Performance Routing Border Router Only Functionality

First Published: April 30, 2010
Last Updated: April 30, 2010

Performance Routing (PfR) introduced support for border router (BR) only functionality on Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1. On software images that support the border router only functionality, no master controller configuration is available. The master controller that communicates with the border router in this situation must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release. In contrast to Performance Routing Border Router Only Functionality on other platforms, Cisco ASR 1000 series routers can provide full border router passive monitoring functionality as well as active monitoring capability.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for PfR Border Router Only Functionality” section on page 12.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

- Prerequisites for PfR Border Router Only Functionality, page 2
- Restrictions for PfR Border Router Only Functionality, page 2
- Information About PfR Border Router Only Functionality, page 2
- How to Configure PfR Border Router Only Functionality, page 5
- Configuration Examples for PfR Border Router Only Functionality, page 9
Prerequisites for PfR Border Router Only Functionality

The Cisco ASR 1000 series aggregation services routers being used as PfR border routers must be running Cisco IOS XE Release 2.6.1, or a later release.

Restrictions for PfR Border Router Only Functionality

In Cisco IOS XE Release 2.6.1 support for using a Cisco ASR 1000 series router as a PfR border router was introduced. Only border router functionality is included in the Cisco IOS Release Cisco IOS XE Release 2.6.1 images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.

Information About PfR Border Router Only Functionality

To configure border router only functionality, you should understand the following concepts:

- PfR Border Router Only Functionality on ASR 1000 Series Routers, page 2
- PfR Border Router Operations, page 4

PfR Border Router Only Functionality on ASR 1000 Series Routers

PfR introduced support for border router (BR) only functionality on Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1. On software images that support the border router only functionality, no master controller configuration is available. The master controller that communicates with the border router in this situation must be a router running Cisco IOS Release 15.0(1)M. In contrast to Border Router Only Functionality on other platforms, Cisco ASR 1000 series routers can provide full border router passive monitoring functionality as well as active monitoring capability.

PfR uses three methods of traffic class performance measurement:

- Passive monitoring—measuring the performance metrics of traffic class entries while the traffic is flowing through the device using NetFlow functionality. Based on the list of learned and configured prefixes, Performance Routing passively monitors TCP flags for traffic on every flow (of the current exit) to measure latency, packet loss, and reachability. Throughput-based load balancing is still supported.
- Active monitoring—creating a stream of synthetic traffic replicating a traffic class as closely as possible and measuring the performance metrics of the synthetic traffic. The results of the performance metrics of the synthetic traffic are applied to the traffic class in the master controller database. Active monitoring uses integrated IP Service Level Agreements (IP SLAs) functionality.
- Both active and passive monitoring—combining both active and passive monitoring in order to generate a more complete picture of traffic flows within the network.
The monitoring mode is configured using the command-line interface (CLI) on a master controller which sends requests to the border routers to enable monitoring modes.

Although the configuration must be performed on a master controller, the border router (BR) only functionality in Cisco ASR 1000 series routers supports the following features:

- **OER Active Probe Source Address**—The OER Active Probe Source Address feature allows you to configure a specific exit interface on the border router as the source for active probes. For more details about configuring OER active probe source addresses, see the “Configuring Advanced Performance Routing” module.

- **OER - Application Aware Routing with Static Application Mapping**—The OER - Application Aware Routing with Static Application Mapping feature introduces the ability to configure standard applications using just one keyword. This feature also introduces a learn list configuration mode that allows Performance Routing (PfR) policies to be applied to traffic classes profiled in a learn list. Different policies can be applied to each learn list. New traffic-class and match traffic-class commands are introduced to simplify the configuration of traffic classes that PfR can automatically learn, or that can be manually configured. For more details about configuring OER active probe source addresses, see the “Static Application Mapping Using Performance Routing” module.

- **OER Support for Policy-Rules Configuration and Port-Based Prefix Learning**—The OER Support for Policy-Rules Configuration feature introduced the capability to select an OER map and apply the configuration under OER master controller configuration mode, providing an improved method to switch between predefined OER maps. For more details about configuring policy rules and port-based prefix learning, see the “Configuring Advanced Performance Routing” module.

- **OER Port and Protocol Based Prefix Learning**—The OER Port and Protocol Based Prefix Learning feature introduced the capability to configure a master controller to learn prefixes based on the protocol type and the TCP or UDP port number. For more details about configuring protocol and port-based prefix learning, see the “Configuring Advanced Performance Routing” module.

- **OER Support for Cost-Based Optimization and Traceroute Reporting**—The OER Support for Cost-Based Optimization feature introduced the capability to configure exit link policies based monetary cost and the capability to configure traceroute probes to determine prefix characteristics on a hop-by-hop basis. Performance Routing support for traceroute reporting allows you to monitor prefix performance on a hop-by-hop basis. Delay, loss, and reachability measurements are gathered for each hop from the probe source (border router) to the target prefix. For more details, see the “Configuring Performance Routing Cost Policies” or the “Performance Routing Traceroute Reporting” module.

- **BGP Inbound Optimization**—PfR BGP inbound optimization supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. PfR uses eBGP advertisements to manipulate the best entrance selection. For more details about configuring BGP inbound optimization, see the “BGP Inbound Optimization Using Performance Routing” module.

- **DSCP Monitoring**—OER DSCP Monitoring introduced automatic learning of traffic classes based on protocol, port numbers, and DSCP value. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values, with the ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested. Layer 4 information such as protocol, port number, and DSCP information is now sent to the master controller database.

---

**Note**

On Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1, the maximum number of internal prefixes that can be learned during a monitoring period is 30.
in addition to the Layer 3 prefix information. The new functionality allows OER to both actively and passively monitor application traffic. For more details about configuring policy rules and port-based prefix learning, see the “Configuring Advanced Performance Routing” module.

- Performance Routing - Protocol Independent Route Optimization (PIRO)—PIRO introduced the ability of PfR to search for a parent route—an exact matching route, or a less specific route—in the IP Routing Information Base (RIB), allowing PfR to be deployed in any IP-routed environment including Interior Gateway Protocols (IGPs) such as OSPF and IS-IS. For more details about configuring PIRO, see the “Performance Routing - Protocol Independent Route Optimization (PIRO)” module.

- Fast Failover Monitoring—Fast Failover Monitoring introduced the ability to configure a fast monitoring mode. In fast failover monitoring mode, all exits are continuously probed using active monitoring and passive monitoring. The probe frequency can be set to a lower frequency in fast failover monitoring mode than for other monitoring modes, to allow a faster failover capability. Fast failover monitoring can be used with all types of active probes: ICMP echo, jitter, TCP connection, and UDP echo. For more details about configuring fast failover monitoring, see the “Configuring Advanced Performance Routing” module.

- EIGRP mGRE DMVPN Integration—The PfR EIGRP feature introduces PfR route control capabilities based on EIGRP by performing a route parent check on the EIGRP database. This feature also adds support for mGRE Dynamic Multipoint VPN (DMVPN) deployments that follow a hub-and-spoke network design. For more details about EIGRP route control and mGRE DMVPN support, see the “Using Performance Routing to Control EIGRP Routes with mGRE DMVPN Hub-and-Spoke Support” module.

- OER Voice Traffic Optimization—The PfR Voice Traffic Optimization feature provides support for outbound optimization of voice traffic based on the voice metrics, jitter and Mean Opinion Score (MOS). Jitter and MOS are important quantitative quality metrics for voice traffic and these voice metrics are measured using PfR active probes. For more details about configuring policy rules and port-based prefix learning, see the “PfR Voice Traffic Optimization Using Active Probes” module.

- VPN IPsec/GRE Tunnel Optimization—PfR supports IP security (IPsec)/Generic Routing Encapsulation (GRE) tunnel interfaces as PfR-managed exit links. Only network-based IPsec VPNs are supported. For more details about configuring IPsec/GRE tunnel interfaces as PfR-managed exit links, see the “Configuring VPN IPsec/GRE Tunnel Interfaces As PfR-Managed Exit Links” module.

### PfR Border Router Operations

PfR is configured on Cisco routers using Cisco IOS command-line interface (CLI) configurations. Performance Routing comprises two components: the Master Controller (MC) and the Border Router (BR). A PfR deployment requires one MC and one or more BRs. Communication between the MC and the BR is protected by key-chain authentication.

The BR component resides within the data plane of the edge router with one or more exit links to an ISP or other participating network. The BR uses NetFlow to passively gather throughput and TCP performance information. The BR also sources all IP service-level agreement (SLA) probes used for explicit application performance monitoring. The BR is where all policy decisions and changes to routing in the network are enforced. The BR participates in prefix monitoring and route optimization by reporting prefix and exit link measurements to the master controller and then by enforcing policy changes received from the master controller. The BR enforces policy changes by injecting a preferred route to alter routing in the network.
How to Configure PfR Border Router Only Functionality

This section contains the following tasks:

- Setting Up a PFR Border Router, page 5
- Displaying PfR Border Router Information, page 7

Setting Up a PFR Border Router

Perform this task to set up a PfR border router. This task must be performed at each border router in your PfR-managed network. Communication is first established between the border router and the master controller with key-chain authentication being configured to protect the communication session between the border router and the master controller. A local interface is configured as the source for communication with the master controller, and external interfaces are configured as PfR-managed exit links.

To disable a border router and completely remove the process configuration from the running configuration, use the `no oer border` command in global configuration mode.

To temporarily disable a border router process, use the `shutdown` command in OER border router configuration mode. Entering the `shutdown` command stops an active border router process but does not remove any configuration parameters. The `shutdown` command is displayed in the running configuration file when enabled.

Prerequisites

- Perform the task “Configuring the PfR Master Controller: Example” section on page 9 to set up the master controller and define the interfaces and establish communication with the border routers. Only border router functionality is included in Cisco IOS XE Release 2.6.1 images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.

- Each border router must have at least one external interface that is either used to connect to an ISP or is used as an external WAN link. A minimum of two external interfaces are required in a PfR-managed network.

- Each border router must have at least one internal interface. Internal interfaces are used for only passive performance monitoring with NetFlow. Internal interfaces are not used to forward traffic.

- Each border router must have at least one local interface. Local interfaces are used only for master controller and border router communication. A single interface must be configured as a local interface on each border router.

Restrictions

- Internet exchange points where a border router can communicate with several service providers over the same broadcast media are not supported.

- When two or more border routers are deployed in a PfR-managed network, the next hop to an external network on each border router, as installed in the RIB, cannot be an IP address from the same subnet.
**SUMMARY STEPS**

1. enable
2. configure terminal
3. key chain name-of-chain
4. key key-id
5. key-string text
6. exit
7. Repeat Step 6
8. oer border
9. local type number
10. master ip-address key-chain key-chain-name
11. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> key chain name-of-chain</td>
<td>Enables key-chain authentication and enters key-chain configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• Key-chain authentication protects the communication session between both the master controller and the border router. The key ID and key string must match in order for communication to be established.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# key chain border1_PFR</td>
</tr>
<tr>
<td><strong>Step 4</strong> key key-id</td>
<td>Identifies an authentication key on a key chain and enters key-chain key configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• The key ID must match the key ID configured on the master controller.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-keychain)# key 1</td>
</tr>
<tr>
<td><strong>Step 5</strong> key-string text</td>
<td>Specifies the authentication string for the key.</td>
</tr>
<tr>
<td></td>
<td>• The authentication string must match the authentication string configured on the master controller.</td>
</tr>
<tr>
<td></td>
<td>• Any level of encryption can be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-keychain-key)# key-string b1</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits key-chain key configuration mode and returns to key-chain configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-keychain-key)# exit</td>
</tr>
</tbody>
</table>
What to Do Next

If your network is configured to use only static routing, no additional configuration is required. The PfR-managed network should be operational, as long as valid static routes that point to external interfaces on the border routers are configured. You can proceed to the “Where to Go Next” section on page 10” for information about further PfR customization.

Displaying PfR Border Router Information

Although PfR features are mostly configured on a master controller, the border routers actually collect the performance information and a number of show commands can be run on a border router. The commands in this task are entered on a border router through which the application traffic is flowing. The show commands can be entered in any order.

SUMMARY STEPS

1. enable
2. show oer border
3. show oer border active-probes
4. show oer border passive prefixes
5. show oer border routes {bgp | cce | eigrp [parent] | rwatch | static}
DETAILED STEPS

**Step 1**  
**enable**  
Enables privileged EXEC mode. Enter your password if prompted.  

```
Router> enable
```

**Step 2**  
**show oer border**  
Displays information about a PfR border router connection and PfR controlled interfaces.  

```
Router# show oer border

OER BR 10.1.1.3 ACTIVE, MC 10.1.1.1 UP/DOWN: UP 00:57:55,  
  Auth Failures: 0  
  Conn Status: SUCCESS, PORT: 3949  
  Exits  
    Et0/0 INTERNAL  
    Et1/0 EXTERNAL
```

**Step 3**  
**show oer border active-probes**  
Displays the target active-probe assignment for a given prefix and the current probing status, including the border router or border routers that are executing the active probes. The following example shows three active probes, each configured for a different prefix. The target port, source IP address, and exit interface are displayed in the output.  

```
Router# show oer border active-probes

OER Border active-probes  
Type = Probe Type  
Target = Target IP Address  
TPort = Target Port  
Source = Send From Source IP Address  
Interface = Exit interface  
Att = Number of Attempts  
Comps = Number of completions  
N = Not applicable

<table>
<thead>
<tr>
<th>Type</th>
<th>Target</th>
<th>TPort</th>
<th>Source</th>
<th>Interface</th>
<th>Att</th>
<th>Comps</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp-echo</td>
<td>10.4.5.1</td>
<td>80</td>
<td>10.0.0.1</td>
<td>Et1/0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>tcp-conn</td>
<td>10.4.7.1</td>
<td>33</td>
<td>10.0.0.1</td>
<td>Et1/0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>echo</td>
<td>10.4.9.1</td>
<td>N</td>
<td>10.0.0.1</td>
<td>Et1/0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
```

**Step 4**  
**show oer border passive prefixes**  
This command is used to display passive measurement information collected by NetFlow for PfR monitored prefixes and traffic flows. The following output shows the prefix that is being passively monitored by NetFlow for the border router on which the *show oer border passive prefixes* command was run:  

```
Router# show oer border passive prefixes

OER Passive monitored prefixes:  

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Mask</th>
<th>Match Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.5.0</td>
<td>/24</td>
<td>exact</td>
</tr>
</tbody>
</table>
```

**Step 5**  
**show oer border routes {bgp | cce | eigrp [parent] | rwatch | static}**
This command is used to display information about PfR-controlled routes on a border router. The following example displays EIGRP-controlled routes on a border router with information about the parent route that exists in the EIGRP routing table. In this example, the output shows that prefix 10.1.2.0/24 is being controlled by PfR. This command is used to show parent route lookup and route changes to existing parent routes when the parent route is identified from the EIGRP routing table.

Router# show oer border routes eigrp

Flags: C - Controlled by oer, X - Path is excluded from control,
       E - The control is exact, N - The control is non-exact

<table>
<thead>
<tr>
<th>Flags</th>
<th>Network</th>
<th>Parent</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>10.1.2.0/24</td>
<td>10.0.0.0/8</td>
<td>5000</td>
</tr>
</tbody>
</table>

Configuration Examples for PfR Border Router Only Functionality

The following example in this section shows a sample PfR link group configuration:

- Configuring the PfR Master Controller: Example, page 9
- Configuring a PfR Border Router: Example, page 10

Configuring the PfR Master Controller: Example

The following configuration example, starting in global configuration mode, shows the minimum configuration required to configure a master controller process to manage the internal network. A key-chain configuration named PFR is defined in global configuration mode.

```
Router(config)# key chain PFR
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string KEYSTRING2
Router(config-keychain-key)# end
```

This configuration is performed on a master controller. Only border router functionality is included in Cisco IOS XE Release 2.6.1 images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.

```
Router(config)# oer master
Router(config-oer-mc)# keepalive 10
Router(config-oer-mc)# logging
Router(config-oer-mc)# border 10.100.1.1 key-chain PFR
Router(config-oer-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-oer-mc-br)# interface GigabitEthernet 0/0/1 internal
Router(config-oer-mc-br)# exit
Router(config-oer-mc)# border 10.200.2.2 key-chain PFR
Router(config-oer-mc-br)# interface GigabitEthernet 0/0/0 external
```

Note

This configuration is performed on a master controller. Only border router functionality is included in Cisco IOS XE Release 2.6.1 images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.
Configuring a PfR Border Router: Example

The following configuration example, starting in global configuration mode, shows the minimum required configuration to enable a border router. The key-chain configuration is defined in global configuration mode.

Router(config)# key chain PFR
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string KEYSTRING2
Router(config-keychain-key)# end

The key-chain PFR is applied to protect communication. An interface is identified to the master controller as the local interface (source) for PfR communication.

Router(config)# oer border
Router(config-oer-br)# local GigabitEthernet 1/0/0
Router(config-oer-br)# master 192.168.1.1 key-chain PFR
Router(config-oer-br)# end

Where to Go Next

After configuring the master controller and border routers, additional configuration may be required to activate the full optimization capabilities of PfR. For more details, see the features supported in Cisco IOS XE as described in the “PfR Border Router Only Functionality on ASR 1000 Series Routers” section on page 2, and the “Configuring Basic Performance Routing” module, or other references in the “Related Documents” section on page 10.

Additional References

The following sections provide references related to the Performance Routing with NAT feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco OER commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples</td>
<td>Cisco IOS Optimized Edge Routing Command Reference</td>
</tr>
<tr>
<td>Basic PfR configuration in Cisco IOS XE releases</td>
<td>“Configuring Basic Performance Routing” module</td>
</tr>
<tr>
<td>Advanced PfR configuration</td>
<td>“Configuring Advanced Performance Routing” module</td>
</tr>
<tr>
<td>Concepts required to understand the Performance Routing operational phases</td>
<td>“Understanding Performance Routing” module</td>
</tr>
<tr>
<td>Location of PfR features in Cisco IOS XE releases</td>
<td>“Cisco IOS XE Performance Routing Features Roadmap” module</td>
</tr>
</tbody>
</table>
# Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
Feature Information for PfR Border Router Only Functionality

Table 1 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the “Cisco IOS XE Performance Routing Features Roadmap.”

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OER Border Router Only Functionality</td>
<td>Cisco IOS XE Release 2.6.1</td>
<td>Performance Routing (PfR) introduced support for border router (BR) only functionality on Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1. On software images that support the border router only functionality, no master controller configuration is available. The master controller that communicates with the border router in this situation must be a router running Cisco IOS Release 15.0(1)M. In contrast to Border Router Only Functionality on other platforms, Cisco ASR 1000 series routers can provide full border router passive monitoring functionality as well as active monitoring capability. The following command was introduced or modified by this feature: show oer border passive cache, show oer master prefix.</td>
</tr>
</tbody>
</table>

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCD, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)