Контрол на достъпа при MikroTik с Dot1X

MikroTik Net Camp 2020

Рожен

Петър Димитров

За мен - Петър Димитров

- MikroTik Trainer: от 2013 г.
- Ubiquiti Trainer: от 2018 г.
- Предлагани обучения:

Въведение в компютърните мрежи

MTCNA, MTCSWE, MTCRE, MTCINE, MTCWE,

MTCEWE, MTCTCE, MTCUME, MTCSE, MTCIPv6E

UBWS, UBWA, UBRSS, UBRSA, UNS, UEWA

Мрежова сигурност

- Защитата на мрежовите ресурси е ключов момент във всяка съвременна мрежа, като използваме комбинация от различни технологии за постигане на адекватна сигурност.
- На Net Camp 2017 говорихме за "Добри практики в мрежовата сигурност", но тогава все още не разполагахме с поддръжка на Dot1X в RouterOS.

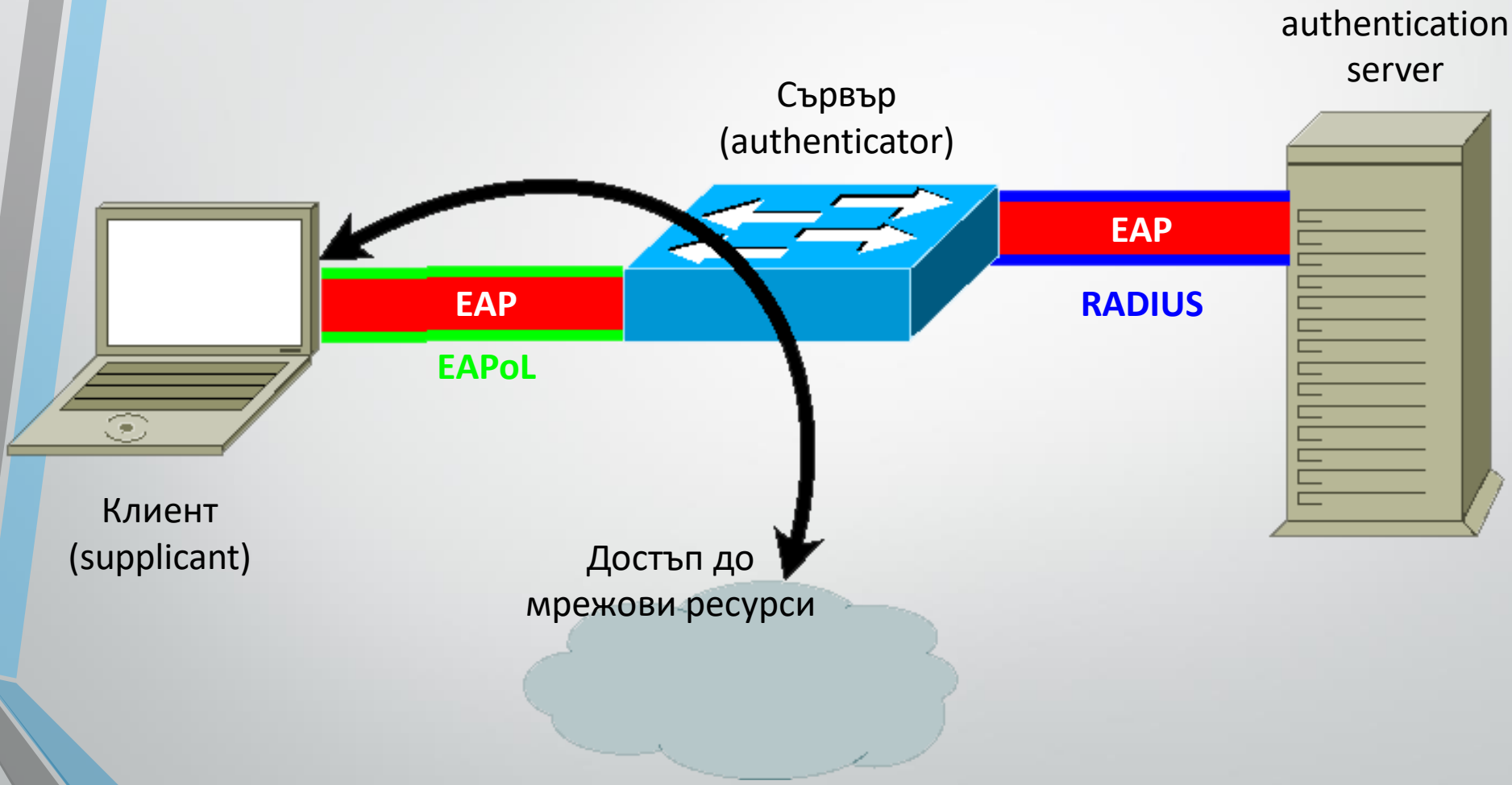
Какво е Dot1X?

- Dot1X е имплементация на IEEE 802.1X стандарта, която осигурява достъп до мрежата чрез EAP автентикация, като може да се конфигурира за всеки порт на мрежовите устройства.
- Най-типичното приложение е за портовете на switch-овете, към които (могат да) се закачат потребителите.
- Преди автентикация Dot1X сървъра блокира всякакъв трафик през порта, освен пакетите за EAP.

Как работи Dot1X?

- Клиента, наричан supplicant, се свързва към порта на мрежовото устройство - например switch, който играе ролята на сървър (authenticator), като се опитва да се автентицира използвайки EAP, капсулиран в EAPOL (единствените фреймове, които сървъра не блокира).
- Сървъра (authenticator-a) отнася EAP автентикацията към RADIUS, който се нарича authentication server.
- При успешна автентикация сървъра (authenticator-a) отблокира порта при съответните параметри.

Как работи Dot1X?



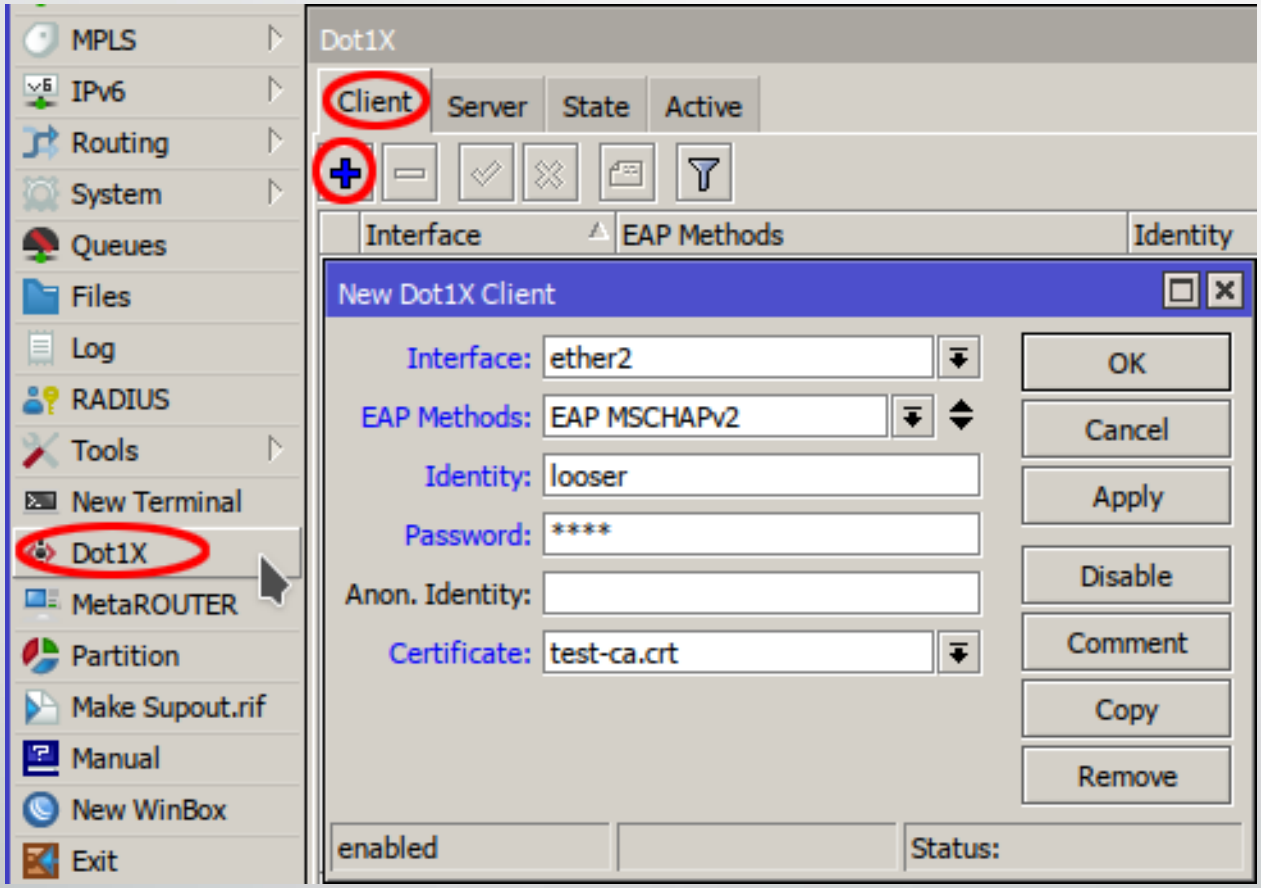
С какво разполагаме в RouterOS?

- От лятото на 2019-та (от версия 6.45.1) в RouterOS имаме имплементирани 802.1X клиент (supplicant) и сървър (authenticator).
- В RouterOS 7 ще има изцяло нов User Manager, който поддържа EAP автентикация (достъпен от версия v7.0beta4).
- С това на практика можем да покрием всички необходими компоненти за имплементиране на Dot1X изцяло с RouterOS.

Конфигурация на клиент

- Ако вашия MikroTik е закачен към порт на мрежово устройство, което изисква автентикация, трябва да настроите Dot1X клиент
- Текущо клиента поддържа EAP-TLS, EAP-TTLS, EAP-MSCHAPv2 и PEAPv0/EAP-MSCHAPv2

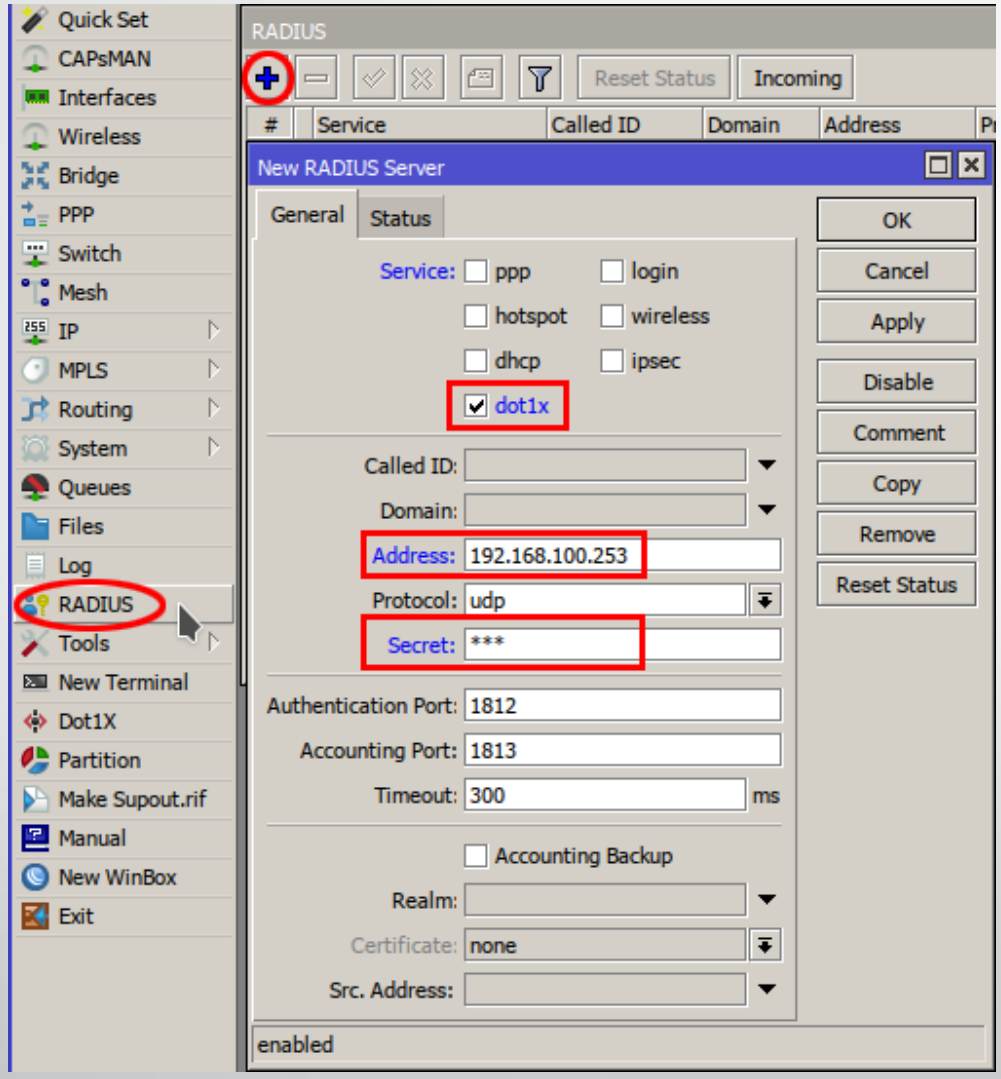
Конфигурация на клиент



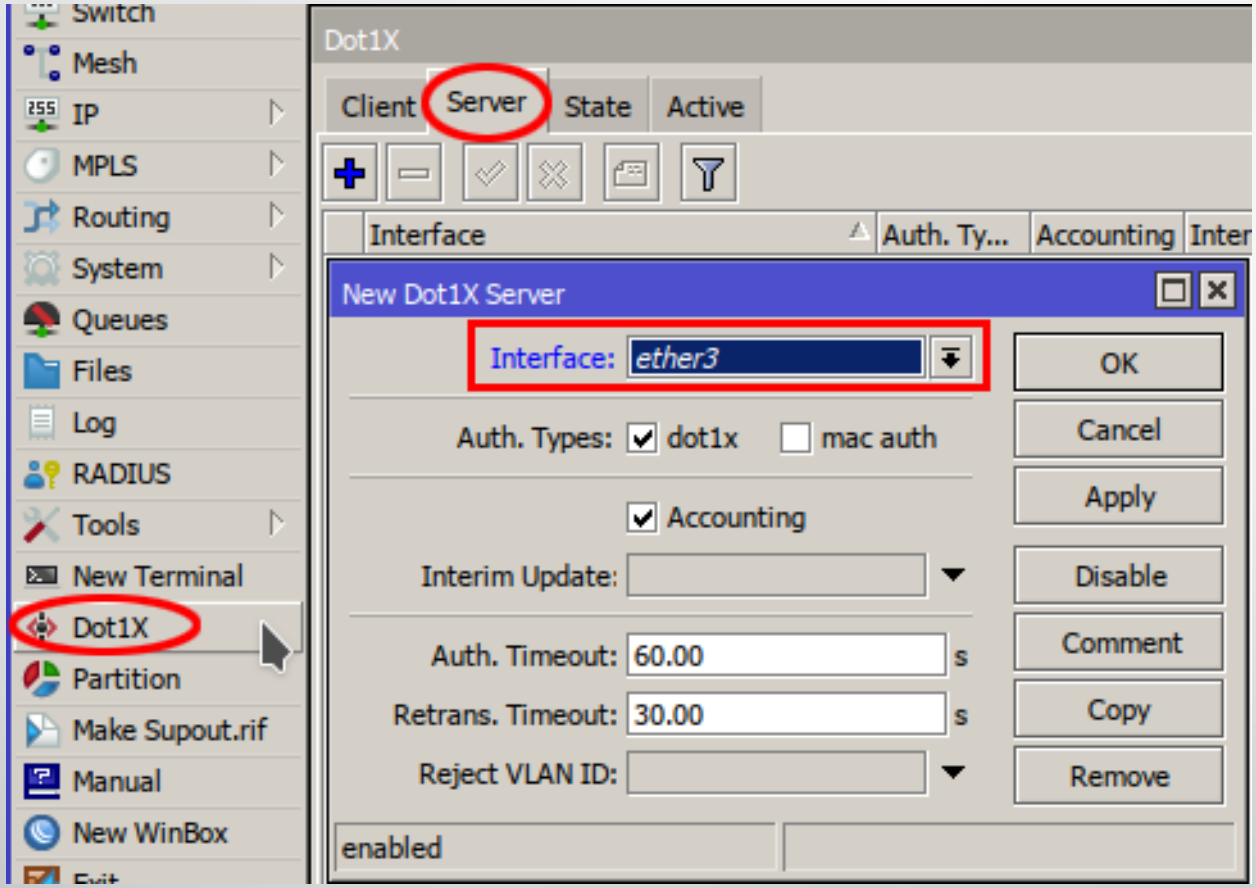
Конфигурация на сървър

- Когато искате потребителите да се автентицират, за да имат какъвто и да е достъп до мрежата, конфигурирате Dot1X сървър за всеки порт, зад който ще изисквате автентикация
- Не забравяйте, че автентикацията се отнася към RADIUS сървър, т.е. трябва да добавите RADIUS сървър към който да се обръщате за Dot1X

Конфигурация на сървър (RADIUS)



Конфигурация на сървър (Dot1X)



Работа с VLAN-и

- Можете да използвате RADIUS атрибути Tunnel-Type, Tunnel-Medium-Type и Tunnel-Private-Group-ID, за да укажете в кой VLAN желаете да бъде конфигуриран порта при автентикация на всеки потребител:

Tunnel-Type (integer) = 13

Tunnel-Medium-Type (integer) = 6

Tunnel-Private-Group-ID (string) = желания VLAN id

Демонстрация

- Да направим следната първоначална подготовка на switch-а, с който ще имплементираме Dot1X:
  - Ether1 ще остане извън конфигурацията (за management)
  - Ether2 ще конфигурираме като trunk порт
  - vlan100 е нашата management мрежа
  - Засега няма да използваме vlan-и за потребителите
  - Switch-а ще получи адрес в management мрежата по DHCP

Демонстрация

```
/interface ethernet
set [ find default-name=ether1 ] name=ether1-mgmt
set [ find default-name=ether2 ] name=ether2-trunk

/interface list
add name=e1e2
add exclude=e1e2 include=all name=all-but-e1e2
/interface list member
add interface=ether1-mgmt list=e1e2
add interface=ether2-trunk list=e1e2
```

Демонстрация

```
/interface bridge
add name=bridge-all vlan-filtering=yes
/interface bridge port
add bridge=bridge-all interface=ether2-trunk
add bridge=bridge-all interface=all-but-e1e2
/interface bridge vlan
add bridge=bridge-all comment=Management tagged=\
ether2-trunk,bridge-all vlan-ids=100

/interface vlan add interface=bridge-all name=\
vlan100-mgmt vlan-id=100
/ip dhcp-client add disabled=no interface=vlan100-mgmt
```

Демонстрация

- На адрес 192.168.100.253 имаме RADIUS сървър, към който да отнесем автентикацията за Dot1X.
- За целта конфигурираме switch-а да го ползва:

```
/radius

add address=192.168.100.253 secret=123 service=dot1x
```

Демонстрация

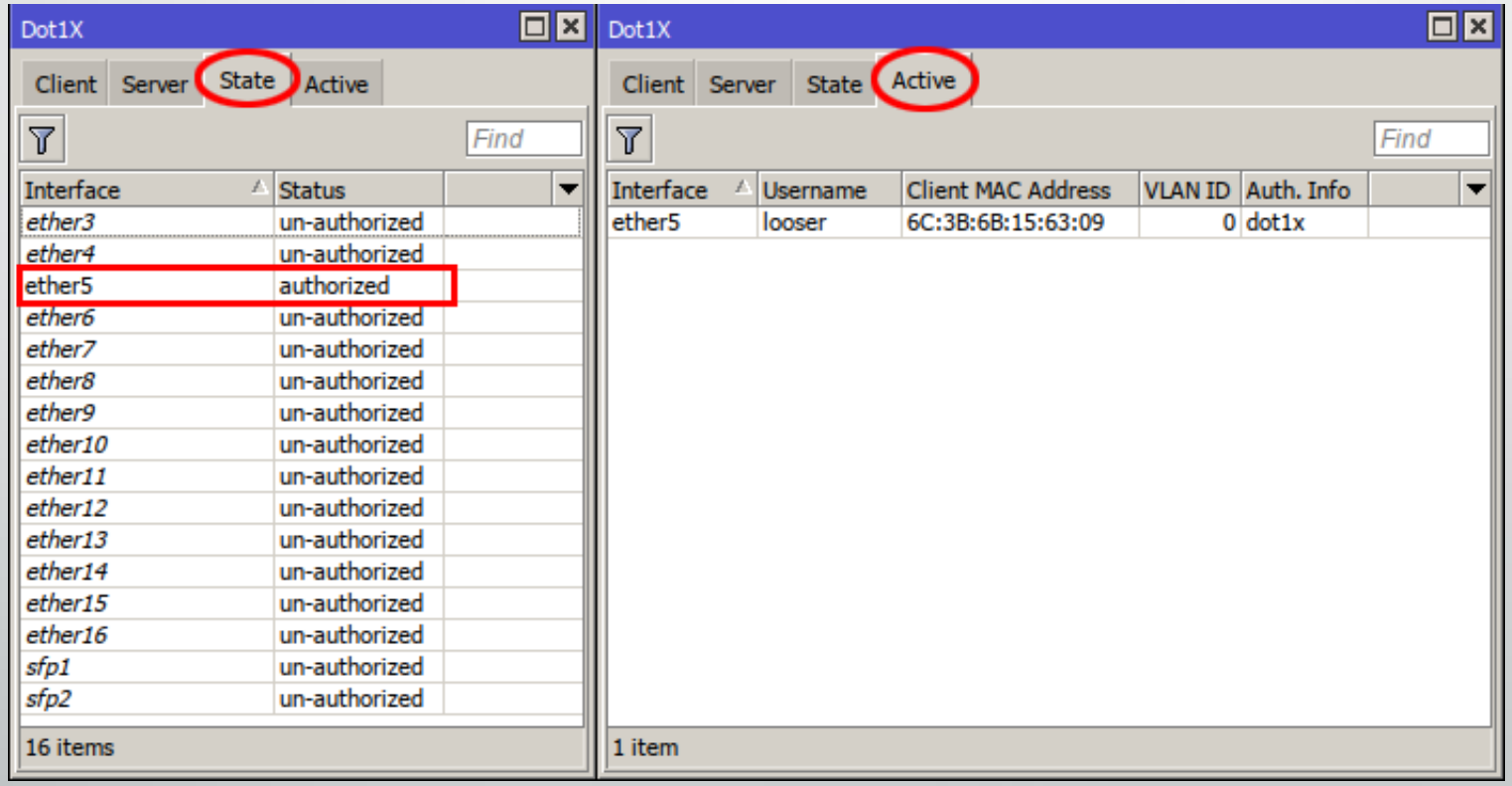
- Dot1X сървър може да бъде добавен към всеки конкретен интерфейс, зад който искаме клиентите да се автентицират, а може и да се използва списък с интерфейси.

- В нашия конкретен случай нека добавим Dot1X сървър с помощта на interface list за всички интерфейси, без management и trunk портовете:

```
/interface dot1x server

add interface=all-but-e1e2
```

Демонстрация

- Разполагаме с потребител looser с парола pass, след успешна автентикация зад ether5 резултата е:



Демонстрация

- Нека разширим конфигурацията с използване на различни vlan-и за потребителите
- Разполагаме с потребители looser10, looser20 и looser30, които са както следва с пароли pass10, pass20 и pass30 и получават Tunnel-Private-Group-ID съответно 10, 20 и 30
- Не забравяйте, че vlan filtering трябва да е включен на bridge интерфейса (vlan-filtering=yes)!

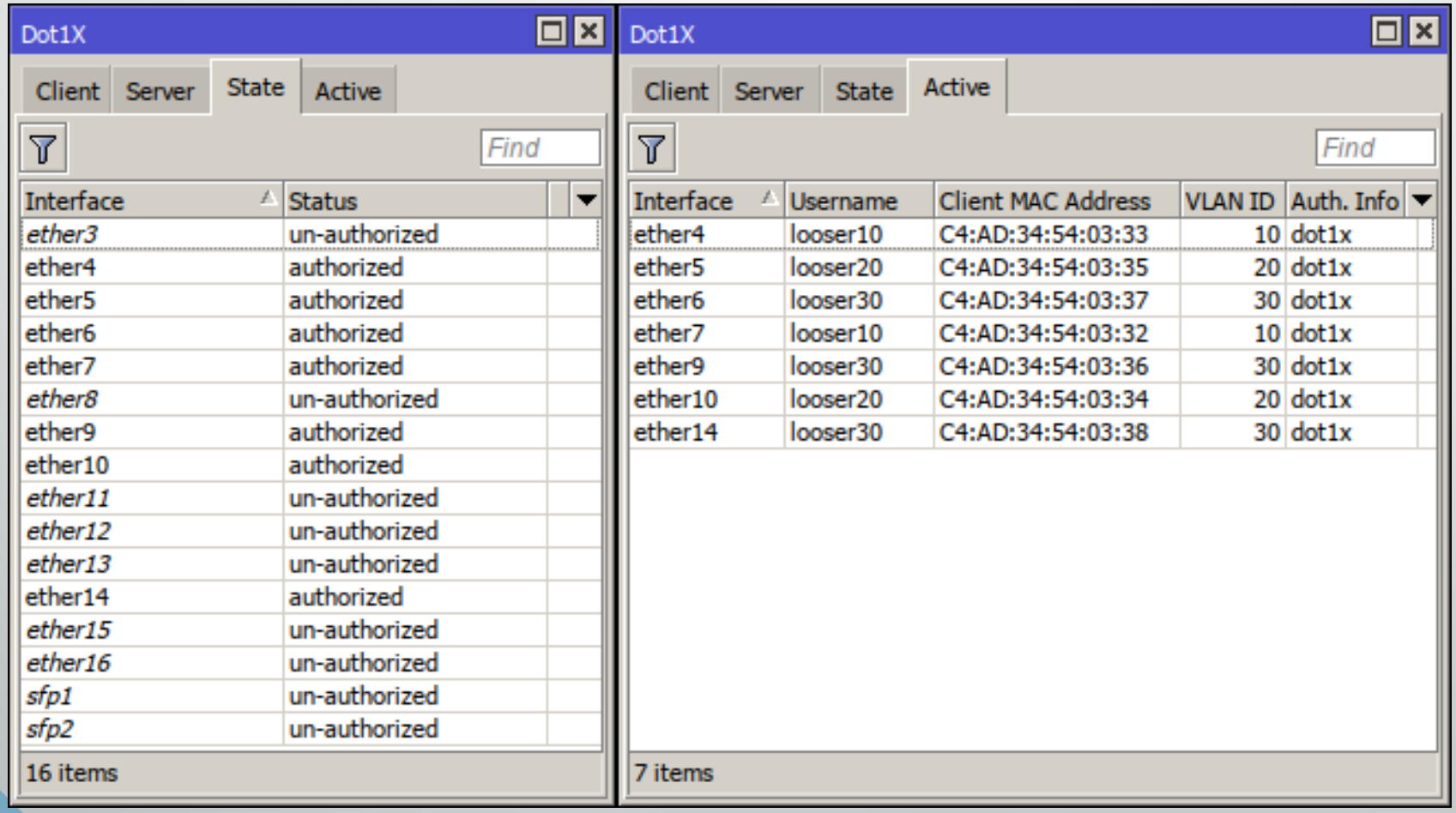
Демонстрация

- Да дефинираме новите vlan-и на switch-а:

```
/interface bridge vlan

add bridge=bridge-all tagged=ether2-trunk vlan-ids=10

add bridge=bridge-all tagged=ether2-trunk vlan-ids=20

add bridge=bridge-all tagged=ether2-trunk vlan-ids=30
```

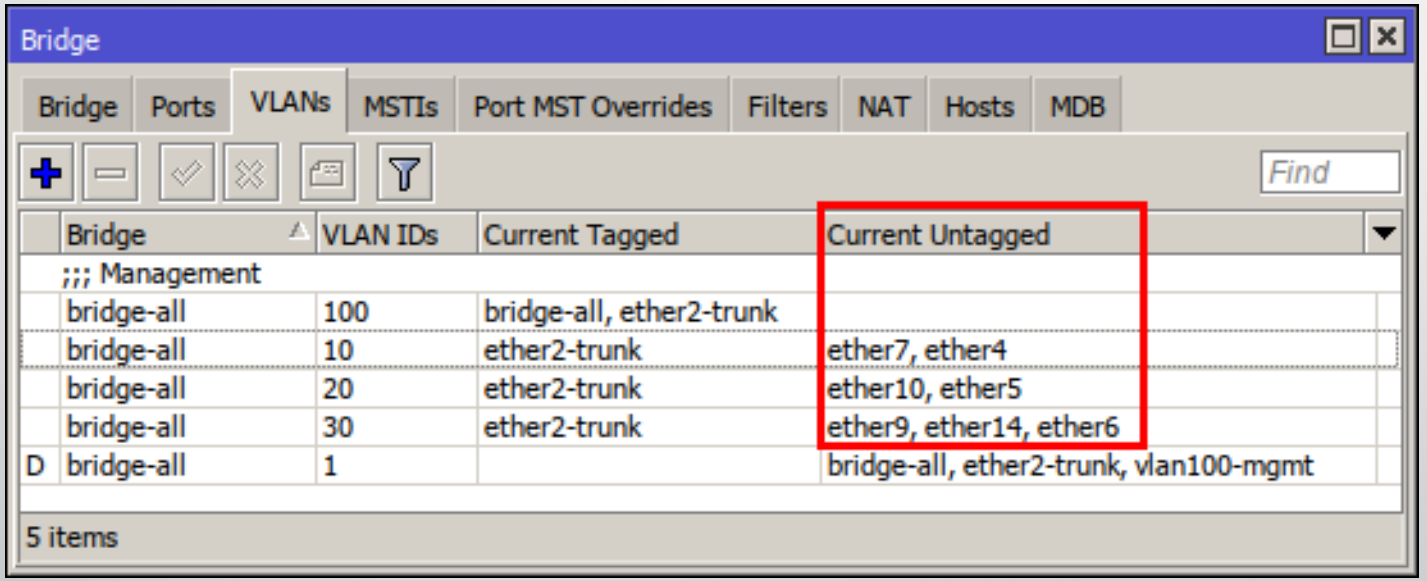
Демонстрация

- След автентикация резултата е:



Демонстрация

- Да обърнем внимание и на untagged vlan-ите на bridge-а по портове:



Благодаря за вниманието!

Допълнение: user-manager конфигурация

```
/user-manager router
add address=192.168.100.252 name=dot1x_switch shared-secret=123

/user-manager attribute
add name=Tunnel-Private-Group-ID type-id=81 value-type=string
add name=Tunnel-Type type-id=64 value-type=uint32
add name=Tunnel-Medium-Type type-id=65 value-type=uint32

/user-manager profile
add name=test-profile

/user-manager user
add name=looser password=pass
add attributes=Tunnel-Type:13,Tunnel-Medium-Type:6,Tunnel-Private-Group-ID:10 name=looser10 password=pass10
add attributes=Tunnel-Type:13,Tunnel-Medium-Type:6,Tunnel-Private-Group-ID:20 name=looser20 password=pass20
add attributes=Tunnel-Type:13,Tunnel-Medium-Type:6,Tunnel-Private-Group-ID:30 name=looser30 password=pass30

/user-manager user-profile
add profile=test-profile user=looser
add profile=test-profile user=looser10
add profile=test-profile user=looser20
add profile=test-profile user=looser30

/user-manager
set certificate=test-server enabled=yes
```