2022

(Data) Network Programme briefing

BRIEFING DOCUMENT

IAIN WATSON

Contents

Preamble

This document is split into 2 parts:

1. The first part provides more general information about the (Data) Network Programme (to be referred to as the Network Programme (NP)), intended for the wider audience; and
2. The second part – the Appendices – provides more detailed information, primarily for the more technical minded but is there for anyone with interest.

The Network Programme has an online information site that will be developed and updated as the Programme progresses. Please visit the Network Program webpages for the latest information.

Introduction

The University network infrastructure, including the Wi-Fi network, has grown over the years to meet an ever-increasing demand. It does that job very well, but it is now aging, over complicated and becoming more fragile as the years pass.

To remedy this and to meet the challenges of the coming years, the University is investing in modernising the network with a complete replacement making it faster, more secure, more widely available and expandable. The vehicle to deliver this is a multi-year Network Infrastructure Investment Programme, simply referred to as the Network Programme (NP).

Programme goals

1. Build a network suitable for delivering 'non-stop' services and eradicate existing Single Points of Failure, including technology, people, processes and places.
2. Build a modern network that is fast, secure and reliable to meet the needs of our staff and students
3. Build an ongoing programme that ensures the network is always fit for purpose and reduces the need for high risk, 'big-bang' project approaches for network enhancements in the future
4. Ensure the UofG has high capacity, low latency connectivity across the campuses that is the foundation for all digital services and supports the user experience for research, teaching and guests and visitors
5. Demonstrate value for money

Outcomes and Benefits

When delivered, the key outcomes and benefits for the University delivered by the Network Programme will include:

- Improved WiFi network access including WiFi outside buildings in busy areas
- Faster wired network access
- Greater security control and insight in-to the network performance
- Improved service delivery
- Giving students and staff greater flexibility to work effectively wherever and whenever they want

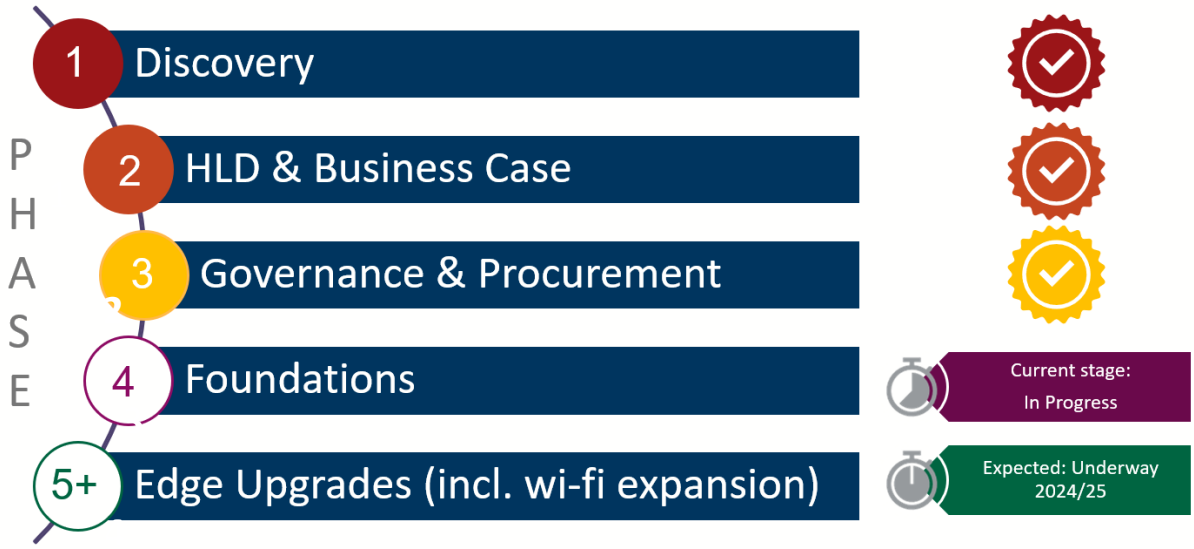
Go to Appendix 5 for some additional technical benefits.

Programme overview

Phase 1-3: The business case and high-level design are in place with the Primary Technology Partner (PTP - Capita) onboarded

Phase 4: Detailed low-level design and implementation of the network foundation whilst also looking at how we work supporting this new and modern network. This Phase will also look to carry out a small pilot on improving the Wi-Fi, fibre and existing network equipment areas (nodes) within the buildings that are required in order to deliver the network campus wide. Finally, we also delivered the new Public Wi-Fi service that is now running across the campus earlier this year (2022).

Phase 5+: Learning from the lessons learned in the Phase 4 pilot, this will deliver a multi-year iterative rollout of the Building / Wi-Fi / Fibre solution for all sites as well as move to the new Business as Usual (BaU) mode of working, continually replacing equipment in a planned manner before the end of its recommended lifespan



Scope

- The programme will upgrade and replace network equipment across:
  - 9 Main distribution points (nodes) (and will add new ones where requirements are identified);
  - 14 Main sites across the UofG; and
  - 240 Equipment rooms
- 219 buildings are in scope
- There are currently around 1500 wireless access points, and it is estimated there will be between 4-6000 by the end of the programme.
- Build a Proof of Concept (PoC) in Phase 4 to evidence the new system and test various scenarios to learn lessons before launching Phase 5. The PoC is a small model environment that can be used as a testing and learning lab.

Go to Appendix 1 for locations

Go to Appendix 6 for more information on the PoC

How can you help us help you?

To build the new network that will deliver you a better wired and wireless experience – bringing you greater speeds and coverage - there will need to be works carried out in buildings throughout the UofG. As well as technical this will also bring space challenges that will result in physical works to varying degrees being undertaken and as such, we ask your help:

- understanding that there will at times be some need for some disruption, whether that:
    - be cabling and minor building works required in order to support our new network; or
    - by way of outages as we transition from the old (current) network to the new.

All disruption, whether it be physical or technical, will be done with you in mind wherever possible, working with you to minimise any disruption and communicating with you in advance to allow you time to take any actions you may feel is necessary.

We need your help in identifying and accommodating the NP suitable space where these situations occur in order to be able to bring these benefits to your building.

Appendix 1 - The estate in scope

Site	Number of Properties	Number of Properties in Scope
ACRE ROAD SITE (GARSCUBE)	3	3
COCHNO FARM	56	8
DENTAL HOSPITAL AND SCHOOL	2	2
DUMFRIES CAMPUS	4	2
GARSCUBE CAMPUS	64	39
GARTNAVEL GENERAL HOSPITAL	2	2
GARTNAVEL ROYAL HOSPITAL	2	2
GILMOREHILL CAMPUS	144	129
HAMPDEN PARK	1	0
KIRKLEE ALLOTMENTS-KIRKLEE ROAD/WYNDHAM ST-G12 0SR	1	0
MILLPORT MARINE STATION SITE	5	0
OUTLYING AREAS	64	12
QUEEN ELIZABETH UNIVERSITY HOSPITAL	7	7
ROWARDENNAN SITE	3	3
ROYAL INFIRMARY	5	5
UOG SINGAPORE SITE	1	0
WESTERN SITE	14	4
YORKHILL HOSPITALS SITE	1	0
Golden Jubilee Hospital	1	1
Total Buildings in Scope		**219**

Appendix 2 - Programme Status

Key activities to date: (as at November 2022)

Activity	Progress	Comments
Infrastructure Workstream		
Initial Surveys of Equipment Nodes, including cabling	Complete	- Due to be completed in October 2022 - Next steps to apply proposed solution / design against all nodes
Fibre Surveys	91% complete	- Scheduled to be completed December 2022
Wireless Surveys	62% complete	- Scheduled to be completed December 2022 / January 2023 - Initial Surveys to date are showing that the internal wireless Access Points will have an uplift of circa 210% against the current population, leading to better coverage capable of supporting location-based services
Buildings / Wi-Fi Pilot	Tbc	- The pilot for our work in upgrading equipment rooms and wi-fi service in selected buildings is currently in planning stage - It is hoped that this will be able to get underway in Q1 2023, however this is dependent upon a lot of factors, including a lot of the work being undertaken above as well as approval for any request for additional space and physical work being received
Network Workstream		
Software Design Access	- Phase 1 Complete - Phase 2 Underway - Phase 3 Not started	- Phase 1 (Data Gathering, Use Cases and Solution Requirements) - Phase 2 (High Level Design) Scheduled for Completion December 2022 - Phase 3 (Low Level Design) Scheduled for Q1 – Q2 2023
Proof of Concept	- Built and Configuration underway	- Currently undergoing testing
Crichton Campus	- Initial onsite survey by Capita - New circuit ordered - Deploy proposal awaited	- Done - On order, awaiting confirmation of activation date - Currently being prepared by Capita and due in Dec ’22 / Jan ‘23
Other		
Network Equipment	- All due to be delivered by 2023	- Equipment impacted by global supply chain issues as a result of the pandemic - Kit has been arriving since summer 2022 with final kit (External Wireless Access Points) due June 2023

Appendix 3 – Technical

The following standards have been agreed as the **starting point** on any infrastructure design - they can be varied by agreement from the UofG Central Networks Team

Safety, Security and Access Control

Network equipment nodes are regulated by a variety of industry and data protection standards (EU / UK GDPR) therefore ensuring physical server room safety and security is paramount. To meet obligations under GDPR the University must ensure that Comms / Server rooms are physically and securely enclosed with controlled access (e.gg. Salto). The enclosed Comms Server rooms must have sufficient dimensions to cater for environmental control, safe working conditions and future expansion

Rack Configurations

All the following 2,3 & 4 rack configurations are based on 42u cabinets

1. 2 Rack Configurations are suitable for a Day 1 total of 480 structured cabling outlets
2. 3 Rack Configurations are suitable for a Day 1 total of 888 structured cabling outlets
3. 4 Rack Configurations are suitable for a Day 1 total of 960 structured cabling outlets

Preferred Cabinet Layouts

- The preferred cabinet layouts for rework/new installations will remain as Active and Passive Racks as the standard going forward
- As a general starting rule, for a 3-rack config, the passive rack that is not full should be dual powered in case equipment is added
    - Power should be that which is required by the active switching equipment, with 25% held in reserve (this may result in 32amp connectivity rather than 16amp in some cases – on a case-by-case basis)

UPS

1. UPS should be scaled to match the switching power requirements (based on manufacturer best practice / guidelines)
2. The UPS autonomy time should be able to manage 'brown-outs' / building works as a general rule – i.e., 10 to 20 mins.
3. Would also require monitoring to ensure that batteries etc are monitored and alerted where appropriate (e.g., battery condition and alerts for when power provision switches over to the UPS)
4. UPS manufacturers should be the same
5. The preferred solution where there is sufficient space available and is pragmatic is to have a rack UPS.

Note: UPS KVA / Autonomy time drives the physical size of the unit and needs to factor into any layouts where a rack mount unit is not suitable.

Air conditioning

1. The distribution node should be able to maintain the air temperature in line with the manufacturers guidelines to ensure full life-span of the equipment (if the solution is AC then a core / distribution node should be n+1)

2. With regards manufacturer etc, advice from Estates is"…no preferred manufacturer – we currently have about every possible manufacturer going. Our only stipulation or preference, would be that it is a know manufacturer i.e. Mitsubishi, Daikin etc…". and that for the Network Programme we would again look for the ACs coming from the same manufacturer.

Dual Distribution and Edge Nodes

Where a distribution node is also an edge node (e.g. 2d), preferred solution is to have a degree of separation between the distribution functionality and edge functionality (e.g. a cabinet holding UPS, routers etc.)

Edge Nodes

1. Edge nodes cabinets should have 2 PDU's off of 2 different breakers

2. General rule is edge nodes will not have a UPS however, where an edge site is dependent on another edge site (in another building) a UPS may be suitable in this situation

3. The node should able to maintain the air temperature in line with the manufacturers guidelines to ensure full life-span of the equipment (in our experience this has not been an issue to date in our edge sites)

Figure 1 Rack configurations: Sizing and guidelines

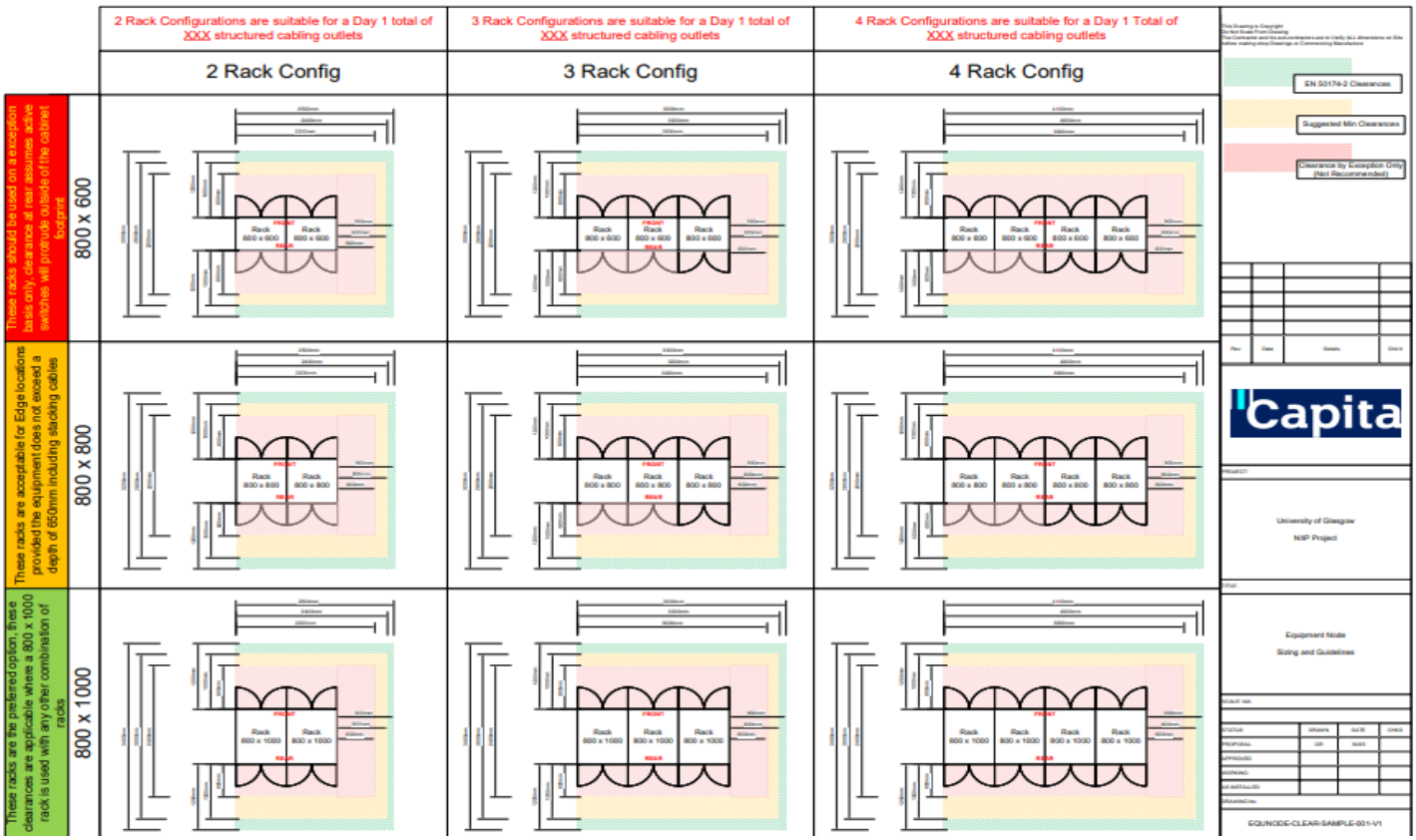
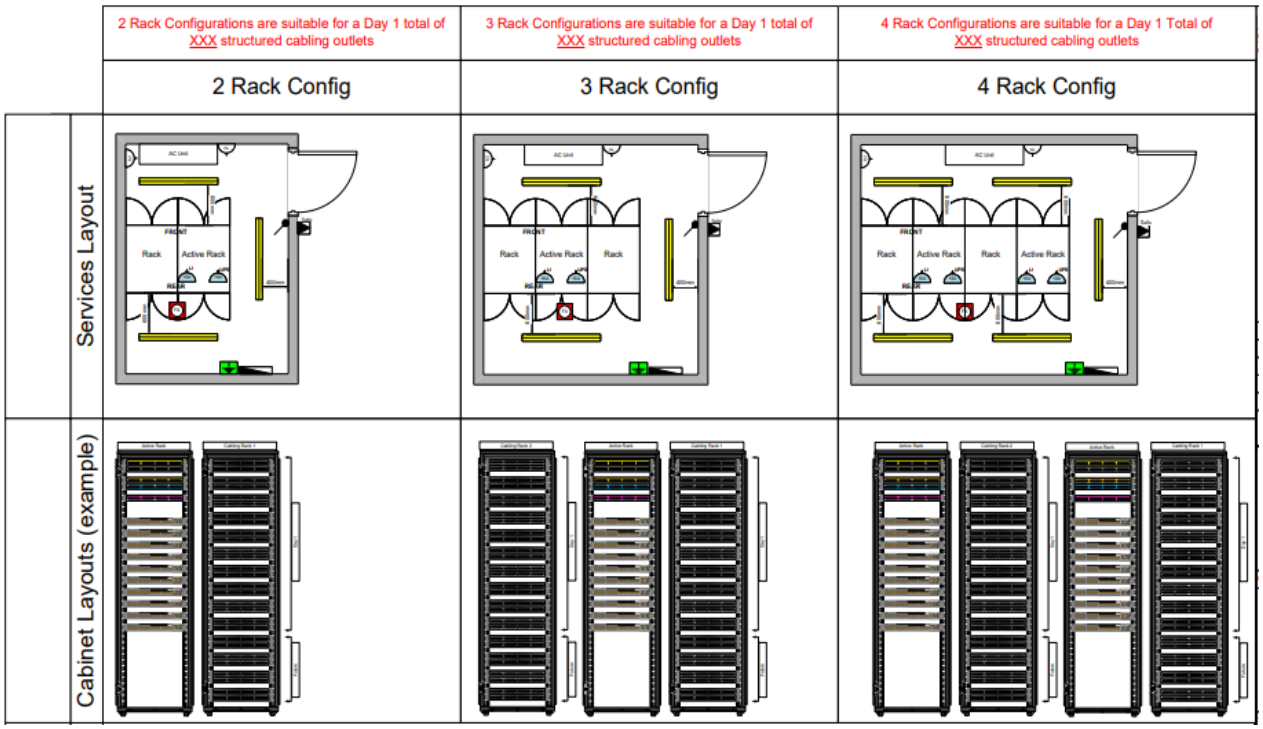


Figure 2 Distribution Node – Services and Cabinet Layout



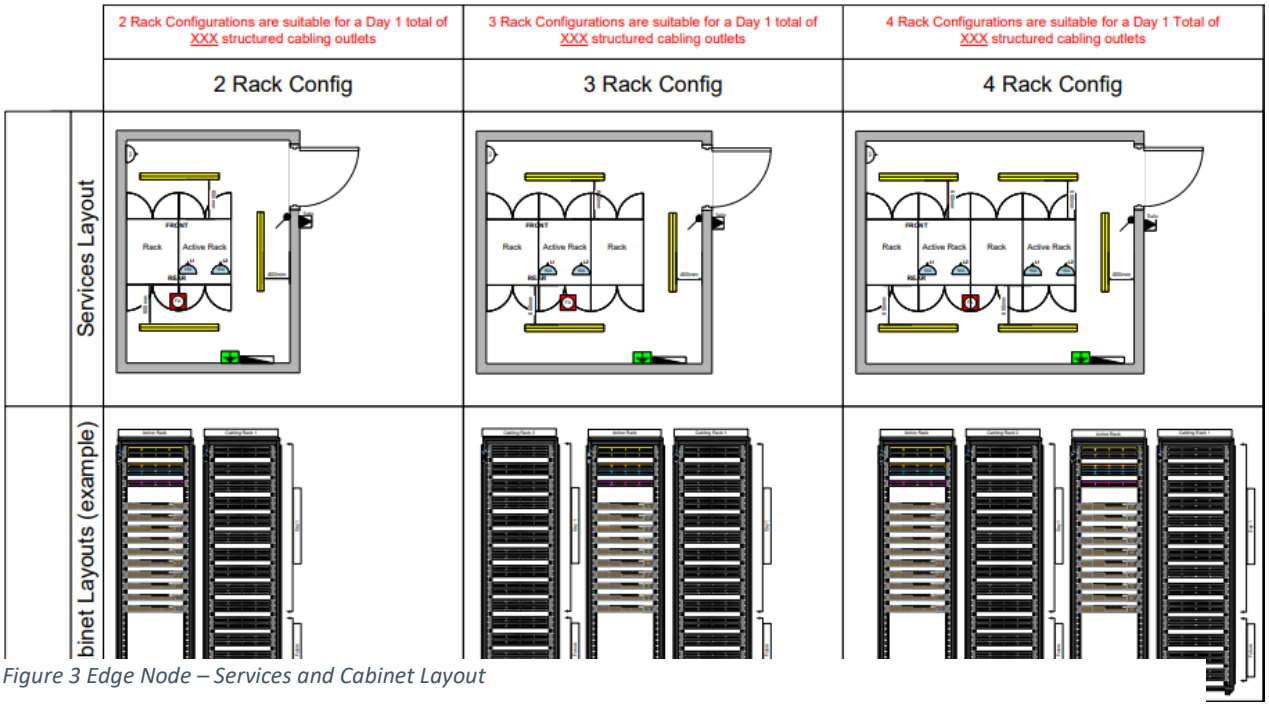


Figure 3 Edge Node – Services and Cabinet Layout

Cabling Standards

The cabling standard that will be the default position for design and costing unless advised otherwise on a case-by-case basis is:

- **Cat5** Cabling – All cabling will be replaced with cat6A
- **Cat5E** Cabling – Where located within a location where Cat5 cabling is being replaced this should also be replaced, otherwise this will be retained (subject to user needs)
- **Cat6** – Will be retained
- **Cat6A** – Will be retained
- **Wireless** – All APs will have Cat 6a cabling to them.
- A **new** node location, that replaces an existing node location, will be fully cabled in cat6A

We will monitor the success and cost of this as part of the Phase 4 pilot (in advance of the commencement of Phase 5).

Appendix 4 - Software Defined Access

The new UofG data network will be a Cisco Software Defined-Access network. Cisco Software Defined-Access provides zero-trust security in the workplace. It secures access—by all users, all devices, and from all locations—across your applications and network environment.

Features and benefits

Identify and verify all endpoints

Includes users and IoT devices that connect to our network.

Establish policy and segmentation

Help to ensure least-privilege access based on endpoint and user type.

Continually monitor endpoint behaviour

Help ensure compliance, including encrypted traffic.

Stop threat migration

Quarantine endpoints that exhibit malicious or out-of-compliance behaviour.

Software defined access components

Cisco DNA Centre

Cisco DNA Centre, with its platform and software, provides the network automation and secure access capabilities at the core of SD-Access.

Cisco Identity Services Engine (ISE)

Policy, segmentation, and enforcement are central to an effective zero-trust workplace solution. Cisco ISE is the engine for defining and enforcing segmentation SD-Access.

Cisco DNA Software subscriptions

Cisco DNA Software subscriptions give you the tools you need in a single, easy-to-consume license. Your SD-Access solution continues to evolve as your needs grow

Cisco Catalyst 9000 infrastructure

The power of SD-Access is its integration with the network. Cisco Catalyst switches and access points help optimize the depth and breadth of access security

Find out more about Cisco Software defined access

- Visit Cisco's SD access webpages
- Watch Cisco's video about SD access

Appendix 5 - other technical benefits

In addition to benefits already highlighted throughout the document, here are some other technical benefits that the Network Programme will bring to the UofG:

Benefit	Details
UofG will run a new Network that will utilise the latest Cisco hardware that supports Cisco's Software Defined Access (SDA).	SDA provides a platform for the IT Teams to respond to additions, changes and deletions much quicker. All configuration activities are carried out centrally from the Cisco Digital Network Architecture (DNA) Centre. This architecture will provide the university a centralised configuration/asset and license management platform for their network assets.
SDA Improves Network Security across the Campus.	Keeping the user, their device and other network traffic separate by means of network segmentation and access policies.
SDA provides more efficient IT operations	SDA automates user access policies by dynamically classifying and applying the right policy for users or devices based on the authorisation rule. This improves the speed in which IT can respond as this is configured centrally via Cisco DNA Centre and Cisco Identity Services Engine (ISE).
Cisco DNA Centre Assurance will improve the ability to fix network issues.	DNA Centre Assurance will allow the IT Team to have early visibility of network issues leading to incident prevention and improved performance.
SDA Provides a consistent user experience	SDA fabric will provide users and endpoints seamless mobility across the campus. Location agnostic network configuration will provide a consistent user experience as well as a simplified access/security policy.
The roll out of Wi-Fi 6 standard throughout the UofG	Wi-Fi 6 will - Increase device battery life for Wi Fi 6 enabled devices - Provide high speed even when congested - increase access point capacity in support of IoT and mobile devices. ... - Be backward compatible with Wi-Fi 5 and Wi-Fi 4 devices among other standards. increase number of devices supported by one router.

Appendix 6 - Proof of Concept (PoC)

A Proof of Concept product is being delivered as part of the Network Programme. It will provide a working miniature model to demonstrate the Software Defined-Access (SDA) capabilities that the UofG data network will receive the benefits of and will provide the UofG Network team with hands on exposure to the Cisco DNA Centre appliance and all its subsidiary integration components such as:

- Cisco Identity Services Engine (ISE);
- Wireless LAN Controller (WLC);
- Cisco Firepower Threat Device (FTD); and
- Infoblox DDI
    - (Domain Name System (DNS)
    - Dynamic Host Configuration Protocol (DHCP)
    - IP Address Management (IPAM))

Cisco Software Defined Access proof of concept build for University of Glasgow will provide the organisation a platform to get hands on exposure to all features of the DNA Centre appliance and it will provide the physical and logical connectivity between different network and security elements included in the production design / migration.

Network Deliverables

The PoC is built by Capita Business Services and will allow us to prove the SDA concept and its associated elements such as:

- Understand the concept of Software Defined Access
- Hands-on experience on the DNA-C (Digital Network Architecture – Centre) appliance
- Testing different use-cases which will have a miniatured version of the campus architecture
- Integration elements such as Cisco ISE and Active directory, Wireless LAN Controller (WLC), Firepower Threat Defence (FTD)

Technical Skills Required to work on the POC

Basic network understanding and an overview of Cisco SDA is required to operate and test the PoC.

Approach

The PoC solution will be delivered at the UofG Data Centre location. The systems that are installed within the DC will be remotely managed via the Campus network. Remote managed PDUs will be installed to remotely control power flow to the equipment.

Solution Scope

The physical and logical topology will be provided to the University and all virtual machines will use snapshot to bring it back to the fully operational state as well as initial configuration. The solution will include a working Cisco Software Defined Access solution and migration scenarios.

Inclusions

The following items are specifically included:

- Install Cisco DNA-Centre and all its associated components

- Install the test virtual machines including the Data Centre (DC) / Certificate Authority (CA) servers
- Build and migration use cases
- Provide necessary demarcation of service for no data overlap or disruption to production services

Exclusions

The following items are specifically excluded from the scope:

- PoC will only test a subset of endpoints
- Migration strategy drawn in this PoC will not cover all details in reference to a multi-stack switch build or all reference designs.
- No Integration to Data Centre equipment or any other live equipment included.

Solution Overview

The solution will include a mix of endpoints, associated hardware, and software to test the capability of the solution and it will include some use-cases to test the end-to-end lifecycle for the product and its capabilities.

The solution will entail multiple use-cases, each use-case will detail a particular functionality, or a working model associated with the new technology.

Software Defined Access solution is centred around Cisco orchestrator called the DNA-C (Digital Network Architecture Centre Appliance). DNA-C is a custom build application which sits on top of Ubuntu operating system and using micro-services (containers) to carry out multiple network / automation functions. The key areas of Cisco DNA-C are:

- Automation (NCP – Network control platform)
    - Desi
    - Policy
    - Provision
- Analytics (Network Data platform)
    - Assurance

DNA-C interfaces with Cisco ISE for policy enforcement. AAA policies are defined in ISE and Scalable Group Tags (SGT's) are assigned based on the policy match conditions.

High Level Approach

PoC build will entail various use-case testing. The system will be built, and a snapshot configuration backup will be taken before handing the service over to the UoG team. Various test use-cases are factored in to provide a conclusive working and migration aspect of software defined access and all its associated components.

PoC setup and use-case summary:

- DNA-C installation and integration of associated components such as
    - Active-directory
    - CA
    - WLC
    - ISE

    - FMC
    - DDI (Infoblox)
- Network build / discovery
    - Fabric Core (Border & Control)
    - Edge
    - Intermediate
- Device onboarding (mix of devices) including telephony
- WLC integration
- Edge migrations use case from non-legacy to SDA
    - Full site migration
    - Partial site migration
- Routing between sites and configuration of Fusion for multi-VN
- Configure Firewall to filter traffic between VN's
- Configure and test Micro and Macro segmentation
- Wireless migration uses cases includes
    - Over The Top (OTT)
    - Partial - like one out of 2 floors are in fabric mode.
    - Full fabric
- Assurance testing and fault emulation
- Local Area Network (LAN) / Wide Area Network (WAN) / Device failure
- Configure multi-site and test transit capability
- Backup and recovery