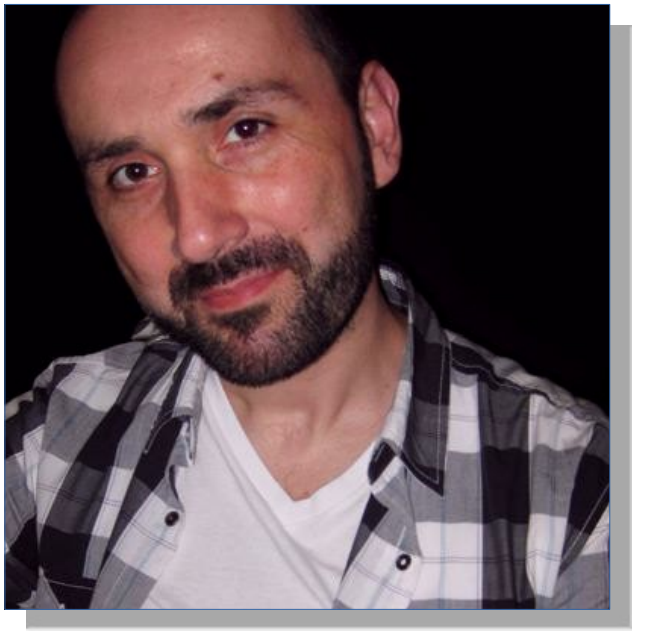
mBUM

802.1x czyli kontrola dostępu do sieci przewodowych i bezprzewodowych

15.10.2022

Jacek Rokicki

- w IT od 1998,
- z MikroTik od 2011,
- entuzjasta systemów operacyjnych z rodziny *nix,
- sys/net/dev ops
- architekt wysoko dostępnych rozwiązań z wykorzystaniem FLOSS,
- na co dzień pomagam w rozwoju kilku platform OTT



MikroTik
MTCNA
MTCRE
MTCINE
MTCSWE
MTCSE
MTCTCE
MTCIPv6E
MTCUME
MTCWE
MTCEWE

Agenda

- Historia protokołu 802.1.x
- Zalety i ograniczenia
- Architektura
- Jak to działa
- Serwery uwierzytelniające
- Obsługa w MT (dot1x)
- WLAN i 802.1x
- Co z urządzeniami typu kamera, drukarka, czujnik środowiskowy?
- Bezpieczeństwo
- Live demo
- Zakończenie

Historia 802.1x

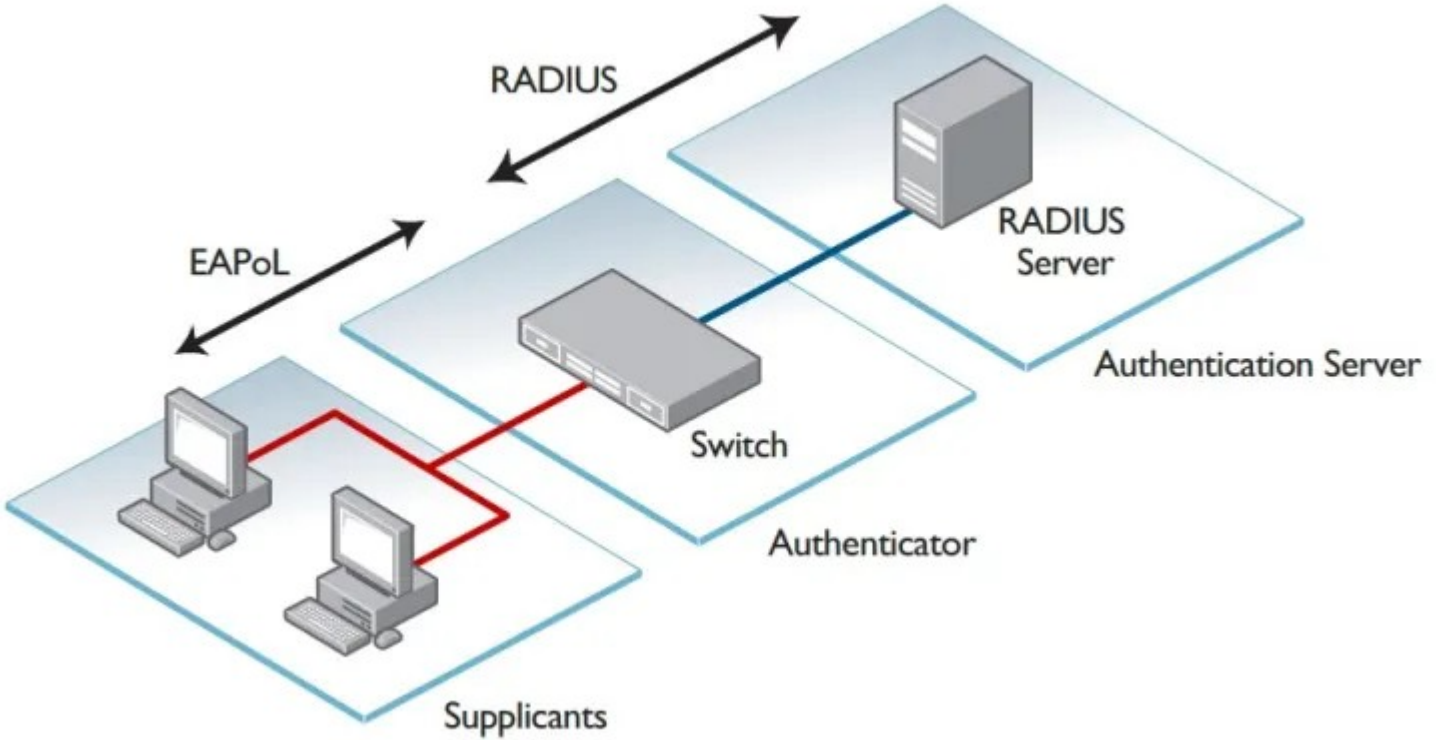
- Standard IEEE dla PNAC (port-based network access control)
- Definiuję enkapsulację EAP w sieciach 802 oraz 802.11, nazywany też EAPoL
- Powstał w 2001 dla sieci przewodowych (Token Ring, FDDI, Ethernet)
- W 2004 rozszerzony o obsługę sieci bezprzewodowych 802.11
- W 2010 dodano obsługę mechanizmów MACsec oraz DevID zwiększających bezpieczeństwo

Zalety i ograniczenia

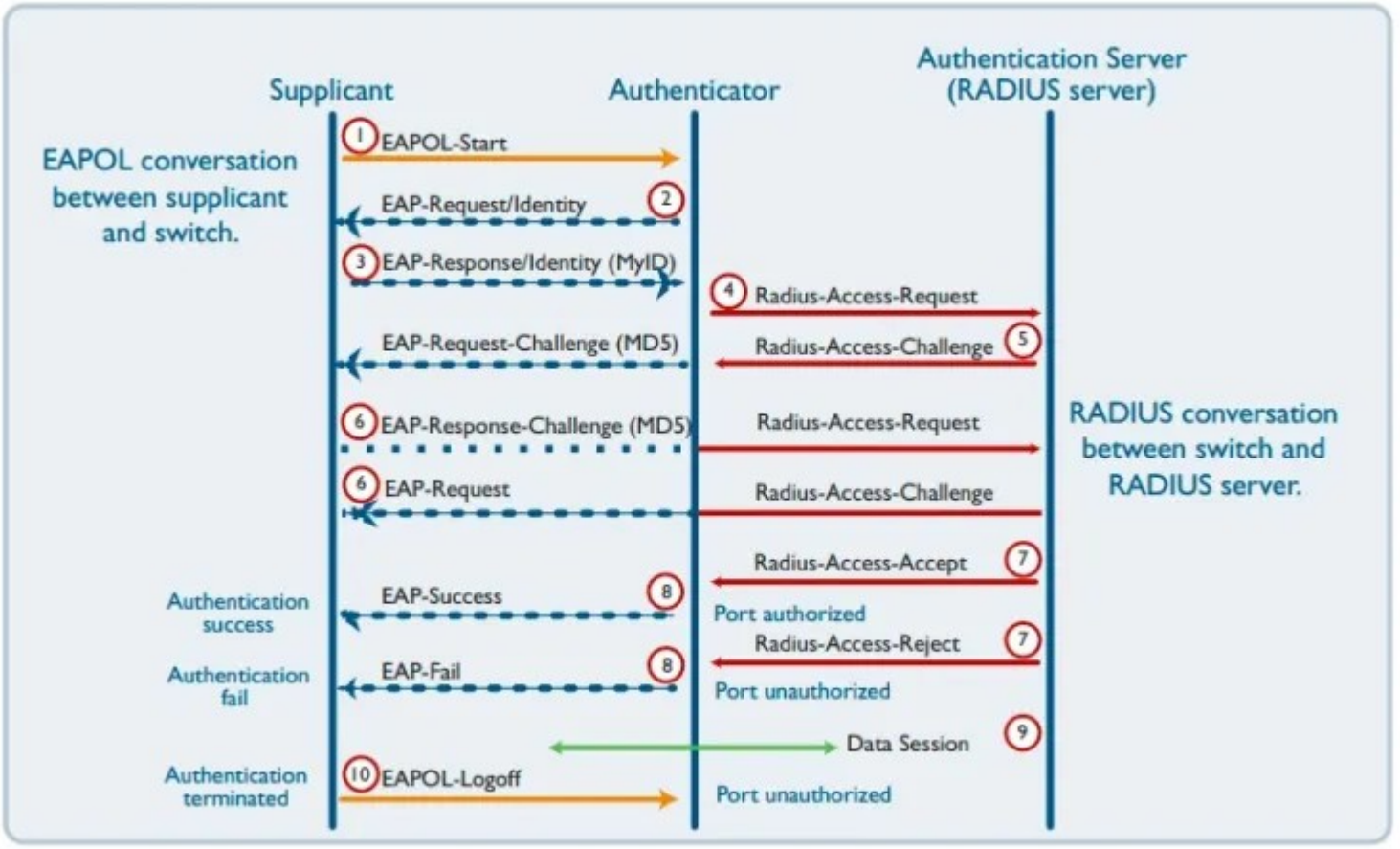
- Otwarty standard
- Bezpieczeństwo
- Elastyczność
- Przejrzystość

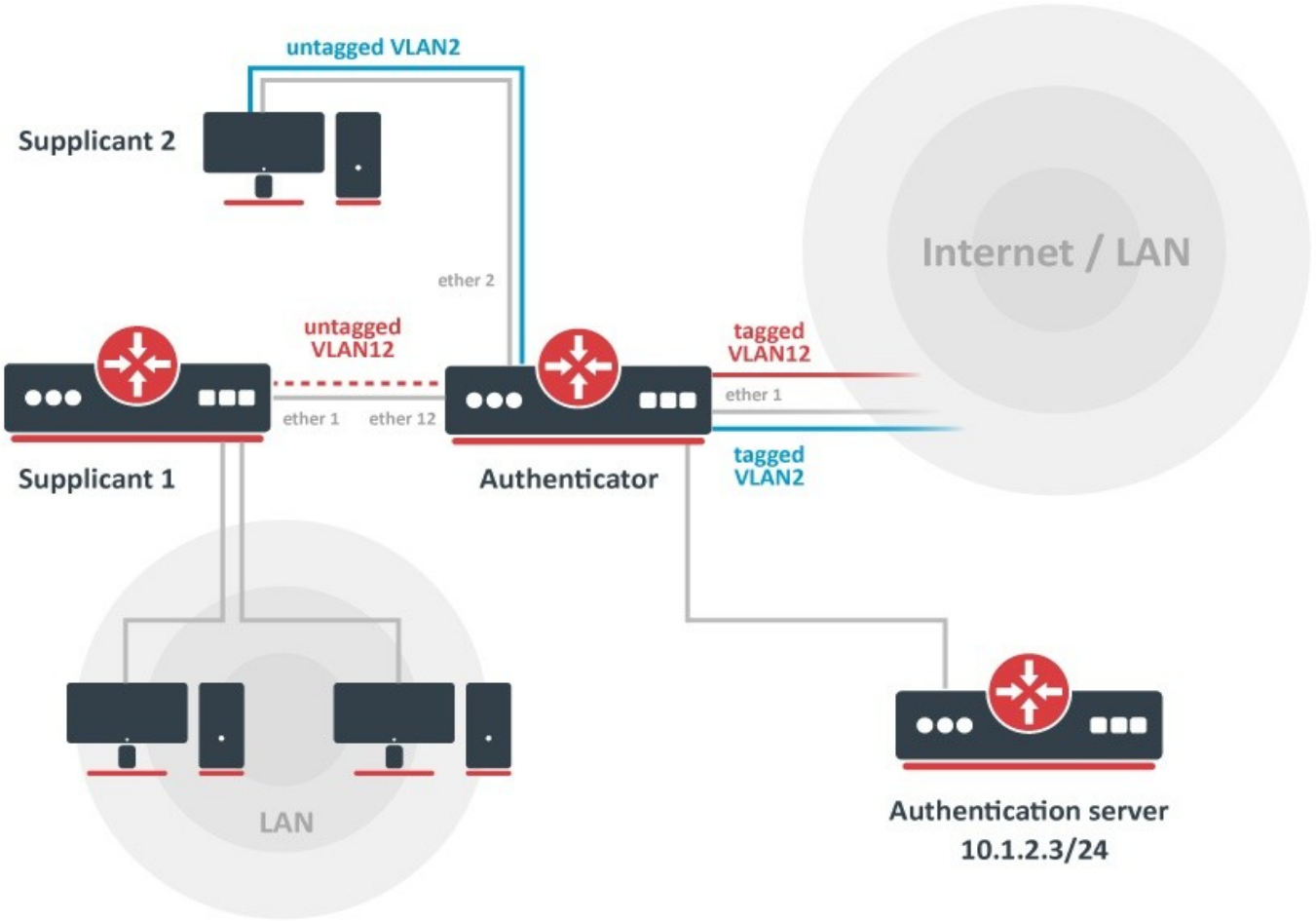
- Wymaga suplikanta
- Wprowadza opóźnienia w dostępie do portu
- Dość złożony proces wdrożenia

Architektura



Jak to działa?




untagged VLAN2
Supplicant 2
ether 2
Internet / LAN
untagged
VLAN12
tagged
VLAN12
ether 1
ether 1
ether 12
Supplicant 1
Authenticator
tagged
VLAN2
LAN
Authentication server
10.1.2.3/24

Serwery uwierzytelniające

- MikroTik User Manager
- freeRADIUS
- Microsoft Network Policy Server

Konfiguracja – serwer Radius

Parametry konfiguracyjne przesyłamy jako atrybuty.
Zestaw atrybutów freeRADIUS: https://freeradius.org/rfc/attributes.html
Dodatkowe atrybuty MikroTika:
https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client/vendor_dictionary

Parametry dla sieci przewodowych:

Tunnel-Private-Group-ID = 20 (vlanID)
Tunnel-Medium-Type = 6 (802)
Tunnel-Type = 13 (VLAN)

Parametry dla sieci bezprzewodowych:

Mikrotik-Wireless-VLANID = 20 (vlanID)
Mikrotik-Wireless-VLANIDtype = 0 (802.1q)

Uwaga: w słowniku freeRADIUS-a jest błąd w nazwie atrybutu Mikrotik-Wireless-VLANIDtype

Konfiguracja MikroTik usermanager:
https://mbum.pl/archive/mbum5/MBUM5-CAPsMAN-EAP.pdf

Konfiguracja MicroSoft NPS:
https://mbum.pl/archive/mbum5/Profilowanie%20Sesji%20VPN.pdf

Konfiguracja freeRADIUS (Debian 11):
apt install -y freeradius

/etc/freeradius/3.0/clients.conf

```
client MT {
    ipaddr = 192.168.88.100
    secret = password1234
    nas_type = other
}
```

/etc/freeradius/3.0/users

```
us1 Cleartext-Password := "us1"
    Tunnel-Private-Group-ID = 20,
    Tunnel-Medium-Type = 6,
    Tunnel-Type = 13
```

Porty, na których działa Radius

1812/udp - authentication
1813/udp - accounting

Serwer freeRadius wspiera kilka rodzajów baz danych o użytkownikach np.: file, sql, ldap, active directory.

W przykładzie na poprzednim slajdzie została wykorzystana najprostsza metoda stworzenia bazy z poświadczeniami przez dodanie użytkownika wraz z niezaszyfrowanym hasłem i atrybutami do pliku wskazanego w konfiguracji usługi.

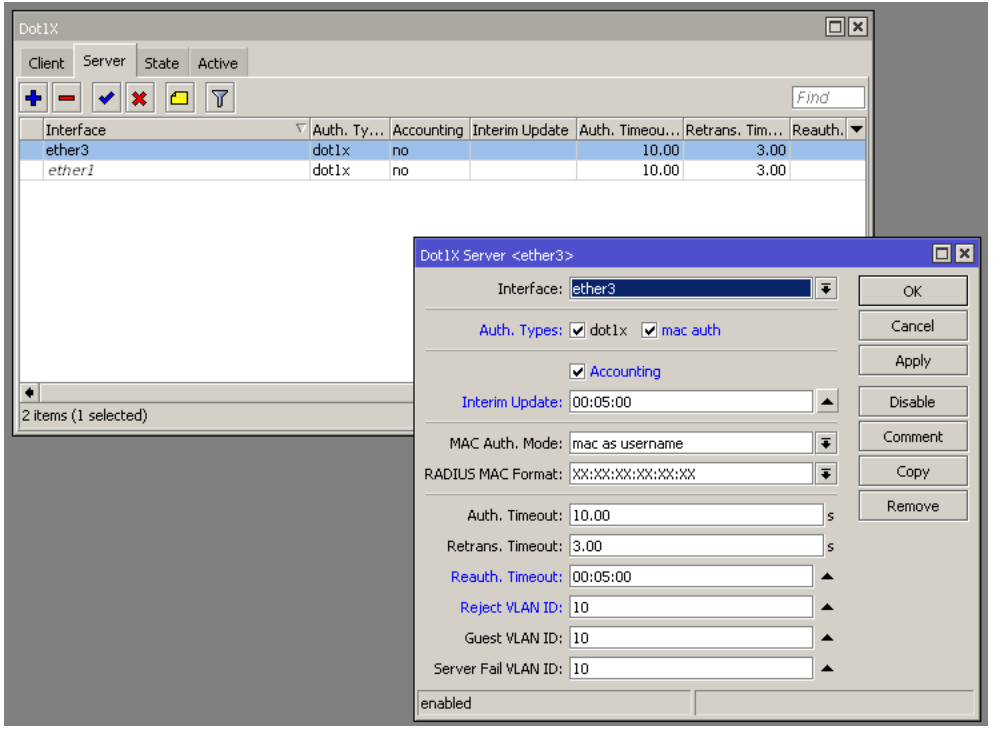
Konfiguracja – authenticator

MAJOR CHANGES IN v6.45: (04.2019)

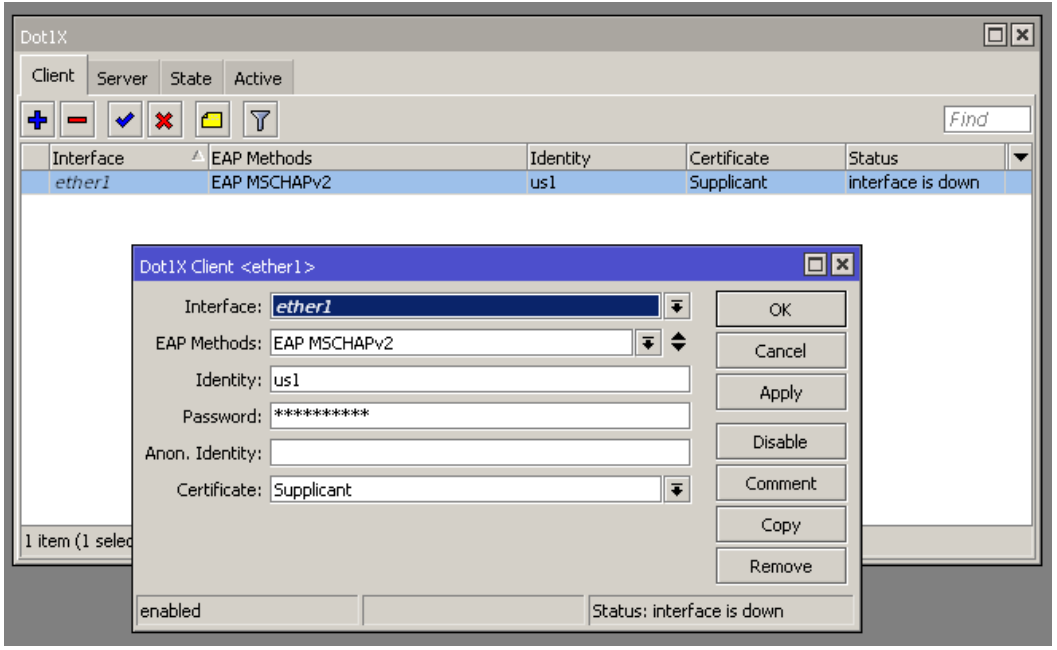
!) dot1x - added support for IEEE 802.1X Port-Based Network Access Control (CLI only);

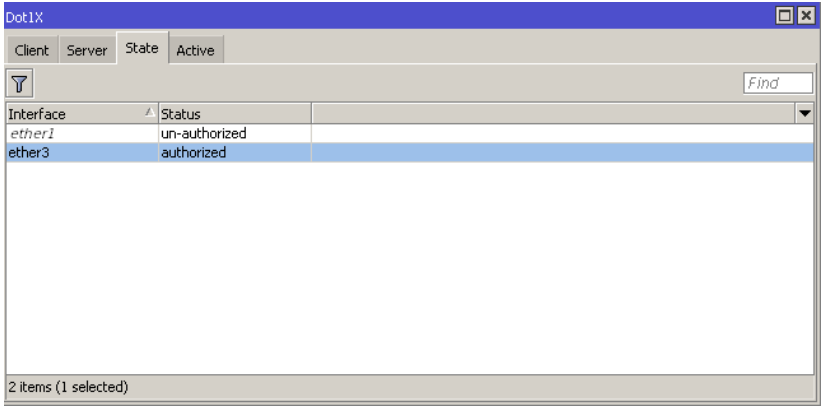
Stan bieżący, RouterOS 7.5 posiada wsparcie dla ról:

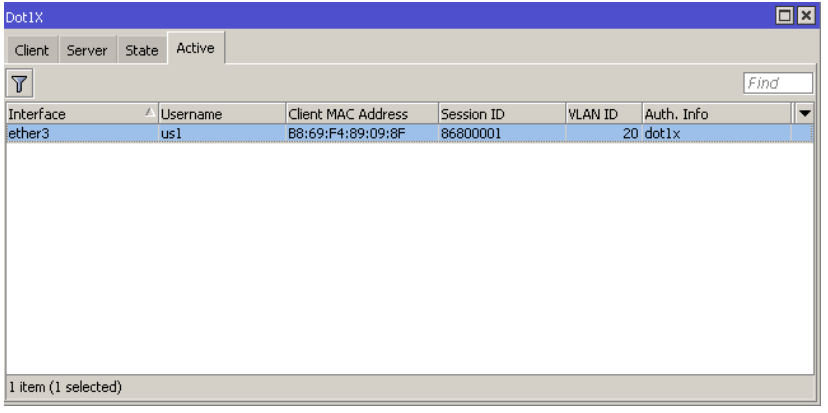
- supplicant
- authenticator (w v7.x dodatkowo guest i server fail vlan)



Konfiguracja – supplicant







- Reject vlanid – vlan, do którego trafia stacja błędnie uwierzytelniona (RADIUS odpowie komunikatem Access-Reject)

- Guest vlanid – vlan, do którego trafi stacja nie obsługująca 802.1x i nie posiadająca konfiguracji dla uwierzytelniania mac-iem

- Server fail vlanid – vlan, do którego trafi stacja w sytuacji awarii serwera RADIUS

Warto uruchomić w vlanie guest hotspot pozwalający, po uwierzytelnieniu przez uprawnionego użytkownika, połączyć się z interface konfiguracji/dodawania nowych userów. Można również skorzystać z funkcji trial hostspota i umożliwić czasowy dostęp do Internetu.

WLAN i 802.1x (WPA2 EAP)

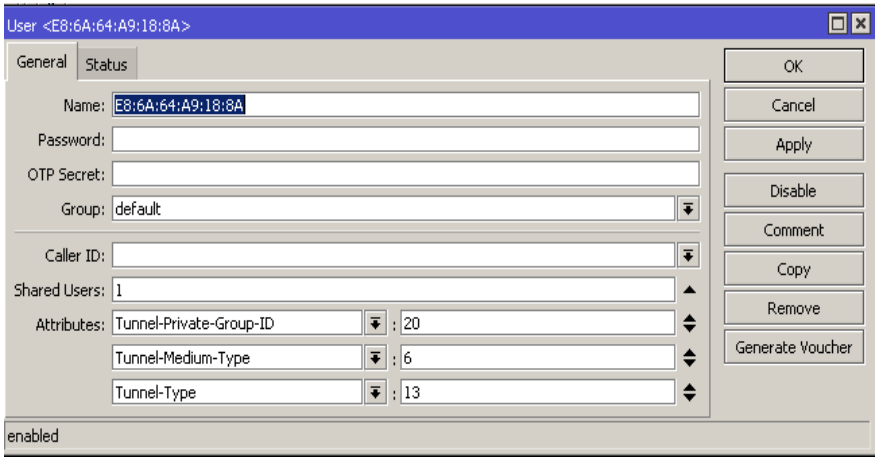
/caps-man datapath
add bridge=bridge-main name=myAP vlan-mode=use-tag
/caps-man security
add authentication-types=wpa2-eap eap-methods=passthrough eap-radius-accounting=no encryption=aes-ccm group-encryption=aes-ccm name=myAP_sec
/caps-man configuration
add country=poland datapath=myAP_dp mode=ap name=myAP_cfg security=myAP_sec ssid=myAP
/caps-man manager
set enabled=yes
/caps-man provisioning
add action=create-dynamic-enabled hw-supported-modes=gn master-configuration=myAP_cfg name-format=identity

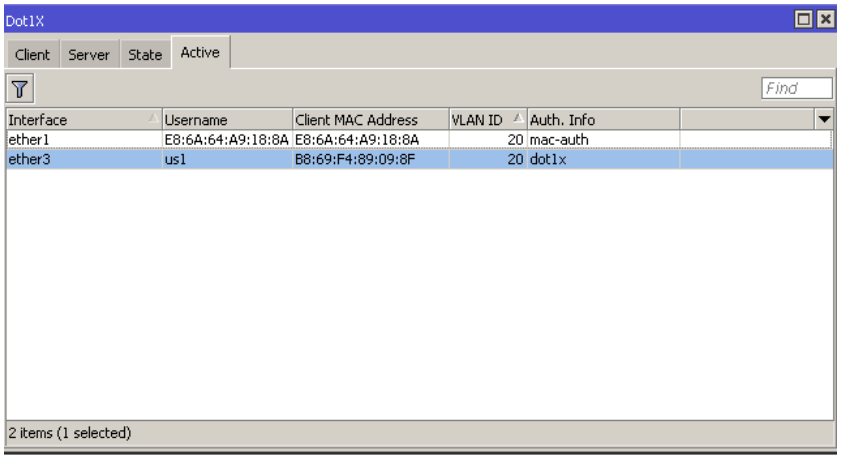
/interface wireless cap
set bridge=bridge-main caps-man-addresses=capsman_IP enabled=yes interfaces=wlan1

Prości klienci

Urządzenia nie posiadające suplikanta uwierzytelniają się swoim adresem MAC

/interface/dot1x/server/add auth-types=mac-auth mac-auth-mode=mac-as-username interface=ether1 accounting=no auth-timeout=10 retrans-timeout=3





Bezpieczeństwo 802.1x

- Wymusza segmentacje sieci i podział na role
- Domyślnie porty przełączników nie przekazują ruchu do wrażliwych podsieci
- Możemy monitorować częstotliwość i czas logowania stacji/użytkowników
- Zmniejsza codzienny nakład pracy administratora oraz minimalizuje pomyłki
- Umożliwia ochronę urządzeń klienckich przed podłączeniem do fałszywej sieci

Live demo
/
pytania

Dziękuję za uwagę