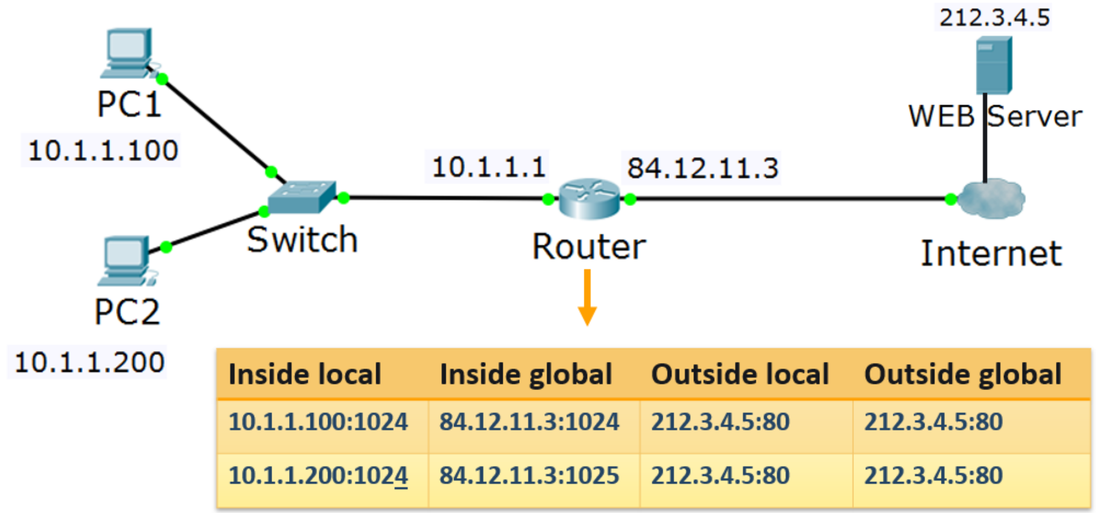
Access Control Lists.
Network Address Translation

Lecture 3



Inside local	Inside global	Outside local	Outside global
10.1.1.100:1024	84.12.11.3:1024	212.3.4.5:80	212.3.4.5:80
10.1.1.200:1024	84.12.11.3:1025	212.3.4.5:80	212.3.4.5:80

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Table of Contents

1. Access control lists overview
2. Access control lists configuration
   - Creating ACLs
   - Assigning ACLs
3. Network Address Translation
4. Demonstration

Have a Question?

Software University

sli.do

#CNA

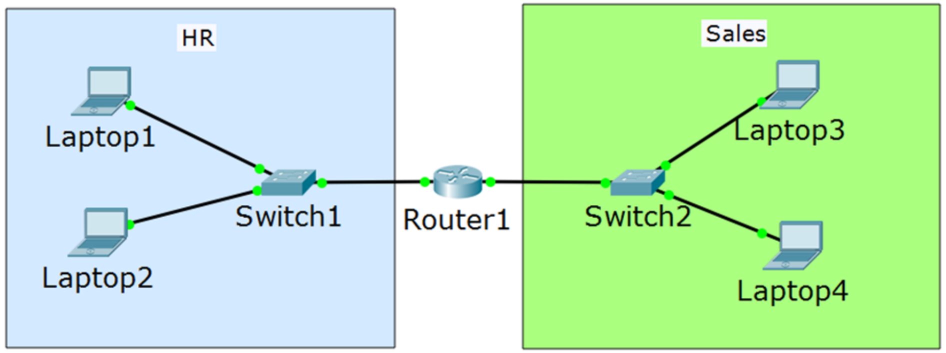
Access Control Lists Overview

What is an ACL?

- ACL: Access Control List
- ACL is a list of rules – each of them is **permit** or **deny**
- Created and applied on a Layer 3 device
- A device with applied ACL acts like a **firewall** ("almost")

Why to Implement ACLs?

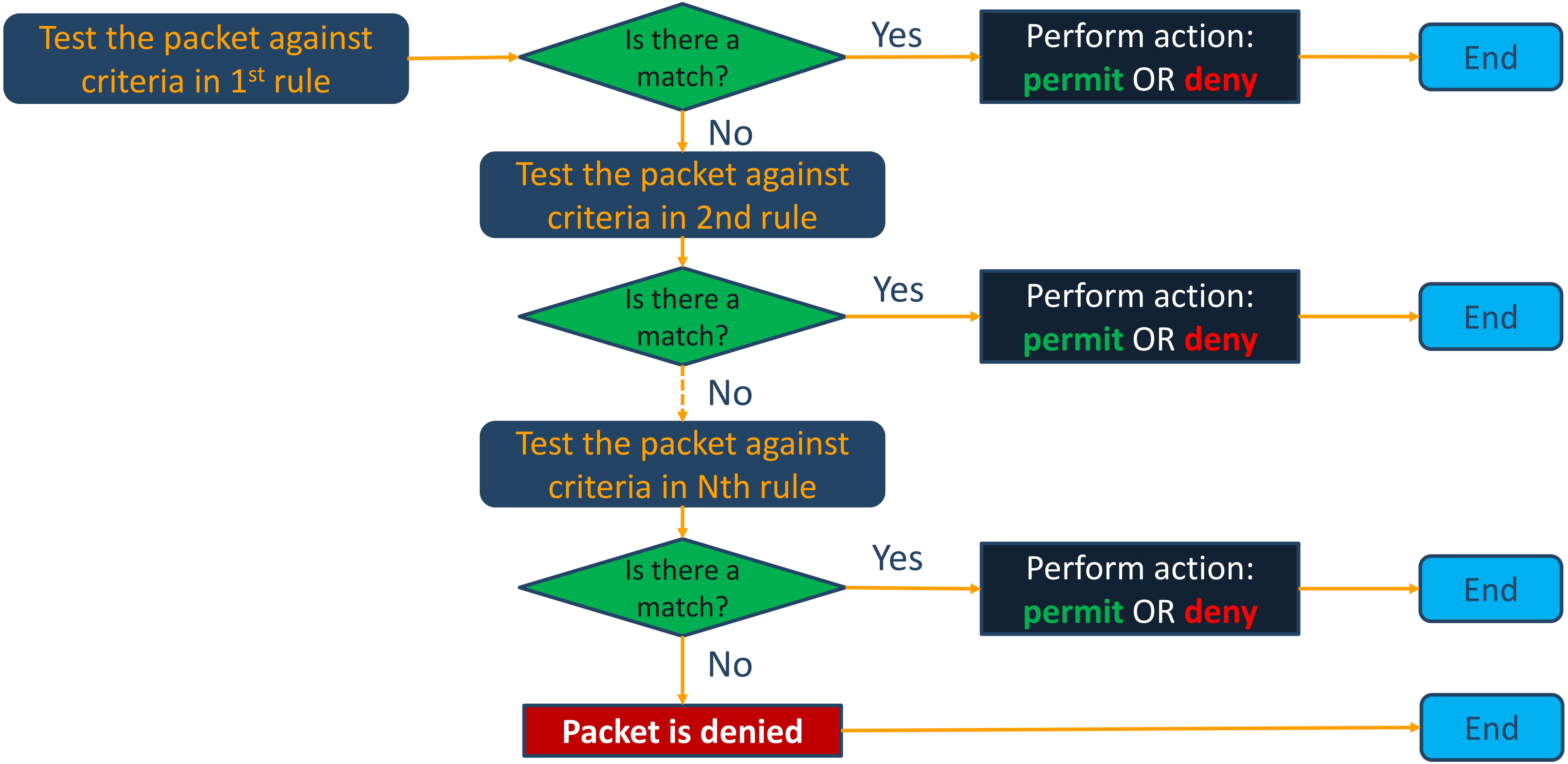
- ACLs filter the network traffic
  - Better security
  - Can increase the overall network performance
- ACLs may just classify (select) traffic for other reasons:
  - Applying QoS
  - NAT
  - Traffic mirroring



ACL Types

- Standard ACLs – can filter only the **source IP** address of a packet
- Extended ACLs – can filter based on:
  - Source and/or destination IP address
  - Source and/or port TCP/UDP number
  - IP protocol (DNS, FTP, HTTP, etc.)
- Ethernet frame header ACLs
  - Filtering based on source or destination MAC address
  - Not very common

ACL Process Order


Test the packet against criteria in 1st rule
Is there a match?
Yes
Perform action: permit OR deny
End
No
Test the packet against criteria in 2nd rule
Is there a match?
Yes
Perform action: permit OR deny
End
No
Test the packet against criteria in Nth rule
Is there a match?
Yes
Perform action: permit OR deny
End
No
Packet is denied
End

Access Control Lists Configuration

Creating ACLs

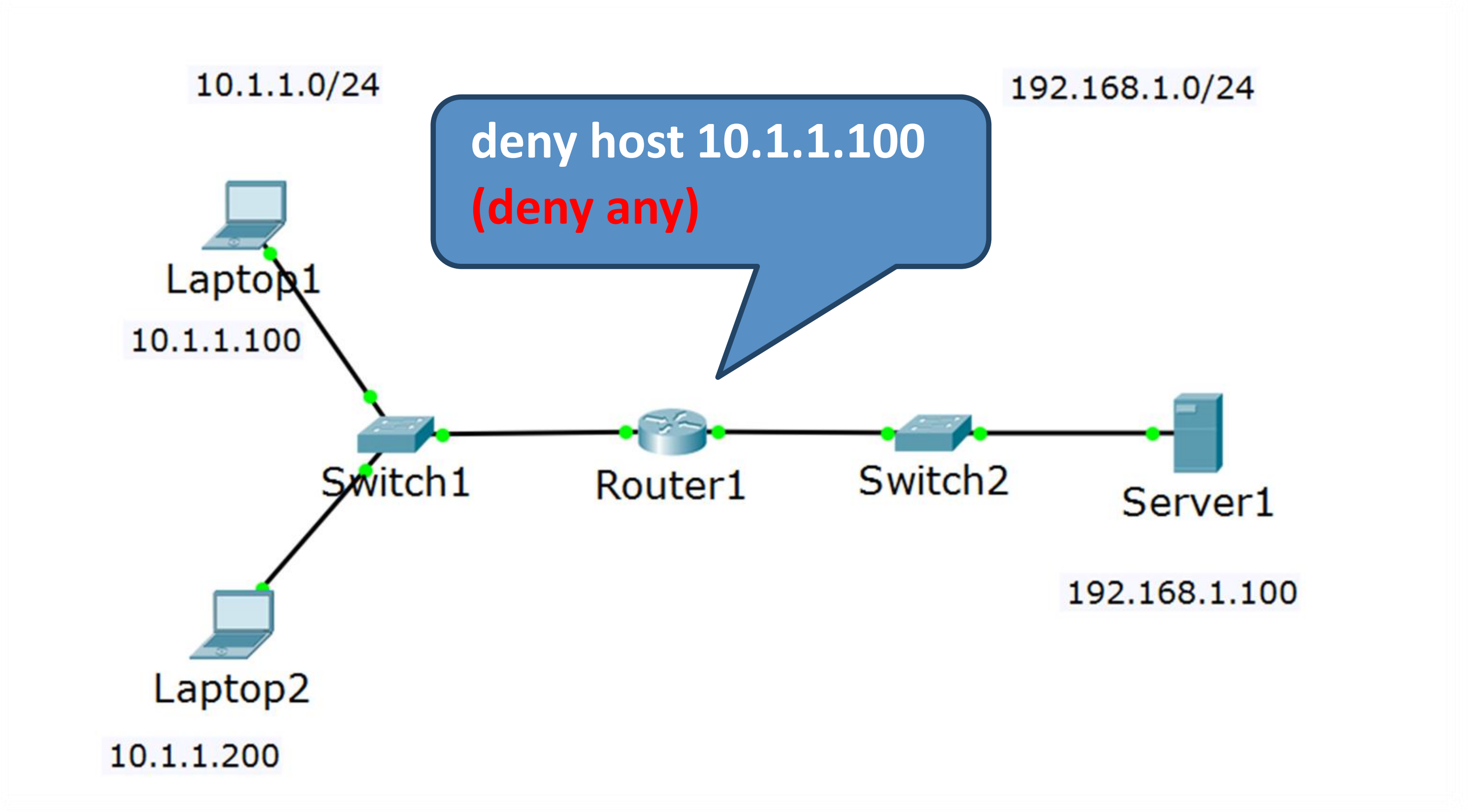
Standard ACLs Configuration

- **ip access-list standard** [<***1-99***> or ***name***]
- [**permit** or **deny**] ***network*** [wildcard mask] or **any** or **host**
- **Example: ip access-list standard test_standard**
  - **permit 192.168.1.0 0.0.0.255** (the whole 192.168.1.X network)
  - **deny host 10.1.1.1** (only the host with IP 10.1.1.1 matches here)
  - **deny host 172.16.34.15** (the exact 172.16.34.15 host)
  - **permit any** (anything else which did not match before)
  - **deny any** (do not forget the implicit deny at the end of each ACL!)

ACL Process Order – Example 1 with Standard ACL

- Q: Is Laptop1 allowed to reach Server1?
  - A: No

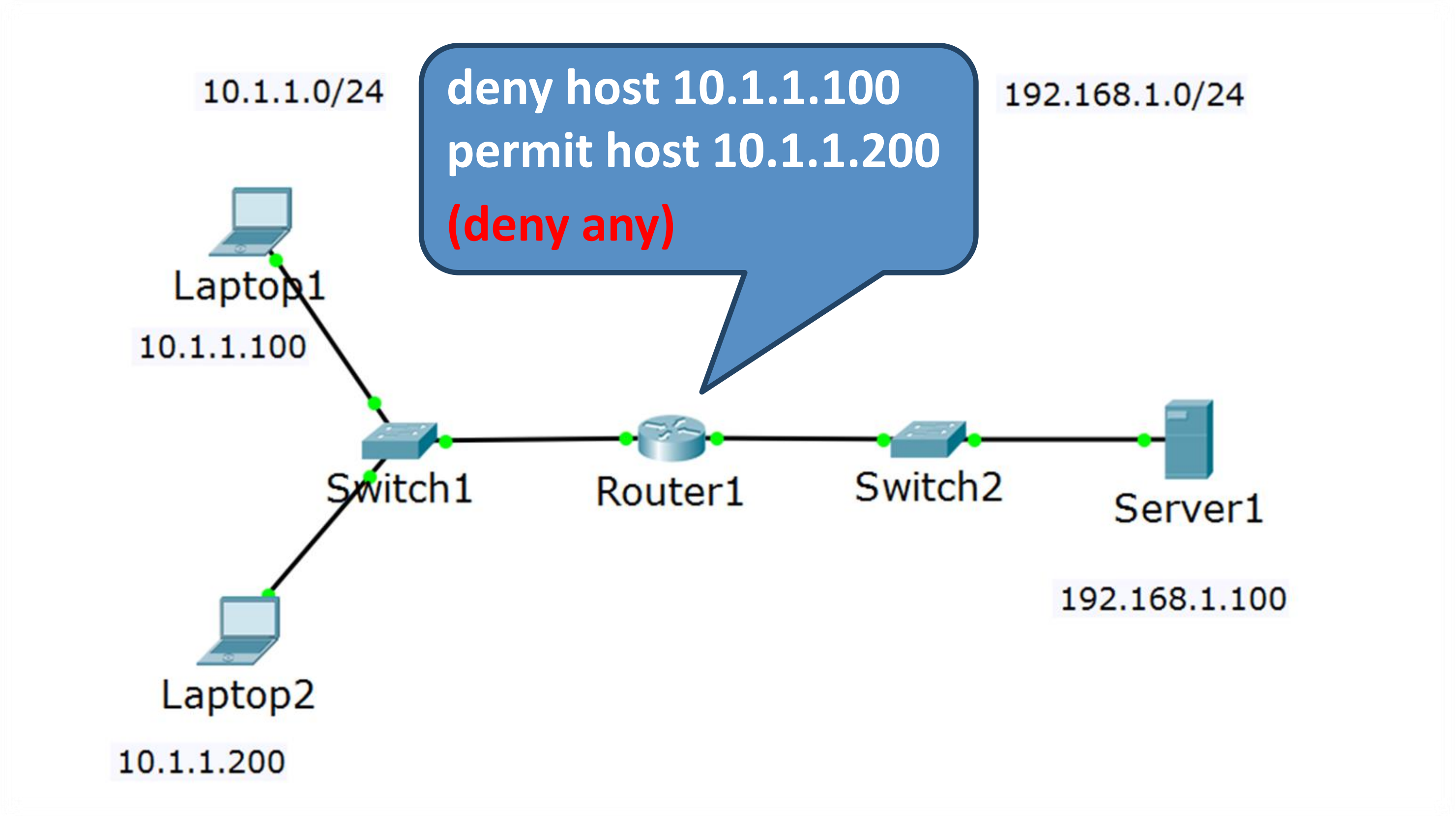
- Q: Is Laptop2 allowed to reach Server1?
  - A: No



*An ACL must also be applied to an interface, this is discussed in the next section

ACL Process Order – Example 2 with Standard ACL

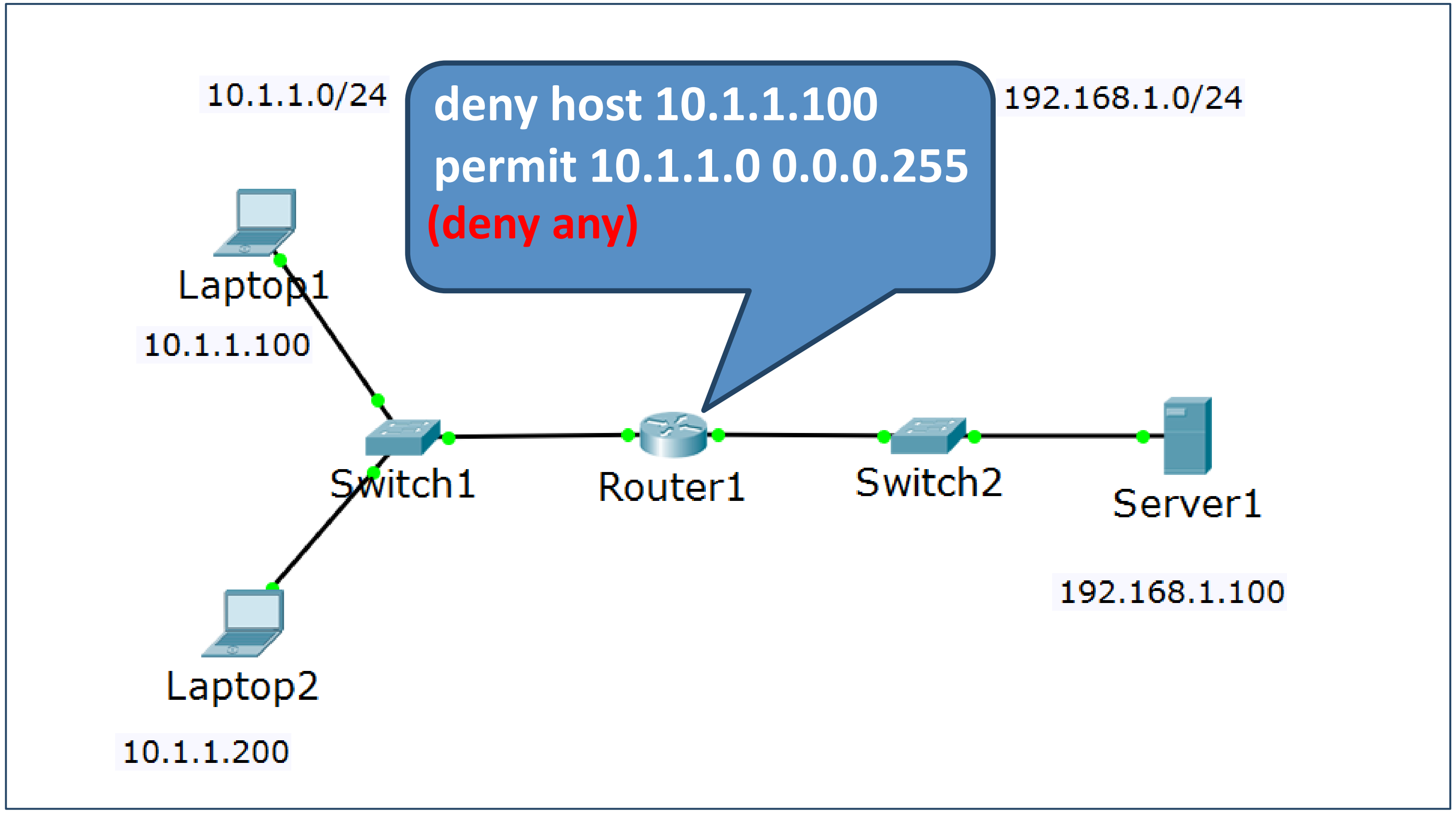
- Q: Is Laptop1 allowed to reach Server1?
  - A: No
- Q: Is Laptop2 allowed to reach Server1?
  - A: Yes



deny host 10.1.1.100
permit host 10.1.1.200
(deny any)

ACL Process Order – Example 3 with Standard ACL

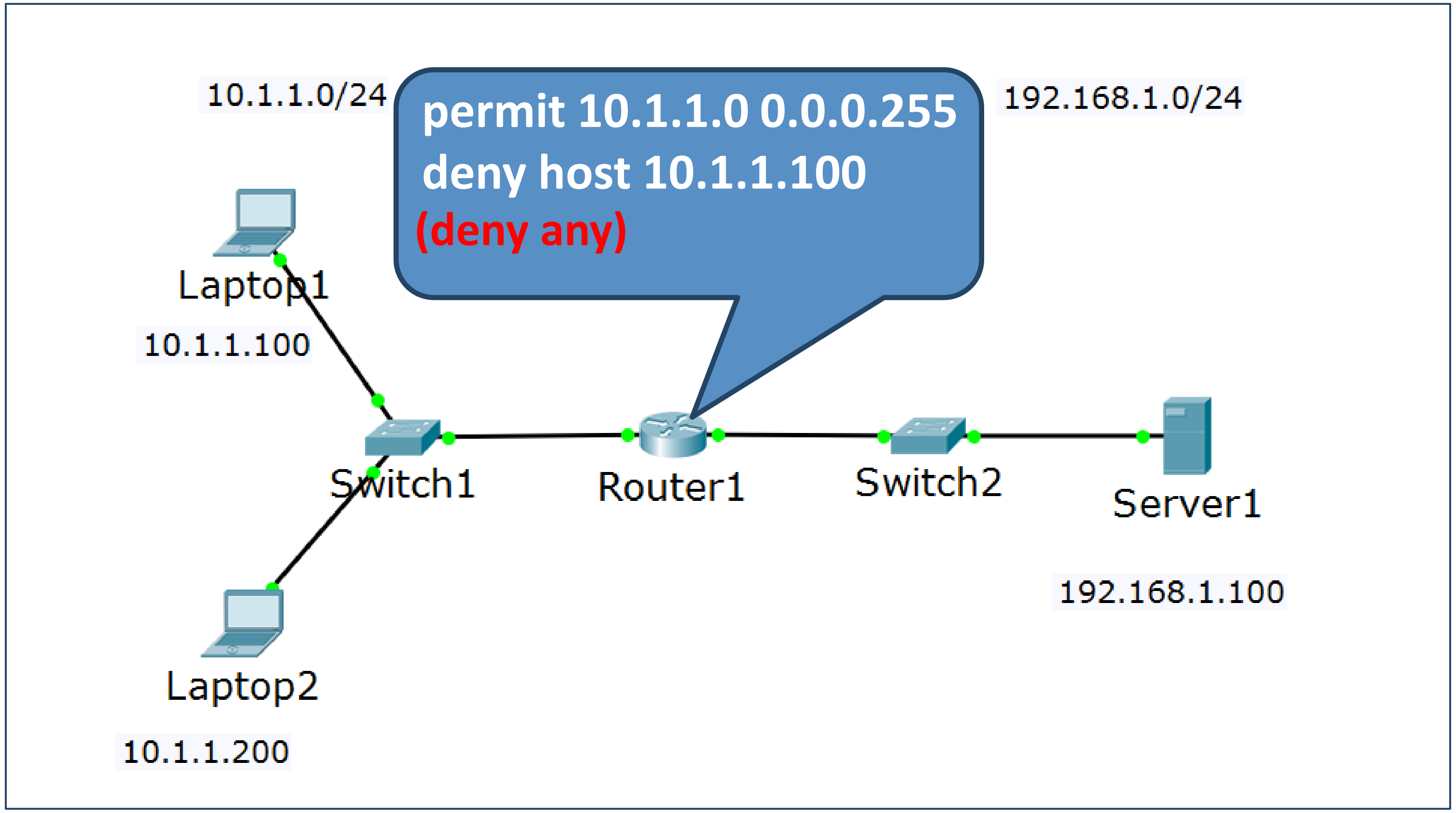
- Q: Is Laptop1 allowed to reach Server1?
  - A: No
- Q: Is Laptop2 allowed to reach Server1?
  - A: Yes



deny host 10.1.1.100
permit 10.1.1.0 0.0.0.255
(deny any)

ACL Process Order – Example 4 with Standard ACL

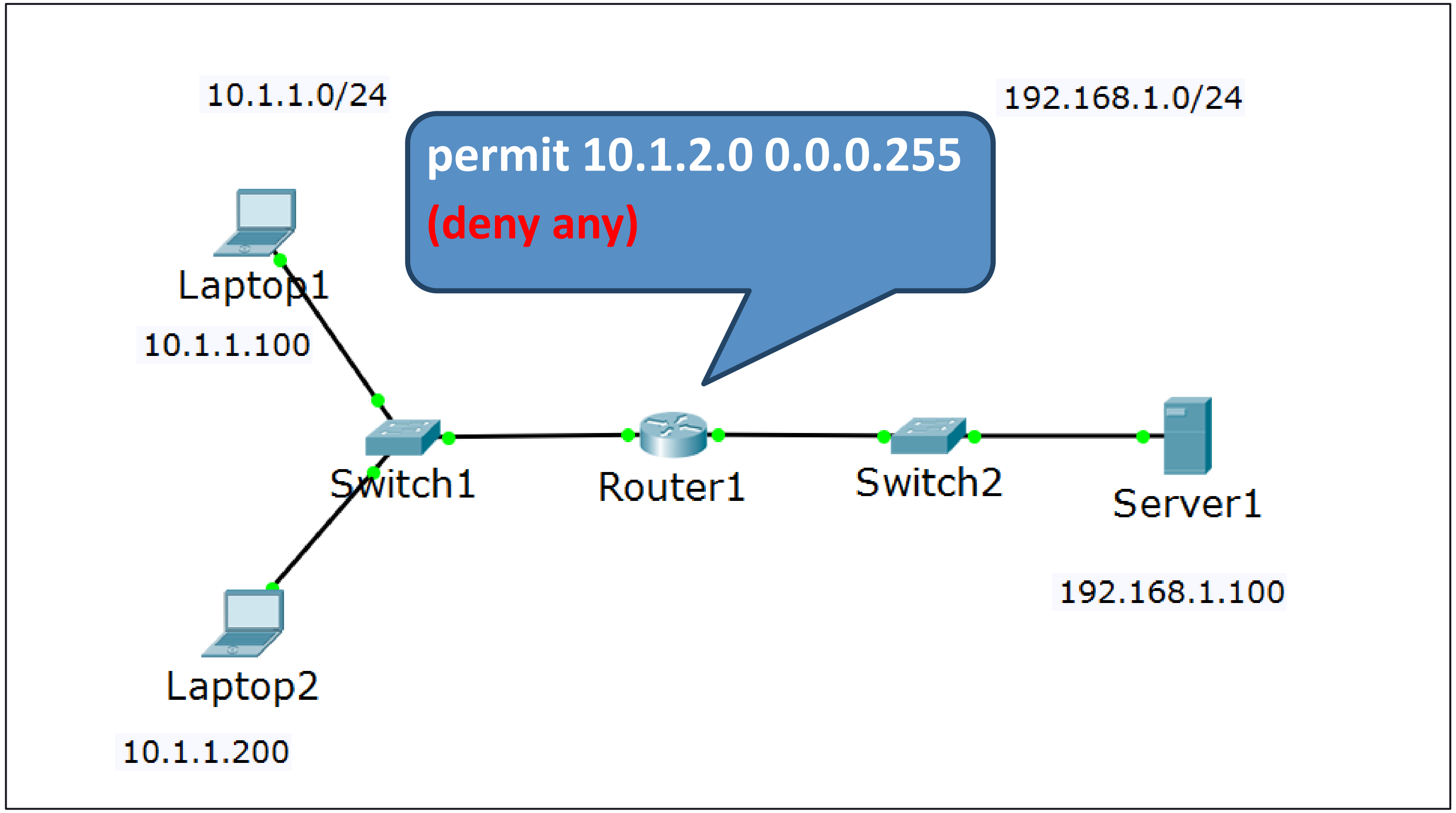
- Q: Is Laptop1 allowed to reach Server1?
  - A: Yes
- Q: Is Laptop2 allowed to reach Server1?
  - A: Yes



permit 10.1.1.0 0.0.0.255
deny host 10.1.1.100
(deny any)

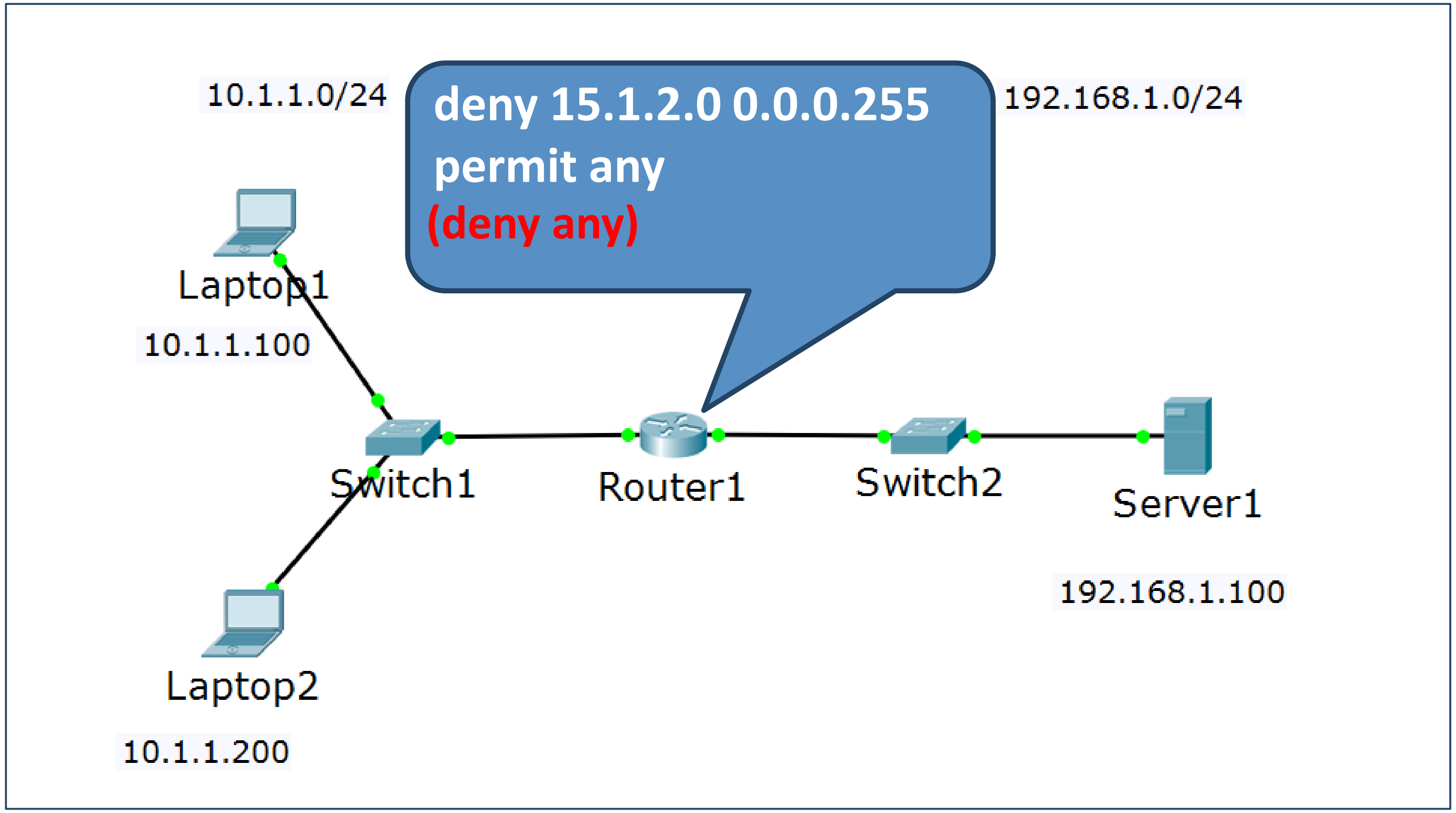
ACL Process Order – Example 5 with Standard ACL

- Q: Is Laptop1 allowed to reach Server1?
  - A: No
- Q: Is Laptop2 allowed to reach Server1?
  - A: No



ACL Process Order – Example 6 with Standard ACL

- Q: Is Laptop1 allowed to reach Server1?
  - A: Yes
- Q: Is Laptop2 allowed to reach Server1?
  - A: Yes

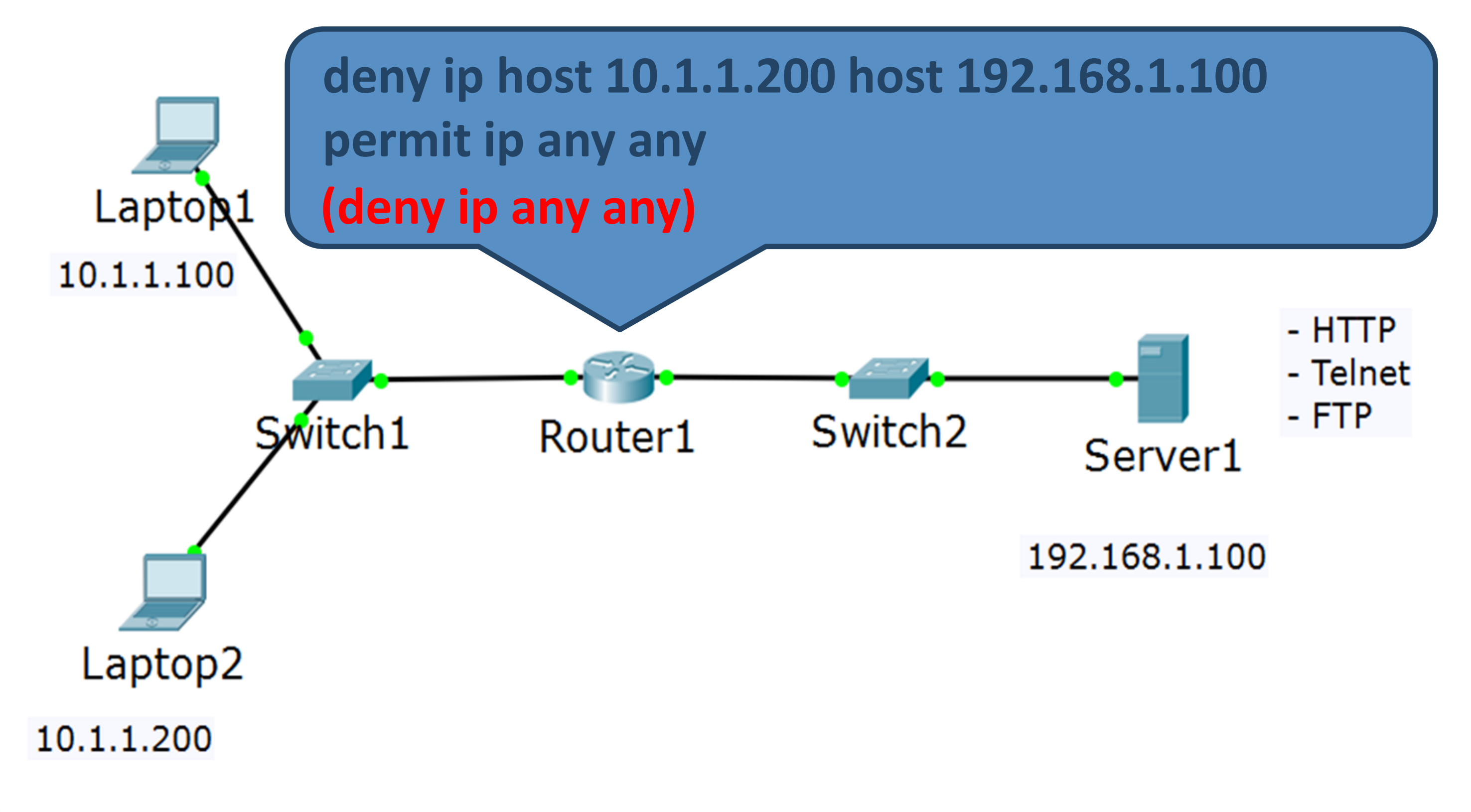


Extended ACLs Configuration

- **ip access-list extended** [<***100-199***> or ***name***]
- [**permit** or **deny**] ***protocol*** [source] ***network*** or **any** or **host** [destination] ***network*** or **any** or **host**
- **Examples: ip access-list extended test_extended**
  - **deny ip host 10.1.1.1 host 20.2.2.2**
  - **permit tcp 10.12.12.0 0.0.0.255 host 20.2.2.2 eq www**
  - **deny icmp any 172.16.0.0 0.0.255.255 echo**
  - **deny ip any any** (do not forget the implicit deny at the end of each ACL)

ACL Process Order – Example 1 with Extended ACL

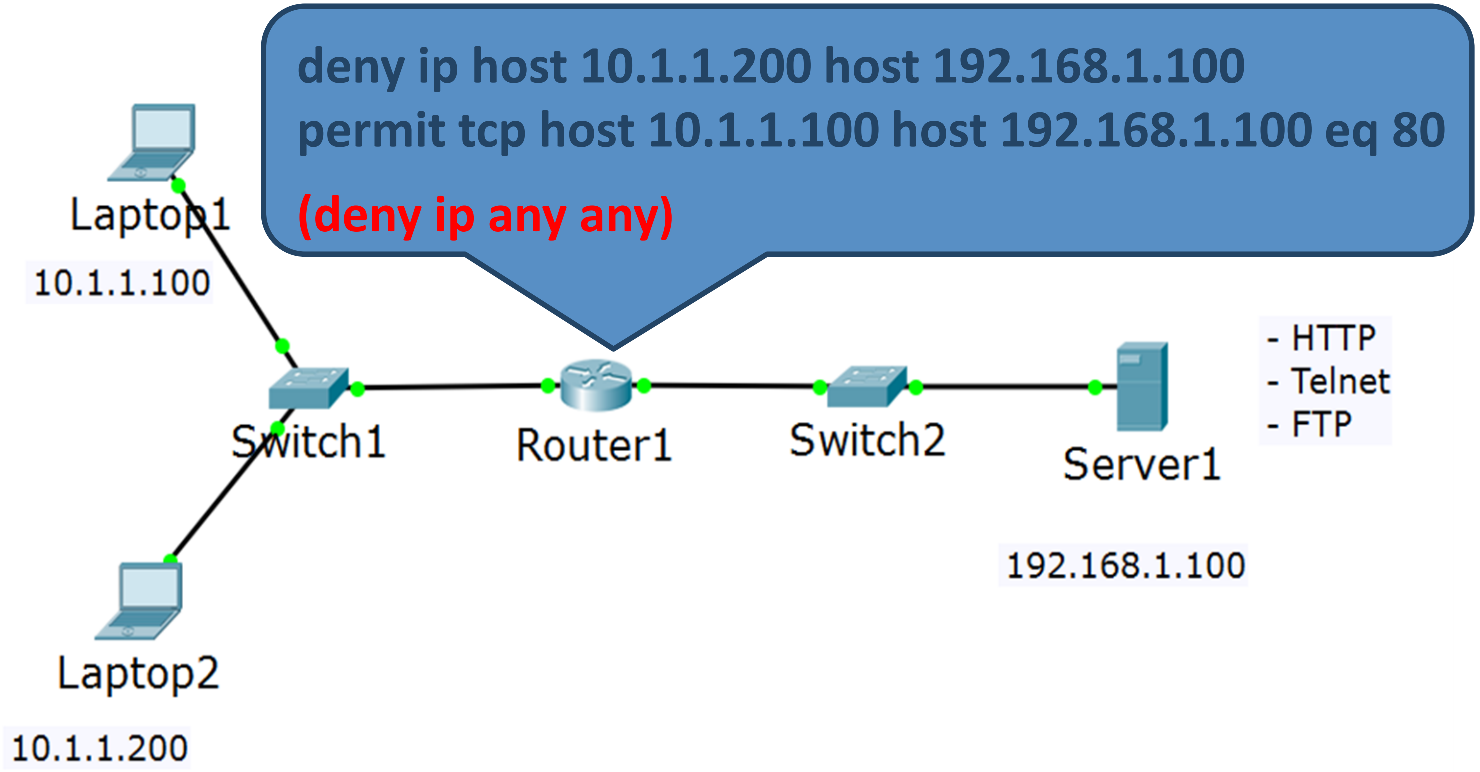
- Q: Is Laptop1 allowed to reach Server1?
  - A: Yes
- Q: Is Laptop2 allowed to reach Server1?
  - A: No



deny ip host 10.1.1.200 host 192.168.1.100
permit ip any any
(deny ip any any)

ACL Process Order – Example 2 with Extended ACL

- Q: Is Laptop1 allowed to reach a web page on Server1?
  - A: Yes
- Q: Can Laptop1 ping Server1?
  - A: No
- Q: Is Laptop1 allowed to reach Telnet and FTP on Server1?
  - A: No



deny ip host 10.1.1.200 host 192.168.1.100
permit tcp host 10.1.1.100 host 192.168.1.100 eq 80

(deny ip any any)

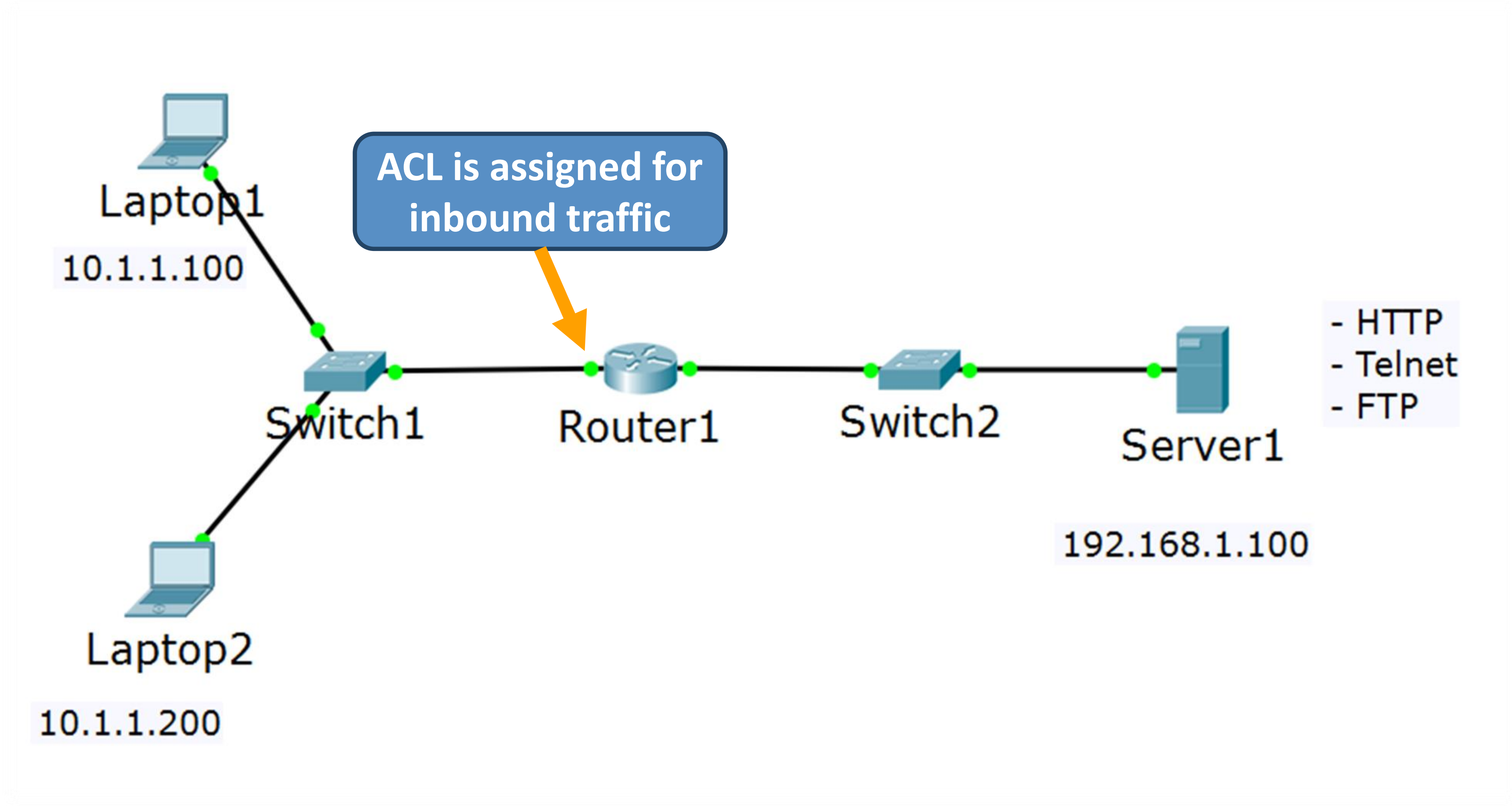
Access Control Lists Configuration

Assigning ACLs

Assigning ACLs

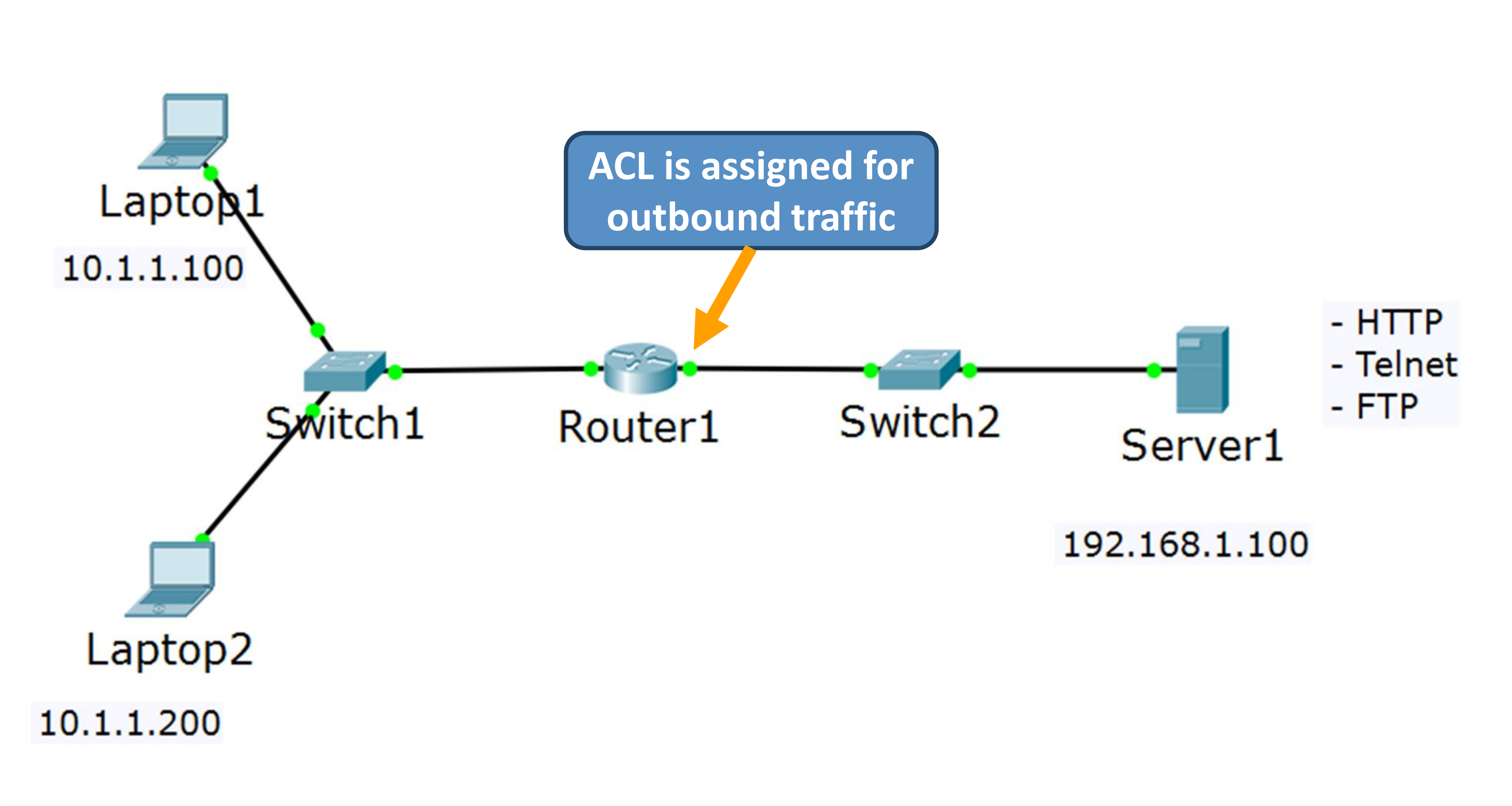
- An ACL in the configuration has zero effect if it is not assigned to interface
- ACLs can be assigned to interfaces inbound or outbound

Assigning ACLs – Inbound



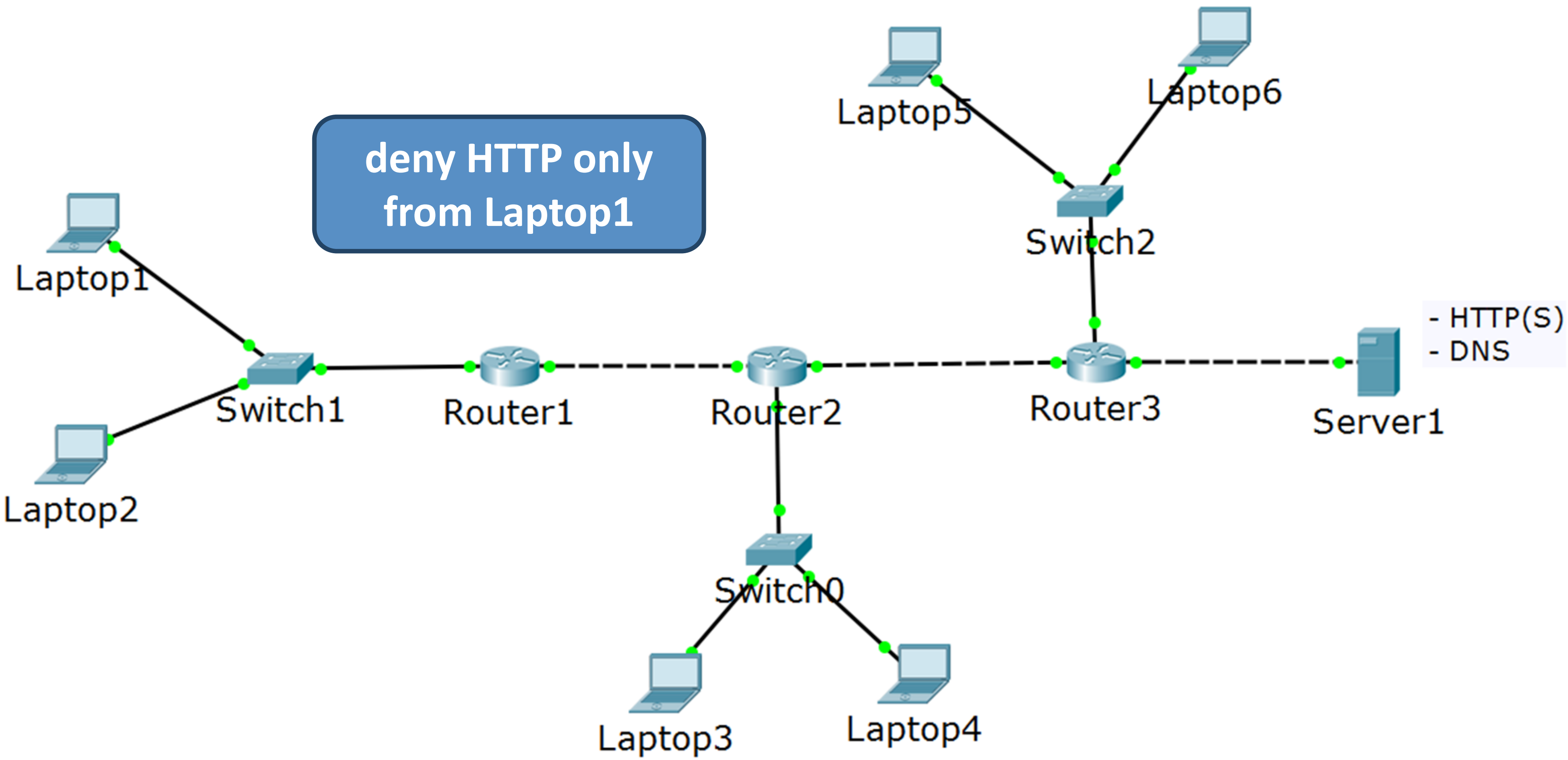
ACL is assigned for inbound traffic

Assigning ACLs – Outbound



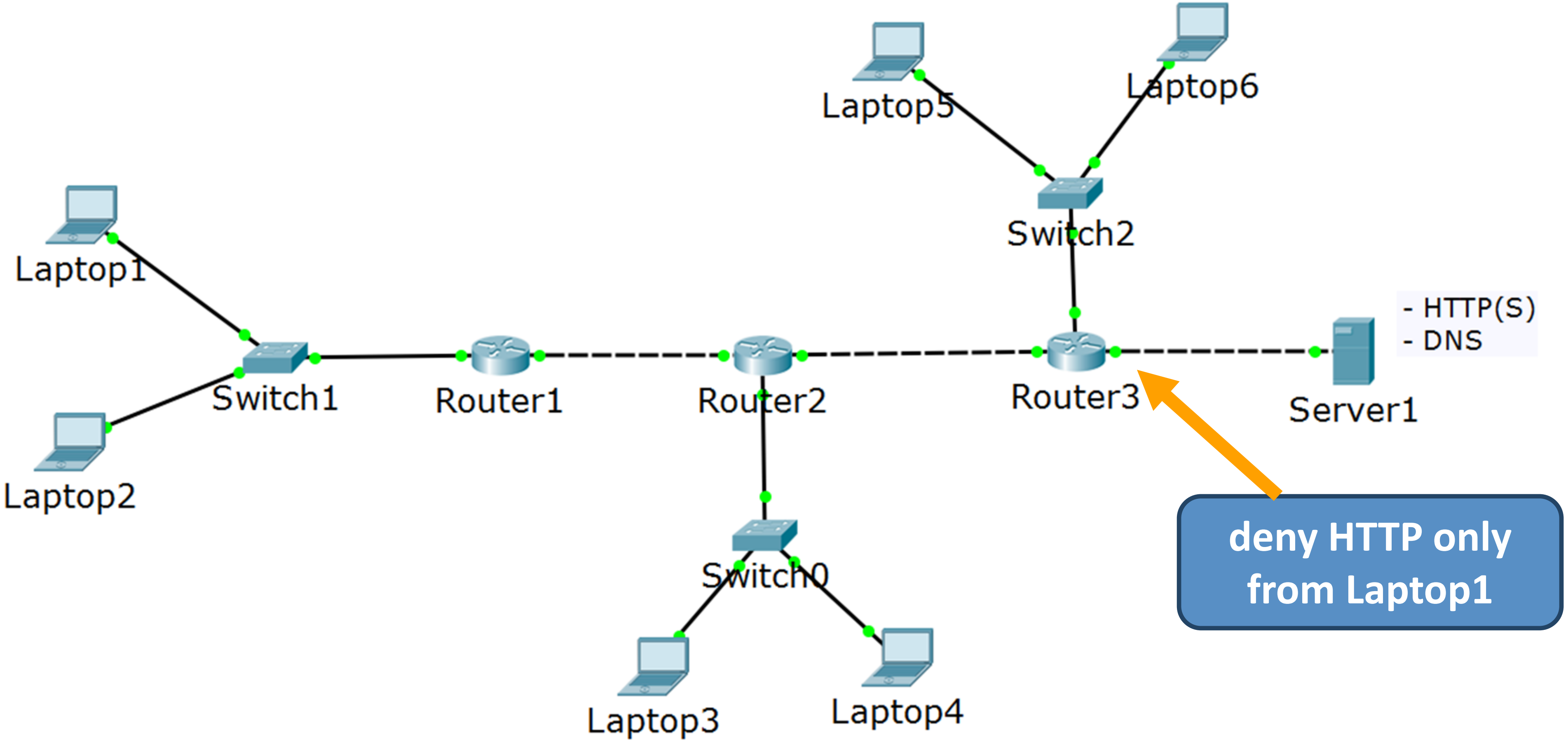
ACL is assigned for outbound traffic

Assigning ACLs – Best Practices



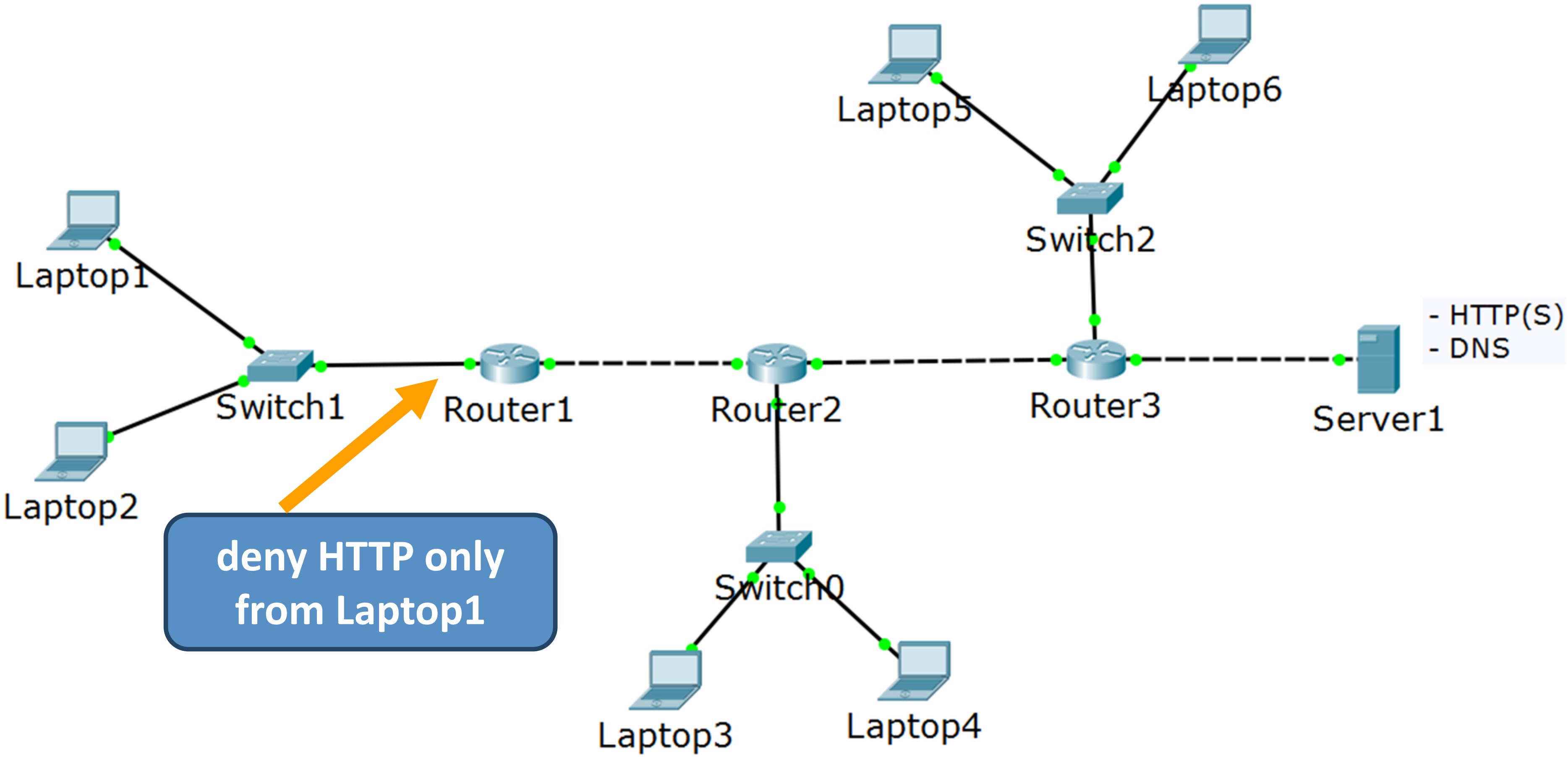
deny HTTP only from Laptop1

Assigning ACLs – Best Practice for Standard ACLs



deny HTTP only from Laptop1

Assigning ACLs – Best Practice for Extended ACLs



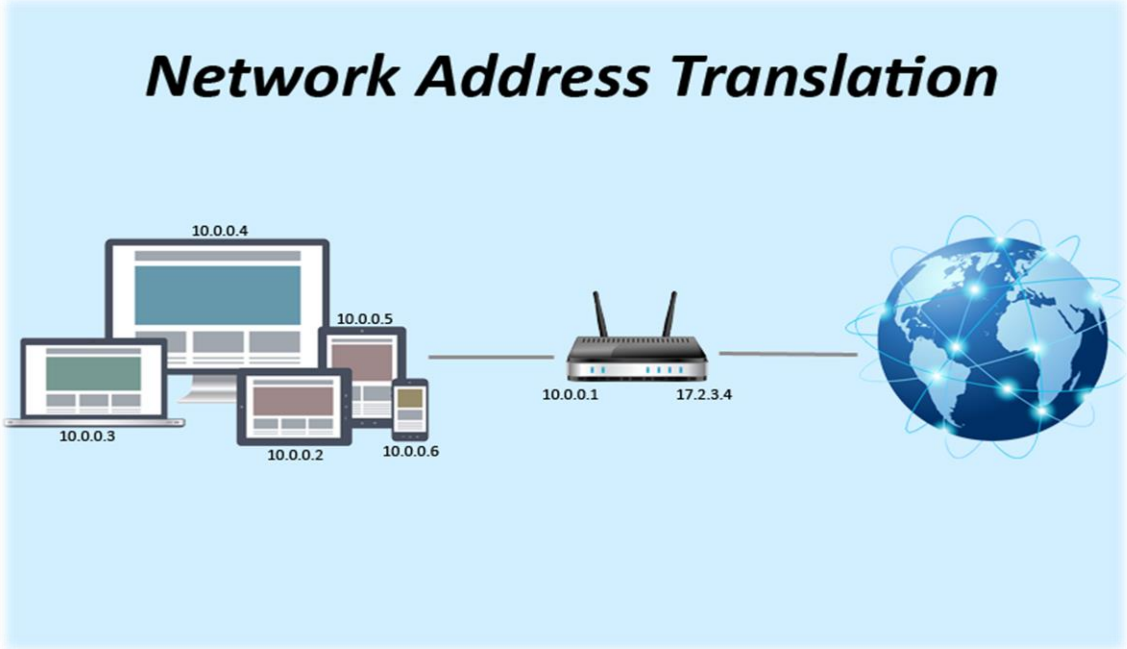
- HTTP(S)
- DNS

deny HTTP only from Laptop1

Network Address Translation

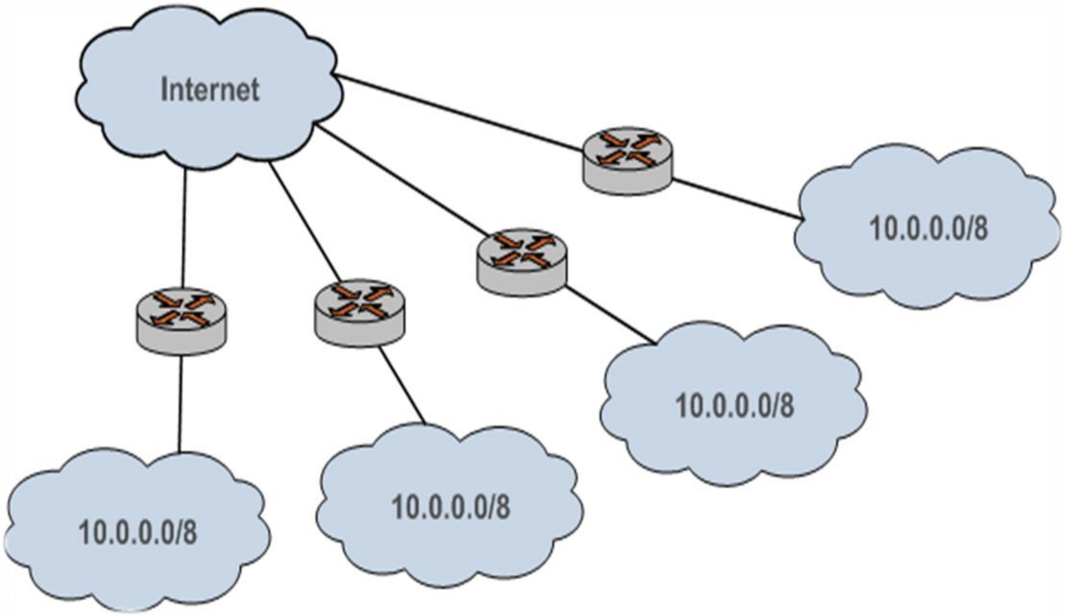
What is NAT?

- NAT: Network Address Translation
- Used to change the source and/or destination IP address of the packets



Why NAT?

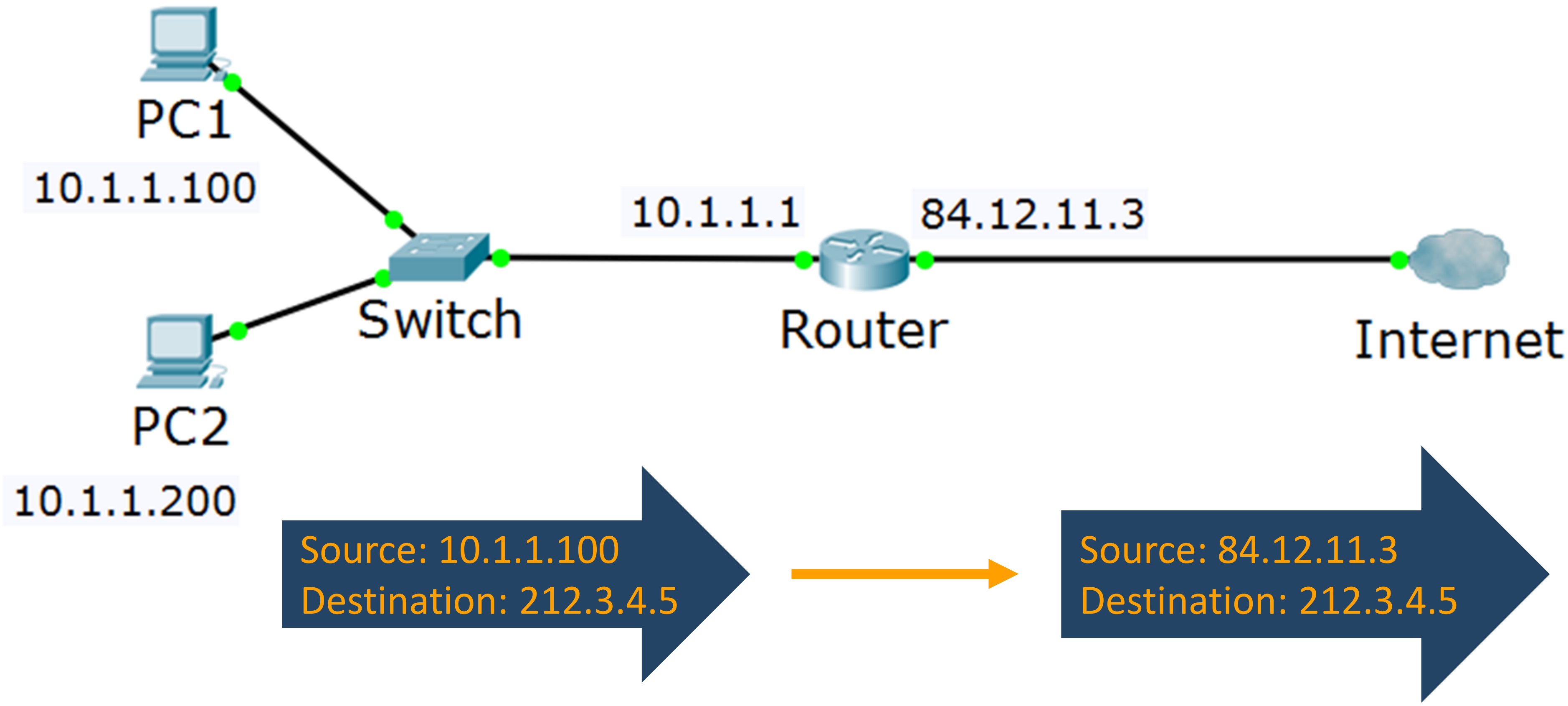
- Primary idea – to solve the "not enough IPv4 addresses" problem
- There are only ≈ 4 billion addresses (in IPv4) – quite insufficient for the huge number of Internet users
- NAT allows the **private addresses** to be **reused** since they are not routed in Internet



Types of NAT

- Static NAT
- Dynamic NAT
- Overloading NAT (PAT)

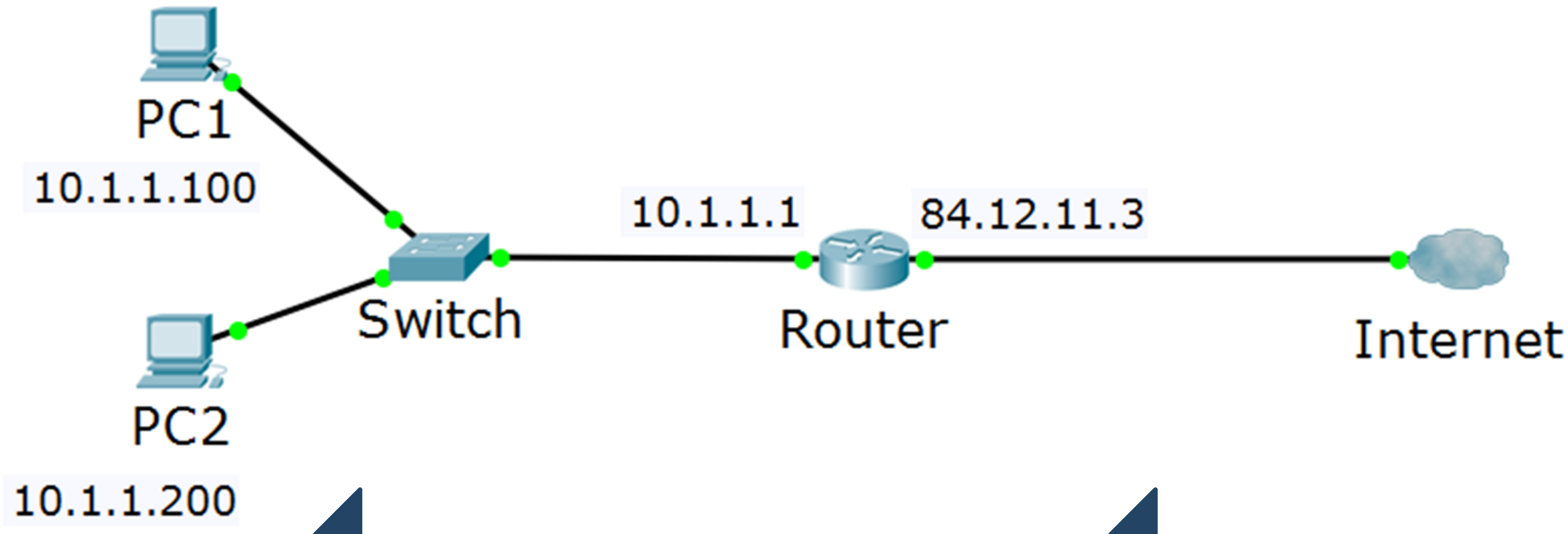
Source NAT – the outgoing packet



Source: 10.1.1.100
Destination: 212.3.4.5

Source: 84.12.11.3
Destination: 212.3.4.5

Source NAT – the returning packet



Source: 212.3.4.5
Destination: 10.1.1.100

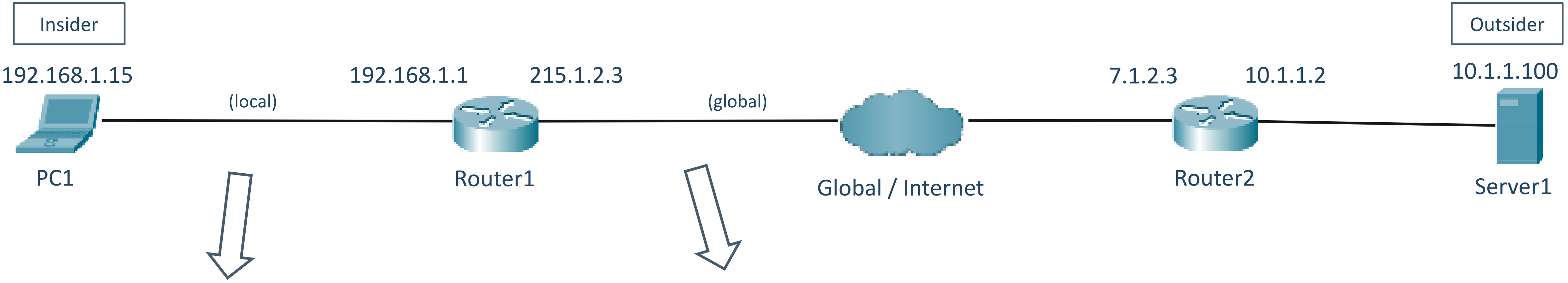
←

Source: 212.3.4.5
Destination: 84.12.11.3

NAT Terminology

- **Inside local** address - assigned to a host on the inside network, typically, private IP address
- **Inside global** address - a public, legitimate IP address that represents one or more inside local addresses to the outside world
- **Outside local** address - IP address of an outside host as it appears to the inside network (can be private address)
- **Outside global** address – public address assigned to a host on the outside network

NAT Terminology – Example



Inside Local: 192.168.1.15

Outside Local: 7.1.2.3

Inside Global: 215.1.2.3

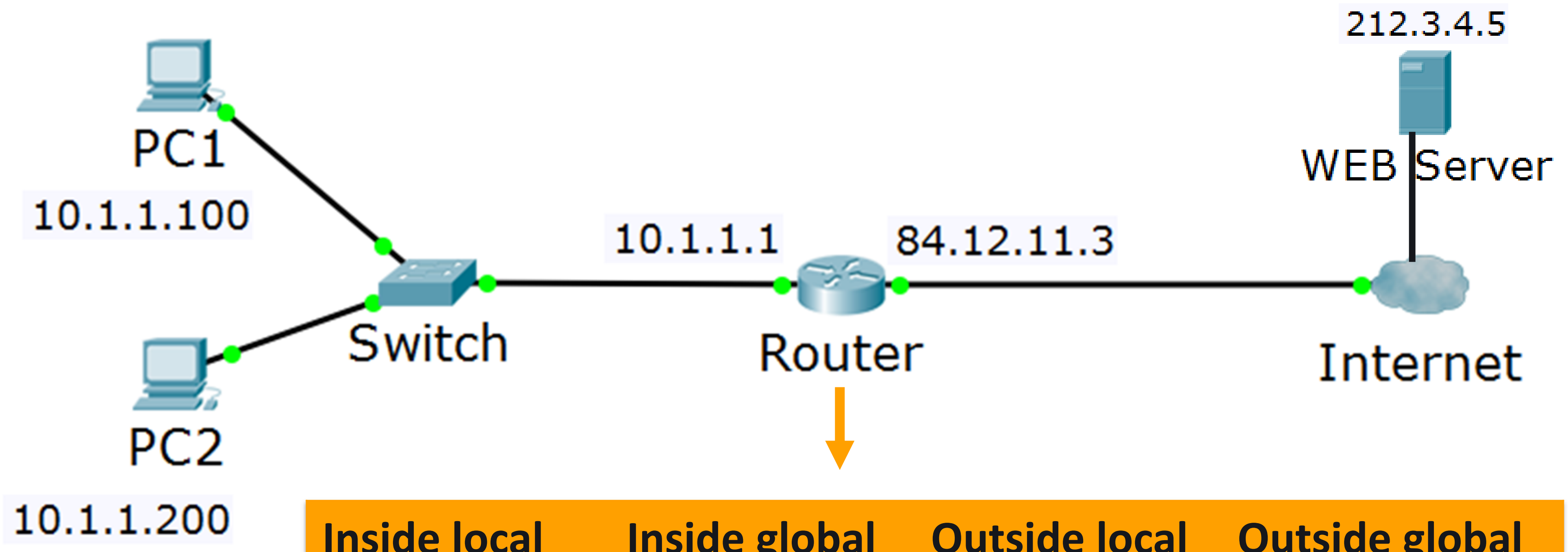
Outside Global: 7.1.2.3

- **PC1 is talking to Server1**
- **Router1 is configured for source NAT and Router2 is configured for destination/static NAT**
- **The terms above are from Router1's perspective**

NAT vs PAT

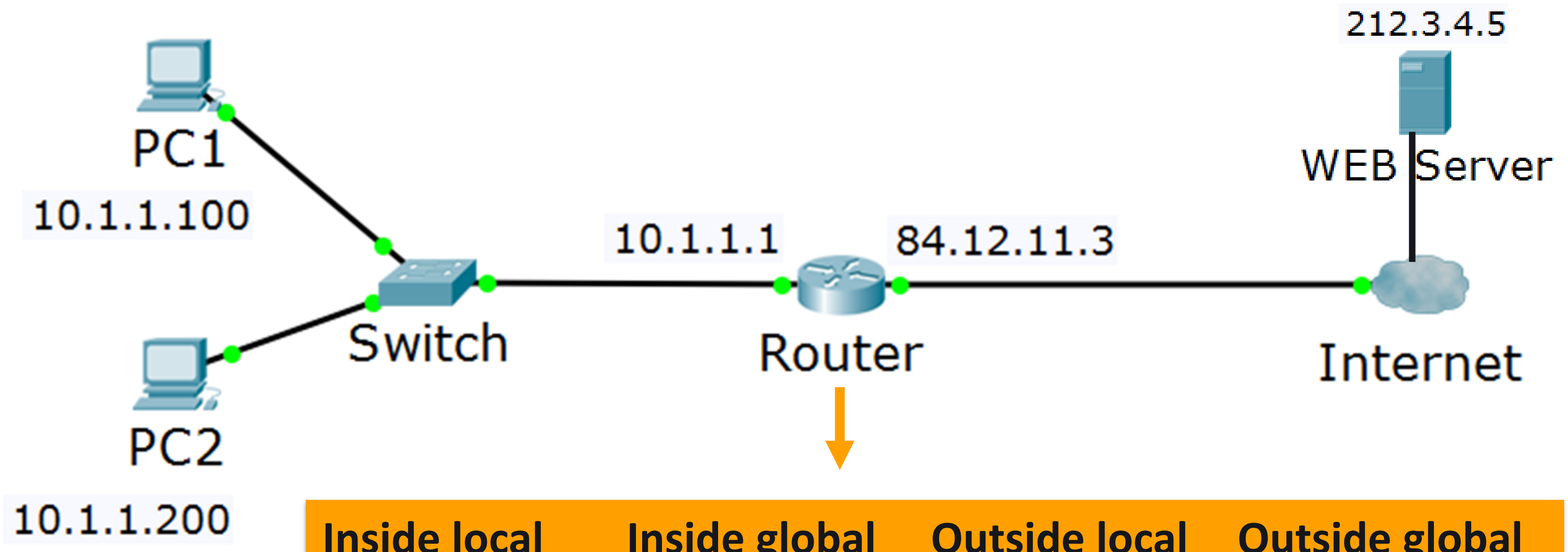
- PAT: Port Address Translation
- In NAT, **1 private** address is translated to **1 public** address
- In PAT, **multiple private** addresses are translated to **1 public**
- PAT creates a table which matches:
  Inside local:source_port -> **Inside global:unique_source_port**
- This way PAT knows to which exact internal host should forward the returning traffic

PAT – Example 1



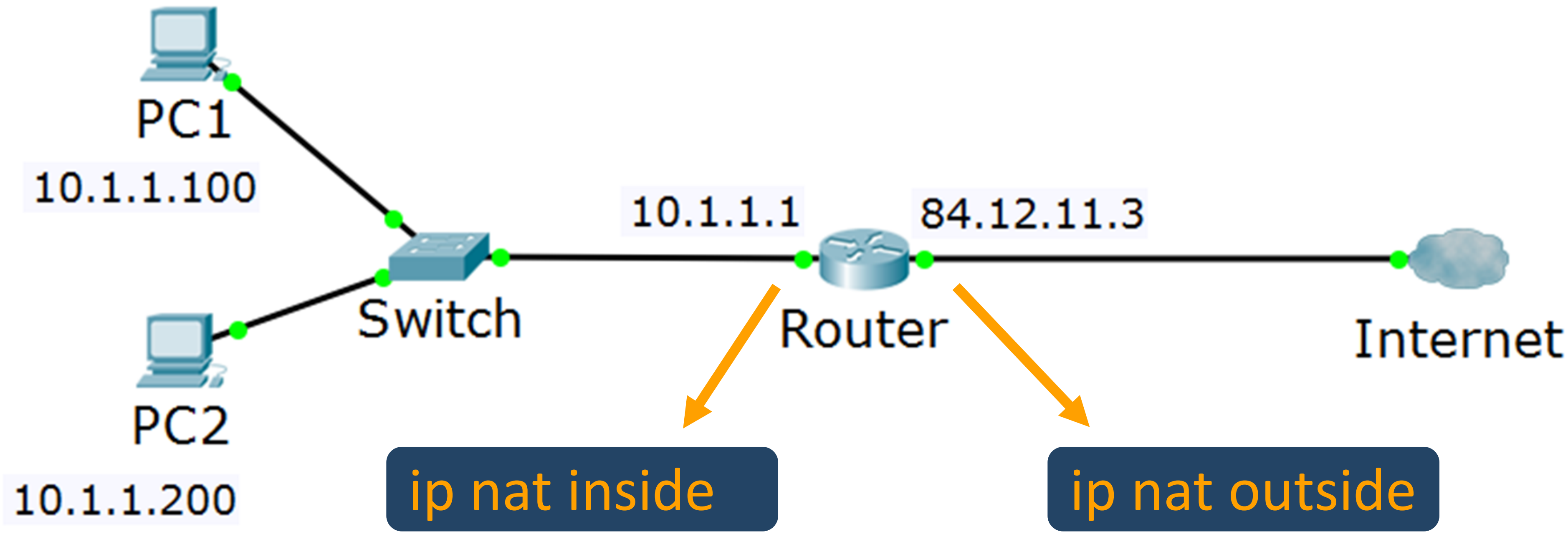
Inside local	Inside global	Outside local	Outside global
10.1.1.100:1024	84.12.11.3:1024	212.3.4.5:80	212.3.4.5:80
10.1.1.200:1025	84.12.11.3:1025	212.3.4.5:80	212.3.4.5:80

PAT – Example 2



Inside local	Inside global	Outside local	Outside global
10.1.1.100:1024	84.12.11.3:1024	212.3.4.5:80	212.3.4.5:80
10.1.1.200:1024	84.12.11.3:1025	212.3.4.5:80	212.3.4.5:80

NAT Configuration – Define the Interfaces



ip nat inside

ip nat outside

NAT Configuration – Define the Translations

- ip nat inside source… command:
  - translates the source of IP packets that are traveling inside to outside
  - translates the destination of the IP packets that are traveling outside to inside
- ip nat outside source… command:
  - translates the source of the IP packets that are traveling outside to inside
  - translates the destination of the IP packets that are traveling inside to outside

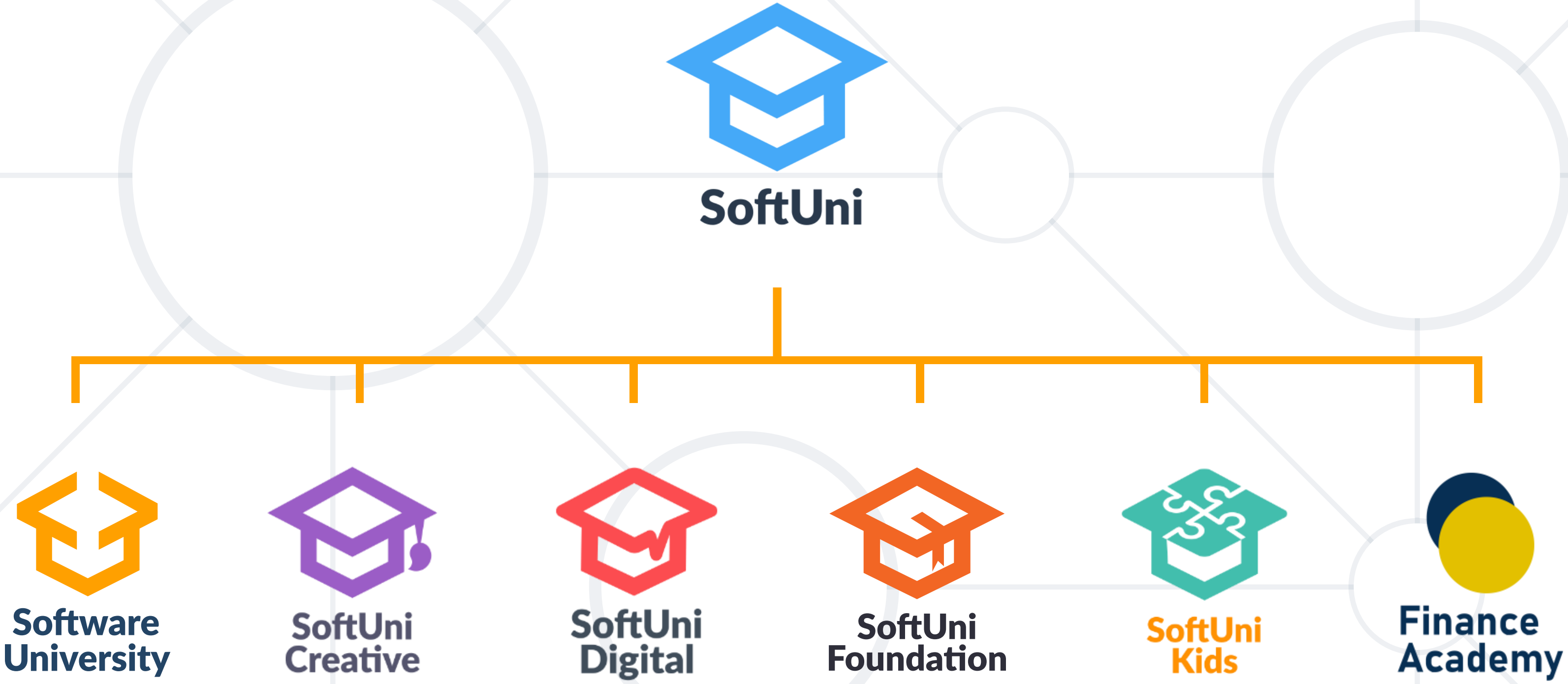
*The first command is used much more often than the second one

Demonstration

Summary

1. Access control lists overview
2. Access control lists configuration
   - Creating ACLs
   - Assigning ACLs
3. Network Address Translation
4. Demonstration

Questions?



SoftUni

Software University

SoftUni Creative

SoftUni Digital

SoftUni Foundation

SoftUni Kids

Finance Academy

SoftUni Diamond Partners

SmartIT

Coca-Cola HBC Bulgaria

SOFTWARE GROUP

DXC TECHNOLOGY

createX

Postbank

Решения за твоето утре

SUPER HOSTING .BG

DRAFT KINGS

VIVACOM

INDEAVR

Serving the high achievers

AMBITIONED

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity
- Software University Forums
  - forum.softuni.bg