Bachelor Thesis in Computer Network Engineering

Network Admission Control (NAC)

Securing end point devices

By

Yusuf Adewale
Vilhelm Wareus
Jerry Lartey

2010-06-11

Supervisor: **Pouria Taslimi**
Examiner: **Nicolina Manson**

School of Information Science, Computer and Electrical Engineering
Halmstad University

Table of Contents

PREFACE **5**

ACKNOWLEDGEMENTS **7**

ABSTRACT **9**

1 INTRODUCTION **11**

1.1 Application area and motivation 12
1.2 Problem 13
1.3 Idea or approach chosen to solve problem 14
1.4 Thesis goals and expected results 15

BACKGROUND **16**

1.5 Endpoint security attacks 18
1.6 Current solution and best practices 20
1.7 Problem improvement potential 20
1.8 Project Scope and Limitation 20

NAC AS AN ENDPOINT SECURITY SOLUTION **22**

1.9 Why is NAC important? 24
1.10 Functionality and Features of IEEE 802.1X (NAC) 26
1.11 Dynamic VLAN Assignment 27
1.12 Extensible Authentication Protocol 28
1.12.1 EAP with Transport Layer Security (TLS) - EAP 28
1.12.2 EAP - MD5 28
1.12.3 EAP TTLS 29
1.12.4 EAP PEAP 29
1.12.5 LEAP 29

NAC IMPLEMENTATION WITH THE VENDORS **30**

1.13 Cisco NAC 31
1.13.1 Cisco NAC Appliance 31
1.13.2 Cisco NAC Framework 33
1.14 Microsoft NAP 35
1.14.1 NAP Overview 35
1.14.2 NAP infrastructure benefits 36
1.14.3 NAP enforcement 37

INTEROPERABILITY **41**

1.15 Cisco NAC and Microsoft NAP 42

RESULTS **46**

1.16 Enforcement of security policies 46
1.17 Implementation Document 48
1.17.1 Planning of Network Access Control 48

CONCLUSIONS OR SUGGESTIONS TO FUTURE WORK.....52
GLOSSARY OF TERMS.....55
REFERENCES 57

Preface

As organisations gets hungrier for the protection of their network, equally so has the need for the protection of end users. In recent surveys, end users have been repeatedly identified as potential threats to network security. Our thesis work addresses Network Admission Control (NAC) and how it can be a vital solution in network security.

This thesis is organised in 7 chapters plus a glossary of terms and an appendix.

Chapter 1: Introduction – In chapter 1, we introduce the problem that our thesis seeks to solve. We also talk about the approach we are using to solve the problem as well as thesis goals and expected results.

Chapter 2: Background – In chapter 2 we introduce network security threats facing any organisation. We further talk more specifically about endpoint security threats. The chapter also explores current solutions and best practises, problem improvement potential, and finally ends with the scope and limitation of our thesis.

Chapter 3: NAC as endpoint security solution – Chapter 3 talks about the depth of NAC and why it really should be given a second look. NAC features, policies, standards and protocols

Chapter 4: NAC implementation with the vendors. This chapter explores NAC implementation with different features and finds out their strengths and weakness, haves and have not's.

Chapter 5: Interoperability – This chapter is centred on interoperability of different NAC vendor solutions and the benefits of interoperability. It has an insider look into some specific vendor interoperability approach.

Chapter 6: Results – This chapter contains reports of all finding for this thesis work as well as possible outcomes.

Chapter 7: Conclusion and suggestions to future work – This is the last chapter of the thesis. It contains our conclusions after thoroughly investigating NAC and suggestions for future work.

Reference: The lists of references to research material, we used.

Acknowledgements

A rewarding experience of course is the opportunity given us as students of Halmstad University especially at the IDE department that is committed to producing fully qualified network professionals. We give thanks firsts to almighty God for giving us health and strength throughout our study period.
Since we began our study in the BSc. Network Engineering program, many people have given us invaluable help and have been quite influential in shaping our career paths as Network Engineers. We are very grateful to Nicolina Manson, study director of the BSc. Network Engineering Program, whose generosity, and enthusiasm has made this BSc. Program a reality. We would also like to thank Mr Pouria Taslimi, our thesis supervisor who provided us with fantastic project coordination, excellent ideas and suggestions and an unending patience as we worked together to produce an excellent thesis work.

We further want to say a **BIG THANK YOU** to everyone who has been helpful. Also thanking IDE department, student colleagues, laboratory assistants, and all who wished us well.

Special thanks also go out to:
Malin Borhager
Olga Torstensson
Ola Lundh
Annette Böhm
Kristoffer Lidström
Mattias Wecksen
Yang Wang
Torben Svane
Jasper Hakeröd
Mikhail Nechaev

Abstract

There have been remarkable growths in wireless communication networks in recent years; this is because of its merits over the wired networks such as Mobility and convenience. Wireless networks transmit the signal over the open air via radio waves of different frequencies, this makes it to be vulnerable to several attacks and anybody on the street can easily intercept the wireless data or inject new data into the entire network. There has been existence of wired equivalent privacy (WEP) protocol (IEEE 802.11i), which was designed for wireless network security. There were concerns of security vulnerabilities in WEP; this made it necessary for the implementation of another solution to overcome the weaknesses of the previous wireless network security. The IEEE 802.1X (port-based network admission control) which is defined on Extensible Authentication protocol (EAP) provides effective and efficient admission control to wireless and other networks devices [8].

Our thesis investigates the efficiency of NAC (IEEE 802.1X) as a security solution, access different vendor solutions, protocols supported and look into the inter-operability of these various vendors. In as much as we support the premise of NAC being an excellent solution, we will also make brilliant recommendations in this thesis to be considered for future refinements of this security solution as well as deployment scenarios for the university network.

1 Introduction

There is growing concerns of the security overview of the computer network. A lot of issues has arisen lately which seek to question how the network can be protected from vulnerable external endpoint connecting devices like laptops, handhelds and quite recently mobile phones that is connected on a daily basis to the cooperate network.

How do we keep track of the security compliance of these devices?
Is our security policy comprehensive enough to cover the compliance of these endpoint devices?

In an attempt to overcome the vulnerabilities of the wireless network, there was an introduction of the wired equivalent privacy (WEP) protocol; this was published by IEEE in 1999 as the security component of 802.11b. WEP has a number of security deficiencies, since there are numbers of WEP cracking software tools available, such as WEPCrack, WEPlab, AirCrack, WEPAttack and AirSnortb etc. There was need for more secure alternatives.
In response to weaknesses of WEP, there was a subsequent introduction of Wi-Fi Protected Access (WPA) protocol; this was published by Wi-Fi alliance in 2003 in order to correct all the security flaws found in WEP.
IEEE 802.1X was subsequently developed to address the security issue in Wireless Local area Network. As a port based network access control, its functionality based on three entities namely Supplicant, Authenticator and Radius server and it uses EAP or EAPOL (Extensible Authentication Protocol over LAN) as the protocol.

The underlining objective of this thesis is to investigate IEEE 802.1X as a fitting security solution, its deployment and maintenance into a specific network. Another objective of this thesis is an investigation of the interoperability of NAC products from different vendors, and the different protocol supported by each of these vendor products. According to some research published on IEEE database about 802.1X standards, some vendors have added proprietary extensions to their commercial 802.1X clients, this poses a challenge to interoperability since theses extensions do not always work with other 802.1X systems.

We compare the protocols used in the implementation of IEEE 802.1X by different vendors including Cisco Systems, and Microsoft NAP networking among others.

At the end of it all, we put across some recommendations based on our research into the issue and what it takes to get it improved in terms of standardization and interoperability.

1.1 Application area and motivation

Organisations today store large amounts of data and information in their networks. These data ranges from important company management information to customer records. These always make organisations targets, and exposed to numerous security threats like unauthorised access which always have profound consequences and degrading effects on organisational networks. Endpoints systems add up exponentially to the threat level of organisational networks.

With the emergence of the dynamics in the internet and the adventurousness of users within the network however, security concerns have been an issue and a topic for many a discussion and forums. With the increase in the number of users using their laptops and other handheld devices such as internet phones, PDAs and home entertainment equipment to connect with the network, it is very likely that the introduction of viruses, worms, backdoors and spyware into corporate networks may stand as a threat to the entire network infrastructure.

It is very apparent that traditional security strategies and mechanisms used to protect the wired network architecture of the company may not be enough to protect and combat the security scenarios posed by bringing personal systems like laptops into the network. This is because the existing security only checks for authentication and secured login situations but does not check if the endpoint system has the latest updates and patches for antivirus programs and operating systems. This is why NAC is an interesting point for discussion.

The application area for NAC is within the LAN environment of an organisation whereby the organisation seeks to protect its boundaries since they are always exposed to the security threats caused mainly by their mobile users. NAC addresses these concerns through a couple of all inclusive steps including;

User Identification: This checks who the endpoint user is? What is the role of this user in the context of the user? Finally but not the least, what rights the user has?

Compliance: This state also seeks to check if the end point complies with established security policies of the organisation. For example, checking if endpoint user has the latest virus definition for its anti-virus program. Compliance also checks if endpoint user has update version of operating system, from where the endpoint is attempting to access the organisational network and which resources the endpoint is trying to access etc.

Enforcement: This addresses how the compliance policies are enforced. For instance how is non-compliant endpoint systems remediated, how systems that cannot be checked for compliance treated etc.

The motivation area for this particular topic was a result of several consultations with our programme director Nicolina Manson with regards of the security concerns of the school network and the need to provide a unified real-time security solution for the network since most students connect to the schools network via their laptops. This particular scenario is a general concern shared by many organisations and after a couple of deliberations however, we both agreed to work on this topic since it will go a long way to help address the security needs of organisational network security as well as college and university campus security of which Halmstad is not an exception.

1.2 Problem

In today's network environments, connectivity is very widely stretched. Users can connect their devices at any connectivity outlet or access point and begin communicating with servers and other network resources. In the long run most of these endpoint devices end up being ideal conditions for compromise which puts the organisational security at risk. These risks range from unfortunate to even catastrophic events that can bring down the entire

network of an organisation. Halmstad University is a classic example. With majority of students connecting to the school network via laptops and quite recently mobile phones, iPads and PDA's the increased risk of compromising the school network has been heightened since these devices may have been at different places before joining the school network at a point in time. This poses a major problem to the school network in terms of threats and a way of introducing vulnerability into the school network.

1.3 Idea or approach chosen to solve problem

There are a myriad of security solutions that intends to cure the problems in today's networks. In this thesis however we have chosen NAC as a unified solution.

NAC comprises two areas. These are pre-admission and post-admission. Pre-admission addresses authenticating the endpoint and its health status at the time of connection while the post admission phase deals with the enforcement of the security policy whiles endpoint is granted access on the network. NAC covers:

User control

Organisations need to identify users that connect to the network and use resources.

Endpoints user access needs to be strengthened using authentication procedures

What resources is the endpoint allowed to access?

Compliance

0 What antivirus endpoints are using and the version?

1 From where is endpoint attempting to access network.

2 Check if endpoint traffic contains any Trojans, malware viruses, worms etc.

Enforcement

How is policy enforcement conducted?

How non-compliant users are helped to re-mediate

How is inaccessible endpoints handled

1.4 Thesis goals and expected results

Our goal for this thesis is an investigative analysis of NAC, standards, various vendors' deployment of the NAC security solution as pertaining to the University College or educational network. Our expected results for this assignment are an outlined policy statement for consideration when deploying NAC security solution in Halmstad University or any other college establishment. We also present findings of industry standards and recommendations related to the NAC security solution.

The main purpose of securing a network is to ensure that the users have freedom to enjoy the network without having fear of losing or compromising important and expensive individual and organization data and resources.
Therefore, an organization network security needs to protect network computers and secure the electronics data, both in transmission over the public internet and in storage within the computer systems and storage devices.
The following are few of common attacks on end users and the networks in general.

***Denial of service attacks (DoS)*:** The main concept of denial of service attacks is to deny or block the legitimate user of their access to get the services they normally get from servers. In most of the time, such attack will force the target system to process a large number of irrelevant processes in an attempt to consume most of its resources. If the attack is targeted to a group of systems distributed in the internet, such attacks may be referred to as Distributed denial of Service **(DDoS)**

***Malicious software*:** These are the programs or software**,** with tendency of harming computer systems. Malicious software can also be referred to as malware. The following are the list of the common malicious software. Trojan horses, virus, worm, logic bombs, backdoors and spyware.

***Identity spoofing*:** In identity spoofing, an attacker can impersonate the authentic user without using he/she login information. The lists of common identity spoofing are including software exploitation attacks, message replay, network spoofing and man-in-the-middle attacks.

***Password sniffing*:** This is the collection of software programs that basically used to capture remote login information, such as user name and user passwords. In some network applications like Telnet, FTP and SMTP. Users are required to use their passwords and usernames for authentication. This may make it possible for password sniffers to intercept the user login information.
There is possibility of encrypting the login information with the use of a program such as SSH in order to make the sniffing of the password difficult.

***Password guessing*:** In guessing, an attacker may be lucky to illegitimately get a password, as this is one of the easiest ways to acquire a password in an unauthorized way. This may happen if a user or administrator forgets to change a default password or is using a very weak password.

***Eavesdropping*:** In network and computer communication, eavesdropping is one of the oldest methods of stealing information; this will allow an attacker to intercept electronics data from network traffic. This can be achieved with the help of packet sniffer, which analyze and monitor the network traffic. The two most popular used network sniffers are TCPdump and Wireshark and these soft wares are available for free download from their respective websites.

***Intrusion*:** This is a situation whereby an unauthorized person, that is, an intruder, gains access to computer network.

***Cyber terrorists*:** Terrorists are the extremists that do not hesitate to destroy public properties and innocent life. Cyber terrorists use computer networks and technologies to carry out attacks on targeted places and equipment.

1.5 Endpoint security attacks

There is growing concerns to where endpoints connect to outside the organizational network. There is also a growing concern in the kinds of threats these endpoints such as laptops, PDAs and mobile devices might introduce to the organizational network.

Endpoints can cause havoc to a network with their infected device, these devices can be removable storage outlets. IPods can introduce viruses, worms Trojan horse, spyware and other forms of threats that can degrade a network and cause extreme problems towards an organization.

The threats of endpoint security are increasing and organizations need to protect their networks from exposure, and hence, in order for organizations to protect their networks, organizations must first determine the kinds of threats and kinds of practices as well as policies that can limit the amount of attacks.

There are a number of attacks that can take place within the endpoints activity and new threats are ever increasing.

Attacks such as viruses, malware, and Trojan horses are a common threat to a network that can be stopped easily by antivirus and antispyware software's to stop spyware and root kits but can cause problem ones these software's are disabled.

The main threats endpoint devices pose to a network includes;
***Non-compliant endpoints*:** This is whereby policies are in affect yet, there are still vulnerabilities due to system patches and fixes which have not yet been installed or applied. Thus security threats/attacks are still likely.

***Antivirus issues*:** This is a problem that can have serious effects toward a network, this deal with hosts or administrators disabling the antivirus software, hence the antivirus does not update in time or applied the scheduled scans delaying virus identification.

***Endpoint security agents*:** Third party agents are a typical problem in endpoint security. This problem deals with different types of solutions toward endpoint security leading to conflicts between security policies which can reduce the integrity of the network.

***Peer-to-peer applications*:** Within a network, peer to peer connections are major security concern in endpoint security. These applications allow outside traffic to gain access to an organization's internal network. An example of these applications can be torrent downloads.

***Mobile computing*:** Remote access into the network as in telecommuters is also a growing threat that can cause security awareness. Smartphone's are also in this category and need to be addressed to meet the necessary security trends.

***Unknown threats*:** In today's environment, new and sophisticated threats are increasing due to stealth based and silent attacks. Average antivirus

programs alone cannot manage to stop these attacks. New technologies must be enforced.

1.6 Current solution and best practices

Having presented the threats we will want to say that, there are equally current practises that helps in fighting these security attacks.
The entire network infrastructure has different approaches in combatting different problems. Some of these solutions include the following:
Firewall
Antivirus
IDS
IPS
VPN
NAT
Email security
SSL
HTTPS
Our best bet for endpoint security solution however is a NAC solution. This is true since it seeks to provide a unified solution integrating other independent security solutions since it seeks to provide a unified solution integrating other independent security solutions.

1.7 Problem improvement potential

Most of the solutions and best practises mentioned in 2.2 work in isolation. Many vendors have come up with fantastic solutions but unfortunately most fall short of providing a unified and interoperable security solution for the network infrastructure.
It is quite interesting to find out that NAC has the potential of providing a unified security solution for these endpoints that connect to the network. We will get into the details of NAC in chapter 3.

1.8 Project Scope and Limitation

As we have discussed prior to starting this thesis with our program director Nicolina Manson and our thesis supervisor, we have agreed that this thesis is

confined to issues pertaining to the university network. It does not cover the implementation face of the NAC in a production environment due to time constraint and availability of equipment. We will investigate NAC; IEEE 802.1X in terms of its deployment issues in the University Network, and investigate on vendor's interoperability, protocols employed by each of these vendors and the limitation of NAC.

NAC as an endpoint security solution

We believe that at this point on, anyone who has looked into our thesis will have a fair idea of what (NAC IEEE 802.1X) is. For the records, however we will like to delve into why it really makes the cut as a security solution.

Network Access Control (NAC) as a security solution does not have one universal definition. There are a couple of definitions that has been curled by various technology experts, developers and vendors alike. However a standard NAC security solution has some defining attributes that makes it complete and we will like to outline here below these characteristics.

Integrity of endpoints*:* Endpoint integrity is one of the issues that NAC seeks to address in terms of providing security. An end point here may be an employee's laptop used in telecommuting, PDA devices that connect to the cooperate network and other portable devices. This is a major deployment component of NAC in that the NAC deployment checks the integrity of any endpoint seeking to connect to the network to make sure that the endpoint in question meets all baseline security controls and access control policies.

0

Organisational security policies*:* Security policies form the heartbeat of any organisational network infrastructure and so does it in nearly all NAC solutions. An organisation can customise its security policy or use a security policy template to define its security policy needs. Either way, a good NAC solution should be able to integrate an organisational security policy into its deployment or all together be able to accommodate one that has been created from scratch.

Health assessment checks: Assessment checks vary from various NAC solutions. Some NAC solutions will do basic check to verify if endpoints have loaded specific applications and whether these applications have been enabled. Other NAC solutions will delve a little deeper with their checks by looking up attributes like version numbers, last scan time and whether endpoint has real-time monitoring enabled. From our view point, a good and standard health assessment check for a NAC solution is a solution that has the capability of performing an extended assessment check. This encompasses checks like operating system checks, certificates, applications, files, MAC addresses, registry and open/closed ports, and IP addresses and the like.
A first check, allows for a health check performed on the endpoint before it is granted access to the network. The second provides a health check on the endpoint after it has been granted access on the network. These two checks combined hopefully provide a comprehensive security.

Endpoint identification: Endpoint identification is the process by which an endpoint system is identified by the network as it initiates a connection request. A NAC solution should be able to detect an endpoint initiation attempt in order to profile the endpoint against the admission control policies in place within the organisation. The endpoint can be identified in a number of ways and at different layers of the IP stack. These ways include DHCP requests, Address Resolution Protocol (ARP) request, and endpoint agents.

Authentication: This is the ascertaining of the claimed identity of an endpoint or resource. A NAC solution should be capable of integrating endpoint users into the network. Authentication methods in use include, 802.1X, IPSEC, VPN and HTTPS solutions.

1.9 Why is NAC important?

NAC has become a force to reckon with on the world stage of security in that it provides consistent network access control capabilities for today's diverse and dynamic user base. It is very interesting that major strides have been made in the standardisation of NAC. Just this May 24th 2010, the Network World [2] published that at long last there NAC wars is over and that there has been truce. In February 2010, the Internet Engineering Task Force (IETF) [16] approved 2 standards as proposed by Trusted Computing Group (TCG) [17] and is now considered as 2 NAC standards as RFCs which will be used as a guideline for implementation within the industry. These RFCs are RFC 5792 and RFC 5793. This is a remarkable achievement since it is bringing closure on the "NAC War" by various vendors in term of what is a standard and what is acceptable.

Trusted Computing Group (TCG) is an industry standards group with over a hundred active members. TCG creates industry standards for secure computing. Among its acknowledged standards it's created includes Trusted Platform Module (TPM), Trusted Network Connect (TNC), and Self-Encrypting Drives (SED).
Internet Engineering Task Force (IETF) on the other hand is an open international community of network designers, vendors, operators, and

researchers with over a thousand members. The IETF creates standards for the internet. Among the remarkable standards of the IETF is; Internet Protocol (IP), Transmission Control Protocol (TCP), and Transport Layer Security (TLS)
The IETF agreed upon TCGs TNC standard for NAC due to a lot of peer reviews by the IETF's Network Endpoint Assessment (NEA) Working Group. It came out that TCGs TNC standard for NAC perfectly met the standardisation requirement by the IETF therefore it was rational for IETF to adopt it rather than developing separate and different standards. In this way both customers, vendors and developers are confident of these standards knowing that it has been reviewed and widely accepted by IETF's professionals.
The approved NAC standard provide 2 capabilities like have been mentioned earlier.
Ability to check the health (security posture) of an end point and grant appropriate level of network access. This corresponds to IF-TNCCS 2.0, a standard protocol for health checking of endpoints.
Standard for basic health checks (eg. Spyware/malware status). This corresponds to IF-M 1.0.

Another important benefit that NAC offers is the reduction and prevention of zero-day and other similar attacks. This is achieved by the prevention of systems that do not meet up with the security standards as defined by the cooperate network. Examples of these systems that could be vulnerable are endpoints that lack anti-virus software, intrusion detection and prevention software, operating systems and upgrades. It not only check for the presence of these security software but also checks to ensure that end systems do have the latest virus definitions of antivirus, intrusion detection and protection have latest updates and also operating systems also have latest updates, patches and hotfixes. The NAC system will check the endpoints to ascertain if the endpoint systems meet up with these security baseline and then deny access to systems that are lacking any or all these security software. This is a preventive measure for the cooperate network since it reduces network's exposure to attacks and also reduces the risk of cross-contamination of other systems with worms and malware.

Added to the benefits that NAC provides is the enforcement of policies. NAC solutions allow that network administrators, chief network officers and system administrators have the possibility of defining security policies for the organisational network. NAC makes it possible for corporate network security policy to be integrated into the NAC solution so that the enforcement will be carried out by the network access devices.

Identity and Access management is another important feature of NAC. With generic network infrastructure access policy is done at the IP addressing edge but in an integrated NAC infrastructure this access policies is done with the identity authentication of users and endpoints. Since most generic network infrastructures do not associate identities of non-pc devices like IP phones, printers, and scanners it becomes over burdensome manually identifying, tracking and securing these devices across the entire network. NAC however makes it possible for automated identification and profiling of devices and further segmentation of these devices within the network based on security policies. This reduces IT staff overheard significantly.

We want to summarise here that there are a lot of mini extended benefits of NAC but upon our assessment and research we have identified the above benefits as those around which all the mini extended benefits evolve.

1.10 Functionality and Features of IEEE 802.1X (NAC)

In this section, we are going to discuss the main features and functionality of IEEE 802.1X and its three main components such as Supplicant, Authenticator and Authentication server. Since 802.1X can be deployed in both WLAN/LAN, we are going to use both Wireless access point (WAP) and Switch interchangeably.

In Wireless Local Area Network (WLAN) and LAN, Supplicant is mostly referred to as Mobile Node and endpoint respectively. The Wireless access point or Switch is referred to as Authenticator, while Authentication server resides in Authentication, Authorisation and Accounting (AAA), server such as RADIUS and DIAMETER.

In an attempt to gain access to the Network, there is existence of 802.1X port, which is an association between supplicant and authentication. The supplicant will send EAP (Extensible Authentication Protocol) packet to Authenticator through the port that connects them together, in order to request for acceptance into the network. The Authenticator control port is in unauthorised mode, that is, it is opened. Authenticator (WAP) will pass the identity of the Supplicant to the Authentication server and AS will verify Supplicant identity and subsequently grant it permission if Supplicant is successfully authenticated. The AS decision will be passed across to Authenticator and AP will then inform endpoint by close the control port and Supplicant will be subsequently admitted into the network.

The diagram in figure 3.2a is the overview explanation of IEEE802.1X functionality.

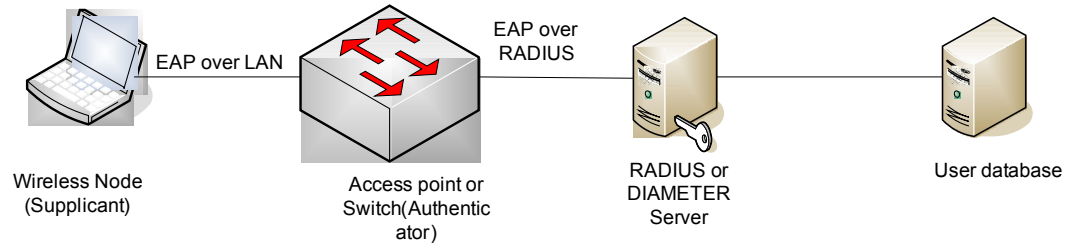


Figure 3.1 Supplicants, Authenticator and Authentication Server

1.11 Dynamic VLAN Assignment

One of the most important features of IEEE802.1X is dynamic VLAN assignment, this works according to Organisation defined policies. Though, this VLAN assignment is not part of IEEE802.1X specification, but it has been implemented by most vendors in an attempt to subject a particular user to a specific VLAN in accordance to the organisation policy. This typically works by checking which VLAN will be assigned to a particular switch port. This decision will be taken base on the privilege given to the user logging to the system. For example, in the case of an educational institution like Halmstad University, a Student logon to the network may be assigned to Students VLAN, the University researchers and other members of staff may be assigned to Staff VLAN, while the guest to the university could be put on guest VLAN. VLAN3 in figure 3.3 bellow is an example of dynamic assignment.

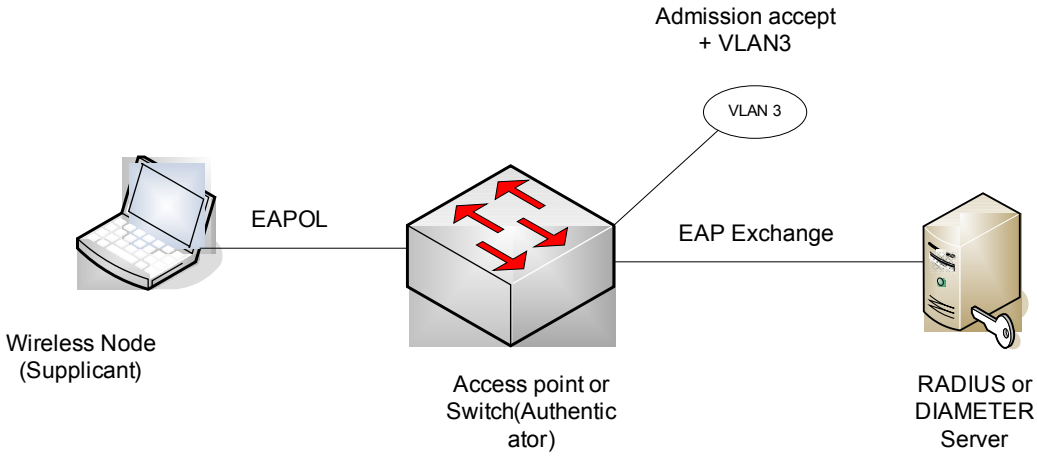


Figure 3.2 IEEE802.1X dynamic VLAN assignment

1.12 Extensible Authentication Protocol

In this section, we will like to briefly discuss EAP (Extensible Authentication Protocol) as an Authentication framework that support multiple Authentication methods. EAP is frequently employed in Wireless network and point-to-point connection. EAP or EAPOL (Extensible Authentication Protocol over LAN) as the protocol used in NAC-IEEE 802.1X implementation. We realised that our thesis cannot be completed without having a brief discussion on EAP.

We will discuss the various types of Authentication that are currently available in practice today for wireless LAN.

1.12.1 EAP with Transport Layer Security (TLS) - EAP

TLS is considered to be the strongest and the best of all the EAP methods around, it requires Public Key Infrastructure in order to allow mutual authentication between both Client and Server. EAP-TLS has a connection with SSLv3.0 Secure Socket Layer version 3.

1.12.2 EAP - MD5

This is referred to as EAP with Message Digest 5, it makes use of MD5 for authentication, and this method is potentially vulnerable to security threat

because it can only authenticate Client to Server not in the other way round. Therefore it is considered as weak EAP methods.

1.12.3 EAP TTLS

Extensible Authentication Protocol - Tunnelled Transport Layer Security is supported and primarily developed by funky people and certicom, it can be deployed easily due to the fact that it only require server-side certificate for sever Authentication, the Client side can employ the Extensible Authentication, such as traditional Microsoft logon User ID and Password for Authentication. This EAP method is regarded as secured because it tunnels user credential inside the TLS tunnel and it avoids the difficulties of using PKI (Public Key Infrastructure) in the client side.

1.12.4 EAP PEAP

Extensible Authentication Protocol-Protected Extensible - PEAP was developed as a result of joint research between Cisco, Microsoft and RSA, it is very similar to EAP TLS in operation. It require server side certificate only and it also tunnels user credential over tunnel. It provides a strong security and can be easily deployed in window environment.

1.12.5 LEAP

Light Weight Extensible Authentication Protocol; This is an Extensible Authentication Protocol that was developed by Cisco (Cisco Proprietary), it is majorly used for Cisco Wireless Local Area Network equipment. It supports mutual Authentication and dynamics per-user, per-session of WEP encryption key. LEAP considered being vulnerable and there is availability of LEAP hash cracking tools such as ASLEAP.

NAC implementation with the vendors

1.13 Cisco NAC

As a major player in the networking and data communication world, Cisco has not been left behind in the 802.1X race. Cisco also has its flavour of this security solution which it has branded Cisco NAC or CNAC. Cisco claims that it has the best NAC solution and explains how security is addressed with its NAC solution. Cisco announced its CNAC in 2004. Cisco's approach to network admission is integrated into the network architecture whereby there is support for industry level standards such as Extensible Authentication Protocol (EAPOL), 802.1X, RADIUS as well as hundreds of third party industry vendors such as anti-virus, IDS, IPS, and malware support providers. Cisco is in fact part of the team championing the course for a standard framework for NAC as it works with the Internet Engineering Task Force (IETF) to achieve these objectives.

At the time of writing our thesis, Cisco has two implementations of NAC. These are the ***Cisco NAC Appliance*** and the ***Cisco NAC framework***.

1.13.1 Cisco NAC Appliance

The Cisco NAC appliance was previously known as the Cisco Clean Access. This variant of NAC by Cisco offers an all in one solution for endpoint assessment, remediation, policy enforcement and management all in one box.

Cisco recommends this solution for initial NAC deployments especially when starting on a clean sheet. However it is just a recommendation and that should not be taken as the gospel truth but rather an IT manager should look into the needs of his organisation to see if it will meet its organisational needs.

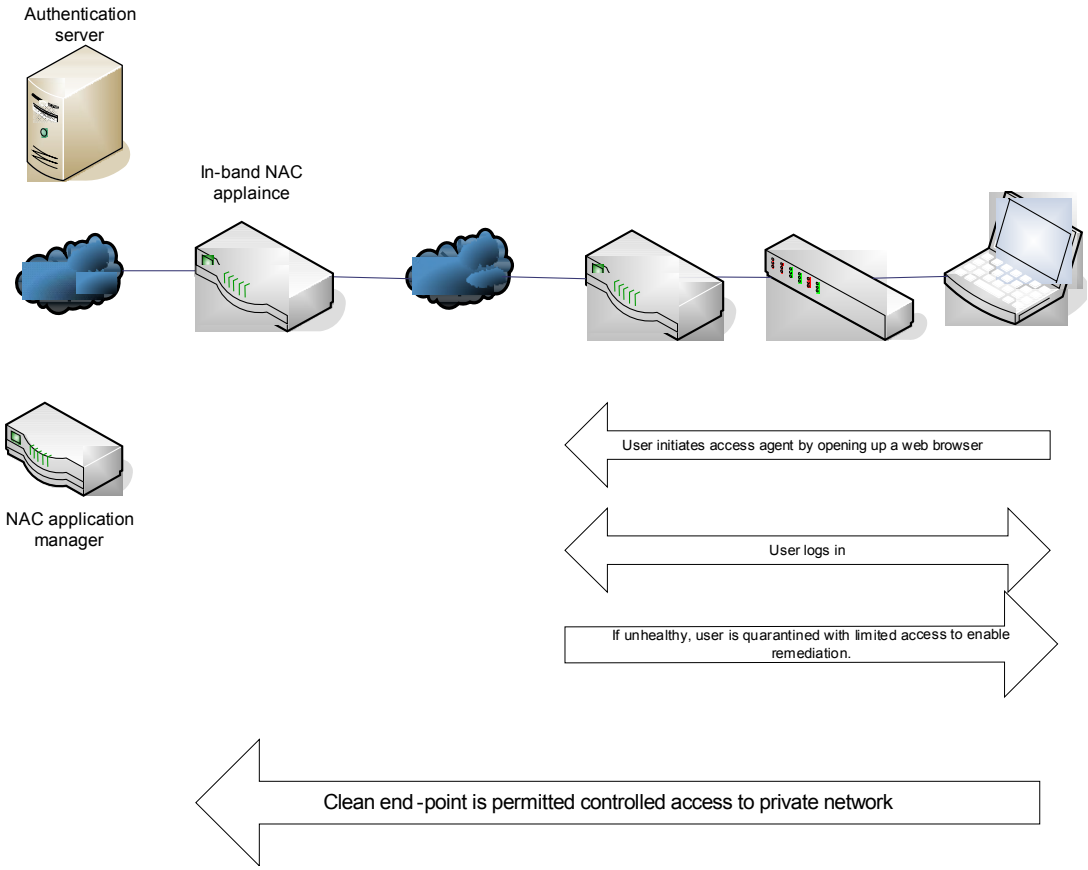


Figure 4.1 Communication flow of Cisco NAC Appliance

Like we have mentioned, the CNAC appliance is a pretty much simplified implementation of 802.1X. It is rather security feature packed and has both in-band and out of band deployment options. As a box, the CNAC Appliance is centrally managed; handling issues like security, access and compliance policies unified rather than spreading it across different devices within the network. The features of CNAC Appliance include user authentication, policy based filtering, and client posture assessment and remediation.

The components that make up the CNAC appliance include:
Cisco Clean Access Agent (CAA). The Cisco Clean Access Agent is an optional window based read only client that resides on the client endpoint. It authenticates the user, and scans for required patches, operating system updates, AV updates prior to being granted access to the network. We want to state that there are agents both for Windows and MAC clients.

Clean Access Manager (CAM). The Clean Access Manager is a secured web console which is responsible for the administration of the CAS. It is capable of administering up to 20 CAS servers or even 40 CAS servers for SuperCAM deployments.

Cisco Clean Access Server. (CAS). The Cisco Clean Access Server is the enforcement server that enforces all the security policies that has been set in the CAM by the system administrator. It interfaces with various third party vendors' policy servers to determine if an endpoint is fit to be allowed access to the network. These third party products include antivirus servers, audit servers and vulnerability management servers. The CAS has the tendency of ensuring authentication as a RADIUS server thereby interfacing with for instance Microsoft Active Directory or LDAP to ascertain whether the user has valid credentials to access the network.

1.13.2 Cisco NAC Framework

The Cisco NAC framework which is the latter of the two NAC deployment of Cisco holds for networks running on 802.1X. This is especially useful when there is the need for interoperability and integration with other vendors as well as scalability needs since the NAC Appliance solution does not particularly scale well. Cisco has published on its website as well as other promotional materials that the NAC framework architecture supports a myriad of devices used in a practical network environment as well as collaboration with over 100 third party security vendors. With the CNAC framework architecture, an endpoint is required to send its authentication credentials and its posture to a specified system responsible for that task, the responsible systems then checks it for clearance before it is granted access to join the cooperate network. This shares some significant resemblance with the 802.1X port based access control standard. These core characteristics like we have said, enhances and simplifies interoperability. Since it uses the same 802.1X illustration diagram, please refer to diagram at fig 3.2 for reference.

To function well, the CNAC framework has a couple of components that makes it tick.

***Cisco Trust Agent*:** This is an agent that resides on the endpoint device and gathers user credentials, authentication information and security posture for CNAC.

Cisco Network Access Devices (NAD): The NAD is basically a switch with 802.1X capability. It is the main point of access to a client. In other scenario's, the NAD can be a wireless access point, VPN concentrator, or even a router.
Since the NAD is the point at which the client uses to get gain access to the network, it is important that the NAD is 802.1X complaint in order to enforce endpoint posture checking.
Cisco AAA policy Server: Authorisation, Authentication and, Accounting (AAA) is the means of whereby endpoints are required to authenticate before getting the right credentials to access the network as well as tracking users for resource consumption. The Cisco Secure Access Control Server (ACAS) is the AAA policy server in this framework. It takes care of all policy decisions within the NAC framework as well as determining endpoint posture of connecting devices. It is the policy system that enables the Cisco NAC to support 802.1X network authentication. It uses the Host Credential Authorisation Protocol (HCAP) to communicate in a multivendor fashion. It can also use TACACS+ as the cisco proprietary or RADIUS but both cannot be implemented at the same time.
Cisco Security Monitoring, Analysis, and Response System (MARS): As can be seen above all these components are Cisco proprietary which raises the question of interoperability. This is where Cisco and Microsoft came up with a union NAP/NAC that seems to address issues with portable devices like PDA and smartphones. We will like to quickly comment here that this union only can be realised with Microsoft systems using Server 2008.
As we have outlined in this chapter on Cisco and its NAC solution we can summarise here that a smaller organisation will go in for the CNAC appliance whiles a larger organisation will integrate the NAC framework whereby integrating 3rd party security ques.

1.14 Microsoft NAP

Network Access Protection (NAP) is the initiative of Microsoft Corporation, towards their contribution to the network access control with the main intention of keeping networks to be healthy. Roaming laptops are always the health threats to any network. While laptops are away from organisation, they might not receive the most recent software updates or configuration changes, these laptops might also have been infected by exposure to unsecure networks. Organisations always allow guests and consultants access to their network and the laptops and PDAs that these people bring may not meet the network requirement of the organisation and in view of this, it may present health risk to the entire network.
Also the desktop computers, which always physically present in the premises of organisation, can also cause health risk to the network through accessing websites and public accessible resources like files.

1.14.1 NAP Overview

Network Access Protection for window server "longhorn" is a new set of operating system components and protocol that provide an interactive platform for protected access to the network. The NAP platform provides an integrated way of detecting the state of network client that is attempting to connect to a network and restricting the access of the network client until the policy requirement for connecting to the network have been met. By using Network Access Protection, Network administrator can check the health of any laptops when it reconnects to the company network, weather by creating a VPN connection to the company network or by physically returning to the office. For visiting laptops, generally, administrators would not require or provide any updates or configuration changes.

The administrator may configure internet access for visiting laptops in the restricted network, but not for other isolated computer resources.
Regarding desktop computers, the network administrator can remotely check for the level of compliance in accordance to the organisation policy. Administrator can check log files to know what areas in which endpoints are not complied. NAP incorporated with the ability for automatic remediation, that is, one can easily configure NAP for automatic remediation in such a

way that NAP client component can automatically attempt to update the client computer when client is not healthy. In view of this, updates can be automatically made to non-compliant System and they will be provided with the most recent software.

It has to be remembered that Network Access Protection (NAP) does not designed to protect network from malicious users, it is designed to help administrators to maintain the health and complaints of the computer system on the network.

1.14.2 NAP infrastructure benefits

- Configure system health requirements for NAP client systems.
- Apply access enforcement such as monitoring procedures.
- NAP client systems can update themselves when connecting to the network to be/ stay compliant to the network policies.
- NAP minimize cost complexity by incorporate some functionalities that include the automation of client remediation, policy enforcement and easily adding new features.

The diagram below is the NAP Architecture that shows the various components of a NAP infrastructure, we will discuss these components below.

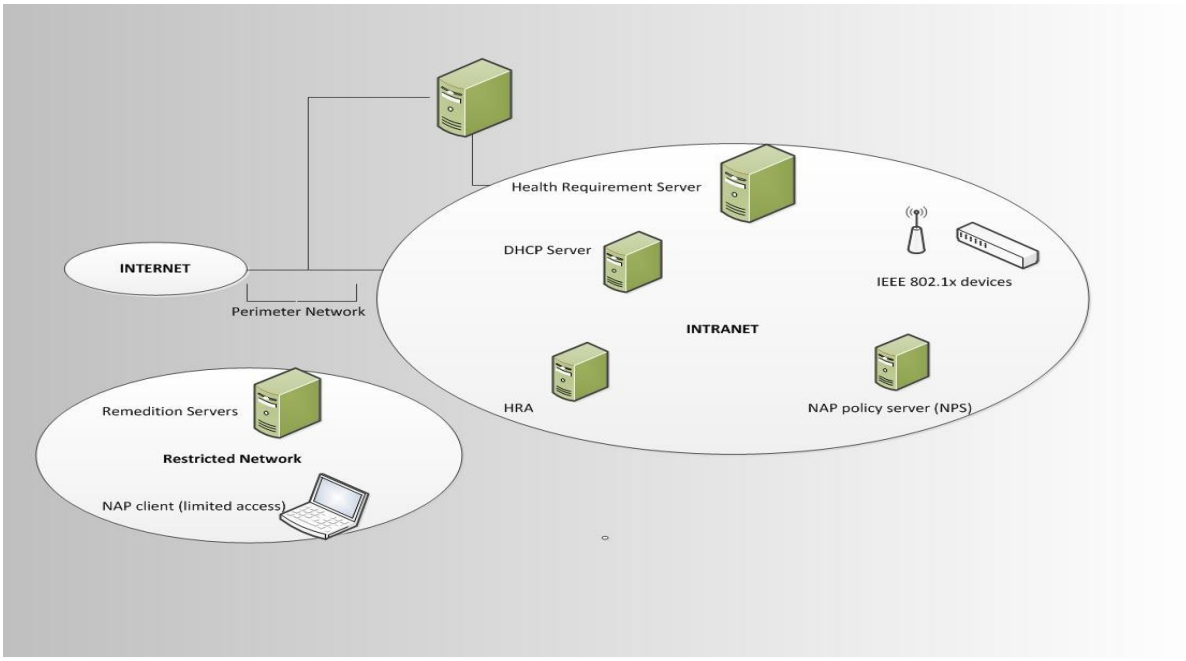


Figure 4.2 NAP infrastructure

"In respect to the vendors discussed prior to Microsoft NAP, some of the policies and names mentioned will/ or be mentioned again and will not be explained of its meaning such as the RADIUS protocol."

NAP client - The NAP client is simply a computer that reports its necessary system health to NAP enforcement point and then the enforcement point will then send the clients health status to the NAP health policy server for complete evaluation by means of the Radius protocol. These are client systems that support the NAP platform as in Windows Server 2008, Windows Vista, and Windows XP SP3.

NAP enforcement services - Enforcement services are devices that obtain health certificate and are typically 802.1x switches and servers that restrict network access after evaluation of a NAP client. Some examples of NAP enforcement points include VPN Servers, DHCP Servers and Wireless Access Points.

NAP health policy servers - These servers are health servers configured by administration that include the security settings and clients health requirements to enter the network. These servers determine the version or updates that are needed for installation onto the NAP clients.

Remediation servers - For noncompliant clients, remediation servers help in the process of correcting NAP clients in a logical subnet of the intranet which is the restricted network. Here NAP clients can gain access into the servers and install or update their systems before performing a new health evaluation.

1.14.3 NAP enforcement

We have talked about Network Access Prevention and what it is in general to enforce compliance with network health policies. We will now discuss how it enforces compliance.

NAP utilize utilizes four main different enforcement mechanisms. We will discuss and discover how NAP utilizes them to perform health variations and enforce network compliance. These are DHCP, VPN, 802.1x and IPSec Enforcement.

1.14.3.1 DHCP enforcement

DHCP Enforcement work where by the DHCP (NAP) Server cheeks the health of the client and if the client is healthy it will lease a valid IP address on which the client will be allowed to enter the network.
In the case of if the client is not healthy, the DHCP Server will lease limited IP addresses and a set of routes to Remediation Servers on a restricted network to provide updates and patches and perform other actions to bring the client to compliance state.
Once this procedure is finalized and brought to compliance state, the DHCP Server will lease full IP addresses and the client can connect to the network.

1.14.3.2 VPN enforcement

VPN enforcement works where by a VPN client tries to connect to the corporate network and a VPN Server cheeks if the client is healthy or not either by a Network Policy Server (NPS) or a RADIUS Server running Windows Server 2008. When the VPNs health is established and is correct, a VPN connection and the remote client are allowed to enter the network.
In the case if the client is not healthy; the VPN Server applies a set of packet filters that quarantines the client by letting it connect only to the restricted network where Remediation Servers are located. Once the client gets updated or patched, the VPN Server removes the packet filters from the client and the client can enter the network.

1.14.3.3 802.1X enforcement

This is done when an Extensible Authentication Protocol (EAP) - capable client device tries to connect to 802.1x capable switch on the network. The switch forwards its health status to the NPS to cheek if it complies with the policy. When its health is correct, the NPS tells the switch to open the port and

thus allowed to enter the network. Once the compliance fails, the switch closes the port and denies client entry or can be placed in a restricted VLAN where it is updated and patched. When the updates and patches are initiated and is compliant, it is allowed access onto the network.

1.14.3.4 IPSEC enforcement

IPSEC is simple and works by configuration on the clients IPSec policy for the devices to acquire health certificates. When configurations are done, Administrators set up Health Registration Authority (HRA) on the network which works together with NPS to issue x.509 health certificates to clients when they attempt to start IPSec- protected connections with other devices on the network.

Interoperability

From Wikipedia, Interoperability is a property referring to the ability of diverse systems to work together. In discussion of NAC however, we look at the term interoperability within the NAC domain as the ability of different NAC vendor solution providers to interoperate in harmony. As we said in chapter 3, NAC is a trend in security and as such many companies have joined the band wagon in producing NAC solutions. Already by 2007 there were a lot of players on the NAC market and even by 2007, Network world did an assessment of 13 NAC solution providers [2]. This clearly shows that there are many solutions on the marker and the need for these products to work with each other is very important.

When there is an established interoperable framework or standard in place, it will assist in organisations to be guarantee that any new technology or product they select will be able to seamlessly work with the already deployed products and services.

With interoperability in place, there could be cost savings since there will be the possibility of choosing from different vendors while at the same time being able to deploy a NAC solution which will meet the needs of the organisation.

Integration is another factor that is achieved in the case of interoperability. NAC is charged with integrating users, endpoints, and other network security related technologies. Some of these technologies that NAC should be able to integrate with are Authentication authorisation, and accounting (AAA), endpoint integrity and security, network policy enforcement and management, as well as quarantine and remediation. Overall, a NAC solution that encompasses industry standards usually will facilitate integration and interoperability of different or like technologies.

1.15 Cisco NAC and Microsoft NAP

We discuss about NAC and NAP in the interoperability section of our thesis due to the fact that it is a union which has proven to work well in terms of interoperability. We also found it prudent to discuss this combination since the school network is operating primarily on Microsoft endpoints. The plus for this combination is a solution that secures the endpoint perimeter with NAP and the network perimeter with NAC. The benefits of NAC and NAP interoperability as stated by Cisco and Microsoft include the following [5][3];

- Interoperability and customer choice
- Investment protection
- Single agent
- Agent deployment and update support

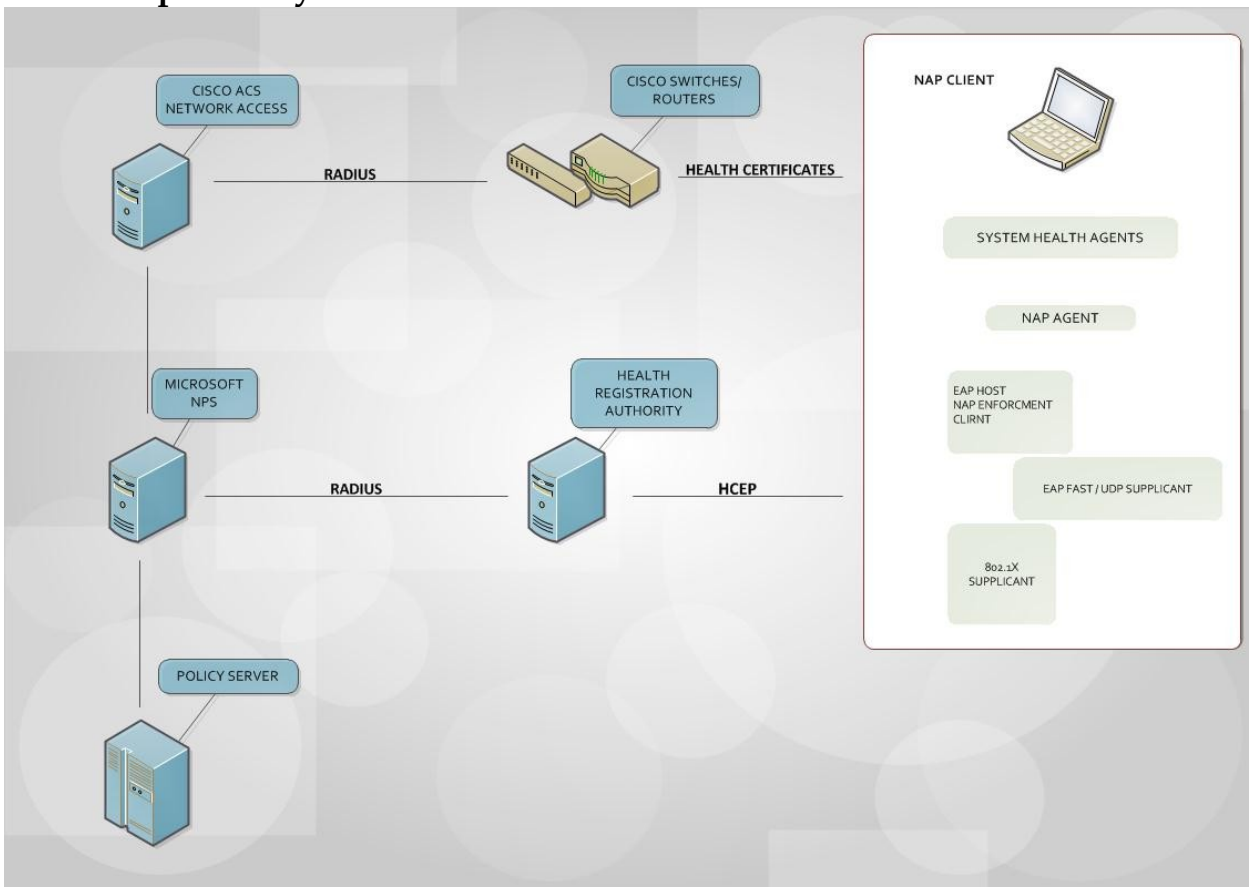
Interoperability and customer choice: NAC and NAP interoperability architecture allows them to work concurrently. The architecture supports the environments for NAC agents which is the Cisco Trust Agent and the NAP AGENT. As Cisco and Microsoft has cross-licensed the NAC and NAP protocols gives the university to use both software and equipment in the future for a combined policy product.

Investment protection: The investment protection plays a role in the future of the university network as the architecture enables the university reuse of their NAC and or NAP deployments. The university can use the NAP employment measures and integrate NAC into the network.

Agent: Endpoints which will run windows as their core operating system will include the NAP Agent which will be used for both NAP and NAC. As the university is currently running Windows XP, It will need to be run by Cisco Trust Agent for NAC and run the NAP agent for NAP.

Agent deployment: Customer experience and deployment issues for the agent interoperability will be similar as deploying as normal windows operating system services. Thus Services form Cisco will be distributed by Microsoft updates.

Interoperability Architecture



Above is a simple diagram to showing the architecture of the NAC and NAP interoperability. We architecture consist of the following;

- ***Microsoft NAP client***

  This is the NAP client computer that will be running windows operating system that will send health certificates.

- ***Cisco network access devices***

  These are network enforcement point devices which provide access to clients. Examples of these are switches, routers, VPN etc

- ***Cisco access control server (ACS)***

  Authorization of network access for the clients based on the identity and health statements. Grant appropriate access level.

- ***Microsoft network policy server***

  Performs validation cheeks and provides remediation instruction for clients.

- ***Microsoft heath registration authority (HRA)***

  Retrieves health certificates

- ***Microsoft policy server***

  Servers that provide health states for systems

For health validations to take effect, a list of SoHs will be passed to Microsoft NPS form NAP agents by the Cisco Secure ACS. In order for NPS to receive the list, it will support the Cisco Host Credentials Authorization Protocol (HCAP).

We found out from our research and it is worth mentioning that, the interoperability of CISCO NAC and Microsoft NAP is only limited to the NAC framework infrastructure. The NAC and NAP interoperability is only true when deploying or integrating into NAC framework architecture. At the time of writing this document the cisco NAC appliance do not support the NAC and NAP interoperability model so if you are using a NAC appliance, this sort of interoperability do not apply.
The reason though why an organization will deploy both NAC and NAP will be in the situation where they have infrastructure that supports IEEE 802.1X. Organizations can leverage Microsoft's directory services by using ***Active Directory*** to use single sign on in authenticating users. The endpoints within this infrastructure also runs Microsoft's NAP client as the agent that checks the health status of these endpoints and then the enforcement carried out by the network access devices like switches, routers and wireless access points which are all Cisco. As we previously mentioned the various components of the NAC and NAP framework we will not mention them here again but we say that the architecture works with these components.

In the case of Halmstad University, the school currently supports Microsoft endpoints and most students that connect their systems to the school's network have endpoints that are running Microsoft operating systems so this NAC and NAP interoperability scenario can be applied.

Results

In this section, we discuss the result of our research, which is based on a research paper published in IEEE database in consultation to a University presently deploying NAC appliances in Sweden (Kristiansand University College) and a University in United State (Virginia Commonwealth University) that have already deployed NAC appliances.

Kristiansand University College is one of the few Universities in Sweden that have deployed NAC appliances as at the time of this report in May 2010, we visited Kristiansand University to have a discussion with the network administrator in charge of their Network. He walks us across the network and he discussed with us some of the advantages of using NAC appliances some of the problem they are facing. This motivated us more to work on the problems that NAC technology is facing presently.

1.16 Enforcement of security policies

Since our thesis is majorly focused on NAC and IEEE802.1X deployment in University, we realised that in response to increasing population of Students and Staffs in and around University, and everybody both Students and Staff are willing to connect their Roaming PC to the School network, this will definitely compromise the security policies of the Universities and they have to define more requirement to secure their network from compromised. The following are the area which NAC is better than the past security techniques.

Post admission control: In most of the currently used network security techniques, there is no proper post admission control. Post Admission Control means monitoring of the Node or supplicants in the network after it is already admitted. NAC appliances can enforce pre-admission security policies and post admission compliance which is necessary to minimize threat to the network. This is one of the features of NAC that makes it better than most of the currently used technologies as listed in section 2.2 above.

Detection of compromise Students or Staffs: One of the features that can achieved in deployment of NAC technology is that if there are some Students trying to Share some copyright materials over the internet, with NAC appliances, such group of Student can be hacked down and located immediately. Contrary to the currently used technology whereby University have to investigate by tracking the IP address to a specific router and to the switch and someone has to be physically there to unplug such a person. And as we know this may take couple of hour to do.

Reduction of attack on School network: We realised that the total deployment of functional NAC appliances will relatively reduce the number of successful attack on School Network.

Full function in dynamic and heterogeneous environment – *NAC* can function effectively and efficiently in a dynamic and heterogeneous environment. For example in academic environment like Halmstad University, where there is a deployment of several operating systems such as Windows, Macintosh and Unix/Linux. Cisco NAC for instance, can provide authentication and post admission control for any operating system with web browser.

The following are the further result of deployment of NAC appliances;

- ✓ Extending of networking resources to virtually any remote user using a variety of operating system and application.
- ✓ Protect endpoint systems, data and internal resources
- ✓ Minimize IT support and operational cost, authentication and communication protection with a defined access policy control and
- ✓ Quarantine and remediation of non-compliant endpoint devices.

1.17 Implementation Document

We have extended our thesis to produce an implementation document of NAC into the Halmstad University network as per the advice of our examiner. This implementation can be used as a reference tool when deploying NAC into the network of Halmstad.

1.17.1 Planning of Network Access Control

1.17.1.1 Getting Started

When talking about NAC there are number of considerations and debates on where to enforce it. From our research and studies we believe the best practice to enforce NAC is at the network layer which is layer 2 and 3.
You have read already about the risks that pose without proper security of the network, having a good NAC solution must provide guests and personal working remote with controlled access to the network resources but doing this needs particular care as not disrupting the network, workers or having a burden to your help desk. The solution to this is that implementation of NAC solution should be done in stages to cancel out burdens or disadvantages that it can bring to the network.

The first stage should be the monitoring of the network environment. This includes gathering of vital information administration need and understanding exactly what is happening within the network. This is a great way to fully understand the network and find out what is really happing around the network and it is one of the greatest benefits that of NAC as IT staff can have a central view of all devices and security statuses of every devices.

1.17.1.2 Authentication

With the use of NAC we must still think about the authentication process of devices and the users. Wi-Fi is a booming technology used for access points to provide easy wireless access to networks but the main problem that it lurks is IT staffs do not implement the necessary security. In spite that WEP provides a reasonably secure alternative, companies and businesses use a shared password for all wireless access, thus meaning that individual users can not be

identified easily. A more secure way is to use an authentication that uses the persons own username and password when connecting with the network by use of WEP Enterprise.

As you may not be able to control all of what the employees or guest do in the network, you as an IT staff individual can win back control from mobile computing and implement policies that are far better to insure devices accessing the corporate network are controlled, healthy and in a secure state.

1.17.1.3 Deployment

In this chapter we will discuss the challenges in deploying NAC and the alternatives for LAN security within NAC.
In the NAC development phase, IT staffs are likely to encounter two or more challenges as in the impact it is likely to have on the network, the establishing policy fiasco and the scope of the initial deployment. The advantage is that you can gain a lot from the NAC deployment and reduce these challenges.
To fully understand the impact of Network Access Control on the network we need to look at the degree of change to the endpoints, devices such as switched, VLANs and ACLs. Reducing this impact to the network and still having control over users access on the LAN the greater the investment return from the deployment time prospective.
Example of this is some NAC devices that need cooperation from switched to enforce policy which intern need the latest update. Other solutions intern will need post admission control relying on diverting users into vlans that do not have the latest update to limit their access on the network LAN, by this administration must change the VLANs to support role-based segmentation and enforcement of ACLs.
The second challenge deals with the establishing the correct policies which is not subsidiary IT responsible. IT needs to work within the business sense to translate desired policies.
To cut the work load of this challenge the easiest way is to look at the NAC architectures that helps to ease the deployment and testing stage of the policies by letting the devices stand on “monitor only” mode, watching the amount of violations that occur for example. This can be helpful in distinguishing the policy mistakes and bad user behavior; as if the violations are very high- it is possible due to policy error.

The third challenge is possible scope. Scope of overall deployment and of the many policies can quickly seem a hard ache.
To lessen the difficult challenge, we should start with the most intense and severe point in the network and grow the deployment over a steady progression of time. For example we can start with network hosting locations and departments first. We can create simple policies composing of those user groups, such as Guest can have sole access to the internet, the student can access the student servers while cooperate employees can gain access wherever. The aim is to select a solution that can grow over time with you as the deployment and network expand.

As Network Professionals we need to ask you on the exact problems you encounter or whether you need alternatives to NAC all depends on the problem you are trying to solve. To enlarge security capabilities you should look at a solution that defines Network Access Control as more than an admission control phase. You may need to ask yourselves a few questions as in "Should I be able to control users once they are authenticated onto the network?" If yes is the answer then you will need to also implement a post-admission phase as in controlling what applications the user can run and which servers the user can access.

Conclusions or suggestions to future work

Securing the perimeter of the cooperate network has been a priority which seeks to consider the CIA and nonrepudiation of data. The CIA which is confidentiality, integrity and access respectively are the main points considered when network security is being considered. A unified approach is however needed to secure the network infrastructure and also endpoints in tandem with cooperate security policy. NAC seeks to provide the unified security that is much needed in today's network infrastructure and when deployed properly there are a number of useful things that organisations can do with NAC.
It is a known fact that a compromised network puts an organisation at risk, thereby exposing valuable information of the organisation. It also highlights trust issues with clients as well as partners not to mention the financial penalties and the toll it takes on productivity.

Securing the cooperate network can never be underestimated neither can endpoints, since a compromised end point can cause a leeway for a corporate network to be compromised.

Throughout our thesis research, the fact that NAC will be a vital solution for the network security of Halmstad University stands out tall. We have researched a couple of Universities that have deployed NAC and the

elimination and reduction of vulnerabilities threats and attacks are a testament to the benefits NAC.

Virginia Commonwealth University in the United States reduced attacks, infections and malicious code and also improved the efficiency of IT security personal as a result of deploying NAC in its network. With 32,000 students, 10,000 staff members, balancing network access and manually protecting the network becomes much of a challenge. After deploying NAC in Virginia Commonwealth University, the Information Security Off Analyst Jesse Crim had this to say, "Since the Cisco NAC solution has been in place , we have seen an approximately 90% drop in infections on the student resident network"[13].

La Marr Peter Associate director of network system at John Carrol University in the United States could not agree any less with Virginia Commonwealth University. He said that resident halls had zero virus of worm infection after deploying NAC and that the university did not know how they were going to survive without NAC [14].

We further take a cue from another case study where the University of Birmingham [15] in UK is ripping the benefits of NAC deployment within their network environment. With mainly focusing on securing their 800 wireless access points, NAC proved to be the perfect solution. Like most high educational institutions of which Halmstad University is not an exception, wireless demand has been very high. The increased wireless access services unfortunately come with a price of increased exposure to threats and inadequate monitoring and controlling of endpoints. When NAC was deployed in the Birmingham University's network however, they reported that, it was only a matter of time for IT staff to be able to inventory all wireless endpoints as well as identify non-compliant endpoints and unauthorised endpoint behaviour.

We have also found out in our thesis process that most of the solutions currently available heavily supported Microsoft endpoints. There is not so much investment in endpoints running open source software.

Due to the time constraint and unavailability of physical equipment, we haven't physically deployed these products to observe performance issues for ourselves.

As a proposal for future study, we suggest further work in the area of endpoints running open source software as well as further work with non-pc devices like IP phones, printers and until quite recently iPhones.
We also suggest that NAC products be brought in for live demonstrations to be carried out for accurate hypothesis to be gathered prior to deploying NAC in the network of Halmstad University.

Having accessed different Universities around the world with similar endpoint security concerns, our assessment over all, should Halmstad University choose to deploy NAC and deploy it properly, will not only be a good investment but it will significantly reduce IT staff workload and also be beneficial for the health of the University network. Halmstad university already have the foundation network infrastructure to run integrate NAC therefore there will be no extra cost for acquiring new technologies.

Glossary of terms

NAC -Network Admission Control
WEP - Wired equivalent privacy
WPA - Wi-Fi Protected Access
RADIUS – Remote authentication dial in user service
LAN – Local area network
EAP – Extensible authentication protocol
EAPOL – Extensible authentication protocol over LAN
NAP – Network Access Protection
PDA – Personal digital assistance
DoS – Denial of service
DDoS – Distributed denial of service
FTP – File transfer protocol
SMTP – Simple mail transport protocol
SSH – Secured shell
IDS – Intrusion detection system
IPS – Intrusion protection system
VPN – Virtual private network
NAT – Network address translation
SSL – Secure socket layer

HTTPS – Secured hypertext transmission protocol

MAC – Media access control

IP – Internet protocol

ARP – Address resolution protocol

IPSEC – Internet protocol security

IETS - Internet Engineering Task Force

TCP – Transmission control protocol

TLS - Transport Layer security

WLAN - Wireless Local Area Network

AAA - Authentication, Authorisation and Accounting

WAP – Wireless access point

VLAN – Virtual local area network

MD5 – Message digest 5

TTLS – Tunnelled transport layer security

LEAP – Lightweight extensible authentication protocol

CAA – Clean access agent

CAM – Clean access manager

CAS – Clean access server

LDAP – Lightweight directory access protocol

NAD – Network access devices

HCAP – Host credential authorisation protocol

DHCP – Dynamic host configuration protocol

ACL – Access control list

References

[1] Network World Editorial on how NAC's standardisation is a winner, 24th May 2010.

[2] www.networkworld.com/reviews/2010/052410-network-access-controltest--standards.html

[3] Microsoft Tech site for networking technologies. http://technet.microsoft.com/en-us/network/bb545879.aspx

[4] Network World's test results of 13 NAC solutions. 30 July 2007. http://www.networkworld.com/reviews/2007/073007-test-nac-main.html

[5] NAC and NAP interoperability benefits 2nd June 2010 http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/-ns8

[6] http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/-ns812/guide c07-491729.html

[7] NAC and NAP interoperability architecture 2nd June 2010 http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/Ns617/net_implementation_white_paper0900aecd8051fc24.pdf

[8] Computer Network Security: Theory and Practise by Jie Wang.

[9] Ya-Chin Sung and Yi- Bing Lin Effects of the EAPOL Timer in IEEE802.1X Authentication IEEE Transaction on Wireless Communications Volume 6, No 6, June 2007.

[10] M.A. Catur Bhakti, A. Abdullah, and L.T. Jung. EAP-based Authentication with EAP Method Selection Mechanism International Conference on Intelligent and Advanced Systems 2007

[11]Fact Sheet IEEE802.1X from www.ja.net

[12]http://www.calsoftlabs.com/whitepapers/network-access-protection.html

[13]http://cisco.biz/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/case_study_univ_virtually_eliminates_infections_v3.pdf

[14]https://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/case_study_c36-548907.html

[15] Campus Technology is a monthly publication of technology issues in higher education. This article is about NAC deployment at Birmingham University. 24th November 2008.
http://campustechnology.com/articles/2008/11/universities-in-texas-and-the-uk-protect-networks-with-mirage-nac.aspx

[16] The trusted computing group.
http://www.trustedcomputinggroup.org/d

[17]The internet engineering task force.
http://www.ietf.org/