

Chapter 7

Summary of Layer 2 VPN Configuration Statements

The following sections explain the major routing-instances configuration statements that apply specifically to Layer 2 virtual private networks (VPNs). The statements are organized alphabetically. Routing instances and the statements at the [edit routing-instances *routing-instance-name* protocols] hierarchy level are explained in the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.

control-word

Syntax	(control-word no-control-word);
Hierarchy Level	[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>] [edit routing-instances <i>routing-instance-name</i> protocols l2vpn]
Description	<p>The control word is 4 bytes long and is inserted between the Layer 2 protocol data unit (PDU) being transported and the VC label that is used for demultiplexing.</p> <p>control-word—Enables the use of the control word. Default: The control word is enabled by default. You can also configure the control word explicitly using the control-word statement.</p> <p>no-control-word—Disables the use of the control word.</p>
Usage Guidelines	See “Disable the Control Word for Layer 2 VPNs” on page 48.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

encapsulation

You configure three encapsulation types: one for the encapsulation on the logical interface, one for the encapsulation on the physical interface, and one for the Layer 2 protocol on the routing instance.

encapsulation (logical interface)

Syntax	encapsulation (atm-ccc-cell-relay atm-ccc-vc-mux atm-tcc-vc-mux atm-cisco-nlpid atm-mlppp-llc atm-nlpid atm-snap atm-tcc-snap atm-vc-mux ether-over-atm-llc ether-vpls-over-atm-llc frame-relay-ccc frame-relay-tcc multilink-frame-relay-end-to-end multilink-ppp vlan-ccc);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Description	Logical link-layer encapsulation type.
Options	<p>atm-ccc-cell-relay—Use ATM cell relay encapsulation.</p> <p>atm-ccc-vc-mux—Use ATM virtual connection (VC) multiplex encapsulation on CCC circuits. When you use this encapsulation, you can configure the family ccc only.</p> <p>atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation, you can configure the family tcc only.</p> <p>atm-cisco-nlpid—Use Cisco ATM NLPID encapsulation. When you use this encapsulation, you can configure the family inet only.</p> <p>atm-mlppp-llc—Use Multilink PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC). This encapsulation type is used only on ATM 2 interfaces. For this encapsulation type, your router must be equipped with a Link Services PIC.</p> <p>atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation, you can configure the family inet only.</p> <p>atm-snap—Use ATM Subnetwork Access Protocol (SNAP) encapsulation.</p> <p>atm-tcc-snap—Use ATM SNAP encapsulation on TCC circuits.</p> <p>atm-vc-mux—Use ATM VC multiplex encapsulation. When you use this encapsulation, you can configure the family inet only.</p> <p>ether-over-atm-llc—For interfaces that carry IPv4 traffic, use Ethernet over ATM logical link control (LLC) encapsulation. When you use this encapsulation, you cannot configure multipoint interfaces.</p> <p>ether-vpls-over-atm-llc—Use Ethernet VPLS over ATM LLC encapsulation. This encapsulation type enables a VPLS instance to support bridging between Ethernet interfaces and ATM interfaces, as described in RFC 2684, Multiprotocol Encapsulation over ATM Adaptation Layer 5. This encapsulation type is used only on ATM 2 interfaces.</p> <p>frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation, you can configure the family ccc only.</p> <p>frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation, you can configure the family tcc only.</p>

multilink-frame-relay-end-to-end—Use Multilink Frame Relay (MLFR) FRF.15 encapsulation for multilink and link services interfaces and their constituent T1 or E1 interfaces.

multilink-ppp—Use Multilink Point-to-Point Protocol (MLPPP) encapsulation. This encapsulation is used only on multilink interfaces and their constituent T1 or E1 interfaces.

vlan-ccc—Use Ethernet VLAN encapsulation on CCC circuits. When you use this encapsulation, you can configure the family ccc only.

Usage Guidelines See “Configure CCC Encapsulation on Interfaces” on page 45 or “Configure TCC Encapsulation on Interfaces” on page 46.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

encapsulation (physical interface)

Syntax encapsulation (atm-ccc-cell-relay | atm-pvc | cisco-hdlc | cisco-hdlc-ccc | cisco-hdlc-tcc | ethernet-ccc | ethernet-vpls | frame-relay | frame-relay-ccc | frame-relay-tcc | multilink-frame-relay-uni-nni | ppp | ppp-ccc | ppp-tcc | vlan-ccc | vlan-vpls | extended-vlan-ccc | extended-vlan-vpls);

Hierarchy Level [edit interfaces *interface-name*]

Description Physical link-layer encapsulation type.

Options atm-ccc-cell-relay—Use Asynchronous Transfer Mode (ATM) cell relay encapsulation.

atm-pvc—Use ATM permanent virtual connection (PVC) encapsulation.

cisco-hdlc—Use Cisco-compatible High-level Data Link Control (HDLC) framing.

cisco-hdlc-ccc—Use Cisco-compatible HDLC framing on circuit cross-connect (CCC) circuits.

cisco-hdlc-tcc—Use Cisco-compatible HDLC framing on translational cross-connect (TCC) circuits for connecting unlike media.

ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces that must accept packets carrying standard Tag Protocol ID (TPID) values.

ethernet-tcc—For interfaces that carry Internet Protocol Version 4 (IPv4) traffic, use Ethernet TCC encapsulation on interfaces that must accept packets carrying standard TPID values. Ethernet TCC is not currently supported on Fast Ethernet 48-port Physical Interface Cards (PICs).

ethernet-vpls—Use Ethernet Virtual Private LAN Service (VPLS) encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values. On M-series routers, the four-port Fast Ethernet TX PIC and the one-port, two-port, and four-port, four-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

extended-vlan-ccc—Use extended virtual local area network (VLAN) encapsulation on CCC circuits with Gigabit Ethernet and four-port Fast Ethernet interfaces that must accept packets carrying 802.1Q values.

`extended-vlan-tcc`—For interfaces that carry IPv4 traffic, use extended VLAN encapsulation on TCC circuits with Gigabit Ethernet interfaces on which you want to use 802.1Q tagging. Extended Ethernet TCC is not currently supported on Fast Ethernet 48-port PICs.

`extended-vlan-vpls`—Use extended VLAN VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901. On M-series routers, the four-port Fast Ethernet TX PIC and the one-port, two-port, and four-port, four-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

`frame-relay`—Use Frame Relay encapsulation.

`frame-relay-ccc`—Use plain Frame Relay (`frame-relay`) encapsulation or Frame Relay encapsulation on CCC circuits.

`frame-relay-tcc`—Use Frame Relay encapsulation on TCC circuits for connecting unlike media.

`multilink-frame-relay-uni-nni`—Use only on link services interfaces functioning as FRF.16 bundles and their constituent T1, E1, or NxDS-0 interfaces.

`ppp`—Use serial Point-to-Point Protocol (PPP) encapsulation.

`ppp-ccc`—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation, you can configure the family `ccc` only.

`ppp-tcc`—Use serial PPP encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation, you can configure the family `tcc` only.

`vlan-ccc`—Use Ethernet VLAN encapsulation on CCC circuits.

`vlan-vpls`—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. On M-series routers, the four-port Fast Ethernet TX PIC and the one-port, two-port, and four-port, four-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

Default PPP encapsulation.

Usage Guidelines See “Configure CCC Encapsulation on Interfaces” on page 45 or “Configure TCC Encapsulation on Interfaces” on page 46.

Required Privilege Level `interface`—To view this statement in the configuration.
`interface-control`—To add this statement to the configuration.

encapsulation (Layer 2 VPN)

Syntax	encapsulation <i>type</i> ;
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols l2vpn]
Description	Layer 2 protocol used for traffic from the customer edge (CE) router.
Options	<p><i>type</i>—The following Layer 2 encapsulation types are supported:</p> <ul style="list-style-type: none"> atm-aal5—ATM Adaptation Layer (AAL/5) atm-cell—ATM cell relay atm-cell-port-mode—ATM cell relay port promiscuous mode atm-cell-vc-mode—ATM virtual circuit (VC) cell relay non-promiscuous mode atm-cell-vp-mode—ATM virtual path (VP) cell relay promiscuous mode cisco-hdlc—Cisco Systems-compatible HDLC ethernet—Ethernet ethernet-vlan—Ethernet VLAN frame-relay—Frame Relay interworking—Layer 2.5 interworking VPN ppp—PPP
Usage Guidelines	See “Configure the Encapsulation Type” on page 43.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
See also	encapsulation on page 70

no-control-word

See “control-word” on page 69.

policer

Syntax	<pre>policer { arp <i>policer-template-name</i>; input <i>policer-template-name</i>; output <i>policer-template-name</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family (ccc inet tcc)]
Description	Use policing to control the amount of traffic flowing over the interfaces servicing a Layer 2 VPN.
Options	<p>arp <i>policer-template-name</i>—For family inet only, name of one policer to evaluate when ARP packets are received on the interface.</p> <p>input <i>policer-template-name</i>—Name of one policer to evaluate when packets are received on the interface.</p> <p>output <i>policer-template-name</i>—Name of one policer to evaluate when packets are transmitted on the interface.</p>
Usage Guidelines	See “Configure Layer 2 VPN Policing on Interfaces” on page 47.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
See Also	<i>JUNOS Internet Software Configuration Guide: Policy Framework</i> and <i>JUNOS Internet Software Configuration Guide: Network Interfaces and Class of Service</i> .

proxy

Syntax	proxy inet-address <i>address</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family tcc]
Description	For Layer 2.5 VPNs using an Ethernet interface as the TCC router, configure the IP address for which the TCC router is proxying. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on one-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet PICs only. Ethernet TCC is not supported on the T640 routing node.
Usage Guidelines	See “Configure TCC Encapsulation on Interfaces” on page 46.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

remote

Syntax	remote (inet-address mac-address) <i>address</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family tcc]
Description	For Layer 2.5 VPNs employing an Ethernet interface as the TCC router, configure the location of the remote router. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on one-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet PICs only. Ethernet TCC is not supported on the T640 routing node.
Options	inet-address—Configure the IP address of the remote site. mac-address—Configure the MAC address of the remote site.
Usage Guidelines	See “Configure TCC Encapsulation on Interfaces” on page 46.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

remote-site-id

Syntax	remote-site-id <i>remote-site-ID</i> ;
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i>]
Description	Controls the remote interface to which the interface should connect. The order of the interfaces configured for the site determines the default value if you do not explicitly configure the remote site ID. This statement is optional.
Usage Guidelines	See “Configure the Remote Site ID” on page 42.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

site

Syntax	<pre> site <i>site-name</i> { site-identifier <i>identifier</i>; interface <i>interface-name</i> { remote-site-id <i>remote-site-ID</i>; } } </pre>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols l2vpn]
Description	Specify the site name, site identifier, and interfaces connecting to the site. Allows you to configure a remote site ID for remote sites.
Options	<p>interface <i>interface-name</i>—Name of the interface.</p> <p>site-identifier <i>identifier</i>—Numerical identifier for the site used as a default reference for the remote site ID.</p> <p>remote-site-id <i>remote-site-ID</i>—(Optional) Control the remote interface to which the interface should connect. The order of the interfaces configured for the site determines the default value if you do not explicitly configure the remote site ID.</p> <p>site <i>site-name</i>—Name of the site.</p>
Usage Guidelines	See “Configure the Site” on page 41.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

site-identifier

Syntax	site-identifier <i>identifier</i> ;
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i>]
Description	The numerical identifier for the site used as a default reference for the remote site ID. It is an unsigned 16-bit number greater than zero.
Usage Guidelines	See “Configure the Site” on page 41.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

tracoptions

Syntax tracoptions {
 file *filename* <replace> <size *size*> <files *number*> <no-stamp>;
 flag *flag* <flag-modifier> <disable>;
 }

Hierarchy Level [edit routing-instances *routing-instance-name* protocols l2vpn]

Description Trace traffic flowing through a Layer 2 VPN.

Options disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file.0*, then *trace-file.1*, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option.

Range: 2 to 1000

Default: 2 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

all—All Layer 2 VPN tracing options

connections—Layer 2 connections (events and state changes)

error—Error conditions

nri—Layer 2 advertisements received or sent by means of the Border Gateway Protocol (BGP)

route—Routing information

topology—Layer 2 VPN topology changes caused by reconfiguration or advertisements received from other PE routers using BGP

flag-modifier—(Optional) Modifier for the tracing flag. You can specify the following modifier:

detail—Provide detailed trace information

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

replace—(Optional) Replace an existing trace file if there is one.

Default: If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When *trace-file* again reaches its maximum size, *trace-file.0* is renamed *trace-file.1* and *trace-file* is renamed *trace-file.0*. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the *files* option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

Usage Guidelines See “Trace Layer 2 VPN Traffic and Operations” on page 44.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.