



ERSPAN Termination from Standalone Production Switches

[New and Changed Information](#) 2

[ERSPAN Termination](#) 2

Revised: September 14, 2021

New and Changed Information

The following table provides an overview of the significant changes to this document.

Cisco NDB Release Version	Feature	Description
3.10	ERSPAN Termination from Production Switches.	This document has details of how to implement ERSPAN termination for traffic from production switches.

ERSPAN Termination

Encapsulated Remote SPAN (ERSPAN) transports mirrored traffic over an IP network and provides remote monitoring of multiple switches across the network. The traffic is encapsulated at the source device and is transferred across the network and decapsulated at the destination device and then sent to the destination interface. ERSPAN is a Cisco proprietary tunnelling protocol and used with generic routing encapsulation (GRE) .

ERSPAN brings GRE for all the packets and allows it to travel across layer 3 networks/domains. To transport data from one network to another network safely this encapsulation mechanism is widely used. In the NDB framework, ERSPAN termination is typically used for remote packets travelling from production switch(es) across multiple networks, reaching the NDB network.

Table 1: Supported Nexus Switches

Nexus Switches	NDB Version	NX-OS Version
9300-EX, 9300-FX, 9300-FX2 and 9500 EoR chassis with -EX and -FX line cards	3.8 and later	9.3(1) and later
9300-GX	3.10 and later	9.3(5) and later

Guidelines and Limitations

Guidelines and Limitations for ERSPAN termination:

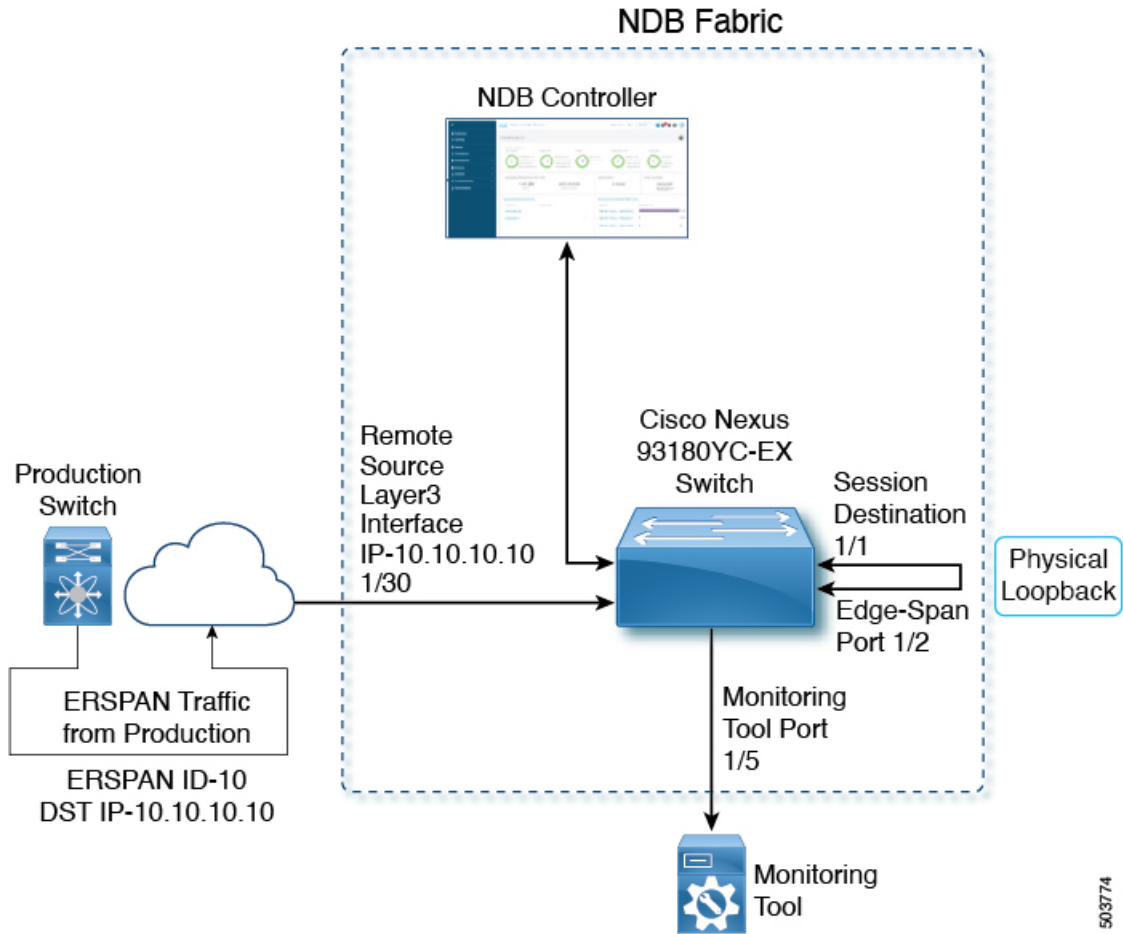
- For proper tunnel terminations, ensure ERSPAN IDs and version (in some cases) should match on both ERSPAN source and destination sessions.
- There should be a physical loopback port (physical recirculation on front panel ports) connected between session destination interface & remote source edge span. For each active ERSPAN destination session, one pair of physical loopback ports should be available on the NDB switches.
- A maximum of four active ERSPAN terminations are supported per NDB switch.

Topology for One ERSPAN Tunnel Termination

Ensure to advertise/install the route in the production switch and NDB switch via static/dynamic routing for proper tunnel termination.

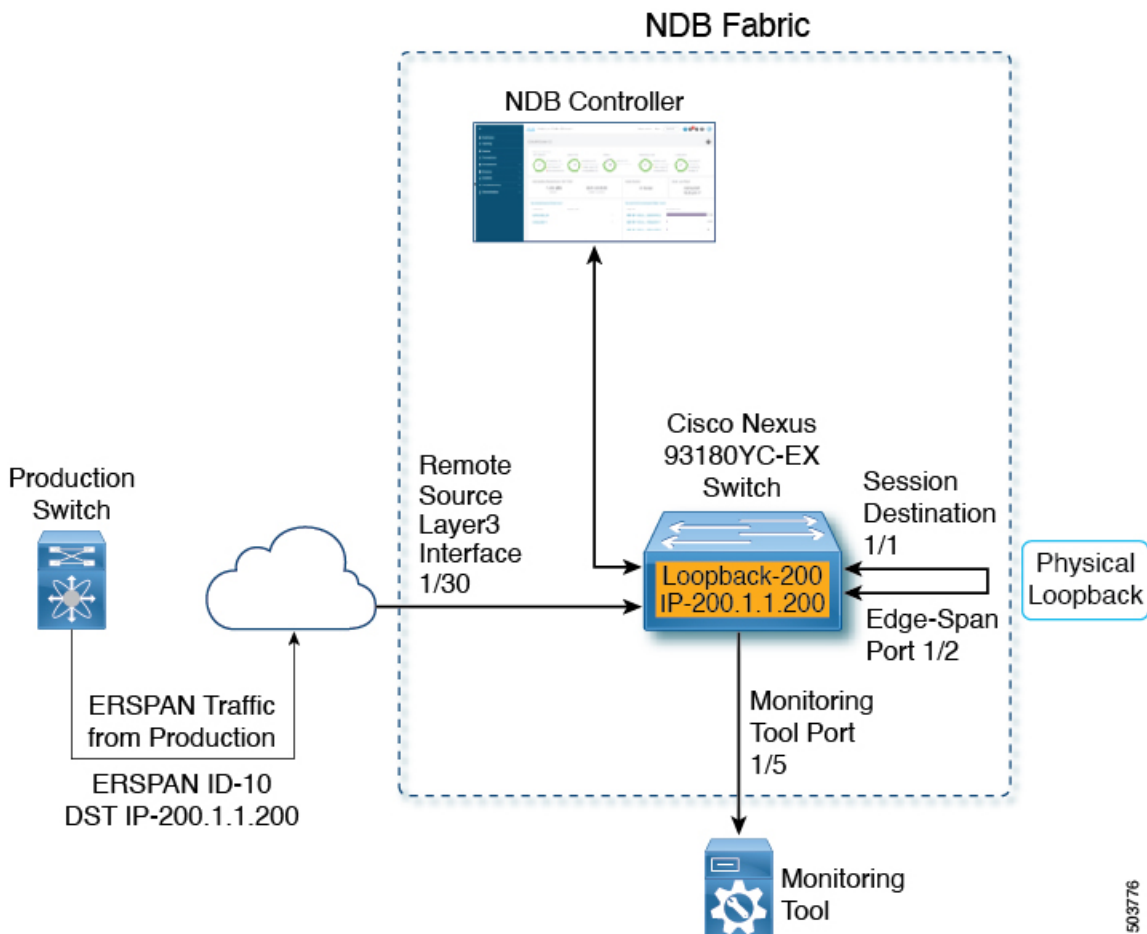
ERSPAN production traffic terminated on remote source interface is handled by session destination to decapsulate. Decapsulated packets are given to Edge-Span/Tap port via physical loopback connection. Edge-Span/Tap port match the packets based on the filters and redirect to the respective Monitor Tool(s).

Figure 1: Terminating one ERSPAN tunnel on NDB switch Layer 3/IP Interface from Production Switch



503774

Figure 2: Terminating one ERSPAN tunnel on NDB switch Loopback Interface from Production Switch



503776



Note Route should be advertised/installed in the production switch and NDB switch via static/dynamic routing for proper tunnel termination on the loopback interface IP.

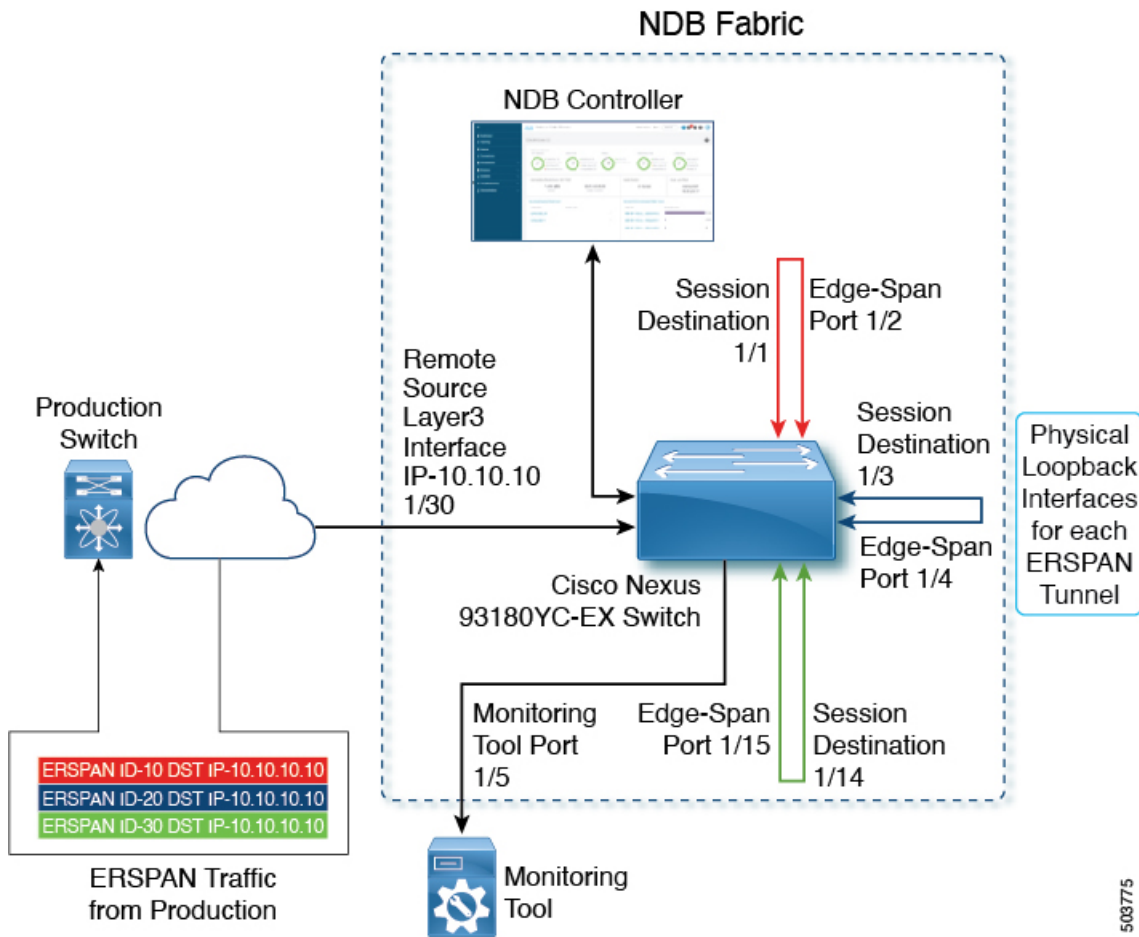
Topology for one ERSPAN tunnel termination.

- Remote Source port (1/30) is the Layer3 interface on which the ERSPAN traffic is terminated from the production switch.
- Session Destination port (1/1) is the port which decapsulates the ERSPAN header and egresses the traffic.
- Edge-Span port (1/2) is the input port on which the inside packets are available for applying Tap Aggregation policy for filtering and redirection.
- Monitoring Tool port (1/5) is the port through which the filtered egress traffic reaches the monitoring tool(s).
- **(applicable only for topology with loopback interface)** ERSPAN source tunnel is destined to the Loopback IP address of the NDB switch but the tunnel is physically terminated on the Layer3 interface.

Topology for Multiple ERSPAN Tunnel Terminations

Ensure to advertise/install the route(s) in the production switch and NDB switch via static/dynamic routing for proper tunnel termination. ERSPAN Production traffic terminated on Remote source interface is handled by session destination session to decapsulate. Decapsulated packets are given to Edge-Span/Tap port via physical loopback connection. Edge-Span/Tap port match the packets based on the filters and redirect the traffic to the respective Monitor Tool(s).

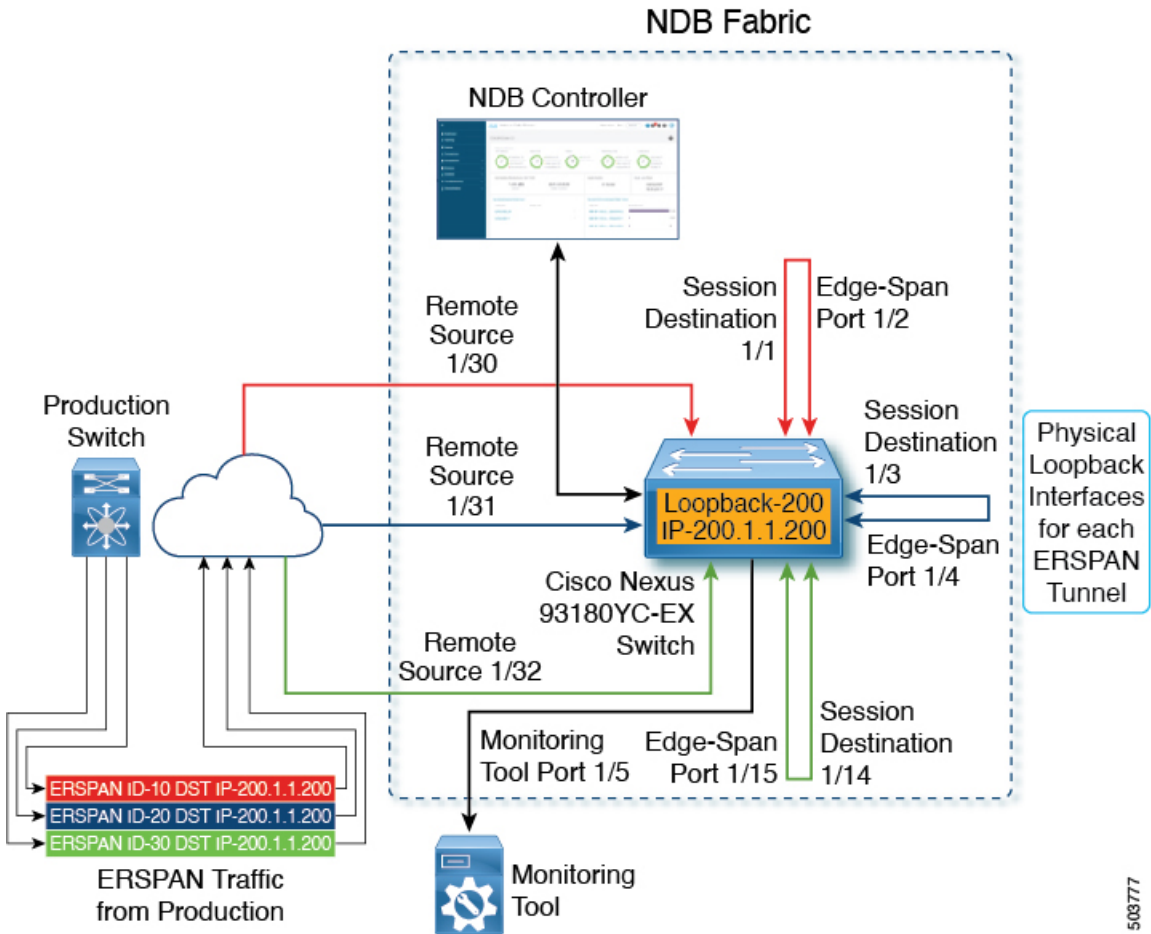
Figure 3: Terminating multiple ERSPAN tunnels on NDB Switch Layer3/IP Interface from Production Switch



Multiple ERSPAN tunnels can be terminated, but all the ERSPAN source session packets should have a destination IP address as Remote Source Layer3 interface.

508775

Figure 4: Terminating multiple ERSPAN tunnels on NDB Switch Loopback Interface from Production Switch



Multiple ERSPAN tunnels can be terminated but destined to the same Loopback Interface. Here, 3 ERSPAN source tunnels from production switch are terminated on 3 different layer3 NDB interfaces, but destined to a common loopback IP.



Note Route should be advertised/installed in Production switch and NDB switch via Static/Dynamic routing for proper tunnel termination on the Loopback interface IP.

The topology described below is for multiple ERSPAN tunnel terminations.

- Physical loopback connection between Session Destination and Edge-Span port is per ERSPAN tunnel termination(s). In this case we have 3 ERSPAN tunnels terminated, so 3 physical loopback connections should be established (total 6 ports burnt for 3 ERSPAN tunnels).
- Remote Source port(1/30) is the Layer3 interface on which the ERSPAN traffic is terminated from the production switch.
- Session Destination (1/1, 1/3, 1/14) is the port which decapsulates the ERSPAN header and egresses the traffic.
- Edge-Span Port (1/ 4, 1/15, 1/ 2) is the input port on which the inside packets are available for applying Tap Aggregation policy for filtering and redirection.
- Monitoring Tool port (1/5) egresses the filtered traffic to respective monitoring tool(s).

- (applicable only for topology with loopback interface) ERSPAN source tunnels are destined to the Loopback IP address of the NDB device but the tunnels are physically terminated on the Layer3 interfaces.

Workflow of Tasks

The following table lists the tasks for the workflow. Complete the tasks in the order as indicated in the table. For a detailed procedure, click the *hyperlink* of each procedure.

Procedure	Description	Result of the Task
Creating a Remote Source Interface	Creates a remote source interface, which is the input port for the NDB device.	<p>Run the show running-config command:</p> <p>Sample output for one ERSPAN tunnel (without loopback):</p> <pre> interface Ethernet1/2 no lldp transmit no lldp receive switchport mode trunk ip port access-group ndb_ipacl_Ethernet1_2 in ipv6 port traffic-filter ndb_ipv6acl_Ethernet1_2 in mac port access-group ndb_macacl_Ethernet1_2 mode tap-aggregation spanning-tree bpdupfilter enable switchport block multicast switchport block unicast interface Ethernet1/1 switchport mode trunk switchport monitor ip port access-group ndb_ipacl_global in ipv6 port traffic-filter ndb_ipv6acl_global in mac port access-group ndb_macacl_global mode tap-aggregation interface Ethernet1/30 no switchport ip address 10.10.10.10/24 no shutdown monitor session 1 type erspan-destination erspan-id 10 source ip 10.10.10.10 destination interface Ethernet1/1 no shut <Monitor Session on the switch> session 1 ----- type :erspan-destination state :up source-ip :10.10.10.10 destination ports :Eth1/1 </pre>

Procedure	Description	Result of the Task
Creating a Monitoring Port	Create a monitoring port, through which the traffic egresses to the monitoring tool.	Run the show running-config command: Sample output for one ERSPAN tunnel (without loopback): <pre> interface Ethernet1/5 no lldp transmit no lldp receive switchport mode trunk ip port access-group ndb_ipacl_Ethernet1_5 in ipv6 port traffic-filter ndb_ipv6acl_Ethernet1_5 in mac port access-group ndb_macacl_Ethernet1_5 mode tap-aggregation spanning-tree bpdufilter enable </pre>
Creating a Connection	Defines the connection between the input port and the monitoring tool port.	Run the show access-lists command: Sample output for one ERSPAN tunnel (without loopback): <pre> IP access list ndb_ipacl_Ethernet1_2 statistics per-entry 49500001 permit ip any any redirect Ethernet1/5 (match=0) 49993001 deny ip any any (match=0) IPv6 access list ndb_ipv6acl_Ethernet1_2 statistics per-entry 49500001 permit ipv6 any any redirect Ethernet1/5 (match=0) 49993001 deny ipv6 any any (match=0) 49993002 deny icmp any any router-advertisement (match=0) 49993003 deny icmp any any nd-na (match=0) 49993004 deny icmp any any router-solicitation (match=0) 49993005 deny icmp any any nd-nd (match=0) 49993006 deny icmp any any (match=0) MAC access list ndb_macacl_Ethernet1_2 statistics per-entry 49500001 permit any any redirect Ethernet1/5 (match=33) 49993001 deny any any (match=431) 49993002 deny any any 0x8848 (match=0) 49993003 deny any any 0x8847 (match=0) 49993004 deny any any 0x806 (match=0) </pre>

Creating a Remote Source Interface

Use this procedure to create a remote source interface which is the input port for the NDB device.

Procedure

Step 1 Navigate to **Components > Input Ports > Actions > Add Input Port**.

The **Add Input Port** window is displayed.

Step 2 Select the **Device** and a **Port** on the device which is to be configured as the remote source.

Step 3 Select **Remote Source Edge-SPAN** from the **Port Type** drop-down list. Enter the following details:

- a) ERSPAN ID
- b) Session Destination
- c) Remote Input port IP address

Note To create a loopback interface, check the **Use Loopback Interface** check box. If there are no configured loopback interfaces, click **Add Loopback** and configure a loopback interface. This enables terminating ERSPAN tunnel with loopback interface.

Use a loopback interface to have more than one remote input port. Traffic from an L3 interface reaches the loopback interface and from there the session destination port. If the first remote source edge span input port was created with a loopback, then the subsequent Remote Source Edge-SPAN ports must also be configured with the same loopback interface. If the first remote source edge span input port was created without a loopback, then the subsequent Remote Source Edge-SPAN ports must also be configured without a loopback interface.

Step 4 Click **Add Input Port**.

Repeat the above steps (Step 1 to Step 4) for terminating multiple ERSPAN tunnels.

What to do next

Use the **show running-config** command to verify the configurations on the input port, session destination port, and remote source port.

Creating a Monitoring Port

Use this procedure to create a monitoring port, through which the traffic egresses to the monitoring tool.

This procedure is for terminating the ERSPAN tunnel on a front panel Layer 3 port or loopback interface, either for one tunnel or multiple tunnels.

Procedure

Step 1 Navigate to **Components > Monitoring Tools > Actions > Add Monitoring Tool**.

The **Add Monitoring Tool** window is displayed.

Step 2 Enter the **Monitoring Tool Name**.

Step 3 Select the **Device** and **Port**, that will be configured as the monitoring tool port.

Step 4 Add a **Port Description**.

The other optional fields of the screen can be left as-is.

Step 5 Click **Add Monitoring Tool**.

What to do next

Use the **show running-config** command, to verify the configuration of the monitoring tool port.

Creating a Connection

Use this procedure to create a connection using the default *match-all* filter.

This procedure is for terminating the ERSPAN tunnel on a front panel Layer 3 port or loopback interface, either for one tunnel or multiple tunnels.

Procedure

- Step 1** Navigate to **Connections > Actions > Add Connection**.
The **Add Connection** window is displayed.
- Step 2** Enter a **Connection Name**.
The other optional fields of the screen can be left as-is.
- Step 3** Under **Connection Topology**, select the **Input Port, Filter** and **Monitoring Tool** to establish the connection sequence using these parameters.
- Step 4** Click **Install Connection** to add and deploy the connection on the NDB device.
-

What to do next

Use the **show access-lists** command, to verify the connection details on the NDB device.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.