White Paper

Ten top problems network techs encounter

Networks today have evolved quickly to include business critical applications and services, relied on heavily by users in the organization. In this environment, network technicians are required to do more than simply add new machines to the network. Often they are called on to troubleshoot more complex issues, thus keeping the network up and running at top speed. This whitepaper discusses ten common problems encountered by technicians today and their symptoms, causes, and resolutions.

Table of contents

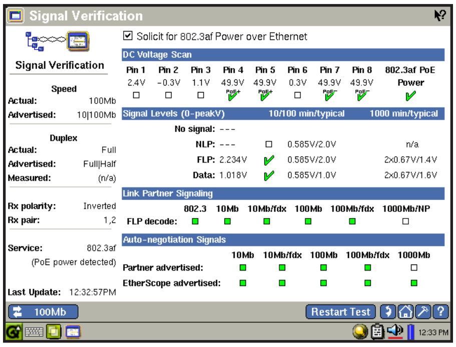
FLUKE networks®

Problem 1 – Dead drop

Symptom: A PC, phone, access point or printer is connected to the wall jack and the connection is not activated. The switch port does not show a link light, nor does the network adapter.

Cause: Dead drops are commonly simple problems that occur when a connection is not patched through to the wall jack. In many organizations, only those connections that are actively being used are patched. When offices or meeting rooms are moved around, sometimes the network jacks are not tested for the new users, or drops that are intentionally left disconnected may not be properly documented. Additionally, the switch port may be administratively disabled.

Resolution: Check to be sure the switch port is activated and that the connection has been properly patched. When any devices have been physically moved in the office, be sure to test the new connections to ensure they are working properly. In the case of an IP Phone, it may also be that power is not being sufficiently supplied to the phone.



Signal Verification

☑ Solicit for 802.3af Power over Ethernet

Speed
Actual: 100Mb
Advertised: 10|100Mb

Duplex
Actual: Full
Advertised: Full|Half
Measured: (n/a)

Rx polarity: Inverted
Rx pair: 1,2

Service: 802.3af
(PoE power detected)

Last Update: 12:32:57PM

DC Voltage Scan

Pin 1	Pin 2	Pin 3	Pin 4	Pin 5	Pin 6	Pin 7	Pin 8	802.3af PoE
2.4V	-0.3V	1.1V	49.9V	49.9V	0.3V	49.9V	49.9V	Power
□	□	□	PoE+ ✓	PoE+ ✓	□	PoE− ✓	PoE− ✓	✓

Signal Levels (0-peakV)			10/100 min/typical	1000 min/typical
No signal:	---			
NLP:	---	□	0.585V/2.0V	n/a
FLP:	2.234V	✓	0.585V/2.0V	2x0.67V/1.4V
Data:	1.018V	✓	0.585V/1.0V	2x0.67V/1.6V

Link Partner Signaling

	802.3	10Mb	10Mb/fdx	100Mb	100Mb/fdx	1000Mb/NP
FLP decode:	🟩	🟩	🟩	🟩	🟩	□

Auto-negotiation Signals

	10Mb	10Mb/fdx	100Mb	100Mb/fdx	1000Mb
Partner advertised:	🟩	🟩	🟩	🟩	□
EtherScope advertised:	🟩	🟩	🟩	🟩	🟩

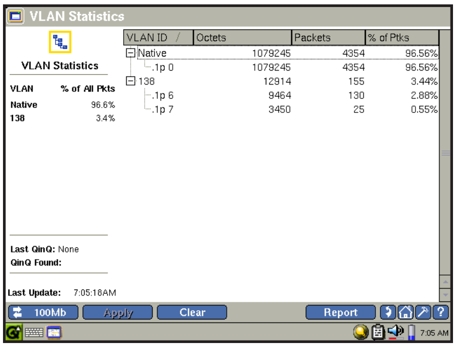
To resolve dead drops, the EtherScope Network Assistant features the Cable Verification test to verify that the network drop is patched to an active device. It also features the Signal Verification test to measure 802.3af PoE voltages by pin.

Problem 2 – Can't get an IP address

Symptom: The network appears down or inoperable. The operating system may alert that an address was not received from the DHCP server. After checking the network adapter status, no address may be configured.

Cause: No address has been received from the DHCP server. The DHCP server may be out of addresses, the server service may be down, the end device may be configured to use a static address instead of a DHCP address, or the DHCP request from the end device never made it to the server in the first place. This may be the case especially if a new device is configured for a VLAN that is not set up to forward DHCP requests to the DHCP server.

Resolution: Key question – is this problem restricted to one user or are many users affected? If only one user is affected, check the NIC settings to be sure it is configured to use DHCP. Next, check the switch to see which VLAN the port is configured as a member. Check that other devices on this VLAN can get addresses. If they cannot, the problem may be that the router is not forwarding DHCP requests to the DHCP server. If many devices across several subnets are having this problem, the problem is likely the server itself. The server may not have the DHCP service running, or it may have run out of addresses to distribute.



VLAN Statistics

VLAN	% of All Pkts
Native	96.6%
138	3.4%

Last QinQ: None
QinQ Found:

Last Update: 7:05:18AM

VLAN ID	Octets	Packets	% of Ptks
⊟ Native	1079245	4354	96.56%
.1p 0	1079245	4354	96.56%
⊟ 138	12914	155	3.44%
.1p 6	9464	130	2.88%
.1p 7	3450	25	0.55%

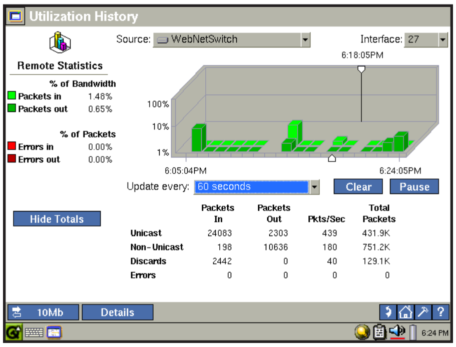
The EtherScope Network Assistant features the VLAN Statistics test for visibility into the VLANs present on the local link. Incorrectly assigned VLAN membership is a frequent cause of not getting an IP address.

Problem 3 – Can't connect to the application server

Symptom: The application the user is trying to open may alert that it cannot connect to the application server. This can be the case when using e-mail applications or CRM Applications. The common complaint into the help desk is that the network is down, even though this is not the true problem.

Cause: Several things can cause this event. The key question to ask the user is whether this problem happens constantly or only sporadically. If the user has a proper IP address for the connection they are on, there may be a routing issue on the network between the user and server. This can be verified with a simple ping. If connectivity is lost sporadically, this can be caused by a busy server that is not responsive to client requests.

Resolution: In the case that routing is not the issue (ping test), check the server load and resources. Is the server busy running another task such as a backup? If this is not the case, check the network load between client and server, focusing on WAN connections if there are any. Often, periods of high network utilization between client and server can cause connectivity problems for the client. The best way to do this is by using an SNMP tool that will monitor utilization over time on these links. Additionally, look for Ethernet Errors on all switches and routers that cause packet loss between client and server.



Source: WebNetSwitch

Interface: 27

	% of Bandwidth
🟩 Packets in	1.48%
🟩 Packets out	0.65%

	% of Packets
🟥 Errors in	0.00%
🟥 Errors out	0.00%

Update every: 60 seconds

	Packets In	Packets Out	Pkts/Sec	Total Packets
Unicast	24083	2303	439	431.9K
Non-Unicast	198	10636	180	751.2K
Discards	2442	0	40	129.1K
Errors	0	0	0	0

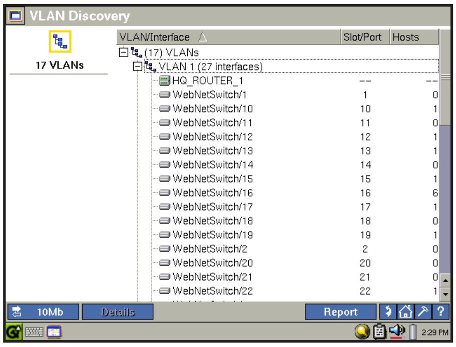
The EtherScope Network Assistant features the SNMP-based Utilization History test to monitor switch port utilization over time. High network utilization can prevent a client from successfully connecting to an application server.

Problem 4 – Incorrect VLAN assignment

Symptom: When installing new services on the network such as wireless or VoIP, VLANs are typically used to isolate this traffic from other users. This requires each switch port supporting these services to be configured for the proper VLAN. If this is not done properly, the service may not work. The IP Phone may not register with the call manager, the PC connected to the phone may not be able to connect to key servers, or the wireless users may not get proper addressing for the wireless environment.

Cause: The switches responsible for connecting these services have not been properly configured. Perhaps it was not communicated within the organization to reconfigure certain ports to support new services.

Resolution: Test the port to verify which VLANs are supported. If possible, use a VLAN Tag to generate VLAN specific traffic to check which VLANs are configured on the port. Check the IP address provided by the DHCP server to determine which VLAN is being provided to the port if it is untagged. Alternatively, check the switch configuration to validate the VLAN configuration.



VLAN/Interface	Slot/Port	Hosts
(17) VLANs		
VLAN 1 (27 interfaces)		
HQ_ROUTER_1	--	--
WebNetSwitch/1	1	0
WebNetSwitch/10	10	1
WebNetSwitch/11	11	0
WebNetSwitch/12	12	1
WebNetSwitch/13	13	1
WebNetSwitch/14	14	0
WebNetSwitch/15	15	1
WebNetSwitch/16	16	6
WebNetSwitch/17	17	1
WebNetSwitch/18	18	0
WebNetSwitch/19	19	1
WebNetSwitch/2	2	0
WebNetSwitch/20	20	0
WebNetSwitch/21	21	0
WebNetSwitch/22	22	1

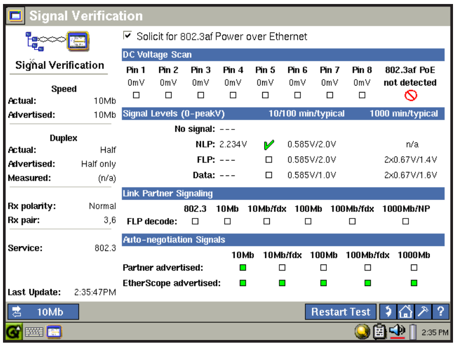
The EtherScope Network Assistant features the VLAN Discovery test to validate switch interface configurations and troubleshoot VLAN assignment issues.

Problem 5 – Duplex mismatch

Symptom: With a duplex mismatch, the connection will work, just poorly. The link lights will become active on both the switch and network adapter. Network performance will suffer greatly, with throughput dropping to 100Kbps or lower.

Cause: One side of the connection is operating in full duplex (transmit and receive at the same time) and the other device is operating in half duplex (transmit OR receive at one time). The full duplex side does not have to wait to transmit, it is configured to transmit whether it is receiving or not. The half duplex side must wait until it is not receiving in order to transmit. This means that the full duplex side has the potential to interrupt the half duplex side, causing the half duplex side to abort transmission. If transmission is aborted, the frame will need to be retransmitted. This will dramatically reduce the bandwidth the half duplex side is able to make use of.

Resolution: In nearly all cases, a duplex mismatch is the result of forcing one side of the connection (usually the switch) to full duplex, while leaving the other side, the PC, to auto-negotiate the link. The myth is that auto-negotiation will determine the forced full setting and match this configuration. This however is not the case. The side forced to full duplex is no longer sending the appropriate signaling that auto-negotiation relies on in order to determine speed and duplex. The auto-negotiating side of the connection will be left to guess at the duplex of the link. When in doubt, auto-negotiation will always default to half duplex. This is how most duplex mismatch issues happen on the network. To resolve this, set all connections on the network to auto-negotiate – unless you have reason not to. In these isolated cases, such as inter-switch connections, be sure to statically set both sides to full duplex.



Signal Verification

☑ Solicit for 802.3af Power over Ethernet

Speed
Actual: 10Mb
Advertised: 10Mb

Duplex
Actual: Half
Advertised: Half only
Measured: (n/a)

Rx polarity: Normal
Rx pair: 3,6

Service: 802.3

Last Update: 2:35:47PM

10Mb

DC Voltage Scan

Pin 1	Pin 2	Pin 3	Pin 4	Pin 5	Pin 6	Pin 7	Pin 8	802.3af PoE
0mV	0mV	0mV	0mV	0mV	0mV	0mV	0mV	not detected
□	□	□	□	□	□	□	□	⃠

Signal Levels (0-peakV)			10/100 min/typical	1000 min/typical
No signal:	---			
NLP:	2.234V	✓	0.585V/2.0V	n/a
FLP:	---	□	0.585V/2.0V	2x0.67V/1.4V
Data:	---	□	0.585V/1.0V	2x0.67V/1.6V

Link Partner Signaling

	802.3	10Mb	10Mb/fdx	100Mb	100Mb/fdx	1000Mb/NP
FLP decode:	□	□	□	□	□	□

Auto-negotiation Signals

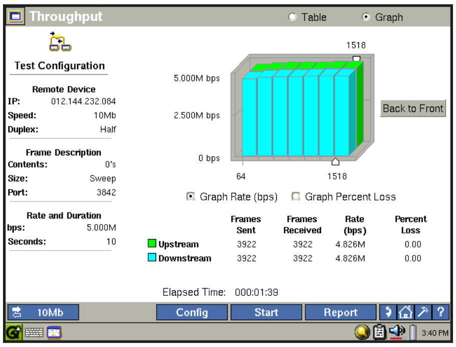
	10Mb	10Mb/fdx	100Mb	100Mb/fdx	1000Mb
Partner advertised:	🟩	□	□	□	□
EtherScope advertised:	🟩	🟩	🟩	🟩	🟩

The EtherScope Network Assistant features the Signal Verification test to monitor the negotiation process and resolve duplex mismatch problems.

Problem 6 – Slow application performance

Symptom: The application appears sluggish. It may freeze on a certain screen or halt while accessing data. Often, the network is blamed for these issues.

Cause: Exonerating the network in application performance problems can assist server maintenance personnel to take out the guesswork and isolate the issue to the right place. Many issues can cause an application to slow down. Among the most common causes are server backups occurring during production hours, slow response from database servers, and packet loss on the network. From a network technician's point of view, the most important thing to determine is whether the problem is caused by the server or by the network. To determine this, a capture of application traffic can be collected from a client machine. Look for any retransmissions between the client and server. If retransmissions exist, there is packet loss on the network, which severely affects application performance. If there are no retransmissions and connectivity between client and server is established, the problem is likely in the server and can be monitored from that perspective.



Test Configuration

Remote Device
IP: 012.144.232.084
Speed: 10Mb
Duplex: Half

Frame Description
Contents: 0's
Size: Sweep
Port: 3842

Rate and Duration
bps: 5.000M
Seconds: 10

10Mb

● Graph Rate (bps) ○ Graph Percent Loss

	Frames Sent	Frames Received	Rate (bps)	Percent Loss
🟩 Upstream	3922	3922	4.826M	0.00
🟦 Downstream	3922	3922	4.826M	0.00

Elapsed Time: 000:01:39

The EtherScope Network Assistant features the Throughput Test to measure network speed and assess whether the network is truly slow. The network is often incorrectly blamed for slow application performance.

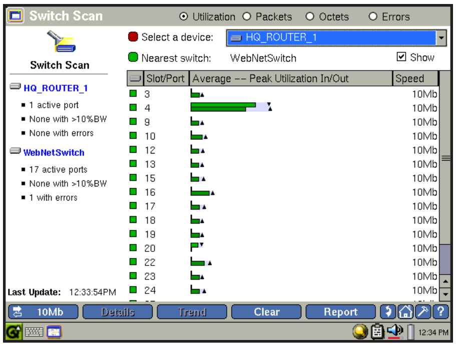
Resolution: Although packet analyzers can be very difficult to use when tracking down a problem, they often are equipped with simple counters displaying TCP retransmissions. Use this counter to assist in determining if there is packet loss on the network between client and server. Look for Ethernet errors (FCS Errors, Alignment Errors, or Late Collisions) on any switches and routers between client and server that could be causing this packet loss. If there are no errors, watch for packet loss on the WAN because of excessive utilization across the link.

Problem 7 – Printing problems

Symptom: Printing does not consistently work on the network. A printer may appear available, but print jobs that are sent to it are not completed.

Cause: Determine if only one user is experiencing this problem or if several people have the same issue. If only one user is having the issue, it may be that the PC is not mapped correctly to the print server. If this is not the cause, the network between client and printer may be to blame. Packet loss can cause printing problems, as well as network connectivity problems on the printer itself.

Resolution: Check the printer configuration to make sure it has a good IP address and can access the print server if it is external to the printer. At times, updating the printer driver has resolved printing issues. Overall, be sure that traffic is getting to and from the printer on the network and that all printer drivers are up to date.



● Utilization ○ Packets ○ Octets ○ Errors

Select a device: HQ_ROUTER_1

Nearest switch: WebNetSwitch ☑ Show

HQ_ROUTER_1
- 1 active port
- None with >10%BW
- None with errors

WebNetSwitch
- 17 active ports
- None with >10%BW
- 1 with errors

Last Update: 12:33:54PM

Slot/Port	Average –– Peak Utilization In/Out	Speed
3		10Mb
4		10Mb
9		10Mb
10		10Mb
12		10Mb
13		10Mb
15		10Mb
16		10Mb
17		10Mb
18		10Mb
19		10Mb
20		10Mb
22		10Mb
23		10Mb
24		10Mb

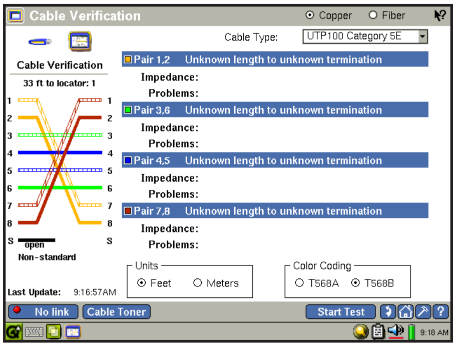
The EtherScope Network Assistant features the Switch Scan test for verifying traffic to and from a problematic printer by monitoring the activity on the switch port where the printer is connected.

Problem 8 – Poor or bad cable

Symptom: If the client PC is able to link to the network, performance may be poor. The PC may not be able to connect at all.

Cause: In networks today, Gigabit to the desktop is common. Gigabit requires four pairs of cable, so anything lower than Category 5 will not work for Gig. In older buildings this must be taken into consideration. In addition, any amount of untwisting of the cable (often near the RJ-45 termination or patch panel) can cause signal loss. This will result in FCS Errors on the switch ports or network adapters.

Resolution: In most cases with cable problems, the cable simply needs to be replaced. If the problem is because the cable has become untwisted, re-terminating the cable may resolve the errors. When supporting new technologies such as Gigabit or Power over Ethernet, the cable must be Cat 5 or better.



● Copper ○ Fiber

Cable Type: UTP100 Category 5E

33 ft to locator: 1

Pair 1,2 Unknown length to unknown termination
Impedance:
Problems:

Pair 3,6 Unknown length to unknown termination
Impedance:
Problems:

Pair 4,5 Unknown length to unknown termination
Impedance:
Problems:

Pair 7,8 Unknown length to unknown termination
Impedance:
Problems:

Units: ● Feet ○ Meters

Color Coding: ○ T568A ● T568B

Last Update: 9:16:57AM

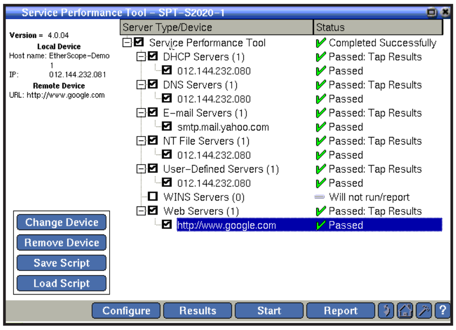
The EtherScope Network Assistant features the Cable Verification test to measure cable characteristics and identify physical layer problems like bad cables.

Problem 9 – DNS problems

Symptom: The user cannot access the internet or key applications. The network appears to be down.

Cause: Domain Name Services may be to blame. The client PC cannot resolve the name of the server with the IP address of that server, so it will not send a connection request. This is often caused by having the wrong DNS server configured on the client, sending DNS requests that the server does not have in its database, or packet loss on the network. DNS is a UDP-based protocol, so packets that are lost will not be retransmitted, causing DNS to fail.

Resolution: Check the client configuration to see which DNS server it is setup to use. If this is the wrong server, adjust this setting in the client or in the DHCP server which provided it. Test the DNS server from the client connection repeatedly to determine if there is delay in response due to packet loss. If packets are lost, look for Ethernet errors between the client and server. Capture failing DNS requests to determine if there is any response at all from the server. Ideally, setup a tool that will constantly test the DNS server and alert when a problem occurs.



Version = 4.0.04
Local Device
Host name: EtherScope–Demo
1
IP: 012.144.232.081
Remote Device
URL: http://www.google.com

Server Type/Device	Status
☑ Service Performance Tool	✓ Completed Successfully
☑ DHCP Servers (1)	✓ Passed: Tap Results
☑ 012.144.232.080	✓ Passed
☑ DNS Servers (1)	✓ Passed: Tap Results
☑ 012.144.232.080	✓ Passed
☑ E–mail Servers (1)	✓ Passed: Tap Results
☑ smtp.mail.yahoo.com	✓ Passed
☑ NT File Servers (1)	✓ Passed: Tap Results
☑ 012.144.232.080	✓ Passed
☑ User–Defined Servers (1)	✓ Passed: Tap Results
☑ 012.144.232.080	✓ Passed
□ WINS Servers (0)	Will not run/report
☑ Web Servers (1)	✓ Passed: Tap Results
☑ http://www.google.com	✓ Passed

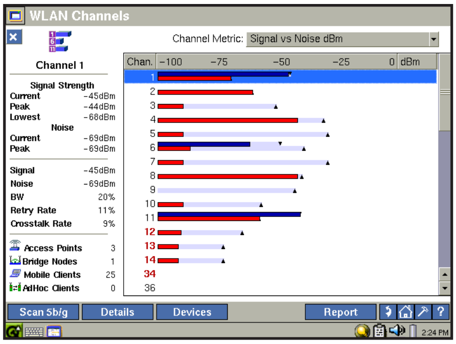
To resolve DNS problems, the EtherScope Network Assistant features the Service Performance Tool to test the availability and responsiveness of key network services like DNS and DHCP.

Problem 10 – Wireless client can't connect

Symptom: The client can detect the wireless access point, but it cannot connect to the wireless network.

Cause: Security credentials, wireless channel interference, and dead spots can cause this problem. Since wireless is invisible, it can be very difficult to track these problems down without a proper wireless tool.

Resolution: Using a wireless monitoring tool measure the signal strength from the affected area, and if possible, conduct a site survey in the area to look for rogue or unknown APs. These may be configured for overlapping wireless channels and can affect known-good users. Check for noise in the signal from surrounding access points or from noise inducing devices such as microwaves and cordless phones. Monitor the client as it attempts to connect to the access point and watch for which step fails – association, authentication, or authorization.



WLAN Channels

Channel Metric: Signal vs Noise dBm

Channel 1

Signal Strength

Current	-45dBm
Peak	-44dBm
Lowest	-68dBm

Noise

Current	-69dBm
Peak	-69dBm

Signal	-45dBm
Noise	-69dBm
BW	20%
Retry Rate	11%
Crosstalk Rate	9%

Access Points	3
Bridge Nodes	1
Mobile Clients	25
AdHoc Clients	0

The EtherScope Network Assistant is a full-featured WLAN analyzer featuring the Channels test for measurement of signal and noise and Security Scan for detecting rogue access points. These tests assist in troubleshooting WLAN connectivity problems.

Summary

We just reviewed 10 of the most common issues encountered on today's networks by technicians. In many cases, the problem can be narrowed down to one or two things and then resolved. Be sure to document the resolution of common problems on the network so other technicians can quickly resolve issues as well. With the right tools, problems can be isolated and resolved quickly, returning the network to top-notch performance in no time.

Troubleshoot networks 15 times faster

The EtherScope Network Assistant significantly reduces the amount of time IT organizations spend troubleshooting networks problems – resulting in annual savings of over $20,000 for many companies. The EtherScope analyzer achieves this savings through numerous breakthrough capabilities:

- Physical layer troubleshooting: the EtherScope analyzer utilizes special hardware for twisted pair and fiber optic physical layer testing not available on a laptop PC.
- Switch visibility: the EtherScope analyzer utilizes proprietary SNMP-based algorithms to pull the most relevant configuration information and performance statistics from LAN switches.
- Network discovery: the EtherScope analyzer utilizes proprietary passive and active discovery algorithms to provide a picture of what is on the network and where it can be found.
- Performance assessment: the EtherScope analyzer can perform hardware-based, dual-ended tests to measure actual Ethernet link performance attributes at rates up to 1 Gig.
- Integrated WLAN analysis: the EtherScope analyzer features wireless LAN analysis in the same tester for comprehensive testing of 802.11 networks.
- Reduced problem escalation: the EtherScope analyzer's menu-driven touch-screen interface is simple enough that technicians can solve complex problems themselves.

To learn more about the EtherScope Network Assistant, visit **www.flukenetworks.com/etherscope**. Take advantage of our free 5-day trial (we'll send you an EtherScope Analyzer to use on your own network for five days at no charge), or you can take EtherScope for a virtual test drive and enter to win one.

Contact Fluke Networks: Phone **800-283-5853** (US/Canada) or **425-446-4519** (other locations). **Email: info@flukenetworks.com**.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 2/2009 3450201 H-ENG-N Rev A