

Chapter 8

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 Routing Protocols Configuration Guide*.

control-word

Syntax	(control-word no-control-word);
Hierarchy Level	[edit logical-routers <i>logical-router-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>], [edit logical-routers <i>logical-router-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn], [edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn]
Description	<p>Specify the control word. The control word is 4 bytes long and is inserted between the Layer 2 protocol data unit (PDU) being transported and the virtual connection (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 “Disabling the Control Word for Layer 2 VPNs” on page 77.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

encapsulation

See the following sections:

encapsulation (Layer 2 VPN) on page 102

encapsulation (Logical Interface) on page 103

encapsulation (Physical Interface) on page 105

encapsulation (Layer 2 VPN)

Syntax `encapsulation type;`

Hierarchy Level [edit logical-routers *logical-router-name* routing-instances *routing-instance-name* protocols l2vpn],
[edit routing-instances *routing-instance-name* protocols l2vpn]

Description Layer 2 protocol used for traffic from the CE router.

Options *type*—The following Layer 2 encapsulation types are supported:

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 “Configuring the Encapsulation Type” on page 72.

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

See also encapsulation on page 102

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-ppp-llc atm-ppp-vc-mux atm-snap atm-tcc-snap atm-vc-mux ether-over-atm-llc ether-vpls-over-atm-llc ethernet frame-relay-ccc frame-relay-tcc multilink-frame-relay-end-to-end multilink-ppp vlan-ccc vlan-tcc vlan-vpls);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-routers <i>logical-router-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Description	Logical link-layer encapsulation type.
Options	<p>atm-ccc-cell-relay—Use Asynchronous Transfer Mode (ATM) cell relay encapsulation.</p> <p>atm-ccc-vc-mux—Use ATM VC multiplex encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the family ccc only.</p> <p>atm-cisco-nlpid—Use Cisco ATM Network Layer Protocol identifier (NLPID) encapsulation. When you use this encapsulation type, you can configure the family inet only.</p> <p>atm-mlppp-llc—For ATM2 intelligent queuing (IQ) interfaces only, use Multilink Point-to-Point (MLPPP) over ATM adaptation layer 5 (AAL5) logical link control (LLC). For this encapsulation type, your routing platform must be equipped with a Link Services or Voice Services PIC.</p> <p>atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the family inet only.</p> <p>atm-ppp-llc—For ATM2 IQ interfaces only, use PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation.</p> <p>atm-ppp-vc-mux—For ATM2 IQ interfaces only, use PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.</p> <p>atm-snap—Use ATM Subnetwork Access Protocol (SNAP) encapsulation.</p> <p>atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.</p> <p>atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the family tcc only.</p> <p>atm-vc-mux—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the family inet only.</p> <p>ether-over-atm-llc—For interfaces that carry Internet Protocol version 4 (IPv4) traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.</p>

`ether-vpls-over-atm-llc`—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

`ethernet`—Use Ethernet II encapsulation (as described in RFC 894).

`frame-relay-ccc`—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the family `ccc` only.

`frame-relay-tcc`—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the family `tcc` only.

`multilink-frame-relay-end-to-end`—Use Multilink Frame Relay (MLFR) FRF.15 encapsulation. This encapsulation is used only on multilink, link services, and voice 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, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

`vlan-ccc`—Use Ethernet virtual local-area network (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the family `ccc` only.

`vlan-tcc`—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the family `tcc` only.

`vlan-vpls`—Use Ethernet VLAN encapsulation on virtual private LAN service (VPLS) circuits.

Usage Guidelines See “Configuring CCC Encapsulation on Interfaces” on page 74 or “Configuring TCC Encapsulation on Interfaces” on page 75.

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-over-atm ethernet-tcc ethernet-vpls extended-frame-relay-ccc extended-frame-relay-tcc extended-vlan-ccc extended-vlan-tcc extended-vlan-vpls flexible-ethernet-services flexible-frame-relay frame-relay frame-relay-ccc frame-relay-port-ccc frame-relay-tcc multilink-frame-relay-uni-nni ppp ppp-ccc ppp-tcc vlan-ccc vlan-vpls);
Hierarchy Level	[edit interfaces <i>interface-name</i>], [edit logical-routers <i>logical-router-name</i> interfaces <i>interface-name</i>]
Description	Physical link-layer encapsulation type.
Options	<p>atm-ccc-cell-relay—Use ATM cell-relay encapsulation.</p> <p>atm-pvc—Use ATM permanent virtual connection (PVC) encapsulation.</p> <p>cisco-hdlc—Use Cisco-compatible High-level Data Link Control (HDLC) framing.</p> <p>cisco-hdlc-ccc—Use Cisco-compatible HDLC framing on CCC circuits.</p> <p>cisco-hdlc-tcc—Use Cisco-compatible HDLC framing on TCC circuits for connecting unlike media.</p> <p>ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces that must accept packets carrying standard Tag Protocol ID (TPID) values.</p> <p>ethernet-over-atm—For interfaces that carry IPv4 traffic, use Ethernet over ATM encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces. As defined in RFC 1483, this encapsulation type allows ATM interfaces to connect to devices that support only bridged-mode protocol data units (BPDU). The JUNOS software does not completely support bridging, but accepts BPDUs as a default gateway. If you use the router as an edge device, then the router acts as a default gateway. It accepts Ethernet LLC/SNAP frames with IP or ARP in the payload and drops the rest. For packets destined for the Ethernet LAN, a route lookup is done using the destination IP address. If the route lookup yields a full address match, the packet is encapsulated with an LLC/SNAP and MAC header and forwarded to the ATM interface.</p> <p>ethernet-tcc—For interfaces that carry 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).</p> <p>ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard TPID values.</p> <p>extended-frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. This encapsulation type allows you to dedicate data link connection identifiers (DLCIs) 1 through 1022 to CCC.</p> <p>extended-frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits to connect unlike media. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to TCC.</p>

`extended-vlan-ccc`—Use extended VLAN encapsulation on CCC circuits with Gigabit Ethernet and 4-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.

`flexible-ethernet-services`—For Gigabit Ethernet IQ interfaces and Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFPs) only, use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. This encapsulation type allows you to configure any combination of route, TCC, CCC, and VPLS encapsulations on a single physical port. Aggregated Ethernet bundles cannot use this encapsulation type. If you configure flexible Ethernet services encapsulation on the physical interface, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

`flexible-frame-relay`—For IQ interfaces only, use flexible Frame Relay encapsulation when you want to configure multiple per-unit Frame Relay encapsulations. This encapsulation type allows you to configure any combination of TCC, CCC, and standard Frame Relay encapsulations on a single physical port. Also, each logical interface can have any DLCI value from 1 through 1022.

`frame-relay`—Use Frame Relay encapsulation.

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

`frame-relay-port-ccc`—Use Frame Relay port CCC encapsulation to transparently carry all the DLCIs between two customer edge (CE) routers without explicitly configuring each DLCI on the two provider edge (PE) routers with Frame Relay transport. When you use this encapsulation type, you can configure the family `ccc` only.

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

`multilink-frame-relay-uni-nni`—Use Multilink Frame Relay (MLFR) UNI NNI encapsulation. This encapsulation is used only on link services and voice services interfaces functioning as FRF.16 bundles and their constituent T1 or E1 interfaces.

`ppp`—Use serial PPP encapsulation.

`ppp-ccc`—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation type, 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 type, 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.

Default PPP encapsulation.

Usage Guidelines See “Configuring CCC Encapsulation on Interfaces” on page 74 or “Configuring TCC Encapsulation on Interfaces” on page 75.

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

no-control-word

See control-word on page 101

policer

Syntax policer {
 arp *policer-template-name*;
 input *policer-template-name*;
 output *policer-template-name*;
}

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family (ccc | inet | tcc)],
[edit logical-routers *logical-router-name* interfaces *interface-name* unit
logical-unit-number family (ccc | inet | tcc)]

Description Use policing to control the amount of traffic flowing over the interfaces servicing a Layer 2 VPN.

Options arp *policer-template-name*—For family inet only, name of one policer to evaluate when Address Resolution Protocol (ARP) packets are received on the interface.

input *policer-template-name*—Name of one policer to evaluate when packets are received on the interface.

output *policer-template-name*—Name of one policer to evaluate when packets are transmitted on the interface.

Usage Guidelines See “Configuring Layer 2 VPN Policing on Interfaces” on page 76.

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

See Also *JUNOS Policy Framework Configuration Guide* and *JUNOS Network Interfaces and Class of Service Configuration Guide*.

proxy

Syntax	proxy inet-address <i>address</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family tcc], [edit logical-routers <i>logical-router-name</i> 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 1-port Gigabit Ethernet, 2-port Gigabit Ethernet, 4-port Gigabit Ethernet, and 4-port Fast Ethernet PICs only. Ethernet TCC is not supported on the T640 routing node.
Usage Guidelines	See “Configuring TCC Encapsulation on Interfaces” on page 75.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

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], [edit logical-routers <i>logical-router-name</i> 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 1-port Gigabit Ethernet, 2-port Gigabit Ethernet, 4-port Gigabit Ethernet, and 4-port Fast Ethernet PICs only.
Options	inet-address—Configure the IP address of the remote site. mac-address—Configure the MAC address of the remote site.
Usage Guidelines	See “Configuring TCC Encapsulation on Interfaces” on page 75.
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 logical-routers <i>logical-router-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i>]
Description	Control the remote interface to which the interface should connect. If you do not explicitly configure the remote site ID, the order of the interfaces configured for the site determines the default value. This statement is optional.
Usage Guidelines	See “Configuring the Remote Site ID” on page 71.
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> { description <i>text</i>; remote-site-id <i>remote-site-ID</i>; } }</pre>
Hierarchy Level	[edit logical-routers <i>logical-router-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn], [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>description—Text description for the interface connecting to a site. If the text includes one or more spaces, enclose it in quotation marks (" "). Any descriptive text you include is displayed in the output of the show route instance detail command and has no effect on operation.</p> <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 “Configuring the Site” on page 70.
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 logical-routers <i>logical-router-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i>]
Description	Specify the numerical identifier for the site used as a default reference for the remote site ID. It can be any number 1 through 65,534.
Usage Guidelines	See “Configuring the Site” on page 70.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

traceoptions

Syntax	<pre>traceoptions { file filename <replace> <size size> <files number> <no-stamp>; flag flag <flag-modifier> <disable>; }</pre>
Hierarchy Level	[edit logical-routers <i>logical-router-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn]
Description	Trace traffic flowing through a Layer 2 VPN.
Options	<p>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.</p> <p>file filename—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" ").</p> <p>files number—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 files Default: 2 files</p> <p>flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p> <ul style="list-style-type: none"> all—All Layer 2 VPN tracing options connections—Layer 2 connections (events and state changes) error—Error conditions nlri—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 <p>flag-modifier—(Optional) Modifier for the tracing flag. You can specify the following modifier:</p> <ul style="list-style-type: none"> 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 “Tracing Layer 2 VPN Traffic and Operations” on page 73.

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