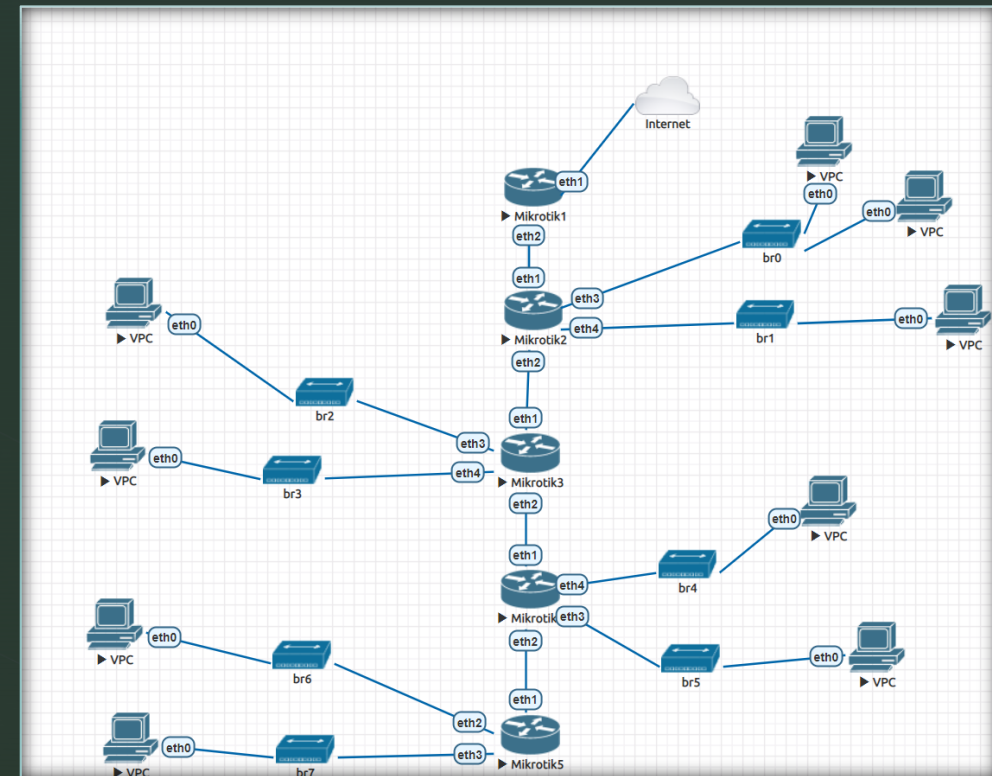


Laboratoare Linux

# Setare VLAN

# Topologie

- In acest scenariu am facut o topologie in cascada unde vlan-urile curg din router in router (care actioneaza mai mult ca un switch cu management).
- Incepem configurarea primului router.



# Setarea trunk VLAN pe Mikrotik1

- Incepem configurarea VLAN-urilor in Interfaces -> VLAN.
- Si setam doua VLAN-uri (10 si 11) pe interfata ether2 care se va propaga in retea.
- Aces router este administratorul VLAN-urilor din retea.

Interface <vlan10>

General Loop Protect Status Traffic

Name: vlan10

Type: VLAN

MTU: 1500

Actual MTU: 1500

L2 MTU:

MAC Address: 50:00:00:01:00:01

ARP: enabled

ARP Timeout:

VLAN ID: 10

Interface: ether2

☐ Use Service Tag

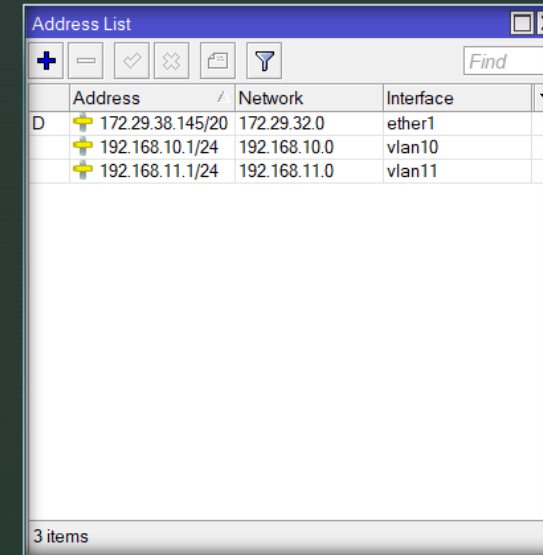
OK Cancel Apply Disable Comment Copy Remove Torch Reset Traffic Counters

enabled running slave passthrough

Interface	Name	Type	MTU	Actual MTU	L2 MTU	VLAN ID	Interface	Tx	Rx
R	vlan10	VLAN	1500	1500		10	ether2	0 bps	0 bps
R	vlan11	VLAN	1500	1500		11	ether2	0 bps	0 bps

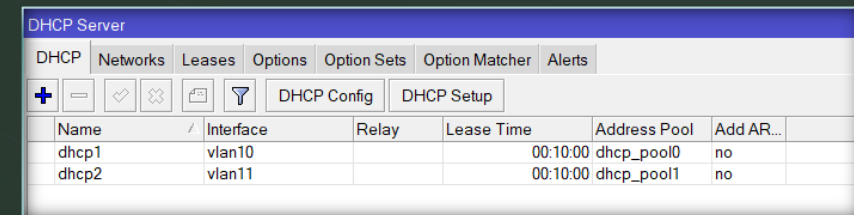
# Setarea trunk VLAN pe Mikrotik1

- Acum ii setam fiecarui VLAN o adresa IP si o clasa.
- Si pentru a verifica usor functionalitatea un server DHCP pentru fiecare interfata de VLAN.
- Acum putem trece la configurarea celorlalte routere.



	Address	Network	Interface
D	172.29.38.145/20	172.29.32.0	ether1
	192.168.10.1/24	192.168.10.0	vlan10
	192.168.11.1/24	192.168.11.0	vlan11

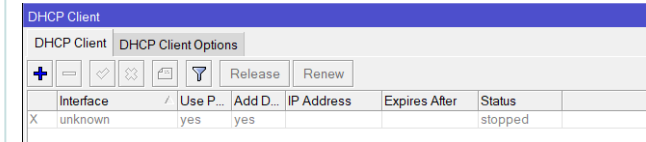
3 items



Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	vlan10		00:10:00	dhcp_pool0	no
dhcp2	vlan11		00:10:00	dhcp_pool1	no

# Setare VLAN MikroTik2

- Imediat dupa conectare ne asiguram ca oprim clientul de dhcp.
- Dupa care facem un bridge mergand in meniul "Bridge" unde facem un bridge simplu.

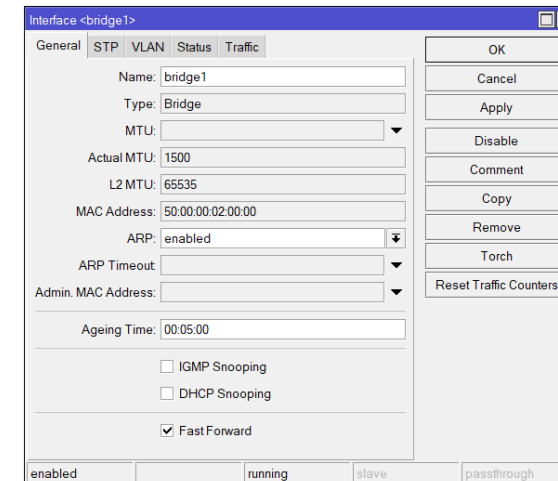


DHCP Client

DHCP Client Options

Release Renew

	Interface	/	Use P...	Add D...	IP Address	Expires After	Status	
X	unknown		yes	yes			stopped	



Interface <bridge1>

General STP VLAN Status Traffic

Name: bridge1

Type: Bridge

MTU: 1500

Actual MTU: 1500

L2 MTU: 65535

MAC Address: 50:00:00:02:00:00

ARP: enabled

ARP Timeout: 00:05:00

Admin. MAC Address: 50:00:00:02:00:00

Ageing Time: 00:05:00

☐ IGMP Snooping

☐ DHCP Snooping

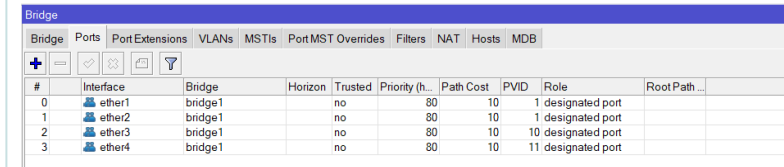
☒ Fast Forward

enabled running slave passthrough

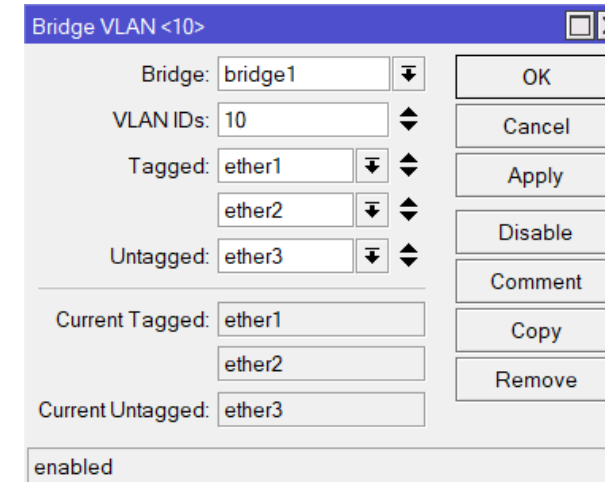
OK Cancel Apply Disable Comment Copy Remove Torch Reset Traffic Counters

# Setare VLAN MikroTik2

- Acum adaugam interfetele slave la bridge (de preferat adaugam toate interfetele routerului daca nu sunt deja adaugate default).
- In acest scenariu este suficient primele 4 interfete pentru ca doar ele sunt conectate la un router sau la un switch.
- Dupa care mergem in tabul VLANs si facem 2 intrari.
- In zona de Tagged setam porturile care sunt si raman trunk iar la Untagged sunt porturile finale, cele prin care se conecteaza calculatoare, servere, etc.
- In cazul VLAN-ului 10 avem ether1 si ether2 trunk iar pe ether3 il conectam la un PC.



#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	PVID	Role	Root Path...
0	ether1	bridge1		no	80	10	1	designated port	
1	ether2	bridge1		no	80	10	1	designated port	
2	ether3	bridge1		no	80	10	10	designated port	
3	ether4	bridge1		no	80	10	11	designated port	



Bridge VLAN <10>

Bridge: bridge1

VLAN IDs: 10

Tagged: ether1, ether2

Untagged: ether3

Current Tagged: ether1, ether2

Current Untagged: ether3

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove



# Setare VLAN MikroTik2

- Pentru VLAN 11 facem un setup asemanator doar ca la Untagged avem ether2 iar ether1 este trunk in si ether4 trunk out.
- Dupa ce am facut tag-urile porturilor trebuie sa facem tag-urile porturilor finale (ether3 si ether4). Mergem in tabul "Ports"
- Selectam ether3 si ether4, mergem la tabul VLAN.
- Unde setam VLAN ID-ul 10 respectiv 11.

Bridge										
Bridge Ports										
#	Interface	Bridge	Horizon	Trusted	Priority (h...	Path Cost	PVID	Role	Root Path ...	
0	ether1	bridge1		no	80	10	1	designated port		
1	ether2	bridge1		no	80	10	1	designated port		
2	ether3	bridge1		no	80	10	10	designated port		
3	ether4	bridge1		no	80	10	11	designated port		

Bridge Port <ether3>

General STP VLAN Status

PVID: 10

Frame Types: admit all

☒ Ingress Filtering

☐ Tag Stacking

OK Cancel Apply Disable Comment Copy Remove

Bridge VLAN <11>

Bridge: bridge1

VLAN IDs: 11

Tagged: ether1 ether2

Untagged: ether4

Current Tagged: ether1 ether2

Current Untagged: ether4

enabled

OK Cancel Apply Disable Comment Copy Remove

# Setare VLAN MikroTik2

- Acum putem activa filtrarea VLAN in bridge. Selectand bridge-ul (in cazul meu bridge1) si mergem la VLAN si bifam "VLAN Filtering".

Interface <bridge1>

General STP VLAN Status Traffic

☒ VLAN Filtering

EtherType: 0x8100

PVID: 1

Frame Types: admit all

☐ Ingress Filtering

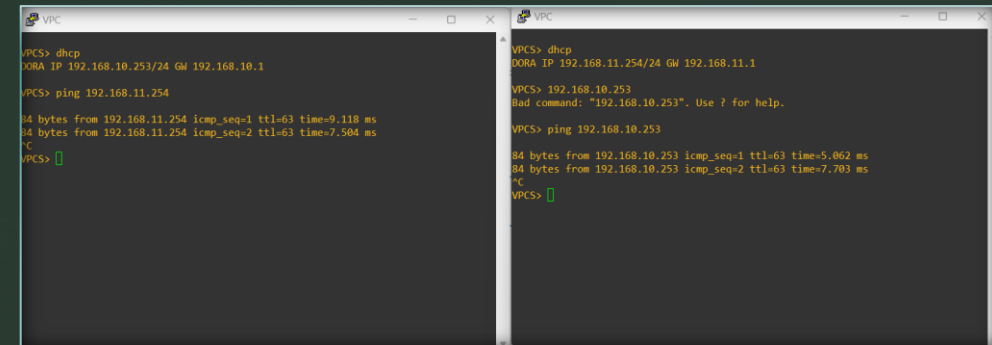
OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Torch  
Reset Traffic Counters

enabled running slave passthrough



# Verificare VLAN pe MikroTik2

- Avem atast pe interfata ether3 si ether4 2 calculatoare de pe care vom face request DHCP si apoi un ping intre masini.



The image shows two terminal windows side-by-side, both titled 'VPC'. The left window shows a VPCS configuration for IP 192.168.10.253 with gateway 192.168.10.1. It then performs a ping to 192.168.11.254, showing successful results with TTL=63. The right window shows a VPCS configuration for IP 192.168.11.254 with gateway 192.168.11.1. It then performs a ping to 192.168.10.253, also showing successful results with TTL=63. Both windows show the standard VPCS DHCP request and ping output.

```
VPCS> dhcp
DORA IP 192.168.10.253/24 GW 192.168.10.1

VPCS> ping 192.168.11.254
84 bytes from 192.168.11.254 icmp_seq=1 ttl=63 time=9.118 ms
84 bytes from 192.168.11.254 icmp_seq=2 ttl=63 time=7.504 ms
^C
VPCS>
```

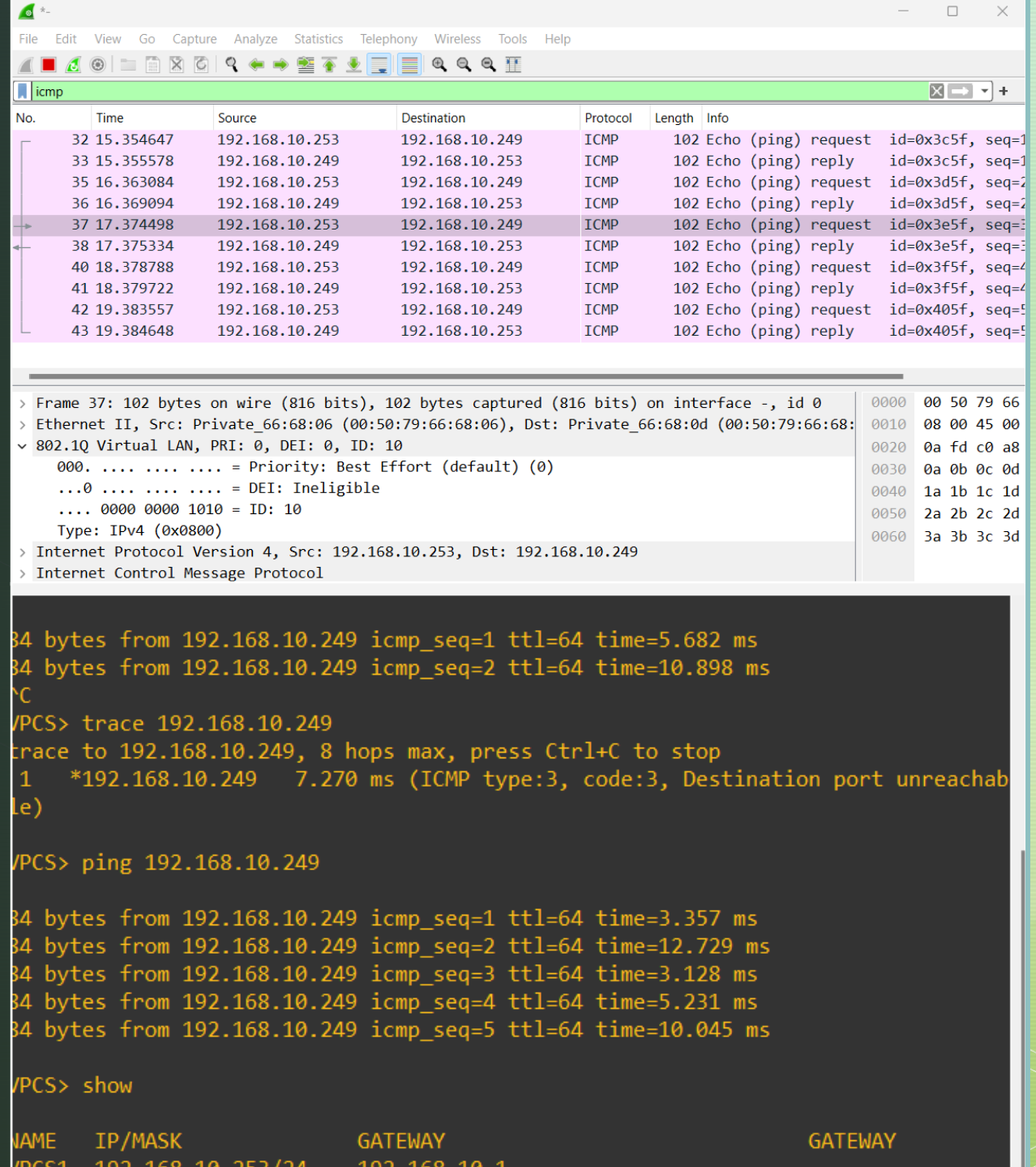
```
VPCS> dhcp
DORA IP 192.168.11.254/24 GW 192.168.11.1

VPCS> 192.168.10.253
Bad command: "192.168.10.253". Use ? for help.

VPCS> ping 192.168.10.253
84 bytes from 192.168.10.253 icmp_seq=1 ttl=63 time=5.062 ms
84 bytes from 192.168.10.253 icmp_seq=2 ttl=63 time=7.703 ms
^C
VPCS>
```

# Setarea celorlalte routere

- Toate routerele in topologia noastra se vor configura indentic.
- Si inceram un ping de ultimul pc din structura la primul.
- Cand dam ping putem face si o captura de pachete unde vedem in headerul pachetului si VLAN-ul in cazul nostru 10.



The image displays a Wireshark packet capture window and a router CLI session. The Wireshark window shows a list of ICMP Echo (ping) requests and replies between 192.168.10.253 and 192.168.10.249. The selected packet (No. 37) is expanded to show the Ethernet II header, 802.1Q Virtual LAN header (VLAN ID 10), and the Internet Protocol Version 4 header. The router CLI output shows the results of a ping command from 192.168.10.249 to 192.168.10.249, followed by a 'show' command.

No.	Time	Source	Destination	Protocol	Length	Info
32	15.354647	192.168.10.253	192.168.10.249	ICMP	102	Echo (ping) request id=0x3c5f, seq=1
33	15.355578	192.168.10.249	192.168.10.253	ICMP	102	Echo (ping) reply id=0x3c5f, seq=1
35	16.363084	192.168.10.253	192.168.10.249	ICMP	102	Echo (ping) request id=0x3d5f, seq=2
36	16.369094	192.168.10.249	192.168.10.253	ICMP	102	Echo (ping) reply id=0x3d5f, seq=2
37	17.374498	192.168.10.253	192.168.10.249	ICMP	102	Echo (ping) request id=0x3e5f, seq=3
38	17.375334	192.168.10.249	192.168.10.253	ICMP	102	Echo (ping) reply id=0x3e5f, seq=3
40	18.378788	192.168.10.253	192.168.10.249	ICMP	102	Echo (ping) request id=0x3f5f, seq=4
41	18.379722	192.168.10.249	192.168.10.253	ICMP	102	Echo (ping) reply id=0x3f5f, seq=4
42	19.383557	192.168.10.253	192.168.10.249	ICMP	102	Echo (ping) request id=0x405f, seq=5
43	19.384648	192.168.10.249	192.168.10.253	ICMP	102	Echo (ping) reply id=0x405f, seq=5

```
> Frame 37: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
> Ethernet II, Src: Private_66:68:06 (00:50:79:66:68:06), Dst: Private_66:68:0d (00:50:79:66:68:0d), Length: 102
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
  000. .... .. = Priority: Best Effort (default) (0)
  ...0 .... .. = DEI: Ineligible
  .... 0000 0000 1010 = ID: 10
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.10.253, Dst: 192.168.10.249
> Internet Control Message Protocol

34 bytes from 192.168.10.249 icmp_seq=1 ttl=64 time=5.682 ms
34 bytes from 192.168.10.249 icmp_seq=2 ttl=64 time=10.898 ms
^C
/PCS> trace 192.168.10.249
Trace to 192.168.10.249, 8 hops max, press Ctrl+C to stop
 1  *192.168.10.249 7.270 ms (ICMP type:3, code:3, Destination port unreachable)

/PCS> ping 192.168.10.249

34 bytes from 192.168.10.249 icmp_seq=1 ttl=64 time=3.357 ms
34 bytes from 192.168.10.249 icmp_seq=2 ttl=64 time=12.729 ms
34 bytes from 192.168.10.249 icmp_seq=3 ttl=64 time=3.128 ms
34 bytes from 192.168.10.249 icmp_seq=4 ttl=64 time=5.231 ms
34 bytes from 192.168.10.249 icmp_seq=5 ttl=64 time=10.045 ms

/PCS> show

NAME IP/MASK GATEWAY
/PCS1 192.168.10.253/24 192.168.10.1
```