29/08/2024

Atelier 00 – activité 10 - Authentification AAA : radius et tacacs+

**Document de l’atelier :**

[Bloc2\_sem3-4\_Atelier-00-activite-1\_Inter-VLAN\_Routing Challenge.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-1_Inter-VLAN_Routing%20Challenge.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-2\_Découverte-NAT-RIP-01.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-2_Découverte-NAT-RIP-01.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-5-Configure-and-Verify-NTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-5-Configure-and-Verify-NTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-6-reconstruction-reseau.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-6-reconstruction-reseau.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut .pka](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut%20.pka)

[Bloc2\_sem3-4\_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-10-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-10-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-11-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-11-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx)

Table des matières

[1. INTRODUCTION 2](#_Toc176818027)

[2. PRINCIPE DES PROTOCOLES D’AUTHENTIFICATION : LE TRIPLE A ! 2](#_Toc176818028)

[3. Le protocole RADIUS (Remote Access Dial-In User Service) 3](#_Toc176818029)

[4. Le protocole TACACS+ (Terminal Access Controller Access Control System) 6](#_Toc176818030)

[5. Comparaison entre TACACS+ et RADIUS 7](#_Toc176818031)

# INTRODUCTION

**On peut s’authentifier** sur un Cisco de plusieurs façons :

* **par un mot de passe local,**
* **via un serveur Radius,**
* **via un serveur TACACS+.**

Lorsque l’on commence à avoir un peu de matériel réseau, il est alors intéressant de centraliser l’authentification et l’autorisation sur ses équipements.

**L’authentification** est un besoin bien défini aujourd’hui. Mais en parallèle de cette authentification, vient se greffer **l’autorisation** (à telle ou telle ressource… Un administrateur authentifié pourra administrer le routeur « *proton* » (il est autorisé à le faire) et ne pas pouvoir administrer le routeur « *neutron* » (il n’est pas autorisé à le faire).

Enfin, la notion **d’accounting** peut se rajouter aux 2 précédentes.

Ce sont les **AAA** ou **triple A**.

Les serveurs d’authentification tels que Cisco Secure Access Control Server proposent ces AAA. Ils sont basés sur des protocoles d’authentification tels que **TACACS+** (protocole propriétaire CISCO, mais compatible avec les principaux autres constructeurs HP, Netgear…) ou **RADIUS** (open source).

# PRINCIPE DES PROTOCOLES D’AUTHENTIFICATION : LE TRIPLE A !

Un protocole d’authentification est un moyen de contrôle d’accès. Il comprend les **trois** **A** (**AAA**) :

* **A**uthentication (authentification)
* **A**uthorization (autorisation)
* **A**ccounting (rapports)
  + **Authentication**

Cela correspond à l’authentification de l’utilisateur, que ce soit une personne physique ou un service.

Cette authentification passe par la **présentation de l’identité de l’utilisateu**r. Cette information est **unique** à chaque utilisateur et **non secrète**. Elle sert de référence dans la base des utilisateurs.

**Le contrôle de cette information d’identification** consiste à vérifier un secret partagé entre l’utilisateur et le serveur d’authentification. Ce contrôle passe par l’envoi d’une information d’authentification qui peut être de plusieurs types :

* **statique :** l’information transmise est alors la même lors d’authentifications successives : mot de passe type UNIX par exemple.
* **dynamique :** on passe alors par un challenge entre le serveur et l’utilisateur, ce qui permet d’avoir une information différente à chaque nouvelle authentification : calculette, carte à puce, badge, clé OTP…
* **physique :** reconnaissance vocale, empreintes, iris…
  + **Autorisation**

L’autorisation permet de déterminer quels sont les droits de l’utilisateur.

Par exemple, après s’être loggué, l’utilisateur peut essayer d’utiliser certaines commandes. L’autorisation détermine alors si l’utilisateur peut ou non les utiliser. Dans certains protocoles, l’authentification et l’autorisation sont regroupées en une seule étape.

* + **Accounting**

L’accounting rassemble et envoie les informations regroupant les actions des utilisateurs.

Les administrateurs réseau peuvent utiliser cette fonctionnalité **pour tracer l’activité d’un utilisateur** pour un audit de sécurité **ou simplement pour des statistiques** (sur l’usage de ressources par exemple) ou bien encore à des fins de facturation (l’objectif des opérateurs de téléphonie mobile !).

Un rapport peut être réalisé pour fournir différentes informations comme

* l’identité de l’utilisateur,
* les heures de début et de fin de sessions,
* les commandes exécutées,
* le nombre de paquets,
* le nombre d’octets échangés.

Les 3 points définis ci-dessus sont importants pour une bonne gestion et une bonne sécurité d’un réseau.

# Le protocole RADIUS (Remote Access Dial-In User Service)

Le protocole **RADIUS** (**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice) a été créé par Livingston et normalisé par l’**IETF** (**I**nternet **E**ngineering **T**ask **F**orce) sous la forme de **RFC** (**R**equest **F**or **C**omments). Actuellement, il s’agit des RFC 2138 et 2139.

Tous les clients RADIUS communiquent généralement à travers le réseau local avec un unique serveur d’authentification, ce qui rend la tâche de l’administrateur plus simple. La gestion des utilisateurs et de leurs droits est alors plus facile par rapport à plusieurs serveurs qu’il faudrait mettre à jour simultanément sur le réseau.

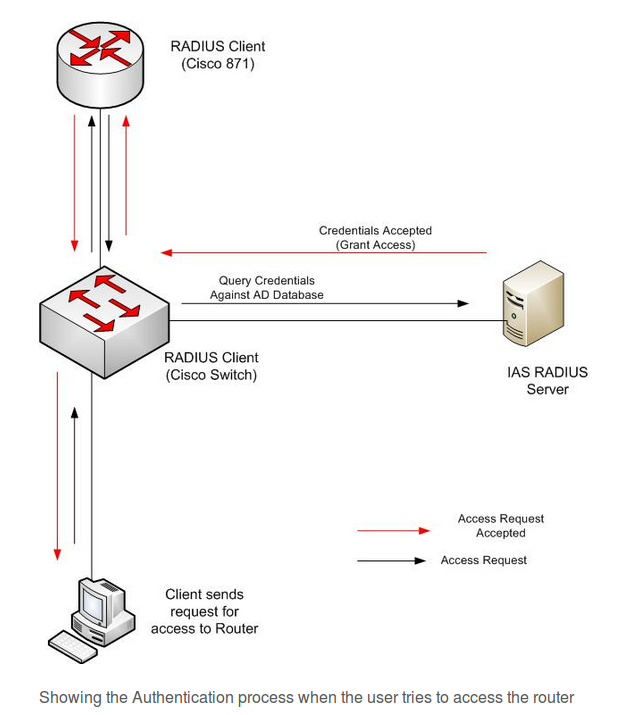
Le standard RADIUS est basé sur un ensemble d’attributs relatifs aux utilisateurs. Ils sont tous stockés dans la base RADIUS du serveur. Au cours d’une connexion, un échange d’information a lieu entre le serveur RADIUS et le client RADIUS appelé **NAS** (**N**etwork **A**ccess **S**erver). **Le NAS est généralement un switch, un point d’accès Wi-Fi ou un routeur CISCO.**

Le protocole RADIUS permet une authentification utilisateur/mot de passe ou utilisateur/challenge/réponse ou les deux, qui peut être configurée spécifiquement pour chaque utilisateur. La vérification est réalisée par le serveur RADIUS, qui retourne alors un « authentication reply » au NAS qui a émis la requête.

L’autorisation, elle, est réalisée par le NAS, en utilisant les informations sur l’utilisateur retournées par le serveur.

Le protocole RADIUS est basé sur un échange de paquets utilisant le protocole **UDP**. Le port généralement employé est le 1645, bien qu’il devrait être normalement configuré sur le port 1812 pour éviter des conflits avec le service Datametrics. Il existe 4 types de paquets différents :

* **« Access-Request ».**
* **« Access-Accept »**
* **« Access-Reject »**
* **« Access-Challenge »**

[](http://www.superwebcrawler.fr/dokuwiki/lib/exe/detail.php?id=secupt:aaa&media=secupt:screenshot_from_2014-01-25_18_59_51.png)

* + **Authentification avec RADIUS**

Afin de se connecter au NAS (switch ou routeur CISCO), l’utilisateur cherchant à s’authentifier envoie toutes les informations nécessaires (login, mot de passe par exemple). La méthode de récupération de ces informations dépend de la configuration du client. Il peut s’agir par exemple d’un prompt invitant l’utilisateur à entrer ces informations.

À la suite de cela, le client RADIUS crée un paquet de type « **Access-Request** » contenant les informations dont le serveur RADIUS a besoin (nom, mot de passe, ID du client, ID du port). Si un mot de passe est présent, il sera chiffré en utilisant MD5.

Une fois que le serveur reçoit la requête, il vérifie d’abord que le client partage un secret avec lui, puis récupère les informations concernant l’utilisateur. Celles-ci sont extraites d’une **base de données** qui peut être **locale au serveur RADIUS**, **ou bien appartenir à un autre serveur du réseau** (dans ce cas, le serveur RADIUS jouera lui-même le rôle de client). Si un mot de passe doit être communiqué, il sera vérifié par le serveur.

D’autres vérifications peuvent être effectuées sur l’ID du client ou du port selon le contenu de la base concernant l’utilisateur.

Dans le cas où l’une des conditions ne serait pas remplie, le serveur retourne un paquet « **Access-Reject** » qui indiquerait au client que la connexion a été refusée et pourrait contenir un message d’explication. Sinon, le serveur retourne un « **Access-Challenge** ». Le paquet contient un nombre aléatoire que le client doit chiffrer. Pour cela, il peut utiliser une calculette, ou un logiciel permettant de faciliter le calcul de la réponse.

En retour, le client émet de nouveau le paquet « **Access-Request** », mais contenant cette fois la réponse au challenge. Le serveur peut alors renvoyer :

* **un « Access-Accept »** si l’authentification est validée,
* **un « Access-Reject »** dans le cas contraire,
* ou **un « Access-Challenge »** si un complément d’information est nécessaire.
  + **Autorisation avec RADIUS**

Lors de l’« Access-Accept », le serveur ajoute, dans le paquet, une liste de valeurs correspondant aux paramètres de l’utilisateur. Elles sont utilisées par le NAS qui réalise la phase d’autorisation.

Si elles sont valides, l’utilisateur est alors connecté.

* + **Accounting avec RADIUS**

Au démarrage d’un service, le NAS émet un paquet « Accounting-Start » au serveur RADIUS. Le NAS centralise les informations, puis les envoie au serveur au moment de la fermeture du service dans un paquet « Accounting Stop » (quantité transmise, débit, bande passante, temps d’émission…).

# Le protocole TACACS+ (Terminal Access Controller Access Control System)

**TACACS+** est la dernière version du protocole TACACS développé à l’origine par BBN, puis repris par Cisco qui va l’étendre une première fois par XTACACS (eXtended TACACS) compatible avec TACACS, puis par TACACS+. Mais cette dernière version n’est plus compatible avec les versions originelles, bien que basée sur celles-ci.

* TACACS+ utilise TCP pour son transport (contrairement à TACACS qui était basé sur l’UDP).
* Il utilise le port 49 (login).
* Il gère séparément les trois fonctions AAA (Authentification, Autorisation, Accounting), contrairement à d’autres protocoles d’authentification.
* TACACS+ prévoit une implémentation pour chacune des 3, mais une configuration n’exige pas de toutes les utiliser.
  + **Authentification avec TACACS+**

TACACS+ peut aussi bien utiliser des techniques d’authentification classiques type login/mot de passe statique, ou bien des procédés plus évolués à base de challenge avec authentification réciproque, par exemple.

Lors d’une nouvelle connexion, le NAS émet un message START au serveur décrivant le type d’authentification à utiliser. En retour, le démon envoie un message REPLY. Ce type de message peut indiquer ou bien que l’authentification est terminée, ou bien qu’elle doit continuer, auquel cas, le client récupère l’information manquante et la retourne dans un message CONTINUE.

Le type de requête provenant du serveur peut être une demande GETDATA, GETUSER ou GETPASS. GETDATA est une requête générique de récupération d’information du profil utilisateur.

* + **Autorisation avec TACACS+**

Lors d’un accès à un service particulier, le NAS ouvre une session d’autorisation. Cette session consiste juste en l’échange d’une paire de messages : REQUEST/RESPONSE. La requête décrit l’authentification pour l’utilisateur ou le processus qui demande l’accès au service.

La réponse du serveur contient un ensemble d’attributs pouvant restreindre ou modifier les actions du client, plutôt qu’une simple réponse affirmative de type oui/non.

* + **Accounting avec TACACS+**

Les échanges utilisés lors de l’accounting sont similaires à ceux employés lors de l’autorisation (REQUEST/RESPONSE).

Au démarrage et à la terminaison d’un service, on émet un paquet START et STOP.

De plus, le protocole TACACS+ propose l’émission de paquets UPDATE servant à confirmer qu’un service est en cours d’utilisation.

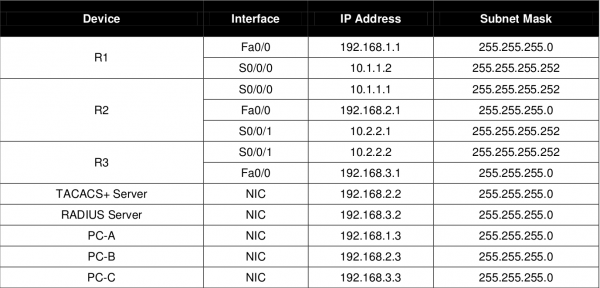
# Comparaison entre TACACS+ et RADIUS

|  | **TACACS+** | **RADIUS** |
| --- | --- | --- |
| **Protocole** | TCP : port 49 | UDP : port 1645 (1812 normalement) |
| **Chiffrement** | Chiffrement du paquet entier | Chiffrement du mot de passe seulement |
| **Architecture AAA** | Les AAA sont indépendants | Autorisation liée à l’authentification |
| **Émission du profil** | Profil émis champ par champ à la demande du NAS | Profil global envoyé au NAS lors de la fin de l’authentification |
| **Protocoles supportés** | Support complet | Pas de NetBEUI |
| **Challenge/Réponse** | Bidirectionnel | Unidirectionnel |

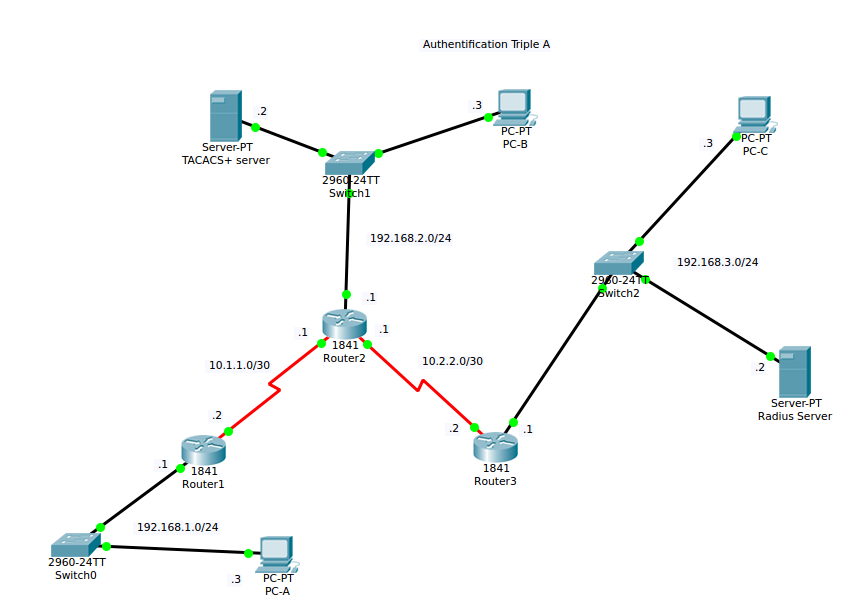
* **Configurer une authentification « triple A » sur routeur CISCO**

On utilisera le fichier : [Bloc2\_sem3-4\_Atelier-00-activite-10-tacacs.pkt](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Encour\Bloc2_sem3-4_Atelier-00-activite-10-tacacs.pkt)

* + **OBJECTIFS**
* Configurer un compte d’utilisateur local sur R1 et s’authentifier sur la console et les lignes VTY utilisant une authentification AAA locale.
* Vérification de l’authentification AAA locale de la console R1 et le PC-A client.
* Configurez une authentification AAA basée sur le serveur en utilisant TACACS+.
* Vérification de l’authentification AAA basée sur le serveur depuis le client PC-B.
* Configurez une authentification AAA basée sur le serveur en utilisant RADIUS.
* Vérification de l’authentification AAA basée sur le serveur depuis le client PC-C.
  + **PLAN D’ADRESSAGE**

[](http://www.superwebcrawler.fr/dokuwiki/lib/exe/detail.php?id=secupt:tp2secucisco&media=secupt:screenshot_from_2014-01-26_14_27_11.png)

* + **Topologie du réseau**

[](http://www.superwebcrawler.fr/dokuwiki/lib/exe/detail.php?id=secupt:tp2secucisco&media=secupt:capture_du_2016-03-06_16_13_01.png)

* + **Introduction**

À la base, toute la sécurité administrative de R1, R2 et R3 est basée sur la connaissance du mot de passe secret. Votre tâche est de configurer et de tester des solutions AAA locale et serveur.

1. Vous allez créer un compte d’utilisateur local et configurer AAA local sur le routeur R1 pour tester la console et les connexions VTY.

* Compte d’utilisateur : **Admin1**
* Mot de passe **admin1pa55**

1. Vous serez ensuite configurer le routeur R2 en charge de l’authentification basée sur le serveur en utilisant le protocole TACACS+

Le serveur TACACS + a été préconfiguré avec les paramètres suivants :

* Client : **R2** en utilisant le mot-clé **tacacspa55**
* Compte d’utilisateur : **Admin2** et mot de passe **admin2pa55**

1. Enfin, vous allez configurer le routeur R3 en charge de l’authentification basée sur le serveur en utilisant le protocole RADIUS.

Le serveur RADIUS a été préconfiguré avec les paramètres suivants :

* Client : **R3** en utilisant le mot-clé **radiuspa55**
* compte d’utilisateur : **admin3** et mot de passe **admin3pa55**

Les routeurs ont également été préconfigurés avec les paramètres suivants :

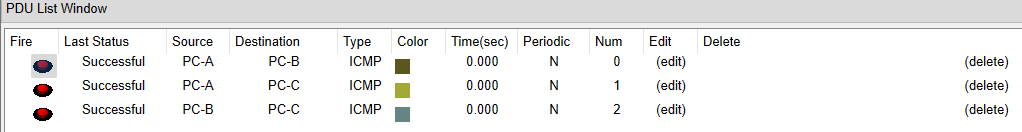
* mot de passe secret : **ciscoenpa55**
* RIP **version 2**.

Pourquoi le protocole RIP1 ne peut convenir ici ?

* + **ÉTAPE 1 : Configurer une authentification locale AAA pour accéder à R1 en mode console**

**Tests de connectivité**

* ping depuis PC-A vers PC-B,
* ping depuis PC-A vers PC-C,
* ping depuis PC-B vers PC-C.



**Configurer un compte local sur R1**

* username : **Admin1**
* password : **admin1pa55**

R1(config)# username Admin1 secret admin1pa55



**Configurer une authentification locale AAA pour accéder à R1 en mode console**

Activer AAA sur R1 et configurer l’authentification AAA pour se connecter sur la console avec le compte local créé précédemment.

R1(config)# aaa new-model

R1(config)# aaa authentication login default local



**Configurer la console 0 pour utiliser la méthode d’authentification définie précédemment.**

R1 (config)# line console 0

R1(config-line)# login authentication default



**Vérification**

R1(config-line)# end

%SYS-5-CONFIG\_I: Configured from console by console

R1# exit

R1 con0 is now available

Press RETURN to get started.

\*\*\*\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\*\*\*

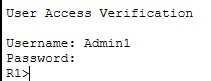
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification

Username: Admin1

Password: admin1pa55

R1>



* + **ÉTAPE 2 : Configurer une authentification locale AAA pour les lignes vty sur R1**

**Créer une liste appelée TELNET-LOGIN pour authentifier les connexions utilisant AAA locale**

R1(config)# aaa authentication login TELNET-LOGIN local



**Configurez les 5 lignes VTY 0 à 4 pour utiliser la méthode d’authentification AAA définie précédemment.**

R1(config)# line vty 0 4

R1(config-line)# login authentication TELNET-LOGIN

R1(config-line)# end



* + **Vérification**

Verify the Telnet configuration. From the command prompt of PC-A, Telnet to R1.

PC> telnet 192.168.1.1

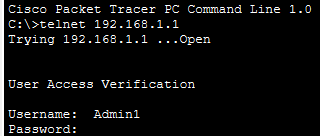
\*\*\*\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\*\*\*

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification

Username: Admin1

Password:



* + **ÉTAPE 3 : Configuration de l’authentification AAA basée sur serveur TACACS+ pour s’authentifier sur R2**

**Configurer une entrée dans la base locale de sauvegarde**

* local username : Admin
* secret password : adminpa55

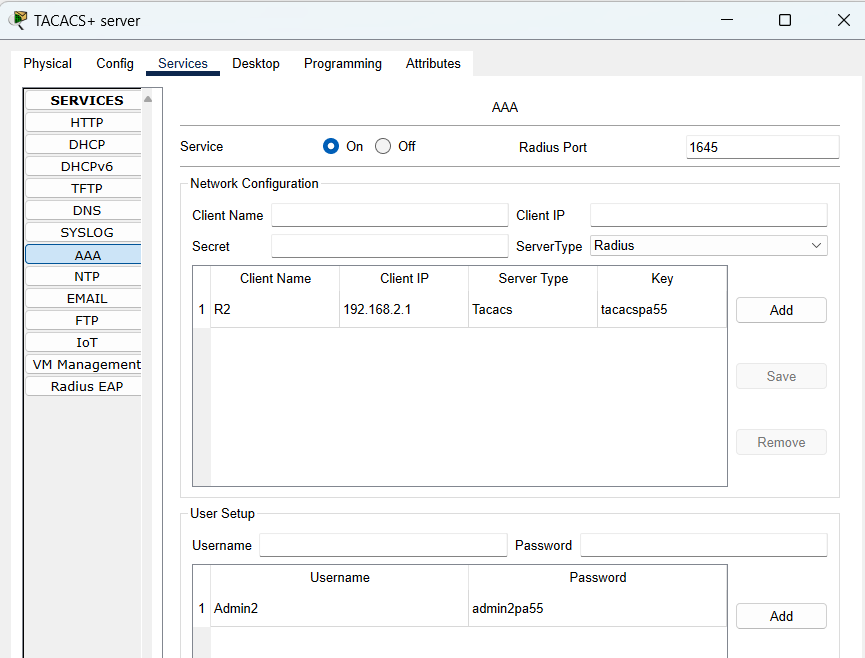
R2(config)# username Admin secret adminpa55



**Configurer le serveur TACACS+**

Sur le serveur TACACS+, il faut créer une entrée pour le client R2 et déclarer un utilisateur admin2.

**Sur R2, déclarer l’adresse IP du serveur TACACS+ et la clé partagée**



R2 (config)# tacacs-server host 192.168.2.2

R2 (config)# tacacs-server key tacacspa55



**Sur R2, activer AAA. tous les logins devront s’authentifier en utilisant le serveur TACACS+. Si TACACS+ est inutilisable alors la base locale de compte suppléra.**

R2(config)# aaa new-model

R2(config)# aaa authentication login default group tacacs+ local



**Configurer la ligne console 0 pour utiliser la méthode d’authentification AAA par défaut**

R2(config)# line console 0

R2(config-line)# login authentication default



Vérification

R2(config-line)# end

%SYS-5-CONFIG\_I: Configured from console by console

R2# exit

R2 con0 is now available

Press RETURN to get started.

\*\*\*\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\*\*\*

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification

Username: Admin2

Password: admin2pa55

R2>

Vous ferez en sorte que la **bannière d’avertissement** :

\*\*\*\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\*\*\*

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

apparaisse !!!!

Pour que la bannière apparaisse il faut utiliser la commande suivante :

**R3(config)# banner motd #**

**\*\*\*\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\*\*\***

**UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.**

**#**

Passez la commande infra sur R2 :

R2#sh aaa sessions

Notez le nom de l’utilisateur connecté ainsi que son numéro d’identification.

Passez la commande infra sur R2 :

R2#sh aaa user 1

Vérifiez bien que la méthode d’authentification est bien « TACACS ».

* + **ÉTAPE 4 : Configuration de l’authentification AAA basée sur serveur RADIUS pour s’authentifier sur R3**

**Configurer une entrée dans la base locale de sauvegarde**

R3(config)# username Admin secret adminpa55



**Configurer le serveur RADIUS**

Sur le serveur RADIUS, il faut créer une entrée pour le client R3 et déclarer un utilisateur admin3.

**Sur R3, déclarer l’adresse IP du serveur RADIUS et la clé partagée**

R3(config)# radius-server host 192.168.3.2

R3(config)# radius-server key radiuspa55



**Sur R3, activer AAA. tous les logins devront s’authentifier en utilisant le serveur RADIUS. Si RADIUS est inutilisable alors la base locale de compte suppléera**

R3(config)# aaa new-model

R3(config)# aaa authentication login default group radius local



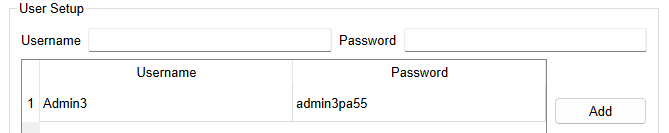
**Configurer la ligne console 0 pour utiliser la méthode d’authentification AAA par défaut**

R3(config)# line console 0

R3(config-line)# login authentication default



Dans le serveur Radius j’ai rajouter l’utilisateur avec Username: Admin3 et Password: admin3pa55



**Vérification**

R3(config-line)# end

%SYS-5-CONFIG\_I: Configured from console by console

R3# exit

R3 con0 is now available

Press RETURN to get started.

\*\*\*\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\*\*\*

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification

Username: Admin3

Password: admin3pa55

R3>

