Wildcard Masks

Rohith Perumalla | 4/9/17

This past week I've learned more about Access List wildcard masks and how to apply Access Lists to interfaces. Access Lists are a series of Access Control Entries, each indicating a permit or deny for a certain IP address or range. Each access control contains a permit or deny statement which is followed by an IP address and a wildcard mask. A wildcard mask is the identifier which tells the router which parts of the IP address to look for as a match or ignore. Each network address is broken down into binary by the router and then compared to the binary form of the wildcard mask. The router compares the address by checking to make sure that the incoming IP on the packet matches all the "0's" in the wildcard mask and ignores any "1's" in the mask. Any IP that matches all the 0's in a wildcard mask to the IP on the ACE is considered a match and then the permit or deny is applied to the packet. Access Lists are implemented on Router interfaces to increase the security of networks. They're applied on Cisco routers on physical interfaces by using the IOS command "access-group" followed by the access list number or name. On Cisco routers, access lists can also be applied on VTY lines using the "access-class" command on the IOS followed by the access list number or name. Using access lists on interfaces or VTY lines provides an extra layer of security. Overall I learned a lot more about Access Lists and how they function and how to use them.