



SURF

Sovereign Campus Networks

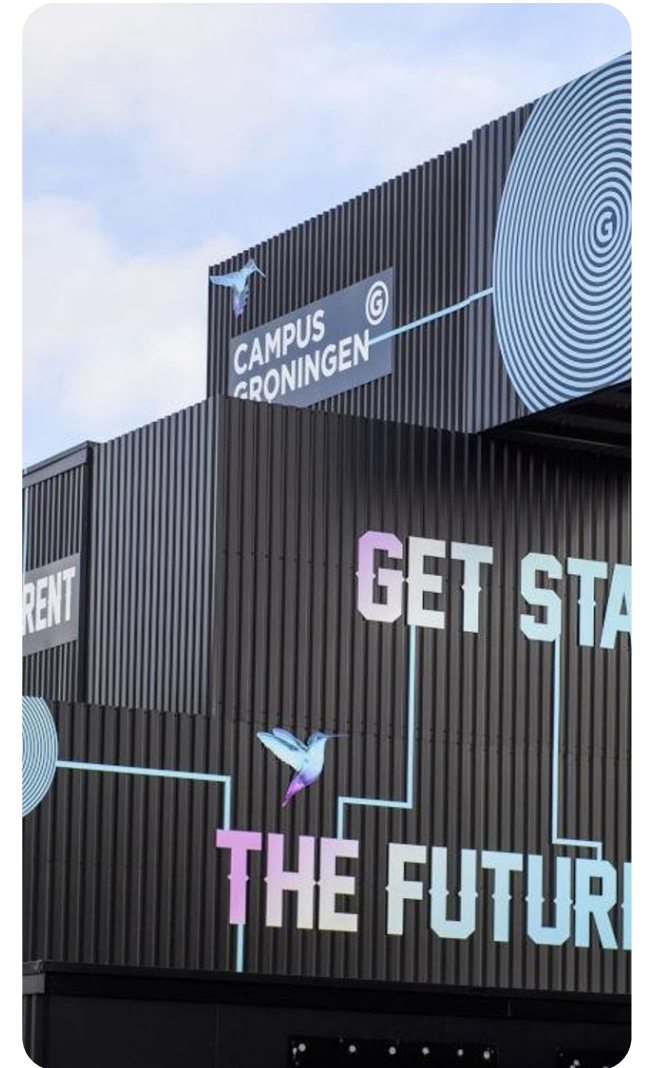
Maurice van den Akker

9/9/2026

| Campus Network trends

Trends on the campus for connectivity needs:

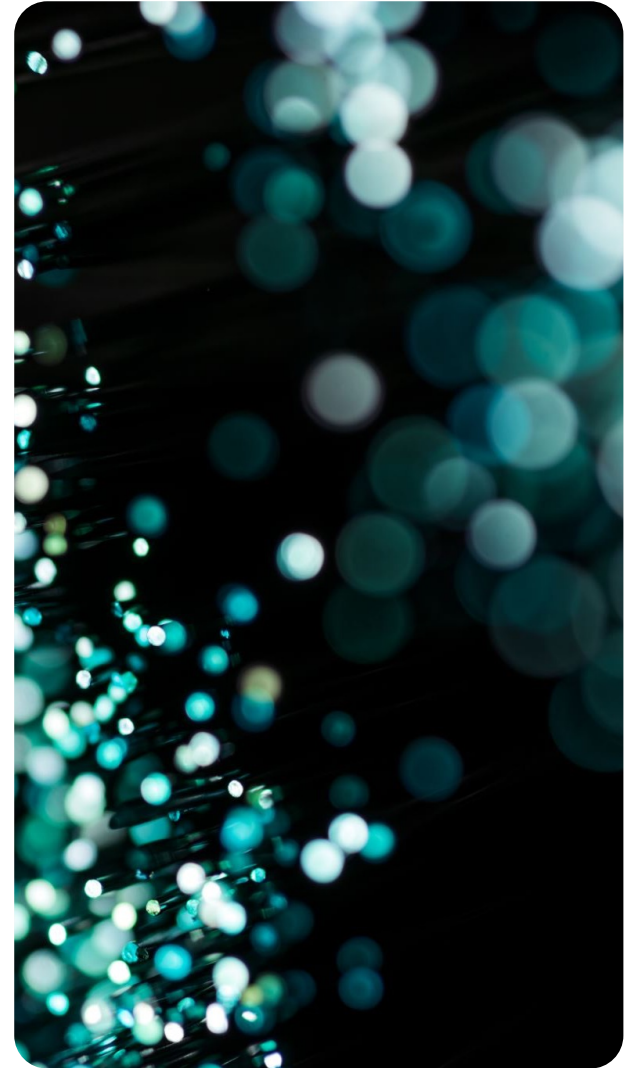
- More users and (type of) devices
- Higher and more variable capacity needs
- Reliable and resilient connectivity: wired/wireless
- Security and segmentation
- Flexibility and interoperability
- Data and infra sovereignty



Challenges

So we have, on the one hand:

- Rapid growth in users, devices, IoT, cloud, AI and data-intensive applications
- Rising requirements for capacity, reliability, low latency and ubiquitous coverage
- Increasing cybersecurity, privacy and data-governance risks



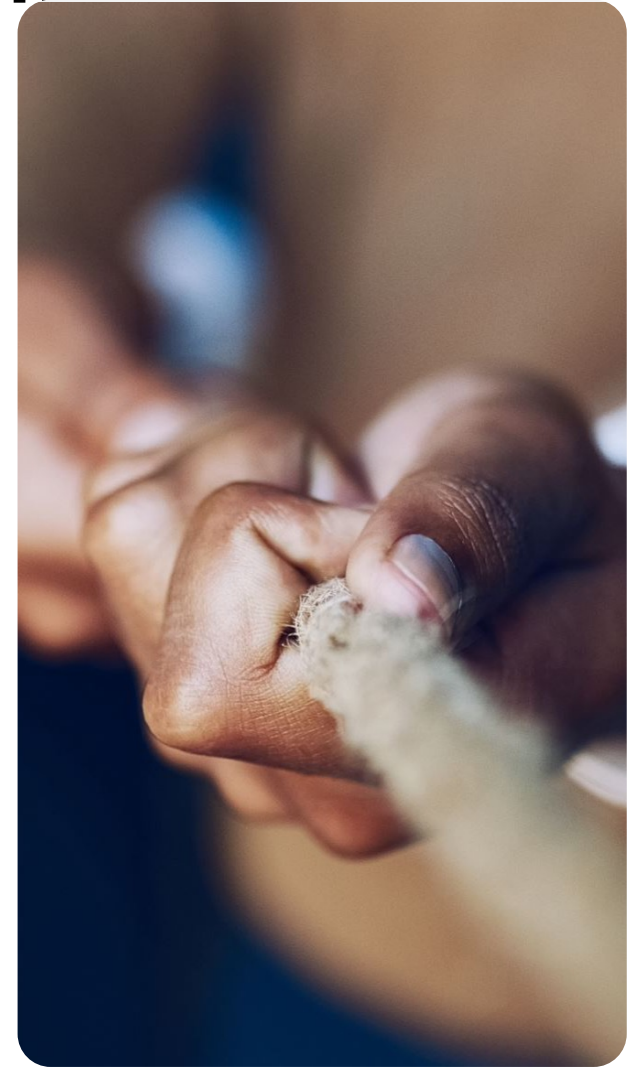
Challenges for campus networks deployments

So we have, on the one hand:

- Rapid growth in users, devices, IoT, cloud, AI and data-intensive applications
- Rising requirements for capacity, reliability, low latency and ubiquitous coverage
- Increasing cybersecurity, privacy and data-governance risks

And on the other hand:

- Legacy infrastructure and costly upgrades
- Shortage of skilled network and security personnel
- Complex, expensive tools and operations
- Dependence on suppliers and risk of vendor lock-in
- Pressure to remain affordable, sustainable and adaptable



Campus networks are of strategic importance

- Dependence of teaching, research, administration, and student services on reliable connectivity
- Increasing expectations for availability, security, mobility, and performance
- Risks of fragmented infrastructure and dependence on a single supplier
- Network services as a combination of technology, policy, operations, and governance

Traditional view	Strategic asset view
Network as utility	Network as institute-wide capability
Focus on hardware/uptime	Focus on mission outcome and resilience
IT-owned infrastructure	Shared institutional platform
Vendor specific systems	Interoperable ecosystem
Reactive support	Proactive automation
Operational expenses	Strategic investment



SURF sees the campus network as strategic critical infrastructure asset, not merely a utility.

it must be scalable, resilient, secure and adaptable to educational and research practices

+

Interoperable and enough sovereign to protect continuity

Reasons for sovereignty

- Reduces migration and licensing costs (after new tender for example)
- Avoids dependence on proprietary data formats and workflows
- Supports multi-vendor environments and future standards
- Protects data ownership during supplier changes
- Allows incremental adoption rather than disruptive replacement



Reasons against sovereignty

- Proven solution from established market party
- Clear support channels
- Faster deployment
- More trust in vendor solutions than in open source community
- More functionality and better user experience

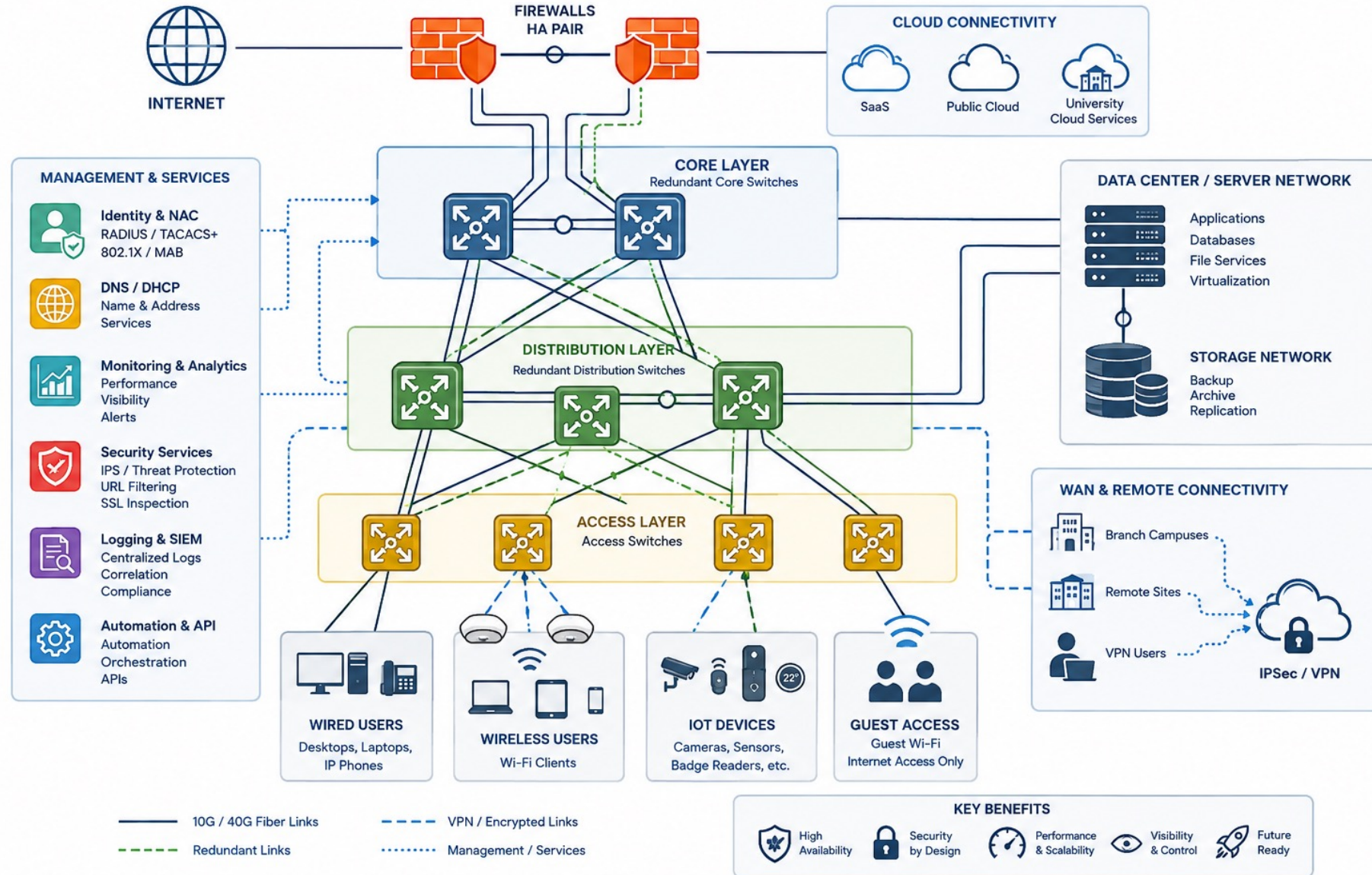


| Strategy in practice: Road to requirements

- **Many options, such as:**
 - Full service / co-creation / do-it-yourself
 - With or without a 3rd party?
 - Open standards/source vs Proprietary
 - Interoperability
- **Many opinions, such as:**
 - Members with high demand (or: eol infra)
 - Member representees (sector level)
 - Engineers
 - Directors / Board

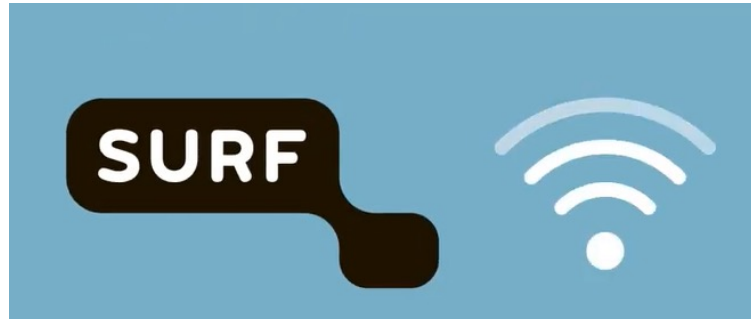


MODERN CAMPUS ARCHITECTURE – COMPLETE VIEW



Pilot time! “as a service”

Many times it is a success



Component
Wi-Fi
eduroam
iotroam
Supported Campus Firewall
VPN
Core, Distribution and Access
Network Access Control
DHCP / DNS / IPAM
IoT network
Indoor 5G/6G Open RAN
CNaaS NMS
Automation, orchestration
Asset Administration systems
Monitoring en alarm aggregation (for 1st, 2nd and 3rd line)

But one time it fails...

- The routing/switching pilots are complex en cost intensive:
 - Goal: see if SURF is able to manage brownfield migration. Challenges:
 - Institutes have legacy
 - Scope creep
 - CNaaS NMS software && Juniper && VXLAN && Institutes Requirements != Standards
 - Service development in short time
 - Direct full migration and service (while in pilot-fase)
 - Unable to charge development costs. Costs grow fast and become too high
 - Biggest risks for SURF (development, maintenance, disturbance)
- Decision to stop this activity in its current format due to lack of funds, commitment and risk profile. ☹️
 - Pilots need to be stopped in a way (complex, negative sentiment!)
 - Impact on strategy



How to provide value without the wired LAN service?

- When wired LAN service cancelled, this jeopardizes the campus strategy:
 - We cannot offer the whole campus network suite “as a service”
 - Demanding Institutes still expect a “one stop shop”, don’t want to do it themselves anymore
 - Markets solutions as quick fix for the short term
 - Threat to existing services wifi/firewall/iotroam/...
- But there are chances:
 - Campus Vision is still endorsed by all
 - Growing demand for more sovereign campus networks for bigger institutes
 - There is sense for cooperation between members

New strategy

Organise a sovereign campus network infrastructure ecosystem which can be strategically coordinated by the institutes in strong collaboration with SURF. Involve vendors and integrators who adopt our vision.

Provide, build and/or procure interoperable services, tools and platform(s) to enable this ecosystem

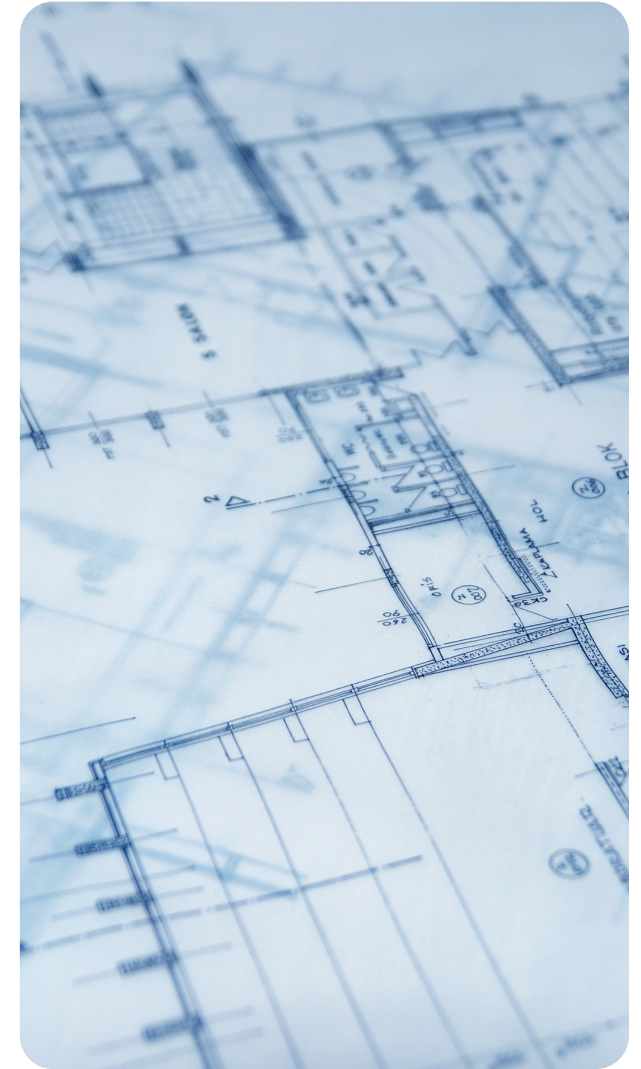
Key differences with previous strategy

- The way to *arrange* each component is the key change:
 - Architectural responsibility at SURF
 - 'As a service' vs 'as a partner'
 - Operational-directive responsibility at the institute
 - Centralised vs decentralised versus Cloud based on sovereignty demands
- Risk for SURF within operations will decrease
- Institute will have more active role
- Type of work for SURF will change (less engineering, more architect/consulting/procuring)
- The financial model changes

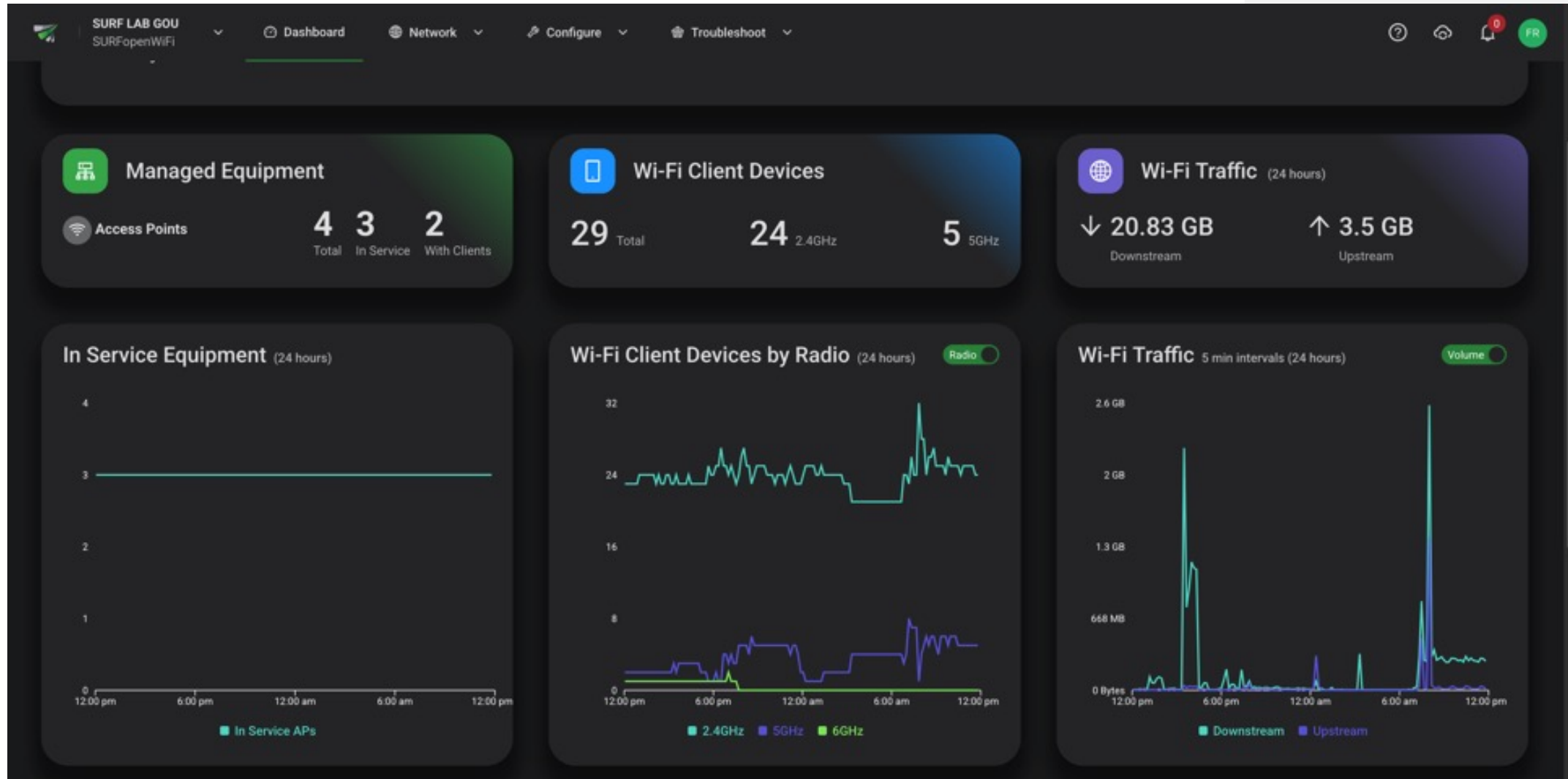
Component
Wi-Fi
eduroam
iotroam
Supported Campus Firewall
VPN
Core, Distribution and Access
Network Access Control
DHCP / DNS / IPAM
IoT network
Indoor 5G/6G Open RAN
CNaaS NMS
Automation, orchestration
Asset Administration systems
Monitoring en alarm aggregation (for 1st, 2nd and 3rd line)

| Todo: Reference architecture

- Physical and virtual network infrastructure: VXLAN based
- Identity, authentication, and access-control services: location?
- IP-address management, DNS and DHCP
- Network management and orchestration: CNaaS and/or LFO/WFO?
- Monitoring, analytics, and AI-driven insights
- SIEM and security operations
- Cable-management and asset-management systems
- APIs, data models, and integration layers connecting the components
- ... and probably a lot more



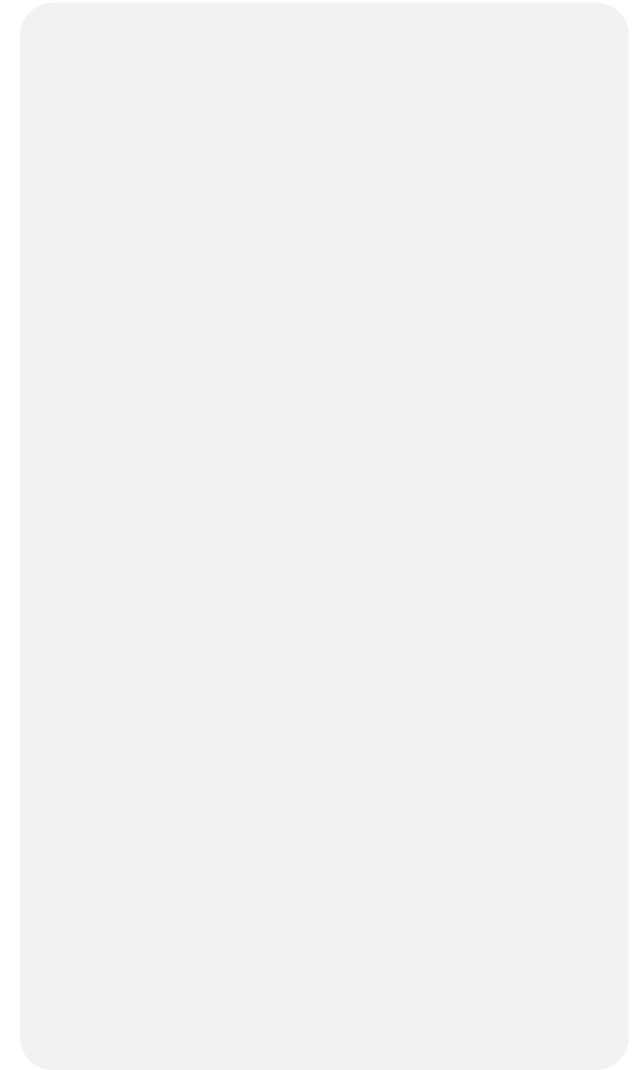
| In progress: research Open Wi-Fi



| In progress: mobile emergency communication

Two parts:

- Federated, secured and controlled out-of-band connectivity to the campus using 5G
- National mesh networks in case of power failures (further than campus only)



Todo: development of an open source NAC

- Who or what gets access?
- What access is granted?
- Under which conditions?

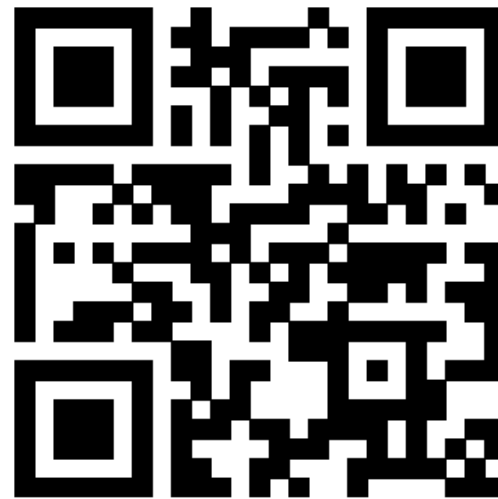
Just like keys control physical access, user groups determine digital access to systems under specific conditions.



Collaboration international: SIG CNaaS

- Collaboration by CNaaS SIG / NORDUNET / GEANT becomes even more important:
 - Use of NAV, ARGUS (Sikt)
 - Use of CNaaS (SUNET)
 - WFO/LFO developments (SURF/Sikt/SUNET)
 - Development of open source NAC (.....)
 - Sharing DDI developments (.....)
 - Overall architecture (.....)

→ Do you want to join us? SIG CNaaS



edu.nl/8gqgm



