Research & Education Network Ecosystem

- **Research & Education Network = REN**
  - NREN = National REN

- **Characteristics:**
  - High bandwidths: 10Gbps is typical, 40G and 100G rolling out
  - Research needs uncongested networks
    - RENs are lightly used, with lots of capacity (headroom)
  - Low latency (terrestrial fibre)
  - Open Networks with **NO** filtering

- **Hierarchical model**
Research & Education Network Ecosystem

• NREN Service Models
  – Peering network
    • Connects campuses together
    • Provides connectivity to international R&E
    • Peers at local IXPs
    • Implications: Campuses also need connectivity from ISP
  – REN provides all Internet connectivity
    • REN is the ISP for the campuses
    • Implications: Simplest for campuses – only one connection to manage
Research & Education Network Ecosystem

• Campus is the foundation of successful R&E network
• But, many:
  – Do not have any structure
  – Make heavy use of NAT and Firewalls limiting performance
  – Are built using unmanaged equipment
  – Are forced do dual home, without skills to manage this
  – Are built using outdated fibre and copper that cannot support high speeds
Campus Design Principles

• Simple design rules:
  – Minimise number of network devices in the path
  – Use hub & spoke (star topology), not daisy chains
  – Segment the network with routers in the core
  – Services at the core, not the edge
  – Always buy managed devices
  – Think very carefully about positioning of firewalls and NAT
    • Firewalls are for protecting servers and the services they host
    • Treat public campus network as untrustworthy as the Internet
Campus Cabling Best Practices

• Two types of cabling:
  – Unshielded twisted pair (UTP): for use inside racks and inside buildings
  – Fibre optic cabling: provides service between buildings and between network racks

• UTP
  – Cat5e – supports up to 1Gbps ethernet to 100metres
  – Cat6 – similar to Cat5e but costs more
  – Cat6a – 4x cost of Cat5e, for supporting 10Gbps over copper – not required for desktop yet

• Fibre Optics:
  – Multi-mode: outdated; expensive; short range; only found in equipment racks now
  – Single-mode: inexpensive; distances up to 80km; speeds over 100Gbps
Switching Architectures: Spanning Tree

• Switching Loops:
  – Unprotected means network traffic swamps network leading to outage
  – Good loops provide backup in case of link or device failure

• Spanning Tree Protocol
  – Runs on all switching devices
  – Calculates optimum path through a network between all L2 devices
  – STP, RSTP, MST flavours – RSTP recommended on all L2 devices
  – Careful selection of Bridge Priorities required
    • Root of the tree needs to be the core switch etc
Switching Architectures: VLANs

• Maximum number of devices on any one L2 broadcast domain should be kept under 100

• Beyond that, introduce virtual LANs
  – Allows one switch to support several different broadcast domains (LANs)
  – Allows the campus network to scale

• Best Practice Design:
  – One or several VLANs per building
  – Do NOT span VLANs across buildings
  – Never use VLAN 1
  – Route between VLANs in the core
Switching Architectures: Advanced L2

- **Link Aggregation**
  - Bundling more than one link between switches
  - Increasing bandwidth between two devices
  - Standard: LACP (Link Aggregation Control Protocol)

- **LLDP or CDP**
  - Link Layer Discovery Protocol / Cisco Discovery Protocol
  - Allows admin to discover other devices on the campus backbone

- **BPDU Guard**
  - Blocks Bridge PDUs on interfaces where not expected
Routing & Forwarding

• Routers
  – L3 devices, routing packets between broadcast domains

• Routing
  – Building tables of destinations based on information shared between routers by routing protocols

• Forwarding
  – Moving packets between interfaces based on information from the routing table

• Routing Protocols:
  – Static
  – Dynamic: OSPF, IS-IS, BGP
L3 Switches

• Contradiction:
  – L2 = switch
  – L3 = router
  – L3 Switch??

• An ethernet switch with some routing capability

• Core of the Campus needs to be a L3 Switch
  – Switch with many interfaces, but able to route at wire-speed between all the VLANs terminating on it
  – And host connection to campus services and link to campus border router
Migrating from Flat to Routed

- Many campuses are one huge flat network
  - Doesn’t work, doesn’t scale
- Migrate to VLANs + core router
  - Star network, not daisy-chain

Best practices:
- Design a migration plan! With rollbacks
- Design an address plan (IPv4 & IPv6)
- Deploy new VLAN scheme in one building first
  - Core → Distribution → Edge
- Test connectivity at each stage
- Migrate users, turn off VLAN 1, and move to next Building
Selecting Campus Devices

• **Edge Switch**
  – L2 only! (No L3 needed)
  – VLANs, RSTP, Encrypted Management, DHCP Snooping, RA Guard
  – Managed! (CLI, serial console, at least SNMPv2)
  – 24 or 48 10/100/1000 ports, fibre uplinks (1Gbps, 10Gbps better)

• **Distribution Switch**
  – Same basic specification as Edge switch
  – 12 or 24 copper or fibre ports, 10Gbps fibre uplink
Selecting Campus Devices

• Core Router
  – L3 Switch – Lots of fibre ports (1G/10G)
  – Robust line rate forwarding at L3
  – Sufficient ARP (IPv4) and NDP (IPv6) entries
  – DHCP relay/helper, full management (SSH, SNMPv2/3)
  – OSPF (v2 & v3), HSRP, Mirror/Span port
  – 2x Small form factor (1RU 48 port) rather than one “redundant” chassis

• Border Router
  – Robust line rate forwarding at L3
  – IPv4/6, OSPF (v2 & v3), BGP, NAT, full management (SSH, SNMPv2/3)
  – Small form factor (few ports needed) rather than one “redundant” chassis
Wireless on Campus

• Two wireless frequency ranges:
  – 2.4GHz – 802.11b/g/n
    • Provides only 4 non-overlapping channels (1, 6, 11, 14)
  – 5 GHz – 802.11a/n/ac
    • Provides 25 non-overlapping channels

• Design:
  – Not all Access Points are created equal – cheap AP → small CPU → few users
  – Avoid channel overlaps, pay attention to physical obstacles
  – Estimate number and type of users per AP
  – 802.11ac means 1Gbps access to the AP
  – Bring Your Own Device is standard today: 2-4 devices per person!
Wireless on Campus

• SSID:
  – “Wireless name”, the network users join
  – SSID planning: names matter, trade-off for roaming
  – Avoid tempting names
  – Users prefer seamless roaming
    • Where? Within a building? Across the whole campus?

• Authentication:
  – MAC address: easily defeated
  – Pre-Share Key: who knows the password? Fine for temporary setups only.
  – Captive Portal: better than PSK
  – 802.1x: WPA2-AES is the global standard, allows for EduRoam too
Dynamic Routing: OSPF

• OSPF:
  – Dynamic Routing protocol using SPF algorithm (same as used for Spanning Tree)
  – IETF standard, must be implemented on all L3 devices (routers)

• Essential next step beyond static routes
  – Small campus would have static default on core to border, and static routes from border to core for VLANs
  – Larger campuses deploy OSPF for scalability and to allow redundancy in the core
NAT

- Was developed to allow entities with non-routable address space to connect to global Internet
  - Now used to prolong IPv4

- Network Address and Port Translation, translates multiple IP addresses into one other IP address
  - TCP/UDP port distinguishes flows

- NAT Best Practices:
  - Deploy IPv6 – offloads majority of content traffic from NAT
  - As close to campus border → on border router!
  - Minimise translation time outs to allow efficient use of public address pool
  - Use different public address pools for different campus user categories
Campus Operations Best Practices

• DNS:
  – Local on-campus resolver, sub-millisecond RTT for cached DNS lookups
  – User experience: webpages load quickly
  – unbound software is simple to install and operate

• DHCP:
  – Without an address, nothing can get a connection
  – Make sure address pools are large enough, and lease times appropriate (short for wireless, longer for fixed ethernet)

• NTP:
  – Without time synchronisation across network devices, authentication protocols and DNS may fail, and security incidents hard to trace across devices
Campus Operations Best Practices

• Many other recommendations!

• Examples:
  – Implement anti-spoofing filters on all access ports (core router interfaces facing users)
  – NAT must only translate addresses used internally for campus
  – Block TCP/25 (SMTP) out bound apart from authorised email relays
  – Rate limit UDP rather than blocking it
    • Bittorrent will just move to TCP if UDP is blocked
  – Deploy IPv6
    • Reduces load on campus NAT device
    • Avoids situation where Bittorrent and other clients tunnel using IPv6
Campus Security Overview

• **Security is Hard – it is NOT a one box solution**
• Campus networks need to be open
• There will always be people being bad
• **Security is a Process:**
  – Assessment of what’s at risk
  – Protection: efforts to mitigate that risk
  – Detection of intrusions
  – Response
  – Repeat!
Campus Security Overview

• Policy Framework: Acceptable Use Policy
  – Without an AUP there is nothing a Campus Admin can do to enforce a security policy

• Network Management
  – MUST have managed equipment in the network
  – MUST run network monitoring tools (LibreNMS, NfSen, smokeping etc)

• Encryption
  – Disable clear text password protocols – deploy letsencrypt for mail servers and websites – no self-signed certs!

• Virus Protection
  – Viruses arrive by email or clickable links (all encrypted)
  – Firewall is useless for this, yet we still deploy firewalls to stop them!

• Authentication
  – Who is using our network? Each user must have account (LDAP or AD)
Campus Security Overview

• Wireless:
  – Who may install APs?
  – 802.1x authentication against central database

• Blocking Traffic:
  – Default needs to be to allow traffic, not block it
  – Block vulnerabilities – border router with simple filters can do this
  – Monitoring system needs to be in place tracking unusual trends
  – Blocking outbound ports seriously inconveniences visitors
  – Remember, Universities are designed to attract clever people, they will work around port blocking
Campus Security Overview

• Bandwidth Shaping
  – Per user? Per department? Some users have legitimate needs to move large datasets around → AUP to the rescue.

• Deep Packet Inspection
  – Won’t work for encrypted traffic. What’s the difference between encrypted humorous cat video and encrypted veterinary medicine video?
  – In-line controls are very expensive and are a serious bottle-neck

• Performance
  – Today’s 100Mbps campus backbone will become tomorrow’s 1Gbps campus backbone, and then on to 10Gbps. Which Firewall/DPI box??
Campus Security Overview

• Conclusion:
  – Firewalls are useless
  – Bandwidth shaping is useless
  – DPI is useless

• Solution:
  – Scalable campus design
  – Security policy including an AUP at its core
  – Monitoring! Monitoring!
  – Firewalls belong in front of servers in campus core
Network Monitoring & Management

• What & Why We Monitor
• Baseline Performance & Attack Detection
• Network Attack Detection
• What & Why We Manage
• Network Monitoring & Management Tools – large number of open source tools
• The NOC: Consolidating Systems – not necessarily a place, but an organizational concept
## Network Monitoring & Management

**Examples of monitoring & management systems for a Campus**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RT</td>
<td>Request Tracker – ticketing system for tracking requests</td>
</tr>
<tr>
<td>RANCID</td>
<td>Device configuration tracking &amp; management</td>
</tr>
<tr>
<td>LibreNMS</td>
<td>Monitoring device health, traffic and interface loads</td>
</tr>
<tr>
<td>NfSen</td>
<td>NetFlow/IPFIX traffic flows crossing border router/NAT</td>
</tr>
<tr>
<td>Smokeping</td>
<td>Monitoring connection health, RTT, response time, jitter within campus and to the REN/ISP</td>
</tr>
<tr>
<td>Nagios</td>
<td>Device availability</td>
</tr>
</tbody>
</table>
Questions?

This document is a result of work by the Network Startup Resource Center (NSRC at https://www.nsrc.org). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.