Access Control Lists (ACLs) - Full Guide

1. What is an ACL?

An Access Control List (ACL) is a set of rules applied to router interfaces to permit or deny traffic based on d

2. Types of ACLs:

Type	Description
Standard ACL	Filters traffic only by source IP.
Extended ACL	Filters by source/destination IP, protocol, and port.
Named ACL	Allows use of names instead of numbers; supports both Standard and Extended.

3. ACL Direction:

- IN: Applies to traffic coming into an interface.
- OUT: Applies to traffic leaving an interface.

4. Wildcard Mask:

Used to match ranges of IP addresses. A wildcard mask is the inverse of a subnet mask.
Example: 192.168.1.0 0.0.0.255 means match 192.168.1.0/24.

5. Standard ACL Example:

```
access-list 10 permit 192.168.1.0 0.0.0.255
interface GigabitEthernet0/0
ip access-group 10 in
```

6. Extended ACL Example:

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 100 deny ip any any
interface GigabitEthernet0/0
ip access-group 100 in
```

7. Named ACL Example:

```
ip access-list extended WEB_CONTROL
 permit tcp 192.168.1.0 0.0.0.255 any eq 80
 deny ip any any
interface GigabitEthernet0/0
ip access-group WEB_CONTROL in
```

8. Useful Commands:

- show access-lists
- show ip interface
- debug ip packet
- no access-list <number/name> (to remove ACL)

9. Tips & Best Practices:

- One ACL per direction per interface.
- Extended ACLs should be placed close to the source.
- Standard ACLs should be placed close to the destination.
- Always have a permit ip any any if you want to allow traffic at the end.

10. Implicit Deny Rule:

All ACLs end with an implicit "deny all" - this line is not shown but always present.