Technology Framework for Higher & Further Education

Part Two: 21st Century Connected Learning Institution Blueprint

Foreword

Cisco has had a team dedicated to the Higher & Further Education market in England and Wales since 1998. In that time we have developed substantial market presence in the communication, collaboration and data services environmnents, and also believe we have also gained real insight into the beneficial application of ICT within Colleges and Universities.

During that time student numbers have grown significantly, there has been a key focus on enhancing the student experience, with current fiscal constraints institutions are looking for alternative methods of funding to supplement the traditional income flows and there is a heightened focus on smart buildings to assist with measuring and reducing carbon emissions. Technology has embedded itself into most parts of institutions whether it be in the way clearing/admissions is achieved to the way institutions collaborate with other institutions and partners or mobile wireless provides access to staff and students for the delivery and reception of educational materials.

Cisco firmly believes that it's technologies provide key components to solutions that address:
enhancing the student experience through secure collaborative tools and mobile connectivity solutions;
a suite of collaborative tools that enable rich, flexible and timely communications assisting communications with additional funding stream partners; smart buildings with granular views of carbon usage requires intelligent connectivity and application integration across a ubiquitous platform, which the network is able to meet.

This 21st Century Connected Learning Institution Blueprint details how a connected approach to the way an institution carries out it's duties can benefit all stakeholders including the leadership team, estates, finance, teaching staff, faculty, students and administration. It provides real examples of where technology can be deployed and the benefits generated to the institution. The overall framework, of which this blueprint is a part, explains how technology can support an institution's wider business and transformation goals.

This Blueprint is, in no small part, based on the contributions of many leaders and technologists involved with education that Cisco has had the pleasure to collaborate with over the years. We would welcome the opportunity for ongoing dialogue on this agenda, so please do let us know of your experiences with technology in the running of a University or College and the creation and delivery of educational material and forward any suggestions for future additions or improvements..

Michael Watkins
Regional Manager
Higher & Further Education
mwatkin@cisco.com

Table of Contents

Acronyms

AES	Advanced Encryption Standard
AP	Access Point (wireless)
API	Application Programming Interface
BMS	Building management Systems
CAPWAP	Control and Provisioning of Wireless Access Points (protocol)
CCTV	Closed Circuit TV
COTS	Commercial off the shelf
CRC	Carbon Reduction Commitment
DC	Data Centre
DMM	Digital Media Manager
DMS	Digital Media Suite
DNS	Domain Name Services
DVR	Digital Video Recorders
FCIP	Fibre Channel over IP
FCoE	Fibre Channel over Ethernet
FHRP	First Hop Redundancy Protocol
GLBP	Load Balancing Protocol
HSRP	Hot-Standby Router Protocol
HVAC	Heating Ventilation & Air Conditioning
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
iLBC	Internet Low Bandwidth Codec
IPTV	A method of transmitting television over an IP packet network
IPS	Intrusion Protection System
IP VPN	IP Virtual Private Network, achieving logical separation of networks over an IP infrastructure
LAN	Local Area Network - a computer network covering a relatively small area
LMS	Learning Management System, a software application that automates the administration, documentation, tracking, and reporting of training events
LWAPP	Lightweight Access Point Protocol
MAN	Metropolitan Area Network - a network that typically spans an area greater than a LAN but less than a WAN
MAP	Mesh Access Point
MIC	Message Integrity Check
MPLS	Multiprotocol Label Switching, a mechanism in high-performance networks which directs and carries data from one network node to the next
NAC	Network Access Control
Netbook	A small, light and inexpensive laptop computers suited for general computing and accessing web-based applications
NGS	NAC Guest Server
PoE	Power over Ethernet
P2P	Peer to Peer
QoS	Quality of Service
RAP	Root Access Point
RF	Radio Frequency
RFID	Radio Frequency ID, a technology for wirelessly tracking and locating an asset, product or person
ROI	Return on Investment
RPO	Recovery Point Objective
RPS	Redundant Power Supplies
RTO	Recovery Time Objective
SAN	Storage Area Network
SCORM	Sharable Content Object Reference Model is a collection of standards and specifications for web-based e-learning
SLA	Service Level Agreement
SNR	Single Number Reach
SRST	Survivable Remote Site Telephony

SSL	Secure Sockets Layer
STP	Spanning-tree protocols
TKIP	Temporal Key Integrity Protocol
TRM	Technical Reference Model
UC	Unified Communications
UCS	Unified Computing System
UPS	Uninterruptible Power Supplies
VCR	Video Cassette Recorder
VDC	Virtual Device Context - virtual segmentation of a physical device
VLE	Vitual Learning Environment
VRF	Virtual Routing and Forwarding, a technology that allows multiple instances of a routing table to co-exist within the same router at the same time with no connection between the tables
VRRP	Virtual Router Redundancy Protocol
VSM	Video Surveillance Manager
VSS	Virtual Switching System
WAAS	Wide Area Application Services
WAN	Wide Area Network - a network that covers a broad geographical area
WCS	Wireless Control System
WLAN	Wireless LAN
WLC	Wireless LAN Controller
802.1x	IEEE Standard for authenticating end points

1. Executive Summary

Today, institutions across England and Wales are operating in a business environment that is challenging traditional funding models, increasing options for the delivery of teaching and learning, coupled with spiraling energy costs. In addition to the pedagogical guidance being provided to institutions, there are also Government directives on energy efficiency e.g. the Carbon Reduction Commitment legislation, that have a direct impact on the sector.

For the last 10 years, the number of students in Higher and Further Education has grown steadily, and are currently standing at around 2.4 million in Higher Education and 5.1 million in Further Education. Currently institutions face the prospect of home student numbers being constrained, this can have a direct impact on the funds available for expansion or improvement. In addition there is a potential change in the near future to the student fee cap that is in place. For Further Education institutions, there are challenges around the funding of new buildings. Both Higher and Further education institutions have the goal of not only attracting new students but also retaining them. This environment makes it all the more important to attract and retain students by delivering an excellent student experience.

With the capabilities of current Information and Communication Technologies (ICT), the borders of traditional institutions are blurring. Institutions need no longer be bound by physical borders for their administration or teaching and learning. Different business models for the creation and sharing of intellectual property are emerging and the way in which business and community engagements are conducted is changing.

With this background Cisco has created 2 blueprints for Higher and Further Education (H&FE). The first document reviews the business and funding aspects associated with H&FE, the purpose of this, the second document, is to overview available ICT, it's direction, and explain how it can be deployed in support of business transformation and curriculum delivery. It provides a set of conceptual, logical and physical reference architectures which can be adopted by institutions to inform each stage of ICT development; from vision and strategy planning through to final implementation. The reference architectures may also be used with internal and external ICT stakeholders. Each institution is either connected directly to the JANET network or their regional MAN, however in depth discussion on the MAN networks and services that can be run over these is outside the scope of this document.

Cisco uses the term 21st Century Connected Learning as model to refer to an educational institution/establishment that is maximising the benefit from it's ICT in it's business planning and curriculum delivery in order to enable transformation and flexible learning. This document - the '21st Century Connected Learning Institution Blueprint' – has been created by Cisco as part of a framework to outline how ICT can have a transformational effect on the business and curriculum delivery by adopting an architectural approach. It is targeted primarily at technical stakeholders within Colleges and Universities – namely CIO, CTO, IT Director, Principal, Chief Executive, Head of Networks and senior technical staff.

There are 3 key areas that ICT links to the operation of Colleges and Universities:

- **Enhancing the Teaching & Learning Environment**– using unified communications and mobility technologies to enhance existing teaching and learning models and enable virtual classrooms delivering up to date, live remote learning, collaborative workspaces, with secure connectivity throughout the borderless campus.
- **Workforce Enablement** – using unified communications, virtual work spaces and mobility technologies to create 'new ways of working' for back office and front line teaching staff.
- **Flexible Workplaces and Spaces** – using technology to radically change how offices, lecture theatres, assets and facilities are monitored, managed and optimised to create the 21st Century Connected Learning Institution Campus.

Cisco would like to extend an offer to discuss the contents of the 21st Century Connected Learning Blueprint. We believe this may assist you in clarifying how their contents might positively impact the daily functions of your College or University. If you would like to take up this offer you will find the details of your local Cisco contact in Appendix A.

1.1 Introduction and Purpose of the 21st Century Connected Learning Institution Blueprint

There has never been a time like today where ICT is able to offer such flexible and diverse options for delivering education, research and collaboration with business partners, enabling greater inclusiveness and diversity. In the current economic climate, when traditional education and research funding models are being challenged, it is especially important for each institution to ensure high quality delivery of the curriculum to enhance the student experience and hence support student attraction and retention rates.

Institutions face the prospect of home student numbers being constrained due to funding models. This creates an opportunity to provide a focus on attracting overseas students either for 'on-campus' or remote delivery of the curriculum as a way for the institute to grow. Colleges are continually looking for ways to recruit and retain students whilst delivering high student achievement as currently measured by Ofsted and the Learning Skills Council. Other Government directives relating to energy efficiency, e.g. the Carbon Reduction Commitment[1] legislation also have a direct impact on the sector. Use of intelligent network based technologies can give an insight into where power is being used and assist in the reduction of power when used in conjunction with other measures.

There is a shift taking place across the education sector in the way in which the underpinning technologies used for the delivery of core services such as business applications and processes along with the delivery of learning materials and interactions are being designed and deployed. Traditional face to face teaching and learning practices are giving way to more blended approaches involving varying amounts of 'virtual' classroom activities, enabling an expansion of the borders of a traditional institution. Network infrastructure and applications are no longer perceived by the business or by the users as being a nice to have, but an essential always on service delivering appropriate and responsive services. The nature of real time applications such as IP Telephony, Unified Communications and video, effectively provide a network monitor to all users giving visibility of availability and responsiveness of the applications and infrastructure. The network is now the platform for delivering these capabilities and has changed from being a best effort connectivity and delivery platform to one that is far more reliable with built in fast failover resiliency capabilities which when deployed according to guidelines and support provides Enterprise grade functionality and availability.

Video, whether it is real time or recalled video content, is a key component in the participation and delivery of the curriculum and staff learning, as well collaboration within the institution and for research acceleration. Having a network that is both video-aware and dynamically responsive to it can increase operational simplicity by reducing complexity, administrative overhead and accelerate deployment of rich media services. Cisco's medianet architectural platform is media and endpoint aware with built in services that provide an optimal quality of experience for the user, whilst automating many aspects of configuration and network optimisation.

The 21st Century Connected Learning Institution Blueprint is intended to assist institutions in understanding available technologies, how they may help the operation of the business and the key steps and capabilities that need to built in order to achieve the desired outcomes. This document provides a set of conceptual, logical and physical reference architectures which can be adopted by institutions to inform each stage of ICT development; from vision and strategy planning through to final implementation. The reference architectures may also be used with internal and external ICT stakeholders.

Each institution is either connected directly to the JANET network or their regional MAN, however in depth discussion on the MAN networks and services that can be run over these is outside the scope of this document.

[1] Information on the CRC may be found at the defra website: http://www.defra.gov.uk/environment/climatechange/uk/business/crc/index.htm

2. What is the 21st Century Connected Learning Institution?

2.1 Introduction

The senior leadership team of an institution is responsible for running a safe, effective and efficient organisation through:

- Development of a consistent set of business goals and effective business plans to meet these goals;
- Recruitment and retention of quality teaching and research staff;
- Attraction and retention of students (both from both home and abroad);
- Increasing the institution's standing, typically measured by their position in league tables/student pass rates for Universities and Ofsted and Learning Skills Council measurements for Colleges;
- Partnership with one or more of the following:
  - other institutions, research organisations, business and the wider community

New business, teaching and learning models can be realised through the use of technology and an architectural approach to the transformation of the learning environment. Cisco uses the term '21st Century Connected Learning Institution' to refer to an educational establishment that is harnessing technology for strategic gain and using it to maximum effect.

The prime responsibility for realising the 21st Century Connected Learning model lies with those who have the mandate to transform an institution's processes, learning delivery, and the student experience. This includes the council, the senate, Principal, Chief Executive, finance, estates, HR and ICT; namely those functions, departments and faculties responsible for the financial health of the institution and recruitment and retention of staff, research academics and students.

Cisco believes that ICT has a critical role in enabling an institution to respond rapidly to changing business requirements. Highlights of key areas where this is the case include:

- Flexible workplaces and spaces – reflecting the capability of the network as the platform for creating borderless networks that unify building services and applications, and the ready availability of virtualising technologies that can be used by staff, students and academics for projects and meetings. The Smart Connected Buildings architecture enables rapid rollout of new ICT infrastructure and services into new buildings in a timely and cost effective manner;
- Teaching and Learning – creation, storage and replay of materials in a SCORM[2] compliant manner can be device and location independent. The location of the student and the lecturer can become immaterial, and collaboration easy to achieve. Correct use of e-assessment[3] technologies can provide efficiency and effectiveness improvements in the teaching practice;
- Research – project times and costs can be reduced through the use of collaboration tools and by supplying flexible, secure computing and information storage. These will facilitate improved collaboration with research partners and aid the attraction, recruitment and retention of top academics;
- Students – enhancing the student experience by providing flexible learning and simple and easy access to, and delivery of, learning materials;
- Staff – technologies can impact staff in the way they collaborate, access information, where they work physically and deliver flexibility to how and where they work, delivering elements of business continuance;
- Access to Data & Information – network and application resilience and virtualisation enable 'always-on' access to user data and information and learning materials. The information and service assurance to protect valuable resources is layered throughout the infrastructure, applications and end-points.

[2] SCORM - Sharable Content Object Reference Model is a collection of standards and specifications for web-based e-learning

[3] Further information on e-assessment can be found at the JISC web site: http://www.jisc.ac.uk/assessment.html#

To create the 21st Century Connected Learning Institution, Cisco recommends that directorates focus upon exploiting technology in three development areas;

- Enhancing the Teaching and Learning Experience
- Workforce Enablement.
- Flexible Workplaces and Spaces

This should be underpinned by development of a foundation ICT infrastructure – the ICT Service Delivery Platform - encompassing data centres, networks, desktops and information and service assurance.

2.2 Enhancing the Teaching & Learning Experience

Technology can help deliver an environment that truly enhances the student experience of an institution and effectiveness of a study programme. The advent of low cost netbooks[4] and high quality mobile devices make it feasible for students to create and access material and to collaborate using them; indeed some Universities are promoting or mandating that students use mobile devices to access a learning platform for learning materials and information.

Student experiences also have strong linkages to the capabilities offered by Flexible Workplaces and Spaces. Increasingly expectations are towards a blending of traditional teaching and learning models with the ambient learning model where there is access to high quality e-learning material at a time, place, pace and context that best suits the individual learner and which provides a personalised learning experience.

Effective use of ICT in the Teaching and Learning environment can help address the following:

- How can staff student interactions be made more flexible and easier to achieve?
- How can learning materials be created and delivered in a more flexible manner?
- How can lesson/lecture review be made easier for students?
- How can room availability/usage be made more visible?
- How can information services be made more visible to the students?

Five of the key areas where ICT can directly impact the teaching and learning environment are:

- **Design & creation of content** to provide flexible content creation options that support a range of input devices - from hand held video recorders to studio based systems - and offer the ability to automatically render prepared content into the format that best suits the end-point device of the student.
- **Content delivery method**. ICT should support a range of delivery methods that are inclusive of the lecturer, student and content. Technologies can enable recording and storage from traditional lecture room/theatres so they are easily achieved, virtual collaborative environments such that remote delivery and teamwork/project work can be carried out, the use of immersive technologies, and use of IPTV[5] recordings so the transmission of programme's and material can be scheduled.
- **Reception and ingestion of material** by the student should be available at the time, place, in an appropriate format and via the device of choice at that point in time.
- **Timetable related information** for access to material can be sent to the student to help ensure classes/ lectures are not missed. Reminders of upcoming lectures, IPTV schedules of their relevant topics, room changes, timetable changes can be sent via text/social network applications or using location aware digital signage, ensuring students have the most up to date information.
- **Content storage** provides the ability to store materials in a secure, highly available always on system with applications providing SCORM compliance for tracking and testing purposes where appropriate.

[4] Netbook - a small, light and inexpensive laptop computers suited for general computing and accessing web-based applications

[5] IPTV – IP Television - a method of transmitting television over an IP packet network

For some users the key to technology adoption is to apply it in such a way that their current behaviour patterns do not have to change, or only in a minimal way. This is best illustrated through the use of a hypothetical example. A lecturer who is used to walking into the classroom/lecture theatre, manually taking a register of attendees, then switching on the over head projector (OHP) for use with acetates and then proceeds to deliver their material, may object to the introduction of a new process that exchanges the OHP for a smart projector and having to start a video camera at the start of the session so that it can be recorded for later reviewing either by students unable to attend or for revision purposes, and then stopping the recording at the end of the session. Through the use of ICT this process can be largely automated. Student attendance could be automatically recorded using RFID[6] technology or location tracking as they walk into the room. A smart projector could be used to take snapshot of the material which synchronises to the camera which starts recording at a time set by the calendaring system used for timetables, stops recording automatically at the end of the session and sends the synchronized contents to a SCORM compliant repository.

Enhancing The Teaching and Learning Experience has direct linkages to ICT:

- **Unified Communications** which allows all voice, video and messaging services to be directed to the chosen work device and location of a member of staff and easy escalation from one form of communication to a more feature rich form, ideal for communications between lecturer and researcher or student;
- **Collaboration** technologies that allow the creation of virtual work spaces, enable slides, documents and spreadsheets to be shared and worked upon across a table, across a room or between buildings. This enables collaborative projects to be created, with contribution from any of the space members;
- **Wireless networks** that allow staff & students to work securely from their preferred location within a campus, and enable wireless voice and data services to be used on the go;
- **Digital signage** that provides the ability to communicate with staff and students, for example to deliver location, current lecture room usage, events, services or health and safety information;
- **Video Portals** that provide storage and recall of content integration into a SCORM compliant Learning Management System[7] (LMS);
- **Data Centre** technologies provide the storage of student information and course materials in a secure manner;
- **Medianet** which provides the underlying intelligent infrastructure that dynamically allocates resources and services to deliver a consistently high quality experience when participating in a video session or viewing video content.

2.3 Workforce Enablement

An effective workforce, both administration and teaching/research, is critical to the operation of any institution and the successful delivery of services. That effectiveness can only be achieved through detailed workforce planning by HR (often including some changes in working practices), finance, ICT and service delivery departments in order that the following be addressed:

- How can the efficiency of employees be maximised?
- How can up-to-date tools - on a par with the best of private sector – be provided for the workforce?
- How can the work-life balance of the employees be enhanced?
- How can employees who are disabled, long term sick or with carer responsibilities be allowed to enter or remain in employment?
- How can employees continue to effectively carry out their roles and responsibilities whilst travelling or working remotely?

[6] RFID – Radio Frequency ID, a technology for wirelessly tracking and locating an asset, product or person

[7] Learning Management System, a software application that automates the administration, documentation, tracking, and reporting of training events

ICT has already demonstrated that it is able to tackle the above issues. Where the use of ICT has been maximised to address these considerations it has delivered real operational efficiencies and provided options for more flexible workstyles that individual employees can exploit to meet their personal needs.

One key area where ICT can assist with the workforce has only recently become a reality; that is the ability for remote workers (part time, full time or mobile users) to exploit Unified Communications, collaboration and security technologies to carry out their role but still feel part of a team and continue to contribute as effectively as they do when on campus.

Technologies which help address these goals are:

- Unified Communications allows all voice, video and messaging services to be directed to the chosen work location of a member of teaching, administration or research staff and also enables easy escalation from instant messaging to a phone call through to a video call;
- Presence Services allow the network to be aware of the availability of users e.g. on the phone, available, and the best mode of communication to use to reach them e.g. Instant Message, phone call, video call;
- Single Number Reach and Fixed Mobile Convergence optimise the reachability of staff and minimise the cost of communicating with them as they move between mobile operator and private networks;
- Collaboration technologies allow presentations, documents and spreadsheets to be reviewed and updated across a table, across a room or between locations. This can help reduce administration, project and research time;
- Wireless networks allow staff to work securely from their preferred location within an office or from home, and enable wireless voice and data services to be used on the go in the campus;
- Secure Remote and Mobile Access technologies allow 'anywhere, anytime' access to information and services in a secure manner, allowing staff to work from home or in a remote location;
- Data Centre technologies provide the storage of staff and institution information in a secure manner;
- Cisco TelePresence provides a virtual in room experience which enables high definition, rich media communication between locations. The use of TelePresence can help reduce project and planning timescales, increase the frequency of meetings without the need for travel for events such as:
  - split location management meetings;
  - initial interviews for faculty, students in remote locations/countries;
  - subject matter expert discussions/teaching across locations/countries;
  - meetings with business partners at remote locations.

Implementation of ICT in support of employees will deliver real benefit to the institution. Firstly it enables employees to work securely from any location that is either part of the campus or has internet connectivity. Secondly the availability of industry-standard tools and the promotion of better work-life balance will enhance staff recruitment and retention. Thirdly, from a business continuance perspective, providing staff have access to broadband, they will be able to continue to work effectively at times where travel is difficult due to flooding, snow, outages at normal workplace or other unforeseen circumstances.

The final, very important, consideration for the development of an ICT strategy to support employees is in the ability for it to link into an institution's Green, Sustainability and Carbon Management strategies and into Carbon Reduction Commitment legislation. Implementation of the above technologies will enable employees to travel less, allow building size and numbers to be optimised, and use of fewer institution resources including energy. This can have a very positive effect on reducing an institutes 'carbon footprint'.

2.4 Flexible Workplaces and Spaces

Directly aligned to the Workforce Enablement and elements of Enhancing the Student Experience is the need for a Flexible Workplaces and Spaces strategy.

Such a strategy looks at the effective use of physical real estate and other virtual work spaces where project work and collaboration may be carried out in the future. The strategy must also look at the creation of modern, flexible learning places, or spaces, which should be able to motivate learners through the promotion of learning that may be formal or collaborative but which is personalised and inclusive for the learner.

Such a strategy has to be underpinned by a robust architecture. In Cisco terms such architectures include:

- **Flexible Location Technologies** help provide a borderless network that enables staff and students to work at their place and location of choice with the same or greater effectiveness as in a fixed desk/location model. This allows work and collaboration to take place in either a physical or virtual environment.
- **Business Video** allows the institution, staff and students alike to select the most appropriate video application/solution to meet their needs at any point in time. The underlying Cisco medianet ensuring a high quality of experience is delivered to the user.
- **The Smart Connected Buildings Architecture** defines a network-based building management and energy monitoring capability, to minimise the use of energy resources by providing a portal into energy usage throughout a campus and the ability to intelligently interact with entities to control when and where energy is used.

Flexible Workplaces are designed quite differently to traditional physical environments. They incorporate fewer traditional desks and substitute a range of open plan and informal work areas, as well as flexible meeting areas of different sizes and capabilities. These new workplace designs encourage informal collaborative working within and between staff, students and researchers; for example meeting around a café table and sharing a document between participant's laptops using web collaboration. Experience within Cisco has shown that changing traditional office layouts can actually increase building utilisation, even though the number of formal desk spaces is reduced.

Flexible Workplaces and Spaces can help with enhancing the student experience, staff recruitment and retention, and create real cost savings. These cost savings are based on a reduction in time to deliver ICT and security services into new and existing buildings and student accommodation, a move towards operating real estate to maximum efficiency in terms of utilisation and energy efficiency, and helping to deliver against Carbon Reduction Commitments.

The Flexible Workplaces and Spaces has direct linkages to ICT:

- **Unified Communications** allows all voice, video and messaging services to be directed to the chosen work location of a member of staff and easy escalation from one form of communication to a more feature rich form. Extension mobility and soft phone applications enable virtual/hot desking policies to be realised.
- **Collaboration** technologies allow the creation of virtual work spaces, enable slides, documents and spreadsheets to be shared and worked upon in a borderless environment, across a table, across a room or between locations.
- **Wireless networks** allow staff & students to work securely from their preferred location within the campus e.g. learning cafe, and enable wireless voice and data services to be used on the go.
- **Network-based IP Video Surveillance** products now operate over a shared network infrastructure and can be integrated with video analytic software as required.
- **Digital signage** provides the ability to communicate with staff and students, for example to deliver location, current lecture room usage, events, services or health and safety information.
- **EnergyWise** enables network-based building and energy visibility and control, and end point power management.
- **Medianet** provides the underlying intelligent infrastructure that dynamically allocates resources to consistently deliver a high quality experience when participating in a video session or viewing video content.

2.5 Foundation ICT Infrastructure

A 21st Century Connected Learning Institution depends on the use of modern and open IT and communications and requires investment in foundation infrastructure to provide a robust ICT Service Delivery Platform.

Due to the need for an Institution's network to support a wide range of services and applications for different stakeholder communities institutions both large and small are beginning to look towards a flexible core infrastructure that can be virtually segmented. The reason for this is that technology now permits a single physical infrastructure to provide secure transport, while supporting separate applications and communities within their own secure logical/virtual environments.

The ICT Service Delivery Platform comprises four main infrastructure elements:

- Access – wired and wireless local area networks and IP VPN[8] solutions for end-user connectivity. Whilst out of scope of this document this can also include end user terminal devices used to access applications and information;
- Transport – to effectively deliver applications, information and services, with the ability to virtualise the infrastructure to offer isolated delivery paths to different parts of the institution e.g. one virtual network for the building and security services such as IP Video Surveillance, lift control, environmental and power monitoring, another virtual network for students access, another for administration, another for research and another for guest (paying seminar & events customers), but all carried over one common physical infrastructure;
- Data Centres – the service delivery points for all administration applications, information databases, converged services, research data and Virtual Learning Environment applications;
- Information and Service Assurance – to protect all information and services, and assure staff, student, institution and business partner data.

Access methods provide connection options for users; typically wired and wireless LANs[9] and IP VPNs. As an adjunct, the move towards fixed mobile convergence begins to provide flexible connectivity between publicly available services and those of the institution.

Transport delivers data and services to and between end users for many different applications. They typically comprise of Campus LAN environments with connection to other institutions via MAN[10] connections via 3rd parties, VPN connectivity to remote users/sites and business partners via the Internet or in fewer cases by private WAN[11] connections. To support the institution effectively they must be delivered in a manner that offers high performance and resilience, and that also offers business continuance capabilities. Transport may be over a virtualised infrastructure which provides separation using one of a number of technologies such as VRF[12] or MPLS[13] to name two.

Data Centres provide the repository for all of the institutions key information and applications. Their design becomes critical to the business success of an institution. Data Centres need to be resilient; offer robust information and service assurance standards; and incorporate business continuity to safeguard service levels and assure information integrity. They should also be virtualised to ensure that physical resources are used to their maximum and that virtual resources can be deployed quickly and flexibly to support new or changed business requirements.

[8] IP VPN – IP Virtual Private Network, achieving logical separation of networks over an IP infrastructure

[9] LAN - Local Area Network - a computer network covering a relatively small area

[10] MAN – Metropolitan Area Network - a network that typically spans an area greater than a LAN but less than a WAN

[11] WAN - Wide Area Network is a network that covers a broad geographical area

[12] VRF - Virtual Routing and Forwarding, a technology that allows multiple instances of a routing table to co-exist within the same router at the same time with no connection between the tables

[13] MPLS - Multiprotocol Label Switching, a mechanism in high-performance networks which directs and carries data from one network node to the next.

Information and Service Assurance capability should be considered part of the foundation Service Delivery Platform. Capability needs to be provided within the IT and network environment to assure the confidentiality of data passing across it, the integrity of that same information, the availability of information and the auditability of access to information as appropriate. These security disciplines are often referred to using the acronym CIAA – Confidentiality, Integrity, Availability and Auditability.

Figure 2.5.1 shows this Foundation ICT Infrastructure – the Service Delivery Platform - in logical terms. Section 4 of this Blueprint introduces a conceptual architecture for this infrastructure and shows how intelligence can be introduced to the transport layer by including services such as quality of service, multicast and virtualisation.

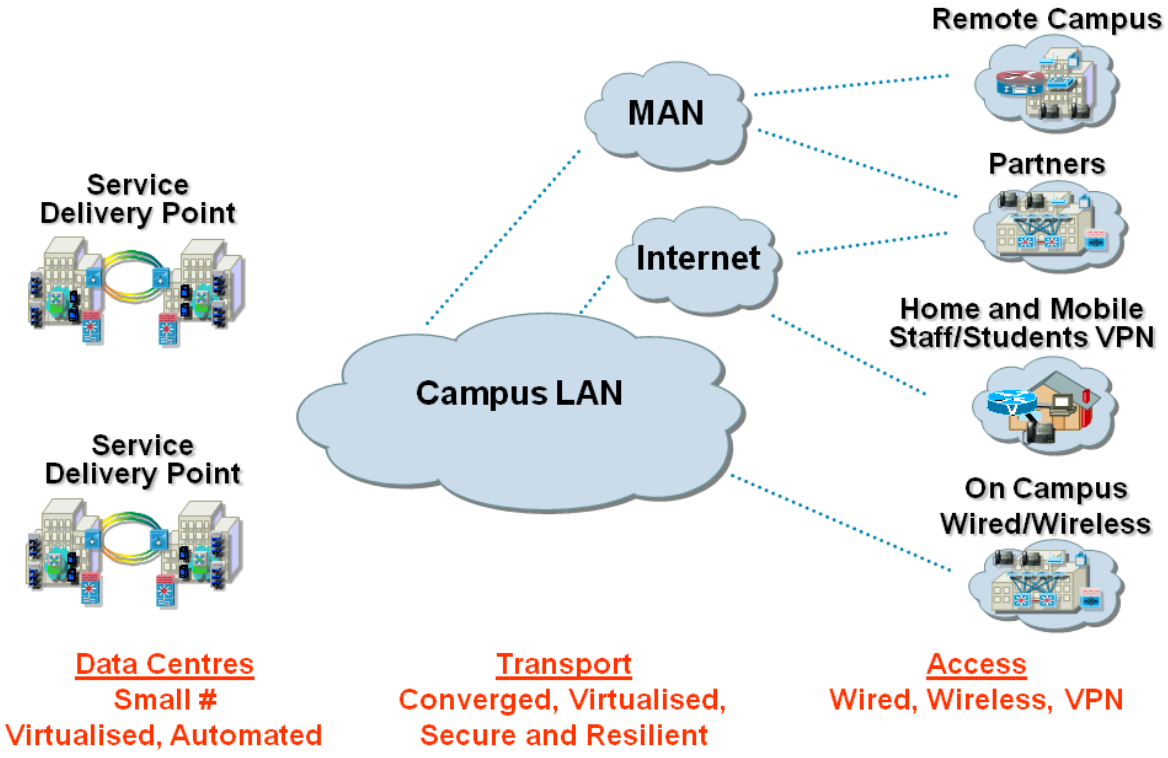


Figure 2.5.1 – Foundation ICT Infrastructure: The Service Delivery Platform

2.6 Roadmap to the 21st Century Connected Learning Institution

Whilst priorities may vary from institution to institution, depending upon business objectives, a pattern of infrastructure deployments has emerged as institutions seek to realise the benefits of technology and the architectural reference models contained in this blueprint.

We believe it is useful to share this information as it shows how a layered conceptual architecture can drive a series of linked developments that, over time, will realise a total ICT solution for an institution.

This deployment pattern, shown in Figure 2.6.1, is intended to be indicative rather than definitive; the key linked development steps are:

- **Foundation Campus Architectures LAN and MAN Networks** virtualised using Virtual LANs (VLANs), VRF, MPLS etc. to provide support for different institution functions and groups.
- **Wireless LAN & Mobility** across campus. A key step towards the Workforce Enablement and Enhancing the Teaching and Learning experience.

- **Virtualised Data Centre's** with appropriate security and business continuance processes. To support the institution business priorities.
- **IP Voice, IP Messaging and IP Contact Centre** – possible with home-based staff - to deliver flexible voice services to staff and in some cases students.
- **Unified Communications applications** – collaboration and business video – to enhance the facilities available to staff and students alike.
- **Information and Service Assurance** policy and practice update; supported by 'Self Defending Network' technology.

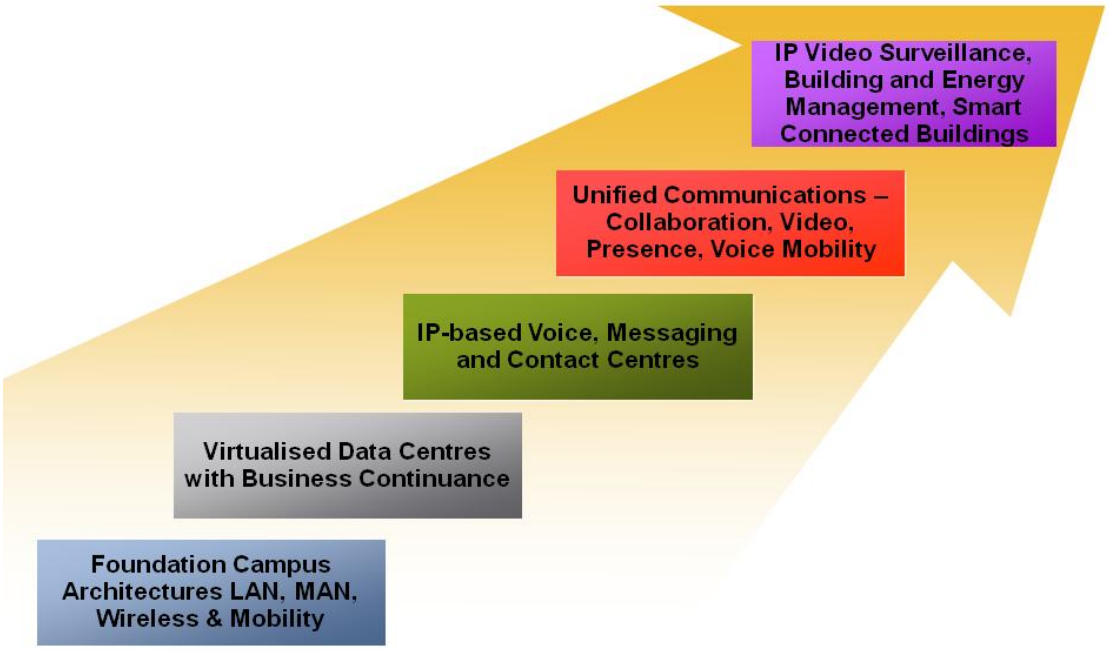


Figure 2.6.1 – Roadmap to the 21st Century Connected Learning Institution

3. The Importance of a Structured, Architectural Approach to ICT

This document defines a generic Higher and Further Education Architecture which Cisco recommend for use by institutions to inform the development of ICT infrastructure and deployment of new applications and services. The 21st Century Connected Learning Institution Architecture provides a representation of ICT system components and the linkages between them and should be viewed both as a standalone technical Blueprint and as a component that could be incorporated into an institutions Enterprise ICT Architecture where appropriate.

Each system component in the architecture has been designed as a re-usable building block. This approach permits an institution to design infrastructure that is virtualised, or service oriented to use modern ICT parlance. Virtualisation means that none of the components are dedicated to a particular application or service, and each may be re-used to ensure more efficient and timely delivery of new applications or services. A good example of this re-usable building block principle would be an identity service. The service could be set-up to authenticate and authorise remote access users but then could be re-used for wired and Wireless LAN users, for voice applications users and for student and educationalists for other ICT services.

An architectural approach to ICT is in line with both general enterprise organisations and Government strategy. There are a number of architectures that could be used, one example is TOGAF (The Open Group Architecture Framework) which provides a methodology for developing Enterprise ICT Architectures. Central to the TOGAF methodology is the development of 'Technical Reference Models' that describe technology components and their relationships. Technical Reference Models from different sources may be amalgamated to create overall Enterprise ICT Architectures. The conceptual architecture set out in this Blueprint is such a technical reference model and, as such, suitable for amalgamation with other similar models from other systems vendors to create an institutions ICT architecture.

An architectural approach to ICT is worthwhile and beneficial for very practical reasons:

- An architecture provides a definitive statement of best practice within what may be a very complex ICT environment; it can be agreed by all parties within an organisation and shared with external stakeholders, such as ICT suppliers and integration partners.
- An architecture contains numerous system components and, as such, provides an indication of what work needs to be carried out over a period; in that way it is representative of an overall ICT programme.
- As it is representative of an ICT programme, it can be used as a vehicle to modify procurement practice - away from discrete projects towards programmes of linked projects; this change in procurement practice can lead to cost savings and a reduction in risk for ICT projects.

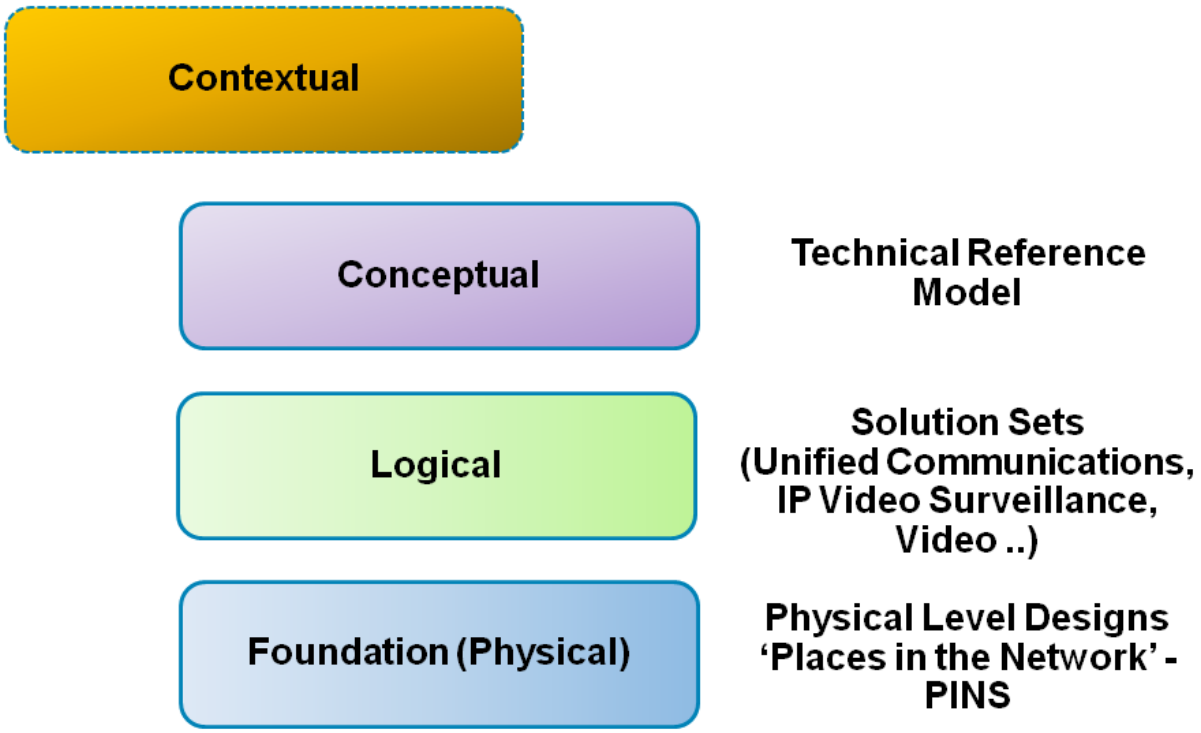


Figure 3.1 – Structure of Cisco 'Reference Architectures'

This 21st Century Connected Learning Institution Blueprint defines three distinct types of reference architecture that we recommend for adoption by institutions. These are shown in Figure 3.1:

- A **Conceptual Architecture** that provides a structured representation of the overall set of ICT services and the linkages between them. It may be viewed either as a standalone technical blueprint, or as a technical reference model suitable for incorporation into a broader Enterprise ICT Architecture. Each component within the Conceptual Architecture has been designed as a 're-usable building block'; this approach permits an institution to design a service-oriented infrastructure capable of virtualisation.
- **Logical Architectures** that show individual technology or end-user solution sets. Examples of Logical Architectures include the Cisco Unified Communications technology solution set, or the Cisco IP Video Surveillance family – a component of the Physical Security solution set.
- **Foundation, or Physical, Architectures** that define underlying campus, wide area and data centre network physical-layer architectures.

We believe these reference architectures have a key role to play; both internally within an institution and externally in an institutions dealings with vendors, service providers and where shared services are embarked upon. Each of the reference architectures represents Cisco 'best practice' that has been built up over many years and which, if deployed, can help ensure ICT deployments are achieved in a timely fashion and with the minimum of risk.

An institution will benefit in four key areas if it adopts the Cisco reference architectures; namely definition of ICT strategy, improved stakeholder engagement, risk management and best practice identification. We hope this document helps deliver these benefits within your institution.

4. The 21st Century Connected Learning Institution Conceptual Architecture

Cisco advocates the use of a Conceptual Architecture to define the overall set of ICT hardware, software and services that is, and may be, deployed within a 21st Century Connected Learning Institution.

The value of a Conceptual Architecture is that it:

1. Provides a graphical representation of the available set of technology components and shows their inter-relationships;
2. Offers a representation of an overall programme of work to implement the architecture, with the prospect of prioritising individual projects to meet institutional needs;
3. Provides a framework that permits individual user or service contexts to be mapped.

The first and second describe how the Conceptual Architecture can be used to gain agreement between internal stakeholders such as the Faculties, the Teaching Professionals and the Board, and to brief external stakeholders, such as vendors and service providers. In this way it can help guarantee that all stakeholders are fully briefed and in agreement on an ICT programme to be executed.

The final point is important as the Conceptual Architecture can be used to focus on a single user type, user function or service type. For example; a University may decide to modernise the admissions process, by introducing an IP Contact Centre, and with links to UCAS application forms and academic results. The Conceptual Architecture can be used to map the technology dependencies that must be met for successful implementation. More detail on this can be found in Section 4.2, User and Service Context.

Cisco encourages Institutions to make this Conceptual Architecture a 'living record' that documents current and target architectures; an 'as-is' architecture that is personalised with the technology, whether vendor or developed internally, in current use and a 'to-be' architecture that defines the Universities strategic goal.

4.1 Description of the Conceptual Architecture

The Conceptual Architecture – the Technical Reference Model - proposed in this blueprint is an expansion of the Cisco Service Oriented Network Architecture (SONA) model. It comprises four functional technology layers and a fifth layer that can be used to define a user or service context. The Conceptual Architecture can be found in Figure 4.1.1.

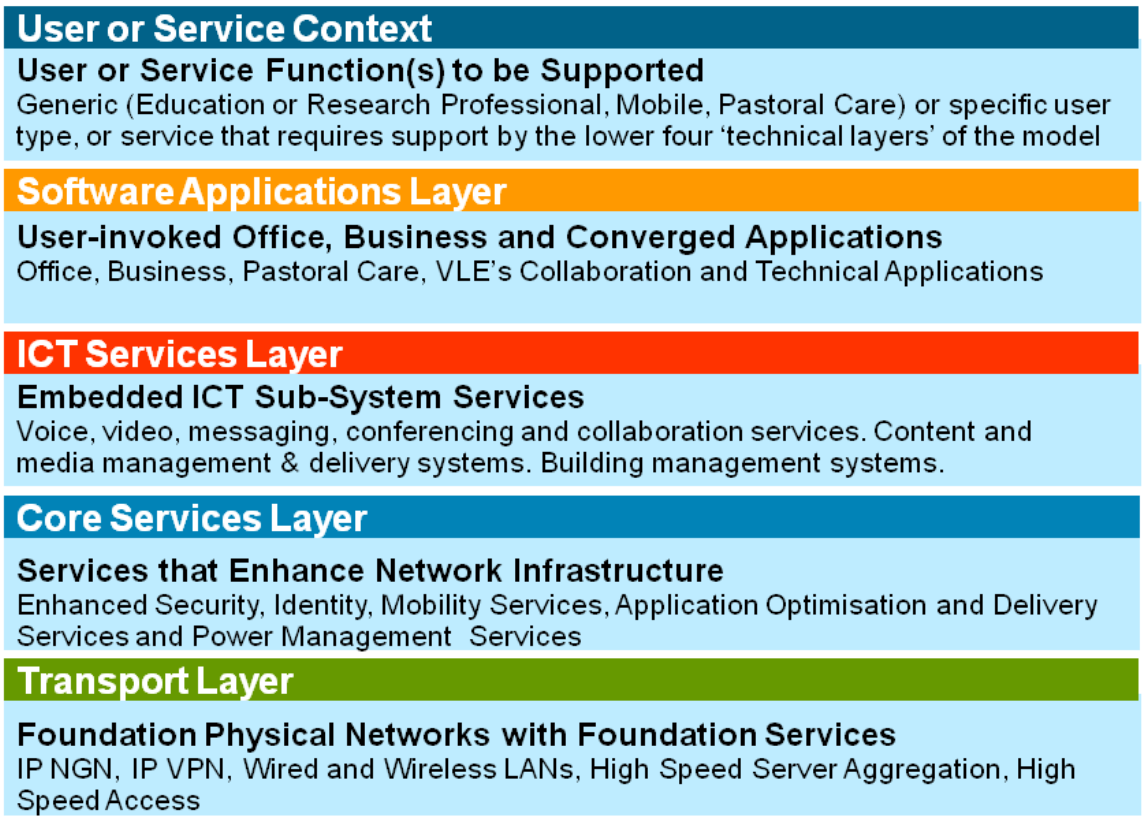


Figure 4.1.1 – Schematic of the Conceptual Architecture

This layered architecture has marked similarities to the technical reference model referenced in the TOGAF (The Open Group Architecture Framework) specification, an industry standard architecture framework. Each of the four functional layers has a well defined role and offers a range of potential services as follows:

The Transport (or Foundation) Layer provides the underlying wired and wireless IP infrastructure along with the key foundation network services, such as security and quality of service (QoS), necessary to create a converged IP infrastructure.

The Core Services Layer provides intelligent network services, such as enhanced security or application acceleration, that enhance the transport layer by delivering increased user function, increased performance or enhanced security.

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 sub-systems.

The Software Applications Layer provides the end-user applications that are directly available to users; for example Microsoft Office, Document Management, Business Software or VLE.

The User or Service Context (Layer) permits the Conceptual Architecture to represent the needs of a particular user or service – see Section 4.2 below.

Each of the lower four layers can be populated with Cisco products and services, vendor products and services, or applications and services developed locally within the community. Figure 4.1.2 shows the Conceptual Architecture populated with Cisco network, service and application offerings. As stated above we actively encourage Institutions to incorporate non-Cisco network offerings, vendor software applications and locally-

developed applications and services; hence to adapt the Conceptual Architecture to the local environment to deliver greater value.

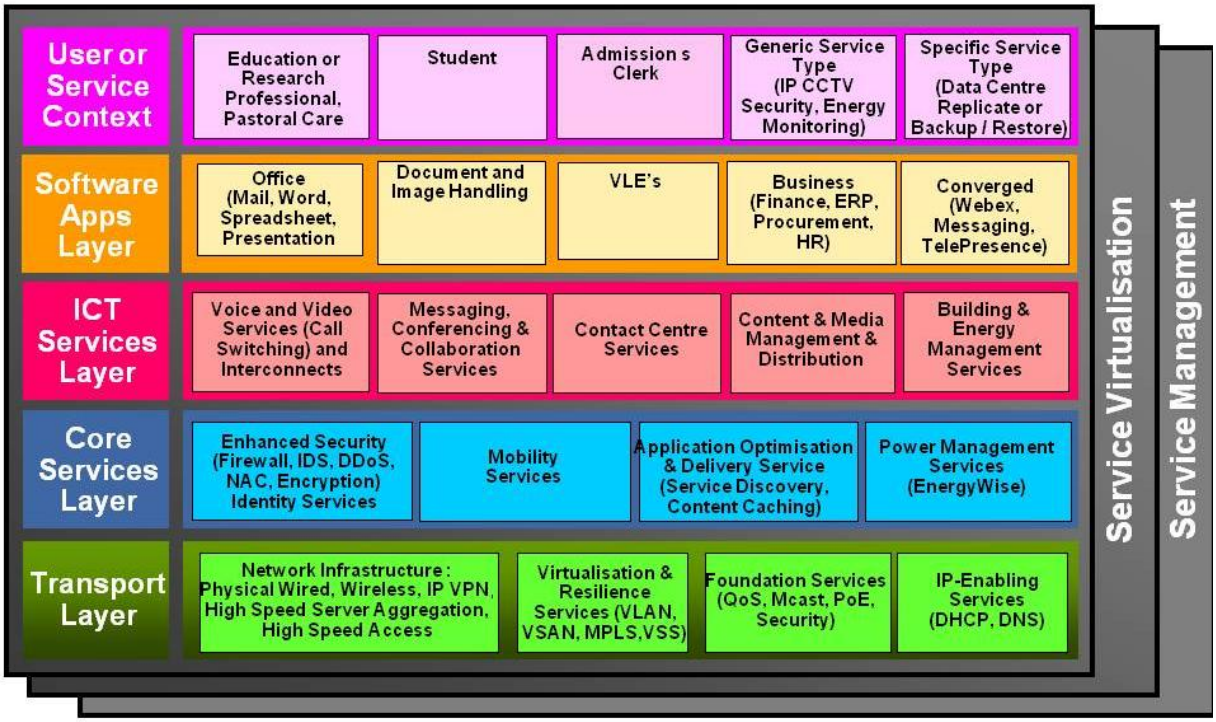


Figure 4.1.2 – Conceptual Architecture Showing Functional Layers in Detail

4.2 User and Service Context

The Conceptual Architecture can be used both to represent overall ICT capability and to focus on the particular functional needs of users or services.

The User and Service Context Layer allows technology dependencies to be mapped for any desired user or service function. For example, an Insitution may decide to modernize their admissions process. The Conceptual Layer allows the Insitution to map the underlying technologies on which the Admissions system will depend for service:

> Clerk ➔ Business, Word and Document Management ➔ Voice and Video Services, Collaboration Services, Contact Centre, Building Management➔ Enhanced Security, Identity Services and Energy Management Services➔ Underlying Transport Network with QoS and Foundation Security

This service context – or set of underlying dependencies – is shown diagrammatically in Figure 4.2.1:

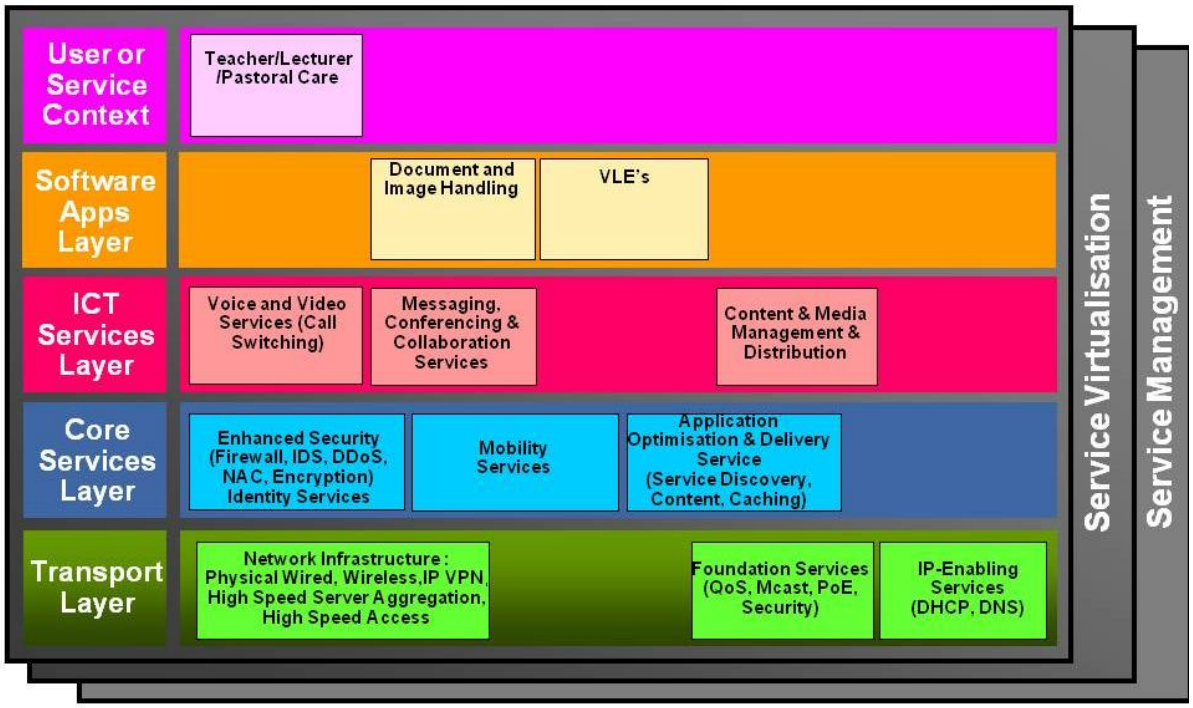


Figure 4.2.1 – Conceptual Architecture Showing University Admissions Clerk

Again take the example of a Replication service., more aligned to a University. This does not require all the layers, and so there would be no entry in that layer, i.e., Replication Services use software such as EMC-SRDF, but does not require any of the ICT Services. This line remains clear.

> Replicate ➔ EMC SRDF ➔ Enhanced Security, Fibre Channel Write Acceleration ➔ Fibre Channel, Fibre Channel over IP, VSAN, Underlying Transport Network with QoS, Hardware Compression and Port Security.

See Figure 4.2.2 Below.

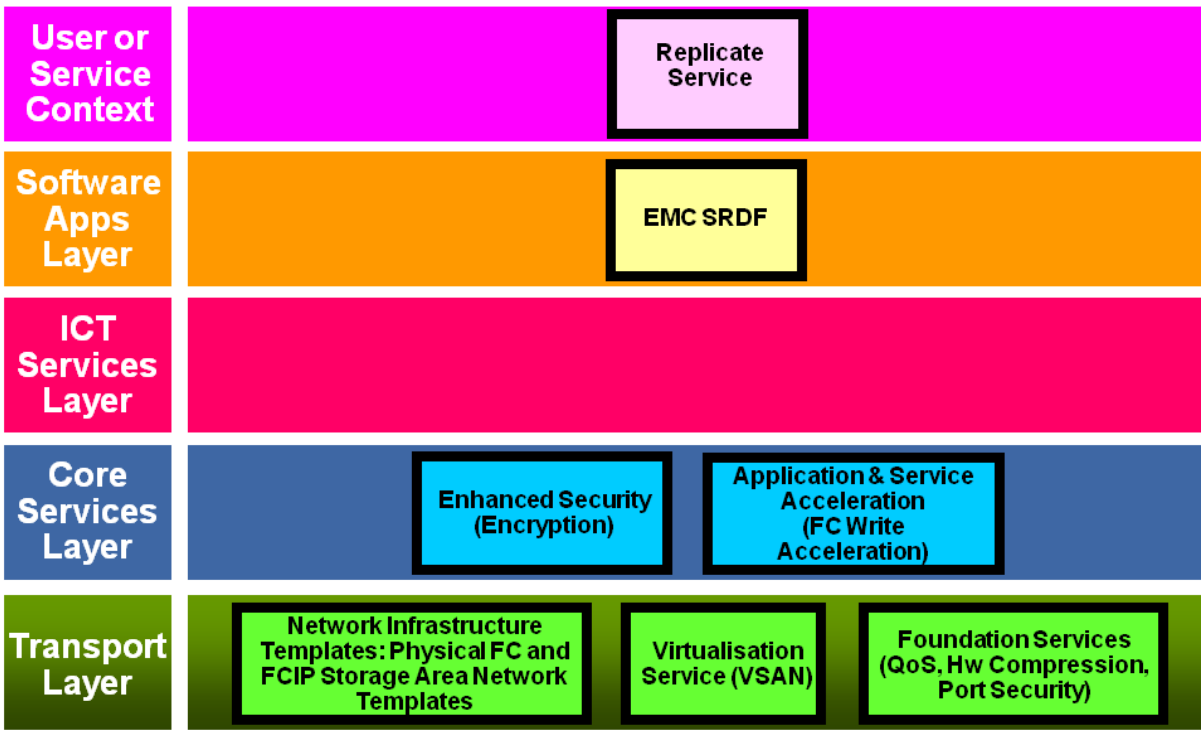


Figure 4.2.2 – Extended use of the TRM

The TRM may be used to fit any user role or service context, i.e. it may be applied to services 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.

5. Foundation (or Physical) Network Architectures

The key Logical Architectures, what they comprise and their relationship to foundation ICT infrastructure are shown in Figure 5.1. This figure indicates the key capabilities each logical architecture provides whilst running over the foundation ICT infrastructure, all working and interworking protected by pervasive layered security:

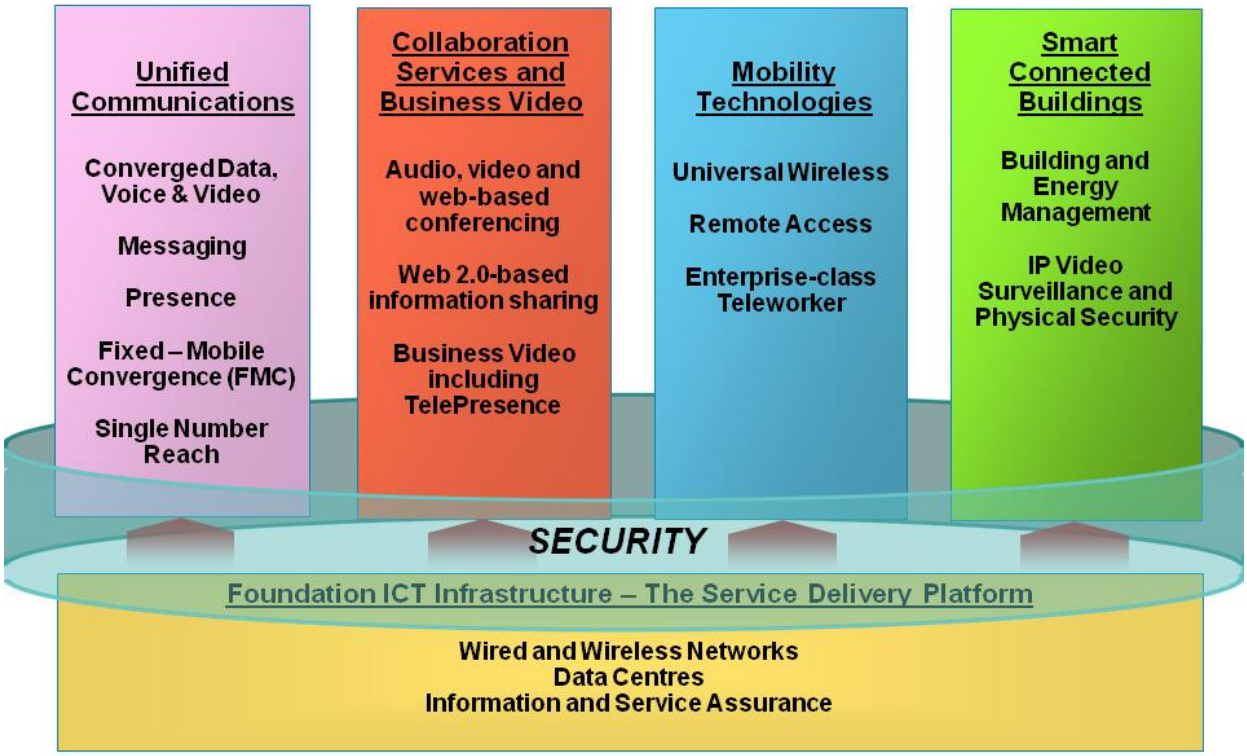


Figure 5.1 – Logical Architectures for the 21st Century Connected Learning Institution

The logical architectures are are described following the foundation infrastructure section.

5.1 Foundation LAN

The Local Area Network is now the key platform for ICT service delivery within any educational institute, providing user connectivity, and a solid baseline for enabling the delivery of more advanced technologies such as Digital Signage, Unified Communications and TelePresence.

Cisco recommends a hierarchical network design model for local area networks. The model uses layered building blocks, with each carrying out a specific role in support of end-to-end information delivery. A layered approach to foundation LAN provides the following benefits to both Higher and Further Education Institutes:

- Scalability;
- Ease of implementation;
- Ease of troubleshooting;
- Predictability;
- Manageability

while still permitting products and features to be specified at each layer that best meet overall functional requirements.

The design model comprises three layers as shown in the schematic in Figure 5.1.1:

The Core Layer – delivers high-speed packet forwarding, typically via high performance Layer 3 switches (or multi-gigabit routers) utilising advanced IP traffic handling capabilities.

The Distribution Layer - provides policy-based connectivity to control user access to the network core. This layer provides the demarcation point between the Access (user) and Core layers of the network, and is where Layer 3–7 policies are applied to control how the network handles individual information flows. Policies can be defined at the Distribution layer to provide security control over access to services, to control Quality of Service mechanisms that apply differential service to applications, and to restrict the advertisement of network resources.

The Access (or User) Layer – connects user end-stations (which may be data or voice devices) into the network infrastructure. This layer allows for logical segmentation of end-stations into groups (Virtual LANs) with common functional and security requirements. Traditionally comprising devices providing fixed wire 10/100/1000 Ethernet ports, the Access Layer now needs to connect to fixed and mobile (wireless) end-points and offer additional capabilities such as in-line power for voice end-points and wireless access points, and support for 802.1x to provide full network user authentication. This is the key point in the network where end device service request negotiation takes place and end point energy control and reporting is conducted.

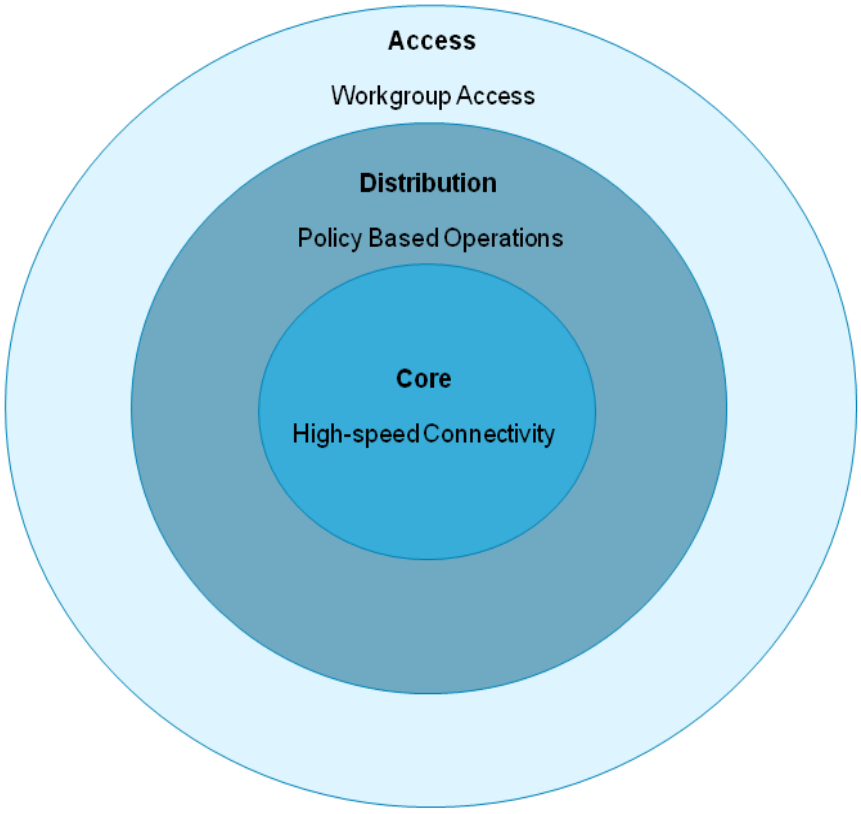


Figure 5.1.1– Graphic representation of the Cisco Hierarchical Network Design Model

A paper describing the Cisco hierarchical network design model for LANs in more detail can be found at: http://www.cisco.com/en/US/netsol/ns340/ns394/ns74/ns149/networking_solutions_white_paper09186a00800a3e16.shtml

Figure 5.1.2 shows how the network design model should be applied to a typical campus. The figure highlights a number of practical considerations for the network design:

- The design is modular in nature affording local scalability without the need for a full network upgrade;
- Each layer should have built-in resilience to eradicate any potential single points of failure;
- Inter-layer connections should be duplicated to build in further resilience;
- Appropriate bandwidth should be provided in each part of the network to meet traffic requirements.

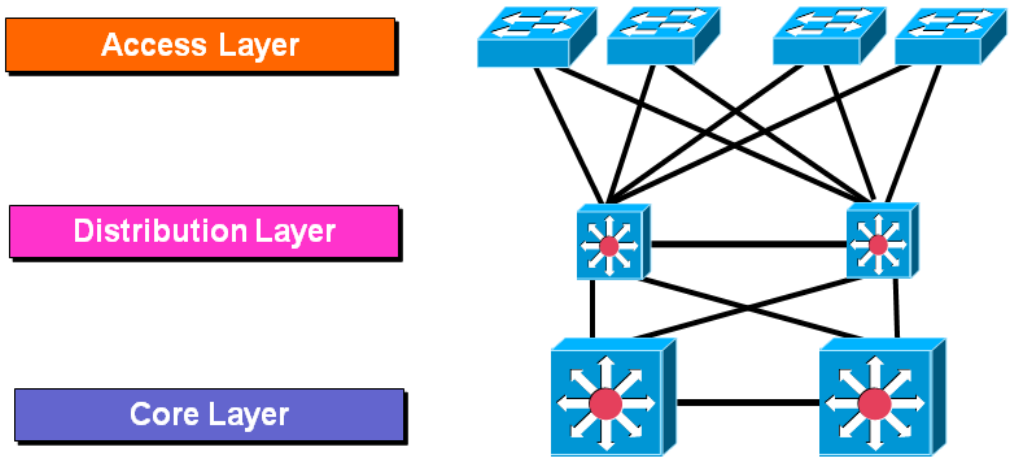


Figure 5.1.2– The 3-Tier Cisco Hierarchical Network Design Model

In addition the above network design model can be optimised for current and future requirements if the following specific recommendations are incorporated:

- Links between distribution/core switches use 10 Gigabit Ethernet to provide maximum levels of scalability;
- Links between distribution/core and access switches use Gigabit Ethernet, bundled Gigabit or 10 Gigabit Ethernet links. Fully resilient links ensure that, in the event of device or cable failure, connectivity is maintained and applications are unaffected;
- Access switches support a mix of 10/100Mbps and 10/100/1000 Ethernet for regular users and 'power' users;
- Power-over-Ethernet on access switches to support Wireless LAN Access Points, Unified Communications end-points such as IP phones and IP Video Surveillance Cameras.

While the above generic model suits large sites, in some instances a consolidated Core/Distribution layer may be sufficient – dependent upon criteria such as fibre capacity, distance limitations, sizing and capacity figures. This is shown in Figure 5.1.3.

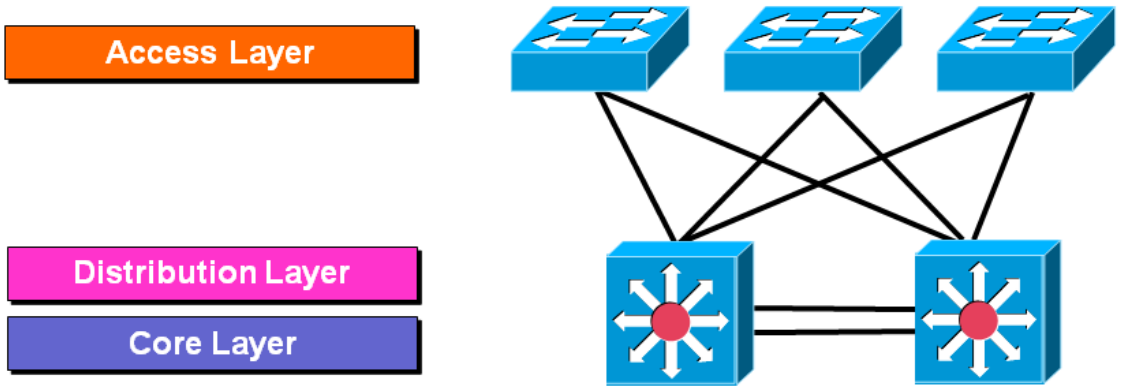


Figure 5.1.3 - The Collapsed Distribution / Core Variant of the Hierarchical Design Model

While the network design model diagrams provide a representation of the physical networks, detailed consideration must also be given to the logical network structures which overlay the physical topology. These considerations include the use of Virtual LANs (VLANs), the use of spanning-tree protocols (STP's), IP addressing structures and optimal IP routing protocols to ensure a robust foundation to support current and future applications.

VLANs provide an easy-to-use mechanism for virtualising campus LANs to create separate logical domains. This is particularly important for departments, such as Finance and Administration, that deal with very sensitive information and who may wish to define their own security policies, for example physical network admission control, policy-based routing or firewall-based access control. Figure 5.1.4 shows how a LAN may be segmented into multiple faculty domains using VLANs.

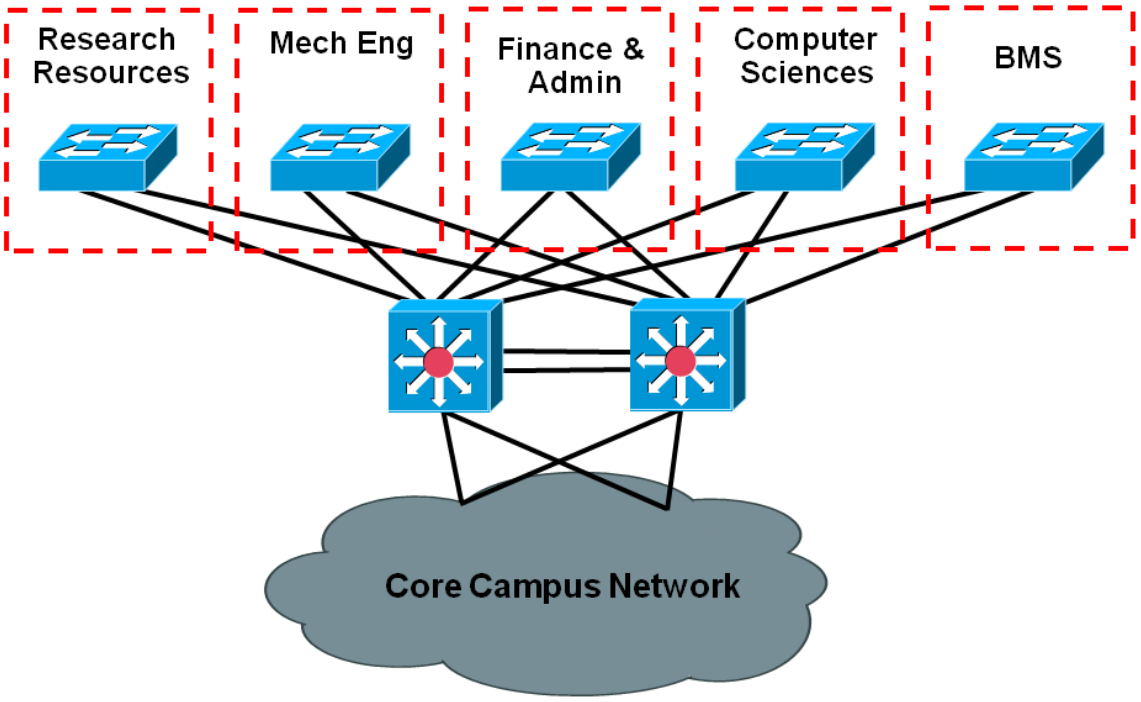


Figure 5.1.4 –Two-Tier LAN with Departmental/Geographic VLANs

Further to this approach, it is now feasible for the network to be further partitioned into multiple virtual routed networks - as a logical extension to that of the VLAN approach- whereby separate faculties, research teams or collaborative partners can be given their own separate virtual network whilst utilising a common physical infrastructure. This approach is discussed in more detail in the Campus Virtualisation Section.

5.1.1 Medianet

Medianet is the next generation of infrastructure with embedded intelligent services that will allow institutions to deploy video applications and services in a scalable and easy to manage manner. This is the unifying point delivering services to, and transport of, all video applications such as TelePresence, Digital Signage, Video Portal, Webex, Unified Communications, and IP Video conferencing to name a few.

There is a consensus that the increase in the use of video within education is growing exponentially, and with the arrival of more bandwidth hungry video applications and high definition end points, network bandwidth on the campus is going to be increasingly in high demand. Medianet simplifies video end point recognition and attachment and efficient video application transport ensuring the available bandwidth is being used to it's maximum potential. This ensures the high quality of experience expected by the participants and viewers of these applications will be met.

Medianet will deliver capabilities which mean that video endpoints will become plug and play, with the ability for them to announce themselves to the access switches they connect to, authenticate securely using 802.1x, and then be permitted onto the network which dynamically allocates the resources and services they require. End points will announce the characteristics they require from the medianet such as bandwidth, jitter and latency, as well as requesting services such as transcription. The medianet will then dynamically ensure these capabilities are delivered for the application throughout the infrastructure.

For further information on medianet please refer to:
http://www.cisco.com/web/solutions/medianet/index.html

5.1.2 Campus Virtualisation

Campus virtualisation techniques cover several topics - two areas in particular will be discussed;

- Virtualisation of Campus Network Devices and Services
- Virtualised Networks

Virtualisation of Campus Network Devices
There are several methods of virtualisation for Campus network devices, dependent upon the devices in question. Devices on which service vitualisation can be achieved include firewalls, where multiple virtual firewalls can reside upon a single physical platform, each firewall instance being a service/device context; load-balancers, where multiple server load-balancers can again reside upon a single physical platform. Devices on which network connectivity virtualisation can be achieved include the Nexus 7000.

However, in reference to the campus network itself, Cisco have now brought to market a solution to address the management, performance and high-availability challenges that are faced in traditional architectures when delivering core/distribution resilience. The Virtual Switching System 1440 (VSS1440) delivers a unified architecture for Core, Distribution or Access layer deployments through the creation of a single logical entity comprising a pair of Catalyst 6500 Series platforms.

By pairing these two devices together various overheads are reduced, when compared with traditional approaches:

- Management
- Resilience
- Bandwidth

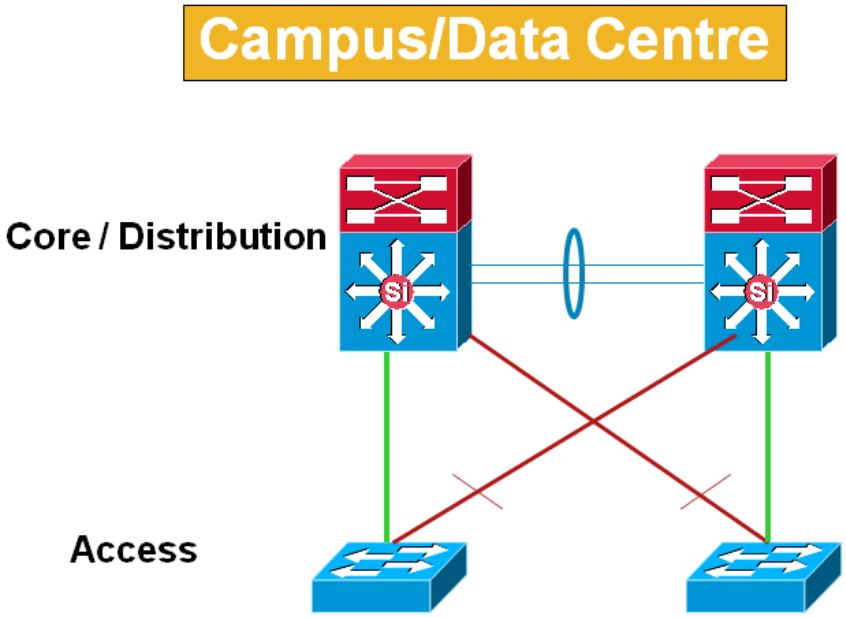


Figure 5.1.2.1 – Traditional L2/L3 Core/Distribution to Access

In the above diagram two Core or Distribution nodes connect to two separate access layer devices. To achieve network connectivity resilience each access device is dual-homed to the upper layer in the hierarchy. However, due to Spanning-Tree being utilised, only one of the links is forwarding – there are techniques available which can result in both uplinks being utilised but these can be complex and create significant overheads for the management of the network. Further to this, the investment which has been made within the cabling infrastructure isn't being realised to its fullest, given only half of it is operational at any one time, resulting in a reduced return on investment (ROI).

In addition, the management of the Core/Distribution layer in this architecture is achieved by managing each node individually, with configuration requirements for First Hop Redundancy Protocols (FHRP's) such as Hot-Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP) or Virtual Router Redundancy Protocol (VRRP). These techniques are necessary in order to provide fault tolerance to host devices, and if mis-configured can result in traffic loss and temporary outage to the services provided by the network.

VSS1440:
Through the use of the VSS1440 technology these challenges can be mitigated, and a highly-available, high-throughput design with simplified management structure can be implemented.

In Figure 5.1.2.2, on the left we have the physical perspective of a VSS1440 deployment, the pair of Catalyst 6500 Series Core or Distribution platforms, with dual-homed interfaces to the access layer. On the right we have the Logical perspective of a VSS1440 deployment, where the two physical Core or Distribution nodes are seen as being a single entity.

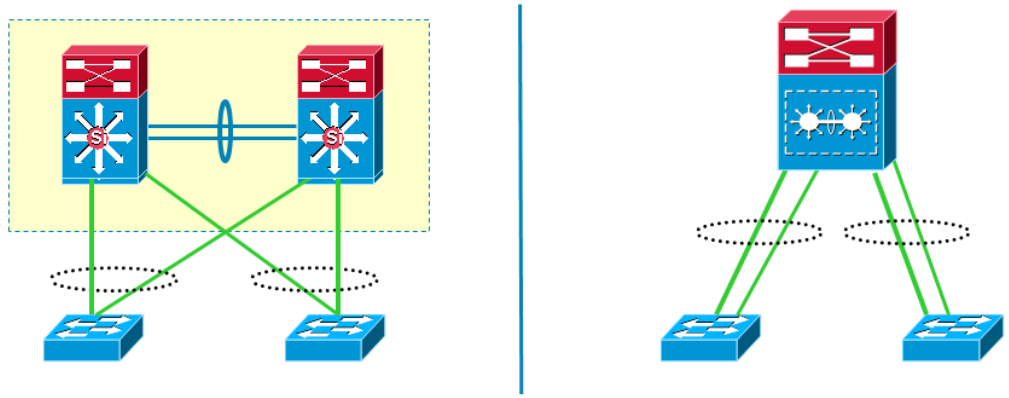


Figure 5.1.2.2 – VSS1440 Deployment

The VSS1440 technology enables the following:

- Improved throughput and Performance;
- A two-fold increase in active bandwidth by utilising both uplinks from the Access layer simultaneously in a single logical EtherChannel (a technique for aggregation of the links bandwidth).

Ease of Management:
VSS1440 creates a single logical entity with a single IP address for management – therefore reducing management by half. In addition to this, a single logical device is seen for configuration purposes, therefore reducing potential mis-configuration points.

Improved Resilience and Reconvergence times:
Given the VSS1440 creates a single logical entity, while enabling cross-stack etherchannel from Access layer to the Core or Distribution points, reliance upon Spanning Tree is reduced from being a loop-prevention mechanism to a loop-detection mechanism. The true impact of this means that reconvergence in event of a link or device failure can be sub-second instead of the 3-5 seconds that Spanning-Tree can achieve today.

Network Connectivity Virtual Devices:
Virtual Devices apply to switches/routers and allow a device to have it's ports and associated services and management separated into multiple groups of virtual switches/routers.

An example of a device which provides network connectivity virtualisation is the Nexus 7000 Series platform. Virtual Device Contexts, or VDC's, are a technology delivered within the Nexus 7000 series platform that enables a single physical device to create multiple isolated virtual versions of the device on the platform.

By creating a VDC within the platform, complete separation from other VDC's is maintained by utilising an isolated set of protocols – both at layer-2 and layer-3 – so that an impact on a routing protocol in VDC Red would not be able to impact any other VDC's running on the platform. VDC's are created and ports are assigned to their operational domain, so the single device appears as multiple platforms.

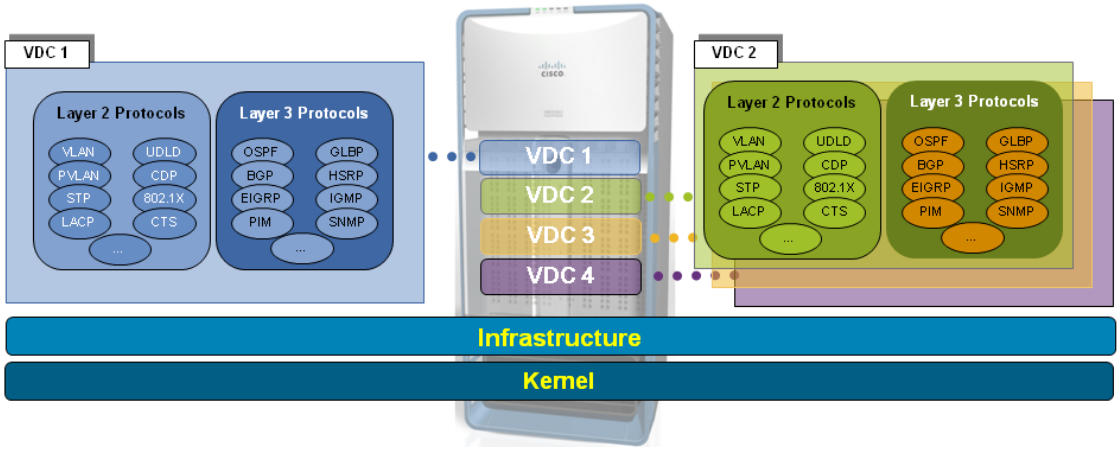


Figure 5.1.2.3 VDC Implementation

By deploying technologies such as VDC's the consolidation of multiple physical networks can be carried out, onto a single common infrastructure – resulting with reductions in footprint, power consumption, cooling, cabling and management – whilst maintaining the high-availability and performance that would be expected from separate physical implementations. VDC's can form a core element to deploying a Shared Services Data Centre Architecture, as discussed in section 5.2.6, though can also enable a Campus Network to be virtualised even further when used in parallel with Network Virtualisation technologies.

Virtualised Networks;
Virtualised Networks enable the single physical infrastructure to be effectively re-utilised for additional requirements with a minimal level of interaction. This capability is commonly known as Path Isolation.

By deploying technologies such as IP/MPLS VRF's or VRF-lite within the campus network, areas which would traditionally require totally separate networks or overlay networks can be deployed on a common network architecture. These technologies effectively deliver isolated infrastructures, so for example, where CCTV networks are traditionally separate physical infrastructure using their own Fibre or Copper infrastructure, by leveraging IP-based Video Surveillance and the virtualisation technologies, a similar approach can be taken though with an "virtual air-gap" between the standard Campus traffic, and the IP Video Surveillance traffic. By deploying virtualisation techniques in this manner, an institute would benefit from reduced Capital and Operational Expenditure through the use of a single infrastructure. The same approach can be taken many times within the infrastructure, providing demarcation from various applications and business processes i.e. finance, IP Video Surveillance/Security and even segmenting students from areas such as business incubation areas, examples of this are shown in figure 5.1.2.4.

Various mechanisms exist to deliver this functionality, varying in levels of complexity, though each delivering their own key points of value. Two technologies currently are widely deployed in this approach – MPLS, or Multi-Protocol Label Switching, or a Cisco innovation known as VRF-lite. Of the two approaches, VRF-lite is the most commonly deployed Campus path isolation technology today, though has a scalability limit of circa 10 – 12 Virtual Private Networks (VPN's), whilst MPLS delivers a much larger scalability.

More information on Path Isolation technologies can be found at:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html

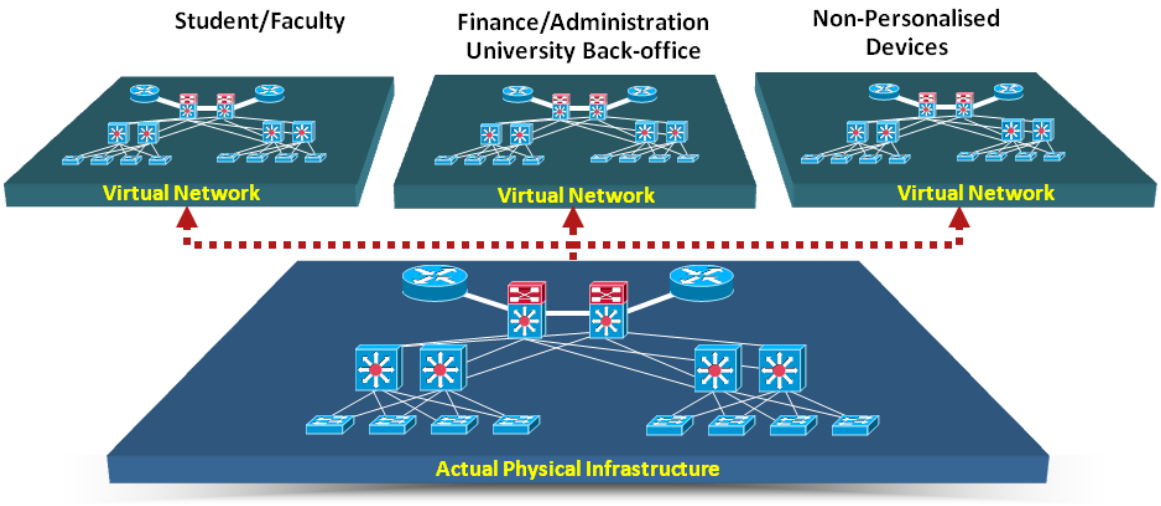


Figure 5.1.2.4 – Campus Virtualisation

5.2 Data Centre

The data centre is the central nervous system of an Education Institute, housing the data delivered in day-to-day operations as well as research and education. In the past, data centres typically have not been designed to strategic templates but have developed around stand-alone application platforms. These environments have proved very expensive to operate and unable to offer the agility to respond to the changing business needs of a Higher or Further Education institute.

Modern data centre design, however, affords the opportunity to build a flexible, future-proof environment that can integrate transparently with other components of ICT infrastructure using a series of complementary functional layers:

- IP Network Infrastructure (The IP Data Centre);
- Application Optimisation;
- Data Centre Security;
- Business Continuance Networking.

Essentially the data centre forms a building block within the modular campus architecture, with a very similar approach – featuring a Core, Distribution and Access layer, depending upon the scale requirements – figure 5.2.1

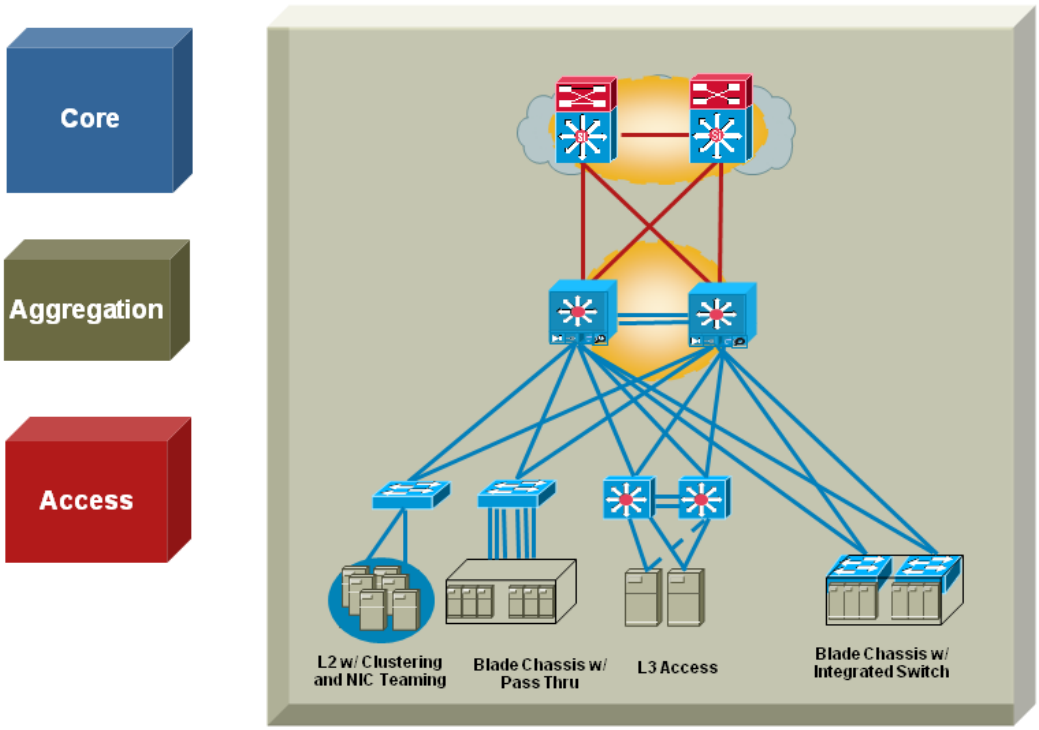


Figure 5.2.1 – Data Centre Modular Design

One additional component that resides within the data centre block is that of the Services layer – this would be the location for deploying Security, Server load balancing, SSL off-load and other service optimisation techniques, figure 5.2.2 Data Centre Services Aggregation Layer:

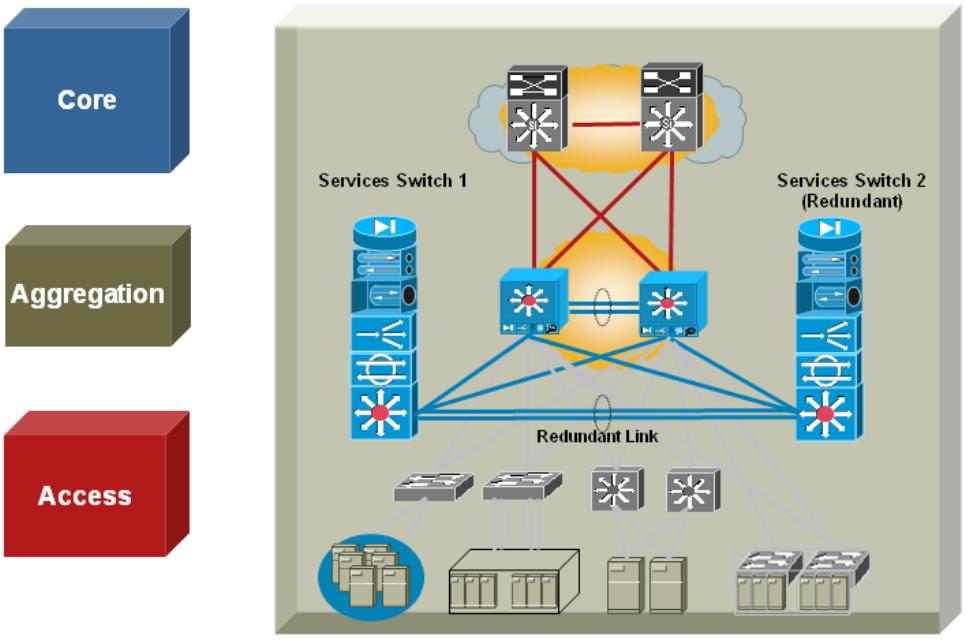


Figure 5.2.2 – Data Centre Services Aggregation Layer

5.2.1 Virtualisation in the Data Centre

Virtualisation can be defined as 'the pooling and abstraction of resources and services in a way that masks their physical nature and boundaries from users'. In effect it is the ability to deliver a personalised service without the need to architect a dedicated system for each service or each user.

The availability of virtualisation for data centres has transformed legacy designs to provide service-oriented infrastructure; a key enabler for automation, higher server and storage utilisations and lights-out operation. Virtualising data centre infrastructure decouples application processing and storage from physical resources, providing ICT managers with the opportunity to deliver and maintain more efficient, resilient and agile data centre services. The key benefits of virtualisation for both Higher and Further Education institutes include:

- Lower total cost of ownership (TCO): Virtualisation helps ICT achieve higher utilisation rates and power efficiency, greater operating efficiency, lower capital costs and carbon footprint savings;
- Improved resilience: The abstraction offered by data centre virtualisation enables non-disruptive planned downtime and more rapid recovery from unplanned outages;
- Greater agility: A fully orchestrated virtualised infrastructure can respond quickly to new application demands and service requirements because IT is not constrained by a predetermined relationship between services and physical hardware.

Virtualisation services can be implemented at a number of points within the data centre as shown in Figure 5.2.1.1. Within the LAN and SAN networks; IP fabric, SAN fabric, firewalls and server load balancers all of these can be virtualised. Within the server pool; physical servers may be dynamically provisioned to meet changes in processing demand driven by fluctuating user loads or the need to provide a new application function. Within the storage pool; storage may be provisioned to meet fluctuating application demands.

Virtualisation offers the ability to provision processing elements – IP network, firewall, server load balancing, server and storage – on demand to meet new or changing needs. This approach decouples logical data centre requirements from physical capacity and permits ICT managers to respond to business needs in a way that has not been possible in the past.

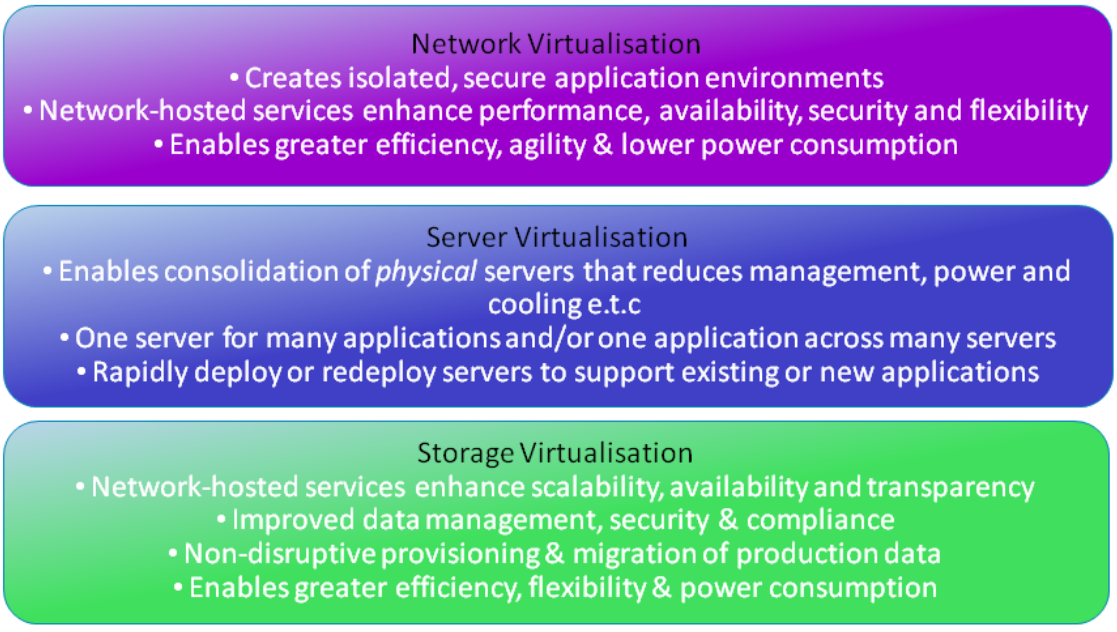


Figure 5.2.1.1 – Data Centre Virtualisation

An emerging technology known as FCoE – Fibre Channel over Ethernet, enables both consolidation and virtualisation to be deployed at the access layer of the network.

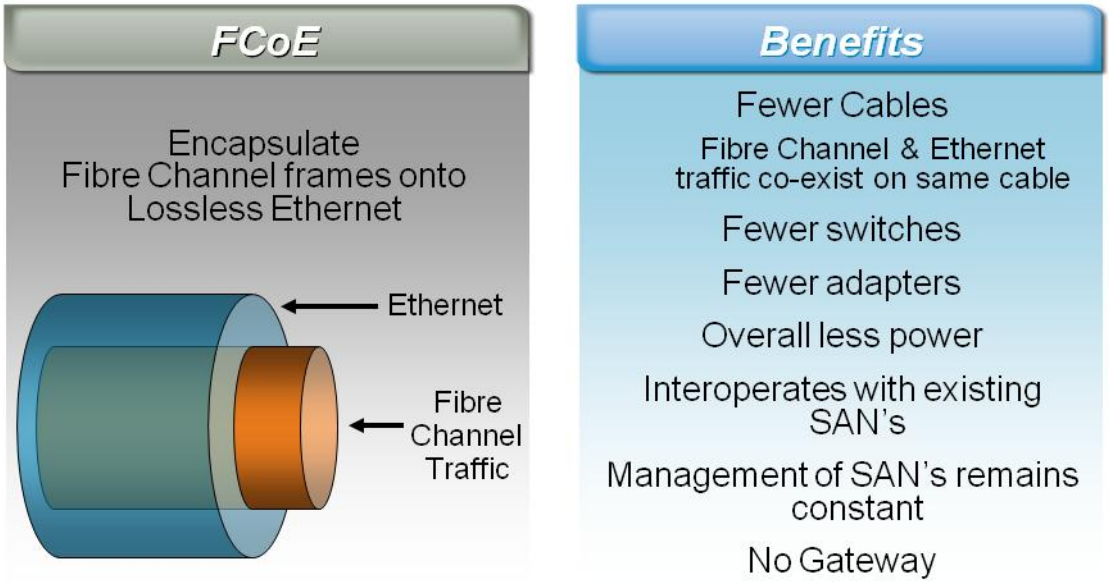


Figure 5.2.1.2 – Fibre Channel over Ethernet

Essentially a platform, such as the Cisco Nexus 5000, is deployed at the Access layer to provide a dedicated 10Gbps link to the Server platform – which can then take advantage of the increased I/O capability that Server Virtualisation techniques by vendors such as VMware, Microsoft or Xen offer – though the real value of FCoE is through the ability to transport Fibre Channel frames over an enhanced Ethernet based network fabric. These enhancements are all based upon Standards revolving around the necessity of enabling Ethernet to become a "lossless" infrastructure, in order to enable the unification of the traditional "lossy" Ethernet-based front-end fabric and the lossless back-end storage fabric utilising Fibre Channel.

By reducing the footprint required at the Access layer much greater economies of scale can be recognised, whereby there is a reduction in switches by 50% (a single Nexus 5000 can replace one Ethernet switch and one Fibre Channel switch), a reduction in adapters in the server by a minimum of 50% and sometimes greater dependent upon the architecture currently deployed, whilst a parallel impact is in the reduction of cabling, rack-space, power and cooling required to deliver the solution, resulting in the Unified Fabric.

FCoE Consolidation and Virtualisation

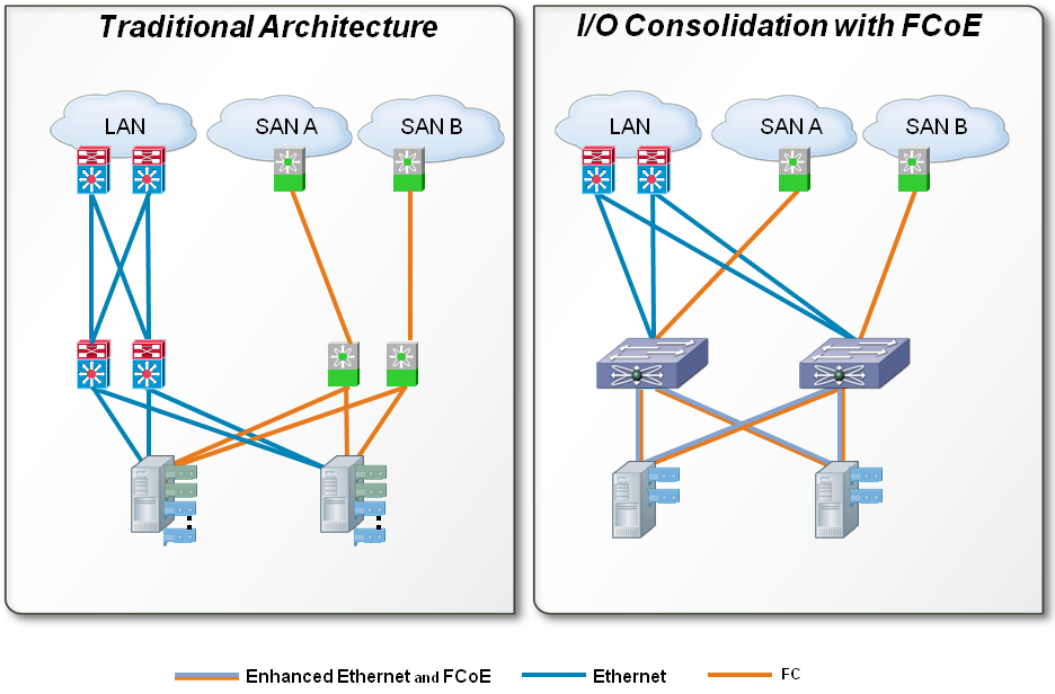


Figure 5.2.1.3 – FCoE Consolidation and Virtualisation

5.2.2 Compute Virtualisation

Compute capability is a major focus within the data centre, being the key resource to enable the delivery of applications and services within an Institute. There have been many approaches to providing Server's ranging from Mainframes, through to today's architecture of Blade Servers, each providing benefits over and above the last iteration – yet deployed primarily based upon the requirements of the application.

With the large-scale use of server virtualisation technologies and the long-term view of Cloud Computing, a differentiated architecture known as Unified Computing is required. Cisco addresses the requirement for the new architecture through the UCS platform – Unified Computing System. UCS is based upon several key building blocks:

- Blade Server Architecture
- Unified Fabric
- Fabric Extension
- Memory Expansion
- Service Profiles

Blade server architecture enables higher density of compute capability to be deployed within a smaller area than would normally be available when using traditional rack-mount servers. Cisco has partnered with Intel to base the blade servers upon the next-generation Intel Xeon 5500 Series processors, delivering a significant enhancement in capability.

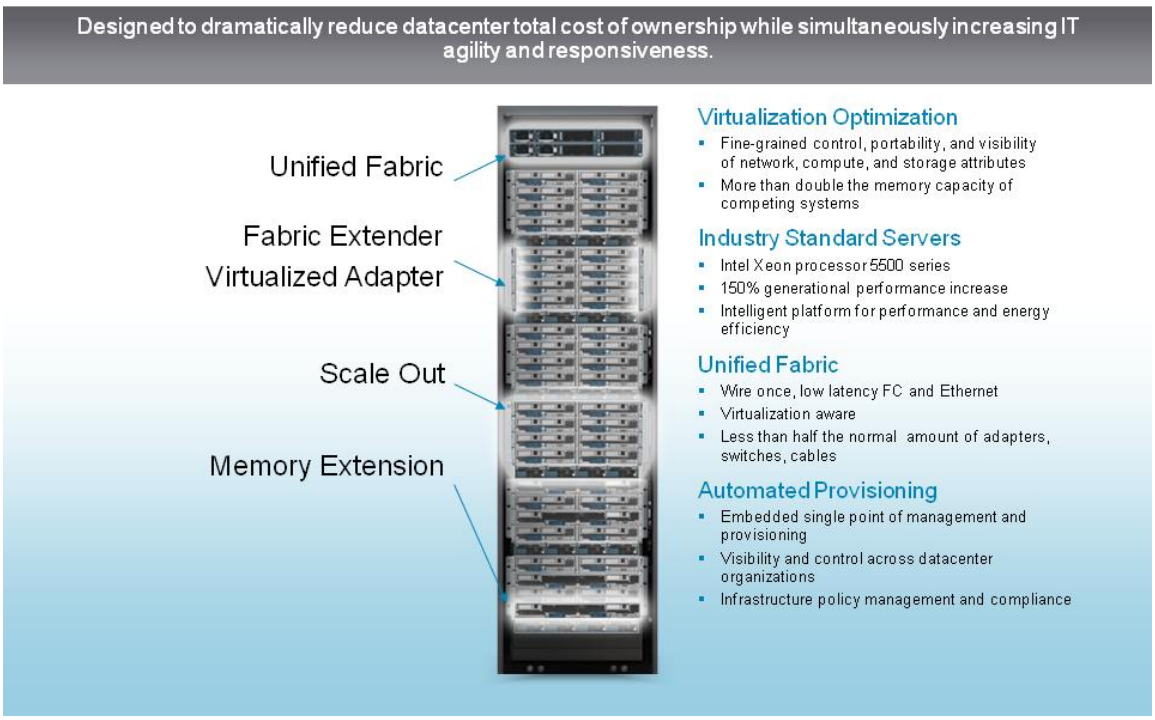


Figure 5.2.2.1 – Unified Computing System – Key components

The UCS architecture enables scalability from a single blade server chassis – containing up to 8 blade servers, through to a maximum of 320 blade servers within 40 blade server chassis. The entirety of this compute real-estate is managed via a single point, providing immense levels of scalability married with a "single pane of glass" approach to management, reducing the overhead for deployment and maintenance of applications and services.

The Unified Fabric and Fabric Extension capabilities enable the UCS to take advantage of technologies such as Fibre Channel over Ethernet (FCoE) and provide 10-Gigabit Ethernet connectivity to the Servers – which, with server virtualisation increasing, provides a much more efficient method of providing I/O connectivity to hosts than traditional approaches. One standout benefit of 10-Gigabit Ethernet to the server is the "wire-once" approach, which enables the typical number of server interfaces to be reduced from an average of 8 individual Gigabit Ethernet interfaces today, to a pair of 10-Gigabit Ethernet interfaces for resilience. This dramatically reduces the required quantity of NIC's, HBA's, switches, cables and the inherent rack-space necessitated by other solutions.

Two areas of significant innovation within the UCS architecture are Cisco Memory Expansion and Service Profiles.

Cisco Memory Expansion technology enables a single blade server to have up to 384GB of local RAM, over 2.5 times greater than traditional architectures. This becomes significantly beneficial when looking at large database applications or within large density Virtual Machine deployments. In parallel to the performance improvements that can be gained through this technology, is the price/performance, as the Cisco Memory Expansion capability enables up to 48 DIMM's to be provided on-board – populated with a range of memory DIMM's – typically 2, 4 or 8GB. Given that memory pricing is non-linear, it can be more cost effective to deploy a larger density of say 4GB DIMM's than a smaller density of 8GB DIMM's to achieve the same memory footprint.

Service Profiles are complementary to server virtualisation, whereby stateless computing can be achieved. In traditional architectures Servers have an identity – be it their LAN MAC address, SAN WWN, their BIOS

settings – through the use of Service Profiles server identity is now an abstraction layer held within a service profile. Server modules can now be re-profiled at will, enabling a defined server real-estate to become essentially a multi-purpose, stateless entity for deployment on demand – which, when deployed alongside technologies such as VMWare Vmotion, enables a powerful virtualisation capability for compute resources. By deploying Service Profiles a reduced footprint of compute is required within the Institute, by enabling an "on-demand" re-profiling of compute resources to meet the application and services needs.

The UCS architecture inherently provides a significant reduction within both Capital and Operational Expenditure. Given the single point of management, Unified Fabric and integrated Fabric Extension capabilities there is a significant reduction in the physical footprint required to deploy the solution, which enables a rationalization of power, cooling and rack-space, as well as a simplified cabling strategy for interconnection of the Compute through to its main I/O focus of users and storage.

5.2.3 Application Optimisation

Most institutes are increasingly seeking solutions that offer:

- improved control over the application performance and resilience;
- aggregation of applications centrally to simplify management and control;
- delivery of secure and accelerated services to users both on campus and externally.

The following section shows how these goals can be addressed.

Content Switching:
The increasing use of centralised, web based applications means performance, scalability, security, and availability of application servers becomes business-critical. The ability to share user load over a cluster of servers using content switching is critical to application performance and resilience.

Content switches are able to inspect application message content, and route messages to individual servers based on pre-defined policies. These policies might include how to handle messages with particular user information, security information or application requirements. In addition, content switches are able to monitor the health of individual servers and provide automatic failover by routing messages to back-up servers in a cluster.

Application security is also becoming ever more important and institutes are seeking to protect both staff and student information through the use of secure, Secure Sockets Layer (SSL), web traffic. Individual servers are not optimised to handle the encryption of SSL traffic so the need has arisen for scalable, cost-effective SSL termination capabilities to be built into network hardware. These capabilities complement content switching, and free up server performance for application handling.

5.2.4 Data Centre Security

Data centre security provision must be aligned with overall organisational security policies, and address specific considerations including:

- Security of the data centre perimeter against external threats;
- Security of the boundaries between functional and administrative regions within the data centre;
- Integrity of data and applications;
- Availability of data and applications.

Also critical is identifying the application architecture in use. If an "N-Tier" application is being delivered, then the baseline network security policy needs to take into account the application flow and interactions.

For example, users will access the front end web server, either via HTTP or HTTPS. The Web Server then needs to speak with the Application Logic Server, which can be carried out over a myriad of ports, however, this will only ever be expected to be received from the fixed IP address of the Web Server front-end, vis-à-vis the same approach would be taken from the Application Logic Servers through to the back-end Database servers.

The security policy should take the application architecture and behaviour into account, in order to assist in creating the holistic policy.

5.2.5 Business Continuance Networking

Both Higher and Further Education institutes data centres already house business critical applications and data. As they gradually assume the role of service delivery points for these institutes, they will support a much wider range of applications including unified communications, collaboration, security and building management.

There is a need therefore, for an institution to have a robust business continuance strategy to ensure that business is not impacted through the loss of devices involved in access/storage of student and staff information, or through loss of critical data centre processing function.

ICT managers face a number of challenges in supporting a data centre business continuance strategy:

- Limitations of tape backup: The traditional mainstay of disaster recovery, tape backup is slow and limited in its ability to restore critical applications and data in time to meet recovery time goals. However, its role in maintaining integrity remains valuable;
- Network Facility Costs: Although bandwidth costs continue to decrease, large-scale data centre mirroring and replication require substantial capacity;
- User Access: Business continuance plans often focus on data and application availability, but they often overlook the need for users to access recovered data and applications;
- Cost: Although the cost of business continuance technologies has dropped in recent years, it remains expensive to invest in mirroring software, duplicate facilities and resources, telecommunication services, and appropriate amount of staff.

Business continuance networking is a critical foundation for any business continuance strategy. It provides connectivity between applications and storage/backup resources, connectivity between production and secondary data centres, and optimises user access to applications before, during, and after a disruption. By providing a resilient, high-capacity networking solution, the complete portfolio of business continuance IT solutions from backup to data centre mirroring can be supported.

A business continuance networking solution should provide the following features:

- A highly resilient data centre IP network;
- A scalable, robust storage network;
- High-capacity, low-latency data centre interconnections;
- Resilient, flexible user access.

It is necessary to first understand the specific requirements of the business and its applications regarding business continuity – the two key factors being the Recovery Time Objective (RTO) relating to the longest time an Institute can tolerate a lack of access to its applications and data before resuming operations, while the Recovery Point Objective (RPO) referring to how current or fresh the data is after an outage, RPO is the maximum data loss that an Institute can tolerate after an outage.

The RTO and RPO enable the business, once identified, to analyse the requirement for either Synchronous or Asynchronous replication of data. Technologies such as Fibre Channel over IP (FCIP), iSCSI and xWDM

enable these services, though each have specific use cases, hence the necessity to identify the RTO/RPO requirements and a solution which will meet the business continuity requirements.

5.2.6 Shared Services Data Centre

Shared Services data centres are based upon the concept of institutes sharing a common hardware implementation within the DC, yet maintaining operational separation – through such technologies such as those mentioned within the Campus Vitualisation section, such as path isolation. Through utilising a Shared Services data centre, institutes are able to reduce the overall power/cooling and space requirements that would normally be required, whilst maintaining service delivery.

A common misconception is that Institutes which choose to utilise a Shared Services infrastructure are required to utilise a common set of applications. This is not the case. By use of path isolation for access to the DC, alongside various virtualisation technologies Institutes are able to implement a complete virtual data centre infrastructure which is isolated from other institutes even though it is running on a common network architecture. This extends not just towards the access of the DC, but to the back-end storage of applications and their associated data.

The Shared Services module takes network virtualisation, from a path isolation perspective, and the data centre architecture and tightly integrates them together, enabling the ability to share this single common architecture at a physical layer, yet segmenting the assets as required, from the network, storage and compute architectures.

Shared Services are essentially the beginning of a Cloud Computing model, where assets are abstracted from the hardware layer, administrators work upon a base unit of the hypervisor and manage their unique virtual machines and associated storage in a scalable manner, with resources essentially being transparent to the end user, creating Virtual Private data centres within the shared services facility.

5.3 Wireless LAN

A recurring theme within Education today is the necessity of secure access to information, in a timely fashion, at the point of need. There can be significant periods of time, both in the office and while mobile, where staff and students just do not have access to wired networking points that enable access to the required information. Mobile data devices (PDA's, laptops, netbooks etc) operating across secure wireless networks meet this need; leading to an increases in effective time for staff and associated cost savings, enabling course delivery and material to students on the go, and to service improvements for staff and students interacting, helping to enhance the student experience.

5.3.1 Centralised Wireless LAN

Centralised Wireless LAN has become the de facto standard for delivering wireless campus LAN services. Figure 5.3.1.1 shows the main components of the Centralised Wireless Architecture that may be implemented over local or distributed campus infrastructure; Cisco refers to this architecture as the Cisco Unified Wireless Architecture.

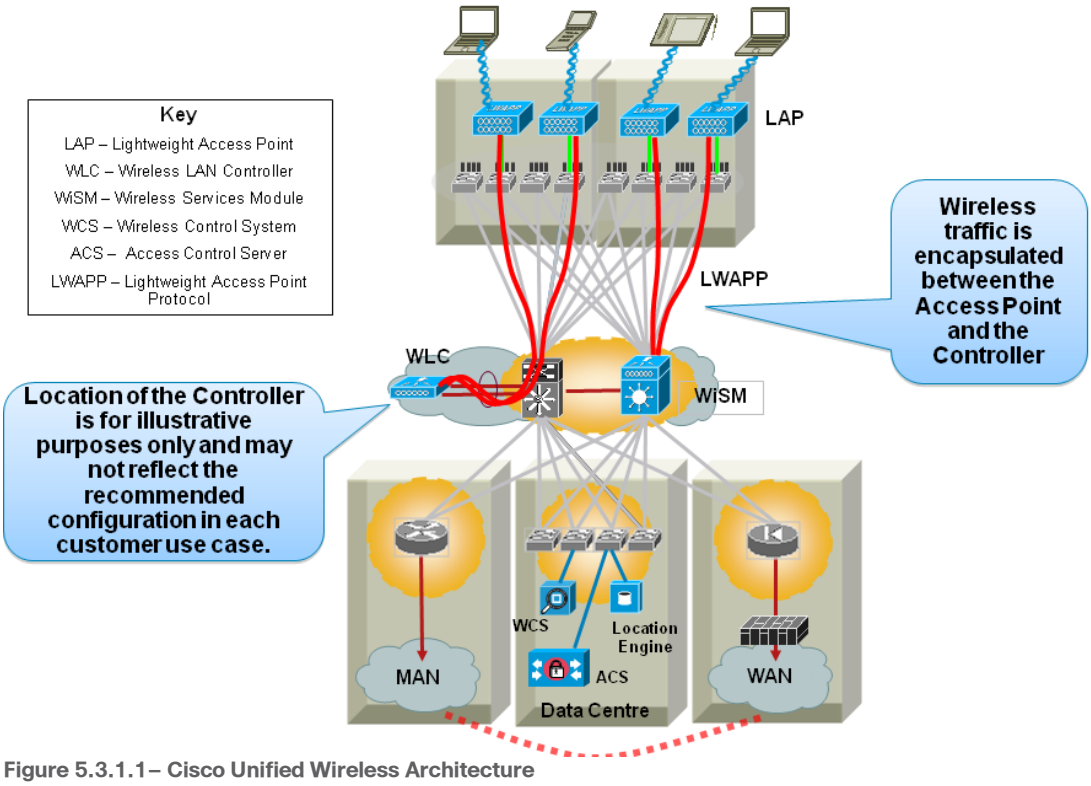


Figure 5.3.1.1– Cisco Unified Wireless Architecture

The central Wireless LAN Controllers (WLCs) may be a standalone appliances or modules located in core network switches (Catalyst 6500 WiSM modules). Wireless Access Points connect to the central controller for control and management using either the CAPWAP protocol (Control and Provisioning of Wireless Access Points) or Lightweight Access Point Protocol (LWAPP) protocols. These protocols have two primary functions:

- Control and management of the Wireless Access Points;
- Tunnelling of WLAN client traffic to the central Wireless LAN Controller.

The benefits of the centralised architecture include:

- Fully-centralised configuration and control through the Wireless LAN Controllers;
- Simplified operational management by collapsing large numbers of managed Wireless Access Points into a single managed system;
- Lower cost 'Lightweight' Access Points controlled by the Wireless LAN Controller;
- Security policies, QoS policies, Radio Frequency (RF) management and mobility management are all centrally controlled.

With the innovative Cisco Client Link capabilities Cisco's range of 802.11n AP's offer industry-leading wireless performance, up to 169 percent faster than wireless from other vendors through Intel and Cisco's collaborative working, as shown in White Paper for the test results from Intels Over-the-Air test facility[14].

[14] Test results for Cisco's 802.11n throughput and coverage:
http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_c11-492743_v1.pdf

5.3.2 Secure Mobility

In the early deployments of Wireless LAN one of the key objections was security; that is integrity of the Wireless LAN itself and confidentiality of information traversing it. With current security methods and implementations Wireless LAN access is one of the more secure ways to access information.

In an Educational environment the required level of security depends upon the requirements of individual departments or user communities, however consideration should be given to:

- Authentication: using standards based or well known protocols such as 802.1X, EAP, and RADIUS. These protocols allow access to be controlled based upon the successful authentication of the WLAN client and just as importantly in the WLAN environment allows the WLAN network to be authenticated by the user, i.e. authentication is mutual. Authentication could also be merged with a Network Admission Control solution as described later in section 5.3.5.
- Encryption: using standards based solutions known as WPA and WPA2. These encryption types are Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES). TKIP is the encryption type certified in WPA supporting legacy WLAN equipment and addressing flaws in earlier solutions. Alternatively AES encryption of WPA2 is the recommended encryption mechanism as it brings the WLAN encryption into alignment with current encryption best practice.

Cisco also offers the following value-added security features in its Wireless LAN solutions:

- Wire detection—a mechanism for tracking and correlating the rogue device to the wired network;
- Wireless Intrusion Detection System (IDS) - The Wireless LAN Controller (WLC) performs IDS analysis upon all its connected Access Points, and reports detected attacks; Rogue Access Point Detection – Cisco's Unified Wireless Network provides a complete Rogue Access Point solution including;
- Air/RF detection—detection of rogue devices by observing or sniffing beacons and responses;
- Rogue Access Point location—use of the detected RF characteristics and known properties of the managed RF network to locate the rogue device;
- Rogue Access Point Isolation —a mechanism to prevent client connection to a Rogue Access Point;
- Management Frame Protection - Cisco mitigates these attacks using a digital signature mechanism to insert a Message Integrity Check (MIC) to 802.11 management frames. This allows the legitimate members of a Wireless LAN deployment to be identified, and therefore allows the identification of rogue infrastructure, and spoofed frames, through their lack of valid MICs.

5.3.3 Borderless Wireless LAN

Traditionally "wireless LAN" has been a phrase coined with reference to wireless connectivity within a building, conference room, lecture theatre or even a hotel room. However, there are technologies available, such as Cisco Wireless Mesh, which enable the wireless LAN to be extended to become truly campus wide, providing External as well as internal connectivity for users and other resources.

Based upon the 802.11 standards, using 802.11a as the backhaul mesh connectivity, and 802.11b/g for user connectivity, devices are able to take advantage of high-speed connectivity without the need to refresh their client devices. Utilising the Centralised Wireless LAN architecture, the External Wireless Mesh solution benefits from the inherent ease of management delivered through the Wireless Control System (WCS) providing a single point of management for both external and internal mobility services.

Wireless network resilience is provided by creating a Mesh architecture. A RAP, or Root Access Point, serves as the primary Root AP to the Wired network, which can connect up to 35 Mesh AP's, a secondary RAP can be deployed to provide resilient connectivity into the wired network. The MAP, or Mesh Access Point, delivers both user access and establishes a self-healing mesh between itself and other MAP's within the Mesh architecture. The MAP will then utilise Cisco's Adaptive Wireless Path Protocol to identify the shortest path to the RAP, and will have a backup path to the secondary RAP to provide resilience for services delivered over the mobility infrastructure.

For more information on Outdoor Wireless visit:
http://www.cisco.com/en/US/products/ps5679/Products_Sub_Category_Home.html

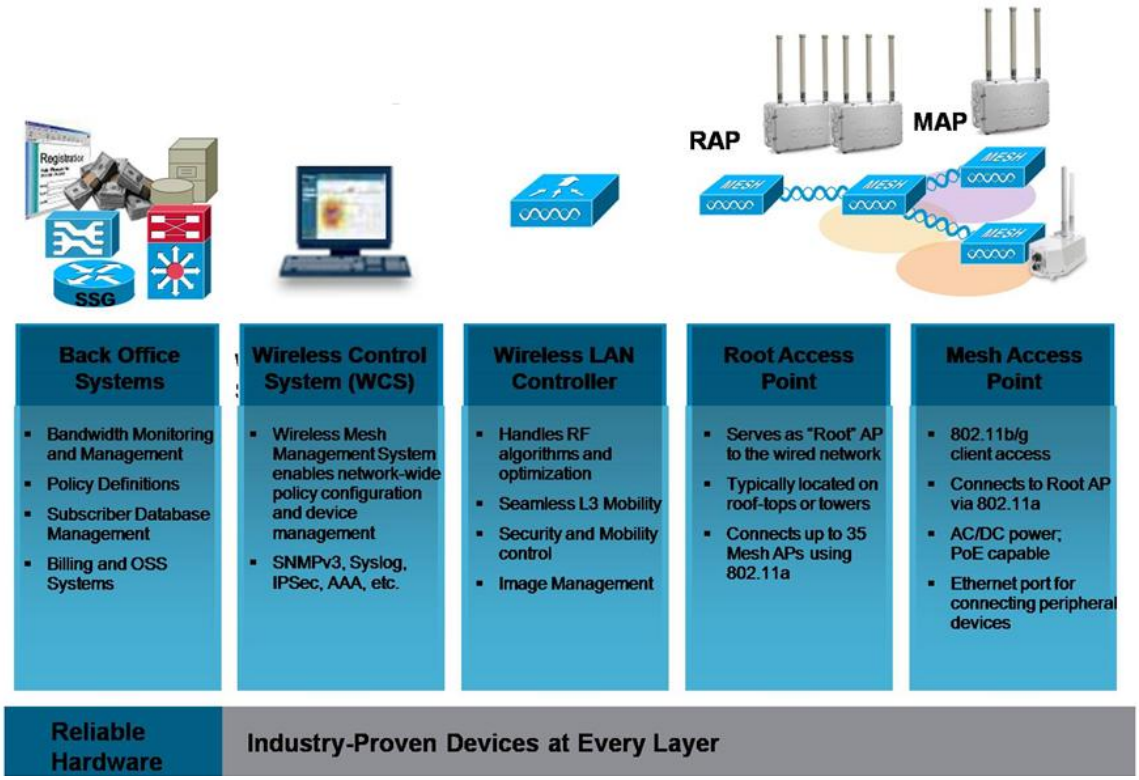


Figure 5.3.3.1 – Outdoor Wireless Mesh Components

5.3.4 Wireless Mobility Services

Upon deployment of a Centralised Wireless Architecture, mobility services can be utilised over the platform of ubiquitous wireless. Various services exist today, ranging from Context-Aware Location Services, through to adaptive Wireless Intrusion Prevention Services.

The cornerstone of Cisco's Mobility Services strategy is the Cisco 3300 Mobility Services Engine (MSE). The MSE is an appliance based solution which transforms existing Wireless LAN's into Mobility Networks. The platform is extensible to support a variety of mobility services in a modular fashion. The MSE is a platform based upon a combined hardware and software solution which:

- Simplifies provisioning and management of mobility services
- Offers scalable and reliable multi-device, multi-network application delivery
- Facilitates a broad partner eco-system for mobile applications development

Unified Application Delivery:
The Cisco 3300 Series MSE abstracts applications and services from the underlying control network to optimise performance and reliability while reducing the operational complexities associated with business mobility. The architecture unifies application delivery across Wi-Fi, Ethernet, WiMax and Cellular networks (making it data transport agnostic) while preserving security and manageability.

Figure 5.3.4.1 shows a graphical representation of the Cisco Mobility Services solution architecture:

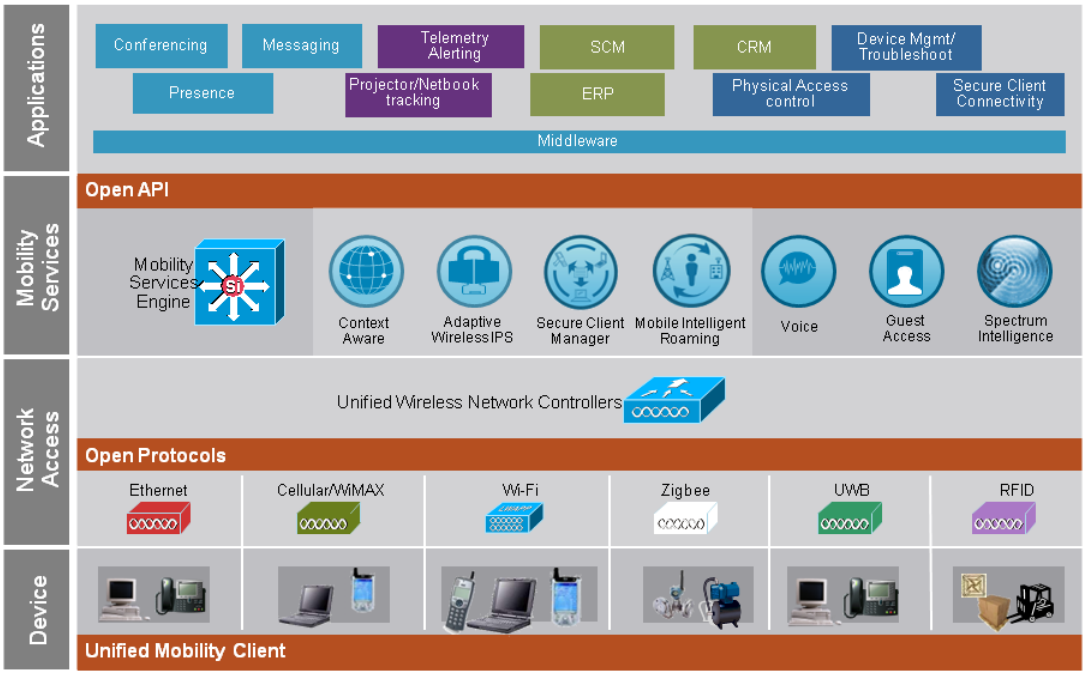


Figure 5.3.4.1 Location Services

One business challenge many institutions face today is the location management of key assets; including service type personnel, portable ICT equipment, information signage monitors, LitePro projectors and similar within lecture rooms or collaborative environments but also extending to a wide variety of assets held in stores and logistics locations. In healthcare for example, location services with application integration into Cisco wireless phones, for tracing mobile equipment and hospital porters is embraced as a high value-add service that exploits existing capital investment in Wireless LANs. This trend will increase with vendor plans to incorporate WiFi tags into PCs and similar devices during the manufacturing process. The technology can genuinely reduce cost and operational inefficiencies associated with the misplacement or loss of high-value assets.

A Location Services solution to track assets can exploit an existing Wireless LAN to actively track assets through the use of WiFi tags attached to key assets. Figure 5.3.4.2 shows a location-aware unified wireless network overlaying a campus network design.

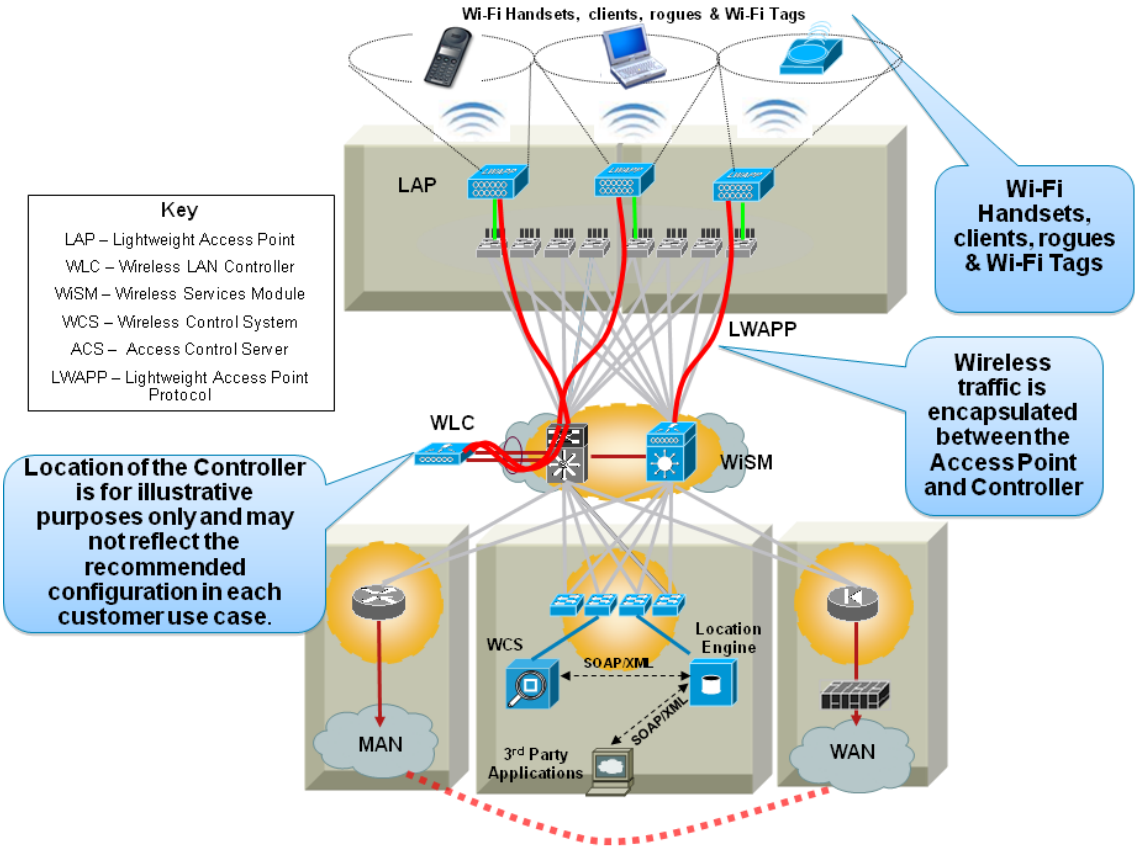


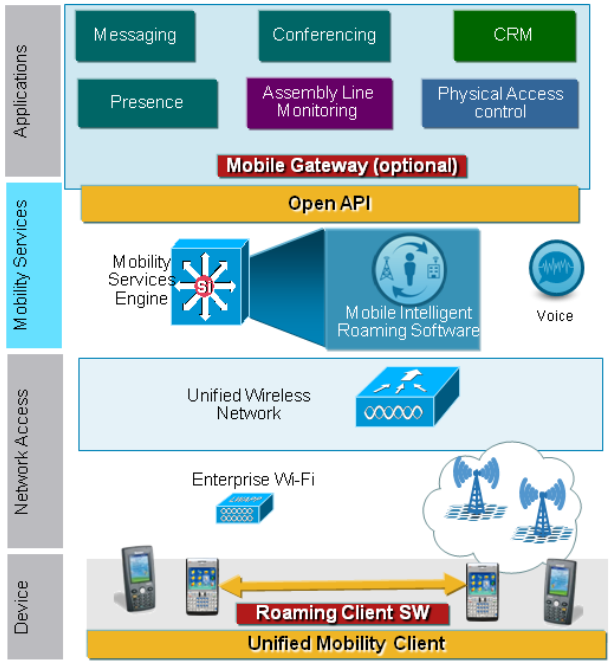
Figure 5.3.4.2– Location Services Architecture

Each access point forwards information to the central WLAN controllers regarding the detected signal strength of any WLAN clients including WiFi asset tags. The signal strength information from every access point is aggregated by the WLAN controllers to build up a two dimensional picture of the location of assets relative to access tags. The Location Services appliance polls each WLAN controller for the latest signal strength information for each category of WiFi-tagged device; hence is able to place each asset onto a logical building plan to report location. This process takes place in real time such that if a WiFi-tagged asset passes through a chokepoint zone, such as an exit, then an immediate alert can be sent to the security department or to the asset owner.

5.3.4.2 Fixed Mobile Convergence Services

A software component within the Mobility Services Engine architecture, known as MIR or Mobile Intelligent Roaming, acts as one of the enablers for Fixed Mobile Convergence (FMC) Services.

The MSE plays a key role within an FMC deployment, acting as the centralised intelligence to provide WLAN assisted hand-off of clients between GSM and Wi-Fi networks. See figure 5.3.4.2.3 for the components to enable an FMC/Mobile Intelligent Roaming solution.



- **Enterprise-grade** notification that can be sent to a Mobile Gateway or to a Roaming Client from various partners for **network assisted intelligent roaming**
- Cisco Partners such as;

Service Providers lacking Enterprise Network Visibility

Device Manufacturers willing to increase the dual-mode phone users' experience

3rd party vendors mobilizing enterprise unified communications

Figure 5.3.4.3– Mobile Intelligent Roaming

Please see section 6.1 for further detail of Fixed Mobile Convergence within the remit of Unified Communications.

5.3.5 Guest Access

Given the transient nature of Staff and Students or fee paying conference attendees, whether involved in research, on-site conferences or even for visitors or contractors attending site, it is necessary to be able to provision access for those users to resources either on the local campus, or from their home organisation. With this in mind, Guest Access solutions are being reviewed as a mechanism to simplify the delivery of this functionality.

One way to achieve this is to use the virtualisation features of Wireless LAN such that non-secured guests can share infrastructure, but not access to applications, data or other services, with secured users from the local institute. This is a very practical approach to guest access as it requires no ongoing configuration changes to wired network infrastructure. Providing a logical Wireless LAN for guest access allows guests to achieve connectivity to their 'home' organisation using VPN technology; the same capability can provide Internet access for visitors.

Figure 5.3.5.1 illustrates a typical guest access deployment. The guest user is provisioned on the network and assigned network credentials. Once the guest has a username and password and they open a browser they are authenticated using the guest SSID identifier. The Wireless LAN controller recognises this user as a guest and segments the traffic onto the 'Guest' VLAN. The guest traffic is encapsulated in an Ethernet over IP tunnel to the 'anchor controller' in the DMZ and subsequently routed separately from the Institutes network. Once a guest user's credentials expire, access to network resources is terminated.

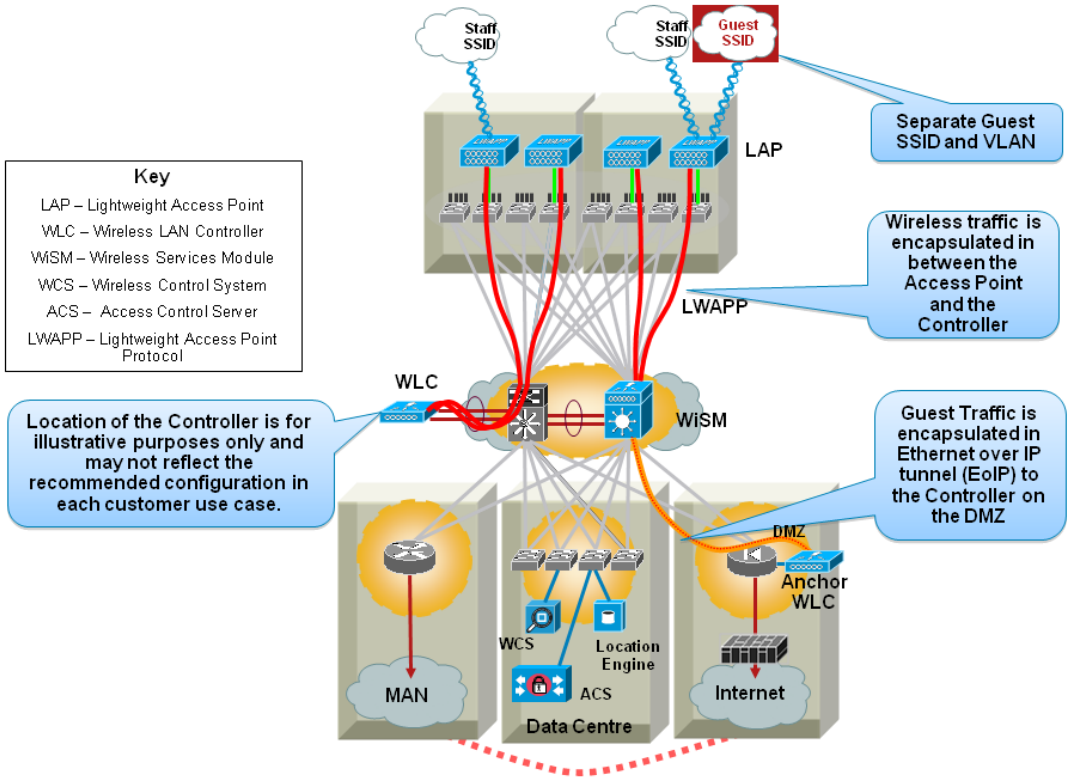


Figure 5.3.5.1– Wireless LAN Guest Access

In certain deployment scenarios, an institute might require a separate guest provisioning appliance to facilitate the creation of guest accounts, management of guest access policies, and reporting of guest network use. The Cisco NAC Guest Server (NGS) offers a centralised capability interface for all guest account creation and guest policy management. The NGS is ideal for institutes which need to provide Internet access to visiting staff, other agencies and visitors as it provides a centralised reporting interface to track statistics on both guest access account and guest network use.

5.3.6 Voice Over Wireless LAN

In an Education environment Wireless LAN infrastructure can support mobile voice as well as data services, enabling both staff and students to communicate with each other at any time and in any place. To achieve this, it is essential that Wireless LAN infrastructure is designed for high availability and with the features to support voice services. There are a number of key design considerations that must be addressed, including:

- Bandwidth: Codecs 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 across access points.

Cisco supports Voice over Wireless LAN voice with a range of wireless IP handsets supporting the Unified Communications solution described in Section 6.1.

5.4 Foundation MAN and WAN

All institutes utilise the JANET core, with regional Metropolitan Area Networks (MAN) for connectivity to external resources. Most HE institutes use a minimum of a single Gigabit Ethernet connection, though given the rise in collaborative technologies as well as the advent of increased video utilisation (i.e. YouTube, BBC iPlayer) there is a move to utilising 10-Gigabit Ethernet as the primary medium of external connectivity. Whilst most FE institutes use a 100Mbps to Gigabit Ethernet connection, connecting directly to the Regional MAN or as a Secondary connection via the Primary Institute local to that region.

In previous incarnations the regional networks provided a single connection to the Institute. With the need and willingness to collaborate becoming more and more a driver for "always-on" connectivity, most institutes are now being offered a dual-connection approach – with active/standby connectivity being the most common deployment, dependent upon the regional MAN operator.

In some cases it is necessary for an Institute to utilise a separate method of external connectivity, where partners may not be a JANET sponsored connection – providing monitoring or remote-diagnostic services, as well as for users on-site such as conference users, who cannot use the JANET connectivity. In this instance, typically a broadband connection is utilised to a local, regional or national provider for a business grade broadband circuit.

Colleges and Universities should be looking to it's regional MAN to deliver Service-Provider class services, utilising highly available, resilient solutions throughout the architecture, providing highly scalable bandwidth capacity. They should typically be capable of providing value-added services such as DNS resilience, IPv6 Unicast and Multicast services as well as Quality of Services - enabling differentiated levels of SLA to enable delivery of services such as Business-to-Business Unified Communications, video conferencing services or Shared Services data centres. As Institutes migrate to Shared Services architectures there will be a need for the regional network operator to be able to provide a method of differentiating institutes and the services they are accessing for visibility, quality of service and management capabilities.

Technologies such as MPLS, IPv6, QoS and Non-Stop Forwarding should be considered not only for the regional MAN operator equipment, but also at the institute's local gateways to ensure as close an end-to-end methodology as possible, in order to simplify management and troubleshooting processes moving forward and reduce the complexity in bringing services online in the future.

5.4.1 Bandwidth Optimisation

Universities have an ever-increasing need to track subscriber traffic patterns, manage network bandwidth resources, and expand their service differentiation to ensure that critical business applications such as VLE traffic are not negatively impacted by non-critical services such as P2P. To ensure network traffic is handled appropriately, the ability to provide visibility, understanding, and control of network traffic is essential.

The Cisco Service Control Engine (SCE) is a low latency high throughput (scaling from 1Gbps to multi 10Gbps) application performance and prioritization solution providing the necessary level of control for existing and evolving Higher and Further Education environments. The SCE provides a range of bandwidth service enhancements scenarios, while delivering cost management and revenue generation opportunities.

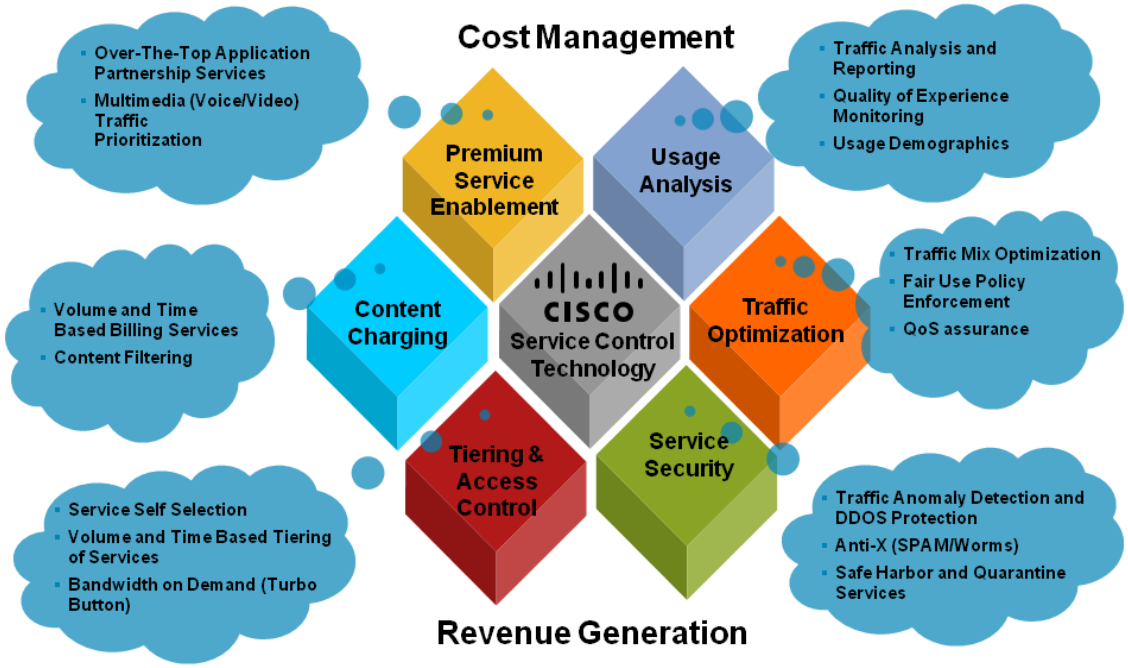


Figure 5.4.1.1 – Service Control Engine Uses

The SCE is a carrier-class service and is designed to fit into the service-provider environment that most educational establishments have become. The SCE technology is able to deliver:

- Application awareness - Stateful deep packet inspection processes packets as individual events with a full reconstruction of flows up through Layer 7.
- Service velocity - Rapidly programmable to support new protocols or applications.
- Real-time control - Application session-level bandwidth shaping, blocking, and redirecting.
- Subscriber intelligence - Subscriber state management with per-subscriber bandwidth management, and quotas.

Through these services the SCE solution is able to provide a range of value-add capabilities for an educational institution.

Traffic analysis – implement monitoring, analysis and reporting on network traffic, providing the ability to determine subscriber and application usage patterns. Implement fair use policies – ensure that applications and users get access to services they need by managing bandwidth-intensive applications through packet flow optimization techniques and the prioritization of real-time applications such as voice and video. This would include volume and time-based limitation.

Implement revenue generation services, including automated processes through a personalised user web portal

- Content filtering;
- Bandwidth on demand, and a bandwidth boost option. Subscribers who may have a standard lower-speed internet service may visit a web page on the provider's site and click on a turbo button to boost their bandwidth for a set period of time or to leave the button engaged until they return and deselect it;

- Allowance or quota based services – an allowance based subscription would allow subscribers to choose volume quota-based or time-based bandwidth for a set period of time, for example on a monthly basis. A "pay as you go" subscription service is ideal for users who use the internet intermittently and only want to buy time or bandwidth as needed;
- Online advertising – place adds directly into internet connections.

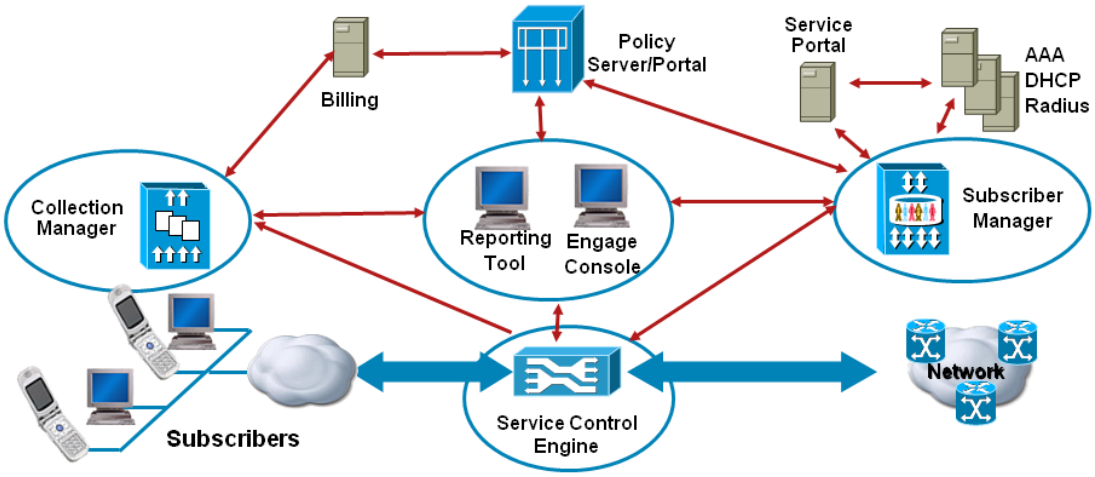


Figure 5.4.1.2 – Service Control Engine Overview

This solution provides state-based protocol monitoring that allows for the detection and control of virtually any network application, including Web browsing, multimedia streaming, and peer-to-peer (P2P). The result is overall reduction of network congestion by optimising application-level traffic, eliminating costly network link usage and infrastructure upgrades. Application and subscriber awareness become the foundation for the deployment of application tiers of service that can be based on content and premium IP service delivery, allowing visibility, control and reporting to optimise education traffic.

6. Logical Architectures for the 21st Century Connected Learning Institution

6.1 Unified Communications

Unified Communications (UC) is the term used for the integration of the rich set of voice, video, collaboration and messaging communications services. These bring together the communications requirements of staff, students, and external parties enabling both service and business transformation by allowing people to change the way they work, teach and learn. The UC solution set ensures that information reaches users on and off campus quickly through the most appropriate medium, no matter where they may be working or what device they may be using. This results in more efficient communications, decision-making, and cost savings through personal productivity improvements.

Cisco Unified Communications uses the pervasive reach of an intelligent network to align communications with business processes. As a result staff and students can:

- Access information easily: Teams can connect in many different ways, whether they're at their desks, in conference rooms, working on remote sites or at home;
- Reach mobile users and key decision-makers quickly: Being able to see which users are available means that users can reach the right resource the first time;
- Communicate spontaneously: Communication applications are integrated with collaboration systems to enable point-and-click data, voice, and video conferencing sessions that use advanced collaboration tools like white boards and application sharing, all from a single, web-based interface;
- Business Continuity: Unified Communications ensures that staff and students can continue to communicate irrespective of the user location challenge that can be brought about by power or building outages or when adverse weather conditions restrict travel to the campus.

UC enables more effective communications: Tools such as instant messaging, presence, mobility, preference, and unified messaging streamline communications and allow users to choose how, when, and where they can be reached. These tools include:

- Video – truly integrated video in the communications environment making video calls as easy to establish as a regular telephone call, improving access to staff and lecturers regardless of location;
- Presence – instant knowledge of a person's availability, reachability, communications preference and even skills, allowing people to be contacted at the right time on the right device;
- Collaboration – the ability to share documents or other information with simultaneous voice, video and instant messaging – ideal in scenarios such as virtual classrooms and scheduled meetings, extending the teaching and learning environment and attracting different demographics of students while offering time, cost and carbon savings;
- Mobility – combine the convenience, flexibility, and reach of mobile communications with the benefits of Cisco Unified Communications, making it possible for people to communicate the way they want, whether at home, at work, or on the road, improving the availability and responsiveness of staff, and allowing flexible teaching and learning environments for students and teachers;
- Messaging – either simple voicemail or unified messaging where e-mail, voicemail and fax can be integrated into a common store. This enables the delivery of any message to teaching or administrative staff on the move at any time and on any communications device. The messages can be retrieved from any device at any time;
- Unified Communications Clients – offers voice, video, instant messaging, conferencing, directory access, and presence information through a single application on a laptop, PC, Mac or mobile handset (this is not an exhaustive list of endpoints);
- Intelligent Endpoints – a range of handsets either wired or wireless provide access to a rich, customisable feature set for end user communication, and the latest technologies to ensure the best audio

communication. Options for Power over Ethernet (PoE) and headset are also available. Analogue devices including handsets, fax and modems are also supported;

- Contact Centre - integrate databases and workflow applications with advanced contact centre capabilities, making it possible to create a virtual call centre or help desk where callers can be matched to the most appropriate agents, delivering an ideal solution for IT helpdesks or clearing. Business statistics in terms of call numbers, average wait times, lost calls etc can be produced to provide visibility on performance in these critical areas;
- XML application services – access and push services to an XML based screen on the IP phone . Services such as registration, room environmentals control, pictures, announcements, advertisement for revenue generation. These applications can be created by the user, or by 3rd parties specialising in the technology;
- Open standards – supporting open protocols to ensure communication standards for call control including SIP, H323 and MGCP, and the integration of 3rd party SIP endpoints, as well as Cisco's native SCCP protocol. All of these protocols are supported simultaneously on the same single platform with no additional hardware or software.

The power of Unified Communications is that services can be offered, for the first time, in a way that is independent of location and independent of communications device. Unified Communications services are ideal therefore, for supporting remote and mobile working for staff and students, and represent an essential technology enabler for the re-design of educational work processes and the delivery of teaching and learning.

A combination of these technologies creates the foundation for collaboration – a key requirement for any learning institution. Please see the Collaboration Services and Business Video section for more information. For further detail on anytime, anywhere access for staff and students, please see the Mobility Technologies section.

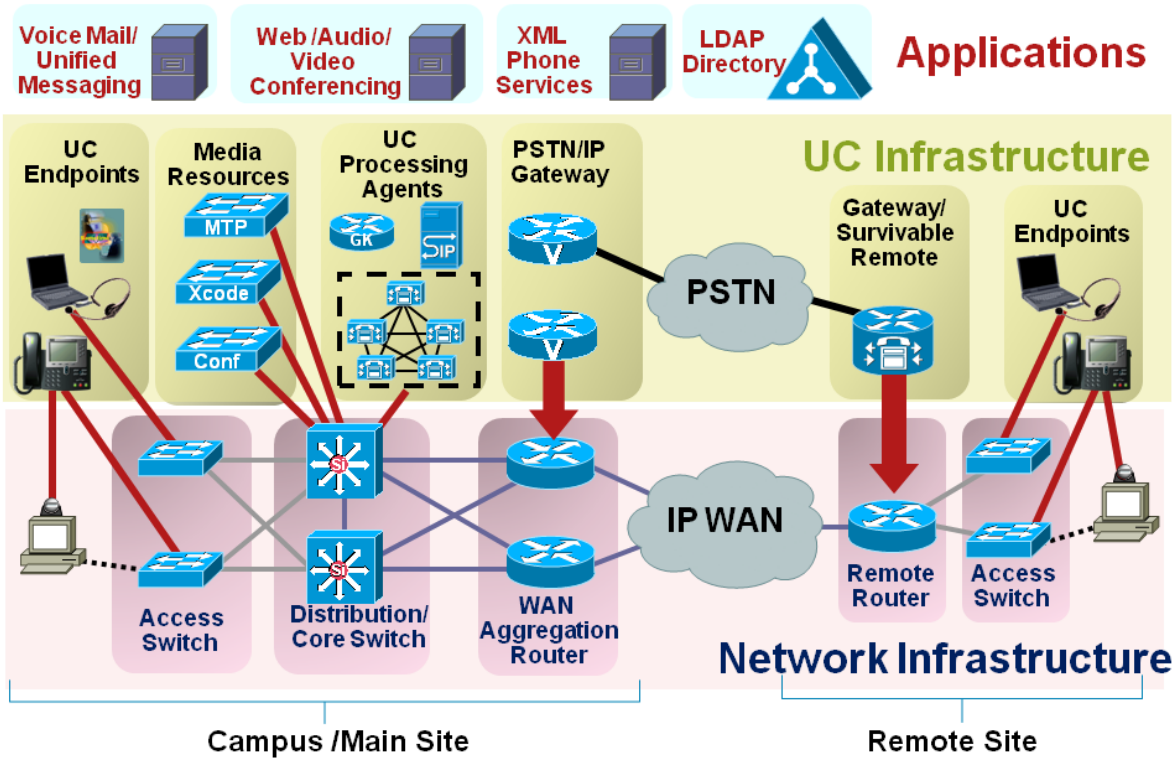


Figure 6.1.1 – Unified Communications Architecture

Foundation Network Architecture
The Unified Communications architecture for the campus environment is shown in figure 6.1.1. When comparing a Unified Communications (UC) environment to traditional telephony solutions, the IP network can be considered to be the switching matrix of the system, without which the UC system would fail to operate. It is therefore a fundamental requirement that the network is designed and constructed with high availability, security, quality of service, management and performance in mind. Design considerations are:

- Overall availability - telephony systems often quote five nines (99.999%) as the expected uptime (not including scheduled downtime or failures of 24 ports or less), data infrastructures can be designed with equal or better up time;
- Network link failures - automatic service restoration within a second is highly desirable ensuring that calls in progress remain active and do not fail;
- Device failure - single device failure being the most common accounted for;
- Power failure - 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 attacks;
- Application prioritisation – Quality of Service 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;
- Multiple paths in case of link or Service Provider Failure;
- Codec tolerance to provide a consistent and predictable experience.

Whilst these requirements are extensive they should be put in perspective, UC is merely another application running over the IP network of which there will be many that an institution relies upon for its continued operation. Most of the considerations listed will be similar for other business critical applications.

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

Advanced Network Architecture As in Service oriented architectures, re-usable intelligent services are essential for a successful UC deployment. In this section we examine some of the more advanced requirements needed within a campus network design. Please visit the following link for the complete Cisco Solutions guidelines: http://www.cisco.com/en/US/netsol/ns818/networking_solutions_program_home.html

Quality of Service (QoS) - All application traffic has different characteristics and demands of the network and this is essential when looking at real-time traffic such as voice or video. In practice, networks are designed to have several different types of traffic with different attributes tailored to the different application demands. Creating a comprehensive Quality of Service model is essential for the real-time characteristics of a UC network to ensure that business critical traffic such as voice and the VLE can be prioritized over non-critical traffic such as peer-to-peer. The full Quality of Service design guide can be found at the following link: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

Call Admission Control (CAC) – is used to ensure that the priority traffic queue 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 priority queue has the required capacity. If not then the call may be refused or maybe re-routed. This type of control is essential to protect the real-time critical voice traffic and to provide a consistent experience to the user, this capability is not offered by all vendors.

Translation Services - During call setup, end-points often negotiate what speed, compression and coding type (codec) will be used during the call. There are occasions when the end-points are unable to identify a common set, in which case the call would fail. 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 codecs (G.711, G729, G722 Wideband, iLBC etc) and similar, principles exist for speed, protocols and other attributes. Additional information on transcoding services can be found at the following link: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/media.html#wp1046264

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

Call Control via the Unified Communications Platform

An IP based Unified Communications 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 6.1.2 below.

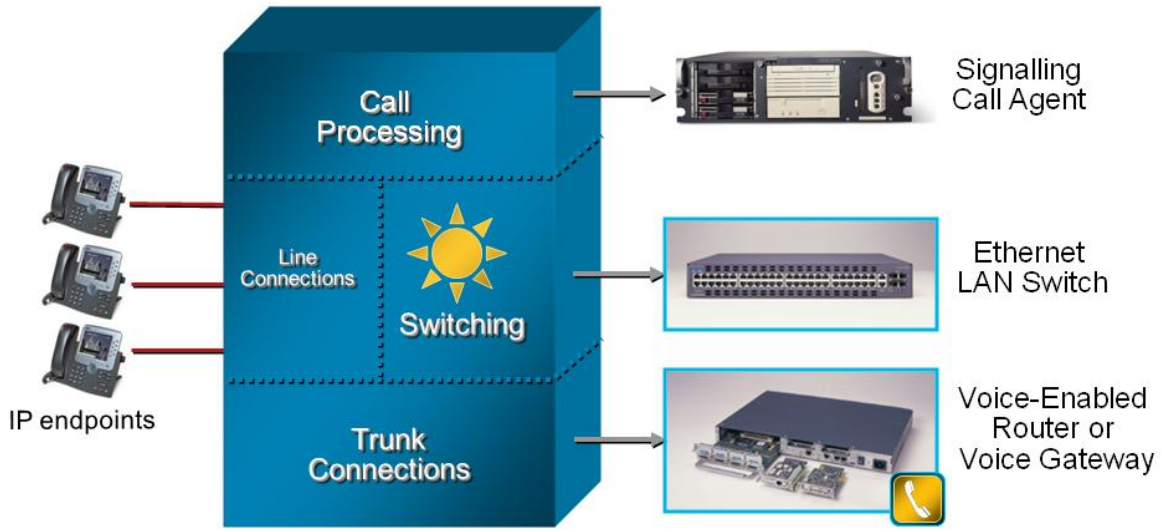


Figure 6.1.2 – Traditional versus IP Telephony

The intelligent 'brain' that provides dial tone and manages call processing and signalling exchange has become a server based software application (Cisco Unified Communications Manager). Multiple servers can be 'clustered' creating a single, highly available virtual service which delivers call control services across all IP connected sites of an educational establishment, including remote sites and remote workers. Intelligent clustering means that servers can be deployed across multiple physical locations reducing the effect of any equipment or site related failure,

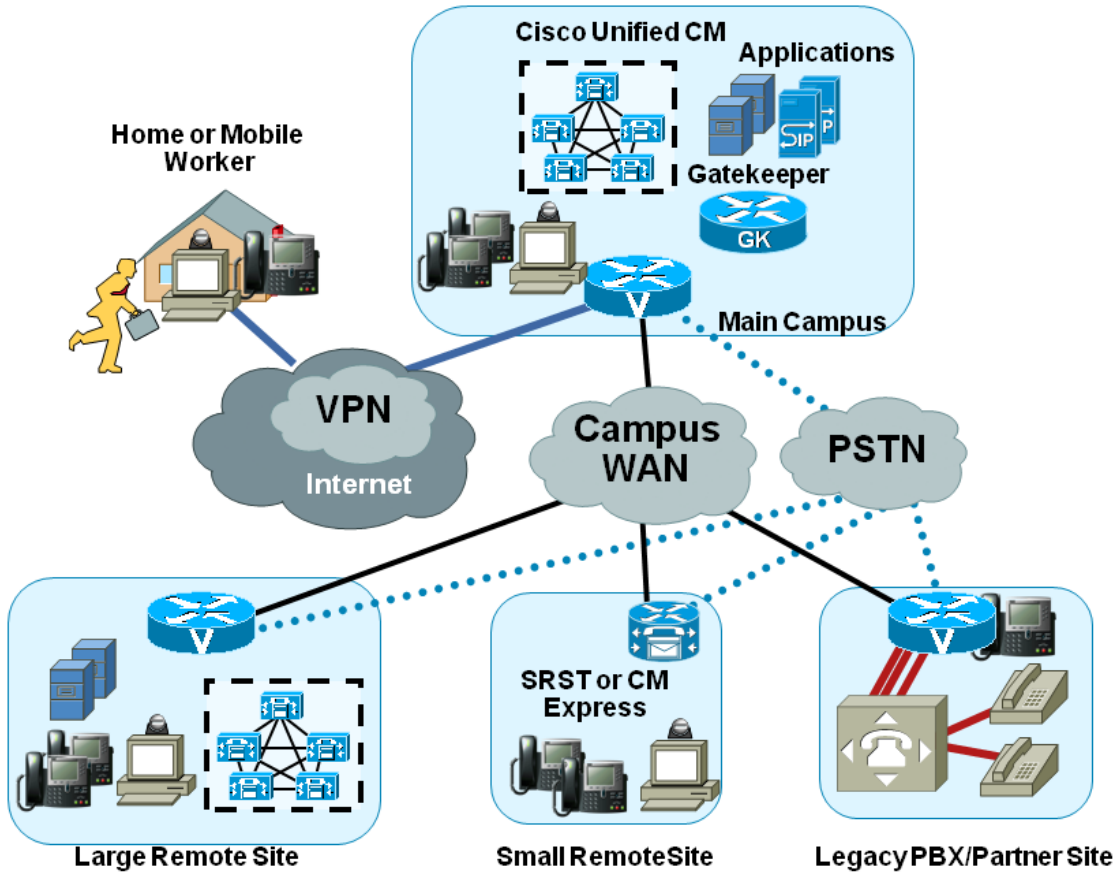


Figure 6.1.3 – Extended Unified Communications Architecture

The extended Unified Communications Architecture, illustrated in Figure 6.1.3 above, shows the extended deployment model for these technologies. Unified Communications Manager servers are deployed in resilient configurations at two main campuses, but are configured to form a single cluster delivering highly available, highly scalable and consistent voice and video services to connected users irrespective of location. This deployment model supports the integration of many other communications technologies. This is designed to maximise flexibility, provide integration with legacy solutions, provide resiliency to smaller sites that do not require a Cisco Unified Communications Manager, and provide investment protection.

High-availability voice services must be maintained at remote locations where there are no Communications Managers and, to do this, it is recommended that Survivable Remote Site Telephony (SRST) be configured into each remote-site router. SRST capability permits the remote-site router to take over call processing in the event of the unavailability of the centralised Communications Managers due to IP WAN failure. IP phone users are able to call one another in the normal way, while PSTN access can be provided through interfaces on the remote-site router. This provides additional reliability for staff and students in remote locations. Interconnections such as trunk connections to the PSTN (Public Switched Telephone Network), 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 ISDN (Integrated Services Digital Network).

Finally the endpoints or terminals can take different formats. Some will be familiar in form to a traditional handset. Others could be software applications such as a softphone on a PC or integrated into a mobile phone. Wireless handsets are also available to support mobility and instant reachability. Typically a range of hardware and software IP voice end-points can be deployed across the network to support differing user needs. As an example a member of the administration staff may only need to make internal and external calls from a fixed desk

environment and would use an IP handset, whereas a lecturer may need to make calls from any room they lecture from and may use a softphone on their laptop. These end-points may be wired or wireless. Video terminals and desktop video cameras can also be deployed to those users with a need for face-to-face communications.

Once the base Unified Communications architecture has been deployed to deliver voice and video telephony, there is the opportunity to layer value-added applications upon that base. Value-added applications are typically server-based and target real business requirements such as increasing levels of user efficiency or reducing cost of ownership, as well as providing flexibility and sustainability goals. Value-added applications are available within the architecture to deliver the following features and benefits:

Voicemail and Unified Messaging Services – permit messages to be left for staff and retrieved either by phone or via e-mail, ncreasing the accessibility of staff and enhancing staff communications.

Instant Messaging Services – permit efficient, easy-to-use messaging services between members of staff and can be extended to students. Increase accessibility of staff and provide an essential tool for making short, ad hoc queries of colleagues, as well as allowing staff to manage their time using presence functionality.

Web Conferencing Services – permit audio, video or web conferences to be established, enhancing staff to staff, teacher/student, and team communication. Permit documents to be shared over the network either for team review or for update. These technologies allow the extension of the classroom so that teaching can be delivered to remote locations, and lessons recorded for future playback or revision. This allows reach to a different demographic of student which is geographically independent, and also time independent.

Virtual Contact Centres – permit staff based at multiple locations to participate in a virtual contact centre with full queuing, skills-based routing, email queuing call reporting statistics and CRM interfaces. This type of functionality allows better management of pools of resources such as IT help desk, clearing, or marketing activities, and with the integration into existing windows-based applications, additional relevant information can be screen-popped to add value to the call. This provides better visibility of processes such as clearing where number of callers, missed calls, average call length time etc can be reviewed.

Single Number Reach (SNR) Services – permits each member of staff to use a single number, for all communications, rather than giving out multiple numbers for mobile, landline, etc. The SNR server directs calls to the single number to specified office, mobile or PSTN numbers to increase the reachability of staff. This Increases the accessibility of staff and eradicates the inefficiencies of multiple messaging servers. Also allows the staff member to manage their own devices to be contacted in a way that is suitable for them.

Mobility Services – permit the use of dual mode end points, such as Nokia and iPhone mobile devices that support GSM and 802.11 wireless connectivity on the local IP infrastructure. This permits mobile phones to make calls over wireless when located in the office, avoiding the cost of unnecessary GSM calls. When outside the coverage of the wireless network the mobile handset acts as a standard GSM device.

Third Party Device Integration – as well as providing open communications signalling via SIP, the Unified Communications Manager allows the full integration of third party clients such as Microsoft Office Communicator through CUCIMOC, or IBM Sametime. This provides additional flexibility and choice for end users. With the addition of a Gateway even Skype calls can be integrated into the solution to provide student communication to staff. With application integration there is the ability to dial from Microsoft applications such as Word using Click to Dial, as well as calendaring information and voicemail direct to the email inbox using Outlook.

Presence - enabling 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 also 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.

Confederation between presence aware systems allows users to broaden their view outside of a single system. Presence systems exchange availability information, ideally using standard protocols allowing a user in one educational establishment to see the availability of others in another establishment or partner organisation. The users are able to communicate using IM chat and then escalate into a voice, video and collaboration session seamlessly. The support of such standards can help support inter-working, collaboration and research between institutions.

Messaging - There are many different ways to communicate using messaging systems across education including email, voicemail, fax and SMS but to a large degree these systems exist in silos resulting in the user interrogating each one individually. Often however, messages remain unread due the user being unaware of a new message or its importance.

Unified Messaging (UM) combines all of the messaging silos enabling the user to access all of their messages from a phone, a mobile device or through an email client. True UM involves all messages being stored in a single user mailbox on a single messaging system. This is a server based model meaning that the user can set up rules or policies to automatically handle messages and take defined actions based on chosen criteria. The user receives the messages in the same format regardless of their current device, desktop or mobile. 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.

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.

With the increased mobility of staff in the campus, between campus' or in different institutions, flexible messaging services ensure important messages can be left and retrieved irrespective of location or device. This also allows students to leave messages with staff.

More information on Cisco value-added Unified Communications services can be found at:
http://www.cisco.com/en/US/products/ps6789/Products_Sub_Category_Home.html

and on Contact Centre services at:
http://www.cisco.com/en/US/products/sw/custcosw/Products_Sub_Category_Home.html

6.2 Collaboration Services and Business Video

Collaboration and business video are extensions to Unified Communications and key technology tools for Connected Learning.

Collaboration services comprise web, video and audio conferencing applications that allow anyone to collaborate in a variety of ways – to share a series of slides around a classroom; to collaborate within a research group on data prior to publication; to embed video within a distance-learning environment to enrich the experience.

Business video comprises a hierarchy of tools; at the lower end the ability to add webcam video to conventional audio calls; through to meeting room systems that allow one-to-one or many-to-many video calls; up to immersive room-based systems, such as Cisco TelePresence, that permit a point to point, or multipoint

conferences to be established that offer an experience near equal to a face-to-face meeting. These solutions sets are overviewed in the following sections.

6.2.1 Collaboration Services

Historically, to reach distance learners, educational institutions have used alternative methods such as correspondence, online delivery, and TV to close the distance from the campus hub and other resources. Hybrid learning has also become popular for many institutions where students spend part of the time on campus and part of the time using distance education tools.

The impact of collaboration and mobility services and technologies on distance learning is particularly profound. Traditionally, a "distance learner" is defined as a student who is not connected to a campus classroom and is not physically present with a faculty member. Collaboration services and technologies, such as Cisco WebEx enable this person to have full access to the campus materials and staff even though he or she may not be on campus at all.

6.2.2 Real-Time Business Video

Video has become popular in college settings in a variety of ways: as a means to broadcast lectures and record classroom sessions, as a medium to complete assigned projects, for vlogs, and for instructional purposes. Consumer devices, such as Flip camera and mobile phones have made producing a video very simple almost free. Thus students, in addition to being consumers of content, have become producers as well. As a result, it is becoming the norm for class assignments and presentations to include a video component or to be rendered completely as video.

One of the more popular trends in education is podcasting, which can incorporate audio, video, and other content that is distributed to any appropriate device. Using iTunes U, many educational institutions have adopted this framework to deliver course content.

Here are some other examples of video's use in Higher and Further education:

- Medical schools connect students to real-time surgeries; streaming underwater marine life to classrooms; and connect students with other students using video.
- Video on demand (VoD) enables students to download videos for later viewing, such as a recorded class or lecture for personal or group study and discussion.
- Videoconferencing and TelePresence enables students to engage with other classes, guest speakers, and researchers in a two-way format, enabling real-time collaboration and discussions.

Video end points can very simply be integrated into the Unified Communications call control platform to enable both audio and video services to seamlessly coexist – all devices share a common dial-plan or numbering scheme. Integrating video with voice in this way provides a single system supporting all communications needs with the following benefits:

- Single, uniform dial plan;
- Centralised management;
- Single point of billing records and administration;
- Calls between ANY communications device;
- High level of telephony capabilities across all endpoints;
- Integrated scheduling of resources;
- UC application support such as voicemail or contact centre across all devices;
- Presence based information for all devices;
- Global CAC mechanism based on real network performance;
- Standards based protocol support of endpoints.

More information on Cisco's Business Video solutions can be found here:
http://www.cisco.com/go/video

6.2.3 Cisco TelePresence

Cisco TelePresence is an advanced technology that enables face-to-face interaction among individuals seated at tables in rooms that may be half a world apart. A key benefit of TelePresence is its ability to bring people together in real time without technology difficulties, eliminating the need to travel to an event or classroom. TelePresence features 1080P high definition video screens, CD quality spatial sound, and meeting rooms designed for optimum acoustics and to create a 'real-life' feel to meetings. The Cisco TelePresence solution ranges from large multipoint room-based systems to personal TelePresence solutions and provides integration with traditional video conferencing end points.

TelePresence has many uses in higher education:

- Collaborative research - Using TelePresence, researchers can easily maintain frequent contact during research cycles, which often involve multiple, globally dispersed teams;
- Administration and cabinet meetings - TelePresence enables regular meetings and eliminates travel costs when members are located at a number of campuses;
- Dissertation defence - Ph.D. completion requires a rigorous defence in front of a panel of experts who are often flown in for the event. TelePresence can reduce travel costs and enable more timely examination;
- Interviews - TelePresence enables universities to recruit faculty from institutions around the world reducing the often requisite multiple interviews at the university;
- Professor's office hours - TelePresence enables office hours with students who may not be on campus or may be on another campus or near a TelePresence centre;
- Student collaborations- Using TelePresence students can collaborate on projects and even work in globally dispersed teams;
- Distance learning - TelePresence enables small, focused classes where key students might be taking the course from a variety of locations;
- One-on-one classes - TelePresence enables students to take advantage of private music and language lessons even when the professor cannot be in the same room;
- Cross-campus meetings - Many universities have a number of campuses. TelePresence eliminates the need for faculty to travel to weekly or monthly meetings.

More information on Cisco TelePresence can be found at:
http://www.cisco.com/en/US/netsol/ns669/networking_solutions_solution_segment_home.html

6.3 Mobility Technologies

User mobility is an ever-increasing requirement within education, not just enabling staff to be productive whilst away from a desk or to work in flexible remote locations such as the home, but increasingly for student inclusion and participation. Mobility provides access to the same applications in use in the office, both voice and data, from anywhere. The user experience should be as rich as possible at all times and as consistent as possible across any device or workspace, regardless of location. It is the end user experience that is the key to mobility adoption within education, and users want the Unified Communications, collaboration, video and wireless solutions to be aware of their changing environment and allow them to communicate seamlessly wherever they are and on a device that suits them. Staff and students can remain connected and productive, whether they're at home and using College or University owned or their own PCs, using public internet terminals, or using internet-enabled mobile phones. See Figure 6.3.1 below for the most common mobility scenarios.

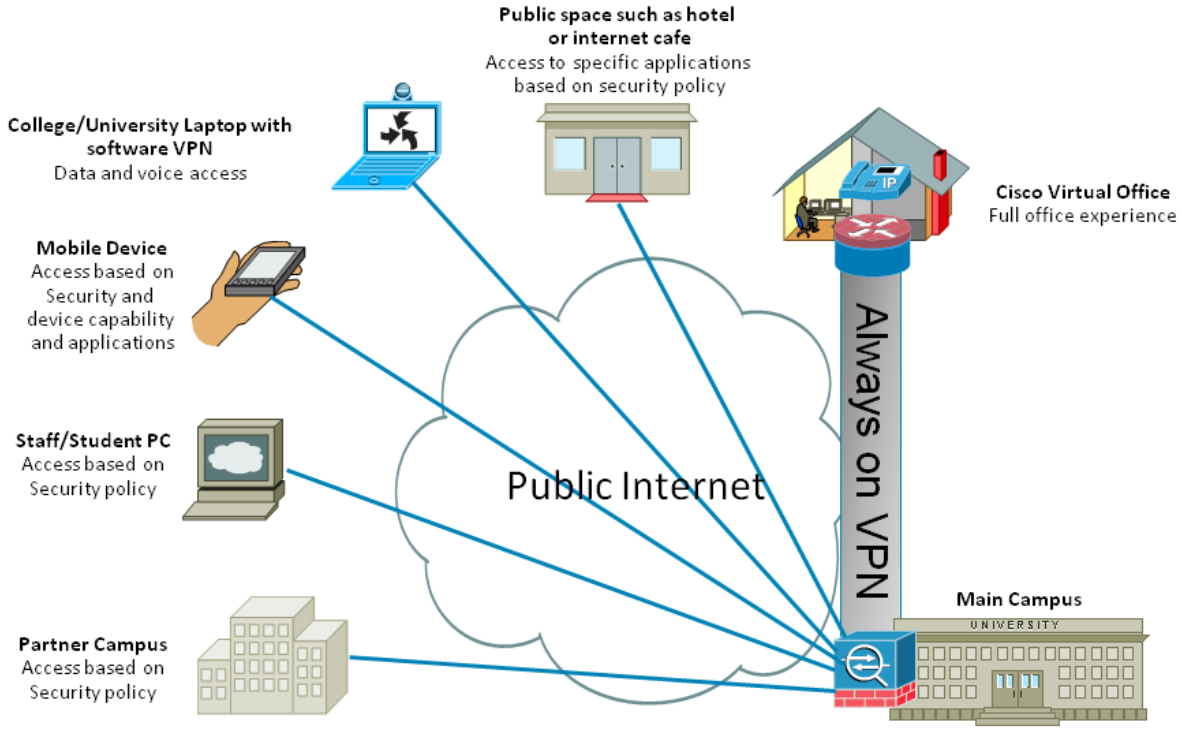


Figure 6.3.1 – Common Mobility Scenarios

Historically mobility technologies have not been widely deployed due to cost, security or limiting technologies. With the relatively low cost and widespread adoption of the internet into the home, hotels, and onto mobile devices, as well as pervasive wireless coverage on campus, these challenges are no longer enough to prevent adoption. In fact security has now become an enabler to ensure mobility technologies can be used in a secure manner. The attraction of staff and students has also contributed greatly to the use of mobility technologies, allowing access into the teaching and learning environments irrespective of geography or time zone. Often, existing infrastructure can be built upon to deliver the capabilities to enable secure and reliable access.

The terms remote and mobile (as well as flexible, home, agile and others) to describe working methods are used in a number of different ways to describe the use of technology, and how it supports work patterns away from the typical office base or location. Cisco suggests the use of these terms in the following manner:

6.3.1 Remote Learning and Working

Remote Learning and Working refers to working from home, from a different campus or while travelling. The term includes teleworking, where a member of staff is formally based at a home office on a part or full time basis. Some examples of this could be a lecturer working at another institution but requiring access to the network, or a student attending a lecture from a home or remote location. This would include a student connecting securely back to the College/University via their pc or handheld device via GSM, broadband or wireless hot spot. This would be typically for accessing course information , uploading material or collaborating with peers. Cisco's WAAS mobile can considerably speed up data transfer whilst enhancing voice services from remote locations.

More information on WAAS mobile can be found at the following link:
http://www.cisco.com/en/US/products/ps9523/index.html

An example for this requirement may where a student studying textiles has an assignment where they need to provide use examples for certain materials. A visit to a shopping centre during the weekend or

during holiday may provide an ideal opportunity to capture images (still or moving), on a camera, Flip or PDA. They can then either transfer the images securely using a VPN via GSM (directly or via pc) or wireless hot spot. After doing this they may create and participate in a Webex collaboration meeting to discuss their findings with peers or lecturer from their pc or iPhone.

6.3.2 Cisco Virtual Office

Cisco Virtual Office introduces a secure end-to-end solution for bringing enterprise quality services—voice, video, wireless, and data—into the home office or remote campus environment. It is designed to provide time and location agnostic service availability for employees' home offices.

The Cisco Virtual Office solution (see Figure 6.3.2.1) is designed to provide full office replica and near office user experience for day extenders, part-time teleworkers, home based students, and full-time teleworkers in their home offices. It provides Wireless services for both employees and household members with fully separate internet access. Integrated security features, including firewall and intrusion prevention, significantly reduce the risk of security breaches, the abuse of network privileges, and the spread of malware. Identity-based networking services provide strong authentication of users and devices to prevent unauthorized use. VoIP services are possible with Cisco Unified IP Phones and QoS capabilities available. The same Unified Communications user experience and services available at the office such as call routing, forwarding, conferencing, one-touch dialling, and voicemail, can be available to the remote worker. The Cisco Virtual Office is provided on one piece of equipment ensuring ease of deployment.

Use of WAAS mobile (as discussed in 6.3.1) in conjunction with CVO can improve application responsiveness.

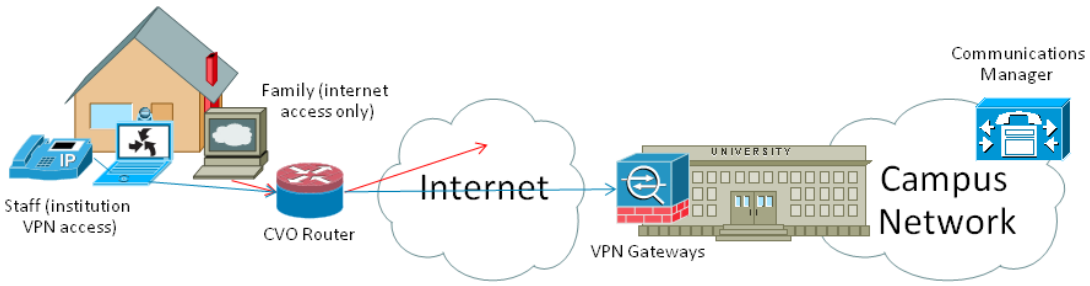


Figure 6.3.2.1 – Cisco Virtual Office

6.3.3 Mobile Learning & Working

With pervasive wireless coverage (see section 6.4 Wireless LAN) the learning environment has expanded so that devices such as laptops and mobile phones become the workspace in which to work, teach and learn.

This has meant that the physical work, teaching or learning location has changed with options of the fixed lecture theatre or room, and now more commonly open learning areas where students can collaborate, to learning on the move, emphasising flexible work places and spaces. Using a secure wireless network students can access lectures, content and even "learning pills" as they move around campus, providing a flexible user-centric experience for learning. With collaboration tools such as Webex and MeetingPlace, meetings can be held and lectures can be delivered without the requirement of a physical room. With this approach we are starting to see increased use of video from any endpoint or physical location on campus to enhance and personalise the experience, content being utomatically pushed to students as they enter certain areas or zones, and more virtual meetings.

From a staff perspective, technologies such as extension mobility on the Unified Communications platform and wireless coverage mean that working can take place irrespective of location. So a similar experience can be achieved in a fixed office, hot-desking, or working in communal areas around campus. Again with increasing features available on mobile devices such as mobile handsets or PDAs, the workspace can be anywhere in the campus environment.

The key here is that the physical learning space is becoming less important, with the focus on the user experience and workspace, and personalization.

6.4 Smart Connected Buildings

Technology touches most aspects of the way people work, learn and teach. However, today's building environments have not evolved to support these changing requirements. In addition, key trends are driving the need for building transformation such as globalisation of the workforce and the drive for environmental and social responsibility. As user requirements evolve, buildings must adapt and change to transform the physical spaces through technology innovation, delivering value-added, revenue generating services while streamlining the processes that create buildings and developments.

Until recently, each building subsystem from access control to heating and ventilation required a separate network, resulting in a complex, costly environment that was difficult to operate and maintain. But today it is possible to efficiently deliver all building services over a single, converged, centrally managed IP-based network. This same network forms the backbone of a 21st-century connected learning institution.

Through foundation, convergence and transformation (See Figure 6.4.1) this approach allows owners and operators to:

- Deliver new services: Generate new revenue opportunities with fee-based or complimentary services to attract and retain tenants and stakeholders and differentiate the property over competition;
- Integrate Communication systems: Deploy IP telephony, video conferencing, rich media, collaboration, and productivity tools over the IP network;
- Integrate Physical security: Deliver converged security applications, including Video Surveillance, access control, visitor management, and fire safety, over the IP infrastructure;
- Integrate Building technologies: Monitor and administer HVAC, lighting, transportation, and energy management, wherever appropriate, over the IP network;
- Provide: A "Building Information Network": Use the IP network foundation for all communications systems, building systems, and personal devices to facilitate greater operational efficiencies and reduce operational expenses·

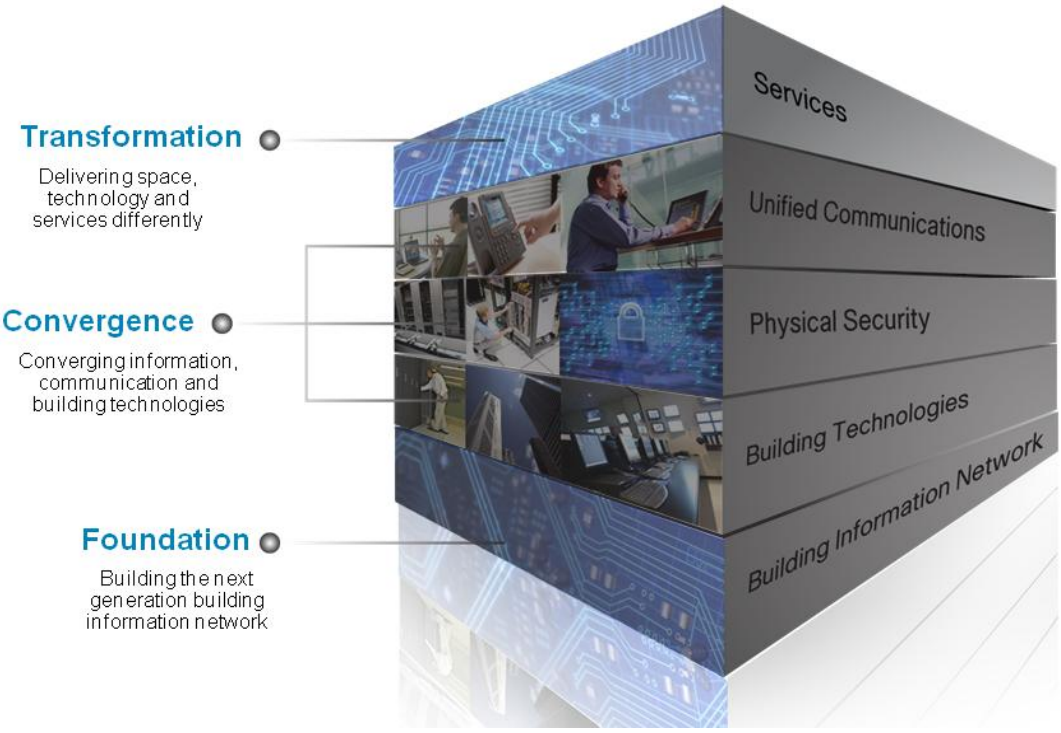


Figure 6.4.1 – Smart Connected Buildings Architecture

One of the main focus areas in the current climate is providing visibility and optimisation of power consumption throughout a building. The Cisco EnergyWise architecture was developed in response to energy costs, environmental concerns, government directives and the increased need for sustainable and "green" business IT operations. Methods to measure power consumption and control energy output are now the focus of businesses worldwide with all customers looking for a method to reduce energy costs and implement increased efficient operation.

Cisco EnergyWise is a new energy management architecture that will allow IT operations to measure and fine tune power usage to realise significant cost savings. EnergyWise focuses on devices connected to a Cisco network ranging from power over Ethernet devices such as IP phones and wireless access points to IP enabled building and lighting controllers. It uses an intelligent network based approach allowing IT and building facilities operations to understand, optimise and control power, and underpins the intelligent or smart building approach, converging building and network technologies under one common management and reporting system (Figure 6.4.2). The network based EnergyWise components are mainly software and can run on many existing Cisco platforms.

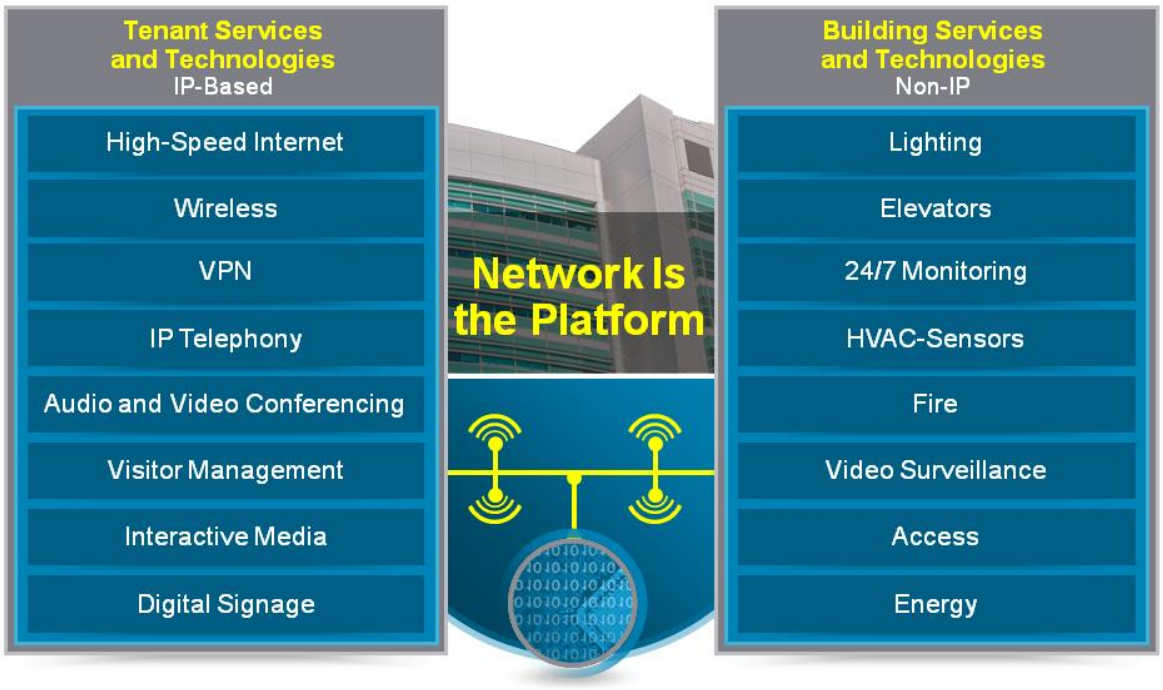


Figure 6.4.2 – Converging IT and Facility Technologies

Traditional IT Business Energy Management

Today many customers are focused on reducing costs related to the power consumed by IT devices across the campus. Normally this involves the comparison of device efficiency, power consumption and the total number of devices needed but no other metrics. However, enterprise professionals lack a holistic means to measure the day to day power consumed by all network attached devices. This problem is compounded as responsibility for building systems is provided by the estates or facilities team who manage heating, cooling, and lighting resources. Many customers realise the cost of maintaining separate networks for the control of heating, cooling and lighting is expensive and because of this building control devices are converging to IP and utilizing the Cisco network. Most customers would benefit from realistic information about the amount of power consumed by IT related devices including switches, routers, IP phones, PC's, surveillance cameras and wireless access points. EnergyWise provides the IT professional with a new method to understand power usage and justify energy costs.

EnergyWise Business Energy Management EnergyWise is a power management architecture designed to measure power consumption and optimise power usage resulting in effective delivery of power across the campus. IT professionals can quickly optimise the power consumed in a building and the result immediate cost saving with a clear return on investment.

EnergyWise measures current power consumption, can automate and take actions to optimise power levels; and advise how much power is being consumed to demonstrate cost saving. After power consumption is understood, regulation using EnergyWise network protocols provides command and control of power usage. Energy consumed per location can easily be found with a realistic view of power consumed per wiring closet, building floor or campus building. Please refer to Figure 6.4.3.

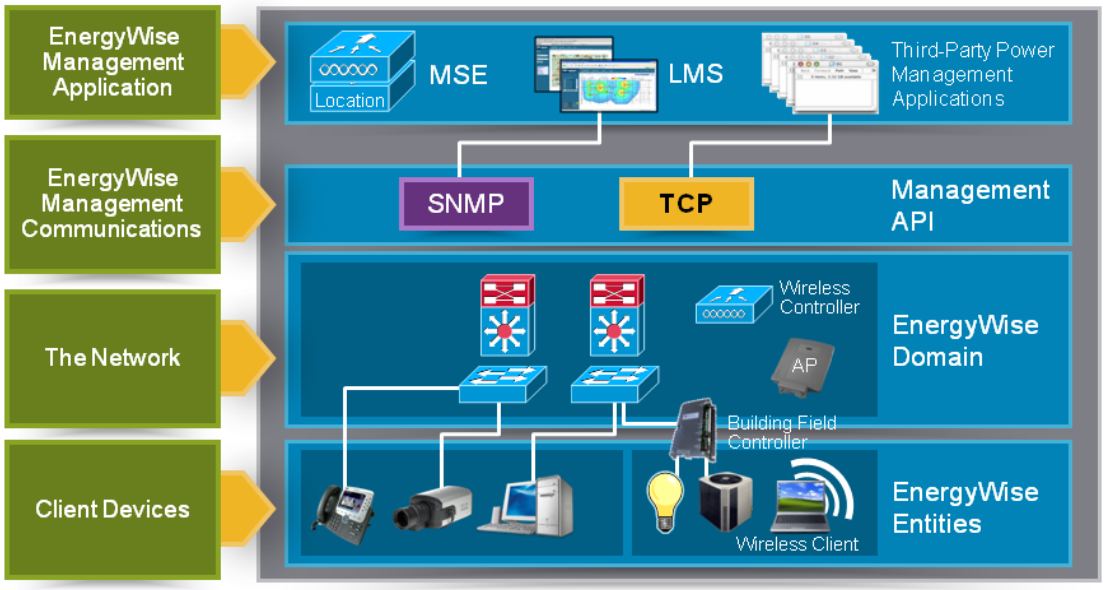


Figure 6.4.3 – EnergyWise Network Overview

More information on EnergyWise can be found at: http://www.cisco.com/go/energywise

As part of the EnergyWise solution Cisco are partnering with specialist companies in the building management, network management and laptop/pc technology areas to ensure the most appropriate solutions for end customers. There will also be an ecosystem partner framework for any organisation wishing to participate. In addition the Cisco Network Building Mediator will link the IP network to proprietary building management systems (See Figure 6.4.4) so that customers can connect legacy or new building technologies into one common solution irrespective of BMS Vendor. As part of Cisco's open API's strategy, some BMS vendors are providing a native interface into Cisco Energywise today, obviating the requirement for Cisco Network Building Mediator.

A series of White Papers relating to Cisco EnergyWise can be found at:
http://www.cisco.com/en/US/products/ps10195/prod_white_papers_list.html

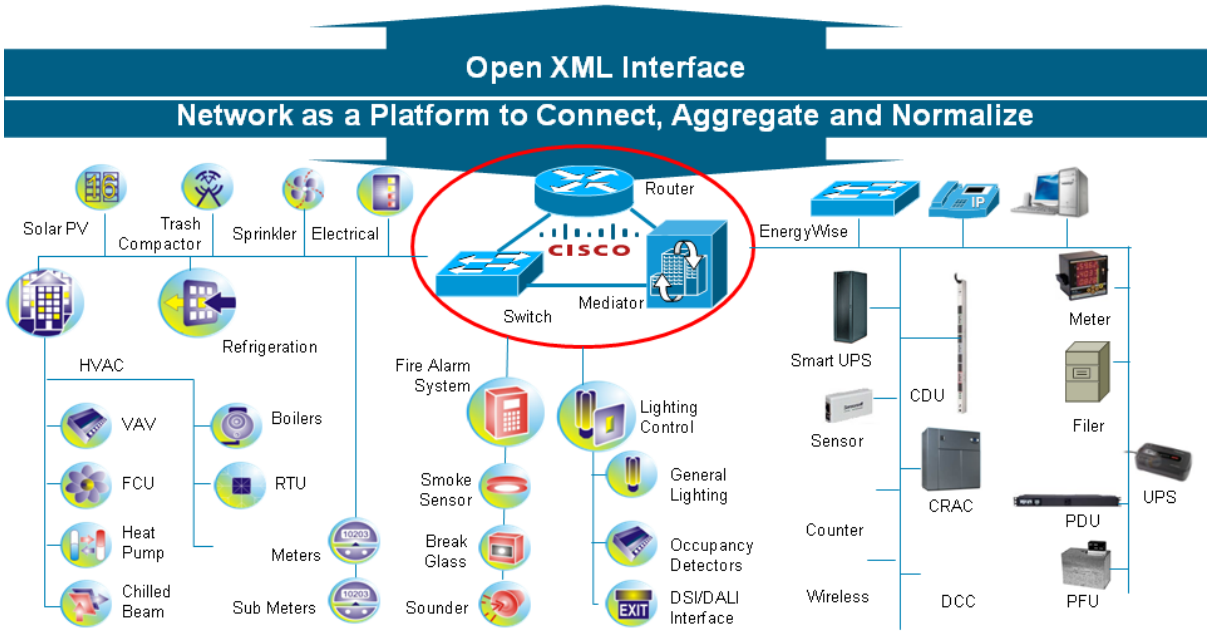


Figure 6.4.4 – Network Building Mediator Architecture

Combining the ecosystem partnership approach with the product technology groups, and middleware providers the Converged Buildings System can be realised, providing a lifecycle approach to sustainability and energy consumption within a building.

In addition, the Cisco solutions in this Technical Blueprint will contribute directly to the reduction in energy usage of an educational environment. Unified Communications, Collaboration and Mobility technologies will allow staff members to optimise and reduce their levels of travel. Smart Connected Building technologies will optimise the management of buildings to reduce energy usage to a minimum. Data centre virtualisation technologies will permit data centres and server rooms to be designed and built to minimise energy usage.

More information on Cisco and how it is using ICT to transform energy usage can be found at:
Cisco and the Environment

6.4.1 IP Video Surveillance and Physical Security

Traditionally Closed Circuit Television systems have utilised a centralised switch architecture, with dedicated fibre or copper interfaces directly from cameras to the switch and from switch to recording systems such as VCR, or Digital Video Recorders (DVR). This resulted in challenges in several areas:

- Resilience
- Collaboration
- Scalability
- Cost-efficiencies
- Single-vendor lock-in

With the network now becoming the platform for service delivery, making use of capabilities such as Quality of Service and network virtualisation, IP is becoming the standard transport medium for delivering services such as voice and video – and now IP based IP Video Surveillance

Cisco Video Surveillance Manager (VSM) removes the need for a dedicated cabling infrastructure and monolithic architectures by delivering a high-performance, scalable platform for video capture, recording, management and integration. Please refer to Figure 6.4.1.1

By using Cisco Appliances based upon commercial off the shelf (COTS) components, and delivering the VSM software, Security teams are now able to use the power of the IP network infrastructure to provide access to security feeds from anywhere in the world, while simultaneously reducing the need for a separate cabling infrastructure by using the existing IP network infrastructure as a transport layer.

Through a server-based approach, the VSM solution can scale from a single server – providing support for up to 100 cameras, up to 18 terabytes of storage and up to 100 users to either administer the system or view content.

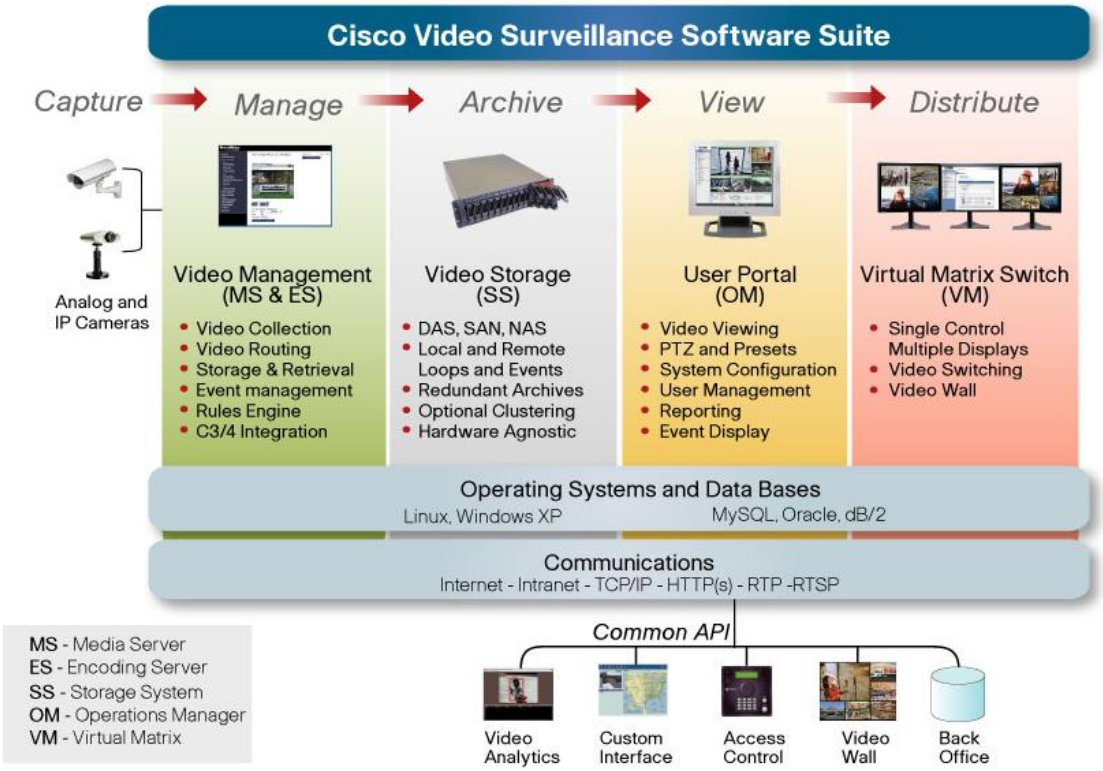


Figure 6.4.1.1 – Cisco Video Surveillance Manager

A multiple server solution can scale to a virtually unlimited quantity of cameras, storage and users, with a "single pane of glass" to manage and administer the system.

- Provides real-time remote monitoring w/virtual matrix switching (VSVM)
- Display live and archived video streams with high quality images.
- PTZ control and presets
- Review and clip archives

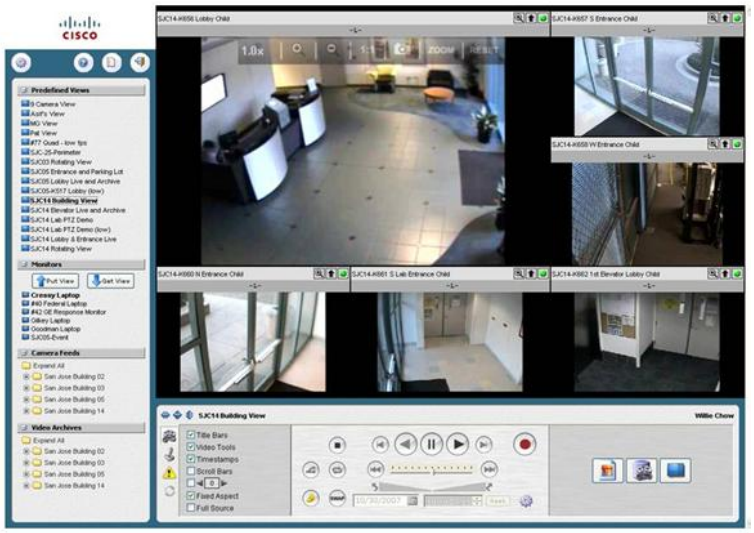


Figure 6.4.1.2 – Cisco Video Surveillance Operations Manager

Given regulatory and compliance requirements media needs to be kept for several months, which traditionally would have taken numerous VCR cassettes, or multiple DVR platforms – neither of which provide a manageable or an easily scalable solution. The VSM architecture enables administrators to take advantage of 3 different approaches for storage of content:

- Direct-Attached Storage of the Media Server itself
- iSCSI connectivity to storage arrays
- Fibre-Channel connectivity direct into Fibre-channel SAN fabrics

By taking advantage of the SAN attached capability, Data centre efficiencies can also be increased, through use of otherwise un-utilised storage capacity.

Through the VSM API integration with numerous EcoSystem partners can be achieved for functionality ranging from Number-plate recognition, through to video analytics, or integration to Cisco's Electronic Access Control Solution (EAC).

Also, the power of the VSM API enables integration with a wide array of IP Video Surveillance cameras – ranging from traditional analogue CCTV cameras through to 3rd party Encoders or Cisco Encoders, or by taking advantage of the nature of the API enabling interaction with numerous 3rd party IP-based Video Surveillance cameras today, enabling protection of existing investments.

Cisco also has multiple offerings within the IP-Video Surveillance endpoint field, delivering Standard and high-definition IP Video Surveillance cameras.

The Cisco 2500 Series cameras offer Standard definition capabilities, with both wired connectivity – using standard based Power over Ethernet, or an independent power supply – as well as wireless connectivity using 802.11b/g /n connectivity to remove the need to cable in hard to reach places, as well as providing an additional level of flexibility for positioning of video capture, whilst making use of network based technologies such as 802.1x to secure connectivity to the network:

Figure 6.4.1.3 – Cisco IP Video Surveillance Cameras

The Cisco 4000 series cameras offer true high-definition at 30 frames per second 1080P resolution, with motion detection, event notification, day/night operation and using standards-based Power over Ethernet or independent power supplies:

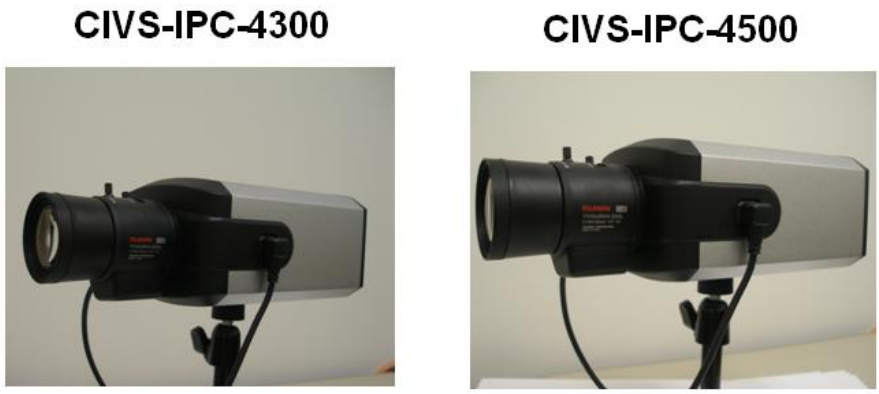


Figure 6.4.1.4 – Cisco HD IP Video Surveillance Cameras

One of the many virtues of the VSM software is the ability to provide an improved collaboration experience, by using a component of the VSM solution known as the Virtual Matrix Client video feeds can be streamed directly to C3 (Command and Control Centres) for incident management, or to provide resilience in the event of an issue at the primary location. Again, through the use of the ubiquitous IP network, access can be provided to users anywhere in the world to the video streams in a secure manner.

6.4.2 Digital Signage

The demand to create, manage and display rich, compelling digital media information within the College or University campus continues to grow. Video content enables new innovative methods to facilitate learning and getting messages across to staff and students in new and visually appealing ways. With the advent of YouTube and other video websites there has come an expectation in the minds of many students and staff that this type of facility should be available on campus. As such, never has the need for managing, accessing and displaying this content been greater.

In many educational establishments there are often a number of siloed solutions around a campus to meet the demand for creating, managing and converting this content. For example there are various solutions for transcoding content from one format to another, other solutions to edit the content, and solutions for displaying the content and management of the workflow from taking a video from a native "raw" state to formatting and delivering that video onto a multitude of different types of device. At the same time there is a need to maximize the investment of installed solutions and ensure they integrate seamlessly with other digital media formats such as IPTV/commercial TV, directional signage, emergency campus alerts, timetable planning and so on. In a distributed campus, or in situations where there are remote learners, there is also a requirement to deliver digital media off-campus, typically to some form of student or staff owned computer. It is important therefore that a video media system interoperates with these various elements and provides a platform for all types of digital media.

See Figure 6.4.2.1 below for an overview of Cisco's Digital Media Suite, a single cohesive system that brings a large number of digital media communications under a unified management entity.

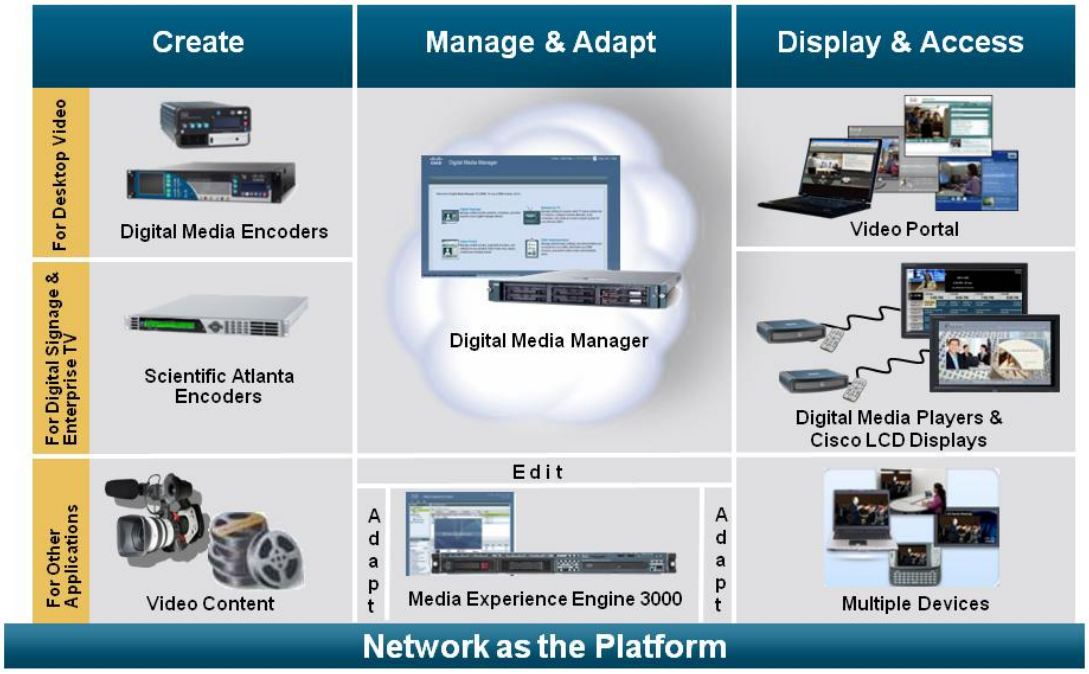


Figure 6.4.2.1 – Digital Media Suite Solution Portfolio

A key benefit of the Cisco Digital Media Suite is that it is a complete end to end solution that runs across an IP network with one management touch point that ensures interoperability and ease of management. The solution also tightly integrates with other aspects of the Cisco portfolio such as TelePresence and Physical security, maximising investment and business benefit and value. These systems can also link into existing customer technologies such as the VLE and include tracking mechanisms such as SCORM compliance. As the solution runs on IP it is accessible to manage or view content from any location where an IP connection exists, scaling across geographies and time zones.

Digital Signage

Digital Signage consists of electronic screens distributed around the University or College campus displaying rich streams of relevant, visually appealing information that is centrally administered and controlled. This information can be presented in a number of areas or zones on the screen which effectively 'carves up' the display allowing multiple streams of information to be viewed on the screen simultaneously. This can include generic information, flash animations, web sites, tickers, presentations, live lectures, live TV channels and other scheduled video. The various parts of the screen can be managed by

different users, and displays can be grouped together and managed by different user groups allowing a completely flexible and scalable deployment. This significantly reduces administrative overhead and allows delegation of parts of the screen area (or the entire screen for that matter) to those responsible for that faculty or department. For example, humanities staff can manage their screens totally independently from the Mathematics department who may want a completely different screen setup and "look and feel" to cater for their students and staffs needs.

This part of the Digital Media Solution includes Digital Media Players and Digital Signage display screens from Cisco, with the ability to use any display screen with the appropriate video connectors.

Figure 6.4.2.2 – Digital Media Sign – Example

Using Digital Signage from Cisco, any relevant digital content or information can be displayed such as:

- Daily Updates/Promotion of Special Events
- Student work such as media study material
- Pre-recorded lectures, expert content
- Live lectures
- Revenue generation via advertisements
- Highlight special events or information specific for that day and time such as timetable changes. Replace posters/flyers
- Directional signs
- Terrestrial TV in a zone on a screen, alongside University or College graphics
- Digital campus maps that can be updated as necessary for various events such as sporting events, graduation, guest speaker events
- Safety/Emergency Broadcasts
- Instant and scalable notification and evacuation information
- Room timetable information displaying the timetable and usage of the room to students

From a single platform this solution is able to deliver this rich content across a single campus, or to multiple campus environments.

Desktop Video

The Digital Media Suite can be used for desktop computer video delivery using a solution called Cisco Show and Share. Cisco Show and Share allows staff and students to publish content and comment on content, and ha s the ability to provide audio transcription. This can be used for College or University communications such as messages from the VC or Principal in order to support a more powerful messaging medium. It can also be used to deliver live or archived recordings of lectures and other forms of e-learning, removing physical and geographical boundaries and potentially attracting more students, and providing more flexibility for remote staff and researchers.

The latter idea in particular lends itself to a lecture theatre type environment (e.g. a Post-Graduate) or alternatively for a situation where content can be stored for archived viewing at the desktop. It could also be integrated into a Virtual Learning Environment (VLE), ensuring tight integration into existing learning systems.

Figure 6.4.2.3 – Digital Media Suite – Cisco Show and Share

The University or College video portal is secure and can be fully customised with the Institutions logos, colours, layouts etc. Customised playlists allow multiple program schedules, as well as detailed search features that allow end users to create their own playlists from content which supports both the teacher and learner in curriculum delivery and exam preparation. From a single, unified platform personalised digital content can be delivered anywhere on a global basis.

Examples:

- Classroom Video/Distance Learning
- Replace other mobile audio/visual delivery mechanisms such as VCR's and DVD players with the Video Portal—extend the classroom and use video for preparation courses, missed classes, specialized virtual classes, geographically remote students etc
- Virtual open days to showcase the institution and attract new students
- Administration and training
- Video on-demand for staff communication and community updates/information
- Event Broadcasts
- Broadcasting videos of sporting events, graduation, theatrical productions, student media work, board meetings
- External Marketing
- Provide video on-demand for potential students, sponsors, etc. to learn more about the offerings and to position as a leader in technology

- Delivery of live TV (terrestrial or satellite) to the desktop computer

Cisco Cast

Cisco Cast is an interactive application that enables organisations to deliver on-demand video and broadcast live TV channels over the institutions IP network to the digital signage displays around the University or College campus.

On-screen menus and program guides give users the ability to interactively access the Cisco Cast content, and organizations can customize lineups and create their own content libraries. Users can navigate through channel menus and select from on-demand content with a remote control or other remote device such as an iPhone or a Cisco IP telephone, removing the need for centralized administration of channel playback. Cisco Cast leverages the same hardware and management platform as the Digital Signage and Video Portal Solutions and interoperates with Cisco Digital Signage displays.

Figure 6.4.2.4 – Digital Media Suite – Cisco Cast

Cisco Cast delivers:

- Live television programs
- Content to support the curriculum
- Advertising
- Sales and marketing information
- Institution communications
- Entertainment content
- Student TV channels

Media Experience Engine

To improve collaboration and address the needs of different individuals and departments, Colleges and Universities need to adapt and customise digital media content for differing types of end user video experiences. This is to allow rich and compelling video content to be viewed on different types of endpoint device such as PDA's, mobile phones, laptop computers etc. For example, it would be very beneficial if a video of a lecture or a campus sports event recorded in a certain format could be easily recoded into other formats that allow it to viewed on differing types of end user device. The Media Experience Engine is a platform for the processing of user-generated content.

Key benefits of the MXE are:

- Media adaptation functionality enables users to view any media content on any end-point device.

- Media files can be shared easily between digital signage, desktop video, mobile devices and other applications. This is particularly applicable as increasing numbers of students wish to view content on their own devices which will probably require different format types from the Universities format
- Editing and production capabilities allow users to customize content with company logo overlays, introductions, and trailers , watermarks, music soundtracks etc
- Media "production" capabilities: video composition, editing, watermarking, text and image overlays, dynamic streaming tickers providing a completely personalised solution for digital media
- Media pre-processing: Color, noise reduction, & aspect ratio adjustments; video editing including clipping, cropping, and stitching

Encoders
Digital Media Encoders are an integral part of the Digital Media Suite and these devices capture content and then re-encode this media into several digital media formats for live and on-demand delivery across the campus IP network. The encoders can be managed across the network no matter what their location from the centralized DMM management platform. Encoders will allow the many legacy formats for media such as video, CD or DVD to be converted to IP-based formats for playback across a common platform via the DMS solution.

For more information: DMS Solution Overview;
http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/digmedsys.html

DMS Design Considerations:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/mrndmsaag.html

6.5 Information and Service Assurance

The increased reliance upon ICT increases the need for adequate assurance of applications, information and services; assurance that falls into three main categories:

- **Information Confidentiality** – ensuring controlled access to information on desktops, servers, Data centres and enterprise networks; ensuring information being transferred is encrypted to maintain confidentiality;
- **Information Integrity** – ensuring information has not been compromised through viruses or other attacks; ensuring adequate backup and restore capability, and disaster recovery procedures;
- **Information Accessibility** – ensuring the availability of LAN, WAN and data centre networks through incorporation of resilience and redundancy in design; ensuring immunity from malicious denial of service attacks that would render desktops, servers or networks unavailable.

Institutes should have security strategies to deploy technology in each of the above three areas in support of overall security policies. The conceptual architecture in Section 4 of the blueprint helps with this process as it shows the overall security capability distributed across several layers of the reference model.

Cisco views security in two dimensions; foundation security that will provide base security for a network or data centre, and enhanced security where additional capability is incorporated to meet particular confidentiality, integrity or availability requirements. Typical, well-assured ICT environments maximise the benefits of foundation security and deploy a range of enhanced security to meet local needs.

Foundation security can be found at the Transport Layer; it comprises a set of standard security features that should be enabled through hardware and software customisation of network devices. Foundation security is available for network devices 'out-of-the-box'; examples include software-based firewall and intrusion detection capability in routers, and 'denial-of-service' and 'man-in-the-middle' attack mitigation in LAN switches.

Enhanced security can be found at the Core Services Layer and above; it offers security features and performance not available within foundation security. Enhanced security may be necessary on a per-department or per-user basis where sensitive citizen or other data is being accessed and processed. It may also be

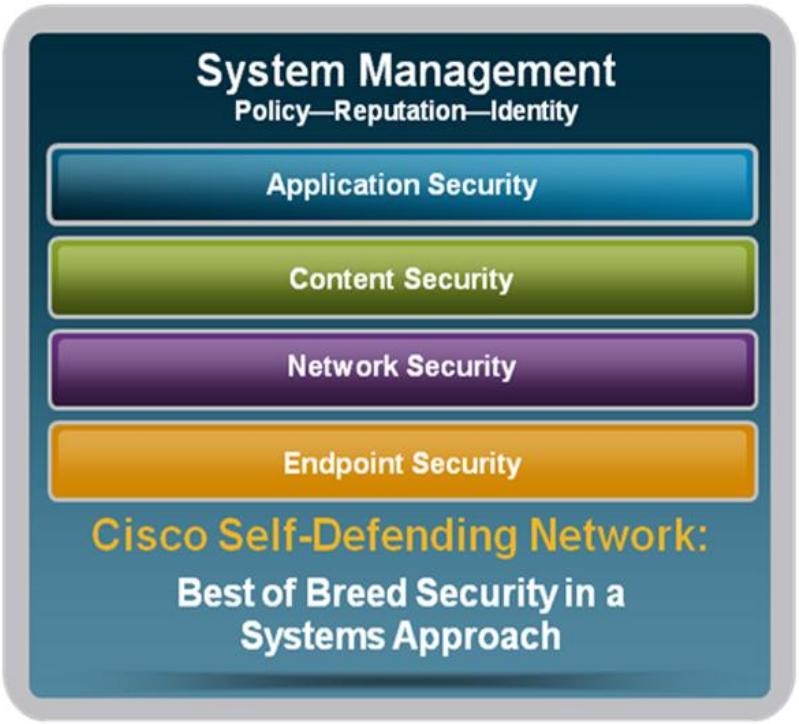
necessary to protect key resources such as data centres, or areas of vulnerability such as remote working VPN concentrators.

6.5.1 Cisco Self-Defending Network

The Cisco Self Defending Network (SDN) approach to ICT security was developed to address the growing security challenges that all organisations, including both Universities and Colleges, face in today's highly connected environment. With the increased need for collaborative working and compliance with strict data handling procedures, more effective controls must be deployed in order to ensure that sensitive data remains protected.

The Cisco SDN solution uses a systematic approach to address these challenges by following the industry recognised defence-in-depth principle. Defence-in-depth represents the concept of implementing multiple layers of security controls, such that the information security of an infrastructure is not reliant on any one component. For example, if an organisation relies solely on a firewall to protect their data and uses no additional controls such as strong authentication or encryption, the compromise of the firewall would lead to a total compromise of the data.

Figure 6.5.1.1 shows the five areas of Cisco SDN described in the following sections.



6.5.2 Endpoint Security

Network endpoints are often seen as one of the weakest and therefore most vulnerable parts of any infrastructure and protection of these devices is left almost exclusively to two technologies; personal firewalls and anti-virus. Generally speaking, anti-virus solutions are signature based which means they will protect against known attacks. When a new threat is discovered, the anti-virus vendor will update their signature database, which has to be downloaded to all systems for them to remain protected. The rate at which new threats are released, and their ever increasing complexity and sophistication, places a strain on signature-based anti-virus systems.

Another significant area of concern for endpoint security across the public services relates to Data Leakage Prevention (DLP). In 2008 there have been many publicly reported data breaches across UK Government departments, some relating to the use of removable storage i.e. USB memory sticks and CD/DVDs. Whilst most breaches were due to lost or stolen media, the question of the effective control and movement of sensitive data through these methods has been called in to question. Clearly, robust controls and audit mechanisms are needed but should not affect the legitimate business benefits these devices can offer to institutes.

In addition to the protection of the endpoint itself and managing the leakage of sensitive data, consideration should also be placed on the compliance of the endpoint with respect to an institute's security policy. Due to the nature of many of its' clients and employees, alongside the increasing use of mobile devices, an institute will likely be in a position where there is a large number of devices connected to the network over which they have no knowledge or control. This situation could present a significant risk to the institute; either of the spread of malicious code or of the leakage of sensitive personal data.

Cisco's approach is to focus on behaviour, rather than signatures. Simplistically, instead of worrying about what an attack looks like, a behavioural system worries about what an attack is doing. Focusing on the attack behaviour rather than the signature means the end system can be protected from a wide range of both known and unknown attacks. In addition this relieves the need for constant reactive patching given the confidence that a critical server is already protected. Patching can then performed in line with the institutes own policies, following thorough testing to ensure no adverse effects on applications or services.

To address the DLP challenges described above, the Cisco advanced endpoint protection solution can be extended to provide support for identifying and controlling the movement of sensitive data. Data can be tagged as sensitive; either on the basis of the data content or the application that produced it and once tagged, controls can be applied that can limit where and how that data can be moved.

Endpoint compliance can be addressed using a technology known as Network Admission Control (NAC) which performs the following:

- Authenticate & Authorise: Identify the user of the system to determine their role and apply the appropriate policy;
- Scan & Evaluate: Scan the device to check for AV version and patch level, operating system version including hot-fixes and service packs;
- Quarantine & Enforce: Isolating non-compliant devices;
- Update & Remediate: Where possible, update the device to bring it in to a compliant state and then and apply the appropriate policy.

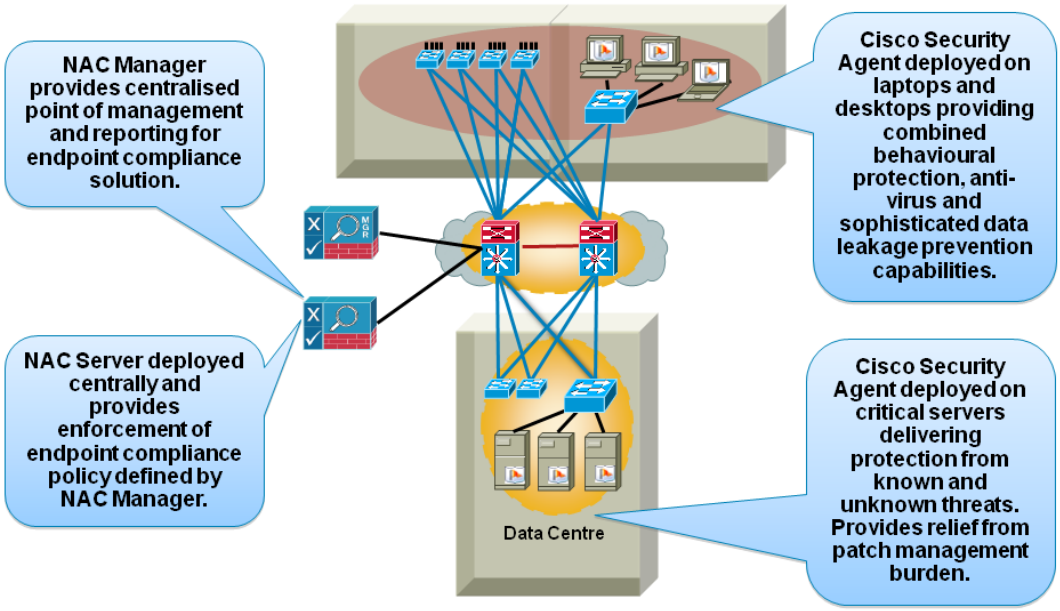


Figure 6.5.2.1 – Endpoint Security

In both University and College environments, NAC can be used in a variety of areas, for example:

- Shared service areas – users with distinctive roles share the same physical infrastructure and PCs but require differentiated access;
- Guest or 3rd party access – Allowing access from non-trusted or semi-trusted users and their devices. Enforce and audit acceptable use policy of these users;
- Wireless or VPN access – Access from remote locations or mobile devices.

An example of how the various Endpoint Security solutions are deployed is shown using a subset of the campus infrastructure template in Figure 6.5.2.1.

6.5.3 Network Security

This layer of the Cisco SDN is where most Colleges and Univerities have traditionally focused; it includes such solutions as:

- Network Foundation Protection;
- Network Firewall;
- Network Intrusion Prevention Systems (IPS);
- Virtual Private Networks (VPN).

These solutions are shown in Figure 6.5.31 using a subset of the campus infrastructure template as an example and showing Cisco solutions.

The most fundamental element of network security is Cisco Network Foundation Protection (NFP). NFP includes a suite of tools that are designed to protect the integrity of network infrastructure such that it remains operational, even when under sustained attack. Without NFP, all organisations are susceptible to network failure due to a worm or virus outbreak. It is important to highlight that the vulnerabilities are not within the network devices themselves, rather the network design does not protect the control plane under abnormal loads.

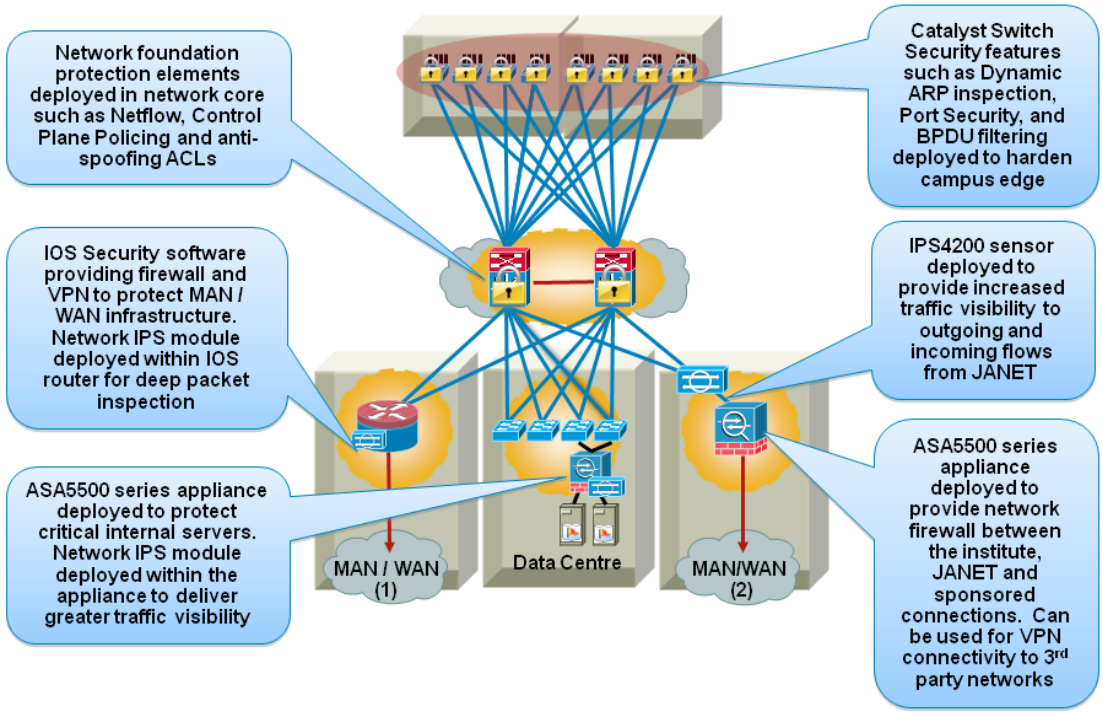


Figure 6.5.3.1 – Network Security

All network devices can be logically split in to a data plane and a control plane. The data plane is where the normal network traffic flows and the control plane is used for management and control i.e. routing protocols, spanning-tree protocol, logging etc. If a worm outbreak inadvertently targets the control plane of a network device, the volume of traffic the device has to deal with can be overwhelming, affecting the ability of the device to process routing updates (for example) and can therefore result in network instability. In this sense it has a direct bearing on the availability of the network.

NFP components are embedded within the standard Cisco IOS routers and Catalyst switches and are shown as foundation security within the Transport Layer of the Conceptual Architecture:

- Control Plane Policing (CPP);
- Unicast Reverse Path Forwarding;
- Cisco AutoSecure;
- Secure Shell;
- Quality of Service;
- Access-Control Lists;
- Netflow;
- Catalyst Security Toolkit.

The detail of these components is outside of the scope of this document, however it is important to emphasise and focus on building a robust foundation since the integrity and availability of all other services that use the network are affected if it is compromised.

Beyond the foundation, the next security element to consider is the network firewall. Designed to be a point of control between two distinct security zones, the network firewall is the most widely deployed network security solution in Institute's today and may exist in many locations; for example between the JANET network and the main institute infrastructure, or between a University and their sponsored connections to local institutes such as Colleges, Libraries or even partner institutes, forming an ExtraNet like environment.

Whilst in the past a firewall to implement perimeter security would have been seen as a cornerstone of network security, it is important that it is now considered as a component of network security complemented by other solutions.

The deployment of a network Intrusion Prevention System (IPS) augments the protection offered by a firewall. This is especially valuable where connections to third parties have to allow a wide range of applications and users to traverse a firewall thus increasing the exposure risk. The primary function of the network IPS is to perform deep packet inspection on network traffic to determine if the information carried is malicious, however the IPS may also be able to identify traffic flows which may not be malicious in themselves, rather they could be used for malicious activity such as peer-to-peer networking. The current threat landscape has led to Institutes deploying network IPS at key network boundaries; also within the network itself to provide increased visibility and protection against malicious traffic flows.

6.5.4 Content Security

Over the past few years, new attacks have focused heavily on the content of data and SPAM, phishing and web content attacks have all been utilised to provide an attacker with a foothold into a target system. These types of attacks are not particularly targeted and can therefore affect any organisation, including both Universities and Colleges. While SPAM e-mail is most often considered a nuisance, it is increasingly damaging and costly to deal with and can introduce malicious code in to a network.

Historically, protection against SPAM was limited to signature-based solutions looking for common words or phrases. However, as SPAM messages have become more sophisticated new solutions are needed. One new technique is referred to as 'reputation filtering'; where a reputation score is allocated to each sending domain such that a simple decision can be made as to whether the message is likely to be SPAM. The simple view is that the higher the reputation of a domain, the lower the probability that a message will be SPAM. By using reputation scoring, SPAM e-mail can be quickly and accurately discarded avoiding CPU intensive inspection.

As e-mail has become a ubiquitous tool for staff and student alike, to share data quickly and easily, there is an increased risk that this data may not be adequately protected. E-mail encryption allows sensitive data to be shared quickly and securely but the choice of solution must be simple to use and permit sharing of encrypted e-mails with third parties. Using a method known as 'secure envelopes', an e-mail sender doesn't have to worry about encrypting their e-mail. Instead, the central e-mail gateway can be configured with rules to encrypt messages based on the sender, recipient and even the content of the message. Furthermore, the recipient of the message requires no prior knowledge of the sender to decrypt the message and read it. This approach would enable users to have the confidence that when they share personal data via e-mail, it will remain protected, even when sent to external parties.

One final area of consideration is web filtering. Often deployed to address the concerns of inappropriate web content, it has more recently been used to address the threat of phishing websites or websites that have been hijacked and may now carry malicious content. As with SPAM filtering for e-mail, these solutions have traditionally focused on relatively static filtering techniques but can be improved by applying the same reputation scoring mechanism described above to web domains.

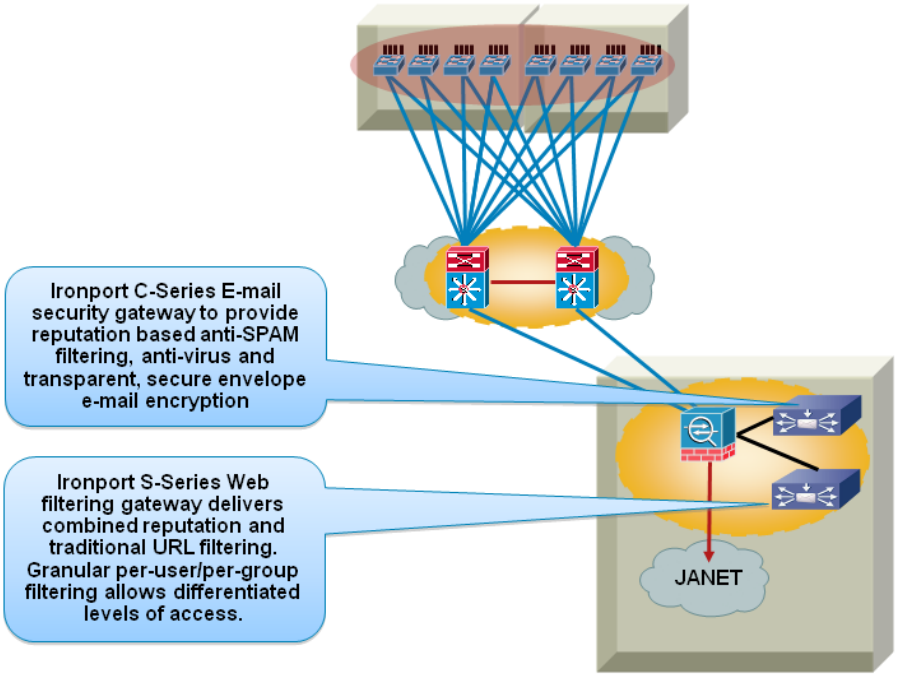


Figure 6.5.4.1 – Content Security

Content Security solutions are shown in Figure 6.5.4.1 which shows Cisco's offerings in this area based on the IronPort platforms.

6.5.5 Application Security

Web applications are often poorly protected. If exploited they can return high value information to an attacker and, as a result, are the most common target of application attacks.

There are a wide range of attacks that can be used against web services; they can lead to anything from site defacement to leakage of sensitive personal data. Traditional network firewalls do little to protect against these web application attacks and more specialised security solutions, such as a Web Application

Firewalls (WAFs) are required. When deployed, a WAF acts as a reverse-proxy between clients and web servers and watches for malicious web activity. If the target website is vulnerable to an attack, the WAF blocks the attack from being sent to web server and can simply return an error message to the user, else redirect them to another URL. The WAF forms part of the defence in depth strategy protecting against this growing area of concern.

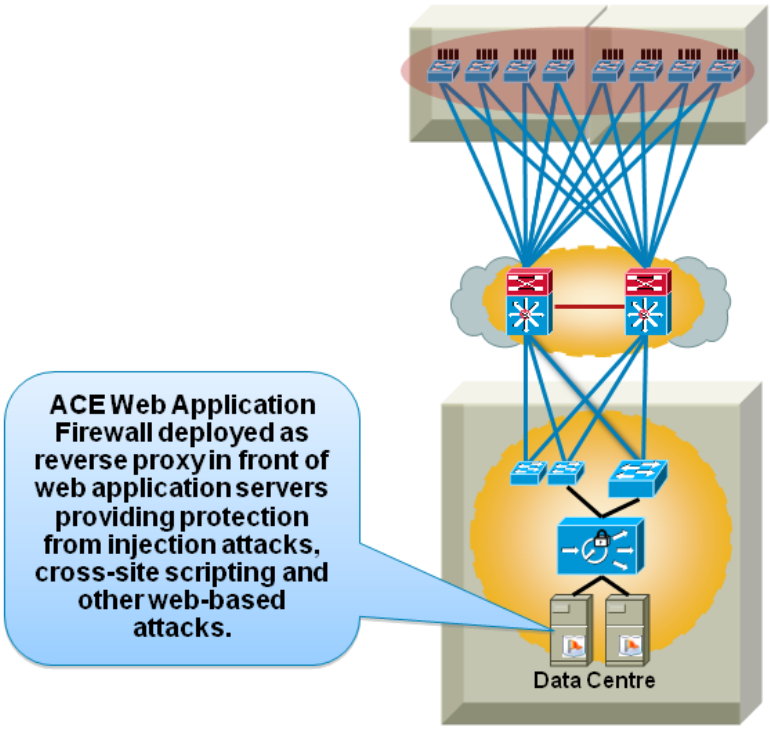


Figure 6.5.5.1 – Application Security

Application Security solutions are shown above in Figure 6.5.5.1.

6.5.6 Security Policy Management and Incident Reporting

The final, but possibly the most important aspect of any ICT security implementation, is effective policy management and reporting. The implementation of security controls should not be considered as a discrete activity; rather their configuration should be reviewed periodically to ensure they continue to fall inline with security policy.

It is essential that a comprehensive set of procedures and tools are in place to ensure that security change control is proactively managed and audited, and regular penetration testing should also be performed on the network and any identified vulnerabilities addressed.

Effective incident management and reporting should also be considered. Implementing technical controls but never reviewing the logging information produced by them greatly reduces their effectiveness. Many organisations will only ever review logging information after a security incident has taken place. This is often due to a lack of resource but is amplified through the lack of effective even management tools.

Following a defence-in-depth security model is effective in systematically securing a network, but it also introduces the challenge of increasing volumes of information that has to be reviewed. A security information event management (SIEM) solution such as Cisco CS-MARS can help by offering greater levels of visibility and intelligence. CS-MARS correlates events from multiple security devices together and quickly extracts relevant information raising it to the attention of an administrator.

6.6 Service and Network Management

Maximising the visibility of ICT infrastructure and the ability to control and manage it to meet changing needs are essential ingredients of service and network management best practice.

Cisco offers a very wide range of service and network management tool sets that operate within particular technology and end-user solutions sets. These are outside the scope of this blueprint because of their number, and because they will not be appropriate to every institute. In addition, however, a core set of tools are available to provide operations management of foundation infrastructure – with a particular focus on inventory, configuration and change management. These tools are likely to be appropriate to the majority of Institute and we recommend they be investigated.

CiscoWorks LAN Management Solution (LMS) is the key foundation management tool, and provides an integrated toolset that simplifies the configuration, administration, monitoring, and troubleshooting of Cisco networks. It offers:

- An integrated system for sharing device information across management applications;
- Automation of device management tasks;
- Visibility into the health and capability of the network;
- Identification and localisation of network problems.

By using common centralised systems and network-inventory knowledge, CiscoWorks LMS helps reduce network administration overhead and provides upper-layer systems integration.

Other common management applications include:

- Cisco Unified Operations Manager – provides a unified view of the entire IP communications infrastructure.
- Cisco Security Manager - an enterprise-class management application designed to configure firewall, VPN, and intrusion prevention security services on Cisco network and security devices.
- Cisco Wireless Control System (WCS) - provides wireless LAN planning, configuration, management, and mobility services enabling ICT staff to design, control, and monitor enterprise wireless networks from a centralised location.

7. Green, Sustainability and Carbon Management

The Stern Review[15], commissioned by HM Treasury in 2005, concluded that the scientific evidence for climate change due to carbon emissions was overwhelming but that the worst effects could be avoided if strong action were taken now. The UK Government has taken the lead in Europe with the announcement of the Carbon Reduction Commitment[16] Legislation from 2010 which means that organisations must proactively manage their carbon footprint.

ICT Technology is estimated to contribute as much as 2% of global emissions. However for a developed country, such as the United Kingdom, ICT in the home and in business could contribute as much as 20 – 25% of all emissions. The contribution of ICT is therefore considerable and has been the subject of detailed work at a Government and departmental level since the publication of the Stern Report.

With information commonly seen as the fourth utility within a building (Figure 7.1), ICT has the ability to drive organisations to work in new ways to manage and optimise energy consumption in order to meet institution and government targets.

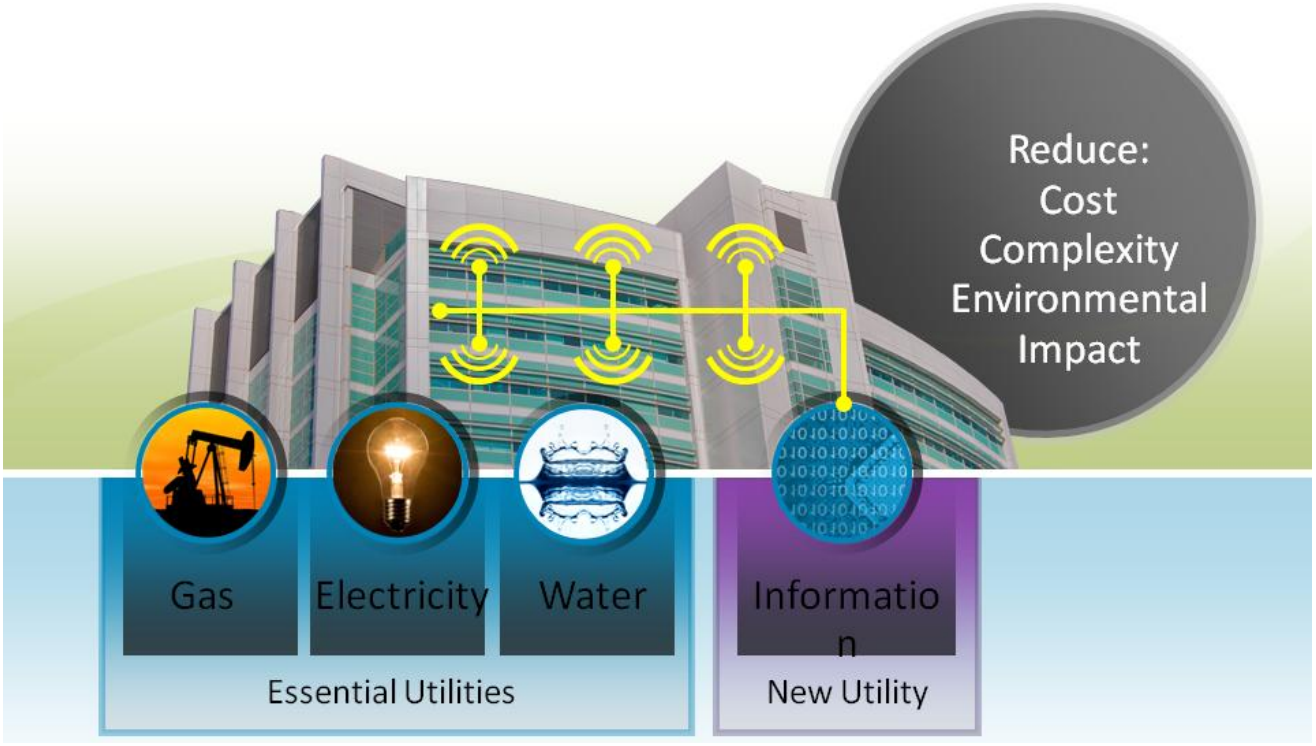


Figure 7.1 – Information, the new Utility

The Cabinet Office published its' Greening Government ICT[17] paper in July 2008. This paper, in Appendix B, re-iterates the Government's green targets and sets out a series of recommended ICT measures for PCs and laptops, other ICT equipment and for data centres that would reduce emissions. The paper highlights three key areas for purchasers of ICT equipment to engage with vendors:

[15] The Stern Review may be downloaded from: http://www.hm-treasury.gov.uk/sternreview_index.htm

[16] Information on the CRC may be found at the defra website: http://www.defra.gov.uk/environment/climatechange/uk/business/crc/index.htm

[17] The Greening Government ICT paper may be downloaded from: http://www.cabinetoffice.gov.uk/cio/greening_government_ict.aspx

- **Lifecycle Sustainability**: What is the whole lifecycle impact of a vendor product; in manufacture, in use and in the disposal phase?
- **Power Management**: What features and operational procedures are available for a vendor product to minimise or eliminate power usage when it is not in use or in standby?
- **Virtualisation**: What features are available in a vendor product to allow it to be used for multiple – maybe non-related tasks – thereby increasing its' utilisation and efficiency?

In addition a scaling of the findings from the University of Sheffield, Lowestoft College and City College Norwich (Sustainable IT, December 2008)[18] suggests that UK universities and colleges as a whole:

- Utilise nearly 1,470,000 computers, 250,000 printers and 240,000 servers
- Will have ICT-related electricity bills of around £116m in 2009
- Are indirectly emitting over 500,000 tons of carbon dioxide (CO2) emissions from this electricity use

As well as fitting into the green strategy of many universities and colleges, there are a number of reasons why sustainability has become an essential requirement from stakeholders; increasingly stringent regulation (outlined below); opportunities for financial savings and reduction of risk; opportunities for new areas of teaching and research; attraction of students; achieving Corporate, Social Responsibility(CSR) targets; and enhancing the sector's reputation

Legislation

The Carbon Reduction Commitment

- A Cap & Trade scheme that aims to improve energy efficiency year on year
- Government will publish a publicly available performance league table showing comparative performance of all participants
- This will apply to all state-funded schools, colleges and universities
- Qualifying organisations must start reporting from Oct 2009
- Scheme still applies even if an institution already buys renewable electricity

Climate Change Act 2008

- Sets legally binding targets for at least 26% reduction in CO2 emissions by 2020 and at least 80% reductions in GHG by 2050 against 1990 levels
- Caps emissions over 5-year periods to set trajectory for 2050. First 3 carbon budgets for 2008-12, 2013-17 and 2018-22 must be set by 1st June 2009

Climate Change Levy

- Environmental tax on industrial and commercial supply of lighting, heating and power

EU directive on Energy Performance of Buildings

- Energy Performance Certificates (EPC) for homes, commercial and public buildings when brought, sold or rented after 1st October 2008. Large public buildings need to display EPC from the same date

Renewable Transport Fuel Obligation (RTFO)

- 5% of all UK fuel sold on UK forecourts to come from a renewable source by 2010

[18] The Sustainable ICT in Further and Higher Education document may be downloaded from: http://www.jisc.ac.uk/publications/documents/sustainableictfinalreport.aspx

Carbon Emissions Reduction Target

- Energy suppliers to spend £1.5 billion over next 3 years to install home based energy efficiency measures for people on low incomes, those with disabilities and the over 70s

Renewables Obligation

- Licensed electricity suppliers to source 15.4% of electricity from renewable sources by 2015/16

As well as government legislation, students have also taken action with the creation of the Universities Green League Table[19]. With student retention capped it is essential that institutions ensure they are as attractive as possible. The Green League is People & Planet's environmental ranking of the UK's universities. It is part of the Go Green campaign, and aims to improve environmental performance in universities by raising the profile of environmental issues and creating a competition mechanism to drive up standards in the sector.

Within Higher Education HEFCE have also produced guidelines on sustainability[20]. HEFCE have a revised target for carbon reduction, sufficient to ensure satisfactory progress towards the government targets of reducing carbon emissions by 60 per cent against 1990 levels by 2050 and at least 26 percent by 2020:

"We want to make sustainable development a central part of our strategy for the future development of the higher education (HE) sector. Our vision is that, within the next 10 years, the HE sector in England will be recognised as a major contributor to society's efforts to achieve sustainability - through the skills and knowledge that its graduates learn and put into practice, its research and exchange of knowledge through business, community and public policy engagement, and through its own strategies and operations."

HEFCE also provide additional funding for innovative green technology[21] to help reduce the carbon footprint of an organisation:

And within Further Education the Learning and Skills Council have also produced guidelines:
"Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs. The UK government is committed to developing a sustainable, innovative and productive economy that delivers high levels of employment and a just society that promotes social inclusion, sustainable communities and personal well-being.

The further education system has a significant role to play in achieving this. The LSC needs to provide leadership for the system and act as an exemplar organisation through its own approach to sustainable development. Over the next 10 years, our vision is that the learning and skills sector will proactively commit and contribute to sustainable development through its management of resources, the learning opportunities it delivers and its engagement with employers and communities. In particular, we have the following vision."

- All providers and learners will know about sustainable development and expect it to be part of normal practice.
- Organisations will have strategies, policies and plans in place to integrate and implement sustainable development, and these will be understood and acted on.
- The LSC will have become an exemplar organisation by integrating sustainable development into its policies and everyday practices.
- Risks and barriers preventing sustainable development will be understood and strategies to overcome them will be shared.
- Continuous improvement in the sustainable development performance of the sector will be recognised and celebrated.

[19] http://peopleandplanet.org/greenleague

[20] http://www.hefce.ac.uk/lgm/sustain/

[21] http://www.hefce.ac.uk/news/hefce/2009/energy.htm

The LSC has already published its strategy From Here to Sustainability[22], following a consultation exercise.

Please note the current responsibilities of the LSC will be transferred from Autumn 2010 and split between the Skills Funding Agency (SFA), the Young Person's Learning Agency (YPLA) and the Local Authorities.

All of this means that the education sector is looking to technology partners to assist in meeting their sustainability objectives.

At a product and technology level Cisco has adopted a lifecycle strategy to minimise the use of energy during both manufacture and in use phases of a product's lifecycle. All Cisco supply chain members are subject to sustainable sourcing vetting and Cisco recycles or re-uses almost 100% of the materials in old products returned via the 'Cisco Takeback Program'[23].

In addition a range of Power Management solutions are becoming available to reduce or eliminate the use of energy by the network or by attached devices during periods of limited or zero usage (for example overnight), or in response to defined triggers. Finally almost all Cisco products - LANs, wireless LANs, WANs, SANs, firewalls, server load balancers, IP call switching processors and others - encompass a virtualisation capability. This permits individual products to serve multiple requirements and ensures that each product (and the energy it consumes) is exploited to the maximum.

[22] From Here to Sustainability: The Learning and Skills Council'sStrategy for Sustainable Development, September 2005.

[23] http://www.cisco.com/web/about/ac227/ac228/ac231/WEEE/English_GB/Introduction.html

8. Cisco Support for Delivering the 21st Century Connected Learning Institution

Cisco Services can provide expert assistance at key points throughout the solution lifecycle to accelerate the delivery of the 21st Century Connected Learning Institution model, while minimising risk through the use of proven architectures and methodologies.

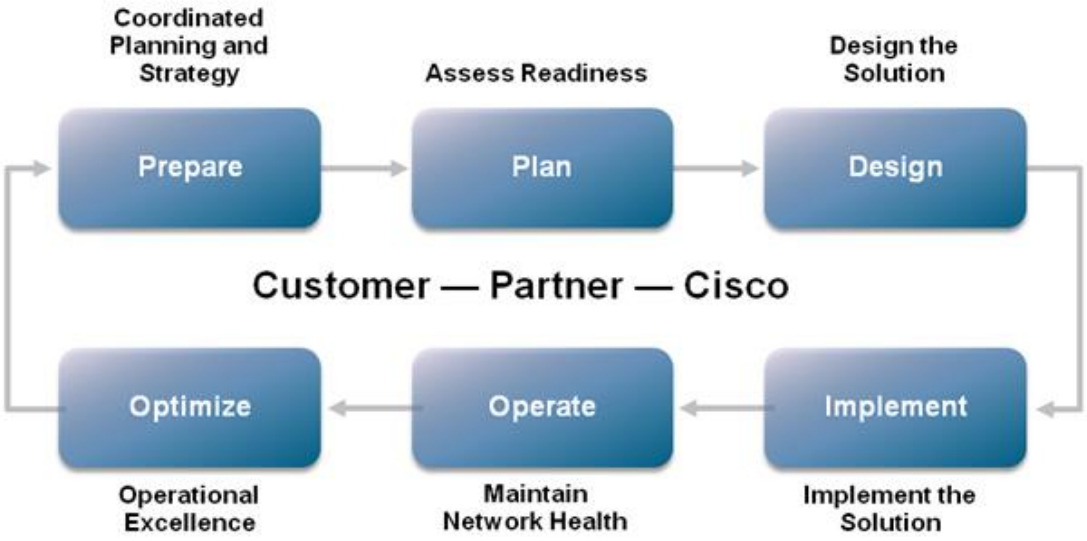


Figure 8.1 – Cisco Lifecycle Services

The Cisco® Lifecycle Services approach defines the minimum set of activities needed, by technology and by network complexity, to help successfully deploy and operate Cisco technologies and optimise their performance throughout the network lifecycle. Cisco Services can support you in the development and deployment of the 21st Century Connected Learning Institution Blueprint through an integrated portfolio comprising of:

- Cisco Advisory Services: to formulate and plan business aligned IT strategies and to provide architectures, deployment and migration plans.
- Cisco Advanced Services: to provide professional services to enhance network performance and to accelerate the deployment of network solutions.
- Cisco Technical Services: to deliver network support services that offer maintenance and proactive diagnostic capabilities to achieve improved network availability.
- Cisco Remote Management Services: to ensure issue resolution and day-to-day management through a comprehensive suite of remote monitoring capabilities.

Cisco uses its extensive network of partners to develop and deliver services using this Cisco® Lifecycle Services approach. This can help you to deploy solutions on time and on budget using a consistent, proven set of service-delivery methodologies.

Appendix A. 21st Century Connected Learning Institution Blueprint Team and Contacts

21st Century Connected Learning Institution Blueprint Team	
John O'Donnell	System Engineer Manager – H&FE England and Wales
Russell Vaughan	System Engineer – H&FE England and Wales
Rik Irons-Mclean	System Engineer – H&FE England and Wales
Matt McKenna	System Engineer – H&FE England and Wales
Stephen Kirk	System Engineer – H&FE England and Wales
Andy Vallely	Consulting Systems Engineer - Europe
Jonathan Taylor	Business Development Manager – Europe

UK Higher and Further Education Primary Contacts August 2009		
Michael Watkins	Regional Manager	0207 496 3742
Lee Simpson	Account Manager	0161 249 5736
Steve Bradley	Account Manager	0161 249 5935
Stuart Player	Account Manager	0208 824 0047
Barbara Ougden	Account Manager	0208 824 5351
Darrell Greenwood	Account Manager	0208 824 9650
Gareth Lewis	Account Manager	0208 824 8284

Appendix B. Technical References

Following is a non exhaustive list of references to public materials related to the topics contained in the 21st Century Connected Learning Institution Blueprint

Use of technologies and spaces in the learning environment.
http://www.jisc.ac.uk/uploaded_documents/JISClearningspaces.pdf

http://www.sfc.ac.uk/information/information_learning/AMA_spaces_for_learning.pdf

http://www.jiscinfonet.ac.uk/infokits/learning-space-design

http://www.smg.ac.uk/documents/PromotingSpaceEfficiency.pdf

Enhancing learning and teaching through the use of technology:
http://www.hefce.ac.uk/pubs/hefce/2009/09_12W/

Green and Carbon Efficiency
HEFCE Funding
http://www.hefce.ac.uk/news/hefce/2009/energy.htm

Guidelines on Sustainability
http://www.hefce.ac.uk/lgm/sustain/

Government Carbon Reduction Commitment
http://www.defra.gov.uk/environment/climatechange/uk/business/crc/index.htm

The Edgeless University
http://www.jisc.ac.uk/edge09

Following is a non exhaustive list of Cisco materials related to the topics contained in the 21st Century Connected Learning Institution Blueprint

Data Centre
http://www.cisco.com/en/US/netsol/ns708/networking_solutions_solution_segment_home.html

Unified Compute System
http://www.cisco.com/en/US/products/ps10265/index.html

Wireless LAN
http://www.cisco.com/en/US/products/hw/wireless/index.html

Cisco 'Virtual Office'
http://www.cisco.com/en/US/netsol/ns855/networking_solutions_package.html

Information and Service Assurance (Security)
http://www.cisco.com/en/US/netsol/ns170/networking_solutions_solution_segment_home.html

Unified Communications
http://www.cisco.com/en/US/netsol/ns151/networking_solutions_unified_communications_home.html

Collaboration Services
http://www.cisco.com/en/US/netsol/ns870/index.html

Mobility
http://www.cisco.com/en/US/netsol/ns175/networking_solutions_solution_segment_home.html

Business Video
http://www.cisco.com/en/US/netsol/ns813/networking_solutions_solution_segment_home.html

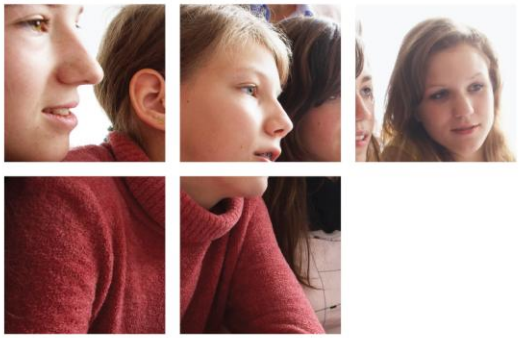
Cisco TelePresence
http://www.cisco.com/en/US/netsol/ns669/networking_solutions_solution_segment_home.html

Connected Building Systems
http://www.cisco.com/web/about/ac79/docs/wp/ctd/ConnectedRealEstate.pdf

Digital Signage
http://www.cisco.com/web/solutions/dms/digital_signage.html

IP Video Surveillance Physical Security
http://www.cisco.com/web/solutions/ps/index.html

Cisco Framework for Higher & Further Education



Important Notice

"The guidance provided in this blueprint is of a generic nature and not specific to your organisation or operational environment. Please contact your Cisco partner or Account Manager to discuss your specific requirements. Errors and omissions are accepted. No warranty is given or implied."

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.**