UTILIZING MODERN NETWORK TECHNOLOGIES IN A CAMPUS NETWORK

Piotr Goetzen, Jan Makuch, Agata Skowrońska-Kapusta,
Alina Marchlewska, Robert Zachlod

IT Institute, Academy of Management, Lodz, Poland
(goetzen, jmakuch, akapusta, amarchlewska)@swspiz.pl

Abstract

The purpose of this paper is to outline concepts and examples of reliable and efficient communication systems for all parts involved in the modern education model. As proven in the presented paper, designing an academic-size network is a real challenge to a team of designers. The outcome vastly depends on the skill and experience of the design team.

Key words: computer networks, security, network design

1 Introduction

1.1 Access to information

The 21 st century with its overwhelming technological progress incorporates new trends into our lives. It also transforms today's education. The evolution in communication, time management and the concept of e-learning require a cutting edge and complex infrastructure to fulfil the needs.

The global e-learning is estimated at around 38 million euro. Access to richer information, interactive tools supporting collaboration, video conferencing, computer simulation and real time communication stand new challenges in the area of computer networks and service integration.

1.2 Digitization

Electronic documents created in the process of digitization have a significant advantage over their analogue counterparts – they are easily searchable, catalogued and shared. Such documents have multiple forms – from electronic documentation (Office documents, PDF, CAD) to electronic maps or podcasts. The process of digitization itself is based on representing the content in

the form of binary code, which – depending on its type and format – can be accessed and read by the user. Quite often, digitization is perceived as the process of scanning documents or pictures, but it also refers to audio files.

1.3 Modern teaching platforms

The definition of E-Learning 2.0 is a neologism created to name Computer-supported Collaborative Learning supporting the education processes developed in the rise of Web 2.0. Unlike the current definition of e-learning, its successor emphasizes on using social networking, blogs, Wikipedia, podcasts or virtual reality as means of information exchange. some of the benefits of this approach are:

- Improving communication
- Instant effects of work
- Integrated leaning environment (e-mail, instant messaging, audio and video transmission)
- Ease of access to information for project groups
- Effective time management

1.4 Accessibility of the data

Portable devices, rising popularity of networks, and ubiquity of the Internet make access to information easier than ever. Modern networking being a hybrid of 3G and WiFi incorporates a revolution in education and changes the common understanding of a class. Research and trial programmes on many universities worldwide confirm the uptake in access to information on the go. Multimedia in education is more attractive for the end user and most of all – more effective. Instant access to Push email, podcasts and mobile platforms are shaping education models of the 21 st century.

2 The problem

2.1 Assessing the requirements

In the past 20 years computer networks have become a key element of education and an essential ingredient in the technological progress. So called “human network”, the symbiosis of the society and technology, illustrates the scale of changes and evolution of computer networks, their size and capabilities. It concentrates on collaboration, interaction and real-time communication of its part-takers, be it a student, academic, client, or visitor. The increasing demand for mobility, rising security standards and the necessity to

identify and segment users groups, devices and sub networks are all implied by the changes in modern education. Some of the challenges to campus networks are as following:

- Global access to information
  - Unifying communication and meeting Service Level Agreements
  - Migration towards centralised data stores
  - 24x7x365 availability for different time zones
- Real time collaboration
  - Customer satisfaction as the key requirement
  - Minimum downtime and disruption for any upgrade or maintenance type work
- Evolution of security risks
- The demand to follow technological progress including future standards
- Requirements for mobile access
- Next-generation applications requiring high throughput
- Growing complexity of networks

All of the above critical requirements of a campus network not only present the need of cutting edge technologies, but also excellent planning, management and network design skills. The successful designer has to consider two best practice concepts: hierarchical design and modularity, as they account for resilience and the ease of growth. By dividing network into subsystems and interconnecting then in a specific manner, we gain a high level of stability, centralised management, increased efficiency and better fault tolerance (fail over redundancy, load balancing) for both single components, as well as the entire network. Some of the questions to be asked are:

- What roles will certain layers of the network play?
- What are the key elements of the system and how they interact?

2.2 Technology involved

2.2.1 VLAN

VLAN stands for Virtual Local Area Network and is a group of hosts communicating within the same broadcast domain, regardless to geographical position. VLAN operates on Layer 2 of the OSI model and retains the same attributes as a physical LAN, except for allowing to group hosts physically connected to a different network switch.

VLANs are used to segment the network and address the issues of scalability, security and management [3].

2.2.2 Spanning Tree Protocol

STP is a protocol of Layer 2 of the OSI model. It addresses the risk of broadcast loops in redundant link topology. STP tackles the problem by blocking the spare link for traffic and allowing only a single path of traffic. The spare ling gets live when the main link goes down. Information is exchanged by participating switches using BPDU messages sent at a defined interval. The successor of STP is RPVST (Rapid Per VLAN Spanning Tree), which propagates changes to topology much quicker and reduces the time from 30-50 seconds down to around 6 seconds.

2.2.3 ACL

Access Control Lists are a set of rules defining data traffic patterns within a network. Cisco devices support two types of ACLs:

- Standard – based on the source address, used on the destination side, disallowing traffic by default

Extended –used on source side, giving more flexibility (source/destination address, port number, protocols of lower layers).

2.2.4 Port Security

To mitigate risks linked to physical access to network infrastructure (for example CAM table overflow), Port Security functionality can be implemented on Cisco devices. Port Security allows specific behaviour in the event of a device MAC address change on the switch port. The switch usually learns the MAC address by adding it to its CAM table, but if the number of MAC addresses advertised on the port exceeds a given value, the port can either be shut down by Port Security, or configured to ignore the flooding MAC addresses.

2.2.5 HSRP

HSRP (Hot Standby Router Protocol) is a gateway protocol providing gateway redundancy. It defines how the traffic behaves in the event of one of the gateways failing. The participating routers nominate a main router to act as the virtual gateway. During normal operation, multicast “hello” packets are exchanged to coordinate the work. In the event of the main routers failure, the router with the second highest priority will take over and respond to ARP requests coming from the hosts.

2.2.6 EIGRP

EIGRP is a distance vector based routing protocol. Its main benefits are fast convergence in the event of the topology change and the marginal use of bandwidth and router processing power, compared to other routing protocols. EIGRP stores routing data in three tables:

- Neighbours table – containing information about other routers
- Topology table – containing routing tables gathered by other routers
- Routing table – containing destination routes

EIGRP supports authentication and is easier to configure than OSPF, but is a Cisco proprietary protocol. The metrics it uses are the following:

- Bandwidth
- Load
- Delay
- Reliability
- MTU

2.2.7 Etherchannel

Etherchannel is a technology used on Cisco devices, which allows link aggregation in order to maximize throughput. It combines 2 up to 8 physical interfaces (Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet) into one logical connection to reach throughput of up to 80Gbit/s. The aggregated interfaces share the same MAC address, which makes it transparent from the Layer 2 point of view. This feature limits the bottleneck effects in the campus network and allows the administrator to overcome performance problems

2.2.8 Multicast communication

In university campuses, the administrator needs to reinstall operating systems on the workstations. This situation occurs very often due to intensive use of computers by students. The process of rebuilding the configuration of the computer laboratory may take a great bandwidth of available throughput of the network. Instead of transmitting the x times of streams of the same data it is possible to transmit one stream of the data to all computers. The multicast communication can also be used to save the bandwidth during multimedia streaming (lectures, podcasts, multimedia applications, etc)

2.3 Hierarchy

2.3.1 Network layers

The network design is based on the Cisco Enterprise Campus architecture and comprises of three layers:

- Core
- Distribution
- Access

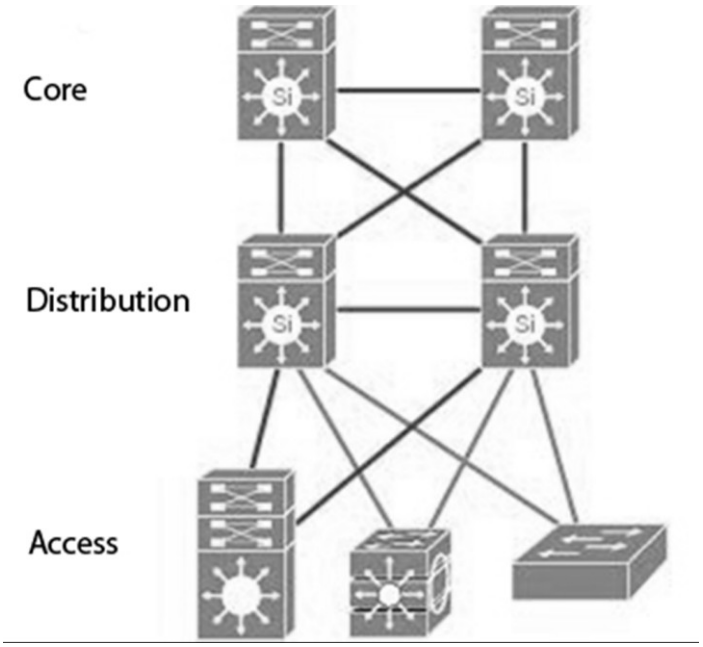

Figure 1. Network layers [1]

2.3.1.1 Core

The core is in a way the simplest, yet most critical layer of the entire network. It provides a limited set of services designed to operate 24x7x365. The most important factor to consider is full hardware redundancy to restore communication in the event of a fail over. The core connects the remaining elements of the network, including the data centre, distribution switches and the network edge.

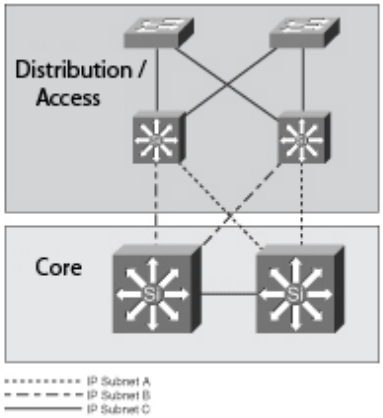

Figure 2. Core layer [4]

2.3.1.2 Distribution layer

The distribution layer is an aggregation point of all access layer switches. It also provides policies and network traffic supervision and takes part in the routing process. Questions to be asked while designing the distribution layer can be as follows:

- How many end users does the distribution layer support?
- What level of redundancy is required?
- Can the layer be extended through better functionality? (multicast, IP telephony)

Since the distribution layer is a bridge between the core and the end user, maximum throughput on each port is expected. To cater for these needs, enterprise networks usually use very fast Layer 3 switches which utilise Quality of Service and packet filtering.

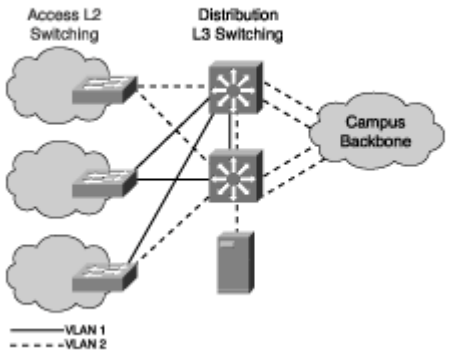

Figure 3. Distribution layer with full redundancy [4]

2.3.1.3 Access layer

The access layer is the network edge, which connects end user hosts and devices using structural cabling. Multitude of devices connected to this layer implies the robustness and flexibility. At the stage of designing the access layer certain constraints have to be taken into account:

- Physical port security
- Access speed
- Traffic prioritisation and classification
- Modularity of hardware
- Required efficiency in Layer 2
- Required redundancy
- VLAN configuration
- Additional functionality (Port Security, VPMS, multicast, QoS)

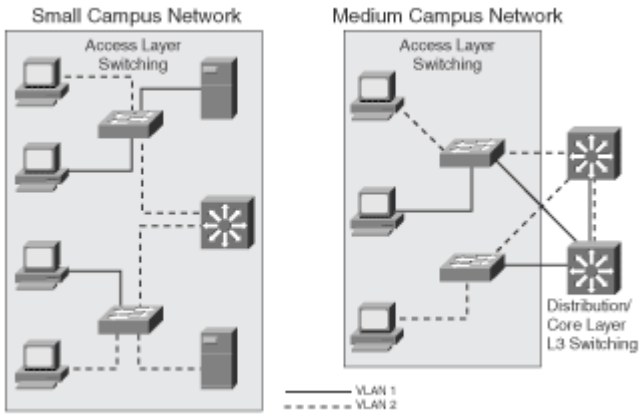

Figure 4. Access layer with full redundancy [4]

Below we present sample services which run within the access layer:

Table 1. Services within access layer

Service	**Function**
Discovery and configuration	CDP, LLDP, 802.1AF
Security	Port security, DHCP snooping, 802.1x, DAI, IPSG
Identification and access	MAB, Web-Auth, 802.1x
Intelligent service management	PVST+, Rapid PVST+, EIGRP, OSPF, DTP, PAgP/LACP, UDLD, FlexLink, Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, Port Security, Root-Guard
Traffic detection	QoS, packet inspection

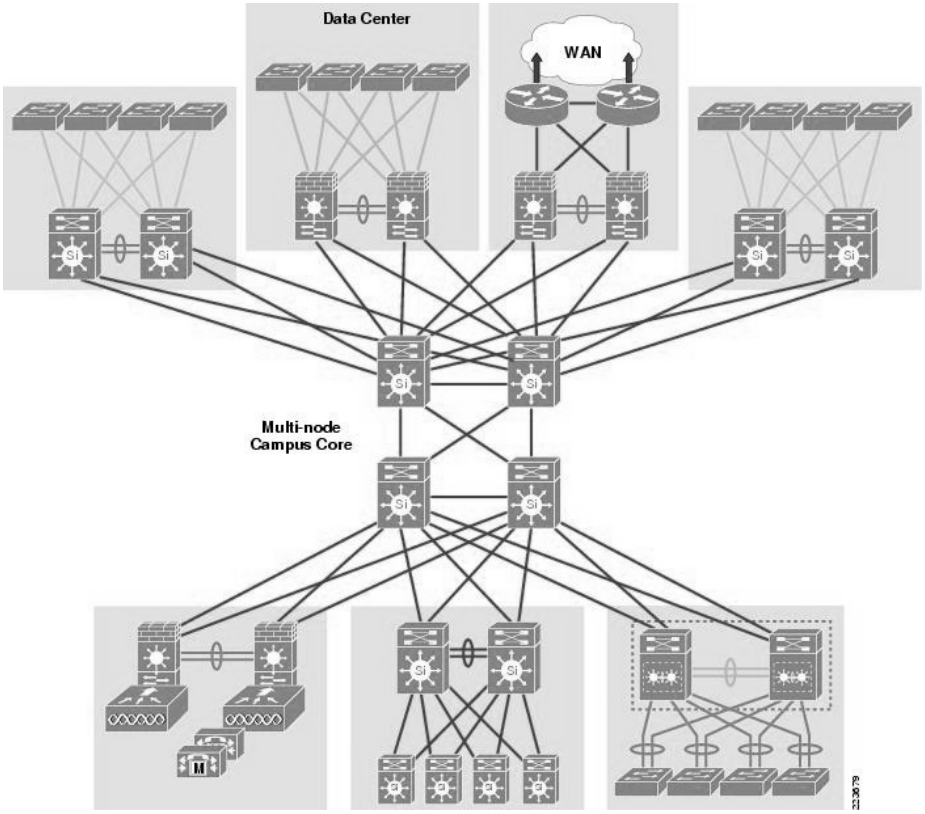

Figure 5. An example of geographically spread network requiring core [1]

2.4 Enterprise network requirements

The network requirements are provided in the table. The technology, scalability, accessibility, performance, price per port are presented for each of network layers.

Table 2. Layers features and requirements

	Access	**Distribution**	**Core**	**Data centre**
Technology	Shared	Layers 2, 3	Layers 2, 3	Layer 3
Scalability	High	Medium	Low	Medium
Accessibility	Low	Medium	High	High
Performance	Low	Medium	High	High
Price per port	Low	Medium	High	High

2.4.1 The 20/80 rule

Until recently the network traffic was described as 80/20, which means 80% of the traffic was local, 20% was external. The evolution of network concepts and viability of data centres result in the traffic pattern changing into 20/80 (most traffic outside VLAN). The increasing traffic in the core of the network is another reason to use fast Layer 3 devices.

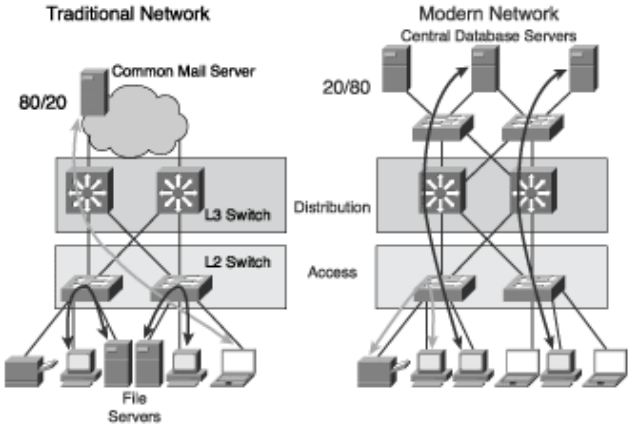

Figure 6. Comparing 20/80 and 80/20 traffic patterns [4]

2.4.2 Addressing

Depending on the needs of departments, colleges and units, they will get assigned /24 subnets (254 usable addresses) up to /22 subnets for large units (1022 usable addresses). To streamline management of IP addressing and DNS, it is advised to implement an IP address management solution. An ex-

ample of such software is IPAM by BlueCat Networks, which offers the following benefits:

- Modelling and managing with large address pools (>million IP)
- Using one interface to centrally manage DNS and DHCP servers
- IP discovery mechanisms providing up to date information on hosts
- Change management and transaction logging [5].

2.4.3 Quality of service

To comply with rigorous data traffic requirements, certain technologies can be implemented. VLANs are used to prioritise real-time traffic for the application of VoIP and video conferencing. The overall quality of services across the network is subject to a set of policies.

2.4.4 Network management

To provide a high level of security, network management can occur only within one subnet, secured and configured accordingly by the network administrators (ACL). To deliver their work in a desired manner, some network technologies and systems can be put into place:

- **CiscoWorks** – a Cisco proprietary LMS system (LAN Management Solution) comprising of a set of tools simplifying the management on a network
- **TACACS+** - a protocol providing centralised access control to routers, switches and other network equipment
- **RADIUS** – a network protocol providing centralised AAA model
- **Netdisco** – a network management utility offering unified Web access to network devices and detailed information gathered via SNMP, CDP, LLDP and stored in a SQL database

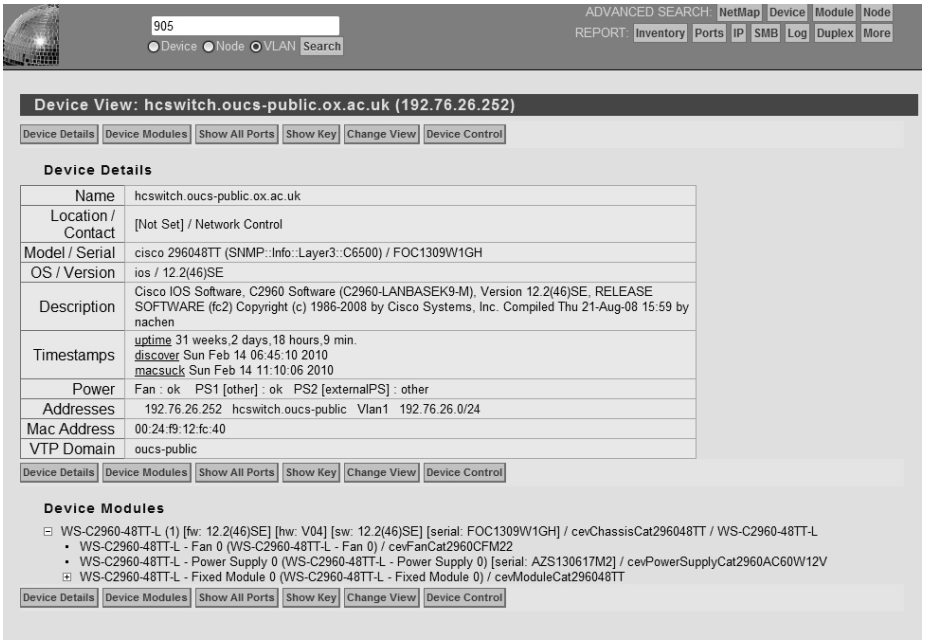

Figure 7. Sample device information page in Netdisco

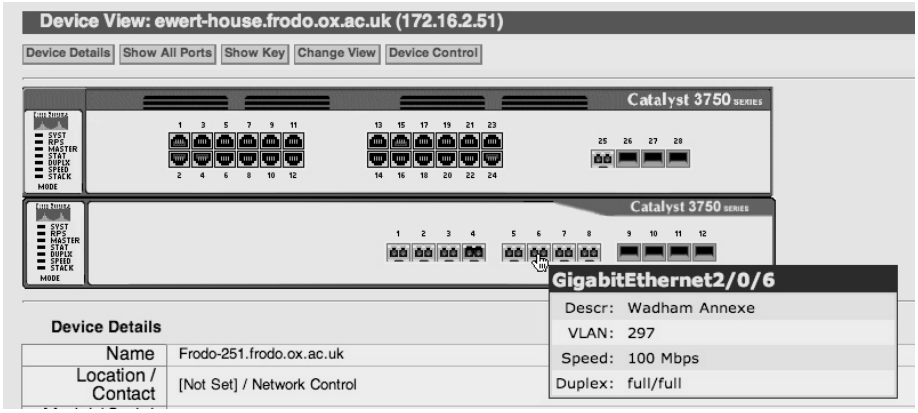

Figure 8. Sample ports view in Netdisco

- **Nagios** is another, open source, monitoring tool renowned for its rich functionality in managing network services and systems (supporting reporting and auditing of SMTP, POP3, SNMP, FTP, SSH and other popular services).

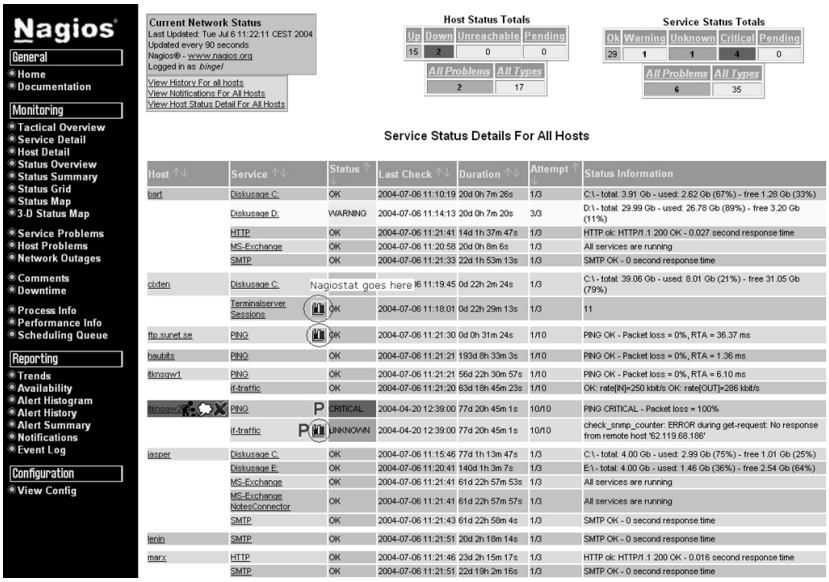

Figure 9. Service monitoring in Nagios, Source: http://www.nagios.org/

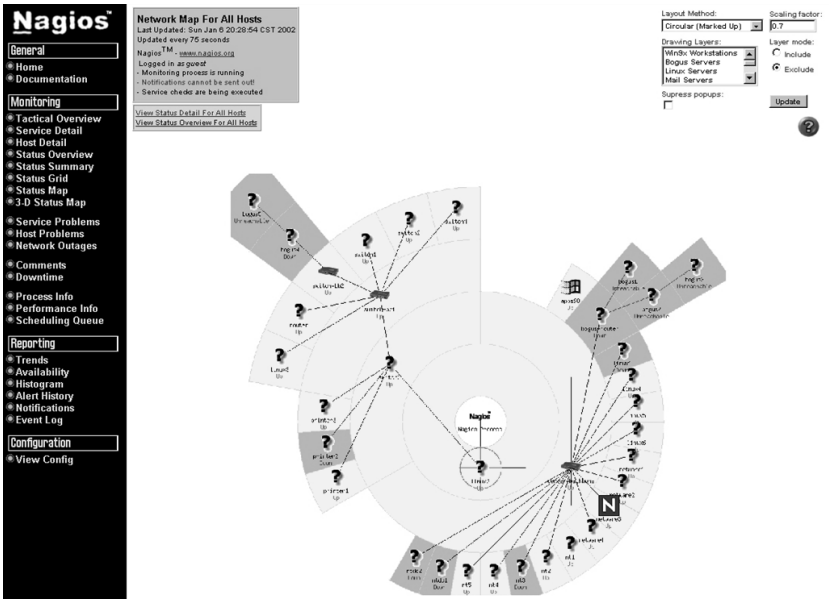

Figure 10. Sample network topology in Nagios Source: http://www.nagios.org/

- Various **VPN** software for access to management subnet from remote locations.

2.4.5 Obstacles

A successful network designer is expected to foresee and mitigate certain risks:

- Geographical – depending on the topology of the area, structural difficulties may arise in the distribution and access layers. To mitigate a possible fail over, maximum redundancy is essential. Regaining convergence in the event of failure is also dependant on the way device configuration files are handled and aggregated.
- Unauthorized access – a dispersed network with high fragmentation and autonomy is subject to access-related risks. To minimize the risk of access breaches, technologies like Port Security, 802.1x and RADIUS can be implemented.
- Service-related threats – a modern computer network faces a wide spectrum of service-related risks. The risks include spam, Denial of Service attacks, password cracking, phishing attacks, ARP spoofing, viruses and spyware, man-in-the-middle attacks and copyright breaches.

3 Solution

3.1 Why Cisco?

After a thorough consideration of available technologies and vendors on the networking markets, it becomes apparent to reveal Cisco as the supplier of technology and hardware. Reasons for this choice are as follows:

- Cisco is a highly recognizable brand and the key player on the market of networking
- It offers innovative products with exceptional levels of reliability and expandability
- Service integration into a high level and a good Return-of-Investment (ROI) are some of many benefits of choosing Cisco as a long term supplier
- Feature-rich and market leading products

3.2 Hardware capabilities

3.2.1 IPv6

The IANA (Internet Assigned Numbers Authority) estimates that the IP version 4 addresses will no longer be available in the next year or two. This emphasizes the importance of IPv6 compliance for any network considerations. Cisco offers support for IPv6 on most of its devices to allow a smooth transition onto the new standard.

3.2.2 Expandability

Modular design of Cisco devices makes hardware upgrades non-disruptive and easy to roll out. Popular supervision modules, as well as 10Gigabit Ethernet modules are at disposal of network designers and administrators to increase overall throughput of the network backbone as well as distribution layers.

3.2.3 Scalability

Scalability describes the capabilities of a system in terms of certain aspects:

- To support an increasing network load
- To improve management and administration of devices
- To increase functionality retaining the least time and effort investment

Cisco improves scalability in many ways and at many levels. Below are only a few considerations on hardware level:

- Modular design of switches and routers. Example: Catalyst 6500 chassis switches can be equipped with slotted modules, ranging from IPS/IDS platforms, through fibre interfaces increasing throughput between vital segments of the network.
- Wireless LAN controllers give a new meaning to wireless hotspots. Instead of using autonomous access points, it makes more sense to employ a WLC, convert all devices to lightweight mode and manage them centrally. In this way, for instance adding an additional SSID to a department utilizing a few dozen APs is a relatively quick job, compared to reconfiguring every single access point.
- Adding complexity to network, for example linking geographically dispersed annexes can be achieved by Q-in-Q tunnelling, which is fully supported by Cisco switches.

  Scalability is a key feature of modern university campus networks.

3.3 Network security

Network security is a critical aspect of the campus network infrastructure, hence it requires relevant emphasis on mitigating the risks. A team of network designers and security analysts has to work closely together to address some of the following issues:

- Confidentiality of data – the risk of wiretapping and man-in-the-middle attacks needs to be minimized
- Physical access – relevant consideration in access to data centres and network equipment
- Authentication and access restrictions based upon it
- Addressing abuse, for instance copyright infringements
- Network traffic monitoring and monitoring

Some of the best practices in the area of network security include:

- Rejecting incoming traffic on firewall except for connections initiated from the inside
- Rejecting outgoing traffic except allowed services
- Identifying service provision systems in order to separate them and tighten security
- Minimizing wiretapping and data sniffing by requiring encrypted connections
- Integrating IDS systems with directory services to allow deep packet inspection in order to mitigate phishing attacks
- Separating hosts breaching security policies (router and switch port block)

Cisco proposes several advanced security solutions which are built in switches, routers, security appliances (NAC, ASA, IronPort), With Cisco NAC Appliance, for example, it is possible to:

- Recognize users, their devices, and their roles in the network, provide guest access
- Evaluate whether machines are compliant with security policies
- Enforce security policies by blocking, isolating, and repairing noncompliant machines

4 Conclusions

Modern campus and military networks are the breeding grounds for emerging computer technologies. The education sector quite often formulates specific requirements and establishes new trends that the industry assimilates since decades. The evolution of education, new forms of communication, cultural changes constantly interact establishing new standards.

There are many risks that need to be addressed to at the stage of designing an “enterprise” network. For example, the expected shortage of IPv4 ad-

dresses is a challenge to network designers and requires more insight into hardware compatibility with IPv6. Cisco, being the largest vendor of network equipment, delivers standard compliance and interoperability. It is also an innovation, compatibility and modularity that determine Cisco as a preferred supplier.

Academic environment is also a challenge for network security. Geographical span of the network combined with large amounts of data and dispersed structure makes it an attractive target for potential attacks. It needs to be pointed out, that the overall security of the network is as weak as its weakest link – deciding upon technology doesn't eliminate the human factor. Cisco offers both devices and technology allowing to minimize risks. With the benefit of intrusion detection and prevention systems (IDS/IPS) the incidents can be eliminated at an early stage.

From the network architecture point of view, full redundancy of crucial network components is necessary (in both core and distribution layer), so that in the event of failure, connectivity can be instantly restored. It is essential to oversee certain scenarios at the planning stage, as certain modifications may turn up impossible at a later stage.[6]

Progressing digitization and ubiquity of computers are a strong sign that the next decade will bring exponential rise in the amounts of data sent across the global network. Availability of that information on the go will also increase. Year 2009 was the first in history, when laptops outsold PCs. This trend is followed by the education sector, which continuously expands wireless infrastructure.

It is worth mentioning that open source, often free software can be successfully used in university campuses to manage network, operating server and client computers, applications. The administrator should pay attention to the amount of time needed to install, setup and maintain such software. Those factors will affect the TCO and ROI.

References

1. Cisco Systems, Enterprise Campus 3.0 Architecture: Overview and Framework. http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html
2. Cisco Systems, Cisco NAC Appliance (Clean Access), http://www.cisco.com/en/US/products/ps6128/index.html.
3. McPherson D.,Dykes B., VLAN Aggregation for Efficient IP Address Allocation, RFC 3069.
4. Teare D., 2004, CCDA Self Study: Basic Campus Switching Design Considerations Sample Chapter is provided courtesy of Cisco Press.

5. Bluecat Networks, The Market Leading IP Address Management (IPAM) Solution, http://www.bluecatnetworks.com/ip-address-management-dns-dhcp-solutions/ip-address-management-ipam.
6. Cisco Systems, 2004, Designing Cisco Network Service Architecture, Cisco Training and Certification, part 1 and 2,