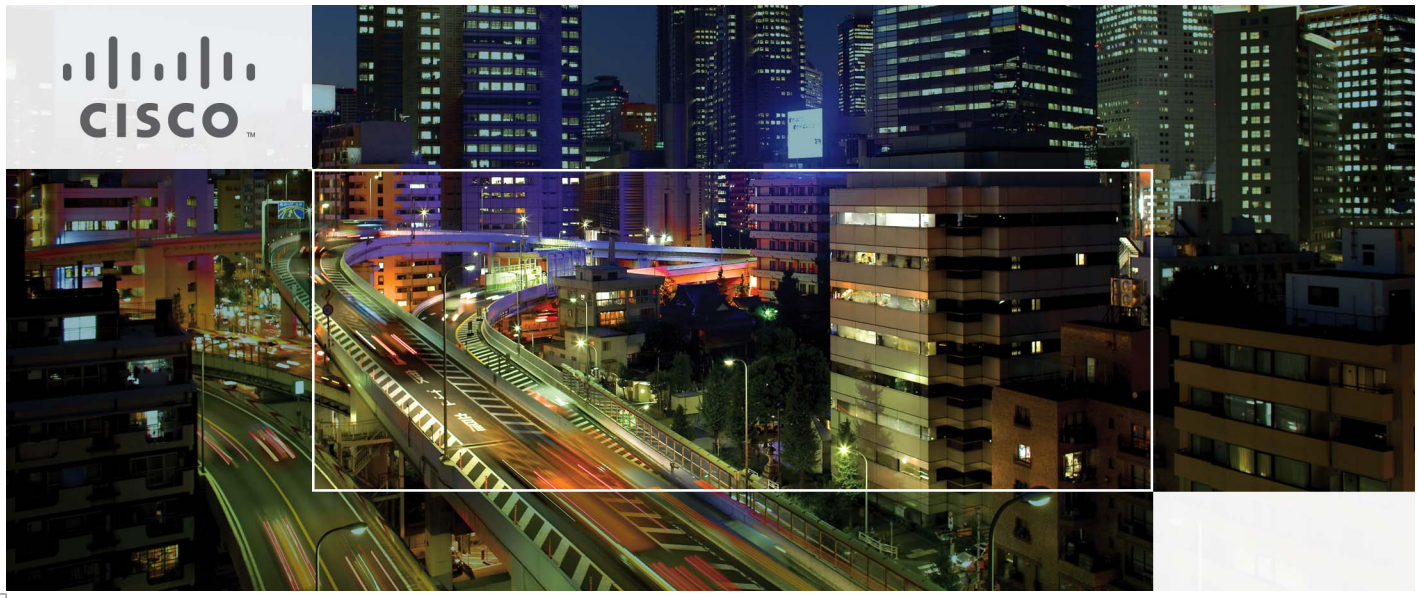


Application Visibility: Delivering BYOD at the Branch Using the Cisco Application Experience (Cisco ISR-AX)

Last Updated: June 16, 2013

Cisco Validated Design

Building Architectures to Solve Business Problems

About the Authors


Bill Reilly

Bill Reilly, Technical Marketing Engineer, SRG Marketing, Cisco Systems

Bill is currently a Technical Marketing Engineer in the Cisco Services Routing Group (SRG). His primary focus is on application acceleration and integrated solutions within the service router portfolio. When Bill joined Cisco in 2005, he worked as both a Technical Marketing Engineer and a Product Manager in Cisco Emerging Technology Group and Service Routing Group. In these groups, Bill focused on solutions with customers to leverage new technologies to enhance customer and employee communications. Bill has over 16 years of enterprise networking experience.


Vivek Achar

Vivek Achar, Technical Marketing Engineer, SRG Marketing, Cisco Systems

Vivek Achar is a Technical Marketing Engineer in the Services Routing Group (SRG) based in the US. He has worked in Technical marketing and Engineering positions while at Cisco. Vivek has been with Cisco for over 12 years and has a broad range of expertise with Cisco IOS routing, deep packet inspection, and broadband technologies. Before Vivek joined Cisco, he worked on deploying Motorola Networking products. Vivek has a Bachelor's degree in Computer Engineering from North Maharashtra University, India.

NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

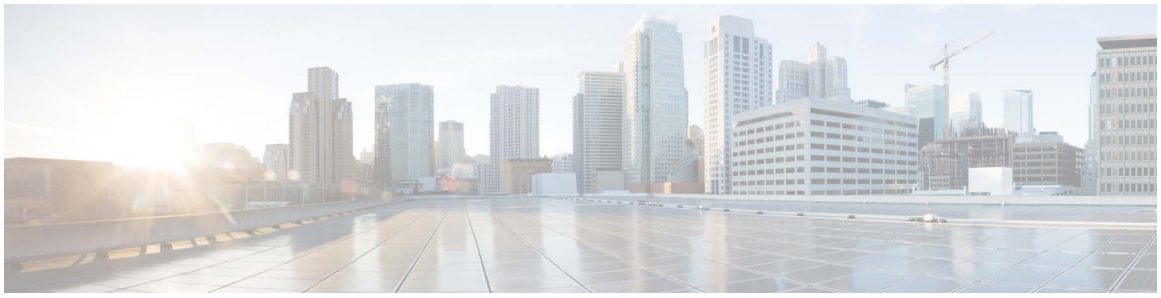
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR NABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

Application Visibility: Delivering BYOD at the Branch Using the Cisco Application Experience (Cisco ISR-AX)

© 2013 Cisco Systems, Inc. All rights reserved.



Application Visibility: Delivering BYOD at the Branch Using the Cisco Application Experience (Cisco ISR-AX)

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2013 Cisco Systems, Inc. All rights reserv

Introduction

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 be able to confidently say that 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 to improve productivity and mobility are countered by the worry that these devices may not be secure and that workers may be distracted by applications rather than using the device for work activities. Above all, supporting and troubleshooting these unmanaged devices and the effect that 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 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. The focus increases on the identity of devices and users accessing the enterprise data from these unmanaged devices. These devices 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. 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. 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. Enterprises want uniformity on how they allow users to bring their own devices.

The number of devices that will access the network is estimated to increase two to three times. IT administrators have a difficult time scaling their systems and network resources. One major constraint would be the WAN bandwidth itself; which must be provisioned to handle traffic for these new devices. Other BYOD adoption challenges relate to network access itself, identity of these devices, and user policy enforcement based on the internal requirements.

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
Wired Access	Cisco TrustSec® architecture allows a secure network where each device is identified by the user/group/role. Each device is provided secure access on the network based on the privileges.	Identity-based secured access

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

Table 1 Branch BYOD Components

WAAS	Cisco WAAS provides an elastic “scale as you grow” enterprise-wide deployment model. WAAS is a software- and hardware-integrated, cloud-ready WAN optimization and application acceleration solution. WAAS appliances offer outstanding deployment scalability and design flexibility, and 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) with control mechanisms like quality of service (QoS) and Cisco Performance Routing (Cisco PfR).	Proactive monitoring of application visibility
Security	Cisco Cloud Web Security enforces a consistent security policy for all web traffic that is generated from an enterprise branch.	Zero-day spyware and malware protection
Identity and Survivability	Cisco Identity Services Engine can act as the identity and policy engine with the Cisco Unified Computing System (Cisco UCS) E-Series module to provide capability to host virtualized applications on the Branch ISR G2 router	User identity and policy control

IT administrators may not be able to control the devices themselves, but 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 BYOD devices are not replacing the existing systems, they are net additions to the infrastructure. Each device has its own profile and all devices 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 challenged when enforcing network policies defined to maintain a consistent end-user experince 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 within the Cisco Integrated Services Router Application Experience (ISR-AX) portfolio provide the IT administrator with the two major components to address 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 provide these benefits:

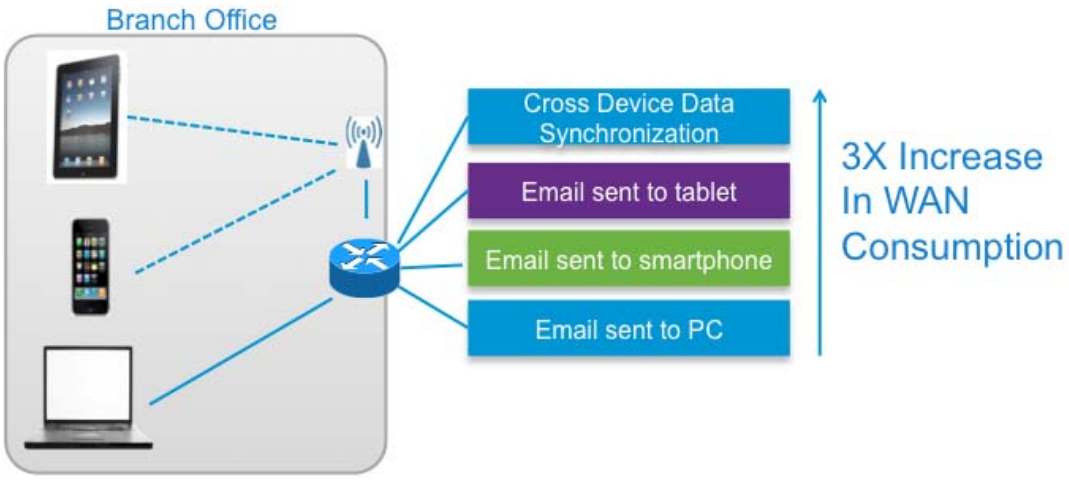
- Enable business applications to run faster.
- Reduce bandwidth costs and latency by more than 50 percent
- Simplify IT with probeless visibility across the network.

These benefits lower the barriers for deploying and consuming applications across cloud and BYOD environments.

The first component of Cisco ISR-AX for BYOD is application visibility. To apply any network policies, you must be able to differentiate BitTorrent traffic from your enterprise portal traffic. The second component 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 skim

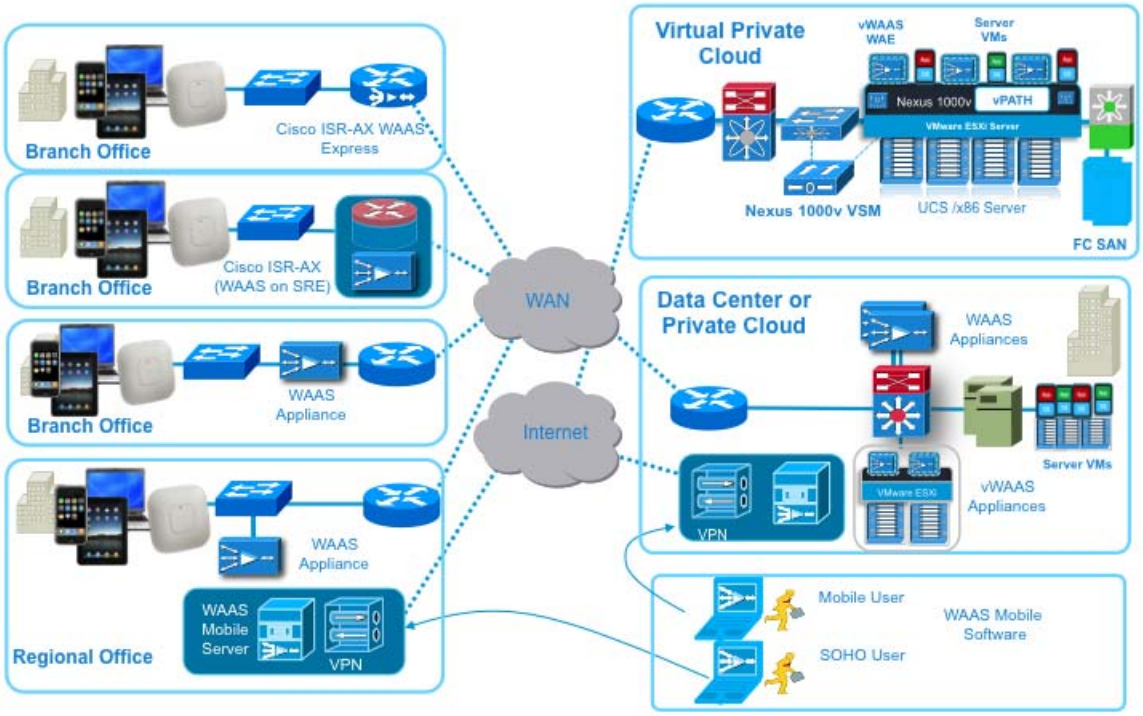
through a few email messages. Finally, in the meeting, she looks down at her iPhone to read the emergency email that she just received. This new connected-employee phenomenon is happening every day, and Molly has not one but three devices that all access her email at the same time. As shown in Figure 1, Molly's bandwidth consumption jumped threefold. When you add this extra traffic to the web and VDI traffic that all of 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 1,000 applications to apply and enforce network policies. Cisco WAAS provides the WAN optimization to control WAN bandwidth and provide application acceleration.

Figure 1 BYOD Bandwidth Consumption



IT administrators can use the reference architecture shown in Figure 2 as a base template in the branch-office BYOD planning for their organization. This solution is based on the three primary components of the Cisco portfolio: Cisco Wireless Access Points, Cisco WAAS, and Cisco AVC solution. For more details about each of these components, go to: www.cisco.com/web/solutions/trends/byod_smart_solution/index.html.

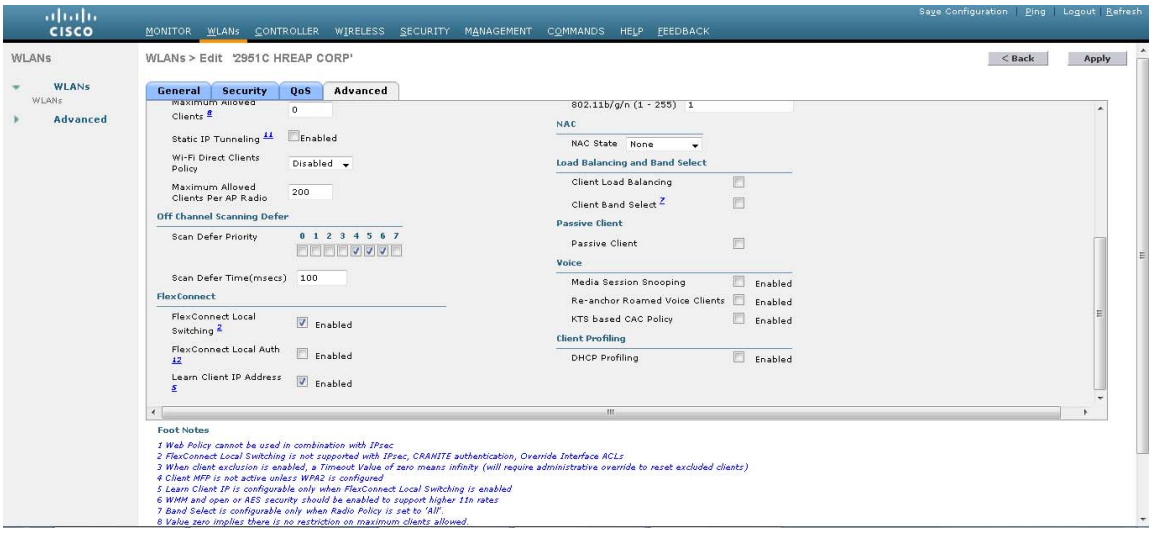
Figure 2 Branch Office BYOD Planning Architecture



Wireless: Cisco Access Points and FlexConnect

The first requirement in supporting wireless BYOD devices is the ability to separate the two planes of the CAPWAP traffic. CAPWAP has 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 administrators must address this CAPWAP tunnel. While the data is in this tunnel, application policies such as 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) and perform client authentication locally when their connection to the controller is lost. Some of the control functionality, such as configuring and controlling the access point, would still reside at the central wireless LAN controller. Full FlexConnect details and deployment are beyond the scope of this document, but you can find more information here:
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bcb905.shtml.

Figure 3 Cisco FlexConnect to Enable Local Switching



One of the other options for a relatively large or medium-sized branch would be to have the wireless LAN controller functionality locally at the branch via the Cisco UCS E-series module deployed on the Cisco Integrated Services Router Generation 2 (ISR G2). The UCS E-series module provides virtualization-ready hardware with support for the VMware vSphere Hypervisor. One of the applications that is hosted could be the Cisco virtual Wireless LAN Controller (vWLC). This functionality allows the Cisco Unified Wireless Network functionality to reside locally at the branch itself, and the Cisco WLC manages the access points locally with no wireless traffic traversing the WAN network.

The growth in the number of devices at the branch also places pressure on the wireless network and the way these devices are supported. The Cisco Access Point or the Integrated AP on the Cisco ISR G2 allows certain features like Cisco BandSelect, which allows the use of the channels and bandwidth that is available on the 5 GHz Wi-Fi band. Cisco BandSelect enables client radios that are capable of supporting dual-band (2.4 GHz and 5 GHz) operation to move to a less congested 5 GHz band. Band selection works by regulating probe responses to clients. 5 GHz channels are made to be more attractive to clients by delaying probe responses to clients on 2.4 GHz channels. This feature directs a client that is capable of using both Wi-Fi bands to associate to the access point on the 5 GHz band. When the access point can associate to the 5 GHz band, more bandwidth is available for the access point and the co-channel interference for nearby access points is reduced.

Other devices, such as wireless security cameras, motion detectors, microwave ovens, radars, or Bluetooth devices, could interfere with the 2.4 GHz or 5 GHz spectrum and impact wireless throughput. Cisco Access Points support the CleanAir technology, which enables the wireless network to self-heal and self-optimize. CleanAir has the unique ability to detect RF interference that other systems cannot see. CleanAir identifies the source, locates the source on a map, and then makes automatic adjustments to optimize wireless coverage. CleanAir gives you access to real-time and historic information about devices and assets located anywhere in the wireless network. If an interference source is strong enough to completely jam a Wi-Fi channel, the system changes channels within seconds to avoid the interference, and client activity is resumed on another channel outside of the affected area. The system remembers intermittent interference from persistent sources such as a microwave ovens, wireless bridges, or wireless video cameras. Through tight integration with Cisco radio resource management technology, the CleanAir solution indicates the channels where these devices operate so that system administrators can optimize performance and minimize future disruption.

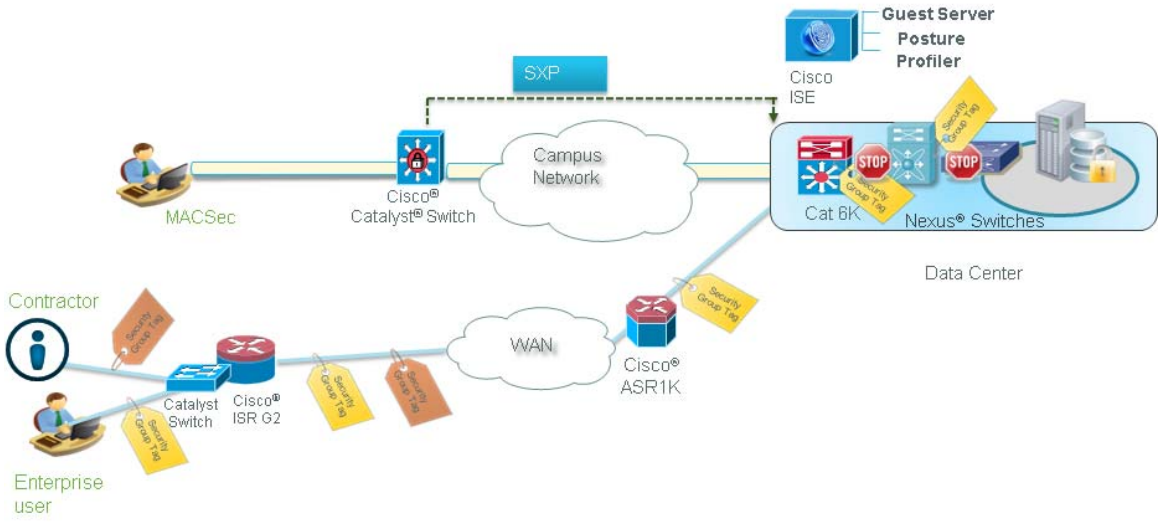
Major characteristics for WLAN communication are seen for traffic for web browsing, email, and file downloads which occur in the downlink direction. Improving the downlink throughput of the slowest clients improves the experience not only for the clients, but also for all other clients on the network. The result is a more reliable roaming experience and increased capacity of the network. Cisco ClientLink technology offers uplink improvements as well as downlink communication from access point to client. In addition, advanced signal processing into the Wi-Fi chipset is provided. Multiple transmit antennas are used to focus transmissions in the direction of the 802.11a/g client. These focused transmissions increase the downlink signal-to-noise ratio and the data rate over range, which reduces coverage holes and enhances the overall system performance. This technology essentially learns the optimum way to combine the signal received from a client, and then uses that information to send packets in an optimum way back to the client. This technique is also referred to as multiple-input multiple-output (MIMO), beamforming, transmit beamforming, or cophasing.

Identity and Security: TrustSec

Enterprise policies must be enforced based on the user, device, and role. With BYOD, the system must provide strong network access control and a classification mechanism that uses user or device identity and associated contexts. In the Cisco TrustSec architecture, after the user gets authenticated, the traffic for that user and from that particular device is encrypted and is allowed a level of access on the network, based on the user privileges. This ability allows enterprise IT administrators to define policies for users based on their roles, irrespective of them using a corporate-owned or personal device. These users can then again be classified as wired and wireless users coming over different media.

For example, Figure 4 shows a user from the Finance department and a contractor who are connected to the same access network. The Finance database has sensitive information, so the need is to allow access to only the users from the Finance department. In a switched environment, after a user connects a device onto the switchports, authentication might happen via 802.1x, MAC Authentication Bypass (MAB), or web authentication. The Cisco Identity Service Engine (ISE) or other RADIUS-based policy server is used to authenticate and provide various authorization parameters such as VLAN, downloadable ACL, and security group tag (SGT). After the user and device combination is authenticated, then all traffic from this device is tagged with a SGT. Cisco TrustSec tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT throughout the network within the Cisco TrustSec header. The SGT is a single label that determines the privileges of the source within the enterprise. Therefore, the users from the Finance department have access to the sensitive financial data because the traffic generated from these devices is SGT tagged.

Figure 4 Identity and Security with TrustSec



Cisco Catalyst Switches allows the SGT at a branch. The tagging of the packets itself requires hardware (ASIC) support, which might not be available on some devices on the network. The devices might still participate in TrustSec authentication via SGT Exchange Protocol (SXP), which allows devices to pass on IP address-to-SGT mappings to Cisco TrustSec-capable hardware. SXP is based on TCP with MD5 authentication and is supported over single or multiple hops. SXP essentially accelerates initial deployment of SGT/SGACL without hardware upgrade.

The Cisco ISR G2 or the Cisco ASR 1000 Series Aggregation Services Router (ASR) enforces traffic based on SGTs with Zone-Based Firewall. This method is otherwise called Security Group Firewall (SG-FW), which performs classification and enforcement based on security group tags. SG-FW allows enterprises to statefully enforce policies for corporate-owned or personal devices and avail some of the rich logging capabilities for auditing and compliance. In Figure 4, the SG-FW could be used to define a policy to not allow access for contractor employees to the Finance databases.

With more devices being added, administrators are worried about man-in-the-middle attacks, snooping, and other forms of attacks. 802.1ae or MACsec is designed to provide secure communication on wired LANs. When MACsec is used to secure the communication between endpoints on a LAN, each packet on the wire is encrypted using symmetric key cryptography so that communication cannot be monitored or altered on the wire. As corporate or personal devices access sensitive data, 802.1ae provides secure 128-bit AES wire-speed encryption.

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, 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 to delay or eliminate increased recurring bandwidth costs: Cisco WAAS enables IT consolidation, which reduces 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 and Cisco WAAS on Cisco Services-Ready Engine (SRE) modules.
- 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[1] 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 may be 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. You can also deploy Cisco WAAS network modules and 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.

These routers use Cisco industry-leading QoS to reprioritize critical applications or enforce application bandwidth use to improve application performance. With 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.

1. 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, which further reduces backup windows and enhances restore operations. Multiple use cases exist because WAN optimization and Cisco WAAS pertain to backup optimization, and appropriate messaging must be delivered depending on the target audience and the architecture.

- 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.

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 1,000 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 and Prime Assurance Manager (PAM), which provide enterprise-grade infrastructure and service monitoring to report application and network performance
- Modular QoS to facilitate optimization and control of application performance

Figure 5 shows how the Cisco Flow Agent (FA) within WAAS shares flow information into the Cisco Prime enterprise and service provider management portfolio.

Figure 5 Cisco Flow Agent and Performance Agent

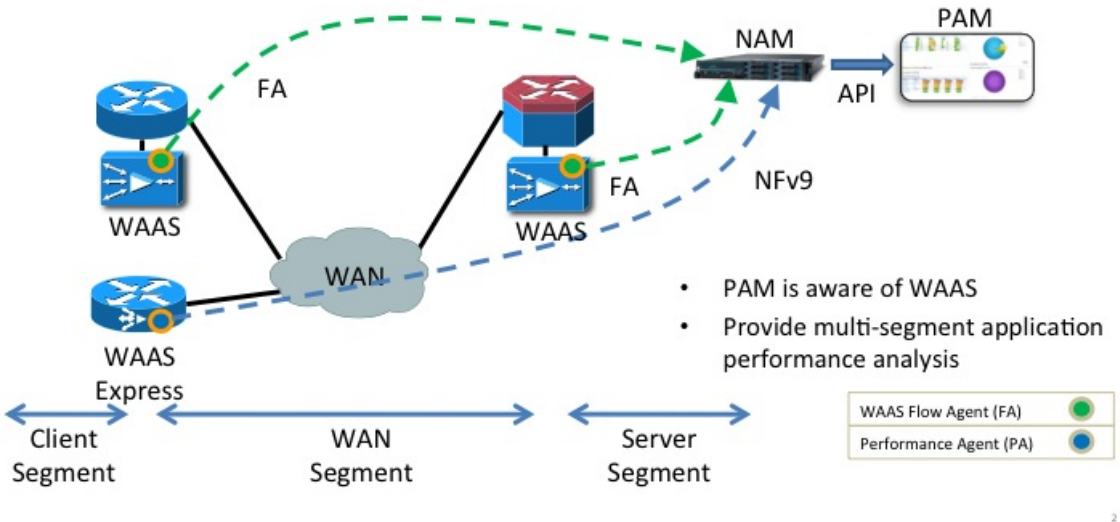


Table 2 describes the components of Cisco AVC.

Table 2 Single Tier Profile Components

Components	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 they can export to the Cisco Prime application. Flow Agent (FA) reports response-time metrics from Cisco WAAS devices.	Flexible NetFlow, NetFlow, 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.	Cisco PfR and QoS

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

With the solution outlined in this document, IT administrators can address the BYOD challenge. When IT administrators address the three pillars of AVC plus WAN optimization in a totally wireless deployment model, they 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 to increase the client density in the branch office while 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 pushing special applications onto the personal devices or restricting a BYOD policy to only certain types of devices.

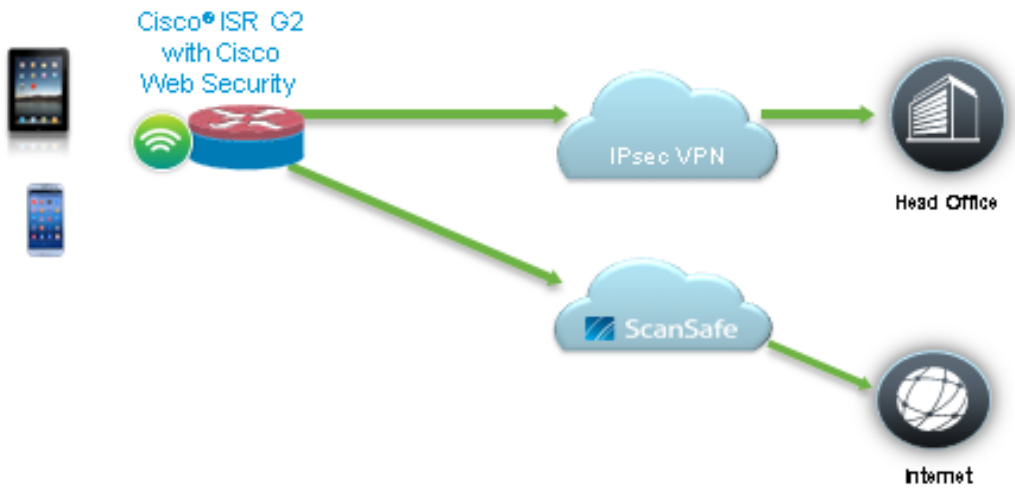
Secure Policy Enforcement

Enterprises apply certain policies to the web traffic on their campus networks that they want to emulate on the branches as well. Application of policies must be consistent across their network, and Cisco Cloud Web Security (CWS, formerly ScanSafe) allows enterprises to ease in administration to have the similar policies for the web traffic that emanates from all branch networks.

Typically enterprise branches have all their traffic encrypted over the public/private network. As shown in Figure 6, the traffic is sent to the enterprise headend and web traffic is split tunneled onto the Internet. The The Cisco CWS connector on the Cisco ISR G2 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 provides granular reporting. The CWS or ScanSafe connector allows enterprises to ensure security for their web traffic and not have all web traffic backhauled to their enterprise headend, which frees up the WAN bandwidth for other crucial enterprise applications like mail and SAP applications.

Figure 6 Cisco Web Security Connector on the Cisco ISR G2



Also, the Cisco CWS solution on the Cisco 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 such as Active Directory and Web Auth, 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. For example, the cloud could be configured to not allow guest users to access entertainment, sports, and social networking websites, whereas enterprise users would still have access to some of these sites.

In summary, Cisco CWS allows enterprise branches to configure policies for the branch. More specifically, Cisco CWS allows policies to be configured for the web traffic for a group of users (for example, the guest users) where the policies allow traffic only to a limited set of URLs, thus still complying to the corporate IT policies.

Manageability and Branch Survivability

The Cisco Identity Service Engine (ISE) provides a centralized identity, access control, policy creation, distribution, and management across the enterprise network. The Cisco ISE combines the features and benefits of Cisco Secure ACS, Cisco NAC Manager, Cisco NAC Server, Cisco NAC Profiler, and Cisco NAC Guest Server with unified policy management and comprehensive monitoring and troubleshooting. Cisco ISE provides a self-service portal that allows employees to install corporate certificates on personal devices. Cisco ISE also provides a centralized location for activities such as creating policies, monitoring endpoints, and generating reports. TrustSec with the Cisco ISE allows enterprises to have a separation of duties.

The enterprise IT infrastructure team can configure a few simple commands make network resources query the Cisco ISE for security policies. This ability allows the security team to change policies without involving the infrastructure team. Cisco ISE is a powerful tool for the BYOD deployments, which means that it must be available when there is a WAN link outage. The Cisco ISR G2 has the unique capability to host the enterprise class UCS E-series service modules. These modules enable enterprises to host some of the critical applications like ISE, DHCP, and DNS servers for high availability for the branch users.

Cisco Prime Network Control System (NCS) delivers visibility and diagnosis of access infrastructure devices, including Cisco access switches, Cisco Wireless LAN Controllers, and Cisco Aironet access points. With this system, you can centrally manage the Cisco Mobility Services Engine (MSE) with support for the Cisco Adaptive Wireless Intrusion Prevention System (wIPS), Cisco Context-Aware Software, and Cisco CleanAir technology. Cisco Prime NCS allows for a consistent wired and wireless endpoint experience. NCS allows for a centralized location to create wired and wireless infrastructure policies and for generating reports and troubleshooting.

Conclusion

When the Cisco wireless solution is coupled with the Cisco 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

Read more about Cisco Wireless FlexConnect, Cisco ISR-AX, Cisco WAAS, Cisco AVC, or contact your local account representative.