

How Are PowerConnect ACLs Different From Cisco ACLs?

This Application Notes relates to the following Dell PowerConnect products:

- PowerConnect 33xx

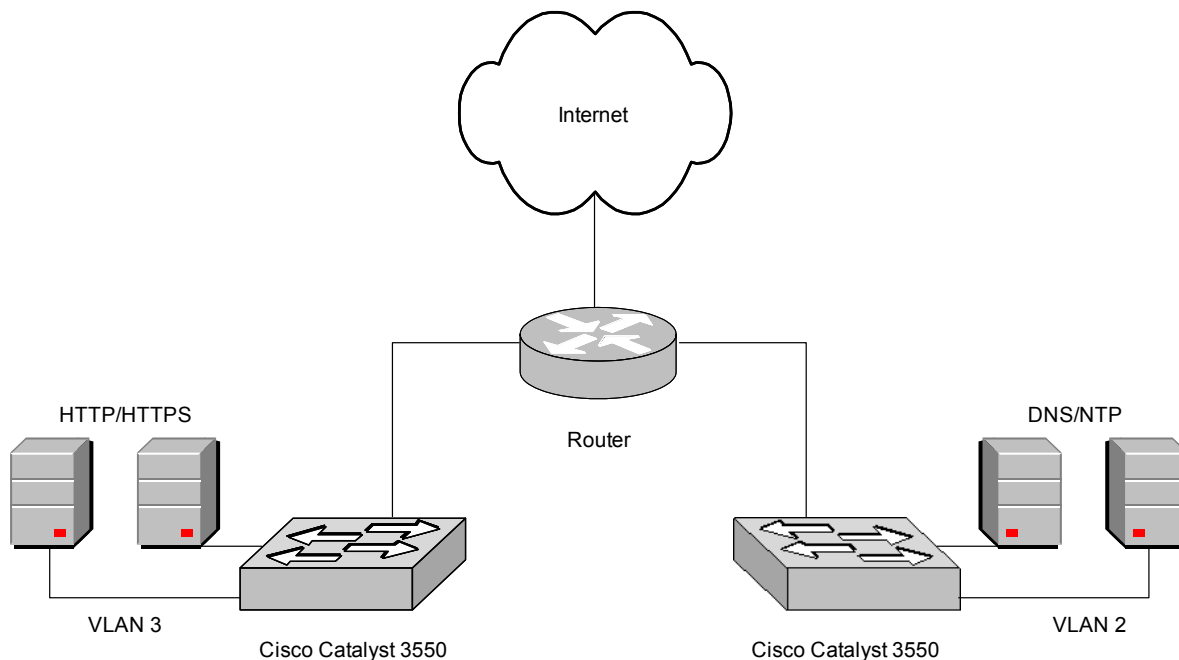
Abstract

This application note explains the differences between access control lists (ACLs) on Dell PowerConnect switches and those on Cisco Catalyst switches. This document will compare common ACL configurations from both platforms to aid network administrators in migrating filters from Cisco equipment to Dell PowerConnect switches.

Applicable Network Scenarios

As network devices are reallocated or replaced, porting key elements of network policy takes on critical importance. Security policies, for example, are essential to maintaining the integrity of a network and the data that flows through it. In particular, this may involve migrating ACLs from Cisco Catalyst switches to Dell PowerConnect switches.

The following diagram shows a switched network comprised of two segments bridged by two Cisco Catalyst 3550s. The Cisco Catalysts use ACLs to filter traffic on virtual local area networks (VLANs) 2 and 3. VLAN 2 provides DNS and NTP services for internal nodes. VLAN 3 provides both HTTP and HTTPS services to the Internet. If the enterprise replaces the two Cisco Catalysts with Dell PowerConnect switches, the ACLs must be migrated from one platform to the other.



Moving the ACLs to the Dell PowerConnect 33xx is a fairly simple process. However, the task requires a working knowledge of the differences in syntax between the Dell and Cisco ACLs.

Technology Background

Dell and Cisco ACLs are similar in most respects. Both Dell and Cisco switches process ACL rules in a sequential fashion. Both switches' ACLs include an implicit deny as the last rule of every set, meaning they drop any frame that does not match any of the rules in the ACL. Both switches allow ACLs to be applied to individual interfaces and/or VLANs. Despite all these similarities, there are enough differences in syntax to merit close inspection.

An ACL is made up of one or more specific filtering rules called access control entries (ACEs).

Cisco switches divide ACLs into two main groups, standard and extended, depending on the granularity required.

Dell ACLs fall into two main groups: Those that operate at layer 2 (data-link layer) of the seven-layer ISO stack, and those that filter traffic at layers 3 or 4 (the network and transport layers, respectively) of the ISO stack. Both groups of ACLs are initiated by a *permit* or *deny* declaration and can filter on such criteria as MAC address, VLAN ID, IP address, generic routing encapsulation (GRE), and open shortest path first. As a variation, network managers also can use the "disable-port" option with the "deny" action to disable the interface and trigger an SNMP trap notification. The switch will send a trap message after receiving traffic that matches the ACL.

At layer 4, ACLs provide filtering of UDP (*permit-udp* or *deny-udp*) and TCP (*permit-tcp* or *deny-tcp*) services.

Below are accepted parameters and respective examples for each Dell group:

Layer 2 ACLs:

permit {any | {host source source-wildcard} any | {destination destination-wildcard}}[vlan vlan-id]

Layer 3/4 ACLs:

permit {any | protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp dscp number | ip-precedence ip-precedence]

Layer 2 ACLs:

deny [disable-port] {any | {source source-wildcard} any | {destination destination-wildcard}} [vlan vlan-id]

Layer 3/4 ACLs:

deny [disable-port] {any | protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp dscp number | ip-precedence ip-precedence]

Examples:

```
deny 00:b0:d0:20:30:0f 00:00:00:00:00:00 any vlan 100
```

The above example discards all traffic sourced from 00:b0:d0:20:30:0f with any destination on VLAN 100.

```
permit any 192.168.0.0 0.0.255.255 any
```

The above example permits all traffic sourced from 192.168.0/16 to any destination network.

permit-tcp {any | source source-wildcard}} {any | source-port} {any | destination destination-wildcard}} {any | destination-port} [dscp dscp number | ip-precedence ip-precedence]

deny-tcp [disable-port] {any | protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp dscp number | ip-precedence ip-precedence]

Example: permit-tcp any any 192.168.0.0 0.0.0.255 80

The above example permits all HTTP traffic destined for 192.168.0/24. We know this example covers HTTP traffic because destination port 80 is a “well-known” port, meaning it has been designated for use by Web traffic. There is a complete list of well-known port numbers for both TCP and UDP traffic at <http://www.iana.org/assignments/port-numbers>.

permit-udp {any | {source source-mask}} {any | source-port} {any | {destination destination-mask}} {any|destination-port} [dscp dscp number | ip-precedence ip-precedence]

deny-udp [disable-port] {any| protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp dscp number | ip-precedence ip-precedence]

Example: permit-udp 172.16.0.25 0.0.0.0 any 192.168.0.12 0.0.0.0 53

The above example permits DNS traffic (UDP port 53) sourced from a single host, 172.16.0.25, to a single server at 192.168.0.12.

Applying ACLs is a similar process on Dell and Cisco switches. The *service-acl* command binds an ACL block to a Dell PowerConnect interface, link aggregation group (LAG), or VLAN.

Example:

```
console> en
console# config
console(config)# interface ethernet 1/e48
console(config-if)# service-acl input dmz-ingress
console# end
console# copy running-config startup-config
```

The above example enters the interface configuration context, applies an ACL named *dmz_ingress* to incoming traffic on interface 1/e48, exits configuration context, and saves the running configuration to the startup configuration.

To get a better idea of how frames are matched against sequential access control elements (ACEs), consider the following ACL:

```
IP access list sample
  permit ip 10.0.0.0 0.255.255.255 12.0.0.1 0.0.0.0
  permit any 192.168.0.0 0.0.255.255 any
  deny ip 10.0.0.0 0.255.255.255 any
  permit tcp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
```

The first ACE uses a “permit” rule. It allows IP traffic sourced from 10.0.0.0/8 to the host 12.0.0.1. The inverted netmasks consider 0s significant and 1s insignificant. Thus, an inverted netmask of 0.0.0.0 requires that the destination address match every octet, in this case 12.0.0.1.

The second ACE also uses a “permit” rule. It permits all traffic sourced from 192.168.0.0/16 (any protocol). Note the netmask of 0.0.255.255; since the first two octets are binary zeros, the first two octets of the IP address must match (in this case, 192.168.x.x).

The third ACE uses a “deny” rule. It discards any IP traffic sourced from 10.0.0.0/8. This, however, will not negate the first ACE since ACLs process ACEs in sequence and this ACE is lower in the list. Thus, the switch will discard any frame sourced from 10.0.0.0/8 and not destined for the host 12.0.0.1.

The fourth ACE uses a “permit-tcp” rule. It allows all TCP traffic sourced from 172.16.0.0/24, sourced from any port, and destined for 10.20.0.0/24 with a destination TCP port of 53 (DNS). This ACE will only allow TCP traffic to that specific TCP port; traffic sourced from 172.16.0.0/24 and destined for 10.20.0.0/24, but not destined for TCP port 53 will be discarded.

The end of this ACL is an invisible “implicit deny”. That means that any traffic not permitted via any of the previous ACEs is dropped by default. So the ACL really looks like:

```
IP access list sample
  permit ip 10.0.0.0 0.255.255.255 12.0.0.1 0.0.0.0
  permit any 192.168.0.0 0.0.255.255 any
  deny ip 10.0.0.0 0.255.255.255 any
  permit tcp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
  (deny any any any)
```

Remembering the implicit deny is a critical requirement when building ACLs. Failing to do so can have dire consequences, such as losing all access to an interface, VLAN, or switch.

Proposed Solution

Overview

To migrate ACLs from a Cisco Catalyst 3550 to a Dell PowerConnect 32xx switch, perform the following steps:

On the Cisco Catalyst 3550:

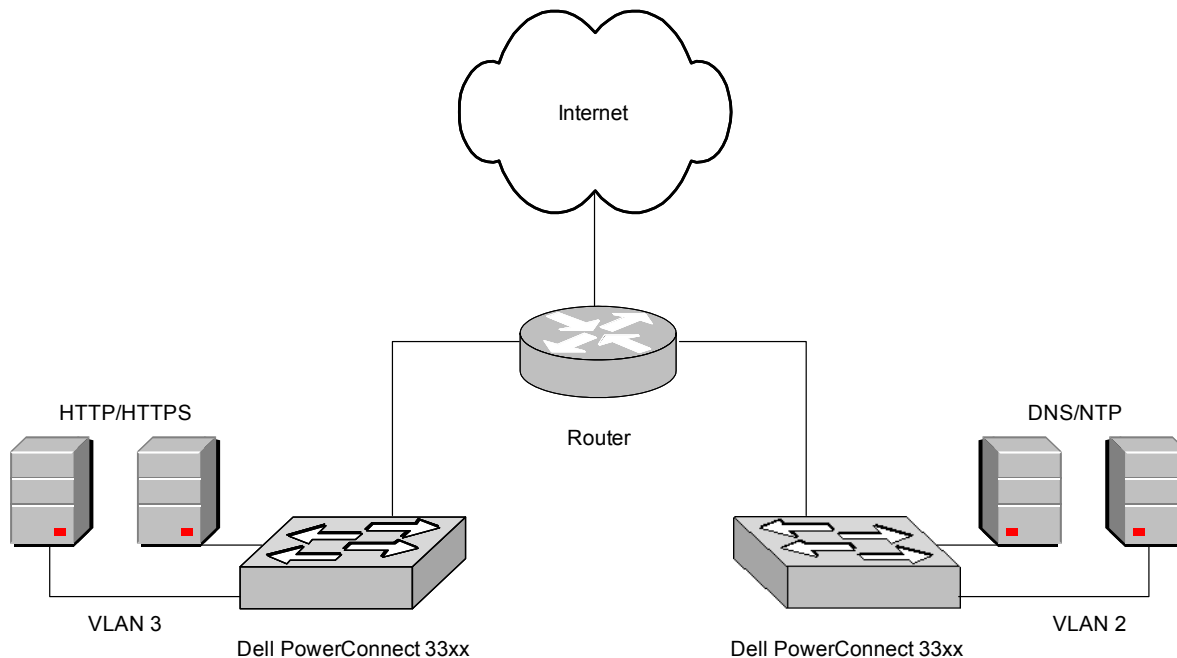
1. Gather necessary ACL configuration.

On Dell PowerConnect switches:

2. Translate Cisco ACLs into Dell PowerConnect ACEs
3. Configure ACLs and ACEs on Dell PowerConnect switches.
4. Assign ACLs to proper VLANs.

Typical Network Designs

We will juxtapose ACLs from the Cisco Catalyst 3550 and the Dell PowerConnect 33xx series to expose differences in syntax. After configuring ACLs on the Dell PowerConnect 33xx and binding them to the necessary interfaces, the Dell switch will provide the same level of security as the Cisco Catalyst did.



Step-By-Step Instructions

The following configuration guidelines work with any Dell PowerConnect 33xx switch. Note that all steps given below must be implemented on both PowerConnect 33xx switches.

The Cisco configuration guidelines work with any Cisco Catalyst switch.

1. Show ACLs on Cisco switch.

Catalyst 3550:

```
Catalyst_3550#show access-lists
Extended IP access list 110
  permit tcp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq domain
  permit tcp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq domain
  permit tcp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq domain
  permit udp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq domain
  permit udp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq domain
  permit udp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq domain
  permit tcp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123
  permit tcp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123
  permit tcp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123
  permit udp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq ntp
  permit udp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq ntp
  permit udp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq ntp
Extended IP access list 120
  permit tcp any 192.168.0.0 0.0.255.255 eq www
  permit tcp any 192.168.0.0 0.0.255.255 eq 443
```

2. Translate Cisco ACLs into respective Dell Powerconnect ACEs (Access Control Elements).

Cisco ACL	Dell ACE
access-list 110 permit tcp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 53	permit-tcp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
access-list 110 permit tcp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 53	permit-tcp 192.168.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
access-list 110 permit tcp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 53	permit-tcp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
access-list 110 permit udp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 53	permit-udp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
access-list 110 permit udp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 53	permit-udp 192.168.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
access-list 110 permit udp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 53	permit-udp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 53
access-list 110 permit tcp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123	permit-tcp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 123
access-list 110 permit tcp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123	permit-tcp 192.168.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 123
access-list 110 permit tcp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123	permit-tcp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 123
access-list 110 permit udp 10.0.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123	permit-udp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 123
access-list 110 permit udp 192.168.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123	permit-udp 192.168.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 123
access-list 110 permit udp 172.16.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 123	permit-udp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255 123
access-list 120 permit tcp any 192.168.0.0 0.0.255.255 eq 80	permit-tcp any any 192.168.0.0 0.0.255.255 80
access-list 120 permit tcp any 192.168.0.0 0.0.255.255 eq 443	permit-tcp any any 192.168.0.0 0.0.255.255 443

3. Configure ACLs and ACEs on Dell PowerConnect switches.

PowerConnect 33xx:

```

console> enable
console# config
console(config)# ip access-list 110
console(config-ip-1)# permit-tcp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
53
console(config-ip-1)# permit-tcp 192.168.0.0 0.0.0.255 any 10.20.0.0
0.0.0.255 53
console(config-ip-1)# permit-tcp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
53
console(config-ip-1)# permit-udp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
53

```

```
console(config-ip-al)# permit-udp 192.168.0.0 0.0.0.255 any 10.20.0.0
0.0.0.255 53
console(config-ip-al)# permit-udp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
53
console(config-ip-al)# permit-tcp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
123
console(config-ip-al)# permit-tcp 192.168.0.0 0.0.0.255 any 10.20.0.0
0.0.0.255 123
console(config-ip-al)# permit-tcp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
123
console(config-ip-al)# permit-udp 10.0.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
123
console(config-ip-al)# permit-udp 192.168.0.0 0.0.0.255 any 10.20.0.0
0.0.0.255 123
console(config-ip-al)# permit-udp 172.16.0.0 0.0.0.255 any 10.20.0.0 0.0.0.255
123
console(config-ip-al)# exit
console(config)# ip access-list 120
console(config-ip-al)# permit-tcp any 192.168.0.0 0.0.255.255 80
console(config-ip-al)# permit-tcp any 192.168.0.0 0.0.255.255 443
console(config-ip-al)# exit
```

4. Apply built ACLs to respective VLANs

PowerConnect 33xx:

```
console(config)# int vlan 2
console(config-if)# service-acl input 110
console(config-if)# exit
console(config)# int vlan 3
console(config-if)# service-acl input 120
console(config-if)# exit
console(config)# int vlan 4
console(config-if)# service-acl input 130
console(config-if)# exit
console(config)# exit
console# copy running-config startup-config
console# exit
console>
```

Note: The above configuration can be duplicated on the second switch.

Conclusion

We have now migrated Cisco ACLs to PoweConnect 33xx switches with no interruption or change in access control policies.

Information in this document is subject to change without notice.

© 2003 Dell Computer Corporation. All rights reserved.

This Application Note is for informational purposes only, and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

Trademarks used in this text: Dell, the DELL logo, PowerConnect, PowerEdge, and PowerVault are trademarks of Dell Computer Corporation; Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.