**Controlul accesului**

Autentificare cu o parolă locală

În subiectul anterior, ați aflat că un dispozitiv NAC oferă servicii AAA. În acest subiect, veți afla mai multe despre AAA și modalitățile de control al accesului.

Pe dispozitivele de rețea pot fi efectuate multe tipuri de autentificare, iar fiecare metodă oferă niveluri diferite de securitate. Cea mai simplă metodă de autentificare cu acces la distanță este configurarea unei combinații de autentificare și parolă pe consolă, linii vty și porturi auxiliare, așa cum se arată în liniile vty din exemplul următor. Această metodă este cea mai ușor de implementat, dar este și cea mai slabă și mai puțin sigură. Această metodă nu oferă responsabilitate, iar parola este trimisă în text simplu. Oricine are parola poate intra pe dispozitiv.

**R1(config)# line vty 0 4**

**R1(config-line)# password ci5c0**

**R1(config-line)# login**

SSH este o formă mai sigură de acces la distanță:

* Necesită un nume de utilizator și o parolă, ambele fiind criptate în timpul transmiterii.
* Numele de utilizator și parola pot fi autentificate prin metoda bazei de date locală.
* Oferă mai multă responsabilitate, deoarece numele de utilizator este înregistrat atunci când un utilizator se conectează.

Următorul exemplu ilustrează metodele SSH și bazele de date locale de acces la distanță.

**R1(config)# ip domain-name example.com**

**R1(config)# crypto key generate rsa general-keys modulus 2048**

**R1(config)# username Admin secret Str0ng3rPa55w0rd**

**R1(config)# ssh version 2**

**R1(config)# line vty 0 4**

**R1(config-line)# transport input ssh**

**R1(config-line)# login local**

Metoda bazei de date locală are câteva limitări:

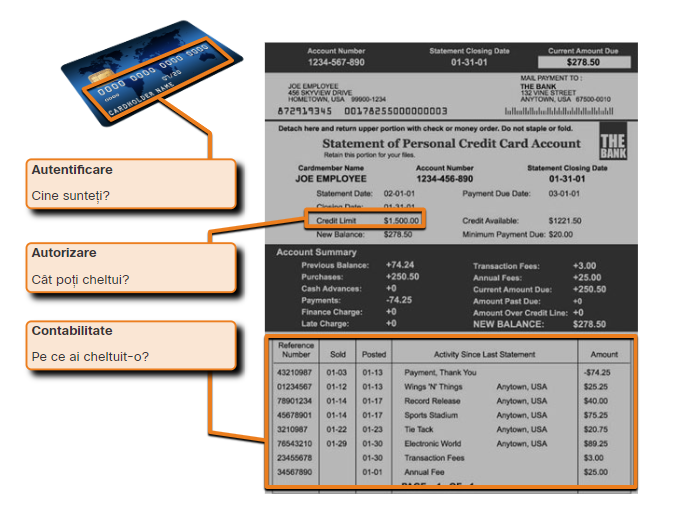
* Conturile de utilizator trebuie configurate local pe fiecare dispozitiv. Într-un mediu de întreprindere mare, cu mai multe routere și comutatoare de gestionat, implementarea și modificarea bazelor de date locale pe fiecare dispozitiv poate dura timp.
* Configurația bazei de date locală nu oferă nicio metodă de autentificare alternativă. De exemplu, ce se întâmplă dacă administratorul uită numele de utilizator și parola pentru dispozitivul respectiv? Fără o metodă de rezervă disponibilă pentru autentificare, recuperarea parolei devine singura opțiune.

O soluție mai bună este ca toate dispozitivele să se refere la aceeași bază de date de nume de utilizator și parole de la un server central.

**Componente AAA**

AAA înseamnă Autentificare, Autorizare și Contabilitate. Conceptul AAA este similar cu utilizarea unui card de credit, așa cum se arată în figură. Cardul de credit identifică cine îl poate folosi, cât poate cheltui acel utilizator și ține cont de articolele sau serviciile achiziționate de utilizator.

AAA oferă cadrul principal pentru a configura controlul accesului pe un dispozitiv de rețea. AAA este o modalitate de a controla cui îi este permis să acceseze o rețea (autentificare), ce pot face în timp ce sunt acolo (autorizare) și de a audita ce acțiuni au efectuat în timpul accesării rețelei (contabilitate).



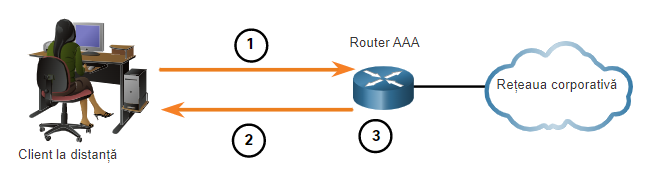
**Autentificare**

Local și bazat pe server sunt două metode comune de implementare a autentificării AAA.

**Autentificare locală AAA**

Local AAA stochează numele de utilizator și parolele local într-un dispozitiv de rețea, cum ar fi routerul Cisco. Utilizatorii se autentifică în baza de date locală, așa cum se arată în figură. Local AAA este ideal pentru rețelele mici.

un client la distanță se conectează la un router AAA, i se solicită un nume de utilizator și o parolă, routerul își verifică baza de date locală înainte de a permite accesul în rețeaua corporativă

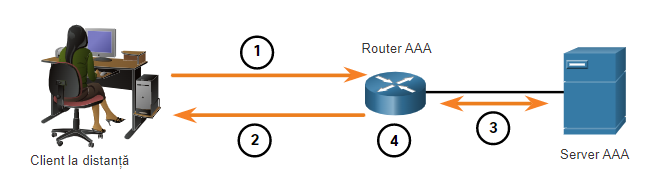


1. Clientul stabilește o conexiune cu routerul.
2. Routerul AAA solicită utilizatorului un nume de utilizator și o parolă.
3. Routerul autentifică numele de utilizator și parola folosind baza de date locală, iar utilizatorului i se oferă acces la rețea pe baza informațiilor din baza de date locală.

**Autentificare AAA bazată pe server**

Cu metoda bazată pe server, routerul accesează un server central AAA, așa cum se arată în figură. Serverul AAA conține numele de utilizator și parolele pentru toți utilizatorii. Routerul folosește fie Serviciul de acces la Remote Authentication Dial-In User Service (RADIUS), fie protocoale Terminal Access Controller Access Control System (TACACS+) pentru a comunica cu serverul AAA. Când există mai multe routere și comutatoare, AAA bazat pe server este mai potrivit.

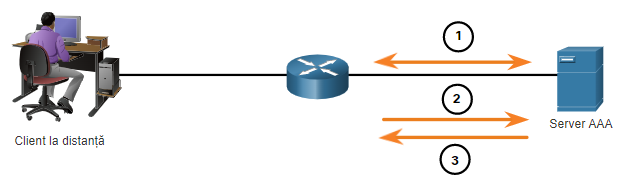
un client de la distanță se conectează la un router AAA, i se solicită un nume de utilizator și o parolă, routerul autentifică acreditările folosind un server AAA și utilizatorului i se oferă acces la rețea



1. Clientul stabilește o conexiune cu routerul.
2. Routerul AAA solicită utilizatorului un nume de utilizator și o parolă.
3. Routerul autentifică numele de utilizator și parola folosind un server AAA.
4. Utilizatorului i se oferă acces la rețea pe baza informațiilor din serverul AAA la distanță.

**Autorizare**

Autorizarea AAA este automată și nu necesită ca utilizatorii să efectueze pași suplimentari după autentificare. Autorizarea guvernează ce pot și nu pot face utilizatorii în rețea după ce sunt autentificați.

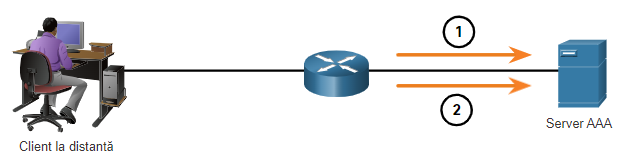
Autorizarea folosește un set de atribute care descriu accesul utilizatorului la rețea. Aceste atribute sunt utilizate de serverul AAA pentru a determina privilegiile și restricțiile pentru acel utilizator, așa cum se arată în figură.

1. Când un utilizator a fost autentificat, se stabilește o sesiune între router și serverul AAA.
2. Routerul solicită autorizarea de la serverul AAA pentru serviciul solicitat de client.
3. Serverul AAA returnează un răspuns PASS/FAIL pentru autorizare.

**Contabilitate**

Contabilitatea AAA colectează și raportează date de utilizare. Aceste date pot fi utilizate în scopuri precum auditul sau facturarea. Datele colectate pot include orele de pornire și oprire a conexiunii, comenzile executate, numărul de pachete și numărul de octeți.

O utilizare principală a contabilității este combinarea acesteia cu autentificarea AAA. Serverul AAA păstrează un jurnal detaliat cu exact ceea ce face utilizatorul autentificat pe dispozitiv, așa cum se arată în figură. Aceasta include toate comenzile EXEC și de configurare emise de utilizator. Jurnalul conține numeroase câmpuri de date, inclusiv numele de utilizator, data și ora și comanda reală care a fost introdusă de utilizator. Aceste informații sunt utile la depanarea dispozitivelor. De asemenea, oferă dovezi pentru cazurile în care indivizii efectuează acte rău intenționate.



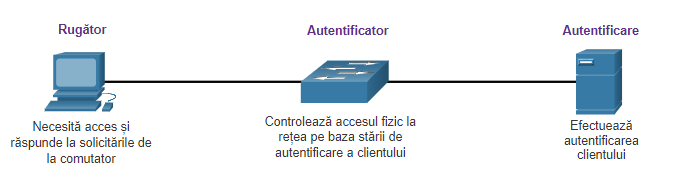
1. Când un utilizator a fost autentificat, procesul de contabilitate AAA generează un mesaj de pornire pentru a începe procesul de contabilitate.
2. Când utilizatorul termină, este înregistrat un mesaj de oprire și procesul de contabilizare se încheie.

**802.1X**

Standardul IEEE 802.1X este un protocol de autentificare și control al accesului bazat pe porturi. Acest protocol restricționează stațiile de lucru neautorizate să se conecteze la o rețea LAN prin porturi de comutare accesibile public. Serverul de autentificare autentifică fiecare stație de lucru care este conectată la un port de comutare înainte de a pune la dispoziție orice serviciu oferit de comutator sau de LAN.

Cu autentificarea bazată pe porturi 802.1X, dispozitivele din rețea au roluri specifice, așa cum se arată în figură.

Diagrama arată dispozitivele implicate în autentificarea bazată pe porturi 802.1x. În stânga se află solicitantul, în acest caz un desktop, care necesită acces și răspunde la solicitările de la un comutator. Solicitantul este conectat la autentificator, în acest caz un comutator, care controlează accesul fizic la rețea pe baza stării de autentificare a clientului. Autentificatorul este conectat la serverul de autentificare care realizează autentificarea clientului.



* **Client (Solicitant)** - Acesta este un dispozitiv care rulează software client compatibil 802.1X, care este disponibil pentru dispozitive cu fir sau fără fir.
* **Switch (Authenticator)** – Comutatorul acționează ca un intermediar între client și serverul de autentificare. Acesta solicită informații de identificare de la client, verifică aceste informații cu serverul de autentificare și transmite un răspuns către client. Un alt dispozitiv care ar putea acționa ca autentificator este un punct de acces wireless.
* **Server de autentificare** – Serverul validează identitatea clientului și notifică comutatorul sau punctul de acces fără fir că clientul este sau nu autorizat să acceseze LAN și serviciile de comutare.