

CISCO CRS-1 MANAGEABILITY

The Cisco® Carrier Routing System supports continuous systems operations and service flexibility through embedded manageability that evolves to keep pace with routing technology and service provider requirements.

PREPARING FOR MULTI-SHELF MANAGEMENT

Most core routers in today's service provider networks are single-chassis systems with numbers of interfaces that can scale to a few thousand. When managing these routers, the quantity of data collected, processed, and forwarded is proportional to the number of active interfaces.

How well does this scale? Consider a router that has a few hundred interfaces, and one or more of its interfaces go down. An alarm or group of alarms is generated and forwarded to an event console, where the alarms are correlated and operators are notified. The correlation, notification, and perhaps even resolution of the problem can occur within seconds or minutes.

Now consider what would happen when the same interfaces are configured as trunks with thousands of channelized interfaces. When one or more go down, a flood of alarms is forwarded to event consoles, forcing operators to use scripting tools such as Practical Extraction and Reporting Language (PERL) and Tool Command Language (TCL) to parse the alarms to determine the nature of the faults. Although this common practice of using custom scripts to process events becomes increasingly complex and time-consuming, it still works. The problem is diagnosed and resolved within an acceptable amount of time.

Now imagine a multi-terabit, multi-shelf routing system with hundreds of 40 Gbps slots containing several thousands of interfaces for tens of thousands of customers. Although less complex than managing individual routing elements configured to provide the same capacity, the volume of alarms rises exponentially. Can the event management system still scale to handle the load? Can event correlation and response occur quickly enough to maintain uninterrupted service and service-level agreements (SLAs) for the number of customers affected by an outage?

With the emergence of multi-shelf routing systems, the balance of where and when processing occurs must shift. Element management systems (EMS) that typically manage multiple network elements are now responsible for managing multiple system and logical elements. Integration processes that usually pass single-chassis management data to northbound operations support system (OSS) applications, must now present data to those applications from a more abstracted source.

Operators of large networks have long expected and advocated the migration of network management intelligence into the network itself. To maintain continuous system operation on multi-shelf routing platforms, embedded and modular instrumentation is required for automation of

operations, administration, maintenance, and provisioning (OAM&P) tasks. Fault, configuration, accounting, performance, and security (FCAPS) management must be in alignment with industry standards to provide integration with existing OSS applications (such as provisioning and billing) to keep revenue up and operational costs down.

CISCO CRS-1 MANAGEABILITY

The Cisco Carrier Routing System (Figure 1) is a multi-shelf routing platform based on a microkernel, distributed, and modular operating system, Cisco IOS® XR.

Figure 1
The Cisco Carrier Routing System



Recognizing that manageability needs to evolve to keep pace with the evolution of high-end routing technology, Cisco Systems® designed CRS-1 manageability within the context of multi-shelf routing. Within this context, the new distributed, modular architecture of CRS-1 places new demands on manageability, but also offers benefits to manageability processes.

In its microkernel architecture, each management process has full memory protection and fault isolation. By separating processes into planes, the management plane cannot affect or be affected by processes on the control and data planes. This modularity also offers enhanced security and the ability to modify management processes without affecting routing control functions or network traffic.

To maintain performance in an embedded management environment, the CRS-1 distributed route processor architecture allows balancing of processing demands across multiple route processors. Under heavy network management load such as data collection or alarm processing, tasks are distributed to any available resource to prevent adverse impact on critical tasks. To support OAM&P functions, persistent storage is provided through Flash memory, and hard-disk resources may be used for temporary storage of debugging and diagnostics data.

To support continuous system operation with flexible management services, CRS-1 has three key embedded manageability functions: embedded instrumentation, embedded interfaces, and embedded application services.

Embedded Instrumentation

A router's instrumentation and management interfaces are the most important aspects of its manageability. If the router does not have the proper instrumentation to provide information and control, operators and OSS applications will not be able to manage it.

Cisco CRS-1 offers embedded FCAPS management that goes beyond simple router instrumentation. By performing much of the management processing previously performed by external management applications, CRS-1 is able to respond to events and requests more quickly than single-chassis platforms and grooms data to help OSS systems scale.

- **Embedded Fault Management**

Highly scalable multi-shelf routing platforms present unique demands on existing event management systems because of the volume of traffic they process and the volume of alarms they can generate.

The embedded CRS-1 event manager supports autonomous event correlation and filtering to reduce the potential flood of events from hundreds of thousands of interfaces. User-defined event filtering and correlation policies support granularity, and event correlation automates actions on events such as launching system recovery tasks like protection switches or user-provided TCL scripts.

For example, a single event such as a line card online insertion and removal (OIR) causes several application communication and interface failure alarms. A correlation policy can be defined that links all associated events to a given root event, provided they arrive within the specified time interval. As a result, only the root event is forwarded, reducing the alarm overload on the event management system. (Users may still query the correlated events.)

The event manager also supports a user-configurable alarm buffer. An external management system or operator can structure and initiate a query to alarms in the buffer for status or trend analysis. Because of the high availability architecture of CRS-1, alarms in the buffer are check-pointed to prevent loss in the case of route processor failover or process restart.

- **Embedded Configuration Management**

Although downtime is often caused by sources outside of the network, it is also caused by sources near the network—operators. Because the configuration of a multi-shelf router is complex and failure or delay can have a detrimental impact on customer services, an embedded and intelligent configuration process is needed to maintain continuous system operation and rapid provisioning.

The embedded CRS-1 configuration manager optimizes the router configuration process during startup, operation, and OIR events. By distributing and applying changes concurrently and in bulk on startup and OIR events, mean time to repair (MTTR) is minimized. By check-pointing incremental configuration updates, the configuration manager enables CRS-1 to support configuration commit or rollback during normal operation.

To solve the challenges of the large Border Gateway Protocol (BGP) route configurations in the multi-shelf routing environment, Cisco IOS XR Software also offers a new route policy language (RPL), which is capable of scaling thousands of BGP peering operations onto a single and more compact, logical router configuration.

- **Embedded Accounting**

Accounting is an indispensable part of network management for traffic engineering, billing, and security.

To support embedded accounting management, CRS-1 offers a new version of NetFlow called Static NetFlow. While NetFlow is dynamic, with massive amounts of data collected, aggregated, and exported for analysis, Static NetFlow treats packet flow like access control lists (ACLs) do, but with extension fields such as source and destination autonomous-system number and Multiprotocol Label Switching (MPLS) labels. With Static NetFlow, a flow filter can be defined with extended ACLs to keep track of packet and byte counters of a particular flow. Static NetFlow counters are stored and retrieved in the same way as Extensible Markup Language (XML) or Simple Network Management Protocol (SNMP) counters.

For efficiency, Static NetFlow is implemented in CRS-1 hardware (microcode) to minimize the impact on the router's CPU performance. Once counters are collected, they are exported to external collectors through line card data interfaces. This averts adverse effect on performance because CRS-1 offers full separation of control and data planes.

- **Embedded Performance Monitoring**

In large networks built on single-chassis platforms, performance monitoring and trending have been difficult to perform. The volume of available data from a large number of network elements is usually too high for the performance monitoring component of the OSS to collect, store, correlate, and process. The volume also has a potentially significant impact on the network traffic between elements and collectors. Typically, the volume of collected data is restricted by targeting specific objects within platforms, as opposed to the ideal of trending across the network.

Because of the scale of multi-shelf routers, traditional data polling from a centralized application is neither adequate nor efficient. As a result, the collection of performance statistics and counters on CRS-1 are performed by the embedded performance monitor.

Cisco CRS-1 performance monitoring allows operators to define which statistics to collect, the frequency of collection, and the total number of samples to be held in memory. Collections may be configured to run on demand or periodically for trending. An on-demand collection is generally used for quick debugging and diagnostics, such as viewing percentage utilization. Whether on-demand or periodic, data collections do not affect other collections in process, and the data may be polled by, or exported to, external collectors after a collection period expires.

The CRS-1 performance monitor locally monitors counters against user-configurable thresholds on all supported entities, such as error counters for interfaces and link utilization for MPLS. Threshold conditions are set as logical operations on the value of an attribute against a threshold value (defined by percentage or absolute value). The threshold rule is evaluated at each collection interval, and a threshold-crossing alert (TCA) is generated as soon as a threshold condition or criteria is met or exceeded. Range operators allow a user to track the value of a counter within a specific range (for example, CPU utilization between 20 and 60 percent), thus providing a powerful notification mechanism when the system is not operating within the expected range. Threshold rearming rules specify whether to generate threshold notifications, even if a threshold condition is met. This avoids a flood of threshold notifications when for instance, a threshold condition is crossed repeatedly within a brief period or interval.

All collected data is check-pointed to prevent data loss in the case of route processor failover or process restart. And as with other events, TCAs generated by the embedded performance monitor can use automatic actions on events as described in the Embedded Fault Management section.

- **Embedded Security**

While instrumentation is required to protect service provider networks from losses caused by security problems, access to that instrumentation must also be protected.

Cisco CRS-1 secure management access is supported through Secure Sockets Layer (SSL), Secure Shell (SSH) Protocol, IP Security (IPSec), TACACS+, and RADIUS-based authentication, authorization, and accounting (AAA). In addition, new task-id based security profiling provides more granular control of each task than typical role-based, access controls. In task-id based security, user types may be defined and then sorted into groups. Each group is associated with a particular task group—BGP and MPLS tasks, for example—with explicit privileges (read or write).

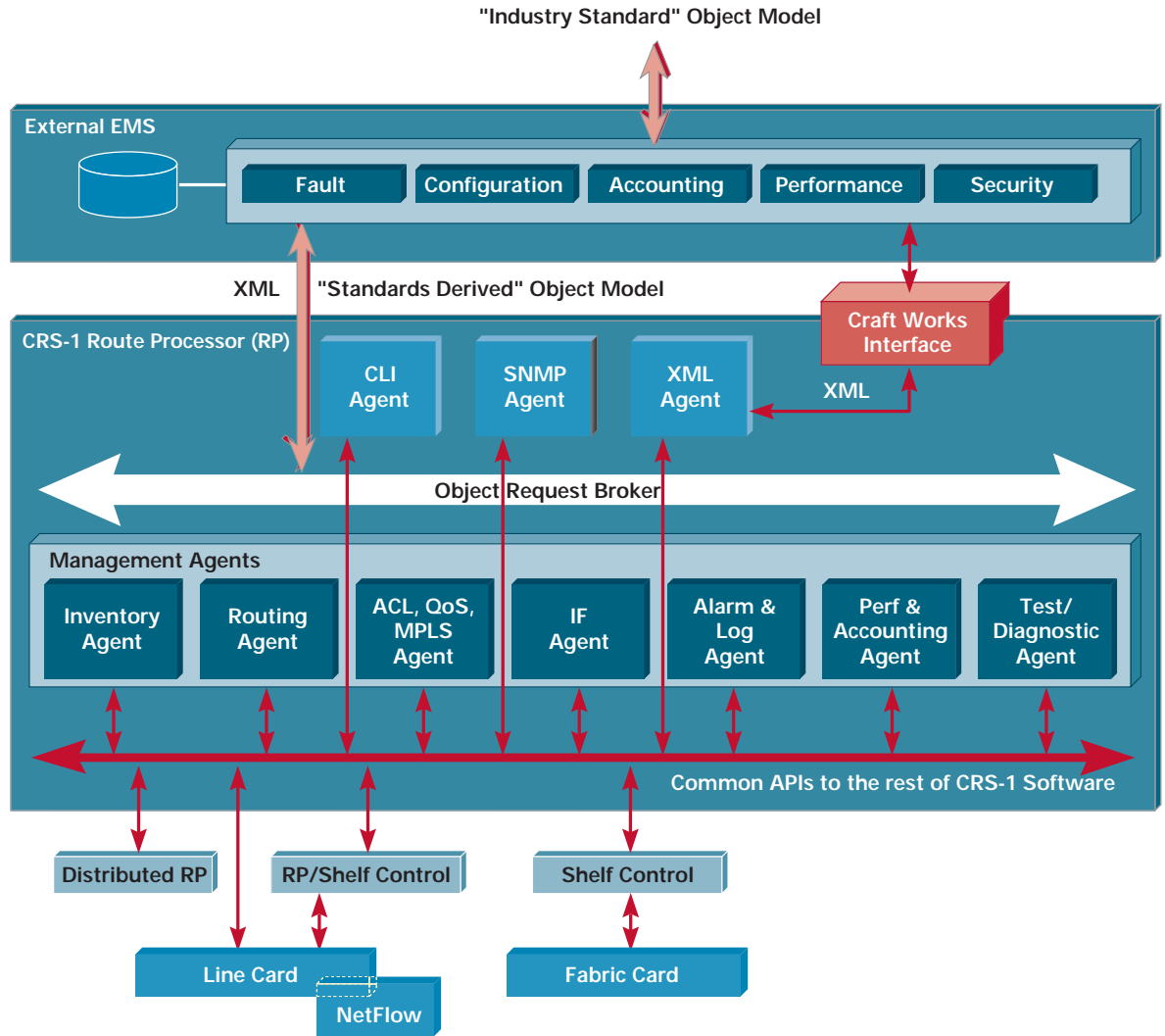
Task-id also provides flexibility in router management task authorization. To help ensure software image integrity, loadable software is digitally signed and authenticated by the installation manager during the installation process. If a package fails authentication, it will not be executed.

Embedded Interfaces

To use the information and control enabled by embedded instrumentation, a routing platform must offer access through interfaces, typically through hardware and software, called application programming interfaces (APIs). These interfaces should be open and based on industry standards. If the interfaces are proprietary, service providers pay significantly higher costs for the integration of the router into their existing OSS infrastructures. And they will continue to pay higher costs to maintain that integration as the OSS evolves, raising the router's overall cost of ownership.

Cisco CRS-1 supports both physical interfaces and standard API access (Figure 2) to the instrumentation embedded within Cisco IOS XR Software, including an internal metadata model that maintains management consistency across access schemes, whether command-line interface (CLI), SNMP, or XML:

Figure 2
Cisco CRS-1 Manageability Architecture



- **Physical interfaces**—Because a network connection to a failing or initializing device is not always available, CRS-1 supports serial console/auxiliary ports and 10/100/1000 Ethernet management interfaces on route processors and distributed route processors. As the management entry points of CRS-1, the Ethernet interfaces are routable ports, supporting ACL control to filter management access traffic according to security policies.
- **Cisco CRS-1 CLI**—As with most networking devices, CLI is a traditional management method that operators are comfortable with. Users familiar with Cisco IOS CLI will quickly learn and adapt to Cisco IOS XR CLI.
- **SNMP**—Although not always the most efficient, SNMP is one of the most pervasive protocols used by management systems. To support integration with the majority of OSS applications—event management in particular—Cisco IOS XR Software supports an extensive list of MIBs and multiple versions of SNMP, including SNMPv1, v2c, and v3.
- **XML**—Perhaps the most popular ARP for provisioning integration, XML provides an excellent mechanism for formatting, encoding, and transmitting complex data between routers and management applications.

The CRS-1 programmatic interface is provided by XML. Its rich schema enables rapid development of management scripts and customized applications for router configuration and monitoring. Using the XML interface, client applications can access CRS-1 management data by encoding the request within an XML stream and sending it to the router over a variety of transport methods such as Common Object Request Broker Architecture (CORBA). The query result is returned to the client as an XML-encoded response stream. XML tags are defined and published in router XML schema documents and may be used by client applications to encode and decode XML streams. A tagged response may be used to customize the presentation and format the data display, thus eliminating the need to parse unformatted ASCII text, which is frequently required with text-based responses.

EMBEDDED APPLICATION SERVICES—CRAFT WORKS INTERFACE

To provide a more efficient and user-friendly multi-shelf management tool, the Craft Works Interface (CWI) is an embedded Java application that uses the CRS-1 XML interface. It supports enhanced CLI features, a text editor, and a GUI (the CWI Desktop) that may be launched from a Web browser.

CWI Config Editor

Using the CWI Config Editor, users can modify and save configuration changes without committing modifications to the running configuration. Network operators benefit from standard full screen editing features such as block copy and paste, typing command completion, the ability to run syntax checks, view changes made before final commit, and verify the configurations before they are applied.

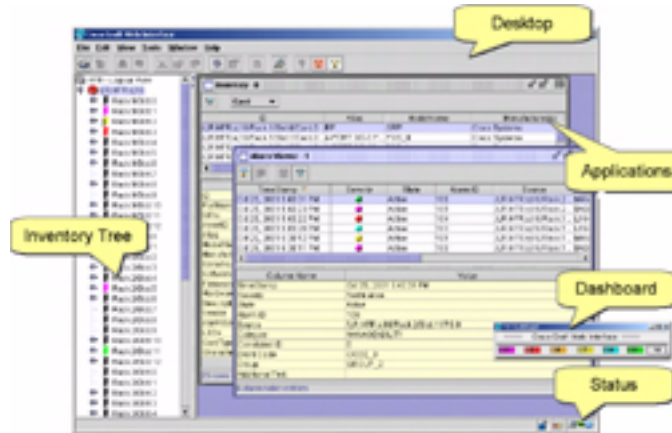
CWI CLI

Cisco IOS XR CLI supports enhanced features such as historical command recall and batch execution to make the management of CRS-1 a more personalized experience. Within SSH/Telnet windows, a local command buffer is provided to save common commands in each user's local storage. Upon login to each router, these common commands may be recalled to expedite and simplify use. In addition, a saved command file may be executed in a batch mode.

CWI Desktop

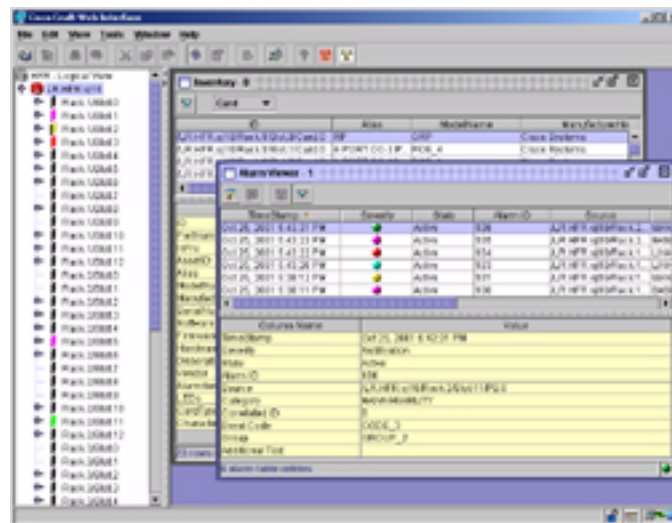
The CWI Desktop (Figure 3) provides a GUI that gives operators a visual overview of system components and their status. It provides access to some of the vital embedded FCAPS functions that CRS-1 supports:

Figure 3
CWI Desktop



- **Inventory Tree**—Because CRS-1 is a multi-shelf system, the Inventory Tree displayed in the left pane (Figure 4) presents the system in either a physical chassis or logical router view. The inventory pane can display rack, card, slot, and port information or can export it into a structured file format. The color-coding of each tree item represents component status and is based on the highest level alarm generated the CWI alarm viewer is context-sensitive; if launched against a particular component, only that component’s alarms are displayed.

Figure 4
CWI Inventory and Alarm Viewer



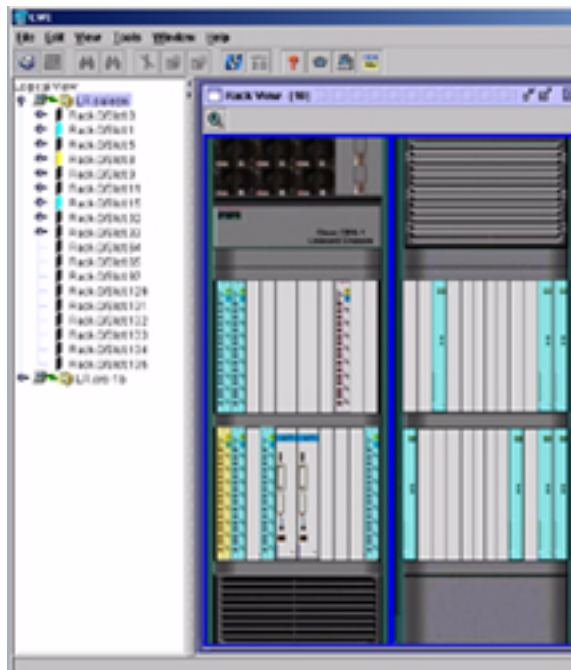
- **Alarm Dashboard**—The Alarm Dashboard (Figure 5) displays the current running alarm total for each alarm severity (Critical, Major, Minor, Warning, and Indeterminate). The right-most counter represents the total number of alarms received during the current session.

Figure 5
CWI Alarm Dashboard



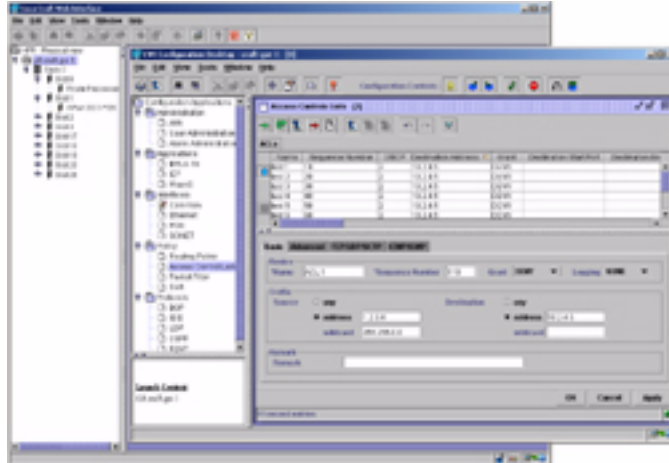
- **Rack View**—Network operators familiar with CiscoView quickly appreciate the intuitive look and feel of the CWI Rack View tool (Figure 6). LEDs within the card display may be programmed to relay simple messages from the network operations center (NOC) operator viewing the graphic representation of the chassis to field technicians at the physical chassis location. For example, a NOC operator can create a text message on a physical card to indicate to field technicians that the card may be removed.

Figure 6
CWI Rack View



- **Configuration Desktop**—The Configuration Desktop (Figure 7) provides a GUI to simplify the configuration of routing policy, ACLs, quality of service (QoS), and protocols such as BGP, Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), MPLS-TE, and Resource Reservation Protocol (RSVP). For example, assume a new MTU must be configured on all interfaces. If the number of interfaces is low, using CLI is feasible. However, when the number of interfaces is in the hundreds, or even in thousands, CLI becomes labor-intensive. In a few clicks, the CWI Configuration Desktop can apply this change across all interfaces consistently, translating to increased productivity and reduced operations costs.

Figure 7
CWI Configuration Desktop



CONCLUSION

Profitable service provider networks depend on next-generation routing platforms that offer continuous system operation and exceptional service flexibility. The key to delivering high availability and service delivery for core routing platforms is a robust manageability solution. Through the support of embedded instrumentation, interfaces, and application services, the Cisco Carrier Routing System offers an evolution of both routing and manageability technology that integrates within existing OSS environments.

For more information about complementary EMS and OSS solutions, please contact your Cisco account representative.

REFERENCES

Cisco Network Management System: Best Practices (PDF)

http://www.cisco.com/warp/public/126/NMS_bestpractice.pdf

Cisco CRS-1 System Overview

<http://www.cisco.com>

Cisco CRS-1 High Availability

<http://www.cisco.com>

Cisco CRS-1 Security

<http://www.cisco.com>



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks of Cisco Systems, Inc. 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.
(0403R) 203254_ETMG_CC_05.04