ACL コマンド

この章は、次の項で構成されています。

ip access-list（IP 拡張）

IPv4 アクセス リスト（ACL）に名前を付けてデバイスを IPv4 アクセス リスト コンフィギュレーション モードにするには、**ip access-list extended** グローバル コンフィギュレーション モードコマンドを使用します。このコマンドに続くすべてのコマンドは、この ACL を参照します。この ACL のルール（ACE）は、permit (IP) （3 ページ） および deny（IP） （6 ページ） コマンドで定義されます。service-acl input （21 ページ） コマンドは、この ACL をインターフェイスに適用する場合に使用します。

アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ip access-list extended *acl-name*

no ip access-list extended *acl-name*

パラメータ

- **acl-name**：IPv4 アクセス リストの名前。（範囲：1 ～ 32 文字）

デフォルト設定

定義されている IPv4 アクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IPv4 ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL または ポリシー マップには、同じ名前を使用できません。

例

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)#
```

permit (IP)

IPv4 アクセス リスト（ACL）の許可条件を設定するには、**permit** IP アクセス リスト コンフィギュレーション モード コマンドを使用します。許可条件は、アクセス コントロール エントリ（ACE）とも呼ばれます。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

permit *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]**

permit udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard}* [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]**

no permit udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

パラメータ

- ***protocol***：IP プロトコルの名前または番号。利用可能なプロトコル名は、icmp、igmp、ip、tcp、egp、igp、udp、hmp、rdp、idpr、ipv6、ipv6:rout、ipv6:frag、idrp、rsvp、gre、esp、ah、ipv6:icmp、eigrp、ospf、ipinip、pim、l2tp、isis です。任意のプロトコルを照合するには、**ip** キーワードを使用します（範囲：0 ～ 255）。
- ***source***：パケットの送信元 IP アドレス。

- ***source-wildcard***：送信元 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 IP アドレス。
- ***destination-wildcard***：宛先 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- **dscp** *number*：DSCP 値を指定します。
- **precedence** *number*：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。echo-reply、destination-unreachable、source-quench、redirect、alternate-host-address、echo-request、router-advertisement、router-solicitation、time-exceeded、parameter-problem、timestamp、timestamp-reply、information-request、information-reply、address-mask-request、address-mask-reply、traceroute、datagram-conversion-error、mobile-host-redirect、mobile-registration-request、mobile-registration-reply、domain-name-request、domain-name-reply、skip、photuris。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***igmp-type***：IGMP パケットは、IGMP メッセージ タイプでフィルタ処理できます。番号または次の値のいずれかを入力します。host-query、host-report、dvmrp、pim、cisco-trace、host-report-v2、host-leave-v2、host-report-v3。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP 宛先ポートを指定します。ポートの範囲を入力するには、ハイフンを使用します。例：20-21。TCP の場合は番号か次の値のいずれかを入力します。bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は、番号または次の値の 1 つを入力します：biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、on500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs-ds (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）。
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）
- **match-all** *list-of-flags*：発生する必要のある TCP フラグのリスト。フラグを設定する場合は「+」を前に付けます。フラグを設定しない場合は「-」を前に付けます。使用可能なオプ

ションは +urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。

- **time-range-name**：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **log-input**：エントリに一致するパケットに関する情報 SYSLOG メッセージを送信することを指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

デフォルト設定

定義されている IPv4 アクセス リストはありません。

コマンド モード

IP アクセスリスト コンフィギュレーション モード

使用上のガイドライン

ある範囲のポートが ACE の送信元ポートに使用されている場合、別の ACE の送信元ポートにも使用されていれば再びカウントされません。ポートの範囲が ACE の宛先ポートに使用される場合、別の ACE の宛先ポートに使用されていても、再カウントはされません。

ポートの範囲が送信元ポートに使用される場合、宛先ポートにも使用されていると、再カウントされます。

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
```

deny（IP）

IPv4 アクセス リストの拒否条件を設定するには、**deny** IP アクセス リスト コンフィギュレーション モード コマンドを使用します。拒否条件は、アクセス コントロール エントリ（ACE）とも呼ばれます。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

deny *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port**|**log-input**]

deny *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]][**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*][**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**match-all** *list-of-flags*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input** *]*

no deny *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input** *]*

no deny tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*][**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

パラメータ

- ***protocol***：IP プロトコルの名前または番号。利用可能なプロトコル名は、icmp、igmp、ip、tcp、egp、igp、udp、hmp、rdp、idpr、ipv6、ipv6:rout、ipv6:frag、idrp、rsvp、gre、esp、ah、ipv6:icmp、eigrp、ospf、ipinip、pim、l2tp、isis です。任意のプロトコルを照合するには、Ip キーワードを使用します。（範囲：0 ～ 255）

- ***source***：パケットの送信元 IP アドレス。
- ***source-wildcard***：送信元 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 IP アドレス。
- ***destination-wildcard***：宛先 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- **dscp** *number*：DSCP 値を指定します。
- **precedence** *number*：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。echo-reply、destination-unreachable、source-quench、redirect、alternate-host-address、echo-request、router-advertisement、router-solicitation、time-exceeded、parameter-problem、timestamp、timestamp-reply、information-request、information-reply、address-mask-request、address-mask-reply、traceroute、datagram-conversion-error、mobile-host-redirect、mobile-registration-request、mobile-registration-reply、domain-name-request、domain-name-reply、skip、photuris。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***igmp-type***：IGMP パケットは、IGMP メッセージ タイプでフィルタ処理できます。番号または次の値のいずれかを入力します。host-query、host-report、dvmrp、pim、cisco-trace、host-report-v2、host-leave-v2、host-report-v3。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP 宛先ポートを指定します。ポートの範囲を入力するには、ハイフンを使用します。例：20-21。TCP の場合は番号か次の値のいずれかを入力します。bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は、番号または次の値の 1 つを入力します：biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、non500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs-ds (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）

- **match-all** *list-of-flags*：発生する必要のある TCP フラグのリスト。フラグのセットが必要な場合は、「+」を先頭に付けます。フラグのセット解除が必要な場合は、「-」を先頭に付けます。使用可能なオプションは+urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。
- **time-range-name**：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **disable-port**：この条件に一致する場合、イーサネット インターフェイスは無効になります。
- **log-input**：エントリに一致するパケットに関する情報 syslog メッセージを送信するように指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

デフォルト設定

定義されている IPv4 アクセス リストはありません。

コマンド モード

IP アクセスリスト コンフィギュレーション モード

使用上のガイドライン

ACL で定義可能な TCP/UDP 範囲の数は制限されています。ある範囲のポートが ACE の送信元ポートに使用されている場合、別の ACE の送信元ポートにも使用されていれば再びカウントされません。ポートの範囲が ACE の宛先ポートに使用される場合、別の ACE の宛先ポートに使用されていても、再カウントはされません。

ある範囲のポートが送信元ポートに使用されている場合、宛先ポートにも使用されていれば再びカウントされます。

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# deny ip 176.212.0.0 00.255.255 any
```

ipv6 access-list（IPv6 拡張）

IPv6 アクセス リスト（ACL）を定義して、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにするには、**ipv6 access-list** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドに続くすべてのコマンドは、この ACL を参照します。

アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 access-list [*acl-name]*

no ipv6 access-list *[acl-name]*

パラメータ

acl-name：IPv6 アクセス リストの名前。範囲：1 ～ 32 文字。

デフォルト設定

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IPv6 ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL または ポリシー マップには、同じ名前を使用できません。

すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-ns any**、**permit icmp any any nd-na any**、および **deny ipv6 any any** ステートメントがあります（前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します）。

IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 ネイバー探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 ネイバー探索プロセスと同等のアドレス解決プロトコル（ARP）は、別のデータリンク層プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

例

```
switchxxxxxx(config)#  ipv6 access-list acl1
switchxxxxxx(config-ip-al)#  permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

permit（IPv6）

IPv6 ACL の許可条件（ACE）を設定するには、Ipv6 アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの **no** 形式を使用します。

構文

permit *protocol* {**any** |{*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input**] [**flow-label** *flow-label-value*]

permit icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

permit tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any** | *destination-port*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

permit udp {any | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any** | *destination-port*} [**ace-priority** *priority*][**dscp** *number* | precedence *number*][**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit *protocol* {**any** |{*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit tcp {**any** | {*source-prefix*/*length*} {**any** | source-port}}{**any** | destination- prefix/length} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

パラメータ

- ***protocol***：IP プロトコルの名前または番号。使用可能なプロトコル名は、icmp (58)、tcp (6) および udp (17) です。任意のプロトコルに一致させるには、ipv6 キーワードを使用します。（範囲：0 ～ 255）
- ***source-prefix / lenght***：許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
- ***destination-prefix / lenght***：許可条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***dscp number***：DSCP 値を指定します。(範囲：0 ～ 63)
- ***precedence number***：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。destination-unreachable (1)、packet-too-big (2)、time-exceeded (3)、parameter-problem (4)、echo-request (128)、echo-reply (129)、mld-query (130)、mld-report (131)、mldv2-report (143)、mld-done (132)、router-solicitation (133)、router-advertisement (134)、nd-ns (135)、nd-na (136)。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP宛先ポートを指定します。TCP の場合は番号か次の値のいずれかを入力します。bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は番号か次の値のいずれかを入力します。biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、non500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）
- ***match-all list-of-flag***：発生するはずの TCP フラグのリスト。フラグのセットが必要な場合は、「+」を先頭に付けます。フラグのセット解除が必要な場合は、「-」を先頭に付けます。使用可能なオプションは+urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **log-input**：エントリに一致するパケットに関する情報 syslog メッセージを送信するように指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。
- **flow-label** *flow-label-value*：IPv6 フローラベル値を指定します。これらの引数の値は、0 ー 1048575 の範囲にする必要があります。

デフォルト設定

IPv6 アクセス リストは定義されていません。

コマンド モード

Ipv6 アクセス リスト コンフィギュレーション モード

使用上のガイドライン

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

フローラベルとポート範囲を同時に設定することはできません。

フローラベルは出力 ACL には設定できません。

例 1。この例では、サーバの名前で ACL を定義し、tcp パケット用のルール（ACE）を入力しています。

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

例 2。次に、**flow-label** キーワードを指定して ACL を定義する例を示します。

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit ipv6 any any flow-label 5
```

deny（IPv6）

IPv6 ACL の拒否条件（ACE）を設定するには、IPv6 アクセスリスト コンフィギュレーション モードで **deny** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

deny *protocol* {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**ace-priority** *priority]*[**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} *[***ace-priority** *priority]*[**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny *protocol* {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

パラメータ

- ***protocol***：IP プロトコルの名前または番号。使用可能なプロトコル名は、icmp (58)、tcp (6) および udp (17) です。任意のプロトコルに一致させるには、ipv6 キーワードを使用します。（範囲：0 ～ 255）
- ***source-prefix*/*length***：許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
- ***destination-prefix / lenght***：許可条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***dscp number***：DSCP 値を指定します。(範囲：0 ～ 63)
- ***precedence number***：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。destination-unreachable (1)、packet-too-big (2)、time-exceeded (3)、parameter-problem (4)、echo-request (128)、echo-reply (129)、mld-query (130)、mld-report (131)、mldv2-report (143)、mld-done (132)、router-solicitation (133)、router-advertisement (134)、nd-ns (135)、nd-na (136)。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP宛先ポートを指定します。TCPの場合は、番号または次の値の 1 つを入力します：bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は番号か次の値のいずれかを入力します。biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、non500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）
- ***match-all list-of-flags***：発生する TCP フラグのリスト。フラグのセットが必要な場合は、「+」を先頭に付けます。フラグのセット解除が必要な場合は、「-」を先頭に付けます。使用可能なオプションは +urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- ***disable-port***：この条件に一致する場合、イーサネット インターフェイスは無効になります。
- ***log-input***：エントリに一致するパケットに関する情報 syslog メッセージを送信することを指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。
- ***flow-label flow-label-value***：IPv6 フローラベル値を指定します。これらの引数の値は、0 ー 1048575 の範囲にする必要があります。

デフォルト設定

IPv6 アクセス リストは定義されていません。

コマンド モード

Ipv6 アクセス リスト コンフィギュレーション モード

使用上のガイドライン

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priorityは、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

フローラベルとポート範囲を同時に設定することはできません。

フローラベルは出力 ACL には設定できません。

例

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

mac access-list

送信元 MAC アドレス フィルタに基づいてレイヤ 2 アクセス リスト（ACL）を定義し、デバイスを MAC アクセス リスト コンフィギュレーション モードにするには、**mac access-list** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドに続くすべてのコマンドは、この ACL を参照します。

アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

構文

mac access-list extended *acl-name*

no mac access-list extended *acl-name*

パラメータ

acl-name：MAC ACL の名前を指します（範囲：1 ～ 32 文字）。

デフォルト設定

定義されている MAC アクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

MAC ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL、またはポリシー マップに同じ名前を付けることはできません。ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

permit（MAC）

MAC ACL の許可条件（ACE）を設定するには、MAC アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

permit *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [***ace-priority** *priority][eth-type 0* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name]*

*[***log-input]**

no permit *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [eth-type 0* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name]*

*[***log-input]**

パラメータ

- ***source***：パケットの送信元 MAC アドレス。
- ***source-wildcard***：送信元MACアドレスに適用されるワイルドカード ビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 MAC アドレス。
- ***destination-wildcard***：宛先 MAC アドレスに適用されるワイルドカード ビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセス コントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***eth-type***：パケットのイーサネット タイプ（16 進表記）。
- ***vlan-id***：パケットの VLAN ID。（範囲：1 ～ 4094）
- ***cos***：パケットのサービス クラス。（範囲：0 ～ 7）
- ***cos-wildcard***：CoS に適用されるワイルドカード ビット。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **log-input**：エントリに一致するパケットに関する情報 syslog メッセージを送信するように指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

使用上のガイドライン

MAC ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL またはポリシーマップを同じ名前にすることはできません。ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

デフォルト設定

定義されている MAC アクセス リストはありません。

コマンド モード

MAC アクセスリスト コンフィギュレーション モード

例

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

deny（MAC）

MAC ACL の拒否条件（ACE）を設定するには、MAC アクセス リスト コンフィギュレーション モードで **deny** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

deny *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [***ace-priority** *priority][{eth-type 0}|* **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name] [***disable-port** |**log-input** *]*

no deny *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [{eth-type 0}|* **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name] [***disable-port** |**log-input** *]*

パラメータ

- ***source***：パケットの送信元 MAC アドレス。
- ***source-wildcard***：送信元MACアドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 MAC アドレス。
- ***destination-wildcard***：宛先 MAC アドレスに適用されるワイルドカード ビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***eth-type***：パケットのイーサネット タイプ（16 進表記）。
- ***vlan-id***：パケットの VLAN ID。（範囲：1 ～ 4094）
- ***cos***：パケットのサービス クラス。（範囲：0 ～ 7）。
- ***cos-wildcard***：CoS に適用されるワイルドカード ビット。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- ***disable-port***：この条件に一致する場合、イーサネット インターフェイスは無効になります。
- ***log-input***：エントリに一致するパケットに関する情報 syslog メッセージを送信することを指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

デフォルト設定

定義されている MAC アクセス リストはありません。

コマンド モード

MAC アクセスリスト コンフィギュレーション モード

使用上のガイドライン

MAC ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL、またはポリシーマップに同じ名前を付けることはできません。

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# deny 00:00:00:00:00:01 00:00:00:00:00:ff any
```

service-acl input

アクセスリスト（ACL）をインターフェイスにバインドするには、インターフェイス コンフィギュレーション モードで **service-acl input** コマンドを使用します。

インターフェイスからすべての ACL を削除するには、このコマンドの **no** 形式を使用します。

構文

service-acl input *acl-name1* [*acl-name2*] [**default-action** {**deny-any** | **permit-any**}]

no service-acl input

パラメータ

- ***acl-name***：インターフェイスに適用する ACL を指定します。ユーザ ガイドラインを参照してください。（範囲：1 ～ 32 文字）。
- **deny-any**：この ACL のルールを満たさないすべてのパケット（ポートで入力されたもの）を拒否します。
- **permit-any**：この ACL のルールを満たさないすべてのパケット（ポートで入力されたもの）を転送します。

デフォルト設定

ACL は割り当てられていません。ACL のデフォルトアクションは deny-any です。

コマンド モード

インターフェイス コンフィギュレーション モード（イーサネット、ポートチャネル、VLAN）

使用上のガイドライン

どのような場合に ACL をインターフェイスにバインドできるか、またはインターフェイスからバインド解除できるかは、次のルールに従います。

- IPv4 ACL と IPv6 ACL は、インターフェイスに一緒にバインドできます。
- MAC ACL は、すでに IPv4 ACL または IPv6 ACL がバインドされているインターフェイスにバインドすることはできません。
- 同じタイプの 2 つの ACL をポートにバインドすることはできません。
- まず現在の ACL を削除することなく、ACL にすでにバインドされているポートに ACL をバインドすることはできません。このコマンドでは、両方の ACL を同時に指定する必要があります。
- 一致基準として VLAN を含む MAC ACL は、VLAN にバインドできません。

- いずれかの ACE に時間ベースの設定が使用されている ACL を VLAN にバインドすることはできません。
- シャットダウン アクションが使用されている ACL は VLAN にバインドできません。
- ユーザが ACL をインターフェイスにバインドすると、TCAM リソースが使用されます。MAC または IP ACE ごとに 1 つの TCAM ルール、IPv6 ACE ごとに 2 つの TCAM ルールが使用されます。TCAM の使用量は常に偶数になるため、ルールの数が奇数になった場合は、使用量が 1 増えます。
- ACL は、出力としてバインドされている場合、入力としてバインドできません。

例

```
switchxxxxxx(config)# mac access-list extended server-acl
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# service-acl input server-acl default-action deny-any
```

service-acl output

出力（伝送パス）上のインターフェイスへのアクセスを制御するには、インターフェイス コンフィギュレーション モードで **service-acl output** コマンドを使用します。

アクセス制御を削除するには、このコマンドの **no** 形式を使用します。

構文

service-acl output *acl-name1* [*acl-name2*] [**default-action** {**deny-any** | **permit-any**}]

no service-acl output

パラメータ

- ***acl-name***：インターフェイスに適用する ACL を指定します。ユーザ ガイドラインを参照してください。（範囲：1 ～ 32 文字）。
- **deny-any**：この ACL のルールを満たさない（ポートの出力上の）すべてのパケットを拒否します。
- **permit-any**：この ACL のルールを満たさない（ポートの出力上の）すべてのパケットを転送します。

デフォルト

ACL は割り当てられていません。デフォルトアクションは deny-any です。

コマンド モード

インターフェイス コンフィギュレーション モード（イーサネット、ポートチャネル）

使用上のガイドライン

ルールアクション：log-input はサポートされていません。使用しようとすると、エラーになります。

拒否ルールアクションの disable-port はサポートされていません。使用しようとすると、エラーになります。

IPv4 ACL と IPv6 ACL は、インターフェイス上でバインドできます。

MAC ACL は IPv4 ACL または IPv6 ACL とインターフェイス上でバインドできません。

同じタイプの 2 つの ACL をポートに追加することはできません。

現在の ACL を最初に削除して 2 つの ACL をバインドせずに、すでに ACL にバインドされているポートに ACL を追加することはできません。

入力としてバインドされている ACL は出力としてバインドできません。

例

次に、出力 ACL をポートにバインドする例を示します。

```
switchxxxxxx(config)# mac access-list extended server
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# service-acl output server
```

time-range

さまざまな機能の時間範囲を定義するには、**time-range** グローバル コンフィギュレーション モード コマンドを使用します。また、このコマンドを使用すると時間範囲コンフィギュレーション モードになります。このコマンドの後は、すべてのコマンドが定義されている時間範囲を参照します。

このコマンドは、時間範囲の名前を設定します。実際の時間範囲を設定するには、absolute （27 ページ） コマンドと periodic （28 ページ） コマンドを使用します。

デバイスから時間範囲を削除する場合は、このコマンドの **no** 形式を使用します。

構文

time-range *time-range-name*

no time-range *time-range-name*

パラメータ

time-range-name：時間範囲の名前を指定します。（範囲：1 ～ 32 文字）

デフォルト設定

時間範囲は定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

time-range コマンドに absolute 値と periodic 値の両方が指定されている場合、periodic 項目は absolute start 時刻を経過した後にのみ評価の対象になり、absolute end 時刻を経過した後は再度評価の対象にはなりません。

すべての時間指定は、現地時間と解釈されます。

時間範囲のエントリを希望の時間に有効にするには、ユーザまたは SNTP がソフトウェア クロックを設定する必要があります。ユーザまたはSNTPがソフトウェア クロックを設定しない場合、時間範囲 ACE は有効になりません。

ユーザは、機能にバインドされている時間範囲を削除することはできません。

時間範囲が定義されている場合は、次のコマンドで使用できます。

- dot1x port-control
- power inline
- operation time
- permit (IP)

- deny (IP)
- permit（IPv6）
- deny（IPv6）
- permit（MAC）
- deny（MAC）

例

```
switchxxxxxx(config)# time-range http-allowed
console(config-time-range)#periodic mon 12:00 to wed 12:00
```

absolute

時間範囲が有効になっている場合に絶対時間を指定するには、**absolute** 時間範囲コンフィギュレーション モード コマンドを使用します。時間制限を削除するには、このコマンドの **no** 形式を使用します。

構文

absolute *start* *hh:mm day month year*

no absolute *start*

absolute *end* *hh:mm day month year*

no absolute *end*

パラメータ

- **start**：関連付けられた機能の許可ステートメントまたは拒否ステートメントが有効になる絶対日時。start 日時が指定されていない場合、その機能はただちに有効になります。
- **end**：関連付けられた機能の許可ステートメントまたは拒否ステートメントが有効でなくなる絶対日時。end 日時が指定されていない場合、その機能は無期限に有効になります。
- **hh:mm**：時間（24 時間形式）および分単位の時刻（範囲：0 ～ 23、mm：0 ～ 5）。
- **day**：日付。（範囲：1 ～ 31）
- **month**：月（名前の最初の 3 文字）。（範囲：Jan ～ Dec）
- **year**：年（省略なし）（範囲：2000 ～ 2097）

デフォルト設定

時間範囲が有効になっている場合の絶対時間はありません。

コマンド モード

時間範囲コンフィギュレーション モード

例

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005
```

periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、**periodic** 時間範囲コンフィギュレーション モード コマンドを使用します。時間制限を削除するには、このコマンドの **no** 形式を使用します。

構文

periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*

no periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*

periodic list *hh:mm* **to** *hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

no periodic list *hh:mm* **to** *hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

periodic list *hh:mm* **to** *hh:mm all*

no periodic list *hh:mm* **to** *hh:mm all*

パラメータ

- **day-of-the-week**：関連付けられた時間範囲が有効になる開始日。2 つ目は、関連付けられたステートメントが有効な終了日です。2つ目は、翌週にすることができます（ユーザ ガイドラインの説明を参照）。有効な値は、mon、tue、wed、thu、fri、sat、sun です。
- **hh:mm**：この引数の 1 つ目は、関連付けられた時間範囲が有効になる開始時間:分（24 時間形式）です。2 つ目は、関連付けられたステートメントが有効な終了時間:分（24 時間形式）です。2つ目は、翌日にすることができます（ユーザ ガイドラインの説明を参照）。（範囲：0 ～ 23、mm：0 ～ 59）
- **list day-of-the-week**：時間範囲が有効になる曜日のリストを指定します。

デフォルト設定

時間範囲が有効になっている場合の定期的な時間はありません。

コマンド モード

時間範囲コンフィギュレーション モード

使用上のガイドライン

2 つ目の曜日は、翌週にすることができます。たとえば、木曜日から月曜日を指定した場合、時間範囲は木曜日、金曜日、土曜日、日曜日、および月曜日に有効になります。

2 つ目の時刻は、翌日にすることができます（「22:00 ～ 2:00」など）。

例

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
```

show time-range

時間範囲設定を表示するには、**show time-range** ユーザ EXEC モード コマンドを使用します。

構文

show time-range *time-range-name*

パラメータ

time-range-name：既存の時間範囲の名前を指定します。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx> show time-range
http-allowed
--------------
absolute start 12:00 1 Jan 2005 end  12:00 31 Dec 2005
periodic Monday 12:00 to Wednesday 12:00
```

show access-lists

スイッチで設定されたアクセス コントロール リスト（ACL）を表示するには、**show access-lists** 特権 EXEC モード コマンドを使用します。

構文

show access-lists [*name*]

show access-lists ***time-range-active*** *[name]*

パラメータ

- **name**：ACL の名前を指定します（範囲：1 ～ 160 文字）。
- **time-range-active**：時間範囲が現在アクティブなアクセス コントロール エントリ（ACE）のみを表示します（時間範囲に関連付けられていないものを含む）。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show access-lists
Standard IP access list 1
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any priority 20 time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any priority 40 time-range weekdays
switchxxxxxx# show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any priority 20
permit 234 172.30.8.8  0.0.0.0 any priority 40
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any priority 20  time-range weekdays
switchxxxxxx# show access-lists ACL1
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any priority 20
permit 234 172.30.8.8  0.0.0.0 any priority 40
```

clear access-lists counters

アクセス リスト（ACL）のカウンタをクリアするには、**clear access-lists counters** 特権 EXEC モード コマンドを使用します。

構文

clear access-lists counters *[interface-id]*

パラメータ

interface-id：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# clear access-lists counters gi1/0/1
```

show interfaces access-lists trapped packets

アクセス リスト（ACL）のトラップ パケットを表示するには、**show interfaces access-lists trapped packets** 特権 EXEC モード コマンドを使用します。

構文

show interfaces access-lists trapped packets *[interface-id | port-channel-number | VLAN]*

パラメータ

- **interface-id**：インターフェイス ID を指定します。このインターフェイス ID は、イーサネット ポートのポート チャネルです。
- **port-channel**：ポート チャネルを指定します。
- **VLAN**：VLAN を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、インターフェイスでのロギングを有効にして、ACEのヒットからパケットがトラップされているかどうかを表示します。

例 1：

```
switchxxxxxx# show interfaces access-lists trapped packets
Ports/LAGs: gi1/0/1-gi1/0/3, ch1-ch3, ch4
VLANs: VLAN1, VLAN12-VLAN15
Packets were trapped globally due to lack of resources
```

例 2：

```
switchxxxxxx# show interfaces access-lists trapped packets gi1/0/1
Packets were trapped on interface gi1/0/1
```

ip access-list（IP 標準）

IP 標準リストを定義するには、**ip access-list** グローバル コンフィギュレーション モード コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ip access-list *access-list-name* {**deny**|**permit**} {*src-addr*[*/src-len*] | **any**}

no ip access-list *access-list-name*

パラメータ

- **access-list-name**：標準 IP アクセス リストの名前。名前には、最大で 32 文字まで使用できます。
- **deny/permit**：条件が満たされた場合にアクセスを拒否または許可します。

  src-addr[*/src-len*] | **any**：IP アドレスと長さで定義された IP プレフィックス、または **any**。**any** 値は、すべての IP アドレスに一致します。*src-len* を定義しないと、値は 32 が適用されます。*src-len* の値は、1 ～ 32 である必要があります。

デフォルト設定

定義されているアクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IP アドレス フィルタリングを設定するには、**ip access-list** コマンドを使用します。一致条件に基づいて IP アドレスを許可または拒否するには、アクセス リストを **permit** または **deny** キーワードを指定して設定します。どのアクセスリストのエントリとも一致しないアドレスには、暗黙の **deny** が適用されます。

アクセスリスト エントリは、IP アドレスとビット マスクで構成されています。ビット マスクは、1 ～ 32 の数値です。

アクセス リストによる IP アドレスの評価は、リストの最初のエントリから始まり、一致が検出されるまでリストを下方向に評価します。IP アドレスの一致が見つかると、そのアドレスに permit または deny ステートメントが適用され、リストの残りは評価されません。

アクセス リストを削除するには、**no ip access-list** コマンドを使用します。

IPv4 標準アクセスリストは、送受信された IPv4 ルーティング情報をフィルタ処理するために使用されます。

例

例 1：次の標準アクセス リストの例では、指定した 3 つのネットワークのみを許可します。アクセス リスト ステートメントに一致しない IP アドレスは拒否されます。

```
switchxxxxxx(config)# ip access-list 1 permit 192.168.34.0/24
switchxxxxxx(config)# ip access-list 1 permit 10.88.0.0/16
switchxxxxxx(config)# ip access-list 1 permit 10.0.0.0/8
```

注：その他のアクセスはすべて暗黙で拒否されます。

例 2：次の標準アクセス リストの例では、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスのアクセスを許可します。この範囲外のすべての IP アドレスは、拒否されます。

```
switchxxxxxx(config)# ip access-list apo permit 10.29.2.64/26
```

注：その他のアクセスはすべて暗黙で拒否されます。

例 3：多数のアドレスの個別の指定を簡略にするには、マスク長が 32 の場合、指定を省略できます。したがって、次の 2 つの設定コマンドは同様に有効です。

```
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3/32
```

ipv6 access-list（IP 標準）

ipv6 access-list グローバル コンフィギュレーション モード コマンドによって、IPv6 標準リストを定義します。リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 access-list *access-list-name* {**deny**|**permit**} {*src-addr*[*/src-len*] | **any**}

no ipv6 access-list *access-list-name*

パラメータ

- **access-list-name**：標準 IPv6 アクセスリストの名前。名前には、最大で 32 文字まで使用できます。
- **deny**：条件に合致した場合にアクセスを拒否します。
- **permit**：条件が一致した場合にアクセスが許可されます。
- **src-addr[/src-len] | any**：IPv6 アドレスと長さまたは any として定義された IPv6 プレフィックス。**any** 値は、すべての IPv6 アドレスに一致します。*src-len* を定義しない場合、値には 128 が適用されます。*src-len* の値は、1 ～ 128 である必要があります。

デフォルト設定

アクセスリストはありません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IPv6 アドレスのフィルタ処理を設定するには、**ipv6 access-list** コマンドを使用します。一致条件に基づいて IPv6 アドレスを許可または拒否するには、**permit** キーワードまたは **deny** キーワードでアクセスリストを設定します。どのアクセスリストのエントリとも一致しないアドレスには、暗黙の **deny** が適用されます。

アクセスリスト エントリは、IP アドレスとビット マスクで構成されています。ビットマスクは 1 ～ 128 の数値です。

アクセスリストによる IPv6 アドレスの評価では、リストの最初のエントリから開始して、一致が検出されるまでリストを下方向に評価します。IPv6 アドレスの一致が見つかると、そのアドレスに permit または deny ステートメントが適用され、リストの残りは評価されません。

アクセスリストを削除するには、**no ipv6 access-list** コマンドを使用します。

IPv6 標準アクセスリストは、受信および送信された IPv6 ルーティング情報をフィルタ処理するために使用されます。

例

次に、指定したプレフィックス1つのみを許可するアクセスリストの例を示します。アクセスリストのステートメントに一致しない IPv6 アドレスは拒否されます。

```
switchxxxxxx(config)# ipv6 access-list 1 permit 3001::2/64
```

注：その他すべてのアクセスは暗黙的に拒否されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。