



White Paper

Cisco Adaptive Threat Defense for Education Networks

At today's colleges and universities, network applications have become an integral component of the academic environment and the institutional mission. But protecting network applications against constantly evolving threats – especially within an open academic network environment – presents major challenges. As a core component of the Cisco® Campus Secure program, Cisco Adaptive Threat Defense for Education Networks provides tools to better identify and mitigate network attacks, consolidate volumes of event data into a meaningful plan of action, and allow administrators to more proactively and effectively respond to security threats.

Introduction

At today's colleges and universities, network based applications now play an integral role in the core mission of the institution. Network applications such as cluster computing, digital libraries, IP telephony, and IP-based distance learning are increasingly becoming critical services, and must be delivered with the same degree of reliability as any other utility. But unlike a water or electricity network, an institution's IP network is under constant threat of attack from viruses, worms, and malicious users intent on harming network assets and data.

Often, an infection originating in just a single computer (which may have been or not have been properly used or updated) can propagate a worm or virus through the entire campus network within minutes. (For example, the "Slammer" worm was able to infect 90 percent of vulnerable hosts in most networks within 10 minutes.) If such attacks do not destroy or steal data, they often cause storms of excess traffic and seriously impair an institution's ability to function, resulting in downtime and lost classroom time. In addition, IT administrators in education are challenged to provide robust protection of critical IP applications, while preserving an inherently open network demanded in a college or university environment.

Colleges and universities have deployed network defenses against attacks, but with newer, faster-propagating attacks appearing all the time, even the best defenses are hard pressed to keep pace. Education networks typically include hundreds of devices and support thousands of users, resulting in thousands of active IP flows. Simply distinguishing a true attack from benign network behavior – much less mapping the path of an attack, once identified – is extremely difficult. And, if the network relies on individually deployed security solutions that are not integrated into an institution-wide system, accurately identifying, correlating, visualizing, prioritizing, and mitigating attacks in progress is an even more complex proposition.

Cisco Adaptive Threat Defense for Education Networks

As many institutions have discovered, deploying individual point solutions (such as firewalls, virtual private network [VPN] concentrators, intrusion detection system [IDS] sensors, host-based security mechanisms, and antivirus clients) that offer little support for coordination among devices often merely increase the complexity of managing network security. Today, more and more network security and IT executives are taking an alternative approach.

Emerging security solutions integrate several security functions into a single device, providing institutions with a more comprehensive, proactive, and manageable security system. Security solutions with integrated functionality are more capable of addressing the latest types of malware that make use of multiple attack mechanisms (known as "blended threats"). Multifunction

security solutions also allow institutions to protect critical resources at multiple transit points, such as VPN segments, departmental boundaries, and network DMZs.

Cisco Adaptive Threat Defense for Education represents the next generation of multifunction security solutions. The strategy focuses on two critical areas of education security: timely identification and mitigation of security threats, and optimal positioning of multifunction security solutions. This strategy is based on two core technologies:

- *Cisco Security, Monitoring, Analysis, and Response System (Cisco MARS) appliances*, which provide comprehensive security monitoring and threat mitigation.
- *Cisco ASA 5500 Series Adaptive Security Appliances*, which combine firewall, intrusion prevention, application security, network anti-virus, and VPN technology into a single device.

The combination of these two solutions offers colleges and universities the ability to implement true institution-wide security, and more intelligently and proactively defend against network attacks.

Cisco Security, Monitoring, Analysis, and Response System

Going beyond first- and second-generation Security Information Management (SIM) systems, Cisco MARS efficiently aggregates and synthesizes the massive amounts of network and security data typically generated in an education network. The solution then uses sophisticated event correlation and validation to identify network and application threats.

IT departments at educational institutions often do not have the luxury of dedicated network security staffs. Designed specifically for such environments, Cisco MARS allows even administrators who are not security specialists to easily identify and respond to attacks. Verified attacks are visualized through an intuitive, drill-down topology map to clarify incident identification, investigation and workflow. Upon attack discovery, administrators have the tools to prevent, contain, or stop an attack in real time by pushing specific mitigation commands to network enforcement devices. Cisco MARS also supports institution-centric rule creation, threat notification, incident investigation, and a host of security posture and trend reports. And, these capabilities are not limited to networks that use only Cisco network and security devices – Cisco MARS can collect and analyze data from third-party devices as well.

Conventional SIM systems provide analysts with huge, cumbersome reporting of every potential incident in the network, even though the vast majority are not actual threats. Instead, Cisco MARS uses its native intelligence to winnow down potential problems to a manageable number of incidents that can be presented to analysts for further investigation. (Comprehensive event details are saved in the Cisco MARS database to ensure that no details are lost which may need to be analyzed later.) As analysts classify false positives, Cisco MARS incorporates this intelligence, allowing it to further reduce the number incidents reported in the future. And, by centralizing this tuning at the appliance level, IT departments no longer have to perform tuning for each device.

Cisco MARS appliances are available in four sizes, depending on the security event processing power an institution requires (Figure 1). The solutions can function individually or in a distributed mode through the use of a global controller.

Figure 1

Cisco MARS Options



Cisco MARS Model	20	50	100e	100	200	Global Controller
Events/Sec	500	1000	3000	5000	10,000	N/A
NetFlow Flows/Sec	15,000	25,000	75,000	150,000	300,000	N/A
RAID Storage	120 GB	120 GB	750 GB	750 GB	1 TB	1 TB
Rack Size	1 RU	1 RU	3 RU	3 RU	4 RU	4 RU

How Does Cisco MARS Work?

To provide robust protection, Cisco MARS must maintain total awareness of an institution’s network. Cisco MARS begins by automatically discovering the network topology, including identifying network address creation and translation processes and protocols operating within the network. This process ensures that Cisco MARS can follow a network attack as it propagates, and its source and destination addresses change. The solution uses complete configuration information from routers and switches, servers, and other computers, along with information from security devices, to build a full picture of the network.

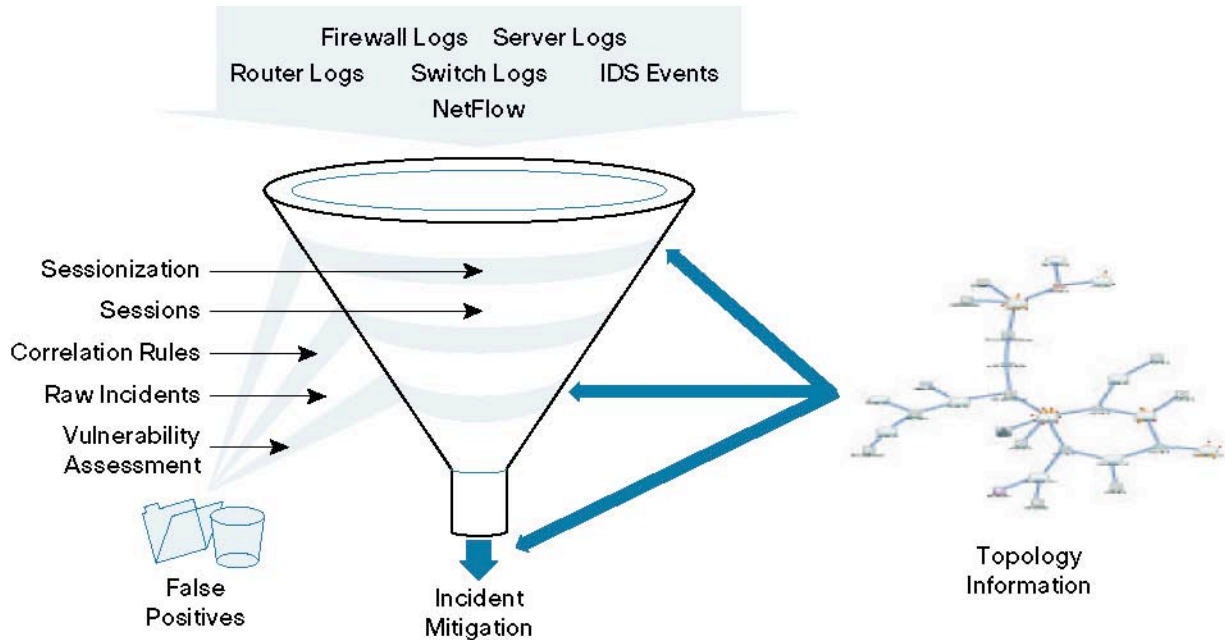
In the event of an attack, Cisco MARS automatically receives notification of network events from security devices and network components. The solution combines this event information with its network awareness to identify “hot spots” where the network attack activity is concentrated, and illustrate the path between endpoints in the network that the attack will take. Cisco MARS then pinpoints the specific network or security device where an administrator can mitigate the attack, and provides the necessary device configuration information to stop the dangerous traffic.

Identifying and Mitigating Attacks

Figure 2 (Read from top to bottom.) illustrates the innovative process which Cisco MARS uses to transform a flood of raw network event data into actionable information that is used to mitigate network attacks.

Figure 2

From Network Events to Event Mitigation



This transformation proceeds through six steps:

1. *Identification* – A typical college or university network may experience thousands of events per second at peak periods, or many millions of events per day. Multiple devices on the network, including security devices, network routers and switches, and network endpoints such as servers send logging and network information to Cisco MARS. The solution can also collect Cisco IOS® Software NetFlow data from routers and switches, allowing it to integrate event data with network performance and accounting data. This process can help Cisco MARS identify anomalous network activity through environmental changes, such as a sudden increase in traffic levels.
2. *Aggregation* – Using a process called Sessionization, Cisco MARS uses its network topology awareness to combine multiple events into end-to-end sessions. For example, Figure 3 shows a typical session with three network devices (a firewall, a Network IDS [NIDS] sensor, and a NIDS blade within a switch) reporting the events. Cisco MARS relies on its awareness of network address translation processes to relate these events and follow an attack as network addresses change along the attack path.
3. *Correlation* – Cisco MARS then uses a technique called Session-Based Active Correlation, which incorporates built-in and user-defined rules, to correlate information about multiple sessions with NetFlow data, and identify potential candidates for complete network attacks, referred to as incidents.
4. *Evaluation* – For each candidate incident, Cisco MARS performs automatic vulnerability scanning. This involves checking whether the attack was successful in reaching its target (The attack may have been blocked by a firewall or by a host-based IDS mechanism in a server.) and whether the target is actually vulnerable to the attack. (An endpoint’s operating system may not be susceptible to the specific attack, even if it was targeted.) This automatic vulnerability scanning allows Cisco MARS to identify false positives, and build rules to reduce future analysis and processing requirements for candidate incidents.
5. *Mitigation* – If the attack is a genuine incident, Cisco MARS then notifies the administrator, and provides mitigation instructions as described above. The solution uses a process called Precision Tracking to automatically gather host information (to the level of the

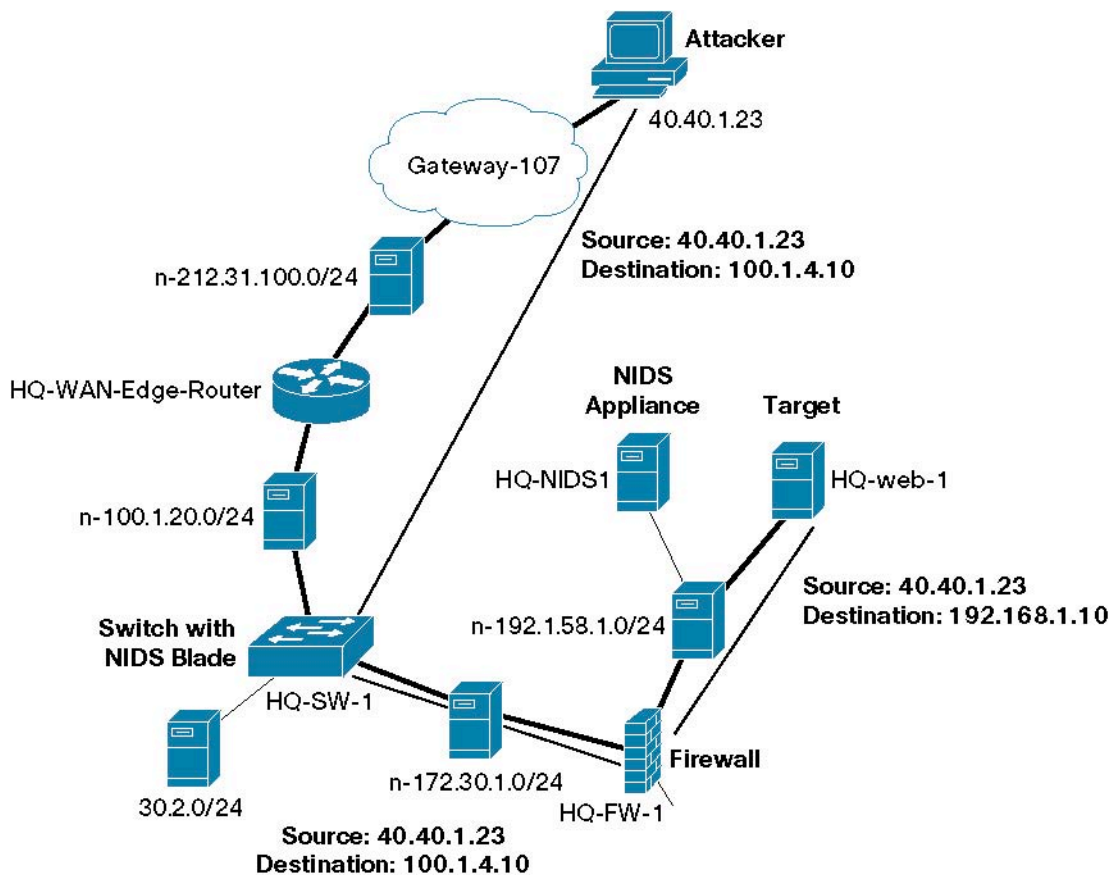
MAC address) to provide complete information about real incidents. In practice, the millions of events per day are reduced to dozens of incidents – a volume of which is well within the ability of a single administrator to interpret and act upon.


6. *Classification* – The administrator can now review a manageable number of incidents that require determination as to whether they are true incidents or false positives. Using Cisco MARS' One Click Tuning feature, administrators can classify false positives with a single decision and quickly reduce the number of future incidents reported by the solution. Centralizing this tuning at within the Cisco MARS appliance removes the need to perform tuning for multiple network devices. The Cisco MARS database also serves as a central repository for all event details, ensuring that no information is lost which may need to be analyzed later.

Aggregating Multiple Events into a Single Session

As an example of the above process, consider the path of an incident as shown in Figure 3. The network topology in this illustration is only one small segment of an overall network, selected because it shows an entire incident path. Individual network events are logged at three points: the NIDS blade on the switch, the firewall, and the NIDS sensor, which monitors the network between the firewall and the target. Cisco MARS receives notification of these events and, using its awareness of the network topology and address translation processes at various points in the network, combines the events into a single session. In Figure 3, note that the destination address of the attack is changed as it is translated at the firewall. Cisco MARS can determine that the events on either side of the firewall are part of the same session despite the different addresses.

Figure 3
Cisco MARS Sessionization During an Attack





The Cisco MARS system compares the details of the session (intra-session correlation) and the details of other sessions (inter-session correlation) to its internal rules to identify a potential incident. If there is a potential incident, the appliance performs a vulnerability analysis, based on an actual scan of the target of the incident, to decide whether there is an actual incident to report and mitigate, or whether this is a false positive to be ignored.

Going Above and Beyond Conventional SIM Systems

Cisco MARS can be used at its simplest level as an efficient, high-performance SIM system. However, institutions can also use the solution to analyze previously received data in order to identify network traffic patterns and perform forensic analysis of network attacks.

Unlike typical SIM systems, Cisco MARS allows for security threat management on several new levels:

- *Thorough data reduction* – Cisco MARS, with its deep awareness of network topology and addressing, can reduce millions of security events to hundreds of actual reported network incidents.
- *Timely attack mitigation* – Cisco MARS incorporates both high performance and built-in expertise to recognize and recommend mitigation for attacks before they can bring down an entire network.
- *End-to-end network awareness* – Using the full configurations of all types of network devices and endpoints, Cisco MARS integrates address translation and MAC address information to identify attackers, targets, and network hot spots, and presents this information graphically to allow quick action.
- *Integrated vulnerability assessment* – Cisco MARS determines whether a possible network attack is genuine or a false positive, further reducing the number of alarms and the time needed to take action.
- *Patent-pending Event Correlation Engine* – Cisco MARS' high-performance inter-session correlation, combined with its highly flexible rules framework, enables timely analysis and mitigation of incidents.
- *One Click Tuning* – Cisco MARS helps administrators and network security analysts focus on the real problems that need immediate attention, without losing any event data that may be needed at a later time. The solution also allows administrators to continually tune the system for even more effective future operation.

Figure 4 compares conventional SIM products to Cisco MARS. The first generation of SIMs concentrated on handling large volumes of security logging data, and provided a small amount of analytic tools for performing forensic analysis. Next-generation systems expanded forensics tools, but focused on better understanding what has already happened, rather than what is currently happening. Cisco MARS provides many additional levels of analysis, with an emphasis on mitigating network security events as they occur, as well as reducing the volume of data that administrators must process.

Figure 4
Comparison of SIM and Cisco MARS

	Collect and Manage Logs	Forensic Analysis - What Happened?	Identify Hot Spots	Graphical Attack Pattern	High-Performance Active Correlation	False Positive Tuning	Timely Attack Mitigation
First-Generation SIMs							
Second-Generation SIMs							
Cisco MARS							

The security event identification and mitigation capabilities of Cisco MARS can provide colleges and universities with unprecedented visibility into institutional networks and much greater intelligence to effectively respond to attacks. However, when combined with Cisco ASA 5500 Series Adaptive Security Appliances, institutions can implement truly ubiquitous security.

Cisco ASA 5500 Series Adaptive Security Appliances

In an education environment, networks constantly face new, highly sophisticated attacks, as well as embedded data and stealth probing. To preserve a secure educational environment (as well as comply with government-mandated information security regulations), colleges and universities have historically deployed a variety of network security technologies. These solutions have included firewalls, VPNs, antivirus systems, Web and application security systems, IDS and intrusion prevention appliances, authentication systems, and host-based security mechanisms.

Previously, colleges and universities had to rely on standalone solutions for each of these services (often from multiple vendors), which increased network complexity and demanded substantial human and financial resources. But today, colleges and universities are increasingly turning to converged, next-generation network security solutions, in which all of these services can be delivered with a single, integrated platform.

The Cisco ASA 5500 Series combines world-class firewall features, IPSec and SSL VPN capabilities, and industry-leading Intrusion Prevention System (IPS) services with a centrally managed, user-friendly GUI. The result is easier setup and management of security solutions, and more effective protection of education networks based on sophisticated, field-proven security technologies (Figure 5).

Figure 5

Aggregate Security Services in the Cisco ASA 5500 Series

Multifunction Threat Mitigation and VPN	Minimal Deployment and Operations Costs	Adaptive Identification and Mitigation
<ul style="list-style-type: none"> ▪ Built on market-proven technologies ▪ High speed – No services performance degradation ▪ Comprehensive security services profile enables uniform network security ▪ Converged services detect and stop worms, viruses, and malware at line rate ▪ Flexible VPN (SSL or IPSec) for any scenario 	<ul style="list-style-type: none"> ▪ Single device, many uses – Platform standardization lowers operations and deployment costs ▪ Network-aware security – No network disruption ▪ Extensive policy flexibility through Modular Policy Framework and virtualization ▪ Easy management of all services via single GUI 	<ul style="list-style-type: none"> ▪ Adaptive security – add new services as needed, without new equipment ▪ Adaptive Security Processing delivers unprecedented technology extensibility ▪ No trade-offs – Services breadth and performance ▪ Extensive services roadmap – Anti-X, Control and Containment, Application Security

Like Cisco MARS, several sizes of Cisco ASA 5500 Series appliances are available, depending on the performance required (Figure 6). Institutions can deploy an ideal solution for any environment, from a small department to the campus network core.


Figure 6

Cisco ASA 5500 Series Options

	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540
			
School Location	Department	Campus Edge	Campus Core
Performance Max Firewall Max Threat Mitig. (FW+IPS) Max IPSec VPN	300 Mbps 150 Mbps 170 Mbps	450 Mbps 375 Mbps 225 Mbps	650 Mbps 450 Mbps 325 Mbps
Base Platform Services	App FW, IPSec and SSL VPN, and more A/S HA (upgrade), 3 FE to 5 FE	Same as 5510, plus A/A Failover, VPN Clustering, 4 GE + 1 FE	Same as 5520, with higher performance and scalability

Evolving Education Security Threats

The threats facing education networks are constantly evolving. In just the past year, the types of security attacks on education networks have changed dramatically. Today, the most frequently encountered threats are worms such as Netsky, which spread by sending out copies of themselves as e-mail attachments using a built-in Simple Mail Transfer Protocol (SMTP) engine. These worms gather target recipients from certain files found on the affected machine, turning an affected system into a virtual propagation launch pad.



The hacking community is also evolving, as growing numbers of casual hackers are “graduating” to become experts. While casual hackers tend to not have specific targets and seldom intend to do damage, the expert class of individuals intend significant harm, and are becoming more organized in their efforts to conduct identity fraud and cyber-warfare.

In its 2004 semi-annual [Internet Security Threat Report](#) – an analysis of malicious code including worms, viruses, Trojans, backdoors, and blended threats – Symantec indicates that malware is increasingly being designed to steal personal data, particularly financial information and passwords. This trend should be alarming news for educational institutions, since they house thousands of student and faculty records. In addition, many colleges and universities are now seeing newer versions of intelligent malware in their networks, which are capable of adapting to the environment they are attacking. If one approach doesn’t work, the malware tries another.

Faced with this dynamic threat environment, college and university IT departments must focus on stopping threats at a single transit point in the network. The Cisco ASA 5500 Series is the ideal solution for such a strategy.

Enhancing Network Protection

In networks that manage firewall, IDS, Anti-X, VPN, application protection, and peer-to-peer control through separate devices, a threat is capable of getting deeper and deeper into the network, until it reaches the specific security device capable of stopping it. (For example, a threat that can get past a firewall can continue traveling into the network until it reaches another IPS device capable of stopping it.) Since the Cisco ASA 5500 Series consolidates several security functions into a single chassis, threats can be stopped at the single point in the network where the solution is deployed. (For example, many institutions position the solution in VLANs where wireless users connect to the network.)

In addition to providing more effective security, integrated Cisco ASA 5500 Series solutions can dramatically reduce the costs and complexity of deploying and managing multiple security devices. And, when multiple security services are converged within a single device, they also are capable of mutual awareness and communications, providing IT and network security administrators with an extremely powerful tool for protecting education networks. When combined with an overarching security mitigation system such as Cisco MARS, colleges and universities can achieve an even more effective and efficient security environment, and ultimately, a true self-defending network.

Providing Comprehensive Threat Defense with the Cisco MARS and the Cisco ASA 5500 Series

While Cisco MARS and the Cisco ASA 5500 Series solutions can offer substantial advantages deployed individually, when operating together the solutions provide an intelligent, comprehensive, and highly effective security strategy for colleges and universities. By combining Cisco MARS’ industry-leading threat identification and mitigation capabilities with the integrated security services of Cisco ASA 5500 Series solutions, institutions can immediately deliver virtually any security function to any part of the network. And, all of these services can be managed easily and centrally – even by network administrators who are not dedicated security specialists.

Today’s colleges and universities face substantial security challenges. As vast networks in an open academic environment, education networks can present an ideal target for opportunistic hackers. But with the next-generation security intelligence and capabilities of Cisco MARS and the Cisco ASA 5500 Series, colleges and universities can effectively protect their students and faculty from even the most malicious network threats.

**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 Website 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 © 1992–2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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. (0502R) JS/LW9391 09/05