VLAN in MikroTik

0

By Mohammed Khomeini Bin ABU MUM Indonesia, 2013



Malaysia



About Presentation

- To help you understand fundamental of Virtual Local Area Network (VLAN) and implementation in MikroTik router
- To explain a few example of implementation in site
- To show example running VLAN in several MikroTik routers



About Me..

Mohammed Khomeini Bin Abu

- MikroTik Certified Engineer (MTCINE, MTCRE, MTCWE, MTCTCE, MTCUME)
- MikroTik Certified Trainer (TR0204)
- MikroTik Certified Academy Trainer (ACTR0062)
- Network Consultant



Introduction

Content

VLAN Implementation

Conclusion

° INTRODUCTION TO VLAN

Virtual LANs – WHAT? (I)

- Most commonly used protocol for VLAN on an ethernet network is 802.1Q
- It insert 4 byte tag into a standard ethernet frame
- Working at Data Link Layer (OSI Layer 2)
- Maximum number of VLAN in one interface is 4095



Virtual LANs – WHAT? (2)

- Each VLANs is treated as separate subnet / broadcast domain.
- Devices on a VLAN are restricted to only communicating with devices that are on their own VLAN
- MikroTik also support Vlan over Vlan / 802.IQinQ / 802.Iad





Virtual LANs – WHY? (I)

Provide segmentation





Virtual LANs – WHY? (2)

- Multiple LAN in a single physical interface
- Make the local network more simple
- Multiple broadcast domain in a single physical interface
- VLANs can increase security and management of different network in one single interface
- Priority

Virtual LANs - Parameter

- Edge ports: (Untagged, in Cisco: called Access Port)
 - Switch port that configure as a part of the vlan
 - This port not send 4 byte vlan tag. Used for device that not pass the VLAN, like computer, printer, server, etc.
- Core port: (Tagged, in Cisco: Trunk Port)
 - Switch port configured to send 4 byte or more VLAN tag. Used for device that support VLAN technologies like switches, manageable switch, routers, etc.



Virtual LANs in MikroTik (1)

- In RouterOS,VLAN can be implemented in switch environment and in router environment simultaneously.
- Also possible to runVLAN in wireless or bridge interface
- It is not possible to have VLAN put on a wireless interface in a station mode
- FILO VLAN tagged is used for 802.1QinQ implementation

Virtual LANs in MikroTik (2)

To create vlan in MikroTik, you should have the interface first (if you want to implement in bridge interface)

Interface for trunk / access

| Interface <vlan-< th=""><th>100></th><th></th></vlan-<> | 100> | |
|--|-------------------|----------|
| General Traff | ïc | ОК |
| Name: | vlan-100 | Cancel |
| Туре: | VLAN | Apply |
| MTU: | 1500 | Disable |
| L2 MTU: | 65531 | |
| MAC Address: | 00:00:AB:B2:BB:04 | |
| ARP: | enabled | ₹ Copy |
| VLAN ID: | 100 | Torch |
| Interface: | bridge-pptp | ▼ |
| | Use Service Tag | |
| | | |
| | | |
| | | |
| | | |
| | | |
| enabled | running | |

| ОК | | | | | | | | | | | | | |
|-----------|--|----------------|---|-------------|-----------|------------|-----------|-----------|----------|--------|------------|--|--|
| Cancel | | Interface List | | | | | | | | | | | |
| Apply | | Inter | face Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN \ | /RRP Bond | ling LTE | | | | |
| Disable | | + | | - 7 | | | | | | | Find | | |
| Comment | | | Name | ∆ Type | | L2 MTU | Tx | Rx | Tx Pac | Rx Pac | Tx Drops 💌 | | |
| Сору | | DR | «-» <pptp-pptp-us< td=""><td> PPTP Ser</td><td>ver</td><td></td><td>26.4 kbps</td><td>2.0 kbps</td><td>3</td><td>3</td><td>0</td></pptp-pptp-us<> | PPTP Ser | ver | | 26.4 kbps | 2.0 kbps | 3 | 3 | 0 | | |
| Deres and | | R | ttt bridge-pptp | Bridge | | 65535 | 26.4 kbps | 1800 bps | 3 | 3 | 0 | | |
| Remove | | R | 🚸 vlan-100 | VLAN | | 65531 | 26.4 kbps | 1800 bps | 3 | 3 | 0 | | |
| Torch | | R | 🚸 vlan-200 | VLAN | | 65531 | 0 bps | 0 bps | 0 | 0 | 0 | | |
| | | R | ether1 | Ethernet | | | 29.6 kbps | 3.6 kbps | 7 | 4 | 0 | | |
| | | R | ether2 | Ethernet | | | 0 bps | 0 bps | 0 | 0 | 0 | | |
| ┝─┛ | | R | ether3 | Ethernet | | | 0 bps | 0 bps | 0 | 0 | 0 | | |
| | | R | ether4 | Ethernet | | | 0 bps | 0 bps | 0 | 0 | 0 | | |
| | | R | ether5 | Ethernet | | | 0 bps | 0 bps | 0 | 0 | 0 | | |
| | | | | | | | | | | | | | |

802. I Q Flow Chart in RouterOS



° VIRTUAL LANS IMPLEMENTATION

How Virtual LANs implemented in :

- Small network (SOHO)
- Medium network (SME)
- Wireless network
- Tunneling



- Have only single router and single/multi managed switch
- Create 2VLAN in MikroTik router
 - Vlan-100 = office
 - Vlan-200= wifi





Virtual LANs – SoHo (3)

- RI Configuration
 - IP Address, Subnet Mask, Default Gateway and masquerade is configured at ether I
 - To be able to forward tagged packet, we need to create trunk bridge [admin@RI] > interface bridge add name=bridge-trunk protocol-mode=rstp
 - Add port (interface) that you want to forward the VLAN in the trunk bridge (at least 1 port)

[admin@R1] > interface bridge port add interface=ether5 bridge=bridge-trunk

 Add VLAN on trunk interface (bridge-trunk) [admin@RI] > interface vlan add name=vlan-100 interface=bridge-trunk vlan-id=100 [admin@RI] > interface vlan add name=vlan-200 interface=bridge-trunk vlan-id=200

Virtual LANs – SoHo (4)

• Create IP Address for VLAN

[admin@R1] > ip address add address=192.168.100.1/24 interface=vlan-100 [admin@R1] > ip address add address=192.168.200.1/24 interface=vlan-200

- Create DHCP setup for interface vlan-100 and vlan-200 with public DNS (8.8.8.8 and 8.8.4.4)
- Connect managed switch into interface=ether5
- Configure managed switch as desired





Virtual LANs – SME (I)

- You have more than one router
- Create 3 VLAN in MikroTik router
 - Vlan-100 = office
 - Vlan-200 = wifi
 - Vlan-230 = voip



Virtual LANs – SME (3)

- RI Configuration
 - IP Address, Subnet Mask, Default Gateway and masquerade is configured at ether I
 - To be able to forward tagged packet, we need to create trunk bridge

[admin@R1] > interface bridge add name=bridge-trunk protocol-mode=rstp

 Add port (interface) that you want to forward the VLAN in the trunk bridge

[admin@RI] > interface bridge port add interface=ether2 bridge=bridge-trunk [admin@RI] > interface bridge port add interface=ether5 bridge=bridge-trunk

Virtual LANs – SME (4)

Add VLAN on trunk interface (bridge-trunk)

[admin@RI] > interface vlan add name=vlan-100 interface=bridge-trunk vlan-id=100 [admin@RI] > interface vlan add name=vlan-200 interface=bridge-trunk vlan-id=200 [admin@RI] > interface vlan add name=vlan-230 interface=bridge-trunk vlan-id=230

 To create access port, create access bridge interface first.

[admin@R1] > interface bridge add name=bridge-vlan-230

 Then add access port interface and VLAN into the access bridge

[admin@RI] > interface bridge port add interface=ether4 bridge=bridge-vlan-230 [admin@RI] > interface bridge port add interface=vlan-230 bridge=bridge-vlan-230

Virtual LANs – SME (5)

Create IP Address

[admin@R1] > ip address add address=192.168.100.1/24 interface=vlan-100 [admin@R1] > ip address add address=192.168.200.1/24 interface=vlan-200 [admin@R1] > ip address add address=192.168.230.1/24 interface=vlan-230

- Create DHCP setup for interface vlan-100, vlan-200, and vlan-230 with public dns (8.8.8.8 and 8.8.4.4)
- Connect managed switch into interface=ether2
- Configure managed switch as desired

Virtual LANs – SME (6)

- R2 Configuration
 - Create bridge interface [admin@R2] > interface bridge add name=bridge-trunk
 - Add interface that we want to forward tagged (trunk) packet to bridge-trunk interface
 [admin@R2] > interface bridge port add interface=ether2 bridge=bridge-trunk
 [admin@R2] > interface bridge port add interface=ether5 bridge=bridge-trunk
 - Connect managed switch into interface=ether2
 - Configure managed switch as desired

Virtual LANs – Wireless (1)



Virtual LANs – Wireless (2)

- RI Configuration
 - IP Address, Subnet Mask, Default Gateway and masquerade is configured at ether I
 - To be able to forward tagged packet, we need to create trunk bridge

[admin@R1] > interface bridge add name=bridge-trunk protocol-mode=rstp

 Add port (interface) that you want to forward the VLAN in the trunk bridge (at least I port) [admin@RI] > interface bridge port add interface=ether5 bridge=bridge-trunk

Virtual LANs – Wireless (3)

 Add VLAN on trunk interface (bridge-trunk) [admin@RI] > interface vlan add name=vlan-100 interface=bridge-trunk vlan-id=100 [admin@RI] > interface vlan add name=vlan-200 interface=bridge-trunk vlan-id=200

Create IP Address

[admin@R1] > ip address add address=192.168.100.1/24 interface=vlan-100 [admin@R1] > ip address add address=192.168.200.1/24 interface=vlan-200

 Create DHCP setup for interface vlan-100 and vlan-200 with public dns (8.8.8.8 and 8.8.4.4)

Virtual LANs – Wireless (4)

- R2 and R3 Configuration
 - Create bridge interface

[admin@R2] > interface bridge add name=bridge-trunk

 Add interface that we want to forward tagged (trunk) packet to bridge-trunk interface

[admin@R2] > interface bridge port add interface=ether1 bridge=bridge-trunk [admin@R2] > interface bridge port add interface=wlan1 bridge=bridge-trunk

 Configure Wireless interface as ap-bridge (for R3, wireless interface is configured as mode=stationbridge)

[admin@R1] > interface wireless set wlan1 mode=ap-bridge disabled=no

 In R3, connect managed switch into interface=ether I and configure managed switch as desired

Virtual LANs over PPTP (I)

- RouterOS supported bridge through Point to Point Tunnel Protocol (PPTP) using BCP (Bridge Control Protocol).
- BCP allows to bridge ethernet packet through PPP link
- To implement VLAN over PPTP tunnel, we should use BCP and MLPPP feature to forward packet between segment / subnet.

Virtual LANs – PPTP (2)



YES

Create IP address and DHCP setup at

Vlan interface

Finish

Create

DHCPserver?

TYES

Create vlan on trunk

interface

NO.

Create

Create vlan on trunk

interface

VES

NO

Virtual LANs over PPTP (3)

- Make sure there is a routing between R1 to R4
- RI Configuration
 - IP Address, Subnet Mask, Default Gateway and masquerade is configured at ether2
 - Create bridge interface

[admin@R1] > interface bridge add protocol-mode=rstp name=bridge-pptp

 Add port (interface) that you want to forward the VLAN in the trunk bridge (at least I port) [admin@RI] > interface bridge port add interface=ether5 bridge=bridge-pptp

Virtual LANs over PPTP (4)

 Add VLAN on trunk interface (bridge-pptp) [admin@R1] > interface vlan add name=vlan-100 interface=bridge-pptp vlan-id=100 [admin@R1] > interface vlan add name=vlan-200 interface=bridge-pptp vlan-id=200

Create IP Address

[admin@R1] > ip address add address=192.168.100.1/24 interface=vlan-100 [admin@R1] > ip address add address=192.168.200.1/24 interface=vlan-200

 Create DHCP setup for interface vlan-100 and vlan-200 with public DNS (8.8.8.8 and 8.8.4.4)

Virtual LANs over PPTP (5)

 Create PPTP-Server with BCP and MLPPP enabled

[admin@RI] > ppp profile add bridge=bridgeI name=pptp-bridge

[admin@R1] > interface pptp-server server set enabled=yes default-profile=pptp-bridge \

[admin@R1] > mrru=5000

[admin@R1] > ppp secret add name=pptp-user password=1234 profile=pptp-bridge \

[admin@R1] > local-address=1.1.1.1 remote-address=2.2.2.2

R4 Configuration

• Create bridge interface

[admin@R4] > interface bridge add protocol-mode=rstp name=bridge-pptp

 Add interface that we want to forward tagged (trunk) packet to bridge-trunk interface

[admin@R4] > interface bridge port add interface=ether5 bridge=bridge-pptp

Virtual LANs over PPTP (6)

 Create PPTP-Server with BCP and MLPPP enabled

[admin@R4] > ppp profile add bridge=bridge-pptp name=pptp-bridge [admin@R4] > interface pptp-client add connect=192.168.12.1 user=pptp-user \ [admin@R4] > password=1234 profile=pptp-bridge mrru=5000 disabled=no [admin@R4] >

- Connect managed switch into interface=ether5
- Configure managed switch as desired



Conclusion

- All VLAN should be put in bridge interface as it is easy to manipulate whether it is a trunk port or an access port. The disadvantage is we create more header on data link layer
- When you don't enable MLPPP in PPP tunnel, you still can use internet but slow, cause the packet has been fragmented.
- In wireless mode, should use other than mode=station
- Remember flow chart



References

- I. wiki.mikrotik.com
- 2. Cisco CCNA modules
- 3. Vlan workshop, www.roamingnet.com
- 4. id-networkers.com
- 5. www.mikrotik.co.id



Credit to

- Mr. Rofiq Fauzi
- Mr. Pujo Dewobroto
- Mr. Gatot Wibowo Hamiseno
- Mr. Herry Darmawan
- Mr. Mat Dawam Abas
- MikroTik Team



Mohammed Khomeini Bin Abu khomeini 1980@gmail.com +6013-7221134 (whatsapp)