MERU NETWORKS®

WINS™: Wireless Interoperability & Network Solutions

Virtual Local Area Network (VLAN) Deployment Guide 1.2

MERU NETWORKS
WINS PARTNER
WIRELESS INTEROPERABILITY
& NETWORK SOLUTIONS

MERUNETWORKS.COM

Overview 3
VLAN Configuration 3
Dual-Ethernet Capability 7
Switch Configuration and Setup 8
Summary 10

Version 1.2, December 17, 2010

Overview

A Virtual Local Area Network (VLAN) is a broadcast domain that can span across wired or wireless LAN segments. Each VLAN is a separate logical network. Several VLANs can co-exist within any given network, logically segmenting traffic by organization or function. In this way, all systems used by a given organization can be interconnected independent of physical location. This has the benefit of limiting the broadcast domain and increasing security.

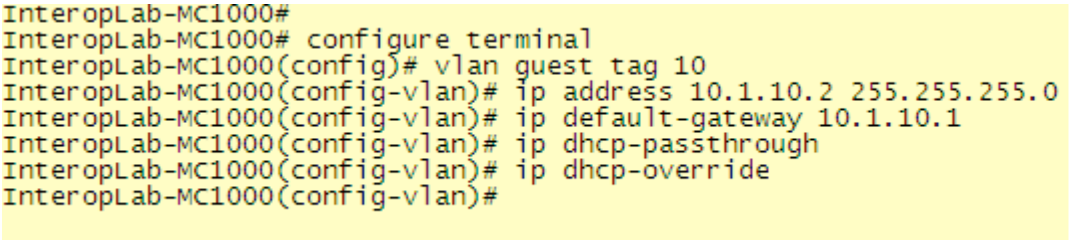
VLANs can be configured in software, which enhances their flexibility. VLANs operate at the data link layer (OSI Layer 2), however, they are often configured to map directly to an IP network, or subnet, at the network layer (OSI Layer 3).

IEEE 802.1Q is the predominant protocol used to “tag” traffic with a VLAN identifier. VLAN1 is called the default or native VLAN. It cannot be deleted, and all traffic on it is untagged. A trunk port is a network connection that aggregates multiple VLANs or tags, and is typically used between two switches or between a switch and a router. VLAN membership can be port-based, MAC-based, protocol-based, or authentication-based when used in conjunction with the 802.1x protocol.

Used in conjunction with multiple ESSIDs, VLANs support multiple wireless networks on a single Access Point using either a one-to-one mapping of ESSID to VLAN, or mapping multiple ESSIDs to one VLAN. By assigning a security profile to a VLAN, the security requirements can be fine-tuned based on the use of the VLAN, providing wire-like security or better on a wireless network.

VLAN Configuration

The Meru VLAN configuration is applied at the Controller. In order to map an ESSID to a VLAN, the VLAN must first be configured as follows:



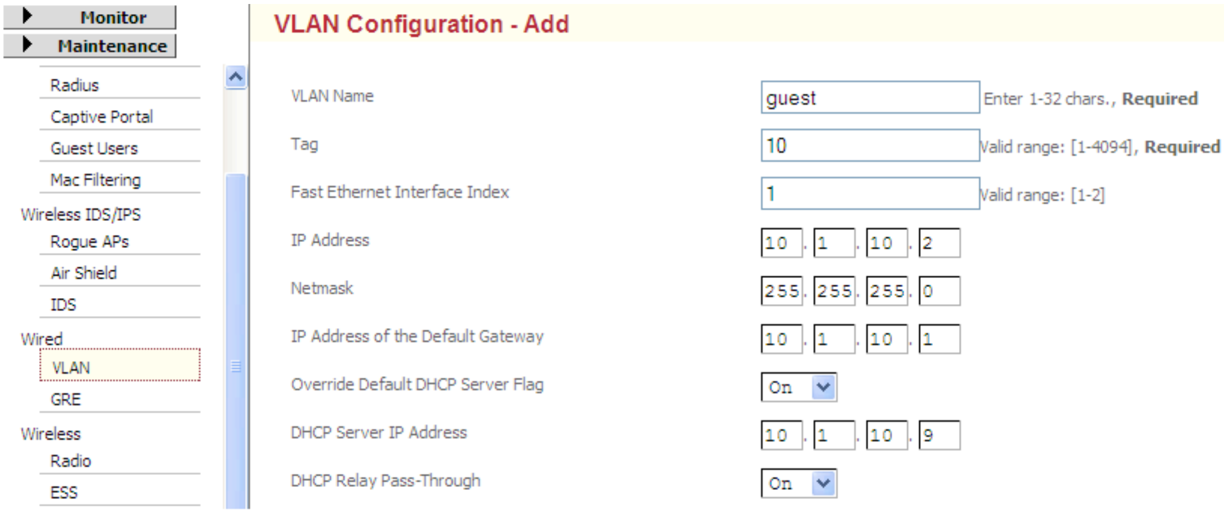
```
InteropLab-MC1000#
InteropLab-MC1000# configure terminal
InteropLab-MC1000(config)# vlan guest tag 10
InteropLab-MC1000(config-vlan)# ip address 10.1.10.2 255.255.255.0
InteropLab-MC1000(config-vlan)# ip default-gateway 10.1.10.1
InteropLab-MC1000(config-vlan)# ip dhcp-passthrough
InteropLab-MC1000(config-vlan)# ip dhcp-override
InteropLab-MC1000(config-vlan)#
```

VLAN Configuration using CLI

The Controller’s IP configuration for the new VLAN is required together with the default gateway for that VLAN. The default gateway is also configured on the router or Layer 3 switch for each VLAN interface, and it is this gateway that clients will use for traffic destined to pass outside of the local logical network.

The *ip dhcp-passthrough* command is enabled by default, and allows DHCP packets to pass through the Controller without modification, i.e., bridged to the server. This configuration eliminates the need for a DHCP relay in most cases, but may require the use of a helper IP address for DHCP on the Layer 3 device (see next section). Alternately, a DHCP server IP address can be configured for each VLAN with the command “*ip dhcp server ip-address”*. When specified for each VLAN, this overrides the Controller-assigned DHCP server configuration. The same can be configured via GUI as follows:

Note: This guide assumes that the user is familiar with configuring Meru Networks Controller. If further information is required for configuring the Controller, refer to the Meru Networks System Director Configuration Guide.



VLAN Configuration - Add

VLAN Name	guest	Enter 1-32 chars., **Required**
Tag	10	Valid range: [1-4094], **Required**
Fast Ethernet Interface Index	1	Valid range: [1-2]
IP Address	10 . 1 . 10 . 2	
Netmask	255 . 255 . 255 . 0	
IP Address of the Default Gateway	10 . 1 . 10 . 1	
Override Default DHCP Server Flag	On	
DHCP Server IP Address	10 . 1 . 10 . 9	
DHCP Relay Pass-Through	On	

VLAN Configugiration using WEB UI

1. Select the VLAN menu from the left pane and click on the **Add** button at the bottom of the page.
2. Enter any preferred **VLAN Name** up to 32 alphanumeric characters long without spaces, in this example guest is used as VLAN name.
3. In the Tag box, type the VLAN tag. The VLAN tag is an integer from 1 to 4,094. You must specify a VLAN tag; in this example 10 is used as VLAN tag.
4. In the Fast Ethernet Interface index type in 1. The second interface is an optional configuration.
5. In the IP address default gateway field, specify the gateway the controller should use to forward packets from wireless stations using this VLAN. The Default Gateway IP address should match the default gateway IP address configured (via either DHCP or statically) on wireless stations using this VLAN. In this example, 10.1.10.2 is used.
6. Enter the Subnet mask in the Netmask field. This should match subnet mask of the default gateway configured in Wireless clients. In this example, 255.255.255.0 is used.
7. Enter the Default Gateway address. This IP address is the default gateway used by the controller to route traffic from clients using this VLAN. In this example 10.1.10.1 is used.
8. Now select the "Override Default DHCP Server Flag" from the dropdown menu. In this example ON is used as the Flag.

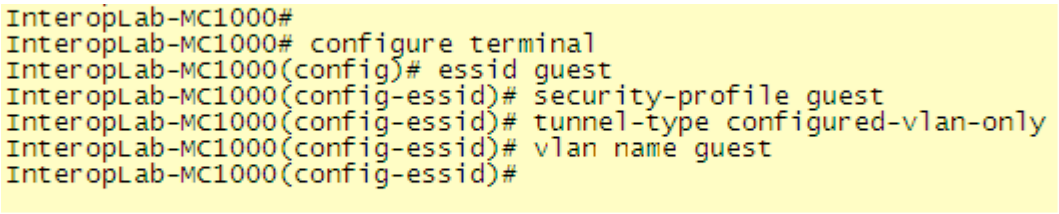
   - **ON** – Enable the use of DHCP server rather than the Global DHCP server configured for the controller.
   - **OFF** - Disable usage of specified DHCP server and return to using global DHCP server configured for the controller.

9. Enter the DHCP server IP address. In this example 10.1.10.9 is used.
10. Now select the "DHCP Relay Pass-Through from the drop down menu

    - **ON** – This is the default feature which enables the use of DHCP pass-through feature.
    - **OFF** - Disable usage of the pass-through DHCP server feature.

Once the required VLANs are configured on the Controller, the ESSID mapping can occur. An ESSID can map to one configured VLAN, or the VLAN information can be provided by a RADIUS server, i.e., for 802.1x configurations. When the RADIUS configuration is used, the "Access Accept" packet comes from the RADIUS server to the Controller, and the VLAN for that STA is updated in the Controller's VLAN table.

Multiple ESSIDs can be mapped to the same VLAN or to different VLANs. The configuration mapping an ESSID to a configured VLAN is as follows:

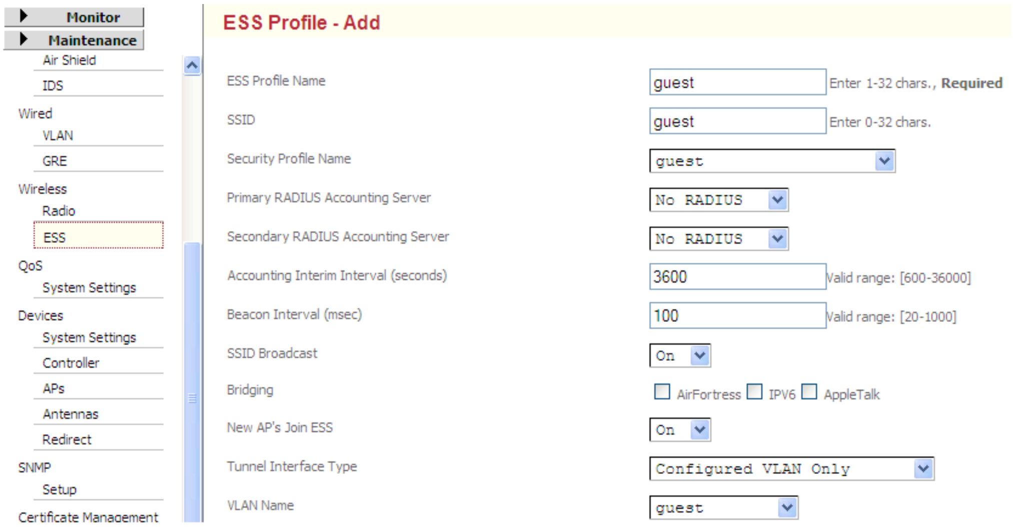


```
InteropLab-MC1000#
InteropLab-MC1000# configure terminal
InteropLab-MC1000(config)# essid guest
InteropLab-MC1000(config-essid)# security-profile guest
InteropLab-MC1000(config-essid)# tunnel-type configured-vlan-only
InteropLab-MC1000(config-essid)# vlan name guest
InteropLab-MC1000(config-essid)#
```

Assigning the VLAN to the ESSID using CLI

The VLAN can also be assigned to the ESSID using the WEB UI as follows:

11. On the configuration tab on the left pane select the ESS option.
12. Click on the **Add** button on the main window.



ESS Profile - Add

ESS Profile Name	guest	Enter 1-32 chars., **Required**
SSID	guest	Enter 0-32 chars.
Security Profile Name	guest	
Primary RADIUS Accounting Server	No RADIUS	
Secondary RADIUS Accounting Server	No RADIUS	
Accounting Interim Interval (seconds)	3600	Valid range: [600-36000]
Beacon Interval (msec)	100	Valid range: [20-1000]
SSID Broadcast	On	
Bridging	□ AirFortress □ IPV6 □ AppleTalk	
New AP's Join ESS	On	
Tunnel Interface Type	Configured VLAN Only	
VLAN Name	guest	

Configuring VLAN to ESS Profile

13. Fill the required ESS profile name with the required name followed by the SSID, In this example guest is used.
14. In the Security Profile dropdown menu, select the Security Profile that has to associate with the ESS profile. By default, an ESS profile is associated with the Security Profile named "*default".* In this example "guest" security profile is selected.
15. In the Tunnel Interface dropdown menu, select one. The options are outlined below. In this example Configured VLAN Only option is used.

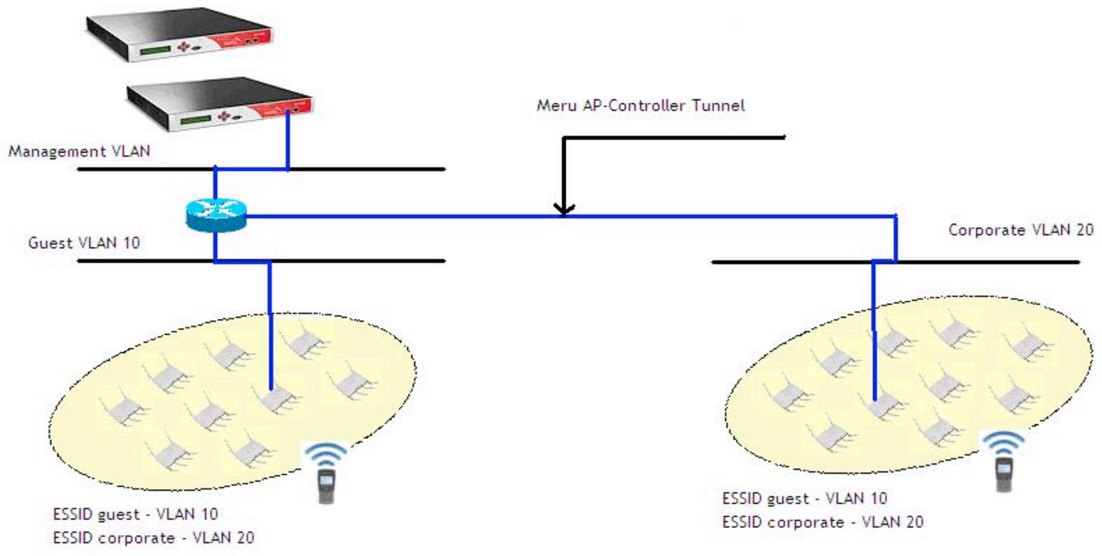
- **No Tunnel**: Specifies that no tunnel is associated with this ESS profile.
- **Configured VLAN Only**: Specifies that only a configured VLAN, listed in the following VLAN Name list, is associated with this ESS profile. If you select this option, go to step 16.
- **RADIUS VLAN Only**: Specifies that only the Radius VLAN is associated with this ESS profile.
- **RADIUS and Configured VLAN**: Specifies that both a configured VLAN and RADIUS VLAN are associated with this ESS profile.
- **GRE**: Specifies a GRE Tunnel configuration.

16. In the VLAN Name drop down menu select one of the existing VLANs that was created and to associate with this ESS profile. This option is used if Configured VLAN only option is selected for Tunneled interface type. In this example guest VLAN is associated with this ESS profile

Note: In this example RADIUS configuration is not used. Refer the Meru Networks System Director Configuration Guide for further information on the RADIUS configuration.

A typical Meru Virtual Cell network has the controllers on separate management VLAN. The access points can be located on the same or different subnet as the controllers. A Layer 3 router segments traffic between different wired subnets that are associated with different VLANs.

ESSIDs are configured to support each desired VLAN. Each contain a configured security profile.



VLAN Configured Network

The Meru controller typically has its management IP address and interface on the native or default VLAN (VLAN 1). Management traffic is therefore untagged as it traverses the wired network. While the access point may be connected to a distinct subnet from the controller, the switch port to which the access point is connected should remain as an access or untagged port.

No trunking is necessary on the switch port connected to the access point because all of the traffic between the Meru controller and the access point traverses the Meru tunnel. The access point will receive the tunneled traffic from the controller and map it to the corresponding ESSID and VLAN on the wireless network. In this way, multiple ESSIDs and VLANs are tunneled to the access point and supported on the wireless side.

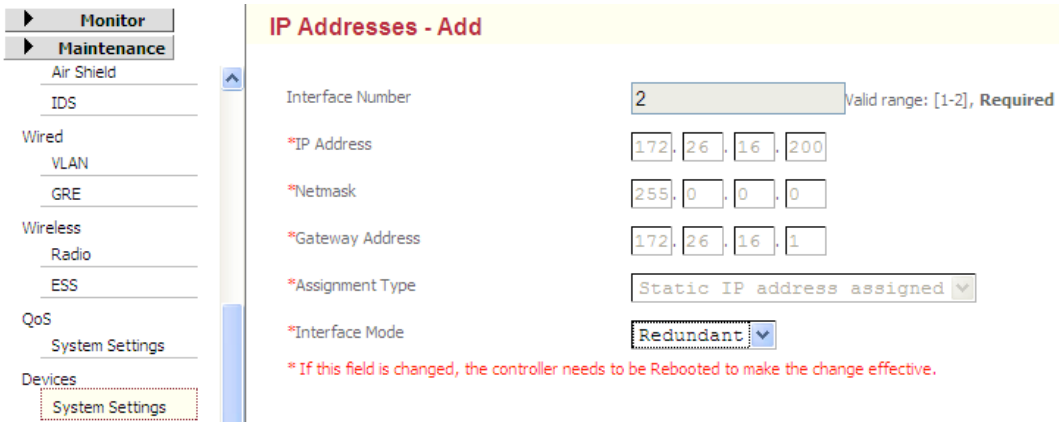
Once the desired VLANs are configured and mapped to their corresponding ESSIDs, the Controller on the wired side connected to the switch will automatically begin trunking on its interface for those VLANs. However, the switch port to connected controllers must also be configured to allow all desired VLANs.

Dual-Ethernet Capability

With Meru's dual Ethernet capability, the Interface Mode can be configured as a redundant (standby) or active. In redundant mode, the backup controller takes place of the primary only if the primary controller goes down. It is important in setting up this configuration to make sure the switch and port that the redundant interface is connected to is configured exactly the same way as the primary interface for trunking and allowed VLANs.

In active mode for example, the second interface can be configured to carry traffic for specified VLANs while the first interface will be used for management and Meru tunnel traffic. In this configuration, the control-plane traffic would be sent out of a separate interface from data traffic, providing increased protection for the control-plane.

Dual Ethernet operation can be configured from WEB UI or from CLI. From the WEB UI go to **Configuration > Devices > System Settings**, on the main page select the IP Address tab and click on the **Add** button.



IP Addresses - Add

Interface Number: 2 Valid range: [1-2], **Required**

*IP Address: 172.26.16.200

*Netmask: 255.0.0.0

*Gateway Address: 172.26.16.1

*Assignment Type: Static IP address assigned

*Interface Mode: Redundant

* If this field is changed, the controller needs to be Rebooted to make the change effective.

Add the following Information:

1. In the Interface Number text box, leave the default assignment 2.
2. In the IP Address field, type the IP address of this interface. For a redundant configuration, this option is greyed out, as the interface takes the static IP address of the primary interface. For an active configuration, the second Ethernet interface must be configured with a static IP address to a different L2 domain as the primary interface. In this example 172.26.16.200 IP address is used.
3. In the Netmask field, type the subnet mask of the interface. In this example 255.0.0.0 is used as subnet mask.
4. In the Gateway field, type the IP address of the gateway. In this example 172.26.16.1 is used as the Gateway address
5. In the Assignment Type list, for the active mode, select **Static IP address assigned.** The static IP address must be set for an active port assignment, and is unavailable for a redundant assignment.
6. In the Interface Mode list, select one of the following:
   - Active
   - Redundant

In this example Redundant is used as the Interface Mode List.

Note: If any of these fields are changed, reboot the controller for changes to take effect.

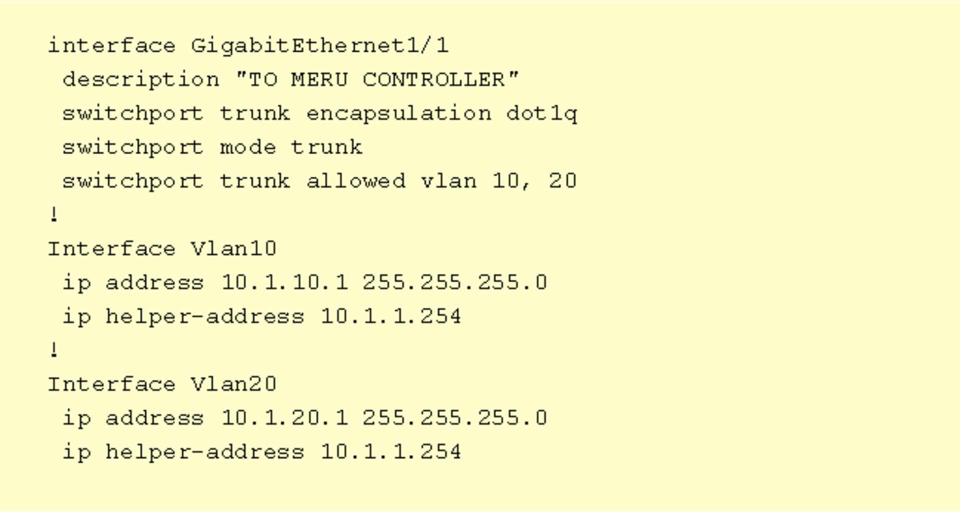
Switch Configuration and Setup

As discussed in the previous section the switch port that is connected to the Meru Controller must be configured to support trunking for the VLANs that are configured on the Controller. If no VLANs are used,trunking is not necessary.

Three commonly used switches along with the configuration and set-up procedures are outlined below:

Cisco Catalyst

The Cisco Catalyst Ethernet Switch configuration below assumes trunking to Meru Controller is desired for VLANs 10 and 20. Note the helper-ip address in the VLAN interface is configured, which is used to make sure the DHCP broadcast messages from the requesting client are forwarded to the unicast IP addresses of the DHCP server across VLANs

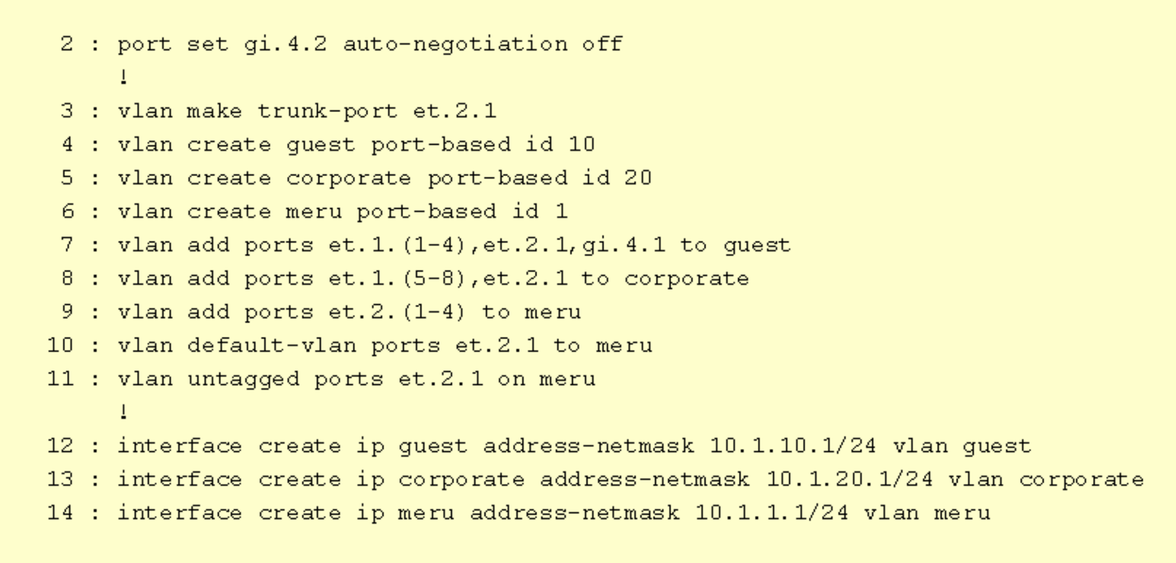


```
interface GigabitEthernet1/1
 description "TO MERU CONTROLLER"
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10, 20
!
Interface Vlan10
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.1.254
!
Interface Vlan20
 ip address 10.1.20.1 255.255.255.0
 ip helper-address 10.1.1.254
```

For Ports that do not need trunking, “switchport mode access” would be used instead of trunk mode, and the access VLAN number would be configured. To confirm the configuration, use the Catalyst switch command “show vlan” for the list of the configured VLANs and associated ports. In order to verify the trunking configuration, use the command “show interface trunk” which will display the status for trunking on each switch port, the encapsulation type used, the native VLAN for the trunk port, and the VLANs that are allowed and active in the management domain.

Enterasys SSR8

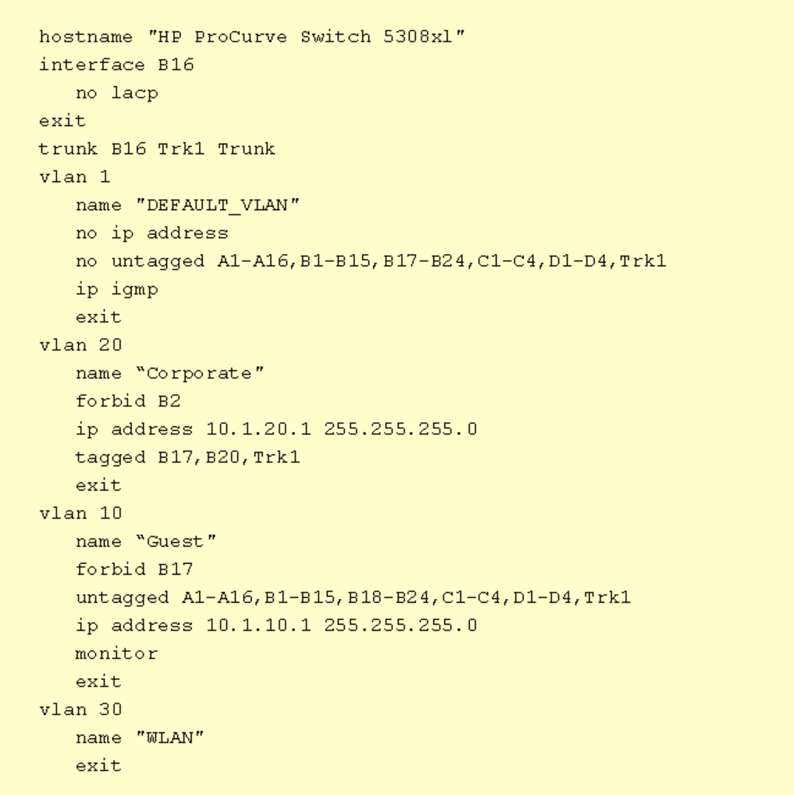
For the Enterasys SSR8 router, the following configuration applies:



```
 2 : port set gi.4.2 auto-negotiation off
     !
 3 : vlan make trunk-port et.2.1
 4 : vlan create guest port-based id 10
 5 : vlan create corporate port-based id 20
 6 : vlan create meru port-based id 1
 7 : vlan add ports et.1.(1-4),et.2.1,gi.4.1 to guest
 8 : vlan add ports et.1.(5-8),et.2.1 to corporate
 9 : vlan add ports et.2.(1-4) to meru
10 : vlan default-vlan ports et.2.1 to meru
11 : vlan untagged ports et.2.1 on meru
     !
12 : interface create ip guest address-netmask 10.1.10.1/24 vlan guest
13 : interface create ip corporate address-netmask 10.1.20.1/24 vlan corporate
14 : interface create ip meru address-netmask 10.1.1.1/24 vlan meru
```

HP ProCurve

For the HP ProCurve switch, the following configuration applies:



```
hostname "HP ProCurve Switch 5308xl"
interface B16
   no lacp
exit
trunk B16 Trk1 Trunk
vlan 1
   name "DEFAULT_VLAN"
   no ip address
   no untagged A1-A16,B1-B15,B17-B24,C1-C4,D1-D4,Trk1
   ip igmp
   exit
vlan 20
   name “Corporate"
   forbid B2
   ip address 10.1.20.1 255.255.255.0
   tagged B17,B20,Trk1
   exit
vlan 10
   name “Guest"
   forbid B17
   untagged A1-A16,B1-B15,B18-B24,C1-C4,D1-D4,Trk1
   ip address 10.1.10.1 255.255.255.0
   monitor
   exit
vlan 30
   name "WLAN"
   exit
```

Summary

Meru provides support for mapping an ESSID to a single VLAN, multiple ESSIDs to a VLAN, or dynamic mapping of a RADIUS-provided VLAN to an ESSID. The Meru Controller and Access Point communicate over the native or untagged VLAN via Meru tunnel, while the controller communicates to the wired network using a trunked port that is configured for all of the desired VLANs.

Meru interoperates with all properly configured Layer 2 and Layer 3 network devices to provide a seamless solution that links wired VLANs to the wireless domain.