MONASH University

Myles Fenton
July 2007

Application Aware Network Management

Agenda

- **Background**
- **The problem**
- **The approach**
- **The solution**
- **The next step**
- **Deployment considerations/issues**
- **Demo/Reporting examples**
- **The education campaign**
- **The business benefits**

Monash data network

- **Campuses**
  - 6 main campuses in Victoria
  - ~10 smaller campuses in Victoria
  - South Africa
  - Malaysia
- **Core**
  - 26 Cisco 6500 series router/switches
- **Edge**
  - 40,000 Gigabit Ethernet-capable ports
  - 420 Wireless Access Points
  - 47,000 registered IP addresses

Pre-existing network utilization software..

- Statseeker has provided port utilization/error reporting for a number of years.
- Has been effective at identifying utilization growth on all core and edge interfaces.
- This has allowed the Network group to install additional capacity when needed. Ie redundant links have exceeded an average 25% utilization (ie >50% load in single link failure mode.

Pre-existing network utilization software..

Limitations to basic port utilization statistics:

- Lack of visibility into network user and application behaviors for fault diagnosis or capacity planning
- No ability to monitor a QOS implementation. ie the real % of traffic being marked above/below Best Effort.
- No ability to baseline network health metrics for a future VOIP rollout

The objective:

- *Lets drill deeper*: Identity technologies and tools which identify traffic by user groups, applications and QOS classifications.
  Ie Application/user aware network management tools

Defining application aware network management…

"The identification of network resource use between users and applications to ensure that services run to user expectations."

- Where on the network are the users and services?
- Who are the users? Which departments?
- What applications/services are they using?
- How do they impact other applications/services?
- When are these services being used?
- Why is the network being used this way? Has it been optimized for maximum performance?

Over coming the assumption that the network should accommodate any and all applications

An analogy: Network traffic akin to Road traffic

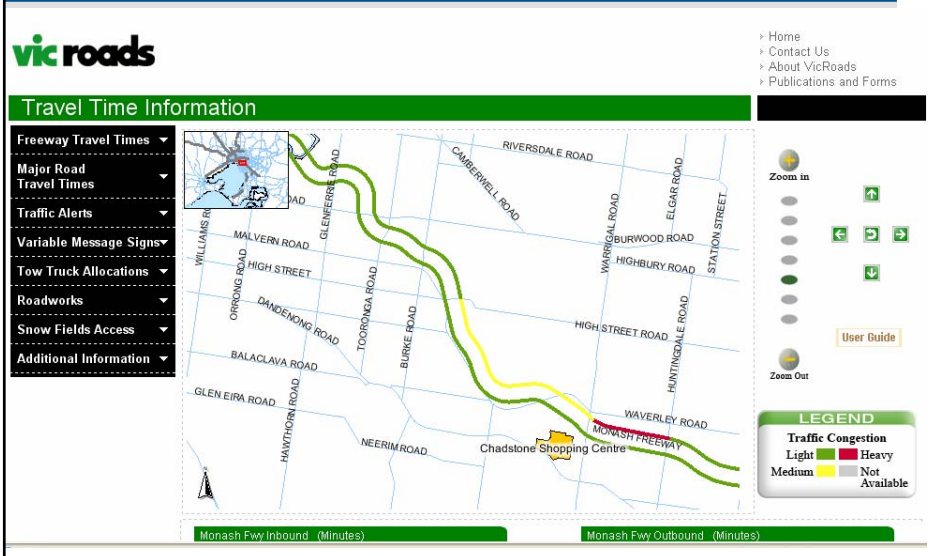
Road Traffic

- Different types of vehicle: cars, buses, trucks, motor bikes, bicycles, emergency vehicles.
- Some road traffic is abnormal and needs special care: wide/long vehicles, light rail, street parades

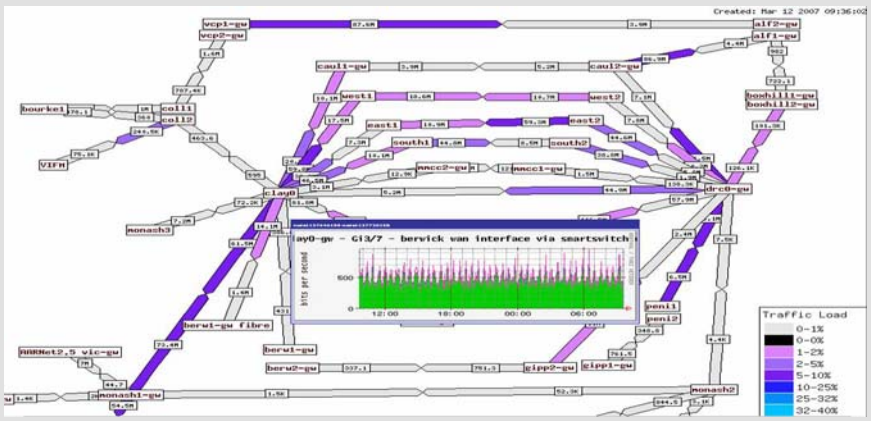
Network Traffic

- Different types of traffic: voice, video, teaching and administration applications, server backups.
- Some network traffic is abnormal and needs special care: lab imaging, eResearch data store transfers ~100TB

The birds eye perspective…Road network health…



The birds eye perspective…Data network health…



MONASH University

www.monash.edu.au

9

The search for better tools: network management data sources

Device health:

- SNMP from routers and switches provides valuable information specific to a device and associated interfaces eg queue buffers, CPU and memory utilization %.
- Limited traffic information

MONASH University

www.monash.edu.au

10

The search for better tools: network management data sources

Traffic sniffing probes:

Advantages:

- very detailed information on application performance and user behavior
- highly granular ms reporting capabilities which is often required for monitoring time sensitive applications like VOIP

Limitations:

- Scalability, cost and volume of data: sniffing individual Gigabit links is possible but not something you deploy everywhere.
- Gigabit probes are not cheap,
- produces a huge amount of data which results in many products heavily summarizing results to reduce storage constraints.

→ Therefore effective for specific deployments where a problem has been identified.

→ Something else required for wide scale deployment

How to drill deep: network management data sources

Cisco Netflow or IPFIX

- IP flow information providing detailed flow information including interface, source/destination ip address, application port/protocol and bytes/packets transferred
- When massaged into a well designed database, can effectively report the flow of network traffic per user (ip address), department (subnet) and application/server group.

Limitations:

- 1 minute granularity: Provides a detail on the % split of traffic between users, departments and applications but may not identify sources of congestion which occur for only a few seconds out of a minute.

How to drill deep: network management data sources

Cisco IPSLA

- A range of synthetic HTTP,VOIP,DNS,ICMP,TCP and UDP tests between IOS devices and servers to measure network latency/jitter and packet loss performance on the per second basis.

Limitations:

- A test probe may run for 10 seconds every minute. This means the reporting will miss an event if it occurs in the 50 seconds in which the test is not running. Balance between running the test more often and possibly observing an event but at the potential cost of the tests themselves creating an unacceptable load on the network or network devices.

Choosing a product

Monash conducted a 3 month pilot of Fluke (previously Crannog) Netflow tracker & Response watch vs Net QOS Report Analyzer/Super Agent.

Netflow product observations & comments:

- Netflow Tracker – comprehensive reporting, easy to use and generally responsive.
- Report Analyzer – fewer reports esp. QOS related. Harder to create custom queries.
- Decided against an In house development: building & supporting a database system which produces 15gig data not a small task and not primary skill set of the Network engineers

The future:

The continual search for greater granularity….

- IPSLA synthetic tests are valuable for a base line but will not diagnose individual VOUP calls faults
- Soon to investigate specific VOIP monitoring tools
- Currently evaluating a Fluke Visual Uptime sniffer unit: providing per call MOS scores.

The search for a management portal….

- Difficulties in wrapping all the different products in use at Monash into a single easy to navigate interface.
- Engineers and operators currently maintaining own bookmarks and homepages for network tool resources.
- Possibly next revision of Fluke One view.

Things to keep in mind when deploying netflow

- Evaluate your router/switch capabilities. Not all devices can do hardware netflow. Ie our 6500 router/switches can. 3750's can not.
- Monash is therefore limited to viewing traffic flowing between routers and therefore has only port utilization visibility for intra department/vlan traffic.
- Different revisions of hardware have slightly different netflow export capabilities.
- Netflow and flow based traffic policing has design limitations when implemented on the same device.

Demonstrating our new reporting capabilities:

MONASH University

www.monash.edu.au

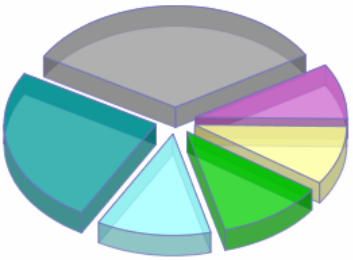
17

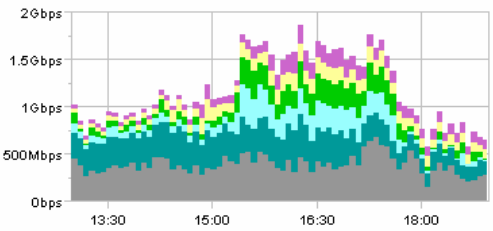
main menu > network overview

Network Overview

Time Range: 9/07/2007, 12:59 EST - 18:59 EST

Top Devices by Traffic Rate



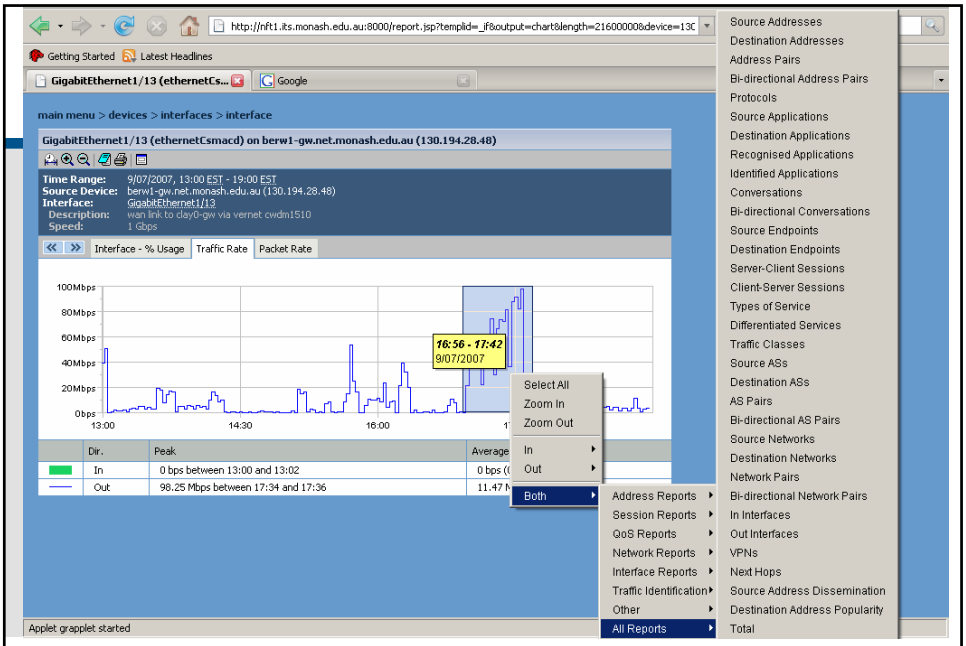


	Device Name	Peak	Average	% of Total
	clay1-gw.monash.edu.au	451.51 Mbps between 16:15 and 16:20	294.73 Mbps (741.11 GB)	25%
	drc1-gw.monash.edu.au	393.63 Mbps between 15:30 and 15:35	142.29 Mbps (357.8 GB)	12%
	south2-gw.net.monash.edu.au	294.07 Mbps between 15:30 and 15:35	132.58 Mbps (333.38 GB)	11%
	south1-gw.net.monash.edu.au	232.53 Mbps between 14:55 and 15:00	110.28 Mbps (277.31 GB)	9%
	caul1-gw.net.monash.edu.au	234.09 Mbps between 16:10 and 16:15	103.8 Mbps (261.01 GB)	9%
	Others	677.07 Mbps between 17:20 and 17:25	387.19 Mbps (973.62 GB)	33%
		1.86 Gbps between 16:15 and 16:20	**1.17 Gbps (2.88 TB)**	

MONASH University

www.monash.edu.au

18



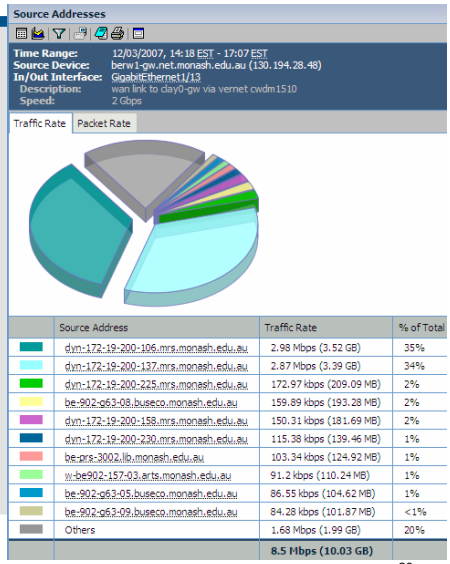
MONASH University

www.monash.edu.au

19

Case 1: Identifying users on the Berwick link

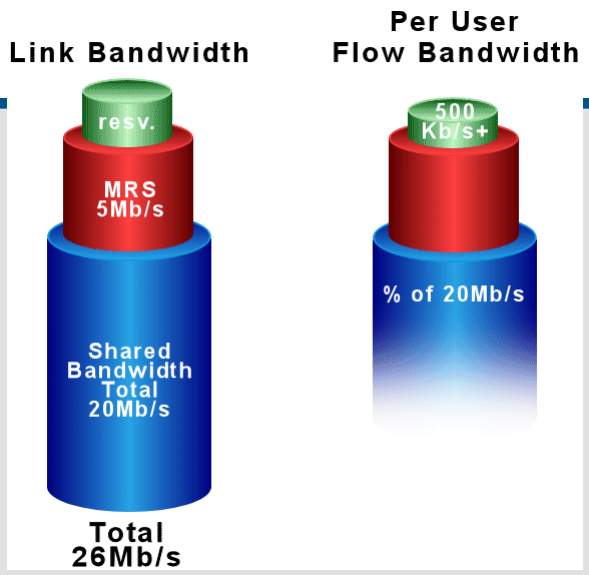
- Monitoring which users and departments are utilizing particular network resources
- Allows for traffic shaping to ensure distribution of network resources is targeted to the teaching and administration applications.



Source Address	Traffic Rate	% of Total
dyn-172-19-200-106.mrs.monash.edu.au	2.98 Mbps (3.52 GB)	35%
dyn-172-19-200-137.mrs.monash.edu.au	2.87 Mbps (3.39 GB)	34%
dyn-172-19-200-225.mrs.monash.edu.au	172.97 kbps (209.09 MB)	2%
be-902-g63-08.buseco.monash.edu.au	159.89 kbps (193.28 MB)	2%
dyn-172-19-200-158.mrs.monash.edu.au	150.31 kbps (181.69 MB)	2%
dyn-172-19-200-230.mrs.monash.edu.au	115.38 kbps (139.46 MB)	1%
be-prs-3002.lib.monash.edu.au	103.34 kbps (124.92 MB)	1%
w-be902-157-03.arts.monash.edu.au	91.2 kbps (110.24 MB)	1%
be-902-g63-05.buseco.monash.edu.au	86.55 kbps (104.62 MB)	1%
be-902-g63-09.buseco.monash.edu.au	84.28 kbps (101.87 MB)	<1%
Others	1.68 Mbps (1.99 GB)	20%
	8.5 Mbps (10.03 GB)	

MONASH University

20



MONASH University

www.monash.edu.au

21

Shaping users on the microwave links

```
class-map match-all SCAV
  match access-group name SCAV
class-map match-all MRS
  match access-group name MRS
!
policy-map SLOWWANOUT
 description restrict MRS to 15Mb/s during bus hours and remark all other >
     20Mb/s
  class MRS
   police cir 15000000 bc 468750 pir 15000000 be 468750 conform-action transmit
     exceed-action drop violate-action drop
  class ALL
   police cir 20000000 bc 625000 pir 20000000 be 625000 conform-action transmit
     exceed-action policed-dscp-transmit violate-action policed-dscp-transmit

policy-map SLOWWANIN
 description drop any CS1 traffic in excess of 512Kb/s
  class SCAV
    police flow 512000 31250000 conform-action transmit exceed-action drop
```

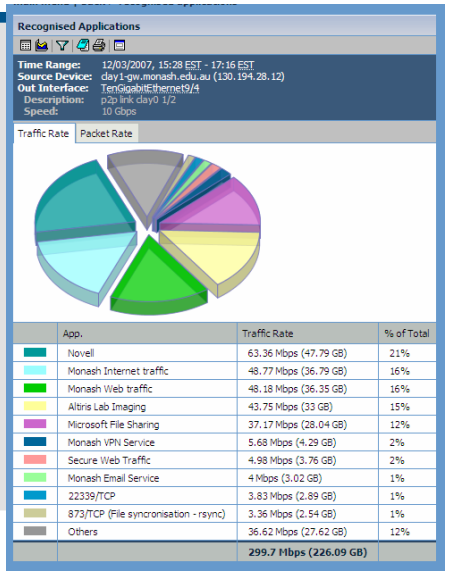
MONASH University

www.monash.edu.au

22

Case 2: Identifying Applications in the Core

- Monitoring which applications are utilizing core network resources



App.	Traffic Rate	% of Total
Novell	63.36 Mbps (47.79 GB)	21%
Monash Internet traffic	48.77 Mbps (36.79 GB)	16%
Monash Web traffic	48.18 Mbps (36.35 GB)	16%
Altiris Lab Imaging	43.75 Mbps (33 GB)	15%
Microsoft File Sharing	37.17 Mbps (28.04 GB)	12%
Monash VPN Service	5.68 Mbps (4.29 GB)	2%
Secure Web Traffic	4.98 Mbps (3.76 GB)	2%
Monash Email Service	4 Mbps (3.02 GB)	1%
22339/TCP	3.83 Mbps (2.89 GB)	1%
873/TCP (File syncronisation - rsync)	3.36 Mbps (2.54 GB)	1%
Others	36.62 Mbps (27.62 GB)	12%
	299.7 Mbps (226.09 GB)	

MONASH University

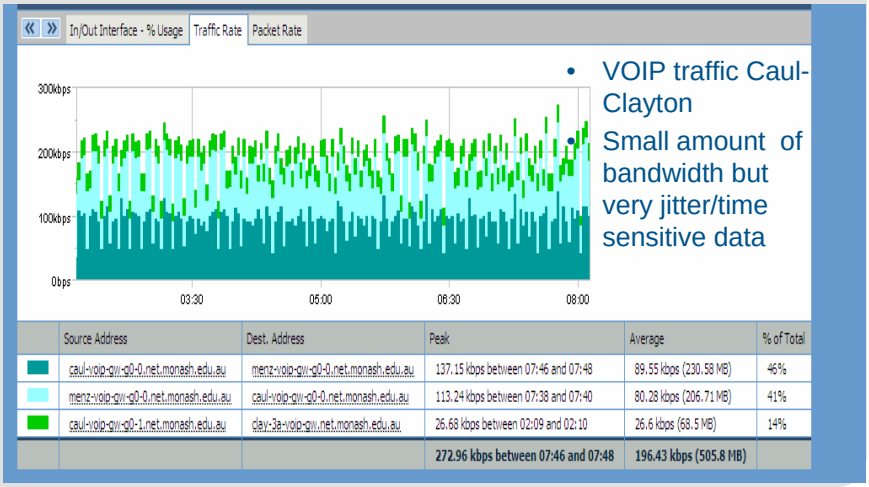
Case 3: Identifying Backup traffic across the 10Gig links

- Monitoring the times when backups are occurring
- Monitoring the peak bandwidth utilized for backups ~500Mb/s

Source Address	Dest. Address	Peak	Average	% of Total
icon.its.monash.edu.au	rhea.its.monash.edu.au	102.45 Mbps between 01:18 and 01:19	62.64 Mbps (78.76 GB)	14%
romulus.its.monash.edu.au	tethys.its.monash.edu.au	127.49 Mbps between 00:48 and 00:49	61.27 Mbps (77.04 GB)	14%
nexus.its.monash.edu.au	tethys.its.monash.edu.au	152.62 Mbps between 01:38 and 01:39	58.69 Mbps (73.79 GB)	13%
dfs-server-501.lib.monash.edu.au	rhea.its.monash.edu.au	180.29 Mbps between 01:31 and 01:32	41 Mbps (51.55 GB)	9%
mango.its.monash.edu.au	mimas.its.monash.edu.au	63.29 Mbps between 00:31 and 00:32	29.29 Mbps (36.83 GB)	7%
dfs-server-502.lib.monash.edu.au	mimas.its.monash.edu.au	43.75 Mbps between 01:59 and 02:00	20.25 Mbps (25.46 GB)	5%
thoth.its.monash.edu.au	mimas.its.monash.edu.au	54.89 Mbps between 02:57 and 02:58	17.44 Mbps (21.93 GB)	4%
ringtail.its.monash.edu.au	tethys.its.monash.edu.au	62.17 Mbps between 01:09 and 01:10	12.14 Mbps (15.27 GB)	3%
webpetal.its.monash.edu.au	mimas.its.monash.edu.au	58.89 Mbps between 02:56 and 02:57	10.98 Mbps (13.8 GB)	2%
calsilev.its.monash.edu.au	mimas.its.monash.edu.au	63.12 Mbps between 00:41 and 00:42	7.72 Mbps (9.71 GB)	2%
Others		423.13 Mbps between 00:17 and 00:18	118.34 Mbps (148.78 GB)	27%
		765.71 Mbps between 01:06 and 01:07	**439.76 Mbps (552.91 GB)**	

MONASH University

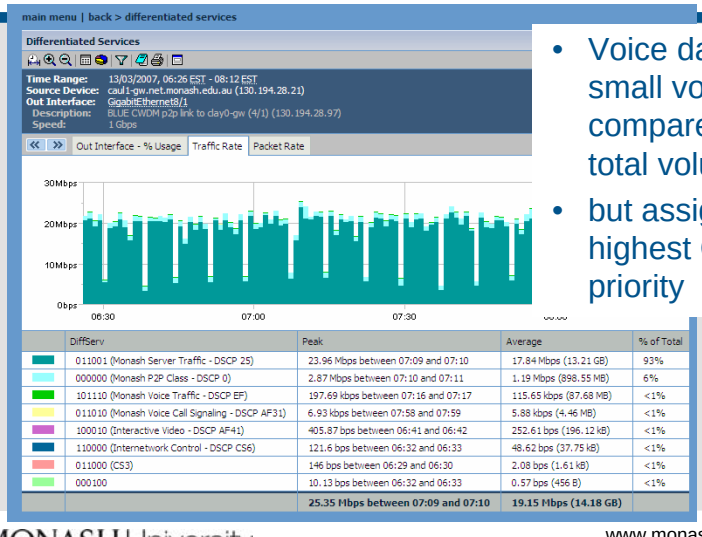
Case 4: Identifying Voice traffic



- VOIP traffic Caul-Clayton
- Small amount of bandwidth but very jitter/time sensitive data

	Source Address	Dest. Address	Peak	Average	% of Total
	caul-voip-gw-g0-0.net.monash.edu.au	menz-voip-gw-g0-0.net.monash.edu.au	137.15 kbps between 07:46 and 07:48	89.55 kbps (230.58 MB)	46%
	menz-voip-gw-g0-0.net.monash.edu.au	caul-voip-gw-g0-0.net.monash.edu.au	113.24 kbps between 07:38 and 07:40	80.28 kbps (206.71 MB)	41%
	caul-voip-gw-g0-1.net.monash.edu.au	day-3a-voip-gw.net.monash.edu.au	26.68 kbps between 02:09 and 02:10	26.6 kbps (68.5 MB)	14%
			272.96 kbps between 07:46 and 07:48	**196.43 kbps (505.8 MB)**	

Case 4: Identifying Voice traffic

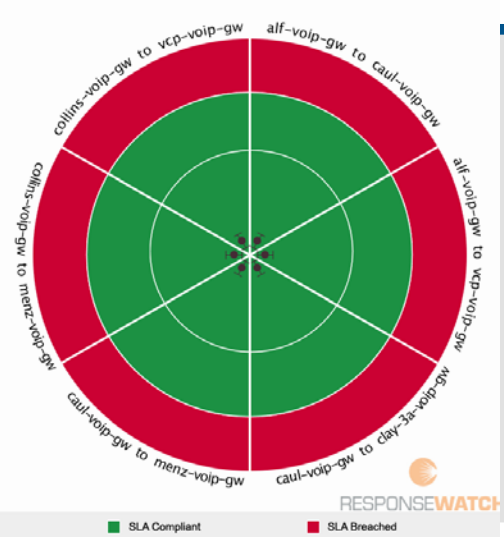


- Voice data small volume compared to total volume
- but assigned highest QoS priority

	DiffServ	Peak	Average	% of Total
	011001 (Monash Server Traffic - DSCP 25)	23.96 Mbps between 07:09 and 07:10	17.84 Mbps (13.21 GB)	93%
	000000 (Monash P2P Class - DSCP 0)	2.87 Mbps between 07:10 and 07:11	1.19 Mbps (898.55 MB)	6%
	101110 (Monash Voice Traffic - DSCP EF)	197.69 kbps between 07:16 and 07:17	115.65 kbps (87.68 MB)	<1%
	011010 (Monash Voice Call Signaling - DSCP AF31)	6.93 kbps between 07:58 and 07:59	5.88 kbps (4.46 MB)	<1%
	100010 (Interactive Video - DSCP AF41)	405.87 bps between 06:41 and 06:42	252.61 bps (196.12 kB)	<1%
	110000 (Internetwork Control - DSCP CS6)	121.6 bps between 06:32 and 06:33	48.62 bps (37.75 kB)	<1%
	011000 (CS3)	146 bps between 06:29 and 06:30	2.08 bps (1.61 kB)	<1%
	000100	10.13 bps between 06:32 and 06:33	0.57 bps (456 B)	<1%
		25.35 Mbps between 07:09 and 07:10	**19.15 Mbps (14.18 GB)**	

Case 4: Measuring Performance - Voice traffic

- Given the jitter/latency ie time sensitive nature of voice, each VOIP gateway is monitored against an SLA metric
- SLA's for other apps.

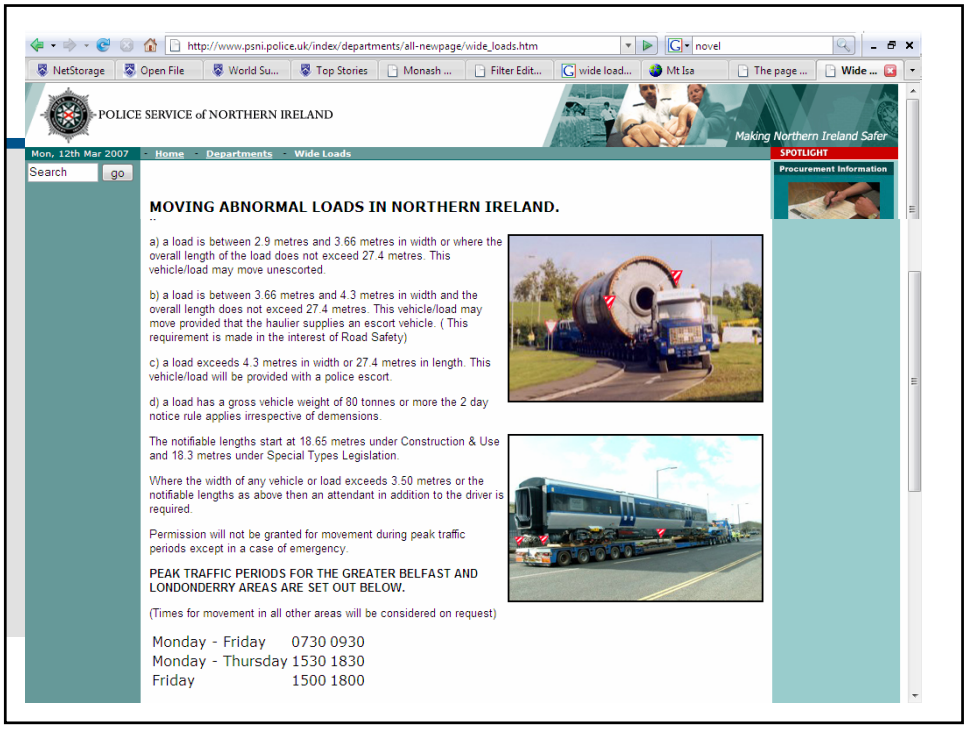


Education campaign: Managing special needs traffic…

- Working with Faculty and desktop support staff to encourage sensible use of network.

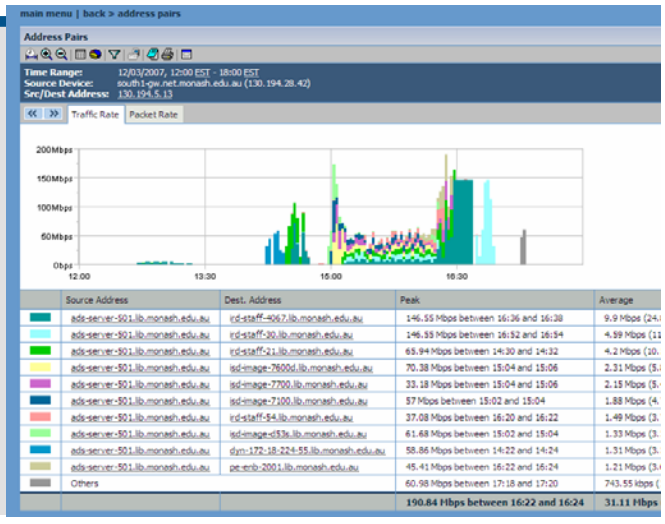
The campaign analogy..

- What is the effect of abnormal traffic on the road?
- When should abnormal traffic be transported?



Case 5: Identifying Lab Imaging

- Imaging has high volume and bandwidth requirements.
- Works on the Clayton 'gigabit everywhere network'
- Fails over 34Mb/s WAN links



MONASH University

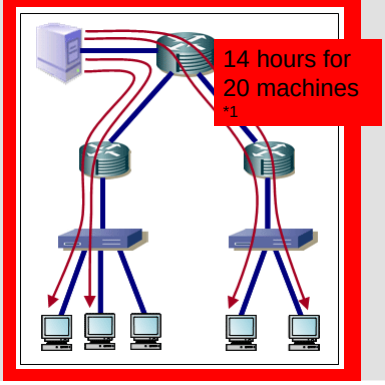
www.monash.edu.au

30

Education campaign: Multicast vs Unicast for Lab imaging

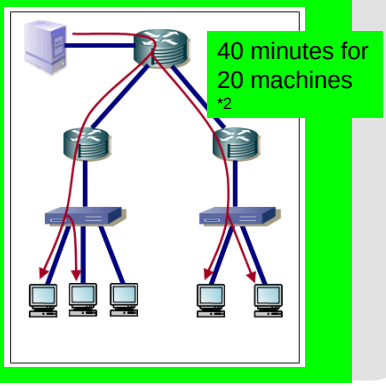
•**Unicast** poor performance

•Poor use of network resources



•**Multicast** excellent performance

•Efficient use of network resources



MONASH University

*1 5GB image @ 5.5Mb/s

*2 5GB image @ 111Mb/s

ITS Networks application approval certificate… *Needed?*

- **Road traffic management**

Left hand side, Traffic lights, roundabouts, bike lanes, road rules..
Drivers license – roadworthy certificate.

- **Network traffic**

TCP/IP, Subnetting, Routing, switching, QoS, Addhost registration
Using existing approved and ITS standardized applications
in future: ITS Networks application approval certificate. ***?***

MONASH University

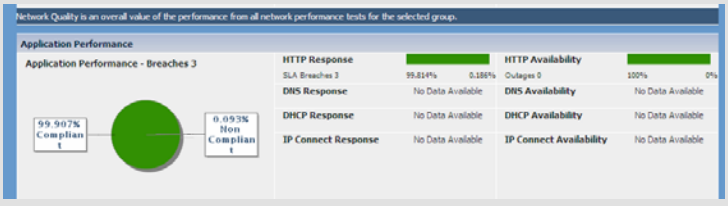
Deploying new applications

Deploying new applications and working with Faculty and Desktop Support staff:

- *How to avoid the killer application that grinds other network services to a halt…*
- Encouraging the use of existing approved and ITS standardized applications in preference to deploying new solutions (IT Architecture).
- For new applications organize a meeting with NIS at the project concept stage to discuss possible network implications.
- Involve NIS in the proof of concept to evaluate the network performance of the application and provide a written report on the applications suitability for the Monash Network.

The benefits: How are we using the Application Awareness?

- Network health monitoring before faults are logged
- Forensic tool for fault and security incident investigation
- Capacity planing & cost justification for upgrades to expensive infrastructure
- Service Availability Management, SLA's and delineation between Server slow/Network slow



Questions?

Further reading:

- **http://www.cisco.com/go/netflow**
- **http://www.cisco.com/go/ipsla**
- **http://www.ietf.org/html.charters/ipfix-charter.html**
- **http://www.flukenetworks.com/fnet/en-us/products/NetFlow+Tracker/Overview.htm**
- **http://www.flukenetworks.com/fnet/en-us/products/ResponseWatch/Overview.htm**

A non-standards based approach….

Image references:

- **http://traffic.vicroads.vic.gov.au/trafficinfo/viewer.aspx**
- **http://www.psni.police.uk/index/departments/all-newpage/wide_loads.htm**
- **http://images.google.com**