Security Monitoring and Investigation

Paul Haskell-Dowland

School of Science
Edith Cowan University

Overview

- Awareness of assets
- Introduction to monitoring
- SNMP
- Netflow
- Intrusion detection
- Investigation

WHAT ARE YOU PROTECTING?

Defining a perimeter…

- It was once possible to draw a line around your network to define your borders…
  - Servers
  - Desktop computers
  - Possibly laptops

- Plus (often overlooked)
  - Network infrastructure

What is an end-point?

- But with advances in IT and in particular the increased use of personal/companion devices, that border is no longer as clearly defined:
  - Smartphones
  - Table devices
  - USB keys
  - Portable hard drives
  - Social media/cloud-based services

What is an end-point?

- There is also a plethora of network connected devices that are often overlooked:
  - Network attached storage (NAS)
  - IP cameras (CCTV)
  - Building Management Systems (BMS)
  - Projectors
  - Printers/copiers/Multi Function Devices
  - Even domestic WiFi routers/switches introduced by employees into an organisation

Think it won’t happen?

- Protocol vulnerabilities
  - Just think about SSL!
- Botnet attack
  - Webcams, DVRs
- Amplification/reflection attack
  - DNS, NTP

- Don’t forget users!

INTRODUCTION TO MONITORING

What do we mean by monitoring

- Can use various tools to measure/evaluate:
  - – Performance
    - Most users mean speed/reliability
    - Reality = complex combination of theoretical and actual bandwidth; latency; packet loss; utilisation; configuration; device load and many others
  - – Security
    - Users often mean Firewall and AV
    - Reality = IDS, IPS, proxies, logs, access control, SEIM (more on these later)

Purpose of monitoring

- Monitor for indicators
  - Discovery of devices
  - Uptime of devices
  - Rule based alerts
  - Behaviour of devices
    - Top talkers and/or listeners
  - Utilisation of devices/links
    - Unusual patterns
    - Changes of utilisation (CPU, memory, ports)

How do we monitor?

- Active or passive monitoring
  - i.e. intrusive or non-intrusive

- We can monitor in an active manner, but this may introduce consequences/side-effects or may be visible to others
- Can monitor the network in a purely passive manner (not interfering with the network) but may miss traffic

Active monitoring

- Active monitoring involves
  - Sending/receiving packets into the network to elicit responses
  - Processing the received packets
  - Calculating metrics/reporting
  - Logging

Passive monitoring

- Usually conducted at a aggregation point
  - Often at the internet/uplink connection
    - aggregation vs distribution
  - Frequently implemented using span/mirror ports
  - Can combine with IDS/IPS
- See ‘all’ traffic passing through monitor point
  - Difficulty with encrypted protocols (may need to combine passive and active approaches)

Monitoring considerations

- Infrastructure
  - Topology, technology
- Traffic level at monitor point
- Application protocols
  - E.g. DNS, Web, P2P
  - What about hidden/tunnelled protocols
- How can we define *typical* behaviour / characteristics / activity?

Challenges

- Capture and log all data
  - – There is just too much; if we filter, what do we lose?
  - – Data storage (store and then access) – how much, how long?
  - – Privacy concerns
  - – Analysis time

Simple solution

- Capture traffic using Linux host
  - tcpdump etc.
  - Store to pcap files etc.
  - Parse, search, extract useful data
- Reporting
  - Visualisations (e.g. gnuplot)
  - RRD visualisations
  - Log to database

Packet sniffers

- Interface configured in ‘promiscuous’ mode
- Can be implemented in
  - hardware devices (e.g. router)
  - software computer (physical or virtual)
- Often described as sniffers or analysers at the network, packet or protocol level

Connection analysis

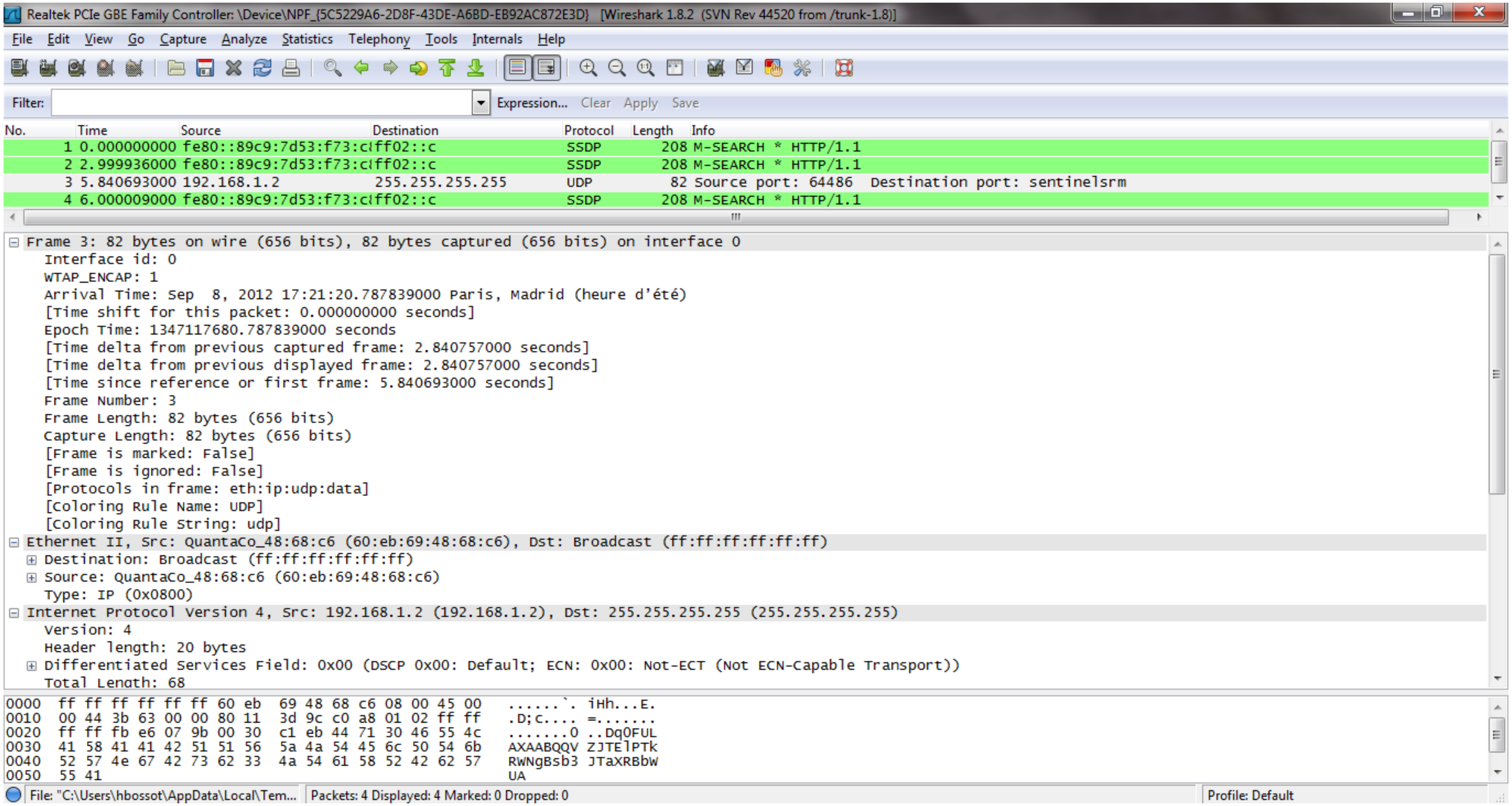
- Extract network/application parameters
  - Packets are correlated into connections
- Can be run in passive host, but more effective using netflow (and others) embedded in high level routers etc.
- Discussion on netflow later

SOME EXAMPLES

Wireshark

- Best known example of a packet sniffer/protocol analyser/network tool
- Supports thousands of protocols from frame up to application level
- Supports filtering of captured traffic as well as de-encapsulation, decoding, conversion and export of data

Wireshark



Realtek PCIe GBE Family Controller: \Device\NPF_{5C5229A6-2D8F-43DE-A6BD-EB92AC872E3D}   [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.      Time        Source                    Destination       Protocol  Length Info
       1 0.000000000 fe80::89c9:7d53:f73:c…ff02::c            SSDP         208 M-SEARCH * HTTP/1.1
       2 2.999936000 fe80::89c9:7d53:f73:c…ff02::c            SSDP         208 M-SEARCH * HTTP/1.1
       3 5.840693000 192.168.1.2           255.255.255.255    UDP           82 Source port: 64486  Destination port: sentinelsrm
       4 6.000009000 fe80::89c9:7d53:f73:c…ff02::c            SSDP         208 M-SEARCH * HTTP/1.1
```

```
⊟ Frame 3: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
    Interface id: 0
    WTAP_ENCAP: 1
    Arrival Time: Sep  8, 2012 17:21:20.787839000 Paris, Madrid (heure d'été)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1347117680.787839000 seconds
    [Time delta from previous captured frame: 2.840757000 seconds]
    [Time delta from previous displayed frame: 2.840757000 seconds]
    [Time since reference or first frame: 5.840693000 seconds]
    Frame Number: 3
    Frame Length: 82 bytes (656 bits)
    Capture Length: 82 bytes (656 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
⊟ Ethernet II, Src: QuantaCo_48:68:c6 (60:eb:69:48:68:c6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: QuantaCo_48:68:c6 (60:eb:69:48:68:c6)
    Type: IP (0x0800)
⊟ Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 68
```

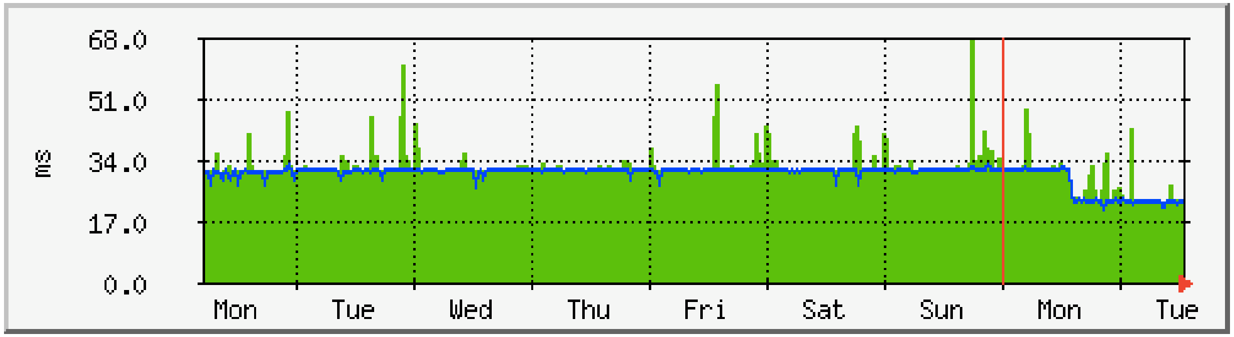
```
0000  ff ff ff ff ff ff 60 eb  69 48 68 c6 08 00 45 00   ......`. iHh...E.
0010  00 44 3b 63 00 00 80 11  3d 9c c0 a8 01 02 ff ff   .D;c.... =.......
0020  ff ff fb e6 07 9b 00 30  c1 eb 44 71 30 46 55 4c   .......0 ..Dq0FUL
0030  41 58 41 41 42 51 51 56  5a 4a 54 45 6c 50 54 6b   AXAABQQV ZJTElPTk
0040  52 57 4e 67 42 73 62 33  4a 54 61 58 52 42 62 57   RWNgBsb3 JTaXRBbW
0050  55 41                                              UA
```

File: "C:\Users\hbossot\AppData\Local\Tem...
Packets: 4 Displayed: 4 Marked: 0 Dropped: 0
Profile: Default

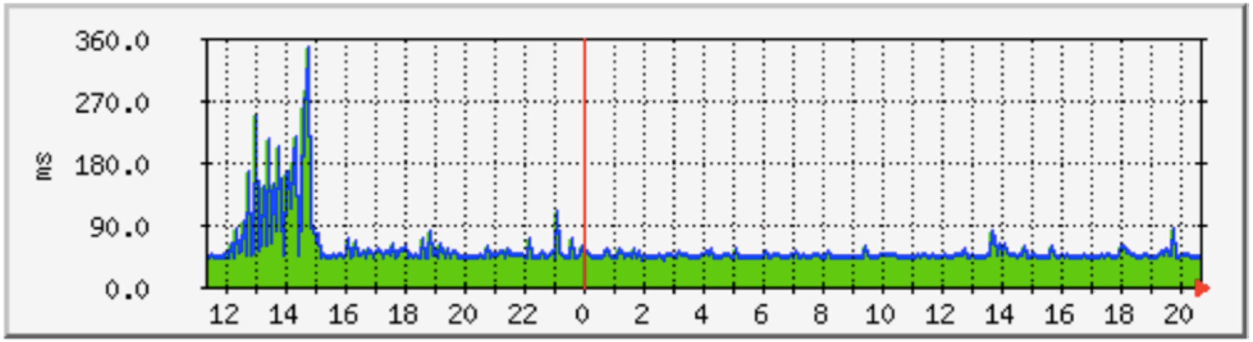
Image from: https://commons.wikimedia.org/wiki/File:Wireshark_-_UDP.png

IPv6 example: http://packetpushers.net/ipv6-and-the-importance-of-the-icmpv6-packet-too-big-message/

RRD graphs

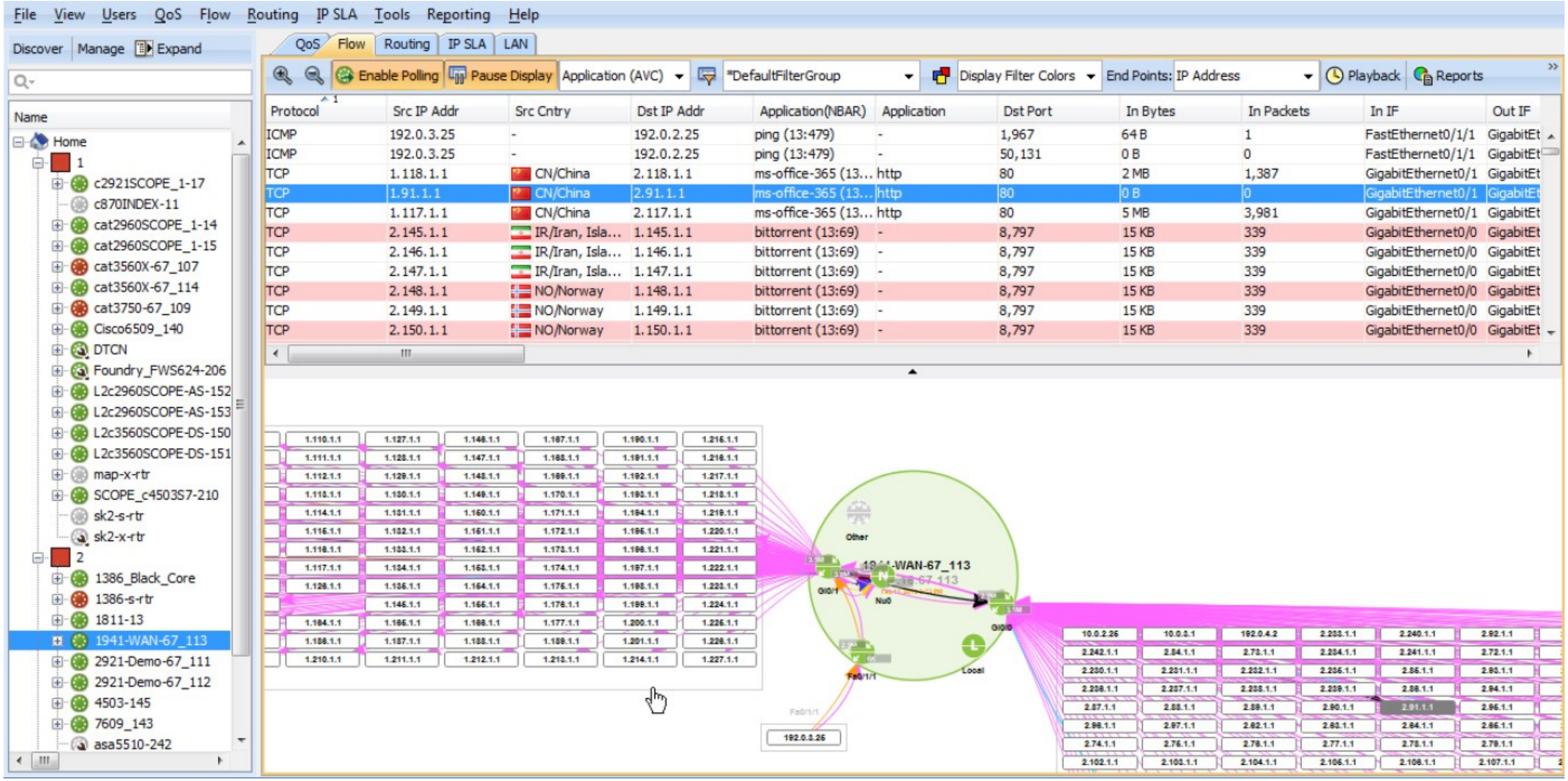


	Max	Average	Current
RTTavg	67.0 ms (0.7%)	31.0 ms (0.3%)	22.0 ms (0.2%)
RTTmin	32.0 ms (0.3%)	30.0 ms (0.3%)	22.0 ms (0.2%)



	Max	Average	Current
Ping in ms	344.0 ms (3.4%)	52.0 ms (0.5%)	41.0 ms (0.4%)

Liveaction

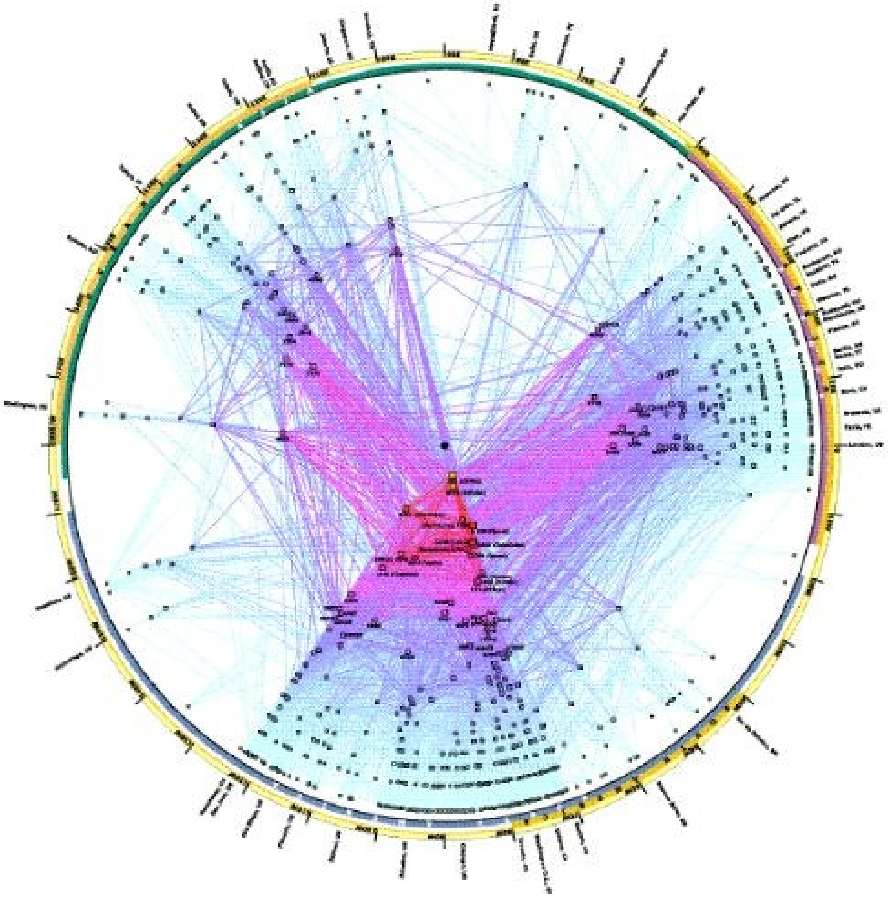


Protocol	Src IP Addr	Src Cntry	Dst IP Addr	Application(NBAR)	Application	Dst Port	In Bytes	In Packets	In IF	Out IF
ICMP	192.0.3.25	-	192.0.2.25	ping (13:479)	-	1,967	64 B	1	FastEthernet0/1/1	GigabitEt
ICMP	192.0.3.25	-	192.0.2.25	ping (13:479)	-	50,131	0 B	0	FastEthernet0/1/1	GigabitEt
TCP	1.118.1.1	CN/China	2.118.1.1	ms-office-365 (13...	http	80	2 MB	1,387	GigabitEthernet0/1	GigabitEt
TCP	1.91.1.1	CN/China	2.91.1.1	ms-office-365 (13...	http	80	0 B	0	GigabitEthernet0/1	GigabitEt
TCP	1.117.1.1	CN/China	2.117.1.1	ms-office-365 (13...	http	80	5 MB	3,981	GigabitEthernet0/1	GigabitEt
TCP	2.145.1.1	IR/Iran, Isla...	1.145.1.1	bittorrent (13:69)	-	8,797	15 KB	339	GigabitEthernet0/0	GigabitEt
TCP	2.146.1.1	IR/Iran, Isla...	1.146.1.1	bittorrent (13:69)	-	8,797	15 KB	339	GigabitEthernet0/0	GigabitEt
TCP	2.147.1.1	IR/Iran, Isla...	1.147.1.1	bittorrent (13:69)	-	8,797	15 KB	339	GigabitEthernet0/0	GigabitEt
TCP	2.148.1.1	NO/Norway	1.148.1.1	bittorrent (13:69)	-	8,797	15 KB	339	GigabitEthernet0/0	GigabitEt
TCP	2.149.1.1	NO/Norway	1.149.1.1	bittorrent (13:69)	-	8,797	15 KB	339	GigabitEthernet0/0	GigabitEt
TCP	2.150.1.1	NO/Norway	1.150.1.1	bittorrent (13:69)	-	8,797	15 KB	339	GigabitEthernet0/0	GigabitEt

http://www.liveaction.com/solutions/cybersecurity/

Caida tools

- Anonymisation
  - Helps with preserving privacy
- Geographic
  - Link traffic patterns/behaviour with geographical location
- Performance
  - Speed and responsiveness
- Topology
  - Visualising infrastructure
  - AS, IPv4 and v6



http://www.caida.org/tools/

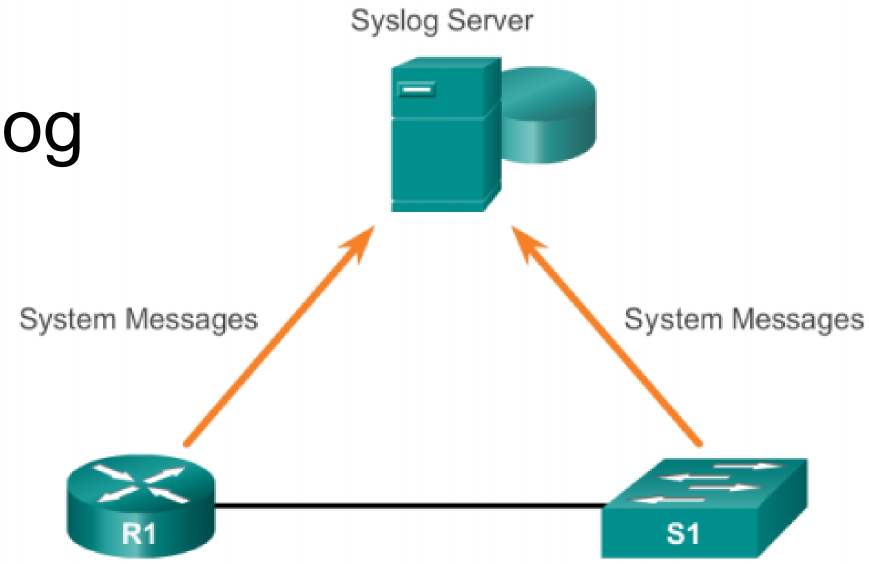
Image from http://www.sdsc.edu/pub/envision/v16.3/caida.html

NTP

- Don’t forget that to make all your data ‘sync’ you need to maintain a common time standard
- Make sure you have a sync’d time server (or use specific external)
  - GPS is an option
- NTP could become yet another vulnerability to your organisation
- Don’t forget to use a common time zone

Syslog

- The commonest form of centralised logging
- UDP port 514
- Simple communication of log data to central repository
- Can collect logging from almost everything
- Don’t forget to actually do something with the logs!



https://upload.wikimedia.org/wikipedia/commons/e/e1/Syslog.png

SIMPLE NETWORK MONITORING PROTOCOL (SNMP)

What is SNMP?

- Simple Network Monitoring Protocol (SNMP)
  - Industry standard v3=3411-8
  - Collecting and organising (modifying) information about managed devices
- Describing three issues:
  - What/how to monitor
  - What information is exchanged
  - How the information is exchanged

SNMP

- Simple protocol (TCP/IP) for monitoring status
  - SNMP manager
    - Responsible for requesting and receiving SNMP data
  - Managed devices
    - Devices run the SNMP service and either respond to requests, or, poll the manager with data
  - Management Information Base (MIB)
    - Categorises the devices and their data

What/how to monitor

- What to monitor – almost any device
  - Network components
  - Servers
  - Printers and other devices (remember vulnerable devices earlier!)
- How to monitor
  - Run a service on the monitored device which
    - Can access status and performance of the device – from CPU/memory levels/temperature even service sensors (e.g. out of paper on a printer)
    - Can communicate with another remote entity – either to transmit 'unsolicited' information or to respond to queries

Typical queries

- Network traffic levels (bytes/flows/errors)
- CPU load (device and hosts)
- Temperature
- Disk space
- Running processes
- Software versions
- Uptime (but can be inferred)

SNMP commands

- GET (query an agent for a value)
- GET-NEXT (next value in a list)
- GET-RESPONSE (returning value to a manager)
- SET (set a parameter/value)
- TRAP (require agent to notify manager when conditions are met)
- Among others…

What SNMP is not

- Intrusive monitoring – but may be possible to use for resource discovery
- Non-intrusive monitoring – no traffic is captured/interpreted

- SNMP was initially designed to observe and control devices, not to monitor traffic or identify attacks

A note on SNMP security

- SNMP v1,v2 – no/poor security
  - Two “communities”, each using a password sent in clear text
  - v2 still the most commonly used
- Situation improved for SNMP v3
  - Encrypted authentication
  - Many devices do not support v3

What information is exchanged

- Each managed device consists of one or more managed objects
  - E.g. managed device – computer; managed objects – CPU, memory, NIC, HDD, etc.
- For each managed object there is a corresponding Management Information Base entry
  - SNMP exchanges information organised in a tree structure – MIB
  - MIB - a database of objects that can be monitored by a network management system

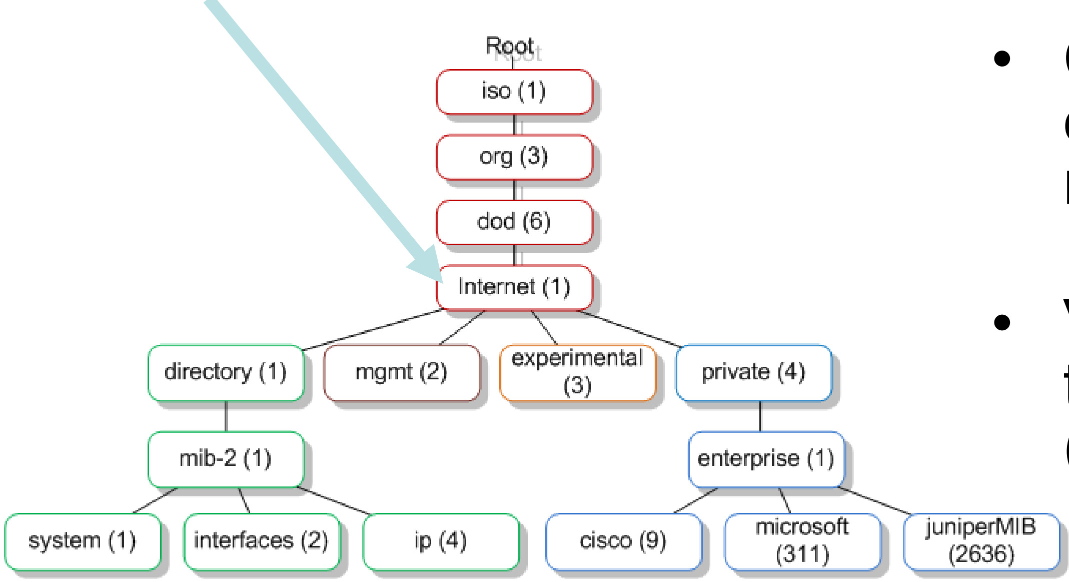
OIDs and MIBs

- An Object IDentifier (OID) is a unique key where a piece of information is stored
- Numerical sequence indicating position in a hierarchical tree

- E.g. Interface statistics
- OID=1.3.6.1.2.1.2.2.1
- The typical MIB used for basic interface statistics
  - Interface status
  - In/out octets
  - Errors
  - Queue length
  - Etc.

MIB tree

Internet = 1.3.6.1



- Tree structure
  - Similar to DNS tree
- Can be used for all environments, not only networking
  - E.g. machinery, telephony
- Vendors may introduce their own branches (objects)
  - Each object includes only relevant attributes
- Provides a standardised description of each object

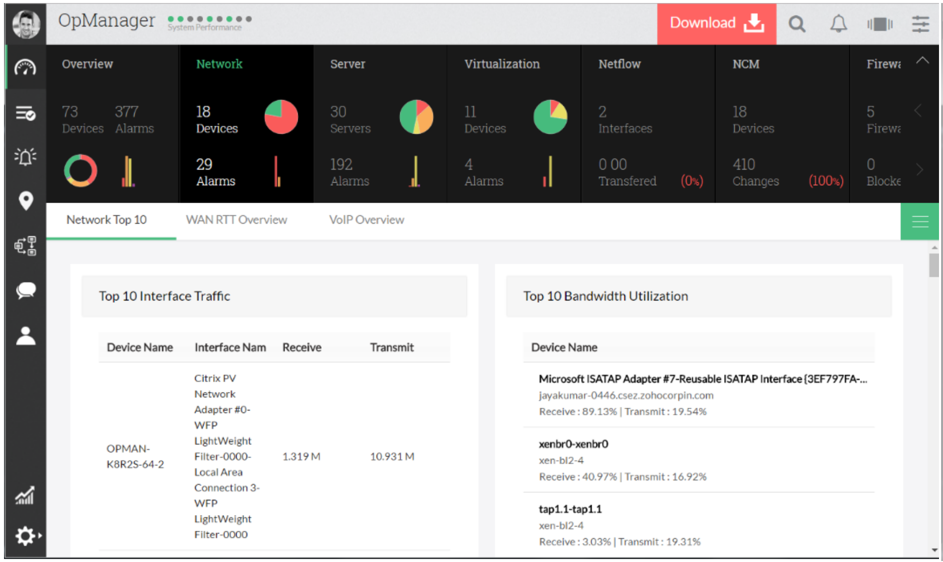
https://commons.wikimedia.org/wiki/File:SNMP_OID_MIB_Tree.png

Messages

- Three types of messages govern SNMP
  - Read – read values from the managed device
  - Write – store values on the managed device
  - Trap – allows managed device to issue (asynchronous) alarms to management station
- SNMP runs on UDP
  - Network friendly, no overheads
  - Port 161 for read/write
  - Port 162 for traps

How to use SNMP

- Plenty of commercial solutions available
  - OpManager from ManageEngine –
    - Demo: http://demo.opmanager.com/DemoLogin.do
  - PRTG - http://www.paessler.com/prtg/
    - Demo: http://prtg.paessler.com

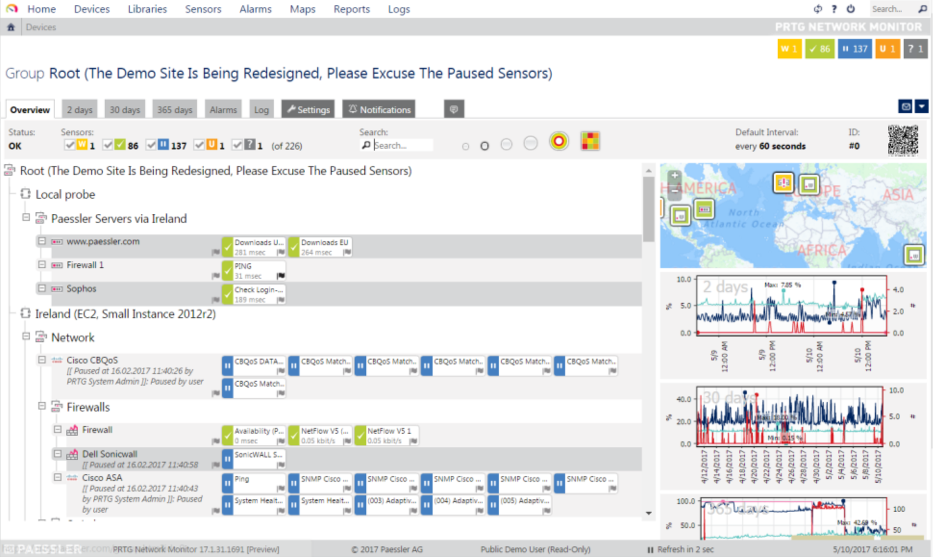


Top 10 Interface Traffic

Device Name	Interface Nam	Receive	Transmit
OPMAN-K8R2S-64-2	Citrix PV Network Adapter #0-WFP LightWeight Filter-0000-Local Area Connection 3-WFP LightWeight Filter-0000	1.319 M	10.931 M

Top 10 Bandwidth Utilization

Device Name
Microsoft ISATAP Adapter #7-Reusable ISATAP Interface {3EF797FA-... jayakumar-0446.csez.zohocorpin.com Receive : 89.13% | Transmit : 19.54%
xenbr0-xenbr0 xen-bl2-4 Receive : 40.97% | Transmit : 16.92%
tap1.1-tap1.1 xen-bl2-4 Receive : 3.03% | Transmit : 19.31%



Group Root (The Demo Site Is Being Redesigned, Please Excuse The Paused Sensors)

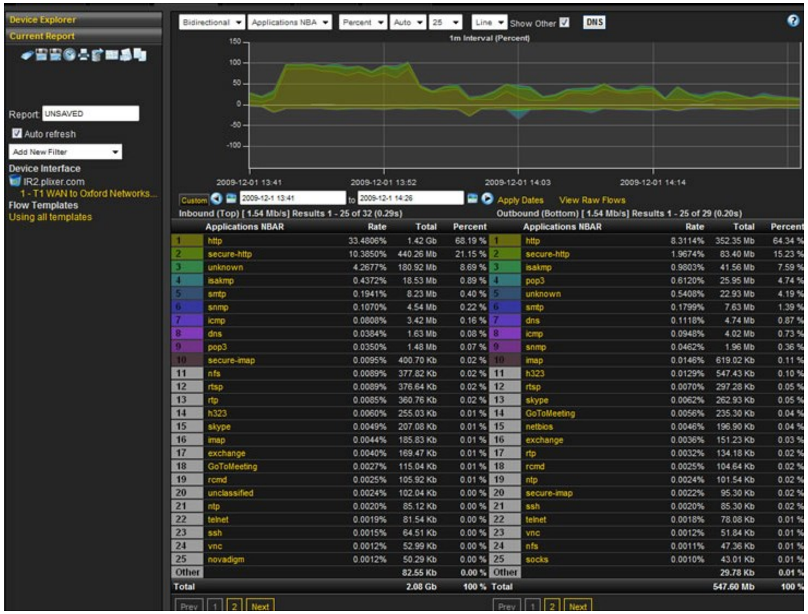
Status: OK
Sensors: W 1 ✓ 86 137 U 1 ? 1 (of 226)
Search: Search...
Default Interval: every 60 seconds
ID: #0

Root (The Demo Site Is Being Redesigned, Please Excuse The Paused Sensors)
- Local probe
  - Paessler Servers via Ireland
    - www.paessler.com — Downloads U... 281 msec; Downloads EU 264 msec
    - Firewall 1 — PING 31 msec
    - Sophos — Check Login-... 189 msec
- Ireland (EC2, Small Instance 2012r2)
  - Network
    - Cisco CBQoS [[Paused at 16.02.2017 11:40:26 by PRTG System Admin]]: Paused by user — CBQoS DATA...; CBQoS Match...; CBQoS Match...; CBQoS Match...; CBQoS Match...; CBQoS Match...; CBQoS Match...
  - Firewalls
    - Firewall — Availability (P... 0 msec; NetFlow V5 (... 0.05 kbit/s; NetFlow V5 1 0.05 kbit/s
    - Dell Sonicwall [[Paused at 16.02.2017 11:40:58 — SonicWALL S...
    - Cisco ASA [[Paused at 16.02.2017 11:40:43 by PRTG System Admin]]: Paused by user — Ping; SNMP Cisco ...; SNMP Cisco ...; SNMP Cisco ...; SNMP Cisco ...; SNMP Cisco ...; System Healt...; System Healt...; (003) Adaptiv...; (004) Adaptiv...; (005) Adaptiv...

PAESSLER PRTG Network Monitor 17.1.31.1691 [Preview] © 2017 Paessler AG Public Demo User (Read-Only) Refresh in 2 sec 5/10/2017 6:16:01 PM

How to use SNMP

- A possible combination for network monitoring: SNMP+RRD=MRTG
  - RRD - Round-Robin Database – maintain time series of data
  - MRTG – Multi Router Traffic Grapher
  - Rapid installation
  - http://oss.oetiker.ch/mrtg/



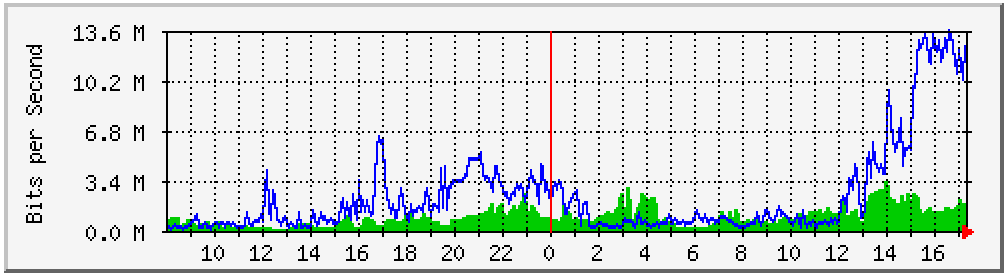
2009-12-1 13:41 to 2009-12-1 14:26

Inbound (Top) [1.54 Mb/s] Results 1 - 25 of 32 (0.29s)

	Applications NBAR	Rate	Total	Percent
1	http	33.4806%	1.42 Gb	68.19 %
2	secure-http	10.3850%	440.26 Mb	21.15 %
3	unknown	4.2677%	180.92 Mb	8.69 %
4	isakmp	0.4372%	18.53 Mb	0.89 %
5	smtp	0.1941%	8.23 Mb	0.40 %
6	snmp	0.1070%	4.54 Mb	0.22 %
7	icmp	0.0808%	3.42 Mb	0.16 %
8	dns	0.0384%	1.63 Mb	0.08 %
9	pop3	0.0350%	1.48 Mb	0.07 %
10	secure-imap	0.0095%	400.70 Kb	0.02 %
11	nfs	0.0089%	377.82 Kb	0.02 %
12	rtsp	0.0089%	376.64 Kb	0.02 %
13	rtp	0.0085%	360.76 Kb	0.02 %
14	h323	0.0060%	255.03 Kb	0.01 %
15	skype	0.0049%	207.08 Kb	0.01 %
16	imap	0.0044%	185.83 Kb	0.01 %
17	exchange	0.0040%	169.47 Kb	0.01 %
18	GoToMeeting	0.0027%	115.04 Kb	0.01 %
19	rcmd	0.0025%	105.92 Kb	0.01 %
20	unclassified	0.0024%	102.04 Kb	0.00 %
21	ntp	0.0020%	85.12 Kb	0.00 %
22	telnet	0.0019%	81.54 Kb	0.00 %
23	ssh	0.0015%	64.51 Kb	0.00 %
24	vnc	0.0012%	52.99 Kb	0.00 %
25	novadigm	0.0012%	50.29 Kb	0.00 %
Other			82.55 Kb	0.00 %
Total			2.08 Gb	100 %

Outbound (Bottom) [1.54 Mb/s] Results 1 - 25 of 29 (0.20s)

	Applications NBAR	Rate	Total	Percent
1	http	8.3114%	352.35 Mb	64.34 %
2	secure-http	1.9674%	83.40 Mb	15.23 %
3	isakmp	0.9803%	41.56 Mb	7.59 %
4	pop3	0.6120%	25.95 Mb	4.74 %
5	unknown	0.5408%	22.93 Mb	4.19 %
6	smtp	0.1799%	7.63 Mb	1.39 %
7	dns	0.1118%	4.74 Mb	0.87 %
8	icmp	0.0948%	4.02 Mb	0.73 %
9	snmp	0.0462%	1.96 Mb	0.36 %
10	imap	0.0146%	619.02 Kb	0.11 %
11	h323	0.0129%	547.43 Kb	0.10 %
12	rtsp	0.0070%	297.28 Kb	0.05 %
13	skype	0.0062%	262.93 Kb	0.05 %
14	GoToMeeting	0.0056%	235.30 Kb	0.04 %
15	netbios	0.0046%	196.90 Kb	0.04 %
16	exchange	0.0036%	151.23 Kb	0.03 %
17	rtp	0.0032%	134.18 Kb	0.02 %
18	rcmd	0.0025%	104.64 Kb	0.02 %
19	ntp	0.0024%	101.54 Kb	0.02 %
20	secure-imap	0.0022%	95.30 Kb	0.02 %
21	ssh	0.0020%	85.30 Kb	0.02 %
22	telnet	0.0018%	78.08 Kb	0.01 %
23	vnc	0.0012%	51.84 Kb	0.01 %
24	nfs	0.0011%	47.36 Kb	0.01 %
25	socks	0.0010%	43.01 Kb	0.01 %
Other			29.78 Kb	0.01 %
Total			547.60 Mb	100 %



SNMP+RRD

- SNMP becomes large over time, making data retrieval inefficient
  - Larger files, more data to parse
- Alternative – round robin database
  - Establish a relevant time period (e.g. 1 year)
  - Remove data beyond time period
  - Aggregate older data so it occupies less time
    - 5 minute samples for past 24 hours
    - 1 hours samples for past week
    - 6 hours samples for past month
    - 1 day samples for past year
- Result: constant size for database
- MRTG also includes support for displaying the results

(more) SNMP reporting systems

- Observium
  - http://www.observium.org
  - http://demo.observium.org (demo/demo)
- Cacti
  - http://www.cacti.net/
- Nagios
  - http://sysnetmon.diglinks.com/nagios/ (guest/guest)
- Argus
  - http://argus.tcp4me.com/demo.html

NETFLOW

NETFLOW

- A flow is a set of related packets
- Flow level data can be captured and stored for analysis
  - Netflow (Cisco)
  - jFlow (Juniper)
  - sFlow (industry standard – but sampled)

Purpose

- A flow is expired/exported/stored when the TCP connection finishes, or when preset timers expire
- Information can be parsed to derive
  - Live patterns
  - Anomalies and incidents
- Need to think about where to capture flow data
- DOES NOT record content

Netflow

- Storing flow-data allows for off-line analysis
  - Observing trends and identifying past events
  - Running back through incidents
  - Reverse-tracing attack sequence
  - Rerun of the analysis from a different perspective

What is a flow?

- A TCP connection is formed of two flows, corresponding to the two directions
  - Source/destination IP address
  - Source/destination port for UDP or TCP (type/code for ICMP, 0 for others)
  - IP protocol number
  - Ingress interface (not all devices can distinguish directionality)
  - IP Type of Service (ToS)
  - *NB some tools combine bidirectional flow traffic*

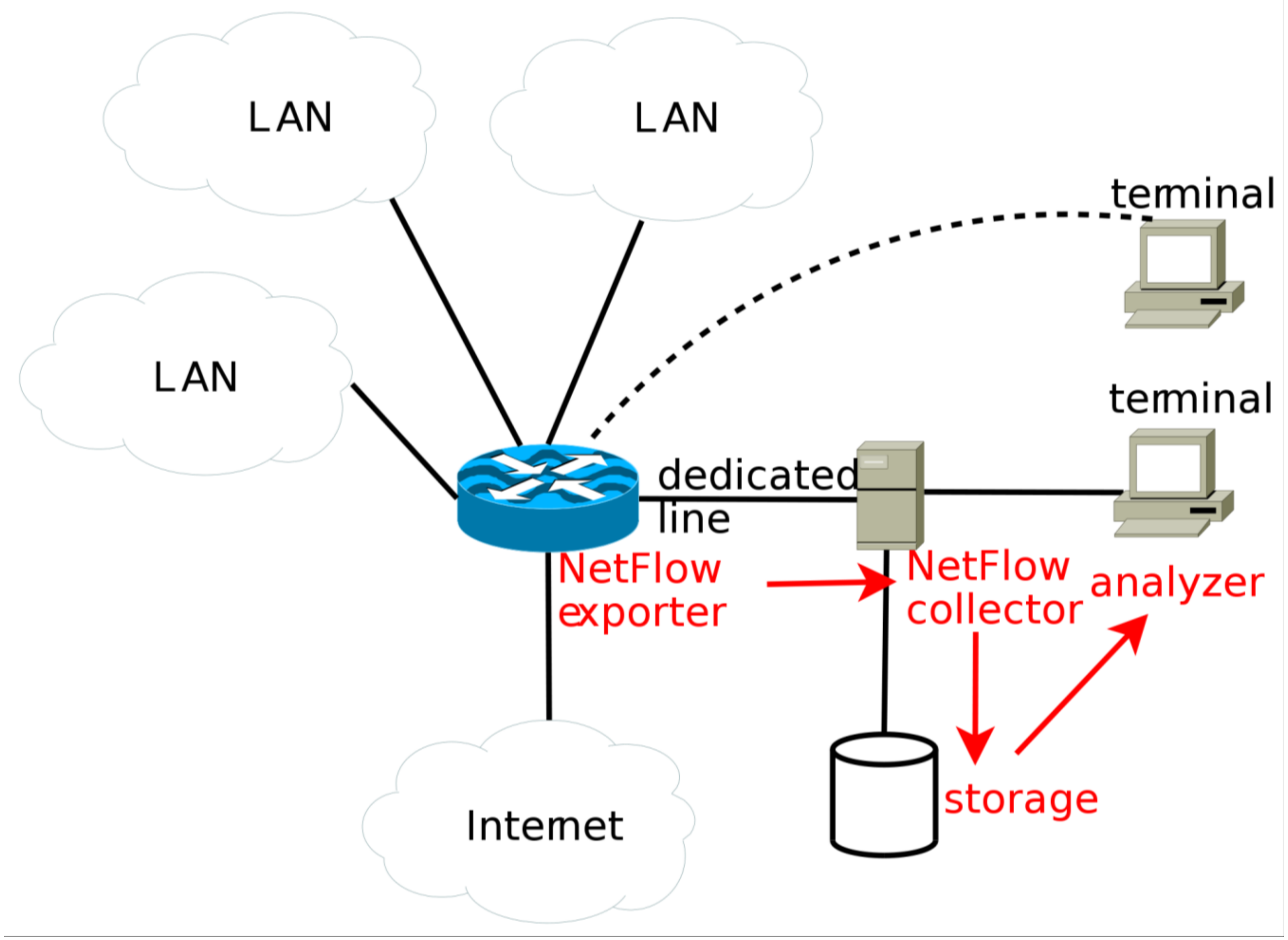
Netflow versions

- v5 – flow/packet/byte accounting
  - BUT does not support IPv6
- v9 – fully flexible, allowing extensions
  - RFC3954
- v10 – the future?
  - RFC5102
- v5 still the most common

Netflow implementation

- Configure device for flow generation
  - – Router (e.g. Cisco) - efficient
  - – dedicated computer (on span/mirror port)
    - Running flow software (e.g. softflowd, pfflowd, ng_netflow)
- Export flows to a collector
- Collector receives/processes flows
- Management terminal analyses/reports

Example architecture



https://commons.wikimedia.org/wiki/File:Netflow_architecture_en.svg

Example flows

```
Date flow start          Duration Proto     Src IP Addr:Port          Dst IP Addr:Port    Packets    Bytes Flows
2016-02-09 23:53:59.749     0.000 UDP     248.38.135.219:53     ->  248.38.135.178:55163        1      202     1
2016-02-09 23:53:59.126     0.000 UDP     248.38.135.219:53     ->  248.38.135.61:63824         1      176     1
2016-02-09 23:53:59.770     0.108 TCP     151.37.198.236:80     ->  248.38.135.146:52877        3      140     1
2016-02-09 23:53:59.733     0.059 TCP     248.38.135.146:52877 ->  151.37.198.236:80           3      436     1
2016-02-09 23:53:59.036     0.000 UDP     248.38.135.219:53     ->  248.38.135.61:59035         1      250     1
2016-02-09 23:47:19.988   399.308 ICMP    141.171.183.121:3     ->  248.38.135.209:0.1         13     1058     1
2016-02-09 23:47:49.394   369.999 UDP     248.38.135.79:34484   ->  141.33.72.159:50162         6      348     1
2016-02-09 23:53:59.110     0.077 TCP     151.37.51.104:80      ->  248.38.135.146:49520        3      140     1
2016-02-09 23:53:59.049     0.146 TCP     248.38.135.47:51595   ->  149.45.3.154:80             6     1268     1
```

ROLL-YOUR-OWN

tcpdump

- Well known tool for traffic capture and analysis
  - Extensive packet filtering options
  - Output to text (various forms) and binary content
  - Can do basic processing of traffic
  - High performance (depending on load)
- Not as convenient
  - Large traffic volumes
  - Complex filter/capture options
  - Usually requires post-processing of captured traffic
- http://www.tcpdump.org/tcpdump_man.html

tcpdump output

```
16:03:50.611202 IP (tos 0x0, ttl  60, id 62110, offset
0, flags [none], proto: TCP (6), length: 1362)
192.171.163.3.80 > 70.240.240.174.17410: .
950409921:950411243(1322) ack 4148432645 win 16352
```

```
Timestamp IP (tos tos, ttl ttl, id id, offset offset,
flags [flags], proto proto (ID), length: length)
srcIP.srcport > dstIP.dstport: . startseq:endseq
(datalength) ack ackno win win
```

Timestamp – timestamp of packet capture

tos – type of service value

ttl – time to live value

id - identification number of datagram

offset – offset of datagram in the stream

flags – fragmentation flags

proto / ID – transport protocol type/value

tcpdump alternatives

- windump – windows port
- tshark – text-based version of wireshark

- Plus visual tools
  - Wireshark
  - Take a look at Kali and other 'hacker' platforms

INCIDENT DETECTION

Definitions

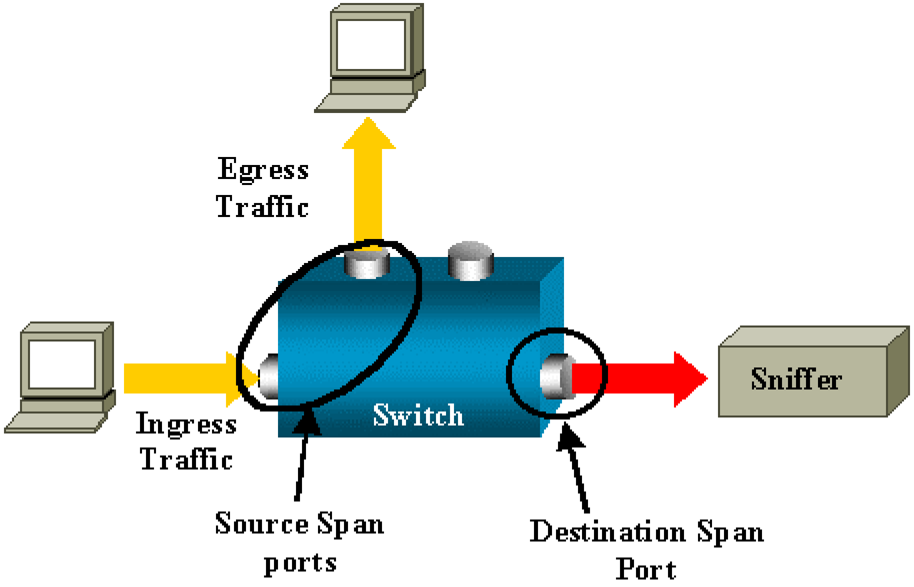
- Intrusion: any attempt (successful or not) to access your infrastructure (devices, hosts, services etc.)
- Intrusion Detection: the mechanism of detecting an intrusion!
- IDS: (Intrusion Detection System) any system that implements the above
- IPS: (Intrusion Prevention System) any system that extends the IDS to actively prevent the attempted intrusion

IDS

- Plenty of commercial offerings
- Most common underlying system is snort
  - Open source IDS
  - Can operate at Gbps speeds
  - Only runs single core, but can have multiple threads (combine multiple instances to achieve high speeds)
  - Can log to database (typically MySQL)
  - Many GUI front-end options
  - Has to be at aggregation point (or distributed)
    - Span/mirror, not in-line

Span/Mirror ports

- Most switches support either span or mirror ports
- Usually have to be specially configured



http://www.cisco.com/c/dam/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41d.gif

Snort rules

- Once implemented, the key element are the snort rules
  - Free (30 day delay)
  - Some community rules
  - Commercial (no delay)
- Rules need to be downloaded
  - Some devices can automate this
  - Or use external tools
  - You need an oinkcode!

https://commons.wikimedia.org/wiki/File:Snort_ids_logo.png

Alerts

- All detection systems will generate some level of false alarms (both positive and negative)
- Up to date rules help, but they need to be applied in the organizational context
- BUT, badly implemented rules can be worse
- Some level of filtering of alerts is needed
  - Do you want to know all 1000 of the port scan alerts from a single external IP?

Resources

- Snort website (including rules downloads)
- Pulled pork (rules updater)
- Emerging threats (community) rules
- SnoGE (Snort unified reporting tool)
- BASE (Basic Analysis and Security Engine)
- And lots more!

INCIDENT RESPONSE/INVESTIGATION

How to Respond: The Incident Respond Process

- Steps
  - Preparation
  - Notification
  - Response
  - Countermeasures
  - Recovery
  - Follow-Up

- Acquire
  - Capture evidence, establish chain or custody, verify evidence
- Analyse
  - Document, repeatable/explainable, independence
- Attest
  - Report findings, evidence-based

Step 1: Preparation

- Plan your response strategy in advance (not while you are under attack
- Response should be planned through risk analysis/assessment and documented as part of your security policy
- Make sure everyone know where the policies and operating procedures can be found

Step 1: Preparation (continued)

- Monitoring service need to be in place (in advance)
- May need dedicated resources, teams, or, even facilities
- A good approach will be proactive and help to minimise risks
- Part of preparedness is testing
  - Internal vs external testing

Step 2: Notification

- How will you receive notifications?
- Who will receive them?
- Contingencies for leave etc.
- This will need more than just someone viewing snort logs – use the tools that are out there
- Is the incident reportable externally?
  - Shareholders
  - Clients/suppliers etc.
  - Banks
  - Police/government

Step 3: Response

- Don’t panic
- Follow the principles established in step 1 (preparing a plan)
- Start to establish impact (refer to risk)
- Think about who needs to be notified
- Be careful not to over-react (or ignore seemingly minor threats)
- What if the system under attack is your main communications method?

Step 4: Countermeasures

- Be prepared to implement countermeasures:
  - Isolating systems, services, subnets, sites etc.
    - Physical/virtual isolation may be preferable to power interruption
  - Think about impact on dependent services
  - What about evidence
    - Legal?
    - Further investigation (i.e. to learn from the incident)
  - Once again, planning

Step 5: Recovery

- Restore services where safe and practical
  - Careful you don’t restore from a modified backup!
- Monitor once recovered
- Make sure it doesn’t happen again
  - In the short term block services, protocols, IPs etc.
  - In the long term, develop/refine signatures to better detect
  - May need to work with others outside of the organisation

Step 6: Follow-Up

- Document everything
- Follow-up with stakeholders to fully evaluate damage/impact
- Lessons can usually be learnt
  - Improve the investigative process
  - Better protect the infrastructure
  - Quicker detection and prevention
  - Review policies

Preparing evidence

- Oversight (don’t work alone)
  - Write everything down
  - Secure the evidence
  - Maintain a chain of custody
  - If you don’t know how to handle potential evidence, you should not be doing it!

Security Monitoring and Investigation

Paul Haskell-Dowland

School of Science
Edith Cowan University