Current Analysis

Streetwise Intelligence.

Lab Challenge: Cisco 2821 Integrated Services Router

Product Profile:

Vendor:
Cisco Systems

Product::
Cisco 2821 Integrated Services Router

Target Market:
Multi-Service Branch Office Router

Testing Period:
June – July, 2004

Report Released:
September 13, 2004

Software Tested:
IOS 12.3(8)T (pre-release)

Features Tested:
- *LAN-LAN Throughput*

- *LAN-WAN Throughput*

- with -

- *IP routing*
- *Layer-2 switching*
- *IOS firewall*
- *IOS IDS/IPS*
- *Access control lists*
- *Extended ACLs*
- *IPsec site-to-site VPN*
- *GRE tunneling*
- *Packet classification*
- *Packet marking*
- *Class-based weighted fair queuing*
- *QoS enforcement*
- *H.323 VoIP toll bypass*
- *CallManager Express*

Market Event

On September 14, 2004, Cisco Systems introduced its next generation branch office router portfolio. The new family of routers, dubbed Integrated Services Routers (ISR), includes the entry-level 1800 series, the mid-range 2800 series, and the higher-end 3800 series. These products are designed and positioned to supersede Cisco's existing 1700, 2600, and 3700 series routers.

These new routing platforms enhance Cisco's ability to deliver multi-service performance while significantly expanding the capacity and scalability of its branch platforms. This technology comes none too soon, as competitors are at Cisco's doorstep with new competitive multi-service offerings. With a portfolio of new products on the horizon from Cisco and its competitors, customers will have to make a choice, but Cisco is well prepared to defend its turf against new and agile competitors.

The Claim

When Cisco designed its new ISRs, one of its primary objectives was to address the multi-service performance concerns that customers have decried and competitors have attacked. With the introduction of the new ISR Routers, Cisco makes the bold claim of "secure, line rate delivery of concurrent services and applications." In fact, Cisco is so confident of its new products, it claims that the Cisco 2821 ISR can forward traffic at line rate, regardless of how many of the integrated services are active.

The Challenge

Current Analysis challenged Cisco to prove that the new Cisco 2821 ISR could actually stand up to a real-world barrage of traffic while still forwarding all traffic at line rate. Specifically, Cisco accepted the Current Analysis Challenge that the Cisco 2821 router could forward full duplex traffic across four T1 circuits (a typical high-performance configuration for the 2821 series) – with any combination of IP services features enabled – at line rate.

Lab Challenge Testing Profile

A four T1 configuration represents a typical high-end real-world deployment of the 2821 router (Cisco recommends a larger router and/or a fractional T3 interface for higher bandwidth deployments). Cisco agreed to an extensive list of standard IP services that Current Analysis wanted to test, including basic (and extended) access control lists, stateful firewall inspection, IDS, point-to-point IPsec, GRE, traffic classification via Layer 4 packet attributes, queuing for quality of service, H.323 call termination and VoIP toll bypass, as well as IP-Telephony PBX services using Cisco CallManager Express. In addition to passing traffic at line rate, the router was also expected to classify, enforce, and preserve all quality of service attributes necessary to support VoIP.

Global Headquarters
21335 Signal Hill Plaza
Sterling, VA 20164
Phone | 703.404.9200

Cisco 2821 Integrated Services Router

Cisco 2821 ISR At-a-Glance:

- *2 Rack Units (RU)*
- *2 x 1000Base-TX Ethernet ports*
- *4 x HWIC slot supporting traditional V/WICs and next generation / higher performance / higher density HWIC interfaces*
- *1 x NME slot supporting traditional Network Modules, or next-generation Extended Network Modules.*
- *1 x EVM slot for increasing analog voice/BRI port density.*
- *3 x DSP slots for transcoding support (necessary for VoIP, voicemail, etc)*
- *2 x AIM slots for future hardware acceleration and for integrated voicemail features.*
- *Built-in hardware encryption and decryption silicon*
- *Space for expanded power supply for supporting integrated 802.3af power over Ethernet.*
- *Front panel USB for Secure configuration distribution and bulk storage flash.*

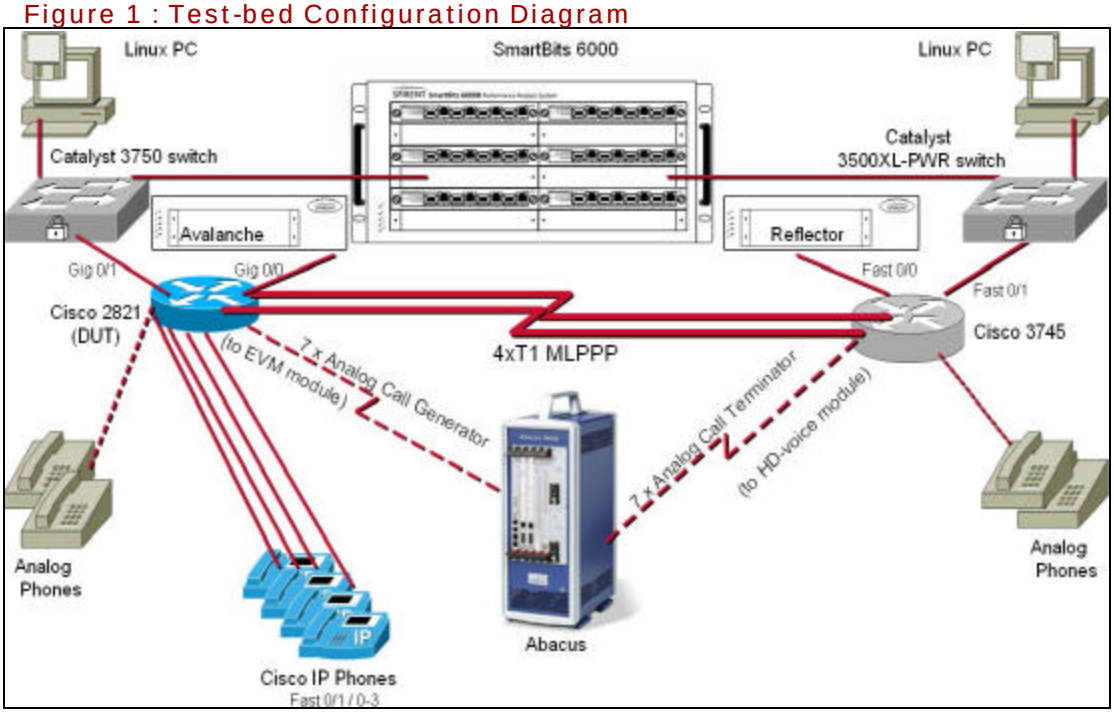
Testing Methodology

To verify Cisco's performance claims, Current Analysis crafted a test bed to exercise the multi-service features of the Cisco 2821 router. The Cisco 2821 was connected via four T1 crossover cables to a Cisco 3745 router, which served as a control device. Performance verification was done in an iterative manner, enabling one service at a time, verifying the performance of that service, and then concurrently verifying the operation of all previously enabled services. The SmartBits 6000 and SmartFlow 4.0 from Spirent Communications were used to generate the bulk IP, TCP, and UDP traffic that was used to benchmark the router. Maximum throughput was verified for each test by running "throughput" binary search, and zero-loss performance was then verified by running a "packet loss" test to validate wire-speed throughput with no packet loss.

Performance tests were initially conducted using the "simple IMIX" traffic profile, denoted as "IMIX 1" in Figure 2. The IMIX traffic profile is used in the industry to simulate real-world traffic patterns and packet distributions. IMIX profiles are based on statistical sampling done on Internet routers, and are published in various levels of granularity, such as "simple" and "complete." For ease of data management and troubleshooting, the "simple IMIX" was used as the foundation for the benchmarks. This distribution provides a real-world traffic mix without pushing the DUT to worst-case extremes.

Firewall, IDS, and ACL rules were verified by either blocking specific traffic flow types, or by injecting additional traffic into the test using the Spirent Avalanche or a Linux workstation. Quality of service matching and enforcement was verified by oversubscribing the NxT1 interface and verifying that high priority traffic arrived intact while low priority traffic was dropped. QoS was also subjectively verified by placing VoIP calls across the test system during oversubscription conditions while listening for delay, stutter, or echo.

Figure 1 : Test-bed Configuration Diagram



Cisco 2821 Integrated Services Router

Device Configurations as Tested:

Cisco 2821 (DUT)
IOS 12.3(8)T (prerelease)
256 MB DRAM
64 MB FLASH
2 x MFT-2T1
HWIC-4ESW-PWR
EVM-HD-8FXS/DID
PVDM2-16

2821 Interfaces:
(4) T1 interfaces (MLPPP)
(4) 802.3af 100BaseTX
(16) 100BaseTX EtherSwitch
(2) 1000BaseTX (onboard)
(8) analog FXS voice ports

Cisco 3745 (support)
IOS 12.3(7)T (release)
256 MB DRAM
64 MB FLASH
2 x MFT-2T1
NM-HDA
AIM-VPN-HPII

3745 Interfaces:
(4) T1 interfaces (MLPPP)
(2) 100BaseTX (onboard)
(8) analog FXS voice ports

Testing Methodology (continued)

To test IP services with IPsec enabled, the "IMIX-3" IPsec IMIX profile -- which lowers the maximum packet size to 1,418 bytes (to avoid fragmentation) -- was used. The system under test was configured to use IPsec and GRE between the DUT and the supporting router. An IMIX profile modified to use TCP-based flows, which more realistically emulate real-world traffic was used. The load profile consisted of traffic with Layer-4 TCP headers resembling HTTP, SMTP, and POP traffic flowing in each direction. Tests were also later run to verify system throughput using the standard IMIX with a reduced MTU.

Figure 2 : IMIX Packet Distributions

IMIX 1 - Standard IMIX	
Frame Size	% of Packets
58	58.67%
62	2.00%
594	23.66%
1518	15.67%

IMIX 2 - TCP IMIX	
Frame Size	% of Packets
90	58.67%
92	2.00%
594	23.66%
1518	15.67%

IMIX 3 - IPsec IMIX	
Frame Size	% of Packets
90	58.67%
92	2.00%
594	23.66%
1418	15.67%

IOS Firewall: The IOS Firewall was required to apply stateful inspection to seven types of traffic. The firewall was configured (in conjunction with extended access control lists) to deny specific traffic types of traffic (e.g., telnet) while passing others (e.g., HTTP). The access control list consisted of ten specifically identified match rules at the TCP layer, one at the IP layer, and a specifically matched TCP deny rule as the twelfth rule.

Intrusion Detection: IDS/IPS was configured to alert and block ICMP traffic dynamically during the tests, exercising the IDS engine. For verifying packet classification and QoS enforcement, the router was configured to classify traffic into one of four class-based queues based on Layer 4 attributes, and policing actions were defined for each queue to color the packets, perform bandwidth shaping, and enforce queuing policies. An NBAR Layer 7 class-map was also included to stress application-layer recognition. NBAR HTTP-layer inspection was first separately verified using a SmartBits Avalanche/Reflector setup.

IPsec: Multi-Link PPP was used as the protocol between the DUT and the supporting router. IPsec was deployed over the Multi-Link PPP NxT1 interface configured with pre-shared authentication. When offering an oversubscribed load to test QoS, anti-replay checking was disabled to overcome IPsec timeouts caused by QoS enforcement.

QoS: To test QoS, an Abacus 5000 voice analyzer connected to seven FXS POTS interfaces on each router was used to measure voice quality while oversubscribing the NxT1 link. To exercise the CPU and routing engine further, Cisco CallManager Express was enabled, and four IP phones were connected to the router. Using the IP handsets, calls were placed to destinations on the DUT and to analog extensions on the supporting router. Router-generated music-on-hold was also tested on two extensions while the full Abacus/SmartFlow Voice test was in progress. The Web-based administrative tool was also exercised while running data throughput tests and while making calls.

To validate that QoS was being properly enforced, calls between analog extensions attached to the DUT and supporting router were manually placed, and voice quality was subjectively measured. The Abacus 5000 was used to quantitatively measure the QoS of seven concurrent cross-WAN analog calls during oversubscription conditions.

Quick Facts:

An individual T1 has 1.536 Mbps of usable bandwidth in each direction.

Four T1's have a total of 12.288 Mbps of bidirectional capacity.

MLPPP splits each packet into 4 fragments, and adds an 8-byte header to each fragment

In plaintext tests with a duration of 30 seconds, the Cisco 2821 forwarded a maximum of 12.16 Mbps of offered Layer-3 traffic with zero packet loss and all IP services enabled. That's 99% of available bandwidth before MLPPP overhead.

With IPsec encryption turned on, the Cisco 2821 forwarded a maximum of 9.85 Mbps of offered Layer-3 traffic with zero packet loss and all IP services enabled.

IPsec adds significant overhead that varies by packet size. 64-byte packets have the worst overhead (125%).

In some cases, the Cisco 2821 was actually able to exceed theoretical wirespeed by buffering packets during congestion periods for the length of the test.

Results and Analysis

In the enterprise branch office, IP services such as stateful firewalling and packet filtering, intrusion detection and prevention, VPN termination, bandwidth shaping, and content scanning and filtering are critical to ensuring the integrity and security of both the branch office network, and the central office that branch is connected to. The uncontrolled nature of many branch offices makes them a natural point of entry for viruses and malicious code.

Next-generation branch-office routers must be capable of delivering these IP services without impacting traffic, and with plenty of headroom for additional services in the future. The widespread adoption of voice over IP (VoIP) technology will drive the need for new IP services in the branch, including key system/PBX functionality, voicemail, and call distribution/call center functionality. With VoIP, the branch office router becomes a natural communications hub for converged traffic. The Cisco 2821 is well equipped to stake an early claim as an all-in-one converged communications hub.

The Cisco 2821 ISR successfully routed full duplex traffic across four T1 interfaces at line rate. The router maintained line rate throughput under the "IMIX-1" traffic profile with Firewall, Intrusion Detection and Prevention, Access Control Lists, Extended Access Control Lists, Qualify of Service Classification, Packet Marking/Coloring, and Quality of Service Enforcement (class-based weighted fair queuing) enabled. The router also maintained line rate throughput while processing and forwarding two H.323 toll bypass VoIP calls, and demonstrated no noticeable latency or reduction in voice quality during the test. The router also passed the same battery of tests using the slightly less aggressive "IMIX-2" traffic profile, which uses TCP packets rather than pure IP packets. Both traffic mixes were ran to ensure that all components of the inspection engine were fully exercised during the test.

With IPsec encryption and GRE tunneling (for voice traffic) enabled between the Cisco 2821 and the supporting router, the Cisco 2821 again successfully routed full duplex traffic across four T1 interfaces at line rate. In this scenario, the "IMIX-3" traffic profile was used to eliminate packet fragmentation. The router successfully encrypted and passed traffic with Firewall, Intrusion Detection and Prevention, Access Control Lists, Extended Access Control Lists, Qualify of Service Classification, Packet Marking/Coloring, and Quality of Service Enforcement (class-based weighted fair queuing) enabled. The router also maintained line rate throughput while forwarding two H.323 toll bypass VoIP calls. In subsequent tests voice quality was quantitatively measured using the Abacus 5000. No measurable changes in latency or reduction in voice quality were recorded.

Under no circumstances did the router drop traffic during the non-oversubscribed tests. CPU utilization under worst-case load (with oversubscription, seven analog calls, four VoIP calls, music-on-hold, and all services enabled) was 74%.

The test results demonstrate that the Cisco 2821 is capable of delivering a broad range of IP services simultaneously without incurring performance penalties. Enterprises can confidently deploy the 2821 router with a broad range of security services and voice features without compromising on performance or quality of service. The 2821 is well suited for enterprise branch offices of 100 users or less, and is capable of delivering real-

Additional tests on the Cisco 2821 router were performed to measure the router's maximum forwarding rate, maximum throughput rate, and to quantify the impact of specific traffic types on the performance of the router with IP services enabled.

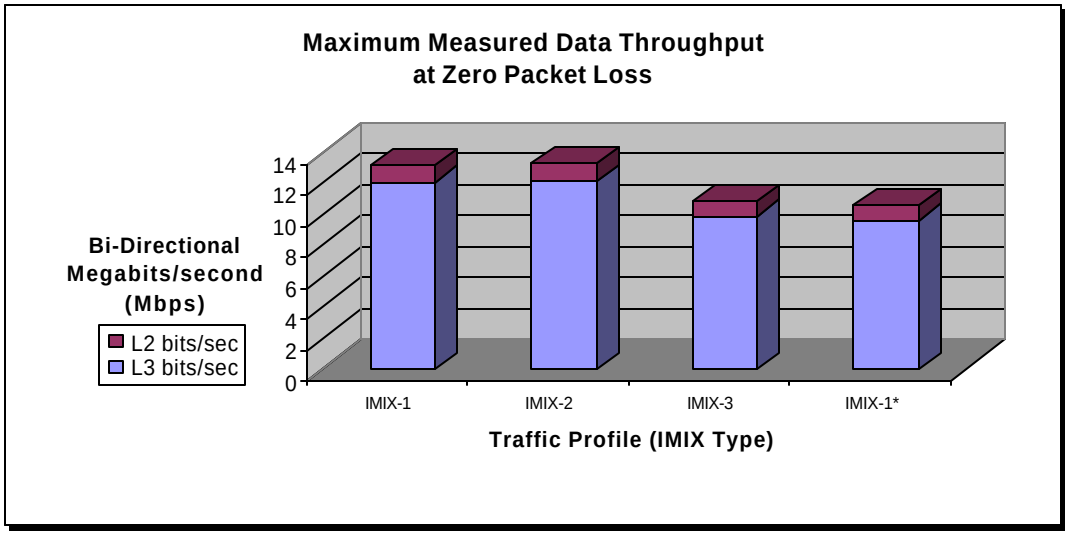
These results, along with additional analysis of Cisco's new router platforms, are available in the extended version of this report. For more information, please visit the Current Analysis Web site.

Current Analysis, Inc.
21335 Signal Hill Plaza
Sterling, VA 20164

Phone: (703) 404-9200
Fax: (703) 404-9300
sales@currentanalysis.com

For more information on this report, or other Current Analysis services, visit www.currentanalysis.com

time security and voice services with sufficient headroom to deal with new features or more processor intensive rules in the QoS, ACL, or IDS rule sets in the future.



Lab Challenge Charter

The Current Analysis Lab Challenge Program is a lab benchmarking research effort funded by Current Analysis. When a vendor steps forward with a new, potentially disruptive product, Current Analysis may challenge that vendor on its claims of performance and/or functionality. A Current Analysis analyst challenges the vendor to substantiate its performance and functionality claims in a lab environment that closely simulates real-world conditions. If the vendor accepts the challenge, it is free to review and assist in developing the test methodology and the vendor may assist in the testing process. At the end of the testing period, all results – whether beneficial or detrimental to the vendor – belong to Current Analysis, and are published in a Lab Challenge summary.

A free copy of any Current Analysis Lab Challenge Summary is available on Current Analysis' public web site, http://www.currentanalysis.com. In addition, a detailed test report that includes specific configurations, additional test results, and an in-depth analysis of the product's strengths and weaknesses is available for purchase from Current Analysis.

Acknowledgements

Current Analysis gratefully acknowledges Spirent Communications for providing the test equipment necessary to conduct this test, including: SmartBits 6000B with TeraMetrics XD, Avalanche 220 and Reflector 220, and the Abacus 5000 Telephony Test System.

IMIX distribution suggestions were taken from BMWG members and the following paper: http://advanced.comms.agilent.com/insight/2001-8/TestingTips/1MxdPktSzThroughput.pdf