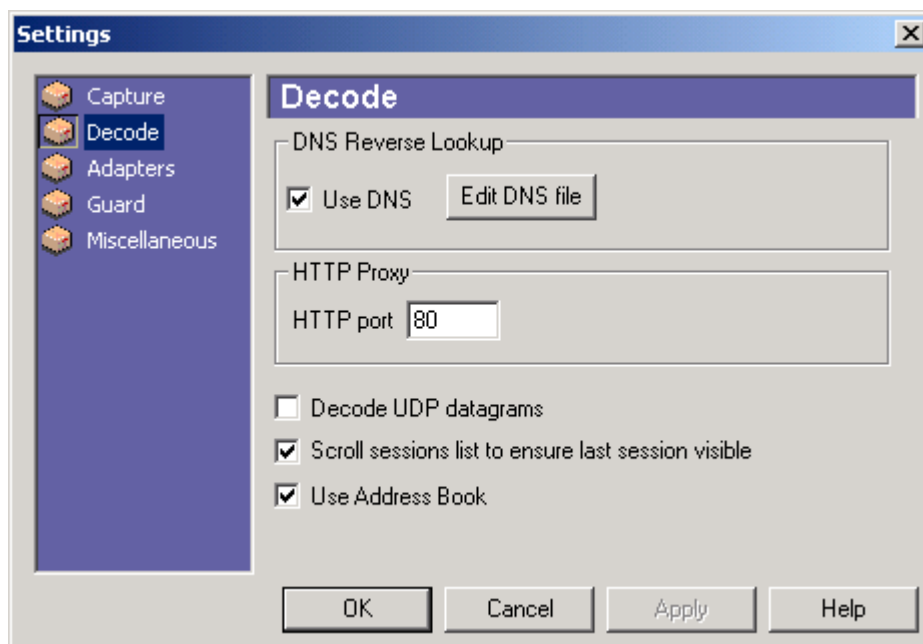
When you have completed your changes, click OK.

Capture



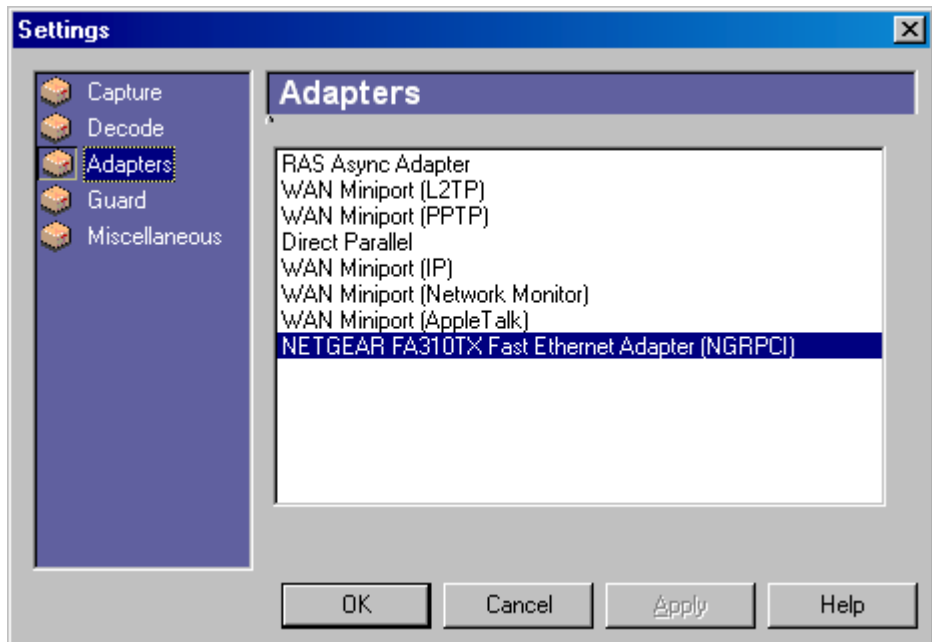
Option	Description
Run continuously	When the buffer is full, Iris will overwrite older packets from buffer.
Stop capture after filling buffer	Iris fills one buffer and then stops capturing packets.
Load this filter at startup	Select the filter that should be loaded and applied by default. Also see Command Line Arguments.
Scroll packets list to ensure last packet visible	Iris will scroll the packets list when a new packet is inserted. This ensures that the most recent data is shown in the packet capture window.
Use Address Book	Iris will use information stored in Address Book. MAC addresses will be replaced with MAC aliases, and IP addresses with corresponding host names.

Decode



Option	Description
Use DNS	Lets you look-up hosts in the Decode View. This provides resolved names (if they are available), making it easier to view the hosts you are dealing with.
Edit DNS file	Iris caches in this file DNS names of local hosts. Use this option to modify the content of the DNS cache file. Once the file is saved back to disk, the modifications will be made available to IRIS.
HTTP proxy	Enter the proxy port value. Use this option in case HTTP traffic is not using the default port (80). This value will be used to recognize HTTP sessions.
Decode UDP Datagrams	Indicate if you want Iris to show the content of UDP datagrams in Decode Mode.
Scroll sessions list to ensure last session visible	Iris will scroll the Sessions list. This ensures that the most recent data is shown in the packet capture window.
Use Address Book	Iris will use information stored in Address Book. MAC addresses will be replaced with MAC aliases, and IP addresses with corresponding host names.

Adapters



Lists all installed adapters. See “*Installing Iris*” for more information about supported Ethernet cards.

To change an adapter,

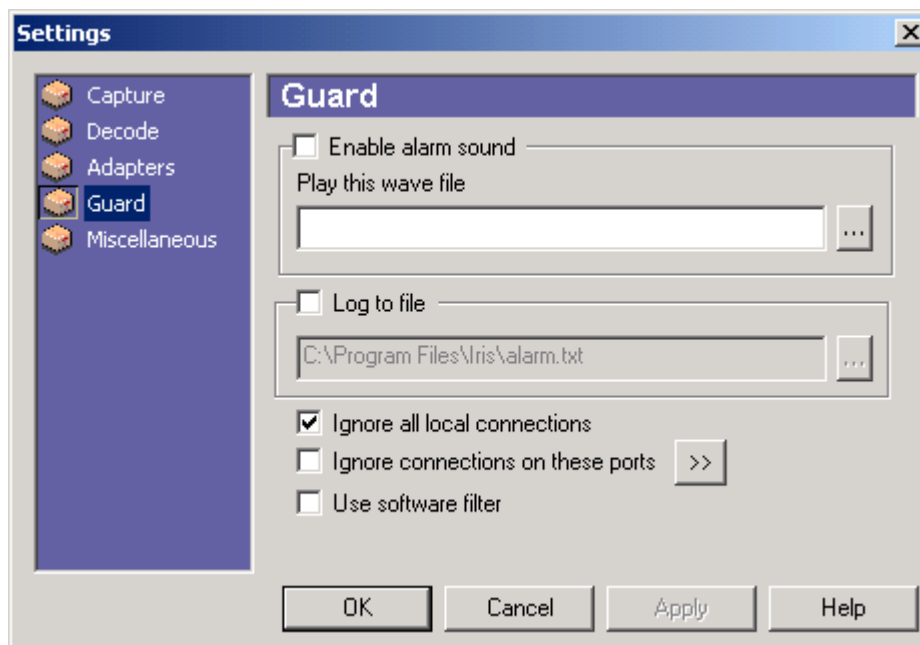
Click the adapter.

Click OK (you don’t need to click Apply).

Adapters can be changed even while capturing.

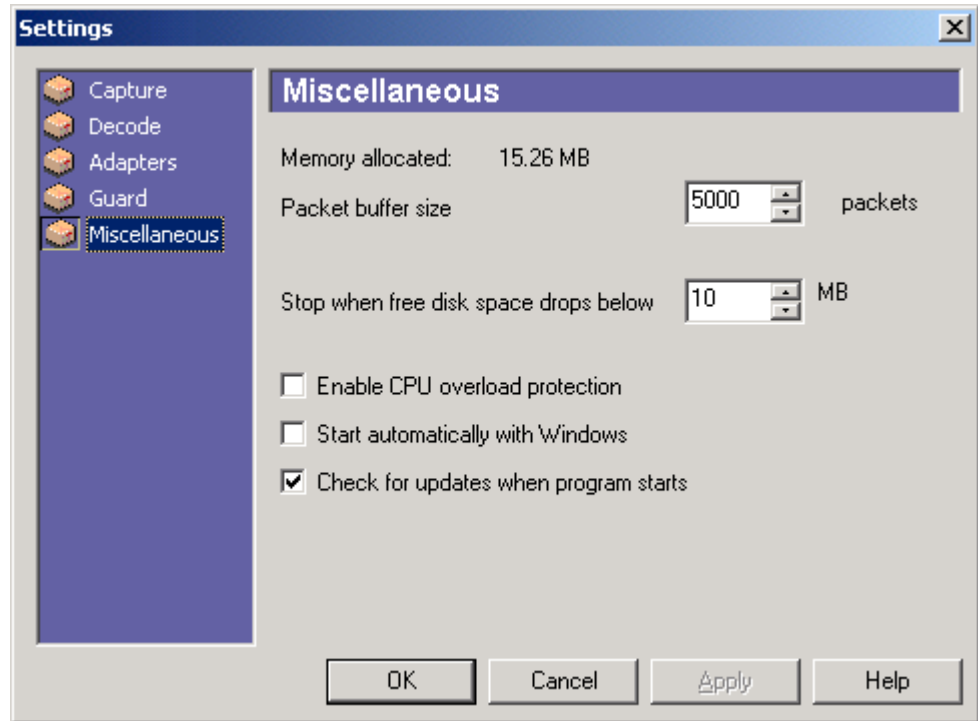
Note: RAS adapters are not supported under Windows 2000/NT/XP. They are supported on Windows 9x/Me.

Guard



Option	Description
Enable alarm sound	Iris will play an audio alarm when a connection attempt is detected.
Play this wave file	Audio file that will be played instead of the default sound.
Log to file	File where connection attempts will be saved.
Ignore all local connections	Iris will use current IP address and network mask to determine if an address is from the local network or if it is from an external host. If this option is checked, Iris will not take into consideration connection attempts initiated by local hosts.
Ignore connections on these ports	Iris will ignore connection attempts seen on a port from the allowed ports list.
Use software filter	If this is checked , Iris will apply filter rules to connection attempts. If this is cleared , Guard will notify all connection attempts (which are not filtered by the <i>allowed port list</i>) regardless of the applied software filter. This option allows the Guard module to function independently of the current filter. However, using the filter gives you the option to watch connection attempts only on specific hosts. In both cases, the Ignore connections on these ports option will be in effect. Note: Even if Use software filter is checked, a filter will be applied only if Apply filter to incoming packets is ON.

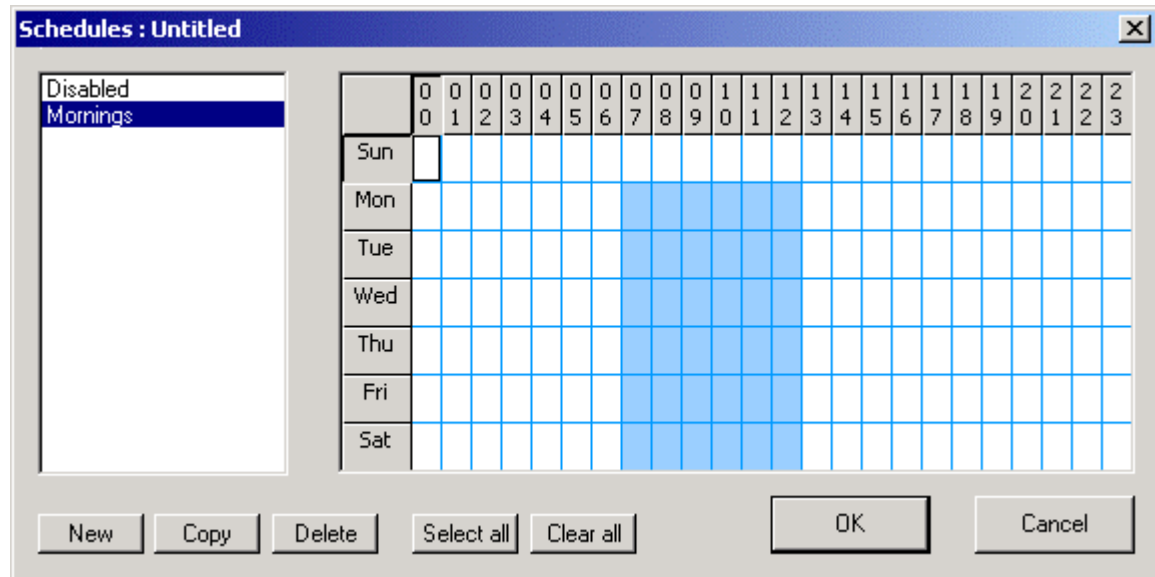
Miscellaneous



Option	Description
Packet buffer size	Number of packets that the internal buffer can hold.
Stop when free disk space drops below	Allows you to set a break-off point for packet logging. Iris will stop logging packets when disk space gets very low. This stops a denial of service (DoS) attack aimed to fill the hard disk of the system that Iris is running on. Note: If Decode module is enabled, Iris will also create temporary files using disk space from the partition where it is installed. These temporary files are deleted when New Capturing Session is selected or when Iris exits.
Enable CPU overload protection	Iris will not display packets when the CPU usage is at 100% for more than 4 seconds. As soon as CPU usage is less than 100%, Iris will start displaying packets again. For advanced users: To customize "CPU Overload Protection" add the following entries to the registry and modify their values: [HKEY_CURRENT_USER\SOFTWARE\Eye Digital Security\Iris\CPU_Usage] "CPU_load_threshold"=dword:00000064 "Seconds_load_threshold"=dword:00000004 Description: CPU_load_threshold means the CPU usage percentage from which Iris starts counting seconds Seconds_load_threshold is the number of overload

	seconds after which Iris starts reducing its processing.
Start automatically with Windows	Starts Iris automatically when Windows starts, allowing a packet-log to occur as soon as possible.
Check for updates when program starts	If checked, Iris will check if a new version is available and will display What's new in the latest version. System has to be connected to Internet for Update to work..

Using schedules



Using Schedules, you can configure Iris to capture packets only in certain timeframes.

Blue means CAPTURE, white means DO NOT CAPTURE.

In the image above, *Mornings* schedule will make Iris capture from 7 am to 1 pm every day except Sunday.

When Iris is managed by a schedule, the caption bar in Capture mode will indicate the name of the running schedule:



Note: Bandwidth Chart will be updated even if Iris capturing is stopped by the scheduling engine.

Optimizing Iris

Through the effective use of filters, you can limit the amount of data Iris captures, resulting in the most efficient performance.

For information on setting Filters, see “*Creating Filters.*”

Using the Packet Interface

The Packet Editor displays packets in Hexadecimal and displays an ASCII representation of the packet on the right side. By clicking any portion of the Hexadecimal display, the corresponding field displays in the packet decoder window.

The Packet Hex Display Window allows you to edit, modify, and send packets. By selecting a place in the Hexadecimal view or the ASCII view of the packet and typing, you can overwrite parts of the existing packet. This new packet can then be sent, pushed into Packet Display Window or saved to disk.

The Packets window displays the capture list, the Packet Decoder window, and the Packet Editor.

The screenshot shows the Iris network monitoring software interface. The main window is titled "Capture" and contains a "Packet Decoder" window on the left and a "Packets" window on the right. The "Packet Decoder" window shows the details of a selected packet, including the TCP header and flags. The "Packets" window displays a list of captured packets with columns for No., MAC source addr, MAC dest. addr, Frame, Protocol, and Addr. IP s.

No.	MAC source addr	MAC dest. addr	Frame	Protocol	Addr. IP s
1	Alice	Bob's adapter	IP	TCP-> SMTP	smtp.dnt.r
2	Bob's adapter	Alice	IP	TCP-> SMTP	ppp-144.d
3	Alice	Bob's adapter	IP	TCP-> SMTP	smtp.dnt.r
4	Alice	Bob's adapter	IP	TCP-> SMTP	smtp.dnt.r
5	Alice	Bob's adapter	IP	TCP-> SMTP	smtp.dnt.r
6	Bob's adapter	Alice	IP	TCP-> SMTP	ppp-144.d
7	Bob's adapter	Alice	IP	TCP-> SMTP	ppp-144.d
8	Alice	Bob's adapter	IP	TCP-> SMTP	smtp.dnt.r
9	Bob's adapter	Alice	IP	UDP->DNS	ppp-144.d
10	Alice	Bob's adapter	IP	UDP->DNS	193.226.1
11	Alice	Bob's adapter	IP	TCP	209.185.1
12	Bob's adapter	Alice	IP	TCP-> POP3	ppp-144.d
13	Alice	Bob's adapter	IP	TCP	209.185.1

The "Packet Decoder" window shows the following details:

- IP Options = None
- TCP header**
- Source port = 25 SMTP
- Destination port = 1345
- Sequence number = 2471537394
- Acknowledgement number = 7360369
- Header length = 5 (20 bytes)
- Flags
 - Urgent pointer = 0
 - ACK = 1
 - Push = 1
 - Reset = 0
 - SYN = 0
 - FIN = 0
- Window = 32120
- Checksum = 0x2482 (Correct)
- Urgent pointer = 0
- TCP Options = None

The "Packets" window shows a list of captured packets with columns for No., MAC source addr, MAC dest. addr, Frame, Protocol, and Addr. IP s. The bottom of the window shows a hexadecimal display of the selected packet data.

Packet Decoder

Using a standard folder-type interface, the packet decoder shows the packet broken down into its parts. This provides a clearer display of the packet aspects.

To display the Packet Decoder,

Click **Capture** if the packet decoder view is hidden.

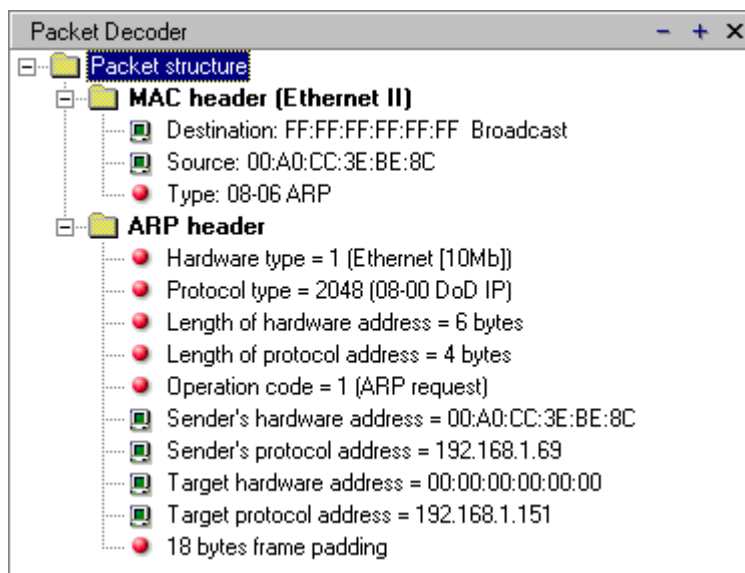
To keep the Packet Decoder view open, click the pushpin .

To hide the Packet Decoder view, click the X displayed at the top.

Each header it finds (MAC, IP, ICMP, TCP, and UDP) will be broken down, displaying each part of the packet and the data it contains.

If the Packet Hex display is open, it will correlate the selected part of the decoded packet to the actual Hex-Dump of the packet. The selected portion will be displayed in the Hex-Dump in red.

Various checksums found in IP, TCP, UDP headers are instantly computed and if they are wrong, the correct value is displayed. This makes it easier to create new packets from captured ones.



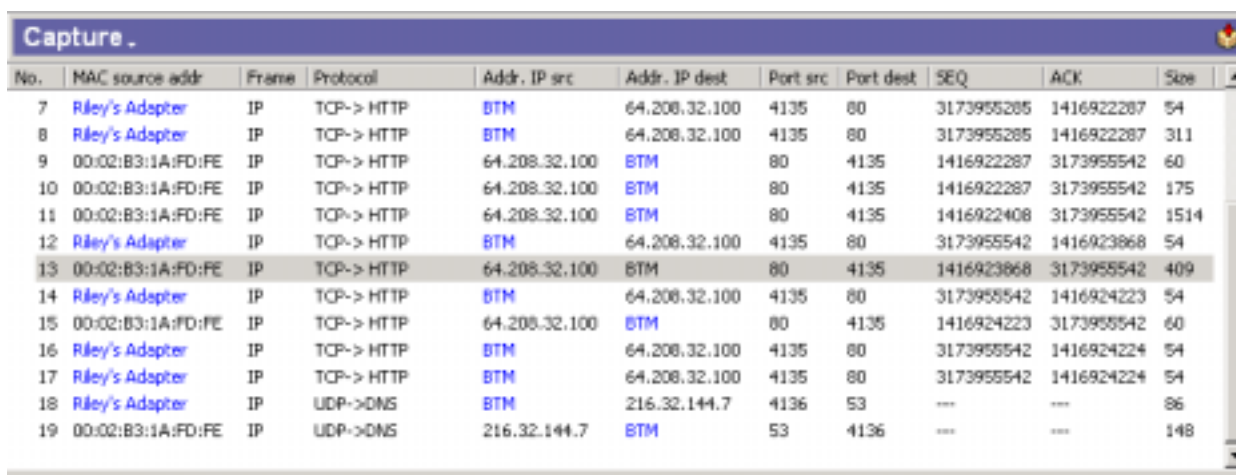
Capture Window

The top portion of the window displays packets as they arrive. You can select specific packets to be shown in the Decoder Window. It also allows you to right click a specific packet and perform certain functions on it.

To reorder packets,

Drag and drop the packet within the window.

Re-order columns by dragging column headers.



No.	MAC source addr	Frame	Protocol	Addr. IP src	Addr. IP dest	Port src	Port dest	SEQ	ACK	Size
7	Riley's Adapter	IP	TCP-> HTTP	BTM	64.208.32.100	4135	80	3173955285	1416922287	54
8	Riley's Adapter	IP	TCP-> HTTP	BTM	64.208.32.100	4135	80	3173955285	1416922287	311
9	00:02:B3:1A:FD:FE	IP	TCP-> HTTP	64.208.32.100	BTM	80	4135	1416922287	3173955542	60
10	00:02:B3:1A:FD:FE	IP	TCP-> HTTP	64.208.32.100	BTM	80	4135	1416922287	3173955542	175
11	00:02:B3:1A:FD:FE	IP	TCP-> HTTP	64.208.32.100	BTM	80	4135	1416922408	3173955542	1514
12	Riley's Adapter	IP	TCP-> HTTP	BTM	64.208.32.100	4135	80	3173955542	1416923868	54
13	00:02:B3:1A:FD:FE	IP	TCP-> HTTP	64.208.32.100	BTM	80	4135	1416923868	3173955542	409
14	Riley's Adapter	IP	TCP-> HTTP	BTM	64.208.32.100	4135	80	3173955542	1416924223	54
15	00:02:B3:1A:FD:FE	IP	TCP-> HTTP	64.208.32.100	BTM	80	4135	1416924223	3173955542	60
16	Riley's Adapter	IP	TCP-> HTTP	BTM	64.208.32.100	4135	80	3173955542	1416924224	54
17	Riley's Adapter	IP	TCP-> HTTP	BTM	64.208.32.100	4135	80	3173955542	1416924224	54
18	Riley's Adapter	IP	UDP->DNS	BTM	216.32.144.7	4136	53	---	---	86
19	00:02:B3:1A:FD:FE	IP	UDP->DNS	216.32.144.7	BTM	53	4136	---	---	148

Option	Description
Resize to fit	Automatically set the sizes of columns to extend as far as the text goes.
Ensure last visible	Iris will scroll the list when a new packet is inserted.
Columns	Customize the displayed columns.
Use Address Book	The address book replaces the 6-byte hardware address (MAC) or network address of the network node with its respective symbolic name and using the specified color.

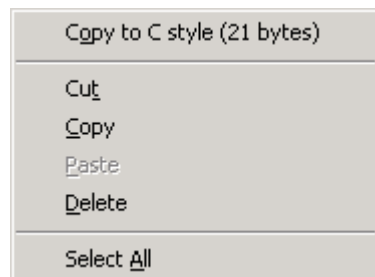
Packet Editor

To edit a packet,

If the packet editor view is not displayed, click Capture > Show Packet Editor.

Highlight the data you want to edit.

Right-click to display a pop-up menu with common Windows editing commands.



Option	Description
Copy to C style	Copies the selected text to the clipboard in a form ready to be used in a C program. For example, if the selected data is 13 00 00 20 11 94 , the clipboard will contain the following string: <code>\x13\x00\x00\x20\x11\x94</code> .

The toolbar at the top of the Packet Editor display window provides the following commands:

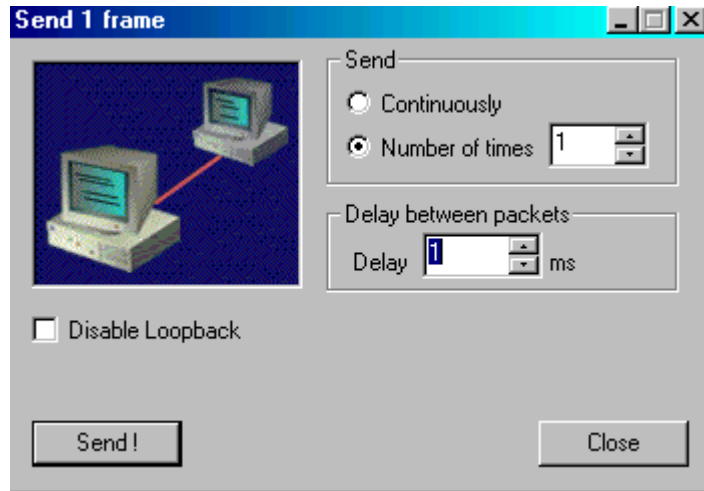
Iris	Option	Description
	Packet Operations	<i>New Empty Packet</i> , Clears the buffer and allows you to enter data to create a completely new packet.
		<i>Delete</i> , deletes the currently selected packet
	Save Packet to Disk	Saves the currently displayed packet to disk.
	Modify Packet Size	Allows you to change the current size of the packet. It can be made bigger or smaller, depending on your needs. Making the packet bigger pads it with NULL (Hex 00) bytes. Making the packet smaller takes the end bytes off.
	Insert this packet into packets list	Pushes the packet into the packet buffer. The new packet will show up in the Packet Display Window.
	Send This Packet	Sends the currently shown packet over the wire.

To open the Packet Editor and send packets,

Click Capture > Show Packet Editor.

Click a packet.

Click Send Packet .



Option	Description
Send Continuously	The selected packet will be sent until you click Stop .
Send Number of Times	Set the number of times you want the packet sent.
Delay between packets	Set the number of microseconds you want between transmissions. If set to 0 ms, Iris will send packets extremely fast bring the bandwidth utilization close to 100%.
Disable Loopback	Click to stop receiving your own packets.
Send	Click to start sending packets.
Stop	Click stop sending packets.

Marking Packets

You can group packets by marking them. Marking can create a specific buffer of captured packets that you would like to save, delete from the screen, or send back to the wire.












To mark one packet,

Right-click a packet and select Mark packet from the pop-up menu.

To mark multiple packets,

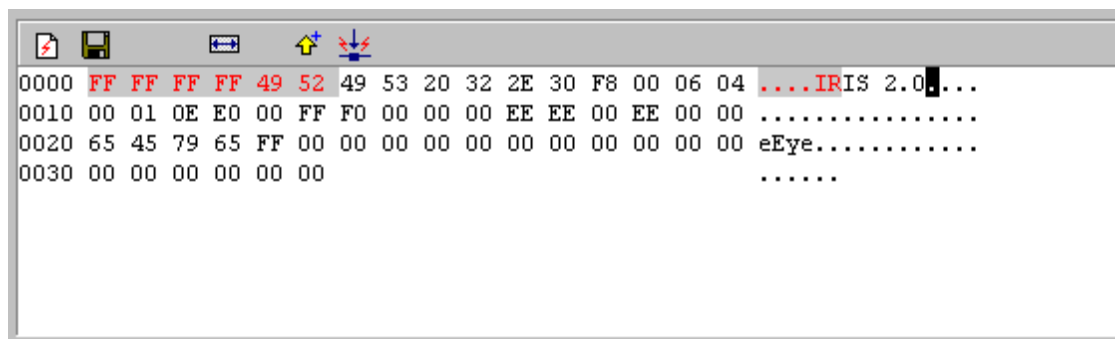
Double-click each packet you want to include in the group.

You can also use the Find Packets command to mark packets using filter rules.

 Unmark packet	Ins	Mark/Unmark selected packet. See Marking packets.
 Mark all packets		Mark all displayed packets.
 Mark whole session		Unmark all displayed packets.
 Unmark all packets		Mark all packets within current packet's communication thread (TCP session, UDP channel)
 Invert selection		Mark unmarked packets or vice versa.
 Send this packet		Send packet.
 Send all marked packets		Send marked packets.
 Save marked packets		Save all marked packets to disk.
 Add to Address Book	▶	Add to address book source or destination host.
 Delete this packet		Delete currently selected packet.
 Delete all marked		Delete all marked packets.

Note: Packet(s) will be deleted only from list but will still be present in buffer.

This command will send marked packets from packets list window to the network.



Sending Packets

There can be only one selected packet. If you want to send more packets to the network, mark packets and use Send Marked Packets command.

To send a selected packet,

Highlight the packet you want to send in the packet list.

Click **Send** .


Using Iris to Troubleshoot Your Network

You can use Iris to troubleshoot and stress-test your network by sending custom packets to specific ports or addresses or sending one or more packets repeatedly across the network.

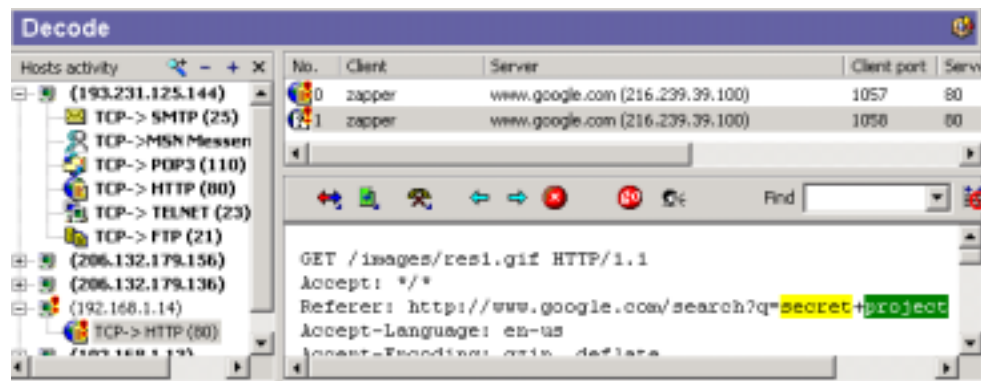
When **Delay between packets** is set to 0 ms, Iris will send packets extremely fast. On a 10 MBPS, Iris can send up to 9000 packets per second bringing the Bandwidth Utilization up to more the 90%.

Using Iris to search traffic for words

Use this feature to locate sessions (like web pages, emails, etc) containing specific words. All sessions displayed in Decode will be searched and those sessions containing the strings will be marked with a red exclamation mark.

To open the Search Traffic dialog, click on the  toolbar icon or use the menu Decode | Find words...

Click Reset to remove marks from sessions.



Decoding and Reconstructing Captured Data



In decode mode captured data is reassembled in a way that allows you to actually view each session as if you were the actual owner of the session.

Decoding and Reconstructing Captured Data

In addition to the expected sniffing functions, Iris lets you reconstruct data and display all content that was captured. In decode mode, captured data is reassembled in a way that allows you to view each session as if you were the actual session owner. Many common protocols can be reconstructed in this manner.

Session assembly

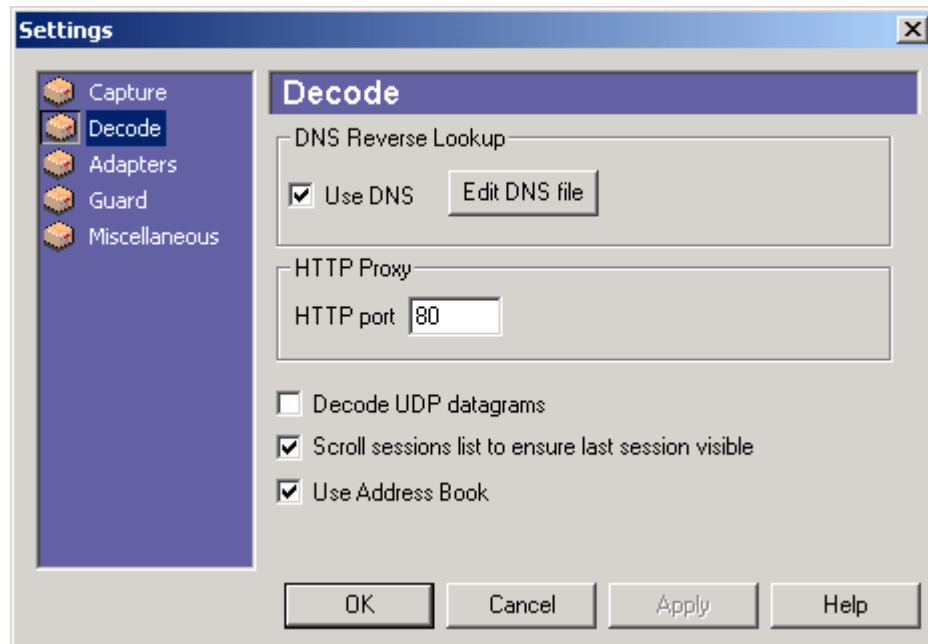
TCP is a connection-oriented protocol. This means that in a normal TCP session, such as downloading a web page, a certain sequence that must be followed to create a connection, and then to destroy that connection. TCP is also session based, meaning that once a connection is established, it remains established and can send data until it goes through a proscribed close sequence.

Traditional sniffers offer you a view of all packets representing a TCP sequence. You can look at each packet in the session in sequence and a knowledgeable administrator can determine what was happening in a TCP session.

Iris takes this one step further. A reassembled HTTP session is fed into a decoder that allows it to be displayed as a fully rendered web page. This allows Iris to not only show you the packet that created the session, but a realistic view of the actual contents of data sent within that session. This applies to other session types as well. Iris can reconstruct emails and their attachments also.

Setting Decode Options

To change your decode settings,
Click Tools > Settings > Decode.



Select the settings as described below.

Setting	Description
Use DNS	Allows you to look-up hosts in the Decode View, providing resolved names (if they are available). This makes it simpler to view which hosts you are monitoring.
HTTP proxy	Enter proxy port value. Use this option in case HTTP traffic is not using the default port (80). This value will be used to recognize HTTP sessions.
Decode UDP Datagrams	Selects whether or not you want Iris to show the content of UDP datagrams in Decode Mode.
Scroll packets list to ensure last session visible	Select whether or not you want the session list to scroll, ensuring the most recent sessions are displayed on the screen at all times.
Use Address Book	The address book replaces the network address of the network node with its respective symbolic.

The Decode Menu

Disable/Enable Decode

When Iris is used to look only at packets, we recommend you disable the decode module. (TCP session's reconstruction). However, if the Decode Logging is enabled, the decoding will take place even if Display Decoding is OFF.

When Decode is disabled, Iris will not send the packets to the Decode engine and therefore the only way to decode packets captured in the past (which are not in the current buffer) is to load a log file containing them.

To Disable or Enable decode output,

Click Decode > Disable Code Output or Enable Code Output.

Note: If Decode Logging is on, Iris will still decode sessions.

Send Buffer to Decode

Iris starts reconstructing TCP sessions when its buffer is completely filled or when Capture is stopped. So, if you set a 5000 packets buffer and your traffic is at about 1000 packets a minute, you have to wait 5 minutes until you see something in Decode Views. The Decode buffer command may be used to start the decoding process sooner, without waiting for the buffer to be completely filled.

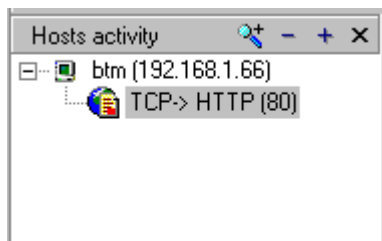
Viewing Host Activity

The Host Activity window displays a tree-view of hosts that have had traffic. If a host is selected, it displays a list of possible types of traffic. The traffic is broken down by service. As a service is selected, a list of sessions between client and server are displayed in the session list window. Selecting one of these session traces will cause it to be decoded in the Session Data View.


To view host activity,

Click Decode. The Hosts Activity window displays at the left in tree form.

The following screen shows computers displayed from the local network.



Viewing Sessions

- To display a reconstructed session,
- From the Decode window,
- Click Decode > Send Buffer to Decode.
- Select a host and click the desired protocol.
- Select a session from the sessions list.
- Click the packet you want to view.
- Click  and select HTML as the viewing type.


The window will display in the lower window.


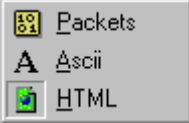
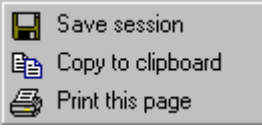


```
GET /cgi-bin/rad/aami.exe/RGROUP=r347 HTTP/1.0
Referer: http://www.nortonweb.com/nws/1033/sym/resources/y2kreadi.st
Connection: Keep-Alive
User-Agent: Mozilla/4.5 [en] (Win95; I)
Host: ads.zdnet.com
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg image/pr
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1, *,utf-8
Cookie: cgversion=4; browser=C1E71572384D58C8; ad=a34610

HTTP/1.0 302 Redirect
Date: Wednesday, 08-Dec-99 14:33:43 GMT
Server: Open-Market-Secure-WebServer/2.0.5.RC0
MIME-version: 1.0
Security-Scheme: S-HTTP/1.1
Set-Cookie: ad=a30044; domain=.zdnet.com; path=/
Location: http://ads3.zdnet.com/i/g=r347&c=30044/http://images.zdnet.
```

The window displays the reconstructed session. In the picture shown above, for example, it shows an HTTP request and below it, the answer from the web server instructing the client browser to redirect to another location. You can also see that the cookie was sent to the server in the request and how the server installed another cookie on client's computer.

Toolbar Button	Description
	Traffic View Control allows you to select which types of traffic you want to view. It offers you the option to watch only server side traffic, client side traffic, or both. Watching both client and server is the default. When Both is selected, meaning that the full session should be shown, data sent by Client will have a blue color, while Server data will be

	colored in red.
	<p>Click this button to display a drop down menu with the following session data display options:</p>  <p>HTML: Allows you to change the format of the displayed session. The default format is HTML, which allows web pages to be displayed as the end user would see them.</p> <p>ASCII: Displays text as normal 8-bit characters within the ASCII range. This format will not display Web pages, but will show the HTML tags.</p> <p>Packets: Displays the packets which comprise the selected session.</p> <p>While the main view mode is HTML, it is sometimes useful to see a session in ASCII mode. For example, if an e-mail is displayed in HTML mode, the MAIL FROM: and RCPT TO: fields won't be shown because they are enclosed in angle brackets <>. Switching to ASCII mode, those fields will be revealed.</p>
	<p>Click this button to display a drop down menu with the following session options:</p>  <p>Save: Save all session's packets that comprise the selected session in a capture file.</p> <p>Copy to clipboard: Copy the content to the clipboard in HTML format.</p> <p>Print this page: Print the window content.</p>
	Standard browser navigation buttons.
	Retrieve sniffed page from Internet, using the original cookies. The Go Get It! button is enabled only when a HTTP session containing valid GET command is selected. This feature does not work with POST or other types of server commands.
	Use this option to instruct Iris to fit session's data in window. Sometimes the displayed content exceeds the window horizontal size, requiring extensive use of the horizontal scroll bar.

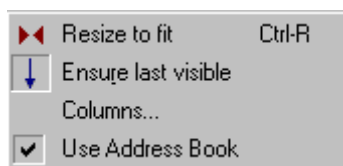
Viewing Session Data

The Sessions list window displays all sessions related to the hosts and ports selected in Hosts activity window.

To view a session,

Click a session to see its data in Session data window.

Right click a column header to display a pop up menu.



Command	Description
Resize to fit	Used to automatically set the column sizes to extend as far as the text goes
Ensure last visible	Scroll the list when a new packet is inserted.
Columns	Opens up a dialog box that allows you to customize the displayed columns
Bytes in	Total number of bytes of data transmitted from server to client.
Bytes out	Total number of bytes of data transmitted from the client to the server.
Total bytes	The sum of the above.

These values reflect only application level data (MAC, IP, and TCP headers are not displayed). That makes it possible for sessions with a Total bytes value of 0, (meaning that the session consists only in TCP/IP configuration packets) to be displayed.

For these sessions, Session Data window will display the following message: This session doesn't contain readable data. Choose Packets format to view packets.

Detecting Connection Attempts




Guard watches over your network, warning you when an intruder tries to connect. It can be also set to notify you when someone inside your network tries to connect to computers without authorization.

Guard displays the date and time of the connection attempt, the victim and intruder IP addresses and the DNS name and port on which the connection attempt has been made.

Note: If Guard raises an alarm, it doesn't mean that the connection was successful. It means only that the victim was probed on the specified port. By looking at victim's sessions in Decode, you can tell if the attempt was successful or not.

Guard Settings

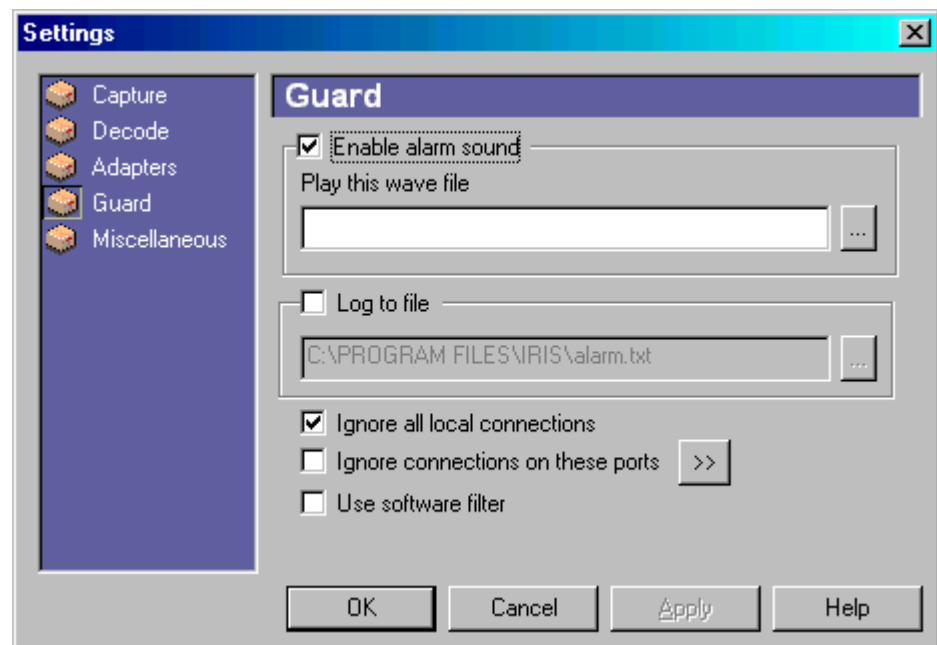
To enable Guard, from the left control pane, click Guard . If Guard is off, you will be asked to turn it on. When enabled, Iris will display the Guard window and will monitor SYN packets addressed to local network computers.

OR

If the left control pane is not visible, click Tools > Guard > Enable Guard.

To change Guard settings,

Click Tools > Guard > Guard Settings.




Make changes on any of the settings and click OK.

Setting	Description
Enable alarm sound	Iris will play an alarm when a connection attempt is detected.
Play this wave file	You can select an audio file that will be played instead of the default sound.
Log to file	File where connection attempts will be logged and saved.
Ignore all local connections	Iris will use the current IP address and network mask to determine if an address is from the local network or if it is from an external host. If this option is checked, Iris will not log connection attempts initiated by local hosts.
Ignore connections on these ports	Iris will ignore connection attempts seen on a port from the allowed ports list.
Use software filter	<p>Apply filter rules to connection attempts. If this field is cleared, Guard will log all connection attempts (which are not filtered by the allowed port list) regardless of the applied software filter.</p> <p>This option is primarily used to allow the Guard module to function independently of the current filter. However, using the filter gives you the option of watching connection attempts only on specific hosts.</p> <p>In both cases, the Ignore connections on these ports option will be in effect.</p> <p>Note: Even if Use software filter is checked, filter will be applied only if Apply filter to incoming packets is ON. (Toolbar button)</p>

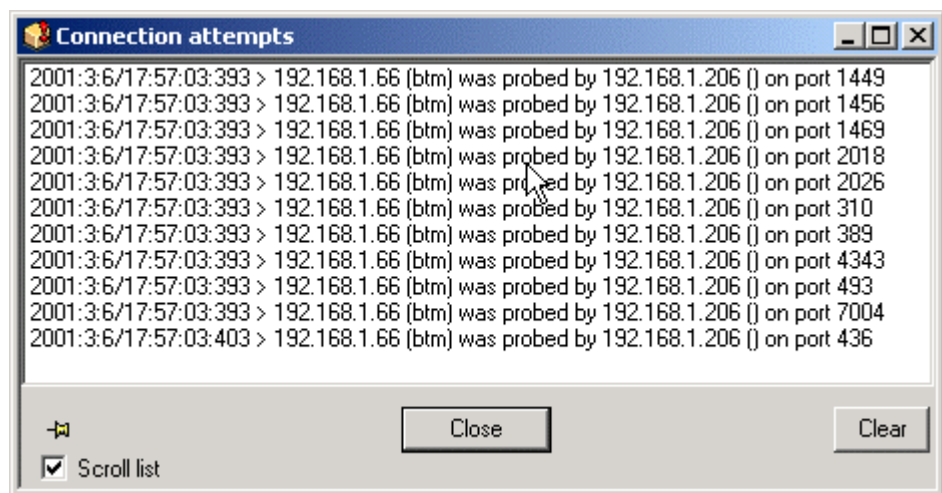
Guard Alerting

To enable Guard,

Click Watch incoming connection requests on the toolbar. 

Open the Guard window by clicking on the Guard icon  or go to Tools | Guard | Show Guard window.

Guard window is shown below.



In this screenshot, you can see how 192.168.1.66 has been port scanned by 192.168.1.206.

Creating Filters



By defining and limiting the type of detail you collect, and saving it as a filter, you can more easily analyze your capture logs.

Filters are selected through the Filter Menu or the Filter icon on the toolbar. They can be saved and reused as needed. The active filter can also be edited before you save it. If a filter is not collecting the data you want, it can be cleared from the main menu.


Using the Address Book in Filters

The Address Book allows you to define your network nodes in more-readable symbolic names.

To use the Address Book in a Filter Definition,

Right-click the packet that contains the address you want to filter on and select Add to Address Book (Add source or Add Destination) menu item. This address can now be used in creating filters.

Click Views > Address Book to open the Address Book.

From the left Control Panel, click Filters  and open the IP Filter property page.

Drag an address from under the Address Book tree branch into a filter cell on the IP or MAC filters dialogs.

When inserting a MAC address that already exists in the Address Book but with a different IP address, Iris will consider it a router entry and will change the type of all entries with that MAC address to Router.

Hardware Filter

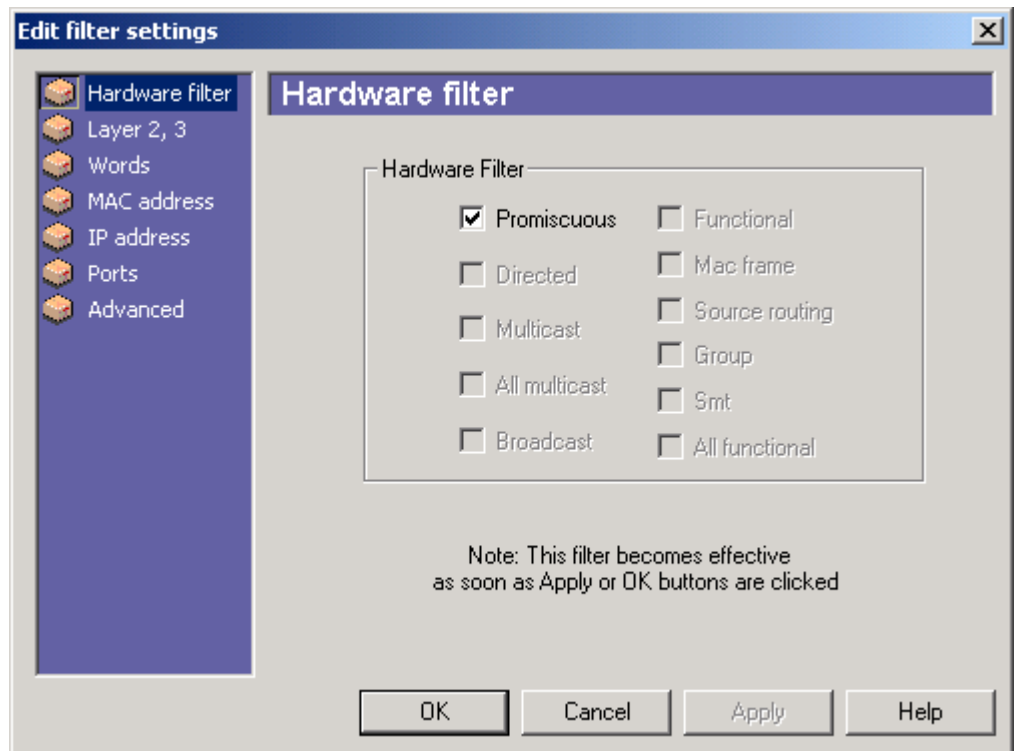
This filter tells the network adapter to capture the identified packets.

To set a hardware filter,

From the left control panel, click  Filters.

Click Hardware Filter.

Select the filtering options as described below.



Setting	Description
Promiscuous	Capture all packets from current network segment. This is the default mode of operation. To function at whole capacity, IRIS must stay in promiscuous mode.
Directed	Let pass only those packets sent directly to this adapter. Packets leaving this adapter will not be captured.
Multicast	Capture multicast packets.
All multicast	All multicast address packets, not just the ones enumerated in the multicast address list.
Broadcast	Broadcast frames (destination MAC address FF:FF:FF:FF:FF:FF)
Functional	Functional address packets sent to addresses included in the current functional address.
Mac Frame	NIC driver frames that a Token Ring NIC receives.
Source Routing	All source routing packets. If the protocol driver sets this bit, the NDIS library attempts to act as a source routing bridge.
Group	Packets sent to the current group address
Smt	SMT packets that an FDDI NIC receives.
All Functional	All functional address packets, not just the ones in the current functional address.

Layer 2,3 Filter

Use this filter to track packets based on their type (level 2) and if there are IP packets, on their subtype (level 3)

To set a Layer 2,3 filter,

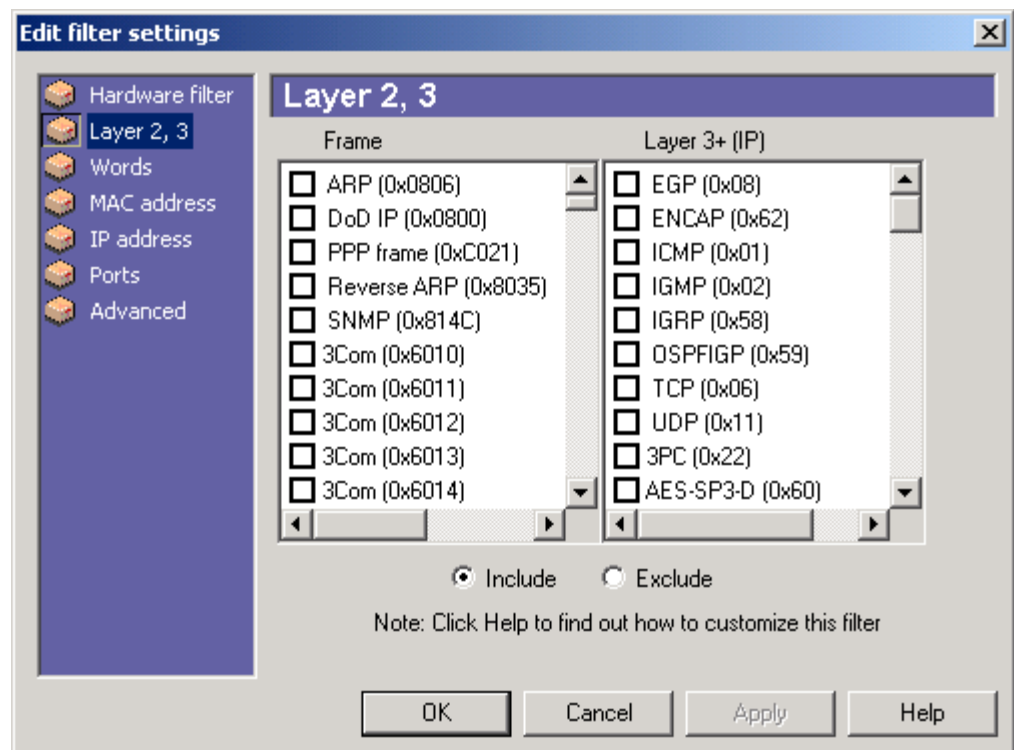


From the left control panel, click  Filters.

Click Layer 2, 3 Filter.

Select the filtering options as described below.

Selecting one protocol from Layer 3 list, will automatically select an IP type from the Layer 2 list.



Select the Mode.

Include: Only packets matching the filter condition will be captured.
Exclude: Packets matching the filter condition will be discarded.

Select the packets you want to include in the Filter.

If you want to test the filter, click Apply.

Customizing protocols

You can customize any protocol by editing *proto.dat*, located in the Iris installation directory.

For Layer 2, edit entries under the [PROTOCOL] section and for layer 3, edit entries under [IP PROTOCOL] section.

To edit the file,

Open WordPad.

Click File > Open.

Select All documents.

Navigate to the Iris installation folder, and select *proto.dat*. (The .dat extension may hidden.)

New protocols can be added and existing protocols can be modified. To place a type among the first ones displayed in this filer, precede its name with an underscore.

Example: (taken from the *proto.dat* file)

01 _ICMP [Internet Control Message]

02 _IGMP [Internet Group Management]

03 GGP [Gateway-to-Gateway]

ICMP and IGMP will be displayed among the first entries while GGP will be displayed where it fits alphabetically order.

Layer 2 entries can be edited to represent a range.

Example:

1001-100F Berkeley Trainer

All 1001,1002,1003...100F values will be decoded as Berkeley Trainer.

Restart Iris to activate the changes.

Words Filter

Use the Words filter to track packets or sessions containing certain strings. The string comparison is case insensitive.

For specific help regarding this rule's controls, keep the mouse over the controls. A tool tip will appear, explaining what are they meant to do.

To set a Words filter:



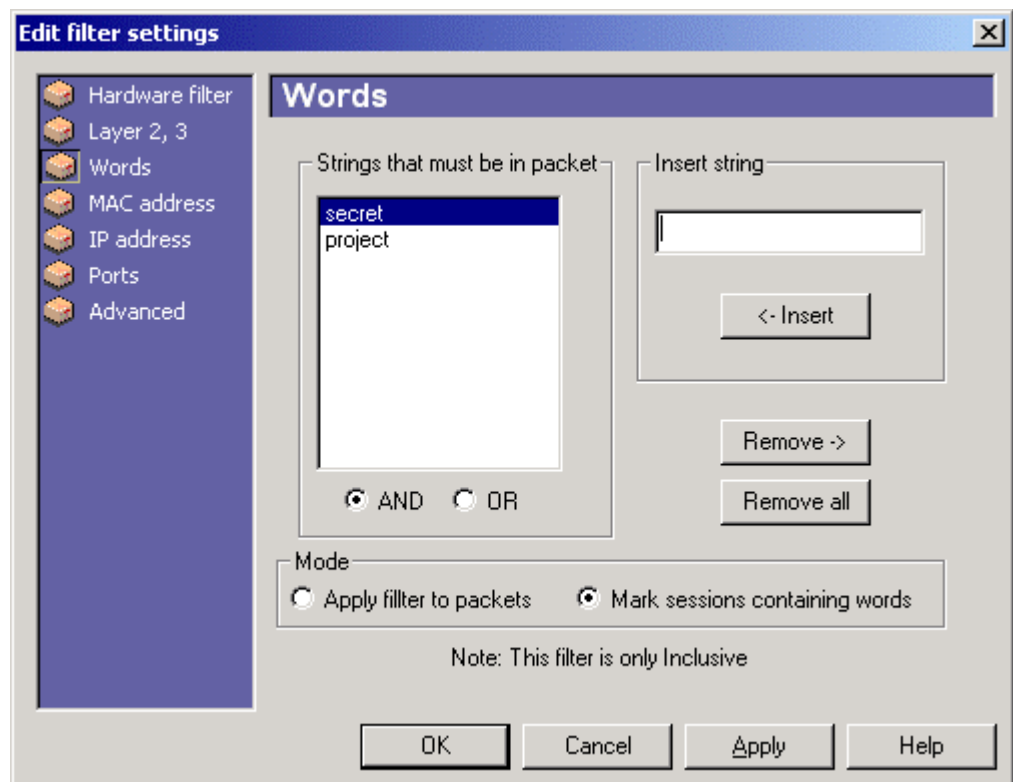
From the left control panel, click  Filters.

Click Words Filter.

Select the filtering options as described below.

Enter the word strings you want to filter on.

Use AND or OR radio buttons to specify if packets should contain at least one string (OR) or all strings from the strings list (AND).



Apply filter to packets:

This is the "traditional" word filter mode where only packets matching the filter rule are captured. All other packets are discarded.

Mark sessions containing words:

In this mode, Words filter will let pass all packets but will mark in Decode view those sessions containing filtered words.

After data is collected, in Decode mode we will see:



Please note the **!** mark. It signifies that "dexter" sent or received data containing both "secret" and "project" words and the words were in a HTTP session (port 80). Clicking on the marked protocol, we will be able to see the session containing the words:

No.	Date/Time (M:D:Y/h:m:s:ms)	Client	Server	Client port	Server port	MAC client
2	6:11:2001/16:27:51:413	dexter	www.google.com (216.239.33.100)	2392	80	dexter
3	6:11:2001/16:28:10:090	dexter	www.google.com (216.239.33.100)	2393	80	dexter
4	6:11:2001/16:42:5:471	dexter	www.google.com (216.239.33.100)	2400	80	dexter


```
GET /search?num=100&hl=en&lr=&safe=off&q=secret+project&btnG=Google+Search HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/javascript, application/x-shockwave-flash, application/xml, application/xhtml+xml, application/vnd.ms-powerpoint
Referer: http://www.google.com/search?num=100&hl=en&lr=&safe=off&q=secret+project
Accept-Language: en-us
```

For specific help regarding this rule's controls, keep the mouse over the controls. A tooltip will appear, explaining what are they meant to do.

Note: This filter is only inclusive. It only captures packets that match the rule.

MAC Address Filter

This filter class allows you to track based on specific hardware layer addresses known as MAC (Media Access Control) addresses. This filter monitors specific packets originating or destined for specific hardware adapters.

To filter on a Mac Address,

From the left control panel, click  Filters.

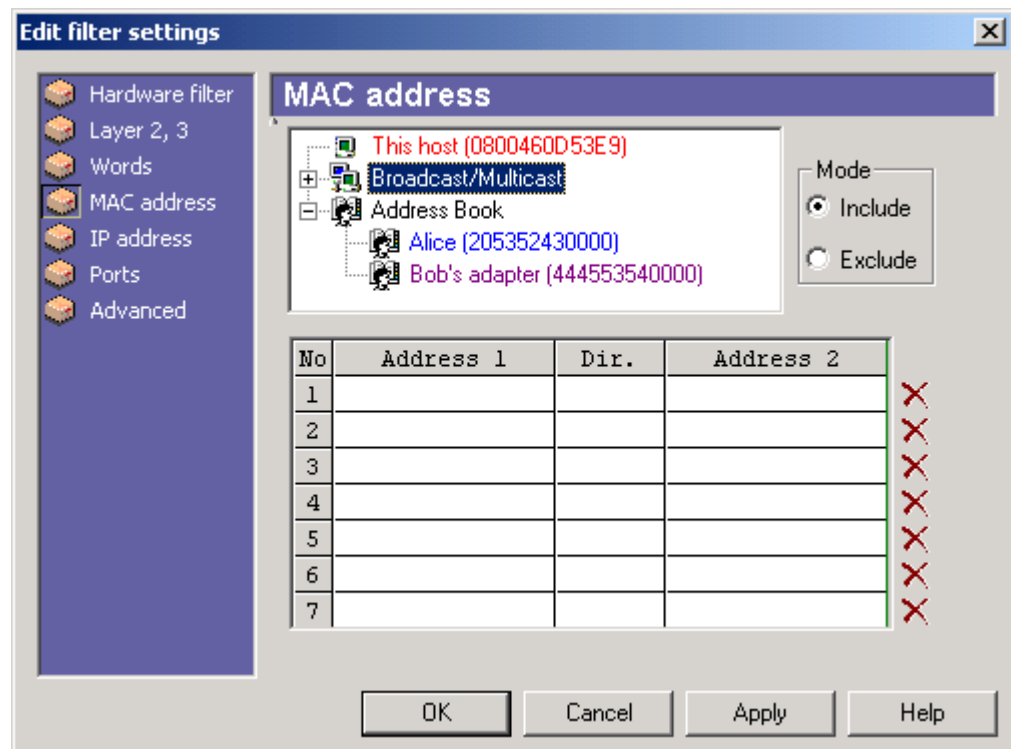
Click MAC Address Filter.

Select the Mode.

Include: Only packets matching the filter condition will be captured.

Exclude: Packets matching the filter condition will be discarded.

The top box includes addresses already known to Iris (including those in the Address Book). You can click and drag addresses from the Known Address box and drop them into the Address 1 or Address 2 fields. If you do not want to click and drag known addresses, you can enter addresses manually by typing them in the appropriate fields.




IP Address Filter

The IP Address filter allows you to filter on source or destination IP addresses.

To filter on IP Address,



From the left control panel, click  Filters.

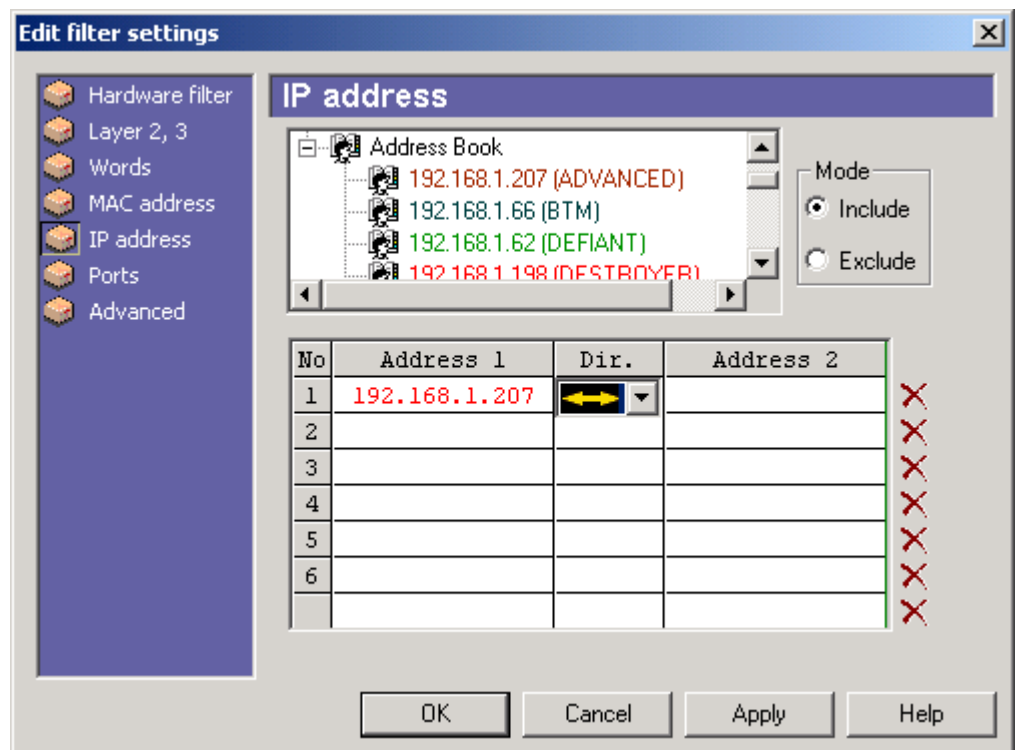
Click IP Address.

Select the Mode.

Include: Only packets matching the filter condition will be captured.

Exclude: Packets matching the filter condition will be discarded.

The top box includes addresses already known to the Iris (including those in the Address Book). You can click and drag addresses from the Known Address box into the Address 1 or Address 2 fields to filter on these addresses. If you do not want to click and drag known addresses, you can also add addresses manually by putting your cursor in the appropriate field and typing.



Ports Filter

The Ports filter allows you to capture data based on source or destination Port numbers including TCP port numbers associated with services like SMTP or HTTP. By watching for traffic on a specific port, you can limit your packets to these types of services.

List of known ports can be sorted by Description or Port number by clicking on corresponding column headers.



From the left control panel, click  Filters.

Click Ports.

Select the Mode.

Include: Only packets matching the filter condition will be captured.

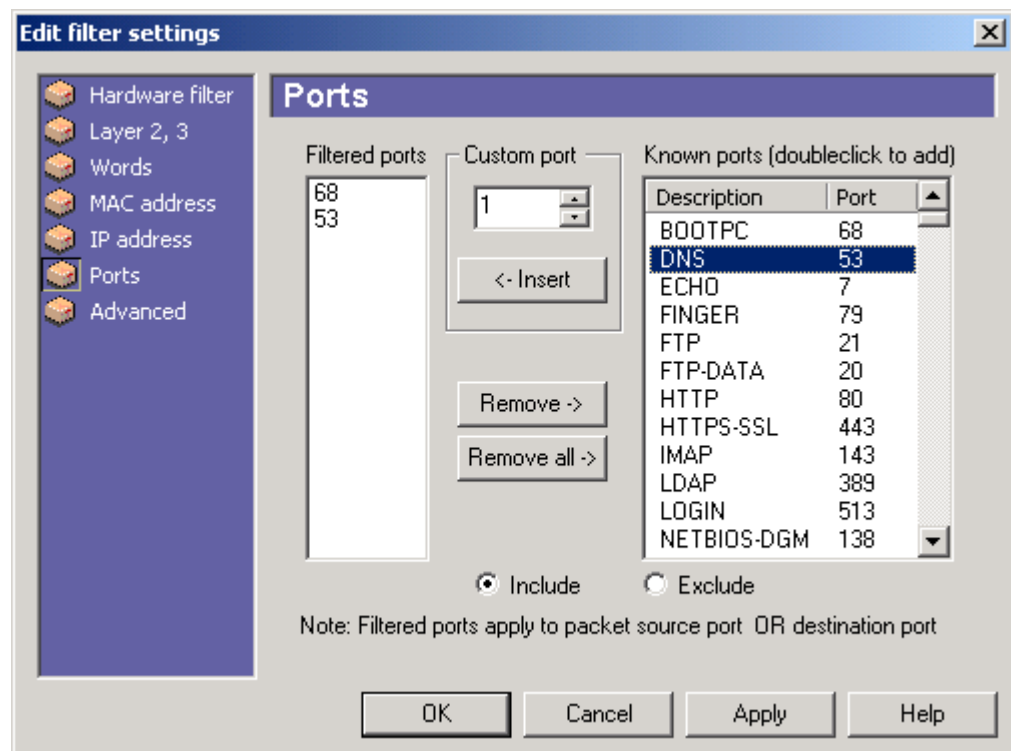
Exclude: Packets matching the filter condition will be discarded.

Select options from the Known Ports list.

Click Insert.

To remove ports from the filter list, click Remove or Remove All.

Click on the corresponding column headers to sort the list of known ports by Description or Port number.



Customizing ports

Open WordPad.

Click File > Open.

Select All documents.

Navigate to the Iris installation folder, and select *proto.dat*. (The .dat extension may be hidden.)

ICMP and IGMP will be displayed among the first entries while GGP will be displayed where it fits in alphabetical order.

Example: (taken from the proto.dat file)

01 _ICMP [Internet Control Message]

02 _IGMP [Internet Group Management]

GGP [Gateway-to-Gateway]

For TCP ports, edit entries under [TCP PORTS] section.

Note: Ports should be entered in decimal.

New ports can be added and existing ports can be modified. To place a port value among the first ones displayed in this file, precede its name with an underscore.

Restart Iris.

Advanced Filter

Two filter rules are available in this filter page; size and packets containing hexadecimal data.



From the left control panel, click  Filters.

Click Advanced.

Select options as described below.

Edit filter settings

Advanced

Size

Show packets having bytes

Data

Show packets having Hex data (max 10 bytes) Offset

at

Data length: 2 bytes

Note: This filter is only Inclusive

OK Cancel Apply Help


Option	Description
Size	Use this filter to let pass packets having more, less, exactly, or a different number of bytes than a given value.
Data	This is useful for packets that can't be properly filtered using other filter rules, if they present a common pattern of having the same data at the same offset. All data bytes and the offset should be entered in hexadecimal. Note: Hex data should be contiguous ("FF A0 xx 11 23" will be considered to be a 2 bytes buffer: FF A0)

Logging Activity



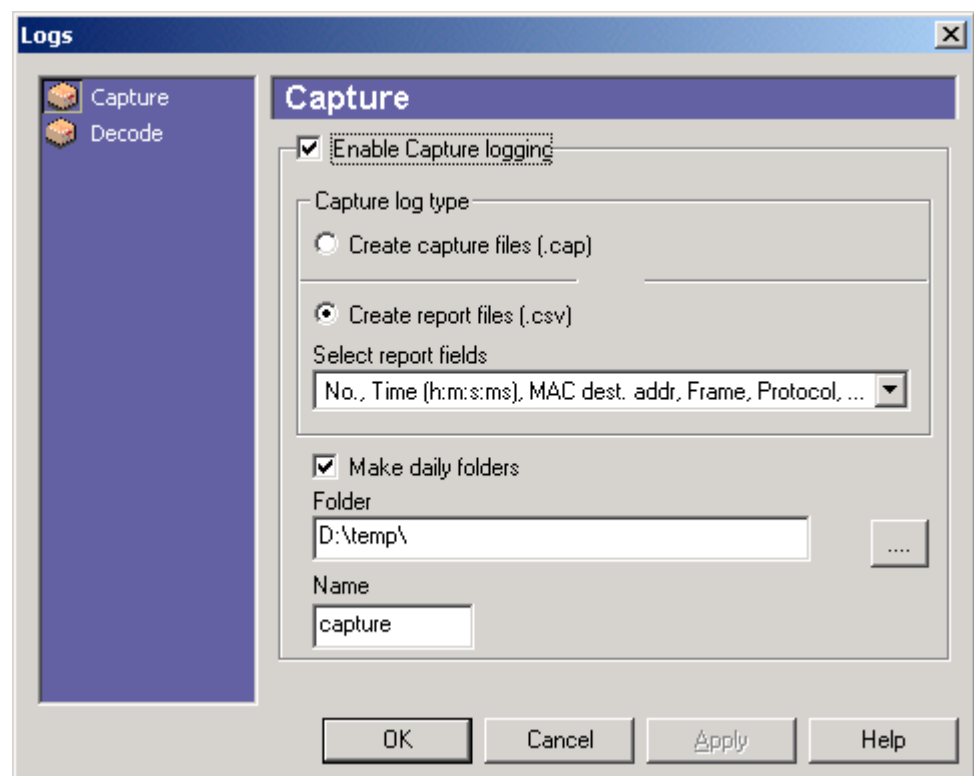
Enable Capture Logging

To enable Capture Logging,

From the left Control Panel, click  Capture, or Click Tools > Logs > Capture Logs.

Select the logging options you want to enable and click OK.

Note: You must select Enable Capture Logging to change any of the other options.




Setting	Description
Create report files	With this option selected, Iris will create text logs in the csv (comma delimited) format. Packets data will not be saved.

No	Timestamp	Type	Protocol	IP src	IP dest	Size
0	3:0:0:000	IP	TCP->POP3	x.x.x.x	x.x.x.x	62
1	3:0:0:000	IP	TCP->POP3	x.x.x.x	x.x.x.x	1514

Setting	Description
Select report fields	Select the fields that should be saved in Capture logs (when saving as traffic reports).
Make daily folders	Iris creates a new folder for each day's logs. This allows you to easily search and sort data.
Folder	Indicate the folder where logs should be stored. Make sure the specified volume has enough free space.

Enable Decode Logging

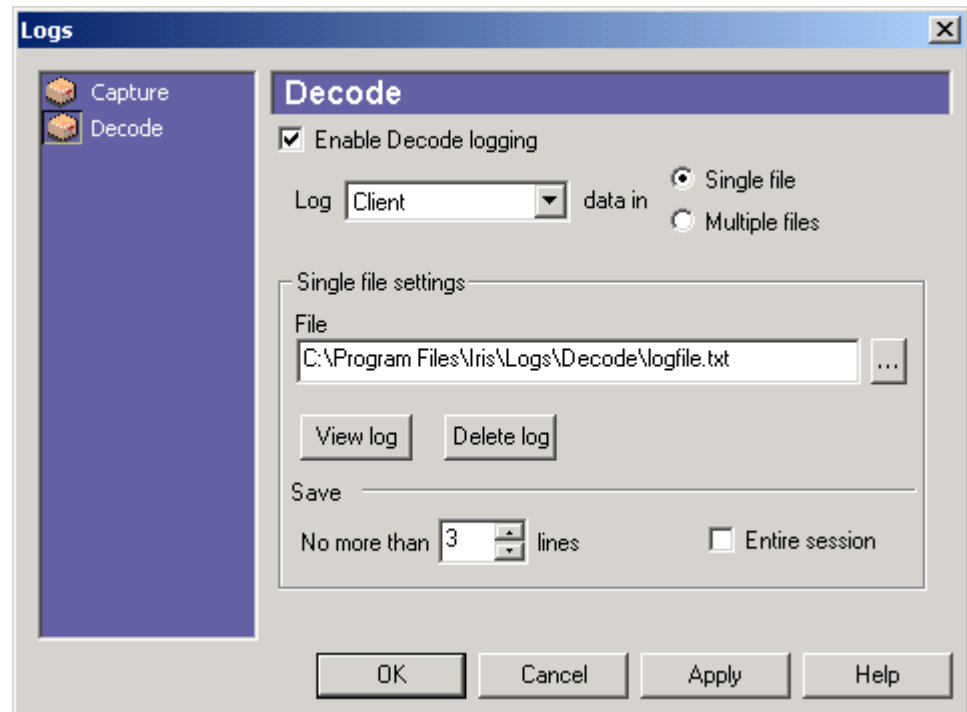
To enable Decode Logging,

From the left Control Panel, click  Decode, or Click Tools > Logs > Decode Logs.

Select the logging options you want to enable.

Note: You must select Enable Decode Logging to change any of the other options.

Make changes on any of the settings and click OK.



Setting	Description
Log to file	File where connection attempts will be logged and saved. Logs can be saved in a single file or in multiple files. Depending on the selection made, the Iris will display the appropriate set of controls. If logging is set to Single file, displayed controls will allow to specify the path and name of the log file. Decoded sessions will be appended to the specified file. If logging is set to Multiple files, you must set the Folder and file size limit. Logs names will start with Decode and will contain the timestamp.
Logs type	Iris can log the reconstructed session pertaining to the client or the server.
Save No more than <number> lines	If the reconstructed session has ASCII text, Iris can save only a number of lines (terminated with <CR>). For example saving 9 lines will usually result in logging only the E-Mail headers and not the content.
Save Entire session	Saves the reconstructed session.

Enable Guard Logging

To enable Guard Logging,

Click Log to File

Enter the file name and location where you want the log file saved.

Guard log file is shown below.

```
2001:2:8/14:30:22:064 > 193.167.11.177 (Iari) was probed by 193.167.11.189 ()
on port 27374
```

```
2001:2:8/14:30:50:145 > 193.167.11.177 (Iari) was probed by 193.167.11.189 ()
on port 27374
```

```
2001:2:8/14:30:52:308 > 193.167.11.177 (Iari) was probed by 193.1.15.17 () on
port 1243
```

In this log file, you can see that in only nine minutes 193.167.11.177, was probed by two different intruders. They tried to connect to ports 27374 and 1243, which are used by Back Orifice and SubSeven Trojan servers.

Importing Iris Log Files to a Spreadsheet

You can import Iris Log Files into spreadsheet programs such as Excel™.

To create files to import into a spreadsheet,

Capture files

Click Tools > Logs > Capture logs.

Select Save as columned traffic report.

Click File > Save decoded packets > Columned report

To import files,

Open the spreadsheet program.

Click File > Open (Text Files) and select the log file to open.

Follow instructions displayed by Excel.

Displaying Network Statistics



Statistics show the number of packets or traffic volume (bytes) and can be viewed in 5 different modes (Horizontal Bars, Pie, Pyramid, Vertical Bars and Doughnut) and can display the following information:

- **Bytes In**
- **Bytes Out**
- **Total Bytes**
- **Packets In**
- **Packets Out**

Statistics can be updated or cleared using the left vertical toolbar.

Configuring Graphs

To configure the graph display,

Click View > [Protocol Distribution, Top Hosts, or Size Distribution].

Click  ▼ to see the graph configurations available.



Select the graph type.

Displaying the Protocol Distribution Graph

The Protocol Distribution graph reports network usage based on the MAC, IP, and IPX layer protocols.

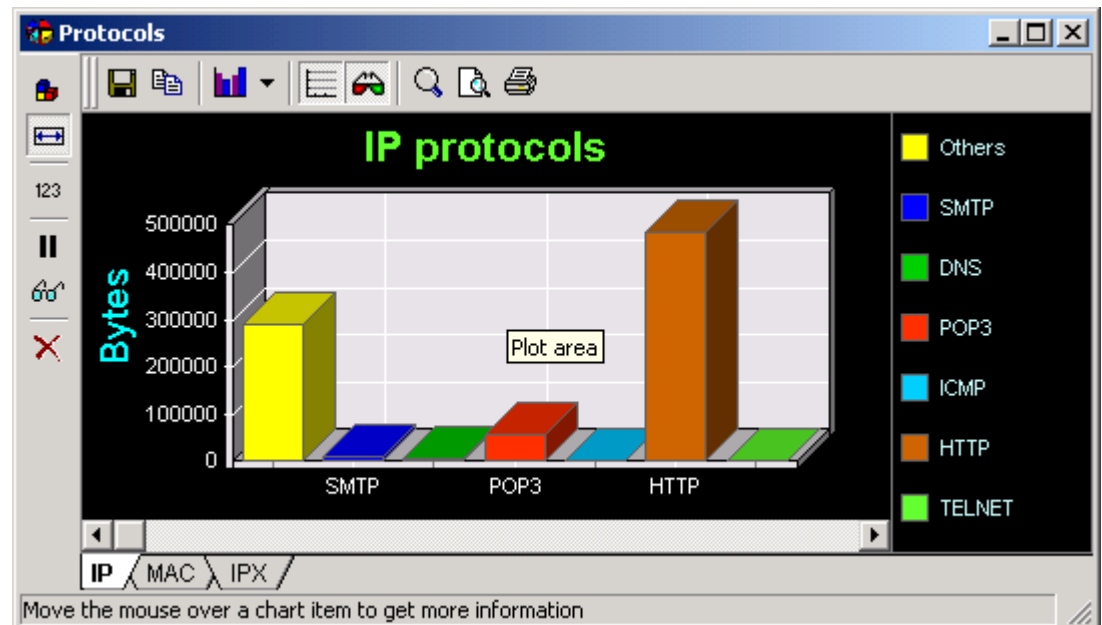
Note: Protocol Distribution statistics are collected only if the Protocol Distribution window is opened. When loading capture files, Iris will always collect statistics.

To display the Protocol Distribution Graph,

Click View > Protocol Distribution.

Click the tab representing MAC, IP, or IPX layer protocols.














Select options as described below.



Note:

The list of ports that Iris will consider as being of interest can be customized by editing **ports.ini** file in Iris installation folder.

If Iris sees a port which is not in the list specified in **ports.ini**, it will add the data in the Others category.

Icon	Command	Description
	Packets	Shows Protocol distribution based on the number of packets.
	Bytes	Shows Protocol distribution based on the traffic volume in bytes.
123	Values	Shows collected values in Horizontal Bars, Pyramid and Vertical Bars modes.
	Pause	Pauses the chart update.
	Update	Updates the chart (useful when the displaying is paused)
	Clear	Clears the chart.
	Save	Saves the chart in FX format.
	Copy to Clipboard	Copies the contents to the Clipboard.
	Gallery	Provides a selection of chart types.
	Horizontal Grid	Displays horizontal grid lines on the chart.
	3D/2D	Changes the view from 3-dimensional to 2-dimensional.
	Zoom	Select Zoom, then drag the mouse over the area you want to view more closely.
	Print Preview	Allows you to preview the graph and set printer options.
	Print	Print the graph

Displaying the Top Hosts Graph

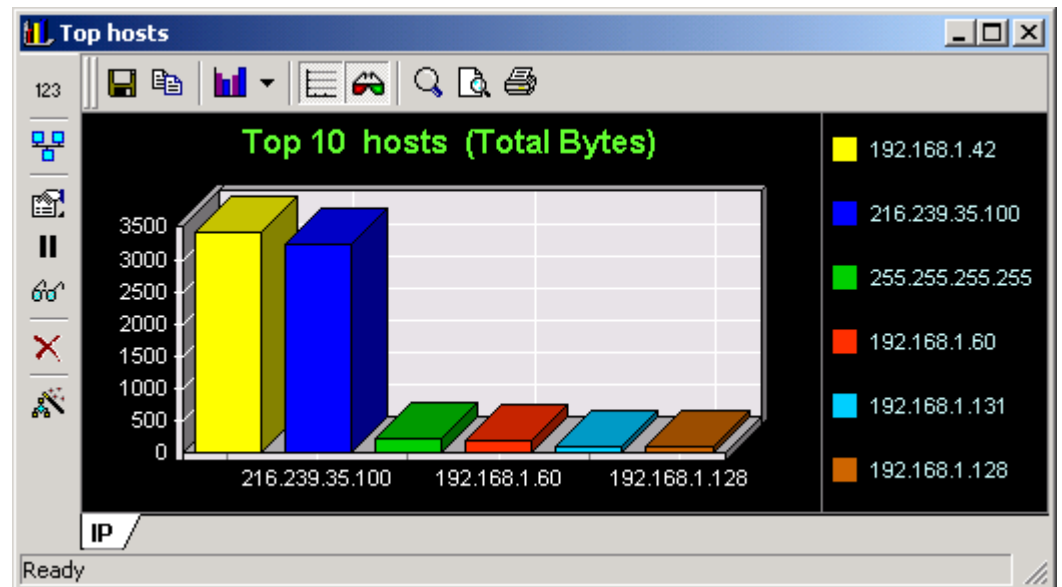
The host table provides an analysis of the IP layer traffic statistics collected for each host in real time.
















Note: Top Host statistics are collected only if the Top Hosts window is opened. When loading capture files, Iris will always collect statistics.

To display the Top Hosts Graph,

Click View > Top Hosts.

Select options as described below.



Icon	Command	Description
123	Values	Shows collected values in Horizontal Bars, Pyramid and Vertical Bars modes.
	Show Local hosts	When selected, IRIS will show only local hosts. To determine which one is local, IRIS uses gateway address and local IP address.
	Sorting Key	Selects the type of information to be displayed.
	Pause	Pauses the chart update.
	Bytes	Shows Protocol distribution based on the traffic volume in bytes.
	Update	Updates the chart (useful when the displaying is paused)
	Clear	Clears the chart.
	Settings	<p>Set Address Book usage, number of hosts displayed, and Update and Sort Intervals.</p> <p><i>Update Interval:</i> Number of seconds after which Iris will update the chart</p> <p><i>Sort Interval:</i> Hosts will be sorted on the specified key after this interval.</p> <p><i>Use Address Book</i> Note: If both Show hosts names and Use Address Book are selected, Iris will try first to use the name from Address Book and then the cached DNS name.</p> <p><i>Show N Hosts:</i> Specify the number of hosts to be displayed.</p> <p><i>Show Hosts Names:</i> If Use DNS is checked in Decode Settings, Iris will use the names discovered instead of IP addresses.</p> <p>Note: The host names will not appear instantly but only when they are resolved by the Decode engine)</p>
	Save	Saves the chart in FX format.
	Copy to Clipboard	Copies the contents to the Clipboard.
	Gallery	Provides a selection of chart types.
	Horizontal Grid	Displays horizontal grid lines on the chart.
	3D/2D	Changes the view from 3-dimensional to 2-dimensional.
	Zoom	Select Zoom, then drag the mouse over the area you want to view more closely.
	Print Preview	Allows you to preview the graph and set printer options.
	Print	Print the graph.

Displaying the Size Distribution Graph

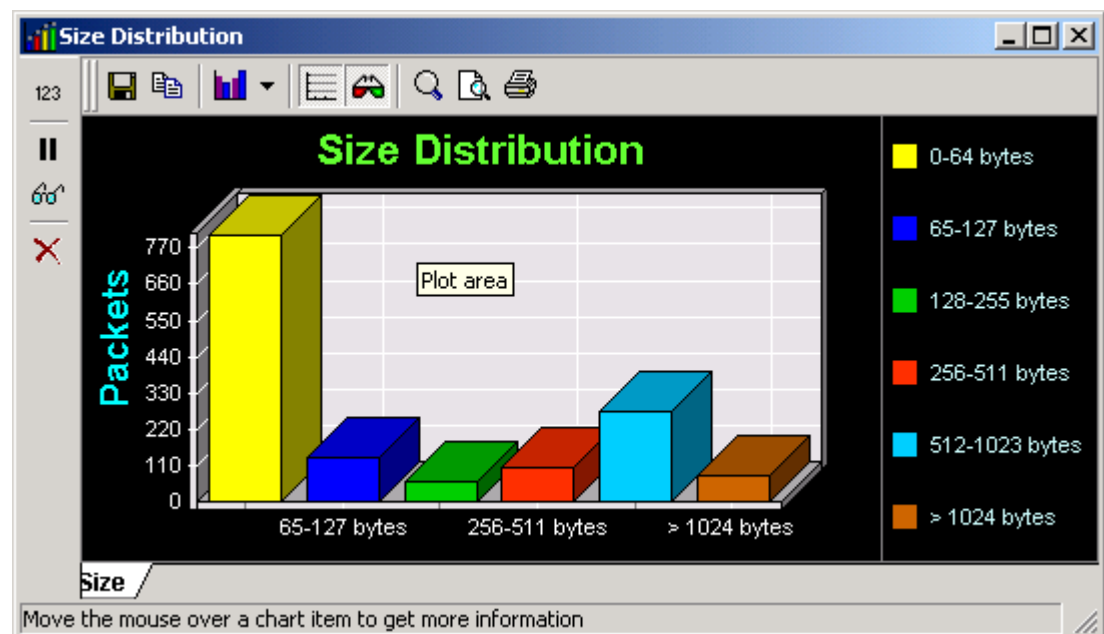
Statistics can show the number of packets with sizes in six different ranges (0-64 bytes, 65-127 bytes, 128-255 bytes, 256-511 bytes, 512-1023 bytes, and more than 1024 bytes).












Note: When capturing, Size Distribution statistics are collected only if the Size Distribution window is opened. When loading capture files, Iris will always collect statistics.

To display the Size Distribution Graph,

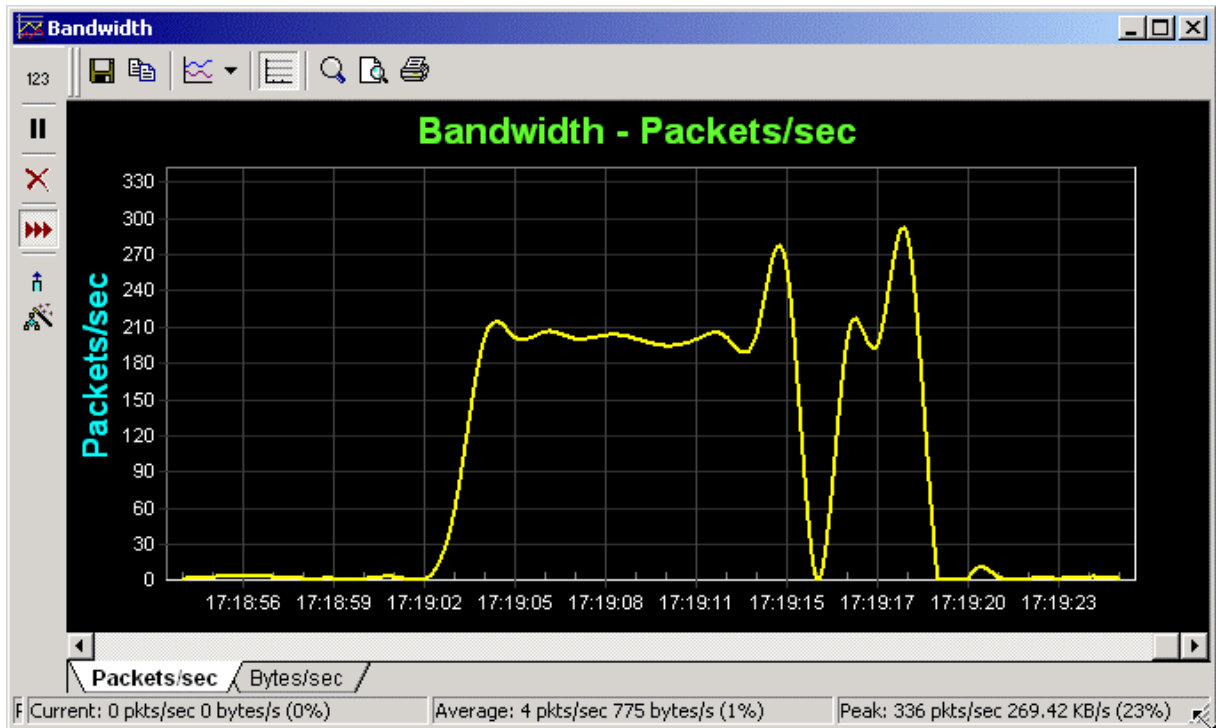
Click View > Size Distribution.

Select options as described below.





Icon	Command	Description
123	Values	Shows collected values in Horizontal Bars, Pyramid and Vertical Bars modes.
	Sorting Key	Selects the type of information to be displayed.
	Pause	Pauses the chart update.
	Update	Updates the chart (useful when the displaying is paused)
	Clear	Clears the chart.
	Save	Saves the chart in FX format.
	Copy to Clipboard	Copies the contents to the Clipboard.
	Gallery	Provides a selection of chart types.
	Horizontal Grid	Displays horizontal grid lines on the chart.
	3D/2D	Changes the view from 3-dimensional to 2-dimensional.
	Zoom	Select Zoom, then drag the mouse over the area you want to view more closely.
	Print Preview	Allows you to preview the graph and set printer options.
	Print	Print the graph.

Displaying the Bandwidth Graph



Icon	Command	Description
123	Values	Shows collected values.
	Pause	Pauses the chart update.
X	Clear	Clears the chart.
▶▶	Scroll	Specify if the chart should be scrolled if new data is available.
↑	Rescale	Rescale the chart making the peak value the maximum value of the Y axis.
🔧	Settings	Modify chart settings.
💾	Save	Saves the chart in FX format.
📄	Copy to Clipboard	Copies the contents to the Clipboard.
📊	Gallery	Provides a selection of chart types.
📏	Horizontal Grid	Displays horizontal grid lines on the chart.
🔍	Zoom	Select Zoom, then drag the mouse over the area you want to view more closely.

	Print Preview	Allows you to preview the graph and set printer options.
	Print	Print the graph.

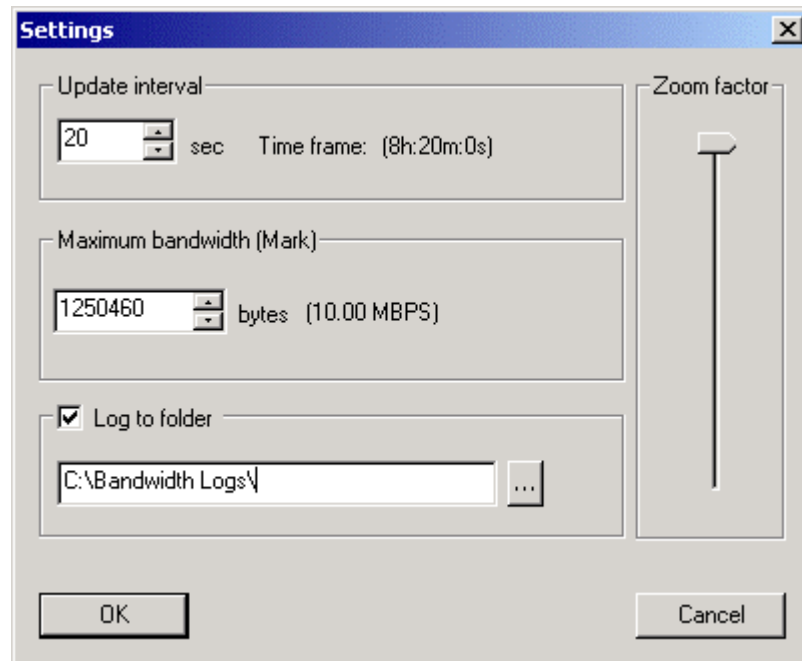
Bandwidth is showing real-time charts with packets per second and bytes per second.

On the status bar there are 3 panes displaying Current, Average and Peak values of packets/second, bytes/second and percentage of utilization based on the Maximum Bandwidth value set in Settings. (by default the value is the bandwidth of the local network)

Shortcuts: Use UP/DOWN arrow to increase/decrease the amount of information displayed while Bandwidth window is active.

Note: Bandwidth chart is collecting data only of the Bandwidth window is opened and will collect data even if the Capture is stopped.

Bandwidth Settings



Update Interval:

Is the number of seconds at which the chart is updated. By default Iris will hold in memory 1500 values. At a sampling rate of 1 second, that means that the chart will hold the latest 25 minutes worth of data (1500*1=1500 seconds = 25 minutes). At 20 seconds, bandwidth chart will hold 8 hours and 20 minutes worth of data. When the time frame ends, Iris will scroll the chart and the oldest value will be deleted.

For advanced users:

The number of points can be modified by adding a registry key specifying the new value. For this, create a new DWORD key named BandwidthPoints containing the new value under HKEY_CURRENT_USER\Software\Eye Digital Security\Iris\Settings\.

Maximum bandwidth:

By default Iris will use the bandwidth of the local network. For example a 10 MB network means 1.250.000 bytes per second. This value will be drawn in red within the chart and will be used to compute the utilization percentage.

Log to folder:

If checked, Iris will save the bandwidth in .csv (comma delimited) files into the specified folder. The time stamped log file will be updated at an interval twice as big as the update interval.

Zoom factor:

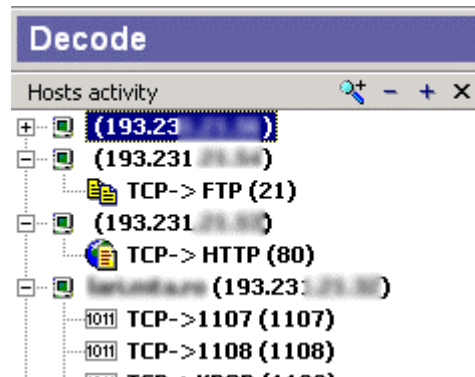
Increase/decrease the amount of information displayed in charts. While chart window is active the same effect can be obtained using UP/DOWN arrows.

Creating Traffic Reports

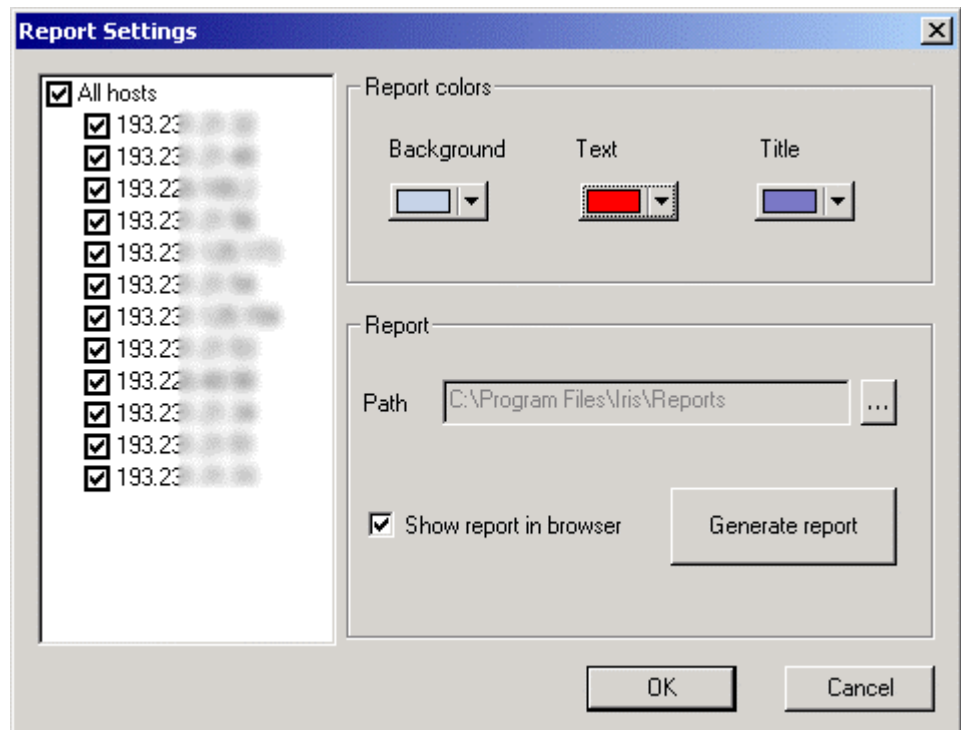
Network traffic reports can be created once the captured/loaded packets have been processed by the Decode engine.

A quick way to produce traffic reports for a specific IP is to click on the host entry in Hosts Activity Window.

See following fig:



If you want to produce reports for a group of hosts, click on Traffic Report toolbar button (or go to View | Traffic Report menu), check the desired hosts and click on Generate Report button.



How to customize reports

There are 3 colors that can be customized for generated reports: background color for tables, text color and Title color.

You can also select the folder where the report to be saved.

The default chart type is Pie, but this can also be modified by opening the Size Distribution chart, modifying the chart appearance and then saving the chart as ChartFX templates (no data) over the installed templ.chd file in Iris installation folder.

To modify the appearance of the chart, right click on chart items.

Note:

The list of ports that Iris will consider as being of interest (and are added to the Main Protocols Distribution section) can be customized by editing ports.ini file in Iris's installation folder.

Using Command Line Arguments



Command	Description
/autostart	Minimize program and start capturing upon loading.
/f: <filter filename>	Load a software filter file.
/?	Display command line argument.
/quiet	Iris will not show the eye icon in systray when minimized, and will reduce its screen messages. This option can be used with /autostart. To regain Iris's control, run Iris again.

Appendix A-Frequently Asked Questions



- What is the “Guard” feature?** Guard can watch over your office and alarm you when someone from the outside (or inside) tries to connect to your computers. Guard displays the date and time of the connection attempt, the victim and intruder IP addresses and DNS names and the port on which the connection attempt has been seen.
- If logging is turned on, the connection attempts will also be logged.
- What is the “Decode” feature?** Decode is the module which reconstructs captured TCP or UDP traffic transforming hundreds of hard to read binary packets into meaningful information showing you the E-mails, web pages, and ICQ sessions traveling on the wire.
- Who should use Iris?** Any organization that has a network should possess some type of traffic analyzer. Iris makes it simple enough so that even a non-technical employee can analyze the network traffic. Iris can also provide enough detail to satisfy the most meticulous Network Security Administrator. Iris can also be a valuable tool for any web developer.
- What differentiates Iris from other sniffers?** Unlike other network sniffers, Iris has advanced, integrated technology that allows it to reconstruct network traffic in a format that is simple to use and understand with a push of a button.
- There is no other sniffer that can show you the actual web page your employee is watching during work hours. Using Iris, you can increase the productivity by enforcing the Internet use policy.
- Iris’s user-friendly interface makes it easy to navigate and use.
- What are the main functionalities of Iris?** Iris utilizes and integrates the following advanced features and functionalities:
- Packet reconstruction
 - Packet manipulation/forging
 - Filter by Protocol Layer, keywords, MAC and IP address, TCP/UDP port, packets size and custom data
 - Logging network-wide foreign connection attempts
 - Reconstruction of common TCP protocols (reconstructs emails, web pages)
 - Logging “sniffed” packets
 - Logging reconstructed sessions

I have a firewall. Why should I get Iris?	Iris works in conjunction with your network firewall. If an attacker plots an intrusion against an organization's network, in most situations the firewall will inform the network administrator. However, the evidence of such an attack is incomplete and difficult to decipher. Iris will capture the evidence of network intrusions and literally reconstruct every keystroke and movement, saving your IT personnel valuable time.
What are the system requirements?	In order to install Iris, you should be running Windows 95/98/NT/2000, Internet Explorer 4.01 or higher, comctl32.dll version 5.00 or higher, and at least on a Pentium 166 processor with 32MB RAM and 1GB HDD.
How does Iris work?	Iris processes every packet that goes in or out of your network and thoroughly examines the critical information in order to obtain a precise picture of the activity occurring on the network in a format that is easy to understand.
What exactly is a sniffer?	Network traffic analyzing or "sniffing" is the process of monitoring network traffic. A packet sniffer is a wiretap device that plugs into computer networks and eavesdrops on the network traffic.
I'm on Token Ring network. Will Iris work?	No. We will add support for Token Ring in future versions.
I'm on a modem under Windows 2000. Will Iris work?	No. We will add support for dial-up under Windows 2000 in future versions. Iris works however with dial-up under Windows 9x and NT.
What types of logs does Iris generate?	Iris logs packets, reconstructed sessions, connection attempts and bandwidth utilization.
Can Iris create and send custom packets?	Yes, it can. Just pick the packet of your choice, modify its data and send it back to the wire.
I am seeing only my own packets! Why?	Because you are probably on a switch port. Try installing Iris on a hub port.

Appendix B – Networking Overview

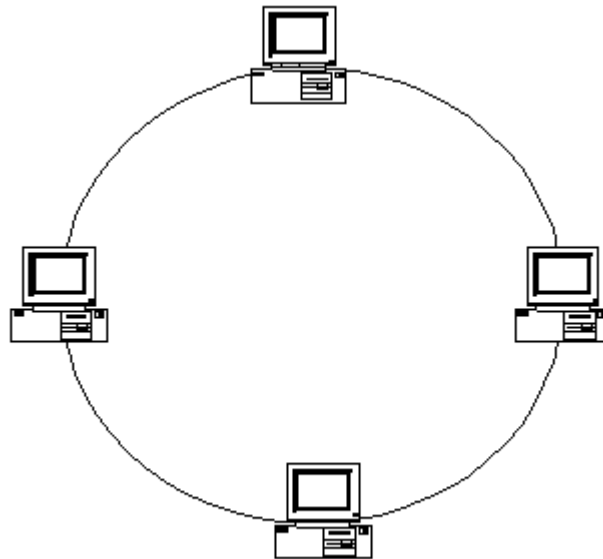


This section provides an overview of network topology. It will help you understand the technology behind sniffers and how they work. This understanding will help you utilize Iris on your network most effectively.

Network basics

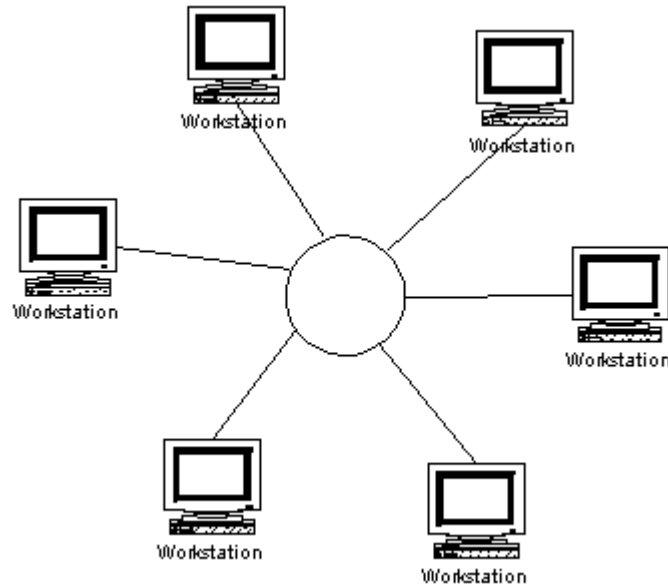
Networks can be considered logical maps of computers. There are a few basic logical topologies in network design: logical rings, logical stars, and horizontal.

Logical Ring Topology



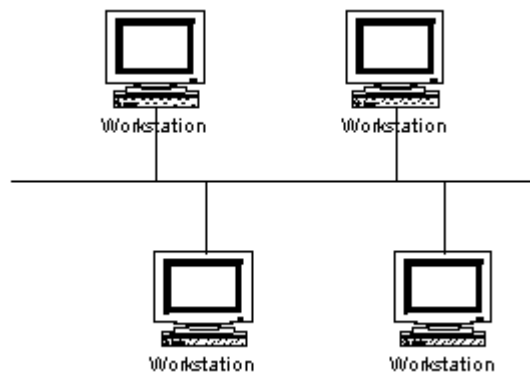
Network technologies like token ring utilize this type of technology. The ring topology requires that the ring remain unbroken, and that each computer on the network passes signals to its peers.

Logical Star Topology



The logical star topology has a central point of congregation for network traffic. All traffic to any node flows through a central point and is redirected to the intended node.

Horizontal Topology



A horizontal topology is distinguished by the use of a shared medium for all nodes. This type of topology is sometimes called a bus topology. Messages are broadcast on the medium with destination information and typically only the node the data is intended for responds. Ethernet is a horizontal Topology.

Ethernet

Ethernet is a Collision Detection, Multiple Access (CDMA) technology. This means that Ethernet enables multiple machines access to a single transmission medium (Multiple Access), and can handle more than one signal at a time (Collision Detection).

Since Ethernet is a Horizontal topology, it affords certain features that neither of the other topologies can. Due to the shared media principle of Horizontal Topology, all data destined to every node on a physical media is visible to all nodes.

Ethernet Segments:

A single shared media for Ethernet is commonly referred to as a segment. All computers sharing the same media are “on the same segment”.

Building an Ethernet based network usually involves the use of connectivity devices such as hubs, repeaters, bridges, switches, and routers.

Hub

A hub is a multiple access point for an Ethernet segment. Multiple nodes can connect to a single hub through its ports. Hubs can include 3 to 48 ports that can be chained together to create even larger networks. Even though this seems to resemble a logical star topology, it is in fact a logical horizontal topology. Hubs allow more than two computers to share the same segment. It does this by receiving signals from one port on a hub and sending them to all the other ports. All nodes on a hub are on the same segment.

Repeater

A repeater is a device intended to overcome distance limitations of Ethernet. It takes signals from one side of the repeater, amplifies them, and sends them out the other side.

Bridge

A bridge is similar to a repeater, except that it sometimes bridges can act as long haul extenders for an Ethernet network. You can use bridges to implement a building-to-building single network by bridging Ethernet over a fiber optic line, or by using an ADSL circuit.

Switch

A switch is similar in concept to a hub, except that it separates segments. Switches can create multiple segments and their software knows which segment to switch a packet to. Switches are often used to reduce segment size for a variety of reasons; smaller segment sizes typically imply fewer collisions per node. They also provide computers in a switched environment the ability to work at higher speeds due to fewer nodes sharing a segment.

Router

Routers are designed to move packets from one logical network to another. They act as gateways between the networks, allowing packets to travel back and forth across. Typically, routers operate at a higher network abstraction level than switches. For example, to get a packet from one network to a different network, a router is used. TCP/IP uses routers extensively to move traffic around the Internet.

Sniffer Theory

Most modern Ethernet cards have multiple modes of operation. In their normal mode, they look only at packets destined to their specific hardware address, or the address assigned to the “Broadcast address”. Broadcast Addresses are implemented so that data can be sent simultaneously to all nodes on the same segment. Promiscuous mode makes all packets on the segment visible and then can be picked up by the Ethernet card.

Sniffing usually entails putting the node's Ethernet card into promiscuous mode so that it can see all packets destined for all nodes on the segment. The sniffer then takes each of these packets, does some post processing, and displays them in a meaningful way to the end user.

Packet filtering

On an average network, a lot of data crosses that is not pertinent to anything you might be looking for. For that reason, sniffers typically allow you to limit the scope of packets that you are looking for. This allows you to focus on pertinent data and not drown in a deluge of extraneous packets. Packet filtering also has the added benefit of decreasing the amount of work a sniffer has to do to achieve specific results.

Packet filtering, for the most part, assumes that you understand a little bit about the underlying protocol. We recommend that you start with general filtering rules and continue to refine them until you get the desired data you are looking for.

Appendix C

Introduction to TCP/IP



Introduction

TCP/IP comprises a suite of protocols that allow computers to communicate with each other, regardless of operating system or vendor. TCP/IP was originally created as a research project and has grown to be the most widely used networking protocol today.

The Four Layers of TCP/IP

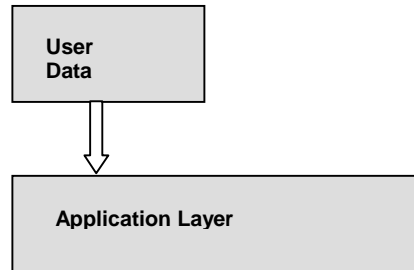
TCP/IP consists of four layers. In this section we will describe each layer, starting at the bottom:

Application
Transport
Network
Link

Layer	Description
Link Layer	The link layer includes the operating system device driver and the corresponding network interface card. The link layer is responsible for handling the hardware details of physically interfacing with the network.
Network Layer (Internet Layer)	The internet layer moves packets of data across the network from node to node.
Transport Layer	The transport layer provides a flow of data between two hosts for the Application Layer. Two different Transport protocols are used at this level.
Application Layer	This layer handles the details of the particular application being used. Some standard TCP/IP applications include: Telnet FTP SMTP SNMP

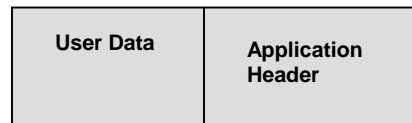
Encapsulation

When an application sends data using TCP, it is sent through each layer in the protocol stack. Each layer adds information to the data by adding a header and sometimes a footer. The data is then sent as a stream of bits across the network.

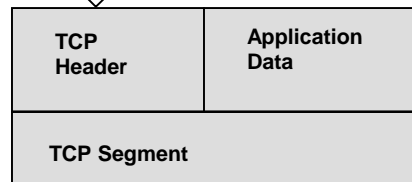


First, the user data is sent down through the application layer.

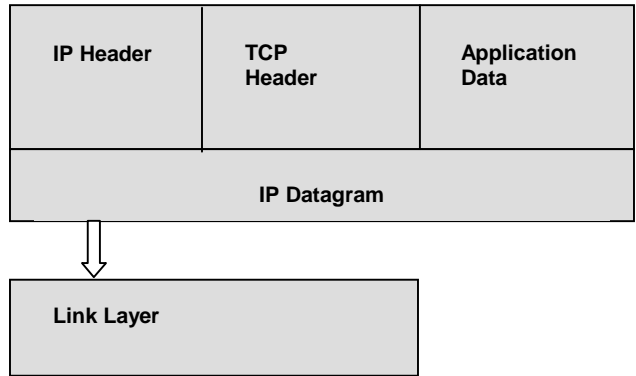
The application layer adds a header and the user data and application header are sent to the Transport Layer.



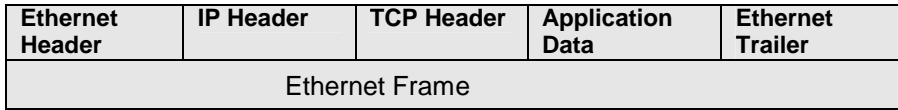
The Transport Layer adds on its own header, known as a TCP Segment. It is then passed to the Network Layer.



The network layer adds an IP Header, the IP Datagram. The datagram is then passed down to the Link Layer.



The link layer adds both an Ethernet Header and Trailer called an Ethernet Frame. The Ethernet frame is now ready to be sent across the network.



De-multiplexing

When a host receives an Ethernet frame, it moves through the protocol stack from the bottom up. Each layer looks at its respective header, strips that header, and decides what to do with the data before passing it up to the next layer

TCP/IP Networking Protocols

This section discusses the different TCP/IP networking protocols; Internet Protocol (IP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

Internet Protocol

The Internet Protocol (IP) is the dominant network layer protocol used by the TCP/IP suite of protocols. IP defines the rules for packaging network traffic into IP datagrams and also defines the rules for moving these datagrams across a network. IP is responsible for fragmenting data whenever necessary and reassembling the datagrams at the other end. The following diagram illustrates an IP header.

4-bit version	4-bit Header Length	8-bit Type of Service	16-bit Total Length (in bytes)			
16-bit Identification			0	D F	M F F	13-bit Fragment Offset
8-bit Time to Live		8-bit Pro to col		16-bit He ad er Ch ec ks um		
32-bit Destination Address						
32-bit Source Address						
Options (If any)						
Data						

Internet Protocol Packet Analysis

The following table shows the content of a packet.

IP Header		
1	Version:	4
2	Header Length:	20 bytes
3	Service Type:	0x00
4	Datagram Length:	40 bytes
5	Identification:	0x5850
6	Flags:	MF=off, DF=on
7	Fragment Offset:	0
8	TTL:	32
9	Encapsulated Protocol:	TCP
10	Header Checksum:	0x9658

11	Source IP Address:	172.16.10.2 (broken)
12	Destination IP Address:	172.16.10.5 (test bed)
13	Options:	
14	Data:	

IP Header Field Descriptions

Field Title	Description
Version	Indicates what version is being used; most commonly version 4.
Header Length	Indicates the header length.
Service Type	Indicates the level of service the datagram will be assigned.
Datagram Length	The length of the entire datagram including the header.
Identification	Uniquely identifies each datagram sent by a host
Flags	There are actually three flags but the first is unused. These flags control the way a datagram is fragmented. DF-Don't fragment. MF-More fragment
Fragment Offset	The fragment offset indicates how many units from the start of the original datagram the current datagram is
TTL (Time to Live)	Indicates how many routers a datagram may traverse before being dropped (max TTL is 255). A max is set to prevent datagrams from bouncing around the network forever if the host drops it.
Encapsulated Protocol	Identifies which protocol handed the IP to data
Header Checksum	A check on the IP header to ensure it is not corrupted
Source IP Address	32-bit address of originating host.
Destination IP Address	32-bit address of destination host.
Options	Currently defined options are security and handling restrictions, record route, timestamp, loose source routing, and strict source routing. These options are rarely used, as most routers cannot handle these options.
	The actual data being sent to the destination host.

Transmission Control Protocol

TCP is a transport layer protocol that a way to reliably connect hosts across a network. It creates a "virtual circuit" between the two hosts. Communicating hosts are required to acknowledge receipt of network traffic. TCP packages its data into segments that contain both data and session control information. Since segments traversing a network may arrive out of order, TCP uses sequence numbers to provide proper segment reassembly. The following ftp transfer tcpdump output demonstrate how the sequence numbers increment. Notice that with each packet the sequence number increases by 1460, the actual number of bytes being sent in each packet.

Packet 49 TCP: port ftp-data -> 26410 seq=1326731397 ack=1518678629 DATA: 1460 bytes
Packet 50 TCP: port ftp-data -> 26410 seq=1326732857 ack=1518678629 DATA: 1460 bytes
Packet 51 TCP: port ftp-data -> 26410 seq=1326734317 ack=1518678629 DATA: 1460 bytes
Packet 52 TCP: port ftp-data -> 26410 seq=1326735777 ack=1518678629 DATA: 1460 bytes

Before we can actually transfer data using TCP we have to establish a connection with a host. TCP uses a 3-way handshake to establish this connection. The handshake allows the originating host and destination host to properly set sequence numbers to ensure a reliable connection.

Before we examine the 3-way handshake works, let's look at sequence numbers. Since TCP uses a virtual (or full-duplex) connection it must have a means of reliably sending information in both directions simultaneously. Sequence numbers are use by both ends of a connection to properly order the data being sent.

3-way TCP handshake:

Host A (originating host) sends a SYN (synchronize) segment. This segment contains the port number the client wishes to connect to and the clients Initial Sequence Number (ISN).

Host A \longrightarrow Host B

SYN ISN = x

Host B responds with a SYN segment containing its own ISN.

Host B also acknowledges Host A's SYN with an ACK (acknowledge) segment. This segment will contain the originating hosts ISN plus one.

Host A \longleftarrow Host B

SYN ISN = y ACK ISN = x+1

Host A acknowledges Host B's SYN with an ACK segment. This segment will contain Host B's ISN plus one.

Host A \longrightarrow Host B

ACK ISN = y+1

At this point we have established a full-duplex connection and can start transferring data.

TCP Header Diagram

16-bit Source Port Number				16-bit Destination Port Number				
32-bit Sequence Number								
32-bit Acknowledgement Number								
4-bit Header Length	Reserved 6-bits	U R G	A C K	P S H	R S T	S Y N	F I N	16-bit Window Size
16-bit Checksum				16-bit Urgent Pointer				
Options (If Any)								
Data (If Any)								

Transmission Control Protocol - Packet Analysis

TCP Header		
1	Source Port:	22 (ssh)
2	Destination Port:	1714 (<unknown>)
3	Sequence Number:	1937534412
4	Acknowledgement Number:	0104479939
5	Header Length:	20 bytes (data=0)
6	Flags:	URG=off, ACK=on, PSH=off RST =off, SYN=off, FIN=off
7	Window Advertisement:	0
8	Checksum:	32
9	Urgent Pointer:	TCP
10	Options:	0x9658
11	Data:	172.16.10.2 (broken)

Description of TCP Header Fields

Field	Description
Source port number	16-bit source port number
Destination port number	16-bit destination port number
Sequence Number	4-byte number assigned by TCP starting with a randomly chosen number. This number is used to determine how many bytes have been transmitted across the network and to properly reassemble segments.
Acknowledgement Number	Acknowledges the last segment sent by the host.
Header Length	Measures the header length in 4-byte words
Flags	Used when negotiating and managing a connection: URG: Indicates segment being sent is urgent ACK: Indicates ack number in segment header is valid PSH: Pass the data to the application as soon as possible RST: Resets the connection SYN: Synchronize sequence numbers to initiate a connection FIN: The sender is finished sending data
Window Advertisement	The number of bytes the receiving host is willing to accept.
Checksum	A 16-bit checksum of the TCP Header and data.
Urgent Pointer	Used only if the URG flag is set
Options	The most commonly used option is the Maximum Segment Size (MSS) option. Determines the maximum size segment the sender is willing to receive.
Data	This portion of the segment is optional. When connections are being established or terminated, no data is sent

User Datagram Protocol

UDP is also a transport layer protocol. Unlike TCP, UDP is a connectionless Protocol and does not have the benefit of error detection, error correction, handshaking, or delivery verification. As a result, UDP has low overhead. UDP is generally not used in applications where error free data transfer is mandatory.

16-bit Source Port Number	16-bit Destination Port Number
16-bit UDP Length	16-bit UDP Checksum
Data (If Any)	

User Datagram Protocol - Packet Analysis

1	Source Port:	2167 (<unknown>)
2	Destination Port:	53 (domain)
3	Datagram Length:	37 bytes (Header=8, Data=29)
4	Checksum:	0xD5B0
5	Data:	

UDP Header Field Description

Field	Description
1	16-bit source port number
2	16-bit destination port number
3	Indicates the length of the length of entire UDP datagram, including header
4	16-Bit UDP Checksum. A checksum of the entire UDP datagram
5	1Data payload

Appendix D—Glossary



A	Acceptable Use Policy	Policies that restrict how a network may be used.
	Access Control List	An Access Control List is the usual means by which access to, and denial of, services is controlled. It is a list of the services available along with a list of the hosts permitted to use each service.
	Adapter	The hardware component of the network architecture, often a card in your computer.
	Address	There are three types of addresses in common use within the Internet. They are email addresses, internet (IP) or Internet addresses; and network interface card (NIC) hardware or MAC addresses.
	Address Mask	A bit mask used to identify which bits in an IP address correspond to the network and subnet portions of the address. This mask is often referred to as the subnet mask because the network portion of the address can be determined by the encoding inherent in an IP address.
	Address Resolution	Conversion of an Internet address to the corresponding Domain Name.
	Administrative Domain	A collection of hosts, routers, and the interconnecting network(s), managed by a single administrative authority.
	Agent	In the client-server model, the part of the system that performs information preparation and exchange on behalf of a client or server application.
	Alias	A name, usually short and easy to remember, that is translated into another name, usually longer and more difficult to remember.
	All Multicast	Collects all multicast packets.
	Anonymous FTP	Anonymous FTP allows a user to retrieve documents, files, programs, and other archived data from anywhere on the Internet without having to establish a user id and password. By using the special user id of "anonymous" the network user will bypass local security checks and will have access to publicly accessible files on a remote system.
	ANSI	American National Standards Institute. This organization is responsible for approving U.S. standards in many areas, including computers and communications. Standards approved by this organization are often called ANSI standards. For example, ANSI C is the version of the C language approved by ANSI. ANSI is a member of the International Standards Organization (ISO).
	Appletalk	A networking protocol developed by Apple Computer for communication between Apple Computer products and other computers. This protocol is independent of the network layer on which it is run. Current implementations exist for Localtalk, a 235Kb/s local area network and Ethertalk, a 10Mb/s local area network.
	Application Program Interface (API)	An API is a set of calling conventions that define how a service is invoked through a software package.
	Application	A program that performs a function directly for users. FTP, mail and Telnet clients are examples of network applications.

Application Layer	The top layer of the network protocol stack. The application layer is concerned with the semantics of work, for example formatting electronic mail messages. How to represent that data and how to reach the foreign node are issues for lower layers of the network.
ARP	Address Resolution Protocol. Used to dynamically discover the low-level physical network hardware address that corresponds to the high level IP address for a given host. ARP is limited to physical network systems that support broadcast packets that can be heard by all hosts on the network. It is defined in RFC 826.
ARPANET	Advanced Research Projects Agency Network. A pioneering long haul network funded by ARPA (now DARPA). It served as the basis for early networking research, as well as a central backbone during the development of the Internet. The ARPANET consisted of individual packet switching computers interconnected by leased lines.
ASCII	American Standard Code for Information Interchange. A standard character-to-number encoding widely used in the computer industry.
ATM	Asynchronous Transfer Mode. A method for the dynamic allocation of bandwidth using a fixed-size packet (cell). ATM is also known as "fast packet."
Authentication	The verification of the identity of a person or process.
Autorun	Starts Iris automatically when Windows starts, allowing a packet-log to occur as soon as the network card becomes active.
B Backbone	The primary connectivity mechanism of a hierarchical distributed system. All systems that can connect to an intermediate system on the backbone are assured of connecting to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.
Bandwidth	Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit.
BIND	Berkeley Internet Name Domain. Implementation of a DNS server developed and distributed by the University of California at Berkeley. BIND provides an automatic means of hostname to IP address resolution.
BOOTP	The Bootstrap Protocol, described in RFCs 951 and 1084, is used for booting diskless nodes. See also: RARP.
Bridge	A device that connects two or more physical networks and forwards packets across them. Bridges can usually be configured to filter packets, that is, to forward only certain traffic. Related devices are repeaters that simply forward electrical signals from one cable to another and full-fledged routers that make routing decisions based on several criteria.
Broadband	A transmission medium capable of supporting a wide range of frequencies. It can carry multiple signals by dividing the total capacity of the medium into multiple, independent bandwidth channels, where each channel operates only on a specific range of frequencies.
Broadcast	A special type of multicast packet that all nodes on the network are always willing to receive. This filter allows all packets addressed to the hardware broadcast address to be seen within Iris.
Broadcast Storm	An incorrect packet broadcast onto a network that causes multiple hosts to respond all at once, typically with equally incorrect packets that causes the storm to grow exponentially in severity.

	Brouter	A device that bridges some packets (forwards them based on data link layer information) and routes other packets (forwards them based on network layer information). The bridge/route decision is based on configuration information.
C	Capture	The Capture utility reads packets from the physical adapter.
	CERT	The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise. It is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
	Checksum	A computed value that is dependent upon the contents of a packet. This value is sent along with the packet when it is transmitted. The receiving system computes a new checksum based upon the received data and compares this value with the one sent with the packet. If the two values are the same, the receiver has a high degree of confidence that the data was received correctly.
	Circuit Switching	A communications paradigm in which a dedicated communication path is established between two hosts, and on which all packets travel. The telephone system is an example of a circuit switched network. See also: Connection-Oriented, Connectionless, Packet Switching.
	Client	A computer system or process that requests a service from another computer system or process. A workstation requesting the contents of a file from a file server is a client of the file server. See also: Client-Server Model, Server.
	Client-Server Model	A common way to describe the paradigm of many network protocols. Examples include the name-server/name-resolver relationship in DNS and the file-server/file-client relationship in NFS. See also: Client, Server.
	Congestion	Congestion occurs when the offered load exceeds the capacity (or bandwidth) of a data communication path.
	Connection-Oriented	The data communication method in which communication proceeds through three well-defined phases: connection establishment, data transfer, and connection release. TCP is a connection-oriented protocol.
	Connectionless	The data communication method in which communication occurs between hosts with no previous initialization See UDP.
	Cracker	A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system.
	Cyberspace	A term coined by William Gibson in his fantasy novel <i>Necromancer</i> to describe the "world" of computers, and the society that gathers around them.
D	Daisy Chain	A local networking topology in which a single cable connects multiple workstations. This tends to be less expensive than the alternative "star" topology, but is also less robust. A break anywhere along the "chain" will disable the entire local network. Daisy chains are most often used in PhoneNet or thinnet cabling.
	DARPA	Defense Advanced Research Projects Agency. An agency of the U.S. Department of Defense responsible for the development of new technology for use by the military. DARPA (formerly known as ARPA) was responsible for funding much of the development of the Internet we know today, including the Berkeley version of Unix and TCP/IP.
	Data Encryption Standard (DES)	DES is a popular, standard encryption scheme. Developed by IBM in the 1970's, DES uses a 56-bit encryption key and was originally designed to run in hardware.

Datagram	A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.
Decode	Condensing information in streams of packets to a viewable display defined for various services. For example, 25 is generally SMTP, 80 is generally HTTP.
Default Route	A routing table entry that is used to direct packets addressed to networks not explicitly listed in the routing table.
DES	See: Data Encryption Standard
Dialup	A temporary, as opposed to dedicated, connection between computers established over a standard phone line.
Directed	The hardware adapter will only read packets directly sent to it.
Distributed Database	A collection of several different data repositories that looks like a single database to the user. A prime example in the Internet is the Domain Name System.
DNS	See: Domain Name System
Domain Name System (DNS)	The DNS is a general purpose distributed, replicated, data query service. Its principal use is looking up host IP addresses based on host names. Some important domains are: .COM (commercial), .EDU (educational), .NET (network operations), .GOV (U.S. government), and .MIL (U.S. military). Most countries also have a domain. For example, .US (United States), .UK (United Kingdom), .AU (Australia). It is defined in std 13, RFCs 1034 and 1035. See also: Fully Qualified Domain Name.
Domain	In the Internet, a domain is part of a naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots).
DoS (Denial of Service)	A DoS attack is a remote attack against a servers TCP/IP stack or services. DoS attacks can saturate a server's bandwidth, saturate all available connections for a particular service, or even crash a server.
Dot Address (dotted decimal notation)	Dot address refers to the common notation for IP addresses of the form A.B.C.D; where each letter represents, in decimal, one byte of a four-byte IP address.
E Electronic Frontier Foundation (EFF)	A foundation established to address social and legal issues arising from the impact on society of the increasingly pervasive use of computers as a means of communication and information distribution.
Electronic Mail (E-mail)	A system in which a computer user exchanges messages with other computer users (or groups of users) across a communications network. E-mail is one of the most popular uses of the Internet.
E-mail Address	The domain-based or UUCP address that is used to send E-mail to a specified destination.
Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Also called tunneling, especially in reference to Novell's IPX protocol.

Encryption	Encryption is the manipulation of packet data in order to prevent any but the intended recipient from reading that data. There are many types of data encryption that are the basis of network security. See also: Data Encryption Standard.
Ethernet	A computer network cabling system designed by Xerox in the late 1970s. Originally, Ethernet ran at three megabits per second (mps) over a thick coaxial cable. Current Ethernet runs at 10mps over fiber, twisted-pair, and several coaxial cable types.
Ethernet Card	A physical device that allows a computer to physically interface to an Ethernet-based network. Also known as Network Interface Card (NIC).
EtherTalk	Networking protocol used by Apple equipment connected directly to Ethernet. Apple equipment on PhoneNet uses LocalTalk.
F	
FAQ	Frequently Asked Questions.
FDDI	Fiber Distributed Data Interface, a high-speed (100Mb/s) LAN standard. The underlying medium is fiberoptics, and the topology is a dual-attached, counter- rotating token ring.
File Transfer	Copying a file from one computer to another over a computer network.
Filter	A set of criteria that allows you to narrow your search for more specific results.
Finger	A standard TCP/IP program for gaining access to user information. "Finger user@hostname" might yield the user's full name, time last logged in, telephone number, and other user-definable information. Frequently used by an attacker to gain information on a remote server.
Firewall	A firewall restricts access to certain parts of a network or a whole network. Firewalls are typically found in a corporate environment where employees are on one side of the firewall and the Internet is on the other side, therefore the firewall creates a protective wall between the two.
For Your Information (FYI)	See FYI.
FQDN	See: Fully Qualified Domain Name.
Fragment	A portion of a packet. When a router is forwarding an IP packet to a network that has a maximum packet size larger than the allowable packet size, it is forced to break up that packet into multiple fragments. The IP layer reassembles these fragments at the destination host.
Frame	A frame is a data link layer "packet" that contains the header and trailer information required by the physical medium. That is, network layer packets are encapsulated to become frames.
FTP	File Transfer Protocol. A protocol that allows a user on one host to access and transfer files to and from another host over a network. Also, FTP is usually the name of the program the user invokes to execute the protocol.
FYI	For Your Information. A sub-series of RFCs that are not technical standards or descriptions of protocols. FYIs convey general information about topics related to TCP/IP or the Internet.
Fully Qualified Domain Name (FQDN)	The FQDN is the full name of a system, rather than just its hostname. For example, "brick" is a hostname and "brick.eeye.com" is an FQDN.

G	Gateway	The original Internet term for what is now called a router or more precisely, IP router. In modern usage, the terms "gateway" and "application gateway" refer to systems that do translation from some native format to another.
	Guard	A watchdog that interprets connection requests and displays any unauthorized attempts to connect.
H	Hacker	A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term. See also: Cracker.
	Hardware Filters	Hardware Filters are directly applied to the MAC layer of the listening network card. They are somewhat limited in function by the underlying card, but most modern cards support all of the supplied filter modes. The most used filter is Promiscuous. It instructs the network card to send all the packets it sees.
	Header	The portion of a packet, preceding the actual data. It contains source and destination addresses, error checking, and other fields. A header is also the part of an E-mail message that precedes the body of a message and contains, among other things, the message originator, date and time.
	Heterogeneous Network	A network running multiple network layer protocols, operating systems, and vendor implementations.
	Hierarchical Routing	The complex problem of routing on large networks can be simplified by reducing the size of the networks. This is accomplished by breaking a network into a hierarchy of networks, where each level is responsible for its own routing. The Internet has, three levels: the backbones, the midlevels, and the stub networks. The backbones know how to route between the midlevels. The midlevels know how to route between the sites. Each site (being an autonomous system) knows how to route internally.
	Hop	A term used in routing. A path to a destination on a network is a series of hops, through routers, away from the origin.
	Host	A node on the network. Usually refers to a computer that both initiates and accepts network connections.
	Host Address	See: Internet Address.
	Hostname	The name assigned to a machine. See also: Fully Qualified Domain Name.
	HTTP	Hypertext Transfer Protocol is used for serving web pages across the Internet.
	Hub	A device connected to several other devices. In ARCnet, a hub is used to connect several computers together. In a message handling service, a hub is used for transferring messages across the network.
I	ICMP	Internet Control Message Protocol.
	IEEE	Institute of Electrical and Electronics Engineers
	IETF	See: Internet Engineering Task Force.
	Import Trace File	Imports a packet buffer created in a different sniffing product for analysis within Iris.
	Interior Gateway Protocol (IGP)	An Internet protocol that distributes routing information to the routers within an autonomous system. The term gateway is historical. Router is currently the preferred term.

International Organization for Standardization (ISO)	A voluntary, non-treaty organization founded in 1946 that is responsible for creating international standards in many fields, including computers and communications. Its members are the national standards organizations of the 89 member countries, including ANSI for the U.S. See also: ANSI, Open Systems Interconnection.
Internet (note the capital "I")	The largest internet in the world consisting of large national backbone nets (such as MILNET, NSFNET, and CREN) as well as regional and local campus networks all over the world. The Internet uses the Internet protocol suite. To be on the Internet you must have IP connectivity, that is, be able to Telnet to, or ping, other systems. Networks with only E-mail connectivity are not actually classified as being on the Internet.
Internet address	A 32-bit address assigned to hosts using TCP/IP.
Internet Assigned Numbers Authority (IANA)	The central registry for various Internet protocol parameters, such as port, protocol and enterprise numbers, and options, codes and types.
Internet Engineering Task Force (IETF)	The IETF is a large, open community of network designers, operators, vendors, and researchers whose purpose is to coordinate the operation, management and evolution of the Internet, and to resolve short-range and mid-range protocol and architectural issues. It is a major source of proposals for protocol standards that are submitted to the IAB for final approval. The IETF meets three times a year and extensive minutes are included in the IETF Proceedings.
Internet Protocol (IP)	The Internet Protocol, defined in STD 5, RFC 791, is the network layer for the TCP/IP Protocol Suite. It is a connectionless, best-effort packet switching protocol. See also: Packet Switching, Request For Comments, TCP/IP Protocol Suite.
Internet Registry (IR)	The Internet Assigned Numbers Authority has the discretionary authority to delegate portions of its responsibility and, with respect to network address and Autonomous System identifiers, has lodged this responsibility with the IR. The IR function is performed by the Defense Data Network Network Information Center.
Internet Relay Chat (IRC)	A worldwide "party line" protocol that allows computer users to converse with each other in real time. IRC is structured as a network of servers, each of which accepts connections from client programs, one per user. See also: Talk.
internet	A collection of networks interconnected by a set of routers that allow them to function as a single, large, virtual network.
Internet-Draft (I-D)	Internet-Drafts are working documents of the IETF, its Areas, and its Working Groups. As the name implies, Internet-Drafts are draft documents. They are valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time. Very often, I-Ds are precursors to RFCs. See also: Internet Engineering Task Force, RFC.
Interoperability	The ability of software and hardware on multiple machines from multiple vendors to communicate meaningfully.
IP	See: Internet Protocol.
IP Address	The 32-bit address defined by the Internet Protocol in STD 5, RFC 791. It is usually represented in dotted decimal notation and is a unique number used to identify a specific computer (for example, 192.168.1.1). An IP address provides a network mapping to a computer. Think of an IP address as your computer's street address.
IP Datagram	See: Datagram.

IPX (Internetwork Packet exchange)	Novell's proprietary protocol used by Netware. A router with IPX routing can interconnect LANs so that Novell Netware clients and servers can communicate. See also: Local Area Network.
IRC	See: Internet Relay Chat.
ISDN	Integrated Services Digital Network. An emerging technology that is beginning to be offered by telephone carriers. ISDN combines voice and digital network services in a single medium making it possible to offer customers digital data services as well as voice connections through a single "wire."
ISO	See: International Organization for Standardization.
K Kerberos	Kerberos is the security system of MIT's Project Athena. It is based on symmetric key cryptography. See also: Encryption.
L LAN	See: Local Area Network
Later 3+	This offers a number of IP-specific protocols at layer 3 or higher to filter on.
Layer	Communication networks for computers may be organized as a set of more or less independent protocols, each in a different layer (also called level). The lowest layer governs direct host-to-host communication between the hardware at different hosts; the highest consisting of user applications. Each layer builds on the layer beneath it. For each layer, programs at different hosts use protocols appropriate to the layer to communicate with each other. TCP/IP has five layers of protocols; OSI has seven. The advantages of different layers of protocols is that the methods of passing information from one layer to another are specified clearly as part of the protocol suite, and changes within a protocol layer are prevented from affecting the other layers. This greatly simplifies the task of designing and maintaining communication programs. See also: Open Systems Interconnection, TCP/IP Protocol Suite.
Layer Two	This offers a variety of layer-two protocols to filter on.
Listserv	An automated mailing list distribution system.
Local Area Network (LAN)	A data network intended to serve an area of only a few square kilometers or less. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit data rates up to 100Mb/s. See also: Ethernet, Fiber Distributed Data Interface, Token Ring, Wide Area Network.
LocalTalk	Networking protocol used by Macintosh computers to communicate over PhoneNet.
Logs	Files containing output in varying degrees of detail.
Loopback	The loopback device is a simulated TCP/IP adapter. If you don't have a loopback device and you're not connected to a LAN/provider, you can't run TCP/IP software.
M MAC Address	The physical hardware address of a device connected to shared media. This filter class allows you to filter based on specific hardware layer addresses. It is helpful for monitoring specific packets originating or destined for specific hardware adapters.
Mail Gateway	A machine that connects two or more E-mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be quite complex, and generally it requires a store-and-forward scheme whereby the message is received from one system in its entirety before it is translated and transmitted to the next system.
Mail Server	A software program that distributes files or information in response to requests sent by E-mail.

Mailing List	A list of E-mail addresses, used by a mail exploder, to forward messages to groups of people. Generally, a mailing list is used to discuss certain set of topics, and different mailing lists discuss different topics. A mailing list may be moderated. This means that messages sent to the list are actually sent to a moderator who determines whether or not to send the messages on to everyone else.
MAN	See: Metropolitan Area Network.
Management Information Base (MIB)	The set of parameters an SNMP management station can query or set in the SNMP agent of a network device, for example a router. Standard, minimal MIBs have been defined, and vendors often have Private enterprise MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. See also: Client-Server Model, Simple Network Management Protocol.
Maximum Transmission Unit (MTU)	The largest frame length that may be sent on a physical medium, usually 1514 bytes on Ethernet medium. See also: Fragment, Frame.
MDF	Main Distribution Frame. The main "telecommunications closet" in a building.
Memory Allocated	A read-only gauge that displays how much memory Iris is currently using.
Metropolitan Area Network (MAN)	A data network intended to serve an area approximating that of a large city. Such networks are being implemented by techniques such as running fiber cables through subway tunnels. A popular example of a MAN is SMDS. See also: Local Area Network, Switched Multimegabit Data Service, Wide Area Network.
MIB	See: Management Information Base.
Mid-level network	Mid-level networks, also known as regionals, make up the second level of the Internet hierarchy. These are the transit networks that connect the stub networks to the backbone networks. See also: Backbone, Internet.
MIME	See: Multipurpose Internet Mail Extensions.
Modem	A device used to permit computers and terminals to communicate over telephone lines.
Moderator	A person, or small group of people, who manage moderated mailing lists and newsgroups. Moderators are responsible for determining which E-mail submissions are passed on to list. See also: Electronic Mail, Mailing List, Usenet.
MTU	See: Maximum Transmission Unit.
Multicast	A packet with a special destination address that multiple nodes on the network may be willing to receive. See also: Broadcast.
Multihomed Host	A host that has more than one connection to a network. The host may send and receive data over any of the links but will not route traffic for other nodes.
Multiport Repeater	An Ethernet device, typically with 8 thinnet ports and one transceiver cable port.
Multipurpose Internet Mail Extensions (MIME)	An extension to Internet email that provides the ability to transfer non-textual data, such as graphics, audio and fax. It is defined in RFC 1341. See also: Electronic Mail.
MX Record	Mail Exchange Record. A DNS resource record type indicating which host can handle mail for a particular domain. See also: Domain Name System, Electronic Mail.
N	
Name Resolution	The process of mapping a Hostname into the corresponding IP address. See DNS.
Name Server	A host that maps Hostnames into IP addresses.

Namespace	A commonly distributed set of names in which every name is unique.
National Institute of Standards and Technology (NIST)	United States governmental body that provides assistance in developing standards, formerly the National Bureau of Standards.
National Science Foundation (NSF)	A U.S. government agency whose purpose is to promote the advancement of science. NSF funds science researchers, scientific projects, and infrastructure to improve the quality of scientific research. The NSFNET, funded by NSF, is an essential part of academic and research communications. It is a high speed "network of networks" that is hierarchical in nature. At the highest level, it is a backbone network currently comprising 16 nodes connected to a 45Mb/s facility that spans the continental United States. Attached to that are mid-level networks and attached to the mid-levels are campus and local networks. NSFNET also has connections out of the U.S. to Canada, Mexico, Europe, and the Pacific Rim. The NSFNET is part of the Internet.
NetBIOS	Network BIOS (Basic Input Output System). The standard interface to networks on IBM PC and compatible systems. NetBIOS, in its basic form, is used for conducting file and printing sharing across a windows network. and print sharing across a Windows network.
Network Time Protocol (NTP)	A protocol that assures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
Network	A computer network is a data communications system that interconnects computer systems at various different sites. A network may be composed of any combination of LANs, MANs or WANs.
Network Address	The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique. See also: Internet, IP Address, Subnet Address, Host Address, Internet Registry.
Network Layer 2 and 3	This filter class allows the user to filter at higher layers in the OSI networking model.
New Capture	Initiates a new session and asks if you want to discard old data (the current packet buffer) or save it.
NFS	Network File System. A protocol developed by Sun Microsystems, and defined in RFC 1094, that allows a computer system to access files over a network as if they were on its local disks. This protocol has been incorporated in products by more than two hundred companies, and is now a de facto Internet standard.
NIC	Network Information Center. A NIC provides information, assistance and services to network users. See also: NOC.
NIC.DDN.MIL	This is the domain name of the DDN NIC. See also: Domain Name System, Network Information Center.
NIS	Network Information Services. A set of services, generally provided by a NIC, to assist users in using the network. See also: Network Information Center.
NIST	See: National Institute of Standards and Technology.
NNTP	Network News Transfer Protocol. A protocol, defined in RFC 977, for the distribution, inquiry, retrieval, and posting of news articles. See also: Usenet.

NOC	Network Operations Center. A location from which the operation of a network or internet is monitored. Additionally, this center usually serves as a clearinghouse for connectivity problems and efforts to resolve those problems. See also: NIC.
Node	An addressable device attached to a computer network. See also: Host, Router.
NSF	See: National Science Foundation.
NSFNet	The National Science Foundation Network. A collection of local, regional, and mid-level networks in the U.S. tied together by a high-speed backbone. NSFNET provides scientists access to a number of supercomputers across the country.
NTP	See: Network Time Protocol.
O Octet	An octet is 8 bits. This term is used in networking, rather than byte, because some systems have bytes that are not 8 bits long.
Open	Opens an existing packet buffer file for examination.
Open and append	Opens a saved packet buffer file and attaches it onto the end of the current open packet buffer.
Open Shortest-Path First Interior Gateway Protocol (OSPF)	A link state, as opposed to distance vector, routing protocol. It is an Internet standard IGP defined in RFC 1247. See also: Interior Gateway Protocol, Routing Information Protocol.
Open Systems Interconnection (OSI)	A suite of protocols, designed by ISO committees, to be the international standard computer network architecture. See also: International Organization for Standardization.
OSI Layer 1	Physical layer. The layer that provides the means to activate and use physical connections for bit transmission. In plain terms, the Physical Layer provides the procedures for transferring a single bit across a Physical Media.
OSI Layer 2	Data Link Layer. This layer handles the movement and routing of packets around a network.
OSI Layer 3	Network Layer. The layer that is responsible for routing, switching, and sub network access across the entire OSI environment.
OSI Layer 4	Transport Layer. The layer responsible for reliable end-to-end data transfer between end systems.
OSI Layer 5	Session Layer. The layer that provides means for dialogue control between end systems.
OSI Layer 6	Presentation Layer. The layer that determines how Application information is represented (encoded) while in transit between two end systems.
OSI Layer 7	Application Layer. The top-most layer of the OSI Model. Provides such communication services as electronic mail and file transfer.
OSI Reference Model	A seven-layer structure designed to describe computer network architectures and the way that data passes through them. This model was developed by the ISO in 1978 to clearly define the interfaces in multi-vendor networks, and to provide users of those networks with conceptual guidelines in the construction of such networks. See also: International Organization for Standardization.
OSPF	See: Open Shortest-Path First Interior Gateway Protocol.

P

Packet Switch Node (PSN)	A dedicated computer whose purpose is to accept, route and forward packets in a packet switched network. See also: Packet Switching, Router.
Packet	The unit of data sent across a network. "Packet" is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units. See also: Datagram, Frame.
Packet Buffer	A temporary holding spot in memory for a group of packets.
Packet Buffer Size	The maximum number of packets kept in a temporary buffer. Increasing this number allows more packets to be handled directly, but also increases memory requirements. After packets fill a buffer, they are filed to disk.
Packet Switch Node (PSN)	A dedicated computer whose purpose is to accept, route and forward packets in a packet-switching network.
Packet Switching	A communications paradigm in which packets (messages) are individually routed between hosts, with no previously established communication path. See also: Circuit Switching, Connection- Oriented, Connectionless.
Physical Media	Any means in the physical world for transferring signals between OSI systems. Considered to be outside the OSI Reference Model, and therefore sometimes referred to as "Layer 0." The physical connector to the media can be considered as defining the bottom interface of the Physical Layer, that is the bottom of the OSI Reference Model.
PING	Packet Internet Groper. A program used to test reach ability of destinations by sending them an ICMP echo request and waiting for a reply.
Point Of Presence (POP)	A site where there exists a collection of telecommunications equipment, usually digital leased lines and multi-protocol routers.
POP3	Post Office Protocol 3 is used for receiving E-mail.
Point-to-Point Protocol (PPP)	The Point-to-Point Protocol, defined in RFC 1171, provides a method for transmitting packets over serial point-to-point links. See also: Serial Line IP.
POP	See: Post Office Protocol and Point Of Presence.
POP3	Post Office Protocol 3 is used for receiving E-mail.
Port	In the network environment, a port is the pathway that a computer uses to transmit and receive data. It is the end point of a socket connection.
Post Office Protocol (POP)	A protocol designed to allow single user hosts to read mail from a server. There are three versions: POP, POP2, and POP3. Latter versions are NOT compatible with earlier versions. See also: E-mail.
Postmaster	The person responsible for taking care of email problems, answering queries about users, and other related work at a site.
PPP	See: Point-to-Point Protocol.
Privacy Enhanced Mail (PEM)	Internet E-mail that provides confidentiality, authentication and message integrity using various encryption methods.
Promiscuous	This filter allows the adapter to see all traffic on the wire. It is the default and broadest filter available in this class. If Promiscuous is selected, no other hardware filters can be selected.
Protocol	A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces, such as the order in which bits and bytes are sent across a wire, or high-level exchanges between allocation programs, for example the way in which two programs transfer a file across the Internet.

Protocol Converter	A device/program that translates between different protocols that serve similar functions, for example TCP and TP4.
Protocol Stack	A layered set of protocols that work together to provide a set of network functions. See also: Layer, Protocol.
Proxy	Form of security on the Internet. When you use a proxy or proxy server, you send a request to a server on the Internet from this proxy. For the server on the Internet it looks like the request is coming from the proxy, not from your machine.
Proxy ARP	The technique in which one machine, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP allows a site to use a single IP address with two physical networks. See also: Address Resolution Protocol.
PSN	See: Packet Switch Node.
Queue	A backlog of packets or connections waiting to be processed.
RARP	Reverse Address Resolution Protocol. A protocol, defined in RFC 903, that provides the reverse function of ARP. RARP maps a hardware (MAC) address to an internet address. Primarily diskless nodes use it when they first initialize to find their internet address. See also: Address Resolution Protocol, BOOTP, internet address, MAC address.
RBOC	Regional Bell Operating Company.
Reassembly	The IP process in which a previously fragmented packet is reassembled before being passed to the transport layer. See also: Fragment.
Remote Procedure Call (RPC)	An easy and popular paradigm for implementing the client-server model of distributed computing. Generally a request is sent to a remote system to execute a designated procedure using arguments supplied, and the result returned to the caller. There are many variations and subtleties in various implementations, resulting in a variety of different (incompatible) RPC protocols.
Remote Login	Operating on a remote computer, using a protocol over a computer network, as though locally attached. See also: Telnet.
Repeater	A device that propagates electrical signals from one cable to another without making routing decisions or providing packet filtering. In OSI terminology, a repeater is a Physical Layer intermediate system. See also: Bridge, Router.
RFC	Request For Comments. The document series, begun in 1969, that describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs. The RFC series of documents is unusual in that the proposed protocols are forwarded by the Internet research and development community, acting on their own behalf, as opposed to the formally reviewed and standardized protocols that are promoted by organizations such as CCITT and ANSI. See also: For Your Information, STD.
Route	The path that network traffic takes from its source to its destination. Also, a possible path from a given host to another host or destination.
Router	A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as "routing metrics." In OSI terminology, a router is a Network Layer intermediate system. See also: Gateway, Bridge, Repeater.

Routing	The process of selecting the correct interface and next hop for a packet being forwarded. See also: Router.
Routing domain	A set of routers exchanging routing information within an administrative domain.
Routing Information Protocol (RIP)	A distance vector, as opposed to link state, routing protocol. RIP is an Internet standard Interior Gateway Protocol defined in STD 34, RFC 1058 and updated by RFC 1388.
RPC	See: Remote Procedure Call.
Serial Line IP (SLIP)	A protocol used to run IP over serial lines, such as telephone circuits or RS-232 cables, interconnecting two systems. SLIP is defined in RFC 1055. See also: PPP.
S	
Server	A provider of resources (e.g., file servers and name servers). See also: Client, DNS, NFS.
Service	A program running on a remote machine that provides a service. For example, when you visit a website the remote server displays a web page via its web server service.
SLIP	See: Serial Line IP.
SMTP	Simple Mail Transfer Protocol. A protocol, defined in STD 10, RFC 821, used to transfer electronic mail between computers. It is a server-to-server protocol, so other protocols are used to access the messages.
SNA	Systems Network Architecture. A proprietary networking architecture used by IBM and IBM-compatible mainframe computers.
SNMP	Simple Network Management Protocol. The Internet standard protocol, defined in STD 15, RFC 1157, developed to manage nodes on an IP network. It is currently possible to manage devices such as wiring hubs, toasters, or jukeboxes.
SQL	Structured Query Language. The international standard language for defining and accessing relational databases. For example, Metaphor uses SQL to communicate with Sybase and other databases on remote systems.
STD	A subseries of Request For Comments (RFC) that specify Internet standards. The official list of Internet standards is STD 1.
Stream-Oriented	A type of transport service that allows its client to send data in a continuous stream. The transport service will guarantee that all data will be delivered to the other end in the same order as sent and without duplicates.
Structure of Management Information (SMI)	The rules used to define the objects that can be accessed via a network management protocol. This protocol is defined in STD 16, RFC 1155. See also: MIB.
Subnet	A portion of a network that may be a physically independent network segment. It shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internet. See also: Internet.
Subnet Address	The subnet portion of an IP address. In a subnet network, the host portion of an IP address is split into a subnet portion and a host portion using an address (subnet) mask. See also: Address Mask, IP Address, Network Address, Host Address.
Subnet Mask	An IP address used in configuring a system. It shows which part of the address is actually the subnet number, for routing purposes, for example: 255.255.0.0.
Switched Multimegabit Data Service (SMDS)	An emerging high-speed datagram-based public data network service developed by Bellcore and expected to be widely used by telephone companies as the basis for their data networks. See also Metropolitan Area

T	Service (SMDS)	Network.
	T1	An AT&T term for a digital carrier facility used to transmit a DS-1 formatted digital signal at 1.544 megabits per second.
	T3	A term for a digital carrier facility used to transmit a DS-3 formatted digital signal at 44.746 megabits per second.
	Talk	A protocol that allows two people on remote computers to communicate in a real-time fashion. See also: IRC.
	TCP	Transmission Control Protocol. An Internet Standard transport layer protocol defined in STD 7, RFC 793. It is connection-oriented and stream-oriented, as opposed to UDP.
	TCP/IP Protocol Suite	Transmission Control Protocol over Internet Protocol is the suite of networking protocols that have been used to construct the global Internet. It is also referred to as the DoD or ARPANET protocol suite. The US Department of Defense (DoD) Advanced Research Projects Agency (ARPA) funded its early development. See also: ICMP, TCP, UDP, FTP, Telnet, SMTP, SNMP.
	Telnet	The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and interact as normal terminal users of that host.
	Terminal Emulator	A program that allows a computer to emulate a terminal. The workstation thus appears as a terminal to the remote host.
	Terminal Server	A device that connects many terminals to a LAN through one network connection. A terminal server can also connect many network users to its asynchronous ports for dial-out and printer access.
	Thinnet	Thin (coaxial) Ethernet cable. Generally used between a multiport repeater and individual workstations.
	TN3270	A variant of the Telnet program that allows you to attach to IBM mainframes and use the mainframe as if you had a 3270 or similar terminal.
	Token Ring	A token ring is a type of LAN with nodes wired into a ring. Each node constantly passes a control message (token) on to the next; whichever node has the token can send a message. Often, "Token Ring" is used to refer to the IEEE 802.5 token ring standard, that is the most common type of token ring. See also: LAN.
	Topology	A network topology shows the computers and the links between them. A network layer must stay abreast of the current network topology to be able to route packets to their final destination.
	Transceiver	Transmitter-receiver. The physical device that connects a host interface to a network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and sense collisions. Transceivers are generally associated with a piece of network gear, for example a repeater, bridge, or workstation.
	Transit Network	A transit network passes traffic between networks in addition to carrying traffic for its own hosts. It must have paths to at least two other networks.
	Trojan Horse	A computer program that carries within itself a means to allow the creator of the program access to the system using it. See also: virus, worm.
	TSO	Telecommunications Services Outlet. A "wall jack" or faceplate in an office, lab, or other work area.
	Tunnelling	Tunnelling refers to encapsulation of protocol A within protocol B, such that A treats B as though it were a datalink layer. Tunnelling is used to get data between administrative domains that use a protocol that is not supported by the internet connecting those domains.

	Twisted Pair	A wiring scheme that uses standard pairs of copper wires. Twisted pair might be used for normal telephone connections, serial data.
	Twisted Pair Ethernet	Ethernet running over twisted pair wiring. Ethernet may also run over a variety of other media.
	Twisted Pair Hub	An Ethernet device, typically with eight twisted pair ports and one transceiver cable port.
U	UDP	User Datagram Protocol. An Internet Standard transport layer protocol defined in STD 6, RFC 768. UDP does not provide error detection, error correction, handshaking, or verification of delivery like TCP does. UDP does provide a connectionless delivery system between two hosts and is generally used for small non-critical applications since it has low overhead. See also: Connectionless, TCP.
	UNIX	Popular multi-user operating system for scientific workstations and file and database servers.
	URL	Universal Resource Locator, used in the World-Wide Web (WWW).
	Usenet	A collection of thousands of topically named newsgroups, the computers that run the protocols, and the people who read and submit Usenet news. Not all Internet hosts subscribe to Usenet and not all Usenet hosts are on the Internet. See also: NNTP, UUCP.
	UTC	Universal Time Coordinated. This is Greenwich Mean Time.
	UUCP	UNIX-to-UNIX Copy. This was initially a program run under the UNIX operating system that allowed one UNIX system to send files to another UNIX system over dial-up phone lines. Today, the term is more commonly used to describe the large international network that uses the UUCP protocol to pass news and E-mail. See also: Electronic Mail, Usenet.
V	Virtual Circuit	A network service that provides connection-oriented service regardless of the underlying network structure. See also: Connection-Oriented.
	Virus	A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. See also: Trojan Horse, Worm.
W	WAN	See: Wide Area Network
	White Pages	The Internet supports several databases that contain basic information about users, such as E-mail addresses, telephone numbers, and postal addresses. These databases can be searched to get information about individuals.
	WHOIS	An Internet program that allows users to query a database of people and other Internet entities, such as domains, networks, and hosts, kept at the DDN NIC. The information for people shows a person's company name, address, phone number and E-mail address.
	Wide Area Network	A network, usually constructed with serial lines that covers a large geographic area.
	Workstation	A node on the network. Typically associated with a single user, for example a PC or Macintosh.
	World Wide Web	A hypertext-based, distributed information system created by researchers at CERN in Switzerland. Users may create, edit or browse hypertext documents. The clients and servers are freely available.

	Worm	A computer program that replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments. Shoch & Hupp of Xerox in ACM Communications Network first defined worms in March 1982. The Internet worm of November 1988 is perhaps the most famous; it successfully propagated itself across the Internet on over 6,000 systems. See Trojan Horse, virus.
	WWW	See: World Wide Web
	WYSIWYG	What You See is What You Get.
Y	Yellow Pages (YP)	A service used on UNIX hosts to manage databases distributed across a network.
Z	Zone	A logical group of network devices (AppleTalk).



- 3**
- 3-way
 - Handshake, 68
- A**
- Activity
 - Viewing, 21
- Adapters
 - Configuring, 9
- Address Book
 - Filters, 28
- Advanced
 - Filter, 38
- B**
- Bridge, 59
- Buffer, 21
- C**
- Capture, 14
 - Configure, 7
- Capture Logging
 - Enable, 39
- Code Output
 - Disable, 21
- COMCTL32.DLL, 3
- Command Line Arguments, 54
- Configuring
 - Adapters, 9
 - Capture, 7
 - Guard, 10
 - Miscellaneous, 11
- Configuring Iris, 7
- D**
- Decode
 - Configuring, 8
 - Menu, 21
 - Options, 20
- Decode Logging
 - Enable, 41
- Decoder, 13
- Decoding and Reconstructing Captured Data
 - Overview, 1
- Decoding Data, 19
- De-multiplexing, 63
- E**
- Encapsulation, 62
- Ethernet, 59
- Ethernet Segments, 59
- Excel
 - Import log files to, 43
- F**
- Filter
 - Advanced, 38
 - FilterLayer 2,3, 30
 - IP Address, 35
 - MAC Address, 34
 - Ports, 36
 - XE "String:Filter" \i Words, 32
- Filters
 - Address Book, 28
 - creating, 1, 12, 28, 30, 32, 34, 35, 36, 38, 78
 - Hardware, 28
- Firewalls**, 4
- Frequently Asked Questions, 55
- G**
- Glossary, 73
- Graph
 - Protocol Distribution, 45
 - Size Distribution, 49
 - Top Hosts, 47
- Graphs
 - Configuring, 44
- Guard
 - Configuring, 10
 - Enable, 25
 - Logging, 27
 - Settings, 25
- Guard Logging
 - Enable, 42
- Guarding Against Intruders
 - Overview, 1
- H**
- Hardware filters, 28
- Header
 - Field Descriptions, 66

- Header Diagram
 - TCP, 68
- Horizontal Topology, 58
- Hub, 59
- Hubs**, 4

- I**
- Installation
 - Planning, 3
- Installing, 3
- Internet Protocol, 64
 - Packet Analysis, 64
- Intruders, 25
- IP Address
 - Filter, 35
- IP Header
 - Field Descriptions, 66
- Iris
 - Configuring, 7
 - Optimizing, 12
 - Starting, 5, 6

- L**
- Layer 2,3
 - Filter, 30
- Log Files
 - Import to Spreadsheet, 43
- Logging, 2, 39
 - Decode, 41
 - Enable Capture, 39
 - Guard, 27, 42
- Logical Ring Topology, 57
- Logical Star Topology, 58

- M**
- MAC Address
 - Filter, 34
- Miscellaneous
 - Configuring, 11
- Monitoring Network Activity
 - Overview, 1

- N**
- nable, 21
- Network
 - Troubleshooting, 18
- Network Statistics, 2
 - Displaying, 44
- Networking
 - Overview, 57
- Networking Protocols
 - TCP/IP, 63

- O**
- Optimizing Iris, 12
- Overview, 1

- P**
- Packet
 - Decoder, 13
 - Editor, 15
 - Filtering, 60
 - Interface, 12
- Packet Analysis, 64
 - UDP, 71
- Packets
 - Marking, 17
 - Sending, 18
- Ports
 - Customizing, 37
 - Filter, 36
- Protocol
 - Internet, 64
- Protocol Distribution
 - Graph, 45
- Protocols
 - Customizing, 31
 - Networking, 63

- R**
- Reconstructing Data, 19
- Repeater, 59
- Requirements, 3
- Router, 60

- S**
- Sending Packets
 - Sending, 18
- Session assembly, 19
 - Overview, 1
- Session Data
 - Viewing, 23
- Sessions
 - Viewing, 22
- Size Distribution
 - Graph, 49
- Sniffer Theory, 60
- Spreadsheet
 - Import log files to, 43
- Starting Iris, 5, 6
- Statistics, 2
 - Displaying, 44
- String
 - Filter, 32
- Switch, 60
- Switches**, 4
- System Requirements, 3

T

TCP, 67

- Handshake, 68

- Packet Analysis, 69

TCP Header, 68

TCP/IP

- Encapsulation, 62

- Four Layers, 61

- Networking Protocols, 63

- Overview, 61

Top Hosts

- Graph, 47

Transmission Control Protocol, 67

- Packet Analysis, 69

Troubleshooting

- Network, 18

U

UDP, 71

Uninstalling, 5

User Datagram Protocol, 71

- Packet Analysis, 71

W

Words

- Filter, 32