

Network Monitoring

Dr. John S. Graham
j.graham@ulcc.ac.uk

Introduction

- **Introduction**
 - Motivation
 - Challenges
 - Approaches
- **Active Monitoring**
 - SNMP Key Concepts
 - MRTG
 - cisco NetFlow
- **Passive Monitoring**
 - The ntop Packet Sniffer
- How Not to Go to Jail

Motivation

Planning

- Bandwidth Usage
- Network Hardening
- Target Services

Protection

- Intrusion Detection
- Compromised Hosts
- Faulty Hardware
- Police AUPs

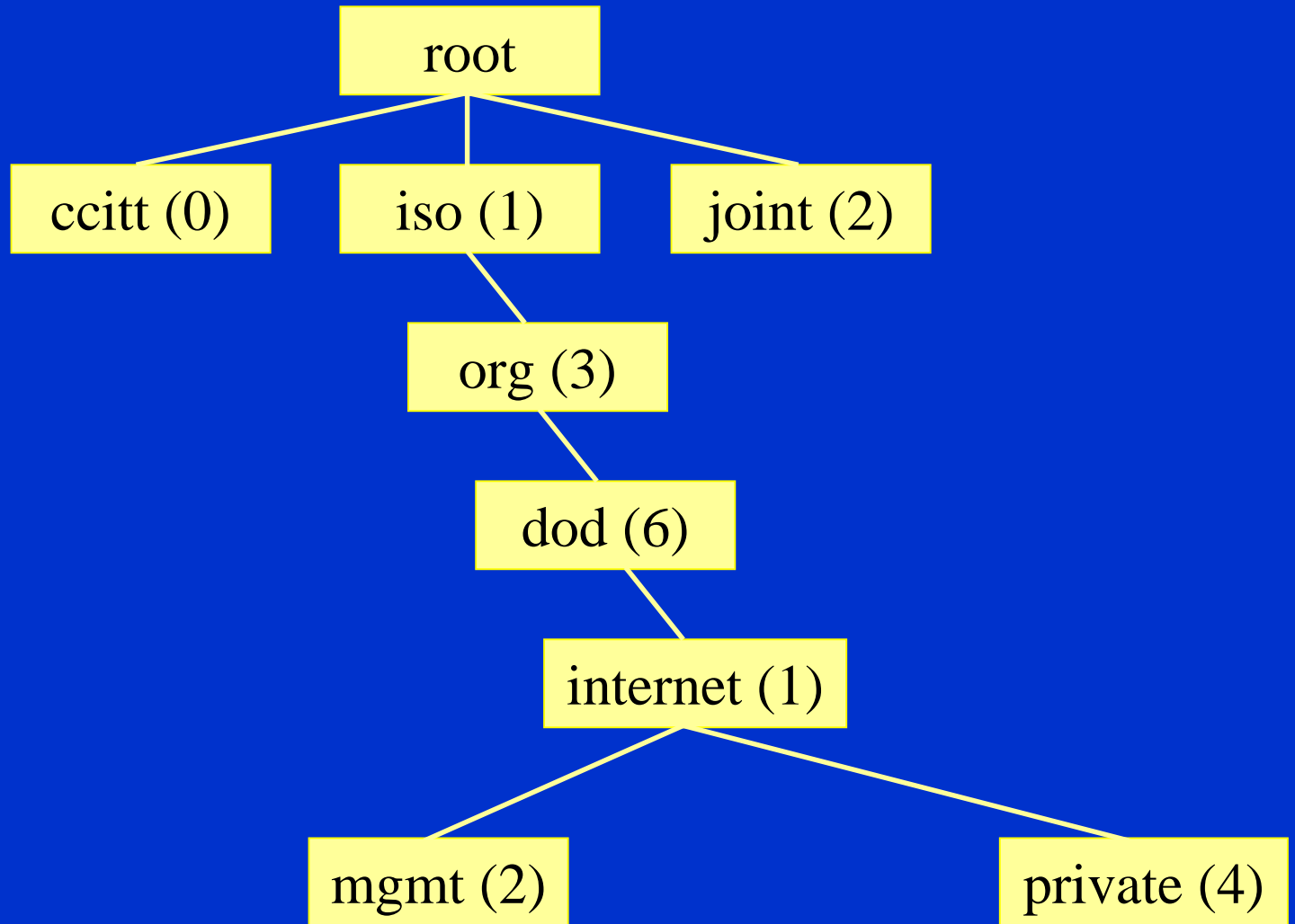
Challenges

- Complexity of networks and operating systems
- Interconnection of autonomous networks
- Users administer own workstations
- Widespread dissemination of 'cracking' techniques and tools

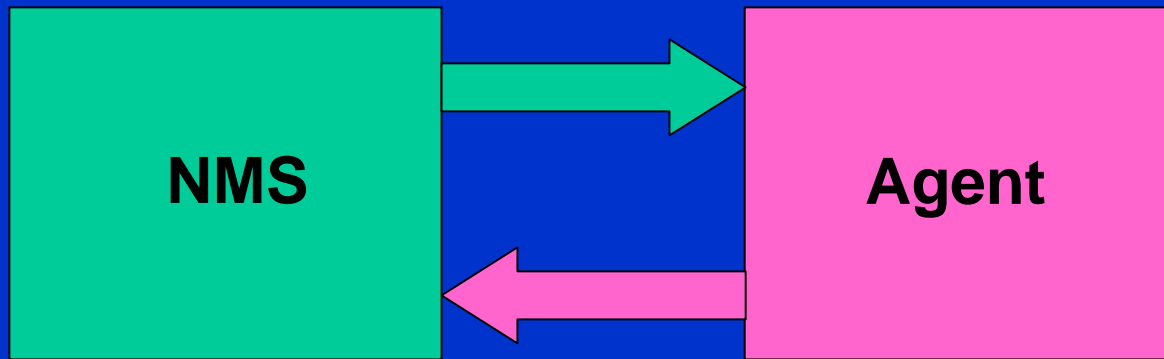
Approaches

- Active
 - Traffic is generated specifically for monitoring purposes
- Passive
 - Network traffic on a broadcast domain is examined to generate alerts or statistics
 - System files are monitored and alerts generated following a change of state

SMI Object Tree



SNMP Operations



```
snmpget gw.sunny.ac.uk public .1.3.6.1.2.1.2.2.1.10.2  
ifInOctets.2 = 17
```

MRTG

- Polls for the MIB-II standard objects:
 - *ifInOctets* (.1.3.6.1.2.1.2.2.1.10.x)
 - *ifOutOctets* (.1.3.6.1.2.1.2.2.1.16.x)
- Produces the following Cartesian plots:
 - Daily with 5-minute average
 - Weekly with 30-minute average
 - Monthly with 2-hour average
 - Yearly with 1-day average

Configuring MRTG

`WorkDir: /mrtg/images/`

`Target[sunny.2]: 2:public@gw.sunny.ac.uk`

`MaxBytes[sunny.2]: 256`

`Title[sunny.2]: gw.sunny:2`

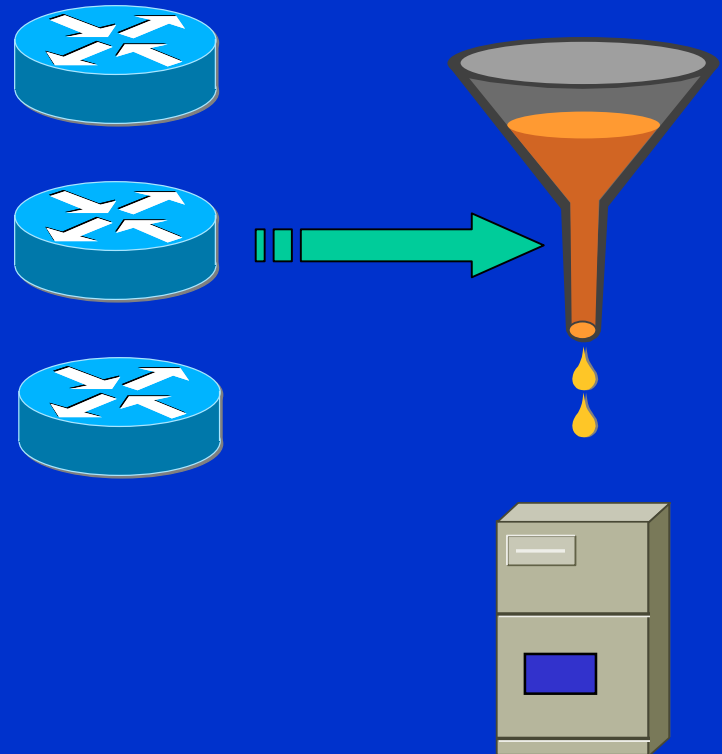
`PageTop[sunny.2]: <H1>Sunny College</H1>`

Standard Traffic Graph

- Almost all sites are net 'importers' of data
- Usage increases evenly from 'opening time', peaking at lunchtime and then declining slowly
- Little consequential traffic at night
- Outbound traffic at 10% - 20% inbound

Flow-based Analysis

- Source Address
- Destination Address
- Source Port
- Destination Port
- Protocol
- TOS Byte
- Input Interface



Configuring NetFlow

1. Enable an interface for flow switching

- `ip route-cache flow`

2. Set source address to use for exported packets

- `ip flow-export source <interface>`

3. Set Version

- `ip flow-export version 5 origin-as`

4. Set the export destination

- `ip flow-export destination <address> <port>`

Flow Collection

Flows are sent to the collector upon:

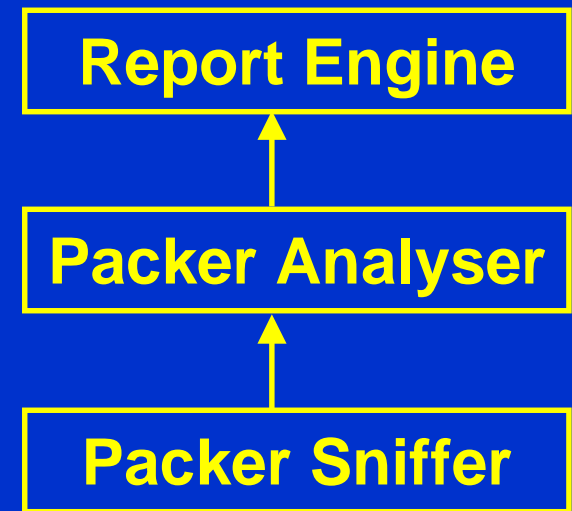
- expiration of an 'inactive' timeout
- expiration of an 'active' timeout
- seeing a FIN or RST
- other (undocumented) heuristics

Passive Monitoring

- Packet Tracers (e.g. tcpdump or snoop)
 - require off-line analysis tools
- Protocol Analysers
 - typically focus on contents of individual packets and not the whole network
- RMON Management Platforms
 - flexible and powerful but complex and costly

Passive Monitoring With ntop

Platforms	UNIX, Win32
Media	Ethernet, Token Ring, PPP, FDDI, Loopback
Protocols	IP, IPX, NetBIOS, AppleTalk, DecNet, DLC
IP Protocols	FTP, SMTP, HTTP, POP, IMAP, SNMP <i>etc</i>



The ntop User Interface

Terminal Mode

- Hostnames
- State
- Bytes Rcvd/Sent
- Total Traffic
- Protocol
- Throughput

Web Mode

How Not to Go to Jail

- RIP Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

What You May Legally Do

- ✓ Ascertain compliance with regulatory procedures
- ✓ National security
- ✓ To prevent or detect crime
- ✓ To prevent or detect unauthorised use
- ✓ To ensure effective systems operation

Further Information

- <http://www.mrtg.org>
- <http://www.uk.ntop.org>
- <http://www.cisco.com/go/netflow>
- <http://www.jisc.ac.uk/legal/>
- <http://traffic.ulcc.net>
- <http://netflow.ulcc.net/~netflow/>
- <http://www.ja.net/netsight>