



Ensuring Service Quality & Security in Converged Networks Through Proactive Monitoring



Rahul Vir
Product Line Manager
Foundry Networks
rvir@foundrynet.com

Agenda

Monitoring of Video Networks

Monitoring MPLS VPN Networks

Monitoring Other Services

Traffic Management Example

Summary

Introduction

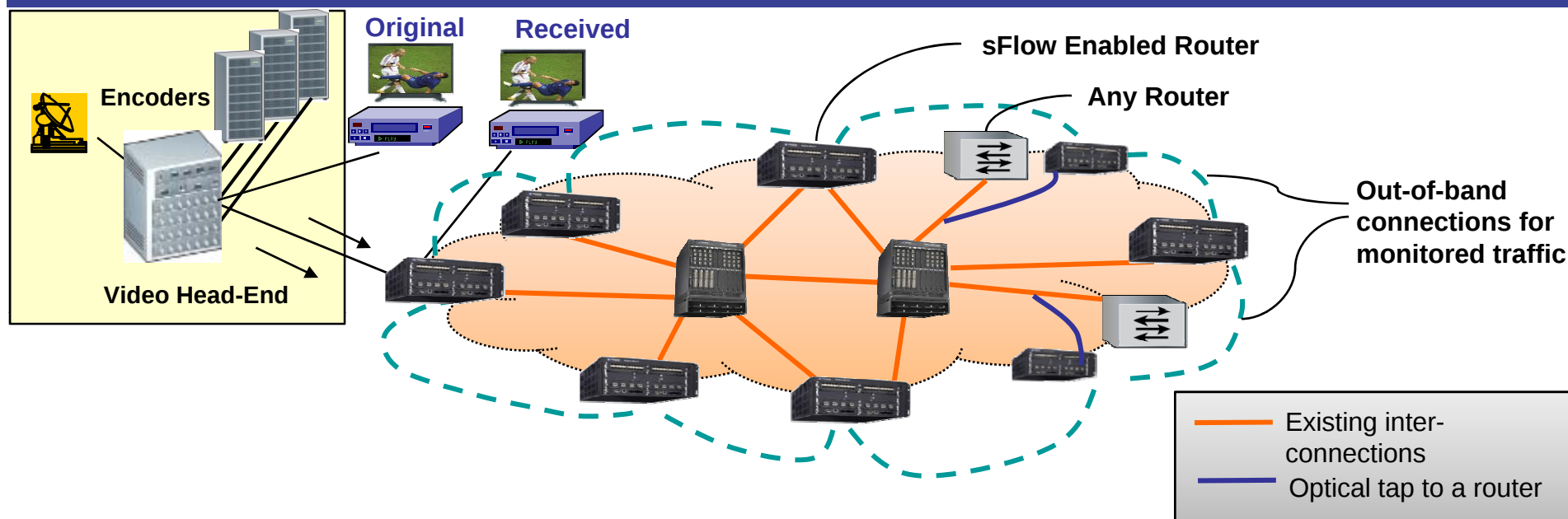
- ❁ Converged Networks offer residential triple-play and business services over a single infrastructure
- ❁ Diverse services require widely different service guarantees
 - Video: VoD, IPTV
 - Voice over IP
 - High Speed Internet Access (HSIA)
 - Layer 2 and Layer 3 VPNs
- ❁ Monitoring in converged networks offers many challenges
 - Multiple targeted solutions for each service not practical
 - Providers wary of destabilizing network
 - Need standards based tools to avoid vendor lock-in
- ❁ Proactive monitoring offers a single solution
 - Enables predicting, detecting and offers tools to isolate potential problems
 - Transparent to customer traffic with not overhead on management processor



Monitoring of Video Networks

Closed Loop Network Visibility

Video Monitoring



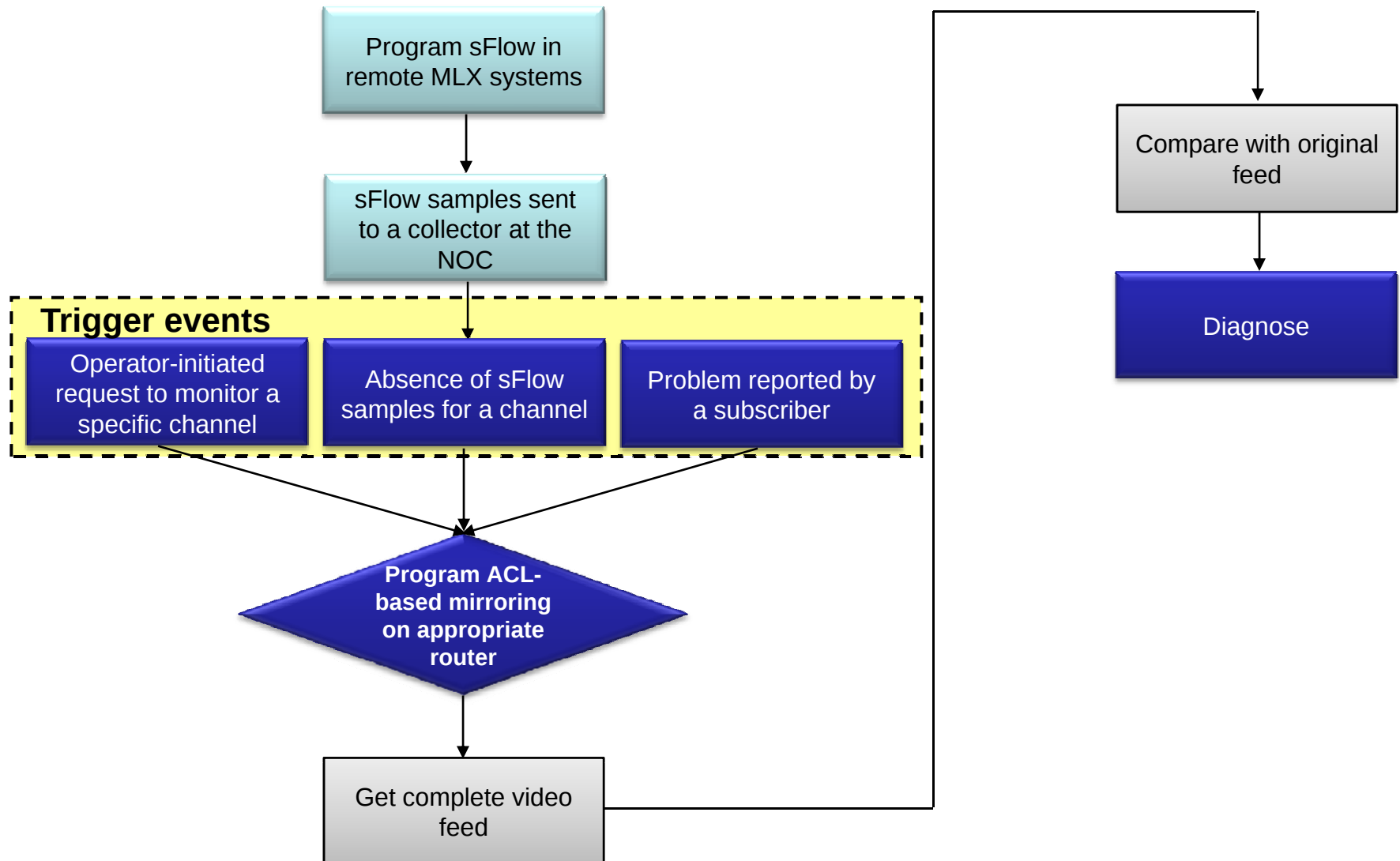
- ❁ Need sFlow enabled routers for monitoring video feeds
- ❁ Passive optical tap when routers do not support sFlow
- ❁ Routers at the NOC for analysis
- ❁ Connectivity for sFlow routers can be in-band or out-of-band
- ❁ Standalone management software for closed-loop analysis
 - Verifies video flows in real-time

Closed Loop Network Visibility

How it works

- ❁ Real-time collection and evaluation of sampled traffic
- ❁ Uses sFlow for a reverse feedback path between the location being monitored and the NOC
 - Sample rate can be as aggressive as 1 in 512
 - sFlow collector running on a server in the NOC
- ❁ Events below trigger the policy management system to request a full replica of the video stream :
 - Absence of sFlow packets for a certain duration OR
 - An operator initiated operation OR
 - A subscriber reported problem
- ❁ Policy Manager activates replication through ACL-based mirroring
- ❁ Router encapsulates the mirrored traffic into a point-to-point Virtual Leased Line to transport the video stream to the NOC
 - To minimize setup time, the VLL is established a priori from each remote router to the router in the NOC

Flowchart of Operations



sFlow Overhead In A Network

Just 0.02% overhead even at aggressive sampling rates!

sFlow overhead calculator

Note: Cells in yellow are configurable values; the rest of the cells are either fixed or derived from other cells

Network assumptions:		
Interface Rate (IR):	10	Gbps
Input Packet Size (IPS):	1362	bytes
Interface MTU (MTU):	1,518	bytes
Network Traffic Rate (NTR):	917,768	pps

sFlow computations:		
sFlow datagram transport overhead (SDTO):	24	sFlow
	8	UDP
	20	IP
	14	MAC header
Total:	66	bytes
Interface Counters Sample (ICS):	108	bytes
Flow Sample Header Bytes (FSHB):	128	bytes
Samples Per Datagram (SPD):	11	
Interface Counters Polling Rate (ICPR):	1/30	
Packet Sampling Rate (PSR):	1/512	

Calculation per 10-GbE interface:		
Interface counter bits per second (ICBPS):	$ICS * 8 * ICPR =$	28.80
Flow Samples Per Second (FSPS):	$NTR * PSR =$	1792.5
Flow Datagram Bits Per Second (FSBPS):	$(ICBPS + FSPS * FSHB * 8 + SDTO * 8) \text{ bps}$	
	1,836,092.78 bps	

Overhead of sFlow therefore is $FSBPS / (IR * 10^9)$
0.02% of interface rate

Benefits of Solution for Video Monitoring

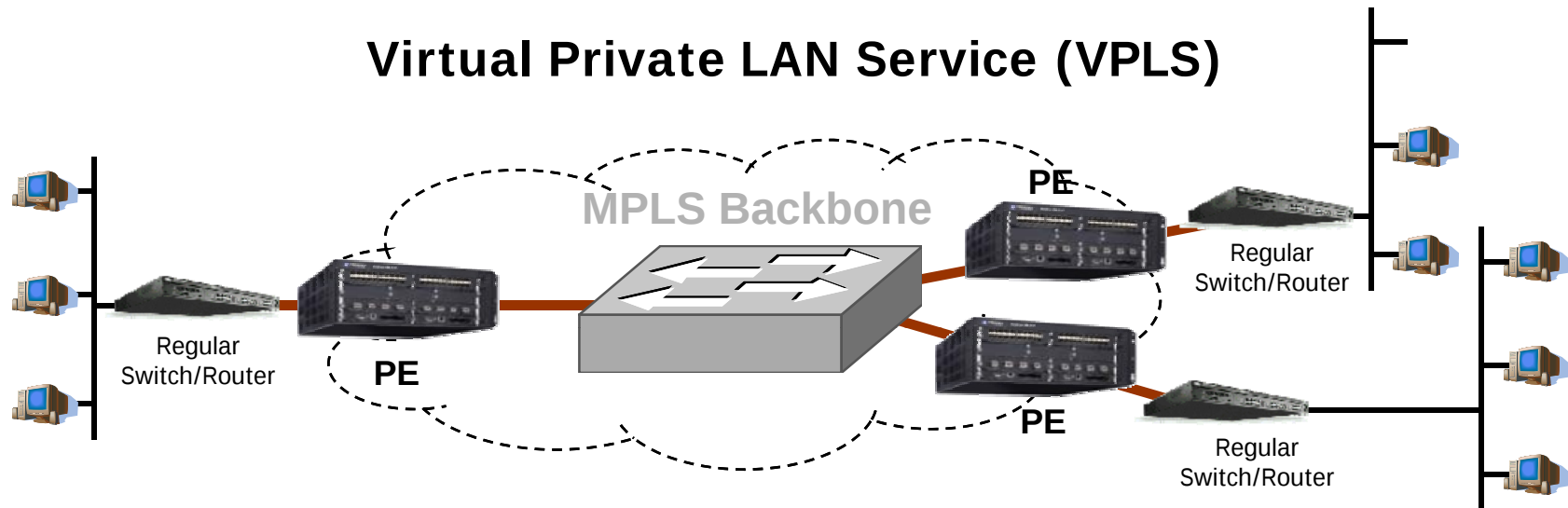
- ❁ Real-time network wide service visibility with no performance degradation
- ❁ Easily integrates to existing infrastructure
 - Sampling-based collection method provides very low overhead monitoring
 - Adapts to different traffic loads by tuning sFlow sample size
 - Can be used in conjunctions with IP-based diagnostic tools such as traceroute
- ❁ Reliable monitoring infrastructure
 - Out-of-band infrastructure ensures that the sFlow feedback and mirror traffic is not affected by outages in core infrastructure
 - MPLS Layer 2 VPN infrastructure ensures high resiliency
 - Multi-location monitoring using multiple sFlow collectors
 - Mirrored traffic and sFlow traffic may be sent to a different NOC center for trouble analysis



Monitoring MPLS VPNs

Monitoring MPLS-based VPN Services

Real-Time Traffic Monitoring



- ❁ MPLS VPNs gaining popularity among business customers
- ❁ Tunnels make traffic analysis more difficult
- ❁ Aggregate statistics have limited utility
- ❁ **Key Requirements for Monitoring L2 and L3 VPNs:**
 - Monitor network performance, availability and security
 - Trending and traffic analysis per VPN endpoint
 - Comprehensive VPN information for troubleshooting and planning
 - Top Talker, traffic trends, threat detection desirable on per VC basis

Monitoring MPLS-based VPN Services

Infrastructure Requirements

- ❁ sFlow capable routers at Provider Edge
- ❁ Enable sFlow on VPN endpoints
- ❁ sFlow collectors can be placed at NOC to monitor PE routers
- ❁ Perform analysis and trending per VC instance
- ❁ Standards based: Standalone sFlow collection and monitoring tools available for MPLS traffic analysis

Monitoring MPLS-based VPN Services

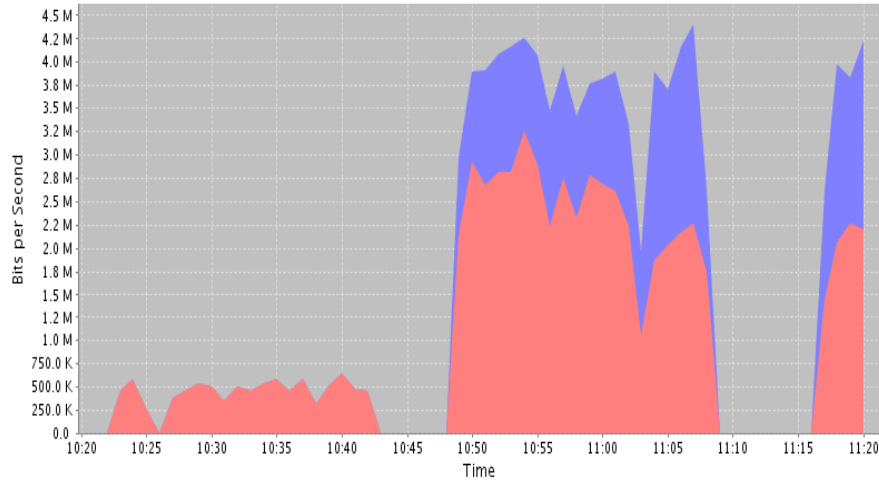
How it works

- ❁ MPLS/VPN information added in sFlow version 5
http://www.sflow.org/sflow_version_5.txt
- ❁ Provider Edge (PE) routers provide sFlow samples
- ❁ At endpoint interface, incoming packets are sampled and additional information is collected and exported in the sFlow packets:
 - MPLS VC information: VC name, VC-ID, and VC label COS
 - MPLS tunnel information: LSP tunnel name, tunnel index as assigned by the router, and tunnel COS
- ❁ Abnormal traffic patterns and excess traffic usage can be detected
- ❁ Examples:
 - Traffic Trends per VC-ID
 - Top Talkers by VC-ID and/or MAC address
 - Traffic Totals based on multiple parameters

Endpoint statistics per VC ID

Traffic Trend per VC ID

23 Jan, 10:21 - 23 Jan, 11:21



to_R1_R4 to_R1_R4_422

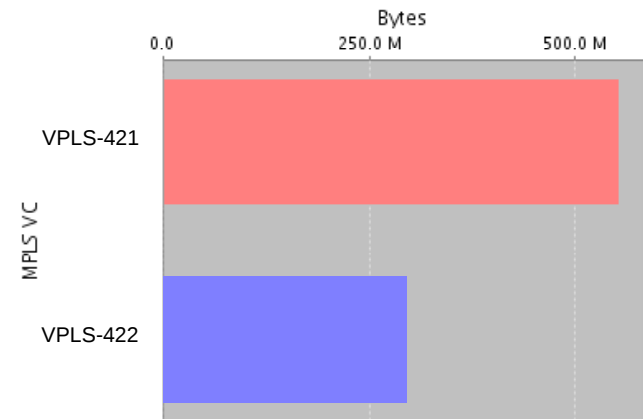
VPLS-421 VPLS-422

Courtesy: InMon Corporation

MPLS VC	Bits per Second
VPLS-421	1.086 M
VPLS-422	535.958 K

Top Talkers

23 Jan, 10:25 - 23 Jan, 11:25



Recent Top N Chart

Top contributors by VC ID

Courtesy: InMon Corporation

Traffic Composition Analysis

Analysis of Traffic Inside VC

Recent Traffic : Table showing per VC traffic totals.

MPLS VC	MPLS VC ID	MPLS VC COS	Ethernet Protocol	Bytes
VPLS-421	421	0	ETHERNET:0xFFFF	10.813 M
VPLS-422	422	0	ETHERNET:0x0800	8.684 M

Courtesy: InMon Corporation

Recent Traffic : Table showing traffic totals for VC, Protocol and MAC src/dst

MPLS VC	MPLS VC ID	MPLS VC COS	Traffic Type	MAC Source	MAC Destination	Bytes
VPLS-421	421	0	ETHERNET:0xFFFF	020200000002	040400000000	1.966 M
VPLS-421	421	0	ETHERNET:0xFFFF	020200000000	040400000003	1.966 M
VPLS-422	422	0	ETHERNET:0x0800	020202000003	040404000004	1.954 M
VPLS-421	421	0	ETHERNET:0xFFFF	020200000003	040400000002	1.720 M
VPLS-422	422	0	ETHERNET:0x0800	020202000003	040404000003	1.520 M
						141.844 M

Foundry Networks – All rights reserved.

Recent Traffic Totals

Determining Accuracy Bounds

Traffic load can be calculated including +-(%Error range)

Historical Traffic Accuracy: Table showing accuracy in long term traffic totals.

MPLS VC	MPLS VC ID	Bytes	Lower Bound	Upper Bound	% Error
VPLS-421	421	168.307 M	158.012 M	178.602 M	6.117
VPLS-422	422	47.226 M	43.967 M	50.484 M	6.900

Courtesy: InMon Corporation

- ✿ Packet sampling performed in hardware to avoid performance degradation
- ✿ Infrequent packet sampling reduces overhead but reduces accuracy
- ✿ Increasing sampling accuracy possible by
 - Increasing sampling rate
 - Increasing sample gathering time
- ✿ Additional details available [here](#).

Benefits of Solution for MPLS Monitoring

- Easily deployed with low overhead on PE routers
- Real-time monitoring of critical business services provides quick anomaly detection
- Helps maintain strict SLAs associated with Platinum customers
- Top Talkers can be
 - Rate Limited
 - Offered higher bandwidth/price services
- Comprehensive visibility and flexible reporting

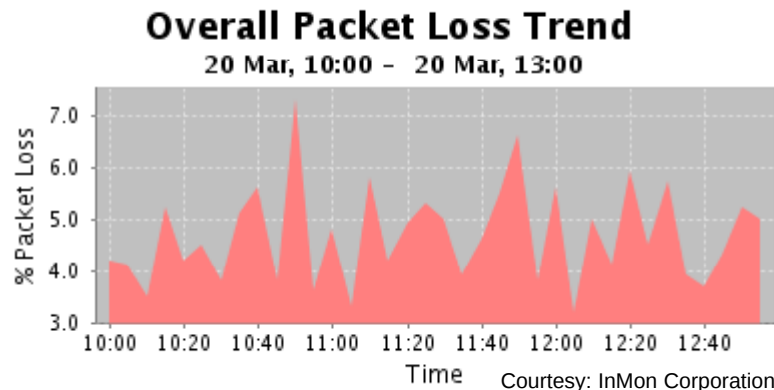


Monitoring Other Services

Monitoring for Other Services (1)

Voice, HSIA, Mission-critical Data

- Service-specific traffic can be monitored using IPv4 ToS or IPv6 priority fields
 - High-priority Voice
 - Mission-critical Data
 - Best Effort Internet Access
- Traffic patterns can be studied on per service class basis
- Voice traffic and quality analysis
 - Monitor RTCP traffic for macroscopic quality metrics
 - Provides quality of service trends in voice traffic
 - Can filter RTP traffic volume by codec and source/destination IP



Monitoring for Other Services (2)

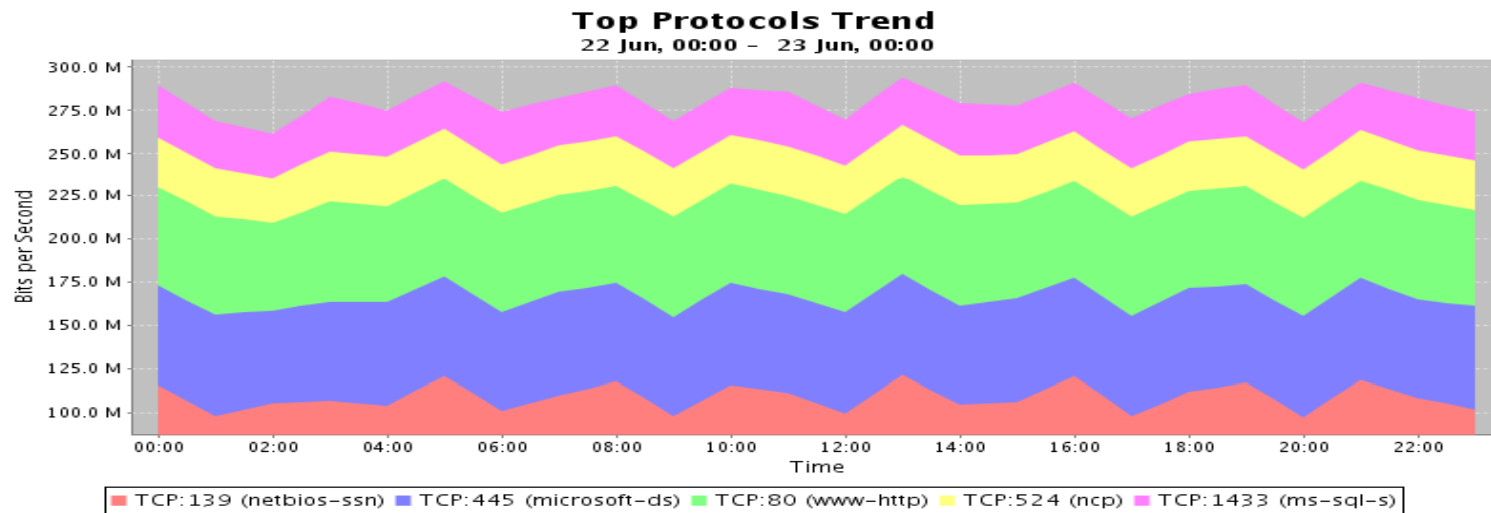
Voice, HSIA, Mission-critical Data

High-Speed Internet Access (HSIA)

- Traffic load trending useful for capacity planning
- Identifying popular content like Google, Yahoo, YouTube, Xbox live
 - Provides opportunities for network optimization i.e. reduce transit costs, reduce latency, manage traffic congestion
- Optimize Peering by tracking traffic based on ASPATH
 - Identify options to reduce transit costs like direct peering relationship

Analysis tools can be used to study patterns and obtain statistics based on traffic type

- Offline analysis with no performance impact to customer traffic





Monitoring for Enhancing Security

Monitoring for Enhancing Security

ACL-Based Inbound sFlow

- ⚙ TCP/UDP ports can be monitored for threats
 - Reconnaissance
 - DOS attacks
 - Network misuse
- ⚙ Provides ability to monitor multiple services (IPv4- or IPv6-based) as well as multiple ports at once

```
//TCP SYN packets
access-list 151 permit tcp host 10.10.10.1 any established syn copy-sflow
// Apply inbound ACL to interface
NetIron(config)# interface ethernet 1/1
NetIron(config-if-e10000-1/1)# ip access-group 151 in
```
- ⚙ Traffic is marked to separate from regular 1-to-N samples
- ⚙ Lower overhead than mirroring
 - Smaller packet header capture
 - Monitors only selected traffic

Benefits of Monitoring for Services and Threats

- Provides threat detection for **known** threats

- Perform offline analysis of captured packets
- Compare packets with signatures of known threats
- Example: NACHI/Welchia Worm

```

alert icmp $EXTERNAL_NET any -> $HOME_NET any \
(\
msg: "NACHI/welchia";\
content: "|aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa  

aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa  

aaaa|";\
dsize:64;\
itype: 8;\
icode: 0;\
classtype:trojan-activity;\
sid: 5800005001;\
rev: 1;\
)

```

Security Warnings Matching Rule for NACHI/Welchia Worm

Time	Type	Value	Address
 6/21/08 10:18 PM	Security	580005001	116.121.53.173
 6/21/08 6:10 AM	Security	580005001	208.127.11.41

- Provides threat detection for **new** threats

- Ability to identify new threats by profiling behavior of hosts
- Example: Scanning behavior could indicate a new worm

- Identify policy violations and network misuse

```

alert tcp 10.0.0.0/8 any -> any 80 \
(\
msg: "Test Rule";\
threshold: type limit, track by_src, count 1,\
seconds 60;\
classtype:bad-unknown;\
sid:700000001;\
)

```

❄ Recovery after threat or anomaly detection

- Apply rate limiting or drop policies for detected threats (ACL-based policies)
- BGP blackhole routing

Security Warnings Matching Rule for Potentially Bad Traffic

	Time	Type	Value	Address
	6/23/08 5:09 PM	Security	70000001	10.1.5.103
	6/23/08 5:05 PM	Security	70000001	10.1.5.103

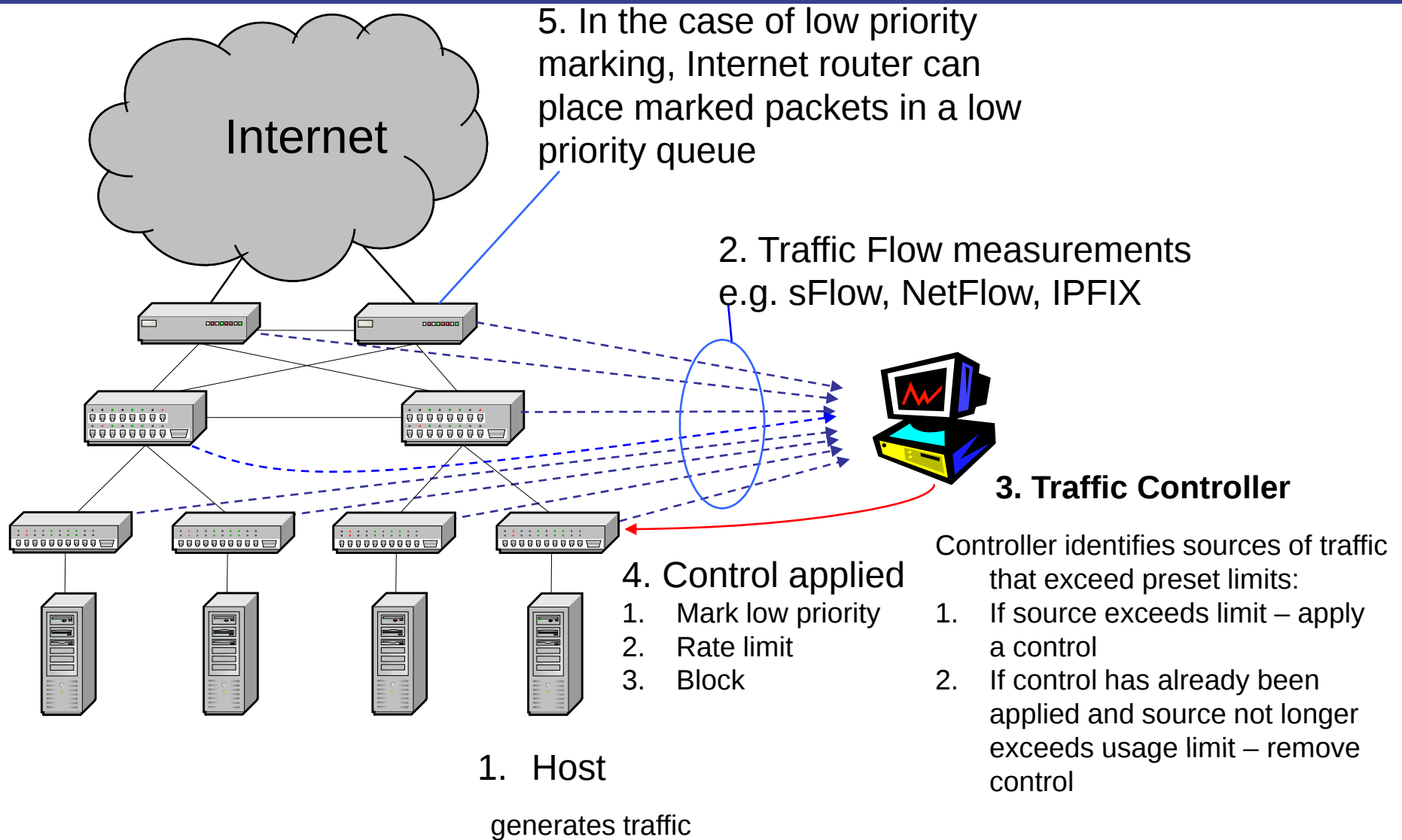


Traffic Management Example

Problem

- ❁ Small percentage of users consume majority of network resources
- ❁ Rapid growth in Video and peer-to-peer traffic is outpacing network capacity growth
- ❁ Effective traffic management is essential to protect critical services and applications, and to control network costs.

Traffic Shaping using sFlow



Automated control

The screenshot shows the Traffic Sentinel web interface running in a Mozilla Firefox browser window. The browser title is "Traffic Sentinel - Mozilla Firefox". The interface has a menu bar with "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". Below the menu bar is the "inMon Traffic Sentinel" logo and a welcome message "Welcome, pp [Logout]". A navigation bar contains tabs for "File", "Home", "Events", "Traffic", "Signatures", "Reports", "Maps", "Controller", "Search", and "Help". Below the navigation bar is a sub-menu with "Settings", "Rules", and "Controls". The main content area has a "Filter:" label, a "Sort ID" dropdown menu, and a "Back" button. Below this is a section titled "Configuration Commands (Switch: fgs)" containing a text area with the following commands:

```
ip access-list extended inmsf469
permit ip host 10.0.0.90 any dscp-marking 10
permit ip any any
exit
interface ethernet0/1/24
ip access-group inmsf469 in
exit
```

At the bottom of the interface, there is a copyright notice: "Copyright © 1999-2008 InMon Corp. ALL RIGHTS RESERVED".

sFlow Traffic Shaping in Action

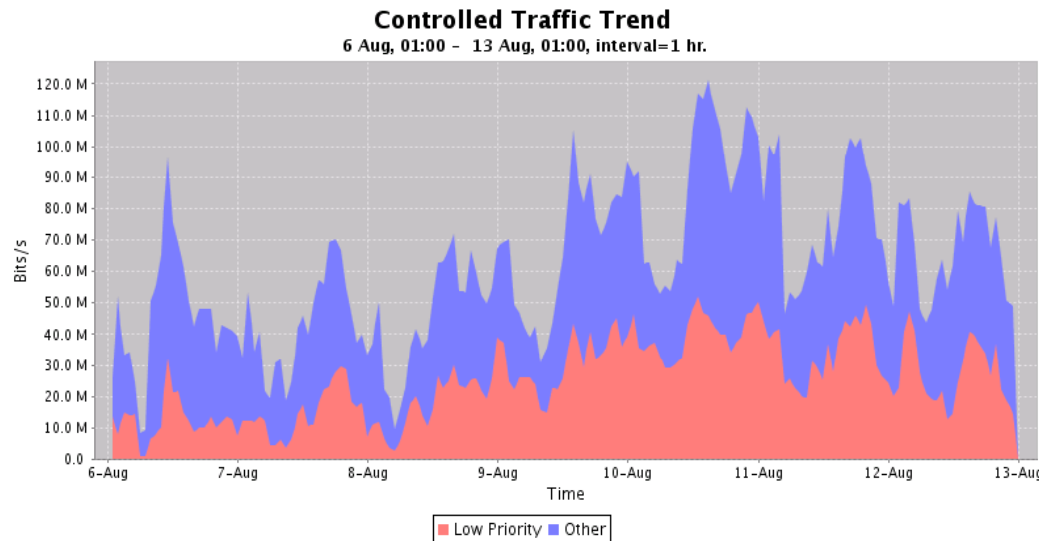


Figure:

- ❁ University network
 - ~ 20,000 switch ports
- ❁ 10-20 control changes (add or remove) per hour
- ❁ ~50% of traffic is marked by the controller (using DSCP)

Advantages

- ❁ *Scalable*: Distributed measurement, coloring and control tasks
- ❁ *Low cost*: embedded measurement, traffic classification and priority queuing mechanisms are utilized
- ❁ *High performance*: mechanisms are built into switch ASICs and operate at wire speed

Summary

Service Assurance Using Proactive Monitoring

- ❁ Real-time monitoring using sFlow offers compelling monitoring solutions for converged networks
- ❁ Offers a low overhead approach for network control and to sell premium services
- ❁ Per customer traffic analysis possible using MPLS VPN endpoint information
- ❁ Enables targeted monitoring for low impact offline analysis
- ❁ Provide an effective anomaly detection and recovery mechanism



Thank You!!