ManageEngine
Powering IT ahead

NetFlow – The De Facto Standard for Traffic Analytics

A Webinar on NetFlow and its uses in Enterprise Networks for Bandwidth and Traffic Analytics

Don Thomas Jacob
Technical Marketing Engineer
ManageEngine NetFlow Analyzer

ZOHO

About ManageEngine

ManageEngine

Network	Servers & Applications	Desktop	ServiceDesk	Windows Infrastructure	Event Log & Compliance	Security
Network Monitoring	Server Monitoring	Desktop Management	Helpdesk	Active Directory	Windows Event Logs	Vulnerability Analysis
NetFlow Analysis	Application Perf Monitoring	Asset Management	ITIL Service Desk	SQL Server	Syslog Management	Patch Management
Network Config Mgmt	End User Experience	Remote Control	Software License Tracking	Exchange Server	Firewall Log Analyzer	Password Management

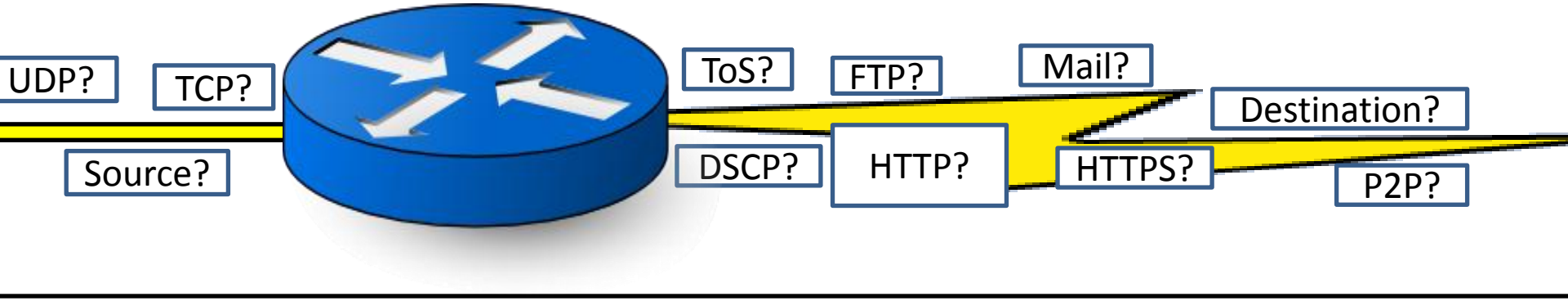
ManageEngine is an IT management vendor focused on bringing a complete IT management portfolio to all types of enterprises

Today's Discussion

- The need for bandwidth monitoring and traffic analytics
- What is NetFlow
- Flexible NetFlow
- Supported Devices
- Use cases
- SNMP, Packet Sniffing or NetFlow
- Questions?

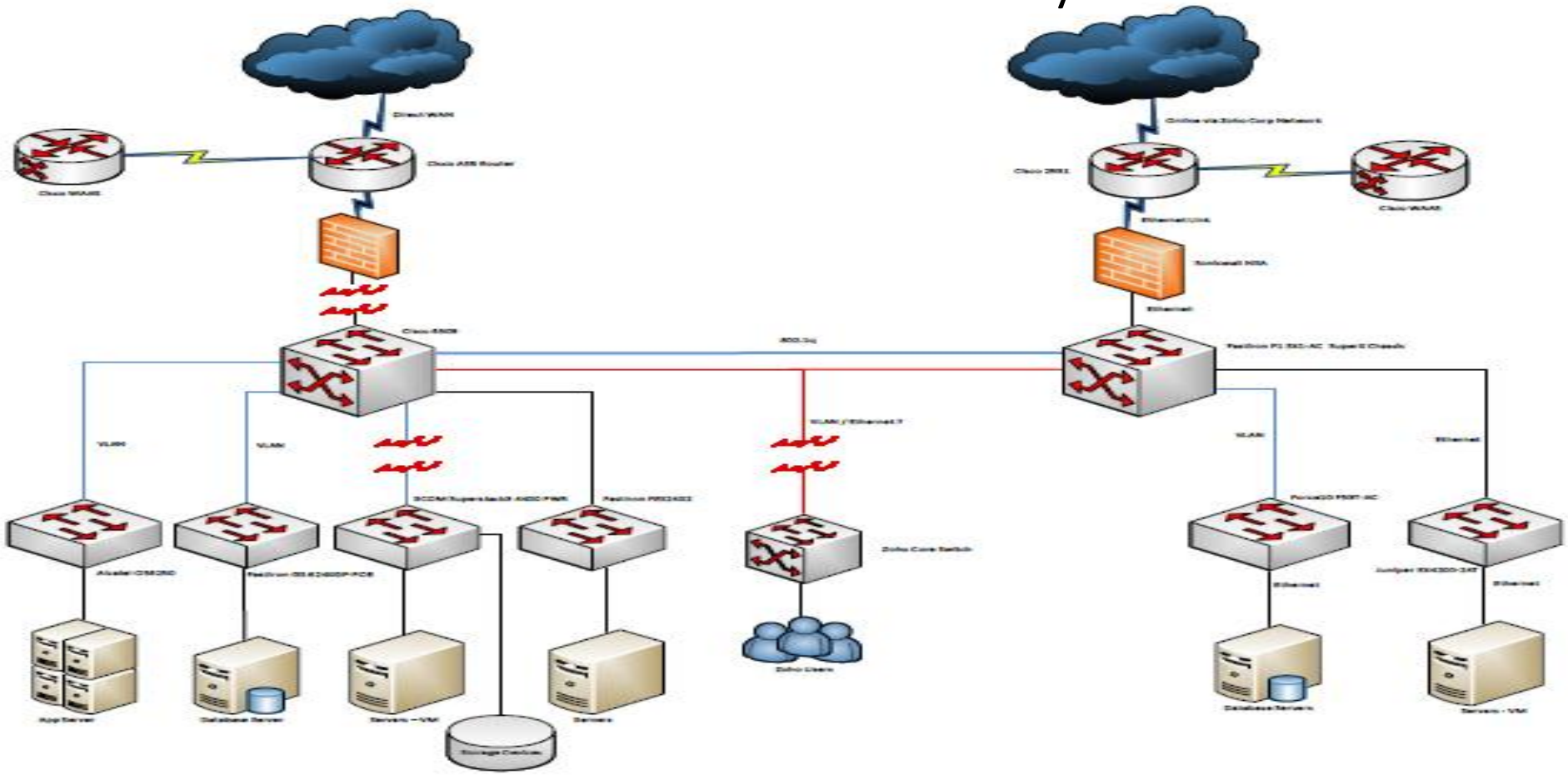
What is Happening

- Profile your network
- Who are the 'Top Talkers'
- Understand application usage patterns
- Protocol distribution
- Performance of QoS policies



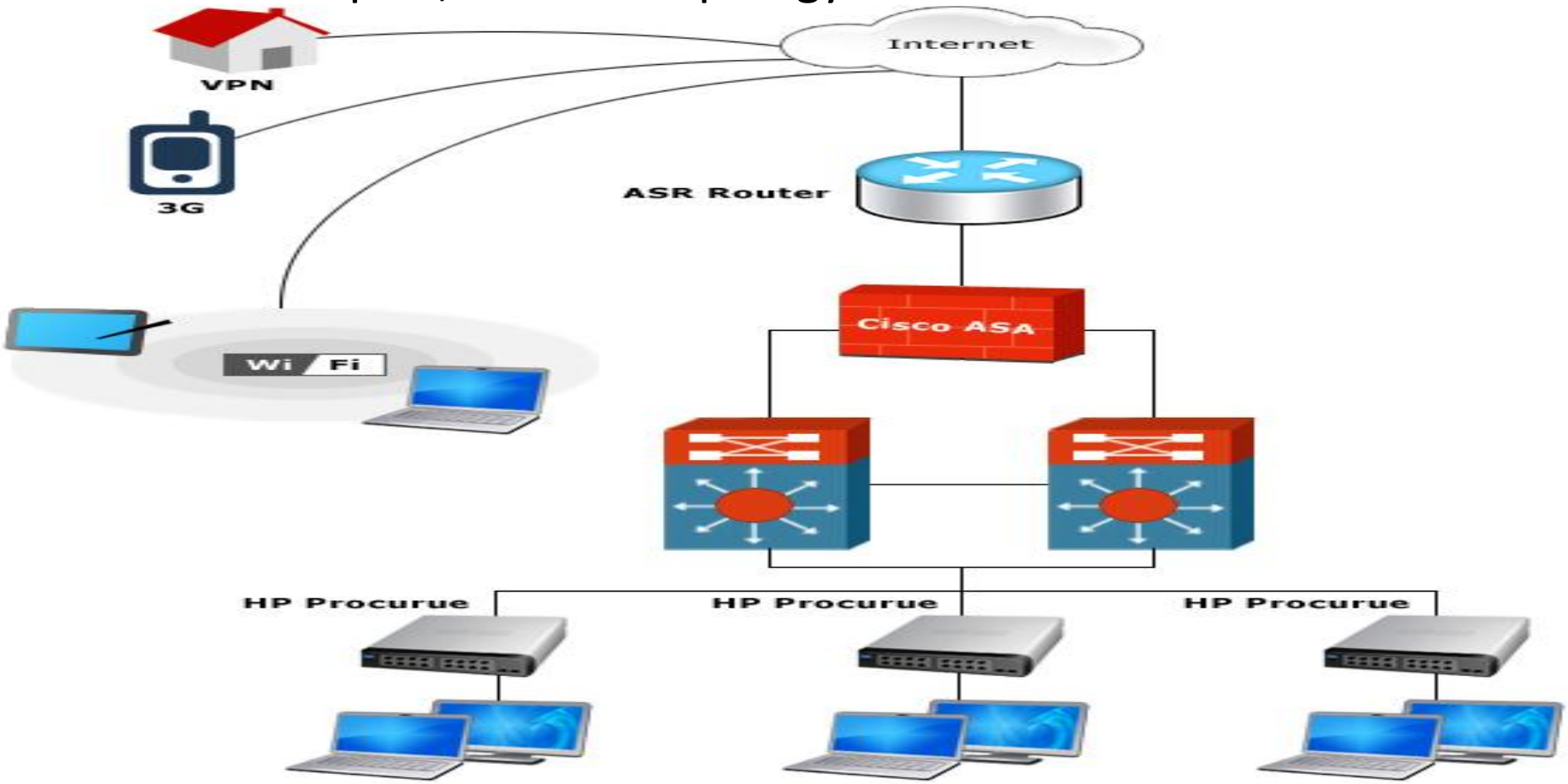
Quicker Troubleshooting

- Drill down to traffic spikes or bottlenecks on leased line
- Find root cause of Internet and application slowness
- Real time voice and video traffic analysis



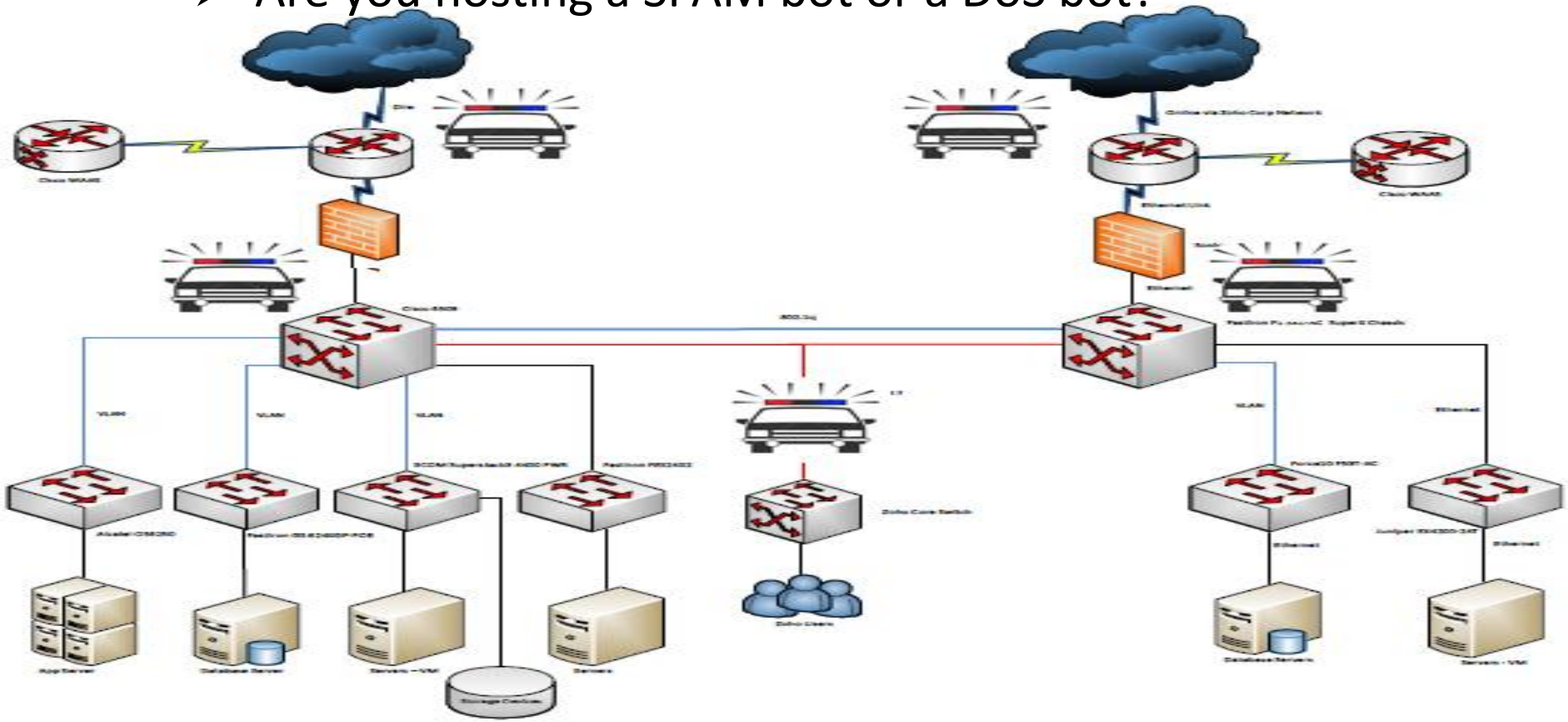
Bigger, Faster and Complex Networks

- Erosion of network perimeter: Telecommuting
- Faster networks: 1G, 10G, 40G and now 100G
- Complex, meshed topology



Network Security

- Increasing BYOD trend and telecommuting
- Remember the 2011 network attacks?
- Zero day malware goes undetected by IDS and IPS
- Are you hosting a SPAM bot or a DoS bot?



Capacity Planning and Cost Savings

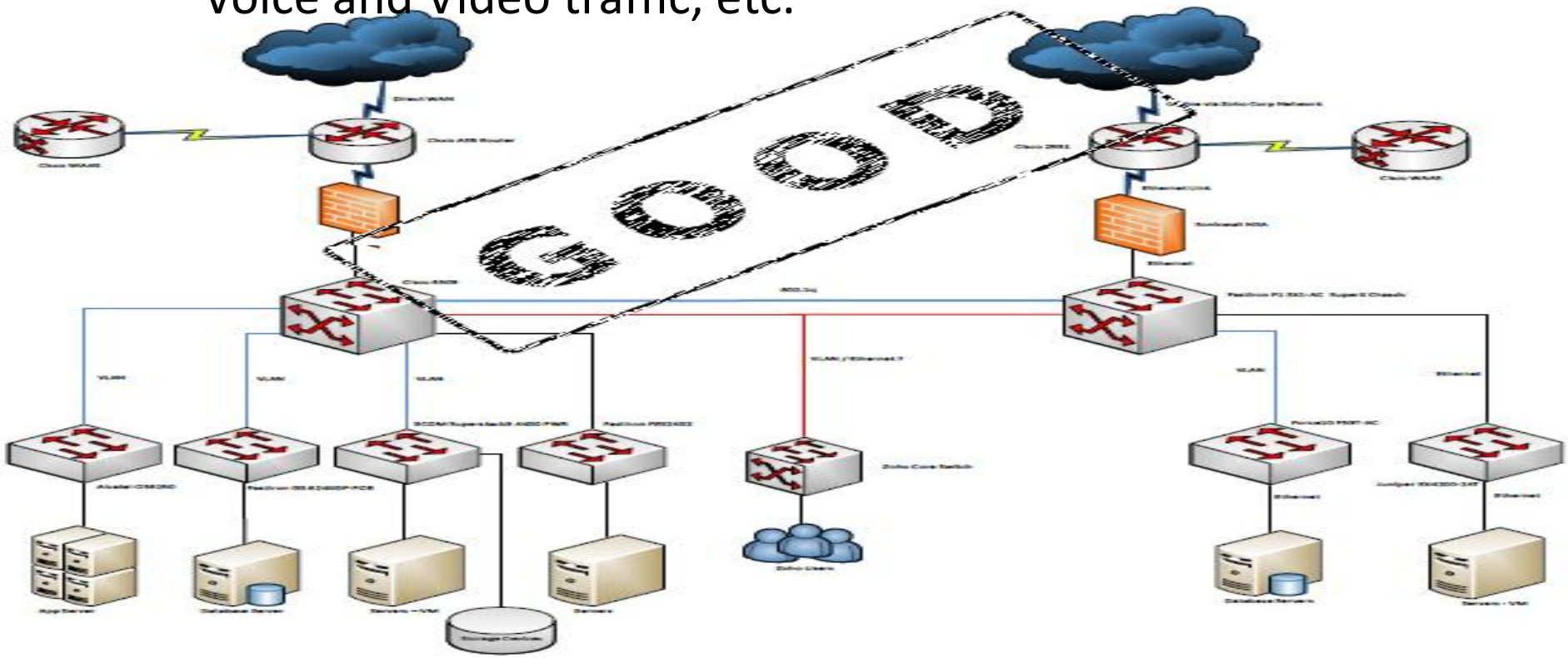
- Is a bandwidth upgrade necessary?
- How much is social media traffic usage?
- Identify congestion causing applications
- Save cost with informed decisions

SLA Verification and Usage based Billing

- ISP meeting Committed Data Rate (CDR)?
- Validate ISP's SLA reports with your custom reports
- Usage data and info for billing / chargeback

Create a high performing network

- Ensure optimal bandwidth usage
- Effect of network changes and new applications
- Validate QoS policies
- Performance of new technology: IPv6, MPLS, 40G or 100G, Voice and Video traffic, etc.



Introducing NetFlow

Technology developed by Cisco - Initially designed as a switching path

Now the **Primary IP Traffic** accounting technology

Answers the WHO, WHAT, WHEN and WHERE question of network IP traffic

All major vendors now support flow export :

NetFlow - Cisco, Adtran, 3COM

sFlow - Alcatel, HP, Brocade, Enterasys, Dell

IPFIX - Nortel

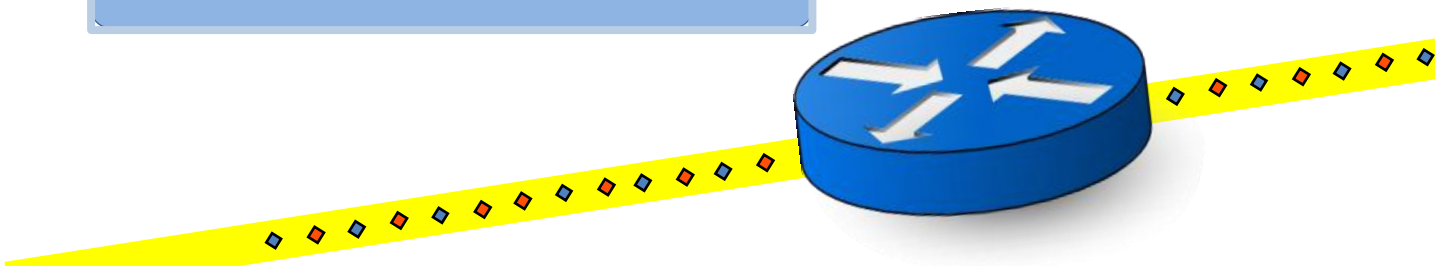
J-Flow - Juniper

What is NetFlow

What is a Flow

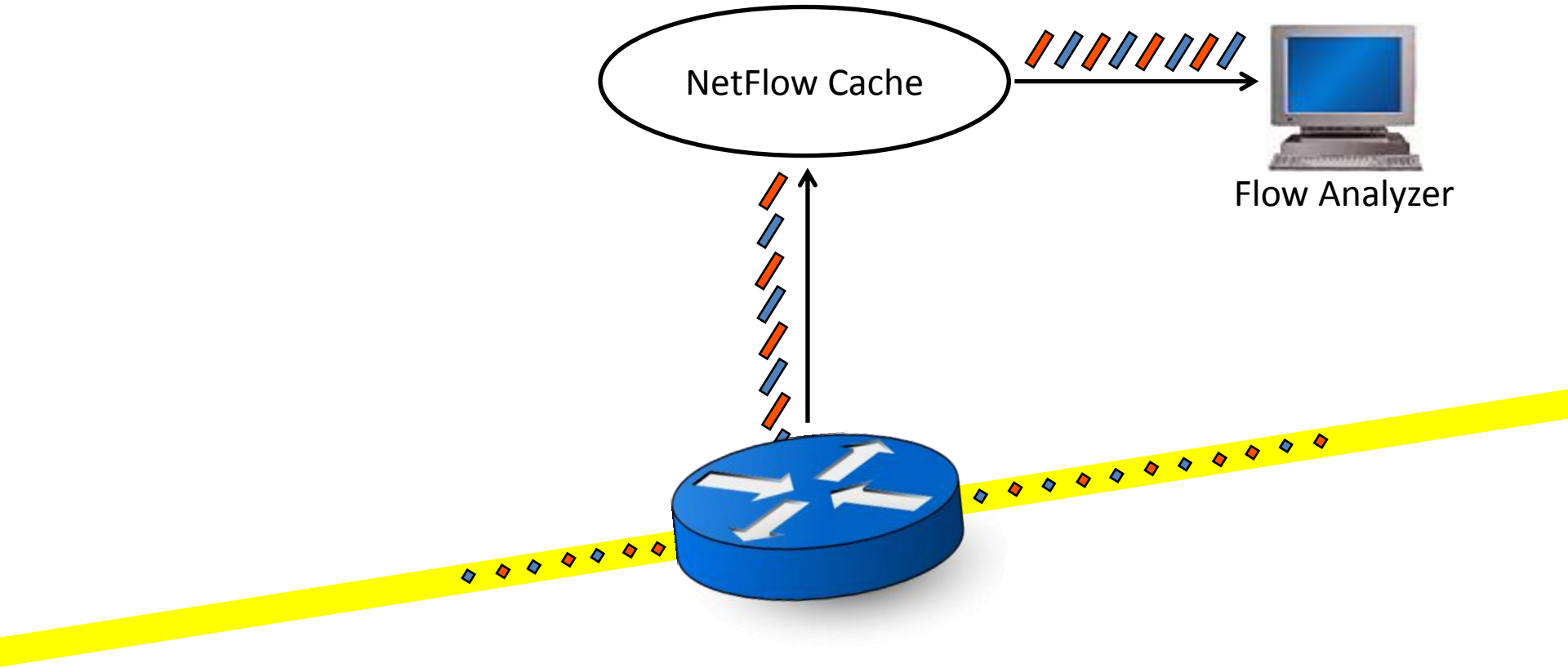
Seven (7) unique fields define a flow

- Source Interface (ifindex)
- Protocol
- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- ToS



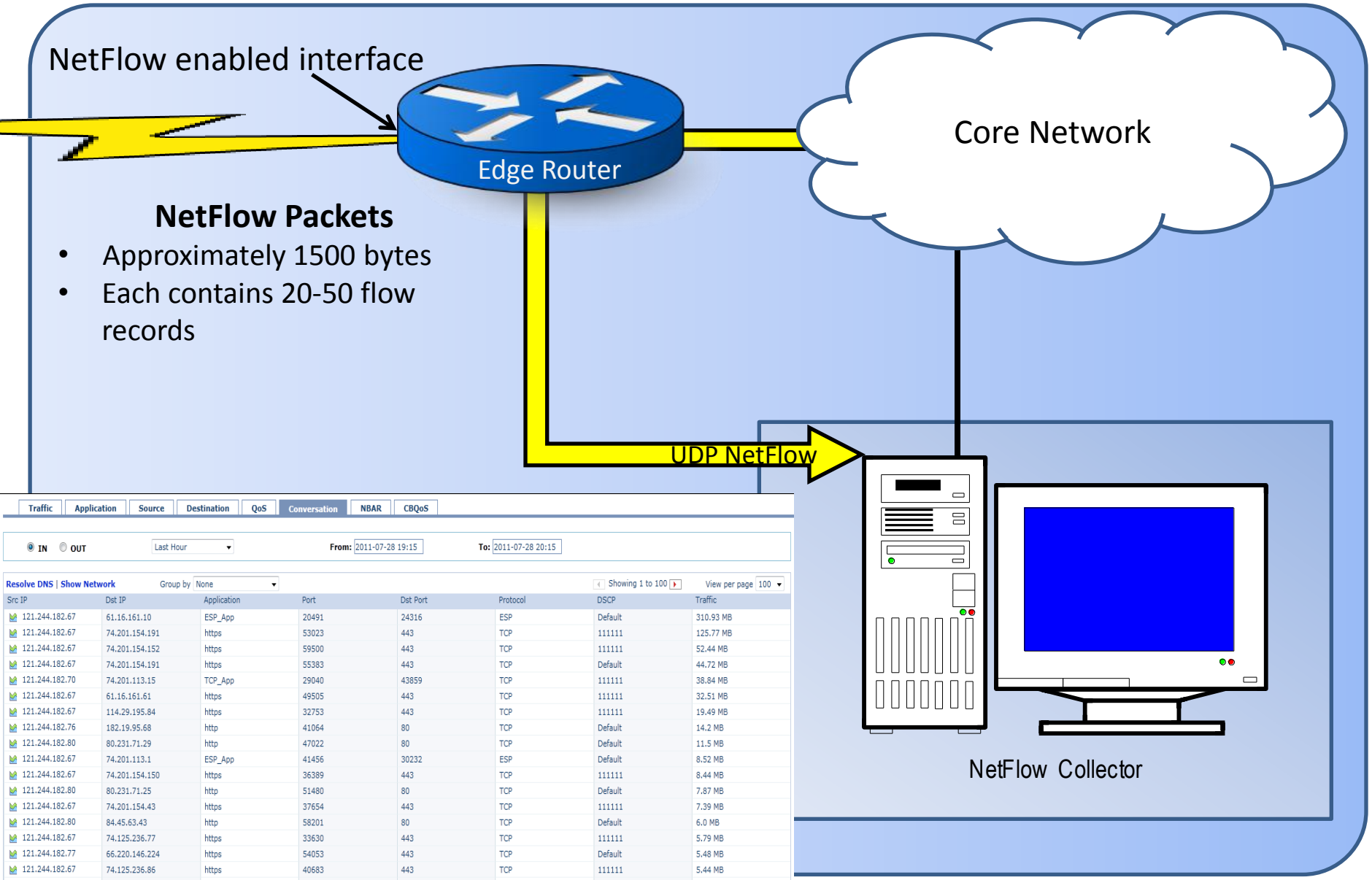
How NetFlow Works

- Traffic passes through routing/switching device interface
- Flow created (remember the 7 fields) and stored in NetFlow cache
- Flows grouped and exported in UDP packets to collector based on active and inactive flow timeout



What is NetFlow

ManageEngine



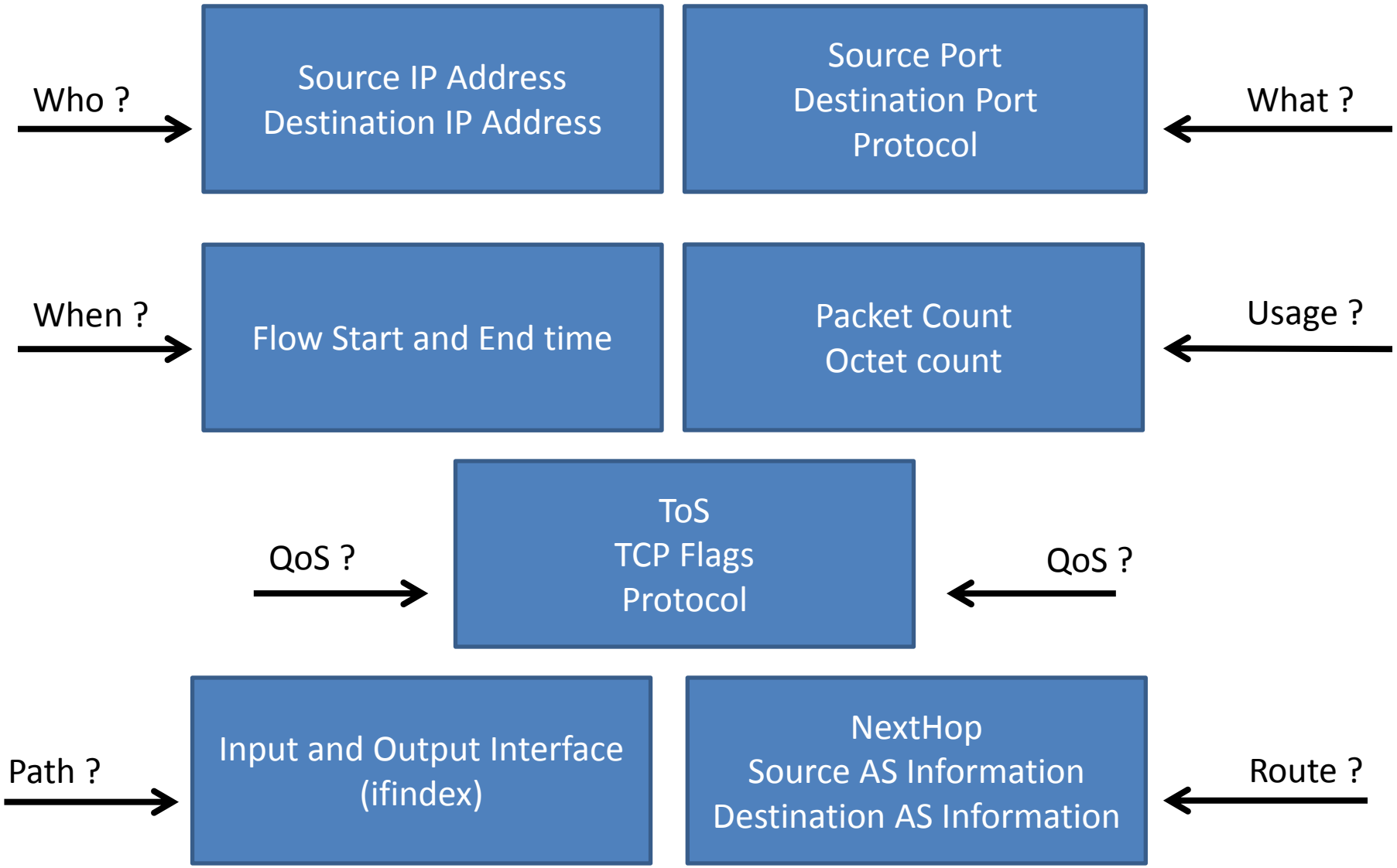
Traffic | Application | Source | Destination | QoS | Conversation | NBAR | CBQoS

IN OUT | Last Hour | From: 2011-07-28 19:15 | To: 2011-07-28 20:15

Resolve DNS | Show Network | Group by None | Showing 1 to 100 | View per page 100

Src IP	Dst IP	Application	Port	Dst Port	Protocol	DSCP	Traffic
121.244.182.67	61.16.161.10	ESP_App	20491	24316	ESP	Default	310.93 MB
121.244.182.67	74.201.154.191	https	53023	443	TCP	111111	125.77 MB
121.244.182.67	74.201.154.152	https	59500	443	TCP	111111	52.44 MB
121.244.182.67	74.201.154.191	https	55383	443	TCP	Default	44.72 MB
121.244.182.70	74.201.113.15	TCP_App	29040	43859	TCP	111111	38.84 MB
121.244.182.67	61.16.161.61	https	49505	443	TCP	111111	32.51 MB
121.244.182.67	114.29.195.84	https	32753	443	TCP	111111	19.49 MB
121.244.182.76	182.19.95.68	http	41064	80	TCP	Default	14.2 MB
121.244.182.80	80.231.71.29	http	47022	80	TCP	Default	11.5 MB
121.244.182.67	74.201.113.1	ESP_App	41456	30232	ESP	Default	8.52 MB
121.244.182.67	74.201.154.150	https	36389	443	TCP	111111	8.44 MB
121.244.182.80	80.231.71.25	http	51480	80	TCP	Default	7.87 MB
121.244.182.67	74.201.154.43	https	37654	443	TCP	111111	7.39 MB
121.244.182.80	84.45.63.43	http	58201	80	TCP	Default	6.0 MB
121.244.182.67	74.125.236.77	https	33630	443	TCP	111111	5.79 MB
121.244.182.77	66.220.146.224	https	54053	443	TCP	Default	5.48 MB
121.244.182.67	74.125.236.86	https	40683	443	TCP	111111	5.44 MB
121.244.182.67	61.16.161.50	https	58025	443	TCP	111111	4.7 MB
121.244.182.76	216.115.212.95	https	47569	443	TCP	Default	4.52 MB
121.244.182.69	61.16.161.10	netmeeting	3389	38260	TCP	111111	4.07 MB

What is NetFlow



Cisco NetFlow Versions

Cisco NetFlow Version	Description
Version 1	Original implementation, Now Obsolete Only IPv4 Traffic
Version 5	Most widely used version Supports AS reporting and few additional fields
Version 7	Specific to Cisco catalyst switches
Version 8	Same as Version 5 but with Flow Aggregation options
Version 9	Flexible, Customizable and template based Supports new data fields

More on NetFlow

- ip flow-export version <version> [origin-as | peer-as |
  - Select the version of NetFlow to be exported and type of AS info.
- ip flow-export destination <address> <port>
  - Exactly what it says. e.g. ip flow-export destination 198.2.1.16 9996
- ip flow export source <interface>
  - The interface through which NetFlow packets are sent from cache to collector. Recommended to use an interface with the best route to the collector.
- ip flow-cache timeout inactive <seconds>
  - The time period for which an expired flow will remain in the cache before being exported. 15 seconds is the default as well as the recommended value
- ip flow-cache timeout active <minutes>
  - Time period for which an active flow will remain in the cache before being exported. 30 minutes is default but the recommended value is 1 minute.

NetFlow Version 9 – Flexible NetFlow

NetFlow Version 9 – Flexible NetFlow

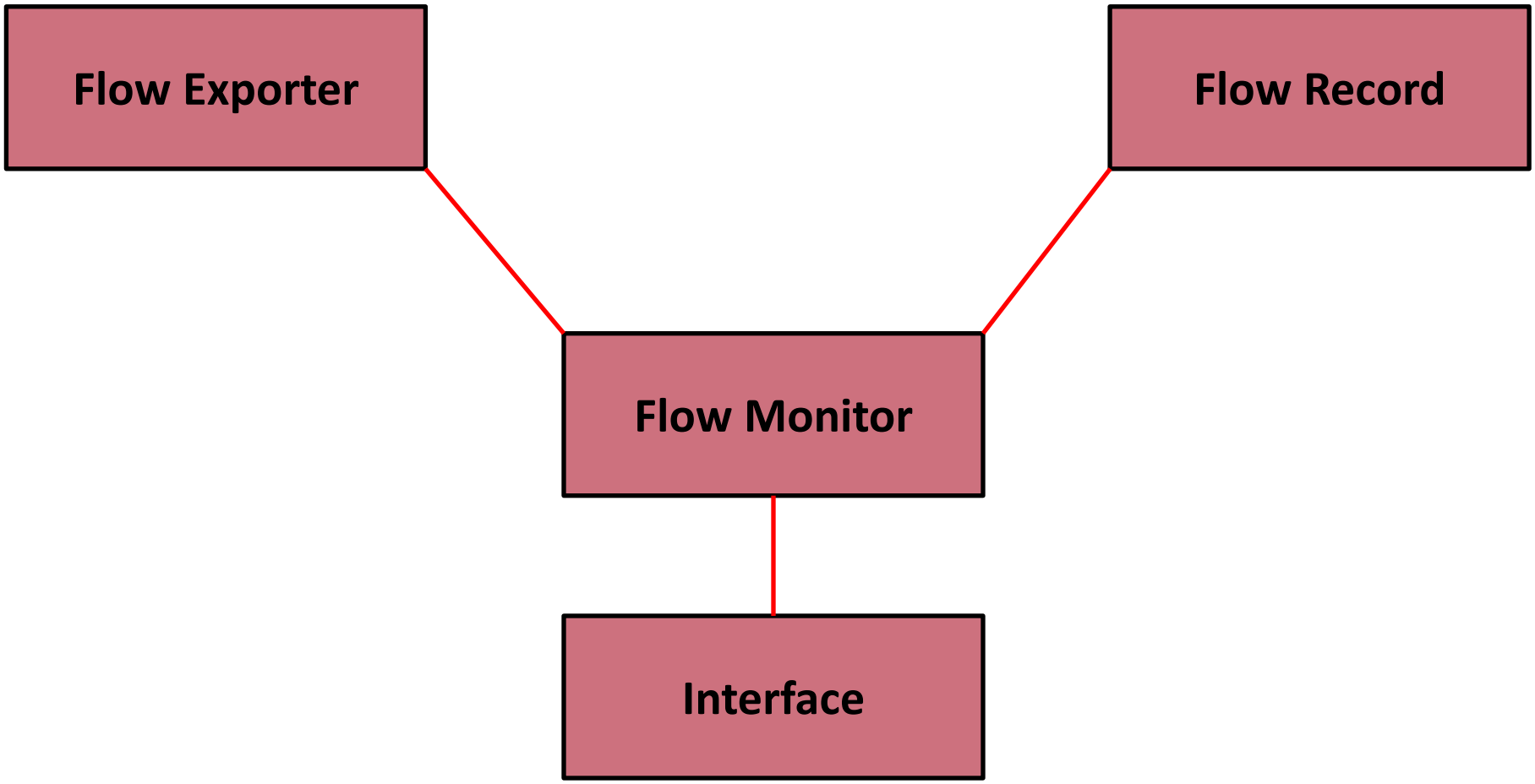
- Highly flexible flow export - Customized traffic monitoring with user defined key and non key fields

- Ability to monitor a wide range of IP packet information which traditional NetFlow did not have

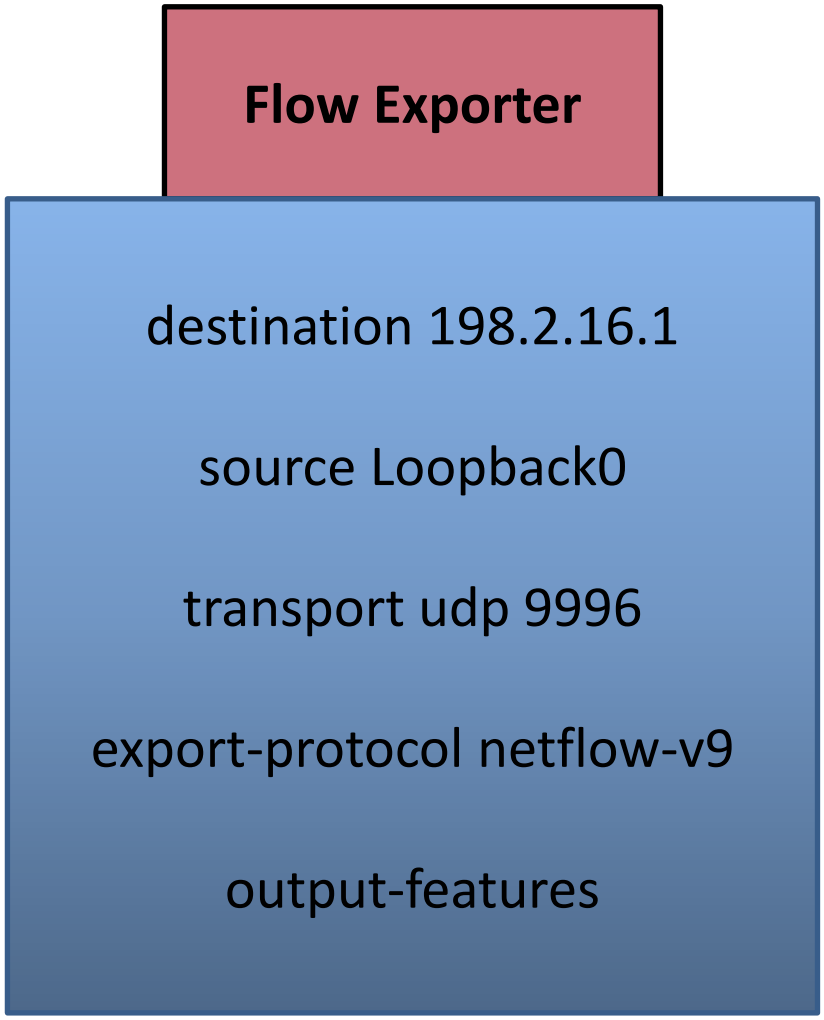
- Analyze the effect of new technology implementations in your network:
  IPv6, VoIP, Webex, Telepresence or other voice and video solutions

- Some of the major custom fields supported are
  - MPLS Labels
  - IPv6 Traffic
  - NBAR protocols
  - Live performance of media flows
  - Multicast IP Traffic
  - VLAN ID

Flexible NetFlow Structure



Flexible NetFlow Structure



Flexible NetFlow Structure

Flow Record

Pre-Defined Flow Records

netflow-original

netflow ipv4 original-input

User-Defined Flow Records

Match statements

match ipv4 source address
match ipv4 destination address
match ipv4 protocol
match transport source-port
match transport destination-port
match interface input

Collect statements

collect routing source as
collect transport tcp flags
collect counter bytes
collect counter packets
collect flow direction

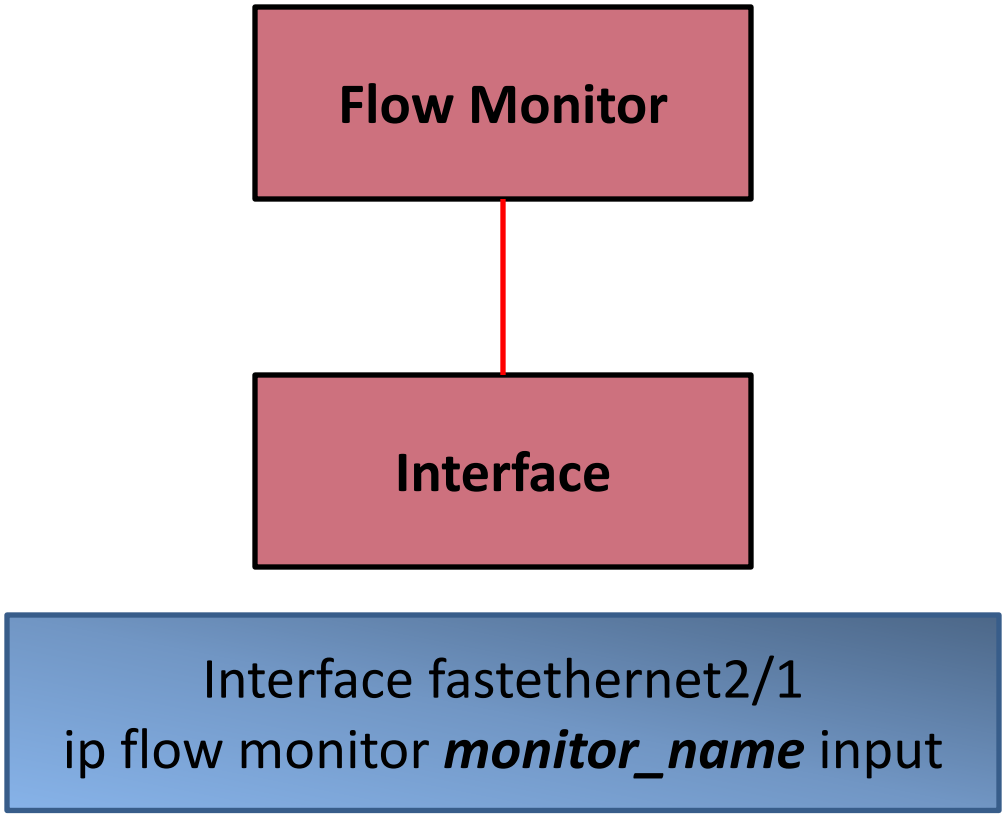
Flexible NetFlow Structure

Flow Monitor

exporter ***exporter_name***

record *netflow-original*
OR
record ***record_name***

Flexible NetFlow Structure



Config Example - User-Defined Flow Record

flow record ***NFArecord***

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match interface input

match ipv4 protocol

match ipv4 tos

match ipv4 dscp

collect routing source as

collect routing destination as

collect routing next-hop address ipv4

collect transport tcp flags

collect counter bytes

collect counter packets

collect timestamp sys-uptime first

collect timestamp sys-uptime last

collect interface output

collect flow direction

collect ipv4 id

collect ipv4 source mask

collect ipv4 destination mask

Config Example - Flow Exporter and Flow Monitor

flow exporter ***NFAexporter***

destination 192.16.1.82

source loopback0

transport udp 9996

export-protocol netflow-v9

flow monitor ***NFAmonitor***

exporter ***NFAexporter***

cache timeout active 1

cache timeout inactive 15

record ***NFArecord*** **or** record ***netflow-original***

Interface fastethernet1/2

ip flow monitor ***NFAmonitor*** input

NetFlow Performance Impact

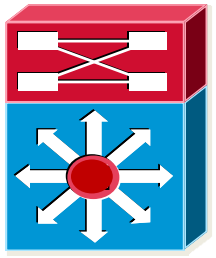
CPU Utilization

- 10,000 active flows – 7.14 % additional CPU
- 65,000 active flows – 22.98 % additional CPU

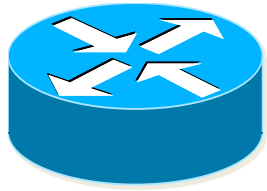
Bandwidth Usage Estimate

- Around 2% to 3% additional bandwidth load on the NetFlow exporting link for the device

Flow Exporting Devices



NetFlow supported Cisco devices



Cisco Catalyst 3560	Cisco 800	Cisco 7200
Cisco Catalyst 3750	Cisco 1800	Cisco 7600
Cisco Catalyst 4500	Cisco 1900	Cisco 12000
Cisco Catalyst 6500	Cisco 2800	Cisco ASR series
Cisco Nexus	Cisco 3800	
Cisco ASA firewall	Cisco 3900	

Other Vendors and Flow Formats

- sFlow: Alcatel, Brocade – Foundry, Dell, Enterasys, Extreme, Force 10, Fortinet, HP ProCurve, Juniper, Vyatta, etc. http://www.sflow.org/products
- J-Flow: Juniper devices
- IPFIX : To be developed as the standard for flow export. Described in RFC 3917. Based on NetFlow v9.
- AppFlow: Extension to IPFIX for application monitoring. Citrix NetScaler captures app-specific network data and generates Appflow records
- NetStream: Huawei / 3COM devices

Some Use Cases

- Which links are most utilized and under-utilized
- Who are the top takers and which are the top applications
- Understand application usage - Peak and non-peak usage, when, application volume and speed
- Traffic priorities and QoS performance

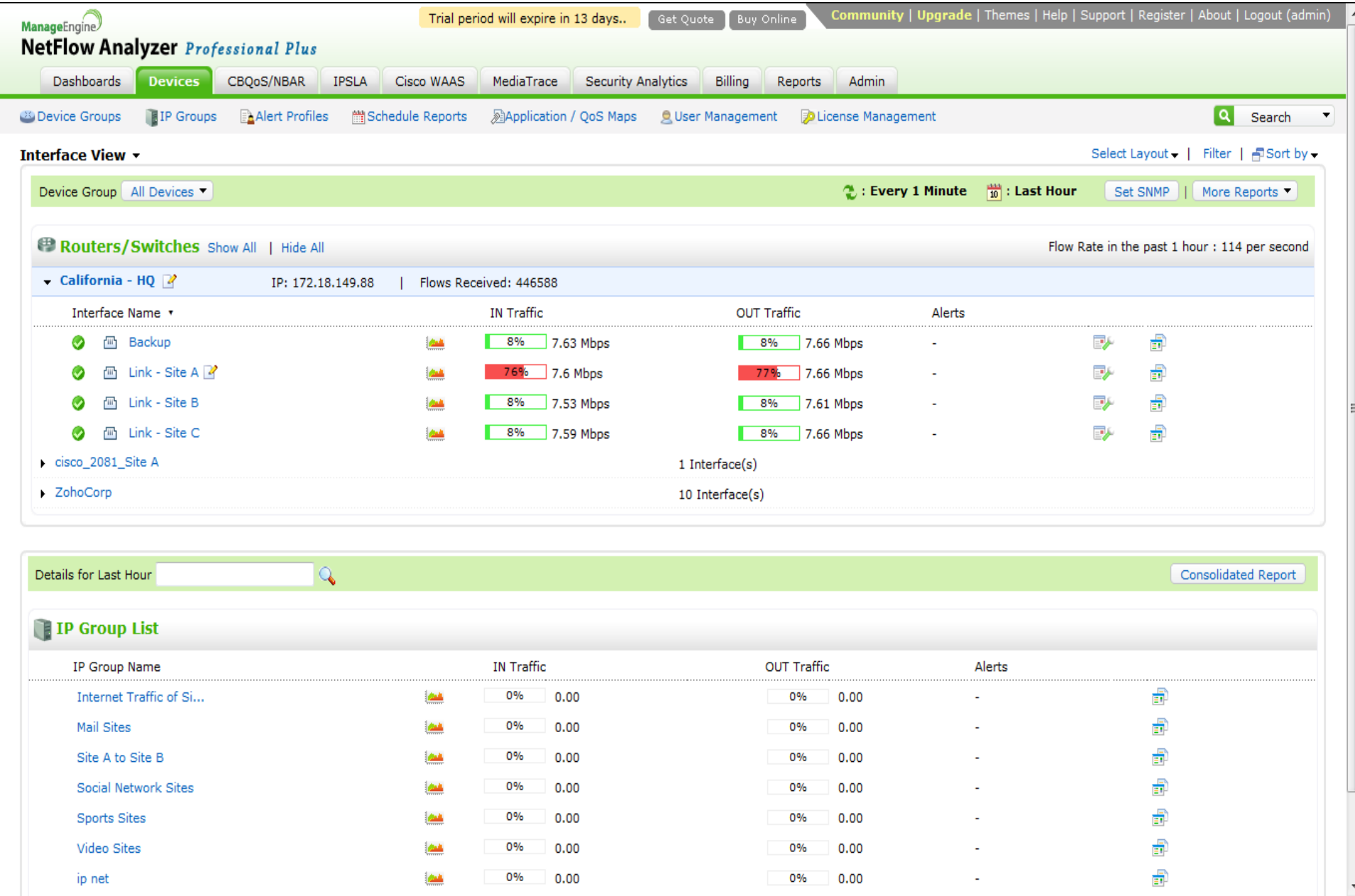
Traffic Usage

Src and Dst

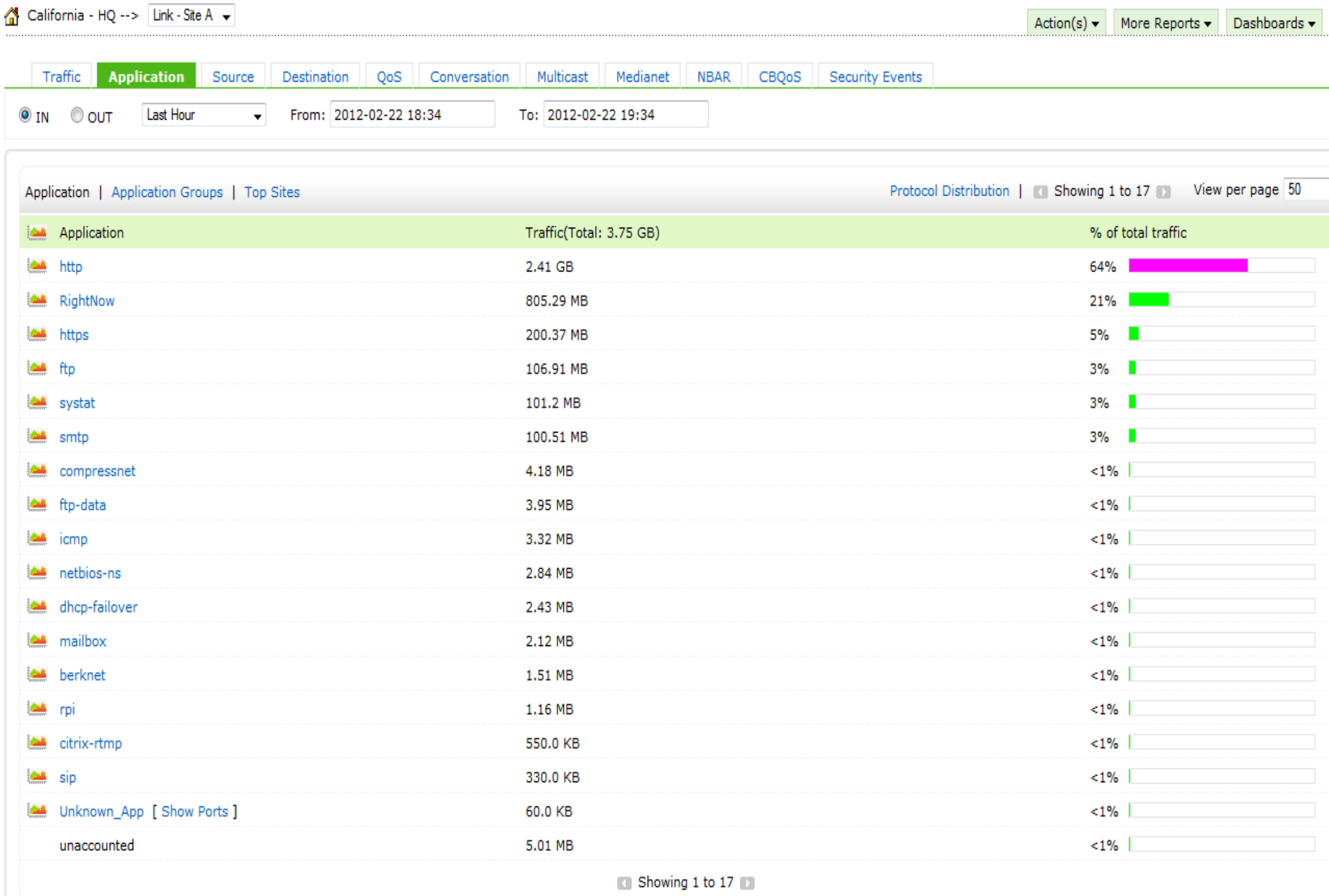
Top Apps

App-wise QoS

Application Slowness – Check link utilization



Check top applications – HTTP more than business application



Incorrect priority for business application

California - HQ --> Link - Site A

Action(s) | More Reports | Dashboards

Traffic | Application | Source | Destination | QoS | Conversation | Multicast | Medianet | NBAR | CBQoS | Security Events

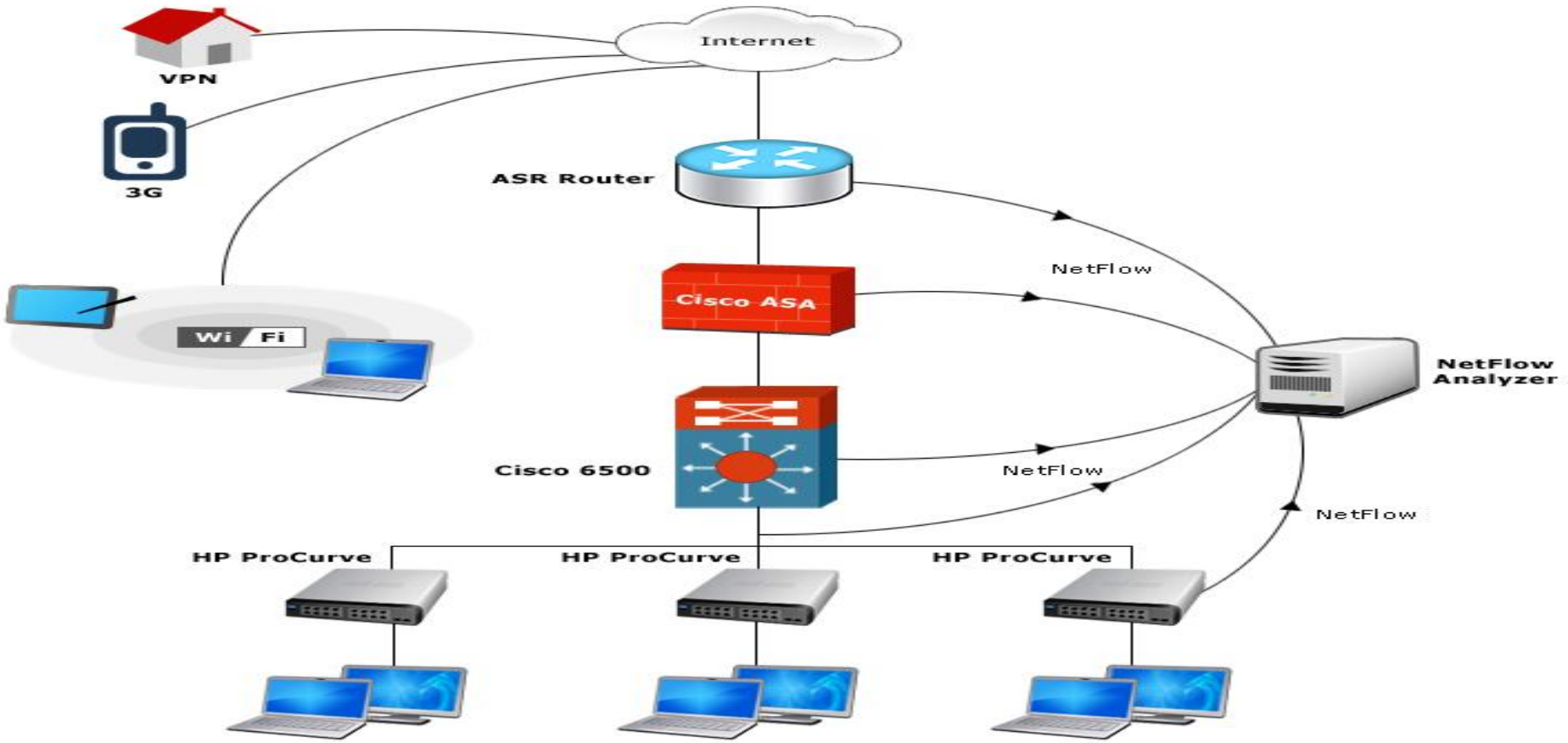
Top Application IN Report - RightNow From: 2012-02-22 20:01 To: 2012-02-22 20:16 Back

Resolve DNS | Group by None Showing 1 to 50 View per page 50

Src IP	Dst IP	Application	Port	Dst Port	Protocol	DSCP	Traffic(43.25 MB)	Percent
69.63.180.2	192.168.1.106	RightNow	107	107	TCP	Default	70.0 KB	<1%
69.63.180.3	192.168.1.201	RightNow	107	107	TCP	Default	50.0 KB	<1%
69.63.180.8	192.168.1.126	RightNow	107	107	TCP	Default	50.0 KB	<1%
69.63.180.1	192.168.1.27	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.10	192.168.1.158	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.11	192.168.1.129	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.11	192.168.1.137	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.11	192.168.1.189	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.12	192.168.1.196	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.12	192.168.1.32	RightNow	107	107	TCP	AF12	40.0 KB	<1%
69.63.180.12	192.168.1.4	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.14	192.168.1.204	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.14	192.168.1.228	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.14	192.168.1.244	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.15	192.168.1.161	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.15	192.168.1.69	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.16	192.168.1.144	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.17	192.168.1.239	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.19	192.168.1.11	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.19	192.168.1.129	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.2	192.168.1.162	RightNow	107	107	TCP	Default	40.0 KB	<1%
69.63.180.2	192.168.1.42	RightNow	107	107	TCP	Default	40.0 KB	<1%

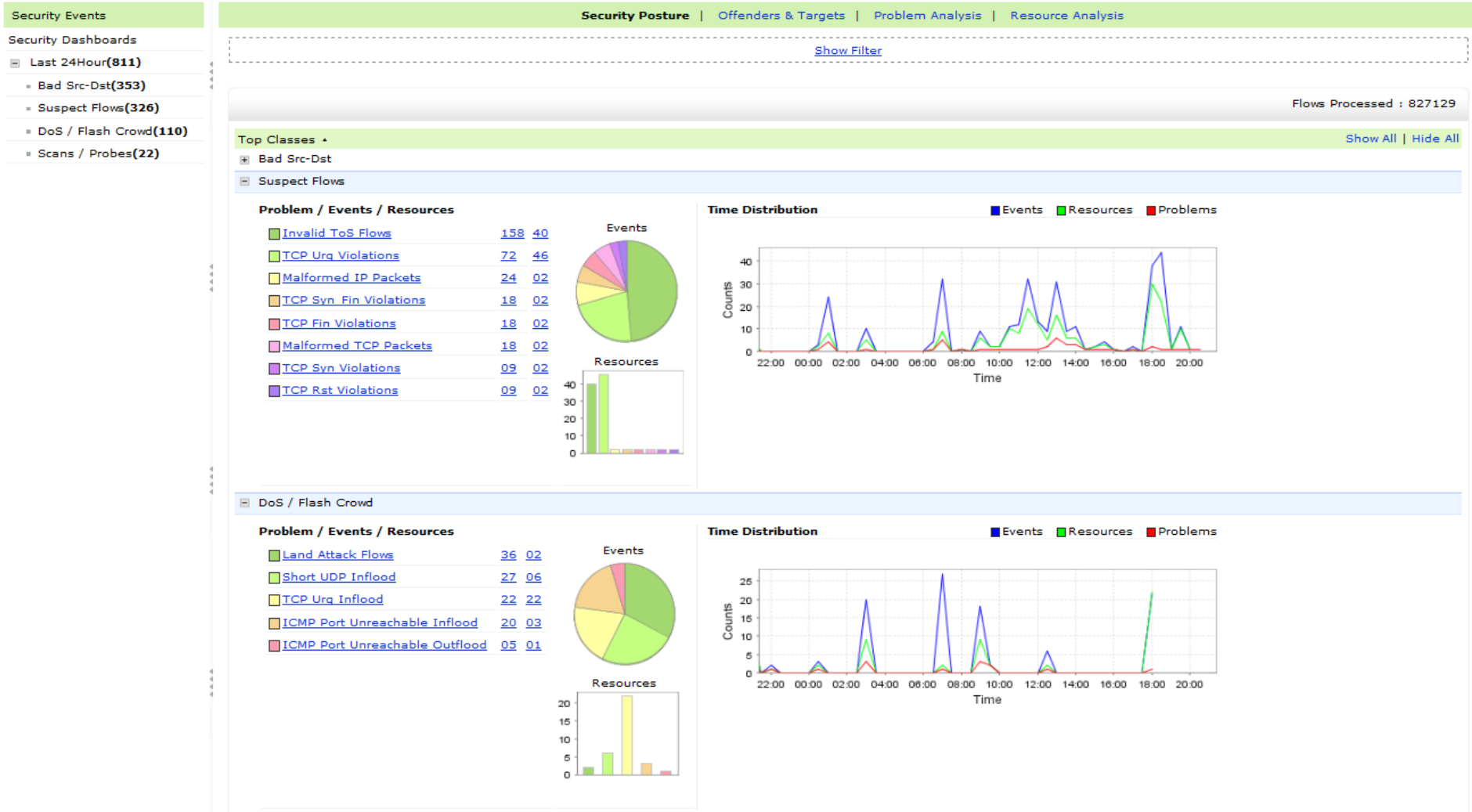
- Specific IP Traffic header information captured - Low overhead on network devices

- Can work in high speed environments as well as new technologies like MPLS or 100G networks



- Non Signature based - Hence can detect zero day malware

- Detects anomalies coming beyond IDS/IPS and firewalls or even those originating from your LAN network



Security Events
Security Dashboards
- Last 24Hour(15585)
  - Suspect Flows(9647)
  - DoS / Flash Crowd(5166)
  - Bad Src-Dst(767)
  - Scans / Probes(5)

Event List

Show Filter

White List | Manage | Algorithm Settings | Location | More Actions | Show DNS | Flows Processed : 67412527

Report Details 1 - 7 Per Page : 25

	ID	Problem		Offender(s)	Routed via		Target(s)	Time ▲	Hits			
	141074	**Suspect Flows** - Excess Short TCP Hands...	NA	10: [192.168.5.1, 192.168.5.2, 192.168.5.3, 192.168.5.4, 192.168.5.5, 192...	3: [172.18.119.150 (IfIndex113), 172.18.119.150 (IfIndex114), 172.18.119....	NA	1: [62.210.136.128]	2012-02-22 13:24:30 -- 2012-02-22 13:24:33	100			View
	141071	**Suspect Flows** - Excess Short TCP Hands...	NA	12: [192.168.5.1, 192.168.5.2, 192.168.5.3, 192.168.5.4, 192.168.5.5, 192...	5: [172.18.119.150 (IfIndex111), 172.18.119.150 (IfIndex112), 172.18.119....	NA	1: [62.210.136.128]	2012-02-22 13:24:28 -- 2012-02-22 13:24:30	100			View
	141070	**Suspect Flows** - Excess Short TCP Hands...	NA	13: [65.204.166.1, 192.168.5.1, 192.168.5.2, 192.168.5.3, 192.168.5.4, 19...	5: [172.18.119.150 (IfIndex111), 172.18.119.150 (IfIndex112), 172.18.119....	NA	1: [62.210.136.128]	2012-02-22 13:24:26 -- 2012-02-22 13:24:28	100			View
	137120	**Suspect Flows** - Excess Short TCP Hands...	NA	2: [62.23.50.192, 62.210.136.128]	5: [172.18.119.150 (IfIndex111), 172.18.119.150 (IfIndex112), 172.18.119....	NA	2: [62.210.136.128, 65.204.166.1]	2012-02-22 07:24:28 -- 2012-02-22 07:24:30	100			View
	137117	**Suspect Flows** - Excess Short TCP Hands...	NA	1: [62.23.50.192]	5: [172.18.119.150 (IfIndex111), 172.18.119.150 (IfIndex112), 172.18.119....	NA	1: [62.210.136.128]	2012-02-22 07:24:28 -- 2012-02-22 07:24:28	100			View
	133106	**Suspect Flows** - Excess Short TCP Hands...	NA	2: [62.23.50.192, 62.210.136.128]	5: [172.18.119.150 (IfIndex111), 172.18.119.150 (IfIndex112), 172.18.119....	NA	2: [62.210.136.128, 65.204.166.1]	2012-02-22 01:24:12 -- 2012-02-22 01:24:14	100			View
	133103	**Suspect Flows** - Excess Short TCP Hands...	NA	1: [62.23.50.192]	5: [172.18.119.150 (IfIndex111), 172.18.119.150	NA	1: [62.210.136.128]	2012-02-22 01:24:12 -- 2012-02-22 01:24:12	100			View

Capacity Planning Decisions

- Is the bandwidth upgrade necessary?
- Analyze application usage. Limit or block bandwidth hogging applications using QoS, ACL, etc.
- Check link utilization and business application distribution over time in lowest possible granularity – 1 minute.
- Do you still need more bandwidth?
- Informed decisions with reports to validate leads to higher cost savings

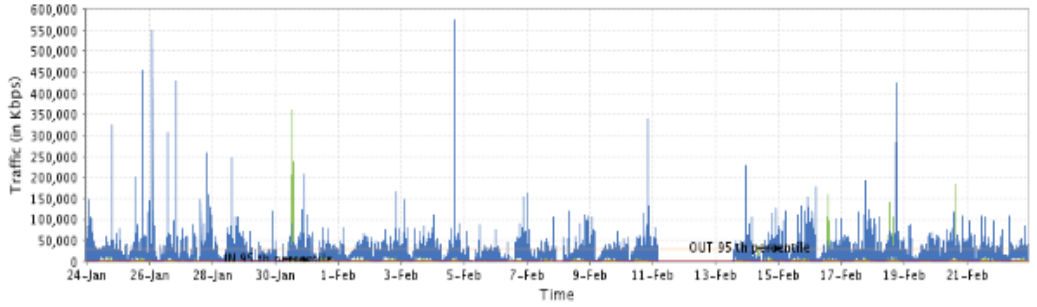
Capacity Planning Decisions

ManageEngine

Report

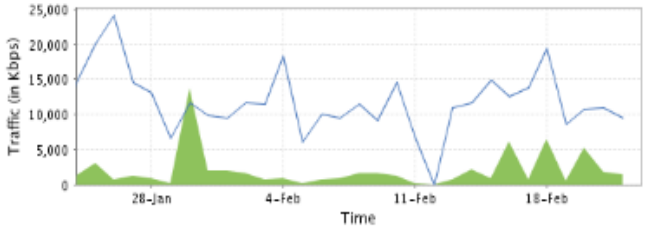
Volume | Speed | Utilization | Packets

1 Minute Average

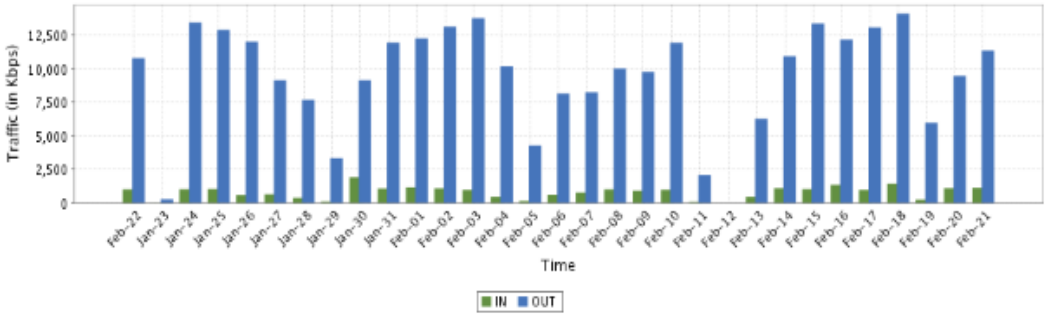


Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	273.19 GB	359.43 Mbps	0.00	843.16 Kbps	3.38 Mbps	1.96 Mbps
OUT	3.14 TB	573.22 Mbps	0.00	9.72 Mbps	13.21 Mbps	29.28 Mbps

Standard Deviation Graph(Daily)



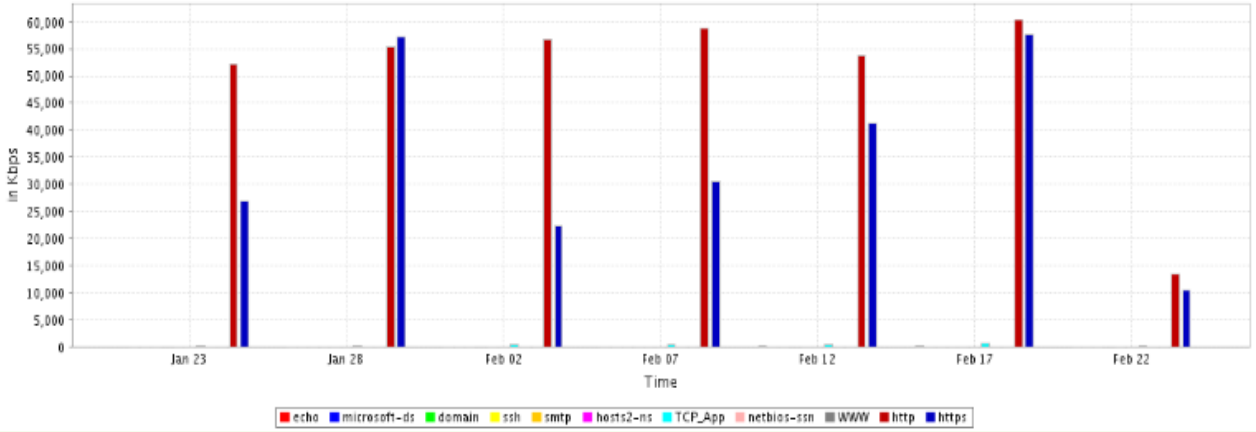
Average Usage(Daily)



Capacity Planning Decisions

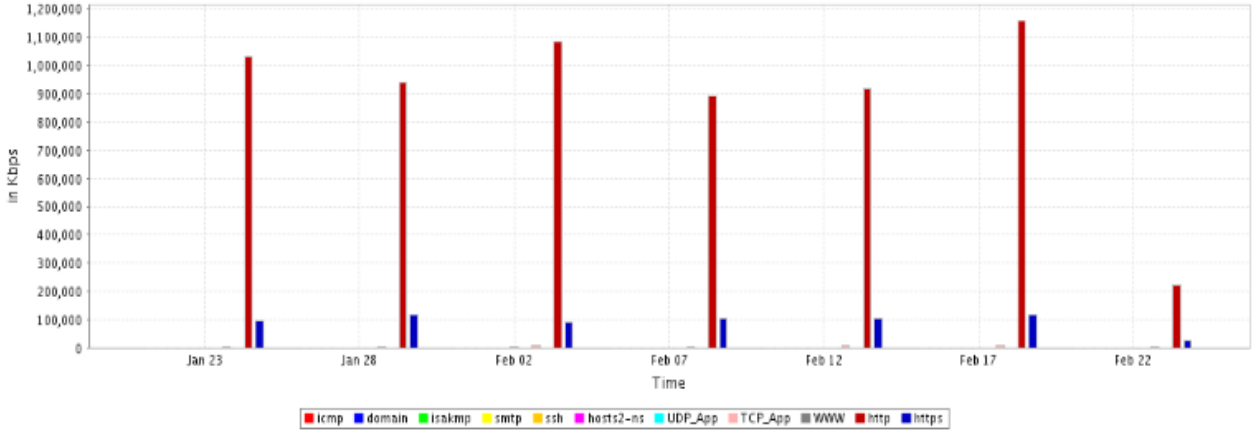
ManageEngine

ApplicationIN Growth Report



ApplicationIN	Jan 23	Jan 28	Feb 02	Feb 07	Feb 12	Feb 17	Feb 22
echo	58.06 Kbps	78.44 Kbps	73.82 Kbps	70.08 Kbps	84.4 Kbps	97.8 Kbps	18.59 Kbps
microsoft-ds	12.82 Kbps	16.63 Kbps	16.25 Kbps	13.3 Kbps	11.04 Kbps	16.96 Kbps	3.17 Kbps
domain	28.48 Kbps	37.77 Kbps	35.17 Kbps	36.89 Kbps	34.3 Kbps	40.64 Kbps	7.16 Kbps
ssh	-	34.0 Kbps	-	53.86 bps	-	0.80 bps	-
smtp	752.18 bps	1.43 Kbps	19.42 Kbps	3.34 Kbps	813.75 bps	21.41 Kbps	352.72 bps
hosts2-ns	20.98 Kbps	10.66 Kbps	41.7 Kbps	2.55 Kbps	2.33 Kbps	4.46 Kbps	3.09 Kbps
TCP_App	296.55 Kbps	278.64 Kbps	375.5 Kbps	386.97 Kbps	377.79 Kbps	560.63 Kbps	125.52 Kbps
netbios-ssn	12.81 Kbps	16.63 Kbps	16.24 Kbps	13.3 Kbps	11.03 Kbps	16.96 Kbps	3.17 Kbps
WWW	14.63 Kbps	51.88 Kbps	3.84 Kbps	6.03 Kbps	1.33 Kbps	13.84 Kbps	114.23 bps
http	52.11 Mbps	55.37 Mbps	56.83 Mbps	58.73 Mbps	53.73 Mbps	60.43 Mbps	13.41 Mbps
https	26.92 Mbps	57.18 Mbps	22.34 Mbps	30.5 Mbps	41.16 Mbps	57.57 Mbps	10.35 Mbps

ApplicationOUT Growth Report



SLA Verification and Billing

- Verify the Committed Information Rate and Committed Data Rate with your own usage based reports
- Generate billing reports and compare with ISP reports
- For department/project level billing : Account per network
- Billing based on 5 minute averages and 95th percentile. 95th percentile can be IN and OUT merged or IN and OUT separate
- Design In-line with generic ISP based billing solutions

SLA Verification and Billing

ManageEngine

Device/Interface : California - HQ --> Link - Site A

Custom Selection | From : 2012-02-22 18:24 | eekends

Enter Billing Details

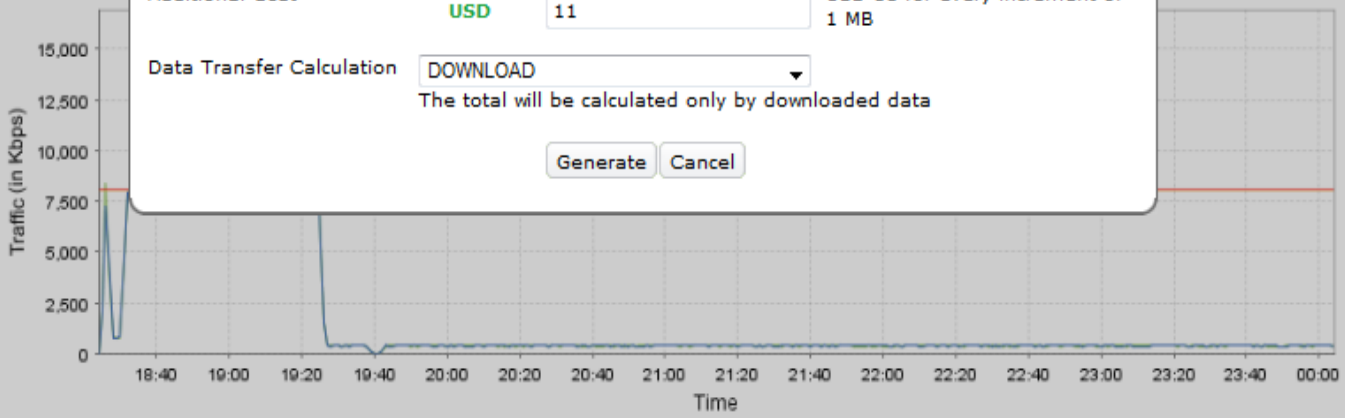
Bill Plan Name	Project A_bill usage	
Billing Type	Volume	
Base Volume	1000000	[Bytes]
Base Cost	American Dollar-USD 32	USD 32 for the initial 1 MB
Additional Volume	1000000	[Bytes](Optional)
Additional Cost	USD 11	USD 11 for every increment of 1 MB
Data Transfer Calculation	DOWNLOAD	The total will be calculated only by downloaded data

Generate | Cancel

Report

Volume | Speed | Utilization | Packets

1 Minute Average



Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	4.81 GB	16.09 Mbps	0.00	1.88 Mbps	3.58 Mbps	8.14 Mbps
OUT	4.82 GB	16.15 Mbps	0.00	1.88 Mbps	3.58 Mbps	8.03 Mbps

Average Usage(Daily)

SLA Verification and Billing

ManageEngine

NetFlow Analyzer Capacity Planning Report

Device/Interface : California - HQ --> Link - Site A

Custom Selection | From : 2012-02-22 18:24 | To : 2012-02-23 00:04 | Show | Business Hour Filter | Exclude weekends

Report

Volume | Speed | Utilization | Packets

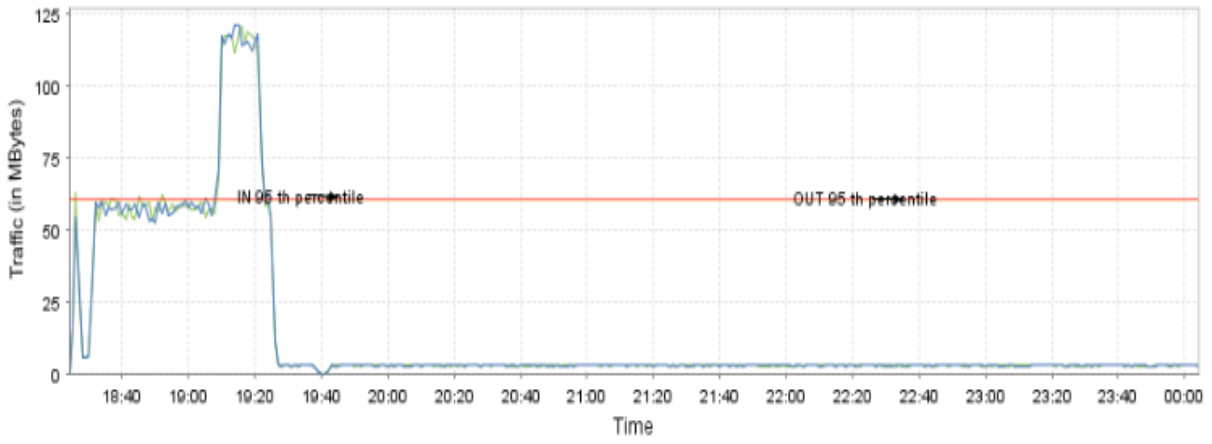
Invoice for plan Project A_bill usage :

Details : **USD 32** for the first **1.0 MB**
USD 11 for every increment of **1.0 MB**

Data Transfer : **4.81 GB**
Calculation : **DOWNLOAD**

Total Cost : **USD 53014.06**

1 Minute Average



Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	4.81 GB	120.74 MB	0.00	14.12 MB	26.87 MB	61.11 MB
OUT	4.82 GB	121.17 MB	0.00	14.16 MB	26.91 MB	60.27 MB

Analyze Application usage and VoIP Conversations

Traffic | Application | Source | Destination | QoS | Conversation | Multicast | Medianet | NBAR | CBQoS | Security Events

IN OUT Today Report From: 2012-02-23 00:00 To: 2012-02-23 10:26

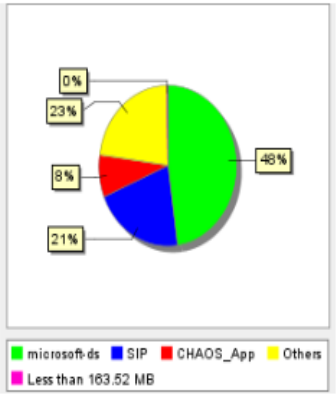
Application | Application Groups | Top Sites Protocol Distribution | Showing 1 to 10 View per page 50

Application	Traffic(Total: 8.17 GB)	% of total traffic
microsoft-ds	3.9 GB	48%
SIP	1.71 GB	21%
CHAOS_App [Show Ports]	687.96 MB	8%
telnet	3.64 MB	<1%
ftp	3.44 MB	<1%
https	3.4 MB	<1%
ftp-data	3.32 MB	<1%
smtp	3.3 MB	<1%
palace-5	3.06 MB	<1%
ms-wbt-server	2.88 MB	<1%
unaccounted	1.84 GB	23%

Showing 1 to 10

Top Traffic - ApplicationIN

California - HQ [Link - Site A]



VoIP Quality Issues

- Bulk Data scheduled during business hours
- Both VoIP and bulk data applications under default priority
- Reschedule bulk data for non peak hours – Get traffic distribution report over time to know peak and non-peak hours
- Assign QoS priority for VoIP traffic – Validate QoS policy performance from NetFlow conversation reports
- Study effect of network changes using various reports

SNMP, Packet Sniffing or NetFlow

Answering an FAQ

- **SNMP**: Basic method
  - Traffic usage information from any SNMP capable device
  - No details - Port, Protocol, IP Address of traffic cannot be seen
  - Negligible overhead on network resources

- **NetFlow**: Optimal method
  - Answers WHO, WHAT, WHEN and WHERE question on IP traffic
  - Detailed information. Very less or ignorable overhead on network

- **Packet Sniffing**: Advanced and detailed
  - Most detailed and In-depth information
  - Every IP Traffic information captured
  - Requires SPAN - High resource requirements and highly expensive

When to Use?

- **SNMP**:
  - No NetFlow available or detailed visibility is not required
  - Accurate bandwidth usage reports is necessary
    - Compare SNMP stats with NetFlow based reports to confirm report accuracy

- **NetFlow**:
  - Implement throughout the network, on all supported devices, at all times
  - Proactive reporting and troubleshooting
  - Many use cases

- **Packet Sniffing**:
  - Resource and data intensive with huge storage requirements
  - Use in high priority environments like data centers, server farms
  - Keep in standby mode and use when problems require packet level analysis

- Network uptime is a business requisite
- To create high performing networks, proactive monitoring is needed
- Use NetFlow, a non-intrusive, zero network impact technology to keep a tab on your complete network
- Cost Savings: Less downtime, Informed decisions, Hold back on WAN optimization & bandwidth upgrades, Secure network
- Small enterprises: Packet Sniffing is highly expensive. Use SNMP reports and NetFlow
- Medium and Large enterprises : Proactive monitoring with NetFlow & Packet Sniffing for detailed analysis at packet level

About NetFlow Analyzer

- Solution for bandwidth monitoring, traffic analysis & network forensics
- Supports flow formats like NetFlow, sFlow, IPFIX, Appflow, etc.
- Many of Cisco's major monitoring technologies supported:
  - Cisco NetFlow
  - Cisco Medianet – Perf Monitoring and Mediatrace
  - Cisco CBQoS
  - Cisco NBAR - via SNMP and Flexible NetFlow
  - Cisco IPSLA - VoIP and Data
  - Cisco WAAS reporting

- Additional features:
  - Network behavior anomaly detection leveraging on Cisco NetFlow
  - Enhanced reporting on Cisco ASA NSEL flows
  - Reporting on Autonomous System information from NetFlow data

- Distributed architecture based enterprise edition available for monitoring more than 250 geo-distributed interfaces or more than 600 high traffic interfaces

- Future enhancements include: Support for more Flexible NetFlow fields, Cisco PfR, Cisco Smart Logging and Telemetry, NBAR2

Questions?

Over 4000 enterprises worldwide uses ManageEngine NetFlow Analyzer for traffic analytics

NetFlow Analyzer: www.netflowanalyzer.com

TAC Team: netflowanalyzer-support@manageengine.com

Sales: sales@manageengine.com

NetFlow Analyzer Blogs: https://blogs.netflowanalyzer.com

User Forums: http://forums.netflowanalyzer.com