International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 12 Issue 03 March 2024, Page no. – 4073-4090

Index Copernicus ICV: 57.55, Impact Factor: 8.316

DOI: 10.47191/ijmcr/v12i3.01

Study of Securing A Wireless Network with A Radius Server

Kamanga Kamono, Jean[1], Kankolongo Mulumba, Godelive[2], Ilunga Meji, Erick[3]
Kalala Kayembe, Barthelemy[4]

[1]Assistant. Science and New Technology. University of Mwene-Ditu (UMD), DRC.
[2]Attachée de Recherche, Domaine des sciences et nouvelle Technologie. Université de Mwene-Ditu (UMD), RDC.
[3,4]Assistant, Domaine des sciences et nouvelle Technologie. Université de Mwene-Ditu, (UMD), RDC.

ARTICLE INFO

Published Online:
15 March 2024

Corresponding Author:
Kamanga Kamono, Jean

ABSTRACT

Radius centralizes logins and passwords. This is a server protocol. It should be noted that the server, Radius, manages authentication for clients, routers and switches. Radius is simply a remote authentication protocol used to centralize authentication data and manage user connections to remote services. This protocol relies primarily on a server (DARIUS server), linked to an identification base (database, LDAP directory, etc.). A Radius client, called NAS (Network Access Server), acting as intermediary between the end-user and the server. All transactions between the Radius client and the server are encrypted.

It works on the basis of a scenario similar to : a user sends a request to the NAS to authorize a remote connection. The NAS in turn forwards the request to the Radius server. The latter consults the requested identification database to find out the type of identification scenario requested for the user. Either the current scenario is suitable, or another identification method is requested from the user. This protocol thus returns one of the four responses we'll discuss in the rest of this article : **ACCEPT** : identification successful, **REJECT** : identification failed, **CHALLENGE** : the Radius server requests additional information from the user and proposes a challenge. Following the above authentication phase, an authentication phase begins, in which the server returns the user's authorizations.

In this article, as a network manager, we're concerned with setting up means of access control, and to do this, we have to square a kind of circle : simplicity for the user, reliability of the mechanisms, high level of security, all while using available standards as much as possible.

KEYWORDS: Study, Security, Network, Server, Radius

I. INTRODUCTION

The growing use of the Internet has enabled many companies to open up their information systems to their partners and suppliers. It is therefore essential to know which company resources need to be protected, and to control access and user rights to the information system.   What's more, wherever staff connect to the information system, they are transporting part of the information system outside the company's secure infrastructure.IT system security is generally confined to guaranteeing access rights to data and system resources, by implementing authentication and control mechanisms to ensure that users of these resources have only the rights they have been granted.

The security mechanisms put in place can, however, cause discomfort for users, with instructions and rules becoming increasingly complicated as the network expands. IT security must therefore be designed in such a way as not to prevent users from developing the uses they need, and to ensure that they can use the information system with complete confidence.

From a technical point of view, security covers both access to information on workstations and servers, as well as the security of information systems. In recent years, new information and communication technologies (NICTs) have considerably changed the way people interact with computers, both professionally and personally. A company's information system (IS) - a combination of hardware and software - is responsible for storing, processing and electronically transporting data. The latter task is essentially performed by computer networks. However, the management of user accounts is one of the tasks absolutely assigned by administrators to ensure connection problems, authentication and user access rights. Indeed, corporate resources are increasingly pooled, leading to a centralization of information. The Remote Authentication Dial In User Service (RADIUS) protocol was designed to manage remote user connections to the network. Its capabilities are summed up by the acronym AAA, which is often associated with it. This expression summarizes the three functions supported : Authentication, Authorization and Accounting. Its use is recommended, but not mandatory, with 802.1x.

Definitions

The term NETWORK [1] defines a set of entities (objects, people, etc.) interconnected with one another so that material or immaterial elements can circulate between each of these entities according to well-defined rules. Depending on the type of entities interconnected, the term network will be defined differently :

1. **Transport network** [2] : a set of infrastructures and arrangements for transporting people and goods between several geographical areas.
2. **Telephone network** [3] : set of infrastructures enabling voice to be transmitted between several telephone sets.
3. **Computer network** [4] : a set of computers linked together by physical lines, exchanging information in the form of digital data (binary values, i.e. coded as signals that can take two values : 0 and 1). A computer network offers a number of advantages :
4. People-to-people communication (e-mail, live chat, etc.),
5. Resource sharing (files, applications, hardware, Internet connection, etc.).

I.1. Objectives Of Computer Networks [5]

Anyone who has ever worked on a network will never be able to do without it. Some of the most obvious advantages are as follows :

1. The extreme ease with which information can be communicated to those around you ;
2. The ease with which users can change workstations without having to transport their files on floppy disks or other storage media.

I.2. Wireless Technologies

So-called "wireless" technologies [6], and the 802.11 standard in particular, make it easier and cheaper to connect large networks. With little hardware and a little organization, large quantities of information can now circulate over several hundred meters, without the need for a telephone company or cabling.

These technologies can be divided into four categories:

- Wireless Personal Area Networks (WPANs);
- Wireless Local Area Network (WLAN);
- Wireless Metropolitan Area Network (WMAN);
- Wireless Wide Area Network (WWAN).

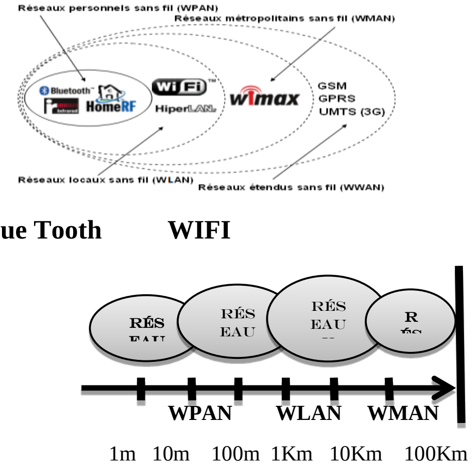

Réseaux personnels sans fil (WPAN)
Réseaux métropolitains sans fil (WMAN)
Bluetooth
HomeRF
Infrared
WiFi
HiperLAN
wimax
GSM
GPRS
UMTS (3G)
Réseaux locaux sans fil (WLAN)
Réseaux étendus sans fil (WWAN)
Blue Tooth
WIFI
RÉS
RÉS EAU
RÉS EAU
R
WPAN
WLAN
WMAN
1m
10m
100m
1Km
10Km
100Km

Figure I-1 : Different wireless technologies.

WiFi [7] :

WiFi is a set of wireless communication protocols governed by the IEEE 802.11 group of standards. WiFi standards make it possible to create high-speed wireless local area networks. In practice, WiFi makes it possible to connect laptops, office machines, PDAs (Personal Digital Assistants), communicating objects or even peripherals to a high-speed link (from 11 Mbit/s theoretical or 6 Mbit/s real in 802. 11b to 54 Mbit/s theoretical or around 25 Mbit/s real in 802.11a or 802.11g over a radius of several dozen meters indoors (generally between twenty and fifty meters), as this is the type of technology we're interested in, we'll briefly explain the three technologies :

a. GSM

GSM is a digital cellular radiotelephony system, offering its subscribers services that enable end-to-end mobile station communication across the network [8]. Telephony is the most important of these services. This network enables communication between two mobile stations, or between a mobile station and a fixed station. Other services include data transmission and short alphanumeric messages.

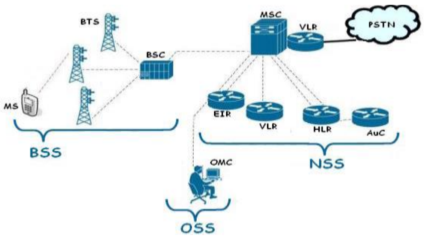


Figure I-2 : GSM network architecture.

BSS (Base Sub-system): radio sub-system, its main function is to manage the allocation of radio resources, independently of subscribers, their identity or their communication.

NSS (Network Sub-System): the routing sub-system, mainly responsible for switching and routing functions. It provides access to the public PSTN (Public Switched Telephone Network) or ISDN (Integrated Services Digital Network)

network. In addition to the essential switching functions, it includes the mobility, security and confidentiality management functions implemented in the GSM standard.

OSS (Operation Sub-System): the operation and maintenance sub-system, it manages and supervises the network. It is the function whose implementation is given the most freedom in the GSM standard. Network supervision takes place at a number of levels:

- Fault detection;
- Site commissioning;
- Parameter modification;
- Statistics

a. GPRS

General Packet Radio Service or GPRS [9] is a mobile telephony standard derived from GSM, enabling higher data rates. It is often referred to as 2.5G. The G stands for generation, and the 2.5 indicates a technology halfway between GSM (2nd generation) and UMTS (3rd generation). GPRS is an extension of the GSM protocol, adding packet transmission. This method is better suited to data transmission. In fact, resources are allocated only when data is exchanged, unlike the "circuit" mode in GSM, where a circuit is established - and the associated resources - for the entire duration of the communication.

GPRS provides constantly available IP connectivity to a mobile station (MS), but radio resources are allocated only when data is to be transferred, thus saving radio resources. Users therefore benefit from low-cost access, and operators save on radio resources. What's more, no dialing delay is required.

Before GPRS, access to a network was circuit-switched, i.e. the radio channel was continuously reserved for the connection (whether or not there was data to be transmitted). The connection followed the following path : MS → BTS → BSC → MSC → Network.

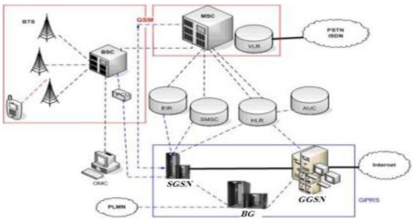


Figure I-3 : GPRS network architecture.

PCU : To deploy GPRS in access networks, existing systems and infrastructures are reused. To these must be added an entity responsible for sharing resources and retransmitting erroneous data. This is the Packet Control Unit (PCU), which is updated by hardware and software in the BSCs.The SGSN (Serving GPRS Support Node) is a gateway for routing data in GPRS mobile networks. It manage the interface with the external packet network via another gateway.

The GGSN (Gateway GPRS Support Node) is an interconnection gateway between the mobile packet network (GPRS or UMTS) and external IP networks. The GGSN forwards traffic to the active SGSN for the Mobile Station (MS) associated with the protocol address (the IP address, for example). A Border Gateway (BG) function terminates the Gp interface to a PLMN (Public Land Mobile Network). This function is usually a border router supporting BGP (Border Gateway Protocol) and security protocols such as IPSec (Internet Protocol Security).

b. UMTS

UMTS [10] stands for Universal Mobile Telecommunications System. This is a fourth-generation mobile telephony technology, the successor to the GSM standard in Europe. Using a wider frequency band and a packet-based data transfer protocol inherited from computer networks, it offers a much higher data rate than its predecessor, reaching 384 kbit/s in its first version released at the end of November 2004. A second version, expected in 2006, could even go up to 2 Mbps. The key to this is the possibility of using a wide range of multimedia services on your cell phone, such as the Internet, video telephony, television, downloading and playing video games, etc.

UMTS technology provides users with a better quality of telecommunications service, particularly in terms of the services offered (possibilities) and transfer speeds. The UMTS network is based on a flexible, modular architecture. This architecture is neither associated with a specific radio access technique, nor with a set of services, which ensures its compatibility with other mobile networks and guarantees its evolution. Such an architecture, illustrated in Figure I-6, is made up of three "domains" :

- The User Equipment (UE) domain ;
- The "universal" radio access network UTRAN (Universal Terestrial Radio Access Network) ;
- The CN (Core Network).
-

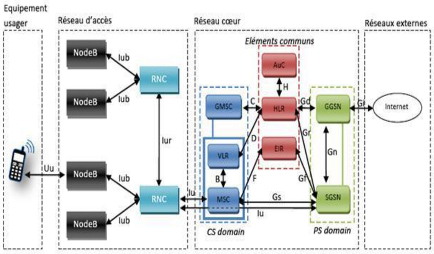


Figure I-4 : General architecture of UMTS.

I.3. Computer Security

These days, the world is experiencing very significant advances in the computer field ; the need for security is a little more pressing, and the predisposition is not necessarily downward. For some years now, we have been witnessing a constant change in techniques, from those designed to secure data exchange to those developed to bypass secure systems. Hence, data security tends to improve. And as the Chinese proverb says : "the art of war is based on deception", so by analogy, computer security [11] must represent a strategy that eradicates this deception.

We all know that computer hardware is virtually everywhere. Indeed, on the one hand, hardware is accessible at a very affordable price, and on the other, software tends to be simpler and easier to learn. What's more, computerized businesses require a secure network for data transfer, both between the company's own machines and with external machines. This being the case, security in general is present at several levels, whether it concerns the different scopes of information. Security must be considered in its entirety, as illustrated in the figure below :

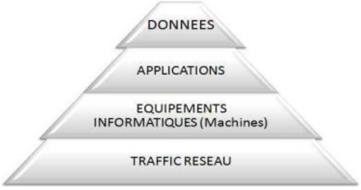


Figure I-5 : General architecture of UMTS.

Levels of IT security

IT security is concerned with protection against IT-related risks ; it must take into account :

- The elements to be protected : hardware, data, users
- Their vulnerability ;
- Their sensitivity : amount of work involved, confidentiality...
- The threats they face
- The means of dealing with them (preventive and curative) : complexity of implementation, cost...

Specifically, this security course aims to :

✓ Provide concepts relating to computer security, focusing on existing security risks and flaws, as well as the establishment of a sound security policy strategy ;

✓ Understand the various security flaws that can result from computer communications systems, through piracy, attacks and espionage ;

✓ A general understanding of the concepts of cryptography and cryptanalysis of information from traditional systems to modern (computer) systems, and the application of corresponding methods ;

✓ Acquire notions and concepts related to computer biometrics, its operating principle and the various techniques used.

I.4. Definition & Study Context

IT security is the set of measures implemented to reduce a system's vulnerability to accidental or intentional threats.

I.5. The Aim Of It Security [12] Is To

Is to ensure that the hardware and/or software resources of an IT system are only used for their intended purpose and by authorized persons. It is important to identify the fundamental requirements of IT security, which characterize what users of IT systems expect in terms of security :

✓ **Confidentiality :** Only authorized persons should have access to data. Data must be encrypted, and only those involved in the transaction must have the key to understanding it.

✓ **Integrity :** We need to guarantee at all times that the data in circulation is what we think it is, and that there has been no alteration (intentional or otherwise) during communication. Data integrity validates data completeness, accuracy, authenticity and validity.

✓ **Availability :** We need to ensure that the system is working properly, and that access to a service and resources is possible at any time. Equipment availability is measured by dividing the time during which the equipment is operational by the time during which it should have been operational.

✓ **Non-repudiation :** A transaction cannot be denied by any of the parties involved. Non-repudiation of the origin and receipt of data proves that the data has indeed been received. This is achieved using digital certificates and a private key.

✓ **Authentication :** limits access to authorized persons. A user's identity must be verified before data is exchanged.

In short, the security of an entire system is measured by the security of its weakest link. So, if an entire system is technically secure, but the human factor - which is often blamed - fails, the whole system's security is called into question.

I.6. IT Security Risk Studies [13]

The costs of an IT problem can be high, and so can the costs of security. It is necessary to carry out a risk analysis, taking care to identify potential problems and solutions, with their associated costs. The set of solutions selected must be organized in the form of a coherent security policy, according to risk tolerance levels. The result is a list of what needs to be protected. However, it is important to bear in mind that the main risks remain : cable pull-out, power failure, disk crash, incorrect user profile, etc.

Here are a few elements that can be used as a basis for a risk study:

✓ What is the value of equipment, software and, above all, information?

✓ What is the cost and timeframe for replacement?

✓ Conduct a vulnerability analysis of the information contained on networked computers (packet analysis programs, logs, etc.).

✓ What would be the impact on customers of public information concerning intrusions on the company's computers?

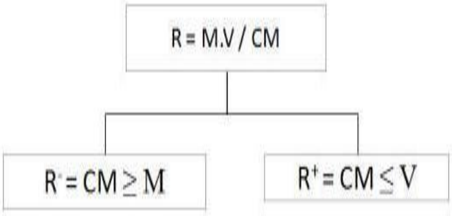
In fact, with the development of Internet use, many companies are opening up their information systems to their partners or suppliers, and are more at the level of three-tier or n-tier architecture. It is therefore essential to know which company resources need to be protected, and to control access and user rights. On the other hand, security is a compromise between costs, risks and constraints. We can better understand the weight of a risk by relying on the following formula:

$$\text{Risk} = \frac{\text{threat } \mathbf{x} \text{ vulnerability}}{\text{counter-measures}}$$

- Risk: The probability that a threat will exploit a vulnerability. In other words, it's the possibility of something harmful happening.
- Vulnerability: A weakness inherent in a system (software or hardware). Sometimes called a flaw or breach, it represents the level of exposure to a threat in a particular context.
- Threat: a danger (internal or external) such as a hacker, virus, etc.
- Countermeasure: a means of reducing risk within an organization.

Consequences of the formula:

- The greater the number of countermeasures, the lower the risk, µ
- The greater the number of vulnerabilities, the greater the risk.



The use of IT tools is likely to expose us to several types of risk. It is therefore important to be able to measure these risks in terms of the probability or frequency of their occurrence, and also by measuring their possible effects. These effects may have negligible or catastrophic consequences :

- ✓ Computer processing in progress fails: simply restart it, possibly using another method if you fear the cause will reappear;
- ✓ The incident is blocking and must be repaired or corrected before continuing. It should be noted, however, that these same incidents can have far more serious consequences:
- ✓ Data irretrievably lost or corrupted, rendering it unusable at a later date;
- ✓ Data or processes that are permanently unavailable, leading to production or service stoppages;
- ✓ Disclosure of confidential or erroneous information that could benefit competitors or damage the company's image;
- ✓ Triggering actions that could lead to physical accidents or human harm.

II. TYPOLOGY OF IT RISKS [14]

In IT security, there are two main types of risk: human and material.

1. Human Risks

These are the most important, even if they are most often ignored or downplayed. They concern not only users, but also the IT specialists themselves.

These include:

a. Clumsiness: making mistakes or carrying out unwanted processing, or unintentionally deleting data or programs; etc.

b. Unconsciousness and ignorance: unknowingly introducing malicious programs (e.g. when receiving mail). Many users of IT tools are still unaware of the risks they pose to the systems they use. Reckless manipulations (both software and hardware);

c. Malicious intent: in recent years, it has become impossible to ignore the various problems posed by viruses and worms. Some users may deliberately jeopardize an information system by knowingly introducing viruses, or by deliberately introducing bad information into a database. There's even talk of "cybercrime»;

d. Social engineering : a method of obtaining confidential information from a person, which one is not normally authorized to obtain, with a view to exploiting it for other purposes.

e. It consists of :

- Pretending to be someone you are not (usually a network administrator) ;
- Requesting personal information (login name, password, confidential data, etc.) under any pretext (network problem, network modification, etc.) ;

This can be done by telephone, e-mail or by visiting the site.

f. Espionage : especially industrial espionage, employs the same means, as well as many others, to obtain information about competitors' activities, manufacturing processes, current projects, future products, pricing policies, customers and prospects, etc.

2. Hardware Risks

These relate to the inevitable faults and failures that occur in all hardware and software systems. These incidents are more or less frequent, depending on the care taken during manufacture and the application of test procedures carried out before computers and programs are put into service. Some of these failures have indirect or very indirect causes, and are therefore difficult to predict.

These include :

- ✓ **Material-related incidents :** most modern electronic components produced in large series can have manufacturing defects. Eventually, they fail. Some of these failures are difficult to detect because they are intermittent or rare. Sometimes, they are the result of a design error.
- ✓ **Software-related incidents :** these are the most frequent. Operating systems and programs are becoming increasingly complex as they do more and more things. They require the joint effort of dozens, hundreds, even thousands of developers. They can make mistakes, individually or

collectively, which the best working methods and the best control or testing tools cannot eliminate entirely.

✓ **Environmental incidents :** electronic machines and communication networks are sensitive to variations in temperature and humidity, as well as to electromagnetic fields. It is therefore possible for a computer to break down permanently or intermittently due to unusual climatic conditions or the influence of electrical installations, particularly industrial ones.

I. IT Risk Management [15]

IT risk management is a set of operations to manage and direct the various incidences linked to the handling of IT tools. Risk management consists of three major actions :

- ✓ Studying potential risks(identifying/uncovering them) ;
- ✓ Impose appropriate safety rules to reduce these risks ;
- ✓ User training.

a. Studying potential risks

This phase consists of a thorough review of the current IT risk assessment methodology. This is achieved by :

✓ Defining the environment : Definition of players and their interests ; Importance of security in the company's strategy ; Type of data involved ; External visibility of security (importance for customers, the public).

✓ Threat analysis : Identify the nature of the threat : accidental (disaster, bugs, etc.) or intentional (attacks, theft, etc.) ; Investigate the source of the threat : unauthorized personnel, intruder, software ; Locate the threat : manual procedures, IT (software, network, storage, hardware), infrastructure (concrete and abstract).

✓ Vulnerability study : Study of the weaknesses generated by the execution of a threat.

✓ Risk assessment : Probability of occurrence of these threats leading to a vulnerability.

✓ Estimation of risk and strategic plan : Risk (Cost of short-, medium- and long-term losses engendered, Cost of implementing countermeasures at both logical and logistical levels, Comparing potential loss with cost of countermeasures) ; Strategic plan (Implementation planning taking into account future needs in terms of security or otherwise, Implementation monitoring planning).

✓ Setting up the security plan : The security mechanisms put in place can be a hindrance to users, and the instructions and rules defined can become increasingly complicated as the network expands. IT security must therefore be designed in such a way as not to prevent users from developing the uses they need, and to ensure that they can use the information system with complete confidence. For this reason, the first step is to define a security policy, to be implemented in four phases :

- ➢ Identify security requirements, IT risks affecting the company and their potential consequences ;
- ➢ Draw up rules and procedures to be implemented in the various departments of the organization for the risks identified ;
- ➢ Monitor and detect vulnerabilities in the information system, and keep abreast of vulnerabilities in the applications and hardware used ;
- ➢ Define the actions to be taken and the people to be contacted if a threat is detected.

➢ Security audit [16] : The security audit consists of relying on a trusted third party (preferably a company specializing in IT security) to validate the means of protection implemented, with regard to the security policy. In fact, the aim of the audit is to verify that each rule of the security policy is correctly applied, and that all the measures taken form a coherent whole.

b. Impose appropriate safety rules

This involves defining internal company procedures based on :

✓ **Administrative rules :** Follow security standards (ISO norms) ; Follow the law.

✓ **Physical rules :** Guards, cameras, alarms, locks and biometric access to secure premises.

✓ **Technical rules :** Determine data classification levels ; Define access levels to data ; Use cryptography for information processing and storage ; Install a hardware and/or software firewall,

c. User training

It is increasingly recognized that security is essential. The cost of data loss due to network attacks and other malware is decreasing significantly year on year1. It is much easier to corrupt the user and his surroundings than the encryption algorithm used, for example :

✓ The user is unaware of the risks involved in keeping a list of passwords on the side of the computer ;

✓ It is often easier to break into the user's computer to retrieve the plaintext (hacking, theft, etc.) ;

✓ It's possible to spy on the user and encourage him/her to denounce.

So it's not a question of explaining to employees how the algorithms they'll be using work, but rather how and under what conditions they should use them, by defining rules that must not be transgressed. There are also several ways of reacting to a risk, from the "safest" to the most unconscious :

✓ Transfer risks to an insurance company ;

✓ Reduce risks by implementing countermeasures, which may include :

- ✓ Deterrents : to prevent an attack ;
- ✓ Preventive : defeat an attack ;
- ✓ Corrective : reduce the damage caused by an attack
- ✓ Ignore/Disregard risks ;
- ✓ Accept risks if countermeasures are too costly

Of course, there is always a risk, however small. The pros and cons need to be weighed up before any countermeasures are taken. However, 2007 saw a rise in total losses due to financial fraud.

II.2 Establishment And Elements Of An It Security Policy

The security policy element [17] is the set of guidelines followed by an organization in terms of security. It is drawn up at management level, as it concerns all system users. A company's IT security policy is based on a sound understanding of the rules by its employees, thanks to training and awareness-raising campaigns aimed at users, but it must also go beyond this, covering the following areas :

- ✓ Implementation of patches ;
- ✓ Definition of security policy ;
- ✓ Objectives, Scope, Responsibilities ;
- ✓ A properly planned backup strategy ;
- ✓ Description of security (physical infrastructure, computer data, applications, network) ;
- ✓ Disaster recovery plan ;
- ✓ Staff awareness of new procedures
- ✓ Sanctions in the event of non-compliance.

Once the risks have been studied, and before any protection mechanisms are put in place, a security policy needs to be drawn up. It sets the main parameters, including tolerance levels and acceptable costs. Here are a few points to help you define a policy :

- ✓ What were the costs of past IT incidents ?
- ✓ How much trust can you place in your internal users ?
- ✓ What do customers and users expect from security ?
- ✓ What will be the impact on customers if security is insufficient, or so strong that it becomes burdensome ?
- ✓ Important information stored on networked computers ? Are they accessible from the outside ?
- ✓ How is the network configured, and are any services accessible from the outside ?
- ✓ What are the legal rules applicable to your company concerning the security and confidentiality of information (e.g. French Data Protection Act, accounting records, etc.) ?

It's also important to remember that security is like a chain, only as strong as its weakest link. In addition to ongoing user training and awareness-raising, security policy can be broken down into several parts :

- **Hardware failure :** All physical equipment is subject to failure (wear and tear, ageing, defects, etc.). Purchasing quality, standard equipment backed up by a good warranty and technical support is essential to minimize downtime. However, only a form of backup can protect data.
- **Software failure :** Every computer program contains bugs. The only way to protect against them is to make copies of the information at risk. Regular software updates and visits to sites dedicated to this type of problem can help to reduce their frequency.
- **Accidents (breakdowns, fires, floods, etc.) :** A backup is essential to effectively protect data against these problems. This backup procedure can combine several means operating at different timescales : RAID disks to maintain server availability ; Backup copy via the network (daily) ; Backup copy in another building (weekly).
- **Human error :** In addition to backup copies, this problem can only be mitigated by properly trained staff.
- **Theft via physical devices (disks and tapes) :** Control access to this equipment : only place diskette and tape drives on computers where they are essential. Set up monitoring devices.
- **Viruses from floppy disks** : This risk can be reduced by limiting the number of floppy disk drives in use. Installing antivirus programs can provide effective protection, but they are costly, reduce productivity and require frequent updates.
- **Hacking and network viruses :** This is a more complex problem, and the ubiquity of networks, particularly the Internet, makes it particularly important. Security problems in this category are particularly damaging, and are the subject of the following study.

III.3. Main Computer Security Faults [18]

Security faults can be considered as accidental or unconscious modifications to the normal operation of IT equipment. The most frequently observed information system security faults are :

- ✓ Installation of default software and hardware ;
- ✓ Updates not carried out ;
- ✓ No or default passwords ;
- ✓ Unnecessary services retained (Netbios...) ;
- ✓ Unused traces ;
- ✓ No separation of operational flows from system administration flows ;
- ✓ Obsolete security procedures ;
- ✓ Test elements and tools left in place in production configurations ;
- ✓ Weak authentication ;
- ✓ Remote maintenance without strong controls.

III. PASSWORD CONCEPTS [19]

III.1. Definition

A password is a word or series of characters used as a means of authentication to prove one's identity when accessing a protected area, a resource (particularly a computer resource) or a service to which access is restricted and protected. The password must be kept secret to prevent unauthorized third parties from accessing the resource or service. It is one of several methods of verifying that a person corresponds to the declared identity. It's a proof that you possess and that you communicate to the service responsible for authorizing access. For example, in the tale "Ali Baba and the Forty Thieves of the Thousand and One Nights", one of the most famous passwords is "Open sesame".

The term "password" is of military origin. Command words" include the "summation word" (i.e. the agreed question) and the "password" (i.e. the corresponding response). These are the verbal signs that enable two units or two soldiers to recognize each other, for example during a night patrol, at the delicate moment of returning to the friendly unit. In this case, the password is shared by a trusted group of people. When it's a personal code, it's better to use the expression "confidential code" to emphasize the secret nature of the code and make the holder feel more responsible.

III.2. Principle And Limitations

In France, for example, there is a legal limit to password security : if encrypted data is seized by the courts, the law on daily security requires the user to provide the encryption method and the keys or passwords. The use of passwords is a compromise between security and practicality. With the multiplication of situations where a password is required, each of us has an ever-increasing number of passwords. While it is legitimate to use the same password for all situations where it is of little importance, there are still many cases where a quality password must be used. This password cannot be the same everywhere, on the one hand to prevent its compromise from leading to unfortunate situations, and on the other because certain sites and software require regular password changes and limit their re-use. As the user's memory is insufficient to memorize all these passwords, the temptation to list them is great. The list of passwords thus created must be even more secure. This is known as a "password safe" :

- Capturing an "unencrypted" password : A password is "unencrypted" when it has not been transformed using a hash function. There are several situations in which a password can be found in the clear,
- Direct spying on the keyboard of the person entering the password ;
- Installation of a keylogger, which captures any text typed by a user without their knowledge ;
- Network eavesdropping. If an attacker manages to eavesdrop on an unencrypted communication in which the target must identify itself with a password, this password will appear unencrypted to the attacker.
- Theft of a handwritten password.

Some software programs make form passwords visible. The characters are "hidden" by circles or asterisks, which are there to prevent someone behind you from reading what you're typing. In the program, at this point, the password is present and still unencrypted ; making it visible simply involves changing a display option.

Capturing an encrypted password : When an encrypted password is captured, it is not directly usable : the malicious person (the attacker) must discover the corresponding plaintext, by decrypting it if possible, or using other techniques. The attacker is said to break or "crack" the password.

There are two types main scenarios : the password is part of a communication, or only the encrypted password is captured.

The entire communication is encrypted : In this case, we need to find a way to decrypt the entire communication in order to find the password. This means finding a flaw in the encryption algorithm or in one of its implementations. If the encryption is broken, no matter how small the password, it will be found in the decrypted text.

Only the encrypted password is captured : This is usually a hash of the password, i.e. the result of a non-reversible algorithm. This is a good practice, used in many cases : web sites, operating system user accounts, etc. In cases where the algorithm is not truly irreversible (due to design or implementation errors), it may be possible to retrieve the clear corresponding to a condensate. For example, the password management used to protect Excel and Word files in Office 97 is flawed, making it easy to find the passwords used.

But in general, other techniques are used to break a condensate. If you know the hash function, you can imagine a number of different attacks :

- **The brute-force attack :** a space of passwords to be explored is set, with a fixed length and set of characters ; all possible passwords in this space are listed ; for each of these passwords, the hash function is used to calculate the fingerprint, and this fingerprint is compared with the one captured. To prevent such attacks, the use of a long, complex password is recommended. By complex password, we mean a password comprising different types of characters : upper and lower case letters, numbers, and non-alphanumeric characters (such as ! /#@ ...). The length of the password will ensure that it is not enumerated during a brute-force attack : the larger the space to be enumerated, the longer the attack will take. See the graph opposite (note that the scale is logarithmic).
- **Dictionary attack :** same as brute-force attack, but where the words are chosen from a dictionary. The use of characters other than letters and numbers will generally ensure that the password does not belong to a dictionary, and will therefore not be susceptible to a dictionary attack.

III.4. Password Selection [20]

If there is one area where security can be lacking, it is in the management of user passwords. Indeed, the security of a system also depends on the level of security of the password used to access it. When creating a password, particular attention must be paid to a number of points :

- If a password generator is used, it should employ a wide variety of characters (to make it more robust to brute force) ;
- It may be useful to use a password checker to test vulnerability to dictionary attacks. At the same time, it can test password size against brute-force attacks ;
- It's a good idea to associate a lifetime with passwords. Regular change provide better protection against brute force attacks.
- You can also limit the number of tries.

a. Robustness criteria

Password quality and length are crucial to security. A password that is too short, or that comes from a dictionary, is likely to be attacked via a table search containing a list of passwords. More systematically, a brute force attack tries all possibilities and, given enough time, it is theoretically possible to recover the password. One compromise is the rainbow table, an improvement on the time-memory compromise principle. The robustness of a password depends on a number of criteria :

✓ Its length - the most important criterion. Passwords should be of sufficient length to protect them from brute-force attacks (this length increases over time with the power of the tools used by attackers - for a password for local use, at least 12 characters are recommended in the 2010s, and even 16 characters for more secure passwords).

✓ Its non-simplicity - 123456, www, 111111, Love, 0000, azerty... are to be avoided, as are dates of birth, the name of your dog or any other information directly related to your private life. Similarly, slogans and quotations can easily be attacked using a dictionary attack. More generally, password content should not follow any logic, but be a simple succession of randomly chosen characters.

✓ Uniqueness - to avoid cascading damage, don't reuse the same password for different services.

✓ The variation of characters used - a password is stronger when it mixes upper and lower case letters, numbers, punctuation marks and special characters. Note that it is always more secure to increase the length of a password than to use as many different characters as possible.

In addition, passwords should be chosen according to their criticality (for example, a password enabling access to the administration interface of an application or piece of equipment will be considered highly critical).

In practice, a study of 32 millions passwords to the RockYou.com website, obtained in 2009 following an attack on the site, showed that 30% of these passwords had six characters or less, and that the most frequent (just under one in a hundred) was "123456"16. Every year, security solutions provider Splash-Data also publishes a list of the most frequently used passwords, referred to as "the worst passwords not to use". The top 5 passwords used by users worldwide in 2015 are17 :

- ✓ 123456 ;
- ✓ Password ;
- ✓ 12345678 ;
- ✓ Qwerty.

a. The "wrong" passwords [21]

- ✓ **Default :** password, mdp, default, admin,
- ✓ **Words :** hello, test, car, silence, . . .
- ✓ **Numbered words :** january31, year154, symbol2024, . . .
- ✓ **Equals login :** john2023, . . .
- ✓ **Double words :** crabcrab, stopstop, treetree...
- ✓ **Sequences :** qwerty, 12345678, bhunji,
- ✓ **Personal :** first name, registration number,
- ✓ **Proper names :** Mutabazi, Gracia, ...

Of course, security needs being what they are, the major difficulty today is that the number of passwords continues to grow. So remembering them remains a problem. However, a few solutions do exist :

- Hardware : Using USB keys to access data. The problem is that it's the key that authenticates, not the individual. And what happens if the key is lost ?
- Software : use password management software : a single password (or passphrase) to store all the others. But what if you forget your master password ?
- Use semi-automatic input ;
- OS level - An advanced solution is known as SSO (Single Sign On). Logging on to a machine enables access to all data. A single authentication phase then takes place, and if successful, the user is free to act with the data and software corresponding to his or her rights, without having to give his or her password for each access. A well-known application based on a similar principle is Kerberos (user authentication on network machines).

b. Other password categories

There's another possibility, but one that can't be used under all conditions. It's called One Time Password (OTP) or Password Under Duress :

✓ **Duress password :** Some alarm monitoring companies use 2 passwords : the normal password and the duress password. When the alarm is triggered, the security company calls the customer and asks for his password to verify his identity. If the customer gives the duress password, the security agent knows that the person giving it is under threat, and triggers an intervention.

✓ **One Time Password :** The password generated here is only valid for a specific period of time. Two methods coexist :

- Synchronous method : Time-synchronous ;
- Asynchronous method : Challenge response.

A good password should be easy to remember (no need to write it down), and use special characters of different case (which makes brute force more tedious and dictionary attacks almost impossible). The advice put forward by the European Commission should be applied when creating a password to protect it from attack. In fact, a good password should : Be long ; Be unique ; Be complex ; Be changed regularly ; Not contain any part of the user account name ; Have a minimum of eight characters ; Contain characters from at least three of the following categories ; Non-alphanumeric symbols ($:"%@# !) ; Numbers ; Upper case letters and Lower case letters.

IV. AUTHENTICATION (USER MANAGEMENT [22]

IV.I. Basics

Implementing an authentication solution on a wired local area network produces significant benefits. The introduction of wireless networks is exacerbating security issues and driving the deployment of these authentication technologies.

They enable users to use their wired or wireless connection at will, without any functional difference, and network management will be optimized and made more secure. The evolution of authentication protocols, combined with high-performance encryption algorithms, means that we can now take advantage of the best of both worlds, wired and wireless.

IV.2. Authentication Criteria [23]

✓ **Authenticate**

Authentication is all very well, but what exactly do we want to authenticate ? Users or machines ?

It's worth asking this question, because depending on the answer, different implementation choices will be made.

If we authenticate users, this means that authentication and authorization, and therefore the VLAN offered, will depend on the user operating the machine. The same machine will be connected to one VLAN or another, depending on the user.

For example, when John connects to machine PC1, it is placed on VLAN 2, and when Durand connects to the same machine, it is placed on VLAN 3. This means that either authentication (and therefore the establishment of the network link) takes place when each user logs into his or her session, or the identity of a single user is considered when the machine starts up.

If machines are authenticated, this means that whatever their users, the machines will always be placed on the same VLAN. The machine then has its own unique identity, which can be used to authenticate it at start-up, or when a user logs on.

IV.3. Wi-Fi Authentication

In terms of Wi-Fi networks, the basic IEEE 802.11 standard originally offered speeds of 1 or 2 Mbps, but successive revisions (802.11b, 802.11a and 802.11g, also known as "physical" 802.11 standards) have enabled these speeds to be optimized. Protection mechanisms also evolved in parallel.

The security modes offered as standard in 802.11, and the WEP (Wireless Encryption Protocol or Wired Equivalent Privacy) protocol, were in fact unreliable, and authentication was downright non-existent with WEP.

Other standards, such as 802.1x and 802.11i, were therefore enacted in an attempt to ensure better security (key management and distribution, encryption and authentication) or, like 802.11e, better interoperability.

When it comes to authentication in a WI-Fi network, several techniques are possible. However, the 802.11x WPA and 802.11i WPA2 standards encompass both authentication and encryption mechanisms.

The first authentication method consists in not requiring "a priori" authentication, as is the case with airport host spots, for example. Since the user has no knowledge of the network, and vice versa, he or she cannot logically use initial authentication by key. In this case, authentication is established via a web portal. The user can do nothing until he/she has tried to consult a web server. At this point, the user's http connection attempt is "spoofed" by the portal, which asks the user for authentication, usually using a login/password (EAP-MD5 protocol). AAA authentication using Radius or LDAP protocol, but other authentication methods, including client certificates, can also be used.

802.11x offers a scalable security architecture that accommodates multiple key management and authentication methods for securing 802.11-based transmissions WPA (Wi-Fi Protected Access), works with all Wi-Fi variants : 802.11b (11 Mbps on the 2.4 GHz band) 802.11a (54 Mbps on the 5 GHz band) and 802.11g (54 Mbps on the 2.4 GHz band).

WPA consists of two parts :

- Dynamic management of encryption keys for use with 802.11 WEP.
- Secondly, user authentication, hitherto absent from WEP, based on the Extensible Authentication Protocol (EAP), originally designed for authenticating users connecting via modem using the Point-to-Point Protocol (PPP), which significantly strengthens the protocol.

The most common authentication methods used with EAP are :

- EAP-TLS (Transport Layers Security) : certificate-based authentication of client equipment and authentication server.
- EAP-TTLS (Tunneled Transport Layers Security) : mixed certificate and password authentication through secure tunnel generation.
- EAP-MD5 (Message Digest) : simple password authentication.
- PEAP (Protected EAP) : simple password authentication via secure encapsulation.
- EAP-FAST : simple password authentication via secure encapsulation (Cisco protocol).
- LEAP (Lightweight EAP) : simple password authentication via secure encapsulation (Cisco protocol).

The authentication server is located on the access point, or on an authentication server, which can be an AAA FreeRadius server.

802.11i, also known as WPA2, is the successor to WPA (Wireless Protected Access), which itself corrected the shortcomings of WEP 802.11i uses AES (Advanced Encryption Standard) as the communications encryption mechanism, for transmissions using 802.11a, 802.11b and 802.11g technologies.

In terms of authentication, the 802.11i protocol provides two modes :

- WPA Personal allows you to set up a secure infrastructure without the need for an authentication server, and is based on the use of a shared key, or PSK (Pre-Shared Key), set on the access point and on client workstations.

Unlike WEP, there's no need to enter a passphrase, which is transformed into a PSK using a hash algorithm.

- WPA Enterprise requires the use of an authentication infrastructure based on the use of an authentication server, generally a RADIUS (Remote Authentication Dial-in User Service) server, and a network controller (the access point).

V. RADIUS AUTHENTICATION SERVER [24]

V.1. Presentation

The RADIUS (Remote Authentication Dial-In User Service) protocol, originally developed by Livingston, is a standard authentication protocol defined by a number of RFCs.

RADIUS works on the basis of a client/server system that defines remote user access to a network. It is the protocol of choice for Internet Service Providers (ISPs), as it is relatively standard and offers accounting features enabling ISPs to bill their customers accurately.

The RADIUS protocol relies mainly on a server (the RADIUS server), connected to an identification base (database, LDAP directory, etc.) and a RADIUS client, called NAS (Network Access Server), acting as intermediary between the end-user and the server. All transactions between the RADIUS client and the RADIUS server are encrypted and authenticated using a shared secret.

It should be noted that the RADIUS server can act as a proxy, transmitting client requests to other RADIUS servers.

V.2. Operation

RADIUS operates on the basis of a scenario similar to the following :

- ✓ A user sends a request to the NAS to authorize a remote connection ;
- ✓ The NAS forwards the request to the RADIUS server ;
- ✓ The RADIUS server consults the identification database to find out what type of identification scenario the user has requested. Either the current credential is accepted, or the user is requested to use another credential method. The RADIUS server returns one of four responses :

- **ACCEPT :** identification successful ;
- **REJECT :** identification failed ;
- **CHALLENGE :** the RADIUS server requests additional information from the user and proposes a "challenge" ;

There's a response called CHANGE PASSWORD where the RADIUS server asks the user for a new password. Change-password is a VSA (Vendor - SpecificAttributes) attribute, i.e. it's specific to a vendor, and in this case, it's a Microsoft attribute and, to be more precise, that of MS-Chap v2. It doesn't belong to the standard radius attributes defined in RFC 2865.Following this so-called authentication phase, an authorization phase begins, in which the server returns the user's authorizations. The following diagram summarizes the elements involved in a system using a RADIUS server :

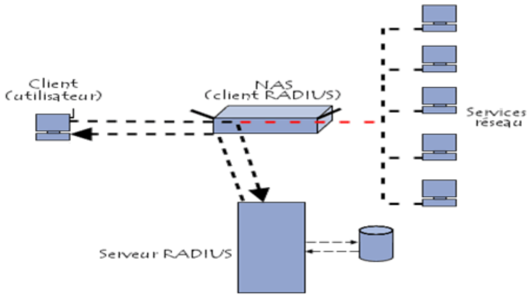


Figure I: 6 diagram showing the elements involved in a system using a RADIUS server

V.3. Standardization

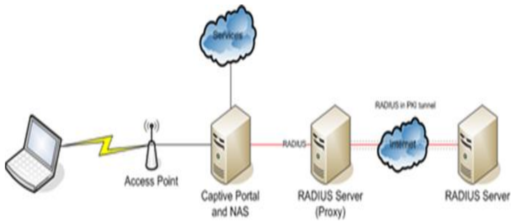


Figure 1 :7 : Radius server standardization diagram

The latest version of the RADIUS protocol is standardized by the IETF in two RFCs : RFC 2865 (RADIUS authentication) and RFC 2866 (RADIUS accounting) of June 2000. The successor to the RADIUS protocol could be the Diameter protocol. The protocol is often referred to as AAA (Authentication Authorization Accounting), the authorization phase (definition of access rights) being performed during the identification response (addition of attributes to the "Authentication Response" packet). Another example of an AAA protocol could have been Cisco's TACACS, but it is proprietary ; and since the publication of the 802.1X standard, which gives the Radius protocol as the only example of implementation in Appendix D, Radius has become a de facto AAA standard.

V.4. Utility

The original purpose of RADIUS was to enable Internet service providers to authenticate remote users using PSTN modem connections from multiple servers but a single user base. In the previous situation, user names and passwords had to be duplicated in every device that needed to identify users. Similarly, POP (e-mail) authentication had to be managed in this way. Web site identification by name and password is also managed by RADIUS, and the Apache server is one of the most widely used Radius clients. This is still the most common use of the RADIUS protocol : name and password for Internet connection, but more and more wireless and wired networks are also using it to identify users.

The RADIUS protocol provides a link between identification requirements and a user base, transporting authentication data in a standardized way. The authentication operation is initiated by a RADIUS service client, which may be a

Network Access Server (NAS), a wireless network access point, a firewall, a switch or another server. The server processes it by accessing an external database, if necessary : SQL database, LDAP directory, machine or domain user accounts ; a Radius server has a number of interfaces or methods for this.

V.5. Identification Operation

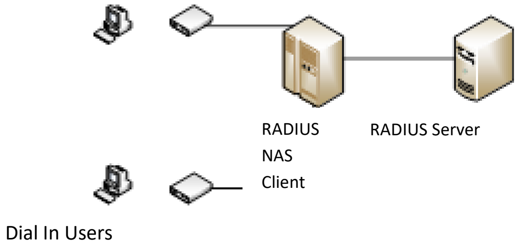


Figure I. 8 : Radius client diagram between user workstations and Radius server

The user station (supplicant in the RFCs) transmits an access request to a RADIUS client to enter the network. This client is responsible for requesting information identifying the user : the username (login) and password, for example. Depending on the protocol, the RADIUS client generates an Access-Request containing the authentication information. The RADIUS server can process this request itself, or forward it to another RADIUS server via a mechanism known as a Radius Proxy. The Radius server responsible for final identification (called Home Radius) can process the request if it has enough elements in the Access-Request, or request additional information by sending back an "Access Challenge" packet, to which the client responds with another "Access-Request", and so on. Exchanges are retransmitted by the chain of intermediate Radius proxy servers in both directions. When the Radius server has enough elements (up to a dozen exchanges for complex EAP-type protocols), the RADIUS server validates or refuses identification by sending back a : Access-Accept or Access-Reject.

V.6. Authorization[25]

RADIUS identification can be enriched with authorization, e.g. for an ISP client its IP address, its maximum connection time, its inactivity time. All these parameters are defined by packet attributes in the RFCs, in this case attribute 8, better known by its "user-friendly" name Framed-IP-Address, although the protocol actually only knows numbers, and the Session-Timeout and Idle-Timeout attributes. Standard attributes are defined in the RFCs, while vendor-specific attributes (VSAs) are multiplexed in attribute 26 : each vendor is assigned a unique number by which it can be identified, and one byte of this attribute defines a VSA number, enabling each vendor to define up to 255 vendor-specific attributes for its hardware. The Radius server adapts to these "dialects" using attribute dictionaries.

V.7. Accounting

The second function of a Radius server is accounting, providing both access logging and billing. Defined by different RFCs, managed on different UDP ports (1646 or 1813 fors the most common, while identification is done on ports 1645 or 1812), this function is often handled by a different program or even a different server. Accounting is based on two main packet types : Accounting Start and Accounting Stop. A session is defined as the interval between a Start and a Stop. The Accounting Start packet issued by the Radius client after the user has logged on following a successful identification phase contains basic data : user name (but not the password, which is not needed here), assigned IP address, date and time of connection, type of connection, type of service, etc. When the user logs off from the service, or when the Radius client logs off from the service, the Radius client sends the user an Accounting Start packet.

When the user disconnects from the service, or when the Radius client disconnects him/her due to inactivity, connection timeout or other reasons, the Radius client sends an Accounting Stop packet with the same session identifier. The Radius server can then close the session and log the disconnection, often with a large number of parameters in the Stop packet : connection time, type of use, number of packets and bytes exchanged according to the various protocols, and possibly more confidential information on sites visited or content exchanged.

There are other types of accounting packets : Intermediate (issued at periodic intervals by the client between Start and Stop, useful in case the Stop is lost), On (the Radius client has started) and Off (the Radius client is about to stop), the latter for the record - it's rare for a device to warn before breaking down or crashing. To facilitate the link between the identification phase and the accounting phase (the Radius server may have received hundreds of other requests in between), the Class attribute is sent to the client with the Access-Accept packet ; the Radius client is instructed to send it back unchanged in the Accounting Start packet. The Radius server can therefore include in this attribute all the information needed to link a successful identification, often accompanied by a reservation of resources - channel, PVC or IP address, for example - with the actual use of these resources.

In the event that the operation is aborted (there is no corresponding Accounting Start packet after successful identification), a mechanism must restore the reserved resources ; most implementations use a timing mechanism for this (phantomaccounting record). Resources reserved by identification and occupied by Accounting Start are normally released by the Accounting Stop packet, which means, for example, that a Radius server can only allocate IP addresses if it also manages the accounting function. Accounting also has a legal function : access to the Internet must be identified, and every user must be traceable at least to an account or credit card number, which is why the accounting function is always activated by ISPs, and the records kept : on the basis of a court order, the ISP can provide the identification at a given moment of any IP address.

V.8. Limitations

- RADIUS was designed for modem-based identification over slow, insecure links, which is why the UDP protocol was chosen, as explained in RFC2138. This technical choice of a non-aggressive protocol leads to laborious exchanges based on retransmission timeouts, and exchanges of acknowledgements of receipt, which were justified as long as Internet connections were based on UDP's "bottle to the sea" principle, but are no longer needed, for example, between operators in roaming or proxy activities Radius → Diameter uses TCP or SCTP
- RADIUS bases its identification on the sole principle of the name/password pair ; perfectly adapted at the time (1996), this notion had to be adapted, for example, to identify mobile terminals by their IMEI number or by their call number (Calling-Station-ID in Radius) without a password (whereas the RFC forbids empty passwords !).
- RADIUS ensures unencrypted transport, with only the password encrypted by hashing ; the protocol's relative security is based solely on the shared secret, requiring exchanges between client and server to be secured by physical security or VPN → Diameter can use IPSec or TLS
- RADIUS limits attributes, managed as a "Pascal" string with a leading byte giving the length, to 255 bytes, consistent with the notion of name/password, but unsuited to any attempt to introduce biometrics (fundus, fingerprint) cryptography (certificate) → Diameter uses 32-bit attributes instead of 8 (already present in some RADIUS EAP extensions, notably TTLS)
- RADIUS is strictly client-server, leading to discussions and fights over proprietary protocols when a server legitimately needs to kill a pirate session on a client → Diameter has mechanisms for the server to call the client.
- RADIUS does not provide a mechanism for identifying the server ; yet impersonating a server is an excellent way of collecting names and passwords → EAP provides mutual identification of client and server

V.9. RADIUS extensions

- EAP (Extensible Authentication Protocol) is a protocol designed to extend the functions of the Radius protocol to more complex types of identification ; it is independent of Radius client hardware and negotiated directly with the supplicant (client workstation, access terminal). This has enabled it to be deployed rapidly on a maximum number of network devices, since it uses only two Radius attributes as transport protocol, and has led to an explosion of EAP types: EAP-MD5 defined in the RFC as an example, but also EAP-TLS, EAP-TTLS, EAP-PEAP (version 0 Microsoft, version 1 Cisco, version 2 soon), EAP-MS-CHAP-V2, EAP-AKA, EAP-LEAP and EAP-FAST (Cisco), EAP-SIM, etc.
- 802.1X is a protocol providing port-based identification for network access ; it is not explicitly linked to RADIUS in principle, and uses the terms "AAA server" and "AAA protocol" in all its definitions, but Appendix D of the reference document mentions RADIUS alone as an "example" of an AAA protocol and server. All known 802.1X implementations therefore rely on RADIUS.
- Diameter is not really an extension but a successor to the RADIUS protocol ; it is TCP/SCTP-based, whereas Radius is UDP-based, uses large attributes (Radius is limited to 254 bytes per attribute) and is intended for exchanges between servers over secure links ; Diameter servers are generally Radius-compatible. A number of Diameter attribute types are already found in EAP-TTLS, for example.

VI. DEPLOYMENT STUDY

VI.1.1. Introduction

In this chapter, we will demonstrate the various steps involved in configuring the Radius server. In Windows Server 2012, we'll set up the AD DS (Active Directory Domain Services) domain, in which we'll create a group, a user account and then activate the AD (Active Directory) certificate. We'll then install and configure the NAP (Network Access Protection) to interact with our Access Point.

VI.1.2. Operating System Used

Windows Server 2012 is our chosen environment for deploying our radius server.

VI.1.3. Radius Server Installation And Configuration

Once the Windows server operating system has been installed, we'll proceed with the essential configurations.

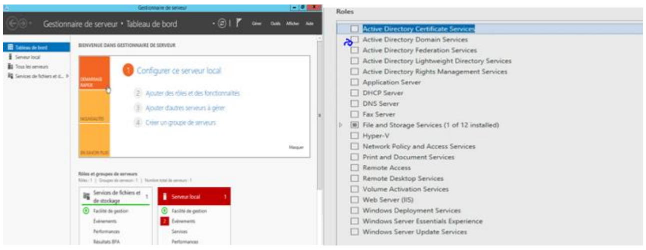
VI.1.4. Configuring Adds (Active Directory Domain Services)

This is the first role to be activated on the server.

It manages everything that happens on the server, including users and user groups.

In the Server Manager:

- ✓ Go to Add roles
- ✓ Click on ADDS


Gestionnaire de serveur
Gestionnaire de serveur • Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
Services de fichiers et d...
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
1 Configurer ce serveur local
2 Ajouter des rôles et des fonctionnalités
3 Ajouter d'autres serveurs à gérer
4 Créer un groupe de serveurs
Masquer
Rôles et groupes de serveurs
Services de fichiers et de stockage 1
Serveur local 1
Facilité de gestion
Événements
Performances
Résultats BPA
Services
Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Figure II. 1 : Adding ADDS roles and functions.

- ✓ We click on add features, then next.
- ✓ We confirm the installation

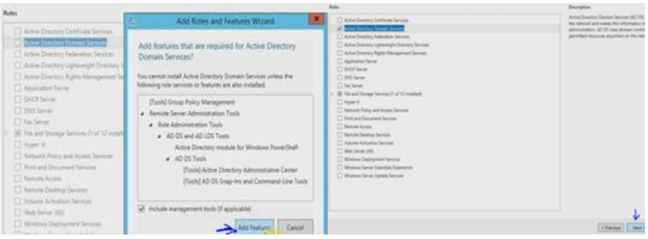
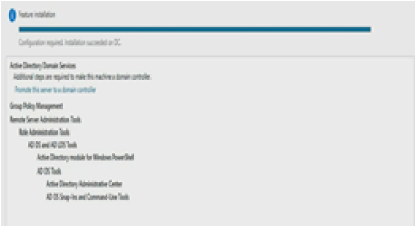


Figure II. 2 : Confirmation that ADDS functionality has been added.



Feature installation

Configuration required. Installation succeeded on DC.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

Figure II. 3 : Successful feature installation.

We go to the AD domain services wizard

- ✓ Check New forest
- ✓ Enter the domain name
- ✓ Enter the restore password and ADDS installation is complete.

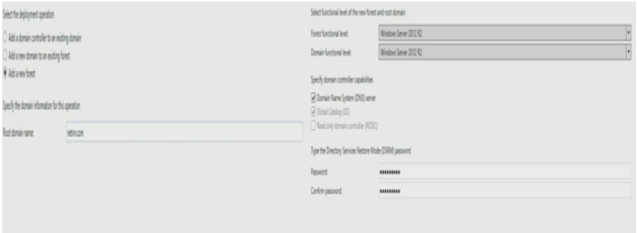


Figure II. 4 : Confirmation of domain name and restore password.

VI.1.5. User Group Creation

- ✓ Access the domain name we've created
- ✓ Right-click on Users
- ✓ Go to new group
- ✓ Create our group, then click ok

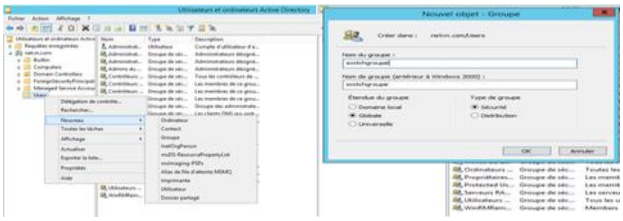
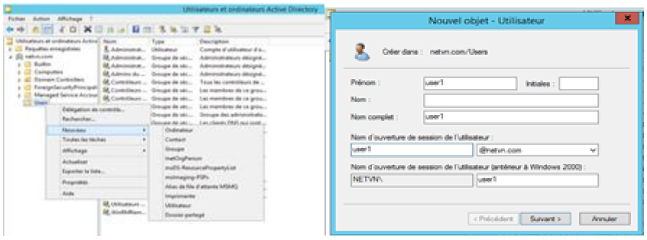


Figure II. 1: Création d'un groupe d'utilisateurs.

VI.1.6. Création Des Utilisateurs

- ✓ On fait un clic droit sur utilisateurs (Users)
- ✓ On va dans nouveau puis utilisateur
- ✓ On crée l'utilisateur et on fait suivant



Nouvel objet - Utilisateur

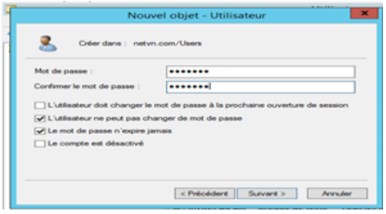
Créer dans : netvn.com/Users

Prénom : user1 Initiales :
Nom :
Nom complet : user1
Nom d'ouverture de session de l'utilisateur :
user1 @netvn.com
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
NETVN\ user1

< Précédent | Suivant > | Annuler

Figure II.6: User creation

- ✓ Give the password to the user
- ✓ Do next and finish



Nouvel objet - Utilisateur

Créer dans : netvn.com/Users

Mot de passe : •••••••
Confirmer le mot de passe : •••••••

□ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
☑ L'utilisateur ne peut pas changer de mot de passe
☑ Le mot de passe n'expire jamais
□ Le compte est désactivé

< Précédent | Suivant > | Annuler

Figure II. 7 : Password creation for the user.

VI.1.7. Integrating Users Into A Group

- ✓ Right-click on the group
- ✓ Go to property then member to integrate the user into the group

- Click on ok

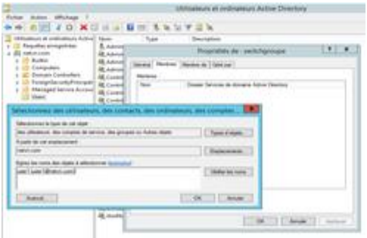


Figure II. 8 : Integrating users into a group.

VI.1.9. Certificate Activation

Certificate activation is like a lifetime given to the authenticating user ; once the time limit has expired, the user will no longer be able to access the network.

- ✓ Click on server role
- ✓ Click on add role
- ✓ Add functionalities
- ✓ Check Active Directory Certificate Service, then Next
- ✓ Installation begins

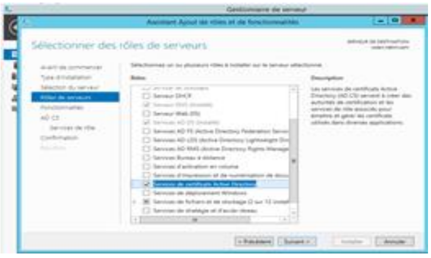


Figure II. 9 : Activating Active Directory certificates.

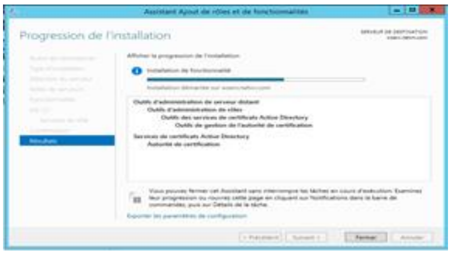

Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
Installation de fonctionnalité
Résultats

Figure II. 10 : Progress of Active Directory certificate installation.

Once installation is complete, click on Close ;

VI.1.8. Activating A Certification Authority

- ✓ Go to Active Directory certificate services configuration
- ✓ Click Next and select Certification Authority
- ✓ Click on Next

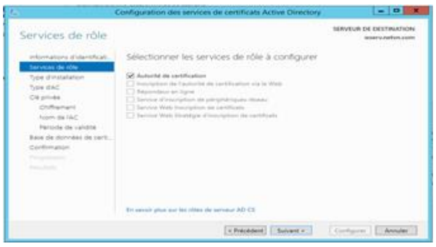

Configuration des services de certificats Active Directory
Services de rôle
Sélectionner les services de rôle à configurer
Autorité de certification

Figure II. 11 : Selecting the certification authority.

Select an encryption provider and click on Next

- ✓ Specify a validity period, then click on configure.
- ✓ Configuration is complete, click on close

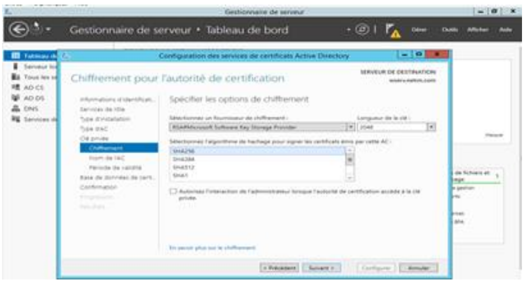

Gestionnaire de serveur • Tableau de bord
Configuration des services de certificats Active Directory
Chiffrement pour l'autorité de certification
Spécifier les options de chiffrement

Figure II. 12 : Encryption provider selection.

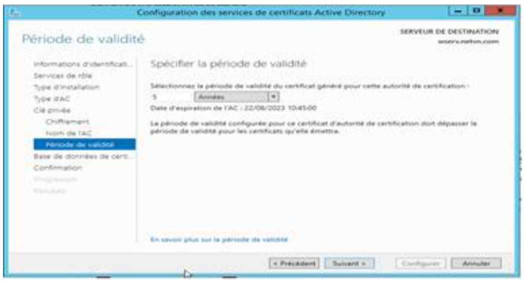

Configuration des services de certificats Active Directory
Période de validité
Spécifier la période de validité

Figure II. 13 : Validity period specification.

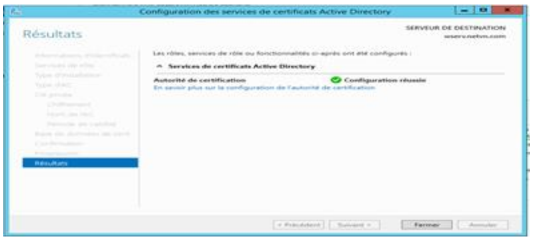

Configuration des services de certificats Active Directory
Résultats
Services de certificats Active Directory
Autorité de certification
Configuration réussie

Figure II. 14 : Configuration success.

VI.2.1. Activation Of The Nap Function

NAP (Network Access Protection) is a technique for controlling user access to the network. NAP is a feature of the NPS (Network Policy Server) server role; we need to enable this feature to achieve RADIUS server configuration.

- ✓ Click on add roles and functionalities
- ✓ Click on Next
- ✓ Check Policy and Network Access Service
- ✓ Click on Add features
- ✓ Click on Next
- ✓ Select the role services to be installed, click on next and install

Once installation is complete, click on Close

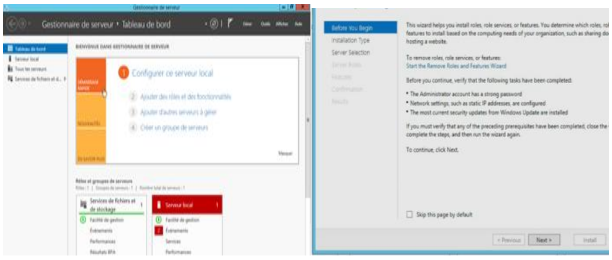

Gestionnaire de serveur • Tableau de bord
Configurer ce serveur local
Before You Begin

Figure II. 15 : Adding roles and functionalities.

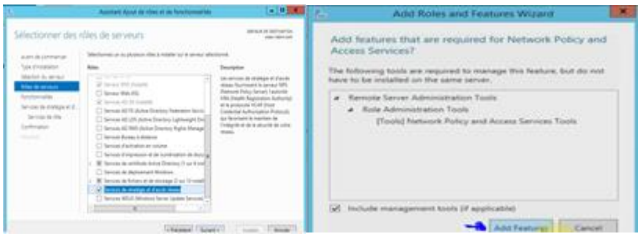

Sélectionner des rôles de serveurs
Add Roles and Features Wizard
Add features that are required for Network Policy and Access Services?
Add Features
Cancel

Figure II. 16: Adding policy and network access services.

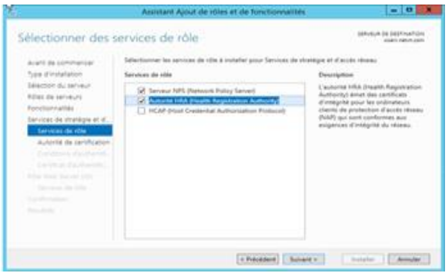

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des services de rôle
Serveur NPS (Network Policy Server)
Autorité HRA (Health Registration Authority)
HCAP (Host Credential Authorization Protocol)

Figure II. 17 : Selecting and installing role services.

VI.2.2. Configuring The Radius Server Using Nps

The NPS (Network Policy Server) manages authentication and authorization according to the different connection modes ; it manages access to local resources via a remote connection.

- ✓ Right-click on the NAP
- ✓ Select NPS server, then access the NPS interface to configure the Radius server and client.
- ✓ Select connection type (802.1X)
- ✓ Check secure wireless connections ; at this point, our Radius server is configured.

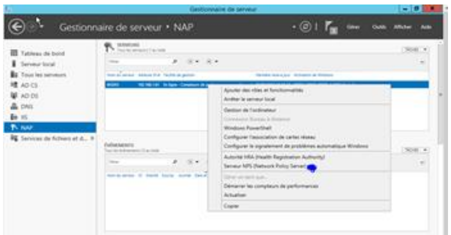


Figure II. 18 : Selecting the NPS.

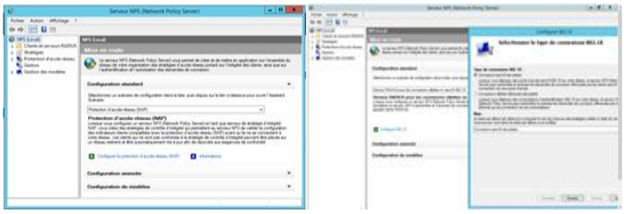


Figure II. 19 : Selection of configuration scenario and 802.1X connection type.

VI.2.3. RADIUS CLIENT CONFIGURATION

After configuring the Radius server, in the Configure 802.1X :

- ✓ Click on Next
- ✓ Then click on Add new Radius client
- ✓ Enter the access point's name and IP address
- ✓ Enter a secret password that the access point will share with the Radius server, then click OK.
- ✓ Our Radius client (Access Point) is now in the server

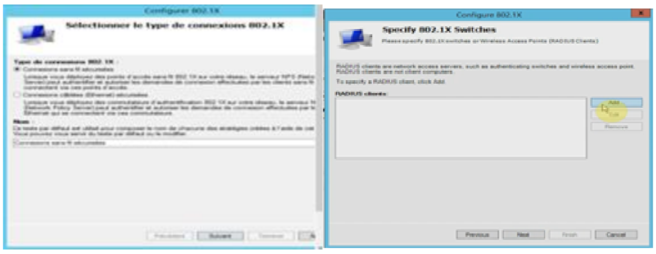


Figure II. 20 : Add a Radius Client

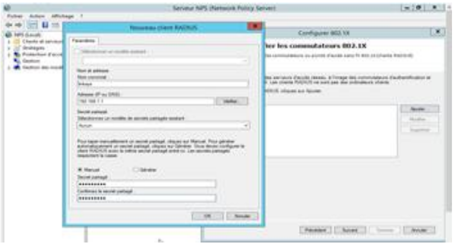


Figure II. 21 : Radius client configuration.

We select the name of our Radius Client (Access Point)

- ✓ Click on Next
- ✓ Configure the authentication method, then next
- ✓ We specify the group we've created, add it and then click next.
- ✓ And that's the end of our configuration

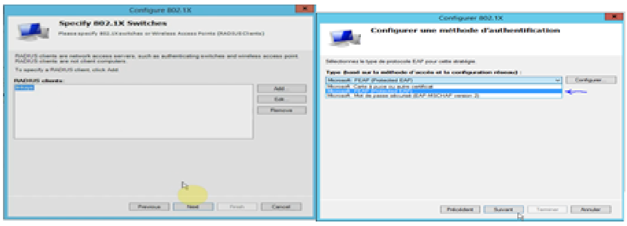
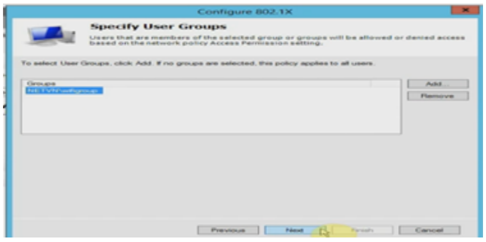


Figure II. 22 : Access point name selection and choice of authentication method



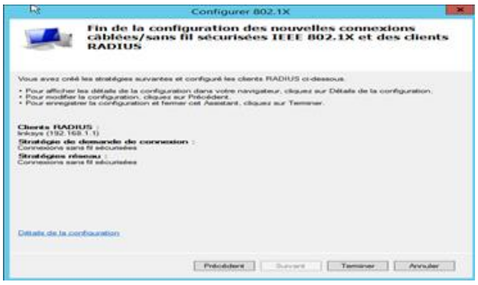
Configure 802.1X

Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Figure II. 23 : Specifying the user group.



Configurer 802.1X

Fin de la configuration des nouvelles connexions câblées/sans fil sécurisées IEEE 802.1X et des clients RADIUS

Vous avez créé les stratégies suivantes et configuré les clients RADIUS ci-dessous.

- Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration.
- Pour modifier la configuration, cliquez sur Précédent.
- Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer.

Clients RADIUS :
linksys (192.168.1.1)
Stratégie de demande de connexion :
Connexions sans fil sécurisées
Stratégies réseau :
Connexions sans fil sécurisées

Détails de la configuration

Figure II. 24 : End of the configuration

VI.2.4. ACCESS POINT CONFIGURATION

- ✓ Go to the search engine, enter the address of the access point and validate.
- ✓ In the access point, click on Wireless, then Wireless Security
- ✓ Select security mode, then Ok
- ✓ Enter the IP address of the Radius server and enter the secret password you created in the Radius server.
- ✓ Ok and you're done

Figure II. 25 : Entering the IP address.

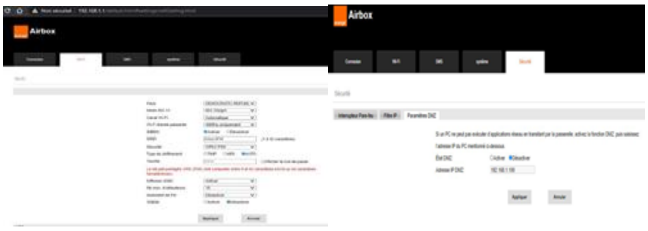
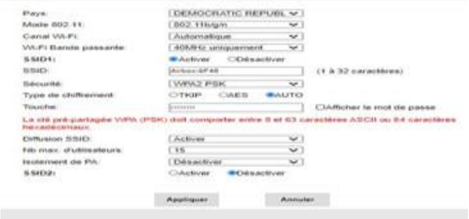
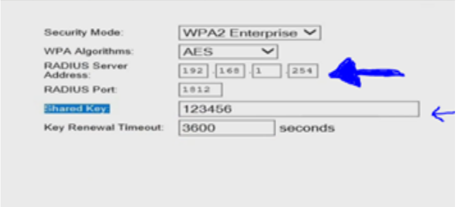


Figure II. 26 : Configuration steps.



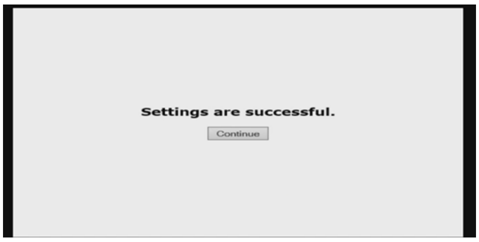
Pays: DEMOCRATIC REPUBL
Mode 802.11: 802.11b/g/n
Canal Wi-Fi: Automatique
Wi-Fi Bande passante: 40MHz uniquement
SSID1: ● Activer ○ Désactiver
SSID: Airbox-6F48 (1 à 32 caractères)
Sécurité: WPA2 PSK
Type de chiffrement: ○ TKIP ○ AES ● AUTO
Touche: •••••••• □ Afficher le mot de passe
La clé pré-partagée WPA (PSK) doit comporter entre 8 et 63 caractères ASCII ou 64 caractères hexadécimaux.
Diffusion SSID: Activer
Nb max. d'utilisateurs: 15
Isolement de PA: Désactiver
SSID2: ○ Activer ● Désactiver

Figure II. 27 : Safety mode selection.



Security Mode: WPA2 Enterprise
WPA Algorithms: AES
RADIUS Server Address: 192 . 168 . 1 . 254
RADIUS Port: 1812
Shared Key: 123456
Key Renewal Timeout: 3600 seconds

Figure II. 28 : Entering IP address and secret password



Settings are successful.

Figure II. 29 : Configuration success.

CONCLUSION

To conclude our article, we've deployed our Radius server and all its associated roles to manage authentication and, at the same time, make our server architecture more functional and secure.

As our article is about "STUDYING SECURING A WIRELESS NETWORK WITH RADIUS SERVER", we feel obliged to conclude with a few words.

It should be noted, however, that while Wi-Fi networks offer considerable advantages in terms of comfort and usability, they are not suitable for heavy loads, and it should be borne in mind that the costs saved by avoiding Ethernet cabling for user workstations may be outweighed by other costs that may not have been thought of at the outset. In practice, Wi-Fi networks perform well in client-server mode with short exchanges (e.g. Internet browsing), which explains their success with local companies.

The network is secured via the RADIUS server, and client users who are not registered as authorized users in the server will not be able to access the network, or even perceive its existence. In the event that a person is in possession of the network's SSID, he or she will still not be able to access it without the certificates installed on both the client workstations and the server. Authentication information is exchanged in encrypted form, using an improved protocol which has not yet been broken. In the event, the chosen solution has been installed, and all tests have been successfully completed. We hope it will be safer, more efficient and, above all, more secure.

To conclude, one of our first recommendations is not to connect wireless equipment with the default options activated. In particular, as soon as an access point is connected to the wired network, a password must be set to authorize access to the configuration menus. MAC address filtering is also recommended, although you should be aware of the limitations of this technique. It's always one more barrier for hackers to overcome. Finally, wherever possible, it is advisable to use AAA Radius authentication mechanisms rather than those configured by default. Finally, it should be remembered that the security mechanisms implemented by 802.11b do not protect access to the wireless network or the confidentiality of exchanges, and that it is therefore advisable to opt for equipment that supports the 802.11i standard.

REFERENCES

1. Ali MAHBOUB, Ali SENOUSSI, Gestion 13(02), 2019
2. A AMRI, FZ LAKEHAL, F SADOUKI, 2014
3. Amir Lamine, Editions Université Européennes, 2015
4. Ali Sadiqui ISTE GROUP, 2019
5. El Hadi Kenane, 2018
6. GUY Pojolle, Editions Eyrolles, 2014
7. http:/ /www.google.com/configuration of the Radius server under Windows server 2012, consulted on 02/05/2023;
8. http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047.pdf
9. http:/ /www.kismetwreless.net
10. Ilunga Mbuyamba Elisée, Kabuyaya Bahavira Patrick, International Journal of innovation and Applied studies 39(3), 2023
11. IT, AKademy, 2020
12. JUSTE Raimbault, University, Paris 7 Denis Diderot, 2018
13. Ken Chen ISTE GROUP, 2014
14. Maryline Laurent, Armen Khatchatourov, Signes de confiance, l'impact des labels sur la gestion des données personnelles, 2018
15. Olivier Fruchier, Philippe Egea, Faissal Bakati,
16. Ouelhadj Mohamed Amine, Université Mouloud Mammeri, 2015
17. Raphael Grevisse Yende, 2018
18. Rochdi Sarraj, Ecole Nationale Supérieure des Mines de Paris, 2013
19. Sylvain Métille, Jusletter, 2017, Huu Quynh Nguyen, Paris, ENST, 2008

20. Thierry Talbert, J3Ea21, 2008, 2022
21. PATRICE KADIONIK, ENSEIRB, 2002
22. Stefan Lueders, 2020
23. Jean Lucat, Global Security, 2016
24. Robin Heron, Stéphane Safin, Anne Bationo-Tillon EPIQUE, 2019
25. Wajih Abdallah, Sami Mnasri, Thierry Val Journées Nationales des communications Terrestres (JNCT 2019), 2019