

# Executando Listas de acesso em Cisco 12000 Series Internet Router

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Visão Geral do Suporte ACL no Cisco 12000 Series Internet Router](#)

[ACLs com base em ASIC versus ACLs com base em CPU](#)

[Controle e gerenciamento da filtragem de plano](#)

[Configurando ACLs de caminho de recebimento de IP](#)

[Suporte IPv4 ACL por tipo de placa de linha](#)

[Mecanismo 0 – Processamento de ACL](#)

[Engine 1 – Processamento de ACL](#)

[Mecanismo 2 - Processamento de ACL](#)

[Mecanismo 3 do ISE \(IP Services Engine\) - Processamento de ACL](#)

[Mecanismo 4 \(POS\) - Processamento de ACL](#)

[Mecanismo 4+ \(POS e DPT\) – Processamento de ACL](#)

[Mecanismo 4+ \(Ethernet\) - Processamento ACL](#)

[Registro de ACL](#)

[IPv4 Saída ACL – Matriz de interoperação de placa de linha](#)

[Suporte ACL de IPv6](#)

[Referência a comandos de ACL do Cisco 12000](#)

[Glossário](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento descreve o apoio para o Access Control Lists (ACLs) nos Cisco 12000 Series Internet Router.

## [Pré-requisitos](#)

## [Requisitos](#)

Cisco recomenda que você tem o conhecimento dos princípios de como um ACL trabalha em um roteador Cisco.

Refira estes documentos para obter informações gerais sobre dos ACL e dos seus aplicativos:

- [Lista de controle de acesso: Vista geral e diretrizes](#)
- [Configurando Serviços IP: Pacotes IP do filtro](#)

## Componentes Utilizados

A informação neste documento é baseada em Cisco 12000 Series Internet Router.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Visão Geral do Suporte ACL no Cisco 12000 Series Internet Router

No Cisco 12000 Series Internet Router, os ACL podem ser processados no hardware (circuitos integrados do aplicativo específicos - ASIC), no software (o CPU de uma placa de linha), ou como uma característica híbrida – processados no software com assistência de hardware. Se um ACL está processado no hardware ou no software depende do aplicativo ACL, do tipo de Engine da placa de linha, e da interação dos ACL em outras placas de linha.

Os mecanismos de placa de linha do Cisco 12000 Series fornecem diferentes recursos de ACL. Para a informação da sustentação ACL para um motor particular da placa de linha, vá à seção correspondente neste documento.

**Nota:** O Protocolo IP multicast ACL não é apoiado no Software Release 12.0S de Cisco IOS®. A característica do limite do Protocolo IP multicast pode ser usada onde o filtragem de transmissão múltipla é exigido. Refira o [Multicast Forwarding do caminho rápido no Engine 2 do Cisco 12000 Series e nas placas de linha ISE](#) para mais informação.

## ACLs com base em ASIC versus ACLs com base em CPU

O Cisco 12000 apoia todas as gerações de processamento ACL. Uma compreensão operacional de como cada um destes modos de processamento trabalha, interage, e se apoia é essencial ao uso eficaz ACL no Cisco 12000.

As gerações anterior de processamento ACL usaram um CPU programável para processar o ACL. Ao longo do tempo, os requisitos de processamento do pacote por segundo (PPS) excederam a capacidade de CPU novos para prosseguir. Os ASIC foram construídos para conseguir umas taxas mais altas PPS para a transmissão e as potencialidades de recursos do roteador. Os ACL que foram carregados no line card (LC) CPU foram carregados então no LC ASIC. Os ASIC continuaram a ser improvisados para segurar umas taxas mais altas PPS. Este a segunda geração ASIC foi construída no trabalho de abertura de caminhos da geração antes, e

oferece mais potencialidades de ASIC. Porque o Cisco 12000 é uma plataforma de roteamento distribuída, a interação entre as várias gerações de processamento ACL pode criar alguma confusão operacional.

Os termos tais como o ACL baseada em ASIC, o ACL baseado em CPU, o caminho rápido, o trajeto lento, e os pontapés ASIC são usados durante todo este documento para ajudar a explicar o que ocorre com o processamento ACL. Estão aqui as explicações destes termos:

- ACL com base em ASIC (caminho rápido) — Os ACL são carregados e processados no hardware ASIC. O envelope de desempenho do ASIC determina a profundidade, o desempenho e as capacidades do ACL. O caminho rápido foi usado no trajeto para ilustrar a diferença entre o processamento com base em ASIC e o processamento feito no CPU de apoio. Mais o termo genérico, com base em ASIC, é usado neste documento.
- ACL CPU-baseados (trajeto lento) — Os ACL são processados no software na placa de linha CPU. Para os cartões da geração anterior (motor 0 e em alguns casos motor 1), toda a processar é feito no LC CPU. Os LC com base em ASIC executam o processamento ACL nos pacotes que punted do ASIC. O trajeto lento foi usado no passado para ilustrar como os pontapés ao LC CPU eram mais lentos do que o ASIC. Mais o termo genérico, CPU-baseado, é usado neste documento.
- Pontapés ASIC — Os ASIC têm envelopes de design restritos. Quando um pacote excede o envelope projetado, obtém punted do ASIC a ser processado no LC que apoia o CPU ou enviado até o route processor (RP). Pacotes ACLs punt com base em ASIC que caem fora do projeto do ASIC. Um exemplo é um ACL que tenha um ACE com um log ou umas palavras-chave de registro de entrada. As informações necessárias para registrar o pacote precisam ser processadas fora da ASIC e, por isso, o pacote é automaticamente apontado para fora da ASIC para a CPU LC e processado como uma ACL com base em CPU normal.

**Nota:** Quando você configura o Policy-Based Routing (PBR) com instruções compatível para combinar ACL, os ACL não devem combinar a porta de origem. O Gigabit Switch Router (GSR) não apoia o switching de hardware para o PBR com ACL que combinam a porta de origem. Provoca o processo que comuta e o desempenho GSR degrada.

## [Controle e gerenciamento da filtragem de plano](#)

O processador de roteador proporciona serviços do controle e do plano de gerenciamento na arquitetura distribuída do Cisco 12000 Series. Receba o trajeto ACL (rACLs) fornecem uma capacidade de filtração distribuída simples para o controle e o tráfego de gerenciamento destinado para o RP. Pode logicamente ser visto como uma camada adicional de Segurança que se aproveita das forças de uma arquitetura distribuída.

## [Configurando ACLs de caminho de recebimento de IP](#)

O rACL foi introduzido com um waiver especial no regulador de pressão da manutenção do Software Release 12.0(21)S2 de Cisco IOS®. É apoiado oficialmente no Cisco IOS Software Release 12.0(22)S. Refira o [IP recebem o ACL](#) para mais informação.

O Processador do Roteador fornece serviços de controle de tráfego aéreo na arquitetura distribuída da série Cisco 12000. A recepção ACL fornece capacidades de filtração para o tráfego de controle destinado para o RP, tal como atualizações de roteamento e perguntas do Simple Network Management Protocol (SNMP).

O rACL é considerado a fase 1 de um esforço da multi-fase para adicionar proteções novas ao controle e ao Gerenciamento do tráfego plano. Os realces novos da taxa limite estão sendo adicionados através das atualizações de software.

## Suporte IPv4 ACL por tipo de placa de linha

As placas de linha do 12000 Series fornecem diferentes capacidades de ACL por tipo de mecanismo. Esta seção descreve as potencialidades de ACL dos motores da placa de linha diferente. Para a informação da sustentação ACL para um motor particular da placa de linha, veja a seção correspondente deste documento.

Há algumas características gerais para todos os ACL (ASIC e CPU baseados):

- Somente uma ACL pode ser aplicada a uma interface para cada direção. Por exemplo, a relação POS 0/0 pode ter somente uma entrada ACL e um emissor ACL.
- Os testes do pacote em relação a uma ACL param quando uma correspondência é localizada. Se um ACL que seja 300 entradas longas combina o pacote na entrada de lista de acesso (ACE) #45, a seguir o pacote está processado e o processamento ACL é parado.
- Há um implícito **nega toda a** entrada no fim de cada ACL. Em consequência, se não há nenhum fósforo no ACL, o pacote obtém deixado cair. Cisco ACL é criado com a *arquitetura de ACL de permissão explícita*. Isto significa que deve haver um ACE para combinar o pacote para que esteja processado e enviado.
- os ACE Novo-adicionados são adicionados sempre ao fim do ACL. Sempre que o ACL exige atualizações, é uma boa prática remover o ACL (use o **comando no access-list**) e adicionar novamente o ACL novo.
- Porque os fragmentos NON-iniciais IP não contêm a informação de protocolo da camada 4 no cabeçalho IP, simplesmente os critérios de verificação de repetição de dados padrão são apoiados para fragmentos não iniciais. Os detalhes completos em como Cisco ACL segue com a filtração do fragmento IP podem ser encontrados nas [listas de controle de acesso e nos fragmentos IP](#).
- Os ACL numerados estão processados e aplicados assim que forem entrados através do comando line interface(cli). Com grandes ACL, isto conduz às vezes a um aumento de CPU no RP ou no LC CPU.

## Mecanismo 0 – Processamento de ACL

O motor 0 é a primeira placa de linha entregada para o Cisco 12000. É todo o processamento baseado em CPU e transmissão. Daqui, as placas de linha do motor 0 processam ACL no LC CPU.

Estas placas de linha são baseadas no motor 0:

Tipo da placa de linha	Tipo de interface	Conectividade
12 x DS3	Coaxial	SMB
12 x DS3	Coaxial	SMB
12 x E3	Coaxial	SMB
1xCHOC12->DS3		IR

1xCHOC12/STM4 ->OC3/STM1	POS	IR
4xOC3c/STM1c	POS	SR
4xOC3c/STM1c	POS	LR
4xOC3c/STM1c	POS	MM
1xOC12c/STM4c	POS	IR
1xOC12c/STM4c	POS	MM
6xCT3->DS1		SMB
2xCHOC3/STM1- >DS1/E1		IR
4xOC3c/STM1c	ATM	IR
4xOC3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	IR
1xOC12c/STM4c	ATM	MM

### [Critérios de correspondência suportados](#)

Todo o padrão, ACL estendido, e turbocompressor ACL do Cisco IOS Software Release 12.0S são apoiados no motor 0.

### [Número de ACE apoiados](#)

O tamanho ACL é limitado somente por requisitos de desempenho e por recursos de memória disponível.

### [Processamento de saída ACL](#)

ACLs de saída são processadas no caminho do recurso de ingresso das outras placas de linha do sistema. Um impulso do emissor ACL ao lado do ingresso dos outros LC protege o backplane dos pacotes da transmissão que estão indo ser deixados cair. Esta é uma função herdada da arquitetura distribuída no Cisco 7500. Uma explicação detalhada, as razões, e as diretrizes operacionais são fornecidas no [emissor ACL do IPv4 - matriz entre operações de line card](#).

### [Comandos do específico da placa de linha](#)

Nenhum.

### [Diretrizes operacionais e interações de placa de linha](#)

- Se o Netflow está configurado em uma placa de linha do motor 0 e um emissor ACL está configurado em um Engine 3 da saída ou em uma placa de linha 4+, o emissor ACL está processado pelas placas de linha do ingresso e da saída a fim permitir que o Netflow esclareça os pacotes negados por ACL assim como por pacotes enviados.

### [Recomendações](#)

Cisco recomenda o uso do turbocompressor ACL no motor 0 para grandes ACL. ACLs lineares pequenos são mais eficazes para ACLs menores porque os ACLs turbo precisam de memória extra.

## [Engine 1 – Processamento de ACL](#)

### [Visão geral](#)

A placa de linha do motor 1 é uma ponte entre o processamento baseado em CPU no motor 0 e a transmissão da primeira geração/característica ASIC no processo ACL das placas de linha do motor 1 do motor 2. no software à revelia. Com Cisco IOS Software Release 12.0(10)S e Mais Recente, o motor 1 fornece o hardware ACL para os cartões equipados com as versões 4 ou 5 da salsa ASIC (veja a referência de comandos da placa de linha abaixo para determinar com que versão da salsa uma placa particular é equipada).

Estas placas de linha são baseadas no motor 1:

<b>Tipo da placa de linha</b>	<b>Tipo de interface</b>	<b>Conectividade</b>
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
1xGE	SX,	GBIC:
1xGE	SX,	GBIC:
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4c	DPT	MM
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4c	DPT	MM

### [Critérios de correspondência suportados](#)

Todo o Cisco IOS Software Release 12.0S apoiou o padrão, estendido, e o turbocompressor ACL é apoiado no LC CPU (trajeto lento). Além, o motor 1 pode a entrada de processo ACL na salsa ASIC. A salsa ASIC trata a entrada ACL que processa junto com a consulta da rota, tendo por resultado o desempenho aumentado quando comparada ao processamento ACL Linear tradicional e ao processamento ACL do turbocompressor. A salsa ASIC não pode as saídas de processo ACL ou a secundário-relação ACL.

### [Número de ACE apoiados](#)

O tamanho ACL é limitado somente por requisitos de desempenho e por recursos de memória disponível.

## Processamento de saída ACL

ACLs de saída são processadas no caminho do recurso de ingresso das outras placas de linha do sistema. Veja o [emissor ACL do IPv4](#) - Seção da [matriz entre operações de line card](#) para mais informação.

## Comandos do específico da placa de linha

- **access-list hardware salsa**
- **mostre o controlador I3 | inclua o ASIC**

## Diretrizes operacionais e interações de placa de linha

- O Salsa ASIC e PSA ASIC não podem ser operados simultaneamente. O comando access-list hardware aceita apenas PSA (Engine 2) ou Salsa (Engine 1), mas não ambos.
- Se o Netflow está configurado em uma placa de linha do motor 1 e um emissor ACL está configurado em um Engine 3 da saída ou em uma placa de linha 4+, o emissor ACL está processado pelas placas de linha do ingresso e da saída a fim permitir que o Netflow esclareça os pacotes negados por ACL assim como por pacotes enviados.

## Recomendações

Para as placas de linha das versões de Engine 1 que não apoiam o hardware ACL, Cisco recomenda o uso do turbocompressor ACL para grandes ACL. ACLs pequenas (com menos de 20 linhas) podem ser implementadas com ACLs lineares para conservar memória.

## Mecanismo 2 - Processamento de ACL

### Visão geral

O Engine 2 foi a primeira placa com um ASIC de encaminhamento/recurso. Com Cisco IOS Software Release 12.0(10)S e Mais Recente, as placas de linha do Engine 2 fornecem potencialidades ACL de hardware no ASIC de switching de pacote de capacidade elevada (PSA). Como com toda a transmissão/característica ASIC, desempenhos restritos compreende limite de lugar na capacidade do ASIC. O envelope do desempenho chave no Engine 2 ACL é devido às limitações de memória no PSA ASIC.

O encaminhamento de pacote no Engine 2 é feito pelo PSA ASIC. O PSA tem três memórias externas principais:

- PLU (PATH-consulta) — Usado para armazenar Nós do mtrie
- TLU (consulta da tabela) — Usado para armazenar MENTIR as folhas e possivelmente as estruturas do loadbalance. Igualmente usado para guardar muitas das estruturas de dados PSA ACL
- SRAM — O local principal para estruturas da compartilha carga

Os recursos ACL PSA são uma aplicação microcódigo-baseada da verificação ACL. Um grupo especial de instruções é carregado na microplaqueta PSA que permite a verificação básica ACL. Há um número de limitações a esta característica que deve com cuidado ser compreendida antes

de distribuir. Um inconveniente principal a PSA ACL é a grande quantidade de memória do encaminhamento de hardware exigida.

Os recursos ACL PSA exigem um grande bloco de memória PLU/TLU PRE-ser atribuídos apesar do número de prefixos, etc. Porque esta atribuição vem primeiramente da área TLU, tem um impacto significativo no número de rotas que podem ser mantidas nestes cartões quando o PSA ACL é configurado.

Além do que as despesas iniciais da memória PLU/TLU, cada prefixo armazenado na memória de TLU exige significativamente mais memória. A quantidade de memória requerida para cada prefixo varia, com base no sentido do ACL aplicado (ingresso contra a saída) e do tipo da placa de linha. Geralmente, a saída ACL exige mais memória do que o ingresso, e as placas de linha com mais portas física exigem mais memória essa aqueles com menos portas.

No argumento onde a placa de linha do Engine 2 não usa ACL, as estruturas de dados para o ACL são construídas apesar dos ACL reais configurados. A fim mudar às estruturas NON-ACL menores, você deve não configurar **nenhum hardware PSA da lista de acesso** no roteador. Este comando desabilita todo o processamento ACL em todas as placas de linha Engine2 em todos os sentidos. Recommends de Cisco para usá-los com cuidado extremo.

## Visão geral

A fim fornecer o desempenho do processamento ACL que é independente de profundidade de compatibilidade, o Engine 2 ACL é integrado na tabela do encaminhamento de hardware. Veja abaixo para explicações em como isto pode impactar a escalabilidade do prefixo.

Estas placas de linha são baseadas no Engine 2:

Tipo da placa de linha	Tipo de interface	Conectividade
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM64c	Habilitador	SR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	ATM	IR
4xOC12c/STM4c	ATM	MM
8xOC3cSTM1c	ATM/TS	IR



8xOC3c/STM1c	ATM/TS	MM
3xGE	SX	GBIC:
3xGE	CWDM	GBIC:
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR

### [Critérios de correspondência suportados](#)

Todo o Cisco IOS Software Release 12.0S apoiou critérios de verificação de repetição de dados do padrão e do ACL estendido, exceto portas de origem da camada 4. As máscaras, as portas de origem descontínuas dos campos de precedência IP, e da camada 4 punted do PSA ASIC e são processadas no LC CPU.

### [Número de ACE apoiados](#)

Até cinco ACLs de entrada de 448 linhas no PSA. Um ACL pode ser configurado pela porta. Os ACL adicionais são administrados pela placa de linha CPU. Veja a seção das “limitações” abaixo para limitações em emissores ACL.

### [Processamento de saída ACL](#)

Um emissor ACL configurado nesta placa de linha será executado no caminho de recurso do ingresso das outras placas de linha no sistema. Veja o [emissor ACL do IPv4 - Matriz entre operações de line card](#) para detalhes.

### [Comandos do específico da placa de linha](#)

- **access-list hardware psa limit 128**
- **no access-list hardware psa**
- **psa bypass**
- **show access-list psa detail**
- **show access-list psa summary**
- **show controller psa feature**

### [Diretrizes operacionais e interações de placa de linha](#)

- O processamento ACL do caminho rápido exige estas circunstâncias ser estado conformes: O ACL aplicado está dentro do limite de 128 ou 448. O comprimento deve ser menos do que 128 ACE se o **comando access-list hardware psa limit 128** é configurado. Quando o pacote de microcódigo de ACL de 448 linhas for necessário, o comprimento deve ser menor que 448 ACEs. A entrada e saída ACL não é configurada junto pelo cartão. Até cinco ACLs de saída

podem ser configuradas no roteador.

- Somente o 128-line ACL é apoiado 8- e em placas de linha 16-port OC-3/STM-1 POS. 448 ACLs de linha são suportados no POS OC-12/STM-4 de 4 portas, no POS OC-48/STM-16 de 1 porta e em placas de linha de Gigabit Ethernet de 3 portas.
- As entradas ACL tomam a prioridade no caminho rápido sobre emissores ACL quando ambos são configurados simultaneamente no mesmo cartão (o emissor ACL está processado no trajeto lento).
- Se um emissor ACL está configurado em um cartão do Engine 2, e a placa de linha do ingresso é o motor 0/1/2/4, um emissor ACL estará processado na placa de ingresso. Para outros tipos de Engine, o emissor ACL será processado no trajeto lento da saída do Engine 2.
- Os emissores ACL não são apoiados para o tráfego IP-à-MPLS (primeira etiqueta MPLS “que está sendo empurrada” em um pacote IP).
- A informação do processamento ACL é integrada no hardware MENTE e pode impactar a escalabilidade do prefixo. A exaustão da memória do prefixo é relatada por falhas de alocação de memória com a assinatura “exmem=1” no mensagem de registro de acompanhamento.

## Recomendações

- A informação do processamento ACL é integrada na tabela do forwarding CEF, que reduz a escalabilidade do prefixo. Os aplicativos que não usam ACL podem desabilitar o apoio ACL na tabela de CEF e desse modo aumentar a memória disponível do prefixo emitindo o **comando no access-list hardware psa**.
- A configuração do **comando no access-list hardware psa** desabilita todo o processamento ACL por cartões do Engine 2 além do que a desabilitação do apoio PSA para ACL. Não força a execução do software dos ACL. Essa condição também se aplica caso a placa de ingresso de saída tenha um ACL de saída configurado.
- A configuração do **comando access-list compiled** depois que o **comando access-list hardware psa** converte os ACE que excedem a capacidade do PSA em um turbocompressor ACL. Isto dá um desempenho de ACL ótimo para ACLs acima de 448 ACEs de comprimento. O microcódigo ACL padrão é 128 (a partir da versão 12.0(14)S/ST do Software Cisco IOS). Se os ACL menores estão no uso e a capacidade do 448-line não está exigida, configurar o **comando access-list hardware psa limit 128** conserva a memória da transmissão (TLU), que melhora a escalabilidade do prefixo). O processamento ACL do turbocompressor deve ser permitido com o **comando access-list compiled** para ACL mais por muito tempo do que as linhas 129 junto com o **comando access-list hardware psa limit 128**. Esta combinação processa as primeiras linhas 128 no PSA ASIC e as linhas restantes com turbocompressor ACL, que aperfeiçoa o desempenho ao conservar enviando a memória.
- A placa de linha 4-port OC12 ATM não apoia entradas ACL, mas fornece a detecção do emissor ACL no microcódigo, que permite o processo de emissores ACL no trajeto lento.
- A placa de linha 8xOC3 ATM apoia por vc 128 a linha ACL com Cisco IOS Software Release 12.0(23)S e Mais Recente. Um máximo de 16 entradas ACL distintas pode ser configurado no caminho rápido. 448-input ACL é apoiado em uma base por voz no trajeto lento somente. As ACLs de saída não são suportadas.

## Mecanismo 3 do ISE (IP Services Engine) - Processamento de ACL

## [Visão geral](#)

O Engine 3 é a primeira placa de linha dupla da transmissão da fase. O Engine 3 possui ASICs de encaminhamento/recursos no caminho de ingresso e saída. Isso permite que as ACLs sejam colocadas no ASIC nos caminhos de entrada e de saída. Além, a estrutura do Engine 3 ASIC é uma disposição híbrida do encanamento/paralela. A estrutura ASIC executa o Ternary Content Addressable Memory de alta velocidade do processamento ACL paralelamente (TCAM), que fornece o processamento de taxa de linha até de 20K ACE pelo ingresso, e o 20K ACE pela saída.

Estas placas de linha são baseadas no Engine 3:

<b>Tipo da placa de linha</b>	<b>Tipo de interface</b>	<b>Conectividade</b>
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xCHOC12/STM4 ->OC3/STM1- >DS3/E3	POS	IR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
8xOC3/STM1c	POS	IR
8xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	IR
4xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	LR
1xOC48c/STM16 c	POS	SR
1xOC48c/STM16 c	POS	LR
1xCHOC48/STM16 ->STM4- >OC3/STM1- >DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	IR
4xOC12c/STM4c	ATM/IP	MM
4xGE	GE	
4xOC12c/STM4c	DPT	IR
4xOC12c/STM4c	DPT	XLR

## [Critérios de correspondência suportados](#)

Todo o padrão do Cisco IOS Software Release 12.0S e critérios de verificação de repetição de dados prolongados são apoiados no caminho rápido à exceção do log ACE que são processados pela placa de linha CPU.

## [Número de ACE apoiados](#)

- Alinhe a taxa que processa no ingresso e na direção de saída pela porta, pelo VLAN, pela subinterface do Frame Relay, e pela subinterface ATM. Até 20.000 ACEs estendidos por direção e por placa são suportados.
- Os critérios de verificação de repetição de dados para a fonte/porta do destino TCP/UDP “escala”, “It”, e “GT” são todos segurados no hardware usando “recursos do operador L4”.
- O número de operandos L4 distintos é limitado a 32 para toda a placa de linha. Os operadores da porta de origem são limitados a um máximo de seis.

## Processamento de saída ACL

Apoio nativo do caminho rápido para o emissor ACL da taxa de linha que processa no pacote transmitir-PATH que processa o ASIC. Veja o [emissor ACL do IPv4 - Matriz entre operações de line card](#) para detalhes.

## Comandos do específico da placa de linha

- o `tcam` do `<slot->` do módulo HW compila sem fusão! ---12.0(21)S3
- `nome do <interface da interface de hardware do show-access-list >`
- mostre o `[x/y]` do `int` pos do `cef | if_number inc`

## Diretrizes operacionais e interações de placa de linha

- Os pacotes que combinam ACE de registro são processados no trajeto lento.
- Pacotes que correspondem aos ACEs negados (acelerados para evitar a interrupção do sistema) são processados no caminho lento.
- Quando um ACL inclui um intervalo de endereço, o hardware usa a “escala chamada os ACE especial ACE” que exigem até três ACE.
- A fusão de ACL pode conservar recursos TCAM compartilhando ACE comuns através dos ACL individuais. Para determinar se um ACL está oculto, use o comando de interface de hardware `show-access-list`.
- Os contadores ACL não são apoiados para ACL fundidos. Com Cisco IOS Software Release 12.0(21)S3 e Mais Recente, a fusão de ACL pode ser desabilitada com o **comando `hw-module <slot -> tcam compile no-merge`**. A fim determinar se um ACL está fundido, use o **comando `show-access-list hardware interface`**.
- Se o Netflow está configurado em uma placa de linha do motor 0/1 e um emissor ACL está configurado em um Engine 3 da saída ou em uma placa de linha 4+, o emissor ACL estará processado pelas placas de linha do ingresso e da saída a fim permitir que o Netflow esclareça os pacotes negados por ACL assim como por pacotes enviados.

## Suporte de contador ACL

	Per-ACE	Per-ACE (hardware counters)	Aggregate
21S3/ST3		X	
22S		X	X
23S	X	X	X

### Definições:

- Por-ACE — O apoio normal do Cisco IOS Software, o comando **show access-list <number>** no RP/LC indica o ACL e o contador associados com cada ACE. Está disponível somente quando a **fusão** é desabilitada antes que você configure todos os ACL. Isto pode ser feito usando este comando configuration:  

```
Router(config)#hw-module slot <number> tcam compile acl no-merge
```

Esta opção quando permitida desliga algumas otimizações de combinação de TCAM e afeta a escalabilidade. O efeito exato depende dos ACLs individuais. Igualmente note que os contadores não estarão corretos se o roteamento baseado em política é aplicado nessa relação. Nesse caso, o contador agregado deve ser usado.
- Por-ACE (TCAM) — Contadores de hardware associados com cada entrada de TCAM. Nenhuma configuração é necessária e não há nenhum impacto no desempenho/escalabilidade. Disponível somente na placa de linha usando este CLI. Esses contadores não podem ser zerados pelo software.  

```
LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace
```

Um CLI genérico novo para este comando estará disponível no Cisco IOS Software Release 22S:  

```
LC-Slot4#show access-list hardware interface p0:1 in
```

Como com o contador por-ACE, os contadores TCAM são válidos somente quando o PBR não é usado nessa relação com ACL.
- Agregado — Cada ACL mostra que uma licença sumária/nega contra. É a soma de todos os contadores ACE individuais. Nenhuma configuração é necessária e não há nenhum impacto no desempenho ou na escalabilidade.

## Recomendações

Nenhum neste tempo.

## Mecanismo 4 (POS) - Processamento de ACL

### Visão geral

O motor 4 fornece este apoio ACL o Cisco IOS Software Release 12.0(18)S e Mais Recente:

- As ACLs de saída são suportadas nas placas de linha E0/1/2 se a placa de linha Engine 4 for a placa de entrada. Nesta configuração, o emissor ACL é processado pela placa de linha CPU da saída.

Estas placas de linha são baseadas no motor 4:

Tipo da placa de linha	Tipo de interface	Tipo de Engine	Conectividade
4xOC48c/ST M16c	POS	E4	
4xOC48c/ST M16c	POS	E4	LR
1xOC192c/S TM64c	POS	E4	IR
1xOC192c/S TM64c	POS	E4	SR
1xOC192c/S	POS	E4	VSR-1

TM64c			
10xGE	SFP	E4	

## Mecanismo 4+ (POS e DPT) – Processamento de ACL

### Visão geral

O motor 4+ introduz a funcionalidade ACL ao portfólio do Cisco 12000 Series 10-Gigabit.

Até 1024 ACEs são suportados em cada caminho de entrada e saída. Ambo a entrada e saída ACL é processada na linha taxa para até 96 ACE. O desempenho de compatibilidades maiores varia de acordo com a complexidade da compatibilidade.

Estas placas de linha POS são baseadas no motor 4+:

<b>Tipo da placa de linha</b>	<b>Tipo de interface</b>	<b>Conectividade</b>
4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	LR
1xOC192c/STM64c	POS	IR
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	LR
4xOC48c/STM16c	DPT	SFP:
1xOC192c/STM64c	DPT	IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LR

### Crítérios de correspondência suportados

Todo o Cisco IOS Software Release 12.0S apoiou o padrão e os critérios do ACL estendido são apoiados no caminho rápido à exceção do log ou do fragmento ACE.

### Número de ACE apoiados

Até 1024 ACEs são suportados por direção no caminho rápido.

**Nota:** 1021 dos ACEs são configuráveis. Três entradas são reservadas para os comandos **permit ip any any**, **deny ip any any**, e **send to CPU** implícitos ACE.

Não há limite máximo para o número de ACEs suportados. Todos os ACE além do limite 1021 são executados no trajeto lento da placa de linha.

### [Processamento de saída ACL](#)

Os ACLs de saída são processados no caminho rápido do lado de transmissão. Veja o [emissor ACL do IPv4 - Matriz entre operações de line card](#) para detalhes.

### [Comandos do específico da placa de linha](#)

- mostre o `tcam appl [ACL-em / ] tcam ACL-para fora <label-nenhum >`
- mostre o `tcam appl [ACL-em / ] <number do <port> da memória ACL-para fora das entradas >`

### [Diretrizes operacionais e interações de placa de linha](#)

- a Secundário-relação ACL não é apoiada.
- O desempenho varia com profundidade do fósforo.
- Entradas de intervalo usam duas regras de ACL (três se as duas entradas cruzarem um limite).
- Um ACL por interface física é suportado .
- Até 1024 ACE (pelo sentido) são apoiados no caminho rápido.
- Algum 1024 do caminho rápido ACE pode ser compartilhado através das portas.
- Os ACE que usam a palavra-chave do fragmento são filtrados no trajeto lento.
- Os pacotes negados não são contados para ACE que estão sendo processados no trajeto lento.
- Se o Netflow está configurado em uma placa de linha do motor 0 e um emissor ACL está configurado em um Engine 3 da saída ou em uma placa de linha 4+, o emissor ACL estará processado pelas placas de linha do ingresso e da saída para permitir que o Netflow esclareça os pacotes negados por ACL assim como por pacotes enviados.

### [Recomendações](#)

Nenhum neste tempo.

## [Mecanismo 4+ \(Ethernet\) - Processamento ACL](#)

### [Visão geral](#)

As placas de linha dos Ethernet do motor 4+ introduzem a funcionalidade da entrada ACL de por-VLAN no hardware ao portfólio dos Ethernet de 10 Gigabit do Cisco 12000. Estes são algumas das características:

- A entrada e saída ACL pode ser aplicada simultaneamente em uma porta única sem um

impacto no desempenho.

- Os ACL podem ser aplicados pelo VLAN ou pela porta.
- O desempenho da entrada ACL até 15K ACE não degrada com profundidade do fósforo.
- Os emissores ACL são processados na linha taxa para até 96 ACE. O desempenho de compatibilidades maiores varia de acordo com a complexidade da compatibilidade.

Estas placas de linha dos Ethernet são baseadas no motor 4+:

Tipo da placa de linha	Tipo de interface	Tipo de Engine
10xGE Rev B ("X-B")	SFP:	E4+
Modular	SFP:	E4+
1x10GE	10G	E4+
1x10GE	10G	E4+

### [Critérios de correspondência suportados](#)

Todo o Cisco IOS Software Release 12.0S apoiou o padrão e os critérios do ACL estendido são apoiados no caminho rápido à exceção do log ou do fragmento ACE.

### [Número de ACE apoiados](#)

- Até 15,000 entradas ACL que podem ser configuradas pela porta ou pelo VLAN.
- 1024 output ACE pelo cartão que pode ser aplicado em uma base por porto. **Nota:** 1021 dos ACEs são configuráveis. Três entradas são reservadas para os comandos **permit ip any any**, **deny ip any any**, e **send to CPU** implícitos ACE.

### [Processamento de saída ACL](#)

As ACLs de saída são processadas originalmente no caminho rápido no lado de transmissão. Veja o [emissor ACL do IPv4 - Matriz entre operações de line card](#) para mais informação.

### [Comandos do específico da placa de linha](#)

- fusão do <number> IP acl do hw-module slot

### [Diretrizes operacionais e interações de placa de linha](#)

- Os ACE que contêm a palavra-chave do fragmento são processados no trajeto lento.
- Os contadores ACL não são apoiados para os ACL combinados com os outros recursos.
- Os contadores ACL não são apoiados para ACL fundidos. Os ACL fundidos são configuráveis com o comando **hw-module slot <slot number> ip acl merge**.
- As operações ascendentes to168 L4 são apoiadas pela placa de linha. Uma vez que isto é excedido, o ACL está executado no trajeto lento.
- Se uma placa de linha do motor 1 tem o Netflow exemplificado permitido e um emissor ACL está permitido em um Engine 3 da saída ou em uma placa de linha 4+, o emissor ACL está processado pelas placas de linha do ingresso e da saída a fim permitir que o Netflow



esclareça os pacotes negados por ACL assim como por pacotes enviados.

## Recomendações

Nenhum neste tempo.

## Registro de ACL

Antes do Cisco IOS Software Release 12.0(21)S, a informação do logging ACL foi enviada ao RP exclusivamente sobre o barramento de manutenção (MBUS). Durante níveis altos da atividade do logging ACL, era possível exceder a capacidade do MBUS. O Cisco IOS Software Release 12.0(21)S introduz diversas otimizações que impedem esta encenação.

As situações de sobrecarga de MBUS são relatadas pelo Cisco IOS Software com estes Mensagens de Erro:

LCLOG-3-INVSTATE

MBUS\_SYS-3-SEQUENCE

Com Cisco IOS Software Release 12.0(21)S e Mais Recente, os mensagens de registro da severidade elevada (severidade 0-4) estão entregados ao RP com o MBUS quando os mensagens de registro da severidade mais baixa (severidade 5-7) forem entregados ao RP através da tela de switching de maior capacidade. Os mensagens de registro ACL são severidade elevada, assim são entregados agora ao RP através da tela de switching.

Isto funcionalidade de registro adicionada é configurável usando estes comandos:

- **[severity] de registro do mbus do método** — Determina que mensagens, pela severidade, serão enviadas ao RP usando o MBUS. Os Mensagens de severidade mais elevada serão enviados através do Switch Fabric.
- **show logging method** - Exibe o método de login atual para todos os níveis de gravidade da mensagem.
- **sequência-NUM de registro** — Este comando permite a placa de linha de emissão aos mensagens de registro do número de sequência de modo que as mensagens possam corretamente ser requisitadas novamente pelo RP. Sem este comando, os mensagens de registro podem ser entregados ao RP na ordem NON-sequencial.

## IPv4 Saída ACL – Matriz de interoperação de placa de linha

Antes que o processamento ACL da introdução à saída com a liberação do Engine 3 e do motor 4+, emissores ACL estiver processado pela placa de linha do ingresso. Os ACLs de saída foram atualizados para aproveitar os recursos de processamento de ACL de saída de alto desempenho do Engine 3 e do Engine 4+.

Esta carta fornece um sumário de onde os emissores ACL sejam processados para combinações da placa de linha diferente:

	Placa de linha da saída					
Placa de	E0	E1	E2	E3	E4	E4+

linha do ingresso (emissor ACL aplicado à interface membro)						
E0	Ingresso	Ingresso	Ingresso	Saída	n/a	Saída
E1	Ingresso	Ingresso	Ingresso	Saída	n/a	Saída
E2	Ingresso	Ingresso	Ingresso	Saída	n/a	Saída
E3	Saída	Saída	Saída	Saída	n/a	Saída
E4	Saída	Saída	Saída	Saída	n/a	Saída
E4+	Saída	Saída	Saída	Saída	n/a	Saída

## [Suporte ACL de IPv6](#)

Os ACL estendido do IPv6 são apoiados no trajeto lento (ingresso e saída) no E0, no E1, no E2, no E3, e no E4+ no Cisco IOS Software Release 12.0(23)S.

No Engine 3, a funcionalidade ACL do IPv6 é apoiada no hardware no Cisco IOS Software Release 12.0(25)S. Os ACL são aplicados a uma relação específica, com uma instrução de negação implícita na extremidade de cada lista de acessos. O IPv6 ACL é configurado usando o comando **ipv6 access-list** com a negação e permite palavras-chaves no modo de configuração global. Os cartões do motor 3-based apoiam a filtração de cabeçalhos de opção tráfego-baseados do IPv6, etiquetas do fluxo, e opcionalmente, tipo de protocolo de camada superior informação.

## [Referência a comandos de ACL do Cisco 12000](#)

### Comandos 1 do motor

- **access-list hardware salsa**
- **mostre o controlador I3 | inclua o ASIC**

### Comandos do Engine 2

- **access-list hardware psa limit 128**
- **no access-list hardware psa**
- **psa bypass**
- **show access-list psa detail**
- **show access-list psa summary**
- **show controller psa feature**

### Comandos do Engine 3

- **o tcam do <slot-> do módulo HW compila sem fusão! --- até à data do Cisco IOS Software Release 12.0(21)S3**
- **nome do <interface da interface de hardware do show-access-list >**

- mostre o contr [tofab/<int alfa acl do frfab] > vnr2ace

#### Comandos do motor 4+

- rótulo show access-list gen7
- mostre o tcam appl [ACL-em / ] tcam ACL-para fora <label-nenhum >
- mostre o tcam appl [ACL-em / ] ><number do <port da memória ACL-para fora das entradas >

#### Comandos ethernet do motor 4+

- fusão do <number> IP acl do hw-module slot

## Glossário

Esta seção fornece definições padrão de termos relevantes:

- Planos do Processamento – um dispositivo de rede pode ser logicamente dividido em três planos de processamento: Plano dos dados — Processamento nos pacotes que correm através do dispositivo de rede. Plano do controle — Processamento nos pacotes usados para colar junto dispositivos de rede. Isso inclui protocolos de linha (como os Protocolos PPP e HDLC), protocolos de roteamento (Protocolo BGP, Protocolo RIPv2, Protocolo OSPF e assim por diante) e protocolos de cronometragem (como o Protocolo NTP). Plano de gerenciamento — Processamento nos pacotes que são usados para controlar os dispositivos de rede. Isto inclui o telnet, o Shell Seguro (ssh), o File Transfer Protocol (FTP), o Trivial File Transfer Protocol (TFTP), o SNMP, e os outros protocolos de gestão.
- **Padrão ACL** — Filtro padrão ACL exclusivamente na camada 3.
- **ACL estendido** — As lista de acesso IP estendido usam endereços de remetente e destinatário para operações de harmonização assim como a informação opcional do tipo de protocolo para a granularidade mais fina do controle.
- **ACL processados Lineares** — Processado linearmente no software. O desempenho varia de acordo com a profundidade da correspondência (o número de entradas que precisam ser verificadas antes que uma correspondência seja determinada).
- **Turbocompressor ACL (compilado)** — O turbocompressor ACL aperfeiçoa o processamento ACL do software compilando um ACL em uma série de tabelas de consulta alto-aperfeiçoada que apressam o processamento do software. O desempenho das ACLs Turbo não varia com a complexidade de compatibilidade.
- **Entradas ACL** — Um ACL aplicou-se para traficar entrando na porta a que é aplicado.
- ACLs de saída - uma ACL aplicada ao tráfego que sai da porta em que é aplicada. Com algumas exceções, os emissores ACL são processados pela placa de linha da entrada.
- Receive Path ACLs - Receive Path ACLs fornecem filtragem para tráfego de controle destinado para o próprio roteador, como atualizações de roteamento e consultas de SNMP.
- **Dual a placa de linha da transmissão da fase** — Placas de linha que têm a transmissão/característica ASIC no ingresso e no trajeto da saída. Isto permite que a placa de linha execute características em ambos o fluxo do pacote de ingresso e fluxo do pacote de saída sem os pacotes punt ao LC CPU. Igualmente permite novas ondas de algoritmos de encaminhamento duplos da fase ser usado dentro do Cisco 12000. A placa de linha do Engine 3 é um exemplo de uma placa de linha dupla da transmissão da fase.
- **Placa de linha da transmissão do estágio único** — Placas de linha que têm a transmissão/característica ASIC apenas no caminho de ingresso. Estas placas de linha

executam somente o processamento com base em ASIC nos pacotes que fluem no caminho de ingresso. O tráfego de saída não é processado (apenas enviado), é segurado pelo ingresso ASIC de outros LC, ou controlado pelo LC CPU. O Engine 2, o motor 4, e o motor 4+ são exemplos de placas de linha da transmissão do estágio único.

## [Informações Relacionadas](#)

- [Cisco 12000 Series Internet Routers](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)