Campus Network as a Service (CNaaS) in Norway - where are we now?

Vidar Faltinsen, director of department, UNINETT

GÉANT workshop on network management and monitoring
Copenhagen, October 21 2019
NREN in Norway
Owned by the Ministry of Education and Research
90 employees
140 customers
300,000 users
Norwegian CNaaS

Service development and pilot in 2019
Operational from 2020

Extending the research network to the researcher, student and lecturer
Why such a service?

- ICT departments are overloaded with tasks
  - little time to focus on network
- ICT departments are vulnerable
  - only one person on network in many cases
- Trend to outsource “bread and butter”
  - In order to strengthen focus on supporting ICT for research and IT for education
- Improve security
- Improve overall quality
  - Improvements for ICT for research and education etc
New digitalization strategy from the Ministry of Education

- 2017 - 2021
- Drive for common ICT services in the HE sector when there is a clear benefit
The CNaaS service package

Included

- Operations of wired and wireless network
- DHCP service
- NAT 44 service
- Radius (for eduroam)
- VPN (eduVPN)
- 24/7 monitoring of critical components (daytime monitoring for the rest)

Will / can offer

- Firewall management
- DNS firewall
- IDS
Number of customers

- 2019: One (pilot)
- 2020: at least two new (moderate ambition)
- 2021 -!: sky is the limit 😊
Organizational setup

- Dedicated department in Uninett for campus network
- We are recruiting more network engineers
- Total MY for CNaaS in 2020 will be 2.7 (service will have a deficit first years)
- Close collaboration with research network department
- Will use our NOC for operations
- Collaboration with Sunet important (next slide)
Joint Swedish and Norwegian high level CNaaS NMS architecture

Customer A

- Customer and Asset Database
- CNaaS-NMS (2nd and 3rd line config)
- NAV (monitor)
- NAV 1st line config
- Campus network
- oxidized (tracking changes)

Connections:
- Uninett to NAV (monitor)
- SUNET to NAV (monitor)
- Uninett to Campus network
- SUNET to Campus network
- Customer and Asset Database to NAV 1st line config
- Customer and Asset Database to NAV (monitor)
- NAV (monitor) to NAV 1st line config
- NAV (monitor) to Campus network
- NAV 1st line config to Campus network

Protocols:
- SNMP read
- Netconf
Formal relation

We set up a contract that defines:

• Services that is included (and what is not included)
• Obligations for the customer
• Service and support level (SLA)
• Ownership of equipment (Uninett owns, maintains and reinvests)
• Price (fixed annual cost)
Lessons learned so far

- Close interaction with customer is key
  - Technical staff at customer need to work WITH us
  - SLA/mutual expectations - both Uninett and customer
  - Clear demarcation line - who is responsible for what
  - Day to day low level changes must be done by the customer
    - access switch port config
    - firewall detailed rules (need better tools)

- CNaaS reference architecture can influence/change campus design for all campuses

- Automation is a continuous improvement process.
  - Focus on the most repetitive processes first
  - 100% automation too expensive (?)
Extra material follows...
From help-with-self-help to help-with-everything

GigaCampus 2009  CNaaS 2019
CNaaS high level objectives

- No vendor lock-in
- High availability (=> fully redundant design)
- Flexible traffic engineering (routing in underlay beats SPT any day - also easier to debug)
- Focus on security - must be implemented through a set of initiatives
- Users & devices should be able to connect from anywhere on campus
Overlay/underlay architecture with EVPN and VXLAN

- ISIS routing in underlay
- MP-BGP routes mac addresses
- VXLAN encapsulation
- dot1X and MAB authentication
- Map VXLAN to Vlans for access layer
- VXLAN all the way to expensive
How can we make security management scalable?

- NOC cannot do all change requests
- Local staff cannot be given all privileges
- ACL text editor management - RIP
- Are there any good tools out there?

*tufin*  ???  *algosec*  ???
### Why must wired and wifi be well integrated?

<table>
<thead>
<tr>
<th>User experience</th>
</tr>
</thead>
</table>
| - User expect same functionality and same level of security  
- Multicast, Bonjour, mDNS (BUM) |

<table>
<thead>
<tr>
<th>Wired and wifi must play well together</th>
</tr>
</thead>
</table>
| - Lab microscope on wire where wireless iPad is used as monitor  
- Apple-TV/Chromecast/Miracast on cable and users on wifi  
- Hearing aid devices on wired and user on wifi  
- Screen sharing equipment for visually impaired in lecture hall - user on wifi |

<table>
<thead>
<tr>
<th>Same management, monitoring and security</th>
</tr>
</thead>
</table>
| - Not so vulnerable  
- Better overview  
- Easier to spread knowledge among network admins |

<table>
<thead>
<tr>
<th>Simpler overall network topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Fault monitoring the same for wired and wireless</td>
</tr>
</tbody>
</table>
Thanks for your attention

www.uninett.no