VPN Interface T1/E1

- Configure VPN interface T1/E1, on page 1

Configure VPN interface T1/E1

Use one of these methods to configure VPN interface T1/E1:

- Configuration group
- Feature template

Configure VPN interface T1/E1 using a configuration group

Follow these steps to configure VPN interface T1/E1 using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the Transport VPN feature in a Transport and Management Profile.

Step 3 Create and configure the T1 and E1 feature for the VPN interface.

a) Configure the basic VPN settings.

Table 1: Basic Configuration

Parameter Name	Description
Shutdown	Click **No** to enable the interface.

Parameter Name	Description
Interface name*	Enter a name for the interface. The name should be in the following format: **serial** *slot* **/** *subslot* **/** *port* **:** *channel-group* You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.
Description	Enter a description for the interface.
More Settings	
IPv4 Address*	Enter an IPv4 address.
IPv6 Address*	Enter an IPv6 address.
Bandwidth	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Clock Rate	Specify a value for the clock rate. Range: 1200 through 800000
Encapsulation	Choose an encapsulation method for traffic that crosses a WAN link. • **hdlc**: High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • **ppp**: Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.

b) Configure the tunnel parameters.

Table 2: Tunnel

Parameter Name	Description
Tunnel Interface*	From the drop-down list, select **Global**. Click **On** to create a tunnel interface.
Per-tunnel QoS	From the drop-down list, select **Global**. Click **On** to create per-tunnel QoS. You can apply a Quality of Service (QoS) policy on individual tunnels, and is only supported for hub-to-spoke network topologies.
Color	From the drop-down list, select **Global**. Select a color for the TLOC. The color typically used for cellular interface tunnels is **lte**.
Color Description	Enter a description associated to the TLOC color.

Parameter Name	Description
Groups	From the drop-down list, select **Global**. Enter the list of groups in the field.
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Maximum Control Connections	Set the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Control Group List	Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allows to establish control connections with. Range: 0 through 100
Manager Connection Preference	Set the preference for using the tunnel to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 9 Default: 5 If the edge device has two or more cellular interfaces, you can minimize the amount of traffic between Cisco SD-WAN Manager and the cellular interfaces by setting one of the interfaces to be the preferred one to use when sending updates to the Cisco SD-WAN Manager and receiving configurations from the Cisco SD-WAN Manager. To have a tunnel interface never connect to Cisco SD-WAN Manager, set the number to 0. At least one tunnel interface on the edge device must have a nonzero Cisco SD-WAN Manager connection preference.
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**

Parameter Name	Description
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Allow Service	Click **On** or **Off** for each service to allow or disallow the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Add Encapsulation	From the drop-down list, select **Global** and choose from one of the two encapsulation methods: • **gre**: Enter a value to set GRE preference for TLOC. Range: 0 to 4294967295 • **ipsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
Preference	From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
Weight	From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Advanced Options	
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*.

Parameter Name	Description
Last-Resort Circuit	From the drop-down list, select **Global** and click **On** to use the tunnel interface as the circuit of last resort. By default, it is disabled. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.

c) Configure ACL/QoS parameters.

Table 3: ACL/QoS

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
ACL	
Select ACL IPv4 Ingress	Enter the name of an IPv4 access list to packets being received on the interface.
Select ACL IPv4 Egress	Enter the name of an IPv4 access list to packets being transmitted on the interface.
Select ACL IPv6 Ingress	Enter the name of an IPv6 access list to packets being received on the interface.
Select ACL IPv6 Egress	Enter the name of an IPv6 access list to packets being transmitted on the interface.

d) Configure the advanced parameters.

Table 4: Advanced

Parameter Name	Description
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 through 1460 bytes Default: 536
MTU	Enter the path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. Default: 1500
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds this service-side interface to the WAN transport, by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.

What to do next

Also see Deploy a configuration group.

Configure T1 or E1 controller using a configuration group

Follow these steps to configure T1 or E1 controller using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the T1 or E1 network interface module (NIM) parameters in a Transport and Management Profile.

a) Configure a T1 Controller.

Table 5: Configure a T1 Controller

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0.
Description	Enter a description for the controller.
Framing	It is an optional field. Enter the T1 frame type: • **esf**: Send T1 frames as extended superframes. This is the default. • **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing.
Line Code	It is an optional field. Select the line encoding to use to send T1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • **b8zs**: Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes
Cable Length	Select the cable length to configure the attenuation • **short**: Set the transmission attenuation for cables that are 660 feet or shorter. • **long**: Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. There is no default length.
Clock Source	Select the clock source: • **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. • **internal**: Use the controller framer as the primary clock. • **loop-timed**: • **network**:

b) Configure an E1 Controller.

Table 6: Configure an E1 Controller

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Description	Enter a description for the controller.

Parameter Name	Description
Framing	Enter the E1 frame type: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do not use CRC4.
Line Code	Choose the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **hdb3**: Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Choose the clock source: • **internal**: Use the controller framer as the primary clock. • **line**: Use phase-locked loop (PLL) on the interface. This is the default.

c) Configure channel group.

Table 7: Channel Group

Parameter Name	Description
Add Channel Group	To configure the serial WAN on the E1 interface, enter a channel group number and a value for the timeslot. • **Channel Group**: Enter a value for the channel group. Range: 0 through 30 • **Time Slot**: Type a value for the timeslot. Range: 0 through 31

What to do next

Also see Deploy a configuration group.

Configure VPN interface T1/E1 using templates

Follow these steps to configure VPN interface T1/E1 using a feature template.

Use the VPN Interface T1/E1 template for Cisco Catalyst SD-WANs running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters, as described in this article.

2. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters.
3. Create a VPN feature template to configure VPN parameters.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

   Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface T1/E1 Serial**.

d) If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0), click **Service VPN** or scroll to the **Service VPN** section.

   In the Service **VPN** drop-down list, enter the number of the service VPN. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface T1/E1 Serial**.

e) From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
f) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
g) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following parameters in the VPN Interface T1/E1 Serial template.

a) Configure basic interface functionality in a VPN.

Table 8:

Parameter Name	Description
Shutdown*	Click **No** to enable the interface.
Interface name*	Enter a name for the interface. The name should be in the format **serial** *slot* / *subslot* / *port* : *channel-group*. You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.
Description	Enter a description for the interface.
IPv4 Address*	Enter an IPv4 address.
IPv6 Address*	Enter an IPv6 address.

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

b) Configure a tunnel interface for the multilink interface.

Table 9:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.

Parameter Name	Description
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5

Parameter Name	Description
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has **Dont Fragment** configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the **Dont Fragment** bit in the IPv4 packet header for packets being transmitted out of the interface. When the **Dont Fragment** bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the **Dont Fragment** bit and the **Dont Fragment** bit is set. For packets not requiring fragmentation, the **Dont Fragment** bit is not affected.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

Configure T1 or E1 controller using templates

Follow these steps to configure T1 or E1 controller using a feature template.

Use the T1/E1 Controller template for Cisco IOS XE Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters, as described in this article.
2. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters.
3. Create a VPN feature template to configure VPN parameters.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

   Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface T1/E1**.

d) From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following T1 or E1 controller parameters.

a) Configure a T1 controller.

Table 10:

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0.
Framing*	Enter the T1 frame type: • **esf**—Send T1 frames as extended superframes. This is the default. • **sf**—Send T1 frames as superframes. Superframing is sometimes called D4 framing.

Parameter Name	**Description**
Line Code	Select the line encoding to use to send T1 frames: • ami—Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • b8zs—Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes
Clock Source	Select the clock source: • internal—Use the controller framer as the primary clock. • line—Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source.
Line Mode	If you choose the Line clock source, select whether the line is a primary or a secondary line.
Description	Enter a description for the controller.
Channel Group	Enter the number of the channel group. If you do so, you must enter a time slot in the Time Slot field. Range: 0 through 30
Time Slot	Enter the time slot or time slots that are part of the channel group. Range: 1 through 24
Cable Length	Select the cable length to configure the attenuation • long—Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. • short—Set the transmission attenuation for cables that are 660 feet or shorter. There is no default length.

Parameter Name	Description
Length	If you specify a value in the **Cable Length Field**, enter the length of the cable. For short cables, the length values can be: • 110—Length from 0 through 110 feet • 220—Length from 111 through 220 feet • 330—Length from 221 through 330 feet • 440—Length from 331 through 440 feet • 550—Length from 441 through 550 feet • 660—Length from 551 through 660 feet For long cables, the length values can be: • 0 dB • –7.5 dB • –15 dB • –22.5 dB

b) Configure an E1 controller.

Table 11:

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Framing*	Enter the E1 frame type: • **crc4**—Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**—Do no use CRC4.
Line Code*	Select the line encoding to use to send E1 frames: • ami—Use alternate mark inversion (AMI) as the linecode. • hdb3—Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Select the clock source: • internal—Use the controller framer as the primary clock. • line—Use phase-locked loop (PLL) on the interface. This is the default.

Parameter Name	Description
Line Mode	If you choose the Line clock source, select whether the line is a primary or secondary line. If you configure both a primary and a secondary line, if the primary line fails, the PLL automatically switches to the secondary line. When the PLL on the primary line becomes active again, the PLL automatically switches back to the primary line.
Description	Enter a description for the controller.
Channel Group	To configure the serial WAN on the E1 interface, enter a channel group number. Range: 0 through 30
Time Slot	For a channel group, configure the timeslot. Range: 1 through 31