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/)
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
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 DHCP OFFERs 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 2960L and 2960X
  - 24 or 48 10/100/1000 ports
    - PoE options if desired
  - Uplink options
    - 4x 1Gbps SFP (2960L-48TS-LL and 2960X-48TS-L)
    - 2x 10Gbps SFP+ (2960X-48TD-L)
  - Stackable (2960X only, 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 2960X**
  - 24 10/100/1000 ports
  - Uplink with 2x 10Gbps SFP+ (2960X-24TD-L)

- **Cisco 3850 (copper)**
  - 24 10/100/1000 ports (3850-24T)
  - Uplink module with 2x 10Gbps SFP+

- **Cisco 3850 (fibre)**
  - 12 SFP fibre ports (3850-12S)
  - 24 SFP fibre ports (3850-24S)
  - Uplink module with 2x 10Gbps SFP+
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
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 C3850-{12,24,48}XS

• 12 or 24 or 48 SFP/SFP+ ports
  – Plus 2-4 optional uplinks ("service module")
  – IP Base image is sufficient for OSPF and IPv6 support
• 12 and 24 port versions are stackable (up to 9 units)
Cisco C4500-X

- 16 or 32 SFP+ ports (1G/10G)
  - Plus optional 8-port 10GE expansion module
- IPv4/IPv6 with IP Base license
  - Enterprise license gives you BGP
- Can stack two, using 10GE ports (“VSS”)
Cisco Nexus 3548-X

• 48 SFP+ ports (1G/10G)
  – Can also run at 100Mbps
• Runs NX-OS
  – Very IOS like, but not the same
• Replaces the Nexus 3064
  – (which also had 4x 40GE ports)
Juniper EX4200-24F

- 24 SFP ports
- Optional 2x10G modules
- Stackable (up to 10)

"Advanced Feature" license not required - only for IS-IS, BGP and MPLS
Juniper EX4500

• 40 SFP+ ports (1G/10G)
• Optional uplink modules

Beware limit of only 1,000 IPv6 NDP entries in hardware; use with L3 distribution switches?
Not big enough?!

• Above this you are looking at chassis switches
• Examples:
  – Cisco 4500E, Nexus 7000
  – Juniper EX8208, EX8216

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
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 7301 or Cisco 7201
  – Now no longer supported by Cisco, but excellent 1RU router with 3 and 4GE interfaces respectively
  – 7301 good for links up to 300Mbps (real world)
  – 7201 good for links up to 600Mbps (real world)

• Not really equivalent, but:
  – Cisco 4451 (2 RU), 4431 (1 RU) & 3945 (4 RU)
  – All offer performance similar to 7201 and 7301
Typical Examples

• Cisco ASR 1000 Series
  – “replaces” Cisco 7201
• Popular choices:
  – ASR1001X (1RU) is popular border router
    • 2x10GE and 6x1GE interfaces
    • 2.5Gbps throughput default
    • License activates 10GE ports allowing up to 20Gbps
  – ASR1002X (2RU)
    • 6x1GE interfaces
    • 5Gbps throughput default
    • License activated throughputs up to 36Gbps
Typical Examples

• Juniper MX5 to MX80
  – One common chassis (2RU)
  – Model upgradable by licence
  – Throughputs from 20Gbps to 80Gbps, but very slow control plane
  – 4x 10GE interfaces (activated on MX40 & MX80)
  – Two expansion slots

• Juniper MX150
  – 1 RU chassis
  – Throughput of 40Gbps
  – 8 10/100/1000 T ports, 2 100/1000 SFP ports, and 2 SFP+ ports
Typical Examples: High End

• Cisco ASR 9001
  – 4 built-in 10GE SFP+ interfaces, with support for 10GE and 40GE modules (2RU chassis)
  – Throughput of 120Gbps

• Juniper MX204
  – 4 built-in 100GE and 8 10GE interfaces
  – Throughput of 800Gbps
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?