VLAN Workshop.

Presenter: Paul Eriksson
About this presentation

- A seed from the forum by Randy (Graham)?: http://forum.mikrotik.com/viewtopic.php?f=2&t=24352
- This Workshop could last for hours..., but there is only 45 min.
About the company

- RoamingNet Sweden.
  - Helps organizations to increase the ROI in networking.
  - Designing and deployment of wired and wireless networks.
  - Network analysis and problem solving.
  - Project managing.
  - Worldwide support for different clients in different countries. Cooperates with Roamingwire Inc.
About me

• Have a technical degree as a Electric Engineer
• Been in networking since 1989.
• Senior networking consultant
• Certified MikroTik network consultant. (MTCZ0016).
• Certified MikroTik Trainer. (TR0027).
Topics

- Why VLANs?
- Brief Ethernet fundamentals.
- Brief VLAN fundamentals
- Switch configurations.
- How VLANs are built in MikroTik RouterOS.
Topics

- How VLANs are built in a wireless environment.
- Demo system.
- Summary.
- Questions.
Why VLANs

• Segment traffic, “Tripple Play”
• Limiting broadcast domains
• Provide unique traffic shaping opportunities (firewall, QoS, etc.)
• Secure the network
• Provide remote maintenance without interfering with the running network.
Why VLANs

- Providing a single HotSpot model
Ethernet fundamentals

• The two types of Ethernet frames used in networking are similar. The DIX V2.0 frame, frequently referred to as the Ethernet II frame, and the IEEE 802.3 frame.

• Both providing OSI level 3 with the needed data field. This field is also sometimes referred to as the MTU size of the packet.
VLAN fundamentals

<table>
<thead>
<tr>
<th>56 bits</th>
<th>8 bits</th>
<th>48 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>SFD</td>
<td>Individual/Group Address Bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Globally/Locally Administered Address Bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source Address</td>
</tr>
<tr>
<td>48 bits</td>
<td>16 bits</td>
<td>368 to 12000 bits (46 to 1500 bytes)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LLC/Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Frame Check Sequence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>32 bits</td>
</tr>
</tbody>
</table>

16 bits 3 bits 1 12 bits
VLAN Protocol ID 0x8100 Priority CFI VLAN Identifier
VLAN fundamentals

- 802.1Q working group provided a VLAN standard that inserts a four-byte tag into a standard Ethernet frame. Since 802.1Q arrived more than 20 years after the invention of Ethernet, there are plenty of VLAN-unaware devices. There still are lots of NICs that do not support the 4 byte extra field. These devices are not suitable for VLAN tagging because the MTU (layer 3 packet) size needs to be limited.
Switch configurations

There are two different types of switch ports.

- **Edge ports**: (Untagged, Cisco: Access Port)
  A switch port is configured to be part of a VLAN without sending the 4 byte tag. Used with VLAN unaware devices i.e client computer, printer.

- **Core port**: (Tagged, Cisco: Trunk Port)
  A switch port is configured to send out the 4 byte tag. Used with VLAN aware devices i.e switches, routers and servers.
Switch configurations

- Core switches interconnect with other switches.
- Edge switches connect to the core and to client computers, printers and other non VLAN aware devices.
How VLANs are built in RouterOS

- Commands:
  - /interface bridge add name=br2
  - /interface bridge port add bridge=br2 interface=ether2
  - /interface bridge port add bridge=br2 interface=ether3
  - /interface vlan add name=br2-vl2 interface=br2 vlan-id=2 disabled=no

- But now we cannot use untagged interfaces in the VLAN
How VLANs are built in a wireless environment.

- Create a WDS interface on both ends.
- Add the WDS interface into the bridge.
How VLANs are built in a wireless environment.

- **Commands:**
  - `/interface wireless wds add name=wds-mt2 master-interface=wlan1 wds-address=01:02:03:04:05:06 disabled=no`
  - `/interface bridge port add bridge=br2 interface=wds-rt-rnet-02`
STP and RSTP

- The problems with multiple bridge and STP/RSTP seem to be caused by an immature Linux kernel 2.6 software.

- The configuration works well, but the RSTP-PVST (PVST=Per VLAN Spanning Tree), meaning Per Bridge Spanning Tree in ROS function would be great. Support for MST 802.1s Multiple Spanning Tree are needed.
Demo network

- The network are built with:
  2 RouterBoard 532A
  1 Cisco Catalyst 2950 (SW-RNET-01)
  1 HP Procurve 2512 (SW-RNET-02)
- There is one main switch network (SW-SW-GE) and tree redundant networks (SW-SW-FE), (RT-RT-Cable) and (RT-RT-WDS)
- Test traffic from LAP-RNET-01 to LAP-RNET-02
### Bridge Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Bridge</th>
<th>Priority</th>
<th>Path Cost</th>
<th>Horizon</th>
<th>Role</th>
<th>Root Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>br2-vl2</td>
<td>br0</td>
<td>80</td>
<td>10000</td>
<td></td>
<td>designated port</td>
<td></td>
</tr>
<tr>
<td>ether1</td>
<td>br0</td>
<td>80</td>
<td>10000</td>
<td></td>
<td>disabled port</td>
<td></td>
</tr>
<tr>
<td>ether2</td>
<td>br2</td>
<td>80</td>
<td>10000</td>
<td></td>
<td>root port</td>
<td>11000</td>
</tr>
<tr>
<td>ether3</td>
<td>br2</td>
<td>80</td>
<td>30000</td>
<td></td>
<td>alternate port</td>
<td>40000</td>
</tr>
<tr>
<td>wds-rnt-mnet-02</td>
<td>br2</td>
<td>80</td>
<td>40000</td>
<td></td>
<td>alternate port</td>
<td>50000</td>
</tr>
<tr>
<td>Interface</td>
<td>Bridge</td>
<td>Priority</td>
<td>Path Cost</td>
<td>Horizon</td>
<td>Role</td>
<td>Root Path Cost</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>----------</td>
<td>-----------</td>
<td>---------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>br2-vl2</td>
<td>br0</td>
<td>80</td>
<td>10000</td>
<td></td>
<td>designated port</td>
<td></td>
</tr>
<tr>
<td>ether1</td>
<td>br0</td>
<td>80</td>
<td>10000</td>
<td></td>
<td>disabled port</td>
<td></td>
</tr>
<tr>
<td>ether2</td>
<td>br2</td>
<td>80</td>
<td>10000</td>
<td></td>
<td>root port</td>
<td>10000</td>
</tr>
<tr>
<td>ether3</td>
<td>br2</td>
<td>80</td>
<td>30000</td>
<td></td>
<td>designated port</td>
<td></td>
</tr>
<tr>
<td>wds-rt-rnet-01</td>
<td>br2</td>
<td>80</td>
<td>40000</td>
<td></td>
<td>designated port</td>
<td></td>
</tr>
</tbody>
</table>
SW-SW-GE cable disconnected
SW-SW-FE disconnected
RT-RT-Cable disconnected
Configuration of RT-RNET-01

# Script for configuring the Mikrotik to have one single bridge and create the VLAN on top of that bridge.

/sys id set name=RT-RNET-01

# Set up wireless
/int wire set wlan1 mode ap country="czech republic" band=5ghz hide yes wds-mode static disabled no
/int wire wds add master wlan1 name=wds-rt-rnet-02 wds-address=00:0C:42:05:AA:B5
/int wire acc add auth yes forw yes int wlan1 mac=00:0C:42:05:AA:B5

# Adding the bridges
/int br add name br2 prot rstp pri 0xffff

# Adding interfaces to the bridges
/int br po add bridge br2 int ether2 path 10000
/int br po add bridge br2 int ether3 path 30000
/int br po add bridge br2 int wds-rt-rnet-02 path 40000

# Adding the VLAN interfaces
/int vlan add name br2-vl2 int br2 vlan 2 dis no
/int vlan add name br2-vl5 int br2 vlan 5 dis no
/int vlan add name br2-vl10 int br2 vlan 10 dis no

# Adding an mgmt IP
/ip addr add add 172.30.99.1/24 int br2-vl2

# Setup SNMP
/snmp set contact=noc@roamingnet.com enabled=yes location="Prag MuM 2009"
Configuration of RT-RNET-02

#Script for configuring the Mikrotik to have one single bridge and create the VLAN on top of that bridge.

/sys id set name=RT-RNET-02

#Set up wireless
/int wire set wlan1 mode ap country="czech republic" band=5ghz hide yes wds-mode static disabled no
/int wire wds add master wlan1 name=wds-rt-rnet-01 wds-address=00:0C:42:05:AA:B0 disabled no
/int wire acc add auth yes forw yes int wlan1 mac=00:0C:42:05:AA:B0

#Adding the bridges
/int br add name br2 prot rstp pri 0xffff

#Adding interfaces to the bridges
/int br po add bridge br2 int ether2 path 10000
/int br po add bridge br2 int ether3 path 30000
/int br po add bridge br2 int wds-rt-rnet-01 path 40000

#Adding the VLAN interfaces
/int vlan add name br2-vl2 int br2 vlan 2 dis no
/int vlan add name br2-vl5 int br2 vlan 5 dis no
/int vlan add name br2-vl10 int br2 vlan 10 dis no

#Adding an mgmt IP
/ip addr add add 172.30.99.2/24 int br2-vl2

#Setup SNMP
/snmp set contact=noc@roamingnet.com enabled=yes location="Prag MuM 2009"
Configuration of SW-RNET-01

```
SW-RNET-01#sho conf
Using 2181 out of 32768 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW-RNET-01
!
enable secret 5 xxxxxxxxxxxxxxxxxxxxxxxxxxxx
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp mode transparent
!
spanning-tree mode mst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
vlan 2
   name mgmt
!
vlan 5
   name ISP-1
!
vlan 10
   name ISP-2
!
vlan 97
!
interface FastEthernet0/1
   switchport trunk allowed vlan 1,2,5,10
   switchport mode trunk
   spanning-tree cost 10000
!
interface FastEthernet0/2
   switchport trunk allowed vlan 2,5,10
   switchport mode trunk
   spanning-tree cost 10000
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
   switchport trunk allowed vlan 2,5,10
   switchport mode trunk
   spanning-tree cost 1000
!
interface GigabitEthernet0/2
   switchport trunk allowed vlan 1,2,5,10
   switchport mode trunk
!
interface Vlan1
   no ip address
   no ip route-cache
   shutdown
!
interface Vlan10
   no ip address
   no ip route-cache
   shutdown
!
interface Vlan12
   ip address 172.30.99.11 255.255.255.0
   no ip route-cache
!
interface Vlan15
   no ip address
   no ip route-cache
   shutdown
!
interface Vlan5
   no ip address
   no ip route-cache
   shutdown
!
interface Vlan2
   ip address 172.30.99.11 255.255.255.0
   no ip route-cache
!
interface Vlan5
   no ip address
   no ip route-cache
   shutdown
!
interface Vlan2
   ip address 172.30.99.11 255.255.255.0
   no ip route-cache
!
interface Vlan5
   no ip address
   no ip route-cache
   shutdown
!
interface Vlan2
   ip address 172.30.99.11 255.255.255.0
   no ip route-cache
!
interface Vlan5
   no ip address
   no ip route-cache
   shutdown
!
end
```
Configuration of SW-RNET-02

Startup configuration:

; J4812A Configuration Editor; Created on release #F.05.69

hostname "SW-RNET-02"
snmp-server contact "noc@roamingnet.com"
snmp-server location "Prag MuM 2009"
max-vlans 16
cdp run
snmp-server community "public" Unrestricted

VLAN 1
   name "DEFAULT_VLAN"
   forbid 1-2,13
   untagged 5-12,14
   no ip address
   no untagged 1-4,13
   exit
VLAN 2
   name "mgmt"
   ip address 172.30.99.12 255.255.255.0
   tagged 1-2,5-6,12-13
   exit
VLAN 5
   name "ISP-1"
   untagged 3-4
   tagged 1-2,5-6,12-13
   exit
VLAN 10
   name "ISP-2"
   tagged 1-2,5-6,12-13
   exit
management-vlan 2
no aaa port-access authenticator active
spanning-tree
spanning-tree priority 5
spanning-tree 13 path-cost 1000
spanning-tree 1-4 path-cost 10000
password manager
password operator
exit
Summary

- VLANs segments the broadcast domain.
- VLANs helps you secure the network.
- For VLAN in wireless networks, create WDS connections first, then layer on the VLAN!
- Spanning Tree can only be used on bridges with physical and WDS interfaces.
- Support for MST 802.1s (Multiple Spanning Tree) is a need if different pathcosts on physical and VLAN interfaces shall be used.
Thank You!

Paul Eriksson

Mobile: +46706210055
eMail: periksson@roamingnet.com
Fax: +46696129010
CV: http://www.linkedin.com/in/periksson