

# Implementierung von Zugriffslisten auf Cisco Internet Router der Serie 1200

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Übersicht über die ACL-Unterstützung auf dem Cisco Internet Router der Serie 12000](#)

[ASIC-basierte ACLs und CPU-basierte ACLs](#)

[Filterung der Steuerungs- und Verwaltungsebene](#)

[Konfigurieren von IP-Receive-Path-ACLs](#)

[IPv4-ACL-Unterstützung nach Line Card-Typ](#)

[Engine 0 - ACL-Verarbeitung](#)

[Engine 1 - ACL-Verarbeitung](#)

[Engine 2 - ACL-Verarbeitung](#)

[ISE \(IP Services Engine\) Engine 3 - ACL-Verarbeitung](#)

[Engine 4 \(POS\) - ACL-Verarbeitung](#)

[Engine 4+ \(POS und DPT\) - ACL-Verarbeitung](#)

[Engine 4+ \(Ethernet\) - ACL-Verarbeitung](#)

[ACL-Protokollierung](#)

[IPv4-Ausgabe-ACL - Line Card-Interoperation-Matrix](#)

[IPv6 ACL-Unterstützung](#)

[Cisco 12000 ACL-Befehlsreferenz](#)

[Glossar](#)

[Zugehörige Informationen](#)

## **[Einführung](#)**

Dieses Dokument beschreibt die Unterstützung für Zugriffskontrolllisten (ACLs) auf den Cisco Internet Routern der Serie 12000.

## **[Voraussetzungen](#)**

## **[Anforderungen](#)**

Cisco empfiehlt, dass Sie über Kenntnisse der Grundlagen einer ACL auf einem Cisco Router verfügen.

Allgemeine Informationen zu Zugriffskontrolllisten und ihren Anwendungen finden Sie in diesen Dokumenten:

- [Zugriffskontrolllisten: Übersicht und Richtlinien](#)
- [Konfigurieren von IP-Services: IP-Pakete filtern](#)

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Internet Routern der Serie 12000.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions \(Technische Tipps von Cisco zu Konventionen\)](#).

# Übersicht über die ACL-Unterstützung auf dem Cisco Internet Router der Serie 12000

Auf dem Cisco Internet Router der Serie 1200 können ACLs in Hardware (Application-Specific Integrated Circuit - ASIC), Software (CPU einer Linecard) oder als Hybrid-Funktion (in Software mit Hardwareunterstützung) verarbeitet werden. Ob eine ACL in Hardware oder Software verarbeitet wird, hängt von der ACL-Anwendung, dem Line Card-Engine-Typ und der Interaktion von ACLs mit anderen Linecards ab.

Die Line Card Engines der Cisco Serie 12000 bieten unterschiedliche ACL-Funktionen. Informationen zum ACL-Support für eine bestimmte Line Card-Engine finden Sie im entsprechenden Abschnitt dieses Dokuments.

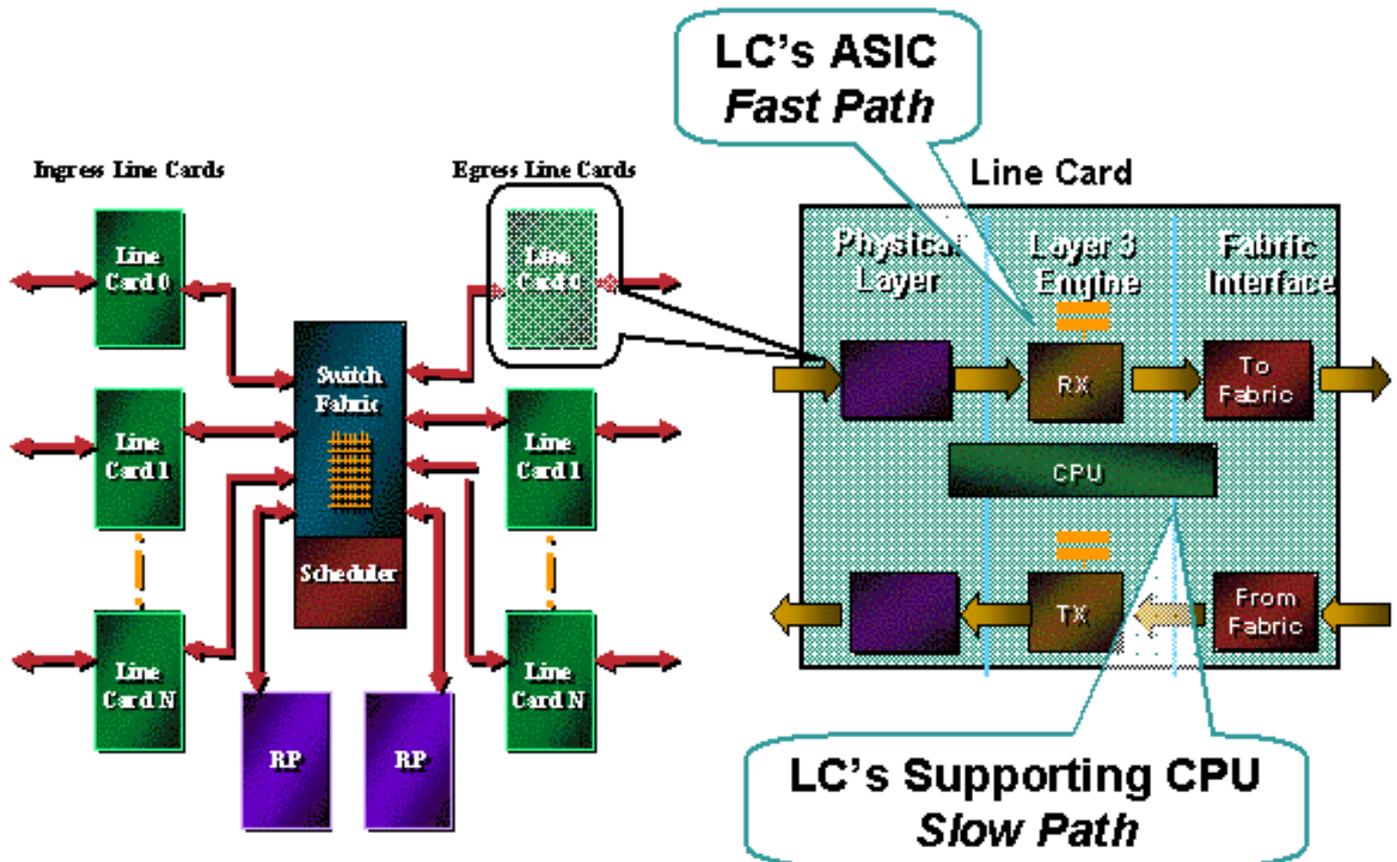
**Hinweis:** IP-Multicast-ACLs werden in der Cisco IOS® Software, Version 12.0S, nicht unterstützt. Die Funktion zur IP-Multicast-Begrenzung kann verwendet werden, wenn Multicast-Filterung erforderlich ist. Weitere Informationen finden Sie unter [Fast-Path Multicast Forwarding auf den Cisco Line Cards der Serie 12000 Engine 2 und ISE](#).

## ASIC-basierte ACLs und CPU-basierte ACLs

Der Cisco 12000 unterstützt alle Generationen der ACL-Verarbeitung. Für die effektive Nutzung von ACL auf der Cisco Serie 1200 ist es entscheidend, dass die einzelnen Verarbeitungsmodi funktionieren, interagieren und sich gegenseitig unterstützen.

Frühe Generationen der ACL-Verarbeitung verwendeten für die Verarbeitung der ACL eine programmierbare CPU. Im Laufe der Zeit überstiegen die Verarbeitungsanforderungen für Pakete pro Sekunde (PPS) die Fähigkeit neuer CPUs, mit der Entwicklung Schritt zu halten. ASICs wurden entwickelt, um höhere PPS-Raten für die Router-Weiterleitung und Funktionen zu erreichen. ACLs, die auf der Linecard (LC)-CPU geladen wurden, wurden dann auf den LC ASIC geladen. ASICs wurden weiterhin verbessert, um höhere PPS-Raten zu bewältigen. Diese ASICs

der zweiten Generation basieren auf der Pionierarbeit der vorherigen Generation und bieten mehr ASIC-Funktionen. Da es sich bei der Cisco Serie 1200 um eine verteilte Routing-Plattform handelt, kann die Interaktion zwischen den verschiedenen Generationen der ACL-Verarbeitung betriebliche Verwirrung stiften.



Begriffe wie ASIC-basierte ACL, CPU-basierte ACL, Fast Path, Slow Path und ASIC Punts werden in diesem Dokument verwendet, um zu erläutern, was mit der ACL-Verarbeitung geschieht. Hier einige Erklärungen zu diesen Begriffen:

- ASIC-basierte ACLs (Fast Path) - ACLs werden in die ASIC-Hardware geladen und verarbeitet. Die Leistungsumgebung des ASICs bestimmt Tiefe, Leistung und Funktionen der Zugriffskontrollliste. Im Pfad wurde Fast Path verwendet, um den Unterschied zwischen ASIC-basierter Verarbeitung und Verarbeitung in der LC-unterstützenden CPU zu veranschaulichen. In diesem Dokument wird der generische Begriff ASIC-basiert verwendet.
- CPU-basierte ACLs (Slow Path) - ACLs werden in der Software der Linecard-CPU verarbeitet. Bei den Karten der ersten Generation (Engine 0 und in einigen Fällen Engine 1) erfolgt die gesamte Verarbeitung auf der LC-CPU. ASIC-basierte LCs führen die Verarbeitung von ACLs auf Paketen durch, die aus dem ASIC ausgelesen werden. In der Vergangenheit wurde mithilfe von "Slow Path" veranschaulicht, wie die Stanzzeiten an die LC-CPU langsamer waren als die ASIC. In diesem Dokument wird der eher allgemeine Begriff CPU-basiert verwendet.
- ASIC Punts: ASICs verfügen über strikte Design-Umschläge. Wenn ein Paket den vorgesehenen Umschlag überschreitet, wird es vom ASIC abgestraft, um entweder auf dem LC, der die CPU unterstützt, verarbeitet oder an den Route Processor (RP) gesendet zu werden. ASIC-basierte ACLs gehen bei Paketen ein, die nicht zum Design der ASIC gehören. Ein Beispiel ist eine ACL mit einem ACE mit einem log- oder log-input-Schlüsselwort. Die für die Protokollierung des Pakets erforderlichen Informationen müssen außerhalb des ASIC

verarbeitet werden, sodass das Paket automatisch aus dem ASIC in die LC-CPU geleitet und wie eine normale CPU-basierte ACL verarbeitet wird.

**Hinweis:** Wenn Sie richtlinienbasiertes Routing (PBR) mit Übereinstimmungsanweisungen konfigurieren, um ACLs zuzuordnen, sollten die ACLs nicht mit dem Quell-Port übereinstimmen. Der Gigabit-Switch-Router (GSR) unterstützt kein Hardware-Switching für den PBR mit ACLs, die mit dem Quell-Port übereinstimmen. Es löst Switching-Prozesse aus, und die GSR-Leistung nimmt ab.

## Filterung der Steuerungs- und Verwaltungsebene

Der Router-Prozessor bietet Services für die Kontroll- und Verwaltungsebene in der verteilten Architektur der Cisco Serie 12000. Receive Path ACLs (rACLs) bieten eine einfache verteilte Filterfunktion für Steuerungs- und Verwaltungsdatenverkehr, der für den RP bestimmt ist. Sie kann logisch als zusätzliche Sicherheitsebene betrachtet werden, die die Stärken einer verteilten Architektur nutzt.

### Konfigurieren von IP-Receive-Path-ACLs

Die rACL wurde durch eine spezielle Verzichtserklärung in die Wartungsdrosselung der Cisco IOS® Software Version 12.0(21)S2 eingeführt. Sie wird offiziell von der Cisco IOS Software, Version 12.0(22)S, unterstützt. Weitere Informationen finden Sie unter [IP Receive ACL \(IP-Empfangszugriffskontrollliste\)](#).

Der Router-Prozessor bietet Services für die Steuerungsebene in der verteilten Architektur der Cisco Serie 12000. Die Receive-ACLs bieten Filterfunktionen für den für den RP bestimmten Steuerungsdatenverkehr, z. B. Routing-Updates und SNMP-Abfragen (Simple Network Management Protocol).

Die rACL wird als Phase 1 einer mehrphasigen Anstrengung betrachtet, um der Steuerung und Verwaltung des Datenverkehrs auf der Ebene neue Schutzfunktionen hinzuzufügen. Neue Verbesserungen bei der Ratenbegrenzung werden durch Software-Updates hinzugefügt.

## IPv4-ACL-Unterstützung nach Line Card-Typ

Die Linecards der Serie 12000 bieten je nach Motorentyp unterschiedliche ACL-Funktionen. In diesem Abschnitt werden die ACL-Funktionen der verschiedenen Line Card Engines beschrieben. Informationen zur ACL-Unterstützung für ein bestimmtes Line Card-Modul finden Sie im entsprechenden Abschnitt dieses Dokuments.

Es gibt einige allgemeine Merkmale für alle ACLs (ASIC- und CPU-basiert):

- Für jede Richtung kann nur eine ACL auf eine Schnittstelle angewendet werden. Die Schnittstelle POS 0/0 kann beispielsweise nur eine Eingangs-ACL und eine Ausgangszugriffskontrollliste haben.
- Das Testen des Pakets mit einer ACL wird beendet, nachdem eine Übereinstimmung gefunden wurde. Wenn eine ACL mit 300 Einträgen mit dem Paket im Access-List Entry (ACE) #45 übereinstimmt, wird das Paket verarbeitet und die ACL-Verarbeitung gestoppt.
- Am Ende jeder Zugriffskontrollliste wird implizit **jede** Eingabe **abgelehnt**. Wenn die ACL keine Übereinstimmung enthält, wird das Paket verworfen. Cisco ACLs werden mit *expliziter* ACL-

Architektur erstellt. Das bedeutet, dass ein ACE vorhanden sein muss, der mit dem Paket übereinstimmt, damit es verarbeitet und weitergeleitet werden kann.

- Neu hinzugefügte ACEs werden immer am Ende der ACL angehängt. Wenn die ACL aktualisiert werden muss, empfiehlt es sich, die ACL zu entfernen (den Befehl **no access-list** zu verwenden) und die neue ACL erneut hinzuzufügen.
- Da nicht initiale IP-Fragmente keine Layer-4-Protokollinformationen im IP-Header enthalten, werden nur Standard-Abgleichkriterien für nicht initiale Fragmente unterstützt. Ausführliche Informationen darüber, wie Cisco ACLs die IP-Fragmentfilterung erfüllen, finden Sie in [Zugriffskontrolllisten und IP-Fragmenten](#).
- Nummerierte ACLs werden verarbeitet und angewendet, sobald sie über die Befehlszeilenschnittstelle (CLI) eingegeben werden. Bei großen ACLs führt dies manchmal zu einer CPU-Spitze auf dem RP oder der LC-CPU.

## Engine 0 - ACL-Verarbeitung

Engine 0 ist die erste Line Card, die für die Cisco Serie 1200 bereitgestellt wird. Dabei handelt es sich ausschließlich um CPU-basierte Verarbeitung und Weiterleitung. Engine 0-Linecards verarbeiten daher ACLs in der LC-CPU.

Diese Linecards basieren auf Engine 0:

Line Card-Typ	Schnittstellentyp	Konnektivität
12 x DS3	Koaxialkabel	SMB
12 x DS3	Koaxialkabel	SMB
12 x E3	Koaxialkabel	SMB
1xCHOC12->DS3		IR
1xCHOC12/STM4 ->OC3/STM1	POS	IR
4 x OC3c/STM1c	POS	SR
4 x OC3c/STM1c	POS	LR
4 x OC3c/STM1c	POS	MM
1 x OC12c/STM4c	POS	IR
1 x OC12c/STM4c	POS	MM
6xCT3->DS1		SMB
2xCHOC3/STM1- >DS1/E1		IR
4 x OC3c/STM1c	Geldautomat	IR
4 x OC3c/STM1c	Geldautomat	MM
1 x OC12c/STM4c	Geldautomat	IR
1 x OC12c/STM4c	Geldautomat	MM

## Unterstützte Anpassungskriterien

Alle Cisco IOS Software Release 12.0S Standard, Extended ACL und Turbo ACLs werden von Engine 0 unterstützt.

### Anzahl unterstützter ACEs

Die ACL-Größe ist nur durch Leistungsanforderungen und verfügbare Speicherressourcen beschränkt.

### Ausgabe-ACL-Verarbeitung

Die Ausgabe-ACLs werden im Eingangs-Featurepfad der anderen Linecards im System verarbeitet. Ein Push der Output ACL an die Eingangsseite der anderen LCs schützt die Backplane vor dem Weiterleiten von Paketen, die verworfen werden. Dies ist eine von der verteilten Architektur des Cisco 7500 geerbte Funktion. Detaillierte Erläuterungen, Gründe und betriebliche Richtlinien finden Sie in der [IPv4-Ausgabe-ACL - Line Card Interoperation Matrix](#).

### Line Card-spezifische Befehle

None.

### Betriebsrichtlinien und Line Card-Interaktionen

- Wenn NetFlow auf einer Line Card der Engine 0 konfiguriert ist und eine Ausgabe-ACL auf einer Line Card der Ausgangs-Engine 3 oder 4+ konfiguriert ist, wird die Ausgabe-ACL sowohl von den Eingangs- als auch von den Ausgangs-Linecards verarbeitet, damit NetFlow Pakete, die von ACLs abgelehnt wurden, sowie weitergeleitete Pakete berücksichtigen kann.

### Empfehlungen

Cisco empfiehlt die Verwendung von Turbo ACLs auf Engine 0 für große ACLs. Kleine lineare ACLs sind für kleinere ACLs effizienter, da Turbo ACLs zusätzlichen Speicher benötigen.

### Engine 1 - ACL-Verarbeitung

#### Übersicht

Die Line Card Engine 1 ist eine Brücke zwischen der CPU-basierten Verarbeitung der Engine 0 und der ASIC der ersten Generation für Weiterleitung/Funktion auf Engine 2. Line Cards der Engine 1 verarbeiten standardmäßig ACLs in der Software. Mit der Cisco IOS Software Version 12.0(10)S und höher stellt Engine 1 Hardware-ACLs für Karten bereit, die mit Version 4 oder 5 des Salsa ASIC ausgestattet sind (siehe Befehlsreferenz für Line Card unten, um zu bestimmen, mit welcher Version von Salsa eine bestimmte Karte ausgestattet ist).

Diese Line Cards basieren auf Engine 1:

Line Card-Typ	Schnittstellentyp	Konnektivität
8 x FE	(RJ45)	100BaseT
8 x FE	(MM)	100Base F

8 x FE	(RJ45)	100BaseT
8 x FE	(MM)	100Base F
1 x GE	SX,	GBIC:
1 x GE	SX,	GBIC:
2 x OC12c/STM4c	DPT	IR
2 x OC12c/STM4c	DPT	LR
2 x OC12c/STM4 c	DPT	XLR
2 x OC12c/STM4c	DPT	MM
2 x OC12c/STM4c	DPT	IR
2 x OC12c/STM4c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2 x OC12c/STM4c	DPT	MM

### [Unterstützte Anpassungskriterien](#)

Alle Cisco IOS Software Release 12.0S-unterstützten Standard-, Extended- und Turbo-ACLs werden von der LC-CPU (Slow Path) unterstützt. Darüber hinaus kann Engine 1 Eingabe-ACLs im Salsa ASIC verarbeiten. Der Salsa ASIC verarbeitet die Eingangs-ACL-Verarbeitung zusammen mit der Routensuche. Dadurch wird die Leistung im Vergleich zur herkömmlichen linearen ACL-Verarbeitung und der Turbo ACL-Verarbeitung erhöht. Der Salsa ASIC kann keine ausgehenden ACLs oder Schnittstellen-ACLs verarbeiten.

### [Anzahl unterstützter ACEs](#)

Die ACL-Größe ist nur durch Leistungsanforderungen und verfügbare Speicherressourcen beschränkt.

### [Ausgabe-ACL-Verarbeitung](#)

Die Ausgabe-ACLs werden im Eingangs-Featurepfad der anderen Linecards im System verarbeitet. Weitere Informationen finden Sie im Abschnitt [IPv4-Ausgabe-ACL - Line Card Interoperation Matrix](#) ([Schnittstellenkartenmatrix](#) für die Line Card).

### [Line Card-spezifische Befehle](#)

- Zugriffslisten-Hardwaresalsa
- Show Controller I3 | ASIC einschließen

### [Betriebsrichtlinien und Line Card-Interaktionen](#)

- Der Salsa ASIC und der PSA ASIC können nicht gleichzeitig betrieben werden. Der **Zugriffslisten-Hardware**-Befehl akzeptiert nur PSA (Engine 2) oder Salsa (Engine 1), aber nicht beide.
- Wenn NetFlow auf einer Line Card der Engine 1 konfiguriert und eine Ausgabe-ACL auf einer Line Card der Ausgangs-Engine 3 oder 4+ konfiguriert ist, wird die Ausgabe-ACL sowohl von den Eingangs- als auch von den Ausgangs-Linecards verarbeitet, damit NetFlow Pakete berücksichtigen kann, die von ACLs abgelehnt wurden, sowie weitergeleitete Pakete.

## Empfehlungen

Für Versionen von Line Cards der Engine 1, die keine Hardware-ACLs unterstützen, empfiehlt Cisco die Verwendung von Turbo ACLs für große ACLs. Kleine ACLs (weniger als 20 Leitungen) können zur Speichereinsparung als lineare ACLs implementiert werden.

## Engine 2 - ACL-Verarbeitung

### Übersicht

Die Engine 2 war die erste Linecard mit einem Weiterleitungs-/Funktionen-ASIC. Mit der Cisco IOS Software, Version 12.0(10)S und höher, bieten Line Cards der Engine 2 Hardware-ACL-Funktionen im leistungsstarken Packet Switching ASIC (PSA). Wie bei allen Weiterleitungs-/Feature-ASICs legen auch bei strengen Performance-Umschlägen die Funktionen des ASICs Grenzen. Die Leistungsumgebung für die Engine 2-ACLs ist auf Speicherbeschränkungen im PSA ASIC zurückzuführen.

Die Paketweiterleitung in Engine 2 erfolgt durch den PSA ASIC. PSA verfügt über drei externe Hauptspeicherorte:

- PLU (Path lookup) - Wird zum Speichern mehrerer Knoten verwendet.
- TLU (Table Lookup) - Wird zum Speichern von FIB-Blättern und möglicherweise Lastausgleich-Strukturen verwendet. Wird auch für die Speicherung vieler PSA ACL-Datenstrukturen verwendet
- SRAM - Der primäre Standort für Strukturen mit Lastverteilung

Die PSA ACL-Funktion ist eine mikrocodebasierte Implementierung der ACL-Überprüfung. Ein spezieller Befehlssatz wird in den PSA-Chip geladen, der eine grundlegende Überprüfung der ACL ermöglicht. Es gibt eine Reihe von Einschränkungen für diese Funktion, die vor der Bereitstellung sorgfältig durchdacht werden sollten. Ein Hauptnachteil bei PSA-ACLs ist die große Menge an Hardware-Forwarding-Speicher, die erforderlich ist.

Die PSA ACL-Funktion erfordert, dass unabhängig von der Anzahl der Präfixe usw. ein großer Block PLU/TLU-Speicher vorab zugewiesen wird. Da diese Zuweisung primär aus dem TLU-Bereich stammt, hat sie erhebliche Auswirkungen auf die Anzahl der Routen, die auf diesen Karten beibehalten werden können, wenn PSA-ACLs konfiguriert werden.

Zusätzlich zur Erstaussgabe des PLU/TLU-Speichers benötigt jedes im TLU-Speicher gespeicherte Präfix erheblich mehr Speicher. Die für jedes Präfix erforderliche Speichergröße variiert je nach der gewählten ACL-Richtung (Eingang/Ausgang) und dem Linecard-Typ. Ausgangs-ACLs benötigen im Allgemeinen mehr Arbeitsspeicher als Eingangs-Linecards, und Linecards mit mehr physischen Ports benötigen mehr Arbeitsspeicher als Linecards mit weniger Ports.

Wenn die Engine-2-Linecard keine ACLs verwendet, werden die Datenstrukturen für die ACL unabhängig von den tatsächlich konfigurierten ACLs erstellt. Um zu den kleineren Nicht-ACL-Strukturen zu wechseln, müssen Sie **keine Zugriffslisten-Hardware-PSA** auf dem Router konfigurieren. Dieser Befehl deaktiviert die gesamte ACL-Verarbeitung auf allen Engine2-Linecards in allen Richtungen. Cisco empfiehlt, diese mit äußerster Vorsicht einzusetzen.

## Übersicht

Um eine von der Match-Tiefe unabhängige ACL-Verarbeitungsleistung bereitzustellen, sind Engine 2-ACLs in die Hardware-Weiterleitungstabelle integriert. Nachstehend finden Sie Erklärungen dazu, wie sich dies auf die Skalierbarkeit von Präfixen auswirken kann.

Diese Linecards basieren auf Engine 2:

Line Card-Typ	Schnittstellentyp	Konnektivität
1 x OC48c/STM16c	POS	SR
1 x OC48c/STM16c	POS	LR
1 x OC48c/STM16c	POS	SR
1 x OC48c/STM16c	POS	LR
1 x OC192c/STM64c	Enabler	SR
16 x OC3c/STM1c	POS	IR
16 x OC3c/STM1c	POS	MM
4 x OC12c/STM4c	POS	IR
4 x OC12c/STM4c	POS	MM
4 x OC12c/STM4c	POS	IR
4 x OC12c/STM4c	POS	MM
4 x OC12c/STM4c	Geldautomat	IR
4 x OC12c/STM4c	Geldautomat	MM
8xOC3cSTM1c	Geldautomat/TS	IR
8xOC3c/STM1c	Geldautomat/TS	MM
3 x GE	SX	GBIC:
3 x GE	CWDM	GBIC:
1 x OC48c/STM16c	DPT	SR

1 x OC48c/STM16c	DPT	LR
1 x OC48c/STM16c	DPT	SR
1 x OC48c/STM16c	DPT	LR

### [Unterstützte Anpassungskriterien](#)

Alle Cisco IOS Software-Versionen 12.0S unterstützten die Kriterien für Standard- und Extended ACL-Übereinstimmungen mit Ausnahme der Layer-4-Quellports. Diskontinuierliche Masken, IP-Prioritätsfelder und Layer-4-Quellports werden vom PSA ASIC abgefragt und auf der LC-CPU verarbeitet.

### [Anzahl unterstützter ACEs](#)

Bis zu fünf 448-Leitungs-Eingangs-ACLs im PSA. Pro Port kann eine ACL konfiguriert werden. Zusätzliche ACLs werden von der Linecard-CPU verwaltet. Einschränkungen für die Ausgabe-ACLs finden Sie im Abschnitt "Einschränkungen" weiter unten.

### [Ausgabe-ACL-Verarbeitung](#)

Eine auf dieser Linecard konfigurierte Ausgabe-ACL wird im Eingangs-Feature-Pfad der anderen Linecards im System ausgeführt. Weitere Informationen finden Sie unter [IPv4-Ausgabe-ACL - Line Card Interoperation Matrix \(Schnittstellenmatrix für Line Cards\)](#).

### [Line Card-spezifische Befehle](#)

- **Zugriffsliste Hardware-PSA-Limit 128**
- **kein Zugriffslisten-Hardware-PSA**
- **PSA-Umgehung**
- **show access-list psa detail**
- **show access-list psa summary**
- **Show Controller PSA-Funktion**

### [Betriebsrichtlinien und Line Card-Interaktionen](#)

- Die schnelle Verarbeitung von Zugriffskontrolllisten erfordert die Erfüllung folgender Bedingungen: Die angewendete ACL liegt innerhalb des Grenzwerts von 128 oder 448 ACE. Wenn der Befehl **access-list hardware psa limit 128** konfiguriert ist, muss die Länge weniger als 128 ACEs betragen. Wenn das 448-Leitungs-ACL-Mikrocodepaket erforderlich ist, muss die Länge weniger als 448 ACEs betragen. Eingabe- und Ausgabe-ACLs werden nicht zusammen pro Karte konfiguriert. Auf dem *Router* können bis zu fünf ausgehende ACLs konfiguriert werden.
- Nur 128-Leitungs-ACLs werden auf 8- und 16-Port OC-3/STM-1 POS Line Cards unterstützt. 448 Line ACLs werden von OC-12/STM-4 POS mit 4 Ports, OC-48/STM-16 POS mit 1 Port und Gigabit Ethernet Line Cards mit 3 Ports unterstützt.
- Eingangs-ACLs haben im schnellen Pfad Vorrang vor Ausgangs-ACLs, wenn beide

gleichzeitig auf derselben Karte konfiguriert werden (die Ausgabe-ACL wird im langsamen Pfad verarbeitet).

- Wenn eine Ausgabe-ACL auf einer Engine 2-Karte konfiguriert ist und die Eingangs-Linecard die Engine 0/1/2/4 ist, wird eine Ausgabe-ACL auf der Eingangskarte verarbeitet. Bei anderen Motortypen wird die Ausgabe-ACL im Ausgangs-langsam folgenden Pfad von Engine 2 verarbeitet.
- Die Ausgabe-ACLs werden für den IP-zu-MPLS-Datenverkehr nicht unterstützt (das erste MPLS-Label wird auf ein IP-Paket übertragen).
- Die Informationen zur ACL-Verarbeitung sind in die Hardware-FIB integriert und können die Skalierbarkeit von Präfixen beeinträchtigen. Die Erschöpfung des Präfixspeichers wird durch Speicherzuweisungsfehler mit der Signatur "exmem=1" in der zugehörigen Protokollmeldung gemeldet.

## Empfehlungen

- Die Informationen zur ACL-Verarbeitung sind in die CEF-Weiterleitungstabelle integriert, wodurch die Präfixskalierbarkeit verringert wird. Anwendungen, die keine ACLs verwenden, können die ACL-Unterstützung in der CEF-Tabelle deaktivieren und so den verfügbaren Präfixspeicher erhöhen, indem sie den Befehl **no access-list hardware psa** eingeben.
- Durch die Konfiguration des Befehls **no access-list hardware psa** wird die gesamte ACL-Verarbeitung durch Engine 2-Karten deaktiviert und die PSA-Unterstützung für ACLs deaktiviert. Sie erzwingt nicht die Ausführung von Zugriffskontrolllisten durch die Software. Diese Bedingung gilt auch, wenn für die Ausgangs-Linecard eine Ausgangs-ACL konfiguriert ist.
- Die Konfiguration des **kompilierten** Befehls **access-list** nach dem Befehl **access-list hardware psa** wandelt ACEs, die die Kapazität des PSA überschreiten, in eine Turbo ACL um. Dies bietet eine optimale ACL-Leistung für ACLs mit mehr als 448 ACEs Länge. Der Standard-ACL-Mikrocode lautet 128 (ab Cisco IOS Software Release 12.0(14)S/ST). Wenn kleinere ACLs verwendet werden und die 448-Leitungs-Funktion nicht erforderlich ist, wird beim Konfigurieren des **Zugriffslisten-Hardware-PSA-Limit 128**-Befehl der Weiterleitungsspeicher (TLU) beibehalten, was die Präfixskalierbarkeit verbessert). Die Turbo-ACL-Verarbeitung sollte mit dem Befehl **access-list compiled** für ACLs mit einer Länge von mehr als 129 Zeilen zusammen mit dem Befehl **access-list hardware psa limit 128** aktiviert werden. Diese Kombination verarbeitet die ersten 128 Zeilen im PSA ASIC und die übrigen Zeilen mit Turbo-ACLs, wodurch die Leistung optimiert und gleichzeitig der Speicher für die Weiterleitung eingespart wird.
- Die OC12 ATM-Linecard mit 4 Ports unterstützt keine Eingabe-ACLs, bietet aber eine Ausgabe-ACL-Erkennung im Mikrocode, wodurch die Verarbeitung von ausgehenden ACLs im langsamen Pfad ermöglicht wird.
- Die 8xOC3 ATM-Linecard unterstützt ACLs mit 12.0(23)S-Version und höher der Cisco IOS-Software für VC-128-Leitungen. Es können maximal 16 verschiedene Eingangs-ACLs im schnellen Pfad konfiguriert werden. 448-Eingangs-ACL wird auf VC-basierter Basis nur in langsamem Pfad unterstützt. Ausgabe-ACLs werden nicht unterstützt.

## ISE (IP Services Engine) Engine 3 - ACL-Verarbeitung

### Übersicht

Die Engine 3 ist die erste Dual-Stage Forwarding Line Card. Die Engine 3 verfügt über Weiterleitungs-/Funktionen-ASICs auf dem Eingangs- und Ausgangs-Pfad. Auf diese Weise können ACLs sowohl auf dem Eingangs- als auch auf dem Ausgangs-Pfaden in ASICs platziert werden. Darüber hinaus ist die ASIC-Struktur der Engine 3 eine Hybridpipeline/ein paralleles Array. Die ASIC-Struktur implementiert die ACL-Verarbeitung im parallelen Ternary Content Addressable Memory (TCAM) mit hoher Geschwindigkeit, der die Verarbeitung von bis zu 20.000 ACEs pro Eingang und 20.000 ACEs pro Ausgang mit Leitungsgeschwindigkeit ermöglicht.

Diese Linecards basieren auf Engine 3:

Line Card-Typ	Schnittstellentyp	Konnektivität
4 x OC12c/STM4c	POS	IR
4 x OC12c/STM4c	POS	MM
4 x CHOC12/STM4->OC3/STM1->DS3/E3	POS	IR
16 x OC3c/STM1c	POS	IR
16 x OC3c/STM1c	POS	MM
8 x OC3/STM1c	POS	IR
8xOC3c/STM1c	POS	MM
4 x OC3c/STM1c	POS	IR
4 x OC3c/STM1c	POS	MM
4 x OC3c/STM1c	POS	LR
1 x OC48c/STM16c	POS	SR
1 x OC48c/STM16c	POS	LR
1xCHOC48/STM16->STM4->OC3/STM1->DS3/E3	POS	SR
4 x OC12c/STM4c	ATM/IP	IR
4 x OC12c/STM4c	ATM/IP	MM
4 x GE	GE	
4 x OC12c/STM4c	DPT	IR
4 x OC12c/STM4c	DPT	XLR

[Unterstützte Anpassungskriterien](#)

Alle Cisco IOS Software Release 12.0S Standard- und Extended Match-Kriterien werden im schnellen Pfad unterstützt, mit Ausnahme von Protokoll-ACEs, die von der Linecard-CPU verarbeitet werden.

### Anzahl unterstützter ACEs

- Verarbeitung der Leitungsgeschwindigkeit in Eingangs- und Ausgangsrichtung pro Port, pro VLAN, pro Frame-Relay-Subschnittstelle und pro ATM-Subschnittstelle. Es werden bis zu 20.000 erweiterte ACEs pro Richtung und Karte unterstützt.
- Die Zuordnungskriterien für TCP/UDP-Quell-/Ziel-Port "Range", "lt" und "gt" werden in der Hardware mit "L4-Operator"-Ressourcen behandelt.
- Die Anzahl der verschiedenen L4-Operanden ist für die gesamte Linecard auf 32 beschränkt. Die Anzahl der Betreiber von Quellports ist auf maximal sechs beschränkt.

### Ausgabe-ACL-Verarbeitung

Native Fast-Path-Unterstützung für die Verarbeitung von ausgehenden ACLs mit Leitungsgeschwindigkeit im Transmit-Path-Paketverarbeitungs-ASIC. Weitere Informationen finden Sie unter [IPv4-Ausgabe-ACL - Line Card Interoperation Matrix \(Schnittstellenmatrix für Line Cards\)](#).

### Line Card-spezifische Befehle

- `hw-module <Steckplatz #> tcam kompilieren ohne Merge!—12.0(21)S3`
- `Hardware-Schnittstelle der show-access-list <Schnittstellename>`
- `show cef int pos[x/y] | inc if_number`

### Betriebsrichtlinien und Line Card-Interaktionen

- Pakete, die die Protokoll-ACEs abgleichen, werden im langsamen Pfad verarbeitet.
- Pakete, die mit deny ACEs übereinstimmen (gedrosselt, um eine Unterbrechung des Systems zu verhindern), werden im langsamen Pfad verarbeitet.
- Wenn eine ACL einen Adressbereich umfasst, verwendet die Hardware spezielle ACEs, die als "Range ACEs" bezeichnet werden und bis zu drei ACEs erfordern.
- Durch das Zusammenführen von Zugriffskontrolllisten können TCAM-Ressourcen eingespart werden, indem gemeinsame ACEs für einzelne Zugriffskontrolllisten freigegeben werden. Um zu bestimmen, ob eine ACL zusammengeführt wird, verwenden Sie den Befehl **show-access-list Hardware interface**.
- ACL-Zähler werden für zusammengeführte ACLs nicht unterstützt. Mit der Cisco IOS Softwareversion 12.0(21)S3 und höher kann die Zusammenführung von Zugriffskontrolllisten mithilfe des Befehls `hw-module <Steckplatz #> tcam compile no-merge` deaktiviert werden. Um zu bestimmen, ob eine ACL zusammengeführt wird, verwenden Sie den Befehl **show-access-list Hardware interface**.
- Wenn NetFlow auf einer Line Card der Engine 0/1 konfiguriert und eine Ausgabe-ACL auf einer Line Card der Ausgangs-Engine 3 oder 4+ konfiguriert ist, wird die Ausgabe-ACL sowohl von den Eingangs- als auch von den Ausgangs-Linecards verarbeitet, damit NetFlow Pakete berücksichtigen kann, die von ACLs abgelehnt wurden, sowie weitergeleitete Pakete.

## Unterstützung für ACL-Zähler

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

### Definitionen:

- Per-ACE (Pro ACE) - Normale Unterstützung für Cisco IOS-Software: Der **Befehl show access-list <number>** im RP/LC zeigt die ACL und den Zähler für jeden ACE an. Sie ist nur verfügbar, wenn die **Zusammenführung** deaktiviert ist, bevor Sie ACLs konfigurieren.

Verwenden Sie dazu den folgenden Konfigurationsbefehl:

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

Wenn diese Option aktiviert ist, werden einige TCAM-Mergeoptimierungen deaktiviert und die Skalierbarkeit wird beeinträchtigt. Die genaue Wirkung hängt von den einzelnen Zugriffskontrolllisten ab. Beachten Sie außerdem, dass die Zähler nicht korrekt sind, wenn richtlinienbasiertes Routing auf diese Schnittstelle angewendet wird. In diesem Fall sollte der aggregierte Zähler verwendet werden.

- Per-ACE (TCAM) - Hardwareindikatoren für jeden TCAM-Eintrag. Es ist keine Konfiguration erforderlich, und die Leistung/Skalierbarkeit wird nicht beeinträchtigt. Nur über diese CLI auf der Linecard verfügbar. Diese Zähler können nicht per Software gelöscht werden.

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

In Cisco IOS Software Release 22S ist eine neue generische CLI für diesen Befehl verfügbar:

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

Wie beim Per-ACE-Zähler sind die TCAM-Zähler nur gültig, wenn an dieser Schnittstelle mit der ACL kein PBR verwendet wird.

- Aggregate (Aggregat): Jede ACL zeigt einen zusammengefassten Zulassen-/Ablehnungszähler an. Dies ist die Summe aller einzelnen ACE-Zähler. Es ist keine Konfiguration erforderlich, und die Leistung und Skalierbarkeit werden nicht beeinträchtigt.

## Empfehlungen

Derzeit keine.

## Engine 4 (POS) - ACL-Verarbeitung

### Übersicht

Engine 4 bietet diese ACL-Unterstützung für die Cisco IOS Software Version 12.0(18)S und höher:

- Ausgabe-ACLs werden auf E0/1/2-Linecards unterstützt, wenn eine Engine 4-Linecard die Eingangskarte ist. In dieser Konfiguration wird die Ausgabe-ACL von der Ausgangs-Linecard-CPU verarbeitet.

Diese Linecards basieren auf Engine 4:

Line Card-Typ	Schnittstellentyp	Motortyp	Konnektivität
4 x OC48c/STM 16c	POS	E	
4 x OC48c/STM 16c	POS	E	LR
1 x OC192c/ST M64c	POS	E	IR
1 x OC192c/ST M64c	POS	E	SR
1 x OC192c/ST M64c	POS	E	VSR-1
10 x GE	SFP	E	

## [Engine 4+ \(POS und DPT\) - ACL-Verarbeitung](#)

### [Übersicht](#)

Mit Engine 4+ wird das 10-Gigabit-Portfolio der Cisco Serie 12000 um ACL-Funktionen erweitert.

Bis zu 1.024 ACEs werden in jedem Eingangs- und Ausgangs-Pfade unterstützt. Sowohl Eingabe- als auch Ausgabe-ACLs werden mit Leitungsgeschwindigkeit für bis zu 96 ACEs verarbeitet. Die Leistung für längere Übereinstimmungen variiert je nach Spieltiefe.

Diese POS-Linecards basieren auf Engine 4+:

Line Card-Typ	Schnittstellentyp	Konnektivität
4 x OC48c/STM16c	POS	SR
4 x OC48c/STM16c	POS	LR
1 x OC192c/STM64c	POS	IR
1 x OC192c/STM64c	POS	SR
1 x OC192c/STM64c	POS	VSR-1
1 x OC192/STM64c	POS	LR
4 x OC48c/STM16c	DPT	SFP:
1 x OC192c/STM64c	DPT	IR

1 x OC192c/STM64c	DPT	SR
1 x OC192c/STM64c	DPT	VSR-1
1 x OC192c/STM64c	DPT	LR

### [Unterstützte Anpassungskriterien](#)

Alle von der Cisco IOS Software Version 12.0S unterstützten Standard- und Extended ACL-Kriterien werden im schnellen Pfad unterstützt, mit Ausnahme von Protokoll- oder Fragment-ACEs.

### [Anzahl unterstützter ACEs](#)

Bis zu 1024 ACEs werden pro Richtung im schnellen Pfad unterstützt.

**Hinweis:** 1021 der ACEs können konfiguriert werden. Drei Einträge sind für die ACEs reserviert, die implizit **permit ip any**, **deny ip any any any any** und **send an CPU**-Befehle ermöglichen.

Es gibt keine Obergrenze für die Anzahl der unterstützten ACEs. Alle ACEs, die den Grenzwert von 1021 überschreiten, werden im langsamen Pfad der Linecard ausgeführt.

### [Ausgabe-ACL-Verarbeitung](#)

Die Ausgabe-ACLs werden im übertragbaren schnellen Pfad verarbeitet. Weitere Informationen finden Sie unter [IPv4-Ausgabe-ACL - Line Card Interoperation Matrix \(Schnittstellenmatrix für Line Cards\)](#).

### [Line Card-spezifische Befehle](#)

- `show tcam appl [acl-in | acl-out] tcam <label-no>`
- `show tcam appl [acl-in | acl-out] memory <port> <Anzahl der Einträge>`

### [Betriebsrichtlinien und Line Card-Interaktionen](#)

- ACLs mit Subschnittstelle werden nicht unterstützt.
- Die Leistung hängt von der Tiefe der Übereinstimmung ab.
- Bereichseinträge verwenden zwei ACL-Regeln (drei, wenn die beiden Einträge eine Grenze überschreiten).
- Pro physischer Schnittstelle wird eine ACL unterstützt.
- Bis zu 1024 ACEs (pro Richtung) werden im schnellen Pfad unterstützt.
- Jeder der 1024 Fast-Path-ACEs kann für alle Ports freigegeben werden.
- ACEs, die das Fragment-Schlüsselwort verwenden, werden im langsamen Pfad gefiltert.
- Abgelehnte Pakete werden nicht für ACEs gezählt, die im langsamen Pfad verarbeitet werden.
- Wenn NetFlow auf einer Line Card der Engine 0 konfiguriert ist und eine Ausgabe-ACL auf einer Line Card der Ausgangs-Engine 3 oder 4+ konfiguriert ist, wird die Ausgabe-ACL sowohl

von den Eingangs- als auch von den Ausgangs-Linecards verarbeitet, damit NetFlow Pakete, die von ACLs abgelehnt wurden, sowie weitergeleitete Pakete berücksichtigen kann.

## Empfehlungen

Derzeit keine.

## Engine 4+ (Ethernet) - ACL-Verarbeitung

### Übersicht

Die Line Cards der Engine 4+ für Ethernet-Schnittstellen bieten eine VLAN-Eingangs-ACL-Funktionalität in der Hardware für das 10-Gigabit-Ethernet-Portfolio der Cisco Serie 12000. Einige der Merkmale:

- Eingangs- und Ausgangszugriffskontrolllisten können gleichzeitig auf einen einzelnen Port ohne Leistungseinbußen angewendet werden.
- ACLs können pro VLAN oder Port angewendet werden.
- Die ACL-Eingangsleistung von bis zu 15.000 ACEs lässt sich nicht mit der Spieltiefe herabstufen.
- Ausgangszugriffskontrolllisten werden mit Leitungsgeschwindigkeit für bis zu 96 ACEs verarbeitet. Die Leistung für längere Übereinstimmungen variiert je nach Spieltiefe.

Diese Ethernet Line Cards basieren auf Engine 4+:

Line Card-Typ	Schnittstellentyp	Motorotyp
10 x GE Rev B ("X-B")	SFP:	E4+
Modular	SFP:	E4+
1 x 10 GE	10 G	E4+
1 x 10 GE	10 G	E4+

### Unterstützte Anpassungskriterien

Alle von der Cisco IOS Software Version 12.0S unterstützten Standard- und Extended ACL-Kriterien werden im schnellen Pfad unterstützt, mit Ausnahme von Protokoll- oder Fragment-ACEs.

### Anzahl unterstützter ACEs

- Bis zu 15.000 Eingangs-ACLs, die pro Port oder VLAN konfiguriert werden können.
- 1024 Ausgabe-ACEs pro Karte, die pro Port angewendet werden können. **Hinweis:** 1021 der ACEs können konfiguriert werden. Drei Einträge sind für die ACEs reserviert, die implizit **permit ip any, deny ip any any any any** und **send an CPU**-Befehle ermöglichen.

### Ausgabe-ACL-Verarbeitung

Die Ausgabe-ACLs werden nativ im übertragbaren schnellen Pfad verarbeitet. Weitere

Informationen finden Sie unter [IPv4-Ausgabe-ACL - Line Card Interoperation Matrix \(Schnittstellenmatrix für Line Cards\)](#).

## Line Card-spezifische Befehle

- **hw-module slot <number> ip acl merge**

## Betriebsrichtlinien und Line Card-Interaktionen

- ACEs, die das Fragment-Schlüsselwort enthalten, werden im langsamen Pfad verarbeitet.
- ACL-Zähler werden für ACLs in Verbindung mit anderen Funktionen nicht unterstützt.
- ACL-Zähler werden für zusammengeführte ACLs nicht unterstützt. Zusammengeführte ACLs können mit dem Befehl **hw-module slot <steckplatznummer> ip acl merge** konfiguriert werden.
- Pro Linecard werden bis zu 168 L4-Vorgänge unterstützt. Wenn diese Grenze überschritten wird, wird die ACL im langsamen Pfad ausgeführt.
- Wenn eine Line Card der Engine 1 eine Sampling-NetFlow-Funktion aktiviert hat und eine Ausgabe-ACL auf einer Line Card der Ausgangs-Engine 3 oder 4+ aktiviert ist, wird die Ausgabe-ACL sowohl von den Eingangs- als auch von den Ausgangs-Linecards verarbeitet, damit NetFlow Pakete berücksichtigen kann, die von ACLs abgelehnt wurden, sowie weitergeleitete Pakete.

## Empfehlungen

Derzeit keine.

## ACL-Protokollierung

Vor der Cisco IOS Software-Version 12.0(21)S wurden Informationen zur ACL-Protokollierung ausschließlich über den Maintenance Bus (MBUS) an den RP gesendet. Bei einer hohen Anzahl von ACL-Protokollaktivitäten war es möglich, die Kapazität des MBUS zu überschreiten. Cisco IOS Software Release 12.0(21)S bietet eine Reihe von Optimierungen, die dieses Szenario verhindern.

MBUS-Überlastungssituationen werden von der Cisco IOS-Software mit folgenden Fehlermeldungen gemeldet:

```
LCLOG-3-INVSTATE
```

```
MBUS_SYS-3-SEQUENCE
```

Ab Cisco IOS Software Release 12.0(21)S werden über den MBUS Protokollmeldungen mit hohem Schweregrad (Schweregrad 0-4) an den RP gesendet, während Protokollmeldungen mit niedrigerem Schweregrad (Schweregrad 5-7) über die Switching Fabric mit höherer Kapazität an den RP übermittelt werden. ACL-Protokollmeldungen weisen einen hohen Schweregrad auf und werden somit über die Switching Fabric an den RP übermittelt.

Diese zusätzliche Protokollierungsfunktion kann mithilfe der folgenden Befehle konfiguriert werden:

- **logging method mbus [Severity]:** Bestimmt, welche Meldungen nach Schweregrad mithilfe des MBUS an den RP gesendet werden. Über die Switch-Fabric werden schwerwiegendere Meldungen gesendet.
- **show logging method:** Zeigt die aktuelle Protokollierungsmethode für alle Schweregrade von Nachrichten an.
- **logging sequenz-nums:** Mit diesem Befehl kann die sendende Linecard Protokollmeldungen mit Sequenznummern-Protokollnachrichten abfolgen, sodass Meldungen vom RP ordnungsgemäß neu bestellt werden können. Ohne diesen Befehl können Protokollmeldungen in nicht sequenzieller Reihenfolge an den RP gesendet werden.

## IPv4-Ausgabe-ACL - Line Card-Interoperation-Matrix

Vor der Einführung der ACL-Ausgangsverarbeitung mit der Einführung von Engine 3 und Engine 4+ wurden ausgehende ACLs mit der Eingangs-Linecard verarbeitet. Die Ausgabe-ACLs wurden aktualisiert, um die leistungsstarken Verarbeitungsfunktionen für ACLs der Engine 3 und Engine 4+ zu nutzen.

Dieses Diagramm bietet eine Übersicht darüber, wo ausgehende ACLs für verschiedene Linecard-Kombinationen verarbeitet werden:

	Ausgangs-Linecard					
Eingangs-Linecard (Ausgabe-ACL auf Mitgliedsoberfläche angewendet)	E0	E1	E2	E3	E	E4+
E0	Eingang	Eingang	Eingang	Ausgehend	K/A	Ausgehend
E1	Eingang	Eingang	Eingang	Ausgehend	K/A	Ausgehend
E2	Eingang	Eingang	Eingang	Ausgehend	K/A	Ausgehend
E3	Ausgehend	Ausgehend	Ausgehend	Ausgehend	K/A	Ausgehend
E	Ausgehend	Ausgehend	Ausgehend	Ausgehend	K/A	Ausgehend
E4+	Ausgehend	Ausgehend	Ausgehend	Ausgehend	K/A	Ausgehend

## IPv6 ACL-Unterstützung

Erweiterte IPv6-ACLs werden in E0, E1, E2, E3 und E4+ im langsamen Pfad (Eingang und Ausgang) in Cisco IOS Software Release 12.0(23)S unterstützt.

In Engine 3 wird die IPv6-ACL-Funktionalität in der Hardware der Cisco IOS Software, Version 12.0(25)S, unterstützt. ACLs werden auf eine bestimmte Schnittstelle angewendet, mit einer impliziten deny-Anweisung am Ende jeder Zugriffsliste. IPv6-ACLs werden mithilfe des Befehls `ipv6 access-list` mit dem Befehl `deny and permit keywords` im globalen Konfigurationsmodus konfiguriert. Engine 3-basierte Karten unterstützen das Filtern von datenverkehrs-basierten IPv6-Optionsheadern, Flow-Labels und optional Informationen zum Protokolltyp der oberen Ebene.

## Cisco 12000 ACL-Befehlsreferenz

### Befehle in Engine 1

- Zugriffslisten-Hardwaresalsa
- Show Controller I3 | ASIC einschließen

### Befehle in Engine 2

- Zugriffsliste Hardware-PSA-Limit 128
- kein Zugriffslisten-Hardware-PSA
- PSA-Umgehung
- `show access-list psa detail`
- `show access-list psa summary`
- Show Controller PSA-Funktion

### Befehle in Engine 3

- `hw-module <Steckplatz #> tcam kompilieren ohne Merge!— ab Cisco IOS Softwareversion 12.0(21)S3`
- Hardware-Schnittstelle der `show-access-list <Schnittstellename>`
- `show contr [tofab/fab] alpha acl <int> vmr2ace`

### Befehle mit Engine 4+

- `show access-list gen7 label`
- `show tcam appl [acl-in | acl-out] tcam <label-no>`
- `show tcam appl [acl-in | acl-out] Arbeitsspeicher <Port><Anzahl der Einträge>`

### Ethernet-Befehle der Engine 4+

- `hw-module slot <number> ip acl merge`

## Glossar

Dieser Abschnitt enthält Standarddefinitionen relevanter Begriffe:

- **Verarbeitungsebenen** - Ein Netzwerkgerät kann logisch in drei Verarbeitungsebenen unterteilt werden: Datenebene - Verarbeitung der Pakete, die über das Netzwerkgerät übertragen

werden. Kontrollebene - Verarbeitung der Pakete, die zum Verbinden von Netzwerkgeräten verwendet werden. Dazu gehören Leitungsprotokolle (wie Point-to-Point Protocol - PPP und High-Level Data Link Control - HDLC), Routing-Protokolle (Border Gateway Protocol - BGP, Routing Information Protocol Version 2 - RIPv2, Open Shortest Path First - OSPF usw.) sowie Timing-Protokolle (wie Network Time Protocol - NTP).

Management Plane (Verwaltungsebene): Verarbeitung von Paketen, die zur Verwaltung der Netzwerkgeräte verwendet werden. Dazu gehören Telnet, Secure Shell (SSH), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), SNMP und andere Verwaltungsprotokolle.

- **Standard-ACLs:** Standard-ACLs filtern ausschließlich auf Layer 3.
- **Erweiterte ACLs** - erweiterte IP-Zugriffslisten verwenden Quell- und Zieladressen für übereinstimmende Vorgänge sowie optionale Protokolltypinformationen für eine feinstufige Kontrolle.
- **Lineare verarbeitete ACLs** - In Software linear verarbeitet. Die Leistung variiert je nach der Tiefe der Übereinstimmung (die Anzahl der Einträge, die überprüft werden müssen, bevor eine Übereinstimmung ermittelt wird).
- **Turbo ACLs (kompiliert)** - Turbo ACLs optimieren die Verarbeitung von Software-ACLs, indem eine ACL in eine hochoptimierte Serie von Suchtabellen kompiliert wird, die die Softwareverarbeitung beschleunigt. Die Leistung von Turbo ACLs variiert nicht je nach Spieltiefe.
- **Eingabe-ACLs** - Eine ACL, die auf Datenverkehr angewendet wird, der in den Port gelangt, auf den sie angewendet wird.
- **Output ACLs (Ausgabe-ACLs):** Eine ACL, die auf Datenverkehr angewendet wird, der den Port verlässt, auf den sie angewendet wird. Mit einigen Ausnahmen werden ausgehende ACLs von der Eingangs-Linecard verarbeitet.
- **Receive Path ACLs** - Receive Path ACLs ermöglichen das Filtern des für den Router selbst bestimmten Kontrolldatenverkehrs, z. B. Routing-Updates und SNMP-Abfragen.
- **Dual-Stage Forwarding Line Card** - Linecards mit Weiterleitungs-/Funktionsgruppen-ASICs für Eingangs- und Ausgangs-Pfade Auf diese Weise kann die Linecard Funktionen sowohl für den eingehenden Paketfluss als auch den ausgehenden Paketfluss ausführen, ohne Pakete an die LC-CPU zu senden. Darüber hinaus können neue Wellen von Dual-Stage-Weiterleitungsalgorithmen in der Cisco Serie 12000 verwendet werden. Die Line Card Engine 3 ist ein Beispiel für eine Dual-Stage Forwarding Line Card.
- **Single-Stage Forwarding Line Card** - Linecards mit Weiterleitungs-/Funktionsgruppen-ASICs nur im Eingangspfad Diese Linecards führen nur eine ASIC-basierte Verarbeitung für die Pakete durch, die über den Eingangspfad fließen. Der Ausgangsverkehr wird entweder nicht verarbeitet (nur weitergeleitet), von den Eingangs-ASICs anderer LCs verarbeitet oder von der LC-CPU verwaltet. Die Module Engine 2, Engine 4 und Engine 4+ sind Beispiele für Single-Stage Forwarding Line Cards.

## Zugehörige Informationen

- [Cisco Internet Router der Serie 1200](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)