FOUNDRY NETWORKS

Network Visibility and Security with sFlow Technology

US

October 2003

Agenda

- **Foundry Overview**
- **Network Visibility and Security Solutions**
- **Application Infrastructure Security Solutions**
- **Customer Case Studies**
- **Summary**

Foundry Company Overview

World Headquarters
San Jose, California

- **Mission: Performance, High Availability, & Feature Leadership for Multilayer Switching (L2, L3, L4-7)**
- **Total Worldwide Customers: 8,000+**
- **Product & Corporate Awards: 50+**
- **2004 Revenue: ~$400 Million**

6th Consecutive Year of Net Profitability

Don't Plan for Yesterday. Plan for Today. Plan for Tomorrow.

FOUNDRY NETWORKS

Complete Layer 2/3 & Layer 4-7 Foundry Product Portfolio

FastIron Layer 2/3 Enterprise Switches

FastIron 400/800/1500

Edge and Workgroup

Power over Ethernet

FES2402-POE
FES4802-POE

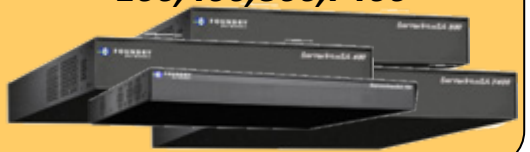
FastIron Edge 12GCF/2402/4802/9604

FI X-Series 10/100/1000 with 10 Gigabit Uplinks

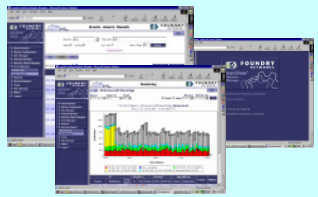
ServerIron Layer 4-7 Application Switches and Web Accelerators

ServerIron XL, GT-E, 450/850 and 100/400/800

ServerIronSA Web Accelerators 100,400,800,F400



IronView Network Management



BigIron Layer 3 Backbone Switches

BigIron Super-X/4000/8000/15000/MG8

NetIron Metro Routers

NetIron 400/800/1500/40G

FOUNDRY NETWORKS

Foundry Leadership and Innovation

Innovation	Year	Product
• 1st Layer 3 Switch	1997	NetIron
• 1st Gigabit Ethernet Switch	1997	FastIron
• 1st Shipping Layer 4-7 Switch	1998	ServerIron
• 1st High-Performance Chassis Family	1999	BigIron
• 1st 1000 Base T (1000Tx) Switch	2000	FastIron GoC
• 1st 10 Gigabit Ethernet switch	2001	BigIron
• 1st ASIC-based Real-time Monitoring	2002	JetCore
• 1st Terabit Architecture – Mucho Grande	2003	BigIron, NetIron
• 1st High Availability 10 Gig Layer 4-7 Switch	2004	ServerIron
• 1st 10 Gigabit Wire-Speed DoS Protection	2005	ServerIron

First with complete End-to-End Internet Router, Layer 2/3, and Layer 4-7 Application Switching and Security Solutions

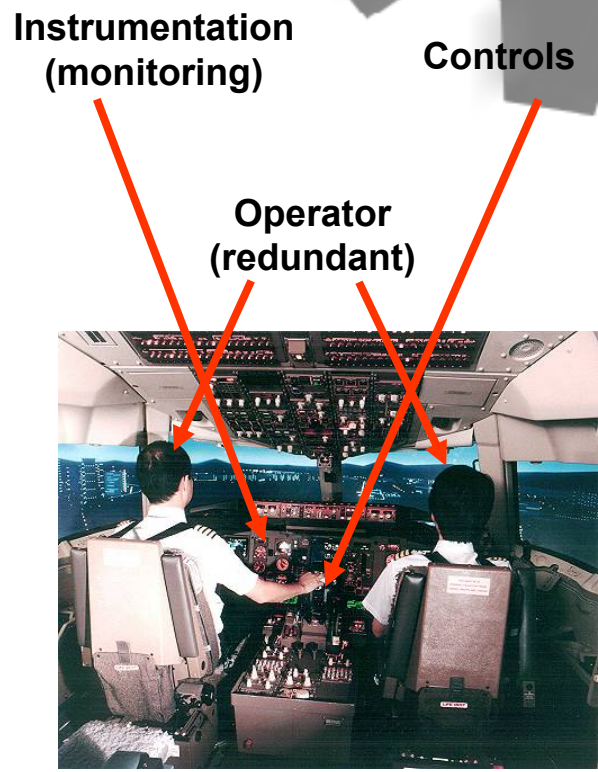
Agenda

- Foundry Overview
- **Network Visibility and Security Solutions**
- Application Infrastructure Security Solutions
- Customer Case Studies
- Summary

Why *Scalable Always-on* Network *Visibility?*

CIO and Network Operations Team's Requirements

CIO	Operations Team
• Ensure Worker Effectiveness • Minimize Downtime	• Rapid Diagnosis and Control of Problems
• Protect Information Assets	• Maintain Security
• Conform with Regulations	• Enforce Policies
• Control Cost of Ownership	• Ease of Management
• Create Additional Business • Better ROI	• Ensure Network's Readiness for New Applications • Plan and Grow On-Demand
• Track and Bill for Usage	• Usage Tracking



Requires Scalable Always-on Visibility

Network Visibility and Security Challenges

- **How do You Know Your Network is Secure?**
  - Only with a Traffic Monitor Hooked at Every Point
- **Existing Network Security Is Insufficient**
  - Most CIO Questions Unanswered
  - Wireless and Remote Access Create New Problems
- **Traditional Network Traffic Monitoring**
  - High Cost (No ROI Justification)
  - Impacts Performance and Business Operations
  - Limited Visibility – Can't Look Inside Truck
  - Requires Large Operations Staff to Manage

FOUNDRY NETWORKS

sFlow Traffic Monitoring Solution

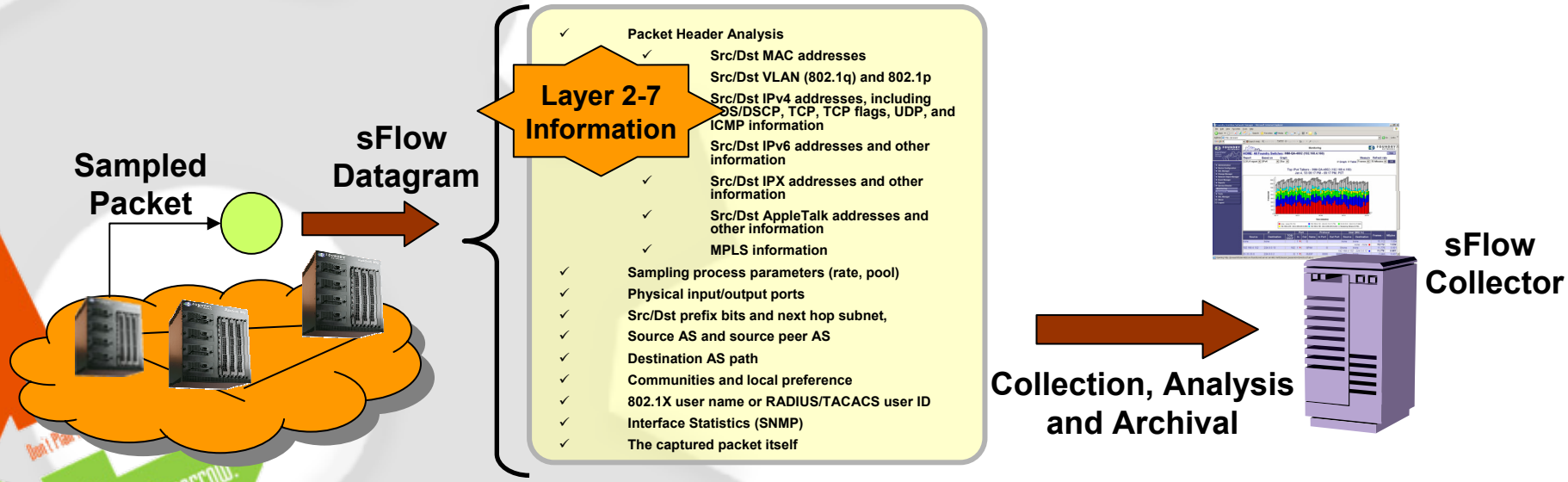
- **Uses Traffic Sampling for Monitoring and Accounting**
- **Gathers Data on All Traffic Flows on Every Port**
  - Provides Detailed Information about Flows
- **Exports Flow Information in Real Time to Collector**
  - Collector Archives Data and Provides Reports On-Demand
- **Wire-Speed Accounting and Performance (Even up to 10G)**
  - Replaces Guesswork with REAL Data
- **Standards Based and FREE!**
  - Embedded in Switch ASIC

FOUNDRY NETWORKS

sFlow (RFC 3176)

Embedded Traffic Monitoring for Switched Networks

- **Statistical Sampling Technology Delivers Visibility to All Traffic Flows**
  - Layer 2 through 7 visibility and analysis
- **Scales with Network Size and Speeds with Zero Performance Impact**
  - No other Technology can Scale to GbE and 10 GbE rates
- **Embedded implementations available today – Free!**



sFlow Technology – RFC 3176, An Open Standard for Network Traffic Accounting

- Statistical Sampling Technology
  - HP–patented and proven technology (over 10 years) that employs "Statistical Packet Sampling" and SNMP data to monitor network flows in a network.
  - Most "Packet Sampling" implementations just use information within an IP packet (e.g., what about VLAN and SNMP information).

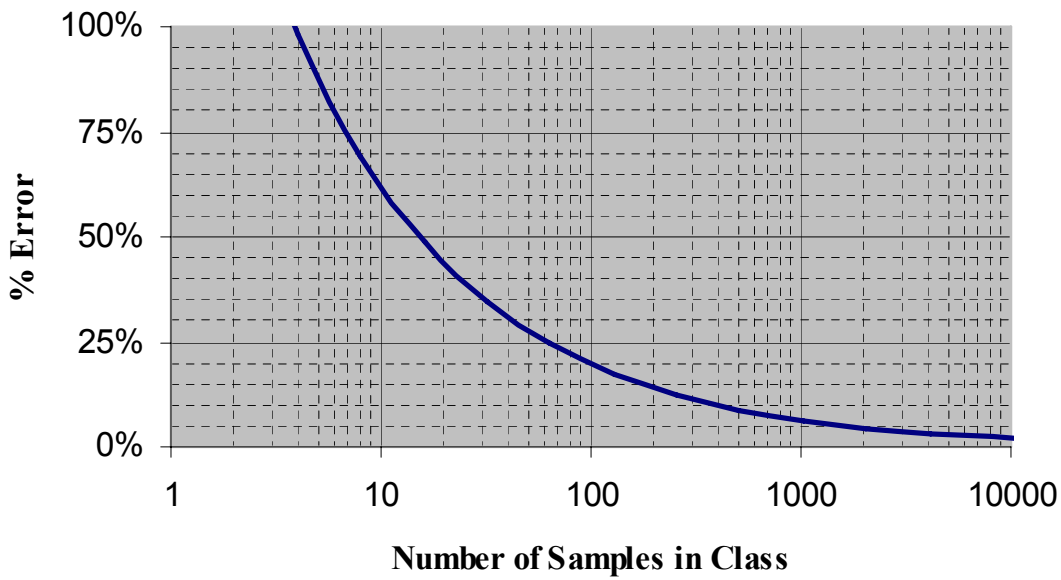
- What is RFC 3176 – sFlow Technology
  - Technology built by InMon Corporation
  - sFlow is a "Statistical Sampling Technology" – an Open Standard
  - sFlow delivers full L2-L4 network-wide traffic flow information

sFlow Accuracy

Estimating Traffic per Protocol

Total number of frames (interface counters) = N
Total number of samples received = n
Number of samples in class = c
Number of frames in the class estimated by:

$$N_c = \frac{c}{n} \cdot N$$

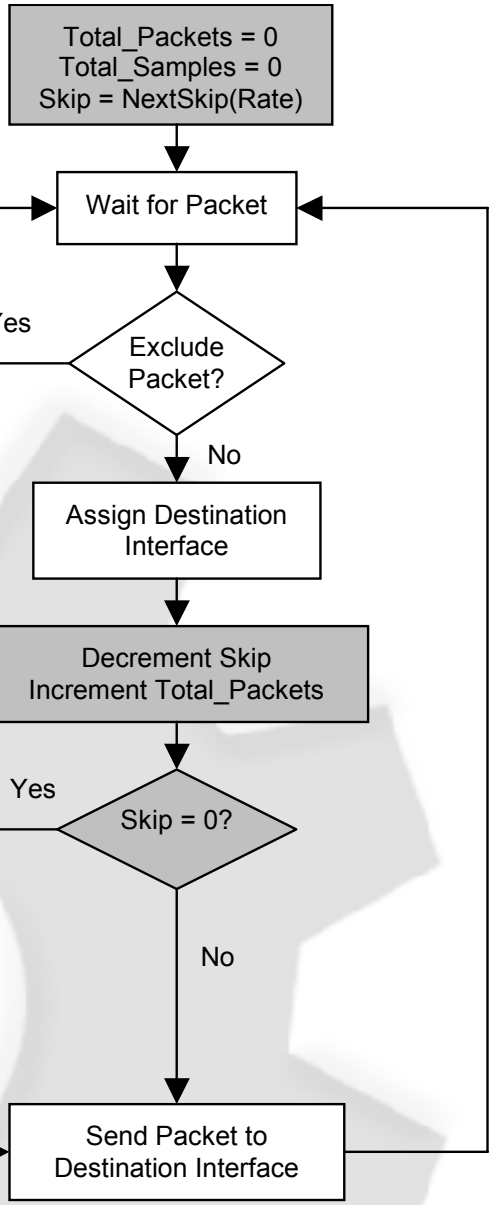


$$\%error \leq 196 \cdot \sqrt{\frac{1}{c}}$$

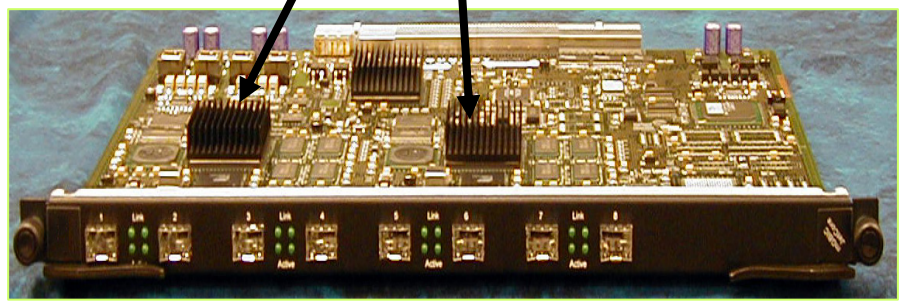
%error decreases by increasing number of samples:

- longer aggregation period
- increased sampling rate
- higher utilization

Packet Sampling Algorithm



Packet Sampling Algorithm Built within the ASIC for Hardware-based Network Traffic Accounting



Plan for Today. Plan for Tomorrow.

FOUNDRY NETWORKS

sFlow Answers Critical Questions Quickly

- **Security Breaches and Virus/Worm Spreads**
  - Identify Who Caused it and Where in Seconds
- **Unauthorized Users and Devices**
  - Where are They and What are They Doing?
- **Hosts and Applications Causing Problems**
- **Network Congestion Points**
- **Capacity Utilization and Availability**
- **Complete Network Activity End-to-End**

FOUNDRY NETWORKS

Why sFlow vs. Alternatives?

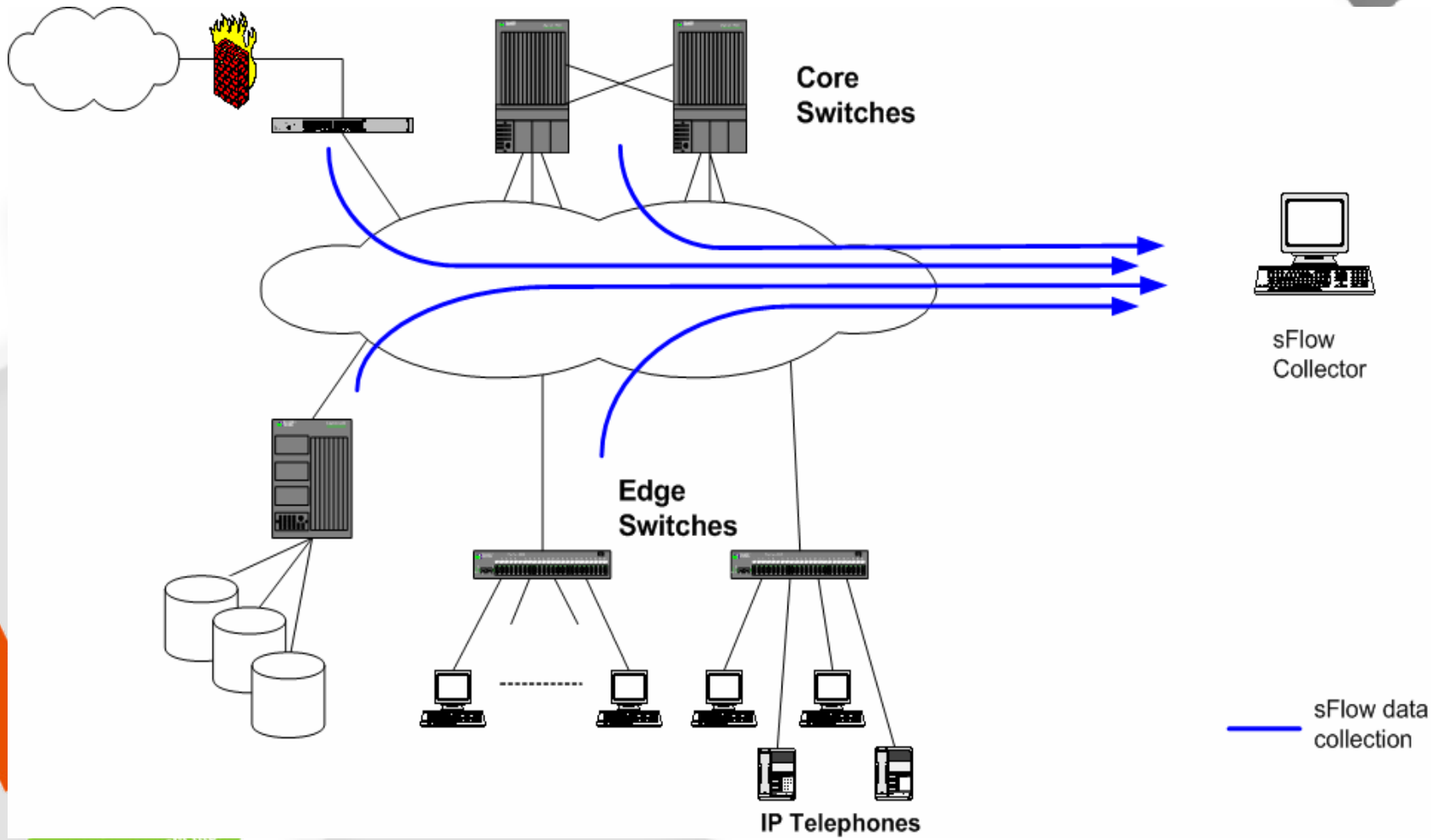
- **Standards Based Solution**
- **Industry's Only Pervasive Wire-Speed Monitoring Solution**
  - Other Technologies Don't Scale to Gigabit and 10 Gigabit Rates
- **Future Proof – Supports All Protocols and Applications**
- **Highest ROI – ZERO Cost**
- **Application Level Visibility – Not Just Network Level**
- **Leverages External Server-Based Collectors**
  - No Extra Expensive On-Device Modules

FOUNDRY NETWORKS

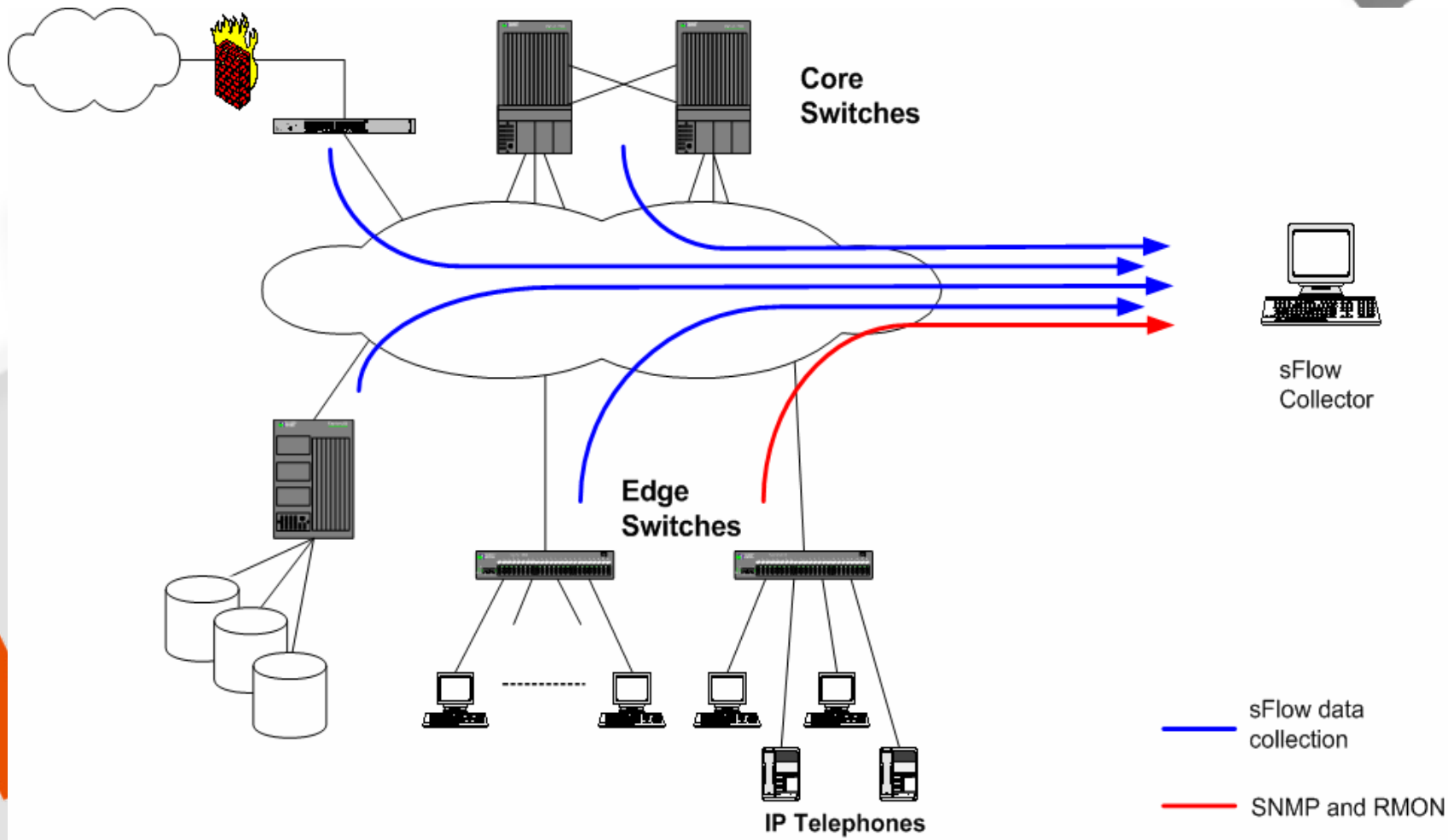
What is the Collector/Management System?

- The sFlow datagrams (sFlow samples) are sent to a central collector, located anywhere on the network. Systems are PC based.
- Management system displays real time view of data, with provision to drill down for additional details.
- Multiple viewing options can present the data in any number of ways for investigation and analysis.
- Data is concurrently captured and stored in a central "history" database.
- Ad-hoc queries for operational or business analysis can be made on the historical data.

Network-wide Visibility with sFlow

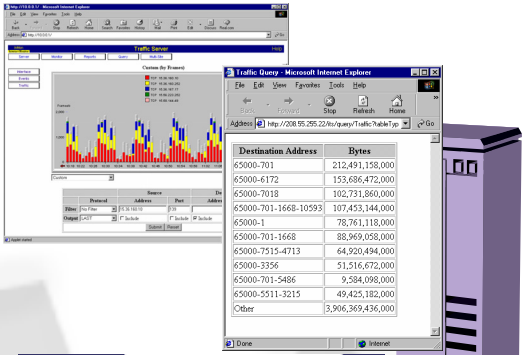


Existing Network Management Technologies are also Supported

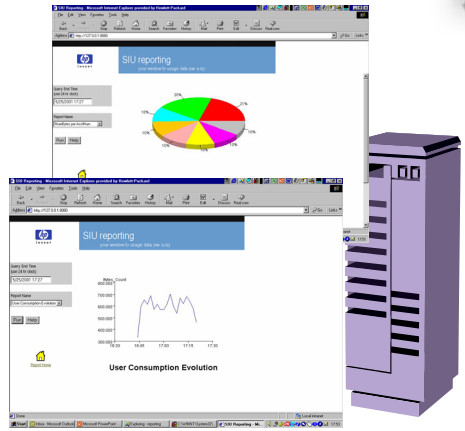


sFlow Management Systems

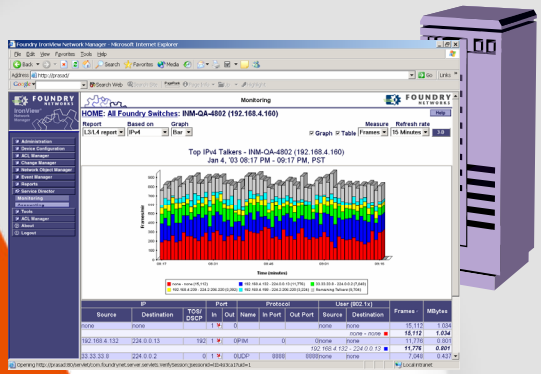
sFlow collection and presentation

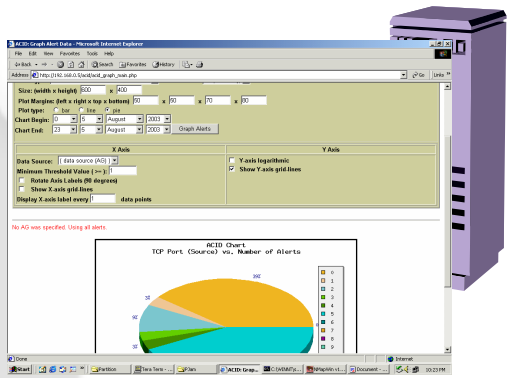


InMon internet monitoring

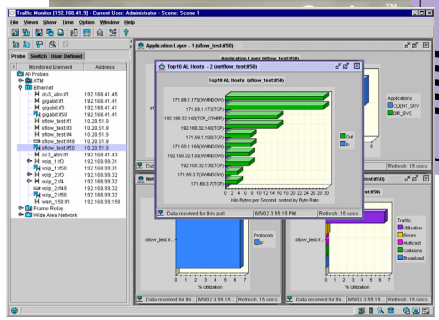


hp IUM invent





NetScout.



FOUNDRY NETWORKS IronView Network Manager

INM

Plan for Today. Plan for Tomorrow.

SNORT

FOUNDRY NETWORKS

Identifying and Mitigating Network Bottlenecks

Step 1: Profile congested segments

Congested Segment Report

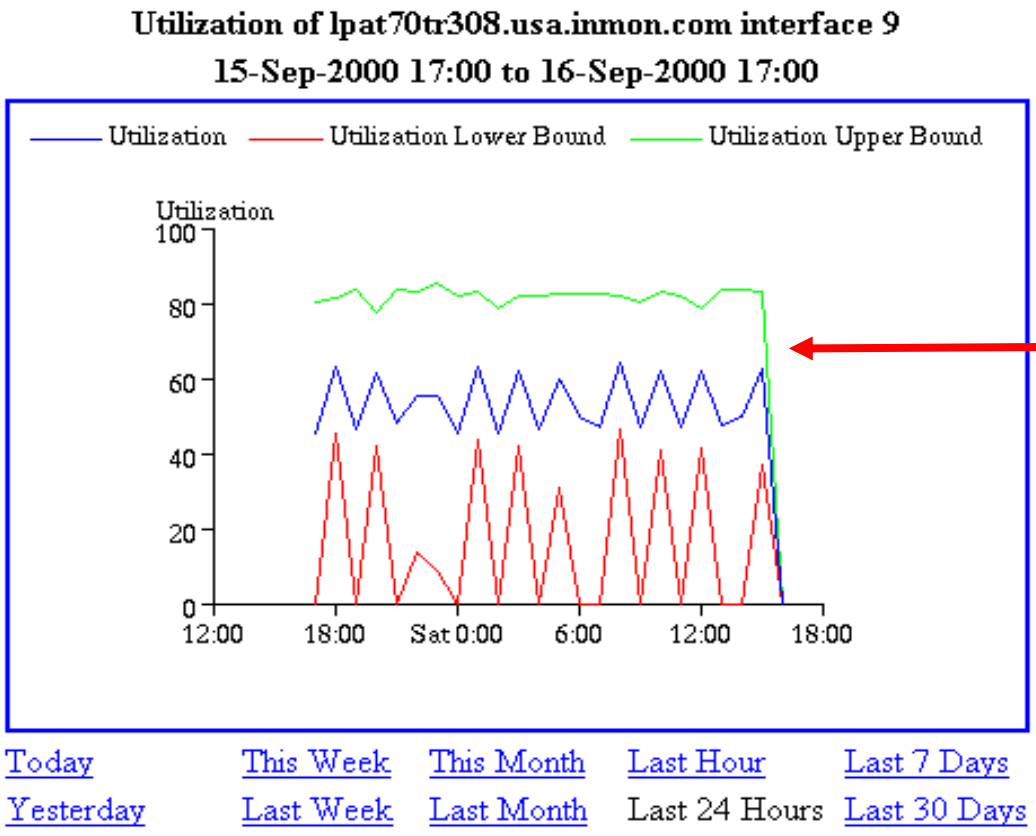
15-Sep-2000 16:00 to 16-Sep-2000 16:00

Location	Utilization		Sources	Time		
	Mins./Day	Peak		Latest	Earliest	Hour of Day
WAN Links 85.192.44.0 85.192.44.35 9	1,325.00	97%	IP:197.164.196.101 7% IP:10.162.248.166 6% IP:10.119.241.11 5%	Sat 16-Sep-2000 15:59	Fri 15-Sep-2000 16:00	
Presidio Office lp2m11tc1212.usa.inmon.com 24	1,283.00	22%	IP:10.163.32.17 73% IP:10.163.32.79 20% IP:10.163.32.77 3%	Sat 16-Sep-2000 15:59	Fri 15-Sep-2000 16:00	
Presidio Office lpat70tr308.usa.inmon.com 9	1,148.00	85%	IP:10.163.32.36 96% IP:10.163.32.139 1% IP:10.167.248.44 0%	Sat 16-Sep-2000 15:59	Fri 15-Sep-2000 16:11	
Embarcadero R&D	793.00	45%	IP:10.167.224.106 45% IP:10.167.224.81 35%	Sat 16-Sep-2000	Fri 15-Sep-2000	

Traffic is peaking at 85% utilization, and a single source is responsible for 96% of traffic during busy periods.

Identifying and Mitigating Network Bottlenecks

Step 2: Investigate trending on busy segment



The utilization for the congested link averages at around 55% and that it exceeds 80% approximately 3 minutes in every hour.

Conclusion: Chronic problem to address.

Identifying and Mitigating Network Bottlenecks

Step 3: Obtain details of host responsible for majority of traffic on segment

Host Report For 10.163.32.36

The following table presents information derived from observing network traffic. The addresses contained in the table have all been seen as source addresses in network packets transmitted by the specified host.

Addresses	
IP	10.163.32.36

The following reports provide real-time traffic information for the selected host (provided the port connecting the host to the network can be located).

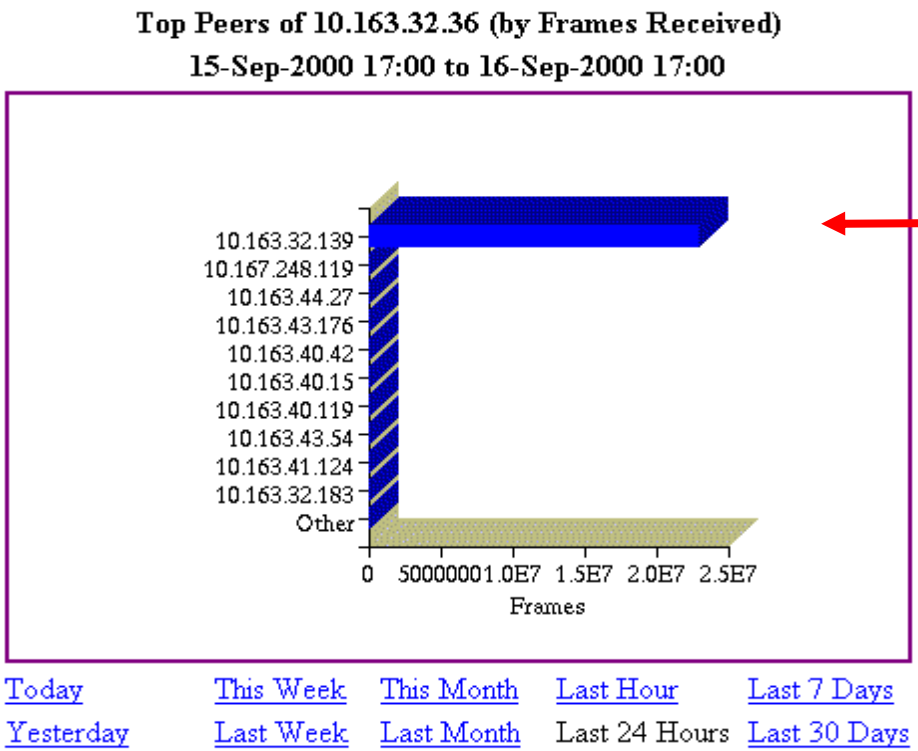
- Monitor selected host's traffic.

The following reports profile the specified host by examining historical network traffic.

- Peers addresses of hosts communicating with the selected host.
- TCP Services Provided services provided by this host to others.
- TCP Services Consumed services consumed by this host.
- UDP Services Provided services provided by this host to others.
- UDP Services Consumed services consumed by this host.

Identifying and Mitigating Network Bottlenecks

Step 4: Understand where traffic from this host is going

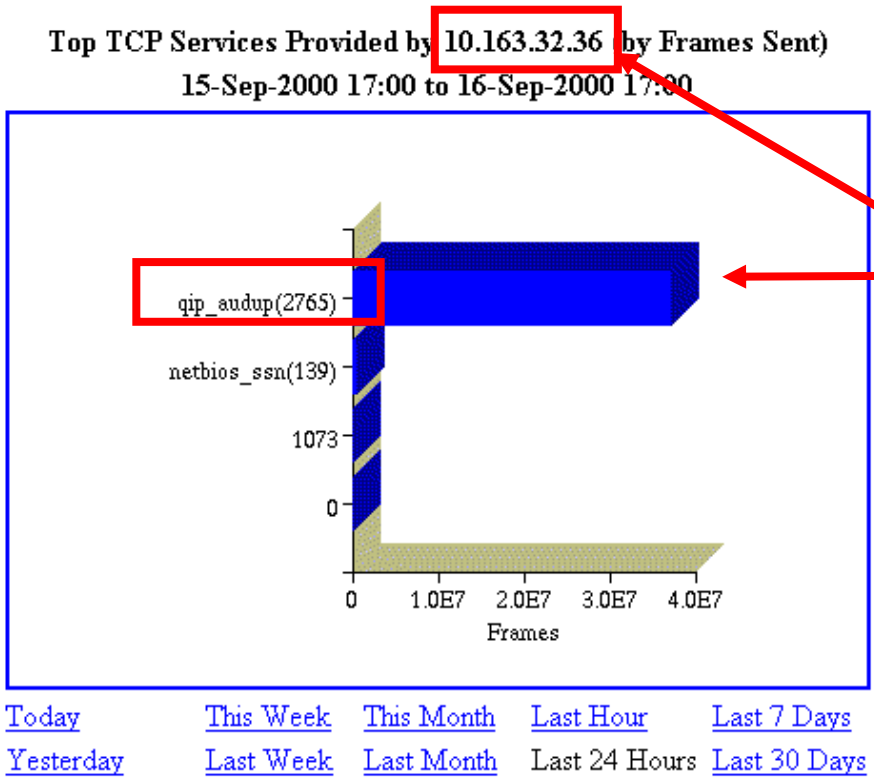


Discovery: Majority of traffic is two hosts talking to one another (10.163.32.36 sends most of its traffic to 10.163.32.139).

Possible Resolution: Ensure that these two machines are connected to the same switch.

Identifying and Mitigating Network Bottlenecks

Step 5: Profile the application(s) causing this traffic



10.163.32.36 is generating traffic primarily to port 2765.

Possible Resolutions:

- Lower the priority for traffic to port 2765
- Set rate limiting.

FOUNDRY NETWORKS

Thank You!