Voer toegangslijsten op 12000 Series internetrouters in

Inhoud

Inleiding

Dit document beschrijft ondersteuning voor toegangscontrolelijsten (ACL's) op Cisco 12000 Series Internet-routers.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van de grondbeginselen van hoe ACL op een router van Cisco werkt.

Raadpleeg deze documenten voor algemene informatie over ACL's en hun toepassingen:

- Toegangscontrolelijsten: Overzicht en richtsnoeren
- IP-services configureren: IP-pakketten filteren

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 12000 Series Internet Routers.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Overzicht van ACL-ondersteuning op Cisco 12000 Series internetrouter

Op Cisco 12000 Series internetrouter kunnen ACL's worden verwerkt in hardware (Application-Specific Integrated Circuit - ASIC), software (CPU's van een lijnkaart) of als een hybride functie - verwerkt in software met hardwareondersteuning. Of een ACL in hardware of software wordt verwerkt hangt af van de ACL-toepassing, het type lijnkaartmotor en de interactie van ACL's in andere lijnkaarten.

De Cisco 12000 Series lijnkaartmotoren bieden verschillende ACL-functies. Ga voor ACL-ondersteuningsinformatie voor een bepaalde lijnkaartmotor naar de bijbehorende sectie in dit document.

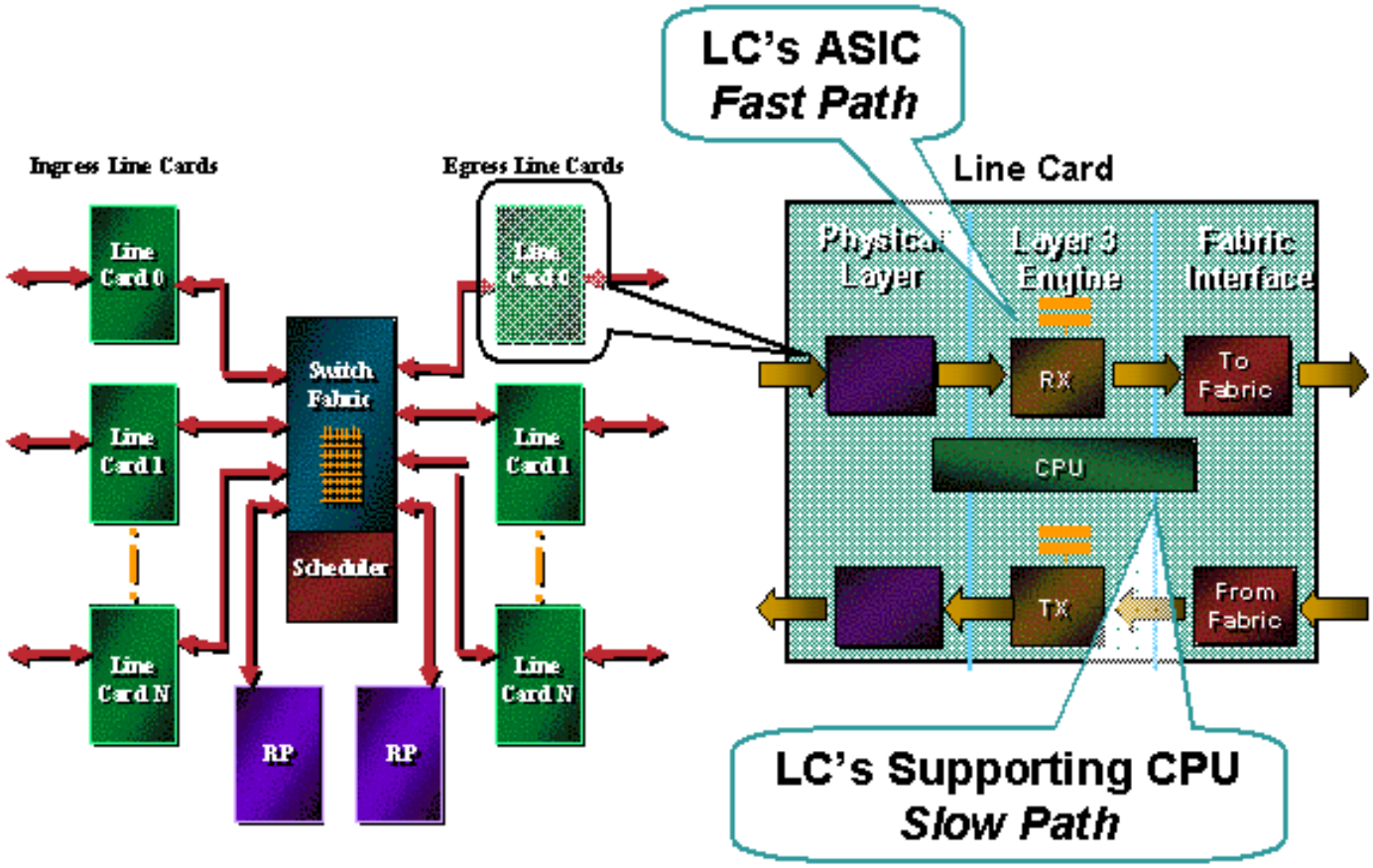
Opmerking: IP-multicast ACL's worden niet ondersteund in Cisco IOS® softwarerelease 12.0S. De IP-multicast grensfunctie kan worden gebruikt waar multicast filtering nodig is. Raadpleeg Fast-Path Multicast Forwarding op Cisco 12000 Series Engine 2 en ISE-lijnkaarten voor meer informatie.

ASIC-gebaseerde ACL's vs. CPU-gebaseerde ACL's

Cisco 12000 ondersteunt alle generaties ACL-verwerking. Een operationeel begrip van hoe elk van deze verwerkingsmodi werkt, op elkaar inwerkt en elkaar ondersteunt, is essentieel voor effectief ACL-gebruik op Cisco 12000.

Vroege generaties van ACL-verwerking gebruikten een programmeerbare CPU om de ACL te verwerken. Na verloop van tijd overtroffen de vereisten voor de verwerking van pakketten per seconde (PPS) de mogelijkheid van nieuwe CPU's om up-to-support te behouden. ASIC's werden gebouwd om hogere PPS-tarieven te bereiken voor het doorsturen van router en mogelijkheden voor functies. ACL's die op de lijnkaart (LC) CPU's waren geladen, werden vervolgens op de LC ASIC geladen. ASIC's bleven geïmproviseerd om hogere PPS-tarieven af te handelen. Deze tweede generatie ASIC's zijn gebaseerd op het pionierswerk van de generatie eerder, en bieden

meer ASIC-mogelijkheden. Omdat Cisco 12000 een gedistribueerd routingplatform is, kan interactie tussen de verschillende generaties van ACL-verwerking tot enige operationele verwarring leiden.



Bepalingen zoals op ASIC gebaseerde ACL, op CPU gebaseerde ACL, Snel pad, Langzaam pad en ASIC Punten worden door dit document gebruikt om te helpen verklaren wat er bij de ACL-verwerking gebeurt. Hier zijn verklaringen van deze termen:

- Op ASIC gebaseerde ACL's (Fast Path) - ACL's worden geladen en verwerkt in de ASIC-hardware. De prestatiemaxima van de ASIC bepaalt de diepte, prestaties en mogelijkheden van ACL. Het Fast Path is gebruikt in het pad om het verschil tussen op ASIC gebaseerde verwerking en verwerking te illustreren dat in de LC-ondersteunende CPU is uitgevoerd. De generieke term ASIC-gebaseerde wordt in dit document gebruikt.
- Op CPU's gebaseerde ACL's (langzaam pad) — ACL's worden in software op de lijnkaart CPU's verwerkt. Voor de kaarten van de vroege generatie (Engine 0 en in sommige gevallen Engine 1) wordt alle verwerking uitgevoerd op de LC CPU. Op ASIC gebaseerde LCs voeren ACL's uit die worden verwerkt op pakketten die uit de ASIC worden geleid. In het verleden werd traag pad gebruikt om aan te geven hoe de puntjes op de LC CPU trager waren dan de ASIC. De generieke term, CPU-gebaseerd, wordt in dit document gebruikt.
- ASIC Punts-ASIC's hebben strikte ontwerpenveloppen. Wanneer een pakket het ontworpen enveloppe overschrijdt, wordt het van ASIC geleid om op of de LC die CPU steunt of naar de Routeprocessor (RP) wordt verzonden. Op ASIC gebaseerde ACL's punten die buiten het ontwerp van de ASIC vallen. Een voorbeeld is ACL dat een ACE met een logbestand of logginginput sleutelwoord heeft. De informatie die vereist is om het pakket te loggen moet buiten de ASIC worden verwerkt, zodat het pakket automatisch uit de ASIC wordt geleid naar de LC CPU's en als een normale CPU-gebaseerde ACL wordt verwerkt.

Opmerking: Wanneer u op beleid gebaseerde routing (PBR) configureren met overeenkomende

verklaringen die overeenkomen met ACL's, behoren ACL's niet overeen te komen met de bronpoort. De Gigabit switch-router (GSR) ondersteunt geen hardwareswitching voor de PBR met ACL's die overeenkomen met de bronpoort. Het veroorzaakt processwitching en GSR prestaties degraderen.

Filtering van besturingsplane en beheerplatform

De routerprocessor biedt controle- en beheersysteemservices in de gedistribueerde architectuur van Cisco 12000 Series. Ontvang ACL's (Pad ACL's) op basis van een eenvoudige gedistribueerde filtermogelijkheid voor controle- en beheerverkeer dat bestemd is voor de RP. Het kan logisch gezien worden als een extra laag van veiligheid die van de sterke punten van een gedistribueerde architectuur gebruik maakt.

IP-ontvangerpad ACL's configureren

De rACL is door een speciale ontheffing geïntroduceerd in het onderhoudspakket van Cisco IOS® softwarerelease 12.0(21)S2. Het wordt officieel ondersteund in Cisco IOS-softwarerelease 12.0(22)S. Raadpleeg IP Ontvang ACL voor meer informatie.

De routerprocessor biedt besturingsplanservices in de gedistribueerde architectuur van Cisco 12000 Series. Ontvang ACL's bieden filtermogelijkheden voor controleverkeer dat voor RP is bestemd, zoals routing updates en Simple Network Management Protocol (SNMP)-vragen.

De rACL wordt beschouwd als fase 1 van een meerfaseninspanning om nieuwe beschermingsmaatregelen toe te voegen aan de controle en het beheer van het vliegverkeer. Nieuwe snelheidsbeperkende verbeteringen worden toegevoegd door software-updates.

Ondersteuning van IPv4 ACL-kaart (lijnkaarttype)

De 12000 Series lijnkaarten bieden verschillende ACL-functies per motortype. In dit deel worden de ACL-functies van de verschillende lijnkaartmotoren beschreven. Zie het corresponderende gedeelte van dit document voor informatie over ACL-ondersteuning voor een bepaalde lijnkaartmotor.

Er zijn enkele algemene kenmerken voor alle ACL's (ASIC- en CPU-gebaseerd):

- Slechts één ACL kan op een interface voor elke richting worden toegepast. Bijvoorbeeld, interface POS 0/0 kan slechts één input ACL en één uitvoer ACL hebben.
- Test van het pakket tegen een ACL houdt op nadat een match is gevonden. Als een ACL die 300 lemma's bevat lang overeenkomt met het pakket op Access-list (ACE) #45, dan wordt het pakket verwerkt en wordt de ACL-verwerking gestopt.
- Er is een impliciete **ontkent alle** ingang aan het eind van elke ACL. Als resultaat hiervan wordt, als er geen overeenkomst op ACL is, het pakje gelaten. Cisco ACL's worden gemaakt met *expliciete* ACL-architectuur. Dit betekent dat er een ACE moet zijn om het pakje aan te passen zodat het verwerkt en doorgestuurd wordt.
- ACE's met toegevoegde waarde worden altijd toegevoegd aan het einde van de ACL. Wanneer ACL updates vereist, is het een goede praktijk om ACL te verwijderen (gebruik het **geen toegang-lijst** bevel) en het nieuwe ACL opnieuw toe te voegen.
- Omdat niet-initiële IP fragmenten geen Layer 4 protocol informatie in de IP-header bevatten,

worden alleen standaard overeenkomende criteria ondersteund voor niet-initiële fragmenten. Volledige details over hoe Cisco ACL's voldoen aan IP-fragmentatie kunnen worden gevonden in toegangscontrolelijsten en IP-fragmentaties.

- Nummering ACL's worden verwerkt en toegepast zodra ze via de opdrachtregel interface (CLI) zijn ingevoerd. Met grote ACL's leidt dit soms tot een CPU-stijging in de RP of de LC CPU's.

Engine 0 - ACL-verwerking

Engine 0 is de eerste lijnkaart die voor Cisco 12000 wordt geleverd. Het is alle op CPU's gebaseerde verwerking en verzending. Vandaar dat Engine 0 lijnkaarten ACL's verwerken in de LC CPU's.

Deze lijnkaarten zijn gebaseerd op motor 0:

Type lijnkaart	Type interface	Connectiviteit
12 x DS3	coaxiaal	MKB
12 x DS3	coaxiaal	MKB
12 x E3	coaxiaal	MKB
1xCHOC12-1>DS3		IR
1xCHOC12/STM-4>OC-3/STM-1	POS	IR
4x OC3c/STM-1c	POS	SR
4x OC3c/STM-1c	POS	LR
4x OC3c/STM-1c	POS	MM
1xOC12c/STM-4c	POS	IR
1xOC12c/STM-4c	POS	MM
6xCT3-1>DS1		MKB
2xCHOC3/STM1-1>DS1/E1		IR
4x OC3c/STM-1c	ATM	IR
4x OC3c/STM-1c	ATM	MM
1xOC12c/STM-4c	ATM	IR
1xOC12c/STM-4c	ATM	MM

Ondersteunde aanpassingscriteria

Alle Cisco IOS-softwarerelease 12.0S standaard, uitgebreide ACL's en Turbo-ACL's worden ondersteund op Engine 0.

Aantal ondersteunde ACE's

De grootte van ACL is uitsluitend beperkt door prestatienormen en beschikbare geheugenbronnen.

Uitvoer ACL-verwerking

Uitvoer-ACL's worden verwerkt in het invoerfunctiepad van de andere lijnkaarten in het systeem. Een druk van de Uitvoer ACL aan de ingangskant van andere LCs beschermt de backplane van het verzenden van pakketten die zullen worden gedropt. Dit is een geërfde functie van de gedistribueerde architectuur op Cisco 7500. Een gedetailleerde uitleg, redenen en operationele richtlijnen worden gegeven in de IPv4 uitvoer ACL-interfacekaart met lijnkaart.

Specifieke opdrachten voor lijnkaart

None.

Operationele richtsnoeren en lijnkaartinteracties

- Als NetFlow op een Engine 0 lijnkaart is geconfigureerd en er op een uitgang ACL op een IP-motor 3 of 4+ lijnkaart is ingesteld, wordt de uitvoer-ACL verwerkt door zowel de ingangen- als perslijnkaarten om NetFlow in staat te stellen om rekening te houden met pakketten die door ACL's worden ontkend en verzonden pakketten.

Aanbevelingen

Cisco raadt het gebruik van Turbo ACL's op Engine 0 aan voor grote ACL's. Kleine Lineaire ACL's zijn efficiënter voor kleinere ACL's omdat Turbo-ACL's extra geheugen vereisen.

Engine 1 - ACL-verwerking

Overzicht

De lijnkaart van Engine 1 is een brug tussen de op CPU gebaseerde verwerking van de motor 0 en de eerste generatie van het verzenden/uitvoeren van de functie ASIC op de lijn 2. Engine 1 verwerkt ACL's in software standaard. Met Cisco IOS-softwarerelease 12.0(10)S en later biedt Engine 1 hardware-ACL's voor kaarten die zijn uitgerust met versie 4 of 5 van de SSA ASIC (zie de opdracht voor lijnkaartopdracht hieronder om te bepalen met welke versie van SSA een bepaalde kaart is uitgerust).

Deze lijnkaarten zijn gebaseerd op motor 1:

Type lijnkaart	Type interface	Connectiviteit
8xFE	(RJ45)	100BaseT
8xFE	(M)	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	(M)	100BaseF
1 GE	SX,	GBIC:
1 GE	SX,	GBIC:
2xOC12c/STM-4c	DPT	IR
2xOC12c/STM-4c	DPT	LR
2xOC12c/STM-4	DPT	XLR

c		
2xOC12c/STM-4c	DPT	MM
2xOC12c/STM-4c	DPT	IR
2xOC12c/STM-4c	DPT	LR
2cOC12c/STM-4c	DPT	XLR
2xOC12c/STM-4c	DPT	MM

Ondersteunde aanpassingscriteria

Alle Cisco IOS-softwarerelease 12.0S ondersteunde standaard-, uitgebreide en Turbo-ACL's worden ondersteund in de LC CPU (langzaam pad). Bovendien kan Engine 1 invoer ACL's in de Salsa ASIC verwerken. Salsa ASIC verwerkt ACL-invoer samen met routeraadpleging, wat resulteert in hogere prestaties in vergelijking met traditionele Lineaire ACL-verwerking en Turbo-ACL-verwerking. De SSA ASIC kan uitvoer ACLs of subinterface ACLs niet verwerken.

Aantal ondersteunde ACE's

De grootte van ACL is uitsluitend beperkt door prestatienormen en beschikbare geheugenbronnen.

Uitvoer ACL-verwerking

Uitvoer-ACL's worden verwerkt in het invoerfunctiepad van de andere lijnkaarten in het systeem. Zie het gedeelte IPv4-uitgang - Lijnkaart voor informatie over de mate van interactie.

Specifieke opdrachten voor lijnkaart

- **hardware-salsa met toegangslijsten**
- **demonstratiecontroller l3 | omvat ASIC**

Operationele richtsnoeren en lijnkaartinteracties

- Salsa ASIC en PSA ASIC kunnen niet tegelijkertijd worden gebruikt. De **toegang-lijst hardwareopdracht** accepteert alleen PSA (Engine 2) of Salsa (Engine 1) maar niet beide.
- Als NetFlow op een Engine 1 lijnkaart is geconfigureerd en er op een uitgang ACL op een IP-motor 3 of 4+ lijnkaart is ingesteld, wordt de uitgevoerde ACL verwerkt door zowel de ingangen- als perslijnkaarten om NetFlow in staat te stellen om rekening te houden met pakketten die door ACL's worden ontkend en doorgestuurd pakketten.

Aanbevelingen

Voor versies van Engine 1 lijnkaarten die geen hardware ACL's ondersteunen, adviseert Cisco het gebruik van Turbo-ACL's voor grote ACL's. Kleine ACL's (minder dan 20 lijnen) kunnen als lineaire ACL's worden geïmplementeerd om geheugen te besparen.

Engine 2 - ACL-verwerking

Overzicht

Engine 2 was de eerste lijnkaart met een verstuurd/kenmerk ASIC. Met Cisco IOS-softwarerelease 12.0(10)S en later bieden Engine 2-lijnkaarten hardware-ACL-functies in de hoogwaardige Packet Switching ASIC (PSA). Zoals bij alle transport/kenmerken-ASIC's zijn er bij strikte prestatiemaxima grenzen aan de capaciteit van de ASIC. De belangrijkste prestatiemaxima op Engine 2 ACL's zijn te wijten aan geheugenbeperkingen in de PSA ASIC.

Packet-expanderen in Engine 2 wordt uitgevoerd door de PSA ASIC. PSA heeft drie belangrijke externe herinneringen:

- PLU (Path-lookup)—gebruikt om knooppunten op te slaan
- TLU (Table Lookup)—gebruikt om FIB-bladeren op te slaan en mogelijk structuren voor de taakverdeling. Wordt ook gebruikt om veel van de PSA ACL-gegevensstructuren te houden
- SRAM—de primaire locatie voor de lastverdeling

De optie PSA ACL is een op microcode gebaseerde implementatie van ACL-controle. Er wordt een speciale set instructies in de PSA-chip geladen waarmee een basiscontrole van de ACL mogelijk is. Er zijn een aantal beperkingen aan deze optie die zorgvuldig moeten worden begrepen voordat u het apparaat implementeert. Een belangrijk nadeel voor PSA ACL's is de grote hoeveelheid vereiste hardware-doorsturen geheugen.

Voor de PSA ACL-functie moet een groot blok PLU/TLU-geheugen vooraf worden toegewezen, ongeacht het aantal voorfixes, enz. Omdat deze toewijzing voornamelijk afkomstig is uit het TLU-gebied, heeft deze een aanzienlijke invloed op het aantal routes dat op deze kaarten kan worden onderhouden wanneer PSA ACL's zijn geconfigureerd.

Naast de initiële investering van PLU/TLU-geheugen, vereist elk voorvoegsel dat opgeslagen is in het TLU-geheugen aanzienlijk meer geheugen. De hoeveelheid geheugen die voor elk voorvoegsel vereist is, varieert afhankelijk van de richting van de toegepaste ACL (spanning versus spanning) en het lijnkaarttype. In het algemeen hebben grotere ACL's meer geheugen dan toegang nodig en linecards met meer fysieke poorten vereisen meer geheugen dat zij met minder poorten hebben.

In het geval waar de lijn van Engine 2 geen ACL's gebruikt, worden de gegevensstructuren voor ACL's gebouwd ongeacht de werkelijk geconfigureerd ACL's. Om aan de kleinere niet-ACL structuren te veranderen, moet u **geen** de **hardware psa van de toegangslijst** op de router configureren. Deze opdracht schakelt alle ACL-verwerking op alle Engine2-lijnkaarten in alle richtingen uit. Cisco adviseert deze met extreme voorzichtigheid te gebruiken.

Overzicht

Om ACL's verwerkingsprestaties te bieden die onafhankelijk zijn van de matchdiepte, worden Engine 2 ACL's geïntegreerd in de hardware-expedentiatietabel. Zie hieronder voor verklaringen over hoe dit de schaalbaarheid van voorvoegsels kan beïnvloeden.

Deze lijnkaarten zijn gebaseerd op Engine 3:

Type lijnkaart	Type interface	Connectiviteit
1xOC48c/STM-16c switch	POS	SR
1xOC48c/STM-	POS	LR

16c switch		
1xOC48c/STM-16c switch	POS	SR
1xOC48c/STM-16c switch	POS	LR
1xOC192c/STM-64c switch	toelaten	SR
16xOC3c/STM-1c	POS	IR
16xOC3c/STM-1c	POS	MM
4x OC12c/STM-4c	POS	IR
4x OC12c/STM-4c	POS	MM
4x OC12c/STM-4c	POS	IR
4x OC12c/STM-4c	POS	MM
4x OC12c/STM-4c	ATM	IR
4x OC12c/STM-4c	ATM	MM
8xOC3c/STM-1c	ATM/TS	IR
8xOC3c/STM-1c	ATM/TS	MM
3x 1 GE	SX	GBIC:
3x 1 GE	CWDM	GBIC:
1xOC48c/STM-16c switch	DPT	SR
1xOC48c/STM-16c switch	DPT	LR
1xOC48c/STM-16c switch	DPT	SR
1xOC48c/STM-16c switch	DPT	LR

Ondersteunde aanpassingscriteria

Alle Cisco IOS-softwarerelease 12.0S ondersteunde standaard- en uitgebreide ACL-criteria, behalve Layer 4 bronpoorten. Ononderbroken maskers, IP-prioriteitsvelden en Layer 4 bronpoorten worden gepunteerd op de PSA ASIC en verwerkt op de LC CPU's.

Aantal ondersteunde ACE's

Tot vijf 448-lijnen ingangsACL's in de PSA. Eén ACL kan per poort worden ingesteld. Aanvullende ACL's worden toegediend door de CPU-lijnkaart. Zie het gedeelte "Beperkingen" hieronder voor beperkingen op uitgevoerde ACL's.

Uitvoer ACL-verwerking

Een ACL-uitgang die op deze lijnkaart is ingesteld, wordt uitgevoerd in het snijpad van de andere lijnkaarten in het systeem. Zie de IPv4 uitvoer ACL-lijnkaartinterfacekaart voor meer informatie.

Specifieke opdrachten voor lijnkaart

- **lijst van beschikbare hardware-psa-limiet 128**
- **geen lijst van hardware-psa**
- **bypass**
- **PSA-details tonen**
- **een samenvatting van de toegangslijst tonen**
- **PSA-functie van controller**

Operationele richtsnoeren en lijnkaartinteracties

- Voor een snelle verwerking van pad-ACL moet aan deze voorwaarden worden voldaan:De toegepaste ACL is binnen de 128- of 448-ACE-limiet.De lengte moet kleiner zijn dan 128 ACE's als de **access-list hardwareconfiguratie 128** opdracht is geconfigureerd.De lengte moet kleiner zijn dan 448 ACE's wanneer de microcodebundel van 448 lijnen is vereist.Invoer- en uitvoerACL's worden per kaart niet samen ingesteld.Tot vijf uitgevoerde ACL's kunnen op de *router* worden geconfigureerd.
- Slechts 128-lijn ACL's worden ondersteund op 8- en 16-poorts OC-3/STM-1 POS-lijnkaarten. 448 lijnen ACL's worden ondersteund op de 4-poorts OC-12/STM-4 POS, 1-poorts OC-48/STM-16 POS en 3-poorts Gigabit Ethernet-lijnkaarten.
- Invoer ACL's hebben prioriteit in het snelle pad via uitvoer-ACL's wanneer beide tegelijkertijd op dezelfde kaart zijn ingesteld (de uitgevoerde ACL's worden verwerkt in het trage pad).
- Als een ACL-uitgang op een Engine 2-kaart is ingesteld en de inbraaklijnkaart op Engine 0/1/2/4 is, wordt een ACL-uitgang op de toegangskaart verwerkt. Voor andere motortypen wordt de uitvoer-ACL verwerkt in de vertragingstactiek Engine 2.
- Uitvoer-ACL's worden niet ondersteund voor IP-naar-MPLS verkeer (eerste MPLS-label wordt "afgedrukt" op een IP-pakket).
- ACL-verwerkingsinformatie wordt in de hardware-FIB geïntegreerd en kan de schaalbaarheid van voorvoegsel beïnvloeden. De voorvoegsel van de uitputting van het geheugen wordt gerapporteerd door geheugenverdelingsfouten met de "exmem=1"-handtekening in het begeleidende logbericht.

Aanbevelingen

- ACL-verwerkingsinformatie wordt geïntegreerd in de CEF-verzendtabel, die de schaalbaarheid van prefix beperkt. Toepassingen die geen ACL's gebruiken kunnen ACL-ondersteuning uitschakelen in de CEF-tabel en daardoor het beschikbare geheugen van het voorvoegsel vergroten door de opdracht **Geen toegangslijst-hardware uit te geven**.
- De configuratie van het **geen toegang-lijst hardwareopdracht** schakelt alle ACL-verwerking door Engine 2-kaarten uit, naast het uitschakelen van de PSA-ondersteuning voor ACL's. Het dwingt geen softwareuitvoering van ACL's. Deze voorwaarde is ook van toepassing als de perslijnkaart een uitvoer ACL heeft ingesteld.
- De configuratie van de **toegangslijst gecompileerde** opdracht na de **toegang-lijst hardware psa** opdracht converteert ACE's die de capaciteit van de PSA in een Turbo ACL overschrijden. Dit

levert optimale ACL-prestaties voor ACL's met een lengte van meer dan 448 ACE's.De standaard ACL-microcode (RL) is 128 (afkomstig van Cisco IOS-softwarerelease 12.0(14)S/ST). Als kleinere ACL's in gebruik zijn en de 448-lijnmogelijkheid niet vereist is, **behoudt** het configureren van de **toegangslijst hardware-limiet 128** opdracht het doorsturen (TLU) geheugen (wat prefix schaalbaarheid verbetert).Turbo ACL-verwerking moet met de **access-list gecompileerde** opdracht voor ACL's langer dan 129 lijnen mogelijk zijn samen met de **access-list hardwareconfiguratie 128** opdracht. Deze combinatie verwerkt de eerste 128 lijnen in de PSA ASIC en de resterende lijnen met Turbo ACLs, die prestaties optimaliseert terwijl het verzenden geheugen behouden blijft.

- De 4-poorts OC12 ATM-lijnkaart ondersteunt geen ACL's (invoersignaal), maar biedt een detectie van ACL-uitvoer in microcode waardoor het proces van uitvoer van ACL's in het trage pad verloopt.
- De 8xOC3 ATM-lijnkaart ondersteunt per-vc 128 lijnen ACL's met Cisco IOS-softwarerelease 12.0(23)S en hoger. Een maximum van 16 verschillende ingangsACL's kan in snel pad worden geconfigureerd. ACL-input (448) wordt per-VC basis alleen bij langzaam pad ondersteund. Uitvoer-ACL's worden niet ondersteund.

ISE (IP Services Engine) 3 - ACL-encryptie

Overzicht

Engine 3 is de eerste tweefasenlijnkaart. Engine 3 heeft ASIC's doorsturen/kenmerken op het ingangspad en het ingangspad. Dit laat ACLs in ASIC op zowel ingress als toegangswegen toe. Daarnaast is de Engine 3 ASIC-structuur een hybride pijpleiding/parallelle array. De ASIC-structuur implementeert ACL-verwerking in parallel snel adresseerbare geheugen (TCAM) met hoge snelheid, dat lijnsnelheidsverwerking biedt van maximaal 20 K ACE's per inloop, en 20 K ACE's per uitgang.

Deze lijnkaarten zijn gebaseerd op Engine 3:

Type lijnkaart	Type interface	Connectiviteit
4x OC12c/STM-4c	POS	IR
4x OC12c/STM-4c	POS	MM
4xCHOC12/STM-4>OC-3/STM-1->DS3/E3	POS	IR
16xOC3c/STM-1c	POS	IR
16xOC3c/STM-1c	POS	MM
8xOC3/STM-1c	POS	IR
8xOC3c/STM-1c	POS	MM
4x OC3c/STM-1c	POS	IR
4x OC3c/STM-1c	POS	MM
4x OC3c/STM-1c	POS	LR
1xOC48c/STM-16c switch	POS	SR

1xOC48c/STM-16c switch	POS	LR
1xCHOC48/STM-16>STM-4>OC-3/STM-1->DS3/E3	POS	SR
4x OC12c/STM-4c	ATM/IP	IR
4x OC12c/STM-4c	ATM/IP	MM
4 GE	GE	
4x OC12c/STM-4c	DPT	IR
4x OC12c/STM-4c	DPT	XLR

Ondersteunde aanpassingscriteria

Alle standaard- en uitgebreide matchcriteria voor Cisco IOS-softwarerelease 12.0S worden op het snelle pad ondersteund, behalve voor log-ACE's die door de CPU-lijnkaart worden verwerkt.

Aantal ondersteunde ACE's

- Verwerking van lijnsnelheden in zowel ingressie- als bovenrichting per poort, per VLAN, per Frame Relay-subinterface en per ATM-subinterface. Tot 20.000 uitgebreide ACE's per richting en per kaart worden ondersteund.
- Overeenkomstcriteria voor TCP/UDP bron/bestemming "range", "lt" en "gt" worden allemaal verwerkt in hardware met behulp van "L4 operator" resources.
- Het aantal afzonderlijke L4-operanden is beperkt tot 32 voor de hele lijnkaart. De exploitanten van de bronhavens zijn beperkt tot maximaal zes.

Uitvoer ACL-verwerking

Ondersteuning van native snelpad voor ACL-uitvoer met lijnsnelheid bij verwerking in het verzenden-pad Packet Processing ASIC. Zie de IPv4 uitvoer ACL-lijnkaartinterfacekaart voor meer informatie.

Specifieke opdrachten voor lijnkaart

- **Hoe-module <*sleuf #*> tcam compileren niet-samenvoegen*—12.0(21)S3***
- **hardware-interface met TOEGANG-lijst <*interfacenaam*>**
- **Cef-punten tonen[*x/y*] | inch if_number**

Operationele richtsnoeren en lijnkaartinteracties

- Pakketten die elkaar koppelen aan logACE's worden in het langzame pad verwerkt.
- Packets matching ontkennen ACE's (gebrand om te voorkomen dat het systeem wordt

onderbroken) worden verwerkt in het trage pad.
- Wanneer ACL een bereik van adressen omvat, gebruikt de hardware speciale ACEs genaamd "Range ACEs" die tot drie ACEs vereist.
- ACL-samenvoeging kan TCAM-middelen besparen door gezamenlijke ACE's over afzonderlijke ACL's te delen. Om te bepalen of ACL wordt samengevoegd, gebruik de **show-access-list** opdracht **hardware interface**.
- ACL-tellers worden niet ondersteund voor samengevoegde ACL's. Met Cisco IOS-softwarerelease 12.0(21)S3 en hoger kan het samenvoegen van ACL's worden uitgeschakeld met de opdracht **voor het compileren van <sleuf#> van de** module. Om te bepalen of ACL wordt samengevoegd, gebruik de **show-access-list** opdracht **hardware interface**.
- Als NetFlow op een lijnkaart van Engine 0/1 is geconfigureerd en ACL-uitgang op een lijnkaart van toegangsmachine 3 of 4+ is ingesteld, wordt ACL-uitgang verwerkt door zowel de ingangskaart als perslijnkaarten om NetFlow in staat te stellen om rekening te houden met pakketten die door ACL's worden ontkend en verzonden pakketten.

ACL-telondersteuning

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

Definities:

- Per-ACE-Normale Cisco IOS softwareondersteuning, **toont** de **show access-list <*number*>** opdracht op de RP/LC die ACL en teller geassocieerd met elk ACE weergeeft. Het is alleen beschikbaar wanneer **samenvoegen** is uitgeschakeld voordat u ACL's configureren. Dit kan gedaan worden door deze configuratieopdracht te gebruiken:
  `Router(config)#hw-module slot <number> tcam compile acl no-merge`

  Deze optie wordt ingeschakeld als een aantal TCAM-optimalisaties worden uitgeschakeld en de schaalbaarheid wordt beïnvloed. Het precieze effect hangt af van individuele ACL's.Merk ook op dat de tellers niet zullen kloppen als op beleid gebaseerde routing op die interface wordt toegepast. In dat geval moet gebruik worden gemaakt van de teller.
- Per-ACE (TCAM) - de tellers van de hardware verbonden met elke ingang van TCAM. Er is geen configuratie nodig en er is geen impact op de prestaties/schaalbaarheid. Alleen beschikbaar op de lijnkaart met deze CLI. Deze tellers kunnen niet door software worden gewist.
  `LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace`

  Een nieuwe generieke CLI voor deze opdracht is beschikbaar in Cisco IOS-softwarerelease 2.S:
  `LC-Slot4#show access-list hardware interface p0:1 in`

  Zoals met de per-ACE teller, zijn de TCAM tellers slechts geldig wanneer PBR niet op die interface met ACL wordt gebruikt.
- Aggregatie-elke ACL toont een summiere vergunning/ontken teller. Dit is de som van alle individuele ACE-tellers. Er is geen configuratie nodig en er is geen impact op prestaties of schaalbaarheid.

Aanbevelingen

Op dit moment niet.

Engine 4 (POS) - ACL-verwerking

Overzicht

Engine 4 biedt deze ACL-ondersteuning bij Cisco IOS-softwarerelease 12.0(18)S en hoger:

- Uitvoer-ACL's worden ondersteund op E0/1/2-lijnkaarten als een Engine 4-lijnkaart de toegangskaart is. In deze configuratie wordt de uitvoer-ACL verwerkt door de opslaglijnkaart CPU.

Deze lijnkaarten zijn gebaseerd op motor 4:

Type lijnkaart	Type interface	Type motor	Connectiviteit
4x OC48c/STM-16c switch	POS	E4	
4x OC48c/STM-16c switch	POS	E4	LR
1xOC192c/STM-64c switch	POS	E4	IR
1xOC192c/STM-64c switch	POS	E4	SR
1xOC192c/STM-64c switch	POS	E4	VSR-1
10x1 GE	SFP	E4	

Engine 4+ (POS en DPT) - ACL-verwerking

Overzicht

Engine 4+ introduceert ACL-functionaliteit voor Cisco 12000 Series 10 Gigabit-portefeuille.

Tot 1024 ACE's worden ondersteund in elk van de ingangen en compressiepaden. Zowel Invoer- als Uitvoer-ACL's worden met lijnsnelheid voor maximaal 96 ACE's verwerkt. Prestaties voor langere overeenkomsten variëren afhankelijk van matchdiepte.

Deze POS-lijnkaarten zijn gebaseerd op Engine 4+:

Type lijnkaart	Type interface	Connectiviteit
4x OC48c/STM-	POS	SR

16c switch		
4x OC48c/STM-16c switch	POS	LR
1xOC192c/STM-64c switch	POS	IR
1xOC192c/STM-64c switch	POS	SR
1xOC192c/STM-64c switch	POS	VSR-1
1xOC192/STM-64c switch	POS	LR
4x OC48c/STM-16c switch	DPT	SFP:
1xOC192c/STM-64c switch	DPT	IR
1xOC192c/STM-64c switch	DPT	SR
1xOC192c/STM-64c switch	DPT	VSR-1
1xOC192c/STM-64c switch	DPT	LR

Ondersteunde aanpassingscriteria

Alle door Cisco IOS-softwarerelease 12.0S ondersteunde standaard- en uitgebreide ACL-criteria worden ondersteund in het snelle pad behalve log- of fragment-ACE's.

Aantal ondersteunde ACE's

Tot 1024 ACE's worden ondersteund per richting in het snelle pad.

Opmerking: 1021 van de ACE's zijn configureerbaar. Drie lemma's zijn gereserveerd voor de impliciete **vergunning van** ACE's **om elke**, **ontken ip om het even welke**, en **verzenden naar CPU** opdrachten.

Er is geen bovengrens aan het aantal ondersteunde ACE's. Alle ACE's die de 1021-limiet overschrijden, worden uitgevoerd in het trage pad van de lijnkaart.

Uitvoer ACL-verwerking

Uitvoer-ACL's worden verwerkt in het snelle pad van de kant-en-klaag. Zie de IPv4 uitvoer ACL-lijnkaartinterfacekaart voor meer informatie.

Specifieke opdrachten voor lijnkaart

- **toon tcam appl [***acl-in***] | [***acl-out***] tcam <***label-no***>**
- **toon tcam appl [***acl-in***] | [***acl-out***] geheugen <***port***> <***aantal items***>**

Operationele richtsnoeren en lijnkaartinteracties

- Subinterface ACL's worden niet ondersteund.
- De prestaties variëren met matchdiepte.
- Bereik gebruikt twee ACL-regels (drie als de twee items een grens overschrijden).
- Eén ACL wordt ondersteund per fysieke interface.
- Tot 1024 ACE's (per richting) worden ondersteund in het snelle pad.
- De 1024 Fast path ACE's kunnen over poorten worden gedeeld.
- ACE's die het fragment gebruiken worden in de langzaam pad gefilterd.
- Gegeven pakketten worden niet geteld voor ACE's die in het langzame pad worden verwerkt.
- Als NetFlow op een Engine 0 lijnkaart is geconfigureerd en er op een uitgang ACL-kaart (toegangsmachine) 3 of 4+ lijnkaart is ingesteld, wordt de uitvoer-ACL verwerkt door zowel de inloop- als perslijnkaarten om NetFlow in staat te stellen om rekening te houden met pakketten die door ACL's worden ontkend en verzonden pakketten.

Aanbevelingen

Op dit moment niet.

Engine 4+ (Ethernet) - ACL-verwerking

Overzicht

Engine 4+ Ethernet-lijnkaarten introduceren per-VLAN invoerfunctionaliteit in hardware van Cisco 12000 10 Gigabit Ethernet-portefeuille. Dit zijn enkele van de kenmerken:

- Invoer- en uitvoerACL's kunnen tegelijkertijd op één poort worden toegepast zonder dat er sprake is van een prestatiekimpact.
- ACL's kunnen per VLAN of per poort worden toegepast.
- Voer ACL-prestaties in (tot 15K) van de ACE's is niet gedegradeerd bij matchdiepte.
- Uitvoer-ACL's worden met lijnsnelheid verwerkt voor maximaal 96 ACE's. Prestaties voor langere overeenkomsten variëren afhankelijk van matchdiepte.

Deze Ethernet lijnkaarten zijn gebaseerd op Engine 4+:

Type lijnkaart	Type interface	Type motor
10x1 GE Rev B ("X-B")	SFP:	E4+
modulair	SFP:	E4+
1 x 10 GE	10G	E4+
1 x 10 GE	10G	E4+

Ondersteunde aanpassingscriteria

Alle door Cisco IOS-softwarerelease 12.0S ondersteunde standaard- en uitgebreide ACL-criteria worden ondersteund in het snelle pad behalve log- of fragment-ACE's.

Aantal ondersteunde ACE's

- Tot 15.000 invoer ACL's die per poort of per VLAN kunnen worden geconfigureerd.
- 1024 output ACE's per kaart die per poort kunnen worden toegepast.**Opmerking:** 1021 van de ACE's zijn configureerbaar. Drie lemma's zijn gereserveerd voor de impliciete **vergunning van** ACE's **om elke**, **ontken ip om het even welke**, en **verzenden naar CPU** opdrachten.

Uitvoer ACL-verwerking

Uitvoer-ACL's worden naar verhouding verwerkt in het snelle pad van de kant-en-klaag. Zie de IPv4 uitvoer ACL-lijnkaartinterfacekaart voor meer informatie.

Specifieke opdrachten voor lijnkaart

- **groef <*number*> ip-*kabel* fuseren**

Operationele richtsnoeren en lijnkaartinteracties

- ACE's die het fragment bevatten worden verwerkt in de langzaam pad.
- ACL-tellers worden niet ondersteund voor ACL's in combinatie met andere functies.
- ACL-tellers worden niet ondersteund voor samengevoegde ACL's. Samengevoegde ACL's zijn Configureerbaar met de opdracht **voor het samenvoegen van de** module **<*sleuf nummer*> IP-telefoon**.
- Tot 168 L4-bewerkingen worden per lijnkaart ondersteund. Zodra dit wordt overschreden, wordt ACL in het langzame pad uitgevoerd.
- Als een engine 1-lijnkaart NetFlow heeft bemonsterd en er een uitvoer-ACL is ingeschakeld op een IP-motor 3 of 4+ lijnkaart, wordt de uitvoer-ACL verwerkt door zowel de ingangen- als perslijnkaarten om NetFlow in staat te stellen om rekening te houden met pakketten die door ACL's worden ontkend en verzonden pakketten.

Aanbevelingen

Op dit moment niet.

Vastlegging ACL

Vóór Cisco IOS-softwarerelease 12.0(21)S werd ACL-loginformatie uitsluitend via de onderhoudstechnop (MBUS) naar de RP verzonden. Tijdens hoge niveaus van ACL-houtkapactiviteit was het mogelijk de capaciteit van de MBUS te overschrijden. Cisco IOS-softwarerelease 12.0(21)S introduceert verschillende optimalisaties die dit scenario voorkomen.

MBUS-overloadsituaties worden door Cisco IOS-software gerapporteerd met deze foutmeldingen:

```
LCLOG-3-INVSTATE
```

```
MBUS_SYS-3-SEQUENCE
```

Met Cisco IOS-softwarerelease 12.0(21)S en later worden de logberichten met hoge dichtheid (ernst 0-4) aan de RP geleverd door de MBUS, terwijl de logberichten met lagere ernst (ernst 5-7) aan de RP worden geleverd door de switchfabric met hogere capaciteit. De ACL-logberichten zijn

zeer zwaar, dus worden nu aan de RP geleverd door de switchfabric.

Deze toegevoegde logfunctionaliteit is Configureerbaar met deze opdrachten:

- **houtkapmethode mbus [*ernst*]** — Hiermee bepaalt u welke berichten, naar ernst, naar de RP worden verzonden met behulp van de MBUS. De zwaardere berichten zullen door het materiaal van de switch worden verzonden.
- **Toont** de huidige logmethode voor alle niveaus van de berichternst.
- **logreeks-nummers**-Deze opdracht stelt de verzendende lijnkaart in staat om de reeks logberichten te sequentiëren zodat de berichten correct opnieuw geordend kunnen worden door de RP. Zonder deze opdracht kunnen logberichten in niet-sequentiële volgorde aan de RP worden geleverd.

IPv4 IP-uitvoerACL-lijnkaart (interfacekaart)

Vóór de introductie van ringweg ACL-verwerking met vrijgave van motor 3 en motor 4+ werden de uitgevoerde ACL's verwerkt door de ingangslijnkaart. Uitvoer ACL's zijn bijgewerkt om te profiteren van de hoogwaardige prestaties van Engine 3 en Engine 4+ ACL-uitvoermogelijkheden.

Deze grafiek geeft een samenvatting van waar uitvoer ACLs voor verschillende lijnkaartcombinaties wordt verwerkt:

	Bovenste lijnkaart					
Toegangslijnkaart (ACL-uitvoer) toegepast op interface van lid)	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**
E0	Ingoor	Ingoor	Ingoor	uitgang	N.v.t.	uitgang
E1	Ingoor	Ingoor	Ingoor	uitgang	N.v.t.	uitgang
E2	Ingoor	Ingoor	Ingoor	uitgang	N.v.t.	uitgang
E3	uitgang	uitgang	uitgang	uitgang	N.v.t.	uitgang
E4	uitgang	uitgang	uitgang	uitgang	N.v.t.	uitgang
E4+	uitgang	uitgang	uitgang	uitgang	N.v.t.	uitgang

Ondersteuning van IPv6 ACL

IPv6 uitgebreide ACL's worden ondersteund in langzaam pad (sterker en sterker) op E0, E1, E2, E3 en E4+ in Cisco IOS-softwarerelease 12.0(23)S.

In Engine 3 wordt IPv6 ACL-functionaliteit ondersteund in hardware van Cisco IOS-softwarerelease 12.0(25)S. ACL's worden toegepast op een specifieke interface, met een impliciete ontkenningsverklaring aan het eind van elke toegangslijst. IPv6-ACL's worden geconfigureerd met behulp van de opdracht **ipv6-toegangslijst** met de ontkennings- en vergunningssleutelwoorden in de wereldwijde configuratie-modus. Engine 3-gebaseerde kaarten ondersteunen het filteren van op verkeer gebaseerde IPv6-optiekoppen, stroometiketten en optioneel informatie over bovenlagen van het protocol.

Cisco 12000 ACL-opdrachtreferentie

Engine 1 opdrachten

- **hardware-salsa met toegangslijsten**
- **demonstratiecontroller l3 | omvat ASIC**

Engine 2 opdrachten

- **lijst van beschikbare hardware-psa-limiet 128**
- **geen lijst van hardware-psa**
- **bypass**
- **PSA-details tonen**
- **een samenvatting van de toegangslijst tonen**
- **PSA-functie van controller**

Engine 3 opdrachten

- **Hoe-module <*sleuf #*> tcam compileren niet-samenvoegen***!— vanaf Cisco IOS-softwarerelease 12.0(21)S3***
- **hardware-interface met TOEGANG-lijst <*interfacenaam*>**
- **toon contr [*tofab|frfab*] alfa acl <*int*> vmr2ace**

Engine 4+ opdrachten

- **label van de toegangslijst gen7**
- **toon tcam appl [*acl-in] | acl-out*] tcam <*label-no*>**
- **toon tcam appl [*acl-in] | acl-out*] geheugen <*port*><*aantal items*>**

Engine 4+ Ethernet-opdrachten

- **groef <*number*> ip-*kabel* fuseren**

Lijst

In deze paragraaf worden standaarddefinities van relevante termen gegeven:

- **Plannen voor verwerking** - Een netwerkapparaat kan logisch worden verdeeld in drie verwerkingsvlakken:Datacenterrein-Verwerking op de pakketten die door het netwerkapparaat stromen.Bedieningsplatform: verwerking op de pakketten die worden gebruikt om netwerkapparaten aan elkaar te koppelen. Dit omvat lijnprotocollen (zoals Point-to-Point Protocol - PPP en High-Level Data Link Control - HDLC), routingprotocollen (Border Gateway Protocol - BGP, Routing Information Protocol versie 2 - RIPv2, Open Shortest Path First - OSPF, enzovoort) en tijdprotocollen (zoals Network Time Protocol - NTP).Beheerplan:

verwerking op pakketten die worden gebruikt om de netwerkapparaten te beheren. Dit omvat telnet, Secure Shell (SSH), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), SNMP en andere beheerprotocollen.

- **Standaard ACL's**- Standaard ACL's-filter uitsluitend op Layer 3.
- **Uitgebreide ACL**'s - Uitgebreide IP-toegangslijsten gebruiken bron- en doeladressen voor matching-operaties evenals optionele protocol-type informatie voor fijnere granulariteit van controle.
- **Lineaire Verwerkte ACL**'s - lineair verwerkt in software. De prestaties variëren met matchdiepte (het aantal items dat moet worden gecontroleerd voordat een match wordt bepaald).
- **Turbo ACL's (Compileerd)**—Turbo's optimaliseren de softwareverwerking door een ACL te compimeren in een zeer geoptimaliseerde reeks lookup-tabellen die de softwareverwerking versnellen. De prestaties van Turbo ACL's variëren niet met de matchdiepte.
- **Voer ACL**'s in - Een ACL die op verkeer wordt toegepast dat de poort in gaat waarop het wordt toegepast.
- **Uitvoer ACLs**—Een ACL die op verkeer wordt toegepast dat de poort waarop deze wordt toegepast verlaat. Op enkele uitzonderingen na worden uitgevoerde ACL's verwerkt door de invoerlijnkaart.
- **Ontvang ACL**'s (**Pad**) - ontvang ACL**'**s (Pad) het filteren voor controleverkeer dat voor de router zelf is bestemd, zoals het routeren van updates en SNMP vragen.
- **Lijnkaart** met **dubbele stap doorsturen**—lijnkaarten die ASIC's met doorsturen/uitvoeren op zowel het ingangspad als het toegangspad. Hierdoor kan de lijnkaart functies uitvoeren op zowel de Packet Flow als de pakketstroom vergroten zonder pakketten naar de LC CPU te lekken. Het maakt het ook mogelijk dat nieuwe golven van algoritmen in twee fasen worden gebruikt binnen Cisco 12000. De Engine 3 lijnkaart is een voorbeeld van een lijnkaart voor tweevoudig doorsturen.
- **Lijnkaart** met **één** fase **doorsturen**-lijnkaarten die ASIC's op alleen het ingangspad hebben doorgestuurd/kenmerken. Deze lijnkaarten voeren alleen op ASIC gebaseerde verwerking uit op de pakketten die op het ingangspad stromen. Het uitgaande verkeer wordt niet verwerkt (net doorgestuurd), verwerkt door de ASIC's van andere LC's, of beheerd door de LC CPU's. Engine 2, Engine 4 en Engine 4+ zijn voorbeelden van lijnkaarten met één stap doorsturen.

Gerelateerde informatie

- Cisco 12000 Series internet-routers
- Technische ondersteuning en documentatie – Cisco Systems