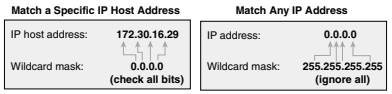
- A wildcard mask bit 0 means check the corresponding bit value.
- A mask bit 1 means do not check (ignore) that corresponding bit value.



To specify an IP host address within a **permit** or **deny** statement, enter the full address followed by a mask of all 0s (0.0.0.0).

To specify that all destination addresses will be permitted in an access list, enter 0.0.0.0 as the address, followed by a mask of all 1s (255.255.255).

Abbreviated Commands in Wildcard Masking

You can use abbreviations rather than typing an entire wildcard mask:

- **Checking all addresses**—To match a specific address, use **host**. For example, **172.30.16.29 0.0.0.0** can be written as **host 172.30.16.29**.
- **Ignoring all addresses**—Use the word **any** to specify all addresses. For example, **0.0.0.0 255.255.255.255** can be written as **any**.

Access Lists and Their Applications Summary

- Access lists filter packets as they pass through the router.
- The two general types of access lists are standard and extended. Standard lists filter based on only the source address, and extended lists filter based on source and destination addresses, as well as specific protocols and numbers.
- Access lists can be set to either inbound or outbound. For inbound access lists, the packets are processed first and then routed to an outbound interface (assuming that the filter passes them). In outbound access lists, the packets are sent to the interface and then routed.
- If a packet meets a **permit** statement's criteria, it is passed to the next statement. If a packet meets a **deny** statement's criteria, it is immediately discarded.
- More-restrictive statements should be at the top of the list.
- Only one access list per interface, per protocol, per direction is allowed.
- Every access list should have at least one **permit** statement.
- For IP, standard access lists use the number range 1 to 99, and extended access lists use 100 to 199. For IPX, standard access lists use 800 to 899, and extended access lists use 900 to 999.
- Wildcard masking is used to filter single IP addresses or blocks of addresses.

Access List Configuration

Principles of Configuring Access Lists

Access lists are processed from top to bottom, making statement ordering critical to efficient operation. Always place specific and frequent statements at the beginning of an access list. Named access lists allow the removal of individual statements (but no reordering). To reorder statements, you must remove and re-create the whole list with the proper statement ordering. Use a text editor to create lists. Remember that all access lists end with an implicit **deny all** statement.

Access List Syntax

The syntax for a standard and extended IP access lists is **access-list access-list-number {permit | deny} source [mask]**.

```
access-list access-list-number {permit | deny} protocol source
    source-wildcard
  [operator port] destination destination-wildcard [operator port]
  [established] [log]
```

operator port can be less than, greater than, equal to, or not equal to a port number. **established** (used for inbound TCP only) allows only established connections to pass packets. **log** sends a logging message to the console.

After the statements are added, they are applied to an access group using the following syntax:

```
ip access-group access-list-number {in | out}
```

Here is the procedure for configuring extended IP access lists:

```
RouterA>enable
RouterA#access-list 101 deny tcp 172.16.4.0 0.0.0.255 72.16.3.0 0.0.0.255 eq
21
RouterA#config term
RouterA(config)#interface ethernet 0
RouterA(config-if)#access group 101 in
RouterA(config)#exit
RouterA#show ip interface
```