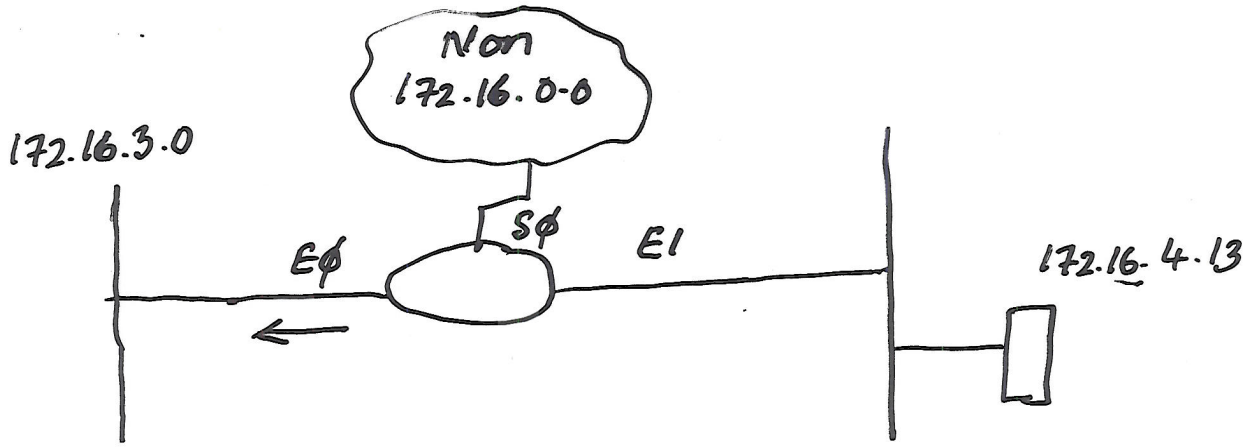
Extended Access Lists

Well-known Port	IP Protocol
20 (TCP)	FTP data
21 (TCP)	FTP control
23 (TCP)	Telnet
25 (TCP)	SMTP
53 (TCP/UDP)	DNS
69 (UDP)	TFTP
80 (TCP)	HTTP

Range: 100 - 199



access-List 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

" " " " " " eq 20

access-list 101 ~~deny~~ permit ip any any

(implicit deny all)

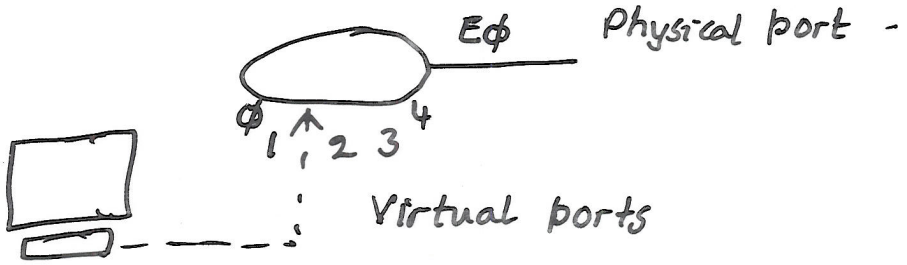
(1)

interface ethernet 0
ip access-group 101 out

VIRTUAL TERMINAL LINE COMMANDS:

```
Router (config)#
    line vty { vty # | vty-range}
```

```
Router (config-line)#
    access-class access-list-number {in|out}
```




```
access-list 12 permit 192.89.55.0 0.0.0.255

line vty ϕ 4
 access-class 12 in
```

Permits any device on network 192.89.55.0 to establish a virtual terminal (Telnet) session with the router. (Needs passwords)

Implicit deny all still applies to the access list..

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
access_list 101 permit ip any any

interface e0
 ip access-group 101 out
```

(2)

(1) DENY FTP FROM SUBNET 172.16.4.0 to SUBNET 172.16.3.0

PERMIT ALL OTHER IP TRAFFIC OUT INTERFACE E0.

(2) DENY Telnet traffic from Subnet 172.16.4.0 out of interface e0

All other IP traffic from any source to any destination is permitted out e0.

PLACE MORE SPECIFIC STATEMENTS FIRST

NO REORDERING OR REMOVAL OF STATEMENTS

USE no access-list numbr TO REMOVE

ENTIRE ACCESS LIST

IMPLICIT DENY ALL

EXTENDED ACCESS LISTS SHOULD NORMALLY BE PLACED AS CLOSE AS POSSIBLE TO THE SOURCE OF THE TRAFFIC TO BE DENIED.

STANDARD ALs – NO DESTINATION @

∴ PLACE IT AS NEAR THE DESTINATION AS POSSIBLE.

VERIFYING AL:

show ip int eth

MONITORING AL:

show ip access-lists