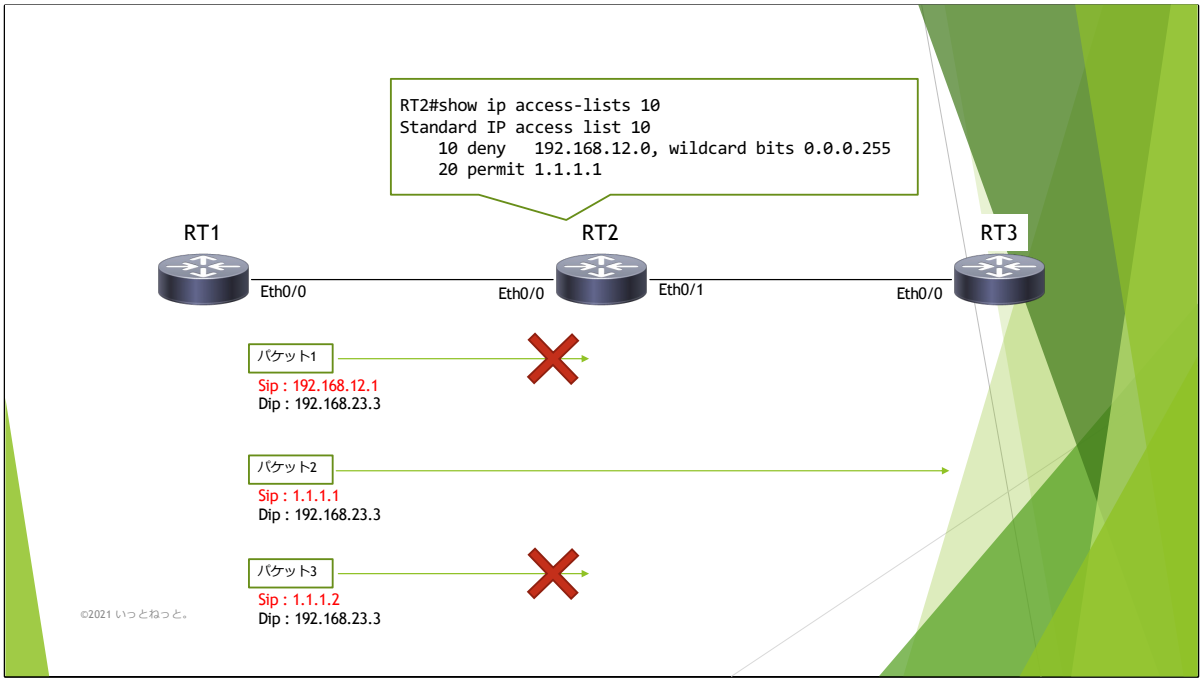
ACL の概要

Agenda

- ACL の概要
- ACL の種類
  - Numbered standard ACLs
  - Numbered extended ACLs
  - Named ACLs
  - Port ACLs
  - VLAN ACLs

ACL の概要



ACL (Access Constrol Lists) は 通信をフィルタしたり分類するために使用されるリストである。

ACE (Access Controls Entries) という Entry から構成されており、 permit と deny で通信を分類する。
シーケンス番号が若い順に評価されていき、何かの Entry に match した時点でそれ以降の Entry は参照されない。

また、どの Entry にも match しない場合は deny として扱われる。

この例では RT2 に 「ACL 10」 が定義されており、以下の ACE が存在する。
シーケンス番号10 : Source IP 192.168.12.0/24 の通信を破棄
シーケンス番号20 : Source IP 1.1.1.1/32 の通信を許可

これが Eth0/0 に inbound で適用されているため、この I/F で受信したパケットがどの Entry に match するか check される。
パケット1 はシーケンス番号10 に match するため破棄され、パケット2 はシーケンス番号20 に match するため許可される。

また、パケット3 はどれにも該当しないため deny として扱われ破棄される。

ACL の種類

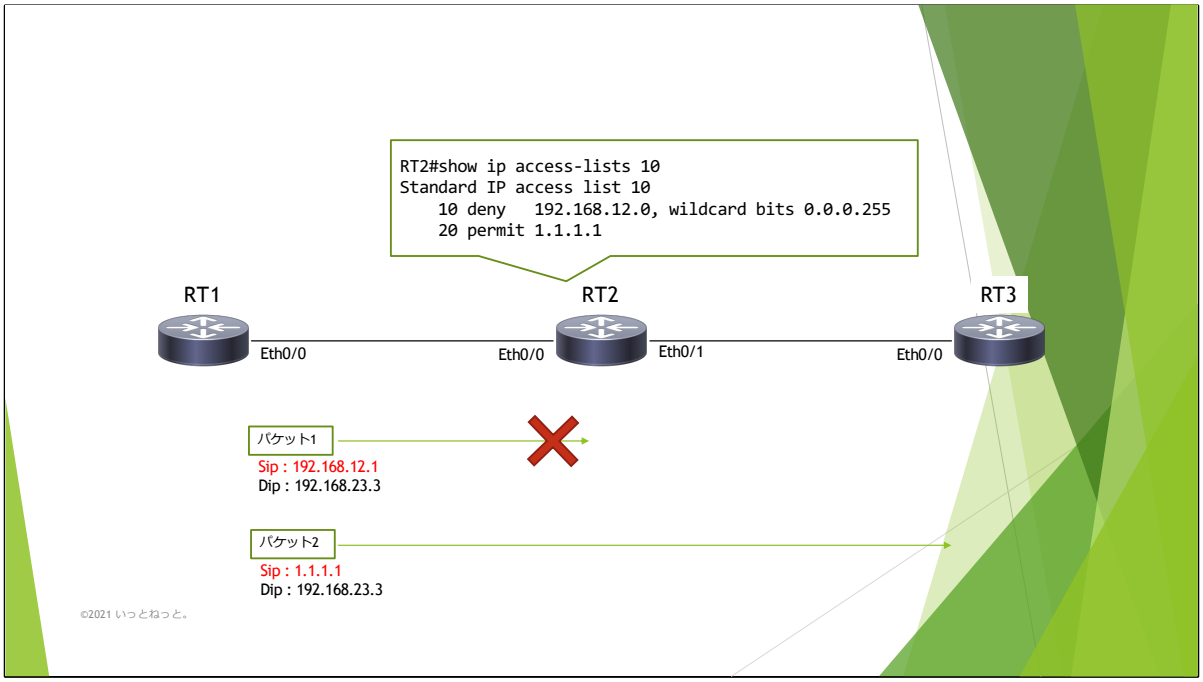
ACL の種類	説明	例
Numbered standard ACLs	Source Network で分類する ACL 。 1-99 と 1300-1999 番で定義する。	RT1(config)#ip access-list standard 10 RT1(config-std-nacl)#10 deny 192.168.1.0 0.0.0.255 RT1(config-std-nacl)#20 permit host 1.1.1.1
Numbered exnteded ACLs	以下要素の組み合わせから分類する ACL。 100-199 と 2000-2699 番で定義する。 ・Protocol ・Source / Destination Network ・Source / Destination Port	RT1(config)#ip access-list extended 100 RT1(config-ext-nacl)#10 deny tcp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 eq 80 RT1(config-ext-nacl)#20 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Named ACLs	動作は Numbered ACL と同じだが、番号ではなく名前で ACL を定義する。 名前をつけることで用途もわかりやすくなるため、一般的に使用されている。	RT1(config)#ip access-list standard TEST1 RT1(config-std-nacl)#10 deny 192.168.1.0 0.0.0.255 RT1(config-std-nacl)#20 permit host 1.1.1.1 ! RT1(config)#ip access-list extended TEST2 RT1(config-ext-nacl)#10 deny tcp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 eq 80 RT1(config-ext-nacl)#20 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Port ACLs (PACLs)	Switchport (Layer2 port) に適用された ACL。 Numbered / Named/ MAC ACL のいずれか 1つをinbound 方向に適用できる。	準備中
VLAN ACLs (VACLs)	VLAN に適用された ACL。 Numbered / Named / MAC ACL から定義し、inbound 方向に適用する。	準備中

ACL には様々な種類が存在する。
それぞれの概要は記載の通り。

ACL は I/F や VLAN などに適用することで、 permit に該当する通信を許可、 deny に該当する通信を破棄といったパケットフィルタリングに使用される。
また、 Numbered ACL や Named ACL は QoS や NAT といった他機能で、どの通信をその機能で使用するかといった分類にも使用されている。

今回は各 ACL をパケットフィルタリングの観点で紹介していく。

ACL の種類
～Numbered standard ACLs～

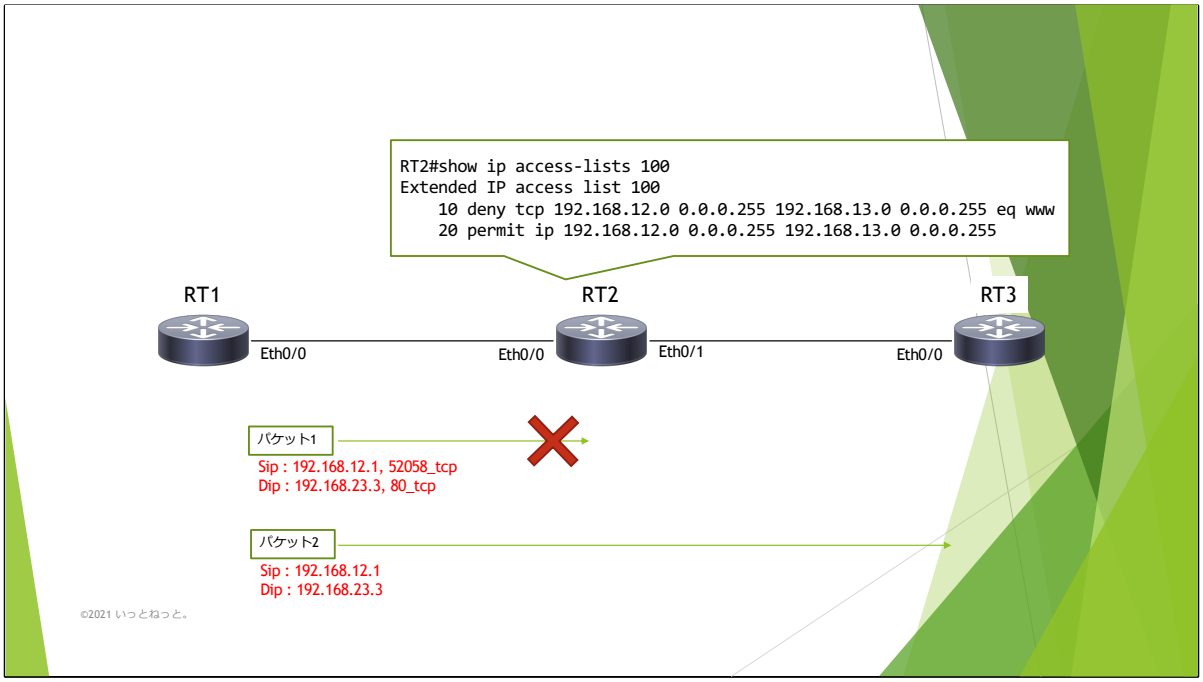


ACL の概要で紹介した通り、 Numbered standard ACLs は Source IP address に基づき通信を分類する。

この例では RT2 に 「ACL 1」 が定義されており、以下の ACE が存在する。
シーケンス番号10 : Source IP 192.168.12.0/24 の通信を破棄
シーケンス番号20 : Source IP 1.1.1.1/32 の通信を許可

これが Eth0/0 に inbound で適用されているため、この I/F で受信したパケットがどの Entry に match するか check される。
パケット1 はシーケンス番号10 に match するため許可され、パケット2 はどれにも該当しないため deny として扱われ破棄される。

ACL の種類
～Numbered extended ACLs～

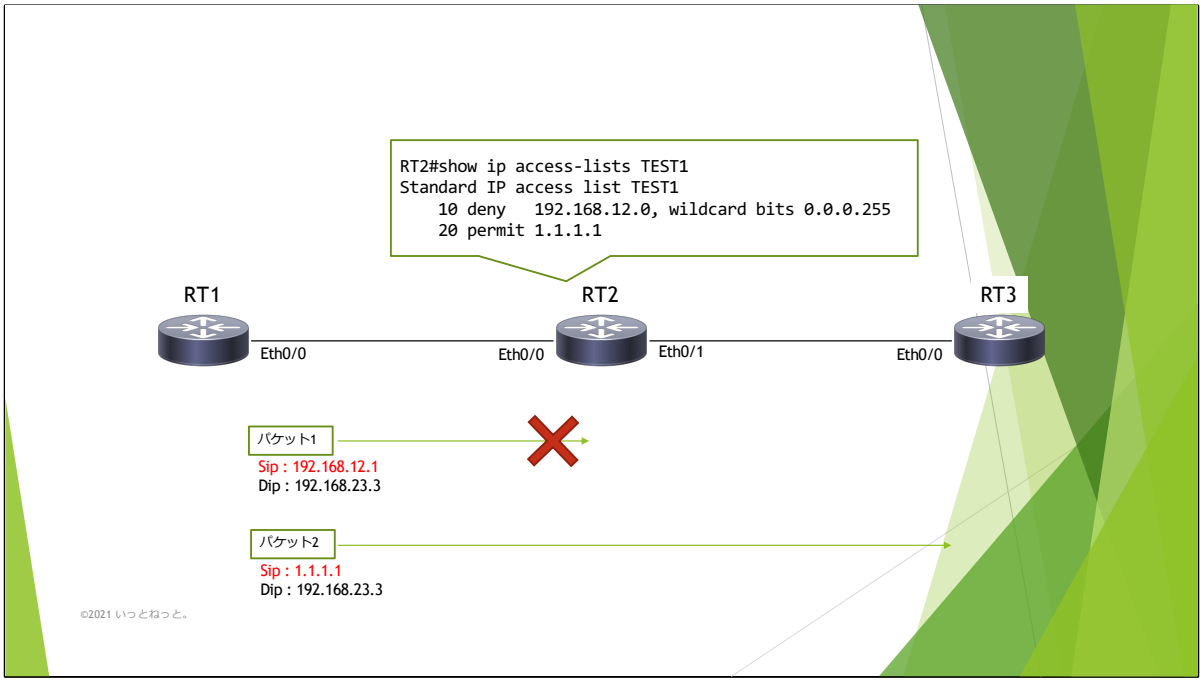


Numbered extended ACLs は 以下の様々な要素の組み合わせから通信を分類する。
・Protocol
・Source / Destination Network
・Source / Destination Port

この例では RT2 に 「ACL 100」 が定義されており、以下の ACE が存在する。
シーケンス番号10 : TCP protocol で Source IP 192.168.12.0/24 から Destination IP 192.168.13.0/24 の 80_tcp (www) 宛通信を破棄
シーケンス番号20 : すべての IP protocol で Source IP 192.168.12.0/24 から Destination IP 192.168.13.0/24 の通信を許可

これが Eth0/0 に　inbound で適用されているため、この I/F で受信したパケットがどの Entry に match するか check される。
パケット1 はシーケンス番号10 に match するため破棄され、パケット2 はシーケンス番号20 に match するため許可される。

ACL の種類
～Named ACLs～

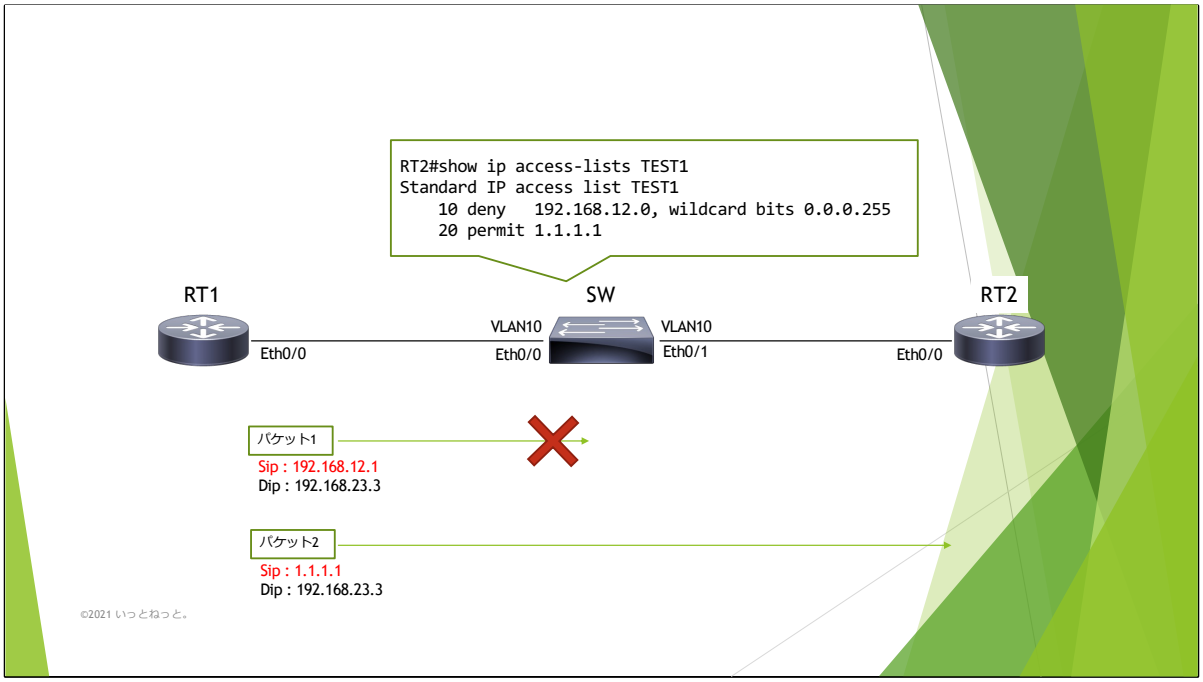


Named ACLs は Numbered ACLs と同様の動作だが、ACL を番号ではなく名前をつけて定義する。
そのため、定義された ACL が何のための ACL かわかりやすく、一般的に ACL を設定する際は Numbered ACLs ではなく Named ACLs を採用することが多い。

この例では RT2 に 「ACL TEST1」 が定義されており、以下の ACE が存在する。
シーケンス番号10 : Source IP 192.168.12.0/24 の通信を破棄
シーケンス番号20 : Source IP 1.1.1.1/32 の通信を許可

これが Eth0/0 に　inbound で適用されているため、この I/F で受信したパケットがどの Entry に match するか check される。
パケット1 はシーケンス番号10 に match するため許可され、パケット2 はどれにも該当しないため deny として扱われ破棄される。

ACL の種類
～Port ACLs～

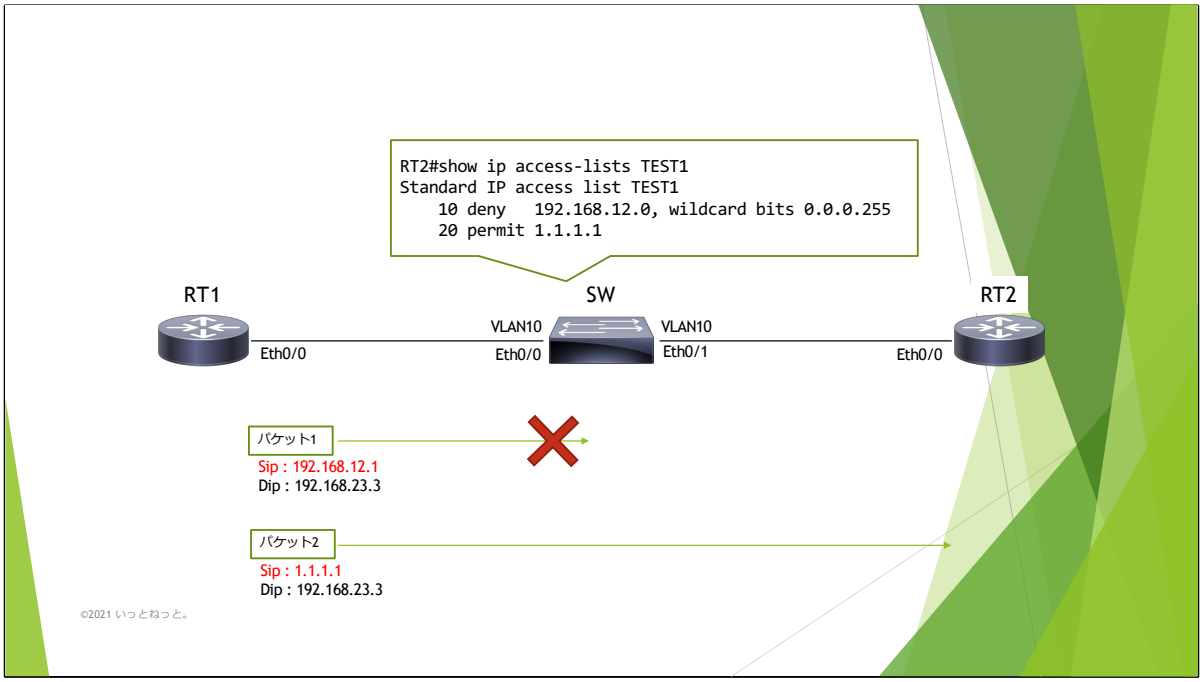


Port ACLs は Router ではなく Switch の Switchport (Layer2 port) に適用する ACL である。
以下種類の ACL のいずれかを inbound 方向に適用し、通信を制御する。

・Numbered ACL
・Named ACL
・MAC ACL

また、 Port ACLs には以下の制約事項が存在する。
(1) Inbound 方向にしか適用できない
(2) CDP, VTP, DTP, PAgP, UDLD, STP といった Layer2 Control packets は
　フィルタできない
(3) Hardware でのみサポートされる
(4) IPv6, ARP, MPLS (Multi Protocol Label Switching) をフィルタするための
　ACL はサポートしない

ACL の種類
～VLAN ACLs～



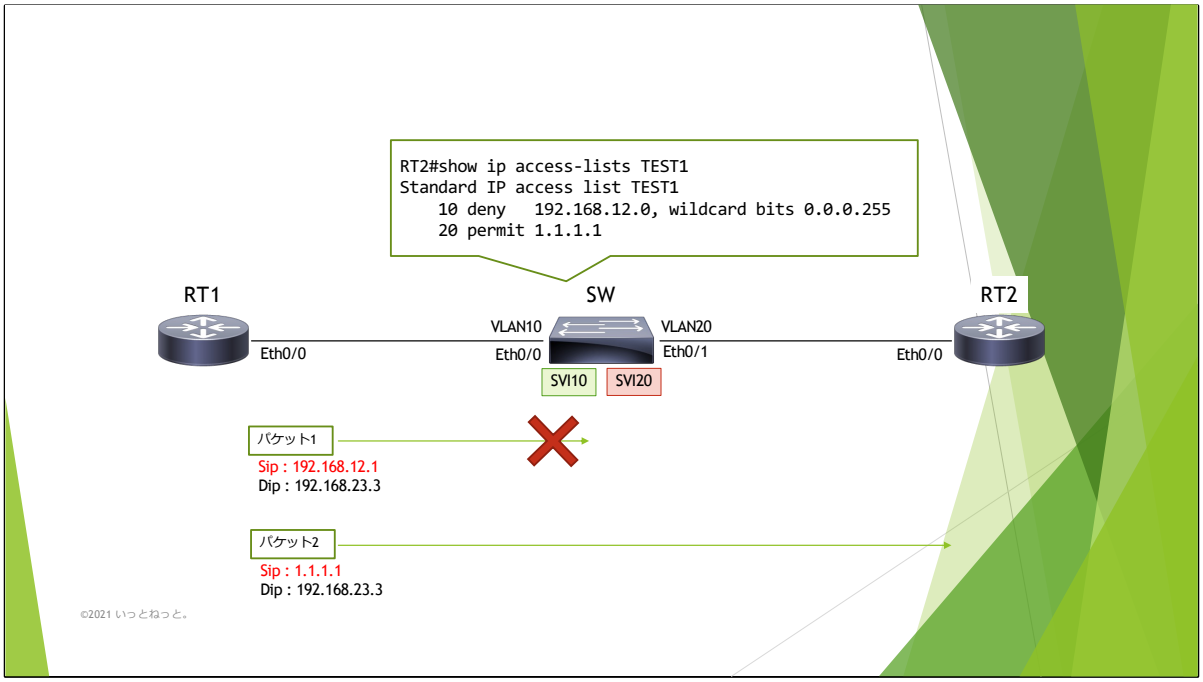
VLAN ACLs は Router ではなく Switch の VLAN に適用する　ACL である。
以下種類の ACL のいずれかを inbound 方向に適用し、通信を制御する。

・Numbered ACL
・Named ACL
・MAC ACL

VLAN ACLs では、同一 VLAN が割り当てられた I/F 間の通信や、 SVI (Switched Virtual Interface) を介した VLAN 間 Routing を制御する。

この例では、 SW1に 「ACL TEST1」 が適用されており、以下のように制御されている。
・
・

これが VLAN10 に適用されているため、 VLAN10 がアサインされた I/F でフレームを受信した際に、 VACLs に基づき制御される。
フレーム1 はシーケンス番号10 に match するため転送され、フレーム2 はシーケンス番号20 に match するため drop として扱われ破棄される。



次の例では、 SW1に 「ACL TEST1」 が適用されており、以下のように制御されている。

・

・

これが VLAN20 に適用されているため、SVI10 から SVI20 に VLAN 間 Routing され、VLAN20 として処理される際に VACLs に基づき制御される。フレーム1 はシーケンス番号10 に match するため転送され、フレーム2 はシーケンス番号20 に match するため drop として扱われ破棄される。

また…