ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

SERVICE AAA SUR UN RÉSEAU WIFI

ENCADRÉ PAR :

M.AKIL

PRÉSENTÉ PAR :

ANASS RHOUZLADI
YOUNES GUERMAT
HNIKICH REDA
RAOUI ABDELKAMEL

ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

SOMMAIRE

INTRODUCTION

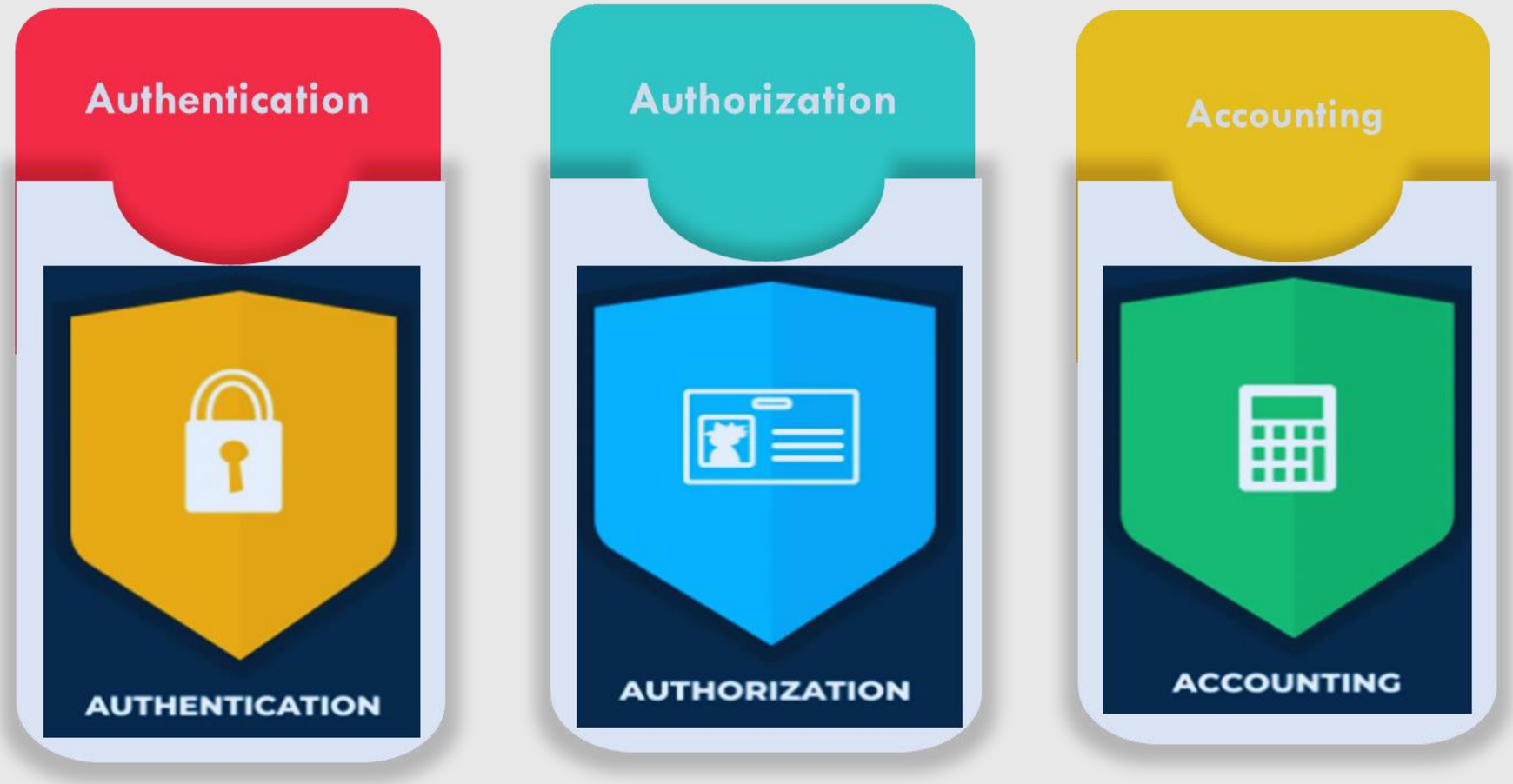
Le Service AAA, qui signifie "Authentication, Authorization, and Accounting" (Authentification, Autorisation et Comptabilité), est une infrastructure essentielle dans la gestion et la sécurisation des réseaux, y compris les réseaux WiFi. Il fournit un ensemble de fonctions cruciales pour contrôler l'accès au réseau, garantir l'identité des utilisateurs, leur accorder les autorisations appropriées et suivre leur activité sur le réseau.

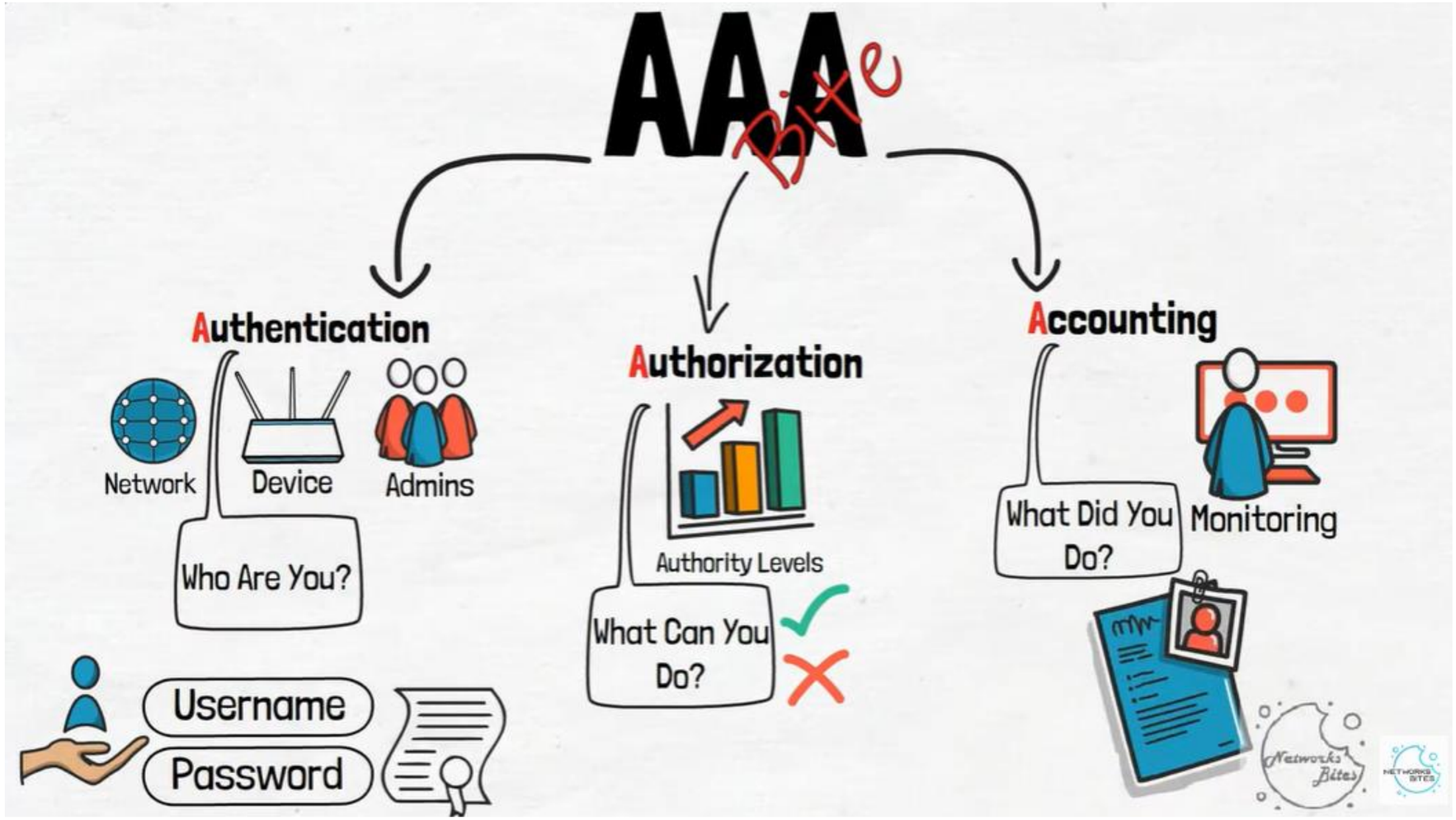
ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

LES 3 FONCTIONS DU AAA

Dans les réseaux informatiques, la sécurité et la gestion des accès sont des aspects cruciaux, notamment dans les réseaux Wi-Fi. Pour assurer un contrôle d'accès efficace, les réseaux sans fil utilisent souvent des services AAA, qui sont des systèmes d'Authentification, d'Autorisation et de Comptabilité. Dans cet exposé, nous allons explorer en détail le fonctionnement et l'importance du service AAA dans les réseaux Wi-Fi.

LES 3 FONCTIONS DU AAA




AAA
Bite
Authentication
Network
Device
Admins
Who Are You?
Username
Password
Authorization
Authority Levels
What Can You Do?
Accounting
What Did You Do?
Monitoring
Networks Bites
NETWORKS BITES

ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

```
R1(config)#username Admin1 secret anas2003
R1(config)#
R1(config)#
R1(config)#aaa new
R1(config)#aaa new-model
R1(config)#
R1(config)#aaa authentication login def
R1(config)#aaa authentication login default local
R1(config)#
R1(config)#line console 0
R1(config-line)#
R1(config-line)#login authe
R1(config-line)#login authentication def
R1(config-line)#login authentication default
R1(config-line)#exit
```

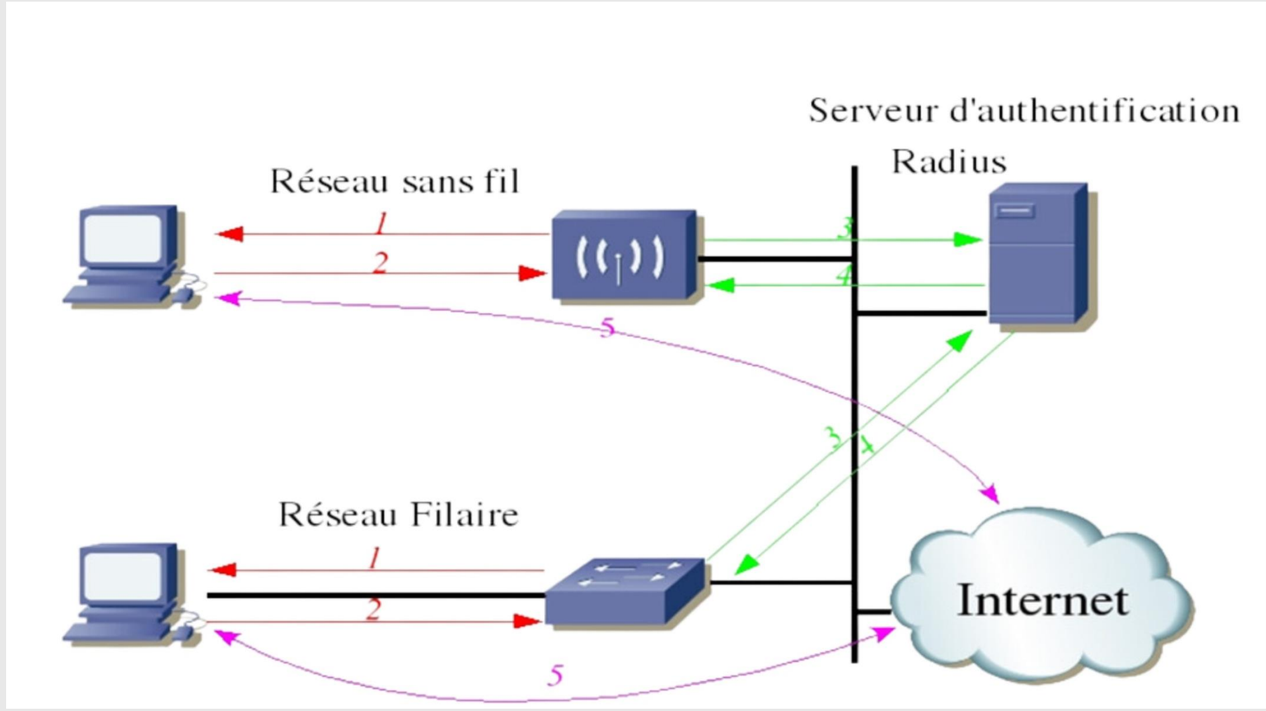
1/AUTHENTIFICATION

L'authentification est le premier pilier du service AAA. Elle consiste à vérifier l'identité des utilisateurs qui tentent d'accéder au réseau WiFi. Cette étape peut se faire de différentes manières, telles que l'utilisation de mots de passe, de certificats numériques, d'identifiants biométriques ou d'autres mécanismes d'authentification. L'objectif est de s'assurer que seuls les utilisateurs légitimes sont autorisés à accéder au réseau . Plusieurs mécanismes peuvent être utilisés pour vérifier l'identité des utilisateurs. Parmi les plus courants :

- Mots de passe : Les utilisateurs doivent saisir un nom d'utilisateur et un mot de passe correspondant pour accéder au réseau. Ces informations sont comparées à celles stockées dans une base de données d'authentification.
- Certificats numériques : Les utilisateurs peuvent être tenus de présenter un certificat numérique qui atteste de leur identité. Ces certificats sont généralement émis par une autorité de certification (CA) de confiance.

LE PROTOCOLE 802.1X

Le protocole 802.1X permet de contrôler l'accès d'équipements informatiques à des réseaux locaux, qu'ils soient filaires ou Wi-Fi.



1/AUTHENTIFICATION

PROTOCOL SSH

Le protocole SSH, qui signifie "Secure Shell" (ou "coquille sécurisée"), est une manière sécurisée de communiquer et d'accéder à un ordinateur sur un réseau non sécurisé, comme Internet.

1. Authentification sécurisée
2. Cryptage des données
3. Accès à distance
4. Transfert de fichiers sécurisé


```
R1(config)#aaa authentication log
R1(config)#aaa authentication login SSH-LOGIN local
R1(config)#line vty 0 4
R1(config-line)#login aut
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport in
R1(config-line)#transport input ssh
R1(config-line)#exit
```

2/AUTORISATION

L'autorisation, deuxième pilier du service AAA, intervient après la vérification de l'identité de l'utilisateur et consiste à déterminer les autorisations appropriées pour cet utilisateur. Voici un détail sur cette étape :

- Privilèges d'accès au réseau : Après l'authentification, le service AAA accorde des privilèges d'accès au réseau, tels que l'accès à Internet, à des serveurs spécifiques ou à des ressources partagées, en fonction des autorisations définies pour l'utilisateur.

Ressources autorisées :
Le service AAA, une fois l'authentification réalisée, attribue des privilèges d'accès spécifiques au réseau et détermine les ressources autorisées, telles que des fichiers, des dossiers ou des applications, en fonction des autorisations de l'utilisateur.

Actions autorisées : En plus de définir les ressources auxquelles l'utilisateur peut accéder, l'autorisation spécifie également les actions qu'il est autorisé à effectuer sur ces ressources. Cela peut inclure la lecture, l'écriture, la modification, la suppression, l'exécution d'applications, etc.

3/ACCOUNTING

accounting: est la troisième composante du service AAA. Elle implique la collecte et l'enregistrement des données sur l'utilisation du réseau par les utilisateurs. Cela comprend des informations telles que la durée de la session, la quantité de données transférées, les services utilisés, etc. Ces données sont essentielles pour la gestion du réseau, la facturation des services et la détection des éventuelles activités suspectes ou non autorisées.

- La durée de la session : le temps pendant lequel un utilisateur est connecté au réseau, mesuré en heures, minutes et secondes.
- La quantité de données transférées : le volume de données échangées entre l'utilisateur et le réseau, souvent mesuré en octets, kilooctets ou mégaoctets
- Les services utilisés : les applications ou les protocoles réseau spécifiques auxquels l'utilisateur a accédé pendant sa session, comme la navigation web, le streaming vidéo, l'envoi de courriers électroniques, etc.
- D'autres informations pertinentes, telles que l'adresse IP de l'utilisateur, le type d'appareil utilisé, l'emplacement géographique, etc.

ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

LES BENEFITS DE AAA FRAMEWORK

Le framework AAA (Authentication, Authorization, Accounting) offre plusieurs avantages importants dans la gestion des réseaux informatiques :

Sécurité renforcée :
En vérifiant l'identité des utilisateurs, en contrôlant leurs privilèges d'accès et en enregistrant leurs activités, le framework AAA aide à renforcer la sécurité du réseau et à prévenir les accès non autorisés.

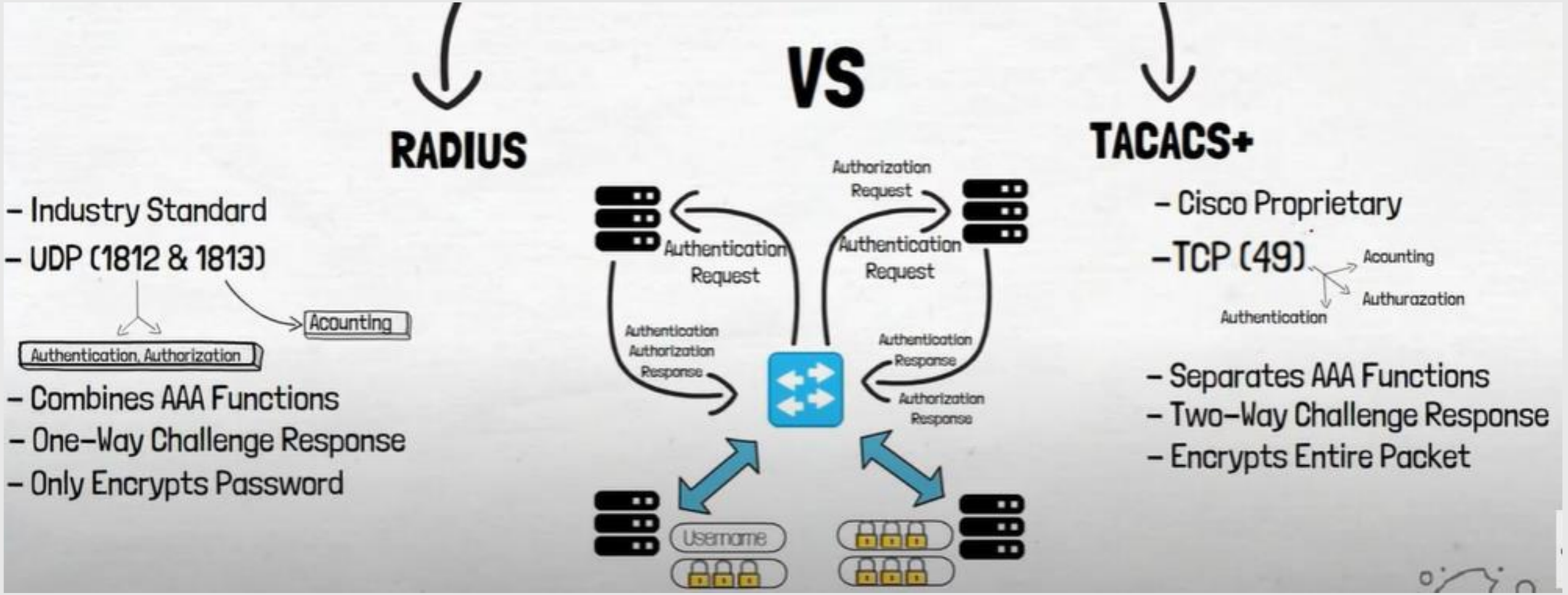
Gestion centralisée des accès :
Le framework AAA permet une gestion centralisée des politiques d'accès, ce qui simplifie l'administration du réseau en permettant aux administrateurs de définir et de contrôler les politiques depuis un emplacement central.

Optimisation des ressources :
En collectant des données sur l'utilisation du réseau, le framework AAA permet aux administrateurs de surveiller et de gérer les ressources réseau de manière plus efficace, en identifiant les goulots d'étranglement et en planifiant les capacités.

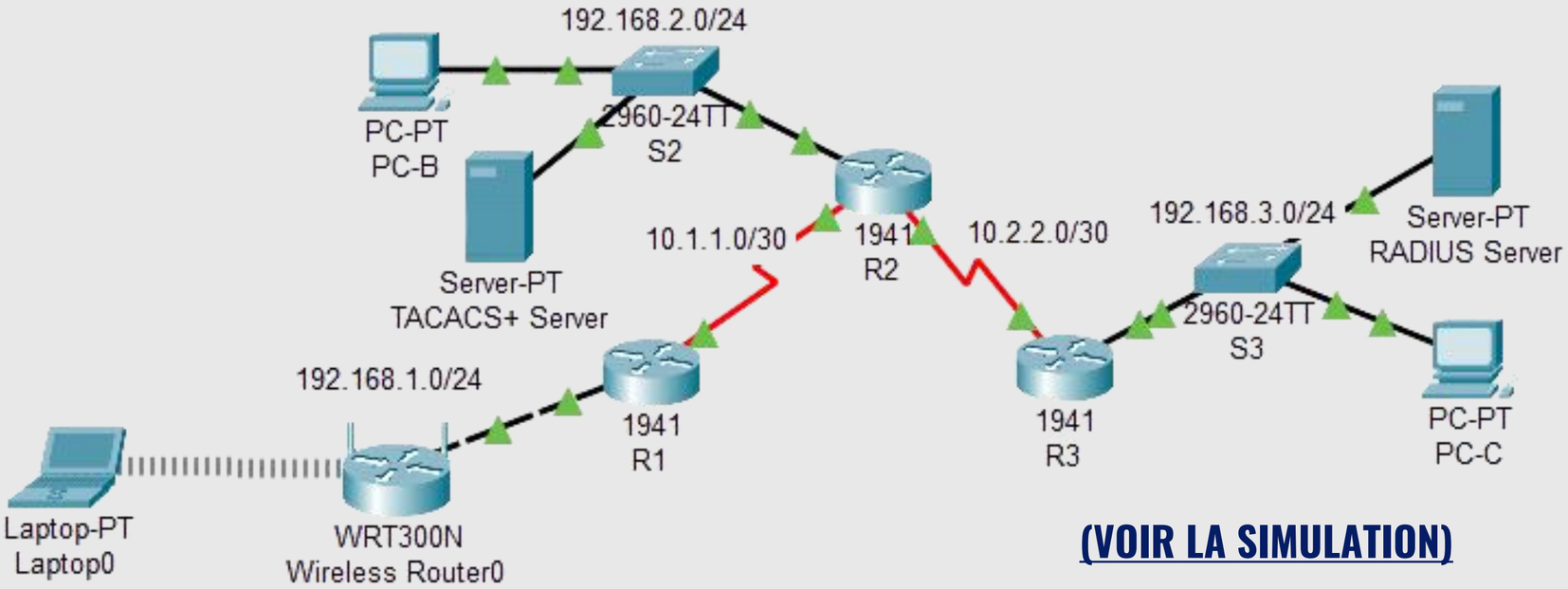
LISTE DE PROTOCOLES AAA

1. RADIUS (Remote Authentication Dial-In User Service) :
   - RADIUS est un protocole de réseau utilisé pour l'authentification, l'autorisation et la comptabilisation (AAA) des utilisateurs qui se connectent à un réseau distant, tels que les réseaux d'accès à distance ou les réseaux sans fil.
2. Diameter :
   - Diameter est un protocole AAA (Authentification, Autorisation, Comptabilité) utilisé pour les réseaux IP, conçu comme une amélioration de RADIUS. Il offre une meilleure extensibilité, sécurité et prise en charge de la mobilité.
3. TACACS (Terminal Access Controller Access-Control System) :
   - TACACS est un protocole de réseau utilisé pour l'authentification et le contrôle de l'accès aux équipements réseau, tels que les routeurs et les commutateurs. Il est principalement utilisé pour les services d'accès en ligne.
4. TACACS+ (Terminal Access Controller Access-Control System Plus) :
   - TACACS+ est une version améliorée de TACACS qui offre des fonctionnalités supplémentaires telles que le cryptage des données d'authentification et une meilleure sécurité globale par rapport à TACACS. Il est largement utilisé dans les environnements réseau pour sécuriser l'accès aux équipements.

LISTE DE PROTOCOLES AAA



IMPLEMENTATION SUR CISCO PACKET TRACER



(VOIR LA SIMULATION)

PART 1: CONFIGURE LOCAL AAA AUTHENTICATION FOR CONSOLE ACCESS ON R1

```
R1>en
R1>enable
Password:
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username Admin1 secret anas2003
R1(config)#
R1(config)#
R1(config)#aaa new
R1(config)#aaa new-model
R1(config)#
R1(config)#aaa authentication login def
R1(config)#aaa authentication login default local
R1(config)#
R1(config)#line console 0
R1(config-line)#
R1(config-line)#login authe
R1(config-line)#login authentication def
R1(config-line)#login authentication default
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

PART 2: CONFIGURE LOCAL AAA AUTHENTICATION FOR VTY LINES ON R1 USING SSH

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto key generate rsa
% Please define a domain-name first.
R1(config)#
R1(config)#ip domain-name ccnasecurity.com
R1(config)#
R1(config)#cry
R1(config)#crypto key gener
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#aaa auth
*Mar 3 20:18:25.240: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#aaa authentication log
R1(config)#aaa authentication login SSH-LOGIN local
R1(config)#line vty 0 4
R1(config-line)#login aut
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport in
R1(config-line)#transport input ssh
R1(config-line)#exit
```

PART 3: CONFIGURE SERVER-BASED AAA AUTHENTICATION USING TACACS+ ON R2

```
R2>en
R2>enable
Password:
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username Admin2 secret admin2pa55
R2(config)#
R2(config)#aaa new
R2(config)#aaa new-model
R2(config)#tacacs-server host 192.168.2.2 key tacacspa55
R2(config)#
R2(config)#aaa authen
R2(config)#aaa authentication login
R2(config)#aaa authentication login def
R2(config)#aaa authentication login default gr
R2(config)#aaa authentication login default group taca
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#
R2(config)#line con
R2(config)#line console 0
R2(config-line)#login auth
R2(config-line)#login authentication def
R2(config-line)#login authentication default
R2(config-line)#exit
R2(config)#exit
```

PART 4: CONFIGURE SERVER-BASED AAA AUTHENTICATION USING RADIUS ON R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface serial0/0/0
R3(config-if)#exit
R3(config)#
R3(config)#username Admin3 secret admin3pa55
R3(config)#
R3(config)#
R3(config)#aaa new
R3(config)#aaa
R3(config)#aaa ne
R3(config)#aaa new-model
R3(config)#radi
R3(config)#radius-ser
R3(config)#radius-server host 192.168.3.2 key radiuspa55
R3(config)#
R3(config)#aaa authen
R3(config)#aaa authentication login de
R3(config)#aaa authentication login default gro
R3(config)#aaa authentication login default group rad
R3(config)#aaa authentication login default group radius lo
R3(config)#aaa authentication login default group radius local
R3(config)#
R3(config)#line cons
R3(config)#line console 0
R3(config-line)#login auth
R3(config-line)#login authentication  def
R3(config-line)#login authentication  default
R3(config-line)#exit
```

MERCI POUR VOTRE ATTENTION