VLAN in MikroTik
By Mohammed Khomeini Bin ABU
MUM Indonesia, 2013
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
Content

- Introduction
- VLAN Implementation
- Conclusion
INTRODUCTION TO VLAN
Virtual LANs – WHAT? (1)

- 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

![Diagram of 802.1Q VLAN Tag Structure]

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Source Address</th>
<th>802.1Q VLAN Tag</th>
<th>Type/Len</th>
<th>Data</th>
<th>Frame Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Bytes</td>
<td></td>
<td>4 Bytes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 802.1Q Tag Structure
  - 2 Bytes
    - Tag Protocol ID
    - User Priority (3 Bits)
    - Canonical Form Indicator (1 Bit)
  - 12 Bits
  - VLAN ID

![Diagram of Ethernet Frame Structure]
Virtual LANs – WHAT? (2)

- Each VLAN 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 / 802.1QinQ / 802.1ad.
Virtual LANs – WHY? (1)

- 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 run VLAN 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)

VLAN ID = unique

Interface for trunk / access
802.1Q Flow Chart in RouterOS

Start

Accept 802.1Q?

YES

Create trunk bridge

Add port (interface) to trunk bridge

Create access port?

YES

Create vlan on trunk interface

NO

NO

NO

2

2

Create access bridge

Add port (interface) and vlan to access bridge

Create DHCP-server?

YES

Create IP address and DHCP setup at Vlan interface

Finish

Created By Mohammed Khomeini Abu
VIRTUAL LANS IMPLEMENTATION
How Virtual LANs implemented in:

- Small network (SOHO)
- Medium network (SME)
- Wireless network
- Tunneling
Virtual LANs – SoHo (I)

- Have only single router and single/multi managed switch
- Create 2 VLAN in MikroTik router
  - Vlan-100 = office
  - Vlan-200 = wifi
Virtual LANs – SoHo (2)
Virtual LANs – SoHo (3)

- **R1 Configuration**
  - IP Address, Subnet Mask, Default Gateway and masquerade is configured at ether1
  - To be able to forward tagged packet, we need to create trunk bridge

```bash
[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 1 port)

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

- Add VLAN on trunk interface (bridge-trunk)

```bash
[admin@R1] > interface vlan add name=vlan-100 interface=bridge-trunk vlan-id=100
[admin@R1] > 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
QUIZ

From

Free! MikroTik
dari MU untuk MU
Virtual LANs – SME (1)

- You have more than one router
- Create 3 VLAN in MikroTik router
  - Vlan-100 = office
  - Vlan-200 = wifi
  - Vlan-230 = voip
Virtual LANs – SME (2)
Virtual LANs – SME (3)

- **R1 Configuration**
  - IP Address, Subnet Mask, Default Gateway and masquerade is configured at ether1
  - 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@R1] > interface bridge port add interface=ether2 bridge=bridge-trunk
  [admin@R1] > interface bridge port add interface=ether5 bridge=bridge-trunk
  ```
Virtual LANs – SME (4)

- Add VLAN on trunk interface (bridge-trunk)
  ```
  [admin@R1] > interface vlan add name=_vlan-100 interface=bridge-trunk vlan-id=100
  [admin@R1] > interface vlan add name=_vlan-200 interface=bridge-trunk vlan-id=200
  [admin@R1] > 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@R1] > interface bridge port add interface=ether4 bridge=bridge-vlan-230
  [admin@R1] > 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=vlans-100
  [admin@R1] > ip address add address=192.168.200.1/24 interface=vlans-200
  [admin@R1] > ip address add address=192.168.230.1/24 interface=vlans-230
  ```

- Create DHCP setup for interface vlans-100, vlans-200, and vlans-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)

- **R1 Configuration**
  - IP Address, Subnet Mask, Default Gateway and masquerade is configured at ether1
  - 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 1 port)
    
    ```
    [admin@R1] > interface bridge port add interface=ether5 bridge=bridge-trunk
    ```
Virtual LANs – Wireless (3)

- Add VLAN on trunk interface (bridge-trunk)
  
  [admin@R1] > interface vlan add name=_vlan-100_ interface=bridge-trunk_vlan-id=100
  [admin@R1] > 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=station-bridge)
    - [admin@R1] > interface wireless set wlan1 mode=ap-bridge disabled=no

- In R3, connect managed switch into interface=ether1 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)

- R1 will become dhcp-server for vlan-100 and vlan-200
- R4 will forward untagged packet to ether5 for client
- Create PPTP Server (R1) and client (R4)
Virtual LANs over PPTP (3)

• Make sure there is a routing between R1 to R4

• R1 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 1 port)
    [admin@R1] > 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@R1] > ppp profile add bridge=bridge1 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 \n  [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
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

1. wiki.mikrotik.com
2. Cisco CCNA modules
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
khomeini1980@gmail.com
+6013-7221134 (whatsapp)