



Fall 2008 • Computer Consultant Support Program

What's on the Horizon for Network Technologies

Charley Kline

Campus IT Architect, CITES



Quickie Updates

- Core Upgrade complete
 - Extremely smooth unlike 2006
 - Same basic architecture with increased redundancy and opportunities for multiple building connections
 - Newer, more flagship equipment
 - VRF- and MPLS-capable
 - Better switching architecture





Quickie Updates

- Research Network is available
 - separate virtual network backbone
 - bypasses the campus exit (no firewall or IPS protection at all)
 - Security needs to sign-off on access
 - Typically very small subnets for HPC clusters



Quickie Updates

- ICCN and OmniPop
 - ICCN is mature and very successful
 - Connectivity to CIC OmniPop provides access to many national resources such as Internet2, ESnet, MREN, and more
 - Along with the campus research network, will be a critical part of any participation in GENI





“Horizon” Network Technologies

- IP version 6
- Security Zones (leveraged by VRF)
- Network Admission Control



IPv6

- IP as we know and love it is IP version 4. It uses 32 bit addresses partitionable into network and host space.
- In 1994 the IETF did some extrapolations showing that the IPv4 address space would be exhausted in 10-15 years.
- There is still some space left but it is **HARD** to get.





IPv6

- We may be unable to obtain more IPv4 space beyond our current allocation
- Current available space in campus IP blocks is getting scarce
- Policy changes and increased use of address-saving features such as NAT may start to be necessary



IPv6

- In the early 90's the IETF handled proposals for larger addressing required to handle the growth of the Internet.
 - CATNIP - same header format for IP, CLNP, and IPX with translations between all
 - TUBA - swap out IP for CLNP (ISO) addresses
 - SIPP - redesign of IP with larger IP addresses





IPv6

- IPv6 addresses are 128 bits long, a space of about 3.4×10^{38} (one address per proton on the earth)
- Length leads to strange-looking IP addresses

2620:0:0E00::/48



IPv6

- Campus has been allocated a /48 network block for v6.
- $128 - 48 = 80$ bits of address space at our disposal
- Enough for 16384 subnets of 2^{64} hosts each... probably sufficient!



IPv6

- New core routers and building routers going forward can route IPv6 in hardware
- As soon as practicable, we intend to enable internal backbone routing of v6
- Then we can solicit “early friendly user” VLAN creation



IPv6 deployment

- Initially we will create v6-only subnets
- Too many issues with dual-stack and DNS resolution
- Too many security issues for now (no scalable v6 firewalls or IDS devices, for instance)



Requirements for IPv6

- Allocation of space (done)
- Ability to route on backbone (done)
- Ability to route to Internet (limited)
- Ability to mix v4 and v6 (problematic)
- DNS (in work)
- Firewall, monitoring, security (hard)



IPv6

- Roadblocks:
 - Chicken-and-egg problem
 - Very hard to run dual-stack in a production network
 - All security and monitoring systems need to be redone
 - 6-to-4 and 6-in-4 interoperability is hard to control and debug



Network-based Security

- Problem: different things on the network have very different characteristics regarding security and vulnerability
 - Administrative desktops
 - Labs
 - Research computing clusters
 - Public network jacks



Network-based Security

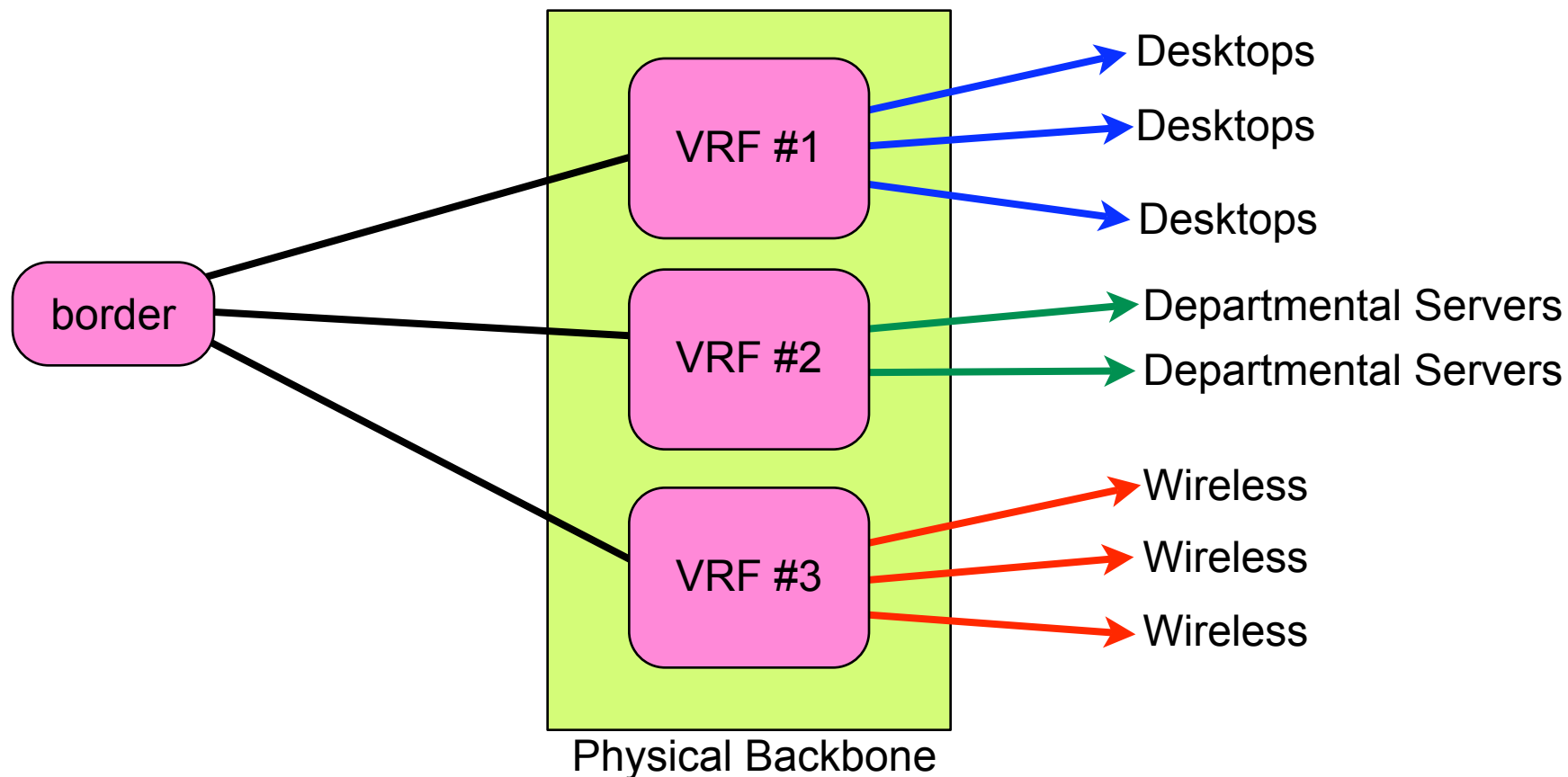
- One solution is a security device (firewall) between every department network and the backbone
- This is a poor solution because the backbone is very fast compared to the speed of (cheap) firewalls
- Does not solve any high-performance network problems



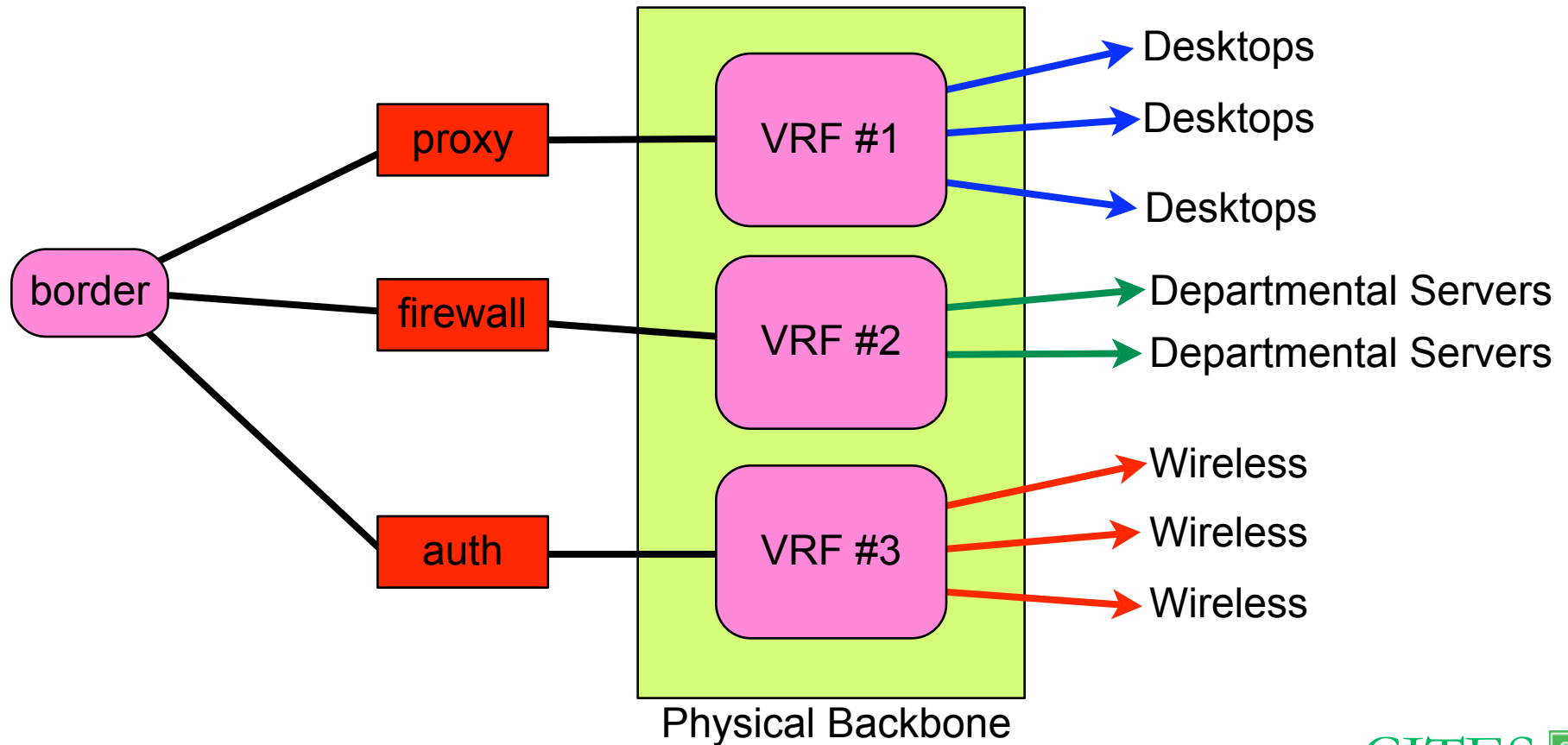
Network-based Security

- Multi-VRF allows us to build multiple parallel networks on the backbone that cannot communicate with one another
- This is the equivalent to VLAN's in an Ethernet switch but applies to IP routing
- We thus have the ability to isolate some building networks from others

Network-based Security



Network-based Security





Network-based Security

- Then define an access matrix that defines both the authentication and access rules between all zones as well as the Internet

to \ from	Desktops	Servers	Wireless	Internet
Desktops	—	no access	no access	no access
Servers	FW controlled	—	FW controlled	FW controlled - certain i/b ports
Wireless	no access	FW controlled	—	no access
Internet	no access - web via proxy only	FW controlled - certain i/b ports	NAT/fully-closed	—





Access Matrix

- “Generic Desktop”
 - Authentication via 802.1x
 - No direct access to Internet
 - Necessary Internet services are via web proxy
 - Some access to other zones



Access Matrix

- “Research Computing Cluster”
 - Authentication by physical jack
 - Direct (no firewall) access to Internet
 - No access to other zones except via campus firewall traversal



Access Matrix

- “Wireless User”
 - Authentication via 802.1x / WPA Enterprise
 - Limited access to Internet (some ports blocked)
 - Full access to campus resources



Network-based Security

- Roadblocks:
 - Gateways may create performance issues
 - Would require a lot of cooperation between CITES and departments
 - Multi-VRF networks for now can only be routed in the main core, not building routers
 - Access matrix may become large and hard to control



Network Admission Control

- Problem
 - Access to network is based on physical access (except in the limited case of wireless)
 - No way to track activity to an individual
 - Compromised devices are dealt with retroactively
 - Security zone membership is fixed by port VLAN assignment



Network Admission Control

- Need a network-wide solution that implements positive authentication
- QuickConnect does this in a limited way
- 802.1x is a standard way to do this already implemented by nearly all our access switches
- Authentication response can also include VLAN membership information



Network Admission Control

- Outside of the switch, external NAC controllers can trigger probes to a “software dongle” on a machine which can do a virus scan, report OS type and version, etc
- NAC controller can then participate in the VLAN assignment decision



Network Admission Control

- Goals:
 - positively identify all users of the network
 - such identification should be automatic (hopefully leveraging Kerberos or AD)
 - use identification to place machine in the proper security zone
 - allow for easy “guest access”
 - identify and quarantine infected/unsafe machines



NAC Requirements

- Leverage 802.1x (already present in network switches)
- Authenticate against Kerberos (or AD)
- Allow for unauthenticated devices
- Programmed control of VLAN membership
- Device health scan via software dongle
- Interoperable with existing equipment



Network Admission Control

- Roadblocks:
 - Need a way to deal with non-authenticating devices like printers and Xboxes
 - Solutions tend to be dependent on OS platform
 - Windows AD authentication tends to be very “hand in glove”
 - .1x setup on some platforms isn’t easy and presents an extra step for the user



Where are we now with IPv6?

- New procurements are all v6-ready, need a couple of bugfixes on core equipment
- Have address space assigned
- Working with providers for native IPv6 route exchange when possible
- Some limited test deployments soon BUT...
- Need many security solutions before full rollout is possible



Where are we now with Zones/ VRF?

- Limited deployment to implement things like the research network and public wireless
- Needs extensive design, architecture, and use case analysis before deployment



Where are we now with NAC?

- 802.1x already in use on Ulpwa2 wireless
- Most access switches are .1x capable
- Authentication system (RADIUS) already deployed
- Exploring third-party appliance solutions for VLAN assignment and host scan portions - hope to evaluate early next year



Questions and Discussion