Traffic Monitoring and Flow Analysis
For IP Networks
Overview

• Introduction SNMP
• Introduction to MRTG and RRD-Tool
• Introduction to Traffic flows
Introduction to SNMP
What is SNMP?

SNMP – Simple Network Management Protocol
   – Industry standard, hundreds of tools exist to exploit it
   – Present on any decent network equipment

Query – response based: **GET / SET**
   – GET is mostly used for monitoring

Tree hierarchy
   – Query for "Object Identifiers" (OIDs)

Concept of MIBs (Management Information Base)
   – Standard and vendor-specific (Enterprise)
What is SNMP?

UDP protocol, port 161

Different versions

  - Original specification
- v2 – RFC1901 ... RFC1908 + RFC2578
  - Extends v1, new data types, better retrieval methods (GETBULK)
  - Used is version v2c (without security model)
- v3 – RFC3411 ... RFC3418 (w/security)

Typically we use SNMPv2 (v2c)
What is SNMP?

Terminology:

– Manager (the monitoring "client")
– Agent (running on the equipment/server)
What is SNMP?

Typical queries
- Bytes In/Out on an interface, errors
- CPU load
- Uptime
- Temperature or other vendor specific OIDs

For hosts (servers or workstations)
- Disk space
- Installed software
- Running processes
- ...

Windows and UNIX have SNMP agents
How does it work?

Basic commands

- **GET** (manager -> agent)
  - Query for a value

- **GET-NEXT** (manager -> agent)
  - Get next value (list of values for a table)

- **GET-RESPONSE** (agent -> manager)
  - Response to GET/SET, or error

- **SET** (manager -> agent)
  - Set a value, or perform action

- **TRAP** (agent -> manager)
  - Spontaneous notification from equipment (line down, temperature above threshold, ...)

The MIB Tree

- root
  - ccitt(0)
  - iso(1)
    - org(3)
    - dod(6)
      - internet(1)
        - directory(1)
        - mgmt(2)
        - experimental(3)
  - joint-iso-ccitt(3)
  - 1.3.6.1

- private(4)
  - enterprises(1)
    - cisco(9)

- ciscoMgmt(9)
  - ciscoEnvMonMIB(13)
  - ciscoEnvMonObjects(1)
    - ciscoEnvMonTemperatureStatusTable(3)
    - ciscoEnvMonTemperatureStatusEntry(1)
    - ciscoEnvMonTemperatureStatusValue(3)
  ...

- mib-2(1)
  - system(1)
  - snmp(11)
    - interfaces(2)
    - ip(4)
The Internet MIB

- **directory** (1)  OSI directory
- **mgmt** (2)  RFC standard objects
- **experimental** (3)  Internet experiments
- **private** (4)  Vendor-specific
- **security** (5)  Security
- **snmpV2** (6)  SNMP internal
OIDs and MIBs

• Navigate tree downwards
• OIDs separated by '.'
  – 1.3.6.1.4.1.9. ...
• OID corresponds to a label
  – .1.3.6.1.2.1.1.5 => sysName
• The complete path:
  – .iso.org.dod.internet.mgmt.mib-2.system.sysName
• How do we convert from OIDs to Labels (and vice versa ?)
  – Use of MIBs files!
MIBs

- MIBs are files defining the objects that can be queried, including:
  - Object name
  - Object description
  - Data type (integer, text, list)
- MIBS are structured text, using ASN.1
- Standard MIBs include:
  - MIB-II – (RFC1213) – a group of sub-MIBs
  - HOST-RESOURCES-MIB (RFC2790)
MIBs - 2

• MIBs also make it possible to interpret a returned value from an agent
  – For example, the status for a fan could be 1,2,3,4,5,6 – what does it mean?
sysUpTime OBJECT-TYPE
SYNTAX TimeTicks
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."
::= { system 3 }

sysUpTime OBJECT-TYPE
This defines the object called sysUpTime.

SYNTAX TimeTicks
This object is of the type TimeTicks. Object types are specified in the SMI we mentioned a moment ago.

ACCESS read-only
This object can only be read via SNMP (i.e., get-request); it cannot be changed (i.e., set-request).

STATUS mandatory
This object must be implemented in any SNMP agent.

DESCRIPTION
A description of the object

::= { system 3 }
The sysUpTime object is the third branch off of the system object group tree.
CiscoEnvMonState ::= TEXTUAL-CONVENTION
  STATUS  current
  DESCRIPTION
  "Represents the state of a device being monitored. Valid values are:
  
  normal(1): the environment is good, such as low temperature.
  warning(2): the environment is bad, such as temperature above normal operation range but not too high.
  critical(3): the environment is very bad, such as temperature much higher than normal operation limit.
  shutdown(4): the environment is the worst, the system should be shutdown immediately.
  notPresent(5): the environmental monitor is not present, such as temperature sensors do not exist.
  notFunctioning(6): the environmental monitor does not function properly, such as a temperature sensor generates a abnormal data like 1000 C.
  "
Querying SNMP agent

Some typical commands for querying:

- `snmpget`
- `snmpwalk`
- `snmpstatus`

Syntax:

```
snmpXXX -c community -v1 host [oid]
snmpXXX -c community -v2c host [oid]
```
Querying SNMP agent

Let's take an example

```bash
-snmpstatus -c s3cr3t -v1
169.223.142.1

-snmpget -c s3cr3t -v1
169.223.142.10
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0

-snmpwalk -c s3cr3t -v1
169.223.142.20 ifDescr
```
Querying SNMP agent

• **Community:**
  – A "security" string (password) to define whether the querying manager will have RO (read only) or RW (read write) access
  – This is the simplest form of authentication in SNMP

• **OID**
  – A value, for example, `.1.3.6.1.2.1.1.5.0`, or it's name equivalent
  – `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0`

• Let's ask for the system's name (using the OID above)
  – Why the `.0`? What do you notice?
References

- *Essential SNMP* (O’Reilly Books) Douglas Mauro, Kevin Schmi
- *Basic SNMP at Cisco*
- Wikipedia:
- IP Monitor MIB Browser
  http://support.ipmonitor.com/mibs_byoidtree.aspx
- Open Source Java MIB Browser
  http://www.kill-9.org/mbrowse
  http://www.dwipal.com/mibbrowser.htm (Java)
- SNMP Link – collection of SNMP resources
  http://www.snmplink.org/
- Net-SNMP Open Source SNMP tools
  http://net-snmp.sourceforge.net/
- Integration with Nagios http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html
Optional Materials

SNMP Version 3
SNMP and Security

• SNMP versions 1 and 2c are insecure
• SNMP version 3 created to fix this

• Components
  – Dispatcher
  – Message processing subsystem
  – Security subsystem
  – Access control subsystem
SNMP version 3 (SNMPv3)

The most common module is based in user, or a “User-based Security Model”

- **Authenticity and integrity:** Keys are used for users and messages have digital signatures generated with a hash function (MD5 or SHA)

- **Privacy:** Messages can be encrypted with secret-key (private) algorithms (DES)

- **Temporary validity:** Utilizes a synchronized clock with a 150 second window with sequence checking.
Security Levels

- **noAuthPriv**
  - No authentication, no privacy

- **authNoPriv**
  - Authentication with no privacy

- **authPriv**
  - Authentication with privacy
Cisco SNMPv3 configuration

snmp-server view vista-ro internet included
snmp-server group ReadGroup v3 auth read vista-ro
snmp-server user admin ReadGroup v3 auth md5 xk122r56

Or alternatively:

snmp-server user admin ReadGroup v3 auth md5 xk122r56
    priv des56 D4sd#rr56
Net-SNMP SNMPv3 configuration

# apt-get install snmp snmpd
# net-snmp-config --create-snmpv3-user -a "xk122r56" admin /usr/sbin/snmpd
# snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A "xk122r56" 127.0.0.1
Introduction to MRTG
MRTG: Multi Router Traffic Grapher

• MRTG is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing PNG images which provide an almost live visual representation of this traffic. You can find MRTG at http://oss.oetiker.ch/mrtg/.

• MRTG has been the most common network traffic measurement tool for all Service Providers.

• MRTG uses simple SNMP queries on a regular interval to generate graphs.
MRTG

- External readers for MRTG graphs can create other interpretation of data.
- MRTG software can be used not only to measure network traffic on interfaces, but also build graphs of anything that has an equivalent SNMP MIB - like CPU load, Disk availability, temperature, etc...
- Data sources can be anything that provides a counter or gauge value – not necessarily SNMP.
- For example, graphing round trip times
- MRTG can be extended to work with RRDTool
MRTG: Issues

• MRTG generates each graph (what if you have hundreds of graphs!) every 5 minutes, creating a lot of overhead.
• It also has very few customizable graphing options.
• Disk space is always an issue.
• MRTG management itself can be tedious work.
Using MRTG

- Get the required packages
- Compile and install the packages
- Make cfg files for router interfaces with `cfgmaker`
- Create html pages from the cfg files with `indexmaker`
- Trigger MRTG periodically from cron or run it in daemon mode
RRDTool

- Round Robin Database for time series data storage
- Command line based
- From the author of MRTG
- Made to be faster and more flexible
- Includes CGI and Graphing tools, plus APIs
- Solves the Historical Trends and Simple Interface problems as well as storage issues
- Find RRDtool here: http://oss.oetiker.ch/rrdtool/
Defining the Output (Archives)

- **RRA:AVERAGE:0.5:1:24**
  - **RRA** = Round Robin Archive
  - **AVERAGE** = consolidation function
  - 0.5 = up to 50% of consolidated points may be UNKNOW
  - 1:24 = this RRA keeps each sample (average over one 5 minute primary sample), 24 times (which is 2 hours worth)

- **RRA:AVERAGE:0.5:6:10**
  - 6:10 = one RRA keeps an average over every six 5 minute primary samples (30 minutes), 10 times (which is 5 hours worth)
  - **Clear as mud!**
  - All depends on original step size which defaults to 5 minutes
RRDTool Database Format

Recent data stored once every 5 minutes for the past 2 hours (1:24)

Old data averaged to one entry per day for the last 365 days (288:365)

--step 300
(5 minute input step size)

RRA 1:24
RRA 6:10
RRA 288:365

Medium length data averaged to one entry per half hour for the last 5 hours (6:10)
So simple…


- `rrdtool create /var/nagios/rrd/apricot-INTL_Ping.rrd -s 300 DS:ping:GAUGE:600:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`

What it looks like...

http://noc.ws.nsrec.org/mrtg/device.html

Traffic Analysis for Fa0/0 -- rtr.ws.nsrec.org

Traffic Analysis for Fa0/1 -- rtr.ws.nsrec.org

Traffic Analysis for Fa0/0.173 -- rtr.ws.nsrec.org
MRTG

• In Ubuntu / Debian

  – $ sudo apt-get install mrtg

  – Configuration
    • /etc/mrtg/<device.mrtg>
    • Global directory : /var/www/mrtg/
    • Run MRTG against the configuration file from cron
cfgmaker

• **Uses `snmpwalk` and creates an `mrtg` configuration file**

• `/usr/bin/cfgmaker
  --output=/etc/mrtg/router.mrtg
  --global 'workdir: /var/www/mrtg'
  --global 'options[_]: growright,bits'
NetManage@10.10.0.254`
Sample

- **Part of /etc/mrtg/device.mrtg**

- ### Interface 1 >> Descr: 'FastEthernet0/0' | Name: 'Fa0/0' | Ip: '' | Eth: '' ###

- Target[10.10.0.254_Fa0_0]: #Fa0/0:NetManage@10.10.0.254:
- SetEnv[10.10.0.254_Fa0_0]: MRTG_INT_IP="" MRTG_INT_DESCR="FastEthernet0/0"
- MaxBytes[10.10.0.254_Fa0_0]: 12500000
- Title[10.10.0.254_Fa0_0]: Traffic Analysis for Fa0/0 -- rtr.ws.nsric.org.nsric.org
- PageTop[10.10.0.254_Fa0_0]: <h1>Traffic Analysis for Fa0/0 -- rtr.ws.nsric.org.nsric.org</h1>
Creating HTML with indexmaker

• Execute **indexmaker** like this:

  • `/usr/bin/indexmaker` \ 
  • `--output=/var/www/mrtg/device.html` \ 
  • `/etc/mrtg/device.mrtg`

• If your mrtg configuration file is well commented, the html is nice and detailed.
Introduction to Traffic Flow
What Are Flows

• Traffic flows:
  – A sequence of packets.
  – Exchanged between discrete sources + destinations.
  – Flow data is not necessary a 1:1 mapping.
  – Can also be a group of packets in the network.
How Are Flows Accessible

• Three well-known methods today:
  – NetFlow (and friends)
  – IPFIX
  – sFlow
How Are Flows Accessible

- NetFlow:
  - Originally developed by Cisco Systems.
  - Developed to capture IP traffic information.
  - Most common implementations are NetFlow v5 + v9.
  - NetFlow v9 adds support for MPLS and IPv6 data.

- The following data can be gleaned from flows:
  - SNMP data.
  - Source + Destination IP addresses.
  - IP protocol.
  - TCP + UDP Source + Destination information.
  - IP ToS data.
How Are Flows Accessible

• NetFlow Friends:
  – Several vendors have developed NetFlow.
  – Are called by other names, but are the same.

  – Other implementations are:
    • AppFlow – Citrix.
    • Cflowd – Alcatel Lucent.
    • JFlow/cflowd – Juniper.
    • NetStream – 3Com.
    • NetStream – Huawei.
    • Rflow – Ericsson.
    • sFlow – Allied Telesis.
How Are Flows Accessible

- **IPFIX:**
  - Internet Protocol Flow Information Export
  - A standard-based flow capture protocol.
  - Is based on Cisco’s NetFlow v9.
  - Developed for any system that requires flow captures.
  - IPFIX uses SCTP as the transport protocol.
  - But also supports TCP and UDP.
How Are Flows Accessible

• sFlow:
  – Captures a sample of all “packets” on the network.
  – Naming of the technology is a misnomer.
  – sFlow does not capture flows. It captures packets.

  – Used mainly on switches for Layer 2 information.
How Are Flows Accessible

• NetFlow/IPFIX Differences with sFlow:
  – With NetFlow, flow cache is built on the router.
  – With sFlow, packet headers exported immediately.
  – With NetFlow, devices are complex, expensive.
  – With sFlow, devices are simpler, cheaper.
  – NetFlow provides great accuracy, even when sampled.
  – sFlow samples packets, which is less accurate.
  – NetFlow permits data set flexibility.
  – sFlow just samples packets.
How Can Flows Be Analyzed

• Three stages in flow analysis:
  – Collect the flows.
  – Export the flows.
  – Analyze the flows.

• In some cases:
  – Flow export is not really necessary.
  – Collection + analysis can be done locally.
  – Not scalable, but can be a “quick & dirty” fix.
How Can Flows Be Analyzed

• Collect the flows:
  – Device must support a NetFlow implementation.
  – NetFlow configured on participating interfaces.
  – Flow cache is built as data crosses the device.
How Can Flows Be Analyzed

• Export the flows:
  – Device resources are limited.
  – Devices built for switching/routing, not flow analysis.
  – So flows can be exported to a dedicated analyzer.

  – Flow cache built on local device.
  – Flow data then exported to a dedicated analyzer.
  – Flow data export sent periodically (configurable).

  – Data could be unsampled (accurate, but unscalable).
  – Data can be sampled (less accurate, but scalable).
How Can Flows Be Analyzed

• Analyze the flows:
  – Exported flow data is raw.
  – Needs to be analyzed for greater feedback.
  – Analyzers can generate a lot of information from flow.

  – Results can be represented in multiple ways.
  – As graphs or tables.

  – Representation flexibility varies.
  – Based on analyzer capabilities and feature set.
How Can Flows Be Analyzed

• Two major types of flow analyzers:
  – Non-commercial and/or free.
  – Commercial and/or paid-for.
How Can Flows Be Analyzed

- Non-commercial and/or free:
  - Based on Linux/UNIX or Windows.
  - Provides reasonable reports.
  - Good for small or medium-sized networks.
  - Not strong on features.
  - e.g., Flow-Tools, Nfsen/Nfdump, e.t.c.
• Commercial and/or paid-for:
  – Based on proprietary systems and technology.
  – A typically quite costly.
  – Are very capable and have extensive features.
  – Very flexible, offering various reporting options.
  – e.g., Arbor Networks, Network Instruments, e.t.c.
How Useful Is Flow Data

• Several legitimate uses:
  – Customer billing.
  – Upstream and peering profiling.
  – IPv6 traffic growth monitoring.
  – Visibility into Layer 2 data, e.g., MPLS, Ethernet, e.t.c.
Acknowledgement and Attribution

This presentation contains content and information originally developed and maintained by the following organisation(s)/individual(s) and provided for the African Union AXIS Project

Mark Tinka: - mtinka@psg.org