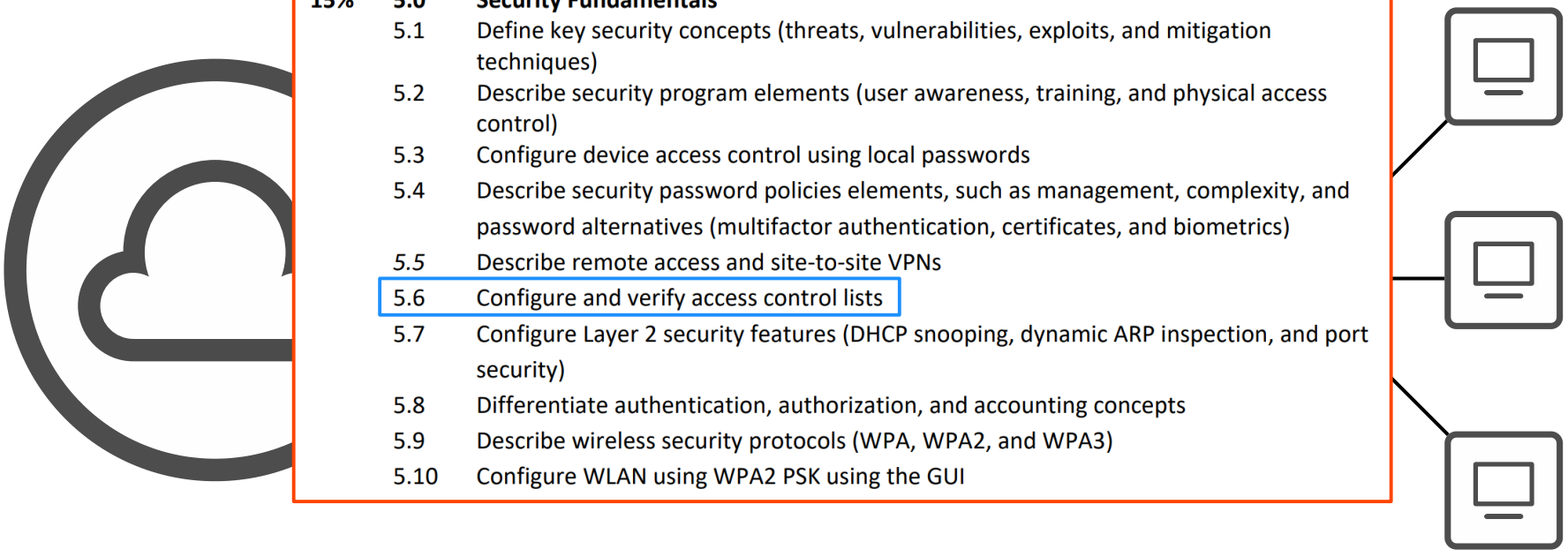
JEREMY'S IT LAB

CCNA 200-301 Day 34

Standard Access Control Lists

15%	**5.0**	**Security Fundamentals**
	5.1	Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
	5.2	Describe security program elements (user awareness, training, and physical access control)
	5.3	Configure device access control using local passwords
	5.4	Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
	5.5	Describe remote access and site-to-site VPNs
	5.6	Configure and verify access control lists
	5.7	Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
	5.8	Differentiate authentication, authorization, and accounting concepts
	5.9	Describe wireless security protocols (WPA, WPA2, and WPA3)
	5.10	Configure WLAN using WPA2 PSK using the GUI

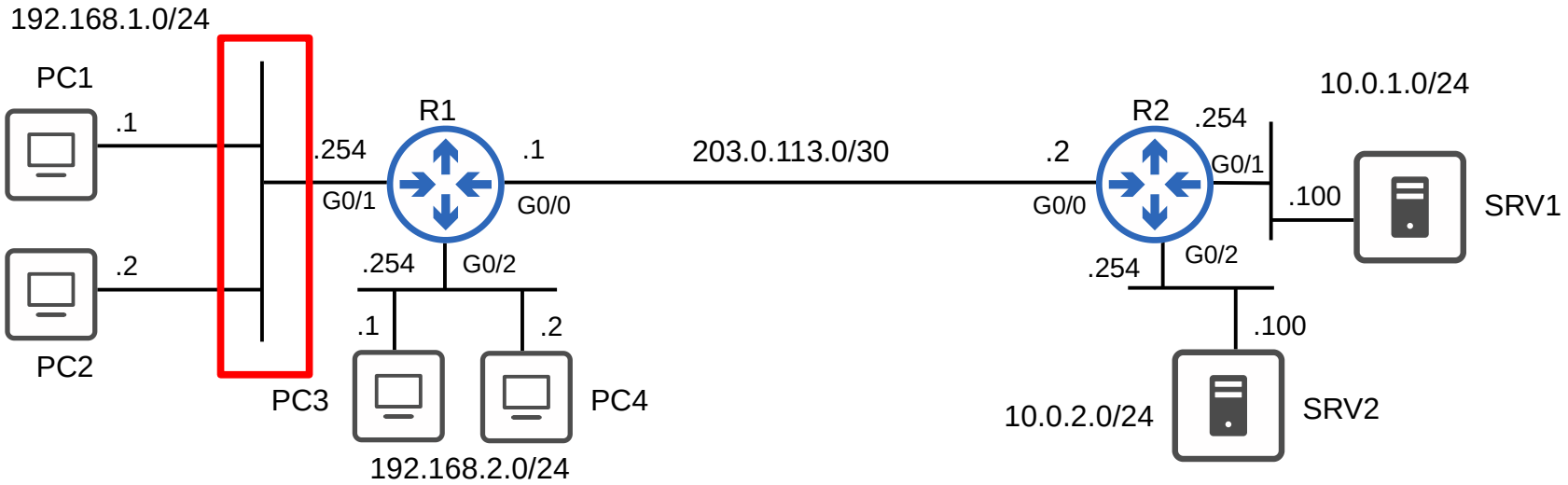


Things we'll cover

- What are ACLs?
- ACL logic
- ACL types
- Standard numbered ACLs
- Standard named ACLs

What are ACLs?

- ACLs (Access Control Lists) have multiple uses.
- In Day 34 and Day 35, we will focus on ACLs from a security perspective.
- ACLs function as a packet filter, instructing the router to permit or discard specific traffic.
- ACLs can filter traffic based on source/destination IP addresses, source/destination Layer 4 ports, etc.



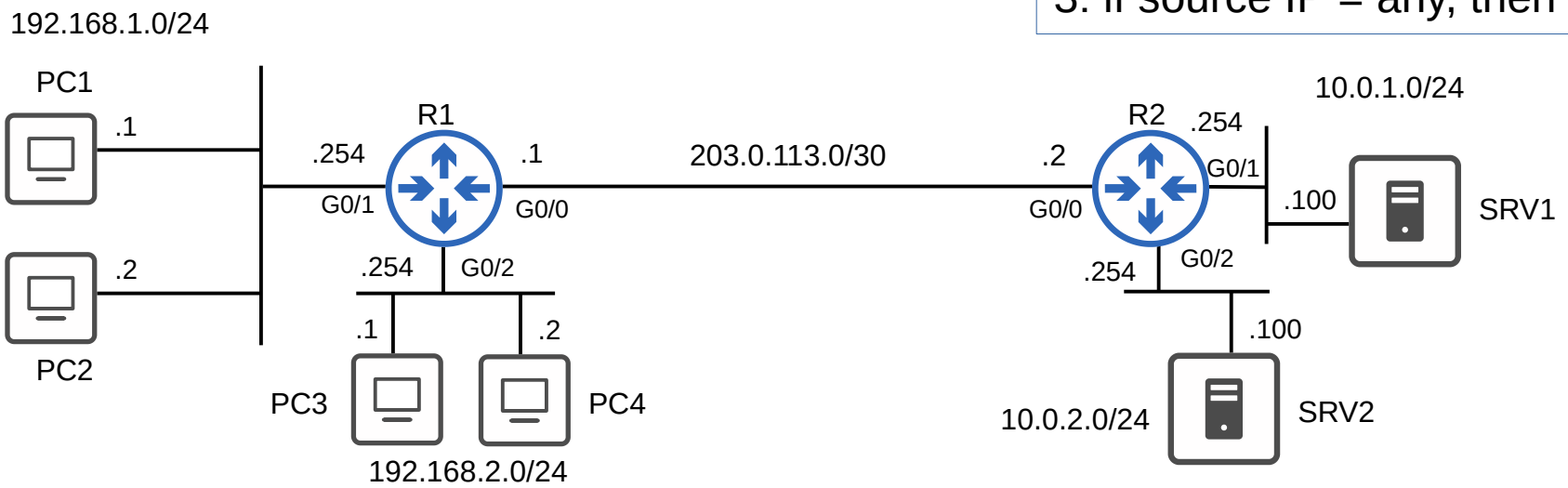
How ACLs work

- REQUIREMENT:
  Hosts in 192.168.1.0/24 can access the 10.0.1.0/24 network
  Hosts in 192.168.2.0/24 cannot access the 10.0.1.0/24 network.

- ACLs are configured globally on the router. (global config mode)

- They are an ordered sequence of ACEs. (Access Control Entries)

ACL 1:
1: if source IP = 192.168.1.0/24, then permit
2: if source IP = 192.168.2.0/24, then deny
3: if source IP = any, then permit

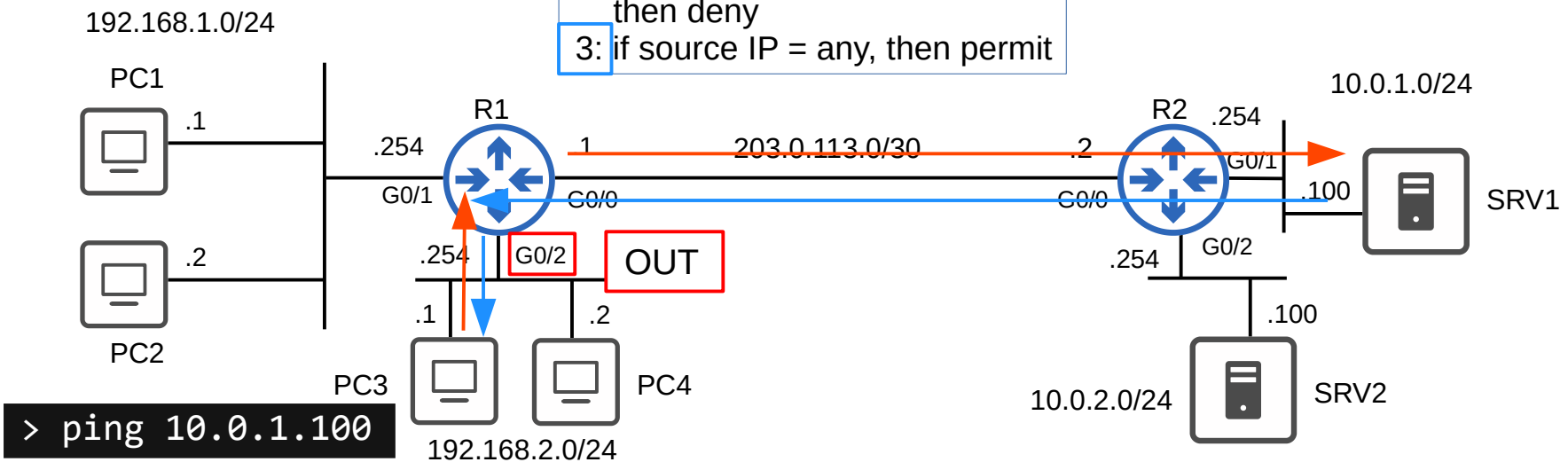


How ACLs work

- Configuring an ACL in global config mode will not make the ACL take effect.
- The ACL must be applied to an interface.
- ACLs are applied either inbound or outbound.

REQUIREMENTS:
192.168.1.0/24 can access 10.0.1.0/24
192.168.2.0/24 can't access 10.0.1.0/24

ACL 1:
1: if source IP = 192.168.1.0/24, then permit
2: if source IP = 192.168.2.0/24, then deny
3: if source IP = any, then permit

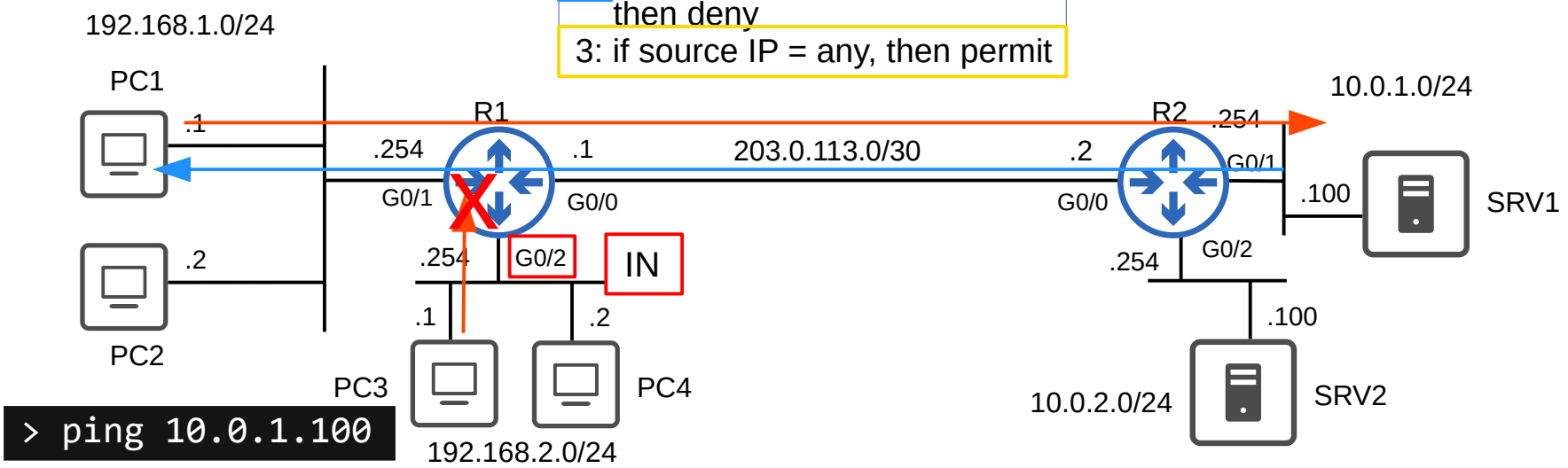


How ACLs work

- Configuring an ACL in global config mode will not make the ACL take effect.
- The ACL must be applied to an interface.
- ACLs are applied either inbound or outbound.

REQUIREMENTS:
192.168.1.0/24 can access 10.0.1.0/24
192.168.2.0/24 can't access 10.0.1.0/24

ACL 1:
1: if source IP = 192.168.1.0/24, then permit
2: if source IP = 192.168.2.0/24, then deny
3: if source IP = any, then permit

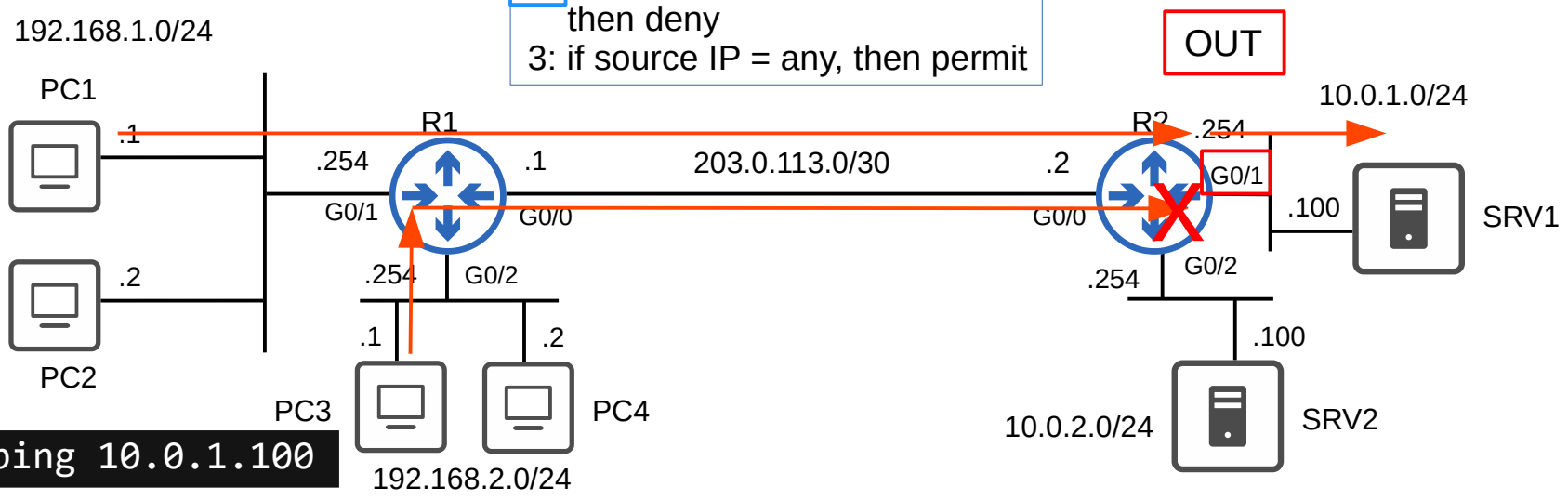


How ACLs work

- Configuring an ACL in global config mode will not make the ACL take effect.
- The ACL must be applied to an interface.
- ACLs are applied either inbound or outbound.

REQUIREMENTS:
192.168.1.0/24 can access 10.0.1.0/24
192.168.2.0/24 can't access 10.0.1.0/24

ACL 1:
1: if source IP = 192.168.1.0/24, then permit
2: if source IP = 192.168.2.0/24, then deny
3: if source IP = any, then permit

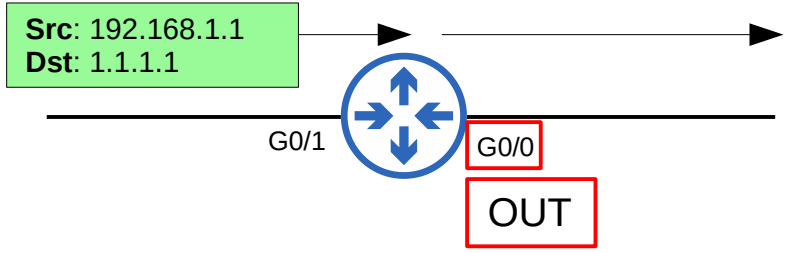


How ACLs work

- Configuring an ACL in global config mode will not make the ACL take effect.
- The ACL must be applied to an interface.
- ACLs are applied either inbound or outbound.
- ACLs are made up of one or more ACEs.

ACL 1:
1: if source IP = 192.168.1.0/24, then permit
2: if source IP = 192.168.2.0/24, then deny
3: if source IP = any, then permit

- When the router checks a packet against the ACL, it processes the ACEs in order, from top to bottom.
- If the packet matches one of the ACEs in the ACL, the router takes the action and stops processing the ACL. All entries below the matching entry will be ignored.



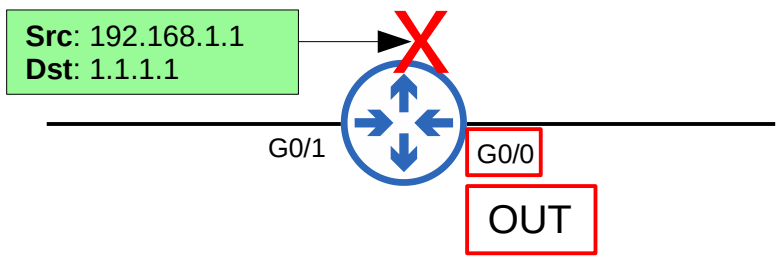
ACL 2:
1: if source IP = 192.168.1.0/24, then permit
~~2: if source IP = 192.168.0.0/16, then deny~~

How ACLs work

- Configuring an ACL in global config mode will not make the ACL take effect.
- The ACL must be applied to an interface.
- ACLs are applied either inbound or outbound.
- ACLs are made up of one or more ACEs.

A maximum of one ACL can be applied to a single interface per direction.
Inbound: Maximum one ACL
Outbound: Maximum one ACL

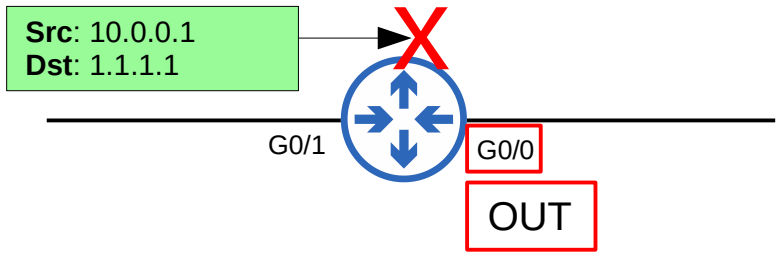
- When the router checks a packet against the ACL, it processes the ACEs in order, from top to bottom.
- If the packet matches one of the ACEs in the ACL, the router takes the action and stops processing the ACL. All entries below the matching entry will be ignored.



ACL 2:
1: if source IP = 192.168.0.0/16, then deny
~~2: if source IP = 192.168.1.0/24, then permit~~

Implicit deny

- What will happen if a packet doesn't match any of the entries in an ACL?



ACL 2:
1: if source IP = 192.168.1.0/24, then permit
2: if source IP = 192.168.0.0/16, then deny
(3: if source IP = any, then deny)

- There is an 'implicit deny' at the end of all ACLs.
- The implicit deny tells the router to deny all traffic that doesn't match any of the configured entries in the ACL.

ACL Types

Standard ACLs: Match based on **Source IP address** only

→ Standard Numbered ACLs

→ Standard Named ACLs

Extended ACLs: Match based on **Source/Destination IP, Source/Destination port,** etc.

→ Extended Numbered ACLs

→ Extended Named ACLs

Standard Numbered ACLs

- Standard ACLs match traffic based only on the source IP address of the packet.
- Numbered ACLs are identified with a number (ie. ACL 1, ACL 2, etc)
- Different types of ACLs have a different range of numbers that can be used.
  → Standard ACLs can use 1-99 and 1300-1999.

Protocol	Range
Standard IP	1–99 and 1300–1999
Extended IP	100–199 and 2000–2699
Ethernet type code	200–299
Ethernet address	700–799
Transparent bridging (protocol type)	200–299
Transparent bridging (vendor code)	700–799
Extended transparent bridging	1100–1199
DECnet and extended DECnet	300–399
Xerox Network Systems (XNS)	400–499
Extended XNS	500–599
AppleTalk	600–699
Source-route bridging (protocol type)	200–299
Source-route bridging (vendor code)	700–799
Internetwork Packet Exchange (IPX)	800–899
Extended IPX	900–999
IPX Service Advertising Protocol (SAP)	1000–1099

Standard Numbered ACLs

- Standard ACLs match traffic based only on the source IP address of the packet.
- Numbered ACLs are identified with a number (ie. ACL 1, ACL 2, etc)
- Different types of ACLs have a different range of numbers that can be used.
  → Standard ACLs can use 1-99 and 1300-1999.
- The basic command to configure a standard numbered ACL is:

  `R1(config)# access-list number {deny | permit} ip wildcard-mask`

```
R1(config)# access-list 1 deny 1.1.1.1 0.0.0.0
R1(config)# access-list 1 deny 1.1.1.1
R1(config)# access-list 1 deny host 1.1.1.1
```

```
R1(config)# access-list 1 permit any
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
```

```
R1(config)# access-list 1 remark ## BLOCK BOB FROM ACCOUNTING ##
```

Standard Numbered ACLs

```
R1(config)#access-list 1 deny 1.1.1.1 0.0.0.0
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 remark ## BLOCK BOB FROM ACCOUNTING ##
R1(config)#
R1(config)#do show access-lists
Standard IP access list 1
    10 deny   1.1.1.1
    20 permit any
R1(config)#
R1(config)#do show ip access-lists
Standard IP access list 1
    10 deny   1.1.1.1
    20 permit any
R1(config)#
R1(config)#do show running-config | include access-list
access-list 1 deny   1.1.1.1
access-list 1 permit any
access-list 1 remark ## BLOCK BOB FROM ACCOUNTING ##
R1(config)#
```

Apply to an interface:

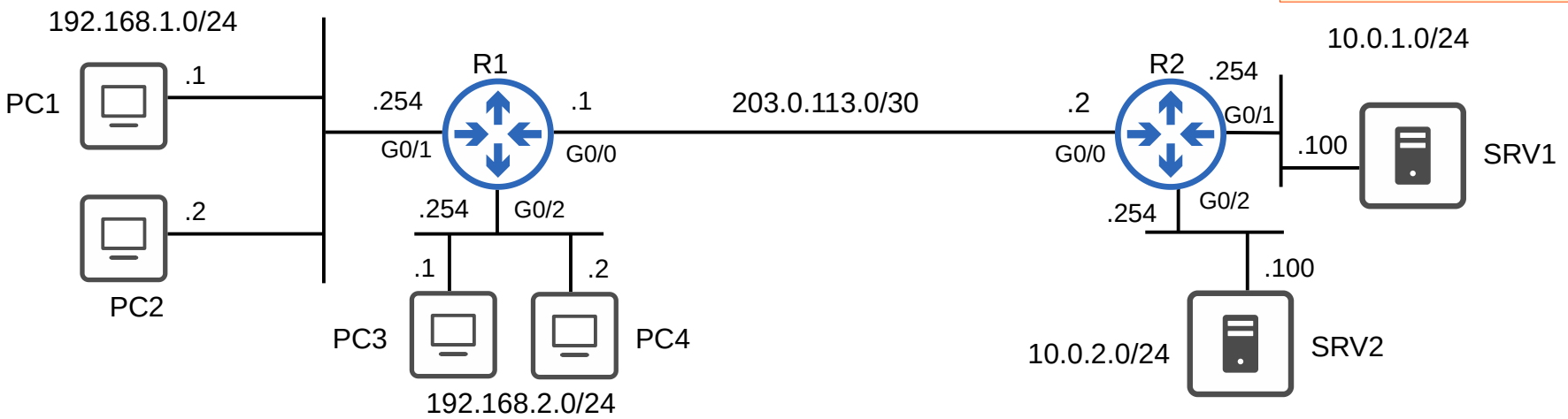
R1(config-if)# **ip access-group** *number* {**in** | **out**}

Standard Numbered ACLs

```
R1(config)#access-list 1 permit 192.168.1.1
R1(config)#access-list 1 deny 192.168.1.0 0.0.0.255
R1(config)#access-list 1 permit any
R1(config)#
R1(config)#interface g0/2
R1(config-if)#ip access-group 1 out
R1(config-if)#
```

Standard ACLs should be applied as close to the destination as possible.

Requirements:
- PC1 can access 192.168.2.0/24.
- Other PCs in 192.168.1.0/24 can't access 192.168.2.0/24.

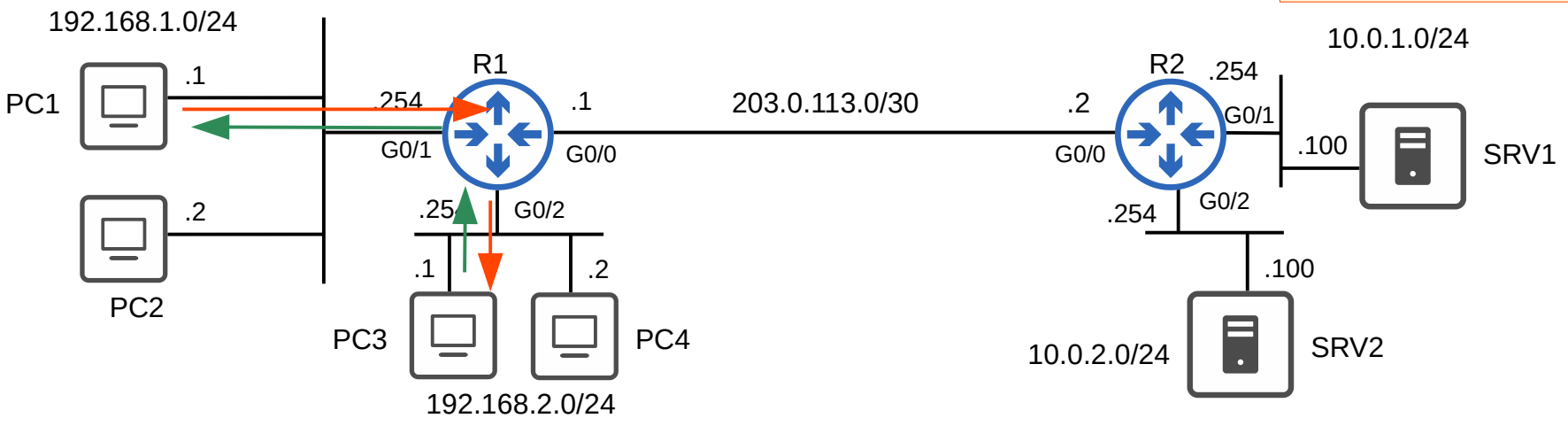


Standard Numbered ACLs

```
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.1.1
    20 deny   192.168.1.0, wildcard bits 0.0.0.255
    30 permit any
R1#
```

Requirements:
- PC1 can access 192.168.2.0/24.
- Other PCs in 192.168.1.0/24 can't access 192.168.2.0/24.

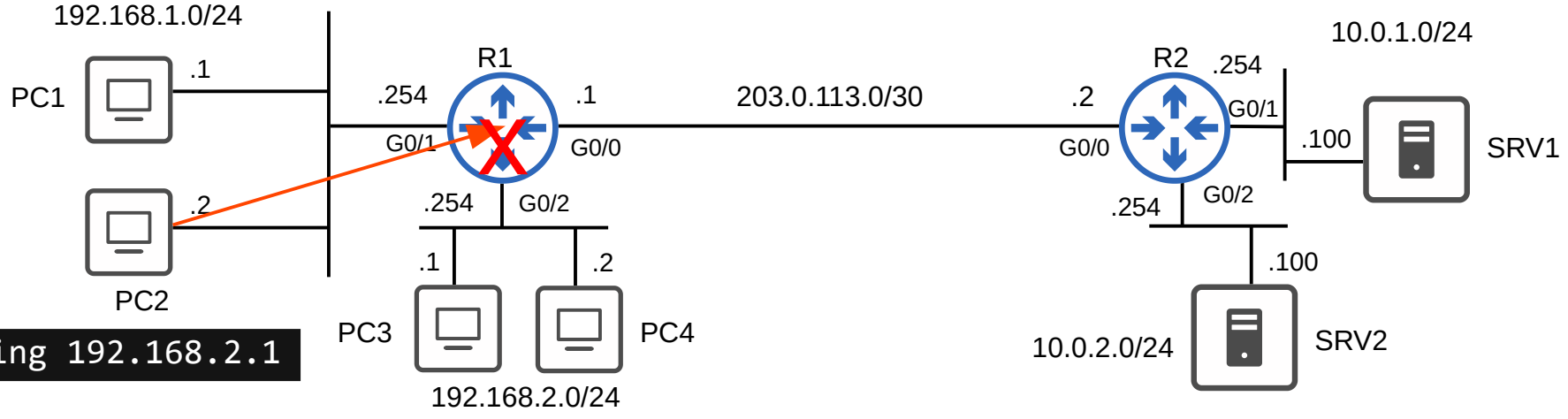
```
> ping 192.168.2.1
```



Standard Numbered ACLs

```
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.1.1
    20 deny   192.168.1.0, wildcard bits 0.0.0.255
    30 permit any
R1#
```

Requirements:
- PC1 can access 192.168.2.0/24.
- Other PCs in 192.168.1.0/24 can't access 192.168.2.0/24.




```
> ping 192.168.2.1
```

Standard Named ACLs

- Standard ACLs match traffic based only on the source IP address of the packet.
- Named ACLs are identified with a name (ie. ‘BLOCK_BOB’)
- Standard named ACLs are configured by entering ‘standard named ACL config mode’, and then configuring each entry within that config mode.

```
R1(config)# ip access-list standard acl-name
R1(config-std-nacl)# [entry-number] {deny | permit} ip wildcard-mask
```

```
R1(config)#ip access-list standard BLOCK_BOB
R1(config-std-nacl)#5 deny 1.1.1.1
R1(config-std-nacl)#10 permit any
R1(config-std-nacl)#remark ## CONFIGURED NOV 21 2020 ##
R1(config-std-nacl)#interface g0/0
R1(config-if)#ip access-group BLOCK_BOB in
```

Standard Named ACLs

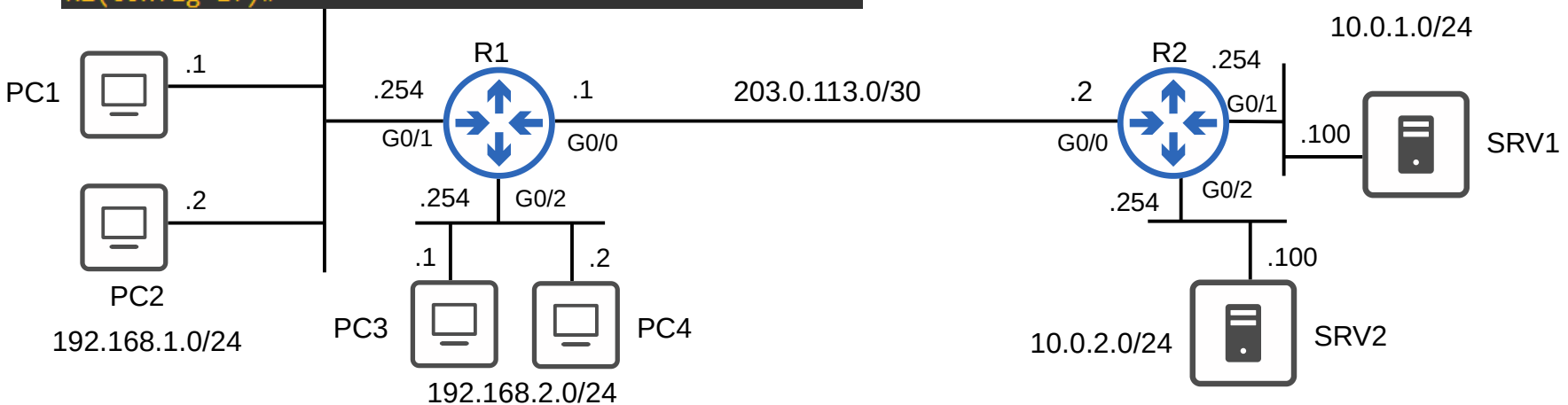
```
R1#show access-lists
Standard IP access list BLOCK_BOB
    5 deny   1.1.1.1
    10 permit any
R1#
R1#show running-config | section access-list
ip access-list standard BLOCK_BOB
 deny   1.1.1.1
 permit any
 remark ## CONFIGURED NOV 21 2020 ##
R1#
```

Standard Named ACLs

```
R2(config)#ip access-list standard TO_10.0.2.0/24
R2(config-std-nacl)#deny 192.168.1.0 0.0.0.255
R2(config-std-nacl)#permit any
R2(config-std-nacl)#interface g0/2
R2(config-if)#ip access-group TO_10.0.2.0/24 out
R2(config-if)#
R2(config-if)#ip access-list standard TO_10.0.1.0/24
R2(config-std-nacl)#deny 192.168.2.1
R2(config-std-nacl)#permit 192.168.2.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.1.1
R2(config-std-nacl)#deny 192.168.1.0 0.0.0.255
R2(config-std-nacl)#permit any
R2(config-std-nacl)#interface g0/1
R2(config-if)#ip access-group TO_10.0.1.0/24 out
R2(config-if)#
```

Requirements:

- PCs in 192.168.1.0/24 can't access 10.0.2.0/24.
- PC3 can't access 10.0.1.0/24.
- Other PCs in 192.168.2.0/24 can access 10.0.1.0/24.
- PC1 can access 10.0.1.0/24.
- Other PCs in 192.168.1.0/24 can't access 10.0.1.0/24.

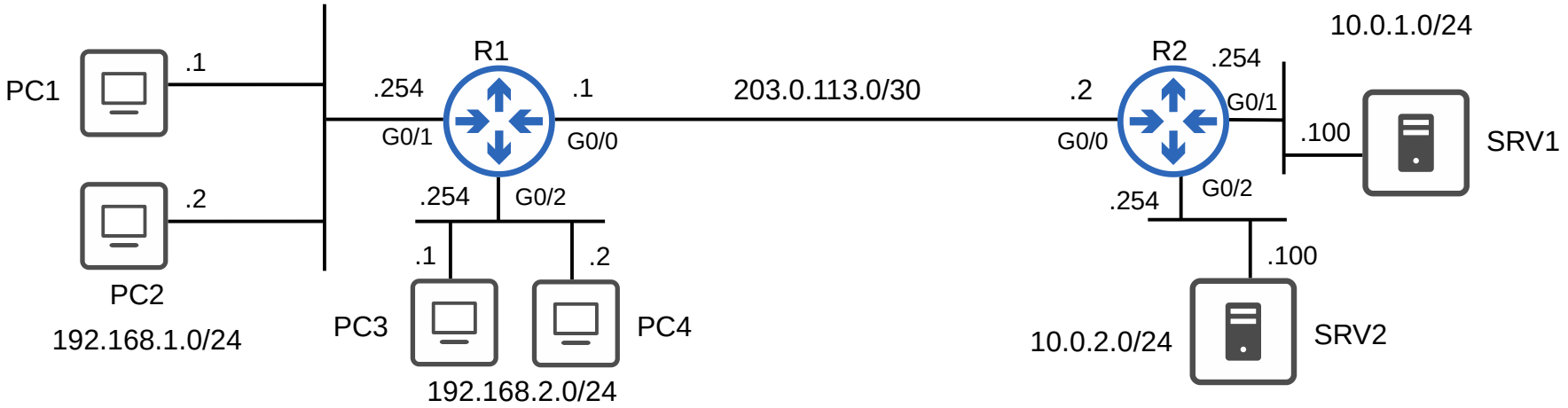


Standard Named ACLs

```
R2#show ip access-lists
Standard IP access list TO_10.0.1.0/24
    30 permit 192.168.1.1
    10 deny   192.168.2.1
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    40 deny   192.168.1.0, wildcard bits 0.0.0.255
    50 permit any
Standard IP access list TO_10.0.2.0/24
    10 deny   192.168.1.0, wildcard bits 0.0.0.255
    20 permit any
R2#
```

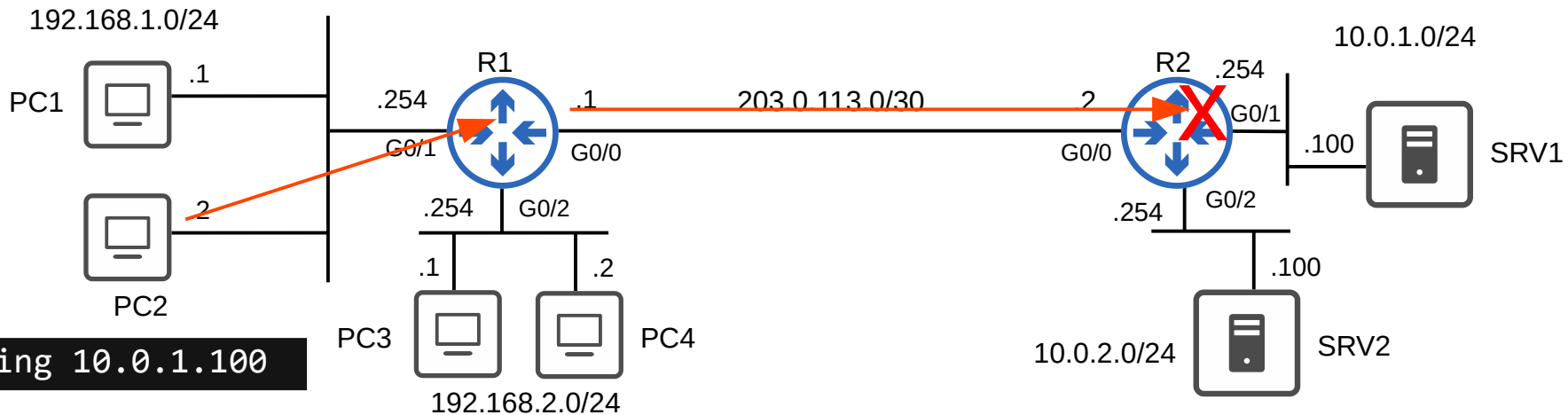
```
R2(config-if)#ip access-list standard TO_10.0.1.0/24
R2(config-std-nacl)#deny 192.168.2.1
R2(config-std-nacl)#permit 192.168.2.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.1.1
R2(config-std-nacl)#deny 192.168.1.0 0.0.0.255
R2(config-std-nacl)#permit any
```

- The router may re-order the /32 entries.
- This improves the efficiency of processing the ACL.
- It **does not** change the effect of the ACL.
- This applies to both standard named and standard numbered ACLs.
- Packet Tracer does not do this.



Standard Named ACLs

```
R2#show ip access-lists
Standard IP access list TO_10.0.1.0/24
    30 permit 192.168.1.1
    10 deny   192.168.2.1
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    40 deny   192.168.1.0, wildcard bits 0.0.0.255
    50 permit any
Standard IP access list TO_10.0.2.0/24
    10 deny   192.168.1.0, wildcard bits 0.0.0.255
    20 permit any
R2#
```




```
> ping 10.0.1.100
```

Things we covered

- What are ACLs?
- ACL logic
- ACL types
- Standard numbered ACLs

```
R1(config)#access-list 1 permit …
R1(config)#access-list 1 deny …
R1(config)#access-list 1 permit …
```

- Standard named ACLs

```
R1(config)#ip access-list standard BLOCK_BOB
R1(config-std-nacl)#permit …
R1(config-std-nacl)#deny …
R1(config-std-nacl)#permit …
```

Quiz 1

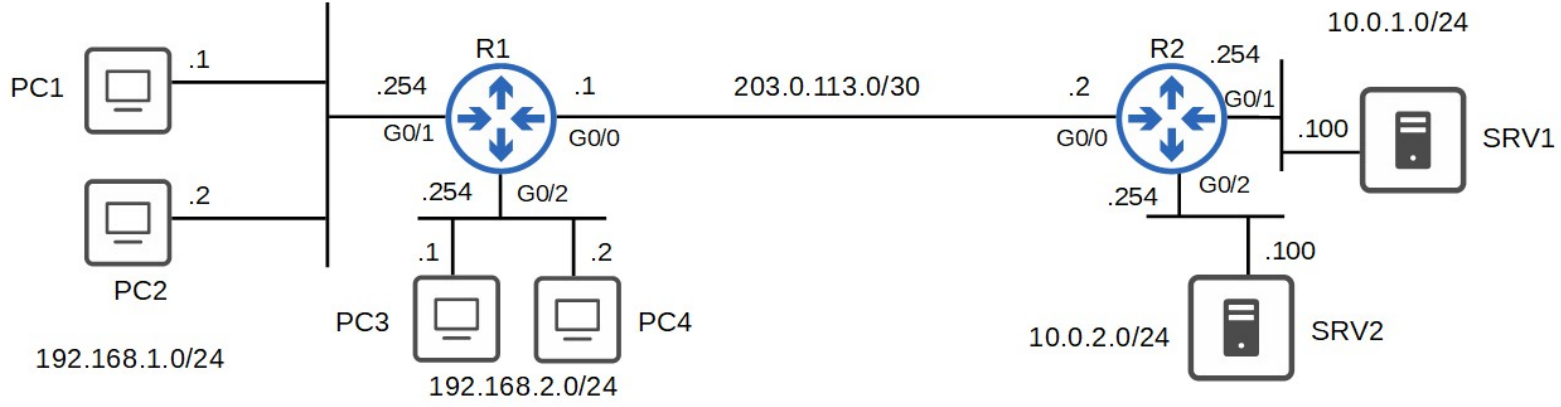
Which ACL, when applied outbound on R2's G0/1, permits ONLY PC1 and PC4 to access 10.0.1.0/24?

```
Standard IP access list 1
    10 permit 192.168.1.1
    20 permit 192.168.2.2
```

```
Standard IP access list 2
    10 permit 192.168.1.0, wildcard bits 0.0.0.255
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    30 deny   any
```

```
Standard IP access list 3
    10 permit 192.168.1.1
    30 permit 192.168.2.2
    20 deny   192.168.1.0, wildcard bits 0.0.0.255
    40 deny   192.168.2.0, wildcard bits 0.0.0.255
    50 permit any
```

```
Standard IP access list 4
    10 permit 192.168.2.2
    30 deny   192.168.1.1
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    40 deny   192.168.1.0, wildcard bits 0.0.0.255
```



Quiz 2

Which interface should the following ACL be applied to, and in which direction, to fulfill the requirement?

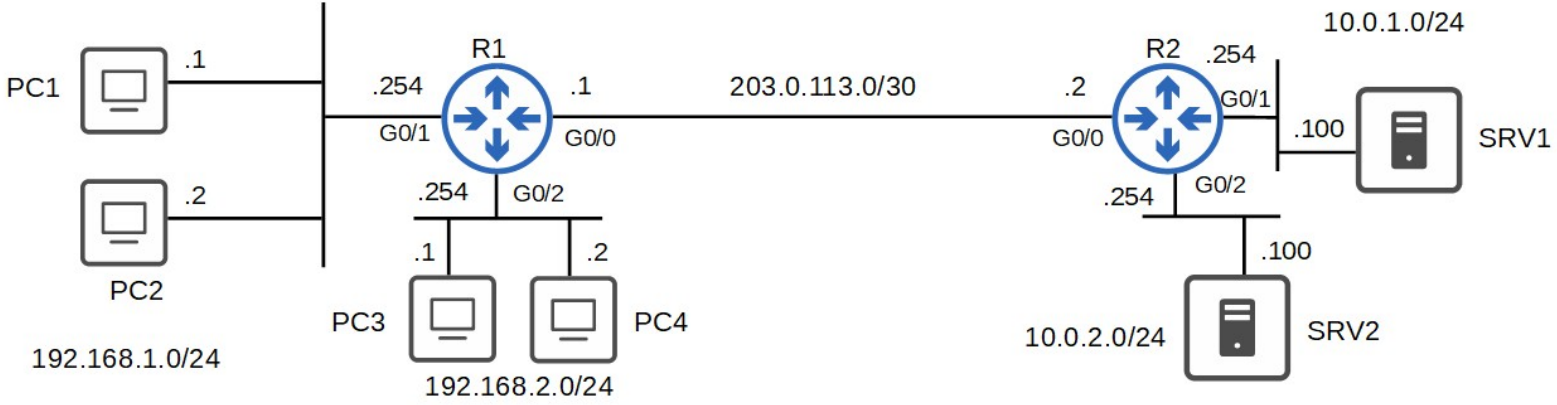
```
Standard IP access list ALLOW_PC3
    10 permit 192.168.2.1
    20 deny   any
```

Requirement:
- Only PC3 can reach SRV2.

Standard ACLs should be applied as close to the destination as possible.

Interface: R2 G0/2

Direction: Outbound



Quiz 3

You issue the following commands on R2. Which statement about the effect of the configurations is correct?

```
R2(config)#access-list 10 deny 10.0.0.0 0.0.0.255
R2(config)#access-list 10 permit any
R2(config)#access-list 20 deny 172.16.0.0 0.0.0.255
R2(config)#access-list 20 permit any
R2(config)#access-list 30 deny 192.168.0.0 0.0.0.255
R2(config)#access-list 30 permit any
R2(config)#access-list 40 deny 0.0.0.0 255.255.255.255
R2(config)#interface g0/0
R2(config-if)#ip access-group 40 out
R2(config-if)#ip access-group 30 out
R2(config-if)#ip access-group 20 out
R2(config-if)#ip access-group 10 out
```

a) All traffic will be denied.

b) Traffic from the 10.0.0.0/24 network will be denied.

c) Traffic from the 172.16.0.0/24 network will be denied.

d) Traffic from the 192.168.0.0/24 network will be denied.

Quiz 4

If this ACL is applied inbound on R1 G0/0, which PCs will be able to ping SRV2?

a) PC1 and PC2.

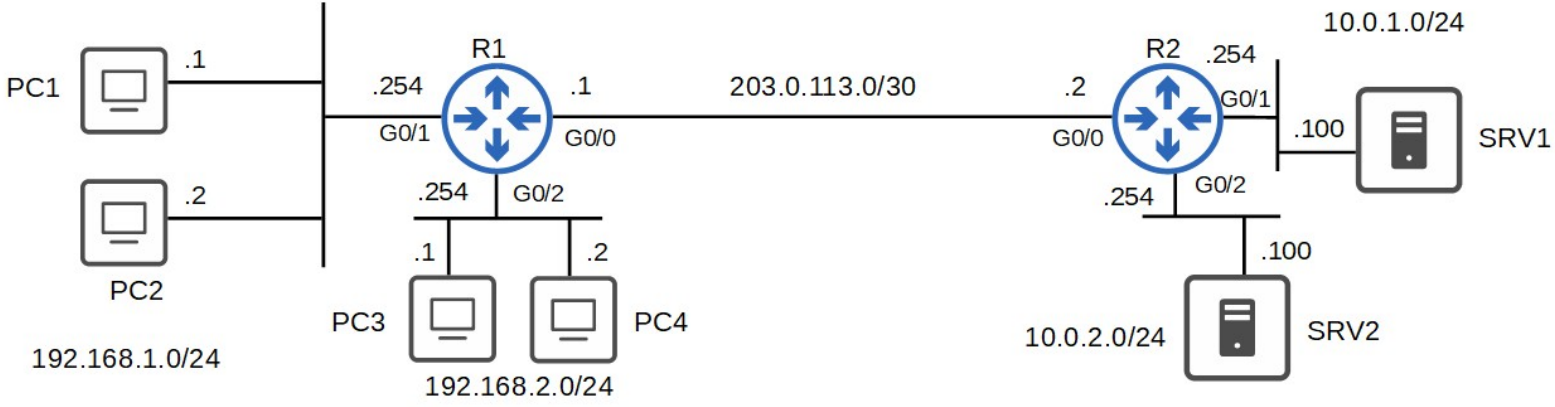
b) PC1, PC2, and PC4.

c) PC1 only.

d) All PCs.

e) PC3 and PC4 only.

```
Standard IP access list TO_10.0.2.0/24
    20 permit 192.168.1.1
    10 permit 192.168.1.2
    40 deny   192.168.2.1
    30 deny   192.168.1.0, wildcard bits 0.0.0.255
    50 permit 192.168.2.0, wildcard bits 0.0.0.255
    60 permit 192.168.0.0, wildcard bits 0.0.255.255
    70 permit any
```



Quiz 5

What happens if a packet doesn't match any entries of an ACL?

a) The packet will be forwarded to the default gateway.

b) The packet will be checked using the next available ACL.

c) The packet will be dropped.

d) The action of the most specific match will be taken.