Miercom

Lab Testing Summary Report

December 2006
Report 061202

Product Category:

Branch Router

Vendor Tested:

Cisco Systems

Products Tested:

Cisco 3845 Integrated Services Router

Miercom PERFORMANCE VERIFIED™

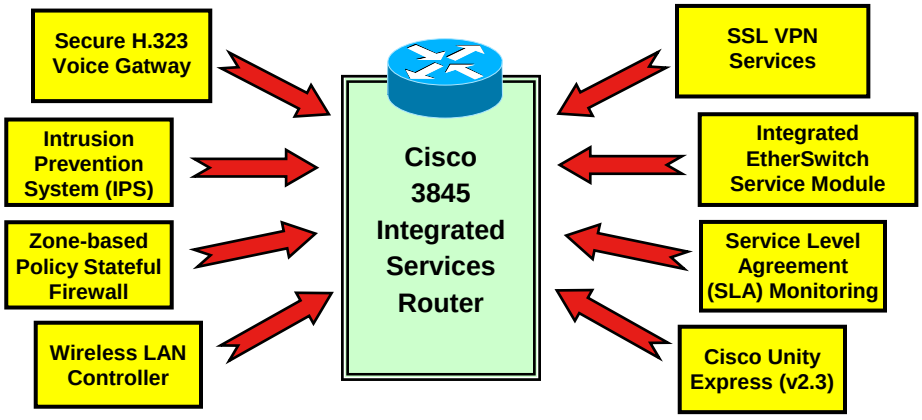
Key findings and conclusions:

- **The Cisco 3845 router can sustain more than 50 Mbps WAN link traffic running concurrent voice, video, data and wireless services with additional processor capacity to spare**
- **More than 95 Mbps of traffic load (near line rate) could be routed between 2 ports on the EtherSwitch Module with no impact on the router's processor utilization**
- **The Wireless LAN Controller module provides a complete and easily deployed Wireless LAN Management System in the branch office**
- **The Cisco 3845 supports comprehensive security capabilities including Zone-based firewalls, IPS, IPsec, and SSL VPNs**
- **SCCP calls (w/SRTP) were tested with Secure Voice Gateway. Cisco SRST (w/TLS) was also tested. H.323 signaling was encrypted with IPsec 3DES**
- **The Cisco Unity Express (v2.3) module provides enhanced voicemail functions from any location**
- **Traffic and performance statistics can be monitored with NetFlow and IP SLA between the branch, HQ, and Internet**

Cisco Systems engaged Miercom to independently verify the configuration, operational and performance aspects of the modular Cisco 3845 Integrated Services Router.

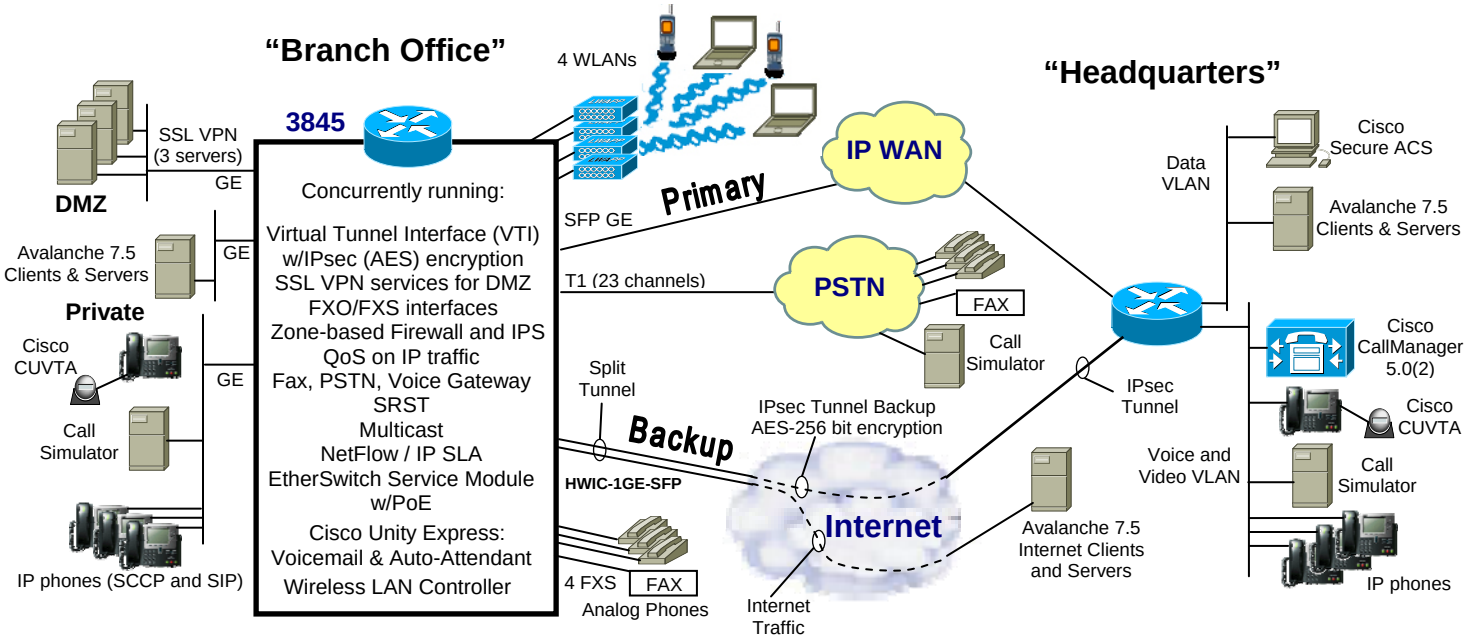
This system, representing an evolution of Cisco's ISR product line, is a single router designed to deliver multiple services to support a branch office with voice, video and data access in a secure environment. The key features we examined included a full-function Integrated EtherSwitch Service Module, the Wireless LAN Controller module, SSL VPN functions providing secure access to branch resources, enhanced secure voice gateway functions, new voicemail functions with Cisco Unity Express (v2.3), and NetFlow/IP SLA/NAM functions for monitoring the performance of the branch network.

The Cisco 3845 router ran Cisco IOS™ Software version 12.4(9)T1 in the test bed. In our performance tests, Miercom verified that, while running a rich set of additional services (see table on page 3), the Cisco 3845 could sustain a high level of bi-directional traffic to the Headquarters site.



Cisco 3845 Integrated Service Router (ISR) provides Secure Converged Access with high performance for voice, video and data, with enhanced security functionality, a wide variety of interface modules, and many other services for the branch office environment.

3845 Test-bed Setup



Data, Voice, Video and Telephony services between the Branch and HQ sites. We tested the Cisco 3845 Integrated Services Router configured with a Gigabit Ethernet link as Primary link to the HQ site (using an onboard SFP GE port), and a backup connection over a GE IPsec/VTI tunnel (using a GE SFP HWIC module and an AIM-VPN/SSL-3 encryption module for AES 256-bit encryption). Telephony services were provided by a Cisco CallManager 5.0(2) at the HQ location (with SRST at the branch for failover), and a Cisco Unity Express Network Module for local voice mail. Local analog and fax connections were handled by an 4-port FXS HWIC module, and PSTN connectivity via a T1 HWIC module. We used one of the Gigabit Ethernet ports on the 3845 motherboard to connect to the DMZ at the branch. A 48 port Integrated EtherSwitch Service Module supported connectivity for local PCs, IP phones and an (SFP) Gigabit Ethernet port for server connectivity. The Cisco 3845 was configured with 4 wireless LANs (AIR-AP1020-A-K9) with the Wireless LAN Controller network module. The Network Analysis Module (NAM) was installed in the HQ router to analyze NetFlow data.

Performance Testing. The branch was setup with voice traffic consisting of a full T1 of traffic (with a FAX) from the PSTN, and over 4 Mbps of real and simulated VoIP calls between the branch and HQ (G.711), most of which were secure (SRTP). We also setup 3 simulated video calls and one real call using Cisco Unified Video Advantage. Application traffic consisted of 40 FTP and 300 HTTP bi-directional user connections between the branch and the HQ. Also, we setup 5 FTP users and 10 HTTP user connections from the branch to the Internet and 10 HTTPS connections (using the Cisco 3845's SSL VPN services) from the Internet to three DMZ servers at the branch. The Zoned-based Policy Firewall services isolated the "Private", "DMZ" and "Internet" networks at the branch.

During the performance tests, a variety of telephony services were exercised including conference calling (with an assortment of IP and PSTN phones, SIP and SCCP, and wireless phones; Cisco 7920s), call forwarding and transfer, FAX transmission between the PSTN and the branch, and leaving and retrieving voicemail.

Failover. During the failover of the primary link, the traffic was re-routed to the IPsec Tunnel through the Internet. We did not have any phone or video calls drop during the failover test.

Modularity and Concurrency

The Cisco 3845 ISR (Integrated Services Router) runs Cisco's IOS™ Software, and offers numerous slots for a variety of module plug-ins. These let the customer selectively add features and functions, as well as tailor the configuration, and modify it to suit their network environment.

We tested an assortment of modules and Cisco IOS™ Software features. The router was configured with an EtherSwitch Service Module and VPN/SSL Hardware Encryption Module. Other modules and features we tested included Wireless LAN Controller, the Layer-2 Security functions handled by the EtherSwitch Service Module, Secured Voice Gateway functions, SSL VPN services, Cisco Unity Express (voicemail module), IP SLA and NetFlow traffic statistics, Cisco Router and Security and Device Manager (SDM) tool, and Survivable Remote Site Telephony (SRST).

Cisco IOS™ Software Warm Reload/Upgrade

Our tests verified that the reload times for the Cisco 3845 router was shortened using the Warm Reload option. This was a nearly 30% savings in time.

We also verified the Cisco IOS™ Software upgrade time was shortened by running tests that upgraded the Cisco 3845 router from release 12.4(9)T to 12.4(9)T1 using the Warm Upgrade option. This was also a nearly 30% savings in time.

Ports on the Integrated EtherSwitch Service Module were not affected by the Cisco IOS™ Software Warm Reload or Warm Upgrade. Voice calls between phones on separate VLANs as well as continuous pings between two VLANs remained connected.

Modules Installed in the 3845 (System Under Test)	
Module	**Description**
Integrated on motherboard	2 Gigabit Ethernet ports (1 Gig-E and 1 Gig-E/SFP port)
HWIC slot 0: VWIC2-2MFT-T1/E1	2-port T1/E1 Multiflex Trunk Voice/WAN Interface Card
HWIC slot 1:	available for other services
HWIC slot 2: VIC-4FXS/DID	Cisco VIC-4FXS/DID Analog Voice Interface Card
HWIC slot 3: HWIC-1GE-SFP	Cisco Gigabit Ethernet High-Speed WAN Interface Card
DSP slots 0-3: PVDM2-64	High-Density Packet Voice Digital Signal Processor Module
AIM slot 0: AIM-VPN/SSL-3	VPN Advanced Integration Module (AIM)
AIM slot 1:	available for other services
NM slots 1-2: NME-XD-48ES-2S-P	48 port Doublewide Cisco EtherSwitch Service Module
NM slot 3: NM-AIR-WLC6-K9	Cisco Wireless LAN Controller Module
NM slot 4: NM-CUE	Cisco Unity Express Voice Mail Network Module (20 GB IDE Disk Daughter Card)

Concurrent Services Running and Verified on the Cisco 3845 Integrated Services Router			
	Services / Features	**How 3845 supports**	**How Tested/Verified**
Data	Routing and QoS	Integrated in Cisco IOS™	OSPF routing; LLQ, CBWFQ, WRED
	EtherSwitch Service Module (48 and 24 port) with 802.3af PoE	NME-XD-48ES-2S-P NME-XD-24ES-2S-P	Voice call and "ping" tests during upgrades and reloads, and port performance test
	Cisco IOS™ Warm Reload/Upgrade	Integrated in Cisco IOS™	Tested Warm Start with/without feature
	Wireless LAN Controller	NM-AIR-WLC6-K9	Observed management, verified with wireless handsets and laptops
Security	L2 Security: DHCP Snooping, 802.1x authentication, IP Source Guard, etc.	NME-XD-48ES-2S-P (Cisco IOS™ Software on the Switch Module)	Attempted to connect unauthorized PCs to ports, verified they would not connect
	IPsec Tunnel, with Virtual Tunnel Interface (VTI) and AES-256 encryption	Integrated in Cisco IOS™ Software and AIM-VPN/SSL-3	Via multiple test systems, link monitors, CLI, 3845 failed primary link to VTI backup
	Zone-based Policy Firewall	Integrated in Cisco IOS™ Software	On GE WAN link; viewed sessions via CLI, reconfigured to block certain traffic
	Inline IPS (Intrusion Prevention)	Integrated in Cisco IOS™	On Split Tunnel IP link to Internet, CLI
	SSL VPNs (clientless connections)	IOS and AIM-VPN/SSL-3	Logged in manually in clientless mode
Voice	Voicemail (stored locally on NM-CUE)	Part of NM-CUE module	Voicemail sent, retrieved under load
	Auto-Attendant	Part of NM-CUE module	Manually checked under load
	Conference Calling	Integrated in Cisco IOS™	Manually checked under load
	Survivable Remote Site Telephony (SRST) for 3845	Integrated in Cisco IOS™ Software	Failed WAN link to remote CallManager; calls placed locally and via PSTN
	Fax, PSTN, Voice gateway	Fax (VIC-4FXS/DID), PSTN (VWIC2-2MFT-T1/E1)	Fax and PSTN voice calls placed
	RSVP Agent with Application ID	Integrated in Cisco IOS™	Manually changed reservation bandwidths
Manage-ment	IP SLA, NetFlow	Integrated in Cisco IOS™ Software, NM-NAM	Network Analysis Module Mgmt. Interface
	Traffic Statistics, Load Monitoring	Integrated in Cisco IOS™	Output viewed via CLI during testing
	Cisco Router and Security and Device Manager (SDM) tool	SDM Configuration cmds	Demonstrated tool functions on the 3845

Integrated EtherSwitch Service Module

Cisco's Integrated EtherSwitch Service Module was derived from Cisco's powerful Catalyst® 3750 switch. The same software now runs on the ISR Integrated EtherSwitch Service Module.

The Cisco EtherSwitch Service Module can run independently from the Cisco IOS™ Software in the main router. Voice calls and data connections routed through the switch module can stay up through the switch even while the Cisco IOS™ Software in the router is being reloaded (see the Cisco IOS™ Software Warm Reload/Upgrade description above.).

Our test bed had a total of 32 powered devices connected – which drew over 340 watts from the system (the system can support 360 watts). An assortment of powered devices including Cisco 7971, 7970, 7961, and 7060 IP phones as well as an IP-powered Sony video camera were used during this test to verify both Cisco pre-standard PoE and IEEE (802.3af) standard PoE being supported.

The CLI showed the total power consumption, and indicated which ports connected devices with IEEE standard (802.3af) PoE and which devices used the Cisco pre-standard PoE.

We ran an inter-VLAN performance test on the integrated Cisco EtherSwitch Service Module under heavily loaded conditions of the switch. The inter-VLAN routing was performed by the Integrated EtherSwitch Service module. A high level of real-world traffic (FTP and HTTP) was delivered on the Cisco 3845 ISR between 2 switch ports (routing across 2 VLANs). We were able to drive the traffic to over 95 Mbps with no impact on the router's CPU utilization.

The Integrated EtherSwitch Service Module also performs a number of L2 security checks to provide increased network security. The Cisco EtherSwitch Service Module supports 802.1x authentication, and we were able to configure PCs to authenticate with the switch using 802.1x, EAP-PEAP, and MSChapV2. The Cisco EtherSwitch Service Module performs Dynamic ARP Inspection to guard against malicious MAC address flooding. Port Security also restricted invalid MAC addresses. We tested and verified the DHCP Snooping and IP Source Guard security checks by connecting unauthorized PCs – the switch recognized the illegal connection and denied the PC network access.

We were able to exploit the integration within the ISRs with our testing of Cisco EtherSwitch Service Module. For the configuration, we used different 802.1q sub-interfaces corresponding to some of the VLANs on the switch. Then, using Zone-based policies, we setup a firewall between the VLANs representing the "Private" zone and "DMZ" zone in our test bed and the Zone-based policies could be directly configured to the VLANs in the Cisco EtherSwitch Service Module.

In another 3845 router we installed a NME-XD-24ES-2S-P EtherSwitch Service Module which is designed to participate in Cisco Catalyst® 3750 StackWise Connections. We connected an external Cisco Catalyst® 3750 switch with primary and redundant cables. In our test we verified traffic continued to be routed from the router's EtherSwitch Service Module to the external Cisco Catalyst® 3750 switch even with a failover of one of the StackWise cables. And, as expected,with a stacked switch, we could configure the external Cisco Catalyst® 3750 switch within the same command line environment together with the router's EtherSwitch Service Module.

Wireless LAN Controller

We tested the Cisco Wireless LAN Controller Module (WLCM) installed in the Cisco 3845. It is a full featured Wireless LAN Controller with support for advanced security, mobility, zero-touch deployment and management of lightweight access points.

The WLCM was tested using 802.1x (LEAP), PEAP, and WEP authentication protocols using several laptops. Cisco says it also supports TTLS, WPA, and 802.11i (WPA2). Additionally, we provisioned a guest network from the branch to the headquarters network. Guest users could gain wireless access at the branch but have their traffic directed to the headquarters site for Internet access policy control. With our guest laptop, we verified the guest traffic was isolated from local private networks, and permitted to the Internet according to the HQ guest policy.

Mobility was demonstrated with Voice over Wireless LAN (VoWLAN). Two AP were configured on different VLANs. A call was placed using a Cisco 7920 wireless handset. The AP the call was associated with was disconnected and the call switched over to the second AP and remained active with hardly any perceptible loss.

We also examined Cisco's Wireless Control System (WCS), a wireless planning, configuration and management tool which runs on a separate server. It allows for a visualization of AP and client locations. Rouge AP units are also depicted and can be mitigated.

We used the WCS to verify the zero-touch deployment with access points which were reset to the factory default configuration and then connected to the EherSwitch module on the 3845. The APs were auto-discovered by the controller and provisioned. We verified the setup by placing a voice call successfully with a Cisco 7920 wireless handset.

Multicast

We tested the Multicast support with a multicast stream sent from the HQ site to the branch. Our configuration used IGMP Snooping on the Cisco EtherSwitch Service Module. We had a multicast server and client in our test bed configuration and verified that while using PIM-SM, multicast streams were properly dispersed. We also examined the Multicast statistics on the router and that the stream was only going to the subscriber port.

Management Instrumentation – Netflow/Network Analysis Modules/IP SLA

During our testing we setup a Management Instrumentation environment using Cisco's NetFlow, IP SLA, and a Network Analysis Module (NAM). This collection of tools allows for troubleshooting and analysis of traffic on the network from any location.

We tested the Management Instrumentation by connecting to a Network Analysis Management (NAM) card in the Headquarters router from a PC in the branch. We could monitor the IP load and performance for the Cisco 3845 in our test bed (representing the branch) via NetFlow. Traffic between the headquarters and branch was captured and analyzed using the web interface. Specific applications such as VoIP were monitored for jitter and latency using the IP SLA monitoring feature. Monitoring was continued under the full performance load detailing the numerous conversation and traffic flows present both from in real-time and using historical data. From the same web interface, we setup reports and generated PDF documents for the traffic flows observed.

SSL VPN

We configured the Cisco 3845 router with the SSL VPN feature – using the clientless SSL VPN connection feature. The Cisco 3845 ISR was configured to terminate remote access SSL VPN sessions on the AIM-VPN/SSL -3 module.

We had a typical user on the Internet use their browser, with only an SSL connection to obtain a VPN connection to servers at the branch. After our test user logged in, a menu was presented with a web portal allowing a connection to any of 3 servers at the branch's intranet site, creating a VPN environment for that user. During our performance tests, we simulated 10 users, for a total of about 5 Mbps being processed by the SSL VPN facilities.

Zone-based Firewall

We tested Cisco's new firewall facilities: "Zone-based Policy Firewall". We configured 3 zones: "Internet", "Private" and "DMZ". This feature simplifies firewall configuration because you only need to select the interfaces that you want to be placed in a specific firewall zone (traffic is inspected as it moves between zones). It was easy to setup our inter-zone policies for multiple host groups connected to the same router interface.

Network Address Translation (NAT) functions were also configured on the Cisco 3845 for all our Internet traffic. The backup link for the Cisco 3845 router was configured as split tunnel through our Internet connection. The branch-to-HQ traffic was configured with a Virtual Tunnel Interface (VTI) with IPsec (AES-256 bit) encryption – using the AIM-VPN/SSL -3 module (for improved IPsec and SSL VPN performance). The VTI makes the IPsec tunnel a native L3 interface and greatly simplified our configuration and design for QoS, VPN and security policy deployment.

Intrusion Prevention System

In our test bed, the Cisco 3845 ISR was configured with Cisco's IOS™ Software Intrusion Prevention System (IPS) using Cisco's signature set (256MB.sdf). We had 740 signatures active during our testing. The Cisco Router and Security Device Manager (SDM) was used to manage the IPS system. The SDM tool provided us with a display where we could examine the signature set and check or update IPS settings, for instance to control whether each signature is active or inactive.

Secure H.323 Voice Gateway

We tested Media encryption with SRTP (Secure Real-Time Protocol) for SCCP calls by using packet captures and a VoIP analysis tool. We captured the VoIP traffic for the call and verified the secured call could not be decoded, but decoded an unsecured call. We found that the RTCP (Real-Time Control Protocol) packets for the secured call could not be viewed. If we made a call from a phone supporting SRTP (secured) to a phone without SRTP support, an un-secured connection was automatically established (and the phone displayed an icon indicating it was an un-secured call).

Our systems were configured to encrypt H.323 signaling to the Cisco Unified CallManager, for the voice gateway, using an IPsec (3DES) tunnel.

If the CallManager was offline, we were still able to make secure calls using the SRST (Cisco's Survivable Remote Site Telephony in Cisco IOS™ Software) using TLS (Transport Layer Security) for signaling encryption.

Cisco Unity Express v2.3

The Cisco Unity Express module (v2.3) for the ISR family of routers contains a number of productivity enhancements. In our system under test. For the Cisco 3845 router, the Cisco Unity Express functions were contained on a Network Module (NM).

We tested Cisco's new Integrated Messaging feature which allow voicemail messages to be integrated with your regular email system. For our email system, we tested Integrated Messaging with Microsoft Outlook®.

Our testers used Cisco 7960 and Cisco 7970 IP phones to remotely access our messages using the Cisco VoiceView Express functions. We were also able to update our mailbox settings directly with the phone.

As we were testing voicemail, we left messages at different extensions and a few of these had Cisco's Remote Message Notification feature configured. For these extensions we verified that the notification feature alerted the remote phone that a message had arrived.

We were able to demonstrate the Future Message Delivery feature by leaving a message for a group of extensions to be delivered a few hours in the future.

We also configured one of our extensions for Mandatory Message Expiry. Then, for this extension, for any messages that were older than our expiration limit (we tested using a one day limit), the subscriber was notified that these messages were to be deleted.

For the auto attendant features, Cisco also provides an editor to ease configuration and deployment of scripts. Elements that can be used in the scripts are presented on the left with the main body of the script on the right. The script appears like a file tree and elements are dragged and dropped into the tree which executes from the top down. We placed the editor into a debug mode in which we could observe a step-by-step execution of the script while a call was being processed. This greatly enhances finding and eliminate bugs within scripts.

Call Admission Control using RSVP Agent

Call Admission Control feature using the RSVP agent was tested on the Cisco 3845 router. This feature allows the router to participate in "reserving" bandwidth for voice and video calls (real-time media). In our tests we configured the RSVP Agent using the Application ID facilities to separate the voice and video bandwidth requests. When the call is setup, typically by the CallManager, the RSVP agents along the path are contacted to assure the requested amount of bandwidth is available and reserves it for the call.

We setup RSVP with bandwidth on the primary IP link to be over 5 Mbps; and made voice (G.711) and video calls with no problems. Then, we reduced the bandwidth and tested a video call (with the "Mandatory, Video Desired" option), the video call would connect with only audio. We further reduced the bandwidth to 50 Kbps, and could only place audio calls with a G.729 codec.

Cisco Router and Security Device Manager

The Cisco Router and Security Device Manager (SDM) tool is a no cost application that guides users through deployment and implementation of security features and best practices. Using the same 3845 as above, SDM was used to setup an SSL VPN, IPsec VPN tunnel back to the headquarters and performed a general security audit on the platform. Upon completion, over 480 lines of CLI were added without disrupting the original configuration setup. The IPsec tunnel was then intentionally mis-configured to demonstrate the troubleshooting aspects of SDM which were able to step through the tunnel negotiation and provide detailed information regarding the error and possible troubleshooting steps to correct it. Adding new configurations or troubleshooting existing security features on a router can be a "daunting" task at best, SDM greatly simplifies that process.

Miercom Verified Performance

Based on Miercom's thorough workout of this system – and examination of its configuration, operation and features, as described herein – Miercom proudly attests to this system's performance, in particular:

- The Cisco 3845 router can sustain more than 50 Mbps WAN link traffic running concurrent voice, video, data and wireless services with additional processor capacity to spare
- More than 95 Mbps of traffic load (near line rate) could be routed between 2 ports on the EtherSwitch Service Module with no impact on the router's processor utilization
- The Wireless LAN Controller module provides a complete and easily deployed Wireless LAN Management System in the branch office
- The Cisco 3845 supports comprehensive security capabilities including Zone-based firewalls, IPS, IPsec, and SSL VPNs
- SCCP calls (w/SRTP) were tested with Secure Voice Gateway. Cisco SRST (w/TLS) was also tested. H.323 signaling was encrypted with IPsec 3DES
- The Cisco Unity Express (v2.3) module provides enhanced voicemail functions from any location
- Traffic and performance statistics can be monitored with Cisco's NetFlow and IP SLA facilities between the branch, HQ, and Internet

Cisco 3845 Integrated Services Router

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134 USA

www.cisco.com

Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

About Miercom's Product Testing Services…

With hundreds of its product-comparison analyses published over the years in such leading network trade periodicals as *Business Communications Review* and *Network World*, Miercom's reputation as the leading, independent product test center is unquestioned. Founded in 1988, the company has pioneered the comparative assessment of networking hardware and software, having developed methodologies for testing products from SAN switches to VoIP gateways and IP PBX's. Miercom's private test services include competitive product analyses, as well as individual product evaluations. Products submitted for review are typically evaluated under the "Net**WORKS** As Advertised™" program, in which networking-related products must endure a comprehensive, independent assessment of the products' usability and performance. Products that meet the appropriate criteria and performance levels receive the "Net**WORKS** As Advertised™" award and Miercom Labs' testimonial endorsement.

Miercom

379 Princeton-Hightstown Rd., Cranbury, N.J. 08512
609-490-0200 ● fax 609-490-0610 ● www.miercom.com

Report 061202