

# Laboratoare Administarea Retelelor de Calculatoare

Securizarea rețelei cu Radius,  
Dot1X și VLAN



# Setarea serverului Radius cu certificate

- In primul intram in System→Certificates si facem un CA (conditia suficienta este sa aibe bifat crl sign si key cert sign).
- Dupa care facem un certificat pentru radius cu optiunile digital signature, key encipherment si tls server apoi semnam cu CA-ul creat anterior si bifam ca trusted.
- In User Manager→Routers→Settings activam serverul si punem certificatul.
- Acum putem face un user (in cazul meu test)

The image shows two overlapping windows from a network management application. The top window is titled 'Certificate <radius>' and has tabs for 'General', 'Key Usage', and 'Status'. The 'Key Usage' tab is active, showing a list of checkboxes for key usage options. The 'Status' tab is also visible, showing a checkbox for 'Enabled' which is checked. The bottom window is titled 'New User' and has tabs for 'General' and 'Status'. The 'General' tab is active, showing fields for 'Name' (test), 'Password' (test123), 'OTP Secret', 'Group' (default), 'Caller ID', 'Shared Users' (1), and 'Attributes'. The 'Status' tab is also visible, showing a checkbox for 'enabled' which is checked.

**Certificate <radius> Settings**

**General** **Key Usage** **Status**

Key Usage: ☒ digital signature ☐ content commitment  
☒ key encipherment ☐ data encipherment  
☐ key agreement ☐ key cert. sign  
☐ crl sign ☐ encipher only  
☐ decipher only ☐ dvcs  
☐ server gated crypto ☐ ocsp sign  
☐ timestamp ☐ ipsec user  
☐ ipsec tunnel ☐ ipsec end system  
☐ email protect ☐ code sign  
☐ tls client ☒ tls server

Authentication Port: 1812  
Accounting Port: 1813  
Certificate: radius  
☐ Use Profiles  
Active Sessions: 0

☒ Enabled

**New User**

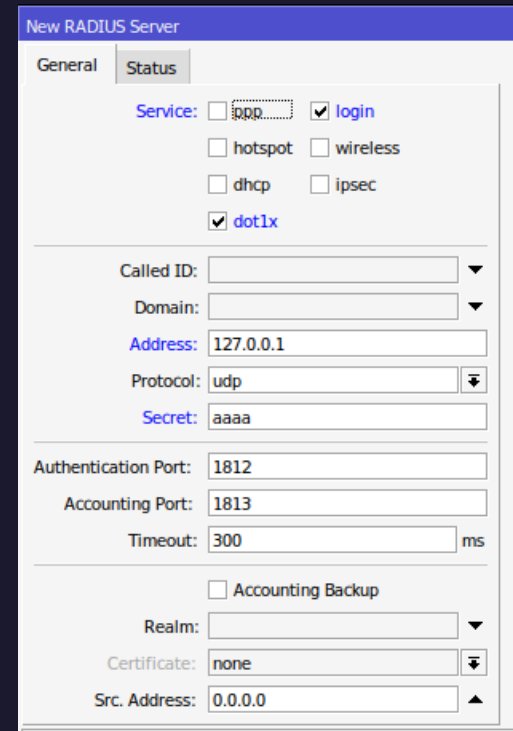
**General** **Status**

Name: test  
Password: test123  
OTP Secret:  
Group: default  
Caller ID:  
Shared Users: 1  
Attributes:

enabled

# Setarea serverului Radius cu certificate

- Acum facem un server nou de radius Radius→+ in care bifam login si dot1x , adresa setam 127.0.0.1 pentru ca ne conectam la acelasi router, alegem un secret intre radius si user manager (in cazul meu “aaaa”).
- In User Manager adaugam un nou router
- Acum vom face un interface list mergand in Interfaces→Inteface List→Lists si o vom numi dot1x (numele nu este important).



New RADIUS Server

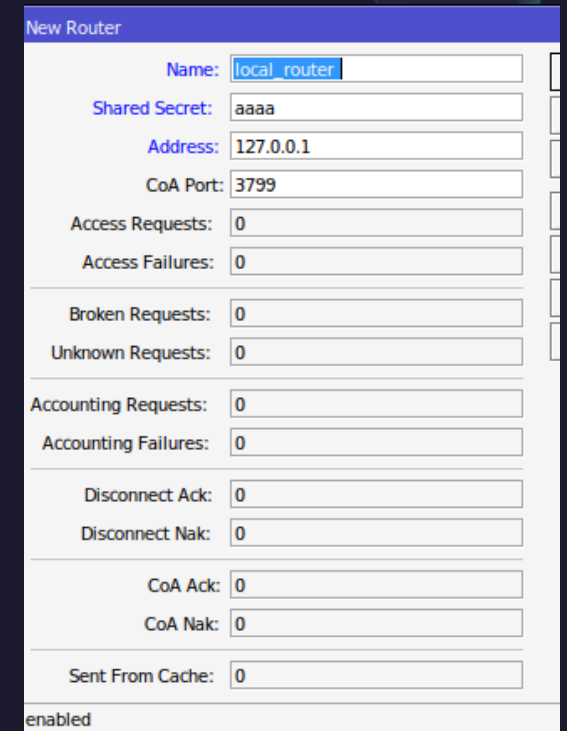
General Status

Service: ☐ ppp ☒ login  
☐ hotspot ☐ wireless  
☐ dhcp ☐ ipsec  
☒ dot1x

Called ID:   
Domain:   
Address: 127.0.0.1  
Protocol: udp  
Secret: aaaa

Authentication Port: 1812  
Accounting Port: 1813  
Timeout: 300 ms

☐ Accounting Backup  
Realm:   
Certificate: none  
Src. Address: 0.0.0.0

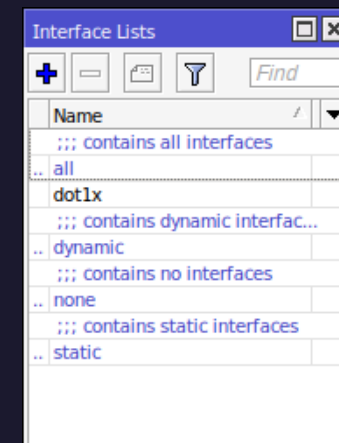


New Router

Name: local\_router  
Shared Secret: aaaa  
Address: 127.0.0.1  
CoA Port: 3799

Access Requests: 0  
Access Failures: 0  
Broken Requests: 0  
Unknown Requests: 0  
Accounting Requests: 0  
Accounting Failures: 0  
Disconnect Ack: 0  
Disconnect Nak: 0  
CoA Ack: 0  
CoA Nak: 0  
Sent From Cache: 0

enabled



Interface Lists

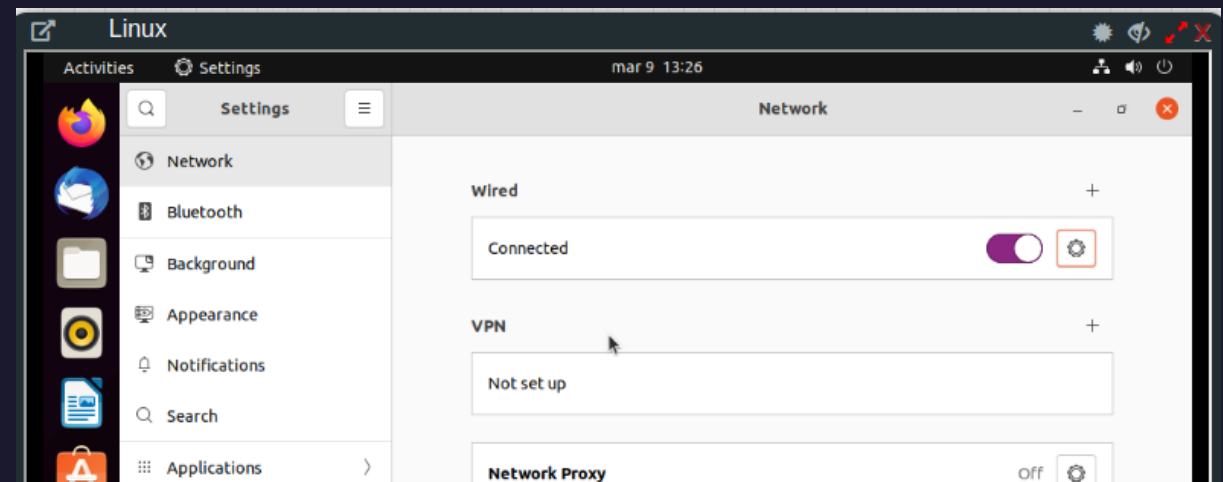
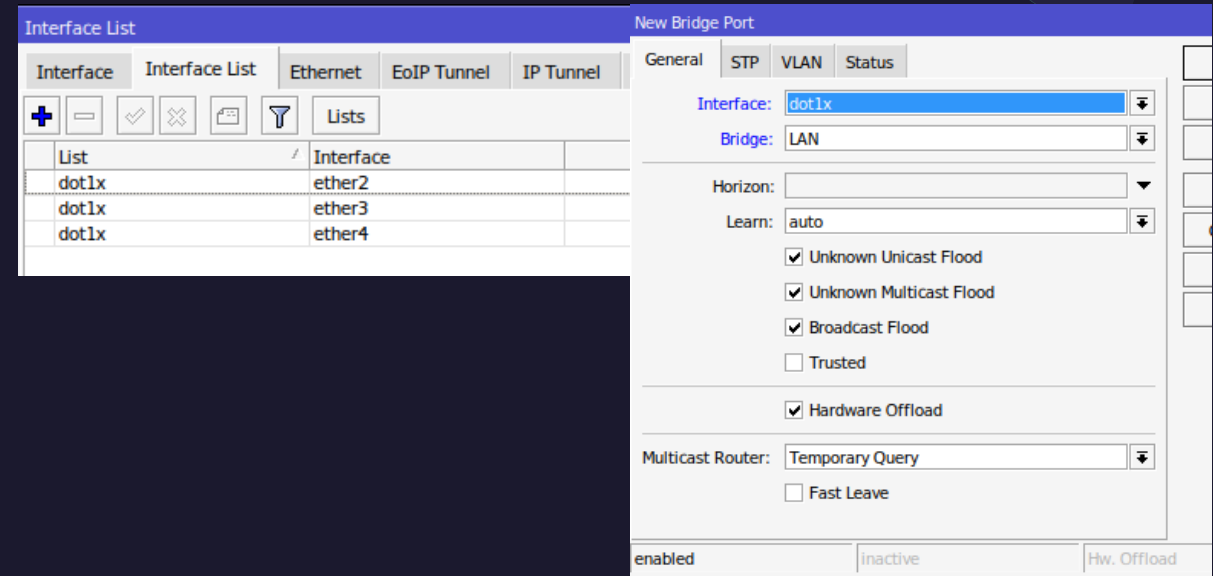
+ - Find

Name
... contains all interfaces
.. all
dot1x
... contains dynamic interfac...
.. dynamic
... contains no interfaces
.. none
... contains static interfaces
.. static

# Setarea serverului Radius cu certificate

- Dupa care adaugam in lista interfetele pe care le vom asigna serviciului dot1x
- Acum facem un bridge pe care il vom numi LAN si asignam lista dot1x facuta mai devreme.
- Acest lucru ne permite o alocare dinamica a porturilor si modificarea lor doar intr-un singur loc.
- Acum configuram un server de DHCP pentru bridge-ul lan (ex: 192.168.10.0/24)
- Si comenctam un Ubuntu Desktop pe una din interfetele asigante

Si putem observa ca suntem conectati.



# Setarea serviciului dot1x

- Acum putem sa intram in meniul DotIX unde vom face un server nou unde vom asigna lista dot1x.
- Dupa ce am activa serverul putem vedea in State ca porturile noastre nu sunt autorizate.
- Ele devin autorizate atunci cand dispozitivul termina cu succes procesul de autentificare.
- Am adaugat pentru debug doua reguli noi pentru manager si radius cu actiunea echo pentru a vedea in terminal logurile.

- Si vedem ca Ubuntu nu se mai poate conecta

Pentru a seta un timeout si a deautoriza dispozitivul putem seta Interim Update.

Dot1X Server <dot1x>

Interface: dot1x

Auth. Types: ☒ dot1x ☐ mac auth

☒ Accounting

Interim Update: Interim Update

Auth. Timeout: 60.00 s

Retrans. Timeout: 30.00 s

Reauth. Timeout: s

Reject VLAN ID: s

Guest VLAN ID: s

Server Fail VLAN ID: s

enabled

Dot1X

Client Server State Active

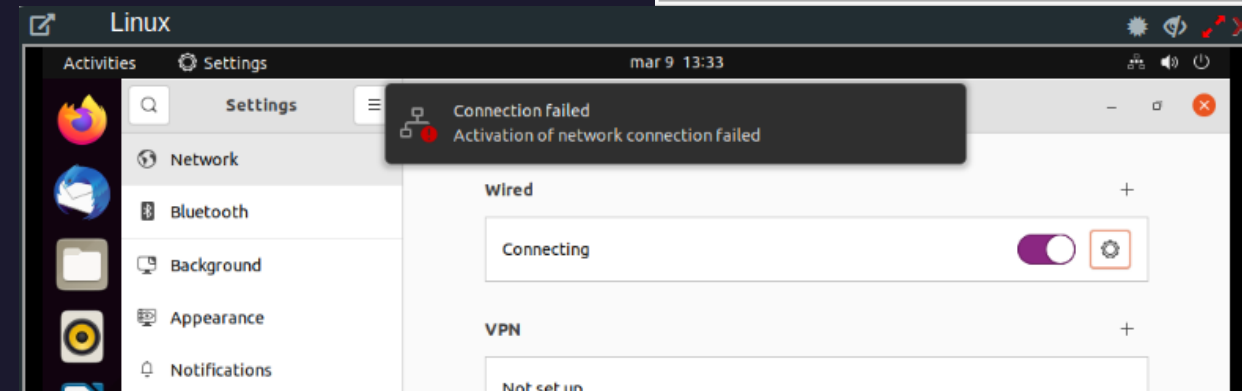
Interface	Status
ether2	un-authorized
ether3	un-authorized
ether4	un-authorized

Logging

Rules Actions

Topics	Prefix	Action
* critical		echo
* error		memory
* info		memory
manager		echo
radius		echo
* warning		memory

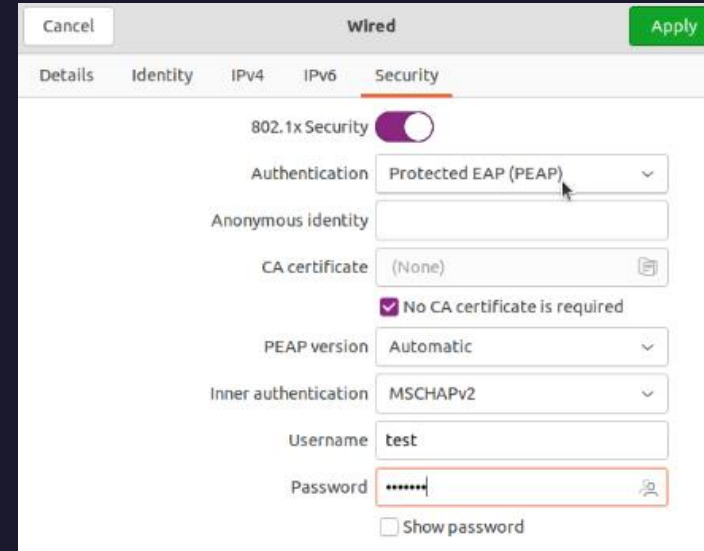
6 items





# Setarea conexiuni dot1x pe client

- Clientul nu are foarte multe de facut in aceasta situatie.
- Trebuie sa intre in retea si sa activeze optiunea 802.1x Security
- Sa aleaga ca metoda de autentificare PEAP
- Sa bifeze No CA certificate is required
- Si sa introduca userul si parola
- In terminal vedem mesajul de la client fara eroare.



```
[admin@MikroTik] >
(86 messages discarded)
11:39:01 echo: radius, debug, packet 00002d030322aceb06a4717f3007fa10
11:39:01 echo: radius, debug, packet 3cc9b7f5687f69c262ccb63160c402b4
11:39:01 echo: radius, debug, packet 88d7b5ecff00c030000005ff01000100
11:39:01 echo: radius, debug, packet 16030305fa0b0005f60005f300030b30
11:39:01 echo: radius, debug, packet 820307308201efa00302010202083038
11:39:01 echo: radius, debug, packet a73292b13e0b300d06092a864886f70d
11:39:01 echo: radius, debug, packet 01010b0500300d310b30090603550403
11:39:01 echo: radius, debug, packet 0c024341301e170d3233303330393131
11:39:01 echo: radius, debug, packet 303735375a170d323430333038313130
11:39:01 echo: radius, debug, packet 3735375a3011310f300d06035504030c
11:39:01 echo: radius, debug, packet 0672616469757330820122300d06092a
11:39:01 echo: radius, debug, packet 864886f70d01010105000382010f0030
[admin@MikroTik] >
```


# Testarea conexiunii

- Vedem ca Ubuntu este conectat la internet.
- Iar in meniul Dot1x vedem ca userul este activ.
- Iar portul este deblocat.

```
user@user-Standard-PC-l440FX-PIIX-1996: ~  
: qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou  
    default qlen 1000  
    link/ether 50:00:00:06:00:00 brd ff:ff:ff:ff:ff:ff  
    altname enp0s3  
    inet 192.168.10.254/24 brd 192.168.10.255 scope global dynamic noprefixroute  
        ens3  
        valid_lft 473sec preferred_lft 473sec  
    inet6 fe80::ff91:639e:781f:b10c/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
user@user-Standard-PC-l440FX-PIIX-1996:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
i4 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=21.9 ms  
i4 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=20.9 ms  
^C  
-- 8.8.8.8 ping statistics --  
: packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 20.854/21.374/21.894/0.520 ms  
user@user-Standard-PC-l440FX-PIIX-1996:~$
```

Dot1X

ClientServerStateActive

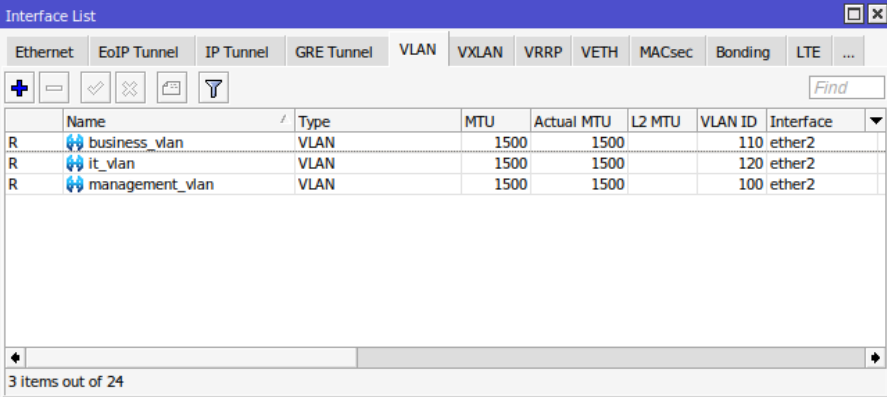


Interface	Username	Client MAC Address	VLAN ID	Auth. Info	
ether2	test	50:00:00:06:00:00	0	dot1x	

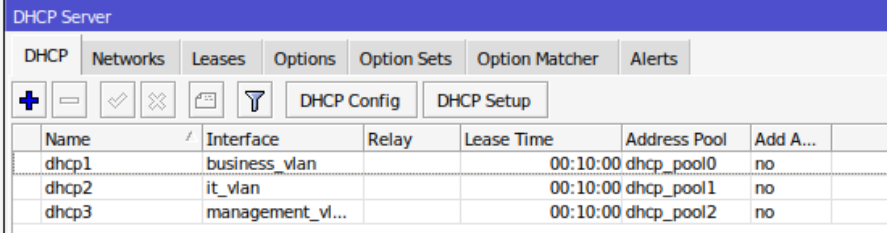
Dot1X		
Client	Server	State
Y		
Interface	Status	
ether2	authorized	
ether3	un-authorized	
ether4	un-authorized	

# Implementarea VLAN-ului dinamic

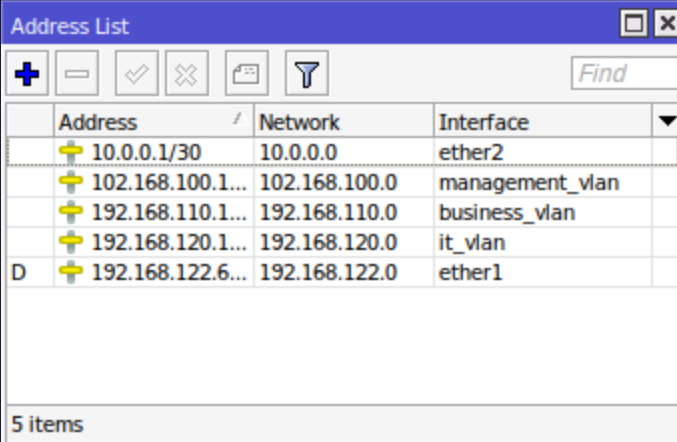
- Vom adauga un nou router in topologia existenta care va prelua functia de autentificare dot1x.
- In routerul principal facem 3 VLAN-uri si asignam un server DHCP fiecaruia.
- Si asignam interfetei eth2 un ip (10.0.0.1/30) pentru a putea comunica cu celalat router.



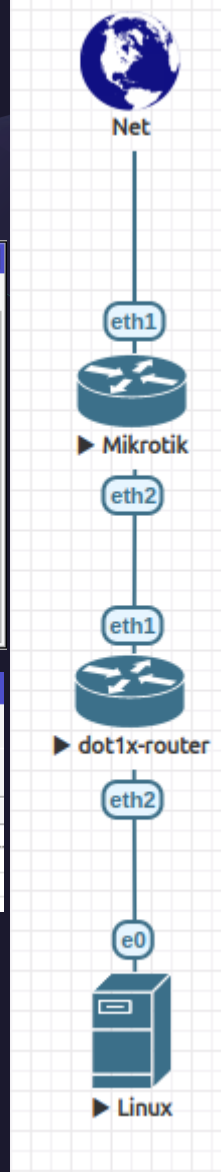
	Name	Type	MTU	Actual MTU	L2 MTU	VLAN ID	Interface
R	business_vlan	VLAN	1500	1500		110	ether2
R	it_vlan	VLAN	1500	1500		120	ether2
R	management_vlan	VLAN	1500	1500		100	ether2



Name	Interface	Relay	Lease Time	Address Pool	Add A...
dhcp1	business_vlan		00:10:00 dhcp_pool0	no	
dhcp2	it_vlan		00:10:00 dhcp_pool1	no	
dhcp3	management_vlan		00:10:00 dhcp_pool2	no	



	Address	Network	Interface
	10.0.0.1/30	10.0.0.0	ether2
	102.168.100.1...	102.168.100.0	management_vlan
	192.168.110.1...	192.168.110.0	business_vlan
	192.168.120.1...	192.168.120.0	it_vlan
D	192.168.122.6...	192.168.122.0	ether1





# Implementarea VLAN-ului dinamic

- Adaugam un router nou in serverul de radius cu ip-ul routerului dot1x.
- Pe routerul dot1x setam clientul de radius
- Facem un bridge nou si o lista de interfete.

Router <dot1x>

Name:	dot1x
Shared Secret:	aaaa
Address:	10.0.0.2
CoA Port:	3799
Access Requests:	136
Access Failures:	2
Broken Requests:	0
Unknown Requests:	0
Accounting Requests:	6

RADIUS Server <10.0.0.1>

General Status

Service: ☐ ppp ☒ login  
☐ hotspot ☐ wireless  
☐ dhcp ☐ ipsec  
☒ dot1x

Called ID:   
Domain:   
Address: 10.0.0.1  
Protocol: udp  
Secret: aaaa

Authentication Port: 1812  
Accounting Port: 1813  
Timeout: 300 ms  
☐ Accounting Backup  
Realm:

Bridge

#	Interface	Bridge	Horizon	Trusted	Priority (...)	Path Cost	PVID	Role
0	ether1	bridge1		no	80	10	1	root port
1	dot1x	bridge1		no	80	10	1	
2 D	ether2	bridge1		no	80	10	1	designated port
3 DI	ether3	bridge1		no	80	10	1	disabled port
4 DI	ether4	bridge1		no	80	10	1	disabled port
5 DI	ether5	bridge1		no	80	10	1	disabled port
6 DI	ether6	bridge1		no	80	10	1	disabled port
7 DI	ether7	bridge1		no	80	10	1	disabled port
8 DI	ether8	bridge1		no	80	10	1	disabled port
9 DI	ether9	bridge1		no	80	10	1	disabled port
10 DI	ether10	bridge1		no	80	10	1	disabled port

# Implementarea VLAN-ului dinamic

- Setam pe eth1 ca port de trunk si activa VLAN filtering pe bridge.
- Inapoi in user management trebuie sa setam noi parametrii utilizatorului pentru a desemna tipul de conexiune si vlan-ul 110 care este business\_vlan (vezi ultimul slide).
- Si activarea dot1x.

The screenshot displays three configuration windows from Mikrotik WinBox:

- Bridge** window: Shows the VLAN configuration for bridge1. The table lists VLAN IDs and their associated ports.
- User <test>** window: Shows the configuration for a user named 'test'. The 'Tunnel-Private-Group-ID' is set to 110.
- Dot1x Server <dot1x>** window: Shows the configuration for the dot1x server. The 'Interface' is set to dot1x, and 'Auth. Types' includes dot1x.

Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	100	ether1	
bridge1	110	ether1	
bridge1	120	ether1	
D bridge1	1		bridge1, ether1

**User <test>**

General

Name: test

Password: test123

OTP Secret:

Group: default

Caller ID:

Shared Users: 10

Attributes:

- Mikrotik-Group: full
- Tunnel-Medium-Type: 6
- Tunnel-Private-Group-ID: 110
- Tunnel-Type: 13

**Dot1x Server <dot1x>**

Interface: dot1x

Auth. Types: ☒ dot1x ☐ mac auth

☐ Accounting

Interim Update: 00:10:00

Auth. Timeout: 60.00 s

Retrans. Timeout: 30.00 s

Reauth. Timeout:

Reject VLAN ID:

Guest VLAN ID:

Server Fail VLAN ID:

# Implementarea VLAN-ului dinamic

- Acum putem incerca activarea conexiuni de pe clientul Ubuntu.
- Putem vedea ca este conectat si a primit un ip din vlan-ul 110.
- Daca ne uitam la sesiunile active din dot1x vedem ca userul are asignat vlan-ul 110.

```
user@user-Standard-PC-i440FX-PIIX-1996: ~  
user@user-Standard-PC-i440FX-PIIX-1996:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 50:00:00:06:00:00 brd ff:ff:ff:ff:ff:ff  
    altnam enp0s3  
    inet 192.168.110.254/24 brd 192.168.110.255 scope global dynamic noprefixroute ens3  
        valid_lft 594sec preferred_lft 594sec  
    inet6 fe80::ff91:639e:781f:b10c/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
user@user-Standard-PC-i440FX-PIIX-1996:~$
```

Dot1X					
Client Server State Active					
Y					
Interface	/	Username	Client MAC Address	VLAN ID	Auth. Info
ether2		test	50:00:00:06:00:00	110	dot1x

# Link-uri utile

<https://wiki.mikrotik.com/wiki/Manual:Interface/Dot1x>

<https://www.iana.org/assignments/radius-types/radius-types.xhtml>

