White Paper

Application Visibility: Cisco ISR-AX at the Branch Delivers Your BYOD Solution

In 2011, IDC research reported that for the first time ever, more devices shipped without an Ethernet port than with one. As IT administrators prepare for this onslaught of wireless mobility in the workplace, we are faced with more challenges than ever before - how much bandwidth is enough? What types of devices might show up? Today most personal devices are Apple or Android devices - but what about next year? How can IT administrators prepare for an unknown set of devices, with unknown bandwidth and connectivity requirements, with the same number of resources, and still rest assured that they can confidently say their networks are secure, high-performance, and ready for the next wave of new technology?

This situation describes the bring-your-own-device (BYOD) predicament. Efforts to allow users to bring their own devices to work in order to improve productivity and mobility are countered by the worry that devices may not be secure and that workers may be distracted by applications rather than using the device for work activities. But above all, supporting and troubleshooting these unmanaged devices and the effect they may have on the network could place an overwhelming burden on the limited IT staff.

In a recent survey of workers[1], more than 80 percent of them bring their personal devices to work, and 87 percent of those are using them for work-related activities. These devices bring new requirements like security, mobility and wireless in motion. It also brings focus on the identity of devices and users accessing the Enterprise data from these unmanaged devices. They have become the primary access for network connectivity, and thus have affected the traffic flows across these networks. Protocols such as Secure Sockets Layer (SSL) are used to encrypt web applications and email, whereas other protocols such as Control and Provisioning of Wireless Access Points (CAPWAP) are used to address central management, control, and security of wireless networks by providing standard access to wireless networks management and data traffic, but both of these protocols can directly affect the WAN when the BYOD environment is introduced at the branch offices. Enterprises realize that connectivity across WAN has its own challenges in terms of bandwidth, latency, management of remote devices and want uniformity on how they allow users to bring their own devices.

[1] Dimensional Research, “Consumerization of IT: A Survey of IT Professionals”, Dell KACE 2011.

With the number of devices that will access the network is estimated to go up 2-3 times, IT administrators have a tough time to scale their systems and network resources. One major constraint would be the WAN bandwidth itself which has to be provisioned to handle traffic for these new devices. Challenges could also be in terms of network access itself, identity of these devices and user policy enforcement based on the internal requirements.

While IT administrators may not be able to control the devices themselves, they can control the traffic to and from these systems, and ensure that an optimized solution with full application visibility is in place to address performance concerns. These new BYO devices are not replacing the existing systems, they are rather net additions to the infrastructure. Each has its own profile and all are accessing email, web portals, and other web-based applications. And yes, people are accessing Netflix and Facebook on them too. So if these applications are encrypted or are using CAPWAP, IT administrators are challanged when it comes to enforcing network policies defined to maintain a consistent end-user experience for corporate applications. Tunneling applications are nothing new, but when you cannot tell the difference between a Citrix client accessing your corporate virtual desktop Infrastructure (VDI) and a client accessing Netflix to watch a TV episode, then there is concern.

The Cisco® Application Visibility and Control (AVC) and Wide Area Application Services (WAAS) solution, part of the Cisco Integrated Services Router Application Experience (ISR-AX) portfolio, provides the IT administrator with the two major components in addressing these challanges. Cisco ISR-AX is a single -box solution based on the Cisco Integrated Services Routers Generation 2 (ISR G2) that extends the role of the router to an application-delivery platform. Cisco ISR-AX includes application services including WAAS and AVC that enable business applications to run faster, reduce bandwidth costs and latency by more than 50 percent, and simplify IT with probe-less visibility networkwide, lowering the barriers for deploying and consuming applications across cloud and BYOD environments.

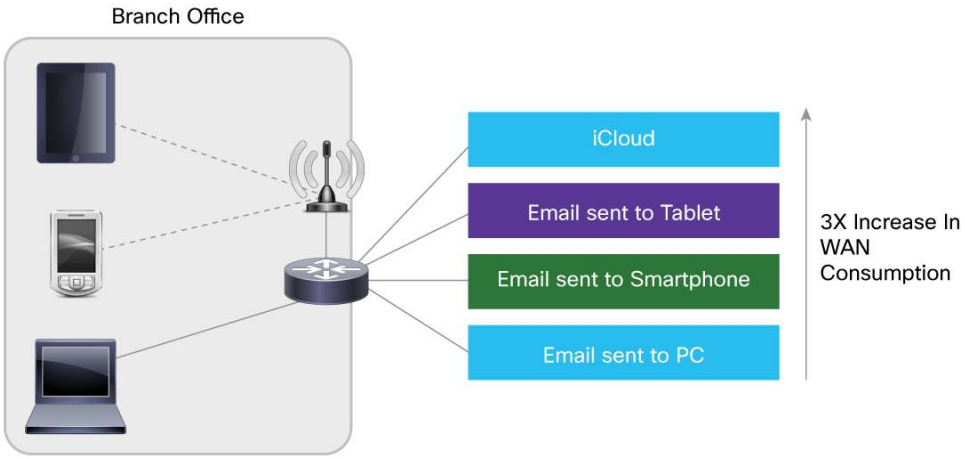
First component of Cisco ISR-AX for BYOD is the application visibility. In order to apply any network policies, you must be able to differentiate BitTorrent traffic from your enterprise portal traffic. The second is WAN optimization. Think about this use case: Molly comes to work, turns on her PC, and launches her email client, then while she is walking to her staff meeting she uses her iPad to see what email messages she can skim through on her way to the meeting room; finally in the meeting she looks down at her iPhone to see the emergency email she just received. This new connected employee phenomenon is happening every day, and if you followed this senario you now realize that Molly has not **one** but **three** devices - all accessing her email at the same time. Her bandwidth consumption just jumped threefold (See Figure 1). When you add this extra traffic to the web and VDI traffic that all these devices can also access, you realize that the average user consumption of bandwidth can and will affect any WAN circuit. Cisco AVC and WAAS can and do solve this challenge. AVC provides the ability to recognize more than 1000 applications to apply and enforce network policies, and Cisco WAAS provides the WAN optimization to control WAN bandwidth and provide application acceleration. See Table 1 for summary of the components.

Table 1. Branch BYOD Components

Features	Description	Benefits
Wireless	One Network: Cisco wired, Wi-Fi and 3G/4G networks are converging. Hotspot 2.0 unifies cellular and Wi-Fi, and Cisco is developing small-cell solutions to remove the border between networks. Policy and management for wired and Wi-Fi are unified in a single platform.	Standards based data stream access
WAAS	Cisco WAAS provides an elastic “scale as you grow” enterprise-wide deployment model. A software- and hardware-integrated, cloud-ready WAN optimization and application acceleration solution. WAAS appliances offer outstanding deployment scalability and design flexibility while WAAS software delivers best-in-class application acceleration for the enterprise network.	Application Acceleration and Bandwidth Optimization
AVC	Cisco Application Visibility and Control (AVC) provide a powerful, pervasive, integrated service management solution based on stateful deep packet inspection (DPI).	Proactive monitoring of application visibility

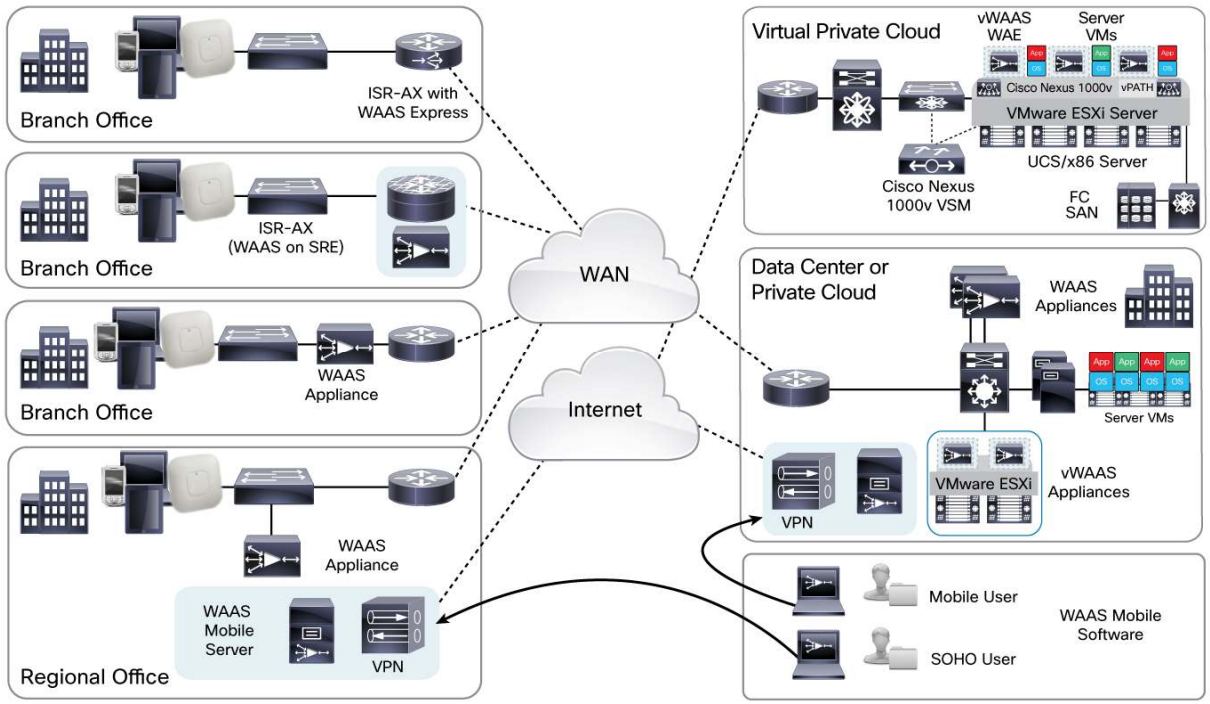
Features	Description	Benefits
Cloud Web Security	Enforces a consistent Web Security policy for all Web traffic generated from an Enterprise.	Zero Day Spyware Malware Protection

Figure 1. BYOD Doubles or Triples the Amount of Traffic to and from the Branch



IT administrators can follow this reference architecture as a base template in their organizations' branch-office BYOD planning. This solution is based on the three primary components of the Cisco portfolio: Cisco Wireless Access Points, Cisco WAAS, and the Cisco AVC solution. Figure 2 shows an example of a BYOD enterprise network design. More details about all of these components is available at: http://www.cisco.com/web/solutions/trends/byod_smart_solution/index.html.

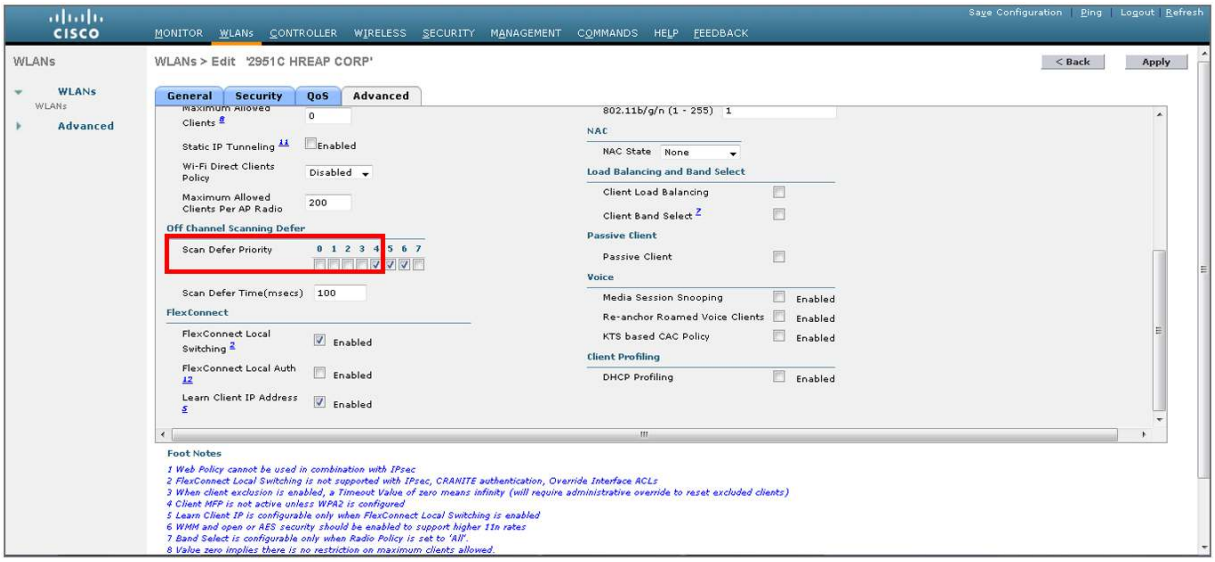
Figure 2. BYOD Enterprise Reference Design



Wireless: Cisco Access Points and FlexConnect

The first requirement in supporting wireless BYO devices is the ability to separate the two planes of the CAPWAP traffic. CAPWAP has both a management plane and a data plane. In normal flows these two planes are encapsulated together from the access point all the way back to the wireless LAN controller. Only then is the data plane separated out and sent off to the server or service requested by the client. It is this CAPWAP tunnel that IT administrators need to address. While the data is in this tunnel, application policies such as quality of service (QoS), security, and WAN optimization cannot be enforced. With the Hybrid Remote-Edge Access Point (H-REAP) solution, Cisco Wireless Access Points can use their FlexConnect modes to provide local switching of the data plane in the CAPWAP traffic (Figure 3). Full FlexConnect details and deployment are beyond the scope of this document, but you can find more information at: http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bcb905.shtml.

Figure 3. Cisco FlexConnect to Enable Local Switching



WAN Optimization: Cisco WAAS

When the Cisco Wireless Access Point has separated out the data traffic and placed it on the branch-office LAN segment, network policies such as WAN optimization and Visibility and AVC can now be applied.

Cisco WAAS is a comprehensive, cost-effective, cloud-ready WAN optimization solution that accelerates applications, optimizes bandwidth, provides local hosting of branch-office IT services, and enables cloud services - all with industry-leading network integration. Cisco WAAS allows IT departments to centralize applications and storage while maintaining productivity for branch-office and mobile users.

Cisco WAAS enables branch-office BYOD rollouts by addressing the following primary IT objectives:

- Enhance productivity by mitigating the effects of WAN latency: Applications perform better, and data is transferred faster.
- Optimize SSL-based web applications such as Office 365 along with BYOD apps such as Mail or other custom Apps that use secure network connections.
- Accelerate Citrix VDI traffic to tablets.

- Reduce bandwidth consumption, delaying or eliminating increased recurring bandwidth costs: Cisco WAAS enables IT consolidation, reducing both capital and recurring expenses for branch-office IT infrastructure.
- Lower operating costs by providing on-demand WAN optimization with integration into Cisco ISR G2 routers through Cisco IOS® Software-based Cisco WAAS Express, Cisco WAAS on Cisco Services-Ready Engine (SRE) Modules or UCS E-Series servers.
- Allow migration of business applications to the cloud without affecting application performance for end users in remote branch offices, campuses, and data centers.
- Enhance business continuity by reducing backup windows[2] and achieving recovery-point objectives (RPOs) for storage administrators.
- Offer a superior end-user application experience by enabling rich-media and collaborative applications with high performance without affecting the performance of other applications across the WAN.

Cisco WAAS is deployed on a physical appliance, virtual appliance, router-integrated service module, or router-integrated Cisco IOS software on each side of the WAN to provide application-specific acceleration and WAN optimization capabilities. You can deploy Cisco WAAS appliances out of the data path or physically in-path in the data center or in the remote branch office, and you can deploy Cisco WAAS network modules as well as service modules out-of-path in the branch office. Regardless of the deployment model, Cisco WAAS provides application performance improvements and enables centralization without compromising high availability and scalability by providing intelligent load-distribution and fail-through operation.

Cisco Application, Visibility, and Control

Cisco AVC provides a powerful, pervasive, integrated service management solution based on stateful DPI. With the Cisco AVC solution, the Cisco ASR 1000 Series Aggregation Services Routers (ASR 1000s) and Cisco ISR G2 routers can identify applications within the traffic flow. They can then collect various application performance metrics on those applications such as bandwidth use, response time, or latency.

Using Cisco industry-leading QoS, these routers can reprioritize critical applications or enforce application bandwidth use to improve application performance. With the Cisco AVC, network administrators can:

- Discover network traffic with application-level insight that includes deep packet visibility into cloud traffic
- Analyze and report on application usage
- Classify and manage application sessions (for example, web browsing, multimedia streaming, and peer-to-peer applications)
- Proactively monitor application usages and anomalies
- Build reporting for capacity planning and compliance

[2] Cisco WAAS reduces backup windows for distributed data, that is, data still stored in branch-office sites and backed up over the WAN. Conversely, Cisco WAAS enables data to be centralized, further reducing backup windows and enhancing restore operations. Multiple use cases exist because WAN optimization and Cisco WAAS pertain to backup optimization, and appropriate messaging needs to be delivered depending on the target audience and the architecture.

Products and Technologies

The Cisco AVC solution consists of recognition technologies on the Cisco ISR G2s and ASR 1000s, as well as visualization and reporting capabilities on management platforms, including:

- Next-generation DPI technology called Network-Based Application Recognition 2 (NBAR2), which can identify more than 1000 applications and support application categorization without requiring a new Cisco IOS Software release.
- Cisco Flexible NetFlow (FNF) infrastructure and NetFlow v9 export to select and export data of interest.
- Application Response Time (ART) engine to collect TCP performance metrics that can be used to measure end-user experiences.
- Reporting and management tools, such as Cisco Prime™ Infrastructure, an enterprise-grade infrastructure and service monitoring tool for use in reporting of application and network performance.
- Modular QoS to facilitate optimization and control of application performance.
- Use of the Cisco Flow Agent (FA) within WAAS to share flow information into the Cisco Prime enterprise and service provider management portfolio (refer to Figure 4).

Figure 4. Cisco Flow Agent and Performance Agent

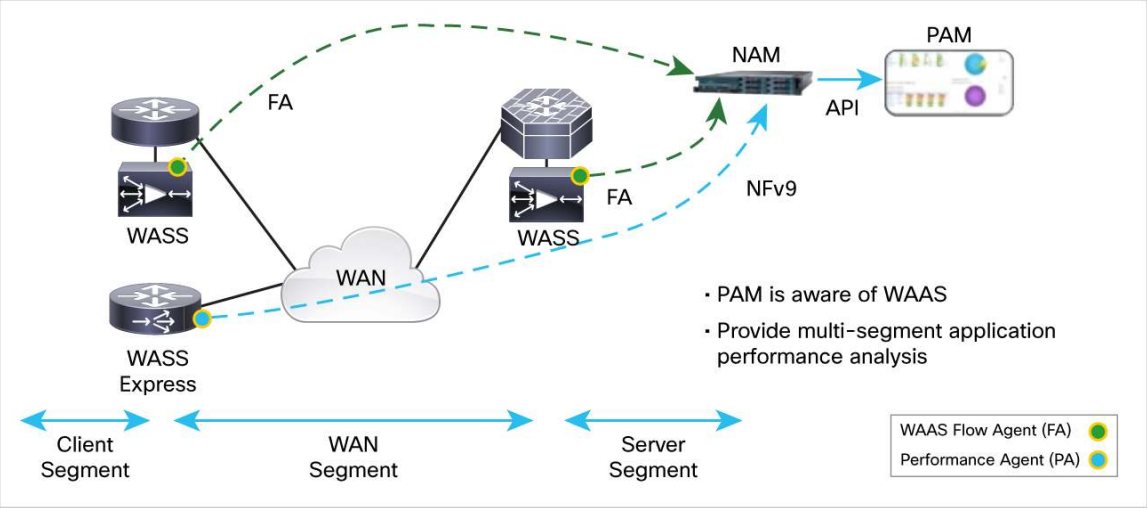


Table 2 describes the components of Cisco AVC.

Table 2. Cisco AVC Components

Component	Description	Technology
Application recognition	Identify applications using DPI NBAR2.	NBAR2
Performance collection and exporting	Cisco ISR G2 and ASR collect application bandwidth and response-time metrics, and can export to the Cisco Prime application. Flow Agent (FA) reports response -time metrics from Cisco WAAS devices.	Flexible NetflowNetFlow and Application Response Time Engine
Management tools	Advanced reporting tools in Cisco Prime Network Analysis Module (NAM) aggregate and report on application performance.	Cisco Prime NAM and Cisco Prime Infrastructure
Control	Control of application usage in the network maximizes application performance and network variances.	Performance Routing and QoS

Delivering the End-User Experience for Mission-Critical Apps: Citrix VDI

With this solution from Cisco, IT administrators can address the BYOD challenge. By addressing the three pillars of AVC plus WAN optimization in a totally wireless deployment model, IT administrators can deploy high-demand applications such as Citrix to provide controlled access to employee devices.

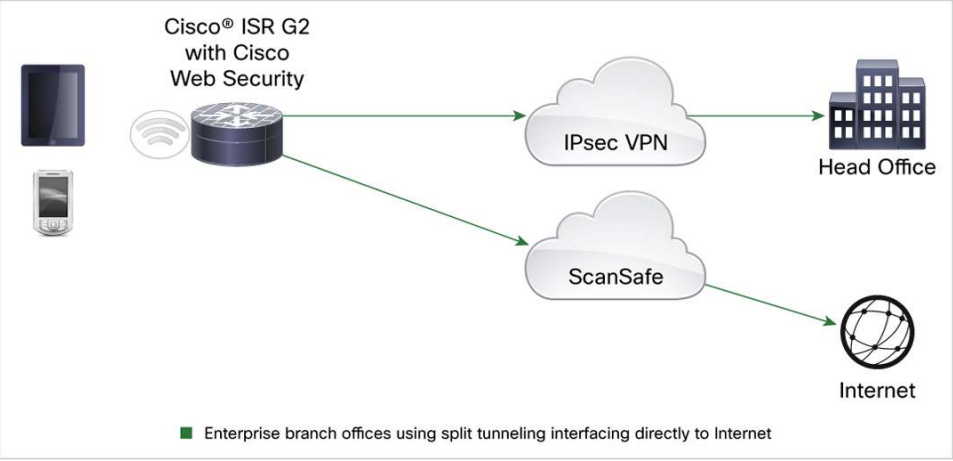
The end-user experience of applications on personal devices will still mandate QoS and security policies. End users will expect better performance than what they can access from their home broadband services. Cisco WAAS can optimize the core Citrix applications, increasing the client density in the branch office while also maintaining a consistent end-user experience for the new device platforms. Empowering users to use their own devices has been shown to improve productivity by giving clients greater degrees of collaboration. At the same time tools such as Citrix xenApps or xenDesktop allow IT administrators to protect sensitive information that is subject to an organization's privacy or compliance mandates without the need to push special applications onto the personal devices or restrict a BYOD policy to only special types of devices.

Secure Policy Enforcement

Enterprises have certain policies applied for the Web traffic on their campus networks which they would want to emulate on the branches as well. As this needs to be consistent across their network the Cisco Cloud Web Security (formerly Scansafe) allows them to ease in administration to have the similar policies for all their Web traffic emanating from all Branch Networks.

Typically enterprise branches have all their traffic encrypted over the public/private network which is sent to the enterprise headend and web traffic split tunnelled onto the Internet. The ISR G2 has the Cisco Cloud Web Security (CWS) connector (See figure 5) which redirects all web traffic to the CWS cloud which applies the various policies on the traffic. The Cisco CWS solution does URL filtering, Zero Day Malware Protection, Heuristic Malware Identification, Protection against Phishing attacks and Granular Reporting. This allows enterprises to ensure security for their web traffic and not have all web traffic backhauled to their enterprise headend and freeing up the WAN Bandwidth for other crucial enterprise applications like Mail, SAP, etc.

Figure 5. Cisco Web Security Connector on the ISR G2



Also, the Cisco CWS solution on the ISR G2 is integrated with other solutions like the Cisco ISE which allows Enterprises to Authenticate and Authorize users to maintain control and provide differentiated access. Identity of these devices can be obtained via multiple methods like Active Directory, Web Auth, etc and the Identity is encrypted before it is sent to the Scansafe Cloud. The Rules and Alerts can be configured differently on the Scansafe cloud for Corporate owned Devices and BYOD devices. It could for instance disallow Guest users access to Entertainment/Sports websites whereas Enterprise users would still have access. Cisco CWS allows you to have policies configured for a group of users (for ex. the BYOD users) where they are allowed only to a limited set of URLs thus still complying to the Enterprise policies.

Conclusion

With Cisco's Wireless solution coupled with the ISR-AX routers, IT administrators can improve experiences for users located anywhere, on any device securely to maximize employee productivity. Enterprises can now fully adopt the growing BYOD trend with confidence that the network can support the needed performance and scalability.

For More Information

For more information, read about the Cisco Wireless FlexConnect, Cisco ISR-AX, Cisco WAAS, or Cisco AVC, or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.

Printed in USA C11-726798-00 03/13