Access Control Lists

- An ACL identifies traffic based on characteristics of the packet such as source IP address, destination IP address, port number
- The router or switch can take an action based on the result of the ACL
- ACL's are supported on both routers and switches. I will refer to 'routers' throughout this section

Access Control Lists for Security

- The original use of ACLs was as a security feature to decide if traffic should be allowed to pass through the router
- By default a router will allow all traffic to pass between its interfaces
- When ACLs are applied the router identifies traffic and then decides if it will be allowed or not

Access Control Lists

- ACL's are also used in other software policies when traffic has to be identified, for example:
  - Identify traffic to give better service to in a QoS Quality of Service policy
  - Identify traffic to translate to a different IP address in a NAT Network Address Translation policy

ACE Access Control Entries

- Access Control Lists are made up of Access Control Entries which are a series of permit or deny rules
- Each ACE is written in a separate line

ACE Access Control Entry Example

R2(config)#

access-list 100 deny tcp 10.10.30.0 0.0.0.255 gt 49151 10.10.20.1 0.0.0.0 eq 23

			Source				Destination			
No.	Action	Protocol	IP	Wildcard	Qual.	Port	IP	Wildcard	Qual.	Port

Access Control List Example

```
R1(config)# access-list 100 deny tcp 10.10.10.10 0.0.0.0
gt 49151 10.10.50.10 0.0.0.0 eq 23
R1(config)# access-list 100 permit tcp 10.10.10.0
0.0.0.255 gt 49151 10.10.50.10 0.0.0.0 eq 23
R1(config)# access-list 100 deny tcp 10.10.20.10 0.0.0.0
gt 49151 10.10.50.10 0.0.0.0 eq 23
R1(config)# access-list 100 permit tcp 10.20.10.0
0.0.0.255 gt 49151 10.10.50.10 0.0.0.0 eq 23
```