SUNET
CNaaS

Campusnät som tjänst
CNaaS

Mikael Ottosson

SUNET

Vem är jag?

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

SUNET

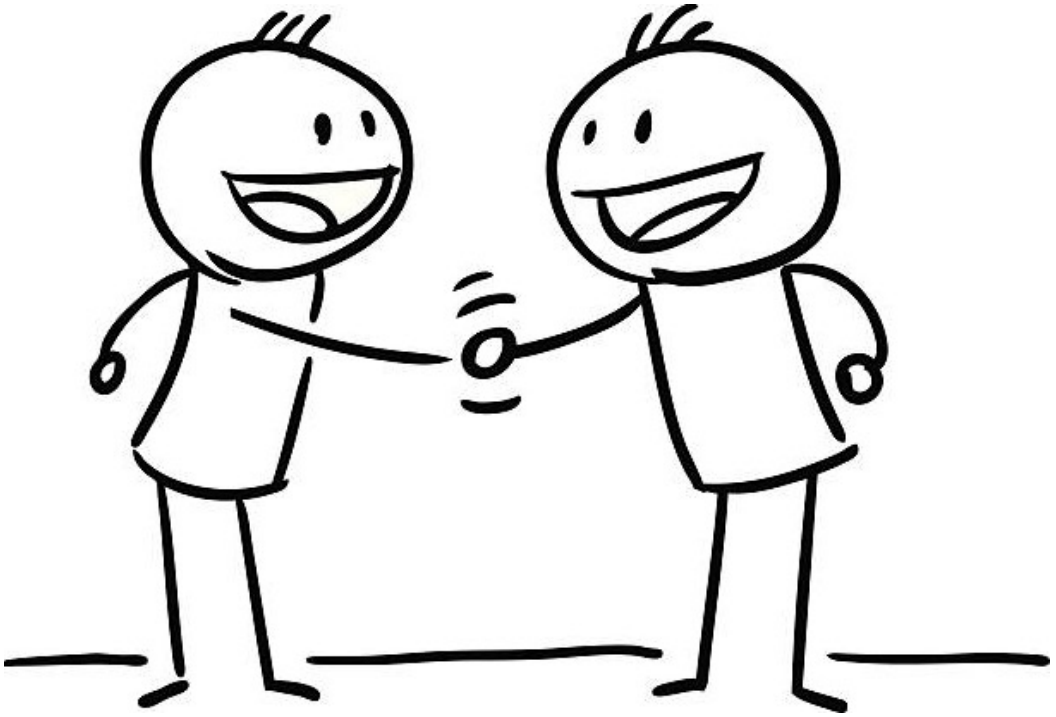
Vad är Campusnät?

- 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

SUNET

Vad är Campusnät?

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



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

SUNET

Tar SUNET över mitt nät nu?

NEJ!

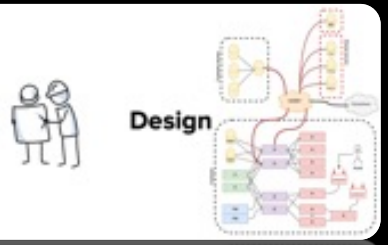
SUNET

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

SUNET

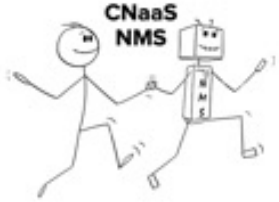
Design



Wi Fi

Dokumentation

CNaaS
NMS



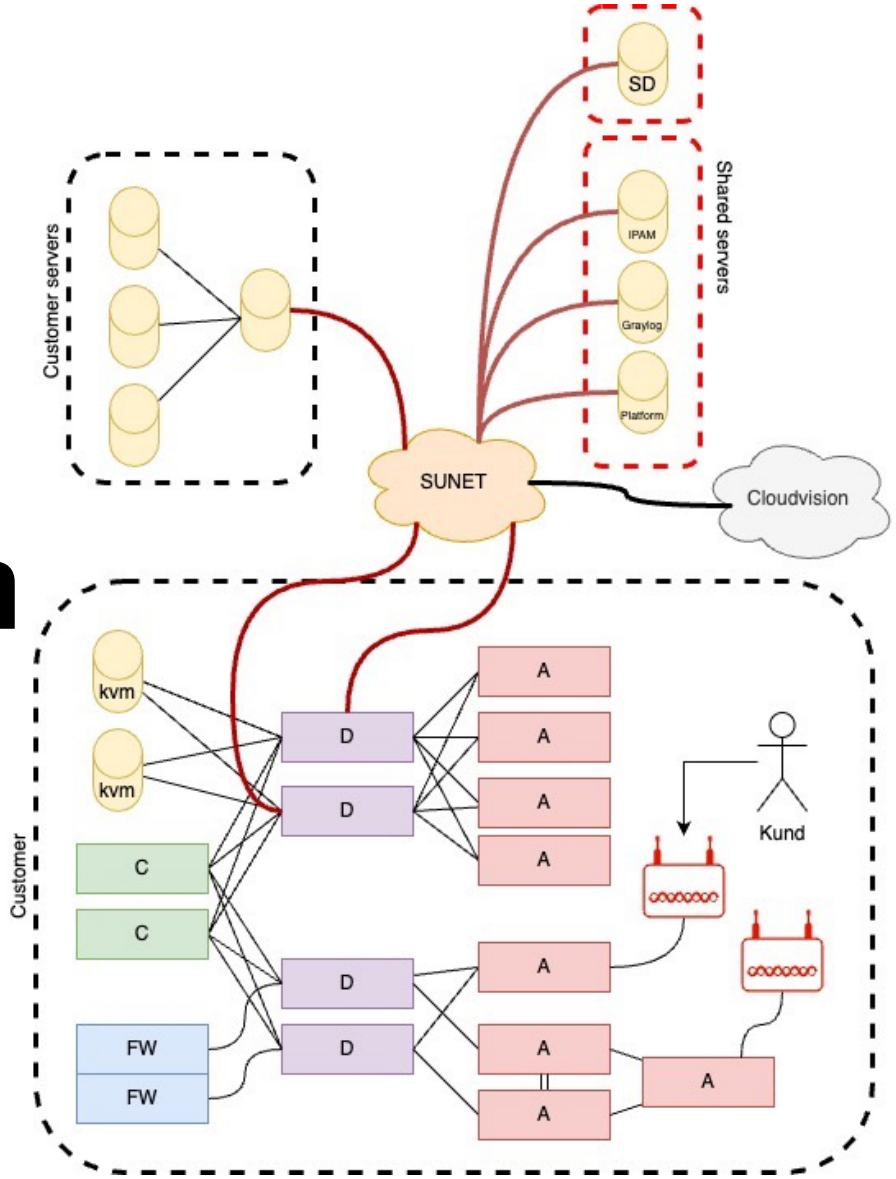
NAC
RADIUS och 802.1X

Brandvägg

Övrigt

SUNET

Design

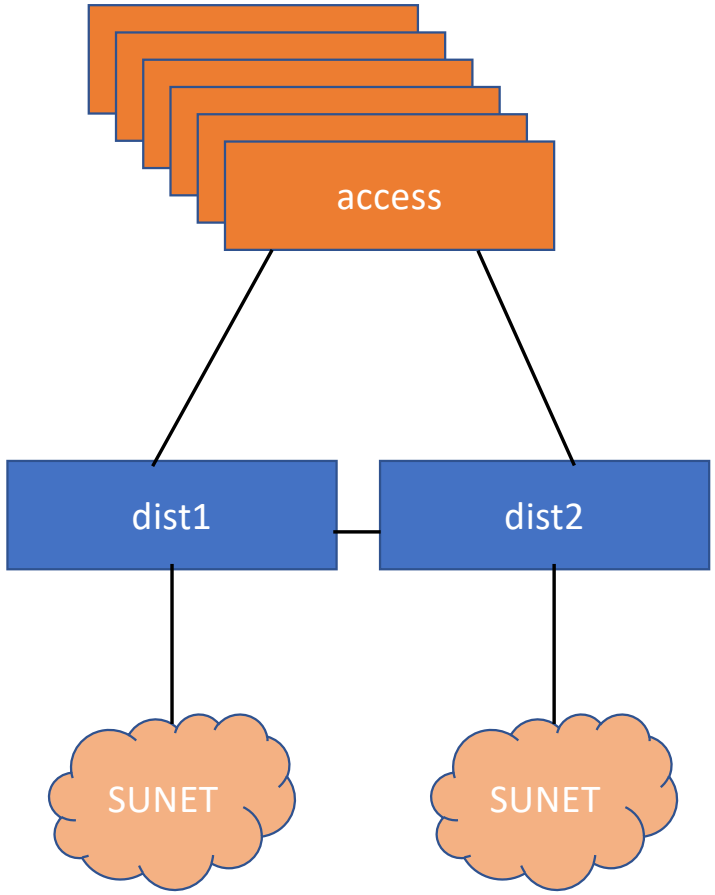

SD
IPAM
Graylog
Platform
Shared servers
Customer servers
SUNET
Cloudvision
kvm
kvm
C
C
FW
FW
D
D
D
D
A
A
A
A
A
A
A
A
Kund
Customer

Design

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

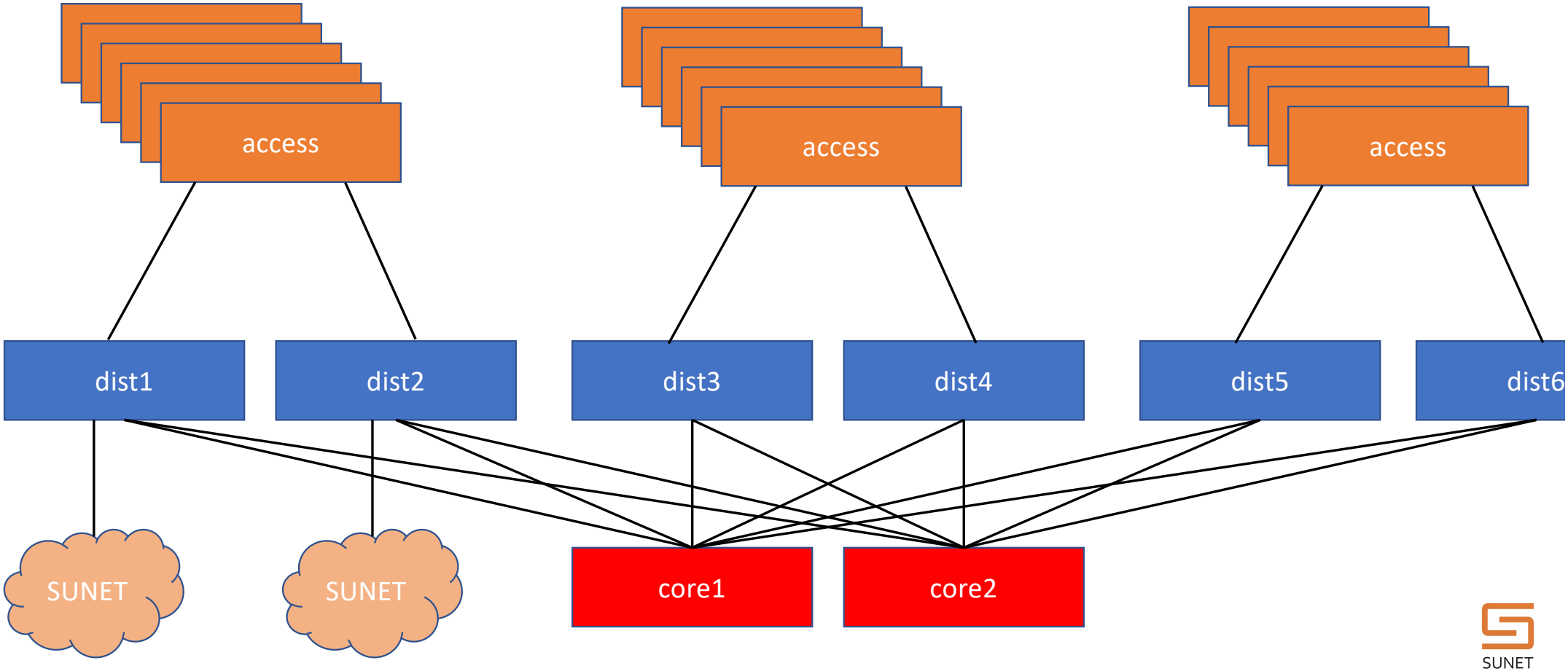
SUNET

Referensdesign

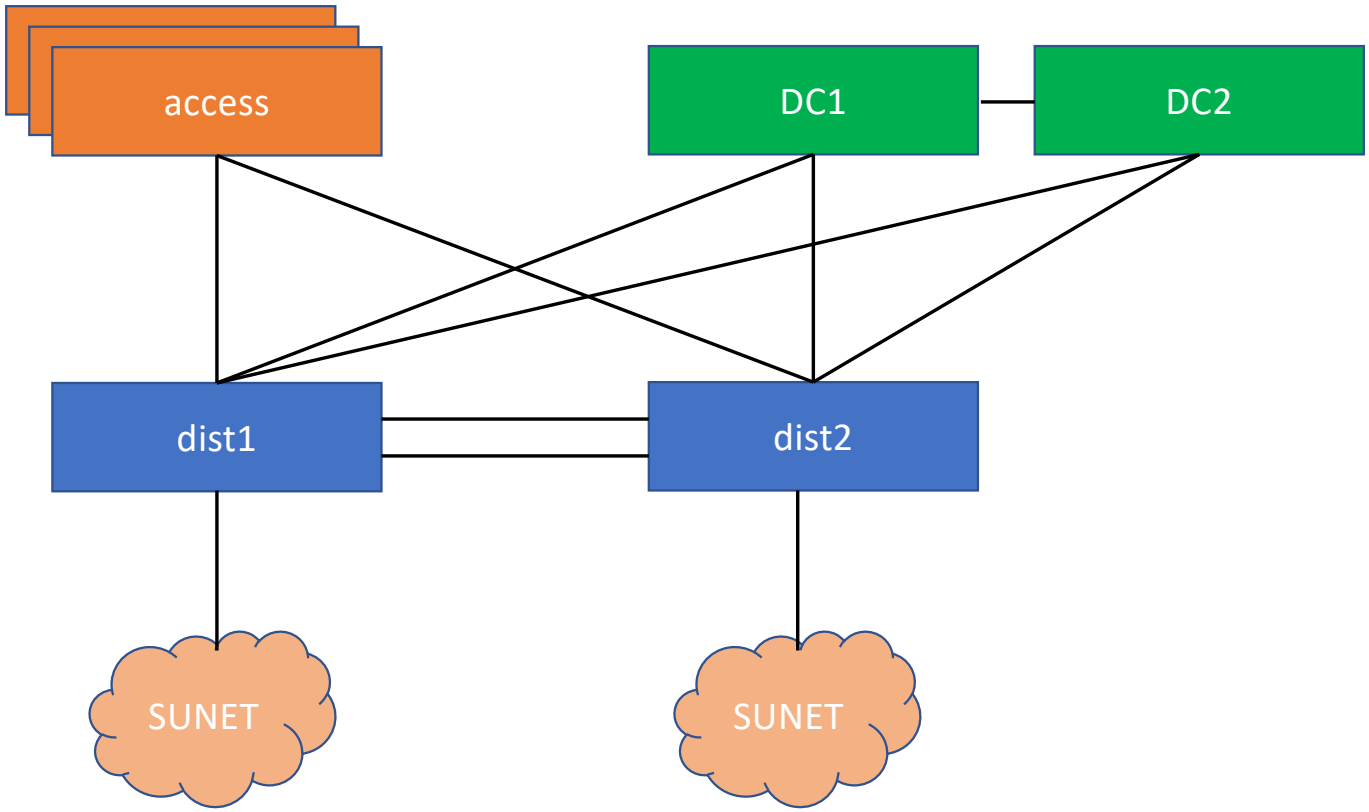


SUNET

Referensdesign stort campus

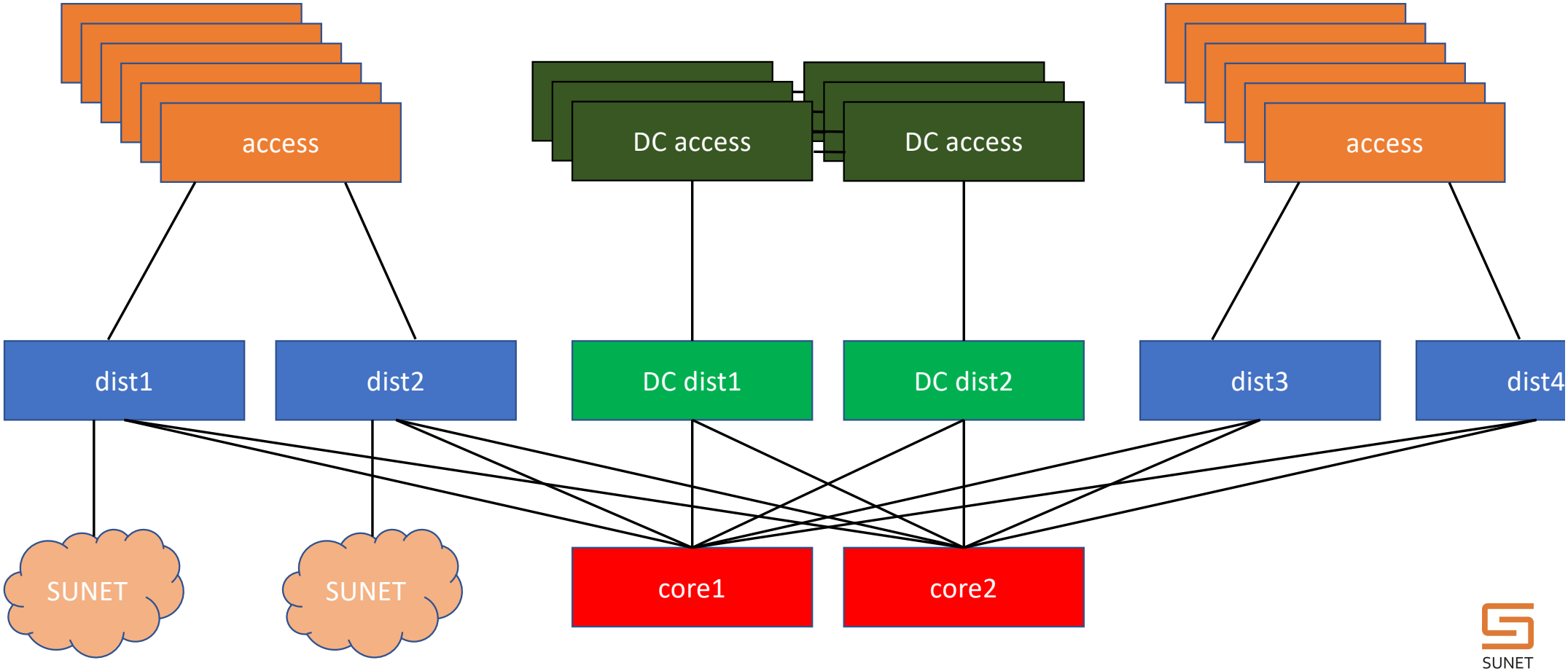


Campus + Datacenter



SUNET

Campus + Större datacenter



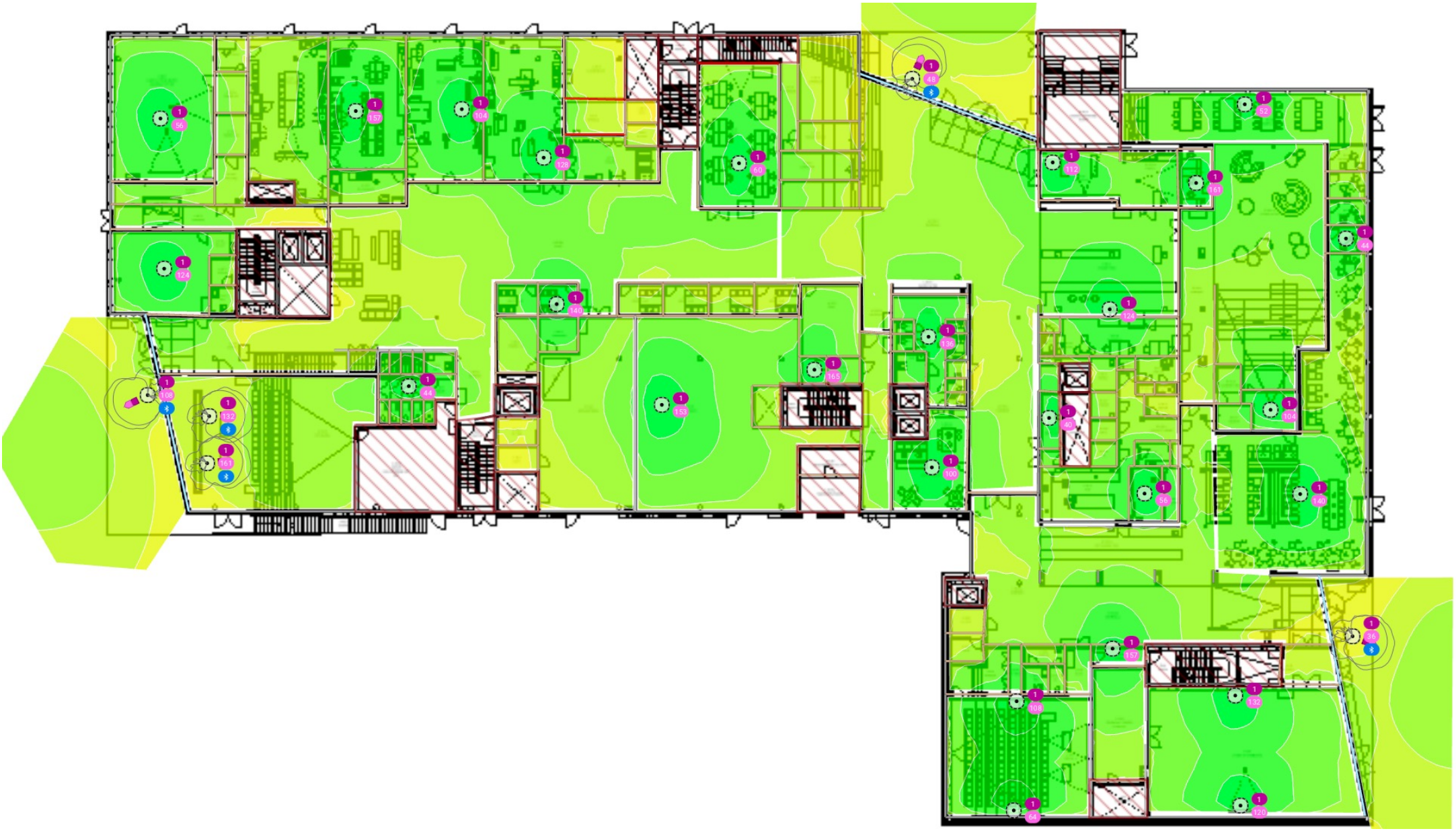
SUNET

SUNET

Wi-Fi

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

SUNET



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

SUNET

Wi-Fi

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

SUNET

Brandvägg

SUNET

Brandvägg

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

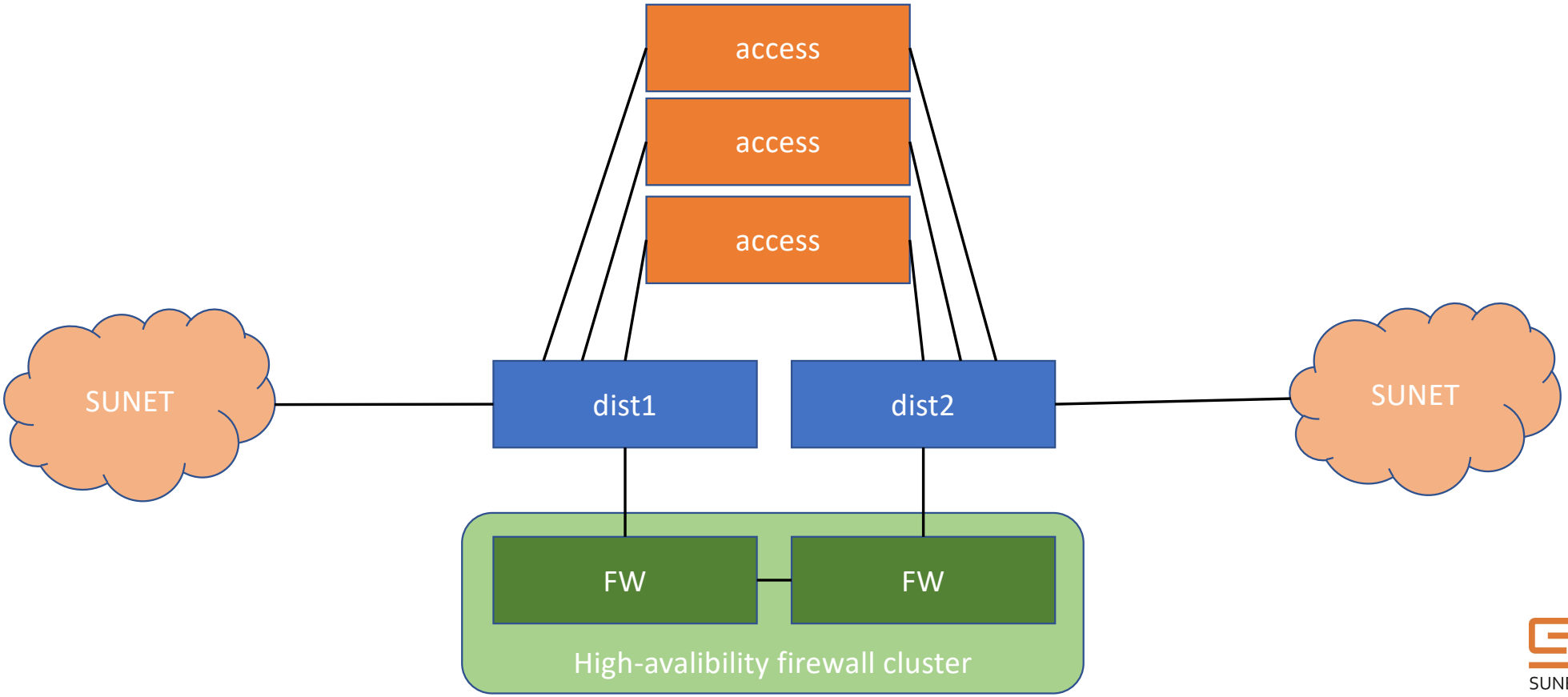
SUNET

Brandvägg

- Sunet hjälper till med designen

SUNET

Firewall on-a-stick



SUNET

Brandvägg

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

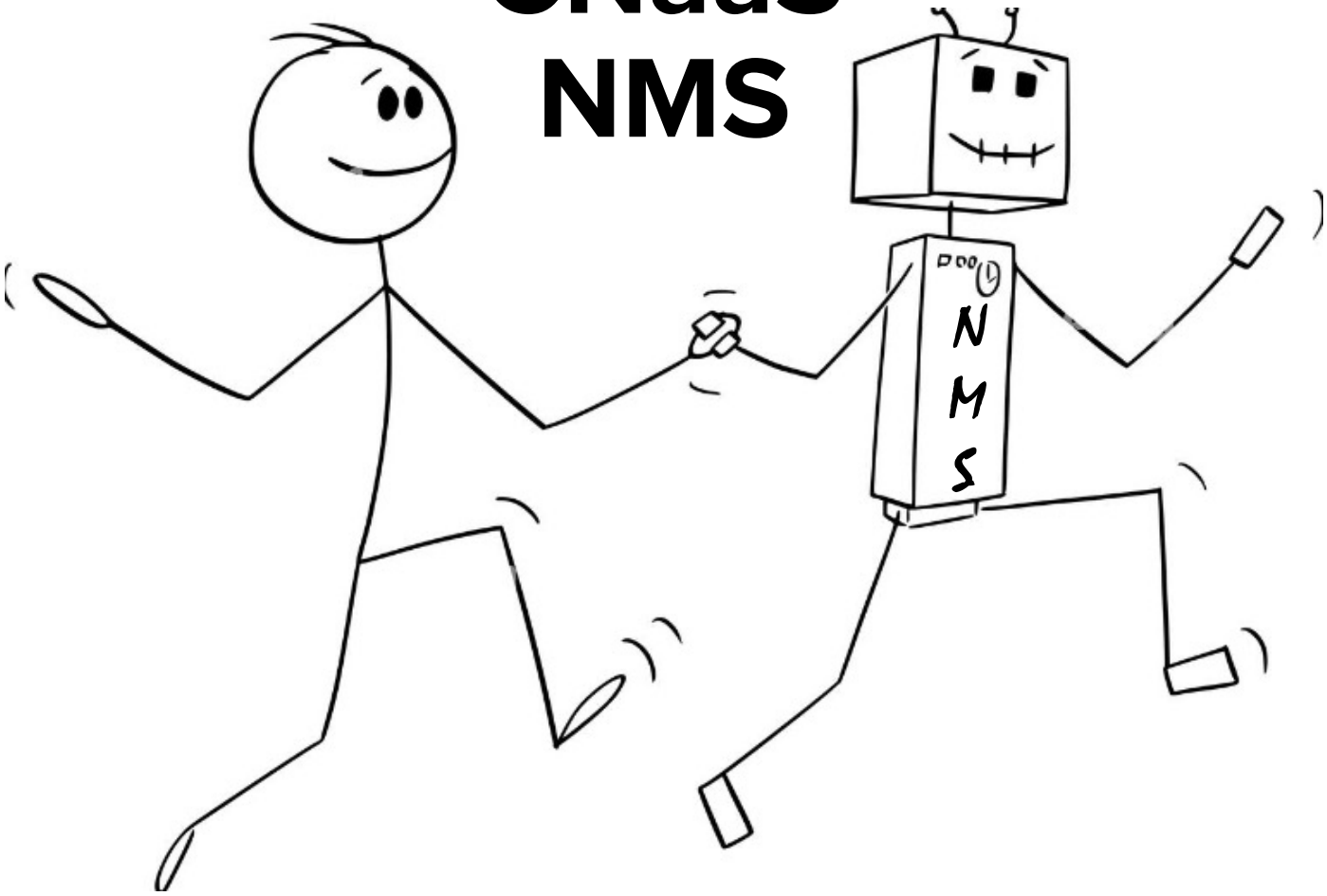
SUNET

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

SUNET

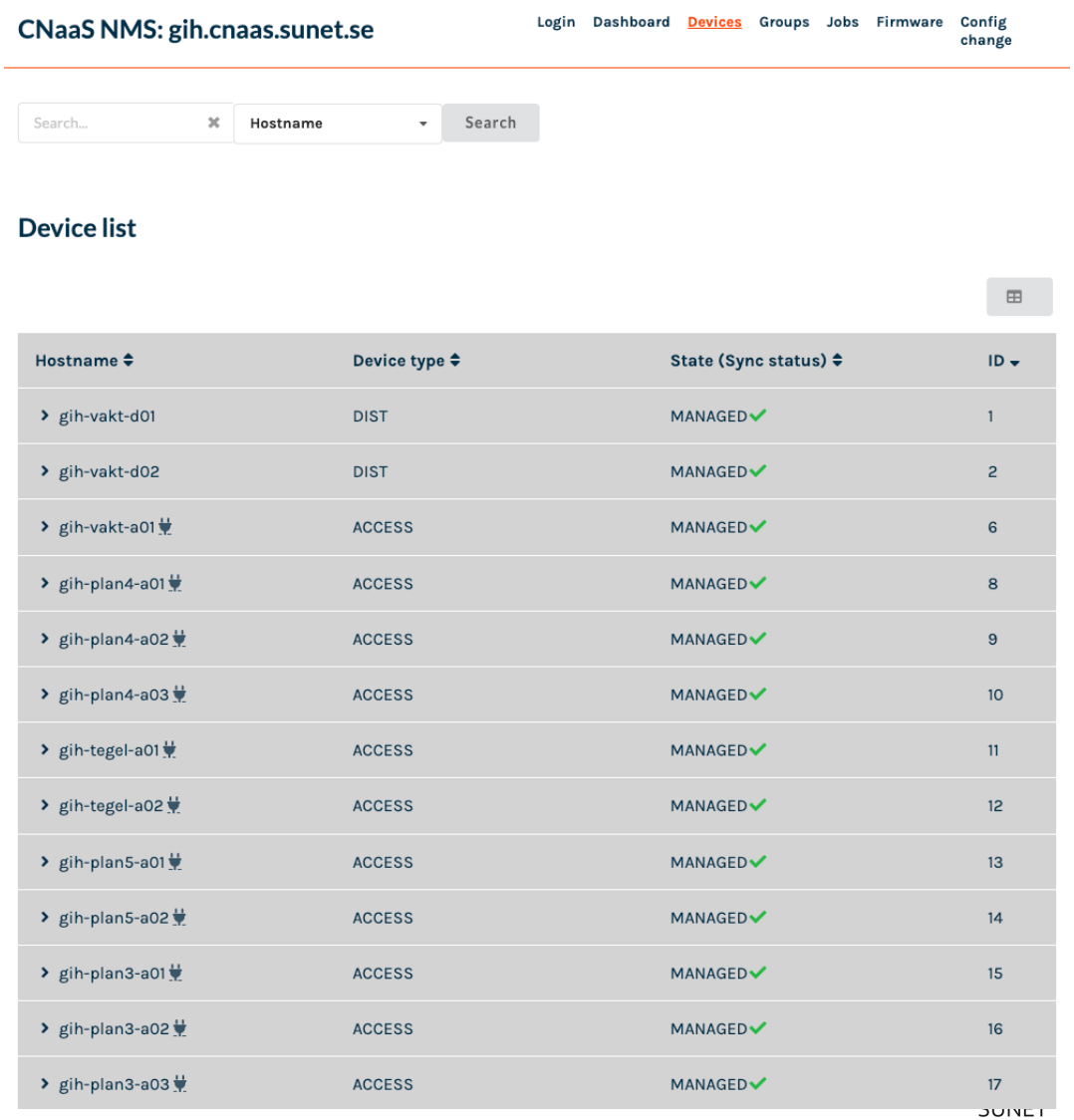
CNaaS NMS



SUNET

Vad är NMS?

- Network management system
  - Zero touch provisioning



Zero Touch Provisioning

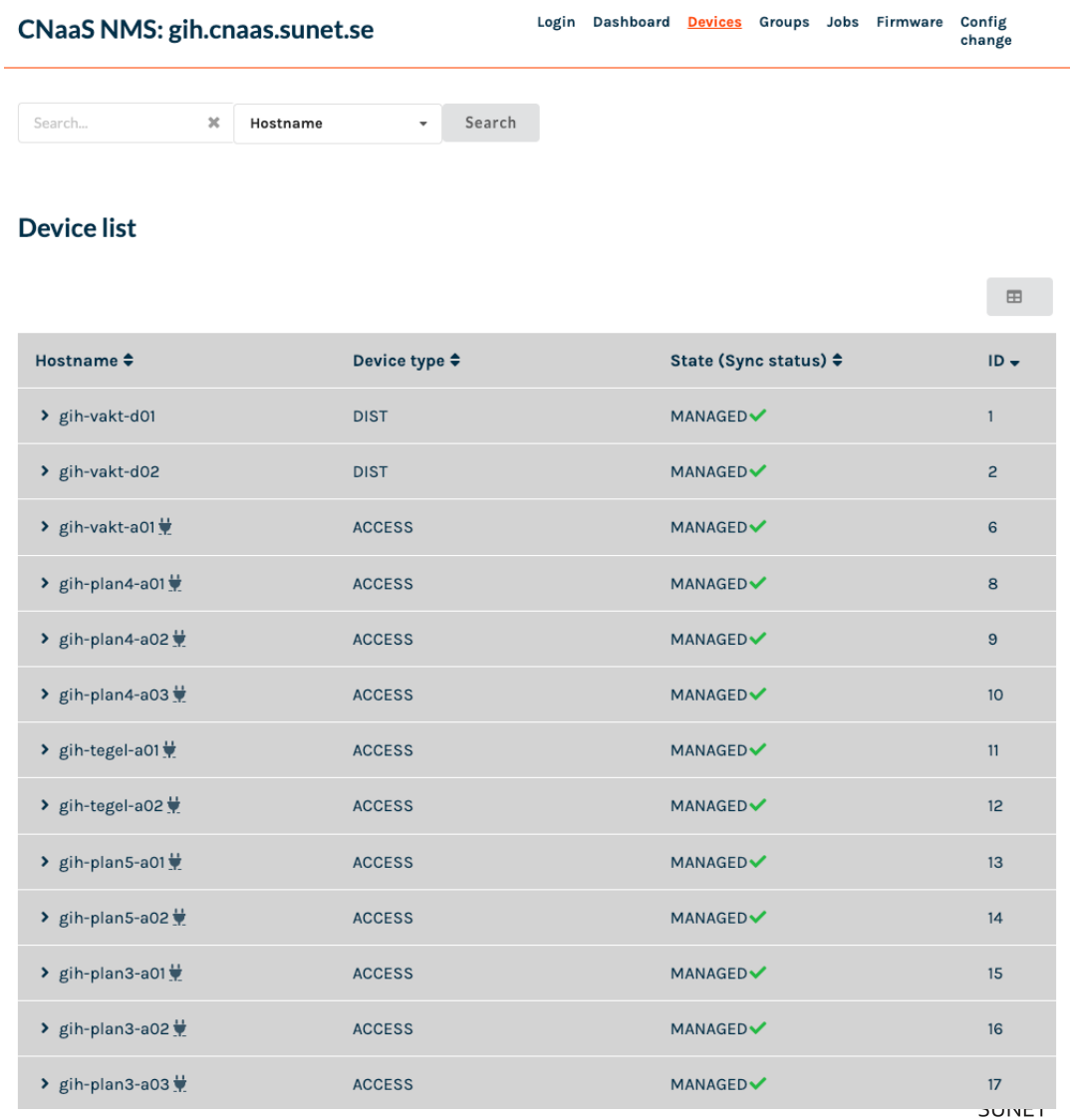
Används vid installation av ny switch (eller utbyte av trasig switch)

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!

SUNET

Vad är NMS?

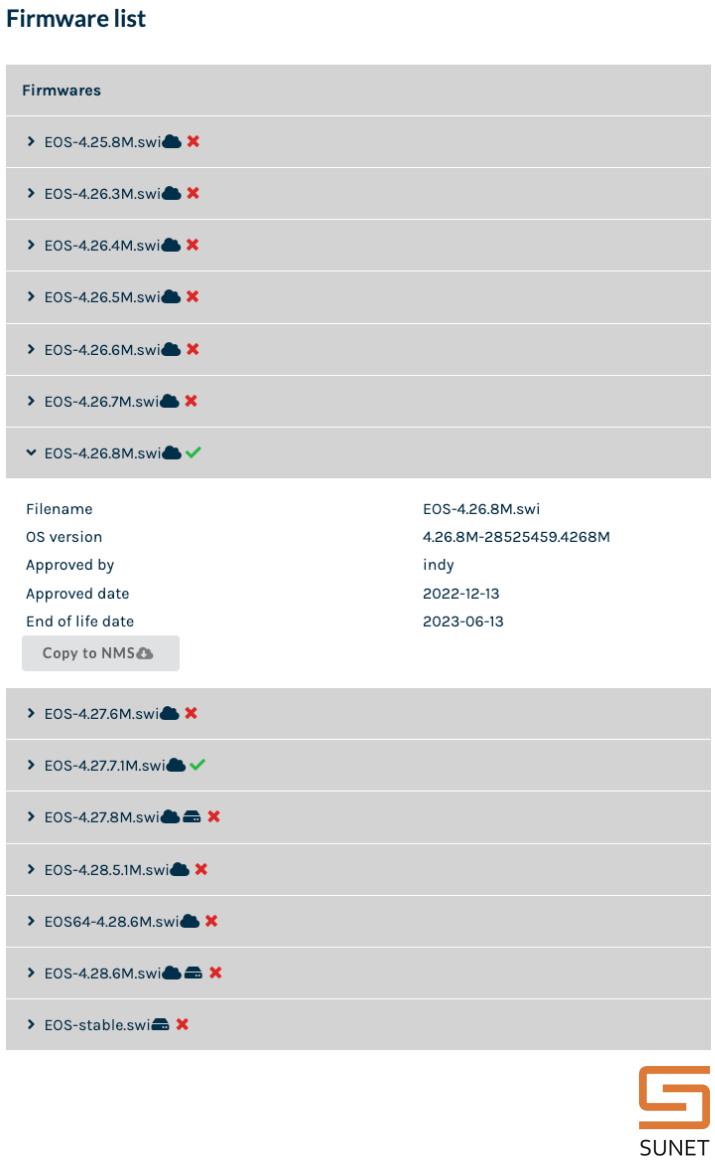
- Network management system
  - Zero touch provisioning
  - Uppgradera mjukvaran



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!

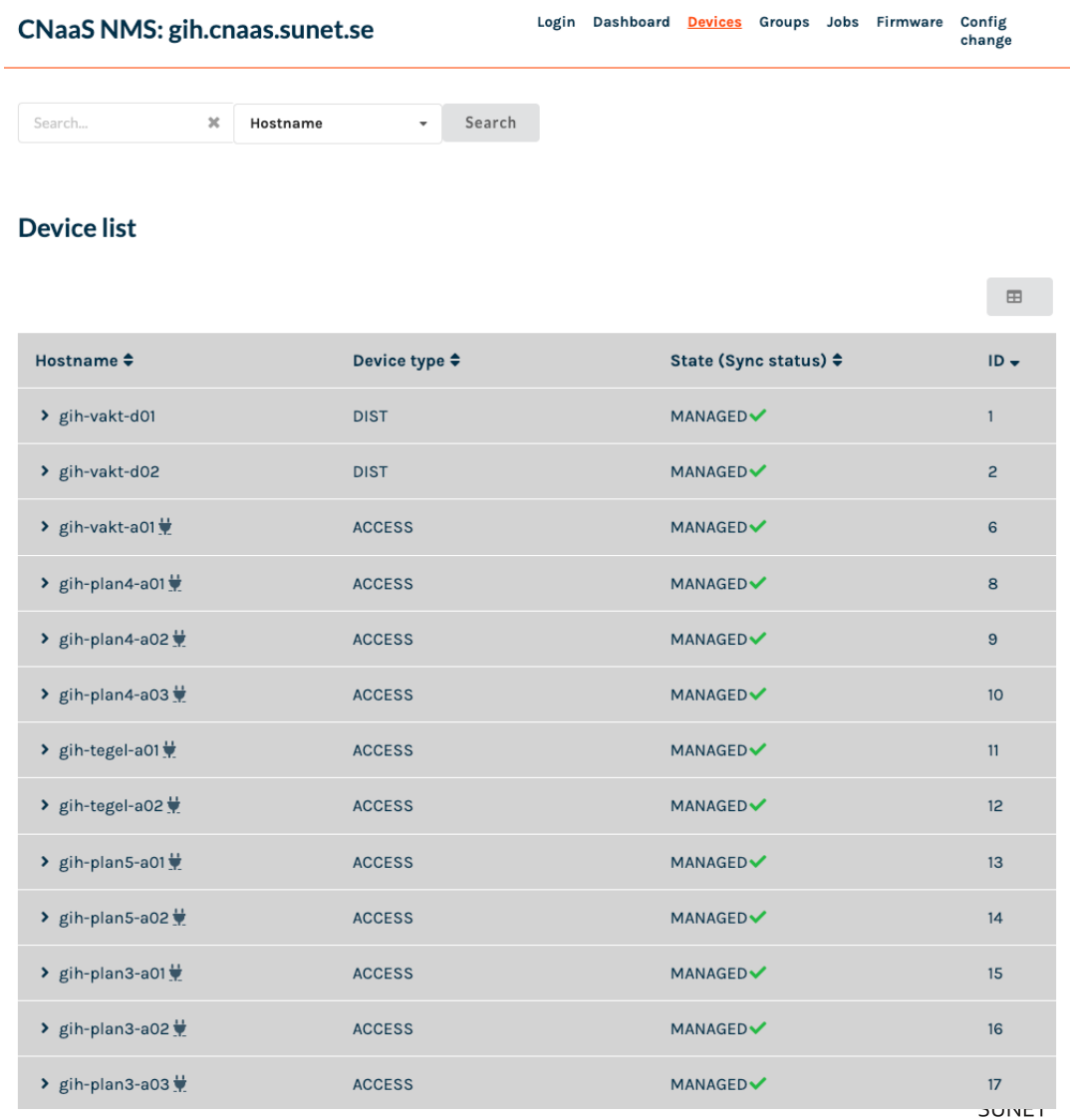
Kan även göras på grupper av switchar



SUNET

Vad är NMS?

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



Hur gör man en konfigurationsändring?

1) Gör dina ändringar på platform

SUNET

Vad är då platform?

Platform är en webbaserat verktyg för konfigurationshantering

Man gör sina konfigurationsändringar i yaml-filer på platform

Versionshantering osv

Varje kund får en slice för sin konfig

Står lokalt på Sunet

53 lines | 1.2 KiB | YAML

```yaml
---
interfaces:
  - name: Ethernet25
    ifclass: downlink
  - name: Ethernet27
    ifclass: downlink
  - name: Ethernet47
    ifclass: downlink
  - name: Ethernet48
    ifclass: downlink
  - name: Ethernet40
    ifclass: custom
    config: |-
      no switchport
      description orval.sunet.se (MGMT)
  - name: Ethernet40.10
    ifclass: custom
    config: |-
      encapsulation dot1q vlan 10
      vrf MGMT
      ip address 10.103.0.1/31
      description orval.sunet.se (MGMT)
  - name: Ethernet40.11
    ifclass: custom
    config: |-
      encapsulation dot1q vlan 11
      vrf STUDENT
      ip address 10.103.0.3/31
      description orval.sunet.se (STUDENT)
  - name: Ethernet42
    ifclass: custom
    config: |-
      description ixia-switch port14
      switchport mode access
      switchport access vlan 225
```

SUNET

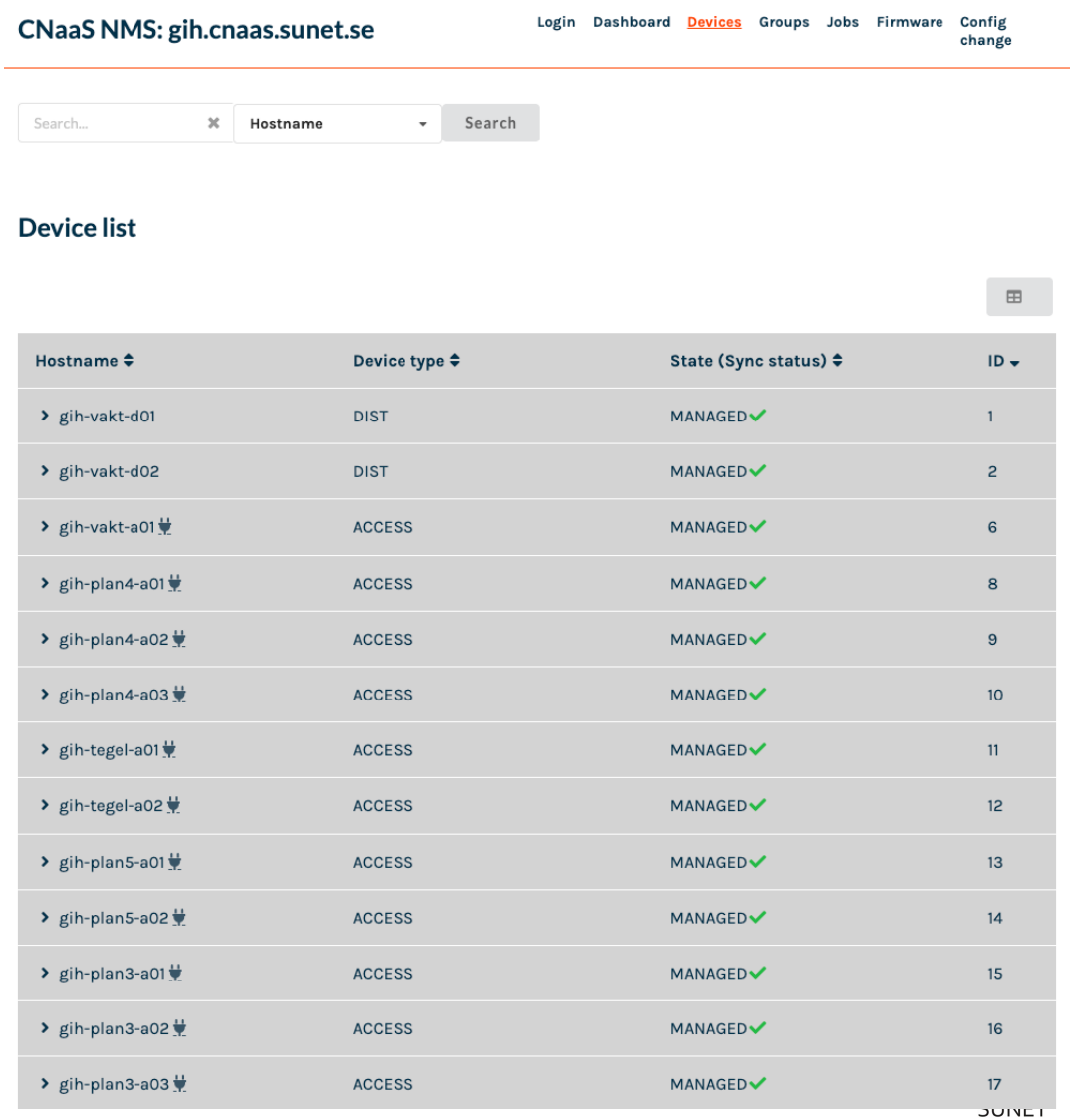
Hur gör man en konfigurationsändring?

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!

SUNET

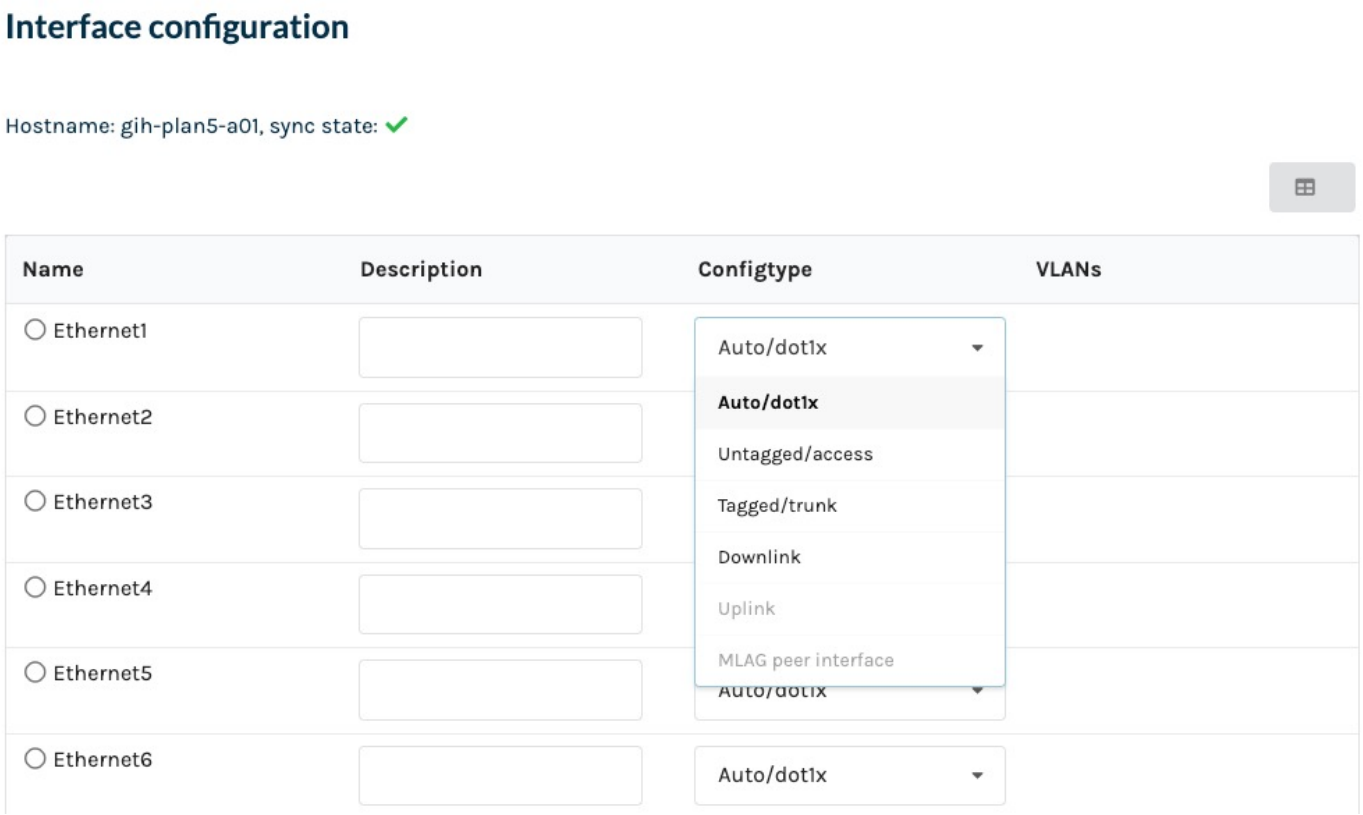
Vad är NMS?

- Network management system
  - Zero touch provisioning
  - Uppgradera mjukvaran
  - Konfiguration
  - Portspecifik konfiguration



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”



SUNET

NAC
RADIUS och 802.1X

SUNET

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.

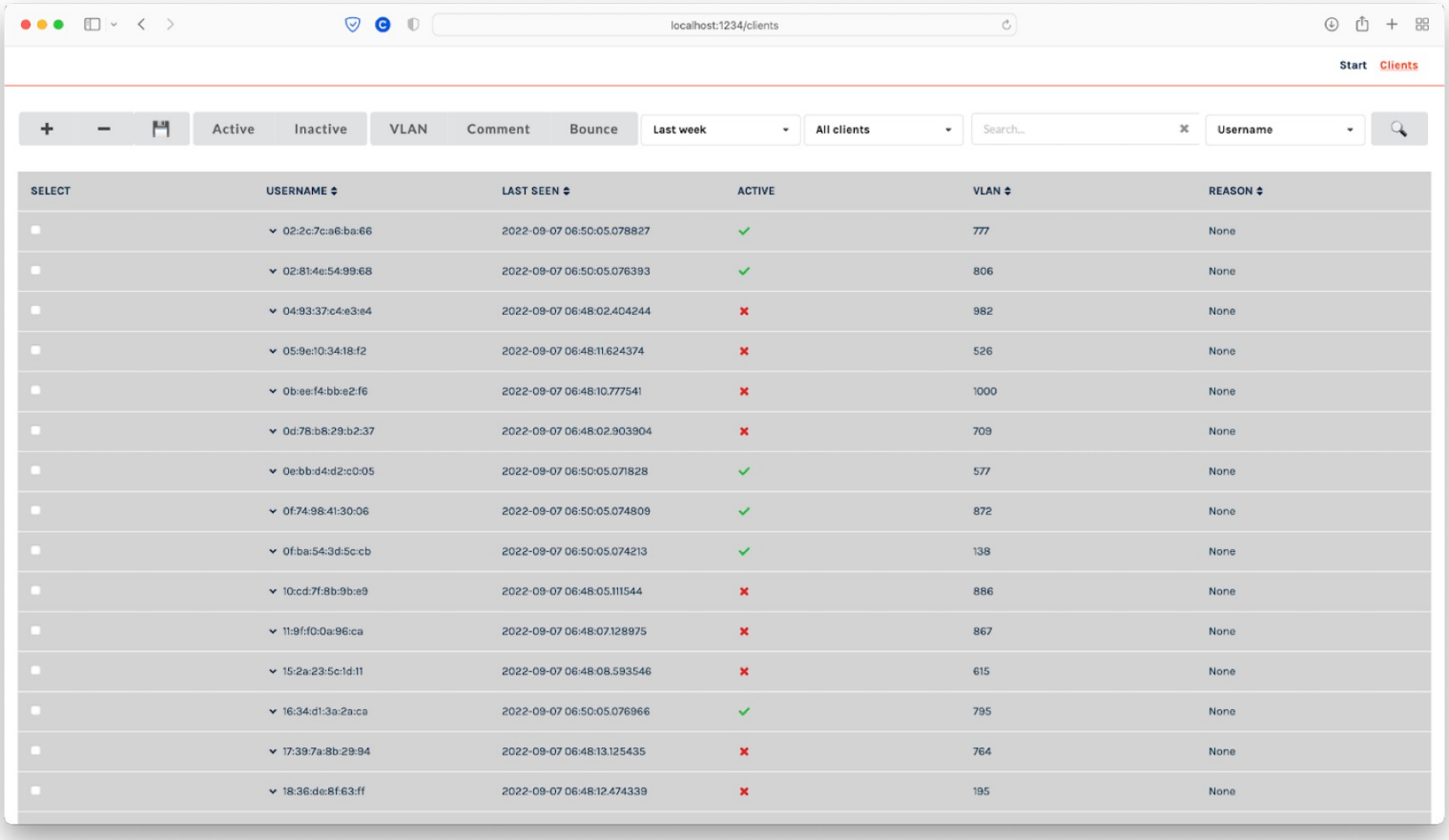
SUNET

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

SUNET

NAC

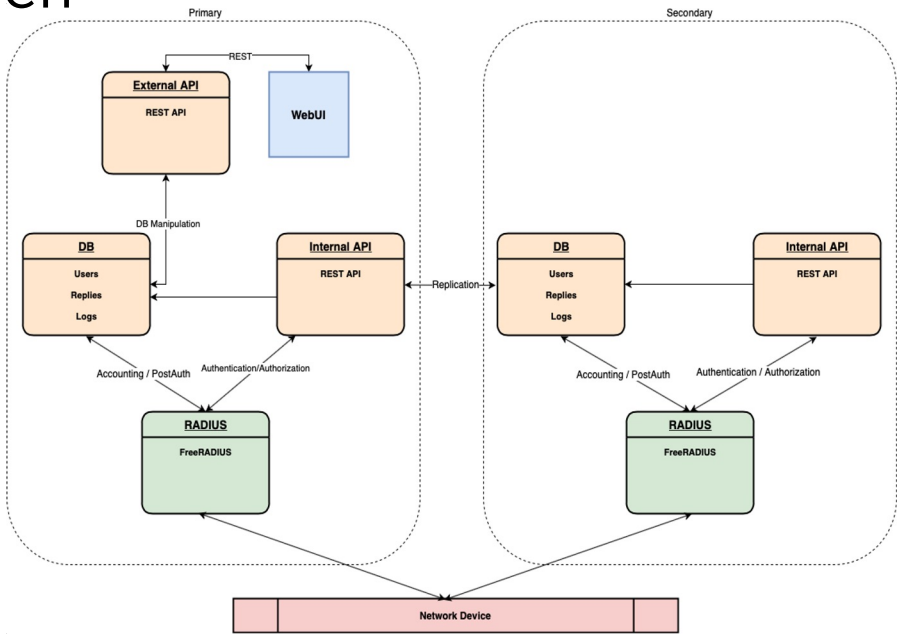


SELECT	USERNAME	LAST SEEN	ACTIVE	VLAN	REASON
	02:2c:7c:a6:ba:66	2022-09-07 06:50:05.078827	✓	777	None
	02:81:4e:54:99:68	2022-09-07 06:50:05.076393	✓	806	None
	04:93:37:c4:e3:e4	2022-09-07 06:48:02.404244	✗	982	None
	05:9e:10:34:18:f2	2022-09-07 06:48:11.624374	✗	526	None
	0b:ee:f4:bb:e2:f6	2022-09-07 06:48:10.777541	✗	1000	None
	0d:78:b8:29:b2:37	2022-09-07 06:48:02.903904	✗	709	None
	0e:bb:d4:d2:c0:05	2022-09-07 06:50:05.071828	✓	577	None
	0f:74:98:41:30:06	2022-09-07 06:50:05.074809	✓	872	None
	0f:ba:54:3d:5c:cb	2022-09-07 06:50:05.074213	✓	138	None
	10:cd:7f:8b:9b:e9	2022-09-07 06:48:05.111544	✗	886	None
	11:9f:f0:0a:96:ca	2022-09-07 06:48:07.128975	✗	867	None
	15:2a:23:5c:1d:11	2022-09-07 06:48:08.593546	✗	615	None
	16:34:d1:3a:2a:ca	2022-09-07 06:50:05.076966	✓	795	None
	17:39:7a:8b:29:94	2022-09-07 06:48:13.125435	✗	764	None
	18:36:de:8f:63:ff	2022-09-07 06:48:12.474339	✗	195	None

SUNET

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

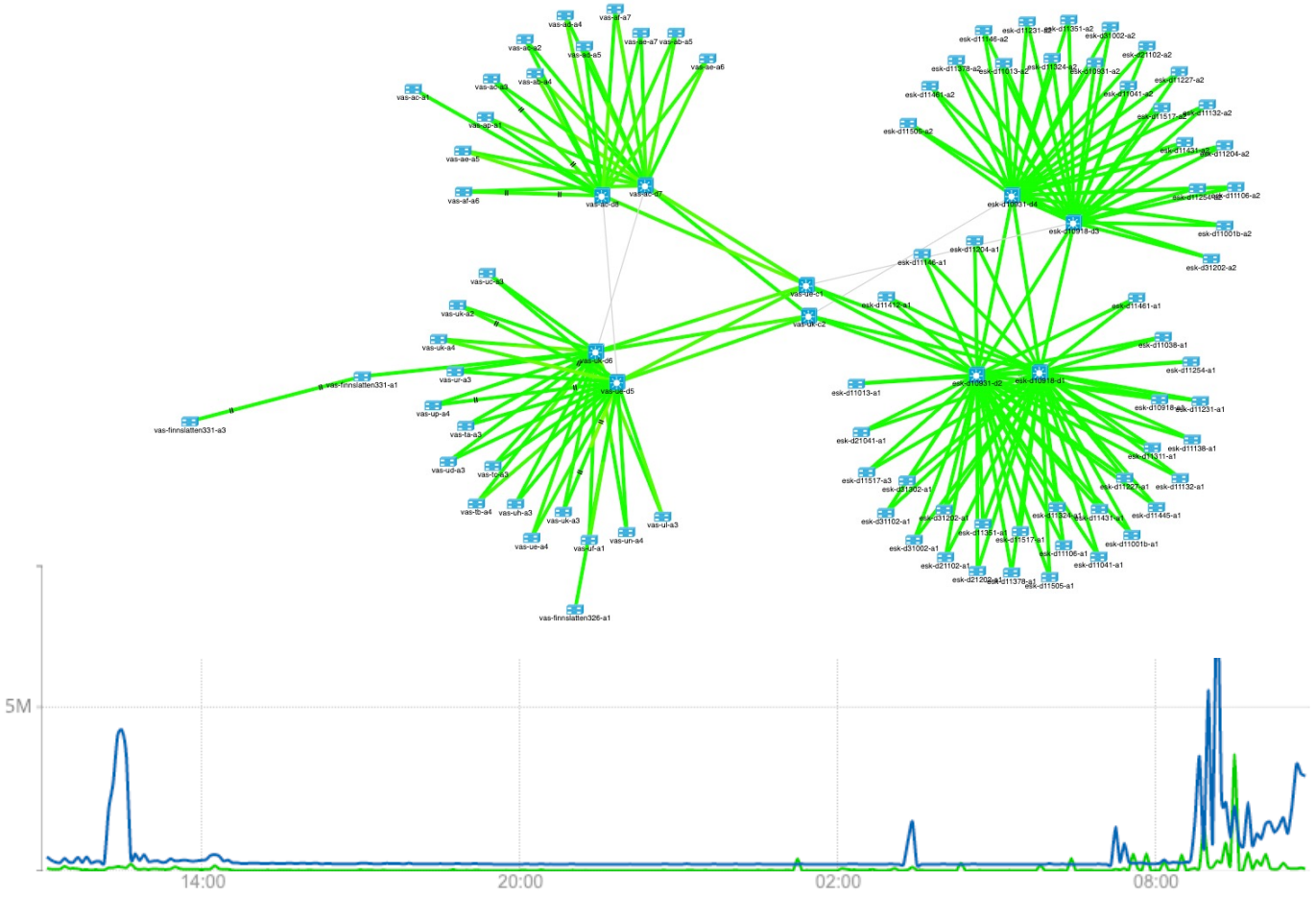
Övervakning

SUNET

SUNET NOC

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

- Nätövervakning
- Larm
- Statistik
- Topologi



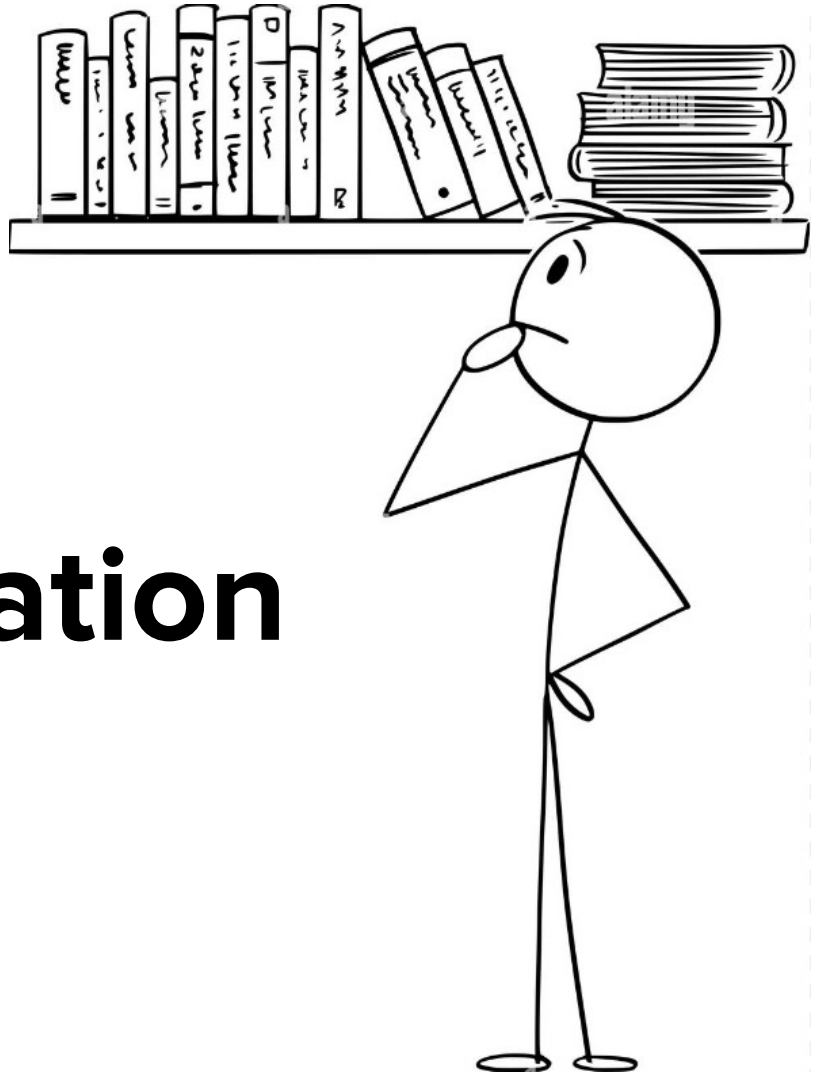
SUNET

Nagios®

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

SUNET

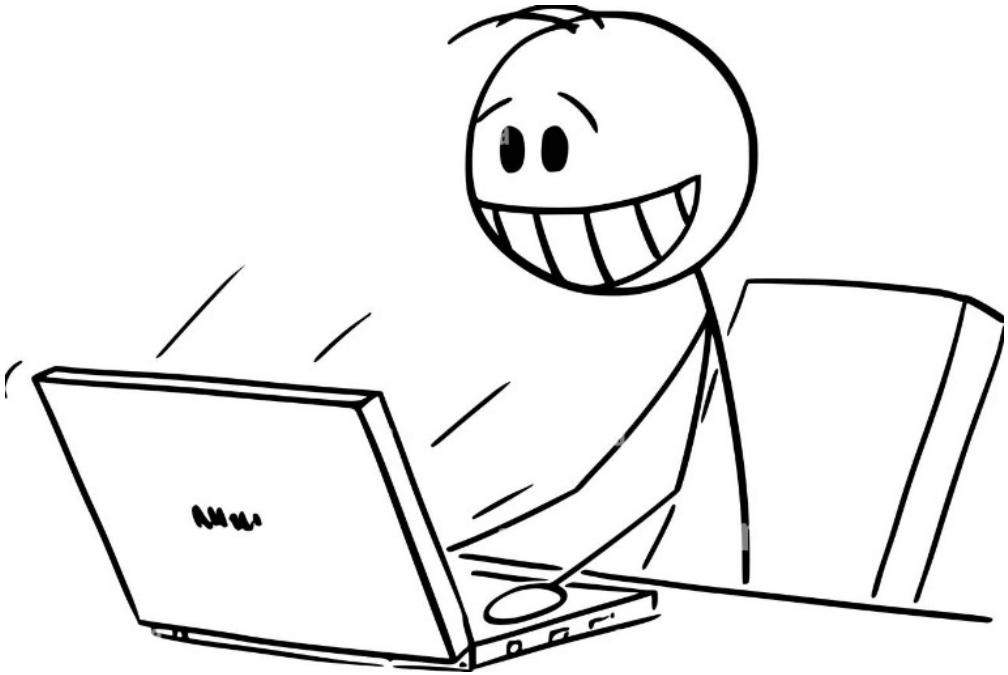
Dokumentation



SUNET

wiki.sunet.se/display/CNaaS

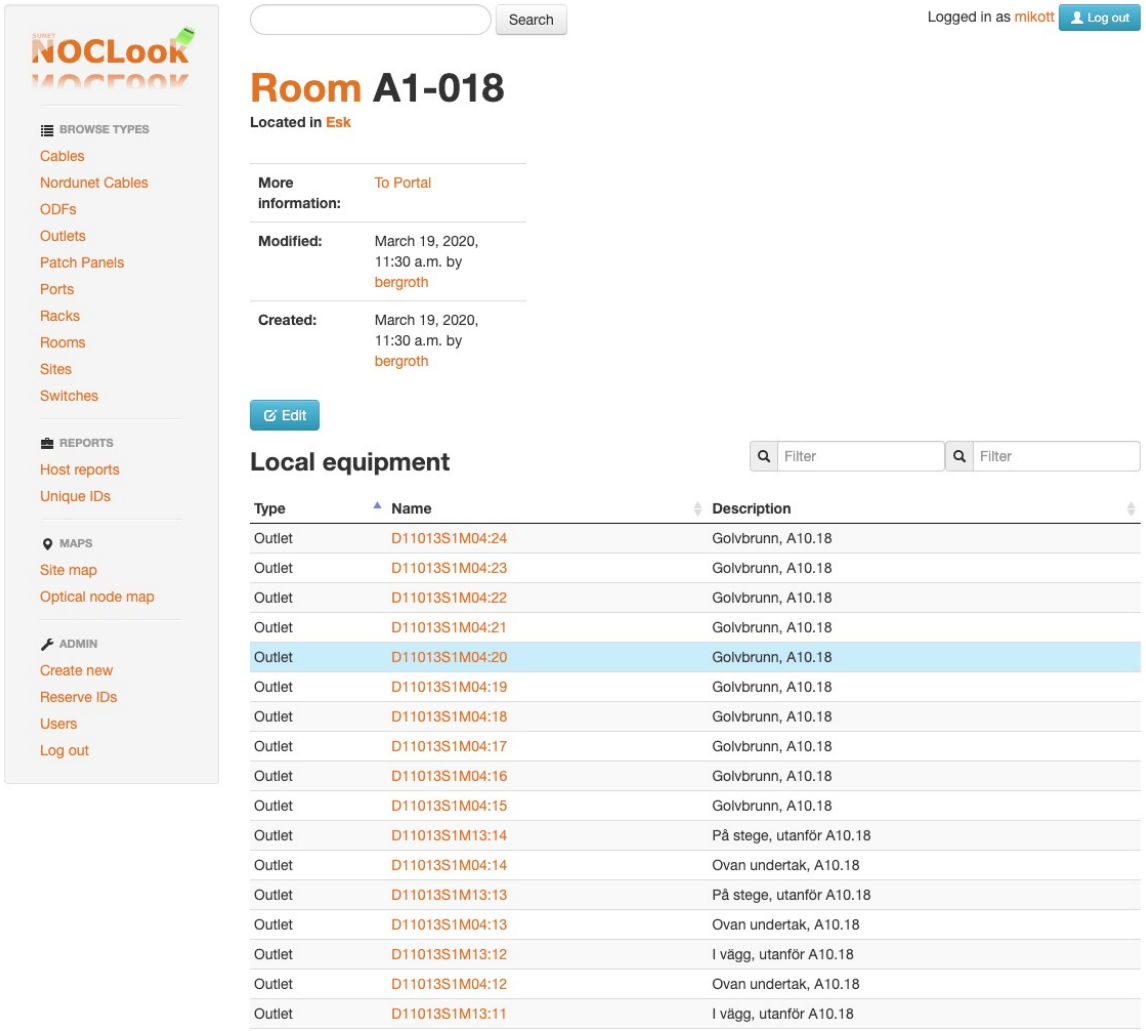
- Innehåller dokumentation för de applikationer som ingår
- Designdokument
- IP/VLAN-planer
- Eskaleringsvägar
- En hel del How-to guider



SUNET

NI

- Dokumentation av nätet



SUNET

IPAM - Netbox

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

SUNET

Övrigt

SUNET

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

SUNET

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

SUNET

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

SUNET

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, supporteskaleringar, implementation eller livscykelhantering.

SUNET

Vem har då campusnät idag?

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

SUNET

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

SUNET

Frågor?

mikott@sunet.se
david@sunet.se
https://sunet.se/services/nat/campusnat-cnaas

SUNET