

IOTROAM

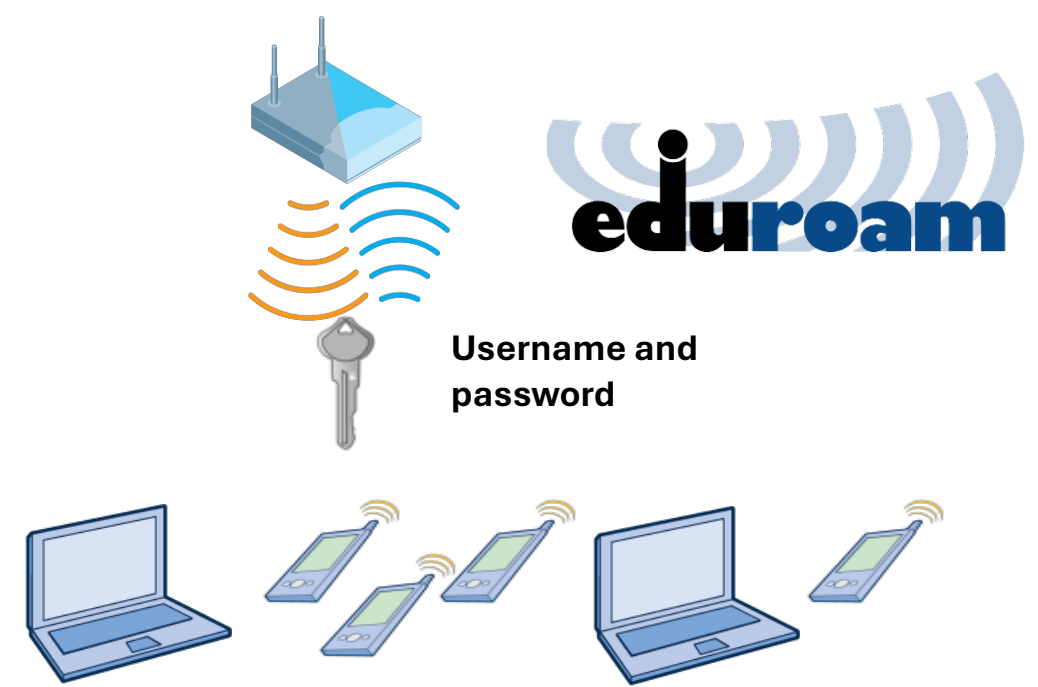
SURF-club
Receptie

SURF



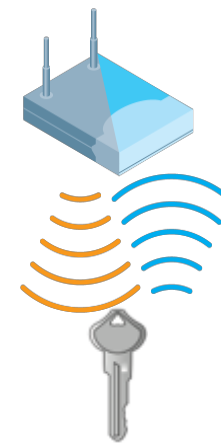
IoT and Enterprise Wi-Fi

- What kind of devices do we have on the Wi-Fi network
 - Notebooks
 - Smartphones
 - Tablets
 - Etc.

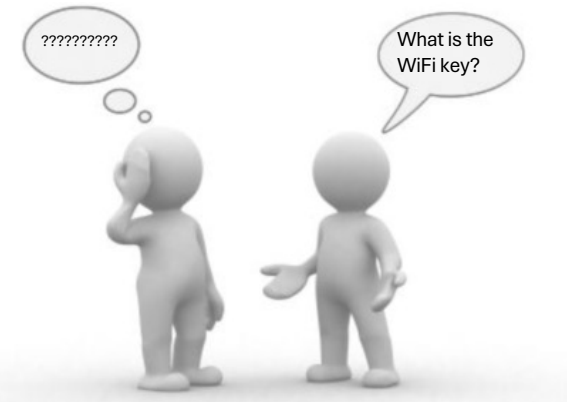


IoT and Enterprise Wi-Fi

- What kind of IoT devices are we expecting on the Wi-Fi
 - Motionsensors
 - Air quality sensor
 - Smart watches
 - Beamers/smartscreens
 - Virtual reality glasses
 - Gameconsoles
 - Vending machines
 - Security camera's
 - Washing machine
 - Doorbell
 - Etc.



Username and password



IoT and Enterprise Wi-Fi

- Why

- Devices often support only PSK authentication because they are designed for simplicity, low power consumption, and to operate on consumer networks where complex, enterprise-grade authentication is unnecessary or impractical. This is particularly common in IoT (Internet of Things) devices, such as smart sensors, printers, and smart home appliances.

- PSK (Pre-Shared Key)

- Benefit

- Recognizable and easy for users, already experience with it from home

- Disadvantage

- One key for everyone
- No traceability (who is the owner)
- Same network policy, same vlan
- When publicly known a disaster to replace in an enterprise



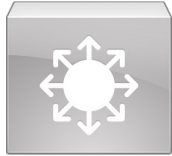
IoT and Enterprise Wi-Fi

- What do you want in an enterprise network
 - Unique psk (still not 100% safe)
 - Per device (per device group) registration
 - Different network policies per device or group
 - Traceability to a responsible person
 - When publicly known, you don't have to change all the other devices
 - Recognizable and easy for users
 - 1 ssid for the entire campus(maybe even further)
 - Proper documentation and administration



Wireless environment

Aruba
education institution A



Cisco
education institution B

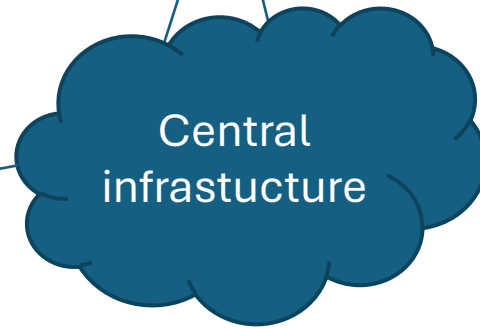
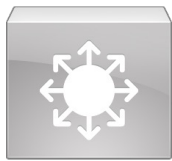


Per device:
a mac address, Pre shared key,
description, and education
institution where it belonged to.
Per institution:
a radius profile with specific
response settings.

Wireless environment

Aruba
education institution A

Cisco
education institution B



Per device:
a mac address, Pre shared key,
description, and education
institution where it belonged to.
Per institution:
a radius profile with specific
response settings.

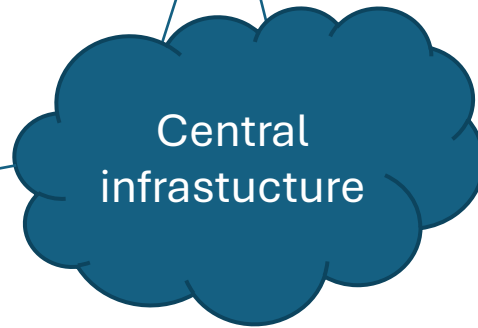
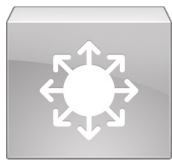
Registration page

Database:
Mac address, preshared key,
description, education institution

Wireless environment

Aruba
education institution A

Cisco
education institution B



Registration page

Database:
Mac address, preshared key,
description, education institution

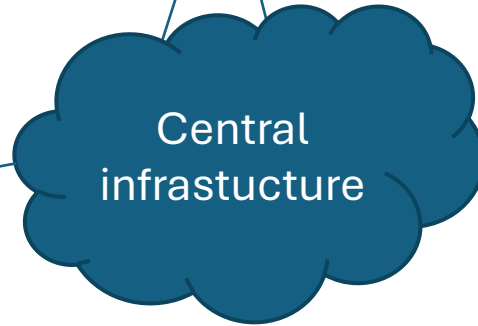
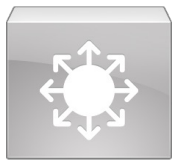
Cisco:
Lookup in database for the key that
belong to the mac adres
Radius reply:
Acces Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk="unique psk"
Cisco-av-pair = role=IoT

Optional:
Radius:IETF:User-Name = "sponsor
username or description"

Wireless environment

Aruba
education institution A

Cisco
education institution B



Registration page

Database:
Mac address, preshared key,
description, education institution

Aruba:
Lookup in database for the key that belong to the mac adres
Radius reply:
Acces Type = ACCESS_ACCEPT
Radius: Aruba: Aruba-MPSK-
Passphrase = "unique psk"
Radius: Aruba: Aruba-User-Role =
"device role"

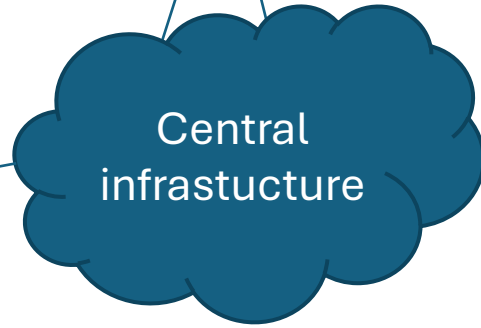
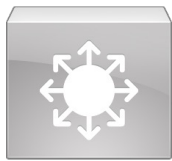
Optional:
Radius:IETF:User-Name = "sponsor
username or description"

Wireless environment

Request during the test:
Can devices belong to a group?

Aruba
education institution A

Cisco
education institution B



Per device:
a mac address, Pre shared key,
description, owner or group and
education institution where it
belonged to.
Per institution:
a radius profile with specific
response settings.

Registration page

Database:
Mac address, preshared key,
description, education institution

IoT and Enterprise wifi

- What kind of IoT devices are we expecting on the wifi
 - Motionsensors
 - Air quality sensor
 - Smart watches
 - Beamers/smartscreens
 - Virtual reality glasses
 - Gameconsoles
 - Vending machines
 - Security camera's
 - Washing machine
 - Doorbell
 - Etc.



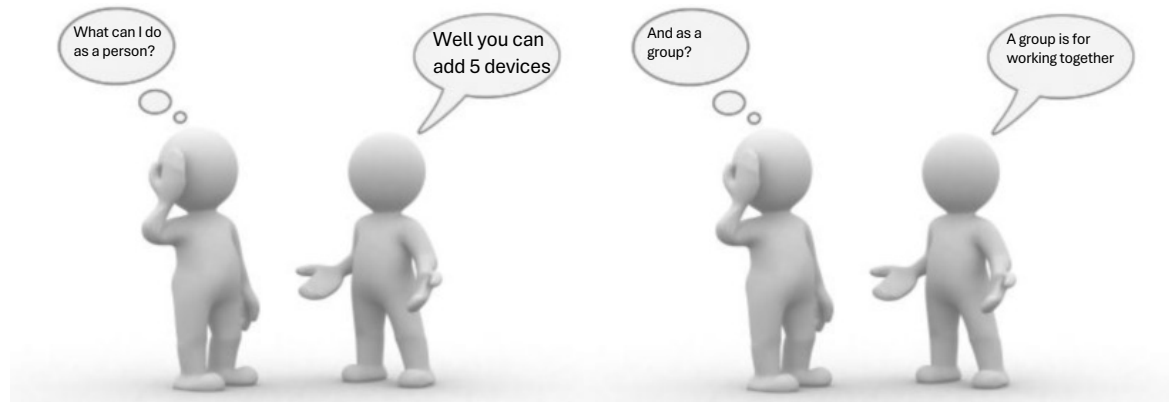
IoT and Enterprise wifi

- Per person

- Maximum of 5(non 802.1x) devices
- Every device is registered with mac address and a unique pre shared key(psk)
- Discouragement ssid(not for a laptop or phone)
 - Think of bandwidth limitation, etc.
- After 3 months not online automatic deletion




- As group

- No limit of amount of devices
- Unique psk for the whole group
- Every mac address is registered.
- A policy for the whole group
- Traceability to a responsible person
- Recognition and convenience for users
- Proper registration of devices
- Working together and shared responsible as a group
- 1 ssid on the campus for all the IoT devices
- (optional)No expiration date for the devices



IoT and Enterprise wifi

GROUP CAMERA

User 1		SSID: iotroam psk: famm6cpR mac: 00:1B:44:11:3A:B7
User 2		SSID: iotroam psk: famm6cpR mac: 00:1B:44:11:3A:C1
User 3		SSID: iotroam psk: famm6cpR mac: 00:1B:44:11:3A:B8

User 6



SSID: iotroam
psk: MMQrPq2
mac: 00:1B:44:11:3A:A7

User 5



SSID: iotroam
psk: UUiV12a
mac: 00:1B:44:11:3A:87

User 4



SSID: iotroam
psk: Yyh59ar
mac: 00:1B:44:11:3A:B6



SSID: iotroam
Authentication: WPA2 Personal
psk: *
Userprofile A VLAN 10 and FW-Policy-5



SSID: iotroam
Authentication: WPA2 Personal
psk: *
Userprofile B VLAN 25 and FW-Policy-2



SSID: iotroam
Authentication: WPA2 Personal
psk: *
Userprofile B VLAN 255 and FW-Policy-255

IoT and Enterprise wifi

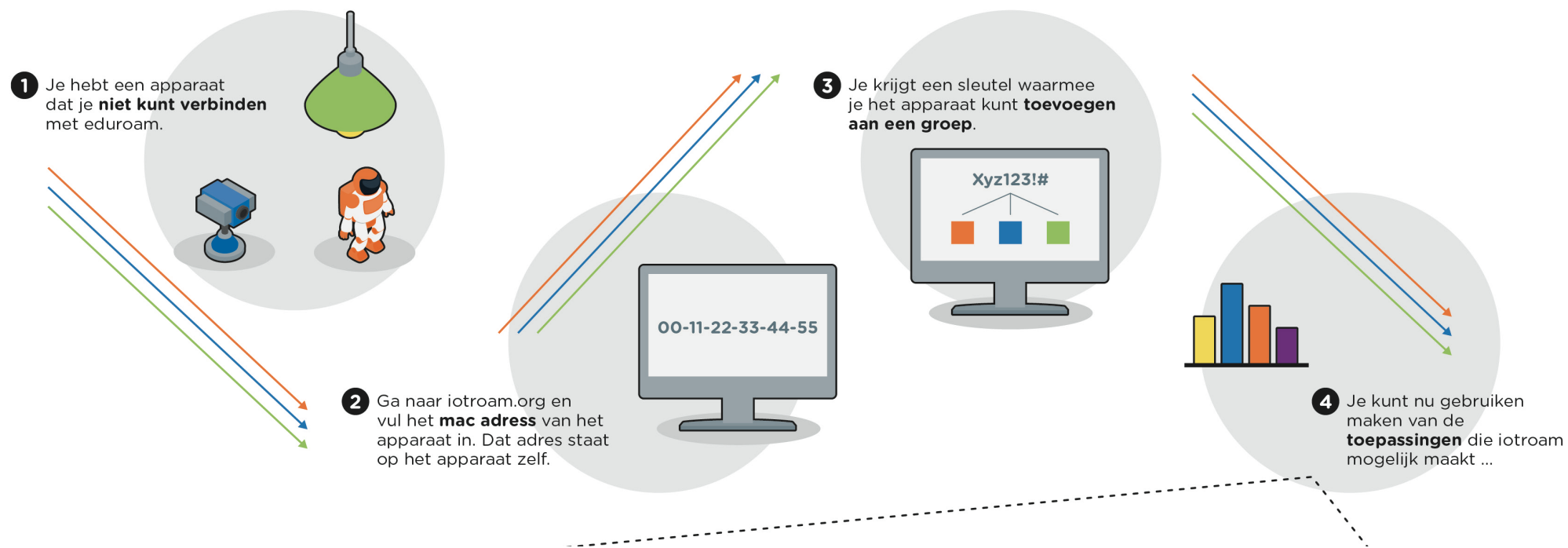
Internet of Things: Gemak dient de mens

SURF werkt aan een Internet of Things netwerk: iotroam. Aan dit netwerk worden apparaten gekoppeld die met het internet zijn verbonden en online gegevens verzenden, zoals smartwatches, digiborden, frisdrankautomaten, enzovoort. Hoe werkt dit precies? En wat kun je ermee?

Een apparaat verbinden met iotroam

De apparaten zijn ingedeeld per groep:

- Groep 1: iot devices. Dit zijn persoonlijke apparaten, zoals bijvoorbeeld een smartwatch.
- Groep 2: ICT devices. Dit zijn apparaten waarvoor de afdeling ICT verantwoordelijk is, zoals bijvoorbeeld een digibord.
- Groep 3: gebouwbeheer. Dit zijn apparaten waarvoor de afdeling gebouwbeheer verantwoordelijk is, zoals bijvoorbeeld een frisdrankautomaat.



IoT and Enterprise wifi

Het gemak van iotroom

De apparaten zijn ingedeeld per groep:

- Groep 1: iot devices
- Groep 2: ICT devices
- Groep 3: gebouwbeheer

Wifi access point



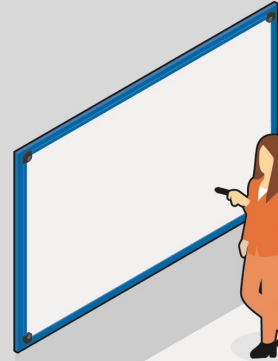
Vergader camera

- Gebruik wordt bijgehouden
- Melding bij storing/defect



Digibord

- Draadloos streamen van content
- Statusoverzicht gebruik



Lamp

- Branduren worden bijgehouden
- Melding bij storing/defect



Frisdrankautomaat

- Voorraad wordt bijgehouden
- Rapportage gebruik



Robotproject van student

- Kan bestuurd worden met app
- Kan samenwerken met andere studenten



Smartwatch

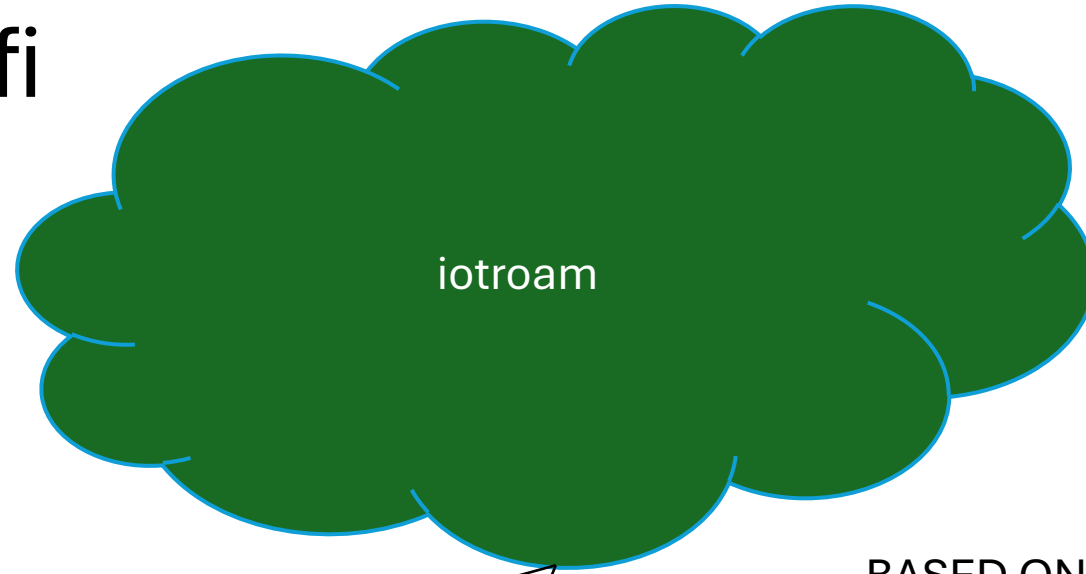
- Meldingen van instelling komen binnen



AED

- Batterij/gezondheidsstatus wordt bijgehouden
- Melding naar BHV bij gebruik

IoT and Enterprise wifi



BASED ON API
FOR CLOSED SYSTEMS

RADIUS BASED

Cisco
Aruba
Juniper Mist
Huwei
Fortinet

