Argonne NATIONAL LABORATORY

... for a brighter future

U.S. Department of Energy

THE UNIVERSITY OF CHICAGO

Office of Science U.S. DEPARTMENT OF ENERGY

A U.S. Department of Energy laboratory managed by The University of Chicago

High Speed Data Transfer from the APS

Kenneth Sidorowicz

September 27, 2006

Deep Inspection Firewalls

- Secure Computing G2 Model 4150 firewalls were installed during the September 2004 accelerator shutdown
- Deep inspection firewalls not only perform stateful packet filtering but also inspects packet payloads using specific attack signatures and Layer 7 protocol engines
- Active/Active high availability configuration with cluster management via Enterprise Management Appliance
- Utilizes Smart Filter web content filtering
- Cloudmark anti-spam filtering and Sophos anti-virus
- Protects against web and e-mail viruses and spyware

Additional Cyber Equipment and Software

- Pair of Cisco Firewall Service Modules (FWSM) in Prism to protect visitor, wireless, and video conferencing networks.
- E-mail is filtered through Cloudmark anti-spam software on Secure Computing G2 Firewalls and Spam Assassin running on a Sun Solaris server. Cloudmark is a commercial product that doesn't allow customization. Spam Assassin configuration files are modified with APS filters.
- Cisco Intrusion Detection System Module (IDSM-2) Installed in Prism
- Automated E-mail blacklisting for 7 days which includes exception list
- Automatic firewall shunning via APS Netflow and firewall log scripts.

Web URL Filtering

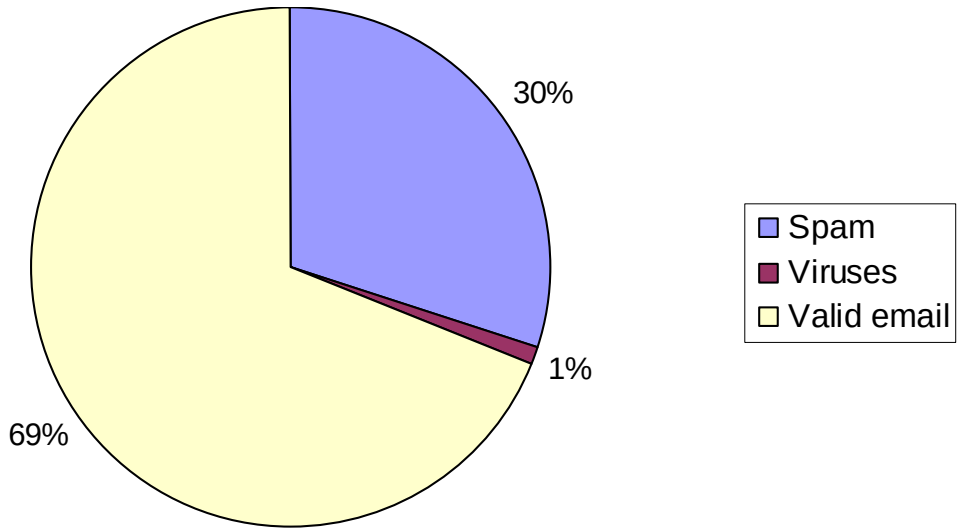
- Smartfilter from Secure Computing built into SideWinder firewall.
- Provides database of millions of blockable web sites in over 70 categories.
- Blocks Spyware and Phishing web sites.
- Increase productivity and preserve bandwidth for business-related activities.
- SmartReporter provides real time reports of web activity.

Automated Network Blocking

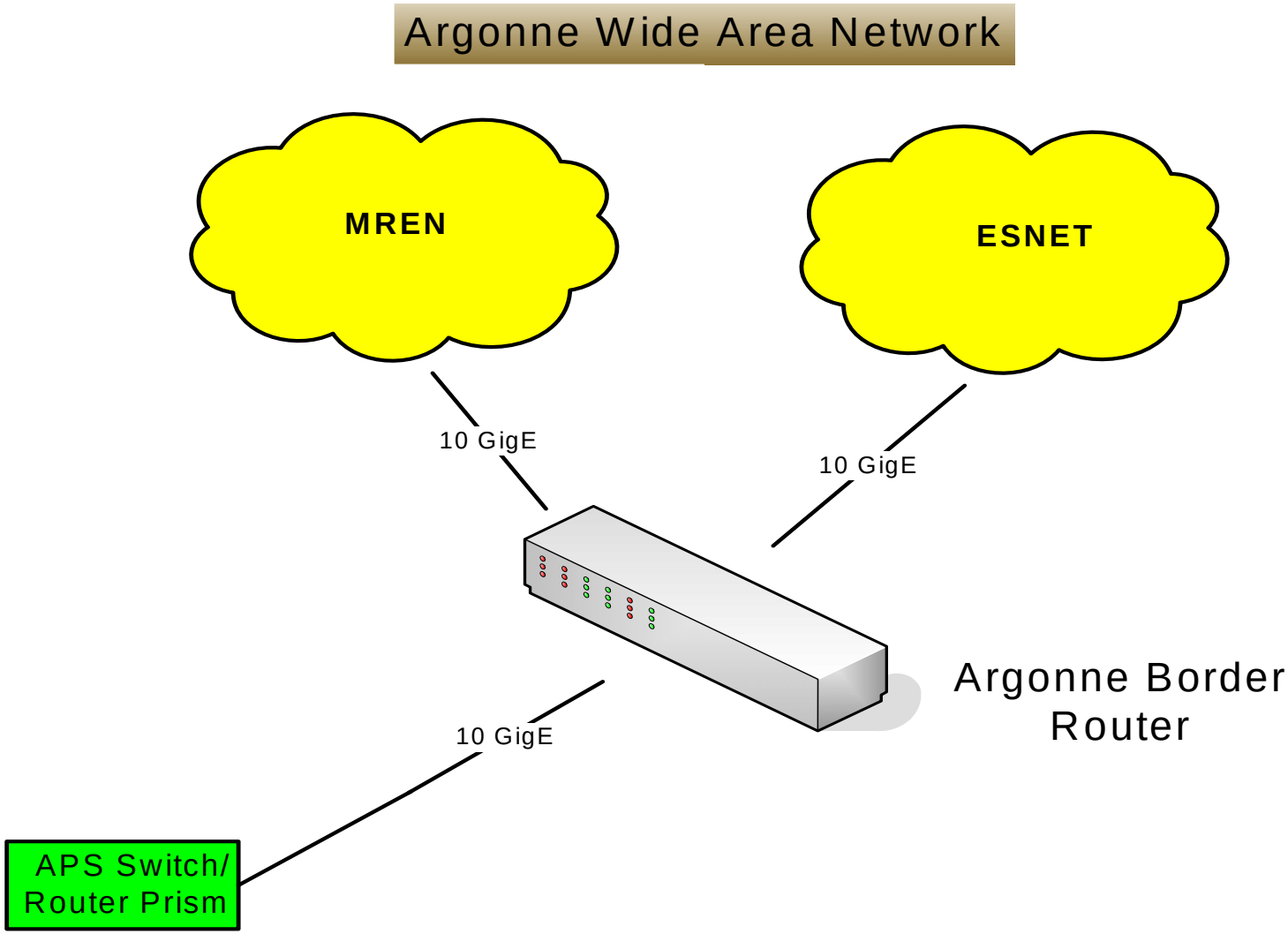
- IT scripts scan firewall and switch data logs looking for suspicious network activity. Once per minute.
- Intrusion Detection System monitors network traffic looking for known virus signatures.
- Blocks are then added automatically to protect our network from intrusion.
- Beamline CSPRs are notified immediately via email when blocks are added.
- 100-400 external network blocks are issued each day.

Mail Stats

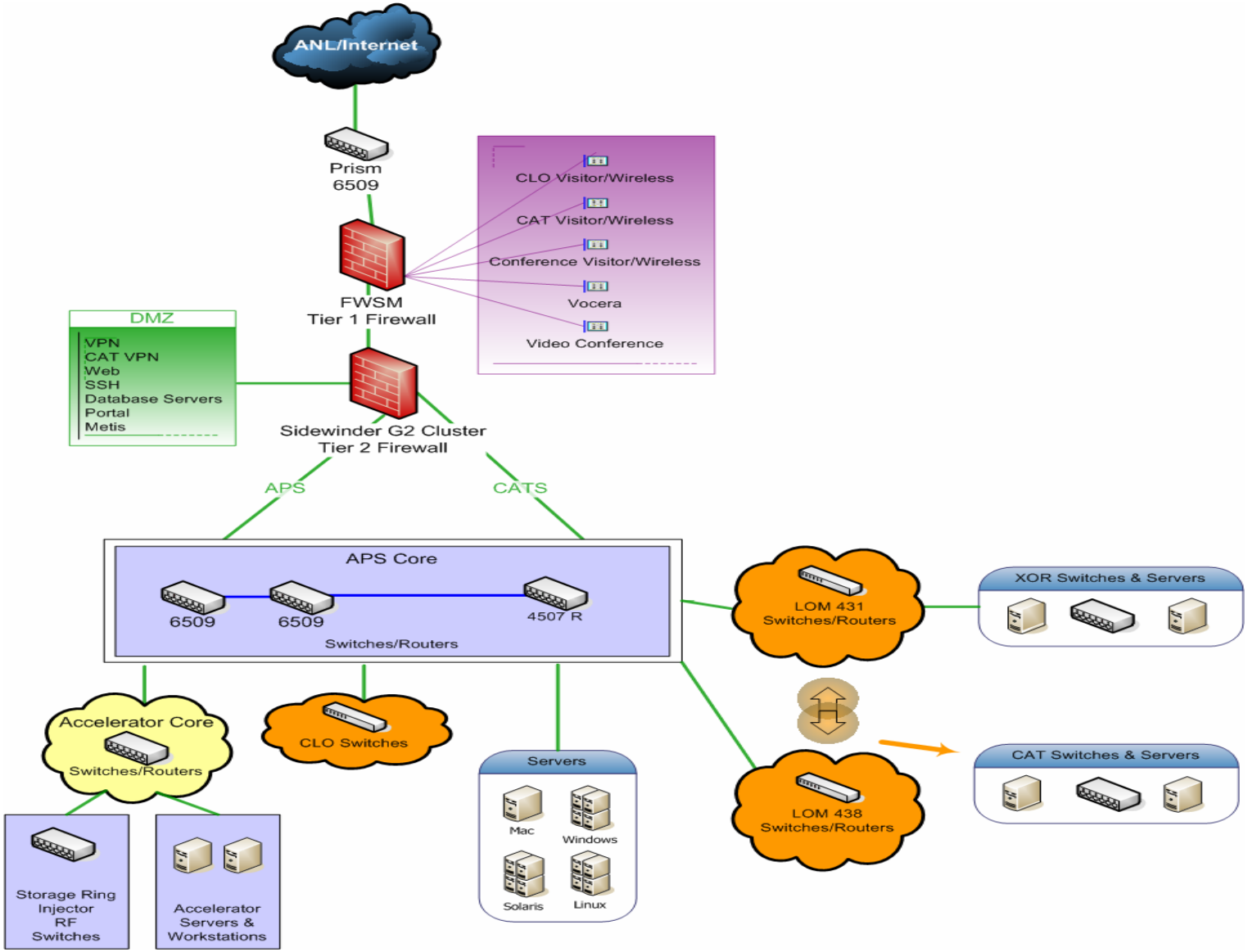
- APS processes between 15,000 and 20,000 emails a day.
- 20% to 30% of all email is detected as spam, 3000-5000 emails.
- Anti-virus signatures are updated hourly.
- Virus infected email varies from 50 to 200 a day.



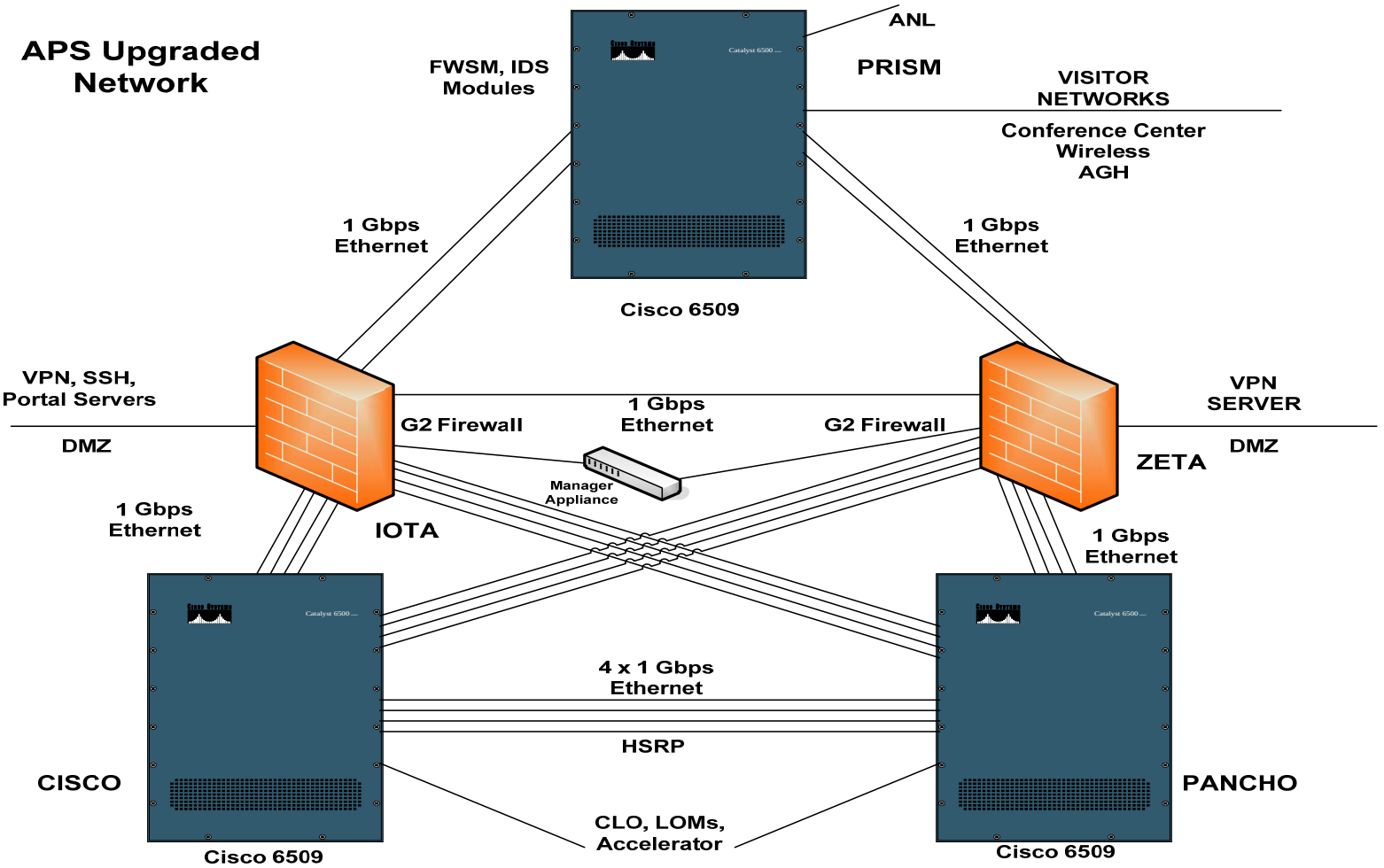
Argonne Wide Area Network Connections



APS Network


ANL/Internet
Prism
6509
FWSM
Tier 1 Firewall
CLO Visitor/Wireless
CAT Visitor/Wireless
Conference Visitor/Wireless
Vocera
Video Conference
DMZ
VPN
CAT VPN
Web
SSH
Database Servers
Portal
Metis
Sidewinder G2 Cluster
Tier 2 Firewall
APS
CATS
APS Core
6509
6509
4507 R
Switches/Routers
LOM 431
Switches/Routers
XOR Switches & Servers
Accelerator Core
Switches/Routers
CLO Switches
Servers
Mac
Windows
Solaris
Linux
LOM 438
Switches/Routers
CAT Switches & Servers
Storage Ring
Injector
RF
Switches
Accelerator
Servers &
Workstations

APS Core Network



Iperf Testing at the APS

- 938 Mbps between LOM's and APS edge router Prism
- 920 Mbps between LOM's and Argonne's edge router
- Iperf measures TCP and UDP bandwidth performance
- Iperf is available at http//dast.nlanr.net/Projects/Iperf

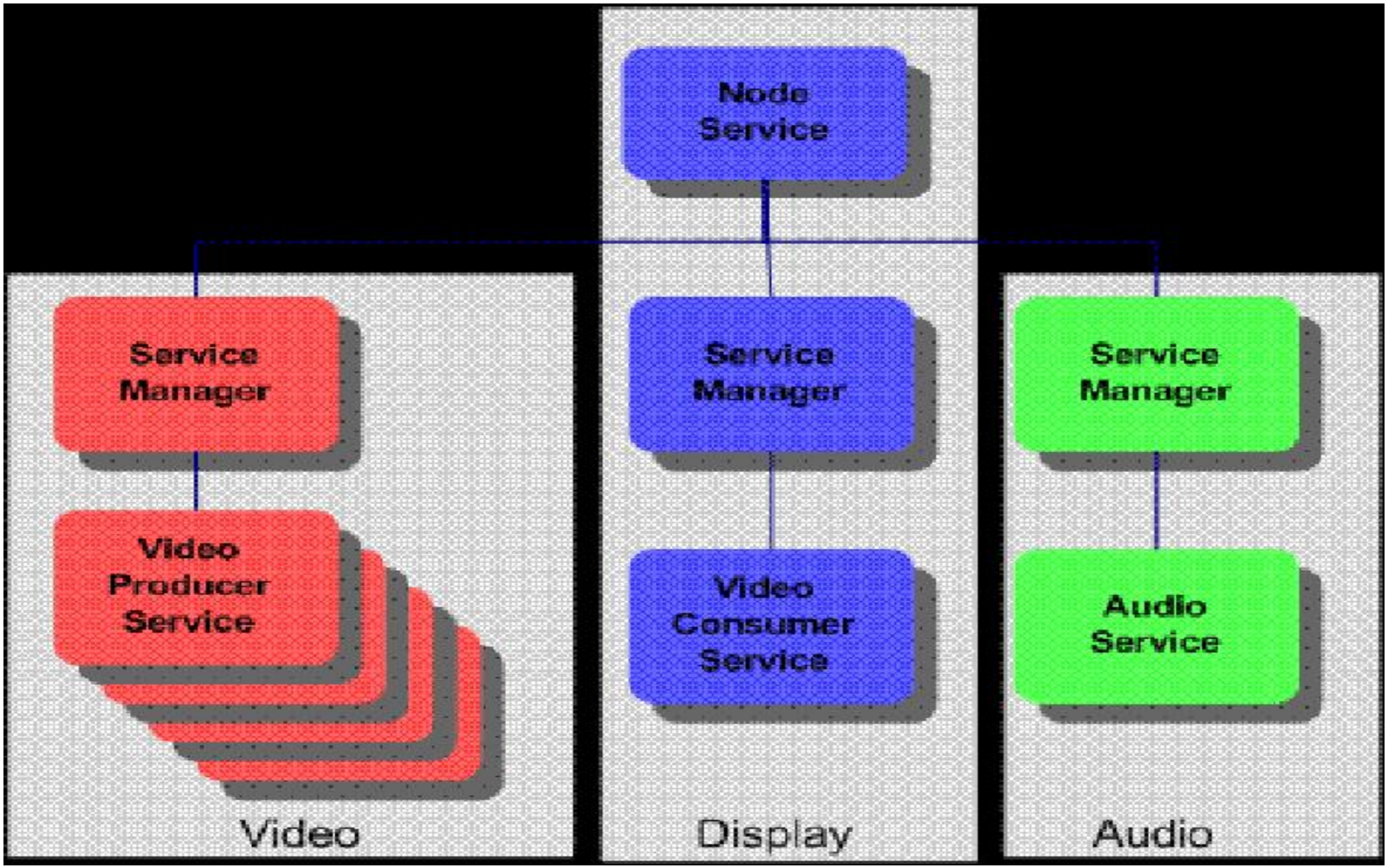
Network Performance

- Over 900 Mbps through Sidewinder G2 firewalls using Iperf
- Over 600 Mbps through the Cisco FWSM
- No shaper appliances at APS or on ANL backbone network
- No throttling of network flows at APS or on ANL backbone network

Network Shaper

- Enables Bandwidth Control
- Classifier traffic into defined Quality of Serve (QOS) classes
- For example – web traffic is deemed more important than ssh traffic
- Can be used to throttle a subnet or user's traffic
- Shapers are used by universities and corporations.

The Access Grid



- From: http://www.accessgrid.org/

Additional Services

Dservs – distributed servers provide the following services

DNS - Domain Name Service

DHCP – Dynamic Host Configuration

EPICS distribution which is

Accessible via Samba & NFS

PV Gateways – Process Variable Gateways

CAT VPN server

Citrix servers – Metis.aps.anl.gov for Argonne administrative applications

10GigE beamline cable infrastructure installations

Future Plans

- Upgrade the backbone network and Argonne uplink to redundant 10 GigE. Vendors are promising new modules will be available in calendar year 2007.
- Upgrade Tier 1 and Tier 2 firewalls to 10 GigE. Vendors are promising new firewalls will be available in calendar year 2007.
- 802.1x authentication for wireless access to internal networks.
- Distributed iperf servers to measure network performance.