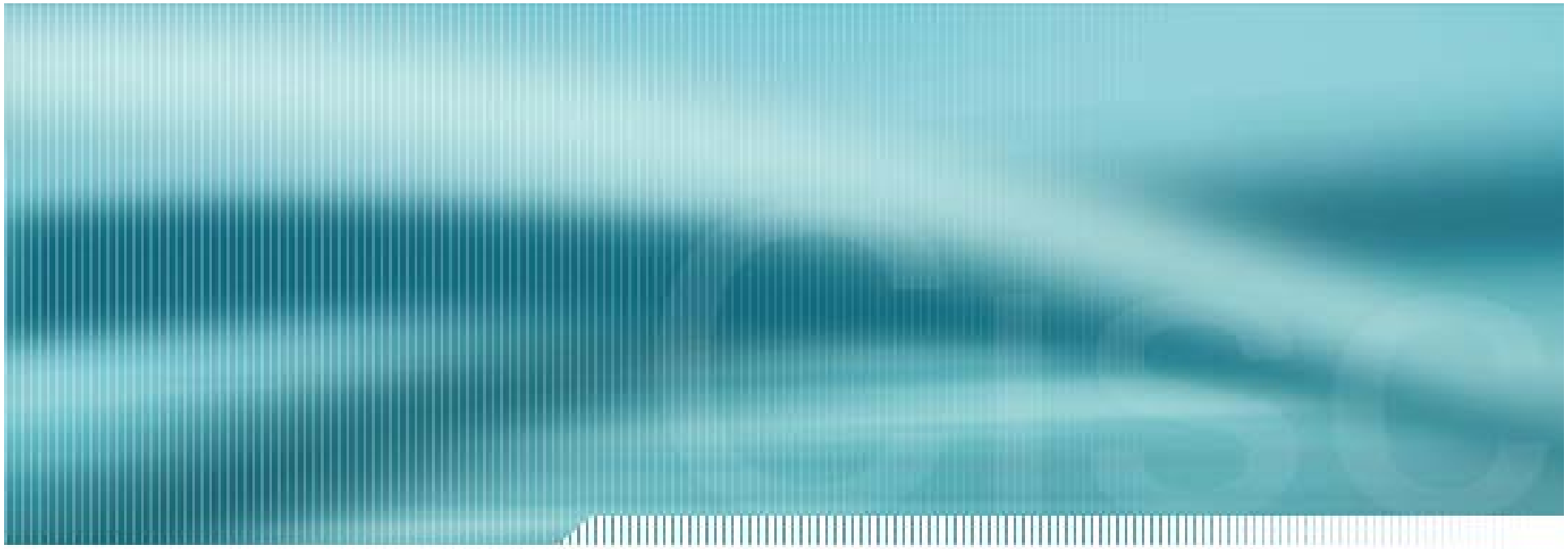


Security and Access Control Lists (ACLs)

Malin Bornhager

Halmstad University

Objectives

- **Security Threats**
- **Access Control List Fundamentals**
- **Access Control Lists (ACLs) Configuration**

Why is network security important?

- Networks have grown in both size and importance
- Loss of privacy, theft of information, legal liability
- The types of potential threats to network security are always evolving

Common Security Threats

Three common factors in network security:

- **Vulnerability**
  - Degree of weakness in routers, switches, desktops, servers, and security devices
  - Technological, configuration and security policy weaknesses
- **Threat**
  - People interested and qualified in taking advantage of each weakness
- **Attack**

Types of Network Attacks

- **Reconnaissance**
  - **Unauthorized discovery and mapping of systems, services or vulnerabilities**
- **Access**
  - **Gain access to a device**
- **Denial of Service (DoS)**
  - **Disables or corrupts networks**
- **Worms, viruses and Trojan horses**
  - **Damage or corrupt a system**

Host and Server Based Security

- Antivirus software
- Personal firewalls
- OS patches
- Intrusion Detection Systems (IDS) can detect attacks against a network and send logs to a management console
- Intrusion Prevention Systems (IPS) can prevent attacks from being executed

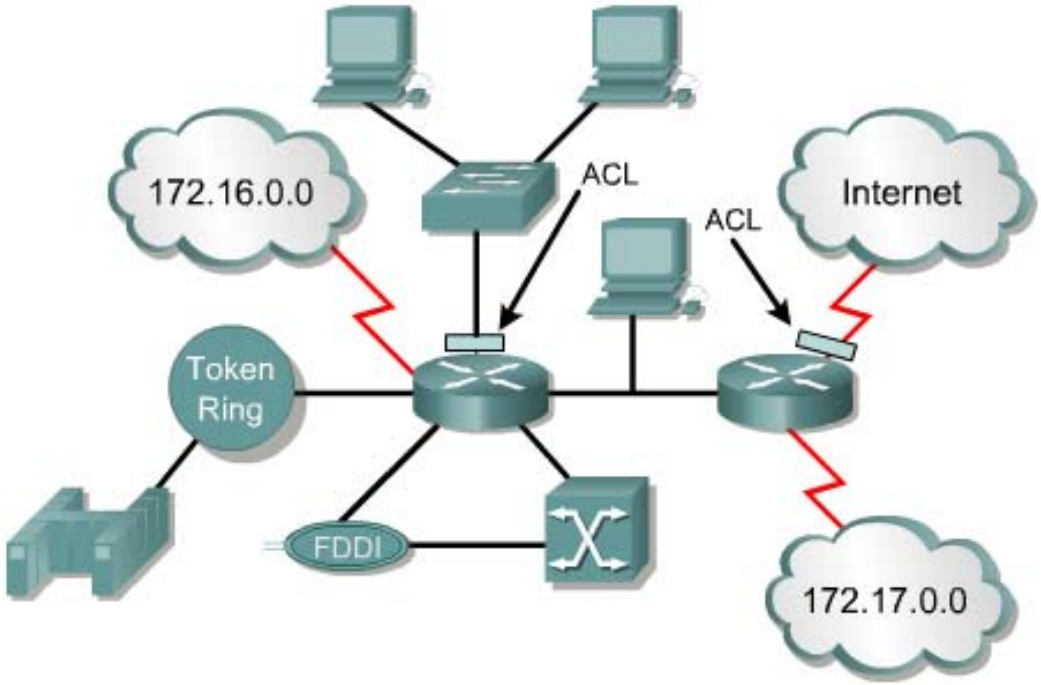
Router Security

- Manage router security
- Secure remote access
- Logging router activity
- Secure vulnerable router services and interfaces
- Secure routing protocols
- Control and filter network traffic
- SDM can be used to configure security features on Cisco IOS based routers

Security Device Manager - SDM

- **Cisco Router and Security Device Manager that simplifies router and security configuration**
- **Easy-to-use, web-based device-management tool**
- **Automatic router security management**
- **Supports a wide range of Cisco IOS software releases**

What are ACLs?



- **ACLs are lists of instructions you apply to a router's interface to tell the router what kinds of packets to accept and what kinds to deny.**

Introduction to ACLs

- **Lists of conditions**
- **Filter network traffic**
- **Accept or Deny**
- **Secure access to and from a network**

Introduction to ACLs

- Per protocol
  - IP
  - IPX
  - AppleTalk
- Per direction
  - In
  - Out
- Per port

Example

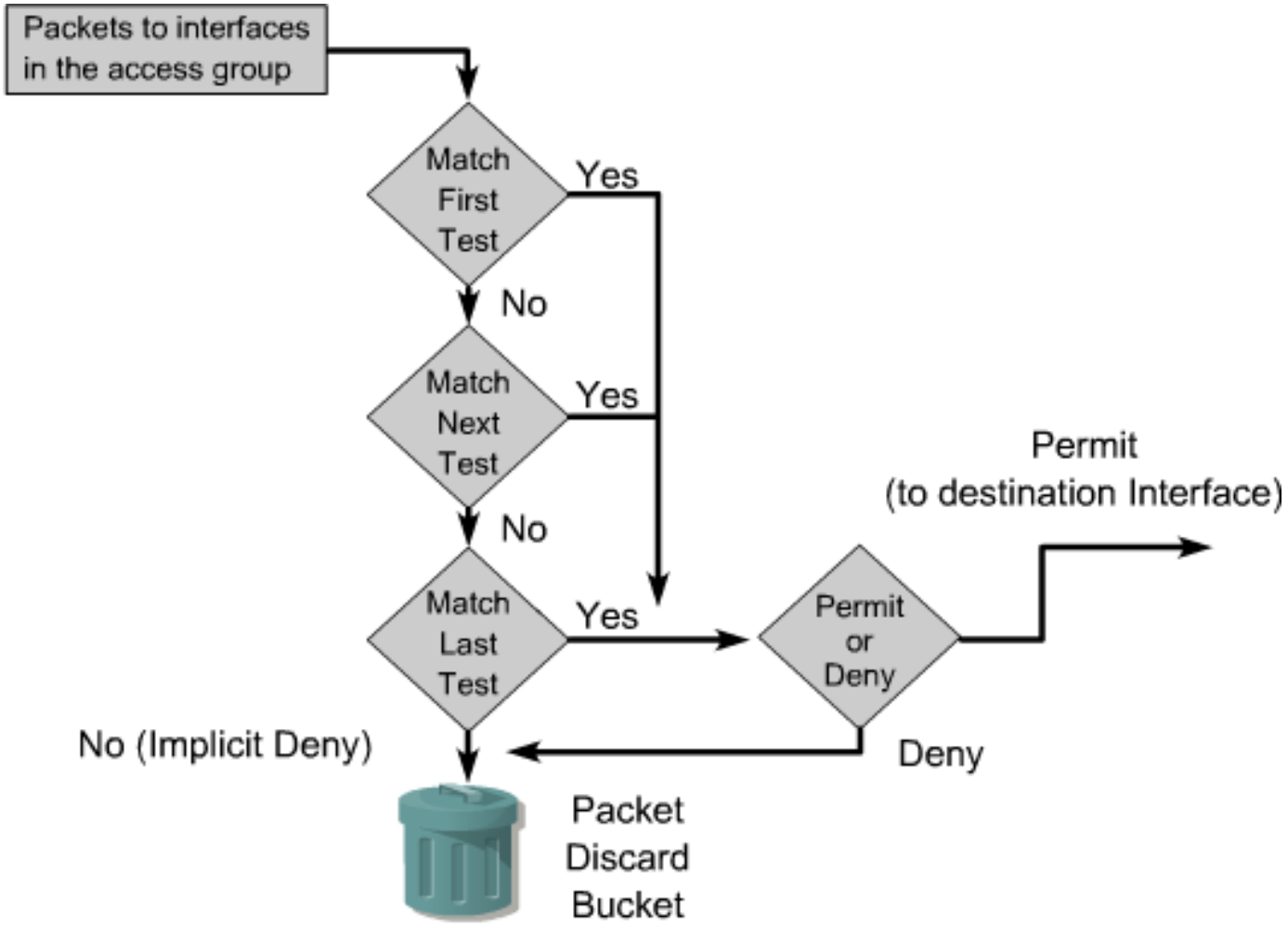
One list per interface, per direction, and per protocol

With two interfaces and three protocols running, this router could have a total of 12 separate ACLs applied.

ACLs can be used to:

- **Limit network traffic and increase network performance**
- **Provide traffic flow control (restrict routing updates)**
- **Basic level of security for network access**
- **Traffic types forwarded or blocked**
- **Control access to areas**
- **Permit or deny host access to network segment**

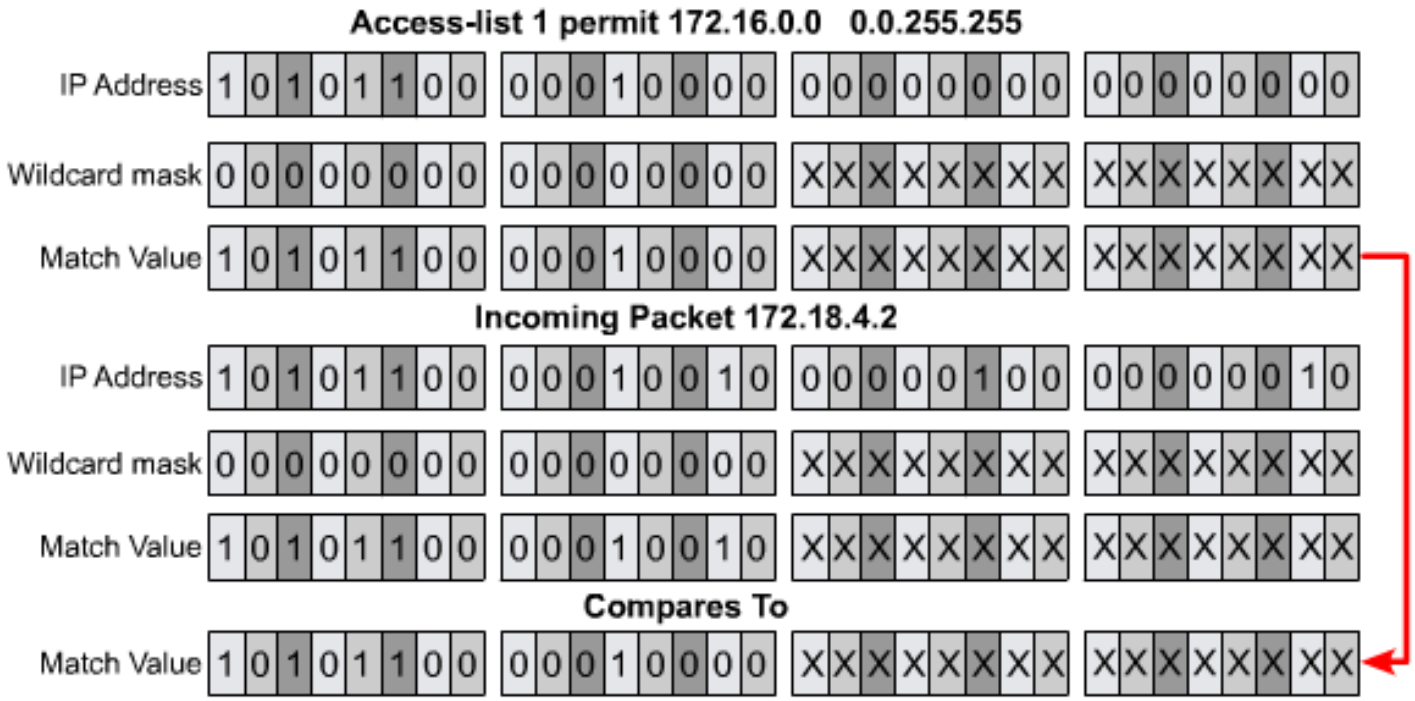
How ACLs Work



Protocols with ACLs Specified by Numbers

Protocol	Range
IP	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

The Function of a Wildcard Mask



The incoming composite value is compared to the internal match value.

Standard ACLs

```
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
```

- Access list number range of 1-99
- Filter only on source IP address
- Wildcard masks
- Applied to port closest to destination

Extended ACLs

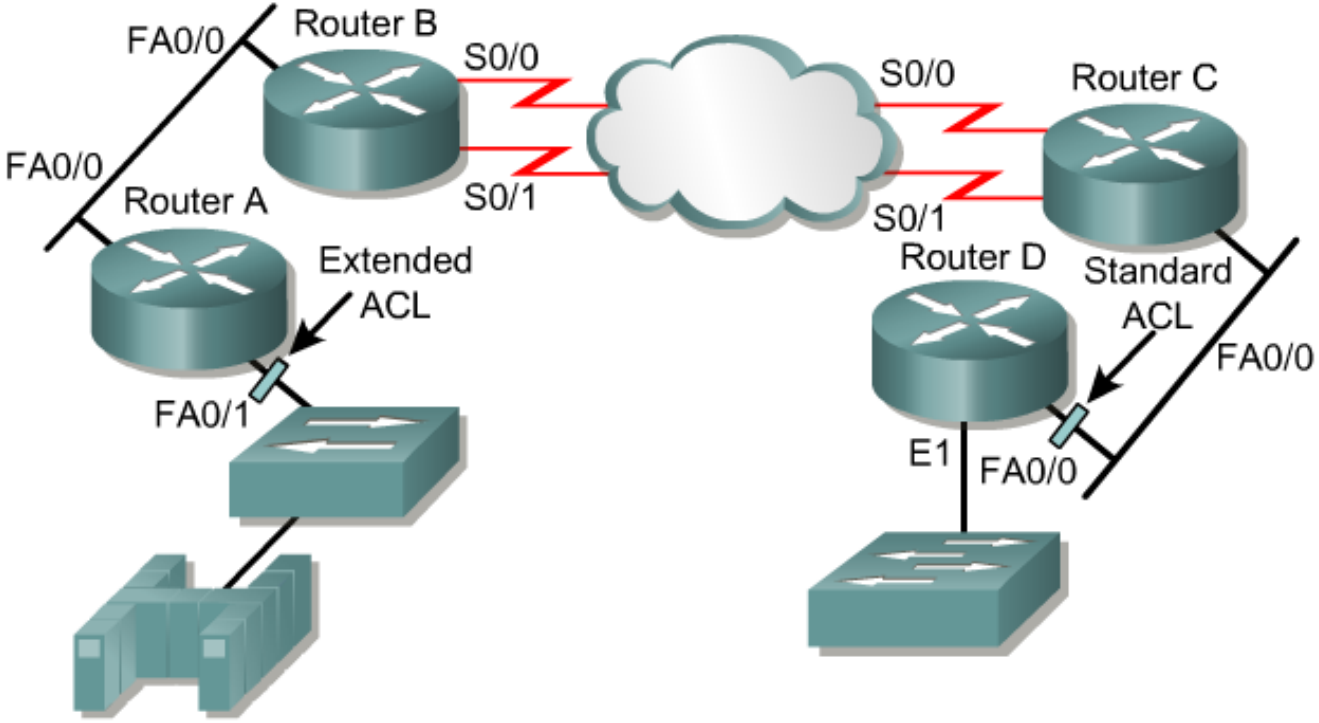
```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

- Access list number range of 100-199
- Source destination IP address
- Layer 4 protocol number
- Applied to port closest to source host

Named ACLs

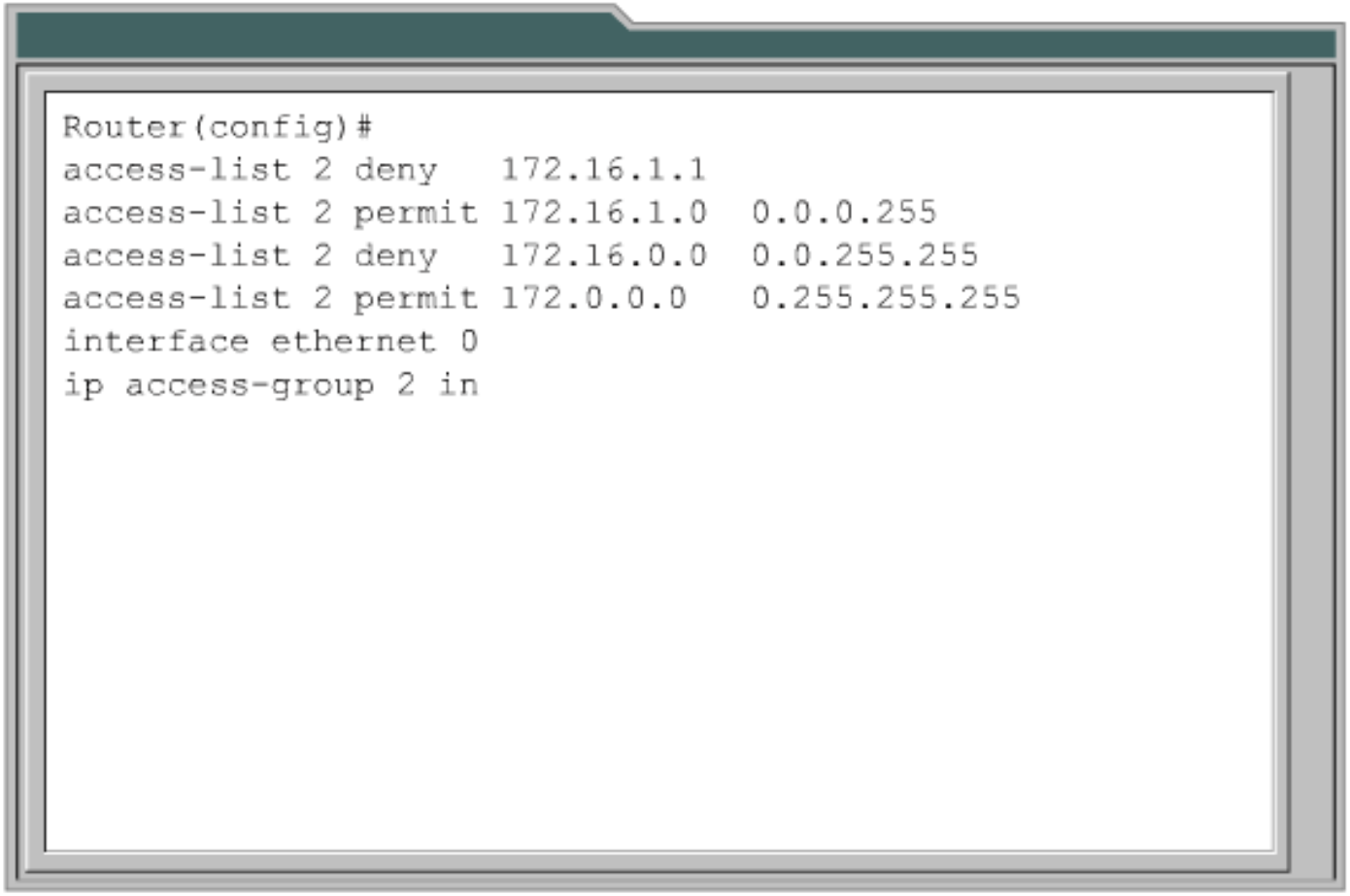
```
Rt1(config)#ip access-list extended server-access
Rt1(config-ext-nacl)#permit TCP any host 131.108.101.99 eq
smtp
Rt1(config-ext-nacl)#permit UDP any host 131.108.101.99 eq
domain
Rt1(config-ext-nacl)#deny ip any any log
Rt1(config-ext-nacl)#^Z
Applying the named list:
Rt1(config)#interface fastethernet 0/0
Rt1(config-if)#ip access-group server-access out
Rt1(config-if)#^Z
```

Placing ACLs



- **Standard ACLs should be placed close to the destination.**
- **Extended ACLs should be placed close to the source.**

Creating ACLs



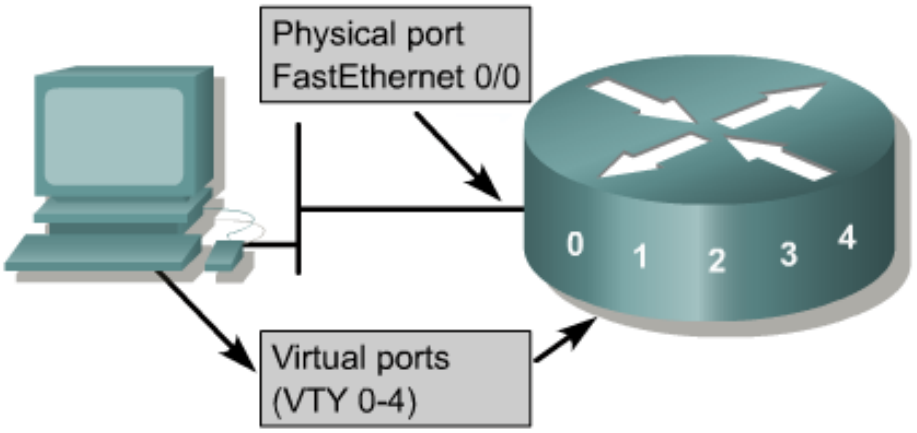
Verifying ACLs

- **There are many `show` commands that will verify the content and placement of ACLs on the router.**
  - **`show ip interface`**
  - **`show access-lists`**
  - **`Show running-config`**

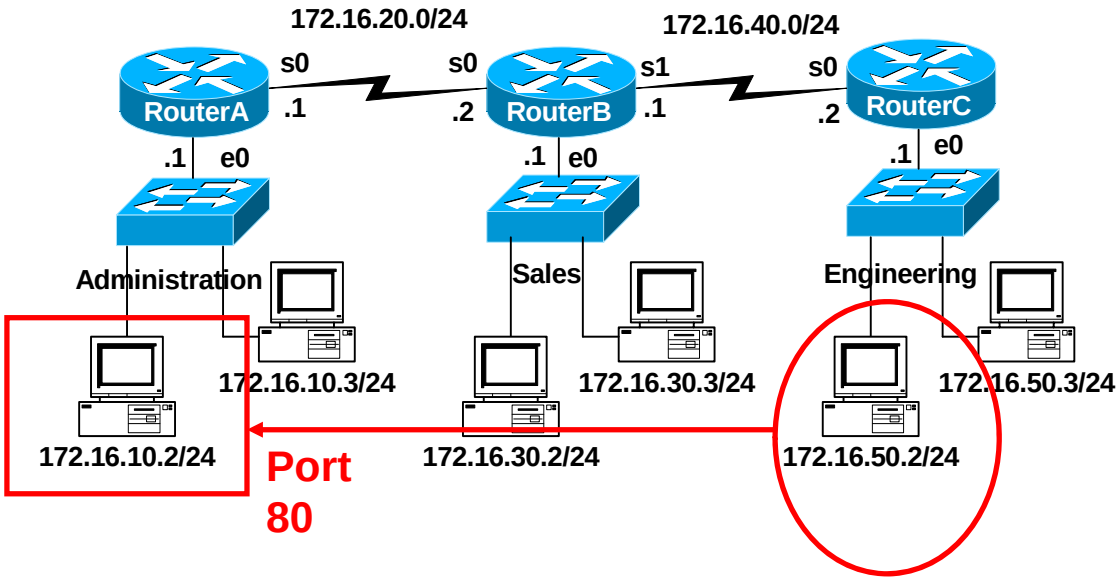
Restricting Virtual Terminal Access

Cisco - Hyperterminal

```
Creating the standard list:

Rt1(config)#access-list 2 permit 172.16.1.0 0.0.0.255
R11(config)#access-list 2 permit 172.16.2.0 0.0.0.255
R11(config)#access-list 2 deny any

Applying the access list:

Rt1(config)#line vty 0 4
Rt1(config)#login
Rt1(config)#password secret
Rt1(config)#access-class 2 in
```



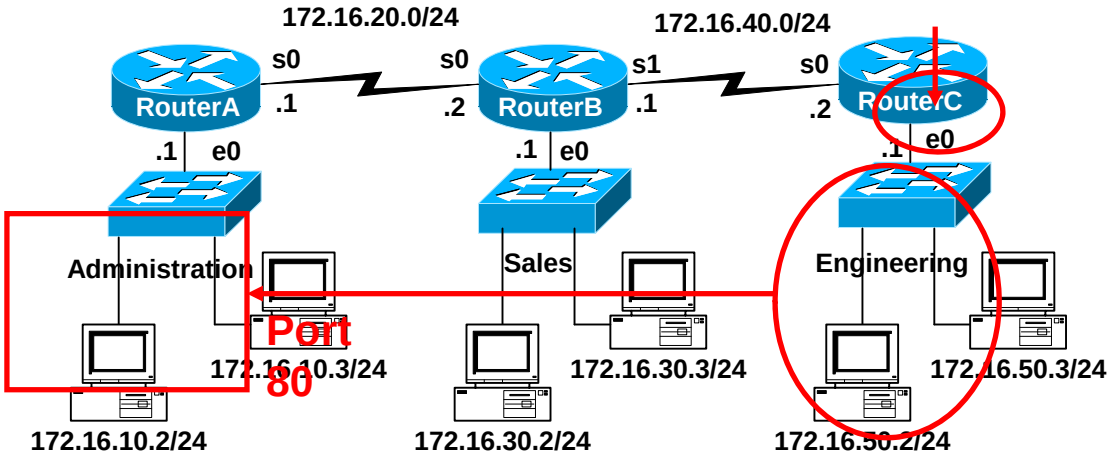
Example



Task

- What if we want to deny only the Engineering workstation 172.16.50.2 to be able to access the web server in Administrative network with the IP address 172.16.10.2 and port address 80.
- All other traffic is permitted.

Example




```
RouterC(config)#access-list 110 deny tcp host 172.16.50.2 host
   172.16.10.2 eq 80
RouterC(config)#permit any any
RouterC(config)#interface e 0
RouterC(config-if)#ip access-group 110 in
```

- Why is better to place the ACL on RouterC instead of RouterA?
- Why is the e0 interface used instead of s0 on RouterC?

Summary

- List of permit and deny statements
- Order of statements important
- Placement of ACLs important
- 32-bit wildcard mask
- Standard ACLs check the source
- Extended ACLs provides a greater range of control