



SUNET
CNaaS

Campusnät som tjänst CNaaS

Mikael Ottosson

Vem är jag?

- Mikael Ottosson, 25+ år
- Från civilisationens vagga Leksand
- Jobbat på SUNET/NORDUnet i 10+ år
- Tjänsteförvaltare för SUNETs Campusnätstjänst

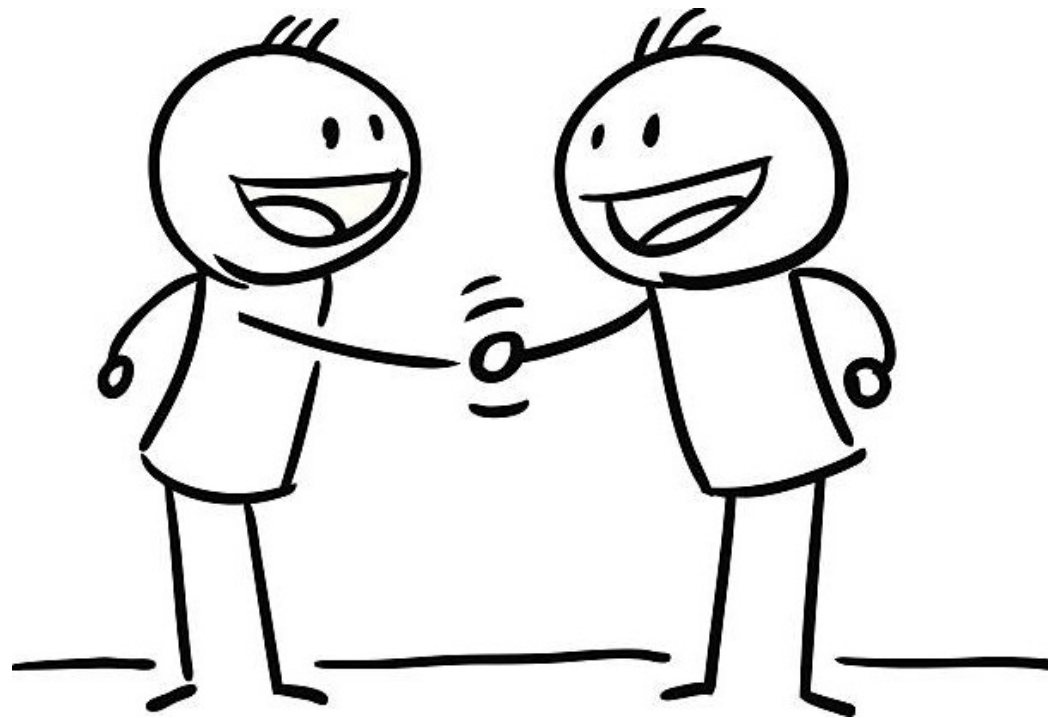


Vad är Campusnät?

- Redundant nätverk som skalar
- Trådat nät
- Wi-Fi - option
- Brandvägg – option
- Manageringsverktyg (NMS och NAC)
- System för övervakning och dokumentation (NAV, Nagios, wiki, Graylog, Platform, Netbox)
- Design, konfiguration

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
- Redundant, 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

Tar SUNET över mitt nät nu?

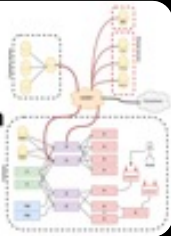
NEJ!

Tar SUNET över mitt nät nu?

- Nej, detta är ett samarbete mellan lärosätet och SUNET
- Vi designar tillsammans
- Vi bygger nätet tillsammans
- Lärosätet driftar nätet och gör konfigurationsförändringar
- SUNET bistår med assistans vid behov
- SUNETs NOC övervakar, men samtliga verktyg som SUNETs NOC använder finns tillgängliga för lärosätet att använda om så önskas



Design



WiFi



Dokumentation



CNaaS
NMS



Övervakning

NAC
RADIUS och 802.1X



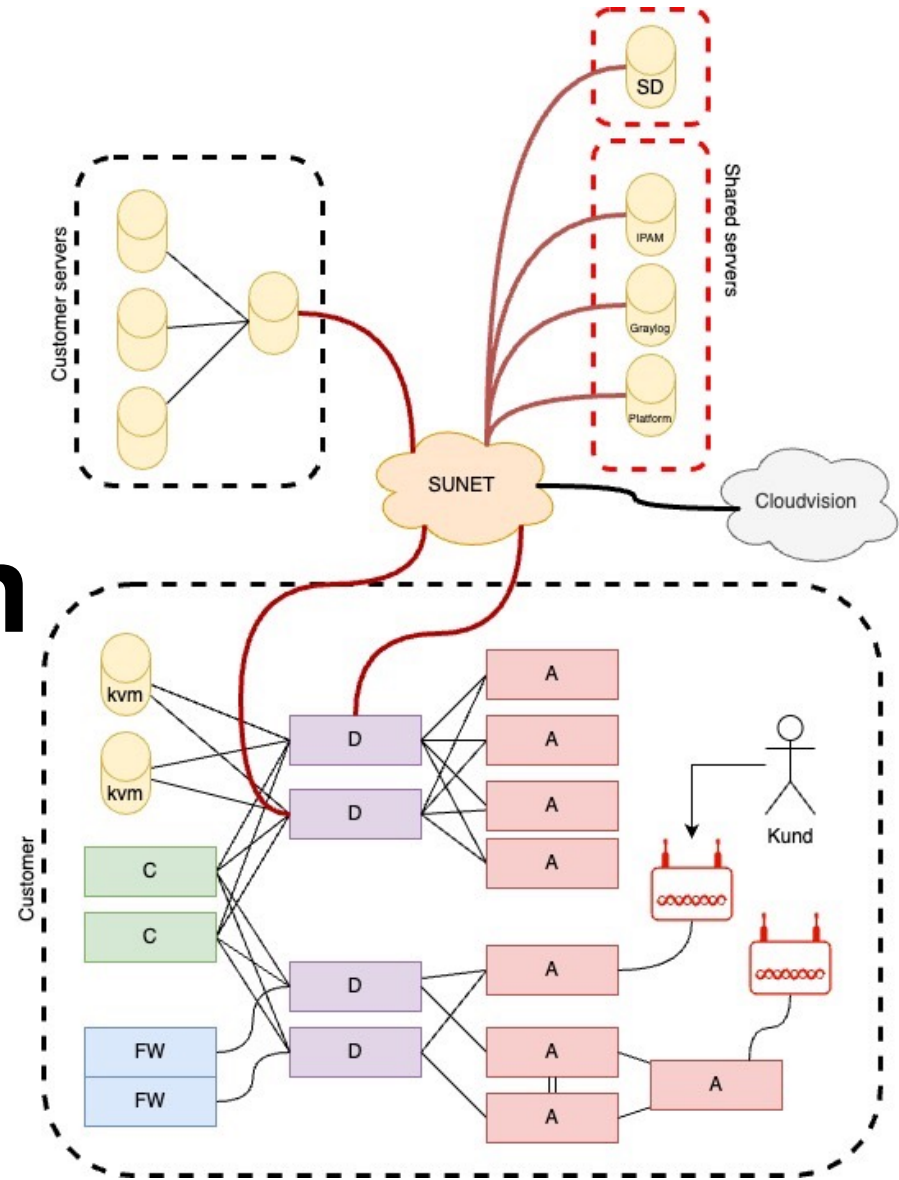
Brandvägg



Övrigt



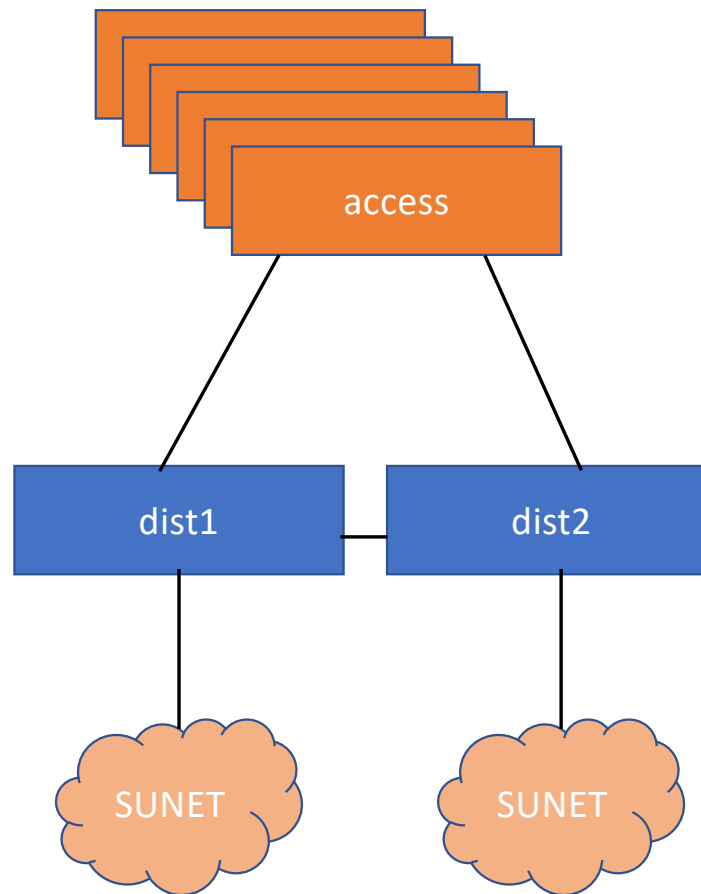
Design



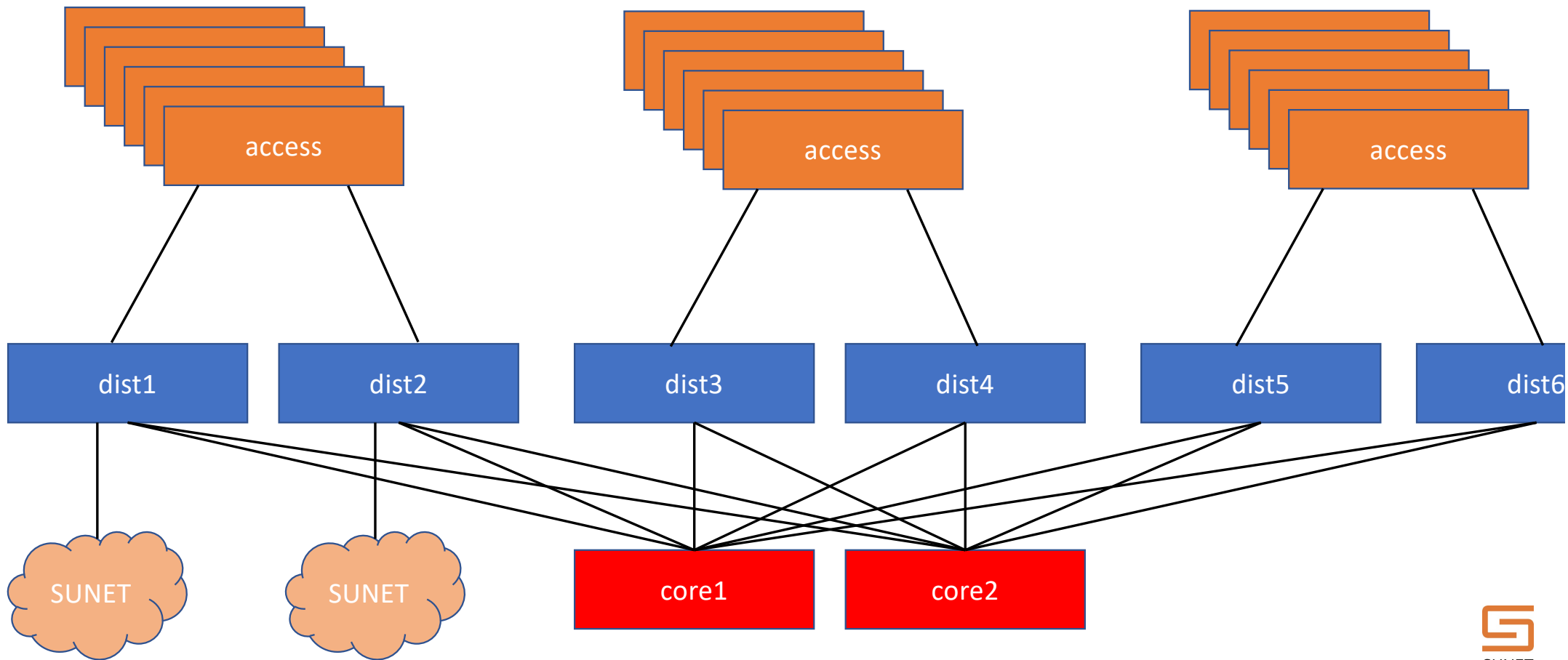
Design

- Sunet och lärosätet tar gemensamt fram en redundant design av nätet
- VLAN och IP-plan
- “Specialare”
- Inventering av befintligt nät
- Migreringsplan/design

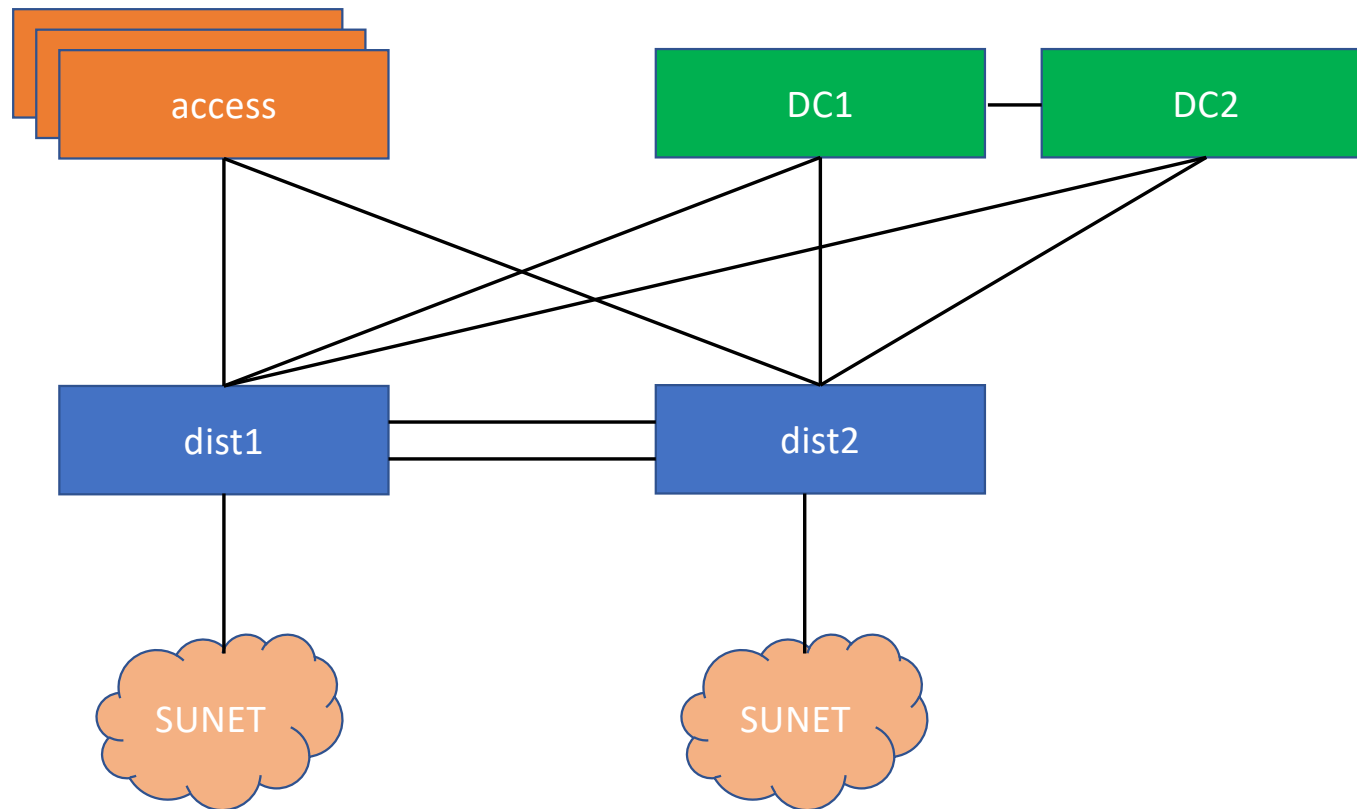
Referensdesign



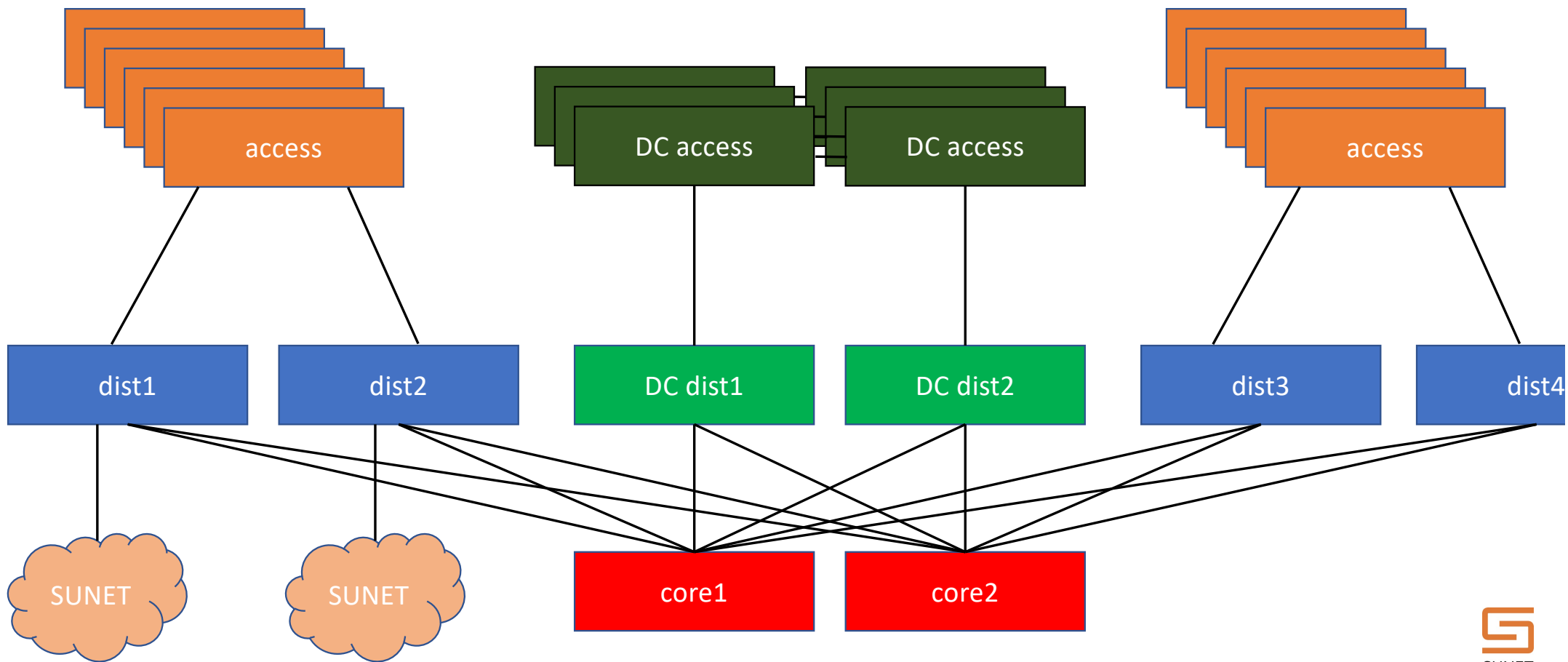
Referensdesign stort campus



Campus + Datacenter



Campus + Större datacenter





Wi-Fi

1. Diskussion – vad vill vi uppnå?
2. Inventering och mätningar
3. Design - ny design eller baserat på befintligt wi-fi?



Wi-Fi

1. Diskussion – vad vill vi uppnå?
2. Inventering och mätningar
3. Design - ny design eller baserat på befintligt wi-fi?
4. Beställa APs
5. Installation
6. Mätning på det nya nätet
7. Eventuella justeringar
8. Mätning igen

Wi-Fi

- Controller i molnet eller on-prem (VM)
- Arista Cloudvision

Brandvägg



Brandvägg

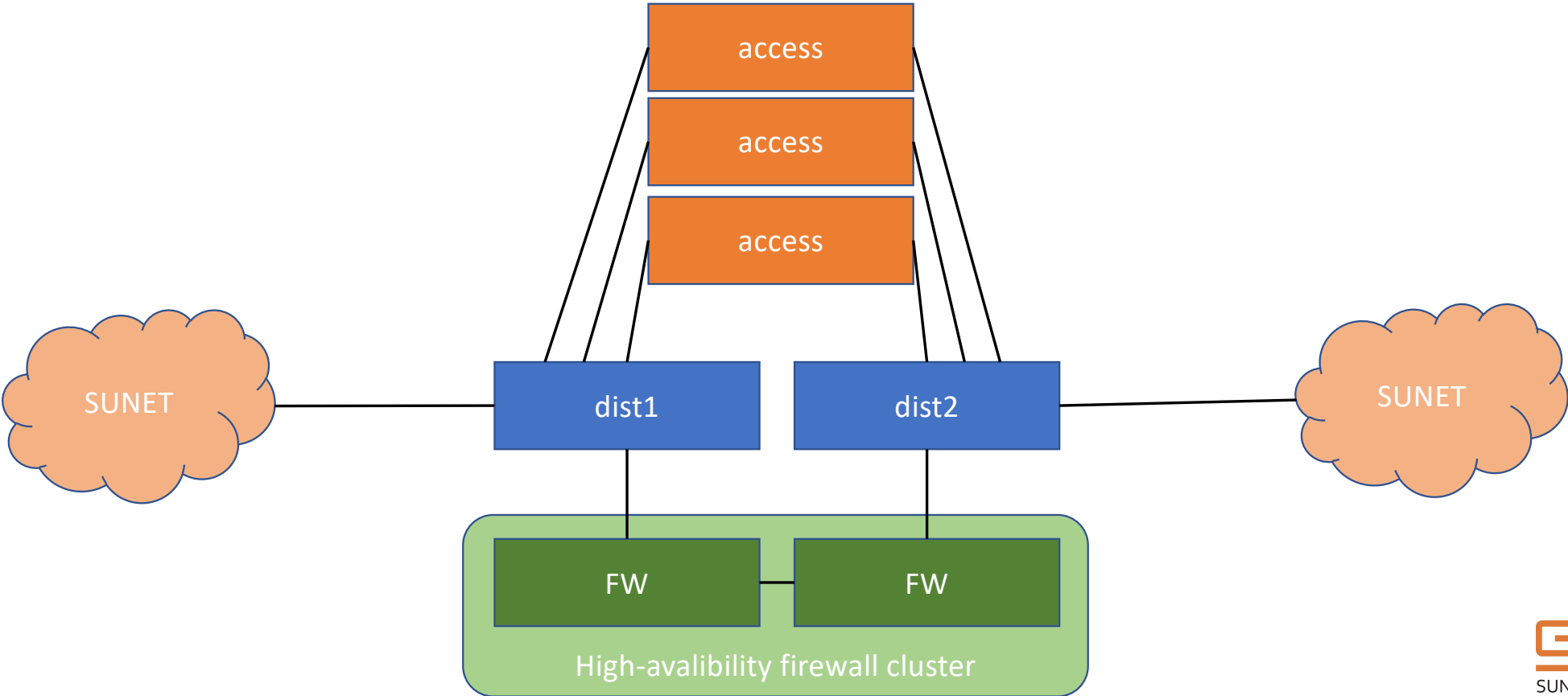
- Juniper SRX eller Palo Alto
- Firewall on-a-stick design



Brandvägg

- Sunet hjälper till med designen

Firewall on-a-stick



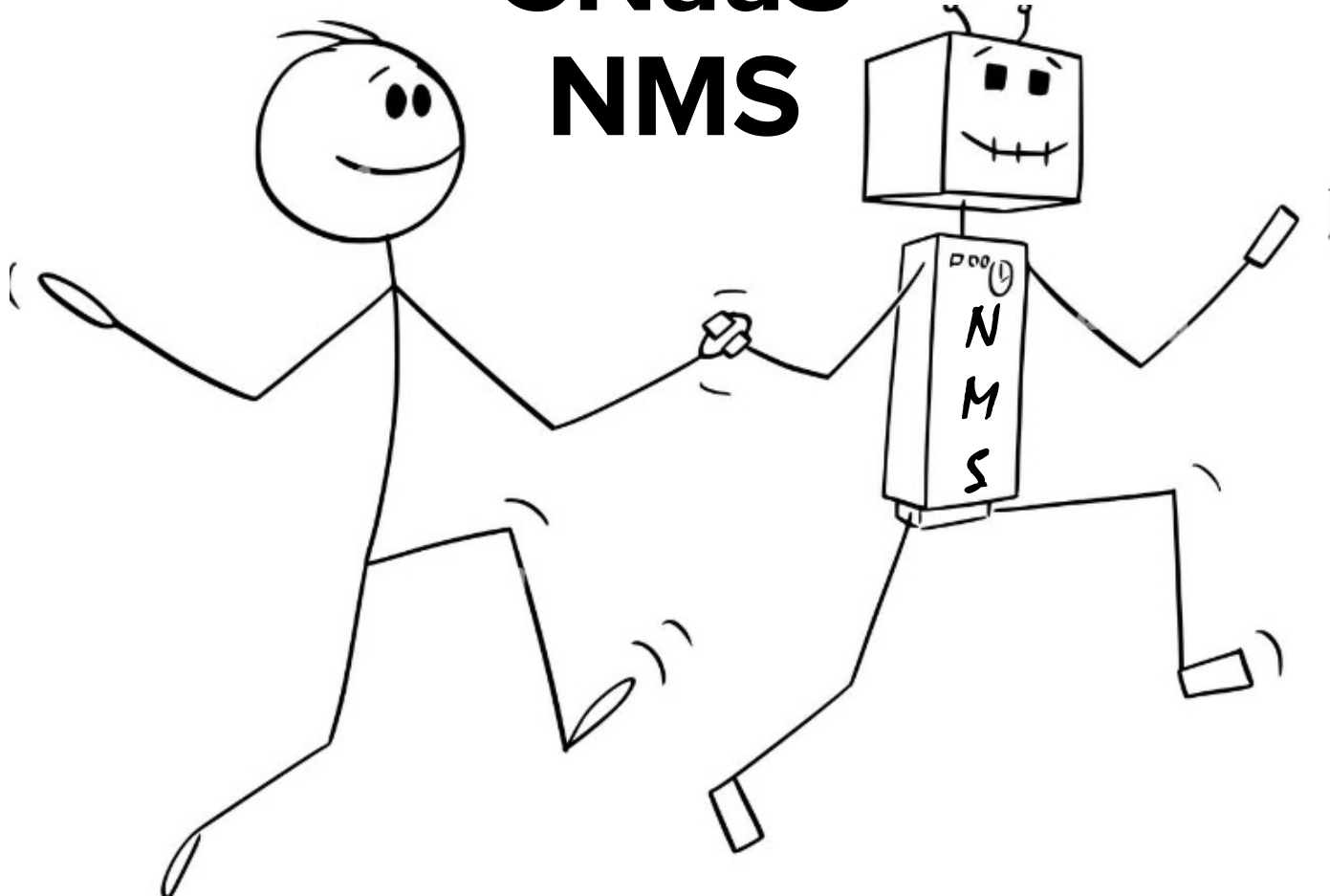
Brandvägg

- Sunet hjälper till med designen
- Vi gör en migreringsplan från nuvarande lösning
- Vi bygger tillsammans
- Tester

Juniper Security Director

- Manageringsverktyg för Junipers brandväggar
- Står centralt på SUNET
- Ingen extra kostnad för lärosätet
- Egen ”instans” per lärosäte
- <https://www.juniper.net/us/en/products/security/security-director-network-security-management.html>

CNaaS NMS



Vad är NMS?

- Network management system
 - Zero touch provisioning

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

Zero Touch Provisioning

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

- 1) Koppla in den nya switchen
- 2) Switchen gör dhcp-boot, uppgraderar sig 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!

Vad är NMS?

- Network management system
 - Zero touch provisioning
 - Uppgradera mjukvaran

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

Uppgradera mjukvaran

- 1) Välj switch/grupp som ska uppgraderas
- 2) Välj firmware du vill ha och aktivera
- 3) När jobbet är klart, starta om direkt eller vid en vald tidpunkt
- 4) Vänta på omstart, klart!

Kan även göras på grupper av switchar

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	☁️ ❌

Vad är NMS?

- Network management system
 - Zero touch provisioning
 - Uppgradera mjukvaran
 - 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

Hur gör man en konfigurationsändring?

- 1) Gör dina ändringar på plattform

Vad är då plattform?

Plattform är en webbaserat verktyg för konfigurationshantering

Man gör sina konfigurationsändringar i yaml-filer på plattform

Versionshantering osv

Varje kund får en slice för sin konfig

Står lokalt på Sunet

```
53 lines | 1.2 KiB | YAML
1 ---
2 interfaces:
3   - name: Ethernet25
4     ifclass: downlink
5   - name: Ethernet27
6     ifclass: downlink
7   - name: Ethernet47
8     ifclass: downlink
9   - name: Ethernet48
10    ifclass: downlink
11  - name: Ethernet40
12    ifclass: custom
13    config: |-
14      no switchport
15      description orval.sunet.se (MGMT)
16  - name: Ethernet40.10
17    ifclass: custom
18    config: |-
19      encapsulation dot1q vlan 10
20      vrf MGMT
21      ip address 10.103.0.1/31
22      description orval.sunet.se (MGMT)
23  - name: Ethernet40.11
24    ifclass: custom
25    config: |-
26      encapsulation dot1q vlan 11
27      vrf STUDENT
28      ip address 10.103.0.3/31
29      description orval.sunet.se (STUDENT)
30  - name: Ethernet42
31    ifclass: custom
32    config: |-
33      description ixia-switch port14
34      switchport mode access
35      switchport access vlan 225
```

Hur gör man en konfigurationsändring?

- 1) Gör dina ändringar på platform
- 2) Spara
- 3) Be NMS hämta ändringarna
- 4) Kör en dry run
- 5) Verifiera diffen du får
- 6) Live run, klart!

Vad är NMS?

- Network management system
 - Zero touch provisioning
 - Uppgradera mjukvaran
 - Konfiguration
 - Portspezifisk 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

Portspecifik konfiguration

- Grafisk vy för att göra ändringar på en port
- Ändra port-typ
- Sätt fasta VLAN
- “Starta om” en port
- Använda tag/templates tex “no PoE”

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

- Används för att autentisera användare med 802.1X
- Vi tillhandahåller RADIUS-servrar som kan agera proxy mellan eduroam och era ordinarie RADIUS-servrar om så önskas.

Ansluta med en användare

1. Switchen försöker autentisera med EAP (“eduroam-inloggning”).
2. Om autentiseringen misslyckas provar switchen att använda sig av MAB/MBA (MAC-adressen)
3. Misslyckas även det, blir enheten flyttad till ett “fail-vlan”
4. Man kan sedan, med hjälp av NACs grafiska vy, flytta en enhet från ett VLAN till ett annat

NAC

localhost:1234/clients

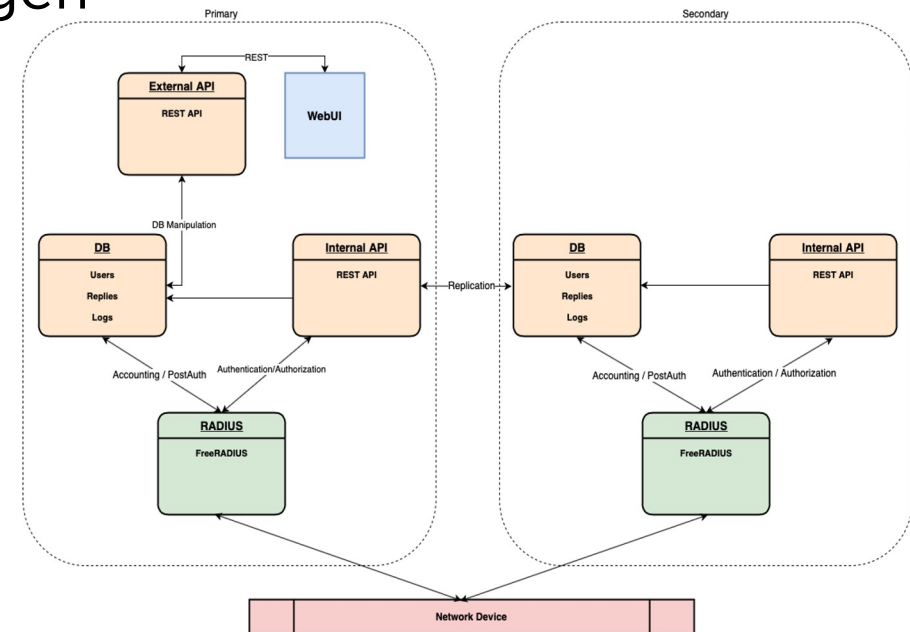
Start Clients

+ - [icon] Active Inactive VLAN Comment Bounce Last week All clients Search... Username [icon]

SELECT	USERNAME	LAST SEEN	ACTIVE	VLAN	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:1d: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
- Helt open source, inga hemligheter





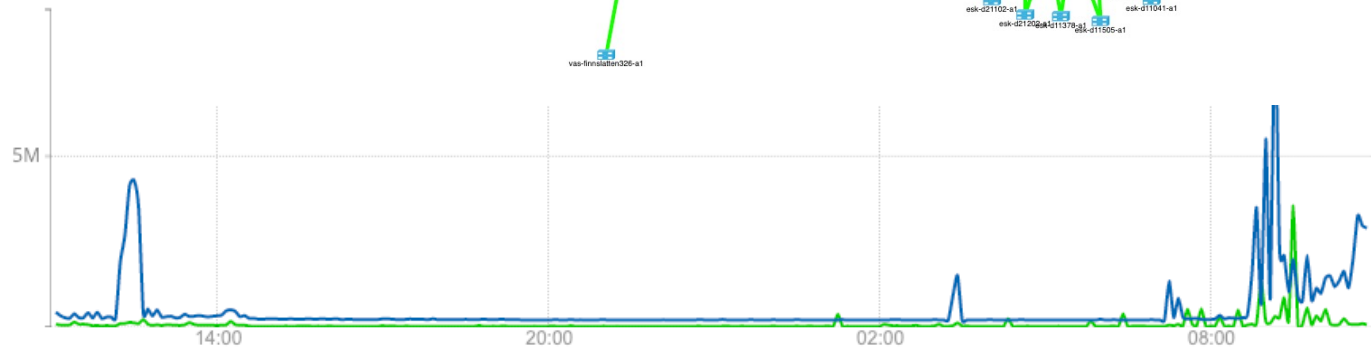
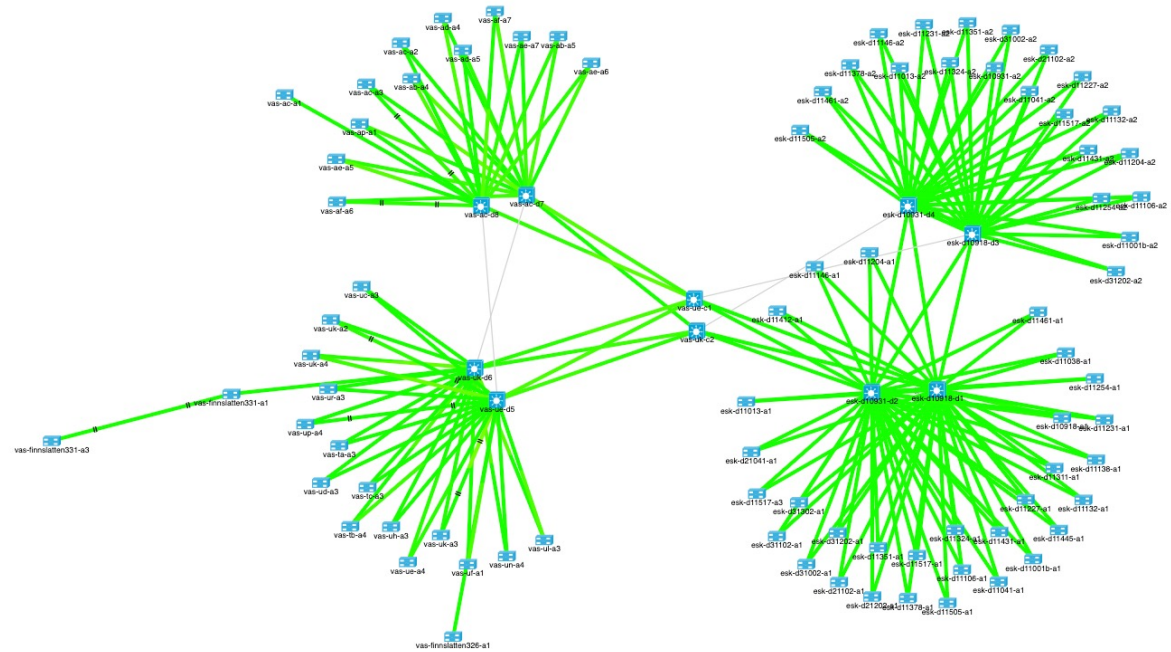
SUNET NOC

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





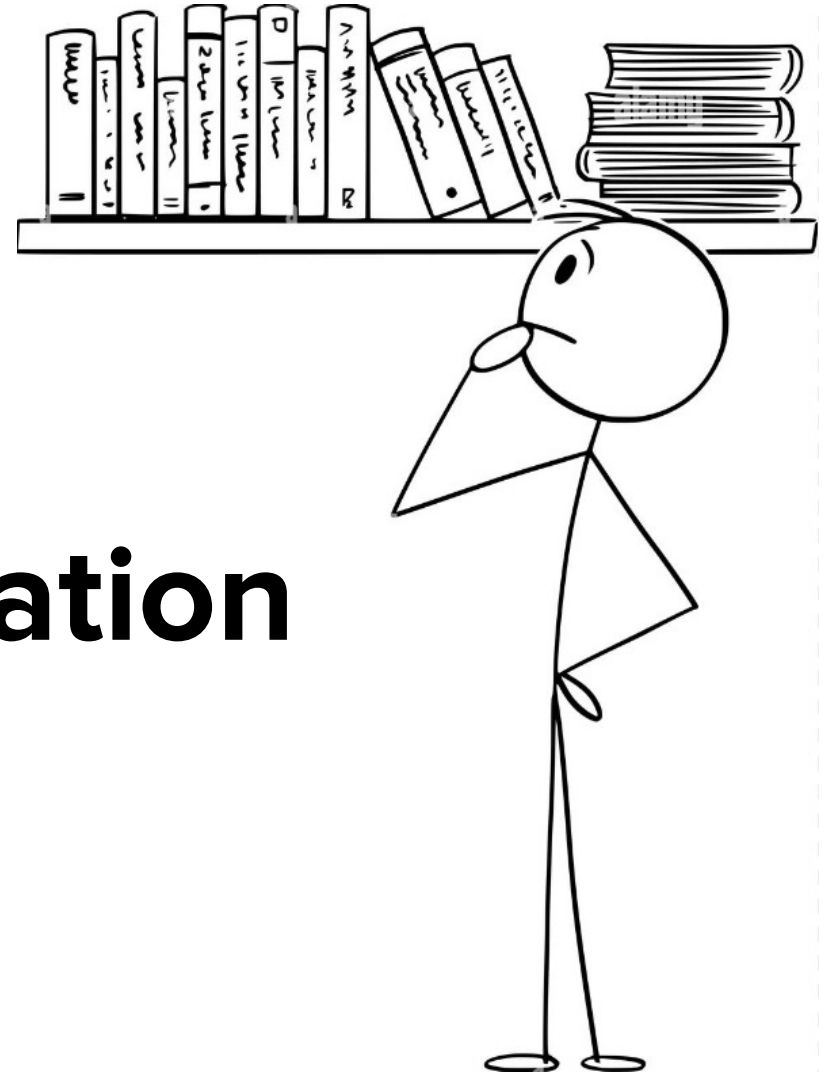
- Nätövervakning
- Larm
- Statistik
- Topologi



Nagios®

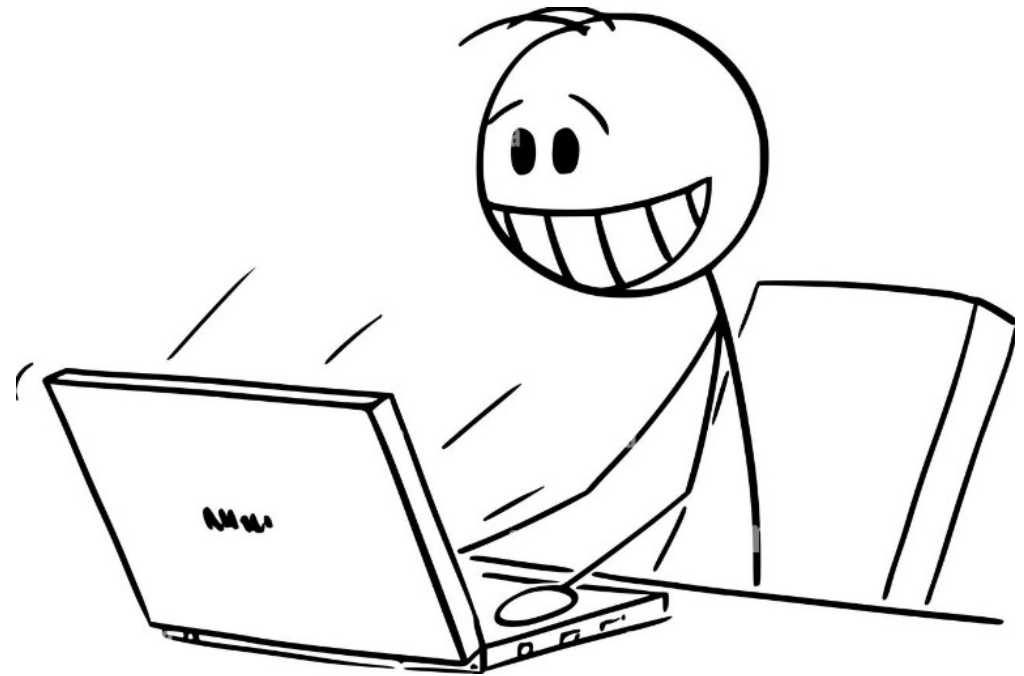
- Övervakning av de “CNaaS-servrar” vi ställer hos en kund
- Larm
- Statistik

Dokumentation



wiki.sunet.se/display/CNaaS

- Innehåller dokumentation för de applikationer som ingår
- Designdokument
- IP/VLAN-planer
- Eskaleringsvägar
- En hel del How-to guider



NI

- Dokumentation av nätet

The screenshot displays the NOCLook web application interface. On the left is a sidebar with navigation options: 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), and ADMIN (Create new, Reserve IDs, Users, Log out). The main content area shows details for Room A1-018, including its location (Esk), more information (To Portal), modification date (March 19, 2020, 11:30 a.m. by bergroth), and creation date (March 19, 2020, 11:30 a.m. by bergroth). Below this is a table of local equipment with columns for Type, Name, and Description. The table contains 17 rows of equipment data, with the row for D11013S1M04:20 highlighted in blue.

Search

Logged in as mikotti [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 stegen, utanför A10.18
Outlet	D11013S1M04:14	Ovan undertak, A10.18
Outlet	D11013S1M13:13	På stegen, 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

IPAM - Netbox

- IP-prefix
- VLAN
- AS-nummer
- Script

Övrigt

**Det här var det bästa sedan skivat bröd,
hur går jag med?**



Sunets inköpscentral

- För att vara med i Campusnät är steg 1 att man går med i inköpscentralen
- 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>

CNaaS-kontrakt

- När man är med i inköpscentralen så kan man gå med i CNaaS
- Mer info finns på <https://sunet.se/services/nat/campusnat-cnaas>

Kostnad

För att dela på kostnaderna så är avgiften till SUNET volymbaserad:

- **330.000kr + 10% av hårdvaruinköpet per år**
- Hårdvaruavgiften har en maxgräns på 1 000 000kr/år oavsett storlek.

Inga extrakostnader för serverinfrastruktur, förstudie, arkitekturdesign, inköpsstöd, supporteskälringar, implementation eller livscykelhantering.

Vem har då campusnät idag?

- 12 lärosäten installerade eller under installation
- 3 “egna” installationer
- 2 nya lärosäten
- Diskussion med flertalet lärosäten

Roadmap

- Nya kunder
- Bygga vidare hos befintliga kunder
- Automatisera/interagera mera mellan systemen
- Centralisera Nagios mha IPv6
- NAV -> NAV 2.0
- Fler utbildningar/workshops
- Mer och intelligentare larm
- VPN

Frågor?

mikott@sUNET.se

david@sUNET.se

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

