Miercom

Lab Testing Summary Report

December 2006
Report 061201

Product Category:
Branch Router

Vendor Tested:
Cisco Systems

Products Tested:
Cisco 2811 Integrated Services Router

and

Cisco 2851 Integrated Services Router

Miercom PERFORMANCE VERIFIED™

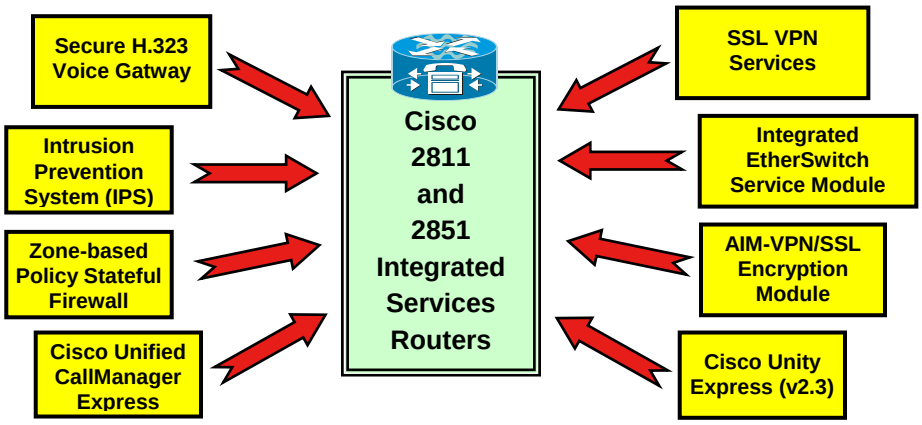
Key findings and conclusions:

- **The Cisco 2811 router can sustain more than 4 Mbps of WAN link traffic with concurrent voice, video, and data services with additional processor capacity to spare**
- **The Cisco 2851 router can sustain more than 20 Mbps WAN link traffic with concurrent voice, video, and data services with additional processor capacity to spare**
- **The EtherSwitch Service Module provides 802.3af PoE, integrated VLAN routing and advanced security features**
- **The Cisco 2811 and 2851 support comprehensive security capabilities including Zone-based firewalls, IPS, IPsec DMVPN and SSL VPNs**
- **SCCP calls (w/SRTP) were tested with Secure Voice Gateway. Cisco SRST (w/TLS) were also tested. H.323 signaling was encrypted with IPsec 3DES**
- **The Cisco Unified CallManager Express and Cisco Unity Express provide a complete branch telephony system**
- **The Cisco Unity Express (v2.3) module provides enhanced voicemail functions from any location**

Cisco Systems engaged Miercom to independently verify the configuration, operational and performance aspects of their modular 2811 and 2851 Integrated Services Routers.

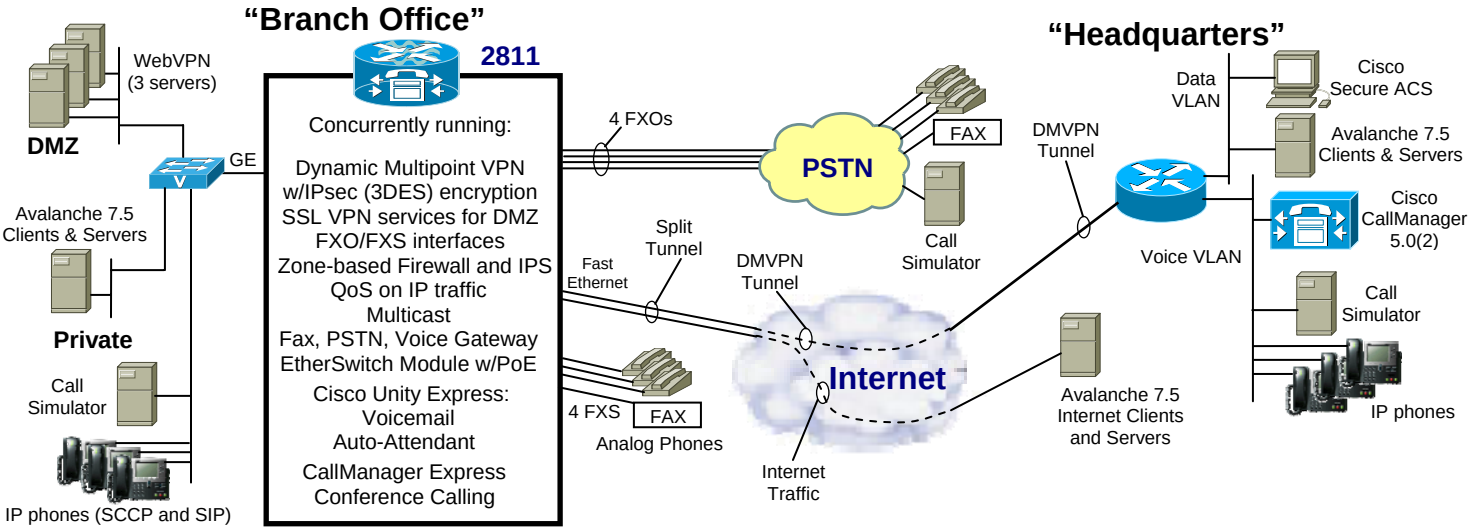
These systems are representative of an evolution of Cisco's ISR product line, designed so a single router can deliver multiple services to support a branch office with voice, video and data access in a secure environment. In our test bed we looked at FXO and FXS modules and a DSL module for a WAN link. In addition, we examined other modules and services including a full-function Integrated EtherSwitch Service Module, SSL VPN functions providing secure access to branch resources, enhanced secure voice gateway functions, and telephony support with Cisco Unified CallManager Express and Cisco Unity Express (v2.3).

The routers ran Cisco IOS™ Software version 12.4(9)T1 in the test bed. Miercom verified that, while running a rich set of additional services (see table on page 3), the Cisco 2811 and 2851 routers could sustain high levels of bi-directional traffic to the Headquarters site.



Cisco 2811 and Cisco 2851 Integrated Service Routers (ISR) provide 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.

2811 Test-bed Setup

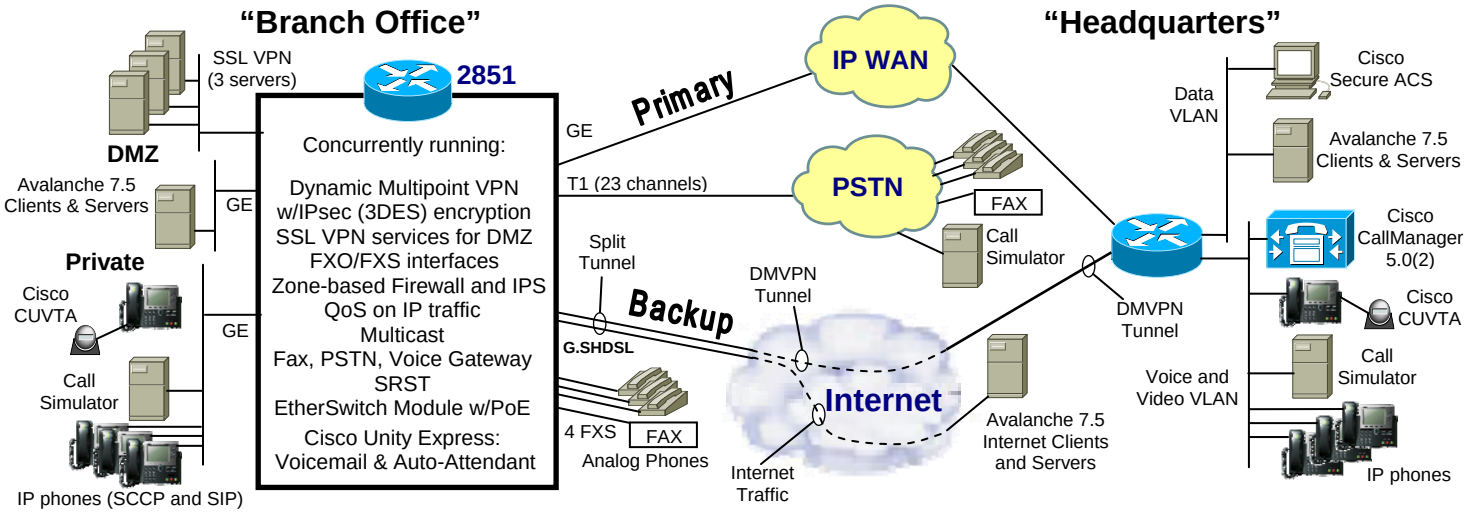


Full telephony services, and mixed data traffic flows between the Branch and HQ sites. We tested the Cisco 2811 Integrated Services Router configured with Cisco 's Unified CallManager Express and a Cisco Unity Express AIM module to support a complete IP telephony environment at the branch office. In addition, an FXO VIC module supported PSTN connectivity, and an FXS VIC module supported local analog and fax connectivity. The 16-port Integrated EtherSwitch Service Module supported connectivity for local PCs, IP phones and a Gigabit Ethernet port for server connectivity.

Performance Testing. The branch was setup with 635 Kbps of voice call traffic on the WAN to the PSTN and HQ site. Application traffic consisted of 10 FTP and 20 HTTP bi-directional user connections between the branch and the HQ over a DMVPN tunnel (using an AIM-VPN/SSL-2 encryption module). Also, we setup 5 FTP users and 10 HTTP users from the branch to the Internet and 3 HTTPS connections (using the Cisco 2811's SSL VPN services) from the Internet to three DMZ servers at the branch. The Zone-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 IP and PSTN phones), call forwarding, transfer, FAX transmission between the PSTN and the branch, and leaving and retrieving of voicemail with the Cisco Unity Express module.

2851 Test-bed Setup



Data, Voice, Video, and Telephony services between the Branch and HQ sites. We tested the Cisco 2851 Integrated Services Router configured with a Gigabit Ethernet link as Primary link to the HQ site (using a fiber SFP HWIC module), and a backup connection over a DSL link/DMVPM tunnel (using a DSL module and an AIM-VPN/SSL-2 encryption module). 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 AIM module for local voice mail in the 2851. Local analog and fax connections were handled by an 8-port FXS module (EVM), and PSTN connectivity via a T1 VWIC module. We used the two Gigabit Ethernet ports on the 2851 motherboard for server connections at the branch. A 24 port Integrated EtherSwitch Service module supported connectivity for local PCs, IP phones and an (SFP) Gigabit Ethernet port for server connectivity.

Performance Testing. the branch was setup with 2.5 Mbps of voice and video call traffic on the WAN to the PSTN (T1) and HQ site. We setup a simulated video call and a real video call using Cisco Unified Video Advantage. Application traffic consisted of 20 FTP and 100 HTTP bi-directional user connections between the branch and the HQ. Also, we setup 5 FTP users and 50 HTTP user connections from the branch to the Internet and 10 HTTPS connections (using the Cisco 2851's SSL VPN services) from the Internet to three DMZ servers at the branch. The Zone-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), 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 Dynamic Multipoint VPN (DMVPN) link through the Internet. We did not have any phone or video calls drop during the failover test.

Modules Installed in the 2811 (System Under Test)	
Module	**Description**
HWIC slot 0: VIC-4FXS/DID	Cisco 4 ports FXS/DID Analog Voice Interface Card
HWIC slot 1: VIC2-4FXO	Cisco 4 ports FXO Analog Voice Interface Card
HWIC slot 2:	available for other services
HWIC slot 3:	available for other services
DSP slots 0-1: PVDM2-64	High-Density Packet Voice Digital Signal Processor Module
AIM slot 0: AIM-CUE	Cisco Unity Express Voice Mail Advanced Integration Module
AIM slot 1: AIM-VPN/SSL-2	VPN Advanced Integration Module (AIM)
NM slot 1: NME-16ES-1G-P	16 port Singlewide Cisco EtherSwitch Service Module (with 1 GE port)
EVM slot: EVM-HD-8FXS/DID	Cisco High Density Analog and Digital Extension Module for Voice and Fax

Modules Installed in the 2851 (System Under Test)	
Module	**Description**
HWIC slot 0: WIC-1SHDSL-V3	GSI G.SHDSL Multi Line ATM WIC
HWIC slot 1: VWIC2-2MFT-T1/E1	2-port T1/E1 Multiflex Trunk Voice/WAN Interface Card
HWIC slot 2: HWIC-1GE-SFP	Cisco Gigabit Ethernet High-Speed WAN Interface Card
HWIC slot 3:	available for other services
DSP slots 0-1: PVDM2-64	High-Density Packet Voice Digital Signal Processor Module
DSP slot 2:	available for other services
AIM slot 0: AIM-CUE	Cisco Unity Express Voice Mail Advanced Integration Module
AIM slot 1: AIM-VPN/SSL-2	VPN Advanced Integration Module (AIM)
NM slot 1: NME-XD-24ES-2S-P	24 port Doublewide Cisco EtherSwitch Service Module
EVM slot: EVM-HD-8FXS/DID	Cisco High Density Analog and Digital Extension Module for Voice and Fax

Concurrent Services Running and Verified on the Cisco 2811 and 2851 Integrated Services Routers			
	Services / Features	**How 2811/2851 supports**	**How Tested/Verified**
Data	Routing and QoS	Integrated in Cisco IOS™	OSPF routing; LLQ, CBWFQ, WRED
	EtherSwitch Service Module (16 and 24 port) with 802.3af PoE	NME-16ES-1G-P NME-XD-24ES-2S-P	Voice call and “ping” tests during upgrades and reloads, and other port tests
	Cisco IOS™ Warm Reload/Upgrade	Integrated In Cisco IOS™	Verified times with/without feature
Security	L2 Security: DHCP Snooping, 802.1x authentication, IP Source Guard, etc.	NME-16ES-1G-P NME-XD-24ES-2S-P	Attempted to connect unauthorized PCs to ports, verified they would not connect
	DMVPN and 3DES encryption	Integrated in Cisco IOS™ Software and AIM-VPN/SSL-2	Via multiple test systems, link monitors, CLI, 2851 failed primary link to DMVPN backup
	Zone-based Policy Firewall	Integrated in Cisco IOS™ Software	On multilink IP WAN; 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)	Cisco IOS™ Software and AIM-VPN/SSL-2	Logged in manually in clientless mode
Voice	Cisco Unified CallManager Express	Integrated in Cisco IOS™	Verified on 2811 with manual calls
	Voicemail (stored locally on AIM-CUE)	Part of AIM-CUE module	Voicemail sent, retrieved under load
	Auto-Attendant	Part of AIM-CUE module	Manually checked under load
	Conference Calling	Integrated in Cisco IOS™	Manually checked under load
	Survivable Remote Site Telephony (SRST) for 2851	Integrated in Cisco IOS™ Software	Failed WAN link to remote CallManager; calls placed locally and via PSTN
	Fax, PSTN, Voice gateway	Fax (FXS module), PSTN (FXOs for 2811, T1 for 2851)	Fax and PSTN voice calls placed
	RSVP Agent with Application ID	Integrated in Cisco IOS™	Manually changed reservation bandwidths
Manage-ment	Traffic Statistics, Load Monitoring	Integrated in Cisco IOS™	Output viewed via CLI during testing
	Unified Communications Express - Quick Configuration Tool (UCE-QCT)	UCE-QCT Configuration commands	Demonstrated tool functions

Modularity and Concurrency

The Cisco 2811 and 2851 ISRs (Integrated Services Routers) run Cisco's IOS™ Software, and offer 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.

The Cisco 2811 ISR is the smaller of the two routers, well suited for smaller branch offices. The Cisco 2851 is a more substantial router both from a throughput (capacity) standpoint and offers a higher density of modules.

We tested an assortment of modules and Cisco IOS™ Software features. Both routers were configured with EtherSwitch Service Modules and the AIM-VPN/SSL-2 Hardware Encryption Modules. Additional modules and features tested included Layer-2 Security functions handled by the EtherSwitch Service Module, Secured Voice Gateway functions, SSL VPN services, Cisco Unity Express (voicemail module), the Quick Configuration Tool (UCE-QCT), and a variety of others.

Cisco IOS™ Software Warm Reload/Upgrade

Our tests verified that the reload times for the Cisco 2811 router and Cisco 2851 router were shortened using the Warm Reload option (a 37% savings for the 2811 and a 24% savings for the 2851). We also verified the Cisco IOS™ Software upgrade time was shortened by running tests that upgraded the two routers from release 12.4(9)T to 12.4(9)T1 using the Warm Upgrade option. For the Cisco 2851 router we saved about 24% of the upgrade time.

Ports on the Integrated EtherSwitch Service Module were not affected by the Cisco IOS™ Software upgrade. Voice calls connected through the module stayed up throughout the upgrade process. Also, we used a continuous ping test to verify that data ports on the switch module were unaffected.

Integrated EtherSwitch Service Module

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

The Integrated 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 upgraded (see the Cisco IOS™ Software Warm Start description above.)

In our test bed the Cisco 2811 and 2851 routers had an assortment of powered devices including Cisco 7970, 7961, 7960 IP phones as well as an IP-powered Sony video camera with an IEEE 802.3af PoE connection. The CLI showed which ports connected devices with IEEE standard (802.3af) PoE and which devices used Cisco pre-standard PoE. Cisco indicates the 2811 can deliver 160 watts and the Cisco 2851 can deliver 360 watts.

The EtherSwitch Service Module also performs a number of L2 security checks to provide increased network security. The switch supports 802.1x authentication, and we were able to configure a PC to authenticate with the switch using 802.1x, EAP-PEAP, and MSChapV2. The module also 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 EtherSwitch Service Module recognized the illegal connection and denied the PC network access.

We were able to exploit the integration within the ISRs with our testing of 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 EtherSwitch Service Module.

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 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.

SSL VPN

We configured both the Cisco 2811 and 2851 routers with the SSL VPN feature – using the clientless SSL VPN connection feature. The routers were configured to terminate remote access SSL VPN sessions on their AIM-VPN/SSL-2 modules.

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 for the Cisco 2811 router, we simulated 3 users, for a total of about 0.5 Mbps being processed by the SSL VPN facilities. And for the Cisco 2851 router we simulated 10 users, for a total of about 4 Mbps being processed by the SSL VPN facilities.

Zone-based Policy 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 both the Cisco 2811 and 2851 routers for all our Internet traffic.

The backup link used in the test bed for the Cisco 2851 router was configured as split tunnel through our Internet connection. The branch-to-HQ traffic was configured with a Dynamic Multipoint VPN (DMVPN) link with IPsec (3DES)

encryption – using the AIM-VPN/SSL-2 module. Both Cisco 2811 and 2851 routers were configured for DMVPN (spoke-to-spoke) and voice calls were made between branches).

Intrusion Prevention System

In our test bed, the Cisco 2811 and 2851 ISRs were 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 (Skinny Call Control Protocol) 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 Transport 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 un-secured).

Our systems were configured to encrypt H.323 signaling to the Cisco Unified CallManager, for the voice gateway, over 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 systems under test (the Cisco 2811 and 2851 routers) the Cisco Unity Express functions were contained on an AIM (Advanced Integration Module).

As we were testing voicemail we left messages at different extensions and a few of these had the 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 2851 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 Unified CallManager Express (CUCME)

We tested the Cisco Unified CallManager Express (v4.0) functions running on the Cisco 2811 router. We made a variety of local calls between SCCP phones and SIP phones and examined basic telephony functions such as call transfer, forwarding and conferencing – between different phone types, and from PSTN lines.

The Cisco Unified CallManager Express supports basic Automatic Call Distribution (ACD) with an auto-attendant. From a PSTN phone, we dialed into the auto-attendant that presented us with a "sales" queue and "customer service" queue. We had two phones on each queue (an assortment of Cisco 7970, 7961 and 7960 IP phones), and if they were both busy, we got Music on Hold until and one of the phones became free.

We also confirmed the interoperation of the Cisco Unified CallManager Express at the branch with the Cisco Unified CallManager running at the HQ location by placing a number of calls between the HQ site and the branch site.

Quick Configuration Tool (QCT)

The Cisco Unified Communication Express – Quick Configuration Tool (UCE-QCT) is a no cost application used for initial provisioning of telephony services for the ISR series routers available on CCO. UCE-QCT guides the user through the setup of the telephony system in a new router (or reset an existing router to a like new state). The tool automatically determines the modules and services physically installed in the new router.

Using a new ISR router and the UCE-QCT we were able to setup a small office PBX with four IP SCCP phones and Cisco Unity Express (voice mail). We enabled Intercom, Call Park and Hunt Groups in our test configuration. The process took less than 20 minutes and inserted over 600 lines of CLI. Support for a bar code reader to scan phone MAC addresses and a CSV file import for user data (extension, DID etc.) accelerated the process. We think this can be a very effective tool for service providers as well as IT departments for rapid deployment.

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 these systems' performance, in particular:

- The 2811 router can sustain more than 4 Mbps of WAN link traffic with concurrent voice, video, and data services with additional processor capacity to spare
- The 2851 router can sustain more than 20 Mbps WAN link traffic with concurrent voice, video, and data services with additional processor capacity to spare
- The EtherSwitch Service Module provides 802.3af PoE, integrated VLAN routing and advanced security features
- The Cisco 2811 and 2851 support comprehensive security capabilities including Zone-based firewalls, IPS, IPsec DMVPN and SSL VPNs
- SCCP calls (w/SRTP) were tested with Secure Voice Gateway. Cisco SRST (w/TLS) were also tested. H.323 signaling was encrypted with IPsec 3DES
- The Cisco Unified CallManager Express and Cisco Unity Express provide a complete branch telephony system
- The Cisco Unity Express (v2.3) module provides enhanced voicemail functions from any location

Cisco 2811 Integrated Services Router

Cisco 2851 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.

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

Report 061201