Configuring IPv6 PACL

This chapter describes how to configure the IPv6 Port based Access Control List (PACL).

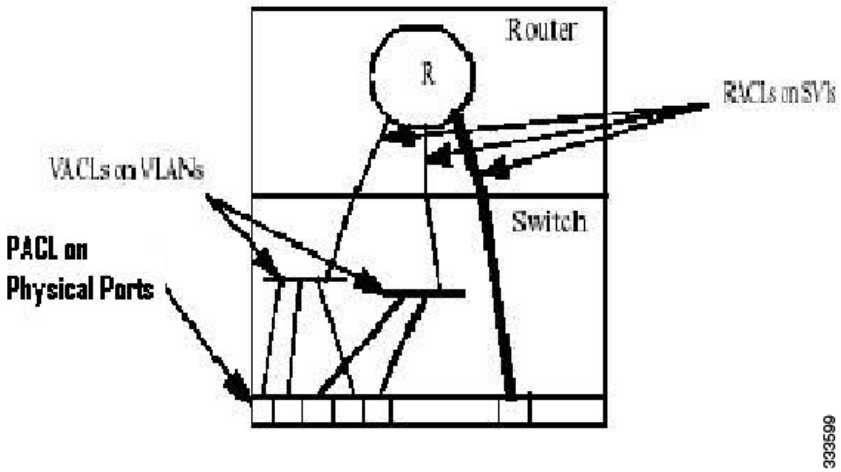
This chapter includes the following sections:

Understanding IPv6 PACL

The c7600 has mechanisms to apply Access Control Lists (ACLs) at various levels such as Router, VLAN, and Port level. Router Access Control Lists (RACLs) are applied on a Switch Virtual Interface (SVI) or physical interface to filter out the layer 3 traffic. VLAN Access Control Lists (VACLs) are configured on VLANs, and are applicable on the layer 2 and the layer 3 packets passing through the VLAN.

PACLs help filter the incoming Layer 3 packets based on layer 2 and layer 4 parameters at the layer 2 switchports.

Figure 40-1 PACL on Physical Ports



Restrictions for IPv6 PACL feature

Following restrictions apply to the IPv6 PACL feature:

- IPv6 PACL is not supported in the IOS software path.
- IPv6 PACL is not supported in the egress direction.
- IPv6 PACL logging is not supported.
- IPv6 PACL does not support routing header match and Differentiated Services Code Point (DSCP) ACL match as these features do not have hardware support.
- IPv6 supports fragment keyword and layer 4 information.
- IPv6 PACL supports time-based ACLs.
- When you configure the **platform ipv6 acl icmp optimize neighbor-discovery** command, a global Internet Control Message Protocol (ICMP) Neighbor Discovery (ND) Value Mask Result (VMR) is appended at the top of the Ternary Content-Addressable Memory (TCAM). This ICMP entry overrides the applicable PACL configured on the interface.
- IPv6 PACL is supported on the layer 2 etherchannel, but not on its member ports.
- IPv6 PACL is supported on the trunk ports only in the port prefer mode.
- IPv6 PACL does not support the **access-list log** and **reflect/evaluate** keywords. These keywords are ignored if you add them to the access list for a PACL.
- Due to the limited size of the flow key in the TCAM, IPv6 addresses along with the layer 4 port information cannot be accommodated unless the IPv6 addresses are compressed. Use the **mls ipv6 acl compress address unicast** command to compress the IPv6 address. You cannot apply the IPv6 PACL to non-compressible addresses, if the filtering is based on layer 4 ports.

Configuring IPv6 PACL

The following sections describe how to configure IPv6 PACL on c7600:

- Creating Access List, page 40-2
- Configuring PACL mode and Applying IPv6 PACL, page 40-4

Creating Access List

Complete the following steps to create an access list:

SUMMARY STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **ipv6 access-list** *access-list-name*

Step 4 **{permit | deny} {protocol/ IPv6 source prefix}** *source [source-ipv6-address] destination [destination-ipv6-address]*

Step 5 **end**

ETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Router(config)# ipv6 access-list list1`	Defines an IPv6 ACL, and enters the IPv6 access list configuration mode. • *access-list name*: Specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.
Step 4	**{permit | deny} {protocol/ IPv6 source prefix}** *source [source-ipv6-address] destination [destination-ipv6-address]* **Example:** `Router(config-ipv6-acl)# permit tcp 1000::1/64 any`	Specifies permit or deny conditions for an IPv6 ACL. • **permit | deny**: Determines whether the specified traffic is blocked or allowed to pass. • **protocol / IPv6 source prefix**: Specifies any source ipv6 prefix, protocol (IPv6 ,ICMP ,tcp ,udp) or a number between 0 and 254. • *source:* Specifies the source of the traffic. • *destination:* Specifies the destination of the traffic. • *source-ipv6-address:* Specifies the source IPv6 address. • *destination-ipv6-address:* Specifies the destination IPv6 address. **Note** The source or destination can be an IPv6 prefix, in the format *prefix/length,* to indicate a range of addresses, the keyword **any** to specify any address, or a specific host designated by **host** *host_ipv6_addr.*
Step 5	**end** **Example:** `Router(config-ipv6-acl)# end`	Ends the current configuration session.

Configuration Example

This example shows how to create an IPv6 ACL:

```
Router# enable
Router# configure terminal
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit tcp 1000::1/64 any
Router(config-ipv6-acl)# end
```

Configuring PACL mode and Applying IPv6 PACL

Complete the following steps to configure the PACL mode, and apply IPv6 PACL on a switchport interface:

SUMMARY STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **interface** *type number*

Step 4 **switchport**

Step 5 **switchport mode {access | trunk}**

Step 6 **switchport access vlan** *vlan-id* **[or] switchport trunk allowed vlan** *vlan-list*

Step 7 **access-group mode {prefer {port | vlan} | merge}**

Step 8 **ipv6 traffic-filter** *access-list-name* **in**

Step 9 **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 3/24`	Configures an interface, and enters the interface configuration mode.
Step 4	**switchport** **Example:** `Router(config-if)# switchport`	Moves the interface into Layer 2 mode.
Step 5	**switchport mode {access | trunk}** **Example:** `Router(config-if)# switchport mode access`	Sets the interface type.
Step 6	**switchport access vlan** *vlan-id* **[or]** **switchport trunk allowed vlan** *vlan-list* **Example:** `Router(config-if)# switchport access vlan 1000` or `Router(config-if)# switchport trunk allowed vlan 1000, 2000`	Sets the VLAN when an interface is in access mode. or Sets the list of allowed VLANs when in trunk mode.
Step 7	**access-group mode {prefer {port | vlan} | merge}** **Example:** `Router(config-if)# access-group mode prefer port`	Sets the mode for the switchport interface. **Note** IPv6 PACL is applied on the trunk port only if the access-group mode on the trunk port is set to prefer port. On access ports, if the access-group mode is set to prefer port, then the features between the SVI and the switchport do not merge.

	Command or Action	Purpose
Step 8	**ipv6 traffic-filter** *access-list-name* **in** **Example:** `Router(config-if)# ipv6 traffic-filter list1 in`	Filters the incoming IPv6 traffic on a switchport interface.
Step 9	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session.

Configuration Example

This example shows how to configure a PACL mode and apply an IPv6 PACL on a switchport interface:

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/24
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 1000
Router(config-if)# access-group mode prefer port
Router(config-if)# ipv6 traffic-filter list1 in
Router(config-if)# end
```

Verifying IPv6 PACL

Use these commands to verify the configuration of IPv6 PACL on c7600:

- The **show ipv6 access-list** command displays the details of all the IPv6 access lists created.

```
Router# show ipv6 access-list

   IPv6 access list PACL
       permit ipv6 host 2001:410:1:0:200:FF:FE00:1 host 2001:410:2:0:200:FF:FE00:1
   sequence 10
       deny ipv6 host 2001:410:1:0:200:FF:FE00:2 host 2001:410:2:0:200:FF:FE00:2 sequence
   20
       permit ipv6 host 2001:410:1::3 host 2001:410:2::3 sequence 30
```

- The **show run interface GigabitEthernet** command displays the IOS interface configuration.

```
Router# show run interface GigabitEthernet 7/0/1

   Current configuration : 179 bytes
   !
   interface GigabitEthernet7/0/1
    switchport
    switchport access vlan 10
    switchport mode access
   ipv6 traffic-filter PACL in
   end
```

- The **show tcam interface GigabitEthernet acl in ipv6** command displays the following output when the IPv6 PACL is configured on an interface.

```
Router# show  tcam interface GigabitEthernet 7/0/1 acl in ipv6
```

```
* Global Defaults shared
-----------------------------------------------------
ICMP Neighbor Discovery Packet Types:
na - neighbor advertisement  ra - router advertisement
ns - neighbor solicit        rs - router solicit
r  - redirect

IPV6 Address Types:
full - IPv6 Full             eui - IPv6 EUI
eipv4 - IPv6 embeded IPv4
-----------------------------------------------------
    permit       ipv6 host 0:2001:410:1:0:200:0:1(eui) host
0:2001:410:2:0:200:0:1(eui)
    deny         ipv6 host 0:2001:410:1:0:200:0:2(eui) host
0:2001:410:2:0:200:0:2(eui)
    permit       ipv6 host 2001:410:1::3(full) host 2001:410:2::3(full)
    permit       icmp(nd-ra) any(eui) any
    permit       icmp(nd-na) any(eui) any
    permit       icmp(nd-rs) any(eui) any
    permit       icmp(nd-ra) any(full) any
    permit       icmp(nd-na) any(full) any
    permit       icmp(nd-rs) any(full) any
    deny         ipv6 any(eipv4) any
    deny         ipv6 any(eui) any
    deny         ipv6 any(full) any
```

- The **show fm interface FastEthernet** command displays all the features configured on a specific interface including the PACLs.

```
Router# show fm interface FastEthernet 2/1
    Interface: FastEthernet2/1 IP is disabled
      hw_state[INGRESS] = not reduced, hw_state[EGRESS] = not reduced
      mcast = 0
      priority = 0
      flags = 0x0
      parent[INGRESS] = none
      inbound label: 65
        Feature IPV6_PACL:
            ACL: test
    ------------------------------------------------------------------------------
     FM_FEATURE_IPV6_PACL - PACL Name: test          Direction:Ingress
    ==============================================================================
    DPort  - Destination Port  SPort  - Source Port       Pro    - Protocol
    PT     - Packet Type       DPT    - Dst. Packet Type  SPT    - Src. Packet Type
    X      - XTAG              TOS    - TOS Value         Res    - VMR Result
    RFM    - R-Recirc. Flag    MRTNPC - M-Multicast Flag  R      - Reflexive flag
           - F-Fragment flag          - T-Tcp Control     N      - Non-cachable
           - M-More Fragments         - P-Mask Priority(H-High, L-Low)
    Adj.   - Adj. Index        C      - Capture Flag      T      - M(Mask)/V(Value)
    FM     - Flow Mask         NULL   - Null FM           SAO    - Source Only FM
    DAO    - Dest. Only FM     SADA   - Sour.& Dest. Only VSADA  - Vlan SADA Only
    ISADA  - Intf. SADA        FF     - Full Flow         VFF    - Vlan Full Flow
    IFF    - Intf. FF          F-VFF  - Either FF or VFF  IFF-FF - Either IFF or FF
    A-VSD  - Atleast VSADA     A-FF   - Atleast FF        A-VFF  - Atleast VFF
    A-SON  - Atleast SAO       A-DON  - Atleast DAO       A-SD   - Atleast SADA
    SHORT  - Shortest          ISADA-L- ISADA Least       FF-L   - FF Least
    IFF-L  - IFF Least         A-SFF  - Any short than FF A-EFF  - Any except FF
    A-EVFF - Any except VFF    SA-L   - Source Least      DA-L   - Dest. Least
    SADA-L - SADA Least        FF-LESS- FF Less           N-FF   - Not FF
    N-IFF  - Not IFF           A-LVFF - Any less than VFF FULL   - Full Pkt Type
    EUI    - EUI 64 Pkt Type   EMBD   - Embedded Pkt Type ELNK   - EUI Link Overlap
    ESIT   - EUI Site Overlap  LINK   - Link Pkt Type     SITE   - Site Pkt Type
    ERR    - Flowmask Error
```

```
+----+-+--------------------------------------+---------------------+----+----+----+---+---+-+------+----+------+
|Indx|T|    Dest IPv6 Addr                    |    Source IPv6 Addr  | DPT| SPT| PT |Pro|RFM|X|MRTNPC|Adj.|
FM  |
+----+-+--------------------------------------+---------------------+----+----+----+---+---+-+------+----+------+

 1    V                                   14::                   2:: FULL FULL ----   0 --- - ----L- ---- SHORT
      M                     FFFF:FFFF:FFFF:FFFF::  FFFF:FFFF:FFFF:FFFF:: EMBD EMBD        0   0
      TM_PERMIT_RESULT

 2    V                                  15::1                    :: FULL  EUI ----   0 --- - ----L- ---- SHORT
      M  FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF                    :: EMBD  EUI        0   0
      TM_PERMIT_RESULT

 3    V                                  15::1                    :: FULL FULL ----   0 --- - ----L- ---- SHORT
      M  FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF                    :: EMBD EMBD        0   0
      TM_PERMIT_RESULT

 4    V                                     ::                    :: ----  EUI ----  58 --- - ----L- ---- SHORT
      M                                     ::                    :: ----  EUI      255   0
      TM_PERMIT_RESULT

 5    V                                     ::                    :: ---- FULL ----  58 --- - ----L- ---- SHORT
      M                                     ::                    :: ---- EMBD      255   0
      TM_PERMIT_RESULT

 6    V                                     ::                    :: ----  EUI ----  58 --- - ----L- ---- SHORT
      M                                     ::                    :: ----  EUI      255   0
      TM_PERMIT_RESULT

 7    V                                     ::                    :: ---- FULL ----  58 --- - ----L- ---- SHORT
      M                                     ::                    :: ---- EMBD      255   0
      TM_PERMIT_RESULT

 8    V                                     ::                    :: ----  EUI ----  58 --- - ----L- ---- SHORT
      M                                     ::                    :: ----  EUI      255   0
      TM_PERMIT_RESULT

 9    V                                     ::                    :: ---- FULL ----  58 --- - ----L- ---- SHORT
      M                                     ::                    :: ---- EMBD      255   0
      TM_PERMIT_RESULT

 10   V                                     ::                    :: ---- ---- ----   0 --- - ----L- ---- SHORT
      M                                     ::                    :: ---- ----        0   0
```

Troubleshooting Tips

For troubleshooting information, contact Cisco Technical Assistance Center (TAC) at:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html