VPN Simulation

The WAE Design virtual private network (VPN) model is a representation of a virtual subnetwork within the plan file. Viewing and simulating VPN within WAE Design facilitates many network tasks and can answer questions, such as:

- Which VPNs are on my network? Where and how are they configured?
- Which VPNs are using congested interfaces?
- Which VPNs will experience congestion under any of a given list of failure scenarios?
- Which failures scenarios cause the worst-case congestion or latency for a VPN?

There are many varieties of VPNs. For example, there are Layer 2 (L2) VPNs and Layer 3 (L3) VPNs, each with different categories within it, and there are vendor-specific VPN implementations. Each VPN type has its own specific configuration and terminology. The WAE Design VPN model supports a number of these VPN types based on either route-target or full-mesh connectivity.

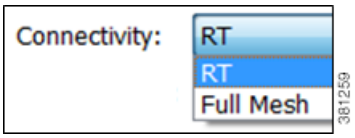
VPN Model

VPN Objects

Object	Description	Examples
VPNs	A set of VPN nodes that can exchange data with each other.	• Layer 2 VPN: The VPN represents an individual VPLS containing virtual switch interfaces (VSIs). • Layer 3 VPN: The VPN represents sets of VRFs associated with a set of VPN nodes that forward traffic between themselves. Often, this set of VRFs signifies a single customer or service.
VPN nodes	Connection points in a VPN. They exist on standard nodes, and each node can contain multiple VPN nodes. A VPN node can be in only one VPN.	• Layer 2 VPN: The VPN node represents the VSIs configured on each router. • Layer 3 VPN: The VPN node represents the VRF instances configured on each router.

VPN Topology and Connectivity

WAE Design VPN topology route connections are established through route targets (RTs) or through a full mesh of VPN nodes. The Connectivity property is set in the VPN Properties dialog box.



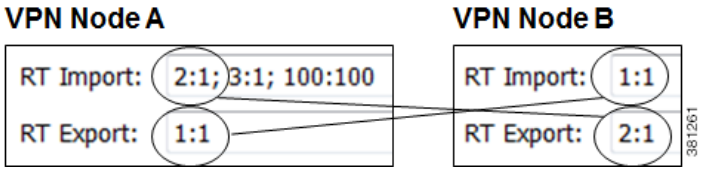
Knowing a VPN's topology and connectivity lets WAE Design calculate which demands between VPN nodes carry traffic for a particular VPN, and thus which interfaces carry traffic for that VPN. In turn, WAE Design can calculate the vulnerability of a VPN to certain failure and congestion scenarios.

A demand is associated with a VPN, meaning it carries traffic for that VPN, if the following is true:

- The two VPN nodes are in the same VPN.
- The demand is in the same service class as the VPN.
- Only for VPNs with RT connectivity, the RT Export property of one VPN node must match the RT Import property of another VPN node.

Once demands are associated with the VPN, this configuration simulates the associated access circuits exchanging traffic as if they were on the same LAN.

Note that a demand associated with a VPN can additionally contain other traffic that is for that VPN.

Connectivity	Description
Full mesh	Full-mesh connectivity is a complete mesh of connections between VPN nodes in a VPN so they can all communicate with one each other. This connectivity is typical in a VPLS, where all VSIs identify one another based on a common AGI.
Route targets	Route targets model the more complex connectivity used in Layer 3 VPNs, such as hub-and-spoke networks. Here, the VRFs exchange data with one another based on the matching of RT Export and RT Import properties set for each VPN node. Having an import/export pair does not create bidirectional communication. Rather, traffic flows in the opposite direction of the routed advertisements. For example, if node A's RT Import matches node B's RT Export, traffic can flow from node A to B. For traffic to flow from node B back to node A, node B must have an RT Import that matches an RT Export of node A. This combination of matching imported and exported RTs defines which VPN nodes can exchange data. The VPN name identifies the VPN itself. 

VPNs

Each VPN consists of a set of VPN nodes that can exchange data within it. VPNs have three key properties that uniquely identify them and define how the traffic within them is routed:

- Name—Unique name of the VPN.
- Type—Type of VPN. You can choose from the defaults (VPWS, VPLS, or L3VPN), or you can enter a string value to create a new one. Once entered, the new VPN type appears in the drop-down list and is available for other VPNs and VPN nodes.
- Connectivity—Determines how WAE Design calculates connectivity and associated demands for VPNs:
  - Full Mesh—Connectivity is between all nodes in the VPN. WAE Design ignores the RT Import and RT Export properties of the VPN nodes.
  - RT—Connectivity is based on the RT Import and RT Export properties of its VPN nodes.

VPNs Table

The VPNs table lists the VPN properties, its associated service class, traffic, and the number of VPN nodes within that VPN (Table 16-1). For information on QoS measurements, see Quality of Service Simulation. For information on the Worst-Case columns not listed here, see Table 16-3.

Note Because the traffic and QoS calculations are based on all interfaces within the VPN for the service class specified for that VPN, the plot view might differ from the table. For example, the plot view could show Internet traffic while a VPN carrying voice traffic is selected.

Table 16-1 VPNs Table Columns for Normal Operation

Columns	Description
All traffic and QoS violations are based on traffic carried on all interfaces used by the VPN for the service class defined for that VPN.	
Service Class	Service class associated with this VPN. All values within the table are associated with this service class.
Num Nodes	Number of VPN nodes in this VPN.
Util Meas	The maximum measured utilization of all interfaces used by this VPN.
Util Sim	The maximum simulated utilization of all interfaces used by this VPN.
Total Src Traff Meas	Total amount of measured source traffic on this VPN.
Total Dest Traff Meas	Total amount of measured destination traffic on this VPN.
QoS Violation Sim	Maximum QoS violation under normal operations for all simulated traffic for all interfaces used by this VPN. If the number is positive, there is a violation.
QoS Violation Sim (%)	QoS violation as a percent of the total simulated interface capacity.
QoS Violation Meas	Maximum QoS violation under normal operations for all measured traffic for all interfaces used by this VPN. If the number is positive, there is a violation.
QoS Violation Meas (%)	QoS violation as a percent of the total measured interface capacity.

Table 16-1 VPNs Table Columns for Normal Operation (continued)

Columns	Description
Latency	Maximum latency of all demands used by this VPN.
Tags	User-defined identifiers that makes it easy to group VPNs.

VPNs are not selectable from the network plot; you can only select and filter to VPNs through tables. When selected, all VPN nodes within the VPN are highlighted in the plot (Figure 16-1).

Identifying Interfaces Used by VPNs

To view which interfaces are associated with a VPN, right-click a VPN in the VPNs table and choose **Filter to Interfaces**. This is useful for viewing the VPN topology in the network plot. If you then choose all of these filtered interfaces, you can see the VPN outlined in the network plot.

To view which VPNs are associated with an interface, right-click an interface in the Interfaces table and choose **Filter to VPNs**. This is useful for determining which VPNs are affected if a circuit fails or goes down for maintenance.

Note Utilization measurements might be different between the tables because the VPN table calculates measurements only for the service class associated with that VPN.

VPN Nodes

VPN nodes are defined by properties that determine which VPNs the nodes belong to and how the demands are routed. The following are required properties:

- Node—Name of the node on which the VPN node resides. This node name corresponds with one in the Nodes table.
- Type—The type of VPN. You can choose from the defaults (VPWS, VPLS, or L3VPN), or you can enter a string value to create a new one. Once entered, the new VPN type appears in the drop-down list and is available for other VPN nodes and VPNs.
- Name—Name of the VPN node.
- VPN—Name of the VPN in which this VPN node resides. The drop-down lists shows existing VPNs of the same type set in the Type field. You can create a VPN node without setting its VPN, but without it, the VPN node is not included in simulations as a member of any VPN.

To simulate RT connectivity, you must set the VPN Connectivity property to RT and then set the RT Import and RT Export properties on the individual VPN nodes within it.

- RT Import and RT Export—The pairing of RT values identifies which VPN nodes connect with each other. For more information, see VPN Topology and Connectivity.
- (Optional) RD—Route distinguisher (RD) uniquely identifies routes within a VRF as belonging to one VPN or another, thus enabling duplicate routes to be unique within a global routing table.

VPN Nodes Table

The VPN Nodes table lists the VPN node properties, as well as columns that identify the VPN nodes' relationship within the VPN and its traffic (Table 16-2).

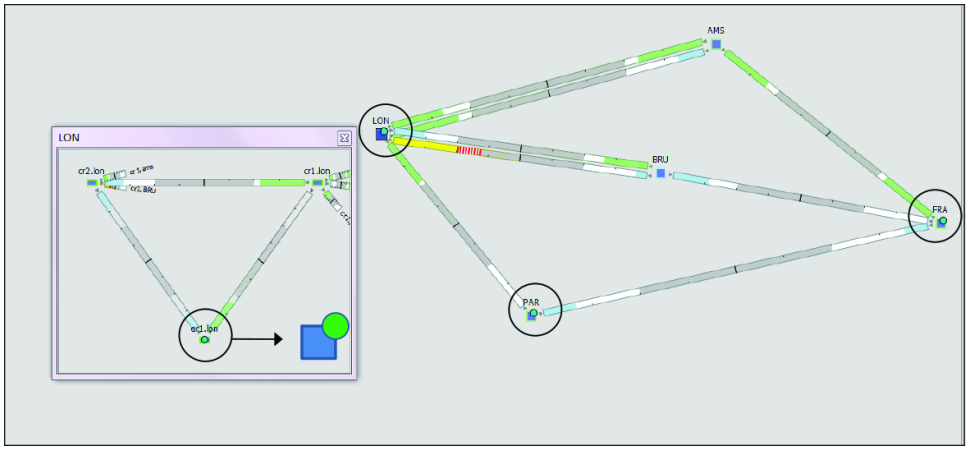
Table 16-2 VPN Nodes Table

Columns	Description
Total Connect	Number of VPN nodes that are connected to this VPN node as defined by the RT Import and RT Export pairings. These may or may not be in the same VPN.
VPN Connect	Number of VPN nodes that are connected to this VPN node and are in the same VPN as defined by the VPN column.
Num VPN Nodes	Number of nodes in the VPN that this VPN node belongs to as defined by the VPN column. This value is "na" if the VPN node does not belong to a VPN.
Src Traff Meas	Total amount of measured traffic entering the VPN at this node (source traffic).
Dest Traff Meas	Total amount of measured traffic leaving the VPN at this node (destination traffic).
Tags	User-defined identifier that makes it easy to group VPN nodes into a single VPN. If you give a VPN node a tag, when you create a VPN later, you can identify its VPN nodes using tags.

VPN nodes are not selectable from the network plot; you can only select and filter to them through tables.

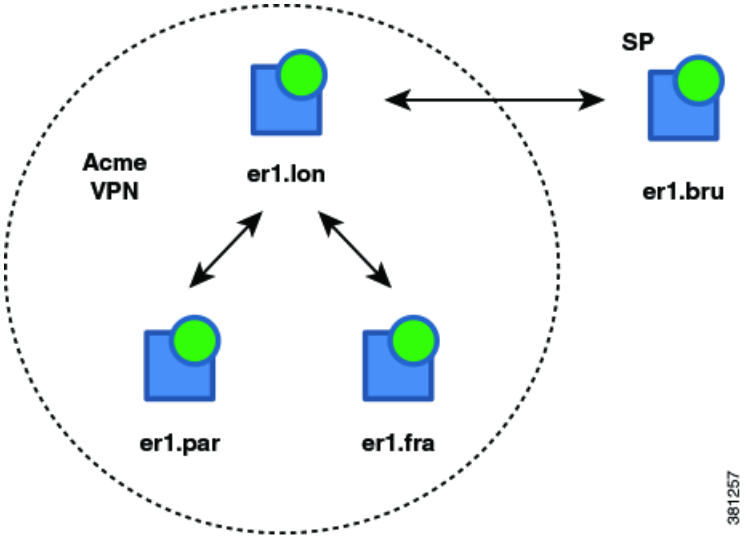
Once selected from the VPN Nodes or VPNs tables, the associated site and the nodes within that site appear with a green circle on it (Figure 16-1).

Figure 16-1 VPN Nodes Within a VPN



Layer 3 VPN Example

This example illustrates a scenario where the Acme manufacturing company has three offices, but permits the two branch (er1.par and er1.fra) offices to exchange data only with headquarters (er1.lon).



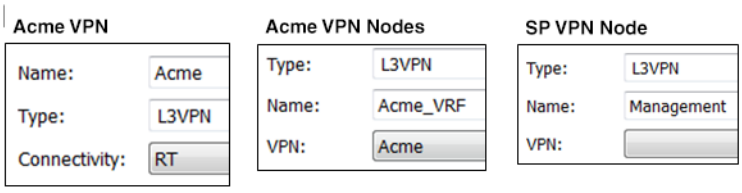
Additionally, headquarters communicates with an SP VPN node (er1.bru) that is not in the Acme VPN. Figure 16-2 shows the footprint of the Acme VPN and the RTs set for all VPN nodes in this example.

- The VPN is named Acme, and it is set to a Connectivity of RT and a Type of L3VPN.

  In turn, each branch office is set to the Acme VPN, with a Type of L3VPN.
- To exchange data with two other VPN nodes in the Acme VPN, headquarters (er1.lon) imports the offices' exported route targets of 2:1 (er1.par) and 3:1 (er1.fra).
- In turn, headquarters (er1.lon) exports a route target of 1:1.

  All three of these other VPN nodes import it (both offices and the SP VPN node).

  Because the SP VPN node (er1.bru) is not in the Acme VPN, its communication with er1.lon is not within the context of that VPN.



The VPN footprint in Figure 16-2 shows that if the circuit between er1.fra and er1.bru became congested or failed, the VPN would be impacted. However, a failure of the circuit between the two branch offices would not impact it. This failure is illustrated in Figure 16-3, which shows that none of the demands associated with the VPN are rerouted.

Figure 16-2 Example RT Connectivity and Acme VPN Footprint

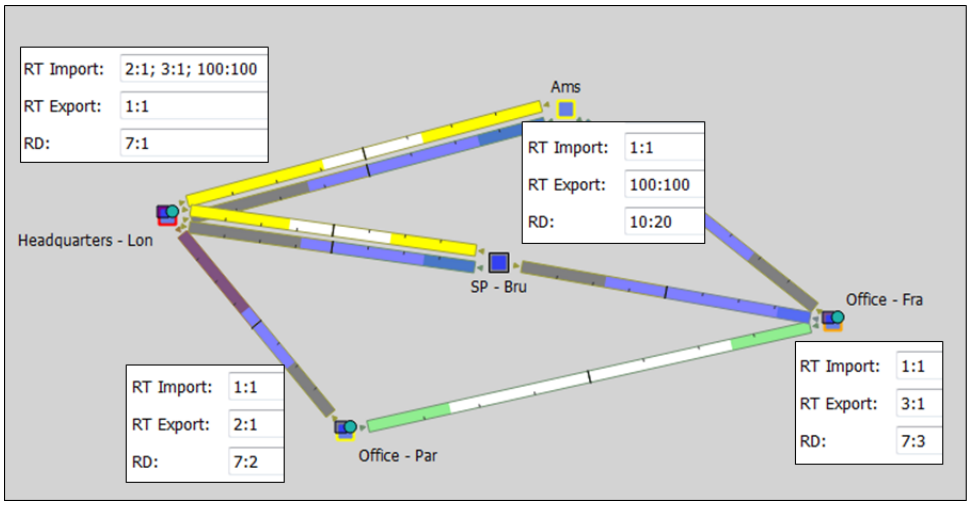
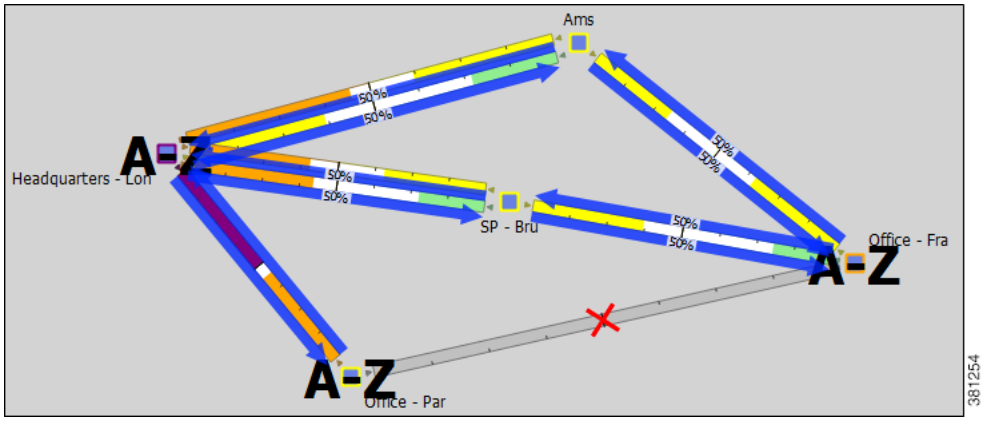


Figure 16-3 Example Failure Between Branch Offices in the Acme VPN



For this example, Figure 16-4 illustrates the filtering of VPN nodes to its associated Acme VPN and the filtering of the Acme VPN to its associated demand traffic. It also shows the calculations of the Total Connect and VPN Connect columns in the VPN Nodes table.

- The Total Connect for the VPN node residing on er1.lon, headquarters is highest because it exchanges data with three other VPN nodes.

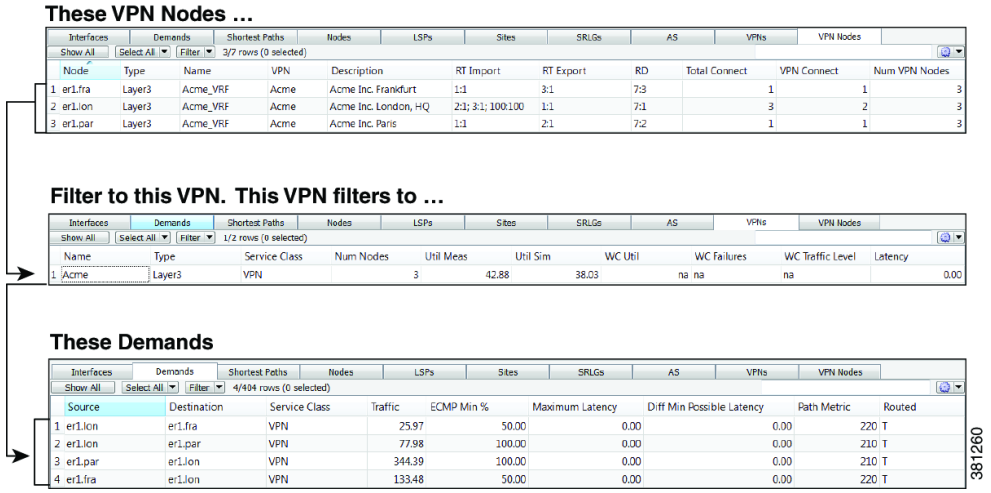
  Each of the offices and the service provider VPN node have only 1 in the Total Connect column because they each exchange data only with (have RT pairings with) headquarters.

- The VPN Connect for the VPN node residing on er1.lon, headquarters is highest because it exchanges data with and is in the same VPN as the two offices; all three VPN nodes share the same VPN name.

  Each office has 1 in the VPN Connect column because it communicates with only one VPN node in the same VPN.

  The service provider VPN node (er1.bru) has 0 VPN Connects because it does not reside in a defined VPN.

Figure 16-4 VPN Nodes Filtered to Acme VPN, and Acme VPN Filtered to Demands



VPN Simulation Analysis

When you run a Simulation Analysis, you have the option to record worst-case utilization and latency for VPNs in the VPNs table (Table 16-3). You can then right-click a VPN to fail it to its worst-case utilization or to fail it to its worst-case latency.

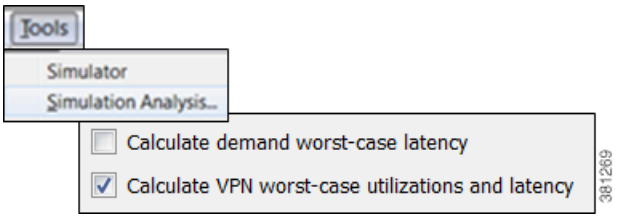


Table 16-3 Simulation Analysis Columns in the VPNs Table

Columns	Description
All calculations are based on traffic carried on all interfaces used by the VPN for the service class defined for that VPN.	
WC Util	Worst-case VPN utilization over all failure scenarios.
WC Failures	Failures causing the worst-case utilization of the VPN.
WC Traffic Level	Traffic level causing the utilization of the interface identified in the WC Util column.
WC QoS Violation	Highest worst-case QoS violation for all interfaces used by this VPN. A QoS violation is equal to the worst-case traffic minus the worst-case capacity permitted (worst-case QoS bound).
WC QoS Violation (%)	Highest worst-case QoS violation for all interfaces in this VPN expressed as a percentage of total capacity.
WC Latency	Maximum VPN latency over failure scenarios considered.
WC Latency Failures	Failures causing the worst-case VPN latency.

Creating VPN Nodes

Step 1 Right-click in an empty plot area and choose **New > VPNs > VPN Node**, or choose **Insert > VPNs > VPN Node**.

Step 2 In the Site and Name fields, choose the site in which the VPN node will exist, and choose the node on which the VPN node is being configured.

Step 3 Choose a VPN type or enter a string value for a new one. The defaults are VPWS, VPLS, and L3VPN.

Step 4 In the Name field, enter the name of the VPN node, which does not have to be unique.

Step 5 From the VPN drop-down list, choose the VPN to which you are adding this VPN node. If you do not see the VPN that you expect to see, verify that you correctly chose the type.

Step 6 (Optional) Enter a description that identifies the VPN node. For example, a customer name might be helpful.

Step 7 If the Connectivity for the VPN is RT, enter the applicable route targets in the RT Import and RT Export fields. All VPN nodes with the same import RT as another VPN node's export RT can receive traffic from that VPN node. Those VPN nodes with the same export RT as another VPN node's import RT can send traffic to that VPN node.

Step 8 (Optional) Enter a route distinguisher in the RD field.

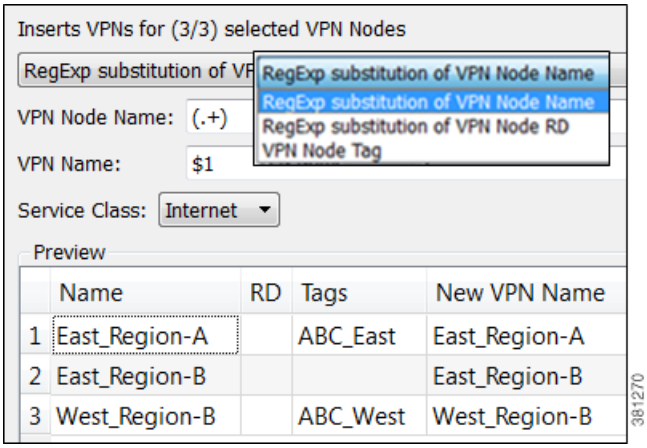
Step 9 Click **OK**.

Creating VPNs

You can create VPNs from existing VPN nodes or you can create new VPNs and then later add VPN nodes with them.

Creating VPNs from Existing VPN Nodes

When you create VPNs from existing VPN nodes, all VPN nodes are assigned to these newly created VPNs and the existing VPNs become empty. This is because VPN nodes can belong to only one VPN at a time.



Step 1 If you are creating a VPN for specific nodes, choose VPN nodes from the VPN Nodes table.

Step 2 Right-click in an empty plot area and choose **New > VPNs > VPNs from VPN Nodes**, or choose **Insert > VPNs > VPNs from VPN Nodes**.

Step 3 From the drop-down list, choose the method for creating the VPN: VPN node name, RD, or VPN node tag.

Step 4 If applicable, enter the VPN node name or VPN node RD, and enter the VPN name. These two fields work together to create and name the VPN. Both fields use regular expressions. The $ in the VPN Name field identifies which parenthetical expression in the VPN Node Name or VPN Node RD field to use. For example, $2 means use the second set of parenthesis from which to create the VPN name.

- The default is a regular expression that matches the entire VPN node name and to create one VPN for each unique VPN node name. That is, the default in VPN Node Name is (.+) and the default VPN Name is $1, which creates a VPN with a name that is identical to each VPN node (or all VPN nodes if none are selected).

  If your convention is to use the same VRF name or the same service ID for every VPN node, this default works well. If, however, the VPN name is encoded in the VRF name or service ID, use a regular expression to isolate the part of the VPN node name that is to be used.

  Example: By adding characters before or after the parenthesis, you can create a set of VPNs that are similar to VPN node names.

  Selected VPN node names: AG-VPN-AMS and AG-VPN-FRA

  VPN Node Name: AG-(.+)

  VPN Name: $1

  Results in two VPNs: VPN-AMS and VPN-FRA

  Example:

  Selected VPN node names: vrf_AKD_V001_Amsterdam, vrf_AKD_V001_Paris, and vrf_AKD_V001_Frankfurt

  VPN Node Name: (vrf)_(.+)_(V[0-9]+)_(.+)

  VPN: $2

  Results in one VPN: AKD

- If you created a VPN from VPN node RDs (Step 3), WAE Design uses regular expressions for both the VPN Node RD and VPN Name fields.

Example: Create a VPN named “7” from three existing VPN nodes with RDs of 7:1, 7:2, and 7:3.

VPN Node RD: (.+):(.+)

VPN:$1

- If you created a VPN from VPN node tags, WAE Design uses a tag to create the new VPN. If a VPN node has more than one tag, only the first tag listed is used. (To create VPN node tags or to change the order of their appearance, use the VPN Node Properties dialog box. Open it by double-clicking one or more VPN nodes.)

Step 5 To see a list of VPN nodes that will be included in the VPN and the VPN names being created, click **Update Preview**.

Step 6 Choose the service class for the VPN and click **OK**.

Creating New VPNs

Step 1 Right-click in an empty plot area and choose **New > VPNs > VPN**, or choose **Insert > VPNs > VPN**.

Step 2 Enter a unique name for the VPN.

Step 3 Choose the VPN type: VPWS, VPLS, or L3VPN.

Step 4 Choose the service class for the VPN.

Step 5 Click **OK**.

Step 6 (Optional) Add VPN nodes to the newly created VPN.

Adding VPN Nodes to VPNs

Step 1 Right-click one or more VPN nodes in the VPN Nodes table and choose **Properties**.

Step 2 In the drop-down list, choose the VPN to which you are adding the VPN nodes.

Step 3 Click **OK**.