



Cisco ISR 871 Report

A Broadband-Testing Report

First published August 2005 (V1.0)

Published by Broadband-Testing
La Calade, 11700 Moux, Aude, France

Tel : +33 (0)4 68 43 99 70
Fax : +33 (0)4 68 43 99 71
E-mail : info@broadband-testing.co.uk
Internet : [HTTP://www.broadband-testing.co.uk](http://www.broadband-testing.co.uk)

©2005 Broadband-Testing

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors.

Please note that access to or use of this Report is conditioned on the following:

1. The information in this Report is subject to change by Broadband-Testing without notice.
2. The information in this Report, at publication date, is believed by Broadband-Testing to be accurate and reliable, but is not guaranteed. All use of and reliance on this Report are at your sole risk. Broadband-Testing is not liable or responsible for any damages, losses or expenses arising from any error or omission in this Report.
3. *NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY Broadband-Testing. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY Broadband-Testing. IN NO EVENT SHALL Broadband-Testing BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.*
4. This Report does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products, or that the products will meet your expectations, requirements, needs or specifications, or that they will operate without interruption.
5. This Report does not imply any endorsement, sponsorship, affiliation or verification by or with any companies mentioned in this report.
6. All trademarks, service marks, and trade names used in this Report are the trademarks, service marks, and trade names of their respective owners, and no endorsement of, sponsorship of, affiliation with, or involvement in, any of the testing, this Report or Broadband-Testing is implied, nor should it be inferred.

TABLE OF CONTENTS

CISCO ISR 871 REPORT – EXECUTIVE SUMMARY	1
INTRODUCTION: THE ULTIMATE BALANCING ACT – ENTERPRISE FEATURES, HOMEWORKER EASE OF USE... ..	2
ISR 871 – FEATURES AND FUNCTIONALITY OVERVIEW	3
Basic Data Features	4
Quality Of Service (QoS)	5
Configuration And Management	6
Security Features	7
Firewall	8
Inline IPS	8
VPN (Virtual Private Networking)	9
WLAN Security & Management	10
CISCO ISR 871 FEATURE & PERFORMANCE TESTS.....	12
Testbed Basics.....	12
Basic Wireless Clients Tests.....	12
Web Traffic Simulation Tests	13
QoS Test	16
OVERALL SUMMARY.....	17
APPENDIX: THE TEST EQUIPMENT DETAILS.....	18
Spirent Avalanche/Reflector 2500.....	18
CMC Emulation Engine	20

TABLE OF FIGURES

Figure 1 – The Cisco ISR 800 Series	2
Figure 2 – The SMB Scenario	3
Figure 3 – QoS Configuration	5
Figure 4 – SDM 2.1 GUI	6
Figure 5 – Security Audit	7
Figure 6 – Setting Up The Firewall	8
Figure 7 – Configuring The IPS	9
Figure 8 – Configuring A VPN	10
Figure 9 – Configuring WLAN Security Settings	11
Figure 10 – Optimising WLAN Settings	12
Figure 11 – Running A Basic WLAN Connectivity Soak Test	13
Figure 12 – Features Enabled Test	14
Figure 13 – WEP Impact Test	15
Figure 14 – QoS Video Streaming Test	16
Figure 15 – Spirent Avalanche 2500	18
Figure 16 – Creating An Avalanche 2500 Test	19
Figure 17 – The CMC Emulation Engine	20
Figure 18 – The CMC Emulation Engine Main Screen	21

Broadband-Testing

Broadband-Testing is Europe's foremost independent network testing facility and consultancy organisation for broadband and network infrastructure products.

Based in the south of France, Broadband-Testing offers extensive labs, demo and conference facilities. From this base, Broadband-Testing provides a range of specialist IT, networking and development services to vendors and end-user organisations throughout Europe, SEAP and the United States.

Broadband-Testing is an associate of the following:

- *NSS Network Testing Laboratories (specialising in security product testing)*
- *Broadband Vantage (broadband consultancy group)*
- *Limbo Creatives (bespoke software development)*

Broadband-Testing Laboratories are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

Broadband-Testing Laboratories operates an **Approval** scheme which enables products to be short-listed for purchase by end-users, based on their successful approval.

Output from the labs, including detailed research reports, articles and white papers on the latest network-related technologies, are made available free of charge on our web site at [HTTP://www.broadband-testing.co.uk](http://www.broadband-testing.co.uk)

The conference centre in Moux in the south of France is the ideal location for sales training, general seminars and product launches, and Broadband-Testing can also provide technical writing services for sales, marketing and technical documentation, as well as documentation and test-house facilities for product development.

Broadband-Testing Consultancy Services offers a range of network consultancy services including network design, strategy planning, Internet connectivity and product development assistance.



CISCO ISR 871 REPORT – EXECUTIVE SUMMARY

- With its ISR (Integrated Services Router) 800 Series, Cisco is looking to combine enterprise-class feature sets and the ease of use associated with its Linksys entry-level products, to deliver a high-end product to the small/medium business marketplace at an affordable price. This is a tough ask, but our test showed that it is possible to achieve this fine balancing act.
- The 871 is a fully-featured product by any standards – integrated Ethernet switch, WLAN Access Point, routing, VoIP support, a host of security options including VPNs, even Quality of Service provisioning, are all included. Integrated DSL is an option.
- This depth of product features, notably in terms of the security options, is what differentiates it significantly from Cisco's Linksys home/SOHO product range. As such, the price differential between the two product lines is certainly justified.
- The GUI (SDM 2.1) used to manage the ISR 871 is genuinely easy to use, with several wizard-based configuration options making setting up the router relatively easy.
- Whereas other products higher up the ISR range have a wealth of optional extras in addition to the basic product, the 871 has very few which helps make the purchasing and configuration process very simple. This is a good thing, given the target customer.
- The ISR 871 also makes a very strong case for being part of a managed service style offering from a service provider or TelCo. Minimal configuration requirements, and the expected reduction in support requirements as a result, should add up to a highly suitable product for this type of operation.

The Aims Of This Report

Within the scope of this report we're looking to achieve three aims:

1. To examine the feature set of the ISR 871 with a focus on ease of use, flexibility and depth of coverage.
2. To test the capabilities of the ISR 871 to cope with what will be substantially heavier traffic loads than those it would realistically find in the real world, and with multiple features enabled. Fair? No, but this is a test after all.
3. To gauge how easy the ISR 871 is to configure and manage on a day-to-day basis, given its intended target user base – SMB, teleworker – where there is no helpdesk support directly at hand. Equally, in a managed services environment, we need to examine what level of support the service provider is likely to need to offer, in order to keep their customers happy.

INTRODUCTION: THE ULTIMATE BALANCING ACT – ENTERPRISE FEATURES, HOMEWORKER EASE OF USE...

Whichever way you look at it, it sounds like utopia – a marriage of enterprise-class features with the simplicity of design that enables a novice computer user to manage their office router on a daily basis.

But this is the remit Cisco asked of its engineers when designing the ISR (Integrated Services Router) 800 series – to create a fully-featured, industrial strength office router for the average small business or even teleworker to use. So, we are not talking about technical support helpdesk teams on standby here, but users who have just about got the hang of Office 2003. And by fully featured we mean just that – wired and wireless connections, routing between LAN and WAN (Internet), optional integrated DSL, a host of security features...

Another point to consider here is that, while the “paperless” office has never actually come of age, the wireless or at least, near wireless, office does stand a better chance. In a small business or teleworker scenario, the less wires the better is the order of the day. Wires are just one other physical component that can create problems, so by excluding them you exclude those potential failures and the head scratching that goes with them. So, with the ISR 871, Cisco is looking to minimise support requirement, maximise the wireless opportunity and not short-change the user on features. A big ask? Yes, but one that is eminently viable and very much needed in the real world.



Figure 1 – The Cisco ISR 800 Series

The Managed Service Option

The diagram illustrates a managed service architecture. At the center is a cloud labeled "Internet IPsec or MPLS VPN". To the left, a building icon is connected to the cloud by a red line, with a laptop icon and the text "Secure WLAN Service" above it. Below this, a laptop and a server icon are connected to the cloud by a red line, with the text "Secure High Speed Internet Service" below them. In the center, a telephone icon is connected to the cloud by a red line, with the text "VoIP Extensions Service" below it. To the right, two building icons are connected to the cloud by red lines, with the text "IPsec or MPLS VPN Service Between Sites" below them.

One obvious channel for the ISR 871 is to be packaged by service providers or TelCo's in the form of a managed service delivered to the customer including all support and Internet access.

In this scenario, a low cost of ownership is critical if the service provider is to actually make any profit on the deal. Here's where the ISR 871 should score, thanks to the speed with which it can be configured, the ease of use the wizard configuration tools bring, the easily accessed usage statistics and the wealth of security options to prevent unwanted problems.

Basic Data Features

The ISR 871 is a small footprint device – the classic small Cisco router platform for anyone familiar with Cisco products historically – with all the ports on the back of the router and a series of LEDs on the front.

Starting at the back, on the device tested we had a four-port managed 10/100 Ethernet switch – all switch ports can be monitored - and a console port for serial-based access to the management CLI (Command Line Interface) which can also be used as a backup WAN interface using an external modem.

As tested, our 871 had an Ethernet WAN port that we connected to a separate ADSL router, but integral ADSL, ADSL over ISDN and SHDSL modules are all options. The Ethernet switch supports up to three VLANs, with 802.1q VLAN tagging supported. There is also the option of an external PoE adapter for powering IP phones, to avoid individual power supplies or power injectors having to be used.

In addition to the Ethernet ports, there are two USB ports. These are not designed for general-purpose use, but specifically for supporting removable security tokens on USB memory sticks. Also from the back panel, two antennae sprout, providing evidence of the internal WLAN Access Point (AP). The AP supports IEEE 802.11b/g wireless networks and the VLAN support extends to the WLAN.

The ISR 871 has a built-in DHCP server for both wired and wireless clients – essential on this type of product – as well as Dynamic DNS (DDNS). DDNS updates make sure that dynamically assigned IP addresses are

associated with an IP host DNS (Domain Name System) name. This feature enables routers and hosts on the LAN to be accessible via a DNS name.

Quality Of Service (QoS)

For real-time applications such as VoIP, Cisco provides QoS support which can be enabled for outgoing traffic over the WAN link. Bandwidth reservation options for a wide range of protocols, including voice and video (as tested, see later) are available, including class-based Weighted Fair Queuing (CBWFQ), Low Latency Queuing (LLQ), class-based marking, policing and others.

This is not a feature you would expect on a low-end device and another clear sign that Cisco is keen to differentiate its ISR range from the Linksys level products. Both real-time and business critical applications can be allocated guaranteed bandwidth availability/priority settings simply by adding to them from a list of supported protocol types. These can be changed or added to as required, as demands change.

This dynamic configuration of QoS, combined with that of other technologies such as IP Multicast and secure tunneling via VPNs (see next section), optimises latency-sensitive applications such as voice and video while securing them at the same time.

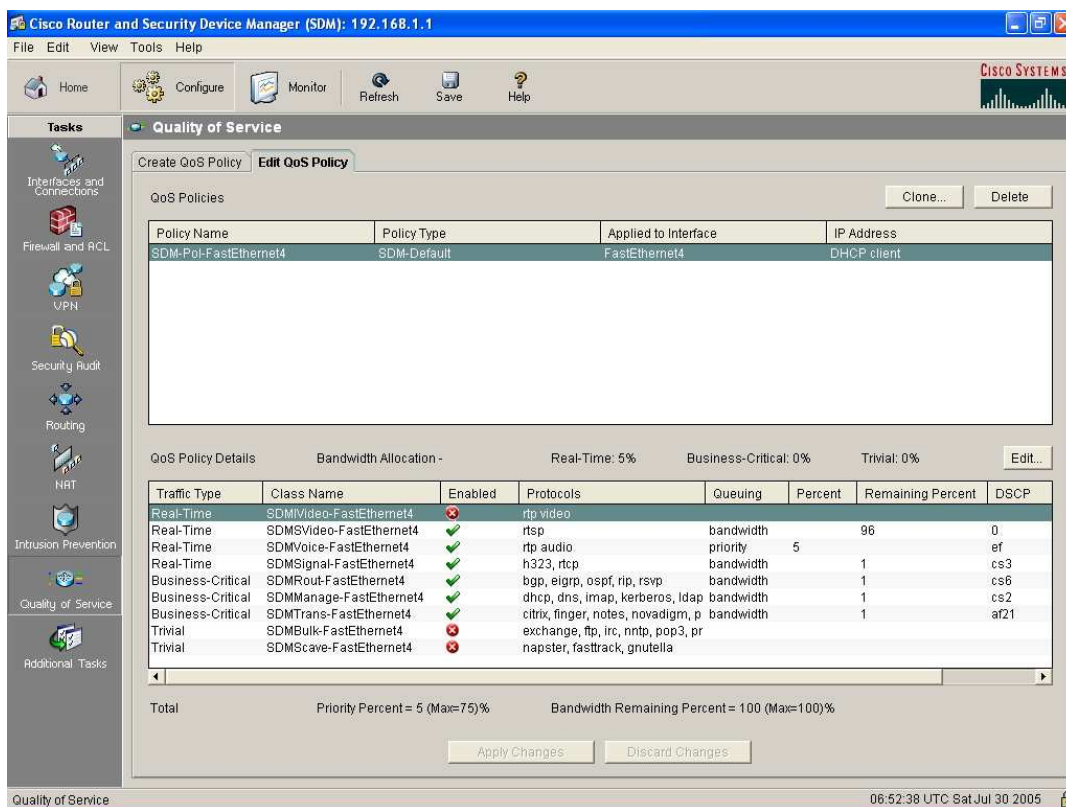


Figure 3 – QoS Configuration

Configuration And Management

As we've already mentioned, the ISR 871 can be configured either via the classic IOS Command Line Interface or CLI (via direct console connection, Telnet or Secure Shell – SSH) or – for most features – via the Cisco Router and Security Device Manager GUI, provided here in SDM 2.1 format.

Most of the basic router functions – configuring the various interfaces, setting up NAT, static routes and similar features – can be set up via the GUI. And it is very easy to use. A home page presents you with a summary of the ISR's configuration and status, using green/red LED simulators to identify the health of the various router components.

A “Configure” option presents a list of feature configuration options: Interfaces and Connections, Firewall and ACL, VPN, Security Audit, Routing, NAT, Intrusion Prevention, Quality of Service and Additional Tasks. A number of wizard options are available to guide you through setting up most of these features. This is a very positive step, compared with Cisco of old, in terms of enabling less specialist users to be able to carry out basic configuration tasks, or at least be easily guided through them via remote support.

A dedicated Monitor section provides a breakdown of statistics across the range of available features enabled on the device. Onscreen statistics are available that show important metrics such as CPU usage so, in the event of a remote support team needing to get a status check on the 871, the information is easily accessed. The device also supports remote, dial-in access at the CLI level, so the ISR 871 is fully supportable locally or remotely, making it ideal for one of the target markets for this product, managed services



Figure 4 – SDM 2.1 GUI

Security Features

A wide range of security features are integrated with the ISR 871, with hardware acceleration provided for VPN and encryption, taking valuable processing requirement off the main CPU. To start with, the 871 has extensive access control options, such as an integrated RADIUS (AAA) server and several WLAN authentication and encryption options, including WEP, WPA, authentication with IEEE 802.1X with Cisco's Extensible Authentication Protocol (LEAP) and Protected EAP (PEAP), and encryption with WPA Temporal Key Integrity Protocol (TKIP). In addition there is a stateful inspection firewall, inline IPS with a 100 strong database of attack signatures, Network Admission Control (NAC), URL filtering and support for MPLS-based VPNs or VPNs using hardware accelerated IPsec AES and 3DES encryption. This is a very complete set of security functions that Cisco can rightly claim to be enterprise-class.

All the security features and other features are configured using either Cisco's CLI or – far preferable for novice users – the truly graphical SDM - Security Device Manager – now in version 2.1 and, an improvement on the slightly ponderous v2.0 we last saw from Cisco. For those feeling paranoid, a one-click option – One-Step Lockdown - enables you to secure the entire network immediately, in the event of a perceived attack or any other emergency state. For a novice user, however, it is not recommended as they might easily lock themselves out of the system. The SDM GUI allows you to configure to ISR, feature by feature. A good starting point is the Security Audit option, which lets you run through a step by step examination of the security state of the ISR, creating a report which allows you to then automatically enable or disable any security features, with recommendations.

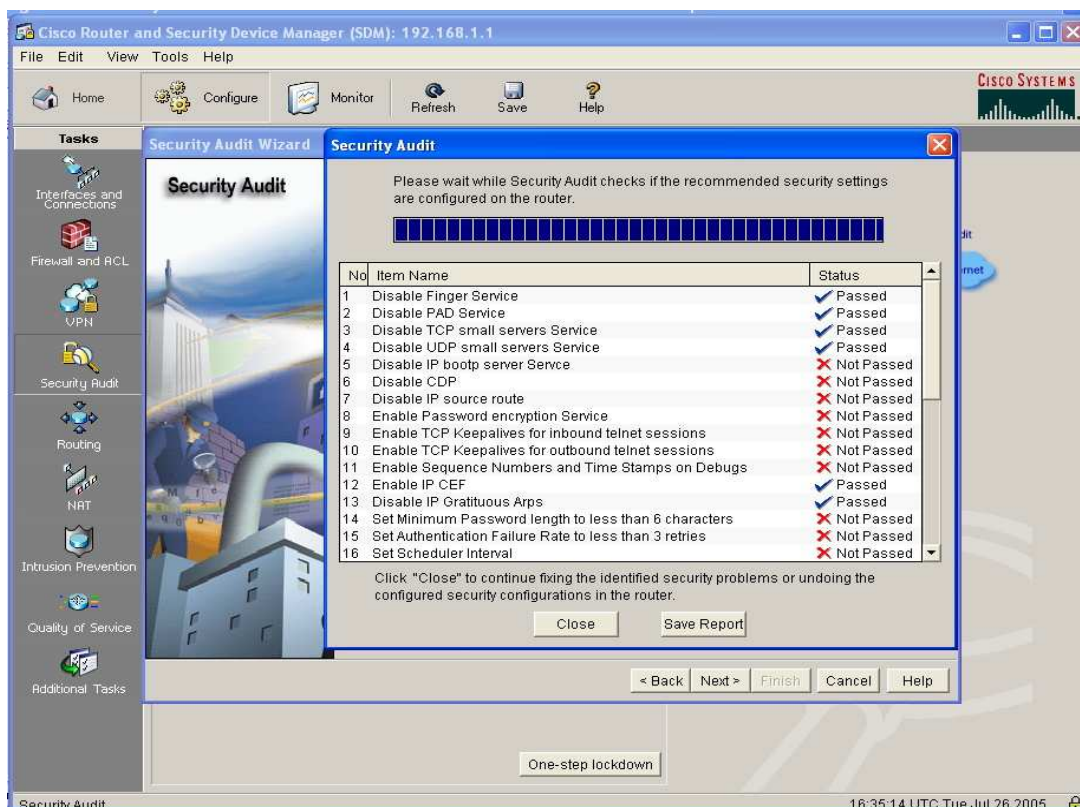


Figure 5 – Security Audit

Firewall

The ISR 871, like its bigger brothers in the range, features a stateful inspection firewall. While this is a genuinely powerful firewall – you can create a series of rules to totally customise it as required – its default settings will satisfy the needs of 99% of users and could not be more simple to configure, care of a firewall installation wizard.

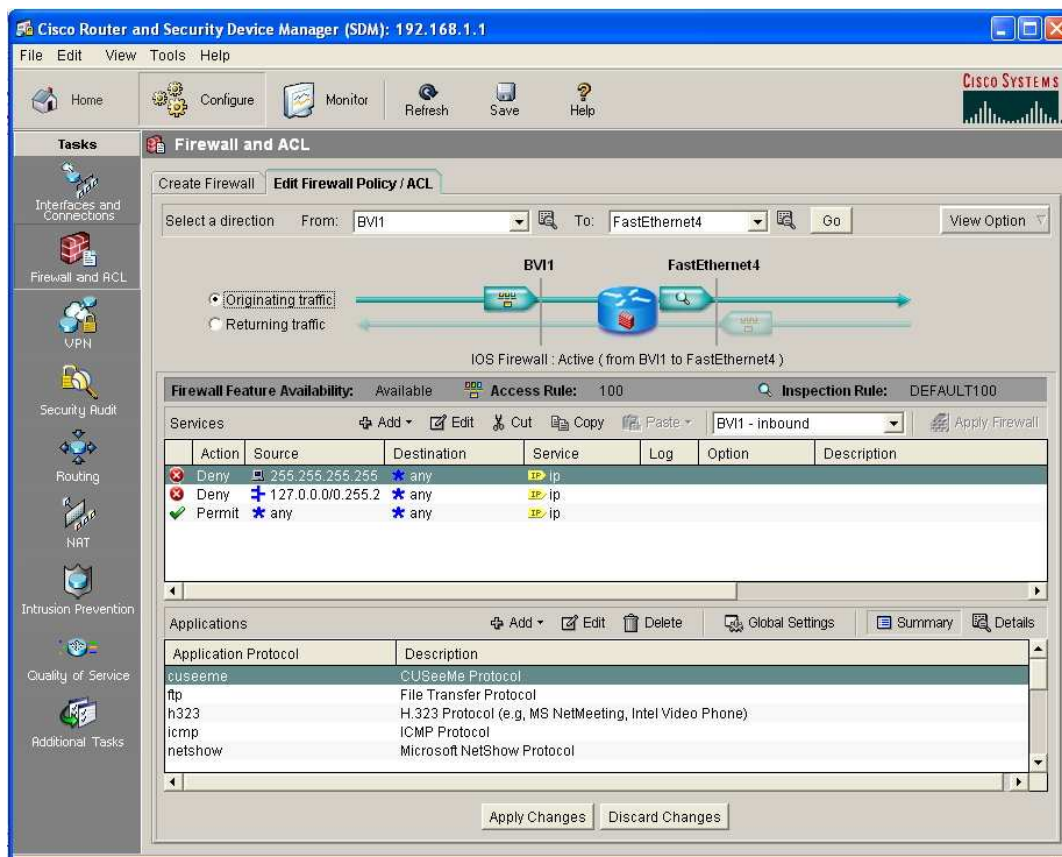


Figure 6 – Setting Up The Firewall

As well providing a configuration wizard, SDM 2.1 graphically displays exactly what the firewall is allowing and denying, viewable from both an outgoing traffic and returning traffic perspective. Neat.

Inline IPS

The ISR 871 also includes an inline Intruder Prevention System (IPS).

This is a deep-packet, inspection-based solution that can drop traffic, send an alarm, or reset the connection, helping enable the router to respond immediately to security threats and protect the network. Working in tandem with the other security features such as IPSec VPN and the Firewall, the IPS can allow decryption, tunnel termination, firewalling, and traffic inspection at the first point of entry into the network, as well as on internal networks.

It is based around a database of 100 IPS signatures which consists of a cross-section of intrusion-detection signatures representing severe breaches of network security, the most common network attacks, and information gathering scans. In practice this means it covers all the primary attacks registered to date. As with the firewall, with which it inter-works

directly, the IPS is easily configured using a wizard. Again it is made very clear just what you have and have not configured, on a per-interface WAN/LAN/WLAN basis.

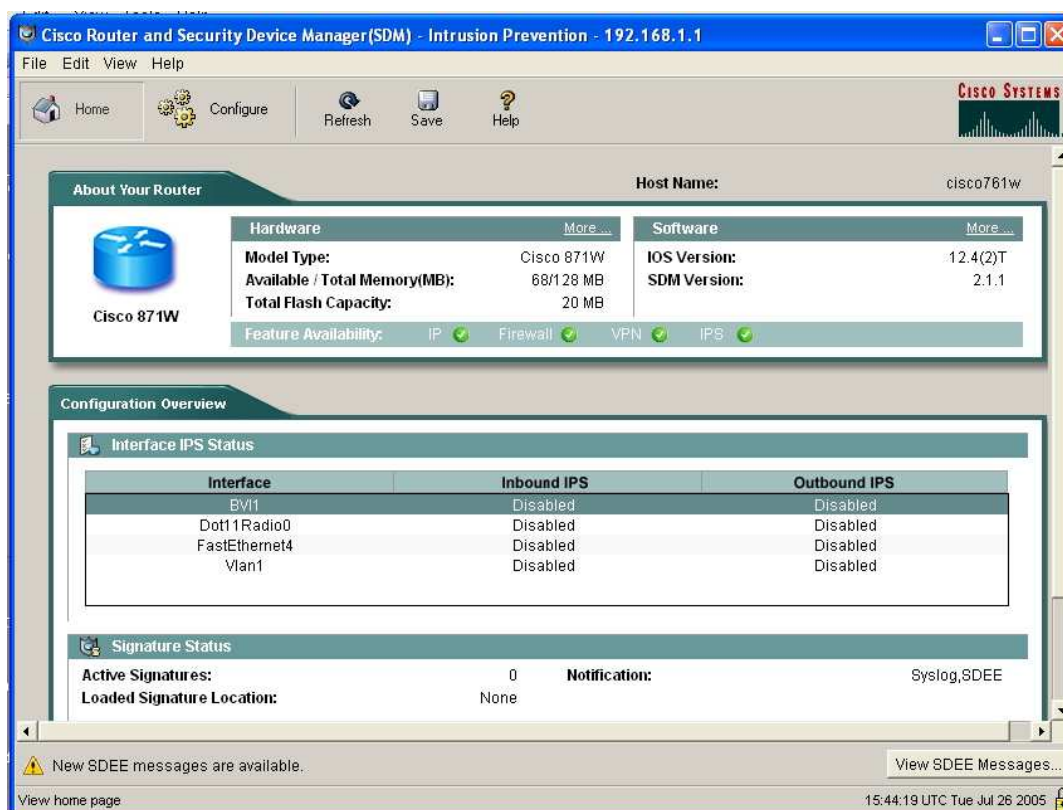


Figure 7 – Configuring The IPS

VPN (Virtual Private Networking)

The ISR 871 supports a broad range of VPN tunnelling and encryption options including MPLS based VPNs or VPNs using IPsec AES and 3DES high-speed encryption, courtesy of built-in hardware acceleration. These provide a user with secure connections to remote sites from the ISR 871.

Up to 10 VPN tunnels are supported by the device. As with the other security features, a wizard complete with graphics showing exactly what tunnels you are setting up helps make the configuration as simple as possible.

Though intended as a small business device, the ISR 871 has very advanced VPN features, handed down from its bigger brethren in the range. Cisco Dynamic Multipoint VPN (DMVPN) helps enable on-demand and scalable full-mesh VPN to reduce latency, conserve bandwidth, and simplify VPN deployment. The DMVPN feature builds upon Cisco IPsec and routing expertise by helping enable dynamic configuration of GRE tunnels, IPsec encryption, Next Hop Resolution Protocol (NHRP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP). DMVPN also eases administrative burden with no configuration at the hub when adding new spokes or when setting up spoke-to-spoke connections. Another option is Easy VPN. This is an IPsec solution designed to support hub-and-spoke VPN topologies with minimal effort and high scalability. Easy VPN simplifies provisioning and management of VPN solutions between

Cisco PIX firewalls, the Cisco VPN 3000 Series Client and routers of all sizes. It uses “policy-push” technology to simplify configuration.

The Cisco ISR 871 also supports V3PN, which provides a VPN infrastructure capable of converged data, voice, and video across a secure, QoS-enabled IPsec network. Cisco claims it allows customers to obtain the same performance for voice and video applications over an IP transport as they would over an alternate WAN link.

Multi-VRF, also referred to as VRF-Lite, provides the ability to configure and maintain more than one instance of a routing and forwarding table within the same physical router. In combination with Ethernet VLAN technologies and WAN VPN technologies such as Frame Relay, Multi-VRF helps enable the provisioning of several logical services using one physical network, extending the privacy and security down to a branch-office LAN. One Cisco router with Multi-VRF can support multiple organisations with overlapping IP addresses while maintaining separation of data, routing, and physical interfaces.

For Voice over IP (VoIP) too, security is in place. Media encryption using secure RTP (SRTP) encrypts the voice conversation, rendering it unintelligible to would-be hackers who have penetrated and gained access to the voice domain. SRTP is designed specifically for voice packets and supports the AES encryption algorithm. Media encryption using secure RTP is more bandwidth-efficient than IPsec.



Figure 8 – Configuring A VPN

WLAN Security & Management

WLAN security features available on the ISR 871 are extensive and include 802.1X, Cisco Extensible Authentication Protocol (LEAP), Protected EAP (PEAP), EAP-Transport Layer Security (EAP-TLS), static and dynamic Wired Equivalent Privacy (WEP), TKIP, and RADIUS accounting for wireless clients.

These are configured from the SDM 2.1 by launching the WLAN manager. This brings up an older style interface which, for us, is one of the weaker points of the ISR 871. While being comprehensive in its capabilities, it is by no means as intuitive an interface as SDM itself. It also means you end up with lots of different windows open on the desktop by this time.

SSID Configuration

1. SSID Broadcast SSID in Beacon

2. VLAN No VLAN Enable VLAN ID: (1-4094) Native VLAN

3. Bridge Bridge Group Number: (1-255)

4. Security No Security

Static WEP Key

Key 1 128 bit

EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

WPA

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

Apply Cancel

SSID Table

Delete	SSID	VLAN	Bridge Grp. Number	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="checkbox"/>	ciscowlan	none	1	none	open	none		<input checked="" type="checkbox"/>

Figure 9 – Configuring WLAN Security Settings

Looking in more detail at some of the key security options themselves, 802.1x and Extensible Authentication Protocol, either Cisco’s LEAP or the industry standard EAP, work hand-in-hand, providing the infrastructure for robust authentication and dynamic key rotation and distribution. EAP provides a means for mutual authentication. Authorised users identify themselves to the wireless network, and the wireless network identifies itself to the user—ensuring that unauthorised users cannot access your network, and authorised users do not inadvertently join a rogue network.

Cisco unsurprisingly supports the 802.11 Wired Equivalent Privacy (WEP) standard at 128 bits. This allows full interoperability with classic WLAN clients or less-critical environments where only basic over-the-air security is required, such as an open public-access application. It also supports Temporal Key Integrity Protocol (TKIP), which addresses well-known vulnerabilities in WEP encryption. TKIP provides key rotation on a per-packet basis along with message integrity check (MIC), which determines if data has been tampered or corrupted while in transit. This robust method of

encryption provides a higher level of protection for data and protects the network from a variety of types of attacks.

On the authentication side, with the ISR 871 supports a 20-user internal RADIUS (AAA) server - perfect for the business customers Cisco is aiming this product at, since it removes the need to set up a costly external RADIUS server.

The WLAN settings can also be optimised by tuning the radio settings for speed or reach (distance transmitted) bias.

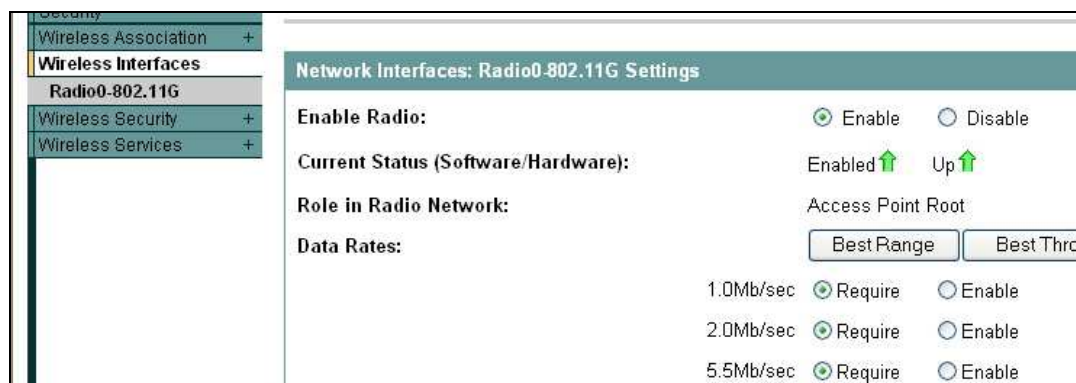


Figure 10 – Optimising WLAN Settings

CISCO ISR 871 FEATURE & PERFORMANCE TESTS

Testbed Basics

For the test we configured the ISR 871 with a basic VLAN – in line with the requirements of a small business, then connected both real and virtual wired and wireless clients. For the performance testing, we created a testbed using a combination of traffic and wireless client generation products from Spirent Communications and CMC.

Using Spirent's Avalanche 2500 we create a flow of web traffic requests that were converted into WLAN client requests using CMC's Emulation Engine (EE). In this way we were able to simulate 20 wireless clients – ideal for our requirements in this test. We used Spirent's Reflector 2500 server simulator to simulate the Internet and connected it via the WAN port. We also ran tests against a real Internet connection via an external ADSL router.

Our primary aim, having established that the 871 can support 20 users running basic traffic (see below), was to look at how adding (enabling) features on the router, both with and without encryption on the wireless clients, impacted on the overall performance of the Cisco device. While this means putting the ISR 871 under levels of stress it will almost never encounter in the real world, this is what this kind of testing is for – to see if we can break the device under test!

So did we? Read on...

Basic Wireless Clients Tests

Using the CMC EE we started with basic, Layer 3 authentication and 1KB packet send and receive tests. Running first with no security, we ran tests in short bursts, then over a 24-hour period, with no dropped packets – i.e. no traffic problems – throughout the test period.

We then enabled 128-bit WEP encryption on the WLAN clients and reran the 24-hour test with 1,000 test iterations.

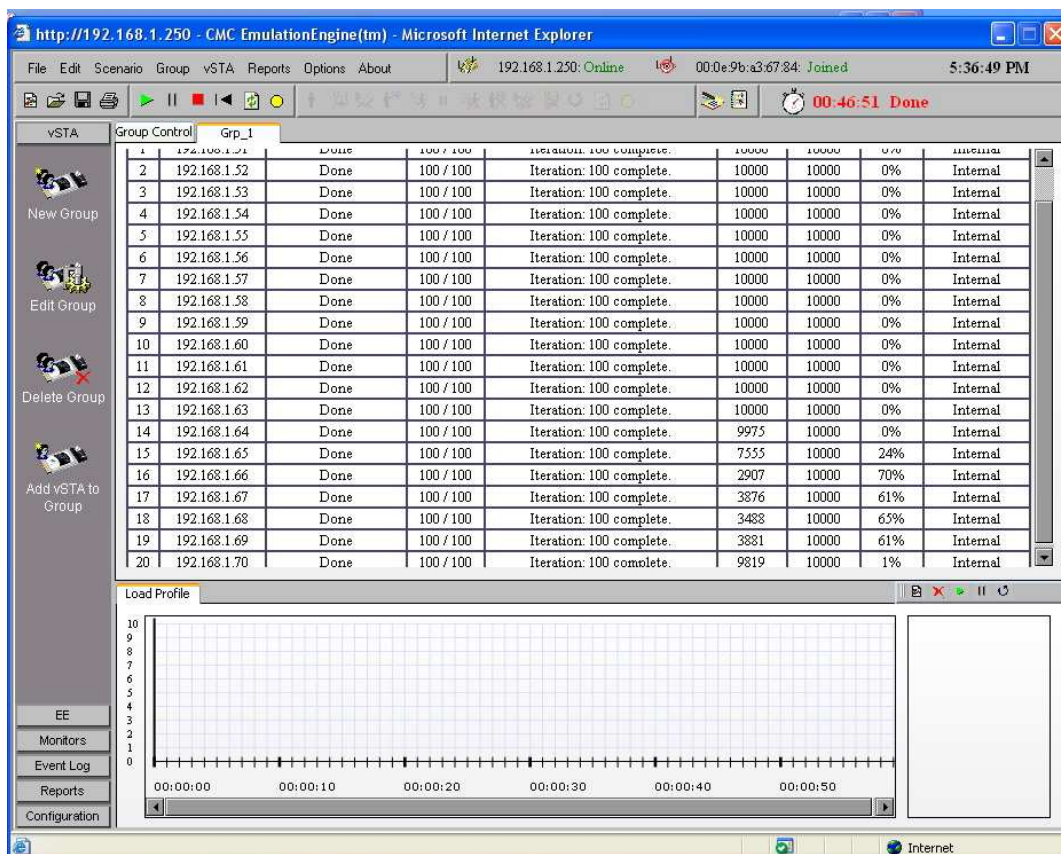


Figure 11 – Running A Basic WLAN Connectivity Soak Test

This time we did see packet loss. While the first 14 connected clients showed absolutely no packet loss over 24 hours – outstanding – clients 15-20 showed packet loss between 2-75%. However, this did not come as a surprise – we have seen more expensive, higher-end WLAN products in the labs exhibiting precisely the same behaviour in long tests.

Web Traffic Simulation Tests

Now we added in real http traffic from 20 virtual clients on the Spirent Avalanche, translated into wireless clients by the EE and targeted a virtual server across our “Internet” link. For these tests we created web pages of 10KB, 64KB and 256KB for the clients to GET. We ran tests in turn against each web page size, the tests starting with one virtual user and gradually rising to all 20 virtual users.

Again we ran tests both without and with WEP encryption. In this series of tests, we began with a “vanilla” default setup on the ISR 871, then enabled features one by one, starting with the firewall, then the IPS on the WAN interface, then on the WLAN and internal network too. Tests ran on average for 90 seconds and were repeated several times to ensure consistency.

The test below shows three levels of configuration and the corresponding results. The first set of figures is with no security features enabled, the second with the Firewall enabled and the third with IPS enabled on the WAN, WLAN and internal interfaces. There is no WEP encryption on the WLAN traffic.

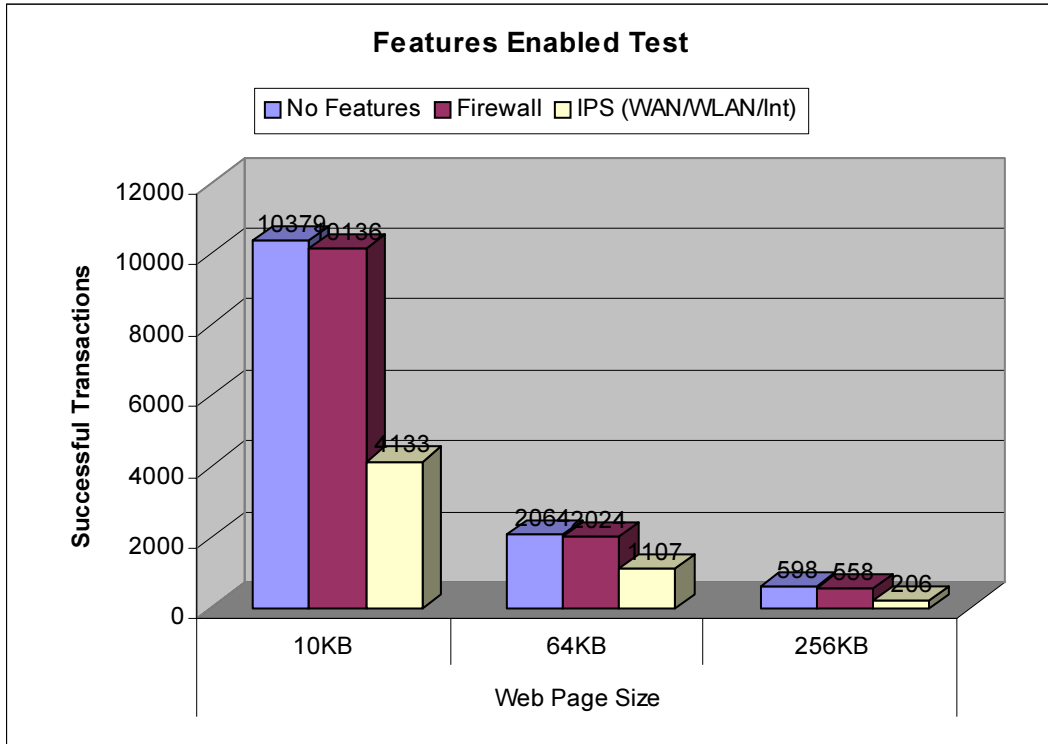


Figure 12 – Features Enabled Test

While enabling the firewall – default settings – produced only a slight decrease in available performance, adding the IPS across all networks did result in a significant overhead, total successful transactions falling by over 50%, the 10KB web page size test, for example, producing 10,136 successful transactions with just the firewall enabled, but falling to 4,133 successful transactions with the IPS enabled on all interfaces.

The impact of adding IPS to the WLAN network has the biggest impact, as you would expect. It is worth noting that enabling the IPS only for the WAN (Internet) interface as we suspect many users will, has minimal impact however.

We then examined the impact WEP encryption (128-bit) had on WLAN traffic by creating a simple configuration with just IPS enabled on the WAN interface, running a test with unencrypted traffic, then encrypting with WEP-128 and comparing the difference.

As we can see from the graph below, there was a significant hit on the number of successful transactions recorded in the test, due to the overhead WEP produces.

With the 10KB web page size, total transactions fell from 11,204 to 5,322, while the 64KB size went down considerably from 2,228 to 208. It is worth

noting that the 10KB web page size is by far the most commonly pulled down from the Internet however.

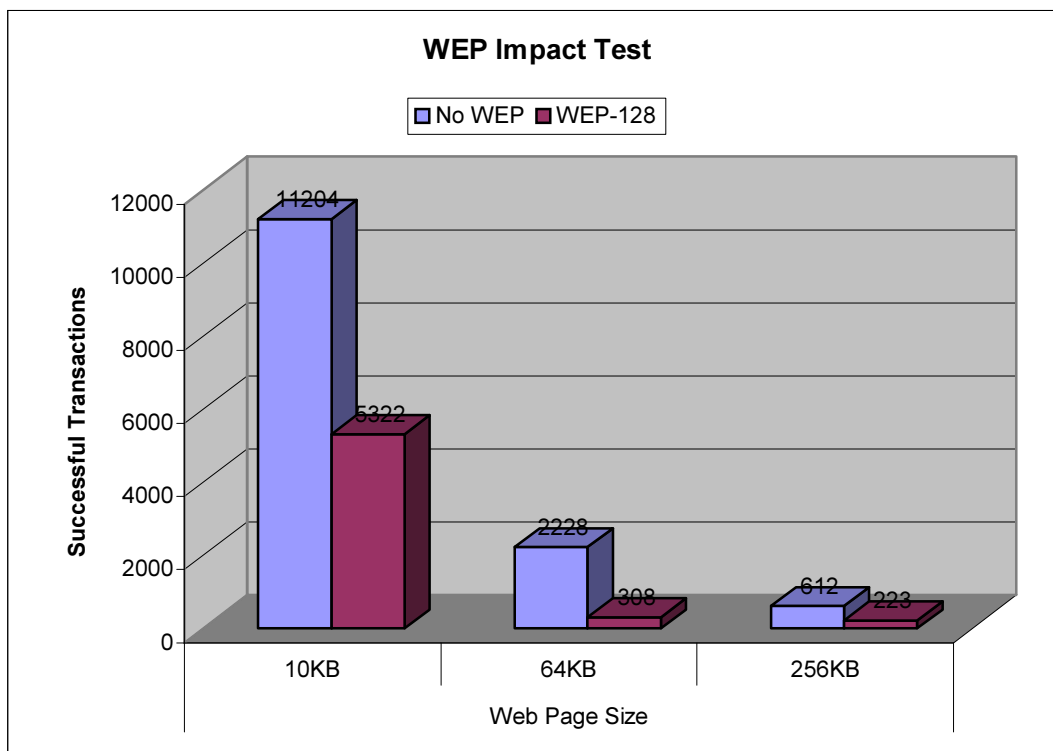


Figure 13 – WEP Impact Test

Obviously, there is always going to be a trade-off between performance and security levels. However, given the typical working pattern of a set of users in a small business, we suspect that, on a day-to-day basis, the average user would neither notice any significant bottleneck, nor be inconvenienced in any way.

The benefits of the added security therefore outweigh any performance downsides.

QoS Test

Finally, we enabled QoS on the WAN interface and added some streaming video traffic (tested both without and with QoS) to the mix, to see if we could optimise the outgoing Internet connection for real-time traffic.

We started by saturating the link with http traffic, GETting a 1MB page size, then enabled QoS with 70% bandwidth reserved for RTSP (QuickTime RealTime Streaming Protocol) traffic and compared how many video streams we were able to push through before and after QoS.

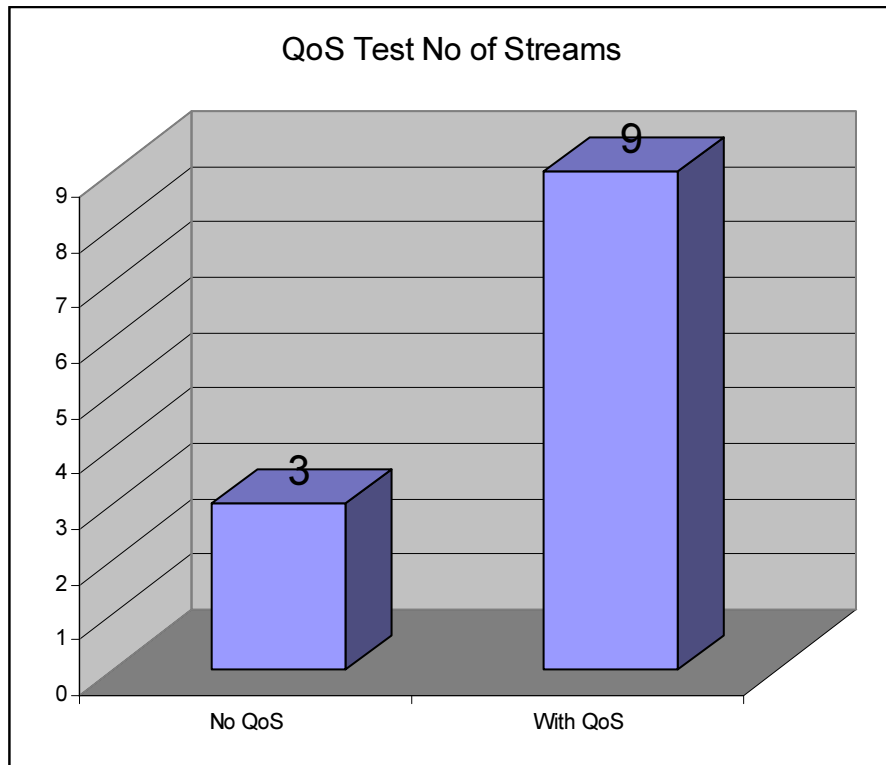


Figure 14 – QoS Video Streaming Test

We found that by enabling QoS our video streams increased by 300% from three to nine. This is as good a result as we could have expected, given the high bandwidth requirements for video. It means that with voice, any VoIP traffic could easily be guaranteed sufficient bandwidth, even for 20 users simultaneously, given the low overhead of voice traffic.

OVERALL SUMMARY

The aims of our testing were to examine the feature set of the ISR 871 with a focus on ease of use, flexibility and depth of coverage, to test the capabilities of the ISR 871 to cope with what will be substantially heavier traffic loads than those it would realistically find in the real world, and to gauge how easy the ISR 871 is to configure and manage on a day- to-day basis.

We found the feature set at all levels – WLAN, security, networking – to be very comprehensive and a clear differentiator between this level of product and something like Cisco's own Linksys brand. If you need real depth of features then the ISR 800 series gives you exactly that.

On the performance front, while we proved that it does dip noticeably when IPS is enabled on the wireless network, or when wireless encryption is enabled, in realistic day-to-day use, there are no issues to worry about. The product worked, day-in, day-out for a month, without requiring a single reboot during that time.

With SDM 2.1, the ISR 871 was easy to configure, even for relatively complex tasks, such as multi-layered security or QoS. Our only downside was the WLAN management which is clearly of a previous generation of interface and less intuitive as a result. However, this is a very minor point, given the overall quality of the management interface. Added to this, the classic CLI is accessible both locally and remotely (and securely) meaning that the router can easily be supported from a remote site, ideal for a managed service operation, for example.

Overall then, we can recommend the ISR 871 to any small business looking for a product where an extensive feature set is the key requirement and day-to-day reliability is an important factor. And who wouldn't be interested in that combination?

Product: Cisco ISR (Integrated Services Router) 871 (800 series)

Price: From \$649

Contact: Cisco – www.cisco.com



APPENDIX: THE TEST EQUIPMENT DETAILS

Spirent Avalanche/Reflector 2500

Internet architectures are becoming increasingly complex.

Whether you're building network equipment or providing a service, you must deliver consistent performance under all conditions. Until now, capacity assessment at high-loads has been a costly and complex process. For this reason, Spirent Communications introduced the Avalanche 2500 and Reflector 2500 appliances to assist with the challenge. At Broadband-Testing we have taken these web application simulation and planning products and integrated them into our test-bed simulating real-life Internet conditions; those that the average user experiences daily.



Figure 15 – Spirent Avalanche 2500

Avalanche 2500 is described by Spirent as a capacity assessment product that challenges any computing infrastructure or network device to stand up to the real world load and complexity of the Internet or intranets. The system determines the architectural effectiveness, points of failure, and the performance capabilities of a network or system. Using Avalanche 2500 to generate Internet user traffic and Reflector 2500 to emulate large clusters of data servers, you can simulate even the world's largest customer environments. The system provides invaluable information about a site's architectural effectiveness, points of failure, modes of performance degradation, robustness under critical load, and potential performance bottlenecks. It is able to set up, transfer data over, and tear down connections at very high rates - all while handling cookies, IP masquerading for large numbers of addresses, and traversing tens of thousands of URLs.

Avalanche 2500 initiates and maintains more than a million concurrent connections, each appearing to come from a different IP address. This allows realistic and accurate capacity assessment of routers, firewalls, load-balancing switches, and Web, application, and database servers. It helps identify potential bottlenecks from the router connection all the way to the database. This accuracy is especially critical for gauging Layer 4-7 performance. The ability to additionally simulate error conditions such as HTTP aborts, packet loss, and TCP/IP stack idiosyncrasies can help

anticipate-and avoid-significant and previously unknown impacts on performance.

To enable more accurate load simulations across multi-tiered Web site architectures, the system also supports extremely realistic user modelling behaviours such as think times, click stream, and HTTP aborts that cause Web servers to terminate connections while back-end application servers continue to process requests. Configuring in this way is simple as both Avalanche 2500 and Reflector 2500 directly from a desktop browser to set up tests, review feedback in real time, and easily reconfigure test parameters.

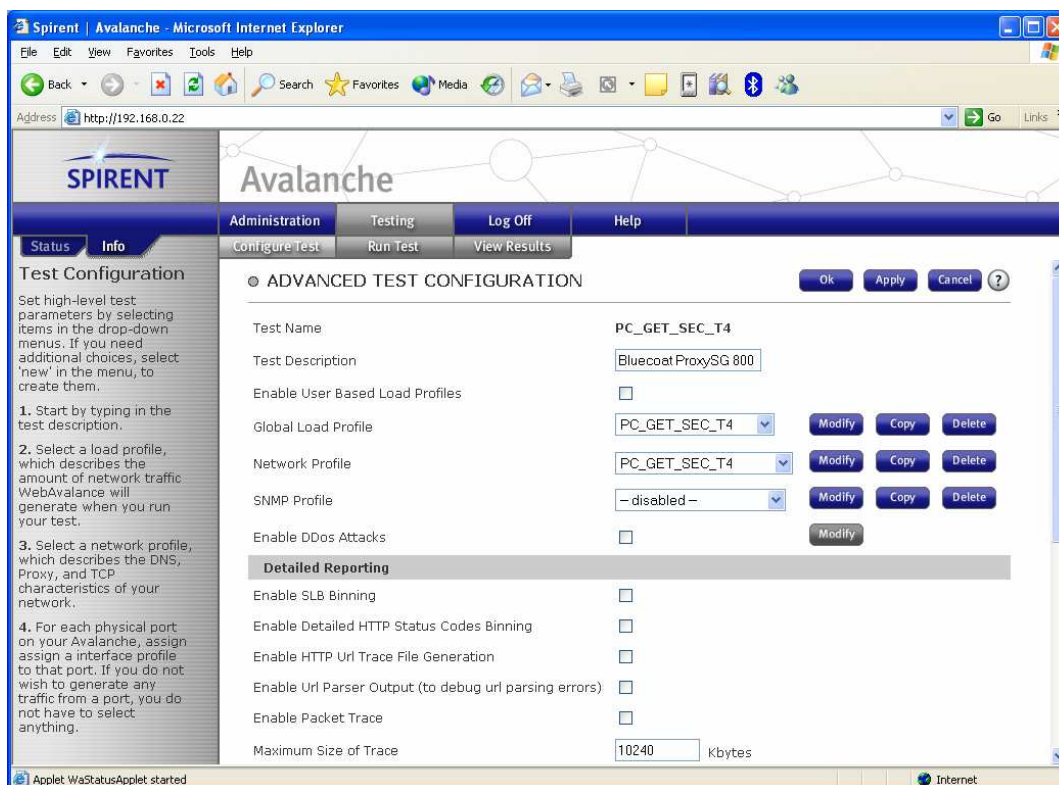


Figure 16 – Creating An Avalanche 2500 Test

The Avalanche 2500 also supports browser cookies, html forms, HTTP posts, and SSL-encrypted traffic. The system therefore gives you the flexibility to specify data sources and mix and match data sets to recreate accurate user behaviour at very high performance levels.

It also simulates SSL loads that can stress the world's most sophisticated secure e-commerce platforms. It also includes configurable cipher suites that enable you to emulate different types of browsers. Avalanche 2500 includes a high-accuracy delay factor that mimics latencies in users' connections by simulating the long-lived connections that tie up networking resources. Long-lived, slow links can have a far more detrimental effect on performance than a large number of short-lived connections, so this approach delivers more realistic test results.

While Avalanche 2500 focuses on the client activity, Reflector 2500 realistically simulates the behaviour of large Web, application, and data

server environments. Combined with Avalanche 2500 it therefore provides a total solution for recreating the world's largest server environments.

CMC Emulation Engine

The EmulationEngine XT's ability to impose a scalable and controllable load of multiple 802.11 compliant Stations has made it an essential tool for product design engineers, test engineers, network installers and network maintainers. The EmulationEngine enables critical scalability and capacity testing of 802.11 products, network devices, network architecture, and backend systems.



Figure 17 – The CMC Emulation Engine

The EmulationEngine features have now been extended to enable the testing of WPA enabled designs. Wi-Fi Protected Access (“WPA”) is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for Wireless LAN systems.

This security is necessary and demanded by Enterprise level Wireless network implementations. When properly designed into an 802.11 product and installed in a WLAN system, it will provide a high level of assurance that data will remain protected and that only authorized network users can access the network. Now with EE-WPA, a core member of the EmulationEngine XT family, engineers have the ability to perform sophisticated capacity, scalability and load stress testing on WPA enabled Enterprise class products and Wireless networks. 1 to 59 of the EmulationEngine's 64 vSTA™ (virtual station) can be selectively configured to enable WPA.

An engineer can now use multiple station loading to test critical aspects of WPA: 802.1x authentication, EAP-TLS, ties to Radius servers with import of certificates, TKIP/AES, MIC and PSK mode. A unique flexibility of the EE-WPA allows the security mode for each of the emulators vSTA's to be set individually and differently: Open; WEP; WPA-PSK; or WPA. This enables

testing of 802.11 products and WLAN systems that support mixed mode security.

The EmulationEngine can be directly connected to a Windows 2000/XP PC using the supplied 802.3 Ethernet crossover cable or through a network. This “Command and Control” PC functions as a configuration, control and monitoring unit for the EmulationEngine via CMC’s GUI (with a Web browser) or a Command Line Interface (CLI).

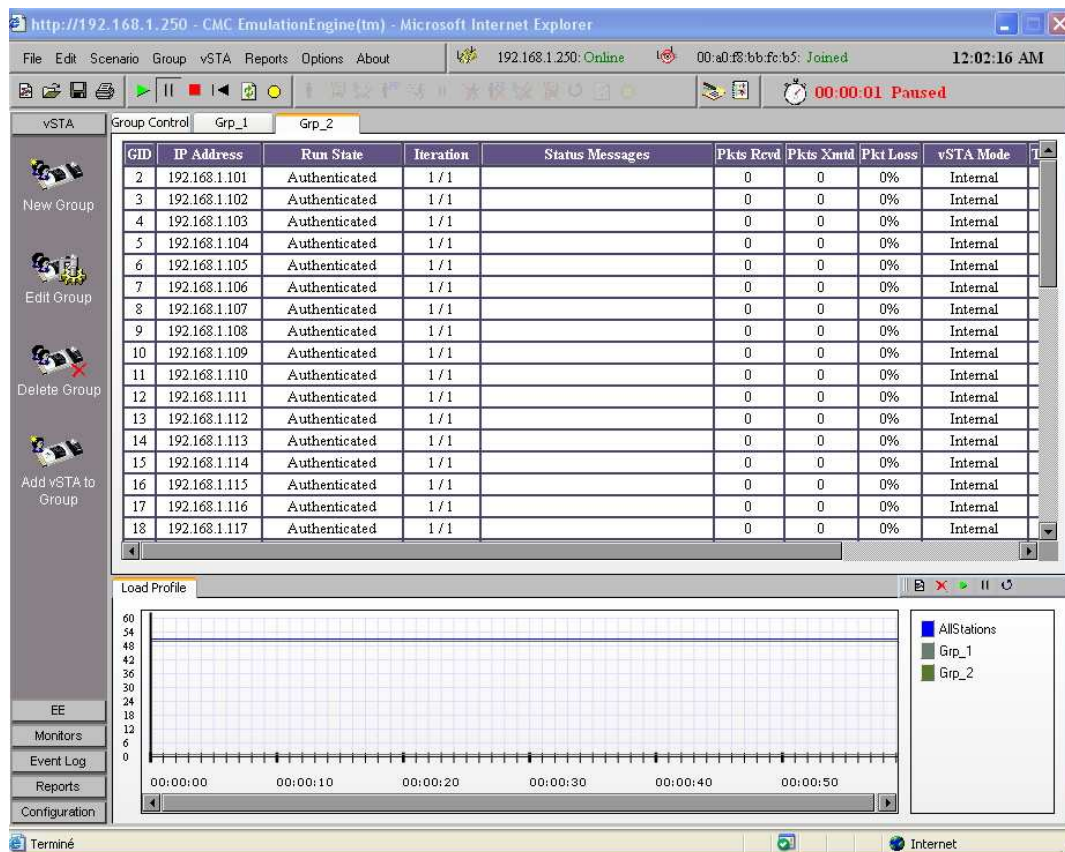


Figure 18 – The CMC Emulation Engine Main Screen

Each EmulationEngine allows you to create multiple virtual WLAN users, vSTAs. The vSTAs are hosted on the EmulationEngine. VSTAs can be defined in groups using an organization defined by the user. The user can manage individual or groups of vSTAs in order to control authentication, association, disassociation, de-authentication, and generation of 802.11 traffic. The user can configure each vSTA to generate traffic. Internal Mode generates traffic load per vSTA, internal to the emulator, using configurable Ping to selectable hosts. Using External Mode a “Third Party Load Generator” can be tied to the emulators 802.3 port and received data packets can be seamlessly redirected as 802.11 traffic by each individual vSTA.

These different configurations enable true testing of the capacity, scalability and performance of a wireless network at the design stage, during pre-installation configuration analysis and deployment, and for back end performance analysis of networks.