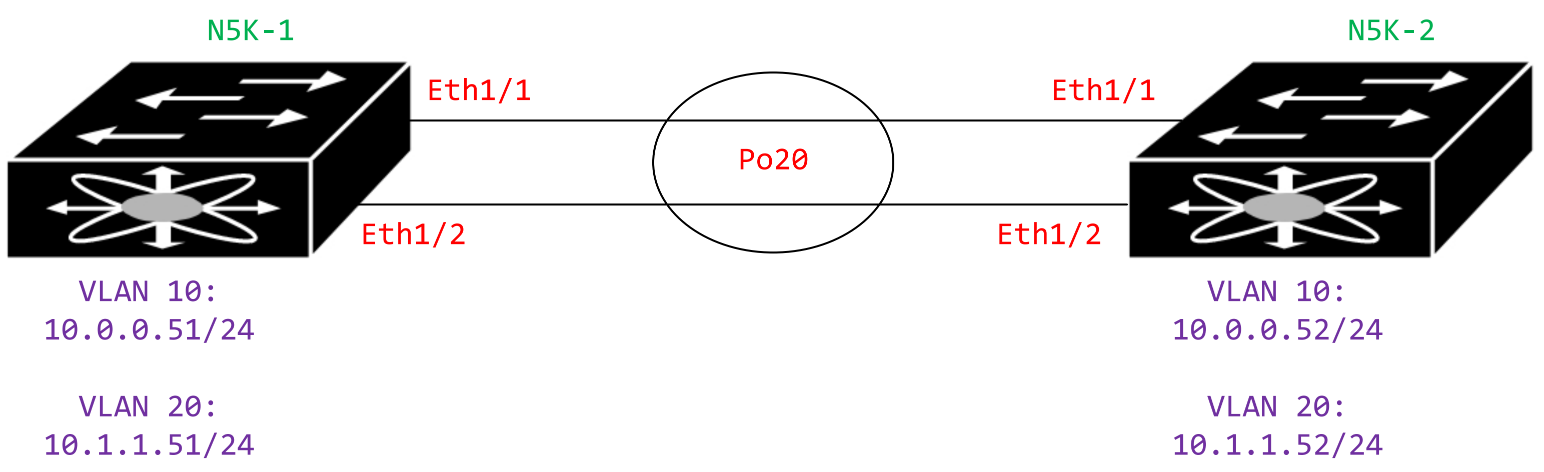

N5K-2 ACL Configuration:

```
N5K-2# show run aclmgr
<output omitted>

ip access-list DROP_ICMP
  10 deny icmp any any
  20 permit ip any any

interface port-channel20
  ip port access-group DROP_ICMP in
```

Result:

```
N5K-1# ping 10.0.0.52 source 10.0.0.51
PING 10.0.0.52 (10.0.0.52) from 10.0.0.51: 56 data bytes
Request 0 timed out
Request 1 timed out
^C
--- 10.0.0.52 ping statistics ---
3 packets transmitted, 0 packets received, 100.00% packet loss

N5K-1# ping 10.1.1.52 source 10.1.1.51
PING 10.1.1.52 (10.1.1.52) from 10.1.1.51: 56 data bytes
Request 0 timed out
Request 1 timed out
^C
--- 10.1.1.52 ping statistics ---
3 packets transmitted, 0 packets received, 100.00% packet loss
```

N5K-2 ACL Configuration:

```
N5K-2# show run aclmgr
<output omitted>

ip access-list DROP_ICMP
  20 permit ip any any
  30 deny icmp any any

vlan access-map DROP_ICMP_VLAN_10
  match ip address DROP_ICMP
  action drop
  statistics per-entry

vlan filter DROP_ICMP_VLAN_10 vlan-list 10
```

Result:

```
N5K-1# ping 10.0.0.52 source 10.0.0.51
PING 10.0.0.52 (10.0.0.52) from 10.0.0.51: 56 data bytes
Request 0 timed out
Request 1 timed out
^C
--- 10.0.0.52 ping statistics ---
3 packets transmitted, 0 packets received, 100.00% packet loss

N5K-1# ping 10.1.1.52 source 10.1.1.51
PING 10.1.1.52 (10.1.1.52) from 10.1.1.51: 56 data bytes
64 bytes from 10.1.1.52: icmp_seq=0 ttl=254 time=1.377 ms
64 bytes from 10.1.1.52: icmp_seq=1 ttl=254 time=0.967 ms
64 bytes from 10.1.1.52: icmp_seq=2 ttl=254 time=0.983 ms
64 bytes from 10.1.1.52: icmp_seq=3 ttl=254 time=0.962 ms
64 bytes from 10.1.1.52: icmp_seq=4 ttl=254 time=0.978 ms

--- 10.1.1.52 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.962/1.053/1.377 ms
```

N5K-2 ACL Configuration:

```
N5K-2# show run aclmgr
<output omitted>

ip access-list DROP_ICMP
  10 deny icmp any any
  20 permit ip any any

vlan access-map DROP_ICMP_VLAN_10
  match ip address DROP_ICMP
  action forward
  statistics per-entry

vlan filter DROP_ICMP_VLAN_10 vlan-list 10
```

Result:

```
N5K-1# ping 10.0.0.52 source 10.0.0.51
PING 10.0.0.52 (10.0.0.52) from 10.0.0.51: 56 data bytes
Request 0 timed out
Request 1 timed out
^C
--- 10.0.0.52 ping statistics ---
3 packets transmitted, 0 packets received, 100.00% packet loss

N5K-1# ping 10.1.1.52 source 10.1.1.51
PING 10.1.1.52 (10.1.1.52) from 10.1.1.51: 56 data bytes
64 bytes from 10.1.1.52: icmp_seq=0 ttl=254 time=1.342 ms
64 bytes from 10.1.1.52: icmp_seq=1 ttl=254 time=1.009 ms
64 bytes from 10.1.1.52: icmp_seq=2 ttl=254 time=0.998 ms
64 bytes from 10.1.1.52: icmp_seq=3 ttl=254 time=0.981 ms
64 bytes from 10.1.1.52: icmp_seq=4 ttl=254 time=0.982 ms

--- 10.1.1.52 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.981/1.062/1.342 ms
```

The above configurations imply:

If the 1st rule in the ACL, that is matched in the VACL, is a permit rule, then the VACL configuration (drop or forward action) matters.

If the 1st rule in the ACL, that is matched in the VACL, is a deny rule, then the VACL configuration (drop or forward action) does NOT matter, as traffic for the VLAN will STILL be dropped.

©Created by Matthew Rich, TCE, Cisco Systems, Inc.