Working With VLANs and Uplink Tagging

Tim Preston, Haven IT Consulting

1. Introduction

This article presents examples of two configurations that may be implemented in special circumstances when **large** WaveRider LMS4000 / LMS8000 system(s) are used in switched or through-only modes. These special circumstances may include the need to:

- reduce the number of routers or router ports in multi-CAP (**c**ommunication **a**ccess **p**oint), multi-sector systems required to break up broadcast domains.
- provide multiple operator support (a.k.a. “open access”).
- provision a separate backhaul.

As the size of a network and the number of users on the network increases, the overhead related to a flat IP network, such as broadcast traffic, becomes a significant fraction of the available bandwidth. Traditionally, the IP network is physically divided into multiple layer 2 broadcast domains (and corresponding IP subnets) connected together by IP routers. However, IP routers are expensive, as is physical separation of traffic, especially on long backhauls. Port-based VLANs offer a method to logically, rather than physically, divide a network using layer 2 switches and a VLAN aware router. Effectively, each VLAN becomes a virtual router port.

The “Port-Based VLANs” example increases the number of broadcast domains while restricting their size, resulting in increased bandwidth and enhanced security. A VLAN capable layer-2 switch (ie. Cisco 2900XL) is used to effectively separate layer-2 traffic at the CCU (**C**AP **c**hannel **u**nit) attached switch ports. No VLAN configuration is required on any LMS device.

The “WAN Segmentation Using Uplink VLAN Tagging” example allows for open access for multiple operators and segregates traffic from different CPEs (**c**ustomer **p**remises **e**quipment) in the backhaul network by appending 802.1q VLAN tags to upstream frames at the specially configured EUM (**e**nd **u**ser **m**odem) and/or MMT (mobile nomadic terminal). Each CCU attached switch port is configured as a trunk to receive or transmit frames tagged with different VLAN IDs. Virtual routing and forwarding (VRF) is used to maintain the flat IP network on the LMS side and to separate traffic at the backhauls. No configuration change on the CCU is required.

Special attention should be given to the mode in which the CCU(s) will operate. In switched mode, radio links between EUMs / MMTs and the CCU to which they are registered are *not* VLAN segmented. That is, broadcasts sent from one EUM / MMT or attached subscriber PC will be received by another EUM / MMT and subscriber PC residing on the same CCU, regardless of switch, router, or EUM / MMT VLAN configuration.

In through-only mode, these same broadcasts are received by the CCU radio and forced out the CCU Ethernet port. Broadcasts are therefore not received by any other EUM/MMT or subscriber. Subscriber to subscriber communication is disabled unless special provision is made on the upstream router or multilayer switch.

All configuration command syntaxes apply to CCUs (models 3100 and 8000), EUMs (models 3005, 3006 and 8000) and MMT 9000s. Both early and late model Cisco devices are demonstrated. All Cisco devices are running Cisco IOS.

For both examples, the IP addressing scheme, as well as the physical location of network segments, devices and server systems are meant as guides only. In most cases, customization will be necessary.

PORT-BASED VLANS

This example segments what would normally be one large broadcast domain into four (4) smaller broadcast domains on the backbone switch, thus improving performance and enhancing security between CAPs. Routing between VLANs is controlled by the VLAN capable router (e.g. Cisco 2621). Since VLAN membership is defined at a particular CCU attached switch port, all devices placed downstream from the port effectively become members of the same VLAN, ergo, broadcast domain.

Aside from requiring the CCU to be operating in switched or through-only mode, no special LMS configuration is required. Furthermore, no LMS device, subscriber PC or server system needs to be 'VLAN aware'. All VLAN related configuration is provided and supported by the VLAN capable switch and router.

EXAMPLE TOPOLOGY OVERVIEW

As shown in Figure 1 below, each CCU is directly attached to one 2900XL switch port. Switch ports are configured in access mode, meaning each is assigned to one (1) VLAN only, effectively becoming a 'member' of that specific VLAN (10, 20 or 30 in this case). All downstream devices including the CCU, EUMs and customer premises equipment (CPE), are also considered members in the respective VLAN.

The 'server farm' network segment is also attached to its own 2900XL switch port (Fa 0/4). It is assigned to VLAN 40, and thus becomes a 'member' of VLAN 40. This segment's layer 2 device can be any managed or non-managed switch or hub. The server systems and the hub or switch to which they are attached are also considered to be members of VLAN 40. It is assumed the NMS (**n**etwork **m**anagement **s**ystem) will operate from this segment. (It should be noted that the server farm could also be placed in its own subnet, attached to a third router interface.)

The 2900XL Fa 0/24 interface's switch port mode is configured as a trunk to allow frames tagged with multiple VLAN IDs (from the 2621) to be adjudicated and passed to the appropriate VLAN member switch port, which then strips the tag, and then sends the traffic (egress) on to the LMS device, CPE or server system.

The Fa 0/1 interface on the 2621 router is configured with four (4) sub-interfaces, each with two (2) IP addresses, one subnet for the subscriber PCs, the other for management purposes. These IP addresses will be used as gateways for the appropriate VLAN member devices. Each of these sub-interfaces is configured to encapsulate (using 802.1q) each frame with the appropriate VLAN ID corresponding to the destination subnet. The actual physical interface's IP address is used to access and manage the router itself.

If desired, EUMs and CPE VLAN members may be configured to use DHCP; however, in order to resolve the correct IP subnet, DHCP relay will need to be configured either on the CCU(s) *or* the 2621's sub-interfaces. Special CCU and DHCP server configuration may be needed, such as DHCP relay agent information option 82, if CPEs are on a different IP subnet than the CCU, as shown. Also, if available, public IP addresses may be used for PCs instead of the private class C addresses used in the example.

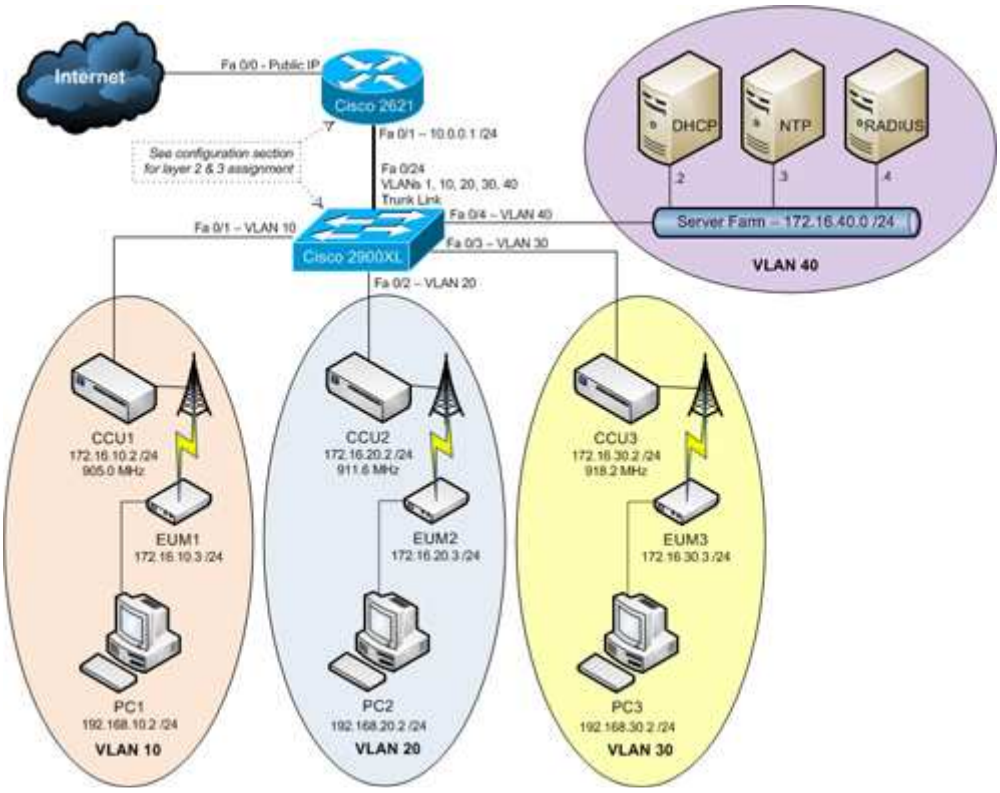

Figure 1: Port-Based VLANs

WAN SEGMENTATION USING UPLINK VLAN TAGGING

In some applications, such as open access, where multiple groups of subscribers share a common infrastructure, it is useful to separate different users' traffic into different streams at the backhaul or network access point. This can be done using separate IP subnets; but in some cases finer granularity may be desired. In this case, traffic from individual EUMs can be labeled with a VLAN ID, which can be used in the switching network to direct the traffic to the appropriate backhaul or network access.

All three (3) of the parameters detailed in the table below may be manually configured or assigned dynamically using RADIUS.

Attribute	Vendor-Type	Vendor-Length	Value
WaveRider-Uplink-VLAN-ID	20	6	The Value field is four octets. Valid VLAN IDs are 0 to 4094. Any other value will disable tagging.
WaveRider-Uplink-VLAN-Priority	21	6	The Value field is four octets. Valid values are 0 to 7. Other values are ignored.
WaveRider-Downlink-VLAN-Strip	22	6	The Value field is four octets. Valid values are 0 (false) and 1 (true). Other values are ignored.

Table 1: EUM Uplink VLAN Tagging RADIUS Attribute Details

EXAMPLE TOPOLOGY OVERVIEW

Uplink VLAN tagging is enabled on the MMT, consisting of a VLAN ID and a priority. The tag is appended to all upstream frames transmitted from or through the MMT (see note below). The EUM does not require VLAN tagging configuration as it will be part of the native, or untagged, segmented network (SN). Since it is possible for the CCU attached switch port to receive frames tagged with multiple VLAN IDs (if, for example, further segmentation is required), it must be configured as a trunk. This results in frames egressing from this switch port to be tagged with the appropriate VLAN ID (or not tagged at all). Therefore, downlink tag stripping is enabled on the MMT to allow non-VLAN aware hosts (e.g. subscriber PCs and/or SOHO routers) to communicate as required with the rest of the network.

EUMs, MMTs and CCUs strip VLAN tags on packets addressed directly to them, so communication between EUMs, MMTs and CCUs or other EUMs or MMTs (but not hosts on other EUMs or MMTs) is not affected.

Upstream traffic is divided based on VRF (virtual routing and forwarding) membership, assigned at the SVIs (switch virtual interfaces) and physical interfaces (in this case, SVI VLAN1, SVI VLAN100, Fa1/0/2 and Fa1/0/3). Note that the flat IP network on the LMS side is maintained by using VRF to allow two separate routing tables to coexist at the NAP (network access point); in this case, the Cisco 3750. The CPE devices' IP gateways are therefore configured based on the SVI for which WAN traffic should be directed. Given the nature of layer-2 segmentation, it is recommended that each virtual network operate its own NMS for providing network services such as DHCP and SNMP, as well as administrative functions such as LMS device telnet access and software upgrading. For example, referencing Figure 2 below, SNMP on 'NMS: SN-A' can be used to monitor all 'SN-A' LMS devices, but not 'SN-B' LMS devices. See section 2.2.3, 'Network Service and Management Considerations' below.

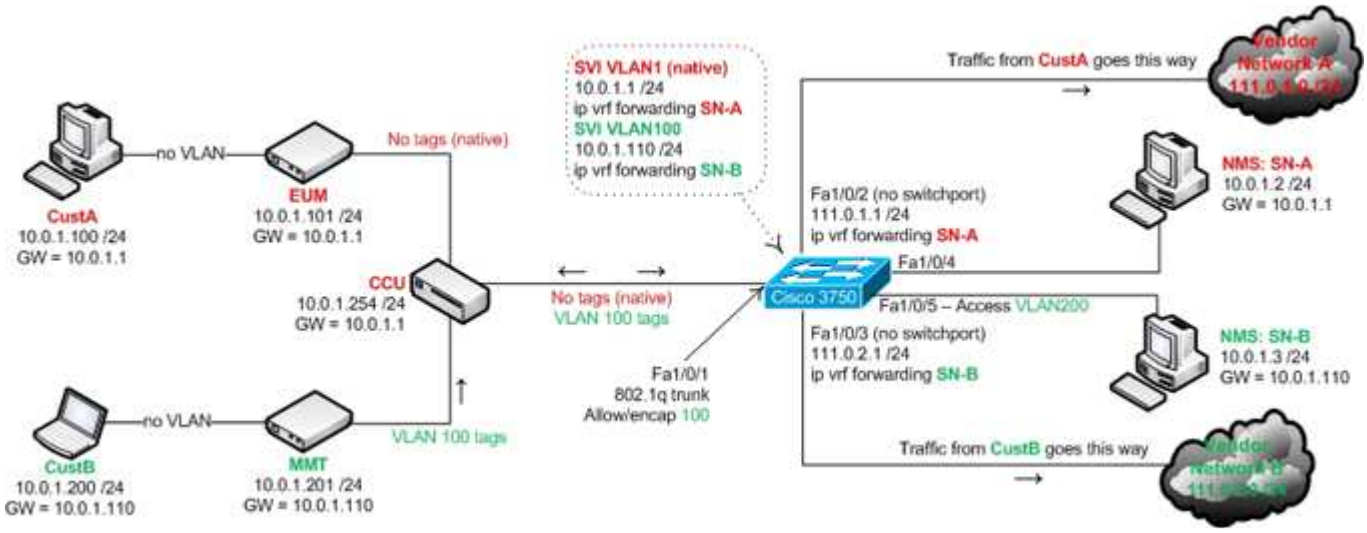

Figure 2: WAN Segmentation Using Uplink VLAN Tagging

2. CONFIGURATION EXAMPLES

To support either example, CCUs and EUMs / MMTs must be running at least the following versions:

LMS Device	Model #	Software Version
CCU	3100	20.6
	8000	40.4
EUM	3005	11.4
	3006	
	8000	30.4
MMT	9000	11.4

Table 2: Supported Software Versions

The configuration examples detailed in this document were not designed or intended for use in every WaveRider deployment. It is understood that systems and/or network administrators customize the examples to best suit the topology and needs of their own deployment requirements. It is highly recommended that the operator following these examples possesses a solid understanding of network switching and routing fundamentals, as well as Cisco devices, in order to take the necessary precautions towards securing the configured system.

PORT-BASED VLANS

Referencing the diagram in Figure 1 above, configure the Cisco router(s) and switch(es) as follows.

Cisco Catalyst 2900XL Switch

i. Set the IP address and default gateway for VLAN1, the management VLAN:

2900XL#**configure terminal**
2900XL(config)#**int vlan 1**
2900XL(config-if)#**ip address 10.0.0.2 255.255.255.0**
2900XL(config-if)#**exit**
2900XL(config)#**ip default-gateway 10.0.0.1**
2900XL(config)#**end**

ii. Set the VTP mode depending on your network (example uses the VTP transparent). Create VLAN10, VLAN20, VLAN30 and VLAN40:

2900XL#**vlan database**
2900XL(vlan)#**vtp transparent**
2900XL(vlan)#**vlan 10**
2900XL(vlan)#**vlan 20**
2900XL(vlan)#**vlan 30**
2900XL9vlan)#**vlan 40**
2900XL(vlan)#**exit**

iii. Enable trunking on FastEthernet 0/24. Also, configure the encapsulation type to 802.1Q:

2900XL#**configure terminal**
2900XL#**int f0/24**
2900XL(config-if)#**switchport mode trunk**
2900XL(config-if)#**switchport trunk encapsulation dot1q**
2900XL(config-if)#**switchport trunk allowed vlan all**

iv. Assign the individual interfaces to their corresponding VLANs:

2900XL(config-if)#**interface f0/1**
2900XL(config-if)#**switchport access vlan 10**
2900XL(config-if)#**end**

v. Save the configuration:

2900XL#**copy run start**

Repeat the configuration steps above to assign Fa 0/2 to VLAN 20, Fa 0/3 to VLAN 30, and Fa 0/4 to VLAN 40. It is assumed that Fa 0/24 is already a member of the native VLAN, VLAN 1. If not, change the VLAN membership for this interface to include VLAN1.

Cisco 2621 Router

Router configuration for 802.1q depends on Cisco IOS version. The following example is valid for IOS versions later than 12.1(3) T.

i. Enable IP routing:

2621#**config terminal**
2621(config)#**ip routing**

ii. Configure the IP address for Fa 0/1 and activate the interface. (Note that the IP address for VLAN 1 is configured on the main interface and no encapsulation should be defined for VLAN 1 under the sub-interface.)

2621(config)#**interface f0/1**
2621(config-if)#**no shut**
2621(config-if)#**ip address 10.0.0.1 255.255.255.0**

iii. Configure 802.1Q encapsulation for VLAN 10 on sub-interface f0/1.1 for subnet 192.168.10.0/24. Create the secondary IP address for the 172.16.10.0/24 subnet:

2621(config-if)#**interface f0/1.1**
2621(config-if)#**encapsulation dot1q 10**
2621(config-if)#**ip address 192.168.10.1 255.255.255.0**
2621(config-if)#**ip address 172.16.10.1 255.255.255.0 secondary**

iv. Configure 802.1Q encapsulation for VLAN 20 on sub-interface f0/1.2 for subnet 192.168.20.0/24. Create the secondary IP address for the 172.16.20.0/24 subnet:

2621(config-if)#**interface f0/1.2**
2621(config-if)#**encapsulation dot1q 20**
2621(config-if)#**ip address 192.168.20.1 255.255.255.0**
2621(config-if)#**ip address 172.16.20.1 255.255.255.0 secondary**

v. Configure 802.1Q encapsulation for VLAN 30 on sub-interface f0/1.3 for subnet 192.168.30.0/24. Create the secondary IP address for the 172.16.30.0/24 subnet:

2621(config-if)#**interface f0/1.3**
2621(config-if)#**encapsulation dot1q 30**
2621(config-if)#**ip address 192.168.30.1 255.255.255.0**
2621(config-if)#**ip address 172.16.30.1 255.255.255.0 secondary**

vi. Configure 802.1Q encapsulation for VLAN 40 on sub-interface f0/1.4 for subnet 192.168.40.0/24:

2621(config-if)#**interface f0/1.4**
2621(config-if)#**encapsulation dot1q 40**
2621(config-if)#**ip address 192.168.40.1 255.255.255.0**
2621(config-if)#**end**

vii. Save the configuration:

2621#**copy run start**

WAN Segmentation using VLAN Tagging

Referencing the diagram in Figure 2 above, configure the EUM, MMT and Cisco Catalyst 3750 multilayer switch as follows.

EUM and MMT VLAN command configuration changes take effect immediately and do not require a reboot. However, changing the IP address *does* require a reboot.

EUMS / MMTS

i. Configure the EUM's IP address and gateway:

EUM>**ip e 10.0.1.101 24**
IP Address: 10.0.1.101 / 24
IP Subnet : 10.0.1.0 (255.255.255.0)
EUM>**ip g 10.0.1.1**
Gateway Route changed
Gateway IP Address: 10.0.1.1

ii. Save the configuration and restart the EUM:

EUM>**save**
Basic Config saved
Port Filter Config saved
EUM>**res**

iii. Configure the MMT's IP address and gateway:

MMT>**ip e 10.0.1.201 24**
IP Address: 10.0.1.201 / 24
IP Subnet : 10.0.1.0 (255.255.255.0)
MMT>**ip g 10.0.1.110**
Gateway Route changed
Gateway IP Address: 10.0.1.110

iv. Configure uplink VLAN tagging; ID = 100, priority = 3:

MMT>**vlan up en 100 3**
[NOTE: The above command will affect communication with non-VLAN-aware hosts and hosts not on this VLAN.]
Uplink VLAN Tag Insertion Enabled - ID: 100, Priority: 3
Downlink VLAN Tag Removal Disabled

v. Configure downlink VLAN tag stripping:

MMT>**vlan down strip**
Uplink VLAN Tag Insertion Enabled - ID: 100, Priority: 3
Downlink VLAN Tag Removal Enabled

vi. Save the configuration and restart the MMT:

MMT>**save**
Basic Config saved
Port Filter Config saved
MMT>**res**

The above EUM / MMT configuration may be performed dynamically using RADIUS (for VLAN attributes) and DHCP (for IP address assignment). See section 2.2.3 below.

Cisco Catalyst 3750 Switch

i. Enable IP routing:

3750#**conf t**
3750(config)#**ip routing**

ii. Enable distributed Cisco Express Forwarding (CEF):

3750(config)#**ip cef distributed**

iii. Create the 'SN-A' VRF and 'SN-B' VRF instances:

3750(config)#**ip vrf SN-A**
3750(config-vrf)#**rd 10.0.1.1:1**
3750(config-vrf)#**ip vrf SN-B**
3750(config-vrf)#**rd 10.0.1.110:100**

iv. Configure VLAN 1's VRF and IP address. This switch virtual interface will act as the gateway for the 'SN-A' segmented devices:

3750(config-vrf)#**int vlan 1**
3750(config-if)#**ip vrf forwarding SN-A**
3750(config-if)#**ip add 10.0.1.1 255.255.255.0**

v. Configure VLAN 100's VRF and IP address. This switch virtual interface will act as the gateway for the 'SN-B' segmented devices:

3750(config-if)#**int vlan 100**
3750(config-if)#**ip vrf forwarding SN-B**
3750(config-if)#**ip add 10.0.1.110 255.255.255.0**

vi. Configure CCU attached Fa 1/0/1 interface's mode, encapsulation type and allowed VLAN IDs:

3750(config-if)#**int f1/0/1**
3750(config-if)#**desc CCU**
3750(config-if)#**switchport trunk encap dot1q**
3750(config-if)#**switchport mode trunk**
3750(config-if)#**switchport trunk allow vlan add 1,100**

vii. Configure vendor network A's Fa 1/0/2's VRF and IP address:

3750(config-if)#**int f1/0/2**
3750(config-if)#**no switchport**
3750(config-if)#**description Connection to vendor network** A
3750(config-if)#**ip vrf SN-A**
3750(config-if)#**ip address 111.0.1.1 255.255.255.0**

viii. Configure vendor network B's Fa 1/0/3 VRF and IP address:

3750(config-if)#**int f1/0/3**
3750(config-if)#**no switchport**
3750(config-if)#**description Connection to vendor network B**
3750(config-if)#**ip vrf SN-B**
3750(config-if)#**ip address 111.0.2.1 255.255.255.0**

ix. Save the configuration:

3750(config-if)#**end**
3750#**copy run start**

3. NETWORK SERVICE AND MANAGEMENT CONSIDERATIONS

Using the topology in Figure 2 as reference, DHCP, SNMP, NTP and RADIUS support considerations for the LMS network are addressed below.

i. **DHCP:** verify DHCP relay is disabled on the CCU(s). This guards against incorrect source network identification by the DHCP server. Instead, locate a DHCP server on each segmented network (assign the appropriate switch port's VLAN access) to assign IP leases to the CPE devices accordingly. Using Figure 2 as an example, the DHCP pool's range on 'NMS: SN-A' may be 10.0.1.5 to 10.0.1.109, and the DHCP pool range on 'NMS: SN-B' may be 10.0.1.111 to 10.0.1.253.

If DHCP relay is required in order to protect against rogue DHCP servers, a combination of relay agent information option (82), EUM IDs and VLAN IDs could be used to distinguish CPE address pool assignment on a central DHCP server. Due to complexity and environment-specific variables, the configuration of such a solution is beyond the scope of this document.

ii. **RADIUS:** configure RADIUS authorization on the CCU(s) as usual. The RADIUS server must be placed in the native (ie. untagged) segmented network.

iii. **SNMP:** Two possibilities exist. 1) Since it is not recommended that SNMP be used to monitor individual EUMs or MMTs, one SNMP server can be located in the native (ie. untagged) segmented network to monitor the CCU(s). 2) If EUM and/or MMT monitoring is absolutely necessary, locate an SNMP system on each segmented network and configure monitoring of devices accordingly.

iv. **NTP:** If providing synchronization locally, locate the time server on the native (ie. untagged) segmented network. Add either the local or public (ie. Stratum 2) time server's IP address to the CCU(s) and enable time relay as usual.

v. **LMS device management:** Two possibilities exist. 1) Each vendor can manage their own LMS devices from their own segmented networks. 2) One computer system may be used to perform these same functions on the entire LMS network, providing the operator manually changes, as necessary, the attached switch port's VLAN membership to coincide with the segmented network containing the devices he or she wishes to manage.

http://www.haven-it.com