ACL

Tags	
Klaar	JA
Week	Week 4 Week 5

ACL Operation

One ACL per protocol - To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.
One ACL per direction - ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.
One ACL per interface - ACLs control traffic for an interface, for example, GigabitEthernet 0/0.

Standard ACL vs Extended ACL

standard ACL = access-list nr 1-99

extended ACL = access-list nr 100-199

Standard ACLs filter packets based on the source address only.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Extended ACLs filter packets based on:

- Protocol type / Protocol number (e.g., IP, ICMP, UDP, TCP, …)

- Source and destination IP addresses
- Source and Destination TCP and UDP ports

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

IPv6 ACL

With IPv6, there is only one type of ACL, which is equivalent to an IPv4 extended named ACL and there are no numbered ACLs in IPv6.

The command used to apply an IPv6 ACL to an interface is ipv6 traffic-filter command.

An IPv6 ACL adds two implicit permit statements at the end of each IPv6 access list.
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any statement

These two additional statements allow IPv6 ICMP Neighbor Discovery (ND) and Neighbor Solicitation (NS) messages to accomplish the same thing as IPv4 ARP.

ACL Placement

Extended ACLs should be located as close as possible to the source of the traffic to be filtered.
Denies undesirable traffic close to the source network without crossing the network infrastructure.

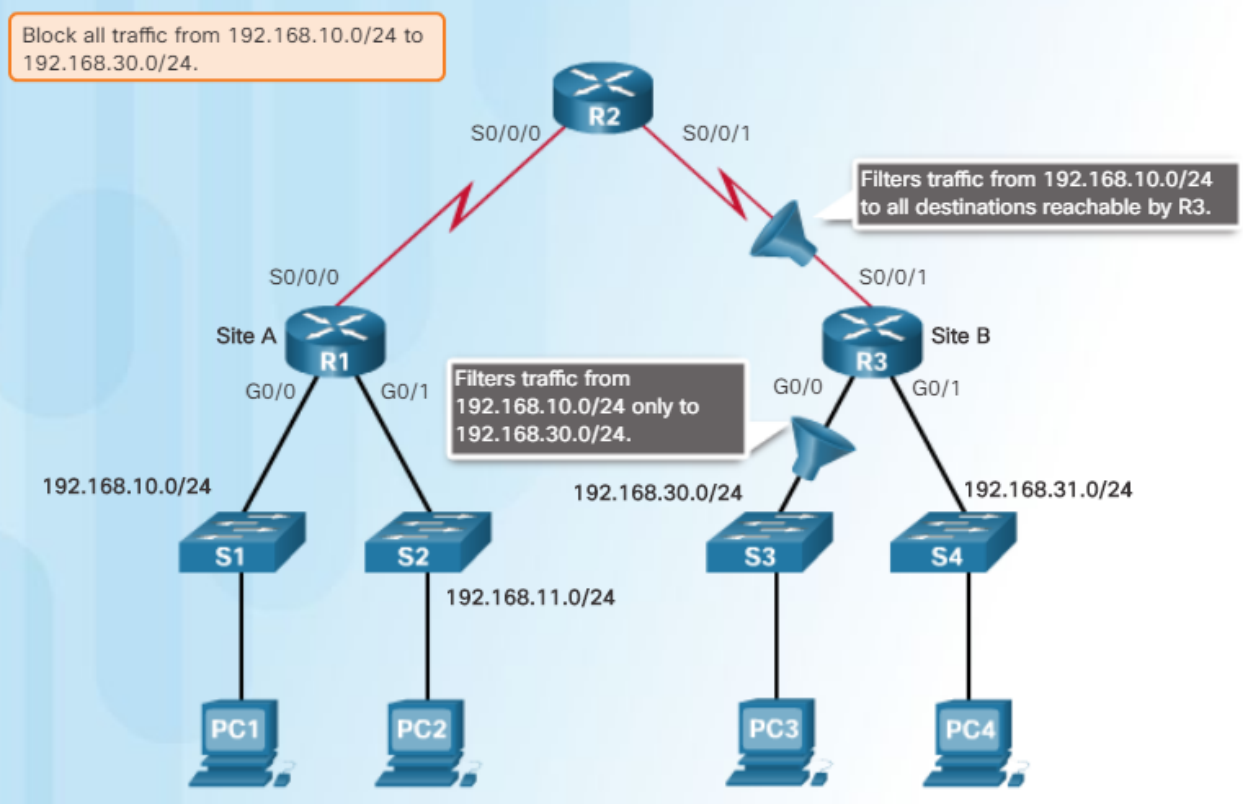
Standard ACLs should be located as close to the destination as possible.
If a standard ACL was placed at the source of the traffic, it would filter traffic based on the given source address no matter where the traffic is destined.

ACL Placement example

Standard ACL

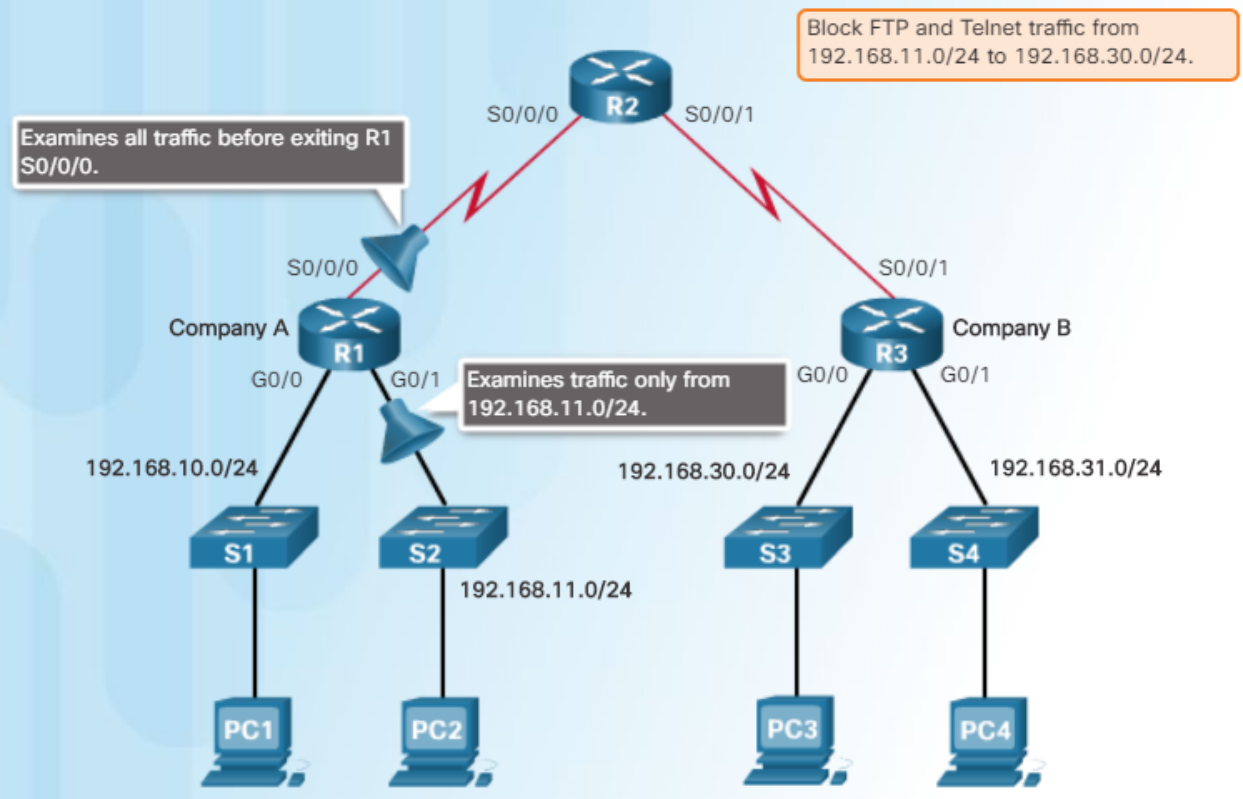
A standard ACL will be configured to block all traffic from 192.168.10.0/24 going to 192.168.30.0/24.

The standard ACL should be applied closest to the destination and therefore could be applied outgoing on the R3 G0/0 interface.
Applying it incoming on the R3 S0/0/1 interface would prevent reaching 192.168.31.0/24 and therefore should not be applied to this interface.



Extended ACL

An extended ACL will be configured to block all FTP and Telnet traffic from 192.168.11.0/24 going to 192.168.30.0/24.
The extended ACL should be applied closest to the source and therefore could be applied incoming on the R1 G0/1 interface.
Applying it outgoing on the R1 S0/0/1 interface would prevent reaching 192.168.31.0/24 but would also needlessly process packets from 192.168.10.0/24.



Named ACL example

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

Verifying Configuration

You can verify the ACL configuration with the following commands:

`show ip int xx`

`showo access-lists`