WiNG 5.x How-To Guide

Tunneling Remote Traffic using L2TPv3

Part No. TME-08-2012-01 Rev. A

Table of Contents

1. Introduction

WiNG 5 supports a number of different protocols which can be utilized to tunnel wired and wireless traffic between Controllers and Access Points. The primary method is to use Media Independent Network Transport (MINT) which is a Motorola Solutions proprietary management / control protocol that can be utilized to encapsulate and bridge layer 2 traffic between two or more WiNG 5 devices. A second method is to utilize IPsec which is an IETF standard protocol that can be utilized to encapsulate IPv4 traffic between two WiNG 5 devices or a WiNG 5 device and a third-party device.

Both MINT and IPsec protocols can be utilized in WiNG 5 for encapsulating traffic but both have their own limitations. For example user traffic can only be forwarded over Level 1 MINT links and cannot be utilized in centrally managed remote Access Point deployments which use Level 2 MINT links. IPsec can be complex to configure, manage and deploy and requires separate IPv4 networks at each end of the tunnel.

This configuration guide focuses on using Layer 2 Tunneling Protocol version 3 (L2TPv3) to address the limitations of MINT and IPsec when tunneling guest and non-guest traffic between WiNG devices in large multi-site deployments. This guide demonstrates how L2TPv3 can be deployed to tunnel guest and non-guest user traffic from remote sites to one or more data centers for remote sites local Controllers or remote Access Points.

1.1 L2TPv3 Protocol

L2TPv3 is an IETF standard protocol used for transporting layer 2 traffic over an intermediate IPv4 network. L2TPv3 is comprised of control messages and data messages (sometimes referred to as "control packets" and "data packets", respectively). Control messages are used in the establishment, maintenance, and clearing of control connections and sessions. Data messages are used to encapsulate the layer 2 traffic being transported over the L2TPv3 session. These control messages are used for dynamic setup, maintenance, and teardown of the sessions. The data message format for tunneling data packets may be utilized with or without the L2TPv3 control channel.

The necessary setup for tunneling a session with L2TPv3 consists of two steps:

1. Establishing the control connection.
2. Establishing a session as triggered by an incoming call or outgoing call.

An L2TPv3 session must be established before L2TPv3 can forward session frames. Multiple sessions may be bound to a single control connection (tunnel), and multiple control connections may exist between the same two peers. In WiNG 5.4 Ethernet pseudowires are the L2TPv3 sessions which are mapped to individual VLANs. Each VLAN that needs to be encapsulated and forwarded over the L2TPv3 tunnel is mapped to a session which includes a pseudowire ID and the VLAN IDs of the source traffic being forwarded over each session.

The control protocol is defined as RFC 3931 while the encapsulation protocol is defined in RFC 4719. L2TPv3 tunnels can be employed with or without the control protocol and can encapsulate layer 2 traffic using IP protocol 115 (default) or UDP port 1701. Most L2TPv3 deployments utilize the control protocol as it provides reachability and peer detection that allows each of the L2TPv3 peers to detect and react to network or device failures.

Encapsulation for the control and sessions is defined on a peer basis. Each peer can utilize either IP or UDP encapsulation. UDP encapsulation can be optionally enabled for compatibility with third-party devices of for environments with NAT when port address translation is enabled on an intermediate router / firewall.

Encapsulation Protocol	IP Protocol	Default Port
IP (default)	115	N/A
UDP	17	1701

Table 1.1 – L2TPv3 Protocol and Ports

1.2 L2TPv3 Policies and Parameters

In WiNG 5.4 L2TPv3 tunnels can be defined using profiles or device overrides. Each L2TPv3 tunnel requires the following parameters to be defined:

1. Tunnel
2. Tunnel Policy
3. One or more Peers
4. One or more Sessions

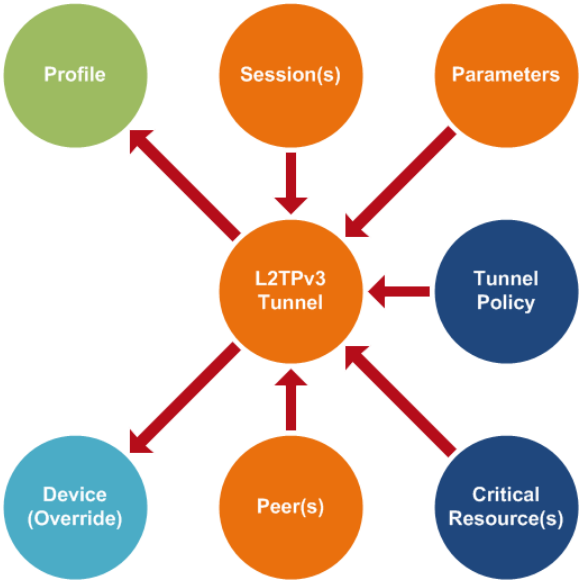


Figure 1.2 – L2TPv3 Configuration

1.2.1 L2TPv3 Tunnel

The L2TPv3 tunnel defines the tunnel policy, peers and sessions as well as the tunnel establishment criteria and critical resource policies. Each WiNG 5 device can support multiple tunnels which can terminate on the same or different peers. Each tunnel must include a tunnel policy and one or more peers and sessions.

Each tunnel also defines the tunnel establishment criteria the WiNG 5 device uses to initiates and terminate the L2TPv3 control and sessions. WiNG 5.4 supports the following tunnel establishment criteria options:

1. Always (default) – Any device can initiate the L2TPv3 when defined.
2. Cluster Master – Only the Cluster Master can initiate or terminate the L2TPv3 tunnel.
3. RF Domain Manager – Only the elected RF Domain Manager can initiate the L2TPv3 tunnel.
4. VRRP Master – Only the VRRP Master can initiate or terminate the L2TPv3 tunnel.

The establishment criteria utilized will depend on the specific deployment model. For example remote distributed Access Point deployments will typically utilize the RF Domain Manager criteria within the Access Point profiles to minimize the number of L2TPv3 tunnels that need to be terminated in the data center from the remote sites. Local RFSX000 Controller based deployments will typically utilize the Cluster Master criteria so that the active Controller in the cluster managing the Access Points initiates the L2TPv3 tunnel.

The establishment criteria for RFSX000 Controllers deployed as L2TPv3 concentrators will also vary depending on the traffic distribution, failover and recovery requirements. For example if the Always criteria is defined, both of the RFSX000 Controllers in the data center are capable of terminating the L2TPv3 tunnels. This allows both the RFSX000 Controllers to forward guest or non-guest traffic from the remote sites. During a failure / recovery event this also means all the L2TPv3 tunnels will remain established to a single RFSX000 Controller as no reversion is possible.

If however the Cluster Master criteria is defined, only the cluster Master for the site will be eligible to terminate the L2TPv3 tunnels. At any time only the elected cluster master will be eligible to terminate the L2TPv3 tunnels from the remote sites. Additionally the L2TPv3 tunnels will always revert back to the preferred cluster master during a failure / recovery event.

Critical Resource Monitoring (CRM) support is also provided allowing remote RFSX000 Controllers or Independent Access Points to monitor the end-to-end network path is available over the intermediate network. For example CRM can monitor the Internet router in each data center to verify that each data center is capable of terminating and forwarding guest user traffic. The results can be utilized by the WiNG 5 devices to determine which remote peer the L2TPv3 control and sessions are established providing failover in the event of an ISP, router / firewall or data center device failure.

1.2.2 Tunnel Policy

Each L2TPv3 tunnel includes an assigned L2TPv3 tunnel policy which defines the timers used for the L2TPv3 control and sessions. The timers determine the interval between hello packets exchanged between the peers for peer detection in addition to hold down timers that define how long each peer waits before failing over to an alternative peer.

Each L2TPv3 tunnel must include an L2TPv3 tunnel policy. By default the WiNG 5 master configuration includes an L2TPv3 tunnel policy named ***default*** which includes default values. The default values can be safely employed for guest user applications providing failover and recovery within 1 – 2 minutes depending on the type of failure event.

The default timers can also be modified to provide compatibility with third-party L2TPv3 peers or to provide faster failover and recovery times if required. For example the ***Hello Interval*** and ***Reconnect Intervals*** can be lowered to improve failure detection and recovery times.

The following table provides the default values f utilized by the default and user defined L2TPv3 tunnel policies:

Parameter	Default Value	Descriptions
Failover Delay	5	Time interval for re-establishing the tunnel after a failover (RF-Domain Manager / VRRP Master / Cluster Master).
Hello Interval	60	The time interval (in seconds) between L2TPv3 Hello keep-alive messages exchanged in the L2TPv3 control connection.
Reconnect Attempts	0	Specifies the number of times a device will attempt to make the L2TPv3 connection with a peer. After this many attempts, it will try to establish the L2TPv3 connection with the alternative peer (if specified).
Reconnect Interval	120	Time interval between the successive attempts to reestablish the L2TPv3 tunnel.
Retry Attempts	5	The maximum number of retransmissions for signaling messages.
Retry Interval	5	The time interval (in seconds) before the initiating a retransmission of any L2TPv3 signaling message.
RX Window Size	10	Number of signaling messages that can be received without sending the acknowledgement.
TX Window Size	10	Number of signaling messages that can be sent without receiving the acknowledgement.

Table 1.2.2 – Default L2TPv3 Tunnel Policy Timers

1.2.3 Peers

Each L2TPv3 tunnel can include a maximum of two peers and each tunnel must have one peer defined. Each peer defines the IPv4 address, hostname or router ID the remote host that the L2TPv3 control and sessions are established with.

For WiNG 5 devices that initiate the L2TPv3 tunnel, the remote devices IPv4 address and hostnames are typically defined. This allows the initiators to identify the remote devices before establishing a control and session with the peers. For the WiNG 5 devices that terminate the L2TPv3 control a sessions, wildcard entries are typically defined permitting any peer to connect.

For high availability each L2TPv3 tunnel configuration can include two peer entries where peer 1 is always preferred over peer 2. During normal operation the control and sessions will be established with peer 1. If peer 1 becomes unavailable the control and sessions are re-established with peer 2. The amount of time it takes for a peer to be marked as un-reachable depends on the timers defined in the L2TPv3 tunnel policy assigned to the L2TPv3 tunnel.

Each peer can also determine the encapsulation used for the sessions. By default each peer is configured to use IP encapsulation which utilizes IP protocol 115. Each peer can alternatively be configured to use UDP encapsulation which by default utilizes UDP port 1701. The UDP port is a user-

configurable value. The encapsulation must match on both peers for the L2TPv3 control and sessions to be established.

1.2.4 Sessions

Each L2TPv3 tunnel can include one or more sessions and each tunnel must have one session defined. Each session determines a name, pseudowire ID and source VLAN IDs for the traffic being bridged over the L2TPv3 tunnel. Each session can support one or more VLANs which are configured in a similar manner to a switch port. For example the traffic source can be a single VLAN or a list of VLAN IDs. You may also optionally specify a Native VLAN if desired.

Traffic can be forwarded on to an L2TPv3 session in multiple ways. Traffic from a physical port, locally bridged VLAN or extended VLAN can be bridged directly to an L2TPv3 session. The WiNG 5 device will simply bridge the traffic from the source VLAN to the L2TPv3 session using the VLAN ID. For the traffic to be bridged the source VLAN ID must be permitted over the L2TPv3 session. Please note however that traffic from an Extended VLAN will only be bridged to the L2TPv3 session if the ***inter-tunnel-bridging*** parameter to be enabled.

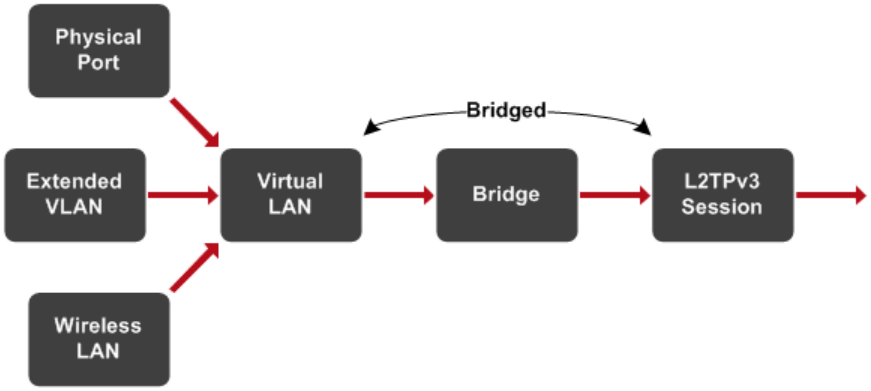


Figure 1.2.4-1 – Bridged Sessions

Traffic can also be routed then forwarded to a L2TPv3 session. In this instance the source traffic is terminated on a switched virtual IP interface defined in the WiNG 5 device and is routed to a VLAN assigned to the L2TPv3 session. Both the source and L2TPv3 VLANs will require a Switched Virtual Interface (SVI) to be defined on the WiNG 5 device that is providing the IP routing services. Routing is useful when large broadcast domains need to be split into smaller sub-networks.

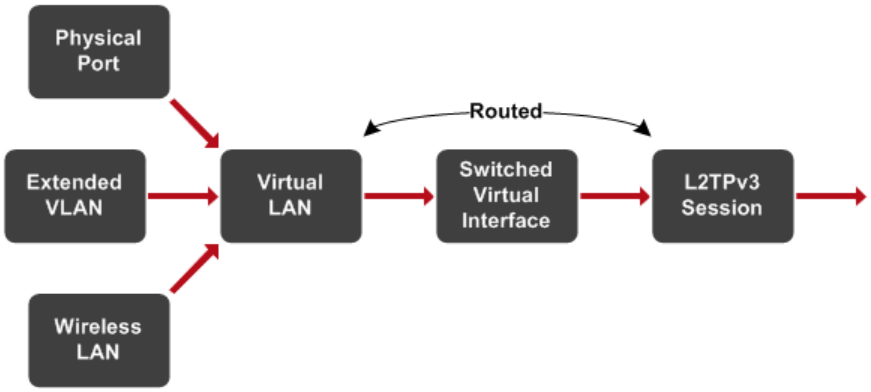


Figure 1.2.4-2 – Routed Sessions

1.2.5 Inter Tunnel Bridging

By default a WiNG 5 device can bridge any traffic to an L2TPv3 session that originated from a VLAN within the device. However traffic that originates from another tunnel such as an Extended VLAN or another L2TPv3 tunnel is not bridged by default. This behavior is controlled using the ***inter-tunnel-bridging*** parameter which can be enabled in the profile or device as an override. When enabled, broadcast packets from a source VLAN will be sent to all the sessions that extend the corresponding VLAN.

The inter-tunnel-bridging parameter must be enabled on any device that is mapping traffic from a tunneled VLAN to an L2TPv3 session. This includes:

1. Remote Access Points when VLANs are extended between the elected RF Domain Manager and non RF Domain Manager Access Points.
2. RFSX000 Controllers at remote sites when VLANs are tunneled from the Access Points to the local Controllers at the site.

The inter-tunnel-bridging parameter may also be optionally enabled on the RFSX000 Controllers in the data center terminating each of the remote L2TPv3 sessions when hosts across different tunnels need to communicate. In most instances this feature will be disabled for guest applications but might be enabled for non-guest applications to support peer-to-peer or voice applications.

Care must be taken when enabling the ***inter-tunnel-bridging*** parameter to ensure that no loops are being introduced into the network. L2TPv3 provides no loop prevention mechanism therefore multiple tunnels from a remote site with ***inter-tunnel-bridging*** enabled on the initiators and the L2TPv3 concentrators can potentially introduce a loop into the network when the VLANs at both sites are extended between both devices. The implementations outlined in this guide only initiate a single L2TPv3 tunnel from each site which eliminates the loop potential.

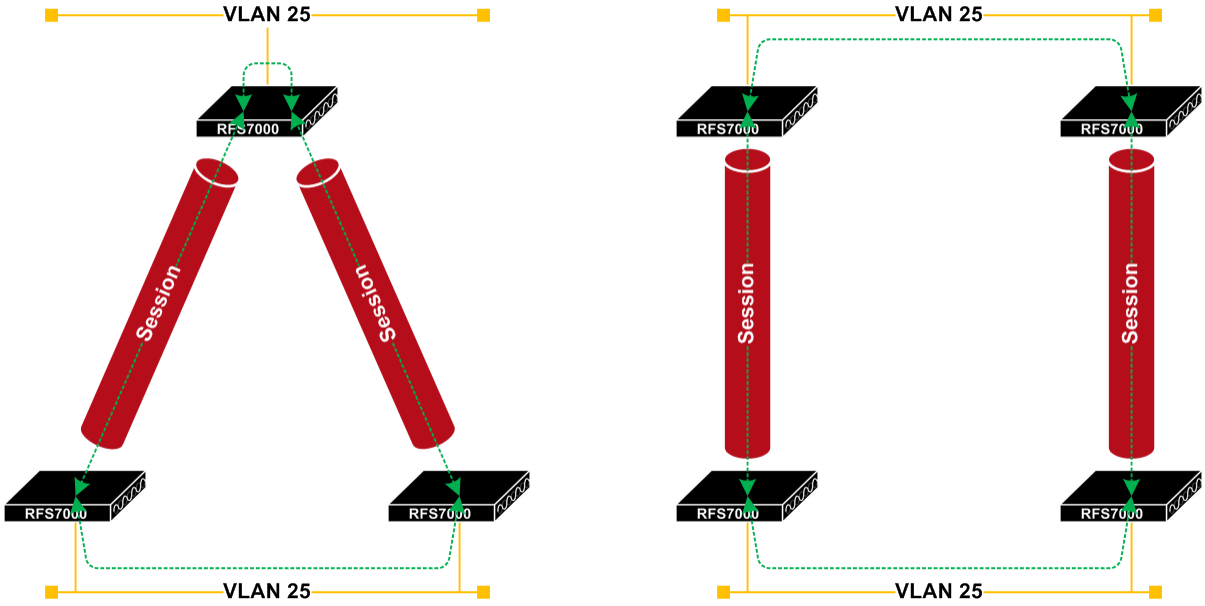


Figure 1.2.5 – L2TPv3 Loop Scenarios

1.3 Platform Support

L2TPv3 support was initially introduced on part of WiNG 5.3 with limited support being provided for specific models of Independent Access Points. As L2TPv3 is standards based this also allows traffic to be tunneled between WiNG 5 and third-party devices such as routers, firewalls and concentrators allowing WiNG 5 Controllers and Access Points to seamlessly integrated into various enterprise and service provider deployments.

WiNG 5.4 builds upon the initial L2TPv3 features introduced with the WiNG 5.3 release and adds various redundancy enhancements. The L2TPv3 enhancements in WiNG 5.4 include:

1. Support for Independent Access Points and RFSX000 Series Controllers.
2. L2TPv3 concentrator support permitting IP and hostname wildcards.
3. Tunnel Establishment Criteria which determines which devices can initiate and terminate L2TPv3 sessions.
4. Broadcast traffic optimization.
5. Optional L2TPv3 tunnel encryption using IPsec.
6. Critical Resource Monitoring.

The L2TPv3 tunnels can be established between WiNG 5 and third-party devices. For service provider deployments a RFSX000 Controller or Independent Access Point can initiate an L2TPv3 tunnel that typically terminates on the services providers existing infrastructure such as a third-party router or concentrator. For enterprise deployments a RFSX000 Controller / Independent Access Point can initiate an L2TPv3 tunnel that typically terminates on another WiNG 5 device such as a cluster of RFSX000 Controllers in the data center.

When utilizing RFSX000 Controllers in the data center as L2TPv3 concentrators to terminate L2TPv3 tunnels from multiple remote sites, it's important to understand that there are scaling limitations that need to be considered. Each model of Controller can terminate a specific number of L2TPv3 tunnels so the choice of platform in the data center will depend on the number of remote sites that need to be supported.

The following table provides the maximum number of L2TPv3 tunnels that are supported per WiNG 5 device with and without the control protocol:

WiNG Platform	Maximum Tunnels (Control Protocol)	Maximum Tunnels (No Control)
RFS7000	1,023	63
RFS6000	511	63
RFS4000	254	63
AP71XX	63	15
AP65XX	31	7

Table 1.3 – WiNG 5.4 L2TPv3 Tunnel Scaling

2. Configuration Examples

2.1 Centralized Controller Deployments

The following scenario demonstrates how to configure WiNG 5.4 and above to tunnel guest user traffic over L2TPv3 tunnels between elected RF Domain Managers at remote sites to a cluster of RFSX000 Controllers in a data center operating as L2TPv3 concentrators. The Access Points at each site are adopted and managed by a cluster of centralized RFSX000/NX Controllers in the data center using Level 2 MINT links.

In this scenario an elected RF Domain Manager at each remote site initiates an L2TPv3 tunnel to an active L2TPv3 concentrator in the data center. The guest user traffic is bridged between the Access Points at each remote site to the elected RF Domain Manager using Extended VLANs and is then tunneled over L2TPv3 to the data center where the Internet or corporate services reside.

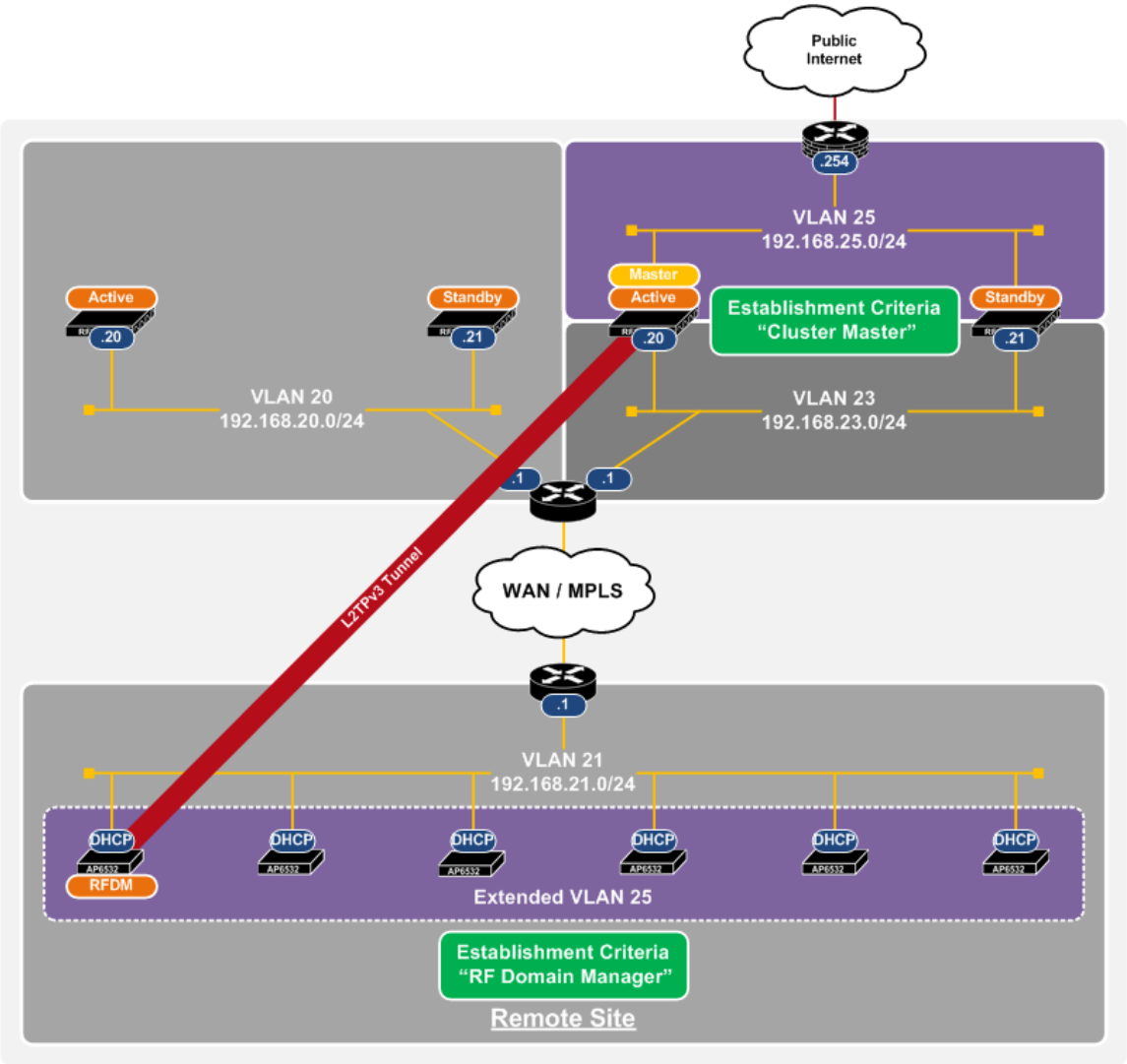


Figure 2.1 – Centralized Controller Topology

2.1.1 Applications

This solution can be deployed in distributed Wireless LAN environments to provide centralized guest access for remote sites with centrally managed Access Points deployed. When remote Access Points are managed using Level 2 MINT links there is no support for tunneling Wireless User traffic over the Level 2 MINT links. Additionally most centrally managed Access Point deployments will utilize NX9000 series Controllers which do not support a data plane which can terminate tunneled traffic.

L2TPv3 provides a graceful tunneling solution that allows traffic from remote sites to be forwarded to the data center over predictable paths as well as provide seamless failover and recovery. L2TPv3 is also much simpler to configure and deploy when compared to site-to-site IPsec VPN tunnels which are typically utilized to provide this functionality.

This deployment model is applicable to any centrally managed remote Access Point deployment. This includes deployments with single Access Points per site or larger deployments with up to 64 Access Points per site. For single Access Point deployments this solution allows additional Access Points to be added to the site with no additional changes being required.

2.1.2 Solution Components

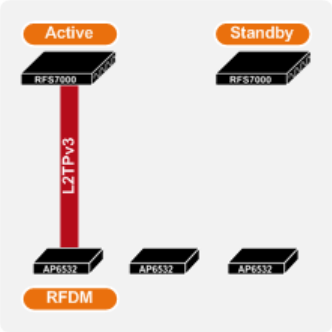
This deployment scenario utilizes the following components to provide a fully redundant solution for tunneling guest and non-guest traffic:

1. RF Domain Managers – One Access Point at each remote site is elected as the RF Domain Manager for the site which ***initiates*** the L2TPv3 tunnel to the active or standby L2TPv3 concentrator in the data center.
2. L2TPv3 Concentrators – A cluster of RFSX000 Controllers are deployed in the data center as L2TPv3 concentrators. One Controller is designated as primary (active) while the second Controller is designated as secondary (standby). The active Controllers are configured as cluster masters (priority 254) who during normal operation will ***terminate*** the L2TPv3 tunnels.
3. Wireless LAN – Guest users connect to the Wireless LAN with the required authentication and encryption enabled. The Wireless LAN must be configured to map the wireless user traffic to a ***Local VLAN*** (i.e. the guest VLAN) which is automatically extended from the Access Points to the cluster of local Controllers within site. The guest user traffic can then be forwarded over the L2TPv3 tunnel to the data center where the Internet and other services reside.

2.1.3 Failover and Recovery

Failover and recovery is provided natively by this solution. Each component provides failure detection and recovery capabilities which allow the L2TPv3 tunnels to be automatically re-established in the event of a RF Domain Manager or L2TPv3 concentrator failure.

2.1.3.1 Normal Operation



During normal operation the L2TPv3 tunnel is automatically established between the elected RF Domain Managers and the active L2TPv3 concentrator in the data center. The active and standby L2TPv3 concentrators IP addresses and hostnames are defined as peer 1 and peer 2 in the L2TPv3 tunnel configuration in the Access Points profiles. During normal operation the peer 1 connection is always preferred over the peer 2 connection.

2.1.3.2 L2TPv3 Concentrator Failure

If the active L2TPv3 concentrator fails, is taken offline for maintenance or is un-reachable over the intermediate network, the elected RF Domain Manager at each remote site will detect that the L2TPv3 peer is dead and will automatically re-establish the L2TPv3 tunnel with the standby L2TPv3 concentrator in the data center. The standby L2TPv3 concentrator will transition to an active state and will automatically become the cluster master for the site.

Upon recovery, the active L2TPv3 concentrator will become the cluster master and the standby L2TPv3 concentrator will transition back into a standby state. Any established L2TPv3 tunnels will be torn down and re-established to the active L2TPv3 concentrator.

If the standby L2TPv3 concentrator fails during normal operation, no action is taken as no L2TPv3 tunnels will be active on the device.

2.1.3.3 RF Domain Manager Failure

If an elected RF Domain Manager at the remote site fails, a new RF Domain Manager will be automatically elected for the site and will initiate the L2TPv3 tunnel to the active L2TPv3 concentrator in the data center.

If the failed RF Domain Manager is re-introduced into the network it will be automatically re-elected as the RF Domain Manager and will re-establish the L2TPv3 tunnel to the active L2TPv3 concentrator in the data center.

2.1.4 Configuration

2.1.4.1 L2TPv3 Concentrators

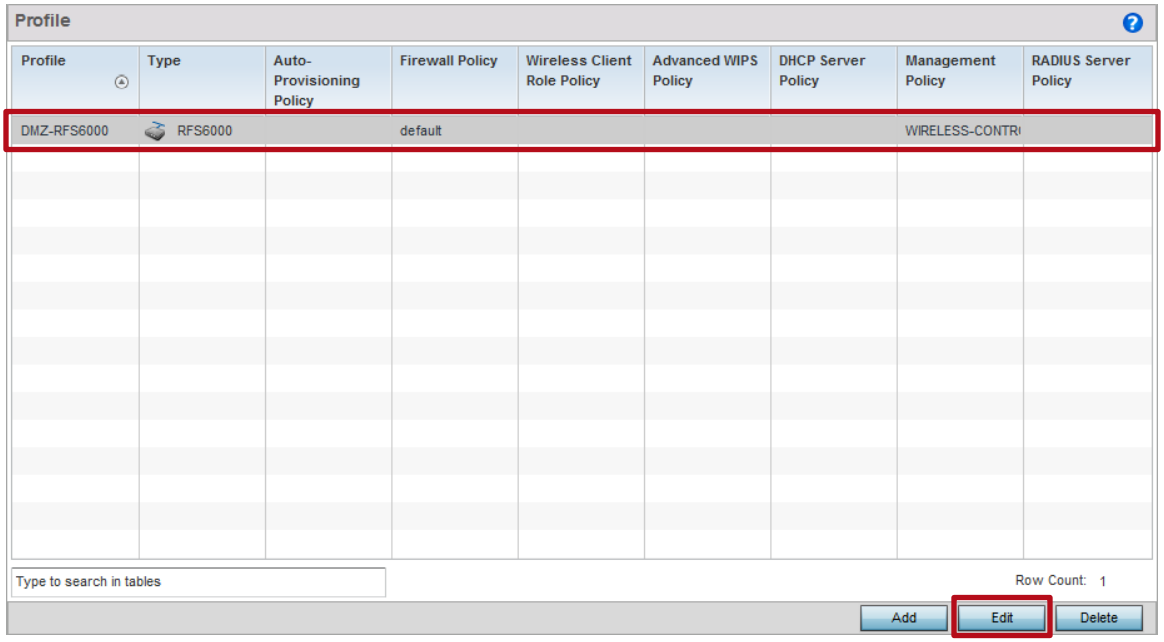
Each of the L2TPv3 tunnels from the elected RF Domain Managers at the remote sites terminate on a pair of RFSX000 Controllers in the data center operating as L2TPv3 concentrators. The L2TPv3 tunnel configuration on the L2TPv3 concentrators is defined using a common profile that is assigned to both RFSX000 Controllers. The L2TPv3 configuration includes a single peer definition that supports wildcards allowing the RFSX000 Controllers to terminate multiple L2TPv3 tunnels without having to define individual L2TPv3 peer entries.

The L2TPv3 tunnel configuration for the L2TPv3 concentrators includes the following parameters:

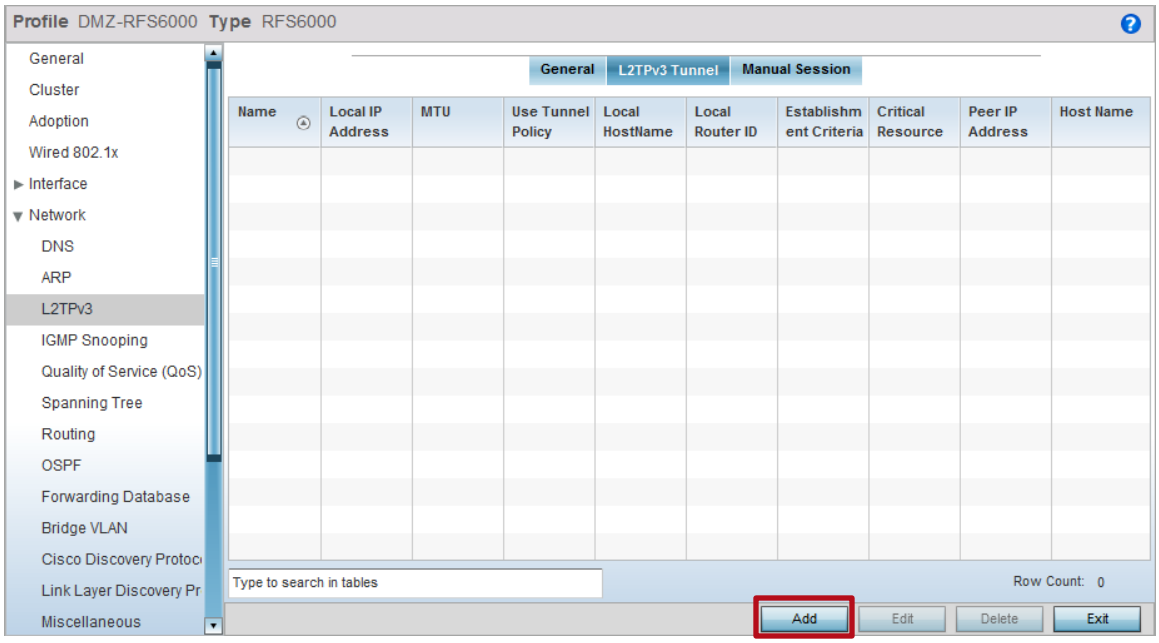
1. The L2TPv3 tunnel ***Name*** is defined as ***vlan25*** (Guest VLAN ID).
2. The ***Establishment Criteria*** is set to ***Cluster Master***.
3. The L2TPv3 ***Peer 1*** entry is defined with the ***Router ID*** and ***Host Name*** set to ***Any*** permitting tunnels from multiple remote peers. This eliminates the need for defining separate L2TPv3 peer entries for each Access Point.
4. The L2TPv3 ***Encapsulation*** is set to ***IP*** which utilizes ***Protocol 115***. Encapsulation can optionally be set to ***UDP*** which utilizes UDP port ***1701***.
5. One L2TPv3 ***Session*** is defined with the name set to ***vlan25*** and ***Pseudowire ID*** and ***Traffic Source Value*** set to ***25*** (Guest VLAN ID).

The following steps demonstrate how to define the L2TPv3 tunnel parameters for a pair of RFSX000 Controllers operating as L2TPv3 concentrators using a profile. This assumes the RFSX000 Controllers are up and operational on the network and the cluster has been pre-established. This also assumes that one of the RFSX000 Controllers is designated as the cluster master and the secondary Controller is operating in a standby mode:

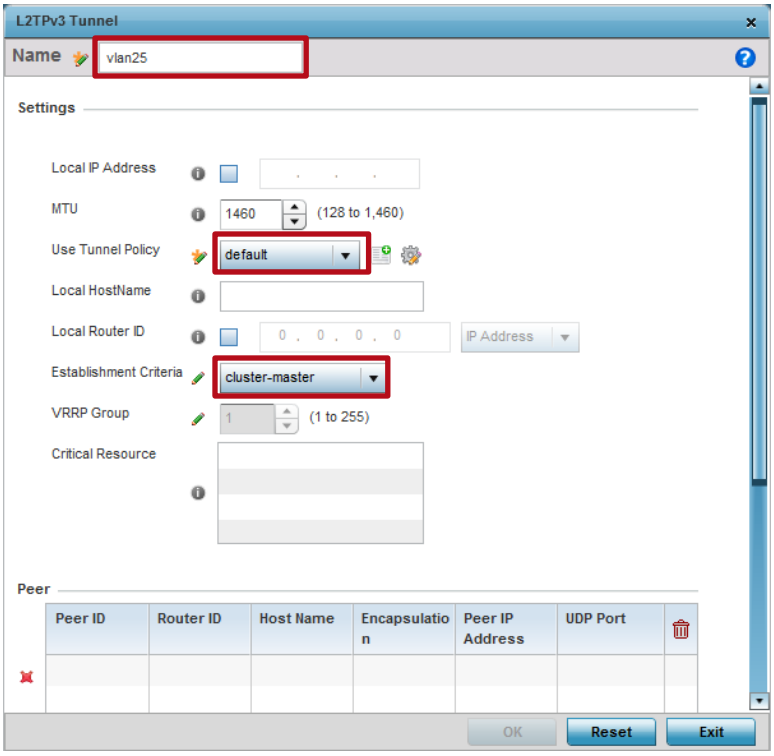
1 Using the Web-UI select *Configuration → Profile → <profile-name> → Edit:*



2 Select *Network* → *L2TPv3* → *L2TPv3 Tunnel* → *Add*:

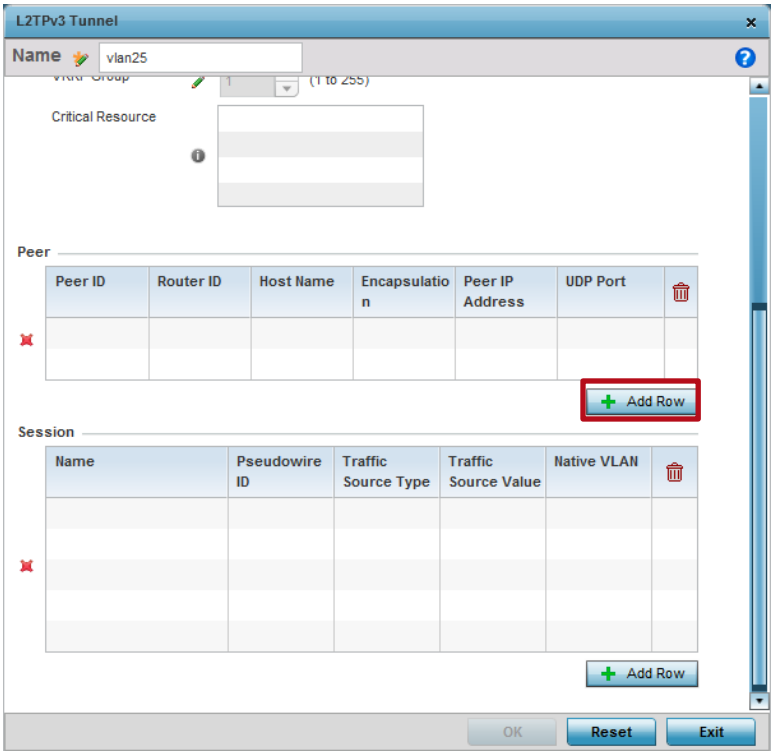


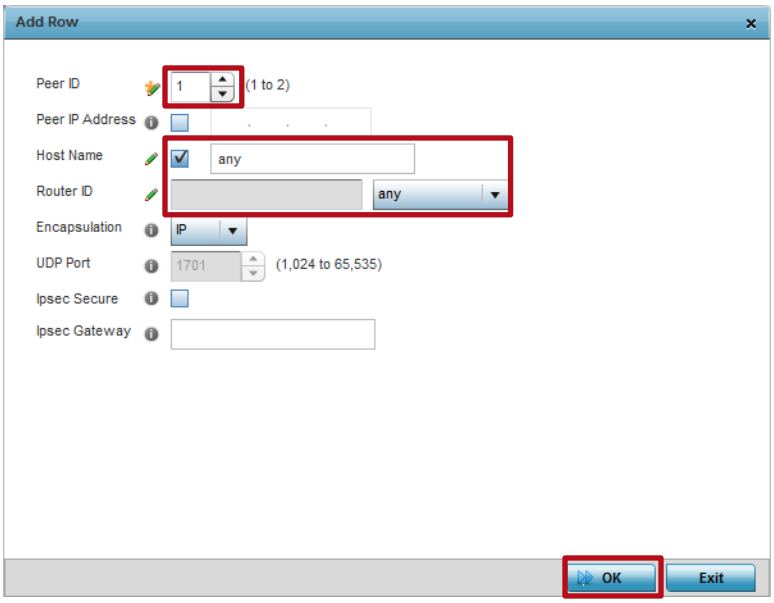
3 Enter a *Name* to identify the tunnel then select the *Tunnel Policy* named *default*. Set the *Establishment Criteria* to *Cluster Master:*



4 Under *Peer* select *Add Row*. Define the following parameters then click *OK*:

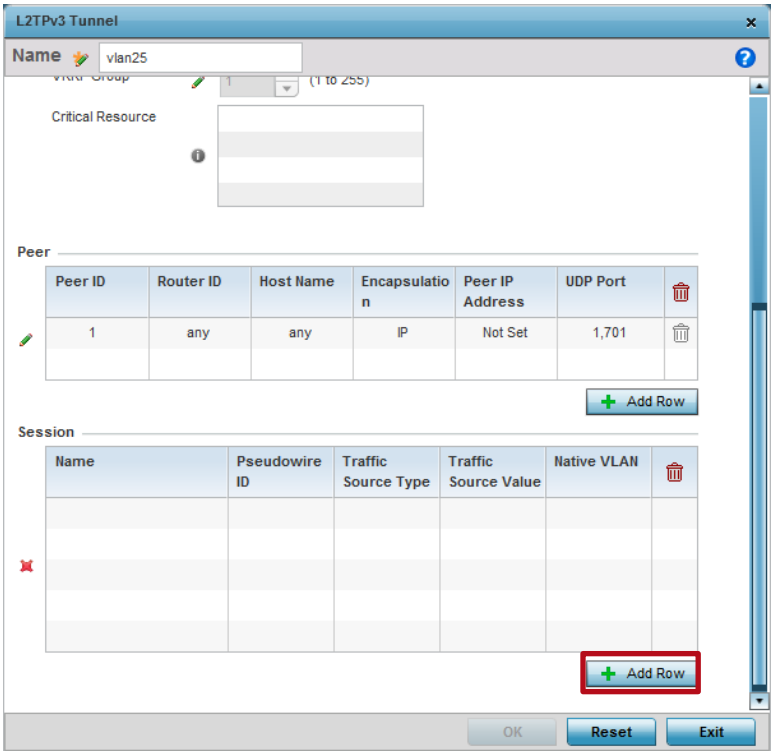
- **a. Set the *Peer ID* to *1*.**
- **b. Enter the *Host Name* value *any*.**
- **c. Set the *Router ID* to *any*.**

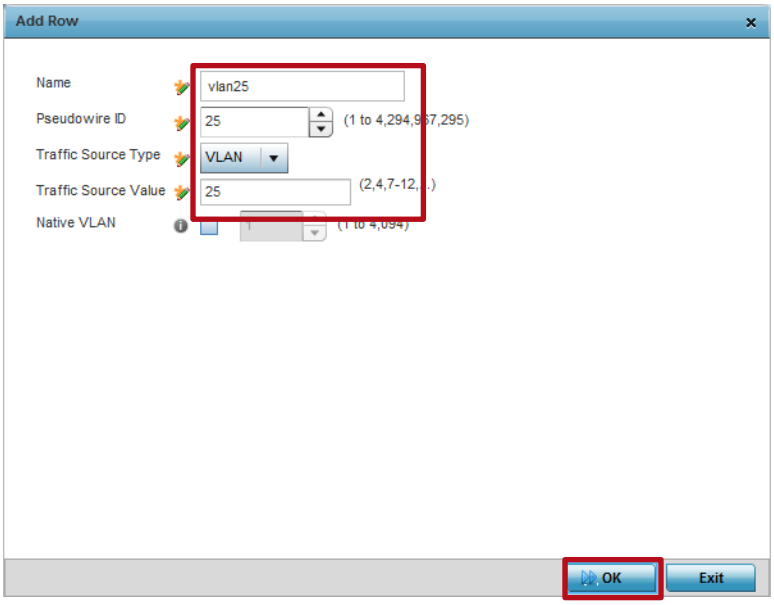




5 Under *Session* select *Add Row*. Define the following parameters then click *OK* and *Exit*:

- **a. Enter the *Name* to identify the session.**
- **b. Enter a Psuedowire ID. It is recommended that this match the Guest VLAN ID!**
- **c. Set the *Traffic Source Type* to *VLAN.***
- **d. Enter the *Traffic Source Value*. Note this must match the Guest VLAN ID!**





6 *Commit and Save* the changes:

The following changes were applied to the L2TPv3 Concentrators Profile:

```
!
profile rfs6000 DMZ-RFS6000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
!
! Configuration Removed for Brevity
!
l2tpv3 tunnel vlan25
  peer 1 hostname any router-id any
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria cluster-master
!
```

Note – By default the ability to tunnel traffic between L2TPv3 tunnels is disabled. This can optionally be enabled in the Controllers L2TPv3 configuration in the profile if hosts at different sites need to communicate over the L2TPv3 tunnels.

*Note – The **pseudowire-id** and **traffic-source** VLAN IDs must match on both L2TPv3 peers. In the above example guest VLAN 25 is being transported over the tunnel named **vlan25** which has the **pseudowire-id** and traffic-source set to **25**. The pseudowire-id and tunnel name may be any alpha numerical string as required.*

2.1.4.2 Remote Access Point Profile

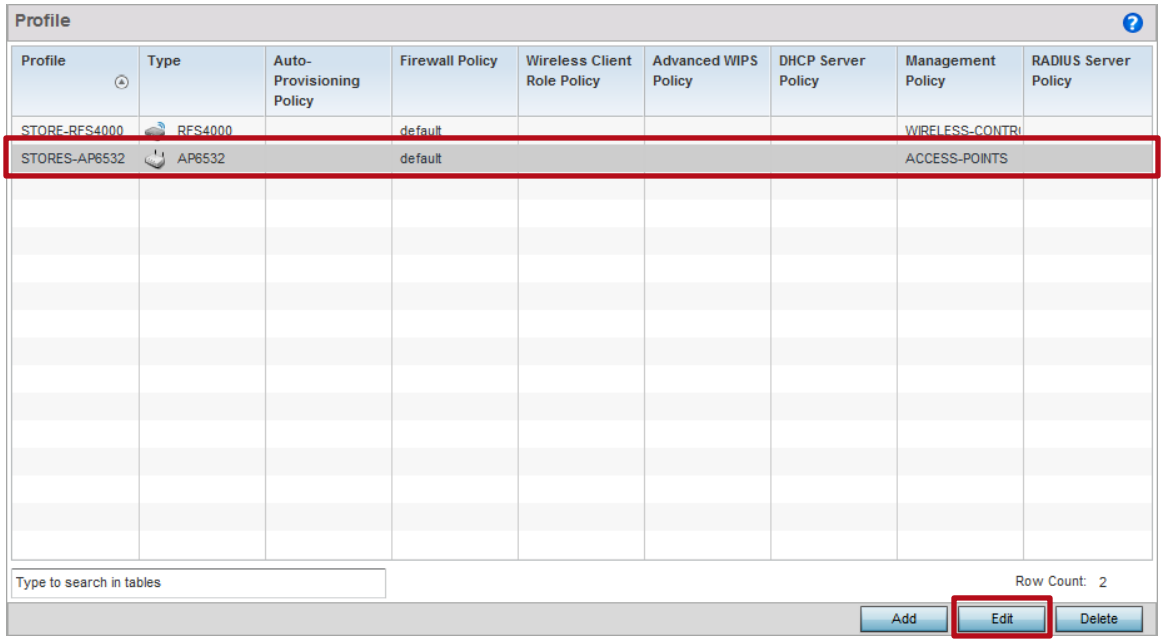
2.1.4.2.1 Bridged VLAN Configuration

Guest user traffic is bridged by each Access Point to a local VLAN. To be able to access the L2TPv3 tunnel on the elected RF Domain Manager the guest user traffic must be tunneled between the Access Points at the site using Extended VLANs. This is achieved by defining the guest VLAN as a Bridged VLAN in the Access Point profiles with the following parameters:

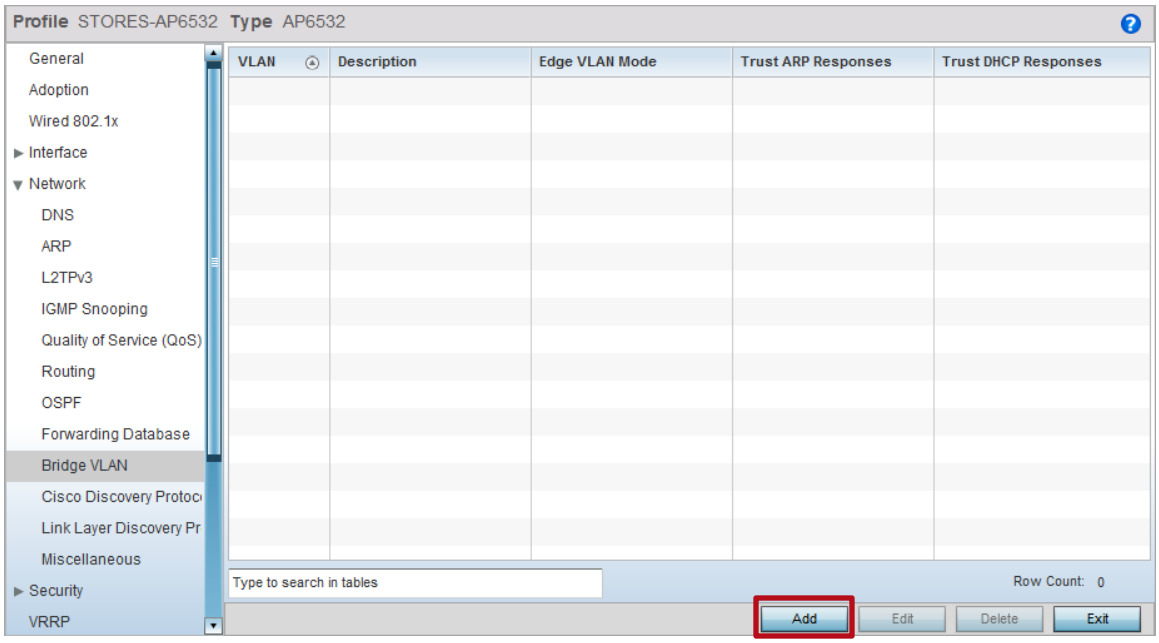
1. The bridged ***VLAN ID*** is set to ***25*** (Guest VLAN ID).
2. The ***Bridging Mode*** is set to ***Tunnel***.

The following steps demonstrate how to define the Bridged VLAN parameters in the Access Point profile. This configuration assumes that a single profile is assigned to all the Access Points at the remote site. If multiple models of Access Points exist, this configuration will be to be applied to each Access Point profile servicing the remote sites:

1 Using the Web-UI select *Configuration → Profile → <profile-name> → Edit:*



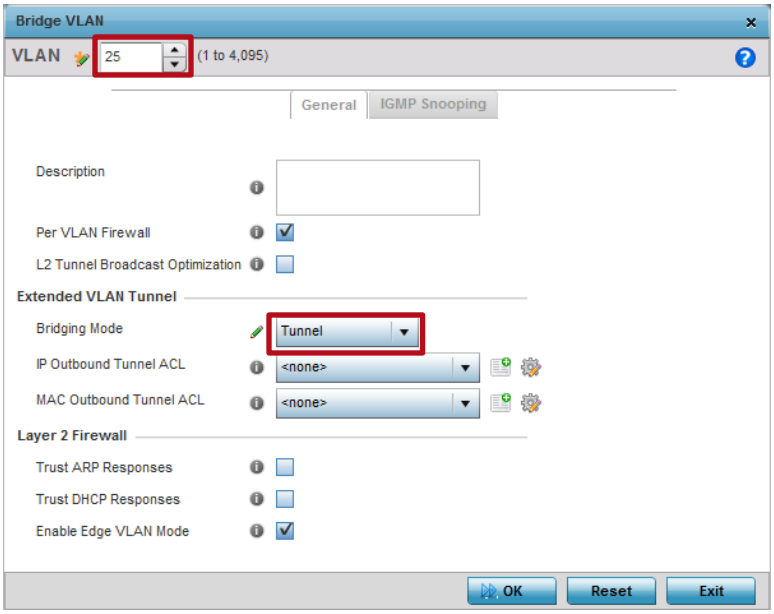
2 Select *Network* → *Bridge VLAN* → *Add*:



3 Define the following parameters then click *OK* and *Exit*:

a. In the *VLAN* field enter the Guest VLAN ID.

b. Set the *Bridging Mode* to *Tunnel*.



4 *Commit and Save* the changes:

The following changes were applied to the L2TPv3 Concentrators Profile:

```
!
profile ap6532 STORES-AP6532
 bridge vlan 25
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
!
! Configuration Removed for Brevity
!
 ntp server 192.168.10.6
 service pm sys-restart
 router ospf
!
```

2.1.4.2.2 L2TPv3 Tunnel Configuration

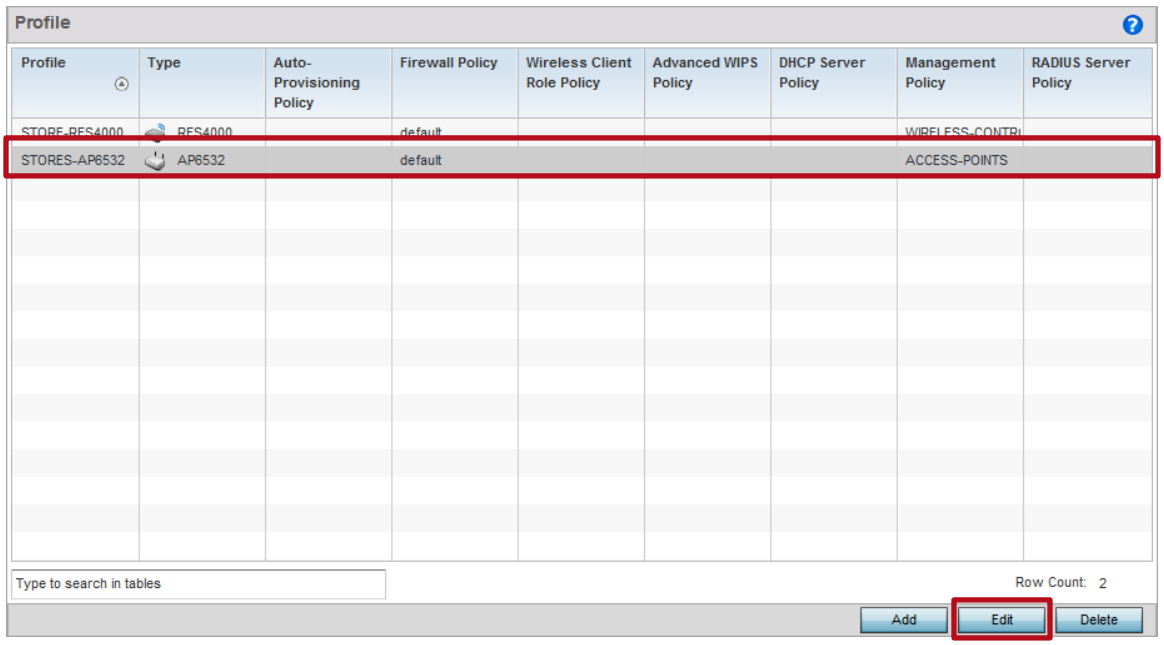
Each of the elected RF Domain Managers at the remote sites initiates a single L2TPv3 tunnel to the active L2TPv3 concentrator in the data center. During normal operation the L2TPv3 tunnel is established to the L2TPv3 concentrator defined as peer 1 and during a failure scenario the L2TPv3 tunnel will automatically failover to the L2TPv3 concentrator defined as peer 2.

The L2TPv3 tunnel configuration is defined using profiles that are assigned to the remote Access Points at each site. The L2TPv3 tunnel configuration includes the following parameters:

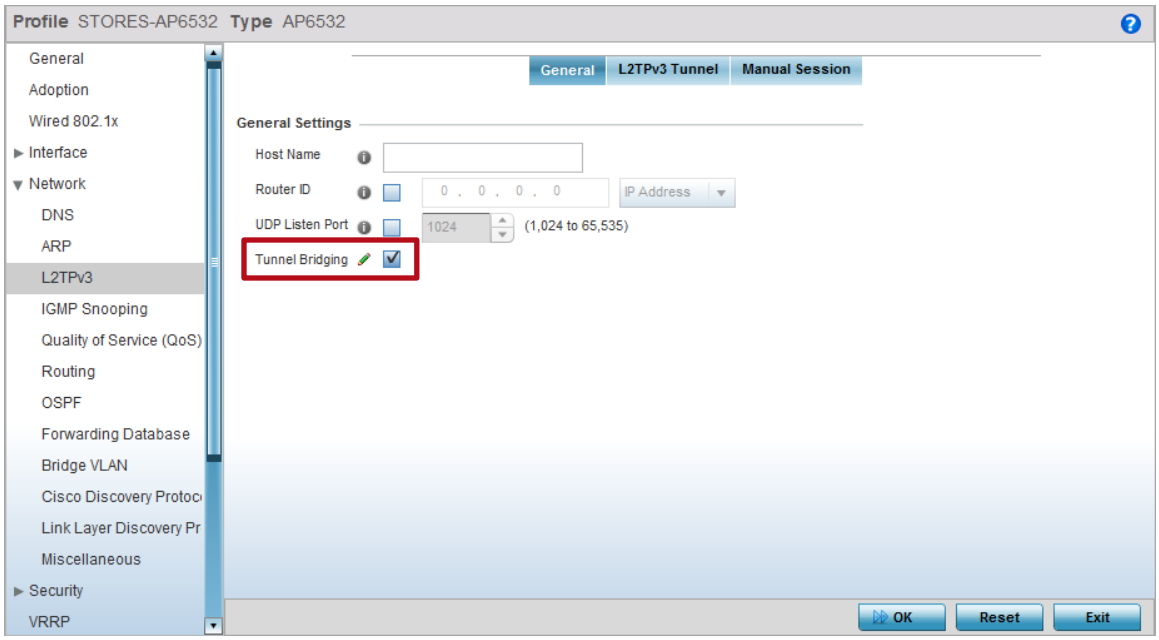
1. ***Inter Tunnel Bridging*** is ***enabled*** so that traffic from the Extended VLAN can be bridged to the L2TPv3 tunnel.
2. The L2TPv3 tunnel ***Name*** is defined as ***vlan25***.
3. The ***Establishment Criteria*** is set to ***RF Domain Manager***.
4. The L2TPv3 ***Peer 1*** entry is defined with the ***Peer IP Address*** set to ***192.168.23.20*** and the ***Host Name*** set to ***L2TPV3-GW-1***. The defined IP Address and Hostname match the IP Address and Hostname assigned to the primary Controller in the data center.
5. The L2TPv3 ***Peer 2*** entry is defined with the ***Peer IP Address*** set to ***192.168.23.21*** and the ***Host Name*** set to ***L2TPV3-GW-2***. The defined IP Address and Hostname match the IP Address and Hostname assigned to the secondary Controller in the data center.
6. The L2TPv3 ***Encapsulation*** is set to ***IP*** which utilizes ***Protocol 115***. Encapsulation can optionally be set to ***UDP*** which utilizes UDP port ***1701***.
7. One L2TPv3 ***Session*** is defined with the name set to ***vlan25*** and ***Pseudowire ID*** and ***Traffic Source Value*** set to ***25***.

The following steps demonstrate how to define the L2TPv3 tunnel parameters in the Access Point profile. This configuration assumes that a single profile is assigned to all the Access Points at the remote site. If multiple models of Access Points exist, this configuration will be to be applied to each Access Point profile servicing the remote sites:

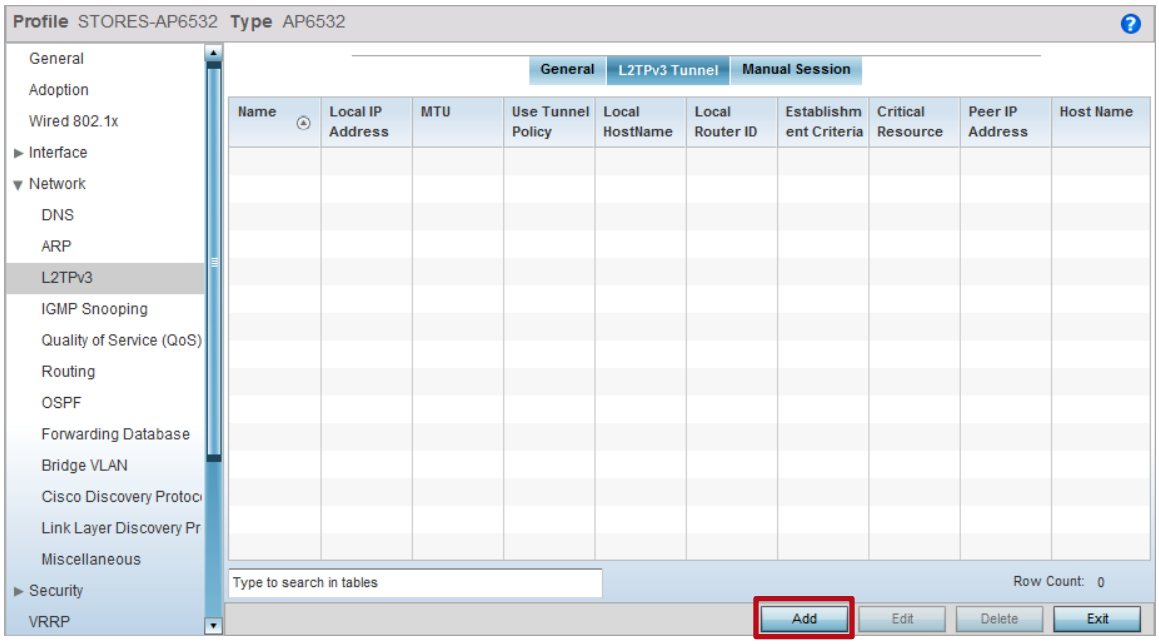
1 Using the Web-UI select *Configuration → Profile → <profile-name> → Edit:*



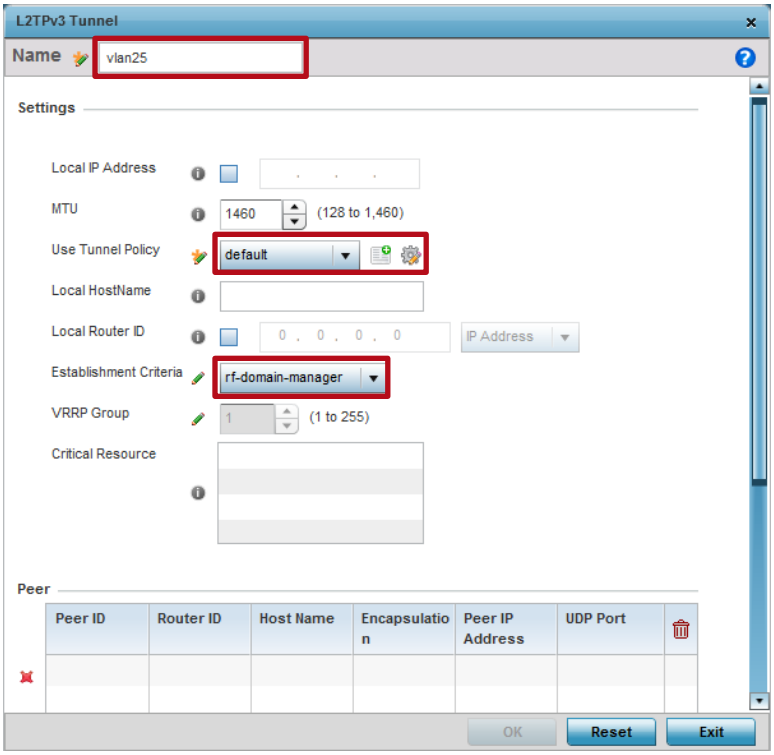
2 Select *Network* → *L2TPv3* → *General*. Enable *Tunnel Bridging* then click *OK*:



3 Select *Network* → *L2TPv3* → *L2TPv3 Tunnel* → *Add*:

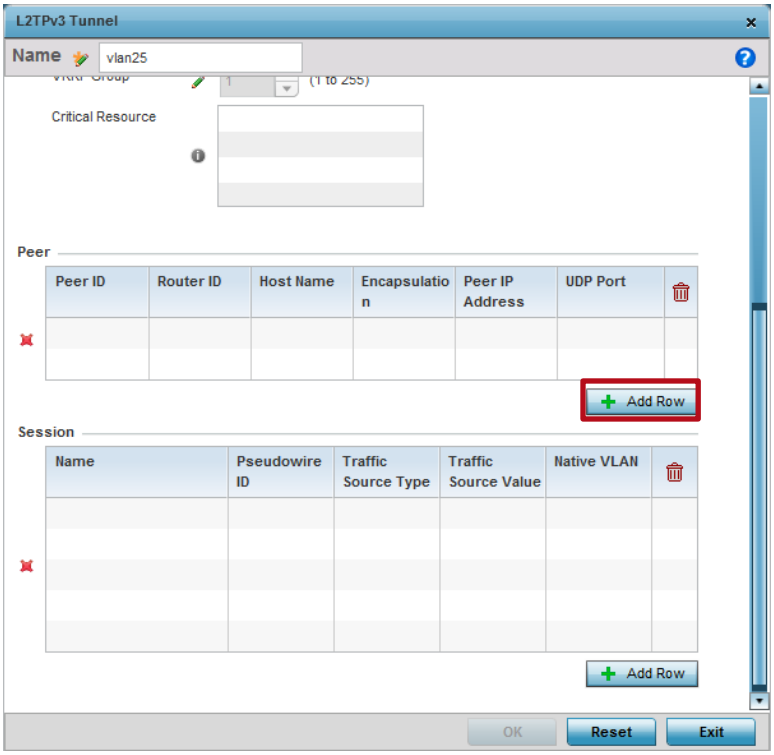


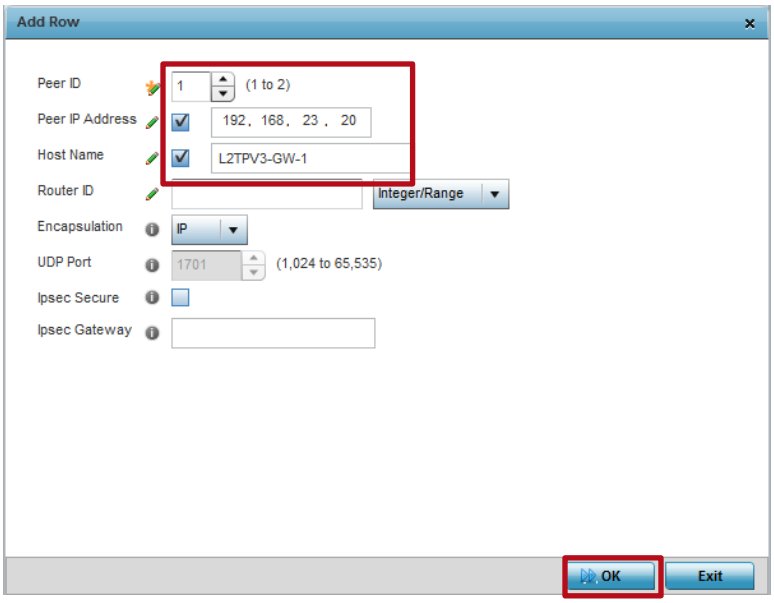
4 Enter a *Name* to identify the tunnel then select the *Tunnel Policy* named *default*. Set the *Establishment Criteria* to *RF Domain Manager:*



5 Under *Peer* select *Add Row*. Define the following parameters then click *OK*:

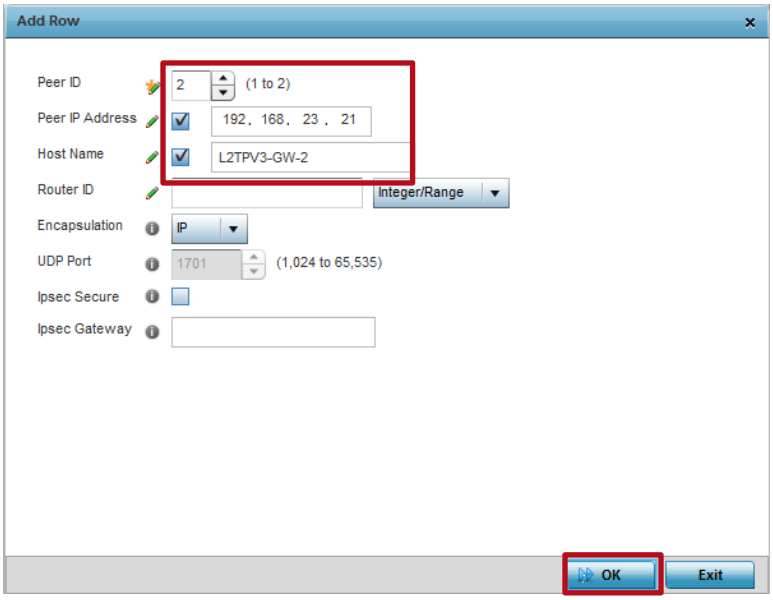
- **a. Set the *Peer ID* to *1*.**
- **b. Set the Peer IP Address to 192.168.23.20 (active L2TPv3 concentrator's IP address).**
- **c. Enter the *Host Name* value *L2TPV3-GW-1* (active L2TPv3 concentrator's hostname).**





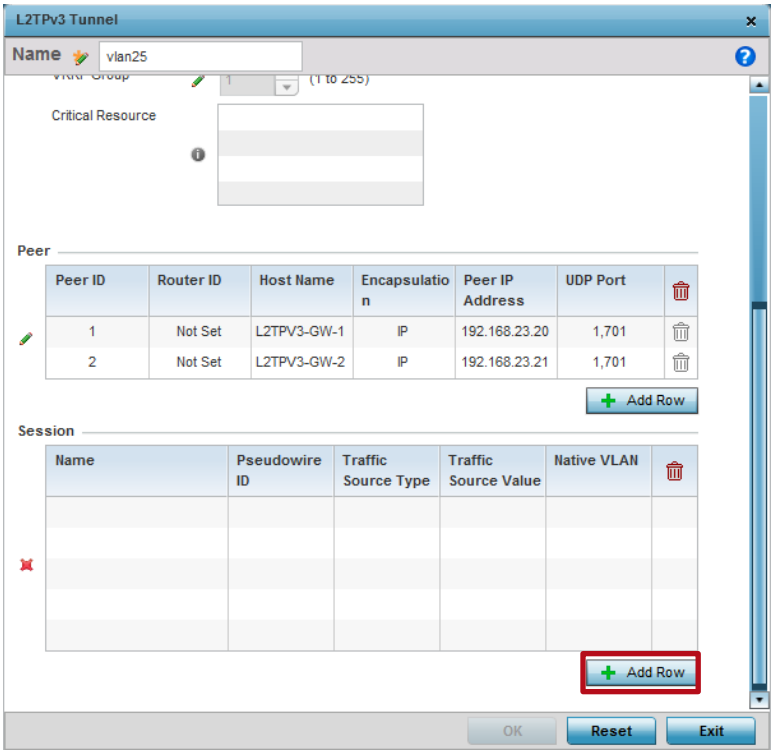
6 Click Add Row and define a second peer. Define the following parameters then click *OK*:

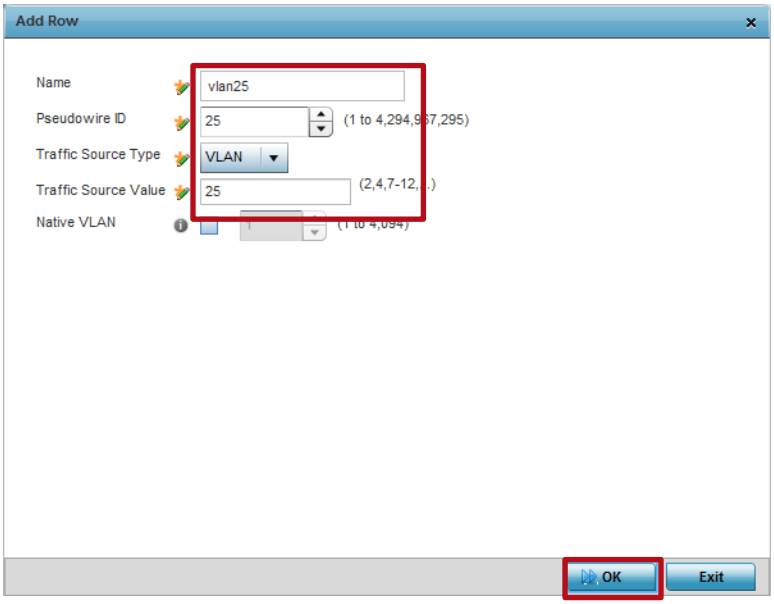
- **a. Set the *Peer ID* to 2.**
- **b. Set the Peer IP Address to 192.168.23.21 (standby L2TPv3 concentrator's IP address).**
- **c. Enter the *Host Name* value *L2TPV3-GW-2* (standby L2TPv3 concentrator's hostname).**



7 Under *Session* select *Add Row*. Define the following parameters then click *OK* and *Exit*:

- **a. Enter the *Name* to identify the session.**
- **b. Enter a Psuedowire ID. It is recommended that this match the Guest VLAN ID!**
- **c. Set the *Traffic Source Type* to *VLAN.***
- **d. Enter the *Traffic Source Value*. Note this must match the Guest VLAN ID!**





8 *Commit and Save* the changes:

The following changes were applied to the L2TPv3 Concentrators Profile:

```
!
profile ap6532 STORES-AP6532
 bridge vlan 25
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
!
! Configuration Removed for Brevity
!
l2tpv3 tunnel vlan25
  peer 1 ip-address 192.168.23.20 hostname L2TPV3-GW-1
  peer 2 ip-address 192.168.23.21 hostname L2TPV3-GW-2
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria rf-domain-manager
 l2tpv3 inter-tunnel-bridging
!
```

Note – Inter Tunnel Bridging must be enabled for the guest user traffic to be bridged between the Extended VLAN and the L2TPv3 tunnel.

*Note – The **pseudowire-id** and **traffic-source** VLAN IDs must match on both L2TPv3 peers. In the above example guest VLAN 25 is being transported over the tunnel named **vlan25** which has the **pseudowire-id** and traffic-source set to **25**. The pseudowire-id and tunnel name may be any alpha numerical string as required.*

2.2 Local Controller Deployments

The following scenario demonstrates how to configure WiNG 5.4 and above to tunnel guest user traffic over L2TPv3 tunnels between a cluster of RFSX000 Controllers at remote sites to a cluster of RFSX000 Controllers in a data center operating as L2TPv3 concentrators. The Access Points at each site are adopted and managed by the local cluster of RFSX000 Controllers using Level 1 MINT links.

In this scenario remote sites contain a cluster of RFSX000 Controllers which initiate an L2TPv3 tunnel to an active L2TPv3 concentrator in the data center. The guest user traffic is tunneled from the Access Points to the local cluster of Controllers within the site using Extended VLANs and is then tunneled over L2TPv3 to the data center where the Internet or corporate services reside.

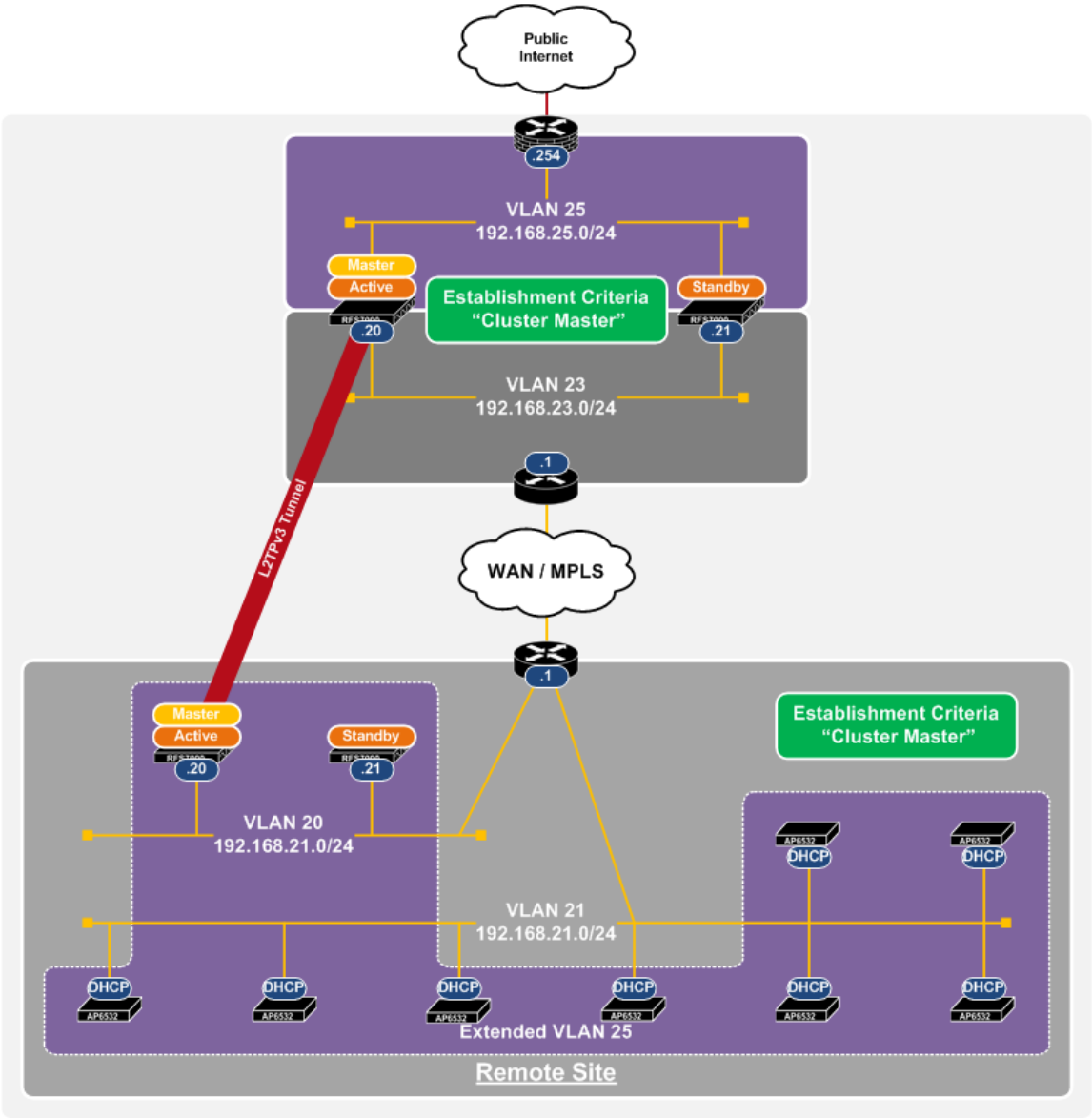


Figure 2.2 – Local Controller Topology

2.2.1 Applications

This solution can be deployed in distributed Wireless LAN environments to provide centralized guest access for remote sites with local RFSX000 Controllers deployed. While level 1 MINT links can provide similar functionality, establishing these links will allow the WiNG 5 devices at each of the remote sites to discover each other over the MINT network which is not desirable in large scale networks.

L2TPv3 provides a graceful tunneling solution that allows traffic from remote sites to be forwarded to the data center over predictable paths as well as provide seamless failover and recovery. L2TPv3 is also much simpler to configure and deploy when compared to site-to-site IPsec VPN tunnels which are typically utilized to provide this functionality.

2.2.2 Solution Components

This deployment scenario utilizes the following components to provide a fully redundant solution for tunneling guest and non-guest traffic:

1. Local Controllers – A cluster of RFSX000 Controllers are deployed at one or more remote sites for Access Point configuration, management and adoption. One Controller is designated as primary (active) while the second Controller is designated as secondary (standby). The active Controllers are configured as cluster masters (priority 254) who during normal operation will ***initiate*** the L2TPv3 tunnels.
2. L2TPv3 Concentrators – A cluster of RFSX000 Controllers are deployed in the data center as L2TPv3 concentrators. One Controller is designated as primary (active) while the second Controller is designated as secondary (standby). The active Controllers are configured as cluster masters (priority 254) who during normal operation will ***terminate*** the L2TPv3 tunnels.
3. Wireless LAN – Guest users connect to the Wireless LAN with the required authentication and encryption enabled. The Wireless LAN must be configured to map the wireless user traffic to a ***Tunneled VLAN*** (i.e. the guest VLAN) which is automatically extended from the Access Points to the cluster of local Controllers within site. The guest user traffic can then be forwarded over the L2TPv3 tunnel to the data center where the Internet and other services reside.

2.2.3 Failover and Recovery

Failover and recovery is provided natively by this solution. Each component provides failure detection and recovery capabilities which allow the L2TPv3 tunnels to be automatically re-established in the event of a local Controller or L2TPv3 concentrator failure.

2.2.3.1 Normal Operation

During normal operation the L2TPv3 tunnel is automatically established between the local RFSX000 Controllers operating as cluster masters and the active L2TPv3 concentrator in the data center. The active and standby L2TPv3 concentrators IP addresses and hostnames are defined as peer 1 and peer 2 in the L2TPv3 tunnel configuration in the local Controllers profile. During normal operation the peer 1 connection is always preferred over the peer 2 connection.

2.2.3.2 L2TPv3 Concentrator Failure

If the active L2TPv3 concentrator fails, is taken offline for maintenance or is un-reachable over the intermediate network, the cluster master at each remote site will detect that the L2TPv3 peer is dead and will automatically re-establish the L2TPv3 tunnel with the standby L2TPv3 concentrator in the data center. The standby L2TPv3 concentrator will transition to an active state and will automatically become the cluster master for the site.

Upon recovery, the active L2TPv3 concentrator will become the cluster master and the standby L2TPv3 concentrator will transition back into a standby state. Any established L2TPv3 tunnels will be torn down and re-established to the active L2TPv3 concentrator.

If the standby L2TPv3 concentrator fails during normal operation, no action is taken as no L2TPv3 tunnels will be active on the device.

2.2.3.3 Local Controller Failure

If the active Controller at the remote site fails, the standby controller will transition to an active state and will become the cluster master for the site. The L2TPv3 tunnel will be automatically initiated to the active L2TPv3 concentrator in the data center. All the Access Points at the site will re-adopt to the standby controller.

Upon recovery the standby Controller will transition back to a standby state and the primary controller will become the cluster master for the site. Any established L2TPv3 tunnels will be torn down and re-established by the active Controller.

2.2.4 Configuration

2.2.4.1 L2TPv3 Concentrators

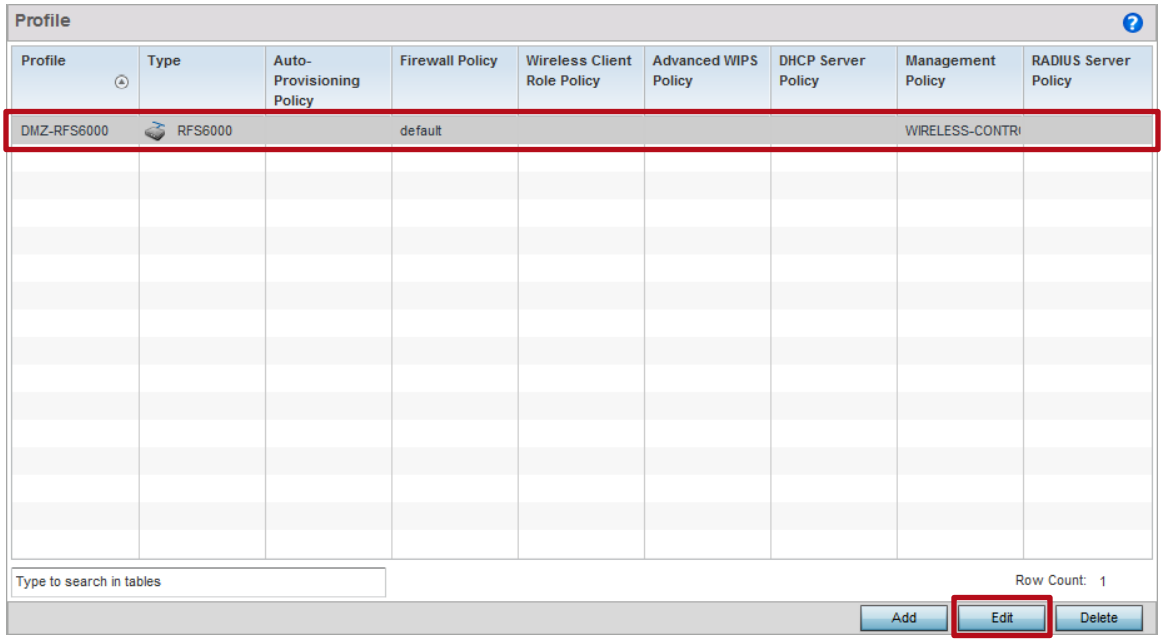
Each of the L2TPv3 tunnels from the local RFSX000 Controllers at the remote sites terminate on a pair of RFSX000 Controllers in the data center operating as L2TPv3 concentrators. The L2TPv3 tunnel configuration on the L2TPv3 concentrators is defined using a common profile that is assigned to both RFSX000 Controllers. The L2TPv3 configuration includes a single peer definition that supports wildcards allowing the RFSX000 Controllers to terminate multiple L2TPv3 tunnels without having to define individual L2TPv3 peer entries.

The L2TPv3 tunnel configuration for the L2TPv3 concentrators includes the following parameters:

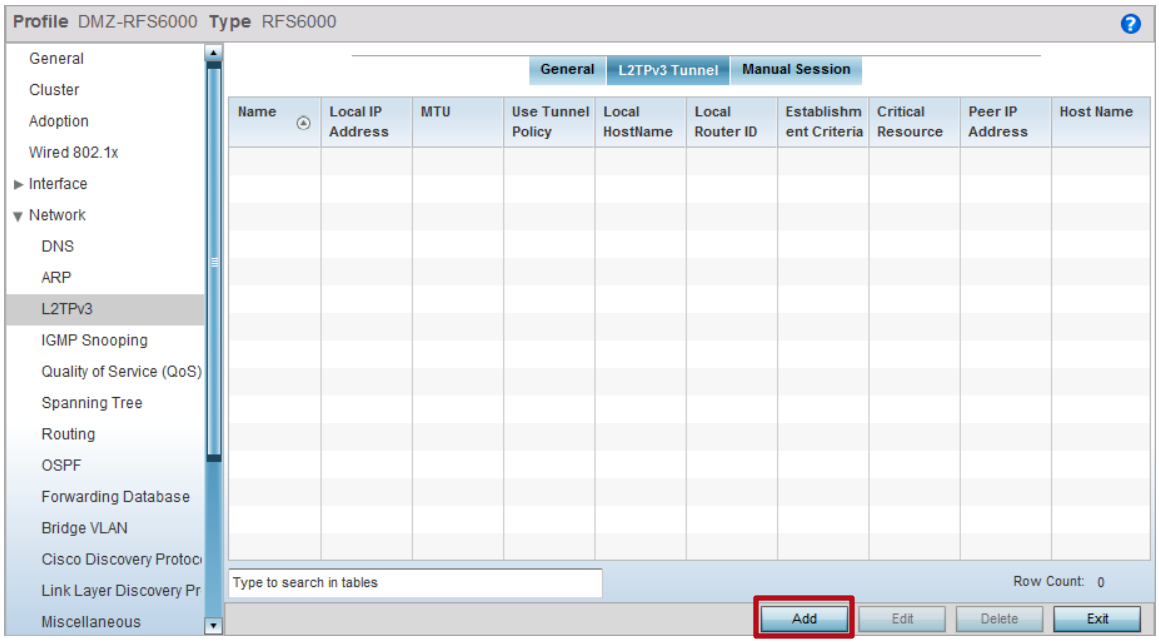
1. The L2TPv3 tunnel ***Name*** is defined as ***vlan25*** (Guest VLAN ID).
2. The ***Establishment Criteria*** is set to ***Cluster Master***.
3. The L2TPv3 ***Peer 1*** entry is defined with the ***Router ID*** and ***Host Name*** set to ***Any*** permitting tunnels from multiple remote peers. This eliminates the need for defining separate L2TPv3 peer entries for each Access Point.
4. The L2TPv3 ***Encapsulation*** is set to ***IP*** which utilizes ***Protocol 115***. Encapsulation can optionally be set to ***UDP*** which utilizes UDP port ***1701***.
5. One L2TPv3 ***Session*** is defined with the name set to ***vlan25*** and ***Pseudowire ID*** and ***Traffic Source Value*** set to ***25*** (Guest VLAN ID).

The following steps demonstrate how to define the L2TPv3 tunnel parameters for a pair of RFSX000 Controllers operating as L2TPv3 concentrators using a profile. This assumes the RFSX000 Controllers are up and operational on the network and the cluster has been pre-established. This also assumes that one of the RFSX000 Controllers is designated as the cluster master and the secondary Controller is operating in a standby mode:

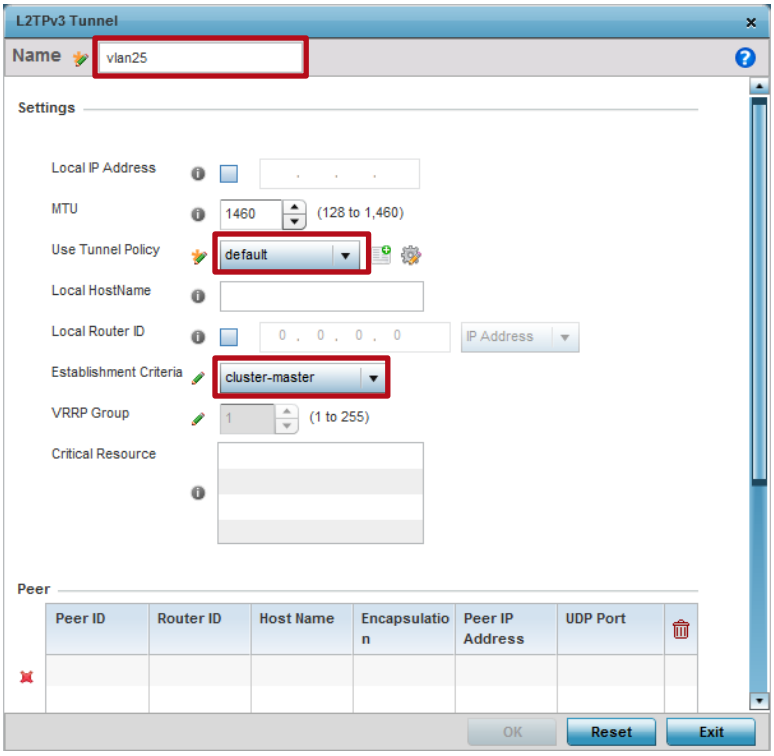
1 Using the Web-UI select *Configuration → Profile → <profile-name> → Edit:*



2 Select *Network* → *L2TPv3* → *L2TPv3 Tunnel* → *Add*:

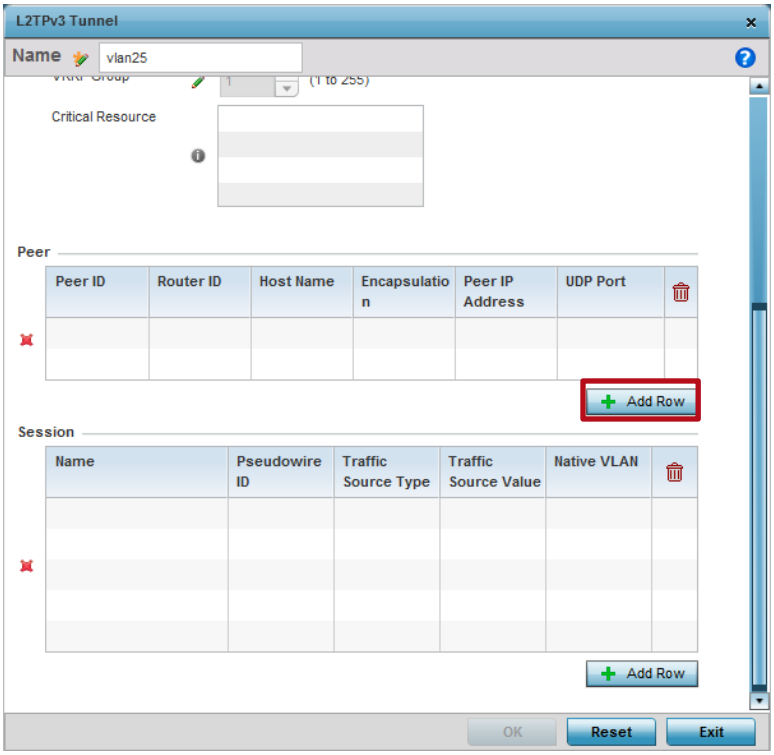


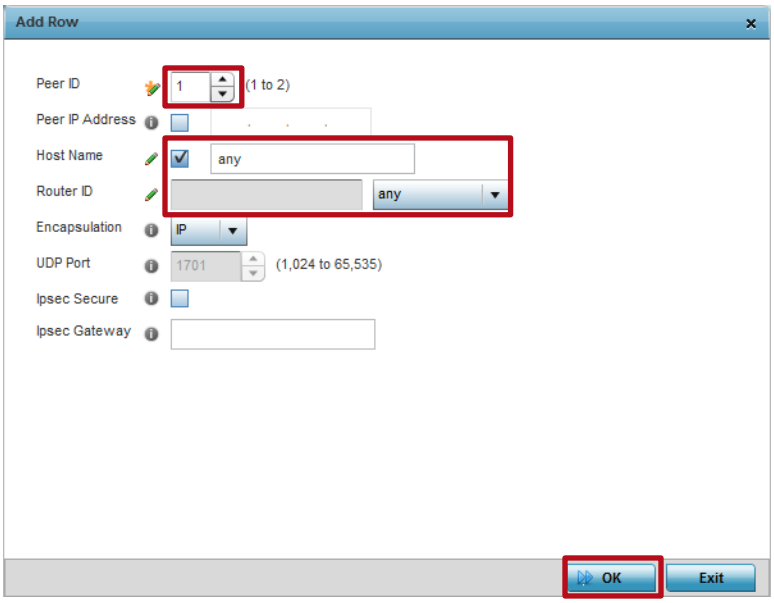
3 Enter a *Name* to identify the tunnel then select the *Tunnel Policy* named *default*. Set the *Establishment Criteria* to *Cluster Master:*



4 Under *Peer* select *Add Row*. Define the following parameters then click *OK*:

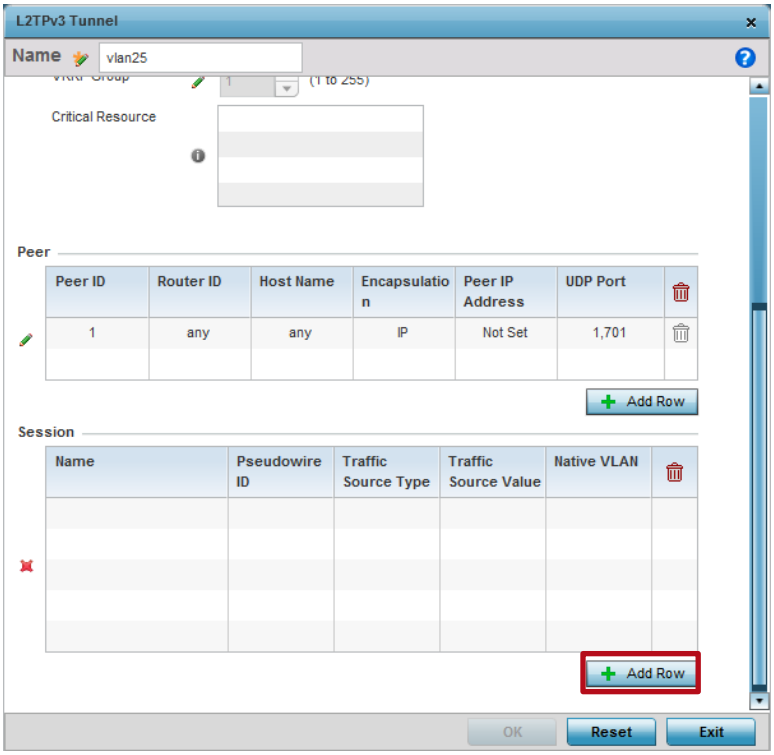
- **a. Set the *Peer ID* to *1*.**
- **b. Enter the *Host Name* value *any*.**
- **c. Set the *Router ID* to *any*.**

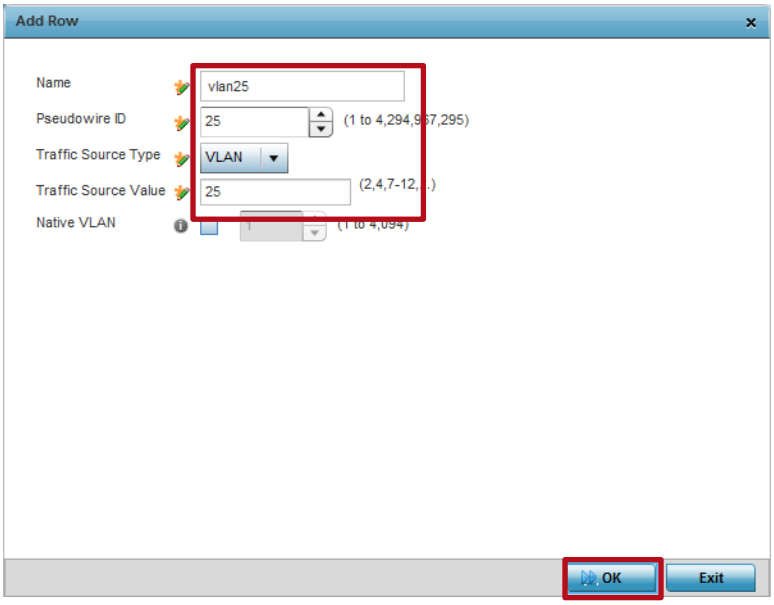




5 Under *Session* select *Add Row*. Define the following parameters then click *OK* and *Exit*:

- **a. Enter the *Name* to identify the session.**
- **b. Enter a Psuedowire ID. It is recommended that this match the Guest VLAN ID!**
- **c. Set the *Traffic Source Type* to *VLAN.***
- **d. Enter the *Traffic Source Value*. Note this must match the Guest VLAN ID!**





6 *Commit and Save* the changes:

The following changes were applied to the L2TPv3 Concentrators Profile:

```
!
profile rfs6000 DMZ-RFS6000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
!
! Configuration Removed for Brevity
!
l2tpv3 tunnel vlan25
  peer 1 hostname any router-id any
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria cluster-master
!
```

Note – By default the ability to tunnel traffic between L2TPv3 tunnels is disabled. This can optionally be enabled in the Controllers L2TPv3 configuration in the profile if hosts at different sites need to communicate over the L2TPv3 tunnels.

*Note – The **pseudowire-id** and **traffic-source** VLAN IDs must match on both L2TPv3 peers. In the above example guest VLAN 25 is being transported over the tunnel named **vlan25** which has the **pseudowire-id** and traffic-source set to **25**. The pseudowire-id and tunnel name may be any alpha numerical string as required.*

2.2.4.2 Local Controllers

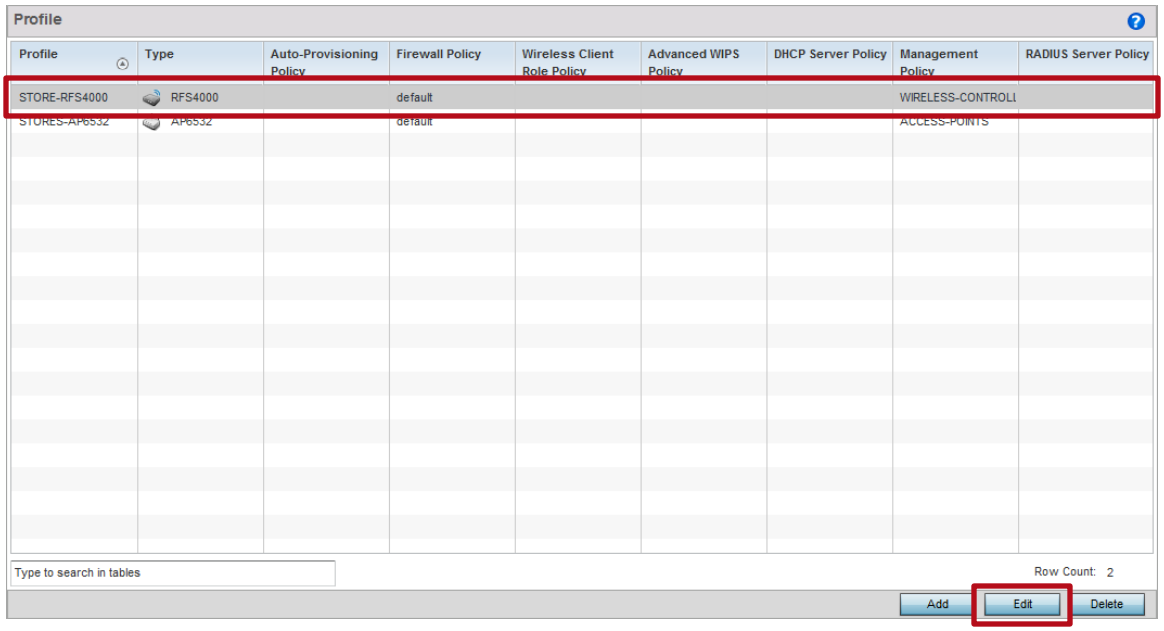
Each of the RFSX000 Controllers operating as a cluster masters at the remote sites initiate a single L2TPv3 tunnel to the active or standby L2TPv3 concentrator in the data center. During normal operation the L2TPv3 tunnel is established to the active L2TPv3 concentrator defined as peer 1 and during a failure event the L2TPv3 tunnel will automatically failover to the standby L2TPv3 concentrator defined as peer 2.

The L2TPv3 tunnel configuration is defined using profiles that are assigned to the local RFSX000 Controllers at each site. The L2TPv3 tunnel configuration includes the following parameters:

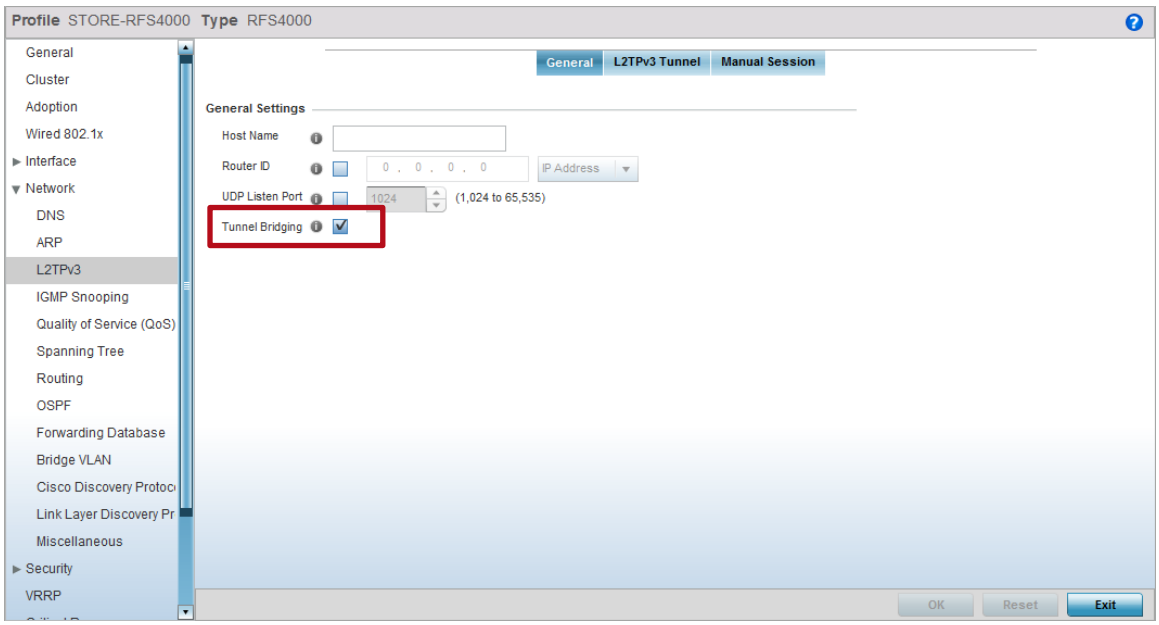
1. ***Inter Tunnel Bridging*** is ***enabled*** so that traffic from the Tunneled Wireless LANs can be bridged to the L2TPv3 tunnel.
2. The L2TPv3 tunnel ***Name*** is defined as ***vlan25***.
3. The ***Establishment Criteria*** is set to ***RF Domain Manager***.
4. The L2TPv3 ***Peer 1*** entry is defined with the ***Peer IP Address*** set to ***192.168.23.20*** and the ***Host Name*** set to ***L2TPV3-GW-1***. The defined IP Address and Hostname match the IP Address and Hostname assigned to the primary Controller in the data center.
5. The L2TPv3 ***Peer 2*** entry is defined with the ***Peer IP Address*** set to ***192.168.23.21*** and the ***Host Name*** set to ***L2TPV3-GW-2***. The defined IP Address and Hostname match the IP Address and Hostname assigned to the secondary Controller in the data center.
6. The L2TPv3 ***Encapsulation*** is set to ***IP*** which utilizes ***Protocol 115***. Encapsulation can optionally be set to ***UDP*** which utilizes UDP port ***1701***.
7. One L2TPv3 ***Session*** is defined with the name set to ***vlan25*** and ***Pseudowire ID*** and ***Traffic Source Value*** set to ***25***.

The following steps demonstrate how to define the L2TPv3 tunnel parameters for a pair of local RFSX000 Controllers at each site using a profile. This assumes the RFSX000 Controllers are up and operational on the network and the cluster has been pre-established. This also assumes that one of the RFSX000 Controllers is designated as the cluster master and the secondary Controller is operating in a standby mode:

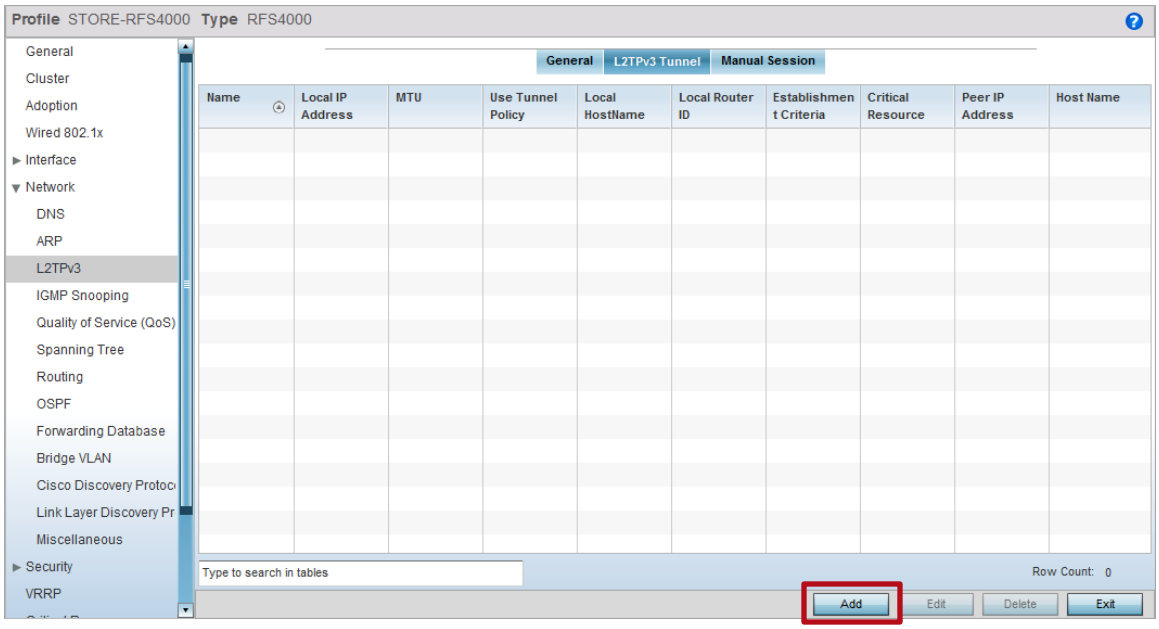
1 Using the Web-UI select *Configuration → Profile → <profile-name> → Edit:*



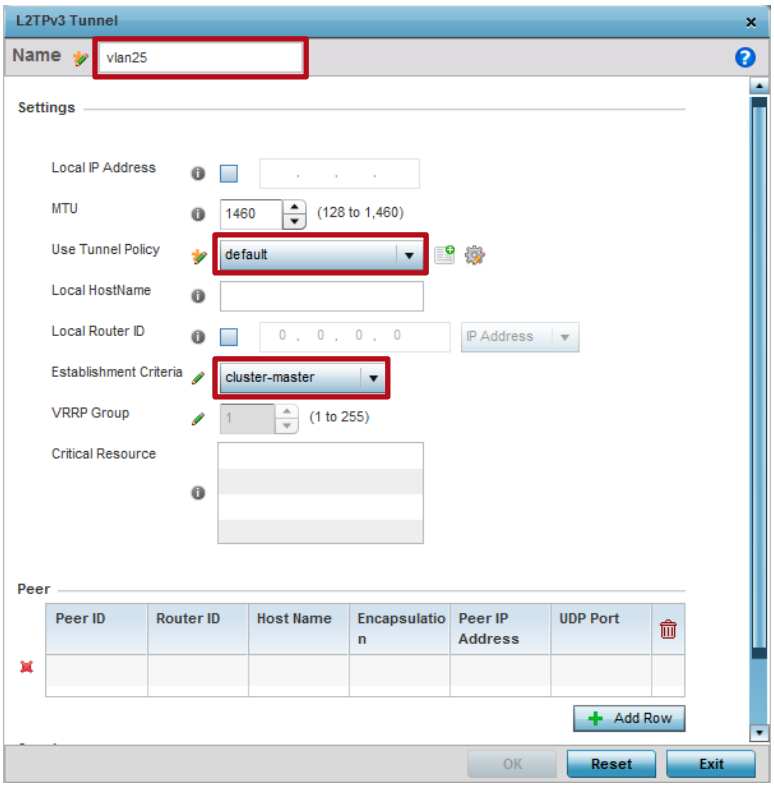
2 Select *Network → L2TPv3 → General*. Enable *Tunnel Bridging* then click *OK*:



3 Select *Network* → *L2TPv3* → *L2TPv3 Tunnel* → *Add*:

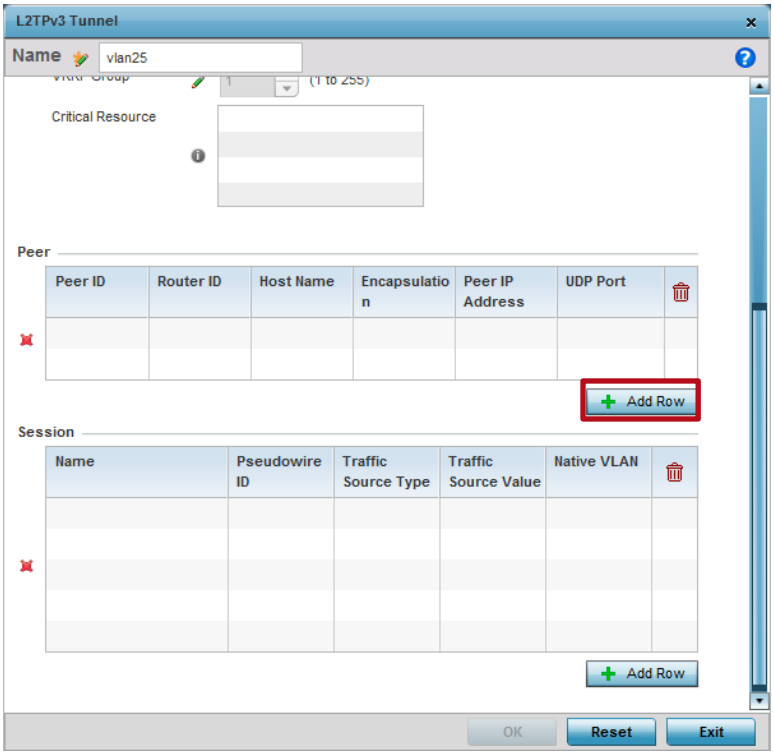


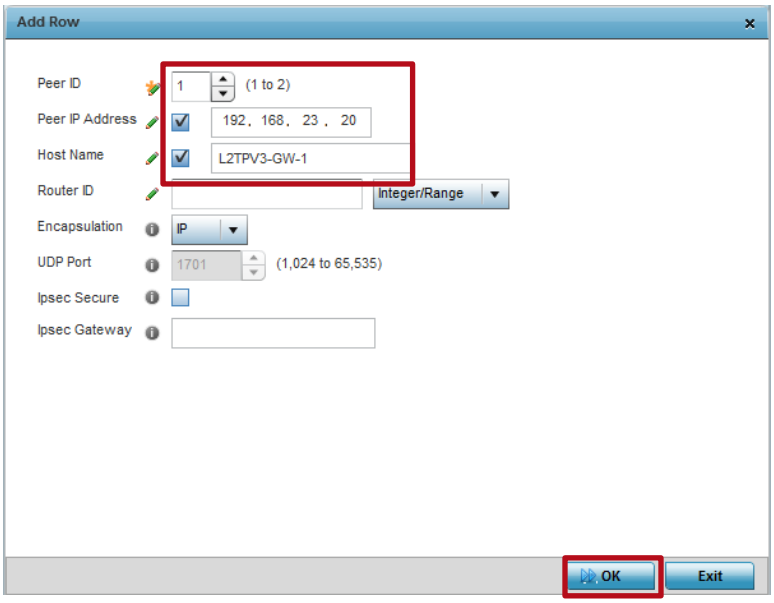
4 Enter a *Name* to identify the tunnel then select the *Tunnel Policy* named *default*. Set the *Establishment Criteria* to *Cluster Master:*



5 Under *Peer* select *Add Row*. Define the following parameters then click *OK*:

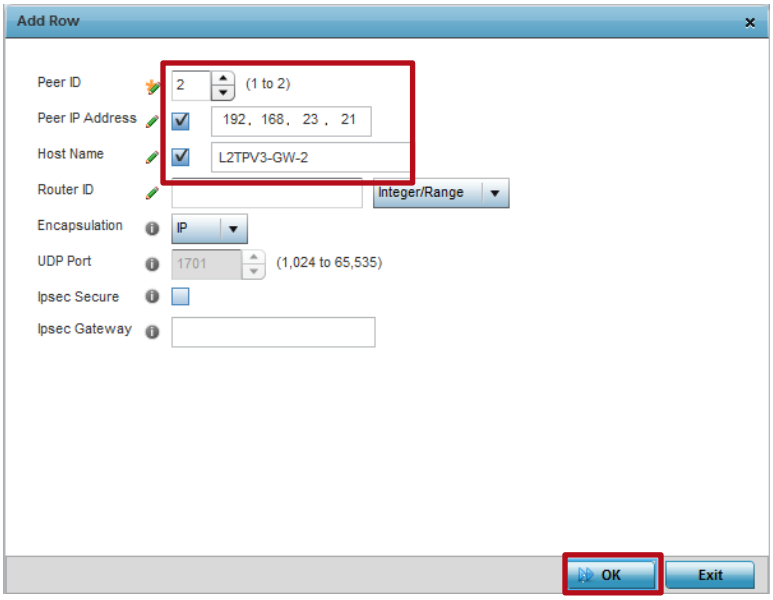
- **a. Set the *Peer ID* to *1*.**
- **b. Set the Peer IP Address to 192.168.23.20 (active L2TPv3 concentrator's IP address).**
- **c. Enter the *Host Name* value *L2TPV3-GW-1* (active L2TPv3 concentrator's hostname).**





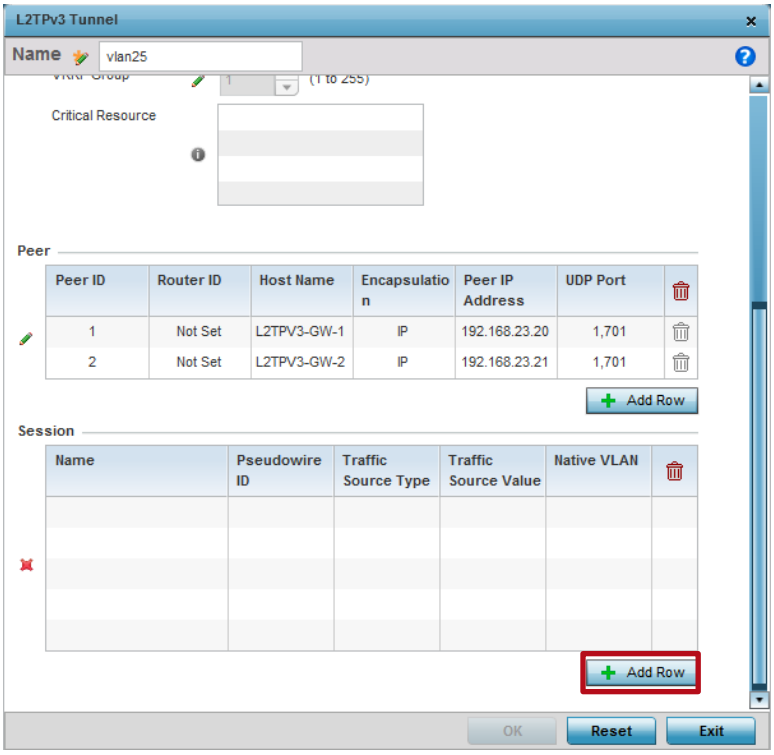
6 Click Add Row and define a second peer. Define the following parameters then click *OK*:

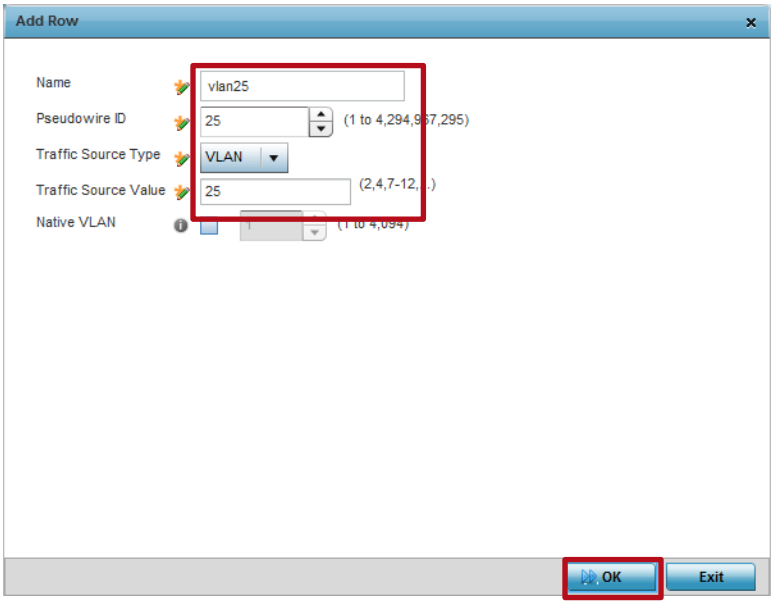
- **a. Set the *Peer ID* to 2.**
- **b. Set the Peer IP Address to 192.168.23.21 (standby L2TPv3 concentrator's IP address).**
- **c. Enter the *Host Name* value *L2TPV3-GW-2* (standby L2TPv3 concentrator's hostname).**



7 Under *Session* select *Add Row*. Define the following parameters then click *OK* and *Exit*:

- **a. Enter the *Name* to identify the session.**
- **b. Enter a Psuedowire ID. It is recommended that this match the Guest VLAN ID!**
- **c. Set the *Traffic Source Type* to *VLAN.***
- **d. Enter the *Traffic Source Value*. Note this must match the Guest VLAN ID!**





8 *Commit and Save* the changes:

The following changes were applied to the L2TPv3 Concentrators Profile:

```
!
profile rfs4000 STORE-RFS4000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
!
! Configuration Removed for Brevity
!
l2tpv3 tunnel vlan25
  peer 1 ip-address 192.168.23.20 hostname L2TPV3-GW-1
  peer 2 ip-address 192.168.23.21 hostname L2TPV3-GW-2
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria cluster-master
 l2tpv3 inter-tunnel-bridging
!
```

Note – Inter Tunnel Bridging must be enabled for the guest user traffic to be bridged between the Extended VLAN and the L2TPv3 tunnel.

*Note – The **pseudowire-id** and **traffic-source** VLAN IDs must match on both L2TPv3 peers. In the above example guest VLAN 25 is being transported over the tunnel named **vlan25** which has the **pseudowire-id** and traffic-source set to **25**. The pseudowire-id and tunnel name may be any alpha numerical string as required.*

3. Verification

3.1 L2TPv3 Tunnel Summaries

A summary of the established L2TPv3 tunnels can be viewed using the CLI or Web-UI on a per device basis. The tunnels and information that are displayed on the device will depend on if the device is initiating or terminating the L2TPv3 tunnel.

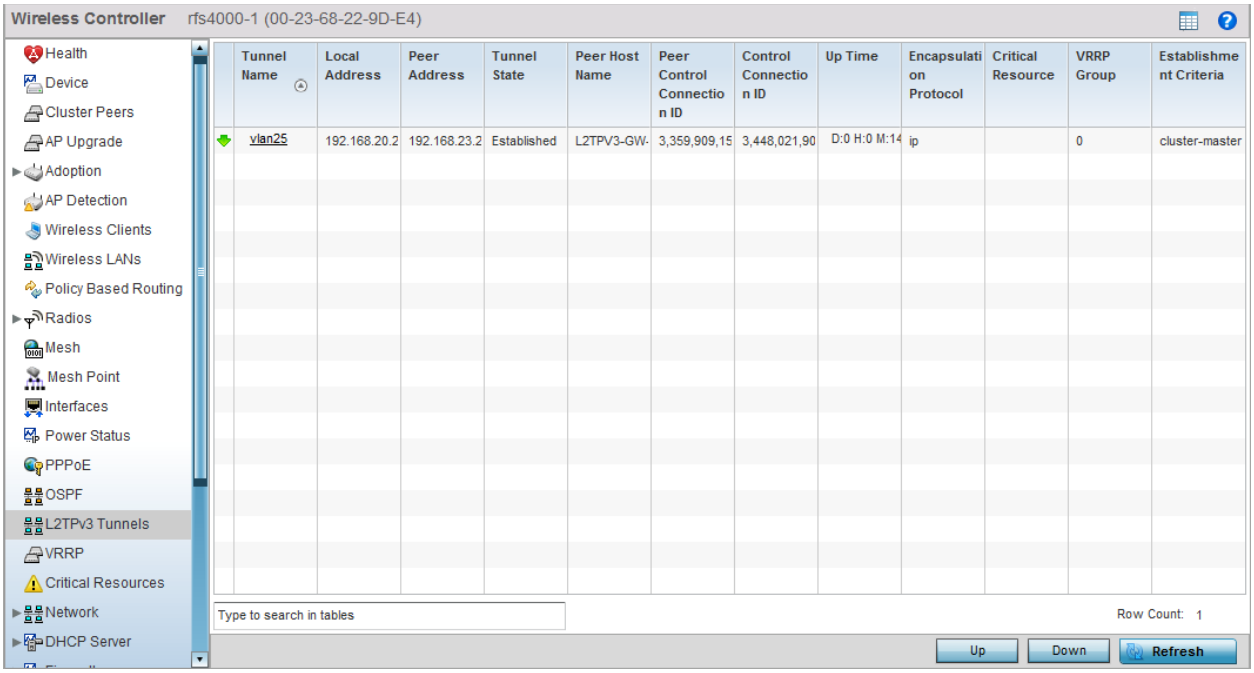
For devices that are initiating the tunnel such as an elected RF Domain Manager or active Controller (i.e. cluster master) at the remote site, the l2TPv3 tunnel summary will display each tunnel with an ***Established*** state. Non RF Domain Managers and the standby Controllers will display the tunnel with a ***STANDBY*** state. The name for each tunnel will match the name you defined in the profile.

For RFSX000 Controllers running as L2TPv3 concentrators in the data center that are terminating the L2TPv3 tunnels, the L2TPv3 tunnel summary will display each tunnel with an ***Established*** state on the active Controller (i.e. cluster master). No tunnels will be displayed on the standby device. The name for each tunnel will include the tunnel name combined with the peer devices hostname.

A summary of L2TPv3 tunnels can be viewed per device using the CLI by issuing the ***show l2tpv3 tunnel-summary on <device-hostname>*** command:

```
-------------------------------------------------------------------------------------------------------
Sl No  Tunnel Name                    Tunnel State       Estd/Total Sessions   Encapsulation Protocol
-------------------------------------------------------------------------------------------------------
 1     vlan25                         Established             1/1             IP
Total Number of Tunnels 1
```

A summary of L2TPv3 tunnels can be viewed per device using the Web-UI by selecting ***Statistics → <rf-domain-name> → <device-hostname> → L2TPv3 Tunnels***:



3.2 L2TPv3 Tunnel Details

Details for each L2TPv3 tunnel can also be displayed in the CLI and Web-UI on a per device per tunnel basis. The tunnel details allow administrators to verify the remote peers each tunnel is established with in addition to providing detailed traffic statistics.

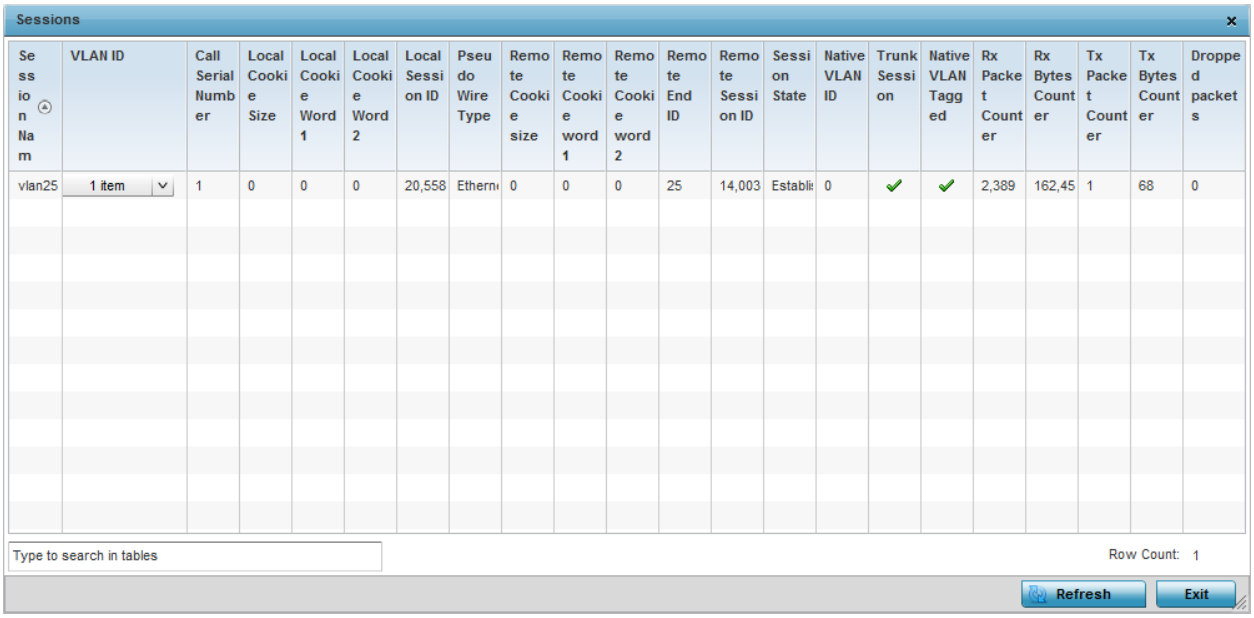
For devices that are initiating the L2TPv3 tunnel, the tunnel names will match the tunnel name assigned in the profile or override. For devices that are terminating the L2TPv3 tunnel, the tunnel name will include the tunnel name combined with the peer devices hostname. The tunnel name is important when viewing the statistics using the CLI.

Detailed L2TPv3 tunnel information can be viewed per device using the CLI by issuing the ***show l2tpv3 tunnel <tunnel-name> on <device-hostname>*** command:

```
------------------------------------------------------------------------------
Tunnel Name : vlan25
  Control connection id : 2868343703
  Peer Address : 192.168.23.20
  Local Address : 192.168.21.105
  Encapsulation Protocol : IP
  MTU : 1460
  Peer Host Name : L2TPV3-GW-1
  Peer Vendor Name : Motorola Solutions
  Peer Control Connection ID : 4053361539
  Tunnel State : Established
  Establishment Criteria : rf-domain-manager
  Sequence number of the next msg to the peer : 4
  Expected sequence number of the next msg from the peer :2
  Sequence number of the next msg expected by the peer : 4
  Retransmission count : 0
  Reconnection count : 0
  Uptime : 0 days 1 hours 38 minutes 41 seconds
  ------------------------------------------------------------------------------
  Session Name : vlan25
    VLANs : 25
    Pseudo Wire Type : Ethernet_VLAN
    Serial number for the session : 2
    Local Session ID : 226443017
    Remote Session ID : 9776015
    Size of local cookie (0, 4 or 8 bytes) : 0
    First word of local cookie : 0
    Second word of local cookie : 0
    Size of remote cookie (0, 4 or 8 bytes) : 0
    First word of remote cookie : 0
    Second word of remote cookie : 0
    Session state : Established
    Remote End ID : 25
    Trunk Session : 1
    Native VLAN tagged : Enabled
    Native VLAN ID : 0
```

```
Number of packets received : 8938
Number of bytes received : 822566
Number of packets sent : 6154
Number of bytes sent : 628880
Number of packets dropped : 0
```

The L2TPv3 tunnel summary for each device can be viewed using the Web-UI by selecting ***Statistics → <rf-domain-name> → <device-hostname> → L2TPv3 Tunnels → <tunnel-name>***:



4. Appendix

4.1 Running Configurations

4.1.1 Centralized Controller Deployment

L2TPv3 Concentrators:

```
!
! Configuration of RFS6000 version 5.4.0.0-027B
!
!
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
 permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
!
management-policy WIRELESS-CONTROLLERS
 no http server
 https server
 ssh
```

```
 user admin password 0 motorola role superuser access all
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
!
l2tpv3 policy default
!
profile rfs6000 DMZ-RFS6000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface up1
  description UPLINK
  switchport mode trunk
  switchport trunk native vlan 23
  switchport trunk native tagged
  switchport trunk allowed vlan 23,25
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
```

```
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge6
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge7
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge8
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use management-policy WIRELESS-CONTROLLERS
 use firewall-policy default
 ntp server 192.168.10.6
 no auto-learn-staging-config
 service pm sys-restart
 router ospf
 l2tpv3 tunnel vlan25
  peer 1 hostname any router-id any
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria cluster-master
!
rf-domain DMZ
 no country-code
!
rf-domain default
 no country-code
!
rfs6000 00-23-68-64-43-5A
 use profile DMZ-RFS6000
 use rf-domain DMZ
 hostname L2TPV3-GW-1
 ip default-gateway 192.168.23.1
 interface vlan23
  ip address 192.168.23.20/24
 cluster name DMZ
 cluster member ip 192.168.23.21
```

```
 cluster master-priority 254
 logging on
 logging console warnings
 logging buffered warnings
!
rfs6000 5C-0E-8B-17-E8-F6
 use profile DMZ-RFS6000
 use rf-domain DMZ
 hostname L2TPV3-GW-2
 ip default-gateway 192.168.23.1
 interface vlan23
  ip address 192.168.23.21/24
 cluster name DMZ
 cluster mode standby
 cluster member ip 192.168.23.20
 cluster master-priority 128
 logging on
 logging console warnings
 logging buffered warnings
!
!
end
```

Centralized Controllers:

```
!
! Configuration of RFS4000 version 5.4.0.0-027B
!
!
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
 permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
!
firewall-policy default
 no ip dos tcp-sequence-past-window
```

```
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
wlan TMELABS-L2TPV3
 ssid TMELABS-L2TPV3
 vlan 25
 bridging-mode local
 encryption-type none
 authentication-type none
!
smart-rf-policy STORES
!
auto-provisioning-policy DATACENTER
 adopt ap6532 precedence 1 profile STORES-AP6532 rf-domain STORE1 ip 192.168.21.0/24
!
!
management-policy ACCESS-POINTS
 no http server
 ssh
 user admin password 0 motorola role superuser access all
 no snmp-server manager v2
 no snmp-server manager v3
!
management-policy WIRELESS-CONTROLLERS
 no http server
 https server
 ssh
 user admin password 0 motorola role superuser access all
 user guestadmin password 0 motorola role web-user-admin
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
!
l2tpv3 policy default
!
profile rfs4000 DATACENTER-RFS4000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
```

```
no autoinstall configuration
no autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface radio1
interface radio2
interface up1
 description UPLINK
 switchport mode trunk
 switchport trunk native vlan 20
 switchport trunk native tagged
 switchport trunk allowed vlan 20
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge1
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge2
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge3
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge4
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge5
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface wwan1
interface pppoe1
use management-policy WIRELESS-CONTROLLERS
use firewall-policy default
```

```
 use auto-provisioning-policy DATACENTER
 ntp server 192.168.10.6
 no auto-learn-staging-config
 service pm sys-restart
 router ospf
!
profile ap6532 STORES-AP6532
 bridge vlan 25
  bridging-mode tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto load-management
 interface radio1
  wlan TMELABS-L2TPV3 bss 1 primary
 interface radio2
  wlan TMELABS-L2TPV3 bss 1 primary
 interface ge1
  description UPLINK
  switchport mode trunk
  switchport trunk native vlan 21
  no switchport trunk native tagged
  switchport trunk allowed vlan 21-22
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan21
  ip address dhcp
  ip dhcp client request options all
 interface pppoe1
 use management-policy ACCESS-POINTS
 use firewall-policy default
 ntp server 192.168.10.6
 service pm sys-restart
```

```
 router ospf
 l2tpv3 tunnel vlan25
  peer 1 ip-address 192.168.23.20 hostname L2TPV3-GW-1
  peer 2 ip-address 192.168.23.21 hostname L2TPV3-GW-2
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria rf-domain-manager
 l2tpv3 inter-tunnel-bridging
!
rf-domain DATACENTER
 location JohnsonCityTN
 contact kmarshall@motorolasolutions.com
 timezone EST5EDT
 country-code us
!
rf-domain STORE1
 location JohnsonCityTN
 contact kmarshall@motorolasolutions.com
 timezone EST5EDT
 country-code us
 use smart-rf-policy STORES
 control-vlan 21
!
rf-domain default
 no country-code
!
rfs4000 00-23-68-22-9D-E4
 use profile DATACENTER-RFS4000
 use rf-domain DATACENTER
 hostname rfs4000-1
 license AP DEFAULT-6AP-LICENSE
 license AAP <string>
 license ADVANCED-WIPS <string>
 license ADSEC <string>
 ip default-gateway 192.168.20.1
 interface vlan20
  ip address 192.168.20.20/24
 cluster name DATACENTER
 cluster member ip 192.168.20.21 level 2
 cluster master-priority 254
 logging on
 logging console warnings
 logging buffered warnings
!
rfs4000 5C-0E-8B-1A-FE-A0
 use profile DATACENTER-RFS4000
```

```
 use rf-domain DATACENTER
 hostname rfs4000-2
 license AP DEFAULT-6AP-LICENSE
 license AAP <string>
 license ADVANCED-WIPS <string>
 license ADSEC <string>
 ip default-gateway 192.168.20.1
 interface vlan20
  ip address 192.168.20.21/24
 cluster name DATACENTER
 cluster mode standby
 cluster member ip 192.168.20.20 level 2
 cluster master-priority 128
 logging on
 logging console warnings
 logging buffered warnings
!
ap6532 00-23-68-31-20-A4
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP1
!
ap6532 00-23-68-86-44-A0
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP2
!
ap6532 5C-0E-8B-33-EE-70
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP3
!
ap6532 5C-0E-8B-A4-48-80
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP4
!
ap6532 5C-0E-8B-A4-4B-48
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP5
!
ap6532 5C-0E-8B-A4-4C-3C
 use profile STORES-AP6532
 use rf-domain STORE1
```

```
 hostname STORE1-AP6
!
!
end
```

4.1.2 Local Controller Deployment

L2TPv3 Concentrators:

```
!
! Configuration of RFS6000 version 5.4.0.0-027B
!
!
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
 permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
!
management-policy WIRELESS-CONTROLLERS
 no http server
 https server
 ssh
```

```
 user admin password 0 motorola role superuser access all
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
!
l2tpv3 policy default
!
profile rfs6000 DMZ-RFS6000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface up1
  description UPLINK
  switchport mode trunk
  switchport trunk native vlan 23
  switchport trunk native tagged
  switchport trunk allowed vlan 23,25
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
```

```
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge6
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge7
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge8
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use management-policy WIRELESS-CONTROLLERS
 use firewall-policy default
 ntp server 192.168.10.6
 no auto-learn-staging-config
 service pm sys-restart
 router ospf
 l2tpv3 tunnel vlan25
  peer 1 hostname any router-id any
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria cluster-master
!
rf-domain DMZ
 no country-code
!
rf-domain default
 no country-code
!
rfs6000 00-23-68-64-43-5A
 use profile DMZ-RFS6000
 use rf-domain DMZ
 hostname L2TPV3-GW-1
 ip default-gateway 192.168.23.1
 interface vlan23
  ip address 192.168.23.20/24
 cluster name DMZ
 cluster member ip 192.168.23.21
```

```
 cluster master-priority 254
 logging on
 logging console warnings
 logging buffered warnings
!
rfs6000 5C-0E-8B-17-E8-F6
 use profile DMZ-RFS6000
 use rf-domain DMZ
 hostname L2TPV3-GW-2
 ip default-gateway 192.168.23.1
 interface vlan23
  ip address 192.168.23.21/24
 cluster name DMZ
 cluster mode standby
 cluster member ip 192.168.23.20
 cluster master-priority 128
 logging on
 logging console warnings
 logging buffered warnings
!
!
end
```

Local Controllers:

```
!
! Configuration of RFS4000 version 5.4.0.0-027B
!
!
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
 permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
!
firewall-policy default
 no ip dos tcp-sequence-past-window
```

```
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
wlan TMELABS-L2TPV3
 ssid TMELABS-L2TPV3
 vlan 25
 bridging-mode tunnel
 encryption-type none
 authentication-type none
!
smart-rf-policy STORE1
!
auto-provisioning-policy STORE1
 adopt ap6532 precedence 1 profile STORES-AP6532 rf-domain STORE1 ip 192.168.21.0/24
!
!
management-policy ACCESS-POINTS
 no http server
 ssh
 user admin password 0 motorola role superuser access all
 no snmp-server manager v2
 no snmp-server manager v3
!
management-policy WIRELESS-CONTROLLERS
 no http server
 https server
 ssh
 user admin password 0 motorola role superuser access all
 user guestadmin password 0 motorola role web-user-admin
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
!
l2tpv3 policy default
!
profile rfs4000 STORE-RFS4000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
```

```
no autoinstall configuration
no autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface radio1
interface radio2
interface up1
 description UPLINK
 switchport mode trunk
 switchport trunk native vlan 20
 switchport trunk native tagged
 switchport trunk allowed vlan 20
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge1
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge2
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge3
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge4
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge5
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface wwan1
interface pppoe1
use management-policy WIRELESS-CONTROLLERS
use firewall-policy default
```

```
 use auto-provisioning-policy STORE1
 ntp server 192.168.10.6
 no auto-learn-staging-config
 service pm sys-restart
 router ospf
l2tpv3 tunnel vlan25
  peer 1 ip-address 192.168.23.20 hostname L2TPV3-GW-1
  peer 2 ip-address 192.168.23.21 hostname L2TPV3-GW-2
  session vlan25 pseudowire-id 25 traffic-source vlan 25
  establishment-criteria cluster-master
 l2tpv3 inter-tunnel-bridging
!
profile ap6532 STORES-AP6532
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto load-management
 interface radio1
  wlan TMELABS-L2TPV3 bss 1 primary
 interface radio2
  wlan TMELABS-L2TPV3 bss 1 primary
 interface ge1
  description UPLINK
  switchport mode trunk
  switchport trunk native vlan 21
  no switchport trunk native tagged
  switchport trunk allowed vlan 21-22
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan21
  ip address dhcp
  ip dhcp client request options all
 interface pppoe1
 use management-policy ACCESS-POINTS
 use firewall-policy default
```

```
 ntp server 192.168.10.6
 service pm sys-restart
 router ospf
!
rf-domain STORE1
 location JohnsonCityTN
 contact kmarshall@motorolasolutions.com
 timezone EST5EDT
 country-code us
 use smart-rf-policy STORE1
!
rf-domain default
 no country-code
!
rfs4000 00-23-68-22-9D-E4
 use profile STORE-RFS4000
 use rf-domain STORE1
 hostname rfs4000-1
 license AP DEFAULT-6AP-LICENSE
 license AAP <string>
 license ADVANCED-WIPS <string>
 license ADSEC <string>
 ip default-gateway 192.168.20.1
 interface vlan20
  ip address 192.168.20.20/24
 cluster name STORE1
 cluster member ip 192.168.20.21
 cluster master-priority 254
 logging on
 logging console warnings
 logging buffered warnings
!
rfs4000 5C-0E-8B-1A-FE-A0
 use profile DATACENTER-RFS4000
 use rf-domain DATACENTER
 hostname rfs4000-2
 license AP DEFAULT-6AP-LICENSE
 license AAP <string>
 license ADVANCED-WIPS <string>
 license ADSEC <string>
 ip default-gateway 192.168.20.1
 interface vlan20
  ip address 192.168.20.21/24
 cluster name STORE1
 cluster mode standby
```

```
 cluster member ip 192.168.20.20
 cluster master-priority 128
 logging on
 logging console warnings
 logging buffered warnings
!
ap6532 00-23-68-31-20-A4
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP1
!
ap6532 00-23-68-86-44-A0
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP2
!
ap6532 5C-0E-8B-33-EE-70
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP3
!
ap6532 5C-0E-8B-A4-48-80
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP4
!
ap6532 5C-0E-8B-A4-4B-48
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP5
!
ap6532 5C-0E-8B-A4-4C-3C
 use profile STORES-AP6532
 use rf-domain STORE1
 hostname STORE1-AP6
!
!
end
```


MOTOROLA SOLUTIONS