Vermeidung der Überlastung von ACLs und QoS-TCAM bei Catalyst Switches der Serie 4500

Inhalt

Einführung

Die Cisco Catalyst Switches der Serien 4500 und 4948 unterstützen die Zugriffskontrollliste (ACL) mit Leitungsgeschwindigkeit und die QoS-Funktion unter Verwendung des Tternary Content Addressable Memory (TCAM). Durch die Aktivierung von ACLs und Richtlinien wird die Switching- oder Routing-Leistung des Switches nicht beeinträchtigt, solange die ACLs vollständig im TCAM geladen sind. Wenn der TCAM erschöpft ist, können die Pakete über den CPU-Pfad weitergeleitet werden, was die Leistung für diese Pakete beeinträchtigen kann. Dieses Dokument enthält Details zu:

- Die verschiedenen TCAM-Typen, die von Catalyst 4500 und Catalyst 4948 verwendet werden
- Wie der Catalyst 4500 die TCAMs programmiert
- So konfigurieren Sie die ACLs und den TCAM auf dem Switch optimal, um eine Erschöpfung des TCAM zu vermeiden

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst Switches der Serie 4500
- Catalyst Switches der Serie 4948

Hinweis: Dieses Dokument gilt nur für Cisco IOS® Software-basierte Switches und nicht für Catalyst OS-basierte Switches (CatOS).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

Hintergrundinformationen

Um die verschiedenen Typen von ACLs und QoS-Richtlinien in der Hardware zu implementieren, werden die Hardware-Suchtabellen (TCAM) der Catalyst 4500-Programme und verschiedene Hardwareregister in der Supervisor Engine eingesetzt. Wenn ein Paket eingeht, führt der Switch eine Suche nach der Hardwaretabelle (TCAM Lookup) durch und beschließt, das Paket entweder zuzulassen oder abzulehnen.

Der Catalyst 4500 unterstützt verschiedene Arten von Zugriffskontrolllisten. In Tabelle 1 sind diese Zugriffskontrolllisten aufgeführt.

Tabelle 1: Typen von ACLs, die von Catalyst Switches der Serie 4500 unterstützt werden

ACL-Typ	Anwenden	Kontrollierter Datenverkehr	Richtung
RACL[1]	L3[2]-Port, L3-Kanal oder SVI[3] (VLAN)	Gerouteter IP-Datenverkehr	Eingehend oder ausgehend
VACL[4]	VLAN (über den Befehl **vlan filter**)	Alle Pakete, die in ein oder aus einem VLAN geroutet oder innerhalb eines VLAN überbrückt werden	richtungslos
PACL[5]	L2[6]-Port oder L2-Kanal	Gesamter IP-Datenverkehr und Nicht-IPv4[7]-Datenverkehr (über MAC-ACL)	Eingehend oder ausgehend

[1] RACL = Router-ACL

[2] L3 = Layer 3

[3] SVI = Switch Virtual Interface

[4] VACL = VLAN ACL

[5] PACL = Port-ACL

[6] L2 = Layer 2

[7] IPv4 = IP-Version 4

Catalyst 4500 ACL- und QoS-Hardwareprogrammierarchitektur

Der Catalyst 4500 TCAM hat folgende Anzahl von Einträgen:

- 32.000 Einträge für die Sicherheits-ACL, die auch als Feature-ACL bezeichnet wird
- 32.000 Einträge für QoS ACL

Sowohl für die Sicherheits-ACL als auch für die QoS-ACL sind die Einträge wie folgt dediziert:

- 16.000 Einträge für die Eingangsrichtung
- 16.000 Einträge für die Ausgangsrichtung

Abbildung 3 zeigt die Widmung des TCAM-Eintrags. Weitere Informationen zu TCAMs finden Sie im Abschnitt TCAM-Typen.

Tabelle 2 zeigt die verfügbaren ACL-Ressourcen für verschiedene Catalyst 4500 Supervisor Engines und Switches.

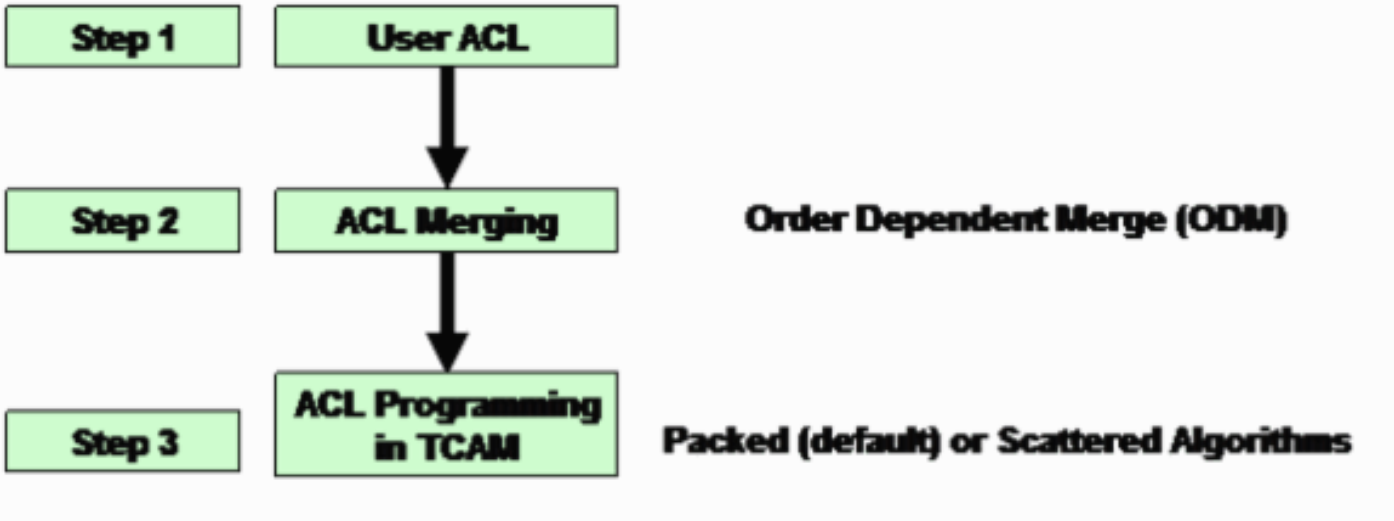
Tabelle 2: Catalyst 4500 ACL-Ressourcen für verschiedene Supervisor Engines und Switches

Produkt	TCAM-Version	Funktion TCAM (pro Richtung)	QoS-TCAM (pro Richtung)
Supervisor Engine II+	2	8000 Einträge, 1000 Masken	8000 Einträge, 1000 Masken
Supervisor Engine II+TS/III/IV/V und WS-C4948	2	16.000 Einträge, 2.000 Masken	16.000 Einträge, 2.000 Masken
Supervisor Engine V-10GE und WS-C4948-10GE	1	16.000 Einträge, 16.000 Masken	16.000 Einträge, 16.000 Masken

Der Catalyst 4500 verwendet separate, dedizierte TCAMs für IP-Unicast- und Multicast-Routing. Der Catalyst 4500 kann bis zu 128.000 Routingeinträge enthalten, die die Unicast- und Multicast-Routen gemeinsam nutzen. Diese Details fallen jedoch nicht in den Anwendungsbereich dieses Dokuments. In diesem Dokument werden nur Sicherheits- und QoS-TCAM-Erschöpfungsprobleme behandelt.

Abbildung 1 zeigt die Schritte zur Programmierung der ACLs in den Hardwaretabellen des Catalyst 4500.

Abbildung 1: Schritte zum Programmieren von ACLs auf Catalyst Switches der Serie 4500



Schritt 1

Dieser Schritt umfasst eine der folgenden Aktionen:

- Konfiguration und Anwendung einer ACL- oder QoS-Richtlinie auf eine Schnittstelle oder ein VLANDie Erstellung von Zugriffskontrolllisten kann dynamisch erfolgen. Ein Beispiel hierfür ist die IP Source Guard (IPSG)-Funktion. Mit dieser Funktion erstellt der Switch automatisch eine PACL für IP-Adressen, die dem Port zugeordnet sind.
- Änderung einer bereits vorhandenen ACL

Hinweis: Die Konfiguration einer ACL allein führt nicht zur TCAM-Programmierung. Die ACL (QoS-Richtlinie) muss auf eine Schnittstelle angewendet werden, um die ACL im TCAM zu programmieren.

Schritt 2

Die ACL muss zusammengeführt werden, bevor sie in den Hardware-Tabellen (TCAM) programmiert werden kann. Die Zusammenführung programmiert mehrere ACLs (PACL, VACL oder RACL) in der Hardware in kombinierter Form. Auf diese Weise ist nur eine einzige Hardware-Suche erforderlich, um alle zutreffenden ACLs im logischen Paketweiterleitungspfad abzugleichen.

Beispiel: In Abbildung 2 kann ein Paket, das von PC-A an PC-C weitergeleitet wird, folgende ACLs aufweisen:

- Eine Eingabe-PACL am PC-A-Port
- Ein VACL in VLAN 1
- Ein Eingangs-RACL auf der VLAN 1-Schnittstelle in Eingangsrichtung

Diese drei ACLs werden zusammengeführt, sodass eine einzige Suche in der Eingabe-TCAM ausreicht, um die Weiterleitungsentscheidung zu treffen, um zu erlauben oder abzulehnen. Ebenso ist nur eine einzelne Ausgabeabfrage erforderlich, da der TCAM mit dem zusammengeführten Ergebnis dieser drei ACLs programmiert ist:

- Die Ausgabe-RACL auf der VLAN 2-Schnittstelle
- VLAN 2 VACL
- Die Ausgabe-PACL am PC-C-Port

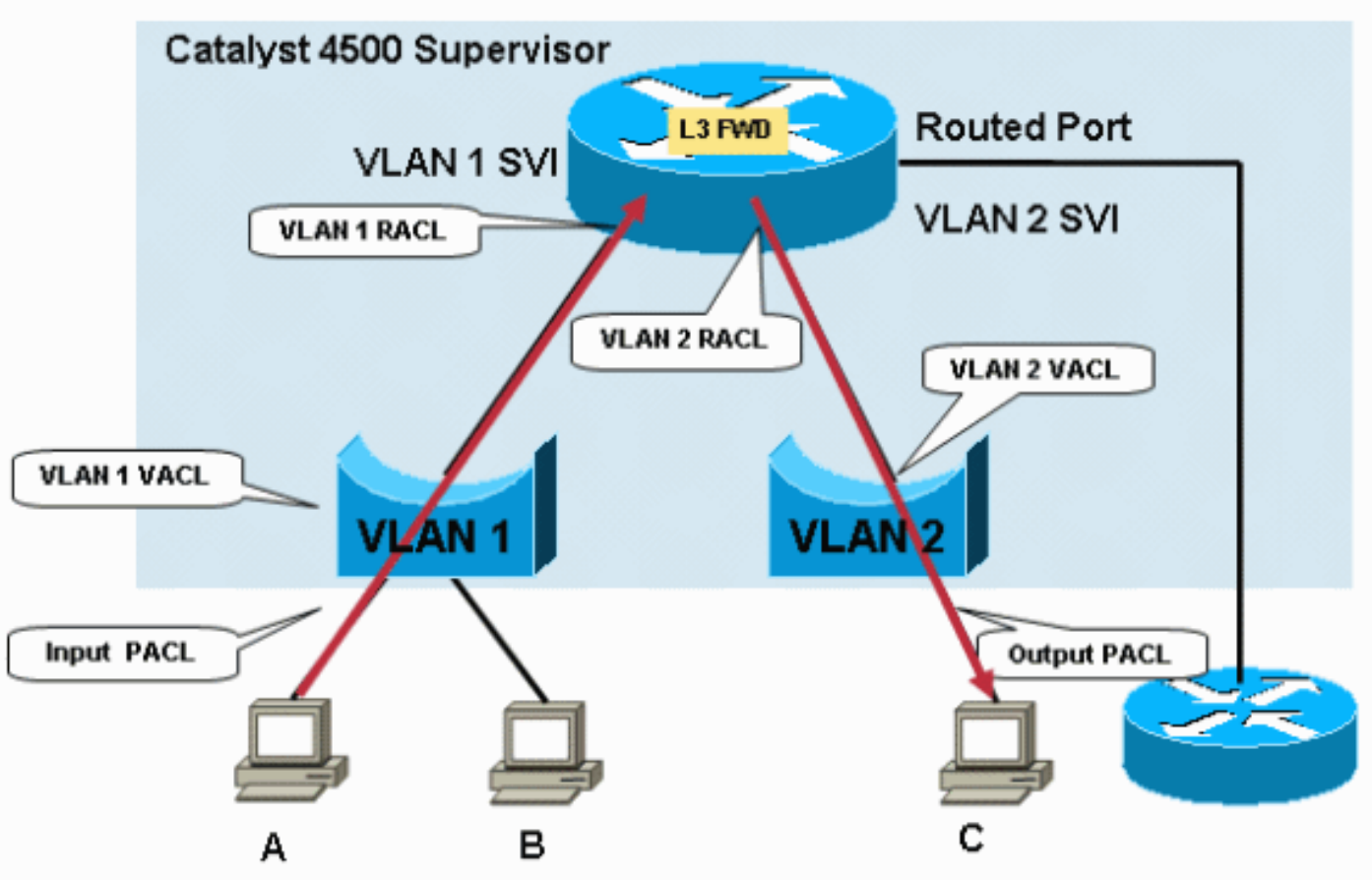
Bei einer einzigen Suche nach Eingabe und einer für Ausgabe gibt es keine Hardware-Strafweiterleitung der Pakete, wenn sich eine oder alle dieser ACLs im Paketweiterleitungspfad befinden.

Hinweis: Die Eingabe- und Ausgabe-TCAM-Suchvorgänge finden gleichzeitig in der Hardware statt. Ein häufiges Missverständnis besteht darin, dass die Ausgabe-TCAM-Suche nach der Eingabe-TCAM-Suche erfolgt, wie der logische Paketfluss nahe legt. Diese Informationen sind wichtig zu verstehen, da die Ausgaberichtlinie des Catalyst 4500 nicht mit den geänderten QoS-Parametern der Eingaberichtlinie übereinstimmen kann. Im Fall von Sicherheitszugriffskontrolllisten wird die schwerwiegendste Aktion ausgeführt. Das Paket wird in einer der folgenden Situationen verworfen:

- Wenn das Ergebnis der Eingangsabfrage verworfen wird und die Ausgabe-Suche zulässig ist
- Wenn das Suchergebnis für die Eingabe zulässig ist und das Ergebnis für die Ausgabe verworfen wird

Hinweis: Das Paket ist zulässig, wenn sowohl die Eingabe- als auch die Ausgabe-Suchergebnisse zulässig sind.

Abbildung 2: Filterung über Security ACLs auf Catalyst Switches der Serie 4500



Die ACL-Zusammenführung beim Catalyst 4500 ist auftragsabhängig. Der Prozess wird auch als Order Dependent Merge (ODM) bezeichnet. Beim ODM werden ACL-Einträge in der Reihenfolge programmiert, in der sie in der ACL erscheinen. Wenn beispielsweise eine ACL zwei Zugriffskontrolleinträge (ACEs) enthält, programmiert der Switch zuerst ACE 1 und dann ACE 2. Die Bestellabhängigkeit besteht jedoch nur zwischen den ACEs innerhalb einer bestimmten ACL. Beispielsweise können ACEs in ACL 120 vor ACEs in ACL 100 im TCAM beginnen.

Schritt 3

Die zusammengeführte ACL ist im TCAM programmiert. Der Eingangs- oder Output-TCAM für die ACL oder QoS wird weiter in zwei Bereiche unterteilt: PortAndVlan und PortOrVlan. Die zusammengeführte ACL wird im PortAndVlan-Bereich des TCAM programmiert, wenn sich *beide* ACLs im gleichen Paketpfad befinden:

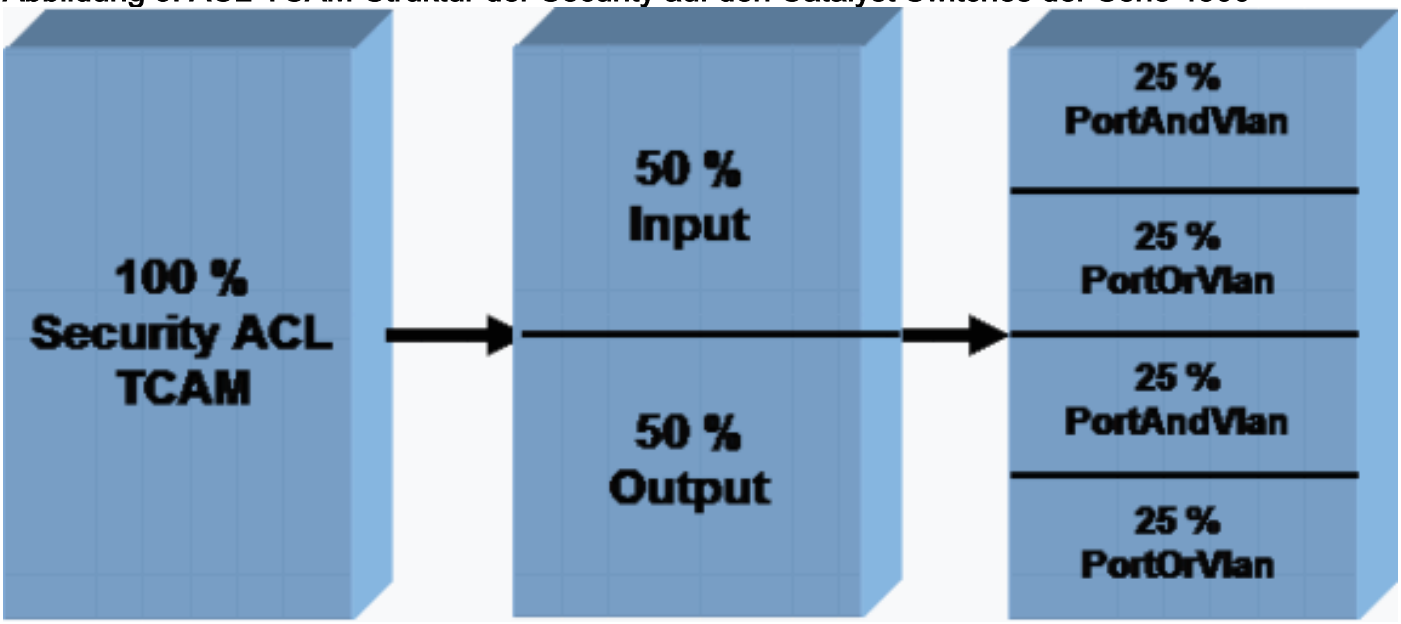
- EIN PACL**Hinweis:** Bei der PACL handelt es sich um eine normale Filterzugriffskontrollliste (ACL) bzw. eine vom IPSG erstellte dynamische Zugriffskontrollliste (Dynamic ACL).
- VACL oder RACL

Eine ACL wird in der PortOrVlan-Region des TCAM programmiert, wenn ein bestimmter Pfad des Pakets nur eine PACL, eine VACL oder eine RACL aufweist. Abbildung 3 zeigt die ACL-TCAM-Carving für die Sicherheit verschiedener Typen von ACLs. QoS verfügt über einen ähnlich geschnitzten, separaten, dedizierten TCAM.

Derzeit können Sie die TCAM-Standardzuweisung nicht ändern. Es gibt jedoch Pläne, die Möglichkeit bereitzustellen, die für die PortAndVLAN- und PortOrVLAN-Regionen verfügbare TCAM-Zuweisung in zukünftigen Softwareversionen zu ändern. Mit dieser Änderung können Sie den Speicherplatz für PortAndVlan und PortOrVlan in den Ein- oder Ausgabe-TCAMs erhöhen oder verringern.

Hinweis: Jede Erhöhung der Zuweisung für die PortAndVlan-Region führt zu einer entsprechenden Verringerung der PortOrVlan-Region im Eingangs- oder Ausgabegeschäft.

Abbildung 3: ACL-TCAM-Struktur der Security auf den Catalyst Switches der Serie 4500



Der Befehl **show plattform hardware ACL statistics Usage brief** zeigt die TCAM-Nutzung pro Region für ACL- und QoS-TCAMs an. Die Befehlsausgabe zeigt die verfügbaren Masken und Einträge und teilt sie nach Regionen auf, wie in Abbildung 3 dargestellt. Diese Beispielausgabe stammt von einer Catalyst 4500 Supervisor Engine II+:

Hinweis: Weitere Informationen zu Masken und Einträgen finden Sie im Abschnitt TCAM-Typen dieses Dokuments.

```
Switch#show platform hardware acl statistics utilization brief
```

```
                                  Entries/Total(%)   Masks/Total(%)
                                 -----------------  ---------------
Input   Acl(PortAndVlan)   2016 / 4096 ( 49)    252 /  512 ( 49)
Input   Acl(PortOrVlan)       6 / 4096 (  0)      5 /  512 (  0)
Input   Qos(PortAndVlan)      0 / 4096 (  0)      0 /  512 (  0)
Input   Qos(PortOrVlan)       0 / 4096 (  0)      0 /  512 (  0)
Output  Acl(PortAndVlan)      0 / 4096 (  0)      0 /  512 (  0)
Output  Acl(PortOrVlan)       0 / 4096 (  0)      0 /  512 (  0)
Output  Qos(PortAndVlan)      0 / 4096 (  0)      0 /  512 (  0)
Output  Qos(PortOrVlan)       0 / 4096 (  0)      0 /  512 (  0)
L4Ops: used 2 out of 64
```

TCAM-Typen

Der Catalyst 4500 verwendet zwei TCAM-Typen, wie Tabelle 2 zeigt. In diesem Abschnitt wird der Unterschied zwischen den beiden TCAM-Versionen dargestellt, sodass Sie das passende Produkt für Ihr Netzwerk und Ihre Konfiguration auswählen können.

TCAM 2 verwendet eine Struktur, in der acht Einträge eine Maske teilen. Ein Beispiel sind acht IP-Adressen in ACEs. Die Einträge müssen die gleiche Maske wie die Maske haben, die sie gemeinsam verwenden. Wenn die ACEs unterschiedliche Masken haben, müssen die Einträge bei Bedarf separate Masken verwenden. Die Verwendung separater Masken kann zu einer Erschöpfung der Masken führen. Die Maskenerschöpfung im TCAM ist einer der häufigsten Gründe für die Erschöpfung des TCAM.

TCAM 3 unterliegt keiner solchen Einschränkung. Jeder Eintrag kann eine eigene eindeutige Maske im TCAM haben. Die vollständige Nutzung aller in der Hardware verfügbaren Einträge ist unabhängig von der Maske dieser Einträge möglich.

Um diese Hardwarearchitektur zu demonstrieren, zeigt das Beispiel in diesem Abschnitt, wie eine TCAM 2- und eine TCAM 3-Programm-ACLs in der Hardware ausgeführt werden.

```
access-list 101 permit ip host 8.1.1.1 any
access-list 101 deny ip 8.1.1.0 0.0.0.255 any
```

Diese Beispiel-ACL enthält zwei Einträge, die zwei verschiedene Masken aufweisen. ACE 1 ist ein Hosteintrag und hat daher eine /32-Maske. ACE 2 ist ein Subnetzeintrag mit einer /24-Maske. Da der zweite Eintrag eine andere Maske hat, können leere Einträge in Maske 1 nicht verwendet werden, und für TCAM 2 wird eine separate Maske verwendet.

Diese Tabelle zeigt, wie diese ACL in TCAM 2 programmiert ist:

Masken	Einträge
Maske 1 Übereinstimmung: alle 32 Bit der Quell-IP-Adresse "Keine Sorge": alle verbleibenden Bits	Quell-IP = 8.1.1.1
	Leerer Eintrag 2
	Leerer Eintrag 3
	Leerer

	Eintrag 4
	Leerer Eintrag 5
	Leerer Eintrag 6
	Leerer Eintrag 7
	Leerer Eintrag 8
Maske 2 Übereinstimmung: wichtigste 24 Bit der Quell-IP-Adresse "Keine Sorge": alle verbleibenden Bits	Quell-IP = 8.1.1.0
	Leerer Eintrag 2
	Leerer Eintrag 3
	Leerer Eintrag 4
	Leerer Eintrag 5
	Leerer Eintrag 6
	Leerer Eintrag 7
	Leerer Eintrag 8

Obwohl es freie Einträge als Teil von Maske 1 gibt, verhindert die Struktur TCAM 2 die Population von ACE 2 im leeren Eintrag 2 für Maske 1. Die Verwendung dieser Maske ist nicht zulässig, da die Maske von ACE 2 nicht mit der /32-Maske von ACE 1 übereinstimmt. TCAM 2 muss den ACE 2 mithilfe einer separaten Maske, einer /24-Maske, programmieren.

Die Verwendung einer separaten Maske kann zu einer schnelleren Erschöpfung der verfügbaren Ressourcen führen, wie Tabelle 2 zeigt. Andere ACLs können weiterhin die verbleibenden Einträge in Maske 1 verwenden. In den meisten Fällen ist die Effizienz von TCAM 2 jedoch hoch, beträgt jedoch nicht 100 Prozent. Die Effizienz variiert je nach Konfigurationsszenario.

In dieser Tabelle ist die gleiche, in TCAM 3 programmierte ACL aufgeführt. TCAM 3 weist jedem

Eintrag eine Maske zu:

Masken	Einträge
Maske 32 Bit für IP-Adresse 1	Quell-IP = 8.1.1.1
Maske: 24 Bit für IP-Adresse 2	Quell-IP = 8.1.1.0
Leere Maske 3	Leerer Eintrag 3
Leere Maske 4	Leerer Eintrag 4
Leere Maske 5	Leerer Eintrag 5
Leere Maske 6	Leerer Eintrag 6
Leere Maske 7	Leerer Eintrag 7
Leere Maske 8	Leerer Eintrag 8
Leere Maske 9	Leerer Eintrag 9
Leere Maske 10	Leerer Eintrag 10
Leere Maske 11	Leerer Eintrag 11
Leere Maske 12	Leerer Eintrag 12
Leere Maske 13	Leerer Eintrag 13
Leere Maske 14	Leerer Eintrag 14
Leere Maske 15	Leerer Eintrag 15
Leere Maske 16	Leerer Eintrag 16

In diesem Beispiel können die 14 verbleibenden Einträge jeweils ohne Einschränkungen Einträge mit verschiedenen Masken enthalten. Daher ist TCAM 3 viel effizienter als TCAM 2. Dieses Beispiel ist sehr vereinfacht, um die Unterschiede zwischen den TCAM-Versionen zu verdeutlichen. Die Catalyst 4500-Software verfügt über zahlreiche Optimierungen zur Steigerung der Effizienz der Programmierung in TCAM 2 für ein praktisches Konfigurationsszenario. Im Abschnitt Suboptimaler TCAM-Programmieralgorithmus für TCAM 2 dieses Dokuments werden diese Optimierungen behandelt.

Sowohl für TCAM 2 als auch für TCAM 3 auf dem Catalyst 4500 werden die TCAM-Einträge freigegeben, wenn dieselbe ACL auf verschiedene Schnittstellen angewendet wird. Durch diese Optimierung wird TCAM-Speicherplatz eingespart.

TCAM-Erschöpfung beheben

TCAM erschöpft sich bei der Programmierung einer Sicherheits-ACL auf den Catalyst 4500-Switches, erfolgt eine teilweise Anwendung der ACL über den Softwarepfad. Die Pakete, die den ACEs entsprechen, die im TCAM nicht angewendet werden, werden in der Software verarbeitet. Diese Verarbeitung in der Software verursacht eine hohe CPU-Auslastung. Da die Catalyst 4500 ACL-Programmierung auftragsabhängig ist, wird die ACL immer von oben nach unten programmiert. Wenn eine bestimmte Zugriffskontrollliste nicht vollständig in den TCAM passt, werden die ACEs am unteren Ende der Zugriffskontrollliste höchstwahrscheinlich nicht im TCAM programmiert.

Eine Warnmeldung wird angezeigt, wenn ein TCAM-Überlauf auftritt. Hier ein Beispiel:

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
```

```
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

Sie können diese Fehlermeldung auch in der Ausgabe des Befehls **show logging** sehen, wenn Sie Syslog aktiviert haben. Das Vorhandensein dieser Meldung weist eindeutig darauf hin, dass eine Softwareverarbeitung durchgeführt wird. Daher kann es zu einer hohen CPU-Auslastung kommen. Die bereits im TCAM programmierte ACL bleibt im TCAM programmiert, wenn während der Anwendung der neuen ACL die TCAM-Kapazität erschöpft ist. Die Pakete, die mit den bereits programmierten ACLs übereinstimmen, werden weiterhin in der Hardware verarbeitet und weitergeleitet.

Hinweis: Wenn Sie Änderungen an einer großen Zugriffskontrollliste vornehmen, wird möglicherweise die Meldung TCAM-exceeded (TCAM überschritten) angezeigt. Der Switch versucht, die ACL im TCAM neu zu programmieren. In den meisten Fällen kann die neue, geänderte ACL vollständig in der Hardware neu programmiert werden. Wenn der Switch die gesamte ACL erfolgreich in den TCAM umprogrammieren kann, wird folgende Meldung angezeigt:

```
*Apr 12 08:50:21: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All configured ACLs
now fully loaded in hardware TCAM - hardware switching / QoS restored
```

Verwenden Sie den **Befehl show platform software acl input summary interface *interface-id*, um zu überprüfen, ob die ACL vollständig in der Hardware programmiert ist.**

Diese Ausgabe zeigt die Konfiguration von ACL 101 zu VLAN 1 und die Überprüfung, ob die ACL vollständig in der Hardware programmiert ist:

Hinweis: Wenn die ACL nicht vollständig programmiert ist, wird möglicherweise eine TCAM-Erschöpfungsfehlermeldung angezeigt.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip access-group 101 in
Switch(config-if)#end
Switch#
Switch#show platform software acl input summary interface vlan 1
Interface Name                 : Vl1
  Path(dir:port, vlan)         : (in :null, 1)
    Current TagPair(port, vlan) : (null, 0/Normal)
    Current Signature          : {FeatureCam:(Security: 101)}
  Type                         : Current
    Direction                  : In
    TagPair(port, vlan)        : (null, 0/Normal)
    FeatureFlatAclId(state)    : 0(FullyLoadedWithToCpuAces)
    QosFlatAclId(state)        : (null)
    Flags                      : L3DenyToCpu
```

Das `Flags`-Feld (`L3DenyToCpu`) gibt an, dass das Paket an die CPU geleitet wird, wenn ein Paket aufgrund der ACL abgelehnt wird. Der Switch sendet dann eine ICMP-Meldung (Internet Control Message Protocol), die nicht erreichbar ist. Dieses Verhalten ist die Standardeinstellung. Wenn die Pakete an die CPU übergeben werden, kann auf dem Switch eine hohe CPU-Auslastung auftreten. In der Cisco IOS Software-Version 12.1(13)EW und höher sind diese Pakete jedoch auf die CPU beschränkt. In den meisten Fällen empfiehlt Cisco, die Funktion auszuschalten, die ICMP-nicht erreichbare Nachrichten sendet.

Diese Ausgabe zeigt die Konfiguration des Switches zum Senden von nicht erreichbaren ICMP-

Nachrichten und die Überprüfung der TCAM-Programmierung nach der Änderung. Der Status von ACL 101 ist jetzt `FullyLoaded`, wie die Befehlsausgabe zeigt. Der verweigerte Datenverkehr geht nicht an die CPU.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#no ip unreachables
Switch(config-if)#end

Switch#show platform software acl input summary interface vlan 1
Interface Name                : Vl1
  Path(dir:port, vlan)        : (in :null, 1)
    Current TagPair(port, vlan) : (null, 1/Normal)
    Current Signature         : {FeatureCam:(Security: 101)}
  Type                        : Current
    Direction                 : In
    TagPair(port, vlan)       : (null, 1/Normal)
    FeatureFlatAclId(state)   : 0(FullyLoaded)
    QosFlatAclId(state)       : (null)
    Flags                     : None
```

Hinweis: Wenn der QoS-TCAM während der Anwendung einer bestimmten QoS-Richtlinie überschritten wird, wird diese spezifische Richtlinie *nicht* auf die Schnittstelle oder das VLAN angewendet. Der Catalyst 4500 implementiert die QoS-Richtlinie nicht im Softwarepfad. Die CPU-Auslastung steigt daher nicht, wenn QoS-TCAM überschritten wird.

```
*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERR: Input Policy Map: 10Mbps - hardware TCAM
limit, qos being disabled on relevant interface.

*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Policy Map: 10Mbps - no
available hardware TCAM entries.
```

Geben Sie den Befehl **show platform cpu packet statistics ein**. Stellen Sie fest, ob die `ACL-Sw-` Verarbeitungswarteschlange eine hohe Anzahl von Paketen empfängt. Eine hohe Anzahl von Paketen weist darauf hin, dass der Sicherheits-TCAM erschöpft ist. Diese TCAM-Erschöpfung bewirkt, dass Pakete zur Weiterleitung der Software an die CPU gesendet werden.

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Packets Received by Packet Queue  Queue                    Total
5 sec avg 1 min avg 5 min avg 1 hour avg ---------------------- --------------- --------- ------
--- --------- ---------- Control                        57902635        22         16
12          3 Host Learning                   464678          0          0          0          0 L3
Fwd Low                       623229          0          0          0          0 L2 Fwd
Low                     11267182          7          4          6          1 L3 Rx
High                          508          0          0          0          0 L3 Rx
Low                       1275695         10          1          0          0 ACL
fwd(snooping)               2645752          0          0          0          0 ACL log,
unreach               51443268          9          4          5          5 ACL sw
processing             842889240       1453       1532       1267       1179

Packets Dropped by Packet Queue

Queue                    Total           5 sec avg 1 min avg 5 min avg 1 hour avg
------------------------ --------------- --------- --------- --------- ----------
L2 Fwd Low                            3270          0          0          0          0
ACL sw processing                    12636          0          0          0          0
```

Wenn Sie feststellen, dass die `ACL-Sw-Verarbeitungswarteschlange` keine übermäßige Menge an

Datenverkehr empfängt, finden Sie für andere mögliche Ursachen Informationen zur hohen CPU-Auslastung auf Cisco IOS Software-basierten Catalyst Switches der Serie 4500. Das Dokument enthält Informationen zur Fehlerbehebung in anderen Szenarien mit hoher CPU-Auslastung.

Der Catalyst 4500 TCAM kann aus folgenden Gründen überlaufen:

- Ein suboptimaler TCAM-Programmierungsalgorithmus für TCAM 2
- Übermäßige Verwendung von Layer-4-Prozessen (L4Ops) in einer ACL
- Übermäßige ACLs für die Supervisor Engine oder den Switch-Typ

Suboptimaler TCAM-Programmieralgorithmus für TCAM 2

Wie im Abschnitt Typen von TCAM beschrieben, ist die Effizienz von TCAM 2 geringer, da acht Einträge eine Maske gemeinsam nutzen. Die Catalyst 4500-Software ermöglicht zwei Typen von TCAM-Programmieralgorithmen für TCAM 2, die die Effizienz von TCAM 2 verbessern:

- Packet - Geeignet für die meisten Sicherheits-ACL-Szenarien**Hinweis:** Dies ist die Standardeinstellung.
- Scattered (Eingeschränkt) - Wird im IPSG-Szenario verwendet

Sie können den Algorithmus in einen verstreuten Algorithmus ändern. Dies ist jedoch in der Regel nicht hilfreich, wenn Sie nur Sicherheits-ACLs konfiguriert haben, z. B. RACLs. Der verstreute Algorithmus ist nur in Szenarien wirksam, in denen die gleiche oder eine ähnliche kleine Zugriffskontrollliste auf zahlreichen Ports wiederholt wird. Dieses Szenario ist bei einem IPSG der Fall, das auf mehreren Schnittstellen aktiviert ist. Im IPSG-Szenario gilt für jede dynamische Zugriffskontrollliste Folgendes:

- Hat eine geringe Anzahl von EinträgenDies umfasst die Genehmigung für zulässige IP-Adressen und eine Ablehnung am Ende, um den Zugriff auf den Port durch nicht autorisierte IP-Adressen zu verhindern.
- Wird für alle konfigurierten Access-Ports wiederholtDie ACL wird für bis zu 240 Ports auf einem Catalyst 4507R wiederholt.

Hinweis: TCAM 3 verwendet den gepackten Standardalgorithmus. Da die TCAM-Struktur eine Maske pro Eintrag ist, ist der gepackte Algorithmus der bestmögliche Algorithmus. Daher ist die Option für einen verstreuten Algorithmus auf diesen Switches nicht aktiviert.

Dieses Beispiel befindet sich auf einer Supervisor Engine II+, die für die IPSG-Funktion konfiguriert ist. Die Ausgabe zeigt, dass zwar nur 49 % der Einträge verwendet werden, jedoch 89 % der Masken verbraucht sind:

```
Switch#show platform hardware acl statistics utilization brief

                                    Entries/Total(%)   Masks/Total(%)
                                   -----------------   ---------------
Input   Acl(PortAndVlan)   2016 / 4096 ( 49)    460 /  512 ( 89)
Input   Acl(PortOrVlan)       6 / 4096 (  0)      4 /  512 (  0)
Input   Qos(PortAndVlan)      0 / 4096 (  0)      0 /  512 (  0)
Input   Qos(PortOrVlan)       0 / 4096 (  0)      0 /  512 (  0)
Output Acl(PortAndVlan)       0 / 4096 (  0)      0 /  512 (  0)
Output Acl(PortOrVlan)        0 / 4096 (  0)      0 /  512 (  0)
Output Qos(PortAndVlan)       0 / 4096 (  0)      0 /  512 (  0)
Output Qos(PortOrVlan)        0 / 4096 (  0)      0 /  512 (  0)
L4Ops: used 2 out of 64
```

In diesem Fall hilft eine Änderung des Programmieralgorithmus vom gepackten Standardalgorithmus zum verstreuten Algorithmus. Durch den verstreuten Algorithmus wird die Gesamtnutzung von Masken von 89 % auf 49 % reduziert.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list hardware entries scattered
Switch(config)#end
Switch#show platform hardware acl statistics utilization brief
                                    Entries/Total(%)  Masks/Total(%)
                                   -----------------  ---------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          L4Ops: used 2 out of 64
```

Informationen zu Best Practices für Sicherheitsfunktionen auf Catalyst Switches der Serie 4500 finden Sie unter Catalyst 4500 Security Features Best Practices for Supervisors.

Übermäßige Verwendung von L4Ops in einer ACL

Der Begriff L4Ops bezieht sich auf die Verwendung der **gt**, **lt**, **neq** und **Range**-Schlüsselwörter in der ACL-Konfiguration. Der Catalyst 4500 hat Beschränkungen hinsichtlich der Anzahl dieser Schlüsselwörter, die Sie in einer einzigen Zugriffskontrollliste verwenden können. Die Beschränkung, die je nach Supervisor Engine und Switch variiert, beträgt entweder sechs oder acht L4Ops pro ACL. Tabelle 3 zeigt das Limit pro Supervisor Engine und ACL.

Tabelle 3: L4Op-Obergrenze pro ACL für verschiedene Catalyst 4500 Supervisor Engines und Switches

Produkt	L4Op
Supervisor Engine II+/ II+TS	32 (6 pro ACL)
Supervisor Engine III/IV/V und WS-C4948	32 (6 pro ACL)
Supervisor Engine V-10GE und WS-C4948-10GE	64 (8 pro ACL)

Wenn die L4Op-Grenze pro ACL überschritten wird, wird in der Konsole eine Warnmeldung angezeigt. Die Nachricht ähnelt der folgenden:

```
%C4K_HWACLMAN-4-ACLHWPROGERR: Input Security: severn - hardware TCAM limit, some
packet processing will be software switched.
19:55:55: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Security: severn - hardware TCAM L4
operators/TCP flags usage capability exceeded.
```

Wenn der L4Op-Grenzwert überschritten wird, wird der spezifische ACE im TCAM erweitert. Zusätzliche TCAM-Nutzungsergebnisse Dieser ACE dient als Beispiel:

```
access-list 101 permit tcp host 8.1.1.1 range 10 20 any
```

Bei diesem ACE in einer ACL verwendet der Switch nur einen Eintrag und einen L4Op. Wenn jedoch bereits sechs L4Ops in dieser ACL verwendet werden, wird dieser ACE auf 10 Einträge in der Hardware erweitert. Eine solche Erweiterung kann möglicherweise viele Einträge im TCAM enthalten. Die sorgfältige Verwendung dieser L4Ops verhindert den TCAM-Überlauf.

Hinweis: Wenn in diesem Fall die Supervisor Engines V-10GE und WS-C4948-10GE betroffen sind, führt die ACE-Erweiterung durch acht zuvor verwendete L4Ops in der ACL.

Beachten Sie bei der Verwendung von L4Op auf Catalyst Switches der Serie 4500 folgende Punkte:

- L4-Vorgänge gelten als unterschiedlich, wenn sich der Operator oder der Operand unterscheidet.Diese ACL enthält beispielsweise drei verschiedene L4-Vorgänge, da **gt 10** und **gt 11** als zwei verschiedene L4-Vorgänge gelten:
```
access-list 101 permit tcp host 8.1.1.1 any gt 10
access-list 101 deny tcp host 8.1.1.2 any lt 9
access-list 101 deny tcp host 8.1.1.3 any gt 11
```

- L4-Vorgänge gelten als unterschiedlich, wenn dasselbe Operator-/Operandenpaar einmal für einen Quell-Port und einmal für einen Zielport gilt.Hier ein Beispiel:
```
access-list 101 permit tcp host 8.1.1.1 gt 10 any
access-list 101 permit tcp host 8.1.1.2 any gt 10
```

- Die Catalyst Switches der Serie 4500 nutzen, wenn möglich, L4Ops gemeinsam.In diesem Beispiel **veranschaulichen** die Zeilen in ***Fettschrift kursiv das*** folgende Szenario:L4Op-Verwendung für ACL 101 = 5L4Op-Verwendung für ACL 102 = 4 **Hinweis:** Das **eq**-Schlüsselwort verwendet keine der L4Op-Hardwareressourcen.Gesamtnutzung von L4Op = **8Hinweis:** ACL 101 und 102 verwenden eine L4Op gemeinsam.**Hinweis:** L4Op wird freigegeben, selbst wenn das Protokoll, z. B. TCP oder UDP, nicht übereinstimmt oder die Aktion "Zulassen/Verweigern" nicht übereinstimmt.

Übermäßige ACLs für die Supervisor Engine oder den Switch-Typ

Wie Tabelle 2 zeigt, ist TCAM eine begrenzte Ressource. Wenn Sie übermäßige Zugriffskontrolllisten oder Funktionen wie IPSG mit einer hohen Anzahl von IPSG-Einträgen konfigurieren, können Sie die TCAM-Ressource einer beliebigen Supervisor Engine überschreiten.

Wenn Sie den TCAM-Speicherplatz für die Supervisor Engine überschreiten, gehen Sie wie folgt vor:

- Wenn Sie über eine Supervisor Engine II+ verfügen und eine Cisco IOS Software-Version ausführen, die *älter* ist als die Cisco IOS-Softwareversion 12.2(18)EW, aktualisieren Sie auf die neueste Cisco IOS Software-Version 12.2(25)EWA-Wartungsversion.Die TCAM-Kapazität wurde in den späteren Versionen erhöht.
- Wenn Sie DHCP-Snooping und IPSG verwenden und wenn Ihnen der TCAM ausgeht, verwenden Sie die neueste Version der Cisco IOS-Software, Version 12.2(25)EWA, und verwenden Sie für TCAM 2-Produkte den verstreuten Algorithmus.**Hinweis:** Der verstreute Algorithmus ist ab Cisco IOS Software Release 12.2(20)EW verfügbar.Die neueste Version bietet außerdem Erweiterungen für eine bessere TCAM-Nutzung mit DCHP-Snooping und DAI-Funktionen (Dynamic Address Resolution Protocol).

- Wenn Ihnen der TCAM zu Ende geht, weil die L4Op-Obergrenze überschritten ist, versuchen Sie, die L4Op-Auslastung in der ACL zu reduzieren, um einen TCAM-Überlauf zu verhindern.
- Wenn Sie viele ähnliche ACLs oder Richtlinien auf verschiedenen Ports im selben VLAN verwenden, aggregieren Sie diese in einer einzigen ACL oder Richtlinie auf der VLAN-Schnittstelle.Durch diese Aggregation wird TCAM-Speicherplatz eingespart. Wenn Sie beispielsweise sprachbasierte Richtlinien anwenden, wird die portbasierte Standard-QoS für die Klassifizierung verwendet. Diese Standard-QoS kann dazu führen, dass die TCAM-Kapazität überschritten wird. Wenn Sie die QoS auf VLAN-basiert umstellen, reduzieren Sie die TCAM-Nutzung.
- Wenn Sie weiterhin Probleme mit dem TCAM-Bereich haben, sollten Sie eine High-End-Supervisor Engine wie die Supervisor Engine V-10GE oder Catalyst 4948-10GE in Betracht ziehen.Diese Produkte verwenden die effizienteste TCAM 3-Hardware.

Zusammenfassung

Der Catalyst 4500 programmiert die konfigurierten ACLs mit dem TCAM. TCAM ermöglicht die Anwendung der ACLs im Hardware-Weiterleitungspfad ohne Beeinträchtigung der Switch-Leistung. Trotz der Größe der Zugriffskontrollliste ist die Leistung konstant, da die Zugriffskontrolllisten mit Leitungsgeschwindigkeit ausgeführt werden. TCAM ist jedoch eine begrenzte Ressource. Wenn Sie daher eine übermäßige Anzahl von ACL-Einträgen konfigurieren, überschreiten Sie die TCAM-Kapazität. Der Catalyst 4500 hat zahlreiche Optimierungen implementiert und Befehle bereitgestellt, mit denen der Programmieralgorithmus von TCAM variiert werden kann, um maximale Effizienz zu erzielen. TCAM 3-Produkte wie die Supervisor Engine V-10GE und Catalyst 4948-10GE bieten die meisten TCAM-Ressourcen für Sicherheits-ACL- und QoS-Richtlinien.

Zugehörige Informationen

- Support-Seiten für LAN-Produkte
- Support-Seite für LAN-Switching
- Technischer Support und Dokumentation - Cisco Systems