

Select Traffic Capture™

Protocol analysis tracking at every location

Benefits

- Improve application availability by getting quickly to the source of problems
- Capture traffic at any location via a Web-based interface
- Save time by filtering data using a capability that matches the levels of top-end protocol analyzers
- Save money by not having to buy expensive portable test gear or dispatch technicians to remote sites
- Buy now or add later as part of the Visual UpTime™ Select® network and application performance management system

Get to the source of difficult problems. The Visual UpTime® Select™ Traffic Capture™ software module gives you a full-function protocol analyzer at every location in your network. Trace, filter and decode the most common network protocols and gain in-depth visibility into subtle problems, such as protocol violations, incorrect configurations and timeouts.

In addition to protocol decoding, Select Traffic Capture includes is available for every Analysis Service Element (ASE) in your network with the point and click of a mouse.

Packet capture and protocol decode

The screenshot shows the 'Traffic Capture' tab in the Visual UpTime Select interface. It displays a table of captured packets and a detailed view of a selected packet.

From	Time	Length	Source	Destination	Protocol	Summary
<input type="radio"/> User	16:40:48.096	68	172.16.20.109	10.31.0.24	TCP	1260 -> 1200 (ACK, PSH)
<input type="radio"/> User	16:40:48.118	630	208.22.47.86	172.16.21.62	HTTP	GET /WebApplicationClient/TrafficCapture
<input checked="" type="radio"/> User	16:40:48.120	177	172.16.21.62	172.16.21.6	SNMP	getRequest
<input type="radio"/> User	16:40:48.120	184	172.16.21.6	172.16.21.62	SNMP	getResponse
<input type="radio"/> User	16:40:48.124	68	10.31.0.24	172.16.20.109	TCP	1200 -> 1260 (ACK, PSH)
<input type="radio"/> User	16:40:48.125	68	172.16.20.109	10.31.0.24	TCP	1260 -> 1200 (ACK, PSH)

Detail Decode	Hex Decode
Packet Number: 86	00: 00 a0 0e 37 2b e7 00 06 ...7+...
Frame source: (User)	08: 5b ee b7 81 ee 00 01 f4 [...]
Length: 177	10: 08 00 45 00 00 9b a0 e4 ..E.....
Time: 01/04/06 16:40:48.120 Eastern Standard Time	18: 00 00 80 11 17 09 ac 10
ETHERNET	20: 15 3e ac 10 15 06 09 64 ->.....d
IEEE 802.1Q Virtual LAN (VLAN)	28: 00 ag 00 87 ef 9f 30 82
Internet Protocol (IP)	30: 00 7b 02 01 00 04 07 70 -{....p
User Datagram Protocol (UDP)	38: 72 69 76 61 74 65 a0 6d rivate.m
getRequest	40: 02 02 1a g9 02 01 00 02
Request ID: 6905	48: 01 00 30 82 00 5f 30 82 ..._..0.
Error Status: OK	50: 00 0f 06 0b 2b 06 01 02

Select Traffic Capture gives you the filtering power you need to get to the heart of the problem without ever leaving your desk. "Plain English" decoding makes it easy to see protocol flows across the applications infrastructure so you can quickly uncover the source of performance issues.

Get the detail you need – securely

Select Traffic Capture details decodes on all layers of the protocol stack – exploding the protocol headers – but skips the packet payload to enhance security. Each protocol header is broken out in its own layer with “plain English” decodes of protocol flows.

Manage most every protocol

The system supports more than 90 of the most common protocols, including Voice over IP (VoIP) protocols such as SIP and H.323 and multiple LMI signaling protocol variants. You can also decode both frame relay and ATM-based packet streams.

Save time with pre-capture filtering

Determine exactly which packets to capture and which to ignore according to criteria you set to get directly to problem symptoms without flooding the screen with irrelevant packets. Filter packets to and from specific DLCIs, IP addresses or subnets. Track specific TCP or UDP ports and other aspects across the protocol header at multiple layers. Apply multiple simultaneous filters with flexible bit-level logic to look for multiple trigger events.

Address trouble with post-capture filtering

When a problem’s cause isn’t clear, run the trace without filters. Then zoom-in on the problem by filtering captured packets and displaying them according to criteria you set based on your hypothesis of the problem’s cause.

Once you’ve captured the traffic trace, you can store it in a common format for further analysis or for consolidation with traces from other analyzers.

Portable analyzer functionality remotely

More enterprises have protocol analyzers at a headquarters locations, but do not have the same tools available for remote site because of the cost of deployment and the lack of IT staff at these locations.

Select Traffic Capture does packet capture and protocol decode at every site in your network – all with a point and click of a mouse. Now you can rapidly identify the source of sudden traffic bursts that are negatively impacting a small circuit at a remote location or you can identify which users might be infected with a virus.

For global enterprises, a language barrier and non-integrated toolsets can compound problems. The solution also delivers identical views of performance whether the location is domestic or international.

NETWORK SUPERVISION

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.

©2006 Fluke Corporation. All rights reserved.
Printed in U.S.A. 6/2006 2671224 D-ENG-N Rev A