Accesslists

What are Access Control Lists?

ACLs...

...are a sequential list of instructions that tell a router which packets to permit or deny.

General Access Lists Information

Cisco.com

Access Lists...

...are read sequentially.

...are set up so that as soon as the packet matches a statement it stops comparing and permits or denys the packet.

...need to be written to take care of the most abundant traffic first.

...must be configured on your router before you can deny packets.

...can be written for all supported routed protocols;

but

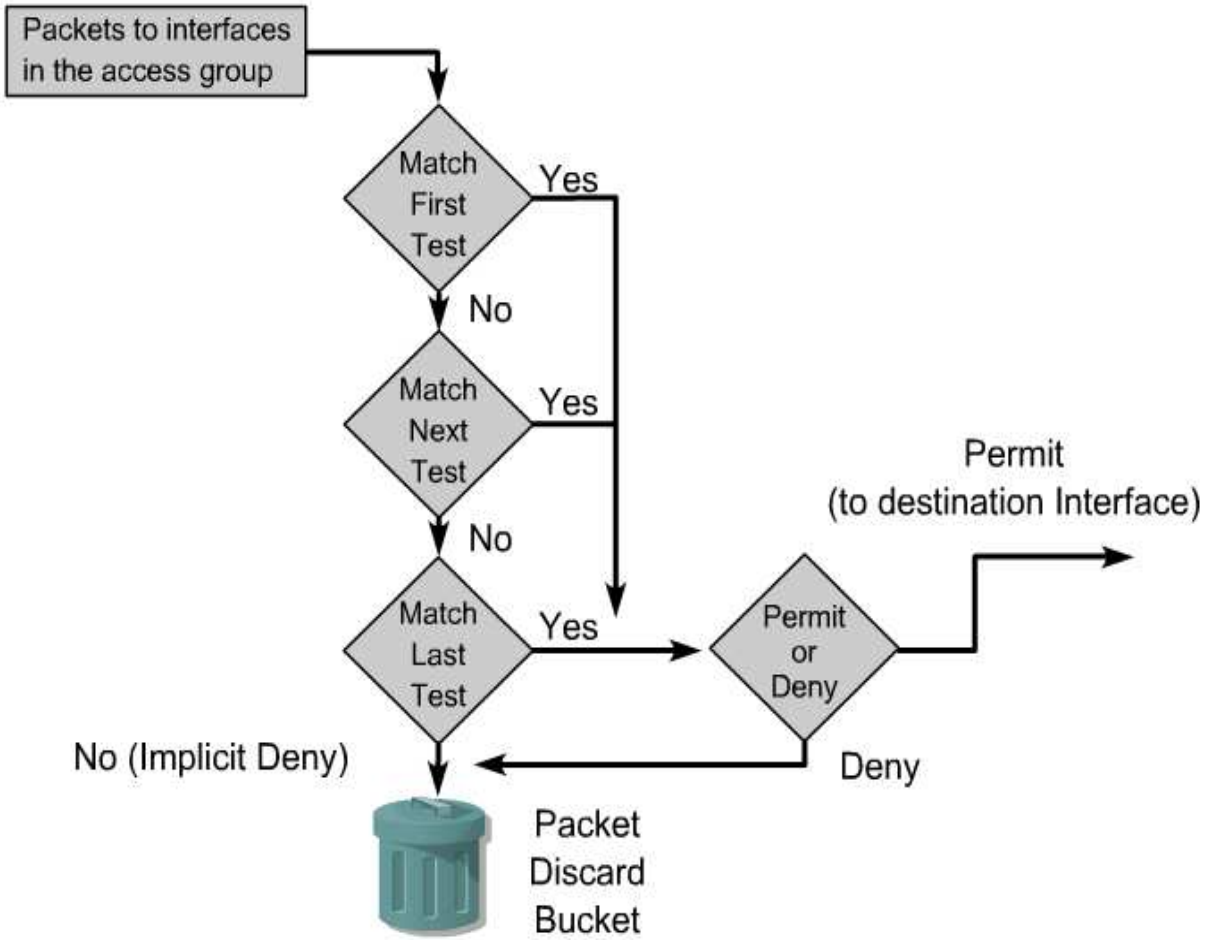
…each routed protocol must have a different ACL for each interface.

...must be applied to an interface to work.

How routers use Access Lists (Outbound Port - Default)

- The router checks to see if the packet is routable. If it is it looks up the route in its routing table.
- The router then checks for an ACL on that outbound interface. If there is no ACL the router switches the packet out that interface to its destination.
- If there is an ACL, the router checks the packet against the access list statements sequentially. Then permits or denys each packet as it is matched.
- If the packet does not match any statement written in the ACL it is denyed because there is an implicit “deny any” statement at the end of every ACL.

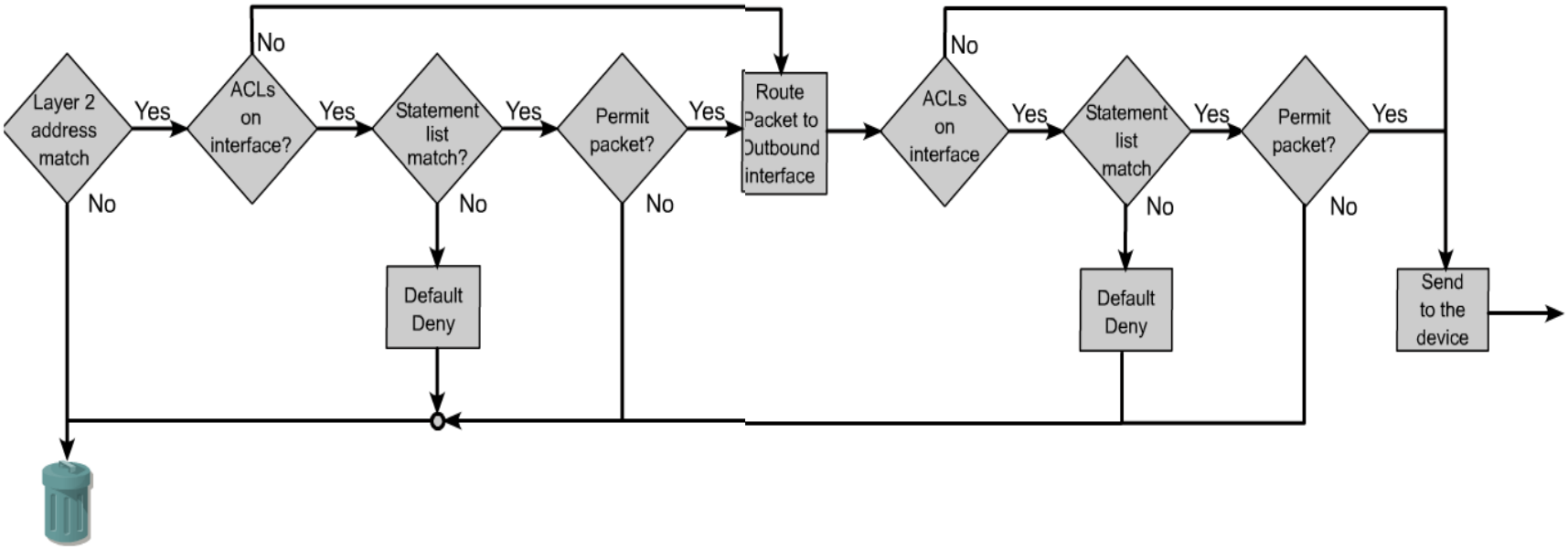
How routers use Access Lists
(Outbound Port - Default)



ACL:s

Cisco.com

ACL and routing processes in a router



Standard Access Lists

Cisco Systems Networking Academy

Cisco.com

Standard Access Lists...

...are numbered from 1 to 99.

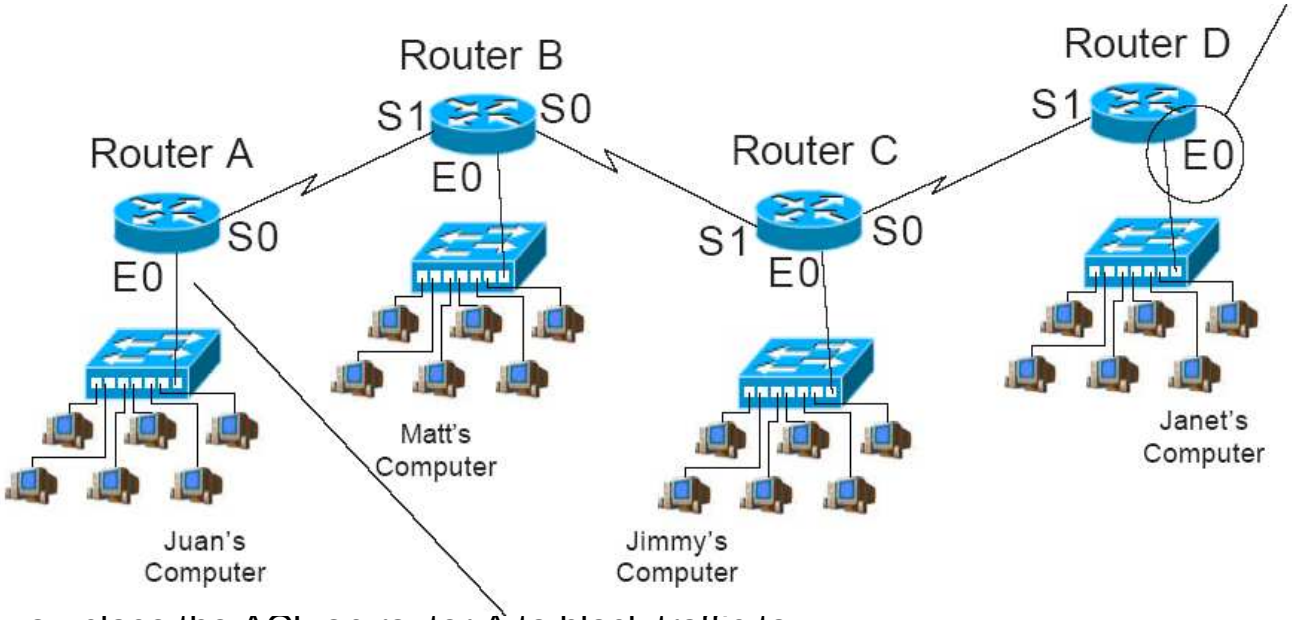
...filter (permit or deny) only source addresses.

...do not have any destination information so it must placed as close to the destination as possible.

...work at layer 3 of the OSI model.

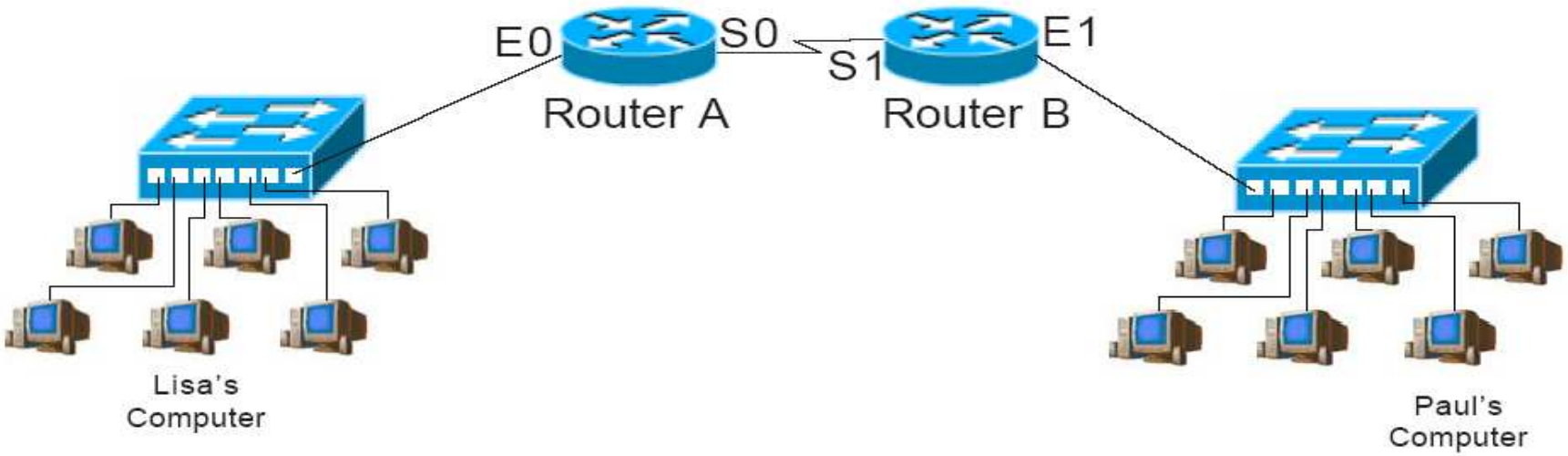
Why standard ACLs are placed close to the destination.

If you want to block traffic from Juan's computer from reaching Janet's computer with a standard access list you would place the ACL **close to the destination** on Router D, interface E0. Since its using only the source address to permit or deny packets the ACL here will not effect packets reaching Routers B, or C.



If you place the ACL on router A to block traffic to Router D it will also block all packets going to Routers B, and C; because all the packets will have the same source address.

Standard Access List Placement Sample Problems



Lisa has been sending unnecessary information to Paul. Where would you place the standard ACL to deny all traffic from Lisa to Paul?
Router Name _____ Interface _____

Where would you place the standard ACL to deny traffic from Paul to
Lisa?
Router Name _____ Interface _____

Extended Access Lists

Cisco Systems Networking Academy

Cisco.com

Extended Access Lists...

...are numbered from 100 to 199.

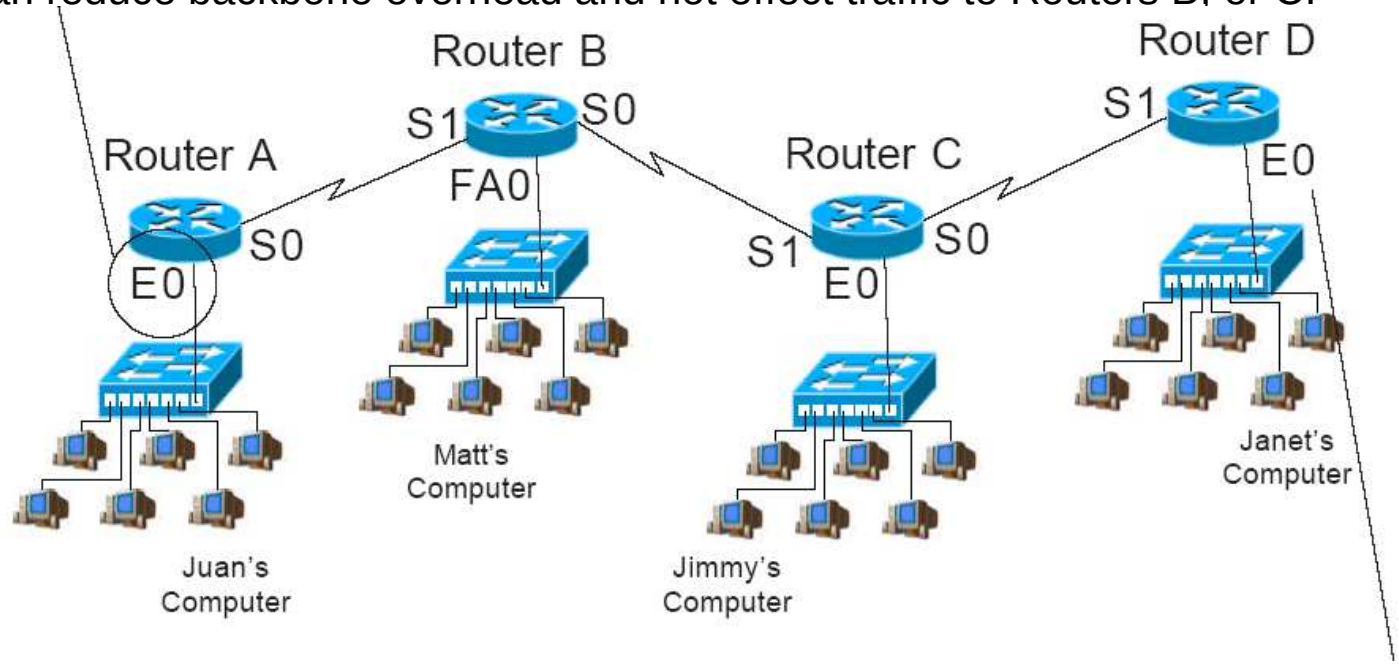
...filter (permit or deny) based on the: source address destination address protocol port number

... are placed close to the source.

...work at both layer 3 and 4 of the OSI model.

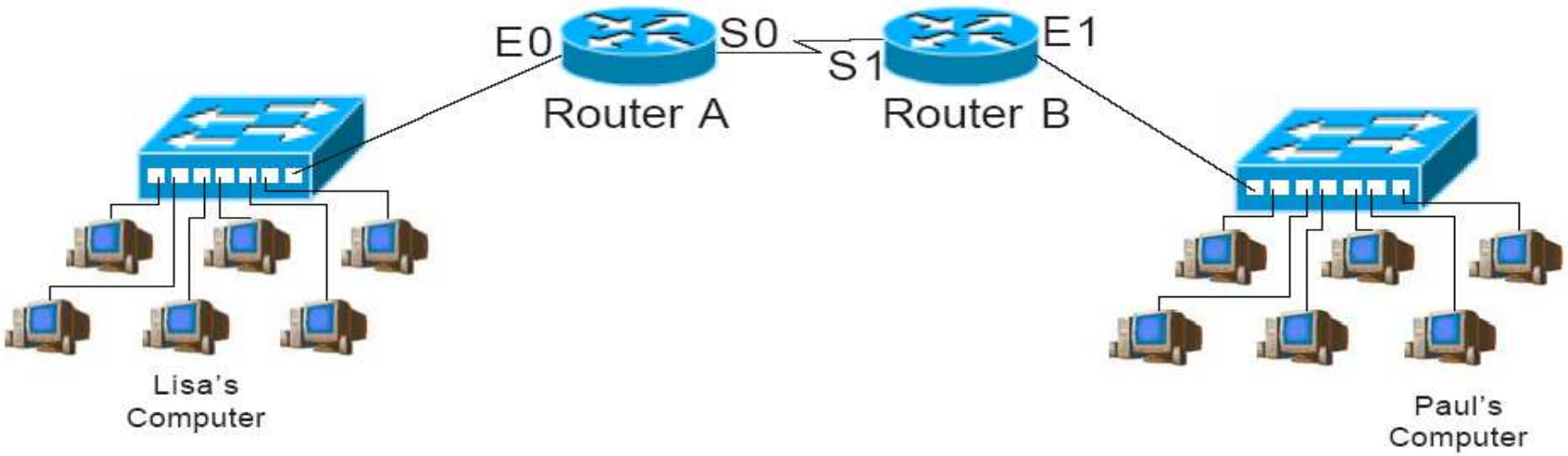
Why extended ACLs are placed close to the source.

If you want to deny traffic from Juan's computer from reaching Janet's computer with an extended access list you would place the ACL **close to the source** on Router A, interface E0. Since it can permit or deny based on the destination address it can reduce backbone overhead and not effect traffic to Routers B, or C.



If you place the ACL on Router D to block traffic from Router A, it will work. However, Routers B, and C will have to route the packet before it is finally blocked at Router D. This increases the volume of useless network traffic.

Extended Access List Placement Sample Problems



Lisa has been sending unnecessary information to Paul. Where would you place the extended ACL to deny all traffic from Lisa to Paul?

Router Name _____ Interface _____

Where would you place the extended ACL to deny traffic from Paul to Lisa?

Router Name _____ Interface _____

Choosing to Filter Incoming or Outgoing Packets

Access Lists on your incoming port...

...requires less CPU processing.

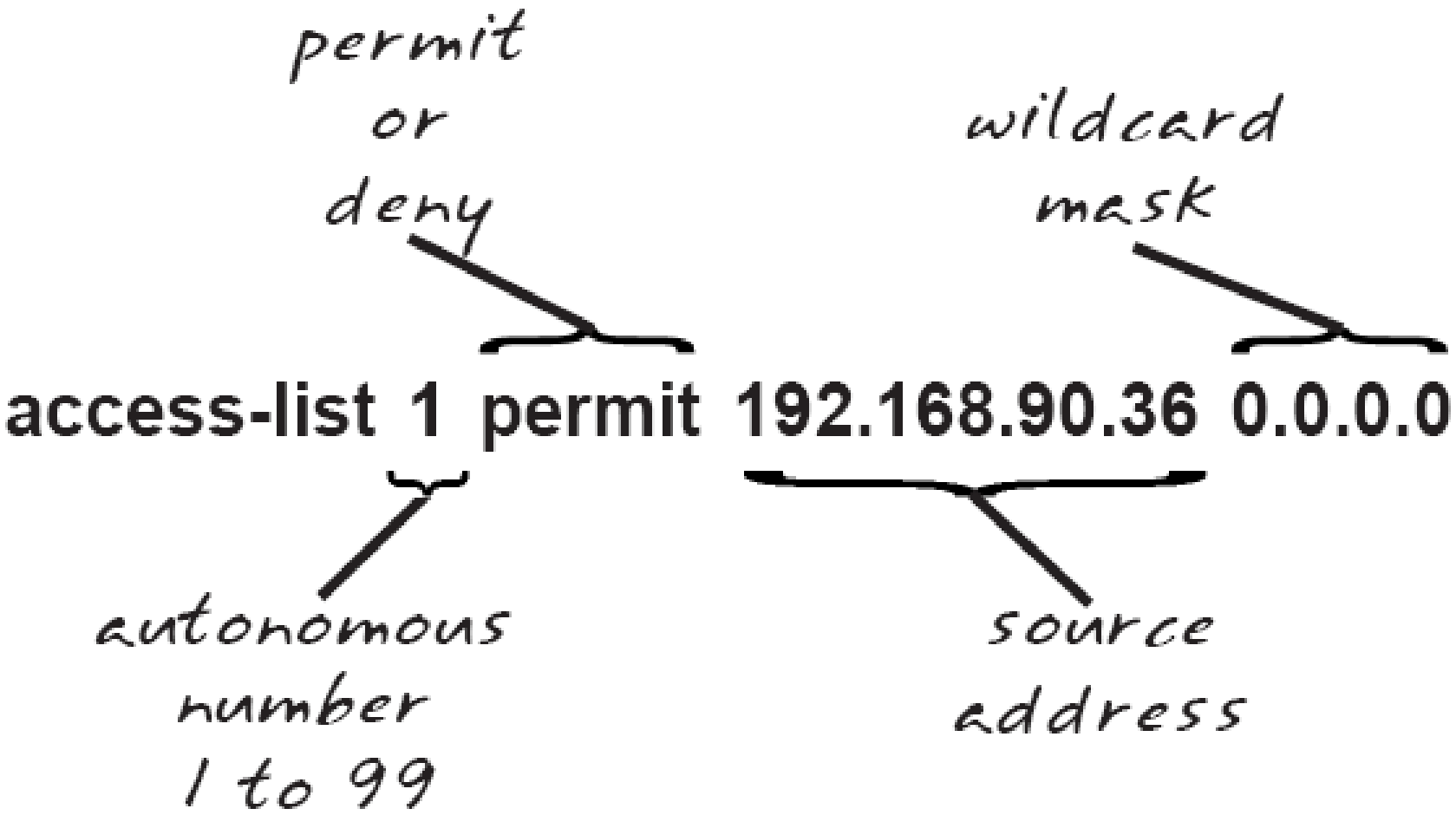
...filters and denys packets before the router has to make a routing decision.

Access Lists on your outgoing port...

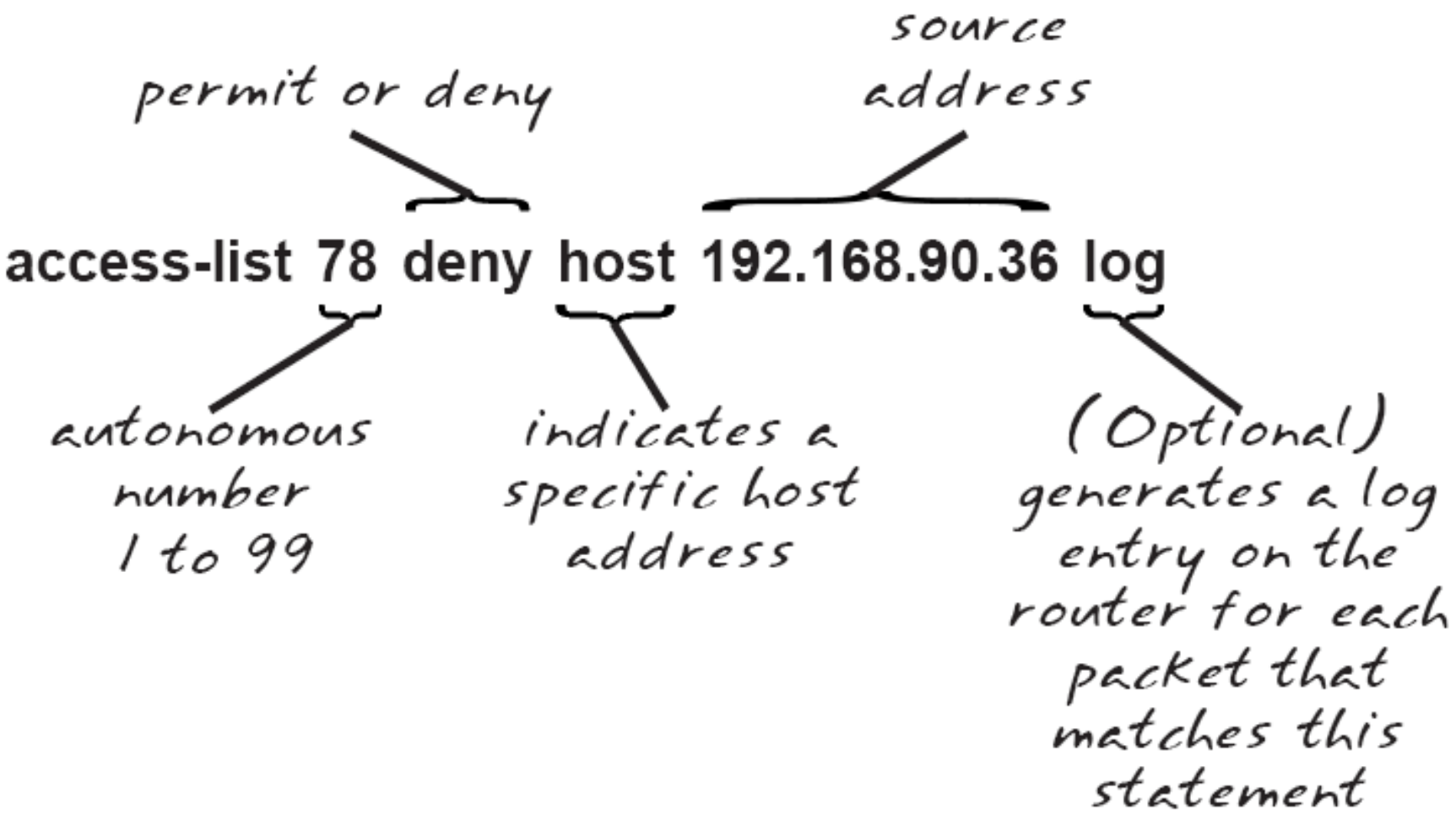
...are outbound by default unless otherwise specified.

...increases the CPU processing time because the routing decision is made and the packet switched to the correct outgoing port before it is tested against the ACL.

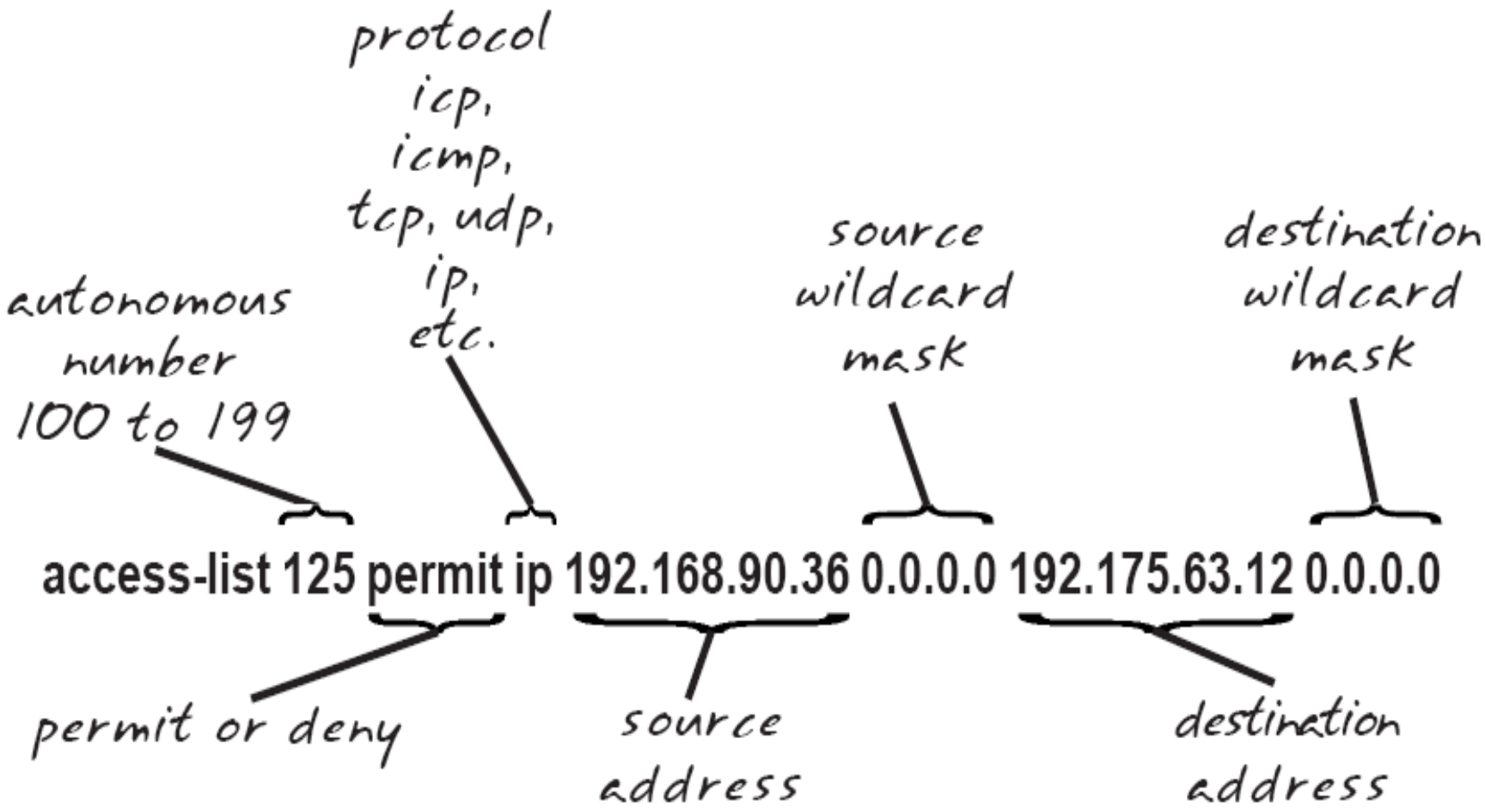
Breakdown of a Standard ACL Statement



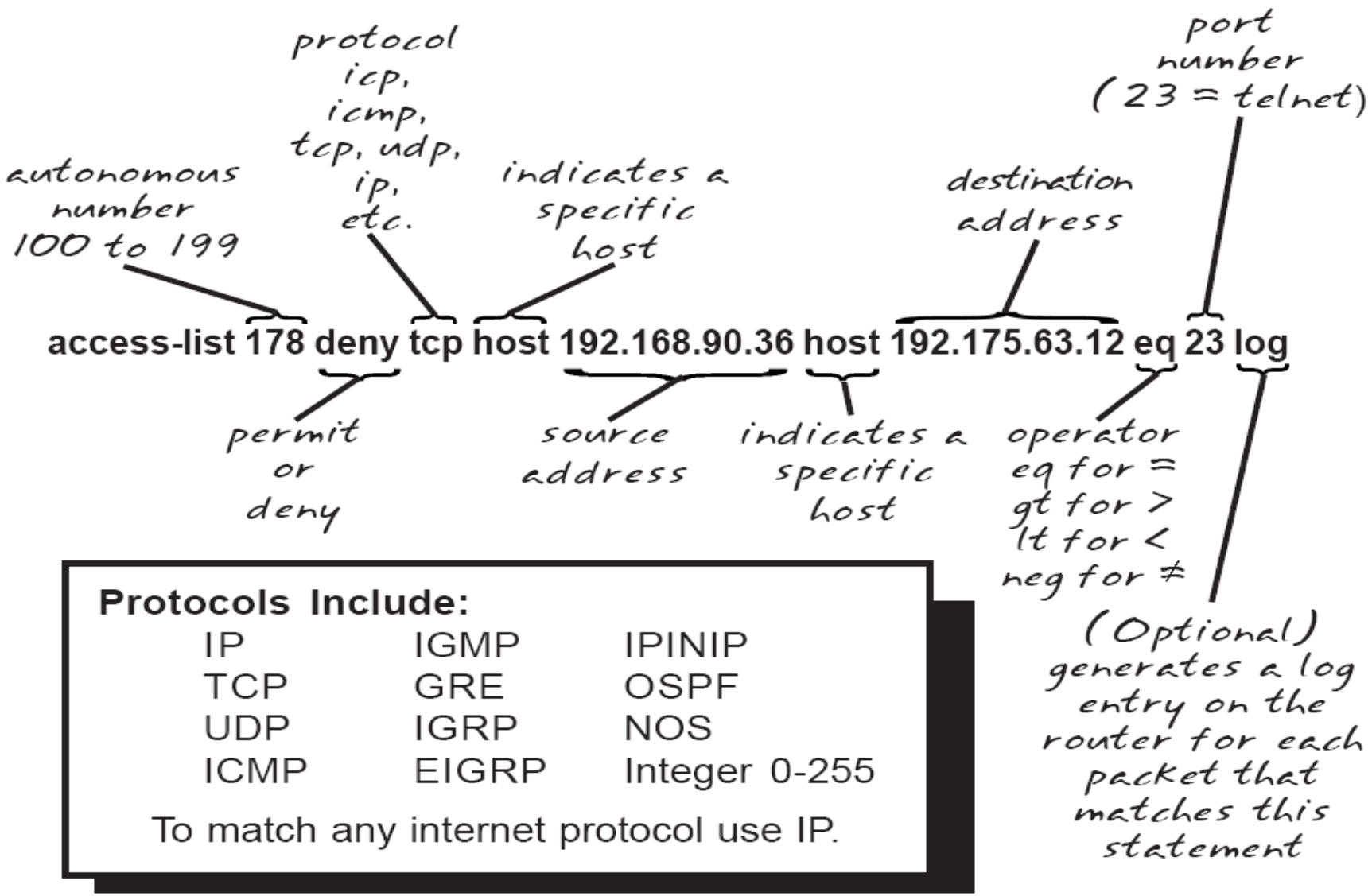
Breakdown of a Standard ACL Statement



Breakdown of an Extended ACL Statement



Breakdown of an Extended ACL Statement



Choices for Using Wildcard Masks

Wildcard masks are usually set up to do one of four things:

1. Match a specific host.
2. Match an entire subnet.
3. Match a specific range.
4. Match all addresses.

1. Matching a specific host.

For standard access lists:

Access-List 10 permit 192.168.150.50 0.0.0.0

or

Access-List 10 permit 192.168.150.50 (standard ACL's assume a 0.0.0.0 mask)

or

Access-List 10 permit host 192.168.150.50

For extended access lists:

Access-list 110 deny ip 192.168.150.50 0.0.0.0 any

or

Access-list 110 deny ip host 192.168.150.50 any

2. Matching an entire subnet

Example 1

Address: 192.168.50.0 Subnet Mask: 255.255.255.0

Access-list 25 deny 192.168.50.0 0.0.0.255

Example 2

Address: 172.16.0.0 Subnet Mask: 255.255.0.0

Access-list 12 permit 172.16.0.0 0.0.255.255

Example 3

Address: 10.0.0.0 Subnet Mask: 255.0.0.0

Access-list 125 deny udp 10.0.0.0 0.255.255.255 any

3. Match a specific range

- **Example 1**
- Address: 10.250.50.112 Subnet Mask: 255.255.255.224

```
                    255.255.255.255
Custom Subnet mask: -255.255.255.224
Wildcard:             0.   0.   0.  31
```

- Access-list 125 permit udp 10.250.50.112 0.0.0.31 any

3. Match a specific range

Cisco.com

Example 2

Address Range: 192.168.16.0 to 192.168.16.127

```
                 192.168.16.127
                -192.168.16.   0
                ---------------
Wildcard:         0.   0.  0.127
```

Access-list 125 deny ip 192.168.16.0 0.0.0.127 any

(This ACL would block the lower half of the subnet.)

4. Match everyone.

For standard access lists:

Access-List 15 permit any

or

Access-List 15 deny 0.0.0.0 255.255.255.255

For extended access lists:

Access-List 175 permit ip any any

or

Access-List 175 deny tcp 0.0.0.0 255.255.255.255 any eq 80