

ICT at the Heart of NHS Reform



Cisco Network Architecture Blueprint (C-NAB)
for NHS Organisations

Volume 2: Technical Requirements – Architectures for Business and Service Transformation



Foreword

ICT at the Heart of NHS Reform



Cisco has had a dedicated Healthcare team offering guidance on Information and Communications Technology (ICT) solutions into the NHS since 1998, a thirteen year period that has seen significant changes in the UK Healthcare environment. Most recently, the Coalition Government signalled its intent to bring about one of the most transformational programmes the NHS has ever seen. Cisco believes that a significant enabler for the proposed reforms is the accelerated deployment of technology to offer business and service transformation.

Standards and best practice are very important to any organisation deploying technology-based solutions and throughout the last decade Cisco has issued many forms of guidance on ICT solutions for NHS organisations. Most significantly, in December 2008, the 'Cisco Network Architecture Blueprint for NHS Trusts' advocated an architectural approach that directly links ICT investment with business and clinical priorities. Given the extent of the Coalition Government's plans for NHS reform, we have revised that guidance in the form of this updated blueprint, once again emphasising the value of an architectural approach.

We hope this blueprint informs your approach to ICT and demonstrates how technology can be embedded into your business planning. Cisco believes that the right ICT foundation can lead to improvements in business processes and service delivery. Please let us know if this is your experience, and if this blueprint has helped your organisation.

Terry Espiner - UK Health Sector Manager

Contents

1. Introduction.....	4
1.1 ICT as the Service Delivery Platform for the Modern NHS	4
1.2 The Scope and Purpose of the Blueprint	4
2. An Architectural Approach to Establish ICT Relevance	6
2.1 Architectural Frameworks	6
2.2 Conceptual Architecture for NHS Organisations	6
2.3 Description of the Conceptual Architecture	6
2.4 User and Service Context	8
2.5 Logical Architectures: Building the Service Delivery Platform	9
3. Borderless Networks	10
3.1 The Transport Layer	10
3.1.1 Campus environments	10
3.1.2 Distributed Care Environments.....	13
3.1.3 Unified Intelligent Network Services	16
3.2 Information Security	17
3.2.1 Cisco Borderless Security	17
3.2.2 Foundation Network Security	18
3.2.3 Perimeter Threat Defence	19
3.2.4 Content and Email Security	19
3.2.5 Secure Network Overlays.....	20
3.2.6 Secure Mobile Working	20
3.3 Borderless Mobility	21
3.3.1 Centralised Wireless LAN	22
3.3.2 Context Aware Location Services.....	23
3.3.3 Voice over Wireless LAN	23
3.3.4 Secure Wireless LAN	24
3.3.5 Guest Access Solutions.....	24
3.3.6 Spectrum Intelligence	25
3.3.7 Unified User, Access and Identity Management.....	26
3.4 Video and Content Delivery.....	26
3.4.1 Cisco Medianet.....	26
3.4.2 Medianet Features.....	27
3.5 Sustainability and Energy Management.....	28
3.5.1 ICT as an Energy Consumer	28
3.5.2 Saving Time, Cost and Carbon.....	28
3.5.3 Managing Power with Cisco Energywise	28
3.6 Network and Service Management	29
3.6.1 Service and Network Management Solutions.....	30
4. Data Centre Virtualisation.....	31
4.1 Logical Architecture for Data Centre Virtualisation.....	32
4.2 Data Centre Unified Fabric.....	32
4.2.1 Virtual Machine Mobility and Management.....	35
4.3 Unified Computing	37
4.4 Unified Network Services	39
4.5 Desktop Virtualisation Solutions	40

4.6 Disaster Recovery and Business Continuance	41
5. Collaboration.....	43
5.1 Unified Communications Essentials	44
5.2 Call Control.....	45
5.3 Real-Time Video Services	46
5.4 Collaboration Services	47
5.5 Presence and Instant Messaging	47
5.6 Messaging	48
5.7 Mobility	48
5.8 Attendant Services	48
5.9 Patient & Customer Contact.....	48
5.10 'Consumerisation'	49
5.11 Social Software.....	49
5.12 N3 Voice and Video Services	50
6. Integrating Patient-Centric Information.....	51
7. Approaches to Shared Services	52
7.1 What are Shared Services ?.....	52
7.2 Current and Future Developments	52
8. ICT at the Heart of NHS Reform.....	53
Appendix A - Contacts	54

Important Notice

"The guidance provided in this report 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 Healthcare organisations up to the date of publication. Errors and omissions are excepted. No warranty is given or implied."

1. Introduction

1.1 ICT as the Service Delivery Platform for the Modern NHS

The challenges in the modern NHS are numerous. They include addressing the Coalition Government's reform and reconfiguration plans, meeting increasing demand and improving the patient centric care that the service offers. These are all set against a backdrop of austerity measures and the consequent need to drive operational excellence and efficiency throughout every NHS organisation.

Addressing any one of these challenges is a broad and complex undertaking, taking them all together determines the need for a different approach, one that looks at solutions that can support more than one area on its own. Cisco believes that strategic investment in ICT solutions can do just this, adopting a strategy of building once and encouraging re-use optimises resources and maximises effectiveness.

ICT deployed strategically is an enabler. It has the potential to allow organisations to collaborate – internally and externally; to connect people regardless of geography; and to facilitate new ways of working that drive efficiencies and operational excellence. Hence, a business-led approach to ICT investment can realise tangible value, addressing the challenges outlined above and creating the Service Delivery Platform for the modern NHS.

1.2 The Scope and Purpose of the Blueprint

The intention of this blueprint is to offer insight in to how ICT can indeed play its part in delivering greater productivity whilst also offering new channels of care. It advocates that ICT transitions to be seen as an asset to the business rather than an operational cost centre. In this way ICT becomes an enabler that is an integral and underpinning part of NHS business as shown in Figure 1.1.

The blueprint consists of two documents as follows:

Volume 1: Business Requirements (the companion document)

- Questions how ICT can become an enabler of change;
- Looks at the global trends in healthcare and the UK and how a strategic approach is needed to meet ever rising demand;
- Considers the UK healthcare priorities and maps ICT solutions to bring tangible value.

Volume 2: Technical Requirements (this document)

- Advocates the architectural approach and introduces a conceptual reference model that establishes the link between business and clinical priorities with the ICT environment;
- Introduces logical architectures or 'solution sets' and shows how they help to address the business and clinical priorities;
- Provides reference technical architectures that may be used by NHS ICT departments as a template for design in their own organisations.

At its heart the blueprint establishes direct linkage between the business and clinical priorities of the NHS and the technology environment. The establishment of a secure, robust and functional foundation can become a platform for innovation.

With productivity, re-configuration and improved patient outcomes as the key drivers, the blueprint demonstrates that there has never been a more opportune time to re-think strategies, placing ICT at the heart of the business of the NHS – creating truly Connected Health.

Note - this document focuses on infrastructure inside autonomous NHS organisations. The scope does not extend to shared services networks (though some coverage is offered) or national infrastructure.

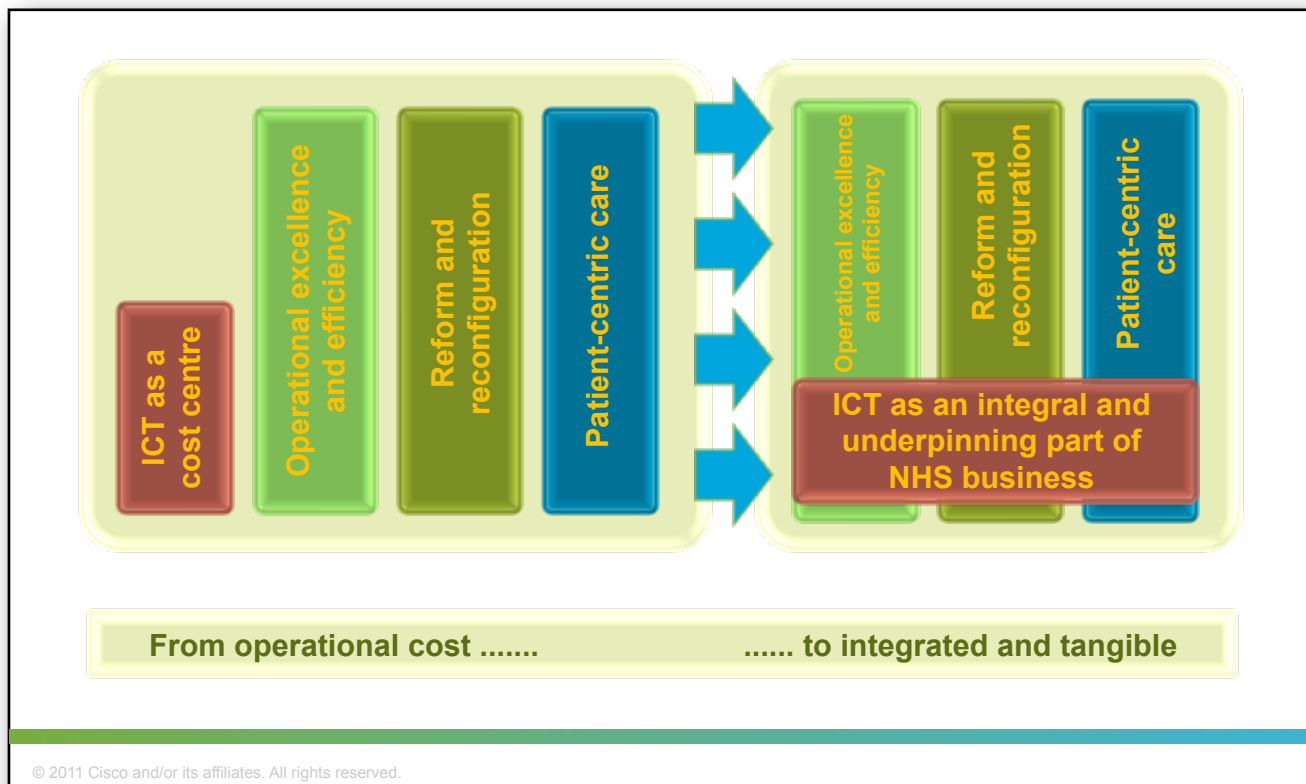


Figure 1.1 - ICT: no longer a cost centre

2 An Architectural Approach to Establish ICT Relevance

ICT at the Heart of NHS Reform

2. An Architectural Approach to Establish ICT Relevance

Part one of this blueprint has highlighted the business and clinical drivers that exist for NHS organisations, as well as identifying key areas where ICT based solutions can deliver efficiencies, costs savings and improved patient outcomes.

This section outlines a methodology to demonstrate the relationship between successful business outcomes and ICT investment. Adopting an architectural approach within an NHS organisation's ICT strategy offers an industry proven and accepted approach.

2.1 Architectural Frameworks

There are a number of Enterprise Architecture frameworks in use today, two examples being TOGAF¹ and Zachman², and whilst they differ to some degree, all contain a structured approach that can help transform ICT from a cost centre into a strategic business asset. In this document Cisco has attempted to use the principles of these frameworks to summarise how business requirements are linked to ICT investment in a healthcare environment, specifically for NHS organisations to follow.

The principle output clearly illustrates the dependencies that exist. The selection of products and solutions in the ICT environment has a direct consequence on the services that are available. This, in turn has a bearing on what capabilities are available in order to support applications, and as a result the business objectives.

This document discusses three architectural stages:

1. **Conceptual Architecture** – based on a set of contextual information, it offers a representation of an overall programme of work to implement the architecture including dependencies, with the prospect of prioritising individual projects to meet local business needs. It also provides a graphical representation of the available set of technology components and shows their inter-relation.
2. **Logical Architecture** – typically a set of end user solutions that respond to business need. These may be clustered around a particular ICT theme or business requirement. In this document Cisco focuses on Borderless Networks, Collaboration and Data Centre Virtualisation.
3. **Technical Architectures** – directly derived from the identified business requirements, a series of reference designs that support ICT in the delivery of the strategy.

2.2 Conceptual Architecture for NHS Organisations

Cisco is introducing the use of a 'conceptual architecture' to define the overall set of technologies that may be deployed within an NHS organisation and demonstrating the relationship to business priorities.

A conceptual architecture can be used to gain agreement between internal authority stakeholders such as an Executive Board and to inform external stakeholders such as vendors and service providers. It can ensure that all parties are fully briefed and in agreement on the programme to be executed, secure in the knowledge that ICT investment is tightly aligned to the aims of the business.

2.3 Description of the Conceptual Architecture

The conceptual architecture proposed in this Blueprint adopts the principles of Enterprise Architecture frameworks and comprises four functional technology layers and a fifth layer that can be used to define the user or service context. Figure 2.1 shows a layered technical model with marked similarities to the Technical Reference Model (TRM) referenced in the TOGAF specification. Each of the four functional layers offers a variety of services.

¹ TOGAF – <http://www.opengroup.org/togaf/>

² Zachman – <http://www.zachman.com/>

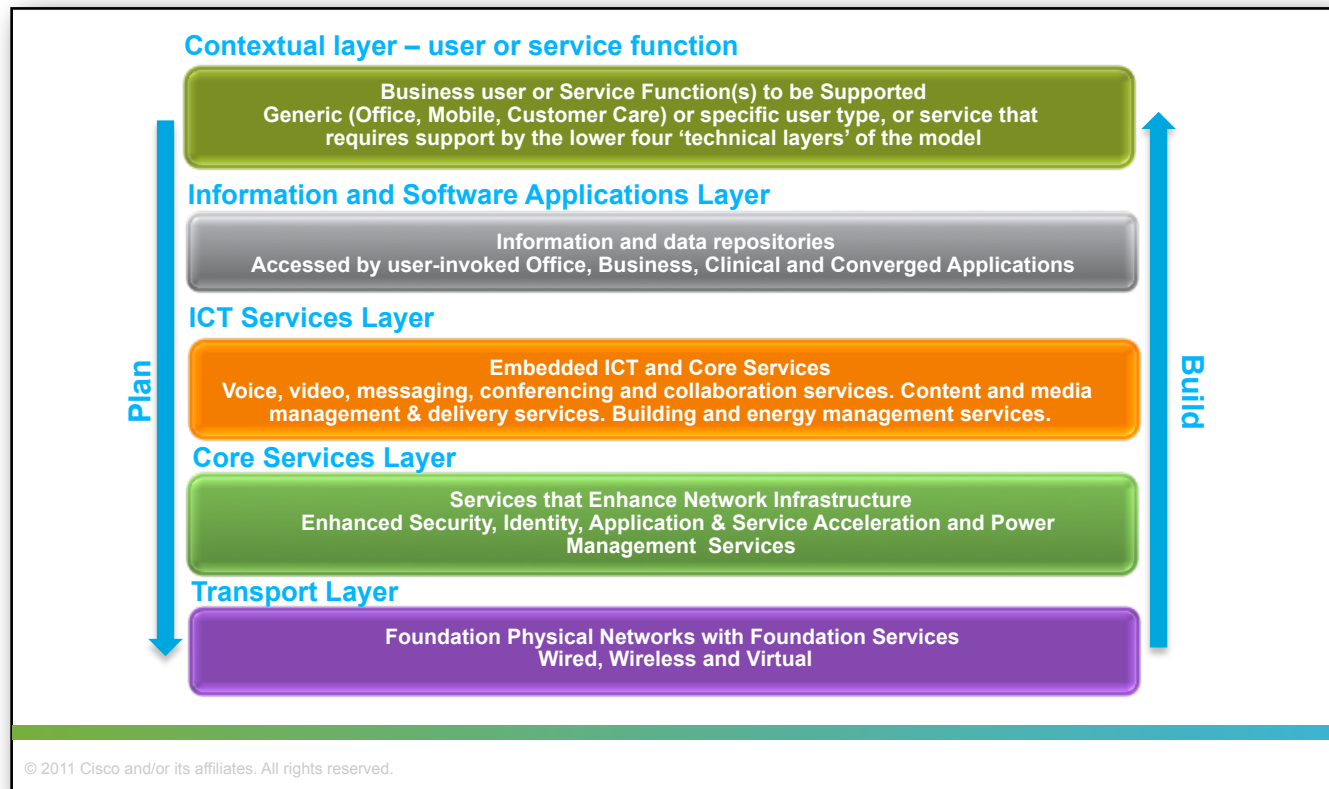


Figure 2.1 - Technical Reference Model Layers

The TRM allows users to quickly identify the dependencies in delivering any ICT strategy and Cisco recommends the 'Plan Down, Build Up' approach. With reference to the model in Figure 2.1 that means planning from the top downwards and then building in the upwards direction, hence establishing a robust functional platform, analogous to the foundations of a house. The key layers are as follows:

- **The Transport Layer** providing the underlying wired and wireless IP infrastructure along with the key network services, such as security and Quality of Service (QoS), to create a converged IP infrastructure;
- **The Core Services Layer** providing intelligent network services, such as enhanced security or application acceleration, that are incremental to the transport layer, and deliver increased user functionality, increased performance or enhanced security to the network;
- **The ICT Services Layer** incorporates embedded applications or service functions that reside within the network and support end-user functions, for example call control or building management services;
- **The Information and Software Applications Layer** provides the end-user business and clinical applications that are directly available to users and considers the links to information repositories;
- **The User or Service Contextual Layer** that permits the architecture to represent the needs of a particular user or service.

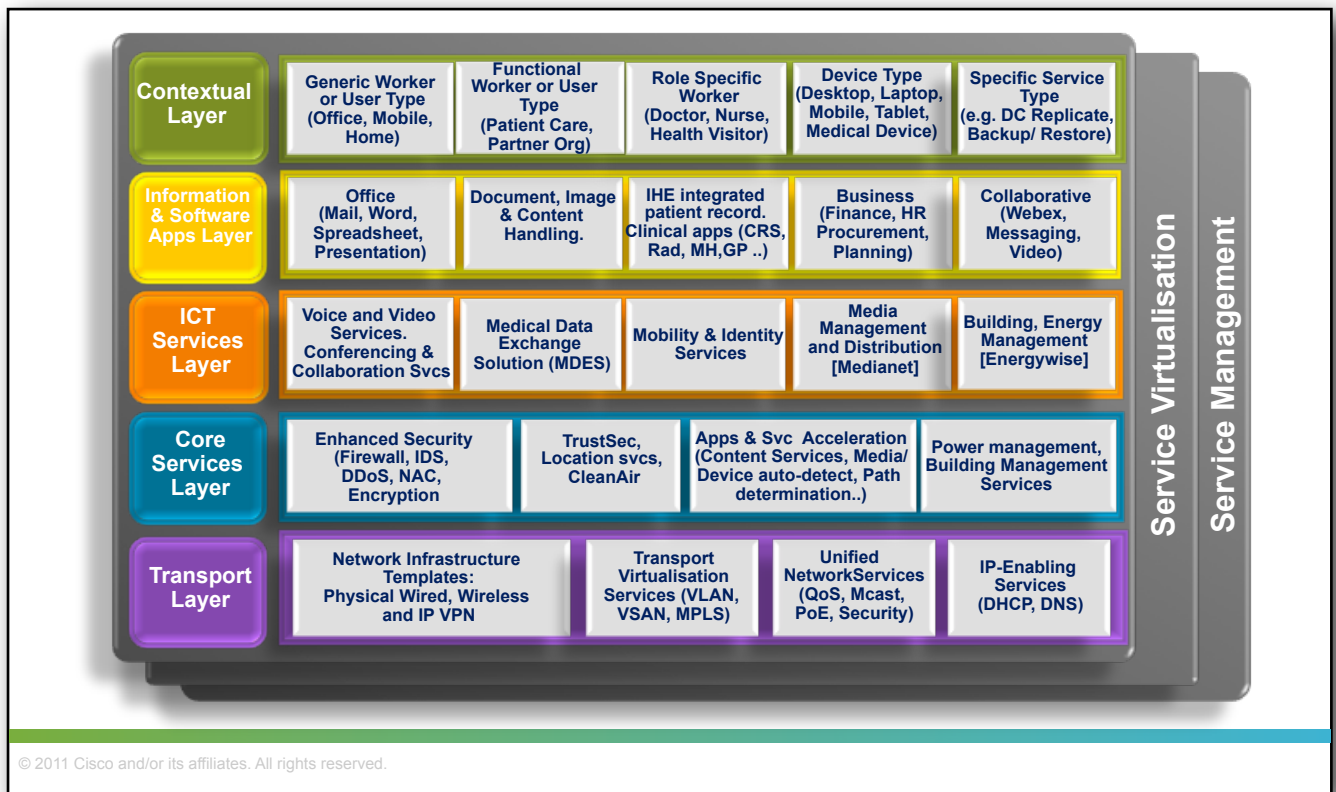


Figure 2.2 - the TRM Functional Layers in Detail

Each of the lower four layers can be populated with Cisco or generic products, applications and services. Figure 2.2 shows the technical reference model populated with Cisco network, service and application offerings; however NHS organisations are encouraged to adapt the framework to suit their own environment.

While information is regarded as a separate but linked strategy, its inclusion in the model is intentional. As we have discussed earlier, the availability of integrated patient-centric information underpins many of the aims of current NHS strategy. Cisco supports a global standards based approach known as Integrating the Healthcare Enterprise (IHE)³ that offers such a platform (see section 6).

2.4 User and Service Context

As described earlier, the Conceptual Architecture can be used to represent overall capability or to focus in on particular user or functional needs. The User and Service Context Layer is particularly powerful as it allows a representation to be made of what technology will be required to service a particular need. It is also worth noting that one of the advantage

approach is that personalising the TRM to any one organisation will determine if the services required are already available as re-usable building blocks. If so, no further investment is required.

The TRM may be used to model any user role or service context, it may also be applied to service functions that derive requirements of the underlying infrastructure, for example, a replication service in the Data Centre or an IP based surveillance system. Where these services are automated they demand intelligent services which must be supported. Cisco encourages the use of the TRM in this way to enhance the work of individual projects and to determine the demands on the underlying infrastructure, hence supporting effective implementations.

³ Integrating the Healthcare Enterprise - <http://www.ihe.net>

2.5 Logical Architectures: Building the Service Delivery Platform

The conceptual model reinforces the linkage between ICT and the aims and challenges of the business. Moving forward towards implementation, we must now consider how ICT based solutions can be used to realise success at the business layers. The next step therefore, is to categorise such solutions so that they respond directly to the business issues described earlier.

Cisco categorises its solutions into three logical architectures – Figure 2.3 demonstrates their relationship to each other.

Borderless Networks is the underpinning, feature-rich platform; the Data Centre must be efficient, high performing and flexible; while the Collaboration architecture offers the tools that enable new ways of working. Together they respond to the NHS priorities of operational excellence, reform and reconfiguration and patient centric care.

In sections 3, 4 and 5, we explore each of these three areas including the solutions contained therein, and their relevance to a healthcare environment.

In addition, we introduce a series of technical architecture diagrams that NHS organisations may find informative or even use as templates for their own solution deployments. The structure is intentional, firstly establishing the robust, secure and feature-rich platform; implementing the high-performing and efficient Data Centre; and ultimately delivering the applications that support business and service transformation.

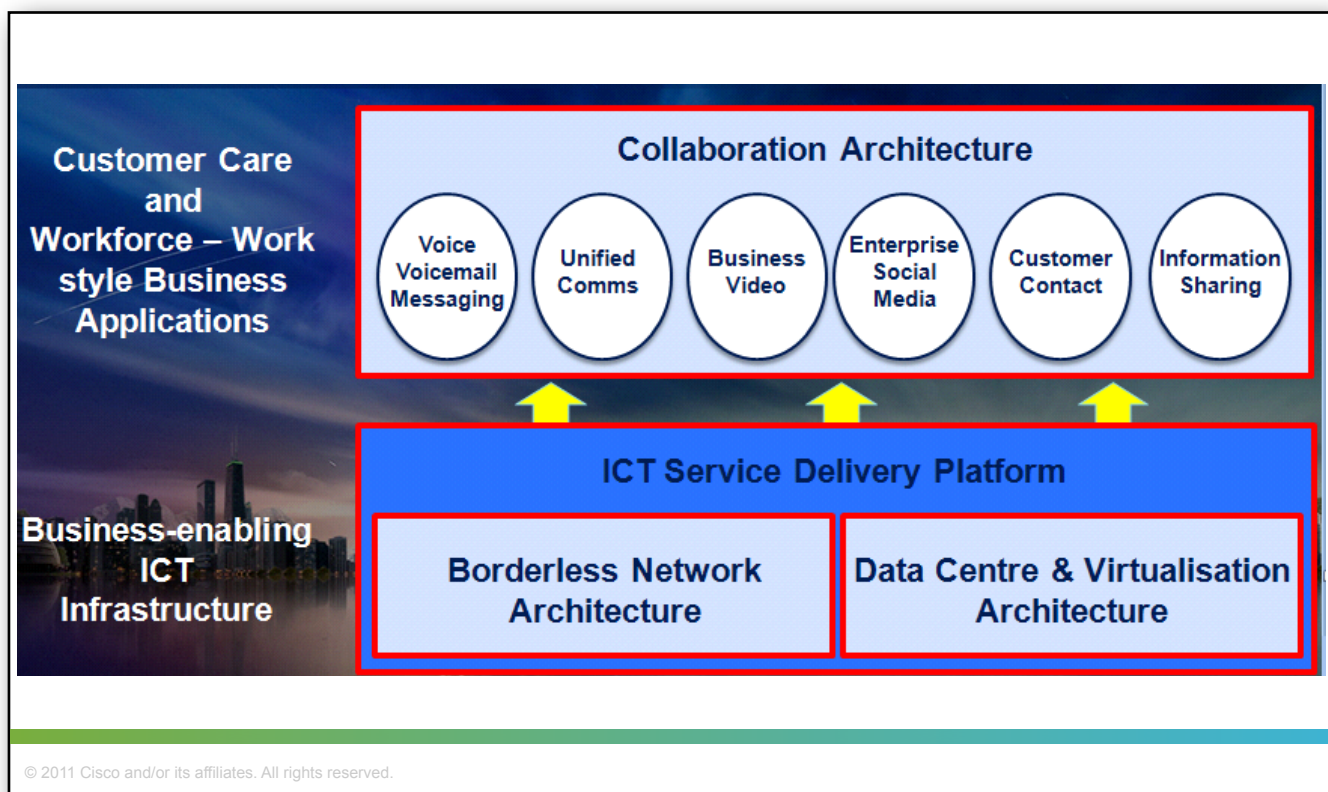


Figure 2.3 - Cisco's Logical Architectures

3. Borderless Networks ⁴

Borderless Networks is a term used to describe secure infrastructure without boundaries. In NHS terms, an example could be a care worker being able to securely access information from any device, anywhere and at any time. The borderless concept includes the infrastructure components themselves, such as routers, switches, wireless and security products, and their associated capabilities.

When considering the 'Plan Down, Build Up' concept described earlier, Borderless Networks is concerned with creating the robust, secure and functional platform, upon which everything in the upper layers of the TRM depends. Hence, correct definition and deployment of the underpinning borderless infrastructure is critical in order to mitigate the risk of failure of business projects that are dependent on ICT.

3.1 The Transport Layer

Any ICT infrastructure strategy must begin with the transport layer. It can be considered as analogous to the roads in a public transport system: we use cars, lorries and buses as applications that are wholly dependent on the platform of roads and intelligent infrastructure such as traffic lights and prioritisation lanes.

The transport layer provides the foundation of all connectivity, and as more applications in the form of data, voice, collaboration and video are placed on infrastructure, its operation becomes increasingly critical in a healthcare environment. Given these dependencies and the ubiquitous nature of the infrastructure, care needs to be taken to ensure that it is appropriately designed and configured.

It is therefore clear that the transport layer should be designed with all current and future priorities in mind, such that it can be designed and built once for re-use for as long as is reasonably foreseeable. The transport layer template should be:

- Flexible: to effectively support a wide range of services and devices;
- Resilient: removing single points of failure and ensuring high availability;
- Adaptable: allowing for inevitable changes in the investment lifetime;

- Secure: providing appropriate data confidentiality, integrity and availability – meeting governance standards;
- Feature rich: where appropriate to support prioritisation and sensitive media;
- Cost effectiveness: measuring value rather than basic price.

Cisco has issued a significant amount of guidance regarding foundation deployments, however this document considers reference templates for two types of NHS organisation:

- A campus environment (e.g. Acute Trust);
- A distributed care environment (e.g. Primary Care or Mental Health).

It is important to note that the templates are not prescriptive, nor are they expected to fit any specific organisation – in fact many organisations are likely to use aspects of both. The intention is to offer an insight into best practice and typical deployment and as a result the principles may be used in other types of NHS organisation, e.g. Ambulance Trusts and Arms Length Bodies. It should also be noted that this section focuses on organisational infrastructure, i.e. for single or merged organisations. Shared Services leading to Cloud-based infrastructure is considered in section 7.

3.1.1 Campus environments

Cisco recommends a three-layer design (core, distribution and access) to support the foundation of campus care environments – including NHS Acute Trusts. In some cases it is possible to collapse the core and distribution layers and this is often seen as an acceptable design for many NHS organisations. Throughout the hierarchical design, intelligent services are provided that support the applications which in turn, support the business. This approach provides the performance, scalability, resilience and flexibility to meet NHS business requirements as they evolve.

The Core Layer provides the critical task of interconnecting all the distribution switches and providing reliable connectivity to the required services, be that a local Data Centre or to remote services using external shared networks or N3.

⁴ Cisco Borderless Networks – <http://www.cisco.com/en/US/netso/ns1015/index.html>

For flexibility and scalability the core is usually based on a minimum of two high performance chassis-based switches with co-location avoided where possible for optimum resilience. This minimises the risk of simultaneous failure due to issues in the operational environment, such as power and cooling. Today's core switches generally support up to 10Gb interfaces with resilient links configured between them.

To offer enhanced performance, resilience and simplified management, Cisco's Virtual Switching System (VSS)⁵ treats the cores switches as one virtualised switch for configuration and management. Alternatively, with Cisco's Virtual Port Channel (VPC)⁶ capability, each switch physical switch is configured independently but delivers similar benefits (see section 3.1.3).

These capabilities are rapidly becoming the norm within the NHS.

LAN core switches will often be co-located with other switches dedicated to tasks such as Data Centre distribution. In such circumstances it may be possible to combine both these functions in a single layer. Virtual Device Context (VDC) technology within the Nexus range of switching platforms (see section 4.2.2) allows a single switch to be logically segmented into multiple independent devices – each with its own configuration.

The Distribution Layer aggregates nodes from the access layer, protecting the core from high-density peering. Additionally, the distribution layer creates a fault boundary providing a logical isolation point in the event of a failure originating in the access layer.

Depending on the number of ports required the distribution layer is usually populated by pairs of small chassis-based switches or standalone fibre switches that are capable of layer 3 forwarding. (As noted earlier the distribution layer is often collapsed into the core layer). High availability in the distribution layer is provided through dual equal-cost paths to the core and access layers resulting in fast, deterministic convergence in the event of a link or node failure.

Co-location should again be avoided where possible, and the use of diverse fibre paths encouraged, mitigating failures in the operational environment.

The Access Layer is the first point of entry on to the network for end-stations of various types and should be connected to two separate distribution switches. Today's intelligent edge switches are able to sense the end-station connected to it and apply policy for the discovered device type. This improves service reliability by ensuring that the Quality of Service (QoS) policy "follows the device" rather than needing to be manually reconfigured every time it is moved. For example, when an IP Phone is connected to a switch-port the appropriate policy is deployed and the phone is assigned to the voice network. Should the IP Phone be replaced by a desktop PC, policy is changed automatically and access granted to the appropriate data network. It is also possible to assign policy based on user credentials.

Access layer switches can take the form of a chassis or enterprise grade stacking solution treated as a single entity, simplifying network administration and improving resilience. Stacking is often considered to offer a more flexible solution and consumes the minimum of cabinet space, often a practical issue in an NHS environment. Increasing bandwidth demands are encouraging the migration towards gigabit speeds at the desktop. Hence, in high performance areas such as Radiology it is not unusual to see a requirement for 10Gb connectivity to the distribution layer. Even with this increase in bandwidth there is still a risk of congestion over the access layer links and end-to-end QoS must be deployed to ensure real time services have priority during times of congestion. Other trends in the access layer include:

- Universal provision of Power over Ethernet (PoE);
- General provision of triple speed links to the desktop (to 1Gb);
- Increasing use of 10Gb uplinks;
- Focus on security due to increasing staff mobility;
- Increasing preference for stacking rather than chassis solutions;
- Endpoint power management.

Simple access layer deployment can be based on layer 2 devices, however layer 3 offers the benefits of faster convergence times, smaller fault domains, and advanced borderless network services for content delivery and security.

⁵ Virtual Switching System – <http://www.cisco.com/go/vss>

⁶ Virtual Port Channel – http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/white_paper_c11-516396.html

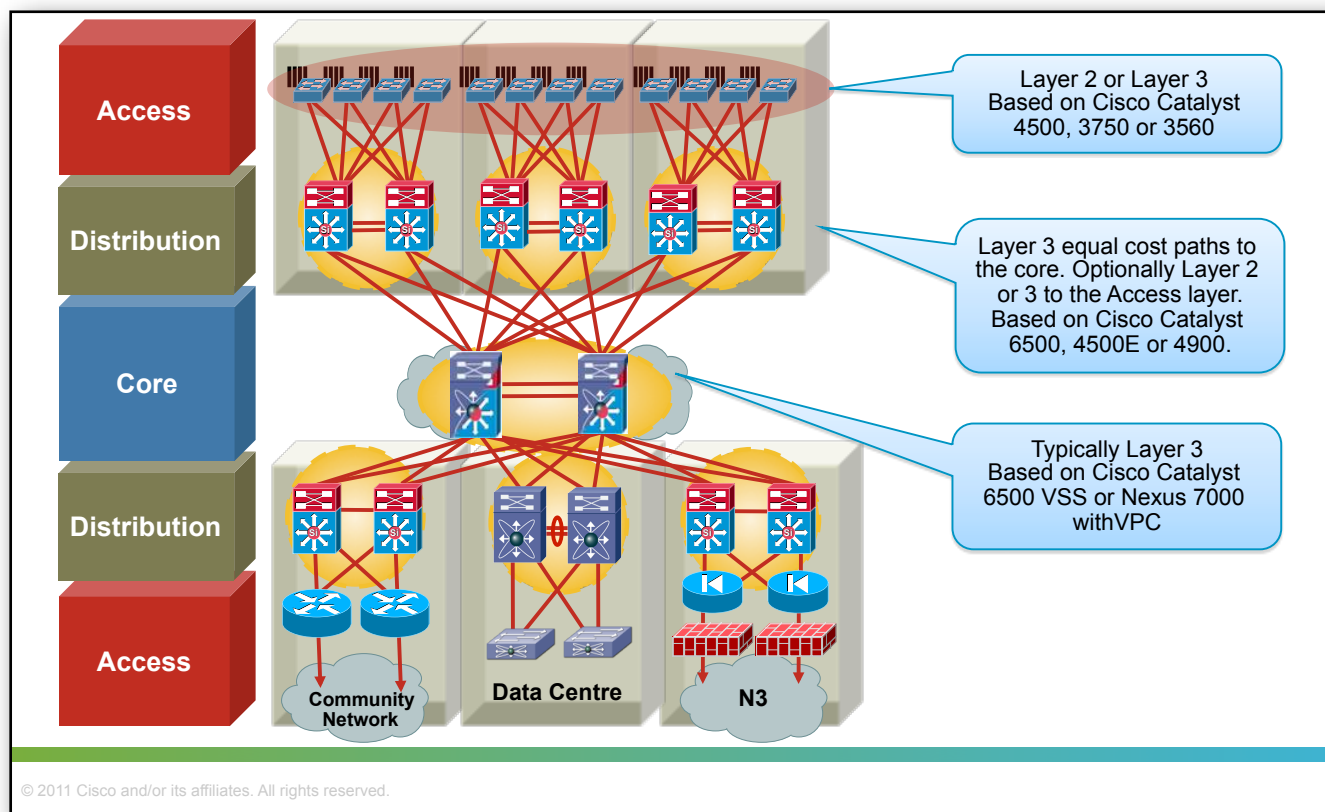


Figure 3.1.1 - Large Acute Hospital (Campus)

Figure 3.1.1 shows the hierarchical model and typical deployment for a large campus such as an Acute hospital. It clearly illustrates a scalable building block approach featuring the core, distribution and access layers. This reference design includes Catalyst⁷ and/or Nexus switching products and comprises:

- A Layer 3, multi-Gigabit (optionally 10 Gigabit) Ethernet Core layer;
- A Distribution layer connected by aggregated and resilient multi-Gigabit (typically 10 Gigabit) links, with multi-layer switching and Layer 3 policy control;
- An Access layer featuring 10/100/1000 BaseT Ethernet to the desktop, with an option for power over Ethernet for IP phones and Wireless LAN access points.

Collapsed Core designs – the hierarchical three layer model is preferred, however it may be possible to reduce the number of switches deployed in order to optimise the deployment. In smaller campuses, the core and distribution layers can be collapsed to form a single layer preserving functionality but reducing the scale of the design as shown in figure 3.1.2.

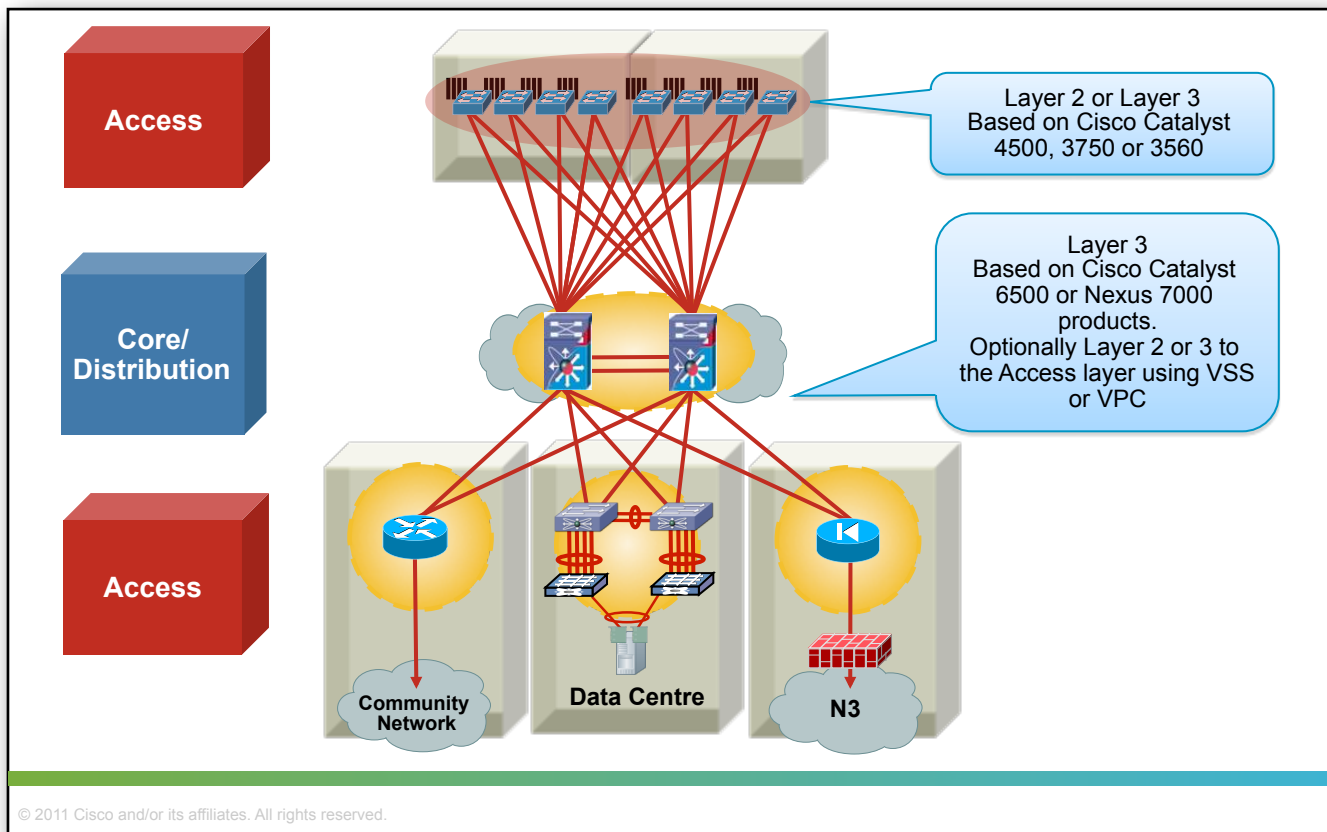


Figure 3.1.2 - Small/Medium Acute Hospital (Campus)

3.1.2 Distributed Care Environments

Whilst the campus designs previously discussed provide an insight to how an individual site should be configured, in practice healthcare organisations span multiple locations. To ensure efficient operation all sites must be interconnected with a consistent policy. Whilst the campus and distributed designs share the same goals, i.e. to provide flexible, resilient, secure and adaptable connectivity, there are clear technical and commercial differences. Considerations include geography, available service provision, cost, network services required and expected utilisation to provide an accurate assessment of individual case needs.

This section covers three principle designs which fit NHS requirements and are in use today. It is important to note these are for reference only and that it is quite likely to see a combination of services used to deliver connectivity across a single, but distributed organisation.

Dynamic Multipoint Virtual Private Network (DMVPN)[®]

is a Cisco IOS Software based dynamic hub and spoke solution for building large scale Virtual Private Networks (VPNs). The solution is growing in popularity and already widely deployed in the NHS today. Traditional VPN technology relies upon statically configured tunnels between devices, typically in a hub-and-spoke configuration. This approach is perfectly adequate for small-scale solutions but if there is a need for spoke-to-spoke communication, all traffic in this topology has to flow through the hub causing increased load and latency.

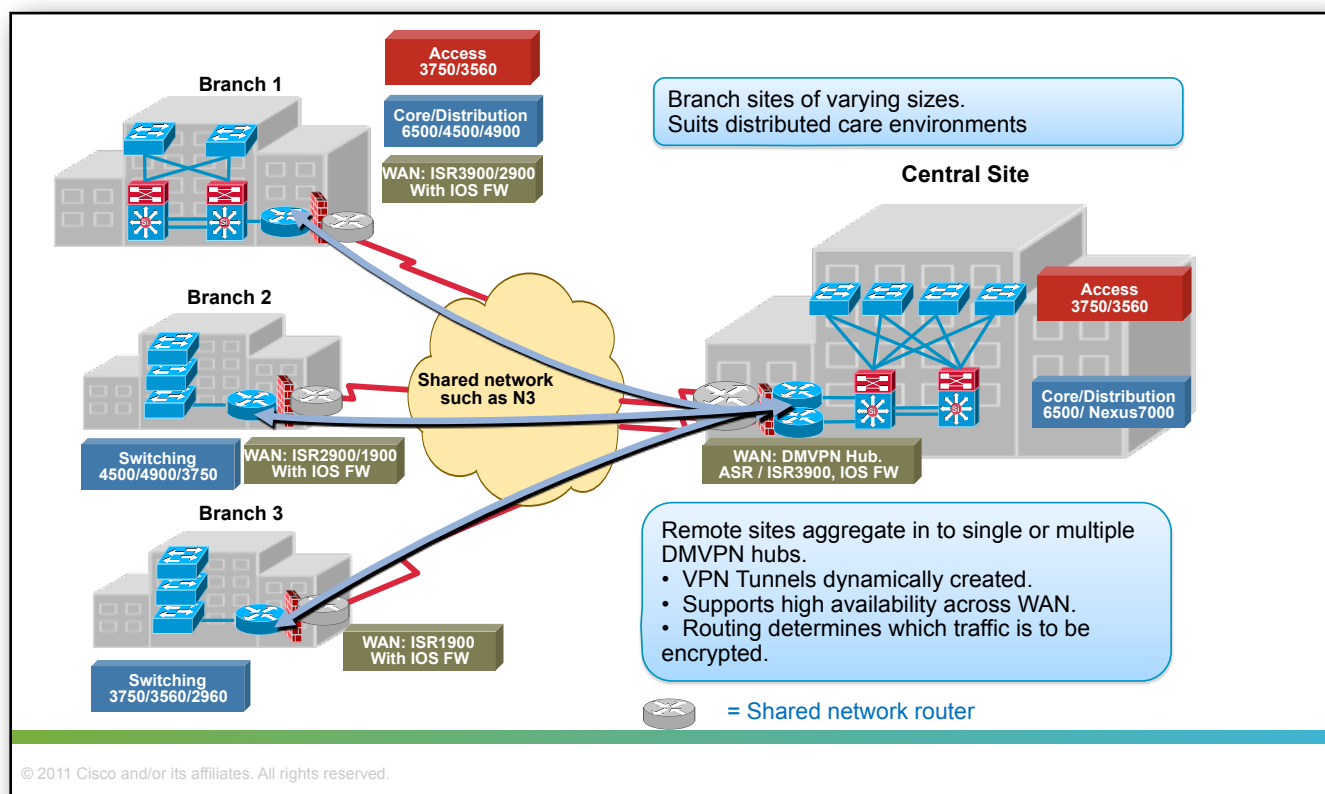


Figure 3.1.3 - DMVPN over N3

DMVPN is based on standard IP Security (IPsec) protocols but combines them with the multipoint Generic Routing Encapsulation (mGRE) protocol to deliver simple, scalable any-to-any VPN solution. Using DMVPN, Cisco routers have the ability to set up secure tunnels automatically. This combines the benefit of a fully meshed network (direct site-to-site connectivity), without the complexity and overhead of managing all of the required tunnels in a traditional IPsec configuration. For example, when traffic is sent to a remote site, it triggers the generation of an IPsec tunnel which is maintained for the duration of the traffic flow. When no further traffic passes the tunnel it is torn down, preserving resources and retaining configuration simplicity. Figure 3.1.3 shows a reference architecture using DMVPN over N3 suitable for distributed healthcare environments.

Group Encrypted Transport VPN (GET-VPN)[®] is VPN technology that delivers any-to-any communications without the need to define any tunnel endpoints. GET-VPN increases the scalability of a fully meshed solution and uses a central provisioning server to simplify deployment and management.

Site-to-Site IPsec VPN - When used alone, IPsec provides a private, resilient network for IP unicast traffic. It remains a valid solution today but lacks some of the advantages of DMVPN described above, e.g. scalability and ease of deployment. IPsec VPN is often combined with the Generic Routing Encapsulation (GRE) protocol allowing IP multicast and non-IP traffic to traverse the IPsec tunnel. This method supports dynamic routing protocols that depend on IP Multicast.

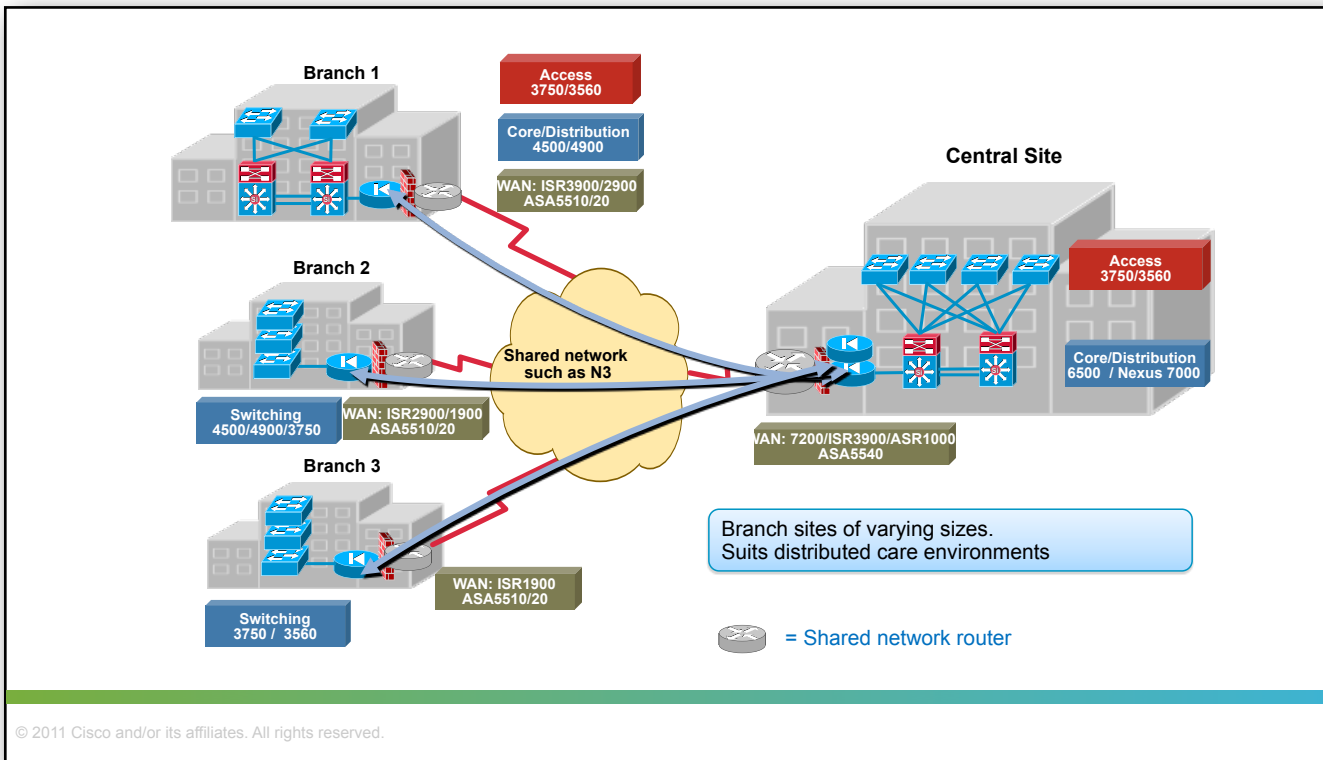


Figure 3.1.4 - Site-to-Site IPsec over N3

Figure 3.1.4 shows an example of a site-to-site IPsec VPN over N3. Routers are used to build point-to-point IPsec tunnels between sites – traffic which needs to access other sites can utilise these secure tunnels. Tunnels are only produced between known devices (mutual authentication) and user traffic within the tunnels can be encrypted to ensure security. Site-to-site QoS can be preserved even within IPsec tunnels by marking the tunnel according to the payload it is carrying. This allows for different QoS markings within sites, and between sites, though it is good practice to impose a consistent policy end-to-end to simplify configuration and avoid mismatches.

Many factors affect scalability of an IPsec VPN design, including access connection speeds, routing peer limits, encryption engine throughput, and tunnel termination. Scaling large IPsec VPN while maintaining performance and high availability can be challenging, and requires careful planning and design – often addressed by using DMVPN as described earlier.

Network Extension – Today's trends of 'consumerisation' and flexible working have dictated the need for borderless networks. The desire to access information from anywhere, at any time and with any device has created a paradigm shift in remote

networking where the network follows the user. Whilst having many advantages including aspects of mobility, the burden of securing remote devices is increasing.

Whilst there are very particular security requirements, e.g. accessing 'Person Identifiable Data (PID)', the NHS faces the same challenges. The drive for flexible working dictates the need to extend the secure NHS network to multiple locations. Examples include a clinician working from home to provide advice "out of hours", or perhaps a mobile health worker using a tablet device to access and update records remotely. Access can be provided by either mobile networks or even consented use of domestic broadband connections, particularly for community support workers on regular home visits.

There are many remote worker solutions available today, including those offered by N3. Cisco recommends that organisations consult the latest NHS guidance with respect to these connections, particularly as it relates to information governance. We would also be happy to advise on any specific customer requirements.

3.1.3 Unified Intelligent Network Services

Increasing business dependence on infrastructure dictates that a borderless network design must be flexible, resilient, adaptable, secure and feature-rich to support the plethora of devices and access methods used. Service requirements are only briefly discussed in this section and if more information is required, Cisco would be happy to advise on any or all of these areas

Deterministic Behaviour: Any network infrastructure must be deterministic in nature such that faults are easily diagnosed and that the infrastructure itself can respond effectively. Here, we introduce some popular features.

In the campus environment features such as Multichassis Etherchannel (MEC) or cross-stack Etherchannel allow bundling of links across platforms improving resilience and supporting sub-second failover. This solution also uses all the available links maximising capacity.

The Spanning Tree Protocol (STP) has undergone many enhancements over the years in order to improve re-convergence times in the network in the event of failure. However, the STP environment must be well understood and controlled to achieve deterministic behaviour and simple errors like adding a switch with an old configuration can cause a perpetual re-calculation of the spanning-tree algorithm, resulting in significant and widespread network downtime. Employing a layer 3 design today means convergence can be faster, more predictable, bounded and reliably tuned. As a result it is often possible to avoid using STP across the core of the network, hence mitigating some of the associated challenges.

As described previously, Cisco's VSS and VPC are features on the high end Cisco platforms that offer enhanced performance, resilience and simplified management:

- Both are based on a port-channelling concept extending link aggregation to two separate physical switches;
- Both allow the creation of resilient layer 2 topologies based on link aggregation;
- They eliminate dependence on Spanning Tree Protocol in the access-distribution layer;

- Offers advantages such as a single gateway IP address; full first hop redundancy; simplified configuration and eliminates the need for gateway redundancy protocols such as Virtual Router Redundancy Protocol (VRRP), Hot Standby Routing Protocol (HSRP) and their associated overhead.

Resilience in a distributed care environment can be more complex and expensive. The capabilities of the router devices themselves offers flexibility in the choice of Wide Area Network (WAN) technologies and different solutions can be provided. Multiple links can be provisioned from a given site and these can be used on a load sharing basis or as a main and standby link. The standby links maybe of lower bandwidth than the main with only key services supported in the event of failure. These multiple links can be terminated on a single router device, or on multiple devices to protect against both hardware and link failure.

Quality of Service (QoS): A detailed analysis of QoS requirements is outside of the scope of this document, however it should be considered as critical in defining deterministic infrastructure.

In general, QoS is needed whenever the best-effort network service does not meet the availability or transmission quality needs of user applications. NHS network administrators should be aware of all application requirements in respect of their demands on the local infrastructure. As a result a QoS schema can be created and maintained on an organisational basis and regularly reviewed as new applications are introduced. QoS has emerged as a critical foundation service as latency sensitive applications have become more prevalent having a major impact on the ability of networks to provide predictable, measurable and guaranteed service. Of particular concern is voice, interactive video or any other application with particular sensitivity to loss, delay and jitter.

Beyond QoS, other services are needed in the network to support the many different types of video communication. Networked video has soared in popularity and a common mistake is to treat all video as the same. In fact there are many different types of video such as streaming or live content, video on demand, push video and interactive video. Each of these places its own demands on the network and should be planned for accordingly. Cisco's architecture for networked video services, Medianet, is covered in section 3.4.

Identification and Posturing: A prerequisite of QoS and Medianet is the ability to identify devices and/or users at the network edge. This allows the network to provide the appropriate network policies dynamically without the need for manual reconfiguration. The ability to identify end devices also assists with security. For example, an IP phone needs to contact other telephony endpoints and a telephony server and only with specific protocols, whereas a desktop PC may need to contact a range of servers using many communications protocols. Attributes may also be assigned based on user credentials – especially important in public buildings such as hospitals.

It is also possible to assess the “posture” of a device and decide if it should be given access, and if so, what level of access. For example a device that is compliant with the organisation’s security policy may be given full or appropriate access, while a device that does not conform may only be granted access to a remediation server, or indeed denied access completely.

Power Provision: The network can also be used to power network devices using Power over Ethernet (PoE). This has the benefit of reducing the need for power cabling as well as giving greater control of power consumption of attached devices. A modern Cisco edge switch can report power consumption to a management application and if required control the power delivered and to even power down unused devices out of hours where it is appropriate to do so. Cisco has developed an open ecosystem approach known as Energywise that can be extended to non PoE devices such as PCs, and even to building management systems should this be appropriate. Further details on Energywise can be found in section 3.5.3.

3.2 Information Security¹⁰

Current NHS reforms, re-configuration of services and closer links with, for instance, Social Care have resulted in some significant challenges in ensuring that information governance objectives can be met, including:

- ‘Consumerisation’: personal devices such as smartphones and tablets;
- Greater demand for multi-agency working driving collaboration with internal and external parties;
- An increasingly location-independent workforce;
- Change in focus of attackers, from direct to indirect e.g. compromise trusted web server to silently inject malware over a trusted connection;
- Further erosion of the network perimeter due to greater levels of inter-departmental collaboration.

Despite these challenges, NHS organisations must continue to provide not only a high degree of information privacy but also maintain 24 x 7 operations for a service that is critical to the successful delivery of patient care.

3.2.1 Cisco Borderless Security

Over the past few years, Cisco has responded to the growing security challenges posed by the new dynamics described above through the introduction of Secure Borderless Networks.

¹⁰ Cisco Borderless Security – <http://www.cisco.com/go/security>

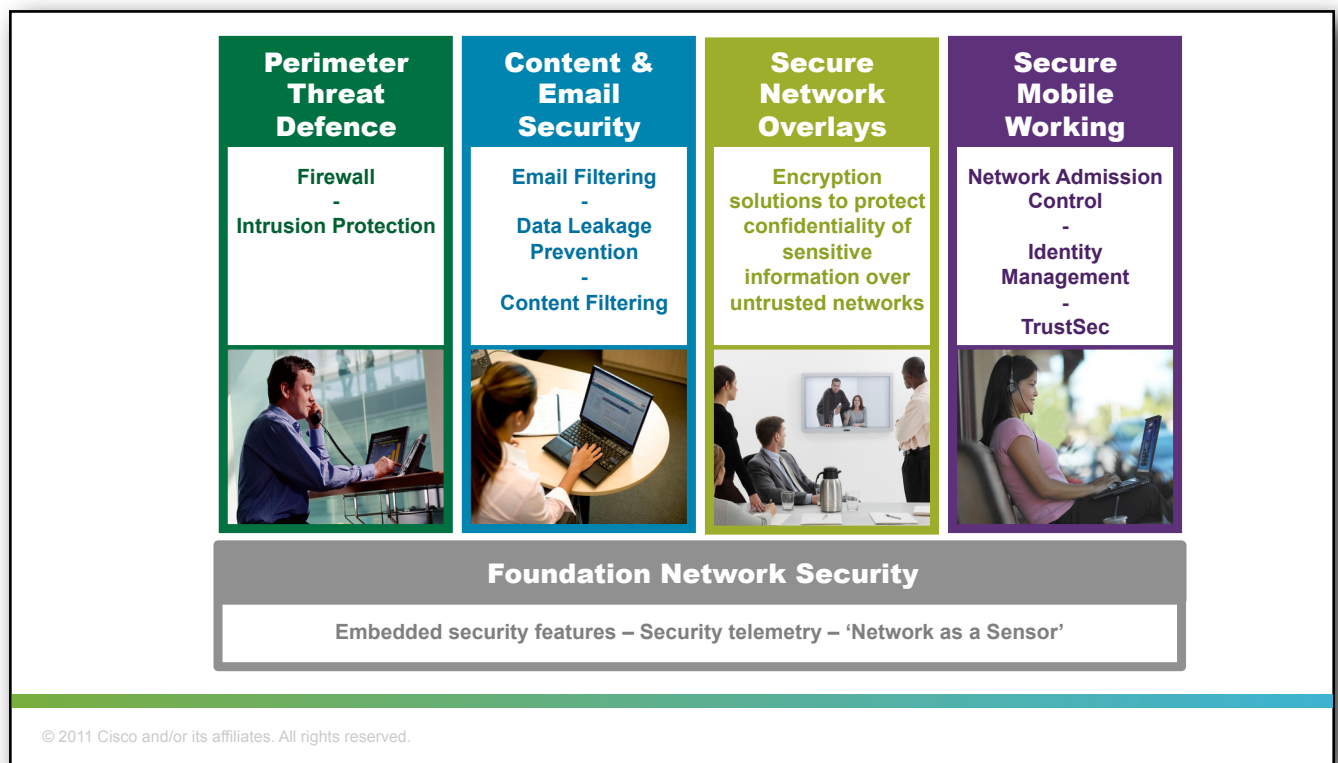


Figure 3.2.1 - Four Pillars of Cisco Security

The secure borderless approach shown in Figure 3.2.1 aims to address the security needs of today's highly interconnected environments through the introduction of a range of complimentary security controls:

- **Foundation network security** – embedded security capabilities provided within Cisco products aimed at protecting the core network infrastructure as well as provide detailed security monitoring;
- **Perimeter Threat Defence** – to mitigate threats that might arise from unauthorised access at network boundaries; for example gateways to N3, the Internet or 3rd party networks;
- **Content and Email Filtering** – to mitigate threats that might arise from content returned by web sites or delivered via email; also to prevent the leakage of sensitive patient data;

- **Secure Network Overlays** – to provide network encryption capability so that the confidentiality of sensitive information can be assured; applicable in Community of Interest Networks (COINs) including N3 and emerging Private Cloud approaches;
- **Secure Mobile Working** – to offer a set of trust, identity and access control tools that secure network access for multi-agency working and mobile or location independent workers.

3.2.2 Foundation Network Security

Today, the network represents a critical component in the delivery of patient care within the NHS and therefore must be protected at all times from not only external attackers, but also threats from inside. These internal threats could be malicious, but could also be due to non-malicious acts such as inadvertent configuration errors.

Many foundation network security capabilities are built into Cisco router and switch platforms and might only need evaluation and subsequent enablement of the features required. At a technical level, Cisco's approach to foundation security visualises the network in three 'planes':

- **Control Plane** – Used by network protocols, e.g. routing protocols;
- **Data Plane** – Used for data traffic forwarding;
- **Management Plane** – Used for managing and monitoring the network.

A structured approach to securing each of these planes is essential if the network is to deliver robustness and performance whilst appropriate auditing and monitoring must also be performed. Audit and monitoring represents one of the most valuable tools in being able to defend against modern cyber attacks that can easily thwart signature-based protection systems. A full discussion on all of the techniques available for protecting the network foundation is beyond the scope of this document, however some of the key capabilities to consider are:

- **Cisco Netflow** – provides administrators with a detailed insight into all traffic flowing across a network; when coupled with analysis tools it can quickly identify anomalous activity, e.g. Denial of Service;
- **Control Plane Policing** – applies policy to network traffic that targets a device's control plane; thereby preventing device overload;
- **Spanning Tree Toolkit** – capabilities in the Cisco Catalyst switches to control and manage Spanning Tree messages (where used).

3.2.3 Perimeter Threat Defence

In the past, NHS organisations have developed ICT environments based upon well-defined wired networks and well-defined security perimeters. Attacks were typically assumed to originate from outside an organisation, so mitigation was based on the creation of securely defended perimeters such as the deployment of firewalls on the N3 boundary. The significant increase in collaboration between NHS organisations and other agencies has led to a gradual erosion of such well-established perimeters. Furthermore, existing perimeters are challenged in maintaining security whilst supporting an ever-increasing range of off-network applications. Recent enhancements in common perimeter defence

technologies, such as firewalls and intrusion prevention systems (IPS) allow more granular policy control than ever before:

- **Global Correlation** – A capability of the Cisco IPS appliances whereby external attacker reputation information is used to inform policy decision-making, e.g. alert or drop traffic;
- **Identity Firewalling** – Reduces exposure of IP address and ports or protocols where instead, access policy could be based on user identity.

In addition, the advent of virtualisation technology has led to a range of new security issues, most importantly how are security controls maintained between virtual machines running on the same host. In this case, new virtualised firewall platforms that run within the hypervisor can allow granular policies to be enforced. Adding these important elements into a perimeter security deployment can offer greater control than ever before, supporting the highly interconnected nature of modern NHS networks.

3.2.4 Content and Email Security

Two of the most exploited attack vectors in recent years have been e-mail and web. For example, today's attackers often rely on attracting unsuspecting users to visit compromised web sites. When the user visits such a site, malicious code can be silently installed on to the victim machine allowing the attacker to use the machine for surreptitious purposes, including stealing sensitive data or simply using the machine as a 'bot' to launch attacks against other victims of the attacker's choosing.

To address the rapidly changing content security landscape, new techniques for detection must be employed, the most effective technique being reputation filtering. As the name suggests, reputation filtering attempts to allocate a relative reputation 'score' to both e-mail senders and web domains. For example, Cisco Secure Intelligent Operations (SIO) provides reputation information to Cisco content security solutions. SIO builds reputation scores by processing vast volumes of data relating to global e-mail and web content behaviour so that policy decisions can be taken quickly and accurately. For example, an e-mail domain that is seen to be sending a disproportionate volume of 'SPAM' will have a low reputation and as such, inbound connections from this domain can simply be denied.

In addition to addressing web and e-mail based attacks, NHS organisations must also be aware of the real potential for data loss via email. Data loss can be very damaging for any organisation that is dealing with sensitive personal data and therefore data loss prevention must form part of the email security solution. Data loss prevention could take the form of e-mail encryption, or could simply be a capability to monitor and block sensitive content from leaving the organisation via e-mail.

3.2.5 Secure Network Overlays

Protecting the confidentiality of information across wide area networks is a key consideration for all Public Sector organisations that deal with sensitive citizen or patient data. In the NHS, the primary focus has always been around the protection of Person Identifiable Data (PID), both at rest and whilst in transit. Protection of data at rest has been largely addressed by the focus on laptop hard disk encryption, but there remains a risk that data in transit may be compromised where application layer encryption is not implemented. Secure network overlays that make use of IPsec protocols are commonly used to ensure that all information flowing across untrusted networks remains protected. In addition to the protection of PID, IPsec VPNs have also been deployed in COIN environments, including over N3.

Cisco offers a range of Secure Network Overlays which have been introduced in section 3.1.2, the preferred options being DMVPN and GET-VPN.

3.2.6 Secure Mobile Working

Secure mobile working is a vital capability in the NHS, supporting the requirement for Trust staff to work from home or remotely. With the new demands for an increasing range of computing devices, as well as requirements to support multi-agency working, existing mobile working solutions are being stretched and often fail to deliver the level of seamless access and control required. Mobile working solutions must also support guest access provision, a requirement which is becoming increasingly important in the NHS, with patients and with 3rd party contractors.

Cisco Trusted Security (TrustSec) offers a range of capabilities designed to support seamless, location independent working whilst maintaining high degrees of security, comprising:

- **IEEE 802.1x** – Wired and Wireless LAN access control technology that can authenticate and authorise Trust users and devices as they attempt to connect to the network.
- **Network Admission Control (NAC)** – NAC builds on 802.1x, providing device posture checking to validate device ‘health’ which can then be used to enforce access policy;
- **Security Group Tagging (SGT)** – Again building on 802.1x, provides topology independent access control by assigning a ‘tag’ to user traffic. Access-control can then be applied using this tag, rather than on IP address and protocol/port information;
- **Guest Access** – Support for patient or contractor access to the network. Includes captive portal to force the user to authenticate prior to gaining access. Policy can be applied to guest users to ensure they simply have access to the Internet, and not internal NHS systems;
- **Secure VPN** – IPsec and Secure Sockets Layer (SSL) based VPN technology to protect remote workers. Includes ‘Always-On’ VPN capabilities to ensure that mobile devices always have to connect via VPN before accessing the network.

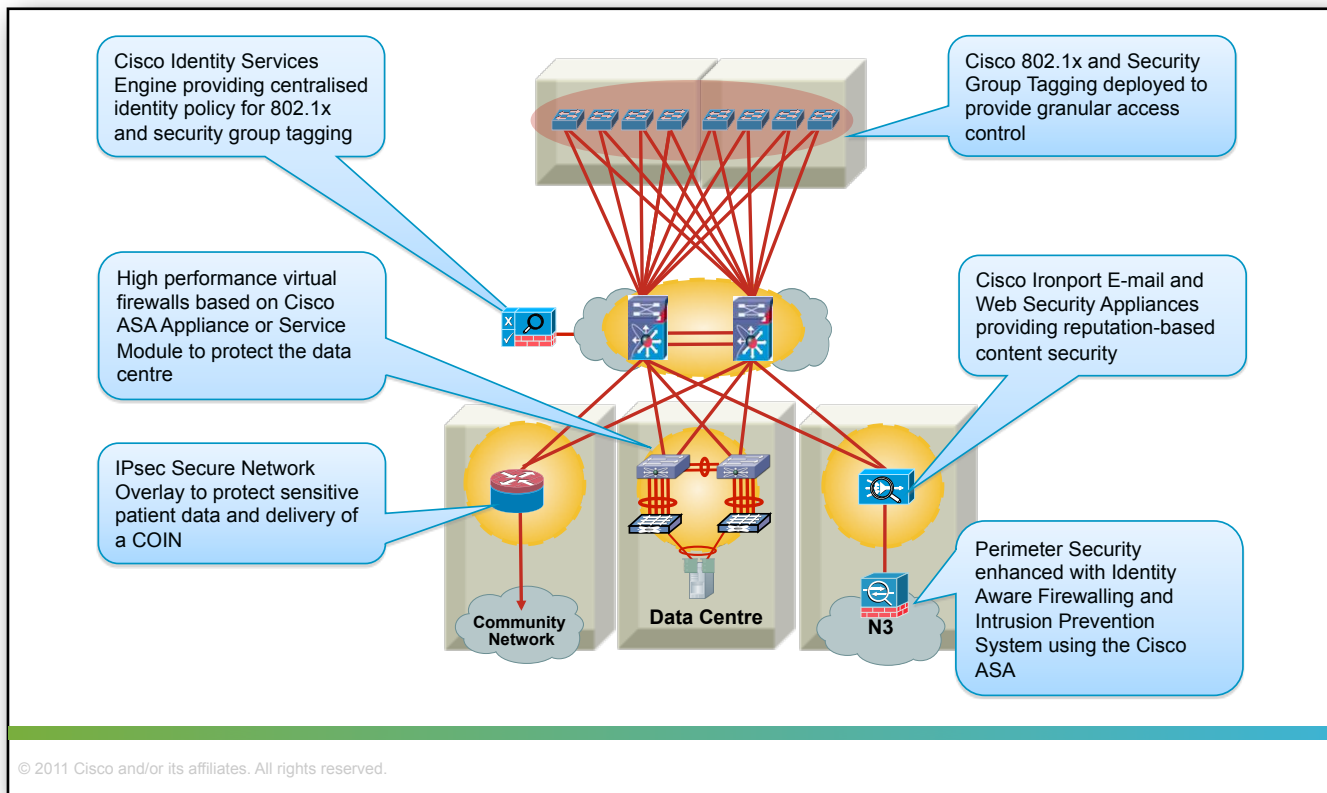


Figure 3.2.2 - Borderless Security Overlay

Figure 3.2.2 shows a number of the solutions discussed in this section overlaid on a campus infrastructure, but equally relevant in distributed care.

3.3 Borderless Mobility¹⁰

Access to, and the availability of, information are perpetual hot topics in healthcare. A proliferation of mobile devices has created new opportunities for offering instant access to information and the ability to update it at the point of need. Given these new opportunities, NHS organisations are increasingly looking at their wireless network infrastructure and understanding how it can facilitate secure access from multiple device types, as well as offering other incremental functionality. In the NHS, Cisco sees the following as key benefits of delivering wireless infrastructure:

- Mobile access to clinical information;
- Integration of Unified Communications and Wireless;
- Guest wireless access;
- Reciprocal wireless access between NHS and other agencies;

▪ Tracking solutions:

- Tracking and identifying the location of clinical equipment;
- Identifying the nearest required skill such as porter, nurse etc;
- Temperature monitoring of clinical fridges;
- Patient safety; and staff safety (such as tracking lone workers);
- Tracking to support equipment maintenance.

In order to realise some of these more advanced benefits, it is critical to define the basic underlying wireless infrastructure correctly – and in accordance with the foreseeable objectives of the organisation.

¹⁰ Cisco Borderless Mobility - <http://www.cisco.com/go/mobility>

3.3.1 Centralised Wireless LAN

Wireless LAN design has evolved over the last decade and in recent years the centralised approach has emerged as the preferred design model. The benefits of a centralised approach include:

- Simplified configuration and control using 'Controllers';
- Simplified operational management by collapsing large numbers of managed Access Points (AP's) into a single managed system;
- 'Lightweight' AP's that can't act independently of the Controller;
- Centrally controlled security policies, QoS policies, Radio Frequency (RF) management and mobility management;
- Enables support for seamless mobility and a number of advanced features in an elegant and scalable way.

Figure 3.3.1 shows the components of a centralised wireless architecture overlaid on a campus infrastructure. In the diagram the Controller may be a standalone appliance known as a Wireless LAN Controller (WLC), or a module located in a network switch, the Catalyst 6500 WiSM2 module.

Access points connect to a Controller using the Control and Provisioning of Access Points Protocol (CAPWAP) which has two primary functions:

- The control and management of Access Points;
- The tunnelling of WLAN client traffic to the Controller.

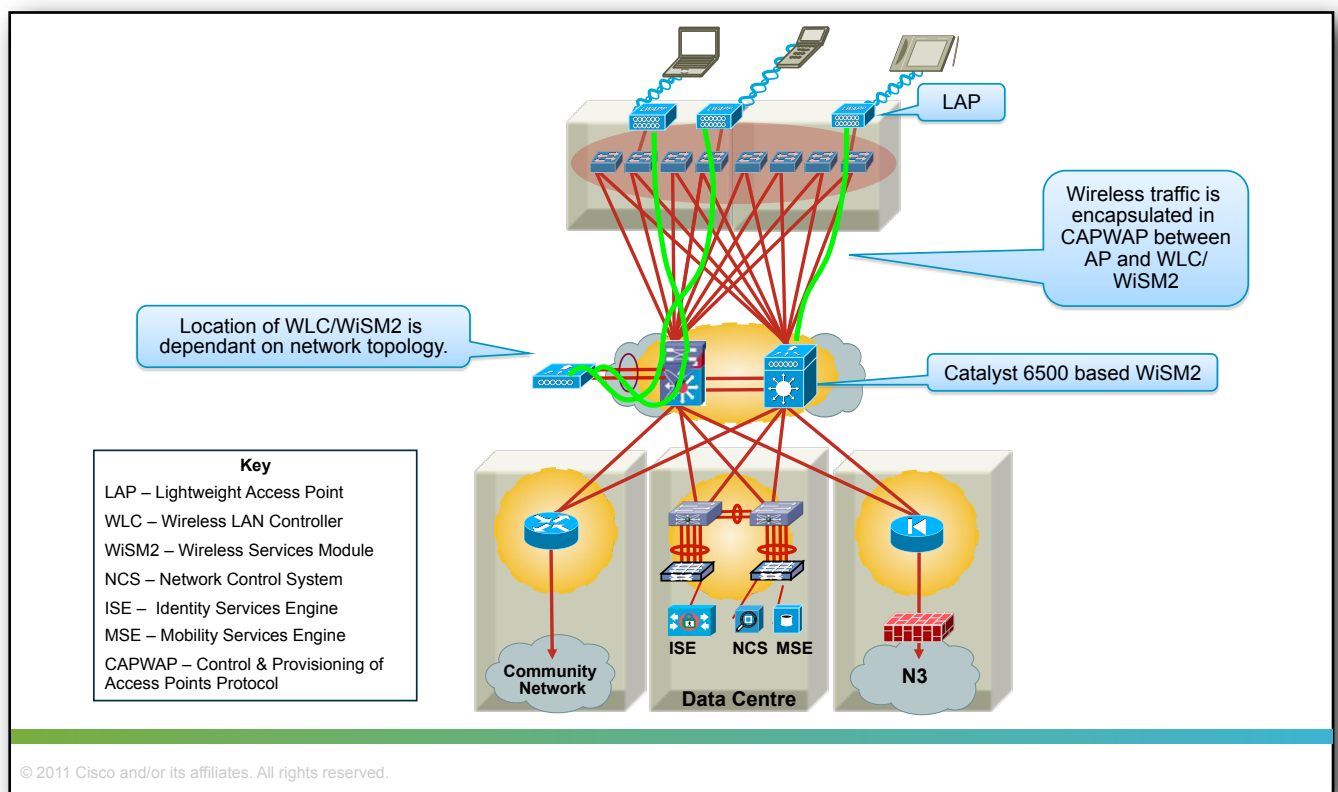


Figure 3.3.1 - Cisco Unified Wireless Architecture

3.3.2 Context Aware Location Services

One of the main areas of concern for NHS organisations today is the management of key assets. Asset tracking solutions can use a correctly designed hospital Wireless LAN infrastructure to actively track assets through the use of Radio Frequency Identification (RFID) tags. This technology enables hospitals to reduce inefficiencies associated with equipment utilisation, patient care and safety, staff productivity and financial loss.

Access points forward information to WLAN controllers regarding the detected signal strength of any WLAN clients, asset tags, rogue Access Points or rogue clients. The collected signal strength information is forwarded to the WLAN controller where it is aggregated and sent to the location engine. The location-enabled Network Control System (NCS) works in conjunction with the location engine by serving as the user interface. Figure 3.3.2 shows a location aware unified wireless network overlaying a campus network design.

3.3.3 Voice over Wireless LAN

Within a hospital environment a Wireless LAN infrastructure can support mobile voice enabling staff to communicate with each other at any time and in any place. The solution offers improved accessibility in comparison to traditional paging systems where a phone is required to respond to the page.

Note: When considering Wireless LAN based solutions for pager replacement, full understanding of the 802.11 environment and its characteristics are essential. Robust back up policies/ systems are advised and should be well known.

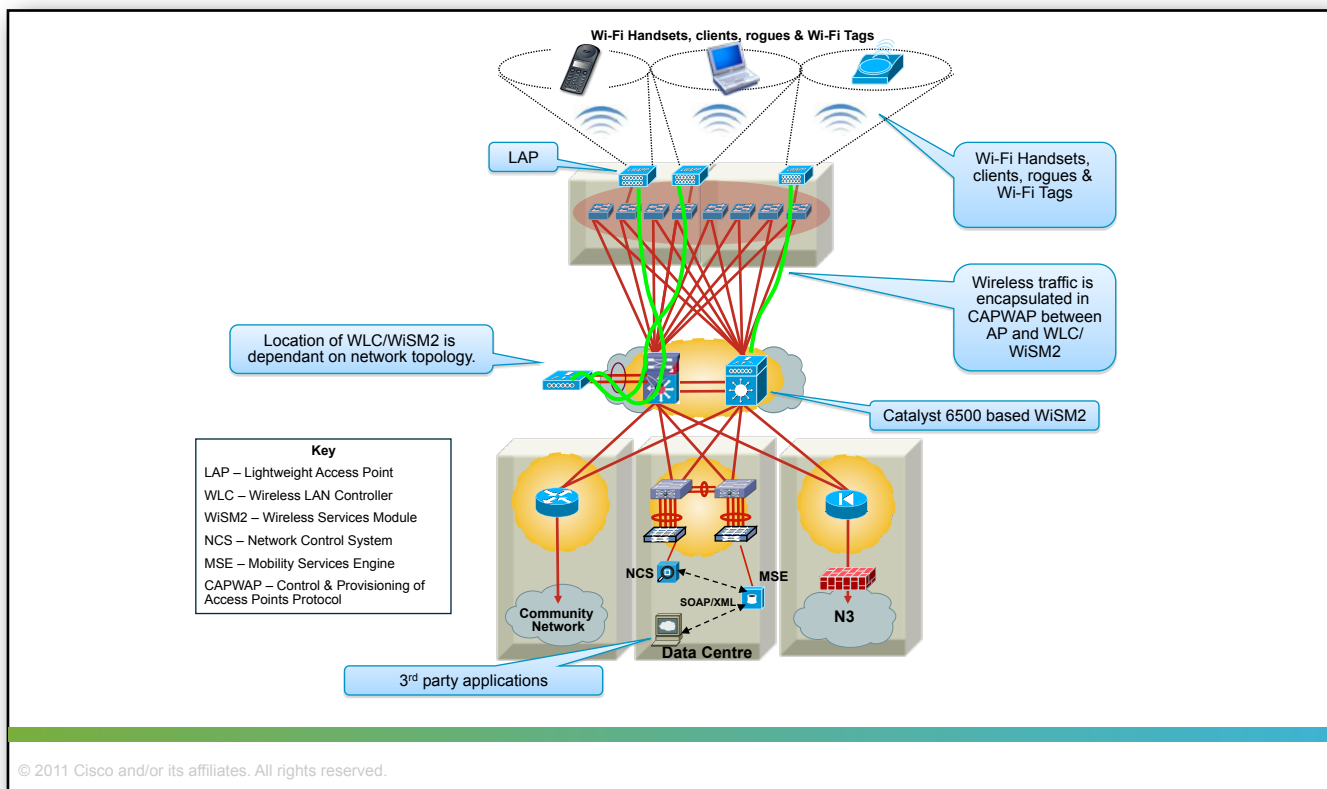


Figure 3.3.2 - Location Services Architecture

In any organisation it is essential that the Voice over Wireless LAN (VoWLAN) environment is designed end-to-end so that high availability can be achieved. In an NHS environment this means a consistent, reliable service must be provisioned within the hospital and associated outbuildings. Some key network considerations must be addressed and these include:

- **Bandwidth:** the coding type (codec) used and the associated bandwidth demands;
- **Quality of Service:** prioritisation of voice traffic to mitigate factors such as packet loss, jitter and delay;
- **Roaming:** fast roaming algorithms to enable smooth transition for Wireless LAN clients from one Access Point to another.

Cisco supports Wireless LAN voice with a range of handsets supported by the Unified Communications solution described in section 5.

3.3.4 Secure Wireless LAN

Building on section 3.2.6, the wireless network should be treated as another access method adhering to the same principles as the wired network. Practically this means understanding the wireless network itself, what it will be used for and the level of access control required.

In the NHS like any other organisation the level of security offered will depend upon each Trust's differing requirements but consideration should be given to:

- **Authentication** – using standards based or well known protocols such as 802.1X, Extensible Authentication Protocol (EAP) and Remote Authentication Dial In User service (RADIUS);
- **Encryption** – using standards based solutions known as Wi-Fi Protected Access (WPA) and WPA2:
 - Temporal Key Integrity Protocol (TKIP) is the encryption type certified in WPA supporting legacy WLAN equipment and addressing flaws in earlier solutions;
 - Advanced Encryption Standard (AES) encryption in WPA2 brings the WLAN environment into alignment with current encryption best practice.

Ever increasing use of mobile devices and wireless networks in NHS organisations has dictated a need for comprehensive wireless threat detection, mitigation and prevention. The Cisco Adaptive Wireless Intrusion Prevention System (IPS) employs network analysis and signature-based techniques to deliver protection against rogue access points and clients, network reconnaissance, eavesdropping, authentication and encryption cracking, man-in-the-middle attacks, wireless Denial of Service (DoS) attacks and Day Zero unknown attacks. The system also provides proactive threat prevention via automated wireless vulnerability and performance monitoring, which proactively and persistently scans the wireless network to mitigate issues before they arise.

3.3.5 Guest Access Solutions

Today's NHS environments encompass an increasingly mobile workforce that requires comprehensive network connectivity and access to critical business and clinical applications leading to increasing interest in Guest Access solutions. Securing part of the Wireless infrastructure to offer Guest Access allows mobile caregivers, clinicians and consultants to gain connectivity to their 'home' organisation using VPN technology. Meanwhile Internet access for patients and visitors can also be securely provisioned.

Figure 3.3.3 shows a typical guest access deployment. Once the guest has a username and password and opens a browser, they enter credentials that are recognised by the Wireless LAN controller and assigned to the 'Guest' VLAN. The guest traffic is encapsulated in an Ethernet over IP tunnel to the 'anchor controller' in the De-Militarised Zone (DMZ) and subsequently routed as appropriate but always separated from the Trust network. Once the guest user's credentials expire, access to network resources is terminated.

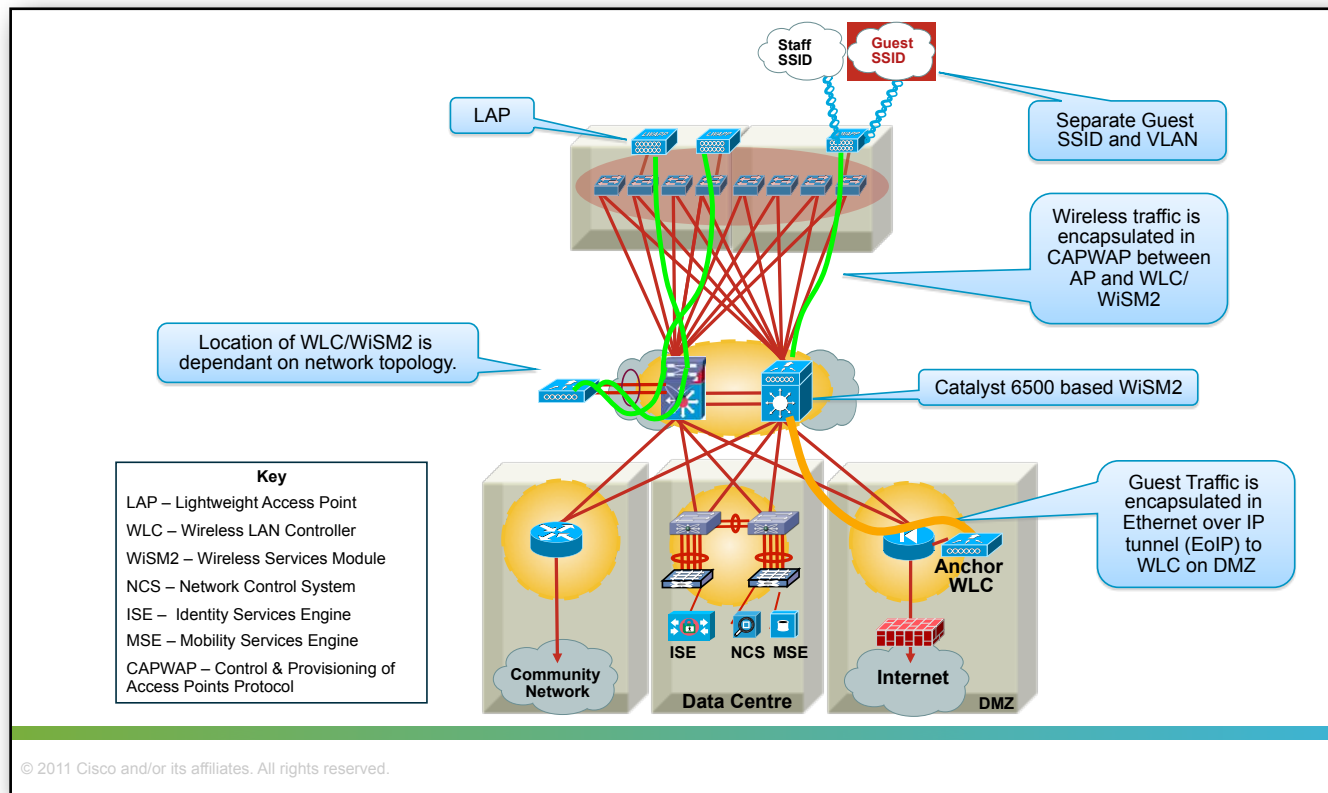


Figure 3.3.3 - Wireless Guest Access Services

In certain deployment scenarios, a Trust might require a separate guest provisioning appliance to facilitate the creation of guest accounts, management of guest access policies, and reporting for guest network use. The Cisco NAC Guest Server (NGS) is a purpose-built guest access provisioning and accounting appliance. NGS is suitable for Acute Trusts that need to provide Internet access to patients and visitors as it provides a centralised reporting interface to track statistics on both guest access account and guest network use.

One other growing area of interest is secure roaming of users between different Public Sector agencies. Cisco offers a solution known as **Reciprocal Wireless Access** which enables secure tunnelling of information to an anchor controller in the user's own organisation network. This solution is particularly suitable for mobile NHS staff working at another NHS site, or perhaps roaming between the NHS, Local Authorities and Universities. It is essential of course that all information governance considerations are taken into account along with central guidance. Cisco would be pleased to assist any organisation considering such a solution.

3.3.6 Spectrum Intelligence

The earliest wireless networks were often designed as an added convenience with a best effort level of performance deemed acceptable. These networks have now matured to the point that they are deployed for many different applications in healthcare. Today's wireless networks are therefore expected to run with very high reliability and it's no longer acceptable to have unexpected downtime due to interference. Cisco's CleanAir solution addresses this challenge and has two principle components:

- **Spectrum intelligence (SI)** is data about RF spectrum activity derived from advanced interference identification algorithms. Spectrum intelligence provides visibility into all the users of the shared spectrum;
- **Spectrum management (SM)** is the active use of spectrum intelligence data to improve performance. Information about the severity and duration of interference can be used to calculate its impact on the network and to troubleshoot problems.

Cisco CleanAir provides NHS IT staff with access to rich spectrum information that is automatically gathered on every non-802.11 interference source and enables the network to address these issues automatically.

3.3.7 Unified User, Access and Identity Management

Cisco Prime Network Control System (NCS) is an evolution of the Wireless Control System (WCS) and is built on this foundation. It offers converged user, access and identity management with complete visibility in to endpoint connectivity, regardless of device, network or location. NCS also provides monitoring of endpoint security policy through the integration with the Identity Services Engine (ISE).

ISE supports the provisioning of applications securely and reliably across wired, wireless and VPN environments. This helps to simplify operations and is particularly suitable for today's trend toward the use of consumer devices ('Bring Your Own Device' – see section 5.10). ISE also helps to gather real-time contextual information from the network, users and devices and supports policy enforcement across the network infrastructure.

3.4 Video and Content Delivery

Following the exponential growth of video in the consumer domain, enterprises are now realising the benefits of the technology. However, the best efforts approach of the consumer world is not acceptable in a formal business or healthcare setting, and there are specific requirements of infrastructure as well as the quality of the video solutions themselves.

In healthcare, there are a number of established use cases.

- Regular or unscheduled business meetings at any level of an organisation typically involve people relocating themselves for attendance in person. This results in travel and time related inefficiencies as well as the impact on costs and the environment that can all be mitigated using video and collaboration technologies;
- Multi-disciplinary team (MDT) meetings are a common practice across the NHS, whether it be Cancer Care organisations, or other clinical specialities. Conferencing solutions are a key tool for MDTs, enabling the sharing of medical

expertise and reduced time spent travelling to meetings – increasing productivity, saving costs and improving the quality of patient care. Video is already extensively used in these environments but often the technology is ageing with a low quality experience and little integration with other information tools;

- Traditionally patients have been securely escorted from prison to an NHS Trust for clinical assessment, diagnosis and treatment of their condition at significant cost. Meanwhile referrals from Care and Residential Homes can cause a significant degree of stress for patients. Both could be mitigated through the use of remote care solutions supported by high quality video;
- The use of video solutions deployed into lecture theatres, seminar rooms, clinical simulation centres and operating theatres enable new ways of learning for the doctors and nurses of tomorrow's NHS;
- Two areas of increasing interest are TeleHealth and Telecare – the benefits being that patients can live independently whilst pressure is released from overburdened healthcare facilities. Many programmes and pilots are in existence across the country and video technology plays a significant role in many of them;
- Surveillance systems – integrated with access control systems providing a holistic physical security solution across a campus or distributed environment.

It is therefore clear that high quality video is evolving as an enabling tool for NHS organisations to deliver business, clinical and operational benefits. This sub-section discusses the support of video in today's networks including the differing types of video and the intelligence required in the borderless network to support a business quality video experience. (We recommend that this section be read in conjunction with section 5 to inform a video and collaboration strategy.)

3.4.1 Cisco Medianet ¹²

Video loads, and radically changes the demands on NHS networks, however not always in the same way. Consider for instance real-time, streaming video that is scheduled, requiring services for reliable delivery to multiple end-stations.

¹² Cisco Medianet – <http://www.cisco.com/go/medianet>

Compare this with a video-on-demand session that is unscheduled and typically requested by one end-station. Other types of video such as conferencing or 'push video' for health promotion, demand different services and have different traffic profiles. It is clear therefore that not all video is equal and an enterprise class, borderless infrastructure must support the required services of all video types to ensure a seamless experience.

Cisco's Medianet architecture addresses these challenges. A Medianet is an end-to-end IP architecture that is media-aware, endpoint-aware, and network-aware. By being media-aware, Medianet detects and optimises different media and application types such as Telepresence, video surveillance, desktop collaboration, and streaming media to deliver the best experience. By being endpoint-aware, it can automatically detect and configure media endpoints. Lastly, by being network-aware, it's able to detect and respond to changes in a device, a connection and service availability.

Medianet technology is supported in many Cisco routers and switches, working together with endpoints that have embedded Medianet technology through the Media Services Interface. This offers tight integration between endpoints and the network, simplifying the deployment and operation of various media and applications and enhancing the quality of experience.

3.4.2 Medianet Features

Auto-configuration and location capabilities help address some of the challenges involved in mass deployments of endpoints such as Digital Media Players (DMPs) and physical security cameras. Auto-configuration mitigates the need for manual configuration of switch ports connected to rich-media endpoints and ensures the correct settings are applied regardless of the port that the endpoint is connected to in the field. This is essential when considering the specific attributes that rich-media endpoints require and elements such as location information, critical to the management of surveillance networks and DMPs.

With auto-configuration the access switch can recognise the device and automatically configure the port for VLAN, QoS, security features and location information.

The Media Services Interface was developed to address the challenge of tightly integrating applications

and network infrastructure services to deliver an optimised experience. The interface provides Cisco rich-media endpoints and applications with a series of application programming interfaces (APIs) to enable them to take advantage of the Medianet services in the network infrastructure. Embedding the Media Services Interface into a wide range of endpoints enables the network to provide a standardised set of services, which can be accessed in a consistent and controlled manner.

Media Monitoring is composed of three features: Performance Monitor, Mediatrace, and IP Service Level Agreement Video Operation (IP SLA VO). These three features form a suite of tools to help enable the network operator to perform media performance monitoring and troubleshooting.

Performance Monitor is a software feature that measures the performance of Real Time Protocol (RTP), TCP and IP Constant Bit Rate (CBR) traffic on network devices. Performance Monitor analyses RTP based audio and video flows and reports on service-affecting metrics like packet loss and network jitter. For TCP flows, Performance Monitor reports on round-trip time and packet loss occurrences. Hop-by-hop knowledge of these metrics along the network path leads to granular fault isolation and thus easier troubleshooting of user traffic flows.

Different media applications, for example Cisco Telepresence compared to Video on Demand (VoD), have different sensitivities to packet loss and jitter. These varying sensitivities can be encoded into Performance Monitor threshold evaluations and actions. An example would be the generation of a Simple Network Management Protocol (SNMP) trap when Cisco TelePresence traffic loss is greater than 1 percent. When a threshold is crossed, an alarm is generated that can notify the operator of the issue. This event may eventually engage further diagnostics such as Mediatrace to troubleshoot and further isolate the cause of degradation.

Mediatrace is a network diagnostic tool that collects information from network nodes along the flow path and presents this information in a single screen that allows for easy analysis. Depending on the type of Mediatrace request, the feature may implicitly enable Performance Monitor to gather flow-specific information. Mediatrace can be manually invoked or run in a periodic fashion along a specific path of routers and switches.

IP SLA VO is a valuable tool to assess the readiness of a network to carry rich-media traffic. It has the ability to synthetically generate video profiles mimicking real application traffic. IP SLA VO can also make use of user-captured packet traces from the NHS organisation's existing network, which can then be included in the synthetically generated traffic stream. This feature can be used to run network readiness tests prior to important collaboration events or meetings (e.g. MDT's) to validate that the network will be able to support the expected rich-media traffic.

It is clear therefore that all video traffic has different demands. Medianet allows the network to assess its ability to support video traffic, to identify video sources and configure the appropriate QoS and security policies based on these video sources.

3.5 Sustainability and Energy Management

Over recent years sustainability has perhaps taken a back seat to global financial challenges. However, the Carbon Reduction Commitment (CRC) and the newly established need to report on sustainability as part of the annual NHS financial reporting process, have led to increasing focus on the environmental impact that organisations have. Happily, a strategy to improve sustainability can result in incremental financial savings as well.

As an energy user, ICT must minimise its own consumption, but technology can be instrumental in areas such as reducing travel and building efficiency.

3.5.1 ICT as an Energy Consumer

Continuing investment in product development has seen product efficiency improve dramatically. Enhancements such as improved power supply efficiency and "idle slot power optimisation" (where unused elements of the infrastructure are automatically powered down until required) ensures that each component of the infrastructure is optimised for energy savings.

There are also some specific areas worthy of mention such as the Data Centre, traditionally a significant consumer of energy. For example the consolidation of traffic onto a single infrastructure (commonly known as Fibre Channel over Ethernet (FCoE)) reduces the total number of interfaces and hence equipment, while

higher performance interfaces have been introduced, but with a lower power requirement. As well as a reduced Data Centre footprint, design principles such as front to back airflow improve efficiencies, the collective effect being reduced demand on cooling requirements.

Whilst it is impractical to detail every product range in this document, these are just a few examples of enhancements that have been recently introduced. Cisco continues to improve the efficiencies of its products and solutions.

3.5.2 Saving Time, Cost and Carbon

One of the areas that ICT can positively impact on sustainability is the reduction of wasted time, cost and carbon equivalents associated with travel. As NHS reforms are put in place, mergers and acquisitions have increased and smaller organisational groups such as Clinical Commissioning Groups have been formed. Meanwhile, organisations spanning broader geographies have been established such as the NHS Commissioning Board structure and Clinical Senates. All of these newly formed organisations need to collaborate effectively, sometimes between disciplines, often over long distances.

Video and collaboration solutions provide an ideal platform to enable these organisations to work across boundaries or distance. With an underpinning and feature rich infrastructure supporting business class video, coupled with collaboration platforms such as Cisco's Webex, NHS organisations can reduce the need for travel to central sites to meet face to face.

3.5.3 Managing Power with Cisco Energywise

Cisco's Energywise¹³ architecture is a network based intelligent power management solution that allows policy control over network connected devices. Policies can be defined to control which devices are powered and when, for example some network attached devices could be powered off completely for 75% of the time with no user impact while the same solution can power other devices continually as dictated by operational need.

¹³ Cisco Energywise – <http://www.cisco.com/go/energywise>

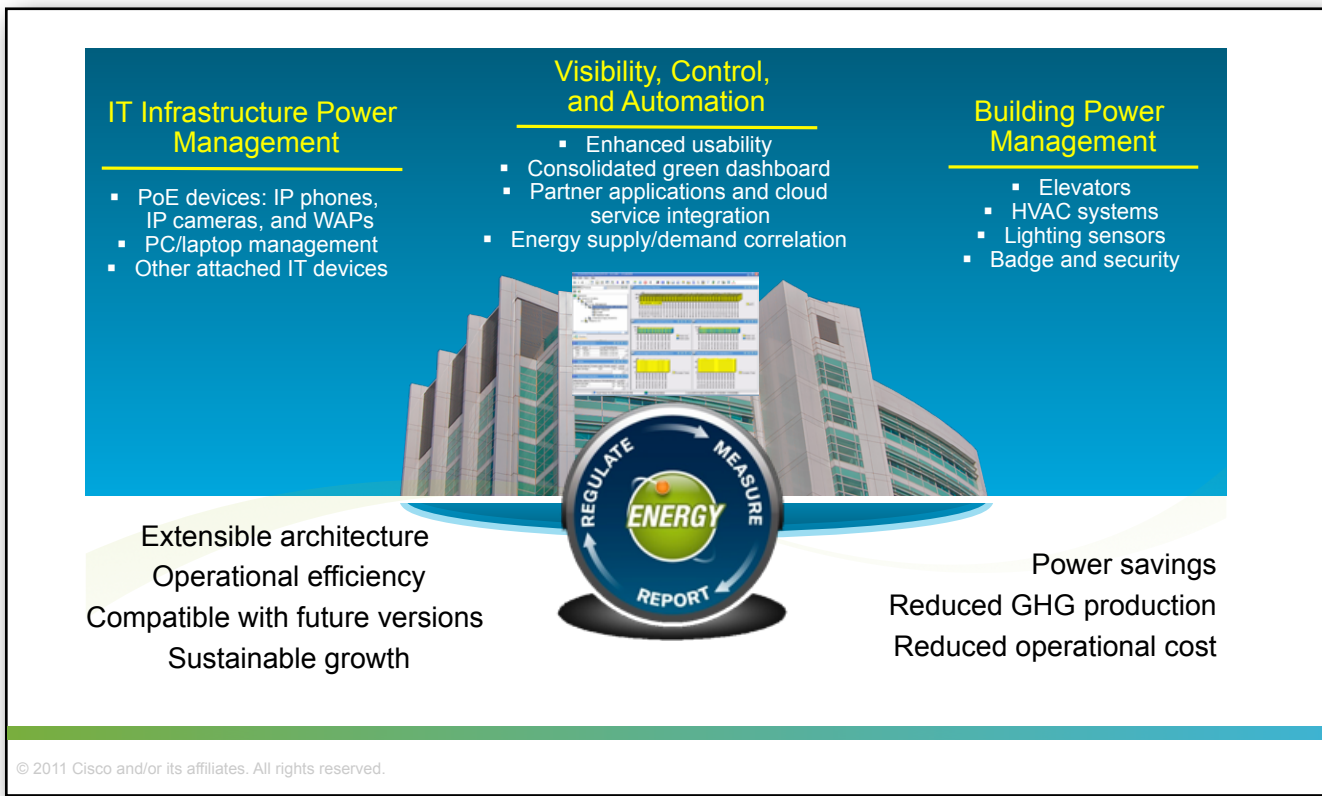


Figure 3.5.1 - Cisco Energywise End to End Solution

As shown in figure 3.5.1, phase one of Energywise supports management of Power over Ethernet (PoE) enabled infrastructure devices such as IP Phones and Wireless Access Points.

Phase two supports devices such as desktop PCs that connect to the IP network but are not PoE powered. Energywise has been extended to allow control from the same policy for both PoE and non-PoE devices. For example the telephony handsets and PCs for individual users can be powered down simultaneously based on a common power policy template. Other devices such as monitors and printers can be managed by using one of a range of Energywise compliant power distribution units.

Meanwhile in phase three, ongoing partnerships with Building Management System (BMS) providers allow the benefits of Energywise to be extended into the infrastructure of buildings. This enables heating, cooling and lighting to be aligned with the NHS organisation's energy management policies.

Energywise is a software feature supported on many Cisco platforms and complements other solutions to offer a holistic but more granular approach to energy management.

3.6 Network and Service Management

Having a holistic view of the networked environment is critical for NHS IT staff to quickly respond to faults or change requests. Whilst management tools can sometimes be considered an afterthought, they are essential to provide the levels of visibility required.

In an effort to provide a clear focus and strategy for running a network securely and efficiently, the International Organisation for Standardisation (ISO) developed a network management model identifying five key areas of network management: Fault management, Configuration management, Accounting management, Performance management, and Security (FCAPS):

- Fault management is concerned with detecting, diagnosing, and correcting network and system faults. This includes alerts, events and diagnostic tools;
- Configuration management focuses on installation, identification and configuration of hardware, software, firmware and services. This includes software and inventory management and change control;
- Accounting management looks at tracking the use of resources in a network, including tracking of communications and computing facilities utilisation, as well as tracking user access to networks and the resources accessed by those users;
- Performance management focuses on measurement and analysis of network and system statistics related to utilisation, response time, availability and error rates. Such tools are also used to assist in planning, design, and performance-tuning of networks;
- Security management is concerned with controlling access to network resources and preventing unauthorised use of or tampering with the network.

In the NHS the importance placed on the availability of information is clear and the performance of the underlying infrastructure and the applications which use it should be considered critical. Centralised device access and control, coupled with monitoring and alert tools for visibility, enable NHS IT to manage the network effectively.

3.6.1 Service and Network Management Solutions

Today's Network Management applications provide a user friendly interface to manage the infrastructure and other solutions such as security, QoS, mobility and the Unified Communications environment. The foundation of every network is the infrastructure composed of routers, switches, gateways and local and wide area connections. Visibility and control of the infrastructure are essential in ensuring proper operation of the network as it evolves.

The Cisco Prime for Enterprise¹⁴ strategy supports integrated lifecycle management of the networks, services and endpoints for Cisco Borderless Networks, Data Centre and Collaboration architectures described throughout this document. It is based on a top-down approach to network management beginning at the application layer and progresses through the services down to the network infrastructure.

Adopting a Prime for Enterprise approach to management enables NHS IT departments to:

- Improved operational efficiencies: Reduce network errors, speed troubleshooting and improve the delivery of services;
- Reduced operating expenses: Speed deployments and reduce training requirements with easy-to-use tools;
- Lower capital expenditures: Optimise network investments through converged management and integration with existing systems.

The Cisco Prime for Enterprise product portfolio includes:

- Network Control System (NCS): Delivers converged user and access management for wired and wireless networks;
- LAN Management Solution (LMS): A comprehensive management suite for Cisco Borderless Networks;
- Collaboration Manager (CM): Includes monitoring and troubleshooting of video sessions and media paths in real time;
- Network Analysis Module (NAM): Provides application and performance visibility to optimise network resources, troubleshoot performance problems and help ensure a consistent user experience.

¹⁴ Cisco Prime for Enterprise – <http://www.cisco.com/en/US/partner/prod/netmgtsw/prime.html>

4. Data Centre Virtualisation¹⁵

Since the original C-NAB documents were issued in 2008, Data Centre has been the fastest growing technology segment. Cisco has been at the forefront of this change advocating a unified approach to Data Centre design in partnership with other established partners who lead in this environment. Within the Data Centre, virtualisation, convergence and consolidation are fast becoming the norm and organisations are looking for solutions that address the following requirements:

- **ICT as a strategic asset:** ICT is no longer a cost centre, but is viewed as a strategic asset that enables business and service transformation. The Data Centre is a key component of the overall ICT strategy;
- **Virtualisation:** Virtualisation is one of the highest impact issues challenging NHS ICT infrastructure and operations, both in the Data Centre and at the desktop;
- **Application performance:** Optimising application performance within the virtualised infrastructure is a significant challenge but must be achieved in order to ensure a quality user experience and productivity;
- **Cloud computing:** With the rising interest in cloud computing, organisations are looking for foundational cloud infrastructures that can support on-demand services;
- **Security:** A top of mind concern, particularly as organisations move into cloud-based models and virtual services;
- **Cost reduction and avoidance:** Reducing physical space requirements resulting in a smaller equipment footprint and reduced power and cooling costs.

Recent advances in technology offer new opportunities for NHS organisations to re-consider the way that services are offered, both for their own organisation and potentially across boundaries.

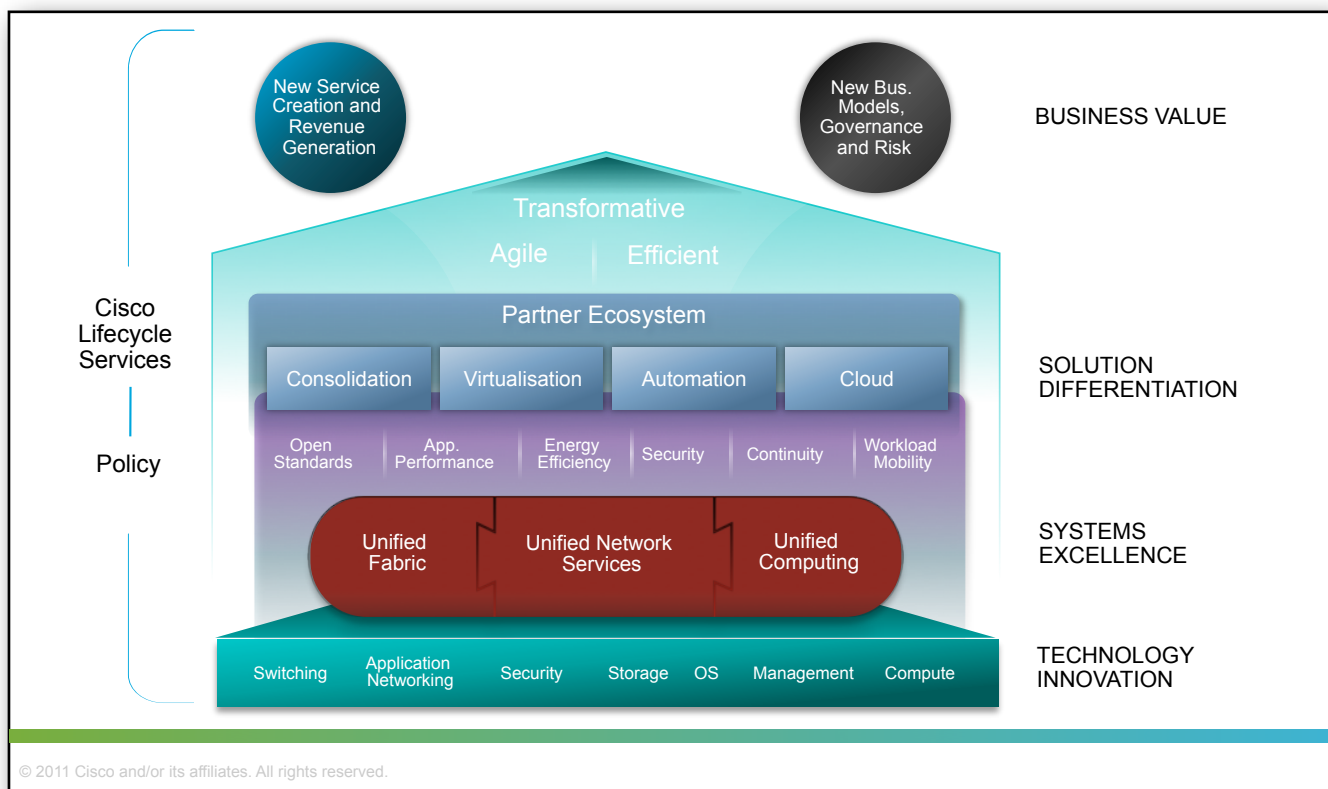


Figure 4.1.1 - Data Centre Business Advantage - Architectural Framework

¹⁵ Cisco Data Centre Virtualisation - <http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/index.html>

4.1 Logical Architecture for Data Centre Virtualisation

Figure 4.1.1 (page 31) shows the framework known as Data Centre Business Advantage (DCBA) demonstrating the link between business objectives and the Data Centre. Offering a holistic and unified approach to the Data Centre, this architectural approach brings system-level benefits such as performance, energy efficiency and resilience whilst addressing key requirements such as workload mobility and security. It also demonstrates the inter-dependencies that exist. As shown, Cisco's Unified Fabric, Unified Computing and Unified Network Services are the three foundational pillars for the DCBA framework.

- **Unified Fabric** consolidates traffic onto a single, high-performance and highly available network to simplify infrastructure and reduce cost;
- **Unified Computing** is a next-generation scalable, multi-chassis platform that unites compute, network and storage into one cohesive system and one unified management domain;
- **Unified Network Services** supports application delivery and security services in the Data Centre network.

4.2 Data Centre Unified Fabric

The architectural approach is based on the principle of establishing a robust, secure and scalable platform in order to support the critical applications that ensure business and clinical needs are met. A two or three layered hierarchical design is preferred as shown in Figure 4.2.1, featuring Core, Aggregation, and Access layers with flexibility to add Services as demand and load increases.

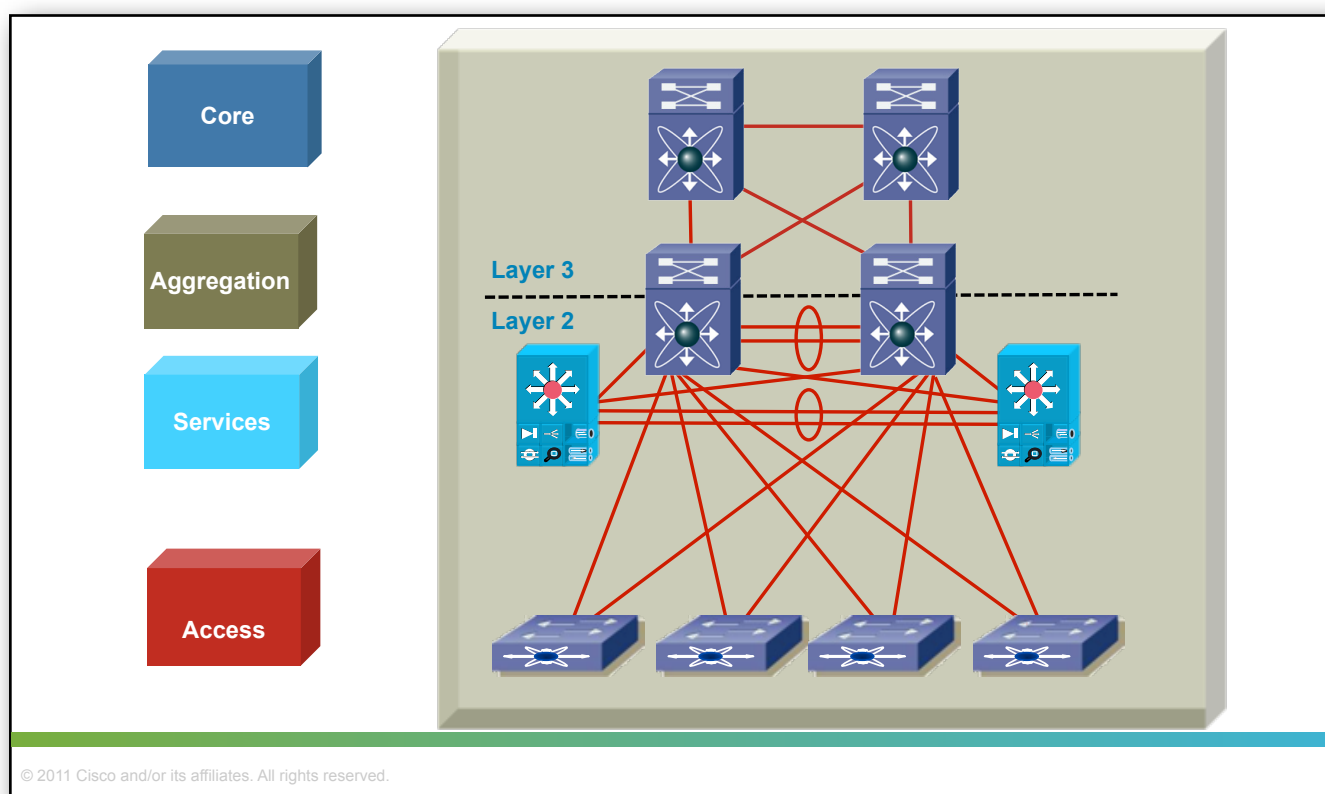


Figure 4.2.1 - Data Centre Hierarchical Network Design

The **Core layer** provides the high-speed packet switching backplane for all flows going in and out of the Data Centre. The core layer connects to, or can be an integral part of, the campus core providing connectivity to multiple aggregation modules providing a resilient layer 3 routed fabric with no single point of failure.

The **Aggregation layer** serves as the layer 3 and layer 2 boundary in Data Centre design and is the connection point for firewalls and other Data Centre services. For smaller or mid-size Data Centres such as those found in many NHS organisations, it is not uncommon to find the core and aggregation layers collapsed together.

Network and security services such as firewalls, server load balancers, intrusion prevention systems, application-based firewalls and network analysis modules are typically deployed at the Data Centre Services layer. Locating service modules in an external chassis allows the aggregation switches to be dedicated to packet forwarding with typical designs using a dual-homed approach for connectivity of the service chassis into both aggregation layer switches. Alternatively, if services chassis' are not part of the architecture, service appliance devices can also be attached directly to Data Centre aggregation switches.

Network and security services such as firewalls, server load balancers, intrusion prevention systems, application-based firewalls and network analysis modules are typically deployed at the Data Centre Services layer. Locating service modules in an external chassis allows the aggregation switches to be dedicated to packet forwarding with typical designs using a dual-homed approach for connectivity of the service chassis into both aggregation layer switches. Alternatively, if services chassis' are not part of the architecture, service appliance devices can also be attached directly to Data Centre aggregation switches.

Finally, the **Access layer** is the point of connectivity for servers and shared resources. Key considerations are high performance end nodes, the migration to 10-Gigabit Ethernet for edge connectivity and the drive for virtualisation. Access layer design is also tightly coupled to server density, form factor and server virtualisation, often resulting in higher interface and port counts. An additional factor influencing access layer design is the convergence of storage and Ethernet traffic onto a unified physical infrastructure.

Cisco Unified Fabric offers a broad Data Centre LAN and Storage Area Network (SAN) switching portfolio from the Hypervisor to the core. All platforms in the portfolio run on a common operating system (NX-OS) offering operational and functional consistency. Platforms include:

- The Nexus¹⁶ 7000 core switch designed specifically for the Data Centre. It offers high availability features and throughput that deliver the operational characteristics NHS organisations need;
- Nexus 5000 switches simplify Data Centre design by enabling a high-performance, standards-based, unified fabric over 10 Gigabit Ethernet for LAN, SAN and cluster traffic. This enables consolidation and greater utilisation of what would traditionally be separate infrastructure, hence reducing the number of adapters and cables required and eliminating redundant switches;
- Nexus 2000 Series Fabric Extenders (FEX) provides a highly scalable and flexible server networking solution that inherits the functionality and benefits offered by upstream Nexus 5000 switches. In effect, the FEX act like remote line cards for a parent Nexus switch. Together, the Nexus 2000 Series Fabric Extenders and the parent switch form a distributed modular system, creating what is commonly referred to as the Virtual Access layer.

The Fabric extenders can be mixed and matched to a parent switch to provide several connectivity options as shown in Figure 4.2.2.

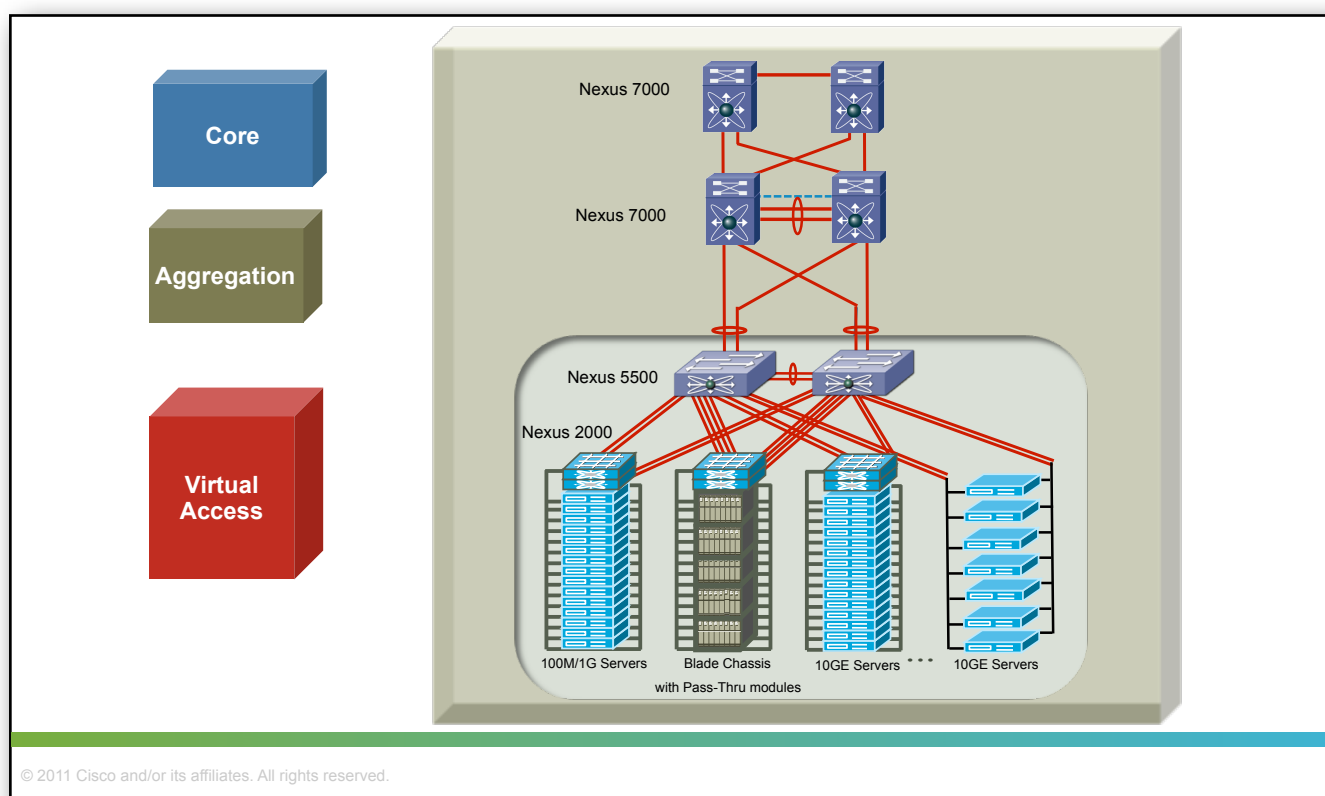


Figure 4.2.2 - Virtual Access Layer - Nexus 5000/2000

4.2.1 Virtual Machine Mobility and Management

Today's drive for virtualisation and mobility features has created a need for virtual machine aware networking solutions that deliver.

- Policy-based virtual machine networking;
- Network and security policy mobility with virtual machine migration;
- Management of both virtual and physical networking resources with a consistent set of tools.

The Nexus 1000V is an intelligent software switch that supports the same network configuration, security policy, diagnostic tools and operational models for physical and virtual servers. Pre-defined network policies can follow mobile virtual machines throughout the network to ensure proper connectivity, consistent access and security policies.

Some virtualisation technologies and clustering solutions require layer 2 Ethernet connectivity to function properly.

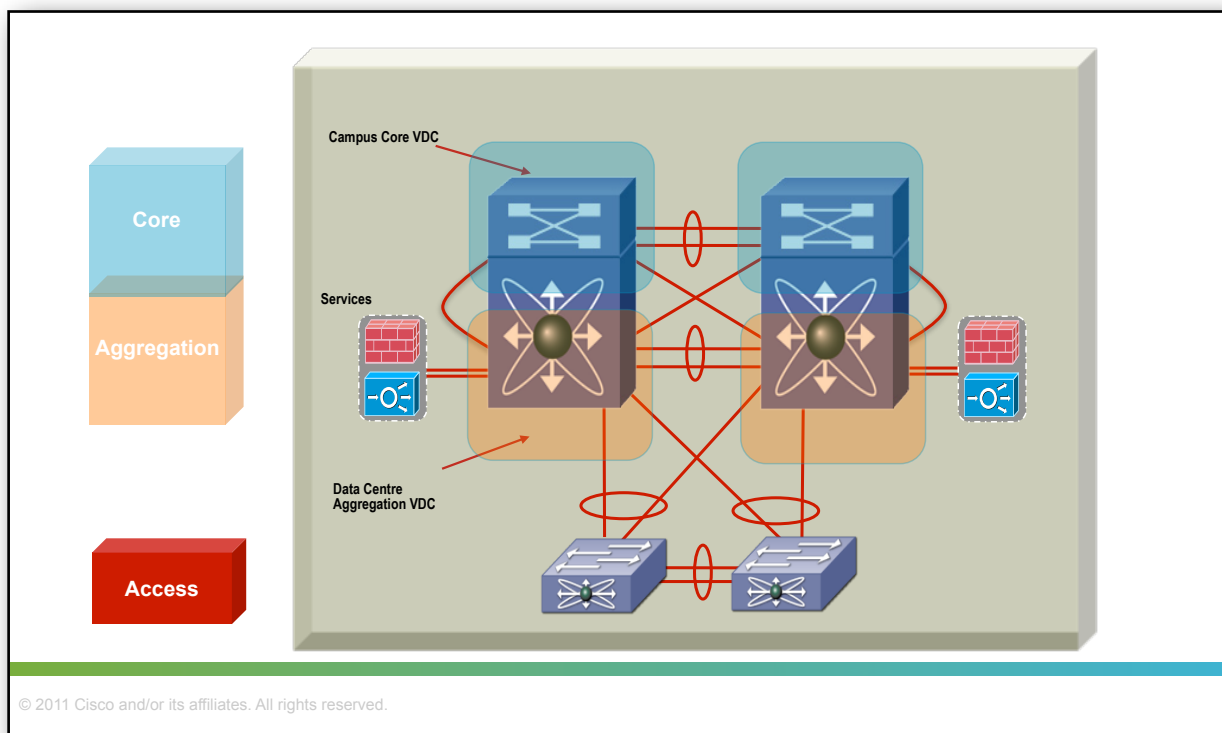
As these solutions become more popular, NHS organisations must consider how to move from the

traditional layer 3 Data Centre network model to a highly scalable layer 2 model. This shift drives the need for new technologies to manage large layer 2 network environments, including migration away from legacy loop management technologies.

Virtual PortChannels (vPCs) technology extends the PortChannel model to remove Spanning Tree Protocol as a loop management technology in large-scale layer 2 Ethernet networks. vPC provides enhanced system availability, full system bandwidth availability and rapid link-failure recovery.

A common consideration is how to realise efficiencies and cost benefits through consolidation of the Data Centre device footprint, i.e. reducing power consumption, cooling and space requirements.

One such solution is **Virtual Device Contexts (VDC)**. VDCs can be used to virtualise a core switch (Nexus 7000), hence presenting it as multiple logical devices. Each VDC can contain its own unique and independent configuration and can be assigned to physical ports allowing the hardware data plane to be virtualised as well. NHS organisations can use this feature to create a segmented, dual purpose platform performing different roles, e.g. the campus LAN core and Data Centre aggregation layers as shown in Figure 4.2.3.



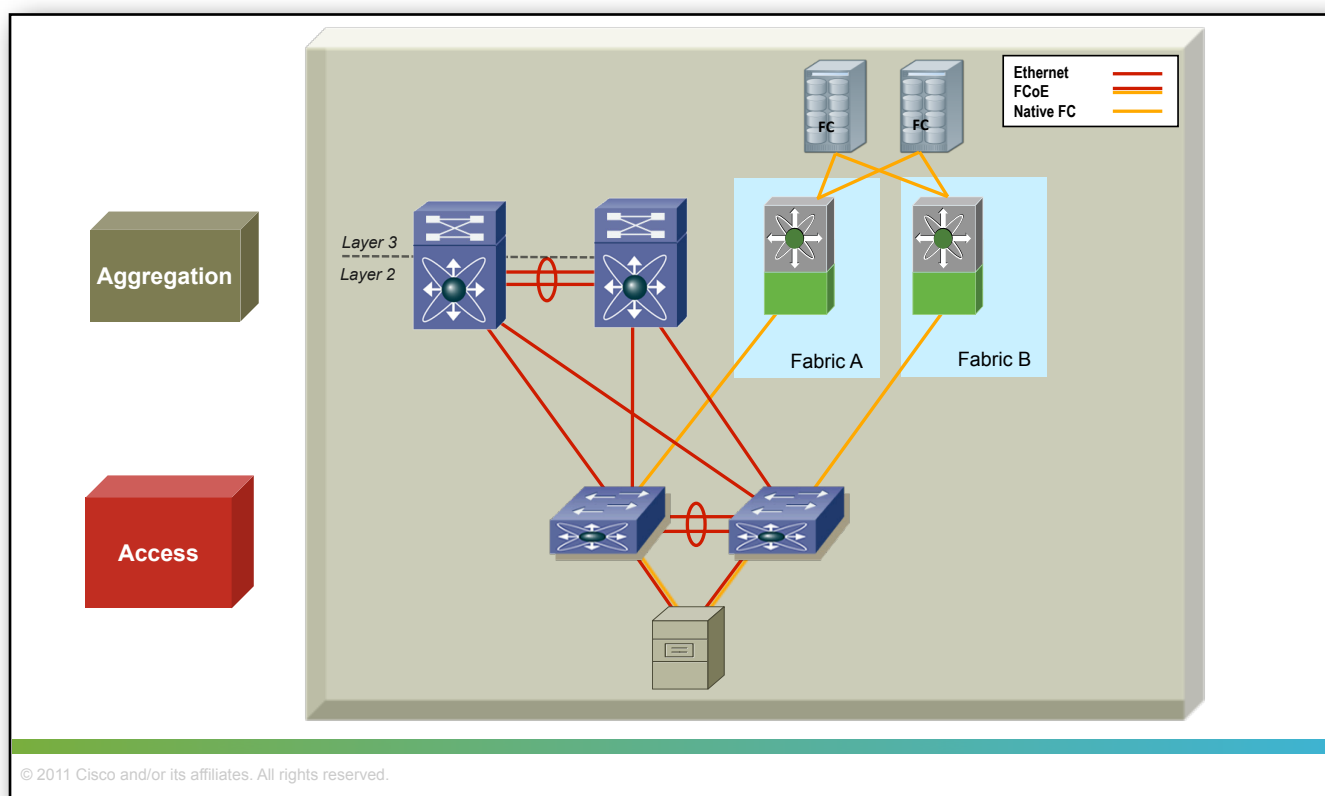
© 2011 Cisco and/or its affiliates. All rights reserved.

Figure 4.2.3 - Virtual Device Contexts (VDC)

Another key factor influencing the design in the Data Centre is the convergence of storage traffic onto the Ethernet network with a unified fabric approach. Today, Data Centres in NHS organisations often contain multiple networks, including an Ethernet network and a Fibre Channel SAN, traditionally using separate redundant interface modules for each, i.e. Ethernet network interface cards (NICs) and Fibre Channel interfaces.

Finally, it's clear that an avalanche of new Data Centre technology has meant that network and storage administrators need a uniform, easy way to carry out essential management operations. The Unified Fabric approach is supported by a converged management tool (Cisco Data Centre Network Manager) that can be licensed to manage a combination of SAN and LAN environments.

Fibre Channel over Ethernet (FCoE) supports Consolidation of I/O in the Data Centre (see Figure 4.2.4), allowing Fibre Channel and Ethernet networks to share a single, integrated infrastructure. This unified fabric approach over 10 Gigabit Ethernet for LAN, SAN, and cluster traffic enables consolidation of disparate networks using multiple interfaces.



© 2011 Cisco and/or its affiliates. All rights reserved.

Figure 4.2.4 - I/O Consolidation with FCoE

4.3 Unified Computing

Through an inherited legacy, today's IT organisations, including many in the NHS, assemble their Data Centre environments from individual components. This can lead to administrators spending significant amounts of time manually accomplishing basic integration tasks.

Gradually the Data Centre is transitioning away from the rigid, inflexible platforms that result and moving toward more flexible, integrated and virtualised environments.

Cisco has introduced the Unified Computing System (UCS)¹⁷, a multi-chassis next-generation platform that unites compute, network, storage access and virtualisation into a unified management domain. The system integrates a low-latency, 10 Gigabit Ethernet unified network fabric with enterprise-class servers. A fully populated logical view of UCS, is shown in figure 4.3.1.

The fabric interconnects have uplink connectivity to both the LAN and SAN. In a high availability configuration using two interconnects, both switches may be configured to actively switch traffic, thereby improving throughput. Meanwhile, the system's fabric extenders pass all network traffic to parent fabric interconnects, where it is processed and managed centrally.

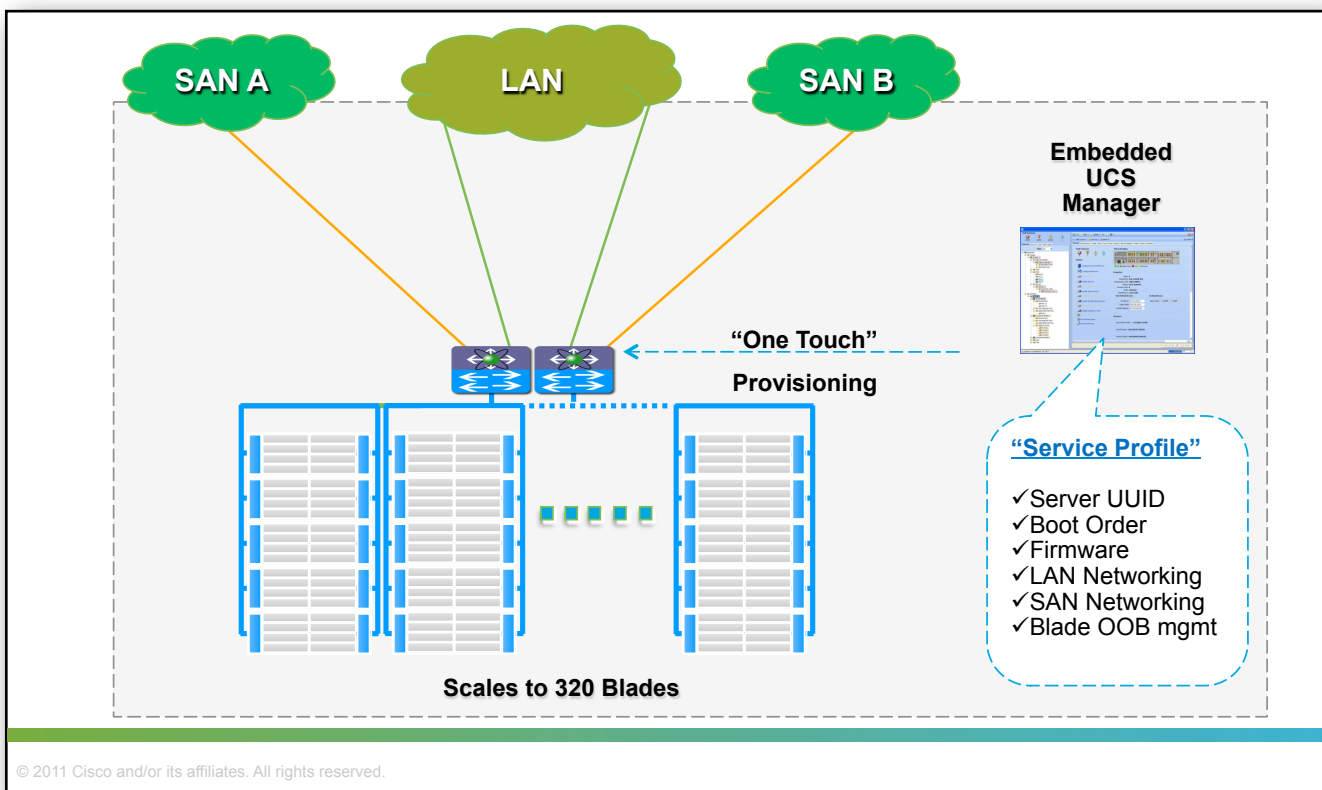


Figure 4.3.1 - UCS Logical Architecture

Cisco UCS Manager implements role and policy-based management using service profiles and templates. Infrastructure policies such as power and cooling, security, identity, hardware health and Ethernet/storage networking needed to deploy applications are encapsulated in the service profile.

Unified fabric technology is also embedded within UCS which, as described previously, reduces cost by eliminating the need for multiple sets of adapters, cables, and switches for LANs and SANs.

Figure 4.3.2 shows a basic UCS design for a small to medium size Data Centre, typical of NHS organisations.

In larger Data Centre environments such as those found in the largest Acute Hospitals, or perhaps when several organisations merge to form part of a shared services organisation, the requirements for high availability Director storage switches such as the Cisco MDS 9500 and Nexus 7000 should be considered. Organisations such as these may also be interested in deploying a Private Cloud architecture and/or virtualised multi-tenancy Data Centre architecture. It is critical to build this foundation on a robust, scalable platform.

In this design network connectivity to UCS servers is provided through Cisco UCS 6100 Series Fabric Interconnects, which separate the LAN and SAN traffic and hands it off to the corresponding upstream LAN and SAN core and aggregation switches.

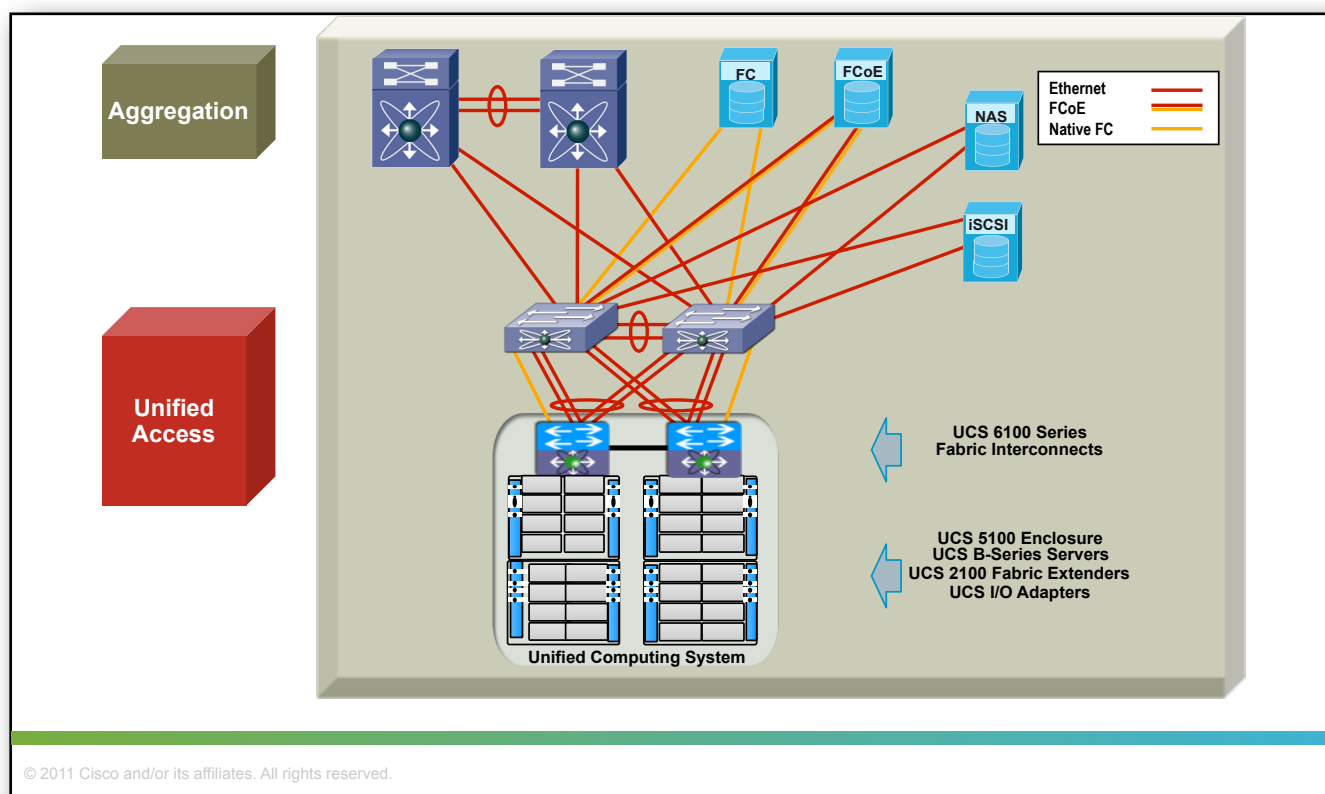


Figure 4.3.2 - UCS Design for Small/Medium Data Centre Environments

4.4 Unified Network Services

Layer 4-7 network services are an integral component of today's virtual Data Centre design. These services provide application acceleration and load balancing that improve user productivity, ensure optimal resource utilisation and monitor QoS. They also provide security services to isolate applications and resources in consolidated Data Centres and cloud environments which ensure compliance and reduce risk. Cisco Unified Network Services (UNS) delivers multiple services that can be configured and provisioned on demand and automatically. It relies on integration with Cisco's Unified Fabric and UCS resources to deliver the complete framework and services portfolio shown in Figure 4.4.1.

UNS includes a portfolio of Application Networking Services (ANS) products and technologies including:

- **Cisco Application Control Engine (ACE)** family, a suite of content switching and server load-balancing functions in a highly secure, virtualised platform;
 - **Cisco Wide Area Application Services (WAAS)**, a WAN optimisation and application acceleration solution that allows ICT departments to centralise servers and storage in the Data Centre while maintaining LAN-like application performance at the remote site.
- Other key services considerations for Data Centre environments are:
- **Security:** The Cisco ASA 5500 Series Adaptive Security Appliances are physical appliances that provide threat defence and highly secure communications services to stop attacks before they affect application availability or business continuity;
 - **The Virtual Security Gateway (VSG) for Cisco Nexus 1000V Series Switches** is a software firewall that enables the creation and enforcement of service policies at the virtual machine level;
 - **The Cisco Network Analysis Module** improves visibility into network performance to help manage and improve application delivery.

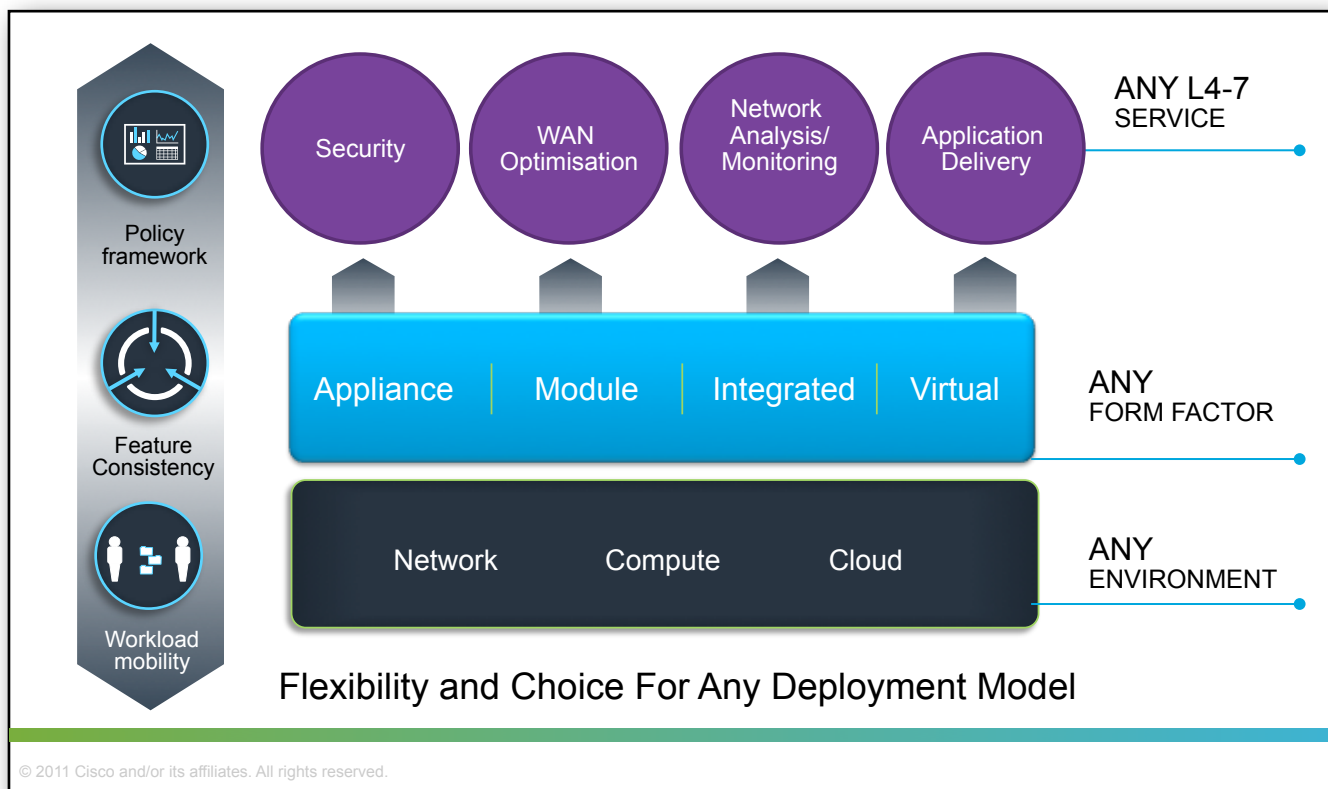


Figure 4.4.1 - Unified Network Services

4.5 Desktop Virtualisation Solutions

Today's ICT users are often just as likely to need application and data access from home PCs or mobile devices as they are from their office desktops. Rather than a place, the desktop has become an end-user environment that can be accessed anytime, anywhere, in a truly borderless way. This has led to an environment where multiple types of devices must be supported including smartphones and tablets, creating a dilemma for NHS ICT departments - how to meet business needs without compromising security, control, manageability or compliance.

Technologies that now fit under the accepted term of Virtual Desktop Infrastructure (VDI) have long been a feature of many NHS ICT services. VDI involves the centralising of employee desktops, applications and data in the Data Centre accessed by users with thin or thick clients. Most of today's VDI solutions run in a virtualised Data Centre environment to further improve manageability and security. Some of the principle advantages of VDI are:

- Simplified desktop management;
- Reduced total cost of ownership (TCO);
- Improved data security and compliance;
- Extended desktop hardware lifecycles;
- Extend business continuity and disaster recovery to enterprise desktops;
- Easier implementation of mobile access.

These advantages are well known but some of the associated challenges can include poor user experience, troublesome implementation across slower WAN links, remote site survivability and real time communications. Recent technology advances have made VDI a much more feasible option.

Figure 4.5.1 introduces Cisco's Virtual eXperience Infrastructure (VXI), a service-optimised desktop virtualisation platform that unifies virtual desktops, voice and video. The solution builds on the benefits of VDI by offering reliable and scalable, real time Unified Communications support.

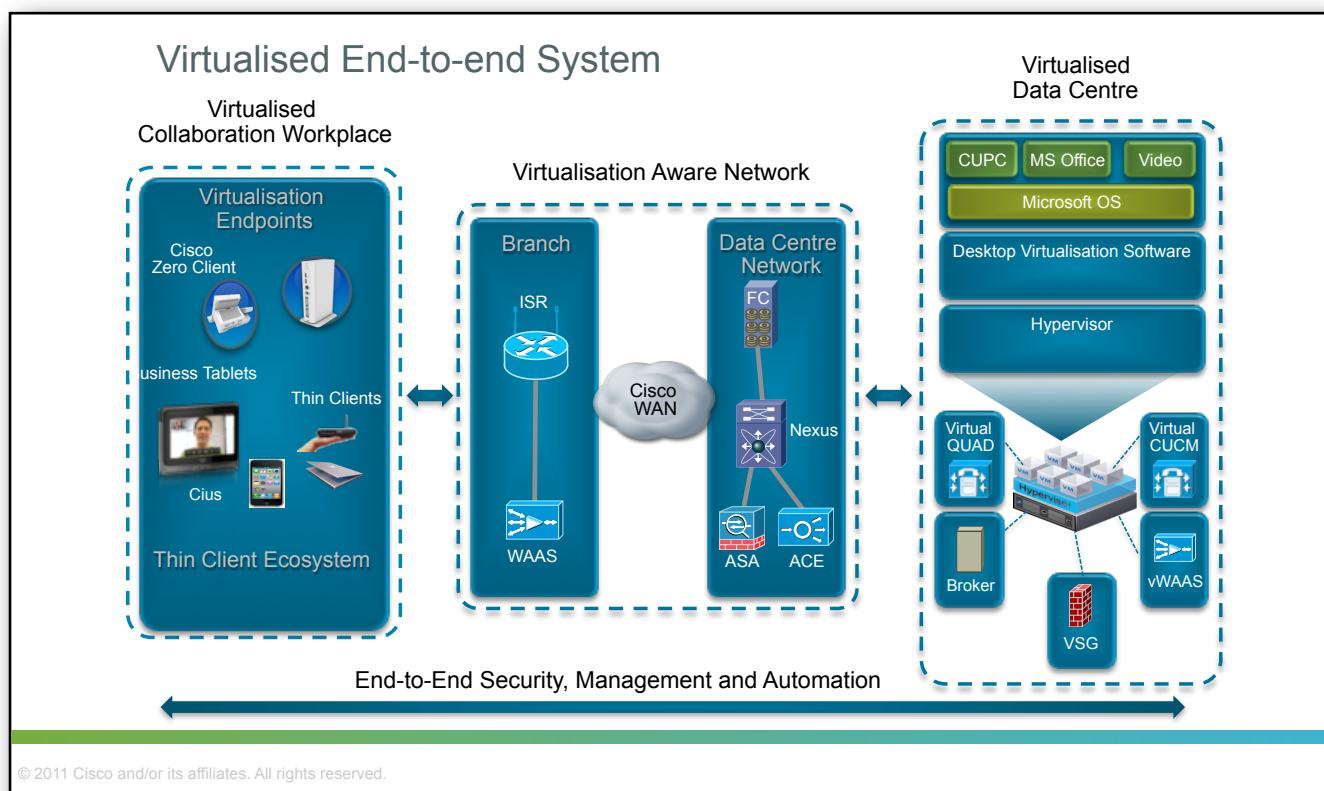


Figure 4.5.1 - Cisco VXI

Use cases in an NHS environment could include a remote care worker using a tablet device to access patient information during a home visit, the benefits being the provision of seamless access for the mobile user without compromised performance or security.

It should be noted that VXI spans all three of Cisco's logical architectures: the Virtualised Data Centre; the Virtualisation-Aware Network (based on the Cisco Borderless Networks architecture) and the Virtualised Collaborative Workspace (builds on the Cisco Collaboration architecture).

4.6 Disaster Recovery and Business Continuity

As ICT investments made by NHS organisations are aligned closer to business and clinical need, the dependence on highly available infrastructure and compute environments becomes ever more important. Convergence of voice and video amongst other applications dictate the need for a scalable, hierarchical network design, but in the Data Centre the need to support business continuity is perhaps even more critical. In the NHS today, reliable access to data is a key requirement for the delivery of patient care and operational efficiency, the Data Centre is at the very heart of that need.

Any business continuity strategy should include elements such as disaster avoidance, disaster recovery (DR) and a contingency plan. These elements are all essential in enabling organisations to apportion funds appropriately – and according to the size and nature of the business. Clearly, in the NHS this includes assessing the level of critical dependency for clinical and priority business services on the Data Centre environment itself. The business goal is to achieve redundancy, high availability, scalability and security – not just of the data itself but also the infrastructure which hosts data and provides access to it.

Responding to this need from a disaster avoidance perspective, many NHS organisations provide operations across two or more Data Centres providing scalability and resilience between them, whilst within the Data Centres themselves every effort is made to avoid single points of failure. At the same time, advances in server virtualisation and clustering technology are helping NHS organisations achieve increased business agility, resilience and efficiency within the Data Centre. Virtualisation can now provide affordable, simpler, infrastructure-level fault tolerance

across many applications. This dramatically simplifies DR planning, implementation and management, which not only reduces the costs but also lowers the risk that the DR plan will ultimately fail.

As these technologies are deployed across split-site or multiple Data Centres other challenges emerge such as ensuring the mobility and policy aspects of the virtualised environments as well as the integrity of storage. ICT managers are therefore tasked with provisioning and maintaining often complex virtualised environments across multiple sites.

Cisco Data Centre Interconnect (DCI) addresses these challenges and enables NHS organisations to meet business continuity and compliance objectives, offering benefits that include:

- Reduced business impact of localised and large disaster events;
- Improved productivity through enhanced availability;
- Meeting compliance objectives and improving data security.

DCI features technology that supports **LAN extension**, **SAN extension** and **Routing Optimisation** between Data Centres. When deployed strategically these features provide accelerated and secure data replication, server clustering and workload mobility between geographically dispersed Data Centre sites.

LAN Extension – A critical network design requirement for deployment of distributed virtualisation and cluster technologies is having all servers in the same layer 2 VLAN. Meeting this requirement often means extending VLANs over layer 3 networks supported by technologies such as Overlay Transport Virtualisation (OTV). The layer 2 connectivity provided by OTV coupled with the scoping of failure domains enables non-disruptive, cluster-based disaster recovery schemes as well as stateful workload mobility that are instrumental in providing disaster avoidance. The capability to move workloads transparently allows maintenance and change management processes to be carried out without requiring downtime. OTV is supported on the Cisco Nexus 7000 Series of switches.

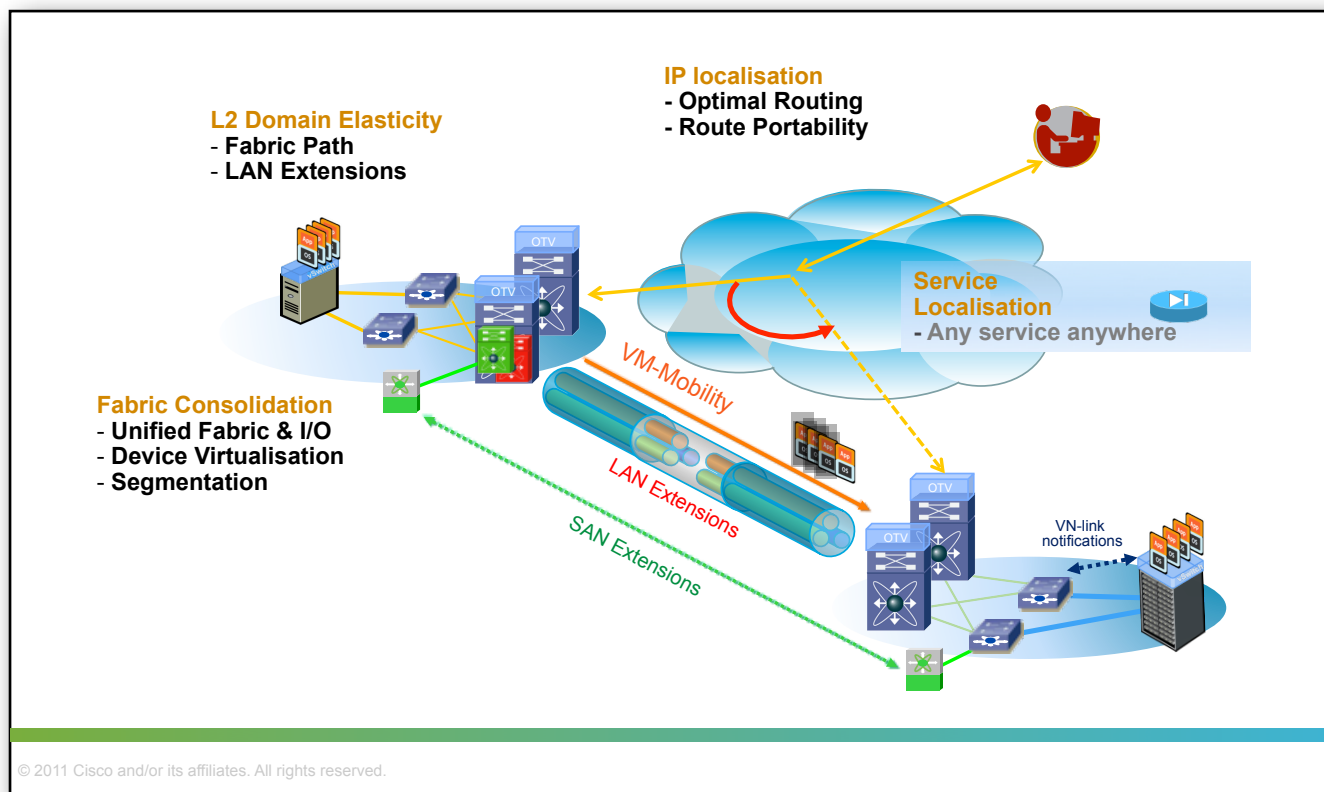


Figure 4.6.1 - Cisco Data Centre Interconnect

SAN Extension technology addresses the challenge of linking SANs in different Data Centres, sometimes over long distances. In virtualised environments there are added challenges such as the availability of virtual machine data on storage devices. For example as one virtual machine moves from one Data Centre to another, access to associated storage must also be considered. Several solutions are possible including:

- Shared storage across Data Centres;
- Storage following virtual machines/applications across Data Centres;
- Cached storage following virtual machines/applications, without moving the origin of the storage.

The Cisco MDS 9000 series of storage switches provide a range of integrated options for linking SANs together between sites in order to support disk or host based data replication, including long reach Fibre Channel and Fibre Channel over IP (FCIP). The MDS platform also delivers enhanced features such as disk

and tape write acceleration, which optimises the protocol exchanges over long distance links, delivering greatly improved performance for replication and tape back-up traffic. High performance hardware compression for IP links ensures maximum throughput for a given bandwidth and integrated IPsec security ensures the privacy of data while in transit between Data Centres.

Business Continence with application mobility across Data Centres is further enhanced by using the **Routing Optimisation** features in DCI. A primary requirement for application mobility is that the migrated virtual machine maintains all of its existing network connections after it has been moved to the secondary Data Centre. Traffic routing to and from the virtual machine must be optimised to maintain performance, independent of location.

Cisco DCI solutions take a systems based approach to put all these components together in a multi-site virtual Data Centre architecture, providing an optimised and resilient Data Centre design, a key component of any Business Continence strategy.

5. Collaboration ¹⁸

Part 1 of this Blueprint identifies the power of collaboration tools both within the NHS and across the wider health community, offering benefits such as responsiveness, time, and cost and carbon savings. However, collaboration tools are dependent on several aspects of ICT infrastructure and are themselves just one element of a much broader Unified Communications (UC) portfolio. This rich set of voice, video, collaboration and messaging services brings together all of the communications requirements of an NHS organisation, enabling both service and business transformation.

Collaboration is the third Cisco logical architecture. It is a collective term that includes the entire UC environment, from the basic converged voice network, to advanced services such as:

- Video – truly integrated video in the communications environment such that as long as each endpoint is video capable, a video call is

established in the same way as making a regular telephone call; Presence – instant knowledge of a person's availability, reachability, location and even skills;

- Collaboration services – share documents or other information with simultaneous voice, video and instant messaging – ideal in scenarios such as virtual case conferences and scheduled meetings;
- Mobility – intelligent UC system services extending reach and applications to mobile staff resulting in improved availability and agility;
- Messaging – either simple voicemail or unified messaging where e-mail, voicemail and fax can be integrated. This enables the delivery of any message to clinical or medical staff on the move at any time and on any communications device.

Figure 5.1.1 shows a logical view of the UC architecture overlaid on a campus care network. The following sections examine some of the essential requirements and the individual solution components.

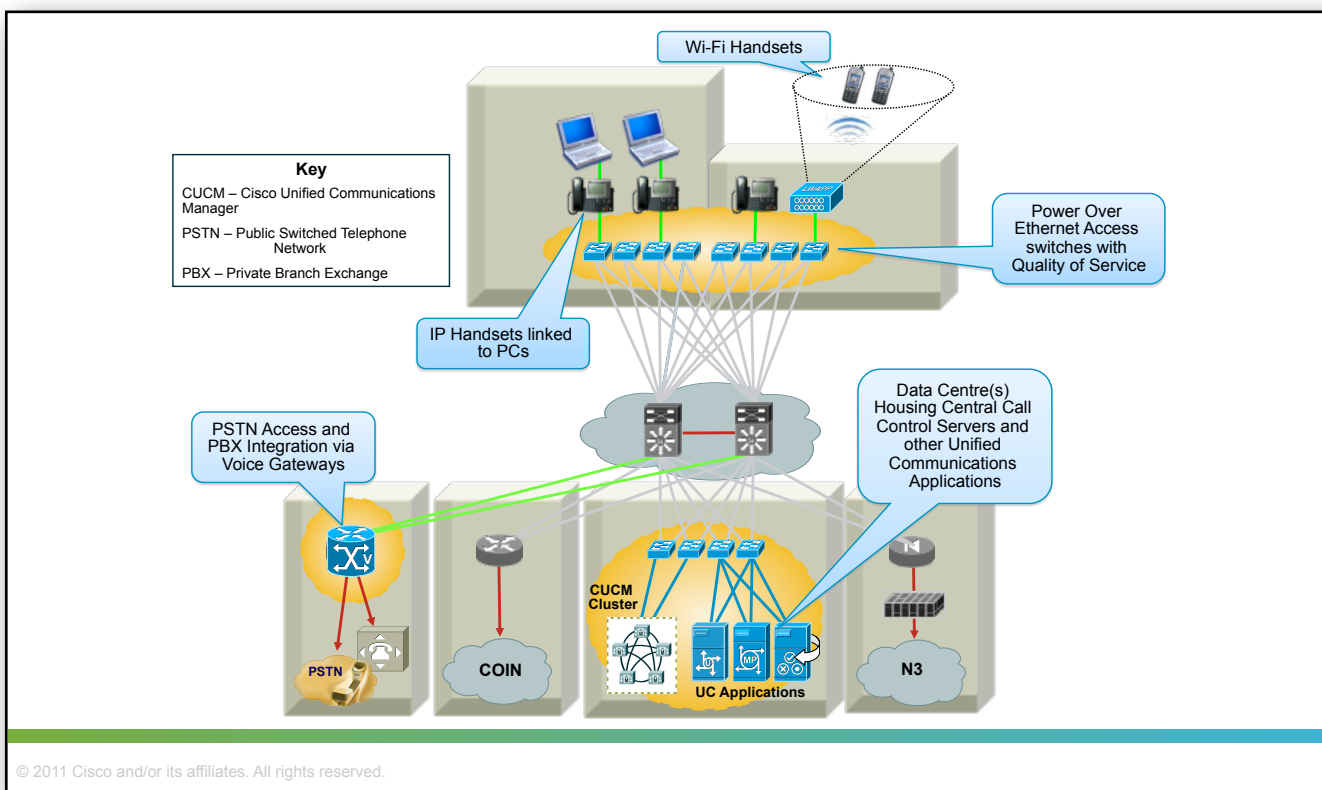


Figure 5.1.1 - Cisco Unified Communications Architecture

5.1 Unified Communications Essentials

When comparing a UC environment to traditional telephony solutions, the IP network can be considered the switching matrix of the UC system and critical to its operation. It is therefore a fundamental requirement that the network is designed and constructed with high availability, security and performance in mind. Design considerations include:

- Overall availability – telephony systems often quote five nines (99.999%) as the expected uptime (not including scheduled downtime);
- Network link redundancy – automatic service restoration within a second is highly desirable ensuring that calls in progress remain intact;
- Device redundancy – single or multiple depending on organisational service level requirements;
- Power – key components should be protected by Uninterruptible Power Supplies (UPS), Redundant Power Supplies (RPS) and/or generators;
- Latency/Jitter – end to end latency should be less than 150ms with jitter reduced to an absolute minimum;
- Security – physical and network based, including denial of service;
- Application prioritisation – QoS tools ensure that the most essential applications are prioritised over less critical ones;
- Bandwidth – adequate bandwidth should be available at all times including during partial network failures;
- Service Provider – e.g. Public Switched Telephone Network (PSTN), provider WAN. Ensuring remote site survivability.

Within the IP network certain services are required for the successful operation of the UC system. Services such as Dynamic Host Configuration Protocol (DHCP – for automated IP address allocation), Domain Name Service (DNS – for name to IP address resolution) and Trivial File Transfer Protocol (TFTP – for download of device configuration and firmware) can be combined to enable zero touch deployment of telephony handsets.

Power over Ethernet (PoE) is often considered to be an essential network service when considering UC deployments whereby the handset or terminal derives its power from the Ethernet switch that it is connected to. Without this method of powering the telephony devices, an external power supply (or power injector) would be required for each handset.

Whilst these requirements are extensive they should be put in perspective, UC is merely another application running over the network of which there will be many that the Trust relies upon for its continued operation. Most of the considerations listed will be similar for other clinical and business critical applications. In the architecture this is reflected by the use of intelligent re-usable services.

Quality of Service (QoS) – A thorough description is outside of the scope of this document, however section 3.1.3 has listed areas for consideration. To re-cap, features needed in infrastructure include traffic prioritisation and the avoidance of loss, delay and jitter. Using an analogy to compare the application traffic on a network to traffic on a motorway helps to understand the basic challenges more easily.

By default any vehicle can use any lane and therefore in times of congestion all traffic will be affected equally with associated consequences. If however one lane (an express lane) is reserved for important vehicles only and congestion occurs, only low priority vehicles will be affected allowing the important ones to pass freely. Similarly in the network the ‘express lane’ is used to protect sensitive traffic such as Voice over IP which has very tight constraints with respect to delays and dropped packets.

In practice, networks are designed to have several different ‘lanes’ of traffic with different attributes tailored to the different application demands, thereby creating a comprehensive prioritisation model.

Call Admission Control (CAC) – is used to ensure that the ‘express lane’ does not become oversubscribed and congested. For example, each time a new voice call needs to be established, a request must be made to ensure that the ‘express lane’ has the required capacity. If not then the call may be refused or maybe re-routed. Call admission control mechanisms fall into one two main categories:

- **Topology-unaware CAC** – based on a static configuration within the call processing agent;
- **Topology-aware CAC** – based on communication between the call processing agent and the network about the available resources.

Topology-unaware CAC is the simplest to understand and deploy and supports most customer requirements.

For example, in a distributed environment, after assigning all the devices located at each branch office to the corresponding site entity, the administrator usually configures a maximum number of calls (i.e. bandwidth) to be allowed in or out of that site. Each time a new call is requested, the call processing agent checks the sites to which the originating and terminating endpoints belong, and verifies whether there are available resources to place the call. If the check succeeds, the call is established and the counters for both sites are decremented. If the check fails, the call processing agent can decide how to handle the call based on a pre-configured policy. For example, it could send a network-busy signal to the caller device, or it could attempt to re-route the call over a PSTN connection.

Topology-aware CAC is defined as; any mechanism aimed at limiting the number of simultaneous calls across networks that can be applied to any network topology and can dynamically adjust to topology changes. The Resource Reservation Protocol (RSVP) is the first significant industry-standard signalling protocol that enables an application to reserve bandwidth dynamically across an IP network.

Medianet – As video becomes pervasive in NHS Trusts and more video devices are used, new demands are placed on the network and traditional IP networks need to evolve to accommodate these changes. Cisco Medianet is an end-to-end IP architecture that helps to enable pervasive media experiences (see section 3.4 for a description of Medianet).

Translation Services – During call setup, end-points often negotiate what speed, compression and codec to be used during the call. Translation services exist to ensure that end-points without common sets can communicate. For example, transcoding allows endpoints to communicate even if they are using different standards-based codecs (G.711, G.729 etc) and similar principles exist for speed, protocols and other attributes.

All of the above are essential network considerations for the support of a reliable UC environment.

5.2 Call Control

An IP based UC solution might initially be viewed as complex due to its distributed nature but in fact can be likened to that of a standard PBX. The comparison is represented in figure 5.2.1.

The intelligent ‘brain’ that provides dial tone and manages call processing and signalling exchange is now a server based software application (Cisco Unified Communications Manager). Multiple servers can be ‘clustered’ creating a single, highly available virtual service that delivers call control services across all IP connected sites of an NHS organisation hence simplifying management. Intelligent clustering means that servers can be deployed across multiple IP connected physical locations reducing the effect of any equipment or site related failure.

The switching matrix is the IP network itself with the voice path connections now being Real Time Protocol (RTP) connections between the endpoints or terminals over the IP network.

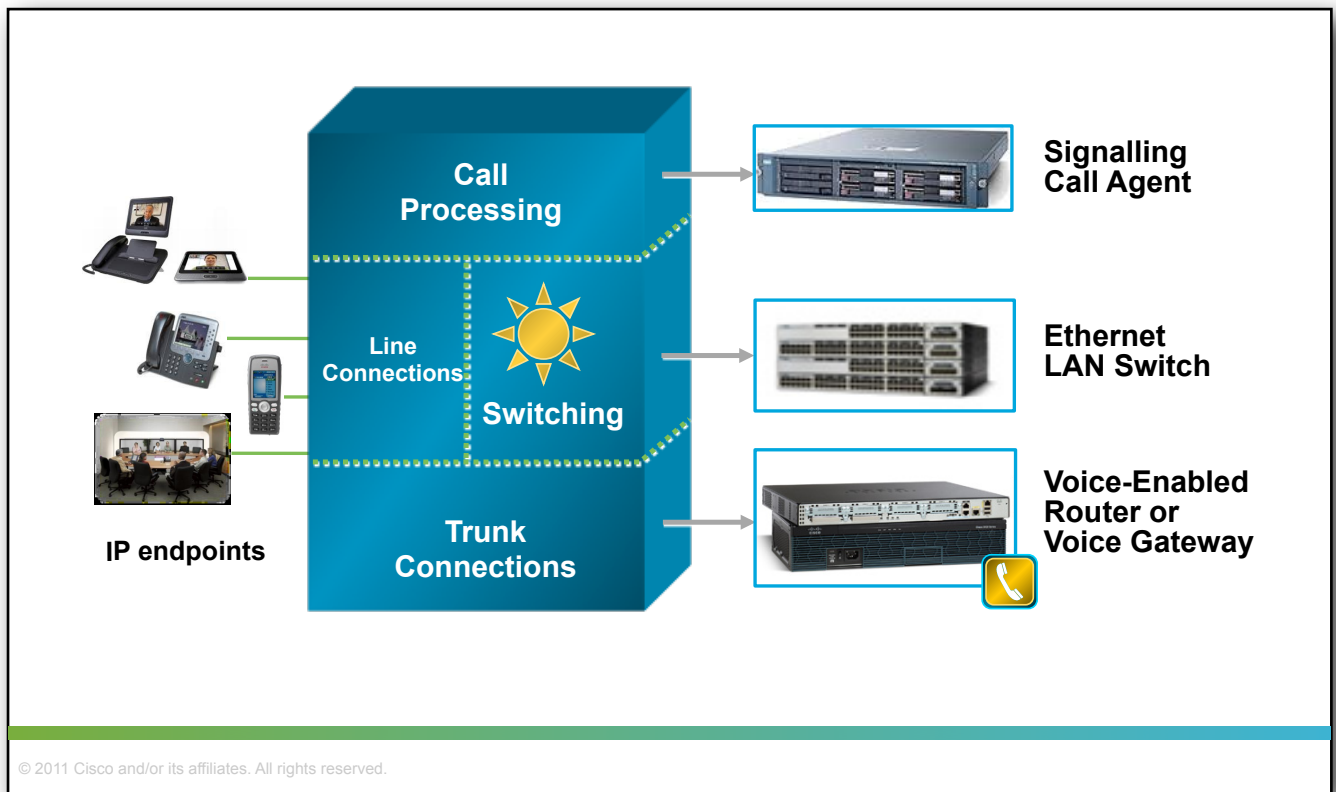


Figure 5.2.1 - Server Based Call Processing

Trunk connections to the PSTN, other telephone switches or telephony services platforms (such as voicemail) are provided using voice gateways, (or voice enabled routers) converting the IP connection to a traditional one like Integrated Services Digital Network (ISDN). Where the interconnecting systems support common, standards based IP protocols such as Session Initiation Protocol (SIP) or H.323, trunks can be achieved by direct connection over the IP network. This simplifies the interconnection strategy allowing any component to connect to any other component without having to add interface cards, shelves or similar hardware.

Finally the endpoints or terminals can take different formats, some will be familiar in form with a traditional handset and dial pad. Others could be integrated software applications such as a softphone on a PC or maybe integrated into a piece of mobile medical equipment. Wireless handsets and tablet devices are also available to support mobility and instant reach.

5.3 Real-Time Video Services

Integration of video terminals into the Unified Communications platform introduces a concept where all devices share a common numbering scheme. Users now dial 'familiar' extension numbers to make video calls and potentially have access to the same telephony features such as hold, transfer etc. during a call. Additional services enjoyed today by IP telephony users such as corporate directory access can also be made available to video users making the use of video telephony transparent to the user. The advantages of integrating video into a UC platform are:

- A single, uniform dial plan and centralised management;
- A single point of billing for records and administration;
- Calls between any communications device;
- Integrated scheduling of resources;
- UC application support, e.g. voicemail or contact centre across all devices;
- Presence based information for all devices;
- Global CAC mechanism based on real network performance.

Integration of video services into the UC platform has broadened the reach of video communications, enabling a new generation of video telephony users from PC desktop based clients, tablet devices, 3G mobile phone users as well as traditional video conferencing terminals through to High Definition TelePresence¹⁹ systems. The benefits to the NHS include scaling expertise as well as remote working solutions for home or mobile workers.

5.4 Collaboration Services

Within the local health community many meetings take place in a central location with all attendees travelling to that site. Whilst this is most true of distributed organisations, the impact will be felt across the NHS as health communities evolve. Travelling to meetings presents a number of inefficiencies including unproductive time, travel costs and the carbon footprint impact of multiple journeys.

It is now possible to schedule virtual, collaborative meetings using standard calendaring tools that can be attended from anywhere with access to a phone. The conference can be extended to include document sharing, Instant Messenger chat and video conferencing. Service providers such as Cisco WebEx offer hosted collaboration services which are particularly attractive for:

- Small NHS organisations;
- Where demands are variable;
- Where the organisation doesn't have the in house skills or desire to maintain the system;
- Where no IP Telephony exists;
- Where rental is more favourable than capital expenditure.

Whilst a secured environment is provided there may be some instances where the hosting of certain content is deemed inappropriate in the NHS. For this reason on-premise, customer owned solutions such as Cisco MeetingPlace are also available. A customer owned system offers much tighter control of service costs, utilisation and security with all data being hosted on components within the organisation.

5.5 Presence and Instant Messaging

Presence is the ability to establish the 'availability' of a person or resource at any given time and builds upon Instant Messenger (IM) technology where it is possible to create 'buddy lists' and check availability in real time. This normally identifies a high level availability status – typically showing:

- Available (when they are online);
- Idle (not actively using their computer);
- Busy (in a meeting or on the phone);
- DND (Do Not Disturb).

Additional information on someone's availability can be provided including their location or perhaps clarifying why they are 'Busy', as well as information automatically derived from an electronic diary or the telephone system. Within the NHS, this technology has significant potential to address challenges faced by healthcare professionals on a daily basis including:

- Locating and communicating with individuals by name;
- Locating and communicating with individuals by role and proximity;
- Locating and communicating with individuals by skill and proximity;
- Locating essential equipment by availability and proximity.

Confederation between presence aware systems allows users to broaden their view outside of a single system. These systems can exchange status information, ideally using standard protocols allowing a user in one NHS organisation to see the availability of individuals in another NHS or partner organisation. The users are able to communicate using IM and then escalate into a voice, video and collaboration session seamlessly.

On the client side, Cisco brings these functions together with applications such as Cisco Unified Personal Communicator (CUPC) and Cisco Jabber. The clients are available for PC, tablet and other mobile devices.

¹⁹ Cisco Telepresence – <http://www.cisco.com/go/telepresence>

5.6 Messaging

There are many different ways to communicate using messaging systems across the NHS including email, voicemail, fax and Short Message Service (SMS). However these systems often exist in silos resulting in the user having to interrogate each one individually.

Unified Messaging (UM) combines messaging silos enabling the user to access all of their messages from a device or application of their choice. This could include phones, tablets or a range of applications including email clients or UC clients. UM features a server-based model meaning that users can set-up rules or policies to automatically handle messages and take actions based on chosen criteria. The user receives the messages in the same format regardless of their current device or application. Once read, the message is marked as such and is reflected across all devices. Messages can be replied to, forwarded or deleted as desired, regardless of the original medium. Cisco supports Unified Messaging in its Unity and Unity Connection platforms.

Integrated Messaging involves the user having a separate email mailbox and voicemail mailbox. The user interrogates email and voicemail systems from their email client resulting in both message types being readable in a single desktop application. Not all UM features are available to the user due to the separate message systems, however the benefits are less impact on e-mail servers and simpler integration. Cisco's Unity Connection can deliver an integrated messaging solution.

5.7 Mobility

User mobility is an ever-increasing requirement within the NHS, enabling staff to be productive whilst away from a desk and the UC system should be aware of their changing mobile environment allowing users to communicate seamlessly. WiFi enabled smartphones are enabling higher degrees of user mobility combined with the delivery of features such as hold, conference and enterprise level caller ID.

Fixed to mobile convergence or call handoff between fixed and mobile networks is a rapidly developing solution allowing the UC system to move a call from a fixed or WiFi handset to a mobile handset and vice versa without user intervention or interruption of the call. For example, manual handoff allows the user to make a call from their deskphone and then, mid-call

move the call to their mobile handset enabling them to leave the office and continue the call. Meanwhile, automatic handoff enables the user to roam within and between locations, while the UC system intelligently tracks their connectivity and moves the call accordingly.

5.8 Attendant Services

The adoption of user mobility and presence awareness services offer telephone operators much greater visibility of the users they are trying to connect calls to. Automated attendant services, UM (or Voicemail) and mobility services should be considered to increase service efficiency and enhance the telephone operator's effectiveness.

A speech recognition based automated attendant system can be integrated with an organisation's directory. This enables any caller (internal or external) to request connection to any employee based on name, job role, department, location or a combination thereof. Speech recognition technology has matured significantly over recent years making this a very effective solution.

5.9 Patient & Customer Contact

IP Contact Centre technology is delivering new and improved services within the NHS providing a higher quality service when handling enquiries from employees or patients. Mobility of call handlers combined with presence (and availability) awareness offers greater flexibility in service delivery.

Almost any environment where large volumes of calls or enquiries are experienced can benefit by applying a defined workflow to enquiry resolution. Callers receive a consistently high and predictable level of service, which can be measured, analysed and ultimately refined to ensure it continually meets the needs of the caller and the NHS organisation.

Cisco offers a selection of IP Contact Centre solutions appropriate to size and feature requirements.

5.10 'Consumerisation'

Many UK NHS organisations are reporting increasing trends in the use of consumer devices, including tablets, often referred to as 'consumerisation'. As a result ICT departments are faced with the challenge of how to support these otherwise 'unauthorised' devices, which presents a need for balance between flexibility and control.

Security is of course the paramount concern but the decision process should begin with the UC solution given its increasing emphasis on mobile communication from a variety of endpoints.

Some points to consider include:

Enterprise-class control: the UC solution should include a comprehensive control policy that provides flexible yet secure access to authorised applications from consumer devices. The network is the most effective place to locate a security framework (with features such as session encryption, intrusion prevention and spam blocking), as well as highly granular access control that can trace, identify and grant or deny access to any resource or service in real time.

User choice: In addition to smartphones, the Cisco UC solution supports many leading consumer tablet devices but also Cisco's business-grade Cius²⁰ device. This support allows you to offer a "best-of-both-worlds" combination of personal user device choice together with an optimised collaboration experience, increasing the chances of adoption and compliance as well as productivity for the Trust.

New application models: The advent of user-accessible application stores that has accompanied consumer devices has also challenged ICT, more used to controlled or "standard-image" provisioning. Once again, rather than blocking progress it is possible to accommodate this new model by allowing users to access a secure, custom "enterprise app store" to download approved applications on a personalised basis. The Cisco UC Solution supports this model with the Cius tablet.

Future device support: Consumer technology evolves rapidly, so the UC solution must be able to embrace new devices and operating systems as they emerge. Cisco's collaboration architecture was specifically designed with a client services framework – a software abstraction layer that allows rich programmatic access to core UC services from any device or operating system – offering reassurance for future support.

In summary, Cisco's approach is to offer support for 'consumerisation' or Bring Your Own Device (BYOD), but also offers the business grade Cius tablet as an alternative for those organisations who want to maintain their own device pool. Connectivity considerations for such devices are discussed in more detail in sections 3.3 and 3.4 of this document. Cisco would be happy to provide further advice as required to this developing area.

5.11 Social Software

Over recent years many organisations have evolved from traditional file server approaches to sharing information, to newer tools such as Wiki's Blogs and Really Simple Syndication (RSS) Feeds. However, the challenges that have emerged include lack of adoption, often due to a lack of uniform deployment. As Internet based and consumer driven social software tools become ever more popular, industry is considering how to realise the benefits that such tools bring without the associated risks, in particular security concerns. The logical place to start is the UC environment because the infrastructure is already in place to facilitate a wide variety of social interactions, but most importantly under policy control.

Cisco offers business-oriented social software applications that supplement the collaboration environment.

- Cisco Quad – enables individuals and teams to build communities in order to connect, share, learn and collaborate;
- Cisco Show and Share – a webcasting and video sharing application that allows organisations to create secure video communities to share ideas and expertise.

²⁰ Cisco Cius tablet – <http://www.cisco.com/go/cius>

The Cisco solution employs elements of consumer-style social networking, context, profiling, and semantic search, together with pre-integrated “click-to-collaborate” functions using IM, conferencing, voice and social video on a variety of devices and environments.

Security and trust are of utmost importance. In addition to standard authentication, authorisation and accounting (AAA) security and encryption provision, communities can be defined as either open or restricted and functions within the social network are role-based and rule directed.

5.12 N3 Voice and Video Services

Existing NHS voice requirements are varied and complex, generally being procured and managed locally. There is an alternative offering for NHS organisations whereby N3 can offer a fully resilient national NHS IP voice switching platform with associated services. This enables NHS organisations to integrate their existing voice estates, giving them access to new and cost effective communication solutions. The N3 Voice Service can also offer the advantage of a fully managed service to the handset.

Two main service categories exist at present which offer complimentary services for both pure IP communications deployments and legacy systems alike:

- **The N3 Local Gateway Service** provides access from existing Trust voice infrastructure to the N3 Voice Services²¹ platform. This access enables free on-net calls to other N3 voice users, and access to the N3 Fixed-Mobile Gateway Service;
- **The N3 Hosted Voice Service** removes the need for on-site voice switches and equipment, providing centrally managed IP telephony handsets and associated services. It can cater for future organisational change, and offers the same free on-net calls and reduced tariff for fixed to mobile calls as the N3 Local Gateway Service.

The N3 Voice service is based on a hosted Cisco Unified Communications platform.

The N3 Managed Video Service²² is a fully managed Video Conferencing service offering all the benefits of existing systems with the addition of a web based management tool (N3 Meeting Manager), multipoint capability and endpoint monitoring.

The service offers efficiencies to NHS organisations. Firstly, because it’s built into the N3 network it negates the need for each organisation to buy expensive bridge equipment to enable the service. Secondly, it extends the communications and collaboration capability of remote staff, hence saving on time, cost and carbon.

The N3 Managed Video Conferencing Service is hosted on Cisco (formerly Tandberg) infrastructure.

Whilst all information is believed to be accurate at time of writing, readers are encouraged to check with N3SP in case of changes to the portfolio of voice and video services.

²¹ N3 Voice Services - <http://www.n3.nhs.uk/ProductsandServices/N3Applications/VoiceServices/default.cfm>

²² N3 Managed Video - <http://www.n3.nhs.uk/ProductsandServices/N3Applications/VideoConferencing/N3VideoConferencingManagedService.cfm>

6. Integrating Patient-Centric Information

One of the most cherished ambitions of any healthcare organisation is to achieve truly integrated and patient-centric information, yet it also presents one of the biggest challenges. There are many opportunities in the NHS to take a fresh look at this challenge such as – but not limited to:

- Acquisitions and mergers;
- The move to integrated care;
- Community approach;
- System replacement.

Standards for interoperability are constantly evolving and hence offer a new approach to healthcare information exchange. Integrating the Healthcare Enterprise (IHE)²³ is an industry initiative that promotes the co-ordinated use of existing healthcare standards such as HL7 and DICOM and offers a set of profiles that help establish communication standards for healthcare information exchange.

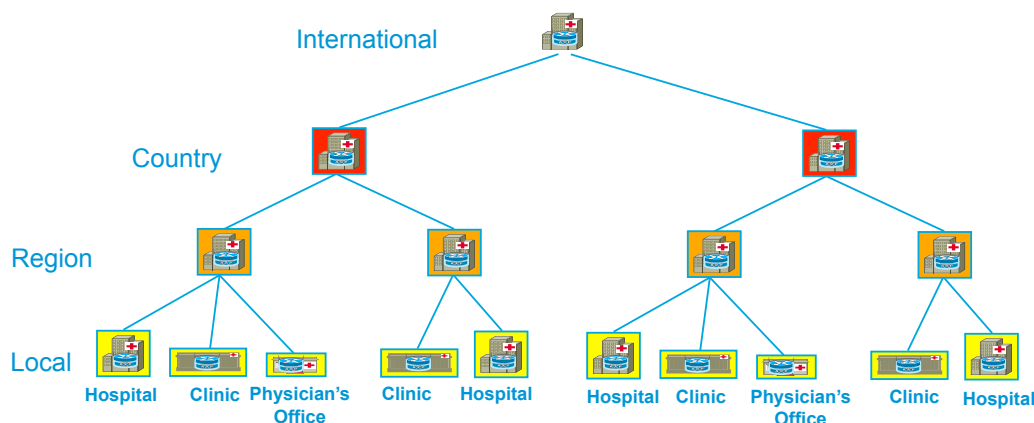
Cisco supports the IHE approach through its Medical Data Exchange Solution (MDES)²⁴. MDES is an infrastructure based solution, deployed in routing platforms or the Unified Computing System. The federated nature of MDES uses common standard patient indexing functionality such that information remains local to the healthcare application while indexing registries are copied across the domains of the solution. Hence, when a patient demographic query is made, all known information can be represented in a single patient-centric view.

In summary the benefits that MDES offers are:

- Enables real-time sharing of critical information;
- Enables hospitals to deploy clinical and business applications that most suit their needs;
- Leverages the existing infrastructure to provide seamless data exchange, translation and message conversion;
- Provides interoperability access and exchange.

Cisco would be happy to discuss this emerging area in more detail with any interested customers.

- Interoperability based on a federated concept
- Avoids copying all data centrally
- Retains data where it was originally produced
- Data is also stored at a regional level for redundancy purposes (orange level)



© 2011 Cisco and/or its affiliates. All rights reserved.

Figure 6.1 - MDES Federated Architecture

²³ Integrating the Healthcare Enterprise – <http://www.ihe.net>

²⁴ MDES – http://www.cisco.com/web/strategy/healthcare/medical_data_exchange_solution.html

7. Approaches to Shared Services

The intention of this document has been to offer guidance on an architectural approach to ICT for NHS organisations as well as providing technical reference material. Hence, the broader NHS considerations such as regional and national networks have largely been treated as out of scope. However, this section does consider some of the benefits and options for approaches to shared services within the NHS.

7.1 What are Shared Services ?

‘Shared services’ is a collective term that applies when two or more groups or organisations share the funding for, and/or provisioning of, a particular application or service.

The benefits of this approach include cost savings and operational efficiencies associated with the consolidation and centralisation of services and the operational benefits of standardisation.

There are already many examples of shared services in the NHS both nationally and regionally. These include National Programme applications and local Health Informatics Services that offer a centralised ICT service.

From a network infrastructure perspective, the most obvious NHS shared service is the Community of Interest Network (COIN). In the COIN model, a service provider delivers the shared network platform and offers inter-site connectivity. The service providers can offer trusted separation between members of the COIN through the use of protocols such as MPLS. In addition more robust separation can be provided using an encryption overlay as described earlier in this document. An example of when this may be required is when transmitting Person Identifiable Data (PID).

Shared services are often referred to using other terminology including:

Hosted Services – where services are hosted by a provider and offered over the Internet or private network connection; N3 voice and video services are good examples in the NHS;

Public Cloud – on-demand services, typically available across the Internet, offering benefits such as agility, usage-based pricing and very low costs due to economies of scale;

Private Cloud – deriving similar benefits to Public Cloud but in a controlled and sometimes wholly-owned manner. This approach mitigates concerns over security and performance. N3 may be considered a first-generation Private Cloud.

7.2 Current and Future Developments

Efficiencies and flexibility make shared services an appealing model for many public sector organisations and Cloud models for ICT consumption are expected to become more prevalent.

In the UK there is a drive to reduce costs and increase collaboration across agencies. The Public Services Network (PSN) programme is aimed at creating a ‘network of networks’ for the UK public sector that enables efficiencies and provides a platform for inter-agency working.

At the time of writing, policy with respect to PSN and N3 is still being developed.

Meanwhile, other options still exist. The development of N3 and privately provided COINs have the ability to develop more feature-rich service offerings, while there are emerging examples of Private Cloud models. Other specific focus projects such as the consolidation of services, Data Centres and infrastructure between NHS organisations is becoming commonplace.

All of these shared service options present opportunities to consolidate and collaborate either between NHS organisations or with other public sector entities where appropriate. In addition, larger organisations, or perhaps existing Health Informatics Services, can begin to build hosted offerings for smaller NHS organisations such as Clinical Commissioning Groups as they emerge. In this case, services that could be offered include compute and collaboration services in conjunction with established offerings such as those offered by N3.

This is clearly an area of rapid development and Cisco would be pleased to assist any customers considering options for their NHS organisation.

8. ICT at the Heart of NHS Reform

The overriding objective of these documents has been to demonstrate how a structured and business-led approach to ICT investment will bring the best value back to NHS organisations. Through both documents it has considered:

1. How ICT can become an enabler;
2. A broader perspective on emerging healthcare trends;
3. How the challenges facing NHS organisations can be summarised in three main categories:
 - a. Operational excellence and efficiency;
 - b. Reform and reconfiguration;
 - c. Patient centric care.
4. ICT solutions that respond directly to each of these categories;
5. Why an architectural approach is essential;
6. The definition of architectural stages:
 - a. Conceptual (business to ICT linkage);
 - b. Logical (solution sets);
 - c. Technical (deployment options).
7. Technical reference diagrams for ICT departments to follow.

By adopting the **‘Plan Down, build Up’** approach, NHS organisations can align ICT directly to the business goals. Taken as a whole the documents form a blueprint for NHS organisations to realise greater value from their ICT investments.

We encourage the application of C-NAB principles for any NHS organisation. Cisco – and its partners – would be very happy to discuss any or all aspects of this blueprint with interested customers to help understand how it might be applied in their environment. Please consult Appendix A for contact details.

Meanwhile, we hope this blueprint is of use to you and your organisation, please let us know if this is the case and how we can help further.

Appendix A – Contacts

Cisco C-NAB Team

Mike Badham	Solutions Architect – UK Healthcare
Rhodri Griffiths	Systems Engineer – UK Healthcare
Adrian Baker	Systems Engineer – UK Healthcare
Andrew Jobson	Systems Engineer – UK Healthcare
Tim Hardwick	Systems Engineer – Borderless Networks (Mobility)
Mubashir Mirza	Systems Engineer – Data Centre/Virtualisation
Mark Jackson	Solutions Architect – Borderless Networks (Security)

UK Healthcare

Terry Espiner	UK Health Sector Manager	0161 249 5793
Ed Powell	Account Manager – Central Accounts	020 8824 8179
David Park	Account Manager – North West	0161 249 5747
Paul Cook	Account Manager – North East	0161 249 5721
Sarah Calveley	Account Manager – East Midlands	0161 249 5734
Gary Eke	Account Manager – West Midlands & Wales	0161 249 5716
Gary Luttman	Account Manager – South East and East	020 8824 0346
Terry Robinson	Account Manager – London	020 8824 8063
Marc Inman	Account Manager – London	020 8824 0778
Graham Small	Account Manager – South West & South Central	020 8824 0296



Cisco Network Architecture Blueprint (C-NAB) for NHS Organisations

© Copyright 2011 Cisco Systems



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems, International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www.europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices

© Cisco 2011. Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.