1H01: Network Traffic Monitoring mit sFlow

Referent:

Christoph Bronold

BKM Dienstleistungs GmbH

- sFlow Übersicht
- sFlow Packet Sampling
- sFlow Network Equipment
- sFlow Applikationen
- sFlow Konfiguration
- sFlow Anwendungsbeispiele

Agenda

sFlow Übersicht

- **Wer benutzt das Netzwerk?**
  - Welche Applikationen laufen über das Netzwerk?
  - Wie viel Bandbreite benötigen die Applikationen?
- **Ist meine IT Security Policy effizient?**
  - Ist diese ordnungsgemäß implementiert?
- **Wie viel Bandbreite benötigen die neuen Applikationen?**
- **Warum ist unsere Applikation so langsam?**
  - Ist die Performance des Netzwerks ausreichend?
- **Warum ist der Server so langsam bzw. nicht erreichbar?**
- **Wie viele Server benötigen wir?**
  - Wo sollen die Server angeschlossen sein bzw. stehen?
  - Können auf einem Server auch mehrere Applikationen laufen?

Die häufigsten Fragen an einen Netzwerk Administrator

- **Genau**
  - Quantitative Traffic Messungen bei Gb/s Geschwindigkeiten
  - Forwarding Information

- **Echtzeit**
  - Up-to-date Statistiken über Traffic Flows

- **Skalierbar**
  - Überwacht tausende Switchports von einer Zentrale aus
  - Switch oder Router
  - Keine Performanceverluste
  - Geringer Netzwerklast

- **Kostengünstiger Implementation**
  - Kein zusätzlicher Speicher nötig
  - Geringe CPU Anforderungen

- **Standard Interface**
  - Interoperabilität zwischen Hardware und Applikation

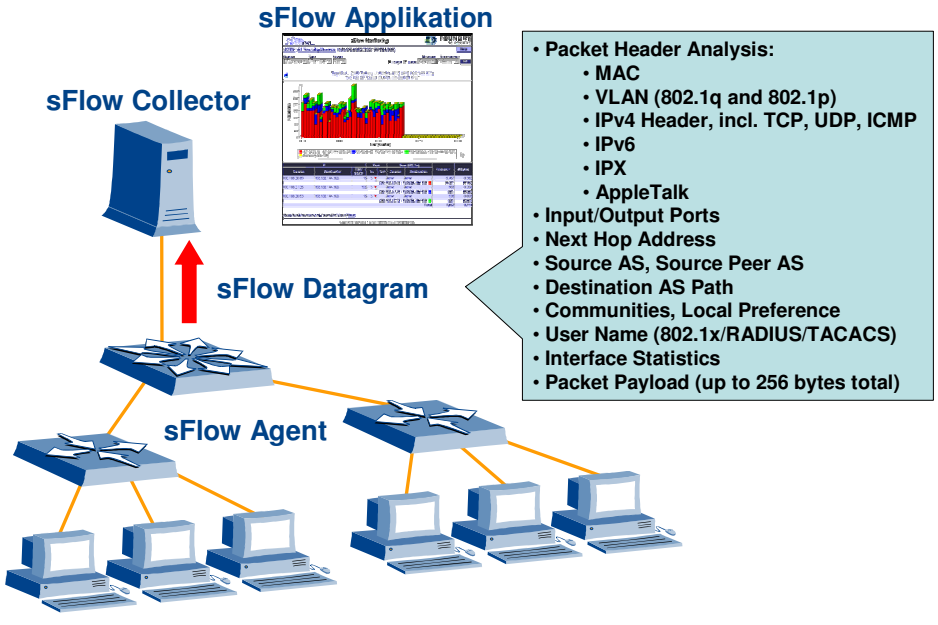
sFlow (RFC 3176) – Making the Network Visible

- **Netzwerkfehlersuche:**
  - Schnelle Identifizierung, Diagnose und Überlastungskontrolle
  - Detaillierte Daten ermöglichen schnelle Problemlösung und minimieren somit die Ausfallzeit(-kosten)
- **Identifizierung von Angriffen:**
  - Angegriffene Hosts
  - Port Scanning, Address Space Scanning
  - Peer-to-Peer Applikationen
  - Nicht autorisierter Zugriff auf Applikationen und Hosts
  - Denial of Service Attacks
- **Definition der Firewall Policies durch Klassifizierung des Datenverkehrs**
- **Netzwerkplanung und kostengünstige Upgrades**

Was kann sFlow für Sie tun?

- **Abrechnung der Netzwerkbenutzung**
  - Detaillierte Daten über die Netzwerknutzung:
    - Benutzer
    - Benutzergruppen
    - Applikation
    - Source/Destination vom Datenverkehr
  - Unterschiedliche Abrechnung für interne und externe Benutzer
- **Berechung von Value Added Services**
  - Voice over IP
- **Neue Abrechnungsmöglichkeiten entwickeln**
  - Kenntnisse über die Benutzeraktivitäten

sFlow Vorteil: Accounting/Billing



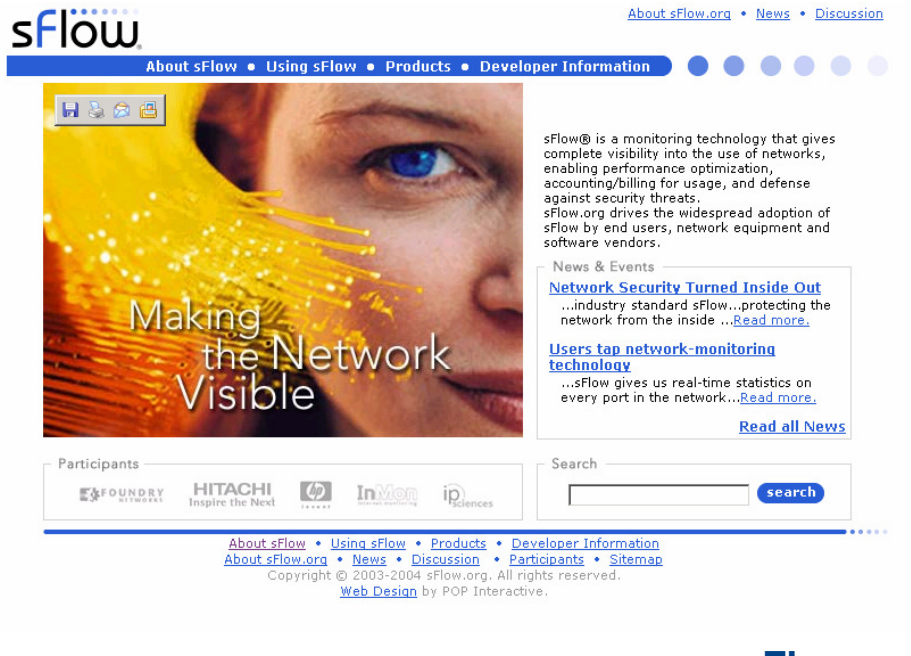
Network Traffic Monitoring mit sFlow

	RMON (4 Groups)	RMON II	NetFlow®	sFlow ®
Packet Capture	N	Y	N	P
Interface Counters	P	P	N	Y
Protocols:				
Packet Headers	N	P	N	Y
Ethernet/IEEE 802.3	N	Y	N	Y
IP/ICMP/TCP/UDP	N	Y	Y	Y
IPX	N	Y	N	Y
AppleTalk	N	Y	N	Y
Layer 2:				
Input/Output Interface	N	N	Y	Y
Input/Output Priority	N	N	N	Y
Input/Output VLAN	N	N	N	Y
Layer 3:				
Source Subnet/Prefix	N	N	Y	Y
Destination Subnet/Prefix	N	N	Y	Y
Next Hop	N	N	Y	Y

	RMON (4 Groups)	RMON II	NetFlow®	sFlow ®
BGP4				
Source AS	N	N	P	Y
Source Peer AS	N	N	P	Y
Destination AS	N	N	P	Y
Destination Peer AS	N	N	P	Y
Communities	N	N	N	Y
AS Path	N	N	N	Y
Real-Time Data Collection	Y	Y	P	Y
Configuration				
Configurable without SNMP	N	N	Y	Y
Configurable via SNMP	Y	Y	N	Y
Low Cost	Y	N	N	Y
Scalable (Switch/Interfaces Collector)	P	N	N	Y
Wire-Speed	Y	P	P	Y

N = Feature not supported
P = Feature partially supported
Y = Feature supported

Vergleich von sFlow mit anderen Technologien

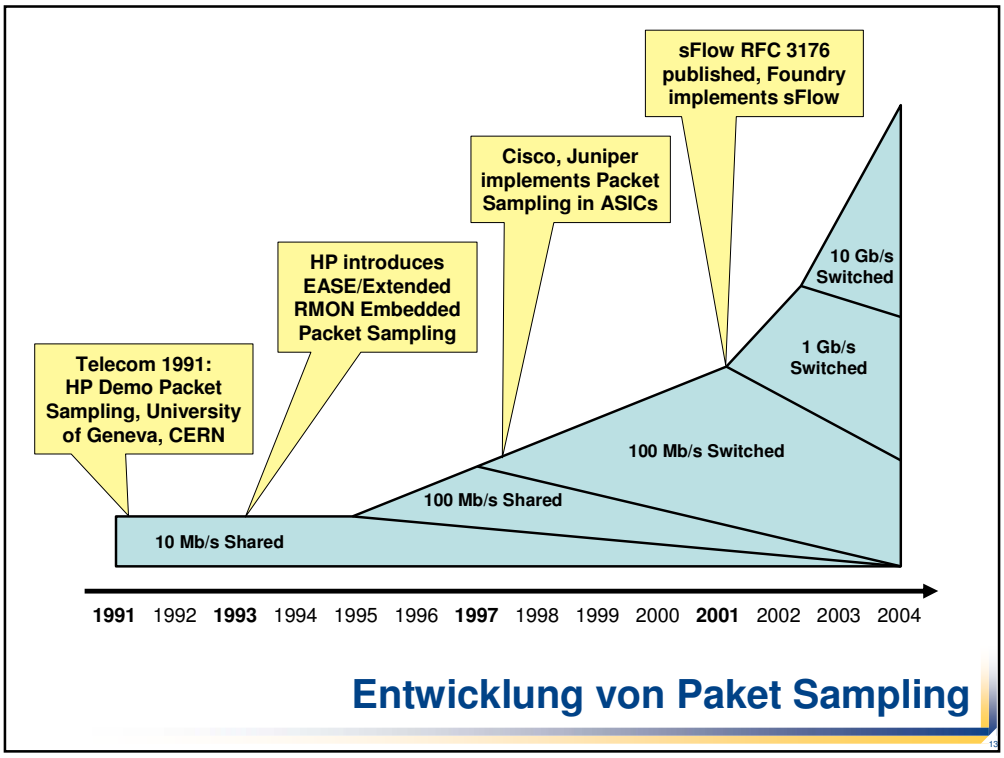


www.sFlow.org

sFlow Packet Sampling

- **Ein Flow ist eindeutig identifizierbar anhand der Kombination von folgenden sieben Feldern:**
  - Source IP Address
  - Destination IP Address
  - Source Port Number
  - Destination Port Number
  - Layer 3 Protocol Type
  - ToS Byte
  - Input logical Interface (ifIndex)

Was ist ein Flow?

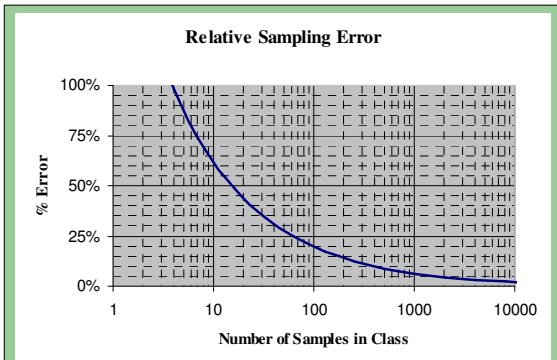


Entwicklung von Paket Sampling

Estimating Traffic per Protocol

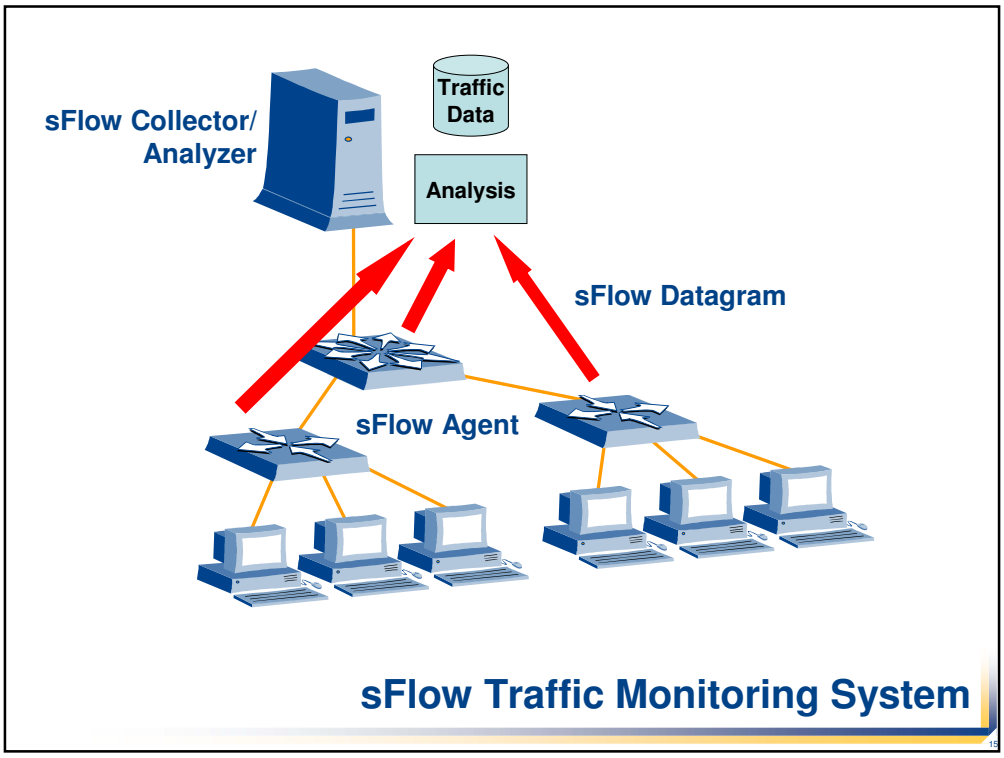
Total number of frames = N
Total number of samples = n
Number of samples in class = c
Number of frames in the class estimated by:

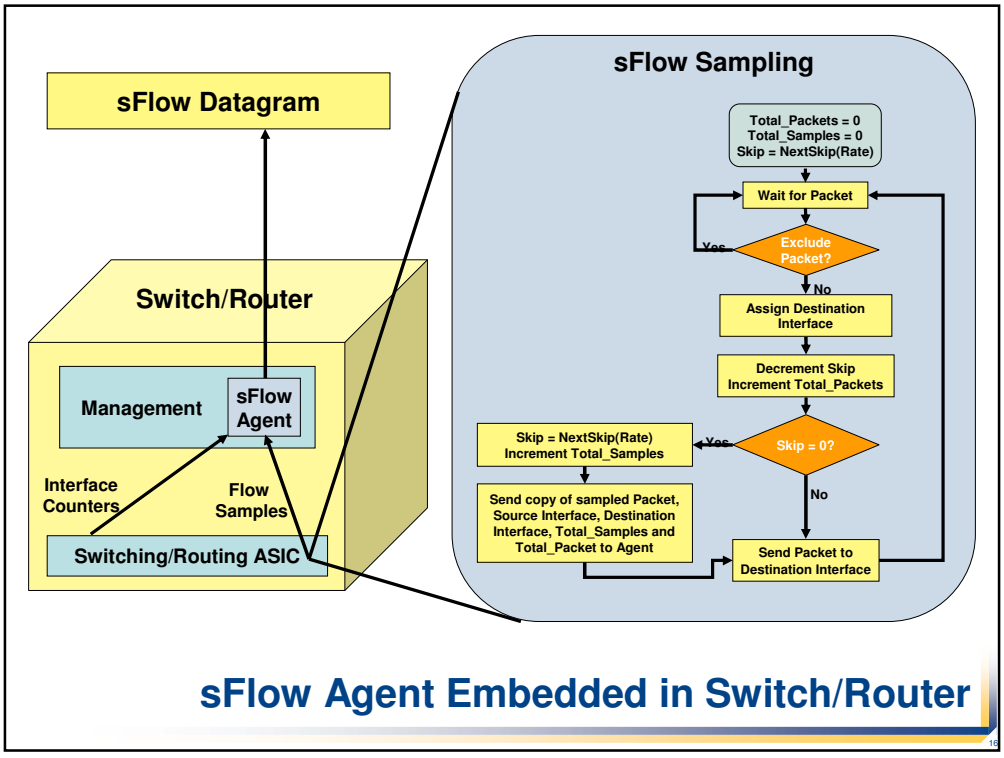
$$N_c = \frac{c}{n} \cdot N$$

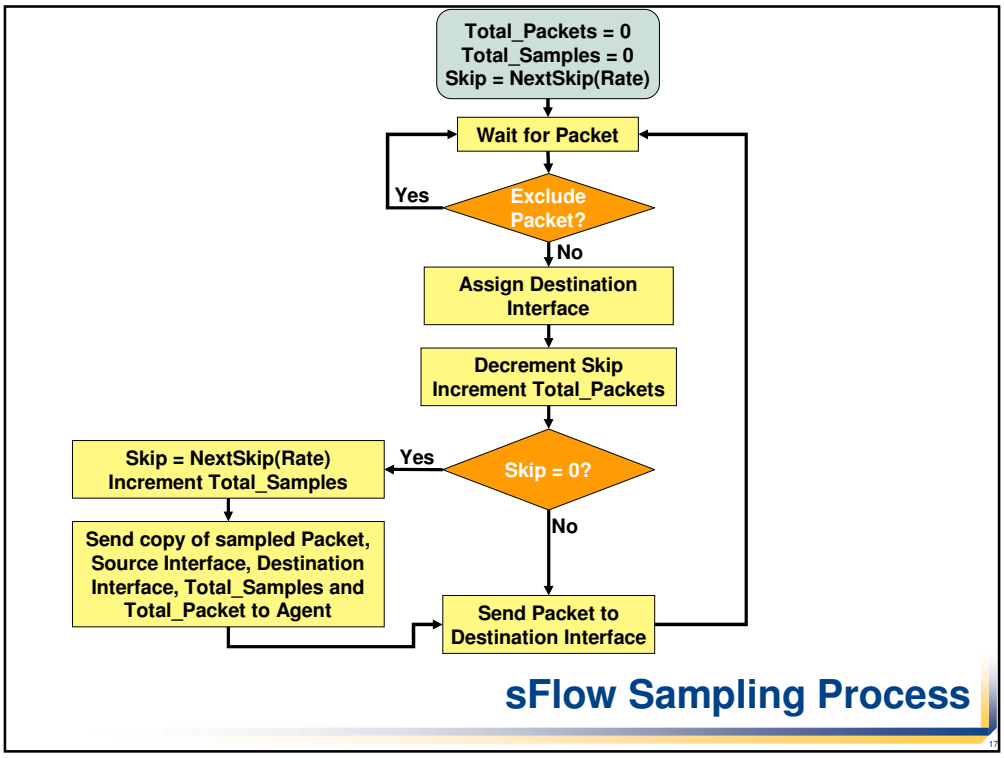


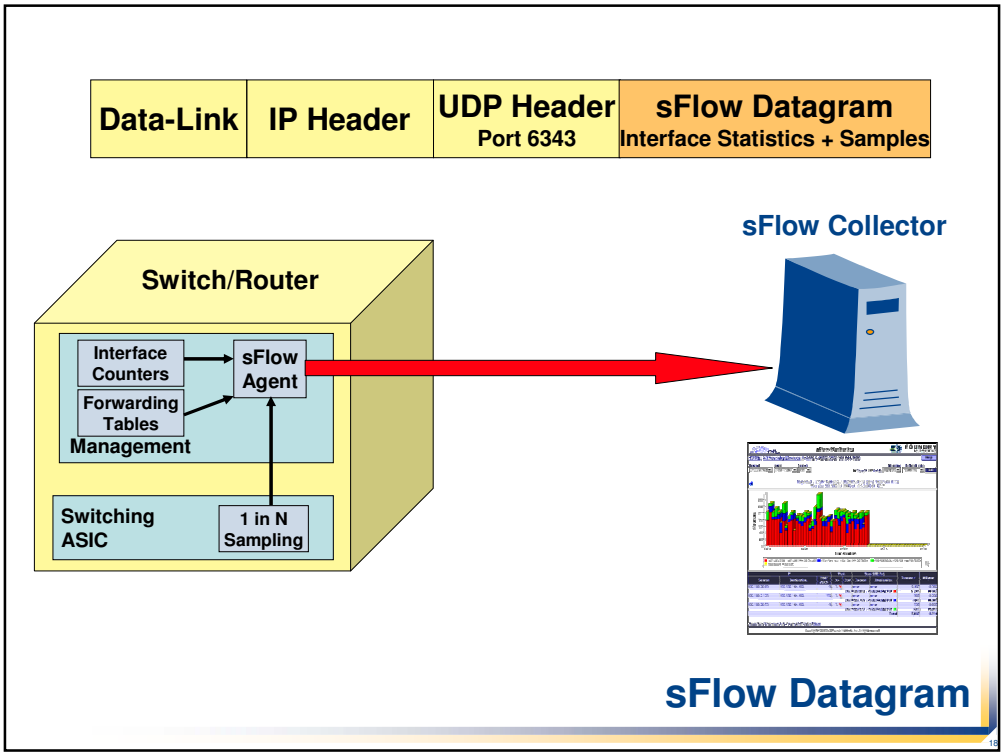
$$\%error \leq 196 \cdot \sqrt{\frac{1}{c}}$$

Statistical Model for Packet Sampling


sFlow Collector/
Analyzer
Traffic
Data
Analysis
sFlow Datagram
sFlow Agent
sFlow Traffic Monitoring System


sFlow Datagram
Switch/Router
Management
sFlow
Agent
Interface
Counters
Flow
Samples
Switching/Routing ASIC
sFlow Sampling
Total_Packets = 0
Total_Samples = 0
Skip = NextSkip(Rate)
Wait for Packet
Exclude
Packet?
Yes
No
Assign Destination
Interface
Decrement Skip
Increment Total_Packets
Skip = 0?
Yes
Skip = NextSkip(Rate)
Increment Total_Samples
No
Send copy of sampled Packet,
Source Interface, Destination
Interface, Total_Samples and
Total_Packet to Agent
Send Packet to
Destination Interface
sFlow Agent Embedded in Switch/Router


Total_Packets = 0
Total_Samples = 0
Skip = NextSkip(Rate)
Wait for Packet
Yes
Exclude Packet?
No
Assign Destination Interface
Decrement Skip
Increment Total_Packets
Skip = NextSkip(Rate)
Increment Total_Samples
Yes
Skip = 0?
No
Send copy of sampled Packet, Source Interface, Destination Interface, Total_Samples and Total_Packet to Agent
Send Packet to Destination Interface
sFlow Sampling Process


Data-Link
IP Header
UDP Header
Port 6343
sFlow Datagram
Interface Statistics + Samples
sFlow Collector
Switch/Router
Interface Counters
Forwarding Tables
Management
sFlow Agent
Switching ASIC
1 in N Sampling
sFlow Datagram

- **Interface statistics samples (RFC 1573, RFC 2233, and RFC 2358):**
  - ifIndex
  - ifType
  - ifSpeed
  - ifDirection
  - ifStatus
  - ifInOctets
  - ifInUcastPkts
  - ifInMulticastPkts
  - ifInBroadcastPkts
  - ifInDiscards
  - ifInErrors
  - ifInUnknownProtos
  - ifOutOctets
  - ifOutUcastPkts
  - ifOutMulticastPkts
  - ifOutBroadcastPkts
  - ifOutDiscards
  - ifOutErrors
  - ifPromiscuousMode

sFlow Datagram: Interface Statistics

- **Flow sample:**
  - Packet header (up to 256 Bytes)
    - MAC, IP, IPX, AppleTalk, HTTP, FTP,DNS…
  - Sample process parameters (rate, pool etc.)
  - Switch
    - Input/Output Ports
    - Priority (IP TOS/DSCP)
    - VLAN (IEEE 802.1q Number and IEEE 802.1p Priority)
  - Router
    - Source/Destination Prefix
    - Next Hop Address
    - Source AS, Source Peer AS
    - Destination AS Path
    - BGP Communities, Local Preference
  - User
    - User IDs (TACACS/RADIUS/802.1X) for source/destination
  - URL
    - URL associated with source/destination

sFlow Datagram: Flow Sample

sFlow Hardware

- **Extreme Networks**
  - BlackDiamond 10808
- **Foundry Networks**
  - BigIron Series (Terathon, JetCore)
  - NetIron Series (Terathon, JetCore)
  - FastIron Series (JetCore)
- **Hewlett-Packard**
  - ProCurve 5300xl series
  - ProCurve 9300m series
- **Hitachi**
  - GR4000
  - GS4000
- **InMon Corp.**
  - sFlow Probe
- **ntop.org**
  - ntop
- **QoSmetrics**
  - NetWarrior

sFlow Network Equipment

- **BigIron**
  - Enterprise-class Layer 2/Layer 3 Switches
- **NetIron**
  - Metro and ISP Router
- **FastIron**
  - Workgroup Layer2/Layer 3 Switches

Foundry Networks

ProCurve 5300xl Series

HP ProCurve Switch 5372xl

HP ProCurve Switch5348x

ProCurve 9300m Series

HP ProCurve Routing Switch 9315m

Hewlett-Packard

```
#nprobe -h
Welcome to nprobe v.3.0 for i686-pc-linux
Built on 01/05/04 04:46:01 PM
Copyright 2002-04 by Luca Deri <deri@ntop.org>

Usage:   nprobe -n <host:port> [-i <interface>] [-t <dump timeout>]
         [-d <idle timeout>] [-l <send timeout>] [-s <scan cycle>]
         [-p <level>] [-f <filter>] [-a] [-b]
         [-P <path>] [-D <format>] [-u <device index>] [-v]
         [-I <probe name>] [-w <hash size>] [-e <flow delay>]
         [-z <min flow size>] [-M <max num active flows>][-R <payload Len>]
         [-x <payload policy>] [-N <key>] [-E <engine>]
         [-m <min # flows>] [-r <dump file>] [-q <host:port>]
         [-S <sample rate>] [-A <AS list>] [-g <PID file>]
         [-T <Flow Template>] [-U <Flow Template Id>]
```

nBox[86]

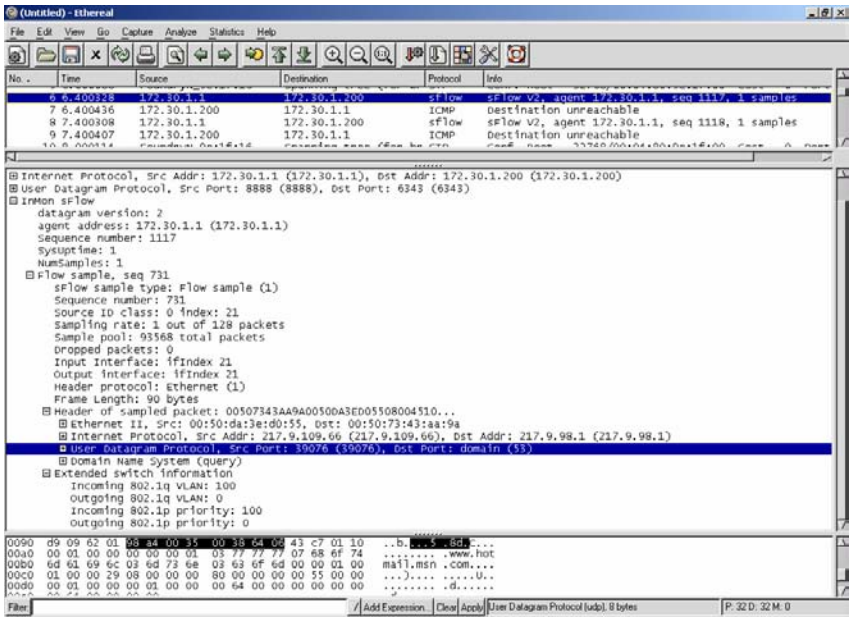
ntop.org

TWIST-IT

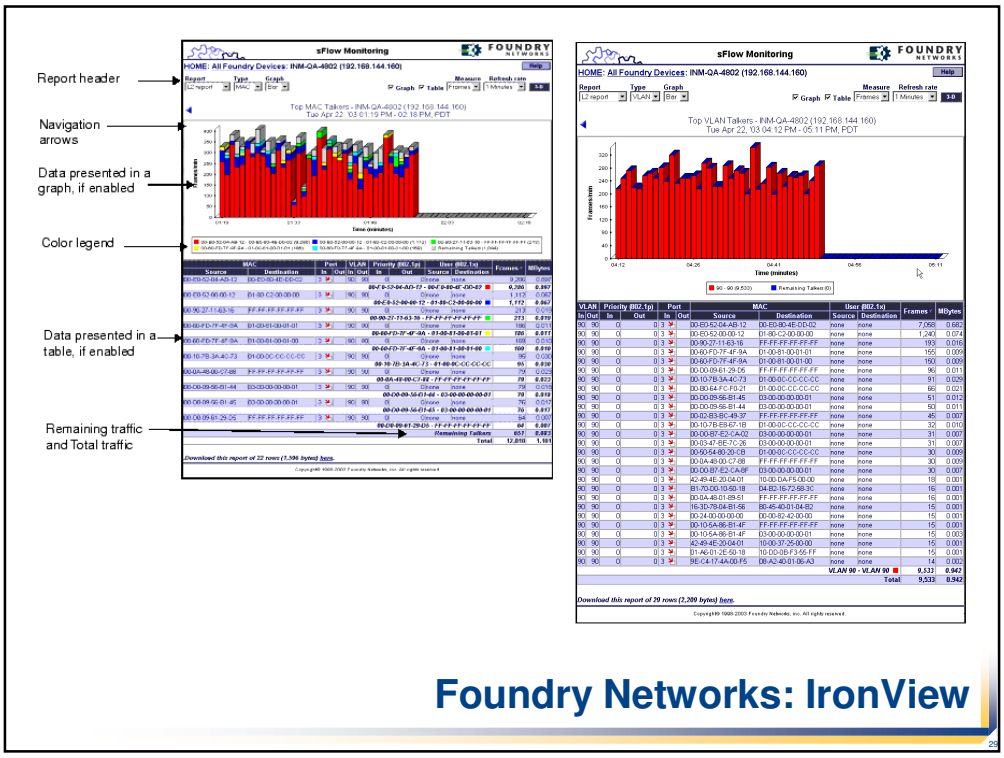
sFlow Applikationen

- **Ethereal:** *Ethereal Network Protocol Analyzer*
- **Foundry Networks:** *IronView*
- **Genie Network Resource Management Inc.:** *GenieNTG 2500*
- **Hewlett-Packard:** *HP Internet Usage Manager, HP OpenView Performance Insight, HP ProCurve Manager Plus*
- **Infosim Networking Solutions AG:** *StableNet PME*
- **InMon Corp.:** *InMon Traffic Server, sflowtool*
- **NetScout:** *nGenius Performance Manager, nGenius Probes*
- **ntop.org:** *ntop*
- **QoSmetrix:** *NetWarrior*

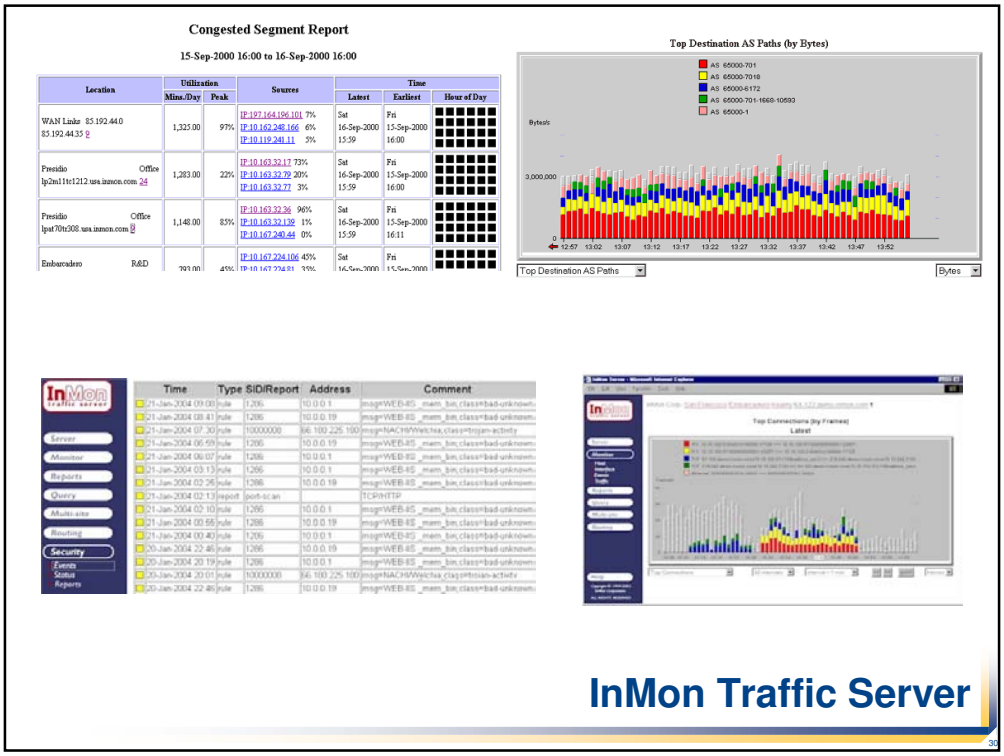
sFlow Applikationen



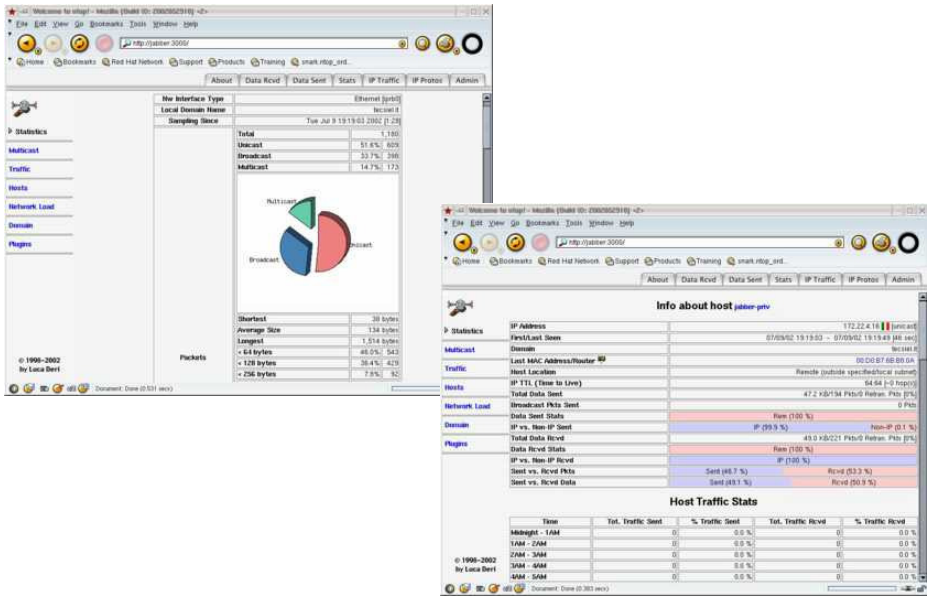
Ethereal Network Protocol Analyzer



Foundry Networks: IronView



InMon Traffic Server



ntop.org: ntop

TWIST-IT

sFlow Konfiguration für Foundry Networks Switch

sFlow Konfiguration für Foundry Networks

- **Konfigurationsschritte:**
  - Spezifizierung der Collector Information (IP Adresse)
  - Optional: Änderung des Polling-Intervalls
  - Optional: Änderung der Sampling Rate
  - Aktivierung von sFlow global
  - Aktivierung von sFlow forwarding auf individuellen Interfaces

Beispiel: sFlow Konfiguration

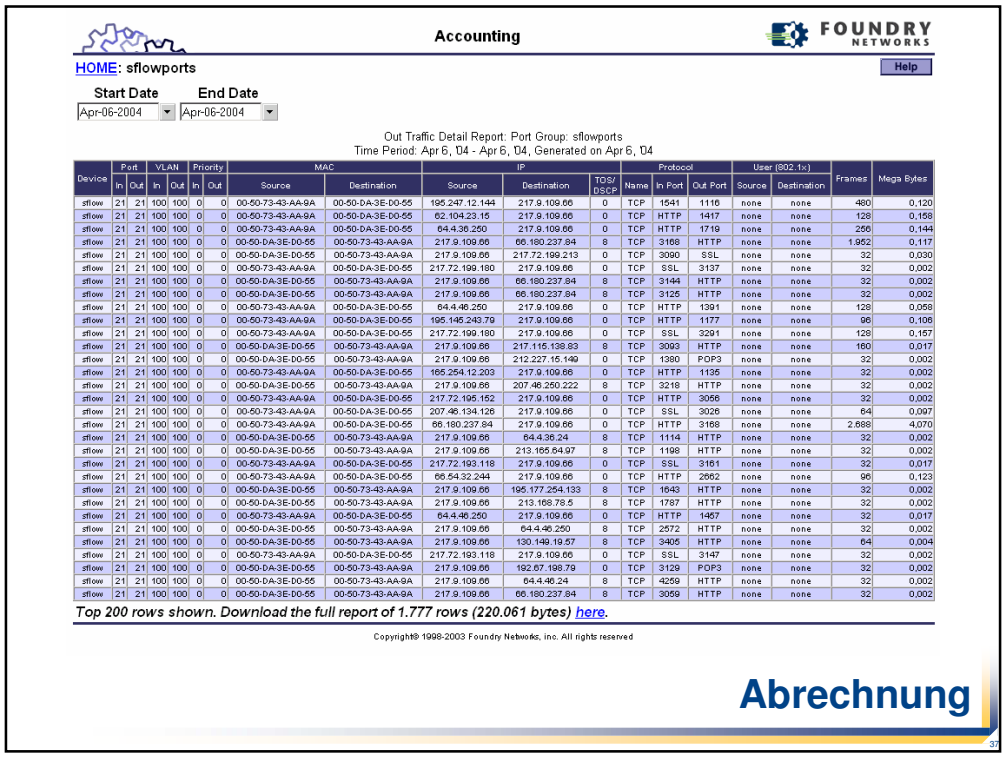
```
!
sflow enable
sflow sample 100
sflow destination 144.100.10.10
!
interface ethernet 1
 sflow-forwarding
!
interface ethernet 2
 ip address 169.144.10.1 255.255.255.0
 sflow-forwarding
!
```

```
FI4802-PREM#show sflow
sFlow services are enabled.
sFlow agent IP address: 144.100.10.1
Collector IP 144.100.10.10, UDP 6343
Polling interval is 20 seconds.
Configured default sampling rate: 1 per 10 packets.
Actual default sampling rate: 1 per 32 packets.
214 UDP packets exported
123 sFlow samples collected.
sFlow ports: ethe 1 to 2
Module Sampling Rates
---------------------
Slot  1 configured rate=10, actual rate=32
Port Sampling Rates
-------------------
Port=1, configured rate=10, actual rate=32, Subsampling factor=1
Port=2, configured rate=10, actual rate=32, Subsampling factor=1
FI4802-PREM#
```

show sflow

sFlow Anwendungsbeispiele

- Accounting/Billing
- Internet Traffic Analyse
- Security Threats



Accounting

FOUNDRY NETWORKS

HOME: sflowports

Help

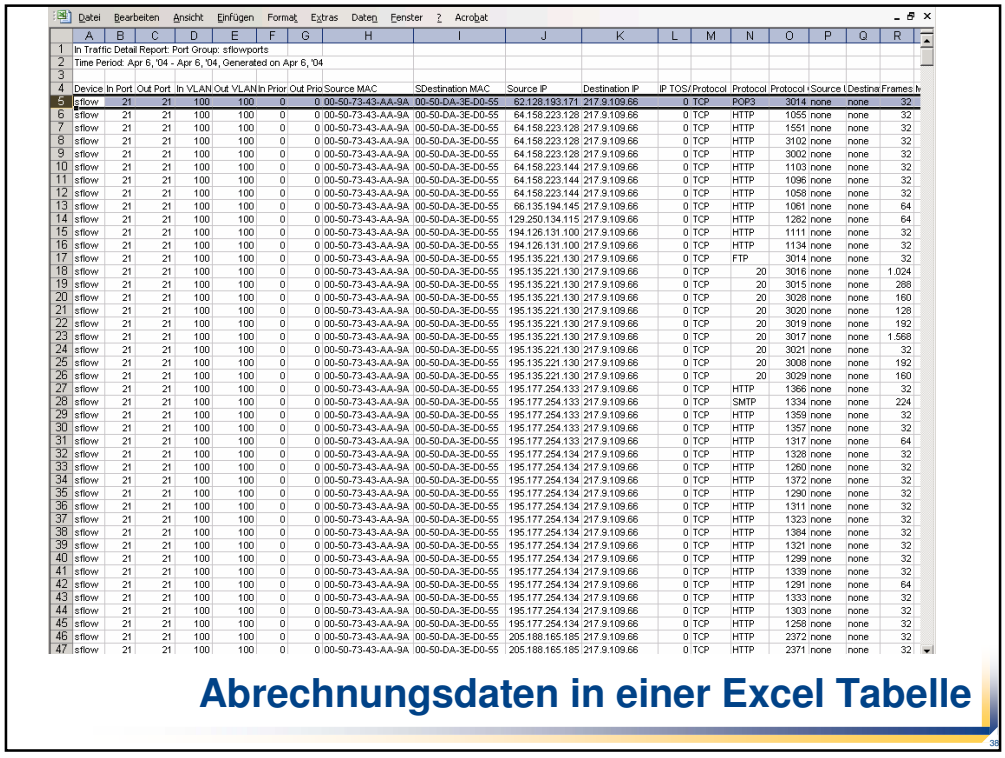
Start Date: Apr-06-2004 End Date: Apr-06-2004

Out Traffic Detail Report: Port Group: sflowports
Time Period: Apr 6, '04 - Apr 6, '04, Generated on Apr 6, '04

Device	Port		VLAN		Priority		MAC		IP			Protocol			User (802.1x)		Frames	Mega Bytes
	In	Out	In	Out	In	Out	Source	Destination	Source	Destination	TOS/ DSCP	Name	In Port	Out Port	Source	Destination		
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.247.12.144	217.9.109.66	0	TCP	1541	1116	none	none	480	0,120
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	62.104.23.15	217.9.109.66	0	TCP	HTTP	1417	none	none	128	0,158
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.4.36.250	217.9.109.66	0	TCP	HTTP	1719	none	none	256	0,144
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	66.180.237.84	8	TCP	3168	HTTP	none	none	1.952	0,117
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	217.72.199.213	0	TCP	3090	SSL	none	none	32	0,030
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	217.72.199.180	217.9.109.66	0	TCP	SSL	3137	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	66.180.237.84	8	TCP	3144	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	66.180.237.84	8	TCP	3125	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.4.46.250	217.9.109.66	0	TCP	HTTP	1391	none	none	128	0,058
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.145.243.79	217.9.109.66	0	TCP	HTTP	1177	none	none	96	0,106
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	217.72.199.180	217.9.109.66	0	TCP	SSL	3291	none	none	128	0,157
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	217.115.138.83	8	TCP	3093	HTTP	none	none	160	0,017
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	212.227.15.149	0	TCP	1380	POP3	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.254.12.203	217.9.109.66	0	TCP	HTTP	1135	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	207.46.250.222	8	TCP	3218	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	217.72.195.152	217.9.109.66	0	TCP	HTTP	3056	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	207.46.134.126	217.9.109.66	0	TCP	SSL	3026	none	none	64	0,097
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	66.180.237.84	217.9.109.66	0	TCP	HTTP	3168	none	none	2.688	4,070
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	64.4.36.24	8	TCP	1114	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	213.155.64.97	8	TCP	1198	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	217.72.193.118	217.9.109.66	0	TCP	SSL	3161	none	none	32	0,017
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	66.54.32.244	217.9.109.66	0	TCP	HTTP	2662	none	none	96	0,123
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	195.177.254.133	8	TCP	1643	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	213.168.78.5	8	TCP	1787	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.4.46.250	217.9.109.66	0	TCP	HTTP	1457	none	none	32	0,017
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	64.4.46.250	8	TCP	2572	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	130.149.19.57	8	TCP	3405	HTTP	none	none	64	0,004
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	217.72.193.118	217.9.109.66	0	TCP	SSL	3147	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	192.67.198.79	0	TCP	3129	POP3	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	64.4.46.24	8	TCP	4259	HTTP	none	none	32	0,002
sflow	21	21	100	100	0	0	00-50-DA-3E-D0-55	00-50-73-43-AA-9A	217.9.109.66	66.180.237.84	8	TCP	3059	HTTP	none	none	32	0,002

Top 200 rows shown. Download the full report of 1.777 rows (220.061 bytes) here.

Abrechnung



Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster ? Acrobat

In Traffic Detail Report: Port Group: sflowports
Time Period: Apr 6, '04 - Apr 6, '04, Generated on Apr 6, '04

Device	In Port	Out Port	In VLAN	Out VLAN	In Prior	Out Prio	Source MAC	SDestination MAC	Source IP	Destination IP	IP TOS/	Protocol	Protocol	Protocol	Source I	Destina	Frames
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	62.128.193.171	217.9.109.66	0	TCP	POP3	3014	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.158.223.128	217.9.109.66	0	TCP	HTTP	1055	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.158.223.128	217.9.109.66	0	TCP	HTTP	1551	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.158.223.128	217.9.109.66	0	TCP	HTTP	3102	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.158.223.128	217.9.109.66	0	TCP	HTTP	3002	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.158.223.144	217.9.109.66	0	TCP	HTTP	1103	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.158.223.144	217.9.109.66	0	TCP	HTTP	1096	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	64.158.223.144	217.9.109.66	0	TCP	HTTP	1058	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	66.135.194.145	217.9.109.66	0	TCP	HTTP	1061	none	none	64
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	129.250.134.115	217.9.109.66	0	TCP	HTTP	1282	none	none	64
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	194.126.131.100	217.9.109.66	0	TCP	HTTP	1111	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	194.126.131.100	217.9.109.66	0	TCP	HTTP	1134	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	FTP	3014	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3016	none	none	1.024
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3015	none	none	288
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3028	none	none	160
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3020	none	none	128
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3019	none	none	192
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3017	none	none	1.568
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3021	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3008	none	none	192
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.135.221.130	217.9.109.66	0	TCP	20	3029	none	none	160
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.133	217.9.109.66	0	TCP	HTTP	1366	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.133	217.9.109.66	0	TCP	SMTP	1334	none	none	224
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.133	217.9.109.66	0	TCP	HTTP	1359	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.133	217.9.109.66	0	TCP	HTTP	1357	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.133	217.9.109.66	0	TCP	HTTP	1317	none	none	64
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1328	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1260	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1372	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1290	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1311	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1323	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1384	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1321	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1299	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1339	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1291	none	none	64
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1333	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1303	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	195.177.254.134	217.9.109.66	0	TCP	HTTP	1258	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	205.188.165.185	217.9.109.66	0	TCP	HTTP	2372	none	none	32
sflow	21	21	100	100	0	0	00-50-73-43-AA-9A	00-50-DA-3E-D0-55	205.188.165.185	217.9.109.66	0	TCP	HTTP	2371	none	none	32

Abrechnungsdaten in einer Excel Tabelle

InMon internet monitoring **Demo**

• Products • Technology • Demo • Support • Corporate

- Overview
- Account/Billing
- BGP 4
- Denial of Service
- Intrusion Detection
- Real-time
- Reporting
- Data Access

Bill by customer

The following table shows a breakdown internal and external traffic by division.

Customer	Traffic to Self			Internal Traffic						External Traffic						Total	
				Sent			Received			Sent			Received				
	MB	Rate	US$	MB	Rate	US$	MB	Rate	US$	MB	Rate	US$	MB	Rate	US$	MB	US$
News	3,541	10	35,408	893	20	17,858	341	20	6,819	7	100	733	8	100	806	4,790	61,625
Sports	7,839	10	78,390	1,507	20	30,142	427	20	8,537	4	100	391	0	100	8	9,777	117,468
Entertainment	1	10	14	313	20	6,262	1,014	20	20,274	1	100	128	1	100	93	1,330	26,770

This summary table is used to split charges among the divisions. In addition, each division head is given a report that itemizes the traffic that contributed to the charge.

Previous Next

Abrechung pro Benutzer

sFlow Monitoring — FOUNDRY NETWORKS

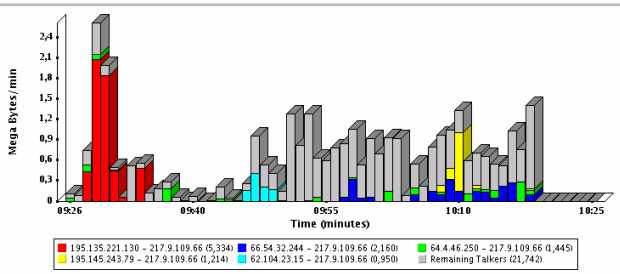
HOME: sflow — Help

Report: L3/L4 report | Type: IPv4 | Graph: Bar

Top IPv4 Talkers - sflow (Group level)
Di Apr 6, '04 09:26 AM - 10:25 AM, CEST

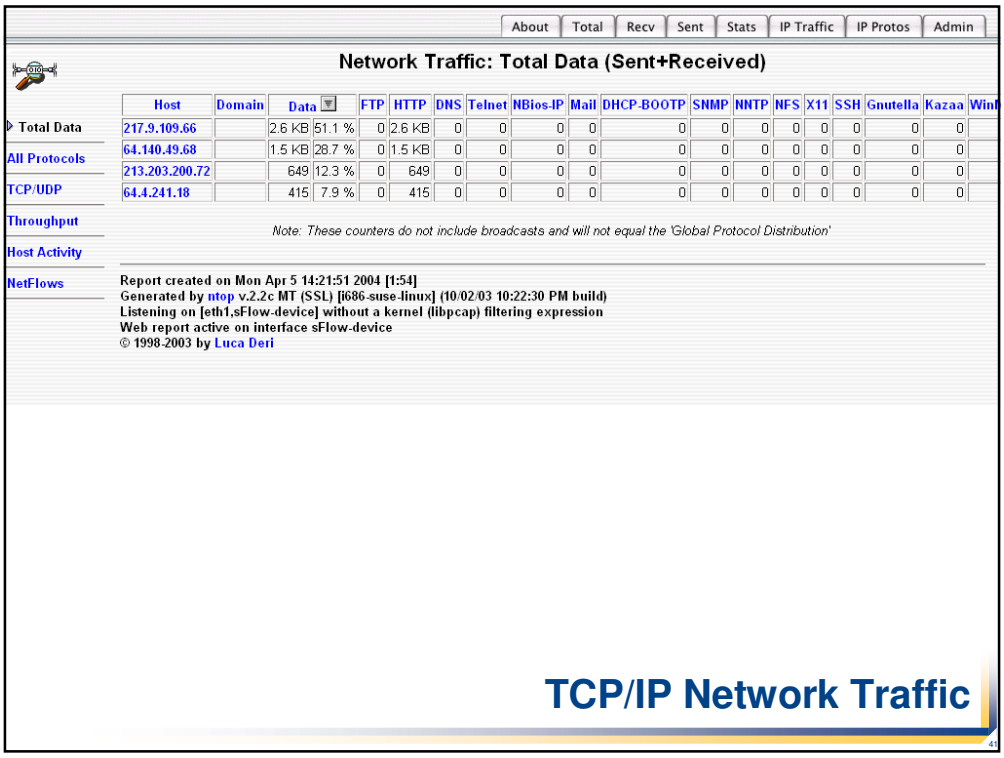
Measure: MBytes | Refresh rate: 3 Minutes | 3-D

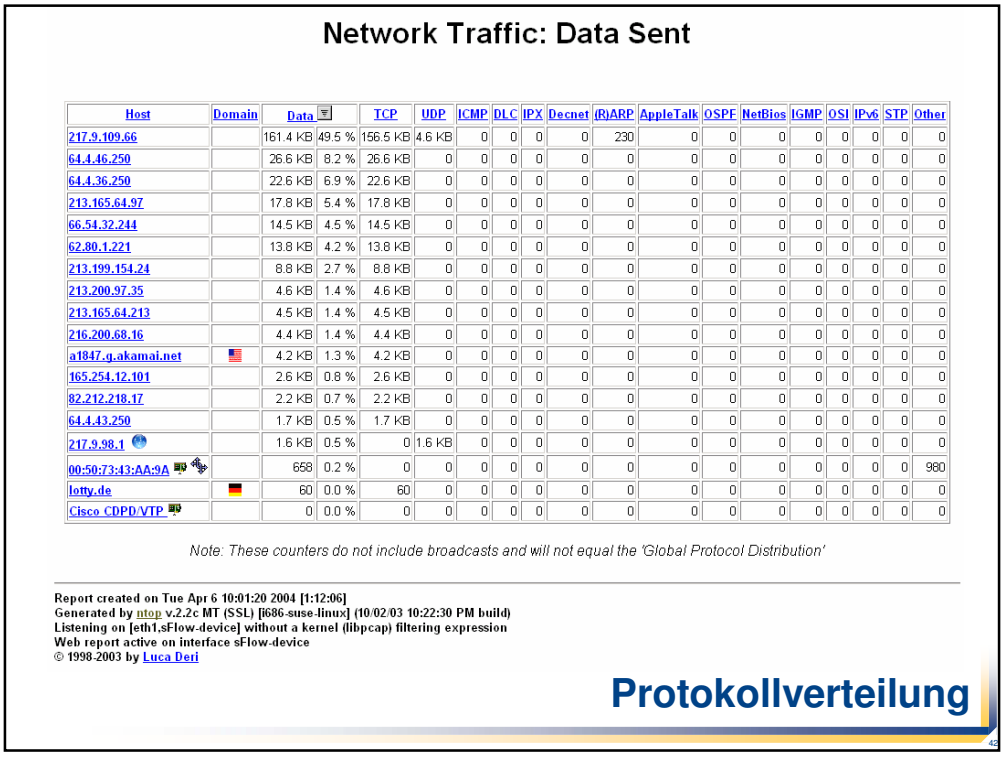
Graph ☑ Table



IP			Port		Protocol			User (802.1x)		Frames	MBytes
Source	Destination	TOS/ DSCP	In	Out	Name	In Port	Out Port	Source	Destination		
195.135.221.130	217.9.109.66	0	21	21	TCP	20	3017	none	none	1.568	2,374
195.135.221.130	217.9.109.66	0	21	21	TCP	20	3016	none	none	1.024	1,550
195.135.221.130	217.9.109.66	0	21	21	TCP	FTP	3014	none	none	32	0,002
							195.135.221.130 - 217.9.109.66 (sflow - 172.30.1.1)			***3.584***	***5,334***
195.145.243.79	217.9.109.66	0	21	21	TCP	HTTP	1146	none	none	32	0,009
195.145.243.79	217.9.109.66	0	21	21	TCP	HTTP	1145	none	none	32	0,004
							195.145.243.79 - 217.9.109.66 (sflow - 172.30.1.1)			***1.120***	***1,214***
195.177.254.133	217.9.109.66	0	21	21	TCP	SMTP	1590	none	none	480	0,438
195.177.254.133	217.9.109.66	0	21	21	TCP	SMTP	1334	none	none	224	0,169
195.177.254.133	217.9.109.66	0	21	21	TCP	HTTP	1317	none	none	64	0,056

Internet Traffic Analyse


About
Total
Recv
Sent
Stats
IP Traffic
IP Protos
Admin
Network Traffic: Total Data (Sent+Received)
Total Data
All Protocols
TCP/UDP
Throughput
Host Activity
NetFlows
Host
Domain
Data
FTP
HTTP
DNS
Telnet
NBios-IP
Mail
DHCP-BOOTP
SNMP
NNTP
NFS
X11
SSH
Gnutella
Kazaa
217.9.109.66 2.6 KB 51.1 % 0 2.6 KB 0 0 0 0 0 0 0 0 0 0 0 0
64.140.49.68 1.5 KB 28.7 % 0 1.5 KB 0 0 0 0 0 0 0 0 0 0 0 0
213.203.200.72 649 12.3 % 0 649 0 0 0 0 0 0 0 0 0 0 0 0
64.4.241.18 415 7.9 % 0 415 0 0 0 0 0 0 0 0 0 0 0 0
Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'
Report created on Mon Apr 5 14:21:51 2004 [1:54]
Generated by ntop v.2.2c MT (SSL) [i686-suse-linux] (10/02/03 10:22:30 PM build)
Listening on [eth1,sFlow-device] without a kernel (libpcap) filtering expression
Web report active on interface sFlow-device
© 1998-2003 by Luca Deri
TCP/IP Network Traffic


Network Traffic: Data Sent
Host
Domain
Data
TCP
UDP
ICMP
DLC
IPX
Decnet
(R)ARP
AppleTalk
OSPF
NetBios
IGMP
OSI
IPv6
STP
Other
217.9.109.66 161.4 KB 49.5 % 156.5 KB 4.6 KB 0 0 0 0 230 0 0 0 0 0 0 0 0
64.4.46.250 26.6 KB 8.2 % 26.6 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
64.4.36.250 22.6 KB 6.9 % 22.6 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
213.165.64.97 17.8 KB 5.4 % 17.8 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
66.54.32.244 14.5 KB 4.5 % 14.5 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
62.80.1.221 13.8 KB 4.2 % 13.8 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
213.199.154.24 8.8 KB 2.7 % 8.8 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
213.200.97.35 4.6 KB 1.4 % 4.6 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
213.165.64.213 4.5 KB 1.4 % 4.5 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
216.200.68.16 4.4 KB 1.4 % 4.4 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
a1847.g.akamai.net 4.2 KB 1.3 % 4.2 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
165.254.12.101 2.6 KB 0.8 % 2.6 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
82.212.218.17 2.2 KB 0.7 % 2.2 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
64.4.43.250 1.7 KB 0.5 % 1.7 KB 0 0 0 0 0 0 0 0 0 0 0 0 0 0
217.9.98.1 1.6 KB 0.5 % 0 1.6 KB 0 0 0 0 0 0 0 0 0 0 0 0 0
00:50:73:43:AA:9A 658 0.2 % 0 0 0 0 0 0 0 0 0 0 0 0 0 0 980
lotty.de 60 0.0 % 60 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Cisco CDPD/VTP 0 0.0 % 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'
Report created on Tue Apr 6 10:01:20 2004 [1:12:06]
Generated by ntop v.2.2c MT (SSL) [i686-suse-linux] (10/02/03 10:22:30 PM build)
Listening on [eth1,sFlow-device] without a kernel (libpcap) filtering expression
Web report active on interface sFlow-device
© 1998-2003 by Luca Deri
Protokollverteilung

Recent Users of Port 80 (http)

Client	Server
	• 217.9.109.66 • a1847.g.akamai.net • 64.4.36.250 • 65.54.194.117 • 165.254.12.131 • 165.254.12.202 • 165.254.12.101 • 62.104.23.15 • 213.200.97.35 • 213.165.64.97 • 62.104.23.38 • 213.199.154.24 • 62.104.23.42 • adserver.freenet.de • 193.201.12.58 • 64.233.161.99 • 62.104.23.17 • 213.165.65.237 • 213.165.65.30 • 213.165.64.213 • 194.112.102.72 • 129.250.134.115 • 209.47.169.10 • 64.4.46.24 • 64.4.46.250

Report created on Tue Apr 6 09:51:06 2004 [1:01:52]
Generated by ntop v.2.2c MT (SSL) [i686-suse-linux] (10/02/03 10:22:30 PM build)
Listening on [eth1,sFlow-device] without a kernel (libpcap) filtering expression
Web report active on interface sFlow-device
© 1998-2003 by Luca Deri

TCP Port User

TCP/UDP Service/Port Usage

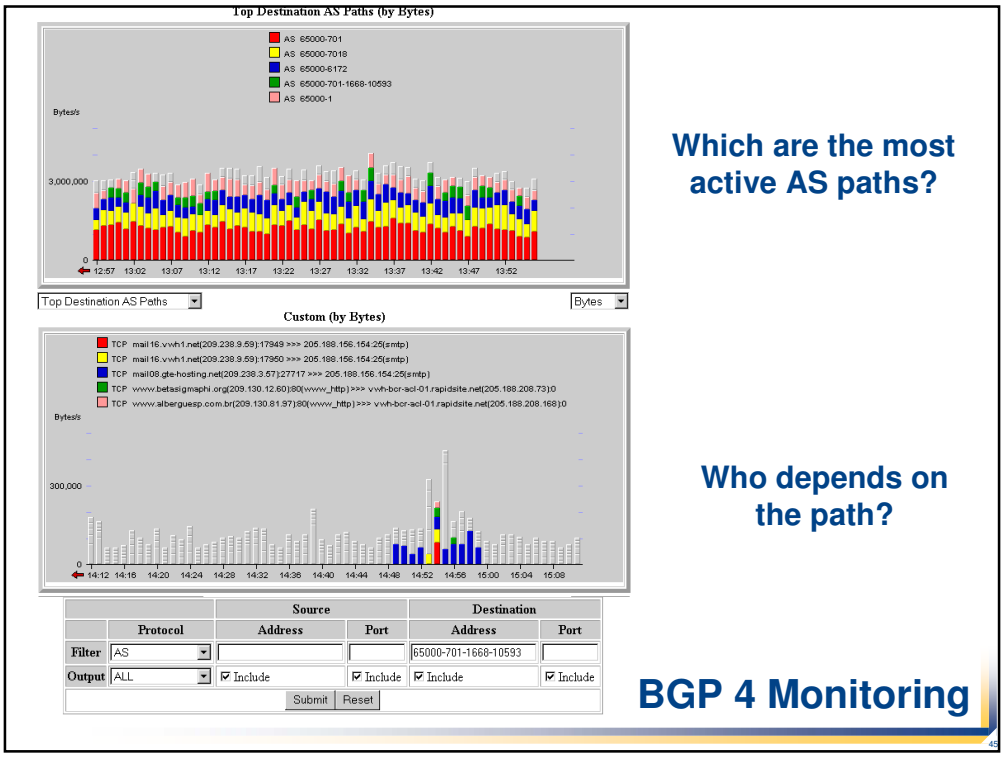
IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
ftp-data	20	195/7.0 KB			
ftp	21	2/53			
smtp	25	10/88		15/360	217.9.96.3
domain	53	25/3.1 KB	217.9.98.1		
http	80	1598/61.7 KB	213.165.64.97	16/334	66.196.72.99
pop3	110	18/352	192.67.198.79		
ntp	123	1/48		1/48	
epmap	135			1/0	64.68.82.172
netbios-ns	137	1/265		1/265	
codaauth2	370	1/41			
https	443	85/2.5 KB	65.54.229.253		

TCP/UDP Recently Used Ports

Client Port	Server Port
• infoman • nrcabq-lm • proshare1 • 39076 • ibm_wrless_lan	• ardus-cntl • ardus-trns • http • ddt • smtp

Report created on Tue Apr 6 09:47:17 2004 [58:03]
Generated by ntop v.2.2c MT (SSL) [i686-suse-linux] (10/02/03 10:22:30 PM build)
Listening on [eth1,sFlow-device] without a kernel (libpcap) filtering expression

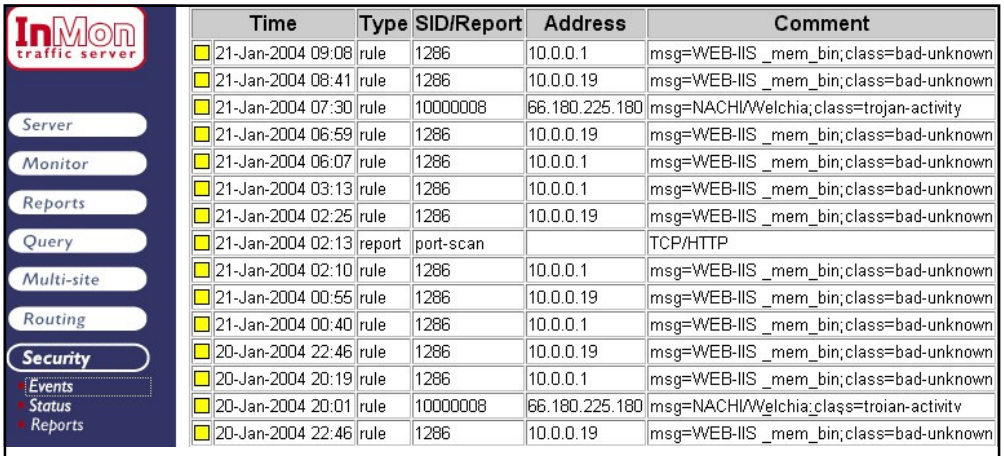
Info über Host TCP/UDP Ports



Which are the most active AS paths?

Who depends on the path?

BGP 4 Monitoring



Time	Type	SID/Report	Address	Comment
21-Jan-2004 09:08	rule	1286	10.0.0.1	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 08:41	rule	1286	10.0.0.19	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 07:30	rule	10000008	66.180.225.180	msg=NACHI/Welchia;class=trojan-activity
21-Jan-2004 06:59	rule	1286	10.0.0.19	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 06:07	rule	1286	10.0.0.1	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 03:13	rule	1286	10.0.0.1	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 02:25	rule	1286	10.0.0.19	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 02:13	report	port-scan		TCP/HTTP
21-Jan-2004 02:10	rule	1286	10.0.0.1	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 00:55	rule	1286	10.0.0.19	msg=WEB-IIS _mem_bin;class=bad-unknown
21-Jan-2004 00:40	rule	1286	10.0.0.1	msg=WEB-IIS _mem_bin;class=bad-unknown
20-Jan-2004 22:46	rule	1286	10.0.0.19	msg=WEB-IIS _mem_bin;class=bad-unknown
20-Jan-2004 20:19	rule	1286	10.0.0.1	msg=WEB-IIS _mem_bin;class=bad-unknown
20-Jan-2004 20:01	rule	10000008	66.180.225.180	msg=NACHI/Welchia;class=troian-activitv
20-Jan-2004 22:46	rule	1286	10.0.0.19	msg=WEB-IIS _mem_bin;class=bad-unknown

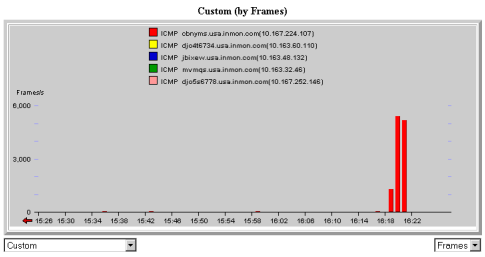
Traffic Server is configured to identify suspicious traffic. Many worms can be identified by looking for unique traffic signatures. The following signature is an example of the type of rules that Traffic Server uses to identify compromised hosts:

```
alert tcp $HOME_NET any -> any 80 (msg:"WEB-IIS _mem_bin"; flow: established;
uricontent:"/_mem_bin/"; nocase; classtype:bad-unknown; sid:1286; rev:1;)
```

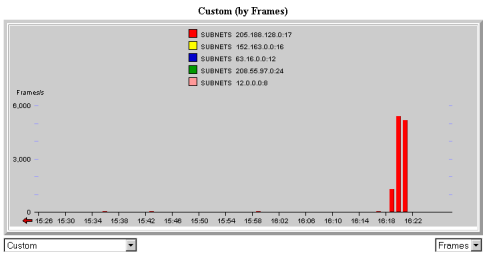
This rule looks for hosts on the home network that are sending web requests containing the pattern "/_mem_bin/" in the URL. When traffic matching the rule is identified, an event is generated.

Intrusion Detection

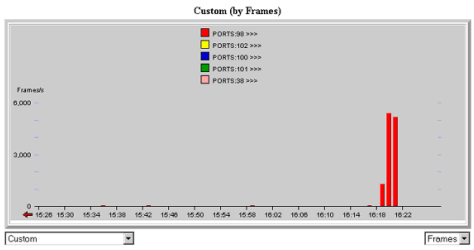
Who is being attacked?



Where is the attack originating?



How are packets entering site?



Block the attack.

The following commands will filter this attack on a Foundry Networks switch.

```
BigIron(config)# access-list 101 deny icmp
205.188.128.0/17 host 10.167.224.107
BigIron(config)# access-list 101 permit ip any any
BigIron(config)# int eth 2/6
BigIron(config)# ip access-group 101 in
BigIron(config)# write memory
```

Denial of Service Attack

Christoph Bronold
Christoph.Bronold@bkm-gmbh.com

BKM Dienstleistungs GmbH
Hauptstrasse 5
D-83607 Holzkirchen
www.bkm-gmbh.com