1. **Introduction to Extended Access Control Lists (ACLs)**

* **Purpose**: Extended ACLs allow for more specific filtering compared to standard ACLs.
* **Key Features**:
  + Specify **source and destination IP addresses**.
  + Filter based on **protocols** and **ports**.
  + Example: Allow HTTP traffic between specific hosts.

1. **Syntax and Numbering**

* **Numbering Range**:
  + **100-199** and **2000-2699** for extended numbered ACLs.
* **Syntax Explanation:**
  + Mandatory parameters: {access-list-number} and {deny|permit|remark}.
  + Optional parameters: [protocol], [operator port number or name].
* **Operators for Ports:**
  + **eq** Equal to.
  + **lt** Less than.
  + **gt** Greater than.
  + **range** Specify two port numbers.

1. **Examples of Extended ACL Usage**

* **Blocking All IP Traffic Between Networks:**
  + Example command: access-list 100 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.255.255.
* **Blocking TCP Traffic but Allowing Others:**
  + Command: access-list 100 deny tcp ... followed by access-list 100 permit ip any any.
* **Blocking Specific Traffic (e.g., HTTP):**
  + Example: access-list 100 deny tcp ... eq 80.

1. **Using Extended Named ACLs**

* **Benefits**: Named ACLs provide easier identification compared to numbered ACLs.
* **Syntax**:
  + Create with ip access-list extended [name].
  + Example: ip access-list extended FIREWALL.

1. **Editing Access Lists**

* **View Existing ACLs**: Use show access-lists.
* **Editing Steps:**
  + Use ip access-list extended [name/number] to enter editing mode.
  + Remove or modify entries with commands like no [sequence number].

1. **Applying ACLs to Interfaces**

* **Syntax:**
  + Use ip access-group [name/number] [in|out].
  + Example: Apply ACL to an interface in the inbound direction.

1. **Mitigating Attacks Using ACLs**

* **Spoofing Attacks**: Deny packets with invalid source IPs, such as:
  + Localhost (127.0.0.0/8).
  + Reserved private addresses (RFC 1918).
  + Multicast addresses (224.0.0.0/4).
* **ICMP Attacks**: Block specific ICMP messages but allow necessary ones, such as:
  + **Echo replies**, **unreachable**, and **source quench**.

1. **Securing Specific Services**

* **Example Protocols**: Allow DNS, SMTP, FTP while blocking unauthorized traffic.
* **Command Example**:
  + access-list 180 permit udp any host [IP] eq domain.
  + access-list 180 deny ... to restrict access.

1. **Using the "Established" Keyword**

* **Purpose**: Allows return traffic for established TCP sessions.
* **Example Command**:
  + access-list 120 permit tcp any [network] established.

1. **Summary of Applications**

* ACLs enhance security by:
  + Controlling traffic flow.
  + Mitigating common attacks.
  + Securing access to services and interfaces.

1. Well known TCP/UDP Port numbers (numbers used in TCP/UDP headers to identify the desired destination server)

* 20/TCP [FTP](http://en.wikipedia.org/wiki/File_transfer_protocol)
* 21/TCP [FTP](http://en.wikipedia.org/wiki/File_transfer_protocol) – control (command)
* 22/TCP,UDP [Secure Shell](http://en.wikipedia.org/wiki/Secure_Shell) (SSH)—used for secure logins, [file transfers](http://en.wikipedia.org/wiki/File_transfer) ([scp](http://en.wikipedia.org/wiki/Secure_copy), [sftp](http://en.wikipedia.org/wiki/SSH_file_transfer_protocol)) and port forwarding
* 23/TCP [Telnet](http://en.wikipedia.org/wiki/Telnet) protocol
* 25/TCP [Simple Mail Transfer Protocol](http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) (SMTP)—used for e-mail routing between mail servers
* 42/TCP,UDP nameserver, [ARPA](http://en.wikipedia.org/wiki/DARPA) [Host Name Server Protocol](http://en.wikipedia.org/wiki/ARPA_Host_Name_Server_Protocol) Official 42/TCP,UDP [WINS](http://en.wikipedia.org/wiki/Windows_Internet_Name_Service)
* 43/TCP [WHOIS](http://en.wikipedia.org/wiki/WHOIS) protocol
* 53/TCP,UDP [Domain Name System](http://en.wikipedia.org/wiki/Domain_Name_System) (DNS)
* 67/UDP [Bootstrap Protocol](http://en.wikipedia.org/wiki/Bootstrap_Protocol) (BOOTP) Server; also used by [Dynamic Host](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) [Configuration Protocol](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) (DHCP)
* 68/UDP [Bootstrap Protocol](http://en.wikipedia.org/wiki/Bootstrap_Protocol) (BOOTP) Client; also used by [Dynamic Host](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) [Configuration Protocol](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) (DHCP)
* 69/UDP [Trivial File Transfer Protocol](http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol) (TFTP)
* 70/TCP [Gopher](http://en.wikipedia.org/wiki/Gopher_%28protocol%29)
* 79/TCP [Finger protocol](http://en.wikipedia.org/wiki/Finger_protocol)
* 80/TCP,UDP [Hypertext Transfer Protocol](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) (HTTP)
* 110/TCP [Post Office Protocol](http://en.wikipedia.org/wiki/Post_Office_Protocol) 3 (POP3)
* 115/TCP [Simple File Transfer Protocol](http://en.wikipedia.org/wiki/Simple_File_Transfer_Protocol) (SFTP)
* 123/UDP [Network Time Protocol](http://en.wikipedia.org/wiki/Network_Time_Protocol) (NTP)—used for time synchronization
* 135/TCP,UDP [DCE](http://en.wikipedia.org/wiki/Distributed_Computing_Environment) [endpoint](http://en.wikipedia.org/wiki/Communication_endpoint) resolution
* 137/TCP,UDP [NetBIOS](http://en.wikipedia.org/wiki/NetBIOS) NetBIOS Name Service
* 138/TCP,UDP [NetBIOS](http://en.wikipedia.org/wiki/NetBIOS) NetBIOS Datagram Service
* 443/TCP,UDP [HTTPS](http://en.wikipedia.org/wiki/HTTPS) ([Hypertext Transfer Protocol](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) over [SSL](http://en.wikipedia.org/wiki/Secure_Sockets_Layer)/[TLS](http://en.wikipedia.org/wiki/Transport_Layer_Security))
* 520/UDP [Routing Information Protocol](http://en.wikipedia.org/wiki/Routing_Information_Protocol) (RIP)
* 554/TCP,UDP [Real Time Streaming Protocol](http://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol) (RTSP)
* 5060/TCP, UDP, Session Initiating Protocol (SIP)
* 8080/TCP,UDP [Hypertext Transfer Protocol](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol)

All the Packet Tracer commands extracted from the document:

**1. Configuring an Extended Numbered Access List**

* **Block all IP traffic between two networks:**

(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.255.255

* **Block only TCP traffic but allow others:**

(config)# access-list 100 deny tcp 10.0.0.0 0.255.255.255 172.16.0.0 0.0.255.255

(config)# access-list 100 permit ip any any

* **Block only HTTP traffic:**

(config)# access-list 100 deny tcp 10.0.0.0 0.255.255.255 172.16.0.0 0.0.255.255 eq 80

(config)# access-list 100 permit ip any any

**2. Example of Extended Numbered Access List**

* **Allow HTTP and HTTPS requests from a specific network:**

(config)# access-list 101 permit tcp 172.31.1.96 0.0.0.31 any eq 80

(config)# access-list 101 permit tcp 172.31.1.96 0.0.0.31 any eq 443

* **Allow replies for established sessions:**

(config)# access-list 103 permit tcp any 172.31.1.96 0.0.0.31 established

**3. Configuring an Extended Named Access List**

* **Create a named extended ACL:**

(config)# ip access-list extended FIREWALL

(config-ext-nacl)# permit tcp any host 192.168.20.254 eq 80

(config-ext-nacl)# permit tcp any any established

**4. Editing Access Lists**

* **Enter extended ACL configuration mode and edit entries:**

R1(config)# ip access-list extended 101

R1(config-ext-nacl)# no 10

R1(config-ext-nacl)# 5 permit tcp 172.31.1.96 0.0.0.31 any eq telnet

R1(config-ext-nacl)# 15 permit tcp 172.31.1.96 0.0.0.31 any eq ftp

**5. Securing SSH and Telnet Access**

* **Allow SSH and Telnet access to a specific host and deny all others:**

R1(config)# ip access-list extended VTY

R1(config-ext-nacl)# permit tcp host 172.16.1.100 host 192.168.2.1 eq 22

R1(config-ext-nacl)# permit tcp host 172.16.1.100 host 192.168.2.1 eq 23

R1(config-ext-nacl)# deny tcp any any eq 22

R1(config-ext-nacl)# deny tcp any any eq 23

R1(config-ext-nacl)# permit ip any any

* **Apply the ACL to an interface:**

R1(config)# int g0/0/1

R1(config-if)# ip access-group VTY in

**6. Using the Established Keyword**

* **Allow return traffic for established connections:**

R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established

* **Apply ACL to an interface:**

R1(config)# interface g0/0/0

R1(config-if)# ip access-group 120 out

**7. Mitigating Spoofing Attacks**

* **Deny traffic from invalid source IPs:**

R1(config)# access-list 150 deny ip host 0.0.0.0 any

R1(config)# access-list 150 deny ip 10.0.0.0 0.255.255.255 any

R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any

R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any

R1(config)# access-list 150 deny ip 192.168.0.0 0.0.255.255 any

R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any

R1(config)# access-list 150 deny ip host 255.255.255.255 any

**8. Permitting Necessary Traffic**

* **Allow specific services:**

R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain

R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp

R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp

R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22

R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog

R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap

**9. Mitigating ICMP Attacks**

* **Allow certain ICMP messages inbound:**

R1(config)# access-list 112 permit icmp any any echo-reply

R1(config)# access-list 112 permit icmp any any source-quench

R1(config)# access-list 112 permit icmp any any unreachable

R1(config)# access-list 112 deny icmp any any

R1(config)# access-list 112 permit ip any any

* **Allow ICMP messages outbound:**

R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo

R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem

R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big

R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench

R1(config)# access-list 114 deny icmp any any