Bolting the door

Network Based Security Mechanisms

David Crooks, Mark Mitchell
on behalf of ScotGrid Glasgow

EGI Tech Forum, Lyon, September 2011

Infrastructure overlooked?

- Network infrastructure attacks less common than host based
- However, more disruptive
- Potential to cause major issues
- Network security doesn't stop at a NIC

Multiple vectors

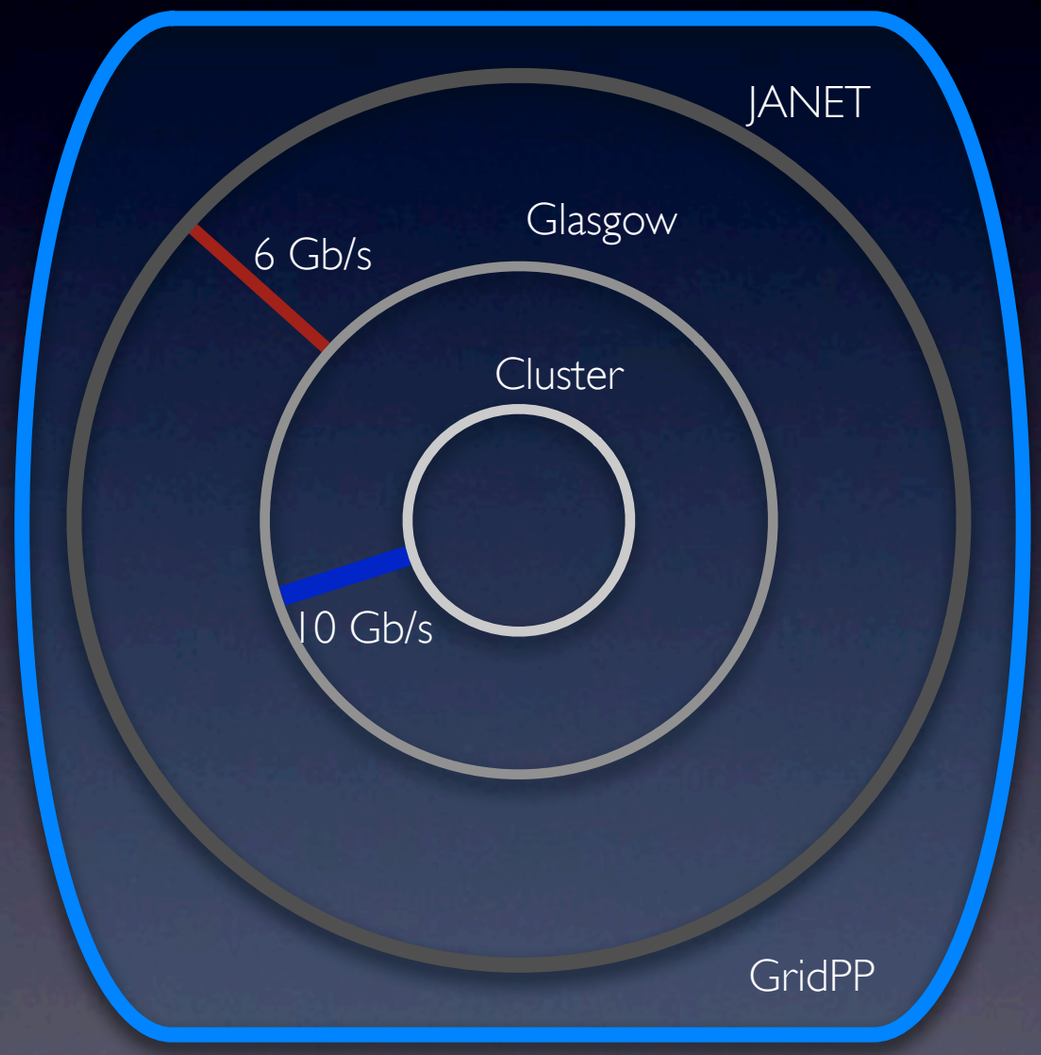
- External (Internet)
- Internal (MAN/LAN and trusted sources)
- Hardware flaws
- Software flaws
- Popularity *vs* obscurity

Multiple solutions

- Hardware/software firewalls
- Hardware/software based IDS (Intrusion Detection Systems)
- Built in security in protocols (IPSEC, IPv6)
- Built in security services in network OS

Networks

- ScotGrid Glasgow cluster
- Glasgow campus
- Janet
- GridPP
- Various security models implemented across this structure (ACL based to optimise transfer rates)

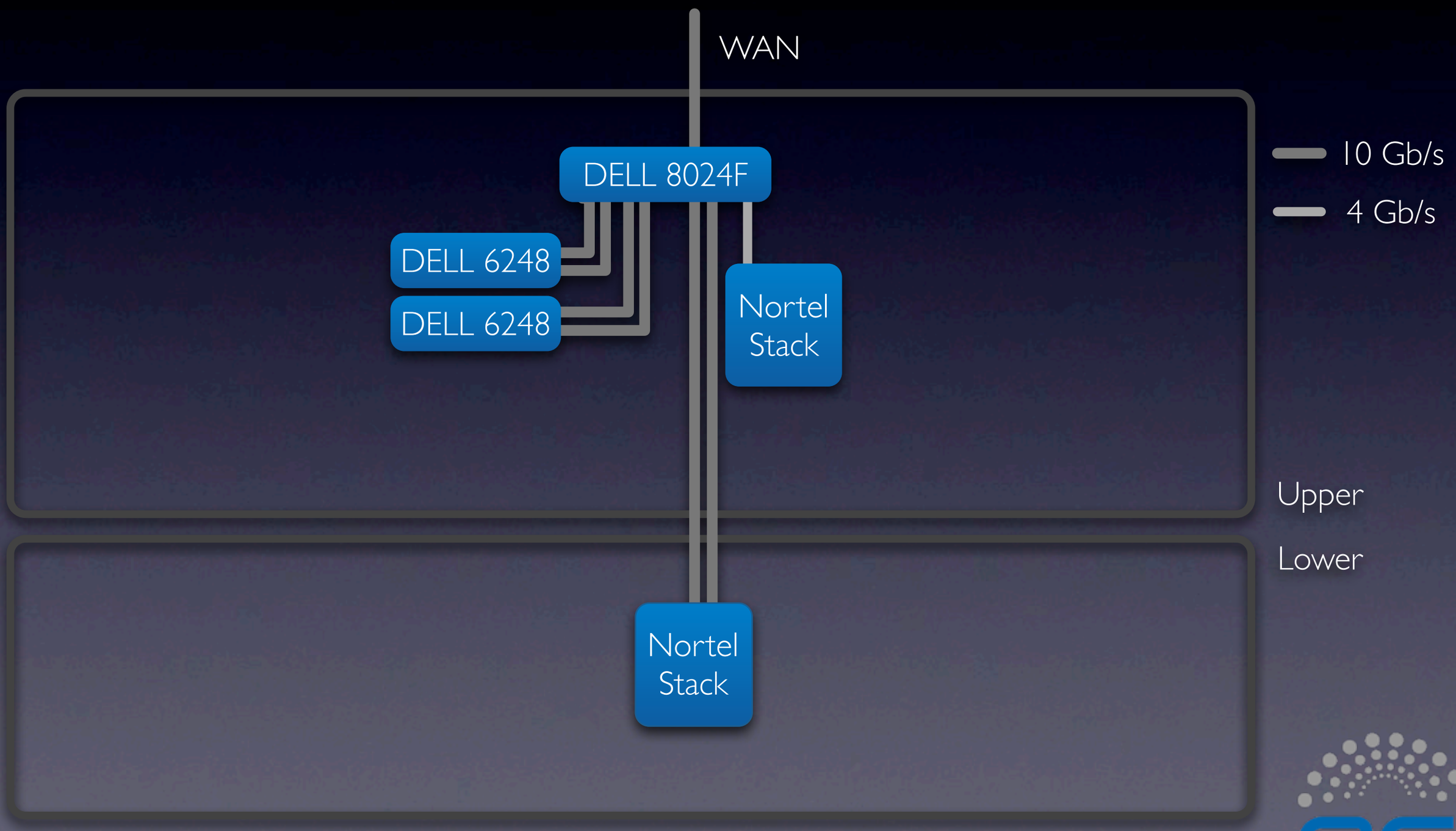


GridPP
UK Computing for Particle Physics

University of Glasgow

ScotGrid

Securing a 10 Gb/s connection at Glasgow

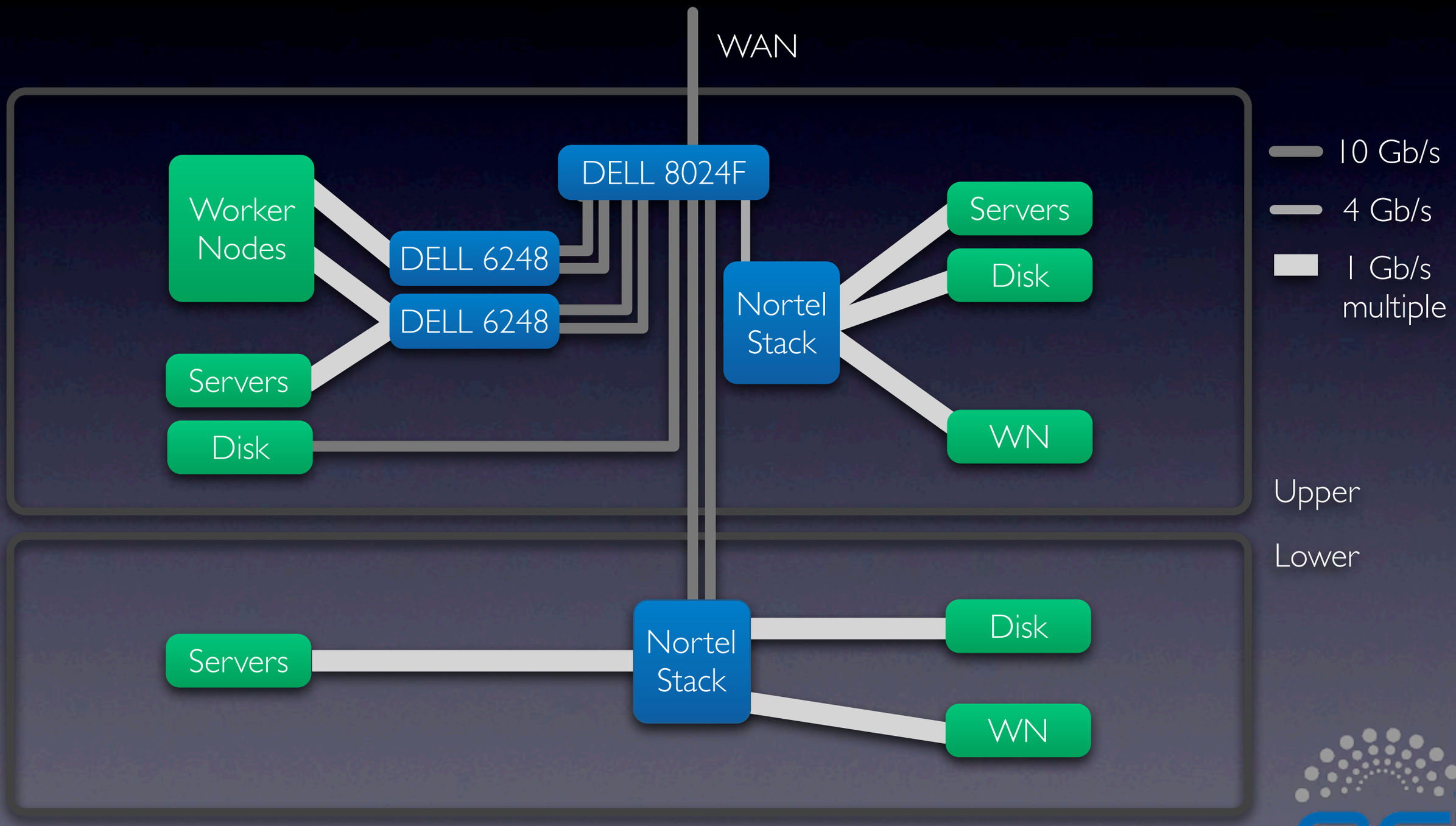


GridPP
UK Computing for Particle Physics

University of Glasgow

ScotGrid

Securing a 10 Gb/s connection at Glasgow

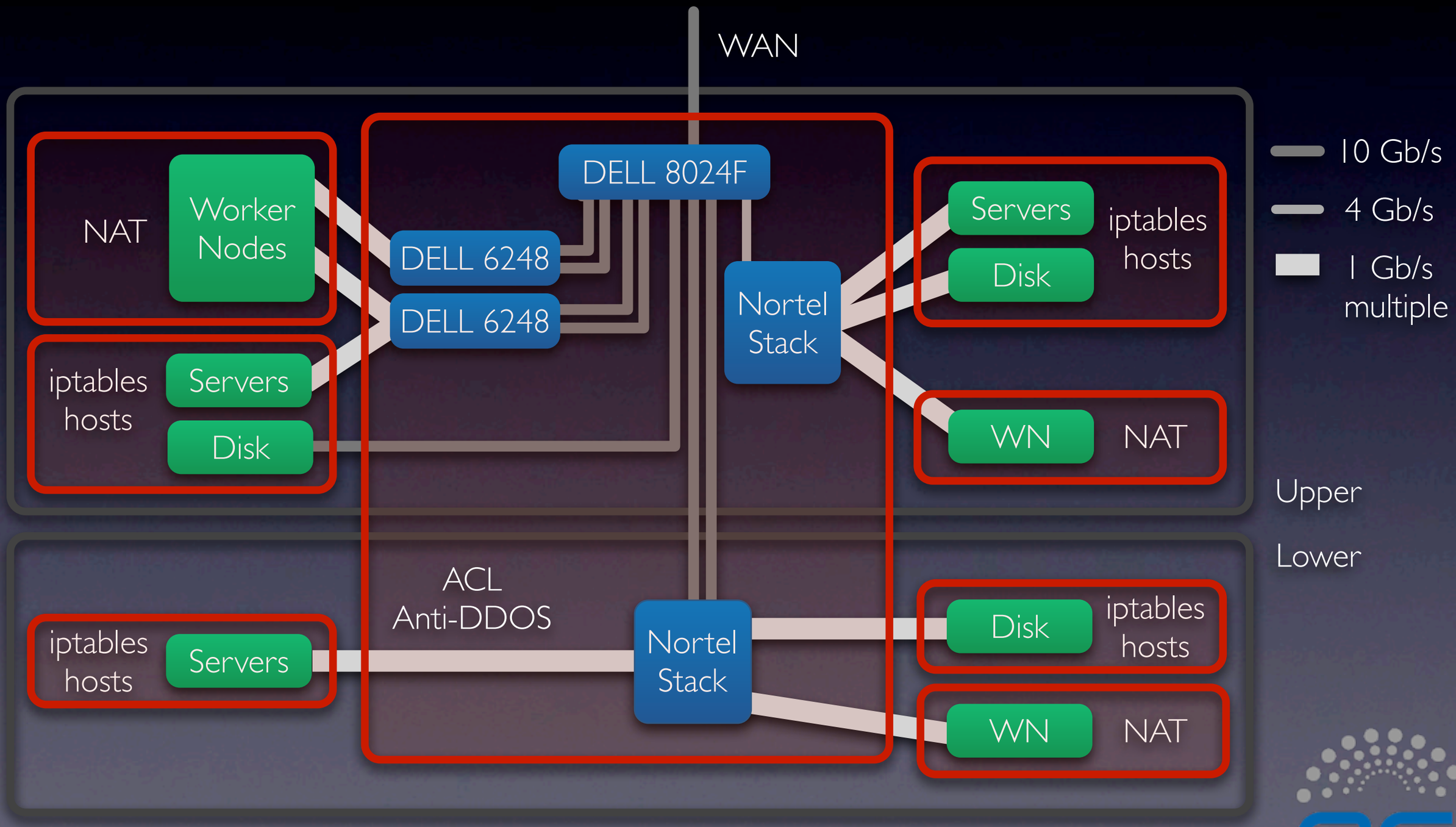


GridPP
UK Computing for Particle Physics

University of Glasgow

ScotGrid

Securing a 10 Gb/s connection at Glasgow



Securing a 10 Gb/s connection at Glasgow

- Equipment - DELL/Cisco/Nortel
- Not all switches are equal
  (mixed vendor - mixed procurement but also security)
- Logging - Applied on all switches (syslog)
- Additional Monitoring Platforms - Nagios etc.
- Traffic flow/spikes monitored at campus level

Securing a 10 Gb/s connection at Glasgow

- Multi tiered solution
- Edge Access Lists (Layer 3, Campus)
- Distribution Access Lists (Layer 2, Cluster)
- Access Devices (Layer 2, to host)
- Host Based Solutions, iptables ⟷ OSSEC

Going a bit further

- Nagios (Reporting)
- OSSEC (Denying, reporting and Logging)
- Host Based Access Lists banning known bad IP Addresses
- MAC Address control on the switch ports

Problems with enhanced security

- Not every command works in a cluster - unexpected effects at different layers
- Vendor interoperability issues
- Enhanced security mechanisms can and do slow network through put
- How Secure are Open Source Solutions?- choose and combine with care

Open source vs proprietary *or* Hardware vs software

- Hardware based firewall/IDS solutions now available from Check Point, Juniper and Cisco which will run at 10 Gb/s transparently.
- Costly and difficult to maintain properly.
- Open Source software and commands on proprietary networking equipment can be deployed effectively but require more setup and planning.
- Cheap and difficult to maintain properly *but* community of practice (National collaboration)

Enhancing the network

- Host Specific network based access lists may require Layer 2 QOS to be applied
- Careful tuning required especially around ICMP (internet control messaging) settings
- Glasgow Cluster went into a partial failure state due to an incorrectly configured ACL on the network

Multi tiered approach

- Balance between security, speed and reliability difficult to implement out of the box
- Careful planning required
- At least three tiers of security must be implemented within the cluster

Multi tiered approach

- At least one mechanism may cause production issues
- Good operational procedure vital to ensure that working security mechanisms are kept up to date and are monitored consistently and effectively
- Importance of communication

GridPP
UK Computing for Particle Physics

University of Glasgow

ScotGrid

Any Questions?

EGI