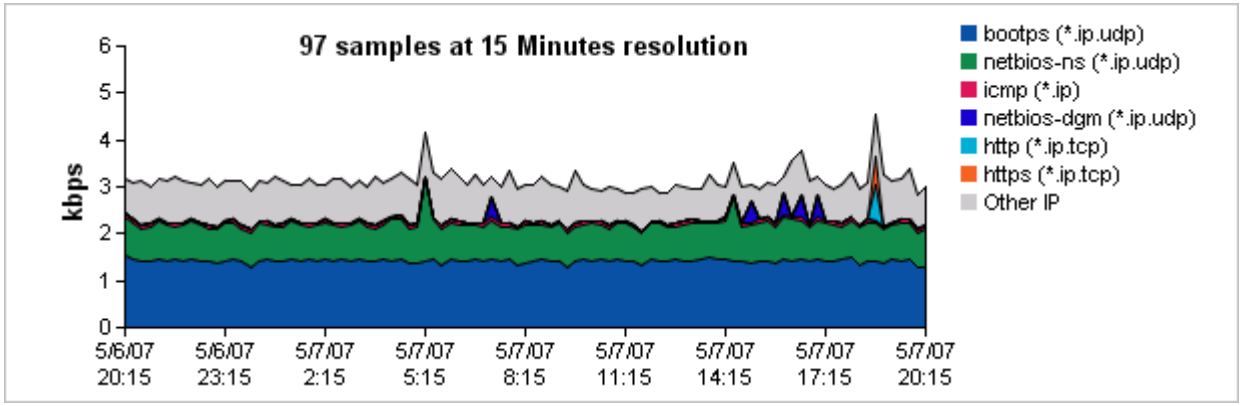
Viete, čo robia Vaši užívatelia na sieti ?

Roman Tuchyňa, CSA

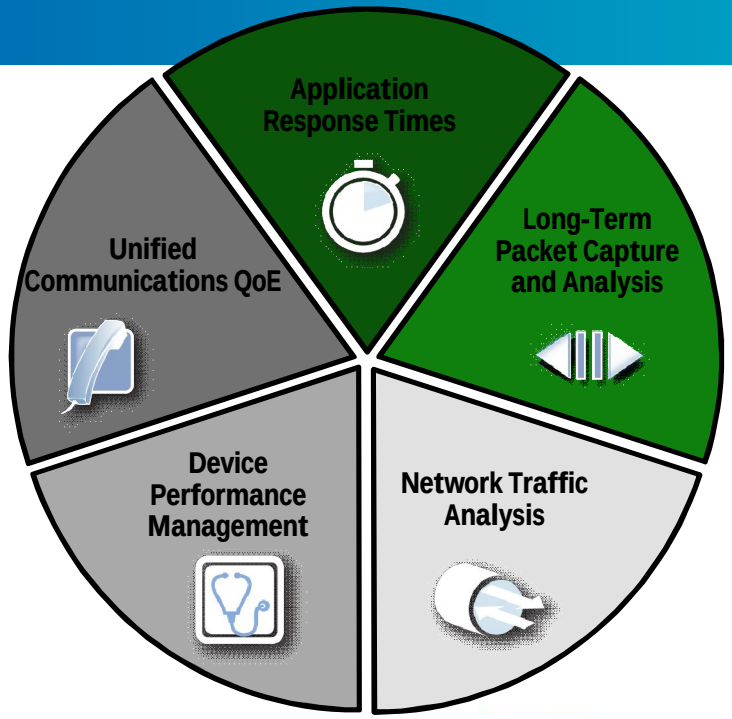
ca Forum | Bratislava 20. október

What is ReporterAnalyzer?

ReporterAnalyzer gives network professionals insight into how application traffic is impacting network performance.

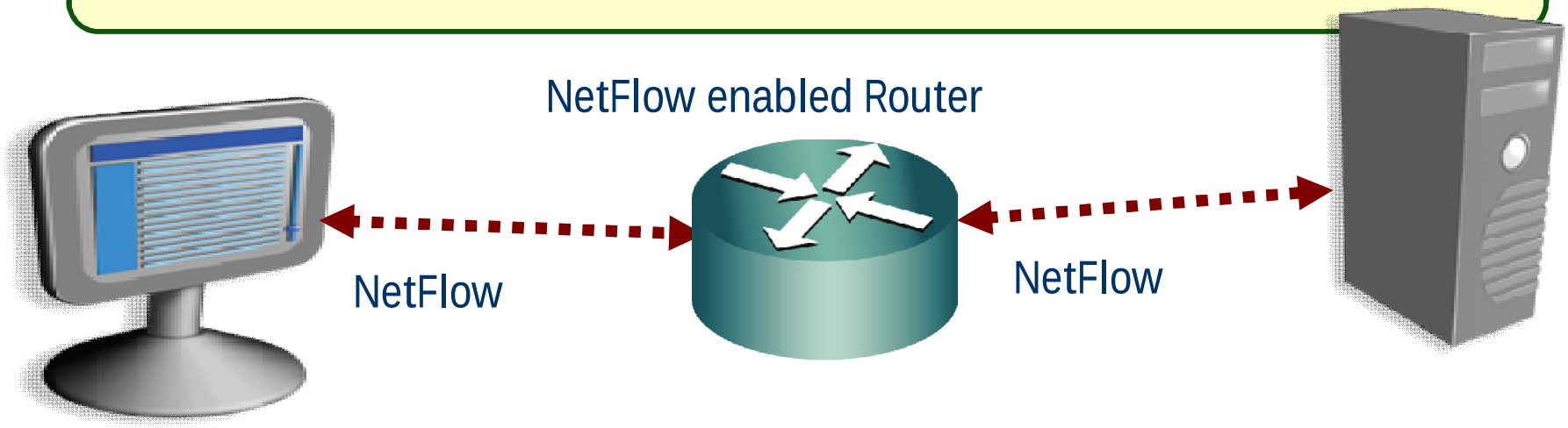


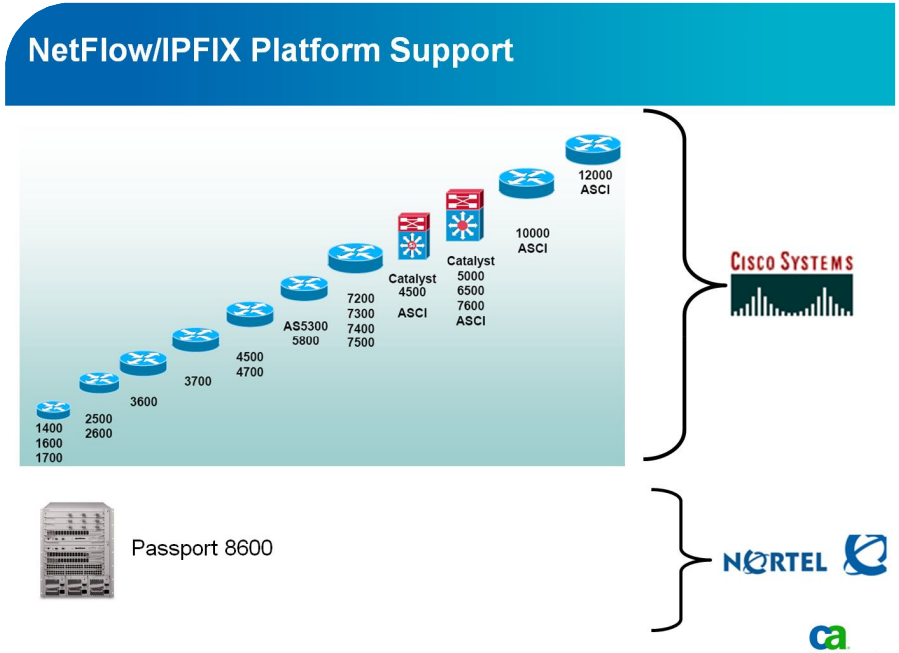
Complete Network Performance Management



NetFlow:

A Cisco IOS application that provides statistics on packets flowing through the router.

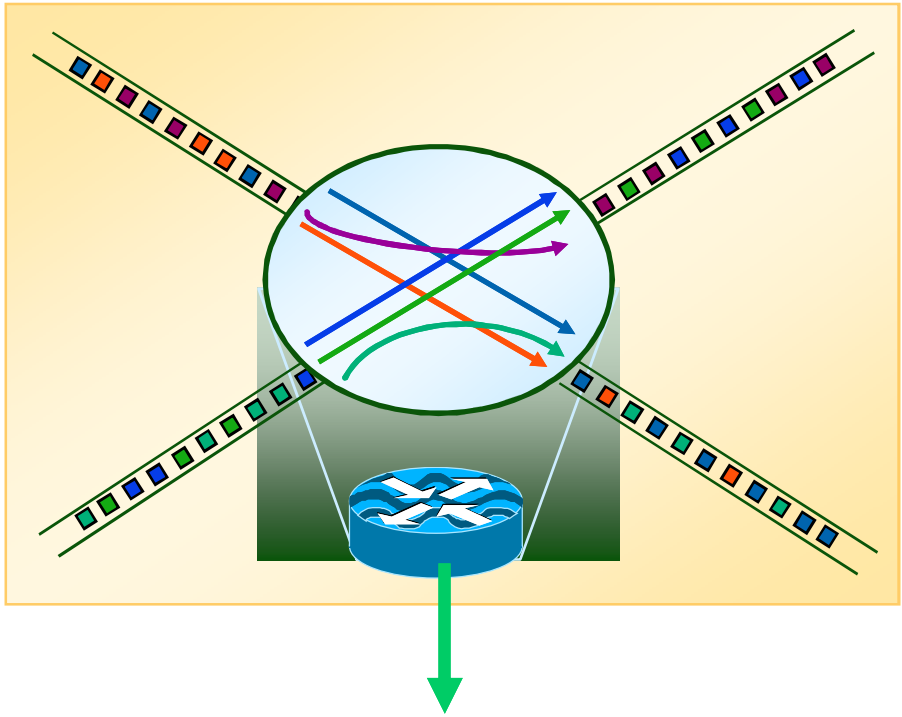




What is a NetFlow flow?

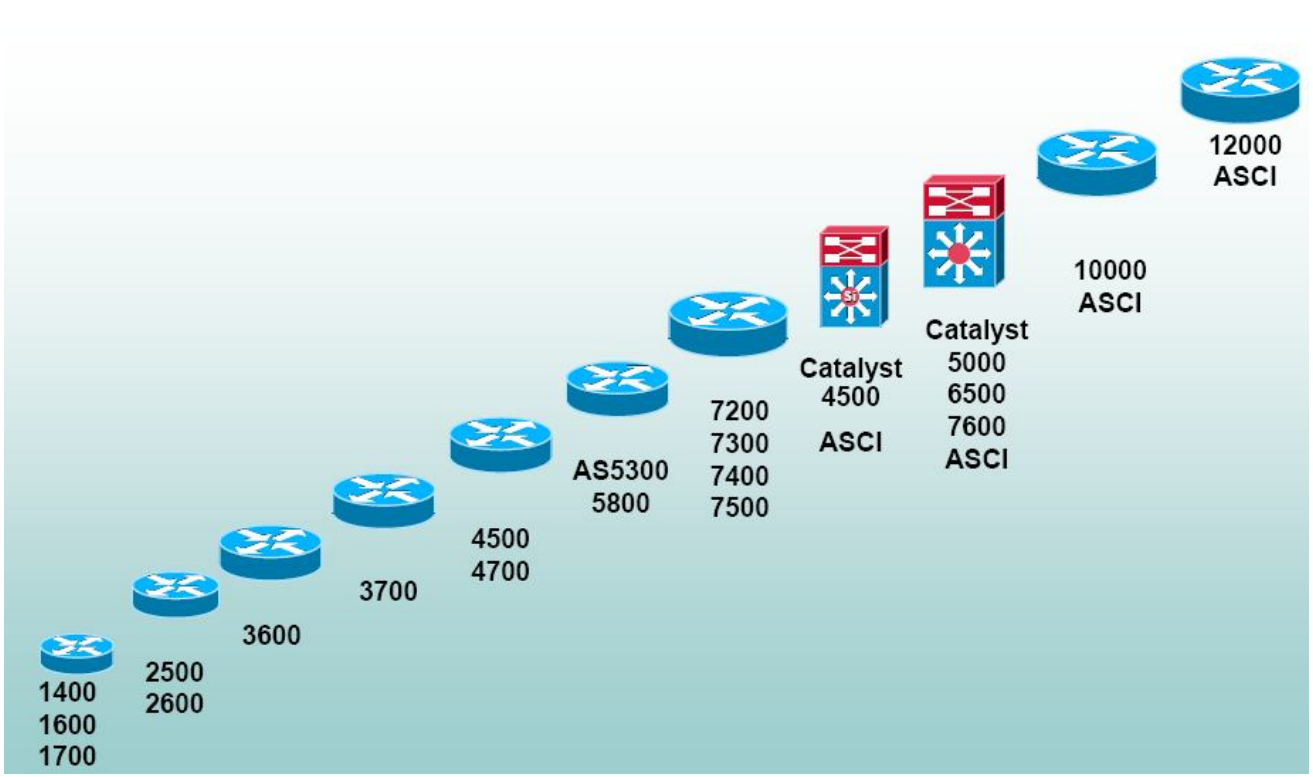
Unidirectional IP stream with unique:

1. Source IP Address
2. Dest. IP Address
3. Source Layer 4 Port
4. Dest. Layer 4 Port
5. Layer 3 IP Protocol
6. Packet Marking (ToS)
7. Input Interface



Router sends stats to a collector (Harvester) via UDP

NetFlow/IPFIX Platform Support



Passport 8600

NetFlow: Past, Present & Future

NetFlow

Cisco

IPFIX

Industry Standard

1996

Cisco developed
IO IOS®
NetFlow
as a switching
technology

Present

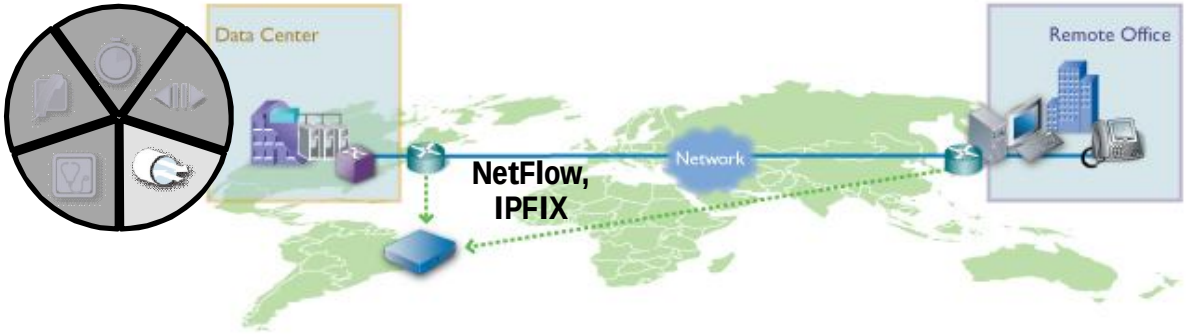
Provides a detailed view of
IP traffic without the need to deploy
Probes

Nortel and other vendors are using
IPFIX to provide the same type of
information technology

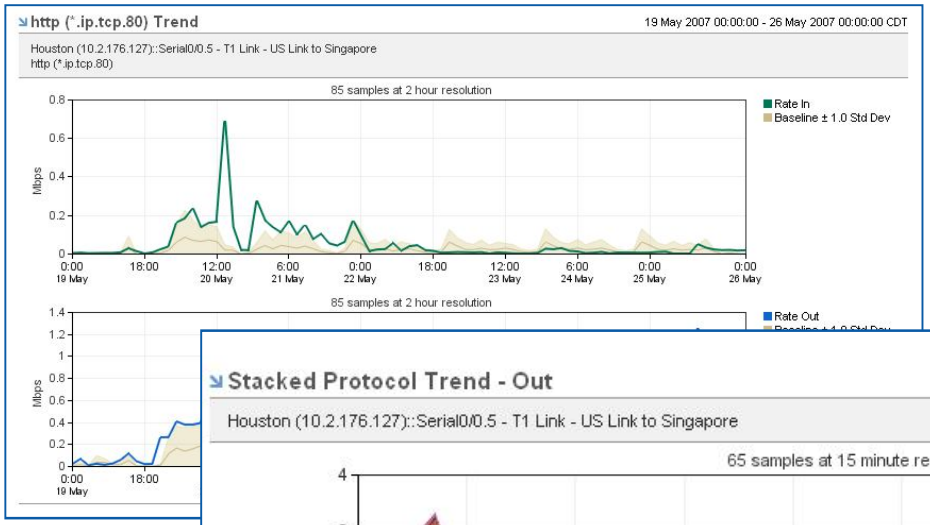
Future

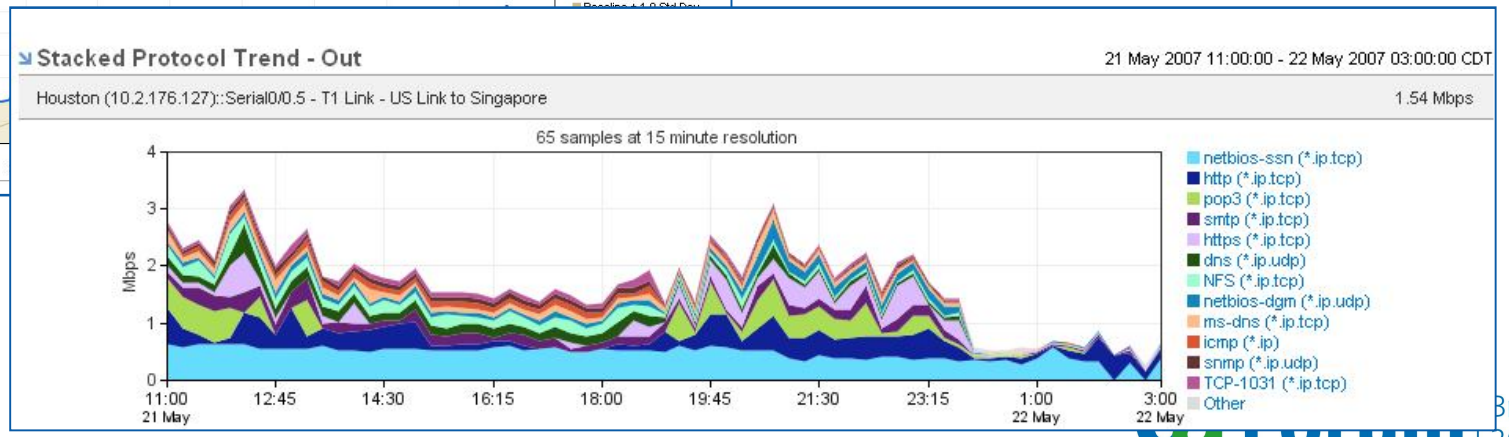
IPFIX as the
standard
in the industry

Network Traffic Analysis



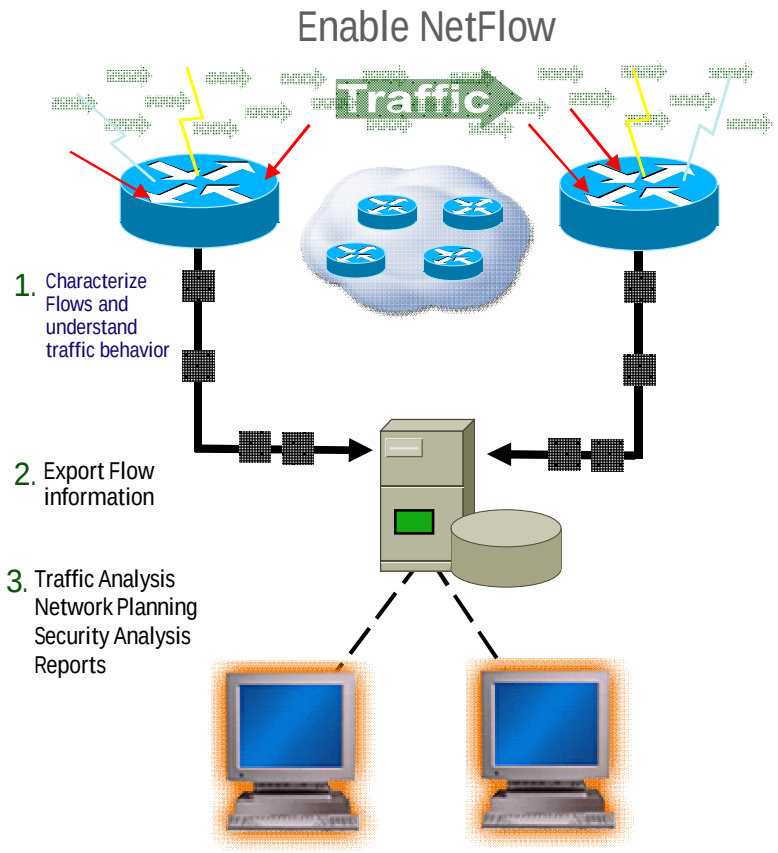
- ***Industry leader for flow-based monitoring***
- ***QoS traffic identification and configuration change validation***
- ***From real-time, enterprise-wide reporting to historical trending to detailed flow forensics***
- ***Network-focused behavior analysis***





How does ReporterAnalyzer help you?

- Make More Informed Capacity Planning Decisions and Infrastructure Investments
- Solve Performance Problems Faster
- Optimize the Network Infrastructure for Application Performance
- Enhance Security by Quickly Identifying and Classifying Attacks

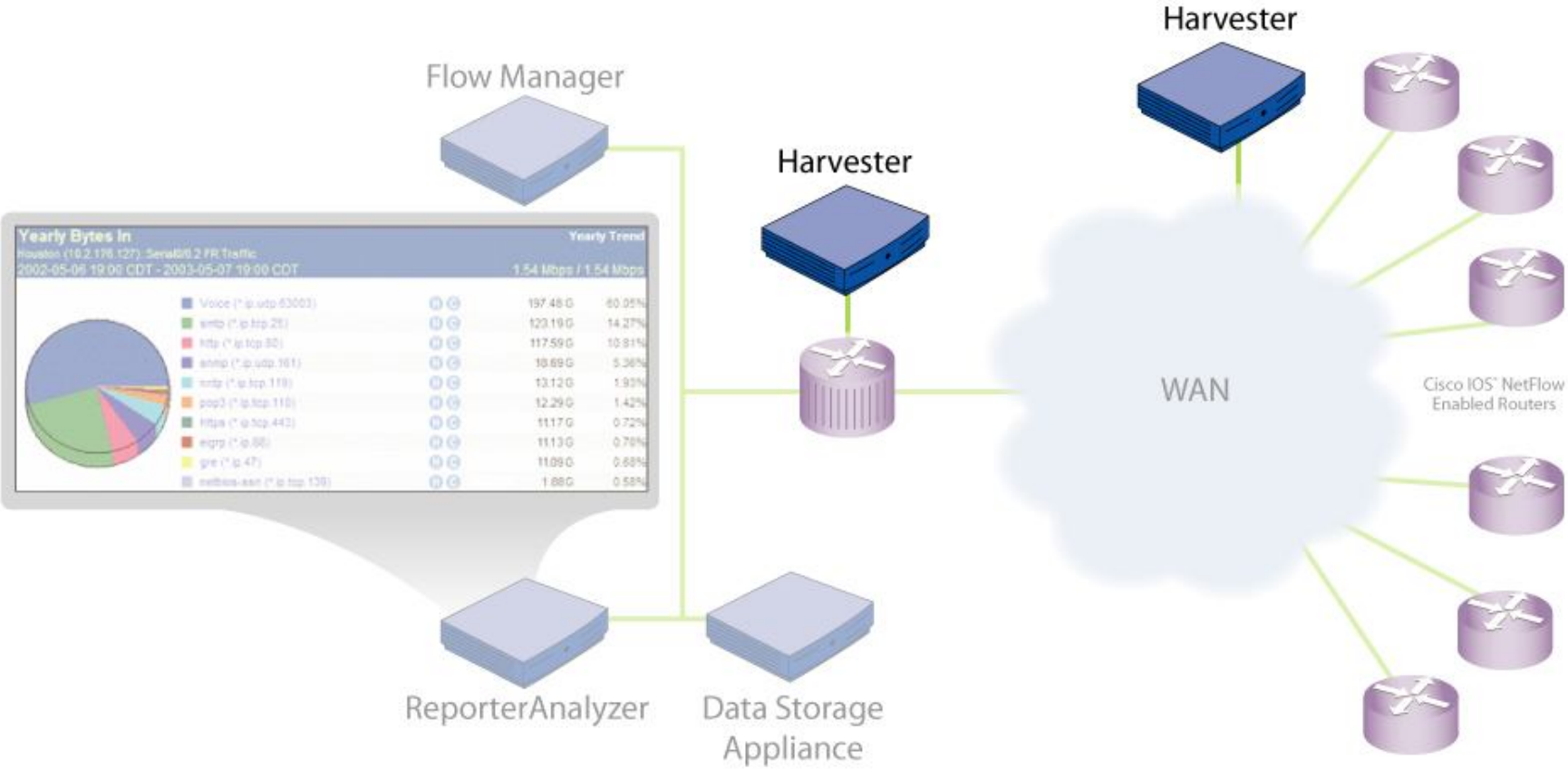


Monitoring

- Who are the users?
  - Top hosts
  - Top conversations
- Where do they go?
  - Intranet
  - Internet

- What do they do?
  - What applications
  - % of traffic
  - Usage patterns
- When are they on?
  - Days
  - Nights
  - Weekends

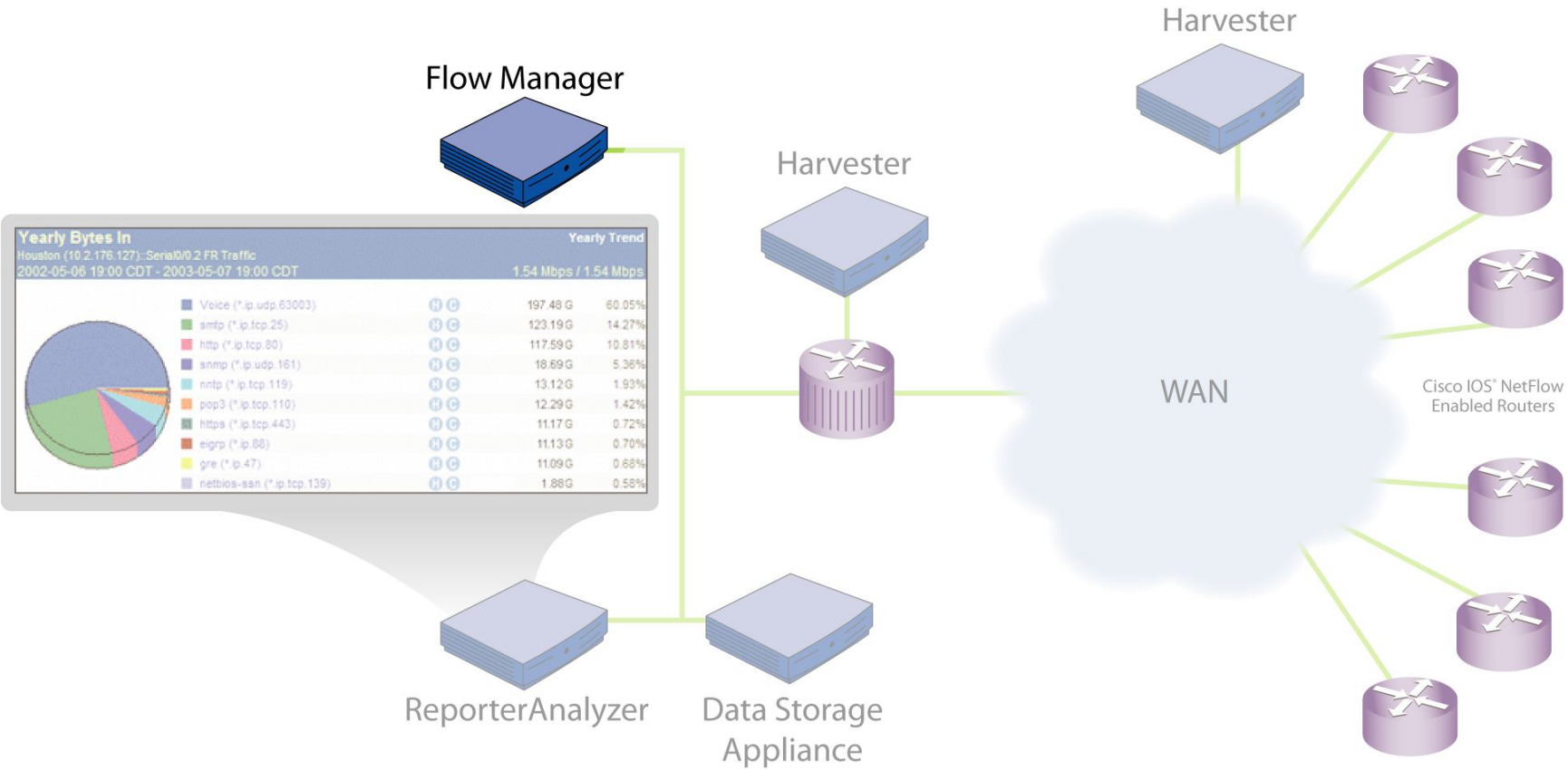
ReporterAnalyzer Components



Harvester

- Passively collects and distills flow data
- Stores real-time data and flow forensics data
- Supports up to 20 Routers or 1 million flows per minute

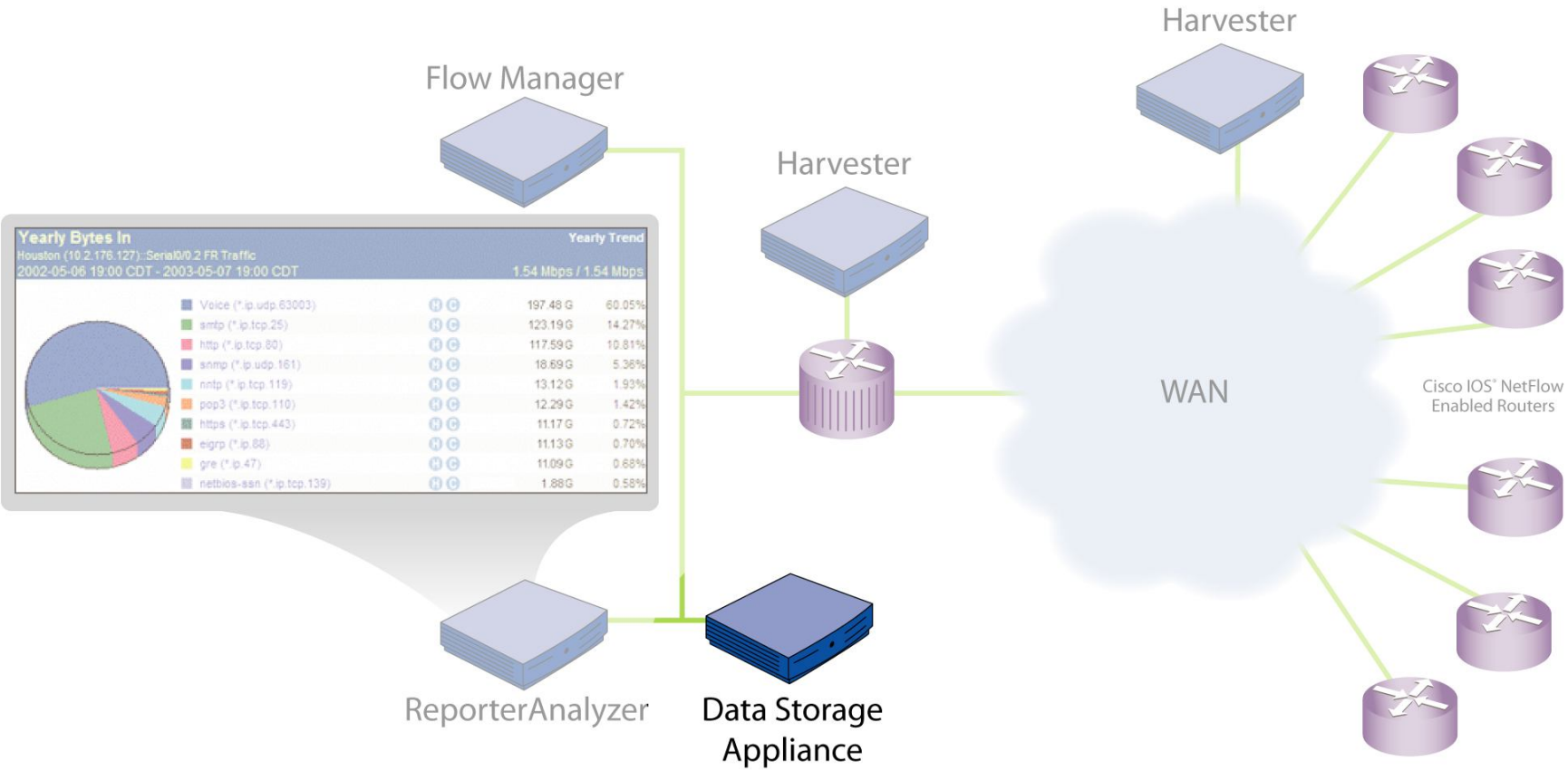
ReporterAnalyzer Components



Flow Manager

- Aggregates data from multiple Harvesters
- Supports up to 10 Harvesters
- Polls Routers for device names and interface descriptions

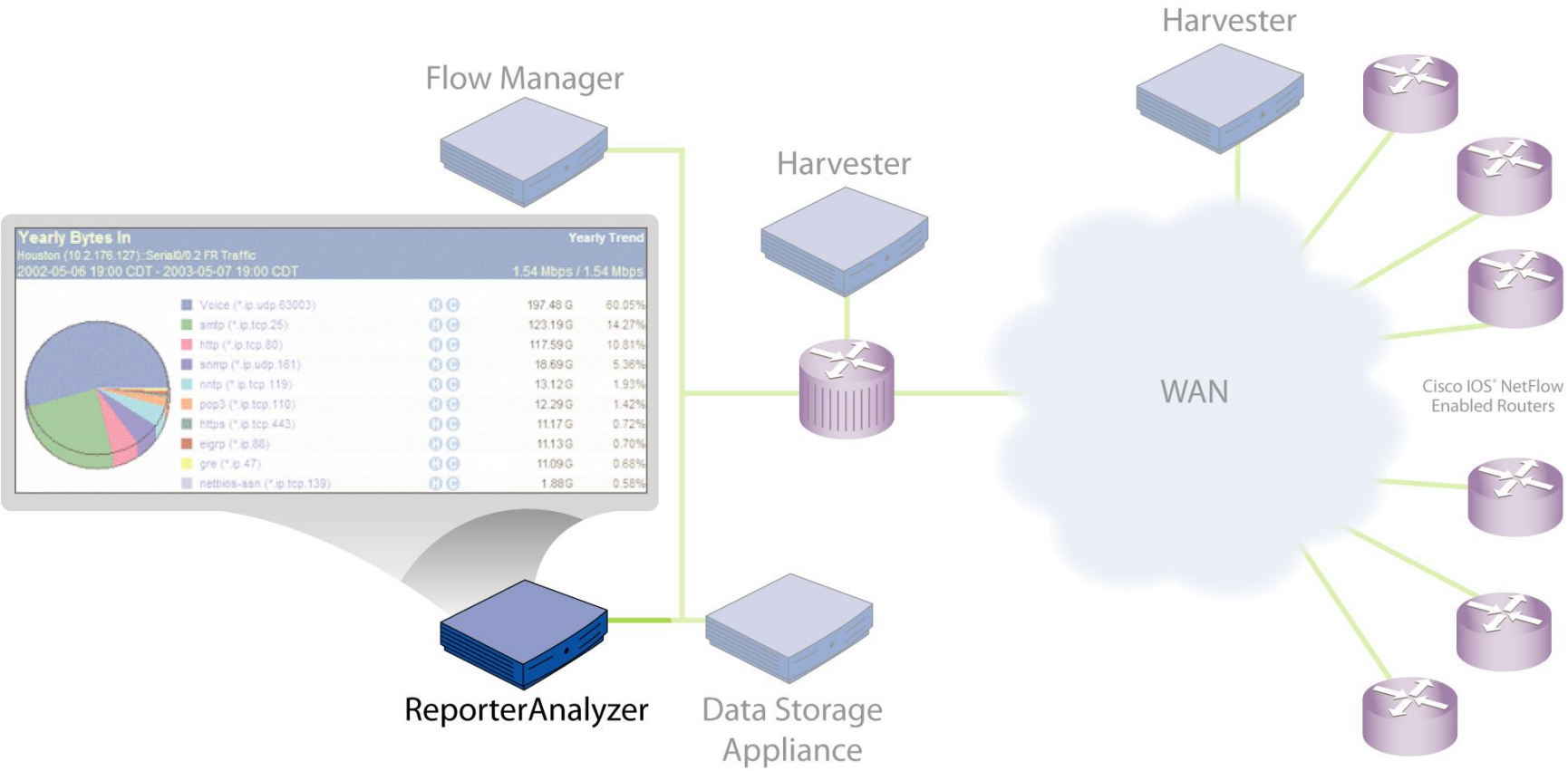
ReporterAnalyzer Components



DSA (Data Storage Appliance)

- Stores Data for up to 500 or 5000 Interfaces
- Stores protocol data 13 months; Host and Conversation data 2 months

ReporterAnalyzer Components



ReporterAnalyzer Console

- Provides web Interface to data
- Supports up to 10 Flow Managers

report types

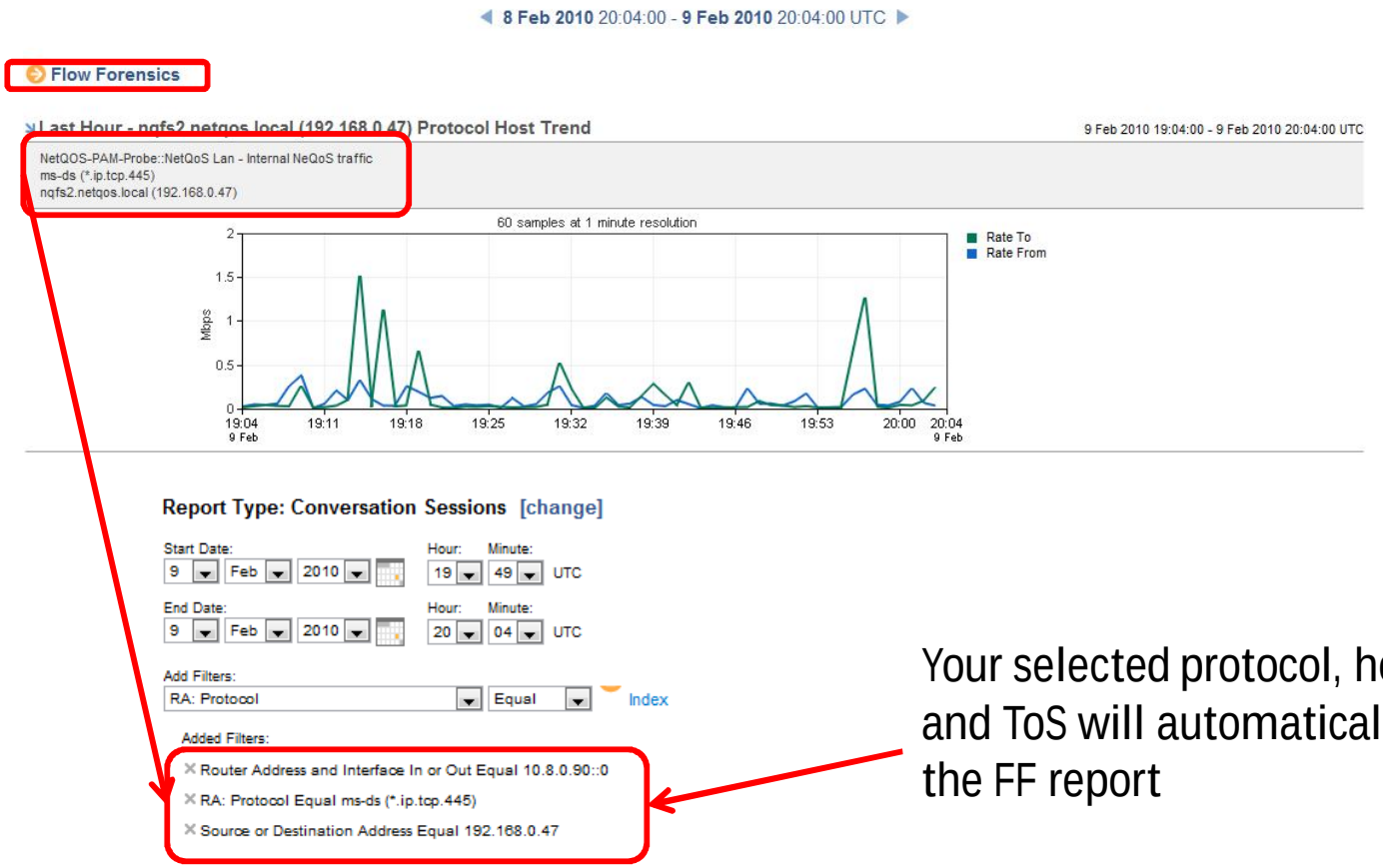
flow forensics

Flow Forensics

— Flow Forensics is the microscope, allowing you to zoom down to the raw flows
  - Data is queried from raw flow files stored at the harvester
  - Report on all hosts, protocols and conversations no matter how small
  - View additional details such as
    - » Source & Destination ports
    - » Packet count
    - » AS numbers
    - » IPv6 sessions
    - » TCP Flags
  - Examples of when to use FF:
    - Identify ALL hosts talking on a protocol
    - Identify all protocols that a host is using

Quickly Building FF Reports

— You can quickly build Flow Forensics reports using the link from the Interface Pages



Your selected protocol, host, conversation and ToS will automatically be built into the FF report

Flow Forensics

Flow Forensics provides the ability to drill into raw data flows.

Create New Report

Select a Report by clicking on the name.

Saved Report Folders

- Flow Forensics Reports

New | Rename | Delete

Reports (Contents of Flow Forensics Reports) New | Delete

Name	Description	Status	Status Message	Last Execution Time
20071109-1726 Conversations		Complete		9 Nov 2007 17:28:17 CST
20071109-2323 Source Address Peer Count		Complete		9 Nov 2007 23:29:51 CST
20071113-1225 Conversations		Complete		13 Nov 2007 12:27:40 CST
20071114-1407 Autonomous System Pairs (with Destination Network)		Complete		14 Nov 2007 14:15:53 CST
20071114-1520 Conversations		Complete		14 Nov 2007 15:22:20 CST

New | Delete

Report Results

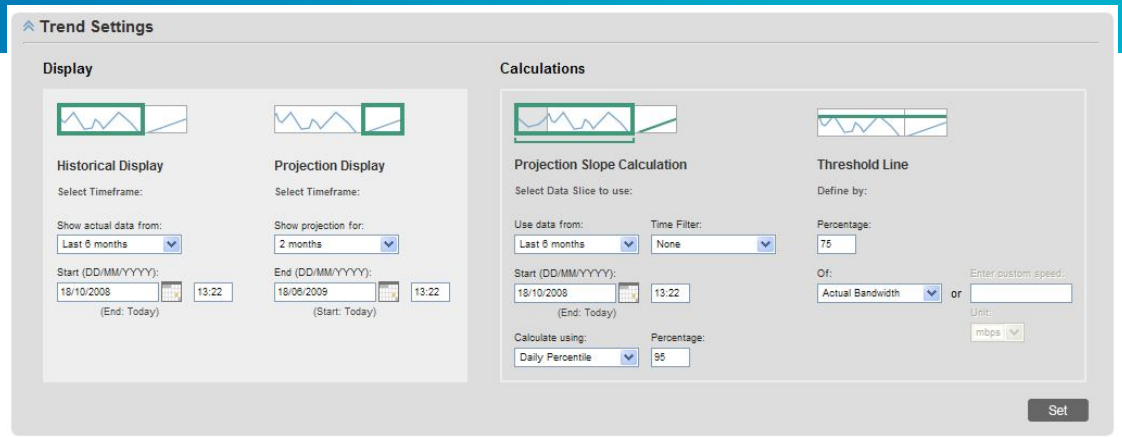
Report Results

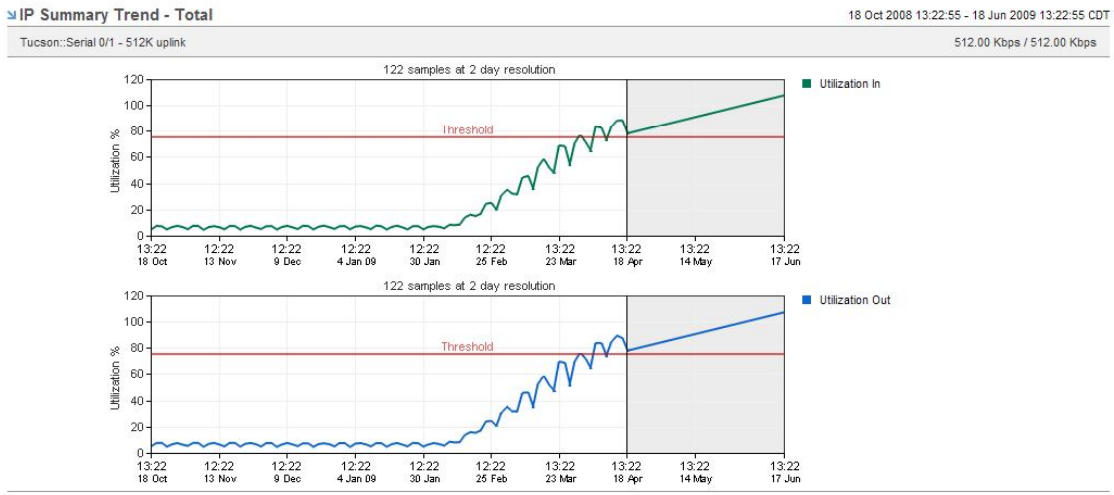
IP Protocol	Router Addr	Interface In	Src Addr	Src Port	Interface Out	Dest Addr	Dest Port	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
icmp (1)	10.168.13.5	Houston - Serial 2/0.1 - T1 Link	10.168.13.5	2816	104	10.1.79.170	4816	204.80 KBytes	228 bps	3.61 %	2	226	0.03 pkts/s	3.51 %
icmp (1)	10.168.13.5	Houston - Serial 2/0.1 - T1 Link	10.168.13.5	2816	104	10.6.63.127	4816	143.36 KBytes	159 bps	2.52 %	2	158	0.02 pkts/s	2.46 %
icmp (1)	10.168.13.5	Houston - Serial 2/0.1 - T1 Link	10.168.13.5	2816	104	10.13.211.52	4816	40.96 KBytes	46 bps	< 1.00 %	1	45	0.01 pkts/s	< 1.00 %

Capacity Planning

Capacity Planning

Allows for projections to be generated based on your actual network traffic.





IP Summary Table

18 Oct 2008 13:22:55 - 18 Jun 2009 13:22:55 CDT

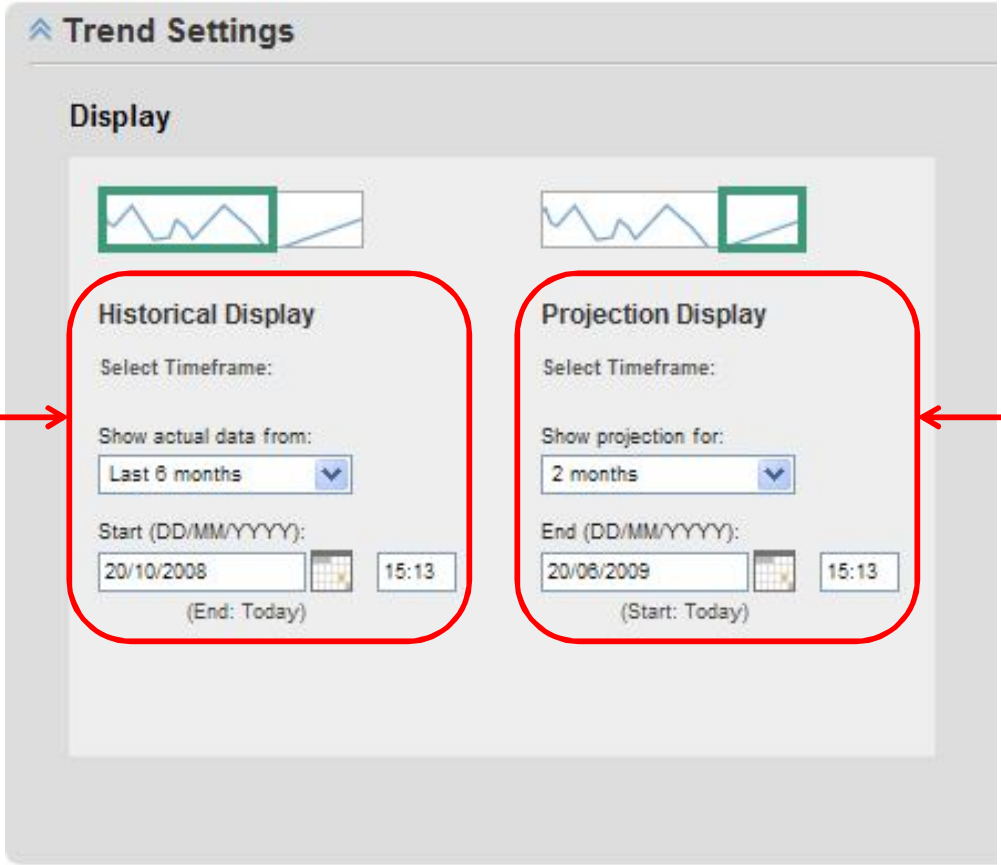
Tucson::Serial 0/1 - 512K uplink

Direction	Trend	Daily Change	Days Until Threshold	Date Of Threshold
In	↗	0.49 %	N/A	Passed
Out	↗	0.49 %	N/A	Passed

Capacity Planning – Display Settings

How much historical data the report will display.

This is NOT the computing time.

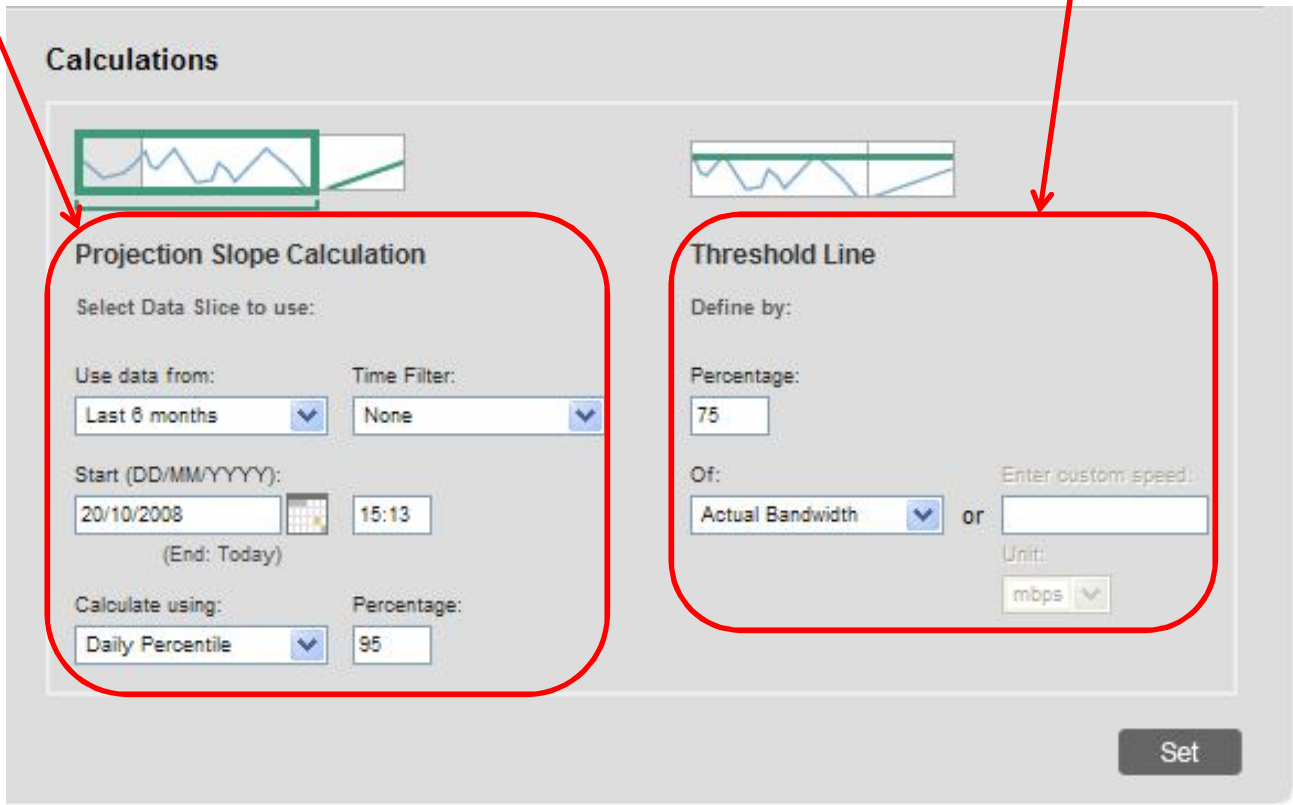


How much projection data the report will display.

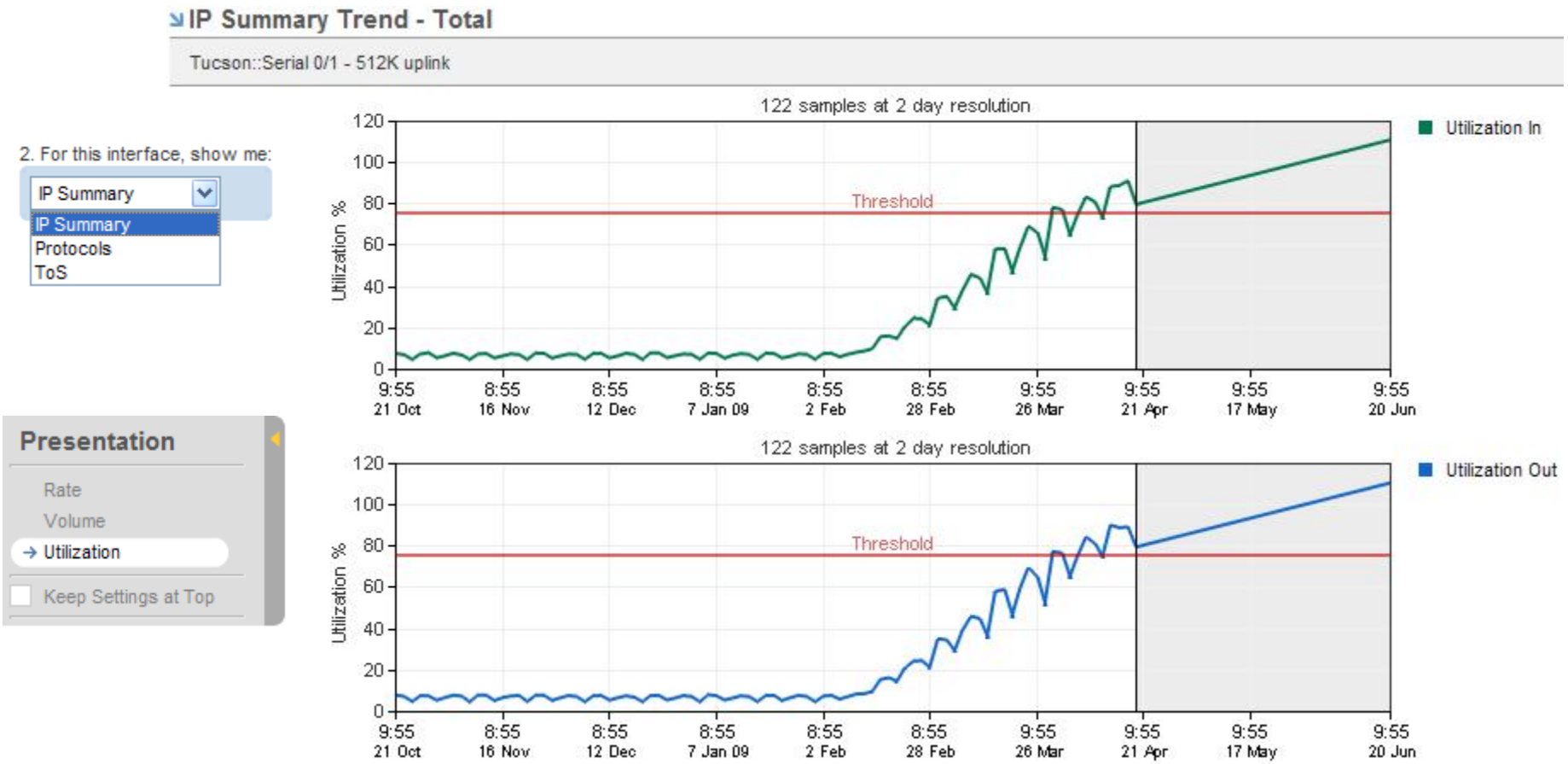
Capacity Planning – Calculations

This determines the time period for calculations but does not display in the report.

Determines the Threshold that will be displayed on the graph.



Capacity Planning - Views



Thoughts? Questions?

thank you

ca Forum | Bratislava 20. október