



WIRELESS & NETWORKING EXPERTS

Port Based Authentication 802.1X (dot1x)

March 2025 © Jono Thompson
Multithread Consultants Ltd



1

WIRELESS & NETWORKING EXPERTS

MIKROTIK

E-COMMERCE TRAINING

CONSULTANCY

ABOUT US:

- LinITX.com eCommerce website started in 2002
- Official MikroTik Master Distributor
- MikroTik Certified Training Partner
- Consultancy including WiFi site surveys
- Two UK warehouses with high stock levels
- Highly trained technical team

@ team@linitx.com

LinITX.com

01449 888000

EXPERT TRAINERS:

JONO THOMPSON
Jono has over 20 years of experience in networking. He holds multiple MikroTik and Ubiquiti qualifications. He is also a fully Certified Ubiquiti and MikroTik Training Partner.

RON TOUW
Ron has 40 years of experience in wireless and networking protocols. He holds multiple certifications in Ubiquiti, MikroTik, Ruckus, Meru, HP, Rohde & Schwarz and more.

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



Lin ITX

- 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



Lin ITX

- 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



Lin ITX

- 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

8

8

Dave



Lin ITX

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

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

10

What is 802.1X?

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



11

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.



12

12

Dot1x Components

Dot1x (802.1X) defines three terminologies:

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



13

13

Dot1x - Supplicant



14

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

15

Dot1x Supplicant

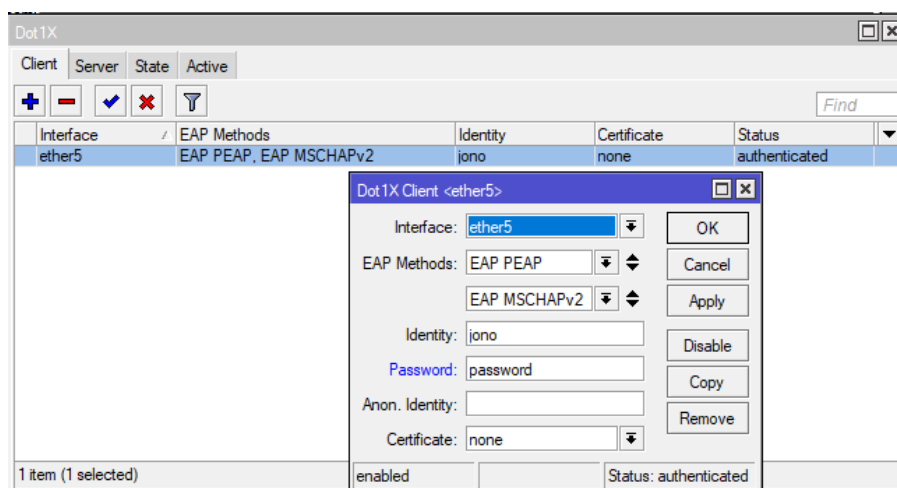
- RouterOS can be a Supplicant (Client) and connect to a network with 802.1x authentication
- RouterOS refers to a Supplication as dot1x Client
- RouterOS supports a number of different EAP types



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

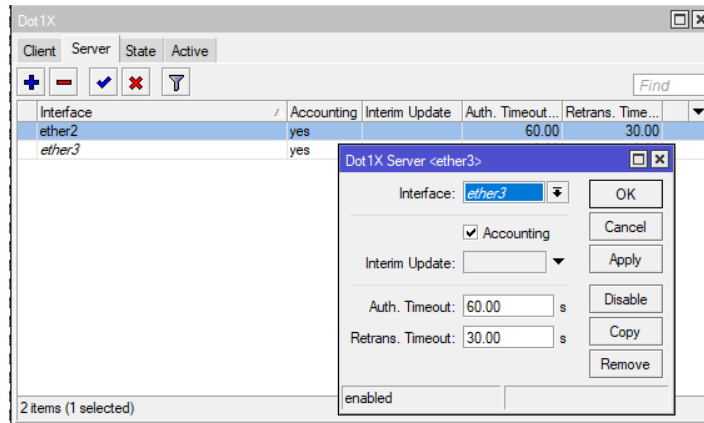


20

20

Dot1x Authenticator

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



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.

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

23

Dot1x Authenticator – MAC auth

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

New Dot1X Server

Interface: ether8

Auth. Types: ☐ dot1x ☒ mac auth

☒ Accounting

Interim Update:

MAC Auth. Mode: mac as username

RADIUS MAC Format: mac as username

Auth. Timeout: 60.00 s

Retrans. Timeout: 30.00 s

Reauth. Timeout:

Reject VLAN ID:

Guest VLAN ID:

Server Fail VLAN ID:

enabled



24

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.

Dot1X Server <ether3>

Interface:

Auth. Types: ☒ dot1x ☐ mac auth

☒ Accounting

Interim Update:

Auth. Timeout: s

Retrans. Timeout: s

Reauth. Timeout:

Reject VLAN ID:

Guest VLAN ID:

Server Fail VLAN ID:

enabled



27

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

Dot1X

Client Server State Active

Find

Interface	Status
ether2	authorized

1 item

Log

Freeze

Time	Source	Destination	Message
Jan/09/2020 10:34:39	memory	radius, debug, packet	received Access-Reject with id 124 from 10.100.200.200:1812
Jan/09/2020 10:34:39	memory	radius, debug, packet	Signature = 0x730630cca03b1d36fb98f4a815f40274
Jan/09/2020 10:34:39	memory	radius, debug, packet	Reply-Message = "username or password wrong, please check your login (PAP)"
Jan/09/2020 10:34:39	memory	radius, debug, packet	Message-Authenticator = 0xd5ce99498bda8d88c3a742258ce00734



28

28

Dot1x Authenticator – Guest VLAN

Dot1x Server <ether8>

Interface: ether8

Auth. Types: ☒ dot1x ☐ mac auth

☒ Accounting

Interim Update: [dropdown]

Auth. Timeout: 60.00 s

Retrans. Timeout: 30.00 s

Reauth. Timeout: [dropdown]

Reject VLAN ID: [dropdown]

Guest VLAN ID: 299

Server Fail VLAN ID: [dropdown]

enabled

- 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 retrans-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.

Dot1x Server <ether8>

Interface: ether8

Auth. Types: ☒ dot1x ☐ mac auth

☒ Accounting

Interim Update: [dropdown]

Auth. Timeout: 60.00 s

Retrans. Timeout: 30.00 s

Reauth. Timeout: [dropdown]

Reject VLAN ID: [dropdown]

Guest VLAN ID: [dropdown]

Server Fail VLAN ID: 199

enabled



30

30

Dot1x Authenticator – Reauth

Dot1x Server <ether3>

Interface: ether3

Auth. Types: ☒ dot1x ☐ mac auth

☒ Accounting

Interim Update: [dropdown]

Auth. Timeout: 60.00 s

Retrans. Timeout: 30.00 s

Reauth. Timeout: 00:30:00 ▲

Reject VLAN ID: [dropdown]

Guest VLAN ID: [dropdown]

Server Fail VLAN ID: [dropdown]

enabled

- The Authenticator can force a client to reauth at a set time interval 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”



33

33

Dynamic Switch Rules



34

34

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

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

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

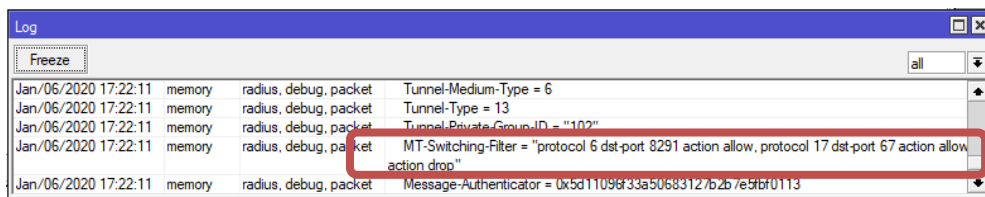
38

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"

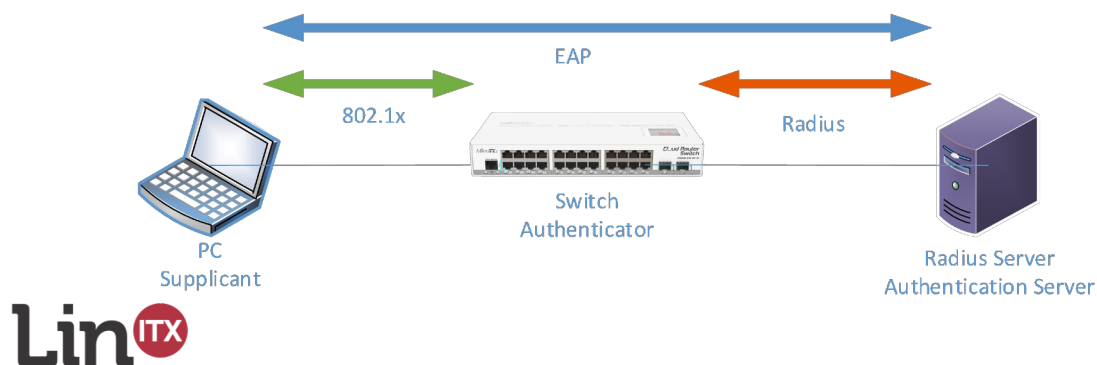


Log			
Freeze			
Jan/06/2020 17:22:11	memory	radius, debug, packet	Tunnel-Medium-Type = 6
Jan/06/2020 17:22:11	memory	radius, debug, packet	Tunnel-Type = 13
Jan/06/2020 17:22:11	memory	radius, debug, packet	Tunnel-Private-Group-ID = "102"
Jan/06/2020 17:22:11	memory	radius, debug, packet	MT-Switching-Filter = "protocol 6 dst-port 8291 action allow, protocol 17 dst-port 67 action allow, action drop"
Jan/06/2020 17:22:11	memory	radius, debug, packet	Message-Authenticator = 0x5d11096f33a50683127b2b7e5fbf0113

EAP

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

Lin ITX

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



43

43

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



45

45

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

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

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

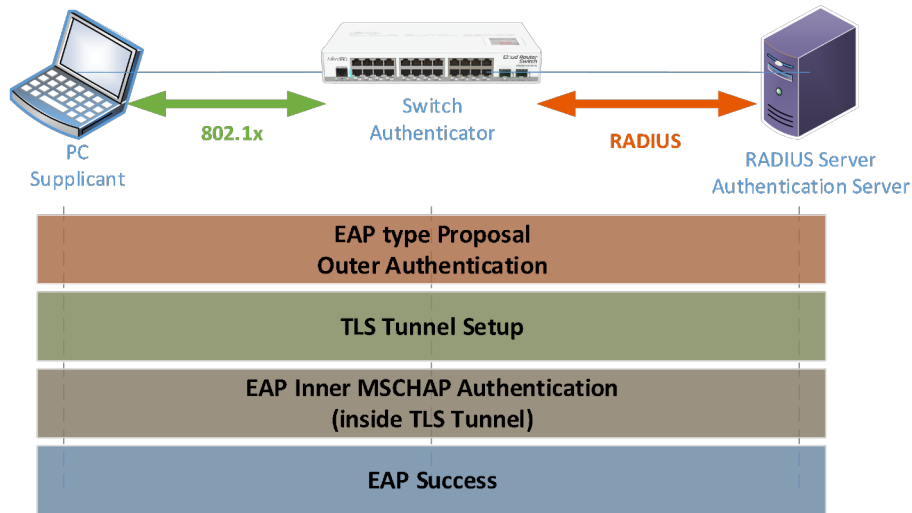
- Protected Extensible Authentication Protocol (PEAP) uses a server side certificate.
- PEAP is an encapsulation, not a authentication method
- PEAP works in 2 phases
- Phase 1 – server-side authentication is performed and a encrypted tunnel (TLS) is created
- Phase 2 – the client is now authenticated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



49

49

PEAP/EAP-MSCHAPv2 Flow



Certificates

- 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>



Dot1x Authentication Server



52

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

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

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

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

56

Debugging What to do when it doesn't work!



57

57

Dot1x Authenticator

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

The image shows two screenshots from a network device's configuration interface. The left screenshot shows the 'Log Rule' configuration for 'radius, debug'. The 'Topics' are set to 'radius' and 'debug', and the 'Action' is set to 'memory'. The right screenshot shows the resulting log output, which includes details about a new request, packet signatures, and various RADIUS attributes like NAS-Port-Type, Called-Station-Id, and Service-Type.

Time	Buffer	Topics	Message
Jan/06/2020 15:33:08	memory	radius, debug	received reply for 82.0d
Jan/06/2020 15:33:08	memory	radius, debug	new request 82.0e code=Access-Request service=dot1x called-id=74-4D-28-DB-FD-9A
Jan/06/2020 15:33:08	memory	radius, debug	sending 82.0e to 10.100.200.200:1812
Jan/06/2020 15:33:08	memory	radius, debug, packet	sending Access-Request with id 25 to 10.100.200.200:1812
Jan/06/2020 15:33:08	memory	radius, debug, packet	Signature = 0xc42#22cae91e62a5c036e143ecc5296
Jan/06/2020 15:33:08	memory	radius, debug, packet	NAS-Port-Type = 15
Jan/06/2020 15:33:08	memory	radius, debug, packet	Called-Station-Id = "74-4D-28-DB-FD-9A"
Jan/06/2020 15:33:08	memory	radius, debug, packet	Calling-Station-Id = "6C-C2-17-EC-BB-8A"
Jan/06/2020 15:33:08	memory	radius, debug, packet	Service-Type = 2
Jan/06/2020 15:33:08	memory	radius, debug, packet	Framed-MTU = 1400
Jan/06/2020 15:33:08	memory	radius, debug, packet	EAP-Message = 0x020300061500
Jan/06/2020 15:33:08	memory	radius, debug, packet	Message-Authenticator = 0x7538745fc99fca1ab312e15ea87fd7
Jan/06/2020 15:33:08	memory	radius, debug, packet	User-Name = "jono2"
Jan/06/2020 15:33:08	memory	radius, debug, packet	State = 0xbcc58e7901c2237a4b5b3a689f98251d
Jan/06/2020 15:33:08	memory	radius, debug, packet	Acct-Session-Id = "01001086"
Jan/06/2020 15:33:08	memory	radius, debug, packet	Unknown-Attribute(type=102) = 0x00
Jan/06/2020 15:33:08	memory	radius, debug, packet	NAS-Identifier = "2_Student_Switch"
Jan/06/2020 15:33:08	memory	radius, debug, packet	NAS-IP-Address = 10.100.2.2
Jan/06/2020 15:33:08	memory	radius, debug, packet	received Access-Challenge with id 25 from 10.100.200.200:1812

58

Dot1x Authenticator - Logs

The image shows a screenshot of the log output with a red box highlighting a specific log entry. The entry is labeled 'Sending Access Request on this Port and sending user details to the radius server'. The log entry details include the time, buffer, topics, and the full RADIUS Access-Request packet details, such as the signature, framed-MTU, NAS-Port-Type, and various attributes like Called-Station-Id, Calling-Station-Id, Service-Type, EAP-Message, Message-Authenticator, User-Name, Acct-Session-Id, NAS-Port-Id, State, Unknown-Attribute, NAS-Identifier, and NAS-IP-Address.

#	Time	Buffer	Topics	Message
969	Jan/28/2024 21:46:43	memory	radius, debug, packet	Sending Access-Request with id 150 to 10.100.250.200:1812
970	Jan/28/2024 21:46:43	memory	radius, debug, packet	Signature = 0xfb17aa56543a90b578cb8ef1bf7d3cc8
971	Jan/28/2024 21:46:43	memory	radius, debug, packet	Framed-MTU = 1400
972	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-Port-Type = 15
973	Jan/28/2024 21:46:43	memory	radius, debug, packet	Called-Station-Id = "2C-C8-1B-08-F9-62"
974	Jan/28/2024 21:46:43	memory	radius, debug, packet	Calling-Station-Id = "74-4D-28-DB-FD-A8"
975	Jan/28/2024 21:46:43	memory	radius, debug, packet	Service-Type = 2
976	Jan/28/2024 21:46:43	memory	radius, debug, packet	EAP-Message = 0x020200061a03
977	Jan/28/2024 21:46:43	memory	radius, debug, packet	Message-Authenticator = 0x5d5dd073f637e00ba78ac45710d046ef
978	Jan/28/2024 21:46:43	memory	radius, debug, packet	User-Name = "student2a"
979	Jan/28/2024 21:46:43	memory	radius, debug, packet	Acct-Session-Id = "46000086"
980	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-Port-Id = "ether8"
981	Jan/28/2024 21:46:43	memory	radius, debug, packet	State = 0x7af4ca2e371f5458d4cc1bd1860088f2
982	Jan/28/2024 21:46:43	memory	radius, debug, packet	Unknown-Attribute(type=102) = 0x00
983	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-Identifier = "Student_2_Switch"
984	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-IP-Address = 10.100.2.252

59

59

Dot1x Authenticator - Logs

#	Time	Buffer	Topics	Message
973	Jan/28/2024 21:46:43	memory	radius, debug, packet	sending Access-Request with id 150 to 10.100.250.200:1812
974	Jan/28/2024 21:46:43	memory	radius, debug, packet	Signature = 0xfb17aa56543a90b578cb8ef1bf7d3cc8
975	Jan/28/2024 21:46:43	memory	radius, debug, packet	Framed-MTU = 1400
976	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-Port-Type = 13
977	Jan/28/2024 21:46:43	memory	radius, debug, packet	Called-Station-Id = "2C-C8-1B-08-F9-62"
978	Jan/28/2024 21:46:43	memory	radius, debug, packet	Calling-Station-Id = "74-4D-28-DB-FD-A8"
979	Jan/28/2024 21:46:43	memory	radius, debug, packet	Service-Type = 8
980	Jan/28/2024 21:46:43	memory	radius, debug, packet	EAP-Message = 0x020200061a03
981	Jan/28/2024 21:46:43	memory	radius, debug, packet	Message-Authenticator = 0x54f4d073f637e00ba78ac45710d046ef
982	Jan/28/2024 21:46:43	memory	radius, debug, packet	User-Name = "student2a"
983	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-Port-Id = "ether8"
984	Jan/28/2024 21:46:43	memory	radius, debug, packet	State = 0x7af9c42e371f3458d4cc1bd1860088f2
985	Jan/28/2024 21:46:43	memory	radius, debug, packet	Unknown-Attributes (type = 100) = 0x00
986	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-Identifier = "Student_2_Switch"
987	Jan/28/2024 21:46:43	memory	radius, debug, packet	NAS-IP-Address = 10.100.2.252

LinITX

60

60

Dot1x Authenticator - Logs

#	Time	Buffer	Topics	Message
985	Jan/28/2024 21:46:43	memory	radius, debug, packet	received Access-Accept with id 150 from 10.100.250.200:1812
986	Jan/28/2024 21:46:43	memory	radius, debug, packet	Signature = 0x66c407a605cb11e118544575898efbdf
987	Jan/28/2024 21:46:43	memory	radius, debug, packet	EAP-Message = 0x03020004
988	Jan/28/2024 21:46:43	memory	radius, debug, packet	MS-MPPE-Recv-Key = 0xce02c80f988e53e99255f9d80afc5bce
989	Jan/28/2024 21:46:43	memory	radius, debug, packet	061b17257de0ade9bfd8eeb45eb615a5
990	Jan/28/2024 21:46:43	memory	radius, debug, packet	7bd9
991	Jan/28/2024 21:46:43	memory	radius, debug, packet	MS-MPPE-Send-Key = 0xfdd4bf602e2db7ab9dbe661f139549b1
992	Jan/28/2024 21:46:43	memory	radius, debug, packet	8b462aa435d767a1c3db5ab171917b64
993	Jan/28/2024 21:46:43	memory	radius, debug, packet	781f
994	Jan/28/2024 21:46:43	memory	radius, debug, packet	Tunnel-Medium-Type = 6
995	Jan/28/2024 21:46:43	memory	radius, debug, packet	Tunnel-Type = 13
996	Jan/28/2024 21:46:43	memory	radius, debug, packet	Tunnel-Private-Group-ID = "102"
997	Jan/28/2024 21:46:43	memory	radius, debug, packet	Class = 0xd71382edc0d4f0b3
998	Jan/28/2024 21:46:43	memory	radius, debug, packet	Message-Authenticator = 0xf07c380558c9b5e4cce3f25333a250d2
999	Jan/28/2024 21:46:43	memory	radius, debug	received reply for 82:f6

LinITX

61

61

Dot1x Authenticator - Logs

Log				
Freeze		Find all		
#	Time	Buffer	Topics	Message
985	Jan/28/2024 21:46:43	memory	radius, debug, packet	received Access-Accept with id 150 from 10.100.250.200:1812
986	Jan/28/2024 21:46:43	memory	radius, debug, packet	Signature = 0x66c407a605cb11e118544575898efbdf
987	Jan/28/2024 21:46:43	memory	radius, debug, packet	EAP-Message = 0x03020004
988	Jan/28/2024 21:46:43	memory	radius, debug, packet	M5-MPPE-Recv-Key = 0xce02c80f988e53e99255f9d80afc5bce
989	Jan/28/2024 21:46:43	memory	radius, debug, packet	061b17257de0ade9bfd8eeb45eb615a5
990	Jan/28/2024 21:46:43	memory	radius, debug, packet	7bd9
991	Jan/28/2024 21:46:43	memory	radius, debug, packet	M5-MPPE-Send-Key = 0xfdd4bf602e2db7ab9dbe661f139549b1
992	Jan/28/2024 21:46:43	memory	radius, debug, packet	8b462aa435d767a1c3db5ab171917b64
993	Jan/28/2024 21:46:43	memory	radius, debug, packet	781f
994	Jan/28/2024 21:46:43	memory	radius, debug, packet	Tunnel-Medium-Type = 6
995	Jan/28/2024 21:46:43	memory	radius, debug, packet	Tunnel-Type = 13
996	Jan/28/2024 21:46:43	memory	radius, debug, packet	Tunnel-Private-Group-ID = "102"
997	Jan/28/2024 21:46:43	memory	radius, debug, packet	Class = 0x01000200040f0b0c
998	Jan/28/2024 21:46:43	memory	radius, debug, packet	Message-Authenticator = 0xf07c380558c9b5e4cce3f25333a250d2
999	Jan/28/2024 21:46:43	memory	radius, debug	received reply for 82:f6

1000 items (1 selected)



62

62

Dot1x Authenticator Status

Dot1X		
Client	Server	State Active
Find		
Interface	Status	
ether2	authorized	
1 item		

Dot1X			
Client	Server	State	Active
Find			
Interface	Username	Client MAC Address	VLAN ID
ether2	jono	4C:5E:0C:D3:3D:94	299
1 item			

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

64

MikroTik dot1x Setup



65

65

Setup

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



66

66

Setup - Topology

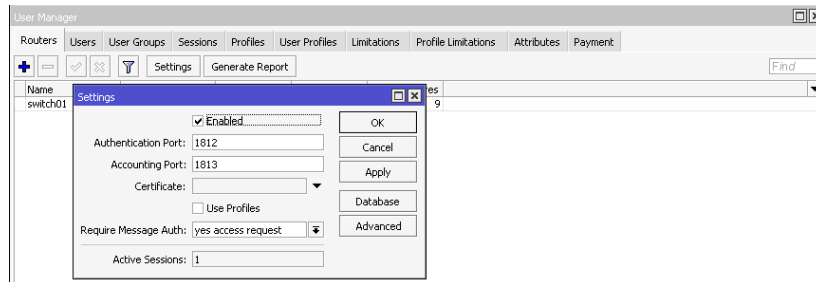


67

67

User manager Setup

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



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

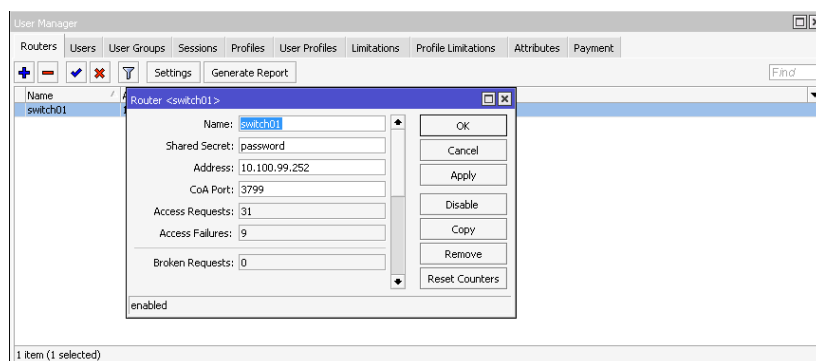


68

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

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
```

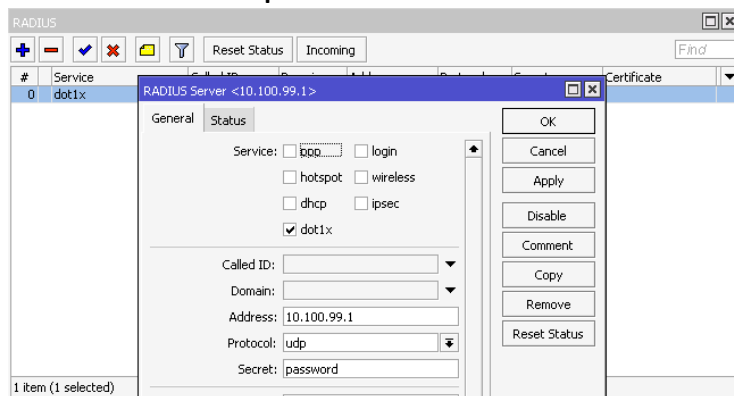


71

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
```

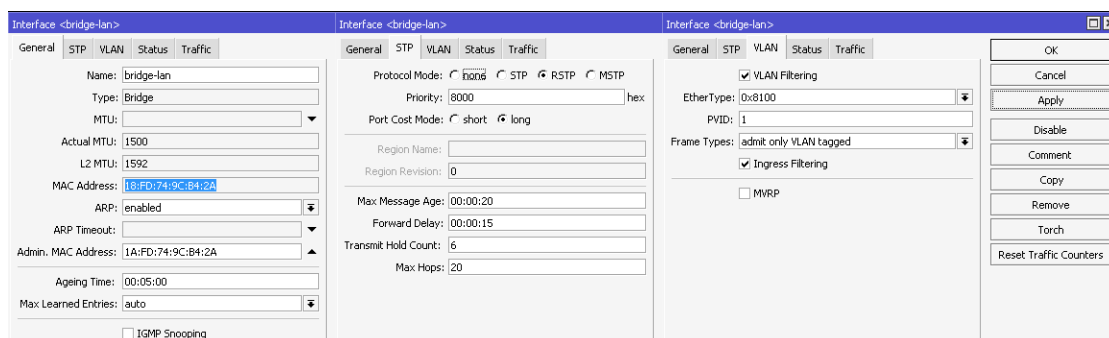


72

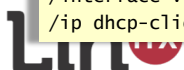
72

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
```

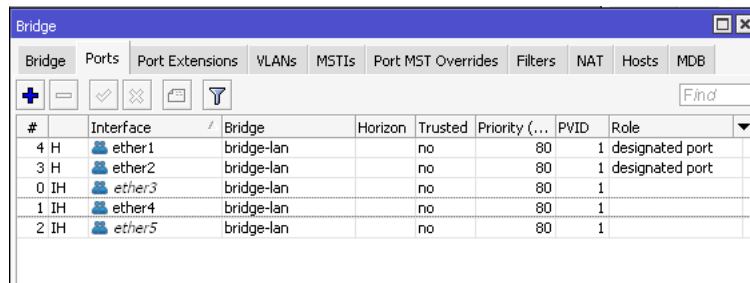


73

73

Authenticator – Bridge Configuration

- Add interfaces as bridge ports



#	Interface	Bridge	Horizon	Trusted	Priority (...)	PVID	Role
4 H	ether1	bridge-lan		no	80	1	designated port
3 H	ether2	bridge-lan		no	80	1	designated port
0 IH	ether3	bridge-lan		no	80	1	
1 IH	ether4	bridge-lan		no	80	1	
2 IH	ether5	bridge-lan		no	80	1	

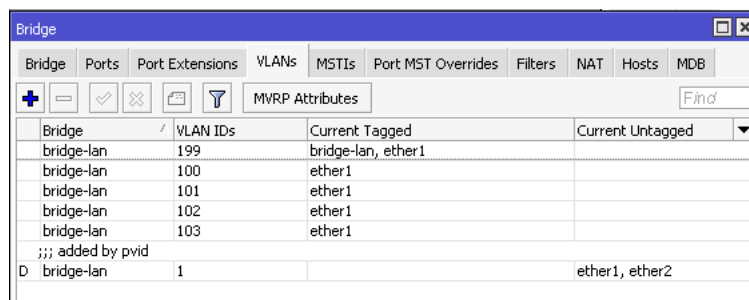
```
/interface bridge port
add bridge=bridge-lan interface=ether1
add bridge=bridge-lan interface=ether2
add bridge=bridge-lan interface=ether3
add bridge=bridge-lan interface=ether4
add bridge=bridge-lan interface=ether5
```

74

74

Authenticator – Bridge Configuration

- Add VLANs to bridge



Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge-lan	199	bridge-lan, ether1	
bridge-lan	100	ether1	
bridge-lan	101	ether1	
bridge-lan	102	ether1	
bridge-lan	103	ether1	
;;; added by pvid			
bridge-lan	1		ether1, ether2

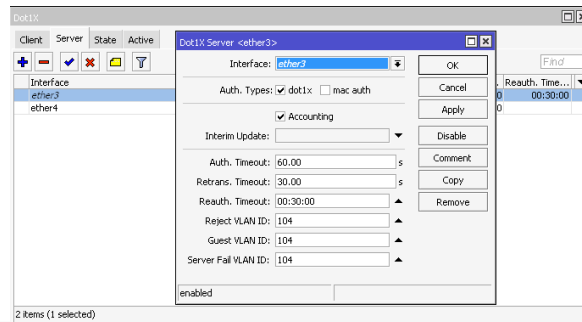
```
/interface bridge vlan
add bridge=bridge-lan tagged=bridge-lan,ether1 vlan-ids=199
add bridge=bridge-lan tagged=ether1 vlan-ids=100
add bridge=bridge-lan tagged=ether1 vlan-ids=101
add bridge=bridge-lan tagged=ether1 vlan-ids=102
add bridge=bridge-lan tagged=ether1 vlan-ids=103
```

75

75

Authenticator – dot1x Server

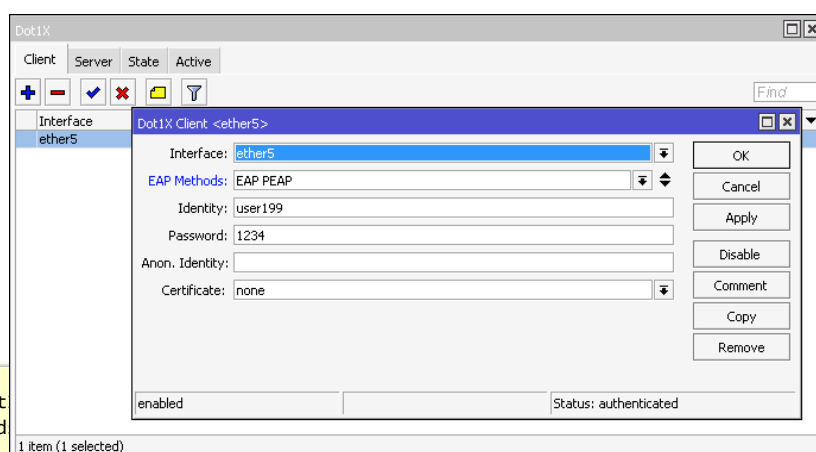
- Set dot1x server to run on the required ports. Set any failback vlans as needed



```
/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

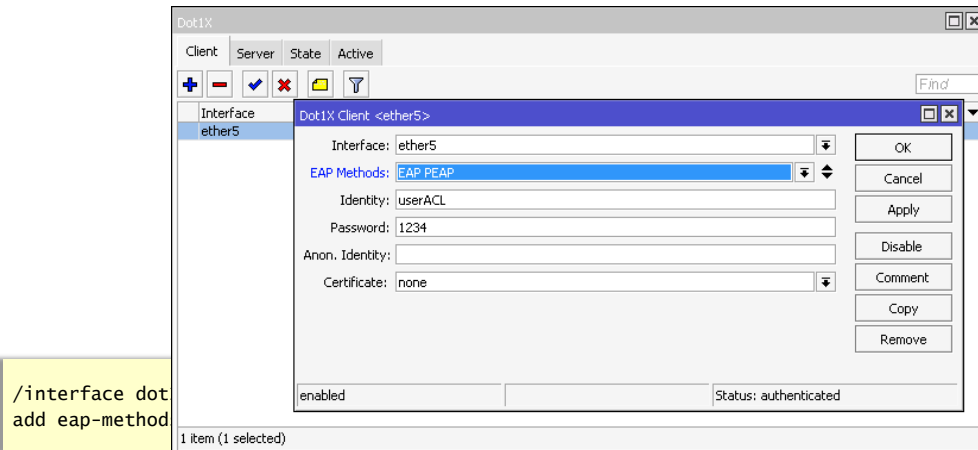
Supplicant (Client) – Dynamic VLAN



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

77

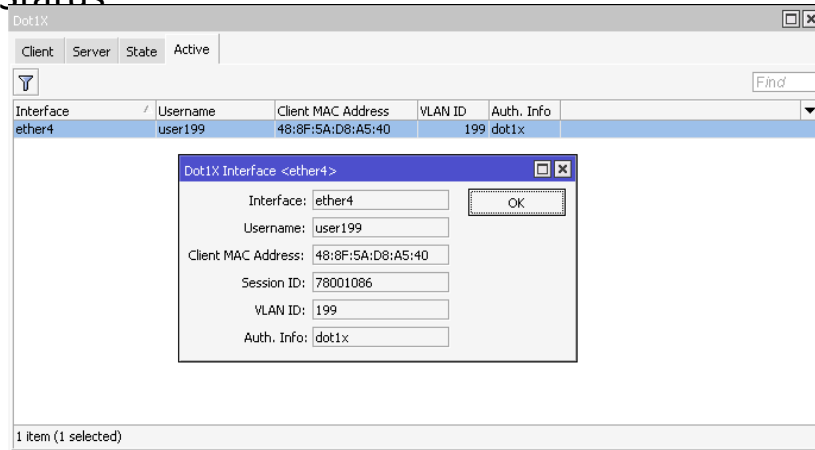
Supplicant (Client) – Dynamic ACL



Results

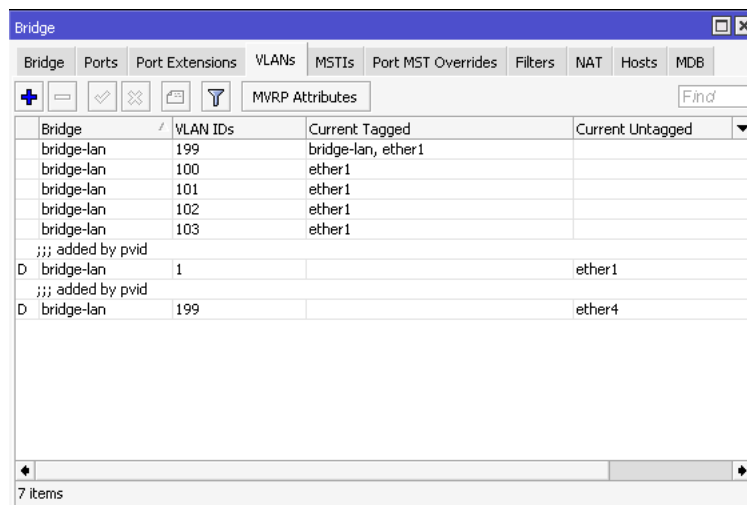
Supplicant (Client) – Dynamic VLAN

- Dot1x Status



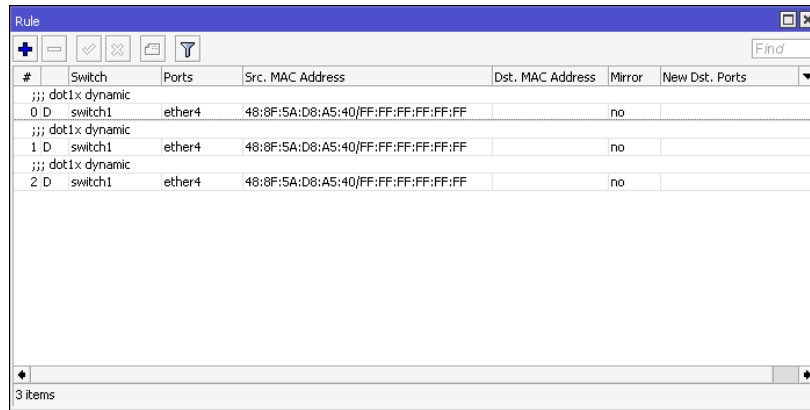
Supplicant (Client) – Dynamic VLAN

- Bridge VLAN



Supplicant (Client) – Dynamic Switch Rule

- Bridge VLAN



#	Switch	Ports	Src. MAC Address	Dst. MAC Address	Mirror	New Dst. Ports
;;; dot1x dynamic						
0 D	switch1	ether4	48:8F:5A:D8:A5:40/FF:FF:FF:FF:FF:FF		no	
;;; dot1x dynamic						
1 D	switch1	ether4	48:8F:5A:D8:A5:40/FF:FF:FF:FF:FF:FF		no	
;;; dot1x dynamic						
2 D	switch1	ether4	48:8F:5A:D8:A5:40/FF:FF:FF:FF:FF:FF		no	

Thank you for Listening

- LinITX Blog

- Linked In



84

84

References



85

85