Small Office Communications Center (SOCC) Version 2 Testing Results Document

Table of Contents

Table of Figures

1 Executive Summary

In an effort to demonstrate the superior performance and flexibility of its Small Office Communication Center (SOCC) solution, Cisco Systems recently performed a series of tests at its Enterprise Solutions Engineering labs. The lead solution designer was Mohamed Babikir, a Solutions Development Manager in Cisco's Commercial Marketing organization, working in partnership with Cisco's Enterprise Solutions Engineering organization, various business units, and field representatives.

The Cisco team performed profile testing based on four different office models, ranging from a single site standalone office with 24 users, to a more sophisticated business with branch locations, teleworkers, and 76 users.

The tests used an IP-based Virtual Private Network (VPN) as the primary WAN transport. Each test profile also incorporated a variety of security features as part of an end-to-end security solution. Some examples included Stateful IOS Firewall (CBAC) for Internet traffic, an Intrusion Detection System (IDS) for both intra-site and inter-site traffic, Cisco IOS-based Intrusion Protection Systems (IPS), and site-to-site and multipoint VPNs. Our tests also included converged voice and data communications, using a combination of Cisco CallManager Express and Cisco Unity Express. We also tested a remote phone configuration tailored for teleworkers. Cisco Network Assistant (CAN) was used for monitoring, configuration, and maintenance of the SMB network, leveraging Cisco Smartports.

After testing specific product features, the Cisco team evaluated the overall solution performance for each profile, gradually increasing the load and complexity of each solution.

The results were outstanding. Even under highly stressful conditions, running fully loaded voice applications and fully loaded end-to-end security, all features remained available and performed as expected. Steady-state CPU and Packet Per Second (PPS) switching load incurred during each profile test demonstrated that the SOCC solution delivers the performance and resiliency needed for businesses of all sizes.

Together, these profile tests provide a compelling proof point that the SOCC solution succeeds in providing right-sized, comprehensive solutions that deliver real bottom-line benefits for small and medium businesses.

2 Introduction

This document summarizes test findings for the SOCC2 version 2 solution, which was conducted at the ESE labs as a partnership between Cisco's Commercial Marketing, Enterprise Solutions Engineering, various business units, and field representatives. This document should be used in conjunction with the SOCC2 Test Requirements Document, which details the test criteria, and the different requirements captured from different stakeholders for the purpose of creating an integrated office solution featuring the Next Generation Integrated Services Routers (ISR).

Profile testing, which also can be referred to as Proof of Concept (POC) testing, has been used to confirm that functional design requirements have been met with an adequate performance safety and acceptance factor. Profile testing has been divided into two likely deployment models that would be seen in an actual customer environment. The first is a “Single Site,” which is a fully contained standalone office. In this model, all network services are provided locally. This model would be expected in a small stand-alone SMB environment. The other model is a “Multi-Site,” which is a

confederation of SMB offices typically configured in a hub and spoke topology. With this model, the SMB customer has a central campus that provides many common services to multiple branch and teleworker offices. Our testing focused on four different office profiles:

- 24 user Office - Single Site
- 48 user Office - Multi-Site
- 76 user Office - Multi-Site
- 76 user Office with Dual Routers - Multi-Site

Note: The limitation of 76-user support was due to the CCME license, which was available in the IOS image we received for the testing phase. By the official release of the Next Generation ISR routers, this limit will go up to 96 users. Based on our test findings, we believe the NG ISR routers can support 96 CCME with very minimal added loads. In our next phase of testing we will run a test scenario with 96 CCME and update this document with the findings.

3 Test Setups

Below are the 4 different office profiles and their associated tested architectures.

3.1 24 User Office - Single Site

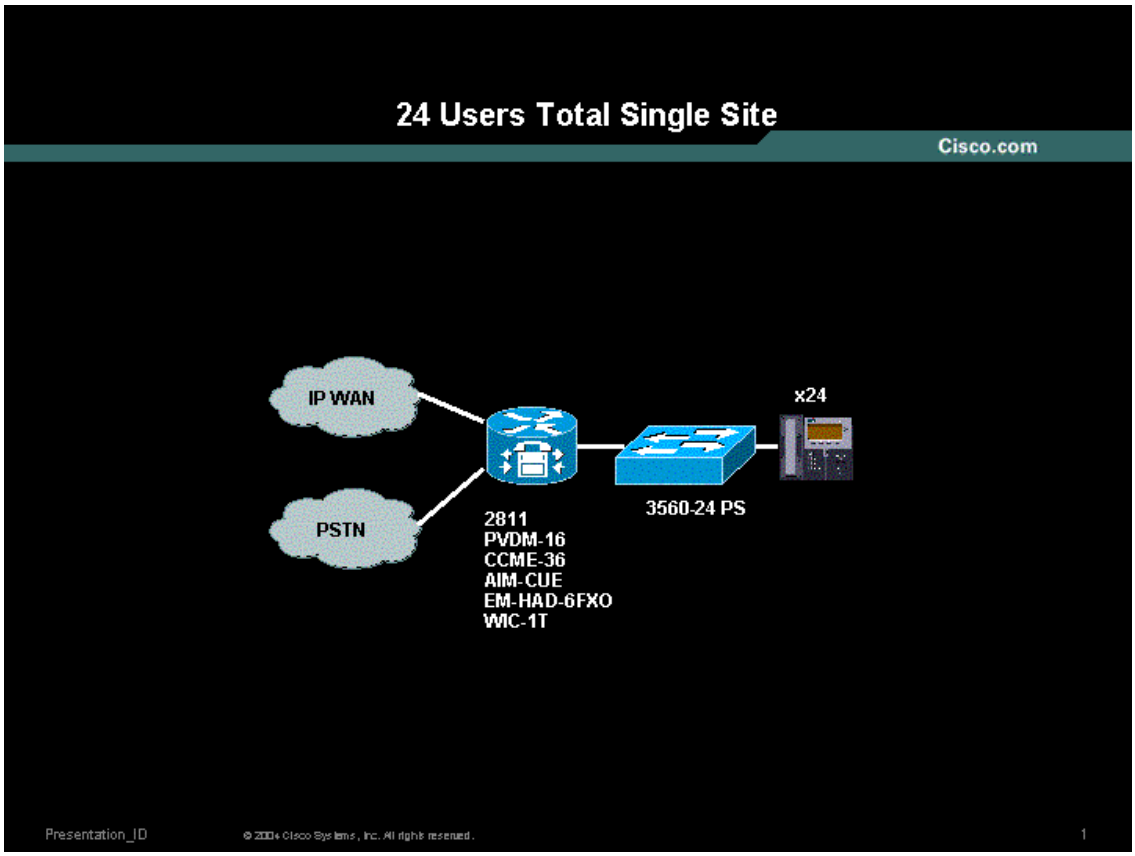


Figure 1 - 24 User Office - Single Site

3.2 48 User Office - Multi-Site

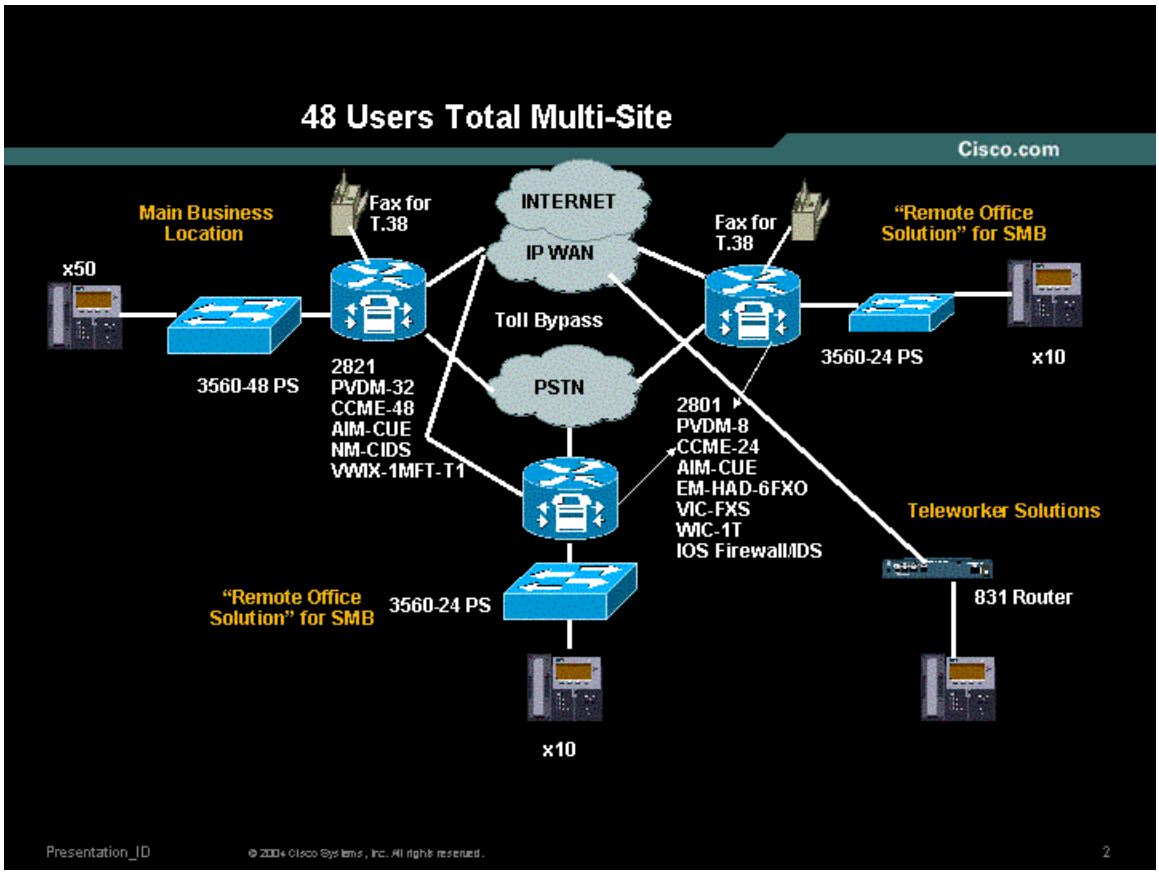


Figure 2 – 48 User Office - Multi-Site

3.3 76 User Office – Multi-Site

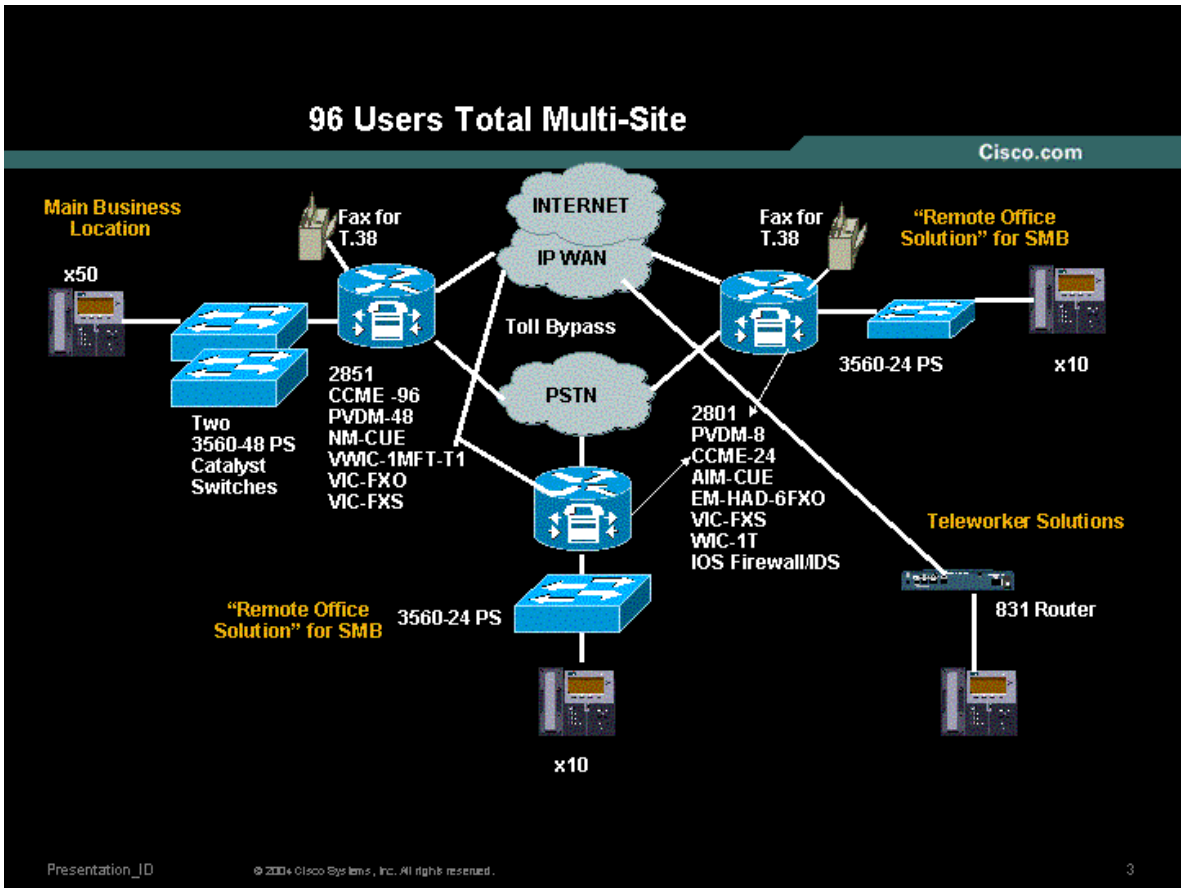


Figure 3 – 76 User Office – Multi-Site

3.4 76 User Office with Dual Routers - Multi-Site

In this configuration we have two 2851 routers in the HQ forming an HSRP virtual group, two remote office routers each with a 2801, and a telecommuter/SOHO user based on an 831 router.

The two routers in the HQ site each connect to a 3560-48 PS LAN switch via an 802.1Q trunk. Redundancy is provided by a trunk connection between each of the 3560-PS LAN switches therefore providing connectivity for LAN devices to each of the office routers. Three VLANs will be configured, one for voice, one for data, and one for the DMZ traffic. There are two T1 WAN interfaces in each 2851 router that are bundled together via MultiLink PPP (MLPPP) and connected to a simulated ISP Internet connection. In addition, T1 voice interfaces are installed in each router that connect to a simulated PSTN switch. Each of the dual routers is designated as a primary for a specific service. One of the 2851 routers is designated as the primary voice router and the backup for the Data and DMZ router. The other 2851 router is designated as the primary Data and DMZ router and the backup for the primary voice router. The primary 2851 voice router hosts the Voicemail Network Module for storing voice mail messages. The primary Data and DMZ router will host the Intrusion Detection System (IDS) Network Module for inline intrusion detection. IOS FW *a.k.a* Content Based Access Control (CBAC) is enabled on both 2851 routers by configuring access lists and the ***IP Inspect in*** command statements on all interfaces serving the office network. The *SIMClient* Tool is used to simulate the IP phone clients that register with CME and generate phone calls. The *Chariot* tool is used to generate data packets to simulate data traffic to and from the Internet, LAN and DMZ.

Each 2851 router has an instance of the Cisco CallManager Express (CCME) software. The IP phones register with the virtual HSRP address, which is bound to the primary 2851 router. In the unlikely case of a failure to the primary voice router, all the phones will re-register with the backup 2851 Data/DMZ router and voice traffic will be routed through this router.

T.38 fax calls were placed to and from the HQ site to one of the remote offices.

Each remote office is composed of a 2801 router and a 3560-24 PS LAN switch. Each 2801 hs a T1 interface to simulate data traffic going into the WAN cloud, and a Foreign Exchange Office/interface (FXO/FXS) interfaces to simulate the IP phone and fax calls going into the PSTN cloud.

The IP WAN/Internet Cloud is composed of *3DES IPSec Dynamic Multipoint Virtual Private Network (DMVPN)* running between the HQ routers and each of the Remote routers over the simulated Internet WAN.

Note: DMVPN was configured in a Hub-and-Spoke configuration and no spoke-to-spoke traffic was tested.

Several ease of use tools are used to configure the different devices, including: Smartports, Cisco Network Assistant (CNA), and Security Device Manager (SDM).

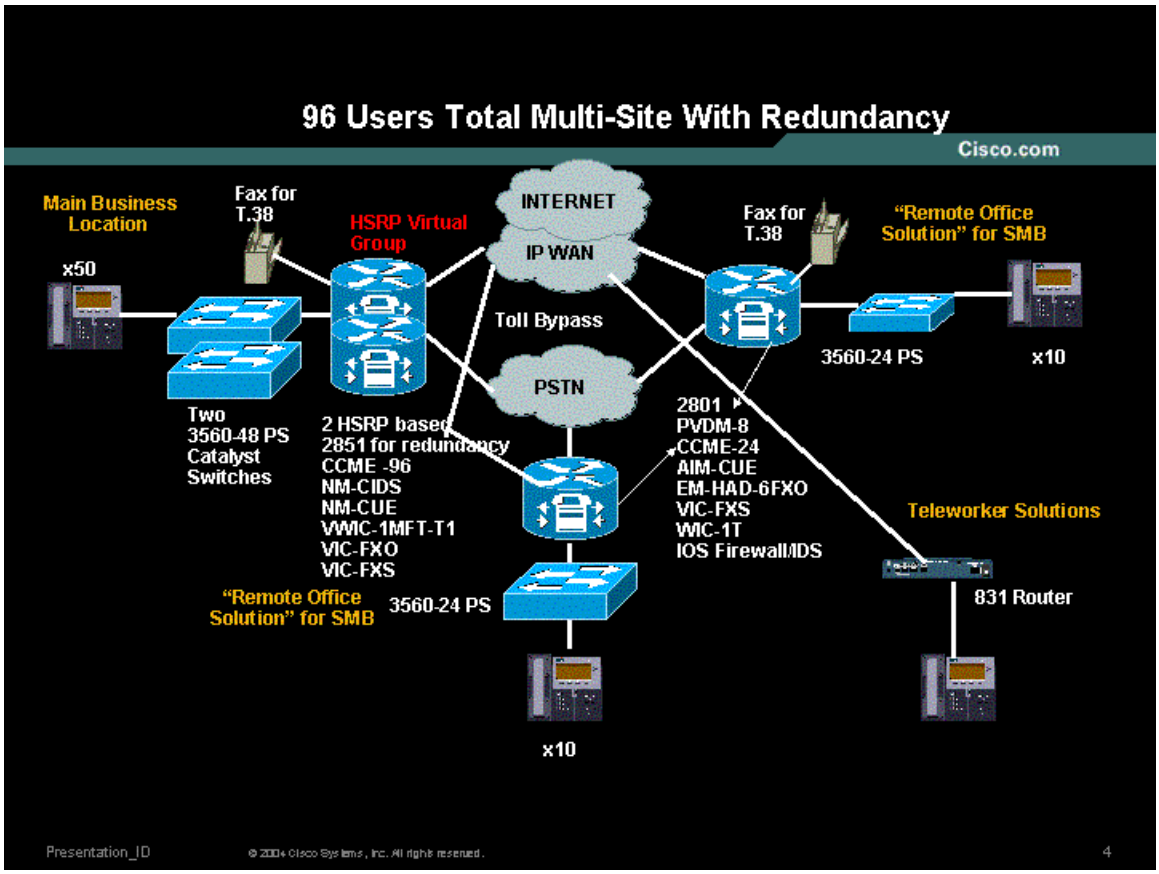


Figure 4 - 76 User Office with Dual Routers – Multi-site

4 Solution Bill of Materials

4.1 24 User Office - Single Site

Product	Description	Quantity
2811	Next Generation Router	1
PVDM-16	DSP SIM for 16 DSPs	1
Adv IP Svcs	IP Advanced image for NG routers	
CCME-36	Cisco CallManager Express license for 36 users	
AIM-CUE	Unity Express incense for 24 Users	
securityEP	Security enabled image	
VIC2-4FXO	Voice Module for PSTN calls	3
WIC-1T	WAN Data Traffic	1
Catalyst 3560-24 L2 Switch	24 Ethernet 10/100 ports with Power over Ethernet (PoE) and 2 small form-factor pluggable (SFP) ports; 1 rack unit (1RU)Cisco Catalyst 3560-48PS	1

4.2 48 User Office - Multi-Site

HQ Configuration		
Product	**Description**	**Quantity**
2821	Next Generation Router	1
PVDM-32	DSP SIM for 32 DSPs	1
Adv IP Svcs	IP Advanced image for NG routers	
CCME-48	Cisco CallManager Express license for 48 users	
AIM-CUE	Unity Express license for 48 Users	
securityEP	Security enabled image	
NM-CIDS-K9	IDS Network Module	1
VWIC-2MFT-T1	1-Port RJ-48 Multiplex Trunk-T1. It supports both PSTN & Data. 24 Channels for Voice & 24 Channels for Data	1
Catalyst 3560-48 L2 Switch	48 Ethernet 10/100 ports with PoE and 4 SFP ports; 1RU	1

Remote Office Configuration for 2 sites		
Product	**Description**	**Quantity**
2801	Next Generation Router	2
PVDM-8	DSP SIM for 8 DSPs	2
Adv IP Svcs	IP Advanced image for NG routers	
CCME-24	Cisco CallManager Express license for 24 users	
AIM-CUE	Unity Express license for 24 Users	

securityEP	Security enabled image	
VIC2-4FXO	Voice Module for PSTN calls	4
WIC-1T	WAN Data Traffic	2
Catalyst 3560-24 L2 Switch	24 Ethernet 10/100 ports with Power over Ethernet (PoE) and 2 small form-factor pluggable (SFP) ports; 1 rack unit (1RU)Cisco Catalyst 3560-48PS	2

Telecommuter Configuration for SOHO site		
Product	**Description**	**Quantity**
831 router	800 series router for SOHO traffic simulation	1

4.3 76 User Office - Multi-Site

HQ Configuration		
Product	**Description**	**Quantity**
2851	Next Generation Router	1
PVDM-48	DSP SIM for 48 DSPs	1
Adv IP Svcs	IP Advanced image for NG routers	
CCME-76	Cisco CallManager Express license for 48 users	
NM-CUE	Unity Express Network Module for 100 Users	1
securityEP	Security enabled image	
VWIC-2MFT-T1	1-Port RJ-48 Multiplex Trunk-T1	2
Catalyst 3560-48 L2 Switch	48 Ethernet 10/100 ports with PoE and 4 SFP ports; 1RU	1

Remote Office Configuration for 2 sites		
Product	**Description**	**Quantity**
2801	Next Generation Router	2
PVDM-8	DSP SIM for 8 DSPs	2
Adv IP Svcs	IP Advanced image for NG routers	
CCME-24	Cisco CallManager Express license for 24 users	
AIM-CUE	Unity Express license for 24 Users	1
securityEP	Security enabled image	
VIC2-4FXO	Voice Module for PSTN calls	4
WIC-1T	WAN Data Traffic	2

Catalyst 3560-24 L2 Switch	24 Ethernet 10/100 ports with Power over Ethernet (PoE) and 2 small form-factor pluggable (SFP) ports; 1 rack unit (1RU)Cisco Catalyst 3560-48PS	2

Telecommuter Configuration for SOHO site		
Product	**Description**	**Quantity**
831 router	800 series router for SOHO traffic simulation	1

4.4 76 User Office with Dual Routers - Multi-Site

HQ Configuration		
Product	**Description**	**Quantity**
2851	Next Generation Router	2
PVDM-48	DSP SIM for 48 DSPs	2
Adv IP Svcs	IP Advanced image for NG routers	
CCME-76	Cisco CallManager Express license for 48 users	
NM-CUE	Unity Express Network Module for 100 Users	1
securityEP	Security enabled image	
NM-CIDS-K9	IDS Network Module	1
VWIC-2MFT-T1	1-Port RJ-48 Multiplex Trunk-T1	4
Catalyst 3560-48 L2 Switch	48 Ethernet 10/100 ports with PoE and 4 SFP ports; 1RU	2

Remote Office Configuration for 2 sites		
Product	**Description**	**Quantity**
2801	Next Generation Router	2
PVDM-8	DSP SIM for 8 DSPs	2
Adv IP Svcs	IP Advanced image for NG routers	
CCME-24	Cisco CallManager Express license for 24 users	
AIM-CUE	Unity Express license for 24 Users	2
securityEP	Security enabled image	
VIC2-4FXO	Voice Module for PSTN calls	4
WIC-1T	WAN Data Traffic	2
Catalyst 3560-24	24 Ethernet 10/100 ports with Power over	2

L2 Switch	Ethernet (PoE) and 2 small form-factor pluggable (SFP) ports; 1 rack unit (1RU)Cisco Catalyst 3560-48PS	

Telecommuter Configuration for SOHO site		
Product	**Description**	**Quantity**
831 router	800 series router for SOHO traffic simulation	1

4.5 Software

For these tests, we were not able to obtain generally-available IOS images for Next Generation routers because these products have not been announced yet. We were limited to testing with private images and engineering builds. NG routers 2800 and 1800 will start shipment with image *12.3(8) T4*. Our testing was based on an experimental release of this image.

4.6 Test Equipment

Throughout the testing setup, we configured a variety of routers, switches and servers to create the test bed. These devices were used to generate traffic loads and gathering results. The devices were used in a way that would not introduce any negative impact on the test results. These devices are not part of the Bill of Materials Section and need not be specified.

5 Feature Description

5.1 WAN Connectivity

The primary WAN transport used was an IP-based VPN. IP VPNs are capable of supporting IP telephony, converged IP, and legacy applications. IP-based VPNs are also compatible with secure partner connections, teleworker, and small/remote branch connections over broadband. When economic or business restrictions prevent the deployment of an IP-based VPN, other VPNs, Layer 2, and legacy private WAN technologies are supported. In our testing, 3DES VPN will be tested over T1 WAN Links.

In the design of our testing we used a WAN cloud consisted of a DMVPN over T1 WAN links. DMVPN was configured in a hub-and-spoke configuration where the primary benefit realized is the ease of headend configuration where a single multipoint GRE interface is configured for all spokes. Although DMVPN does support dynamic tunnel creation between spokes, that functionality was not tested in this phase of SOCC testing. For more technical information about DMVPN, please visit:

http://www.cisco.com/warp/customer/105/dmvpn.html

We have also deployed EasyVPN between the Cisco 831 SOHO router and the hub routers as a demonstration of a data-only teleworker configuration. A remote phone configuration was also tested, and is discussed later in this document.

5.2 Security

Our testing incorporated many security features, forming an end-to-end security offering. Some of the features used were: Static IPSec with GRE tunneling for site-to-site VPN; dynamic multipoint VPN, NAT and Stateful IOS Firewall (CBAC) for Internet traffic' and IDS for both intra-site and inter-site traffic using NM-CIDS-K9 in the 48 and 76 user segments; and IOS-based Intrusion Protection Systems (IPS).

5.2.1 ACLs, IOS Firewall and IDS Configuration

The recommended philosophy for securing the office network is as follows.

- Use ACLs to tightly restrict traffic inbound to the office network at every entry point.
- Configure firewall inspection (see Figure 21) and IDS protection anywhere external sources of traffic are introduced into the office network (see Figure 22).
- The DMZ is considered a traffic sink, and hosts on the DMZ shall not initiate any sessions. Only inbound sessions are allowed to initiate sessions back to the source, whether it's a LAN- or Internet-based host.

Security policies were configured as follows:

- Packets flow from the Perimeter (source) to the Perimeter (destination).
- ACL policies are applied at the Perimeter (source) to filter inbound traffic.
- Firewall inspection and IDS packet monitoring is applied at the source of inbound packet flows.

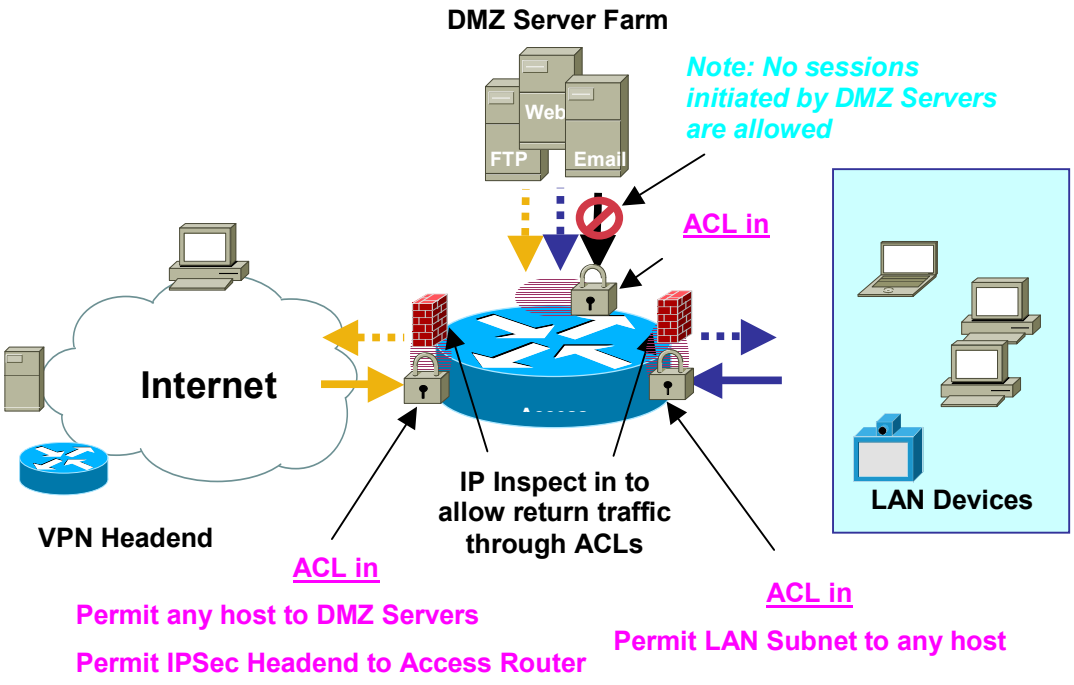


Figure 5 - ACL and IOS FW Configuration

5.3 Integrated IP Communications

Our tests deployed converged voice and data communications using a combination of Cisco CallManager Express (CCME) and Cisco Unity Express (CUE). CCME lets customers enable feature-rich branch or small office call processing via their existing or planned multiservice access routing platform. In conjunction with CCME, CUE offers integrated voice mail and auto attendant functionality. Together, CCME and CUE provide a simple, consistent, distributed architecture that can be easily replicated for multiple small branch locations across an enterprise network. We also tested a remote phone configuration tailored for teleworkers, where call processing is performed by the central site CME for the teleworker IP phone. Teleworker voice mail is also supported and located in the central site CUE module. We tested remote phone support with DMVPN only because this feature is not supported over EZVPN.

5.4 Ease-of-Use Tools

5.4.1 Cisco Network Assistant & SmartPorts

Cisco Network Assistant integrates monitoring, configuration, and maintenance of the SMB network, providing all the functionality required to maximize network value by leveraging Cisco Smartports. This is offered at zero cost to the reseller or end user, since CNA is available as a free download from CCO. Cisco Smartports enable Cisco partners and customers with limited Cisco IOS Knowledge to take full advantage of Cisco's Best Practices in the deployment of advanced services such as IP telephony.

In our tests, the Smartports feature was used to configure multiple ports on the Catalyst 3560 POE switches for setting up IP phones and desktops. It was also used to configure trunk ports to the router. Smartports was also used to configure security and QoS features for IP phones and desktops by applying Cisco recommended settings through GUI interface. Below is a screen snapshot of the CNA tool:

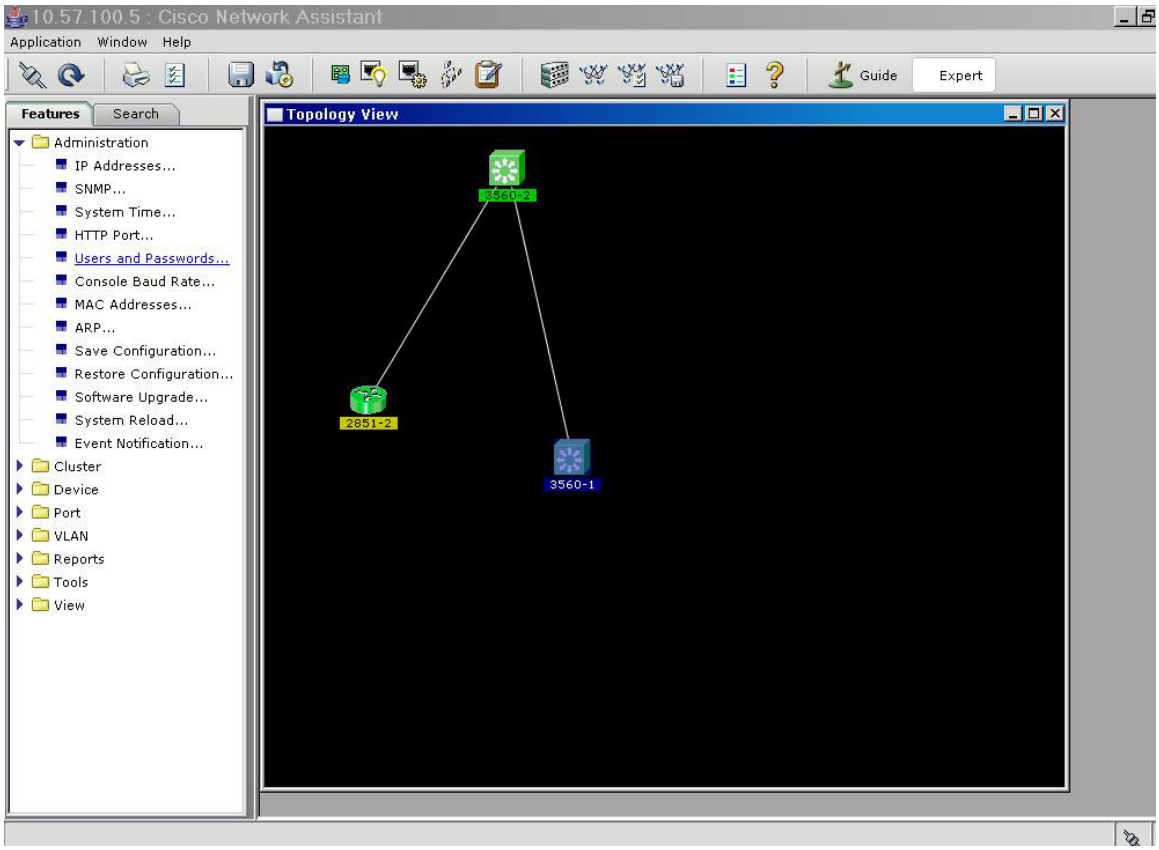


Figure 6 - Cisco Network Assistant Screenshot

Below is a snapshot of the SmarPort GUI we used during the testing, launched from within the CNA tool:

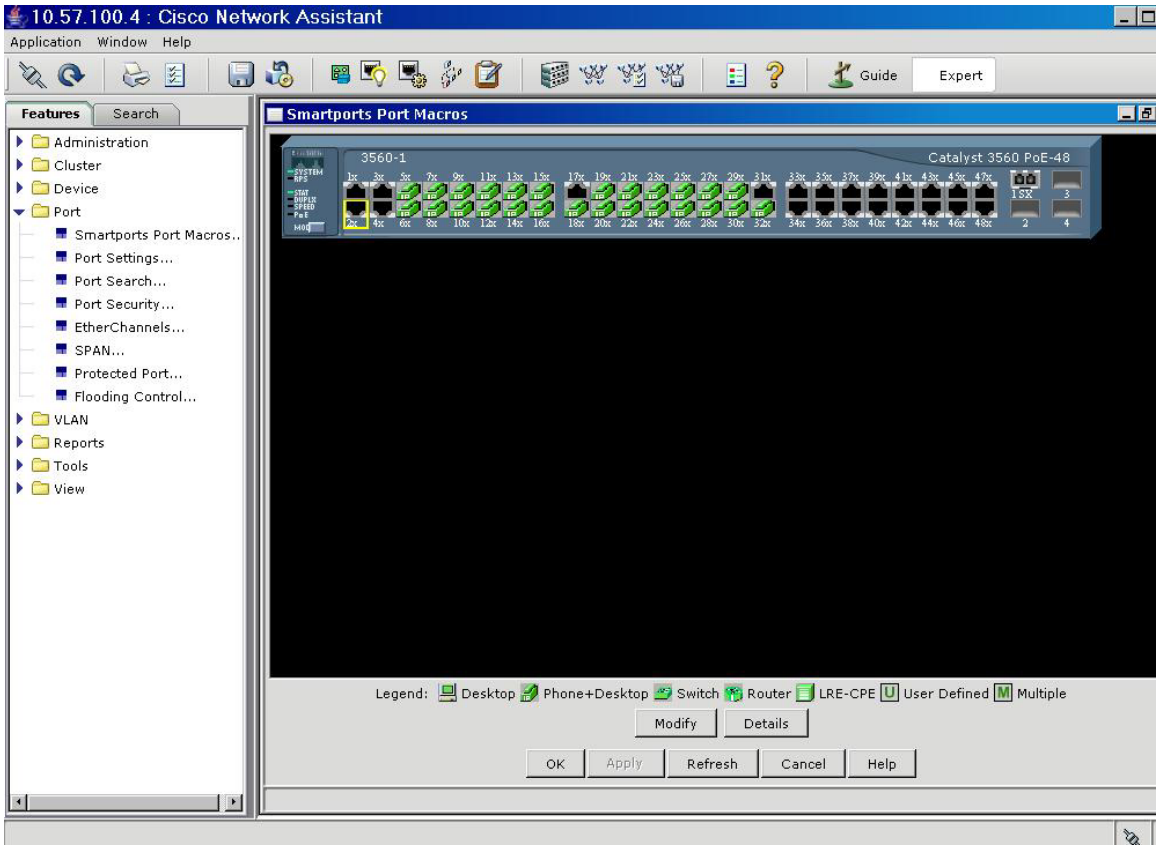


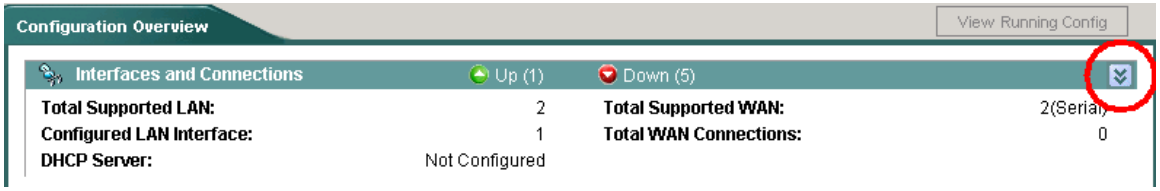
Figure 7 - Cisco Network Assistant Smartport Port Configuration

5.4.2 SDM

The Cisco Security Device Manager (SDM) is an intuitive, easy to use, web-based device management tool embedded within the Cisco IOS access routers. SDM was used to configure the Next Generation routers and all of the associated IOS-based Security features.

We used the SDM tool in the SOCC Version2 solution tests for:

1. **Configuring Easy VPN** between the remote teleworker to the headquarters site.
2. **Security Audit**: after applying the firewall and VPN settings, a security audit was done to test the security of the network.
3. Show the Configuration Overview and get a high level snapshot of the router resources like interface and configuration.



To show more information

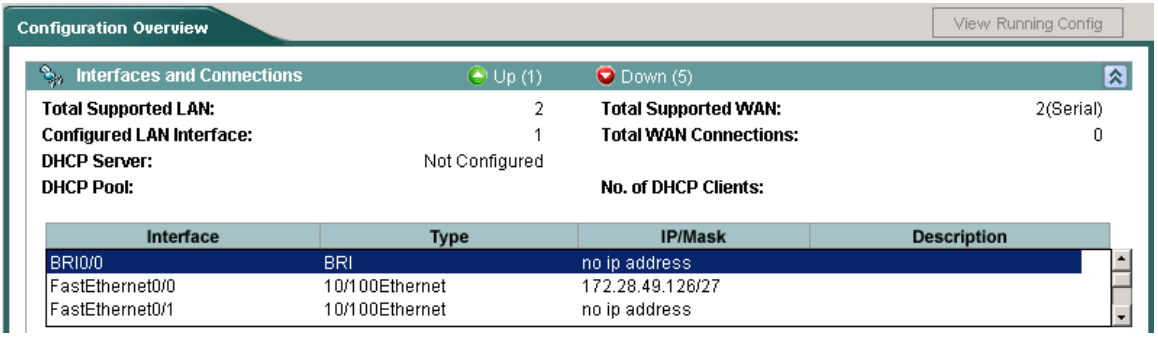


Figure 8 - Cisco Security Device Manager Easy VPN Configuration

5.5 IP Routing Redundancy

IP routing redundancy provides support for transparent fail-over at the first-hop IP router. We deployed the Hot Standby Routing Protocol (HSRP) to test failover of IP phones and PSTN trunks. This test was used on the 76-user segment. In our tests, HSRP was configured between the two 2851 routers in the main business location for the 76-user segment profile. Two HSRP groups were configured: one for voice and the other for data. One 2851 router was designated as a primary voice router. It had 2 T1s for voice and 1 T1 for data. The other 2851 was designated as a primary data router. It had 2 T1s for data and 1 T1 for voice.

6 Testing Methodology

The below diagram illustrates the test topology that was deployed for the multi-site 48 to 76-ser dual router profile. It depicts all the test tools and how the main office and remote offices were simulated over the WAN cloud. The color-coded lines show the various links and how voice, LAN data, and data DMZ traffic is routed in the network. This topology shows where and how traffic was generated and can be used as a reference to how the other office profiles were tested.

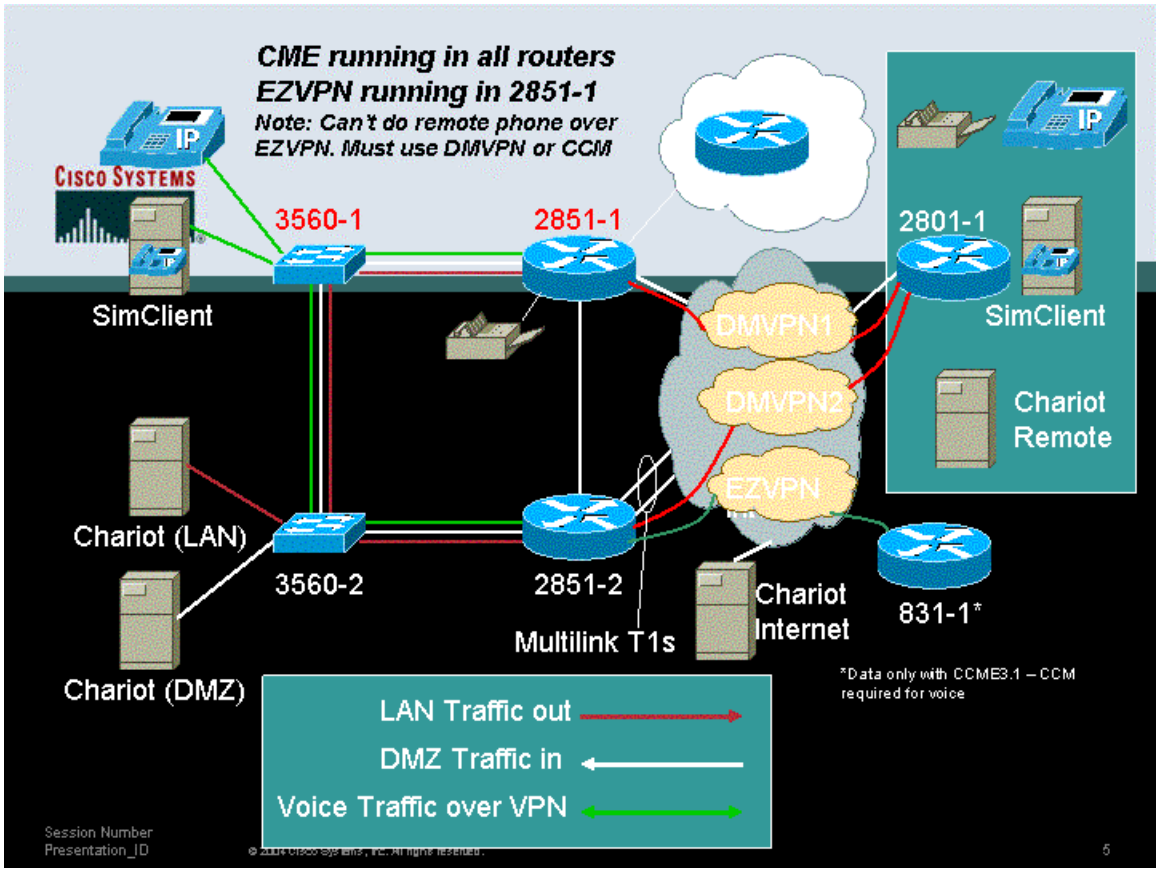


Figure 9 - 76 User Office with Dual Router Tested Configuration

7 Discrete Features Functionality Test Cases

The table below highlights the individual features that were tested and verified for each profile mentioned above. The goal of this phase was to monitor the behavior of each NG router module. We focused on the way in handled each discrete feature, which enabled us to isolate any interoperability issues that may have arisen

Title	Description	Expected Results	Comments
Security			
Security-IPSec DMVPN	Bring up a DMVPN IPsec GRE tunnel utilizing NHRP & routing protocol between the HQ and a RO.	Verify connectivity by ping.	Done. Was able to launch the tunnel using NHS in the hub and acquire IP address of remote router.
Security-IPSec Easy VPN Tunnel	Bring up an EasyVPN tunnel between the HQ & 831.	Verify connectivity by ping.	Done. EasyVPN profile was installed correctly on the 831.
Security-IOS-FW	Enable IP inspection over the WAN/LAN/DMZ interfaces with access list.	Verity HTTP inspection using traffic generated across the WAN, use show ip inspect session to verify ip inspection. Verify ICMP inspection using ping command.	Done. Logged traffic to verify FW functionality.
Security-NAT	Enable NAT translation between	Verify connectivity by	Enabled NAT

	DMZ/WAN & LAN.	ping	between the DMZ and the local LAN.
Security-IPS	Enable IOS based as well as HW based IPS monitor/blocking on LAN/DMZ/WAN interfaces.	Get a list of supported signatures generated from the IDS.	Loaded IOS IPS on voice 2851 router & HW IPS on Data 2851 router.
Content-filtering	Configure IP URL Filtering on the router to block specific URLs.	Verify router denies URLs designated as prohibited.	Configured Static lists due to unavailability of a URL filtering server. Feature is confirmed to work in other test scenarios.
IP Telephony			
IP-Telephony-CCME-registration	Configure CCME for 24/48/76 users, use sim client/IP phone to register to CCME.	Verify phone register correctly and able to make calls to each other.	Done. E-phones registered to CCME correctly with the right load.
IP-Telephony-CCME-Call-Transfer	Configure CCME for blind call transfer..	Verify calls can be blind transfer.	Successful.
IP-Telephony-CCME-Remote phone dialing	Configure CCME to receive calls from remote phones across the WAN.	Verify Phone register correctly and able to make calls to each other.	Phone behind the 831 registered to CCME behind the HQ 2851.
IP-Telephony-CCME-Call-Transfer	Configure CCME for call transfer.	Verify calls can be transferred.	Done. Call transferred successfully.
CCME-Call-conference	Configure CCME for conference/call transfer.	Verify calls can be conferenced	3 e-phones were conferenced in.
CUE-Basic-VM	Configure CUE.	Verify voice mail system is initialized properly.	Done. Need to configure two peers: H.323 & SIP for CUE module.
CUE-user-import	Import users from CCME.	Verify user is imported correctly.	Done. Need to configure two peers: H.323 & SIP for CUE module
CUE-VM-busy	Leave a VM to a IP phone which is busy	Verity VM is left correctly and MWI is working properly	Done. Need to configure two peers: H.323 & SIP for CUE module.
CUE-VM-no-answer	Leave a VM to a IP phone which no one is answering	Verity VM is left correctly and MWI is working properly	Done. Need to configure two peers: H.323 & SIP for CUE module.
CUE-VM Site-to-Site Networking	Configure CUE on HQ Router and RO router and send a VM message from one site to the other.		Not supported. Supported only between extensions off the same CCME.
T.38 IP Fax Support			
T.38 Fax Relay	Initiate fax calls between the HQ and RO routers. Fax calls originate	Verify T.38 Relay works properly.	Done. T.38 fax was configured between the 2851 & 2801 RO.

	from PCs behind each router.		
IP Redundancy			
IP-HSRP	Configure HSRP between the two 2851 routers in the HQ. IP phones should register with the virtual HSRP IP address, which is tied to the primary voice router. IP phones must re-register with the backup data router.	Verify IP phones will re-register with the CCME on the backup router after the master HSRP router goes down. Also verify PSTN trunks failover.	We used Multilink PPP for 2 ISPs one primary and one secondary. To ensure failover will work properly, secondary provider agrees to advertise the addressing space of the DMZ, which belongs to the primary provider. This is a real world scenario. When primary ISP goes down, secondary ISP will advertise DMZ subnet.
Ease of Use Tools			
	Cisco Network Assistant (CNA)	Load CNA 1.0 on the LAN switches and verify that it can: 1- Discover Network topology 2- Launch Smartports to configure IP phones and router macros 3- Save switch configs	Done.
	Smartports	Launch smartports from within CNA in the catalyst 3560 switch ports to configure: 1. Switch trunks 2. Router Trunks 3. IP Phone + Desktop 4 Desktop	Done.
	Security Device Manager (SDM)	Launch SDM on the routers to: 1- Configure DMVPN 2- Easy VPN server/client 3- IOS FW & IDS	Done.

8 Performance Test Cases

The section below shows the solution performance procedure for each profile. Each feature is layered on top and added to the overall test. This was done to increase the load and complexity of the solution, and monitor how the solution behaves.

8.1 24 User Office - Single Site

Title	Description	Test Setup	Test Launch	2811 NG Router Under Test
24 User Profile based on 2811 NG router	**Voice Testing Order:** 1) On the 2811 NG router, LAN phone A calls LAN phone_ B, two way audio streams is setup over H.323 Peer. 2) LAN phone_B is sent to VM, if LAN phone_A (Rings No Answer) RNA. Two way Audio with CUE from phone_B is established. 3) Phone_A displays Message Waiting Indicator (MWI) light on. 4) Phone_A can retrieve message with "message" button, mailbox ID known. 5) Phone_A MWI light goes off after message retrieval. 6) Phone_A dials callgen channel, hears test tone. 7) LAN_to_LAN T.38 FAX passes in both directions 8) Measure CPU/memory usage and PPS throughput.	1) Callgen test file is loaded. 2) Callgen is configured to call Simclient phones PLUS one real 7960 phone. 3) 7960 phone is picked up to verify audio and is also left to forward to CUE. 4) ISDN status shows multiple frames. 5) Simclient phones register with CCME. 6) Simclient scripts set to call callgen channels. 7) Simclient scripts staggered to prevent synchronization. 8) Simclient set to generate RTP payloads. 9) Chariot test file is built and loaded. 10) Chariot data mix is set to standard ESE loads: 60% TCP & 40% UDP.	1) Simclient is started with the test duration set to unlimited. 2) Callgen channels 1-24 are set to active, duration unlimited. 3) Chariot test file is set to 10 minutes. 4) Verify real phone is ringing. 5) Verify voice quality from phone_A to phone_B.	1) Collected show commands from the router to illustrate router behavior under load and that all features such as FW CBAC, IPS, CUE, DMVPN and FAX are working as expected. 2) After the Chariot test has completed, the results were analyzed to ensure the appropriate date streams were permitted or blocked depending on the firewall and DMZ settings. 3) Test duration was for 10 minutes for a complete load. Background voice was continuously running.

8.2 48 User Office - Multi-Site

Title	Description	Test Setup	Test Launch	2811 NG Router Under Test
48 User Profile based	**Voice Testing Procedure:**	1) Callgen test file is loaded.	1) Simclient is	1) Collected show commands

on 2821 NG router	1) On the 2821 NG router, LAN phone A calls remote phone_ B over the IPSec DMVPN cloud, two way audio streams is setup over H.323 peer. 2) Remote phone_B is sent to VM, if LAN phone_A (Rings No Answer) RNA. Two way Audio with CUE from phone_B is established. 3) Phone_A displays Message Waiting Indicator (MWI) light on. 4) Phone_A can retrieve message with "message" button, mailbox ID known. 5) Phone_A MWI light goes off after message retrieval. 6) Phone_A dials callgen channel, hears test tone. 7) T.38 FAX over the DMVPN tunnel passes on both directions. 8) Measure CPU/memory usage and PPS throughput. **Data Testing Procedure**: 1) DMVPN tunnels were setup between the two remote offices. Next Hop Routing Protocol (NHRP) is used along with dynamic routing to find the IP address of the Next Hop Client (NHC) from the Next Hop Sever (NHS), which is the 2821. 2) EZVPN tunnel is setup between the 2851 & 831.	2) Callgen is configured to call Simclient phones PLUS one real 7960 phone. 3) 7960 phone is picked up to verify audio and is also left to forward to CUE. 4) ISDN status shows multiple frames. 5) Simclient phones register with CCME. 6) Simclient scripts set to call callgen channels. 7) Simclient scripts staggered to prevent synchronization. 8) Simclient set to generate RTP payloads. 9) Chariot test file is built and loaded. 10) Chariot data mix is set to standard ESE loads: 60% TCP & 40% UDP.	started with the test duration set to unlimited. 2) Callgen channels 1-24 are set to active, duration unlimited. 3) Chariot test file is set to 10 minutes. 4) Verify real phone is ringing. 5) Verify voice quality from phone_A to phone_B.	from the router to illustrate router behavior under load and that all features such as FW CBAC, IPS, CUE, DMVPN and FAX are working as expected. 2) After the Chariot test has completed, the results were analyzed to ensure the appropriate date streams were permitted or blocked depending on the firewall and DMZ settings. 3) Test duration was for 10 minutes for a complete load. Background voice was continuously running.

8.3 76 User Office - Multi-Site

Title	Description	Test Setup	Test Launch	2811 NG Router Under Test
76 User Profile based on 2851 NG routers with and without HSRP	**Voice Testing Procedure:** 1) On the 2851 NG router, LAN phone A calls remote phone_ B over the IPSec DMVPN cloud, two way audio streams is setup over H.323 Peer. 2) Remote phone_B is sent to VM, if LAN phone_A (Rings No Answer) RNA. Two way Audio with CUE from phone_B is established.	1) Callgen test file is loaded. 2) Callgen is configured to call Simclient phones PLUS one real 7960 phone. 3) 7960 phone is picked up to verify audio and is also left to forward to CUE. 4) ISDN status shows multiple frames.	1) Simclient is started with the test duration set to unlimited. 2) Callgen channels 1-24 are set to active, duration unlimited. 3) Chariot	1) Collected show commands from the router to illustrate router behavior under load and that all features such as FW CBAC, IPS, CUE, DMVPN and FAX are working as expected. 2) After the Chariot test has

	3) Phone_A displays Message Waiting Indicator (MWI) light on. 4) Phone_A can retrieve message with "message" button, mailbox ID known. 5) Phone_A MWI light goes off after message retrieval. 6) Phone_A dials callgen channel, hears test tone. 7) T.38 FAX over the DMVPN tunnel passes on both directions. 8) Measure CPU/memory usage and PPS throughput. **Data Testing Procedure**: 1) DMVPN tunnels were setup between the two remote offices. Next Hop Routing Protocol (NHRP) is used along with dynamic routing to find the IP address of the Next Hop Client (NHC) from the Next Hop Sever (NHS), which is the 2821. 2) EZVPN tunnel is setup between the 2851 & 831. 3) Test HSRP by failing the voice router and see all the phones re-register with the backup 2851 NG router. Please reference the IP redundancy section on the previous section for more details on setup of the HSRP group.	5) Simclient phones register with CCME. 6) Simclient scripts set to call callgen channels. 7) Simclient scripts staggered to prevent synchronization. 8) Simclient set to generate RTP payloads. 9) Chariot test file is built and loaded. 10) Chariot data mix is set to standard ESE loads: 60% TCP & 40% UDP.	test file is set to 10 minutes. 4) Verify real phone is ringing. 5) Verify voice quality from phone_A to phone_B.	Chariot test has completed, the results were analyzed to ensure the appropriate date streams were permitted or blocked depending on the firewall and DMZ settings. 3) Test duration was for 10 minutes for a complete load. Background voice was continuously running.

8.4 Test Results

The office routers were placed under the load conditions that emulated the office profiles and network topologies described above. Figure 10 illustrates the steady-state CPU and Packet Per Second (PPS) switching load incurred during each profile test. Three voice and data office profiles are shown, as well as the dual router profile where one router acted as the primary for voice and the other for data.

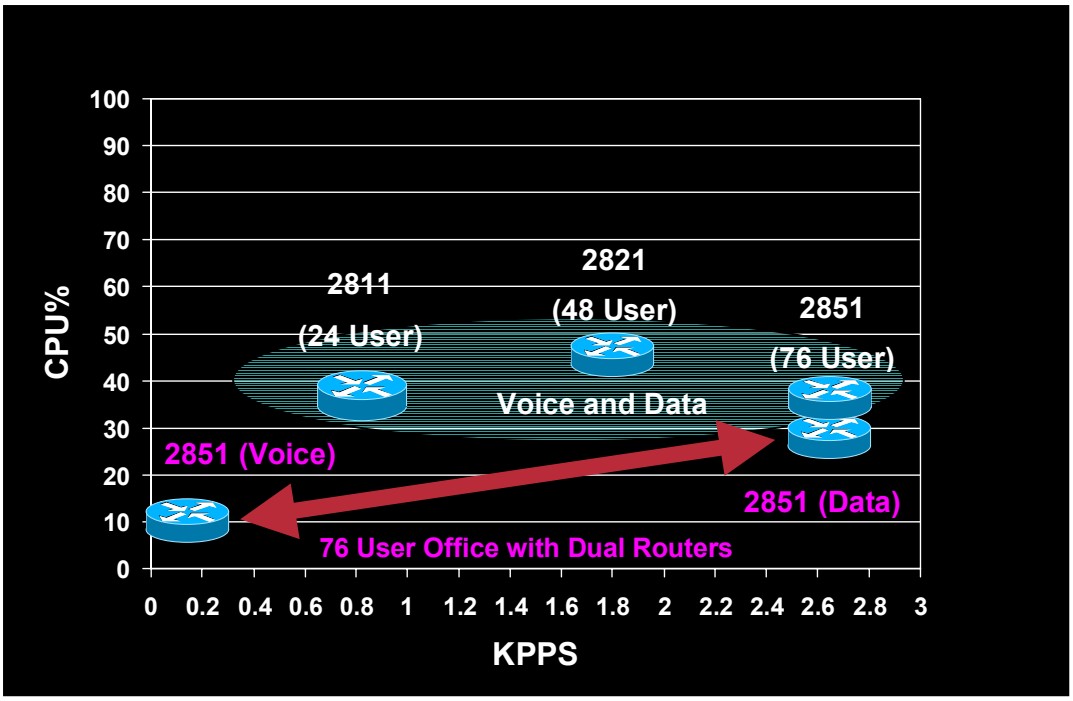


Figure 10 - CPU and PPS Performance