CHAPTER 43

Cisco IOS ACL サポートの概要

この章では、Cisco IOS Release 12.2SX の Cisco IOS Access Control List（ACL; アクセス制御リスト）サポートについて説明します。

（注） Cisco IOS ACL 設定の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*, Release 12.2』の「Traffic Filtering and Firewalls」を参照してください。

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_accs_list_rmap_ps6017_TSD_Products_Configuration_Guide_Chapter.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

ハードウェアおよびソフトウェアの ACL サポート

ACL は、ハードウェアの場合には Policy Feature Card（PFC; ポリシー フィーチャ カード）、Distributed Forwarding Card（DFC）で、ソフトウェアの場合には Route Processor（RP; ルート プロセッサ）で処理できます。

- 標準 ACL および拡張 ACL（入力および出力）の「deny」文に一致する ACL フローは、「ip unreachables」がディセーブルに設定されている場合、ハードウェアによってドロップされます。
- 標準 ACL および拡張 ACL（入力および出力）の「permit」文に一致する ACL フローは、ハードウェアで処理されます。

- VLAN ACL（VACL）フローおよび Port ACL（PACL; ポート ACL）フローはハードウェアで処理されます。VACL または PACL で指定されたフィールドのハードウェア処理がサポートされていない場合、このフィールドは無視されるか（ACL の **log** キーワードなど）、または設定全体が拒否されます（IPX ACL パラメータを含む VACL など）。
- VACL ロギングはソフトウェアで処理されます。
- ダイナミック ACL フローはハードウェアで処理されます。
- アイドル タイムアウトはソフトウェアで処理されます。

（注）　アイドル タイムアウトは設定できません。Cisco IOS Release 12.2SX では、**access-enable host timeout** コマンドがサポートされていません。

- MPLS インターフェイス以外では、セッション内の最初のパケットが RP 上のソフトウェアで処理された後、リフレクシブ ACL フローがハードウェアで処理されます。
- 特定のポート上の ACL アクセス違反の IP アカウンティングは、そのポート上で拒否された全パケットを RP に転送し、ソフトウェアで処理させることによってサポートされます。この動作は他のフローには影響しません。
- PFC では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、RP のソフトウェアでサポートされます。
- 名前ベースの拡張 MAC アドレス ACL は、ハードウェアでサポートされています。
- 次の ACL タイプは、ソフトウェアによって処理されます。
  - Internetwork Packet Exchange（IPX）アクセス リスト
  - 標準 XNS アクセス リスト
  - 拡張 XNS アクセス リスト
  - DECnet アクセス リスト
  - 拡張 MAC アドレス アクセス リスト
  - プロトコル タイプコード アクセス リスト

（注）　ヘッダー長が 5 バイト未満の IP パケットは、アクセス制御されません。

- Optimized ACL Logging（OAL; 最適化された ACL ロギング）を設定しない場合、ロギングを必要とするフローはソフトウェアで処理され、ハードウェアでの非ロギング フローの処理には影響しません（「最適化された ACL ロギング」（P.43-8）を参照）。
- ソフトウェアで処理されるフローの転送レートは、ハードウェアで処理されるフローに比べると、大幅に小さくなります。
- **show ip access-list** コマンドの出力に表示される一致カウントには、ハードウェアで処理されたパケットは含まれません。
- **show policy-map interface** コマンドの出力に表示されるカウンタには、すべてのハードウェア スイッチング プラットフォーム カウンタは含まれない場合があります。

Cisco IOS ACL 設定時の注意事項および制約事項

Cisco IOS ACL をさまざまな機能とともに使用するための設定には、次の注意事項および制約事項が適用されます。

- Cisco IOS ACL をレイヤ 3 ポートおよび VLAN（仮想 LAN）インターフェイスに直接、適用できます。
- VACL と PACL をレイヤ 2 インターフェイスに適用できます（第 45 章「ポート ACL および VLAN ACL の設定」を参照）。
- 各タイプの ACL（IP、IPX、および MAC）は対応するトラフィック タイプだけをフィルタリングします。Cisco IOS MAC ACL が IP または IPX トラフィックと一致することはありません。
- PFC では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、RP のソフトウェアでサポートされます。
- デフォルトでは、パケットがアクセス グループによって拒否された場合、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）到達不能メッセージが RP によって送信されます。

  ip unreachables コマンドがイネーブルの場合（デフォルト）、Switch Processor（SP; スイッチ プロセッサ）は拒否されたパケットの大部分をハードウェアでドロップし、一部のパケット（最大で 10 パケット/秒）だけが RP に送信されてドロップされます（これにより ICMP 到達不能メッセージが生成されます）。

  拒否されたパケットをドロップし、ICMP 到達不能メッセージを生成することによって RP の CPU にかかる負荷を軽減するには、**no ip unreachables** インターフェイス コンフィギュレーション コマンドを入力して、ICMP 到達不能メッセージをディセーブルにします。これにより、アクセス グループによって拒否されたすべてのパケットがハードウェアでドロップされます。
- パケットが VACL または PACL によって拒否された場合、ICMP 到達不能メッセージは送信されません。
- 名前付き ACL を使用すると、ACL 設定の作成または変更時およびシステム再起動中の CPU 使用率を低く抑えられるため、番号付き ACL ではなく名前付き ACL を使用してください。ACL エントリを作成する（または既存の ACL エントリを変更する）場合、ソフトウェアでは ACL 設定を PFC ハードウェアにロードするために ACL マージと呼ばれる CPU 中心の動作が行われます。ACL マージはまた、システム再起動中にスタートアップ コンフィギュレーションを適用する際にも発生します。

  名前付き ACL を使用すると、ユーザが **named-acl** コンフィギュレーション モードを終了するときにだけ ACL マージが開始されます。ただし、名前付き ACL では、ACL 定義すべてについて ACL マージが開始されるため、中規模のマージが ACL 設定中に何度も行われることになります。

PB ACL

Policy-Based ACL（PBACL; ポリシーベース ACL）は Release 12.2(33)SXH 以降のリリースでサポートされます。ここでは、PBACL について説明します。

PBACL の概要

PBACL により、オブジェクト グループ全体にアクセス制御ポリシーを適用することができます。オブジェクト グループとはユーザまたはサーバの集合です。

オブジェクト グループを IP アドレスの集合として、またはプロトコル ポートの集合として定義します。それからポリシー（許可や拒否など）をオブジェクト グループに適用する Access Control Entry（ACE; アクセス制御エントリ）を作成します。たとえば、ユーザ グループがあるサーバ グループにアクセスすることを許可するポリシーベース ACE を作成することができます。

グループ名を使用して定義された ACE は、ACE が複数あるのと同じです（オブジェクト グループの各エントリに 1 つ適用されます）。PBACL ACE はシステムにより複数の Cisco IOS ACE に拡張され（グループ内の各エントリに対して 1 つの ACE）、ACE は TCAM に読み込まれます。したがって、PBACL 機能により設定が必要なエントリ数が削減されますが、TCAM 使用率は削減されません。

グループ メンバシップまたはアクセス グループを使用する ACE の内容に変更を行う場合、TCAM 内の ACE がシステムにより更新されます。次に、更新を開始する変更のタイプを示します。

- グループへのメンバーの追加
- グループからのメンバーの削除
- アクセス グループを使用する ACE のポリシー文の変更

Cisco IOS ACL 拡張コンフィギュレーション コマンドを使用して PBACL を設定します。通常の ACE と同様に、同じアクセス ポリシーを 1 つまたは複数のインターフェイスと関連付けることができます。

ACE の設定時にオブジェクト グループを使用して送信元、宛先、またはその両方を定義できます。

PBACL に関する注意事項および制約事項

PBACL を設定する際、次の注意事項および制約事項に注意してください。

- PBACL はレイヤ 3 インターフェイスでサポートされています（ルーテッド インターフェイスおよび VLAN インターフェイスなど）。
- PBACL 機能によりサポートされるのは IPv4 ACE だけです。
- PBACL 機能では、Cisco IOS ACL だけがサポートされます。それ以外の機能との組み合わせはサポートされません。キーワード **reflexive** および **evaluate** はサポートされていません。
- PBACL 機能では、名前付き Cisco IOS ACL だけがサポートされます。番号付き ACL はサポートされません。
- ポリシーベース ACL の相互作用機能は Cisco IOS ACL と同じです。

PBACL の設定

PBACL を設定するには、次の作業を行います。

- 「PBACL の IP アドレスのオブジェクト グループの設定」（P.43-5）
- 「PBACL のプロトコル ポートのオブジェクト グループの設定」（P.43-5）
- 「PBACL オブジェクト グループを使用する ACL の作成」（P.43-6）
- 「インターフェイスでの PBACL の設定」（P.43-7）

PBACL の IP アドレスのオブジェクト グループの設定

PBACL の IP アドレスのオブジェクト グループを作成または変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **object-group ip address** *object_group_name*	オブジェクト グループ名を定義します。IP アドレス オブジェクト グループ コンフィギュレーション モードを開始します。
ステップ 2	Router(config-ipaddr-ogroup)# {*ip_address mask*} | {**host** {*name* | *ip_address*} }	グループのメンバーを設定します。メンバーは、ネットワーク アドレスにマスクを付加したものか（ホスト名または IP アドレスにより識別される）ホストかのどちらかです。
ステップ 3	Router(config-ipaddr-ogroup)# {**end**} | {**exit**}	コンフィギュレーション モードを終了するには、**end** コマンドを入力します。 IP アドレス オブジェクト グループ コンフィギュレーション モードを終了するには、**exit** コマンドを入力します。
ステップ 4	Router# **show object-group** [*object_group_name*]	名前付きグループ（または名前が入力されていない場合はすべてのグループ）のオブジェクト グループの設定を表示します。

次に、3 つのホストと 1 つのネットワーク アドレスを含むオブジェクト グループを作成する例を示します。

```
Router(config)# object-group ip address myAG
Router(config-ipaddr-pgroup)# host 10.20.20.1
Router(config-ipaddr-pgroup)# host 10.20.20.5
Router(config-ipaddr-pgroup)# 10.30.0.0 255.255.0.0
```

PBACL のプロトコル ポートのオブジェクト グループの設定

PBACL のプロトコル ポートのオブジェクト グループを作成または変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **object-group ip port** *object_group_name*	オブジェクト グループ名を定義します。ポート オブジェクト グループ コンフィギュレーション モードを開始します。
ステップ 2	Router(config-port-ogroup)# {**eq** *number*} | {**gt** *number*} | {**lt** *number*} | {**neq** *number*} | {**range** *number number*}	グループのメンバーを設定します。メンバーは、ポート番号と等しいまたは等しくない、ポート番号より大きいまたは小さい、またはポート番号の範囲のいずれかです。

	コマンド	目的
ステップ 3	`Router(config-port-ogroup)# end | exit`	コンフィギュレーション モードを終了するには、**end** コマンドを入力します。 ポート オブジェクト グループ コンフィギュレーション モードを終了するには、**exit** コマンドを入力します。
ステップ 4	`Router# show object-group [object_group_name]`	名前付きグループ（または名前が入力されていない場合はすべてのグループ）のオブジェクト グループの設定を表示します。

次に、プロトコル ポート 100 と、300 以外の 200 より大きいポートと一致するポートのオブジェクト グループを作成する例を示します。

```
Router(config)# object-group ip port myPG
Router(config-port-pgroup)# eq 100
Router(config-port-pgroup)# gt 200
Router(config-port-pgroup)# neq 300
```

PBACL オブジェクト グループを使用する ACL の作成

PBACL オブジェクト グループを使用するように ACL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip access-list extended acl_name`	名前を指定して拡張 ACL を定義します。拡張 ACL コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ext-nacl)# permit tcp addrgroup object_group_name addrgroup object_group_name`	IP アドレスのオブジェクト グループを送信元ポリシーとして、オブジェクト グループを宛先ポリシーとして使用する、TCP トラフィックの ACE を設定します。
ステップ 3	`Router(config-ext-nacl)# exit`	拡張 ACL コンフィギュレーション モードを終了します。
ステップ 4	`Router# show access-lists [acl_name]`	名前付きグループ（または名前が入力されていない場合はすべてのグループ）のオブジェクト グループの設定を表示します。

次に、プロトコル ポートが myPG に指定されたポートと一致する場合に、myAG 内のユーザからのパケットを許可するアクセス リストを作成する例を示します。

```
Router(config)# ip access-list extended my-pbacl-policy
Router(config-ext-nacl)# permit tcp addrgroup myAG portgroup myPG any
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
Router# show ip access-list my-pbacl-policy
Extended IP access list my-pbacl-policy
10  permit tcp addrgroup AG portgroup PG any
20  permit tcp any any

Router# show ip access-list my-pbacl-policy expand
Extended IP access list my-pbacl-policy expanded
20 permit tcp host 10.20.20.1 eq 100 any
20 permit tcp host 10.20.20.1 gt 200 any
```

```
20 permit tcp host 10.20.20.1 neq 300 any
20 permit tcp host 10.20.20.5 eq 100 any
20 permit tcp host 10.20.20.5 gt 200 any
20 permit tcp host 10.20.20.5 neq 300 any
20 permit tcp 10.30.0.0 255.255.0.0 eq 100 any
20 permit tcp 10.30.0.0 255.255.0.0 gt 200 any
20 permit tcp 10.30.0.0 255.255.0.0 neq 300 any
```

インターフェイスでの PBACL の設定

インターフェイスでの PBACL を設定するには、**ip access-group** コマンドを使用します。このコマンド構文および使用方法は Cisco IOS ACL と同じです。詳細については、「Cisco IOS ACL 設定時の注意事項および制約事項」（P.43-3）を参照してください。

次に、アクセス リスト my-pbacl-policy と VLAN 100 を関連付ける例を示します。

```
Router(config)# int vlan 100
Router(config-if)# ip access-group mp-pbacl-policy in
```

IPv6 アドレス圧縮の設定

ACL は、ハードウェアの場合には PFC に実装されています。PFC はパケット内の送信元 IP アドレスまたは宛先 IP アドレス、およびポート番号を使用して ACL テーブルのインデックスを作成します。インデックスの最大アドレス長は 128 ビットです。

IPv6 パケットの IP アドレス フィールドは 128 ビットで、ポート フィールドは 16 ビットです。ACL ハードウェア テーブルの IPv6 アドレスをすべて使用するには、**mls ipv6 acl compress address unicast** コマンドを使用して、IPv6 アドレスの圧縮を有効にします。この機能は、IPv6 アドレスの使用されていない 16 ビットを削除することで、IPv6 アドレスをポートも含めて 128 ビットに圧縮します。圧縮可能なアドレスのタイプであれば、情報を損失することなく圧縮できます。圧縮方式の詳細については、表 43-1 を参照してください。

デフォルトで、このコマンドは圧縮を行わないように設定されています。

注意　ネットワークで圧縮できないアドレスのタイプを使用している場合は、圧縮モードをイネーブルにしないでください。表 43-1 に、圧縮可能なアドレスのタイプおよびアドレスの圧縮方式の一覧を示します。

表 43-1　圧縮可能なアドレスのタイプおよび方式

アドレスの種類	圧縮方式
MAC アドレスに基づく EUI-64	このアドレスは、ビット ロケーション [39:24] から 16 ビットを削除することにより圧縮されます。ハードウェアがこれらのアドレスを圧縮する際、情報の損失はありません。
組み込み型 IPv4 アドレス	このアドレスは、上位 16 ビットを削除することにより圧縮されます。ハードウェアがこれらのアドレスを圧縮する際、情報の損失はありません。

表 43-1　圧縮可能なアドレスのタイプおよび方式 （続き）

アドレスの種類	圧縮方式
リンク ローカル	これらのアドレスは、ビット [95:80] のゼロを削除することにより圧縮され、組み込み型 IPv4 アドレスと同じパケット タイプを使用して識別されます。ハードウェアがこれらのアドレスを圧縮する際、情報の損失はありません。
その他	上記のカテゴリに該当しない IPv6 アドレスは、その他に分類されます。IPv6 がその他に分類される場合、次のようになります。 • 圧縮モードがオンの場合、IPv6 アドレスは EUI-64 圧縮方式（ビット [39:24] の削除）と同様に圧縮され、レイヤ 4 のポート情報を QoS（Quality of Service）TCAM を検索するのに使用されるキーの一部として使用できますが、レイヤ 3 情報の損失が発生します。 • グローバル圧縮モードがオフの場合、IPv6 アドレスの 128 ビット全体が使用されます。レイヤ 4 のポート情報は IPv6 検索キーのサイズ制限のため、QoS TCAM を検索するためのキーに含まれません。

IPv6 アドレスの圧縮を有効にするには、**mls ipv6 acl compress address unicast** コマンドを入力します。IPv6 アドレスの圧縮を無効にするには、このコマンドの **no** 形式を入力します。

次に、IPv6 アドレスのアドレス圧縮を有効にする例を示します。

```
Router(config)# mls ipv6 acl compress address unicast
Router(config)#
```

次に、IPv6 アドレスのアドレス圧縮を無効にする例を示します。

```
Router(config)# no mls ipv6 acl compress address unicast
Router(config)#
```

最適化された ACL ロギング

ここでは、最適化された ACL ロギング（OAL）について説明します。

OAL の概要

OAL は、ACL ロギングをハードウェアでサポートしています。OAL を設定しないかぎり、ロギングを必要とするパケットは、RP のソフトウェアで完全に処理されます。OAL では、PFC3 のハードウェアでパケットの許可またはドロップを行います。情報は最適化ルーチンを使用して RP に送信され、ロギング メッセージが生成されます。

OAL に関する注意事項および制約事項

OAL には、次の注意事項および制約事項が適用されます。

- OAL と VACL キャプチャには互換性がありません。スイッチに両方の機能を設定しないでください。OAL を設定した場合、SPAN を使用してトラフィックをキャプチャします。
- OAL は、PFC3 でだけサポートされます。
- OAL は IPv4 ユニキャスト パケットだけをサポートしています。
- OAL は、許可された入力トラフィックの VACL ロギングをサポートしています。
- OAL はポート ACL（PACL）をサポートしていません。
- OAL は、次のものに対してはハードウェアでのサポートをしていません。
  - リフレクシブ ACL
  - 他の機能（QoS など）のトラフィックのフィルタリングに使用される ACL
  - Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）チェック例外のための ACL
  - 例外パケット（TTL 障害や MTU 障害など）
  - IP オプションが指定されたパケット
  - レイヤ 3 でルータへのアドレスが指定されたパケット
  - ICMP 到達不能メッセージを生成するために RP へ送信されるパケット
  - ハードウェアでは加速されず、機能によって処理されるパケット
- 拒否されたパケットに対する OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。
- OAL と **mls verify ip length minimum** コマンドには互換性がありません。両方を設定しないでください。

OAL の設定

ここでは、OAL の設定手順について説明します。

- 「OAL グローバル パラメータの設定」（P.43-10）
- 「インターフェイスでの OAL の設定」（P.43-10）
- 「OAL 情報の表示」（P.43-11）
- 「キャッシュされた OAL エントリのクリア」（P.43-11）

（注）

- この項で使用しているコマンドの構文および使用方法の詳細については、『Cisco IOS Master Command List, Release 12.2SX』を参照してください。
- 拒否されたパケットに対する OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。

OAL グローバル パラメータの設定

OAL グローバル パラメータを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# logging ip access-list cache {{entries number_of_entries} | {interval seconds} | {rate-limit number_of_packets} | {threshold number_of_packets}}`	OAL グローバル パラメータを設定します。

OAL グローバル パラメータを設定する場合、次の情報に注意してください。

- **entries** *number_of_entries*
  - キャッシュされるエントリの最大数を設定します。
  - 範囲：0 ～ 1,048,576（カンマを付けずに入力）
  - デフォルト：8192
- **interval** *seconds*
  - ログのためにエントリが送信されるまでの最大時間を設定します。この時間中エントリが非アクティブの場合、キャッシュから削除されます。
  - 範囲：5 ～ 86,400（1440 分つまり 24 時間、カンマを付けずに入力）
  - デフォルト：300 秒（5 分）
- **rate-limit** *number_of_packets*
  - ソフトウェアで 1 秒間にログに記録されるパケット数を設定します。
  - 範囲：10 ～ 1,000,000（カンマを付けずに入力）
  - デフォルト：0（レート制限がオフになり、すべてのパケットがログに記録されます）
- **threshold** *number_of_packets*
  - エントリがログに記録されるまでに一致するパケット数を設定します。
  - 範囲：1 ～ 1,000,000（カンマを付けずに入力）
  - デフォルト：0（一致したパケットの数ではログの記録を開始しません）

インターフェイスでの OAL の設定

インターフェイスで OAL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port}`	設定するインターフェイスを指定します。
ステップ 2	`Router(config-if)# logging ip access-list cache in`	インターフェイスの入力トラフィックに対して OAL をイネーブルにします。
ステップ 3	`Router(config-if)# logging ip access-list cache out`	インターフェイスの出力トラフィックに対して OAL をイネーブルにします。

1. *type* = レイヤ 3 スイッチド トラフィックをサポートする任意のタイプ

OAL 情報の表示

OAL 情報を表示するには、次の作業を行います。

コマンド	目的
`Router # show logging ip access-list cache`	OAL 情報を表示します。

キャッシュされた OAL エントリのクリア

キャッシュされた OAL エントリをクリアするには、次の作業を行います。

コマンド	目的
`Router # clear logging ip access-list cache`	キャッシュされた OAL エントリをクリアします。

ACL におけるレイヤ 4 演算の使用上の注意事項および制約事項

ここでは、レイヤ 4 ポート演算を含む ACL を設定する場合の注意事項および制約事項について説明します。

- 「レイヤ 4 演算の使用」（P.43-11）
- 「論理演算ユニットの使用」（P.43-12）

レイヤ 4 演算の使用

次のタイプの演算子を指定できます。

- gt（geater than：より大きい）
- lt（less than：より小さい）
- neq（not equal：等しくない）
- eq（equal：等しい）
- range（inclusive range：包含範囲）

1 つの ACL に指定する演算は、*9* つまでにすることを推奨します。この数を超えると、新しい演算によって影響される ACE が、複数の ACE に分割されることがあります。

レイヤ 4 演算を使用するときは、次の 2 つの注意事項に従ってください。

- レイヤ 4 演算は、演算子またはオペランドが異なっていると、違う演算であると見なされます。たとえば、次の ACL には 3 つの異なるレイヤ 4 演算が定義されています（「gt 10」と「gt 11」は 2 つの異なるレイヤ 4 演算です）。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```

（注）「eq」演算子の使用に制限はありません。「eq」演算子は Logical Operator Unit（LOU; 論理演算ユニット）またはレイヤ 4 演算ビットを使用しないためです。LOU については、「論理演算ユニットの使用」（P.43-12）を参照してください。

- レイヤ 4 演算は、同じ演算子 / オペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算になります。たとえば次の ACL では、1 つの ACE には送信元ポート、もう 1 つの ACE には宛先ポートが指定されているので、2 つの異なるレイヤ 4 演算が定義されていることになります。

```
... Src gt 10 ...
... Dst gt 10
```

論理演算ユニットの使用

論理演算ユニット（LOU）は、演算子 / オペランドの組み合わせを保存するレジスタです。ACL はすべて、LOU を使用します。最大 32 の LOU があります。各 LOU には、2 つの異なる演算子 / オペランドの組み合わせを保存できますが、range 演算子だけは例外です。レイヤ 4 演算は、次のように LOU を使用します。

- gt は、1/2 LOU を使用します。
- lt は、1/2 LOU を使用します。
- neq は、1/2 LOU を使用します。
- range は、1 LOU を使用します。
- eq は、LOU を使用しません。

たとえば、次の ACL では、1 つの LOU に 2 つの異なる演算子 / オペランドの組み合わせが保存されます。

```
... Src gt 10 ...
... Dst gt 10
```

以下は、より詳細な例です。

```
ACL1
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny

ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

レイヤ 4 演算数と LOU 数は、次のとおりです。

- ACL1 のレイヤ 4 演算：5
- ACL2 のレイヤ 4 演算：4
- LOU：4

LOU は、次のように使用されています。

- LOU 1 に、「gt 10」と「lt 9」が保存されます。
- LOU 2 に、「gt 11」と「neq 6」が保存されます。
- LOU 3 に、「gt 20」が保存されます（半分は空き）。
- LOU 4 に、「range 11 13」が保存されます（range には LOU の全領域が必要）。

ヒント

Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

ヒント