WIRELESS & NETWORKING EXPERTS

Port Based Authentication
802.1X (dot1x)

March 2025 © Jono Thompson
Multithread Consultants Ltd

1

2

Jono Thompson

- Networking background started as a Cisco Engineer
- Started using ROS June 2010
- MikroTik Consultant Since Dec 2014
- MikroTik Trainer since March 2017
  - MTCNA
  - MTCRE
  - MTCINE
  - MTCWE
  - MTCTCE
  - MTCUME
  - MTCSE
  - MTCIPv6
  - MTCSWE
  - MTCEWE

3

3

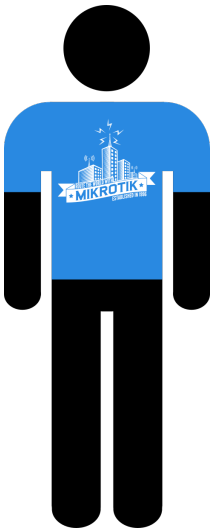
Presentation Objectives

- Look at the components of dot1x
- See how to configure dot1x on RouterOS
- See a demo of dot1x in action

4

4

Meet Mike

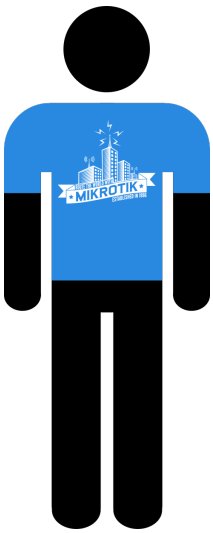


- Last time we met Mike, he had just installed his new MikroTik Switches
- He has finally got all his switches working really well thanks to some really cool guy from the EU MUM
- Mike has not had any problems with his network performance since

6

6

Mike's Problem



- However
- Mike keeps finding that visitors come and plug into his data outlets and can then access his network
- Mike doesn't think that's a good idea!

7

7

Dave

- Mike ring his friend Dave
- Mike explains his problem to Dave
- Dave suggests that he should pay more attention to the release notes and look at the new MikroTik feature of dot1x

LinITX

8

8

Dave

- Dave also suggests that Mike should go on the brand new MTCSWE (MikroTik Switching Engineer) Training Course

LinITX

9

9

What is Dot1x?

- MikroTik Dot1x is an implementation of IEEE 802.1X standard in RouterOS
- Dot1x is not available on RouterBOARDs with smips hardware

10

What is 802.1X?

- 802.1X defines port-based authentication on a client-server bases to restrict unauthorized clients from connecting to a LAN.

11

What can Dot1x do?

- An authenticated interface can also be assigned a specific VLAN ID if using bridge VLAN filtering
- Dot1x can also create dynamic switch rules to apply to a switch port.

Dot1x Components

Dot1x (802.1X) defines three terminologies:

- Supplicant (Client)
- Authenticator (Switch)
- Authenticator Server (radius)

Dot1x - Supplicant

14

Dot1x - Supplicant

- The Supplicant is a device (normally an end user device eg laptop/desktop) that is requesting access to the LAN.
- Supplicant is typically a user's workstation but can be a router, switch, printer or IP phone

15

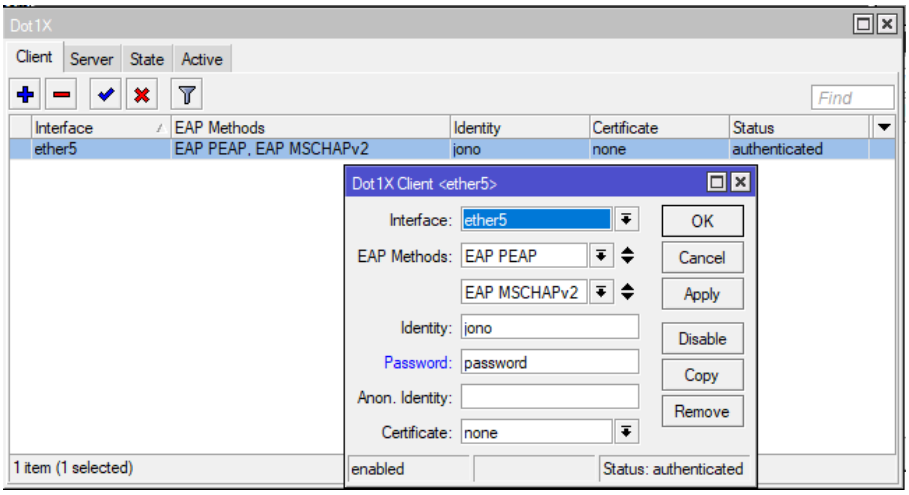
Dot1x Supplicant

- RouterOS can be a Supplicant (Client) and connect to a network with 802.1x authentication
- RouterOS refers to a Supplication as dot1x Client
- RouterOS supports a number of different EAP types

16

16

Dot1x Supplicant



18

18

Dot1x Authenticator

19

19

Dot1x Authenticator

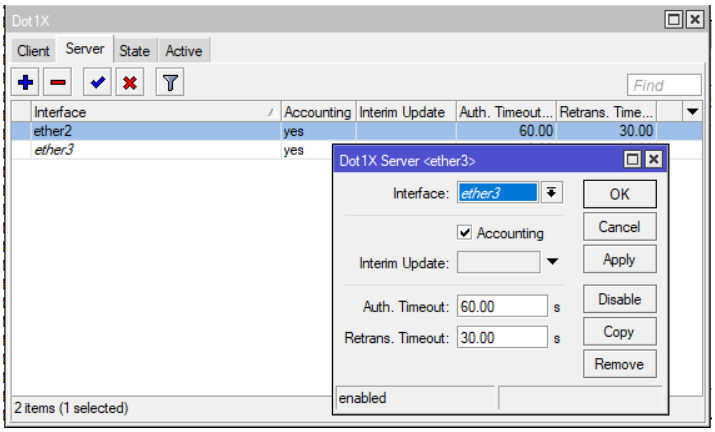
- A device that controls the physical access to the network (eg a switch or a wireless access point) is called the Authenticator
- The Authenticator requests the identity from the supplicant and verifies that information with the Authentication Server.
- The Authenticator will include a RADIUS client.
- The Authenticator will encapsulate and decapsulate the EAP messages while interacting with the Authenticator server

20

20

Dot1x Authenticator

- RouterOS can be an Authenticator on one or more ports
- RouterOS refers to an Authenticator as Dot1x Server



21

21

Dot1x Authenticator

- If using dot1x on a bridge port then the bridge must be running (R/M)STP otherwise the EAP packets from the client will not be accepted.
- A newly created bridge by default runs RSTP.

22

22

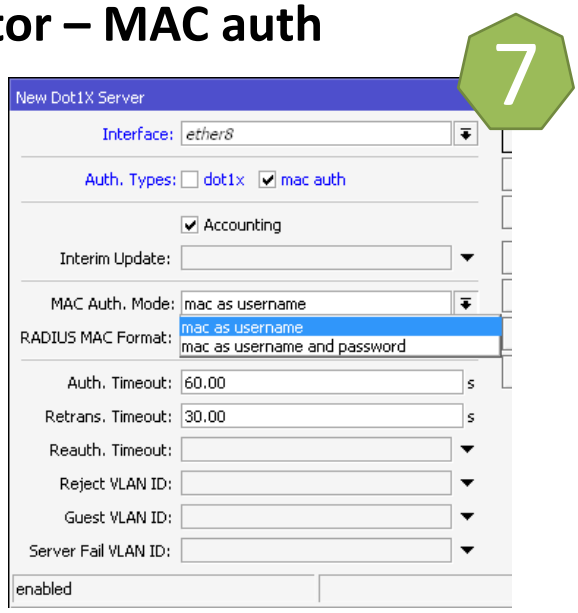
Dot1x Authenticator

- When an interface has dot1x server configured, it will block all traffic except for EAPoL (Extensible Authentication Protocol over LAN) packets.
- Once the port has been successfully authenticated the interface will accept ALL received traffic on the port.
- If the interface is connected to a shared medium with multiple hosts then traffic will be accepted from ALL hosts.

23

Dot1x Authenticator – MAC auth

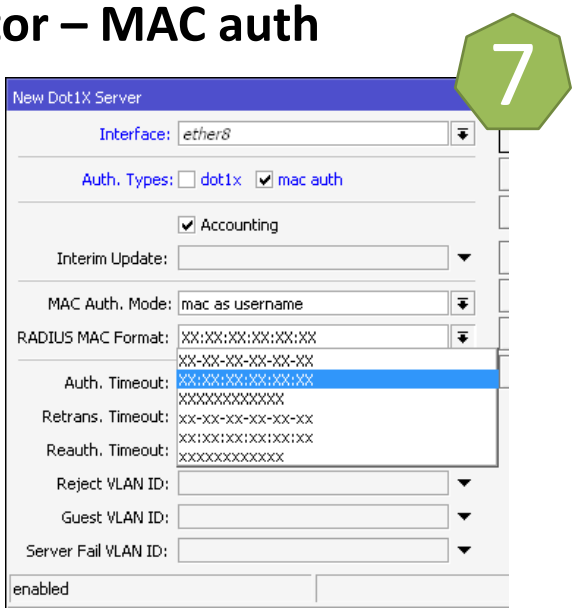
- Mac-auth-mode – used to control the username and password Radius Attributes



24

Dot1x Authenticator – MAC auth

- RADIUS MAC Format - Controls the format used for MAC of the client when sending username and/or password in the RADIUS attributes



25

25

Dot1x Authenticator – Additional settings

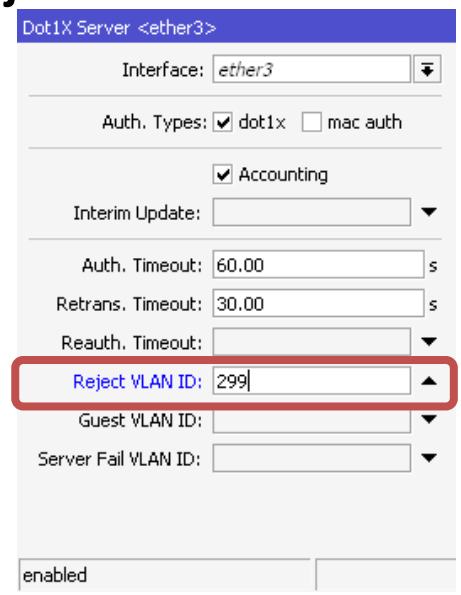
- Additional settings can be applied to define what happens in a number of different cases
  - Radius Server is down or unreachable
  - Client does not support 802.1X
  - Client fails to authenticate 802.1X

26

26

Dot1x Authenticator – Reject VLAN

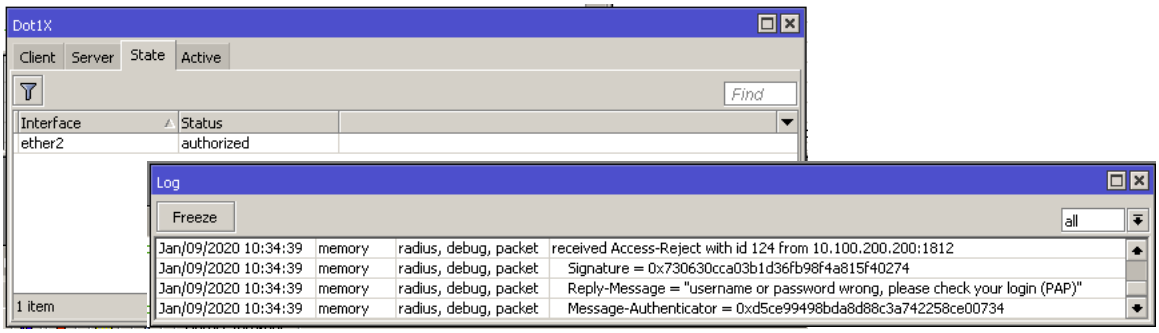
- Reject-vlan-id is configured when dot1x authenticator receives an access-reject from radius
- Normally an incorrect username/password
- Clients will be show as authenticated and placed into reject-vlan
- Only applies when bridge VLAN-Filtering is enabled.



27

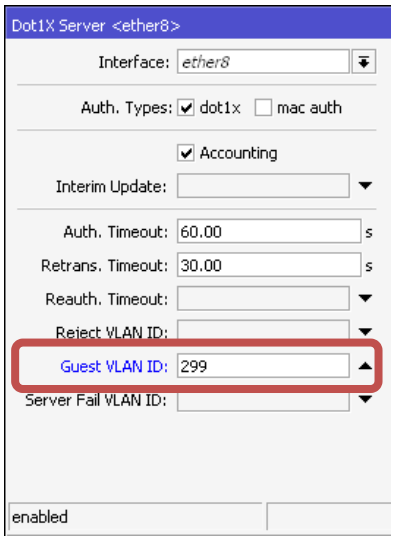
Dot1x Authenticator – Reject VLAN

- Server will show port as authorised
- Can be used with mac-auth to create a guest VLAN
- Logs will show any incorrect username / password attempts



28

Dot1x Authenticator – Guest VLAN



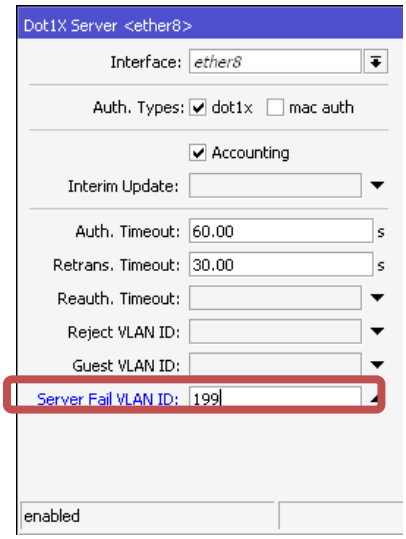
- VLAN assigned when client devices does not support 802.1x authentication and no mac-auth fall back has been configured
- VLAN is assigned after 3 retrains-timeout periods.
- Only applies when bridge VLAN-Filtering is enabled.

29

29

Dot1x Authenticator – Server Fail VLAN

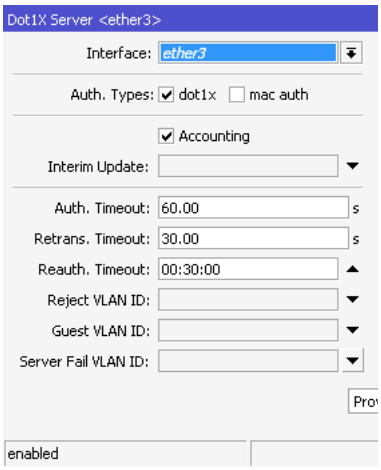
- VLAN assigned when RADIUS server does not respond and request timeout as elapsed.
- Only applies when bridge VLAN-Filtering is enabled.



30

30

Dot1x Authenticator – Reauth



- The Authenticator can force a client to reauth at a set time intervale to ensure any changes to the user's parameters on the radius server are applied.

Port based VLAN assignmernt

Dot1x VLAN assignment

- Dot1x can assign an authenticated interface to a specific VLAN ID
- This requires bridge VLAN filtering to be enabled
- This is done using radius attributes of
  - Tunnel-Type=13
  - Tunnel-Medium-Type=6
  - Tunnel-Private-Group-ID= “VLANID”

Dynamic Switch Rules

Dot1x Authenticator Dynamic Switch Rules

- If additional access rules are required then switch rules can be assigned by the radius server.
- Dynamic switch rules can be added using the MikroTik Switching-Filter Radius attribute
- These rules are only active as long as the client session is active and the interface is running.

35

Dot1x Authenticator Dynamic Switch Rules

- Each rule needs to end with an action of either drop or allow. If no action is set then default action of allow will be used.
- Multiple rules must be separated by a comma.
- Chain has default action of allow so may need a final rule of action drop at the end.

36

Dot1x Authenticator Dynamic Switch Rules

- Following Parameters are supported
  - Mac-protocol – Hex or decimal format eg Protocol 17 or Protocol 0x11
  - Src-mac-address – supports format "xx:xx:xx:xx:xx:xx" or "xxxxxxxxxxxx" also can be set as src-mac address none
  - Src-address & Dst-address – IPv4 address/mask
  - Protocol – IPv4
  - Src-port/dst-port – supports single or range values src-port 10 or src-port 10-20

37

37

Dot1x Authenticator Dynamic Switch Rules

- src-mac-address (if not specified), switch and ports parameters are dynamically configured for each rule

38

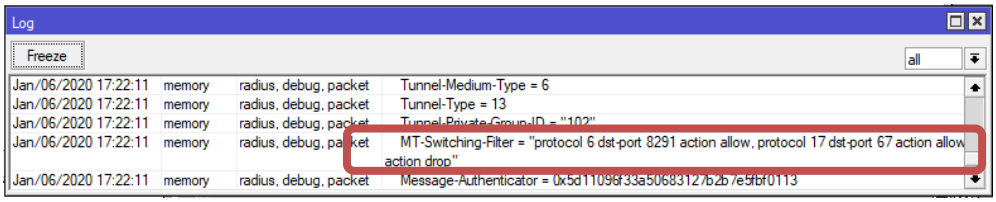
38

Dot1x Authenticator Dynamic Switch Rules

Example:

- Allow Winbox access (tcp port 8291) and DHCP (udp 67) and drop all other traffic

```
MikroTik-Switching-Filter = “protocol 6 dst-port 8291 action allow,
protocol 17 dst-port 67 action allow, action drop”
```



39

39

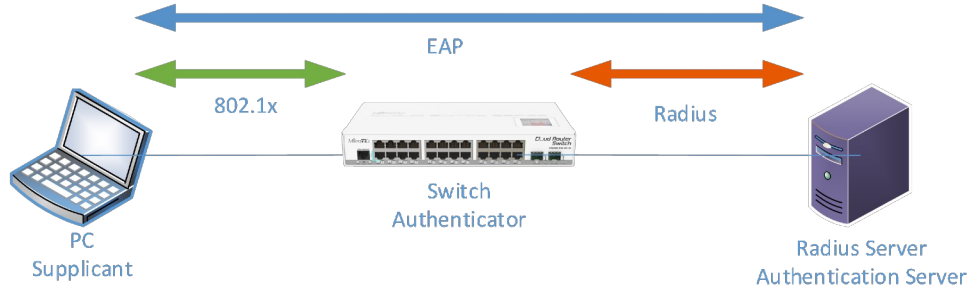
EAP

40

40

EAP

- Extensible Authentication Protocol (EAP) is used to pass authentication between the supplicant and the authentication server (Radius)
- The EAP type handles and defines the Authentication



41

41

EAPoL

- Dot1x uses EAP encapsulation over LANs (EAPoL) for the communication between the Supplicant and the Authenticator Server
- EAPoL uses EtherType of 0x888e
- EAPoL uses a special destination multicast MAC address of 01:80:C2:00:00:03

42

42

EAP

- The Authenticator takes the EAPoL frames relays them to the Authentication server (Radius)
- The Ethernet header is stripped and the remaining EAP frame is re-encapsulated in Radius Format.
- The Authenticator does not modify or examine the EAP frames

EAP Types

- RouterOS supports one or more of the following supplicant EAP Types:
  - EAP-TLS v1.0 – v1.2
  - EAP-TTLS
  - EAP-MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2

EAP-TLS

- Transport Layer Security (TLS)
- Both sides require a Certificate.
- With a client side certificate a compromised password is not enough to break into EAP-TLS protected systems.
- This could require more work to deploy client certificates to systems

46

EAP-TTLS

- Tunnelled Transport Layer Security
- Only the server needs a certificate
- The client verifies the server using the certificate on the server
- The server now uses this secure tunnel to authenticate the client

47

EAP-MSCHAPv2

- Microsoft Challenge Handshake Authentication Protocol
- EAP version of common MSCHAPv2 authentication mechanism
- Most common authentication method used with Microsoft windows clients
- Commonly used as the inner authentication for PEAP

48

48

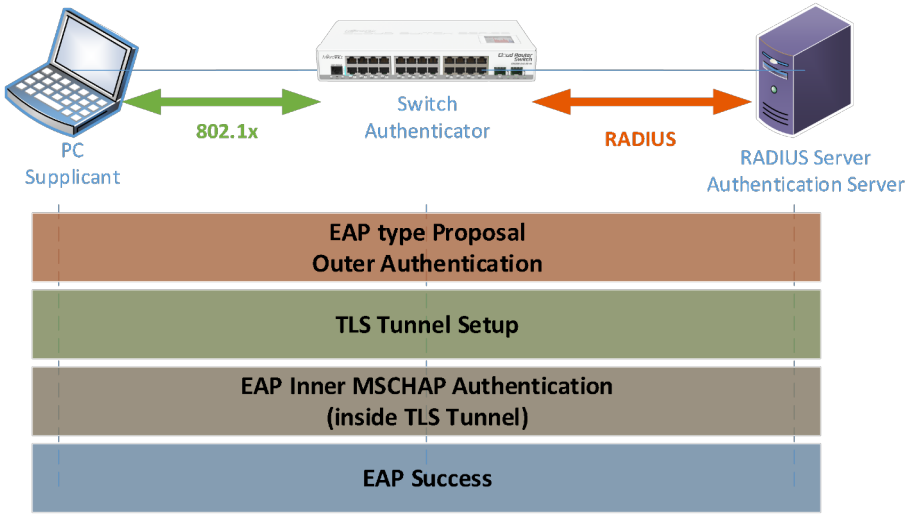
PEAP/EAP-MSCHAPv2

- Protected Extensible Authentication Protocol (PEAP) uses a server side certificate.
- PEAP is an encapsulation, not a authentication method
- PEAP works in 2 phases
- Phase 1 – server-side authentication is performed and a encrypted tunnel (TLS) is created
- Phase 2 – the client is now authenticated using EAP-MSCHAPv2 inside the TLS Tunnel

49

49

PEAP/EAP-MSCHAPv2 Flow



50

50

Certitificates

- The use of Certificates is not covered in this presentation
- For more information on the use of certificates in RouterOS see https://help.mikrotik.com/docs/display/ROS/Certificates

51

51

Dot1x Authentication Server

52

Dot1x - Authentication Server

- The authentication server is the device that performs the actual authentication of the supplicant (client)
- The Authentication server validates the identity of the supplicant and notifies the Authenticator if the supplicant is allowed to use the LAN and any network parameters to be assigned.

53

Dot1x - Authentication Server

- Dot1x requires Authentication server(s) which is the user database which is a Radius (Remote Authentication Dial In User Service) Server
- MikroTik User Manager can be an Authentication Server
- User manager requires an additional package to be installed

54

Authenticator Server (Radius)

- Radius server does not need to be in the same LAN as the authenticator nor running on the authenticator
- As Radius communications are done in plain text if using radius over untrusted networks then consider using either an encrypted tunnel or using RadSec

55

Dot1x Authentication Server

- Dot1x can assign an authenticated interface to a specific VLAN ID
- This requires bridge VLAN filtering to be enabled
- This is done using radius attributes of
  - Tunnel-Type=13
  - Tunnel-Medium-Type=6
  - Tunnel-Private-Group-ID= “VLANID”

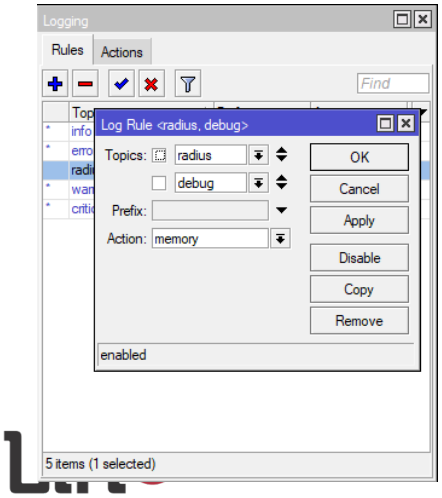
56

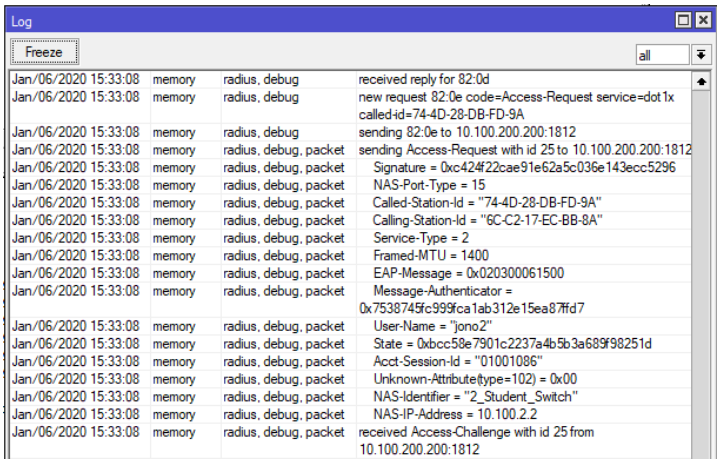
Debugging
What to do when it doesn’t work!

57

Dot1x Authenticator

- Enabling radius debug logs will enable you to see the radius messages being sent to check for any errors!

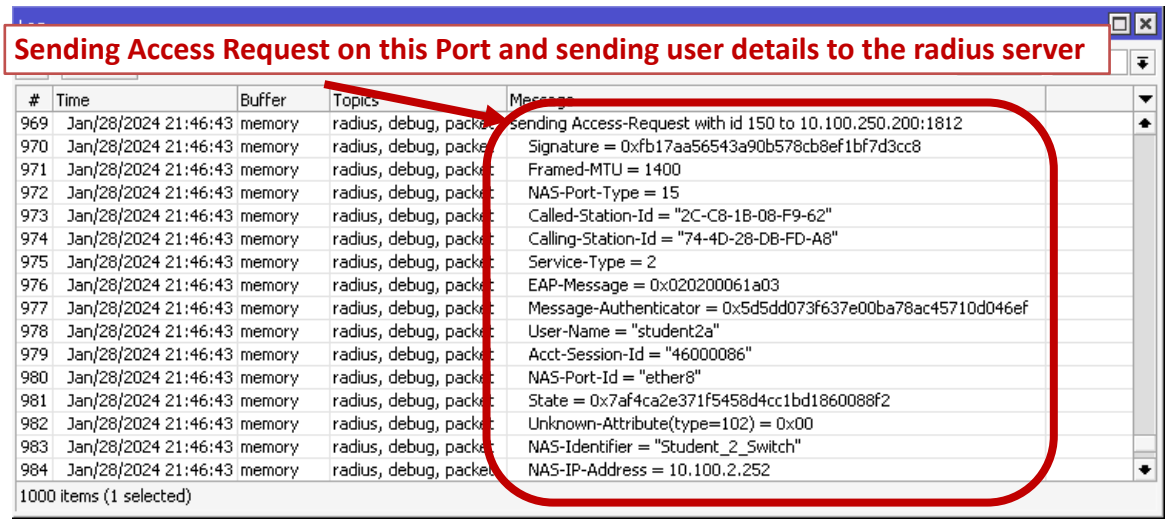




58

58

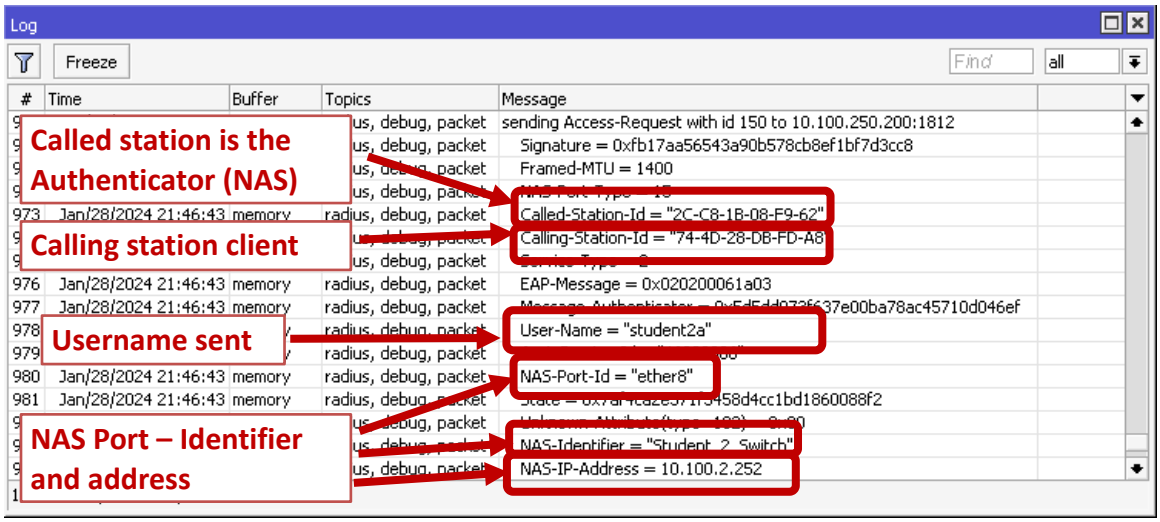
Dot1x Authenticator - Logs



59

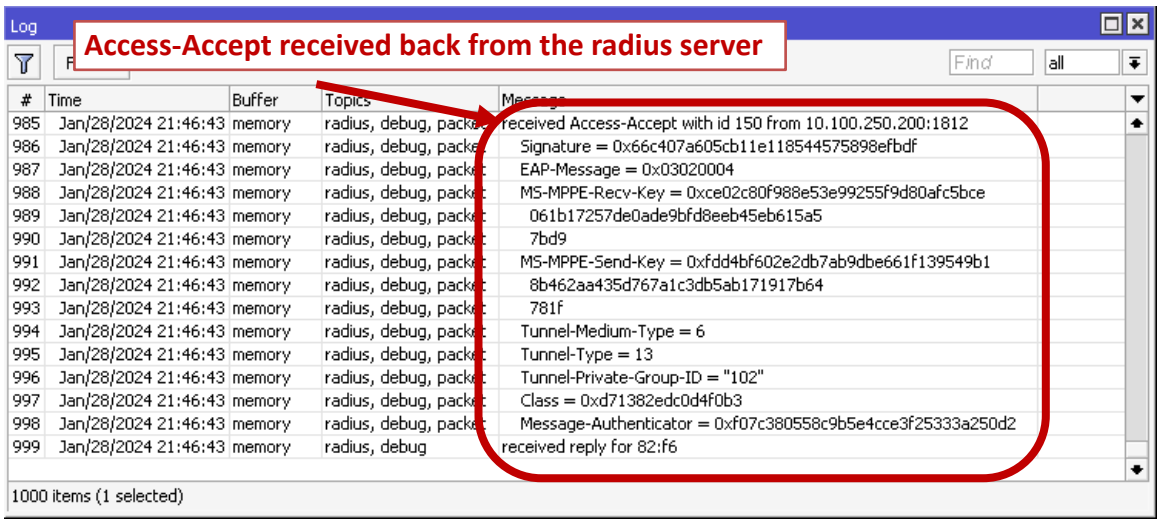
59

Dot1x Authenticator - Logs



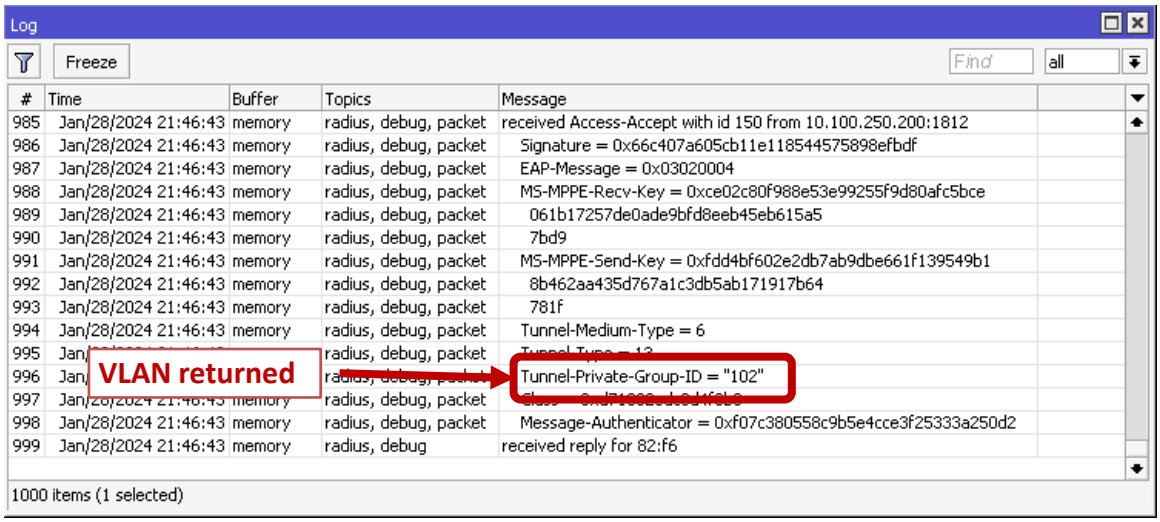
60

Dot1x Authenticator - Logs



61

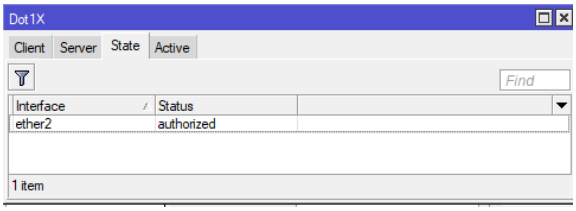
Dot1x Authenticator - Logs

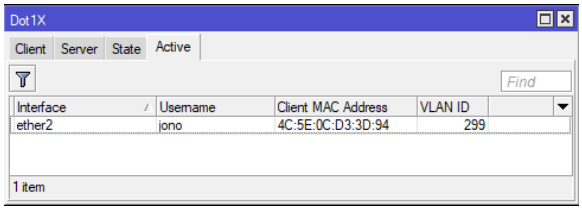


62

62

Dot1x Authenticator Status





Status

- **authorized** - access to interface is granted
- **iface-down** - interface is not running
- **rejected-holding** - access was rejected by the RADIUS server
- **un-authorized** - access to interface is not granted

63

63

64

MikroTik dot1x Setup

65

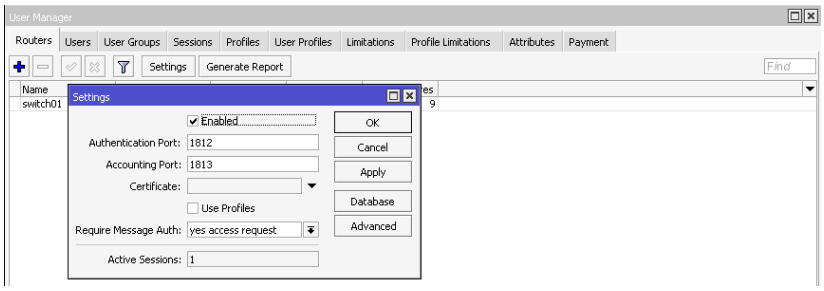
Setup

- Show configuration for Usermanager
- Show configuration for Authenticator
- Show configuration for RouterOS as a supplicant
- Show VLAN allocation
- Show Dynamic Switch rules

Setup - Topology

User manager Setup

1. Install User-manager additional package
2. Enable User-manager

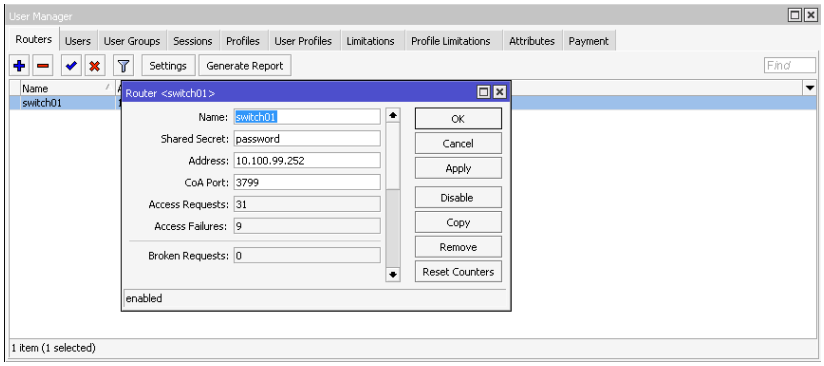



```
/user-manager
set certificate=*0 enabled=yes
```


68

User manager Setup

3. Add a ‘router’ for the authenticator

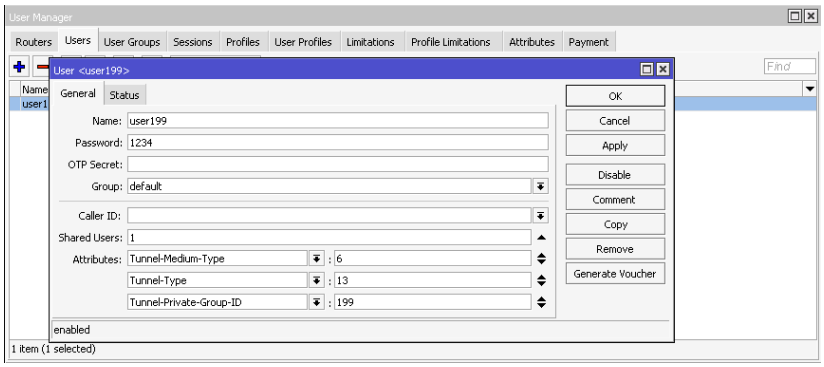



```
/user-manager router
add address=10.100.99.252 name=switch01 shared-secret=password
```


69

User manager – Create Users

4. Create users and set Radius Attributes



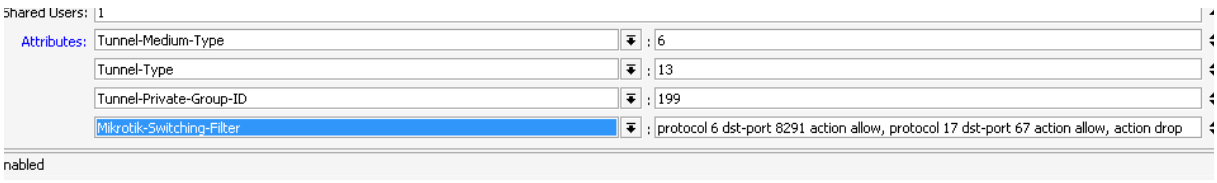

```
/user-manager user
add attributes=Tunnel-Medium-Type:6,Tunnel-Type:13,Tunnel-Private-Group-ID:199 name=user199
password=1234
```

70

70

User manager – Create Users

- Create user with radius attributes for switch rule



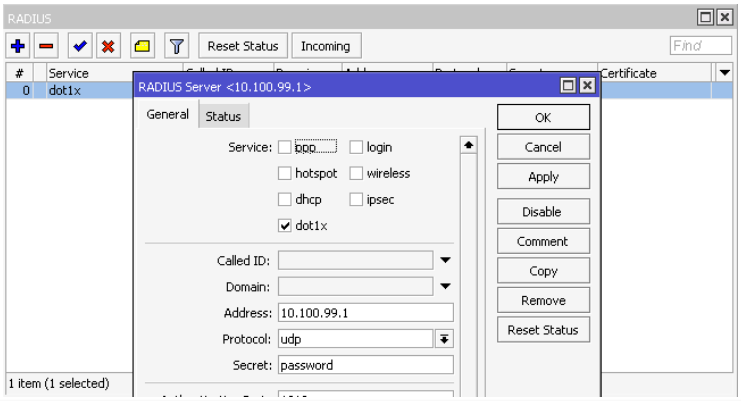

```
/user-manager user
add attributes="Tunnel-Medium-Type:6,Tunnel-Type:13,Tunnel-Private-Group-ID:199,Mikrotik-Switching-
Filter:protocol 6 dst-port 8291 action allow, protocol 17 dst-port 67 action allow, action drop"
name=userACL password=1234
```

71

71

Authenticator – Radius Client

- Add a radius client to point to the Authenticator server



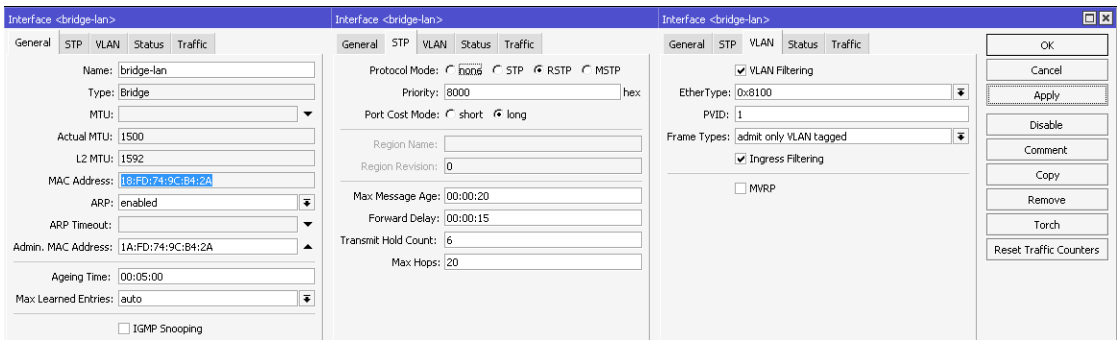

```
/radius
add address=10.100.99.1 service=dot1x src-address=10.100.99.252 timeout=3s
```

72

72

Authenticator – Bridge Configuration

- Create a bridge running RSTP and VLAN Filtering



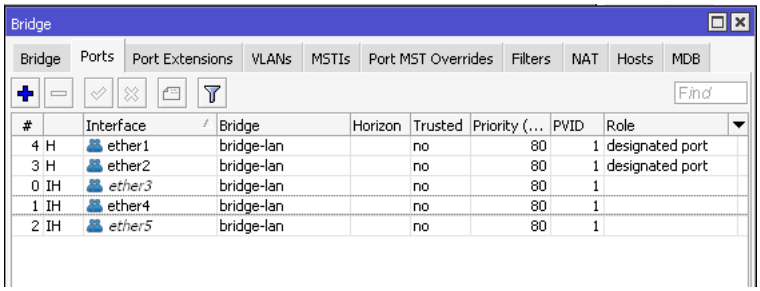

```
/interface bridge add admin-mac=1A:FD:74:9C:B4:2A auto-mac=no frame-types=admit-only-vlan-tagged
protocol-mode=rstp name=bridge-lan vlan-filtering=yes
/interface vlan add interface=bridge-lan name=vlan199 vlan-id=199
/ip dhcp-client add interface=vlan199
```

73

73

Authenticator – Bridge Configuration

- Add interfaces as bridge ports



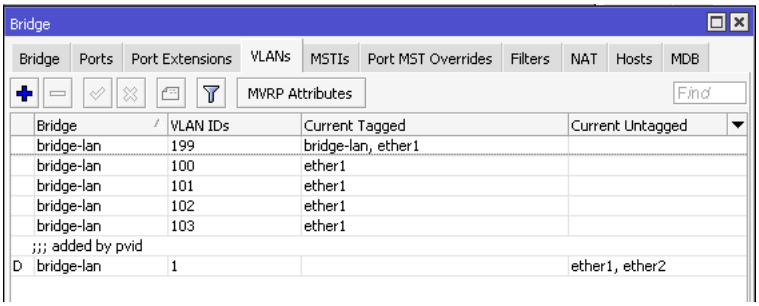

```
/interface bridge port
add bridge=bridge-lan interface=ether1
add bridge=bridge-lan interface=ether2
add bridge=bridge-lan interface=ether3
add bridge=bridge-lan interface=ether4
add bridge=bridge-lan interface=ether5
```

74

74

Authenticator – Bridge Configuration

- Add VLANs to bridge



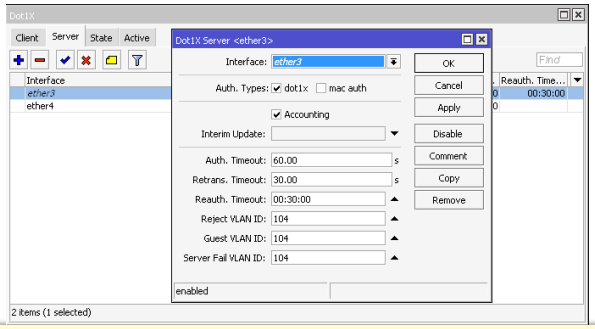

```
/interface bridge vlan
add bridge=bridge-lan tagged=bridge-lan,ether1 vlan-ids=199
add bridge=bridge-lan tagged=ether1 vlan-ids=100
add bridge=bridge-lan tagged=ether1 vlan-ids=101
add bridge=bridge-lan tagged=ether1 vlan-ids=102
add bridge=bridge-lan tagged=ether1 vlan-ids=103
```

75

75

Authenticator – dot1x Server

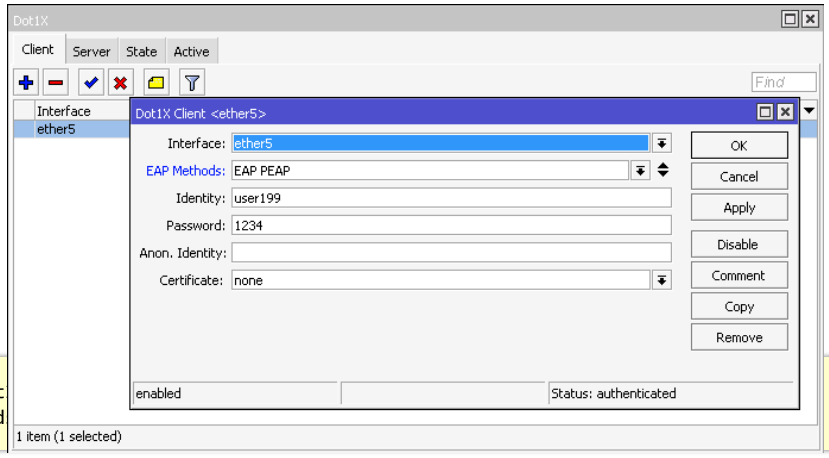
- Set dot1x server to run on the required ports. Set any failback vlans as needed




```
/interface dot1x server
add guest-vlan-id=104 interface=ether2 reauth-timeout=30m reject-vlan-id=104 server-fail-vlan-id=104
add guest-vlan-id=104 interface=ether3 reauth-timeout=30m reject-vlan-id=104 server-fail-vlan-id=104
add guest-vlan-id=104 interface=ether4 reauth-timeout=30m reject-vlan-id=104 server-fail-vlan-id=104
add guest-vlan-id=104 interface=ether5 reauth-timeout=30m reject-vlan-id=104 server-fail-vlan-id=104
```

76

Supplicant (Client) – Dynamic VLAN

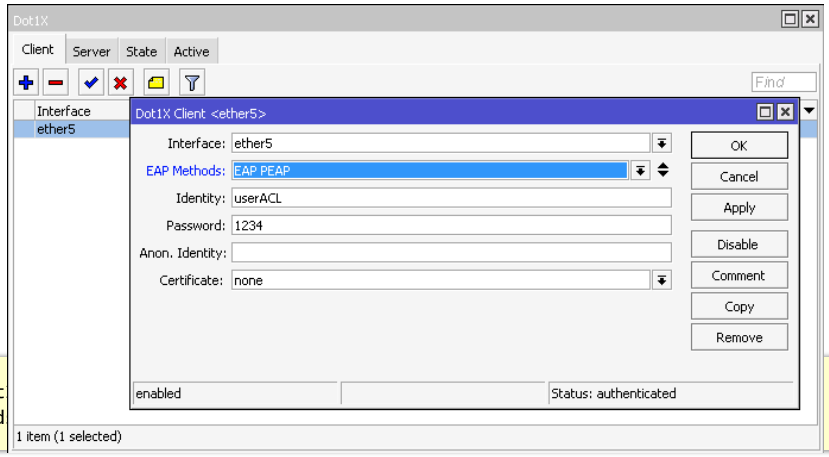



```
/interface dot
add eap-method
```

77

77

Supplicant (Client) – Dynamic ACL




```
/interface dot
add eap-method
```

78

78

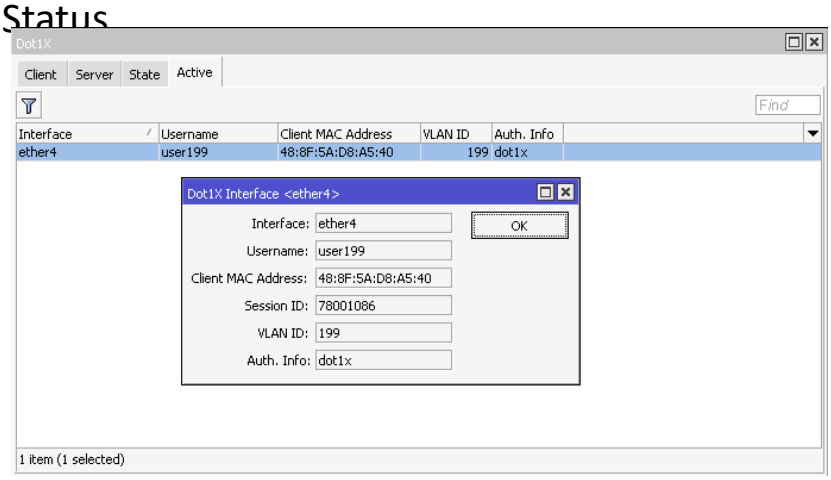
Results

79

79

Supplicant (Client) – Dynamic VLAN

- Dot1x Status

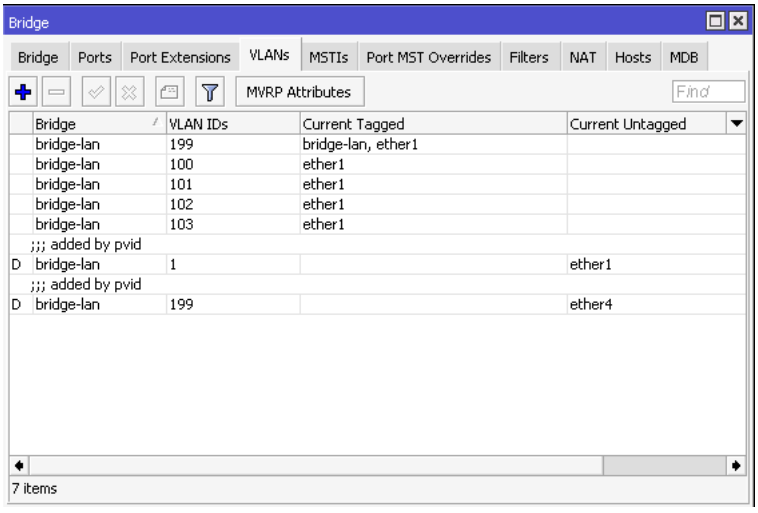


80

80

Supplicant (Client) – Dynamic VLAN

- Bridge VLAN

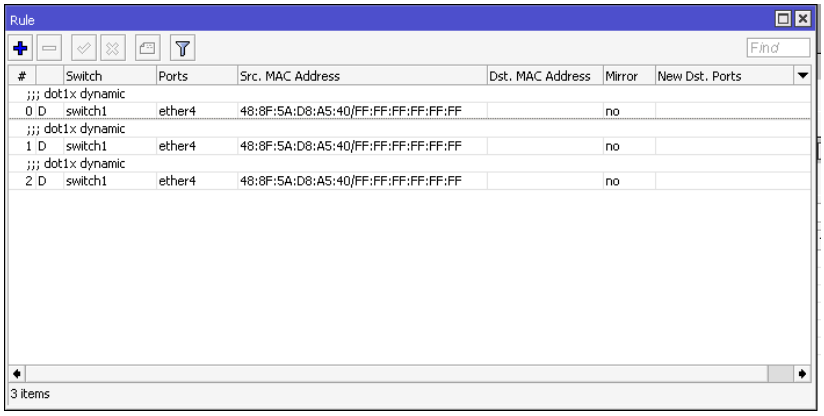


81

81

Supplicant (Client) – Dynamic Switch Rule

- Bridge VLAN



LinITX

Thank you for Listening

LinITX

- LinITX Blog
- Linked In

84

84

References

85

85