L3VPN at UCAR

John Hernandez
NCAB 10/15/14
What is L3VPN?

• A collection of subnets that share a virtual routing domain, or “VRF”
• Provides separation from standard UCAR nets in the router’s “Global Table”
How does it work?

• We use Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP)
• An “MPLS label” is prepended to the IP packet to indicate the VRF (eg, red or green)
• This is reasonably scalable – we can support dozens of VRFs
How can we use it?

• Building isolated networks
  – IPMI, security, building automation
  – Backend storage, replication
  – Can use a “bastion host” to gain access

• Enterprise security zones
  – Guest networks can be routed to central IPS
  – Desktop networks can be routed to central firewalls
Production Examples

- CISTL zStax deployment leverages L3VPN to provide replication between ML and NWSC
  - zStax design prescribes isolated interfaces

- FRGP uses L3VPN to provide separation between Research (I2, etc) and Commodity Internet.
  - Participants connect to both VRFs and control traffic.
Zstax Replication via L3VPN on MPLS

QFX3500 ml-mr-j1-es replaces 6509 ml-mr-c6 during spring power-down

At ML, ZStax L3VPN router is 192.168.12.15/28 on vlan 420
(But existing vlan 64 could be used for testing)

At NWSC, ZStax L3VPN
router is 192.168.12.31/28 on vlan 1420
(but existing vlan 177 could be used for testing)