**Notes**

Module 13

* Access Control Lists
  + Spot traffic or permit only specific traffic on networks
  + A sequential list of the permit or deny statements that apply to addresses or upper-layer protocols
* What is an ACL?
  + Series of IOS commands that control whether a router forwards or drops packets based on information found in the packet header
* When configured they perform these tasks:
  + Limit network traffic to increase network performance
  + Provide traffic flow control
    - Restrict the delivery of routing updates
      * If updates aren’t required because of network conditions, bandwidth is preserved
  + Provide a basic level of security for network access
    - Allow one host to access part of the network and prevent another
  + Filter traffic
  + Screen hosts to permit or deny access to network services.
* By default, a router doesn’t have ACLs configured
  + Doesn’t filter traffic
    - Traffic that entered is solely based on information within the routing table
* TCP Conversation
  + TCP Communication
    - Requests data, IP manages the communicator between the PC (source) and the server (destination). TCP manages the communications between the web browse an (application) and the network server software
  + TCP is responsible for breaking data down into segments
  + Provides a connection-oriented, reliable, byte stream service.
    - Connection-oriented = two applications must establish a TCP connection prior to exchanging data.
  + TCP is a full-duplex protocol
    - Each connection supports a pair of byte streams, each stream flowing in one direction
      * Includes a flow control mechanism for each byte (limit how much data the sender can transmit)
    - Implements a congestion-control mechanism
* Packet Filtering
  + Packet filtering(static packet filtering) controls access to a network by analyzing the incoming and outgoing packets and passing or dropping them based on given criteria
    - Source IP address
    - Destination IP addresses
    - Protocol carried within the packet
* A router acts as a packet filter
* Layer 4 = transport layer
* A router can filter packets based on the source port and destination port of the TCP or UDP segment. (Defined using ACLs)
* ACEs also called ACL. ACEs can be created to filter traffic based on certain criteria
  + Source address
  + Destination address
  + The protocol
  + Port numbers
* To evaluate network traffic, the ACL extracts the following info from the Layer 3 packet header:
  + Source IP address
  + Destination IP address
  + ICMP message type
* ACL also extracts upper layer info from Layer 4 header:
  + TCP/UDP source port
  + TCP/UDP destination port
* ACL Operation
  + Define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router.
  + ACLs configured to apply to inbound traffic or apply to outbound traffic
    - Inbound ACLS:
      * Incoming packets are processed before routed to the outbound interface. An inbound is efficient since it saves the overhead of routing loops if the packet is discarded.
      * Best used to filter packets when the network attached to an inbound interface is the only source of the packets
    - Outbound ACLs
      * Incoming packets are routed to the outbound interface. Processed through the outbound ACL
      * Bes used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface
  + The last statement of ACL is an implicit deny.
    - Statement automatically inserted at the end of each ACL
    - Implicit deny blocks all traffic
    - An ACL that doesn’t have one permit statement will block on traffic
* Types of Cisco IPv4 ACLs
  + Two types: Standard and extended
  + Standard
    - Used to permit or deny traffic only from source IPv4 addresses.
      * Destination of the pack/ports are not evaluated
      * Created in global config mode
  + Extended
    - Filter IPv4 packets based on:
      * Protocol type
      * Source IPv4 address
      * Destination IPv4 address
      * Source TCP or UDP ports
      * Destination TCP or UDP ports
      * Optional protocol type information for finer control
* Numbering and Naming ACLs
  + Usinger numbered is effective for determining ACL type on smaller networks
    - Does not provide information about the purpose of ACL
  + Numbers 200 to 1299 are off limits because they are used by other protocols (legacy or obsolete)
* Introducing ACL Wildcard Masking
  + IPv4 ACEs have wildcard masks
    - A string of 32 binary digits used by a router to determine which bits of the address to examine for a match
  + 1 and 0 identify how to treat corresponding IP address bits
  + Subnet = binary
    - Identify network, subnet, host of an IP
  + Wildcat uses binary
    - Filter individual IP addresses or groups of IP addresses to permit or deny access to resources
  + Wildcard mask bit 0 = match the corresponding bit value in the address
  + Wildcard mask bit 1 = ignore the corresponding bit value in the address
    - (Inverse mask)
* General Guidelines for Creating ACLs
  + Using ACLs in firewall routers positioned between your internal network and an external network such as the Internet
  + Use ACLs on a router positioned between two parts of your network to control traffic entering or exiting a specific part of your internal network
  + Configure ACLs on border routers, that is, routers situated at the edges of your networks This provides a very basic buffer from the outside network, or between a less controlled area of your own network and a more sensitive area of your network
  + Configure ACLs for each network protocol configured on the border router interfaces
  + Configure ACL per protocol, per direction, per interface
    - One ACL per protocol
      * To control traffic flow on the interface. Must be defined for each protocol and enabled on the interface
    - One ACL per direction
      * Control traffic in one direction at a time. Two separate ACLs to control inbound and outbound traffic
    - One ACL per interface
      * Control traffic for interface
* Where to Place ACLs
  + Extended ACLs
    - Locate as close as possible to the source of traffic to be filtered (undesirable traffic is closer to the source network without crossing the network infrastructure
  + Standard ACLS
    - Close to the destination. Effectively prevent traffic from reaching any other network
  + Can also Depend on:
    - The extent of network admin control
    - Bandwidth
    - Ease of configuration
  + Standard
    - As close as possible to the destination network