# Introducere

Protocolul 802.1X este un standard de securitate care permite autentificarea utilizatorilor și a dispozitivelor la nivel de port într-o rețea Ethernet. Protocolul se bazează pe trei componente principale: clientul 802.1X, switch-ul 802.1X și serverul de autentificare.

Clientul 802.1X este dispozitivul sau software-ul care solicită acces la rețea. De obicei, acesta este un computer, laptop, smartphone sau alt dispozitiv care se conectează la rețeaua Ethernet. Înainte de a fi autorizat să utilizeze rețeaua, clientul 802.1X trebuie să fie autentificat de serverul de autentificare.

Switch-ul 802.1X este dispozitivul care conectează clientul 802.1X la rețeaua Ethernet și facilitează procesul de autentificare. Switch-ul 802.1X poate fi configurat pentru a permite sau a refuza accesul la rețea în funcție de starea autentificării clientului.

Serverul de autentificare este dispozitivul sau software-ul care verifică identitatea clientului 802.1X și decide dacă acesta are sau nu permisiunea de a utiliza rețeaua Ethernet. Serverul de autentificare poate utiliza diverse metode de autentificare, cum ar fi parole, certificate digitale sau autentificare bazată pe token-uri.

Într-un scenariu tipic de utilizare a protocolului 802.1X, clientul 802.1X solicită accesul la rețeaua Ethernet prin intermediul switch-ului 802.1X. Switch-ul 802.1X răspunde prin deschiderea unui canal de comunicare între clientul 802.1X și serverul de autentificare. Serverul de autentificare solicită apoi informații de autentificare de la clientul 802.1X, cum ar fi numele de utilizator și parola. Dacă informațiile de autentificare sunt corecte, serverul de autentificare transmite un semnal de acceptare către switch-ul 802.1X, iar switch-ul deschide portul pentru ca clientul să poată utiliza rețeaua Ethernet.

Implementarea protocolului 802.1X poate fi realizată utilizând un server de autentificare compatibil cu protocolul, cum ar fi un server RADIUS. Serverul RADIUS poate fi utilizat pentru a gestiona autentificarea și autorizarea utilizatorilor și a dispozitivelor la nivel de port într-o rețea Ethernet. Implementarea protocolului 802.1X poate fi o soluție excelentă pentru orice organizație care dorește să-și protejeze rețeaua împotriva atacurilor și să asigure un control precis asupra accesului la rețea.

În concluzie, protocolul 802.1X este un standard important de securitate pentru rețelele Ethernet, care permite autentificarea utilizatorilor și a dispozitivelor la nivel de port. Implementarea protocolului 802.1X poate ajuta la prevenirea accesului neautorizat la rețea și la creșterea nivelului de securitate a rețelei.

Este important să se înțeleagă că implementarea protocolului 802.1X nu este o soluție completă de securitate pentru rețea. Acesta este doar unul dintre multele instrumente disponibile pentru a asigura securitatea rețelei. Este important să se utilizeze o gamă completă de soluții de securitate, cum ar fi firewall-uri, antivirus și software de detectare a intruziunilor, pentru a asigura un nivel adecvat de securitate pentru rețea.

Pe lângă securitate, implementarea protocolului 802.1X poate aduce și alte beneficii. De exemplu, acesta poate ajuta la gestionarea eficientă a utilizării rețelei prin limitarea accesului la rețea numai pentru utilizatorii autorizați. Acest lucru poate ajuta la prevenirea suprasolicitării rețelei și la asigurarea unei performanțe optime.

În concluzie, protocolul 802.1X este un standard important de securitate pentru rețelele Ethernet. Implementarea protocolului poate ajuta la prevenirea accesului neautorizat la rețea și la creșterea nivelului de securitate a rețelei. Este important să se utilizeze o gamă completă de soluții de securitate, împreună cu protocolul 802.1X, pentru a asigura securitatea adecvată a rețelei.

# Funcționare

Într-o rețea 802.1X, dispozitivele care doresc să se conecteze la rețea trebuie să se autentifice în prealabil la serverul de autentificare. Acest proces de autentificare are loc la nivel de port, ceea ce înseamnă că accesul la rețea poate fi restricționat pe baza identității utilizatorului și a drepturilor sale de acces. Înainte de a permite accesul la rețea, switch-ul Ethernet care protejează rețeaua (denumit "supapa" în standardul 802.1X) trimite un mesaj de autentificare către dispozitivul care se conectează.

Dispozitivul care se conectează trebuie să răspundă la acest mesaj cu un mesaj de autentificare. Acest mesaj de autentificare include identitatea dispozitivului (de obicei un nume de utilizator și o parolă), care este verificată de serverul de autentificare pentru a verifica că utilizatorul are dreptul de a accesa rețeaua. Dacă autentificarea este reușită, serverul de autentificare trimite un mesaj de autorizare către switch-ul Ethernet, care permite dispozitivului să acceseze rețeaua.

# Componente

Există trei componente principale într-o rețea 802.1X:

- Dispozitivul care se conectează: Acesta poate fi un calculator, un laptop, un smartphone, un dispozitiv IoT sau orice alt dispozitiv care dorește să acceseze rețeaua Ethernet. Dispozitivul trebuie să ofere un client 802.1X pentru a se conecta la rețea.

- Supapa (switch-ul Ethernet): Acesta este dispozitivul care protejează rețeaua și care controlează accesul la rețea pe baza stării de autentificare a dispozitivelor care se conectează la el. Supapa trebuie să ofere un server 802.1X pentru a gestiona autentificarea utilizatorilor.

- Serverul de autentificare: Acesta este serverulcentralizat care verifică autenticitatea utilizatorilor și a dispozitivelor și autorizează accesul la rețeaua Ethernet. Serverul de autentificare poate fi un server RADIUS, un server LDAP sau un alt tip de server de autentificare compatibil cu protocolul 802.1X.

# Implementare

Pentru a implementa protocolul 802.1X într-o rețea, este necesar să se instaleze și să se configureze un server de autentificare compatibil cu protocolul 802.1X (de obicei un server RADIUS) și să se configureze switch-ul Ethernet pentru a utiliza serverul de autentificare. Fiecare dispozitiv care se conectează la rețea trebuie să aibă un client 802.1X configurat pentru a se autentifica la serverul de autentificare.

Pentru a configura un switch Ethernet pentru a utiliza protocolul 802.1X, este necesar să se configureze supapa Ethernet pentru a utiliza un server RADIUS pentru autentificarea utilizatorilor și a dispozitivelor. În plus, este necesar să se configureze porturile Ethernet pentru a utiliza protocolul 802.1X și să se specifice politicile de autentificare și autorizare. Acest lucru poate fi realizat utilizând interfața CLI (linie de comandă) a switch-ului Ethernet.

# Avantaje

Protocolul 802.1X oferă mai multe avantaje importante pentru rețelele Ethernet, printre care se numără:

Securitate îmbunătățită: Protocolul 802.1X permite restricționarea accesului la rețea pe baza identității utilizatorului și a drepturilor sale de acces, ceea ce face ca rețeaua să fie mult mai sigură și mai protejată împotriva atacurilor și a accesului neautorizat.

Control de acces flexibil: Protocolul 802.1X permite configurarea politicilor de autentificare și autorizare pentru fiecare port Ethernet, ceea ce înseamnă că administratorii de rețea pot controla accesul la rețea într-un mod foarte flexibil și precis.

Management simplificat: Protocolul 802.1X permite administrarea centralizată a autentificării utilizatorilor și a dispozitivelor, ceea ce face ca managementul rețelei să fie mult mai simplu și mai eficient.

Integrare ușoară cu alte servicii de securitate: Protocolul 802.1X poate fi integrat cu alte servicii de securitate, cum ar fi VPN sau autentificarea în două etape, pentru a oferi o protecție suplimentară și pentru a asigura o securitate mai bună a rețelei.

Concluzie

Protocolul 802.1X (dot1x) este un standard de securitate esențial pentru rețelele de comunicații Ethernet. Acesta permite autentificarea utilizatorilor și a dispozitivelor la nivel de port, ceea ce face ca rețeaua să fie mult mai sigură și mai protejată împotriva atacurilor și a accesului neautorizat. Protocolul 802.1X poate fi implementat utilizând un server de autentificare compatibil cu protocolul, cum ar fi un server RADIUS, și este disponibil pe majoritatea switch-urilor Ethernet moderne.

Implementarea protocolului 802.1X oferă numeroase avantaje pentru rețelele Ethernet, printre care se numără securitate îmbunătățită, control de acces flexibil, management simplificat și integrare ușoară cu alte servicii de securitate. Implementarea protocolului 802.1X poate fi o soluție excelentă pentru orice organizație care dorește să-și protejeze rețeaua împotriva atacurilor și să asigure un control precis asupra accesului la rețea.

În concluzie, protocolul 802.1X este un standard important de securitate pentru rețelele de comunicații Ethernet. Acesta permite autentificarea utilizatorilor și a dispozitivelor la nivel de port, ceea ce face ca rețeaua să fie mult mai sigură și mai protejată împotriva atacurilor și a accesului neautorizat. Implementarea protocolului 802.1X poate oferi numeroase avantaje pentru rețelele Ethernet, inclusiv securitate îmbunătățită, control de acces flexibil, management simplificat și integrare ușoară cu alte servicii de securitate.

Acum vom discuta despre cum să configurați un server 802.1X în MikroTik. Configurarea unui server 802.1X în MikroTik implică următoarele etape:

1. Configurați serverul RADIUS:

Primul pas este să configurați serverul RADIUS pe routerul MikroTik. Acesta este necesar pentru a permite serverului 802.1X să comunice cu dispozitivele care se conectează la rețea. Pentru a configura serverul RADIUS, urmați acești pași:

a. Accesați interfața de configurare a routerului MikroTik.

b. Selectați meniul "Radius" din bara laterală stângă și faceți clic pe butonul "Servers".

c. Faceți clic pe butonul "+" pentru a adăuga un nou server RADIUS.

d. Introduceți adresa IP a serverului RADIUS, portul și cheia partajată.

e. Selectați metoda de autentificare pe care doriți să o utilizați, cum ar fi PAP (Password Authentication Protocol) sau CHAP (Challenge Handshake Authentication Protocol).

2. Configurați serverul 802.1X:

După ce serverul RADIUS este configurat, trebuie să configurați serverul 802.1X pe routerul MikroTik. Pentru a face acest lucru, urmați acești pași:

a. Accesați interfața de configurare a routerului MikroTik.

b. Selectați meniul "Interfaces" din bara laterală stângă și faceți clic pe butonul "802.1X".

c. În fereastra care se deschide, faceți clic pe butonul "Settings".

d. Configurați serverul 802.1X, inclusiv interfața la care se conectează dispozitivele, tipul de autentificare și serverul RADIUS care să fie utilizat.

e. Salvați setările.

3. Configurați autentificarea utilizatorilor:

După ce serverul 802.1X este configurat, trebuie să configurați autentificarea utilizatorilor. Acest lucru se face de obicei prin intermediul serverului RADIUS. Pentru a configura autentificarea utilizatorilor, urmați acești pași:

a. Accesați interfața de configurare a serverului RADIUS.

b. Configurați utilizatorii și parolele în funcție de nevoile dvs.

c. Configurați setările de autentificare, cum ar fi modul în care se face autentificarea și serverul 802.1X care să fie utilizat.

4. Configurați dispozitivele client:

În final, trebuie să configurați dispozitivele client pentru a se conecta la rețeaua dvs. Configurarea dispozitivelor client diferă în funcție de dispozitiv, dar trebuie să urmați instrucțiunile furnizate de producător pentru a se conecta la rețea prin intermediul protocolului 802.1X.

Acestea sunt pașii generali pentru a configura un server 802.1X în MikroTik. Este important să rețineți că acestproces poate varia în funcție de configurația specifică pe care doriți să o utilizați, dar acești pași ar trebui să ofere o idee generală despre ceea ce este necesar.

În ceea ce privește avantajele implementării 802.1X, aceasta poate aduce o serie de beneficii pentru rețelele dvs. de afaceri, cum ar fi:

1. Securitate îmbunătățită:

802.1X oferă o securitate mai mare pentru rețelele dvs. prin utilizarea autentificării bazate pe certificat sau pe parole. Aceasta înseamnă că doar utilizatorii autorizați pot accesa rețeaua dvs.

2. Mai puține probleme cu dispozitivele necunoscute:

Dacă aveți o rețea deschisă sau cu autentificare ușoară, dispozitivele necunoscute pot accesa cu ușurință rețeaua dvs. și pot aduce probleme de securitate sau de performanță. Cu 802.1X, dispozitivele trebuie să fie autentificate înainte de a avea acces la rețeaua dvs.

3. Administrare mai ușoară a rețelei:

802.1X poate ajuta la reducerea numărului de conturi de utilizator și de parole care trebuie gestionate pentru rețeaua dvs. În plus, poate ajuta la identificarea și eliminarea dispozitivelor neautorizate care sunt conectate la rețeaua dvs.

În concluzie, protocolul 802.1X poate fi o modalitate utilă de a securiza rețelele dvs. și de a gestiona mai eficient accesul utilizatorilor. Implementarea sa într-un server MikroTik poate fi destul de simplă și poate aduce beneficii semnificative pentru rețeaua dvs.