Detailed Lab Report

CISCO INTEGRATED SERVICES ROUTER GENERATION 2

October 2009

Contents

Introduction

Cisco engaged Miercom to conduct independent third party performance testing and Cisco IOS feature validation on the Cisco Integrated Services Router Generation 2 platforms in branch office scenarios. The objective was to validate the increased levels of service integration with voice, video, security, wireless, mobility and data services. Our task was to test the features and services offered by the ISR G2 Branch routers while observing if these activated services affected performance and throughput values.

The branch routers of today need to be able to serve the needs of current branch offices and at the same time, scale to the needs of evolving and integrated branch needs. This involves meeting increased bandwidth requirements, supporting advanced security features and future WAN and VPN technologies with rich multi-media collaboration. A solution that provides security, wireless capabilities, unified communications, and WAN optimization all in one single box, while maintaining existing performance and throughput metrics is the true integrated solution. The Cisco ISR G2 platforms-Cisco 1941W, Cisco 2911, Cisco 2951 and Cisco 3945 platforms are able to deliver these services and performance metrics while deployed in branch office topologies scaling from small branch offices to large remote branches.

Executive Summary

Miercom was engaged by Cisco Systems, Inc. to evaluate the performance characteristics and validate integrated features of the Cisco ISR G2 platforms – 1941W, 2911, 2951, and 3945. All tests were conducted in feature intensive branch office deployments, taking into consideration actual branch settings deployed by current ISR customers.

The ISR G2 platforms are architected to enable the next phase of branch-office evolution enabling richer media experience with video, voice and WAN evolution. Adding to the breadth of integrated services available on the Cisco ISR G2 platforms such as integrated security, unified communication, wireless, and application optimization services, the Cisco ISR G2 platforms further reduces branch office expenses with the introduction of pay as you grow software licensing and simplified Cisco IOS software packaging. The evolving branch of the future is going to be driven by economic challenges to deliver better methods of communication and collaboration for less. The new ISR G2 platforms build on the previous generation ISR platforms to integrate multiple services into a single cost-effective and easily manageable platform for a truly integrated branch experience

This report provides results, which were used to qualify the Cisco ISR G2 platforms as "Performance Verified'.

Summary of Findings

- Cisco ISR G2 platforms with integrated services, delivered throughput exceeding branch bandwidth requirements, and delivered 5X times performance compared to previous generation ISRs

- The Cisco ISR G2 routers displayed exceptional integrated security countermeasures and resiliency. The Cisco ISR routers were subjected to attacks as a standalone appliance, without any other security device and with an un-tuned IOS IPS in use.

- Cisco ISR G2 platforms offer 'Services Ready Engine' providing the flexibility to turn on services on demand, by decoupling the hardware and software.

- The subscription based Cisco IOS Content Filtering, available on the 1941W and 2911 demonstrated category blocking to static black-and-white lists with keyword blocking and security ratings to websites requested. Since the URL database is not saved on the router, it is not restricted by the router memory. With this IOS access feature available at the router itself, additional devices are not required for content filtering functions.

- The Cisco ISR G2 platforms demonstrated SIP trunking capabilities with Cisco Unified Border Element in branch offices. It supported 30 simultaneous calls– regardless of branch size, which is more than typically needed.

- The UC (Unified Communications) Trusted firewall and TRP (Trusted Relay Point) was shown to securely support voice media traffic and unified communications. By effectively proving the Zone Based Policy Firewall for TRP enabled phones, Cisco ISR G2 platforms have a competitive edge in the market for providing secure UC.

- Call processing redundancy at the branch offices is critical. The Cisco SRST (Survivable Remote Site Telephony) function embedded in the Cisco IOS software demonstrated survivability of telephony services at the branch office when the access to the corporate network failed due to WAN link failure.

- The Cisco ISR G2 platforms demonstrated voice and video call capabilities supporting H.263, H.264 and H.323 codec. The Cisco FXO interface on the ISR 2911 allowed calls to be made between branch IP phones and PSTN phones.

- Cisco ISR G2 platforms support bandwidth-optimized and scalable video including Telepresence, media rich video-conferencing and desktop video streaming.

- The Cisco 3G Wireless WAN HWIC (High-Speed WAN Interface Card) on the ISR 1941W combines, advanced IP services and security with the mobility capabilities of 3G WAN access. Testing revealed failover time to 3G WWAN link to be 15 seconds which included time for EzVPN tunnel to establish and pings to reply.

- The Cisco ISR 1941W provides secure, manageable WLANs for branch offices, with fast secure mobility, authentication and simplified management and configuration. The Cisco ISR 1941W meets WLAN needs with a single device offering native 802.11n access point and security features such WPA/WPA2, IEEE 802.1x with Cisco Light Extensible Authentication Protocol (LEAP) and Protected EAP (PEAP) and encryption with WPA Temporal Key Integrity Protocol (TKIP).

- WAN optimization provides optimal performance for applications delivered from a central data center to branch office users. Testing revealed 100 times drop in WAN bandwidth usage for HTTP traffic.

- The Cisco MGF (Multi Gigabit Fabric) allows high bandwidth module-to-module communication at speeds up to 1Gbps without adding overhead to the processor. The traffic between service modules is switched at line rate to one another without being forwarded to the router CPU.

- When populated with RPS (Redundant Power Supply) the Cisco ISR G2 platforms can operate in POE boost mode instead of redundant power supply

mode, offering almost twice the normal power to support additional PoE ports. The Cisco 3945 demonstrated an increase from 520W to 1000W of available power with POE boost.

- A successful demonstration of Cisco EnergyWise technology slots and interface power management was shown using “time policies” for power shut downs at specific predetermined times for the ISR G2 platforms. By setting a power management policy on ISR G2 to turn off ports of the Service Modules for 12 hours during non-operational hours (7.00 PM-7.00 AM), Cisco EnergyWise enables energy savings of 50%.

Branch Architectures

The various branch office scenarios along with performance metrics, services, features and recommended Cisco ISR G2 branch office router deployments are described below.

Table 1: Description of branch office deployment scenarios and features applied

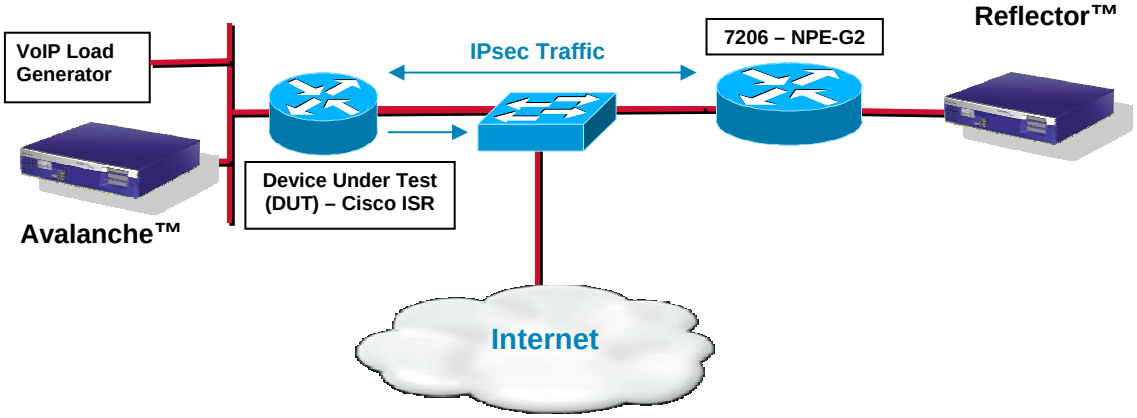
	Small Branch	**Medium Branch**	**Large Branch**	**Regional Office**
Typical Example	Retail store	Bank Branch	Corporate Branch	Regional Office, Large Store
Number of Users	10-25	25-40	40-75	75-150
Link Speed	25Mbps	35Mbps	75Mbps	150Mbps
Typical NG ISR	***1941W***	***2911***	***2951***	***3945***
Configuration Method	USB Console	USB Console	USB Console	USB Console
Feature Licenses	Data, Security	Data, UC, Security	Data, UC, Security	Data, UC, Security
Primary Connectivity	Ethernet WAN	Ethernet WAN	Ethernet WAN	Ethernet WAN
Backup Connectivity	3G WAN	Ethernet WAN	Ethernet WAN	Ethernet WAN
Integrated Switch Ports	8 ports PoE	16 ports PoE	24 ports PoE	48 ports PoE
QoS	5 Class HQoS	5 Class HQoS	5 Class HQoS	5 Class HQoS
VPN	DMVPN	DMVPN	DMVPN	DMVPN
Firewall	Zone-Based FW	Zone-Based FW	Zone-Based FW	Zone-Based FW
Intrusion Prevention	Yes	Yes	Yes	Yes
Content Filtering	Yes	Yes	No	No
WAN Acceleration	No	Yes	Yes	Yes
Local Voice Features	NA	CME-as-SRST TDM PSTN (FXO) Video Telephony	CME CUE VM/IVR SIP Trunk for PSTN	SRST CUBE + SIP Trunk for PSTN
IP Phones	8	12	50	120
Telepresence	No	1 low bandwidth	1 high bandwidth	1 high bandwidth
802.11n Wireless	Corporate & Guest SSID	No	No	No

The branch offices have been categorized into small, medium and large categories with unique requirements for each size office. The configurations shown above represent feature intensive branch deployments today and are likely to be closer to the norm in the future. All testing and test cases described in this document was conducted based on the branch office requirements for the respective Cisco ISR G2 routers

Note: These scenarios were selected after surveying current ISR customers and reflect actual branch office deployments. Performance and scalability numbers used here are not the maximums for any current or future generations of Cisco ISR. The values and features selected for inclusion here are used because they represent levels that many customers are interested in deploying.

How We Did It

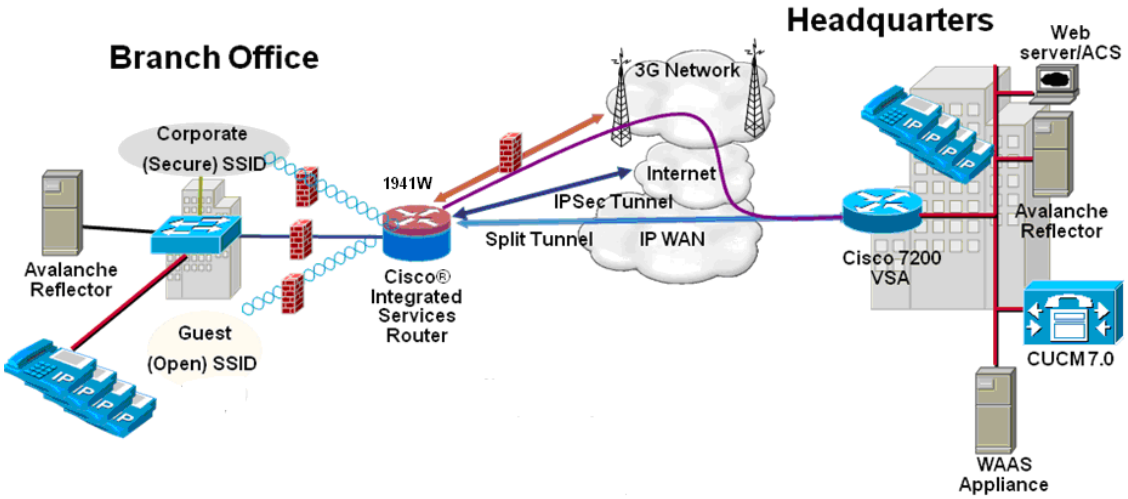
Similar network topologies were used for all tests with small variations added to meet the requirements of different branch sizes. Spirent TestCenter, Spirent Avalanche and Reflector were utilized to generate data traffic. Spirent Abacus was used to generate voice traffic and simulate SCCP call activity. Since there isn't any available standard test tool to simulate Telepresence sessions, a custom Cisco traffic generation tool was used. This tool sends actual Telepresence video streams, monitors for any frame loss, jitter, and latency. All traffic used for performance testing of the Cisco ISR G2 SUT were set to meet SLAs of zero frame loss and acceptable latency or jitter values. The WAN interface of the ISR G2 DUT utilized a secure VPN connection as well as a backup connection specific to the size of the branch. For our tests, the headquarters location was represented by a Cisco 7200 Series router, terminating the other side of the VPN connection providing the core side connections for traffic generation and monitoring.



To simulate the various streams found in a typical branch setting, generic stateful HTTP data traffic consisting of 25-, 30- and 130-Kbyte objects, with 10 objects per TCP session was utilized. This matches typical branch protocol traffic patterns. All performance testing was conducted with router CPU maintained in the 50-70% utilization range, which also is the typical recommended load to allow sufficient overhead and tolerance for real world network activity.

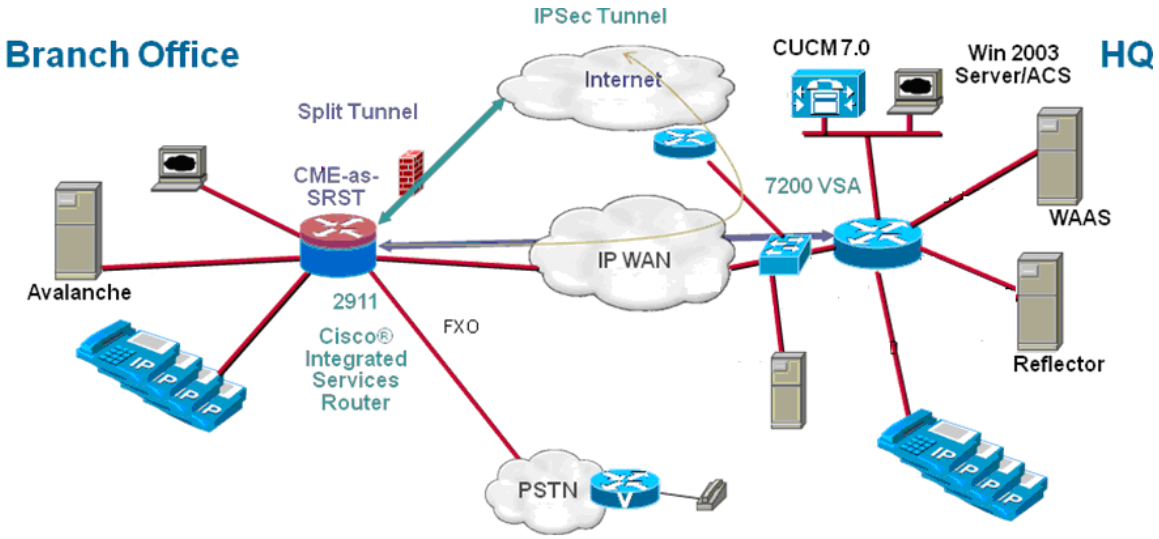
To evaluate the effectiveness of the security features of the Cisco ISR G2 platforms, offensive security tests were conducted using the Mu Test Suite.

Small Branch Office Cisco ISR 1941W Platform



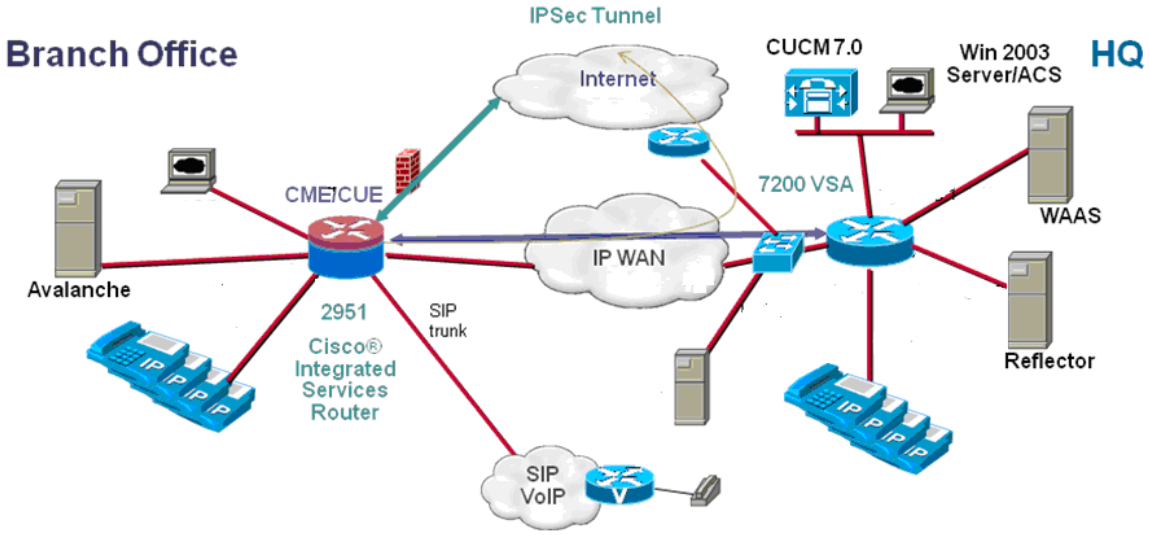
To simulate a small branch office, the Cisco ISR 1941W was configured as a branch router serving a dozen employees. Primary network connectivity was established via a public internet connection with a DMVPN (Dynamic Multipoint Virtual Private Network) encrypted link to corporate headquarters. A 3G wireless data connection was setup for branch redundancy in the event of a primary WAN link failure. The Cisco ISR 1941W was also configured to support wireless utilizing 802.11n radio to extend the corporate wireless network into the branch office as well as provide guest network connectivity for visitors to the office. Security features – Zone Based Firewall, Cisco IOS IPS and content filtering were activated. The Voice services were provided by a headquarters-based CUCM (Cisco Unified Communications Manager).

Medium Branch Office Cisco ISR 2911 Platform



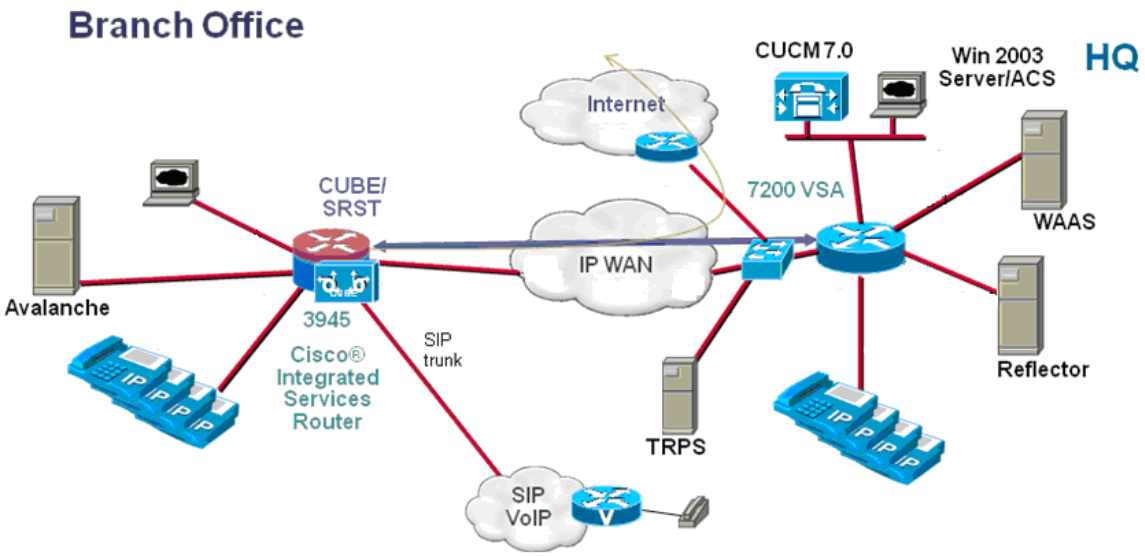
A medium branch office deployment was simulated using a Cisco ISR 2911. This branch scenario supports about 25 users. Primary and backup network connections were to be provided by two separate Ethernet WAN links. An IP WAN provided primary network connectivity with a DMVPN secure connection serving as backup to corporate headquarters. Security features – Zone Based Firewall, Cisco IOS IPS were activated. Voice services were provided by a headquarters-based CUCM with local POTS (Plain Old Telephone Service) access from the Cisco ISR 2911. Cisco Unified SRST (Survivable Remote Site Telephony) was supported to provide redundant local call control in the branch offices in the event the central CUCM is unreachable. Telepresence and video are also supported and enabled for this deployment.

Large Branch Office Cisco ISR 2951 Platform



A large branch with 40 to 60 users was created using a Cisco ISR 2951. In this scenario, the 2951 was configured to provide both primary and backup corporate access via an IP WAN connection as the primary connection to the headquarters and a public Internet connection with a DMVPN secure connection acting as backup. In this scenario the 2951 was configured to support all voice functions including Cisco Unified Communications Manager Express (CUCME) for call control and voice-mail with Cisco Unity Express. Local PSTN access is provided by a SIP trunk from the 2951 to the local phone network. Zone Based Firewall, Cisco IOS IPS and Cisco WAAS were also activated in the router.

Regional Branch Office Cisco ISR 3945 Platform



A large regional office with 150 or more employees was simulated with a Cisco 3945. Primary and backup connectivity to the headquarters was provided with redundant IP WAN connections. The 3945 was configured to support CUBE (Cisco Unified Border Element) functionality for call control in conjunction with a CUCM at corporate headquarters. SRST functionality was also enabled at the 3945 in the event that connectivity with the central CUCM is lost. Local PSTN access was provided by a SIP trunk to the local telephone network. Zone Based Firewall, Cisco IOS IPS and Cisco WAAS were also activated in the router.

ISR Branch Router Performance Test

Description

To measure and record throughput and performance values for various categories of branch router deployments with integrated features such as, DMVPN, ZBF, IPS and HQOS (Hierarchical Quality of Service) enabled. When these features are activated additional resources are required to perform deep packet inspection, stateful filtering, IPsec and crypto, increasing CPU utilization, which might cause reduced throughput. Our goal for this test case was to subject the Cisco ISR G2 routers platforms to their recommended branch settings with integrated services and features enabled (See Table 1) and observe the throughput achieved.

Testing tools

Spirent Avalanche and Reflector were used to generate HTTP traffic. Spirent Abacus was used generate voice calls. Cisco Telepresence tool VSSA (Video SLA Assessment Agent) was used to generate actual TelePresence video streams.

Test

The Spirent Avalanche and Reflector were used to generate stateful HTTP 25-, 30- and 130- Kbyte Object with 10 objects per TCP session. The traffic profile was adjusted so that the router's CPU would not exceed more than 75%. This setting allows sufficient overhead and tolerance for real world network activity and accommodates periodic fluctuations in router load similar to router table convergence. Full availability of services with zero frame loss, acceptable jitter and latency values were maintained. The Spirent Abacus was used to simulate voice calls and SIP/SCCP call activity using standard G.711 codec. The VSSA was used to add TelePresence traffic to the mix. This Cisco TelePresence tool sends actual video streams consisting of 5 minutes of H.264 video streams, iterated for longer durations. The CTS 3000 (Cisco TelePresence System 3000) profile was used and simulated by multiplexing 3 single profiles. This is the recommended model for business meetings and supports up to 6 participants per room.

Cisco ISR 1941W was subjected to a traffic mix consisting of only data traffic from the Spirent Avalanche as recommended for small branch deployment.

Cisco ISR 2911 was subjected to a traffic mix consisting of data and voice traffic as recommended for medium branch deployment.

Cisco ISR 2951 was subjected to a traffic mix consisting of data, voice and TelePresence traffic as recommended for large branch deployment.

Cisco ISR 3945 was subjected to a traffic mix consisting of data, voice and TelePresence traffic as recommended for regional branch deployment.

The IOS integrated services DMVPN, ZBP, IOS IPS and HQoS were enabled for all routers under test and the throughput, CPU utilization and session information were recorded.

Observation

Table 2: Performance test results

	Small Branch	Medium Branch	Large Branch	Regional Office
Device Under Test	***1941W***	***2911***	***2951***	***3945***
Observed CPU Load	*74%*	*75%*	*73-75%*	*74%*
Observed Data Bandwidth	*54Mbps*	*54.15Mbps*	*98.06Mbps*	*136Mbps*
Observed Voice Bandwidth	*NA*	*2.85Mbps*	*2.42Mbps*	*2.5Mbps*
Observed Telepresence Bandwidth	*NA*	*NA*	*14.52Mbps*	*14Mbps*
Total Observed Bandwidth	*54Mbps*	*57Mbps*	*115Mbps*	*153Mbps*
Target Positioning Bandwidth	*25Mbps*	*35Mbps*	*75Mbps*	*150Mbps*

The Cisco ISR G2 branch routers-1941W, 2911, 2951, 3945 delivered performance and throughput values greater than the target positioning bandwidth requirements while integrated services and features were activated. All test results were observed without any frame loss and maintaining CPU utilization of 75%.

Offensive Security Assessment

Description

Evaluate the effectiveness of the integrated security features, offered by the Cisco ISR G2 routers. These security features include IPS (Intrusion Prevention System), ZBF (Zone Based Policy Firewall) and DMVPN (Dynamic Multipoint Virtual Private Network).

Test tools

Mu Test Suite

Test

The Cisco ISR G2 router models 1941W, 2911, 2951 and 3945 were penetration tested with over 1,450 current and in-the-wild attacks and exploits using Mu Dynamics PVA (Published Vulnerability Attack) test suite. The Mu Dynamics test suite maintains a database of attack signatures for published vulnerabilities, updating the database as new vulnerabilities are released in the security community. We used these signatures for published vulnerability attacks to find faults and gaps in IPS and firewall protection capabilities. All the Cisco ISR G2 routers under test were loaded with the latest version of Cisco's advanced signature set. The results obtained reflect standalone assessment of the router's thwarting capabilities and un-tuned deployment of the IOS IPS. Each Cisco ISR G2 router was evaluated with a total of 2,670 signatures loaded on the box.

Observations

- The Cisco ISR G2 platforms loaded with 2,670 signatures thwarted 55.5% of the attacks. The IOS IPS responded and fired signatures before the network security could be compromised.
- Zone based policy firewall proved to be resilient against network and application layer attacks, viruses and worms and added more flexibility and granularity to already existing IOS stateful inspection. Different inspection policies can be applied to multiple host groups connected to the same router interface.
- Evasive actions/protective options available included dropping offending packets, blocking an attacker or dropping the connection.

The Cisco ISR G2 routers displayed sophisticated security countermeasures and resiliency for branch office deployments. The routers integrated security features proved impressive, thwarting more than half of the attacks. It is important to note that the Mu Dynamics PVA test suite used is one of the most comprehensive and advanced set of published vulnerability attacks and the Cisco ISR G2 routers were subjected to these as a standalone appliance, without additional protection from other security devices and with an un-tuned IOS IPS. Tuning the IOS IPS to a customer network deployment would typically increase the blocking rate of the IPS.

Cisco IOS Software Licensing and Packaging

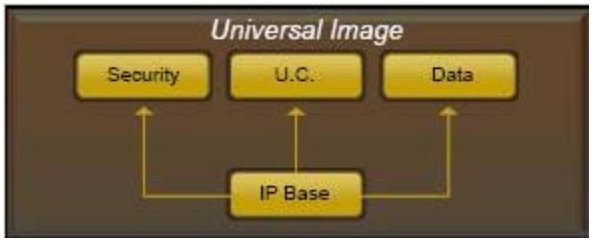
Product Information

Cisco's roll out of the Cisco ISR G2 routers also introduces a new licensing and packaging scheme for the Cisco IOS software. The packaging and licensing of the Cisco IOS software was demonstrated using a Cisco ISR 2951 router. Many customers might order their Cisco ISR G2 branch routers with pre-installed software, including feature package licenses, as well as default configurations that will allow quick deployment of new branch routers. For this demonstration we assumed that the router was delivered with only default options enabled and without configuration of software or features.

All Cisco ISR G2 platforms are shipped with a single universal IOS image. This universal image is loaded during manufacturing and contains all IOS features. All integrated service and features are now in four suites; previously offered in eight images and required a new software image every time.

The level of IOS functionality available depends on the licenses purchased. To unlock or upgrade to a suite of IOS functionality, only a new license needs to be applied.
The four categories for which licenses are divided are:

- IP base: Default packaging
- Data
- Unified Communications
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)



Cisco software licenses currently available are:

Permanent License
Permanent licenses are valid for the life of the device. These include IOS technology packages – IP Base, UC, Data and Security, and feature licenses for CME, CUBE.

Counted License
Counted licenses have a defined number of users. These include CME user licenses.

Subscription License
Subscription licenses are for a predetermined time period or a term. These include URL filtering and IPS.

Temporary License
Temporary licenses are for a specific period - generally a 60-day trial period. An End-User License Agreement must be accepted before being activated.

Cisco IOS Content Filtering

Description

Cisco IOS Content Filtering feature was demonstrated on Cisco ISR 1941W and 2911 platforms. It utilizes a subscription-based service provided by Trend Micro Inc.

Configurable parameters include keyword blocking, local black-and-white listing of up to 100 URLs, blocking by categories and website reputation checking. Management was provided through Cisco Configuration Professional application, which allows configuration of up to 5 routers simultaneously using a GUI interface with the same functionality as the CLI.

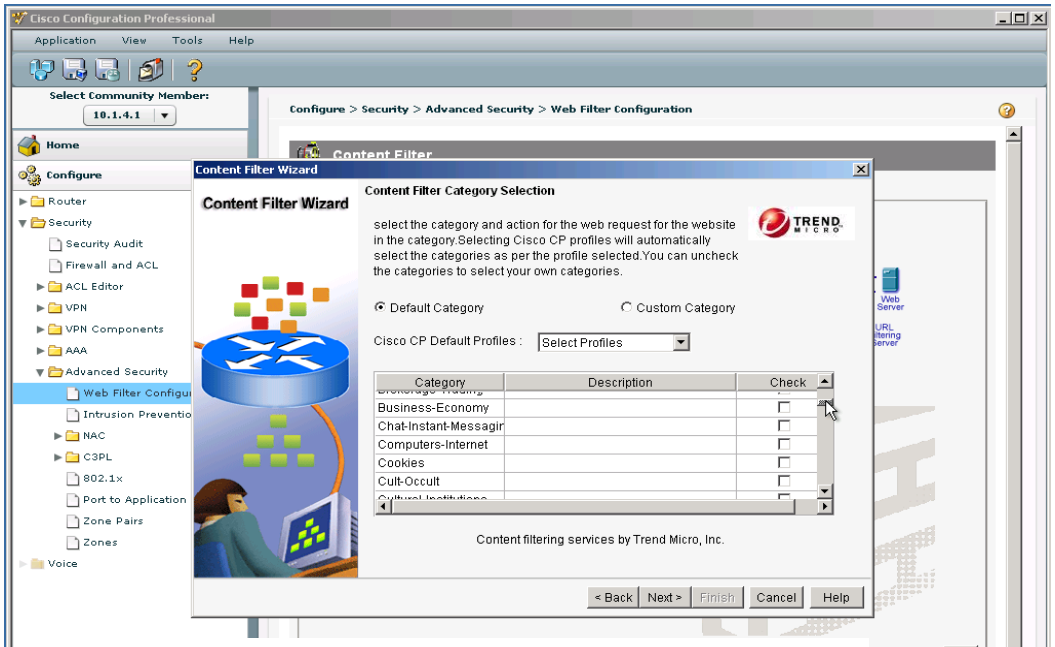
Demonstration

Ease of filter configuration using CCP wizard was demonstrated. Cisco CP Default Profiles which select filtering categories based on application were demonstrated, as well as granular select/deselect of categories within these profiles. Default local action to take when content filtering server is not available was also shown.

Filter policy was configured to block www.facebook.com.

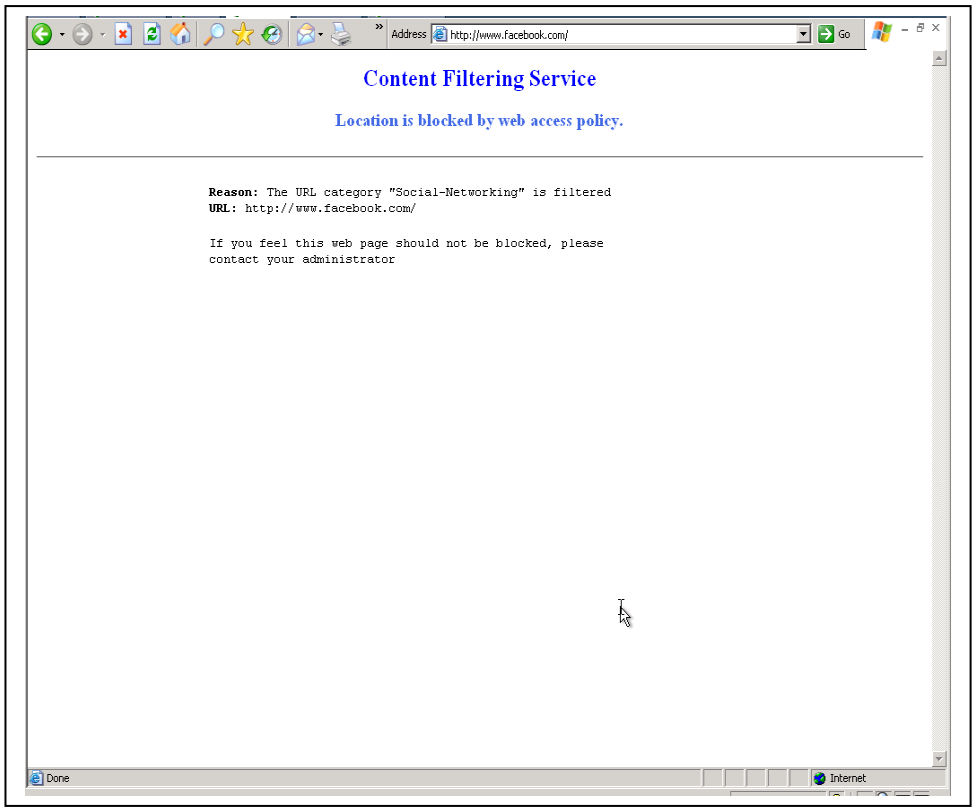
An attempt to navigate to Facebook was successfully denied, and logged on the console. If a Syslog server is available, the log of denied attempt will be sent there. Cisco IOS Content Filtering is a scalable solution and does not require per user licenses.

Figure 1: Content Filter Wizard



The wizard provides selection of default profiles, or easy customization of categories to fit specific business needs.

Figure 2: Content Filter URL blocking by category



URL category blocking message as displayed in user's Web browser.

The subscription based Cisco IOS Content Filtering, available on the 1941W and 2911 demonstrated category blocking to static black-and-white lists with keyword blocking and security ratings to requested websites. Since the URL database is not on the router, it is not restricted by the memory capacity of the router. With this feature accessible from the router, additional devices are not required to perform content filtering functions.

UC trusted Firewall

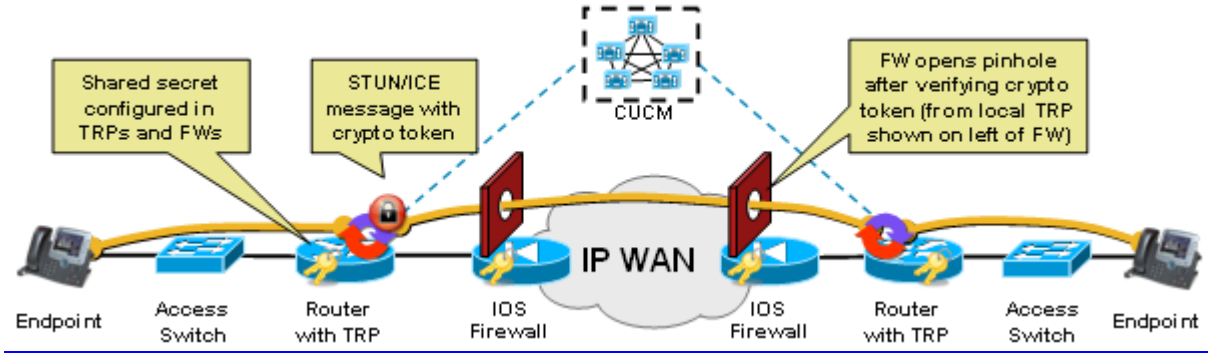
Description

The UC Trusted Firewall feature was evaluated for providing secure Unified Communication. The validation scenario incorporated wired phones (Voice, VLAN), wired PCs and wireless devices including VoIP. The UC trusted Firewall was deployed with TRP (Trusted Relay Points). The TRP is a software function that runs on Cisco network devices and controlled by Cisco Unified Communications Manager.

STUN (Simple Traversal of UDP) Authentication and Pinhole Connection

Only TRP authorized flows were allowed through the firewall. The TRP Inspected the STUN messages for authentication by checking agent id, verifying the shared secret and validating candidate address information. Only after all checks succeed, the STUN message is treated as authenticated and a bidirectional pinhole is opened in the firewall.

The Deploying topology used for this validation is shown below:



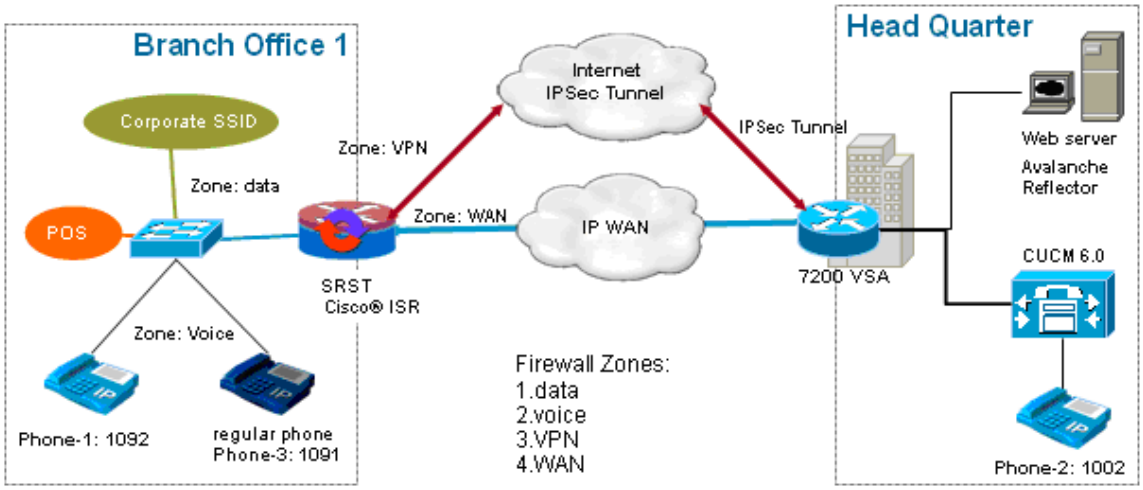
In the diagram above, IOS Firewall and TRP are deployed in two different routers to explain the functionality. Generally, a customer deploys the IOS firewall and TRP in the same router.

Demonstration

Zone Based Policy Firewall for TRP enabled secure phone

This feature was validated for Zone based policy for voice in the IOS firewall and its ability to block rogue phones registered with the CUCM (Cisco Unified Communications Manager) from placing calls to an unauthorized network.

The deploying topology used for this validation is shown below:

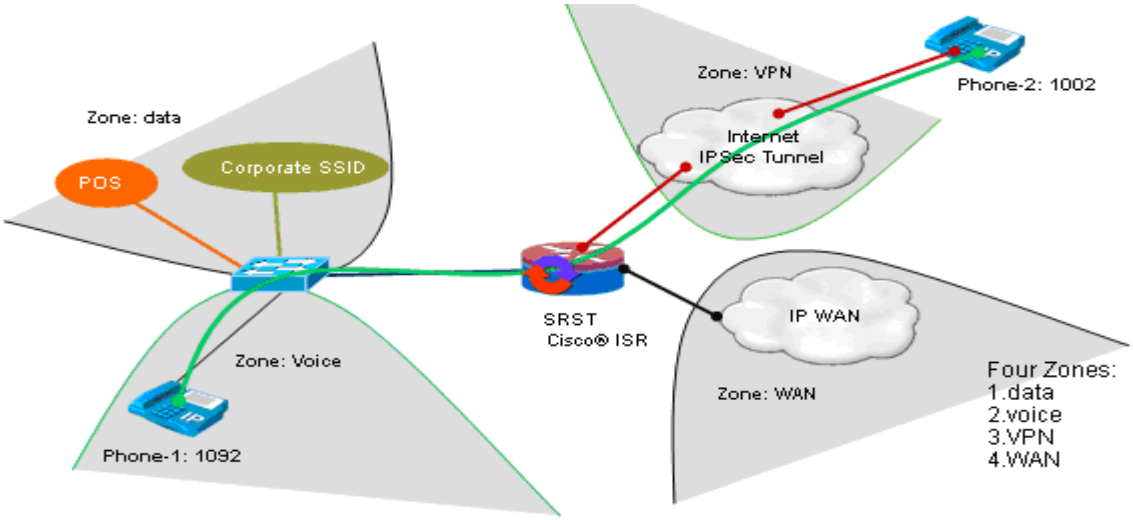


When an interface is a member of a security zone, all traffic to and from that interface is dropped unless a policy is placed to permit traffic.

Phone 1 is a TRP enabled secure phone at the branch office and registered with the CUCM. Phone 2 located at headquarters is also registered to the same CUCM. The ISR G2 router is configured with zone based policy firewall to allow traffic between voice and VPN zones.

Observation

Figure 3: Call Flow for a valid TRP enabled phone



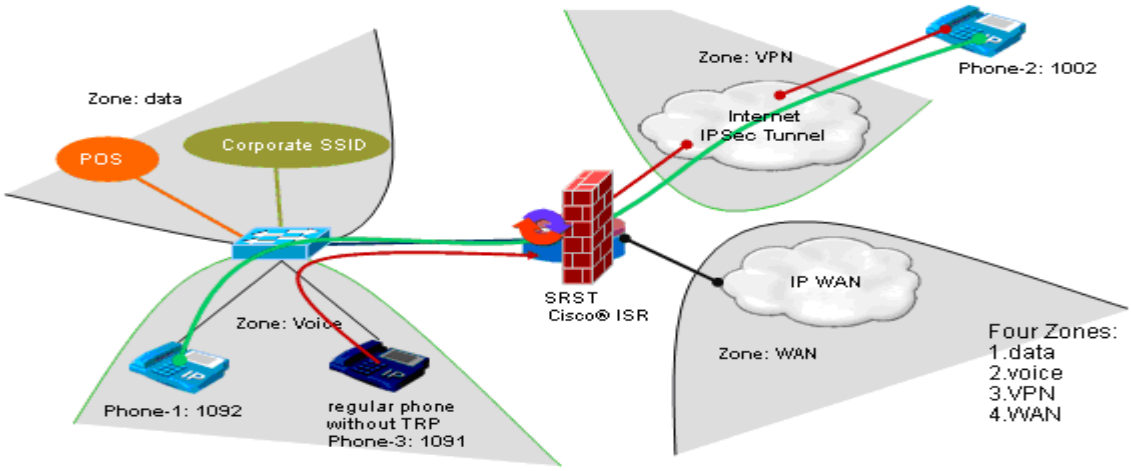
- Phone 1 makes a call to phone 2
- CUCM triggers the TRP associated with phone 1
- IOS firewall opens the pinhole for RTP packets based on STUN-ICE negotiation and media flows

Figure 4:

```
policy exists on zp self-VPN
 Zone-pair: self-VPN

  Service-policy inspect : self-VPN-pmap

    Class-map: skinny-cmap (match-any)
      Match: access-group name skinny-port-list
        0 packets, 0 bytes
        30 second rate 0 bps

   Inspect

      Number of Established Sessions = 3
      Established Sessions
        Session 86BB1FC0 (10.1.122.1:64375)=>(10.1.1.5:2000) skinny:tcp SIS_OPEN
          Created 01:42:57, Last heard 00:00:26
          Bytes sent (initiator:responder) [3244:4460]
        Session 873F5980 (10.1.122.1:18310)=>(10.1.120.4:28178) skinny-RTP-data:
udp SIS_OPEN
          Created 00:00:50, Last heard 00:00:00
          Bytes sent (initiator:responder) [443404:442992]
        Session 873F5F80 (10.1.122.1:18022)=>(10.1.122.2:20336) skinny-RTP-data:
udp SIS_OPEN
          Created 00:00:50, Last heard 00:00:00
          Bytes sent (initiator:responder) [443168:0]
```

Above is the log file showing RTP port assigned and successful call.

Figure 5: Call flow for an invalid phone



- We bring in phone 3 which is not TRP enabled and try to make a call to phone 2 at headquarters
- The signaling is observed and the phone rings
- The IOS firewall does not open pinhole for RTP packets and voice traffic was not allowed to flow through to phone 2

Figure 6:

```
policy exists on zp self-VPN
 Zone-pair: self-VPN

  Service-policy inspect : self-VPN-pmap

    Class-map: skinny-cmap (match-any)
      Match: access-group name skinny-port-list
        0 packets, 0 bytes
        30 second rate 0 bps

   Inspect

      Number of Established Sessions = 1
      Established Sessions
        Session 86BB1FC0 (10.1.122.1:64375)=>(10.1.1.5:2000) skinny:tcp SIS_OPEN
          Created 01:52:45, Last heard 00:00:15
          Bytes sent (initiator:responder) [3484:4812]
```

Above is the screenshot of the log file. Here the RTP ports are not assigned for the voice traffic resulting in failed call.

The UC Trusted firewall and TRP securely support voice media traffic and unified communications. There is no need to open ranges of ports for SIP. Cisco has effectively proven that Zone Based Policy Firewall for TRP enables secure phones.

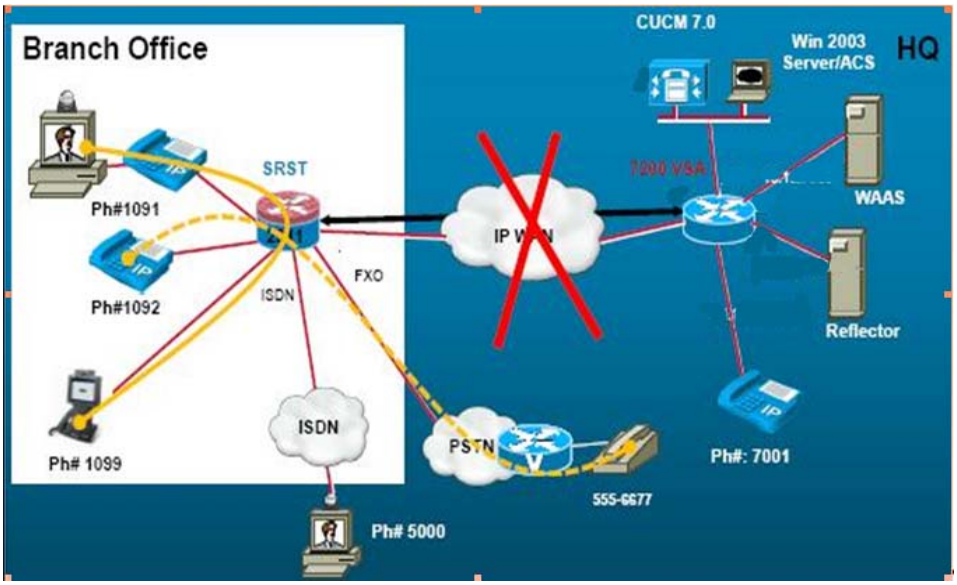
Cisco Unified Survivable Remote Site Telephony

Description

Cisco Unified SRST (Survivable Remote Site Telephony) is a voice feature available on all Cisco IOS platforms. This voice technology was demonstrated on the ISR 2911 medium branch router. When activated, the Cisco Unified SRST acts as a call processing engine for the IP phones located in the branch office during a WAN blackout.

For testing we used two Cisco Unified IP phones on the branch side with call activity confirmed over WAN link from branch to headquarters. Primary WAN network connectivity was established via a public internet connection with a DMVPN (Dynamic Multipoint Virtual Private Network) encrypted link to corporate headquarters.

Figure 7*: *Call processing established at the Cisco ISR 2911 using SRST functionality when WAN link fails and access to Cisco CUCM is denied.



Demonstration

Once the WAN link failed, the Cisco SRST function in the ISR 2911 automatically detected a failure in the network and initiated the SRST services to provide call processing backup for the IP phones at the branch office. Calls were then made between branch IP phones to confirm availability of telephony service while the WAN link was down. Logs from the router indicated that the IP phones were registered. Upon restoration of WAN connectivity, the system automatically shifted call processing back to the primary Cisco Unified Communications Manager at headquarters.

Observation

The Cisco Unified SRST configuration and setup was completed only once, during initial installation. No staff was required at the branch office to manage the Cisco Unified SRST once the WAN link was down.

Call processing redundancy at the branch offices is critical. The Cisco SRST function embedded in the Cisco IOS software demonstrated survivability of telephony services at the branch office when access to the centralized Cisco Unified Communication Manager residing in the corporate network is denied due to WAN link failure.

Cisco ISR 2911 - FXO and Video Capability

Description- FXO

The FXO (Foreign Exchange Office) capabilities and video call capabilities were evaluated on the Cisco ISR 2911. We tested the FXO function by making calls from branch office IP phones to a PSTN phone number. The ISR 2911 supports Cisco FXO interface which is a RJ-11 connector allowing analog connection to be directed to the PSTN central office.

Observation

Calls were placed from branch IP phone to a PSTN number. Good voice quality was observed and no issues were found.

Description-Video

Video capabilities of the Cisco ISR 2911 were assessed with CUVA (Cisco Unified Video Advantage) feature and the enhanced DSP architecture. Using the CUVA feature Cisco Unified IP phone 7965 at the branch could make video calls to other IP video phones. It utilizes CUVA software and a video telephony USB camera. The Cisco High Density Packet Voice Digital Signal Processor Module (PVDM3) slots on the motherboard offer enhanced DSP architecture which accommodates a new packet processing engine optimized for richer voice and video applications. The PVDM3 slots integrate with the Multi Gigabit Fabric for higher IP throughput back to the router architecture.

Observation

Connecting the access port of the video enabled Cisco Unified IP Phone 7965 to a PC with a USB video telephony camera; we placed calls to a video IP phone residing in the branch. The call was made using the familiar phone interface and was displayed successfully with video on the PC without pushing any buttons or clicking a mouse.
The Cisco ISR 2911 under test demonstrated the ability to transmit H.263, H.264 and H.323 codec and make successful video calls. The Cisco FXO interface on the ISR 2911 allowed for calls to be established between branch IP phone clients and PSTN phones.

Fig 8: Video feeds for remote and local user with Cisco CUVA

Cisco ISR 2951 – Cisco Communications Manager Express

Description

The Cisco CME (Communications Manager Express) function was demonstrated on the ISR 2951 to provide call processing services at the branch office. The integrated Cisco CME feature adds call processing functionality for locally attached IP and analog phones at the Cisco ISR G2 branch routers itself for small or branch offices. All the necessary files and configurations for IP phones are stored internally on the appliance, providing a single-platform solution. In addition, this integrated feature offers a robust set of public-switched-telephone-network (PSTN) interfaces, integrated voicemail and Automated Attendant, and a full phone portfolio.

Demonstration

Calls were made using Cisco Unified IP Phones 7965 to test the call processing functionality of the CME. Voice mails were left to demonstrate the messaging features offered by the CME. Using VoiceView express feature we could easily browse, listen, and manage voicemail from the Cisco IP phone display and soft keys.

Observation

The Cisco ISR 2951 delivered integrated IP telephony services including call processing, voicemail and easy voice mail retrieval functionality all in one device. This along with integrated data and security features of the ISR 2951 suitably addresses branch needs in just one box.

Cisco ISR 3945 - SIP Trunking

Description

SIP Trunking capabilities on the Cisco ISR 3945 platform were demonstrated using the Spirent Abacus test suite. For this test scenario the CME on the Cisco ISR 3945 was set and configured, which is the PBX that will interpret the SIP signal and pass the traffic. The service provider side configurations also had to be made and a SIP Proxy server was installed.

Observations

The Spirent Abacus was used to simulate SIP Trunking, generating 30 SIP sessions per second. The following VoIP parameters were recorded for this test:

- No RTP packet loss was reported.
- Stable MOS scores of 4.55 were achieved. Recommended values are 4.0 to 5.0 with 5 as the best.
- There were no out-of-order RTP packets and no late arrivals.
- RTP jitters values of 0.233 msec were observed.
- R-factor of 93.2 was achieved, which falls in the desirable range for VoIP quality.

Cisco ISR 1941W - Wireless LAN

Description

Wireless LAN capabilities were demonstrated for the Cisco ISR 1941W which includes native 802.11n access point in the 1941W and security features available to support secure mobility.

The Cisco ISR 1941W offers an integrated access point in the device itself. This access point is based on the IEEE 802.11n draft 2.0 standard that utilizes MIMO (Multi-Input, Multiple-Output) to improve coverage for both existing 802.11a/b/g and 802.11n clients. The router supports dual radios 802.11b/g/n and 802.11a/n and can operate in autonomous or unified modes.

Demonstration

Testing was conducted on ISR 1941W in HREAP (Hybrid Remote Edge Access Point) mode. This mode allows customers to configure and control access points in a branch office from the corporate headquarters through a WAN link without deploying a controller in each location. The Cisco ISR 1941W access point was configured for two profiles and broadcasted two SSIDs a guest and a corporate. Two PCs were used to simulate these SSIDs. The user associated as guest used a simple 802.11 open association. Also the guest user had internet access with no restrictions on web page content. The WLAN traffic was unencrypted and 802.1X authentication was not required. All access to the corporate network was blocked.

A PC simulating a corporate user required 802.1 X RADIUS authentications, prompting for username/password. Once associated, the user was allowed internet access but was prevented from going out to certain websites based on URL filtering. In this test case the corporate user was prevented from going to gaming and social networking sites. The user could access the corporate network and all WLAN traffic was WPA2/WPA encryption.

Observation

The Cisco ISR 1941W enables deployment of secure, manageable WLANs optimized for branch offices, with fast secure mobility, authentication and simplified management and configuration. These routers help extend corporate networks to secure remote sites while allowing access to the applications found in the corporate offices. The Cisco ISR 1941W successfully meets WLAN needs with a single device, offering native 802.11n access point and combining security features such as WPA/WPA2, IEEE 802.1x with Cisco Light Extensible Authentication Protocol (LEAP) and Protected EAP (PEAP) and encryption with WPA Temporal Key Integrity Protocol (TKIP).

Cisco ISR 1941W - 3G Wireless WAN

Description

The Cisco 3G Wireless WAN HWIC (High-Speed WAN Interface Card) was tested on the Cisco ISR 1941W for primary and backup WAN link connectivity as an integrated feature offering.

The Cisco 3G Wireless WAN HWIC CDMA offers up to 3.2 Mbps downlink and 1.8Mbps uplink. For GSM the 3G HWIC offers up to 7.2 Mbps downlink and 382kbps uplink. The Cisco 3G WWAN HWIC also supports HSPA (High Speed Packet Access) and EVDO (Evolution Data Optimized) and with HSPA they offer up to 7.2 Mbps downlink and 2 Mbps uplink. On the CDMA version two antennae connectors offer diversity, allowing for stronger signal reception in areas where a signal might be poor or otherwise degraded.

Demonstration

The 3G WWAN was tested as primary link with IOS security feature DMVPN (Dynamic Multi point VPN) enabled. Pings were made to confirm connectivity over 3G WAN links from branch to headquarters. To test for multimedia traffic over 3G WAN link we placed voice calls and monitored the MOS scores and call quality. Voice could be heard with clarity, all sessions were maintained and no calls were dropped. 3G WWAN as backup link was tested with IOS security feature EzVPN enabled. The primary WAN link was failed and the time for failover to 3G backup was recorded.

Observation

The Cisco ISR 1941W router failover time to 3G WWAN link was noted to be 15 seconds which included time for EzVPN tunnel to establish and pings to reply.

The Cisco 3G Wireless WAN HWIC on the ISR 1941W successfully combines traditional enterprise router functionality, advanced IP services like VoIP and security with the mobility capabilities of 3G WAN access. This provides a true multipath WAN backup and the ability to rapidly deploy it for primary WAN connectivity.

Wide Area Application Services

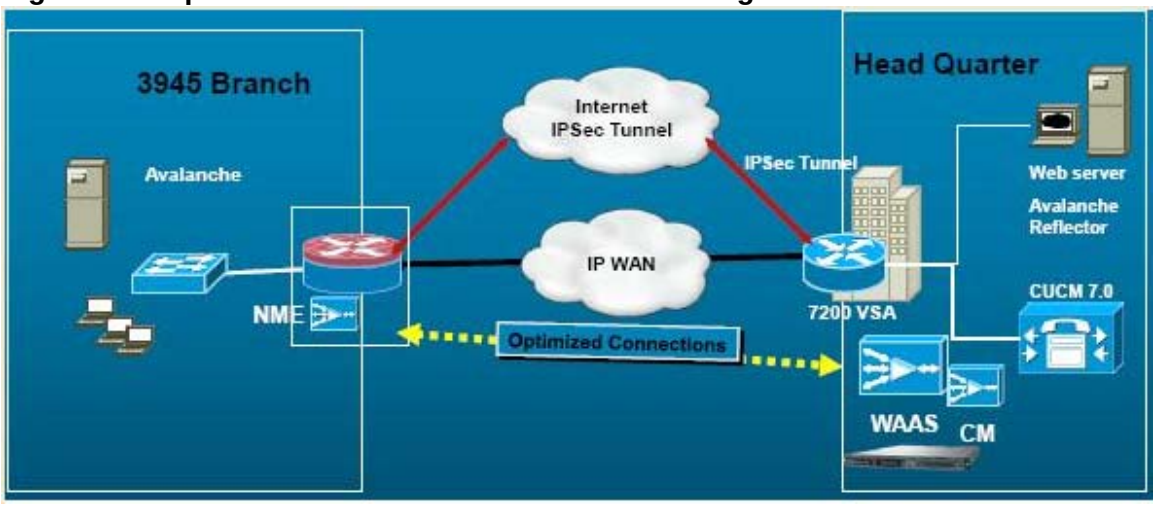
Description

Cisco WAAS (Wide Area Application Services) module, demonstrated on the ISR 2911, 2951 and 3945 provides integrated WAN Optimization features in the ISR G2 platforms. WAN Optimization are capabilities that improve the performance of high speed LAN applications when accessed by lower-speed WANs. Among the WAAS functions demonstrated were advanced data redundancy elimination (DRE), Persistent LZ compression, and TCP flow optimization (TFO), all of which accelerated application response times by alleviating WAN traffic loads and congestion. All these features were implemented by a physically integrated WAAS module in the ISR G2 branch router at the branch office.

The Cisco WAAS module has it own hardware, software, and processing resources dedicated just to perform WAN Optimization functions. The module does not detract from the operation and performance of other networking functions in the ISR G2 router.

We used the Spirent Avalanche to generate real world HTTP traffic to traverse the WAN link to the corporate network and was terminated by the Spirent Reflector. WAAS functions DRE, TFO and Persistent LZ were activated to accelerate application response time. It is important to note these functions are a typical set of features for WAN optimization at the branch.

Fig 9: WAN optimization test with WAAS module integrated with ISR 3945



DRE is an advanced form of network compression that allows Cisco WAAS to maintain a database that has been seen previously on the network. This information is used to remove redundant transmission patterns from the network, minimizing bandwidth usage and offering up to 100:1 compression capability. The Persistent LZ compression can be

used in conjunction with DRE or independently. For our test we included it with DRE. It offers a standard based compression providing 2:1 to 5:1 compression based on data transmitted. TFO provides acceleration for TCP based applications based by overcoming TCP limitations such as inefficient handling of congestion or packet loss resulting from the throughput constraints associated with TCP.

Observations

Testing results revealed that without the WAAS module providing integrated WAN Optimizations features, the bandwidth usage was recorded at 140 Mbps for HTTP traffic. When the ISR G2 router was deployed with the WAAS module, the bandwidth usage for the same HTTP traffic dropped to 1.4 Mbps decreasing the bandwidth usage by a 100 times.

Cisco High Speed Multi Chassis Module Interconnect and Multi Gigabit Fabric

Description

Cisco HIMI (High Speed Multi Chassis Module Interconnect) is a dedicated, point-to-point interconnection from an enhanced NME (Network Module) to another NME. This feature establishes a Layer 2 connection of 1Gbps between the NMEs. For our test case, the ISR 3945 was demonstrated, using the new Cisco Etherswitch Service Modules (ESM). The Cisco ESM is a NME which is optionally available to integrate switch ports within a router. Each module integrates with the MGF (Multi Gigabit Fabric) and has a traditional link to the router CPU. The MGF is a new integrated solution added to the architecture of the ISR G2 platforms allowing high bandwidth module-to-module communication at speeds up to 1Gbps without adding overhead to the router processor. The traffic between service modules is switched at line rate to one another without being forwarded to the router CPU, thereby improving LAN/WAN performance and scalability.

Two 24 port Cisco ESMs were used for testing, with Spirent Avalanche/Reflector used to generate traffic traversing from one Etherswitch module to the other. The objective of this test was to validate the 1Gbps interconnect between NME and as well as to validate the router CPU utilization remained unaffected for traffic flow between the modules.

Observations

From the Cisco ISR 3945 log file we observed the CPU utilization was zero and 1Gbps of traffic was passing through the Etherswitch modules. The receive bandwidth percentage utilization and transmit bandwidth percentage utilization for the port going to the platform CPU recorded zero indicating no router processing power was used.

PoE Boost

Description

Cisco ISR 2911, 2951 and 3945 offer RPS (Redundant Power Supply) options, allowing for power redundancy through an external RPS device, and thereby decreasing network downtime and protecting network from power-supply failures. When populated with dual power supplies, the routers can operate in a PoE boost mode configuration in lieu of redundant power mode. In this PoE boost configuration the power capacity of the platform is increased to almost twice the normal power to support additional PoE ports. Using the following commands on the ISR 3945 we were able to extend the inline power to support more powered devices.

Observations

	RPS Mode	***POE Mode***
Maximum Power	520W	1000W
Allocated Power	6.3W	6.3W

Log Output

```
Miercom-3945 # show power inline
Power Supply   SlotNum.   Maximum   Allocated      Status
-----------    --------   -------   ---------      ------
INT-PS          0         520.000   6.300          PSU1 GOOD   PSU2 GOOD

Interface   Config   Device    Powered    Power Allocated
---------   ------   ------    -------    --------------
Gi1/0       auto     Unknown   On         6.300 Watts
Gi2/0       auto     Unknown   Off        0.000 Watts

Miercom-3945(config)#no power inline redundant
Miercom-3945#show power inline
Power Supply   SlotNum.   Maximum   Allocated      Status
-----------    --------   -------   ---------      ------
INT-PS          0         1000.000  6.300          PSU1 GOOD   PSU2 GOOD

Interface   Config   Device    Powered    Power Allocated
---------   ------   ------    -------    --------------
Gi1/0       auto     Unknown   On         6.300 Watts
Gi2/0       auto     Unknown   Off        0.000 Watts
```

From the log files of the ISR 3945 we can see that before, with RPS in place, the maximum power available was 520W. By disabling the RPS, maximum power available for allocation increased to 1000W.

Cisco EnergyWise

Description

The Cisco Etherswitch Modules are enhanced network modules which are optional for integration of switch ports within a router. These modules expand the capabilities of integrated switching within Cisco routers. Cisco EnergyWise is a new feature added to Cisco Catalyst switches, as well as to the Etherswitch modules to promote green IT.

Cisco EnergyWise technology allows users to measure the power consumption of network infrastructure and network attached devices (IP phones, PC, access points etc.) and manages power consumption with specific settable policies.

This IOS feature was demonstrated on the ISR 3945 platform fitted with two 24 port Etherswitch modules.

Demonstration

Power monitoring and management capabilities of the Cisco EnergyWise feature were tested for slots and interface power management on the router. With Cisco EnergyWise, the Service modules could be powered up or turned down using simple commands.

```
Miercom-3945#hw-module sm 1 EnergyWise level?
  0     SHUT
  10    FULL
 <0-10> Select appropriate level from the list
```

'Time of day' policies were applied to extend EnergyWise functionality to control power to certain ports. Based on this policy, PoE power to interfaces was automated to turn on/off at various times. These time policies could also be applied by device type, device location, priority of device and other settable parameters.

RFC 2544 Performance Test

Description

Cisco ISR G2 routers models 1941W, 2911, 2951 and 3945 were subjected to the RFC 2544 standard test suite to make measurements on IPv4 forwarding, NAT (Network Address Translation) and IPSEC VPN performance.

Test Tools

Spirent Avalanche/Reflector

Test

The testing was conducted in compliance with the RFC 2544 IPv4 standard and with a variety of packet sizes including 64 byte, IMIX and 1518 byte packets. The IMIX profile mix consisted of 64, 594, and 1518 byte Ethernet frames at 58.3%, 33.3% and 8.3% respectively. Tests were repeated for each router under different traffic profiles for each NAT and IPSEC (AES) services activated, separately.

Observation

	RFC2544 Throughput	**Small Branch**	**Medium Branch**	**Large Branch**	**Regional Office**
	Device Under Test	***1941W***	***2911***	***2951***	***3945***
64 byte packets	IPv4 Forwarding (Mbps)	*214.06*	*232.50*	*384.38*	*711.30*
	NAT (Mbps)	*31.24*	*38.28*	*104.38*	*207.02*
	IPSec (AES) (Mbps)	*4.67*	*5.51*	*5.93*	*5.80*
IMIX packets	IPv4 Forwarding (Mbps)	*981.02*	*1017.18*	*1713.90*	*2988.69*
	NAT (Mbps)	*168.52*	*174.26*	*479.72*	*938.82*
	IPSec (AES) (Mbps)	*62.36*	*70.78*	*149.80*	*239.34*
1518 byte packets	IPv4 Forwarding (Mbps)	*2000.00+*	*3000.00+*	*3000.00+*	*3000.00+*
	NAT (Mbps)	*692.18*	*713.28*	*1908.59*	*2000.00+*
	IPSec (AES) (Mbps)	*146.56*	*164.84*	*195.78*	*739.64*