



SUNET

Campusnät som tjänst

Mikael Ottosson

Vem är jag?

- Mikael Ottosson, 25+ år
- Från Leksand
- KTH
- Tidigare i ISP-världen
- Jobbat på SUNET/NORDUnet i 10+ år
- Tjänsteförvaltare för SUNETs Campusnätstjänst



Vad är Campusnät?

- Redundant campusnätverk
- Trådat nät (även till off-campus “satellitkontor”)
- Wi-Fi
- RADIUS
- Brandvägg
- Manageringsverktyg (NMS och NAC)
- System för övervakning, loghantering och dokumentation

Vad är Campusnät?

- Men framför allt är Campusnät ett samarbete mellan de lokala lärosätena och SUNET

Varför Campusnät?

- Standardiserat, testade på flertalet campus
- Hög säkerhet
- Tydlig prisbild
- Stabil men flexibel design
- Ingen “vendor lock-in”
- Fortbildning av lokal personal
- Samtliga förbättringar delas med alla kunder
- Övervakning och felavhjälpning 24/7/365 av SUNET NOC
- Redo att kopplas in direkt på nya SUNET-nätet

Inköpscentralen

- För att vara med i Campusnät är steg 1 att man går med i inköpscentralen
- Alla anslutna organisationer har rätt att avropa från avtalen
- Anlitande sker på initiativ från respektive organisation
- Ej tvingande för framtida köp!
- Fritt fram att gå med (och gå ur om man så vill)

Mer info: <https://wiki.sunet.se/display/InkopC>

Kostnad

- För att dela på kostnaderna så är månadsavgiften volymbaserad:
- 27 000kr + 0.833% av hårdvaruinköpet/månad
- Maxgräns på 1 000 000kr/år oavsett storlek.
Inga extrakostnader för serverinfrastruktur, förstudie, arkitekturdesign, inköpsstöd, supporteskaleringar, implementation eller livscykelhantering. Större implementeringsprojekt än normalt skapas efter överskommelse. Exempelvis 150 000kr som engångskostnad

Design

Wi-Fi

**Dokumentation
och loggar**

CNaaS-NMS

Campusnät

Övervakning

**NAC
RADIUS och 802.1X**

Brandvägg

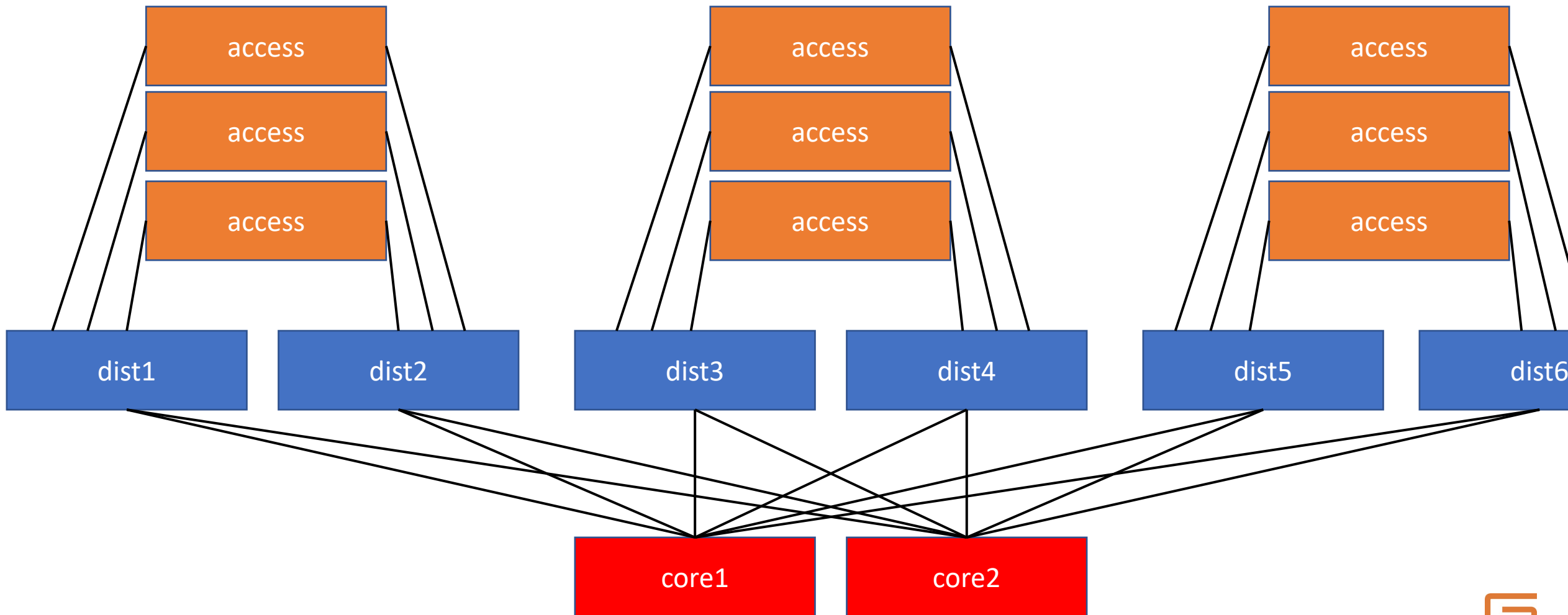
Vägen framåt

Design

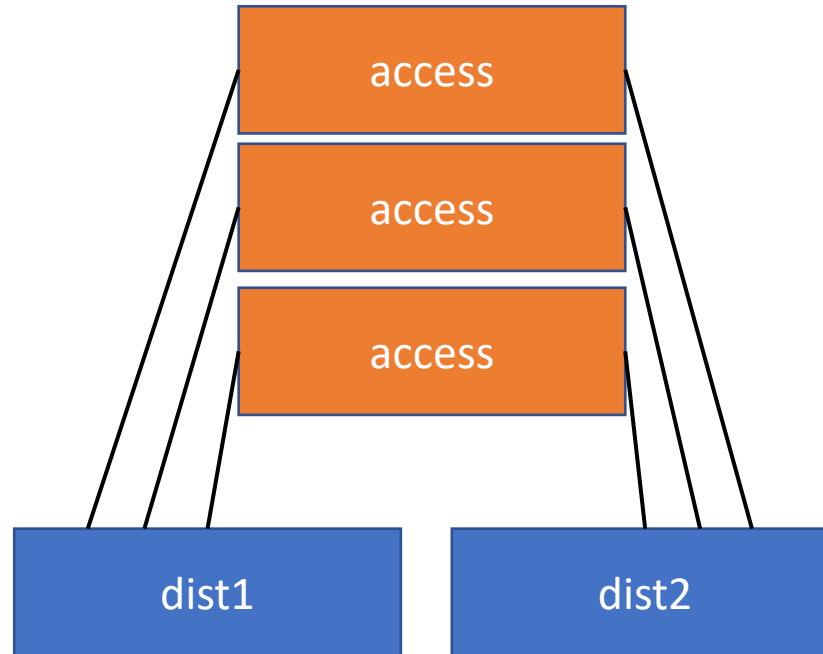
Design

- SUNET hjälper till att göra en redundant design av nätet, både på Wi-Fi, switchnät och brandvägg
- VLAN och IP-plan
- “Specialare”
- Inventering av befintligt nät

Referensdesign stort campus



Referensdesign mindre campus



Wi-Fi



- SUNET hjälper till att göra inventering, design och implementation baserat på önskemål



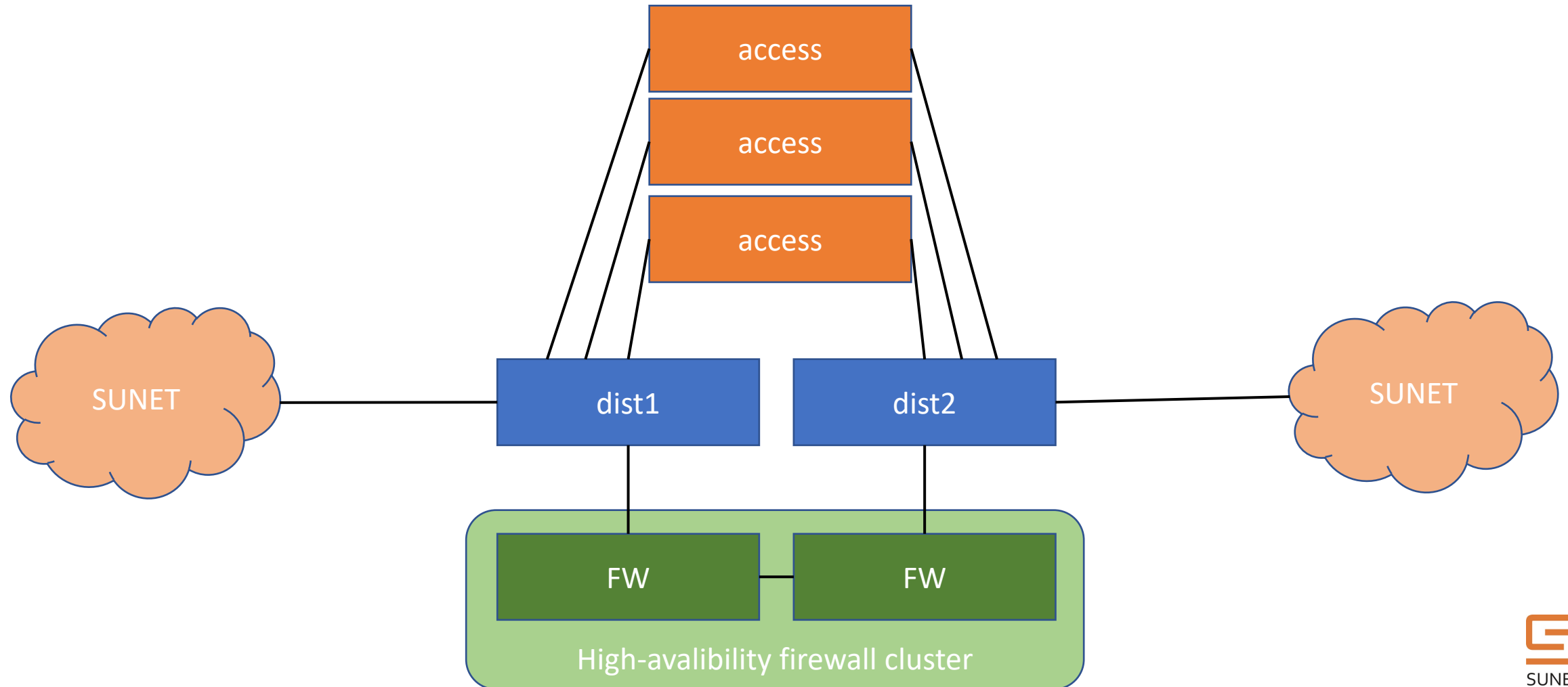
Brandvägg

Brandvägg

- Relativt ny tjänst, utveckling pågår
- Juniper SRX eller Palo Alto
- Firewall on-a-stick design



Firewall on-a-stick



CNaaS-NMS

Vad är NMS?

- Zero touch provisioning
- Firmwareuppgradering
- Konfiguration

Search... Hostname Search

Device list

Hostname	Device type	State (Sync status)	ID
> gih-vakt-d01	DIST	MANAGED ✓	1
> gih-vakt-d02	DIST	MANAGED ✓	2
> gih-vakt-a01	ACCESS	MANAGED ✓	6
> gih-plan4-a01	ACCESS	MANAGED ✓	8
> gih-plan4-a02	ACCESS	MANAGED ✓	9
> gih-plan4-a03	ACCESS	MANAGED ✓	10
> gih-tegel-a01	ACCESS	MANAGED ✓	11
> gih-tegel-a02	ACCESS	MANAGED ✓	12
> gih-plan5-a01	ACCESS	MANAGED ✓	13
> gih-plan5-a02	ACCESS	MANAGED ✓	14
> gih-plan3-a01	ACCESS	MANAGED ✓	15
> gih-plan3-a02	ACCESS	MANAGED ✓	16
> gih-plan3-a03	ACCESS	MANAGED ✓	17

ZTP

Används vid installation av ny switch (eller utbyte av trasig switch)

- 1) Koppla in den nya switchen
- 2) Switchen gör dhcp-boot och dyker upp i NMS som status: Discovered
- 3) Välj vilken typ av switch du vill ha samt namnge den
- 4) Commit, vänta på att jobbet körts och sen är det klart!

Uppgradera mjukvaran

- 1) Välj switch/grupp som ska uppgraderas
- 2) Välj firmware du vill ha och aktivera
- 3) När jobbet är klart, reboot
- 4) Vänta på omboot, klart!

Firmware list

Firmwares	
> EOS-4.25.8M.swi	☁️ ❌
> EOS-4.26.3M.swi	☁️ ❌
> EOS-4.26.4M.swi	☁️ ❌
> EOS-4.26.5M.swi	☁️ ❌
> EOS-4.26.6M.swi	☁️ ❌
> EOS-4.26.7M.swi	☁️ ❌
▼ EOS-4.26.8M.swi	☁️ ✅

Filename	EOS-4.26.8M.swi
OS version	4.26.8M-28525459.4268M
Approved by	indy
Approved date	2022-12-13
End of life date	2023-06-13

Copy to NMS ☁️

> EOS-4.27.6M.swi	☁️ ❌
> EOS-4.27.7.1M.swi	☁️ ✅
> EOS-4.27.8M.swi	☁️ 🚫 ❌
> EOS-4.28.5.1M.swi	☁️ ❌
> EOS64-4.28.6M.swi	☁️ ❌
> EOS-4.28.6M.swi	☁️ 🚫 ❌
> EOS-stable.swi	🚫 ❌

Hur gör man en konfigurationsändring?

- 1) Gör dina ändringar i settings-fil(er) eller templates
- 2) Commit och push till git
- 3) Be NMS hämta ändringarna från git
- 4) Kör en dry run
- 5) Verifiera diffen du får
- 6) Live run, klart!

Interface config

- Ny feature
- Ändra port-typ
- Sätt fasta VLAN

Interface configuration

Hostname: gih-plan5-a01, sync state: ✓

Name	Description	Configtype	VLANs
<input type="radio"/> Ethernet1	<input type="text"/>	Auto/dot1x	
<input type="radio"/> Ethernet2	<input type="text"/>	Auto/dot1x	
<input type="radio"/> Ethernet3	<input type="text"/>	Untagged/access	
<input type="radio"/> Ethernet4	<input type="text"/>	Tagged/trunk	
<input type="radio"/> Ethernet5	<input type="text"/>	Downlink	
<input type="radio"/> Ethernet6	<input type="text"/>	Uplink	
		MLAG peer interface	
		Auto/dot1x	
		Auto/dot1x	

NAC

RADIUS och 802.1X

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service.

RADIUS

- Vi hjälper till med integrationen
- Pratar med lärosätets AD (eller vad man nu har) för att på så sätt få in användare på rätt VLAN
- Med hjälp av eduroam kan även användare från ett annat lärosäte autentiseras
- Kan inte användaren autentisera sig hamnar den på ett “fail-vlan”

NAC

Grafiskt gränssnitt som används primärt för hantering av “dumma” enheter som inte kan certifikat eller användarnamn och lösenord

SELECT	MAC	LAST SEEN	ACTIVE	IP	REASON
<input type="checkbox"/>	02:2c:7c:a6:ba:66	2022-09-07 06:50:05.078827	✓	777	None
<input type="checkbox"/>	02:81:4e:54:99:68	2022-09-07 06:50:05.076393	✓	806	None
<input type="checkbox"/>	04:93:37:c4:e3:e4	2022-09-07 06:48:02.404244	✗	982	None
<input type="checkbox"/>	05:9e:10:34:18:f2	2022-09-07 06:48:11.624374	✗	526	None
<input type="checkbox"/>	0b:ee:f4:bb:e2:f6	2022-09-07 06:48:10.777541	✗	1000	None
<input type="checkbox"/>	0d:78:b8:29:b2:37	2022-09-07 06:48:02.903904	✗	709	None
<input type="checkbox"/>	0e:bb:d4:d2:c0:05	2022-09-07 06:50:05.071828	✓	577	None
<input type="checkbox"/>	0f:74:98:41:30:06	2022-09-07 06:50:05.074809	✓	872	None
<input type="checkbox"/>	0f:ba:54:3d:5c:cb	2022-09-07 06:50:05.074213	✓	138	None
<input type="checkbox"/>	10:cd:7f:8b:9b:e9	2022-09-07 06:48:05.111544	✗	886	None
<input type="checkbox"/>	11:9f:f0:0a:96:ca	2022-09-07 06:48:07.128975	✗	867	None
<input type="checkbox"/>	15:2a:23:5c:d1:11	2022-09-07 06:48:08.593546	✗	615	None
<input type="checkbox"/>	16:34:d1:3a:2a:ca	2022-09-07 06:50:05.076966	✓	795	None
<input type="checkbox"/>	17:39:7a:8b:29:94	2022-09-07 06:48:13.125435	✗	764	None
<input type="checkbox"/>	18:36:de:8f:63:ff	2022-09-07 06:48:12.474339	✗	195	None

NAC

- Finns externt API om man vill använda ett annat system för att styra användarhanteringen
- Går att “massprovisionera” enheter, antingen med hjälp av OUI eller en CSV-fil
- Helt open source, inga hemligheter.
- Ingen AI, än.

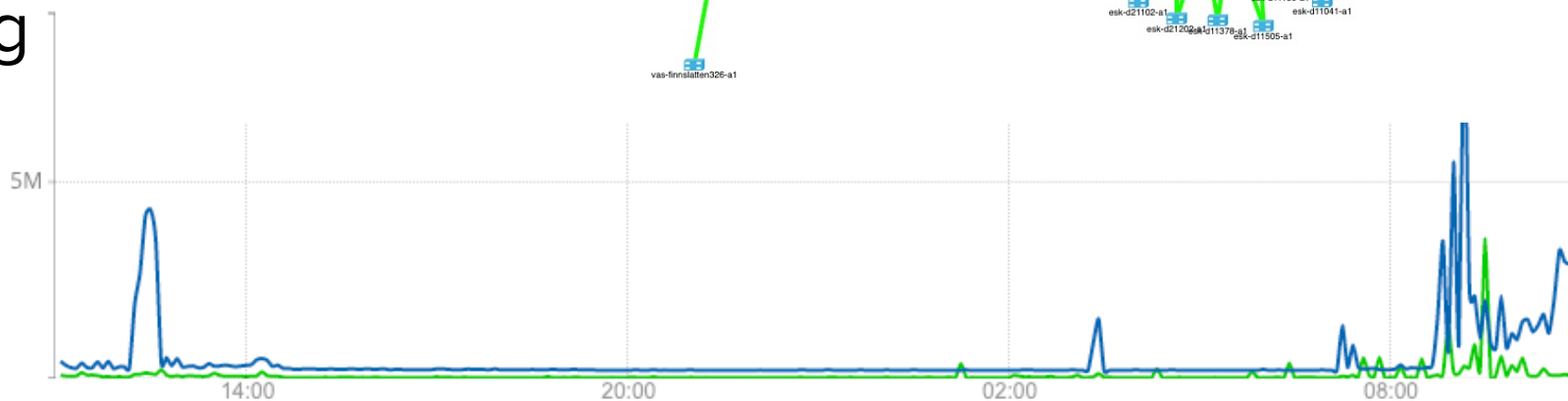
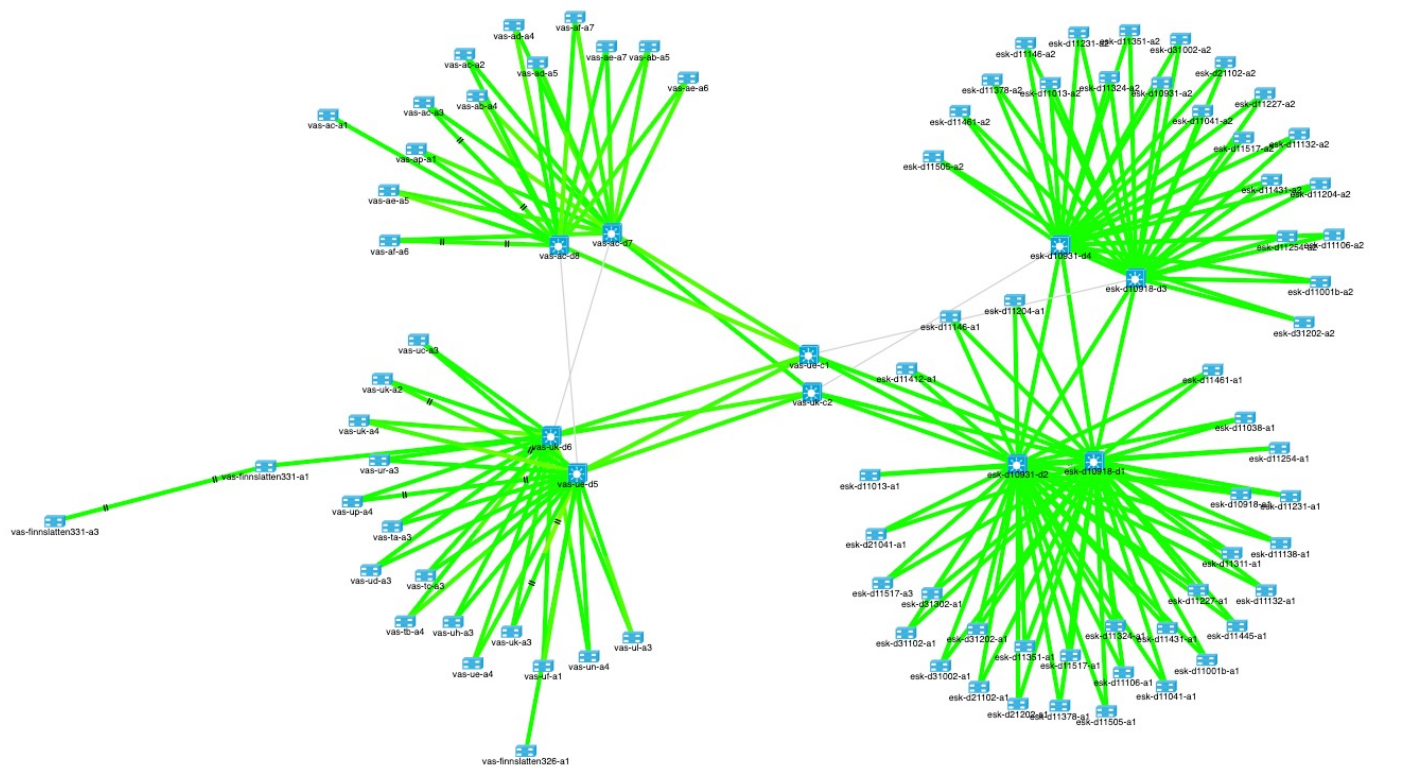
Övervakning

SUNET NOC

- SUNET NOC övervakar, eskalerar och felavhjälp dygnets alla timmar, varje dag, året runt



- Nätövervakning
- Larm
- Statistik
- Topologi
- Viss managring



Nagios®

- Serverövervakning
- Larm
- Statistik


Dokumentation och loggar

wiki.sunet.se/display/CNaaS

- Innehåller dokumentation för de applikationer som ingår
- Designdokument
- IP/VLAN-planer
- Eskaleringsvägar

NI

- Dokumentation av nätet



BROWSE TYPES

- Cables
- Nordunet Cables
- ODFs
- Outlets
- Patch Panels
- Ports
- Racks
- Rooms
- Sites
- Switches

REPORTS

- Host reports
- Unique IDs

MAPS

- Site map
- Optical node map

ADMIN

- Create new
- Reserve IDs
- Users
- Log out

 SearchLogged in as **mikott** [Log out](#)

Room A1-018

Located in **Esk****More information:** [To Portal](#)**Modified:** March 19, 2020, 11:30 a.m. by [bergroth](#)**Created:** March 19, 2020, 11:30 a.m. by [bergroth](#)[Edit](#)

Local equipment

 Filter Filter

Type	Name	Description
Outlet	D11013S1M04:24	Golvbrunn, A10.18
Outlet	D11013S1M04:23	Golvbrunn, A10.18
Outlet	D11013S1M04:22	Golvbrunn, A10.18
Outlet	D11013S1M04:21	Golvbrunn, A10.18
Outlet	D11013S1M04:20	Golvbrunn, A10.18
Outlet	D11013S1M04:19	Golvbrunn, A10.18
Outlet	D11013S1M04:18	Golvbrunn, A10.18
Outlet	D11013S1M04:17	Golvbrunn, A10.18
Outlet	D11013S1M04:16	Golvbrunn, A10.18
Outlet	D11013S1M04:15	Golvbrunn, A10.18
Outlet	D11013S1M13:14	På stege, utanför A10.18
Outlet	D11013S1M04:14	Ovan undertak, A10.18
Outlet	D11013S1M13:13	På stege, utanför A10.18
Outlet	D11013S1M04:13	Ovan undertak, A10.18
Outlet	D11013S1M13:12	I vägg, utanför A10.18
Outlet	D11013S1M04:12	Ovan undertak, A10.18
Outlet	D11013S1M13:11	I vägg, utanför A10.18



- Graylog används för loganalys
- Servrarna som placerats på campus kör syslog som skickas vidare till Graylog

Vägen framåt

Roadmap

- Integrera vissa funktioner i brandväggen med NMS
- Förbättra dokumentationen
- Förbättra övervakningen
- Ny upphandling
- Nya kunder
- Bygga vidare hos befintliga kunder
- Fler utbildningar/workshops

Frågor?

Boka gärna ett möte med oss så kan vi diskutera vidare

<https://sUNET.se/services/nat/campusnat-cnaas>

mikott@sUNET.se