OptiView Workgroup Analyzer Help

Table of Contents

OptiView Workgroup Analyzer Help Contents

Welcome to Help

Analyzer Problems

Getting Started

Security

Network Troubleshooting

Using the OptiView Browser

Screen Help by OptiView Tab

Front Page

Front Page
Front Page Screen Help

Statistics

Utilization
Protocols
Top Hosts
Top Conversations
Statistic Screen Help

Discovery

Device Discovery
Network Discovery
Problem Discovery
Discovery Screen Help

Tools

Overview
Ping
SNMP Tables
Interfaces (Multi-Port Statistics)
Services
Trace Switch Route
Problems
Tools Screen Help

Cable Test

Overview
Twisted-Pair Detail
Fiber Test
Setting Up the Fiber Optic Test Kit
Fiber Inspector
Cable Test Screen Help

Capture/Generator

Packet Capture Filter
Traffic Generator
Packet Capture Screen Help

Setup

TCPIP
Ethernet
Version
Security
Options
Setup Screen Help

How To:

Changing the Analyzer MAC Address
Configure through the Serial Interface
Connect to the Network
Contact Fluke Networks
Control Access to Packet Capture
Control the Remote User Interface
Disabling Outgoing Traffic (Silent Mode)
Generate Traffic
Identify all Devices on Network
Load a .CAP and .NAM File
Look for Problems
Perform a NIC Test
Save Packet Captures
Save Reports
Set the Management Port IP Address
Set the OptiView Inspector Console Address
Set the Remote PC Address
Set Up the Fiber Test Kit
Set Up the NUT Port
Set Up the Packet Capture Filter
Set Up Traps
Test Cable Integrity
Updating the OptiView Workgroup Analyzer
Use the MIB Browser
Use the OptiView as an RMON Probe
Use the OptiView Browser
Use Packet Capture
Use Remote
View/Filter Packets

Welcome to Help

Welcome to the OptiView Workgroup Analyzer Help

Congratulations on your purchase of the most excellent piece of network test equipment on this planet!

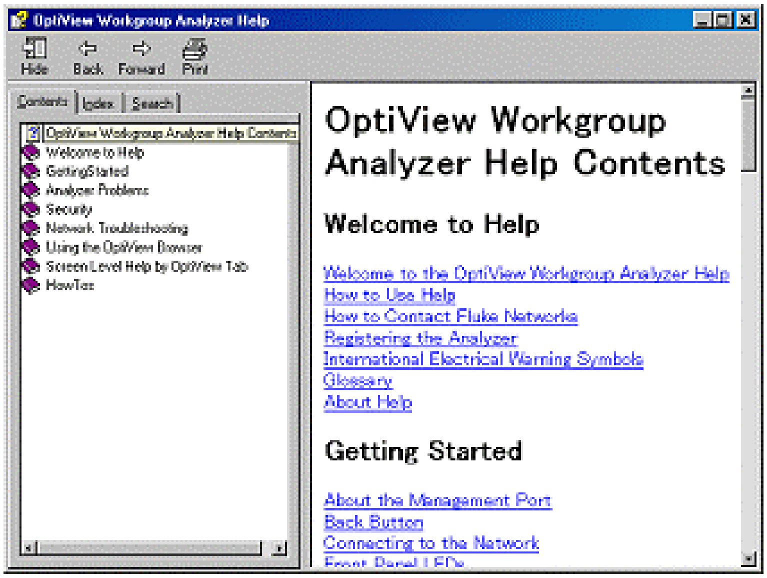
Goals and Expectations

The goal of our help system is to provide you with quick access to superior information. Through a comprehensive glossary, full search capability, and expert information on troubleshooting your network, we hope our help will answer all your questions and leave you confident using this quality piece of network test equipment.

Should you have any questions or concerns, please send them to http://www.flukenetworks.com.

How to Use Help

The help system is an integral part of the analyzer. While using the OptiView Workgroup Analyzer user interface software on your PC, help can be accessed by selecting the Help button located on the bottom-right of the user interface screen. When you click on Help at the bottom of the user interface screen, the help opens and the topic related to the current screen you are in is displayed.



- OptiView Workgroup Analyzer Help Contents
- Welcome to Help
- GettingStarted
- Analyzer Problems
- Security
- Network Troubleshooting
- Using the OptiView Browser
- ScreenLevel Help by OptiView Tab
- HowTos

OptiView Workgroup Analyzer Help Contents

Welcome to Help

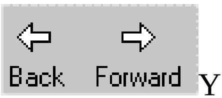
Welcome to the OptiView Workgroup Analyzer Help
How to Use Help
How to Contact Fluke Networks
Registering the Analyzer
International Electrical Warning Symbols
Glossary
About Help

Getting Started

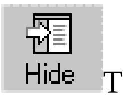
About the Management Port
Back Button
Connecting to the Network
Front Panel LEDs

Help Navigation

Ÿ While that help screen is open, you may now select from the table of contents (TOC), choose an index entry, or perform a full text search on any analyzer help topic or term.



Ÿ You can also click the **Back** and **Forward** buttons to move to and from previous viewed topics.



Ÿ The **Hide** button collapses the left pane of the Help screen giving you more room to view Help topics. The **Hide** button is replaced by the **Show** button. The **Show** button expands the left pane of the Help screen.

Ÿ The **Print** button allows you to either print the selected topic or print the selected heading and all subtopics.

The Help is organized into eight sections as follows:

Welcome to Help contains information on how to use help, how to contact Fluke Networks, how to register the analyzer, a glossary, and version information. **Analyzer Problems?** contains information about known analyzer defects that Fluke Networks is trying to resolve.

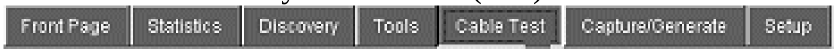
Getting Started describes fundamental analyzer information.

Security contains valuable information on setting up passwords for Packet Capture and Remote Access.

Using the OptiView Browser describes how to install and use the OptiView remote user interface, referred to as the OptiView Browser, on a PC

Network Troubleshooting describes how to maintain a healthy network and how to debug a not so healthy network.

Screen Level Help by OptiView Tab describes all the analyzer screens. It is organized around the seven analyzer functions (tabs) as follows:



How Tos: lists some of the important things you can do with the analyzer.

Changing the Default Help Language

The Help is displayed by default in English. The Help language can be changed in the **Setup | Version** screen. Simply select the language from the Help Language drop-down list.

Accessing the Online Documentation

The Getting Started Guide is also provided in electronic PDF format on the OptiView Resource CD-ROM provided with the analyzer, and on your PC in the default OptiView Workgroup Analyzer user interface installation directory C:\Program Files\Fluke Networks\OptiView.

How to Contact Fluke Networks

Visit the Fluke Networks website at www.flukenetworks.com. Send email to fluke-assist@flukenetworks.com. To order accessories or get the location of the nearest Fluke Networks distributor or service center, call:

- USA: 1-800-283-5853
- Canada: 1-800-363-5853
- Europe: +31-402-675-200
- Japan: +81-3-3434-0181
- Singapore: +65-6738-5655
- Anywhere in the world: +1-425-446-4519

For operating assistance in the USA, call 1-800-283-5853.

Registering Me

Please take the time to register your OptiView analyzer. A registration card is supplied in the shipping box. You can also register online by going to http://support.flukenetworks.com, click on **support**, then click on **Registration**. A Log in screen is displayed. Click on **create** to setup an account password if you have not done so before. Then you will be able to log in using your email address and password. Once logged in, you can fill out the online registration form by clicking on **Register a product**.

As a registered user, you are entitled to entry level product support, including three free telephone support incidents during the first 60 days of ownership, access to entry level online Knowledge Base library of product operation and application information, and Web-based trouble ticketing. We will also be sending you Fluke Networks company and product information updates.

International Electrical Warning Symbols

⚠Warning: Risk of electrical shock.

⚠ Warning or Caution: Risk of damage or destruction to equipment or software.

⊗ Do not connect this terminal to public communications networks, such as telephone systems.

Glossary

10BASE2

Sometimes called ThinLAN or CheaperNet, 10BASE2 is the implementation of the IEEE 802.3 Ethernet standard on thin coaxial cable. The maximum segment length is 185 meters.

10BASE5

Sometimes called ThickLAN, 10BASE5 is the implementation of the IEEE 802.3 Ethernet standard on thick coaxial cable. The maximum segment length is 500 meters.

10BASEF

A point-to-point fiber link. This is the draft specification for IEEE 802.3 Ethernet over fiber optic cable.

10BASE-T

10BASE-T is the implementation of the IEEE 802.3 Ethernet standard on unshielded twisted-pair wiring. It is a star topology, with stations directly connected to a multi-port hub and has a maximum cable length of 100 meters.

100BASE-TX

Fast Ethernet; 100 Megabit version of Ethernet that operates on two pair of a 4 pair category 5 cable.

100BASE-FX

Fast Ethernet; 100 Megabit version of Ethernet that operates on two fiber optic fibers using 850nm wavelength.

10/100BASE-FLP

10/100BASE Fast Link Pulse (FLP) Burst; FLP is the basic mechanism that Auto-Negotiation uses to advertise the device's abilities. It is a series of link pulses which encode a 16 bit word. An FLP Burst is composed of 17 to 33 link pulses which are identical to the link pulses used in 10BASE-T to determine whether a link has a valid connection (sometimes referred to as Normal Link Pulses or NLPs.) FLP Bursts occur at the same interval as NLPs, 16.8ms. An FLP Burst has a nominal duration of 2 ms.

An FLP Burst interleaves clock pulses with data pulses to encode a 16 bit word. The absence of a pulse within a time window following a clock pulse encodes a logic zero and a pulse within the time window following a clock pulse encodes a logic one.

1000BASE-X

1000BASE-X is the standard for fiber optic Gigabit Ethernet. The 802.3z standard describes the specifications for the 1000BASE-X fiber optic Gigabit Ethernet system.

802.2

This IEEE standard specifies Logical Link Control (LLC), which defines services for the transmission of data between two stations at the data-link layer of the OSI model.

802.3

Often called Ethernet, this IEEE standard governs the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) networks. Typical cabling standards are 10BASE-T, 10BASE2, and 10BASE5.

Access Method

The set of rules by which the network determines what node has access to the network. The most popular access method is Collision Sense Multiple Access/Collision Detection

(Ethernet).

Anomaly

An impedance discontinuity causing an undesired signal reflection on a transmission cable.

AppleTalk

The set of protocols that define Apple Computer's networking specification.

ARCNET

Attached Resource Computer NETwork. A token bus local area network standard developed by Datapoint Corporation. ARCNET runs on RG-62 coax, twisted pair, or fiber optic cable with a basic signaling rate of 2.5 Mbps.

ARP (Address Resolution Protocol)

A member of the TCP/IP protocol suite, ARP is the method by which a station's MAC address is determined given a station's IP (Internet Protocol) address.

ARP Cache

The ARP cache is where each IP host maintains the most recent IP to MAC address mapping. The ARP cache is maintained so that the IP can quickly send IP packets with the correct Ethernet, Token Ring, or FDDI MAC address.

ASCll (American Standard Code for Information Interchange)

A standard for character-to-number encoding that is widely used in the computer industry. An ASCII file is generally referred to as a text file.

Attenuation

Attenuation is the loss of signal strength over the length of the cable. It is caused by a loss of electrical energy due to the resistance of a cable and by leakage of energy through a cable's insulating material. Attenuation losses due to cable resistance increase as the transmission frequency increases, and losses due to insulation leakage increase as temperature increases.

Autonomous System

A group of routers exchanging routing information via a common routing protocol.

Backward Explicit Congestion Notification (BECN)

Notification by the network that an end user is sending frame relay data onto the network that is either causing or encountering congestion within the WAN network.

Bandwidth

Bandwidth is the rate at which data can be transmitted over a channel. It is measured in bits per second. For example, Ethernet has a 10 Mbps bandwidth and FDDI has a 100 Mbps bandwidth. Actual throughput is almost always less than the theoretical maximum.

Basic Rate Interface (BRI) ISDN

ISDN service consisting of two 64 Kbps B channels for data transmission and one 16 Kbps D channel for signaling information. Some providers may provide alternate configurations of BRI ISDN.

Beaconing

The condition of a ring that has one or all NICs transmitting beacon frames.

BNC

A coaxial cable connector used with ThinLAN (10BASE2) Ethernet networks.

Bindery

A Novell NetWare 2.x and 3.x database which stores information about the resources (services) and clients on an IPX network, such as passwords, client accounts, and client restrictions.

Bootstrap Protocol

A protocol that provides a subset of the services provided by DHCP. It is used for the central administration and distribution of IP addresses and other boot-process information. BootP is normally used on large networks where IP management is an issue and where IP devices need to acquire IP parameters at power up.

Border Gateway Protocol 4 (BGP-4)

Border Gateway Protocol 4 (RFC 1771) is used to connect different autonomous systems. While most routing protocols (such as OSPF, IGRP and RIP) use broadcast or multicasts, BGP uses TCP which requires that you be in the two routers' connection path to discover the use of BGP.

BOOTP (Bootstrap Protocol)

BOOTP is a protocol that lets a network user be automatically configured (receive an IP address) and have an operating system booted or initiated without user involvement. The BOOTP server, managed by a network administrator, automatically assigns the IP address from a pool of addresses for a certain duration of time.

BOOTP is the basis for a more advanced network manager protocol, the Dynamic Host Configuration Protocol (DHCP).

BPS

Bits per second. A measure of speed or raw data rate. Often combined with metric prefixes as in Kbps (for thousands of bits per second) or Mbps (for millions of bits per second).

Bridge

A device that links two or more networks that use the same OSI Data Link protocol. A bridge evaluates source and destination addresses to pass only frames that have a destination on the connecting network.

Broadcast

A message that is addressed to all stations on a network. For Ethernet networks, the MAC broadcast address is FFFFFFFFFFFF; for Token Ring networks, the broadcast addresses are FFFFFFFFFFFF and C000FFFFFFFF.

Broadcast Storm

A situation in which a large number of stations are transmitting broadcast packets. This typically results in severe network congestion. This problem is usually a result of a misconfiguration.

Browser

A program that provides a graphical interface to the World Wide Web.

Bus Topology

A bus topology is a network architecture in which all of the nodes simultaneously receive network traffic. Ethernet is a bus topology.

Byte

A collection of bits. A byte usually contains 8 bits.

Cable Types

The following cables can be tested by the analyzer.

UTP100 Category 3
UTP100 Category 4
UTP100 Category 5
UTP Cat 5e
UTP100 Category 6
ScTP100 Category 3
ScTP100 Category 4
ScTP100 Category 5
ScTP100 Cat5e
ScTP100 Category 6
ScTP120 Category 3
ScTP120 Category 4
ScTP120 Category 5
ScTP120 Category 6

UTP is the abbreviation for unshielded twisted pair, and ScTP is the abbreviation for screened twisted pair.

Category 3 is typically used in 10 Mbit Ethernet.
Category 4 is typically used in 10 Mbit Ethernet and 16 Mbit Token Ring.
Category 5 is typically used in 10/100 Mbit Ethernet with Category 5E extending to 1000 Mbit copper. Category 5 is the default setting in Cable Test.
Category 6 is a proposed standard in the final stages of approval (05/00).

Characteristic Impedance

Characteristic impedance is the opposition (resistance and reactance) to signal propagation on a cable. It depends on the physical properties of a cable, which are determined at the time of manufacture. Manufacturing variations can cause slight differences in characteristic impedance for the same cable type.

Client

A client is a computer that make requests of a server. A client has only one user; a server is shared by many users.

Coaxial

A type of cable in which the inner conductor is surrounded by a tubular conductor, which acts as a shield. Coaxial cables typically have a wide bandwidth.

Collision

A collision is the result of two or more nodes transmitting at the same time. Excessive collisions are most often caused by a problem with the physical media.

Collision Frames = 1 RFC-1643

"Single Collision Frames", a count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Collision Frames > 1 RFC-1643

"Multiple Collision Frames", a count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Committed Burst Rate (Bc)

A contractually agreed upon, guaranteed, bandwidth rate above the Committed Information Rate that a carrier agrees to provide a frame relay PVC (under normal network conditions).

Committed Excess Burst Rate (Be)

A contractually agreed upon, guaranteed, bandwidth rate above the Committed Burst rate that a carrier agrees to try and sustain for a frame relay PVC. Excess burst rate traffic is automatically flagged as discard eligible.

Committed Information Rate (CIR)

For frame relay service, a contractually agreed upon minimum bandwidth that is available to an end user's permanent virtual circuit (PVC) at all times.

Crossed Pair

A wiring error in twisted pair cabling in which a pair on one connector of the cable is wired to a different pair on the other end of the cable.

Crosstalk

Crosstalk is electrical interference generated by signal coupling between wires in a multiwire cable.

CSMA/CD (Carrier Sense, Multiple Access with Collision Detection)

In CSMA/CD, each node or station has equal access to the network. Before transmitting, each station waits until the network is not busy. Since each node has equal access to the network, a collision (two stations transmitting at the same time) can occur. If a collision occurs, the affected nodes will wait a random time to retransmit. Ethernet uses the CSMA/CD access method.

DLCI (Data Link Connection Identifier)

The local frame relay permanent, virtual circuit address assigned by a frame relay provider to designate the channel between the user and the network.

DB

Abbreviation for decibel. A logarithmic unit of measure expressing the amplitude ratio between two signals.

DB-9 Connector

A modular connector used for STP wiring. The DB-9 connector has nine conductors to accommodate two pairs of wires and has become the dominant connector used in Token Ring STP installations.

DECnet

Digital Equipment Corporation's set of communication protocols for networking computers.

Designated Bridge

For IEEE 802.1d or DEC spanning tree, only the designated bridge (one per LAN segment or collision domain) can forward frames and transmit spanning tree Bridge Protocol Data Units (BPDU). The designated bridge is the bridge on a given segment that has the lowest cost to the root bridge.

Destination Address

The address of the station receiving a frame.

DHCP (Dynamic Host Configuration Protocol)

A protocol established to lessen the administrative burden of manually configuring TCP/IP hosts on a network. DHCP provides a service that allows a device attached to the network to learn all or at least some of its network configuration automatically.

Discard Eligible (DE) bit

Frame relay users can designate the discard eligibility of frames by configuring their routers or switches to set flags within the frame relay data frames. When the network becomes congested, the frames with the discard eligible bit set will be the first to be discarded.

DNS (Domain Name Server)

A general purpose distributed data query (or look up) service based on host names that are in the form of domain names. A domain is a unique name given to a logical collection of computers connected to one or more networks. Domain names typically end in a suffix denoting the type of site (such as, **flukenetworks.com**). The **.com** stands for a commercial company.

Downstream

Downstream is in the direction of data flow on a Token Ring network.

E1

Digital line service that provides a transmission rate of 2.048 Mbps. Most common outside North America.

EIA568

Electronic Industries Association Commercial Building Telecommunications Wiring Standard. Specifies maximum cable lengths, installation practices, and performance specifications for generic building wiring.

EIGRP

Cisco Systems Enhanced version of their IGRP routing protocol. While still a distance-vector routing protocol, EIGRP offers fast reaction to network changes.

Encapsulation

Encapsulation is the method of placing one protocol into another protocol's format. For example, in a Novell Ethernet environment there are four different methods to encapsulate IPX in Ethernet/802.3 frames: 802.3 raw, 802.2, Ethernet II, and SNAP.

Ethernet

Ethernet is a 10 Mbps topology that runs over thick coax, thin coax, twisted-pair, and fiber-optic cabling systems.

Excess Collisions

RFC-1643 Excessive Collisions, a count of frames for which transmission on a particular interface fails due to excessive collisions.

Fast Ethernet

Industry standard terminology for 100Base-T. Industry groups do not agree on using the term to refer to 100VG-AnyLAN; some call 100VG-AnyLAN a Fast Ethernet technology while others do not.

Fault Domain

The fault domain defines the boundaries of a problem on a Token Ring network. The fault domain limits the problem to two stations, their connecting cables, and any equipment, such as a MAU, between the two stations. The two fault domain stations are the station reporting the error and its Nearest Active Upstream Neighbor (NAUN).

FCS (Frame Check Sequence)

A field transmitted in LAN frames that encodes error checking information.

Fiber-Optic Cable
Communications cable that use light as the signal carrier. Fiber-optic cable is immune to electrical and magnetic interference.

Fiber-Optics
A technology that transmits light beams along optical fibers. The light beams are used as a digital information carrier. The optical fibers are formed into fiber optic cables and are a direct replacement for conventional cables and wire pairs. Fiber optic cables are immune to electrical and magnetic interference and occupy much less physical space than conventional cables and wire pairs.

Forward Explicit Congestion Notification (FECN)
Notification by the network to an end user that frame relay data being received is either causing or encountering congestion within the WAN network.

Frame
A frame is the transmission unit on a network. In Token Ring, a frame is the token joined with node data.

Frame Errors
For FDDI, Frame Errors (RFC 1512) is the number of frames that were detected to be "in error" by this MAC and were not detected to be "in error" by another MAC.

Frame Relay
A fast form of packet switching that is accomplished with smaller packet sizes and less error checking.

Full-Duplex
10Base-T and 100Base-TX network operation using a switching Hub to establish a point-to-point connection between LAN nodes that allows simultaneous sending and receiving of data packets. Full-duplex performance is twice that of half-duplex performance. A 10Base-T full-duplex network is capable of 20 Mb/s data throughput; likewise, a full-duplex 100Base-TX network is capable of 200 Mb/s throughput.

Half-Duplex
Network operation is one direction at a time only; either sending or receiving data packets, but not both at the same time.

Hermaphroditic Connector
A loopback, or self-shorting, connector typically used with Type 1 (STP) cable.

Hops
Most commonly defined as the number of routers traveled by a frame to reach its destination.

Host
A computer that is configured to allows users to communicate with other host computers on a network. Individual users can communicate with other individuals by using application programs, such as electronic mail, browser, and FTP.

HTTP (Hypertext Transfer Protocol)
The protocol used to communicate between Web clients and servers.

Hub
Today, most often referred to in 10BASE-T or 100BASE-T networks. A 10BASE-T/100BASE-T hub is essentially a multiport repeater hub with each segment dedicated to a single connection.

Hyperlink

Highlighted words on a Web page that provide a jump (hyper link) to a different document (or page) on the World Wide Web when it is selected. The jump can be to an additional page at the current Web site or to a completely different Web site.

ICMP (Internet Control and Message Protocol)

A communication protocol used by every device that uses IP. ICMP reports errors that occur during the delivery of packets on the network.

Integrated Service Digital Network (ISDN)

The combination of voice and digital network services in a single medium. This provides voice connections and digital data services over the same phone line.

Interior Gateway Routing Protocol (IGRP)

Interior Gateway Routing Protocol is a Cisco Systems proprietary distance-vector protocol (such as RIP) that takes into account the potential bandwidth of links in its routing table determination. This makes a 10 Mb LAN have a lower cost assessment than a 9600 serial line.

Internet

The Internet is a global network of networks connecting millions of users worldwide via many computer networks using a simple standard common addressing system and communications protocol called TCP/IP (Transmission Control Protocol/Internet Protocol).

Internet Protocol (IP)

IP is the network layer protocol for the TCP/IP suite.

Internetwork Packet Exchange (IPX)

IPX is the network layer protocol for Novell's NetWare protocol suite.

Jabber

A frame greater than the maximum legal size (1518 bytes) with a good or bad frame check sequence. In general, you should not see jabbers. The most likely causes of jabbers are a faulty NIC/driver or perhaps a cabling problem.

Key Devices

The analyzer Discovery supports logging key devices selected by the user. This category can consist of all servers, switches, and routers since these are the devices an administrator most likely wants to monitor regularly. Key devices can also be considered to be the devices that provide infrastructural support to the network by keeping it operational. The analyzer checks the up/down status of key devices approximately every 2 minutes. A key device can be changed to a non-key device and vice versa.

LAN (Local Area Network)

A physical network technology used over short distances to connect many workstations and network devices using a communication standard (Token Ring or Ethernet, for example).

Late Collision

A collision that occurs after the first 64 bytes in a frame. The analyzer will generally only see late collisions on a coaxial segment. In 10BASE-T networks, late collisions will be seen as frames with a bad FCS. Causes of Late Collisions are a faulty NIC or a network that is too long.

Layer

One of seven levels in the Open Systems Interconnection (OSI) reference model. See OSI.

Link Error Rate (LER)

For FDDI, Link Error Rate (RFC 1512) is an estimate of the error rate for each physical port (PHY). Most devices will shutdown the port if the error rate is any greater than 10E-7. Error rates of 10E-12 are good, error free links.

Link Pulse

A single-bit test pulse that is transmitted at least every 150 milliseconds during idle periods on 10BASE-T link segments to verify link integrity.

Lobe Cable

Lobe cable is the length of cable connecting the MAU to the NIC. The lobe cable can be several connected cable segments.

Loopback Connector

A connector used anywhere on a cable for returning test signals.

MAC (Media Access Control)

The MAC protocol defines the access method (i.e., token passing or CSMA/CD) for a particular network topology.

Manufacturer Prefix

The standard partial address used to identify a particular manufacturer. The prefix of the address is predefined uniquely for each manufacturer, while the remainder of the address uniquely identifies the station.

MAU (Multi-station Access Unit)

A wiring concentrator for lobes on a Token Ring network that provides connectors for attaching devices to the ring. A MAU consists of a bank of electromechanical relays used to physically connect or remove stations from a ring.

Mbps

Millions of bits per second. See BPS.

MDI and MDI-X

MDI is a media dependent interface. It is the IEEE standard for the interface to an unshielded twisted pair (UTP) cable.

In order for two devices to communicate, the transmitter of one device must connect to the receiver of the other device. The connection can be established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

Ports that implement a crossover function internally are known as MDI-X ports, where X refers to the crossover function.

MIB (Management Information Base)

The set of objects that can be used by an SNMP management station to query for information or to set parameters in the SNMP agent, such as a router. Also see RMON MIB.

MIME (Multipurpose Internet Mail Extensions)

An Internet formatting standard used for encoding files that will be attached to email messages. Also see UU Encoding.

Misaligned

RFC-1643 "Alignment Errors", a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.

Multicast

Packets that are directed to a group of nodes rather than to a single node or all nodes. This is contrasted to a broadcast packet, which is directed to all nodes.

NAUN (Nearest Active Upstream Neighbor)

The active station that is directly upstream from a given station.

Neighbor Notification Protocol

The Token Ring protocol that notifies every station of changes in NAUN.

NEXT

NEXT (Near-End Crosstalk) is a measure of the crosstalk coupled from one wire pair to another pair.

NIC (Network Interface Card)

A network interface card is the adapter card that plugs into a computer to provide a network connection.

NOS (Network Operating System)

A network operating system is the software that runs on a group a computers (clients and servers) that mediates the access to the files and resources. Examples of NOSs include Novell NetWare, and Banyan VINES.

Not Copied

For FDDI, Not Copied (RFC 1512) is a count that should, as closely as possible, match the number of frames that were addressed to this MAC but were not copied into its receive buffers. This might occur due to local buffer congestion.

NVP (Nominal Velocity of Propagation)

The speed of a signal through a cable expressed as a percentage of the speed of light. Typically, the speed of a signal through a cable is 60-80% of the speed of light.

Open

A break in the continuity of a circuit which prevents signal transmission.

Open Shortest Path First (OSPF)

Open Shortest-Path First (RFC 2328) is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a list of least cost paths.

OSI (Open Systems Interconnection)

OSI is the international standard for data communication between computer systems. The OSI model provides the foundation for products from different vendors to function in the same network. The following is a list of the seven layers of the OSI model:

Layer 1: The **Physical Layer** handles the electrical and mechanical connections of network components to insure bit transmission between stations.

Layer 2: The **Data Link Layer** handles the way frames are transmitted and provides frame error controls for reliable communication between stations.

Layer 3: The **Network Layer** determines the path for communication between stations and handles routing and congestion issues on the network.

Layer 4: The **Transport Layer** handles the exchange of entire messages between stations and error recovery.

Layer 5: The **Session Layer** handles the communication sessions between computers.

Layer 6: The **Presentation Layer** provides transparent data communications between stations of different types.

Layer 7: The **Application Layer** provides all functions to support end-user services or applications.

Packet

A group of bits in a defined format, containing a data message that is sent over a network.

Permanent Virtual Circuit (PVC)

A circuit that is kept up permanently such as a dedicated leased line on the telephone network.

Plenum Cable

A Plenum cable is one that has been certified for installation in air ducts and open spaces over suspended ceilings when not using conduit. Plenum cable is fire-resistant and does not emit toxic fumes when burned.

Pop-Up Window

A window that the analyzer displays to communicate information or to prompt you with a choice of actions.

Primary Rate Interface (PRI) ISDN

ISDN service based on a rate of 1.544 Mbps and including 23 B channels and one 64 Kbps D channel. The B channels provide data transmission while the D channel provides signaling information.

Propagation Delay

Propagation Delay is the time it takes for a signal to go from one end of a cable to the other. There should be similar delay characteristics between cable pairs. Propagation Delay is very important for technologies that use parallel transmission techniques, such as 100BASE-T4 and 100BASE-VG.

Protocol

A set of rules that machines must follow to exchange information on a network.

Proxy ARP

Routers with Proxy ARP enabled will respond to ARP requests for off-net hosts. When a node relies on Proxy ARP, the node only has to ARP for the target node instead of forwarding the packet to the correct local IP router. Some vendors' routers respond incorrectly to on-net ARP requests, which can create confusing network behavior.

Remote Collision

A collision that occurs on the other side of a repeater. Since a 10/100BASE-T hub is a multi-port repeater with a "segment" dedicated to each station, 10/100BASE-T collisions are remote collisions.

Remove Ring Station

The act of taking an active device from the ring.

Repeater

A repeater is a layer-1 device that regenerates and retimes frames.

Report Soft Error Frame

A MAC frame that is transmitted when an intermittent, or soft, error causes data to be transmitted more than once. The Report Soft Error Frame contains information about the error, or errors, on the ring.

Reversed Wire

A wiring error in twisted pair cabling in which the pins on a pair are reversed between connectors on each end of the cable.

RFC-1398

Definitions of Managed Objects for the Ethernet-like Interface Types

RJ-45 Connector

A modular connector used for UTP wiring. The RJ-45 connector has eight conductors to accommodate four pairs of wires, and has become the dominant connector used in Ethernet and Token Ring UTP installations.

RMON MIB (Remote Network Monitoring MIB)

The set of objects defined in various RFCs and private MIBs that are used to monitor various network activity. Also see MIB.

Router

A router is a network-layer device that connects networks using like network-layer protocols. Routers can span different network topologies. For example, a router can interconnect Token Ring and Ethernet Novell NetWare networks. For a router to pass traffic, unlike a bridge, it must be configured for the desired protocol. Routers are more difficult to configure but offer greater security.

Routing Information Protocol (RIP)

Routing Information Protocol (RFCs 1058, 1388, 2453) is the most widely supported IP routing protocol. RIP is a distance-vector protocol and bases its routing decisions on the number of hops.

Runts

Typically defined as an Ethernet frame which is less than 64 bytes. Depending on which device is counting the runts, the frame check sequence may be good or bad.

Screened Twisted-Pair (ScTP)

ScTP is a cable type that has four twisted pairs (similar to UTP), and has a foil shield (unlike UTP). Used in Europe and America.

Server

File servers store files that may be shared by the network workstations. A server (file server) is a computer that contains files and is dedicated to delivering those files to other computers upon request.

Short

A near-zero resistance connection between two wires of a circuit.

Short Frame

A frame less than the minimum legal size (less than 64 bytes) with a good frame check sequence. In general, you should not see Short Frames. The mostly likely cause of a Short Frame is a faulty adapter card or driver.

Signal/Noise Ratio

The ratio of worst-case received signal level to noise level measured at the receiver input (expressed in DB). The S/N ratio may be expressed as NEXT(DB) - Attenuation(DB), provided idle channel background noise is low. Higher S/N ratios provide better channel performance.

SMTP (Simple Mail Transfer Protocol)

A protocol used to transfer email between hosts and ultimately to its final destination.

SMTP Host

A computer running the Simple Mail Transfer Protocol (SMTP) that handles email delivery.

SNMP (Simple Network Management Protocol)

The Internet standard protocol for communicating between network managers and other network nodes. Also see MIB (Management Information Base) and RMON MIB (Remote Network Monitoring MIB).

Soft Error

An intermittent error or operation of a Token Ring network that interferes with the transmission of a frame. A soft error causes a frame to be retransmitted until it is properly received.

Source Address

The address of the station originating a frame.

Source Routing

Source routing, normally used with Token Ring, is a method by which a station discovers the route to a target station.

Split Pair

The error of using wires from two different twisted pairs. This error cancels the crosstalk elimination characteristics of twisted pair wiring and produces crosstalk. Use a single twisted pair for transmit and another twisted pair for receive to minimize crosstalk.

Static Router

A device on the network that is assumed to be a router based on information monitored on the network.

STP (Shielded Twisted Pair)

Cable that is both twisted and shielded by pairs. This eliminates crosstalk to a greater degree than UTP cable and minimizes crosstalk at high transmission rates.

Symbolic Name

A symbolic name is the name given to an address to make it easier to use (MKG_SERVER versus 0003e8000008, for example).

T1

Digital line service that provides a transmission rate of 1.544 Mbps. The 1.544 Mbps bandwidth of T1 is usually divided into twenty-four 64 Kbps channels.

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is the protocol suite originally developed by the Advanced Research Projects Agency (ARPA) to interconnect a research network. The TCP/IP is an open standard not owned by any particular organization. The term TCP/IP is often used to refer to the entire suite of related protocols that includes IP, FTP, Telnet, RIP.

TDR (Time Domain Reflectometry)

A TDR is a method to determine a cable's length, characteristic impedance, and other parameters by transmitting a pulse into a cable and examining reflected energy.

Telnet

Telnet is a session-layer protocol in the TCP/IP protocol providing terminal emulation.

Terminator

A resistor connected to the end of a coax cable which is intended to match the characteristic impedance of a cable. Signals are dissipated in the terminator, eliminating reflections.

Too Long

RFC-1643 "FrameTooLongs", a count of frames received on a particular interface that exceed the maximum permitted frame size.

Topology

Topology is the organization of network components.

Transceiver

In Ethernet networks, a transceiver is used to couple electrical signals to and from an adapter to the transmission media. In ThinLAN and 10BASE-T networks, the transceiver is integrated directly onto the network adapter card.

Transmit Delay

RFC-1643 "DeferredTransmissions", a count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.

Twisted Pair

A pair of wires that are twisted to minimize crosstalk. Crosstalk is minimized with twisted pair wiring by canceling the magnetic fields generated in each of the twisted wires. Twisted pair cable (UTP or STP) is typically made up of several twisted pairs of wires.

Unicast

A packet that is directed to a single node is a Unicast packet. This is contrasted to a broadcast packet, which is directed to all nodes.

UTP (Unshielded Twisted Pair)

Cable that is twisted by pairs but not shielded. This minimizes crosstalk by canceling the magnetic fields generated in each of the twisted wires.

UU Encoding

A standard Internet format used for encoding files that will be attached to email messages. Also see MIME (Multipurpose Internet Mail Extensions).

Virtual Circuit

A network capability that lets two ports communicate as if they were directly connected without regard for the structure of the physical layer.

VLAN (Virtual LAN)

A group of ports configured into one broadcast domain (or logical LAN). VLANs can only be detected by using the private MIB associated with the device.

WAN (Wide Area Network)

A network that is usually constructed with serial lines, which covers a large geographic area. Also see LAN (Local Area Network).

Wavelength

The length of the optical wave used in fiber optic transmissions. Also used to specify the different optical sources available for fiber optic usage.

Wire Fault
A hard error caused by opened or shorted network wires.

World Wide Web (WWW)
A hyperlink-based, distributed information system that can be used to create, edit, or browse documents. It is a powerful, global, information system. The hyperlinks provide access to other information sources on the Internet. Also see Hyperlink.

About Help

Version 2.5_10/31/02

Help was created using RoboHELP for Microsoft HTML Help 9

Additional Documents

The OptiView analyzer is shipped with the following documents in PDF format. They are installed with the OptiView analyzer user interface software by default in C:\Program Files\Fluke Networks\OptiView.

If you install the user interface software in a different location, the links below will not work. But you can still go to the OptiView directory and launch these PDFs.

Ÿ Getting Started Guide

Ÿ Help

Analyzer Problems

CRC Alignment Errors are Reported Briefly

When the analyzer is first connected to a network, CRC alignment errors *sometimes* are briefly reported in the **Statistics | Utilization | Errors** screen. The CRC alignment errors are not actually on your network, and the analyzer corrects itself after a short period of network monitoring.

Fluke Networks is continuing to find a fix to this problem and will provide a software update on www.flukenetworks.com when it becomes available.

MIB Browser Does Not Install Correctly in Japanese Windows 2000

The MIB browser software is located on your OptiView Resource CD. On Japanese Windows 2000, the MIB browser is installed by default in C:\Winnt\profiles\all-users. It must be installed in C:\Program Files\MG-Soft\Bin for it to work correctly with the analyzer.

Power-On Self Test Fails

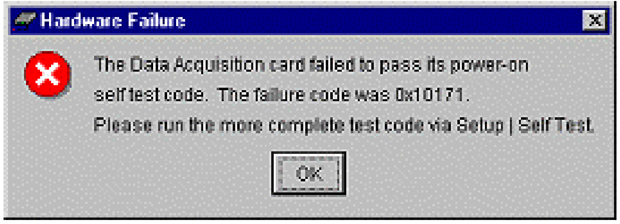
When an OptiView analyzer is powered on, it will perform a self test. In the rare event that self test should fail, it will display a popup similar to the example below. To view more detail on the failure, press **OK,** go to the **Setup | Self Test** screen, and press **Run Self Test** .

If the test passes in the **Setup | Self Test** screen, the hardware condition may be intermittent, marginal, or the failure may be specifically related to the power-up sequence. You may continue to use the analyzer, but should consider having it checked out by a Fluke Networks service center.

If the self test fails consistently on the **Setup | Self Test** screen, the analyzer **should NOT be used**, but immediately returned to a Fluke Networks service center for service.

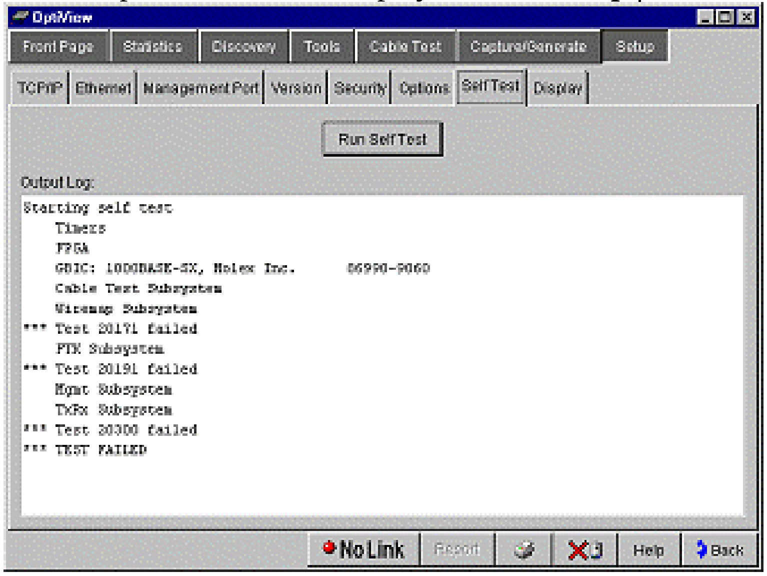
The following example shows a possible power-up self test failure. In this example, the error code is *0x10171*. It should be noted that the first digit after the "0x" is a "1" which indicates this failure occurred in power-on self test. In the **Setup | Self Test** screen self test, it is replaced with a "2" to indicate the error has been detected in the **Setup | Self Test** screen self test.

An example of a possible power-up self test failure



The Data Acquisition card failed to pass its power-on
self test code. The failure code was 0x10171.
Please run the more complete test code via Setup | Self Test.

An example of the failure displayed in the **Setup | Self Test** screen



Output Log:

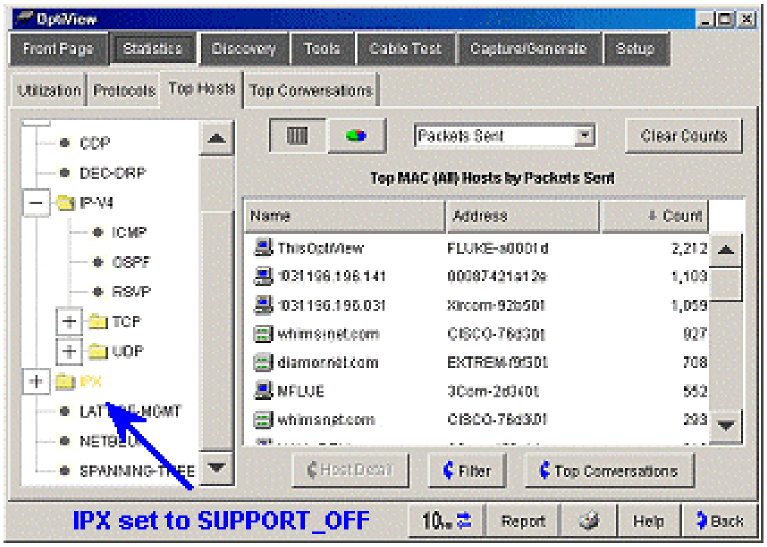
```
Starting self test
    Timers
    FPGA
    GBIC: 1000BASE-SX, Molex Inc.      06990-9060
    Cable Test Subsystem
    Wiremap Subsystem
*** Test 20171 failed
    FTK Subsystem
*** Test 20191 failed
    Mgmt Subsystem
    TxRx Subsystem
*** Test 20300 failed
*** TEST FAILED
```

Protocol Types Display Red or Orange

If in the analyzer's **Protocol** tab, the protocol list displays some protocol types in red or in orange (actually, it's more yellow/orange), this is an indication that the analyzer's RMON MIB has been modified.

The OptiView analyzer is an RMON device. Being an RMON device, its RMON MIB settings could be modified under certain conditions. An IT professional at the console who knows the correct community strings for an RMON device can reconfigure MIB settings for that device. And in rare situations, some devices on the network can configure other RMON devices on the network based on their network configuration.

A protocol displaying in red results when the RMON2 Protocol Directory entry for that protocol has been set to "UNSUPPORTED". A protocol displaying in yellow/orange results when the RMON2 Protocol Directory entry for that protocol has been set to "SUPPORT_OFF" (see below).



Top MAC (All) Hosts by Packets Sent

Name	Address	Count
ThisOptiView	FLUKE-a0001d	2,212
1031196.196.141	00087421a12e	1,103
1031196.196.031	Xircom-92b501	1,059
whimsinet.com	CISCO-76d301	927
diamondnet.com	EXTREM-f9f301	708
NFLUE	3Com-2d3i01	552
whimsnet.com	CISCO-76d301	293

IPX set to SUPPORT_OFF

Example Top Hosts screen showing the IPX protocol set to "SUPPORT_OFF"

To reset OptiView's RMON agent and this MIB setting back to factory default, use a MIB Browser such as the one supplied with the analyzer software (**Start | Programs | MG-SOFT MIB Browser | MIB Browser**), and:

SET probeResetControl in the RMON2 MIB 1.3.6.1.2.1.16.19.5

(iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).probeConfig(19).probeResetControl(5)) to a value of “3” (for Cold Start).

Back Button

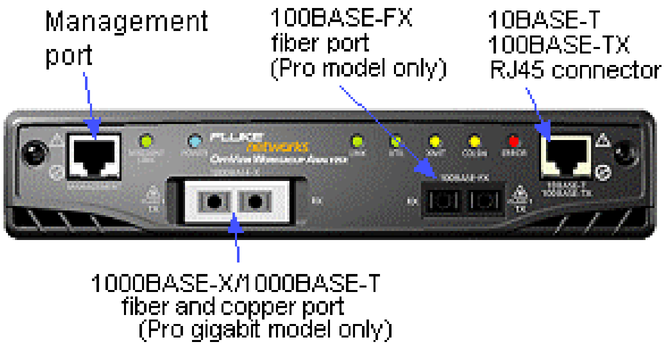
Takes you back to the previous viewed screen. Initially after starting the OptiView Workgroup Analyzer, it is gray until you go to another screen. The Back button Back works in conjunction with buttons containing the forward arrow ↩. When going to a screen using a forward arrow button, the Back button then returns you to that particular screen.

Connecting to the Network

Depending on which model you have ordered, the OptiView Workgroup Analyzer can be connected to 10/100 and 1000 (gigabit) Ethernet networks via an RJ-45 or fiber cabling. When using a copper cable to connect the 10/100 network test interface (RJ-45), the analyzer will automatically swap and correctly map connections if you use a MDI-X (cross-over) cable.

The analyzer supports a number of different fiber types which include:

100BASE-FX 1310nm, 50 and 62.5 micron multi mode fiber
1000BASE-SX 850nm, 50 and 62.5 micron multi mode fiber
1000BASE-LX, 1310nm, 10 micron single mode fiber


Management port
100BASE-FX fiber port (Pro model only)
10BASE-T 100BASE-TX RJ45 connector
1000BASE-X/1000BASE-T fiber and copper port (Pro gigabit model only)

For the 10BASE-T/100BASE-TX Ethernet RJ-45 connection, connect one end of the RJ-45 connector to the top of the analyzer labeled 10BASE-T 100BASE-TX and connect the other end of the cable into your network.

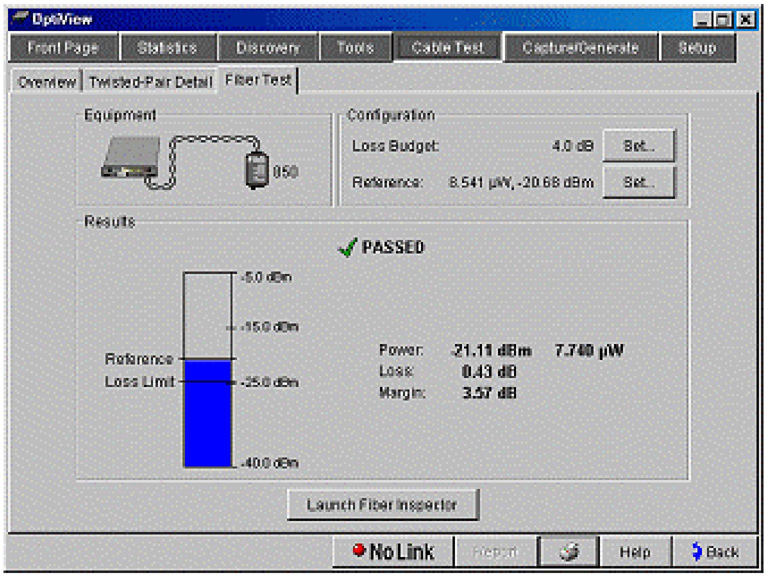
For a 100BASE-FX fiber connection (OptiView Workgroup Analyzer Pro and Pro Gigabit models), connect to the 100BASE-FX port making sure Tx and Rx are correctly connected. Remember, on the analyzer, light comes out of the Tx side, and light goes in the Rx side. Connect the other end of the fiber into your network.

The GBIC port (OptiView Workgroup Analyzer Pro Gigabit model only) supports 1000BASE-SX fiber, 1000BASE-LX fiber, and 1000BASE-T copper adapters. Each is ordered separately. Each flavor of GBIC uses a unique adapter which is inserted into the GBIC port.

Fiber Test Dialog

What is on this screen?

The results of the fiber optic cable test are displayed on this screen. Click on an area of the screen to see more about that function. For more details about testing fiber optic cable, check the Setting Up the Fiber Optic Test Kit topic.



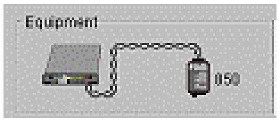
Loss Budget: 4.0 dB Set...

Reference: 8.541 µW, -20.68 dBm Set...

✓ PASSED

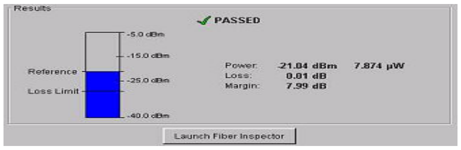
Power: -21.11 dBm 7.740 µW
Loss: 0.43 dB
Margin: 3.57 dB

Equipment



Ÿ Icons representing the Analyzer itself and the Fiber Optic Meter (FOM) connected to it are displayed. The FOM switch setting is shown (850, 1300, or 1550). If the FOM battery level is low, an indicator displays in this area.

Configuration



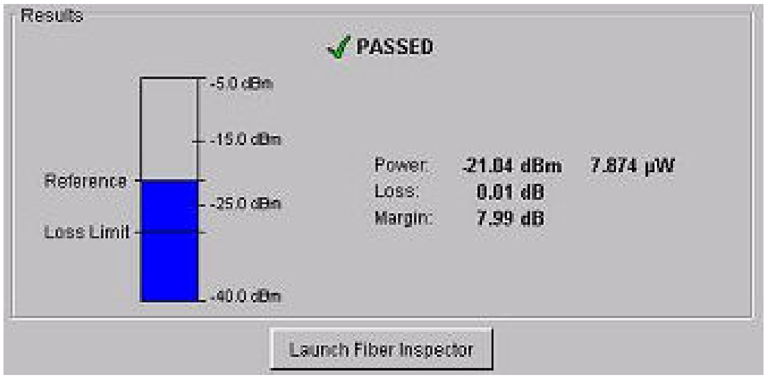
✓ PASSED

Power: -21.84 dBm 7.874 µW
Loss: 0.01 dB
Margin: 7.99 dB

Ÿ Loss Budget - Press **Set** (Set Loss Budget) to enter a Loss Budget value (1.0 - 20.0 dB). This value represents the amount of acceptable power loss. If, upon testing a cable, loss is greater than this value, the test reports "FAIL". Different cabling standards carry different loss limits.

Ÿ Reference - The reference power represents a baseline amount of power emitted by the source. This value is used as a reference from a "known good" patch cable to test other cables. The **Set** button records the current power reading as the new reference value. Configure the FOM and source with a short good cable before pressing the **Set** button.

Results



✓ PASSED

Power: -21.04 dBm 7.874 µW
Loss: 0.01 dB
Margin: 7.99 dB

Ÿ Analyzer displays messages based the results of the test:

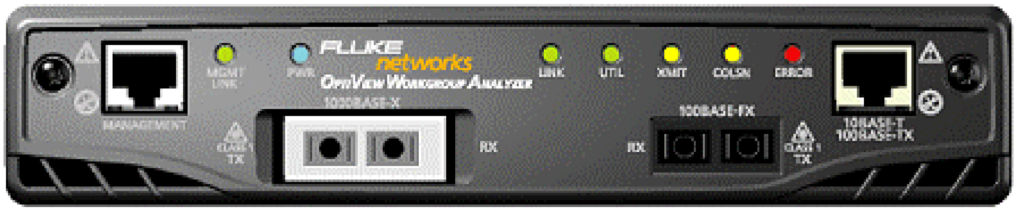
The Fiber Optic Meter is not connected
The Fiber Optic Meter is off
The FOM battery is too weak for reliable measurements
FAILED: Signal very weak. Light source turned off?
Power value is greater than reference!
FAILED: Signal loss exceeds the loss budget
PASSED

Ÿ Graph - A visual representation of the Loss Budget, Reference, and results.

Ÿ When the Analyzer detects a Fiber Optic Meter on the 10/100 TX interface, it continually displays the Power in both microwatts and dB on the right side of the Results section.

Ÿ If you have purchased the option, the **Launch Fiber Inspector** button initiates a separate program to visually inspect the ends of fiber cables. Contact Fluke Networks for more information about this option.

Front Panel LEDs



The LEDs on the front of the OptiView Workgroup Analyzer represent the following conditions:

Management Link (MGMT LINK): Indicates that link has been established on the Management connection (green). Flashing green indicates activity is present.

Power (PWR): Indicates whether the analyzer is Off or On (blue).

Link (LINK): Indicates one of the test interfaces is connected to the network and Link has been established. Blinking red = no link, green = link established via straight-through patch cable, yellow = link established via a cross-over patch cable.

Utilization (UTIL): Indicates the percent of utilization the network under test is experiencing (green = 0 - 49%, yellow = 50 - 79%, red = 80 - 100%).

Transmit (XMIT): Indicates analyzer transmit activity (yellow). When the analyzer is first powered on, it will generate transmit activity while trying to identify devices on the network. Ping, Trace Route, Trace Switch Route, and Traffic Generator will cause this LED to flash in proportion to the amount of transmit activity.

Collision (COLSN): Indicates by yellow flashing intensity the amount of Collisions being experienced on the network (yellow).

Error (ERROR): Indicates by red flashing intensity the amount of Errors being experienced on the network (red). The Ethernet layer 2 error types include CRC alignment, undersize, oversize, and jabber errors.

Print Button

The Print button 🖨 allows you to print the current screen to the default printer.

Report Button

The Report button allows you to generate tabular reports on select screens. The reports are saved to the c:\Program Files\Fluke Networks\OptiView\Reports folder. When the Report button is clicked, you are prompted to use the provided filename, or specify your own. The list of screens that reports can be generated on include:

- Statistics | Protocols
- Statistics | Top Hosts
- Statistics | Top Conversations
- Discovery | Devices
- Discovery | Networks
- Discovery | Protocols
- Tools | Ping | Trace Route
- Tools | SNMP Tables | Route Table
- Tools | SNMP Tables | ARP Table
- Tools | IPX Services
- Tools | Interfaces
- Tools | Trace Switch Route

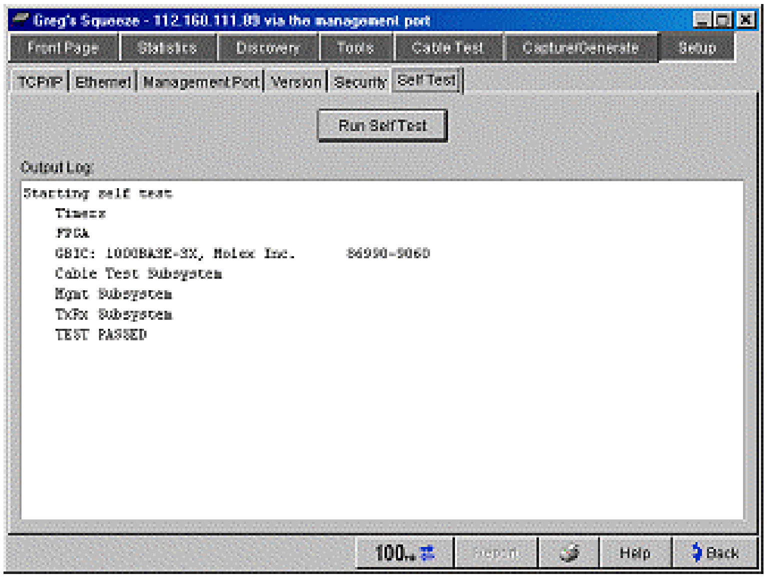
Rerun Test Button

Rerun Test allows you to clear the gathered statistics and discovery information. The Front Page screen is then updated with the latest network information.

Self Test

This screen is only available through the Management port. It provides access to the functionality verification tests available in the analyzer.

To execute the Self Test press Run Self Test. The Output Log will display the results similar to the following:



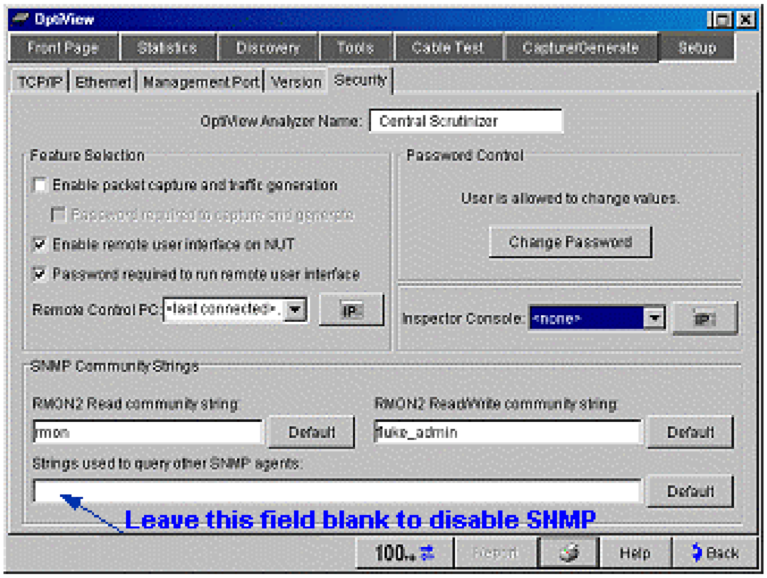
```
Starting self test
    Timers
    FPGA
    GBIC: 1000BASE-SX, Molex Inc.      86990-9060
    Cable Test Subsystem
    Mgmt Subsystem
    TxRx Subsystem
    TEST PASSED
```

If Self Test fails, contact Fluke Networks.

SNMP Security Issues

Some Networks may have SNMP traps enabled to detect a breach in security due to SNMP access by an unauthorized device. SNMP queries by this OptiView analyzer can be disabled, however this will limit Discovery.

To disable SNMP queries, simply go to the **Setup | Security** screen, and make the *Strings used to query other SNMP agents* field blank as shown below. This can be done by highlighting the existing string and pressing <Backspace>.



OptiView Analyzer Name: Central Scrutinizer

□ Enable packet capture and traffic generation

□ Password required to capture and generate

☑ Enable remote user interface on NUT

☑ Password required to run remote user interface

Remote Control PC: <last connected>

User is allowed to change values.

Inspector Console: <none>

RMON2 Read community string: rmon

RMON2 Read/Write community string: fluke_admin

Strings used to query other SNMP agents:

Leave this field blank to disable SNMP

Note: If SNMP is disabled, the status bar will indicate "SNMP disabled on this OptiView" for tools that require SNMP.

Switches Supported by the OptiView Integrated Network Analyzer

The analyzer's ability to discover switches and report VLAN, port/slot, and device list information is impacted by a vendor's use of private MIBs and protocols versus standard MIB and protocol implementations. What the analyzer can discover is very much dependant on how devices are configured and to what degree the standards have been implemented. The analyzer supports some vendors' private MIBs but not all.

The analyzer discovers switches through active SNMP queries and traffic monitoring. Switches are discovered with the following methods:

- Monitor management frame types -- Cisco Discovery Protocol (CDP), Bay Network Management Frame (SONMP)
- Monitor spanning tree frame types -- 802.1d BPDU, DEC Bridge Spanning Tree, Bay Network Bridge (Lattice) Spanning Tree
- SNMP queries - 802.1d Bridge MIB
- Private MIB queries - Cisco, Nortel LAN Switch List

In an effort to offer more information about the switch - VLAN number, port/slot number and devices on a port - the analyzer draws first from a vendor's Private MIB if supported, second from the Bridge MIB (Standard MIB) and third from the Interface Table. If a device supports VLANs, the vendor has generally implemented a private MIB.

If private VLAN or a non-standard Bridge MIB is not supported, the analyzer behaves as follows:

- May not find VLAN #, Slot #, Port #
- No listing of addresses residing on a port (non-standard Bridge MIB)
- Trace SwitchRoute fails (OptiView and OptiView Inspector Console)
- The slot and port information found in the interface table may not be easily correlated to information provided in the private MIB

Manufacturer Device Support

Note: The analyzer does not support non-std Bridge MIBs

3ComLink

- Switch 1000
- Superstack 610
- Superstack 1100
- Superstack 3000 Series

Cisco

- C350
- C1900/2820
- C2900 (private MIB support)
- C3100/3200 (private MIB support)
- C3500 (private MIB support)
- C4000 (private MIB support)
- C5000/5500 (private MIB support)
- C6000 (private MIB support)

- C8500 (private MIB support)

Dell Power Connect

- 3024
- 3048
- 3248
- 5012

Enterasys (Cabletron)

- SmartSwitch 2000
- Series SmartSwitch 6000
- Series SmartSwitch 9000
- Series SmartStack

Extreme

- Summit 24/48
- Alpine 3808/3904
- Summit 1i,4, 5i, 7i
- BlackDiamond 6808

Foundry

- FastIron II
- FastIron II Plus
- ServerIron XL

Hershman

- ALS Switches (no support for non-std forwarding database MIB)

Lucent Cajun (AVAYA)

- P110/120 (but no support for non-std Bridge MIB)
- Cajun P220/550/770/880/882

Nortel

- Baystack 70
- Baystack 350
- Baystack 450
- 28000 Series (private MIB support)
- 58000 (private MIB support)

The following switches do not support the standard Bridge Forwarding MIB, and thus will not show up in the Front Page as the nearest switch. They will however, show up in the **Discovery | Devices** screen in the Switch category.

- Passport (Accelar) 700
- Passport (Accelar) 8000
- Centillion 50
- Centillion 100
- Centillion 1000

User Events that may Terminate a User Interface Session

The active TCP/IP session between the user interface software and the analyzer can be severed under the following conditions:

When connnected via the management port.

- IP parameters are manually changed on the analyzer and Apply is selected in the Management port TCP/IP setup screen

When connected via the 10/100BASE-T, 100BASE-FX, or 1000BASE-X network test interface.

- **Auto Reconfigure on Network Change** is checked in the TCP/IP setup screen and the analyzer patch cable is disconnected and reconnected to another jack
- **Rerun Auto Configure** is selected in the TCP/IP setup screen
- **Find Unused IP and Apply** is selected in the TCP/IP setup screen
- IP parameters are manually changed and **Apply** is selected in the TCP/IP setup screen
- **Rerun Cable Test** is selected

In the previous conditions, the popup message "*This user interface and n others may lose connection to the remote OptiView. Proceed anyway?*" with **Yes** and **No** buttons displayed.

User Interface PC Requirements

Operating Systems:

- Win98 SE, WinNT 4.0 with Service Pack 5 or greater (with Administrative privileges), Win2000, and WinXP Professional

Minimum PC configuration:

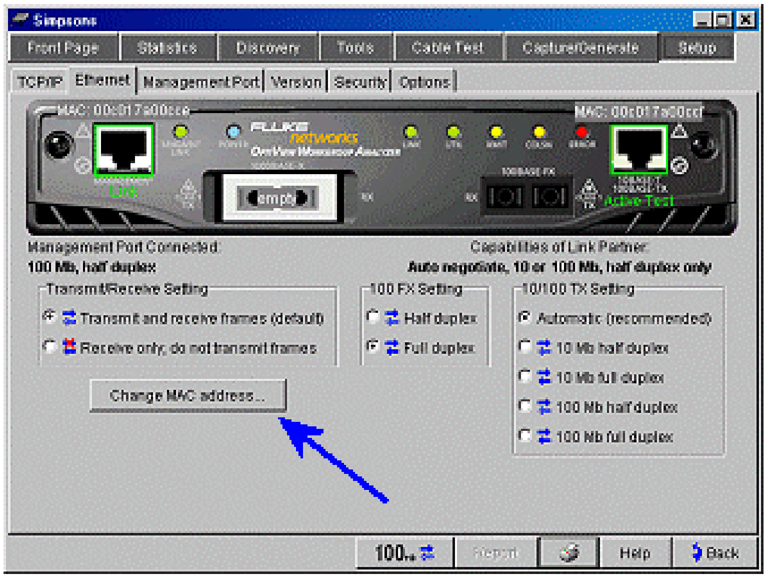
- The user interface install uses a temporary folder which requires a minimum of 32MB of temporary hard disk space
- Microsoft TCP/IP Stack
- Winsock 2.0
- 200Mhz MHz Pentium processor
- 64MB System RAM (Running multiple instances of the software requires more memory, i.e., 96 MB for 8 simultaneous sessions)
- 800 x 600 Video SVGA display
- 70MB MB hard drive space
- CD-ROM Drive

Security

Changing the Analyzer MAC Address

You may change the analyzer's MAC address. This may be useful to give it a MAC address that looks like a device on your network, rather than a Fluke Networks MAC address.

To change the OptiView Analyzer MAC address, go to the **Setup | Ethernet** screen and press Change MAC address... . The Change MAC Address popup is displayed where you can enter a custom OptiView Analyzer MAC address. Press the **Factory Default** button to restore the original analyzer MAC address. Press **OK** when finished for changes to be saved.



MAC: 00:c0:17:a0:0c:ce

MAC: 00:c0:17:a0:0c:cf

Management Port Connected:
100 Mb, half duplex

Capabilities of Link Partner:
Auto negotiate, 10 or 100 Mb, half duplex only

Transmit/Receive Setting
- ● Transmit and receive frames (default)
- ○ Receive only, do not transmit frames

100 FX Setting
- ○ Half duplex
- ● Full duplex

10/100 TX Setting
- ● Automatic (recommended)
- ○ 10 Mb half duplex
- ○ 10 Mb full duplex
- ○ 100 Mb half duplex
- ○ 100 Mb full duplex

Controlling Remote Access to the Analyzer

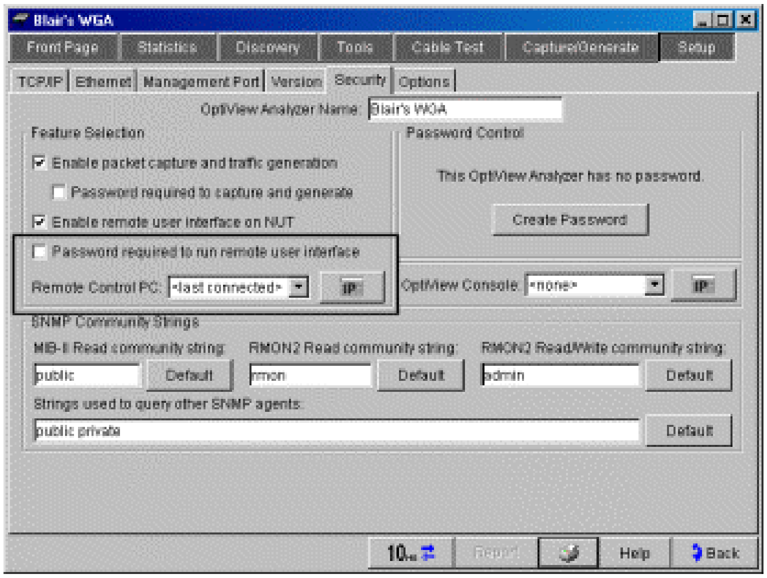
You can prevent unauthorized Remote User Interface access to an OptiView Workgroup analyzer by setting a password on that analyzer.

Note: If the password is changed by a remote user or via the serial configuration port, all remote users will remain active. New remote users will have to use the new password.

Setting Password Protection for Remote User Interface Access

Use the User Interface software to connect to the analyzer that you want to set the password protection on. Navigate to the **Setup | Security** screen and select the **Password required to run remote user interface** check box.

Note: The "Enter new password" dialog displays if a password has not been previously set. Enter a new password, and enter it again in the **Confirm new password** field, select **OK**, and the password is set.



OptiView Analyzer Name: Blair's WGA

Feature Selection

☑ Enable packet capture and traffic generation

☐ Password required to capture and generate

☑ Enable remote user interface on NUT

☐ Password required to run remote user interface

Remote Control PC: <last connected>

Password Control

This OptiView Analyzer has no password.

OptiView Console: <none>

SNMP Community Strings

MIB-II Read community string: public

RMON2 Read community string: rmon

RMON2 Read/Write community string: admin

Strings used to query other SNMP agents: public private

Setting the Remote Control PC Field

This field allows the analyzer to send out its identification to a remote PC. Then, when the PC specified in this field starts the OptiView Browser software, the analyzer will appear in the device list. This makes it easier to locate and select the analyzer from a remote site.

Set this field to <*none*>, <*last connected*>, or manually enter the IP address of the remote PC that will be running the remote user interface software. <*last connected*> is the last remote session to terminate from the analyzer, and that PC's IP address is saved into this field.

Note: <last connected> does not take affect until zero user interfaces are connected.

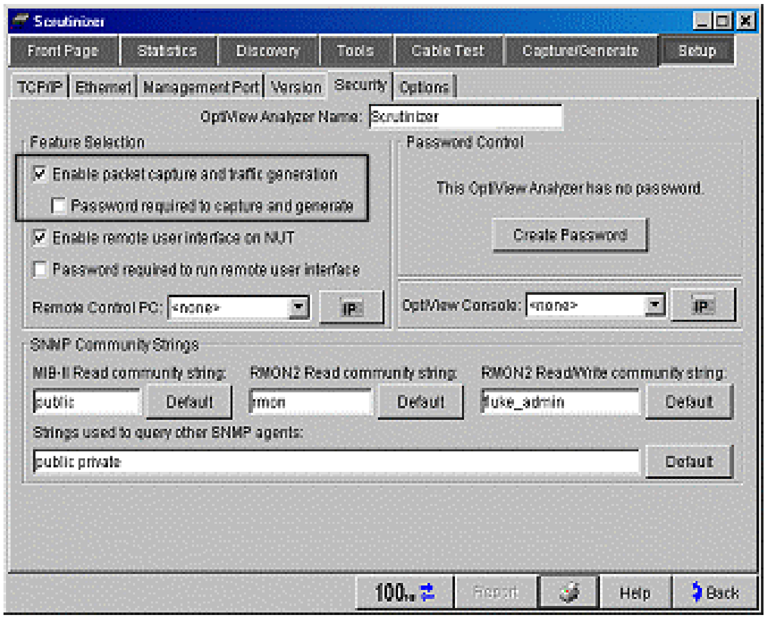
Controlling Access to Packet Capture and Traffic Generation

You can prevent unauthorized capturing of data by password protecting the analyzer's Packet Capture feature, and you can also prevent unauthorized remote access to a packet capture that is currently held in the capture buffer.

Setting Password Protection on Capturing Data (Packet Captures) and Traffic Generation

To prevent unauthorized access to the Packet Capture and Traffic Generation features, connect to the analyzer that you wish to set this security feature on and navigate to the **Setup | Security** screen, select the **Password required to capture and generate** check box. You must leave this screen for the setting to take affect.

Note: If a password has not been previously set, the **Enter new password** dialog displays. Enter a new password, and enter it again in the **Confirm new password** field, select **OK**, and the password is set.



OptiView Analyzer Name: Scrutinizer

☑ Enable packet capture and traffic generation

☐ Password required to capture and generate

☑ Enable remote user interface on NUT

☐ Password required to run remote user interface

Remote Control PC: <none>

This OptiView Analyzer has no password.

OptiView Console: <none>

MIB-II Read community string: public

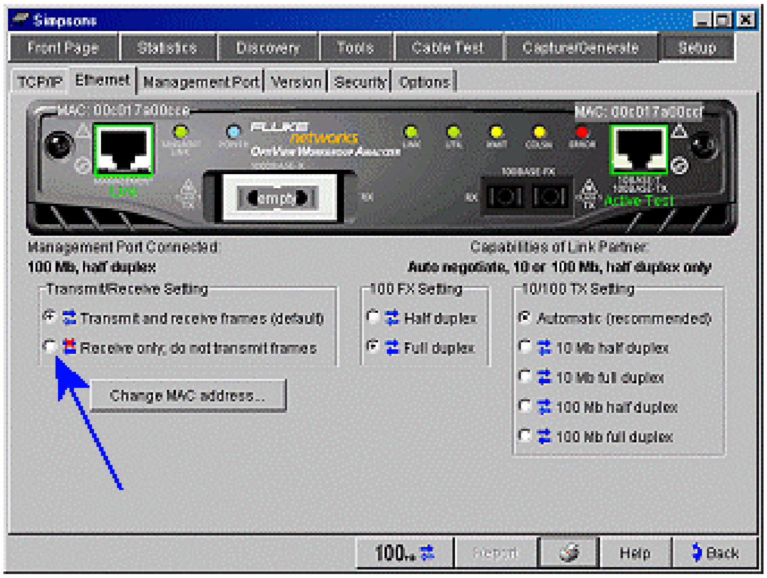
RMON2 Read community string: rmon

RMON2 Read/Write community string: fluke_admin

Strings used to query other SNMP agents: public private

Disabling Outgoing Traffic (Silent Mode)

In the **Setup | Ethernet** screen, the Transmit/Receive Setting field allows you to disable all transmit activity originating from the analyzer (◉ Receive only, do not transmit frames). This applies to Packet Capture, Traffic Generator, and during the analyzer discovery of devices and name resolving.



Management Port Connected:
100 Mb, half duplex

Capabilities of Link Partner:
Auto negotiate, 10 or 100 Mb, half duplex only

Transmit/Receive Setting
- ◉ Transmit and receive frames (default)
- ○ Receive only, do not transmit frames

100 FX Setting
- ○ Half duplex
- ◉ Full duplex

10/100 TX Setting
- ◉ Automatic (recommended)
- ○ 10 Mb half duplex
- ○ 10 Mb full duplex
- ○ 100 Mb half duplex
- ○ 100 Mb full duplex

Generally, the analyzer will not discover as many devices and resolve as many names with transmit frames disabled. Disabling transmit frames may be particularly important where analyzer generated frames are not allowed (silent mode). By default, transmit and receive frames are enabled.

Network Troubleshooting

First Aid for a Healthy Network

The key to successful troubleshooting is for the technician to know how the network functions under normal conditions. This enables the technician to quickly recognize abnormal operation. Any other approach is little better than a shot in the dark.

Unfortunately, many LAN products are not delivered with adequate performance specifications, theory of operation, or condensed technical data to aid in troubleshooting. The successful technician will thoroughly study whatever data is available, as well as develop in-depth insight into the function of all components and how to operate them. Finally, he or she will remember that conditions appearing to be serious defects are often the result of improper usage or operator error.

The foundation of this insight is gained only with formal training. But the true troubleshooting master learns in the trenches, through trial and error, comparing notes with others, and discovering tried-and-true methods that are not taught in school. The following information can help shorten your learning curve and give you proven advice on how to isolate and solve network problems.

Two approaches to troubleshooting almost always result in disappointment, delay, or failure. On one extreme is the theorist, or "rocket scientist" approach. On the other is the practical, or "caveman" approach.

- The rocket scientist analyzes and re-analyzes the situation until the exact cause of the problem has been identified-rather than simply pinpointing the root of the problem and correcting it. This sometimes requires taking a high-end protocol analyzer and collecting a huge (megabytes) sample of the network traffic while the problem is present and inspecting it in minute detail. While this process is fairly reliable, few companies can afford to have their networks down for the hours or days it can take for proper analysis.
- The caveman's first instinct is to start swapping cards, cables, hardware, and software until, miraculously, the network begins operating again. This does not mean it's working properly, just that it's operating. Unfortunately, the troubleshooting section in some manuals actually recommends caveman-style procedures as a way to avoid providing more technical information. While it may be faster, this approach is not very reliable, and the root cause of the problem may still be present. In fact, the parts used for swapping may include marginal or failed parts swapped out during prior troubleshooting episodes.

For the technician in search of the proper way to troubleshoot, the following approach makes the most sense:

Analyze the network as a whole rather than in a piecemeal fashion. One technician, following a logical sequence, will almost always be more successful than a gang of technicians, each with their own theories and methods for troubleshooting.

The logical technician asks the operator questions, runs diagnostics, and thoroughly collects information. In a short time, he or she can analyze and evaluate the symptoms, zero-in on the root source of problems, make one adjustment or change one part, and cure the problem. The key is to simply isolate the smallest failing element and replace it. Complete understanding of the cause of the failure is not required. After the network is again running, further analysis may be undertaken preferably in a lab environment.

There are many technicians with years of experience who have not yet mastered the following basic concept: a few minutes spent evaluating symptoms can eliminate hours of time lost chasing the wrong problem. All information and reported symptoms must be evaluated in relation to each other, as well as how they relate to the overall operation of the network; only then can the technician gain a true understanding of what they indicate. Once you have collected data about the symptoms, you will then need to conduct tests to validate or eliminate what you think the problems could be. Once you think you understand the problem, you must then verify it. At this stage your efforts will be directed toward attempting to cause the problem to recur on demand.

Just as important, the logical technician always performs a checkout procedure on any repaired equipment or system, no matter how simple the repair. Far too often, the obvious problem is the symptom of another less-obvious problem, and until the source is eliminated, the situation will continue.

Five Key Steps to Successful Troubleshooting

1. Collect all available information, and analyze the symptoms of failure.
2. Localize the problem to within a single network segment, to a single complete functional unit or module, or to a single user.
3. Isolate the problem to specific hardware or software within the unit, module, or user's network account.
4. Locate and correct the specific problem.
5. Verify that the problem has been resolved.

Note: To avoid unwanted repetition, and to make it possible to "back out" any changes made, be sure to carefully and to completely document all actions taken during the troubleshooting process.

Step 1. Collect information

First, ask yourself if you understand the symptoms. Have the operator explain how normal operation appears, then demonstrate the problem. Verify the reported problem yourself, if possible. Is there any normal function missing, or is there an abnormal response?

Determine whether something was altered at that station or on the network just before the problem started. Often the operator does not realize that changing something unrelated can cause problems on the network, such as rearranging the location of a portable heater or photocopier, or installing a new piece of software or adapter card.

Note: Check to be sure that you are not troubleshooting something that never worked before. Treat that situation like a new installation.

Step 2. Localize the problem

Once the problem has been confirmed, all available information collected, and an analysis made of what is known, the next step is to reduce the problem to a single segment or functional unit. Based on the analysis, determine whether the problem is related to a segment of the network, or localized to a single station. Reducing the scope of the problem in this way is where divide-and-conquer begins, and isolating the problem to the smallest unit in Step 3 is the goal.

Can the problem be duplicated from another station or using other software applications at the same station? Identify whether the problem is limited to one station, or one network resource such as a printer.

If the problem affects more than one station try a different hub for multi-segment networks.

Step 3. Isolate the problem

Step 3a. If the problem affects an entire network segment, isolate the problem by reducing the variables to the smallest possible number. Turn off or disconnect all but two stations. Once those two are communicating add more stations. If they are not communicating, check the physical layer possibilities such as the termination of the cable, the cable itself, or the specific hub port.

Step 3b. If the problem can be isolated to a single station, try a different network adapter, a fresh copy of the network driver software (without using any of the network software or configuration files presently found on that station), or connect a new network cable to that station. If the network connection seems intact, determine whether only one application exhibits the problem. Try other applications from the same drive or file system. Compare configurations with another workstation. Try a fresh copy of the application software (again using none of the existing software or configuration files).

Step 3c. If only one user experiences the problem, check the network security and permissions for that user. Find out if any changes have been made to the network security that might affect this user. Has another user account been deleted that this user was made security equivalent to? Has this user been deleted from a security grouping within the network? Has an application been moved to a new location on the network? Have there been any changes to the system login script, or the user's login script? Compare this user's account with another user that is able to perform the desired task.

Step 4. Correct the problem

Once a single operation, application, or connection is localized as the source of the problem, identifying the specific fault should be simple. For network hardware, it is most expedient to simply replace a part, and attempt to repair the part later. Remember: The goal is to restore full operation of the network as soon as possible.

Two avenues exist for solving software problems. The first option is to reinstall the problem software, eliminating possibly corrupted files and ensuring that all required files are present. This is an excellent way to ensure that the second option, "reconfiguring the software", works on the first try. Most new applications allow for a software switch that tells the configuration program to disregard any existing configuration files, which is a good way to avoid being misled by the error and duplicating it yet again.

If the problem is isolated to a single user account on the network, it is often easiest to delete the entire account and start over, or repeat the steps necessary to grant the user access to the problem application or operation as if the user had never been authorized before. By going through each of these steps in a logical order, you will probably locate the missing element faster than by spot-checking.

Step 5. Verify problem resolution

Ensure that the entire problem has been resolved by having the operator test for the problem. This can be done by simply operating the equipment in the "normal" way. Also, have the operator quickly try several other normal operations with the equipment. Sometimes a repair in one area causes other problems, and sometimes whatever was repaired turns out to be a symptom of another underlying problem.

Ethernet Errors

A certain number of normal errors can be expected on Ethernet under standard operating conditions. The most common error experienced on an Ethernet segment is a collision. Collisions are so common that the rules of Ethernet operation not only define collisions as being normal, but provide an explanation of how the segment should operate in the presence of a variable amount of collisions. The rules further explain that performance should not be adversely affected unless relatively heavy loads are experienced. The MAC layer of the Network Interface Card (NIC) is not expected to report collisions to the next higher layer.

Diagnosing Ethernet problems

Troubleshooting errors on Ethernet presents special problems, almost all of which are related directly to the bus structure of Ethernet. For messages to get from one station to another quickly, the bus structure delivers all messages nearly simultaneously to all stations within a collision domain (up to 1024 stations within approximately 2500 meters of each other). This also results in problems anywhere within the system appearing at all other parts of the system nearly simultaneously. Making the distinction between errors that are nearby and more distant errors requires a degree of skill, and often requires the divide-and-conquer approach to troubleshooting. To aid this process, it is important to understand the often minor differences between errors.

Description of error types

CRC Alignment Errors

CRC and alignment errors indicate a byte positioning problem in a packet. No level of CRC alignment errors is "normal" for an Ethernet LAN, but CRC errors above 3% (for overall network traffic) are considered excessive. Possible causes of CRC/Alignment errors include the following:

- noise (electromagnetic interference, lightning, high voltage cable)
- cable or cable connection problem
- a bad NIC or transceiver
- failure of a connected repeater or wiring hub port

If CRCs are coming from multiple stations, check grounding.

Solutions:

Identify the one or more stations that are generating errors. If you can attribute the CRCs to a single station, check the controller card or drop cable. A drop cable must conform to the 802.3 standard. In the case of twisted pair, check that wires are well twisted.

If errors are coming from multiple stations, it is likely that there is too much noise on your network. Sources of noise include lightning flashes, an electric motor, a high voltage cable and crosstalk. Make sure the network is well grounded.

Undersized Packets

Packets that are less than 64 bytes. These are usually caused by a faulty or corrupt LAN driver.

Oversized Packets

Packets that are more than 1518 bytes. These are usually caused by a faulty or corrupt LAN driver.

Fragments

A Fragment is an Ethernet frame that has a length less than 64 bytes and has a CRC/Alignment error. It can be generated by a collision or bad controller card. Fragments are considered to be problems on the network. Possible causes of fragments include the following:

- a bad NIC or transceiver
- a faulty LAN driver
- a problem on the other side of a concentrator or repeater
- a router not respecting frame size restrictions for two dissimilar network types

Solutions:

Identify the node(s) sending out excessive errors. If you detect that the source address of the fragment is always the same, check the NIC in the node. You may also want to check the version number of the LAN driver and replace it if it is old. If you suspect the fragments have filtered over from another segment (i.e., remote collisions), it may be that a specific node on another side of a repeater or concentrator has a bad NIC or transceiver. If so, you will have to troubleshoot with Packet Capture function and filter on the packet type Errors frames to capture fragments. Look for packets with "AA" or "55" (hex). These packets (padded packets) are sent by the repeater to tell you there are collisions on one of its sides.

Jabbers

Jabber is defined in the 802.3 standard as a frame longer than the maximum legal size (greater than 1518 bytes). However, there is no indication as to whether the frame has a good or bad FCS. In general, you should not see jabbers. The most likely causes of jabber are a faulty NIC and/or faulty or corrupt NIC driver files, bad cabling, or grounding problems. Possible causes of jabbers and oversize packets include the following:

- bad NIC or transceiver
- nodes jamming the network due to above normal collision rates

Solutions:

Identify the node(s) sending out excessive errors. If you suspect a jabbering transceiver, look at the transmit light to see if it is continuously transmitting. If yes, replace the transceiver.

Collision

Collisions occur when two nodes transmit at the same time, because of different cable types, and because interim devices between source and destination stations delay the signal. And, since not all equipment operates properly forever, and not all networks are constructed exactly according to the specifications, there are predictably some minor variations between one collision and another. These differences allow the distinctions listed below to be made.

If the collision is detected by the transmitting station(s) early enough, there may not be even a start frame delimiter (SFD) in the aborted message. Many network monitoring tools are unable to see collisions that occur in the preamble (before the SFD is transmitted) because they rely on the Ethernet chipset to pass information up the protocol stack. In normal Ethernet operation, the physical layer in the NIC does not forward any data to the data link layer until after the SFD has been seen. Special hardware is required to observe signals prior to the SFD.

When a collision is detected by a station that is transmitting, it will send a jam signal that is at least 32 bits long. The standard does not specify what the jam signal should look like (except it should not form a proper frame check sequence (FCS) for what was sent), so most NICs simply use a 10 or 100 MHz clock signal. If this clock signal is sent early in the message and replaces just the right part of the header, the destination or source address may translate to all A's, or all 5's. Repeaters detecting a collision on one port will send a jam signal on all other ports to ensure that all stations detect the collision. The portion of a message that is left over after a collision is sometimes known as a collision fragment, because the original message has been damaged and is no longer complete.

Description of causes and cures

There are two factors to remember when trying to isolate Ethernet problems. First, test results are often influenced by where on the segment the measurement is made and are substantially enhanced if the test device is generating traffic while it is monitoring. Second, because an Ethernet collision domain can be described as a distributed single point of failure, e.g., a problem detected in one area could be coming from a failure that is hundreds, or even thousands of feet away physically.

Knowing which specific errors are present will help you determine the causes of Ethernet network problems. However, because of the nature of a bus topology, your best approach in troubleshooting Ethernet is still the divide-and-conquer method of isolating problems. Keep dividing the segment until the smallest common denominator can be removed or replaced. So long as an error can be detected, there is a good chance of isolating it.

Cabling

The majority of LAN problems are cable-related. Cable problems can appear in many forms. If a FCS error is associated with many stations, it generally is traceable to bad cabling, a faulty hub port, or induced noise.

Noise source

Common sources of induced noise include fans, heaters, photocopiers, fluorescent lights, elevators, any type of electric motor, etc. These sources create short, powerful bursts or spikes of noise called impulse noise, which is what usually corrupts data.

The fastest way to isolate either cabling or noise problems is to test suspect cables with a cable tester. If the problem is intermittent, some cable testers can be used to run a long-term (i.e., 24 hours) test. Any noise spikes that occur during that period will be identified, helping to determine the cause of the noise by correlating the time of the event with what was occurring in the area. Replacing or rerouting the cable away from the noise source should solve the problem.

If poor cabling has been used throughout the network, errors may be reported by all stations. However, those with the longest cable runs will have the most problems. Poor-quality cable is very susceptible to electrical noise, and will typically present a variety of problems, usually intermittent. Use tools such as Fluke Networks' DSP Series cable tester, or the analyzer's Cable Test function to diagnose these problems.

Power problems

Bad AC power can cause hubs or concentrators to introduce noise into the cable system. The result is data corruption as it passes through the device.

Important: The power problem does not have to come from your office, your floor, or even your building. It could come from down the block or farther away, depending on what is connected between you and the substation. If your UPS power supply gives an overload alarm, but is reporting a load less than its rating, it is likely a harmonics problem. A Fluke 41 Power Harmonics Analyzer will help identify problems related to potentially dangerous harmonics in your electrical distribution system.

Bad cable or connector

Coax cables using BNC connectors are frequently the source of problems because of abuse by users. If the connector can be pulled free of the cable with moderate tension, the connection should be re-terminated. UTP cables are often constructed improperly. Typical problems include using wire pairs that are not twisted, using multi-wire (stranded) RJ-45 connectors for solid core wire (or the opposite), low-quality wire, punch-down blocks and patch panels (that do not meet even Category 3 requirements), etc. Use tools such as Fluke Networks' DSP Series cable testers, or the analyzer's Cable Test to diagnose these problems.

Cable too long

If a cable is too long, it may cause excessive loss of bandwidth to collisions, or in extreme cases late collisions. A network that is too long is one in which the end-to-end signal propagation time is greater than the minimum legal-sized frame.

Note: It is unlikely that simply too much cable is the cause of late collisions, as it would require more than five kilometers of cable. Parameters such as attenuation and NEXT have a greater effect than simple length. Station drop cables that exceed the specified maximums may result in dropped connections for the station that is attached to the network through that cable.

Faulty or misconfigured NIC

A faulty NIC can be the source of virtually all types of Ethernet errors. In most cases though, the problem can be traced to improperly configured software driver files or cable problems. Errors such as short frames and FCS errors from a single station are most often configuration or corrupted-driver problems. Errors such as late collisions and jabbers are often caused by marginal or failed hardware.

Hard fault

On coaxial networks the incidence of hard failures is substantially increased because users often do not understand that while there is no problem removing the tee connector from the back of their PC, removing either of the cables from the tee connector causes the network to fail. Similarly, the function and placement of termination resistance is not understood, nor is the reason for forbidding stub cables to be attached to the tee connector (which is sometimes done when a PC is moved).

Illegal hardware configuration

The common bus architecture and variety of cabling options permit users to construct Ethernet networks into a variety of interesting and creative designs. Unfortunately, this also means there are a variety of interesting and creative ways to violate the rules defined in the standard. Worse still, the protocol is robust enough to mask many minor and some major violations at low to moderate utilization rates. This means that when utilization increases significantly, typically at the worst possible times during the workday, performance of poorly designed or poorly installed networks will drop off rapidly, and the network may cease operating altogether. Correcting problems related to standards violations often requires long hours of physical inspection of all cables and connections. If this is necessary, it is strongly recommended that a complete set of network documentation be developed at the same time. This will help avoid similar problems in the future, and will greatly facilitate troubleshooting when problems do occur.

Addressing/routing

When troubleshooting Ethernet problems, it is important to remember that Ethernet MAC addresses can cross hubs, switches, and bridged connections. But they will never cross routed connections. The local MAC address of the router is used when a message is retransmitted on a new segment, while the source and destination network-layer address is undisturbed.

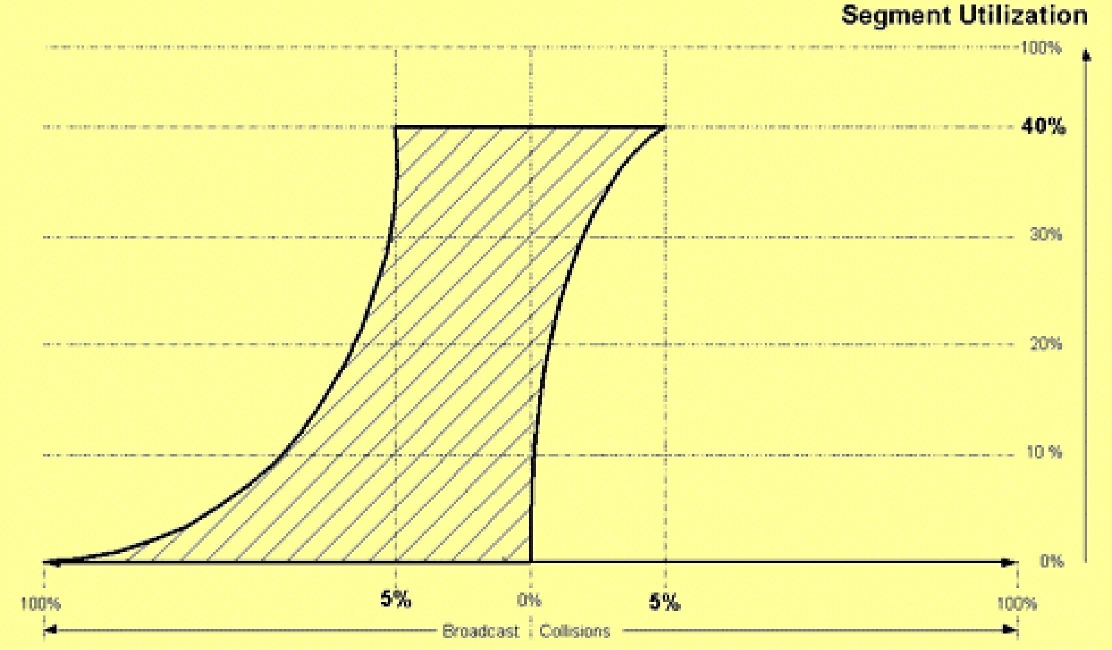
Also, an Ethernet collision domain crosses hub and repeater connections, but stops at bridges and routers. That means that errors affect all stations on this side of a bridge or router; however, depending on the technology implemented in a switch, the collision domain may extend partly into the next segment. If the switch is using store-and-forward technology, it may be thought of as a bridge. But if the switch is using cut-through technology, then many errors are forwarded before the switch realizes that the frame has an error. If the first half of the frame is intact (at least 20 bytes good), then the switch will have already begun forwarding regardless of what follows. More sophisticated switches will temporarily change from cut-through to store-and-forward if the error level on a port goes too high.

Interpreting Network Activity

When analyzing utilization, collisions, broadcast and errors, it is essential to understand the interaction between these critical network parameters. The Rule of thumb is 40, 5, 5, 0.

The 40, 5, 5, 0 Rule

Utilization should not exceed an average of 40%. Collisions and Broadcast should each not exceed an average of 5%. In general, no errors should exist. Although errors should not be present, a small amount may occur when the collision rate is high. Errors present without collisions are a "red flag" and should be investigated.



Interpreting the Graph

The following values will assist you when interpreting the Segment Utilization graph.

Note: Readings that fall within the "lined" area denote that the local segment is healthy. Readings outside of this area should be investigated.

Utilization: This value displays the total amount of bandwidth consumed by local traffic. 100% represents line rate of the media (10Mbps, 100 Mbps, etc.) Traffic is considered to be frames on the segment that are valid or invalid (i.e., fragment frames caused by collisions.)

Collision: This value displays the total amount of frames colliding with each other on the local segment. The displayed value is a percentage of Utilization. Example: If the collision value displayed is 10%, and the utilization is 60%, then 10% of the 60% is collisions, 6% (at 10Mbps) of all the segment traffic is collisions.

Broadcast: This value displays the total amount of traffic that is not data, being placed on the local segment devices, i.e. advertisement from PC's and printers. This displayed value is also a percentage of Utilization. Example: If the broadcast value displayed is 20% and the utilization is 50%, then 20% of that 50% is broadcast traffic, or 10% (at 10Mbps) of all traffic on the segment is broadcast traffic.

Error: Although not reflected on the graph, this value displays the total amount of errors (invalid data) such as Frame Check Sum, Jabbers or Runts on the local segment. This value is a percentage of Utilization. Example: If the error value displayed is 5% and the utilization is 50%, then 5% of the 50% is error traffic, or 2.5% (at 10Mbps) of all traffic on the segment is error traffic.

To calculate the percentage of overall bandwidth consumed by Utilization, Collisions, Broadcast, or Errors, use the following formula:

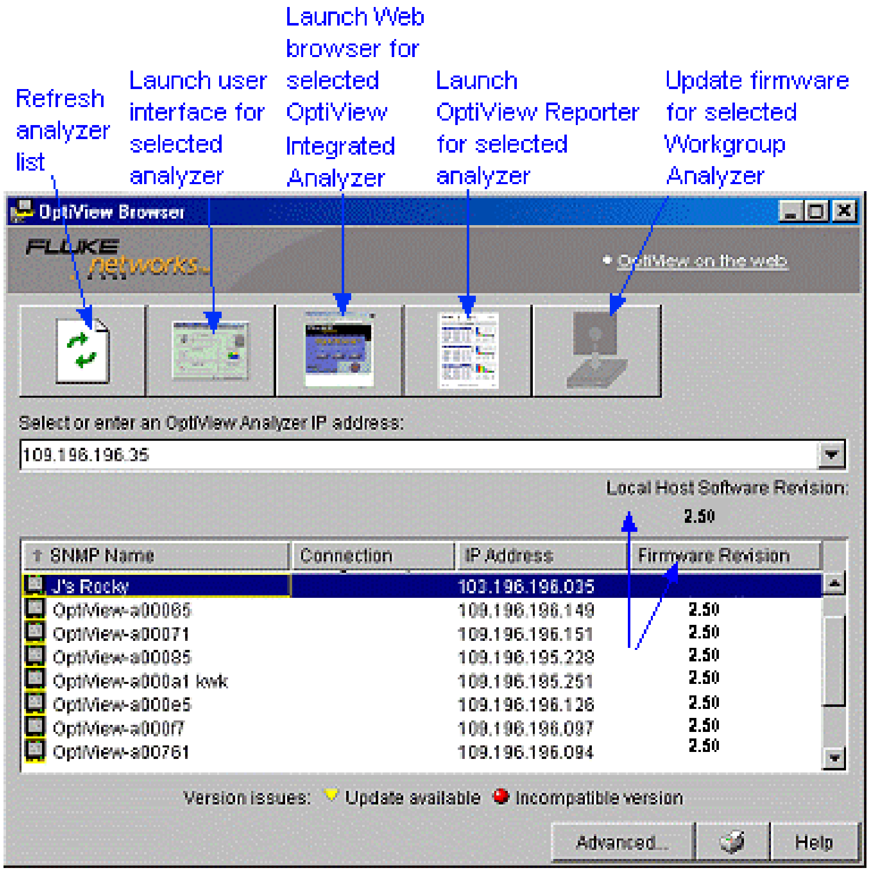
$$\frac{\text{\%Collisions, or \%Errors, or \%Broadcast} \times \text{\%Utilization} \times \text{Line Rate (10Mbps)}}{\textbf{Line Rate (10Mbps)}} \times \mathbf{100 = \%\ of\ bandwidth\ consumed}$$

Using the OptiView Browser

Using the OptiView Browser

The OptiView Browser is the first screen presented when the OptiView remote user interface is run on your PC. The OptiView Browser allows access to OptiView Integrated and Workgroup Analyzers through a browseable user interface.

Note: For the latest release of the OptiView Browser and user interface software, visit www.flukenetworks.com.


Refresh analyzer list
Launch user interface for selected analyzer
Launch Web browser for selected OptiView Integrated Analyzer
Launch OptiView Reporter for selected analyzer
Update firmware for selected Workgroup Analyzer
OptiView Browser
FLUKE networks
• OptiView on the web
Advanced...
Help

Select or enter an OptiView Analyzer IP address:

109.196.196.35

Local Host Software Revision:

2.50

SNMP Name	Connection	IP Address	Firmware Revision
J's Rocky		103.196.196.035	
OptiView-a00065		109.196.196.149	2.50
OptiView-a00071		109.196.196.151	2.50
OptiView-a00085		109.196.195.228	2.50
OptiView-a000a1 kwk		109.196.195.251	2.50
OptiView-a000e5		109.196.196.126	2.50
OptiView-a000f7		109.196.196.097	2.50
OptiView-a00761		109.196.196.094	2.50

Version issues: ▼ Update available ● Incompatible version

Note: If a gold shield ▼ appears by Local Host Software Revision number, an update is available for the UI software. If the gold shield appears by the Firmware Revision number of an OptiView found on the network, that OptiView has old firmware and an update is available for it.

In the OptiView Browser window, double-click on an analyzer from this list and the user interface is launched. If an analyzer is password protected, you will be prompted to enter a password.

In order for analyzers that are not in the same local network (broadcast domain) to be displayed in the OptiView Browser list, you must first connect to your analyzer(s) using the Remote User Interface software and configure the Remote Control PC address setting. This is found in the analyzer's **Setup | Security** screen. The Remote Control PC address should match the IP address of the PC that you intend to run the user interface software on. Then, the remote analyzer will send its identification back to the controlling PC. The Remote Control PC address may also be set through the analyzer's Serial Interface Port.

OptiView Browser Navigation

Refresh analyzer list

Re-displays the analyzer list with current active analyzers. Analyzers that are not in the same local network which have their Remote Control PC address set to this PC will appear in this list within 15 seconds.

Launch user interface for selected analyzer

Launches the user interface software to the selected analyzer. The selected analyzer is the analyzer that is highlighted in the OptiView Browser analyzer list or the IP address entered in the **OptiView Browser IP address** field.

Launch Web browser for selected OptiView Integrated Network Analyzer

Enabled only for OptiView Integrated Analyzers and not for OptiView Workgroup Analyzers. Launches the default web browser on your PC and connects to the home page on the selected OptiView Integrated Analyzer. From the home page, you can access saved reports, packet capture files located on the OptiView Integrated Analyzer's hard drive, and install the remote user interface software on your PC.

Launch OptiView Reporter for selected analyzer

Launches the OptiView Reporter software application. The Fluke Networks OptiView Reporter software application provides you with a simple way to generate a variety of reports based on data obtained from analyzer connected to your network.

Update firmware for selected OptiView Workgroup Analyzer

Updates the analyzer's firmware by downloading the needed files from the controlling PC. Enabled only when selecting an OptiView Workgroup Analyzer through the Management port. It does not apply to OptiView Integrated Network Analyzers.

Recovering from an Interrupted Analyzer Firmware Update

When an analyzer firmware update is taking place, the firmware is being transferred from your PC to the selected analyzer via an FTP server connection (the FTP server application is part of the analyzer user interface software on your PC).

If your computer or network connection fails in the middle of the transfer, press Advanced..., and then Start FTP Server to restart the FTP server application and resume the analyzer firmware update. When the update is complete, press Stop FTP Server to close the FTP server connection.

Note: Only one FTP server connection can be run on a PC at a time.

Versions Issues

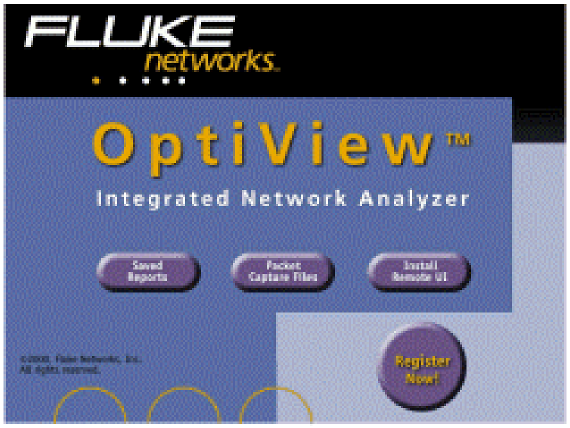
▼ **Update available** - If a gold shield ▼ appears by Local Host Software Revision number, an update is available for the UI software. If the gold shield appears by the Firmware Revision number of an OptiView found on the network, that OptiView has old firmware and an update is available for it.

● **Incompatible version** indicates the analyzer firmware is not compatible with the user interface software on your PC. You will need to update the analyzer firmware by selecting the button, and following the on-screen instructions.

Installing the User Interface Software

The user interface software can be installed on Win98 SE, WinNT 4.0, Win2000, and WINXP operating systems.

To install the user interface software, either run the install Install Remote UI from the analyzer home page as shown below,



or execute the file Launch.exe located in the root directory of the supplied OptiView Resource CD. Follow the on-screen instructions to complete the installation.

Once the installation is complete, you will be able to launch the OptiView Browser from your desktop, select an analyzer from the OptiView Browser list, or enter the analyzer's IP address, and gain access to valuable network information through the analyzer's user interface.

After selecting an analyzer from the OptiView Browser and launching the user interface. The first screen to appear is the Front Page screen. When you select an analyzer from the

OptiView Browser list, you may either double-click on it or click the **Launch** button.

See also, User Interface Events that will Terminate a Remote Session.

Screen Level Help by OptiView Tab

Front Page

Front Page

What is the Front Page screen all about?

Front Page is the first screen that appears after power-up. This screen is intended to provide you with everything needed to monitor and test your network. This screen provides an overview of your network by presenting the closest switch (seen in the Switch Statistics block), any network problems (seen in the Problem Discovery block), all connected devices (seen in Device Discovery block), statistics (seen in the Protocol and Utilization Statistics blocks), etc. The health of your network is discovered and at a quick glance presented to you.

What does the Front Page Do For You?

At startup, a representation of the network cable attached to the analyzer (if present) appears. (Cable presence is auto-detected). Initially, the **OptiView** button and cable are the only elements shown. After the cable test has completed, the remaining screen elements appear.

The remaining buttons provide an indication of their respective areas. The total combined information provides a "signature" of the network letting you know how things are going. This information will allow you to quickly dismiss some hypotheses during troubleshooting without "drilling-in" only to have to back out. Buttons show a green check mark or red X to draw your attention to probable problem areas.

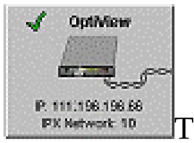
Screen Components

OptiView on the web opens the OptiView Home web page where you can then go to the Fluke Networks web site. Go to Fluke Network's web site for late breaking news, support, and software updates.

Rerun Test **Rerun Test** allows you to clear all statistics and discovery information, and restart all network device discovery. Cable Test is not rerun. Cable Test is rerun when a cable change is detected.

0 **Remote Sessions** displays the number of users connected to the analyzer through the OptiView user interface software. The number to the left of the workstation icon can be from 1 to 8 users.

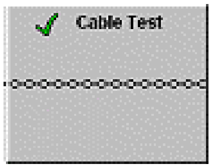
When you select this button, the Remote Sessions dialog is displayed. This dialog displays the Name, IP Address, MAC Address, Test Port, and Management Port number of each host connected to the analyzer. A single PC can connect multiple times to an analyzer. It can also connect through the management port and 10/100/1000 Mb interface (Test Port).



The **OptiView** analyzer button represents the configuration status of the analyzer. A ✓ or ✗ in this block indicates the status of the analyzer. ✓ indicates that the analyzer has a valid IP address within the subnet of the connected location.

If a valid IP address was not found, the analyzer will still be able to analyze traffic for statistics, and discover devices. However, without a valid IP address, the analyzer will not be able to actively discover names or use the features in the **Tools** screen. Clicking on the **OptiView** analyzer button takes you to the **Setup | TCP/IP** network configuration screen.

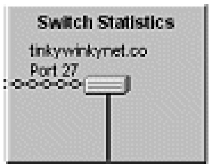
Note: A ✗ in this block indicates that the analyzer does not have a source IP address, or that the analyzer has misconfigured TCP/IP settings. Look in the TCP/IP screen's status bar for the type of error message.



The **Cable Test** button summarizes the status of the copper or fiber cable:

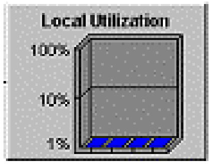
a) ✓ no problems found.

b) ✗ indicates there is a problem with the cable. Status for the other blocks/buttons on this screen are dependent on the cable test passing. Clicking on the **Cable Test** block/button takes you to the **Cable Test | Overview** screen for more detail.

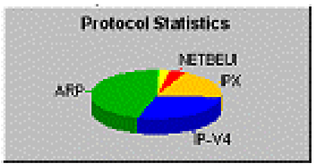


The **Switch Statistics** button displays the nearest switch (including Slot, port, and VLAN ID if available) discovered by examining the bridge forwarding tables of all the local switches. Selecting this button takes you directly to the **Tools | Interface** screen for this switch.

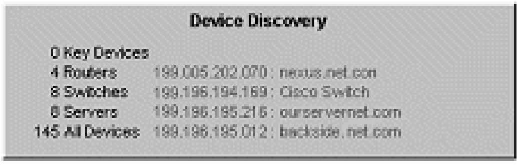
Note: The Switch Statistics block will show the nearest switch that the analyzer can talk to via SNMP. The displayed switch may not actually be the nearest switch if the analyzer does not have the proper community strings configured, or the nearest switch does not support the forwarding database in the Bridge MIB.



The **Utilization Statistics** button shows network unicast, multicast, broadcast, collisions, and error percent detail for the connected network segment. Clicking on this button navigates to the **Statistics | Utilization** screen where information is provided in both tabular and graphical views.



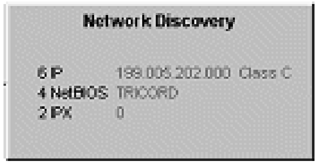
The **Protocol Statistics** button shows protocol mix information. The analyzer continuously updates the protocol list based on protocols used on the network segment the analyzer is connected to. Clicking on this button takes you to the **Statistics | Protocols** screen for more detail.



Device Discovery

0 Key Devices
4 Routers 199.005.202.070 : nexus.net.con
8 Switches 199.196.194.169 : Cisco Switch
8 Servers 199.196.195.216 : ourservernet.com
145 All Devices 199.196.195.012 : backside.net.com

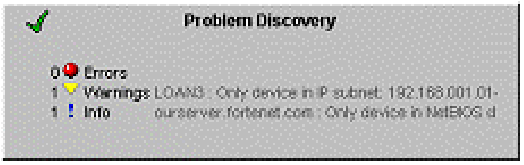
The **Device Discovery** button summarizes the device discovery process. Specific address and domain names are given. Network interconnect devices and servers are broken out along with the total number of hosts. The number of devices provides a signature of the network. Example devices are shown by category. The names and addresses of the devices are given to help "ground" you. Device Discovery is periodically cycled and updated. Clicking on this button takes you to the **Discovery | Devices** screen.



Network Discovery

6 IP 199.005.202.000 Class C
4 NetBIOS TRICORD
2 IPX 0

Network Discovery summarizes the network discovery process. IP Subnets, NetBIOS Domains, and IPX Networks are displayed. Clicking on this button takes you to the **Discovery | Networks** screen.

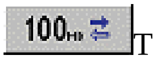


Problem Discovery

0 ● Errors
1 ▼ Warnings LOAN3 : Only device in IP subnet: 192.168.001.01-
1 ! Info ourserver.fortenet.com : Only device in NetBIOS d

The error ● , warning ▼ , and info ! icons shown on the **Problem Discovery** button are used throughout the user interface to tag problem devices. Problem Discovery is periodically cycled and updated. Clicking on this button takes you to the **Discovery | Problems** screen.

Status Bar Buttons



This button indicates the link speed, and duplex mode (shown by solid and outlined arrows). In this example it shows a 100 Mbit half duplex connection (one solid and one outlined arrow). Two solid arrows represents full duplex. Click this button to go to the **Setup | Ethernet** screen.

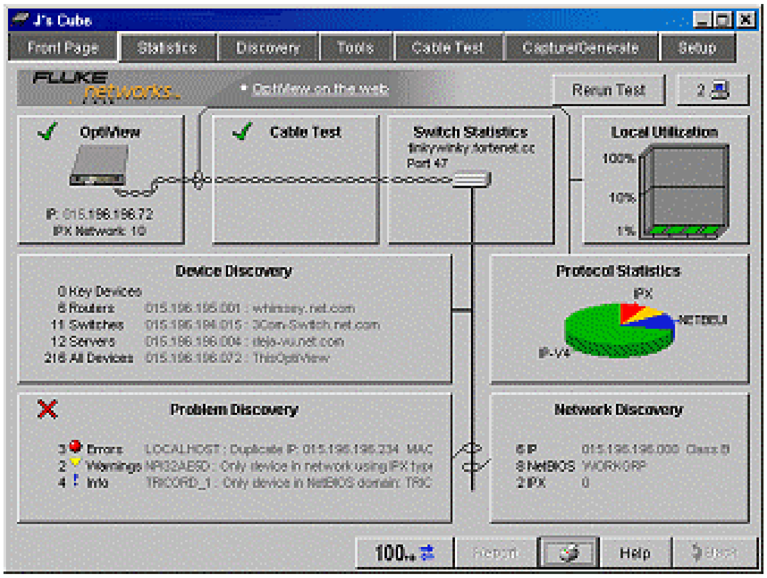
This button generates tabular HTML reports on select screens. The reports are stored in the analyzer installation directory under \Reports (C:\Program Files\Fluke Networks\OptiView\Reports). When this button is clicked you are prompted to specify a filename or to use the default name provided.

This button opens the help system and will display help information on the current screen.

This button works in conjunction with buttons containing the forward arrow . When going to a screen using a forward arrow button, the Back button then returns you to that particular screen.

Front Page Screen Help

Select any area on the graphic below for more information.



IP: 015.196.196.72
IPX Network: 10

Switch Statistics
tinkywinky.fortenet.cc
Port 47

Device Discovery

```
  0 Key Devices
  8 Routers      015.196.195.001 : whimsey.net.com
 11 Switches     015.196.194.015 : 3Com-Switch.net.com
 12 Servers      015.196.196.004 : deja-vu.net.com
216 All Devices  015.196.196.072 : ThisOptiView
```

Problem Discovery

```
3 ● Errors    LOCALHOST : Duplicate IP: 015.196.196.234  MAC
2 ▼ Warnings  NPI32AE5D : Only device in network using IPX type
4 ! Info      TRICORD_1 : Only device in NetBIOS domain: TRIC
```

Network Discovery

```
6 IP       015.196.196.000  Class B
8 NetBIOS  WORKGRP
2 IPX      0
```

Statistics

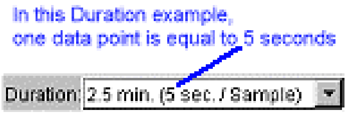
Utilization

Utilization provides a historical analysis on the performance and health of the network segments across your network including the segment to which the analyzer is connected.

The Utilization graph is broken out by percentage of utilization on the y-axis, and time on the x-axis. Time is divided into 30 bars, each bar representing one sample period.

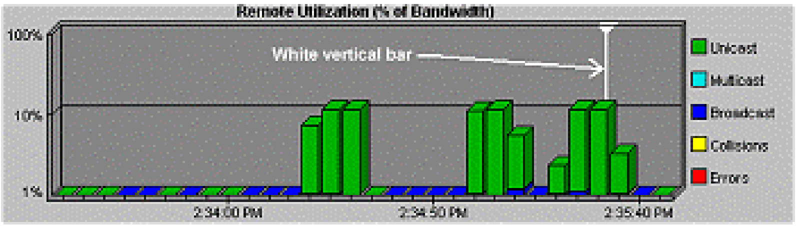
A bar is one sample period. The first bar will not show until the RMON device has been up and running longer than the sample period.

For example, a Duration of 2.5 minutes, with a sample period of 5 seconds per sample (see Utilization graph below), will take 5 seconds before the first bar will display. Unicast, Multicast, Broadcast, Collisions/Fragments (for "ThisOptiView", just Collisions for other devices), and Error counts are displayed in this screen.



In this Duration example, one data point is equal to 5 seconds

Duration: 2.5 min. (5 sec. / Sample)



You can select a device on your network through the Data Source drop-down box to view History studies. Devices with multiple ports can be further drilled down to a specific port by selecting the port number from the Interface drop-down list (Interface is gray if only one port exists or it supports history for that device).

Note: Data Source is a list of RMON/RMON2 devices that have History studies enabled. Only devices that have RMON History studies enabled will show in the Data Source list.

Errors

The total number of errors is displayed in the table below the Utilization graph. Clicking on the **Errors** button breaks out the errors by CRC Alignment Errors, Undersized Packets, Oversized Packets, Fragments (see note below), and Jabbers. The sum of the errors displayed in the **Errors** screen represents the total error total displayed in the **Utilization** screen. Both the Utilization and Error tables are relative to the position of the white vertical bar in the Utilization and Errors graphs. You will notice the tabular data will reflect utilization (or errors) for the sample period by the position of the white vertical bar. See also Ethernet Errors.

Note: When "ThisOptiView" is selected in the **Data Source** field, the **Utilization** screen shows the combination of collisions and fragments (Collisions/Frags), and fragments are not reported in the **Errors** screen. The analyzer COLLISION LED also shows combined collisions and fragments. It should be noted, under normal circumstances, virtually all fragments are due to collisions, and reasonable levels do not indicate any network problem.

For all other devices selected in the **Data Source** field, collisions are reported in the **Utilization** screen, and fragments are reported in the **Errors** screen. This is to be consistent with typical RMON applications displaying collisions separately from fragments.

Sample/Bucket Time Stamp: Each sample (a sample/bucket is one bar in the graph) is annotated with the time from the beginning of the sampling period. For example: a sample with a 30 minute duration that started at 8:00:00 AM and ended 8:30:00 AM will be annotated with 8:00:00 AM.

Screen Components

Data Source

Allows you to select the switch port or RMON probe on which to view history studies. For remote data sources, statistics will be relative to the remote device instead of the analyzer. The analyzer will use the RMON History group to gather statistics information.

The analyzer will automatically query all discovered hosts for RMON History data sources using the configured community strings. Check the community string settings (in the **Setup | Security** screen) if RMON devices that have History studies enabled do not appear in the **Data Source** field.

Note: There may be fewer History study entries in this screen than in the **Tools | Interface** screen's MIB 2 Interface Table. This screen shows the list of configured History studies. Switches can be configured to have History studies on any number of their interfaces. The **Tools | Interface** screen shows all configured History studies.

Interface

When a device selected in the **Data Source** field has more than one port (or interface), then this field allows you to select a specific port on a switch to gather statistics. The analyzer will automatically discover all interfaces that support RMON History.

Duration

Based on the pre-configured RMON History studies for the selected device (and interface), you can choose from any of the existing History durations. The analyzer will automatically discover all RMON History studies for devices that support RMON History.

Note: The graph is divided into 30 bars. The Duration and sample period selected may or may not fill all 30 bars initially. As time progresses the graph will be populated.

For example, a switch port is selected that has a history duration of 2 minutes, and sample period of 30 seconds (2 minutes divided by 30 seconds = 4 bars/sample periods) will initially show 4 bars in the graph with new data being updated in the graph as it is reported. The new "bars" will populate from right to left. Soon the entire graph will be populated with new data.

View

The Utilization screen will display either utilization or error information depending on the view selected.

Select Sample

The ◄ ► buttons position the graph's white vertical bar over a specific sampling period on the graph. You may also position the white vertical bar using the cursor, e.g., clicking with your mouse on the graph to move the white vertical bar and display that sample period's history.

The **Pause** button ⏸ is a convenient way to stop the graph to view interesting data before it marches off the screen. Samples that leave the left side of the graph can not be seen again. Clicking on the ⏸ button again resumes displaying current data.

Other Interesting Things About the Graph

Initially, the white vertical bar is on the right side of the graph. As data is displayed, the white vertical bar remains in the right position. Each new sample period (bucket) moves under the white vertical bar and its data is displayed below the graph.

When you move the white vertical bar off the right side and place it on a specific sample period, it remains on that sample period. It remains on that sample period even as new data is being updated until the white vertical bar and sample period march off the left side of the display. At that point the white vertical bar flips to the right side of the graph and remains.

The graph is always divided into 30 sample periods (buckets) regardless of the duration and sample period of the RMON History study.

Note: Top Talkers, Top Multicasters, Top Broadcasters, and Top Errors are grayed and disabled if any other Data Source is selected other than the analyzer. These buttons provide information that is relative to the LAN segment to which the analyzer is physically connected.

Protocols

The Protocols screen displays the current list of active protocols as seen on the network segment to which the analyzer is connected.

Note: The Protocol list is always relative to the network segment the analyzer is connected to, even when another data source is selected.

The left column on this screen is the protocol tree. This list is continually updated. The analyzer can detect many more protocols than typically appear in the list. For a complete list of protocols the analyzer can detect, see the expanded protocol list. For definitions of the top level protocols, see the protocol definition list.

The right side of this screen displays protocol information in either tabular ▦ or pie chart ◕ format. The protocol(s) selected in the left column of this screen determines which protocols and sub-protocols are displayed in the right column. In the tabular ▦ view, the right side of the screen displays the protocol(s), packet size, and octet size. You may sort by packet or octet size by clicking on the packet or octet column header.

Screen Components

Clear Counts resets all counts for Protocols, Top Hosts, and Top Conversations.

Top Hosts takes you to the Top Hosts screen indicating the top talkers for the selected protocol.

Top Conversations takes you to the Top Conversations screen indicating the top conversations for the selected protocol.

Filter takes you to the Packet Capture Filter screen with the highlighted protocol preloaded in the filter setup.

Sorting

The table (right pane) can be sorted by selecting either the Packets or Octets column heading (descending order only).

Top Hosts

Top Hosts displays the top 50 transmitting or receiving hosts (devices) for the specified protocol on the network relative to the LAN segment the analyzer is physically connected to. Top Hosts includes any hosts that are generating error packets. Error packets that Top Hosts recognizes includes: undersized packets, oversized packets, CRC alignment errors, and jabbers.

Note: Collision fragments do not show up in Top Hosts because the MAC address that is displayed is typically meaningless and a small percentage of collision fragments are normal.

An asterisk (*) in the manufacture prefix symbolic MAC address indicates the Locally Administered bit is set. A pound sign (#) indicates that the Multicast bit is set. For example:

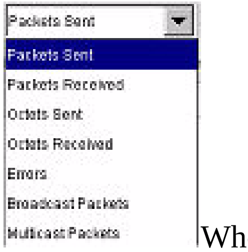
- 3Com*1fd04d is the symbolic MAC for 0250da1fd04d
- DEC#16.30 is the symbolic MAC for ab0004001e40

Top Hosts is dependent on whether destination addresses (e.g., **Packets/Octets Received**) or source addresses (e.g., **Packets/Octets Sent**) is selected at the top of this screen.

Top Hosts is always relative to the LAN segment which is physically connected to the analyzer. It is not affected by the "Data Source" selected in the **Statistics | Utilization** screen or the "Device" name selected in the **Tools** screens.

Screen Components

Pressing and toggles between a tabular (text) and 3D pie chart (graphic) display of the top 50 hosts.



When the MAC (All) protocol is selected in the left column, counts are presented either by Packets, Octets, Errors (errored frames transmitted by host), Broadcast Packets, or Multicast Packets. When a specific protocol is selected in the left column, counts are presented by Packets or Octets.

Clear Counts resets the Count column to zero and starts the count over. The protocol list is also reset and all protocol types are grayed. They become un-grayed when protocol activity is seen by the analyzer.

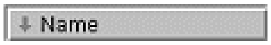
Host Detail opens the **Tools | Overview** screen which displays further detail on the selected device.

Filter opens the **Capture/Generate | Packet Capture Filter** screen with the selected device and protocol preloaded in the filter setup.

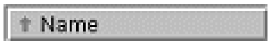
opens the **Statistics | Top Conversations** screen.

Sorting

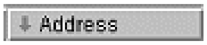
The table (right pane) can be sorted by selecting a top column heading. Each column can be sorted as follows:



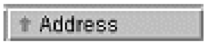
Descending Name



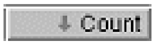
Ascending Name



Descending Address



Ascending Address



Descending Count

Note: Count can only be sorted descending.

Top Conversations

Top Conversations displays the top 50 conversations between hosts for the selected protocol. It is always relative to the LAN segment that is physically connected to the analyzer.

Note: Top Conversations is not affected by the "Data Source" selected in the Utilization screen or the "Device" selected in the **Tools** screens. It is always relative to the LAN segment that is physically connected to the analyzer.

An asterisk (*) in the manufacture prefix symbolic MAC address indicates the Locally Administered bit is set. A pound sign (#) indicates that the Multicast bit is set. For example:

Ÿ 3Com*1fd04d is the symbolic MAC for 0250da1fd04d

Ÿ DEC#16.30 is the symbolic MAC for ab00040001e40

Screen Components

Pressing ▦ and ◕ toggles between a tabular (text) and 3D pie chart (graphic) display of the top 50 conversations.

Host Detail B When the MAC (All) protocol type is selected in the left column, counts can be displayed either by Packets, Octets, or Errors. When a specific protocol is selected in the left column, counts can be displayed by Packets or Octets.

Addresses is used to toggle between names and addresses. Normally, names are displayed for the devices. Pressing the **Address** button will cause devices to be listed by their address. This also causes the button to be re-labeled as **Names**. Pressing the **Names** button will cause the best name to be shown in the table's Name column.

Clear Counts resets the Packets, Octets and Errors count to zero and starts the count over. The protocol list is also reset and all protocol types are grayed. They become un-grayed when protocol activity is seen by the analyzer.

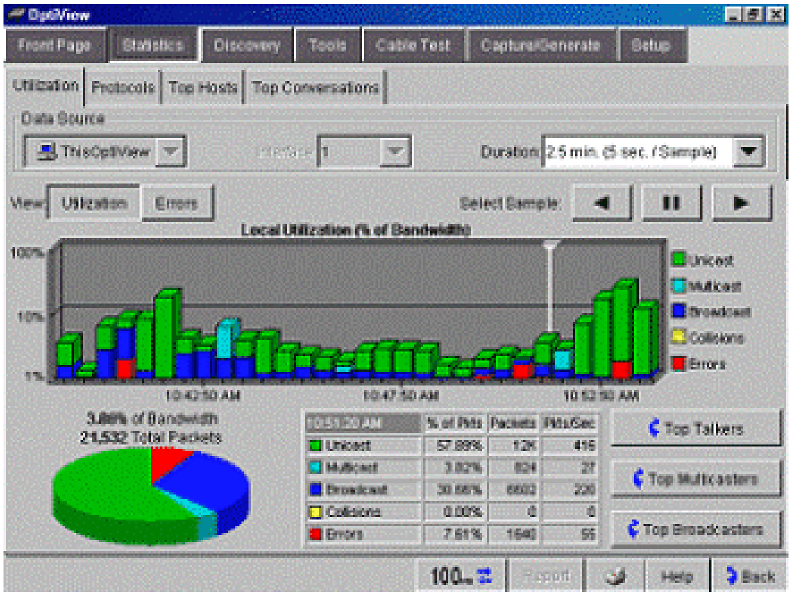
Pressing either Host Detail A or Host Detail B jumps to the **Overview screen** with valuable detail on host A or host B respectively.

Filter opens the **Capture/Generate | Packet Capture Filter** screen with the selected devices and protocols preloaded in the filter setup.

Note: Sorting is not supported for Top Conversations.

Statistics Screen Help

Select any area on the graphic below for more information, or select a topic from the left pane.



Data Source: ThisOptiView

Interface: 1

Duration: 2.5 min. (5 sec. / Sample)

3.86% of Bandwidth
21,532 Total Packets

10:51:50 AM	% of Pkts	Packets	Pkts/Sec
🟩 Unicast	57.89%	12K	416
🟦 Multicast	3.82%	824	27
🟦 Broadcast	30.66%	6602	220
🟨 Collisions	0.00%	0	0
🟥 Errors	7.61%	1640	55

Discovery

Device Discovery

This screen displays network devices discovered by the analyzer. The devices are categorized by device type. These devices include key devices, interconnect devices (routers, switches, SNMP hubs, Access Points), servers, printers, Other Hosts, and MIB SNMP Agents

The analyzer starts discovering devices on your network automatically with no interaction required. Discovery will present the near real-time results in a Windows-Explorer like view. Devices are discovered via traffic monitoring and by actively querying the hosts. Up to 4000 devices can be reported.

For all discovered devices, the best possible description (e.g. DNS name, NetBIOS name, SNMP system, IPX name, address, etc.) is displayed along with an icon indicating the device type.

Note: A device that appears in the list of switches, routers, printers, etc., and talks SNMP, will also appear in the SNMP Agents list. SNMP Agents is particularly useful for looking for SNMP devices such as RMON probes. Use the Host Detail screen's SNMP Agents: ◄ ► to easily step through all SNMP Agents and view information on each device.

Note: If SNMP is disabled, the status bar will indicate "SNMP disabled on this OptiView" for tools that require SNMP. See SNMP Security Issues.

Warning: Do not use the "@" symbol in the community string entry. This will produce inconsistent results and may be very difficult to troubleshoot.

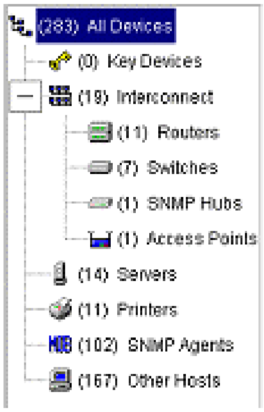
Note: This screen will also show off net switches, servers and key devices. Offnet devices are hosts not on the local broadcast domain. They are found by entering an address or name for Ping, intermediate hops for Trace Route, viewing protocol statistics on off network (offnet) devices, and "drilling" into IPX services.

See also Switches Supported.

Screen Components

The left pane of this screen displays a Windows-Explorer like tree view of all the devices the analyzer detects on your network.

All Devices in the top of the of the tree view displays the sum of all discovered local devices and discovered remote switches and servers. It does not include any remote devices you may have manually added to the **Key Devices** list.



+ / − Expanding and Collapsing a tree

(119) Other Hosts Number of Devices Found

Note: (1) Access Points will display SNMP enabled 802.11b Wireless Access Points (The analyzer looks for the 802.11b enabled MIB using SNMP). Most Access Points are not SNMP enabled, and thus, this feature may not be used to discover rogue Access Points. Most SNMP enabled Access Points are a combination of a wireless Access Point and a Ethernet Switch.

Based on the device type selected in the left pane, the right pane of this screen displays all detected devices in that category. The right pane can be sorted by Name, IP Address, or MAC address by selecting the desired column heading. An error ● , warning ▽ , or information ! symbol will be displayed next to a device when certain conditions occurs.

Note: An asterisk (*) in the manufacture prefix symbolic MAC address indicates the Locally Administered bit is set. A pound sign (#) indicates that the Multicast bit is set. For example

Ÿ 3Com*1fd04d is the symbolic MAC for 0250da1fd04d

Ÿ DEC#16.30 is the symbolic MAC for ab0004001e40

The same DNS names (and IP addresses) may appear more than once in **Discovery | Device** if the analyzer has been running for an extended period of time on the same network. This is the nature of networks running DHCP. This a characteristic of the DHCP server handing out a once used IP address to a new device where the server reuses IP addresses released by hosts no longer on the network.

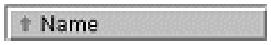
Host Detail Button

Highlight a device (host) in the right pane and select the **Host Detail** button to go to the Overview screen. The Overview screen shows valuable information about the selected device Name, Address, Protocols, and network configuration.

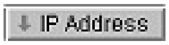
Sorting

The table (right pane) can be sorted by selecting a top column heading. Each column can be sorted as follows:

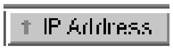
⇩ Name Descending Name



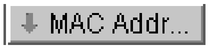
Ascending Name



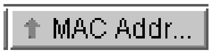
Descending IP Address



Ascending IP Address



Descending MAC Address



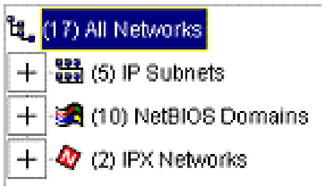
Ascending MAC Address

Network Discovery

This screen displays your network categorized by network type. Network discovery is automatic with no interaction required. Networks and all associated devices are discovered via traffic monitoring and by actively querying the hosts.

What is on this Screen?

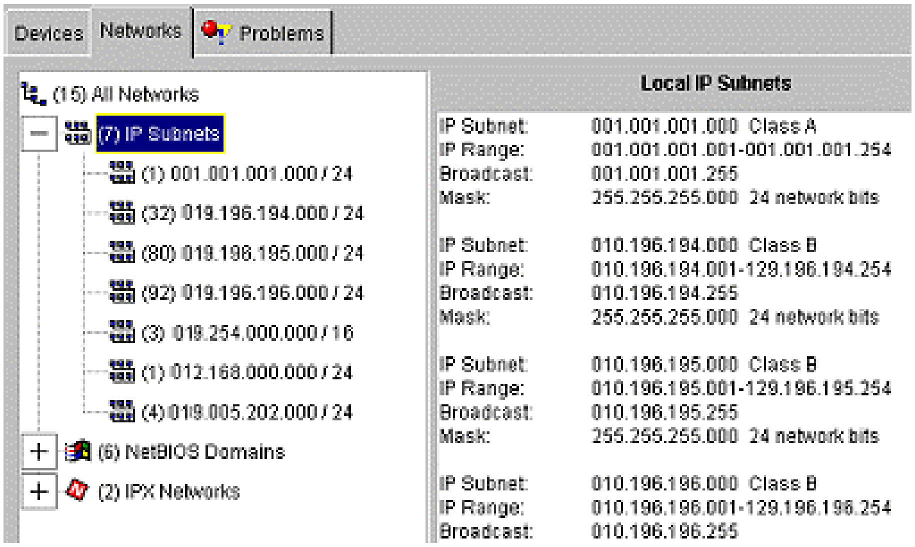
The left pane of this screen displays the network types (IP, NetBIOS, and IPX) as shown below.



(17) All Networks
- (5) IP Subnets
- (10) NetBIOS Domains
- (2) IPX Networks

When All Networks is selected as shown above, then their graphical summary is displayed in the right pane. By expanding and selecting the network type in the left pane, detailed network summary for all local networks of the selected type will be displayed in the right pane as shown below.

Note: The left pane shows each IP subnet with the number of network mask bits, e.g., 001.000.000.000 / 24 where 24 is the number of network bits (e.g., 255.255.255.0)



(15) All Networks
- (7) IP Subnets
  - (1) 001.001.001.000 / 24
  - (32) 019.196.194.000 / 24
  - (80) 019.196.195.000 / 24
  - (92) 019.196.196.000 / 24
  - (3) 019.254.000.000 / 16
  - (1) 012.168.000.000 / 24
  - (4) 019.005.202.000 / 24
- (6) NetBIOS Domains
- (2) IPX Networks

Local IP Subnets

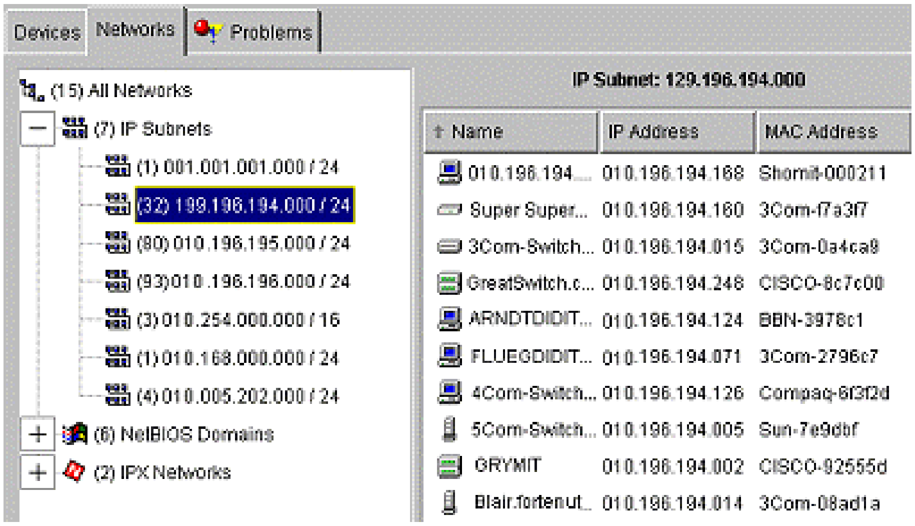
```
IP Subnet:     001.001.001.000  Class A
IP Range:      001.001.001.001-001.001.001.254
Broadcast:     001.001.001.255
Mask:          255.255.255.000  24 network bits

IP Subnet:     010.196.194.000  Class B
IP Range:      010.196.194.001-129.196.194.254
Broadcast:     010.196.194.255
Mask:          255.255.255.000  24 network bits

IP Subnet:     010.196.195.000  Class B
IP Range:      010.196.195.001-129.196.195.254
Broadcast:     010.196.195.255
Mask:          255.255.255.000  24 network bits

IP Subnet:     010.196.196.000  Class B
IP Range:      010.196.196.001-129.196.196.254
Broadcast:     010.196.196.255
```

By further expanding (drilling in) the network in the left pane, host information is displayed in the right pane as shown below. Hosts can be any device type (e.g., routers, servers, switches, etc.) in that network. Highlight a host name and select the **Host Detail** button to view device detail.

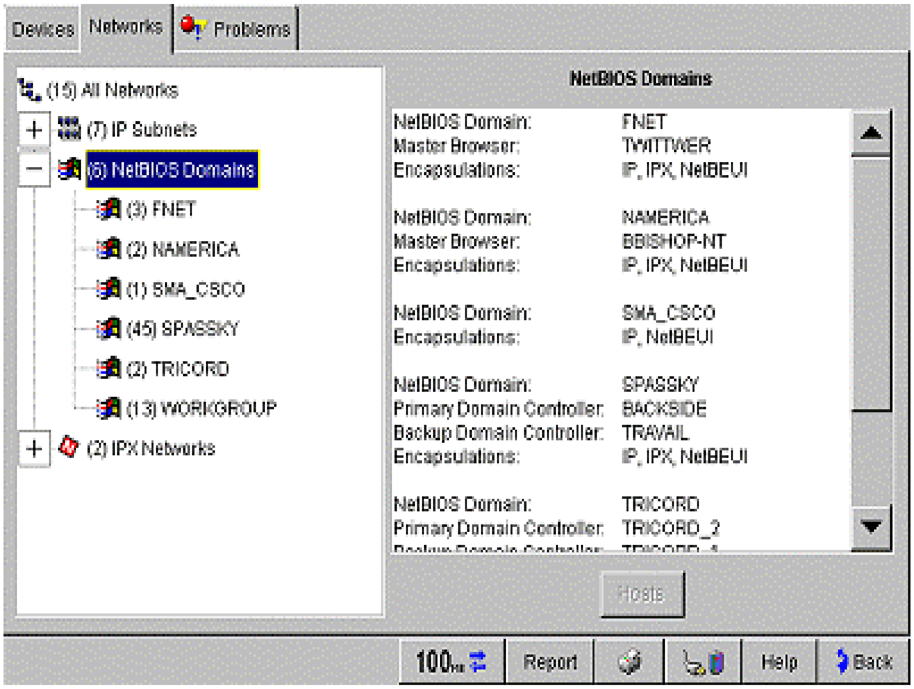


(15) All Networks
(7) IP Subnets
(1) 001.001.001.000 / 24
(32) 199.196.194.000 / 24
(80) 010.196.195.000 / 24
(93)010.196.196.000 / 24
(3) 010.254.000.000 / 16
(1) 010.168.000.000 / 24
(4) 010.005.202.000 / 24
(6) NetBIOS Domains
(2) IPX Networks

IP Subnet: 129.196.194.000

↑ Name	IP Address	MAC Address
010.196.194...	010.196.194.168	Shomit-000211
Super Super...	010.196.194.160	3Com-f7a3f7
3Com-Switch...	010.196.194.015	3Com-0a4ca9
GreatSwitch.c...	010.196.194.248	CISCO-8c7c00
ARNDTDIDIT...	010.196.194.124	BBN-3978c1
FLUEGDIDIT...	010.196.194.071	3Com-2796c7
4Com-Switch...	010.196.194.126	Compaq-6f3f2d
5Com-Switch...	010.196.194.005	Sun-7e9dbf
GRYMIT	010.196.194.002	CISCO-92555d
Blair.fortenut...	010.196.194.014	3Com-08ad1a

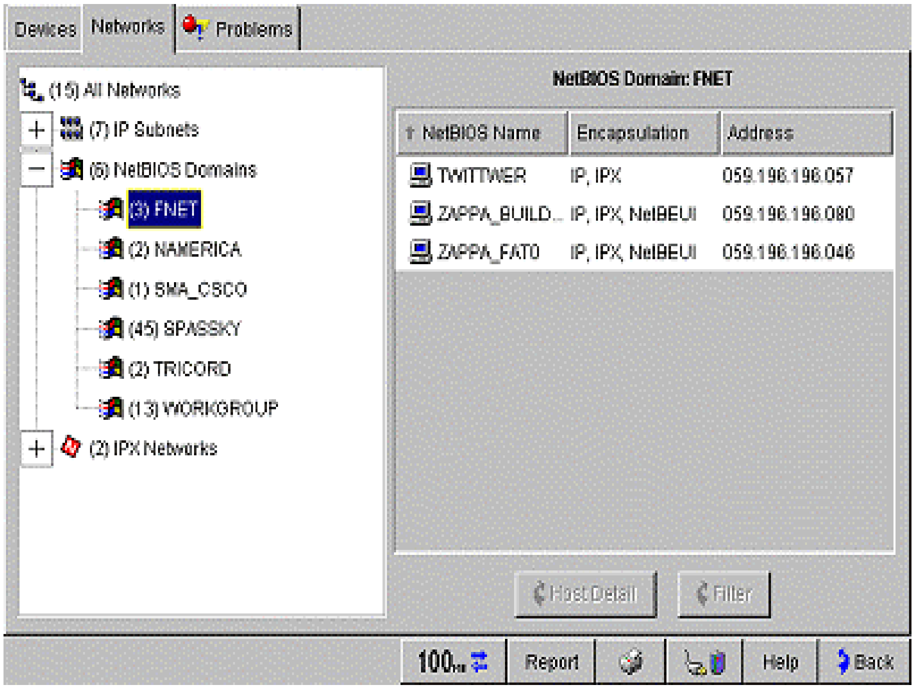
The same scenario goes for NETBIOS Domains as shown below.



(15) All Networks
(7) IP Subnets
(6) NetBIOS Domains
(3) FNET
(2) NAMERICA
(1) SMA_CSCO
(45) SPASSKY
(2) TRICORD
(13) WORKGROUP
(2) IPX Networks

NetBIOS Domains

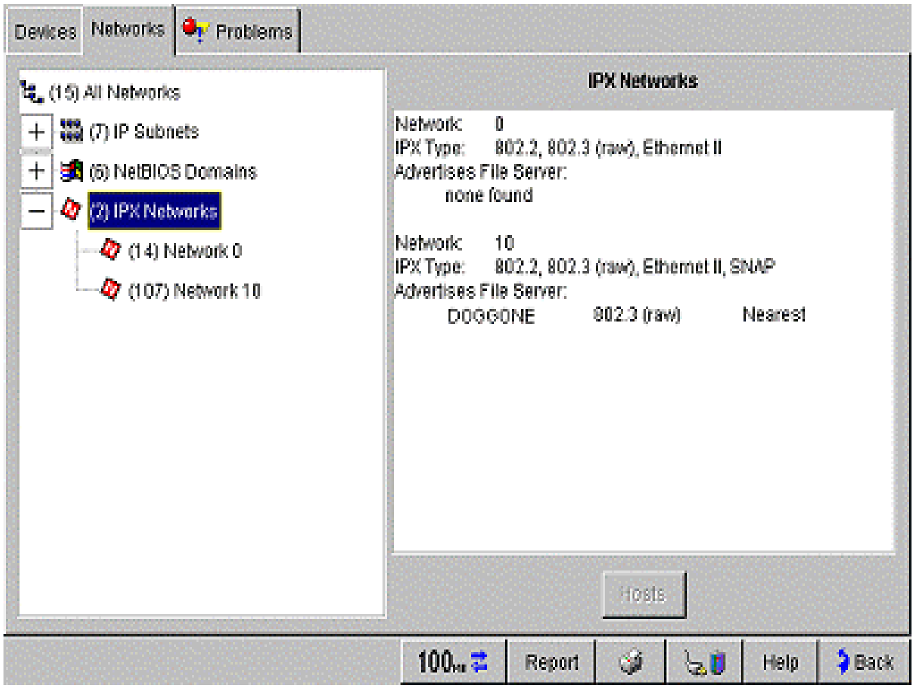
NetBIOS Domain:	FNET
Master Browser:	TWITTWER
Encapsulations:	IP, IPX, NetBEUI
NetBIOS Domain:	NAMERICA
Master Browser:	BBISHOP-NT
Encapsulations:	IP, IPX, NetBEUI
NetBIOS Domain:	SMA_CSCO
Encapsulations:	IP, NetBEUI
NetBIOS Domain:	SPASSKY
Primary Domain Controller:	BACKSIDE
Backup Domain Controller:	TRAVAIL
Encapsulations:	IP, IPX, NetBEUI
NetBIOS Domain:	TRICORD
Primary Domain Controller:	TRICORD_2



NetBIOS Domain: FNET

↑ NetBIOS Name	Encapsulation	Address
TWITTWER	IP, IPX	059.196.196.057
ZAPPA_BUILD...	IP, IPX, NetBEUI	059.196.196.080
ZAPPA_FAT0	IP, IPX, NetBEUI	059.196.196.046

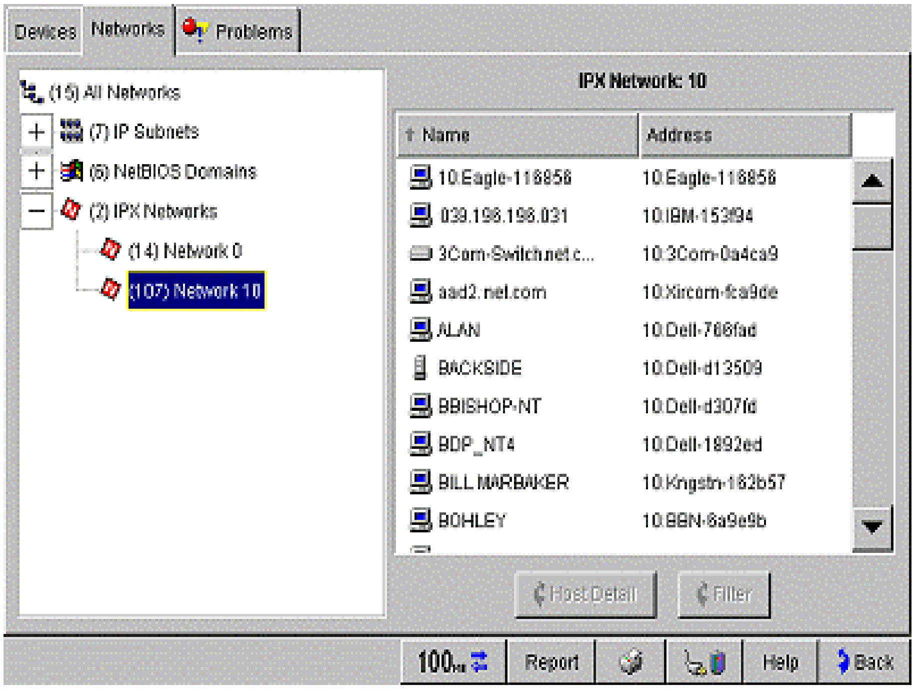
The same scenario goes for NETBIOS Domains as shown below.



IPX Networks

```
Network:      0
IPX Type:     802.2, 802.3 (raw), Ethernet II
Advertises File Server:
          none found

Network:      10
IPX Type:     802.2, 802.3 (raw), Ethernet II, SNAP
Advertises File Server:
          DOGGONE          802.3 (raw)          Nearest
```



IPX Network: 10

Name	Address
10:Eagle-116858	10:Eagle-116858
039.198.198.031	10:IBM-153f94
3Com-Switch.net.c...	10:3Com-0a4ca9
aad2.nel.com	10:Xircom-fca9de
ALAN	10:Dell-788fad
BACKSIDE	10:Dell-d13509
BBISHOP-NT	10:Dell-d307fd
BDP_NT4	10:Dell-1892ed
BILL MARBAKER	10:Kngstn-182b57
BOHLEY	10:BBN-8a9e9b

IPX net 0

The analyzer uses network 0 to show the list of devices talking IPX that do not respond to a valid local network number. This can include devices using the wrong IPX encapsulation type and devices that are not able to get the nearest server.

The NetWare file server (which behaves as your nearest file server) will not let you enter 0 as a server network number (for both its internal and external network numbers). NetWare clients will also not let you enter that number (they require you to enter the same network number as the servers external or internal network number).

Network number 0 indicates:

1. Your local network. The number to be used by the device which receives the packet is the network number acquired by the sending device (in its bootup process) for the frame encapsulation the packet was sent on.
2. It can also be interpreted as the network number of the source IPX address used in the packet. It will be the same source address as the network number of the destination device.
3. Since 0 network number destination packets are never forwarded by routers, they are to be interpreted as described in steps 1 or 2 above.
4. Network number 0 is used by many devices to mean "I don't care what network I'm on, but interpret this number to mean your network number, and reply to this request." Some Hewlett Packard printer devices will use this mechanism to advertise that they are powering down as well.

If the analyzer acquires a network number when it boots up, then the network number 0 should be interpreted as the analyzer's network number for the encapsulation seen on the packet, or the network number seen in the source field of the packet.

Problem Discovery

Problem Discovery shows any network hosts (devices) that may be experiencing problems. Problems are reported by error, warning, or informational severity. Resolved problems are also displayed. A corresponding symbol (errors ● , warnings ▼ , and informational !) displays next to the host. As the severity changes, so does the host status. The problem conditions are given below. Select a condition to obtain a recommended solution.

Note: Problem Discovery will retain a problem log until either the Front Page screen Rerun Tests is selected, the analyzer is plugged into a new network, or the unit is turned off.

Errors

Duplicate IP: <ip> MAC: <mac>
Incorrect subnet mask: <mask>
IP address is subnet address: <ip>
IP address is subnet broadcast address: <ip>
Key device not responding to IP (up/down x time(s))
Key device not responding to IPX (up/down x time(s))
DHCP Server offered IP already in Use: <ip>
Lost DHCP lease (for this analyzer): <ip>

Warnings

Default router not responding: <ip>
Only device in IP subnet: <ip>
Only device in IPX network: <network number>
Only device in network <network number> using IPX type: <type>
Proxy ARP reply for local IP: <ip>

Info

Only device in NetBIOS domain: <domain>

Duplicate IP: <ip> MAC: <mac>, Incorrect subnet mask: <mask>

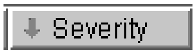
Host Detail

Clicking on Host Detail opens the **Tools | Overview** screen with detail on the selected problem device.

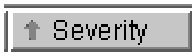
Sorting

The Problems table can be sorted by selecting a top column heading. Each column can be sorted as follows:

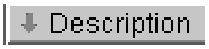
↓ Host Descending Host
↑ Host Ascending Host



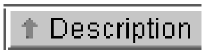
Descending Severity



Ascending Severity



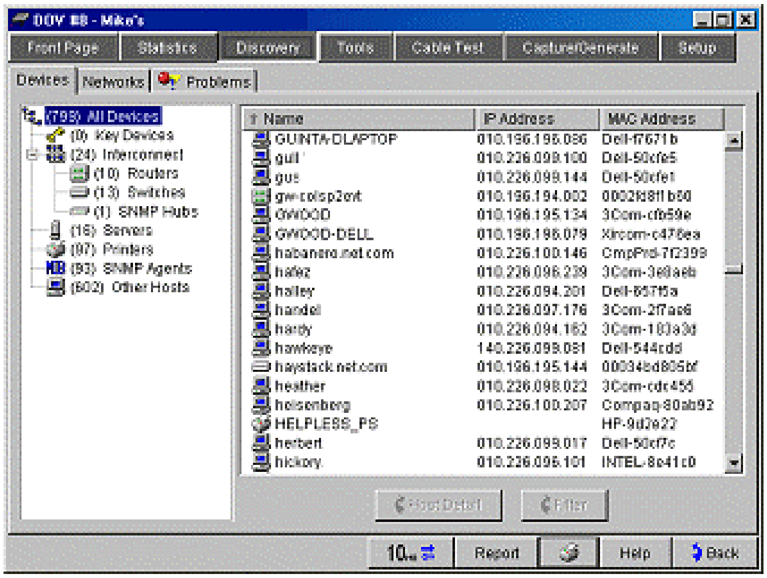
Descending Description



Ascending Description

Discovery Screen Help

Select any area on the graphic below for more information.



Name	IP Address	MAC Address
GUINTA-DLAPTOP	010.196.195.086	Dell-f7671b
gull	010.226.099.100	Dell-50cfe5
gus	010.226.099.144	Dell-50cfe1
gw-colsp2ovt	010.196.194.002	0002fd8f1b60
GWOOD	010.196.195.134	3Com-cfb59e
GWOOD-DELL	010.196.196.079	Xircom-c476ea
habanero.net.com	010.226.100.146	CmpPrd-7f2399
hafez	010.226.096.239	3Com-3e8aeb
halley	010.226.094.201	Dell-657f5a
handel	010.226.097.176	3Com-2f7ac6
hardy	010.226.094.162	3Com-183a3d
hawkeye	140.226.099.081	Dell-544cdd
haystack.net.com	010.196.195.144	00034bd805bf
heather	010.226.098.022	3Com-cdc455
heisenberg	010.226.100.207	Compaq-80ab92
HELPLESS_PS		HP-9d2e22
herbert	010.226.099.017	Dell-50cf7c
hickory	010.226.096.101	INTEL-8e41c0

Tools

Overview

The Tools Overview screen displays valuable detail about the device selected or entered in the Device list box (upper-left corner of this screen). Device detail can include Names, Addresses, Protocols, NetBIOS, Services, Router, Printer, and Remote Monitor that the device supports.

The ◄ ► button allows you to single step through Overview detail on all the discovered devices.

The device name and an associated symbol are displayed at the top of the screen. The device symbols are: ▤ routers, ▭ switches, ▯ servers, 🖨 printers, 🖥 hosts, OFF NET not on local network, and ⊘ device is not reachable.

Note: Offnet OFF NET indicates the device is not in the local broadcast domain, and ⊘ indicates the analyzer can not successfully communicate with that device. You may see traffic between devices in Top Conversations and Top Hosts that the analyzer can not communicate with. This could be a firewall issue. The only offnet devices that will be shown in device discovery are switches, servers and key devices. A user entered name or address will show ⊘ until the analyzer has had a chance to communicate with the device.

Screen Components

Device list

The Device drop-down list box allows you to select discovered devices and view detail on them. In the Device list, an associated icon (▤ routers, ▭ switches, ▯ servers, 🖨 printers, 🖥 hosts) is displayed to the left of the device. Devices that do not display an icon are offnet devices, and are not part of the local network. Offnet devices do not display in the **Discovery | Device** screen unless they are added as a Key Device. See **Add to Key Devices Button** below for more information on adding devices to the Key Device list in the Discovery | Devices screen.

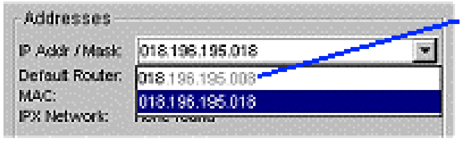
Names

The device name order of precedence presented is:

DNS name, SNMP name, IPX service name, NetBIOS name, IP address, IPX address, MAC address.

Addresses

Displays the appropriate address, otherwise "none found" is reported. An address that appears grayed indicates that at some time earlier the IP address was used by the device, but has been configured to use a new IP address.



Addresses

IP Addr / Mask: 018.196.195.018

Default Router: 018.196.195.008

018.196.195.018

MAC:

IPX Network:

This IP address is grayed because it was at one time used by this device but is no longer.

This is useful for tracking device changes. For example, there is a resolved problem "only device in IP Subnet." Select the device and use this list to show all the IP addresses that this device has used since rerunning Discovery.

Protocols

Supports IP, IPX, and NetBIOS if discovered.
IPX types supported are 802.3 and 803.2 (RAW, Ethernet II, SNAP)

NetBIOS

Displays the NetBIOS Domain and Transparent (IP, IPX, and NETBEUI).

Services

Only displayed if present.

Router

IP routers detected include: RIP, RIP-2, RIP-2 in compatible mode, OSPF, IGRP, EIGRP, HSRP, IRDP (ICMP Router Discovery), Proxy ARP, or Statically Configured can be displayed.

IP routers detected also Advertise: default RIP route, RIP with no routes, only reverse poison RIP route.

IPX routers detected display RIP.

Switches

If present then 802.1d sending Spanning Tree, sending DEC spanning Tree, sending lattice Spanning Tree, Discovered via SNMP, Transparent, and Source Routed can be displayed.

Printer

If present then IP or IPX printer can be displayed.

Remote Monitor

If present then SNMP agent, RMON probe, or RMON2 probe can be displayed.

Add to Key Devices Button

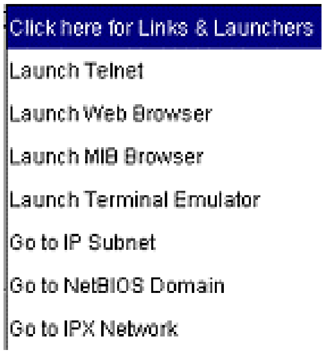
Select this button to add the device into the Key Device group. The Key Device group is seen in the **Discovery | Device** screen's left pane at the top. See also Key Devices.

Filter

Jumps to the Packet Capture Filter screen with the HOST address preloaded.

Click Here for Links and Launchers

The device selected determines the choices displayed (in the drop-box). If the Device supports IP, IPX, and NetBIOS, the drop-down list displays:



Launch Telnet, **Launch Web Browser**, and **Launch MIB Browser** are IP address enabled. When they are launched, they are initialized with the IP address of the device selected. Launch MIB Browser is launched with the SNMP community string if one has been found that works.

Any list item that starts with "Go to" is a link to an OptiView Workgroup Analyzer specific screen. For example, **Go to NetBIOS Domain** takes you to the **Discovery | Networks** screen with the NetBIOS Domains selected.

Note: Applications launched through the Links and Launchers drop-down list are run through the OptiView user interface on the PC, not through the analyzer. The analyzer may be connected to a different network (broadcast domains) than the network your PC is connected through. In this case, some of the Links and Launchers applications may or may not work depending on your network's router configuration.

PING

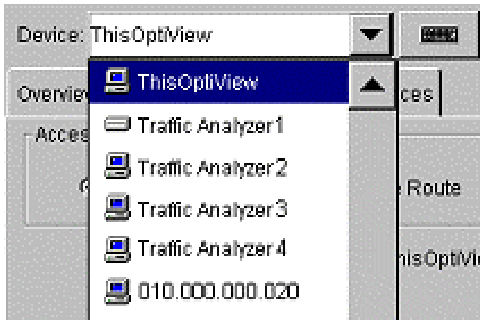
Ping is for testing network connectivity to a device. Ping can test devices via IP Ping, IPX Ping, or with Trace Route.

IP Ping

The analyzer automatically Pings the device selected in the Device drop-down list when you select the IP Ping screen. The analyzer sends an Internet Control Message Protocol (ICMP) echo request to the IP address selected. The results are displayed on this screen in the "Results" area.

The Results box (bottom-right on this screen) displays the results of the IP Ping.

You can select a device to Ping from the "Device" drop-down list as shown below. By selecting the device, the Ping test is automatically run. If the device is not in this list, enter the device's IP address or DNS name, and press Enter.

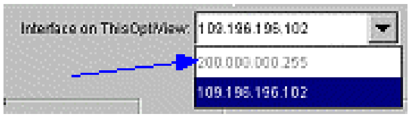


Interface on <device name>

If the selected device has more than one address associated with it, the "Interface on *device* drop-down list will list all of the discovered IP addresses (with the best one for connectivity selected by default).

Some devices may have multiple IPs associated with them. If that is the case, you can select from the Interface list of IP addresses.

Note: An address that appears grayed indicates that at some time earlier the IP address was used by the device, but is no longer used (see example below).



Ping Parameters

Continuous, when checked, enables IP Ping to run continuously. When not checked, Ping runs once.

Rate sets how often a packet is sent. Using a faster Rate can be used to detect Burst problems. Rate can be set to 10 per second, 5 per second, 1 per second, or once every 5 seconds. The Rate value is only used in continuous mode.

Data Size sets the ICMP packet data size that is sent and received. It can be set from 18 bytes (64 byte minimum packet size) to 1472 bytes (1514 byte maximum packet size). Using a larger Data Size can be used to stress the network and detect Burst problems.

Results

Requests is the number of packets sent. In continuous mode, you can set the Rate to 10 per second, 5 per second, 1 per second, or once every 5 seconds.

Replies is the number of packets received and optimally should equal the number of Requests sent. On slow or congested links, this number can be less than the requests if the rate is higher than the latency. Clicking **Stop** will continue to count all late replies.

Note: Hosts with more than one IP stack can return more than one Ping reply.

Success Rate represents the percentage between the number of packets sent and received. Realistically, it should be close to 100% (allowing for initial lost packets through routers to resolve ARP caches). Red indicates less than 60 percent, blue indicates less than 90 percent, and black indicates greater than 90 percent.

Response Time represents the minimum, average, maximum, and last round trip response times.

IPX Ping

When you open the IPX Ping screen, the analyzer automatically Pings the device selected in the "Device" drop-down list.

You can select a device to Ping from the "Device" drop-down list. By selecting the device, the Ping test is automatically run. If the device is not in this list, then enter the device's address, and select **Enter**. If the selected device has more than one IPX address associated with it, the "Interface on " drop-down list will contain all of the discovered IPX addresses for this device.

The Results block (bottom-half on this screen) displays the results of the IPX Ping.

Ping Parameters

Continuous, when checked, enables IPX Ping to run continuously. When not checked, Ping runs once and will time out after 5 seconds of no response.

Rate sets how often a packet is sent. Using a faster Rate can be used to detect Burst problems. Rate can be set to 10 per second, 5 per second, 1 per second, or once every 5 seconds.

Results

Requests is the number of packets sent. In continuous mode, you can set the Rate to 10 per second, 5 per second, 1 per second, or once every 5 seconds.

Replies: is the number of packets received and optimally should equal the number of Requests sent.

Note: If the device is responding slower than the request rate, then late responses will be discarded.

Success Rate: represents the difference between the number of packets sent and received. On a healthy network, it should be close to 100%.

Encapsulation displays IPX encapsulation type. It can be either 802.2, 802.3 (raw), Ethernet II, or SNAP.

Min, Max, Avg, and Last display the round trip response times. Last is the response time of the most recent packet received.

Trace Route

When you select the Trace Route screen, the analyzer automatically runs a trace route to the device selected in the "Device" drop-down list.

You can select a device to run Trace Route to, from the "Device" drop-down list. By selecting the device, the Trace Route test is automatically run. If the device is not in this list, then enter the device's IP address or DNS name, and select **Enter**. If the device you have selected has more than one address associated with it, the "Interface on " drop-down list will contain all of the discovered IP addresses for this device.

The results of the Trace Route are displayed in the bottom-half of this screen.

Hop displays the number of routers traversed to get to the destination device.

Name displays the device description for a given Hop count.

IP Address displays the IP Address of the device at a specific Hop count.

Try 1, 2, 3 displays the total round trip response times for each request. This column will be red if there was no reply, and blue if there is a split route detected.

Split Routes

Trace Route can detect split routes taken to the destination device. Split routes are due to load balancing or route Flapping.

Load Balancing is when several equal-cost routes to a destination exist, traffic is distributed equally among the routes.

Route Flapping: When LAN or WAN links have serious problems, they will often cycle up and down every several seconds. Whenever one of these links changes state, it may trigger routing protocol updates. Whenever these networking protocols indicate a changed route, routers may make changes in their routing information that create "black holes." These "black holes" are parts of the network that, for several seconds, may not be accessible by all or part of the network. After additional time, routing protocol updates have had time to traverse the network, bringing the network back into a stable state. If network segments (WAN or LAN) are cycling every several seconds, the network as a whole is unstable and the routing information will be constantly inconsistent. This "route

Flapping" will also waste a router's CPU resources.

Host Detail gives you valuable detail on a device selected from the results in the bottom half of this screen.

How Trace Route Works

Trace Route determines the route taken to a destination by sending UDP echo packets with varying Time-To-Live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a Hop count. When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to the source address. Trace Route determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on subsequent transmissions until the target responds. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Some routers silently drop packets with expired TTLs and are invisible to Trace Route. Each Hop is tested up to 3 times and the round trip response time is displayed in the Try 1, Try 2, and Try 3 columns.

In many installations, LANs or WANs that are experiencing intermittent physical problems can create performance problems by discarding packets or by creating congestion as the routers queue traffic waiting for the link. A lost packet will result in a retransmission. Intermittent physical problems can also create a routing issue, which is called "route Flapping." As the links cycle from up to down and up again, the routing protocols send updates regarding the changing status of the link and the impact on the available routes. These routing updates can negatively impact router performance throughout the network as they spend processor time recalculating routes.

The analyzer can be used to view the routing tables (use **Host Detail | SNMP Tables | Route Table**) of all routers that separate two hosts. If routes are unstable, then rerunning the route table will reflect the instability. Another way to find this problem is to conduct a Trace Route test to a variety of target stations on distant LAN segments.

Note: The Ping or trace route stops when leaving the screen. It is only active when the screen is visible.

SNMP Tables

SNMP Tables gives you managed device information on the System Group, Route Table, and ARP Table.

Note: This is disabled when "**Strings used to query other SNMP agents**" is left blank in the **Setup | Security screen**.

System Group

Name: An administratively assigned name (often the TCP/IP DNS name).

Description: An administratively assigned textual description of the device.

Up Time: The time since the network management portion of the system was last reinitialized.

Contact: A person responsible for the node, along with information such as a phone number.

Location: The physical location of the device.

Services: Indicates the Layer(s) for which this node performs services.

Object Id: An authorization identifier assigned to this product by its vendor. Also used for the private MIB extension.

Route Table

Use the Route Table to obtain the following MIB II Route Table information:

#: The order of the Route Table. Used primarily to re-sort table in this screen.

Destination: Network or Host to reach.

Route Name: Name of the Route Address (e.g., Next Hop) if the next hop is on an attached segment.

The message "invalidated entry" indicates that this route entry has timed out or is in the process of being discarded.

Route Address: IP address of the interface or Next Hop Router reach the destination.

Mask: The subnet mask to be used with the destination address. The mask is logically-ANDed with the Destination address. Together with the Destination address, it represents a group of IP addresses.

Protocol: How the route was learned. If the field is blank, then the route is a "static" or direct entry.

Route Tables come from:

· statistically configured entries.
· an Internet Control Message Protocol (ICMP) Redirect message.
· neighboring routers that propagate routing protocols (e.g., RIP, OSPF, IGRP, ...).

Note: Entries in the Route Table that have ICMP displayed in the Protocol column, indicate a redirect was issued to a more optimal router by the default router (This only applies to IP Ping and SNMP Queries). This only applies to "This OptiView." Trace Route always uses the default router.

ARP Table

ARP (Address Resolution Protocol) is responsible for discovering the LAN physical layer address that corresponds to a given network layer address. LAN physical addresses are called MAC (Media Access Control) addresses.

#: The order of the ARP table. Used primarily to re-sort table in this screen.

Name: The best name for that host or has become inaccessible, but has not timed out of the ARP cache yet. Names that are left blank are devices which are off-net or are inaccessible.

IP Address: The host IP address.

MAC Address: The corresponding physical address for the host.

Interface: The interface index to use for this host.

Type: Can be "static", "invalid", or "blank."

Interfaces (Multi-Port Statistics)

Multi-port segments can be viewed in this screen simultaneously, thus enabling you to diagnose hard-to-analyze switched LAN segments. It also allows you to see activity that is occurring on numerous locations on your network.

It provides a tabular and graphical, multi-port view of switches and routers at a glance. Statistics are updated every 5 seconds. If you have purchased the WAN Vision option, you can also obtain Permanent Virtual Circuit (PVC) Frame Relay Wide Area Network (WAN) information and port-by-port bridge forwarding table information.

The analyzer uses SNMP to automatically query numerous MIBs (including private MIBs) to gather information. For each interface, the best supported MIB will automatically be selected as the data source.

Note: If the target does not support SNMP, is not accessible, or the correct community string is not configured in Security, the query will fail.

Note: There are no hard coded limits to the number of ports the OptiView analyzer can discover. If you have purchased the WAN Vision option, up to 100 virtual circuits per device can be discovered. The only other limitation is the amount of shared memory available on the OptiView analyzer.

Interface and WAN statistics continues to gather statistics on the most recent selected device even after leaving this screen. Statistics are updated once per minute while away from this screen. This allows you to go to other screens and perform tests and not lose valuable statistics information upon returning to this screen. If you wish to stop gathering statistics on a device, select another device from this screen's Device drop-down list. If you do not wish to gather statistics on any of your network devices, then select **ThisOptiView** from the Device drop-down list.

This screen has the following three distinctive views:

Table (tabular view) displays the device's interface table. If the device is a switch that supports the standard 802.1d bridge MIB forwarding database, then it also shows all hosts residing on the selected port.

Statistics (graphical view) displays port/interface statistics sorted by average utilization, average errors, or port/interface number. You can select each device's port and view detailed statistics.

Note: The following WAN information is only available when you purchase the WAN Vision option (see the analyzer Getting Started Guide for the part number and sales contact):

WAN (wide area network view) displays graphical information on the virtual circuit for the selected interface, and displays information about DLCIs, Octets, Frames, FECNs, BECNs, and Utilization. This view is only available for routers that support the Frame Relay DTE MIB.

See also: Layer 2 WAN MIB Support and Layer 3 WAN MIB Support.

IPX Services

Lists the IPX Services advertised by the selected device by Service Name, Address, Service Type, Hops, and Encapsulation.

Service Type: File, Netware Directory. Netware Access, Print, Time Synchronization, Netware Management Station, Netware Management Station 2, RIP.

Encapsulation: 802.2, 802.3 (raw), Ethernet II, SNAP.

Nearest File Server: For all file servers, the first to respond to an analyzer's request will be indicated with the text "nearest" (one per Encapsulation type).

Hops: This is the number of router hops to the device that provides the service. A value of 1 typically indicates that the current host provides the service, and the Address would match the selected device in the Device drop-down list.

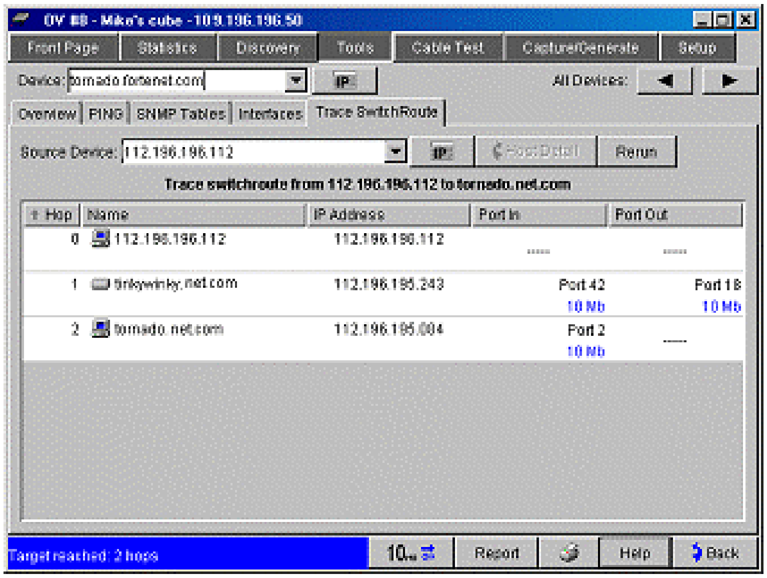
Note: Some routers do not properly increment the hop count when forwarding IPX packets.

Trace SwitchRoute

Trace SwitchRoute works within the subnet (local broadcast domain) that the analyzer is connected to, and only switches are detected and displayed. The Trace SwitchRoute discovers from the specified Source Device (default is **ThisOptiView**) to the specified Device (default is **ThisOptiView**) . The resulting display shows all the switches between those two devices. Included in the resulting trace switch route display are the switch port, slot, and VLAN identifiers, as well as speed and duplex if that information is available.

Warning: Do not use the "@" symbol in the community string entry. This will produce inconsistent results and may be very difficult to troubleshoot.

Note: The Device and Source Device lists may contain devices outside of your local network (broadcast domain). These devices were discovered by the analyzer when a Ping or Trace Route was performed to an off-network (off-net) device. If you select a device that is outside of your local network, an error message will display.



Device: tornado.fortenet.com

Source Device: 112.196.196.112

Trace switchroute from 112.196.196.112 to tornado.net.com

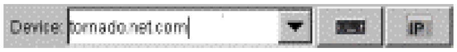
Hop	Name	IP Address	Port In	Port Out
0	112.196.196.112	112.196.196.112	-----	-----
1	tinkywinky.net.com	112.196.195.243	Port 42 10 Mb	Port 18 10 Mb
2	tornado.net.com	112.196.195.004	Port 2 10 Mb	-----

Target reached: 2 hops

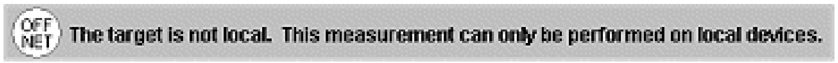
Note: The status bar will report at the time the measurement was started, the total number of switches, plus the analyzer and destination device. The count could potentially be the total number of switches plus three (e.g., analyzer, plus source, plus destination device (if the analyzer was not one of the end points).

Note: When a “?” appears in front of a device on this screen, it indicates that the analyzer knows the switch is somewhere in the route, but is not 100% sure where. The analyzer will display its best guess which means it could be displayed in the wrong location in the route.

Note: At the beginning of this measurement, a ping is sent out by the analyzer from the source to the destination device. When a red "X" is displayed next to the source or destination device, it indicates the device did not respond to the ping. This indicates that the results may be incomplete.



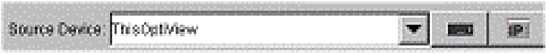
The **Device** field determines the ending point in the Trace SwitchRoute measurement. You may select from the drop-down list, enter a DNS name, or enter an IP address. Devices outside the broadcast domain are not permitted to be used. the following message is displayed when selecting an Off-net device:



The target is not local. This measurement can only be performed on local devices.

Devices outside of the broadcast domain do not provide their MAC address to the analyzer and will be displayed as Off-net devices which indicates they can not be used in this measurement.

◄ ► Allows you to step through the devices seen in the Device drop-down list. Each time you step to a new device, a new Trace SwitchRoute is performed.



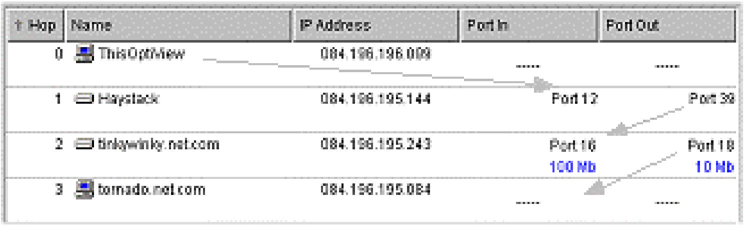
The Source Device determines the starting point in the Trace SwitchRoute measurement. Devices outside the broadcast domain are not permitted to be used. The following message is displayed when selecting an Off-net device:

Host Detail Highlight a device in the Trace SwitchRoute Name column and select **Host Detail** (or double-click on the device) to view information about the device's network configuration.

Rerun Clicking this button reruns the Trace SwitchRoute measurement. While this measurement is running, this button is replaced with the **Stop** button.

Target reached: 3 hops

The lower left-hand corner of this screen displays the Trace SwitchRoute status. When the measurement is successfully completed, it will display "*Target Reached*" and the distance in hops between the devices.



↑ Hop	Name	IP Address	Port In	Port Out
0	ThisOptiView	084.196.196.009	-----	-----
1	Haystack	084.196.195.144	Port 12	Port 39
2	tinkywinky.net.com	084.196.195.243	Port 16 100 Mb	Port 18 10 Mb
3	tornado.net.com	084.196.195.084	-----	-----

The above Trace SwitchRoute results can be sorted by column heading. Also, sorting on either Port column will sort the column by link speed.

Note: In the above example, the arrows indicate the physical switch connections, e.g., the "Haystack" switch's Port 39 is connected to the "tinkywinky.net.com" switch's Port 16.

Hop displays the number of switches traversed to get to the Source Device.

Name displays the device description for a given Hop count.

IP Address displays the IP Address of the device at a specific Hop count.

Port in displays the port/slot/VLAN number coming into the switch and the link speed (and duplex when available).

Port out displays the port/slot/VLAN number leaving the switch and link speed (and duplex when available).

When Duplex Information is available, it is displayed as shown below.

Ÿ ⇄- Full Duplex
Ÿ ⇄- Half Duplex
Ÿ ⇄- Auto Negotiate State

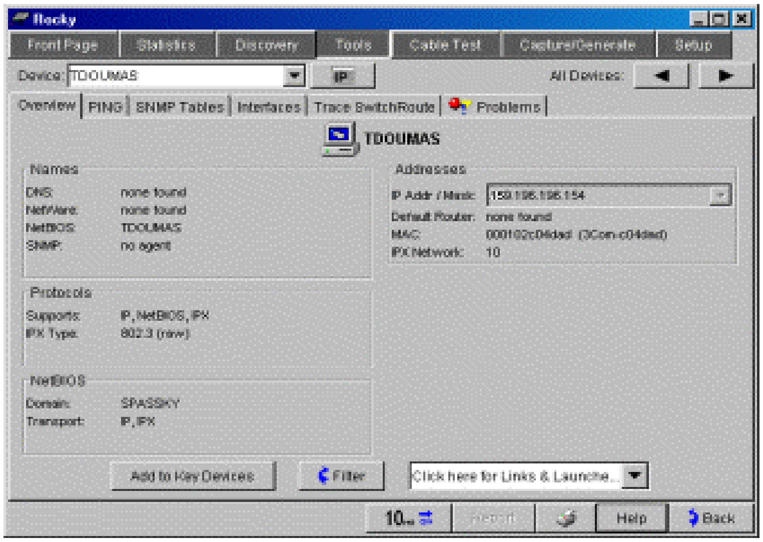
Problems

This screen is available only when the selected device has a problem, e.g., error ● , warning ▼ , or informational ! . It displays the condition of the selected device.

See Problem Discovery for a description of all errors, warnings, and informational conditions.

Tools Screen Help

Select any area on the graphic below for more information, or select a topic from the left pane.



Device: TDOUMAS

TDOUMAS

Names

DNS: none found
NetWare: none found
NetBIOS: TDOUMAS
SNMP: no agent

Protocols

Supports: IP, NetBIOS, IPX
IPX Type: 802.3 (raw)

NetBIOS

Domain: SPASSKY
Transport: IP, IPX

Addresses

IP Addr / Mask: 159.196.196.154
Default Router: none found
MAC: 000102c04dad (3Com c04dad)
IPX Network: 10

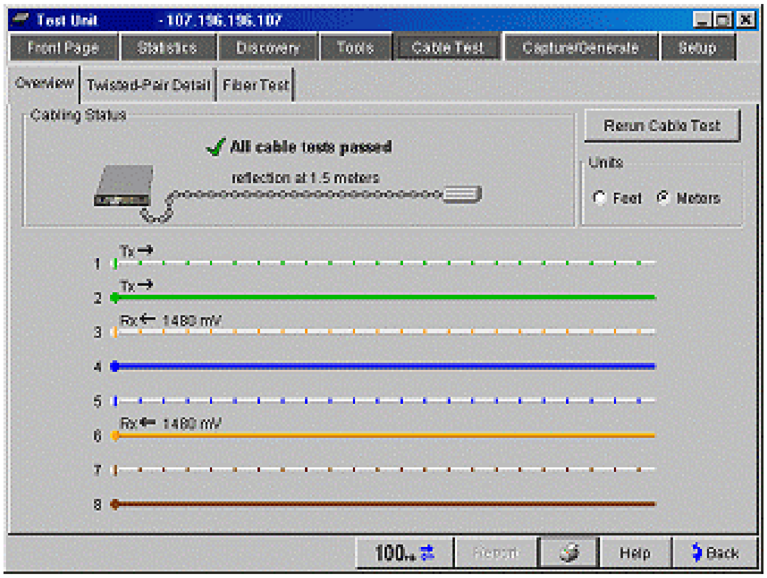
CableTest

Cable Test Overview

Note: See the Twisted-Pair Detail screen for additional information on the location of the faults such as split-pairs and shorts.

What is on this Screen?

Units determines which measurement units are displayed throughout the Cable Test screens. Units are either Feet or Meters.



Test Unit - 107.196.196.107

Cabling Status

✓ All cable tests passed

reflection at 1.5 meters

Units: ○ Feet ● Meters

Cable wire mapping is displayed in this screen. This includes the data flow direction (Tx, Rx), cross mapping, wire condition (opens, shorts, etc.), and color code for twisted pairs. The color representation of the wire pairs is in accordance to TIA TSB-67 specification for wire categories 3 through 6 as shown below:

Note: The color code is selectable on the Twisted-Pair Detail screen.

T568A

1	2	3	4	5	6	7	8
W-G	G	W-O	BL	W-BL	O	W-BR	BR

T568B

1	2	3	4	5	6	7	8
W-O	O	W-G	BL	W-BR	G	W-BR	BR

Note: Measurable cable lengths are from 3 feet (1 meter) to 1000 feet (304 meters). The correct cable type must be selected for Cable Test to report correct measurements. The cable type is selected in the **Twisted-Pair Detail** screen. Unshielded Twisted Pair Category 5 (UTP Cat-5) is the default cable type selected. Cable Test depends on the cable type selected for:

- Cable length accuracy
- Impedance measurement accuracy
- Accuracy of split pair, bridge-tap, and broken wire detection
- Accuracy of anomaly reflection values A misidentified cable type will have the following effect:
- Lengths may vary by as much as 15% from what they should be
- Split pairs, bridge-taps, and broken wires may either not be detected or may be misidentified when not actually present
- Anomaly reflection values may be several percent off It is not necessary to open or place special devices at the far end of the cable for the length to be measured. Cable length can be measured terminated to a Wire Map Adapter, open, or while connected to an active hub, switch, or NIC. This measurement is made automatically at power-up or anytime a new cable is connected. Results are displayed on the Front Page screen and additional details are viewable on the **Cable Test** screens. Tests may be manually repeated by clicking the **Rerun** button on the **Cable Test** screens.

Setup

Note: All tests are safe to perform with active network devices connected at the far end of the cable. Any stimulus generated by the analyzer is limited to safe levels.

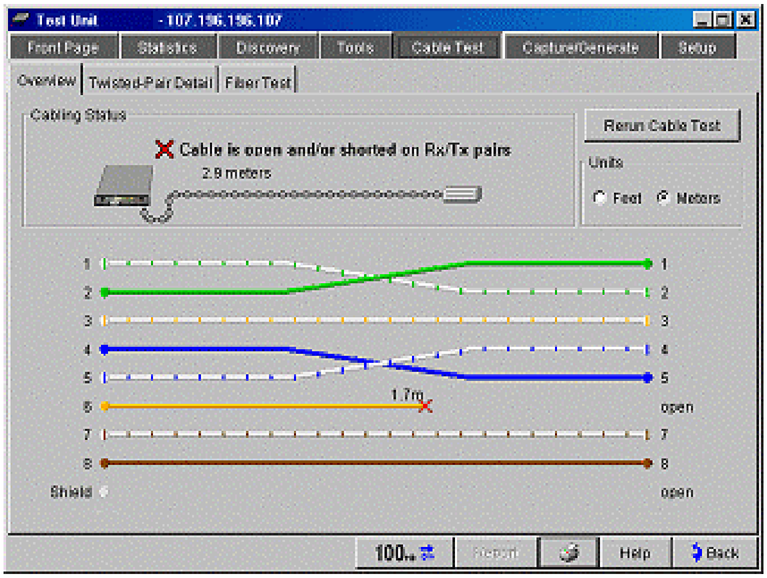
100 and 120 Ohm shielded and unshielded twisted-pair cables terminated with RJ-45 modular connectors can be tested. The analyzer can also be configured to optimize tests according to characteristics for a variety of cable types, such as UTP-Cat5 and ScTP Cat-6.

An optional Wire Map Adapter (office locator) must be connected to the far end of the cable to get a complete picture of the cable continuity. When connected this way, shorts, opens, mis-wired pins, and the shield are detected and displayed.

Note If shorts are detected, the test does not attempt to complete all other wire mappings. Repair the shorts and opens first, then retest the cable.

Understanding the Cable Test Results

Example 1, Open Wire and Mis-wired Twisted Pair



Cable is open and/or shorted on Rx/Tx pairs
2.9 meters

Units: ○ Feet ● Meters

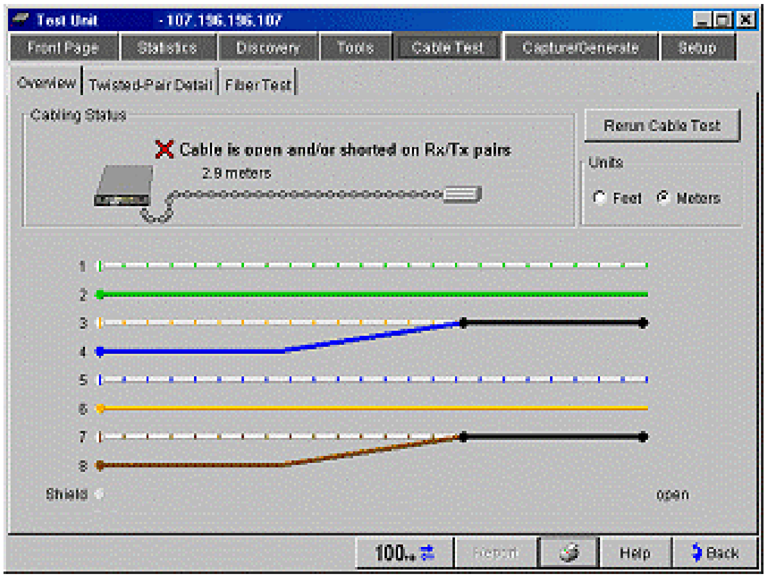
1.7m

6: open

Shield: open

In the above example, pairs 1-2 and 4-5 are cross wired (polarity inverted), and pins 4 and 5 are mis-wired. Notice the end of the cable (right-side) is terminated with a ball and pin number. This indicates it is terminated into a wire map adapter. The distance is also given. Pin 6 is also open. This could indicate a break in the wire.

Example 2, Shorted, Mis-wired Twisted Pair



Cable is open and/or shorted on Rx/Tx pairs
2.9 meters

Units: ○ Feet ● Meters

Shield: open

In the above example pins 3 and 4 and pins 7 and 8 are shorted and mis-wired. When either pins 1-2 or 3-6 are not properly wired, the length is not given. Length is always given in the **Cable Test | Twisted-Pair Detail** screen.

Other General Cable Test Notes

Without an office locator/ wire map adapter present at the far end of the cable, the following differences in results may occur:

- Pin numbers at the far end are unknown

- Opens affect each wire pair, e.g., 1-2, 3-6, 4-5, or 7-8. The pair is indicated as an open, and the individual pin is not identified
- There is no wire map adapter (office locator) ID number

See also: Fiber Test

Cable Test Twisted-Pair Detail Screen

Cable Wire Pair, Impedance, Length to End, Length to Reflection, and Status/Anomalies (e.g., shorts, opens, termination, and split-pairs) are displayed in a tabular format. The Wire Pair is referenced from the cable end to which the analyzer is connected.

Additional information is discovered and presented if it occurs such as Receive Wire Pair, Transmit Wire Pair, Receive Voltage, Receive Polarity, Transmit Polarity, MDI/MDI-X, Locator ID and Shield Presence.

Note: Most information on this screen derives from measurements performed on each of the twisted-pairs, one pair at a time. See the Overview screen for more complete information on continuity or shorts between pins of unrelated pairs.

What is on this Screen?

Cable Type: The **Cable Type** drop down list allows you to select from 100 and 120 Ohm unshielded (UTP) and screened (ScTP) twisted-pair cables terminated with RJ-45 modular connectors. The analyzer can also be configured to optimize tests according to characteristics for a variety of cable types, such as UTP-Cat5 and ScTP Cat-6.

Note: The correct cable type must be selected for optimal measurements to be obtained. Category 5 is the default setting until it is changed.

Color Coding: The wiring color code displayed both in this screen and the **Cable Test | Overview** screen is based on either T568A (default) or T568B wiring.

For reference, the wiring color code for T568B is pairs 1,2 are orange, pairs 3,6 are green, pairs 4,5 are blue, and pairs 7,8 are brown.

The wiring color code for T568A is pairs 1,2 are green, pairs 3,6 are orange, pairs 4,5 are blue, and pairs 7,8 are brown.

Units: Lengths can be displayed in either Feet or Meters. The resolution is one foot or one tenth meter.

Wire Pair, Impedance, Length to end, Length to reflection, and Status/Anomalies: Detail on Wire Pair, Impedance, Length, and Status/Anomalies are presented. The anomalies the analyzer detects and the conditions the analyzer looks for are explained below.

Note: "*p*" is (Greek letter rho) the reflection coefficient.

Open (*p* is less than -50%) - A wire pair that is electrically unconnected, both ends ending at the same location.
Short (*p* is greater than +50%) - A wire pair that is electrically connected together at its end with a low resistance connection. This is typically due to a fault at a punch-down patch panel.
Terminated End of Cable (*p* is greater than +/-0.5%) - +/- 0.5% represents a +/- 1 Ohm

mismatch, much better than typical installations.

Terminated at Active Device (*p* is greater than +/- 0.5% and is less than +/- 7%)

Unidentified Anomaly (*p* is greater than +/- 6% and is less than +/- 15%, but is not identified as an active device) - A miscellaneous impedance imperfection. This may be due to cable damage such as crimping, crushing, stretching, pinching or splicing. poor assembly techniques at connectors and punch-downs; excessive lengths of separated untwisted wire; dirty oxidized connections; or connector hardware with inferior electrical properties.

Errors, Warnings, Info

An error, warning, or information symbol ●▼! is presented next to a wire pair if certain conditions occur. These conditions are as follows:

● Errors	▼ Warnings	! Info
Red indicates an open or mis-wired wire, that the voltage level may be too low causing the link signal to drop, or out of impedance level greater than 15%.	*Yellow* indicates an out of range impedance value greater than 10%, or a voltage level that is less than the optimum voltage level. In a less than the optimum voltage level condition, an intermittent link signal may occur with excessive FCS errors.	*Blue* indicates condition that is not necessarily an error such as a detected swap cable.

Transmit/Receive Info

Receive Wire Pair indicates which wire pair the receive Rx signal is traveling relative to the analyzer. Wired for MDI, Rx is on 3-6; MDI-X, Rx is on 1-2.

Transmit Wire Pair indicates which wire pair the transmit Tx signal is traveling relative to the analyzer. Wired for MDI, Tx is on 1-2; MDI-X, Tx is on 3-6.

Receive Voltage indicates the peak-to-peak receive signal amplitude. The value is displayed in millivolts.

Received Polarity can be normal, inverted or unknown.

Transmit Polarity can be normal, inverted or unknown.

Wire Mapper Info displays the Wire Map Adapter ID number (if wire mapper is present), and whether the cable is shielded or unshielded (if wire mapper is present).

Clicking the **Rerun Cable Test** button can be used to repeat the cable testing at any time.

Note: The cable tests are automatically run when:

Ÿ a cable is connected to the analyzer

Ÿ a terminating device is connected to the far end of the cable, e.g., hub, switch, or

NIC

Ÿ a terminating device is disconnected from the far end of the cable

Ÿ link is lost due to disconnection or other reason, e.g., hub power is turned off

See also: Fiber Test

Setting Up the Fiber Optic Test Kit

This test measures optical power in units of dBm and microwatts. It also determines calculated optical power loss (attenuation). The loss value (in dB) is the difference between the level measured on a nearly lossless, short reference cable and the power level measured across the fiber cable under test.

You can measure optical loss and output power on multimode or singlemode cable, the two types of fiber in common use. Multimode has a bigger core and is used with LED sources at wavelengths 850 nm and 1300 nm for LANs. Singlemode has a smaller core and is used for WAN, telephony, and CATV applications with laser sources having wavelengths of 1310 nm or 1550 nm. Singlemode is often employed in backbones as well.

For more information on results from this test, check Fiber Test Dialog.

Testing fiber optic cable requires the following:

Ÿ A Fluke DSP-FOM (Fiber Optic Meter - check www.flukenetworks.com for ordering information).

Ÿ A multimode fiber optic source (such as is included with the Fluke DSP-FTK).

Ÿ Two fiber optic patch cables (provided with DSP FOM and DSP-FTK). Make sure they are "tested good."

Ÿ Latest Analyzer firmware.

Ensuring Accurate measurements

Ÿ Maintain clean fiber connections and clean connections as needed.

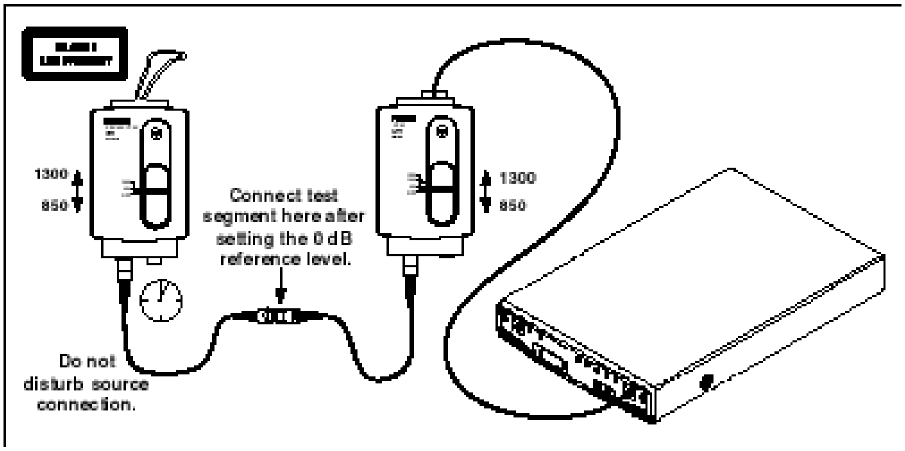
Ÿ Before using the optical source, turn it on and let it stabilize for at least two minutes. In colder climates, it will require more time to stabilize.

Ÿ Run the OptiView Analyzer Self Test to verify the FTK Subsystem passes self test.

Setting a Reference

Measuring an installed cable's optical loss requires that you first set a reference level by measuring the source power, less the loss in fiber patch cables and connectors as follows:

1. Make the connections shown below.


1300
850
Connect test segment here after setting the 0 dB reference level.
1300
850
Do not disturb source connection.

2. Make sure to properly match cables and FOS (multimode with 10 mW source,

singlemode with 100 mW source). When setting the reference use the same type of cable as the cable you wish to test (multimode 50/125 µm or 62.5/125 µm, singlemode 9/125 µm).

3. Make sure the FOM is connected to the analyzer's 10/100 BASE-TX port. Use a short (<= 3m/10ft), non-crossed twisted pair patch cable (may be shielded or unshielded). After you make the connections, switch on the fiber optic source and meter and let it stabilize.

Important! Ensure that the wavelength setting of the FOS matches the setting on the FOM and that the correct corresponding output connection from the FOS is used. Otherwise, measurements will be invalid.

4. From the Analyzer's Front Page, press Cable Test then the **Fiber Test** tab. If all connections are properly made, the Analyzer detects the active fiber optic meter and the wavelength setting of its switch.
5. Set the reference by pressing the **Set** button. A note displays reminding you of set up requirements. Press **OK** to proceed. This causes the current power reading to become the reference point for testing cables. It represents a baseline amount of power emitted by the source.

Setting the Loss Budget

Sometimes called Loss Limit, the purpose of setting a Loss Budget is to test the integrity of installed cables and to ensure network equipment will work over the installed fiber optic link. It is best to be conservative over the specifications and give yourself some margin. Make the threshold high enough so if you try to set the power to the maximum amount of loss expected, it is still within the power range of your meter.

1. After setting the reference, do not disturb the source as you connect to the installed cable to set the Loss Budget.
2. After you have connected the cable to be tested, press **Set** (Loss Budget) in the configuration area. Press the up or down arrow buttons to enter a value.
3. What loss is acceptable? ANSI/TIA/EIA-568-B defines the acceptable loss based on calculating the sum of loss of the individual components. Below is a list of values specified in ANSI/TIA/EIA-568-B.
    - for each connector, <0.75 dB loss.
    - for each mechanical splice, <0.3 dB (standards based).
    - multimode fiber - loss is 3.5 dB per km for 850 nm, 1.5 dB per km for 1300 nm. This equates to roughly 0.1 dB per 100 feet for 850 nm, 0.1dB per 220 feet for 1300 nm.
    - singlemode fiber (outside plant) - loss is 0.5 dB per km for 1310 nm and 1550 nm, a loss of 0.1 dB per 656 feet for 1310 nm and 1550 nm sources.
    - singlemode fiber (inside plant) - loss is 1.0 dB per km for 1310 nm and 1550 nm, a loss of 0.1 dB per 328 feet for 1310 nm and 1550 sources.
    - loss = (0.75 dB X # connectors) + (0.3 dB X # splices) + loss of fiber cable. Check this sample calculation.
    - If you are testing to a specific application such as Gigabit Ethernet over multimode 62.5/125 µm cable at 850 nm, this will have a fixed loss. In this case it would be 2.38 dB. Refer to IEEE standards for the specific values.

4. If you have high loss in a cable, reverse the cable and retest in the opposite direction. This can help you isolate a bad connector or the cable itself.

Warning: Never look directly into the fiber optic source connector or attempt to adjust or modify the source. Doing so might expose you to hazardous radiation and damage your eyes.

Read the instruction sheet provided with the DSP-FOM/FTK for specifications and maintenance information for the fiber optic meter and source.

Fiber Inspector

The OPV-FT500 OptiView™ Fiber Inspector option is a video microscope that connects to an OptiView™ analyzer and allows you to inspect the ends of fiber optic cables. The probe’s 400X magnification reveals dirt, scratches, and other defects that can cause poor performance or failure in fiber optic networks.

The product consists of two main pieces:

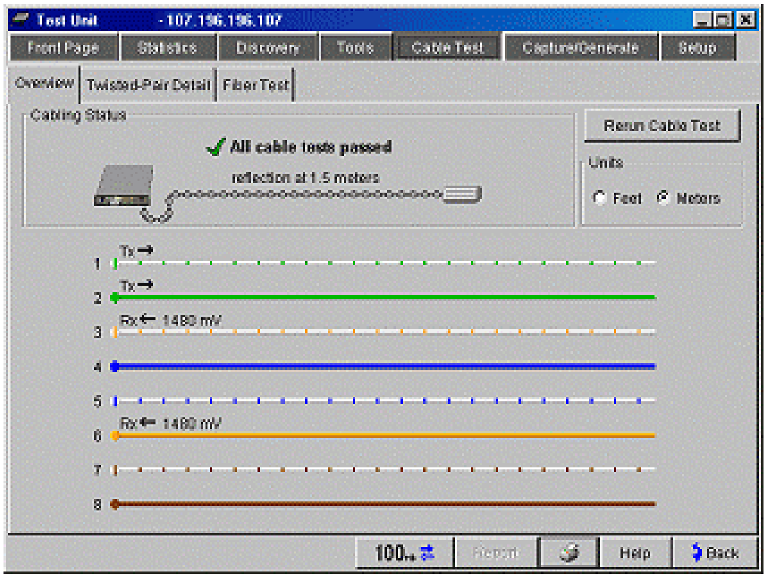
- The probe and signal conversion box
- The software application that allows you to use the product with your OptiView analyzer

The OptiView™ Fiber Inspector option includes the following items:

- 400X video inspection probe with NTSC output
- Conversion Box for NTSC-to-USB signal conversion and video probe power supplies
- Probe adapter tips (SC, ST, FC, & universal for 2.5 mm patch cords)
- Fiber Inspector Getting Started Guide (with example endface images)
- OptiView Driver Installation CD
- Warranty/Registration Card
- Registration Incentive Card

Cable Test Screen Help

Select any area on the graphic below for more information.



Test Unit - 107.196.196.107

Cabling Status

✓ All cable tests passed

reflection at 1.5 meters

Units

○ Feet ● Meters

1 Tx →

2 Tx →

3 Rx ← 1480 mV

4

5

6 Rx ← 1480 mV

7

8

Capture/Generate

Packet Capture Filter

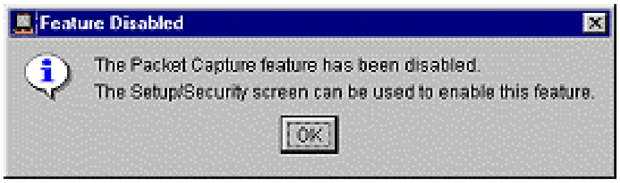
Without any modifications to this screen, you can start capturing packets on your network. Any time you see a [Filter] button in a screen, that button will take you to this screen. If you have highlighted a device in the Discovery screen and clicked [Filter], you will see that name populated automatically in the **Source name** field of this screen. It's that easy!

This screen enables you to customize the information you want to store in the capture buffer, eliminating useless information you do not wish to view. You can then click the [Launch Packet Viewer] button and launch the optional OptiView Protocol Expert (if it is installed on your PC) to perform protocol analysis on the packet capture buffer on the OptiView Workgroup Analyzer. Clicking this button launches OptiView Protocol Expert if it is installed on your PC (OptiView Protocol Expert is purchased separately). You can also just save the packet capture buffer contents to a file for later retrieval by clicking [Save File...].

Note: If you wish to view packets transmitted by the analyzer, the analyzer must be configured to 10 Mb half duplex, or 1000 Mb with an external physical interface (PHY). Received packets are seen in both half and full duplex modes. Setting to half or full duplex is configured in the **Setup | Ethernet** screen. This applies to 10/100 Mb only, since gigabit must run in full duplex.

The left column in the Packet Capture Filter screen represents the current list of active protocols on your network. The list is continually updated. The protocols that appear on your network may only be a subset of all protocols that can be detected by the analyzer. For a complete list of protocols the analyzer can detect, see the Protocol List. The packet capture filter will filter only those protocols that are in the left column, thus eliminating the need to filter out protocols not currently being used on your network.

Note: Packet Capture can be password protected or disabled through Setup | Security. It is grayed out when it has been disabled. The first time you go to a disabled Packet Capture screen, the following message is displayed:



Feature Disabled

The Packet Capture feature has been disabled.
The Setup/Security screen can be used to enable this feature.

Screen Components

Note: If the capture buffer contains data from a previous capture (Start/Stop Capture), and a new filter is set up, a message [Buffer≠Filter] is displayed indicating the capture buffer contents do not match the filter settings. This just means that when you run a new capture, the contents of the capture buffer will be overwritten. If you see Buffer≠Filter, and you are not sure if you want to overwrite the capture buffer contents, simply click the Save File... button and save the current contents of the capture buffer to a file.

Protocol (left column on screen)

Highlight a protocol from the protocol tree in the left column to filter by protocol. Protocols appear in this column as they are detected on your network, e.g., protocols that have not been detected will not appear in this list. A grayed protocol indicates that the **Clear Counts** button has been clicked in the one of the Statistics screens and that protocol has not been rediscovered (no packets seen using that protocol).

Source and Destination

Allows you to specify the source device and destination devices between which packets will be captured. You may also select a device and then check ☑ Not to exclude that device's packet capture activity. All other devices will be included in the capture.

You will also notice below both address drop-down lists, the MAC address is also supplied. If an IP or IPX protocol has been selected, then there is a choice to filter on IP or IPX addresses instead of MAC addresses.

Filtering on a particular IP address can be very useful when monitoring devices that have multiple IP addresses.

● → select this radio button to filter only on packets being sent from the left address to the right address.

● ← select this radio button to filter only on packets being sent from the right address to the left address.

● ↔ select this radio button to filter on all packets being sent between the two different addresses.

Packet Type

Allows you to further filter down to the packet types: Errors, MAC Broadcast, or MAC Multicast. You may also select a packet type and then check ☑ Not to exclude that type of packet from the capture. All other discovered packet types will be captured.

Encapsulation

Allows you to further filter down to the packet encapsulation types: Ethernet II, SNAP, or 802.2. You may also select an encapsulation type and then check ☑ Not to exclude that encapsulation type from the capture. The encapsulation choice 802.3 (raw) is also available when filtering packets of the IPX protocol.

Buffer Configuration

Stop when full - When "Stop when full" is selected, and the packet capture buffer becomes full, packet capture stops. The packet capture buffer size is set through the Buffer Size drop-down list (see Buffer Size below).

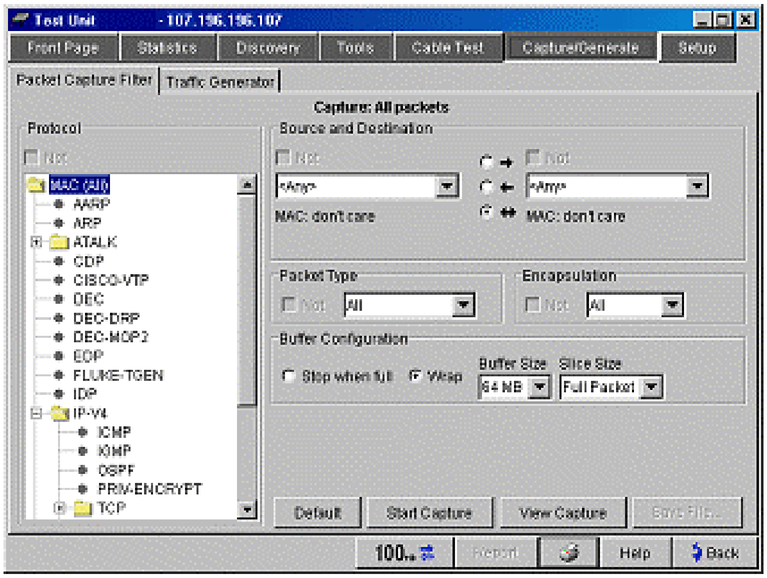
Wrap - Select Wrap to allow packet capture to continue even after the capture buffer is full. The first packets are discarded and replaced by the last captured packets until Stop Capture is selected.

Buffer Size - Can be 1, 4, 8, 16, 32, or 64 Mbytes. Select the smallest buffer size that will still allow you to view the data you want to view. A smaller buffer size will allow faster transport if you save the capture buffer to a file (.cap), and will also allow faster inspection when you view the capture buffer.

Slice Size - Determines how much of the packet is captured. The first 128, 256, 512 bytes can be captured, or Full Packets can be captured.

Default

Resets this screen to the following default values:



Capture: All packets

Protocol: □ Not; MAC (All)

Source and Destination: □ Not <Any> MAC: don't care; ○ → ○ ← ● ↔; □ Not <Any> MAC: don't care

Packet Type: □ Not All

Encapsulation: □ Not All

Buffer Configuration: ○ Stop when full ● Wrap; Buffer Size 64 MB; Slice Size Full Packet

Start Capture

Click this button to start the packet capture process. As soon as the packet capture process starts, this button is replaced with **Stop Capture**. Click **Stop Capture** to stop the capture process. If **Stop when full** is selected, the capture will automatically stop when the packet capture buffer is full.

View Capture

This button is only available if you have purchased the OptiView Protocol Expert (formerly Protocol Inspector) protocol analysis application and have installed it on the same PC that is running the remote user interface software

View Capture launches the OptiView Protocol Expert packet viewer application which downloads the contents of the analyzer's capture buffer and displays the decoded packets. Within the OptiView Protocol Expert application, you may open a previously saved packet capture file.

Note: The OptiView Protocol Expert decode view window takes about 15 seconds to open. Only one user at a time can load the contents of the packet capture buffer. If multiple remote users click the **View Capture** button at nearly the same time, the first occurrence will launch the OptiView Protocol Expert application and load the contents of the packet capture buffer from the analyzer. The other user will launch the OptiView Protocol Expert application, but will not load the contents of the packet capture buffer. A message in the OptiView Protocol Expert application will display "*busy uploading, try again later*."

Within the OptiView Protocol Expert application, the packet capture can be saved in Sniffer format by selecting the **Tools | Snoop to Sniffer Conversion** menu item.

Note: The OptiView Protocol Expert application is purchased separately. Contact Fluke Networks Sales/Service Center for ordering information.

Save File...

Saves the contents of the packet capture buffer to a capture buffer file (.cap) on the remote controlling PC under the default directory /Captures. You may open the saved file by clicking **View Capture** or you can open it directly using the OptiView Protocol Expert application.

Note: The contents of the packet capture buffer is automatically loaded into the OptiView Protocol Expert decode view window. If the contents of the packet capture buffer is empty, the OptiView Protocol Expert decode view window will display "Empty Buffer".

Once OptiView Protocol Expert is opened, you may load existing packet capture files by selecting **File | Open** from the menu bar.

Note: The captured data can be viewed by any tool that reads Snoop file format version 2 (RFC 1761).

Traffic Generator

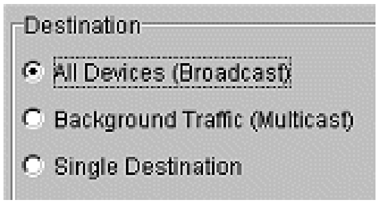
The Traffic Generator screen enables the creation of different traffic loads to stress test the network. The type of protocol, size of packet, number of packets per second, and percent utilization are configurable along with the type of traffic, e.g., Broadcast, Multicast, or to a specific Device. Traffic can be generated to devices on the local network or to devices specified outside of the local network.

WARNING: This feature should only be used by highly skilled IT professionals. Failure to use this feature correctly could result in unacceptable network utilization.

After setting the **Destination** and **Traffic** fields and slide bars, click **Start** to initiate traffic generation. Click **Stop** to terminate the traffic generation. The lower portion of this screen shows a graphical representation of switches, routers, and hosts that traffic is reaching.

Note: If the Traffic Generator is run from a remote user interface, and all remote user interface connections fail, the analyzer will terminate the Traffic Generator session as a safety precaution

Destination Block Description



Destination

● All Devices (Broadcast)

○ Background Traffic (Multicast)

○ Single Destination

	All Switch Ports	Processed by NIC
All Devices (Broadcast)	yes	yes
Background (Multicast)	yes	no
Single Destination (Unicast)	depends on results of switch seeding*	only one NIC

***Note:** See Switch Seeding section below.

All Devices (Broadcast)

Select this for loading network and hosts on the local broadcast domain (up to the first router). Traffic is sent to hosts in the local broadcast domain. The destination MAC address of the frame is set to FFFFFFFFFFFF. All devices will process this packet.

Background Traffic (Multicast)

Select this for loading only the network (no hosts). Traffic goes to the Host NIC card and stops. It is not processed by the NIC card. The frame is sent with a destination MAC Multicast address. The packet is forwarded by switches and routers. No other devices will process it.

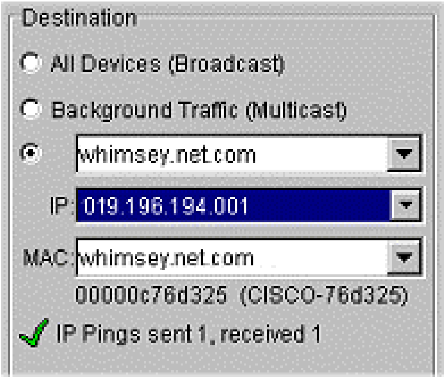
Single Destination

Choices vary by protocol selected. They are different for IP and non-IP protocols. For IP protocols, the device name or IP address, and MAC address can be specified. If the device selected supports multiple IPs (such as a switch), then the IP field drop-down list will become enabled and selectable. Typically, the IP address and MAC address will be for the same device. This would be a non-routed packet. But the destination MAC address can be changed to a router MAC address. A router that is different than the analyzer's default router can easily be selected. For Non-IP protocols, only the destination MAC address can be specified.

Note: The device list may contain devices outside of your local network (broadcast domain). These devices were discovered by the analyzer when a Ping or Trace Route was performed to an out of network (off-net) device.

Select **Single Destination** and then select a traffic destination device. The traffic destination device is the name of the device or for IP protocols, its IP address. It may be in the local broadcast domain (On-net) or outside the local broadcast domain (Off-net). On-net devices are those which reside in the same subnet as the analyzer (the analyzer's IP address is shown in the lower-left-corner of this screen)

For example, a device with an IP of 10.196.195.0 and a subnet mask of 255.255.255.0 will be in the subnet 10.196.195. Any device (1 - 254) with this subnet would be considered an On-net device.



Destination

○ All Devices (Broadcast)

○ Background Traffic (Multicast)

● whimsey.net.com

IP: 019.196.194.001

MAC: whimsey.net.com

00000c76d325 (CISCO-76d325)

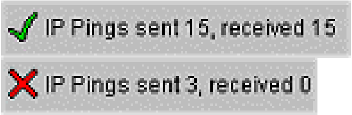
✓ IP Pings sent 1, received 1

Note: The MAC address must be a Unicast MAC address. It can not be a Multicast or Broadcast MAC address. By definition, the least significant bit of the most significant byte (1st byte) must be an even number (i.e., 0, 2, 4, 6, 8 ,a, c, e) to be a Unicast address.

Switch Seeding

When **Single Destination** is selected and a device name or IP address is entered, the analyzer will attempt to solicit a response from that device. This is to insure that the selected device appears in the forwarding table of every switch in its path. If a switch does not have the target's MAC address in its switch forwarding table, the switch will forward the frame out on all switch ports. Switch port seeding will prevent this (switch does port seeding). If the device does not respond, a ❌ will appear below the **Single Destination** field as shown below. If the analyzer does receive a reply from the selected device, then a ✓ is displayed. The selected protocol determines whether an IP Ping, ARP, or 802.2 TEST request is sent as shown below.

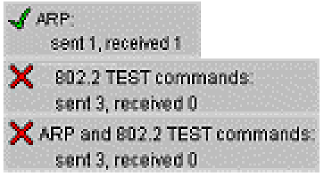
IP Protocols



✓ IP Pings sent 15, received 15

✗ IP Pings sent 3, received 0

Non-IP Protocols

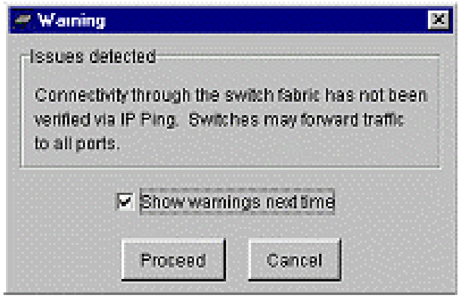


✓ ARP:
sent 1, received 1

✗ 802.2 TEST commands:
sent 3, received 0

✗ ARP and 802.2 TEST commands:
sent 3, received 0

If you start Traffic Generator and the device has not responded, then an error message similar to the one below is displayed informing you that traffic may go out on all switch ports rather than directly to the specified device.



Warning

Issues detected

Connectivity through the switch fabric has not been verified via IP Ping. Switches may forward traffic to all ports.

☑ Show warnings next time

Note: If you inadvertently turn off the above **Issues detected** dialog, it can be turned back on by restarting the user interface session.

Traffic Block Description

Presets - Select from the following predefined list of network utilization rates:

- Custom (use slide bars to right)
- 50% of 512Kbps
- 50% of 1.544Mbps
- 50% of 2.048Mbps
- 50% of 10Mbps
- 50% of 100Mbps

Note: Clicking in the Utilization slide bar and clicking **Page Up** and **Page Down** will cause a preset value to double or half respectively. The up/down arrow keys can be used for fine adjustment.

Protocols - Selects the packet protocol which can be set to the following:

- Benign Ethernet (Ethernet type 1996 hexadecimal) - A legal, unroutable Ethernet frame with random data.
- Benign 802.2 - A legal, unroutable 802.2 frame that has unused DSAP and SSAP

values.

Ÿ NetBEUI - NetBIOS over 802.2 (NetBEUI) with random data.

Ÿ Benign IP - A routable IP packet that has an unused value in the **Next Protocol** field and random data.

Ÿ IP ICMP Echo (bidirectional traffic) - A legal “PING” request (may cause bidirectional traffic).

Ÿ IP UDP Discard - This packet should be discarded by any host that is listening to UDP ports.

Ÿ IP UDP CharGen - Targeted at the “Character Generator” port. This service may not be implemented on all systems. (may cause bidirectional traffic).

Ÿ IP UDP NFS - This packet contains sample data to and from UDP ports that are often used for NFS traffic containing random data.

Ÿ IP UDP NetBIOS - This packet contains sample data to and from the UDP ports used by NetBIOS over TCP/IP containing random data.

Note: When running a packet capture with one of the above protocols selected, the packet viewer will display the packet ASCII description with the analyzer name, serial number, source MAC address, source IP address, and the label "Fluke Networks, Inc.".

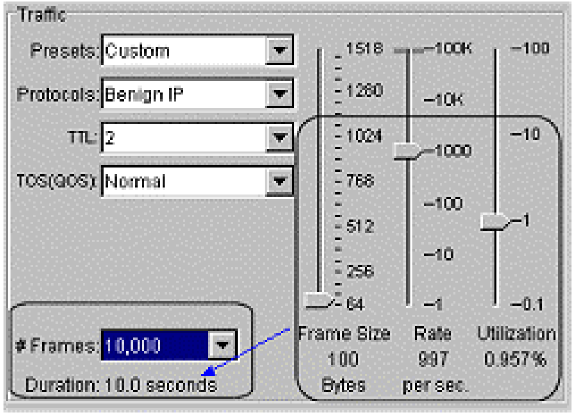
WARNING: Sending any of these frames and packets directly to a host may cause unexpected and undesirable results that may include causing that computer system to fail.

WARNING: Sending IP traffic directly to a host may cause ICMP traffic to be sent back through the network. This traffic may have undesirable effects on the target node and/or intermediate switches and routers.

WARNING: When you send traffic through a router and it overloads its ability to forward traffic, user interface sessions will disconnect.

#Frames - Sets the number of transmitted frames allowed. This value should be set to a small value initially to avoid prolonged undesired network utilization.

The **Duration** field below shows how long the selected number of frames will take at the currently selected frame rate.



Traffic

Presets: Custom

Protocols: Benign IP

TTL: 2

TOS(QOS): Normal

Frames: 10,000

Duration: 10.0 seconds

Frame Size 100 Bytes

Rate 997 per sec.

Utilization 0.957%

TTL - (only applies to IP protocols) Time to Live is the number of router hops, or device jumps allowed before the last device communicated with discards the packet instead of forwarding it. The final device may or may not respond with an ICMP Time-to-Live Count Exceeded packet. The value can be set to 1 through 20, 32, 64, 128, or 255.

TOS(QOS) - (only applies to IP protocols) Type of Service (or Quality of Service) within the packet. It can be set to Normal, based on Minimum Delay, Maximum Throughput, Maximum Reliability, Minimum Monetary Cost, or Maximum Security.

Frame Size - Allows you to set the frame size from 64 to 1518 bytes using a slide bar. The up/down arrow keys allow you to single step through the range. Different Frame Sizes can affect the frame Rate, and vice versa.

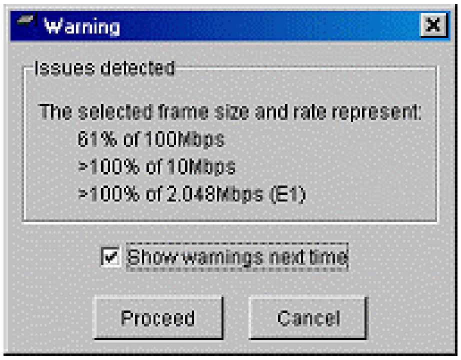
Note: If a gray area appears on the slider, it reflects the largest value of Frame Size which will leave Frame Rate unaffected.

Rate - Sets the transmission rate in frames per second. The upper value varies based on link speed. The up/down arrow keys allow you to make fine adjustments. Different frame Rates can affect the Frame Size, and vise versa.

Note: If a gray area appears on the slider, it reflects the largest value of Frame Rate that will leave Frame Size unaffected.

Utilization - Reflects the Utilization represented by the Frame Size and Rate at the current link speed. Adjustments to Utilization will affect Frame Rate and not Frame Size. The up/down arrow keys perform fine adjustments.

Note: When Utilization is set to greater than 50% and the **Start** button is clicked, a warning is displayed messages based on the Traffic Generator Utilization setting. This warning message is provided as a precaution prior to generating traffic on your network. An example is shown below.



The selected frame size and rate represent:
61% of 100Mbps
>100% of 10Mbps
>100% of 2.048Mbps (E1)

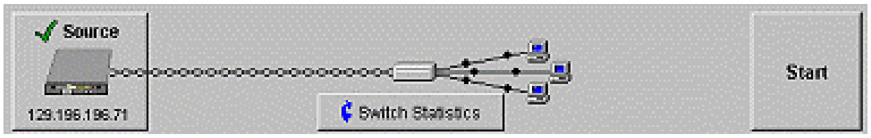
☑ Show warnings next time

Lower Screen Description

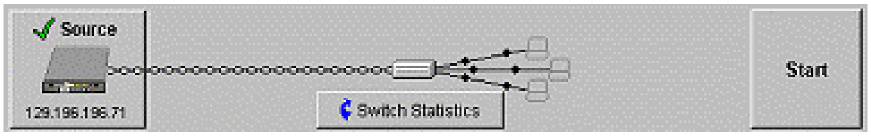
The lower portion of this screen consists of a graphical representation of the analyzer, a switch and/or router, and hosts. This illustrates the direction of traffic. When **Start** is clicked, little graphical balls move from left to right to illustrate traffic generation flow.

Depending on what devices are connected on your network, the buttons **Trace SwitchRoute**, **Switch Statistics**, **Router Detail**, **Traceroute**, and **Host Detail** may be displayed.

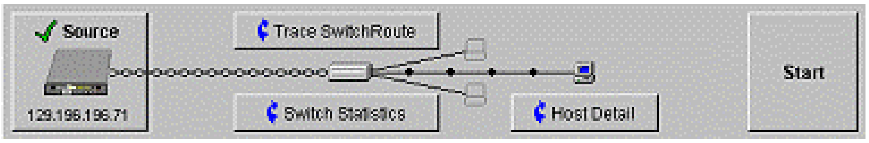
Broadcast - The picture below is of the lower portion of the screen when **Broadcast** is selected. It illustrates that traffic will go from the analyzer through switches, and reach all hosts within the local broadcast domain.



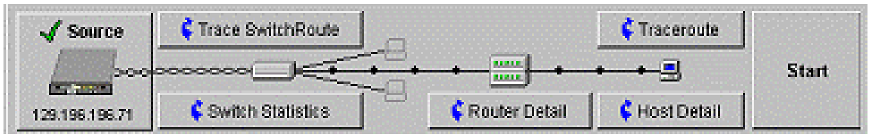
Multicast - The picture below is of the lower portion of the screen when **Multicast** is selected. It illustrates that traffic will go from the analyzer through switches, but will not reach any hosts within the local broadcast domain as indicated by being grayed out .



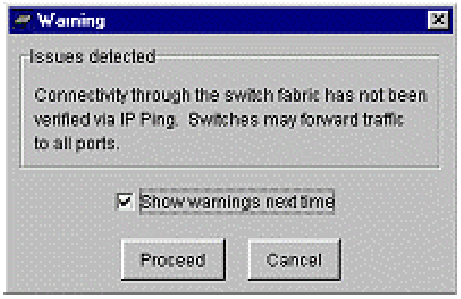
Single Destination - The picture below is of the lower portion of the screen when **Single Destination** is selected. It illustrates that traffic will go within the local subnet from the analyzer through switches, and reach the device selected.



Single Destination - The picture below is of the lower portion of the screen when **Single Destination** is selected. It illustrates that traffic will go within the local subnet from the analyzer through switches, and at least one router.



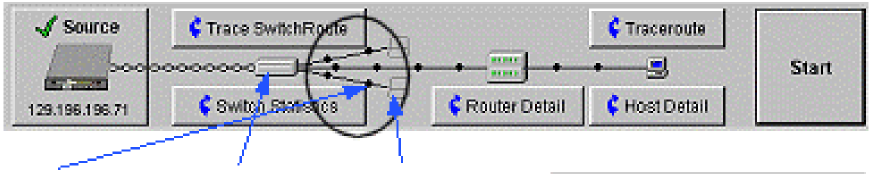
Single Destination - Not responding - If a device does not respond to the IP Ping, ARP, or 802.2 request, and Traffic Generator is started, a warning is displayed as shown below, and a similar traffic flow map is displayed.



Issues detected

Connectivity through the switch fabric has not been verified via IP Ping. Switches may forward traffic to all ports.

☑ Show warnings next time

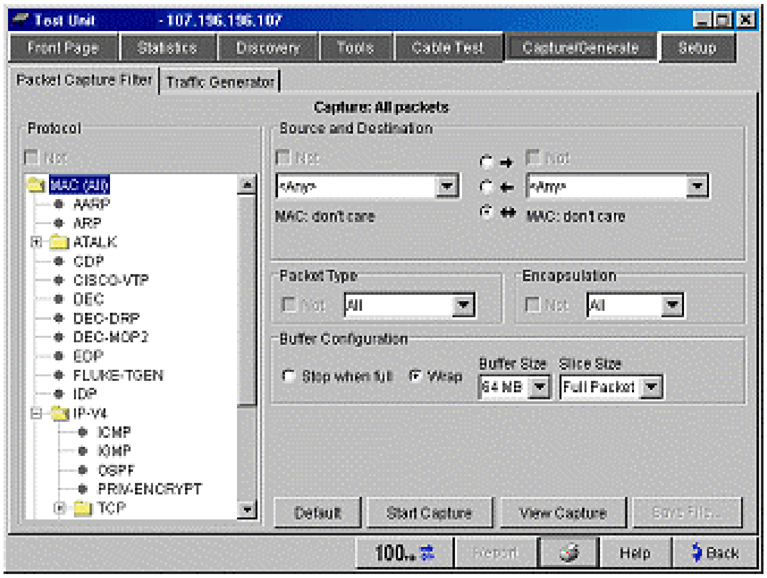


Balls going from switch to grayed hosts
indicate traffic may go out on all switch
ports to all hosts because the analyzer
could not get a response from the selected device.

IP Pings sent 3, received 0

Packet Capture/Traffic Generator Screen Help

Select any area on the graphic below for more information.



Capture: All packets

Source and Destination

<Any>

○ → ○ ← ● ↔

<Any>

MAC: don't care

MAC: don't care

Packet Type: All

Encapsulation: All

Buffer Configuration: ○ Stop when full ● Wrap

Buffer Size: 64 MB

Slice Size: Full Packet

Setup

TCP/IP

It is not necessary to reconfigure this screen. The analyzer will auto configure and determine the best settings (provided Auto Reconfigure on Network Change is checked). It should not be altered unless you are familiar with your network settings. If you do change the settings, and the analyzer is not responding the way you anticipated, select Rerun Auto Config to let the analyzer resume with auto configured settings.

Note: If you do make manual changes to this screen, you must select Apply to make the changes apply to the analyzer. If you are remotely connected to the analyzer via the network test interface, your session will be terminated when you click on the **Apply** button. Reconnect to the remote analyzer by entering the new IP address into the OptiView Browser screen and clicking on the launch user interface button.

When the analyzer is first powered up, or is disconnected and then reconnected to the network, it will go out and determine its IP configuration settings via DHCP. If there is no DHCP response, the analyzer will look at the current IP configuration and determine if it is valid. If it is not valid, the analyzer will select a Local IP Subnet (right column on this screen) based on which IP Subnet has the most hosts. It will then pick an IP address starting with the value stored in the **Find Start Octet** field (top-right on this screen). It will keep decrementing the IP address until an unused IP address is found or after 20 attempts have failed. Auto Config will time out after 20 attempts. If it times out, you must manually configure a valid IP address.

Note: If another device on the network with the same IP address as the analyzer is turned on, the analyzer will stop using that IP address. The status bar at the bottom of the screen will reflect "No IP Address", and the Problem screen will have an error (red ball is displayed) next to the analyzer's IP address.

If the IP address is set to none, IP Discovery will only see active network traffic. IPX networks will still be discovered.

Automatic Configuration Settings

Auto Reconfigure enables the analyzer to go out and select a valid IP address as described above. If it is not checked, the previous IP settings are used so long as they are compatible with the currently attached network.

Rerun Auto Config allows the analyzer to find the best configuration settings.

Find Start Octet increments or decrements the octet value that can be stored in the Source IP address when **Copy to TCP/IP Settings** is selected. The Find Start Octet value only applies when the **Copy** button is clicked, or when **Rerun Auto Configure** is running and DHCP has failed.

TCP/IP Settings

Source is the IP source address the analyzer will use. The drop-down list box will contain all IP addresses that have been used by this analyzer since the user interface was started.

Mask is the subnet mask that determines which part of the IP address is the network number and which part is the host number. For a proper network configuration, the router must be set to the same subnet as the Source IP address and Mask address. Masks that are displayed in blue are "supernetting" masks. A supernetting mask is used to combine several smaller networks into one larger network. A blue mask is dependent on the IP address class selected in the **Source** field (e.g., 8 adjacent Class C subnets would use a mask of 255.255.248.0).

Router is the IP address of the router the analyzer should use to reach hosts not on its subnet. The list of choices includes all discovered routers and any values manually entered by the user.

Primary DNS is the IP address of the Domain Name Server. The DNS is used to look up DNS names and get their IP addresses. If you are having difficulties with accessing other networks, make sure this DNS address and the server are operational.

Secondary DNS is optional. Some organizations have multiple Domain Name Servers, each having unique name lists. The Secondary DNS is never modified by Auto Configure. The Secondary DNS is used only when the Primary DNS has failed.

Apply is disabled until you make a change to any of the TCP/IP settings. You must select **Apply** after making a change in order for that change to affect the analyzer configuration.

Find Unused IP and Apply is used to do a localized search for an unused IP address. The search begins with the IP address that is in the **Source** field. If this address is not currently being used by another device then that value will become the source IP of the analyzer. If the address is being used then the address decrements and this new address will be tested. This continues until an unused IP address is found, or there have been 20 failed attempts. The **Find Unused IP and Apply** button is grayed-out until one of the TCP/IP settings has been changed.

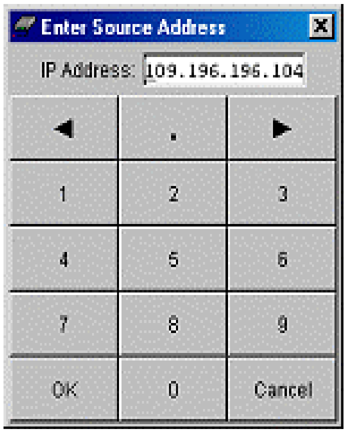
Note: Changing the **Find Start Octet** value does not cause the **Find Unused IP and Apply** button to become un-grayed.

Local IP Subnets

IP Subnets are displayed in this list box along with each Mask and the number of hosts associated with each subnet.

Copy to TCP/IP Settings copies the highlighted Subnet address to the TCP/IP Settings. Source, Mask, and Router values are populated. One of the routers in the selected subnet will become the new selected router. Of course, the user may change these settings at any time. The Source IP address is a combination of the Local Subnet and the Find Start Octet value.

Anytime you see the **IP keypad** button IP, you can manually enter an IP address. Click on this button to launch the IP keypad.

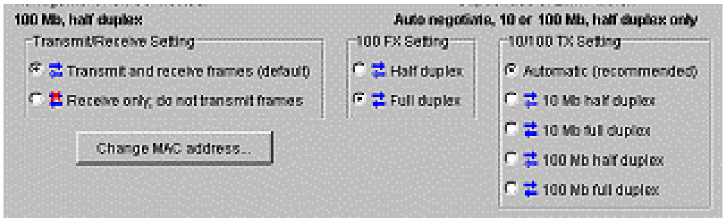


Enter Source Address

IP Address: 109.196.196.104

After entering an address, you must select **OK**.

Ethernet Setup



100 Mb, half duplex

Auto negotiate, 10 or 100 Mb, half duplex only

Transmit/Receive Setting
- ● Transmit and receive frames (default)
- ○ Receive only, do not transmit frames

Change MAC address...

100 FX Setting
- ○ Half duplex
- ● Full duplex

10/100 TX Setting
- ● Automatic (recommended)
- ○ 10 Mb half duplex
- ○ 10 Mb full duplex
- ○ 100 Mb half duplex
- ○ 100 Mb full duplex

10/100 TX Setting

The Ethernet Setup screen allows you to override the default Ethernet port settings. By default the factory 10/100 TX Settings are all set to Automatic.

100 FX Setting

You may also manually select the duplex mode to be half or full duplex. The analyzer automatically detects the duplex mode, so it is not necessary to change this field.

Transmit/Receive Setting

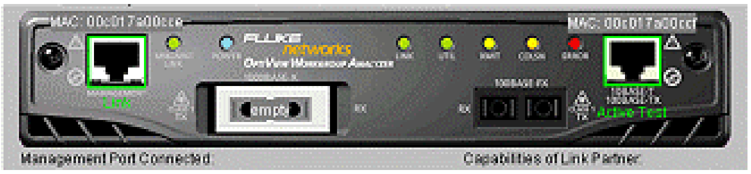
The Transmit/Receive Setting field allows you to disable all transmit activity originating from the analyzer (● Receive only, do not transmit frames). This applies to Packet Capture, Traffic Generator, and during the analyzer discovery of devices and name resolving. Generally, the analyzer will not discover as many devices and resolve as many names with transmit frames disabled. Disabling transmit frames may be particularly important where analyzer generated frames are not allowed (silent mode). By default, transmit and receive frames are enabled.

Change MAC Address (OptiView Analyzer MAC Address)

You may change the analyzer's MAC address. This may be useful to give it a MAC address that looks like a device on your network, rather than a Fluke Networks MAC address. To change the OptiView analyzer MAC address, press Change MAC address... . The Change MAC Address popup is displayed where you can enter a custom OptiView analyzer MAC address. Press the **Factory Default** button to restore the original analyzer MAC address. Press **OK** when finished for changes to be saved.

Active Port

A highlighted port with the word "Active" indicates the port that is currently being used. The instrument's MAC address is also displayed.



MAC: 00c017a00cce
Link
FLUKE networks
OptiView Workgroup Analyzer
empty
100BASE-FX
MAC: 00c017a00ccf
Active Test
Management Port Connected
Capabilities of Link Partner

Note: Make sure you are testing devices that will communicate at the selected port speed; otherwise, no link will be present. If you are not sure, set it to Automatic.

The OptiView analyzer ONLY supports operational loopback in 10 Mb half-duplex mode. "Operational loopback" is the ability to see the OptiView analyzer transmit frames along with the receive frames. Operational loopback is not supported in 100 Mb or 1000 Mb.

Version

This screen is useful if you ever need to troubleshoot the analyzer with Fluke Networks technical support, or determine if you need a software update.

Software

User Interface Version: This number is the local host software version number. This will be either the OptiView analyzer or remote user interface software version number. Compare this number against any software upgrades when you click the **Latest OptiView Software** link.

Data Acquisition Version: The data acquisition module (card) collects network data. The RJ-45 and fiber ports on the analyzer are connected to the data acquisition module. This is the firmware revision number that the module is running.

OS Version (Running UI): PC Operating System.

Hardware

Data Acquisition Module: The manufacture date of the data acquisition module (card).

Network Interfaces: The ports on the data acquisition card. The OptiView Workgroup Analyzer comes in three models: Standard (10/100 RJ45), Pro (10BASE-T, 100BASE-TX, fiber 100BASE-FX), and Pro Gigabit (10BASE-T, 100BASE-TX, fiber 100BASE-FX, and fiber 1000BASE-X)

Help

The **Language** field allows you to select the language in which online Help is displayed. Select the language from the drop-down list.

Latest OptiView Software

To update the analyzer software, select the **Latest OptiView Software** link and follow the on-screen instructions.

NOTE: The software update process can take several minutes depending on the speed of the network connection to the analyzer.

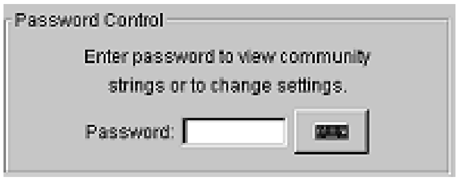
Security

This screen provides instrument security settings for packet capture, remote access, and SNMP configuration.

Feature Selection and Password Control

Allows you to enable/disable packet capture and traffic generation, enable the remote user interface, and set the password for packet capture and traffic generation, and for a remote user access. If you have packet capture and traffic generation enabled with a password, you will be queried to supply a password before any packet capture or traffic generation can occur. This same scenario occurs when the user password is enabled and you are trying to access the instrument remotely.

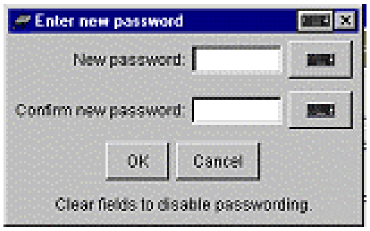
Setting a Password: To create a password, select the Create Password button. Enter a password in the **Enter new password** screen shown below. The password is case sensitive, has a maximum length of 40 characters, and any printable ASCII character can be used, including spaces. Once you have entered a password, you must re-enter it in the **Confirm new password** field. Select **OK** for the password to be accepted.



Password Control

Enter password to view community strings or to change settings.

Password:



Enter new password

New password:

Confirm new password:

Clear fields to disable passwording.

Once a password has been set, and you return to this screen, you will be asked to enter a password.

Fields that are secure are displayed with "*".

Clearing a Password: To clear a password, you must first know and enter the existing password. Once you have entered the password, select **Change Password**. The **Enter new password** screen is displayed. Simply select **OK** to clear the password (leave the **New password** field blank).

Setting the Remote Control PC IP Address

The **Remote Control PC** field is used by the analyzer to send its identification to the IP address specified. Typically this will be the address of the remote PC that will be running the OptiView remote user interface software. With this field set, once an analyzer is connected to a network, the analyzer will then send "hello packets" with its identification to that PC. It does this by transmitting routable messages to either the last PC’s IP address that had connected to the analyzer, or to a statically configured IP address. The analyzers identification will then display on that PC in the OptiView Browser analyzer list. This is particularly useful when the analyzer and PC are in separate networks and the analyzer IP address is unknown.

Note: Discovery "hello" packets are sent periodically from both the Network Test interface and the Management port if both are connected to Ethernet networks and have an active link.

Setting the OptiView Console Address

The OptiView Console application is a PC application for network engineers, LAN administrators, and network technicians who maintain LANs (Local Area Networks). The application allows you to monitor, map, and troubleshoot a LAN segment that could consist of servers, routers, switches, printers, managed hubs, and clients (hosts and other network devices).

The **OptiView Console** field is used to enhance the interoperability of the analyzer and the OptiView Console product. The address you enter should be the IP address of the PC running the OptiView Console program. The analyzer will send packets to this address when it is connected to the network, or when the IP address of the analyzer changes.

These packets assist the OptiView Console product in keeping its information current. OptiView Console maintains a special list of all Fluke Networks' products that are connected to the network and can even be used to launch a user interface session on any analyzer.

OptiView Console is purchased separately. A 7 day evaluation copy can be downloaded from www.flukenetworks.com.

SNMP Community Strings

The **MIB II Read community string**, **RMON2 Read community string**, and **RMON2 Read/Write community string** fields prevent other clients from accessing the MIB II and RMON agent information on the OptiView Pro and Pro Gigabit analyzers.

The RMON community strings are strings that other devices or network management software must use to access the RMON data in the OptiView analyzer. This means that these fields are not available on OptiView Standard models because the Standard does not offer RMON data.

The OptiView analyzer uses the values in the **Strings used to query other SNMP agents** field to query SNMP enabled devices on the network.

Enter the most commonly used community string first, the next most commonly used string second, etc. This way, the analyzer will not waste time using incorrect community strings.

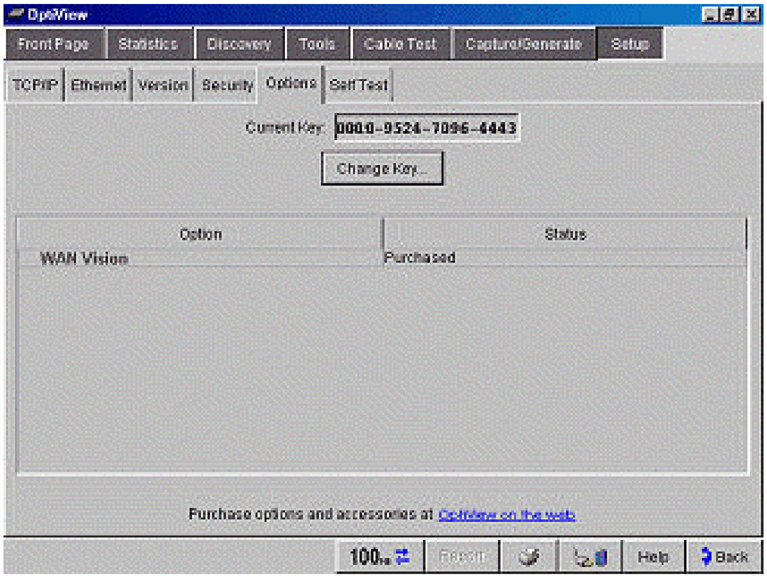
Note: *Strings used to query other SNMP agents* can have multiple entries, each separated by a space. The order they are entered is the order they are searched. RMON agents can have only one community string. The community string field will accept up to 256 characters.

Warning: Do not use the "@" symbol in the community string entry. This will produce inconsistent results and may be very difficult to troubleshoot.

See SNMP Security Issues.

Options

This screen allows you to enable OptiView options (purchased separately) by entering a key code. The key code is obtained by purchasing option either through the Fluke Networks WEB site at www.flukenetworks.com or through your nearest Fluke Networks Sales/Service center.



Current Key: 0000-9524-7096-4443

Option	Status
WAN Vision	Purchased

Purchase options and accessories at OptiView on the web

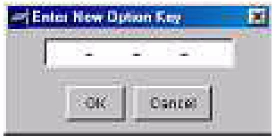
When you initially purchase an OptiView Integrated Network Analyzer with software version 2.5 or greater, you are given a 15 day trial period to explore the WAN Vision option. The WAN Vision option enhances the reporting capabilities of the **Tools | Interfaces | WAN** screen. The WAN option supports the following:

Layer 2 WAN Support:
Ÿ DS1, DS3, SONET, ISDN, Frame-Relay

Layer 3 WAN Support:
Ÿ Frame-Relay and ATM

Layer 3 WAN Private MIB Support:
CISCO-CONN-MIB and CISCO-AAL-MIB

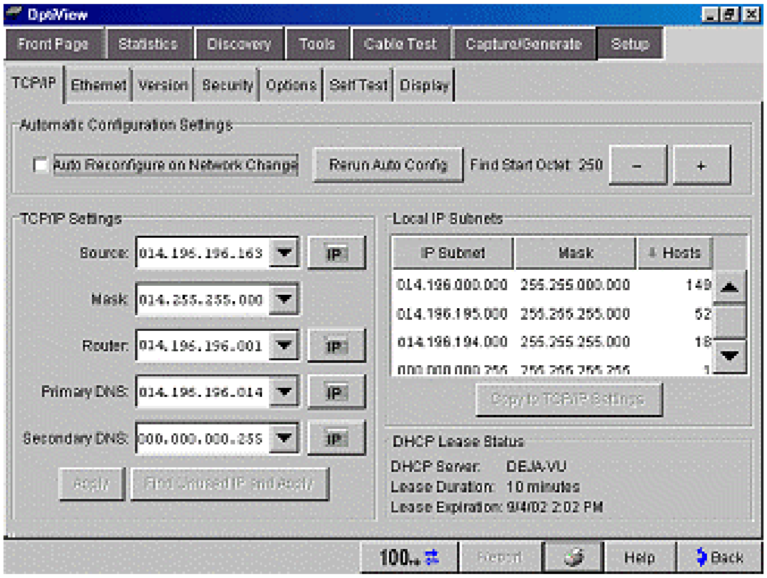
To enter or change a key code, select the **Change Key** button. The Enter New Option Key popup is displayed as shown below.



Enter a new key code supplied by Fluke Networks and press **OK**.

Setup Screen Help

Select any area on the graphic below for more information, or select a topic from the left pane.



□ Auto Reconfigure on Network Change

Find Start Octet: 250

Source: 014.196.196.163

Mask: 014.255.255.000

Router: 014.196.196.001

Primary DNS: 014.196.196.014

Secondary DNS: 000.000.000.255

IP Subnet	Mask	# Hosts
014.196.000.000	255.255.000.000	149
014.196.195.000	255.255.255.000	52
014.196.194.000	255.255.255.000	18
000.000.000.255	255.255.255.255	1

DHCP Server: DEJA-VU
Lease Duration: 10 minutes
Lease Expiration: 9/4/02 2:02 PM

HowTos

Configuring through the Serial Interface Port

You may want to statically configure the analyzer IP address parameters for both the Network-Under-Test and Management ports before connecting the analyzer to a network. The analyzer has a serial configuration port that provides this capability.

To configure the analyzer through the configuration port:

1. Connect the supplied RS-232 cable between the analyzer serial configuration port and a serial port on a PC or terminal.
2. Run a terminal emulation application on the PC to access the configuration port command line interface.
3. Press <Enter> and a prompt will appear that includes the SNMP name of the analyzer. If the analyzer is password protected, a prompt for the password will appear to gain configuration access. If the analyzer is not password protected, configuration access is directly available.

The configuration port, command line interface provides three configuration "modes": Root, Management configuration, and Network configuration. The commands associated with each mode are described below.

Warning: If the analyzer was in the middle of a software updated, and the software update process was interrupted, the analyzer command line interface (serial interface) may look like it is in an infinite loop (hung). If this is the case, the analyzer must be reconnected to where it was connected when the update process was started, and in the OptiView Browser screen, the **Advanced** button and then the **Start TFTP Server** button must be pressed to resume the software update process. An interrupted software update may leave the analyzer un-operable.

Root mode user commands:

"management" Allows the user to enter "Management" configuration mode. This mode allows the user to configure IP parameters for the out-of-band Management port. The text "/Management>" is appended to the prompt while in this mode.

"network" Allows the user to enter "Network" configuration mode. This mode allows the user to configure IP parameters for the in-band Network-Under-Test (NUT) port. The text "/Network>" is appended to the prompt while in this mode.

"default" Restores the analyzer configuration parameters back to factory defaults and reboots the analyzer. Password settings are retained.

“password” Set remote access password (one password for all interfaces). The user is prompted for a password, then again for confirmation. Upon entering a password, password protection will be enabled. If no password is entered, password protection will be disabled. The password is case sensitive, is restricted to 40 characters, and any printable ASCII character can be used (including spaces). If you forget the password, you will need to contact your authorized service center or Fluke Networks product support for procedures. See page 2 for phone numbers.

“remoteipaddr A.B.C.D” Set the IP address (A.B.C.D) of the PC that will be running the user interface software. The analyzer will then send it’s identification to that PC so that the OptiView Browser will display that analyzer for selection. Address is entered in decimal dot notation. See Setting the Remote Control PC IP Address for more information about setting the Remote PC IP address.

“inspectoripaddr A.B.C.D” Set the IP address (A.B.C.D) of the PC that will be running the OptiView Inspector Console software. The analyzer will then send it’s identification to that PC so that the console software can use the analyzer as a data source, receive the problem log from the analyzer and display the analyzer within the “Fluke Tools” device discovery tab.

“exit” Exits the Root mode if password protection is enabled. The user must enter the correct password to regain configuration access.

“show (user command)” Displays the current value of an individual setup parameter of interest within the Root mode.

“show all” Displays the current values of all setup parameters within the Root mode.

Management configuration mode user commands:

“ipaddr A.B.C.D E.F.G.H” Statically assign the IP address (A.B.C.D) and subnet mask (E.F.G.H) of the Management port. Address and subnet mask are entered in decimal dot notation.

“ipaddr dhcp” Enable the automatic configuration of the Management port IP parameters via a DHCP server.

“iprouter A.B.C.D” Statically assign the IP address (A.B.C.D) of the default router on the Management port. Address is entered in decimal dot notation.

“apply” Applies the changes (if any) made to the Management port configuration. Management port configuration changes do not take effect until this command is entered.

“exit” Exits the Management configuration mode. Exiting will discard any Management port configuration changes unless ‘apply’ is entered.

“show (user command)” Displays the current value of an individual setup parameter of interest within the Management configuration mode.

“show all” Displays the current values of all setup parameters within the Management configuration mode.

Network configuration mode user commands:

“ipaddr A.B.C.D E.F.G.H” Statically assign the IP address (A.B.C.D) and subnet mask (E.F.G.H) of the Network port. Address and subnet mask are entered in decimal dot notation.

“iprouter A.B.C.D” Statically assign the IP address (A.B.C.D) of the default router on the Network port. Address is entered in decimal dot notation.

“ippridns A.B.C.D” Statically assign the IP address (A.B.C.D) of the primary Domain Name Server (DNS) on the Network port. Address is entered in decimal dot notation.

“ipsecdns A.B.C.D” Statically assign the IP address (A.B.C.D) of the secondary DNS on the Network port. Address is entered in decimal dot notation.

“apply” Applies the changes (if any) made to the Network port configuration. Network port configuration changes do not take effect until this command is entered.

“exit” Exits the Network configuration mode. Exiting will discard any Network port configuration changes unless ‘apply’ is entered.

“show (user command)” Displays the current value of an individual setup parameter of interest within the Network configuration mode.

“show all” Displays the current values of all setup parameters within the Network configuration mode.

Configuration Port Guidelines

- The analyzer serial configuration port communication parameters are fixed to 9600 baud, 8 data bits, no parity, 1 stop bit.
- Commands are case insensitive. Password is case sensitive.
- Parameters that are applied via the configuration port are retained after turning off the power to the analyzer.
- Entering an invalid command will cause a list of available commands to be displayed for the current configuration mode.
- Entering an invalid parameter to a command (where applicable) will cause a command usage message to be displayed.
- Access to change the configuration will time out after a period of inactivity when password protection is enabled. You will have to enter the correct password to regain configuration access.

Loading Packet Captures Files into OptiView Protocol Expert

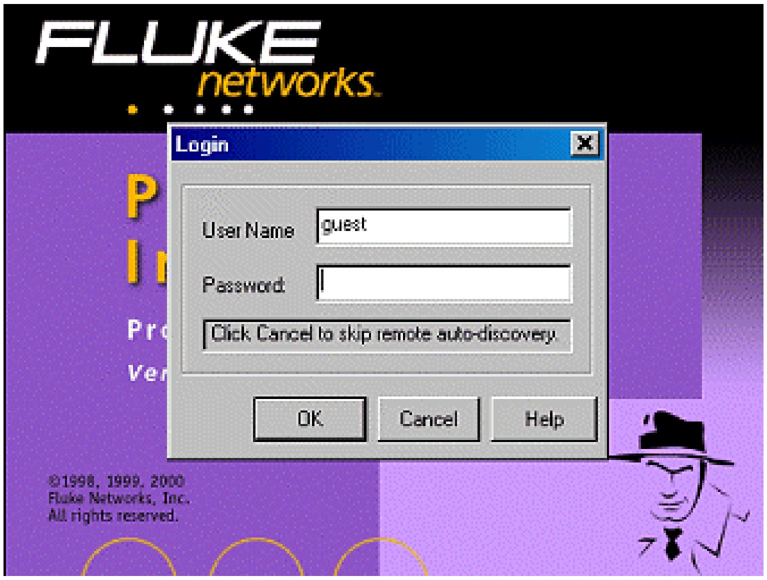
When you press the View Capture button in the Packet Capture Filter screen, OptiView Protocol Expert is opened. The contents of the packet capture buffer are automatically loaded into OptiView Protocol Expert. In OptiView Protocol Expert, you can manually open previously saved packet capture files (.CAP) and manually load the associated name table file (.NAM).

Follow the procedures below to save the Packet Capture file to disk, and manually load it into OptiView Protocol Expert.

1. If you have not saved the Packet Capture to a file, go back to the Packet Capture Filter screen and click the **Save File...** button. The Save dialog is displayed.

   Note: By default, Packet Capture files are saved into the OptiView installation directory under C:\Program Files\Fluke Networks\OptiView\Captures.

   Note: The Save dialog gives a default filename in date and time format (month_day_year_hour_minute_AM/PM).
   Remember this filename, you must load it into the OptiView Protocol Expert application.
2. Click the **Save** button to complete saving the Packet Capture file to disk.
3. The OptiView Protocol Expert Login dialog should now be displayed on your desktop as shown below.



Login

User Name: guest

Password:

Click Cancel to skip remote auto-discovery.

©1998, 1999, 2000
Fluke Networks, Inc.
All rights reserved.

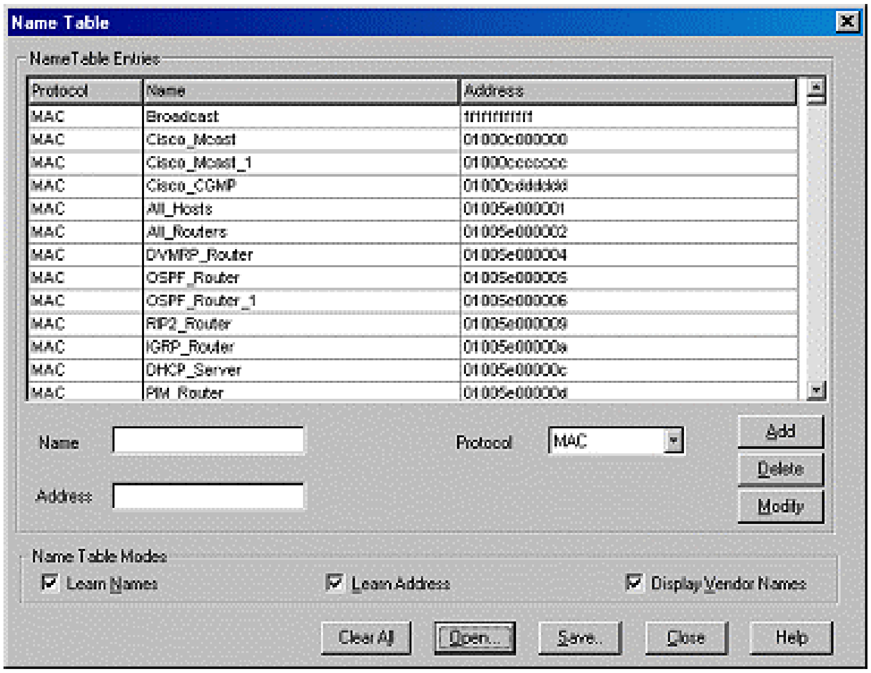
Click on **Cancel** to continue. The above Login dialog allows you to control and monitor specified OptiView Protocol Experts and OptiView Link Analyzers (formerly referred to as Distributed Protocol Inspectors). Since your intention is to view a Packet Capture file, simply click on **Cancel** to continue. Refer to the OptiView Protocol Expert help for usage of the Login dialog.

Loading a Packet Capture File

1. From the OptiView Protocol Expert toolbar, select **File | Open**, or click the button.
2. Browse to the directory where the Packet Capture file is stored. By default it is stored in C:\Program Files\Fluke Networks\OptiView\Captures. Packet Capture files have an extension of .CAP.
3. Highlight the Packet Capture file, and click **Open**.

Loading a Name Table File

A default Name table file is also created and saved in the same directory, with the same filename as the Packet Capture file, except the extension is .NAM. The Name table file contains names associated with known hexadecimal representations as shown below.



Name Table

NameTable Entries

Protocol	Name	Address
MAC	Broadcast	ffffffffffff
MAC	Cisco_Mcast	01000c000000
MAC	Cisco_Mcast_1	01000ccccccc
MAC	Cisco_CGMP	01000cdddddd
MAC	All_Hosts	01005e000001
MAC	All_Routers	01005e000002
MAC	DVMRP_Router	01005e000004
MAC	OSPF_Router	01005e000005
MAC	OSPF_Router_1	01005e000006
MAC	RIP2_Router	01005e000009
MAC	IGRP_Router	01005e00000a
MAC	DHCP_Server	01005e00000c
MAC	PIM_Router	01005e00000d

Name:

Address:

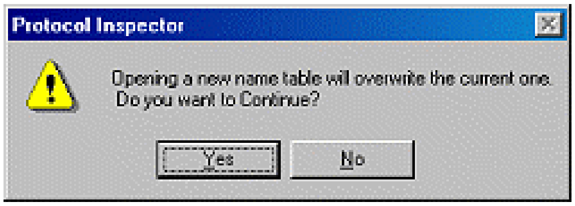
Protocol: MAC

Name Table Modes

☑ Learn Names ☑ Learn Address ☑ Display Vendor Names

To load the Name table:

1. From the OptiView Protocol Expert - Detail View toolbar, select **Tools | Name Table...**, or click the NAM button.
2. Press the **Open** button. The following dialog is displayed.



Protocol Inspector

Opening a new name table will overwrite the current one.
Do you want to Continue?

3. Select **Yes** to continue.
4. Browse to the directory where the Name table file is stored. By default it is stored in C:\Program Files\Fluke Networks\OptiView\Captures. Name table files have an extension of .NAM.
5. Highlight the Name table file, and press **Open**.
6. Click the Name Table **Close** button.

Perform a NIC Test

A NIC test can be performed by disconnecting the computer under test from the network and connecting it directly to an OptiView Workgroup Analyzer. Once the analyzer is connected to the computer, link should establish (orange link light on the analyzer indicates a MDI-X or cross-over connection). Run the user interface software on the PC and look at the user interface Front Page Protocol Statistics and Network Discovery information.

Saving Packet Captures

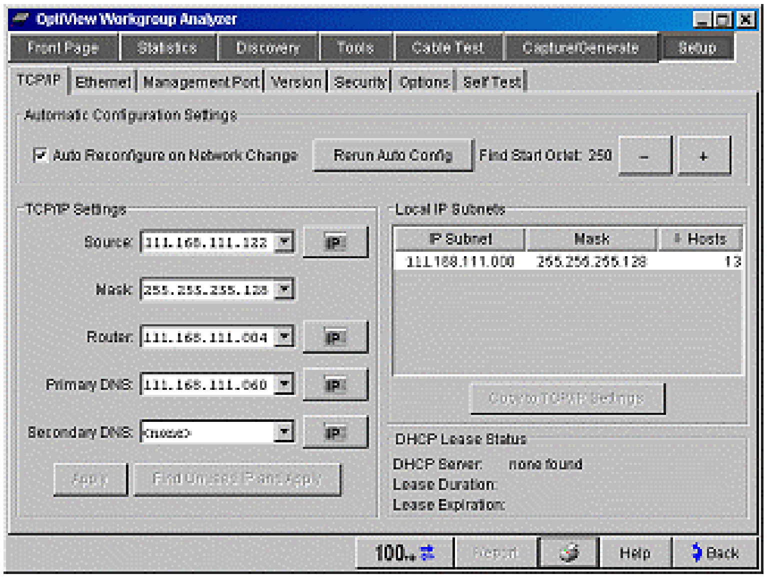
The analyzer Pro and Pro Gigabit versions are capable of filtering and capturing data on your network, and storing the data to disk. Packet Capture files can be saved anywhere you have access to disk space. By default they are saved to your computer in the user interface installation directory under the directory \Captures.

Packet Capture files are saved as .CAP files which can be read by Fluke Networks optional OptiView Protocol Expert (formerly Protocol Inspector) software or by other 3rd party decoder software.

Saving Reports

The analyzer is capable of creating and saving reports from the Discovery Devices, Networks, Problems, Statistics Protocols, Top Hosts, Top Conversations, SNMP Tables, Interfaces, IPX Services, Trace Switch Route, and Trace Route screens. By default they are saved as HTML files to your PC in the user interface installation directory under the directory \Reports.

Setting the Management Port IP Address



Automatic Configuration Settings

☑ Auto Reconfigure on Network Change

Find Start Octet: 250

TCP/IP Settings

Source: 111.168.111.122

Mask: 255.255.255.128

Router: 111.168.111.004

Primary DNS: 111.168.111.060

Secondary DNS: <none>

Local IP Subnets

IP Subnet	Mask	# Hosts
111.168.111.000	255.255.255.128	13

DHCP Lease Status

DHCP Server: none found

Lease Duration:

Lease Expiration:

The Management Port TCP/IP settings can be configured by the following methods:

Ÿ Select **Run DHCP to acquire settings**. This method allows the DHCP server to assign the Management Port's IP address, Mask, and default router IP address. The Source IP, Subnet Mask, and Default Router address are automatically entered in the TCP/IP Settings fields based on the information obtained from the DHCP server.

Ÿ Select **Configure settings manually,** enter the Source IP address, Subnet Mask, and default router IP address. Click **Apply** to make the changes apply to the Management Port configuration.

The Management Port should be configured either through the Network Under Test (NUT) interface connection, or through the analyzer serial interface. When you try to configure the management port IP address through the management port connection, the connection will be dropped when the TCP/IP settings are changed.

Note: In the above picture, ● No Link applies to the NUT interface connection.

Setting the OptiView Inspector Console Address

The Fluke Networks OptiView Inspector Console application (formerly called Network Inspector) is a software application for network engineers, LAN administrators, and network technicians who maintain LANs (Local Area Networks). The application allows you to monitor, map, and troubleshoot a LAN segment that could consist of servers, routers, switches, printers, managed hubs, and clients (hosts and other network devices).

The **OptiView Inspector Console** field is used to enhance the interoperability of the analyzer and the OptiView Inspector Console product. The address you enter should be the IP address of the machine running the OptiView Inspector Console program. The analyzer will send packets to this address when it is connected to the network, or when the IP address of the analyzer changes.

These packets assist the OptiView Inspector Console product in keeping its information current. OptiView Inspector Console maintains a special list of all Fluke Networks' products that are connected to the network and can even be used to launch a user interface session on any OptiView Workgroup Analyzer. OptiView Integrated Network and Workgroup Analyzers can be used as remote agents for the OptiView Inspector Console.

OptiView Inspector Console is purchased separately. A 7 day evaluation copy can be downloaded from www.flukenetworks.com.

Setting the Remote Control PC IP Address

Set this field to specify an off-net PC running the OptiView Browser remote user interface software. By setting this field, the analyzer will send its identification back to the specified PC running the remote user interface software.

Set this field to <none>, <last connected>, or manually enter the IP address of the remote PC that will be running the OptiView Browser remote user interface software. <last connected> is the last remote session to terminate from the analyzer, and that PC's IP address is saved into this field.

This address is configured in the **Setup | Security** screen. Optionally, this address can be configured through the RS-232 configuration port. This is done so that analyzers that are placed on network segments other than the one the controlling PC is on will still automatically show up in the OptiView Browser list of available analyzers.

Note: Discovery hello packets are sent periodically out both the Network Test interface and the Management port if both are connected to Ethernet networks and have an active link.

Setting the NUT Port IP Address

The Network Under Test Interface represents the 10/100-BASE-T, 100BASE-FX, and 1000BASE-X ports. It does not set the IP address of the Management port. To set the IP address of the Network Under Test Interface, select **Setup | TCP/IP**.

Setting Up Traps on OptiView

The OptiView analyzer can be configured to send SNMP Traps for each of the Problems it posts to Discovery Problems. The analyzer uses the RMON2 Trap Destination Table to configure which RMON clients or network management systems should receive the trap.

Overview:

Many RMON client and network management applications have the capability to manage the RMON2 Trap Destination Table. The OptiView analyzer will send any IP SNMP Trap to a Trap Destination with a community of “optiview”. There can be more than one destination configured in the table.

How to manually configure the OptiView analyzer to send SNMP Traps:

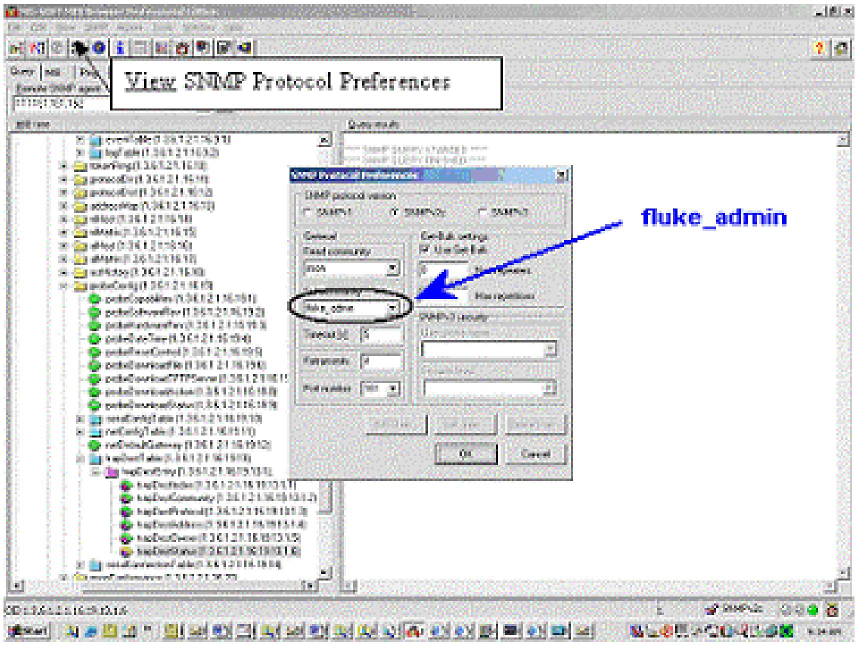
Step # 1: Create entry(s) in the RMON2 Trap Destination Table

Configure IP Address in SNMP MIB Browser

Launch the MG-Soft MIB Browser (supplied with OptiView analyzers and remote control software) and configure the correct IP address of the OptiView agent.

Community Strings

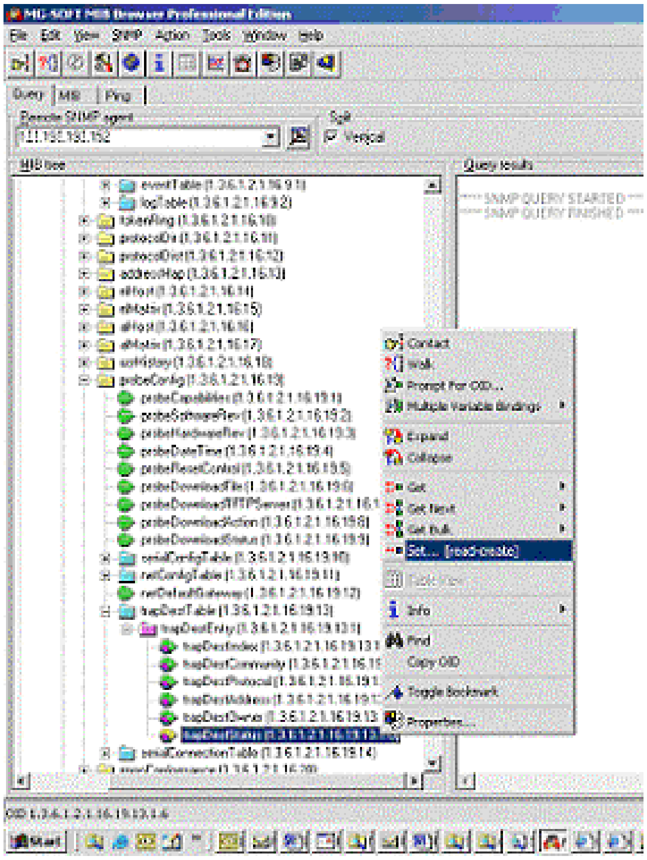
Next, make sure the Read and Write (Set) Community strings are correct. From the MIB Browser menu bar, select **View | SNMP Protocol Preferences** as shown below.



Checking Read & Write (Set) Community Strings

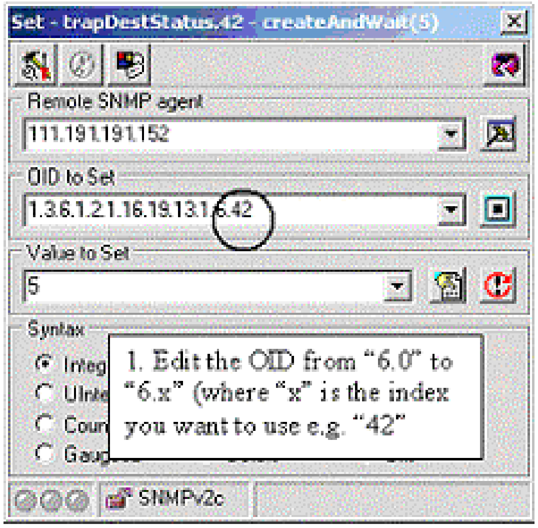
Select TrapDestinationTable and status object

Expand the MIB tree to highlight the object iso(1), org(3), dod(6), internet(1),mgmt(2), mib-2(1), rmon(16), probeConfig(19), trapDestTable(13), trapDestEntry(1), trapDestStatus(6). Then select the SET icon or use the right mouse button, and select **Set...** as shown below.


MG-SOFT MIB Browser Professional Edition
File Edit View SNMP Action Tools Window Help
Query MIB Ping
Remote SNMP agent
Split
Vertical
MIB tree
Query results
***** SNMP QUERY STARTED *****
***** SNMP QUERY FINISHED *****
eventTable (1.3.6.1.2.1.16.9.1)
logTable (1.3.6.1.2.1.16.9.2)
tokenRing (1.3.6.1.2.1.16.10)
protocolDir (1.3.6.1.2.1.16.11)
protocolDist (1.3.6.1.2.1.16.12)
addressMap (1.3.6.1.2.1.16.13)
nlHost (1.3.6.1.2.1.16.14)
nlMatrix (1.3.6.1.2.1.16.15)
alHost (1.3.6.1.2.1.16.16)
alMatrix (1.3.6.1.2.1.16.17)
usrHistory (1.3.6.1.2.1.16.18)
probeConfig (1.3.6.1.2.1.16.19)
trapDestTable (1.3.6.1.2.1.16.19.13)
trapDestEntry (1.3.6.1.2.1.16.19.13.1)
trapDestIndex
trapDestCommunity
trapDestProtocol
trapDestAddress
trapDestOwner
trapDestStatus
Contact
Walk
Prompt For OID...
Multiple Variable Bindings
Expand
Collapse
Get
Get Next
Get Bulk
Set... (read-create)
Table View
Info
Find
Copy OID
Toggle Bookmark
Properties...
OID 1.3.6.1.2.1.16.19.13.1.6
Start

Select the OID to SET, then the right-mouse button, and Select SET...

If the **Table Instance** screen appears when creating a new table row, Close the window to show the **SET** window.



Set - trapDestStatus.42 - createAndWait(5)

Remote SNMP agent: 111.191.191.152

OID to Set: 1.3.6.1.2.1.16.19.13.1.6.42

Value to Set: 5

Syntax: ● Integ ○ UInte ○ Coun ○ Gaug

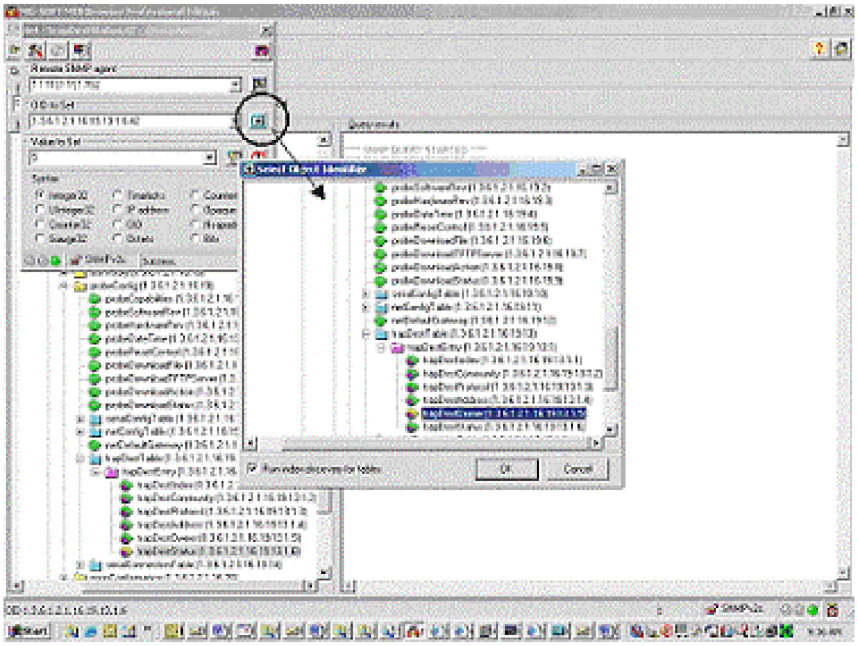
1. Edit the OID from "6.0" to "6.x" (where "x" is the index you want to use e.g. "42"

First SET trapDestStatus to create index (change OID from 6.0 to 6.x) and Value to 5 (Create and Wait)

To create a new row instance, replace the last portion of the “OID to Set” from “1.6.0” to “1.6.x”, where “x” is the index you want to use (can be any 32 bit integer). In the example above, the index being created is “42”, which is being set to a value of 5 (Create and Wait).

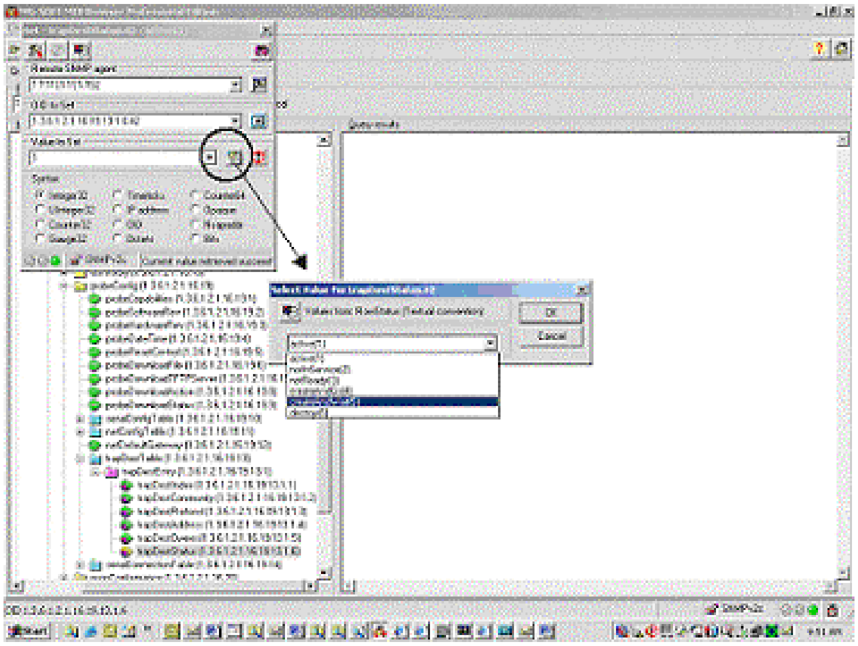
When ready, select the “SET” button.

Note: You MUST change both the OID AND the Value.

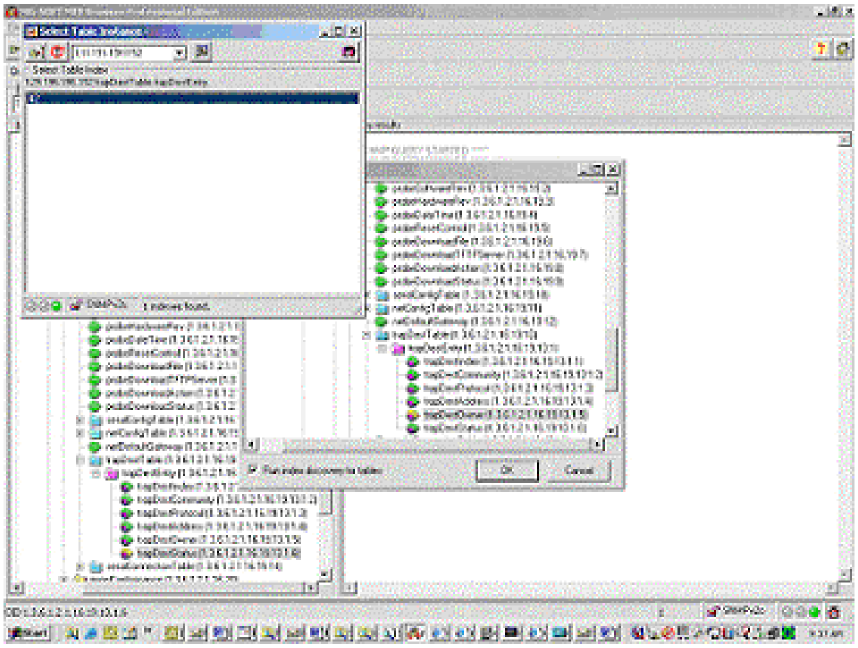


Use "Select OID from Tree" button to select next value

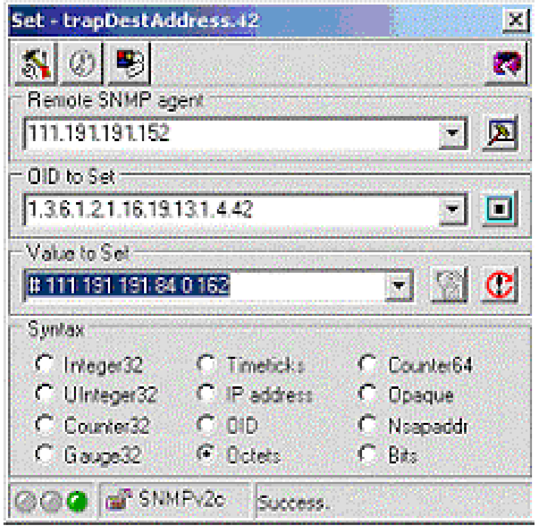
Next, select the row index you created in the previous step, select the “OID to Select” button and select the object “trapDestOwner”. It is customary to set this value to your name and IP address so that others using this analyzer know who created these entries.



Press the "Select Value from List" button, or type a value in "Value to Set" field



After Index is created from previous step, select the new index of the table



Set - trapDestAddress.42

Remote SNMP agent: 111.191.191.152

OID to Set: 1.3.6.1.2.1.16.19.13.1.4.42

Value to Set: # 111 191 191 84 0 162

Syntax:

○ Integer32	○ Timeticks	○ Counter64
○ UInteger32	○ IP address	○ Opaque
○ Counter32	○ OID	○ Nsapaddr
○ Gauge32	● Octets	○ Bits

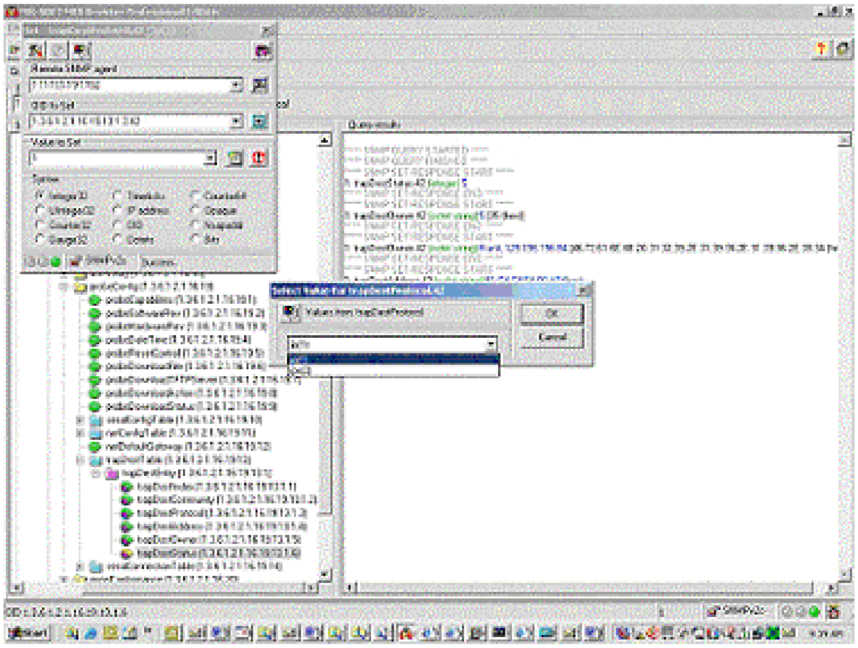
SNMPv2c Success.

Use this syntax to load the correct IP address and Trap UDP port number

Then select the OID to set to “trapDestAddress” using the syntax shown in the figure above.

In this example, the destination IP address where you want the TRAPs to be sent to is “111.191.191.84”. The “0 162” is required as it configures the Trap packets to be sent to UDP port 162.

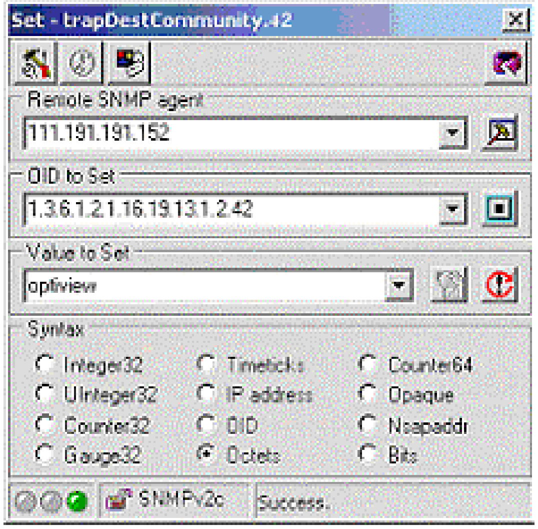
The MG-Soft MIB Browser requires this syntax for this particular field. It MUST start with a “#”, each number needs to be separated with a space, and have “ 0 162” after the Destination IP address.



Select Value for trapDestProtocol.42
Values from trapDestProtocol
OK
Cancel

Select "IP" (1) for Trap Protocol

Next select the OID to Set to “trapDestProtocol”



Set - trapDestCommunity.42

Remote SNMP agent: 111.191.191.152

OID to Set: 1.3.6.1.2.1.16.19.13.1.2.42

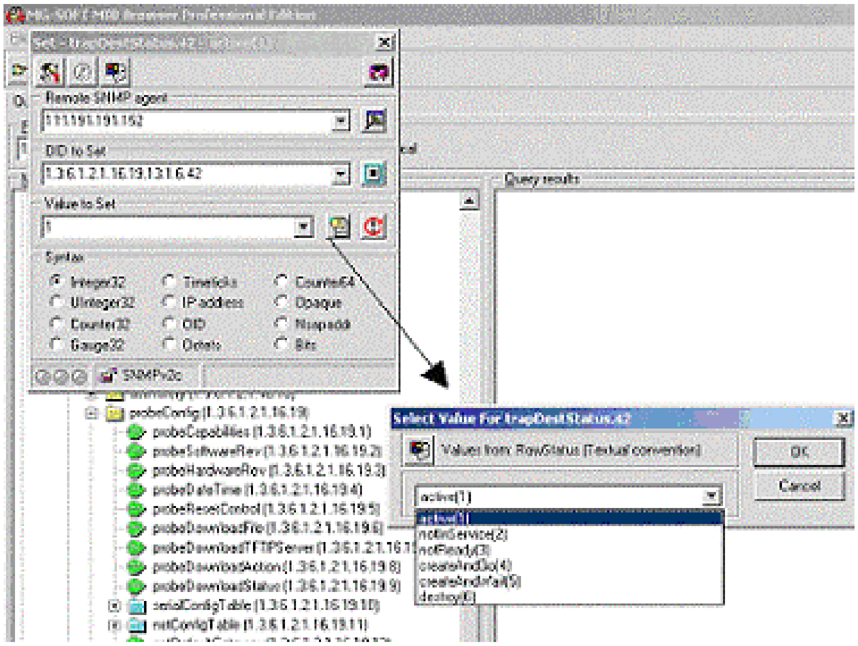
Value to Set: optiview

Syntax: ○ Integer32 ○ UInteger32 ○ Counter32 ○ Gauge32 ○ Timeticks ○ IP address ○ OID ● Octets ○ Counter64 ○ Opaque ○ Nsapaddr ○ Bits

SNMPv2c Success.

trapDestCommunity MUST BE "optiview" for OptiView Analyzer traps to be sent to the correct address

The trapDestCommunity field is used to link the Trap Destination table with the RMON Event table. When events occur and there is an entry in the RMON Event table with a community of “optiview” (lower case), the agent will send Traps to the IP address(s) with the same “optiview” community in the trapDestination Table.



Remote SNMP agent: 111.191.191.152

OID to Set: 1.3.6.1.2.1.16.19.13.1.6.42

Value to Set: 1

Syntax: ● Integer32 ○ UInteger32 ○ Counter32 ○ Gauge32 ○ Timeticks ○ IP address ○ OID ○ Octets ○ Counter64 ○ Opaque ○ Nsapaddr ○ Bits

SNMPv2c

Select Value For trapDestStatus.42

Values from RowStatus (Textual convention)

active(1)

MG-Soft MIB Browser Professional Edition
Query results
probeConfig (1.3.6.1.2.1.16.19)
probeCapabilities (1.3.6.1.2.1.16.19.1)
probeSoftwareRev (1.3.6.1.2.1.16.19.2)
probeHardwareRev (1.3.6.1.2.1.16.19.3)
probeDateTime (1.3.6.1.2.1.16.19.4)
probeResetControl (1.3.6.1.2.1.16.19.5)
probeDownloadFile (1.3.6.1.2.1.16.19.6)
probeDownloadTFTPServer (1.3.6.1.2.1.16.1
probeDownloadAction (1.3.6.1.2.1.16.19.8)
probeDownloadStatus (1.3.6.1.2.1.16.19.9)
serialConfigTable (1.3.6.1.2.1.16.19.10)
netConfigTable (1.3.6.1.2.1.16.19.11)
active(1)
notInService(2)
notReady(3)
createAndGo(4)
createAndWait(5)
destroy(6)
OK
Cancel

After the row values are set, change trapDestStatus to "active" (1)

After setting owner, the destination IP address, the trap protocol and the trap community, finish creating the row by setting trapDestStatus to Active(1)

Listed below is the output from “Query Results” portion of the MG-Soft MIB Browser.

```
***** SNMP SET-RESPONSE START *****
1: trapDestStatus.42 (integer) 5
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: trapDestOwner.42 (octet string) Frank 111.191.191.84
[46.72.61.6E.6B.20.31.32.39.2E.31.39.36.2E.31.39.36.2E.38.34 (hex)]
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: trapDestAddress.42 (octet string) 81.C4.C4.54.00.A2 (hex)
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: trapDestProtocol.42 (integer) 1
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: trapDestCommunity.42 (octet string) optiview
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: trapDestStatus.42 (integer) 1
***** SNMP SET-RESPONSE END *****
```

Deleting a row

To delete the entry, set the status OID to “Delete” (6).
To disable the entry, but leave it in the table, set the status OID to “notInService” (2).
To enable the entry again, set the status OID back to “active” (1).

Test Cable Integrity

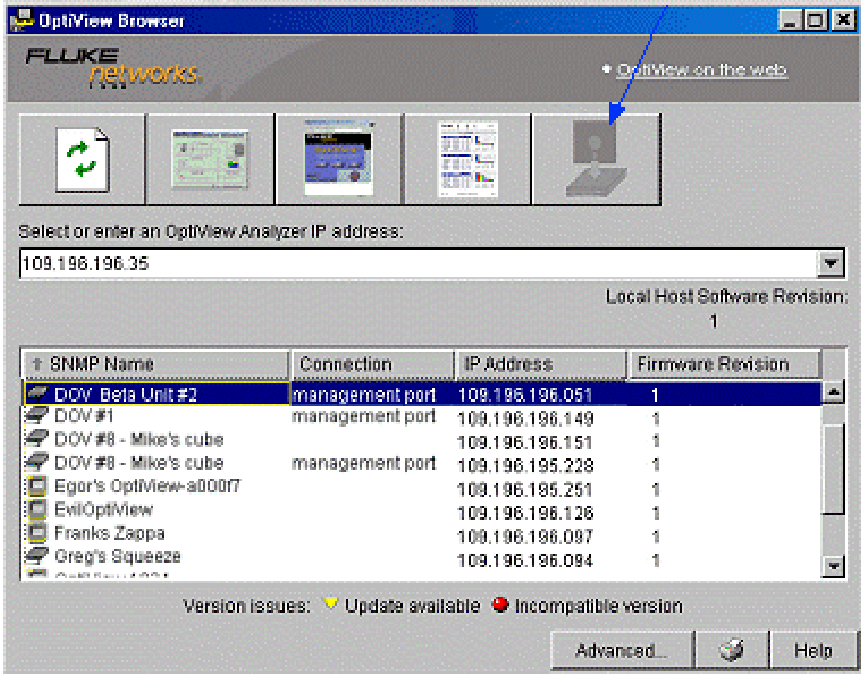
The analyzer Cable Test can test cable wire pair, length, impedance, and status/anomalies (e.g., shorts, opens, termination, and split-pairs).

- Your cable test needs will determine which testing methods are right for you
- You can test cables on the analyzer's 10/100 Network Under Test interface connector
- You can test cables in a live network
- You can test cables using an external wire map adapter (office locator, Fluke Networks part number 1567629) terminating device

In all , you will connect the analyzer to the cable you wish to test and run Cable Test.

Updating the OptiView Workgroup Analyzer Software

Updating the OptiView Workgroup Analyzer software is accomplished through the OptiView Browser user interface as shown below. Simply press the button to start the update process on the selected OptiView Workgroup Analyzer. The software update process must be done through the management port.
Refer to the analyzer help topic Using the OptiView Browser for installation instructions.



Update firmware for selected Workgroup Analyzer

Select or enter an OptiView Analyzer IP address: 109.196.196.35

Local Host Software Revision: 1

SNMP Name	Connection	IP Address	Firmware Revision
DOV Beta Unit #2	management port	109.196.196.051	1
DOV #1	management port	109.196.196.149	1
DOV #8 - Mike's cube		109.196.196.151	1
DOV #8 - Mike's cube	management port	109.196.195.228	1
Egor's OptiView-a000f7		109.196.195.251	1
EvilOptiView		109.196.196.126	1
Franks Zappa		109.196.196.097	1
Greg's Squeeze		109.196.196.094	1

Version issues: ▼ Update available ● Incompatible version

Using the MIB Browser

The MIB Browser can be launched from the **Tools | Overview** screen. An SNMP enabled device must be selected in the **Tools | Overview Device** field for the MIB Browser to be selectable.

To launch the MIB Browser from the **Tools | Overview** screen, select the **Click here for Links and Launchers** button (at bottom of screen), and select **Launch MIB Browser**.

Note: The MIB Browser can also be started from the Windows desktop by selecting **Start | Programs | MG-SOFT MIB Browser | MIB Browser**.

Once the MIB Browser has started, drill into the MIB tree (left column) and select **View | MIB Node Properties** (CNTL D) to display detail on the selected node. Detail is displayed in a popup.

Refer to the MIB Browser help system for MIB Browser usage.

Using the OptiView Analyzer as an RMON Probe

User-Created Studies:

The OptiView Analyzer makes network traffic statistics available via the RMON and RMON 2 MIBs. A third party RMON client, such as HP OpenView or Concord eHealth, is able to configure additional RMON studies. The OptiView's RMON agent will automatically be configured on power-up for OptiView's own use. If an RMON client modifies the OptiView analyzer created studies with an owner of "MONITOR", the proper operation of the analyzer may be jeopardized! Modifying the OptiView analyzer's write community string will prevent third party RMON clients from modifying the studies.

A third party RMON client, using the correct READ and WRITE community strings (see the **Setup | Security** screen), is able to create, modify or remove additional RMON / RMON II studies. User-created studies will be preserved and restarted after a power cycle. Note, however, that many additional system resources will be used by these user-created studies. Out of memory conditions due to large, user-created studies may result in poor OptiView analyzer performance.

To reduce or eliminate any performance affect of user-created studies, the individual user created study must be removed using an RMON client or SNMP MIB Browser (which requires detailed knowledge of RMON row creation and deletion), or the analyzer can be reset to factory defaults.

To reset the RMON agent back to factory defaults, use a MIB Browser and SET probeResetControl (iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).probeConfig(19).probeResetControl(5)) to a value of “3” (for Cold Start).

OptiView sending SNMP Traps for problems found:

The OptiView analyzer is able to send an SNMP Trap for each reported problem in the **Discovery | Problems** screen. A compilable Fluke Networks MIB is available for registered users at www.flukenetworks.com.

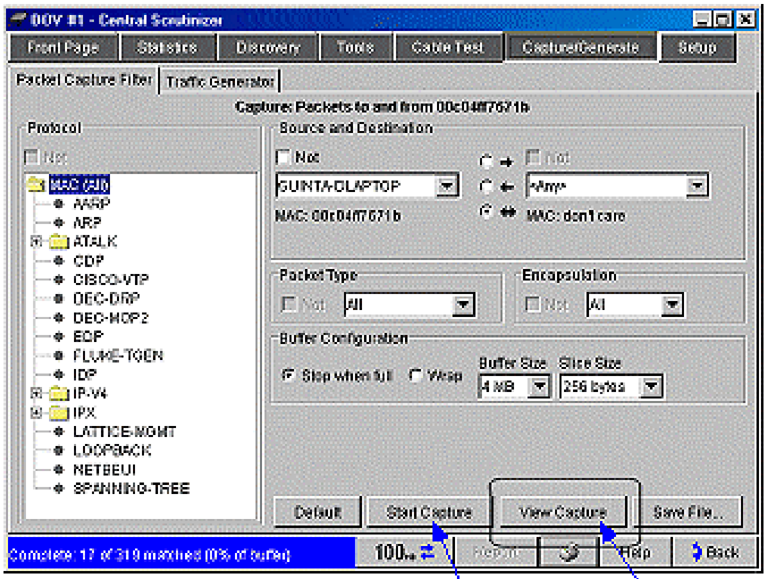
To enable sending problem traps, a third-party SNMP client must be used.

One or more trap destinations may be configured in the RMON Trap Destination group (iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).probeConfig(19).trapDestTable(13)). The “community” object must be set to “optiview”. More than one trap destination is supported.

To reset the trap destinations, Event Table and Trap Destination Table entries must be manually deleted or the entire RMON agent must be reset with a ColdStart (see instructions above).

Viewing Packets

One of the great features of this product is the ease of use to setup a filter, capture packets, and view the packet decodes.



Capture: Packets to and from 00c04ff7671b

Protocol: □ Not

MAC (All)
- AARP
- ARP
- ATALK
- CDP
- CISCO-VTP
- DEC-DRP
- DEC-MOP2
- EGP
- FLUKE-TGEN
- IDP
- IP-V4
- IPX
- LATTICE-MGMT
- LOOPBACK
- NETBEUI
- SPANNING-TREE

Source and Destination: □ Not GUNTA-DLAPTOP; MAC: 00c04ff7671b; ○ → ○ ← ● ↔; □ Not <Any>; MAC: don't care

Packet Type: □ Not All

Encapsulation: □ Not All

Buffer Configuration: ● Stop when full ○ Wrap; Buffer Size 4 MB; Slice Size 256 bytes

Complete: 17 of 319 matched (0% of buffer)

1. Select from the list of protocols (this selection is preselected if you have Filtered on the protocol from a previous screen such as Statistics | Protocol, Top Host, or Top Conversations)

2. Select a Source and Destination (this selection is preselected if you have Filtered on the device from a previous screen such as Discovery | Device, Networks, Statistics | Top Host, or Top Conversations)

3. Start and Stop capture

4. Launches the OptiView Protocol Expert in the decode view if installed

The first thing you probably will do is setup the Packet Filter. This is optional, but very useful. You probably don't want to sift through line after line of decodes when you can filter on just what you want to see.

Setting up the Packet Filter can be done directory from any screen that has a Filter button, or you can go directly to the **Packet Capture** Filter Screen by selecting the Packet Capture tab.

If you select a device in either the **Discovery | Device or Discovery | Network** screen, and select Filter, the **Packet Capture** filter screen is displayed with the source device populated with your selection.

If you select a protocol in the **Statistic | Protocols** screen and select Filter, the **Packet Capture** filter screen is displayed with the selected protocol.

If you select Filter from the **Top Hosts** or **Top Conversations** screens, the source device and protocol are pre-selected.

Cable Troubleshooting Tips

Twisted pair

- UTP cable used for medium- to high-speed networks requires a specified minimum number of twists per inch. The higher the speed, the greater the number of twists per inch. Flat, gray untwisted cable used for telephone systems (sometimes referred to as "silver-satin") should never be used for LAN applications. While the network may continue to operate after one or more of these links is installed, a quick look at the MAC-layer protocol is apt to show a noticeable increase in errors. Even if the network survives a small number of these links without a significant increase in errors, these links may yet be what pushes the network into failure when something else becomes marginal.
- Purchase and use only high-quality crimp tools for UTP. Poor-quality crimp tools often fail to press the pins evenly into the RJ-45, either by not pressing one end as firmly as the other, or by flexing in the center and not pressing the middle pins as firmly as the outside pins. The resulting problems tend to be intermittent, and are quite difficult to troubleshoot.
- When building your own UTP links, be particularly careful to purchase the correct connectors for the type of wire used. Stranded wire is always used for patch cables, and is almost always the connector type offered unless you specifically request solid wire connectors. In the short term, both will function adequately, but if the wrong connector is used, will result in intermittent connections over time. Connectors for solid wire use a pin that straddles the wire, and a pressure fit to maintain the connection. For stranded wire, the pins are driven into the tight bundle of individual wires, where contact is again maintained by pressure. If a stranded wire connector is used for solid wire, the pin simply touches the top of the wire and will stop making contact after the link is flexed during normal use.
- Although it may work for slower-speed applications like telephone service, a single UTP link should never be used by two network stations, or two types of service unless your LAN has been specifically designed to be coexistent with the other service. Leave unused pairs idle if you want to avoid intermittent problems (like losing data every time the telephone rings). As the data transmission speed increases, the likelihood of problems increases (a 235 kHz LocalTalk connection is nearly immune to this problem, but a 80 MHz 100BASE-TX connection would be highly susceptible).
- No product is able to perform a link test on a UTP link without connecting a loopback device to the other end of the run. Part of the reason for this is that, in order to comply with the requirements of the Standards that govern link testing, a pass or fail judgment may not be given unless the suite of tests includes a "wire map" test, which cannot be made without the loopback device. Another reason is that the link must be terminated with a resistance value equal to the impedance of the link for other measurements to be made.
- If UTP cables are to be bound, they should be bound loosely. There are a number of commercial fastening systems available that can be used to tidy-up a wiring

closet or a cable bundle. Be sure not to over-tighten! When bundles of UTP cable are too tightly bound at intervals along the length of the link, the electrical characteristics will change, causing network errors. You should always be able to slide a single cable in the bundle forward and backward through a fastening with little effort. If you must pull strongly (TIA/EIA-568-A paragraph 10.6.3.2 allows for a maximum of 25 pound feet of pulling tension), or if the cable cannot be moved at all, then your data is at risk. There have been instances where network problems disappeared when cable fastenings were cut to allow troubleshooting to begin.

- Handle LAN cable carefully during installation and later during use. If the cable is kinked severely, walked upon, or driven over, it will cause localized changes in the characteristic impedance, and may physically damage the insulation and wire.
- Be careful when specifying interconnecting hardware for UTP. Make sure that you use TIA/EIA-568-A pinouts for either the T568A or T568B specification throughout the entire network. If hardware made for both pinouts is used together, the color codes for the wire positions will be wrong, and the links will not work unless custom patch cables are used.
- If high-speed protocols will ever be used on the UTP cabling, it is vitally important to follow all of the installation guidelines for Category 5 cabling. This includes no sharp bends or kinks in the cable. Also, do not untwist the pairs more than absolutely necessary for any connection, and avoid routing cables near any sources of electrical noise such as fluorescent light fixtures, etc.
- Never mix cables with different characteristic impedance. Media filters can be used to adapt between new and old cable systems, but they introduce yet another potential failure point and should be avoided wherever possible.
- When untwisting wire pairs to install connectors or make connections at punch-down blocks, make the untwisted sections as short as possible. For compliance with Category 5 cabling standards, the untwisted section cannot exceed 13mm (about half an inch).
- Do not make sharp bends or kinks in the cable. The radius of bends in a cable should be larger than one inch, though TIA/EIA-568-A paragraph 10.6.3.2 permits four-pair UTP cable bend radii as tight as four times the diameter of the cable.
- Avoid installing long cable runs near ground planes, in metallic conduit, or near any other conducting surface. The result will be an additional 2-3% change in attenuation. High temperatures will also affect attenuation significantly.

New cabling--short-sighted or thrifty?

A common estimate is that 50% of the cost of a new network goes into the cable plant. It has also been said that cabling is a "once-in-a-decade" investment. It may seem like a great cost-cutting measure to install cable only to the places where it is currently required, to use Category 3 cable instead of Category 5, or to install only two pairs to each connection. Before you do so, consider how much more it will cost to rebuild the cable plant when you have outgrown your current network or must move to a media access protocol that requires four pairs of Category 5 wire.

The real cost for good-quality components, using four pairs instead of two, and running spare cables into spaces that may be needed in a year or two, is incremental compared to having a contractor come back again. Some companies are even having "dark" fiber optic cable pulled everywhere unshielded twisted pair (UTP) cable is installed, as a cost-savings measure, anticipating the time when the current network is unable to support the load. A well-designed and installed cable system can provide many years of service if the designers take into account the direction that leading-edge network solutions are headed.

Minimizing Impedance Discontinuities

Characteristic impedance is usually altered slightly by cable connections and terminations. Sharp bends or kinks in LAN cable can also alter the cable's characteristic impedance. Networks can operate with small discontinuities because the resulting signal reflections are small and are attenuated in the cable. Larger impedance discontinuities can interfere with data transmission. Such discontinuities are caused by poor electrical contacts, improper cable terminations, mismatched cable or connector types, and by disturbances in the twisting pattern of twisted pair cable.

You can avoid problems with impedance discontinuities by observing the following precautions during installation:

- Never mix cables with different characteristic impedance unless you use special impedance-matching circuitry.
- When untwisting cable pairs to install connectors or make connections at punch-down blocks, make the untwisted sections as short as possible.
- Do not make sharp bends or kinks in the cable. Check the cable manufacturer's specifications for the minimum bend radius.
- Handle LAN cable carefully during installation. Do not step on the cable or pinch it with tight cable ties.

Grounding and shielding cable

Although the primary purpose of requiring Screened UTP (ScTP) or Shielded Twisted Pair (STP) throughout most of Europe is to prevent network signals from leaking out of the cable, most people think of shielding as a way to prevent signals from leaking into the cable.

The use of shielding is a good way to meet both requirements; however, there are some potential problems. Restated: the fundamental purpose of a shield is to fully enclose a signal so no radiated field can enter the cable and disturb the signal lines, and equally important, so no field is radiated out of the cable, where it could interfere with other electronic devices. Note that is absolutely essential that shields fully enclose the signals in every regard. Extending a drain wire even a short distance past the shield of a cable to make a connection defeats the quality of the shield significantly. Proper installation requires mounting clamps that are located inside enclosed metal spaces, so that openings are absolutely minimal.

Generally speaking, a connection to ground is made for personal-safety reasons. To meet current safety requirements, all equipment must have a third wire safety connection to ground. The issue then becomes where (at what locations) connections have to be made between the earth ground (chassis) and the shield.

All earth ground connections eventually lead to a building ground location. Voltage potentials in the earth ground lead are caused by leakage currents in the various pieces of electrical equipment. The leakage current times the resistance of the ground wires cause voltage potentials, which easily can exceed several volts. Voltage potentials between buildings are generally very significant. Lightning is another important consideration when connecting buildings. For data communication between buildings, fiber optic connections are the only practical and safe solution.

You do not want to have a cable shield become a ground return path. This can be avoided in one of two ways:

1. Permit only a single connection between earth ground and the shield, or
2. Make certain that there is no substantial voltage potential between the earth ground connections of the equipment and any connection to data communications systems.

If there is no voltage, there will be no current, and therefore no problem. This is the solution that is followed for shielded twisted pair cabling systems (STP, ScTP).

When using shields with twisted pair cabling systems (ScTP, STP), one can verify the absence of ground loop potentials by testing for them after all non-LAN electrical equipment has been installed and is operational. Then, activate the LAN equipment and measure the voltage potential between the shield of the other end and the chassis of the equipment to be connected. If the voltage is less than 1 volt ac, one may be reasonably assured that there will be no ground loop effect.

If the voltage is substantially higher, you must locate the source of the leakage. This normally involves working with a qualified electrician to correct the problem that is creating the voltage potential. This is not always easy to do, and if not possible, you should convert the connection from copper to fiber optic cable.

Cable Types

The following cables are supported by Cable Test.

UTP is the abbreviation for unshielded twisted pair, and ScTP is the abbreviation for shielded twisted pair.

- Category 3 is typically used in 10 Mbit Ethernet
- Category 4 is typically used in 10 Mbit Ethernet and 16 Mbit Token Ring
- Category 5 is typically used in 10/100 Mbit Ethernet with Category 5E extending to 1000 Mbit copper. Category 5 is the default setting in Cable Test
- Category 6 is a proposed standard in the final stages of approval (05/00)

Supported Cable Types

- **UTP100 Category 3**
- **UTP100 Category 4**
- **UTP100 Category 5**
- **UTP100 Category 6**
- **ScTP100 Category 3**
- **ScTP100 Category 4**
- **ScTP100 Category 5**
- **ScTP100 Category 6**
- **ScTP120 Category 3**
- **ScTP120 Category 4**
- **ScTP120 Category 5**
- **ScTP120 Category 6**

ScTP or FTP type cables are typically constructed with a single foil shield around the bundle of wires. Use the equivalent ScTP cable type to test FTP type cables.

STP type cables are typically constructed with a foil shield around each individual wire pair, and an additional foil or braided shield around the entire bundle of wires. Select the equivalent ScTP cable type for testing STP cables if the cable type desired is missing from the list of supported cable types.

Sample Loss Limit Calculation

Standard: TIA-568-B (at 850 nm) Link length under test is 300m	*Limit per item*	*Qty*	*Loss*
Fiber loss	3.5dB/km	0.3km	1.05dB
Loss from adapters	0.75 dB	2	1.50dB
Loss from splices	0.3	0	0
			Total: 2.55 dB

Rerun Cable Test

Rerun Cable Test restarts the cable test. All Cable Test measurements are updated.

Note: Any OptiView analyzer remote access sessions are terminated if **Rerun Cable Test** is run.

Units Radio Buttons

Units determines which measurement units are displayed throughout the Cable Test screens. Units are either Feet or Meters.

Default router not responding:

Indicates that the analyzer can not communicate with the default router for the specified host.

Check the network configuration for the specified host to see if it is using an incorrect default router. Also check if default router is down or connection between the analyzer and router has failed.

Note: When the default router starts responding (problem corrected), the error message reported by the analyzer gets changed to "resolved" in Problem Discovery.

DHCP Server offered IP already in Use

While the analyzer was performing an auto configure, the DHCP server offered an IP address that was already in use.

Verify if a device is using a misconfigured static IP address or if the DHCP server is misconfigured.

Duplicate IP

Two devices on your network are using the same source IP address at the same time.

Change the IP address of one of the duplicate IP devices to fix the problem.

Note: If two devices use the same IP address at different times (e.g., DHCP reissuing expired leases), no problem will be reported.

A valid IP address should be obtained from your LAN administrator.

To search for unused IP addresses perform the following:

1. Select Discovery.
2. Select Devices.
3. Select the IP Address column to sort by IP address.
4. Find an unused IP address in the subnet the device needs to be part of.

Note: When this error is resolved, the analyzer changes the reported "error" to "resolved" in Problem Discovery.

How do you fix it?

If the device supports SNMP, in the **Tools | SNMP Tables** screen, try looking at the SNMP System Group and Interfaces for both hosts to identify the offending station.

Incorrect Subnet Mask

Device is incorrectly configured. Its mask is inappropriate for its subnet.

Change the IP subnet mask on the device.

To see a complete list of subnets:

1. Select Discovery.
2. Select Networks.
3. Select IP Subnets.

The right-hand side of the screen displays the correct mask for each of the discovered subnets.

IP address is subnet address

Device is misconfigured. A different address should be used. The IP address is the same as the subnet address.

The **Discovery | Networks** screen displays the range of addresses which are valid for each of the discovered IP networks.

To view the valid range of IP addresses for the discovered IP networks:

1. Select Discovery.
2. Select Networks.
3. Select the IP Subnet item in the tree of choices on the left side of the screen.
4. Look for the IP Range values on the right side of the screen.

IP address is subnet broadcast address

Device is misconfigured. A different address should be used. The IP address is the same as the subnet broadcast address.

The **Discovery | Networks** screen displays the range of addresses which are valid for each of the discovered IP networks.

To view the valid range of IP addresses for the discovered IP networks:

1. Select Discovery.
2. Select Networks.
3. Select the IP Subnet item in the tree of choices on the left side of the screen.
4. Look for the IP Range values on the right side of the screen.

Key device not responding to IP (up/down x time(s))

Indicates that the key device is not responding because that key device is down or network connectivity to that device has failed.

1. Select the problem in the **Discovery | Problem** screen.
2. Click on the Host Detail button.
3. Select the **Ping** tab.
4. Select the **Trace Route** radio button. The Trace Route automatically runs. Use the results to identify where connectivity failed.

Key device not responding to xx (up/down x time(s)) - IPX

Indicates that either the analyzer IPX address is incorrect or the key device is not responding because something in its path is down, or that key device is down.

Lost DHCP Lease

DHCP lease expired and the analyzer was not successful in renewing lease with the DHCP server.

Verify the DHCP server is running and functioning properly. Also, check if the network connection between the analyzer and DHCP server has failed.

Only device in IP subnet

What does this warning mean?

This warning indicates that the IP device associated with this warning is using the IP address specified to the right of this message, and that using this address makes it the only device in an IP subnet. Most likely, the device is not properly configured for IP operation.

What are the symptoms?

It is unlikely that any of the TCP/IP networking is operating correctly for this device. However, if some networking is still functional, it most likely is local networking using the NetBEUI or IPX protocol.

How do you fix it?

Find an IP address in the correct IP subnet that is not in use, and then reconfigure the device to use this address.

To determine which IP addresses are being used, go to the **Discovery | Networks** screen and select **IP Subnets** in the left column. The list of IP Subnets are displayed. Select the subnet you want your IP address to be within. All the devices in the selected subnet are displayed on the right side of the screen with their associated IP address. Look for an unused IP address.

How does the analyzer application know?

As the analyzer collects information about the devices on the network, it identifies the IP subnets on the network. No other device is using this configuration. That is, it appears that this is the only device in an IP subnet.

Are there any exceptions?

It is possible and permissible to have IP subnets with only a single device, but it is not recommended.

What else should I look at to understand this?

Common causes of this problem include the following:

· The device is connected into the wrong port in the wiring closet. (Is the address correct for a different subnet?)
· The device has been reconfigured and not rebooted.
· A configuration mistake was made, for example, a transposition of numbers was done when it was configured.
· A printer has been installed on the network and it still has its default configuration.

Only device in IPX network

What does this warning mean?

This warning indicates that the IPX device associated with this warning is the only device in the IPX network number specified to the right of this message.

At boot up, most network devices send a request for network information. A server or router on the network provides this information to the devices. This warning can be caused by several things:

- A server or router is advertising a network number that no other device is using. This usually is due to a configuration error on the device
- Some service device (like a hub or printer) picked up this network number when a change was being made on the network, and the device has not been rebooted since then, and thus it may be advertising the wrong network number
- The device is bound to the wrong network
- The device was manually configured with the wrong network number

What are the symptoms?

This condition might result in a router having to forward information when the information really shouldn’t need to be routed. For example, communicating with a printer that is configured incorrectly might require the router to duplicate every message in a communication.

Overall, networking will still operate as expected, but there will be unnecessary traffic on the network.

How do you fix it?

If the device that is using this network number is a router or server, it must be reconfigured. For other devices (like printers), simply reboot the device.

How does the analyzer application know?

The application examines the address information that is used by each device and compares it to what other devices are using on the network.

Are there any exceptions?

IPX networks can span IPX routers. For example, there could be a server on one side of an IPX router and a group of devices on the other side of the IPX router. In such a situation, if the application has not seen any communication from the group of devices on the other side of the IPX router, it could report this warning for the server.

What else should I look at to understand this?

In the **Discovery | Networks** screen, see what network numbers are listed under the IPX Networks category.

Only device in NetBIOS domain

What does this warning mean?

This warning indicates that the NetBIOS device associated with this warning appears to be the only device in the NetBIOS domain specified to the right of this message. This can be caused by a misconfigured PC or a PC that is trying to join the wrong domain, because its domain name was mistyped when it was configured. When the PC does not see the domain it is configured for, it then becomes the Master Browser (MB) and will advertise this domain as a workgroup.

Domains are constructed to allow users to share information. If there is only one user in the domain, it is not adding any value to the network.

What are the symptoms?

If the device is misconfigured, it might not be able to access the domains that you want it to be able to access (if access control or other security measures are in place).

This condition will not adversely effect network operation in any way. Therefore, this condition is reported as a information, rather than an error. However, you need to be aware of any users that are setting up their own domains and workgroups, since Microsoft networking uses domains and workgroups for network administration. In domains, the network administrator has centralized control over network resources and users. Therefore, a single device in a domain can be a potential security hole that you do not have authority over.

How do you fix it?

Do the following to change the device’s workgroup or domain:

1.From the Windows Control Panel, open the **Network** dialog box.
2.Click the **Identification** tab.

The **Workgroup** field specifies in which workgroup the device is a member.

3.Click the **Configuration** tab, highlight **Client for Microsoft Networks**, and then click the **Properties** button.

The tab that opens contains the specification as to what domain the device should log on to.

Note: The domain and the workgroup do not have to be the same.

How does the analyzer know?

Unlike Microsoft networking, which collects domain and workgroup information from the device that is the Master Browser, the analyzer communicates with each device to discover its membership configuration.

The analyzer does not differentiate between domains and workgroups. It collects information about the available groups of networking devices and it examines these groups for consistent configuration.

Are there any exceptions?

There are situations in which you would want to have a single station in a workgroup. Probably the most common is when you are using SAMBA on a UNIX device to share directories with PCs.

What else should I look at to understand this?

In the **Discovery | Networks** screen, in the left column, select the NetBIOS Domains category. The right side of the screen will list all the domains and workgroups that were discovered along with the discovered information for the local PDC (Primary Domain Controller) and BDCs (Backup Domain Controllers), and any local MBs (Master Browsers).

Only device in network using IPX type

What does this warning mean?

This warning indicates that the IPX device associated with this warning is the only device running the encapsulation specified to the right of this message.

This can mean either of the following:

- This device is the only device running that encapsulation on a particular IPX network number.
- This device is the only device running that encapsulation on any of the discovered IPX networks.

Note: This warning does NOT mean the specified encapsulation is the only encapsulation the device is using.

IPX supports four different frame encapsulations on Ethernet networks: 802.2, 802.3, Ethernet II, and SNAP. In order for communication to occur between devices, the devices must be using the same encapsulation. This warning indicates that this device cannot communicate (with the specified IPX type) with any other device on the network.

What are the symptoms?

This device probably cannot communicate with the server.

How do you fix it?

Modify the configuration of the device to be consistent with the server that it needs to access. On Microsoft Windows 2000, Windows 98, and Windows NT machines, it is usually easiest to configure the IPX encapsulation to Auto. Then the PC will simply use what ever encapsulation the server is using. Auto might not work if you are using multiple encapsulations on the same network.

How does the application know?

The application examines the frames sent by each device and tracks the type of encapsulation that is being used.

Are there any exceptions?

No.

What else should I look at to understand this?

Examine the device in the **Tools | Overview** screen. In the Protocols area, note what encapsulations are in use on the device. Select **Discovery | Networks** and select IPX Networks to see what IPX types are supported for each IPX Network.

Proxy ARP reply for local IP

Routers with Proxy ARP enabled will respond to ARP requests for off-net hosts. Some vendors' routers will incorrectly respond to on-net ARP requests, which can create confusing network behavior.

Some sites disable Proxy ARP, forcing end-nodes to have the proper subnet mask and router configurations. Other sites depend on Proxy ARP to add robustness to the network so that applications work even if the end-node is misconfigured. Use of Proxy ARP is mostly benign, although there may be a slight increase in ARP broadcast traffic, an increase in ARP cache table sizes, and possibly some decrease in performance.

Proxy ARP reply for local IP (host IP may be misconfigured; host may have been moved to new subnet without changing its IP address; routers may be misconfigured; routing loops may exist.

Proxy ARP is enabled as a default on many routers.

Other Hosts

Other Host is the category for all devices that do not fit in any of the other groups. Hosts are discovered by traffic monitoring and by querying hosts.

Ÿ Detects MAC Address, IPX Address, IP Address, DNS Name, SNMP System Name, IP Subnet Mask, Default IP Router, NetBIOS Name, NetBIOS Domain Name, IPX Server Name and correlates all information for the same host.

Interconnect Devices

Routers

IP and IPX routers are discovered by traffic monitoring and by querying hosts. The IP routers are discovered with the following methods:

- Monitoring IP routing protocols (RIP, RIP-2, OSPF, IGRP, EIGRP, IRDP, ICMP, HSRP)
- Monitoring ICMP messages
- Sending IRDP requests
- SNMP queries (IP forwarding enabled and multiple interfaces in the route table)
- Proxy ARP discovery
- Router advertises default RIP route
- Router advertises no RIP route
- Router advertises only reverse poison RIP routes

The IPX routers are discovered by sending IPX RIP requests and by monitoring IPX RIP. IPX routers running only NLSP will not be detected.

Switches

Switches are discovered by traffic monitoring and by querying hosts with the following methods:

- Monitoring spanning tree frames (802.1d BPDU, DEC Span, Lattice Span)
- Monitoring management frames (CDP, SONMP)
- SNMP queries (802.1d Bridge MIB)
- Private MIB queries (Cisco Nortel LAN Switch List) See also Switches Supported.

SNMP Hubs

The analyzer will discover SNMP manageable hubs that support the 802.3 Repeater MIB.

Key Devices

Key Devices allows you to create a list of devices, and at a glance gives you a quick summary of your crucial network devices and services. It also provides automatic connectivity testing from the local network to other crucial networks.

All Key Devices are continuously tested by performing an IP (or IPX) ping. Every Key Device is automatically pinged every 30 seconds, and if no response is detected three times in a row, an error will be displayed. An occasional intermittent "no response" will be ignored.

Key Devices not responding will show in the Problems screen with the error "Key Device not responding to IP (or IPX)." It reports the number of times connectivity was lost and restored, including the time of the first failure.

If the key device begins responding, that key device will change to a resolved status and the Problems screen will also indicate the time connectivity was most recently restored.

Number of Devices Found

The number next to each device type is the number of device types found.

Expanding and Collapsing a Tree

A ⊞ indicates the item can be expanded. Select the ⊞ to show all devices under that device type. When a device type is expanded, a ⊟ displays. Select the ⊟ and the expanded device list collapses.

Printer Devices

The analyzer will identify IP printers via the SNMP Printer MIB and IPX printers via diagnostic requests and queries.

Servers

NT & IBM LanServer

The analyzer will discover the following NT servers with active queries for all NetBIOS protocols (NetBEUI over TCP/IP, and over IPX/SPX), all IPX encapsulation types (SNAP, Ethernet II, 802.3 (RAW), 802.2), and by monitoring traffic:

- Primary Domain Controllers
- Backup Domain Controllers
- Master Browser
- Domain Master Browser
- IP servers

Netware

The analyzer will discover IPX servers for all encapsulation types. The IPX servers are discovered by sending IPX Nearest Server and SAP requests. All local or the nearest IPX servers will be displayed along with the IPX server name.

- IPX File server
- IPX Nearest server for 802.2
- IPX Nearest server for NEAR Raw
- IPX Nearest server for NEAR Ethernet II
- IPX Nearest server for NEAR SNAP
- IPX Netware Management Station 2
- IPX Time Synchronization server
- IPX Print server
- IPX Netware Access server
- IPX Netware Directory server

Name & Address Servers

Wins

- IP server running BOOTP
- IP server running DHCP
- IP server running DNS

NetBIOS name servers (WINS) are discovered by monitoring IP traffic.

DNS

DNS servers are discovered by monitoring IP traffic and sending local DNS discover requests.

DHCP / BOOTP

The analyzer will discover DHCP/BOOTP servers by monitoring IP traffic. DHCP servers will also be discovered by sending DHCP discover requests.

SNMP Agents

The analyzer will discover SNMP agents and will also detect RMON and RMON2 probes. All community strings configured in the **Security screen** will automatically be tested.

Front Page Screen

This is the Front Page screen. For more information see the Front Page topic.

Sample Loss Limit Calculation

Standard: TIA-568-B (at 850 nm) Link length under test is 300m	*Limit per item*	*Qty*	*Loss*
Fiber loss	3.5dB/km	0.3km	1.05dB
Loss from adapters	0.75 dB	2	1.50dB
Loss from splices	0.3	0	0
			Total: 2.55 dB

atalk

rtmp
 nbp
 atp
 aep
 rtmp2
 zip
 adsp
 snmp
 snmptrap

Expanded Protocol List

aarp
atalk
arp
cdp
chaosnet
dec
dec-diag
drp
edp
fluke-tgen
idp
ip-v4 **Note: Port numbers are provided for tcp and udp protocols**
ipv6
ipx **Note: Packet types and socket numbers are provided for ipx protcols**
iso-clnp
lat
lavc
loopback
mop
mop2
netbeui
netbios-3com
rarp
sna-th
snmp
spanning-tree-bpdu
vecho
vecho2
vip
vloop
vloop2

idp

pup
 xns-rip
 xns-echo
 xns-error
 xns-pep
 xns-pep xns-rip
 xns-pep xns-echo
 xns-pep xns-error
 xns-pep smb
 xns-pep smb2
 xns-spp
 xns-spp xns-courier
 xns-spp smb
 xns-spp smb2

ip-v4

active-networks
adf
argus
aris
ax-25 azhp
bbn-rcc-mon
bna
br-sat-mon
cbt
cftp
chaos
compaq_peer
cphb
cpnx
dcn-meas
ddp
ddx
dgp
egp
eigrp
emcon
encap
etherip
ggp
gmtp
gre
hmp
iatp
icmp
idpr
idpr-cmtp
idrp
ifmp
igmp
igrp
il
i-nlsp
ip-comp
ipcv
ipip
ipip4
ippc
ipv6
ipv6-frag

ipv6-icmp
ipv6-no-nxt
ipv6-opts
ipv6-route
ipx-in-ip
irtp
iso-ip
iso-tp4
kryptolan
l2tp
larp
leaf-1
leaf-2
merit-inp
mfe-nsp
mhrp
micp
mobile
mtp
mux
narp
netbit
nfsnet-igp
nvp2
ospf
pgm
pim
pnni
priv-encript
priv-host
priv-net
prm
pup
pvp
qnx
rdp
rsvp
rvd
sat-expak
sat-mon
scc-sp
schedule-xfer
scps
sdrp
secure-vmtp
sep

sipp-ah
sipp-esp
skip
snp
sprite-rpc
srp
st2
sun-nd
swipe
tcf
tcp protocols and ports numbers
third-pc
tlsp
tp-plus-plus
trunk-1
trunk-2
ttp
udp protocols and ports numbers
vines
visa
vmtp
vrrp
wb-expak
wb-mon
wsn
xnet
xns-idp
xtp

ip-v4 tcp

3com-tsmux
914c-g
acas
aci
acr-nema
aed-512
alternate-http
alternate-rtsp
america-online
anet
ansanotify
ansatrader
at-3-5-7-8
at-echo
at-nbp
at-rtmp
at-zis
audionews
audit
auditd
auth
banyan-vip
bftp
bgp
bh-fhs
bl-idm
cai-lic
ccmail
cdc
chargen
cisco-fna
cisco-sys
cisco-tna
citrix-ica
cl-1
compressnet
compressnet-mgmt
covia
csnet-ns
ctf
cu-seeme
cvs-pserver
daynachip
daytime

dbase
dcp
deos
discard
dixie
dls
dls-mon
dn6-nlm-aud
dn6-smm-red
dns
dnsix
doom
dsp
dsp3270
echo
edp
emfis-cntl
emfis-data
endpoint-mapper
erpc
exec
filenet-NCH
filenet-RPC
filenet-TMS
finger
fln-spx
ftp
ftp-data
ftps
ftps-data
gacp
genrad-mux
gopher
gppitnp
graphics
gss-xlicen
gupta-sqlbase
h323
hostname
hosts2-ns
https
ibm_db2
ibm_db2-conn-svc
ibm_db2-int-svc
ichat
imap2_n_4

imap3
imaps
ingres-net
ingress-lock
irc
ircs
ircu
isi-gl
iso-ip
iso-tp0
iso-tsap
jargon
kis
knet-cmp
ldap
ldaps
link
locus-con
locus-map
login
mailq
matip
mcidas
metagram
mfcobol
mit-dov
mit-ml-dev
mpp
msg-auth
msg-icp
ms-mqs
msp
ms-sms
ms-sna-base
ms-sna-server
ms-sql-monitor
ms-sql-server
ms-streaming
ms-terminal-server
multiplex
mumps
namp
netbios-dgm
netbios-ns
netbios-ssn
netsc-dev

netsc-prod
newacct
nextstep
nicname
ni-ftp
ni-mail
nntp
nntps
notes
npp
nss-routing
nsw-fe
ntalk
objcall
ocbinder
ocserver
openwindows
oracl-coauthor
oracl-em1
oracl-em2
oracl-names
oracl-remdb
oracl-srv
oracl-tns
oracl-vp1
oracl-vp2
osu-nms
pc-anywhere-data
pcmail-srv
peer-direct
pop2
pop3
pop3s
printer
print-srv
priv-dialout
priv-file
priv-mail
priv-print
priv-rje
priv-term
priv-termlink
profile
prospero pt-pt-tunneling
pwdgen
qft

qotd
quake
quickmail
rap
realaudio
remote-kis
ris
rsh-spx
rsvd
rtsp
sap-r3
send
shell
smakynet
smtp
smtps
smux
snagas
s-net
snmp
snmptrap
softpc
sql-net
sql-net
sqlserv
sqlsrv
src
srmp
ssh
sshell
su-mit-tg
sunrpc
sur-meas
swift-rvf
sybase-sqlany
sybase-sqlanywhere
systat
t-120
tacacs
tacacs-ds
tacnews
talk
tcpmux
telnet
telnets
the-palace

timbuktu-srv
time
uaac
uarps
unify
unitary
uucp
uucp-path
vdolive
vettcp
vmnet
vmpwscs
whois++
www-http
xfer
xns-auth
xns-ch
xns-courier
xns-mail
xns-time
xwin
xyplex-mux
z39-50

ip-v4 udp

3com-tsmux
914c-g
aci
aed-512
anet
ansanotify
ansatrader
at-3-5-7-8
at-echo
at-nbp
at-rtmp
at-zis
audionews
audit
auditd
backweb
banyan-vip
bh-fhs
biff
bl-idm
bootpc
bootps
cai-lic
ccmail
cdc
cfdptkt
chargen
cisco-fna
cisco-sys
cisco-tna
citrix-icabrowser
cl-1
csnet-ns
ctf
cu-seeme
daynachip
daytime
dbase
dcp
deos
discard
dixie
dls
dls-mon

dns
dsp
dsp3270
echo
edp
emfis-cntl
emfis-data
endpoint-mapper
erpc
filenet-NCH
filenet-RPC
filenet-TMS
fln-spx
gacp
genrad-mux
gppitnp
graphics
gss-xlicen
h323-gatekeep-disc
h323-gatekeep-ras
hosts2-ns
ipx-tunnel
irc
ircs
isi-gl
iso-ip
iso-tp0
iso-tsap
ivisit
jargon
kerberos
kis
la-maint
ldap
ldaps
link
mailq
metagram
mit-ml-dev
msg-auth
msg-icp
ms-mqs-discovery
ms-mqs-ping
msp
multiplex
mumps

nameserver
namp
netbios-dgm
netbios-ns
netbios-ssn
netsc-dev
netsc-prod
nextstep
ni-mail
notes
npp
nss-routing
nsw-fe
ntalk
ntp
ocbinder
ocserver
openwindows
osu-nms
pc-anywhere-stat
peer-direct
pop3
pop3s
print-srv
priv-dialout
priv-file
priv-mail
priv-print
priv-rje
priv-term
priv-termlink
pwdgen
qotd
quake
quickmail
realaudio
re-mail-ck
remote-kis
rip
ris
rlp
rsh-spx
rsvd
rtcp
rtp
send

smakynet
s-net
snmp
snmptrap
softpc
sql-net
sqlserv
src
srmp
ssh
streamworks-mpeg
subnet-bcast-tftp
sunrpc
sur-meas
swift-rvf
syslog
systat
tacnews
talk
tftp
the-palace
timbuktu
timbuktu-srv
time
uaac
uarps
unify
unitary
vettcp
vmnet
vmpwscs
who
xdmcp
xfer
xns-auth
xns-ch
xns-courier
xns-mail
xns-time
xyplex-mux

ipx

nov-echo
nov-error
nov-netbios
nov-pep
nov-pep2
nov-pep3
nov-rip
nov-spx

ipx nov-pep

burst
 ipxwan
 ncp
 nlsp
 nov-bcast
 nov-diag
 nov-netbios
 nov-rip
 nov-sap
 nov-sec
 nov-watchdog
 smb
 smb2
 snmp
 snmptrap

ipx nov-pep2

burst
ipxwan
ncp
nlsp
nov-bcast
nov-diag
nov-netbios
nov-rip
nov-sap
nov-sec
nov-watchdog
smb
smb2
snmp
snmptrap

ipx nov-pep3

burst
ipxwan
ncp
nlsp
nov-bcast
nov-diag
nov-netbios
nov-rip
nov-sap
nov-sec
nov-watchdog
smb
smb2
snmp
snmptrap

ipx nov-spx

citrix-ica
 gupta-sqlbase
 ibm_db2
 ibm_db2-conn-svc
 ms-sna-server
 ms-sql-server
 oracl-tns
 smb
 smb2
 sybase-sqlany

IPX nov-pep Packet Type and Socket Numbers (decimal and hex)

Protocol	Packet Type (decimal)	Socket# (decimal)	Socket # (hex)
ncp	0	1105	0x451
nov-sap	0	1106	0x452
nov-rip	0	1107	0x453
nov-netbios	0	1109	0x455
nov-diag	0	1110	0x456
nov-sec	0	1111	0x457
smb	0	1360	0x550
smb2	0	1362	0x552
burst	0	3333	0xd05
nov-watchdog	0	16388	0x4004
nov-bcast	0	16389	0x4005
eigrp	0	34238	0x85be
nlsp	0	36865	0x9001
ipxwan	0	36868	0x9004
snmp	0	36879	0x900f
snmptrap	0	36880	0x9010

IPX nov-pep2 Packet Type and Socket Numbers (decimal and hex)

Protocol	Packet Type (decimal)	Socket# (decimal)	Socket # (hex)
ncp	4	1105	0x451
nov-sap	4	1106	0x452
nov-rip	4	1107	0x453
nov-netbios	4	1109	0x455
nov-diag	4	1110	0x456
nov-sec	4	1111	0x457
smb	4	1360	0x550
smb2	4	1362	0x552
burst	4	3333	0xd05
nov-watchdog	4	16388	0x4004
nov-bcast	4	16389	0x4005
eigrp	4	34238	0x85be
nlsp	4	36865	0x9001
ipxwan	4	36868	0x9004
snmp	4	36879	0x900f
snmptrap	4	36880	0x9010

IPX NOV-PEP3 Packet Type and Socket Numbers (decimal and hex)

Protocol	Packet Type (decimal)	Socket# (decimal)	Socket # (hex)
ncp	17	1105	0x451

nov-sap	17	1106	0x452
nov-rip	17	1107	0x453
nov-netbios	17	1109	0x455
nov-diag	17	1110	0x456
nov-sec	17	1111	0x457
smb	17	1360	0x550
smb2	17	1362	0x552
burst	17	3333	0xd05
nov-watchdog	17	16388	0x4004
nov-bcast	17	16389	0x4005
eigrp	17	34238	0x85be
nlsp	17	36865	0x9001
ipxwan	17	36868	0x9004
snmp	17	36879	0x900f
snmptrap	17	36880	0x9010

IPX NOV-SPX Packet Type and Socket Numbers (decimal and hex)

Protocol	Packet Type (decimal)	Socket# (decimal)	Socket # (hex)
smb	5	1360	0x550
smb2	5	1362	0x552
oracl-tns	5	32884	0x8074
sybase-sqlany	5	32965	0x80c5
gupta-sqlbase	5	32981	0x80d5
ms-sql-server	5	33854	0x843e
ms-sna-server	5	33992	0x84c8
citrix-ica	5	34234	0x85ba
ibm-db2-conn-svc	5	34718	0x879e
ibm-db2	5	34722	0x87a2

Discovered Protocols

AARP

AppleTalk Address Resolution Protocol

For outgoing packets, supplies the hardware destination address corresponding to a higher-level protocol address, and filters incoming packets to pass only those that are broadcast or specifically addressed to it. Interpreted in the AppleTalk Protocol Interface suite.

AEP

AppleTalk Echo Protocol

A protocol within AppleTalk that allows any node to send a datagram to any other node, and to receive an echoed copy of that packet.

AFP

AppleTalk Filing Protocol

AFP is a remote filing system protocol that provides a workstation on an AppleTalk network with access to a server that is implemented according to the AFP file system structure. AFP also includes user authentication support and an access control mechanism that supports volume-level and folder-level access rights. AppleShare is the AFP file server that is implemented on Macintosh computers.

Through the native file system and AFP, your application can run on one node and manipulate files on another node. You can use AFP commands to:

- obtain and modify information about the file server and other parts of the file system structure
- create and delete files and directories
- read files or write to them
- retrieve and store information within individual files

AFP is implemented by the .XPP driver. The .XPP driver maps an AFP function call from the client workstation into one or more ASP function calls.

ATALK

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. [Source: NNSC]

ARP

Address Resolution Protocol

Conversion of a network-layer address (e.g., IP address) into the corresponding physical address (e.g., MAC address).

ASP

AppleTalk Session Protocol

A general protocol built upon ATP providing session establishment, maintenance, and tear-down, along with request sequencing.

BGP

Border Gateway Protocol

BGP is an exterior protocol for communication between routers in different autonomous systems. BGP is a replacement for the older EGP that was used on the ARPANET.

BOOTP

Boot Protocol

A protocol within TCP/IP that is used for downloading initial programs into networked stations.

CDP

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a protocol for discovering devices on a network. Each CDP-compatible device sends periodic messages to a well-known multicast address. Devices discover each other by listening to that address.

CDP operation can be enabled or disabled on the hub through the object cdpInterfaceEnable. When enabled, the network management module (NMM) SNMP agent discovers neighboring devices and builds its local cache with information about these devices. A management workstation can retrieve this cache by sending SNMP requests to access the CDP MIB.

CLNP

Connectionless Network Protocol

An OSI protocol similar to IP. It provides much larger addresses with a variable length of up to 20 bytes.

CSLIP Compressed SLIP

Since SLIP lines are often too slow (19200 bits/sec or below) and are frequently used for interactive traffic (such as Telnet), there tends to be many small TCP packets exchanged across a SLIP line. Recognizing this performance drawback, the newer version CSLIP was specified in RFC 1144. CSLIP normally reduces the 40-byte header to 3 or 5 bytes. It maintains the state of up to 16 TCP connections on each end of the CSLIP link and knows that some of the fields in the two headers for a given connection normally do not change. Of the fields that do change, most change by a small positive amount. The smaller headers greatly improve the interactive response time.

DAP

Data Access Protocol

The DECnet protocol that provides remote file access.

DDP

Datagram Delivery Protocol

Extends the service of the underlying link access protocol to include an internet of interconnected AppleTalk networks, with provision to address packets to sockets within a node.

DIA

Document Interchange Architecture

DIA distributions consist of data and an associated profile. This profile contains information about the document, such as its name, type, and subject. When sending a distribution, it is possible to specify whether it is high or normal priority, and whether the data is personal or public. A "Confirmation of Delivery" and a "Return Receipt" can also be requested; Confirmation of Delivery indicates that the message has been put in the destination user's post box, while a Return Receipt indicates that the user has actually read the message.

Many implementations of DIA, however, do not incorporate Return Receipts. DIA also uses "status" distributions. A negative status distribution is always returned to the sender if an error occurs, whilst a positive status distribution is only returned if the sender has requested "Confirmation of Delivery". A "Return Receipt" is a text message.
(C) 1992-1997 David Goodenough & Associates Limited.

EGP

Exterior Gateway Protocol

A protocol within TCP/IP used to exchange routing information among gateways belonging to the same or different systems. A generalization of gateway-to-gateway protocols.

FTP

File Transfer Protocol

1. A protocol based on TCP/IP for reliable file transfer.
2. A protocol transmitted by a Net RPC frame in Banyan VINES.

GGP

Gateway-to-gateway Protocol

A protocol within TCP/IP used to exchange routing information between IP gateways and hosts.

HTTP

Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

Essential concepts that are part of HTTP include the idea that files can contain references to other files whose selection will send out additional transfer requests. Any Web server machine contains, in addition to the HTML and other files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive.

Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator (URL) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol address indicated by the URL. The HTTP daemon in the destination server machine receives the request and, after any necessary processing, the requested file is returned.
Sources: George McDaniel. IBM Dictionary of Computing, Tenth Edition, McGraw-Hill, (1993).

ICMP

Internet Control Message Protocol

A protocol within TCP/IP used principally to report errors in datagram transmission.

IDP

Internet Datagram Protocol

Delivers to an internet address a single frame as an independent entity, without regard to other packets or to the addressee's response.

IGRP

Interior Gateway Routing Protocol

IGRP uses a combination of user-configurable metrics, including internetwork delay, bandwidth, reliability, and load. IGRP also advertises three types of routes: interior, system, and exterior.

Interior routes are routes between subnets in the network attached to a router interface. If the network attached to a router is not subnetted, IGRP does not advertise interior routes.

System routes are routes to networks within an autonomous system. The Cisco IOS software derives system routes from directly connected network interfaces and system route information provided by other IGRP-speaking routers or access servers. System routes do not include subnet information.

Exterior routes are routes to networks outside the autonomous system that are considered when identifying a gateway of last resort. The Cisco IOS software chooses a gateway of last resort from the list of exterior routes that IGRP provides. The software uses the gateway (router) of last resort if it does not have a better route for a packet and the destination is not a connected network. If the autonomous system has more than one connection to an external network, different routers can choose different exterior routers as the gateway of last resort.

By default, a router running IGRP sends an update broadcast every 90 seconds. It declares a route inaccessible if it does not receive an update from the first router in the route within 3 update periods (270 seconds). After 7 update periods (630 seconds), the Cisco IOS software removes the route from the routing table.

IGRP uses flash update and poison reverse updates to speed up the convergence of the routing algorithm. Flash update is the sending of an update sooner than the standard periodic update interval of notifying other routers of a metric change. Poison reverse updates are intended to defeat larger routing loops caused by increases in routing metrics. The poison reverse updates are sent to remove a route and place it in holddown, which keeps new routing information from being used for a certain period of time.

Sources: George McDaniel. IBM Dictionary of Computing, Tenth Edition, McGraw-Hill, (1993).

IMAP2

Interactive Mail Access Protocol, Version 2

The Interactive Mail Access Protocol, Version 2 (IMAP2) allows a workstation or personal computer to access electronic mail from a mailbox server. Since the distinction between personal computers and workstations is not always clear, it is desirable to have a single solution that addresses the need in a general fashion. IMAP2 is the "glue" of a distributed electronic mail system consisting of a family of client and server implementations on a wide variety of platforms, from small single-tasking personal computing engines to complex multi-user timesharing systems.

IP

Internet Protocol (IP, IPv4)

The Internet Protocol (version 4), defined in RFC 791, is the network layer for the TCP/IP Protocol Suite. It is a connectionless, best-effort packet switching protocol.

IP-FRAGMENTS

Whenever an IP packet length exceeds the network interface MTU (maximum transmission unit), the packet will be fragmented into multiple individual IP packets. When an IP packet is fragmented, it is not reassembled until it reaches its final destination. Even though IP fragmentation is transparent, it can be undesirable because if one fragment is lost, then all fragments must be retransmitted.

Since IP fragmentation is performed at the IP layer, only the first fragment will contain the UDP or TCP header information. The analyzer will categorize and report the first packet in the Protocol Statistics screen by the corresponding UDP or TCP protocol. All subsequent IP fragments are categorized as FRAGMENTS.

Note: Excessive IP fragmentation should be investigated for possible misconfigured network interfaces or less than optimal route paths.

IP-FRAGMENTs are not the same as Fragments reported in the analyzer Utilization screen.

IP-v6

Internet Protocol Version 6

IPv6 is a new version of the Internet Protocol which is designed to be an evolutionary step from its predecessor, version 4. There are many RFCs defining various portions of the protocol, its auxiliary protocols, and the transition plan from IPv4. The core RFCs are 1883 through 1886.

IPX

Internetwork Packet eXchange

Novell's protocol used by Netware. A router with IPX routing can interconnect LANs so that Novell Netware clients and servers can communicate.

IS-IS

1. **International Standard** The final phase for an OSI protocol definition. At this point, the protocol is fully specified and guaranteed not to change.
2. **Intermediate System** An OSI term for a system that originates and terminates traffic, and that also forwards traffic to other systems.

LAT

Local Area Transport

The DECnet protocol that handles multiplexed terminal (keyboard and screen) traffic to and from timesharing hosts.

LU 6.2

Logical Unit 6.2

A subset of the SNA protocols used for peer-to-peer communications between computers.

MOP

Maintenance Operations Protocol

A protocol under DECnet for remote testing and problem diagnosis.

MOUNT

A protocol developed by Sun Microsystems that provides request access checking and user validation. It is used in conjunction with NFS.

NBP

Name-Binding Protocol

Used in AppleTalk networks to permit network users to use character names for network services and sockets. NBP translates a character-string name within a zone into the corresponding socket address.

NetBIOS Protocol

Used in 3Com Open software. Interpreted in the XNS Protocol Interface suite.

NCP

Netware Core Protocol

Novell's application-level protocol for the exchange of commands and data between file servers and workstations.

ND

Network Disk

A protocol within the Sun Microsystems NFS family used to access virtual disks located remotely across the network.

NetBEUI

NetBIOS Extended User Interface

NetBEUI is an extended version of NetBIOS, the program that enables computers to communicate within a local area network. NetBEUI organizes the frame format that was not specified as part of NetBIOS. NetBEUI was developed by IBM for its LAN Manager product and is adopted by Microsoft for its Windows NT, LAN Manager, and Windows for Workgroups products. Hewlett-Packard and DEC use it in comparable products.

NetBEUI is the best performance choice for communication within a single LAN. It does not support the routing of messages to other networks, so its interface must be adapted to other protocols such as IPX or TCP/IP. A recommended method is to install both NetBEUI and TCP/IP in each computer and set the server up to use NetBEUI for communication within the LAN and TCP/IP for communication within and beyond the LAN.

NetBIOS

Network Basic I/O System

Netware supports emulation of the protocol implemented by the IBM PC LAN Program to support communication between symbolically named stations and the exchange of arbitrary data. In the Netware context, NetBIOS is a top IPX.

NFS

Network File System

A protocol developed by Sun Microsystems for requests and responses to a networked file server.

NICE

Network Information and Control Exchange

The DECnet protocol for network management.

NIS

Network Information Services

Previously known as "Yellow Pages." A set of services in the Network File System (NFS) that propagate information from masters to recipients. Used for maintenance of system files on complex networks.

NSP

Network Services Protocol

The DECnet Microsystems that provides reliable message transmission over virtual circuits.

PAP

Printer Access Protocol

A protocol within AppleTalk that uses ATP XO commands to create a stream-like service for communication between user stations and the Apple LaserWriter or similar stream-based devices.

PEP

Packet Exchange Protocol

A protocol within the XNS family used to exchange datagrams.

PMAP

Port Mapper

A protocol developed by Sun Microsystems for mapping RPC program numbers to TCP/IP port numbers.

POP3

Post Office Protocol 3

A protocol designed to allow single user hosts to read electronic mail from a server. Version 3, the most recent and most widely used, is defined in RFC 1725.

PPP

Point-to-Point Protocol

PPP is a protocol for communicating between two computers using a serial interface, typically a personal computer connected by modem to a server. For example, your Internet Server Provider (ISP) can provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. It packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair, fiber optic lines, or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

PPTP

Point-to-Point Tunneling Protocol

Used for creating Virtual Private Networks (VPNs), developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known as the

PPTP Forum. Since the Internet is essentially an open network, the Point-to-Point Tunneling Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.

QLLC

Qualified Logical Link Control

Qualified Logical Link Control is an IBM-defined data-link-layer protocol that allows SNA data to be transported across X.25 networks.

RARP

Reverse Address Resolution Protocol

A protocol, defined in RFC 903, which provides the reverse function of ARP. RARP maps a hardware (MAC) address to an internet address. It is used primarily by diskless nodes when they first initialize to find their internet address.

RIP

Routing Information Protocol

A distance vector, as opposed to link state, routing protocol. It is an Internet standard IGP defined in RFC 1058. An updated version of this protocol called RIP version 2 is defined in RFC 2453.

RPC

Remote Procedure Call

An easy and popular paradigm for implementing the client-server model of distributed computing. In general, 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 [Source: RFC1208]. RPC is defined in RFC 1057.

SCP

Session Control Protocol

The DECnet protocol concerned with the establishment of virtual circuits over which NSP transfers data, interpreted in the DECnet Protocol Interface suite.

SDLC

Synchronous DataLink Control

An older serial communications protocol that was the model for LLC and with which it shares many features.

SLIP

Serial Line IP

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, but is not an Internet Standard. It is being replaced by PPP.

SMB

Simple Message Block

A message type used by the IBM PC LAN Program to make requests from a user station to a server and receive replies. Many of the functions are similar to those made by an application program to a DOS or to OS/2 running on a single computer.

SMTP

Simple Mail Transfer Protocol

A protocol used to transfer electronic mail between computers. It is specified in RFC 2821. It is a server to server protocol, so other protocols are used to access the messages.

SNA

Systems Network Architecture

SNA is a proprietary IBM architecture and set of implementing products for network computing within an enterprise. It existed prior to and became part of IBM's Systems Application Architecture (SAA) and it is currently part of IBM's Open Blueprint. With the advent of multi-enterprise network computing, the Internet, and the de facto open network architecture of TCP/IP, IBM is finding ways to combine its own SNA within the enterprise with TCP/IP for applications in the larger network.

SNA itself contains several functional layers and includes an application program interface called the Virtual Telecommunications Access Method (VTAM), a communications protocol for the exchange of control information and data, and a data link layer, Synchronous Data Link Control (SDLC). SNA includes the concepts of nodes that can contain both physical units that provide certain setup functions and logical units, each associated with a particular network transaction.

Sources: George McDaniel. IBM Dictionary of Computing, Tenth Edition, McGraw-Hill, (1993).

SNA/DS

SNADS enables the user to send DIA (Document Interchange Architecture) distributions across the SNA/DS network. DIA is a further protocol defining the format and structure of a distribution. The application information held within a distribution is regarded by the SNA/DS network as nothing more than a string of bytes. It is of no significance to the network whether these bytes represent human-readable ASCII or EBCDIC formats or machine-readable binary data. A DIA document is itself only one form of SNA/DS data. En route to the destination, this information should be transparent to all intermediary nodes. It should not be used in any of the processing performed at those nodes.

Sources: George McDaniel. IBM Dictionary of Computing, Tenth Edition, McGraw-Hill, (1993).

SNMP

Simple Network Management Protocol

The Internet standard protocol developed to manage nodes on an IP network. The first version is defined in RFC 1157 (STD 15). SNMPv2 (version 2) is defined in too many RFCs to list. It is currently possible to manage wiring hubs, toasters, jukeboxes, etc.

SPP

Sequence Packet Protocol

1. The XNS protocol that supports reliable connections using sequenced data; interpreted in the XNS Protocol Interface suite. A variant called SPX is used by Novell Netware.
2. The transport-level protocol that provides virtual connection service in Banyan VINES, based upon the protocol of the same name in XNS. Interpreted in the Banyan VINES Protocol Interface suite.

SPX and SPX2

Sequential Packet Exchange

Novell's version of the Xerox protocol called SPP. SPX communications are used for programs such as Novell's Print Server (PSERVER) and Remote Printer (RPRINTER), as well as Remote Console (RCONSOLE). SPX provides sequenced and acknowledged communications. It does not, however, provide sliding window functionality. SPX II, an enhanced version of SPX, does offer sliding window functionality.

TCP

Transmission Control Protocol

An Internet Standard transport layer protocol defined in RFC 793. It is connection-oriented and stream-oriented, as opposed to UDP. See TCP/IP below.

TCP/IP

Transmission Control Protocol/Internet Program

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in the private networks called intranets and in extranets. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layered program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "connectionless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being connectionless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not connectionless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

Most Internet users are familiar with the even higher layer application protocols that use TCP/IP to get to the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet (Telnet) which lets you logon to remote computers, and the Simple Mail Transfer Protocol (SMTP. These and other protocols are often packaged together with TCP/IP as a "suite."

Personal computer users usually get to the Internet through the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP). These protocols encapsulate the IP packets so that they can be sent over a dial-up phone connection to an access provider's modem.

Protocols related to TCP/IP include the User Datagram Protocol (UDP), which is used instead of TCP for special purposes. Other protocols are used by network host computers for exchanging router information. These include the Internet Control Message Protocol (ICMP), the Interior Gateway Protocol (IGP), and the Exterior Gateway Protocol (EGP).

TELNET

Telnet is the Internet standard protocol for remote terminal connection service. It is defined in RFC 854 and extended with options by many other RFCs.

TFTP

Trivial File Transfer Protocol

Trivial File Transfer Protocol is a network application that is simpler than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in RFC 1350.

UDP

User Datagram Protocol

A protocol within TCP/IP for sending unsequenced data frames not otherwise interpreted by TCP/IP. UDP is used by applications that need only a connectionless, best effort transport service. In order to use UDP, the application must supply the IP address and port number of the destination application. A port is an abstraction to allow transport protocols like UDP and TCP the capability of handling communications between multiple hosts. It allows a communication to be uniquely identified. Ports are identified by a positive integer. UDP is defined in RFC 768.

Sources: George McDaniel. IBM Dictionary of Computing, Tenth Edition, McGraw-Hill, (1993).

URL

Universal Resource Locator

A full URL is defined as follows:

Service://ServerAddress:PortNumber/PathToResource

The port number can usually be omitted because all standard services have default port numbers associated with them. For instance, http://www.flukenetworks.com/index.html is a URL that points to the document index.html on the server www.flukenetworks.com using the hypertext transfer protocol (World Wide Web access).

For the Service, you can use http, news, mailto, ftp, or others.

If you are referencing a document on the same service and server as a current request, you can omit the Service://ServerAddress portion of the URL.

You can also abbreviate the PathToResource by using relative paths in lieu of absolute paths where appropriate.

VINES

Virtual Network Software

The networking operating system developed by Banyan VINES, and the protocols used therein. Notable components are StreetTalk and Net RPC.

VIP

VINES Internet Protocol

The lowest-level protocol in Banyan VINES that is responsible for end-to-end forwarding and long packet fragmentation control.

X.25

The X.25 protocol, adopted as a standard by the Consultative Committee for International Telegraph and Telephone (CCITT), is a commonly-used network protocol. The X.25 protocol allows computers on different public networks (such as CompuServe, Tymnet, or a TCP/IP network) to communicate through an intermediary computer at the network layer level. X.25's protocols correspond closely to the data-link and physical-layer protocols defined in the Open Systems Interconnection (OSI) communication model.

Sources: George McDaniel. IBM Dictionary of Computing, Tenth Edition, McGraw-Hill, (1993).

XNS

Xerox Network System

A protocol suite developed by Xerox Corporation to run on LAN and WAN networks, where the LANs are typically Ethernet. Implementations exist for both Xerox's workstations and 4.3BSD, and 4.3BSD-derived, systems. XNS denotes not only the protocol stack, but also an architecture of standard programming interfaces, conventions, and service functions for authentication, directory, filing, email, and remote procedure call. XNS is also the name of Xerox's implementation.

[Source: Jeff Hodges]

XRD

eXternal Data Representation

A standard for machine independent data structures developed by Sun Microsystems and defined in RFCs 1014 and 1832. It is similar to ASN.1.

[Source: RFC1208]

See also http://www.iana.org/assignments/port-numbers.

TCP Protocols and Port Numbers

Protocol	Port # (decimal)
tcpmux	1
compressnet-mgmt	2
compressnet	3
echo	7
discard	9
systat	11
daytime	13
qotd	17
msp	18
chargen	19
ftp-data	20
ftp	21
ssh	22
telnet	23
priv-mail	24
smtp	25
nsw-fe	27
msg-icp	29
msg-auth	31
dsp	33
priv-print	35
time	37
rap	38
graphics	41
nicname	43
ni-ftp	47
auditd	48
tacacs	49
xns-time	52
dns	53
xns-ch	54
isi-gl	55
xns-auth	56
priv-term	57
xns-mail	58
priv-file	59
ni-mail	61
acas	62

via-ftp	63
covia	64
tacacs-ds	65
sql-net	66
gopher	70
priv-dialout	75
deos	76
priv-rje	77
vettcp	78
finger	79
http	80
hosts2-ns	81
xfer	82
mit-ml-dev	83
ctf	84
mfcobol	86
priv-termlink	87
su-mit-tg	89
dnsix	90
mit-dov	91
npp	92
dcp	93
objcall	94
dixie	96
swift-rvf	97
tacnews	98
metagram	99
newacct	100
hostname	101
iso-tsap	102
gppitnp	103
acr-nema	104
csnet-ns	105
3com-tsmux	106
snagas	108
pop2	109
pop3	110
sunrpc	111
mcidas	112
auth	113
audionews	114
ansanotify	116
uucp-path	117
sqlserv	118

nntp	119
erpc	121
smakynet	122
ansatrader	124
locus-map	125
unitary	126
locus-con	127
gss-xlicen	128
pwdgen	129
cisco-fna	130
cisco-tna	131
cisco-sys	132
ingres-net	134
endpoint-mapper	135
profile	136
netbios-ns	137
netbios-dgm	138
netbios-ssn	139
emfis-data	140
emfis-cntl	141
bl-idm	142
imap2-n-4	143
edp	144
uaac	145
iso-tp0	146
iso-ip	147
jargon	148
aed-512	149
sql-net	150
bftp	152
netsc-prod	154
netsc-dev	155
sqlsrv	156
knet-cmp	157
pcmail-srv	158
nss-routing	159
snmp	161
snmptrap	162
xns-courier	165
s-net	166
namp	167
rsvd	168
send	169
print-srv	170

multiplex	171
cl-1	172
xyplex-mux	173
mailq	174
vmnet	175
genrad-mux	176
nextstep	178
bgp	179
ris	180
unify	181
audit	182
ocbinder	183
ocserver	184
remote-kis	185
kis	186
aci	187
mumps	188
qft	189
gacp	190
prospero	191
osu-nms	192
srmp	193
irc	194
dn6-nlm-aud	195
dn6-smm-red	196
dls	197
dls-mon	198
smux	199
src	200
at-rtmp	201
at-nbp	202
at-3-5-7-8	203
at-echo	204
at-zis	206
quickmail	209
z39-50	210
914c-g	211
anet	212
vmpwscs	214
softpc	215
cai-lic	216
dbase	217
mpp	218
uarps	219

imap3	220
fln-spx	221
rsh-spx	222
cdc	223
peer-direct	242
sur-meas	243
daynachip	244
link	245
dsp3270	246
bh-fhs	248
matip	350
ldap	389
https	443
smtps	465
exec	512
login	513
shell	514
printer	515
talk	517
ntalk	518
ibm-db2	523
uucp	540
rtsp	554
nntps	563
banyan-vip	573
alternate-http	591
sshell	614
ldaps	636
doom	666
ftps-data	989
ftps	990
telnets	992
imaps	993
ircs	994
pop3s	995
socks	1080
lotus-notes	1352
timbuktu-srv	1417
ms-sql-server	1433
ms-sql-monitor	1434
ms-sna-server	1477
ms-sna-base	1478
citrix-ica	1494
sybase-sqlany	1498

imtc-mcs	1503
oracl-tns	1521
ingress-lock	1524
oracl-srv	1525
oracl-coauthor	1529
oracl-remdb	1571
oracl-names	1575
america-online	1590
h323-gatekeep-ras	1719
h323	1720
pt-pt-tunneling	1723
cisco-works	1741
oracl-em1	1748
oracl-em2	1754
ms-streaming	1755
ms-sms	1761
ms-mqs	1801
oracl-vp2	1808
oracl-vp1	1809
callbook	2000
gupta-sqlbase	2155
csp1	2221
csp2	2222
csp3	2223
cvs-pserver	2401
sybase-sqlanywhere	2638
ccmail	3264
ms-terminal-server	3389
sap-r3	3601
ibm-db2-conn-svc	3700
ibm-db2-int-svc	3701
ichat	4020
pc-anywhere-data	5631
xwin	6000
ircu	6665
vdolive	7000
realaudio	7070
cucme	7648
alternate-rtsp	8554
the-palace	9992
quake	26000
filenet-TMS	32768
filenet-RPC	32769
filenet-NCH	32770

Top Broadcasters

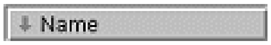
Selecting Top Broadcasters takes you to the Top Host screen and displays the top 50 MAC addresses sending broadcast packets.

Excessive broadcasts can cause networking performance problems since this traffic gets forwarded to all switch ports. Excessive broadcasts can also waste precious server and host resources (on the local broadcast domain), since the NICs will receive the packet and forward it to the higher layer software only to be discarded.

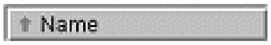
Note: Top Broadcasters is active when this analyzer is the selected source of statistics information. It is grayed out if the data source is anything other than the analyzer.

Sorting

The table (right pane) can be sorted by selecting a top column heading. Each column can be sorted as follows:



Descending Name



Ascending Name

Descending Address

Ascending Address

Descending Count

Note: Count can only be sorted descending.

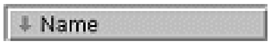
Top Errors

Top Errors displays the top 50 MAC addresses which are generating error packets. Each is displayed with an errored frame count.

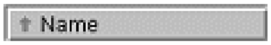
Note: Top Errors is active when this analyzer is the selected source of statistics information. It is grayed out if the data source is anything other than the analyzer.

Sorting

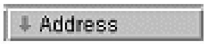
The table (right pane) can be sorted by selecting a top column heading. Each column can be sorted as follows:



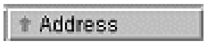
Descending Name



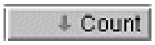
Ascending Name



Descending Address



Ascending Address



Descending Count

Note: Count can only be sorted descending.

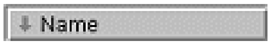
Top Multicasters

Selecting Top Multicasters takes you to the Top Hosts screen showing the top 50 MAC addresses sending Multicast packets.

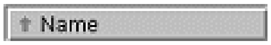
Note: Top Multicasters is active when this analyzer is the selected source of statistics information. It is grayed out if the data source is anything other than the analyzer.

Sorting

The table (right pane) can be sorted by selecting a top column heading. Each column can be sorted as follows:



Descending Name



Ascending Name

Descending Address

Ascending Address

Descending Count

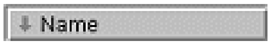
Note: Count can only be sorted descending.

Top Talkers

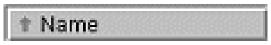
Selecting Top Talkers takes you to the Top Hosts screen showing the top 50 MAC addresses sending packets.

Sorting

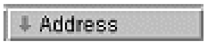
The table (right pane) can be sorted by selecting a top column heading. Each column can be sorted as follows:



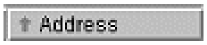
Descending Name



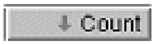
Ascending Name



Descending Address



Ascending Address



Descending Count

Note: Count can only be sorted descending.

See also http://www.iana.org/assignments/port-numbers.

UDP Protocols and Port Numbers

Protocol	Port # (decimal)
echo	7
discard	9
systat	11
daytime	13
qotd	17
msp	18
chargen	19
ssh	22
priv-mail	24
nsw-fe	27
msg-icp	29
msg-auth	31
dsp	33
priv-print	35
time	37
rlp	39
graphics	41
nameserver	42
auditd	48
re-mail-ck	50
la-maint	51
xns-time	52
dns	53
xns-ch	54
isi-gl	55
xns-auth	56
priv-term	57
xns-mail	58
priv-file	59
ni-mail	61
bootps	67
bootpc	68
tftp	69
priv-dialout	75
deos	76
priv-rje	77
vettcp	78
hosts2-ns	81

xfer	82
mit-ml-dev	83
ctf	84
priv-termlink	87
kerberos	88
npp	92
dcp	93
dixie	96
swift-rvf	97
tacnews	98
metagram	99
iso-tsap	102
gppitnp	103
csnet-ns	105
3com-tsmux	106
pop3	110
sunrpc	111
audionews	114
ansanotify	116
sqlserv	118
cfdptkt	120
erpc	121
smakynet	122
ntp	123
ansatrader	124
unitary	126
gss-xlicen	128
pwdgen	129
cisco-fna	130
cisco-tna	131
cisco-sys	132
endpoint-mapper	135
netbios-ns	137
netbios-dgm	138
netbios-ssn	139
emfis-data	140
emfis-cntl	141
bl-idm	142
edp	144
uaac	145
iso-tp0	146
iso-ip	147
jargon	148
aed-512	149

sql-net	150
netsc-prod	154
netsc-dev	155
nss-routing	159
snmp	161
snmptrap	162
xns-courier	165
s-net	166
namp	167
rsvd	168
send	169
print-srv	170
multiplex	171
cl-1	172
xyplex-mux	173
mailq	174
vmnet	175
genrad-mux	176
xdmcp	177
nextstep	178
ris	180
unify	181
audit	182
ocbinder	183
ocserver	184
remote-kis	185
kis	186
aci	187
mumps	188
gacp	190
osu-nms	192
srmp	193
irc	194
dls	197
dls-mon	198
src	200
at-rtmp	201
at-nbp	202
at-3-5-7-8	203
at-echo	204
at-zis	206
quickmail	209
914c-g	211
anet	212

ipx-tunnel	213
vmpwscs	214
softpc	215
cai-lic	216
dbase	217
uarps	219
fln-spx	221
rsh-spx	222
cdc	223
peer-direct	242
sur-meas	243
daynachip	244
link	245
dsp3270	246
subnet-bcast-tftp	247
bh-fhs	248
codaauth2	370
ldap	389
timbuktu	407
biff	512
who	513
syslog	514
talk	517
ntalk	518
rip	520
banyan-vip	573
ldaps	636
ircs	994
pop3s	995
lotus-notes	1352
timbuktu-srv	1419
streamworks-mpeg	1558
citrix-icabrowser	1604
h323-gatekeep-disc	1718
h323-gatekeep-ras	1719
ms-mqs-ping	1801
hsrp	1985
callbook	2000
ccmail	3264
ms-mqs-discovery	3527
rtp	5004
rtcp	5005
pc-anywhere-stat	5632
realaudio	6970

cucme	7648
ivisit	9943
the-palace	9992
quake	26000
filenet-TMS	32768
filenet-RPC	32769
filenet-NCH	32770

vip

vipc
 vspp
 varp
 vrtp
 vicp

Back/Forward Buttons

The back and forward buttons ◄ ► allow you to easily step through all the discovered devices in the same order as they appear in the Device Discovery screen. Device (host) detail is updated as each host is stepped through.

Glossary

10BASE2

Sometimes called ThinLAN or CheaperNet, 10BASE2 is the implementation of the IEEE 802.3 Ethernet standard on thin coaxial cable. The maximum segment length is 185 meters.

10BASE5

Sometimes called ThickLAN, 10BASE5 is the implementation of the IEEE 802.3 Ethernet standard on thick coaxial cable. The maximum segment length is 500 meters.

10BASEF

A point-to-point fiber link. This is the draft specification for IEEE 802.3 Ethernet over fiber optic cable.

10BASE-T

A point-to-point copper link. This is the implementation of the IEEE 802.3 Ethernet standard on unshielded twisted-pair wiring. It is a star topology, with stations directly connected to a multi-port hub and has a maximum cable length of 100 meters.

100BASE-TX

A point-to-point copper link. Fast Ethernet; 100 Megabit version of Ethernet that operates on two pair of a 4 pair category 5 cable.

100BASE-FX

A point-to-point fiber link. Fast Ethernet; 100 Megabit version of Ethernet that operates on two fiber optic fibers using 850nm wavelength.

10/100BASE-FLP

A point-to-point copper link. 10/100BASE Fast Link Pulse (FLP) Burst; FLP is the basic mechanism that Auto-Negotiation uses to advertise the device's abilities. It is a series of link pulses which encode a 16 bit word. An FLP Burst is composed of 17 to 33 link pulses which are identical to the link pulses used in 10BASE-T to determine whether a link has a valid connection (sometimes referred to as Normal Link Pulses or NLPs.) FLP Bursts occur at the same interval as NLPs, 16.8ms. An FLP Burst has a nominal duration of 2 ms.

An FLP Burst interleaves clock pulses with data pulses to encode a 16 bit word. The absence of a pulse within a time window following a clock pulse encodes a logic zero and a pulse within the time window following a clock pulse encodes a logic one.

1000BASE-X

A point-to-point fiber or copper link. This is the standard for fiber optic Gigabit Ethernet. The 802.3z standard describes the specifications for the 1000BASE-X fiber optic Gigabit Ethernet system.

802.2

This IEEE standard specifies Logical Link Control (LLC), which defines services for the transmission of data between two stations at the data-link layer of the OSI model.

802.3

Often called Ethernet, this IEEE standard governs the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) networks. Typical cabling standards are 10BASE-T, 10BASE2, and 10BASE5.

Access Method

The set of rules by which the network determines what node has access to the network. The most popular access method is Collision Sense Multiple Access/Collision Detection (Ethernet).

Anomaly

An impedance discontinuity causing an undesired signal reflection on a transmission cable.

AppleTalk

The set of protocols that define Apple Computer's networking specification.

ARP (Address Resolution Protocol)

A member of the TCP/IP protocol suite, ARP is the method by which a station's MAC address is determined given a station's IP (Internet Protocol) address.

ARP Cache

The ARP cache is where each IP host maintains the most recent IP to MAC address mapping. The ARP cache is maintained so that the IP can quickly send IP packets with the correct Ethernet or FDDI MAC address.

ASCll (American Standard Code for Information Interchange)

A standard for character-to-number encoding that is widely used in the computer industry. An ASCII file is generally referred to as a text file.

Attenuation

Attenuation is the loss of signal strength over the length of the cable. It is caused by a loss of electrical energy due to the resistance of a cable and by leakage of energy through a cable's insulating material. Attenuation losses due to cable resistance increase as the transmission frequency increases, and losses due to insulation leakage increase as temperature increases.

Autonomous System

A group of routers exchanging routing information via a common routing protocol.

Backward Explicit Congestion Notification (BECN)

Notification by the network that an end user is sending frame relay data onto the network that is either causing or encountering congestion within the WAN network.

Bandwidth

Bandwidth is the rate at which data can be transmitted over a channel. It is measured in bits per second. For example, Ethernet has a 10 Mbps bandwidth and FDDI has a 100 Mbps bandwidth. Actual throughput is almost always less than the theoretical maximum.

Basic Rate Interface (BRI) ISDN

service consisting of two 64 Kbps B channels for data transmission and one 16 Kbps D channel for signaling information. Some providers may provide alternate configurations of BRI ISDN.

Beaconing

The condition of a ring that has one or all NICs transmitting beacon frames.

BNC

A coaxial cable connector used with ThinLAN (10BASE2) Ethernet networks.

Bindery

A Novell NetWare 2.x and 3.x database which stores information about the resources (services) and clients on an IPX network, such as passwords, client accounts, and client restrictions.

Bootstrap Protocol

A protocol that provides a subset of the services provided by DHCP. It is used for the central administration and distribution of IP addresses and other boot-process information. BootP is normally used on large networks where IP management is an issue and where IP devices need to acquire IP parameters at power up.

Border Gateway Protocol 4 (BGP-4)

Border Gateway Protocol 4 (RFC 1771) is used to connect different autonomous systems. While most routing protocols (such as OSPF, IGRP and RIP) use broadcast or Multicast, BGP uses TCP which requires being connected in the connection path to discover the use of BGP.

BOOTP (Bootstrap Protocol)

BOOTP is a protocol that lets a network user be automatically configured (receive an IP address) and have an operating system booted or initiated without user involvement. The BOOTP server, managed by a network administrator, automatically assigns the IP address from a pool of addresses for a certain duration of time.

BOOTP is the basis for a more advanced network manager protocol, the Dynamic Host Configuration Protocol (DHCP).

BPS

Bits per second. A measure of speed or raw data rate. Often combined with metric prefixes as in Kbps (for thousands of bits per second) or Mbps (for millions of bits per second).

Bridge

A device that links two or more networks that use the same OSI Data Link protocol. A bridge evaluates source and destination addresses to pass only frames that have a destination on the connecting network.

Broadcast

A message that is addressed to all stations on a network. For Ethernet networks, the MAC broadcast address is FFFFFFFFFFFF.

Broadcast Storm

A situation in which a large number of stations are transmitting broadcast packets. This typically results in severe network congestion. This problem is usually a result of a misconfiguration.

Browser

A program that provides a graphical interface to the World Wide Web.

Bus Topology

A bus topology is a network architecture in which all of the nodes simultaneously receive network traffic. Ethernet is a bus topology.

Byte

A collection of bits. A byte usually contains 8 bits.

Cable Types

The following cables can be tested by the analyzer.

UTP100 Category 3
UTP100 Category 4

UTP100 Category 5
UTP Cat 5e
UTP100 Category 6
ScTP100 Category 3
ScTP100 Category 4
ScTP100 Category 5
ScTP100 Cat5e
ScTP100 Category 6
ScTP120 Category 3
ScTP120 Category 4
ScTP120 Category 5
ScTP120 Category 6

UTP is the abbreviation for unshielded twisted pair, and ScTP is the abbreviation for screened twisted pair.

Category 3 is typically used in 10 Mbit Ethernet.
Category 4 is typically used in 10 Mbit Ethernet.
Category 5 is typically used in 10/100 Mbit Ethernet with Category 5E extending to 1000 Mbit copper. Category 5 is the default setting in Cable Test.
Category 6 is a proposed standard in the final stages of approval (05/00).

Characteristic Impedance

Characteristic impedance is the opposition (resistance and reactance) to signal propagation on a cable. It depends on the physical properties of a cable, which are determined at the time of manufacture. Manufacturing variations can cause slight differences in characteristic impedance for the same cable type.

Client

A client is a computer that make requests of a server. A client has only one user; a server is shared by many users.

Coaxial

A type of cable in which the inner conductor is surrounded by a tubular conductor, which acts as a shield. Coaxial cables typically have a wide bandwidth.

Collision

A collision is the result of two or more nodes transmitting at the same time. Excessive collisions are most often caused by a problem with the physical media.

Collision Frames = 1 RFC-1643

"Single Collision Frames", a count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Collision Frames > 1 RFC-1643

"Multiple Collision Frames", a count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Committed Burst Rate (Bc)

A contractually agreed upon, guaranteed, bandwidth rate above the Committed Information Rate that a carrier agrees to provide a frame relay PVC (under normal network conditions).

Committed Excess Burst Rate (Be)

A contractually agreed upon, guaranteed, bandwidth rate above the Committed Burst rate that a carrier agrees to try and sustain for a frame relay PVC. Excess burst rate traffic is automatically flagged as discard eligible.

Committed Information Rate (CIR)

For frame relay service, a contractually agreed upon minimum bandwidth that is available to an end user's permanent virtual circuit (PVC) at all times.

Crossed Pair

A wiring error in twisted pair cabling in which a pair on one connector of the cable is wired to a different pair on the other end of the cable.

Crosstalk

is electrical interference generated by signal coupling between wires in a multiwire cable.

CSMA/CD (Carrier Sense, Multiple Access with Collision Detection)

In CSMA/CD, each node or station has equal access to the network. Before transmitting, each station waits until the network is not busy. Since each node has equal access to the network, a collision (two stations transmitting at the same time) can occur. If a collision occurs, the affected nodes will wait a random time to retransmit. Ethernet uses the CSMA/CD access method.

DLCI (Data Link Connection Identifier)

The local frame relay permanent, virtual circuit address assigned by a frame relay provider to designate the channel between the user and the network.

DB

Abbreviation for decibel. A logarithmic unit of measure expressing the amplitude ratio between two signals.

DB-9 Connector

A modular connector used for STP wiring. The DB-9 connector has nine conductors to accommodate two pairs of wires.

DECnet

Digital Equipment Corporation's set of communication protocols for networking computers.

Designated Bridge

For IEEE 802.1d or DEC spanning tree, only the designated bridge (one per LAN segment or collision domain) can forward frames and transmit spanning tree Bridge Protocol Data Units (BPDU). The designated bridge is the bridge on a given segment that has the lowest cost to the root bridge.

Destination Address

The address of the station receiving a frame.

DHCP (Dynamic Host Configuration Protocol)

A protocol established to lessen the administrative burden of manually configuring TCP/IP hosts on a network. DHCP provides a service that allows a device attached to the network to learn all or at least some of its network configuration automatically.

Discard Eligible (DE) bit

Frame relay users can designate the discard eligibility of frames by configuring their routers or switches to set flags within the frame relay data frames. When the network becomes congested, the frames with the discard eligible bit set will be the first to be discarded.

DNS (Domain Name Server)

A general purpose distributed data query (or look up) service based on host names that are in the form of domain names. A domain is a unique name given to a logical collection of computers connected to one or more networks. Domain names typically end in a suffix denoting the type of site (such as, **flukenetworks.com**). The **.com** stands for a commercial company.

E1

Digital line service that provides a transmission rate of 2.048 Mbps. Most common outside North America.

EIA568

Electronic Industries Association Commercial Building Telecommunications Wiring Standard. Specifies maximum cable lengths, installation practices, and performance specifications for generic building wiring.

EIGRP

Cisco Systems Enhanced version of their IGRP routing protocol. While still a distance-vector routing protocol, EIGRP offers fast reaction to network changes.

Encapsulation

is the method of placing one protocol into another protocol's format. For example, in a Novell Ethernet environment there are four different methods to encapsulate IPX in Ethernet/802.3 frames: 802.3 raw, 802.2, Ethernet II, and SNAP.

Ethernet

is a 10 Mbps topology that runs over thick coax, thin coax, twisted-pair, and fiber-optic cabling systems.

Excess Collisions

RFC-1643 Excessive Collisions, a count of frames for which transmission on a particular interface fails due to excessive collisions.

Fast Ethernet

Industry standard terminology for 100Base-T. Industry groups do not agree on using the term to refer to 100VG-AnyLAN; some call 100VG-AnyLAN a Fast Ethernet technology while others do not.

FCS (Frame Check Sequence)

A field transmitted in LAN frames that encodes error checking information.

Fiber-Optic Cable

Communications cable that use light as the signal carrier. Fiber-optic cable is immune to electrical and magnetic interference.

Fiber-Optics

A technology that transmits light beams along optical fibers. The light beams are used as a digital information carrier. The optical fibers are formed into fiber optic cables and are a direct replacement for conventional cables and wire pairs. Fiber optic cables are immune to electrical and magnetic interference and occupy much less physical space than conventional cables and wire pairs.

Forward Explicit Congestion Notification (FECN)

Notification by the network to an end user that frame relay data being received is either causing or encountering congestion within the WAN network.

Frame

A frame is the transmission unit on a network.

Frame Errors

For FDDI, Frame Errors (RFC 1512) is the number of frames that were detected to be "in error" by this MAC and were not detected to be "in error" by another MAC.

Frame Relay

A fast form of packet switching that is accomplished with smaller packet sizes and less error checking.

Full-Duplex

10Base-T and 100Base-TX network operation using a switching Hub to establish a point-to-point connection between LAN nodes that allows simultaneous sending and receiving of data packets. Full-duplex performance is twice that of half-duplex performance. A 10Base-T full-duplex network is capable of 20 Mb/s data throughput; likewise, a full-duplex 100Base-TX network is capable of 200 Mb/s throughput.

Half-Duplex

Network operation is one direction at a time only; either sending or receiving data packets, but not both at the same time.

Hermaphroditic Connector

A loopback, or self-shorting, connector typically used with Type 1 (STP) cable.

Hops

Most commonly defined as the number of routers traveled by a frame to reach its destination.

Host

A computer that is configured to allow users to communicate with other host computers on a network. Individual users can communicate with other individuals by using application programs, such as electronic mail, browser, and FTP.

HTTP (Hypertext Transfer Protocol)

The protocol used to communicate between Web clients and servers.

Hub

Today, most often referred to in 10BASE-T or 100BASE-T networks. A 10BASE-T/100BASE-T hub is essentially a multiport repeater hub with each segment dedicated to a single connection.

Hyperlink

Highlighted words on a Web page that provide a jump (hyper link) to a different document (or page) on the World Wide Web when it is selected. The jump can be to an additional page at the current Web site or to a completely different Web site.

ICMP (Internet Control and Message Protocol)

A communication protocol used by every device that uses IP. ICMP reports errors that occur during the delivery of packets on the network.

Integrated Service Digital Network (ISDN)

The combination of voice and digital network services in a single medium. This provides voice connections and digital data services over the same phone line.

Interior Gateway Routing Protocol (IGRP)

Interior Gateway Routing Protocol is a Cisco Systems proprietary distance-vector protocol (such as RIP) that takes into account the potential bandwidth of links in its routing table determination. This makes a 10 Mb LAN have a lower cost assessment than a 9600 serial line.

Internet

The Internet is a global network of networks connecting millions of users worldwide via many computer networks using a simple standard common addressing system and communications protocol called TCP/IP (Transmission Control Protocol/Internet Protocol).

Internet Protocol (IP)

IP is the network layer protocol for the TCP/IP suite.

Internetwork Packet Exchange (IPX)

IPX is the network layer protocol for Novell's NetWare protocol suite.

Jabber

A frame greater than the maximum legal size (1518 bytes) with a good or bad frame check sequence. In general, you should not see jabbers. The most likely causes of jabbers are a faulty NIC/driver or perhaps a cabling problem.

Key Devices

The OptiView analyzer Discovery supports logging key devices selected by the user. This category can consist of all servers, switches, and routers since these are the devices an administrator most likely wants to monitor regularly. Key devices can also be considered to be the devices that provide infrastructure support to the network by keeping it operational. The OptiView analyzer checks the up/down status of key devices approximately every 2 minutes. A key device can be changed to a non-key device and vice versa.

LAN (Local Area Network)

A physical network technology used over short distances to connect many workstations and network devices using a communication standard (Ethernet, for example).

Late Collision

A collision that occurs after the first 64 bytes in a frame. The analyzer will generally only see late collisions on a coaxial segment. In 10BASE-T networks, late collisions will be seen as frames with a bad FCS. Causes of Late Collisions are a faulty NIC or a network that is too long.

Layer

One of seven levels in the Open Systems Interconnection (OSI) reference model. See OSI.

Link Error Rate (LER)

For FDDI, Link Error Rate (RFC 1512) is an estimate of the error rate for each physical port (PHY). Most devices will shutdown the port if the error rate is any greater than 10E-7. Error rates of 10E-12 are good, error free links.

Link Pulse

A single-bit test pulse that is transmitted at least every 150 milliseconds during idle periods on 10BASE-T link segments to verify link integrity.

Lobe Cable

Lobe cable is the length of cable connecting the MAU to the NIC. The lobe cable can be several connected cable segments.

Loopback Connector

A connector used anywhere on a cable for returning test signals.

MAC (Media Access Control)

The MAC protocol defines the access method for a particular network topology.

Manufacturer Prefix

The standard partial address used to identify a particular manufacturer. The prefix of the address is predefined uniquely for each manufacturer, while the remainder of the address uniquely identifies the station.

Mbps

Millions of bits per second. See BPS.

MDI and MDI-X

MDI is a media dependent interface. It is the IEEE standard for the interface to an unshielded twisted pair (UTP) cable.

In order for two devices to communicate, the transmitter of one device must connect to the receiver of the other device. The connection can be established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

Ports that implement a crossover function internally are known as MDI-X ports, where X refers to the crossover function.

MIB (Management Information Base)

The set of objects that can be used by an SNMP management station to query for information or to set parameters in the SNMP agent, such as a router. Also see RMON MIB.

MIME (Multipurpose Internet Mail Extensions)

An Internet formatting standard used for encoding files that will be attached to email messages. Also see UU Encoding.

Misaligned

RFC-1643 "Alignment Errors", a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.

Multicast

Packets that are directed to a group of nodes rather than to a single node or all nodes. This is contrasted to a broadcast packet, which is directed to all nodes.

NAUN (Nearest Active Upstream Neighbor)

The active station that is directly upstream from a given station.

NEXT

(Near-End Crosstalk) is a measure of the crosstalk coupled from one wire pair to another pair.

NIC (Network Interface Card)

A network interface card is the adapter card that plugs into a computer to provide a network connection.

NOS (Network Operating System)

A network operating system is the software that runs on a group a computers (clients and servers) that mediates the access to the files and resources. Examples of NOSs include Novell NetWare, and Banyan VINES.

Not Copied

For FDDI, Not Copied (RFC 1512) is a count that should, as closely as possible, match the number of frames that were addressed to this MAC but were not copied into its receive buffers. This might occur due to local buffer congestion.

NVP (Nominal Velocity of Propagation)

The speed of a signal through a cable expressed as a percentage of the speed of light. Typically, the speed of a signal through a cable is 60-80% of the speed of light.

Open

A break in the continuity of a circuit which prevents signal transmission.

Open Shortest Path First (OSPF)

Open Shortest-Path First (RFC 2328) is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a list of least cost paths.

OSI (Open Systems Interconnection)

OSI is the international standard for data communication between computer systems. The OSI model provides the foundation for products from different vendors to function in the same network. The following is a list of the seven layers of the OSI model:

Layer 1: The **Physical Layer** handles the electrical and mechanical connections of network components to insure bit transmission between stations.

Layer 2: The **Data Link Layer** handles the way frames are transmitted and provides frame error controls for reliable communication between stations.

Layer 3: The **Network Layer** determines the path for communication between stations and handles routing and congestion issues on the network.

Layer 4: The **Transport Layer** handles the exchange of entire messages between stations and error recovery.

Layer 5: The **Session Layer** handles the communication sessions between computers.

Layer 6: The **Presentation Layer** provides transparent data communications between stations of different types.

Layer 7: The **Application Layer** provides all functions to support end-user services or applications.

Packet

A group of bits in a defined format, containing a data message that is sent over a network.

Permanent Virtual Circuit (PVC)

A circuit that is kept up permanently such as a dedicated leased line on the telephone network.

Plenum Cable

A Plenum cable is one that has been certified for installation in air ducts and open spaces over suspended ceilings when not using conduit. Plenum cable is fire-resistant and does not emit toxic fumes when burned.

Pop-Up Window

A window that the analyzer displays to communicate information or to prompt you with a choice of actions.

Primary Rate Interface (PRI) ISDN

service based on a rate of 1.544 Mbps and including 23 B channels and one 64 Kbps D channel. The B channels provide data transmission while the D channel provides signaling information.

Propagation Delay

Propagation Delay is the time it takes for a signal to go from one end of a cable to the other. There should be similar delay characteristics between cable pairs. Propagation Delay is very important for technologies that use parallel transmission techniques, such as 100BASE-T4 and 100BASE-VG.

Protocol

A set of rules that machines must follow to exchange information on a network.

Proxy ARP

Routers with Proxy ARP enabled will respond to ARP requests for off-net hosts. When a node relies on Proxy ARP, the node only has to ARP for the target node instead of forwarding the packet to the correct local IP router. Some vendors' routers respond incorrectly to on-net ARP requests, which can create confusing network behavior.

Remote Collision

A collision that occurs on the other side of a repeater. Since a 10/100BASE-T hub is a multi-port repeater with a "segment" dedicated to each station, 10/100BASE-T collisions are remote collisions.

Remove Ring Station

The act of taking an active device from the ring.

Repeater

A repeater is a layer-1 device that regenerates and retimes frames.

Report Soft Error Frame

A MAC frame that is transmitted when an intermittent, or soft error causes data to be transmitted more than once. The Report Soft Error Frame contains information about the error, or errors, on the ring.

Reversed Wire

A wiring error in twisted pair cabling in which the pins on a pair are reversed between connectors on each end of the cable.

RFC-1398

Definitions of Managed Objects for the Ethernet-like Interface Types

RJ-45 Connector

A modular connector used for UTP wiring. The RJ-45 connector has eight conductors to accommodate four pairs of wires, and has become the dominant connector used in Ethernet UTP installations.

RMON MIB (Remote Network Monitoring MIB)

The set of objects defined in various RFCs and private MIBs that are used to monitor various network activity. Also see MIB.

Router

A router is a network-layer device that connects networks using like network-layer protocols. Routers can span different network topologies. For example, a router can interconnect Ethernet Novell NetWare networks. For a router to pass traffic, unlike a bridge, it must be configured for the desired protocol. Routers are more difficult to configure but offer greater security.

Routing Information Protocol (RIP)

Routing Information Protocol (RFCs 1058, 1388, 2453) is the most widely supported IP routing protocol. RIP is a distance-vector protocol and bases its routing decisions on the number of hops.

Runts

Typically defined as an Ethernet frame which is less than 64 bytes. Depending on which device is counting the runts, the frame check sequence may be good or bad.

Screened Twisted-Pair (ScTP)

ScTP is a cable type that has four twisted pairs (similar to UTP), and has a foil shield (unlike UTP). Used in Europe and America.

Server

File servers store files that may be shared by the network workstations. A server (file server) is a computer that contains files and is dedicated to delivering those files to other computers upon request.

Short

A near-zero resistance connection between two wires of a circuit.

Short Frame

A frame less than the minimum legal size (less than 64 bytes) with a good frame check sequence. In general, you should not see Short Frames. The mostly likely cause of a Short Frame is a faulty adapter card or driver.

Signal/Noise Ratio

The ratio of worst-case received signal level to noise level measured at the receiver input (expressed in DB). The S/N ratio may be expressed as NEXT(DB) - Attenuation(DB), provided idle channel background noise is low. Higher S/N ratios provide better channel performance.

SMTP (Simple Mail Transfer Protocol)

A protocol used to transfer email between hosts and ultimately to its final destination.

SMTP Host

A computer running the Simple Mail Transfer Protocol (SMTP) that handles email delivery.

SNMP (Simple Network Management Protocol)

The Internet standard protocol for communicating between network managers and other network nodes. Also see MIB (Management Information Base) and RMON MIB (Remote Network Monitoring MIB).

Source Address

The address of the station originating a frame.

Source Routing

Source routing is a method by which a station discovers the route to a target station.

Split Pair

The error of using wires from two different twisted pairs. This error cancels the crosstalk elimination characteristics of twisted pair wiring and produces crosstalk. Use a single twisted pair for transmit and another twisted pair for receive to minimize crosstalk.

Static Router

A device on the network that is assumed to be a router based on information monitored on the network.

STP (Shielded Twisted Pair)

Cable that is both twisted and shielded by pairs. This eliminates crosstalk to a greater degree than UTP cable and minimizes crosstalk at high transmission rates.

Symbolic Name

A symbolic name is the name given to an address to make it easier to use (MKG_SERVER versus 0003e8000008, for example).

T1

Digital line service that provides a transmission rate of 1.544 Mbps. The 1.544 Mbps bandwidth of T1 is usually divided into twenty-four 64 Kbps channels.

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is the protocol suite originally developed by the Advanced Research Projects Agency (ARPA) to interconnect a research network. The TCP/IP is an open standard not owned by any particular organization. The term TCP/IP is often used to refer to the entire suite of related protocols that includes IP, FTP, Telnet, RIP.

TDR (Time Domain Reflectometry)

A TDR is a method to determine a cable's length, characteristic impedance, and other parameters by transmitting a pulse into a cable and examining reflected energy.

Telnet

Telnet is a session-layer protocol in the TCP/IP protocol providing terminal emulation.

Terminator

A resistor connected to the end of a coax cable which is intended to match the characteristic impedance of a cable. Signals are dissipated in the terminator, eliminating reflections.

Too Long

RFC-1643 "FrameTooLongs", a count of frames received on a particular interface that exceed the maximum permitted frame size.

Topology

Topology is the organization of network components.

Transceiver

In Ethernet networks, a transceiver is used to couple electrical signals to and from an adapter to the transmission media. In ThinLAN and 10BASE-T networks, the transceiver is integrated directly onto the network adapter card.

Transmit Delay

RFC-1643 "DeferredTransmissions", a count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.

Twisted Pair

A pair of wires that are twisted to minimize crosstalk. Crosstalk is minimized with twisted pair wiring by canceling the magnetic fields generated in each of the twisted wires. Twisted pair cable (UTP or STP) is typically made up of several twisted pairs of wires.

Unicast

A packet that is directed to a single node is a Unicast packet. This is contrasted to a broadcast packet, which is directed to all nodes.

UTP (Unshielded Twisted Pair)

Cable that is twisted by pairs but not shielded. This minimizes crosstalk by canceling the magnetic fields generated in each of the twisted wires.

UU Encoding

A standard Internet format used for encoding files that will be attached to email messages. Also see MIME (Multipurpose Internet Mail Extensions).

Virtual Circuit

A network capability that lets two ports communicate as if they were directly connected without regard for the structure of the physical layer.

VLAN (Virtual LAN)

A group of ports configured into one broadcast domain (or logical LAN). VLANs can only be detected by using the private MIB associated with the device.

WAN (Wide Area Network)

A network that is usually constructed with serial lines, which covers a large geographic area. Also see LAN (Local Area Network).

Wavelength

The length of the optical wave used in fiber optic transmissions. Also used to specify the different optical sources available for fiber optic usage.

Wire Fault

A hard error caused by opened or shorted network wires.

World Wide Web (WWW)

A hyperlink-based, distributed information system that can be used to create, edit, or browse documents. It is a powerful, global, information system. The hyperlinks provide access to other information sources on the Internet. Also see Hyperlink.

Layer 2 WAN MIB Support

Listed below are the technologies and details for the WAN layer 2 and layer 3 user interface:

DS1 (T1/E1)
RFC2495

In tabular display

- Line Coding
- Send Coding
- Line Type
- Signal Mode
- Circuit Id
- Line Id

In graphical Utilization display

- Line Status (Red or Yellow Alarm State)

In graphical Errors display

- Ess – Errored Seconds
- Sess – Severely Errored Seconds
- Sefs – Severely Errored Framing Seconds
- Uass – Unavailable Seconds
- Csss – Controlled Slip Seconds
- Pcvs – Path Coding Violations
- Less – Line Errored Seconds
- Bess – Bursty Errored Seconds
- Lcvs – Line Coding Violations

DS3 (T3)
RFC2496

In tabular display

- Line Coding
- Send Coding
- Line Type
- Line Length
- Circuit Id
- Line Id

In graphical Utilization display

- NA

In graphical Errors display

- Pess – P-Bit Errored Seconds
- Psess – P-Bit Severely Errored Seconds

- Sefs – Severely Errored Framing Seconds
- Uass – Unavailable Seconds
- Lcvs – Line Coding Violations
- Pcvs – P-Bit Coding Violations
- Less – Line Errored Seconds
- Ccvs – C-Bit Coding Violations
- Cess – C-Bit Errored Seconds
- Csess – C-Bit Severely Errored Seconds

SONET (OC-n, SDH-n)
RFC2558

In tabular display

- Indicates if Path, Line or Section information is being displayed
- Medium Type
- Line Coding
- Circuit Id-Line Id

In graphical Utilization display
Status Alarms:

- SLOS – Section Loss of Signal (RED)
- SLOF – Section Loss of Frame (RED)
- LAIS – Line Alarm Indicate Signal (RED)
- LRDI – Line Remote Defect Indication (RED)
- PAIS – Path Alarm Indicate Signal (YELLOW)
- PLOP – Path Loss of Pointer (YELLOW)
- Path Remote Defect Indication (YELLOW)

Note: Sonet “Path” information will be shown if available for graphical views.

In graphical Errors display

- SectEss – Section Errored Seconds
- SectSess –Section Severely Errored Seconds
- SectSefs – Section Severely Errored Framing Seconds
- SectCvs – Section Coding Violations
- LineEss – Line Errored Seconds
- LineSess - Line Severely Errored Seconds
- LineCvs – Line Coding Violations
- LineUass – Line Unavailable Seconds
- PathEss – Path Errored Seconds
- PathSess - Path Severely Errored Seconds
- PathCvs – Path Coding Violations
- PathUass – Path Unavailable Seconds

I**SDN Bearer Channel**
RFC2127

- Type

- Channel Number
- Channel Type
- Operation Status
- Info Type

ISDN Basic Rate
RFC2127

- Interface Type
- Line Topology
- Interface Mode
- Signal Mode

ISDN D “Signaling” Channel
RFC2127

- Type
- Signal Index
- In Calls
- In Connections
- Out Calls
- Out Connections

ATM
Note: An entry will display in the interface table for ATM, but no additional L2 statistics are available. The ATM interface table entry is usually NOT the same as the associated L2 (such as SONET) interface. If a non-Layer 3 interface is selected, the **WAN** button will go to the first interface with Layer 3 information (this is often the correct one).

Layer 3 WAN MIB Support

Frame Relay
RFC1315 (SNMPv1)

ATM
RFC2515 (error information only)
Cisco Private MIBs (1.3.6.1.4.1.9.10.13.1.2.1.1)
(Cell counts & Cell drops)
CISCO-AAL-MIB (1.3.6.1.4.1.9.9.66.1.1.1.1)
(per VC packet / octet counts)

In tabular display

Ÿ Number of configured VCIs
Ÿ Number of configured VPIs
Ÿ Max Active VPI Bits
Ÿ Max Active VCI Bits
Ÿ ILMI VPI-ILMI VCI

In graphical WAN display

Ÿ Current Cell Drops (see Frame Relay FECN+BECN)
Ÿ Previous Cell Drops (see Frame Relay FECN+BECN)
Ÿ Virtual Path ID
Ÿ Virtual Channel ID
Ÿ Admin Status
Ÿ Utilization (Cisco MIB)
Ÿ Octets In (Cisco MIB)
Ÿ Octets Out (Cisco MIB)
Ÿ Cells In (Cisco MIB)
Ÿ Cells Out (Cisco MIB)
Ÿ Cells Dropped

ISDN
RFC2127 See Layer 2 table

Statistics (graphical view)

Presents a graphical view of each device interface's utilization usage. The device is selected at the top of the screen (**Device** field) and the interface can be selected by moving the white vertical bar over an interface in the graph. Data Source, Utilization, and Error information is given on the selected interface.

Note: This screen sorts by port number first, then interface number. If an interface is not tied to a port number, it shows at the end of the graph.

MultiPort Statistics - Presents the segment's multi-port information in a graphical view. Moving the position of the white vertical bar determines the Interface/Port number, or selecting the Interface/Port number from the Interface drop-down list moves the white vertical bar over the corresponding Interface/Port number

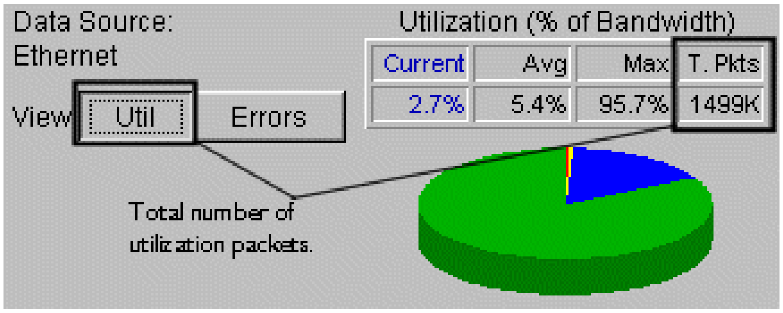
Good Frames Versus Errors - Each vertical bar represents statistics for one interface. The green portion of the vertical bar represents Good Frames and the red portion represents the Bad Frames. Together, the Good and Bad Frames make up the entire vertical bar which represents the % utilization of that interface.

Note: If the Device selection is not a switch or router, only one interface will typically be shown.

Sort by: Presents the Interface data either by Average Utilization, Average Errors, or Port/Interface.

View - The lower portion of this screen displays either Utilization or Error information depending on whether Errors or Util is selected.

Note: The Max Errors reported in the graph is a percentage of the total height of the utilization bar (not the % axis). The % axis, seen on the left of the graph, represents the total utilization of a port.



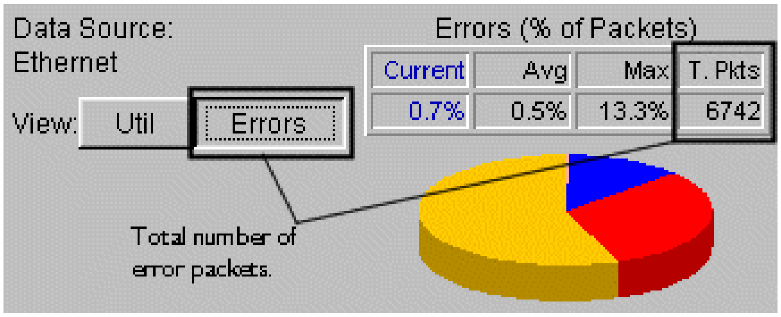
Data Source:
Ethernet

View Util Errors

Utilization (% of Bandwidth)

Current	Avg	Max	T. Pkts
2.7%	5.4%	95.7%	1499K

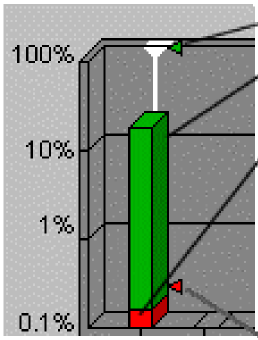
Total number of utilization packets.



Data Source: Ethernet

Current	Avg	Max	T. Pkts
0.7%	0.5%	13.3%	6742

Total number of error packets.



Maximum % utilization.

The green vertical bar shows the current utilization (Good Frames) for a particular port (Interface).

Red in the vertical bar indicates the percentage of errors based on the total size of the vertical bar.

Press the Util button to see the total number of packets (T. Pkts), and press the Errors button to see the total number of error packets (T. Pkts) and error type detail (depends on MIB supported by interface).

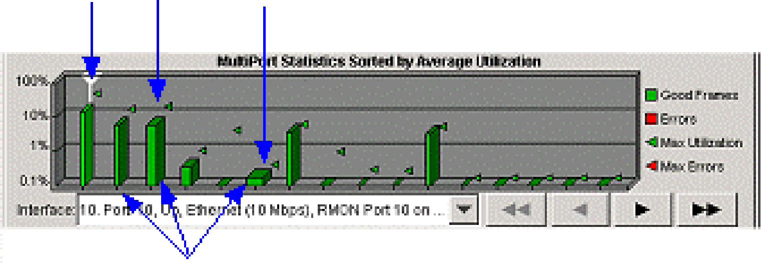
Maximum % errors. Relative to the height of the vertical bar, not the % axis.

White vertical bar is on 10 Mbit port

100 Mbit

10 Mbit

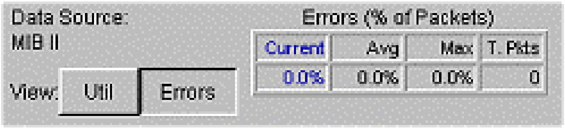
1000 Mbit



MultiPort Statistics Sorted by Average Utilization
100%
10%
1%
0.1%
🟩 Good Frames
🟥 Errors
Max Utilization
Max Errors
Interface: 10. Port 10, Up, Ethernet (10 Mbps), RMON Port 10 on ...

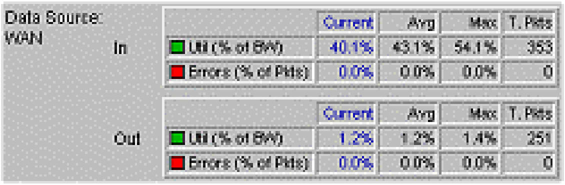
There can be up to three different bar widths, the widest and middle size bars represent the highest port speeds, and the smallest bar represents all other port speeds if more than three exist.

Data Source- Displays device utilization and error information. Depending on the device selected (upper-left of screen), different information is displayed as shown below:



Data Source: MIB II

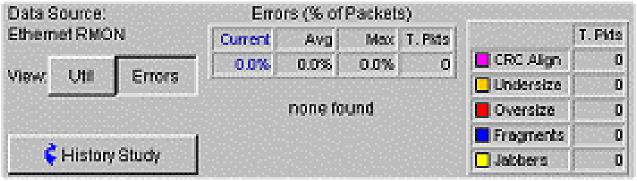
Current	Avg	Max	T. Pkts
0.0%	0.0%	0.0%	0



Data Source:
WAN

In	Current	Avg	Max	T. Pkts
🟩 Util (% of BW)	40.1%	43.1%	54.1%	353
🟥 Errors (% of Pkts)	0.0%	0.0%	0.0%	0

Out	Current	Avg	Max	T. Pkts
🟩 Util (% of BW)	1.2%	1.2%	1.4%	251
🟥 Errors (% of Pkts)	0.0%	0.0%	0.0%	0



Data Source:
Ethernet RMON

Errors (% of Packets)

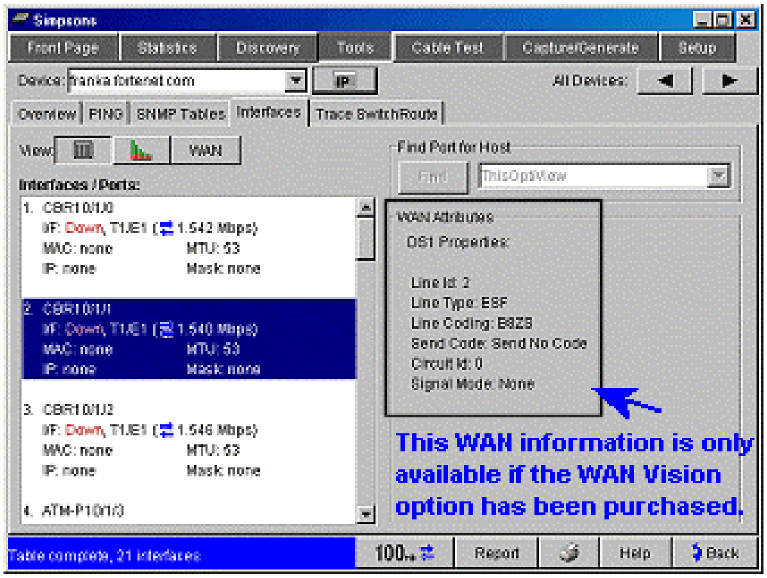
Current	Avg	Max	T. Pkts
0.0%	0.0%	0.0%	0

none found

	T. Pkts
🟪 CRC Align	0
🟨 Undersize	0
🟥 Oversize	0
🟦 Fragments	0
🟨 Jabbers	0

For an Ethernet RMON device, the **History Study** button allows you to view History studies in the **Statistics | Utilization** screen.

Tabular View



Device: franka.fortenet.com

Interfaces / Ports:

1. CBR1 0/1/0
   IF: Down, T1/E1 (1.542 Mbps)
   MAC: none MTU: 53
   IP: none Mask: none
2. CBR1 0/1/1
   IF: Down, T1/E1 (1.540 Mbps)
   MAC: none MTU: 53
   IP: none Mask: none
3. CBR1 0/1/2
   IF: Down, T1/E1 (1.546 Mbps)
   MAC: none MTU: 53
   IP: none Mask: none
4. ATM-P1 0/1/0

ThisOptiView

WAN Attributes

DS1 Properties:

Line Id: 2
Line Type: ESF
Line Coding: B8ZS
Send Code: Send No Code
Circuit Id: 0
Signal Mode: None

This WAN information is only available if the WAN Vision option has been purchased.

Table complete, 21 interfaces

This view presents switch information based on the device selected in the **Device** field (at the top of this screen). Interface/port information on the selected device is displayed on the left side of the screen, and depending on the type of device selected, information is displayed on the right side of screen. If that interface is a port for a switch, the devices in the switch forwarding table is displayed. If it is a WAN interface, technology specific interface configuration information is displayed. The information available is limited to the information available in the MIB.

Interface/Ports - Displays the Interface Table for the selected device in a tabular view.

Find - Available for switches that support 802.1d bridge MIB forwarding database. Locates the port where the host selected in the **Find** list box resides. If **Find** is successful, the right-side of the screen will display Hosts Residing on Port detail.

You may also highlight (press) any interface, and if there are hosts residing on that interface, they will be listed in the Hosts Residing on Port section (to the right of the interface table).

Host Detail- Available if a Find was successful. Opens the Overview screen on the selected host (device).

The Interfaces/Ports list displays the following information:

Ÿ The interface type on the target device
Ÿ Interface description
Ÿ Interface status is Up, Down, Testing, and Dormant
Ÿ Interface Speed
Ÿ Port and Slot number (if applicable for switches)
Ÿ VLAN numbers (for some switches using private MIB support)

- MAC address
- Maximum Transmission Unit (MTU)
- All Interface IP addresses and associated subnet masks

When Duplex Information is available, it is displayed as shown below.

- ⇄- Full Duplex
- ⇄- Half Duplex
- ⇄- Auto Negotiate State

WAN Attributes

The following are displayed in the WAN attributes section of this screen for each WAN type:

DS1 (T1/E1)

Line Id

- Other
- ESF
- D4
- E1
- E1-CRC
- E1-MF
- E1-CRC-MF

Line Coding

- JBZS
- B8ZS
- HDB3
- ZBTSI
- AMI
- Other

Send Coding

- Send No Code
- Send Line Code
- Send Payload Code
- Send Reset Code
- Send QRS
- Send 511 Pattern
- Send 3in24 Pattern
- Send Other Test Pattern

Circuit Id

Signal Mode

- None
- Robbed Bit
- Bit Oriented

- Message Oriented

DS3 (T3)

Line Type

- dsx3other
- dsx3M23
- dsx3SYNTRAN
- dsx3CbitParity
- dsx3ClearChannel
- e3other
- e3Framed
- e3Plcp

Line Coding

- dsx3Other
- dsx3B3ZS
- e3HDB3

Send Code

- Send No Code
- Send Line Code
- Send Payload Code
- Send Reset Code
- Send DS1 Loop Code
- Send Test Pattern

Circuit Id #

Line Length (meters)

SONET (OC-n, SDH-n)

Medium Type

- Sonet
- SDH

Line Coding

- Other
- B3ZS
- CMI
- NRZ
- RZ

Line Type

- Other
- Short Single Mode
- Long Single Mode
- Multi-Mode
- Coax

- UTP

Circuit Id

- STS-1
- STS-3c
- STM-1
- STS-12c
- STM-4
- STS-24c
- STS-48c
- STM-16

ISDN

Bearer Interface labels:

Type

Channel Number

Channel Type

- Dialup
- Leased

Operation Status

- Idle
- Connecting
- Connected
- Active

Info Type

- Unknown
- Speech
- Unrestricted Digital
- Unrestricted Digital56
- Restricted Digital
- Audio 31
- Audio 7
- Video
- Packet Switched

Basic Rate Interface Labels:

Interface Type

- S/T
- U

Line Topology

- Point to Point
- Point to MultiPoint

Interface Mode

- TE
- NT

Signal Mode

- Active
- Inactive

ISDN D (Signaling) Channel Interface Labels:

Type

- Signaling (D) Channel

Signal Index

In Calls

In Connections

Out Calls

Out Connections

ATM

Num Virtual Paths Configured

Num Virtual Circuits Configured

Max Active VPI Bits

Max Active VCI Bits

ILMI VPI

ILMI VCI

Frame Relay

Multicast

Polling Interval

Enquiry Interval

Error Interval

WAN (Wide Area Network view)

Note: A WAN device with MIB support must be selected to see the WAN screen.

Interface: - Selects from a list of available interfaces.

Sort by: - Selects whether the data is displayed in the graph by average utilization, average errors, or by port/interface.

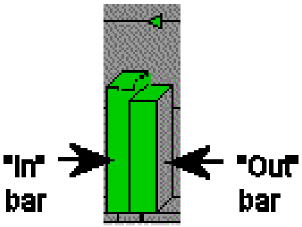
DLCI - -The DataLink Connection Identifier for this virtual circuit. The white vertical bar moves over the selected DLCI and vice versa. All detail on this screen is relative to the DLCI selected.

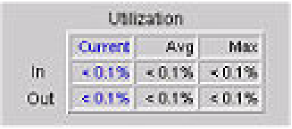
State and Last Time Change - The operational status of this VC and how long it has been in that state.

About the Graph

The height of each bar in the graph represents the current utilization, regardless of the color. The color of the bar (orange, yellow, or red) flags the occurrence of congestion notifications. A blue Max Utilization flag is displayed next to each bar representing the maximum utilization since WAN statistics was selected, or the **Clear Counts** button was pressed.

For most full duplex (FDX) interfaces there will be an “In” (left bar) and “Out” (right Bar) as shown below. The WAN screen displays the labels “In" and "Out”. Additional graphics showing this relationship is displayed in the numeric table on the lower portion of the screen.





Utilization

	Current	Avg	Max
In	< 0.1%	< 0.1%	< 0.1%
Out	< 0.1%	< 0.1%	< 0.1%

If the interface is Ethernet with RMON as the data source, it will be labeled *data source RMON*, and will be shown with one bar (as RMON only has *out-going* octet counters).