Roteadores de Serviços Integrados – CISCO ISR G2

Visão geral sobre Desempenho

Descrição do Conteúdo

Os roteadores de serviços integrados de nova geração (ISR G2) proporcionam uma plataforma para serviços de conectividade WAN além de permitir serviços adicionais como comunicações unificadas, segurança e diversas aplicações para escritórios remotos. Esta plataforma foi projetada para suportar circuitos de acesso WAN existentes e oferecer o desempenho necessário para a transição para os serviços de acesso baseados em Ethernet.

Este documento discute a arquitetura de desempenho dos roteadores ISR G2 e apresenta informações específicas de desempenho a partir de distintas configurações de serviços. O objetivo é ajudar a entender os fatores que afetam o desempenho e a melhor maneira de usar os números divulgados para o correto dimensionamento de um roteador de acesso.

As informações de desempenho deste documento são divididas em duas seções. A primeira seção apresenta detalhes sobre os valores máximos de desempenho enquanto a segunda seção mostra dados para serem usados no design de uma rede em um ambiente real

Arquitetura para Serviços Integrados e Desempenho

Os roteadores da família ISR G2 foram projetados para oferecer serviços integrados com o maior desempenho para um escritório remoto. Os roteadores funcionam com o sistema operacional Cisco IOS® em uma CPU central usando recursos compartilhados de memória, permitindo ao processador alocar memória dinamicamente de acordo com as funções e serviços habiltados.

Os roteadores Cisco ISR G2 possuem dois hardwares com funções específicas

1) **Processador integrado para criptografia:**

   Trata-se de um co-processador dedicado a acelerar os serviços de criptografia em hardware. Alguns processos que são beneficiados por este hardware:

   - Segurança em IP (IPsec) usando o padrão Triple Digital Encryption Standard [3DES] ou Advanced Encryption Standard [AES])
   - Acesso remoto via SSL VPNs (Secure Sockets Layer Virtual Private Network)

   Este processador integrado minimiza a carga de processamento da CPU do roteador se encarregando dos complexos cálculos matemáticos dos algoritmos de criptografía enquanto a CPU se encarrega de identificar o tráfego para o processo de criptografia, da negociação das associações de segurança (SA) e o encaminhamento dos pacotes (criptografados ou não).

2) **Processador de Sinais Digitais (DSP):**

   Os DSPs são oferecidos através dos módulos PVDM3 que são opcionalmente instalados em slots internos de alguns modelos da família ISR G2. O PVDM3 alivia a carga da CPU do roteador por possuir CPU independente para recursos de voz como conferência, transcoding, conectividade com a rede pública (STFC) ou com um PABX.

Taxas sem perdas de pacote (NDR) e testes baseados na RFC 2544

Os testes de desempenho dos roteadores geralmente são baseados na RFC 2544 ou procedimentos similares . A RFC 2544 exige que os testes sejam executados a uma taxa sem perda de pacotes (NDR). Estes testes são realizados usando um tamanho de pacote fixo, geralmente de 64 bytes e os resultados são publicados em pacotes por segundo (pps). Os testes realizados neste documento tiveram o intuito de mostrar o desempenho da CPU e da capacidade de processamento de cada plataforma em geral. (Tabela 1)

Outra técnica popular de testes de desempenho também baseada no NDR, é executada com o tamanho máximo de pacote e apresentado como taxa de transferência (“throughput”) e os resultados apresentado em bits por segundo (bps)

A seguir os resultados obtidos com os testes de desempenho por modelo da familia ISR G2

Tabela 1. Desempenho do Cisco ISR G2 baseado na RFC 2544 (kpps and Mbps)

Plataforma	Cisco 860	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
kpps (pacotes com 64 bytes)	25	50	100	290	290	330	330
Mbps (pacotes com 1500 bytes)	197	198	1400	2770	2770	2932	3114
Plataforma	**Cisco 2911**	**Cisco 2921**	**Cisco 2951**	**Cisco 3925**	**Cisco 3925E**	**Cisco 3945**	**Cisco 3945E**
kpps (pacotes com 64 bytes)	352	479	579	833	1845	982	2924
Mbps (pacotes com 1500 bytes)	3371	3502	5136	6903	6703	8025	8675

Nos testes com NDR as plataformas podem processar e encaminhar os pacotes mais rápido que a banda agregada das interfaces que os modelos podem suportar. Nesta situação, todas as interfaces disponíveis são utilizadas na sua taxa máxima e o uso da CPU registrado.

Estes testes não tem a pretensão de fornecer uma indicação que como o roteador irá se comportar em um ambiente real. Os testes assumem que a CPU dos roteadores escalam linearmente até o ponto onde eles começam a descartar pacotes.

Outro ponto a considerar é que uma rede real utiliza pacotes de tamanho variado, aplicações como voz ou ACKs de TCP tendem a ser muito pequenos, entre 64 a 80 bytes, já aplicações de vídeo ou uma transferência de arquivos tendem a usar pacotes maiores (~1500 bytes). Ou seja, os testes com NDR que usam tamanho fixo de pacote não proporcionam uma visão do desempenho do roteador em um ambiente real de uso.

Desempenho dos Serviços de Segurança

Desempenho em segurança pode ser agrupado em duas categorias:

1) Segurança da conectividade: Baseados em IPsec ou SSL VPN
2) Proteção contra ameaças: Baseados em tecnologias de firewall

No caso de IPsec o foco está na escalabilidade e taxa de transferência (throughput), a taxa de transferência em IPsec é medida usando um único túnel com pacotes de 1400 bytes, sem o algoritmo "Secure Hash Algorithm (SHA)" ou autenticação "Message Digest Algorithm 5 (MD5)". O tamanho do pacote deve ser reduzido para contabilizar os bytes adicionais acrescentado no cabeçalho pelo IPsec.

No que diz respeito a segurança da conectividade, o governo dos Estados Unidos mantém um controle rígido na exportação de produtos que usam criptografía forte, tanto em termos de tecnologia como de desempenho. Como muito outros produtos, os roteadores ISR G2 estão sujeitos a esta regulamentação. No intuito de estar em conformidade com as exigências do governo americano e permitir a livre exportação para os países autorizados como o Brasil, tanto a licença temporária como a licença definitiva de segurança (SEC) são limitadas em desempenho e quantidade de túneis. Esta limitação é aplicada na quantidade de túneis e na taxa de transferência, sendo válido para os túneis com IPsec, SSL VPN, GETVPN ou o protocolo Secure Real-Time Transport Protocol (SRTP). Atualmente a limitação é de 170Mbps (85Mbps em cada direção) e 225 túneis, sendo este limite controlado pela licença de segurança (SEC). Para ultrapassar estes limites será necessário a ativação da licença HSEC (High-Performance Security) disponível para os modelos 2921 e superiores. Importante notar que para habilitar a licença HSEC é necessário habilitar previamente a licença de segurança (SEC)

Tabela 2 Desempenho para IPSEC por plataforma

Tabela 2. Desempenho máximo de IPsec por Plataforma

Plataforma	Cisco 860	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
IPsec em Mbps (apenas com licença SEC)	46	102	125	149	149	170	170
Plataforma	**Cisco 2911**	**Cisco 2921**	**Cisco 2951**	**Cisco 3925**	**Cisco 3925E**	**Cisco 3945**	**Cisco 3945E**
IPsec Mbps (com as duas licenças SEC e HSEC)	170	207	282	770	1494	848	1503

Uma das métricas utilizadas nos testes em segurança da conectividade é o número máximo de conexões. Esta métrica não é aplicável para os roteadores ISR G2 pois eles foram projetados para roteadores de acesso, instalado como um CPE (equipamento instalado no cliente) em um ambiente de serviços gerenciados, o que significa que na maioria das instalações em ambiente real, os roteadores irão utilizar uma quantidade pequena de túneis. No caso do IPsec um túnel é representado no roteador por uma interface virtual "Virtual Tunnel Interface (VTI)".

Tabela 3 indica a quantidade de túneis criptografados por plataforma

Tabela 3. Quantidade de túneis criptografados por plataforma

Plataforma	Cisco 860*	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
Túneis criptografados (com licença SEC)	5	20	50	150	150	150	150
Túneis SSL VPN	-	10	25	50	50	75	75
Plataforma	**Cisco 2911**	**Cisco 2921**	**Cisco 2951**	**Cisco 3925**	**Cisco 3925E**	**Cisco 3945**	**Cisco 3945E**
Túneis criptografados (com licença SEC)	225	225	225	225	225	225	225
Túneis SSL VPN	100	100	150	200	500	200	500
Túneis criptografados (com licenças SEC e HSEC)	-	900	1000	1500	3000	2000	3000

Nota: O modelo Cisco 860 não suporta SSL VPN

Proteção contra ameaças

No caso de proteção contra ameaças, os testes com Firewal são mais complexos que os outros tipos de testes discutidos neste documento. Uma das funcionalidades do Cisco IOS para esta proteção é o firewall baseado em zonas ou “Zone-Based Firewall (ZBF)”. ZBF é um serviço “stateful”, ou seja, que monitora e mantém o estado de todas as conexões TCP que passam por ele. Também possui múltiplos ALGs (Aplication Layer Gateway) que permitem inspecionar e monitorar aplicações e protocolos específicos além de inspecionar o tráfego entre as zonas. Portanto algumas metodologias de testes afetam o desempenho de forma significativa, pois para o teste de distintas aplicações são necessários ALGs específicos, cada um afetando os resultados de forma diferente. Muitas ferramentas de testes permitem a utilização de pacotes com cabeçalhos TCP, mas nunca completam o “handshake” e estabelecem um estado de monitoração. Em algumas situações, o firewall pode encarar esta situação como um ataque de indisponibilidade de serviço (DoS) pois esta situação raramente seria encontrada em um ambiente real a não ser que seja um ataque. O uso de UDP ou outros padrões de tráfego “stateless” também pode produzir resultados variados.

Nos testes realizados neste documento, o firewall foi configurado com duas zonas com todo o tráfego enviado entre elas. O tráfego gerado é “stateless” e usa a mesma porta UDP. O desempenho é medido na taxa de transferência máxima e com o número máximo de sessões simultâneas. Um elemento que influencia a métrica de sessões é a quantidade de memória instalada, para a elaboração deste documento foi utilizada a memória padrão de cada plataforma nos testes realizados.

A tabela 4 indica o desempenho de firewall por plataforma

Tabela 4. Desempenho de Firewall por plataforma

Plataforma	Cisco 860	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
Taxa de transferência máxima (Mbps)	30	43	54	530	530	569	625
Número máximo de sessões simultaneas (1000s)	0.3	0.5	1.1	50	50	63	63
Plataforma	**Cisco 2911**	**Cisco 2921**	**Cisco 2951**	**Cisco 3925**	**Cisco 3925E**	**Cisco 3945**	**Cisco 3945E**
Taxa de transferência máxima (Mbps)	676	801	1350	2567	6112	3133	7473
Número máximo de sessões simultaneas (1000s)	90	130	150	270	300	305	345

Reforçando que os dados apresentados nesta seção são indicações de desempenho máximo, não sendo adequados para uso em um ambiente real. Embora o roteador seja capaz de encaminhar mais de 1 Gbps de tráfego criptografado em um ambiente de testes este número não deve ser esperado em uma rede real, onde o tamanho dos pacotes varia e os roteadores não devem ser usados em sua capacidade máxima

O desempenho de Firewall varia de acordo com a natureza do tráfego, uma vez que o ZBF monitora o estado do tráfego além de aplicações e protocolos específicos.

Recomendações e Posicionamento sobre desempenho

Posicionamento sobre desempenho é uma tentativa de capturar os cenários mais comuns e fazer uma recomendação que atenda a grande maioria das exigências de mercado. Não é uma métrica que inclui todas as possibilidades muito menos uma limitação de utilização. Sempre haverá situações onde o desempenho do roteador pode exceder as recomendações dependendo dos serviços ou configurações específicas que podem também apresentar um desempenho abaixo destes limites.

Os testes de posicionamento foram realizados usando o tráfego IMIX. IMIX é uma combinação de pacotes com tamanhos distintos que visa simular o tráfego da internet. Apesar de não ser um padrão de mercado é o mais utilizado pelos fabricantes de ferramentas de testes. Cada fabricante tem sua própria versão do IMIX, mas as diferenças não são significativas.

Tamanho do Pacote

Para os testes dos roteadores ISR G2 foram utilizados dois tipos de tráfego IMIX

No caso dos testes sem criptografia, a seguinte combinação de pacotes foi utilizada:

- 15 pacotes de 1518 bytes (15%)
- 61 pacotes de 64 bytes (61%)
- 24 pacotes de 594 bytes (24%)

Na media, o tamanho do pacote fica em 409 bytes.
[(15 x 1518) + (64 x 61) + (24 x 594)] /100 = 409

Para os testes com criptografia o tamanho máximo de pacote foi reduzido para evitar fragmentação. Esta redução está de acordo com as melhores práticas em redes VPN que fixam o MTU em 1440 bytes em uma interface para permitir os bytes adicionais do cabeçalho IPsec.

- 15 pacotes de 1418 bytes (15%)
- 61 pacotes de 90 bytes (61%)
- 24 pacotes de 594 bytes (24%)

O tamanho do pacote fica em 410 bytes, na média
[(15 x 1418) + (61 x 90) + (24 x 594)] /100 = 410

Utilização da CPU

A grande maioria dos testes realizados em laboratório utilizaram as interfaces Ethernet integradas dos roteadores, mas no caso dos modelos Cisco 3900 foi necessário incluir mias interfaces devido a sua grande capacidade de processamento. As interfaces Ethernet são as que menos utilizam CPU, pois o roteador deve simplesmente trocar cabeçalhos MAC, já as interfaces seriais como T1/E1, discadas e outras exigem encapsulamento de nível 2 e portanto exigem mais ciclos da CPU.

Outro foco em reproduzir uma rede próxima ao ambiente real é medir a CPU do roteador. Os testes NDR usam a CPU entre 99 e 100%, pois este nível é o fator limitante em um desempenho máximo. Entretanto nenhuma rede em produção pode operar com este nível de utilização.

O tráfego em um ambiente real é em rajadas, não é homogêneo e consistente como um teste de laboratório. Os roteadores sob teste não precisam convergir protocolos de roteamento devido aos eventos que ocorrem em uma rede real. Um roteador operando com CPU a 99% de uso não seria capaz de lidar com estes eventos.

A maioria dos provedores de serviços programam alarmes de utilização da CPU entre 60 e 65%. Muitos clientes corporativos operam suas redes com a CPU entre 70 e 75%. Neste documento, para posicionamento dos roteadores ISR G2, foi utilizado o limite de uso da CPU em 75%.

Serviços do sistema operacional Cisco IOS

Um recente estudo indicou que o sistema operacional Cisco IOS em sua versão 12.4 possuia mais de 4000 funcionalidades conhecidas. A grande maioria dos clientes usam uma pequena parcela destas funcionalidades, geralmente apenas 5 delas, como listas de controle de acesso (ACL), qualidade de serviço (QoS), tradução de endereço de rede (NAT) e funcionalidades de segurança como firewall e criptografia, sendo estas últimas cobertas na seção de segurança deste documento.

Qualidade de serviço é uma técnica que prioriza tráfego em tempo real, ou seja, sensível a latência, perda de pacotes e atrasos. Nos testes de QoS foi utilizada a técnica hierárquica (HQoS) que usa uma política de hierarquia superior, geralmente com um limitador de banda (shaper) e políticas de hierarquia inferior para identificar e enfileirar o tráfego de acordo com a política estabelecida pela hierarquia superior. A configuração usada nos testes foi de cinco classes de serviço na hierarquia superior e cinco políticas na hierarquia inferior.

Nos testes realizados, os pacotes de QoS foram marcados para classificação pelo gerador de pacotes e o roteador sob teste fez a classificação baseadas nestas marcações. Nenhum congestionamento foi simulado para forçar o enfileiramento para evitar perda de pacotes.

Tabela 5 Informação sobre desempenho de HQoS por plataforma

Tabela 5. Desempenho de HQoS por plataforma com tráfego IMIX e CPU a 75%

Plataforma	Cisco 860*	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
Mbps	-	45	64	110	110	120	125
Plataforma	Cisco 2911	Cisco 2921	Cisco 2951	Cisco 3925	Cisco 3925E	Cisco 3945	Cisco 3945E
Mbps	125	168	293	455	1368	572	1704

*** HQOS não é suportado no modelo 860**

Uma das funções principais do NAT é a de trocar o endereço IP dos pacotes que entram e saem de uma rede privada para proteger os endereços IP privados usados em um ambiente corporativo e permitir a comunicação na internet com endereços públicos. NAT pode usar mapeamento estático ou dinâmico ou uma combinação dos dois.

A função de mapeamento de um endereço IP privado para vários endereços IP públicos é chamado de NAT "overload" ou Port Address Translation (PAT). Nos testes realizados neste documento foi utilizado PAT (Tabela 6)

Tabela 6. Desempenho de PAT por plataforma com tráfego IMIX e CPU a 75%

Plataforma	Cisco 860	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
Mbps	27	60	75	80	80	91	101
Plataforma	Cisco 2911	Cisco 2921	Cisco 2951	Cisco 3925	Cisco 3925E	Cisco 3945	Cisco 3945E
Mbps	114	138	275	418	1067	496	1334

As ACLs podem ser usadas para classificar ou filtrar o tráfego. Muitas funções do Cisco IOS utilizam ACLs para identificar o tráfego para os serviços que precisam ser implementados, por este motivo, utilizamos ACLs na maioria dos testes realizados

Posicionamento de Segurança

Recomendações de serviços de segurança são baseados em algumas considerações como tamanho do pacote, uso da CPU a 75%, efeito do estabelecimento das associações de segurança (SAs) e várias técnicas usadas como ZBF.

Tabela 7. Recomendações de desempenho para serviços de segurança

Plataforma	Cisco 860*	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
Túneis IPsec	5	20	50	150	150	150	150
IPsec (Mbps)	6	20	30	35	35	48	53
Plataforma	**Cisco 2911**	**Cisco 2921**	**Cisco 2951**	**Cisco 3925**	**Cisco 3925E**	**Cisco 3945**	**Cisco 3945E**
Túneis IPsec	225	400	500	750	1500	1000	2000
IPsec (Mbps)	61	72	103	154	477	179	670

Combinações de Serviços e Posicionamento

Testes com um único serviço habilitado mostra o efeito da funcionalidade do Cisco IOS nos fluxos padrões de tráfego. A maioria dos clientes implementam vários serviços simultâneos. Teste com vários serviços habilitados mostra o efeito do desempenho de vários algoritmos operando simultaneamente e o efeito de cada serviço entre si. A tabela 8 mostra o desempenho das plataformas com serviços de QoS, ACLs e NAT habilitados simultaneamente.

Tabela 8. Desempenho por plataforma com NAT, ACL, QoS com tráfego IMIX e CPU a 75%

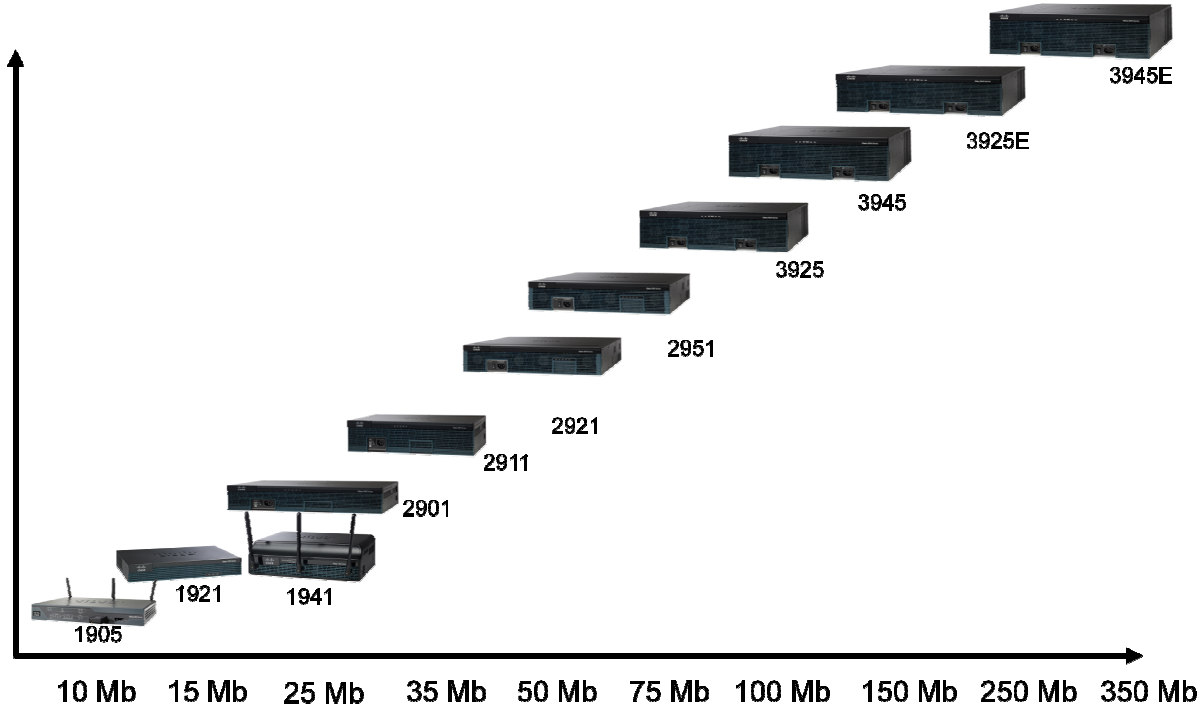
Plataforma	Cisco 860*	Cisco 880	Cisco 890	Cisco 1905	Cisco 1921	Cisco 1941	Cisco 2901
Mbps	-	30	45	68	68	76	77
Plataforma	**Cisco 2911**	**2921**	**2951**	**3925**	**3925E**	**3945**	**3945E**
Mbps	81	105	114	198	534	223	668

* Cisco 860 não é recomendado para os serviços testados

O posicionamento de desempenho é baseado nos resultados dos testes com uma variedade de serviços habilitados. Ao realizar vários testes com serviços distintos e medir o desemepenho do roteador é possível determinar uma média que atenda a maioria dos casos utilizados em redes em produção. Esta métrica é tanto uma métrica de posicionamento como uma recomendação Cisco. Vale ressaltar que o posicionamento de desempenho não é um limitante de uso e os clientes podem perceber números de desempenho maiores do que os indicados de acordo com a configuração usada em seu ambiente.

A figura 1 é uma recomendação de posicionamento que atende a grande maioria de clientes de médio e grande porte, onde foi considerado a largura de banda utilizada na WAN por cada plataforma com vários serviços habilitados. Mais uma vez, não é um limitante e sim uma recomendação para ajudar no posiconamento de cada plataforma.

Figure 1. Posicionamento de Desempenho com serviços habilitados por plataforma



Conclusão

O desempenho do roteador pode ser medido usando taxas de transferência máxima ou resultados NDR para verificar a capacidade máxima da CPU em encaminhar os pacotes, mas sem nenhuma informação específica sobre os algoritmos de software, reconhecimento de aplicações ou outros serviços.

Uma outra alternativa é medir o desempenho com vários serviços habilitados para produzir resultados que os técnicos possam projetar e atualizar os roteadores de suas próprias redes (ambiente real).

Os roteadores ISR G2 foram projetados para oferecer o máximo desempenho com diversos serviços integrados em um escritório remoto ou qualquer rede de acesso WAN. Conforme explicado neste documento o desempenho pode variar de acordo com os serviços configurados, os pacotes utilizados e os ciclos de CPU disponíveis.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-595485-00 04/10