

Logging & Monitoring

Syslog, Timestamp, SNMP, Visualization, NMS

version : 2.0

Fakrul (Pappu) Alam
fakrul@dhakacom.com

Acknowledgement

- Original slides prepared by Randy Bush

In your network

- Traffic/access trend of this month
- Packets discarded yesterday
- Reason of the recent outage
- Person who changed the configuration
- ... and so on

Back Tracable

- What's happened in the past
- Syslog
 - to record messages from software
- SNMP
 - to monitor resources
- Netflow
 - to monitor packet flows

Syslog Message



```
Nov  9 15:19:14.390 UTC:  
config[65775]: %MGBL-SYS-5-  
CONFIG_I : Configured from  
console by maz on vty0  
(2001:db8:120:100:e1dd:  
97f3:fd98:a51f)
```



```
Nov 12 13:53:38 maz sudo:  
maz : user NOT in sudoers ;  
TTY=pts/3 ; PWD=/home/maz ;  
USER=root ; COMMAND=/bin/bash
```

Syslog Message

61547: Jan 18 05:41:07.636 UTC: %SEC-6-IPACCESSLOGP:
list AUTHORIZED_IPV4_HOST denied tcp
61.160.247.225(6000) -> 0.0.0.0(22), 1 packet

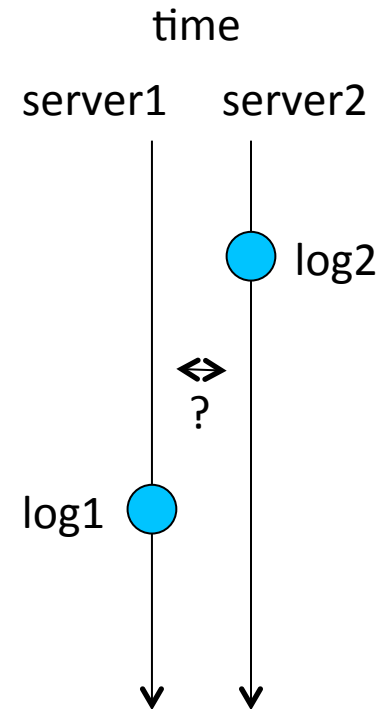
761548: Jan 18 05:56:37.735 UTC: %SEC-6-
IPACCESSLOGP: list AUTHORIZED_IPV4_HOST denied tcp
61.160.247.225(6000) -> 0.0.0.0(22), 46 packets

761549: Jan 18 06:00:53.626 UTC: %SEC-6-
IPACCESSLOGP: list AUTHORIZED_IPV4_HOST denied tcp
61.160.215.227(6000) -> 0.0.0.0(22), 1 packet

761550: Jan 18 06:30:07.280 UTC: %SEC-6-
IPACCESSLOGP: list AUTHORIZED_IPV4_HOST denied tcp
193.107.16.206(54630) -> 0.0.0.0(22), 1 packet

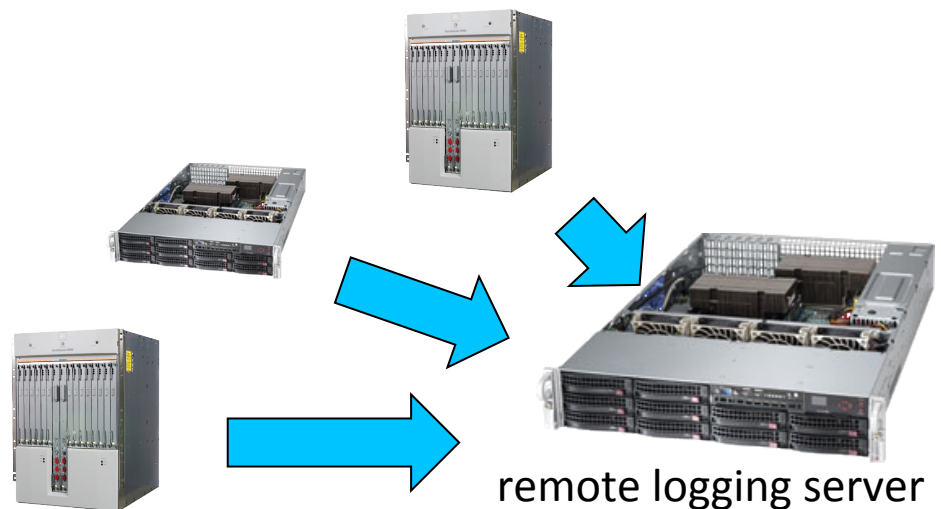
Timestamp

- Useful if system clock is synchronized
- ntp (network time protocol)
 - ntpd
- Timezone
 - UTC/GMT is scalable

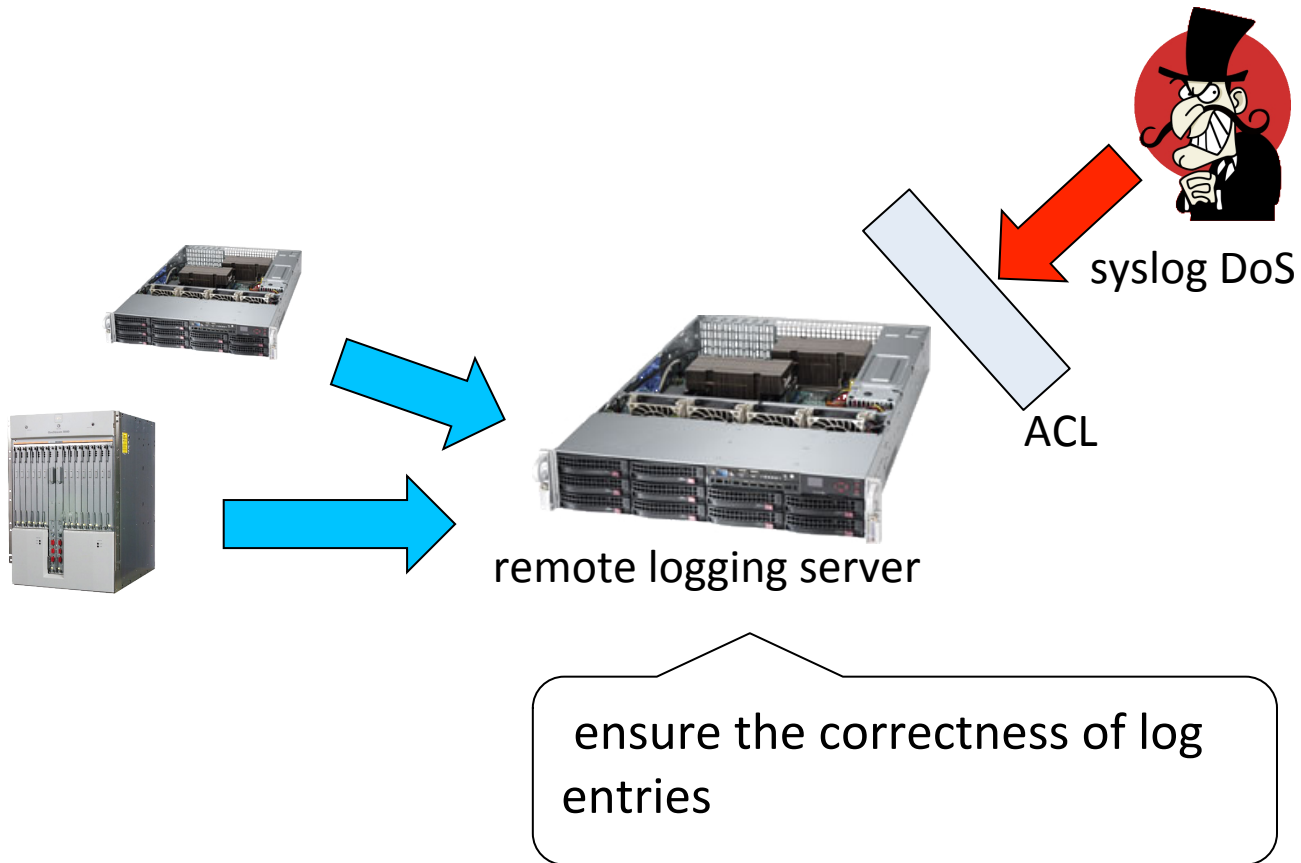


Remote Logging

- log messages could be modified/deleted
 - if the system is compromised
- remote logging servers
 - receive log messages from other devices
 - syslogd/syslog-ng

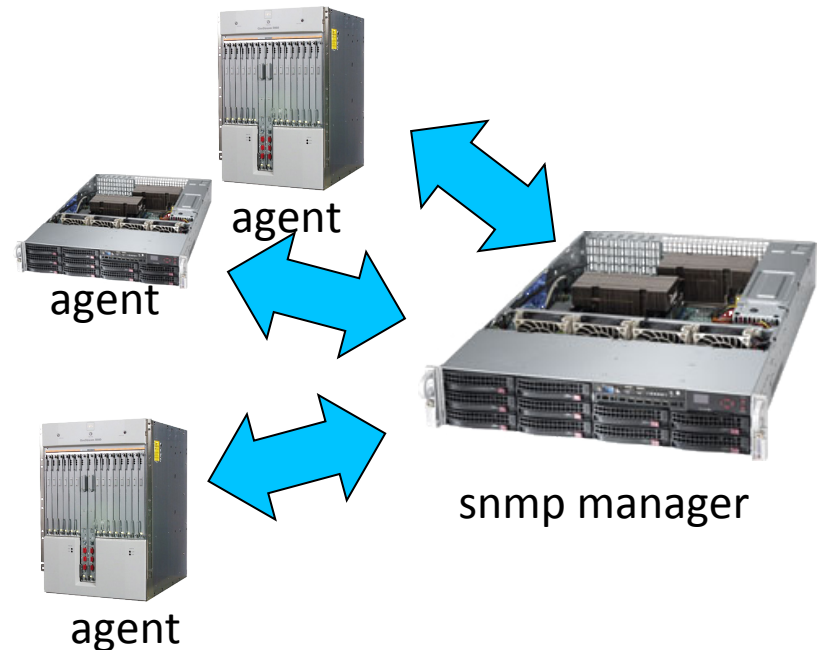


Protecting Syslog



SNMP

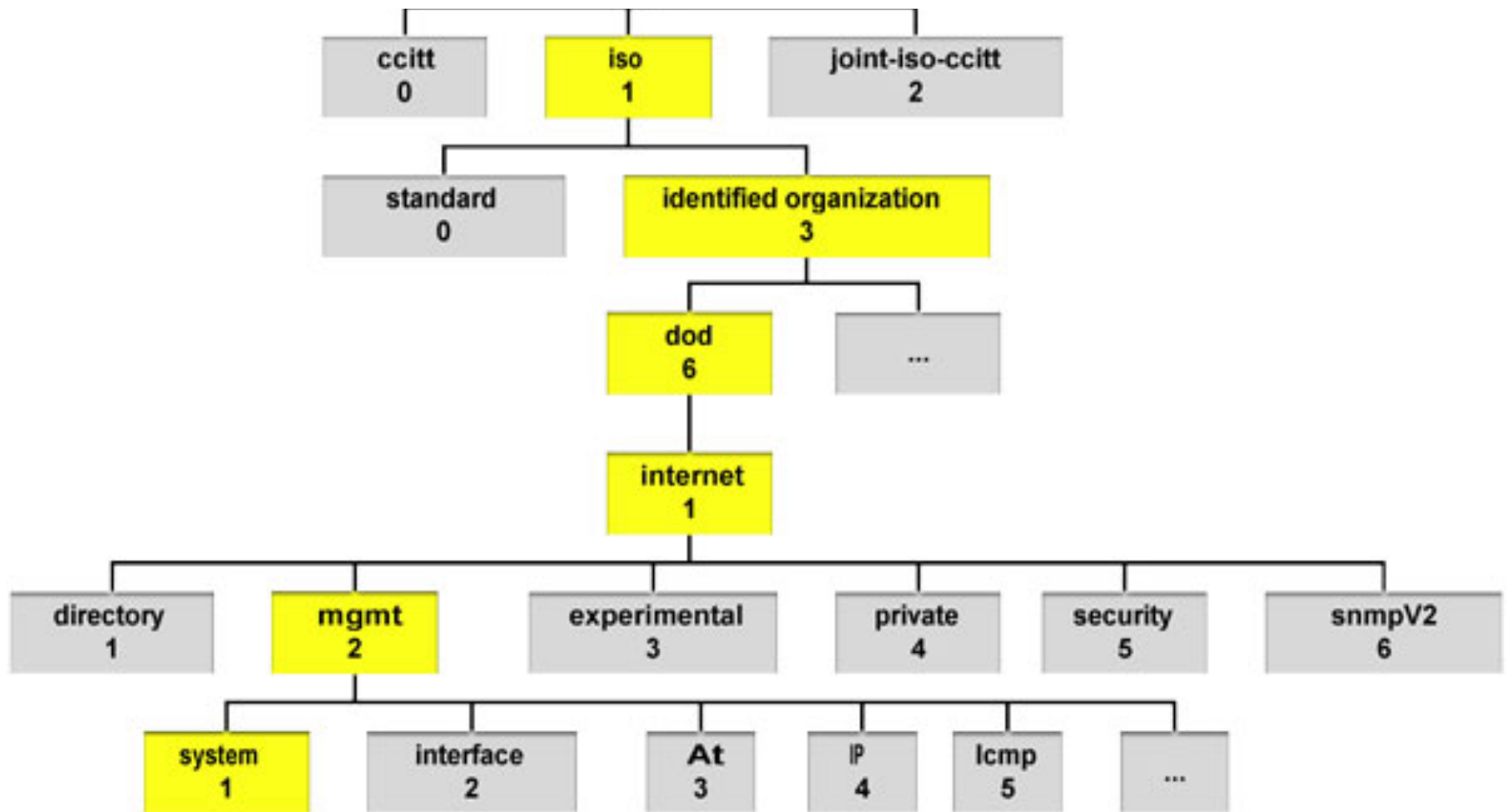
- Can read/write information and send a trap
 - use version 3, and set password
 - prevent 'write' function, or just disable it on agents
 - snmp agent/manager
- net-snmp/bsnmpd



SNMP MIB

- Management information base
 - MIB-2, IF-MIB, vender-specific MIB
 - You can get information if an agent supports the MIB you want
- You can specify the information by OIDs
- ifHCinOctets = .1.3.6.1.2.1.31.1.1.1.6
- ifHCOctets = .1.3.6.1.2.1.31.1.1.1.10

SNMP MIB



SNMP Counters

- Frequency of updating counters
 - Depends on agents (0-30sec)
 - 5min is widely used as snmp polling time
- Counter overflow
 - 32bit counters(ifIn/OutOctets) could wrap in 5.7min at 100Mbps
 - Consider 64bit counters(ifHCInOctets) for 1Gbps or more interfaces

Netflow

```
interface GigabitEthernet0/1
  description Connected with CORE01
  ...
  ip flow ingress
```

```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-cache timeout active 5
ip flow-export destination
147.28.0.666 42
```

cache flow

ROUTER#show ip cache flow

IP packet size distribution (490668M total packets):

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.027	.379	.119	.029	.018	.009	.124	.005	.004	.003	.021	.002	.003	.002	.001
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.001	.001	.003	.017	.222	.000	.000	.000	.000	.000	.000				

IP Flow Switching Cache, 278544 bytes

4081 active, 15 inactive, 1512415762 added

3296743739 age polls, 0 flow alloc failures

Active flows timeout in 30 minutes

Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 34056 bytes

0 active, 1024 inactive, 0 added, 0 added to flow

0 alloc failures, 0 force free

1 chunk, 1 chunk added

last clearing of statistics never

cache flow (cont)

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	7663265	1.7	12	56	21.8	0.0	0.9
TCP-FTP	42868722	9.9	4	55	42.0	0.4	0.4
TCP-FTPD	9159818	2.1	10	917	22.8	0.4	0.3
TCP-WWW	11050914413	2572.9	6	775	15507.4	0.3	0.4
TCP-SMTP	221463325	51.5	10	705	529.1	0.3	0.3
TCP-X	109028816	25.3	24	40	613.2	0.0	0.8
TCP-BGP	8448184	1.9	4	379	9.0	0.2	0.5
TCP-NNTP	167143	0.0	7	543	0.2	0.2	0.3
TCP-Frag	3453638	0.8	2	585	2.0	0.0	0.6
TCP-other	23446865011	5459.1	4	522	25183.1	0.2	0.5
UDP-DNS	971690745	226.2	2	73	494.8	0.0	0.8
UDP-NTP	12749722	2.9	7	77	23.1	0.0	0.9
UDP-TFTP	128546	0.0	6	192	0.1	0.3	0.8
UDP-Frag	62728581	14.6	9	771	144.5	0.4	0.4
UDP-other	24867360713	5789.8	7	334	45182.5	0.2	0.5
ICMP	2722517003	633.8	20	55	12923.4	0.0	0.7
IPINIP	56078918	13.0	66	1106	868.3	0.5	0.1
IPv6INIP	24870880	5.7	2	422	16.0	0.2	0.7
GRE	1962929974	457.0	26	405	12124.9	0.3	0.5
IP-other	355858828	82.8	6	333	533.8	0.2	0.5
Total:	65936946245	15352.1	7	417	114242.9	0.2	0.5

cache flow (cont)

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi0/0	68.67.176.23	Gi0/2.3207	118.179.151.13	06	0050	D59B	1
Gi0/2.6	118.179.218.28	Gi0/0*	103.4.110.173	06	C8AB	01BB	1
Gi0/2.8	118.179.151.67	Gi0/0*	217.76.78.143	01	0000	0300	1
Gi0/1.16	202.4.111.18	Gi0/0*	190.6.233.117	11	B6F1	C903	1
Gi0/2.8	118.179.151.67	Gi0/0*	81.39.204.17	11	2D6D	8143	2
Gi0/2.9	118.179.220.130	Gi0/0*	103.7.249.141	06	C4D5	01BB	2
Gi0/2.9	118.179.220.130	Gi0/0*	197.230.82.11	11	39B4	F3AB	1
Gi0/0	202.4.96.201	Gi0/1.36	10.6.4.15	11	3454	863C	21
Gi0/2.3207	118.179.151.12	Gi0/0	178.164.247.38	11	80B0	FD07	1
Gi0/0	82.227.60.18	Gi0/2.8	118.179.151.67	11	B1D5	2D6D	1
Gi0/0	124.6.236.250	Gi0/2.8	118.179.151.58	06	684D	5A6F	1
Gi0/2.24	118.179.175.2	Gi0/0*	192.111.149.74	06	C1D2	0D3D	3
Gi0/2.24	118.179.175.2	Gi0/0*	74.125.200.189	06	D93B	01BB	2
Gi0/0	10.111.102.10	Gi0/1.34	10.111.10.10	2F	0000	0000	3
Gi0/0	94.23.145.27	Gi0/2.9	118.179.220.130	06	0050	55F2	4
Gi0/2.9	118.179.220.130	Gi0/0*	23.67.252.171	06	D87A	01BB	1
Gi0/0	188.0.193.173	Gi0/2.8	118.179.151.67	11	8B6B	E070	1
Gi0/0	184.26.162.11	Gi0/2.8	118.179.151.67	06	01BB	0FC5	1

Top Talker

```
ip flow-top-talkers
top 50
sort-by bytes | packets
```

ROUTER#show ip flow top-talkers

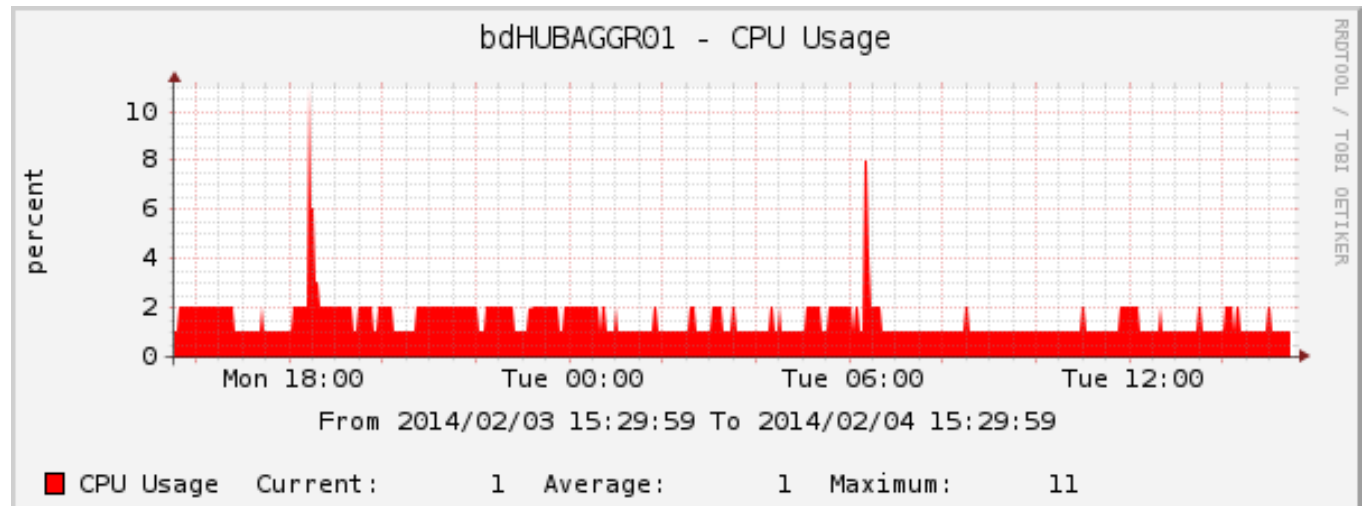
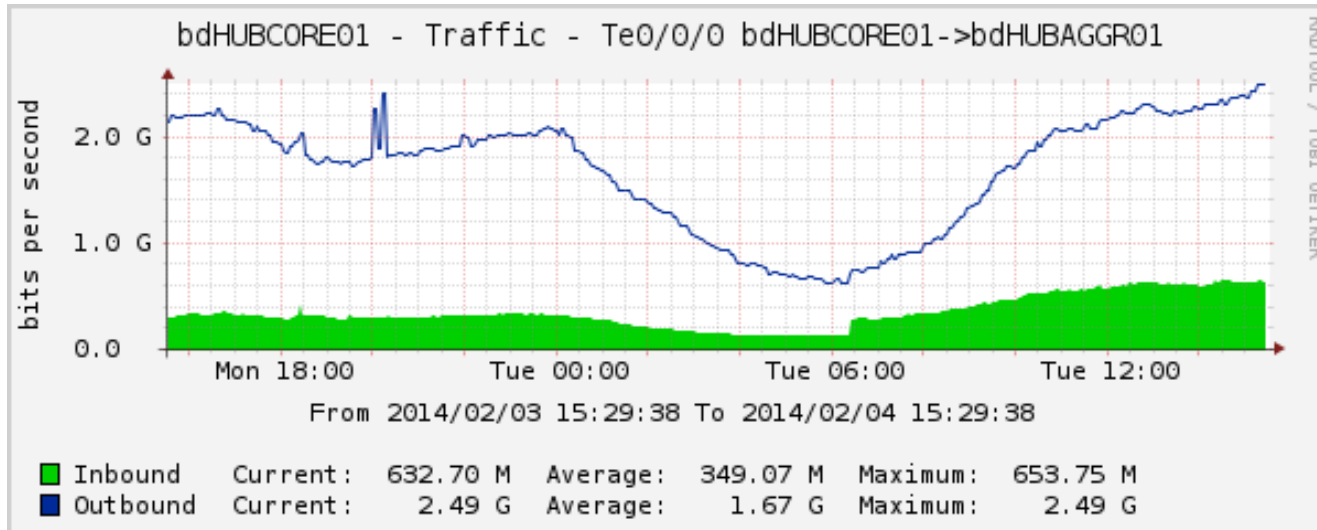
SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Bytes
Gi0/0	185.19.212.92	Gi0/2.6	118.179.218.253	06	0050	301D	573K
Gi0/2.9	118.179.220.131	Gi0/0*	118.179.208.186	2F	0000	0000	174K
Gi0/1.16	202.4.105.236	Gi0/0*	83.138.133.170	06	D128	C3C7	134K
Gi0/0	118.179.136.50	Gi0/0	10.10.13.18	04	0000	0000	115K
Gi0/0	118.179.136.50	Gi0/0	10.10.13.10	04	0000	0000	107K
Gi0/0	118.179.136.50	Gi0/0*	10.10.13.10	04	0000	0000	107K

Too much CLI

Visualization

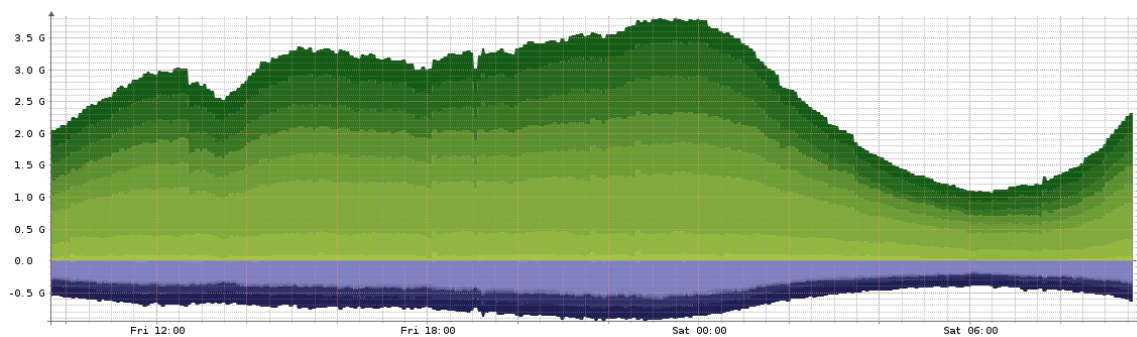
- Helps to understand a trend
 - cpu load, disk space, bps, pps, etc
 - also helps to convince your boss to upgrade ;)
- Visualization tools
 - MRTG
 - RRDtool

Visualization (MRTG/CACTI)

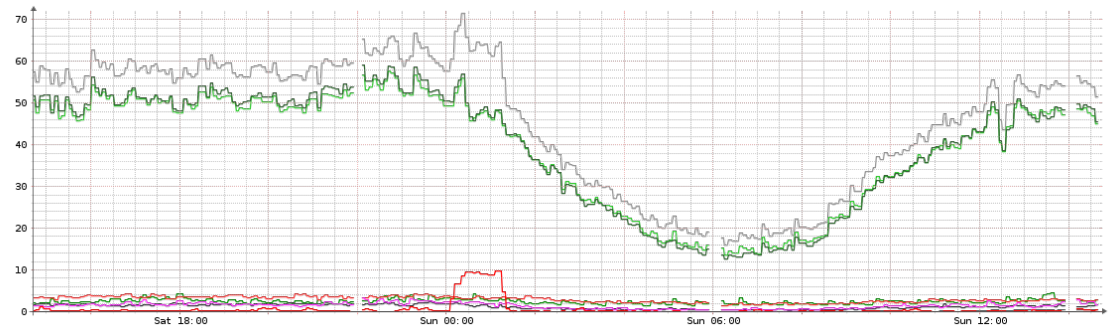


Visualization (Observium)

< Observium /
system health



bps	Current	Average	Maximum	Total
core01.bdhub.com	0.00 b	0.00 b	0.00 b	0.00 B
Gi0/1/2	0.00 b	0.00 b	0.00 b	0.00 B
aggr01.newtexbd.co	67.45Mb	73.45Mb	145.12Mb	6.28TB
Gi0/3/5	21.54Mb	17.22Mb	36.19Mb	1.47TB
core02.bdhub.com	275.18Mb	284.37Mb	393.41Mb	24.57TB
Pos0/2/1	301.37Mb	334.78Mb	526.07Mb	28.93TB
core02.bdhub.com	567.92Mb	663.72Mb	958.01Mb	57.35TB
Po1	31.54Mb	26.38Mb	42.42Mb	2.28TB
core02.bdhub.com	281.63Mb	332.89Mb	480.75Mb	28.76TB
Gi0/3/6	16.04Mb	12.49Mb	21.83Mb	1.08TB
core02.bdhub.com	286.94Mb	332.78Mb	488.19Mb	28.75TB
Gi0/3/7	15.46Mb	13.89Mb	25.46Mb	1.20TB
core01.bdhub.com	1.67 b	4.65 b	26.82 b	401.69kB
Gi0/1/0	3.53 b	1.43 b	3.76 b	123.84kB
core01.bdhub.com	236.24Mb	298.98Mb	607.57Mb	25.83TB
Pos3/0/0	102.08Mb	110.39Mb	171.33Mb	9.54TB
core02.bdhub.com	293.28Mb	369.63Mb	566.14Mb	31.94TB
Pos0/2/0	150.49Mb	159.15Mb	211.14Mb	13.75TB
core01.bdhub.com	303.42Mb	307.77Mb	436.79Mb	26.59TB
Pos3/0/1	6.14kb	9.35kb	268.78kb	807.67MB
Aggregate Totals	28.76TB	2.65Gb	3.80Gb	
	7.28TB	671.80Mb	948.79Mb	



Count	Last	Avg	Min	Max
Responses sent	51.6	45.7	15.9	71.5
Successful answers	45.0	39.4	13.6	57.7
Authoritative answer	2.8	2.5	1.5	4.5
Non-authoritative answer	45.5	39.6	12.5	59.0
Referral answer	0.0	0.0	0.0	0.0
Empty answers	1.6	1.2	310.2m	2.9
SERVFAIL answer	2.9	3.0	1.5	4.4
FORMERR answer	0.0	0.0	0.0	0.0
NXDOMAIN answers	1.8	1.5	377.7m	3.3
Dropped queries	394.2m	59.3m	0.0	580.3m
Failed queries	371.8m	674.4m	19.4m	9.8
Transfers completed	0.0	0.0	0.0	0.0

Observium / >
Application Monitoring

Visualization (Icinga/Nagios)

42 UP10 / 0 / 0 DOWN0 / 0 / 0 UNREACHABLE0 PENDING10 / 52 TOTAL

7 OK0 / 0 / 0 WARNING0 / 0 / 0 CRITICAL0 / 0 / 0 UNKNOWN0 PENDING0 / 7 TOTAL

General

Home

Documentation

Search:

Status

Tactical Overview

Host Detail

Service Detail

Hostgroup Overview

Hostgroup Summary

Servicegroup Overview

Servicegroup Summary

Status Map

Problems

Service Problems

Unhandled Services

Host Problems

Unhandled Hosts

All Unhandled Problems

All Problems

Network Outages

System

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Tactical Monitoring Overview

Last Updated: Sat Jan 18 09:40:39 BDT 2014 - Update in 78 seconds [pause]

Icinga 1.8.4 - Logged in as icingaadmin

Network Outages

0 Outages

Hosts

10 Down0 Unreachable42 Up0 Pending

Unhandled Problems10 Active

Services

0 Critical0 Warning0 Unknown7 Ok0 Pending

Service Checks

Active

Enabled7 EnabledEnabled

General

Home

Documentation

Search:

Status

Tactical Overview

Host Detail

Service Detail

Hostgroup Overview

Hostgroup Summary

Servicegroup Overview

Servicegroup Summary

Status Map

Problems

Service Problems

Unhandled Services

Host Problems

Unhandled Hosts

All Unhandled Problems

All Problems

Network Outages

System

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Reporting

Trends

Availability

Alert Histogram

Alert History

Alert Summary

Notifications

Current Network Status

Last Updated: Tue Feb 4 15:32:36 BDT 2014 - Update in 83 seconds [pause]

Icinga 1.8.4 - Logged in as icingaadmin

Warning: Status data OUTDATED! Last status data update was 119 seconds ago!

View Alert History For All Hosts

View Notifications For All Hosts

View Host AND Services For All Hosts

View Service Status Detail For All Hosts

ICINGA

48 / 0 / 00.02 / 10.05 / 1.084 s7 / 0 / 00.01 / 0.02 / 0.016 s15.05 / 15.41 / 15.213 s0.13 / 0.24 / 0.216 s

Commands for checked host(s)

Select command

Submit

Host Status Details For All Hosts

Page 1 of 1Results: 50

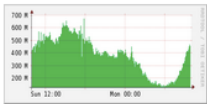
Host	Status	Last Check	Duration	Attempt	Status Information
localhost	UP	2014-02-04 15:25:58	334d 4h 12m 31s	1/10	PING OK - Packet loss = 0%, RTA = 0.04 ms
ALO-BD	UP	2014-02-04 15:25:58	19d 21h 53m 37s	1/10	PING OK - Packet loss = 0%, RTA = 2.19 ms
AsiaNet	UP	2014-02-04 15:25:58	41d 17h 34m 16s	1/10	PING OK - Packet loss = 0%, RTA = 1.21 ms
AsiaNet_Secondary	UP	2014-02-04 15:25:58	20d 22h 8m 4s	1/10	PING OK - Packet loss = 0%, RTA = 1.58 ms
BDHUB-Syhat-POP	UP	2014-02-04 15:25:58	35d 14h 38m 25s	1/10	PING OK - Packet loss = 0%, RTA = 5.60 ms
BHARTI-ASIA-STM-18	UP	2014-02-04 15:25:58	0d 2h 45m 21s+	1/10	PING OK - Packet loss = 0%, RTA = 72.73 ms
BRACNET-AS-24342	UP	2014-02-04 15:25:58	23d 15h 57m 52s	1/10	PING OK - Packet loss = 0%, RTA = 209.47 ms
BSCCL	UP	2014-02-04 15:25:58	109d 10h 28m 14s	1/10	PING OK - Packet loss = 0%, RTA = 1.97 ms
BpyOnline	DOWN	2014-02-04 15:25:58	25d 15h 51m 48s	1/10	PING CRITICAL - Packet loss = 100%
CITech_Cybernet	UP	2014-02-04 15:25:58	44d 16h 12m 31s	1/10	PING OK - Packet loss = 0%, RTA = 3.21 ms
CFM_BLUE	UP	2014-02-04 15:25:58	18d 15h 54m 15s	1/10	PING OK - Packet loss = 0%, RTA = 1.57 ms
Comilla_Online	UP	2014-02-04 15:25:58	5d 22h 5m 4s	1/10	PING OK - Packet loss = 0%, RTA = 1.01 ms
ConnecBO	UP	2014-02-04 15:25:58	77d 14h 40m 20s	1/10	PING OK - Packet loss = 0%, RTA = 190.90 ms
Daffodi	UP	2014-02-04 15:25:58	19d 22h 28m 35s	1/10	PING OK - Packet loss = 0%, RTA = 0.80 ms
DhakaCom	UP	2014-02-04 15:25:58	56d 18h 32m 54s	1/10	PING OK - Packet loss = 0%, RTA = 2.71 ms
Dhaka_Fiber_Net	UP	2014-02-04 15:25:58	2d 22h 46m 14s	1/10	PING OK - Packet loss = 0%, RTA = 2.12 ms

Visualization (Netflow)

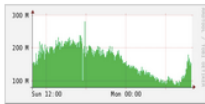
Home Graphs Details Alerts Stats Plugins live [Bookmark URL](#) Profile: live ▼

Profile: live

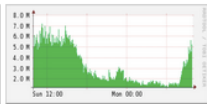
TCP



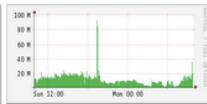
UDP



ICMP

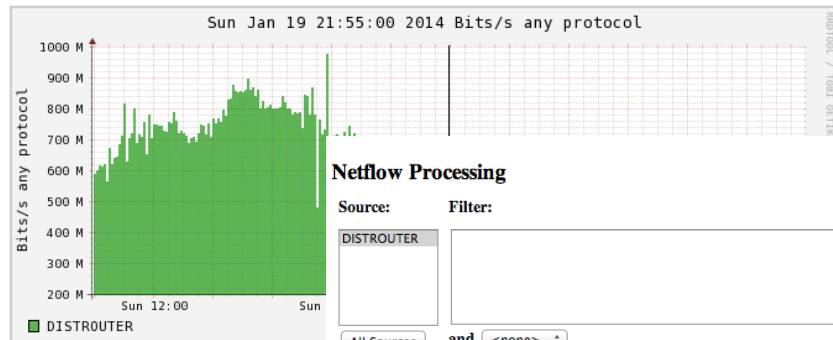


other



Profileinfo:

Type: live
Max: unlimited
Exp: never
Start: Oct 06 2012 - 13:27 BDT
End: Jan 20 2014 - 09:55 BDT



tstart 2014-01-19-21-55

tend 2014-01-19-21-55

Packets



Netflow Processing

Source:

DISTROUTER

Filter:

All Sources

and <none>

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: Any IP Address order by bytes

Limit: ☐ Packets ☐ 0

Output: ☐ / IPv6 long

Select Single Timeslot

Display

Clear Form process

```
** nfdump -M /usr/local/nfsen/profiles-data/live/DISTROUTER -T -R 2014/01/19/nfcapd.201401191740:2014/01/19/nfcapd.201401191755 -n 10 -s ip/bytes
nfdump filter:
any
```

Top 10 IP Addr ordered by bytes:

Date first seen	Duration	Proto	IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2014-01-19 17:41:00.980	1454.982	any	202.4.114.18	226291(2.0)	8.3 M(3.8)	6.9 G(6.0)	5737	38.0 M	828
2014-01-19 17:40:33.951	1483.004	any	118.179.151.67	942935(8.4)	10.5 M(4.8)	5.7 G(4.9)	7105	30.8 M	542
2014-01-19 17:40:31.153	1485.450	any	118.179.201.251	405171(3.6)	9.4 M(4.3)	5.1 G(4.4)	6336	27.4 M	540
2014-01-19 17:40:37.581	1479.406	any	118.179.133.146	622080(5.6)	8.0 M(3.6)	5.0 G(4.3)	5399	26.8 M	620
2014-01-19 17:40:34.318	1482.413	any	202.4.116.178	324428(2.9)	5.9 M(2.7)	3.8 G(3.3)	4002	20.6 M	644
2014-01-19 17:40:37.165	1478.789	any	118.179.151.58	72285(0.6)	4.9 M(2.2)	3.8 G(3.3)	3320	20.6 M	775
2014-01-19 17:40:43.393	1473.210	any	202.4.97.11	23036(0.2)	16.3 M(7.5)	3.2 G(2.7)	11088	17.3 M	194
2014-01-19 17:40:52.726	1463.461	any	180.211.201.12	5400(0.0)	2.6 M(1.2)	2.3 G(2.0)	1774	12.8 M	900
2014-01-19 17:41:36.049	1410.259	any	202.4.116.242	1219(0.0)	8.6 M(3.9)	2.3 G(2.0)	6081	13.1 M	268
2014-01-19 17:40:46.017	1468.963	any	202.4.96.69	6595(0.1)	1.6 M(0.7)	2.2 G(1.9)	1069	12.1 M	1414

Summary: total flows: 11205509, total bytes: 115.9 G, total packets: 218.9 M, avg bps: 623.8 M, avg pps: 147320, avg bpp: 529

Time window: 2014-01-19 17:40:31 - 2014-01-19 18:05:16

Total flows processed: 11205509, Blocks skipped: 0, Bytes read: 761983424

Sys: 3.820s flows/second: 2933058.4 Wall: 4.650s flows/second: 2409412.8

Visualization (Netflow)

Getting NTP reflection attack.

```
** nfdump -M /opt/nfsen/profiles-data/live/CORE01:AGGR01:CORE02 -T -r 2014/02/18/nfcapd.201402180805 -o long -c 50
nfdump filter:
dst net 223.27.112.11/32
```

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	Flows
2014-02-18 08:01:06.942	3.552	UDP	180.250.83.170:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.941	3.552	UDP	180.92.184.252:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.938	3.552	UDP	180.240.180.1:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.969	3.520	UDP	182.161.78.165:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.968	2.976	UDP	120.192.76.9:123	->	223.27.112.11:123		32	9	4212	1
2014-02-18 08:01:06.968	3.136	UDP	207.210.126.66:123	->	223.27.112.11:123		0	5	180	1
2014-02-18 08:01:06.966	2.976	UDP	211.140.5.53:123	->	223.27.112.11:123		0	7	3276	1
2014-02-18 08:01:06.966	3.552	UDP	182.161.78.169:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.966	3.456	UDP	211.73.23.2:123	->	223.27.112.11:123		0	6	216	1
2014-02-18 08:01:06.966	3.136	UDP	207.7.131.58:123	->	223.27.112.11:123		0	5	180	1
2014-02-18 08:01:06.963	3.552	UDP	182.161.78.155:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.962	3.136	UDP	207.210.122.18:123	->	223.27.112.11:123		0	5	180	1
2014-02-18 08:01:06.962	3.552	UDP	182.161.78.48:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.960	3.552	UDP	182.171.233.72:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.959	3.168	UDP	208.111.165.39:123	->	223.27.112.11:123		0	5	180	1
2014-02-18 08:01:06.958	3.552	UDP	182.171.245.163:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.957	3.552	UDP	182.161.78.196:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.933	3.840	UDP	188.64.50.12:123	->	223.27.112.11:123		0	467	215532	1
2014-02-18 08:01:06.933	3.584	UDP	182.173.178.170:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.962	2.976	UDP	35.8.223.116:123	->	223.27.112.11:123		0	289	135252	1
2014-02-18 08:01:06.961	3.552	UDP	182.18.194.20:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.960	3.616	UDP	184.22.229.50:123	->	223.27.112.11:123		0	407	187452	1
2014-02-18 08:01:06.960	2.976	UDP	182.173.178.170:123	->	223.27.112.11:123		0	600	280800	1
2014-02-18 08:01:06.958	3.552	UDP	182.24.124.244:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.955	0.000	UDP	219.121.145.218:123	->	223.27.112.11:123		16	100	46800	1
2014-02-18 08:01:06.954	3.584	UDP	182.55.103.96:123	->	223.27.112.11:123		0	7	252	1
2014-02-18 08:01:06.952	3.584	UDP	182.55.116.234:123	->	223.27.112.11:123		0	7	252	1

Visualize Log

- ELSA (enterprise-log-search-and-archive)
 - Syslog framework build on Syslog-NG, MySql
 - High-volume receiving/indexing (a single node can receive > 30k logs/sec, sustained)
 - Dashboards using Google Visualizations
 - Email alerting, scheduled reports
 - Plugin architecture for web interface
 - Distributed architecture for clusters
 - Ships with normalization for some Cisco logs, Snort/Suricata, Bro, and Windows via Eventlog-to-Syslog or Snare
- <https://code.google.com/p/enterprise-log-search-and-archive/>

Visualize Log

- ELSA (enterprise-log-search-and-archive)

Queries ▾ Admin ▾

Enterprise Log Search and Archive

Query

Start Time Add Term Group By

End Time Use

srcip:10.124.19.11 dstip>74.125.0.0 dstip<74.125.255.255 (5486)

Result Options... ▾

Field Summary

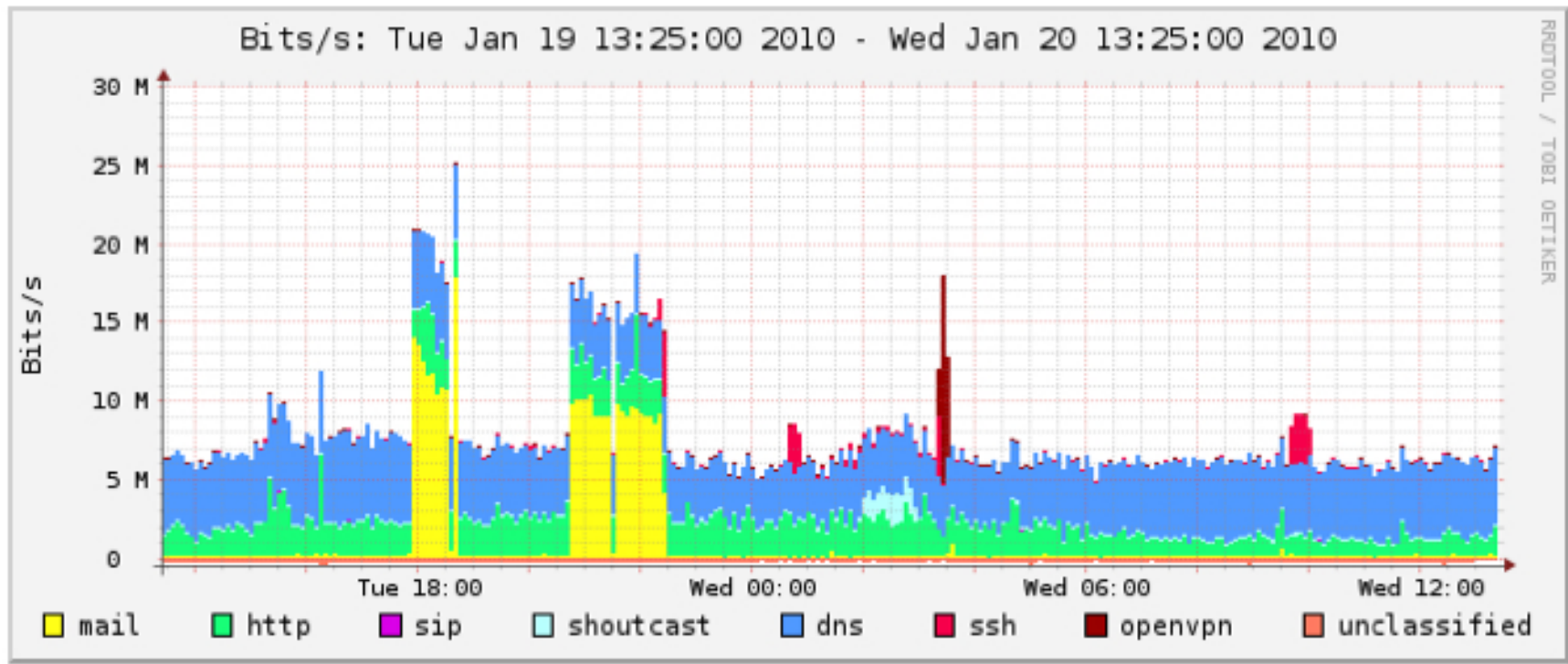
host(3) program(2) class(2) srcip(1) dstip(19) status_code(2) content_length(21) country_code(1) method(2) site(5) uri(15) referer(3) user_agent(4) domains(5) proto(1) srcport(41) dstport(2) conn_bytes(34) o_int(2) i_int(1) conn_duration(20)

Records: 100 / 5486 4732 ms

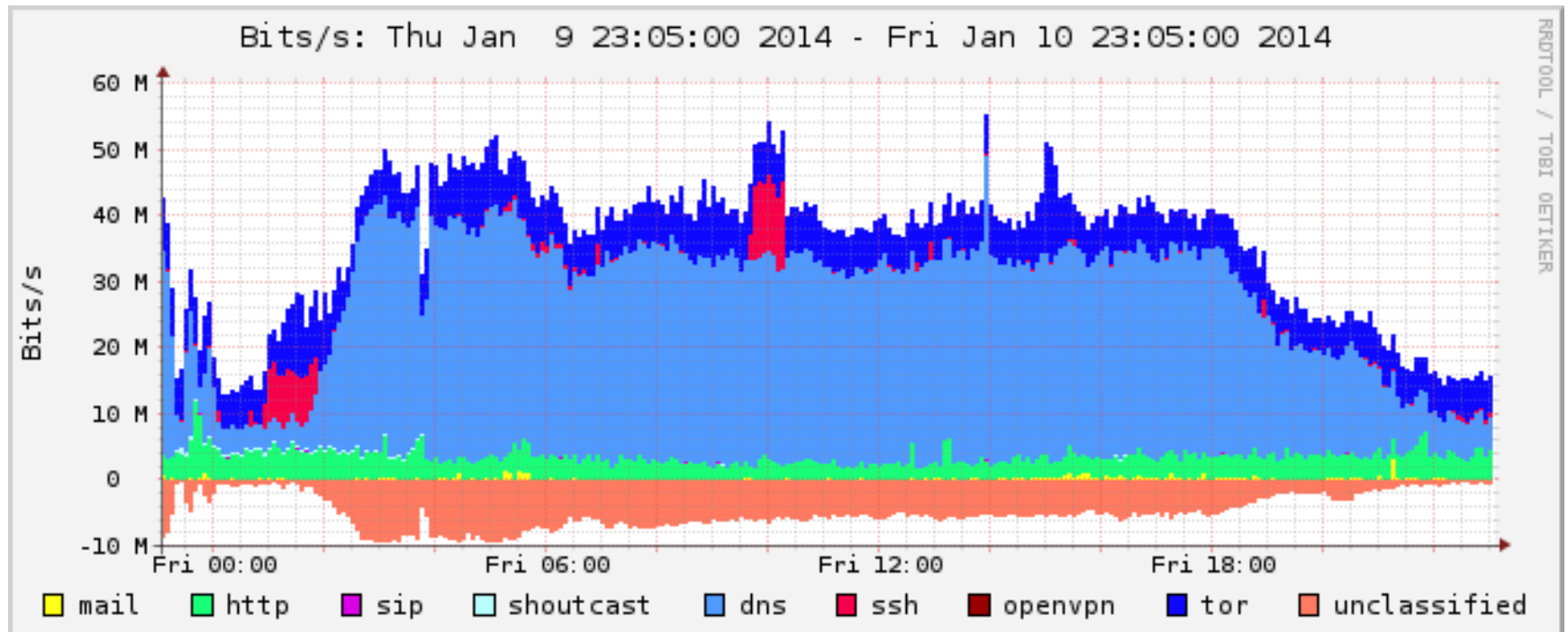
	Timestamp ▴	Fields
Info	Sat Mar 05 01:14:44	Teardown TCP connection 144677618557444178 for DET-SEC-124.19:10.124.19.11/3520 to OUTSIDE:74.125.225.4/443 duration 0:04:00 bytes 5188 TCP FINs host=165.189.82.68 program=fwsm-5-302014 class=FIREWALL CONNECTION END proto=TCP srcip=10.124.19.11 srcport=3520 dstip=74.125.225.4 dstport=443 conn_bytes=5188 o_int=DET-SEC-124.19 i_int=OUTSIDE conn_duration=0:04:00
Info	Sat Mar 05 01:14:44	Teardown TCP connection 144677618557444179 for DET-SEC-124.19:10.124.19.11/3521 to OUTSIDE:74.125.225.4/80 duration 0:04:00 bytes 1690 TCP FINs host=165.189.82.68 program=fwsm-5-302014 class=FIREWALL CONNECTION END proto=TCP srcip=10.124.19.11 srcport=3521 dstip=74.125.225.4 dstport=80 conn_bytes=1690 o_int=DET-SEC-124.19 i_int=OUTSIDE conn_duration=0:04:00
Info	Sat Mar 05 01:28:52	10.124.19.11 74.125.225.13 POST[safebrowsing.clients.google.com/safebrowsing/downloads?client=navclient-auto-ffox&appver=3.6.14&pver=2.2&wkey=AKEgNisfcTJ9nd0qpBpORbqLanfE0NeoSWlcaou4yRQUBrsolysQ8gRp7EIRRV6tPf1WB30WfcRowXyid82xtRy1A5-Vpu3Og== - Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.14) Gecko/20110218 Firefox/3.6.14 (.NET CLR 3.5.30729)] com.google.com,clients.google.com,safebrowsing.clients.google.com 200 502 8583 host=10.68.2.28 program=url class=URL srcip=10.124.19.11 dstip=74.125.225.13 status_code=200 content_length=502 country_code=US method=POST site=safebrowsing.clients.google.com uri=safebrowsing/downloads?client=navclient-auto-ffox&appver=3.6.14&pver=2.2&wkey=AKEgNisfcTJ9nd0qpBpORbqLanfE0NeoSWlcaou4yRQUBrsolysQ8gRp7EIRRV6tPf1WB30WfcRowXyid82xtRy1A5-Vpu3Og== referer=- user_agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.14) Gecko/20110218 Firefox/3.6.14 (.NET CLR 3.5.30729) domains=com.google.com,clients.google.com,safebrowsing.clients.google.com
Info	Sat Mar 05 01:30:52	Teardown TCP connection 144677618557444322 for DET-SEC-124.19:10.124.19.11/3586 to OUTSIDE:74.125.225.13/80 duration 0:02:00 bytes 2419 TCP FINs host=165.189.82.68 program=fwsm-5-302014 class=FIREWALL CONNECTION END proto=TCP srcip=10.124.19.11 srcport=3586 dstip=74.125.225.13 dstport=80 conn_bytes=2419 o_int=DET-SEC-124.19 i_int=OUTSIDE conn_duration=0:02:00
Info	Sat Mar 05 01:30:56	Teardown TCP connection 145634550155716435 for INSIDE:10.124.19.11/3586 to OUTSIDE:74.125.225.13/80 duration 0:02:00 bytes 2419 TCP FINs host=165.189.65.10 program=fwsm-5-302014 class=FIREWALL CONNECTION END proto=TCP srcip=10.124.19.11 srcport=3586 dstip=74.125.225.13 dstport=80 conn_bytes=2419 o_int=INSIDE i_int=OUTSIDE conn_duration=0:02:00
Info	Sat Mar 05 01:34:23	10.124.19.11 74.125.225.15 POST[safebrowsing.clients.google.com/safebrowsing/downloads?client=googlechrome&appver=9.0.597.107&pver=2.2&wkey=AKEgNiuVZBzXpt50yLGAJhQqibY93ybZPnB-BWcm7bISuv3qSKsmEUXDTJRR8P2EfxbKLNNgmwS8avJ-SIW_FMLwsdJHrqQw== - Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.107 Safari/534.13 com.google.com,clients.google.com,safebrowsing.clients.google.com 200 502 8583 host=10.68.2.28 program=url class=URL srcip=10.124.19.11 dstip=74.125.225.15 status_code=200 content_length=502 country_code=US method=POST site=safebrowsing.clients.google.com uri=safebrowsing/downloads?client=googlechrome&appver=9.0.597.107&pver=2.2&wkey=AKEgNiuVZBzXpt50yLGAJhQqibY93ybZPnB-BWcm7bISuv3qSKsmEUXDTJRR8P2EfxbKLNNgmwS8avJ-SIW_FMLwsdJHrqQw== referer=- user_agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.107 Safari/534.13 domains=com.google.com,clients.google.com,safebrowsing.clients.google.com
Info	Sat Mar 05 01:38:23	Teardown TCP connection 144677618557444337 for DET-SEC-124.19:10.124.19.11/3592 to OUTSIDE:74.125.225.15/80 duration 0:04:00 bytes 2419 TCP FINs host=165.189.82.68 program=fwsm-5-302014 class=FIREWALL CONNECTION END proto=TCP srcip=10.124.19.11 srcport=3592 dstip=74.125.225.15 dstport=80 conn_bytes=2419 o_int=DET-SEC-124.19 i_int=OUTSIDE conn_duration=0:04:00
Info	Sat Mar 05 01:38:25	Teardown TCP connection 145143321861170861 for INSIDE:10.124.19.11/3592 to OUTSIDE:74.125.225.15/80 duration 0:04:00 bytes 2419 TCP FINs host=165.189.65.10 program=fwsm-5-302014 class=FIREWALL CONNECTION END proto=TCP srcip=10.124.19.11 srcport=3592 dstip=74.125.225.15 dstport=80 conn_bytes=2419 o_int=INSIDE i_int=OUTSIDE conn_duration=0:04:00

Know Your Traffic

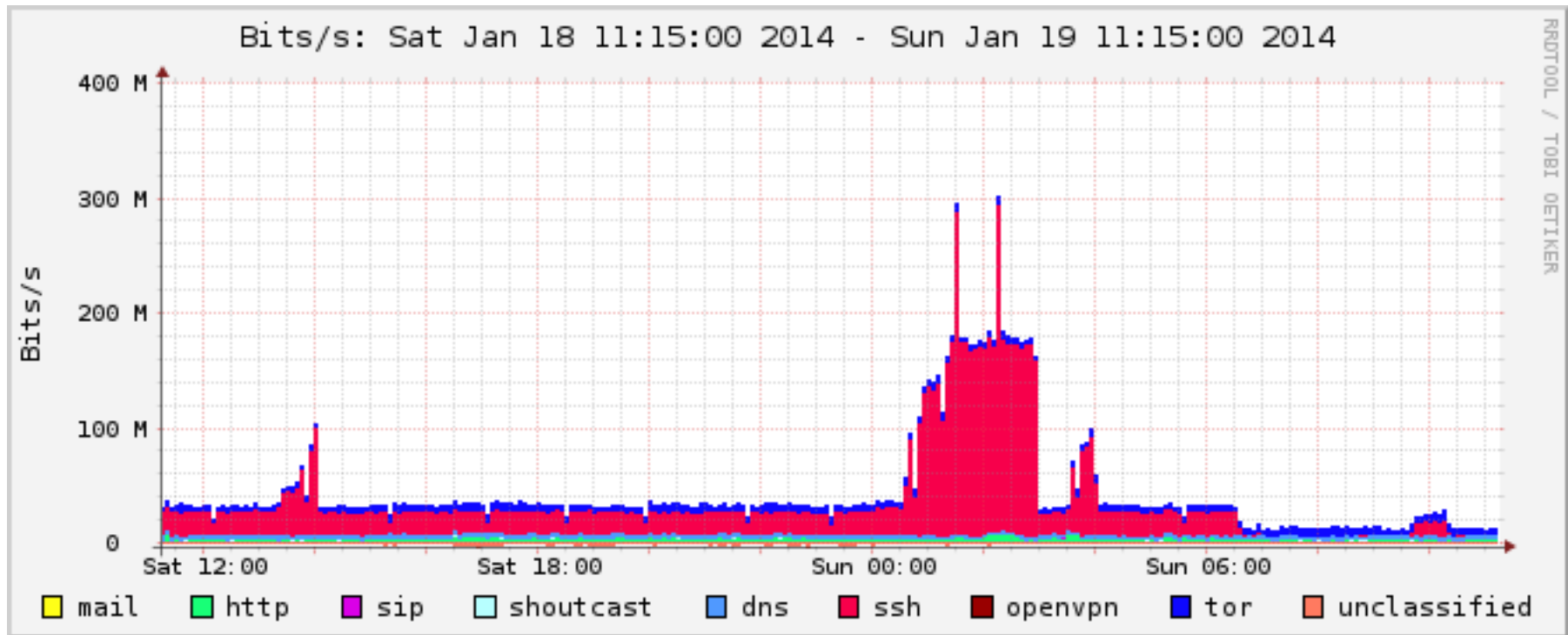
Sudden Spikes in Mail Volume



Too Much DNS Traffic



It's Not an Attack (It is Backup)



Visualization

- Provide monitoring your devices, and notify you in case of troubles
 - even if you are sleeping
 - syslog, snmp, ping, service(http, smtp, dns)
- Many implementations
 - Nagios, Cacti, Observium etc.
- It's really important to know your traffic pattern.