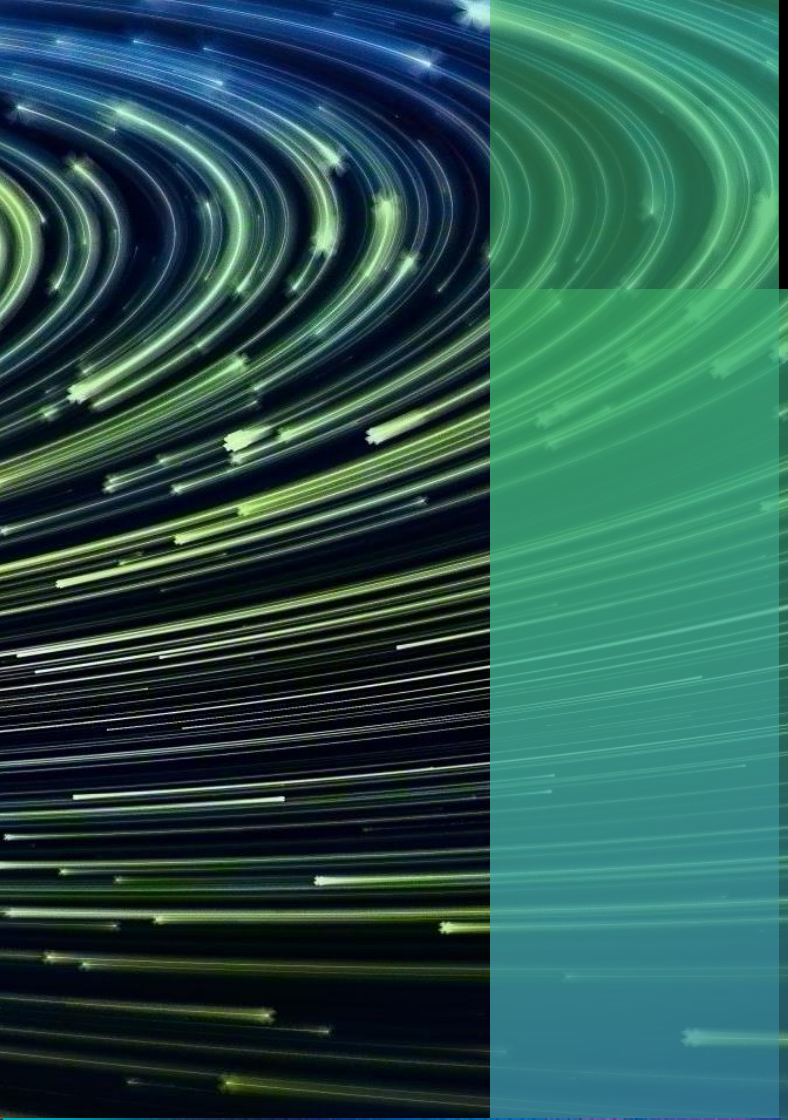


Cross campus network upgrade, and the move to (wired) 802.1x authentication

Charlene McGoohan, Peter Gaughran

Maynooth University, IT Services, Infrastructure Team

Maynooth University
National University of Ireland Maynooth

HEAnet Conference '22

Introduction

- About Us
- Why was the project needed?
  - eLearning
  - Ageing estate of hardware
  - Increased reliability
  - Network segmentation
  - 802.1x security
  - Network investments
- How was the project implemented?
  - Hardware chosen
  - Resourcing - project evolution
  - Methodology – equipment installs
  - Network segmentation
  - Methodology – 802.1x roll out
  - 802.1x – and a problem
  - SCEPman – and a solution
  - The present
  - The immediate future

About Us

Peter Gaughran

worked in IT for over 20 years - in IT Services, Maynooth University, as a Systems Administrator for 15 years, and now also in Networks

- AD
- Azure AD
- backup/recovery
- 802.1X
- Intune
- And many, many more...

About Us

Charlene McGoohan

worked in IT for over 10 years - in IT Services, Maynooth University, as an ICT Project Manager for 4 years, projects include:

- Network Upgrade
- MFA for Staff
- Security Operations Improvements
- On-prem File Storage Migration
- Managed Support Desk
- Data Centre Storage
- HEAnet ICT Security Services

Why?

- **Covid and the move to distance/online learning**
  - eLearning streaming tools i.e. Teams, Panopto, etc.
  - Panopto uses HLS streaming which consolidates video network traffic to HTTP/S. This ensures compatibility and optimal playback experiences across devices and connections.
  - Risks:
    - Network capacity may not handle Panopto along with general day to day staff and students use of the network
- **Ageing estate**
  - The switches at the access and distribution layer of the MU network had reached or were approaching end of life.
  - Over 100 + Access Layer Switches were in excess of 15 years old
  - Risks:
    - Lack of manufacturer support
    - No updates, patches, or bug fixes
    - No security updates

Why?

- **Greater bandwidth and throughput - increased reliability**

- **Network Segmentation**
  - Segment autonomous networks from campus network
  - Keep traffic secure and separated depending on access points and controller
  - The network is defended based on user/device/app/location before connection has even reached the firewall

Why?

- **802.1x security**
  - Comprehensive visibility of devices on the network
  - Authentication with the least amount of access necessary to each device, based on VLANs
  - Role based access controls (currently device-based access controls)
  - Continuous monitoring
  - Automatic security event responses and event triggered actions

- **Continue with Network Investments**
  - Core Switches Upgraded in 2015
  - Data Centre Networks Upgraded in 2015
  - Firewall Upgraded in 2018
  - WiFi Upgrade in 2019

How?

- A survey was conducted to determine the impact eLearning software would have on the network, it concluded that:
  - The current switches had a very high potential to cause congestion on the MU network.
  - The switches at the access and distribution layer of the network had reached or were approaching end of life.
- December 2020, the Networks team in IT Services, Maynooth University embarked on a new project to upgrade the majority of the existing campus network infrastructure. The new Aruba CX line was chosen for this purpose, along with a commitment to rolling out 802.1x authentication for managed devices.

Hardware

Aruba CX series chosen

- Aruba 8320 for routing
  - 48 ports of 1GbE/10GbE, with 40 GbE to the spine.
- Aruba 6200 switches, stacked
  - Up to 8 stack members, at 48 ports per member

This is what half a million euro of network equipment looks like!

C

Resourcing

April 2021 – July 2021

Project Manager

Infrastructure Manager – Networking SME

Network Engineer

Senior Infrastructure Specialist

Network Engineer

Supplier Contractor

Supplier Contractor

Project Delivery Team: July 2021 – January 2022

Project Manager

Infrastructure Manager – Networking SME

Network Engineer

Senior Infrastructure Specialist

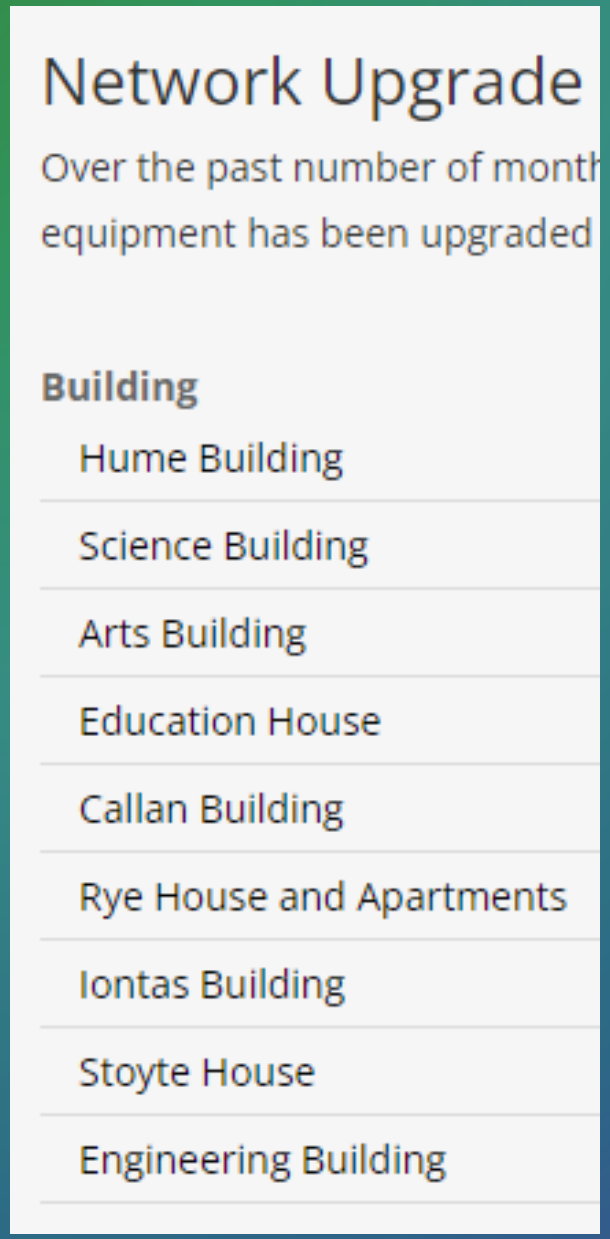
Network Engineer

Methodology – Upgrading Equipment

- **Physical installs – building by building approach**
  - Updating on a live campus network.
  - Managed and communicated the timing of tasks and ensured they are completed during non-critical times of the academic calendar.
  - Fallback plan: The switches could be rolled back if needed.
  - One building at a time approach. All buildings identified as part of survey were buildings with teaching spaces, to accommodate eLearning software network requirements.
  - A lot of communications!
  - Covid allowed us to communicate with specific users we knew were on campus, instead of an all staff list.

Tasks per Building:

1. Created inventory for the building (power supply, capacity, patching needed)
2. Documented new configurations for building
3. Installed hardware in the building
4. Configured the building's network, remotely
5. Communicated with specific users in given building
6. Patch from old network to new (Access Layer)
7. Migrated to new network (Distribution Layer)
8. Live test



Methodology

- New switches, connected to old
- Copper migration, with old router still in the mix.
- On an agreed & communicated day, flip over to new router, with minimal outage.
- *1 gig to 10!*

Lather, rinse, repeat!

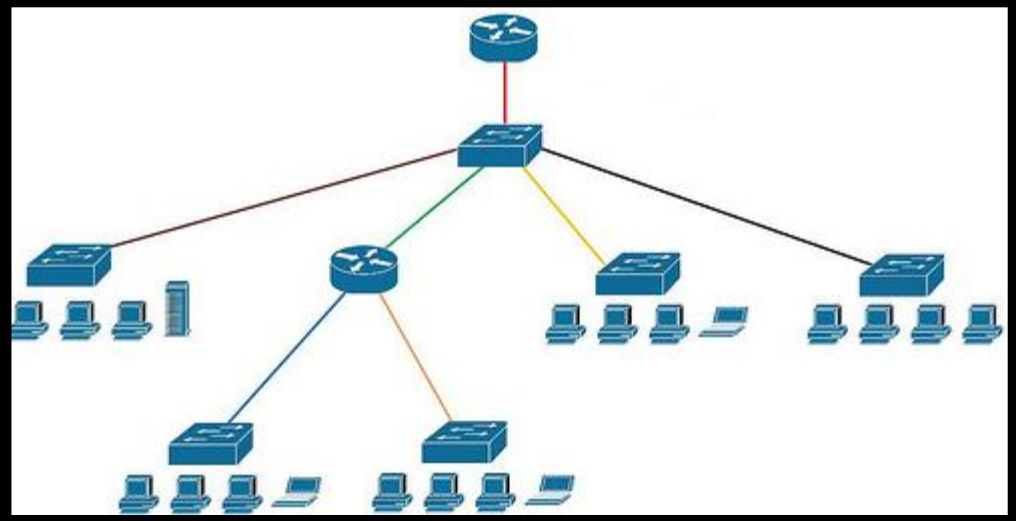
An aside – network segmentation

14th of May, 2021 – the HSE ransomware attack occurred. So what was to be a careful, well communicated change for several departments and the network at large, had to happen overnight!

Top down support from University Executive

Departments running their own infrastructure/services segmented, e.g.,

- Computer Science
- Mathematics
- Engineering
- Theoretical Physics



Methodology – 802.1x Roll Out

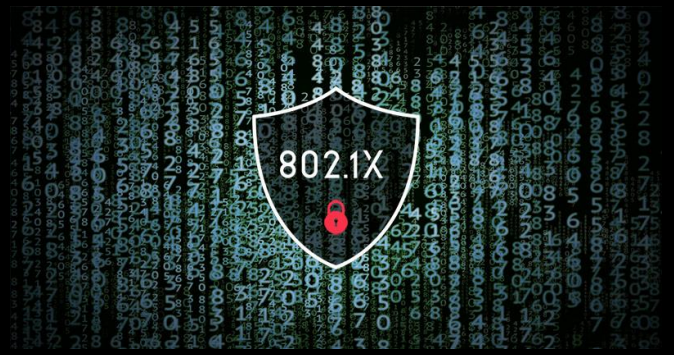
- **Building by Building Approach**
  - With contractors, we started with one building as a POC and knowledge share (July)
  - Used our second building to gain feedback on end-user impact
    - General feedback was that people didn't notice anything
  - Going forward – week on, week off approach
    - This allowed for investigation into potential tickets raised in Service Desk, and breathing room for BAU tasks

Building	Roll out week commencing
Hume Building	19th July 2021
Iontas Building	6th September 2021
Rye House and Apartments	27th September 2021
Arts Building	11th October 2021
Science Building	25th October 2021
Callan Building	8th November 2021
Education House	22nd November 2021
Stoyte House	20th December 2021

Tasks per Building:

1. Document VLAN details per building, based on types of users in building
2. Using ClearPass policies, enforce 802.1x
3. Testing, included all device types i.e. student and staff PCs, phones, printers, etc.

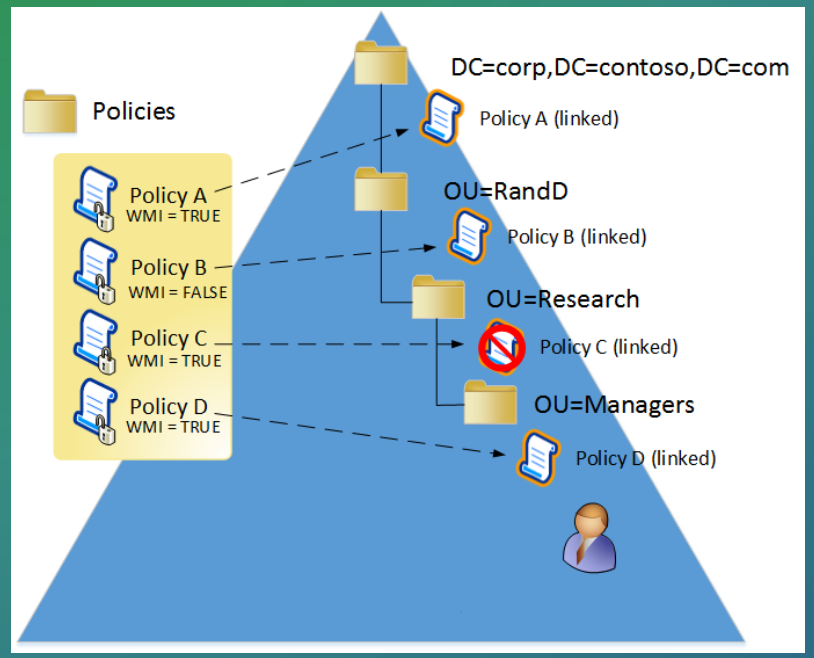
802.1x...



- ClearPass – pointed at Active Directory
- For example,

Tips:Role *EQUALS* [Machine Authenticated] *AND* Tips:Role *EQUALS* Bioscience *AND* Authorization:Maynooth Active Directory:UserDN *CONTAINS* OU=PCs, DC=ad,DC=mucampus,DC=ie	Bioscience_Staff_Vlan, [Allow Access Profile]

802.1x and client settings



- Service has to be turned on (Wired AutoConfig on Windows clients)

- Settings have to be applied to the interface profile
  - *Use EAP (PEAP)*
  - *Computer authentication*
  - *Fallback to unauthorised network access (**users still get the 'at home' experience**)*

802.1x... and a problem

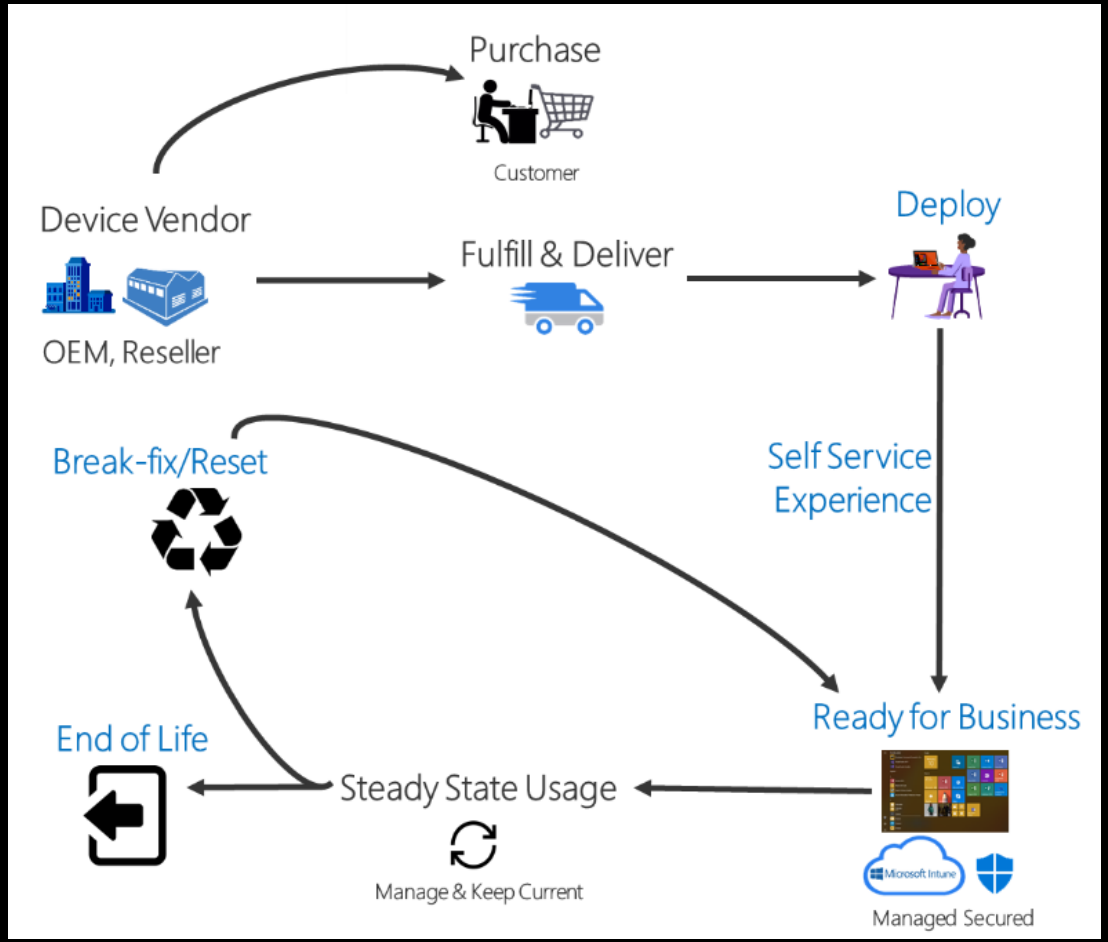
- What about machines in Azure Active Directory, being managed by Intune?

- From about 3 months into the pandemic, all new staff machines provisioned with Autopilot!

With no presence in AD whatsoever…

Autopilot

- Devices go straight to the client
- Log on, and away you go!
- All in Azure AD, though...



802.1x... and a problem

- In order for Intune managed machines to use computer authentication, EAP-TLS (and a valid certificate) is required

- *As part of managing devices, Intune issues certificates but they **cannot be used for authentication***

At the time, ~600 machines affected

Today - ~1,000!

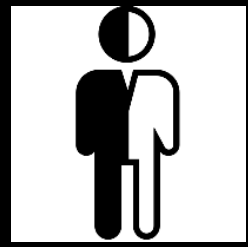
Authentication certificates

- Certificates are great!
- Certificates take time to
  - Issue
  - Install

Certificates have to be renewed… Again… And again… For 1,000 (and growing) machines

Business case required

- Option 1: Build our own on-premise infrastructure and deploy to Azure Application Proxy
  - Complex to set up, maintain, and operate
  - Certs would need to be manually generated for all existing and new staff machines
  - Certs would need to be updated each time they expire or require renewal
  - Issuing and re-issuing of certificates for a large estate would be (roughly!) half a sys admin's working life



- Option 2: Take the advice of Microsoft and Aruba
  - ClearPass will only authenticate such machines using EAP-TLS certificates
  - Both Aruba and Microsoft recommend the use of an Azure based, fully unattended CA...

Enter SCEPman – and a solution

- SCEP == Simple Certificate Enrolment Protocol
- SCEPman == SCEP-as-a-service

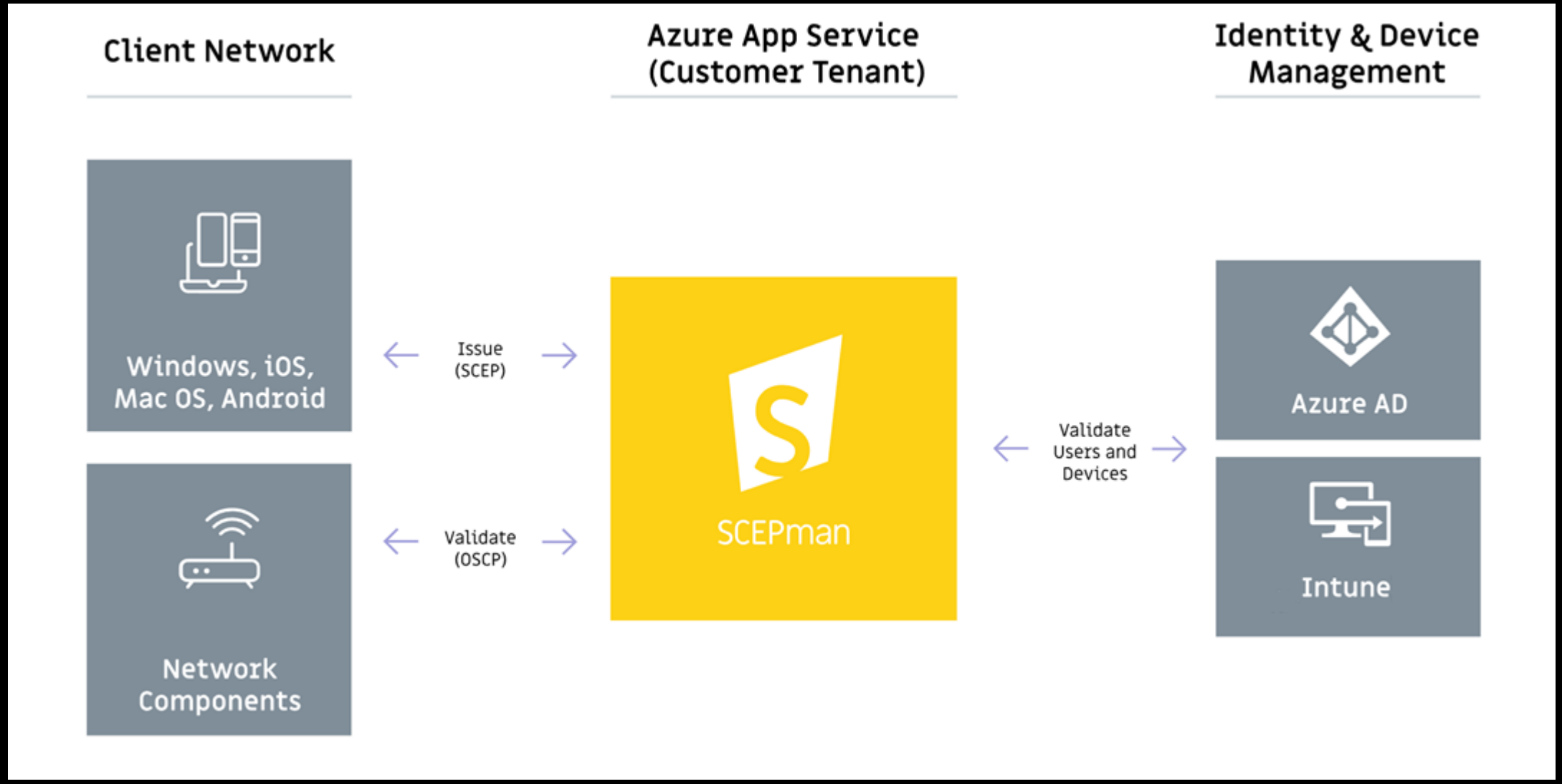
Runs in your Azure tenant, and can issue certificates for clients (device & users.)

SCEPman validates certificates (OCSP) and checks the corresponding device/user with your identity provider.

Saves massive amounts of time!

P

SCEPman architecture



SCEPman – how does it *really* work?

- Devices are added to an Azure AD group
- A Device Configuration Profile is set up for
  - ✓Root CA
  - ✓Windows devices
  - ✓Macs

Profiles then pointed at the relevant group. Certificates are re-issued at a percentage of the validity, e.g., 80%, at a cost* per certificate.

**Educational pricing for SCEPman available.*

Configure 802.1x for Intune managed devices..?

- Service has to be turned on (Wired AutoConfig on Windows clients)

- Settings have to be applied to the interface profile
  - *Use EAP-TLS*
  - *Machine authentication*
  - *Fallback to unauthorised network access (**users still get the ‘at home’ experience**)*
  - *Use simple certificate selection*

Intune doesn’t play nice with these things, though.

Configure 802.1x for Intune managed devices

You will need...

- Relevant registry entries to turn the service on, and for its settings
- An xml profile for the interface settings (EAP-TLS, machine auth etc.)

Create an IntuneWin Package to deploy the registry entries and import the profile.

Apply to the relevant Intune group, and you're done!

P

802.1x + Intune + SCEPman = Success!

- Single service in Clearpass, both AD & AAD machines can authenticate.

Tips:Role *EQUALS* [Machine Authenticated] *AND* Tips:Role *EQUALS* Bioscience *AND* Authorization:Maynooth Active Directory:UserDN *CONTAINS* OU=PCs,DC=ad, DC=mucampus,DC=ie	Bioscience_Staff_Vlan, [Allow Access Profile]
Tips:Role *EQUALS* Bioscience *AND* Authorization:[Endpoints Repository]:Intune Azure AD Device Id *EXISTS* *AND* Tips:Role *EQUALS* [Machine Authenticated]	Bioscience_Staff_Vlan, [Allow Access Profile]

Port configuration

```
interface 1/1/1
    no shutdown
    vlan trunk native 1
    vlan trunk allowed all
    spanning-tree loop-guard
    spanning-tree port-type admin-edge
    spanning-tree root-guard
    aaa authentication port-access client-limit 2
    aaa authentication port-access critical-role fallback_role
    aaa authentication port-access preauth-role fallback_role
    aaa authentication port-access reject-role fallback_role
    aaa authentication port-access dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        reauth
        enable
    aaa authentication port-access mac-auth
        cached-reauth
        cached-reauth-period 86400
        quiet-period 30
        enable
```

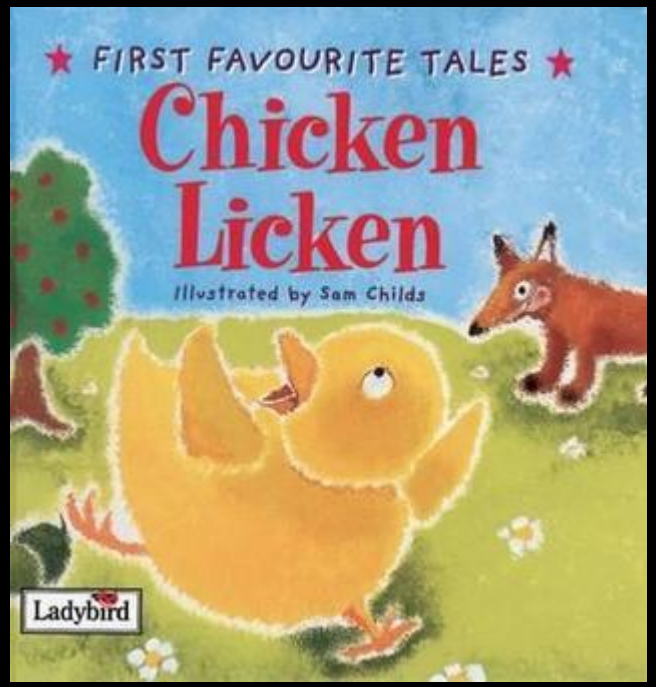
What if ClearPass goes down? Or if AD is unavailable?

ClearPass

- *Physical devices*
- *Dual homed power supplies*
- *Two nodes*

Active Directory

- *Two on-prem DCs*
- *Load balanced*
- *4 VM hosts, with failover between physical locations*



Fallback VLAN still grants access to the outside world! At present, anyway...

The Present

- Staff machines, be they AD or AAD joined, can auth properly and ‘be’ where they need to be.
- Library or Access ‘loaner’ laptops can authenticate seamlessly to the Wi-Fi and not require anything messy – no saved profiles/passwords, no generic accounts.
- Certificates are issued and re-issued *quietly*, and *efficiently*.

The Immediate Future?

- eduroam – auto auth to Wi-Fi (using user certs)
- Security posture assessment for other services e.g. VPN, Intranet access

Thank you!

Any questions?