PowerConnect W-Series
Basic Topology

Validated Reference Design Version 8

DELL

The VRD example campus network emulates the recommended campus network. Figure 1 shows the VRD example network setup.

Figure 1 *VRD example campus network*
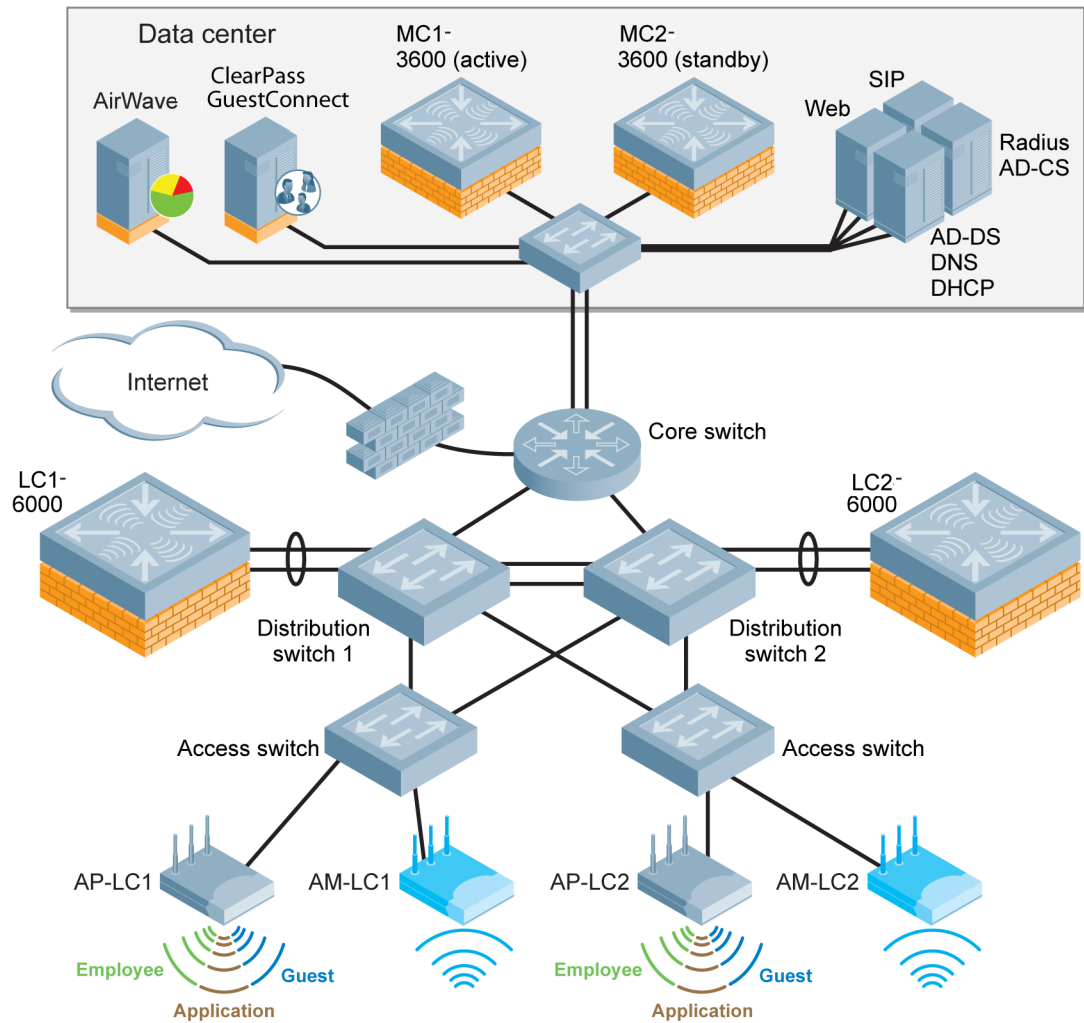
This example network is used to explain the concepts; it is not designed to prove scalability. Engineering teams perform extensive testing that is related to scalability. All screen shots and configurations used in the VRDs are from this example network.

The example network is not an exact replica of the recommended campus deployment at the core layer. This example network uses the collapsed core architecture. Dell recommends that the two master controllers be connected to two data center distribution switches to form a full mesh topology. The following sections explain the setup of the example network.

Data Center Setup

The data center consists of the master controllers, AirWave®, ClearPass GuestConnect™, and most of the other servers used in a typical campus network. The master controllers are deployed in the hot standby redundancy model, which is the recommended redundancy design for master controllers in campus deployments. For details about setting up master controller redundancy, see the *Campus Network Validated Reference Design*.

Table 1 summarizes the network parameters of the data center devices.

Table 1 *Data Center Network Parameters*

Network Devices	VLAN	IP
AirWave	130	10.169.130.2
ClearPass GuestConnect	130	10.169.130.50
DHCP	130	10.169.130.3
Active Directory Domain services (Windows Server 2008) and DNS	130	10.169.130.4
Windows Network Policy server for RADIUS authentication and Active Directory Certificate Service (Windows Server 2008)	130	10.169.130.20
SIP server	130	10.169.130.33
Microsoft Lync server 2010	130	10.169.130.35
Web server	130	10.169.130.30
MC1-3600 (active master)	130	10.169.130.6
MC2-3600 (standby master)	130	10.169.130.7

A Kiwi Syslog Server running on the Windows Server 2008 is used for syslog services and interface 10.169.130.5 is configured as the logging server interface on all the network devices. All the data center devices are connected to the core switch through the data center distribution switch.

Core Layer

The core switch is connected to the Internet through a gigabit ISP connection. The Open Shortest Path First (OSPF) routing protocol is implemented between the core switch and the two distribution switches.

Table 2 summarizes the VLAN and IP parameters of the core switch.

Table 2 *Core Switch Network Parameters*

VLAN	IP
128	10.169.128.4 (for OSPF)
130	10.169.130.1 (default gateway for all data center devices)

Distribution Layer

The distribution layer (see Figure 2) consists of two distribution switches and a PowerConnect W-6000 Mobility Controller with two M3 controller modules. The two local controllers, LC1-6000 and LC2-6000, are connected to the respective distribution switches SW-1 and SW-2 using link aggregation with the Link Aggregation Control Protocol (LACP).The distribution switches are the default gateways for all subnets except the guest subnet. The Dell PowerConnect W-Series controllers are deployed at Layer 2.

Figure 2 *Distribution layer setup in the example network*
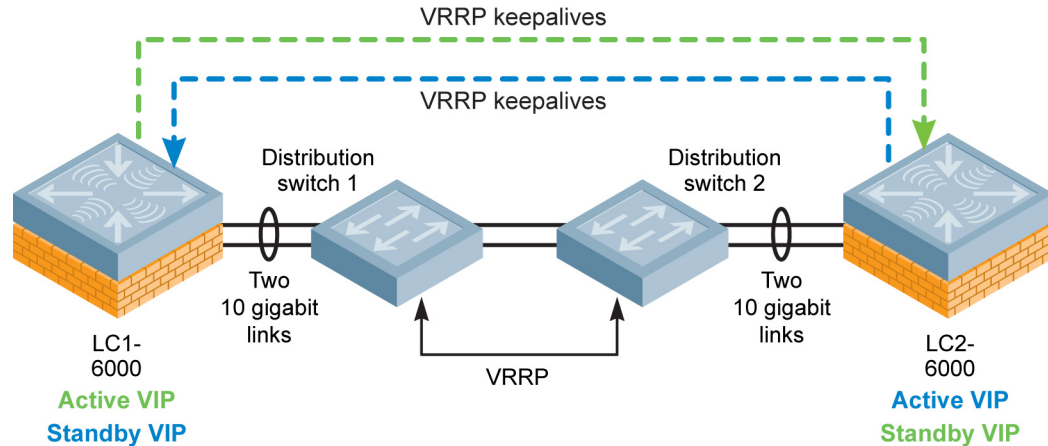
PowerConnect W-Series Mobility Controller Setup

- Each M3 controller module acts as a local controller.
- The local controller is not the default gateway for the user VLANs except for the guest VLAN. The outbound traffic on the guest VLANs, which is local to the PowerConnect W controllers at the aggregation layer, is source-NATed with the IP of the controller that manages that guest VLAN.
- Dell recommends that the local controllers act as default gateways and the DHCP server only for the guest VLANs.
- The local controllers are deployed at Layer 2, so the user VLANs defined on these controllers do not require an IP address. However, the implementation of IGMP proxy for multicast video optimization requires that every user VLAN on the local controllers that participates in IGMP proxy must have a Layer 3 address.
- If IGMP proxy is not required in network, IP parameters need not be defined for the user VLANs.
- Spanning tree is disabled on the PowerConnect W-Series controllers in the example network. However, to avoid loops, spanning tree has been implemented between other devices in the network. On the PowerConnect W-Series controllers, spanning tree is enabled by default, but network administrators must verify whether to disable it, depending on their network topology.
- The local controllers are deployed in the active-active redundancy model. Two Virtual Router Redundancy Protocol (VRRP) instances, VRRP-7 and VRRP-8, are used to provide active-active redundancy between the local controllers. Active-active redundancy is recommended for local controller redundancy in campus deployment.
- To prepare for failover situations, all user VLANs are defined on both local controllers.

Figure 3 *Active-active redundancy, mobility controller unreachable*
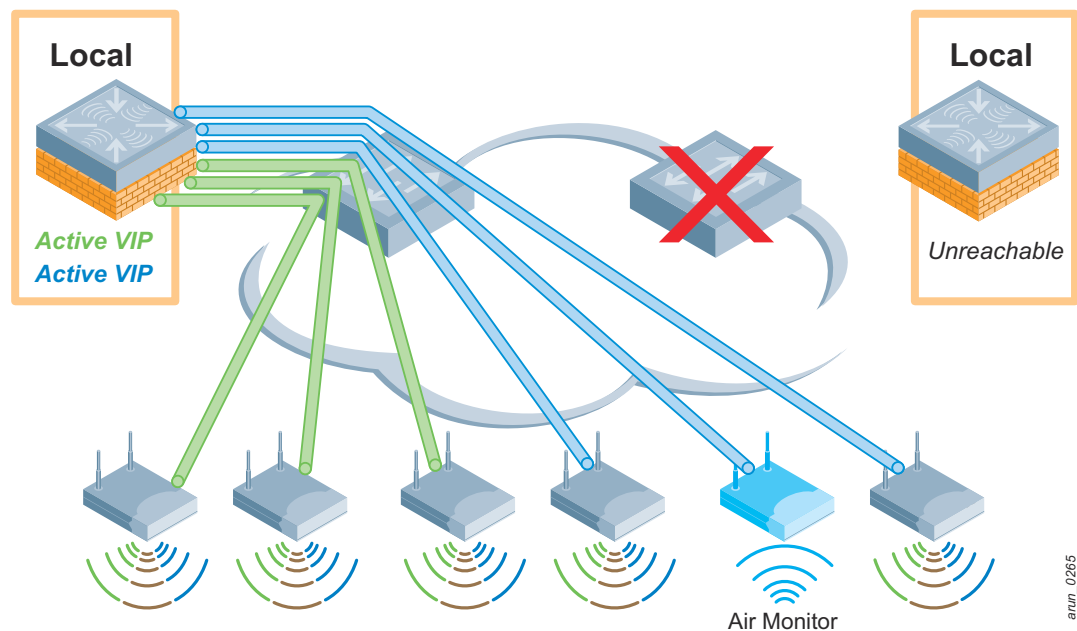
In the example network, LC1-6000 is the active controller for VRRP-7 VIP and LC2-6000 is the active controller for VRRP-8 VIP. The VAPs in the AP groups configured to terminate on VRRP-7 VIP are designed to use VLANs 150-154 for VLAN pooling. Similarly, the VAPs in the AP groups that terminate on VRRP-8 VIP use VLANs 155-159 for VLAN pooling. If LC1-6000 becomes unavailable, LC2-6000 becomes the active controller for the VRRP-7 IP. The APs that originally terminated on LC1-6000 now terminate on LC2-6000. So the LC2-6000 controller should have user VLANs 150-154 to support the WLANs that are broadcast by the VAPs of these APs. Support for such failover situations requires that all user VLANs be defined on both controllers.

NOTE: PowerConnect W-Series controllers are OSPF capable, but because they are typically deployed at Layer 2, they do not participate in OSPF in the example network.

The following figures and tables summarize the network parameters configured on PowerConnect W-Series controllers in the distribution layer of the example network.

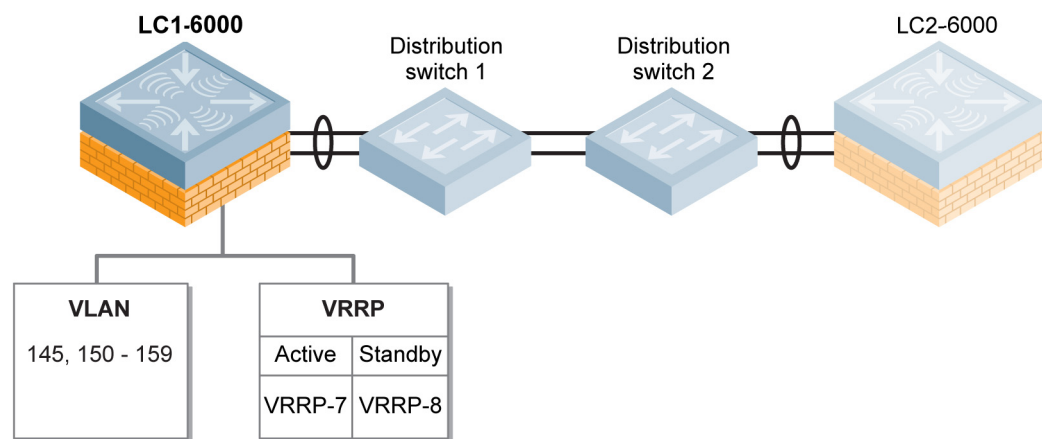**Figure 4** *LC1-6000 network parameters*

Table 3 *LC1-6000 Network Parameters*

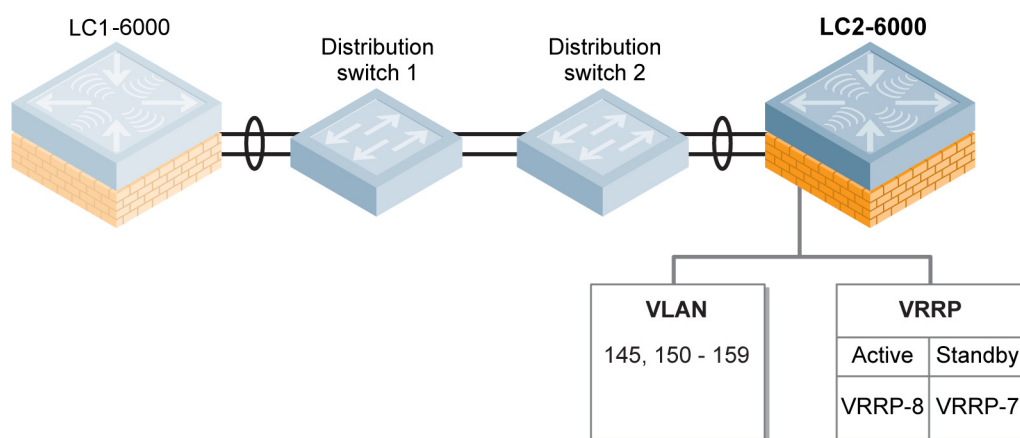| VLAN	IP (If IGMP Proxy is enabled, all user VLANs must have an IP address.)	IP (If IGMP Proxy is disabled, user VLANs do not require IP addresses.)	DHCP Scope	Purpose
145	10.169.145.4	10.169.145.4	__	Controller IP
150	10.169.150.4	__	__	Corporate user VLAN
151	10.169.151.4	__	__	Corporate user VLAN
152	10.169.152.4	__	__	Corporate user VLAN
153	10.169.153.4	__	__	Corporate user VLAN
154	10.169.154.4	__	__	Corporate user VLAN
155	10.169.155.4	__	__	Corporate user VLAN
156	10.169.156.4	__	__	Corporate user VLAN
157	10.169.157.4	__	__	Corporate user VLAN
158	10.169.158.4	__	__	Corporate user VLAN
159	10.169.159.4	__	__	Corporate user VLAN
900	192.168.200.20	192.168.200.20	192.168. 200.1 thru 192.168. 200.19, 192.168. 200.21 thru 192.168. 200.254	The guest VLAN. The local controller is the default gateway for the guest VLAN and acts as the DHCP server to the guest network.

Figure 5 *LC2-6000 network parameters*

Table 4 *LC2-6000 Network Parameters*

VLAN	IP (If IGMP Proxy is enabled, all user VLANs must have an IP address.)	IP (If IGMP Proxy is disabled, user VLANs do not require IP addresses.)	DHCP Scope	Purpose
145	10.169.145.5	10.169.145.5	__	Controller IP
150	10.169.150.5	__	__	Corporate user VLAN
151	10.169.151.5	__	__	Corporate user VLAN
152	10.169.152.5	__	__	Corporate user VLAN
153	10.169.153.5	__	__	Corporate user VLAN
154	10.169.154.5	__	__	Corporate user VLAN
155	10.169.155.5	__	__	Corporate user VLAN
156	10.169.156.5	__	__	Corporate user VLAN
157	10.169.157.5	__	__	Corporate user VLAN
158	10.169.158.5	__	__	Corporate user VLAN
159	10.169.159.5	__	__	Corporate user VLAN
900	192.168.201.20	192.168.201.20	192.168. 201.1 thru 192.168. 201.19, 192.168. 201.21 thru 192.168. 201.254	The guest VLAN. The local controller is the default gateway for the guest VLAN and acts as the DHCP server to the guest network.

Distribution Switch Design

● The distribution switches are the default gateways for all subnets except the subnet used for guest WLAN.

● To prepare for failover situations, all subnets are defined on both switches.

● VRRP is used between the distribution layer switches to establish redundancy for all the subnets that extend to the distribution switches. Instead of VRRP, Cisco® proprietary Hot Standby Router Protocol (HSRP) can also be used between the Cisco® distribution layer switches.

The following figure and tables summarize the network parameters configured on Cisco® switches in the distribution layer of the example network.

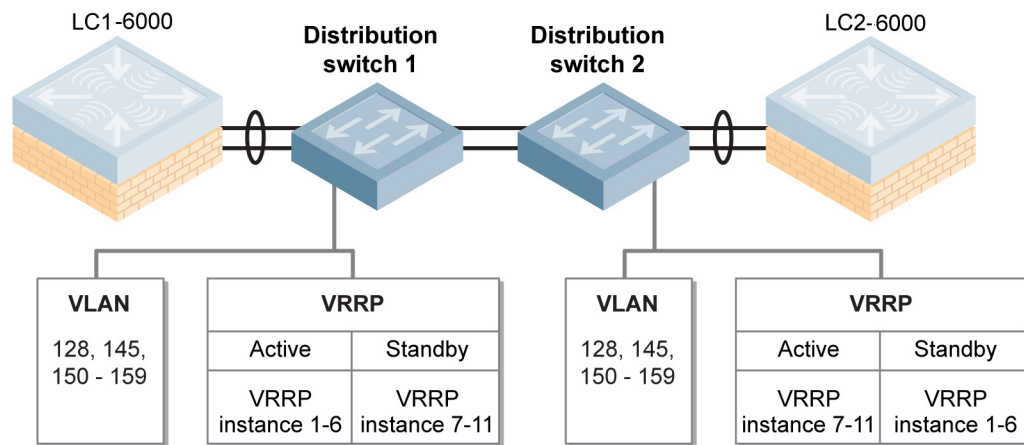**Figure 6** *Network parameters of distribution switches*

Table 5 *Distribution SW-1 Network Parameters*

VLAN	IP	Purpose
128	10.169.128.5	For OSPF routing
145	10.169.145.2	For OSPF routing and switch management
150	10.169.150.2	User VLAN
151	10.169.151.2	User VLAN
152	10.169.152.2	User VLAN
153	10.169.153.2	User VLAN
154	10.169.154.2	User VLAN
155	10.169.155.2	User VLAN
156	10.169.156.2	User VLAN
157	10.169.157.2	User VLAN
158	10.169.158.2	User VLAN
159	10.169.159.2	User VLAN

Table 6 *Distribution SW-2 Network Parameters*

VLAN	IP	Purpose
128	10.169.128.6	For OSPF routing
145	10.169.145.3	For OSPF routing and switch management
150	10.169.150.3	User VLAN
151	10.169.151.3	User VLAN
152	10.169.152.3	User VLAN
153	10.169.153.3	User VLAN
154	10.169.154.3	User VLAN
155	10.169.155.3	User VLAN

VLAN	IP	Purpose
156	10.169.156.3	User VLAN
157	10.169.157.3	User VLAN
158	10.169.158.3	User VLAN
159	10.169.159.3	User VLAN

Table 7 *VRRP Table*

VRRP Instance	VRRP Virtual IP	Active Switch	Standby Switch
1	10.169.145.1	Distribution SW-1	Distribution SW-2
2	10.169.150.1	Distribution SW-1	Distribution SW-2
3	10.169.151.1	Distribution SW-1	Distribution SW-2
4	10.169.152.1	Distribution SW-1	Distribution SW-2
5	10.169.153.1	Distribution SW-1	Distribution SW-2
6	10.169.154.1	Distribution SW-1	Distribution SW-2
7	10.169.155.1	Distribution SW-2	Distribution SW-1
8	10.169.156.1	Distribution SW-2	Distribution SW-1
9	10.169.157.1	Distribution SW-2	Distribution SW-1
10	10.169.158.1	Distribution SW-2	Distribution SW-1
11	10.169.159.1	Distribution SW-2	Distribution SW-1

Access Layer

Dell PowerConnect W-AP105 access points are used in the example network. AP-LC1 and AP-LC2 are the APs; AM-LC1and AM-LC2 are the dedicated AMs. In the example network, all the wired clients are placed in VLAN145. The APs are also deployed on the same VLAN as any other wired client.

Figure 7 *Access layer*
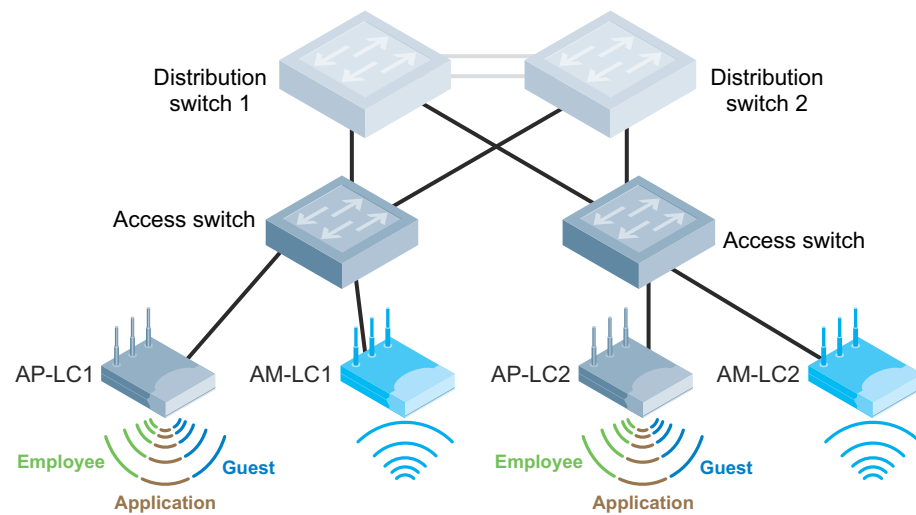
Any wireless users in the example network would associate to one of the following Service Set Identifiers (SSIDs):

- Employee SSID: Employee users and all corporate devices that are capable of 802.1X authentication use the employee SSID. An employee user has full access to all the network resources and the Internet. This SSID uses 802.1X/EAP for authentication and AES for encryption.

- Application SSID: Only corporate devices that are not capable of 802.1X authentication associate to the application SSID. These devices are assigned a role that limits their access only to the necessary application servers. For example, a VoIP phone running SIP can access only the SIP server to make calls. This SSID uses pre-shared key (PSK) for authentication and AES for encryption.

- Guest SSID: Guests use the guest SSID. Guest users are permitted to access only the Internet using specific protocols such as HTTP and HTTPS. This SSID uses open authentication at Layer 2 and there is no encryption. However, ClearPass GuestConnect is used to provide Layer 3 authentication through captive portal.