在 Cisco 12000 系列互联网路由器上实现访问列表

目录

简介

本文描述访问控制列表(ACL)的支持在Cisco 12000系列互联网路由器。

先决条件

要求

思科建议您有基础的知识ACL如何在Cisco路由器工作。

参考这些文档关于ACL和他们的应用程序的一般信息：

- 存取控制表：概述和指南
- 配置IP服务：过滤器IP信息包

使用的组件

本文档中的信息根据Cisco 12000系列互联网路由器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Cisco 12000 系列互联网路由器的 ACL 支持的概述

在Cisco 12000SERIES互联网路由器上， ACL可以处理在硬件(专用集成电路- ASIC)，软件(线路卡CPU)方面，或者作为一个混合的功能–处理在与硬件协助的软件方面。ACL是否在硬件或软件方面处理取决于ACL应用程序、线卡引擎类型和交互作用从ACL在其他线卡。

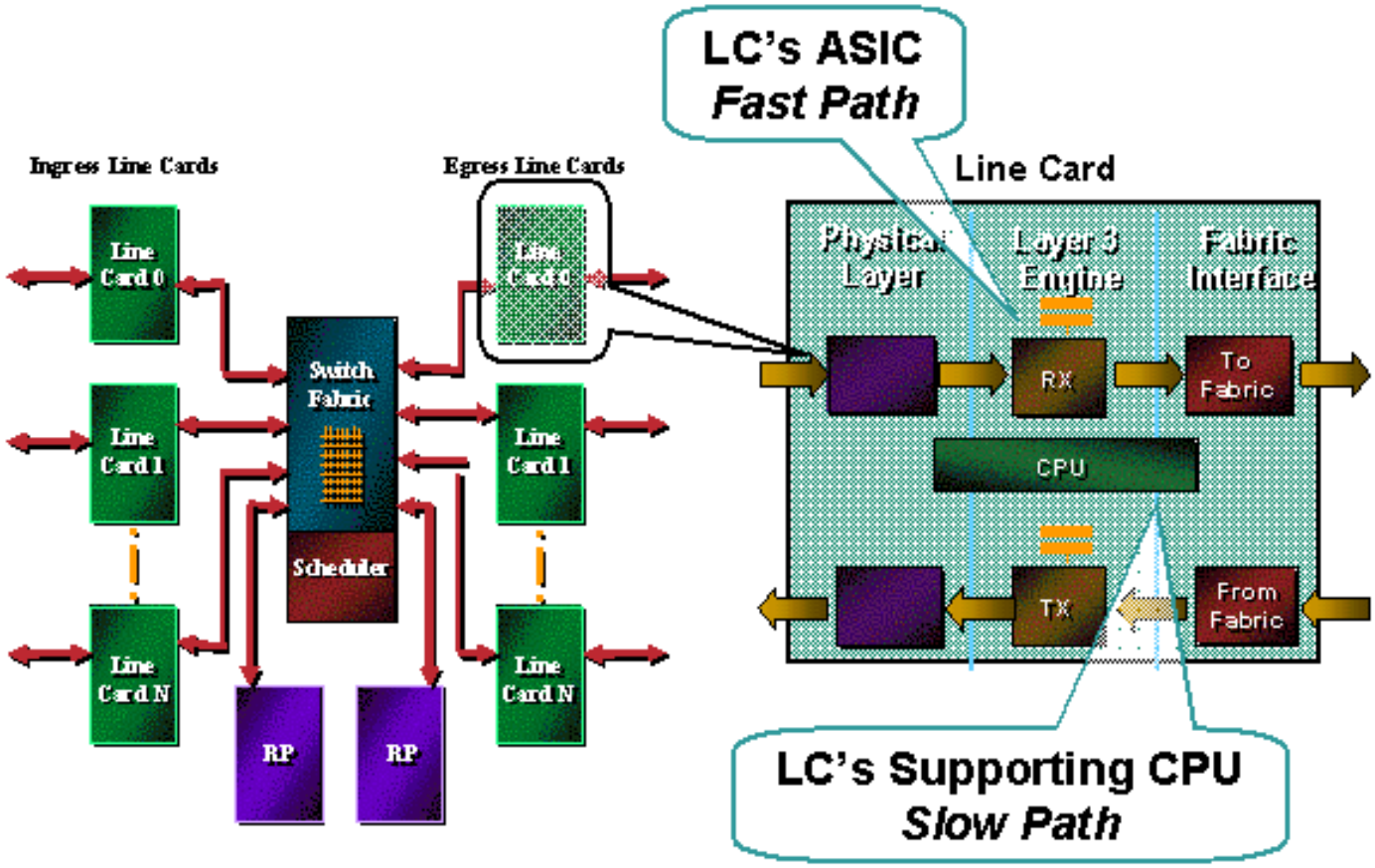
Cisco 12000系列线卡引擎提供不同的ACL功能。对于特定的线路卡引擎的ACL支持信息，请去在本文的对应的部分。

注意： Cisco IOS软件版本12.0S.不支持IP组播ACL可以使用Ip multicast boundary功能组播过滤要求的地方。参考在Cisco 12000系列引擎2和ISE线卡的Fast-Path组播转发欲知更多信息。

基于 ASIC 的ACL 与基于 CPU 的 ACL 的比较

Cisco 12000支持ACL处理的所有生成。可操作的了解这些处理的模式中的每一个如何工作，呼应，并且互相支持对在Cisco 12000的有效ACL使用是重要的。

ACL处理早期世代使用可编程的CPU处理ACL。随着时间的推移，数据包每秒(PPS)处理要求超出了新的CPU的能力跟上。ASIC被构件达到路由器转发和功能功能的更高的PPS速率。在线卡的ACL (LC) CPU装载然后装载在LC ASIC上。ASIC继续被即兴创作处理更高的PPS速率。这些第二代ASIC在生成的作早期工作在的工作被构件前面，并且提供更多ASIC功能。由于Cisco 12000是一个分布式路由选择平台， ACL处理之间的多种生成的交互作用能创建若干可操作的混乱。



术语例如基于ASIC的ACL、基于CPU的ACL、快速路径、慢路径和ASIC平底船用于在本文中帮助解释什么发生在ACL处理。这是这些期限的说明：

- 基于ASIC的ACL (快速路径) — ACL在ASIC硬件里装载并且处理。ASIC的性能信封确定ACL深度、性能和功能。快速路径用于路径说明在基于ASIC在LC-supporting CPU完成之间的处理和处理的区别。更多统称，基于ASIC，用于本文。
- 基于CPU的ACL (慢路径) — ACL在线路卡CPU的软件方面处理。早期世代卡(所有处理引擎0和在某些情况下的引擎1)，在LC CPU执行。基于ASIC LCs执行在从ASIC被踢的数据包的ACL处理。慢路径以前用于说明对LC CPU的平底船如何比ASIC慢。更多统称，基于CPU的，用于本文。
- ASIC踢— ASIC有严格设计信封。当数据包超出设计的信封时，从在LC将处理的ASIC踢给支持CPU或发送至路由处理器(RP)。基于ASIC的ACL踢ASIC的设计的外部落的数据包。有与日志或日志输入关键字的ACE的示例是ACL。记录数据包的需的信息需要ASIC的外部处理，因此数据包自动地被踢在ASIC外面，到LC CPU，并且处理类似正常基于CPU的ACL。

注意： 当您配置与匹配语句的基于策略的路由(PBR)匹配ACL时， ACL不应该匹配源端口。千兆交换路由器(GSR)不支持PBR的硬件交换与匹配源端口的ACL。它触发交换的进程，并且GSR性能降低。

控制和管理平面过滤

路由器处理器提供控制和管理层面服务在分布式体系结构Cisco 12000系列里。接收路径ACL (rACL)为控制提供一个简单分布式过滤被注定的功能和管理数据流为RP。它可以逻辑上查看作为利用分布式体系结构的力量安全的一块另外的层。

配置 IP 接收路径 ACL

rACL通过特殊放弃介绍到Cisco IOS软件版本12.0(21)S2维护节流孔。Cisco IOS软件版本12.0(22)S正式支持它。参考的IP接收ACL欲知更多信息。

路由器处理器在分布式体系结构提供控制层面服务Cisco 12000系列里。接收ACL为为RP注定的控制流量提供过滤功能，例如路由更新和简单网络管理协议(SNMP)查询。

rACL认为一多元状况的对平面数据流的控制和管理的努力添加新建的保护的阶段1。新的速率限制增强通过软件更新被添加。

线路卡类型提供的 IPv4 ACL 支持

12000系列线卡提供不同的ACL功能每种引擎类型。此部分描述不同线路卡引擎的ACL功能。关于特定的线路卡引擎的ACL支持信息，请参阅本文的对应的部分。

有所有ACL的某些一般特性(基于的ASIC和CPU) ：

- 仅一个ACL可以应用到接口为每个方向。例如， interface pos 0/0只能有一输入ACL和一个输出ACL。
- 在找到后，数据包的测试ACL的终止匹配。如果是长300个的条目的ACL匹配在访问列表条目(ACE) #45的数据包，则数据包处理，并且ACL处理被终止。
- 隐式**拒绝所有**条目在每个ACL结束时。结果，如果没有在ACL的匹配，数据包被撤销。思科ACL创建与*明确permit* ACL体系结构。这意味着必须有匹配的ACE能将处理和转发的它的数据包。
- 新加的ACE总是被添附对ACL的结尾。每当ACL要求更新，它是良好的做法删除ACL (请使用**no access-list命令**)和重新加写新的ACL。
- 由于非初始IP段不包含在IP报头的第4层协议信息，只有标准的匹配标准为??液初始分段支持。关于怎样的全面的详细信息思科ACL遵照IP分段过滤可以在访问控制列表和IP段找到。
- 当他们通过命令行界面(CLI)，被输入编号ACL处理并且应用。使用大ACL，这有时导致在RP或LC CPU的CPU峰值。

引擎 0 - ACL 处理

引擎0是为Cisco 12000传送的第一线卡。它是所有基于CPU的处理和转发。因此，引擎0线卡处理在LC CPU的ACL。

这些线卡根据引擎0 ：

卡类型	接口类型	连接
12个x DS3	同轴电缆	SMB
12个x DS3	同轴电缆	SMB
12 x E3	同轴电缆	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

支持的匹配标准

引擎0支持所有Cisco IOS软件版本12.0S标准、扩展ACL和涡轮ACL。

支持的ACE编号

ACL大小由性能要求和可利用的内存资源仅限制。

输出ACL处理

输出ACL在其他线卡的入口功能路径在系统的处理。输出ACL的推送对另一个LCs的入口侧的保护从丢弃的转发数据包的背板。这是从分布式体系结构的一个被继承的功能在Cisco 7500。详细说明、原因和可操作的指南在IPv4输出ACL提供-线卡互操作矩阵。

线卡特定命令

无。

可操作的指南和线卡交互作用

- 如果Netflow在引擎0线卡配置，并且输出ACL在出口引擎3或4+配置线卡，输出ACL由入口和出口线路卡处理为了允许Netflow占ACL以及转发的数据包拒绝的数据包。

建议

思科推荐使用在引擎0的涡轮ACL大ACL的。因为涡轮ACL要求额外内存，小线性ACL是更加小的ACL的更有效的。

引擎 1 - ACL 处理

概述

默认情况下引擎1线卡是在基于CPU的处理在引擎0和第一代转发/功能ASIC之间的一网桥在引擎2.引擎1线卡进程ACL在软件方面。使用Cisco IOS软件版本12.0(10)S和以后，引擎1提供硬件ACL为卡配备有萨尔萨ASIC的版本4或5 (请参阅下面线卡命令参考确定与萨尔萨哪个版本特定卡被装备)。

这些线卡根据引擎1 ：

卡类型	接口类型	连接
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

支持的匹配标准

LC CPU (慢路径)支持所有Cisco IOS软件版本12.0S支持的标准，扩展和涡轮ACL。另外，引擎1能在萨尔萨ASIC的进程输入ACL。萨尔萨ASIC处理处理与路由查找一起的输入ACL，造成更完善的性能，当与传统线性ACL处理和Turbo ACL处理比较。萨尔萨ASIC不能进程输出ACL或sub-interface ACL。

支持的ACE编号

ACL大小由性能要求和可利用的内存资源仅限制。

输出ACL处理

输出ACL在其他线卡的入口功能路径在系统的处理。请参阅IPv4输出ACL -线卡互操作矩阵部分欲知更多信息。

线卡特定命令

- **访问列表硬件辣调味汁**
- **show controller l3|包括ASIC**

可操作的指南和线卡交互作用

- 萨尔萨ASIC和PSA ASIC不可能同时操作。**access-list hardware命令**只接受PSA (引擎2)或萨尔萨(引擎1)，但是不是两个。
- 如果Netflow在引擎1线卡配置，并且输出ACL在出口引擎3或4+配置线卡，输出ACL由入口和出口线路卡处理为了允许Netflow占ACL以及转发的数据包拒绝的数据包。

建议

对于的引擎1线卡版本不支持硬件ACL，思科推荐使用大ACL的涡轮ACL。斯莫尔ACL (少于20条线路)可以实现作为线性ACL保存内存。

引擎 2 - ACL 处理

概述

引擎2是与转发/功能ASIC的第一线卡。使用Cisco IOS软件版本12.0(10)S和以后，引擎2线卡提供硬件在高性能Packet Switching ASIC (PSA)的ACL功能。如同所有转发/功能ASIC，严格性能包围在ASIC的功能的地方限定范围。在引擎2 ACL的关键性能信封归结于在PSA ASIC的内存限制。

信息包转发在引擎2方面由PSA ASIC完成。PSA有三个主要外部内存：

- PLU (PATH查找) —用于存储mtrie节点
- TLU (表查找) —用于存储FIB分支和可能负载均衡结构。并且曾经拿着许多PSA ACL数据结构
- SRAM —负载分担结构的主要的位置

PSA ACL功能是ACL检查的一个基于微码的实施。特殊的说明装载到允许基本ACL检查的PSA芯片。有一定数量的限制对应该在部署前仔细了解的此功能。对PSA ACL的一个主要缺点是要求的很多硬件转发内存。

PSA ACL功能要求PLU/TLU内存一大块将被预先分配的不管前缀等等数量。由于此分配来自主要TLU区域，有在这些卡可以维护路由的数量的一个重大影响，当PSA ACL配置时。

除PLU/TLU内存之外最初的支出，在TLU内存存储的每个前缀要求更内存。根据ACL应用的(入口与出口)和线路卡类型的方向变化的，每个前缀的所需的内存大小。一般来说，出口ACL比入口要求更多的内存，并且线路卡用更多物理端口要求更多的内存该那些用少量端口。

在引擎2线路卡不使用ACL的论点中，数据结构ACL的被建立不管配置的实际ACL。为了变成更加小的非ACL结构，您必须配置在路由器的**no access-list hardware psa**。此命令四面八方禁用在所有Engine2线路卡的所有ACL处理。非常小心地使用他们的思科recommeds。

概述

为了提供对立于匹配深度的ACL处理性能，引擎2 ACL集成到硬件转发表。下面请参阅关于关于怎样的说明这能影响前缀可扩展性。

这些线卡根据引擎2 ：

卡类型	接口类型	连接
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM64c	启动器	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

支持的匹配标准

所有Cisco IOS软件版本12.0S支持的标准和扩展ACL匹配标准，除了Layer4源端口。不连续的掩码、IP优先级字段和Layer4源端口从PSA ASIC在LC CPU被踢并且处理。

支持的ACE编号

五在PSA的448-line输入ACL。一个ACL可以每个端口配置。其他ACL是由线路卡CPU管理的。请参阅下面“限制”部分关于在输出ACL的限制。

输出ACL处理

在此线卡配置的输出ACL在其他线卡的入口功能路径在系统的将执行。请参阅IPv4输出ACL -线卡互操作矩阵关于详细信息。

线卡特定命令

- **访问列表硬件psa限制128**
- **no access-list hardware psa**
- **psa旁路**
- **show access-list psa详细信息**
- **show access-list psa摘要**
- **show controller psa功能**

可操作的指南和线卡交互作用

- 快速路径ACL处理要求将满足的这些情况：已应用ACL在128-或448- ACE限制内。如果**access-list硬件psa限制128**命令配置，长度少于128 ACE必须是。当448-line ACL微码套件要求时，长度少于448 ACE必须是。输入和输出ACL没有每个卡一起配置。五个输出ACL在*路由器*可能配置。
- 8和16端口OC-3/STM-1 POS线路卡支持仅128-line ACL。4端口OC-12/STM-4 POS、1端口OC-48/STM-16 POS和3波尔特千兆以太网线路卡支持448个线路ACL。
- 输入ACL在快速路径采取优先级在输出ACL，当两个在同一个卡时同時配置(输出ACL在慢路径处理)。
- 如果输出ACL在引擎2卡配置，并且进入线路卡是引擎0/1/2/4，输出ACL在进入卡将处理。对于其他引擎类型，输出ACL在引擎2出口慢路径将处理。
- 输出ACL不为IP到MPLS流量(“推送”在IP数据包上)的第一个MPLS标签支持。
- ACL处理信息集成到硬件FIB，并且能影响前缀可扩展性。前缀内存耗尽由有“exmem=1”签名的内存分配失败报告在随附于的日志消息。

建议

- ACL处理信息集成到CEF转发表，减少前缀可扩展性。不使用ACL的应用程序在CEF表里能禁用ACL支持和从而通过发出**no access-list hardware psa命令**增加可用的前缀内存。
- 除ACL的，禁用的PSA支持之外配置**no access-list hardware psa命令**由引擎2卡禁用所有ACL处理。它不强制ACL的软件执行。如果出口线路卡有配置的一个输出ACL此情况也应用。
- 配置**access-list compiled命令，**在**access-list硬件psa**命令转换超出PSA产能到Turbo ACL的ACE后。这为ACL提供最佳的ACL性能长度448 ACE。默认ACL微码是128 (和从Cisco IOS软件版本12.0(14)s/st)。如果更加小的ACL是在使用中，并且448-line功能没有要求，配置**access-list硬件psa限制128**命令保存转发(TLU)内存，改进前缀可扩展性)。应该用**access-list compiled命令**启用Turbo ACL处理ACL长比129条线路的与**access-list硬件psa限制128**命令一起。此组合处理在PSA ASIC的前128条线路和有涡轮ACL的剩余的线路，优化性能，当保存转发内存时。
- 4端口OC12 ATM线路卡不支持输入ACL，然而提供在微码的输出ACL检测，在慢路径允许输出ACL进程。
- 8xOC3 ATM线路卡支持与Cisco IOS软件版本12.0(23)S的每个vc 128个线路ACL和以后。16明显的输入ACL最大数量可以在快速路径配置。逐个VC支持448输入ACL在仅慢路径。不支持输出ACL。

ISE（IP 服务引擎）引擎 3 - ACL 处理

概述

引擎3是第一个双重阶段转发线卡。引擎3有在入口和出口路径的转发/功能ASIC。这允许在ASIC将安置的ACL在入口和出口路径。另外，引擎3 ASIC结构是一个混合的渠道/并行阵列。ASIC结构平行实现高速的ACL处理三重内容可编址存储器，提供至20K ACE线路速率处理每个入口和20K ACE每出口。

这些线卡根据引擎3 ：

卡类型	接口类型	连接
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/STM16c	POS	SR
1xOC48c/STM16c	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

支持的匹配标准

由线路卡CPU处理快速路径支持的所有Cisco IOS软件版本12.0S标准和扩展的匹配标准除了日志ACE。

支持的ACE编号

- 处理在入口和输出方向每个端口，每个VLAN，每帧中继子接口和每ATM子接口的线路速率。每个方向和每个卡支持20,000扩展的ACE。
- TCP/UDP来源/目的地端口的匹配标准“范围”，“Lt”和“gt”是在硬件方面处理的全部使用“L4操作员”资源。
- 明显的L4操作数数量被限制到32全部的线卡的。源端口操作员对最多六被限制。

输出ACL处理

处理在路径信息包的线路速率输出ACL的本地快速路径支持处理ASIC。请参阅IPv4输出ACL -线卡互操作矩阵关于详细信息。

线卡特定命令

- **hw-module <slot-> TCAM编译不合并*!! ---12.0(21)S3***
- **显示访问列表硬件接口<interface name>**

- 显示CEF int pos [x/y]|Inc if_number

可操作的指南和线卡交互作用

- 匹配记录的ACE的数据包在慢路径处理。
- 匹配拒绝ACE的数据包(被节流保证系统中断)在慢路径处理。
- 当ACL包括地址范围的ACE呼叫“范围的硬件用途特殊要求三ACE ACE”。
- ACL合并能通过共享在个人ACL间的普通的ACE保存TCAM资源。要确定ACL是否合并，请使用**show-access-list hardware interface命令**。
- ACL计数器不为合并的ACL支持。使用Cisco IOS软件版本12.0(21)S3和以后， ACL合并可以禁用与**hw-module <slot-> TCAM编译不合并**命令。为了确定ACL是否合并，请使用**show-access-list hardware interface命令**。
- 如果Netflow在引擎0/1线卡配置，并且输出ACL在出口引擎3或4+配置线卡，输出ACL将由入口和出口线路卡处理为了允许Netflow占ACL以及转发的数据包拒绝的数据包。

ACL计数器支持

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

定义：

- 每ACE —正常Cisco IOS软件软件支持， **show access-list <number>** on命令RP/LC显示ACL和计数器关联与每个ACE。它是可用的，只有当**合并**禁用时，在您配置所有ACL前。通过使用此配置命令，这可以执行：`Router(config)#`**`hw-module slot <`***`number`***`> tcam compile acl no-merge`** 此选项，当已启用关闭一些TCAM合并优化并且影响可扩展性。确切的效果取决于个人ACL。并且请注意计数器不会正确，如果基于策略的路由在该接口应用。在那种情况下，应该使用聚集计数器。
- 每ACE (TCAM) —硬件计数器关联与每个TCAM条目。配置不是必要的，并且没有在性能/可扩展性的影响。仅联机在线卡使用此CLI。这些计数器不可能被软件清除。`LC-Slot4#`**`show contr tofab alpha acl <`***`if-number`***`> vmr2ace`** 此命令的新的通用的CLI将是可用的在Cisco IOS软件版本22S ：`LC-Slot4#`**`show access-list hardware interface p0:1 in`** 只有当PBR在该接口没有使用与ACL时，如同每ACE计数器， TCAM计数器有效。
- 聚合—每个ACL显示一概略的permit/拒绝计数器。这是所有单个ACE计数器的总和。配置不是必要的，并且没有在性能或可扩展性的影响。

建议

无此时。

引擎 4 (POS) - ACL 处理

概述

引擎4提供此ACL支持Cisco IOS软件版本12.0(18)S及以上版本：

- 如果引擎4线卡是进入卡， E0/1/2线卡支持输出ACL。在此配置中，输出ACL由出口线路卡CPU处理。

这些线卡根据引擎4 ：

卡类型	接口类型	引擎类型	连接
4xOC48c/STM16c	POS	E4	
4xOC48c/STM16c	POS	E4	LR
1xOC192c/STM64c	POS	E4	IR
1xOC192c/STM64c	POS	E4	SR
1xOC192c/STM64c	POS	E4	VSR-1
10xGE	SFP	E4	

引擎 4+（POS 和 DPT）- ACL 处理

概述

引擎4+介绍ACL功能对Cisco 12000系列10 Gigabit投资组合。

其中每一个入口和出口路径支持1024 ACE。两个输入和输出ACL处理以96 ACE的线路速率。更加长的匹配的性能变化与匹配深度。

这些POS线路卡根据引擎4+ ：

卡类型	接口类型	连接
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

支持的匹配标准

快速路径支持所有Cisco IOS软件版本12.0S支持的标准和扩展ACL标准除了日志或分段ACE。

支持的ACE编号

1024 ACE是支持的单向在快速路径。

注意： 1021 ACE可配置。三个条目为ACE隐式**permit ip any any**、**deny ip any any**和**发送**保留**对CPU**命令。

没有对支持的ACE数量的上限。在1021限制之外的所有ACE在线卡慢路径执行。

输出ACL处理

输出ACL在transmit-side快速路径处理。请参阅IPv4输出ACL -线卡互操作矩阵关于详细信息。

线卡特定命令

- **show tcam appl [***acl-in|acl-out***] tcam <label-no>**
- **show tcam appl [***acl-in|acl-out***] *entries*>内存<port> <number**

可操作的指南和线卡交互作用

- 不支持Sub-interface ACL。
- 性能变化与匹配深度。
- 范围条目使用两ACL规则(三，如果两个条目超过边界)。
- 一个ACL每个物理接口支持。
- (每个方向)快速路径支持1024 ACE。
- 1024快速路径ACE中的任一条可以在端口间共享。
- 使用片段关键字的ACE在慢路径被过滤。
- 已拒绝数据包没有为在慢路径处理的ACE计数。
- 如果Netflow在引擎0线卡配置，并且输出ACL在出口引擎3或4+配置线卡，输出ACL将由入口和出口线路卡处理允许Netflow占ACL以及转发的数据包拒绝的数据包。

建议

无此时。

引擎 4+（以太网）- ACL 处理

概述

引擎4+以太网线路卡在硬件方面引入每VLAN输入ACL功能对Cisco 12000万兆以太网投资组合。这些是某些特性：

- 输入和输出ACL在单个端口可以同时应用，不用性能影响。
- ACL可以应用每个VLAN或每个端口。
- 至15K ACE的输入ACL性能不降低与匹配深度。
- 输出ACL处理以96 ACE的线路速率。更加长的匹配的性能变化与匹配深度。

这些以太网线路卡根据引擎4+ ：

卡类型	接口类型	引擎类型
10xGE B (“X-B”)	SFP ：	E4+
模块化	SFP ：	E4+
1x10GE	10G	E4+
1x10GE	10G	E4+

支持的匹配标准

快速路径支持所有Cisco IOS软件版本12.0S支持的标准和扩展ACL标准除了日志或分段ACE。

支持的ACE编号

- 15,000可以配置每个端口或每个VLAN的输入ACL。
- 1024输出ACE每个在a可以应用每个逐个端口的卡。**注意：** 1021 ACE可配置。三个条目为ACE隐式**permit ip any any**、**deny ip any any**和**发送保留对CPU**命令。

输出ACL处理

输出ACL在transmit-side快速路径本地处理。请参阅IPv4输出ACL -线卡互操作矩阵欲知更多信息。

线卡特定命令

- **hw-module slot <number> ip ACL合并**

可操作的指南和线卡交互作用

- 包含片段关键字的ACE在慢路径处理。
- ACL计数器不为与其它特性一起的ACL支持。
- ACL计数器不为合并的ACL支持。合并的ACL用**hw-module slot <slot number> ip ACL合并**命令是可配置。
- to168 L4操作每线卡支持。一旦这被超出， ACL在慢路径运行。
- 如果引擎1线卡有启用的抽样的NetFlow，并且输出ACL在出口引擎3或4+启用线卡，输出ACL由入口和出口线路卡处理为了允许Netflow占ACL以及转发的数据包拒绝的数据包。

建议

无此时。

ACL 记录

在Cisco IOS软件版本12.0(21)S前， ACL记录信息完全发送对RP在维护总线(MBUS)。在ACL记录活动期间高水平，超出MBUS的产能是可能的。Cisco IOS软件版本12.0(21)S引入防止此方案的几优化。

MBUS超载情况由与这些错误消息的Cisco IOS软件报告：

```
LCLOG-3-INVSTATE
```

```
MBUS_SYS-3-SEQUENCE
```

使用Cisco IOS软件版本12.0(21)S和以后，高严重程度(严重性0-4)日志消息传送对RP通过MBUS，当低严重性(严重性5-7)时日志消息传送对RP通过更高能力交换结构。ACL日志消息是高严重程度，因而当前传送对RP通过交换结构。

此已添加记录日志功能使用这些命令是可配置：

- **logging method mbus [severity]** —确定使用MBUS，哪些信息，由严重性，将传送对RP。高严重程度信息通过交换矩阵将传送。
- **show logging method** —显示所有消息严重性级别的当前记录日志方法。
- **logging sequence-nums** —此命令启用发送的线卡对序号日志消息，以便消息可以由RP适当地重新命令。没有此命令，日志消息可以传送到RP按不连续的顺序。

IPv4 输出 ACL - 线路卡互操作矩阵

在出口ACL处理的介绍用引擎3和引擎4+版本，输出ACL由进入线路卡前处理。输出ACL更新利用高性能引擎3和处理功能的引擎4+输出ACL。

此图表提供输出ACL为不同线路卡组合处理的摘要：

	出口线路卡					
进入线路卡(输出ACL应用对成员接口)	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**
E0	入口	入口	入口	出口	n/a	出口
E1	入口	入口	入口	出口	n/a	出口
E2	入口	入口	入口	出口	n/a	出口
E3	出口	出口	出口	出口	n/a	出口
E4	出口	出口	出口	出口	n/a	出口
E4+	出口	出口	出口	出口	n/a	出口

IPv6 ACL 支持

IPv6慢路径支持扩展ACL (入口和出口) E0、E1、E2、E3和E4+的在Cisco IOS软件版本12.0(23)S。

在引擎3中，在Cisco IOS软件版本12.0(25)S的硬件方面支持IPv6 ACL功能。ACL应用对一个特定

接口，与一隐式拒绝语句在每访问列表结束时。IPv6 ACL配置使用**ipv6 access-list命令**与拒绝并且允许在全局配置模式的关键字。引擎3根据基于通信量的IPv6选项报头卡支持过滤，流标签，和或者，上层协议类型信息。

Cisco 12000 ACL 命令参考

引擎1命令

- **访问列表硬件辣调味汁**
- **show controller l3|包括ASIC**

引擎2命令

- **访问列表硬件psa限制128**
- **no access-list hardware psa**
- **psa旁路**
- **show access-list psa详细信息**
- **show access-list psa摘要**
- **show controller psa功能**

引擎3命令

- **hw-module <slot-> TCAM编译不合并***!! ---自Cisco IOS软件版本12.0(21)S3*
- **显示访问列表硬件接口<interface name>**
- **显示contr [***tofab|frfab***]阿尔法ACL <int> vmr2ace**

引擎4+命令

- **show access-list gen7标签**
- **show tcam appl [***acl-in|acl-out***] tcam <label-no>**
- **show tcam appl [***acl-in|acl-out***] *entries*>内存<port><number**

引擎4+以太网命令

- **hw-module slot <number> ip ACL合并**

词汇表

此部分提供相关期限的标准的定义：

- **飞机处理**—网络设备可以逻辑上分开成三架飞机处理：数据层面—处理在流经网络设备的数据包。控制层面—处理在用于的数据包胶合网络设备。这包括线路通信协议(例如点对点协议- PPP和高级数据链路控制(HDLC) - HDLC)，路由协议(边界网关协议- BGP，路由信息协议版本2 - RIPv2，开放最短路径最初的OSPF，等)和时间协议(例如网络时间协议- NTP)。管理层面—处理在使用管理网络设备的数据包。这包括telnet、安全壳SSH、文件传输协议(FTP)、简单文件传输协议(TFTP)、SNMP和其他管理协议。
- **标准ACL** —独有标准ACL过滤器在第3层。
- **延长的ACL** —扩展IP访问列表使用源地址和目的地址匹配操作以及可选协议类型信息控制精细的。
- **线性处理的ACL** —线性地处理在软件方面。性能变化与匹配深度(必须检查条目的数量，在确定匹配)前。

- **涡轮ACL (编译)** —涡轮ACL通过编译ACL优化软件ACL处理到加速软件处理查询表的最佳的系列。涡轮ACL性能随匹配深度不变化。
- **输入ACL** — ACL应用对输入应用的端口的流量。
- **输出ACL** — ACL应用对退出应用的端口的流量。有一些例外，输出ACL由输入线卡处理。
- **接收路径ACL** —接收路径ACL为为路由器注定的控制流量提供过滤，例如路由更新和SNMP查询。
- **双倍阶段转发线卡**—有在入口和出口路径的转发/功能ASIC的线卡。这允许线卡执行在入口数据包流和出口数据包流的功能没有punting信息包对LC CPU。它也允许在Cisco 12000内将使用的新一轮双重阶段转发算法。引擎3线卡是一双重阶段转发线卡的示例。
- **单级转发线卡**—有在入口路径的转发/功能ASIC的线卡。这些线卡只执行基于ASIC处理在入口路径流的数据包。出口流量没有处理(转发)，由其他LCs入口ASIC处理或者由LC CPU管理。引擎2、引擎4和引擎4+是单级转发线卡示例。

相关信息

- Cisco 12000 系列互联网路由器
- 技术支持和文档 - Cisco Systems