

PacketTrap IT

Capture the state of your network

Get PacketTrap IT on ALL your network devices

PacketTrap supports industry standard traffic analysis protocols NetFlow®, sFlow® and J-Flow, however over 80% of routers and switches on the market do not support one of these standards. This means the traffic traversing your network can't be viewed at a granular level. PacketTrap is the only solution on the market to solve this problem, and it's done with ptFlow, PacketTrap's own packet capturing which provides a granular inspection of data as it traverses your network.

NETWORK TRAFFIC ANALYSIS MODULE

You can't evaluate the health of your network without traffic flow monitoring and analysis. PacketTrap IT's Network Traffic Analysis module provides unparalleled visibility into traffic network patterns and usage. The functionality plugs directly into the PacketTrap dashboard so traffic data can be monitored, alerts can be triggered, issues can be remediated and reports generated along with all the data collected by SNMP and WMI.

KEY FEATURES AND BENEFITS



EASY TO INSTALL AND USE

Network Traffic analysis integrates seamlessly with PacketTrap and can be up and running in 10 minutes. All data and reports are viewed through the customizable dashboard so traffic data can be viewed along with other network data.



MONITOR ALL YOUR DEVICES

Capture traffic data for any network device that supports NetFlow, J-Flow or sFlow. For devices that do not support these standards, ptFlow technology provides granular data from any router or switch on the network. Install a ptFlow agent for data from servers on the network.



FIRST LINE OF DEFENSE

Network Traffic Analysis detects abnormal network activity as it occurs, such as when applications are hogging too much bandwidth or when an end user is consuming excessive bandwidth. Problems can be quickly stopped in real time to limit the productivity impact on users.



DON'T LET APPLICATIONS AFFECT THE BOTTOM LINE

Application performance immediately affects productivity. Network Traffic can identify which applications are active on the network and provide usage statistics in the form of charts and graphs on those applications

SUPPORTED NETWORK DEVICES

- Cisco NetFlow v1, 3, 5, 7 and 9
- Juniper J-Flow
- sFlow
- ptFlow technology monitors traffic from any other network devices that do not support the above standards
- Traffic to and from servers can be monitored by an installed ptFlow agent

LICENSING

PacketTrap's Network Traffic Analysis module is licensed as an optional module and is based on the number of network devices to be monitored.

MONITOR

- Monitor traffic for any device on the network—routers, switches, servers
- Supports Cisco® NetFlow v1, 3, 5, 7 and 9, Juniper J-Flow, and sFlow
- For devices that do not support the standards above, ptFlow technology is used to capture all packets on the network

ALERT

- Alerts for traffic conditions can be integrated with alerts based on SNMP and WMI data
- Qualified alerts across all networked devices
- Configure alerts for related events or conditions
- Configure alerts for traffic load
- Automatically escalate unresolved issues

REMEDiate

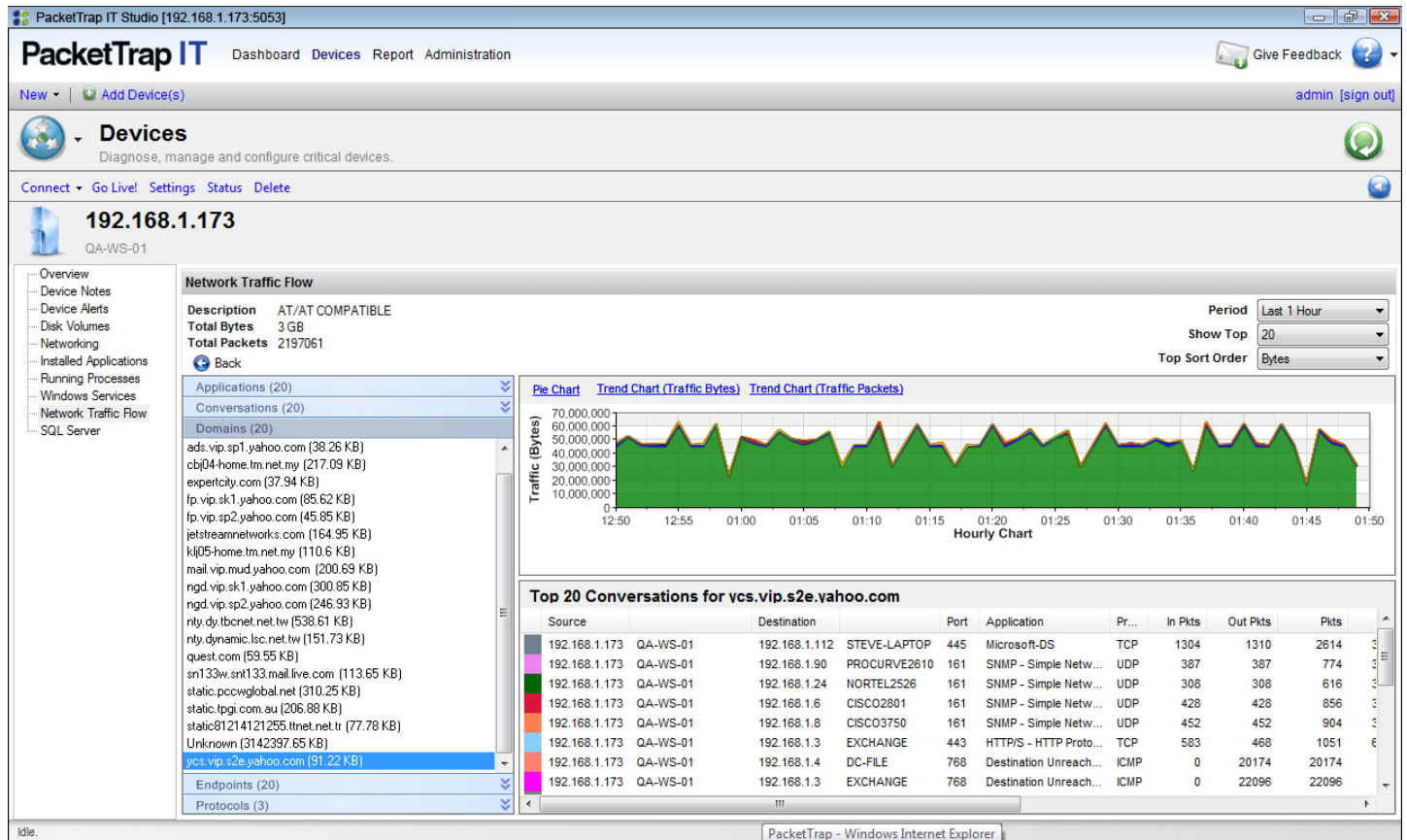
- See traffic from the perspective of each device for easier troubleshooting
- Pinpoint exactly who or what is causing traffic congestion on your network

REPORT

- View applications, conversations, devices, endpoints, and protocols
- Generate reports for all collected traffic data
- All reports can be printed, emailed and saved
- Schedule automatic reports

PLAN

- Traffic Flow Analysis provides historical trends for all flows for network capacity planning
- Identify usage for different traffic types and plan for future needs



PacketTrap IT Studio [192.168.1.173:5053]

PacketTrap IT Dashboard Devices Report Administration

New | Add Device(s) admin [sign out]

Devices
Diagnose, manage and configure critical devices.

Connect ▾ Go Live! Settings Status Delete

192.168.1.173
QA-WS-01

Network Traffic Flow

Description AT/AT COMPATIBLE
Total Bytes 3 GB
Total Packets 2197061
Back

Period Last 1 Hour
Show Top 20
Top Sort Order Bytes

Applications (20)
Conversations (20)
Domains (20)

ads.vip.sp1.yahoo.com (38.26 KB)
cbj04-home.tn.net.ny (217.09 KB)
expertcity.com (37.94 KB)
fp.vip.sk1.yahoo.com (85.62 KB)
fp.vip.sp2.yahoo.com (45.85 KB)
jetstreamnetworks.com (164.95 KB)
kj05-home.tn.net.ny (110.6 KB)
mail.vip.mud.yahoo.com (200.69 KB)
ngd.vip.sk1.yahoo.com (300.85 KB)
ngd.vip.sp2.yahoo.com (246.93 KB)
nly.dy.tbcnet.net.tw (538.61 KB)
nly.dynamic.lsc.net.tw (151.73 KB)
quest.com (59.55 KB)
sn133w.snt133.mail.live.com (113.65 KB)
static.pccwglobal.net (310.25 KB)
static.tpgi.com.au (206.88 KB)
static81214121255.tinet.net.tr (77.78 KB)
Unknown (3142397.65 KB)
yca.vip.s2e.yahoo.com (91.22 KB)

Endpoints (20)
Protocols (3)

Hourly Chart

Traffic (Bytes) vs Time (12:50 to 01:50)

Top 20 Conversations for yca.vip.s2e.yahoo.com

Source	Destination	Port	Application	Pr...	In Pkts	Out Pkts	Pkts		
192.168.1.173	QA-WS-01	192.168.1.112	STEVE-LAPTOP	445	Microsoft-DS	TCP	1304	1310	2614
192.168.1.173	QA-WS-01	192.168.1.90	PROCURVE2610	161	SNMP - Simple Netw...	UDP	387	387	774
192.168.1.173	QA-WS-01	192.168.1.24	NORTEL2526	161	SNMP - Simple Netw...	UDP	308	308	616
192.168.1.173	QA-WS-01	192.168.1.6	CISCO2801	161	SNMP - Simple Netw...	UDP	428	428	856
192.168.1.173	QA-WS-01	192.168.1.8	CISCO3750	161	SNMP - Simple Netw...	UDP	452	452	904
192.168.1.173	QA-WS-01	192.168.1.3	EXCHANGE	443	HTTP/S - HTTP Proto...	TCP	583	468	1051
192.168.1.173	QA-WS-01	192.168.1.4	DC-FILE	768	Destination Unreach...	ICMP	0	20174	20174
192.168.1.173	QA-WS-01	192.168.1.3	EXCHANGE	768	Destination Unreach...	ICMP	0	22096	22096