Named ACL Example

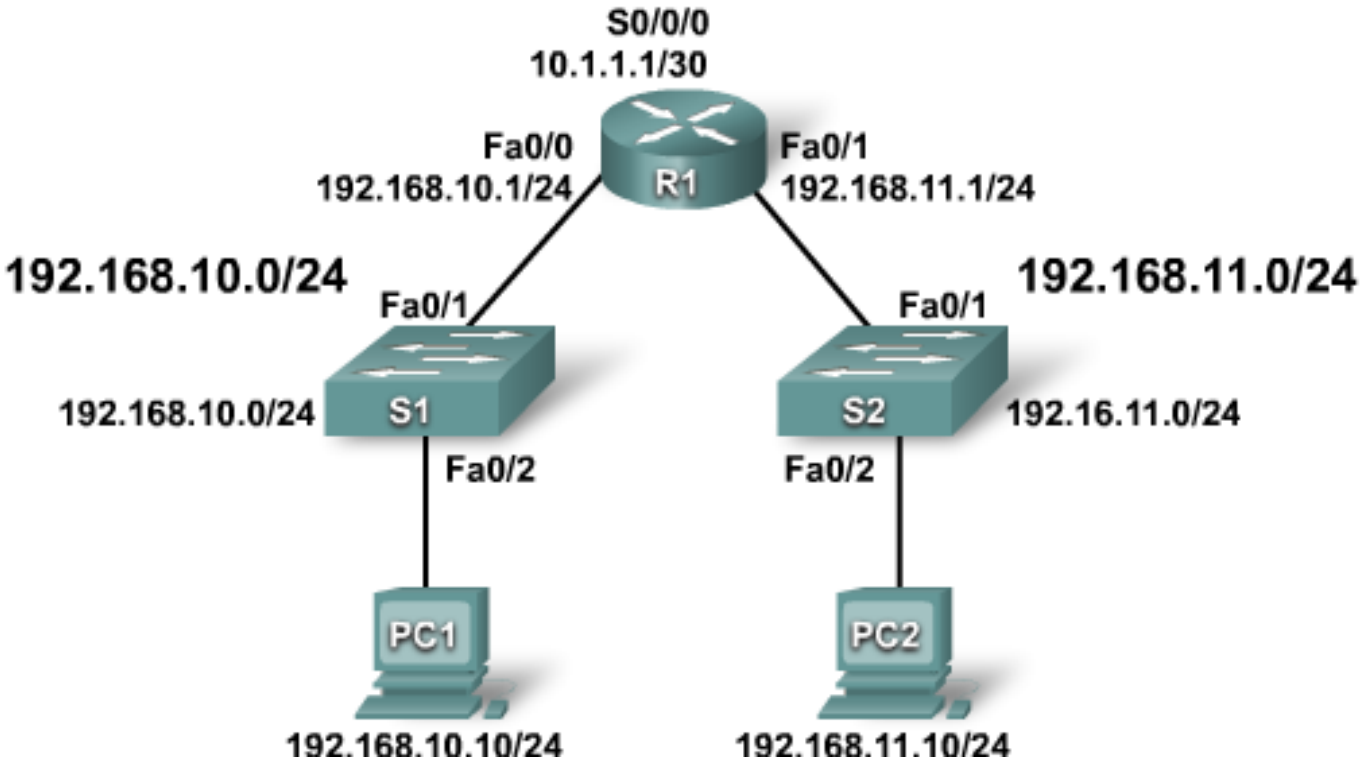
```
Router(config)# ip access-list [standard | extended] name
```

- Alphanumeric name string must be unique and cannot begin with a number

```
Router(config-std-nacl)# [permit | deny | remark] {source [source-
wildcard]} [log]
```

```
Router(config-if)#ip access-group name [in | out]
```

- Activates the named IP ACL on an interface




```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#interface Fa0/0
R1(config-if)#ip access-group NO_ACCESS out
```

Monitoring ACL Statements

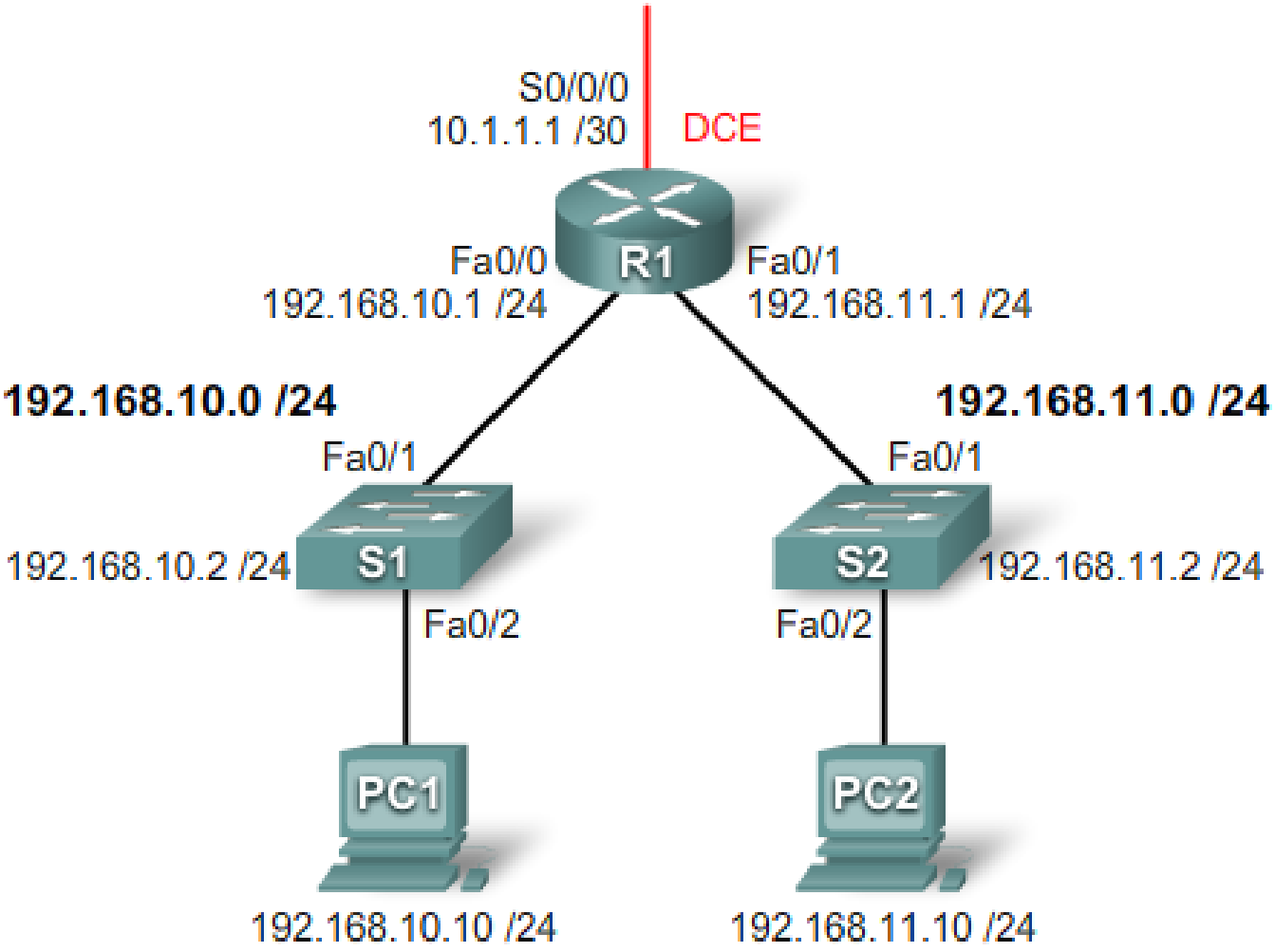
```
R1# show access-lists {access-list-number|name}
```

```
R1# show access-lists
Standard IP access list SALES
    10 deny   10.1.1.0 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 192.168.10.2 any eq telnet (25 matches)
    20 permit tcp host 192.168.10.2 any eq ftp
    30 permit tcp host 192.168.10.2 any eq ftp-data
```

Editing ACLs

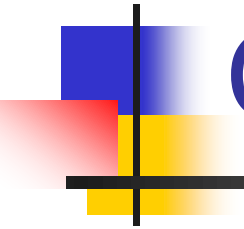
- **Numbered ACLs:** there is no built-in editing feature that allows you to edit a change in an ACL. You cannot selectively insert or delete lines.
- **Named ACLs:** Named ACLs have a big advantage over numbered ACLs in that they are easier to edit.
  - **named IP ACLs allow you to delete individual entries in a specific ACL.**
  - **You can use sequence numbers to insert statements anywhere in the named ACL.**
  - **!!! If you are using an earlier Cisco IOS software version, you can add statements only at the bottom of the named ACL.**

Adding a Line to a Named ACL



Adding a Line to a Named ACL

```
R1# show access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard WEBSERVER
R1(config-std-nacl)# 15 permit host 192.168.11.10
R1(config-std-nacl)# end
R1#
*Nov  1 19:20:57.591: %SYS-5-CONFIG_I: Configured from console by console
R1# sho access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    15 permit 192.168.11.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1#
```



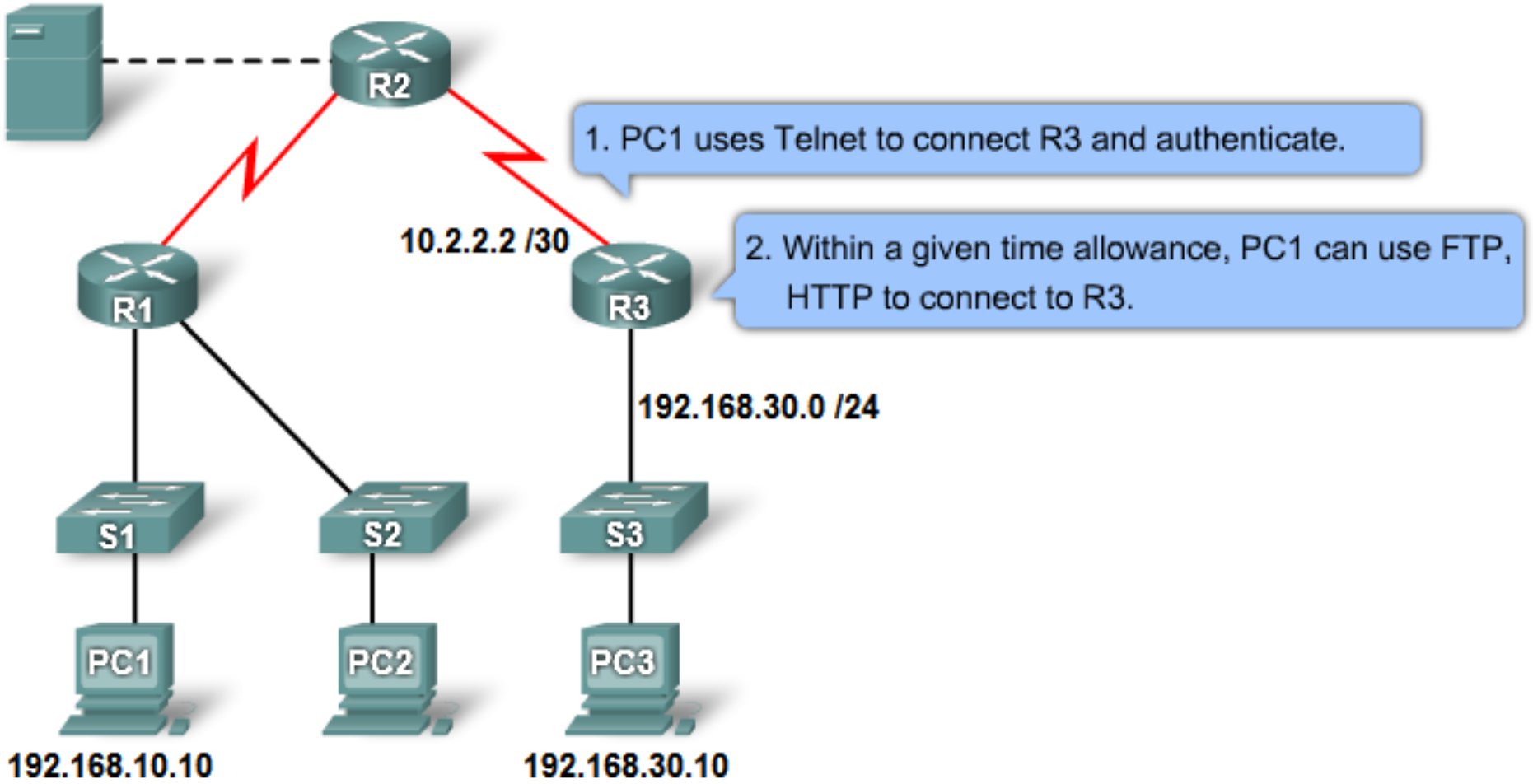
Complex ACL

CCNA

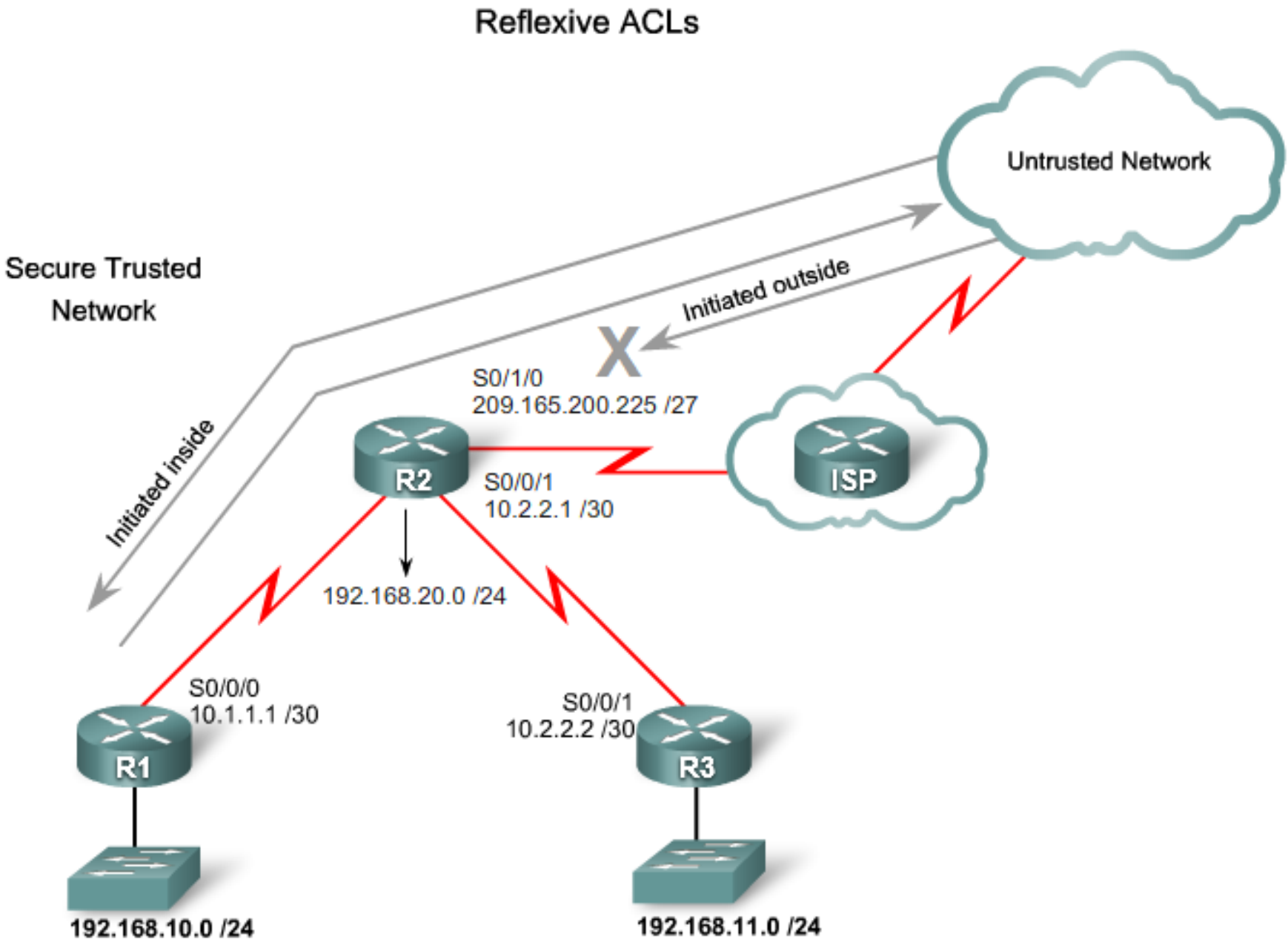
Types of Complex ACLs

Complex ACL	Description
Dynamic ACLs (lock-and-key)	Users that want to traverse the router are blocked until they use Telnet to connect to the router and are authenticated
Reflexive ACLs	Allows outbound traffic and limits inbound traffic in response to sessions that originate inside the router
Time-based ACLs	Allows for access control based on the time of day and week

Dynamic ACLs



Step 1	R3(config)#username Student password 0 cisco
Step 2	R3(config)# access-list 101 permit any host 10.2.2.2 eq telnet R3(config)#access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
Step 3	R3(config)#interface serial 0/0/1 R3(config-if)#ip access-group 101 in
Step 4	R3(config)#line vty 0 4 R3(config-line)#login local R3(config-line)# autocommand access-enable host timeout 5


Reflexive ACLs
Untrusted Network
Secure Trusted Network
Initiated outside
Initiated inside
S0/1/0
209.165.200.225 /27
R2
S0/0/1
10.2.2.1 /30
ISP
192.168.20.0 /24
S0/0/0
10.1.1.1 /30
S0/0/1
10.2.2.2 /30
R1
R3
192.168.10.0 /24
192.168.11.0 /24

Step 1

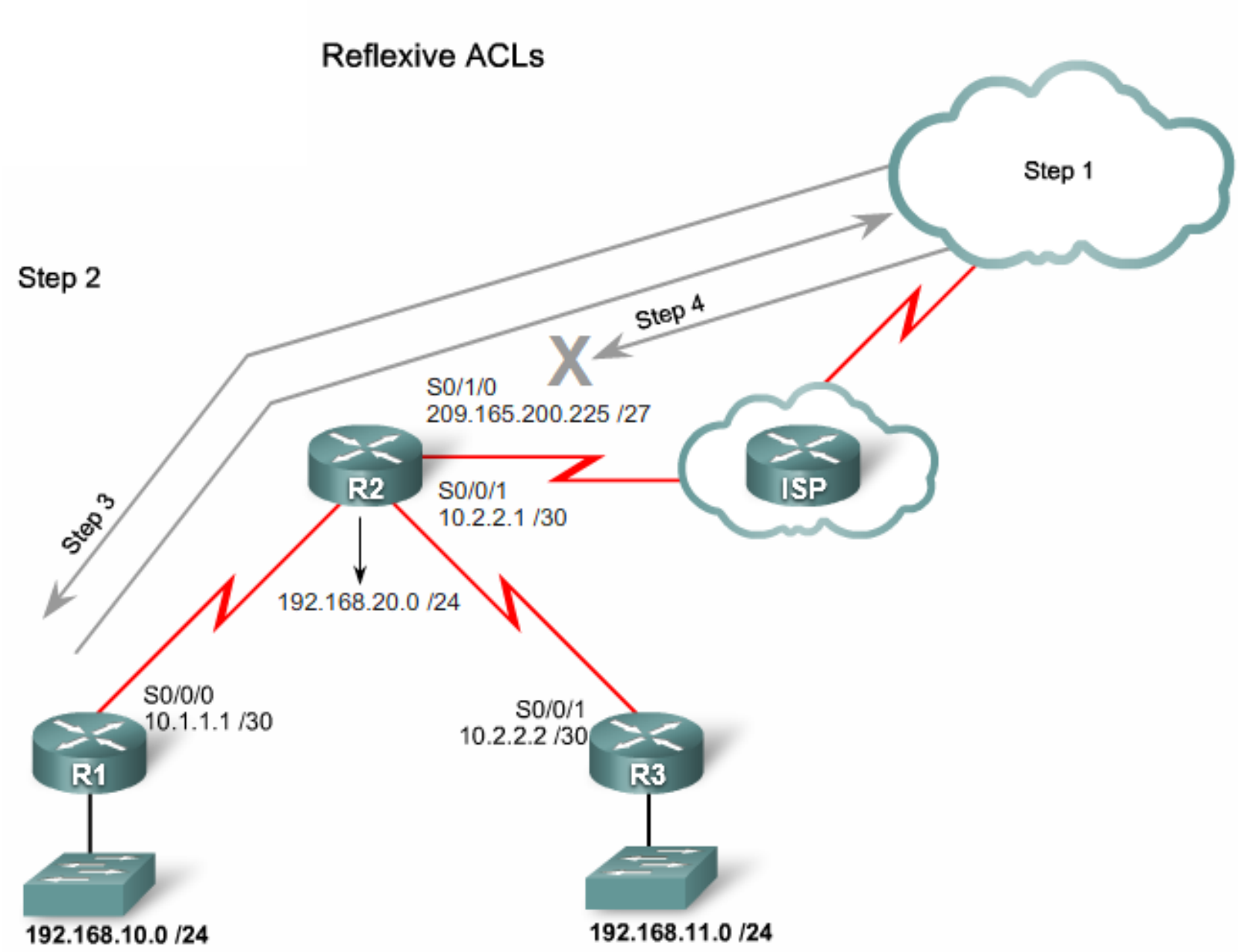
```
R2(config)#ip access-list extended OUTBOUNDFILTERS
R2(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255 any
reflect TCPTRAFFIC
R2(config-ext-nacl)# permit icmp 192.168.0.0 0.0.255.255 any
reflect ICMPTRAFFIC
```

Step 2

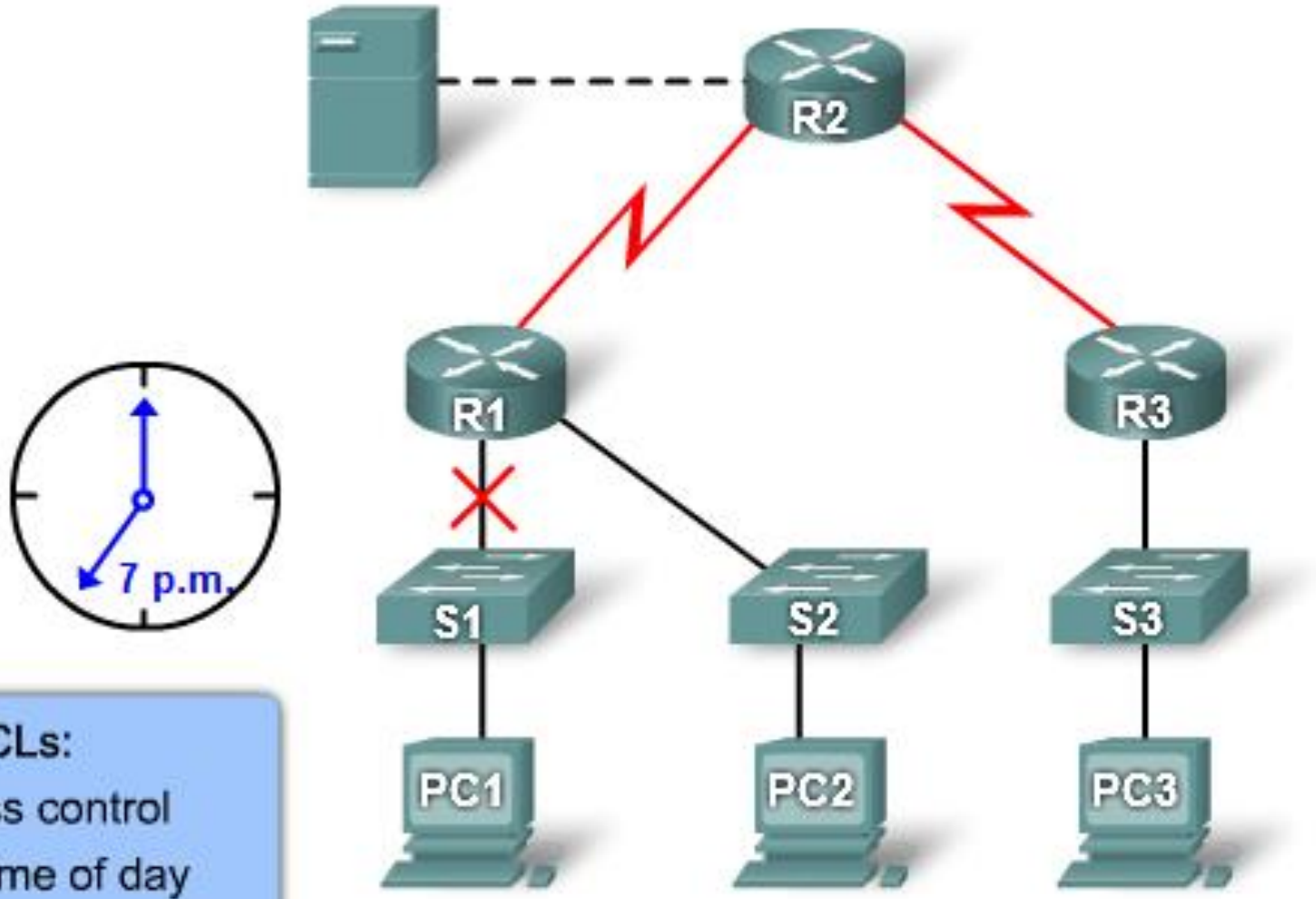
```
R2(config)#ip access-list extended INBOUNDFILTERS
R2(config-ext-nacl)# evaluate TCPTRAFFIC
R2(config-ext-nacl)# evaluate ICMPTRAFFIC
```

Step 3

```
R2(config)#interface S0/1/0
R2(config-if)#ip access-group INBOUNDFILTERS in
R2(config-if)#ip access-group OUTBOUNDFILTERS out
```

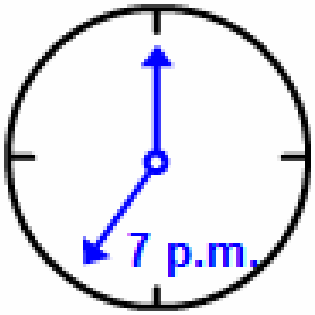

Reflexive ACLs
Step 1
Step 2
Step 3
Step 4
X
S0/1/0
209.165.200.225 /27
R2
S0/0/1
10.2.2.1 /30
ISP
192.168.20.0 /24
S0/0/0
10.1.1.1 /30
R1
S0/0/1
10.2.2.2 /30
R3
192.168.10.0 /24
192.168.11.0 /24

Time-based ACLs

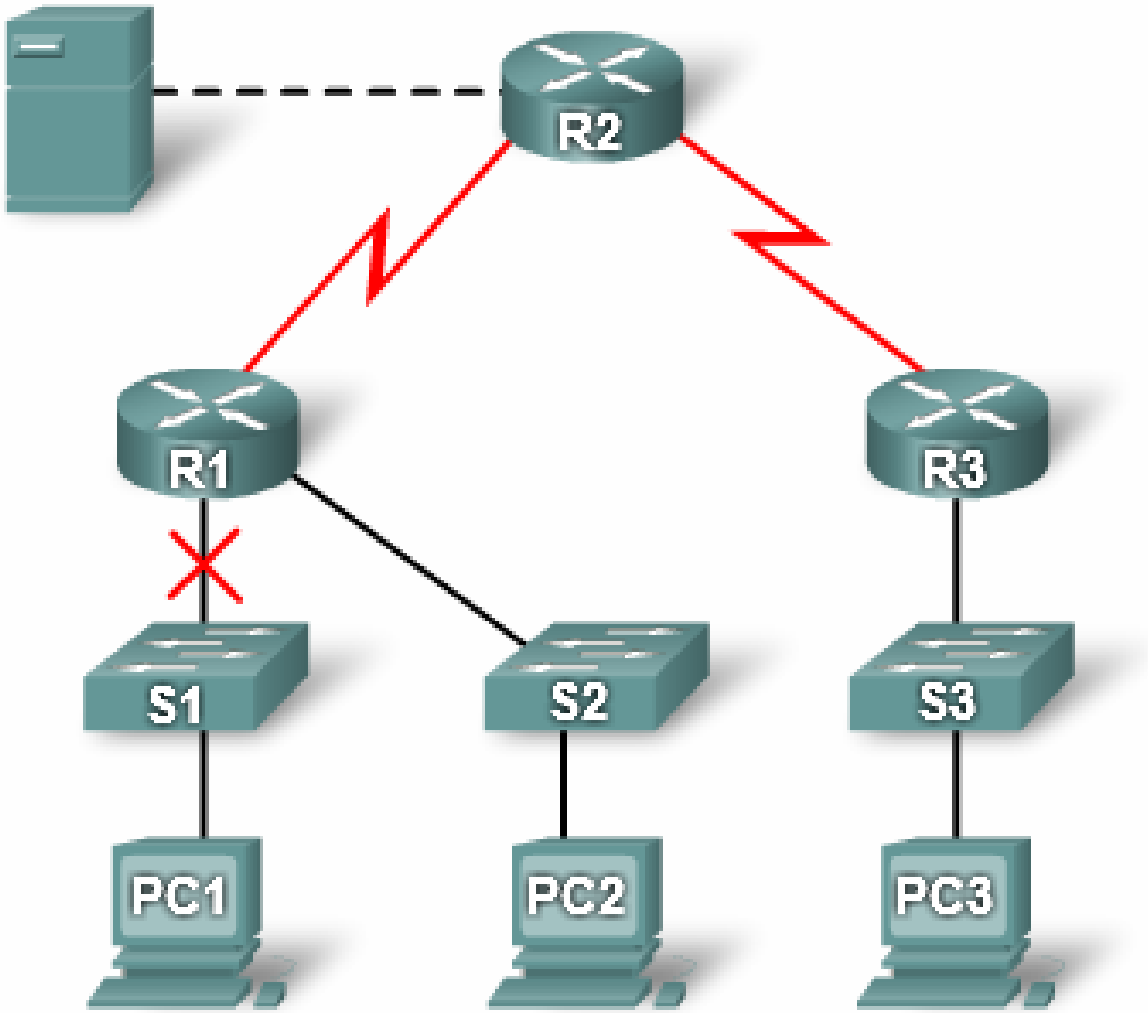


Time-based ACLs:
Allow for access control based on the time of day and week

Step 1	R1(config)#**time-range EVERYOTHERDAY** R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00**
Step 2	R1(config)#**access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY**
Step 3	R1(config)#**interface s0/0/0** R1(config-if)#**ip access-group 101 out**

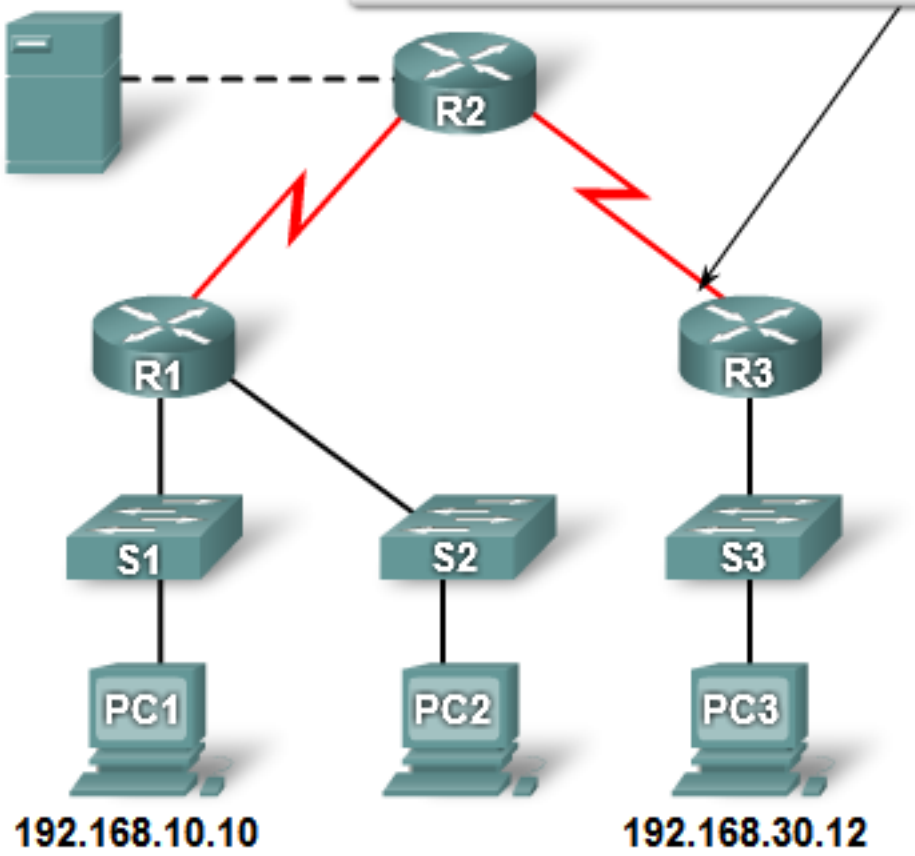


Time-based ACLs:
Allow for access control based on the time of day and week



Troubleshooting Common ACL Errors

```
# show access-lists 10
    10 deny tcp 192.168.10.0 0.0.0.255 any
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

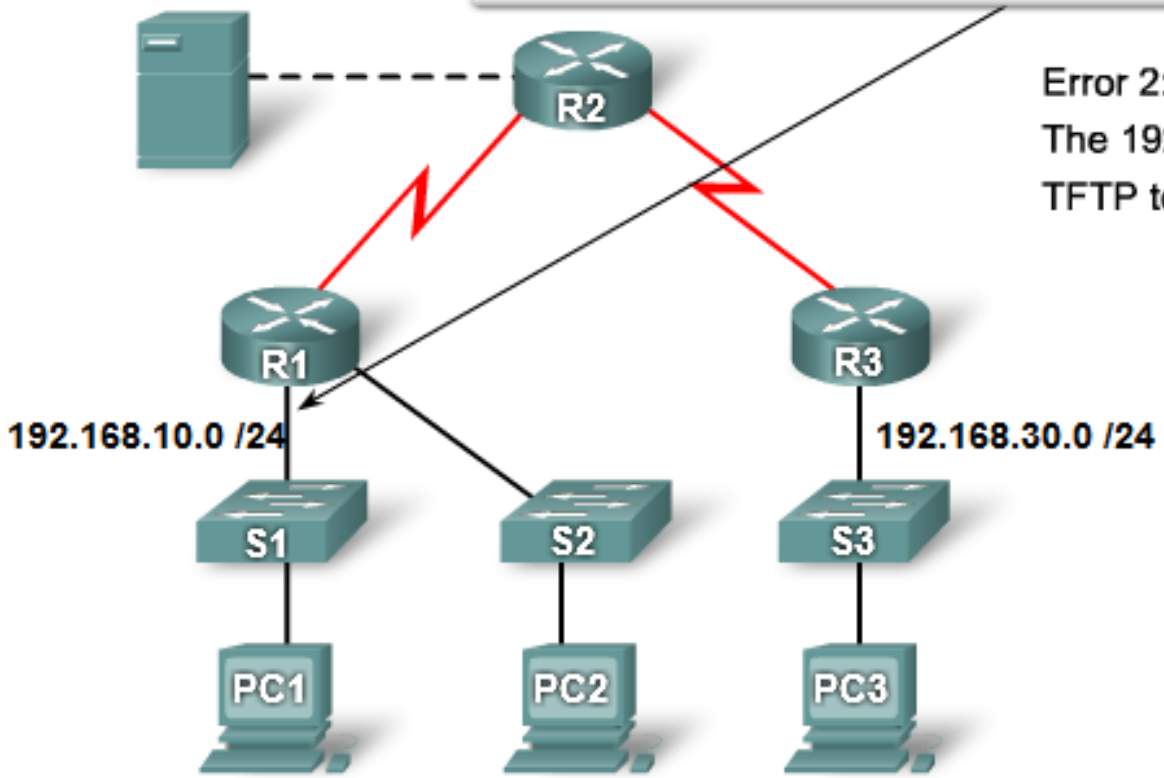


Error 1:

Host 192.168.10.10 has no connectivity with 192.168.30.12

Troubleshooting Common ACL Errors

```
# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.255.255 any eq telnet
    20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
    30 permit tcp any any
```

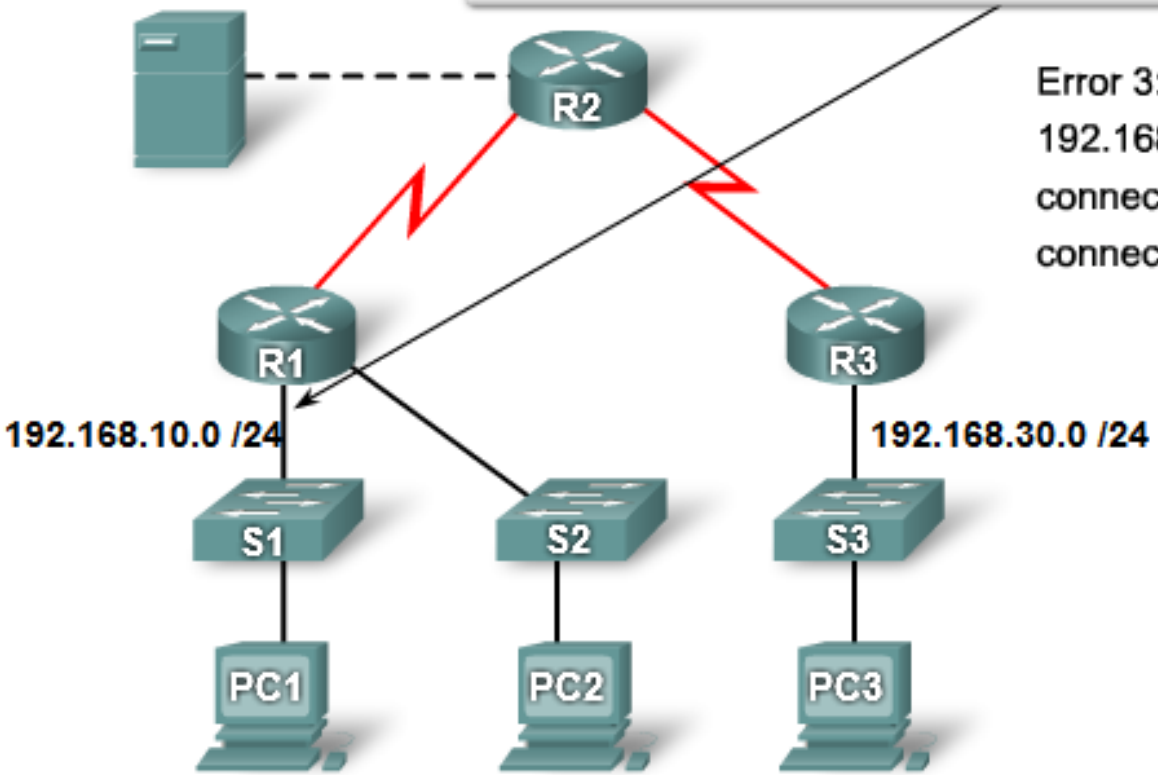


Error 2:

The 192.168.10.0 /24 network cannot use TFTP to connect to the 192.168.30.0 /24.

Troubleshooting Common ACL Errors

```
# show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.1.0 0.0.0.255 host 192.168.30.0 eq smtp
    30 permit ip any any
```

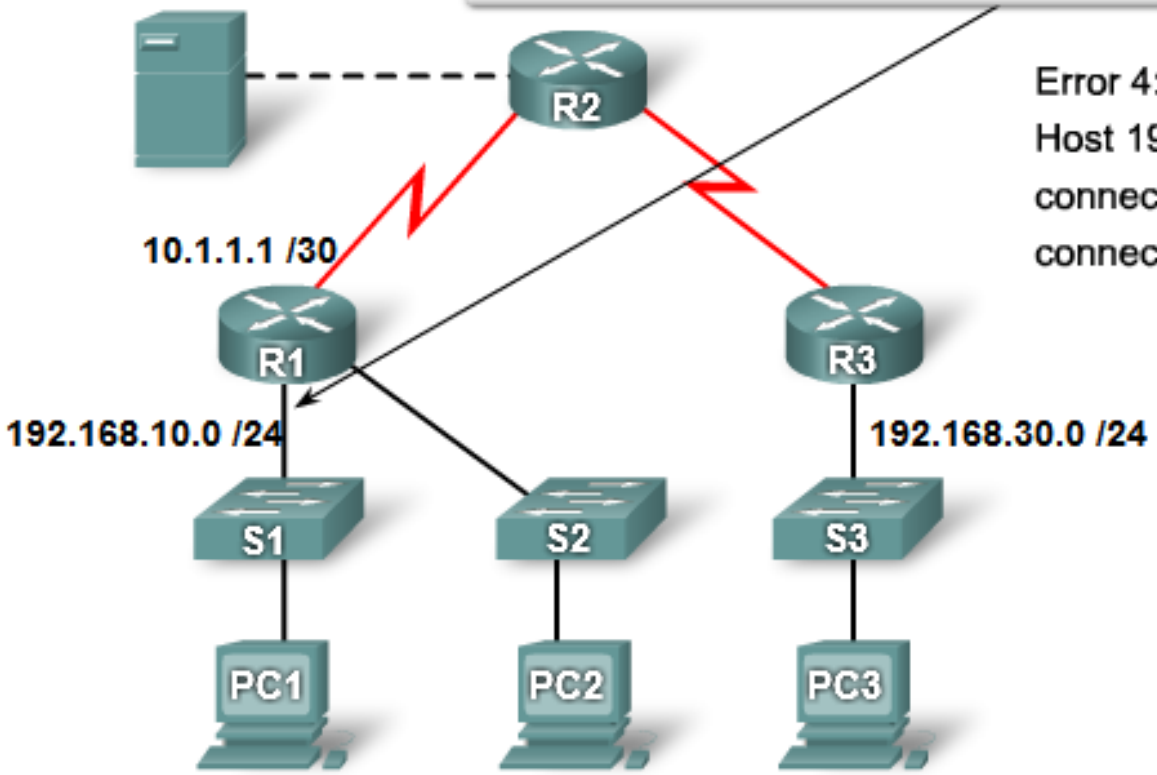


Error 3:

192.168.10.0 /24 network can use Telnet to connect to 192.168.30.0 /24, but this connection should not be allowed.

Troubleshooting Common ACL Errors

```
# show access-lists 140
Extended IP access list 140
10 deny tcp host 192.168.10.1 0.0.0.255 any eq telnet
   20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
   30 permit ip any any
```

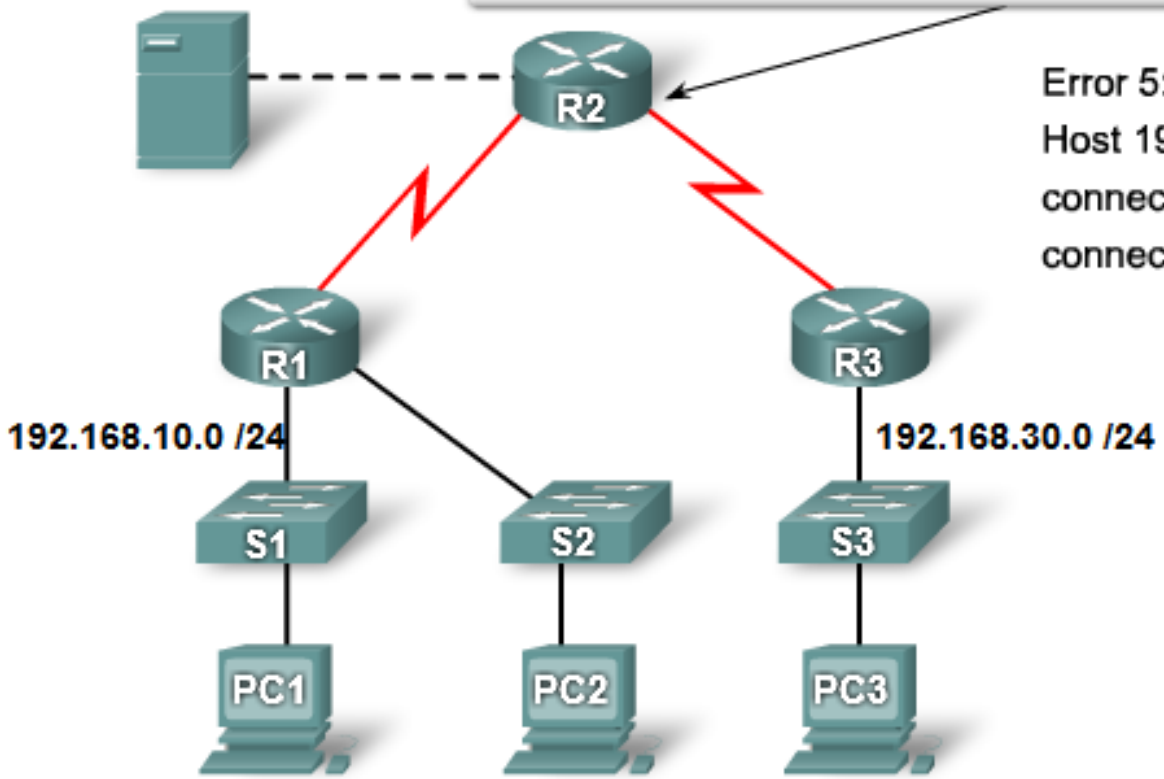


Error 4:

Host 192.168.10.10 can use Telnet to connect to 192.168.30.12, but this connection should not be allowed.

Troubleshooting Common ACL Errors

```
# show access-lists 150
Extended IP access list 150
    10 deny tcp host 192.168.30.12 any eq telnet
    20 permit ip any any
```



Error 5:

Host 192.168.30.12 can use Telnet to connect to 192.168.10.10, but this connection should not be allowed.

حالات خاصة

- لمنع الاتصال بالأنترنت يمكن استخدام WWW بدلاً من رقم البوابة
  - Deny ip 192.168.0.0 0.0.255.255 any eq WWW
- للسماح بالإجابة على اتصال TCP ومنع تأسيس اتصال TCP نستخدم established
  - Permit tcp 192.168.0.0 0.0.255.255 any established
- للسماح بالإجابة فقط على أي رسالة ping
  - Permit icmp 192.168.0.0 0.0.255.255 any echo-reply

Public and Private Internet Addresses

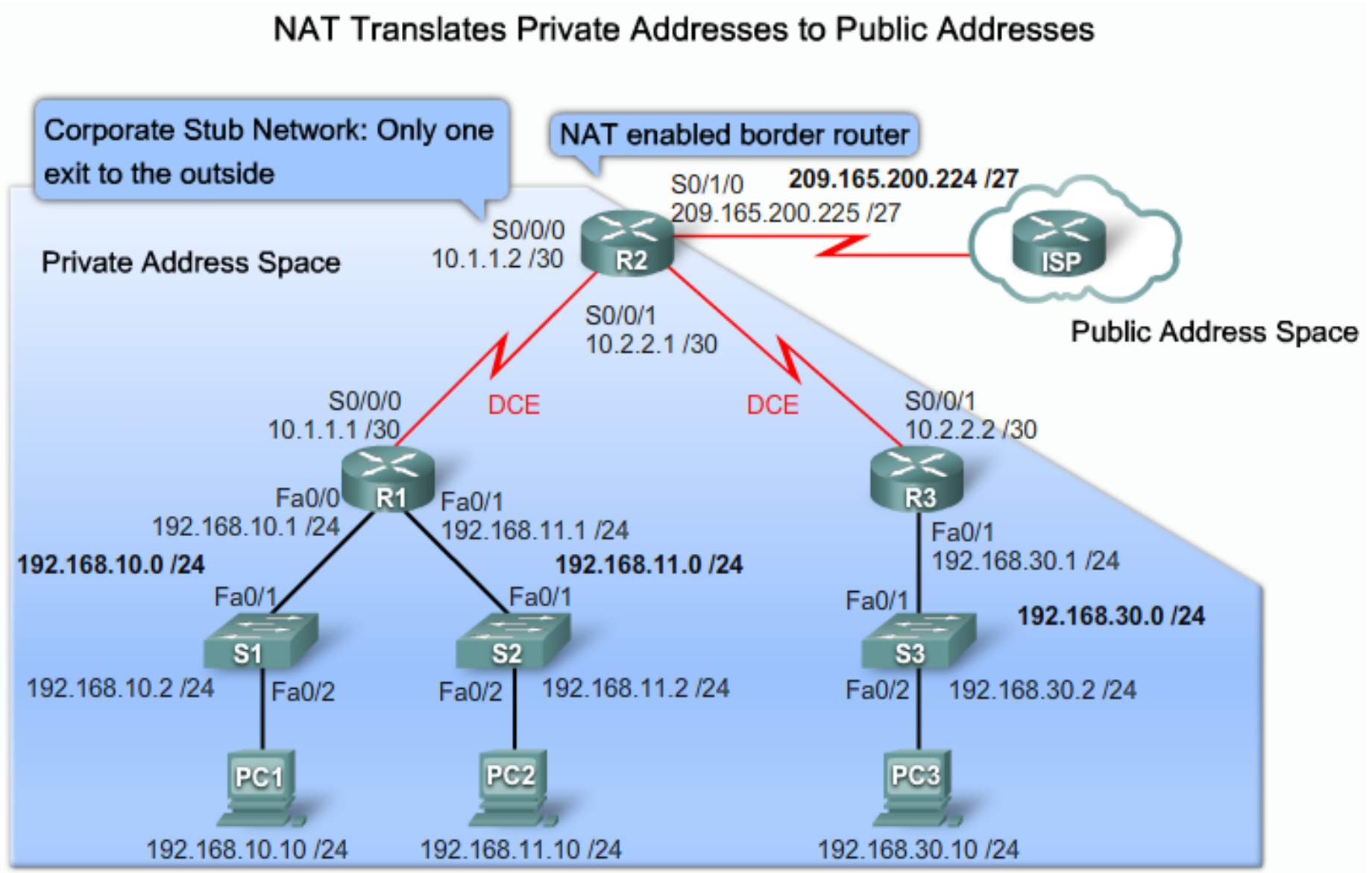
Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

- ARIN
- RIPE
- APNIC
- LACNIC
- AfriNIC

Private Internet addresses are defined in RFC 1918:

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

NAT Translates Private Addresses to Public Addresses



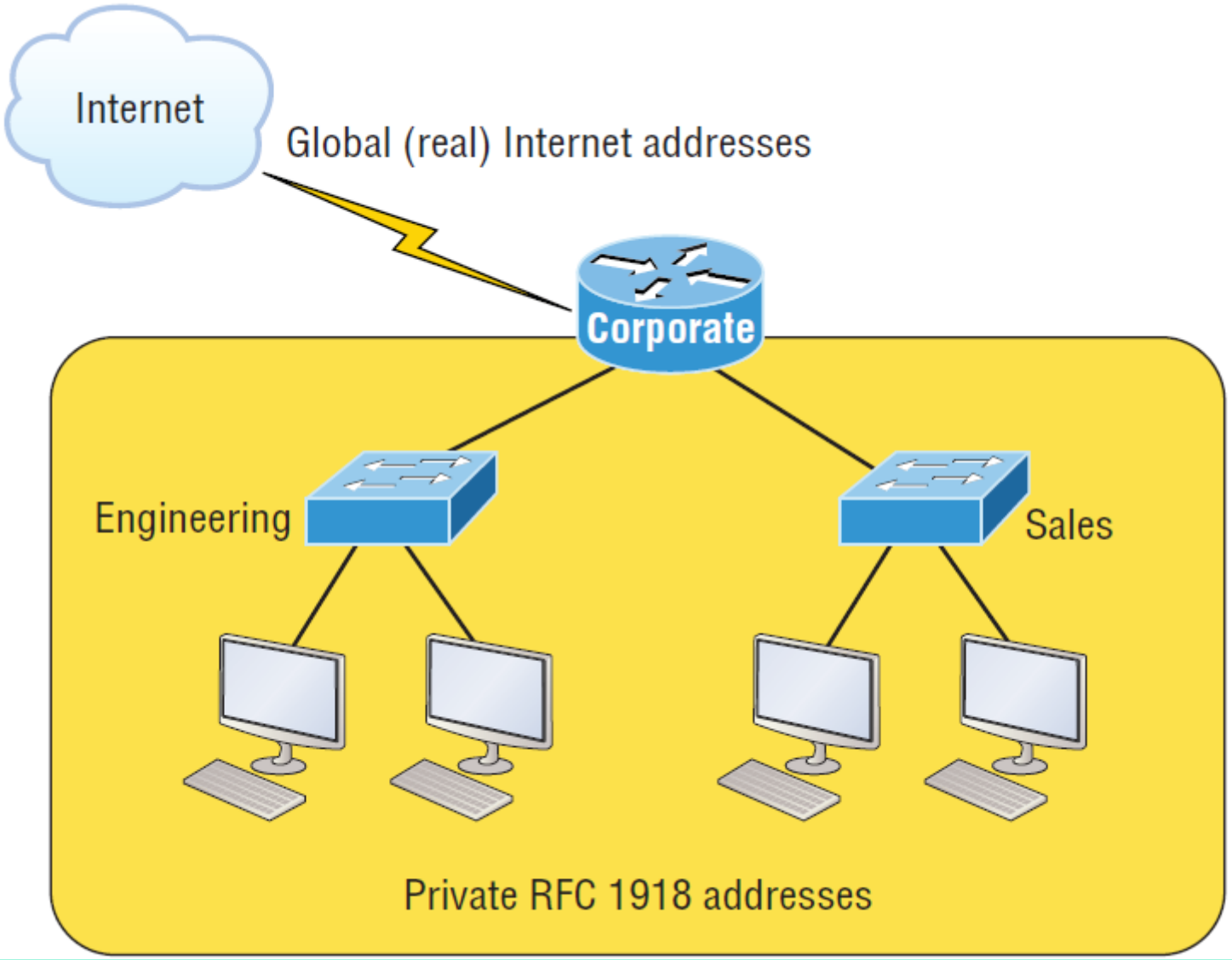
When Do We Use NAT?

- ***Network Address Translation (NAT)*** is similar to **Classless Inter-Domain Routing (CIDR)** in that the original intention for NAT was to slow the depletion of available IP address space by **allowing multiple private IP addresses to be represented by a much smaller number of public IP addresses**.
- A useful tool for **network migrations** and mergers, **server load sharing**, and **creating "virtual servers."**
- decreases the overwhelming **amount of public IP** addresses required in a networking environment
- use when an organization **changes its Internet service provider (ISP)** but the networking manager needs to avoid the hassle of changing the internal address scheme.

situations when NAT can be especially helpful

- When you need to connect to the Internet and your hosts don’t have globally unique IP addresses
- When you’ve changed to a new ISP that requires you to renumber your network
- When you need to merge two intranets with duplicate addresses

You typically use NAT on a border router.



NAT is used on the Corporate router connected to the Internet

Advantages and disadvantages of implementing NAT

Advantages	Disadvantages
Conserves legally registered addresses.	Translation results in switching path delays.
Remedies address overlap events.	Causes loss of end-to-end IP traceability
Increases flexibility when connecting to the Internet.	Certain applications will not function with NAT enabled
Eliminates address renumbering as a network evolves.	

Types of Network Address Translation

- **Static NAT**
  - This type of NAT is designed to allow one-to-one mapping between local and global addresses.
  - Keep in mind that the static version requires you to have one real Internet IP address for every host on your network.
- **Dynamic NAT**
  - This version gives you the ability to map an unregistered IP address to a registered IP address from out of a pool of registered IP addresses.
  - You don't have to statically configure your router to map each inside address to an individual outside address as you would using static NAT, but you do have to have enough real, bona fide IP addresses for everyone who's going to be sending packets to and receiving them from the Internet at the same time.

Types of Network Address Translation

- **Overloading**
  - This is the most popular type of NAT configuration.
  - Understand that overloading really is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different source ports.
  - Also known as *Port Address Translation (PAT)*, which is also commonly referred to as NAT Overload.
  - Using PAT allows you to permit thousands of users to connect to the Internet using only one real global IP address
  - NAT Overload is the real reason we haven't run out of valid IP addresses on the Internet.

NAT Names

- Addresses used after NAT translations are called ***global addresses***.
- These are usually the public addresses used on the Internet, which you don't need if you aren't going on the Internet.
- ***Local addresses*** are the ones we use before NAT translation.
- This means that the **inside local address** is actually the private address of the sending host that's attempting to get to the Internet.
- The **outside local address** would typically be the router interface connected to your ISP and is also usually a public address used as the packet begins its journey.

NAT Names

- After translation, the inside local address is then called the ***inside global address*** and the **outside global address** then becomes the address of the destination host.
- Keep in mind that these terms and their definitions can vary somewhat based on implementation.

Names	Meaning
Inside local	Source host inside address before translation—typically an RFC 1918 address.
Outside local	Address from which source host is known on the Internet. This is usually the address of the router interface connected to ISP—the actual Internet address.
Inside global	Source host address used after translation to get onto the Internet. This is also the actual Internet address.
Outside global	Address of outside destination host and, again, the real Internet address.