Extending VLANS through Several Broadcast Domains Inside Enterprise LAN

Eugene Prokhorenko
Institute for Informatics and Automation Problems of the National Academy of Sciences of the Republic of Armenia
Yerevan, Armenia
e-mail: eugene@sci.am

Mary Khachatryan
Institute for Informatics and Automation Problems of the National Academy of Sciences of the Republic of Armenia
Yerevan, Armenia
e-mail: mary@sci.am

ABSTRACT
Modern networks with scattered topology require deploying sophisticated routing rules in order to achieve network nodes reachability across multiple isolated broadcast domains.
Commonly used tunnel-based routing techniques suffer from MTU fragmentation and high CPU load.
An alternative VLAN-based solution is proposed in order to overcome limitations associated with L3-level routing.
Specifically, MikroTik implementation of hybrid VLANs technology is considered. The proposed approach is shown to be more efficient compared to commonly used L2TP, P2TP, GRE tunnels.
Using private IPs for extended VLAN simplifies the security management as only one subnet must be configured in firewalls.
Lastly, a case-study of ASNET-AM configuration for AM TLD is presented to provide dedicated channels to two definite upstream links implemented in practice is presented.

Keywords
Layer2, Layer3, Bridge, Hybrid Ports, VLAN, MikroTik.

1. BASIC CONCEPTS
Wildly using network equipment allows us to configure network interfaces both as a router interface (Layer 3) or as a switch interface (Layer 2). In this article it's shown how to get Layer 3 access from one location in the enterprise LAN to another physical location via several enterprise routers without creating tunnels. This can be done using VLAN technology, specifically hybrid VLANS [1]. This setup is shown to be more efficient then the commonly used L2TP, P2TP, GRE tunnels. The reason for efficiency is usage Layer 2 for playing with VLAN tags, not calculating routing information like in tunnel setup. VLAN extension setup is useful for monitoring equipment, for switch management. Using private IPs for extended VLAN gives us more security (only one subnet must be used for extended VLAN in firewalls). If Internet access for extended VLAN is needed, NAT must be configured on one of the routers, used in setup. It's clearly, that several extended VLANs can be configured at the same time.

2. APPLICATION IN ASNET-AM NETWORK
We are using two extended VLANs for providing proper Internet upstream links for AM TLD. ASNET network is built on MikroTik products (routers, switches) and extended VLANs are configured in RouterOS.
Inside large networks (enterprise scale) sometimes it's needed to configure subnet, consisted of two parts, physically located on different network edges, bounded by several routers (see Fig.1 We want to build one subnet from LAN1 and LAN2). Well-known tunnel technologies can be used for that. But in that case we must take into account MTU restrictions and possible packet fragmentation as a consequence. In case of MikroTik routers it's convenient to use VLANs for needed configuration. Here only 4 addition bytes are used. MikroTik RouterOS allows to combine all kinds of router ports into bridge, specifically VLAN interfaces [2]. We will use the so called hybrid VLAN configuration: on the same cable we will have both tagged and untagged frames.

For example, we configured two subnets on the router RT2:
ether1: 192.168.0.1/24 and ether2: 192.168.1.1/24
We want to allow VLAN traffic with VLAN ID 100 between ether1 and ether2 interfaces.
To accomplish this we create bridge "bridge1-vlan100" on router RT2 and add VLAN interfaces "vlan100-0" and "vlan100-1", configured on ether1 and ether2, accordingly. The same way we configure all other intermediate routers. On the first router RT1 we don't need VLAN interface on ether1, so we add to bridge ether1 itself.
On the last router we do the same with ether2 (see Fig 2).

In case of having switches between routers, we need to configure two trunk ports for VLAN ID 100 on each.

In general case it's possible to create several independent subnets on the existing cabling infrastructure, based on VLAN technology. This is very useful, for example, for creating service subnet for network monitoring devices, management network, tunneling specific traffic to the definite border router, etc.

Note, that VLAN traffic can be restricted by a simple queue or a queue tree.

Also it's another advantage, that VLAN traffic doesn't participate in routing process and this gives less CPU load, because bridging, described in this presentation is more efficient for CPU usage. Bridging is working on Layer 2 (L2) of OSI model and it's finding for each Ethernet frame bridge port, on which destination host resides. This is done by browsing MAC address table. Routing is working on Layer 3 (L3) of OSI model and it's finding for each IP packet routing network interface for sending packet to destination. This is done by browsing routing table (quite a large list of known network prefixes). That is at first Ethernet frame is processing on L2, then IP packet (it's part) going to L3, processed, then go back to L2 to become frame again and then sending to network [3].

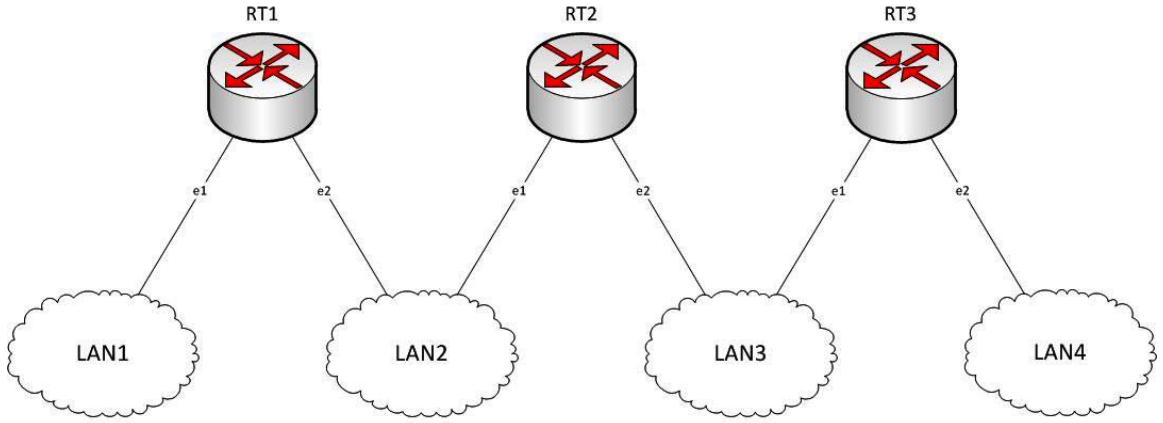

Fig.1. Initial Setup

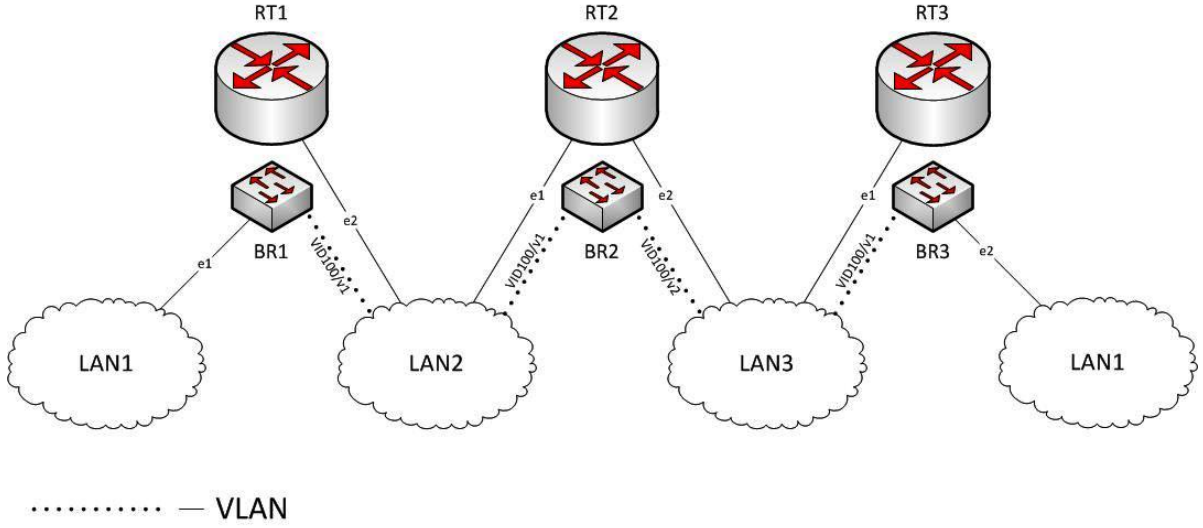

Fig.2. VLAN100 resides in two locations

3. ACTUAL ROUTEROS CONFIGURATION EXAMPLE

Router1 Setup

```
[admin@RT1] > interface vlan pr detail
Flags: X - disabled, R - running, S - slave
0 R     name="vlan100-to-RT2" mtu=1500l2mtu=1594
        mac-address=64:D1:54:8E:C8:70 arp=enabled
        arp-timeout=auto loop-protect=default
        loop-protect-status=off
        loop-protect-send-interval=5s
        loop-protect-disable-time=5m vlan-id=100
        interface=ether2-LAN2 use-service-tag=no
[admin@RT1] > interface bridge port pr detail
Flags: X - disabled, I - inactive, D - dynamic, H - hw-offload
 0      interface=vlan100-to-RT2 bridge=BR1
        priority=0x80 path-cost=10 internal-path-cost=10
        edge=auto point-to-point=auto external-fdb=auto
        horizon=none hw=yes auto-isolate=no
        restricted-role=no restricted-tcn=no
        pvid=1 frame-types=admit-all ingress-filtering=no
 1 I H  interface=ether1-LAN1 bridge=BR1 priority=0x80
        path-cost=10 internal-path-cost=10 edge=auto
        point-to-point=auto external-fdb=auto
        horizon=none hw=yes auto-isolate=no
        restricted-role=no restricted-tcn=no
        pvid=1 frame-types=admit-all ingress-filtering=no
```

Router2 Setup

```
[admin@RT2] > interface vlan pr detail
Flags: X - disabled, R - running, S - slave
 0      name="vlan100-from-RT1"mtu=1500 l2mtu=1594
        mac-address=64:D1:54:8E:C8:6F arp=enabled
        arp-timeout=auto loop-protect=default
        loop-protect-status=off
        loop-protect-send-interval=5s
        loop-protect-disable-time=5m vlan-id=100
        interface=ether1-LAN2 use-service-tag=no
 1 R    name="vlan100-to-RT3" mtu=1500 l2mtu=1594
        mac-address=64:D1:54:8E:C8:70 arp=enabled
        arp-timeout=auto loop-protect=default
        loop-protect-status=off
        loop-protect-send-interval=5s
        loop-protect-disable-time=5m vlan-id=100
        interface=ether2-LAN3 use-service-tag=no
[admin@RT2] > interface bridge port pr detail
Flags: X - disabled, I - inactive, D - dynamic, H - hw-offload
 0      interface=vlan100-to-RT3 bridge=BR2
        priority=0x80 path-cost=10 internal-path-cost=10
        edge=auto point-to-point=auto external-fdb=auto
        horizon=none hw=yes auto-isolate=no
        restricted-role=no restricted-tcn=no pvid=1
        frame-types=admit-all ingress-filtering=no
 1 I    interface=vlan100-from-RT1 bridge=BR2
        priority=0x80 path-cost=10 internal-path-cost=10
```

edge=auto point-to-point=auto external-fdb=auto horizon=none hw=yes auto-isolate=no restricted-role=no restricted-tcn=no pvid=1 frame-types=admit-all ingress-filtering=no

Router3 Setup

```
[admin@RT3] > interface vlan print detail
Flags: X - disabled, R - running, S - slave
 0          name="vlan100-from-RT2"mtu=1500 l2mtu=1594
            mac-address=64:D1:54:8E:C8:6F arp=enabled
            arp-timeout=auto loop-protect=default
            loop-protect-status=off
            loop-protect-send-interval=5s
            loop-protect-disable-time=5m vlan-id=100
            interface=ether1-LAN3 use-service-tag=no
[admin@RT3] > interface bridge port pr detail
Flags: X - disabled, I - inactive, D - dynamic, H - hw-offload
 0          interface=vlan100-from-RT2 bridge=BR3
            priority=0x80 path-cost=10 internal-path-cost=10
            edge=auto point-to-point=auto external-fdb=auto
            horizon=none hw=yes auto-isolate=no
            restricted-role=no restricted-tcn=no
            pvid=1 frame-types=admit-all ingress-filtering=no
 1 I H      interface=ether2-LAN1 bridge=BR3 priority=0x80
            path-cost=10 internal-path-cost=10 edge=auto
            point-to-point=auto external-fdb=auto
            horizon=none hw=yes auto-isolate=no
            restricted-role=no restricted-tcn=no
            pvid=1 frame-types=admit-all ingress-filtering=no
```

REFERENCES

[1] MikroTik provides hardware and software for Internet connectivity, https://wiki.mikrotik.com/wiki/Manual:CRS1xx/2xx_series_switches_examples

[2] MikroTik provides hardware and software for Internet connectivity, https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge

[3] E. Prokhorenko, M. Khachatryan, "ASNET-AM Experience in Implementation of Hybrid VLANs for Customers Links", *Proceedings of the Conference CSIT-2017*, pp. 405-406, Yerevan, 25-29.09.2017.