***ACLs (Access Control Lists):***

Configured on L2. An ACL is a collection of permit/deny conditions that apply to packets.

A switch will test a packet against the conditions set, and determine whether to forward or drop a packet.

If no ACLs are set on a switch, then all packets will be forwarded.

An ACL contains an ordered list of Access Control Entries (ACEs).

A switch supports these types of ACLs;

* IP ACLs to filter traffic of both TCP and UDP
* Ethernet ACLs to filter L2 traffic

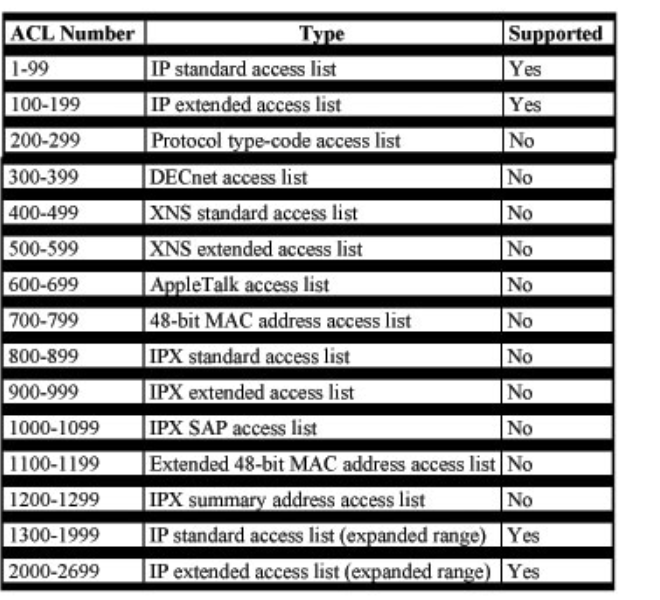
ACLs can be applied on management VLANs and physical L2 interfaces (FOR INBOUND DIRECTIONS.)

STANDARD IP access lists use source addresses for matching operations.

EXTENDED IP access Lists use source and destination addresses and optional protocol type info for matching operations.

MAC EXTENDED access lists use source and destination MAC addresses and optional protocol type info for matching operations.

ACL chart:



FLEXCONNECT ACLs:

* Cannot be configured with per-rule direction
* Applied per AP per VLAN
* Supported on native VLAN

**How to create a standard ACL:**

*Access-list <access-list-number> {permit | deny} {host | source source-wildcard | any}*

**After an ACL is defined, it must be applied to the interface (inbound or outbound):**

*Ip access-group number {in | out}*

**Example: a standard ACL to block all traffic except from source 10.1.1.x**

*Interface Ethernet0/0*

*Ip address 10.1.1.1 255.255.255.0*

*Ip access-group 1 in*

*Access-list 1 permit 10.1.1.0.0.0.0.255*

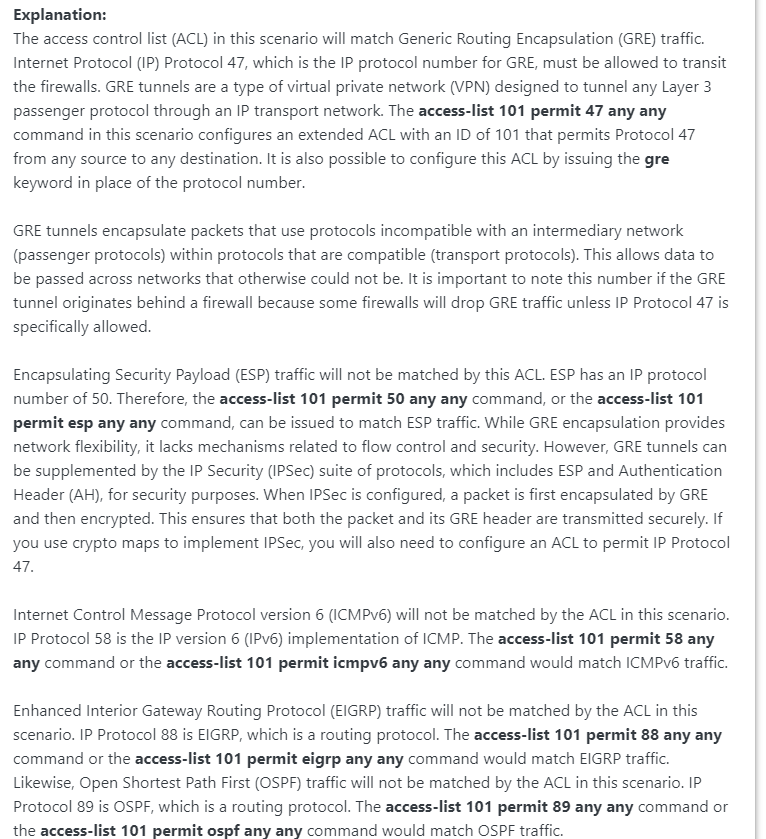
**How to create an Extended ACL:**

Access-list access-list-number

[dynamic dynamic-name [timeout minutes]]

{deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence]

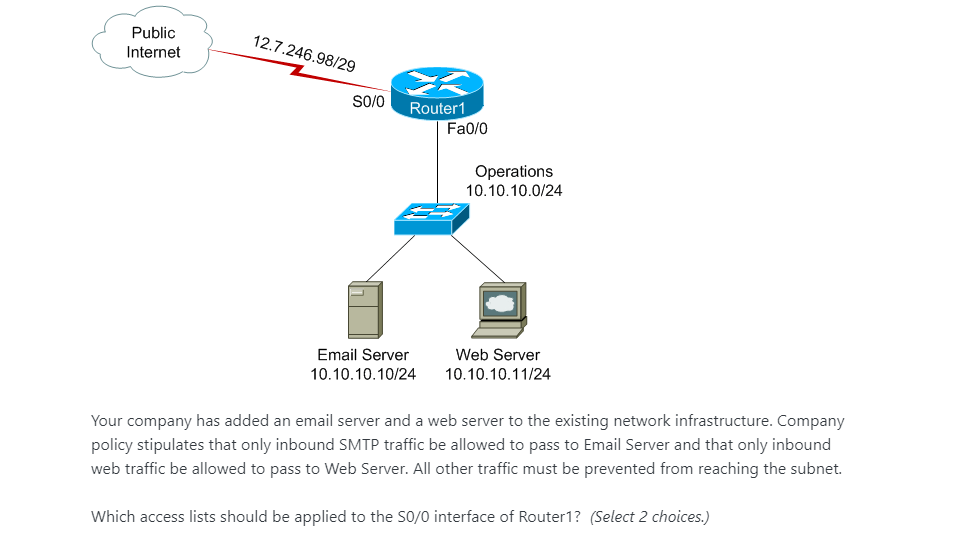
[tos tos] [log | log-input] [time-range time-range-name]



[Configure Commonly Used IP ACLs - Cisco](https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html#anc19)

[Cisco Software-Defined Access FAQ - Cisco](https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-09-sda-faq-cte-en.html)

Example:



Appropriate commands:

Access-list 101 permit tcp any 10.10.10.11 0.0.0.0 eq 80

Access-list 101 permit tcp any 10.10.10.10 0.0.0.0 eq 25

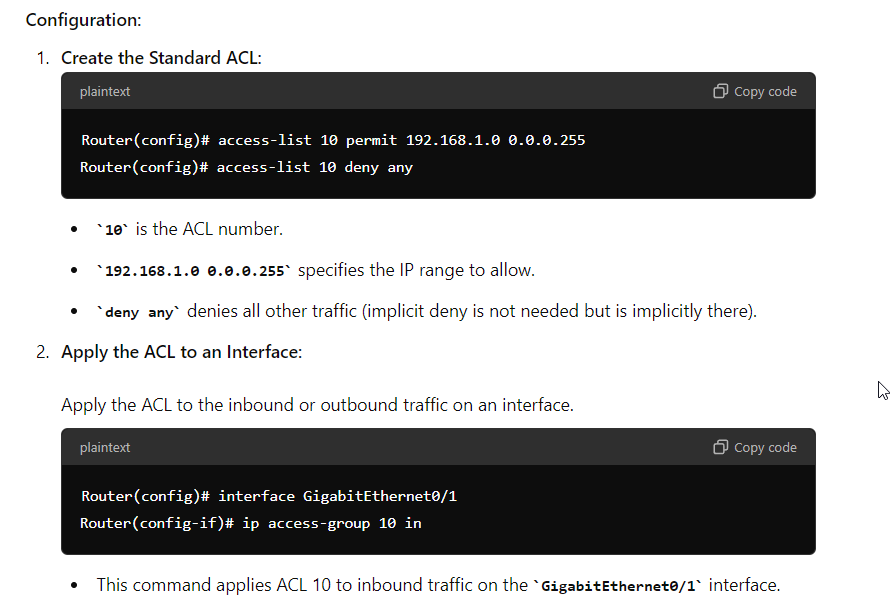
Individual ACL is applied to a specific interface in one direction

Here, two ACLs need to be applied to S0/0 interface of R1

Eq 25 is for email servers

Eq 80 is for receiving web traffic

Access listers are created in router config first, then applied to the interface(s)



ACL NOTES 03/09:

Standard ACLs:

* 1-99, 1300-1999
* Filter based on source IP address only
* DO NOT filter based on protocols or ports

Extended ACLs:

* 100-199, 2000-2699
* Filter based on source and dest. IP, protocols (like OSPF), and ports

Examples:

**Your colleague calls you to say that he has added an access list but now all OSPF traffic is being blocked. Which config line do you tell him to add?**

**access-list 101 permit ospf any any**

**access-list 101 permit ip ospf any any**

**access-list 101 ip any any eq 89**

**access-list 101 permit any any eq ospf**

Explanation:

Access-list 101 permit ospf any any is correct.

This is because the all options specify ospf or a port number (This means all options are extended access lists), so number has to be atleast 100

“Any any” means that OSPF traffic from any SOURCE to any DEST. is allowed

access-list 101 ip any any eq 89 is incorrect as “eq” is used for port numbers in TCP/UDP, not protocol numbers

access-list 101 permit ip ospf any any is incorrect as the syntax of “ip” followed by “ospf” is incorrect

*Configuring an ACL like the above would look like:*

*En*

*Conf t*

*Access-list 101 permit ospf any any*

*Int <int>*

*Ip access-group 101 in*

*End*

*Copy run start*

Which access-list format will block TFTP traffic from host 10.1.1.1 to any host or network.

access-list 102 deny udp host 10.1.1.1 any eq 69

access-list 102 deny udp any host 10.1.1.1 eq 69

access-list 102 deny udp host 10.1.1.1 any eq 53

access-list 102 deny udp any host 10.1.1.1 eq 53

access-list 10 deny udp host 10.1.1.1 any eq 69

access-list 102 deny udp 10.1.1.1 any eq 69

Access-list 102 deny udp host 10.1.1.1 any eq 69 is correct because…

102 represent an extended ACL.

A specific host IP AND specific port AND specific protocol (udp) mean an extended ACL is required

“Any” after the host IP means it will block traffic going to any destination

TFTP is port 69 UDP

*Configuring an ACL like the above would look like:*

*En*

*Conf t*

*Access-list 102 deny udp host 10.1.1.1 any eq 69*

*Access-list 102 permit ip any any*

*Int <int>*

*Ip access-group 102 in*

*End*

*Copy run start*

**This blocks TFTP traffic from host 10.1.1.1 and permits all other traffic (in bound traffic)**

Access-list 102 deny udp host 10.1.1.1 any eq 69

102 = ACL number

Deny udp = denies UDP traffic

Host 10.1.1.1 = specific source IP address of traffic to be blocked

Any = destination can be any IP address

Eq 69 = specifies that only traffic on port 69 TFTP will be denied

Access-list 102 permit ip any any

Allows all other traffic. Offsets implicit deny statement. Ensures all other traffic is permitted

You are a network administrator for a small company. You have a router that connects to three different subnets:

* **Subnet A:** 192.168.10.0/24
* **Subnet B:** 192.168.20.0/24
* **Subnet C:** 192.168.30.0/24

The company wants to restrict access to Subnet C. Only hosts from Subnet A should be allowed to access Subnet C. Hosts from Subnet B should be denied access to Subnet C.

**Task:**

1. Create a **standard ACL** to meet the company's requirements.
2. Apply the ACL to the correct interface on the router to filter traffic from Subnet B going into Subnet C.

**Requirements:**

* Use ACL number 15.
* Apply the ACL in the most efficient manner to achieve the desired outcome.
* Only traffic from Subnet A should be allowed to reach Subnet C.

### **Questions:**

1. Write the configuration commands to create the standard ACL that allows traffic from Subnet A and denies traffic from Subnet B to Subnet C.
2. Specify the interface and direction where you would apply this ACL.

*En*

*Conf t*

*Access-list 15 permit 192.168.10.0 0.0.0.255*

*Int <int>*

*Ip access-group 15 in*

*This access list allows traffic from subnet A. By default, traffic from the other subnets will be denied due to implicit deny rule*

*I then apply this to the appropriate interface and indicate “in” as it will apply the ACL to incoming traffic on the interface*