

Choosing Switches and Routers for the Campus

Campus Network Design & Operations Workshop



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (<http://creativecommons.org/licenses/by-nc/4.0/>)



UNIVERSITY OF OREGON

Last updated 6th December 2020



Choices!

- Minimum requirements for L2 devices
 - Edge Switch
 - Distribution Switch
 - Campus Core Router
 - Campus Border Router
-
- In all cases examples of mainstream vendor models are given to *guide* campus network administrators



Selecting Switches



UNIVERSITY OF OREGON



Selecting Switches

- Minimum features:
 - Standards compliance
 - Encrypted management (SSH/HTTPS)
 - VLAN trunking
 - Spanning Tree (RSTP at least)
 - SNMP
 - At least v2 (v3 has better security)
 - Traps
 - Remote management and configuration backup
 - CLI preferred, also serial console desirable



Selecting Switches

- Other recommended features:
 - DHCP Snooping
 - Prevent end-users from running a rogue DHCP server
 - Happens a lot with little wireless routers (Netgear, Linksys, etc) plugged in backwards
 - Uplink ports towards the legitimate DHCP server are defined as “trusted”. If DHCPOFFERS are seen coming from any untrusted port, they are dropped.
 - RA Guard
 - Prevent end-users from sending IPv6 Router Advertisements
 - Happens a lot with older Windows devices with IPv6 enabled, building automatic tunnels, and then announcing themselves as routers to the LAN



Selecting Switches

- Other recommended features:
 - Dynamic ARP inspection
 - A malicious host can perform a man-in-the-middle attack by sending gratuitous ARP responses, or responding to requests with bogus information
 - Switches can look inside ARP packets and discard gratuitous and invalid ARP packets.



Selecting Switches

- Other recommended features:
 - IGMP Snooping:
 - Switches normally flood multicast frames out every port
 - Snooping on IGMP traffic, the switch can learn which stations are members of a multicast group, thus forwarding multicast frames only out necessary ports
 - Very important when users run Norton Ghost, for example.



Selecting Edge Switches

- In addition to the previous general features:
 - L2 device only – connecting end users!
 - 24 or 48 10/100/1000 copper ports
 - Opt for some Power over Ethernet (POE) ports if requirement to connect wireless access points and/or IP phones
 - Two 1Gbps/10Gbps uplink ports (copper or fibre)
- Only connects to the building distribution switch
 - Copper at 1Gbps may well be enough
 - Fibre installation allows future growth to 10Gbps from edge to distribution by swapping SFP for SFP+



Example Low Cost Edge Switch

- Netgear “Smart Managed Pro” switches¹
 - GS748 and GS752 have 48 10/100/1000 ports
 - PoE options if desired (TP and TPP)
 - 4x 1Gbps SFP
 - 24 port versions also available
 - GS110TP has 8 10/100/1000 ports
 - All PoE, plus 2x 1Gbps SFP
 - Full SNMP, management access (HTTP and telnet²)
 - 802.1x, DHCP snooping, Dynamic ARP inspection
 - Shallow form factor – good for wall mount cabinets

¹ Avoid “Smart Managed Plus” – those are web-only, no SNMP

² But no HTTPS, SSH or serial console. More expensive M4100 has these.



Example Low Cost Edge Switch

- Dell EMC Switch N1524 & N1548
 - 24 port and 48 port respectively (10/100/1000)
 - 4x 10Gbps SFP+ uplink
 - N1524P and N1548P have PoE
 - CLI (Cisco like) and GUI, serial console port
 - SSH and HTTPS access
 - DHCP snooping, Dynamic ARP inspection, etc



Example Edge Switch

- Cisco Catalyst 2960X or Catalyst 9200 (newer)
 - 24 or 48 10/100/1000 ports
 - PoE options if desired
 - Uplink options
 - 4x 1Gbps SFP or 2x 10Gbps SFP+
 - Catalyst 9200 also offers modular uplink ports with 25Gbps and 40Gbps ethernet
 - Stackable (up to 8 units)



Selecting Distribution Switches

- In addition to the previous general features:
 - L2 device only – connecting edge switches!
 - 12 or 24 copper or fibre 1Gbps ports
 - 1 or 2 10Gbps fibre uplink ports
- Aggregates edge switches towards the core
 - May also connect end users
 - Copper ports for edge aggregation
 - Fibre ports for uplink



Example Distribution Switches

- Cisco Catalyst 2960X or Catalyst 9200
 - 24 10/100/1000 ports
 - Uplink with 2x 10Gbps SFP+ (2960X) or 4x 10Gbps SFP+ (9200)
- Cisco Catalyst 9300 (fibre)
 - 24 SFP fibre ports (C9300-24S)
 - 48 SFP fibre ports (C9300-48S)
 - Uplink modules include 4x 1G, 8x 10G, 2x 40G



Summary

- Edge Switch
 - Focus on access ports
 - Fibre to building distribution, or is copper enough?
 - Do NOT need any L3 capability
- Distribution Switch
 - Fibre ports to connect Edge Switches
 - 10Gbps fibre link to Campus Core Router
 - Do NOT need any L3 capability



Choosing a Core Router



UNIVERSITY OF OREGON



Core router: essential features

- Lots of fiber ports
 - SFP (1G) or SFP+ (10G)
- Robust, line-rate routing (layer 3 forwarding)
 - IPv4 and IPv6, static routes
- Sufficient ARP (IPv4) and NDP (IPv6) entries
- DHCP relay (DHCP helper)
- Management: SSH, SNMPv2/v3
- OSPF (v2 and v3) or IS-IS

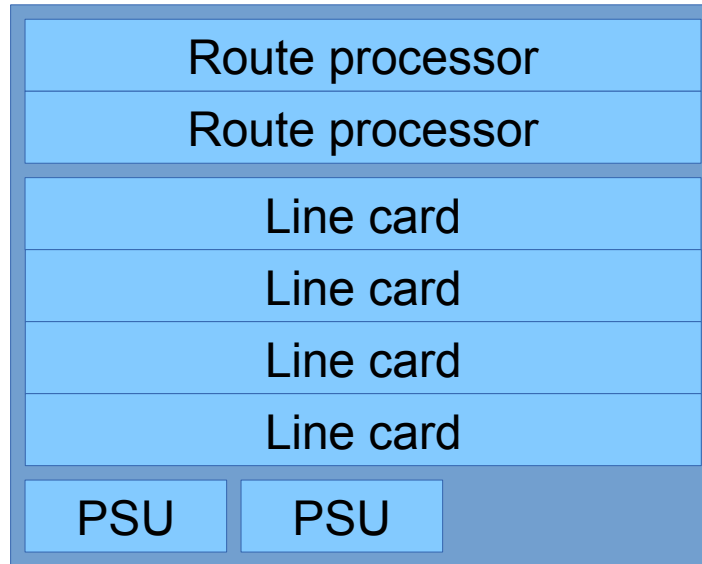


Core router: optional features

- HSRP/VRRP
- Mirror/span port
- Hardware redundancy (e.g. dual PSU)
 - But would you be better buying a whole second device?



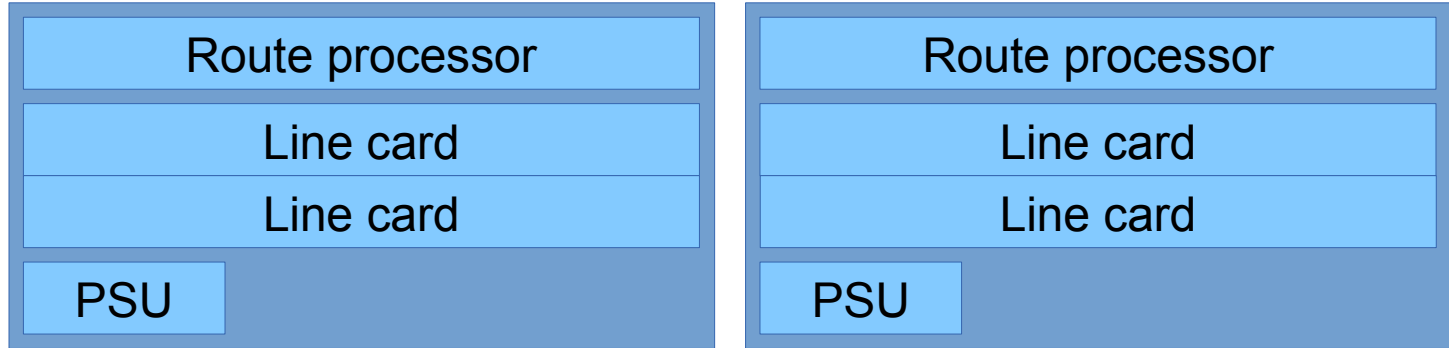
One super-redundant device



- Chassis failures are not unknown ■■
- What would you do if that happened?



Two less-redundant devices



- Running “live-live” so everything is tested
- In emergency, can move key users to other side
- Key buildings can be dual-homed
 - This is where OSPF and HSRP/VRRP come in



Don't spend too much!

- Many “edge” L3 switches make fine campus core routers
- You won't be carrying a full routing table
 - So a limit of say 16K routes isn't a problem
 - Check how many IP interfaces/VLANs it supports
- Whatever you buy today will be obsolete in 3-5 years anyway
- If it's cheap you can afford two



Cisco Nexus C36180YC

- 48 SFP/SFP+ ports
 - Each port supports 1G/10G/25G ethernet
- 6x 40G/100G uplink ports
 - Will also operate as 4x25G or 4x10G with breakout cable
- Runs NX-OS
 - Very IOS like, but not the same
 - LAN Enterprise license needed for L3 routing protocols



Cisco Catalyst 9500-48Y4C

- 48 SFP/SFP+ ports
 - Each port supports 1G/10G/25G ethernet
- 4x 40G/100G uplink ports
 - Check transceiver/DAC/AOC support
- Needs “Network Advantage” license for BGP/OSPF/IS-IS
 - Beware: Cisco 3/5/7-year license for “DNA Advantage” for L3 feature set



Juniper EX4650

- 48 SFP/SFP+ ports
 - Each port supports 1G/10G/25G ethernet
- 8x 40G/100G uplink ports
 - Will also operate as 4x25G or 4x10G with breakout cable
- Premium Feature License needed for BGP and IS-IS support
 - Base Feature license has OSPF and RIPv2



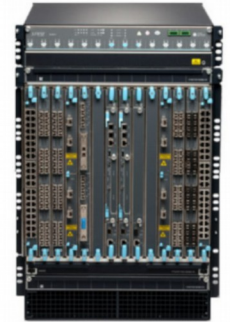
Juniper QFX5120-48Y

- 48 SFP/SFP+ ports
 - Each port supports 1G/10G/25G ethernet
- 8x 40G/100G uplink ports
 - Will also operate as 4x25G or 4x10G with breakout cable
- Advanced 1 Feature License needed for OSPF/IS-IS/BGP support
 - Beware: 3/5-year license for Software Feature Licenses



Not big enough?!

- Above this you are looking at chassis switches
- Examples:
 - Cisco Catalyst 9600, Nexus 9000
 - Juniper EX9204/08/14, QFX10000



UNIVERSITY OF OREGON

– But do you need anything this big and power hungry??



Maybe you already have one!

- Check the features of your existing devices
 - And check on forums for experiences of people using the same device for routing
- May need to enable it: “ip routing” or similar
- May need to update to latest stable firmware
- Test with a spare device if you have one



Choosing a Border Router



UNIVERSITY OF OREGON



Border router: essential features

- Robust, line-rate routing (layer 3 forwarding)
 - IPv4 and IPv6, static routes
- Strong CPU, Large Memory
- Management: SSH, SNMP, netflow/jflow/sflow/IPFIX
- OSPF (v2 and v3) or IS-IS
- NAT (if using internal private IPv4 address space)
- Hardware redundancy (e.g. dual PSU)
 - but would you be better buying a whole second device?



Border router: optional features

- If Multihoming:
 - Full support for BGP
 - Ability to carry full BGP table (if needed)
 - Support of all BGP Attributes, implementing BGP policies



Sizing a Border Router

- Consider connection to upstream provider
 - Allow for headroom far greater than link capacity
 - Bandwidth upgrades needed
 - Traffic growths larger than expectation
 - Dealing with Denial-of-Service Attacks from outside
- Physical chassis size is irrelevant
 - Smaller the better, reduced power and space requirements
- Border router needs:
 - Internal interface (to network core)
 - External interface(s) (to upstream provider(s))
 - 1 Rack Unit is usually enough



Typical Low Cost Example

- MikroTik CCR1036-8G-2S+
 - 8 Gigabit Ethernet ports (copper)
 - 2 SFP/SFP+ ports
 - Real world throughput well in excess of 1Gbps
 - BGP only runs on one core – not suitable for full BGP table
 - IPv6 implementation not complete



Typical Examples

- Cisco ASR1001-X

- 1 RU chassis
- 2x10GE and 6x1GE interfaces
- 2.5Gbps throughput default
- License activates 10GE ports allowing up to 20Gbps



- Juniper MX150

- 1 RU chassis
- Throughput up to 40Gbps
- 8 10/100/1000 copper ports, 2 100/1000 SFP ports, and 2 SFP+ ports



Typical Examples: High End

- Juniper MX204
 - Popular high-end border router
 - 4 built-in 100GE and 8 10GE interfaces
 - Throughput up to 400Gbps



- Cisco ASR 9001
 - 4 built-in 10GE interfaces & 4 100GE interfaces
 - Throughput up to 240Gbps
 - Slow control plane



Summary

- Core Router
 - Focus on scalability, sufficient CPU to ensure current and immediate future needs
 - Router or “L3 Switch” is often appropriate, as routing needs in the Core are not onerous
- Border Router
 - Physical size unimportant → small!
 - Needs v few interfaces
 - Needs big CPU to handle border functions
 - Consider future BGP needs



Questions?



UNIVERSITY OF OREGON

