**Networking 1B - ACL Syntax**

**Standard ACL**

Access-List <ACL# (1 to 99) > <PERMIT/DENY> <SOURCE IP ADDRESS> <SOURCE WILDCARD MASK>

Examples:

Access-List 10 Deny 201.100.11.122 0.0.0.0

Access-List 10 Deny 25.0.0.0 0.255.255.255

Access-List 10 Permit any

**Extended ACL – (Blocking by IP address only)**

Access-List <ACL# (100 to 199)> <PERMIT/DENY> IP <SOURCE IP > <SOURCE WILDCARD> <DEST IP > <DEST WILDCARD>

Access-List 106 Deny IP 1.2.3.4 0.0.0.0 205.7.5.0 0.0.0.255 (Blocks 1.2.3.4 from reaching the 205.7.5.0 network)

Access-List 106 Deny IP any 144.12.0.0 0.0.255.255 (Blocks everyone from reaching the 144.12.0.0 network)

Access-List 106 Permit IP any any (Opens up all remaining ports and IP addresses)

**Extended ACL – (Blocking by specific ports)**

Access-List <ACL# (100 to 199)> <PERMIT/DENY> TCP <SRC IP > <SRC WILD> <DEST IP > <DEST WILD> EQ <Port#>

Access-List 106 Deny tcp 1.2.3.4 0.0.0.0 205.7.5.0 0.0.0.255 eq 80 (Blocks 1.2.3.4 from 205.7.5.0 network via http)

Access-List 106 Deny tcp any 144.12.0.0 0.0.255.255 eq 23 (Blocks all from 144.12.0.0 network via telnet)

Access-List 106 Permit IP any any (Opens up all remaining ports and IP addresses)

**Applying ACLs**

Remember that the application of an ACL is done on a router interface. Choosing the correct router, interface and direction is the key to creating the proper filter.

Interface F0/0

Router(config-if)# IP ACCESS-GROUP <ACL #> <IN/OUT>

Example:

IP Access-group 106 In

IP Access-group 15 Out

**Removing an ACL from an Interface**

NO IP Access-Group <ACL#> <IN/OUT> No IP Access-group 106 IN

**Erasing an Access-List**

NO Access-List <ACL #> NO Access-List 106