NETWORK MANAGEMENT
AND MONITORING

Developed by: Alberto Escudero Pascual, IT +46
Goals

• We need to know what we want, to be able to know what we need

• Are Monitoring and Network Management the same thing?

• Do not follow tools, follow methods!
Table of Contents

• Methodology of this unit
• Goals versus Data Monitoring
• Monitoring Service Goals
• Technical Principles
  – SNMP/MIB
  – Traffic Accounting
  – Traffic Shaping
  – Bayesian filters
  – Virus Fingerprints
• Tools (MRTG, Ntop, SpamAssassin, Clam AV)
Methodology

• Focus on goals, not tools
• Understand the technical principles behind the tools
• Understand which technical principles we need to achieve our goals
Goals versus Data monitoring
Monitoring Service Goals

Three examples:

- Save cost by reducing International bandwidth use
- Provide better QoS for VoIP
- Manage Service and Network growth
Goal 1: Save costs in International Bandwidth

<table>
<thead>
<tr>
<th>Layer</th>
<th>Technical principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Caching, Detect/Block Spam/Viruses (Bayesian Filters)</td>
</tr>
</tbody>
</table>
| 3     | Traffic shaping (Queueing Principles)  
         | Traffic accounting (SNMP, Promisc) |
| 2     | Network Access Control (Firewalling)  
         | Traffic shaping  
         | Traffic accounting (SNMP, Promisc) |
| 1     | Wireless Access Control  
         | Collect Wireless Layer-2 Data (SNMP) |
## Goal 2: QoS for VoIP

<table>
<thead>
<tr>
<th>Layer</th>
<th>Technical principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Traffic shaping (Queueing Principles)  &lt;br&gt; Traffic accounting (SNMP, Promisc)</td>
</tr>
<tr>
<td>2</td>
<td>Traffic shaping (Queueing Principles)  &lt;br&gt; Traffic accounting (SNMP, Promisc)</td>
</tr>
<tr>
<td>1</td>
<td>Collect Layer-2 Data (SNMP)  &lt;br&gt; Reduce wireless latency</td>
</tr>
</tbody>
</table>
Goal 3: Managing service and Network Growth

<table>
<thead>
<tr>
<th>Layer</th>
<th>Technical principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Virus/Spam, SQL (<em>Service Balancing</em>)</td>
</tr>
<tr>
<td>3</td>
<td>Collect TCP/UDP Statistics, Firewall Balancing</td>
</tr>
<tr>
<td>2</td>
<td>Collect IP Layer Statistics, <em>Routing principles</em></td>
</tr>
<tr>
<td>1</td>
<td>Collect Layer-2 Data (SNMP)</td>
</tr>
</tbody>
</table>
Technical Principles

Five technical principles:

- SNMP/MIB
- Traffic Accounting
- Traffic Shaping
- Bayesian Filters
- Virus fingerprints
SNMP/MIB

• Operation and maintenance protocol for network computer networks and network devices
• Server/client architecture
• Client queries remote network devices
  – Statistical information, private data
• SNMP-enabled device contains a statistical information database (MIB)

Interoperability and ability to be extended

Complex encoding rules, inefficient coding
SNMP/MIB

• SNMP is also “traffic” in your network
  – Minimize overhead by asking smart queries
• SNMPv1 does not provide encrypted authentication
  – Mind your passwords
• SNMP consumes CPU
SNMP/MIB

- Wireless vendors implement *proprietary sets* of wireless information in MIBs
- The mechanism to retrieve certain kind of wireless data varies
- Wireless devices are equipment with own “Management tools”
- Integration of different management tools is normally complicated as the code seldom is open source
- Write your own wireless management system!
Traffic Accounting

General principal for monitoring traffic statistics:

- Network decisions
- Troubleshooting
- Monitoring host activities
Traffic Accounting

- Packet and byte counts
- Protocol distribution statistics
- IP checksum errors
- Discovery of active hosts
- Data activity among hosts
Traffic Accounting

- **Active**
  - Enable SNMP in all routers/bridges of the network

- **Passive**
  - Promiscuous mode
  - Requires direct access to channel and CPU to gather and digest information
Traffic Shaping

• Control traffic flow
• Guarantee certain performance
• Queueing disciplines in IP layer
  – Latency and congestion
  – Bandwidth and fairness
Traffic Shaping

- Modification of IEEE 802.11 MAC layer in IEEE 802.11-based products to implement similar behaviour using proprietary mechanisms that does not ensure interoperability
- Proxim has implemented a proprietary polling mechanism (WORP) to allocate network capacity by using time slots
Queuing disciplines and latency

- Applied on outgoing traffic
  - Outgoing is normally bottleneck

- Buffet overflow
  - Dropping TCP packets -> Retransmission
  - Latency

- Prioritization of packets
  - User interaction (ssh, rtp)
  - Bulk traffic (ftp, http)
Bandwidth management
by packet queuing

Can ensure:

- QoS
  - A certain bitrate to a specific host
  - Limited throughput for a specific service
- Fair network
  - Customer gets what he/she paid for
Bandwidth management by packet queuing

- Classful queuing disciplines
  - Hierarchical structure
  - Class specifies queueing algorithm, bitrate, ceiling limit (depending on protocol, IP, subnet)
- HTB (classful)
  - Controlling bandwidth by simulating slow links
- SFQ (classless)
  - Fairness with saturated link
Bayesian Filters

• Content based anti-spam filter
  – Header (sender and message paths)
  – Embedded HTML code
  – Word pairs and phrases
  – Meta information

• Adaptive – self learning by error reports

• No manual wordlist
  – Initial list created by analysing content
Bayesian Filters

- Place your anti-spam filter before the mails enter your wireless infrastructure
- Placing mail rely agent with anti-spam filters on the other side of you international link can save 10-20% of your international bandwidth costs
Virus Fingerprints (signatures)

• Fingerprints: Computer instructions or derivatives of them used by known viruses

• Antivirus programs
  – Uses virus fingerprints to scan code
  – Online constantly updated databases

• Heuristic scanning algorithms
  – Creates permutations of known viruses to predict future mutated viruses
Monitoring Tools

Free and open source tools:

- MRTG
- Ntop
- SpamAssassin
- Clam Antivirus (Clam AV)
Monitoring the wireless

- Vendor specific monitoring tools (for certain operating system)
  - Brings limited usage
- N vendors implies n network monitoring tools
- Single interface by integration (SNMP/MIB -> MRTG)
MRTG

• Multi Router Traffic grapher
• Monitor and display network parameters (CPU, traffic load)
• Uses data from SNMP-enables devices
• Graphical web based interface
MRTG

Configuration of MRTG:

• Pre-requisites: web server, MRTG installed, IP address and SNMP password of device you want to monitor

• Create configuration file for MRTG *(cfgmaker)*

• Create a “cron” process that runs MRTG
MRTG: Bandwidth monitoring

1. Create default config file for mrtg

   > cfgmaker password@IP  > /etc/mrtg_b.cfg

2. Change working directory of MRTG in mrtg_b.cfg

   WorkDir: /var/www/mrtg

3. Create periodic task by adding the following line in /etc/crontab

   */5 *** * * * root /usr/bin/mrtg /etc/mrtg_b.cfg
MRTG: SN/R monitoring

- Need data from MIB of wireless device
- How to find the right queries (OID)?
  - Reverse engineering!
- Use proprietary network manager to monitor traffic (link-test)
MRTG: SN/R monitoring

19:41:21.448323 10.10.10.12.1260 > 10.10.10.254.snmp: GetRequest(29) .1.3.6.1.4.1.762.2.1.7.0
0x0000 4500 0048 77b2 0000 8011 99d5 0a0a 0a0c E..Hw.........
0x0010 0a0a 0afe 04ec 00a1 0034 64bb 302a 0201 ..........4d.0*..
0x0020 0004 0670 7562 6c69 63a0 1d02 0201 0302 ...public......
0x0030 0100 0201 0030 1130 0f06 0b2b 0601 0401 .....0.0...+....
0x0040 857a 0201 0700 0500 .z......

19:41:21.448854 10.10.10.254.snmp > 10.10.10.12.1260: GetResponse(30) .1.3.6.1.4.1.762.2.1.7.0=2 (DF)
0x0000 4500 0049 0037 4000 4011 1150 0a0a 0afe E..l.7@.@..P....
0x0010 0a0a 0a0c 00a1 04ec 0035 62b5 302b 0201 ..........5b.0+..
0x0020 0004 0670 7562 6c69 63a2 1e02 0201 0302 ...public......
0x0030 0100 0201 0030 1230 1006 0b2b 0601 0401 .....0.0...+....
Connected users to AP

Write Integer 50 in OIDs:
1.3.6.1.4.1.762.2.5.5.1,
1.3.6.1.4.1.762.2.5.5.1,
1.3.6.1.4.1.762.2.5.5.3

Write Integer 3 in OIDs:
1.3.6.1.4.1.762.2.5.4.1,
1.3.6.1.4.1.762.2.5.4.2,
1.3.6.1.4.1.762.2.5.4.3

Retrieve the OID:
1.3.6.1.4.1.762.2.5.1.0
Signal & noise parameters

Write Integer 1500, 25, 80 in OID
1.3.6.1.4.1.762.2.5.2.1.27.n
1.3.6.1.4.1.762.2.5.2.1.26.n
1.3.6.1.4.1.762.2.5.2.1.25.n

Retrieve signal by reading:
1.3.6.1.4.1.762.2.5.2.1.32.n

Retrieve noise by reading:
1.3.6.1.4.1.762.2.5.2.1.33.n

where <n> refers to the integer assigned to the wireless device
Wireless with MRTG

*MRTG – IP information (Layer 3) and wireless information (Layer 2)*
Ntop

Free and open source (GPL)

• Traffic measurement
• Traffic characterization and monitoring
• Detection of network security violations
• Network optimization and planning
Traffic measurement

- Sent and received data per protocol
- IP multicast
- TCP session history
- TCP/UDP services used and traffic distribution
- Bandwidth utility (actual, average, peak)
- Traffic distributions (among subnets)
Traffic characterization and monitoring

Identifying situations where network rules and thresholds are not followed by detecting:

- Duplicated use of IP addresses
- NICs in promiscuous mode
- Misconfigurations in software
- Service misuse (proxy servers etc.)
- Excessible bandwidth utilization
Detection of network security violations

Detection of network attacks such as:

- Portscan
- Spoofing
- Spyes
- Trojan horses
- Denial of Service (DoS)
Network and optimization and planning

Identify suboptimal configurations and non-efficient utilization of available bandwidth

- Unnecessary protocols
- Suboptimal routing (ICMP redirect)
- Traffic patterns and distribution
Ntop
SpamAssassin

• Don't block, just tag!
• Gives each message a score based on:
  • Header and body phrases
  • Bayesian filter
  • Whitelists/blacklists
  • Collaborative spam identification databases
  • DNS blocklists
  • Character sets and locales
Clam Antivirus

- Does not delete or clean infected file, just tags it
- Fast scanning of directories and file
- Detection of over 30 000 viruses, worms and trojan horses
- Scans archives and compressed files
- Contains advanced database updater with support for virus signatures
Flooding the network

18:12:36.432838 172.168.0.36.2231 > 172.168.82.53.445: S 1068540375:1068540375(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000 4500 0030 119f 4000 8006 3d7f aca8 0024 E..0.@...=.....$
0x0010 aca8 5235 08b7 01bd 3fb0 a1d7 0000 0000 ..R5....?......
0x0020 7002 faf0 i088 0000 0204 05b4 0101 0402 p............

18:12:36.441460 172.168.82.53.445 > 172.168.227.122.445: S 2018273998:2018273998(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000 4500 0030 8a9c 4000 8006 3349 aca8 0017 E..0..@...3I....
0x0010 aca8 e37a 0599 01bd 784c 6ace 0000 0000 ...z....xLj.....
0x0020 7002 faf0 60db 0000 0204 05b4 0101 0402 p... ..........
Conclusions

- Monitoring raw data will not help
- You need to monitor to have a good network management
- Set your goals, find the technical principles and then choose your tools
- If a tool does NOT do what you want or does far more of what you need, consider building one.