Healthcare Secure Infrastructure

Creating Secure, Agile and Resilient Healthcare Infrastructure

Providing EPR Ready Solutions to NHS

Matt Graham – Systems Architect

Amit Mehra – Business Solutions Architect

Paul Hambleton – Systems Engineering Leader

Version	Date
1.0	21st April 2023

Disclaimer:

“The guidance provided in this document is of a generic nature and cannot be specific to your organisation or operations. Please contact your Cisco partner or Account Manager to discuss your specific requirements. The guidance is provided in good faith based upon reference materials sourced from the NHS, Department of Health and other health and care organisations up to the date of publication. Errors and omissions are excepted. No warranty is given or implied.”

Contents

1. Introduction

Healthcare organisations face unique challenges when it comes to building secure, agile, and resilient infrastructure that can support critical patient care workflows. Data security and privacy concerns, complex regulatory requirements, legacy technology systems, and limited IT budgets and resources all contribute to the difficulty of creating infrastructure that can withstand evolving healthcare needs and constantly shifting threat landscape for cybersecurity.

In addition to these challenges, healthcare organisations are also increasingly recognising the importance of Electronic Patient Records (EPRs) in improving patient care and outcomes, and to enable the clinicians make quicker decisions while also eliminating reliance on paper-based records. However, implementing EPRs requires a robust and interoperable infrastructure that can support the data-intensive workflows involved in modern healthcare establishments. The UK government has set a target for electronic patient records (EPRs) must be implemented in at least 90% of NHS trusts by December 2023.

In this whitepaper, we will explore the key components to build a secure, agile, and resilient healthcare IT infrastructure. We believe this would provide NHS the foundation for a robust and secure EPR system and other applications which rely on such infrastructure. Our goal is to provide guidance and insights that can help NHS trusts to improve their infrastructure maturity and patient care outcomes by adopting these solutions powered by Cisco's industry leading technology.

The intended audience for this whitepaper is healthcare executives, IT leaders, network managers and administrators, clinical staff, and other healthcare professionals who are involved in the development, implementation, and maintenance of healthcare IT infrastructure. This may also include CIOs, CTOs, IT managers, clinical informatics specialists, and other professionals who are responsible for implementation, maintenance, design, and architecture of such systems. Additionally, this whitepaper may also be useful for vendors, partners and developers who provide healthcare IT solutions and services, as well as for policymakers and regulators who are involved in shaping healthcare policy and regulations.

1.1. Challenges for NHS Healthcare Infrastructure in the UK

1. Limited IT budgets: The NHS is one of the largest healthcare systems in the world, serving a population of over 66 million people. However, it operates within a tight budget, which can make it difficult to invest in new technology solutions and hire additional IT staff.

2. Complex regulatory requirements: The NHS is subject to a wide range of regulatory requirements, including GDPR, the Data Protection Act 2018, and the Caldicott Principles. Compliance with these regulations can be challenging, particularly in a large, decentralised organisation.

3. Legacy technology systems: The NHS relies on a variety of legacy technology systems, including paper-based records and outdated software applications. Upgrading these systems can be costly, time-consuming and may require significant changes to existing workflows.

4. Interoperability challenges: The NHS uses a variety of different systems and technologies that are not always designed to work together, making it difficult to share patient data and collaborate effectively. This can create inefficiencies and lead to gaps in patient care.

5. Cybersecurity threats: The NHS is a prime target for cyber-attacks due to the sensitive nature of the data it handles. In 2017, the WannaCry ransomware attack affected over 200,000 computers across the NHS, causing widespread disruption and highlighting the need for improved cybersecurity measures.

6. Aging population: The UK has an aging population, which will put additional strain on the NHS and its IT infrastructure. Older patients often have complex medical needs that require coordinated care across multiple providers and settings, which can be challenging to manage using traditional paper-based records. This also pose the challenge to avoid exclusion which means designing system such that people with disabilities are also able to use it and not get excluded.

While these challenges may make it difficult for the NHS to create and maintain an IT infrastructure fit to support modern healthcare workflows. The NHS has made significant investments in technology in recent years, including the development of the NHS App, the rollout of the NHS Digital Academy and strategic guidelines provided by Health and Social Care Information Centre which is otherwise simply called ‘NHS Digital’, which aims to improve digital skills among healthcare professionals and adoption of latest technologies to enable clinicians and drive better healthcare outcomes. By continuing to invest strategically in technology and IT infrastructure, the NHS can better meet the needs of its patients and improve health outcomes.

2. Key Components

At a fundamental level we will focus on zero-trust, network segmentation and 802.1X implementation as the key components for our discussion amongst other solutions that will help build a strategic network architecture for a healthcare secure infrastructure.

1. Zero-trust security: A zero-trust model is a 'security-first' approach which means no one and nothing is trusted, all users, devices, and applications are treated as potential threats and must be verified before being granted access to the network and sensitive data. This approach helps to minimise the risk of unauthorised access and data breaches. Cisco's Zero-Trust solution offering is based on the fundamentals of enforcing security policies using network segmentation and identity and access management. We will discuss this in detail throughout this document.

2. Network segmentation: Network segmentation involves dividing a network into smaller subnetworks or segments. This approach helps improve network security posture by isolating types of traffic and restricting access to sensitive data based on contextual information such as device and user identity. To implement network segmentation at scale we also need to introduce automation and envision the network as a programable system. Cisco's software-defined networking (SDN) solutions, such as Cisco DNA Center helps implementing this concept. We have dedicated a section to discuss the software driven approach and how it applies to both wired and wireless networks.

3. 802.1X authentication: 802.1X authentication is a standard for network access control that can help healthcare organisations enforce access policies based on user identity and device type. To implement 802.1X authentication, healthcare organisations can use Cisco Identity Services Engine (ISE). ISE provides granular access control policies and can integrate with other security solutions to provide comprehensive identity and access management.

   Effective use of these technologies help establishes a strong security posture for the NHS network based on strict Identity and access management policy with the goal of protecting data privacy which is a fundamental requirement for any EPR system. By leveraging Zero Trust approach along with segmentation and automation techniques, NHS organisations can create a secure, agile, and resilient infrastructure that protects patient data, ensures compliance with regulations, and improves patient outcomes. This will also ensure that NHS organisations can identify and mitigate potential threats before they can cause harm, ensuring that patient data always remains safe and secure.

3. Background and Principles

Before starting the technical discussion, it is important to understand the motivation and driving factors behind the shift required in adopting the technologies which influence the future roadmap for NHS' digital infrastructure.

Information technology has been a critical and evolving component of the NHS' healthcare ecosystem for a significant period. Some of the use cases that technology helps drive across the NHS can be broadly classified as patient experience, clinical care, and operational efficiency.

1. Patient Experience
    - Increased patient satisfaction
    - Easy access to health services
    - Self-managed appointments
    - IOT and Wearable Tech
    - Mobile and Remote Clinics
2. Clinical Care
    - Staff enablement
    - Staff efficiency increase
    - Staff optimisation
    - IOT (medical, estates, assets, and wearables)
    - Remote patient monitoring
    - Multi-Disciplinary Teams
3. Operational Efficiency
    - IT Staff efficiencies and optimisation
    - Lifecycle Management
    - Hybrid Work
    - Reduced time to respond to threats
    - Reduced time to fix problems.

For maximum efficiency and flexibility these need to be built on a common platform which works seamlessly within and outside the physical campus boundaries. This increases the complexity of delivering an advanced infrastructure capable of supporting the diverse set of use cases listed. A representative subset of dependencies is listed below.

1. A clear demand for high-availability to support clinical systems - Always on
2. Provision of internet access for both patients and visitors – Wireless Access
3. Protection of assets and infrastructure - Security First
4. High-bandwidth applications – Access within and outside the campus
5. Multi-disciplinary teams – cross functional and multi-organisation collaboration
6. Infrastructure Management – not just device provisioning but response time
7. Rapid change required to support user demands - which includes hybrid working
8. Observability – have confidence that everything is working as expected and gain actionable insights while allowing network to heal itself.

4. Solutions and Technologies

To provide excellent care, clinicians need access IT systems wherever they are - secure access needs to be available both from wired devices and from mobile devices which can be either on-prem or off site. Developments in WiFi and encryption technologies make this possible. The current standards are designed to allow a disparate range of devices to coexist on the mobile network without compromising performance or security. Access to EPR systems can also be extended off site using VPN technologies to provide secure encrypted access, these can also support the zero-trust deployment.

The convenience of the EPR systems will also mean an increased demand and increased dependency on it, and it will always need to be accessible. This will put greater demands on the IT network infrastructure. Fortunately, it is possible to architect networks with redundant elements to overcome component failure, and modern techniques need to be deployed to rapidly reconfigure the network to provide sub-second restoration to ensure service availability.

To optimally support these capabilities there is a need to closely coordinate activities across the network, associated policies, and security elements. To achieve this a central controller is required to collate all the information from and centrally manage the network. This can then share information with security elements via APIs and provide a platform to verify the service provided.

Cisco has made a commitment to move away from purely hardware-based solutions to focus on software that works in harmony with the industry leading hardware, to provide an integrated, scalable, and manageable infrastructure which provides best in class end to end solution.

This move to a software led portfolio is now the key focus across all technologies. The driving principle behind this is to enable platforms that are adaptable, easier to deploy and manage, and provide users with actionable insights that were previously unavailable or were extremely complex to maintain.

All the technologies contained within this document, are now built on this principle, where automation, orchestration and visibility are driven through software solutions, and enable tight integration through standards-based approaches and open systems.

This document is written as a “how to”, but links to appropriate reference material are included as footnotes.

The sections that follow will aim to provide specifics for each of the following areas in consideration.

It is structured in such a way that an organisation, regardless of their digital maturity level, will be able to identify required capabilities and propose suitable enhancements.

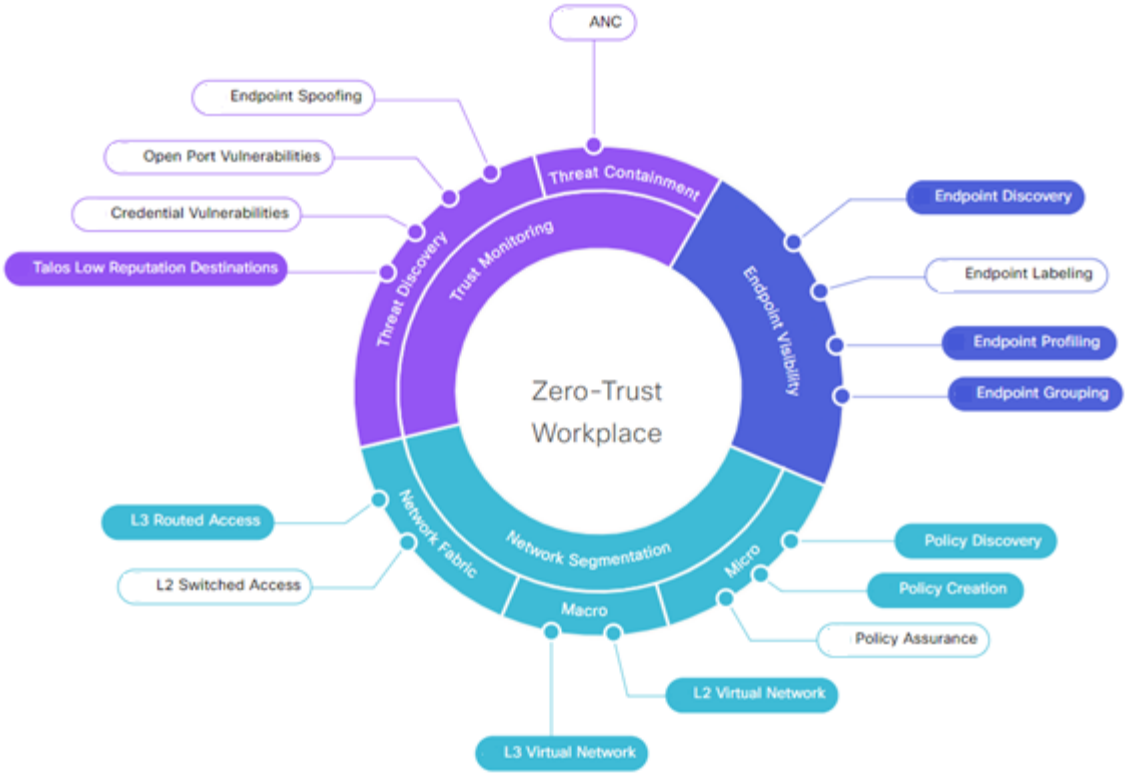
- Zero Trust - Security First Approach: If it is connected it should be secured
- Segmentation – The one thing that brings everything else together
- 802.1X – Authentication mechanism
- Access Anywhere – wired, wireless, remote, and agile.
- One Network, One Policy, One Experience – Fabric based network
- Network Visibility – If it is connected it should be visible
- Quality Of Experience

These guiding principles should be applied consistently across Wired device access, Wireless device access and include remote access for agile and collaborative user experience. From an end user perspective, access should be simple, consistent, and available regardless of location.

To further expand on the principle of secure and agile infrastructure, while developing this document, several key requirements were identified. These requirements have been collated through discussions with NHS staff across the UK, and subsequently aligned to produce a guide for use by IT Professionals to deliver an infrastructure ready to meet the demands of all disciplines within the Health Service, extending into other partners and agencies within the Integrated Health Boards.

It is clear, Information Technology plays a crucial role in enabling the NHS to provide high-quality healthcare services to its patients. As healthcare becomes increasingly digitised, it is important that the NHS continues to invest in information technology systems strategically to ensure that it remains at the forefront of healthcare innovation.

The diagram below forms the basis of areas that should be a fundamental when modernising any healthcare infrastructure.

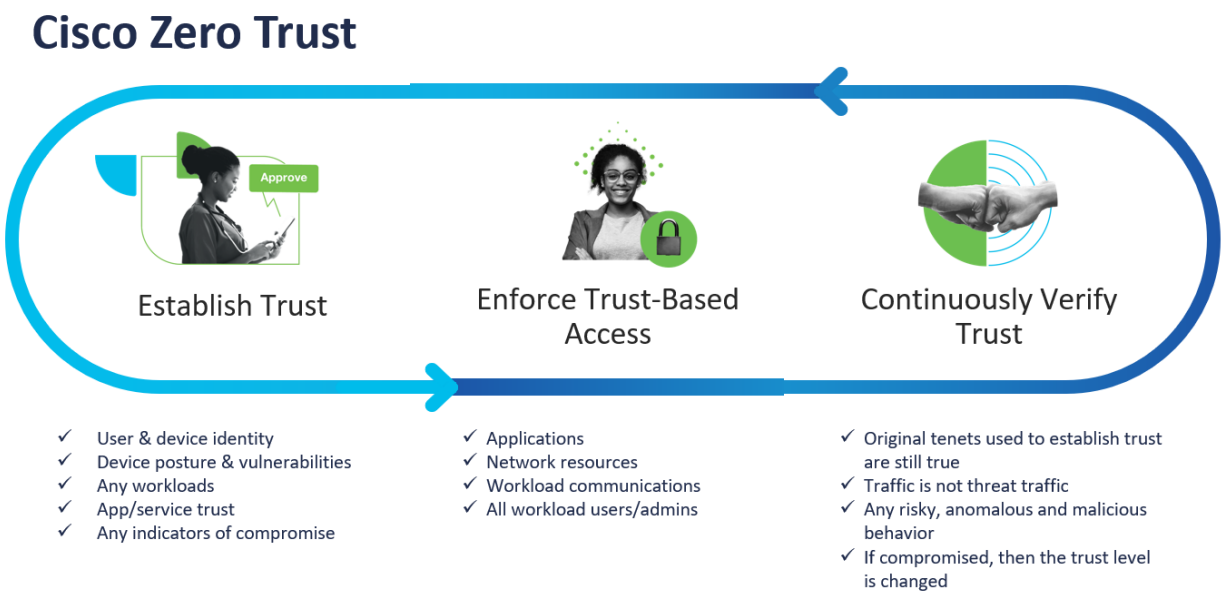


4.1.Zero Trust – Security First Approach

Only approved devices, endpoints and users should be able to connect to the network!

The traditional security model of perimeter-based security assumes that everything inside a network can be trusted and that everything outside the network is a potential threat. However, this approach has proven to be inadequate in the face of increasingly sophisticated cyber threats, such as malware, phishing attacks, and insider threats. A breach of the perimeter can compromise the entire network and sensitive data. Increasingly the threat actors are exploiting vulnerabilities in medical devices which go unmanaged to take control and initiate a security breach.

In response to these challenges, the zero-trust security model was developed. Zero-trust security assumes that every user, device, and application is potentially untrustworthy and must be verified before being granted access to sensitive data. This approach helps to minimise the risk of unauthorised access and data breaches.



The zero-trust security model is based on the following principles:

1. Verification: All users, devices, and applications must be verified before being granted access to sensitive data. Verification includes authentication, authorization, and continuous monitoring of user behaviour.

2. Least privilege: Users should only be granted the minimum level of access necessary to perform their jobs. This approach helps to limit the potential damage that can be caused by a compromised user account.

3. Micro-segmentation: The network should be divided into smaller segments, and access policies should be enforced at each segment. This approach helps to limit the lateral movement of attackers within the network.

4. Continuous monitoring: All activity within the network should be continuously monitored for signs of suspicious behaviour. This approach helps to detect and respond to threats in real-time.

5. Automation: Zero-trust security should be implemented using automated tools and processes to reduce the risk of human error and ensure consistency.

By applying these principles, healthcare organisations can create a security model that provides granular control over access to sensitive data, limits the risk of data breaches, and ensures compliance with privacy regulations. Implementing zero-trust security requires a comprehensive approach that includes network segmentation, identity and access management, and continuous monitoring of user and device behaviour. Cisco Identity Services Engine (ISE) plays a key role in establishing a strict security posture.

Zero trust verifies the user identity, the endpoint devices, and the device health, considers available context e.g location of the user, time of day etc., and based on this provides the minimum access to allow that user to successfully complete their current duties.

This approach not only help build GDPR compliance by design but also aligns the network to comply with the Caldicott Principles at the infrastructure level.

The Caldicott Principles also allow for the secure transfer of sensitive information across other agencies, for example Social Services, Education, Police and Judicial System. The seven Caldicott Principles relating to the use of patient identifiable information are:

1. Justify the purpose(s) of using confidential information
2. Only use it when necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

The network is fundamental to this “zero trust” security approach, being segmented in such a way that communication is only allowed between devices which need to communicate, by the users who are

authorised to access such data, provide the ability to contain a threat before it becomes a breach, and to limit the impact of any data breaches that may still occur. As the network sees all traffic, it also needs to detect anomalous behaviour, deviation from expected behaviour or an activity which may suggest a compromise to allow rapid containment and investigation. The network can be configured to take an action defined by security policy such as limiting access or quarantine the anomalous device, or revoke access for a user dynamically, thus dramatically improving the response time. This is where end to end visibility will play a crucial role as will be discussed later in this document.

4.2. Cisco ISE: At the Core of Zero Trust Strategy

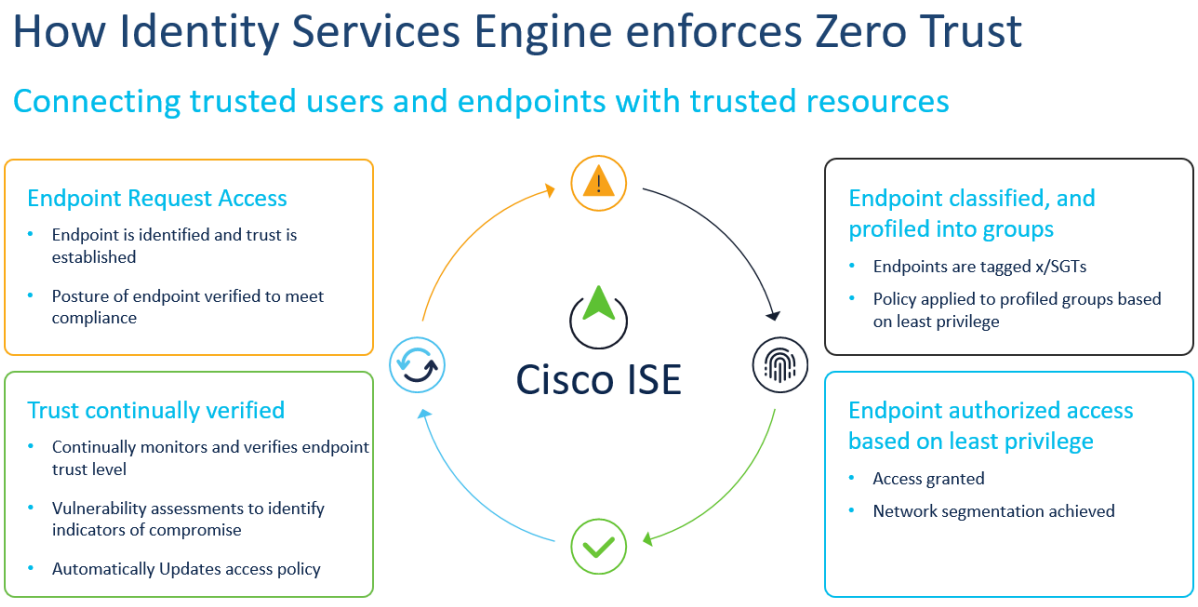
Cisco Identity Services Engine (ISE) is a network access control (NAC) solution that is at the core of implementing a zero-trust security model. It uses a combination of user and device authentication, network segmentation, and policy-based access control to enforce security policies and ensure that only authorised users and devices have access to network resources.

One of the key features of Cisco ISE is its ability to enforce access policies based on user and device attributes, such as the user's role or the device's operating system. This allows network administrators to define granular access policies that are tailored to specific users and device types. This can be further enhanced by capturing contextual data from medical devices (IoT) and using this data to secure not only IT endpoints but medical devices connecting to the network.

Cisco ISE also supports integration with other security system, such as firewalls and intrusion prevention systems (IPS), to provide an end-to-end security solution. This enables network administrators to create a unified security posture that spans across the entire network infrastructure and helps deliver the security policy consistently both within and outside the physical network boundaries.

In addition to access control, Cisco ISE provides visibility and control over network devices, medical devices, sensors, and applications. It can detect and classify devices on the network, and enforce policies based on device type and behaviour. It can also detect and block unauthorised applications and anomalous behaviour that could pose a security risk. Therefore, further enhancing and strengthening the security posture.

One Network, One Policy, One Experience



This concept provides several benefits, specifically –

- Multi-site – same policy regardless of location whether on-prem or hybrid working.
- Consistent user experience – within and outside the campus
- Medical Grade NAC – authenticate all devices, including medical devices

In relation to the overall security of the network, with the original objective of a closed secure network by default, the following benefits have been realised:

- Secure closed authentication and authorisation
- One Policy – Wired, Wireless and Remote
- Machine and User Authentication
- Same port config on every device
  Cisco TrustSec – simplifying policy

4.3. Network segmentation – The Basics

Network Segmentation is the process of dividing a network into smaller, more manageable sections or subnetworks. Each subnetwork is isolated from the others, creating a more secure and resilient network. This technique is particularly important in a hospital network, where patient data and other sensitive information are constantly transmitted and stored.

Some ways in which network segmentation can be applied in a hospital network and its benefits:

1. Protecting patient data: Patient data is one of the most sensitive types of information that is transmitted and stored in a hospital network and is protected by regulations. Network segmentation can be used to create a separate subnetwork for patient data, which is isolated from the rest of the network. This along with identity management can help prevent unauthorised access to patient data, which can lead to privacy violations and data breaches.

2. Segregating medical devices: Medical devices, such as MRI machines, ultrasound scan, X-Ray system and heart monitors, are often connected to a hospital network. These devices can be vulnerable to cyber-attacks, if left unmanaged, which can have serious consequences for patient health and safety and result in serious data breaches. Network segmentation can be used not only to create a separate subnetwork for medical devices, which is isolated from the rest of the network but isolate such devices if an anomaly or deviation from standards is detected, thus blocking a threat at the point of origin.

3. Isolating guest networks: Hospitals often have separate guest networks for visitors and patients. Network segmentation can be used to isolate these networks from the rest of the campus, preventing unauthorised access and reducing the risk of cyber-attacks originating from uncontrolled users and their devices.

4. Enhancing network performance: Network segmentation also help improve network performance by reducing congestion and optimising network traffic. By dividing the network into smaller subnetworks, network administrators can better manage network traffic and reduce the risk of wider network outages.

Network segmentation is an essential technique for creating a secure and resilient hospital network. By isolating sensitive information, protecting medical devices, and optimising network traffic, network segmentation can help to improve healthcare delivery resulting in better patient experience and protect patient privacy at the same time. Cisco Identity Services Engine (ISE) and Software-Defined Access (SD-Access) solutions will play a key role in implementing network segmentation effectively and efficiently.

The mechanisms traditionally adopted for segmentation are as follows:

- Virtual Routing and Forwarding: VRFs (also known as virtual networks)
- Virtual Local Area Networks L VLANs (virtual LAN) – most used to span “functions” across a site. Also used to reduce “broadcast domains”.

As we expand on these through the document, several operational challenges are identified – usually these are lack of flexibility, time taken to deploy, reliance on firewalls or ACLs to control access.

An access control list (ACL) consists of one or more access control entries (ACEs) that collectively define the network traffic profile.

When we look at the flexibility component, it is often seen that individual access ports are statically assigned to a VLAN e.g., "switchport access vlan 100". Any device plugged into this port would by default, inherit any access to the network that is permitted for VLAN100. Clearly this isn't an optimal solution especially when we have a variety of devices such as medical devices, sensors, and cameras connected to the network.

To put this into context, in a typical NHS local area network, literally thousands of devices (endpoints) require connectivity – both wired and wireless. Whilst that statement may appear to be obvious, enabling this requirement at scale can be a time-consuming and resource intensive task, usually carried out by a relatively small team of people.

There are a variety of solutions that can be used to implement network segmentation in a hospital network. The main emphasis needs to be on automation and policy driven approach. An example is using the Cisco Identity Services Engine (ISE) and Software-Defined Access (SD-Access).

Cisco ISE is a policy-based access control system that enables network administrators to control access to network resources based on user identity, device type, and location. With Cisco ISE, network administrators can create policies that restrict access to sensitive information and resources, ensuring that only authorised users and devices can access them. Cisco ISE can also be used to create micro-segmentation, which is the process of dividing a network into further smaller subnetworks based on organisation's security policies.

Cisco SD-Access is a fabric-based networking solution that enables network administrators to automate network segmentation and policy enforcement. With Cisco SD-Access, network administrators can create policy-based network segments, based on user identity, device type, and location. Cisco SD-Access also helps automate network segmentation, making it possible to implement and manage segmentation throughout the network at scale which is otherwise difficult to achieve if done manually.

Steps involved in implementing network segmentation:

1. Identify network resources: identify the network resources that need to be protected and isolated. This includes patient data, medical devices, and guest networks.

2. Define security policies: define security policies that restrict access to these network resources based on user and device posture which is based on user identity, device type, and location. This can be done using Cisco ISE, allowing to create policy-based access control.

3. Create network segments: create network segments based on these security policies. This can be done using Cisco SD-Access, allowing to create policy-based network segments.

4. Implement network access control: implement network access control using Cisco ISE. This can be done by configuring Cisco ISE to enforce security policies and restrict access to network

resources based on user identity, device type, and location.

5. Monitor network activity: monitor network activity to ensure that security policies are being enforced effectively. This can be done using Monitoring and Troubleshooting Service in Cisco ISE and Thousand Eyes.

    Monitoring: Provides real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and monitor operational conditions.

    Troubleshooting: Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide resolution in a timely manner.

    Reporting: Provides a catalogue of standard reports that you can use to analyse trends and monitor system performance and network activities. You can customize reports in various ways and save them for future use.

    ThousandEyes: integrates monitoring and visualisation of device health, end-to-end network paths and the performance of your internally hosted and cloud applications in one place. Identify critical dependencies in your network and monitor how device health impacts application performance.

Segmentation and 802.1X are two different concepts, but they are often used together to enhance network security. We have dedicated a section to discuss 802.1X implementation in detail. Please refer section 5

Cisco Software-Defined Access (SD-Access) is a comprehensive solution for network segmentation. SD-Access uses an Identity Services Engine (ISE) for policy-based segmentation. SD-Access uses Virtual Extensible LAN (VXLAN) for segmentation, which enables the creation of logical networks that span across multiple physical networks. We have dedicated a section to just focus on this. Please refer Section 7

Cisco TrustSec. TrustSec is a policy-based access control solution that allows network administrators to define and enforce segmentation policies across the entire network, from the access layer to the data center. TrustSec uses Security Group Tags (SGTs) and Security Group Access Control Lists (SGACLs) to control access to network resources. This is explained in the section that follows.

4.4. Cisco TrustSec

Most organisations have evolved or developed their infrastructure based on Core-Distribution-Access or Collapsed Core/Distribution and Access topologies - where the VLAN SVI (switch virtual interface aka default gateway for the subnet assigned to the VLAN) resides on the core switch. As mentioned earlier, in a resilient link architecture, this exposes the entire LAN to convergence issues with spanning-tree, HSRP etc.

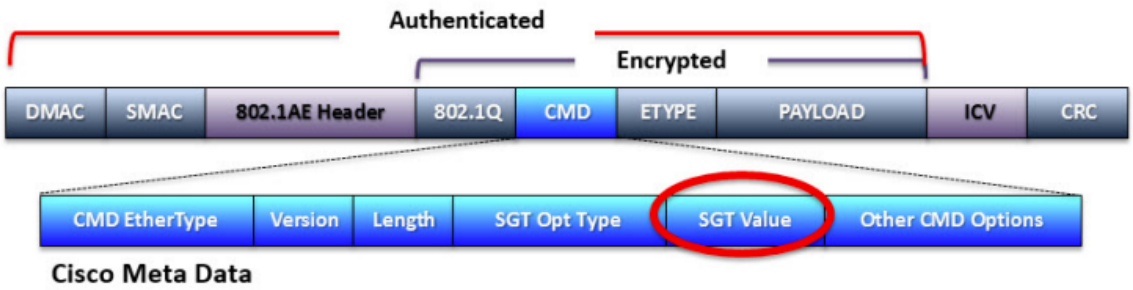
An additional consideration is access control under this methodology. Usually, control of what an endpoint device can access is based on Access Control Lists or Firewall rules. Both of which require constant adds/moves/changes. This consumes valuable time in the Network Operations (NetOps), Security Operations (SecOps) and server teams, and is prone to human error.

The result is access switch configuration, which is unique to each device, for example: switchport access vlan xxx, switchport trunk allowed vlan xxx etc. Every time a device moves, potentially, someone must change the VLAN associated to that port. Or the devices end up in a different VLAN, with a different subnet assigned, so a firewall rule or ACL must be changed as the user/device can no longer connect to the required service.

Cisco TrustSec uses Security Group Tags (SGTs), Security Group Access Control Lists (SGACLs), and the Identity Services Engine (ISE) to enforce access control policies. This is to overcome the limitations as posed by the traditional way to configure devices as explained above.

SGTs are used to tag network devices and users with a unique identifier that represents their security group membership. Cisco TrustSec uses these tags to represent logical group privilege. and is used to define and enforce access policies. The SGT is understood and is used to enforce traffic policies by Cisco switches, routers, and firewalls.

Security Group Tags (SGTs) allow for the abstraction of a host's IP Address through the arbitrary assignment to a Closed User Group, represented by an arbitrarily defined SGT. These tags are centrally created, managed, and administered by the ISE. The Security Group Tag is a 16-bit value that is transmitted in the Cisco Meta Data field of a Layer 2 MACsec Frame as depicted below.



Security Group Tags allow an organisation to create policies based on a user's, device's, or server's role in the network providing a layer of abstraction in security policies based on an SGT as opposed to IP Addresses in ACLs.

This grouping into SGTs forms the basis of Micro-Segmentation. Before we look at CTS and SGT segmentation, we should first look at a higher-level concept – Macro-Segmentation.

SGACLs are used to enforce access control policies based on security group membership. These policies can be defined at the access layer, distribution layer, and core layer of the network, providing a comprehensive solution for network segmentation and access control. Using security group access control lists (SGACLs), you can control the operations that users can perform based on the security group assignments of users and destination resources. Policy enforcement within the Cisco TrustSec domain is represented by a permissions matrix, with source security group numbers on one axis and destination security group numbers on the other axis. Each cell in the body of the matrix can contain an ordered list of SGACLs which specifies the permissions that should be applied to packets originating from the source security group and destined for the destination security group.

4.5. Macro Segmentation - VNs, VRFs, Virtual Networks.

Virtualisation is a technique for hiding the physical characteristics of computing resources from the way in which other systems, applications, or end users interact with those resources. This includes making a single physical resource (such as a server, an operating system, an application, storage device, or network) appear to function as multiple logical resources; or it can include making multiple physical resources (such as storage devices or servers) appear as a single logical resource.

One of the impactful ways of providing segmentation, for example, separating guest traffic from hospital core requirements, is using Virtual Networks.

Network virtualization allows a single physical router to have multiple route tables. The global table contains all IP interfaces that are not part of a specific virtual network and route tables are for each unique virtual network assigned to an IP interface.

Virtual Route Forward (VRF) is a technique which creates multiple virtual networks within a single network entity. In a single network component, multiple VRF resources create the isolation between virtual networks.

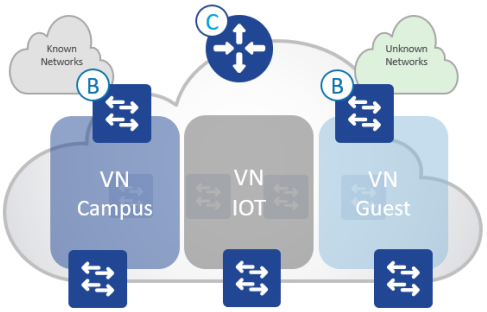
Very simply, by default and by design, traffic in different VRFs cannot communicate.

Virtual Routing and Forwarding or VRF allows a router or switch to run more than one routing table simultaneously. When running multiple routing tables at the same time, they are completely independent. This has the added advantage of allowing overlapping RFC1918 IP addressing schemas, if required.

Traditionally, VRF were in the realm of Service Providers running large scale MPLS based infrastructure and required the use of protocol such as MP-BGP. However, similar functionality in relating to segmentation or path-isolation – keeping traffic apart, can be achieved using VRF-lite on Cisco Switches.

Virtual Network maintains a separate Routing & Switching table for each instance

- Control-Plane uses Instance ID to maintain separate VRF topologies ("Default" VRF is Instance ID "4098")
- Nodes add a VNID to the Fabric encapsulation
- Endpoint ID prefixes (Host Pools) are routed and advertised within a Virtual Network
- Uses standard "vrf definition" configuration, along with RD & RT for remote advertisement (Border Node)
- Up to 256 VRF's supported on Cat.9k platforms



VRFs are created, usually on the core / border switch. When each VRF is configured, each VRF needs route distinguisher to become functional.

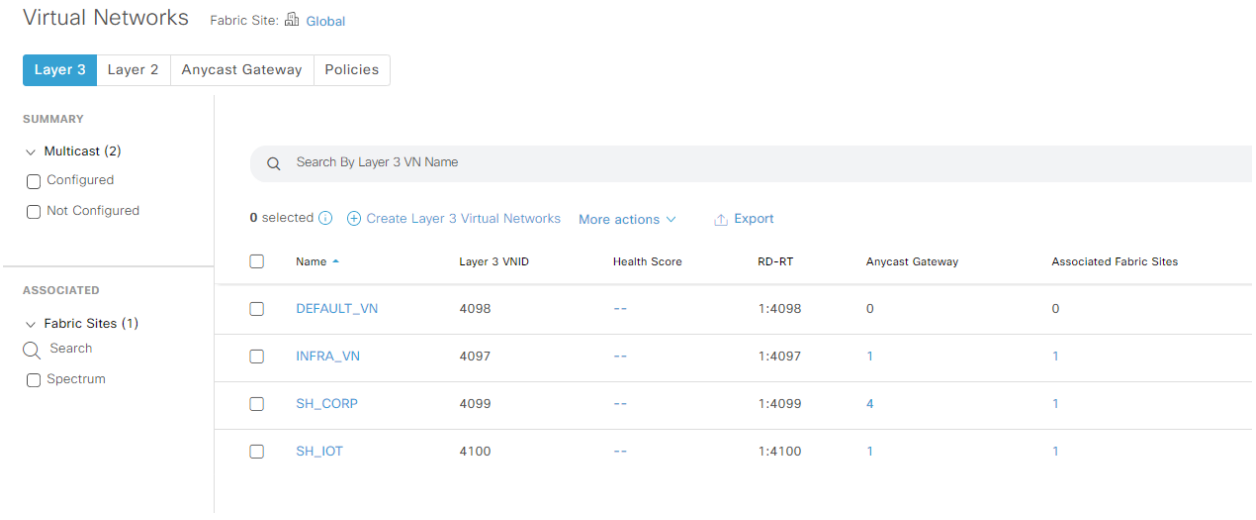
```
sda2cpb1#sho run | s vrf
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
vrf definition SH_CORP
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
vrf definition SH_IOT
 rd 1:4100
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family
```

When used with traditional VLANs, macro segmentation can be enabled simply by including a single line in the interface vlan configuration (SVI)

ip vrf forwarding (vrf-name)

It should be noted, that by default, traffic in different VRFs cannot communicate, unless the traffic traverses a firewall where access rules can allow such inter-vrf communication, or via a concept referred to as “route-leaking” which can be performed on an upstream device – usually the core switch in a traditional collapsed core topology.

When we consider this with Software Defined Access, the process becomes fully automated across the entire campus through Cisco DNA-Centre.



4.6. Micro-Segmentation

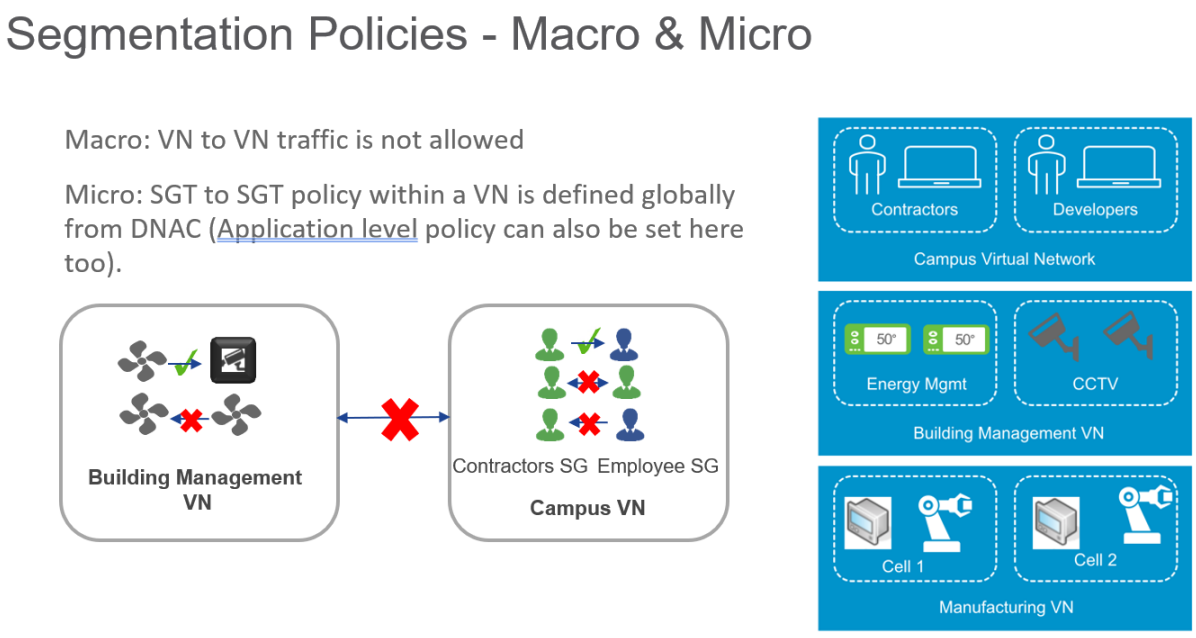
When macro segmentation is deployed with VRFs, there are clearly requirements to further control access between devices within the same VN/VRF.

In a traditional methodology using VLANs, again this would be achieved using ACLs or Firewall rules.

Security policy in CTS/SDA (Cisco TrustSec/ Software Driven Networks) is group-based. Policy is based on groups of entities as opposed to creating IPACLs for each individual endpoint or location. Each group is defined by a Security Group Tag (SGT). Security policy is disassociated from the local constructs such as VLAN, Subnet and IP address and is based on group names which is meaningful to the organisation and is relevant globally.

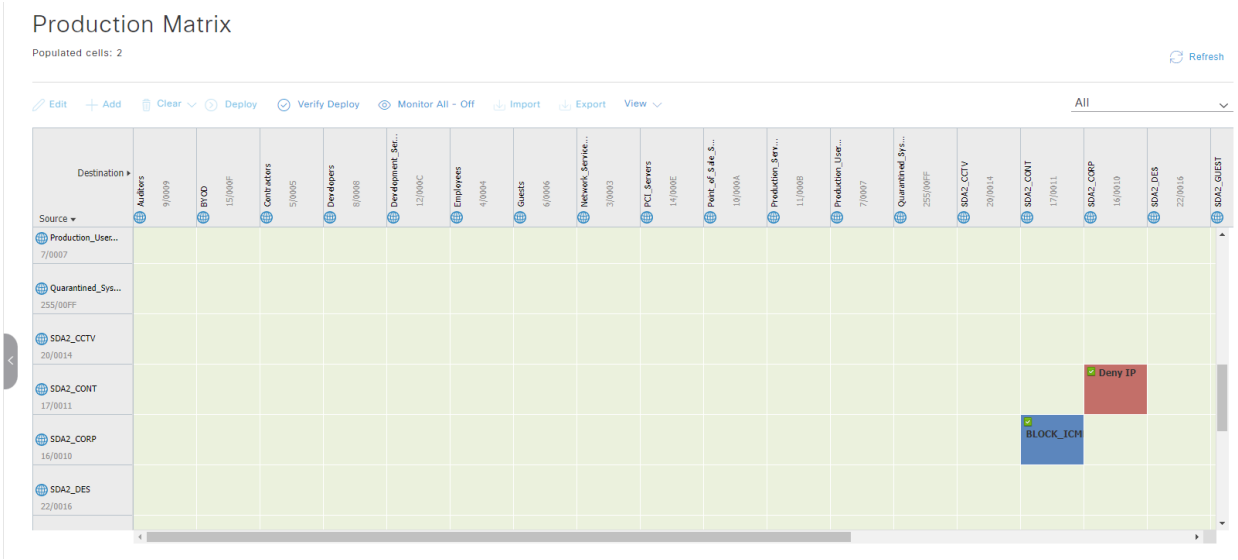
Endpoints are classified into groups either dynamically or statically. When users connect to the network, the edge/access devices communicate with ISE and an SGT is assigned by ISE by using configured conditions. ISE learns a large amount of context which can be used within these conditions.

Once endpoints and users are classified into groups then the security policy can be defined. The policy can be defined from one group to another, between two groups or between members of the same group. The contract used within the policy is either a pure permit, a pure deny, or a list of Security Group Access Control Entries (SGACE's) for granular traffic control.

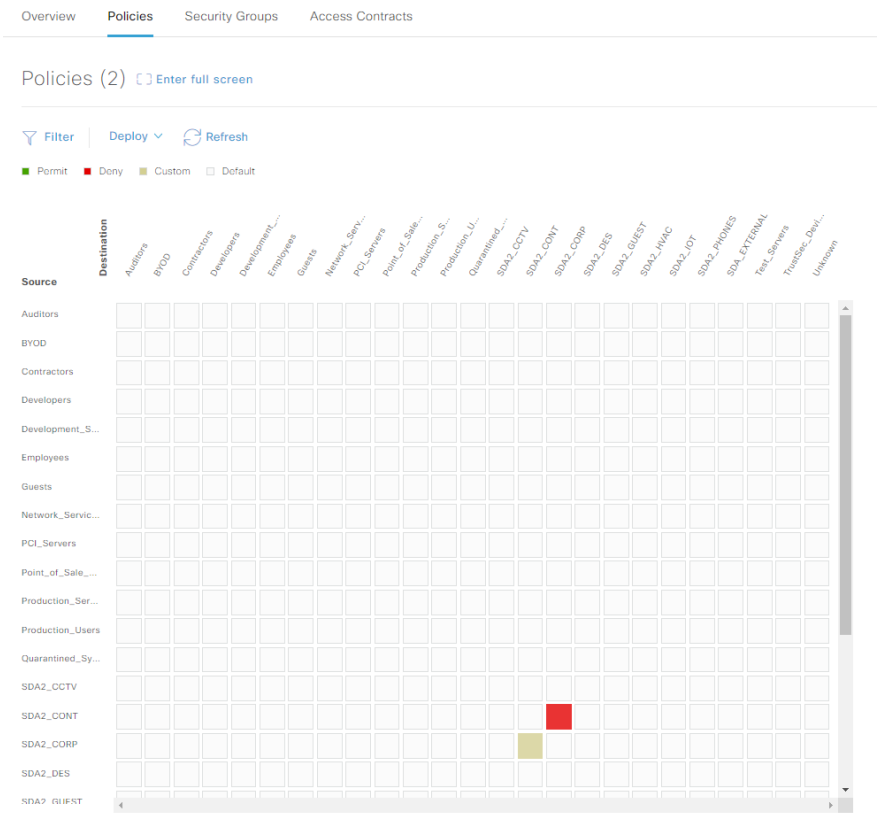


With CTS, access contracts are created in a TrustSec matrix. This can be achieved either through ISE, or when DNA-C is integrated with ISE, all functionality is then configured and displayed via DNAC.

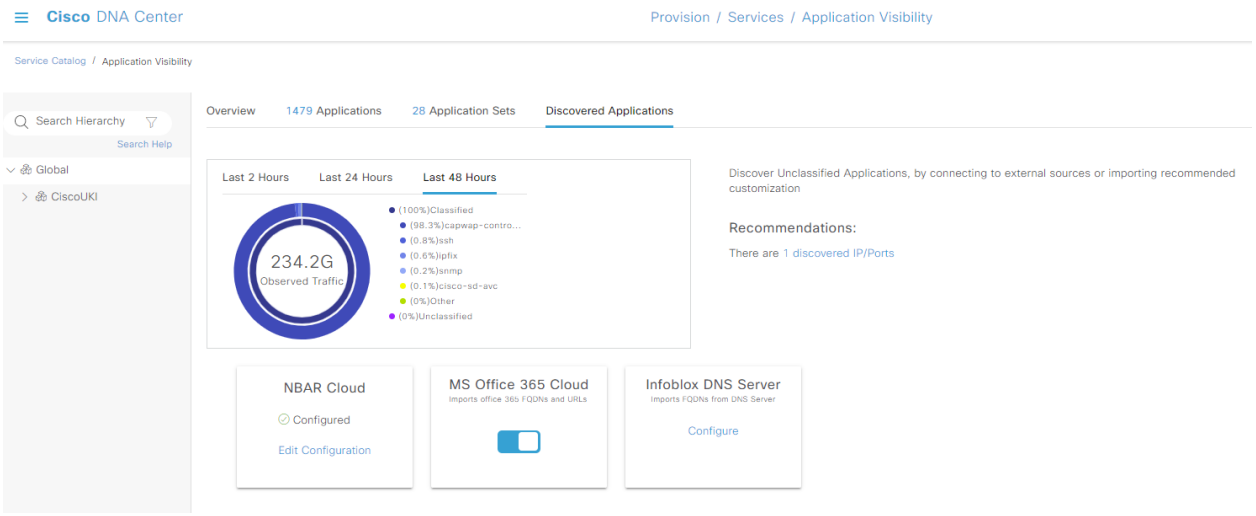
Example of ISE CTS Matrix:



Example of Group Based Access Control in DNAC

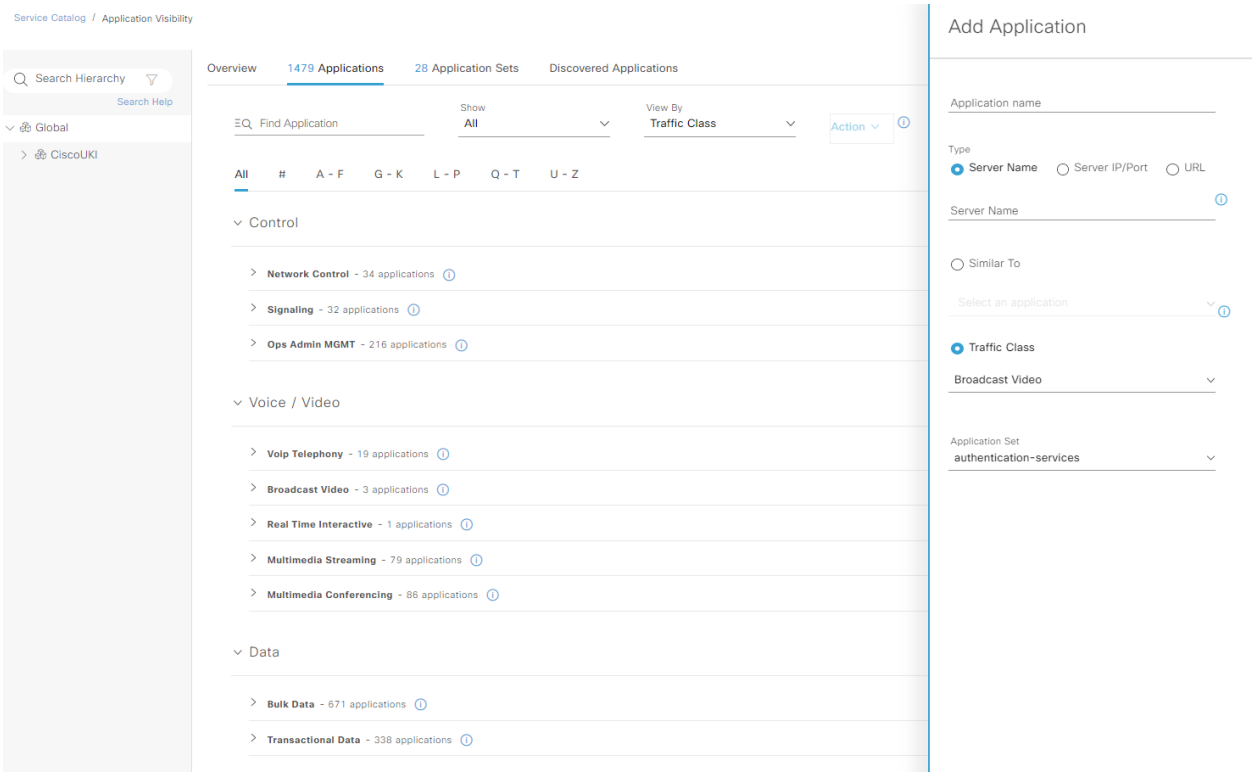


Access contracts (policies) are simple created by clicking on the intersection between SGTs, or even the same SGT. These contracts can be permit, deny, or even based on specific applications – the list is populated through NBAR (network-based application recognition) or CBAR (controller-based application recognition). The latter allowing for custom defined applications:

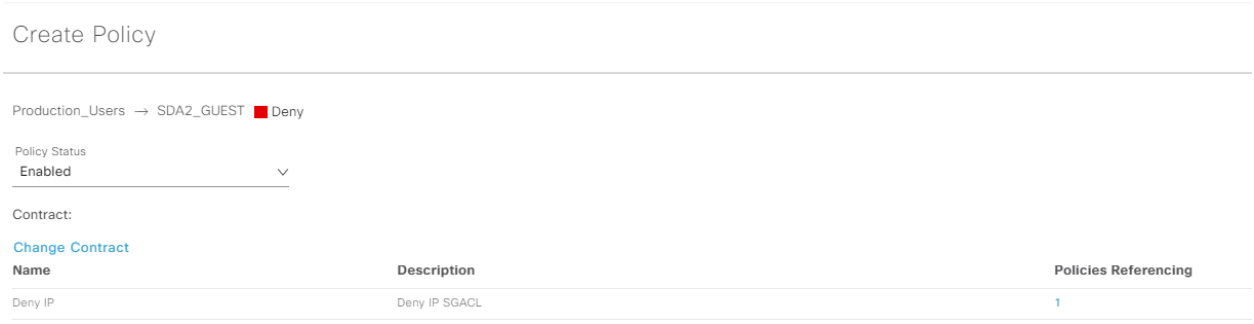


Cisco DNA-C, using telemetry enabled on edge/access devices, will automatically learn of new applications based on traffic flows, and recommend creation of the app to add to the list.

A policy for application can easily be created from within DNA-C as shown below:



These policies are then applied and deployed from a single point of interface within DNA-C.

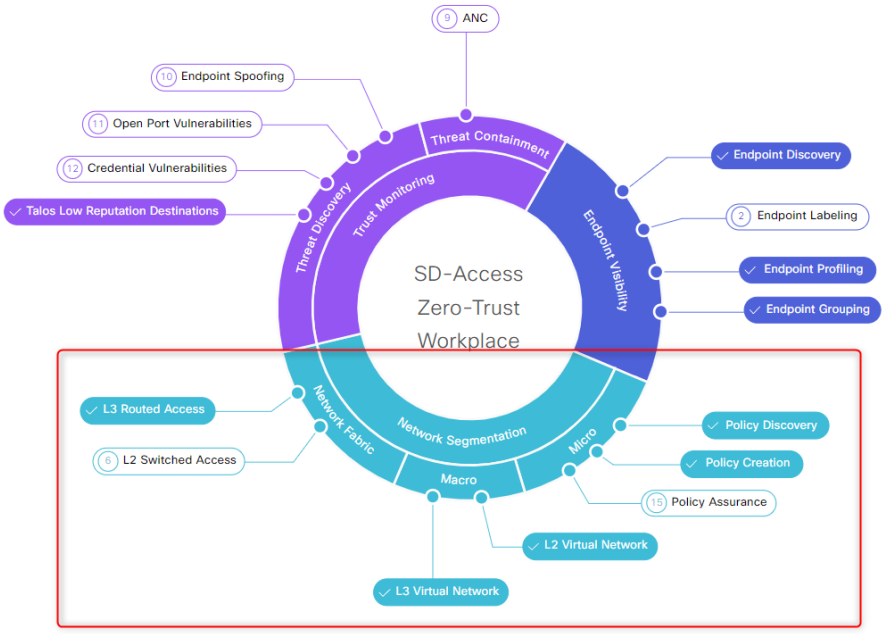


With CTS enabled, IT teams no longer need to configure or change ACLs, firewall rules etc. And deployment of new policies becomes instantaneous.

It is worth noting that CTS can be deployed in a fabric or non-fabric environment.

CTS policies apply to both Wired Access and Wireless Access – the same policy is enforced.

From a Zero Trust Perspective, we have now covered another section:



The following are links to the detailed guides on this technology:

- https://community.cisco.com/t5/networking-documents/cisco-ai-endpoint-analytics-and-cisco-ise-integration/ta-p/4093538#toc-hId--1272194461
- https://community.cisco.com/t5/security-documents/segmentation-strategy/ta-p/3757424
- https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_auth_pol.pdf
- https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/TrustSec/branch-segmentation.pdf
- https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Segmentation-Design-Guide-2018MAY.pdf
- https://community.cisco.com/t5/security-knowledge-base/policy-provisioning-and-operation-in-sda/ta-p/3712744

5. Deploying 802.1X

802.1X is a network access control (NAC) protocol that provides authentication and authorization for devices connecting to a network. It requires devices to provide valid credentials before being granted access to the network. This allows network administrators to control who has access to network resources and enforce security policies.

By using 802.1X in conjunction with network segmentation, network administrators can ensure that devices are only allowed to access the resources that they are authorised to access. For example, a guest device connecting to a hospital network can be placed in a separate network segment and given limited access, while a medical device can be placed in a separate segment with more stringent security policies.

Segmentation and 802.1X are complementary concepts that can be used together to create a more secure and resilient hospital network. By segmenting the network and using 802.1X to control access to each segment, network administrators can ensure that sensitive resources are protected and only accessible to authorised users and devices.

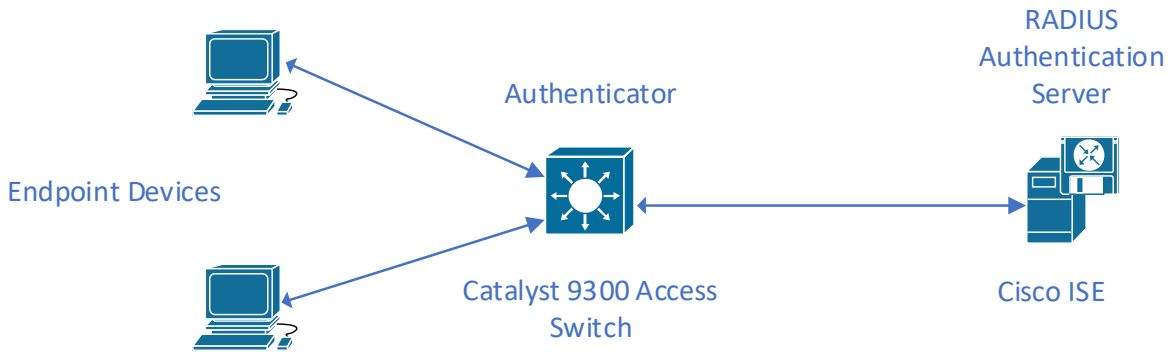
To expand on this concept, the starting point is to enable 802.1X for both wired and wireless access.

802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the end user or device.

802.1X enables port-based access control using authentication. An 802.1X-enabled port can be dynamically enabled or disabled based on the identity of the user or device that connects to it[1].

Most organisations already use 802.1X (802.1X) on their Wireless LAN (WLAN) infrastructure – it's almost enabled by default!

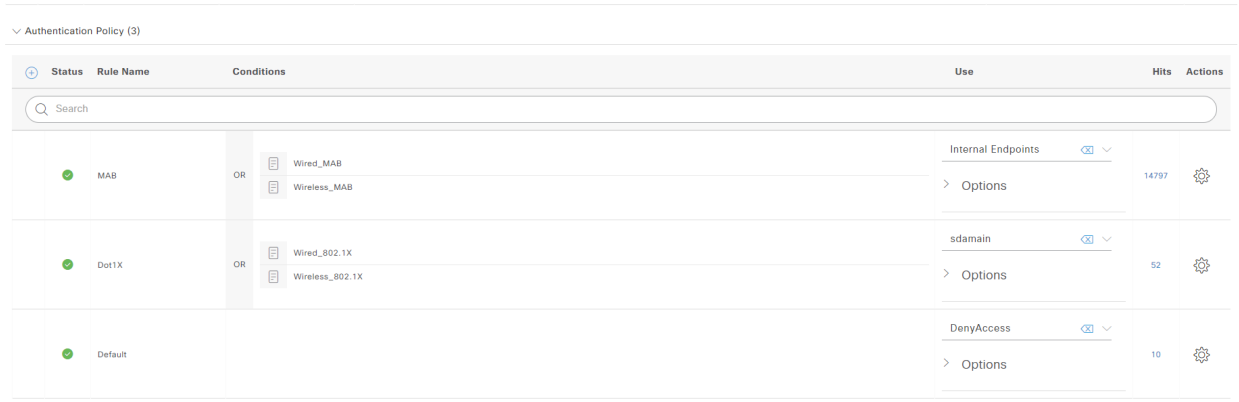
With 802.1X enabled, IT can control access to the network based on Identity – a key component of Cisco Digital Network Architecture (DNA).



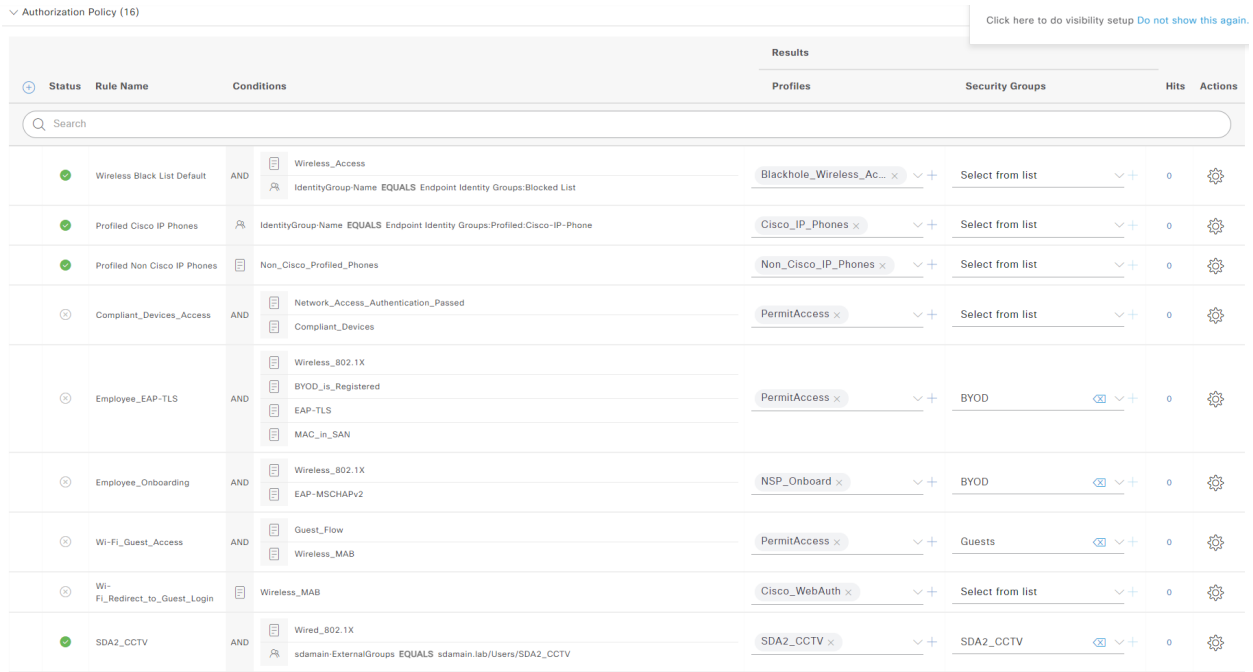
**This is only an example diagram and not representative for products that support 801.1X technology and features.*

[1] Wired 802.1X Deployment Guide - https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html

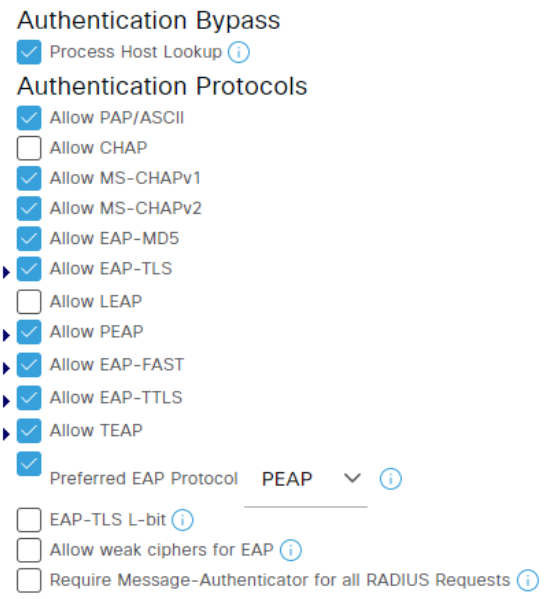
Authentication Rules. - With 802.1X enabled, typically, dynamic VLAN allocation can be performed, based on the user's identity. Cisco ISE will be integrated into MS Active Directory (or other identity source, LDAP etc) where a user's credentials can be checked.



Authorization Rules (and results) are then created in Cisco ISE to assign endpoints (users, devices) with a specific VLAN, or in the case of TrustSec a Security Group – more on that to follow!



The actual authentication mechanism is called EAP (Extensible Authentication Protocol) of which there are many variants – typically in a wireless environment, user credentials are used: PEAP, or certificate based – EAP-TLS, or a combination of both. (EAP-Chaining) or TEAP.



The result is that IT teams do not have to manually configure individual ports to specific VLANs, and only approved users/devices can access the network!

A deployment guide[2] is available to assist with the deployment of 802.1X using Cisco Identity Service Engine, along with a video[3].

For devices that can't enter credentials, or use a trusted Certificate based mechanism MAC Authentication Bypass can be used.

As we discuss the use of 802.1X to establish strict control to network resources, specifically on the wired environment, we often hear that it is simply too difficult to deploy.

Fortunately, we now have mechanisms to simplify and rapidly deploy this technology.

It should be well noted from the start, that the business objectives of providing segmentation must be well planned and considered – to put it simply, who or what can access what? It is this process that usually consumes time and effort.

A common method of adoption is to maintain VLAN access – but to dynamically assign the VLANs to devices, this removes the need for static assignment, and importantly, different configurations on each access port.

The objective is to simplify the network deployment – make every port the same. This obviously hugely reduces the administrative and operational overhead on the IT function.

Some of the guides identified above go into considerable details on this process, however, it can be broken down into smaller steps.

[2] Cisco ISE Wired Access Deployment Guide - https://community.cisco.com/t5/security-knowledge-base/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515
[3] 802.1X Simplification & Automation (video): https://www.youtube.com/watch?v=ivfP1rJrtfU

1. Deploy the AAA – Authentication, Authorisation and Accounting services onto the access layer. This provides the references to the RADIUS (in this case – ISE) servers that will provide the access control.
2. Configure Identity Based Networking (IBNS) templates on the access layer. This provides the options for monitor, low impact and closed authentication modes.
3. Assign the templates to access layer ports.

The 3 steps identified above can easily and rapidly deployed using Cisco DNA Centre's PnP functionality for DayN templates. These features allow IT to "push" configurations to existing devices with minimal manual configuration.

The Plug-and-Play (PnP) functionality is built-in feature in Cisco DNA Center which can help automate onboarding for switches, routers, and wireless access points to the network.

A Day N template in Cisco DNAC refers to a configuration template that can be used to automate ongoing configuration changes.

With IBNS/802.1X deployed across the access layer, the organisation can then start to identify what devices are in use, where they are connected, and importantly, what those devices are communicating with.

Again, it is worth re-iterating that 802.1X does NOT require SDA or a Fabric to be deployed. This can be deployed using the traditional VRF and or dynamic VLAN assignment. Dynamic VLAN assignment is one such feature that places a user into a specific VLAN based on the credentials supplied by the user. However, as we have previously discussed – the use of TrustSec and SGTs greatly reduces the administrative overhead and provides insightful analytics into device communication.

The concern over how devices can get onto the network when they have no "supplicant" available – i.e., no login screen, is addressed through MAB – "MAC Authentication Bypass". We have already discussed how IBNS/802.1X can be deployed in Monitor mode – i.e., see what's there, but ensure access is still provided. With this mechanism in place, organisations can fully discover every device connected, without impacting access.

This is especially important for medical devices, building management systems (BMS) etc, as previously identified.

Low impact mode – where policies can be tested, again, without impacting access, can be deployed to provide a "what-if" scenario before fully securing the network.

The end goal is to achieve "closed mode" – this is where only recognised, authenticated, and authorised devices can connect to the network.

In addition to securing the network, this also establishes the basis for segmentation.

5.1. MAC Authentication Bypass (MAB)

The need for secure network access has never been greater. Consultants, contractors, and even guests now require access to network resources over the same LAN connections as regular employees, who may themselves bring unmanaged devices into the workplace. As data networks become increasingly indispensable in day-to-day business operations, the possibility that unauthorised people or devices will gain access to controlled or confidential information also increases.

One access control technique that Cisco provides is called MAC Authentication Bypass (MAB). MAB uses the MAC address of a device to determine the level of network access to provide. MAB offers visibility and identity-based access control at the network edge for endpoints that do not support IEEE 802.1X. With the appropriate design and well-chosen components, you can meet the needs of your security policy while reducing the impact on your infrastructure and end users.

For numerous devices across the Campus, they do not have the ability to enter credentials or have certificates stored for authentication. Typical examples:

- Medical Devices
- Building Management Systems
- Printers
- IoT
- CCTV
- Door Access Controllers

Cisco ISE can authenticate these devices using MAB. This can be further enhanced through specific Unique Device Identifiers - UDI.

Devices are placed into endpoint groups, and again authentication rules (802.1X/MAB) are used to enable access. Based on the device group membership, authorisation rules can be used to allocate – for example, a VLAN ID or allow/deny access to resources on the network such as electronic patient records.

A sample of step-by-step process for how Cisco ISE along with Cisco DNA Center (DNAC) can be used to implement secure access:

1. Determine access policies: The first step is to define the access policies that will be enforced on the network. This includes defining who can access which resources, and under what conditions. Access policies should be based on user and device attributes, such as user role, device type, and location.

2. Configure Cisco ISE: Once the access policies have been defined, the next step is to configure Cisco ISE to enforce those policies. This includes configuring authentication methods, such as 802.1X, and defining access policies based on user and device attributes.

3. Deploy Cisco DNA Center: Cisco DNA Center is used to provision, manage, configure the network devices, and to automate network operations.

4. Deploy and provision network devices using DNAC: Network devices, such as switches, routers, wireless access points and firewalls can now be deployed. This includes configuring the devices to use 802.1X authentication and configuring them to communicate with Cisco ISE.

5. Configure network segmentation: Cisco DNAC can now be used to configure network segmentation based on user and device attributes. This includes configuring virtual networks and access control policies based on Security Group Tags (SGTs) as explained in detail earlier.

6. Monitor and manage network: After deploying and configuring the network, it is crucial to monitor and manage it to ensure proper enforcement of access policies and security measures. This involves keeping track of network traffic and promptly responding to security threats. For a comprehensive solution that offers end-to-end visibility and actionable insights, you might consider using Cisco ThousandEyes. Additionally, the monitoring and troubleshooting capabilities built into Cisco ISE can be utilised to provide additional support.

Cisco DNA-Centre will also form a bi-directional exchange with ISE to further enhance endpoint classification and profiling.

With the endpoint database automatically populated, devices can then be sorted either manually – or automatically via profiling, into endpoint groups.

Network Probes Used by Profiling Service:

Network probe is a method used to collect an attribute or a set of attributes from an endpoint on your network. The probe allows you to create or update endpoints with their matched profile in the Cisco ISE database.

Cisco ISE can profile devices using several network probes that analyse the behaviour of devices on the network and determine the type of the device. Network probes help you to gain more network visibility.

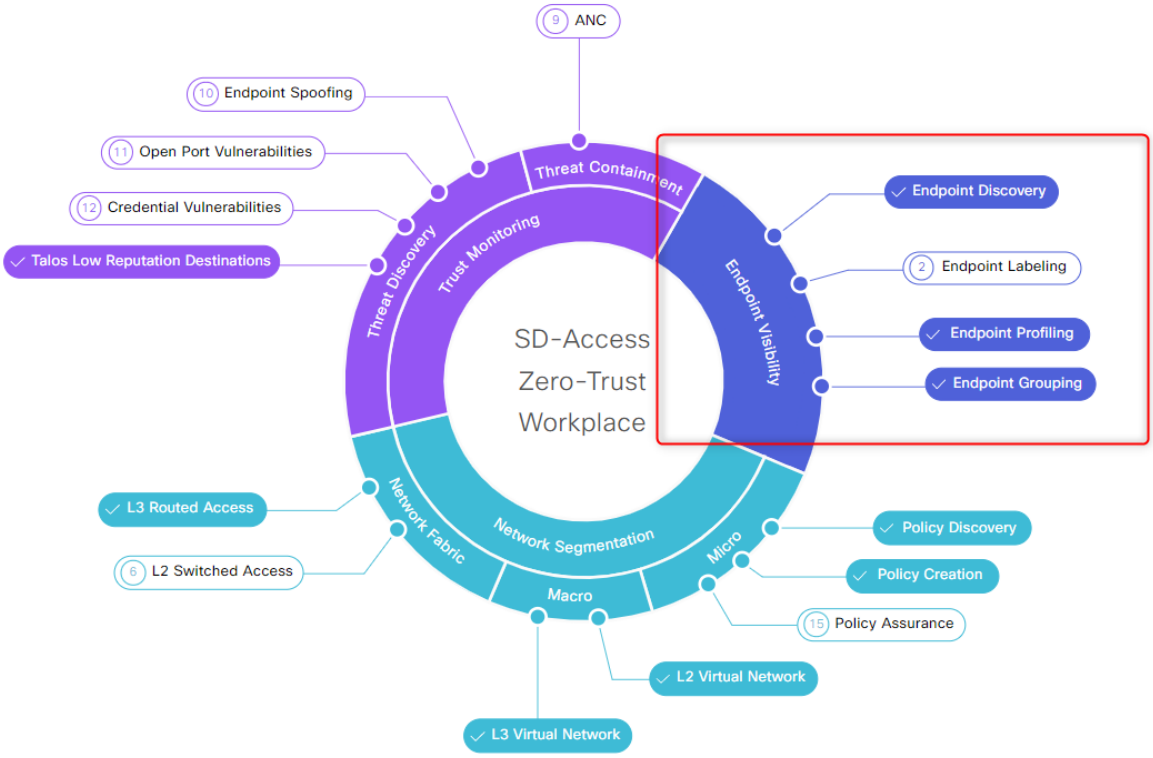
- IP Address and MAC Address Binding
- NetFlow Probe
- DHCP Probe
- DHCP SPAN Probe
- HTTP Probe
- HTTP SPAN Probe
- pxGrid Probe
- RADIUS Probe
- Network Scan (NMAP) Probe
- DNS Probe
- SNMP Query Probe
- SNMP Trap Probe
- Active Directory Probe

Where does this all fit with Zero Trust?

Zero Trust is a concept built between Cisco ISE and Cisco DNA-C. DNA-C is used as the primary interface for identification, management, classification, and visibility into devices across the campus.

DNA-C incorporates the use of AI Endpoint Analytics to further enhance this functionality.

It is crucial to understand that by deploying 802.1X on both wired and wireless access, we have already achieved the first and fundamental aspect of the HIS – the network is no longer in an "open" state, and only authorised devices will be permitted to access the network.



5.2. AI Endpoint Analytics

Cisco AI Endpoint Analytics is our next-generation endpoint visibility solution that provides deeper context by analyzing your network and IT ecosystem. This solution makes all endpoints easily visible and searchable and employs advanced techniques to detect and reduce the number of unknown endpoints in your enterprise. Some of these techniques are as follows :

1. Deep packet inspection (DPI) gathers deeper endpoint context by scanning and understanding applications and communications protocols of IT, Building Automation and Healthcare endpoints.

2. Machine learning (ML) intuitively groups endpoints with common attributes and helps IT administrators label them. These unique labels are then anonymously shared with other organisations as suggestions, where similar groups of unknown endpoints may be observed. This helps reduce the unknown endpoints and group them based on newer labels.

3. Integrations with Cisco and third-party products provide additional network and non-network context that is used to profile endpoints.

In summary, Cisco AI Endpoint Analytics[7] reduces or eliminates the first hurdle that many of our healthcare customers face when implementing security policies: overcoming a lack of visibility of endpoints, with high fidelity.

The network is now secure. Only approved endpoints can connect, including devices where no authentication mechanism is available. However, we still have a dependency on VLANs, and all the complexities and weaknesses associated with it.

If we recap on the increased burden of managing ACLs, firewall rules etc, it still means there is a high-level of manual administration required to ensure appropriate access control is enabled. I.E., what devices can talk to what, for example, preventing Canteen PoS terminals communicating with X-Ray imaging DICOM servers.

If we are to further reduce this burden, there needs to be another mechanism of controlling access policies - Cisco TrustSec.

To safeguard your critical business assets, network segmentation is crucial. However, traditional approaches can be complicated. Thankfully, Cisco TrustSec offers a simpler solution with software-defined segmentation, which is much easier to enable compared to VLAN-based segmentation.

Cisco TrustSec is an open standard developed by Cisco and submitted to the Internet Engineering Task Force (IETF) as a proposed standard, making it accessible to a wider range of users, and it is available within 'OpenDaylight', a popular open-source software-defined networking (SDN) platform. Additionally, TrustSec is supported on both third-party and Cisco platforms, providing users with greater flexibility in their network infrastructure choices.

[7] Cisco AI Endpoint Analytics White Paper - https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-ai-endpoint-analytics-wp-cte-en.html

5.3. Profiling

Endpoint profiling starts with aggregating and analysing endpoint data from various data sources. Examples of these data sources include network devices or appliances supporting deep packet inspection, Cisco Identity Services Engine (ISE), external configuration databases, and more. Endpoints are categorized and labelled by comparing data from these sources and from endpoints themselves to an extensive library of endpoint fingerprints or system rules to find the best match[8].

Cisco AI Endpoint Analytics provides you with granular endpoint profiling details by defining the endpoint type, manufacturer, model, and operating system. To support this goal, system rules are updated frequently by constantly listening and analysing endpoint data from a large set of application and discovery protocols and from more than 250 attributes. The system rule library is a composite of a variety of IT and IoT devices in an enterprise's carpeted space, healthcare, building management, and more. Beyond the system rule library, Cisco AI Endpoint Analytics has a machine-learning component that helps build endpoint fingerprints, when they are not otherwise available, to reduce the net unknown endpoints in your environment.

We have already learned that ISE and DNA-C can discover endpoints connected to the network, and specifically, where they are connected. This alone will enable IT to further understand who or what is on the network.

Device profiling then takes this functionality and enhances it to easily allow IT to ensure correct policies are in place for specific devices. E.G., access from a tablet device may be deemed to be different from access from a PC or workstation.

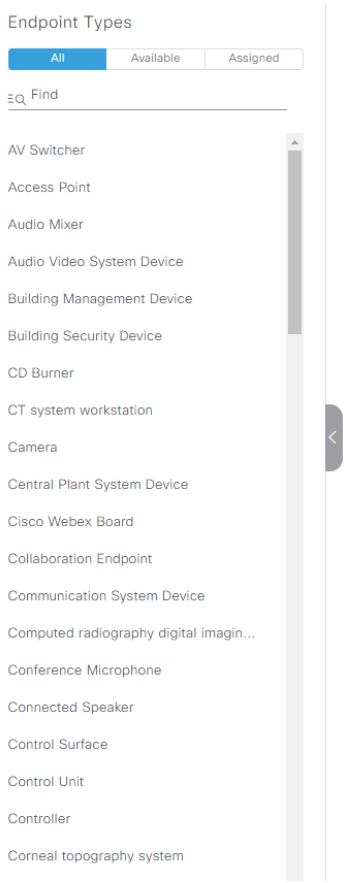
This becomes increasingly more significant when Medical Device NAC[9] is required. Very often a block to deploying a future proof access control and segmentation policy is when medical devices are involved. We have previously shown how these can be accommodated in the infrastructure.

Some of the benefits of Medical NAC are shown below:

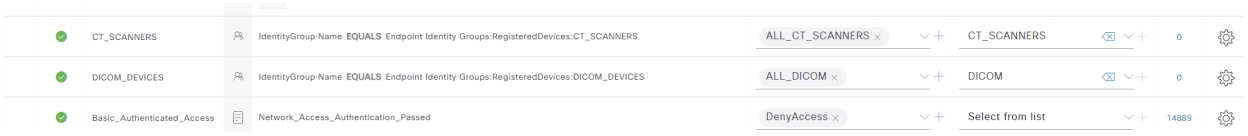
- Improve patient safety: Automate many expertise- and labor-intensive functions while protecting clinical devices used for patient well-being.
- Control regulatory postures: Maintain consistency and compliance for ePHI, HIPAA, PCI, HITECH, ISO 80001, and other regulations on a converged network.
- Offer more services: Easily add technologies such as those for bedside care while giving access to personal, IT-issued, and clinical devices.

The main benefit of device profiling is to enable access control decisions based on a device group – when a device is discovered, it can then be placed into a specific "endpoint group" and the authorization policy defined accordingly.

[8] Cisco ISE Profiling Design Guide - https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456
[9] Cisco Medical NAC - https://www.cisco.com/c/en/us/solutions/security/medical-nac/index.html



Example of Authorization policies for MAB based authenticated devices using profiled endpoint groups:



This level of granularity can be expanded to meet any criteria for any number of devices. Again, it should be noted that this does not require specific configuration on switchports, it is all controlled via ISE.

Ultimately, the access/edge switch device will have a consistent and simplified port configuration – for example:

```
!
interface GigabitEthernet1/0/1
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 ip flow monitor dnacmonitor input
 ip flow monitor dnacmonitor output
 ipv6 flow monitor dnacmonitor_v6 input
 ipv6 flow monitor dnacmonitor_v6 output
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip nbar protocol-discovery
end

SH_FEN-3#
SH_FEN-3#sho run int gil/0/2
Building configuration...

Current configuration : 437 bytes
!
interface GigabitEthernet1/0/2
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 ip flow monitor dnacmonitor input
 ip flow monitor dnacmonitor output
 ipv6 flow monitor dnacmonitor_v6 input
 ipv6 flow monitor dnacmonitor_v6 output
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip nbar protocol-discovery
end
```

Device profiling further helps the organisation to define a suitable policy for devices – this is again important where medical devices, building management system etc. are considered. The questions – what's on my network and what are they doing are often asked.

We previously outlined the role Cisco AI Endpoint Analytics provides in profiling devices, but to further expand on this, in addition to the hundreds of device profile packages included by default in ISE, it has been recognised that obviously, this is not an exhaustive list – especially where medical devices are concerned, and this is possibly the most asked question from IT Departments!

AI Endpoint analytics will use intelligence to identify similar or identical devices discovered, and then suggest the creation of a new device profile package – which will be shared between DNAC and ISE. This again removes the administrative burden, and even the "guesswork" required to create device profiles.

AI Endpoint Analytics can also be used, when required, to create custom device profile packages manually, prior to a device being added to the network. This can be used where unique device identifiers are known, which can then be used as criteria to profile the device.

It is often the case that certain systems in a Healthcare Environment are managed and maintained by the vendor/supplier, specifically when we refer to systems such as PACS, Laboratory Systems, etc.

IT are often constrained by the supplier in what they are able to do – i.e. admin level access is often not provided to IT, this obviously creates a problem with ensuring the device does not pose a threat to network security, i.e. patch levels, passwords, exposure to malware being some of the examples.

The usual rules of “posture checking” – described later, do not apply to such devices, so it becomes essential that corrected identification – profiling, and segmentation are in place to contain any potential threats from these systems.

In terms of AI Endpoint analytics, in conjunction with IBNS/802.1X, most needs of organisations can be achieved without additional expenditure on additional systems to “scan” the network.

5.4. Posture

Posture is a service in Cisco Identity Services Engine (ISE) that allows you to check the status of the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a network.

Security experts estimate one-third of all endpoints that connect to the corporate network are insecure. When the average employee is using multiple devices at work, this creates multiple chances for an insecure endpoint to access sensitive information, or an infected one to spread malware. Vigilance on what is on your network is just as important as who is on the network.

We can summarise some of the issues/threats that can be mitigated using posture checking – Device compliance:

- OS Versions
- Patch levels
- AV/Malware protection
- Unique registry keys/hidden files present to allow access.
- Excessive device access privileges – jailbroken/rooted.
- Unauthorised applications installed and/or running.

These are just a few of the components that can be assessed before network access is fully permitted.

It's clearly not just a case of checking the devices' posture compliance, there must be a process to remediate or restrict access based on those checks.

This is where segmentation again plays a role – it is not possible, for example, to place a device into a remediation VLAN, if dynamic VLAN allocation is not in use!

Nor is possible to block access completely if a device does not meet requirements or becomes compromised while in use. This is possibly the most significant threat to healthcare environments at present.

We will explore the use of Adaptive Network Control (ANC) with Cisco TALOS* integration further in this document, as it significantly augments the use of posture checking, using real-time telemetry and packet inspection – without requiring any additional agents or network scans!

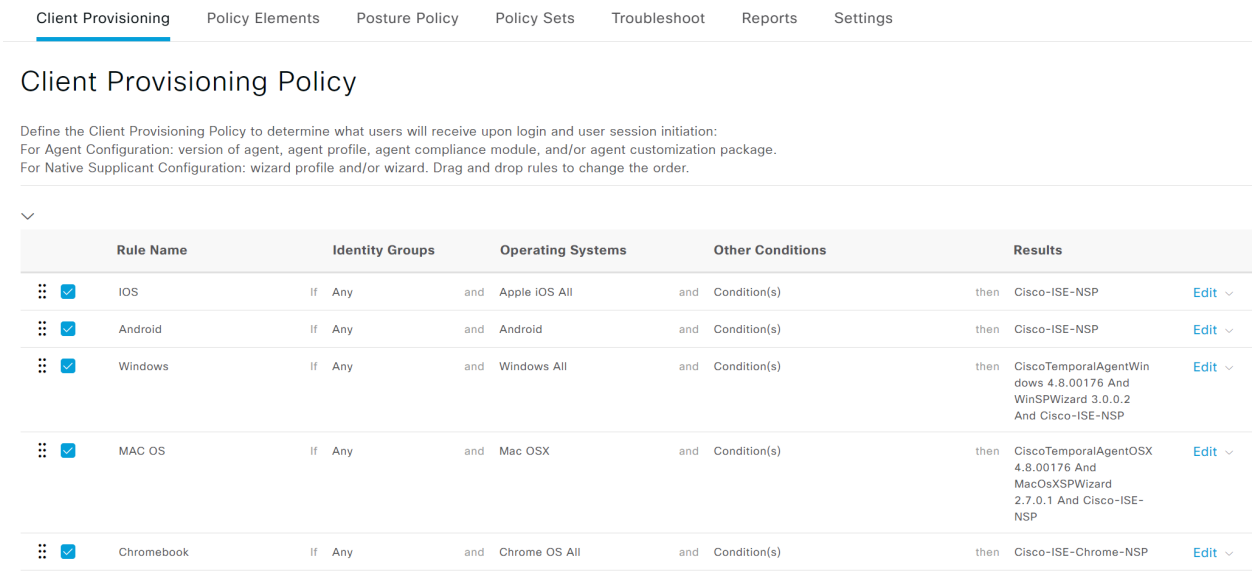
** Cisco Talos is a threat intelligence and research organization that is focused on providing protection against known and emerging cyber threats.*

To consider the options available for posture checking itself, we can deploy this using several methods.

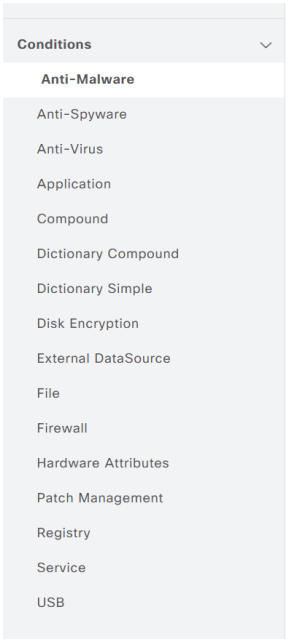
- Use of a supplicant or agent (e.g., AnyConnect/Cisco Secure Client)
- Native Supplicant – via a web-browser
- Temporal Agents – i.e., deployed just for the compliance check then removed
- Agentless – only requires limited device control.

Each of these methods have benefits and indeed limitations, for example, remediation actions can be limited when using Agentless posture, due to the nature of the limited control of the device. However, even agentless can provide a significant benefit when we consider, for example, medical devices maintained by the supplier. It could be used to assess compliance and consequently reduce risk to the organisation.

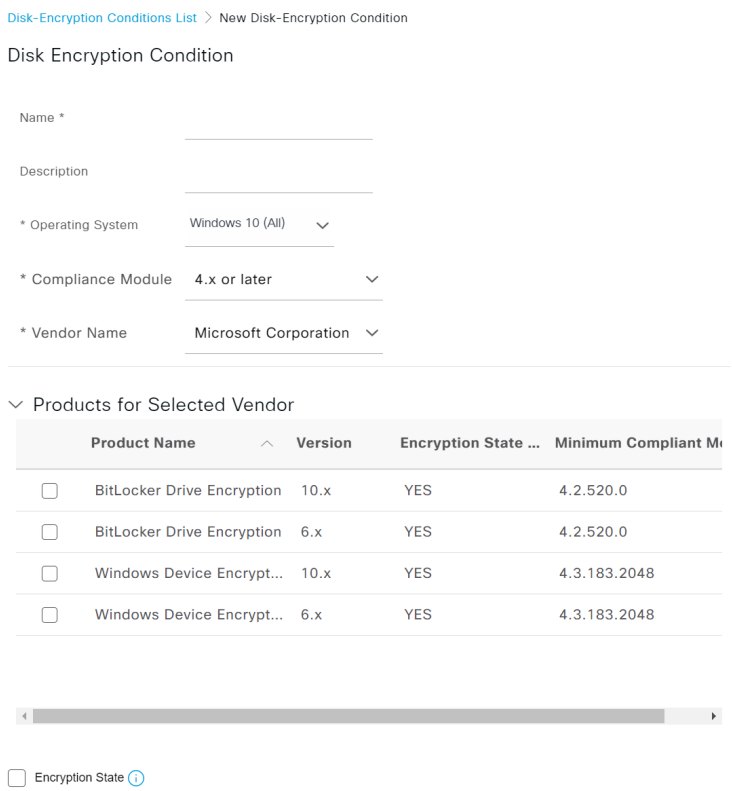
Policies can be created to decide what method is used for "provisioning". These can be based on OS, identity groups derived from IBNS/802.1X and profiling, method of access e.g., guest portal etc.



The conditions for assessing device posture or compliance are extensive, a summary of these is shown below:

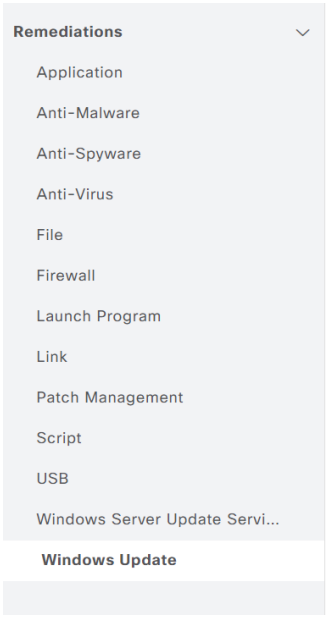


Each of these conditions can be customised as required, for example, to ensure a device has disk encryption enabled –

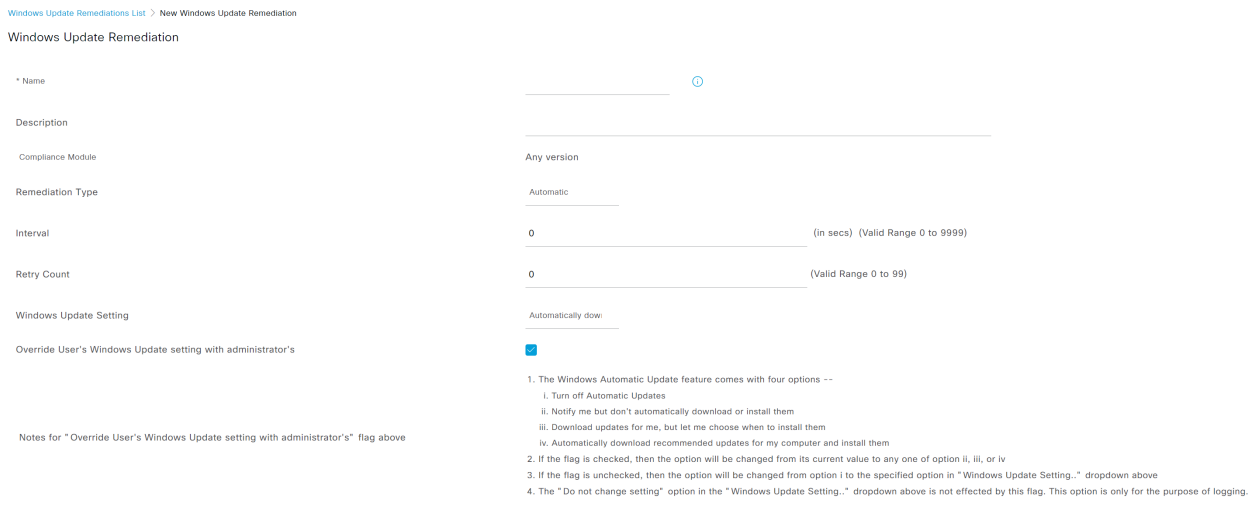


This is a very high-level example of conditions, as there can be multiple conditions or very few conditions enabled, with appropriate authorization rules actioned on the results.

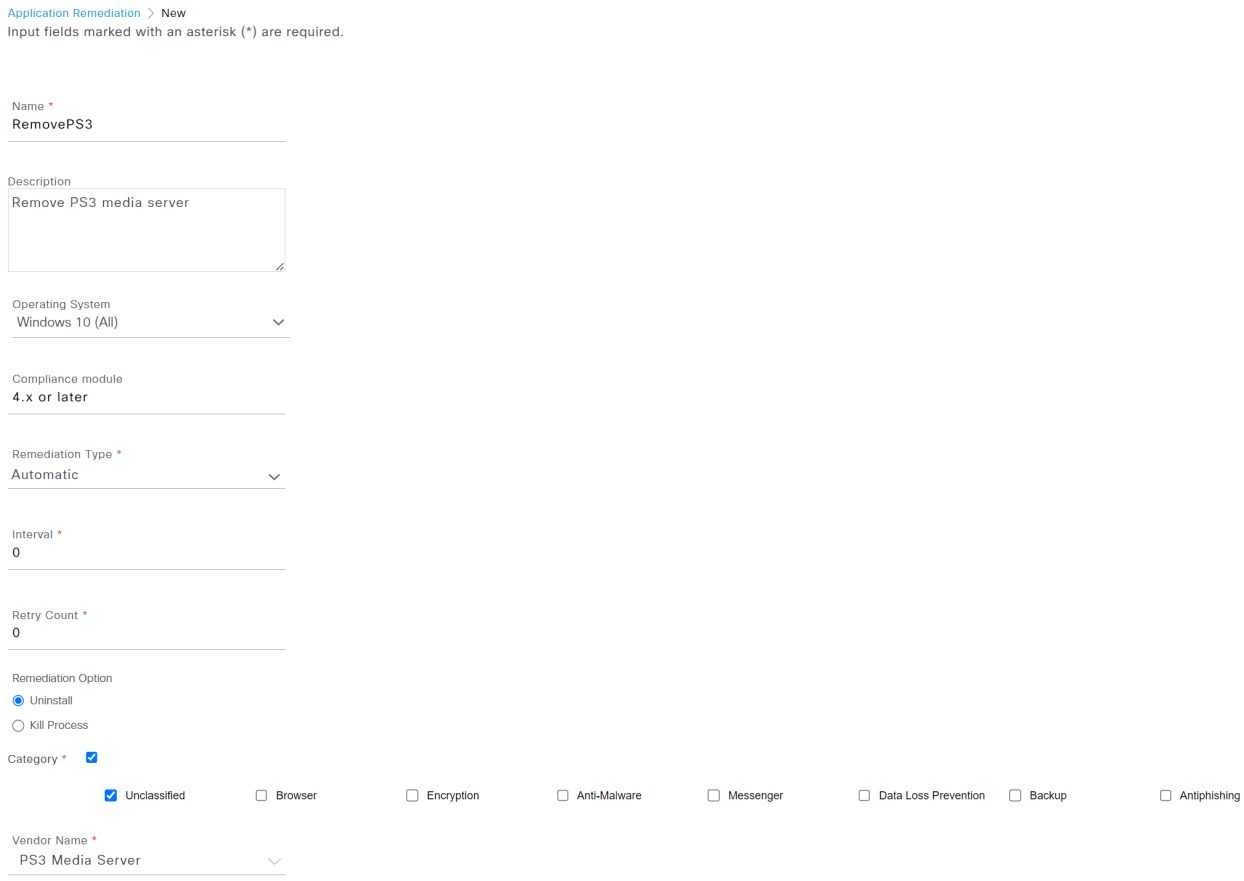
The key element of posture checking is remediation, again, multiple remediation scenarios are included by default.



Each of these can be configured or customized as required – for example, remediation for Windows update patches:



Or to check if unauthorised applications are installed:



Again, the list is extensive in relation to the depth of remediation functions that can be achieved.

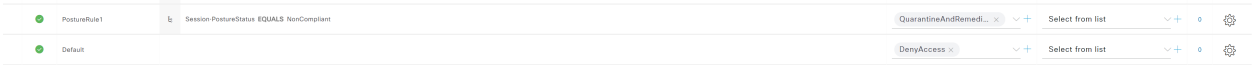
Polices are defined by default within ISE to be used either by default, or as a basis for creating custom policies to meet the organisations requirements.

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
	Policy Options	Default_AntiMalware_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Any_AM_Installation_Mac Edit
	Policy Options	Default_AntiMalware_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Mac_temporal Edit
	Policy Options	Default_AntiMalware_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Any_AM_Installation_Win Edit
	Policy Options	Default_AntiMalware_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Win_temporal Edit
	Policy Options	Default_AppVis_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_AppVis_Requirement_Mac Edit
	Policy Options	Default_AppVis_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_AppVis_Requirement_Mac_temporal Edit
	Policy Options	Default_AppVis_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_AppVis_Requirement_Win Edit
	Policy Options	Default_AppVis_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_AppVis_Requirement_Win_temporal Edit
	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Mac Edit
	Policy Options	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal Edit
	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Win Edit

Based on the result of the posture or compliance check, appropriate rules can be applied, for example, deny access, required to a web portal to remediate, assign to a specific VLAN or SGT. Again, the options are numerous:



A few links are included below which outline the full process for Posture Checking.

https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/admin_guide/b_ise_admin_3_1/b_ISE_admin_31_compliance.html

https://community.cisco.com/t5/security-documents/how-to-agentless-posture-configuration-validation-amp/ta-p/4152763

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html

https://www.cisco.com/c/en/us/td/docs/security/ise/videos/policy_sets/v1/cisco-Implementing-Policy-Sets-for-Posture.html

Some useful YouTube videos on Posture:

ISE Posture Configuration:

https://www.youtube.com/watch?v=6Kj8P8Hn7dY

https://www.youtube.com/watch?v=GTHcEjJOKvc

ISE 3.x Posture and Compliance:

https://www.youtube.com/watch?v=1qjvZlQ1HzY

6. Access Anywhere – Wired, Wireless, Remote and Agile.

Access Anywhere refers to the ability for healthcare providers and staff to access healthcare information and services from anywhere, at any time, using any device or network. This includes wired and wireless networks, remote access, and the use of agile technologies. This also applies to the applications and data being available with the same reliability both within and outside the hospital campus and the security polices to be applied consistently and universally irrespective of how or from where the data is being accessed.

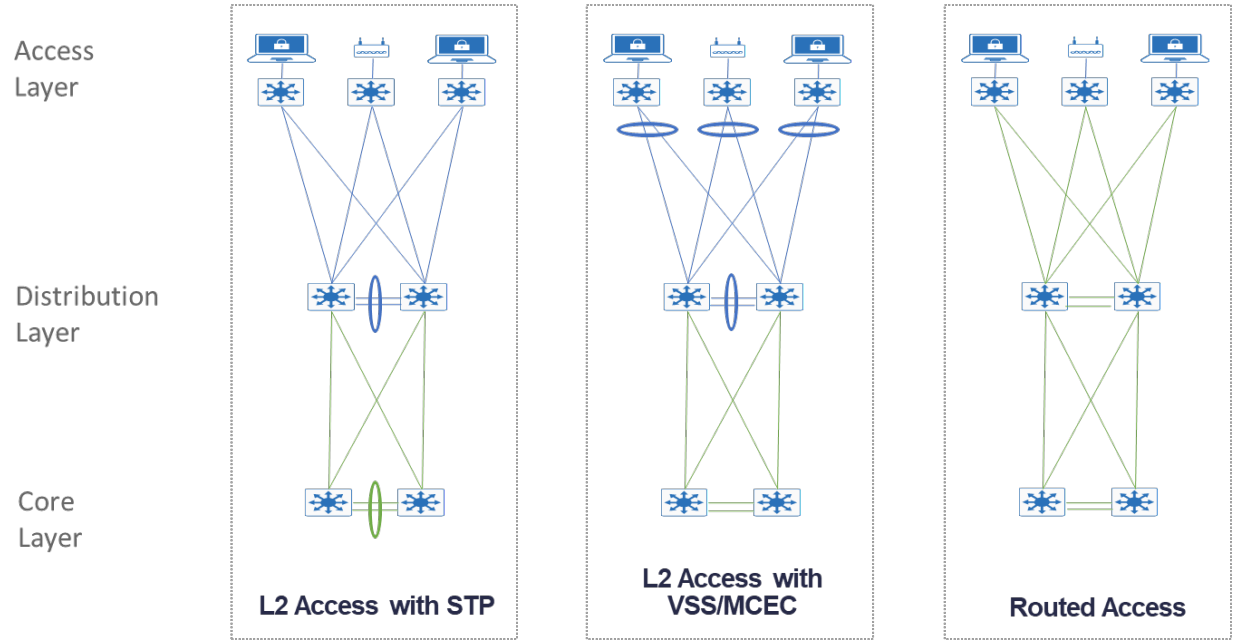
Healthcare providers need access to information quickly and easily, regardless of their location. Hospitals and clinics rely on both wired and wireless networks to connect their devices, including computers, medical equipment, and IoT devices. Wired networks provide reliable and secure connections, while wireless networks enable mobility and flexibility.

The COVID-19 pandemic has highlighted the importance of remote access to healthcare services. Telehealth and remote patient monitoring have become increasingly important, as they enable healthcare providers to deliver care to patients who are unable to visit a clinic or hospital. Remote access also enables healthcare providers to work from home, reducing the need for them to be physically present in a healthcare facility.

By enabling access anywhere, healthcare providers can improve the quality and efficiency of healthcare delivery. Access to healthcare information, including EPR and other services from anywhere, at any time, using any device, can enable healthcare providers to make better, faster decisions and provide better care to their patients which in turn would improve patient experience. Cisco's Secure Access Service Edge (SASE) and Cisco Meraki solutions can help healthcare providers enable access anywhere, while also ensuring security and compliance.

6.1. Wired Access

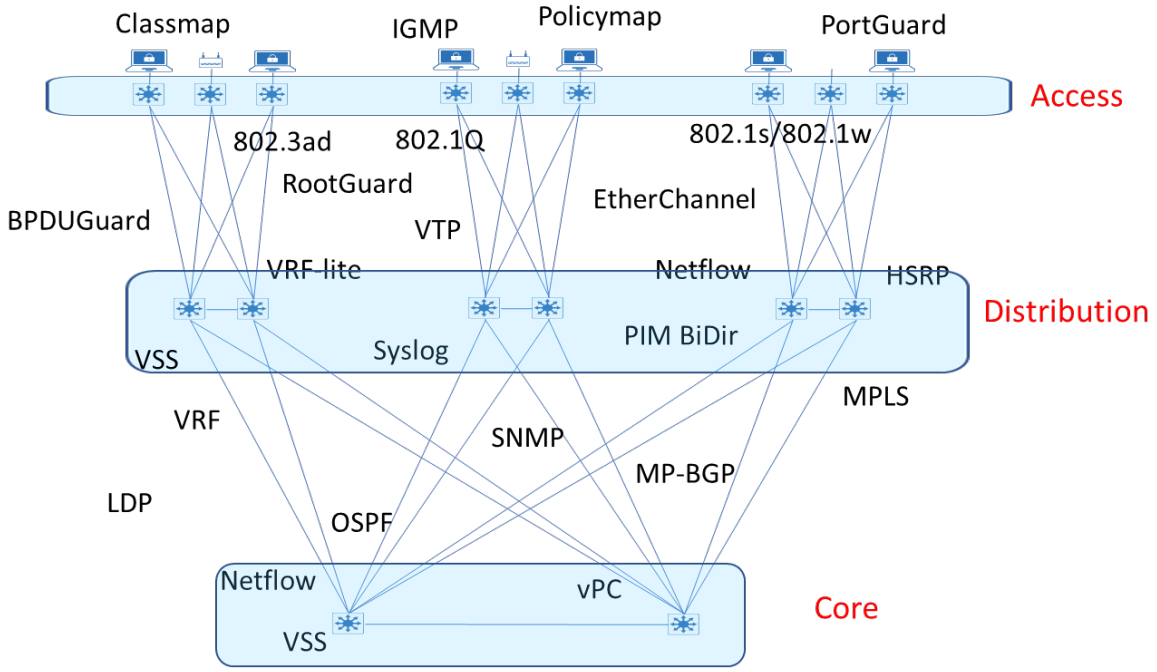
Traditionally, Local Area Networks have been constructed using the concept of Core, Distribution and Access.



Originally, this offered a relatively simple methodology, and was appropriate for design techniques fit for technology available at the time. However, as technology advanced, more features were required to safeguard against failures such as link, device, protocol etc.

Network segmentation became an absolute fundamental – VLAN being the first in the line of adoption. With the implementation of VLANs and resilient dual links, other technologies were required – for example, Spanning-Tree Protocol (STP), this itself going through various iterations – RapidSTP, R-PVST, MST etc. Further segmentation with the use of Virtual Routing & Forwarding (VRFs) introduced even more complexity, usually with cross VRF access through firewalls and/or route-leaking. Consequently, more protocols to achieve this, and longer time to make additions, moves and changes.

The diagram below shows where a simple methodology now requires a multitude of safeguards to operate correctly.



Some of the challenges seen daily can be summarised below:

- Ensure each port is secure – shutdown state not viable.
- Unplug a device to gain access – lack of security.
- Install new devices – assign port to a VLAN.
- Create or change an Access-Control List (ACL) – cumbersome and time-wasting.
- Trombone traffic via a firewall – least optimal.
- Shadow-IT networking – departments attaching non approved switches/hubs etc into the network. Huge security vulnerability and loss of control.
- Re-use of available IPv4 subnets.
- Network consolidation – overlapping RFC1918 addressing.
- Potential malware infection through unprotected devices – posture assessment.
- Growth of Internet of Things (IoT) – building management, medical devices, physical access control, CCTV to name but a few.
- Medical system supplier demands – “we want our own network”.
- Identification of devices on the network – “we simply don’t know what’s out there”.
- Network Management and Monitoring - not just config back-up and link down detection.
- Traffic shaping and prioritisation – QoS. “Throwing more bandwidth at it” is not a viable solution.

This is by no means an exhaustive list, and only scrapes the surface of some of the day-to-day challenges of every IT Department.

Solutions now exist to simplify, rationalise, and automate the delivery of the LAN infrastructure.

As mentioned earlier, organisations can see this guide as a pointer to adopt completely, in stages or in part. However, it should be stated that to achieve the digital maturity required to support the demands of present and future requirements, all elements should be considered strategically.

Some key concepts to be considered when creating a reliable and versatile network design are:

- Always on and resilient — Continuously on and available.
- Intelligent —The ability for network to see and respond to actionable insights, including a proactive security posture to drive both the network and security operations in tandem
- Secure — Protecting the organisation, its users, and data irrespective of physical location.
- Modular and Flexible: Change and adapt in response to change in demand and evolution of technology landscape.

Planning for the Future

As you look at a network design, consider the networking trends and future needs of an organisation:

- The network must be ready to appropriately scale over time to meet the demands of the organisation it is supporting.
- Modern Access Points (802.11ac and later) are capable of throughput far more than the traditional 1 Gbps ports that they are connected to. The IEEE has ratified the 802.3bz standard that defines 2.5 Gbps and 5 Gbps Ethernet over existing Cat5e cabling. Consider deploying Multigigabit capable switches to accommodate the enhanced throughput of wireless devices.
- Devices such as lighting, surveillance cameras, virtual desktop terminals, remote access switches, and Access Points continue to demand more power. Support for power over Ethernet up to 90W per port is offered with Cisco Universal Power Over Ethernet Plus, and the access layer should also provide PoE perpetual power during switch upgrade and reboot events. The Cisco Catalyst 9000 Series access layer switches are perpetual PoE-capable and ready for 100W per port, as that technology becomes available.
- Compliance issues drive a choice of platforms required when you support standards certifications and MACsec. For those cases, you should also be prepared to make analytic data available, using technologies such as NetFlow.
- The Internet of Things (IoT) impacts today's network design. Your network should support TrustSec and other segmentation and virtualization technologies, such as Cisco Software-Defined Access (SD-Access) to enable the scale and expanded uses and policies for the network driven by these trends.
- Bandwidth needs are doubling potentially multiple times over the lifetime of a network so that the network deployed today needs to be prepared to aggregate using 10 Gbps Ethernet to 25 Gbps to 40 Gbps to 100 Gbps capacities or more over time.
- To reduce operational complexity, you can use a centralised controller with open APIs, allowing for very fast, lower-risk and consistent deployment of network devices and services through UI and existing orchestration system. Cisco Digital Network Architecture Center (Cisco DNA Center) automates this network device configuration and management to achieve your organisation's intent.

Taking each of the areas identified above, the following sections expand on the detail behind each concept.

It should be considered a given that any Healthcare infrastructure should be deployed with the maximum availability. This applies to both links, device, and software resilience.

This comes with its own set of challenges. As previously mentioned, spanning tree on "legacy" layer 2 based solutions being the biggest.

From as early as 2007, Cisco developed a High Availability Campus Design Guide[10] based on routed access to the edge[11].

However, whilst this took care of the rapid converging high availability infrastructure – what about VLANs? They didn't traverse a Layer-3 boundary. Most hospitals and healthcare providers still rely on having that "VLAN span across the entire site". Or even multiple sites.

The answer to this is simply the "Campus Fabric". This will be discussed in detail in the section dedicated to network fabric. Please refer section 7.

[10] High Availability Design Guide - https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html
[11] Routed Access Design Guide - https://www.cisco.com/c/dam/en/us/td/docs/nsite/campus/ha_campus_routed_access_cvd_ag.pdf

6.2. Wireless Access

Wireless access is more relevant than ever, staff, patients and visitors have an expectation that network access is available, 24x7. Wireless is now often viewed as an essential utility, along with water and electricity! To meet this demand and expectation, the following must be considered when deploying the wireless infrastructure.

- Location aware = good coverage by default
- Best practices – hot environment, not out of the box.
- Wi-Fi 6/6E enhancements, TWT, BSS Colouring, OFDMA
- Cell size
- Outdoor essential
- Band steering where appropriate
- MCS and why it's important.

Many forward-looking healthcare provider organisations are deploying mobile solutions to help improve quality of care, patient satisfaction, staff efficiency, and clinical outcomes. These include mobile point-of-care (MPOC) solutions that combine mobile devices, mobilized applications, and wireless infrastructure to support delivery of healthcare to the patient. As populations continue to age, wireless technologies are expected to facilitate more home-based monitoring and long-term care.

Healthcare organisations are already realising the benefits of mobile and wireless technologies:

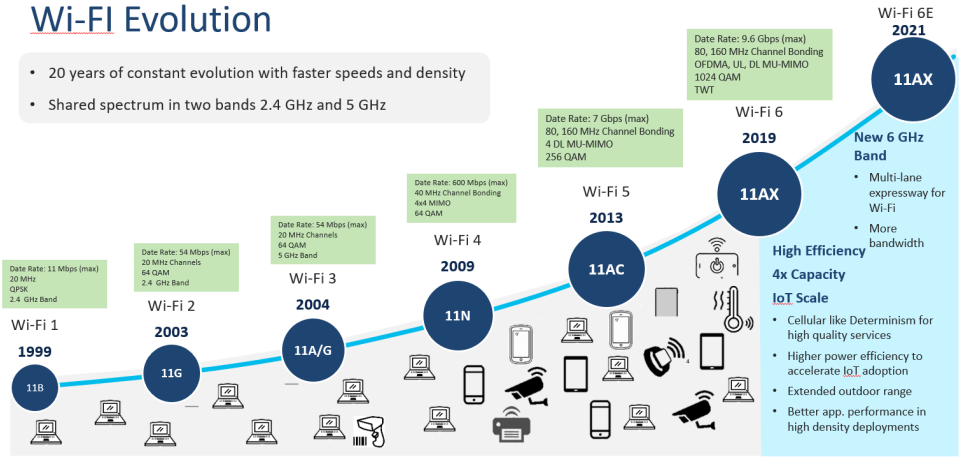
- It has been demonstrated that providing mobile access to clinical information systems can produce significant time and resource savings.
- Automation of routine data collection and elimination of manual entry processes can reduce errors and dependency on paperwork. Many common medical errors can be avoided with better communication and computing links.
- Real-time information can be captured and instantly made available to care providers. Access to patient information, test results, records, and medical reference sources at the point of care helps accelerate evaluation and improve diagnostic accuracy.
- Wireless handheld devices and patient bracelets employing radio frequency identification (RFID) make it possible to track the location and status of patients throughout a hospital campus. Real-time location systems (RTLSs) are used for accurate asset tracking and location, driving cost savings and workflow productivity gains.

These benefits are ultimately dependent on the successful deployment of wireless infrastructure and clients. Wireless implementation in a healthcare facility requires many steps and decisions.

The wireless deployment cycle comprises six main phases:

- Prepare—Understand the various challenges and requirements of a wireless infrastructure deployment and identify roles and types of usage.
- Plan—Determine the requirements of the wireless infrastructure and clients by investigating the targeted usages, applications, environment, network performance, security, and management.
- Design—Become familiar with key wireless architectural choices and their impact on the entire network.
- Implement—Execute the plan based on design decisions made in the previous step.
- Operate—Deploy various methods for providing optimum service to end users.
- Optimise—Understand how to continuously monitor the performance and reliability of the network to make optimal changes.

It is beneficial to first understand the evolution of Wireless based networks:



Hospitals have been deploying Wireless Networks for over two decades, but the relatively low bandwidth and congestion on the 2.4 Ghz spectrum limited its usefulness in a clinical setting. The availability of the 5Ghz spectrum, faster data rates and enhancements in high availability have led to wide scale deployments, a huge proliferation of mobile devices and the use of wireless for mission critical applications.

Some of the typical use-cases in a healthcare environment have been:

- Beside patient care – viewing results, medical records, prescribing etc.
- Location Based Services – identifying where devices, or people, are within the building. E.g., Asset tracking, wayfinding, access control.
- Mobile telephony
- Replacement of staff paging systems – with location intelligence.
- CCTV
- Building Management
- Environmental reporting – air quality etc.

This is clearly not an exhaustive list, and more and more applications are being delivered utilising the WiFi infrastructure.

6.2.1. Coverage and Location Awareness

The first principle of a successful WiFi deployment is simple – Coverage.

Historically, a simple design would be based purely on data coverage, with little attention given to "coverage holes". Since WiFi first is now an essential consideration, it is imperative to ensure that coverage is pervasive and resilient across a hospital campus.

A key aspect of ensuring adequate coverage exists is the wireless survey. This process, albeit time consuming, is an absolute necessity.

Where previously data-only coverage was used, by default, Location based coverage should be planned from the start. This will ensure that coverage holes are removed, but also the service will be provided to allow for mobile telephony and importantly – RTLS – real-time location services.

Inevitably, this will increase the number of access points required, but also, can potentially case issues on the 2.4Ghz frequency.

Tools are available to be used as a guide for the survey, called a predictive or desk-based survey, i.e., Prime Infrastructure, Ekahau[12] or DNA-Centre. This will give a prediction of where to place access points, based on coverage requirements and access point model.

Reiterating the significance of conducting surveys cannot be overstated in achieving the intended result.

To look at the baseline requirements, when it comes to voice enabled or location-based deployments, several factors must be considered.

6.2.2. Channel Utilisation

The existing WiFi protocols in the 2.4 GHz band need to interoperate with each other, which brings additional overhead, reducing channel throughput. Many sites already have products using the WiFi 2.4 GHz band. In addition, many other products use the same 2.4 GHz frequencies used by WiFi. Other products include Bluetooth, wireless handsets, video game controllers, surveillance cameras, and microwave ovens. Because of the existing use of the channel-limited 2.4 GHz bands, the crowding in the 2.4 GHz spectrum and the constraints in a channel allocation mean that you should consider the 5 GHz and 6 GHz bands. However, some of the previous constraints on channel utilisation on 2.4GHz have been somewhat alleviated with the arrival of 802.11ax and associated "BSS colouring", this effectively now removes the previous assumption that 2.4GHz was a "junk band".

[12] https://www.ekahau.com

6.2.3. Cell Coverage

Cisco Radio Resource management (RRM) is the mechanism for controlling channels in use, power levels etc of all Access Points in an environment. RRM continuously monitors all access points, and their visibility in terms of Received Signal Strength Indicator (RSSI) to other access points.

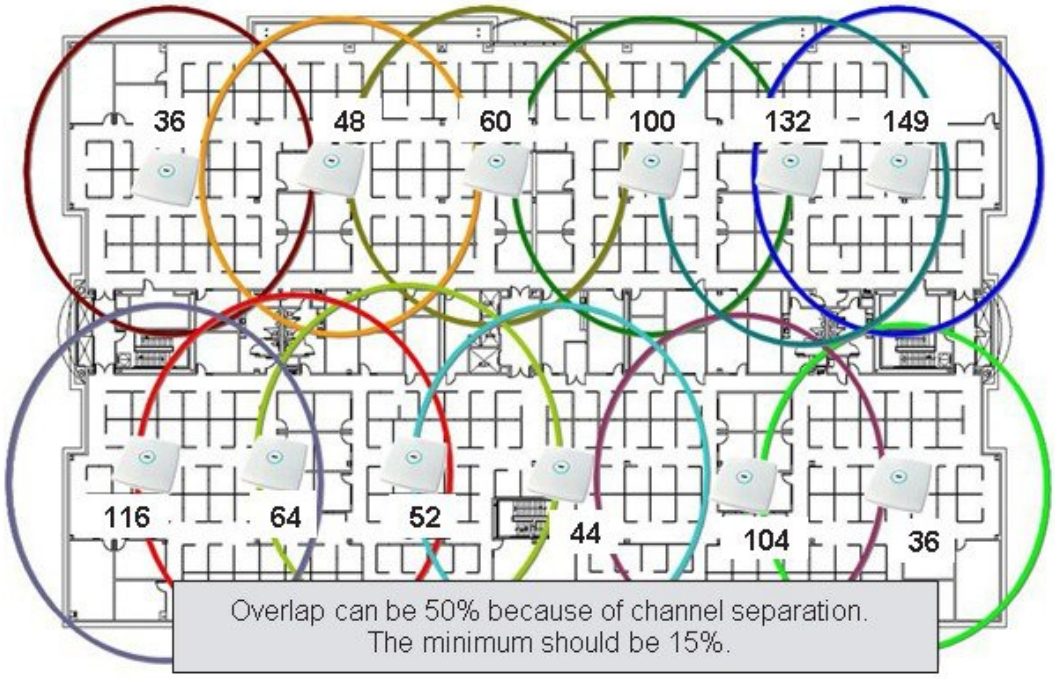
RRM consists of four algorithms:

- RF Grouping
- DCA (Dynamic Channel Assignment)
- TPC (Transmit Power Control)
- CHDM (Coverage Hole Detection and Mitigation)

RRM was designed to manage the RF environment in a dynamic way with little to no user intervention. RRM's default settings are generally the best fit initially. In a new controller the Day 0 setup wizard will allow you to fine tune many settings by picking the deployment type that you are working with.

Additionally, RRM can be further tuned, especially where it relates to high density deployments.

For typical voice-based coverage, there must be at least -67dbm RSSI at the cell edge, with a minimum of 15% cell overlap. This should form the baseline, or minimum requirements for the system.



It should be noted that this is an example – access point placement becomes crucial for location services – Access points in a straight line as shown above would not yield accurate location-based reporting.

The -67 dBm threshold is a general recommendation for achieving a packet error of one percent, which requires an SNR value of 25 dB or greater (local noise conditions impact this requirement).

6.2.4. RF Profiles

RRM at the Global Level sets configuration parameters that apply to every AP associated with the RF Group. Different use cases like High Client Density or Capacity model vs. Coverage models require different optimisations to be efficient and meet design goals. In High Density, we are asking to optimise users experience when close to a lot of APs – at minimal distances. For Coverage we are optimising for maximum cell coverage and reliable connection at distance from the AP in thin coverage.

RF Profiles allows for modifications to be applied to select groups of APs contained in the same AP Group. You can configure an RF Profile for each radio on the AP, 2 RF Profiles per AP Group may be applied. The classic use case for this is an outpatient department (OPD), where a high-capacity design is required to manage a high client density. Surrounding this OPD however are hallways and open areas where coverage is the bigger concern. A single global RRM setting for all the APs will result in a configuration that is likely not optimised for either environment. Placing the APs inside the OPD in one AP group (perhaps grouped with APs from other High Client density locations) and the APs in the coverage areas like hallways and open areas in another AP group. Now you can configure RF Profiles that optimise the required configurations to the intended design.

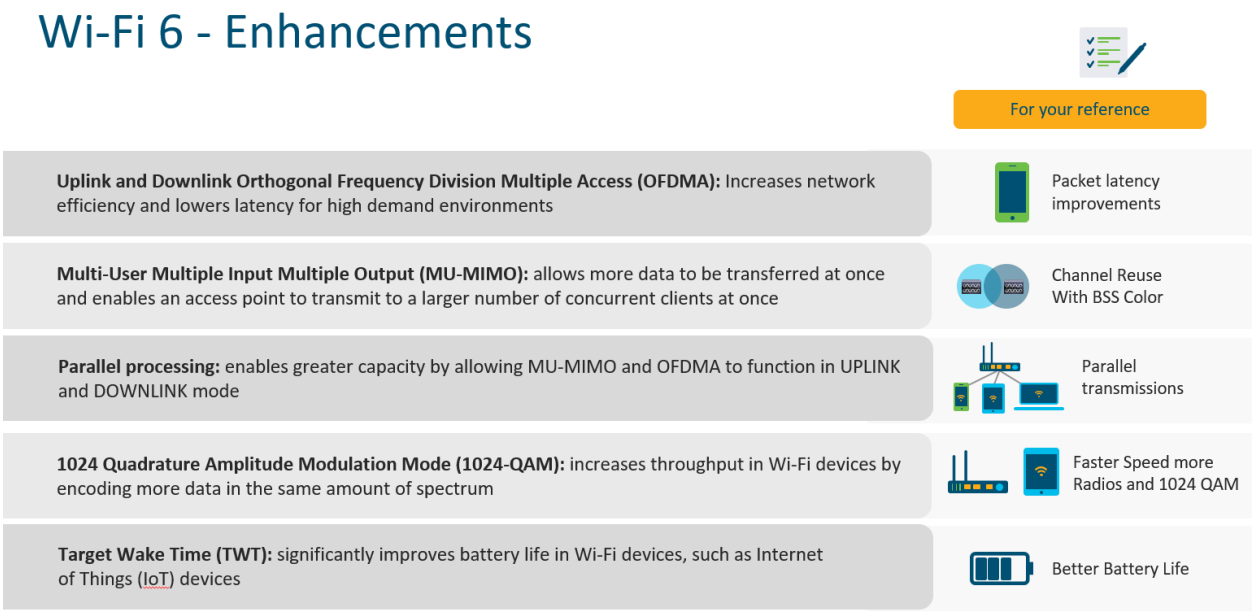
RF profiles can be used to control the minimum and mandatory data rates enabled. It is recommended that data-rates below 11mb be disabled.

There are numerous options that are configurable under RF profiles, including for example RX-SOP (receiver sensitivity), TPC (transmit power control), Coverage RSSI threshold to name but a few. Clearly the purpose of this document is not to provide a comprehensive guide, however, links to the appropriate guides are included.

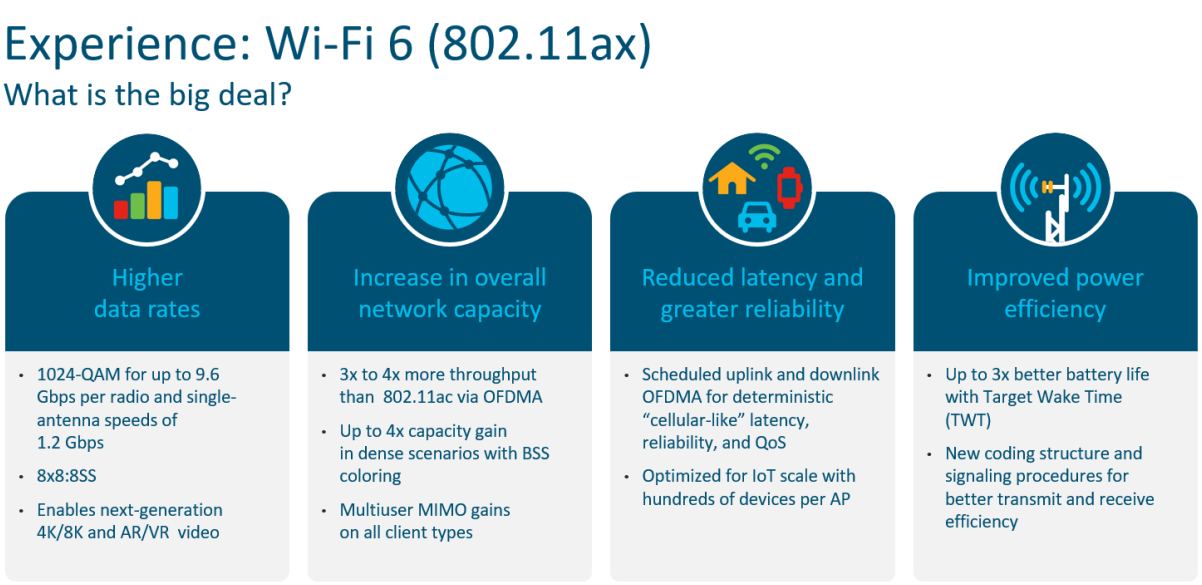
6.2.5. Wifi 6 and 6E

In 2019, and major improvement to WiFi arrived in the form of 802.11ax (Wifi-6) and later Wifi-6E. With 6E allowing the use of the 6 GHz frequency in addition to the 2.4 and 5 GHz frequencies.

Some of the key new features that arrived in 802.11ax were:



These reduced some of the limitations that were becoming apparent with the previous 802.11ac standards. Especially around client performance, and importantly, channel use (2.4Ghz specifically).



As can be seen from the table below, theoretical data rates for a client with a single spatial stream were a significant improvement.

.11ax data-rate chart for 1 spatial stream

New 1024 QAM introduces a 25% performance in throughput with single Radio

MCS Index	Modulation type	Coding Rate	Data rate (in Mb/s)							
			20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI
0	BPSK	1/2	4[1]	8.6	8[1]	17.2	17[1]	36	34[1]	36[1]
1	QPSK	1/2	16	17.2	33	34.4	68	72.1	136	144
2	QPSK	3/4	24	25.8	49	51.6	102	108.1	204	216
3	16-QAM	1/2	33	34.4	65	68.8	136	144.1	272	282
4	16-QAM	3/4	49	51.6	98	103.2	204	216.2	408	432
5	64-QAM	2/3	65	68.8	130	137.6	272	288.2	544	576
6	64-QAM	3/4	73	77.4	146	154.9	306	324.4	613	649
7	64-QAM	5/6	81	86	163	172.1	340	360.3	681	721
8	256-QAM	3/4	98	103.2	195	206.5	408	432.4	817	865
9	256-QAM	5/6	108	114.7	217	229.4	453	480.4	907	961
10	1024-QAM	3/4	122	129	244	258.1	510	540.4	1021	1081
11	1024-QAM	5/6	135	143.4	271	286.8	567	600.5	1134	1201

Up to **1.2Gb with 1 radio**, up to 10 Gb* with 8 radios @ 160 MHz

However, whilst these theoretical rates may be appealing, they should be approached with caution, especially in a high-density environment, such as healthcare.

We previously discussed channel utilisation and the impact in performance associated with that. When we look specifically at the 5Ghz part of the spectrum, with a default 20Mhz channel bandwidth, we have up to 16 discrete non-overlapping channels available. Obviously, this would solve our problem of channel interference.

Unfortunately, not the case. The temptation is there to “get the most out of it” and trying to achieve the high data rates shown above. This is only achievable by increasing the 20Mhz channel bandwidth up to 160Mhz, and by doing so, decreasing the number of non-overlapping discrete channels down to 2. For every double of channel bandwidth = half available channels.

Clearly great care must be taken to ensure there is no trade-off between performance and availability by introducing RF issues due to lack of available channels.

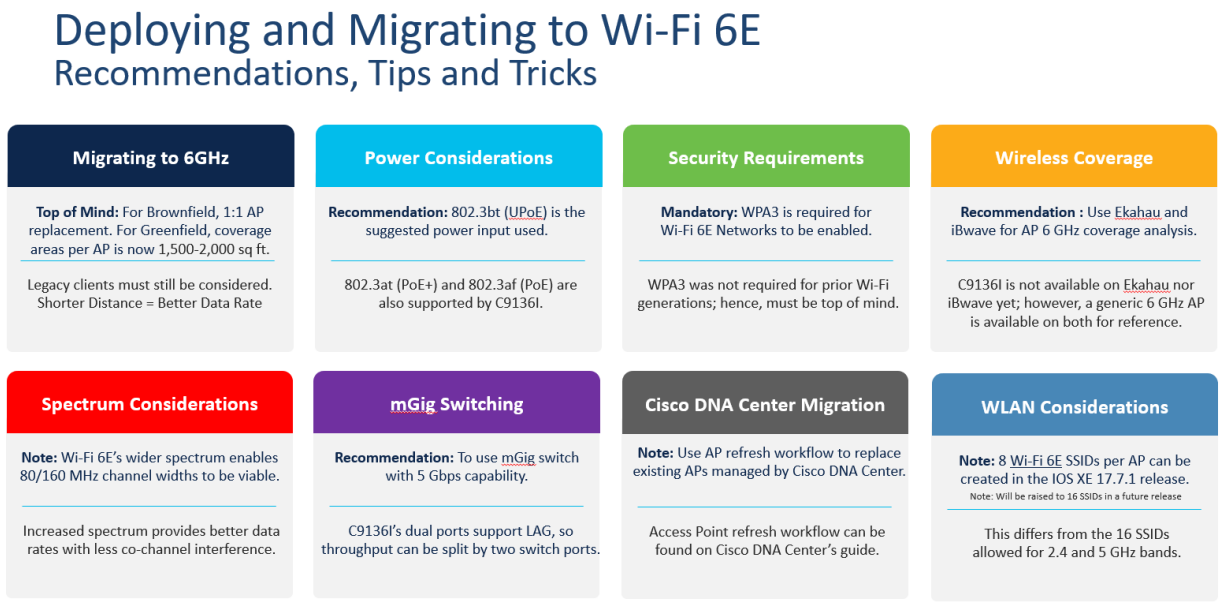
Typically, 40Mhz channel bandwidth would provide more than adequate throughput, whilst still maintaining 8 non-overlapping channels.

However, the benefits of migration to WiFi6/6E are far greater such as improved network performance, increased capacity, enhanced security, and better support for emerging technologies such as IoT devices.

6.2.6. Migration from Legacy to WiFi6/6E

As technology development increases, the requirement to keep pace with user demands imposes a larger burden on HealthCare IT Departments.

The process to migrate to 802.11ax should be considered in detail – as identified from the benefits of 802.11ax above, the overall infrastructure essentially must keep pace. Some of the considerations are highlighted below:



For a more detailed and comprehensive in-depth explanation of WiFi and RF, and why these elements are important, Cisco frequently provide a one-day seminar on the theory of RF and WiFi free of charge to Public Sector customers.

Some useful reference links are included below.

Location aware deployment:

https://www.leitwert.ch/patient-monitoring/

https://www.cisco.com/c/en/us/products/collateral/wireless/nb-06-preparing-for-wifi-6-ebook-cte-en.html#Missioncriticalnetwork

https://www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/WLAN-Deployment-Guide-for-Healthcare.pdf

Best Practices:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/cat9800-ser-primer-enterprise-wlan-guide.html

802.11r, 802.11k, 802.11v, 802.11w Fast Transition Roaming:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/Chapter-11.html

WiFi6:

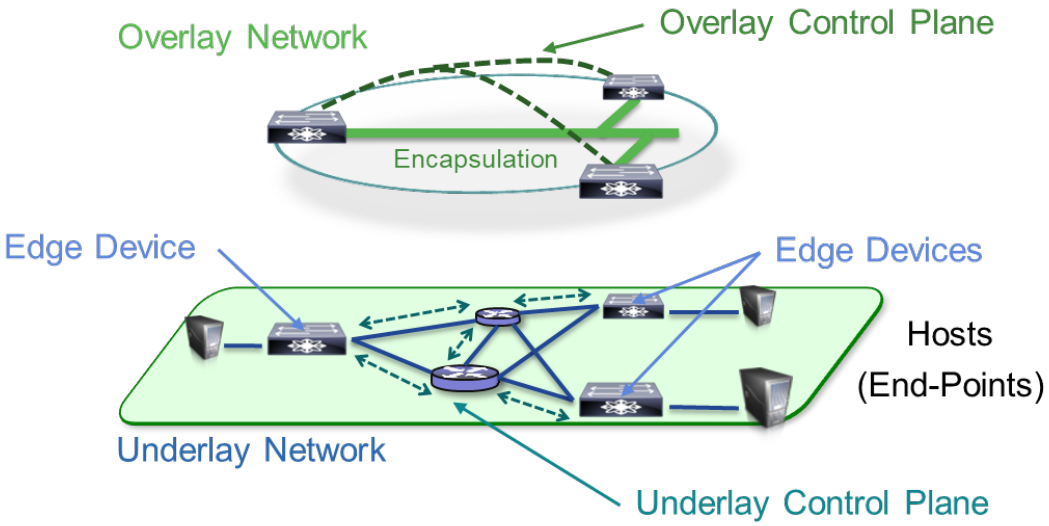
https://www.cisco.com/c/en/us/products/collateral/wireless/white-paper-c11-740788.html

7. Campus Fabric – Enabling a programable network.

When we refer to a Campus, this can be a single remote site, an acute Hospital site (containing multiple buildings), or even multiple sites spread across a geographic region connected with resilient high-speed circuits. The campus is the managed infrastructure – end to end.

So, what's a fabric?

A fabric is essentially an overlay to the underpinning "plumbing". Overlays are widely deployed across organisations globally – for example GRE, MPLS, CAPWAP, IP-SEC etc.

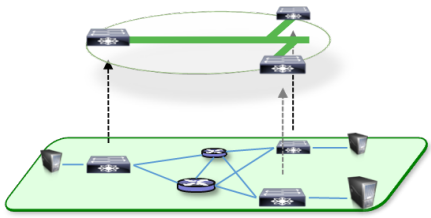


A "Fabric" is an "Overlay"

An Overlay network is a *virtual topology* used to *logically connect* devices, built on top of an arbitrary Underlay physical topology.

An Overlay network often uses *alternate forwarding attributes* to provide *additional services* not provided by the Underlay network.

Examples of Network Overlays	
• GRE , mGRE , NVGRE	• OTV
• MPLS , EoMPLS , VPLS	• LISP
• GETVPN , DMVPN	• DFA
• Fabric Path (FP)	• ACI



The result of the fabric is to abstract the data-plane from the control-plane.

By doing so, the “user traffic”, i.e., endpoint to endpoint can traverse boundaries as if they were local.

This principle is underpinned by Virtual Extensible LAN – VXLAN.

VXLAN is a technology which uses MAX-in-UDP encapsulation to allow overlaying a Layer 2 (L2) network over a Layer 3 (L3) underlay using any IP routing protocol.

VXLAN solves three main problems:

- 16M VNIs (broadcast domains) versus the 4K offered by traditional VLANs.
- Allows L2 to be extended anywhere in an IP network.
- Optimised flooding.

Why VXLAN?

VLAN Scalability - VXLAN extends the L2 Segment ID field to 24-bits, which potentially allows up to 16 million unique L2 segments over the same network.

L2 Segment Elasticity over L3 Boundary - VXLAN encapsulates an L2 frame in an IP-UDP header, which allows L2 adjacency across router boundaries.

Leverages multicast in the transport network to simulate flooding behaviour for broadcast, unknown unicast, and multicast in the L2 segment.

Leverage Equal Cost Multi-pathing (ECMP) to achieve optimal path usage over the transport network.

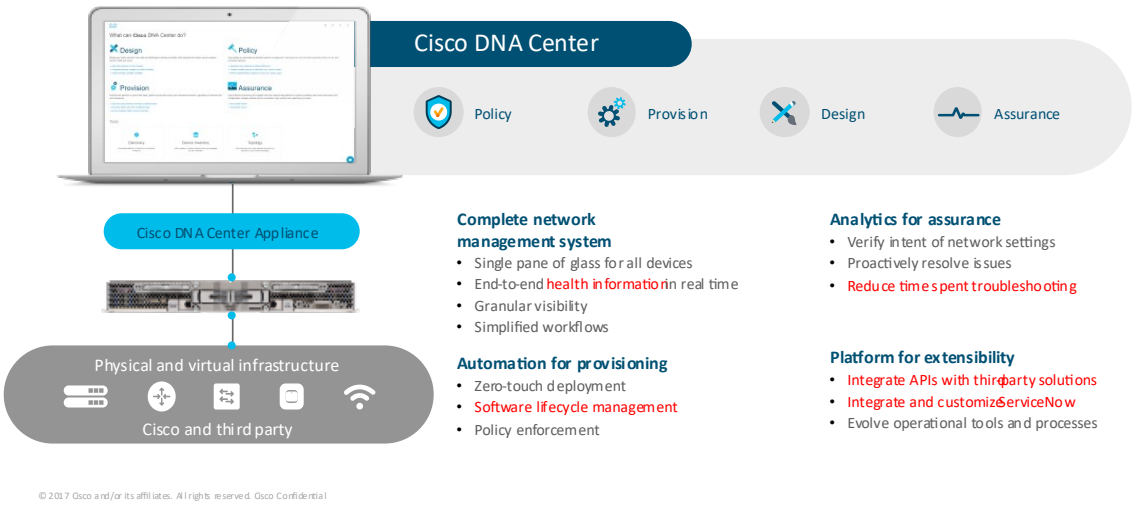
VXLAN technology is used in several solutions:

- Campus LAN via Cisco Software Designed Access
- Application Centric Infrastructure (ACI) in the Data Centre
- BGP-EVPN[13] – campus or data centre fabric configured manually (or via Ansible, python etc)

However, as mentioned earlier, Cisco is now focused on providing software-based solutions to work in harmony with Cisco Hardware infrastructure.

The key element to this solution is Cisco DNA Centre, which can be deployed in both fabric-based and traditional non-fabric network infrastructure. Cisco DNA-C is not a traditional Network Management System. The core functionality of DNA-C includes:

[13] BGP EVPN Configuration Guide - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-12/configuration_guide/vxlan/b_1612_bgp_evpn_vxlan_9300_cg/configuring_evpn_vxlan_layer_2_overlay_network.html



The other key component in the overall Infrastructure solution is the Cisco Identity Services Engine (ISE). Cisco ISE is not just another RADIUS server, it forms the core integration for access control, device classification (profiling), device assurance (posture checking) and enables interoperability via API and PxGrid. (Platform Exchange Grid)

Cisco ISE allows you to provide highly secure network access to users and devices. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities with integrated solutions from Cisco technology partners, so you can identify, contain, and remediate threats faster.

With Cisco PxGrid[14] (Platform Exchange Grid), multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps automate security to contain threats faster.

Cisco maintains several “Validated Designs”[15], which are tested and documented approaches to help design, deploy and extend technologies successfully. These guides document building possible network configurations, how to ensure these fit into existing systems, and offer best practices for successful deployments. CVDs are available for SDA[16] and Campus Design[17]

[14] Cisco pxGrid Overview - https://www.cisco.com/c/en/us/products/security/pxgrid.html
[15] Cisco Design Zone - https://www.cisco.com/c/en/us/solutions/design-zone.html
[16] SDA Design Guide - https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html
[17] Campus Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

8. SASE: Secure Access Service Edge

The core task of a network transport is to securely connect users to applications and data from anywhere using any device.

Users are dispersed, they need the ability to work from home, office and while roaming. The IT staff need the ability to run and manage the IT systems from anywhere. Clinical staff need access to systems which allow them to make decisions and connect with patients. The patients need the ability to participate in the care journey, access patient medical record and manage appointments.

The number and type of devices connecting to the network has exploded, the network is quickly becoming a network of things, connecting medical devices, user wearables, security and building management systems. This changing landscape has increased demands on the network in terms of management, network security, data integrity and identity management.

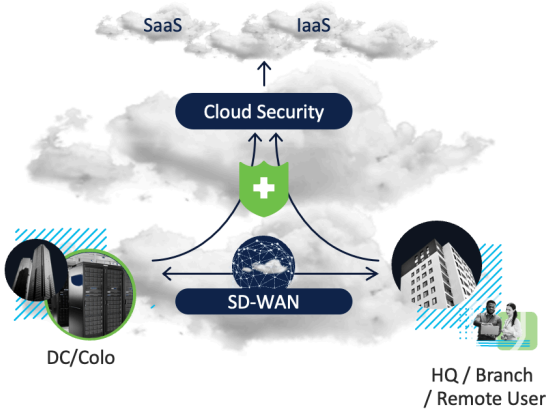
Furthermore, the applications are not limited to on-prem data centers but are increasingly hosted in a hybrid environment which could be SaaS, public/private clouds and on prem data centers. This requires universal policy enforcement to achieve consistent security posture and user experience.

Adapting to these changes requires a shift in approach, changes to network design, provisioning, management and security. SASE provides an architecture approach to view the network, security and management functions as one and evolve as a unified network fabric focused on business outcomes and user experience.

8.1. The SASE Vision

Consider SASE as a comprehensive solution that offers universal and consistent security posture implementation, a unified network security function, and a policy-driven environment.

The threat and network access landscape are constantly evolving and shifting with access anywhere, heterogeneous connected devices and hybrid application install-base, this demands that we shift the security permitter to where user, device, application, and data is. This requires an integrated cloud native security system that can deliver complete, universal, and consistent security posture. The network also needs consolidation to act as 'one' hybrid fabric delivering services and experience to its users.



CISCO SASE is an architecture approach to converge network and security functions while enabling secure access to applications for users using any device, from any location and at any time. This approach also enables provisioning access policies, security policies, identity management and user experience consistently across the network fabric.

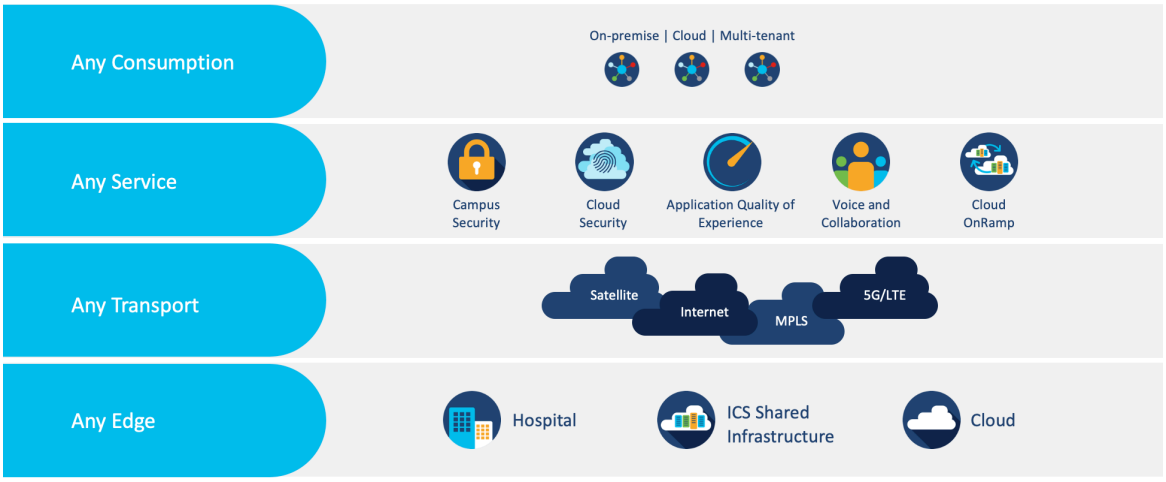
In addition to combining networking and security functions, SASE enables the concept of supporting users and applications for a hybrid cloud strategy and provides end to end visibility into solution performance, network, and security events. This capability for predictive troubleshooting not only enables the IT teams to take proactive actions and mitigate risks before an impact to production environment but also provides a foundation for the network to evolve into a self-healing network of future.

Cisco's approach to SASE is simple. It is based on the 3 Cs viz. Connect, Control and Converge.

Connect: **connecting** users to the applications and data that enables the workforce and provide a seamless experience.

Combine with Cisco SD-WAN and Cisco Security Client (AnyConnect) to deliver secure, seamless connections to applications anywhere.

Cloud scale SD-WAN is foundational for WAN Edge



The Cisco SD-WAN solution is based on the same routing principles as the traditional networks but emphasise virtualisation and policy driven approach. SD-WAN also emphasise a true separation between control and data planes which is essential for the solution to be able to run over any transport such as MPLS or direct internet access.

The control plane is governed using centralised controllers which oversee provisioning, maintenance, security policy & network policy enforcement and quality of experience for the overlay network.

The data plane passes traffic between the network devices, together with control plane creating the SD-WAN fabric.

The solution offers flexibility to run on a range of devices both physical such as WAN edge routers and virtual such as virtual machines in the cloud.

Please refer the solution overview and configuration guides for solution details, features and use cases that match your requirements.

Cisco SD-WAN powered by Viptela.

https://www.cisco.com/c/en_uk/solutions/enterprise-networks/sd-wan/index.html

CISCO SD-WAN Solution Overview

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.html?oid=otren012099

Cisco SD-WAN Cloud Scale Architecture

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

Cisco SD-WAN Design Guide

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

Cisco SD-WAN powered by Meraki

https://meraki.cisco.com/products/security-sd-wan/

Meraki SDWAN Architecture and Best Practices

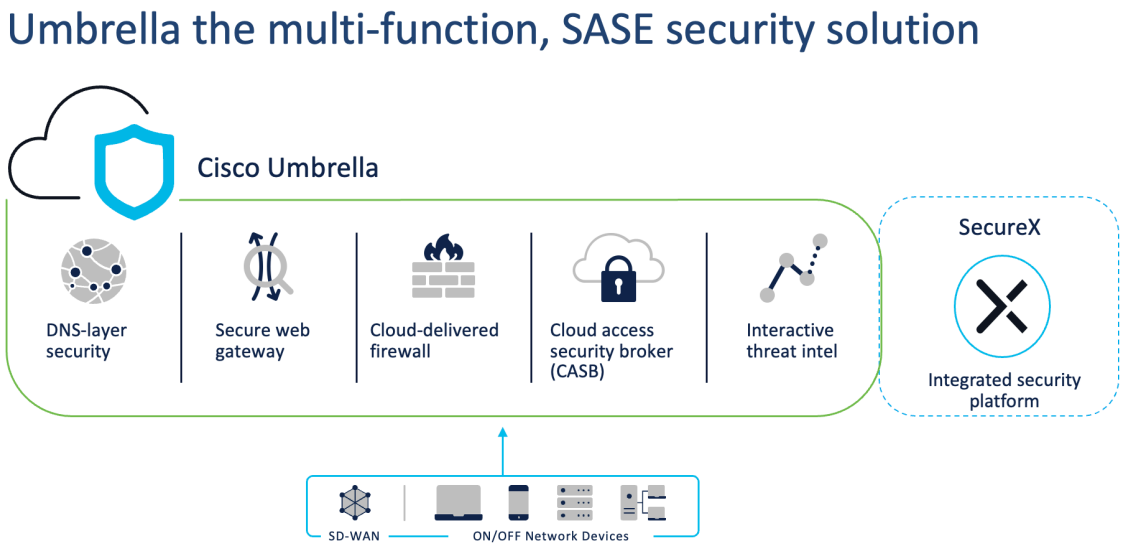
https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_SD-WAN

Cisco Secure Client (Including AnyConnect) Administrator Guide

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0.html

Control: **control** is about extending secure services from the data center to a hybrid cloud enabling consistent policy enforcement, security posture and end to end visibility.

Control with Umbrella and Duo security: Establish zero trust access and cloud-delivered security with leading threat protection.



Cisco Umbrella provides the cloud security pillar of the SASE (Secure Access Service Edge) architecture.

Umbrella integrates multiple security services — DNS-layer security, firewall, secure web gateway, cloud access security broker, and more — to centrally manage protection for all your locations.

Having this functionality in a single platform is important because it helps to reduce the time, money, and resources previously required for deployment, configuration, and integration tasks.

Equally important, is the flexibility to deploy what is needed by locations and users:

- For some, that means DNS-layer security is the perfect fit.
- While for others, deeper inspection with the web gateway or cloud-delivered firewall is needed.

Umbrella also includes Cisco SecureX which is a built-in experience that connects data from across the Cisco Security portfolio and third–party tools in your security infrastructure to unify visibility, enable automation, streamline operations, and strengthen security.

If all capabilities of Umbrella are enabled, traffic flow will be:

DNS Security: Umbrella DNS is resolved first. It is the first check for malicious or unwanted domains and is based on the defined DNS policies. This reduces the quantity of traffic that is sent to the CDFW and SWG, improving responsiveness and performance.

Cloud Delivered Firewall: All traffic that has made it through DNS checks will be inspected by the CDFW. The firewall provides visibility and control for outbound internet traffic across all ports and protocols (Layer3/Layer4) as well as Layer7.

Secure Web Gateway: The SWG will inspect any traffic that is destined for ports 80/443 after it has been permitted by the CDFW to provide a deeper security inspection. It will also apply visibility, application, and control policies.

Cisco Umbrella User Guide

https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella

Cisco SDWAN integration with Umbrella

https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214155-configure-integration-with-cisco-umbrell.html

Cisco Duo

https://www.cisco.com/c/en_uk/products/security/duo/index.html

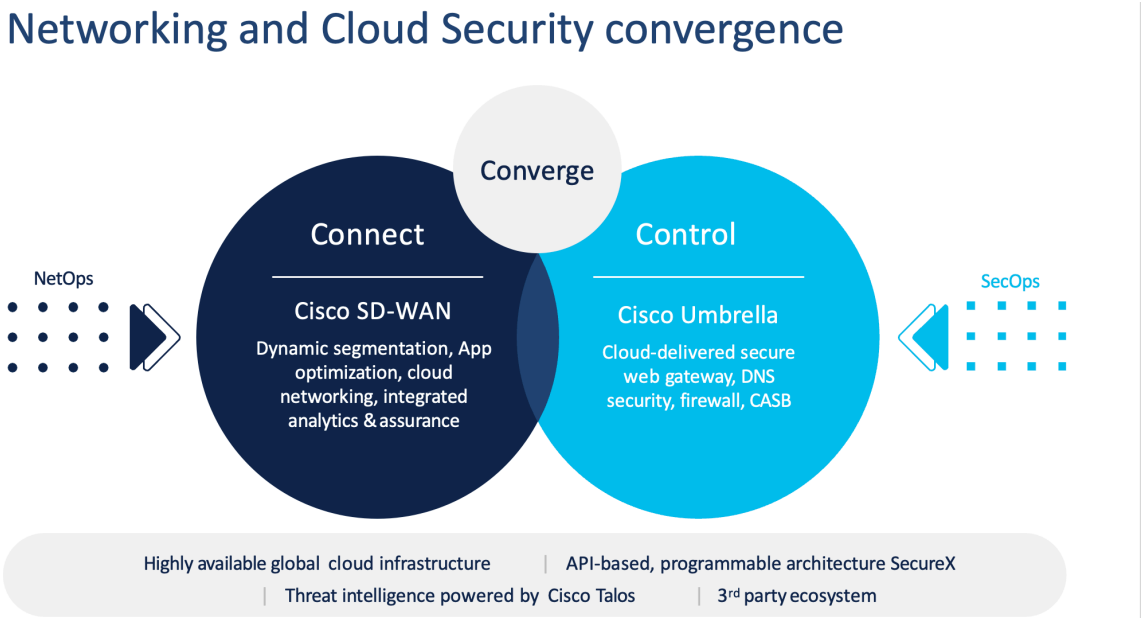
Getting Started with DUO

https://duo.com/docs/getting-started

Duo Deployment Best Practices

https://duo.com/assets/pdf/Duo-Liftoff-Guide.pdf

Converge: **convergence** of networking and security functions making it an integrated system. It is a network with security at its core and delivering a secure hybrid cloud strategy.



8.2.ThousandEyes Observability

With the evolution of network from just being a network of IT device and endpoints to a network of things and people the network path from user end device to the application is no longer static but dynamic in nature. The traffic now moves to different destination via different paths which makes it more difficult to isolate problem and troubleshoot issues.

What we need is the ability to monitor traffic end to end, detect issues as they happen or in some cases avoid them from occurring, be precise with fault finding, optimise our traffic flows, receive actionable insights from our network and deliver consistent user experience irrespective of their location. This is where ThousandEyes joins our SASE architecture approach by providing us the ability to observe end to end, find and mitigate problems anywhere in the network and deliver a predictable user experience.

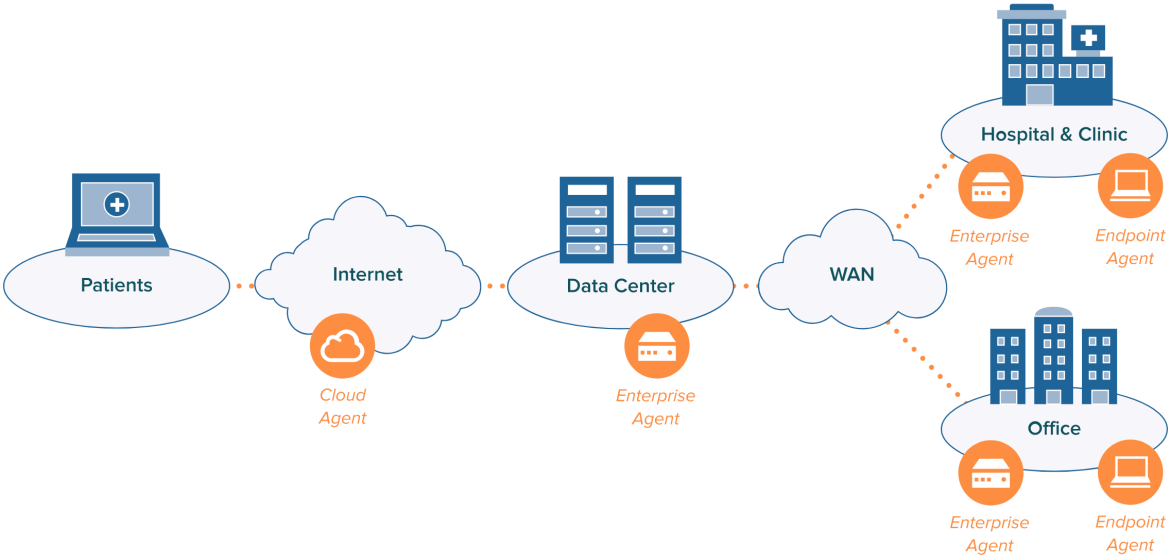
Thousand eyes primarily use three agent types or vantage points. External, internal and end-user.

External: These are the **cloud agents** which are globally distributed and observe from a point of view of geographically dispersed locations on the internet. These are deployed in tier 2 and tier 3 data centers and managed and maintained by the ThousandEyes Operations team.

Internal: These are locally available **enterprise agents** installed within the enterprise network environment and observe from the point of view of someone using the network from within the enterprise network. They provide visibility to applications installed in enterprise data centers (local and remote) as well as cloud based services.

End User: These are the **endpoint agents** deployed on end-user workstations and observe the experience from end-user perspective. These are ideal for home based or mobile users as it provides visibility of any issues from the laptop through the local ISP to the healthcare network or cloud service as appropriate.

The data collected in real time from these three agents is correlated and processed by Big Data Analytics which is then presented in a user-friendly web view to provide meaningful insights, key performance indicators, fault reporting, optimisations, user experience etc.



Cisco ThousandEyes

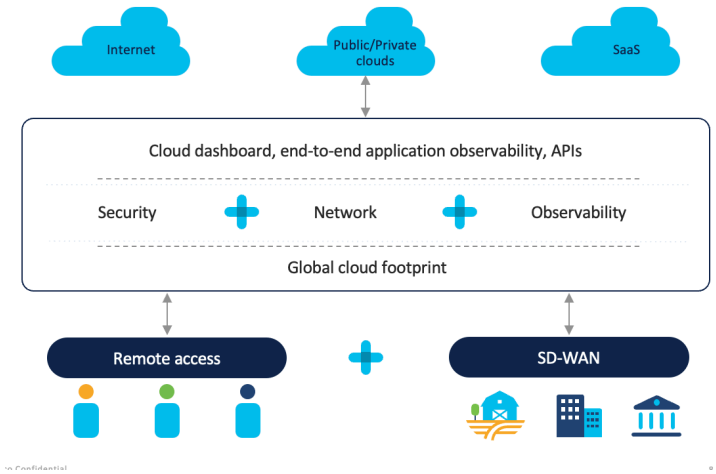
https://www.cisco.com/c/en/us/products/cloud-systems-management/internet-cloud-intelligence/index.html

Getting Started with ThousandEyes

https://docs.thousandeyes.com/product-documentation/getting-started

8.3. Introducing Cisco+ Secure Connect

Cisco+ Secure Connect is a SASE offer that radically simplifies the way companies can enable secure access to applications and resources hosted anywhere – across multiple public and private clouds – from any location at any time. The solution is easy to deploy, use, and manage through a unified cloud dashboard, it significantly reduces organisation's operational complexities to deliver greater agility, speed, and scalability.



Cisco+ Secure Connect offering brings together networking, client connectivity, security, and monitoring capabilities into a single subscription service that will deliver seamless, secure access to any application, over any network, regardless of location.

This solution focus on addressing three main challenges:

Simple: provide an offer that is simple, easy to consume, cost effective and use as-a-service subscription.

Secure: provide an intent-based security model with minimum user intervention enabled by a unified management interface and enforce security closest to threats.

Innovate: provide an Intelligent and agile solution focused on delivering business value by delivering actionable, predictable insights helping to enhance user experience.

Cisco+ Secure Connect

https://www.cisco.com/c/en/us/products/plus-as-a-service/secure-connect.html

https://www.cisco.com/c/en/us/products/collateral/plus-as-a-service/secure-connect-now-ds.html

https://documentation.meraki.com/CiscoPlusSecureConnect

https://documentation.meraki.com/CiscoPlusSecureConnect/overview/Cisco__Secure_Connect_Now-_Quick_Start

8.4. Introducing Cisco Secure X

Secure X is Cisco's cloud-native integrated security platform with Extended Detection & Response (XDR) capabilities. Secure X aims to simplify security and accelerate detection, response & recovery. This is achieved by an integrated approach to combine multiple otherwise disparate sensor and detection technologies into one unified location for **visibility** and provides automation and orchestration capabilities to maximize operational **efficiency**.

Orchestration

Automate routine tasks using prebuilt workflows that align to common use cases. Or build your own workflows with our low- to no-code, drag-and-drop canvas.

Threat response

Detect, respond, and recover faster with superior insights and context. Accelerate threat investigations and incident management by gathering and correlating global intelligence in a single view.

Device insights

Get a comprehensive device inventory with the contextual awareness needed to identify gaps in coverage and simplify security investigation.

Ribbon and single sign-on

Use the dashboard ribbon for quick access to SecureX features. Single sign-on helps you share and maintain context around incidents in one location.

For key capabilities, use cases and platform specifications please refer the Data Sheet.

Secure X Data Sheet

https://www.cisco.com/c/en/us/products/collateral/security/securex/secure-x-datasheet.html?CCID=cc001528&DTID=olgmcdc001463&OID=trlsc021059

Secure X Resources

https://www.cisco.com/c/m/en_us/products/security/securex/setup-guide.html

Secure X At a Glance

https://www.cisco.com/c/en/us/products/collateral/security/securex/at-a-glance-c45-744497.html?CCID=cc001528&DTID=olgmcdc001463&OID=trlsc021059

Secure X Product Integrations

https://www.cisco.com/site/uk/en/products/security/securex-platform/integrations.html?CCID=cc001528&DTID=olgmcdc001463&OID=trlsc021059

9. Quality of Service (QoS)

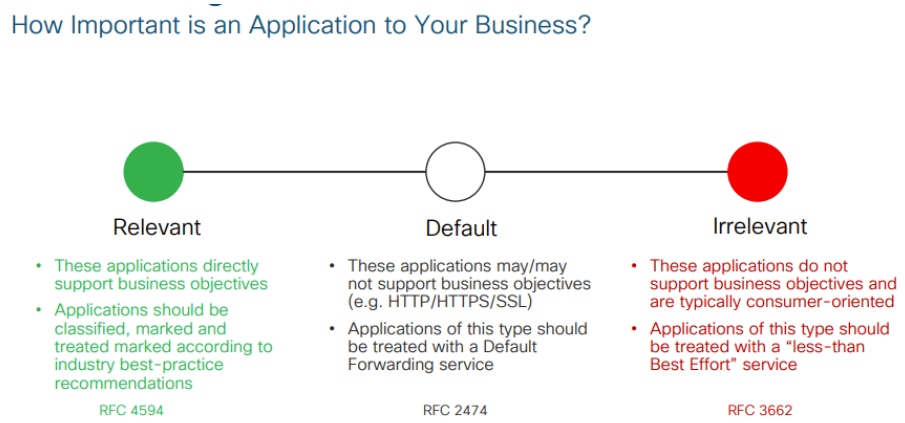
When we consider on-going operation of any Infrastructure, the requirement to control or "prioritise" traffic is a significant factor. The primary role of QoS in campus networks is to manage packet loss:

- It takes only a few milliseconds of congestion to cause drops.
- Rich medial applications are extremely sensitive to packet drops.
- Queuing policies at every node can prevent packet loss for real-time applications.

As hospitals continue their digitisation journey the demands placed on the network will only increase. A typical hospital will have hundreds of applications, all with different characteristics, business priorities and requirements. For example, clinical system traffic should be prioritised over web browsing.

Historically, a network administrator would need to read and understand the entire QoS Configuration Guide[31] (Classification, Marking, Shaping, Policing, Queuing and Trust) to build out a script to deploy across the network. This would need to be updated every time a new application was deployed. Instead, many organisations chose to continually add bandwidth to avoid deploying QoS. Unfortunately, this leaves the organisation susceptible to Denial-of-Service and Distributed Denial-of-Service attacks by an attacker exploiting vulnerabilities in software or misconfigured servers and devices.

DNA Center seeks to simplify the deployment of QoS by asking a simple question: "How Important is an Application to Your Business?". Relevant, Default or Irrelevant?



[31] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/qos/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html

When looking at deploying QoS across the organisation, some principles should always be adhered to:

QoS Design Best Practice / Principles:

- Always perform QoS in hardware rather than software when a choice exists.
- Classify and mark applications as close to their sources as technically and administratively feasible.
- Establish the QoS trust boundary at the access-edge of the network.
- Trust QoS within the distribution and core layers of the network – and across the WAN
- Police unwanted traffic flows as close to their sources as possible
- Enable queuing policies at every node where the potential for congestion exists.

The components of QoS can be summarised below:

- Classification— Classification is the process of distinguishing one type of traffic from another based upon access control lists (ACLs), Differentiated Services Code Point (DSCP), Class of Service (CoS), and other factors.

- Marking and mutation— Marking is used on traffic to convey specific information to a downstream device in the network, or to carry information from one interface in a device to another. When traffic is marked, QoS operations on that traffic can be applied. This can be accomplished directly using the set command or through a table map, which takes input values and translates them directly to values on output.

- Shaping and policing— Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that downstream devices are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface. Policing is used to impose a maximum rate on a traffic class. If the rate is exceeded, then a specific action is taken as soon as the event occurs.

- Queuing — Queuing is used to prevent traffic congestion. Traffic is sent to specific queues for servicing and scheduling based upon bandwidth allocation. Traffic is then scheduled or sent out through the port.

- Bandwidth—Bandwidth allocation determines the available capacity for traffic that is subject to QoS policies.

- Trust— Trust enables traffic to pass through the device, and the Differentiated Services Code Point (DSCP), precedence, or CoS values coming in from the end points are retained in the absence of any explicit policy configuration.

To examine some of the detail, it is simple to establish how the prioritisation and queuing of the infrastructure is performed. If we look at the configuration of a typical switch port:

```
L2_EDGE2#sh interface capabilities
GigabitEthernet1/0/1
  Model:                 C9300-24T
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,half,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Unicast suppression:   percentage(0-100)
  Multicast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),
                         tx-(2p6q3t)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            yes
  Dot1x:                 yes
  Multiple Media Types:  rj45
```

We can see from the above that this switch QoS mechanisms are 2p6q3t - In this case, that means – 2 priority, 6 queues, 3 threshold per queue.

However, this very quickly starts to add complexity, especially when we start to look at the deployment guides for QoS – class maps, policy maps, DSCP-COS values, shaping, WRED, tail-drop – these are just some of the concepts required to facilitate a successful deployment of QoS.

9.1. QoS Deployment

Fortunately, we now have the tools available to alleviate all the issues identified above, which provides rapid deployment of QoS to meet the business needs – "Intent Based Networking".

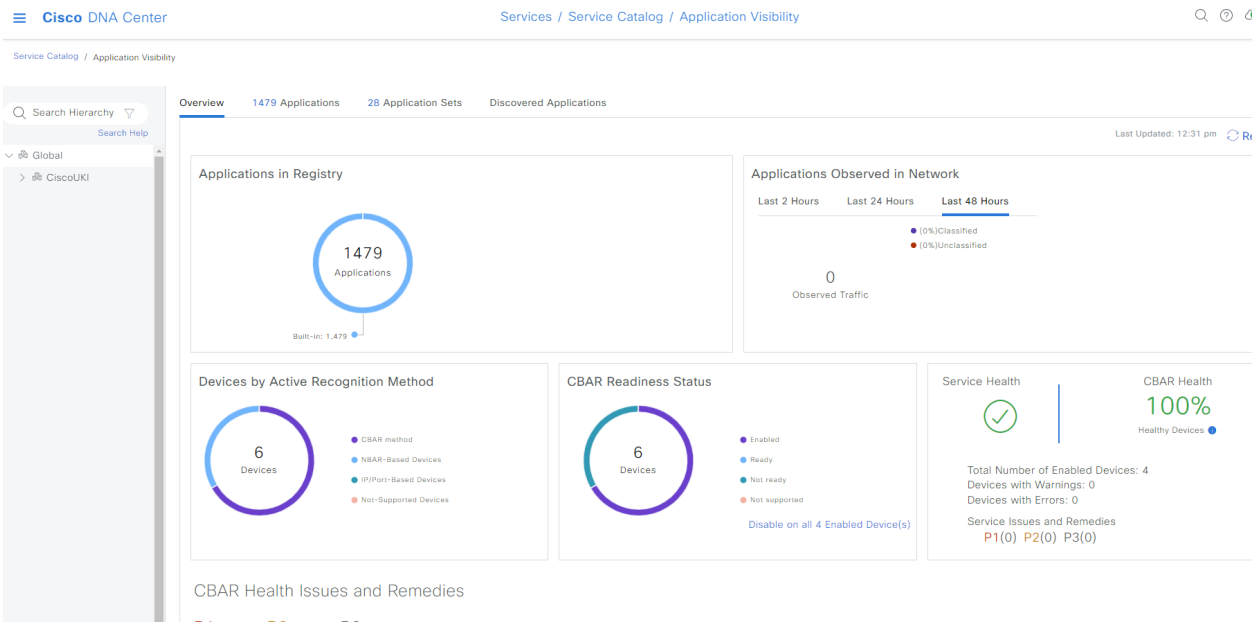
It is worth re-iterating at this point, that these tools do not necessarily require a fabric – Software Defined Access also applies to non-fabric deployments.

The main intent of an organisation, if we recap, is to enable:

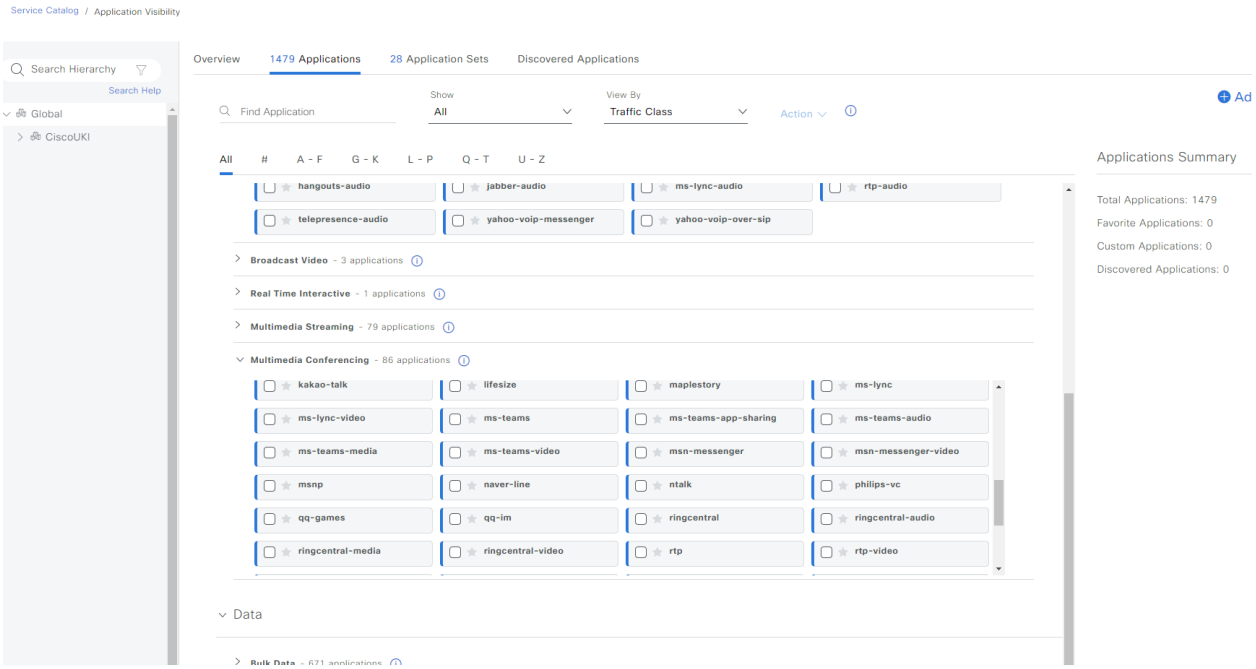
- Identification of applications – automatically through AI or manually defined.
- Prioritisation of mission critical applications.
- Protection of network resources – Scavenger class.
- Provide rapid change – i.e., add and prioritize a new application.

Cisco has been utilising Network Based Application Recognition (NBAR) for a considerable amount of time, which is crucial when formulating QoS policies such as class maps and policy maps, as it serves as the foundation for matching criteria.

We know have the concept of CBAR – Controller Based Application Recognition. Fundamentally, this allows organisations to define their own applications.



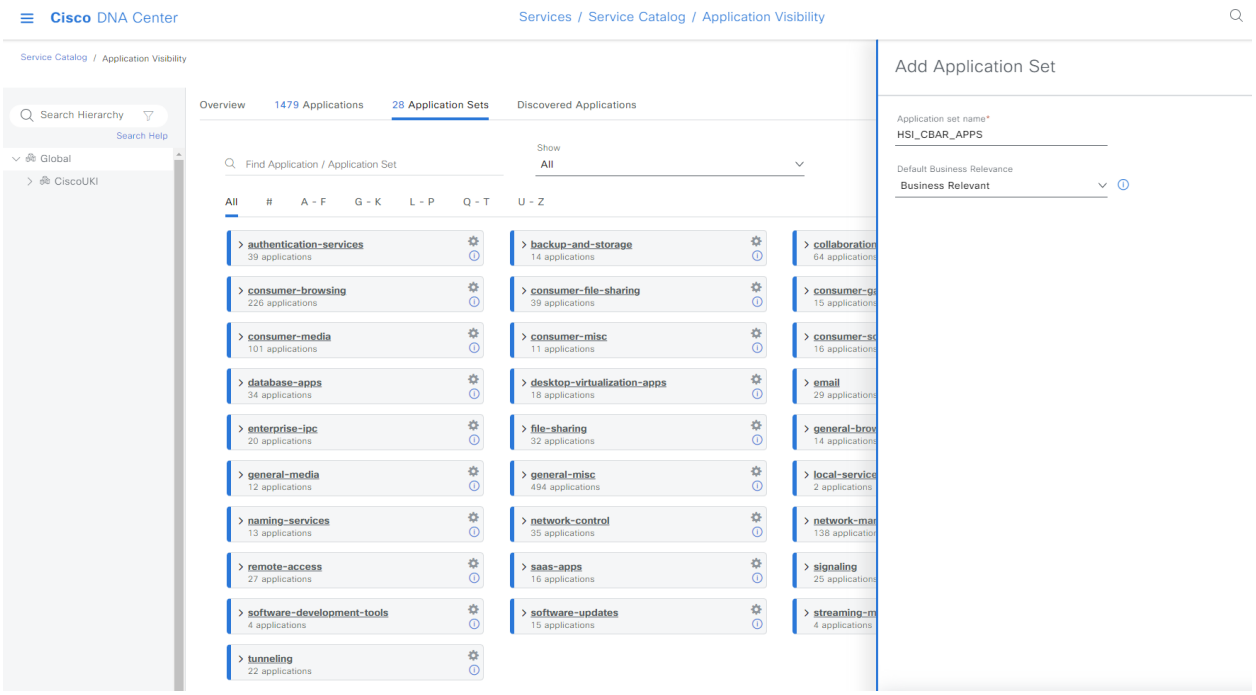
If we look at the applications defined by default – NBAR:



We can see the some of the important applications are already there, e.g., Cisco Telephony, WebEx, MS Teams.

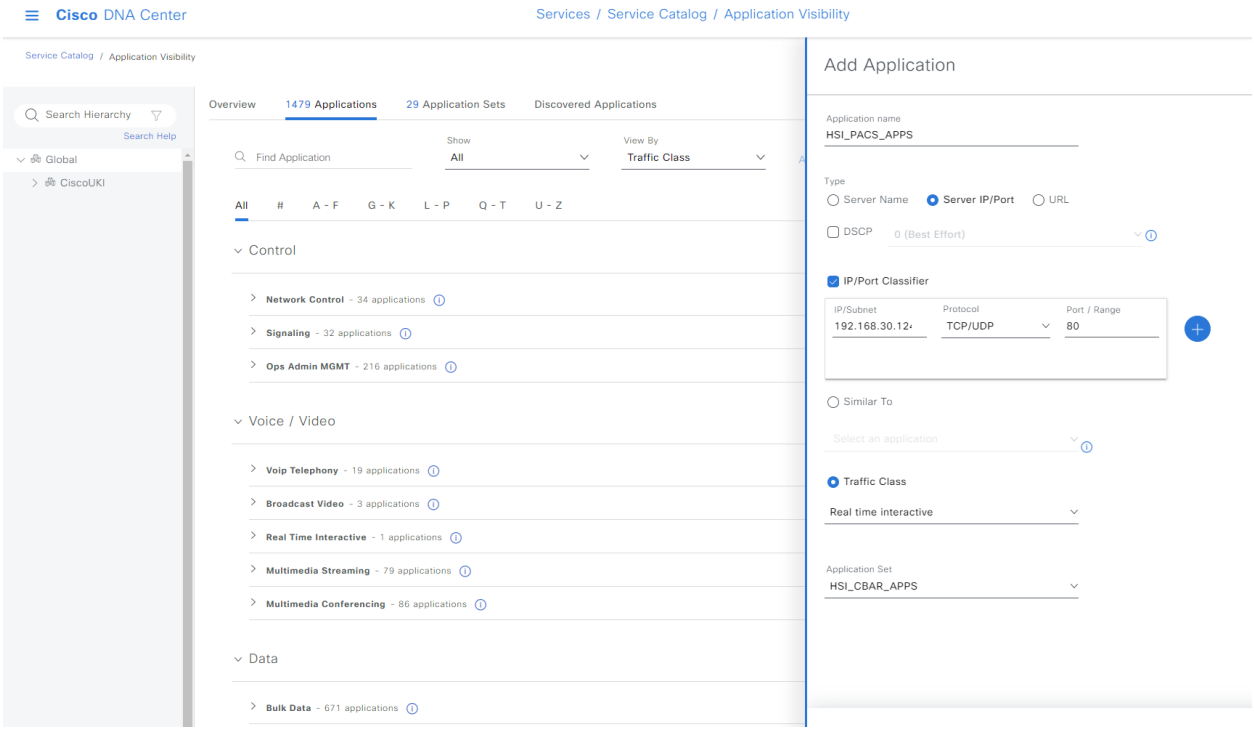
Using this as a base, organisations can define their own applications very easily:

First – create an application set:

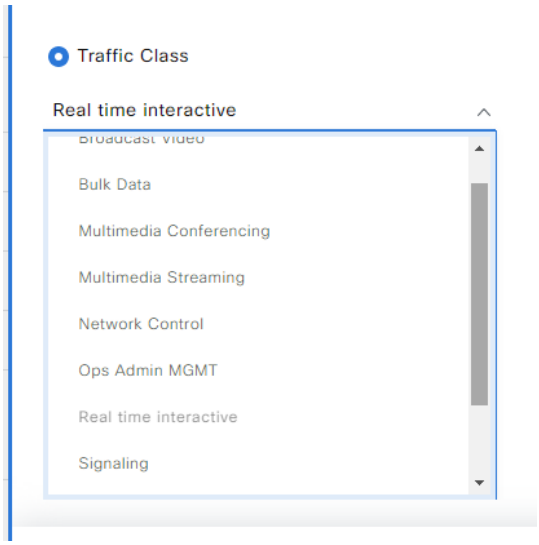


Note the reference to Business Relevant.

Then define an application and add it to the application set:

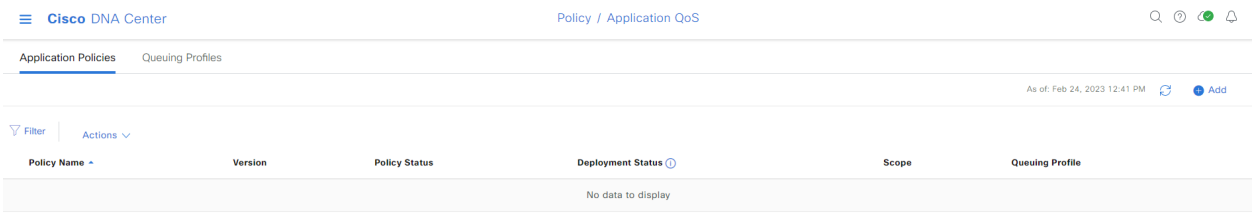


Note the Traffic Class identified – there are several options available:



Again, this forms the basis of Intent Based Networking – the outcome is relevant, the mechanism to achieve it should be automated.

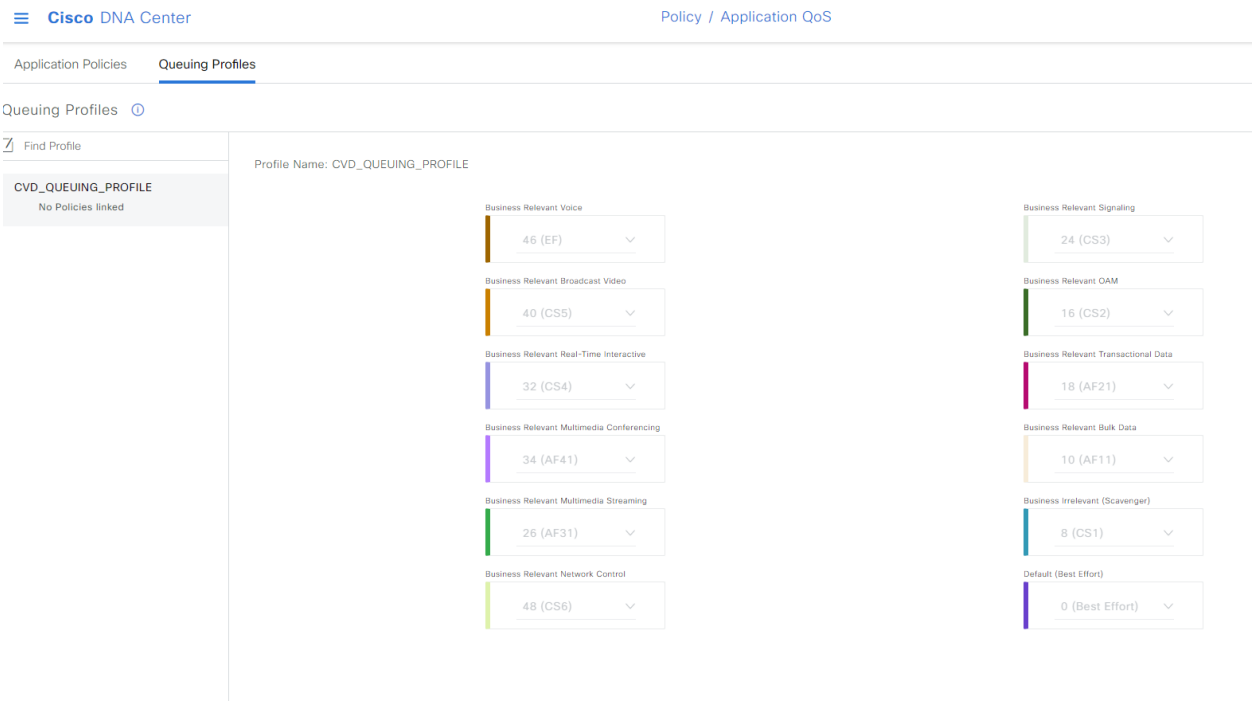
With our applications defined, the next step is to simply deploy – this is achieved through the Application QoS function.



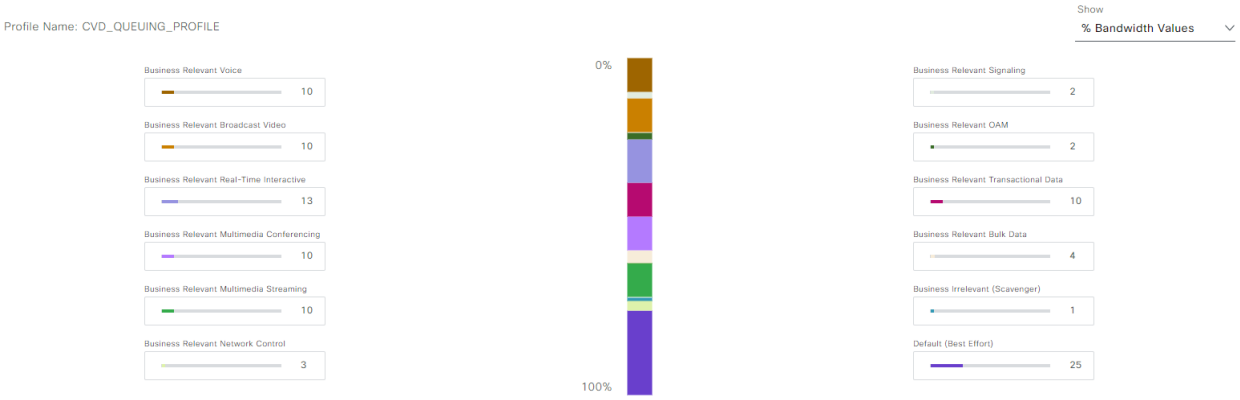
If we look at the queuing profiles, we can see that it is derived from the Cisco Validated Design (CVD) for QoS:

(For interest, one of the original CVDs dated 2005 was a mere 330 pages!)

https://community.cisco.com/legacyfs/online/legacy/3/2/6/64623-qossrnd.pdf

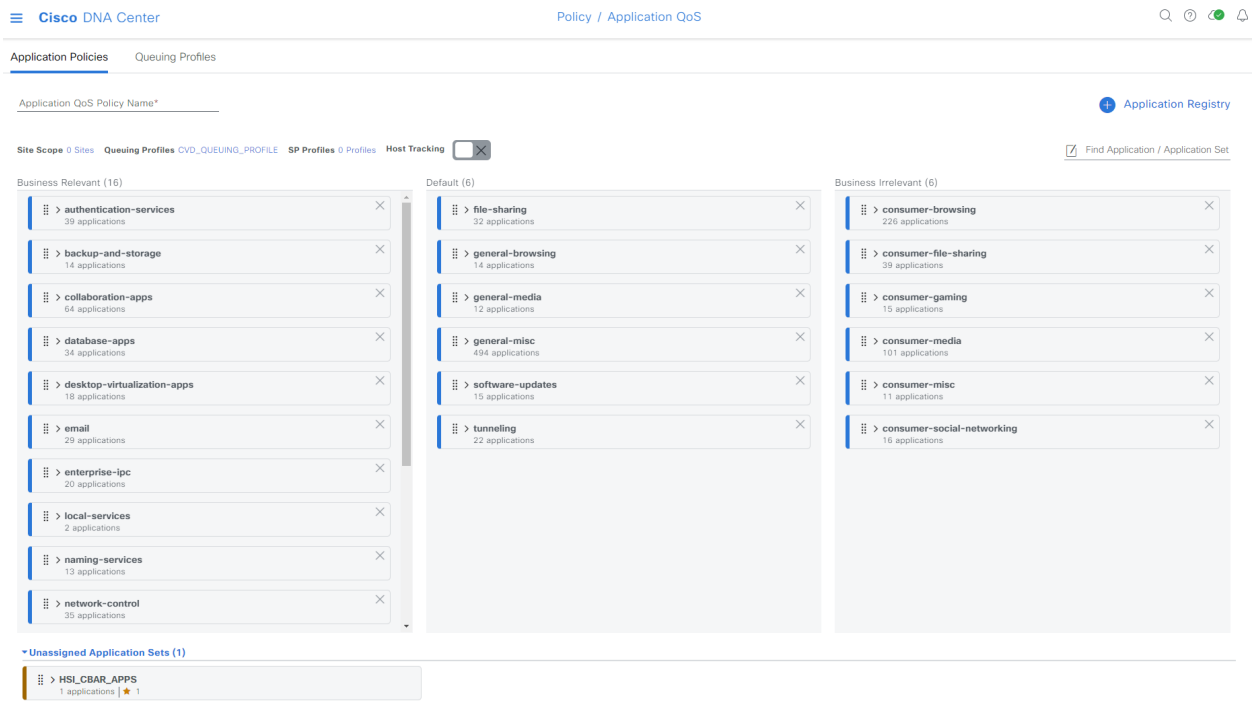


Again, it's worth noting that EF (Expedite Forward), CS1 – Scavenger are pre-defined. Along with the recommended bandwidth percentages:



All the necessary technical components are built into the DNA Application itself. All that is required is to define what the business relevance is of the previously CBAR defined applications:

Here we can see the three pillars:

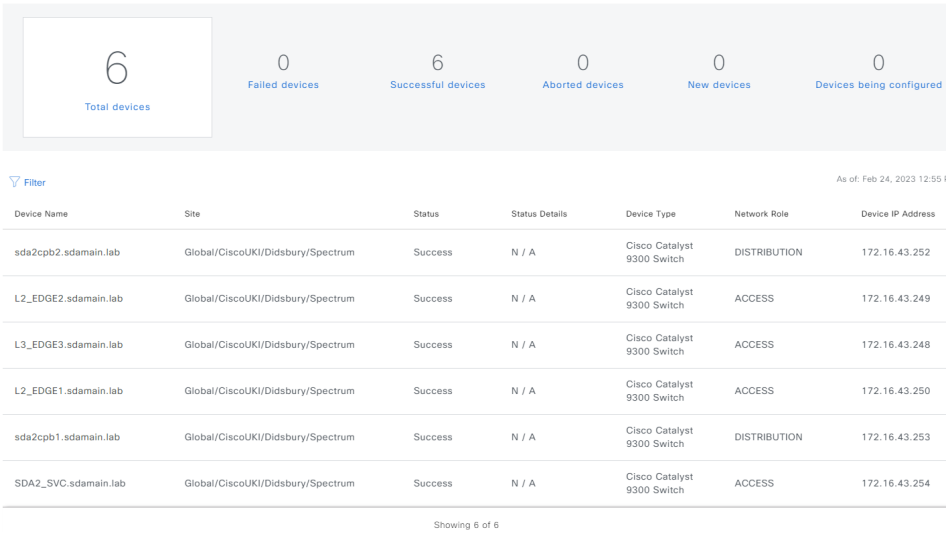


And our custom applications defined ready to be placed under one of the pillars. We could for example, create multiple application sets for apps that are not already defined – or importantly, if we identify a badly performing device, we can simply create a new “app” for that device, classify it as “scavenger” position it under Irrelevant, and deploy – issue mitigated.

For our critical applications defined previously – add to the Business Relevant Pillar –

Assign the policy a name, select site or sites and then deploy.

HSI_QOS_POL1



Within seconds – the full CVD derived QoS policy is deployed across the organisation.

An extract of a completed configuration is shown below:

```
class-map match-all DNA-MARKING_IN#VOICE
 match protocol attribute traffic-class voip-telephony
 match protocol attribute business-relevance business-relevant
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any DNA-EZQOS_2P6Q3T_9K#BULK-DATA
 match dscp cs1
 match dscp af12
 match dscp af13
 match dscp af11
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-high-rate-app
  description High Rate Applications
class-map match-any system-cpp-police-multicast
  description MCAST Data
class-map match-any DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE
 match dscp cs3
 match dscp cs2
 match dscp cs7
 match dscp cs6
class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
 match dscp af43
 match dscp af41
 match dscp af42
```

```
policy-map DNA-MARKING_IN
 class DNA-MARKING_IN#TUNNELED-NBAR
 class DNA-MARKING_IN#VOICE_CUSTOM
  set dscp ef
 class DNA-MARKING_IN#BROADCAST_CUSTOM
  set dscp cs5
 class DNA-MARKING_IN#REALTIME_CUSTOM
  set dscp cs4
 class DNA-MARKING_IN#MM_CONF_CUSTOM
  set dscp af41
 class DNA-MARKING_IN#MM_STREAM_CUSTOM
  set dscp af31
 class DNA-MARKING_IN#CONTROL_CUSTOM
  set dscp cs6
 class DNA-MARKING_IN#SIGNALING_CUSTOM
  set dscp cs3
 class DNA-MARKING_IN#OAM_CUSTOM
  set dscp cs2
 class DNA-MARKING_IN#TRANS_DATA_CUSTOM
  set dscp af21
 class DNA-MARKING_IN#BULK_DATA_CUSTOM
  set dscp af11
 class DNA-MARKING_IN#SCAVENGER_CUSTOM
  set dscp cs1
 class DNA-MARKING_IN#VOICE
  set dscp ef
 class DNA-MARKING_IN#BROADCAST
  set dscp cs5
 class DNA-MARKING_IN#REALTIME
  set dscp cs4
 class DNA-MARKING_IN#MM_CONF
  set dscp af41
 class DNA-MARKING_IN#MM_STREAM
  set dscp af31
 class DNA-MARKING_IN#CONTROL
```

The purpose of including descriptions of the steps involved is to demonstrate that the complexities of QoS should in no way be a block to it being successfully deployed and provide the fundamental building block for securing ongoing network operations.

10. Use case: Secure remote worker.

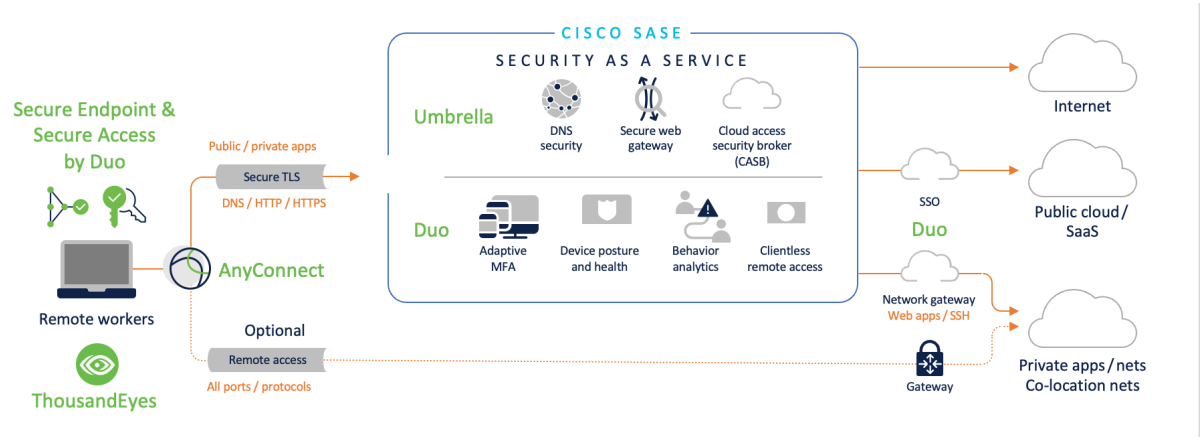
CORE ELEMENTS

- Cloud security
- Zero trust secure access
- Remote access + ZTNA
- Observability

ENHANCEMENTS

- MDM
- Endpoint security

High Level Solution: Cisco AnyConnect client integrates with Cisco Umbrella. Umbrella helps delivery cloud-delivered security which helps segregating traffic based on Zero trust policy and provides DNS security even when the VPN is not connected. DUO provides identity management, secure multifactor authentication, posture assessment and heuristics and act as a Zero trust broker before access is granted. ThousandEyes converges the network and security observability into a single platform, help observe traffic and isolate issues while traffic is traveling via different paths.



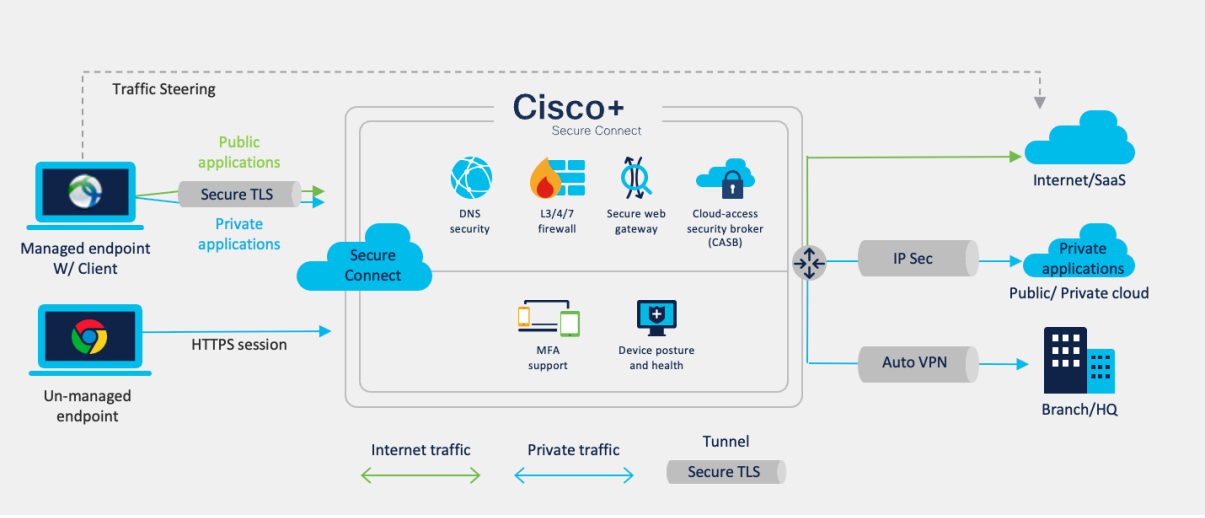
When implementing a remote worker solution, we must consider security of the end device as well as establishing user identity. Both the user and the device are outside the hospital network, and it becomes vital to establish identity and access requirements so that the security posture of the hospital is not compromised. As said earlier in the document with changing threat landscape the network security boundary moves with the users and the devices.

In the suggested SASE approach to remote worker enablement, we only allow connection to the hospital network and applications if the end user successfully establish identity and the end device successfully pass posture assessment such as operating system version, anti-malware scan, antivirus scan and other anomaly detection mechanisms. The security configuration and device posture are then continuously validated for continued access.

With SASE approach we also address evolving remote access requirements. The suggested architecture allows to route traffic depending on the applications' zero trust policy. This means, the ability to route traffic directly over the internet for zero trust enabled applications such as Office 365 and similar SaaS services, all public internet traffic is directed via the secure web gateway and all corporate traffic such as on-prem hosted applications are routed over the encrypted VPN tunnel. This approach provides an optimal way of routing traffic by providing a shorter path to destination and avoiding hair-pinning of all traffic via the enterprise data centers.

While we optimise traffic routing and improve user experience by routing traffic to different locations via different paths, we introduce the challenge of observing this traffic and our ability to identify and fix problems. This is where ThousandEyes plays the key role of monitoring traffic and user experience for business applications and allow to identify and fix problems with precisions. ThousandEyes makes it possible to pinpoint the source of the problem and avoid costly downtimes by accelerating response time.

Cisco+ Secure Connect Secure Remote Worker



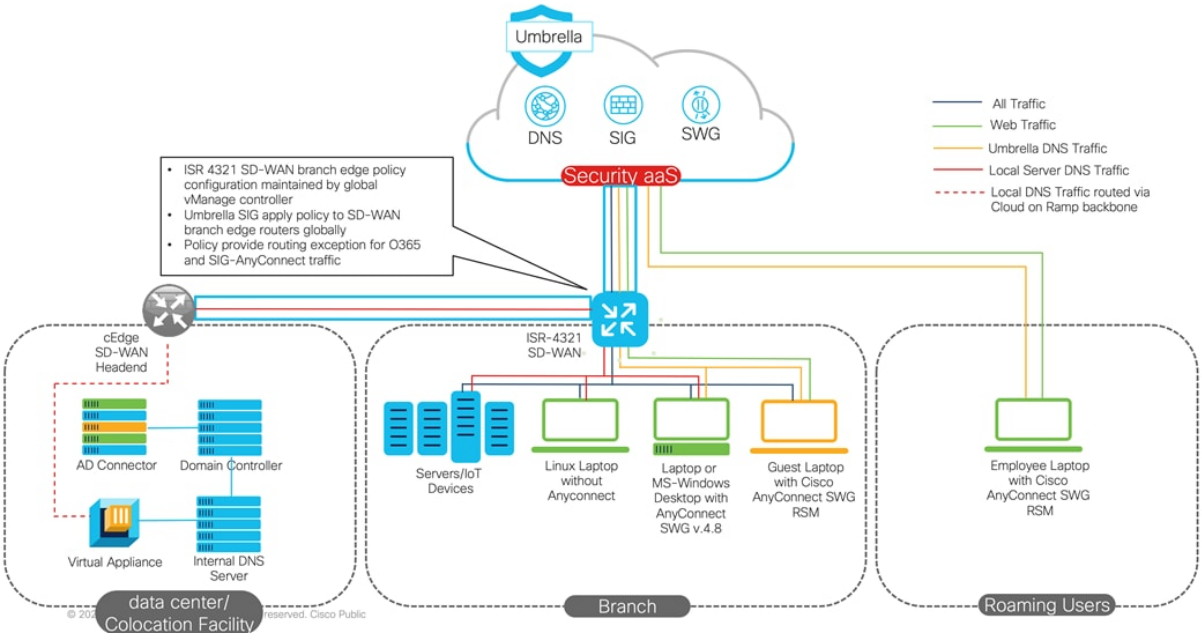
Please refer the design guide for use cases, capabilities, and features.

Cisco Remote Worker Design Guide

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/srw-design-guide.pdf

11. Use Case: SD-WAN deployment with Umbrella integration

The following diagram shows a typical SD-WAN/Umbrella deployment: Local Site (branch), roaming guest devices, and the Cisco SD-WAN branch edge router . On-premises traffic flows to Umbrella cloud via the SIG IPSec tunnel, off-premises traffic flows to Umbrella cloud via AnyConnect agent. Various site edge devices are connected via SD-WAN TLS tunnels for local/internal traffic. DNS traffic from the data center is sent to the Umbrella cloud via the Virtual Appliance. Next project phase should address migrating remote roaming devices to Umbrella.



The unified Umbrella service allows the customer to secure their Internet-bound traffic in the following ways:

On-Premises Traffic

Web Traffic: all on-prem users/machines web traffic (ports TCP/80 for HTTP, and TCP/443 for HTTPS) will be forwarded to the Umbrella SWG (Secure Web Gateway) to be inspected, controlled, and filtered by the Umbrella cloud proxy (via SIG IPSec tunnel)

Non-Web Traffic: all on-prem users/machines non-web traffic will be forwarded to the Umbrella CDFW to be filtered by the Umbrella Layer3/Layer4 cloud firewall (via SIG IPSec tunnel)

DNS traffic: all on-prem users/machines DNS traffic (port UDP/53) will be forwarded to the Umbrella DNS (Domain Name System) to be controlled and filtered by the Umbrella cloud DNS (via Virtual Appliance servers)

Off-Premises Traffic

Web Traffic: all off-prem users web traffic (ports TCP/80 for HTTP, and TCP/443 for https) will be forwarded to the Umbrella SWG to be inspected, controlled, and filtered by the Umbrella cloud proxy (via AnyConnect client)

DNS traffic: all off-prem users DNS traffic (port UDP/53) will be forwarded to the Umbrella DNS (Domain Name System) to be controlled and filtered by the Umbrella cloud DNS (via AnyConnect client.

With this solution in place, users will have a uniform experience regardless of their location (on- or off-prem) and will be always protected from Internet threats. Backing all this is threat intelligence from Cisco Talos, one of the largest commercial threat intelligence teams in the world.

Please refer the design guide for use cases, capabilities, and features.

Cisco SD-WAN Design Guide

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

Cisco Umbrella Design Guide

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/umbrella-design-guide.pdf

Cisco SDWAN integration with Umbrella

https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214155-configure-integration-with-cisco-umbrell.html

12. Multi Agency – WWA.NET

Increasingly, especially with the advent of Integrated Care Boards/Systems, there is a requirement for full agility, cross-organisation or service, shared and cooperative working.

Several organisations have deployed various methods of achieving this “nomadic” working principle, most of which rely on client driven VPN based solutions, or mutual “anchoring” arrangements.

Whilst these have provided a stop-gap solution, they lack scalability in relation to number of organisations participating, and importantly, added complexity for end users.

Cisco have developed a model for multi-agency working. This removes the burden of connectivity from the end users and provides a scalable and repeatable solution.

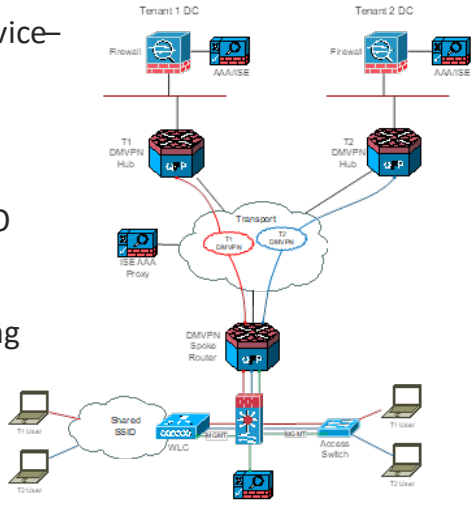
The key driver was to ensure the Cross Organisation Agility – same user experience in different organisation premises. Also, where organisations are not connected to a common infrastructure (e.g HSCN), they are also able to participate.

The following provides the overview and detail of how this may be deployed.

PO = Participating Organisation

The Technical High Level View

- One of the POs provide the “Central Service– DMVPN Hub and AAA Proxy(ISE)
- Each PO has a single “Spoke”– usually in their DMZ/DC.
- Secure “Mesh” formed between each PO
- **No Extra VPN solution required.**
- DHCP/VLAN/Policy controlled for roaming users via their own PO



10

Benefits of Solution over client based VPN

- Quality of Service (QoS) – performance at LAN speeds not VPN speed.
- Ease of use/familiar method of working for end users
- Usage of solution visible to each PO via their own AAA server
- Full stack observability – tunnel egresses onto PO own LAN
- Users appear to be on PO local LAN.
- Simple to deploy
- Again, no additional client VPN termination required.

Rules of sovereignty

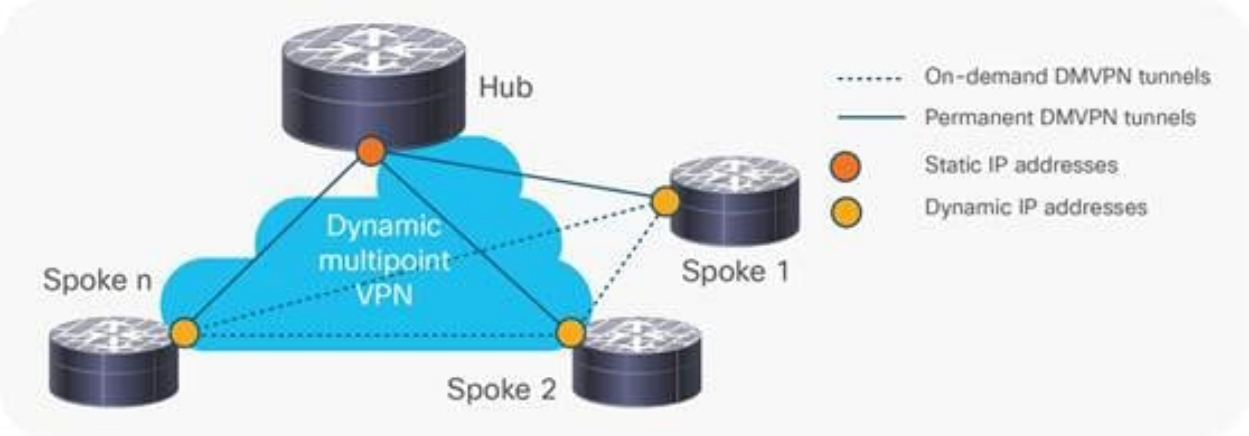
Within an ICS -

- No major network redesigns
- Each PO maintains control of their network, no new links etc.
- Very RAPID deployment.
- Access Policies, Certificates, Credentials, GP managed by each PO
- No federation required
- Works with overlapping RFC1918 IP Addresses (172.x, 192.x, 10.x)

A more technical explanation is provided below:

12.1. High-level Shared Workplace Infrastructure Design

Cisco Dynamic Multipoint VPN (DMVPN) is a security solution for building scalable enterprise VPNs that support distributed applications such as voice and video.



Cisco DMVPN is widely used to combine enterprise branch, teleworker, and extranet connectivity. Major benefits include:

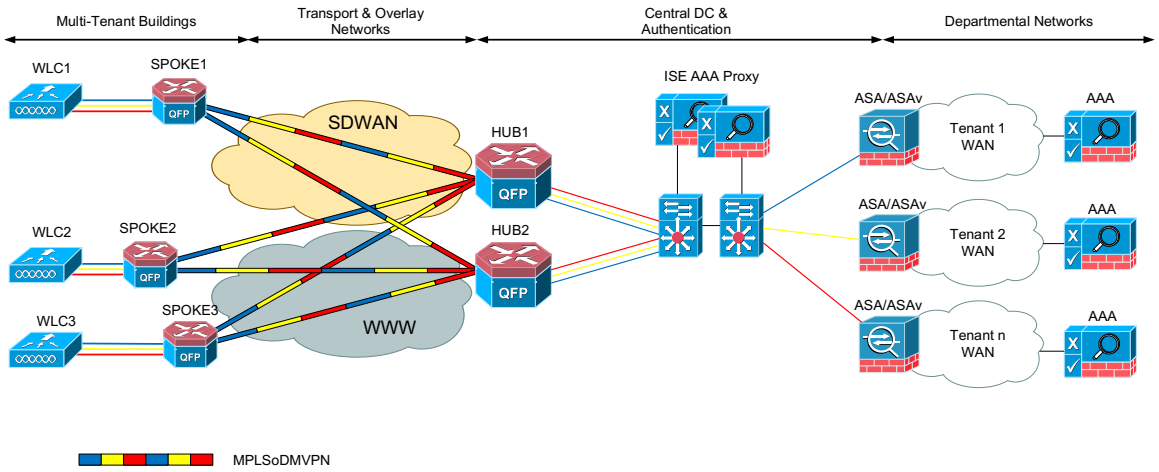
- On-demand full mesh connectivity with simple hub-and-spoke configuration
- Automatic IP Security (IPSec) triggering for building an IPSec tunnel
- "Zero-touch" deployment for adding remote sites
- Reduced latency and bandwidth savings

DMVPN is fully VRF-aware. This allows DMVPN tunnels to be sourced from and attached to VRF's on a Cisco router as well as the global/default routing table. Cisco routers can join multiple DMVPN networks with each in a separate VRF if required. This facilitates the construction of different overlay topologies for each VRF or tenant.

DMVPN can also take advantage of Front VRF (fVRF) and Inside VRF's (iVRF) which allow the tunnel source interface and the tunnel interface to be in different VRF's. The tunnel source interface is placed in the fVRF and the GRE encapsulation/decapsulation process forms a secure "conduit" through to the tunnel interface placed in an iVRF. This allows the internet to be used as a tunnel transport network safely as the internet connection is placed in a separate VRF to the internal corporate networks.

A single MPLS enabled DMVPN. An MPLS enabled DMVPN reduces the overlay network to a single DMVPN which is shared by all tenant traffic. Separation of the traffic flows is maintained by MPLS VPNv4 labels applied to the packets on ingress to the router from the iVRFs. This model requires DMVPN hubs to be provided centrally.

MPLS over DMVPN



An MPLS over DMVPN design requires:

- **A single DMVPN overlay.** A single DMVPN overlay will be created to tunnel the traffic for each of the participating organisations from the multi-tenant buildings to a central datacenter. Traffic from the multi-tenant buildings will be aggregated at the central datacenter and forwarded onto the individual tenant networks, typically using an Option-A interconnect dual MPLS enabled DMVPN's over two different transport networks can be used for resilience.
- **Centralised DMVPN Hub routers**. The MPLS enabled DMVPN will require hubs located in the central datacenter. Dual Hubs should be used for resilience.
- **One or more DMVPN Spoke routers**. The DMVPN routers at the multi-tenant buildings will be spokes in the MPLS enabled DMVPN. All tenants will share the DMVPN routers, and their traffic will remain separated by VRF's.
- **Dynamic full-mesh DMVPN deployments.** The DMVPN should be deployed in dynamic full-mesh mode to support peer-to-peer applications between remote users at different locations on the DMVPN, e.g., voice/video calls with Cisco WebEx. Traffic between multi-tenant buildings will be MPLS switched over dynamic on-demand tunnels.
- **GRE encapsulation with IPSec protection on unassured transport networks.** IPSec tunnel protection must be enabled on Internet based DMVPN's in accordance with CPA Foundation Grade IPSec Security Gateway guidance.
- **Use of Global Routing Table and iVRF's.** In an MPLS enabled DMVPN, the tunnels MUST be sourced from and terminated in the Global Routing table for BGP VPNv4 next-hop resolution to work correctly. All customer facing interfaces, i.e. the tenant VLAN's are placed in iVRFs.
- **Multi-Protocol BGP (MP-BGP)**. MP-BGP with VPNv4 SAFI is the only dynamic routing protocol permitted on the MPLS enabled DMVPN overlay although IGP's can be run within the iVRF's and redistributed into MP-BGP just as in a normal MPLS L3VPN network. The hubs should be configured as VPNv4 Route Reflectors and spokes should peer with all hubs.

IPSec Requirements

Internet Based DMVPN must use one of the following CESG approved IPSec profiles. At time of writing, the guidance[32] states:

CESG Foundation and PRIME cipher suites

Algorithm	Foundation	End-State PRIME
Encryption ESP	AES-CBC 128	AES-GCM 128
Key Exchange	IKEv1	IKEv2
Hash	HMAC-SHA256-128	HMAC-SHA256-128
Diffe-Hellman	Group 14	Group 19
Authentication	RSA X.509v3	ECDSA 256bit X.509v3
Certificate Enrolment/Re-Enrolment	SCEP	EST

Additional Considerations

IP Addressing

As there will be no direct routing between the VLAN's of the different tenants, the IP subnets to be used to address the devices on each VLAN should be supplied from each tenant's own internal addressing schemes. This avoids the complexity of having to find an RFC1918 address range which is unique across all tenants.

DHCP & DHCP Relay

Once an authenticated user has been placed onto the appropriate VLAN, the user's device will attempt to obtain an IP address via DHCP.

At smaller sites, the WAN router can provide DHCP service by either:

[32] CESG document – Network Encryption at OFFICIAL v2.3

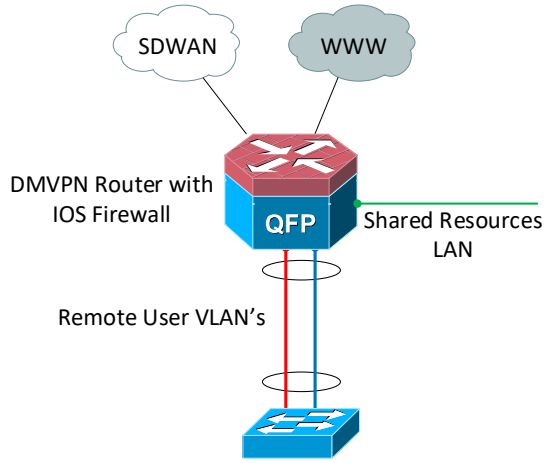
- Running a VRF-aware IOS DHCP server to offer IP configuration locally.
- Running DHCP Relay on the VLAN sub-interface to unicast the DHCP request to a central DHCP server at the user's home network via the DMVPN – preferred option.

At larger sites, DHCP can be offered by either:

- Local DHCP server(s); Running IP-Helper on the SVI interfaces of the LAN switches to unicast the DHCP request to a central DHCP server at the user's home network via the WAN router.

Access to Shared Resources

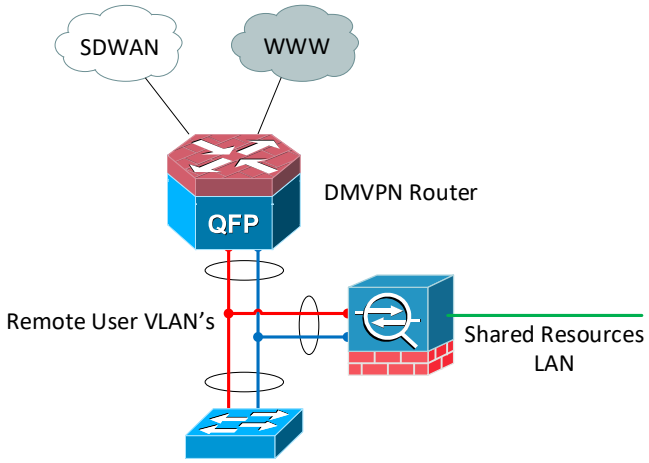
Two possible approaches to accessing shared resources from the VLAN's are detailed below.



IOS-XE Zone-Based Firewall for Inter-VRF Routing

- Place the shared resources into their own iVRF.
- Use the Zone-Based Firewall in the IOS-XE router to provide routing and filtering between the tenant iVRF's and the Shared Resources iVRF.
- This solution is best suited to smaller locations.

- Use a dedicated firewall to provide routing and filtering between the Remote User VLAN's and the Shared Resources VLAN.
- The DMVPN router can use ICMP redirects to send traffic for shared resources to the firewall.
- Or use static NAT for shared resources so the devices appear on the Remote User VLAN's.
- This solution is best suited to larger locations.



Federated RADIUS Authentication Proxy Service

Authentication of users onto the shared SSID and wired LAN is ultimately performed by a RADIUS server located within the user's "home" network. This allows each organisation to maintain control and monitoring of users accessing their network and avoids reliance on a third-party. The WLC's and switches providing access to the shared infrastructure service send authentication requests to a local RADIUS server within the multi-tenant building in the first instance. The local RADIUS server uses the domain name or realm included in the user's credentials to identify if the user can be authenticated locally or if the request should be forwarded to the central RADIUS proxy servers. The central RADIUS proxy servers also use the domain name in the user's credentials to identify the RADIUS server to forward the request to. The internal RADIUS servers and central RADIUS proxy servers must have connectivity over the transport network to facilitate the proxy operation.

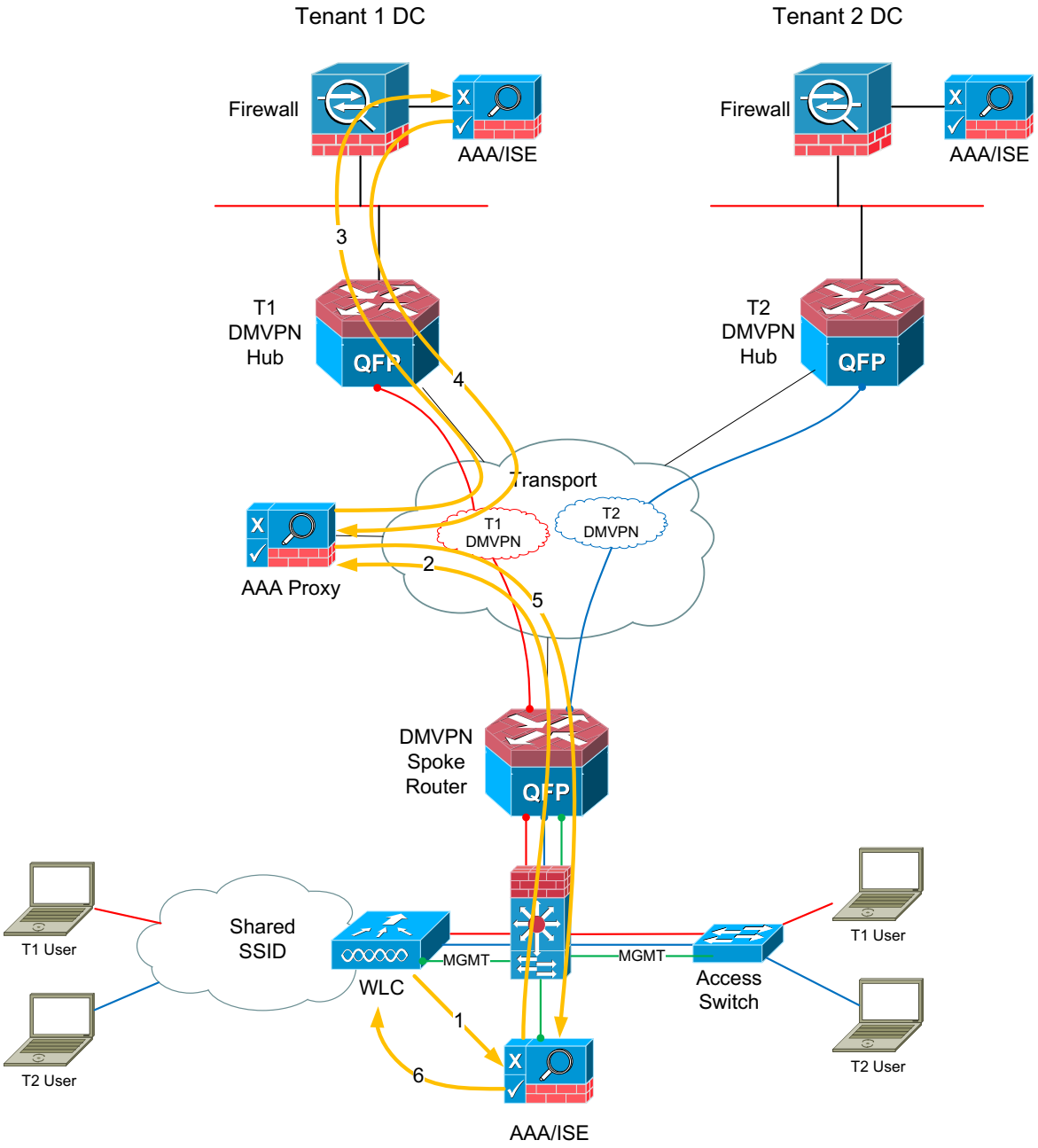
Ideally, client PC based devices should be capable of supporting TEAP (Tunnel Extensible Authentication Protocol (TEAP; RFC 7170)). Cisco ISE 2.7 and Windows 10 build 2004 (May 2020) added support for TEAP. This will allow for both user and machine authentication at the same time.

When the RADIUS Accept messages are returned to the local RADIUS server via the proxy, the local RADIUS will perform dynamic VLAN assignments by injecting RADIUS attributes (IETF64, IETF65 and IETF81) into the RADIUS Accept messages before forwarding them to the WLC or access switch. This ensures each tenant's VLAN's are only locally significant to the shared LAN infrastructure within the multi-tenant building.

Each multi-tenant building will require a standard VLAN mapping to be created for the tenant organisations.

Example of Tenant VLAN mapping

Organisation	Tenant VLAN
Tenant 1	10
Tenant 2	20
Tenant 3	30
Tenant 4	40



Radius Accept plus the following attributes:
IETF 64 (Tunnel Type) = VLAN
IETF 65 (Tunnel Medium Type) = 802
IETF 81 (Tunnel Private Group ID) = VLAN ID eg. 10 for Tenant 1

Authentication Flow and Dynamic VLAN Assignment

Authentication Workflow

1) Radius authentication request message from WLC or access switch sent to local Radius server.
2) Local Radius cannot authenticate user from its own local user list so forwards the authentication request to the Federated Radius Proxy
3) Radius Proxy forwards the authentication request to the user's home Radius server.
4) User's home Radius server authenticates the user and responds to the Proxy with Radius Accept message.
5) Proxy forwards the Radius Accept to the Radius server at the shared building.
6) Local Radius server performs dynamic VLAN assignment by injecting Radius attributes into the Radius Accept message before forwarding it onto the WLC or access switch.

Change of Authorisation (CoA) – RFC 5176

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy.

The standard RADIUS authentication and authorisation process typically uses a "pull" model, in which the requests originate from a network device and a response is sent from the queried RADIUS servers. RADIUS CoA requests defined in RFC 5176 are used in a "push" model, in which external servers can request network devices to initiate or re-initiate the authorisation process. This mechanism allows RADIUS servers to dynamically update the policy applied to individual sessions after they have been authenticated, e.g., moving a user to a quarantine VLAN or terminating their session in response to the detection of suspicious behaviour. Wired and wireless LAN equipment with support for CoA / RFC5176 should be deployed at multi-tenant buildings.

Conclusion

In conclusion, a secure, agile, and resilient healthcare infrastructure which is EPR ready is crucial to ensure the safety and privacy of patient records and other sensitive information that NHS must deal with on a regular basis. There are several challenges in implementing such infrastructure that meets the ever-increasing need for secure access, data privacy, identity management, and resilience to cyber-attacks.

Cisco provides a range of solutions and architectures that can address these challenges, including Cisco ISE, Cisco DNAC, and Cisco TrustSec. These solutions provide a comprehensive network access control solution that ensures only authorized users and devices have access to sensitive healthcare data.

Using network segmentation, 802.1X authentication, and zero-trust security principles, Cisco's solutions enable healthcare organisations to enforce access policies based on user and device attributes, to not only protect identity and privacy but also to protect organisation against cyber threats.

These technologies when implemented correctly helps ensure compliance to regulations and help deliver consistent policy enforcement both within and outside the hospital campus this enabling seamless hybrid working experience.

There are several business outcomes to be realised but primarily NHS can realise the following benefits.

Improve Patient Experience: improve patient experience by ensuring privacy and security of their sensitive health information. This will result in increased patient confidence and trust in the healthcare organisation, leading to better patient engagement.

Improve Operational Efficiency: improve operational efficiency by enabling secure remote access to healthcare services. This can lead to faster and more accurate diagnoses and reduced wait times which would increase staff satisfaction and make easier access to healthcare services for patients.

Strengthen Security Posture: reduce the risk of cyber-attacks and data breaches, which can lead to significant financial and reputational damage to healthcare organisations. By implementing network segmentation, zero-trust security principles, and access policies based on user and device attributes, healthcare organisations can significantly reduce the risk of cyber threats.

Ensure Regulatory Compliance: help healthcare organisations comply with regulatory requirements and standards, such as HIPAA and GDPR. This can help avoid costly fines and legal penalties and maintain the trust of patients and stakeholders.