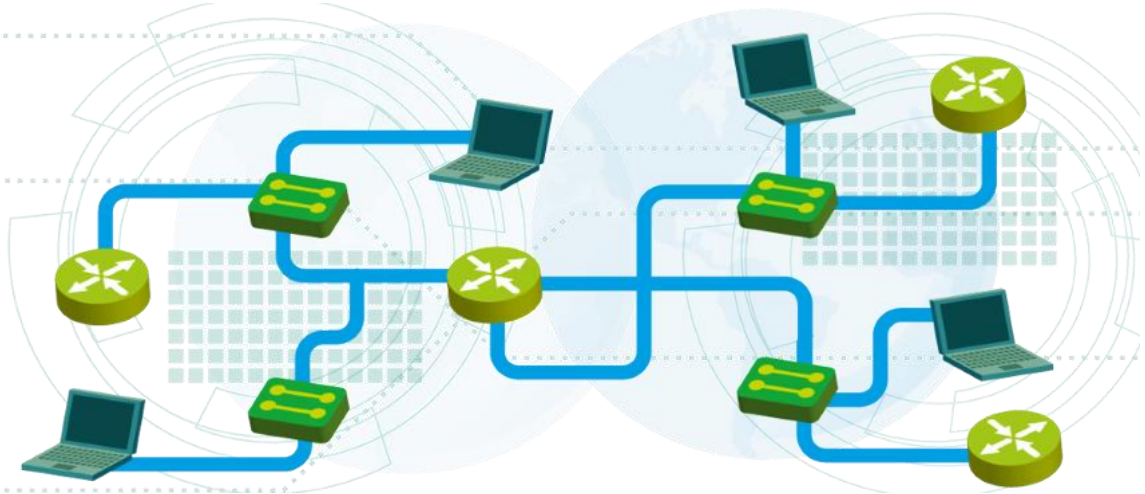
Course summary and exam preparation

Lecture 9



SoftUni Team

Technical Trainers

Software University

http://softuni.bg

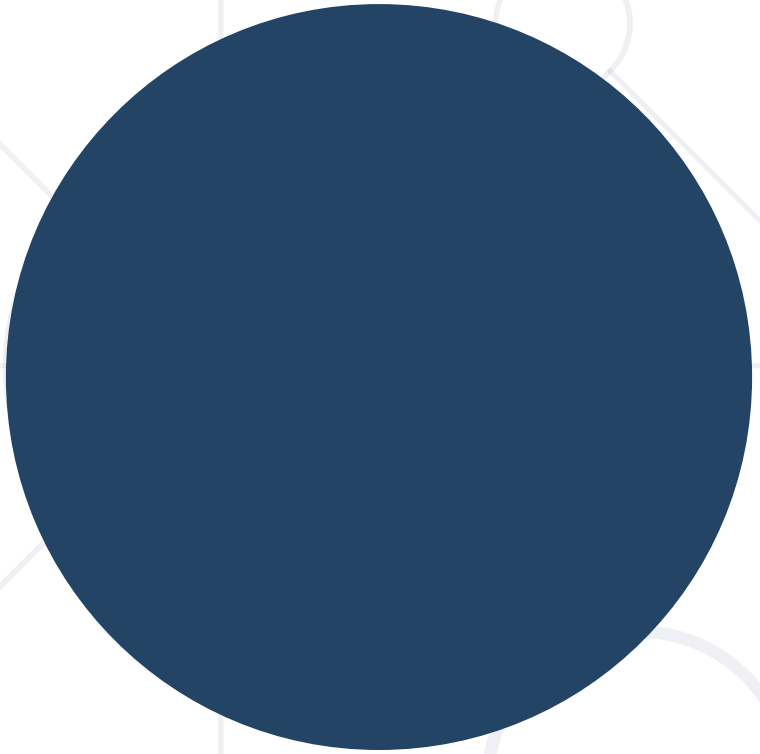
Questions

Software University

sli.do

#CNF

Table of Contents



Basic networking concepts

Back to ToC

What is a computer network?

- Multiple computers linked together
- Why? To communicate and share resources

How did it start?

- ARPANET - The Advanced Research Projects Agency NETwork
- Established in 1969
- It is the first packet switching network which will use TCP/IP
- It was designed for scientific purposes and to share computer resources
- ARPANET's purpose was more academic than military

Common Types of Computer Networks

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Wireless Local Area Network (WLAN)
- Storage Area Network (SAN)
- Home Area Network (HAN)

Common Types of Networking Devices

Software University

- Hub (obsolete, not secure and very slow)
- Switch
- Router
- Modem
- Firewall
- Bridge (like a Switch, fewer ports)
- Repeater (like a Hub, it just amplifies the signal)
- Access point

What is a (network) protocol?

Software University

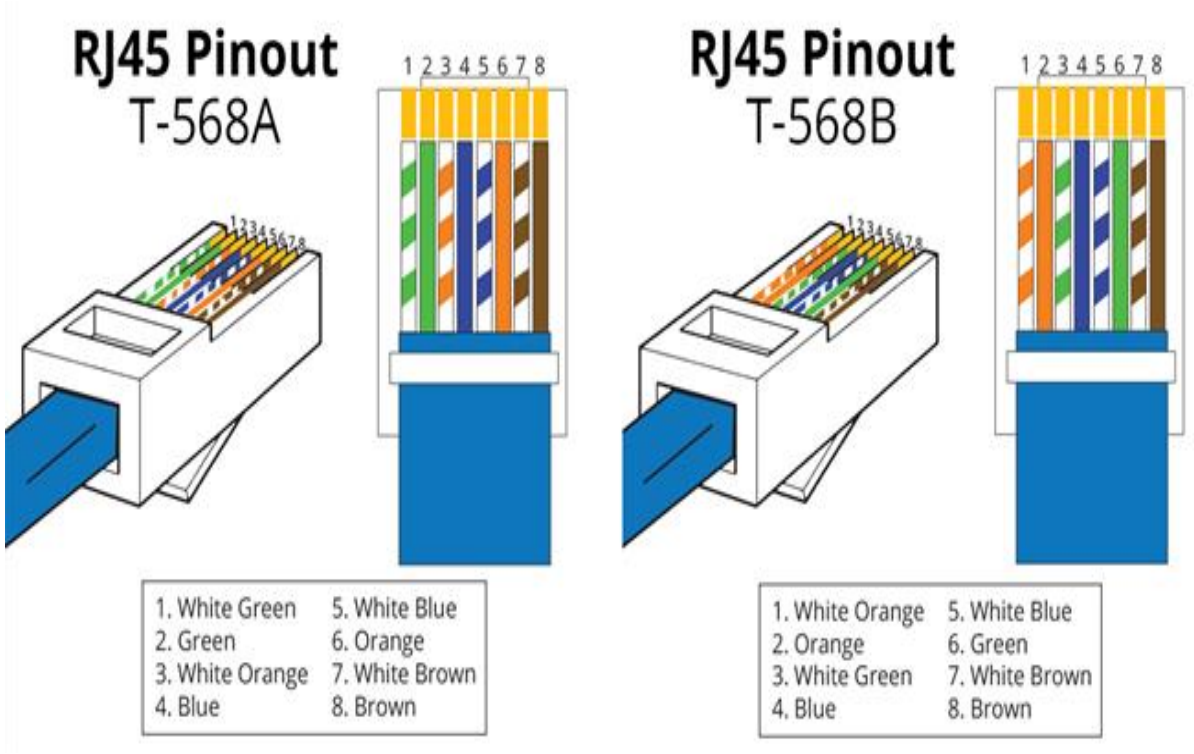
- Protocol: A general term, typically defining a system of rules and acceptable behavior
- Can be used in politics, diplomacy, science, medicine, etc.

What is a network protocol?

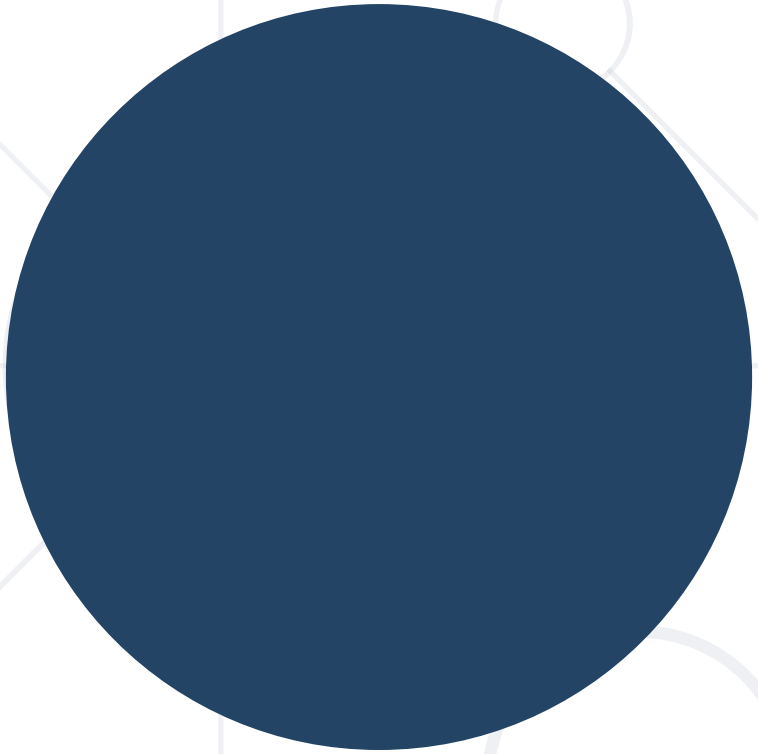
CLOUDFLARE

In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.

EIA/TIA Standards

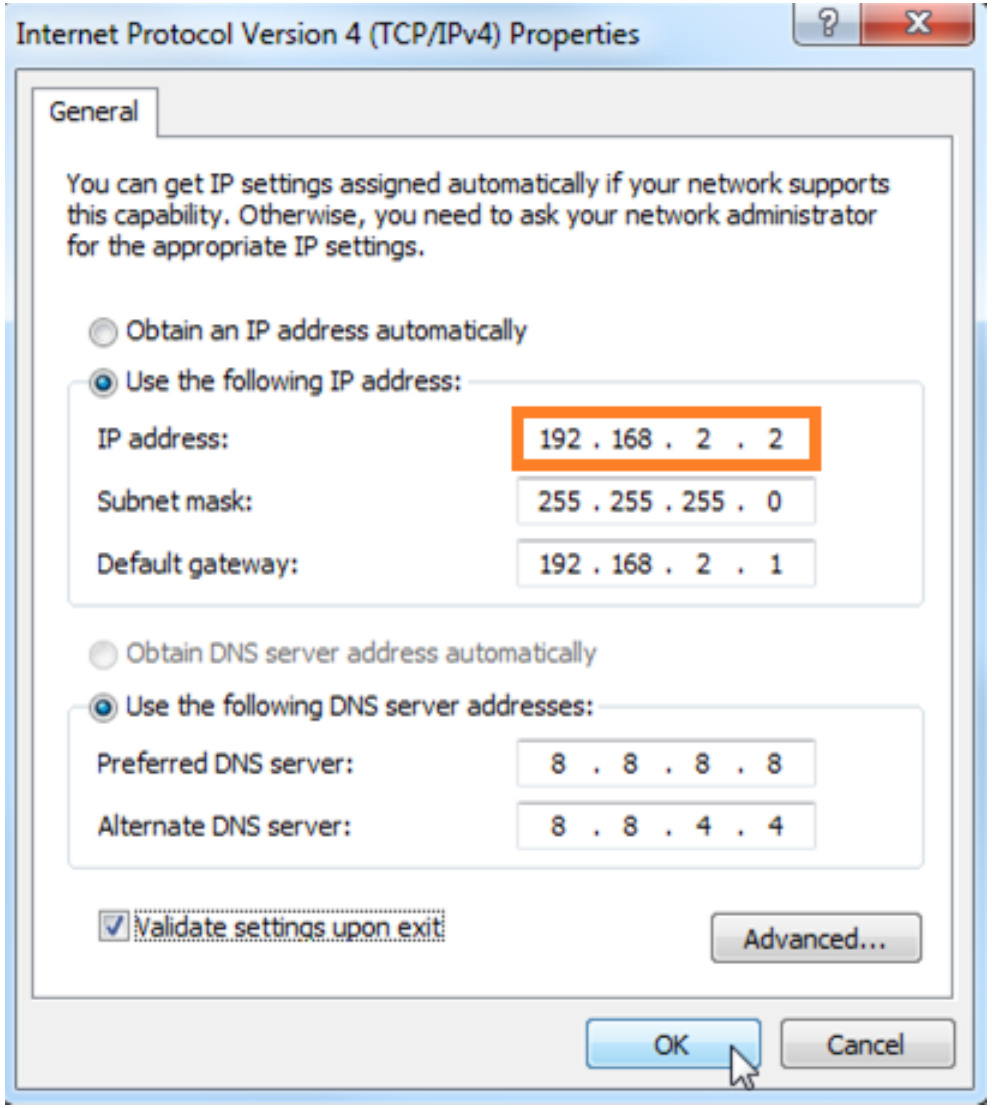


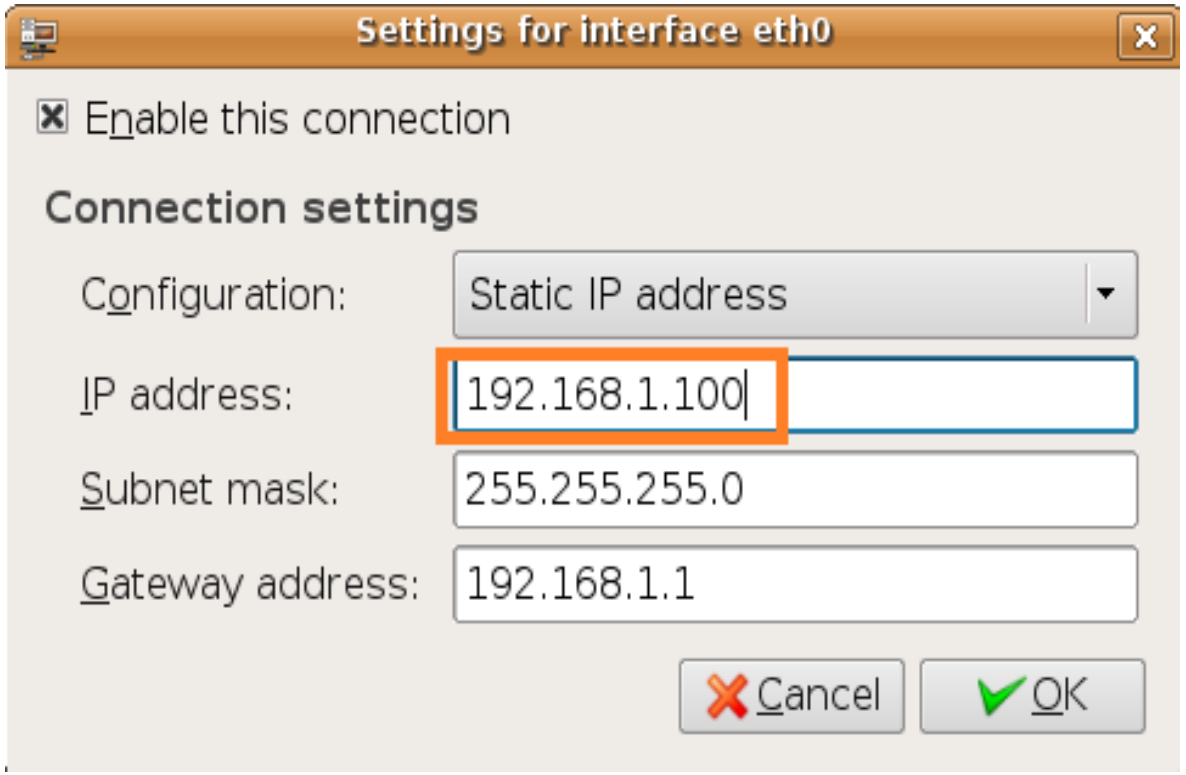
- EIA = Electronic Industries Alliance
  TIA = Telecommunications Industry Association
- T568B is most frequently used



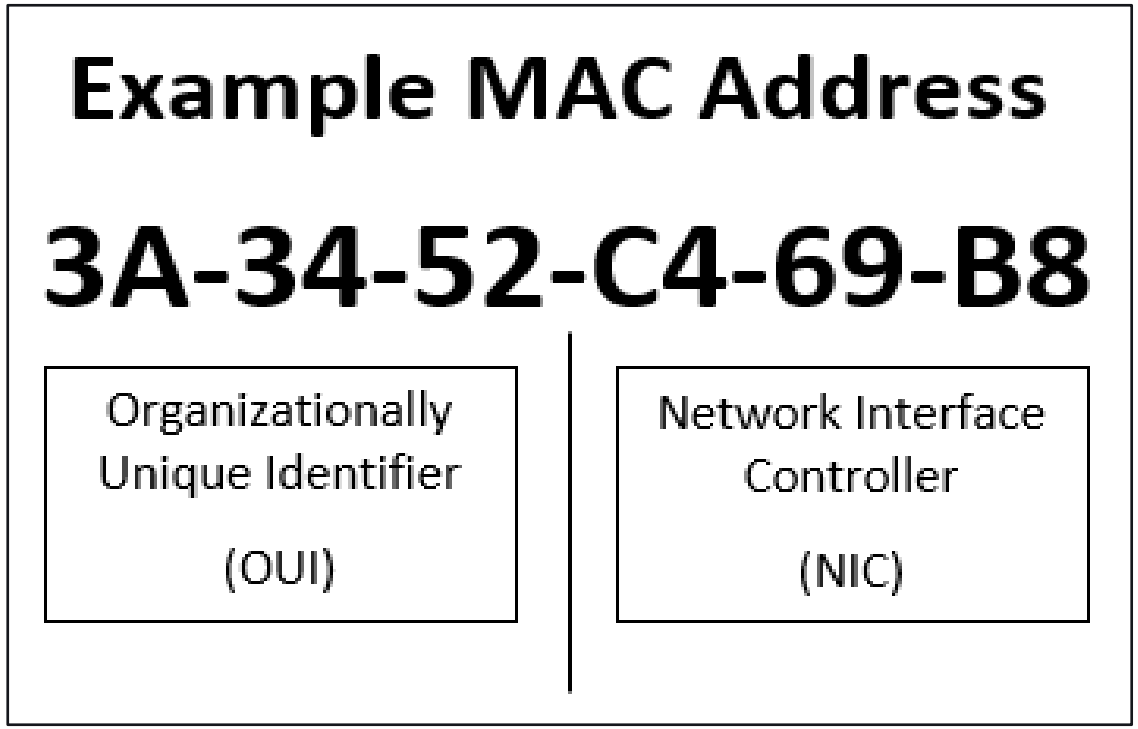
IP and MAC addresses

IP Addresses (2)

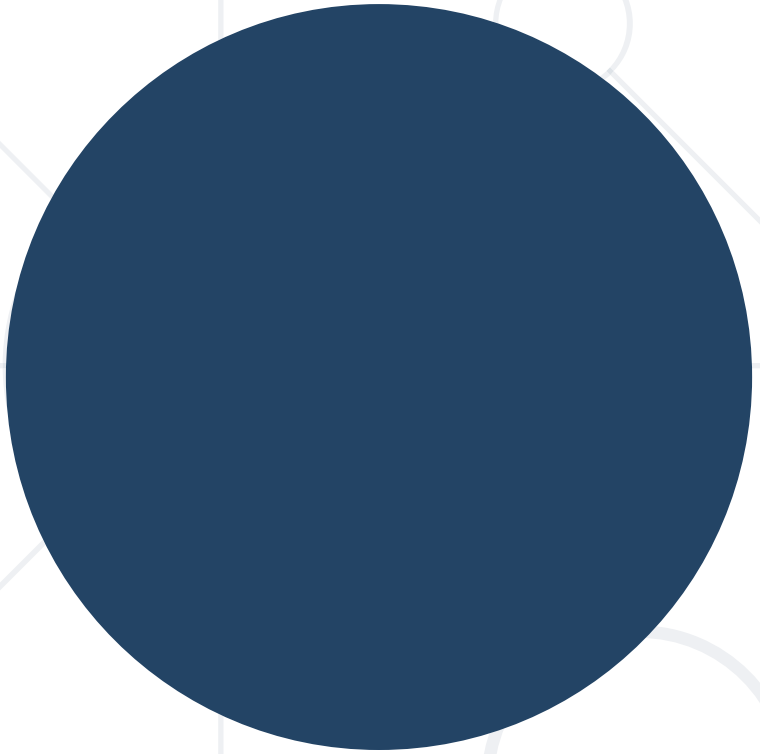




MAC Addresses



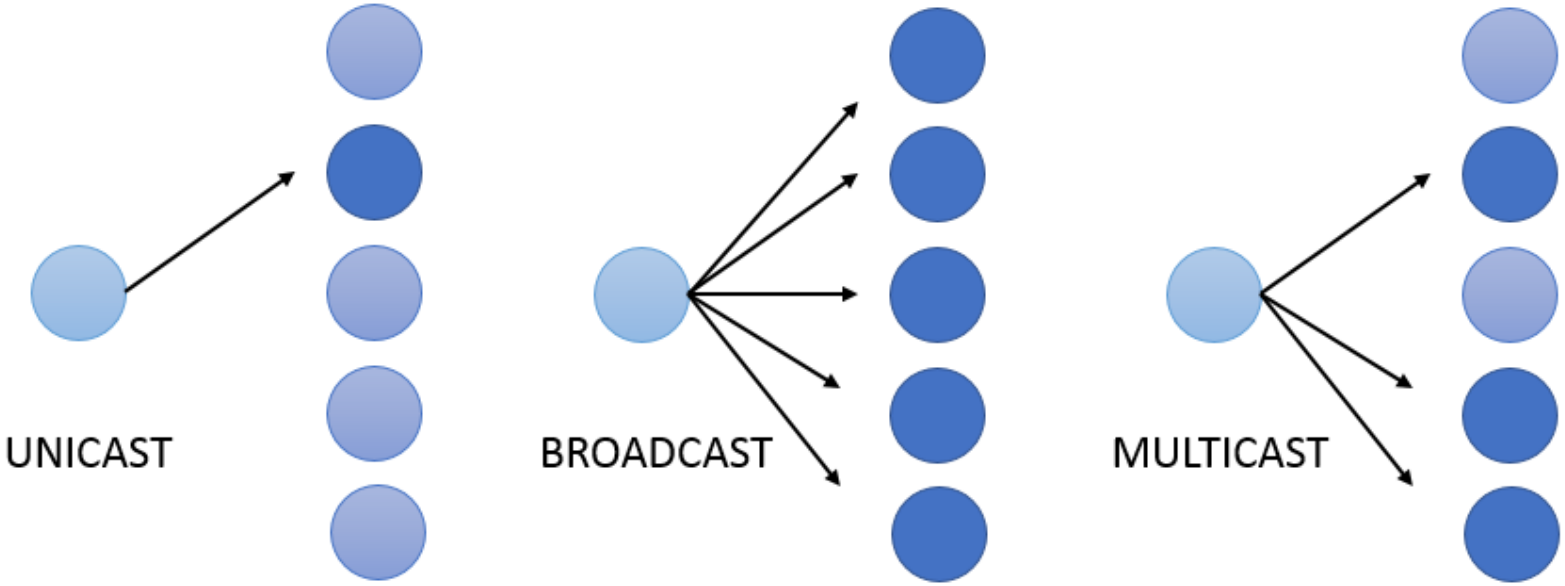
- Known as physical address
- Unique identifier assigned to network interfaces
- 48 bits or 6 bytes in a hexadecimal format (discussed later in the course)
- Can you change it?

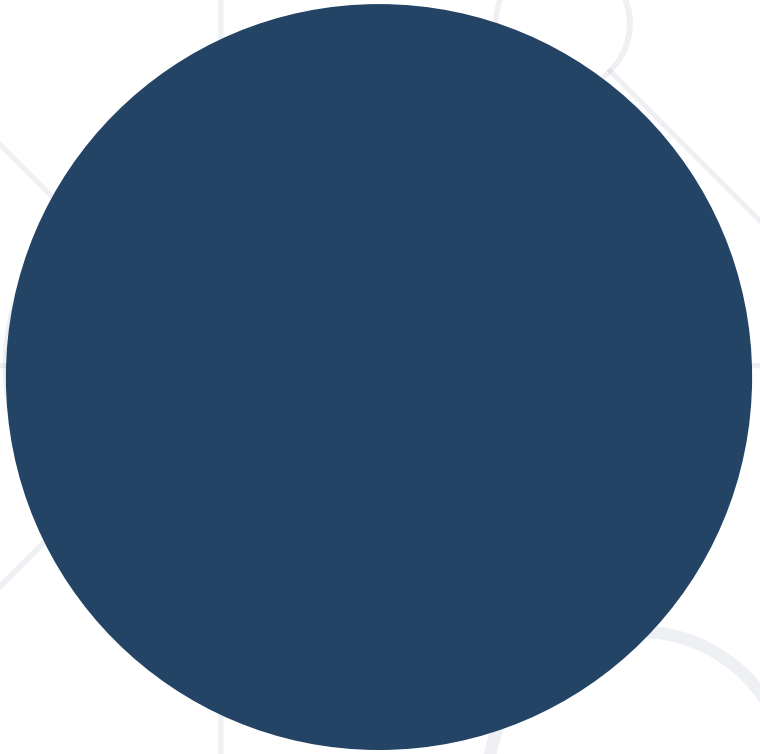


Traffic types

Types of traffic

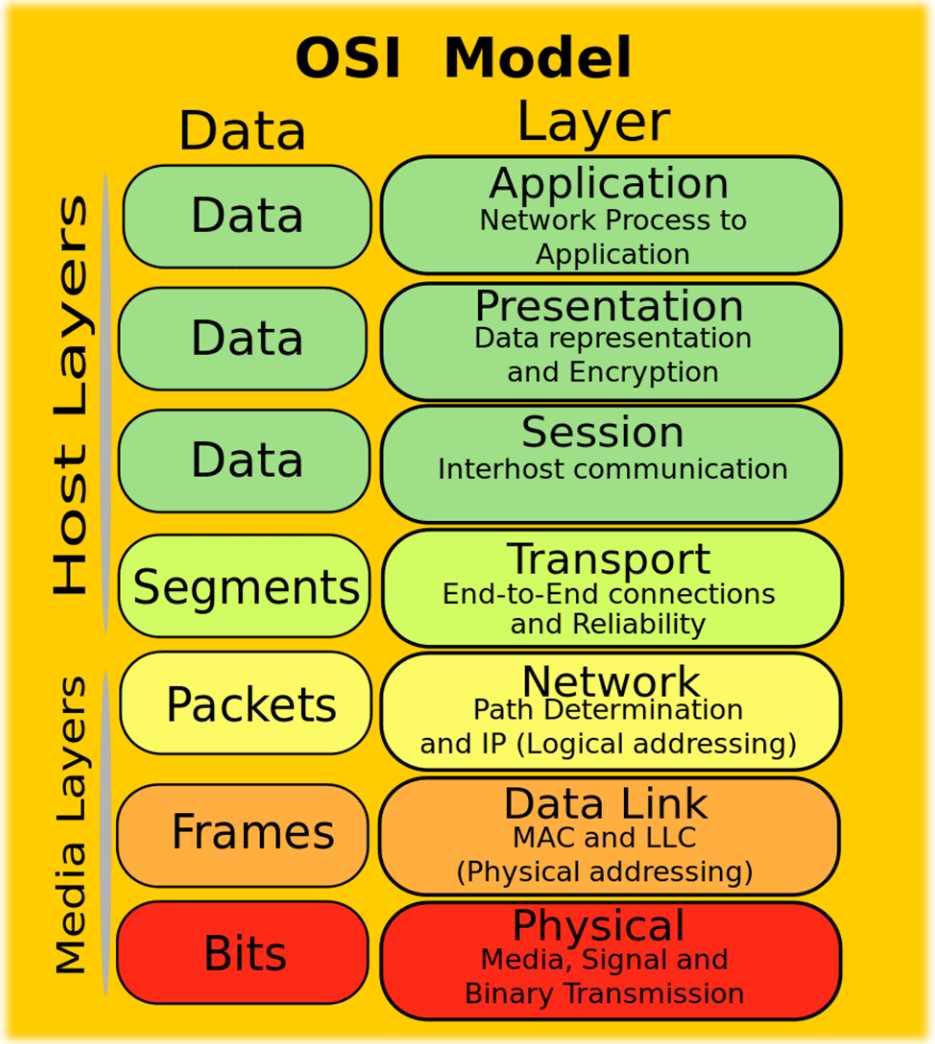
- ONE TO ONE (UNICAST)
- ONE TO ALL (BROADCAST)
- ONE TO SEVERAL (MULTICAST)





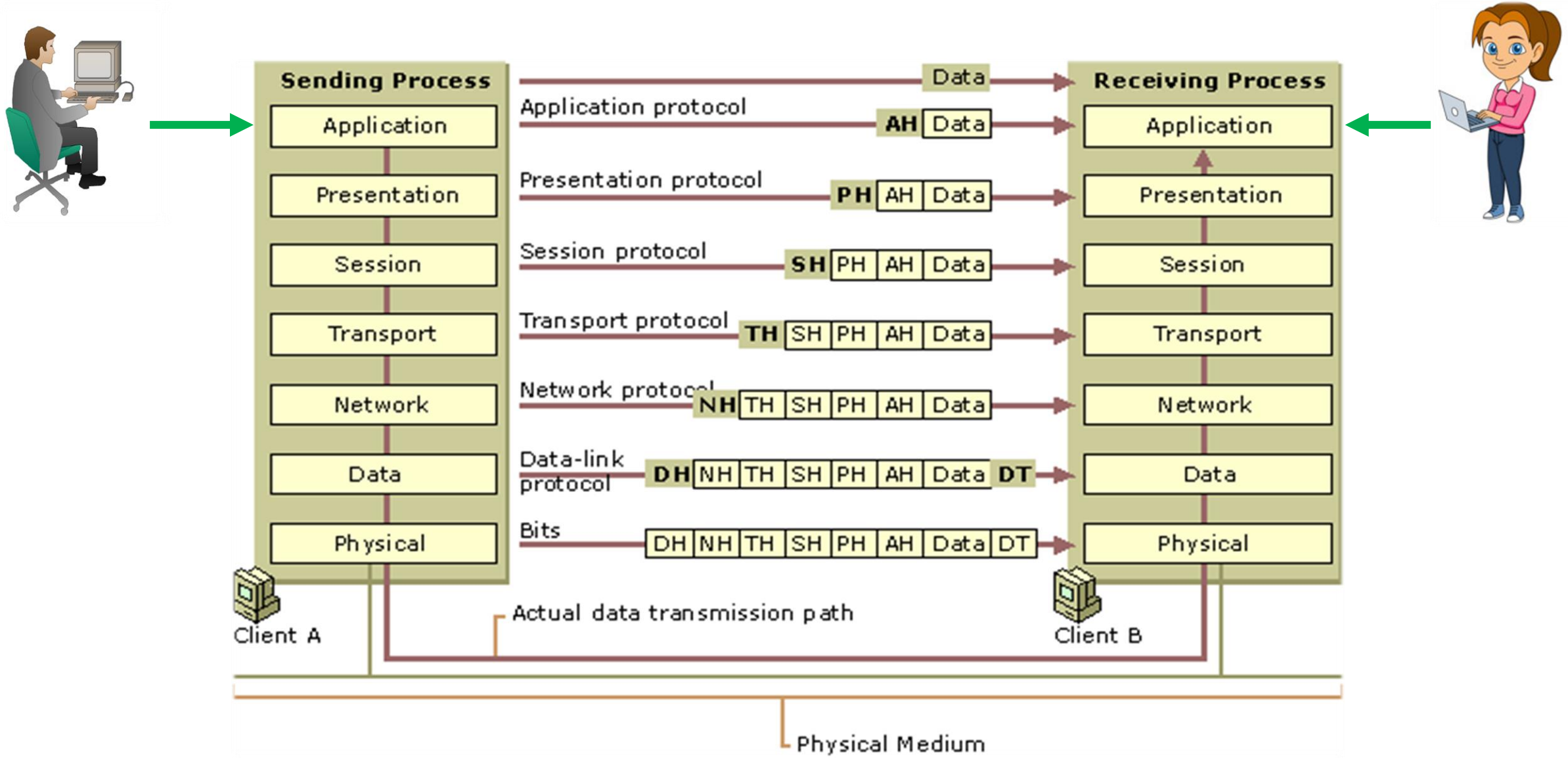
OSI and TCP/IP models

OSI Model

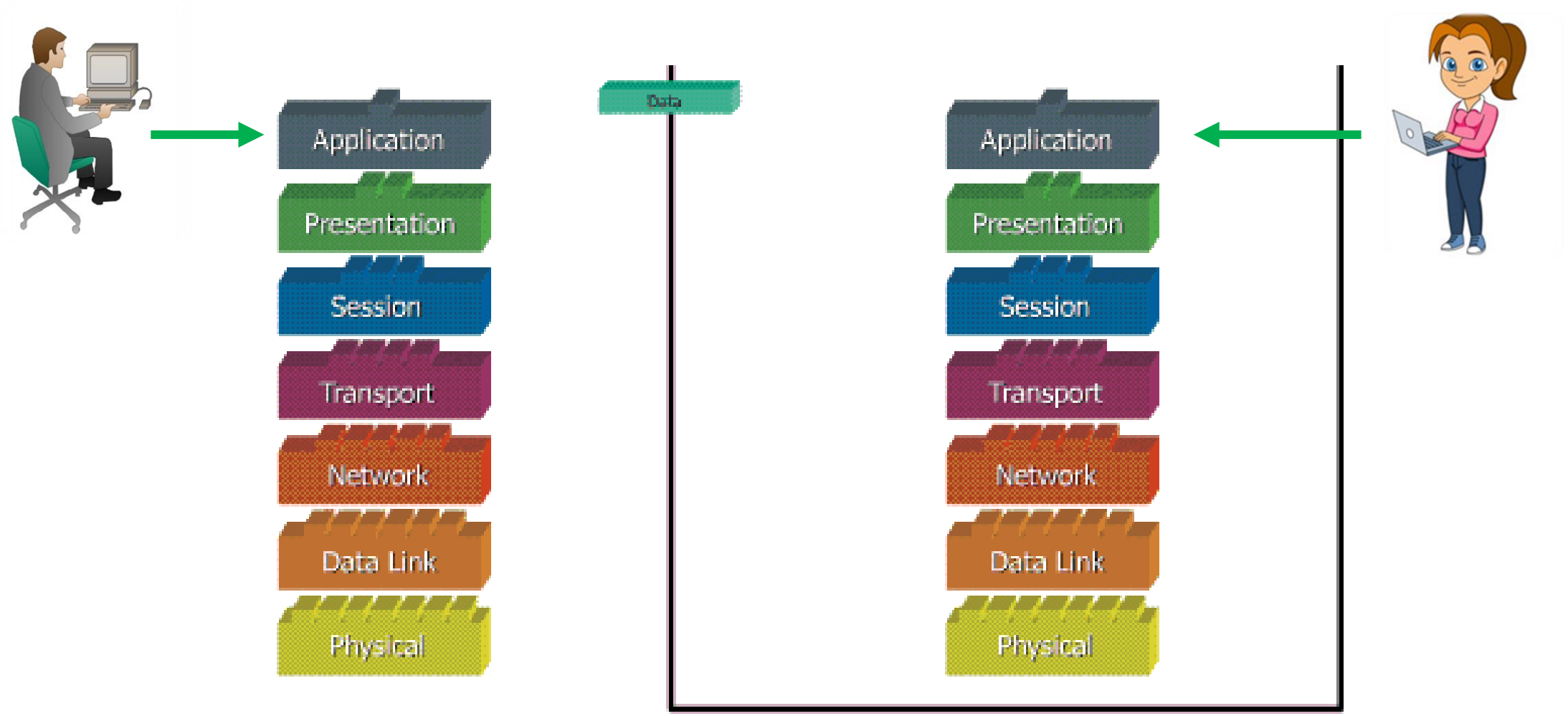


- OSI = Open Systems Interconnection
- Why?
  - Organizes the information
  - Simplifies learning
  - Standards for the vendors
  - Easier troubleshooting
- Protocol Data Unit (PDU) – different data format at each layer

Data Flow in the OSI Model

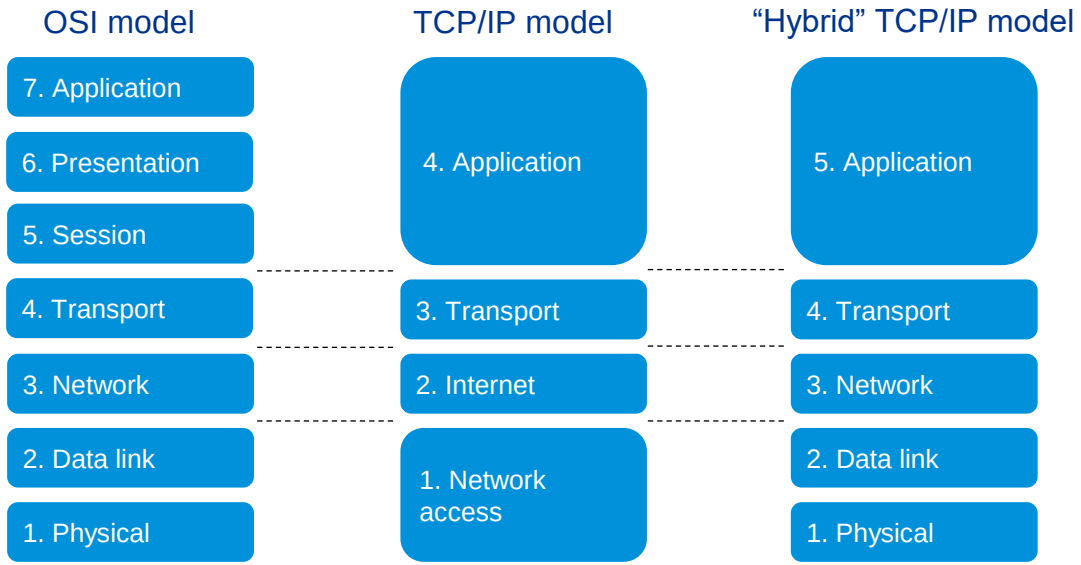


Data Flow in the OSI Model (2)

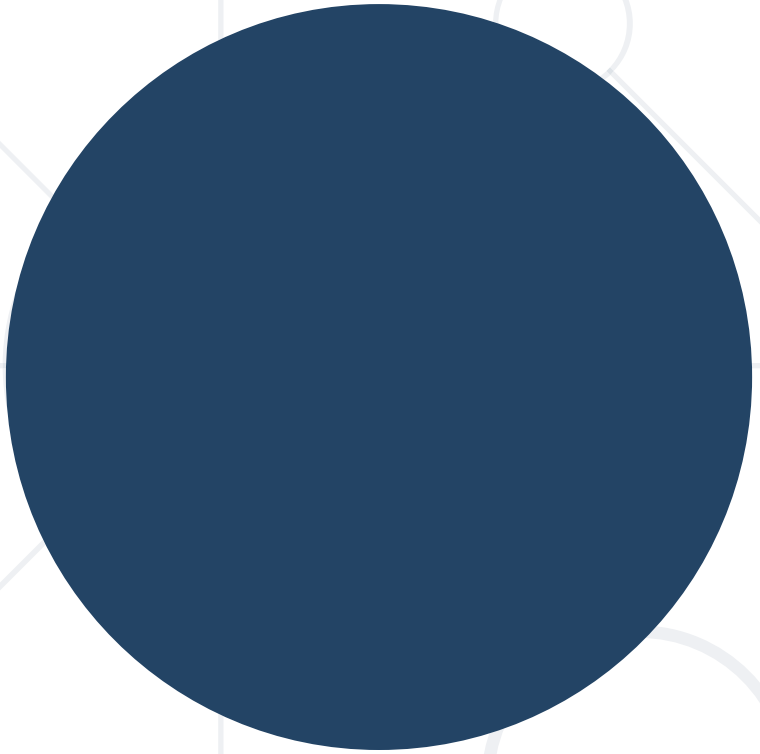


OSI and other networking models

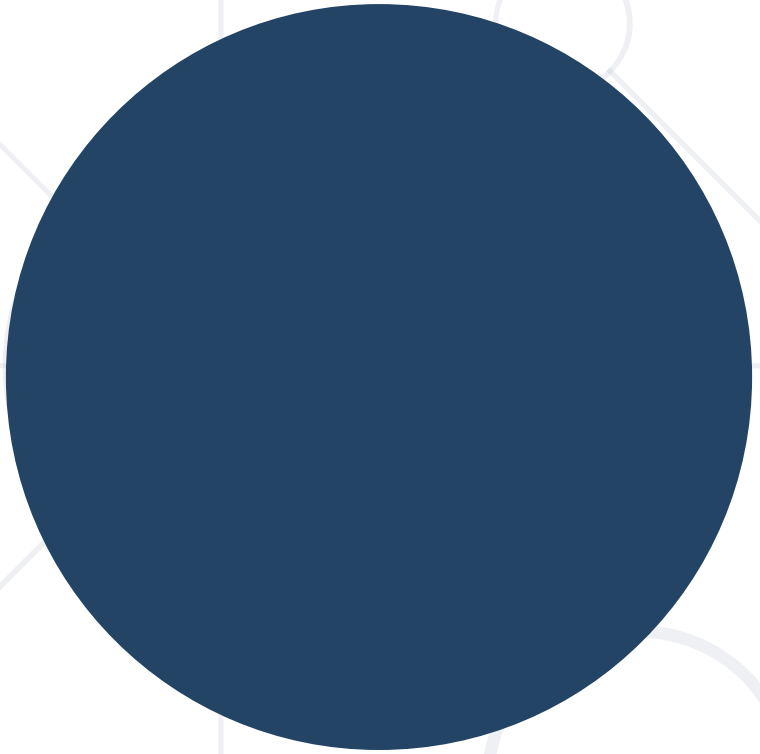
- Originally, the “TCP/IP model” was developed before the OSI model
- Later on, multiple other models were created
- The “hybrid TCP/IP model” is considered as one of the most practical models today



Wikipedia: Internet protocol suite



Cisco Packet Tracer - Introduction



Binary, decimal and hexadecimal numbers

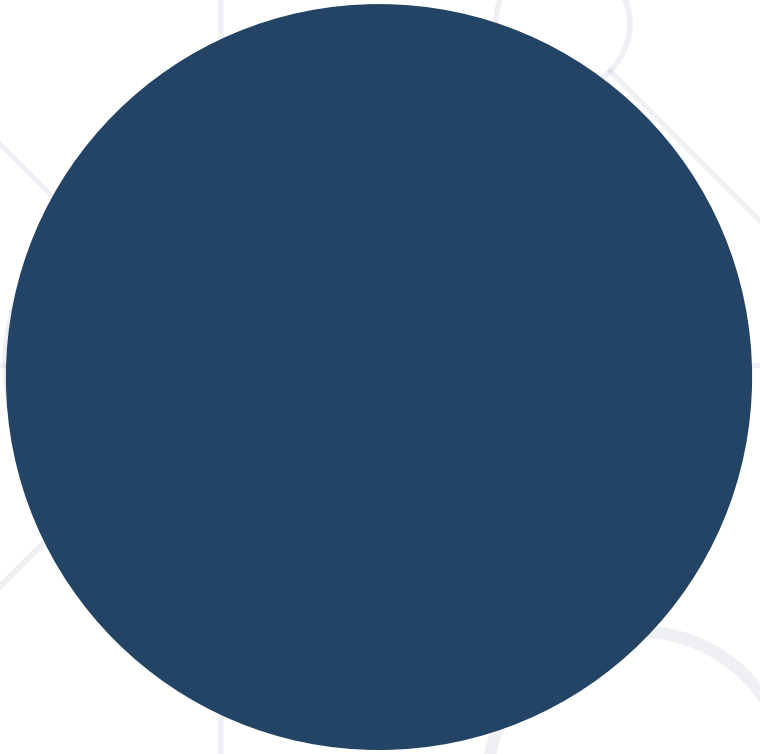
Back to ToC

Different numeral systems

Hexadecimal	Binary	Decimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

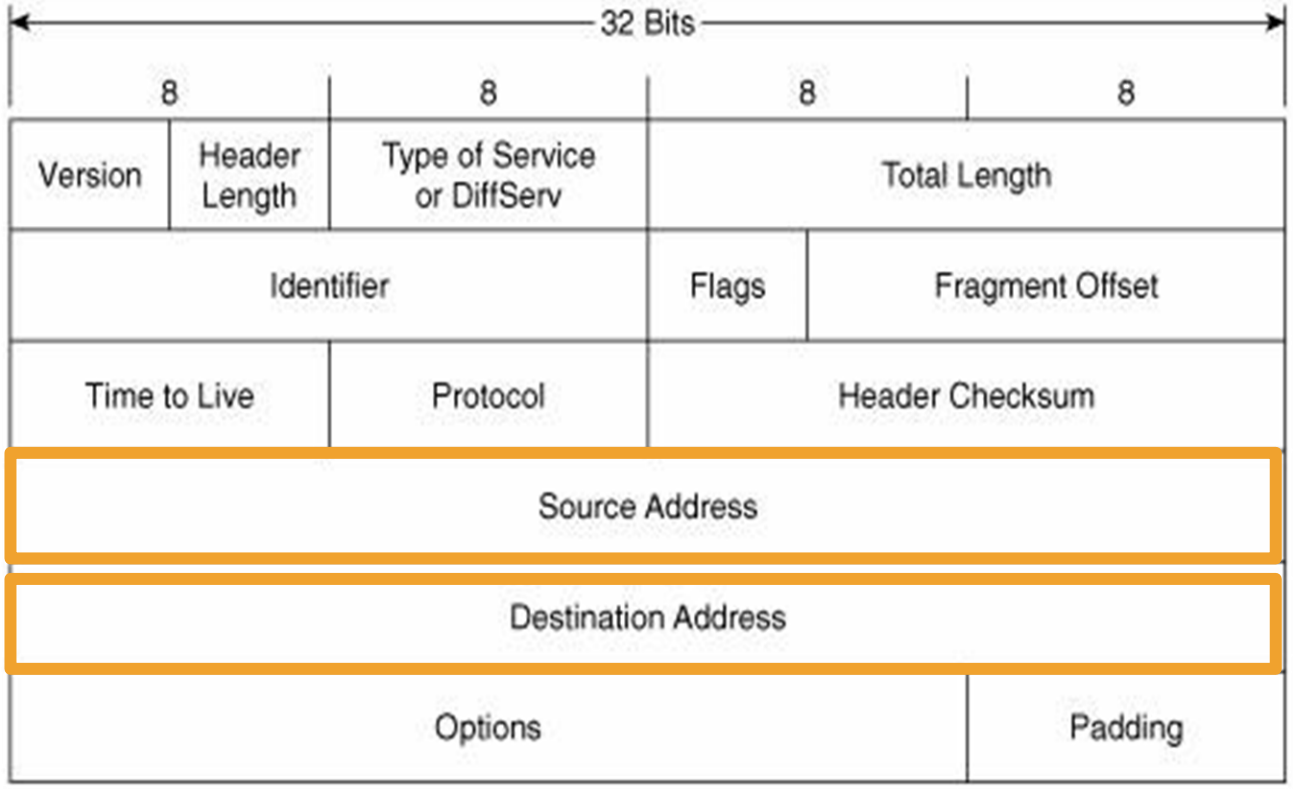
Common Numeral Systems in computer networking:

- Decimal
- Binary
- Hexadecimal



IPv4

IPv4 Address



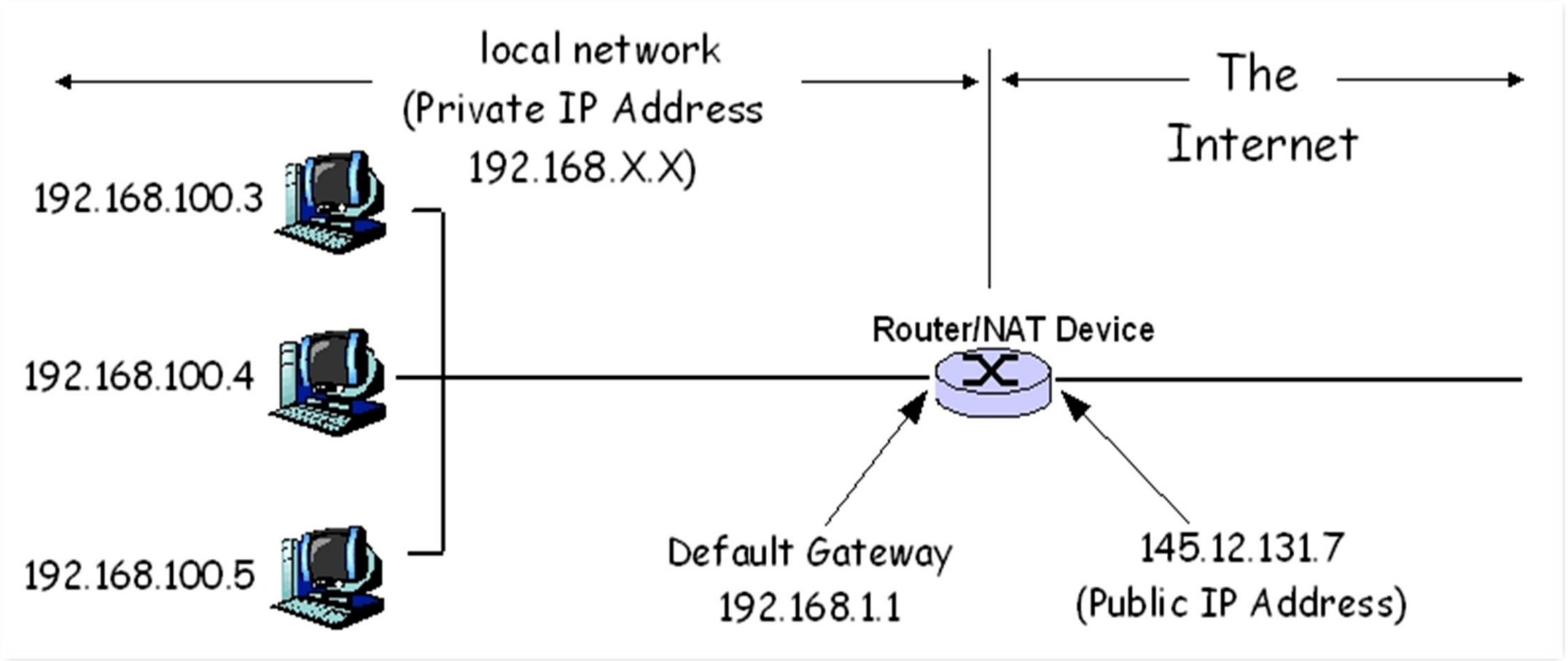
- Plays important role for device connectivity
- It is a 32-bit address
- There are
  4 294 967 296
  IP addresses (2^{32})

Private IP addresses

Class	Start of range	End of range
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

- Used for addressing internal networks (offices, HQs etc.)
- Not routable on the Internet
- Can be reused in many networks
- Range of private addresses for each class (classes are discussed later)

NAT – Network address translation



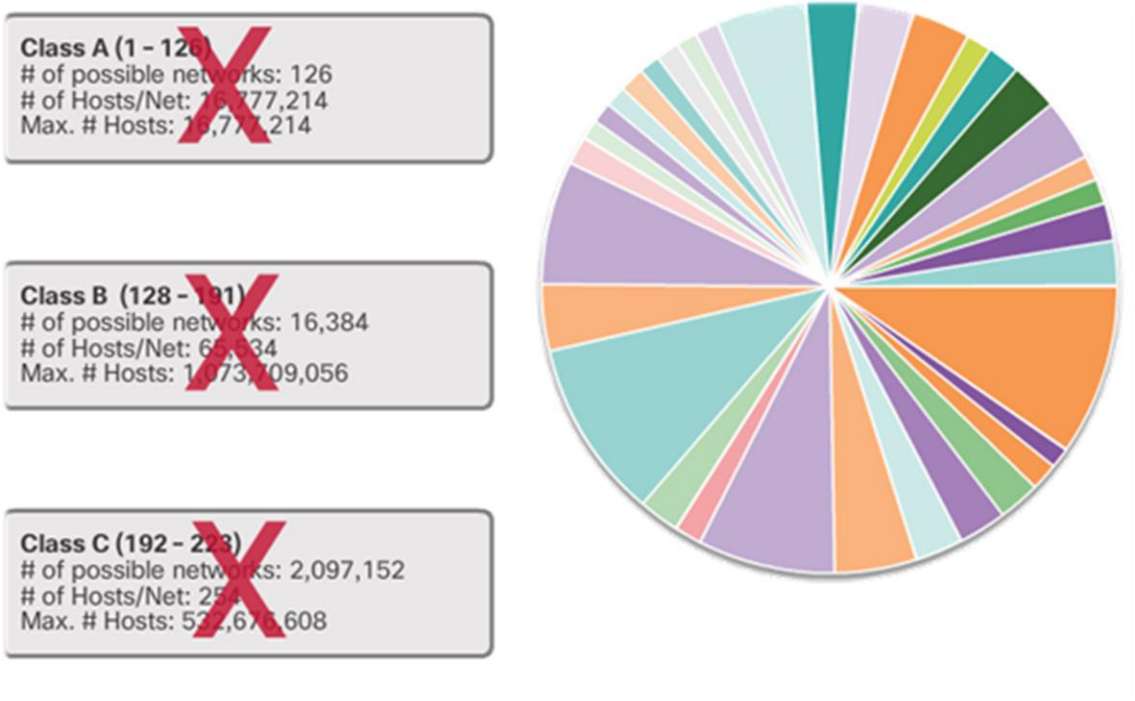
Network masks

IP address: 50.211.197.5
Subnet Mask: 255.0.0.0

	IP network	Host Addresses		
IP address	**50.**	211.	197.	5
Subnet Mask	**255.**	0.	0.	0

- Define the border between the network and the hosts part
- Segment the network

Introduction to CIDR



- CIDR = Classless Inter-Domain Routing
- Ignores the concept Network Address Classes
- Reduces the amount of route advertisements

Without VLSM and CIDR:

10.1.1.0 /24 will be “seen” as 10.0.0.0 /8

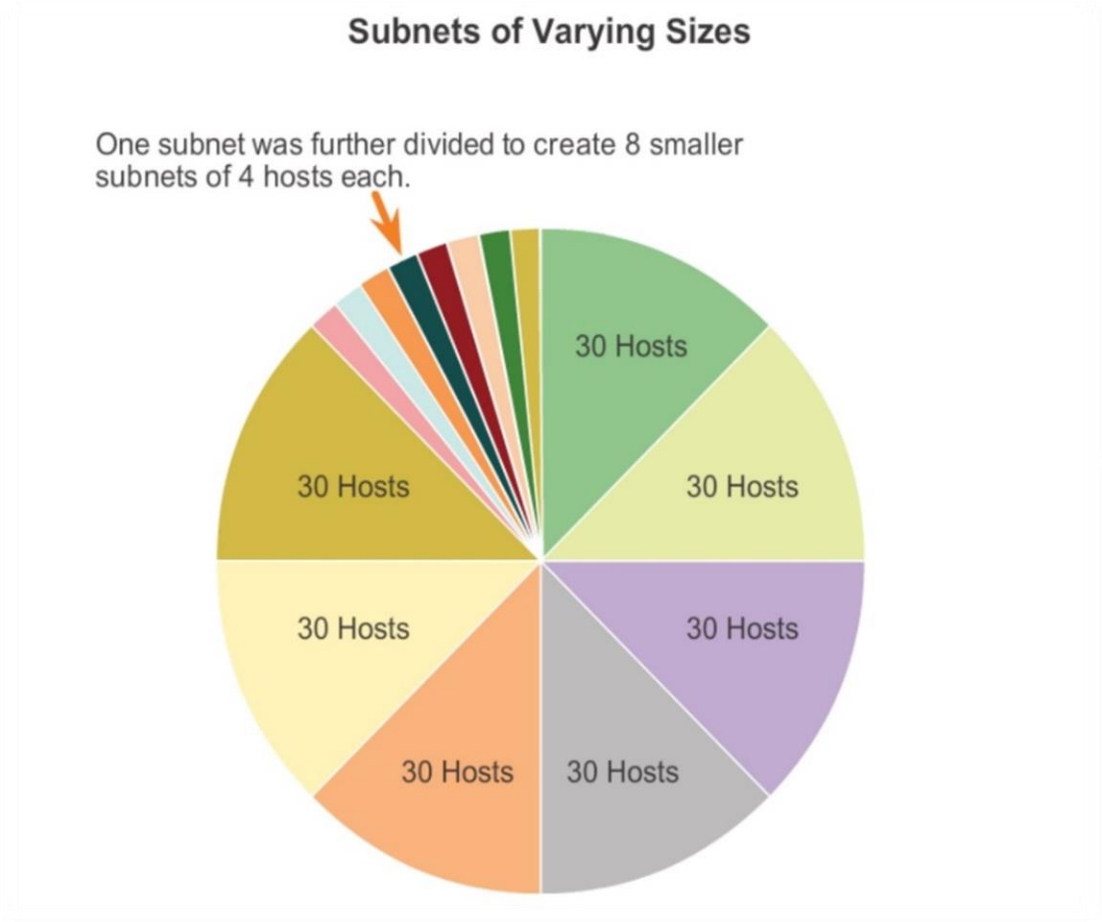
(because /8 is default for Class A)

With VLSM and CIDR:

10.1.1.0 /24 is “seen” as it is

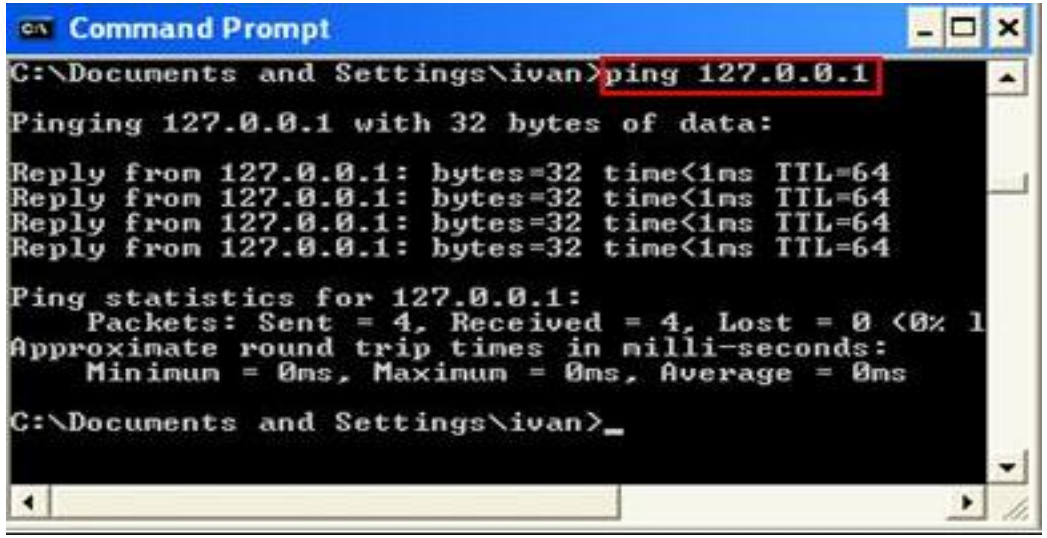
(although the mask is NOT the default)

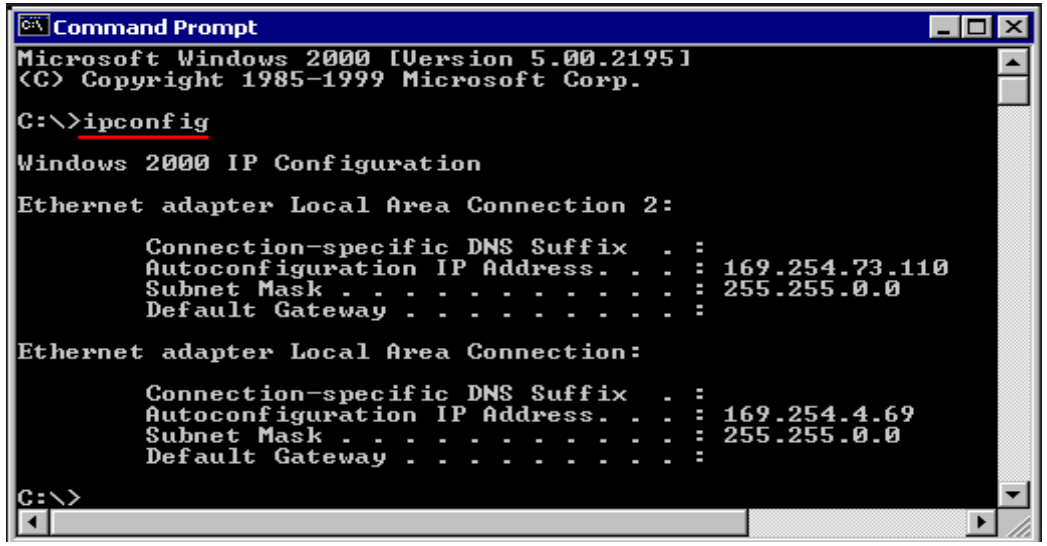
Introduction to VLSM



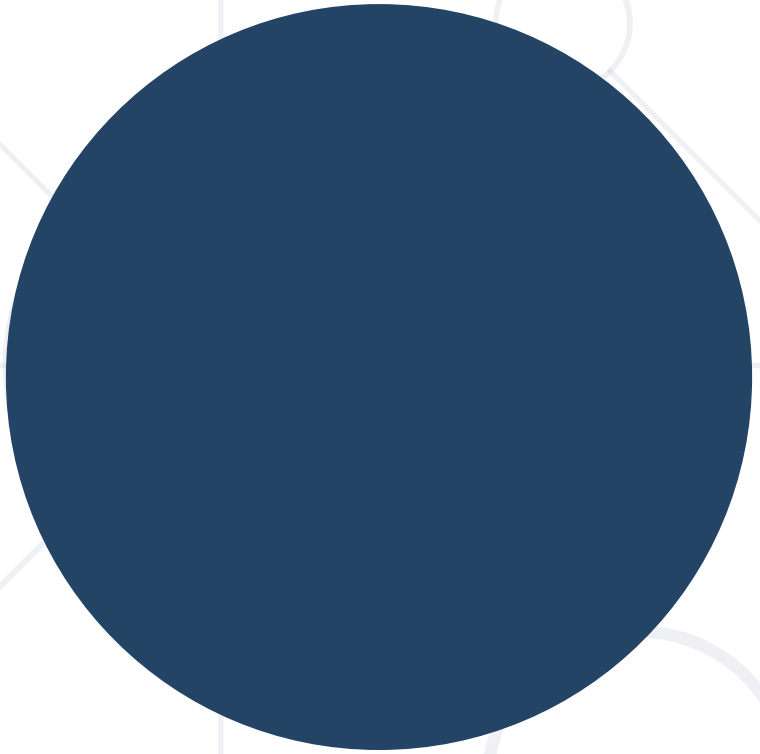
- VLSM: Variable-Length Subnet Masking
- Breaks the IP address classes idea
- “Subnetting of subnets”

Reserved/Special IP addresses





- There are some special IP addresses. For example:
  - 127.0.0.1 /8
    - Known as loopback address
    - On most computer systems, "localhost" resolves to the IP address 127.0.0.1
  - 169.254.X.X /16
    - When DHCP is not reachable
    - Known as APIPA (Microsoft)

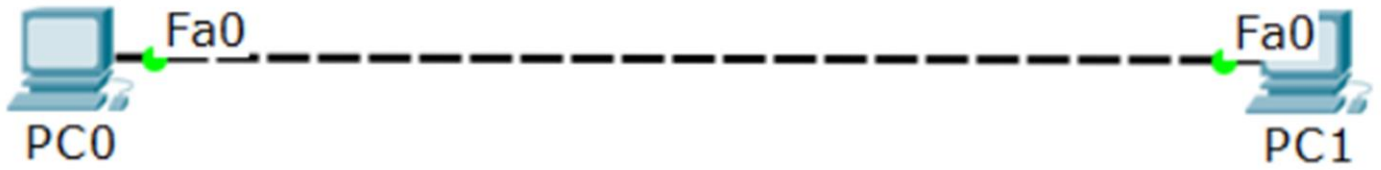


Host-to-host communication without routers

Four addresses required

- There are 4 addresses needed for Ethernet communication:

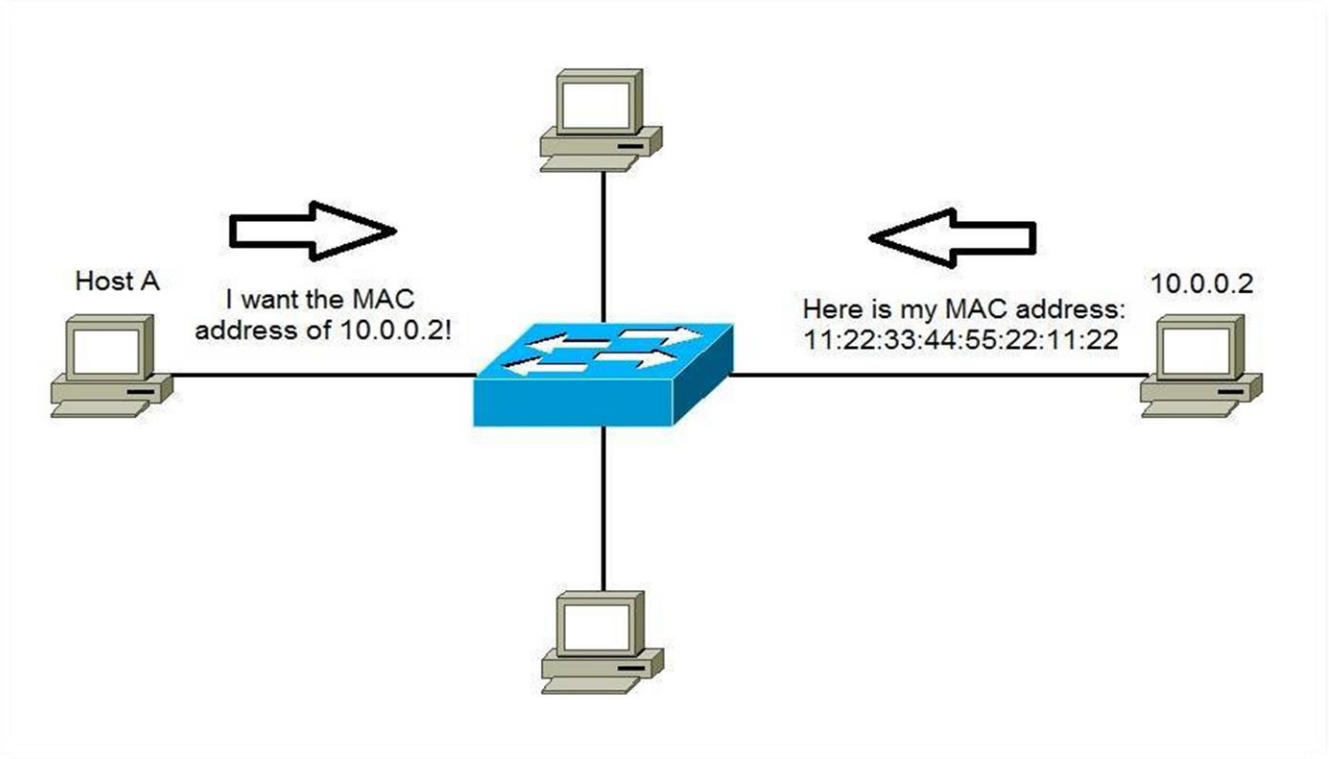
▪ Source IP	▪ Destination IP
▪ Source MAC	▪ Destination MAC



MAC Address: 00E0.F792.0D43
IP Address: 10.0.0.1/24

MAC Address: 000C.CF77.1713
IP Address: 10.0.0.2/24

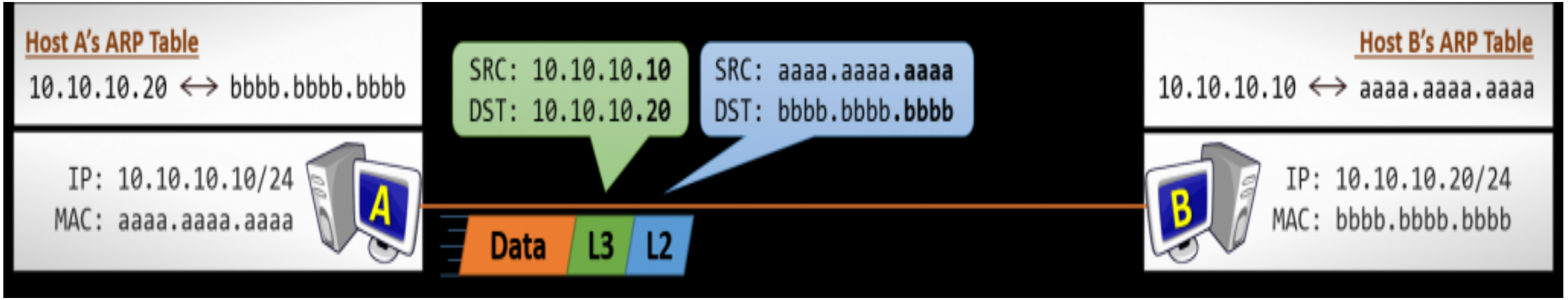
ARP: Address Resolution Protocol



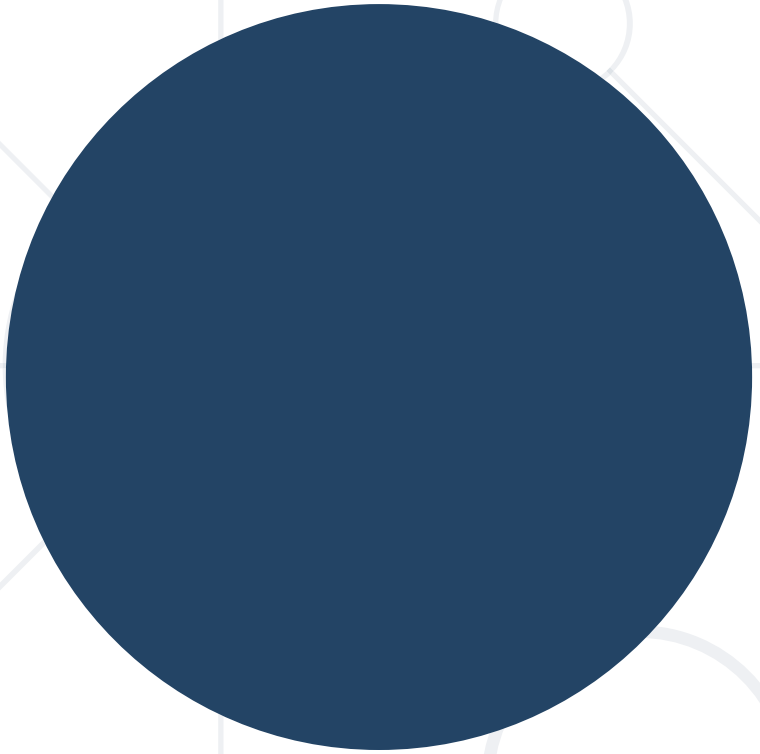
- Used to find the MAC address of the destination
- Uses Broadcast

Direct communication (without router)

- Source and destination MAC addresses are constant
- Source and destination IP addresses are constant



Software University

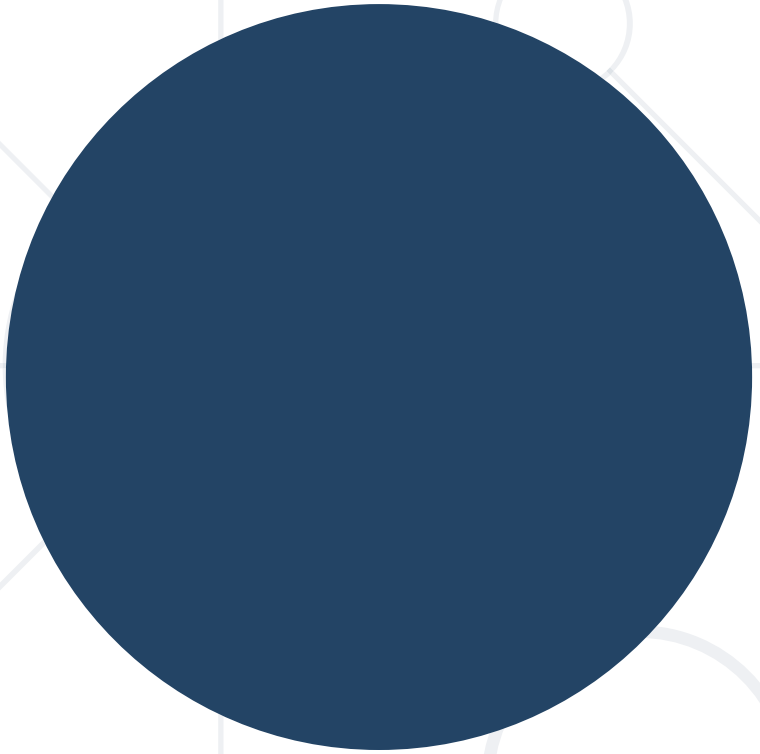


Basic connectivity checks

Basic Connectivity Checks

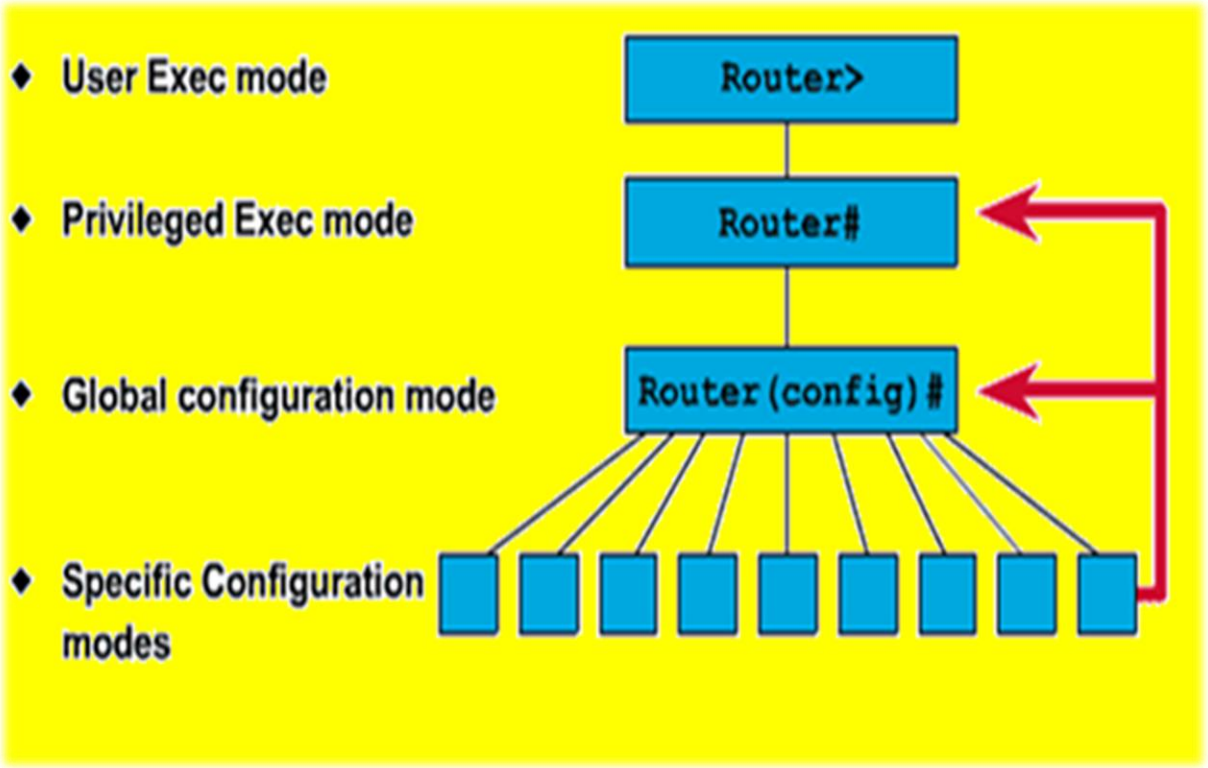
- Ping (Layer 3)
- Traceroute (Layer 3)
- LLDP (Layer 2)
- CDP (Layer 2)

Software University

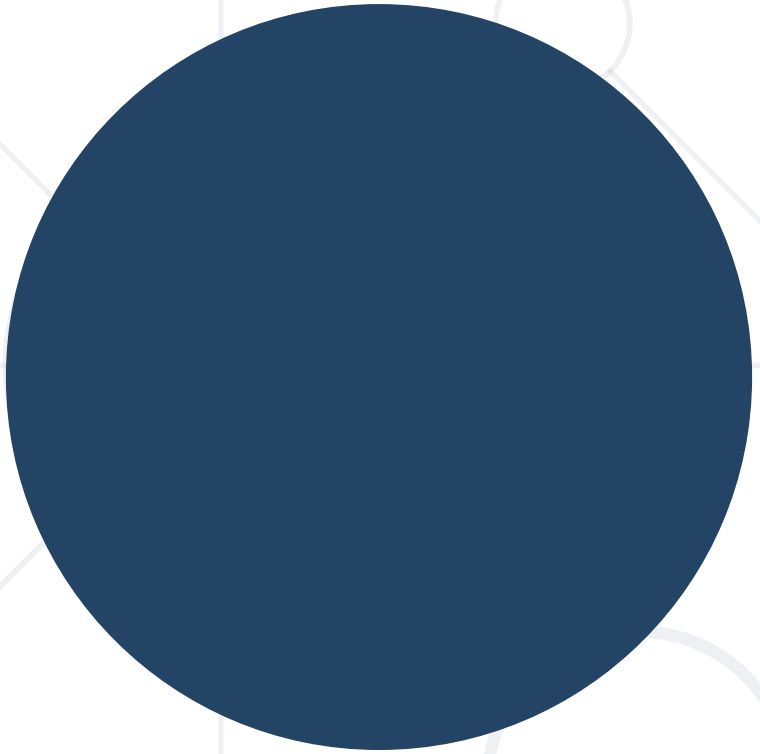


The command line

Command line introduction



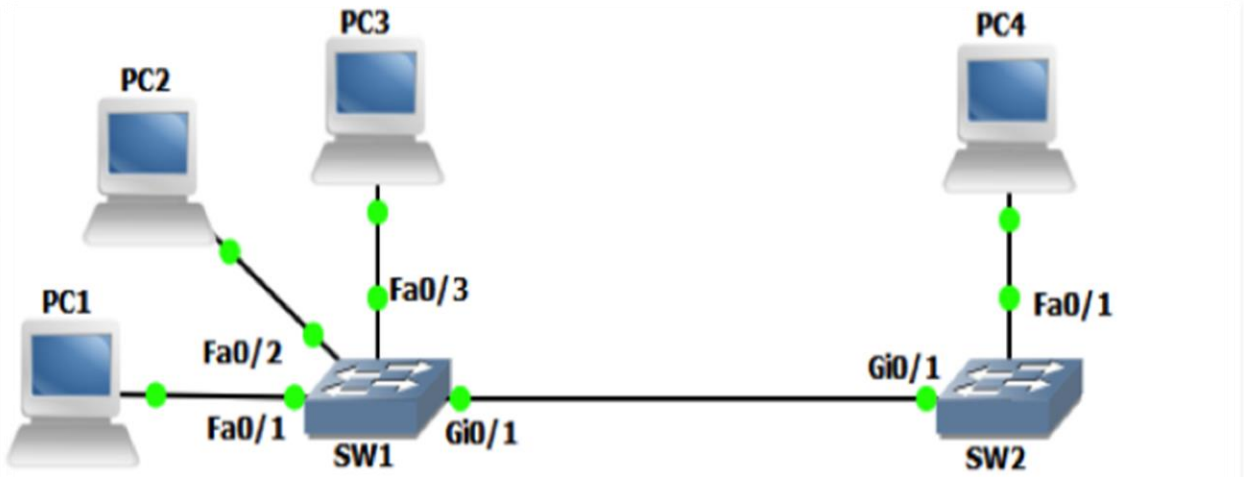
- Different vendors use different names but the logic is similar
- Typical CLI modes:
  - Read-only (User)
  - Read-write (Privilege)
  - Configuration (Global config)
  - Sub-configuration



Switch MAC address table

Back to ToC

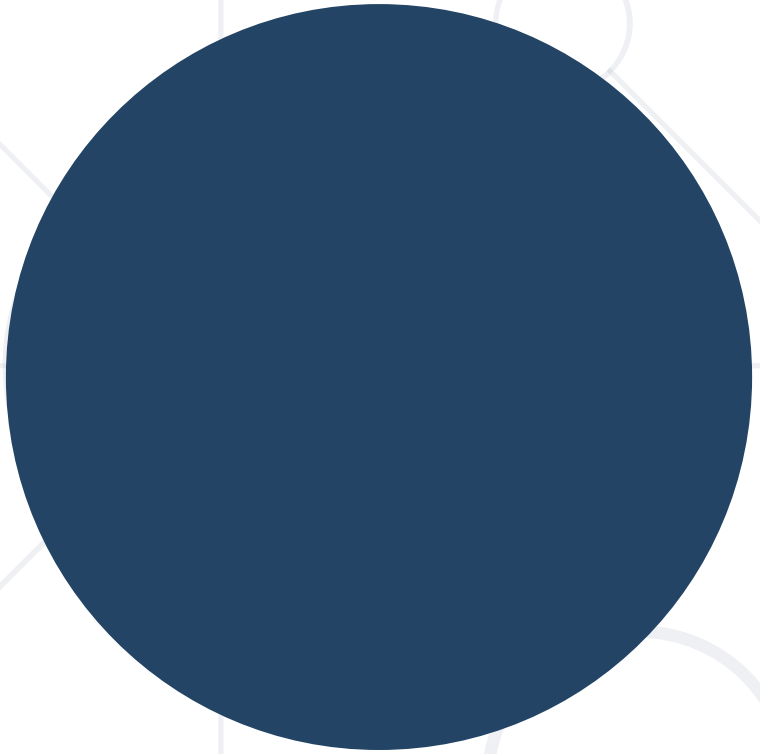
The MAC address table




```
SW1# show mac address-table dynamic
        Mac Address Table
------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  20    0200.1111.1111    DYNAMIC     Fa0/1
  20    0200.2222.2222    DYNAMIC     Fa0/2
  20    0200.3333.3333    DYNAMIC     Fa0/3
```

```
SW2# show mac address-table dynamic
        Mac Address Table
------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

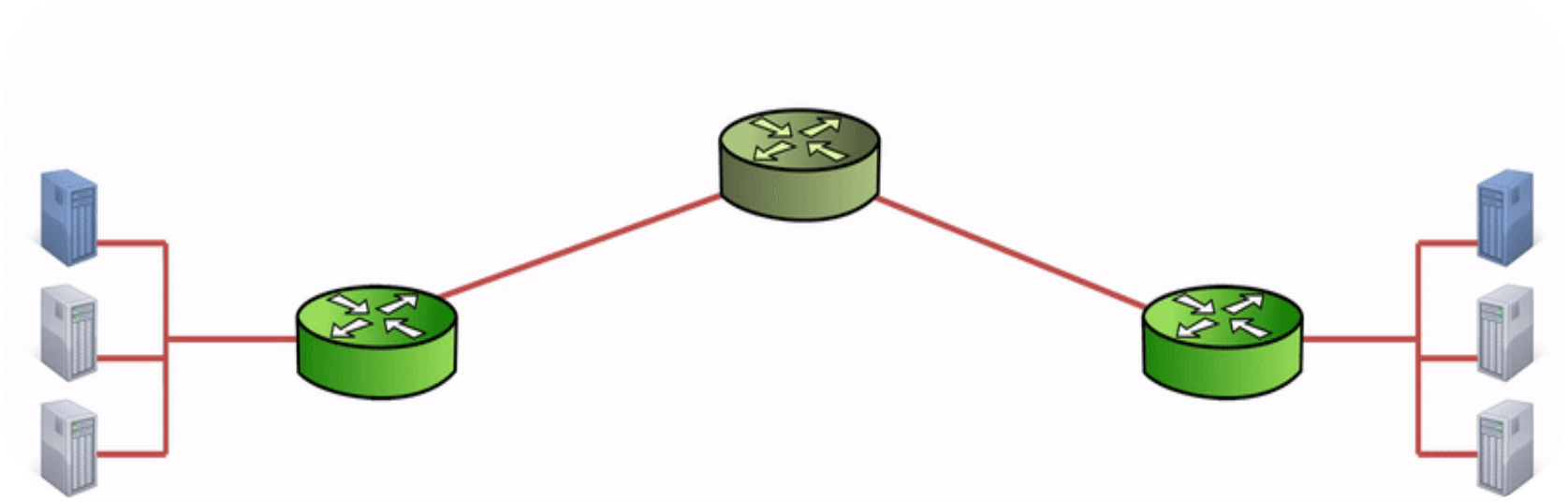
- It is a (dynamic) table that maps MAC addresses to ports
- Used to find the proper interface when the switch forwards a packet

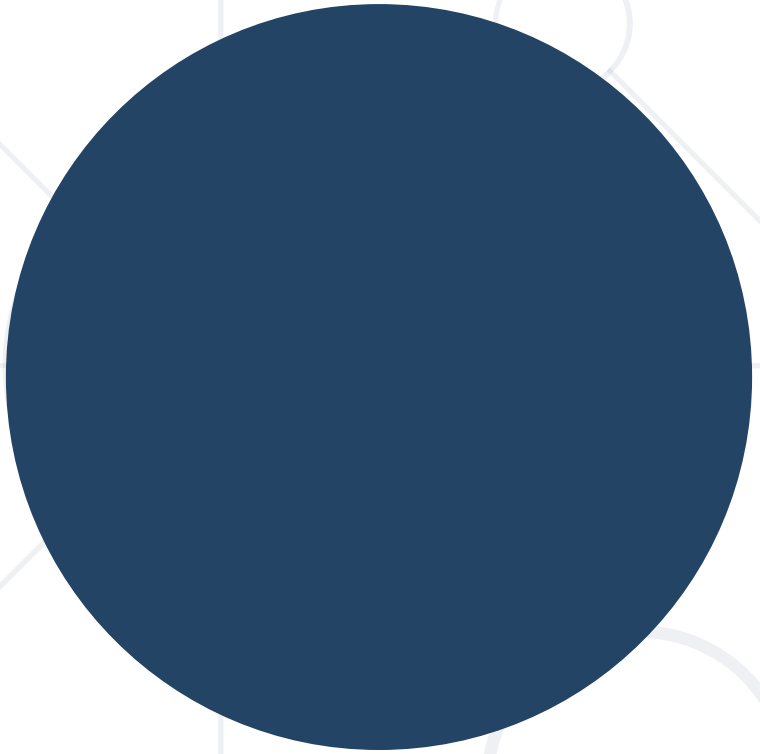


Host-to-host communication with routers

Host-to-host communication with routers

- Source and destination MAC addresses are changed at every hop (router)
- Source and destination IP addresses are constant
  (if we do not use NAT)





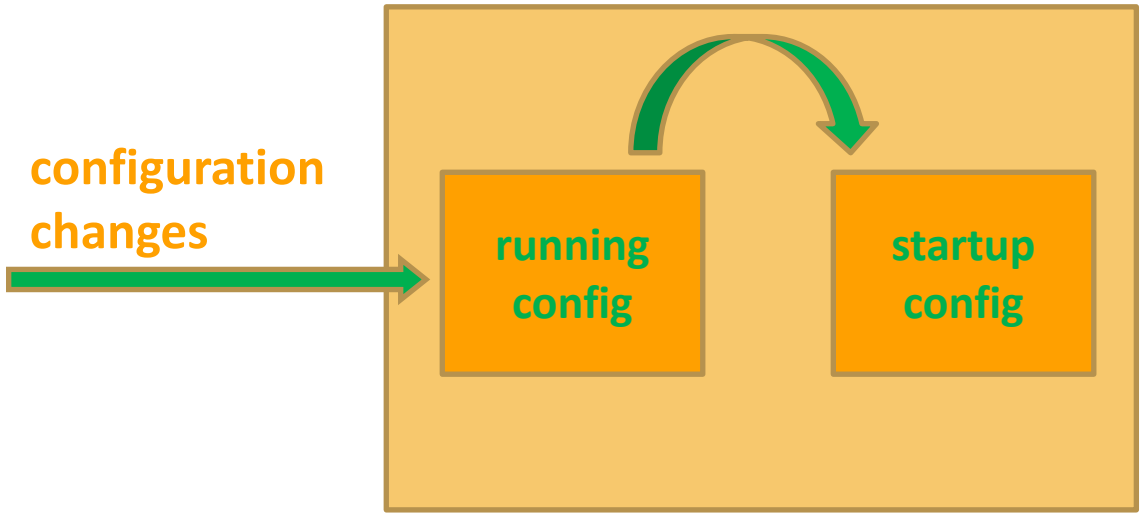
Device memory components

Main memory components in a network device

Software University

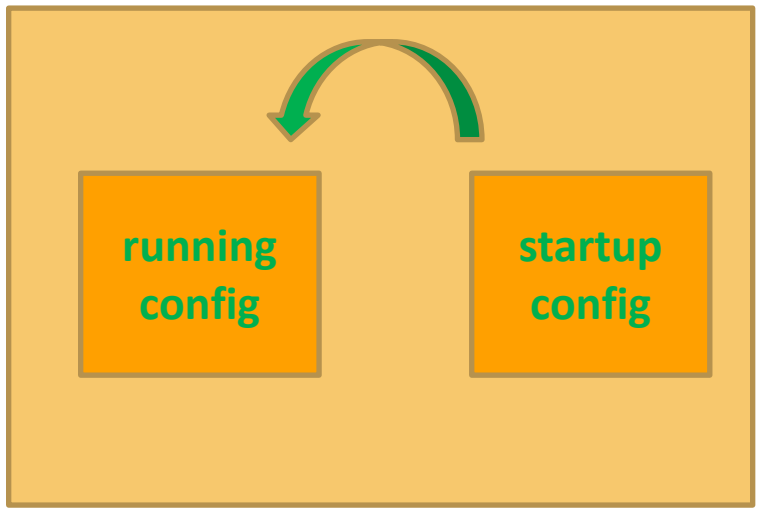
- RAM (Random Access Memory)
  - stores the running configuration file
  - loses content when the power goes down
- NVRAM (NonVolatile RAM)
  - stores the startup configuration file
  - retains content when the power goes down
- Flash memory
  - stores the device image (operating system)
  - retains content when the power goes down
- ROM (Read-Only Memory)
  - maintains instructions for power-on self test (POST) diagnostics
  - Stores bootstrap program and basic operating system software
  - retains content when the power goes down

Saving the configuration

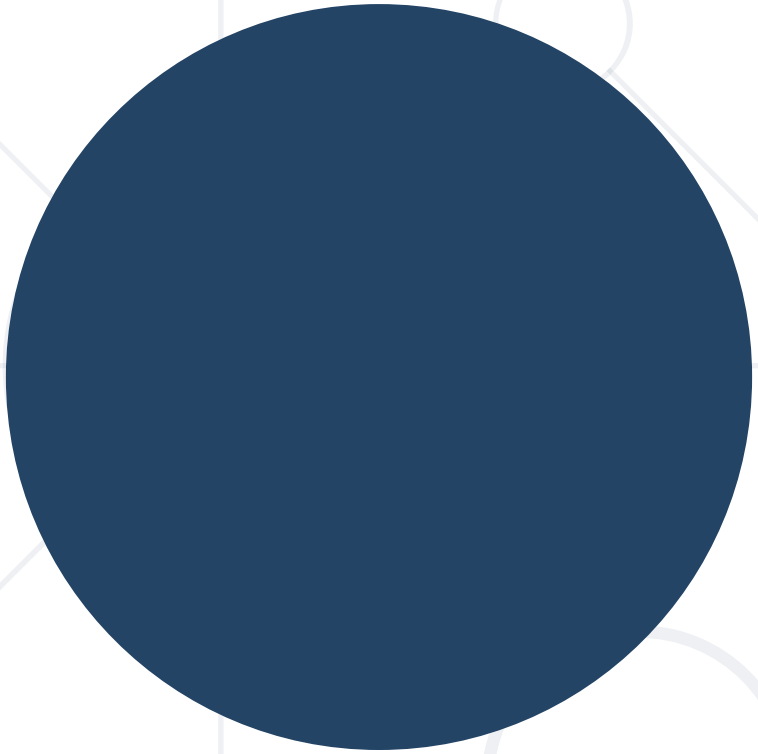


- The configuration file must be saved to survive reboot
- To save the running configuration file (stored in RAM) to the startup configuration file (stored in NVRAM), use either:
  - copy run start
  - write memory

Loading the configuration



- The saved configuration file (startup config file) will go in the RAM (the running config file) when:
  - the device is restarted
  - a copy start run command is executed



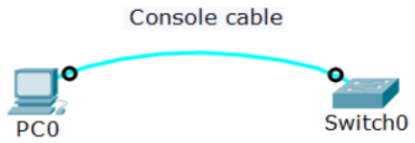
Accessing network devices

Back to ToC

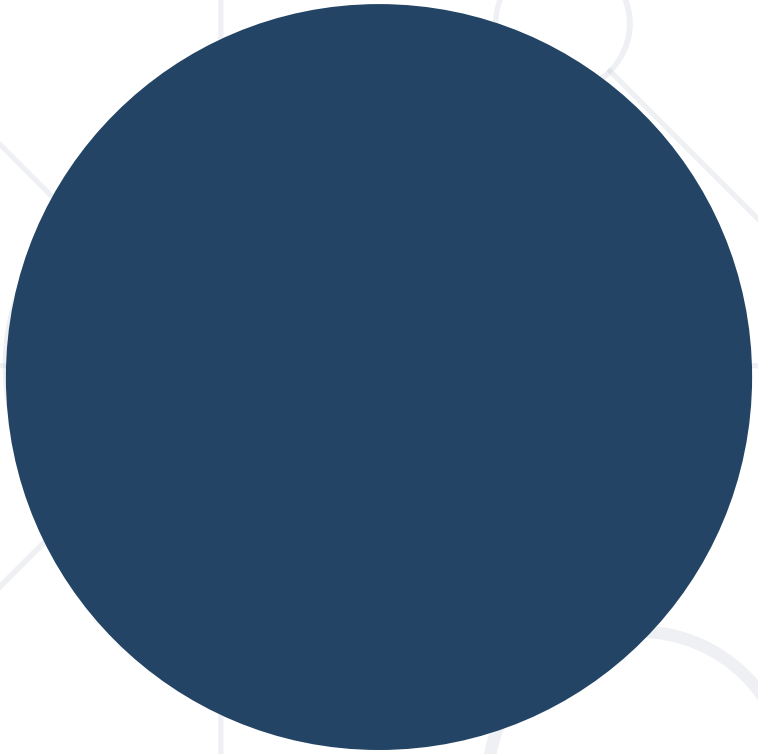
Out-of-band vs in-band management

- Out-of-band:
  - Management traffic uses separate path from the user traffic
  - Typical protocol: Console
- In-band management
  - Management traffic travels the same path as user traffic
  - Typical protocols: Telnet, SSH, SNMP, Web

Out-of-band management



- Dedicated channel for management only
- Needs terminal emulator software (Putty, SecureCRT, etc.)
- No IP addresses are required
- More secure & reliable for management
- Traffic is local and not routed



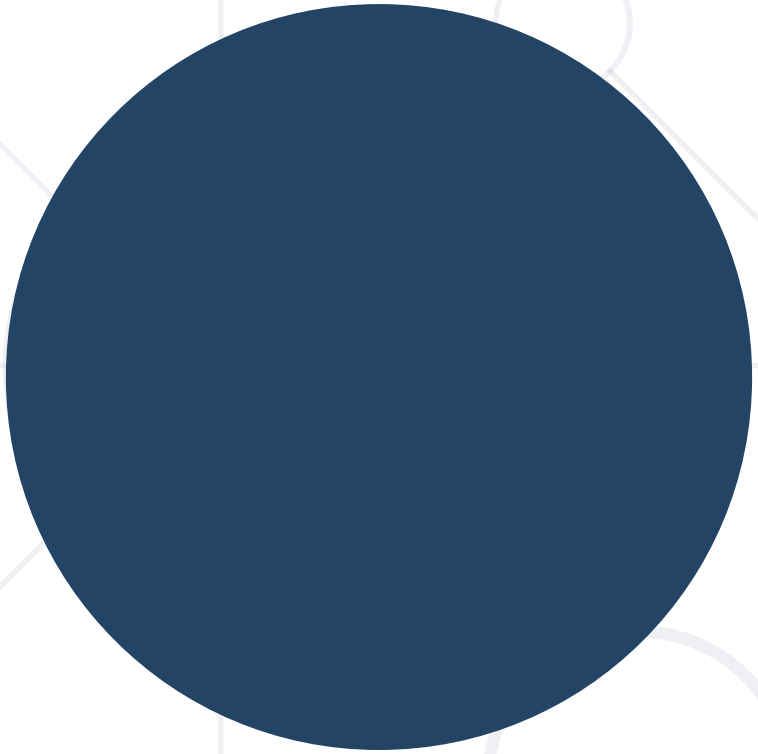
Securing network device access

(Lecture 4)

Secure access - best practices

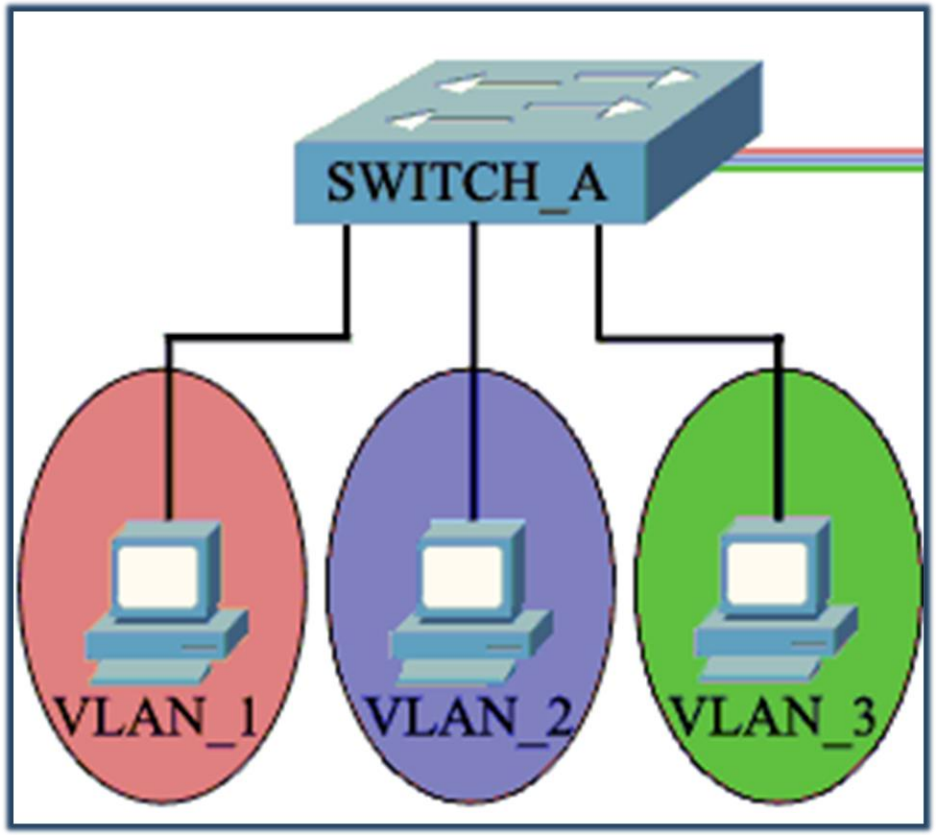
Software University

- Physically secure the devices
- Use SSH instead of Telnet
- Use SNMPv3 instead of v1 or v2
- Use HTTPS instead of HTTP
- Out-of-band management (console) is considered more secure than in-band management
- Create strong passwords for each privilege level and method of access (console, VTY)



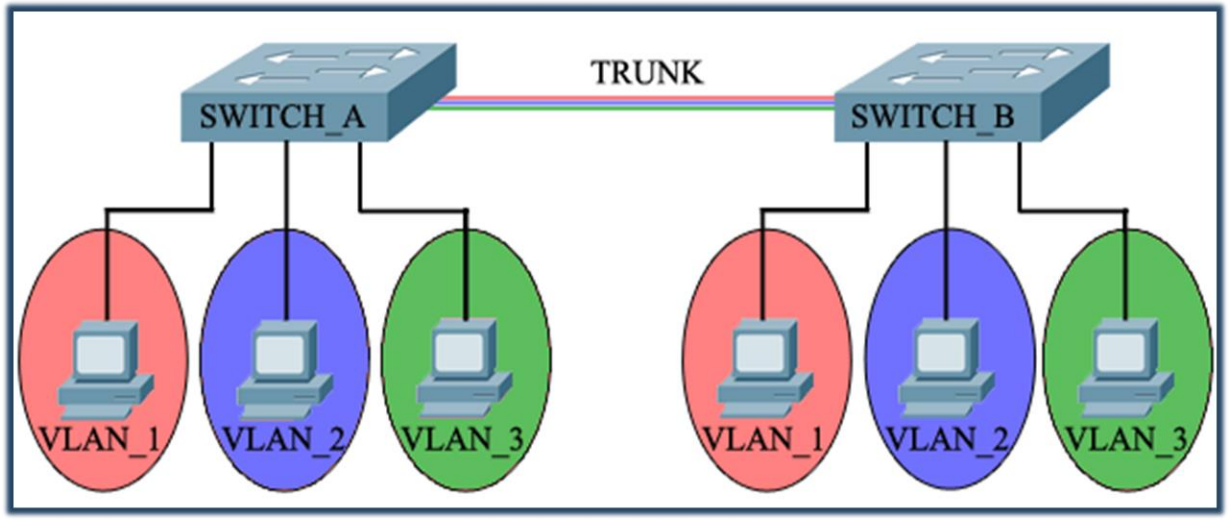
Introduction to VLANs

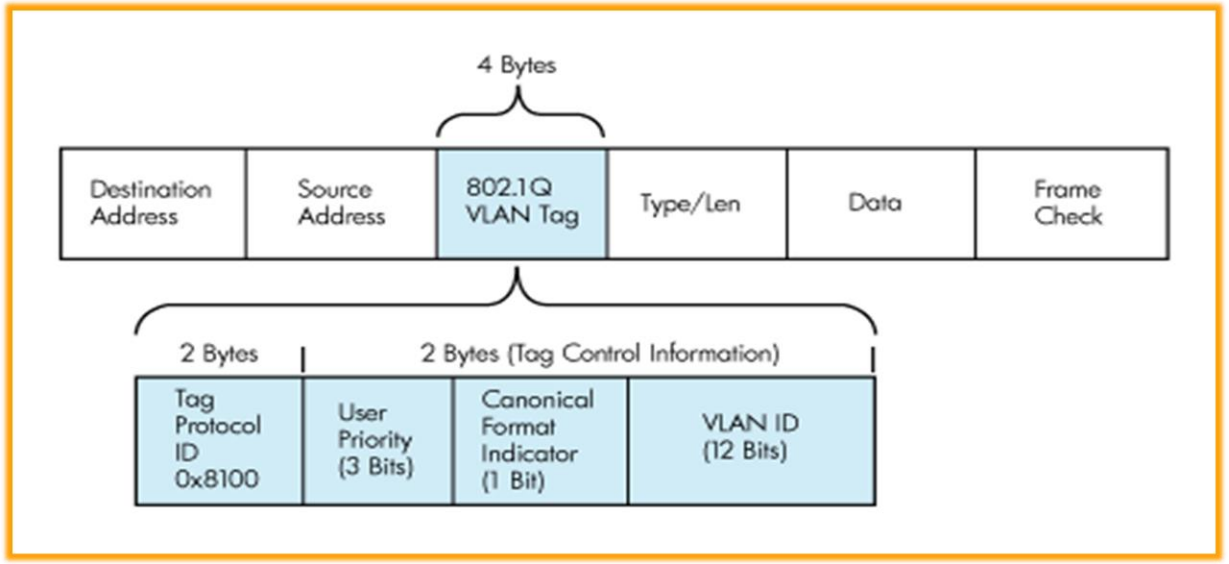
Access (untagged) ports



- Used to connect to end-user devices
- Can be associated with only one VLAN
- Uses the “normal” ethernet frame where there is no VLAN information - no VLAN tag

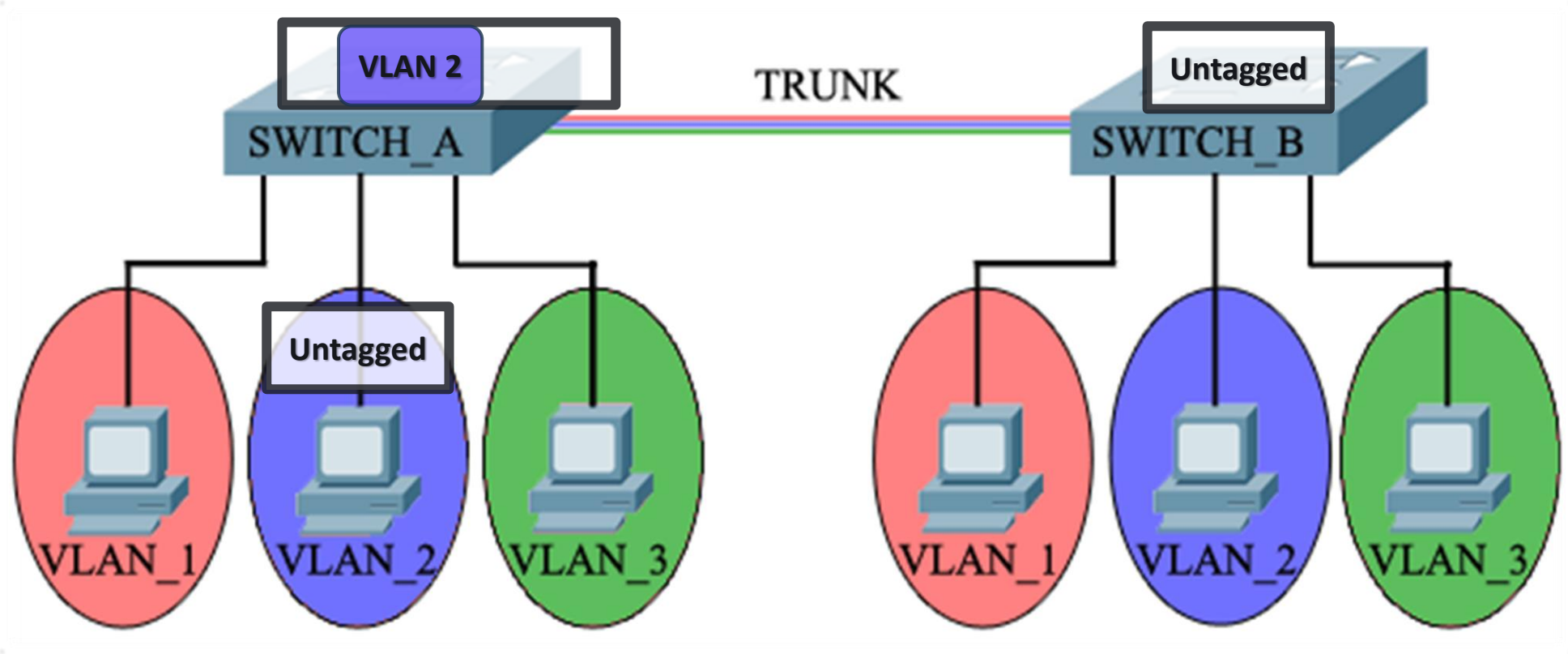
Trunk (tagged) ports

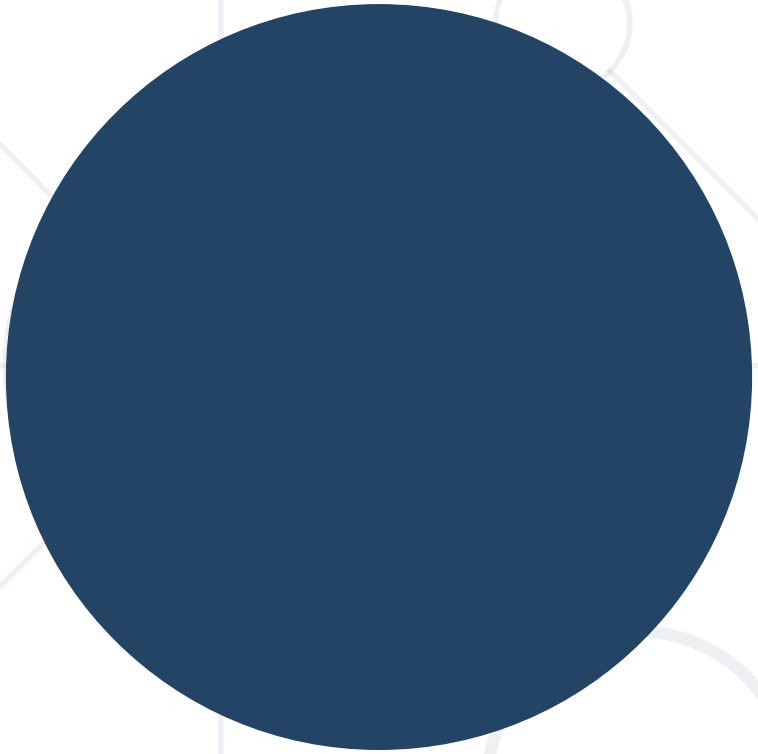




- Used to connect between switches
- Can carry information from/to multiple VLANs
- Uses the 802.1Q tagged frame

Tagging between switches

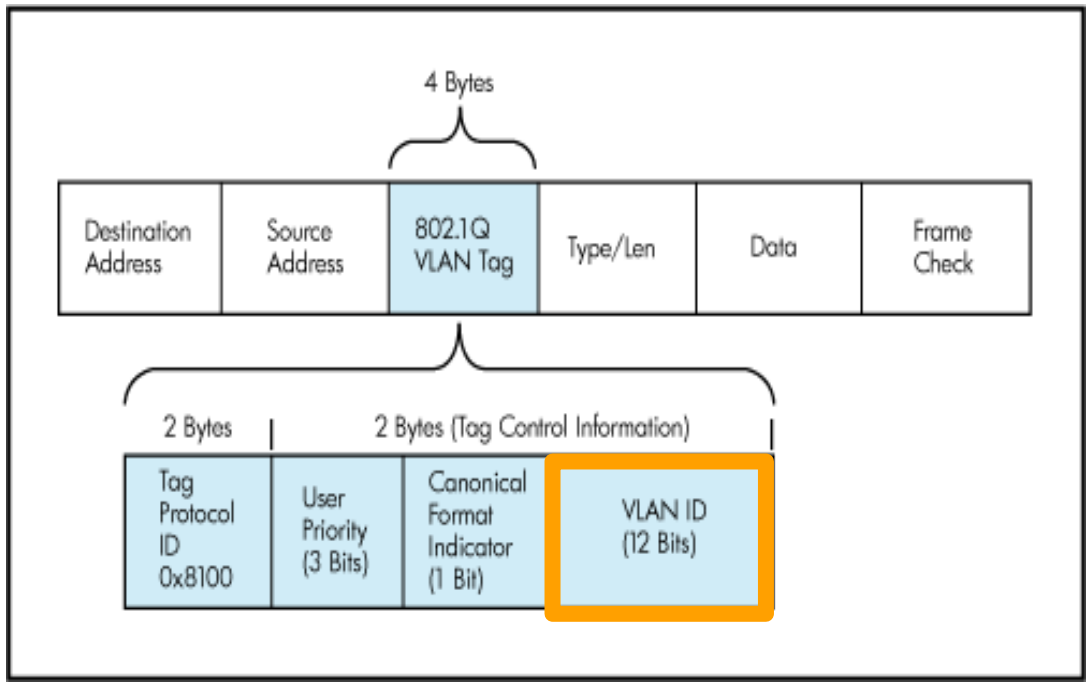




VLAN details

(Lecture 4)

Trunk port details



- Uses IEEE 802.1Q tag to identify each frame
- A trunk carries multiple tagged VLANs and (maximum) one untagged VLAN
- The untagged VLAN on a trunk is called:
  - Native VLAN (Cisco)
  - PVID (HPE Comware)
  - Untagged VLAN (HPE Provision)

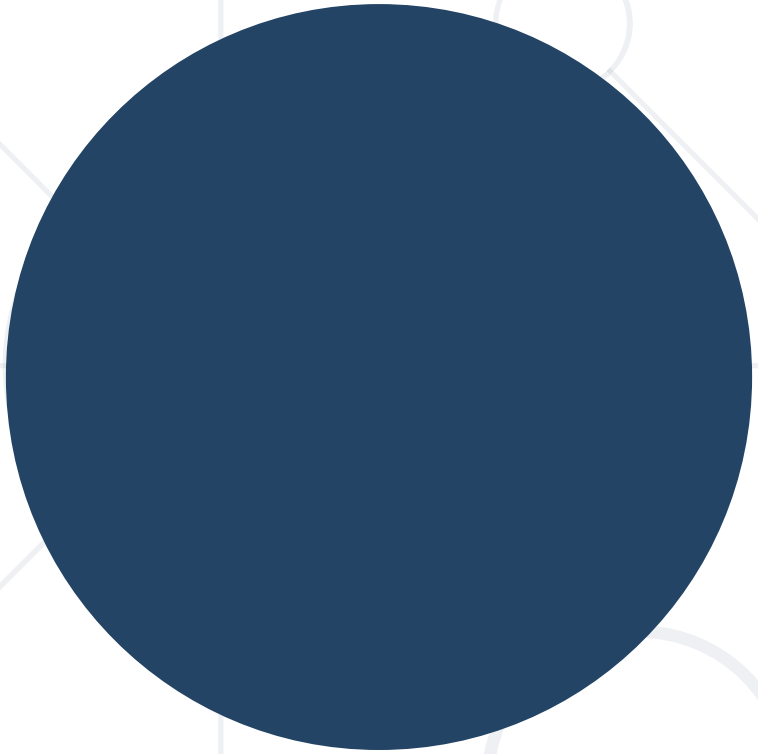
Trunk port details (2)

- When a port is configured as a trunk port, different vendors may have different default behavior:
  - All VLANs are automatically allowed on the trunk - Cisco
  - None of the VLANs (except VLAN 1) are auto-allowed on the trunk - HPE Comware

- The configuration can be changed to overwrite the default behavior depending on your needs

Inter-VLAN routing

- Traffic is transferred from one VLAN to another via routing
- Layer 3 device with IP address in each VLAN is required
- Do I have Layer 3 support on my switch?
  - Cisco – L3 default state depends on the device
  - HPE Comware - L3 is always on
  - HPE Provision - need to manually turn on the ip routing



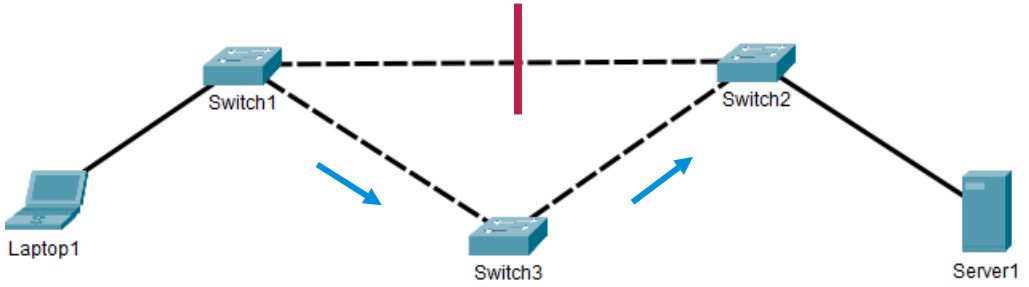
Spanning Tree Protocol (STP)

Back to ToC

Layer 2 networks and redundancy

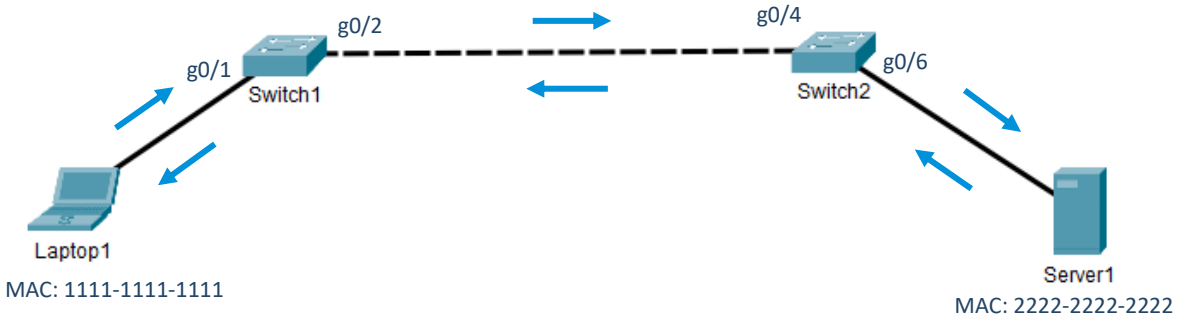
- No redundancy for the link between Switch1 and Switch2
  - If the link fails, the communication stops

- With redundancy - two paths between Switch1 and Switch2
  - If one path fails, the communication can continue over the other



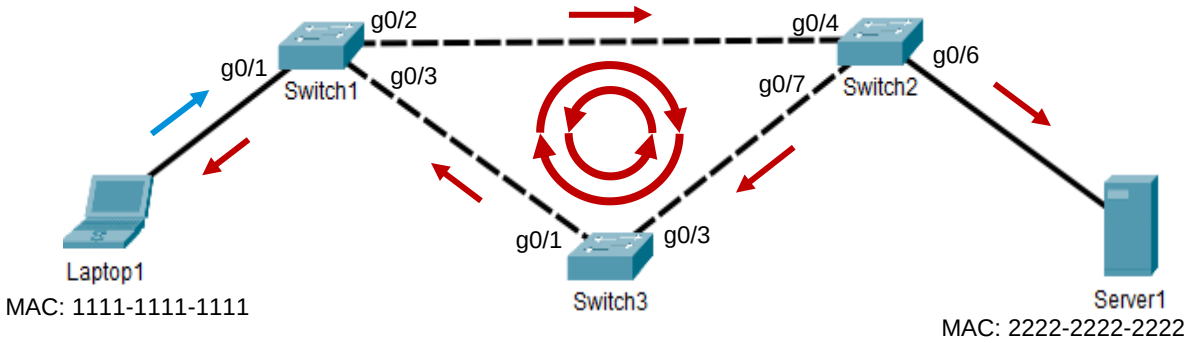
The problem with layer 2 network redundancy

- Normally, the switches will build and use MAC address tables to help them with the forwarding decisions
- When redundant paths are present, the switches are confused and will forward the received packet everywhere
  - Their MAC address tables become unstable
  - Multiple copies of the same frame (data) are received by all devices, endlessly
  - The links are overloaded
  - This is known as **Layer 2 loop and is very bad situation!**



Switch2 MAC Table

MAC address	Port
1111-1111-1111	g0/4
2222-2222-2222	g0/6

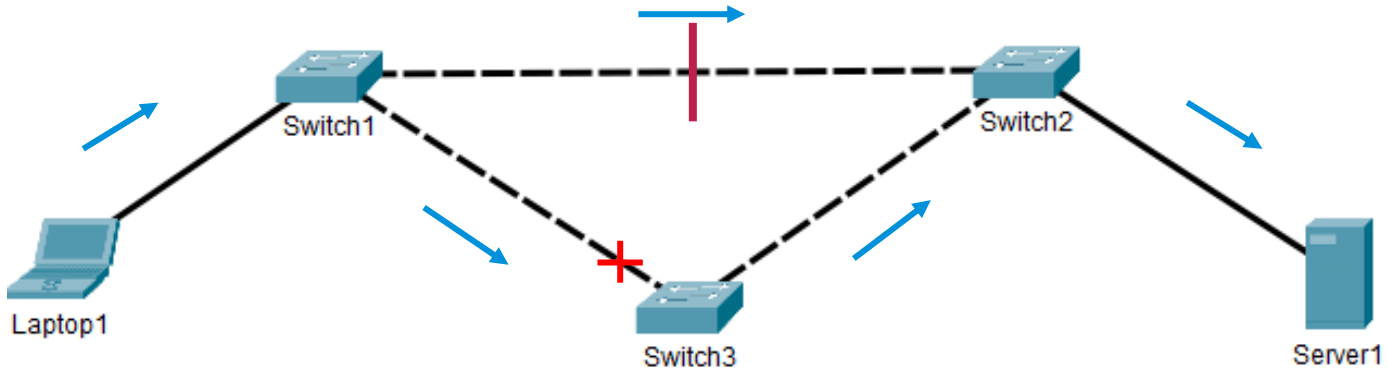


Switch2 MAC Table

MAC address	Port
1111-1111-1111	~~g0/4~~, ~~g0/7~~, ~~g0/4~~…?
2222-2222-2222	~~g0/6~~, ~~g0/7~~, ~~g0/4~~…?

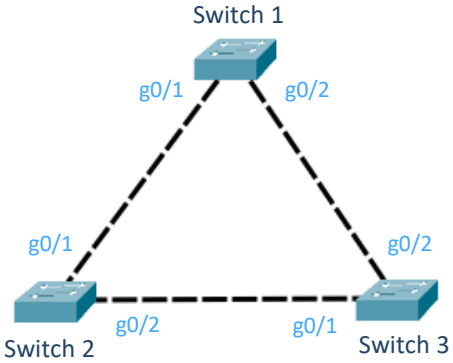
What is Spanning Tree Protocol (STP)?

- STP helps the network switches to deal with a problem which they can not handle alone – the Layer 2 loops
- STP will logically block a port (or multiple ports) in a redundant topology and will leave only one active path at a time
- If the active path is broken, STP will automatically unblock the port(s) to restore the connectivity



The STP algorithm

1. Elect the Root switch (a.k.a. Root bridge or just Root)
   - This is the switch with the lowest BID (Bridge ID)
   - BID = Switch Priority and MAC
   - Default priority = 32768
2. Select the root ports
   - They have the best (lowest) cost to the Root
   - Selected per switch – maximum one
   - Only the non-Root switches have root ports
3. Select the designated ports
   - They have the best (lowest) cost to the Root
   - Selected per segment (connection) – exactly one
4. All other ports go to blocking state
   - The role of these ports is called “alternate”



The STP tie-breakers

- If there is a tie situation - the same path cost via different paths, use the following tie-breakers:
  - When selecting Root port or Designated port, chose the neighboring switch which has the lowest Bridge ID
  - If the Bridge ID is the same, select the lowest Port ID (PID)
- Port ID = Port priority and port number

BPDUs, Bridge ID and Priority

- Switches communicate with each other by exchanging BPDUs (Bridge Protocol Data Units) - this is how they "talk the STP language"
- One piece of information that the BPDU contains is the Bridge ID (BID) = 8 byte value
- BID = Priority (2 bytes) and "system ID" / MAC address (6 bytes)
- STP Priority:
  - A number between 0 and 61440
  - Must be configured in increments of 4096
  - Default is 32768 (+ the VLAN ID)
  - The switch with the lowest priority will become the Root
- If equal values for priority -> lowest MAC address wins (BID = Priority and MAC)

The priority field

- Initially, the priority field allowed for 65536 different values (2^{16})

Priority (16 bits)															
(32768)	(16384)	(8192)	(4096)	(2048)	(1024)	(512)	(256)	(128)	(64)	(32)	(16)	(8)	(4)	(2)	(1)

- Later it was realized that some changes are required
- Nowadays, the priority field looks like this:

Priority (4 bits)				Extended system ID (12 bits)												
(32768)	(16384)	(8192)	(4096)	(2048)	(1024)	(512)	(256)	(128)	(64)	(32)	(16)	(8)	(4)	(2)	(1)	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	= 0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	= 4096
0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	= 8192 (2x4096)
.....																
																Default
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	= 32768 (8x4096)
.....																
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	= 61440 (15x4096)

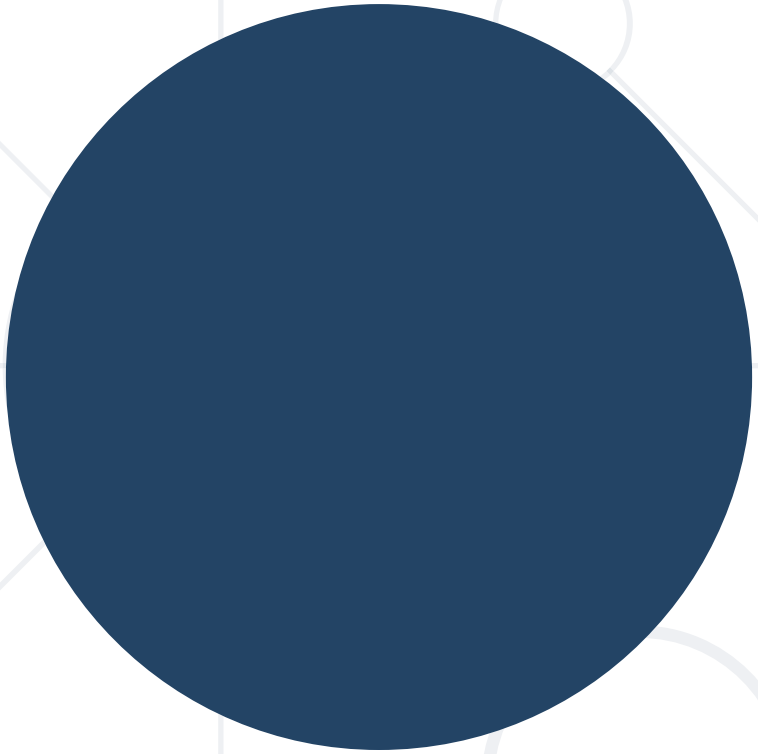
Link costs (path costs)

- This is the cost to get to the Root
- Calculated from the cost of a port and the number of links
- Higher port speed -> lower port cost
- The default values can be changed by administrator

Ethernet Speed	IEEE Cost: 1998	IEEE Cost: 2004
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2,000
100 Gbps	N/A	200
1 Tbps	N/A	20

Spanning Tree Protocol – Main Flavors

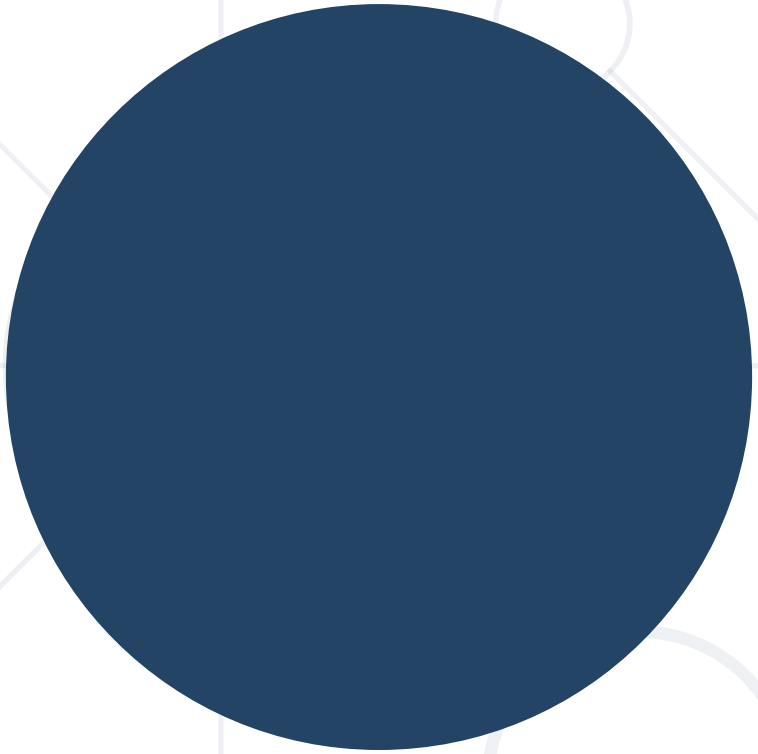
- STP - Spanning Tree Protocol, IEEE 802.1D
- RSTP - Rapid STP, IEEE 802.1W
- MSTP - Multiple STP, IEEE 802.1S (802.1Q-2005)
- PVST+ - Per-VLAN STP, Cisco proprietary



Rapid STP (RSTP)

RSTP (the faster STP)

- Rapid STP
- The industry standard name is IEEE 802.1W
- Much faster convergence than STP
- Introducing Edge port – a port which is connected to an end device
- RSTP uses the same algorithm as STP
- Port states:
  - Discarding
  - Learning
  - Forwarding

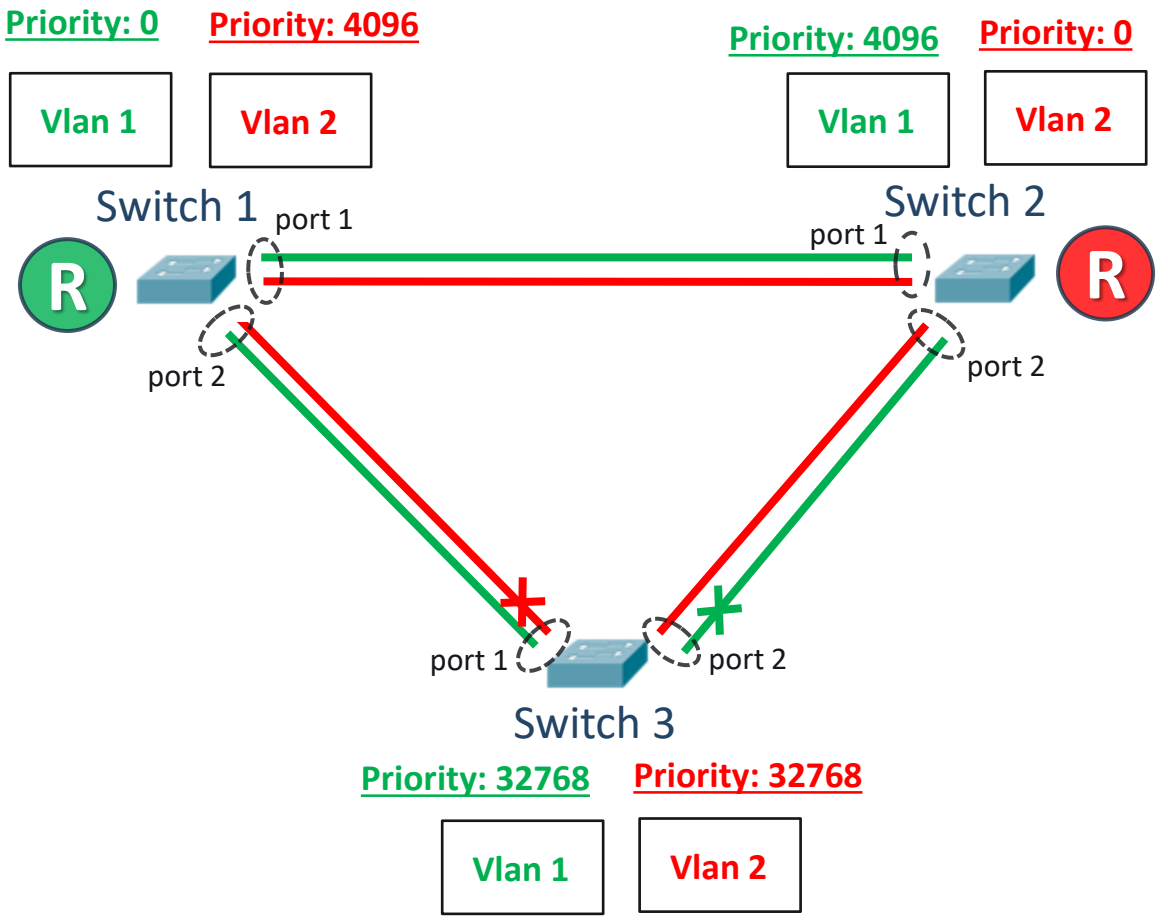


Per-VLAN STP plus (PVST+)

PVST+

- Per-VLAN Spanning Tree is Cisco protocol
- Why? It has a similar idea as MSTP - to distribute the load
- Creates a spanning tree topology for each VLAN separately
- PortFast in PVST+ is similar to Edge port in STP/RSTP

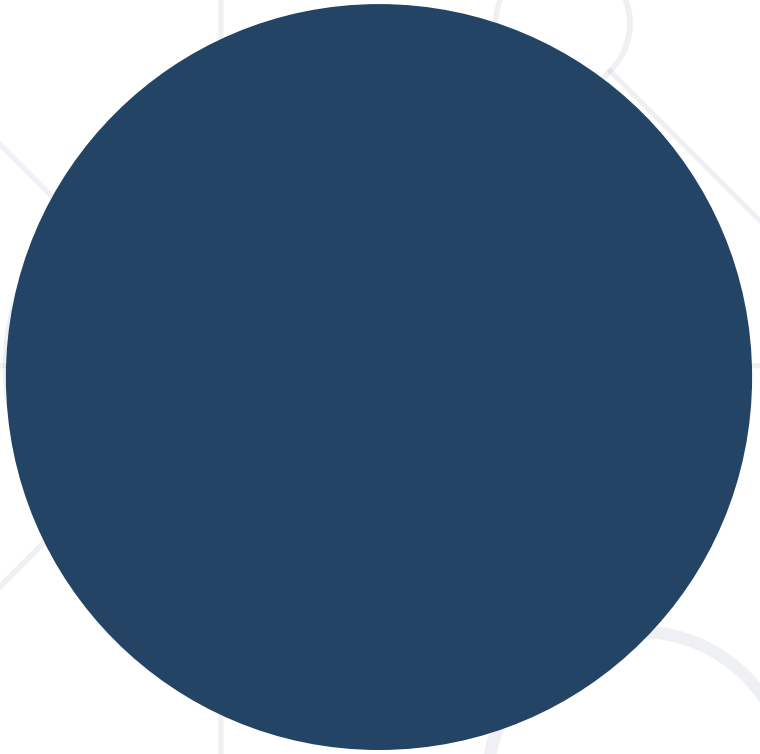
PVST+ (3)


Priority: 0
Priority: 4096
Vlan 1
Vlan 2
Switch 1
port 1
port 2
Priority: 4096
Priority: 0
Vlan 1
Vlan 2
Switch 2
port 1
port 2
R
R
port 1
port 2
Switch 3
Priority: 32768
Priority: 32768
Vlan 1
Vlan 2

The good and the bad about PVST+

Software University

- PVST+ advantages:
  - triggers STP calculation only if there is a potential loop in a particular VLAN
  - detailed "look" of the network – does not block ports when there is no loop on the trunks for a given VLAN
- PVST+ disadvantages
  - generates a lot of overhead in the network
  - proprietary protocol



IP services: DHCP and DNS

Back to ToC

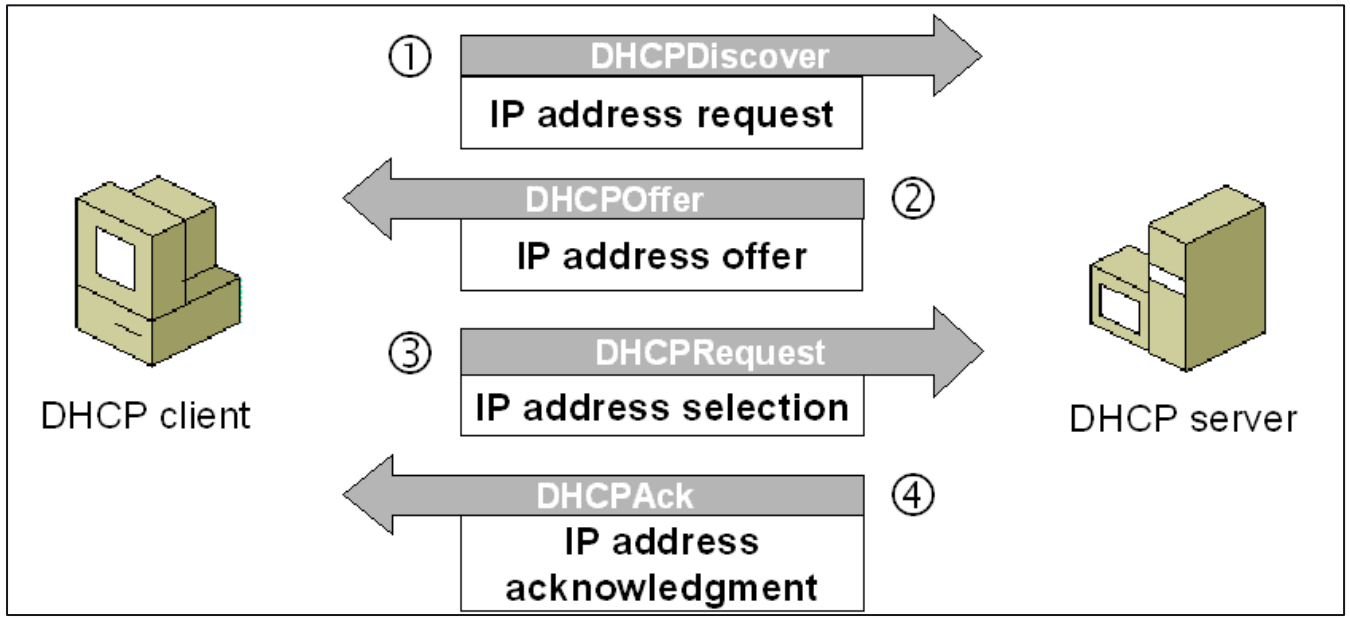
What is DHCP?

- DHCP: Dynamic Host Configuration Protocol
- Provides automatic distribution of IP addresses and other networking parameters such as:
  - Subnet mask
  - Default gateway
  - DNS servers
  - More…
- Industry standard

DHCP Components

- Server
  - DHCP scope - range of addresses (pool), lease time, reservations, etc.
  - Uses port UDP 67
- Client
  - Must be configured to use DHCP
  - Uses port UDP 68
- (Relay agent)
  - Used to serve multiple (V)LANs with a single DHCP server

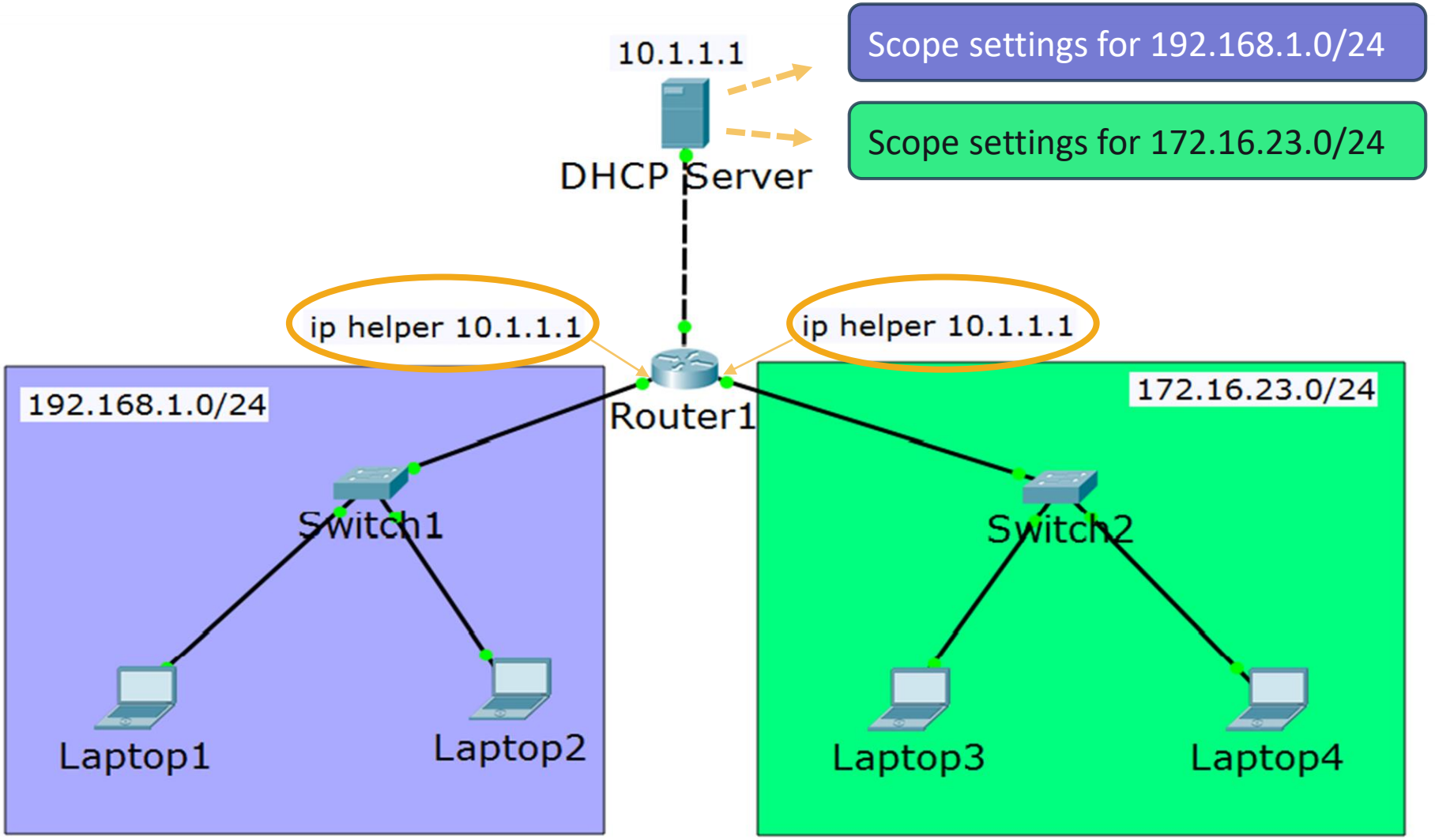
The DHCP Process



- "DORA"
  - Discover
  - Offer
  - Request
  - Acknowledge

All messages use broadcast (IPv4)

DHCP Relay (2)


10.1.1.1
DHCP Server
Scope settings for 192.168.1.0/24
Scope settings for 172.16.23.0/24
ip helper 10.1.1.1
ip helper 10.1.1.1
Router1
192.168.1.0/24
172.16.23.0/24
Switch1
Switch2
Laptop1
Laptop2
Laptop3
Laptop4

DNS Introduction

- DNS: Domain Name System
- DNS Usage:
  - To translate names to IP addresses
  - To translate IP addresses to names
  - To find a particular service in the network

*DNS will be discussed in more details in the advanced course

DNS “A” Records

Software University

- One of the most commonly used records in DNS
- Matches a hostname (or FQDN) to an IP address
- Examples:
  - pc1 -> 192.168.1.1
  - pc2 -> 192.168.1.2
  - server -> 192.168.1.100
  - www.abv.bg -> 194.153.145.104

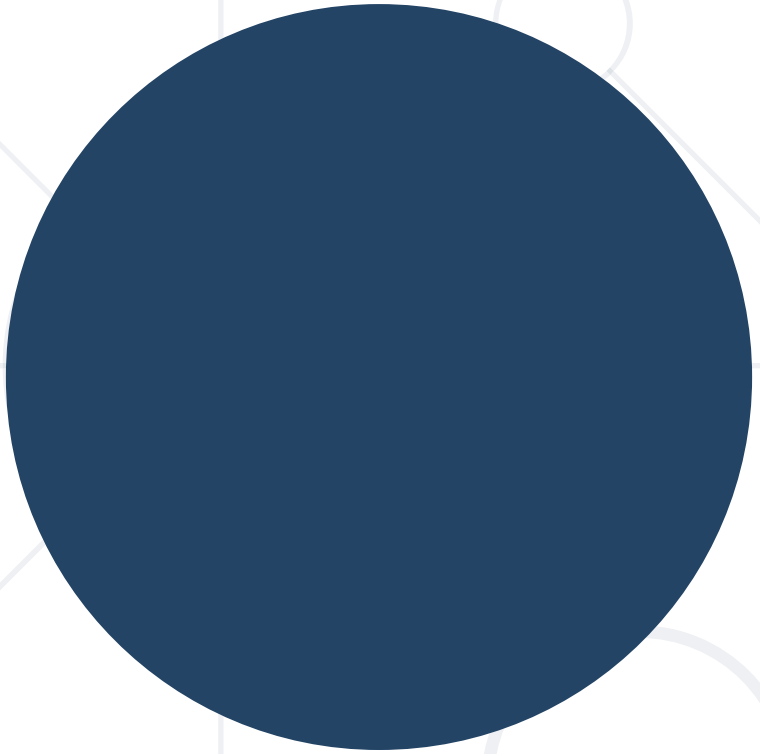
*FQDN = Fully Qualified Domain Name

DNS: Client-to-Server Communication

- The clients need to know the address of their DNS server(s)
- It can be either:
  - Statically configured

  OR

  - Dynamically received from a DHCP server
- DNS uses server port 53 (both UDP and TCP)



Introduction to routing

Switching vs Routing

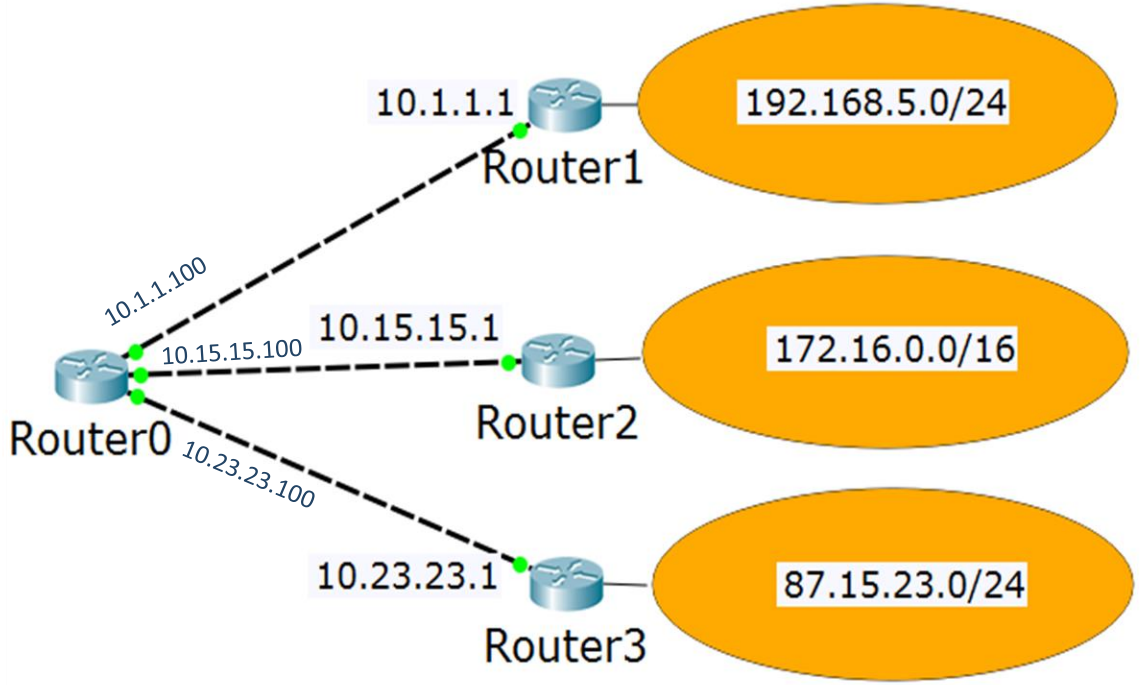
- Switches:
  - Use Layer 2 information (MAC addresses)
  - Forwarding decisions based on the MAC address tables
  - Not scalable for big networks
- Routers:
  - Use Layer 3 information (IP addresses)
  - Forwarding decisions based on the routing tables
  - Scalable for large networks

The Routing Table

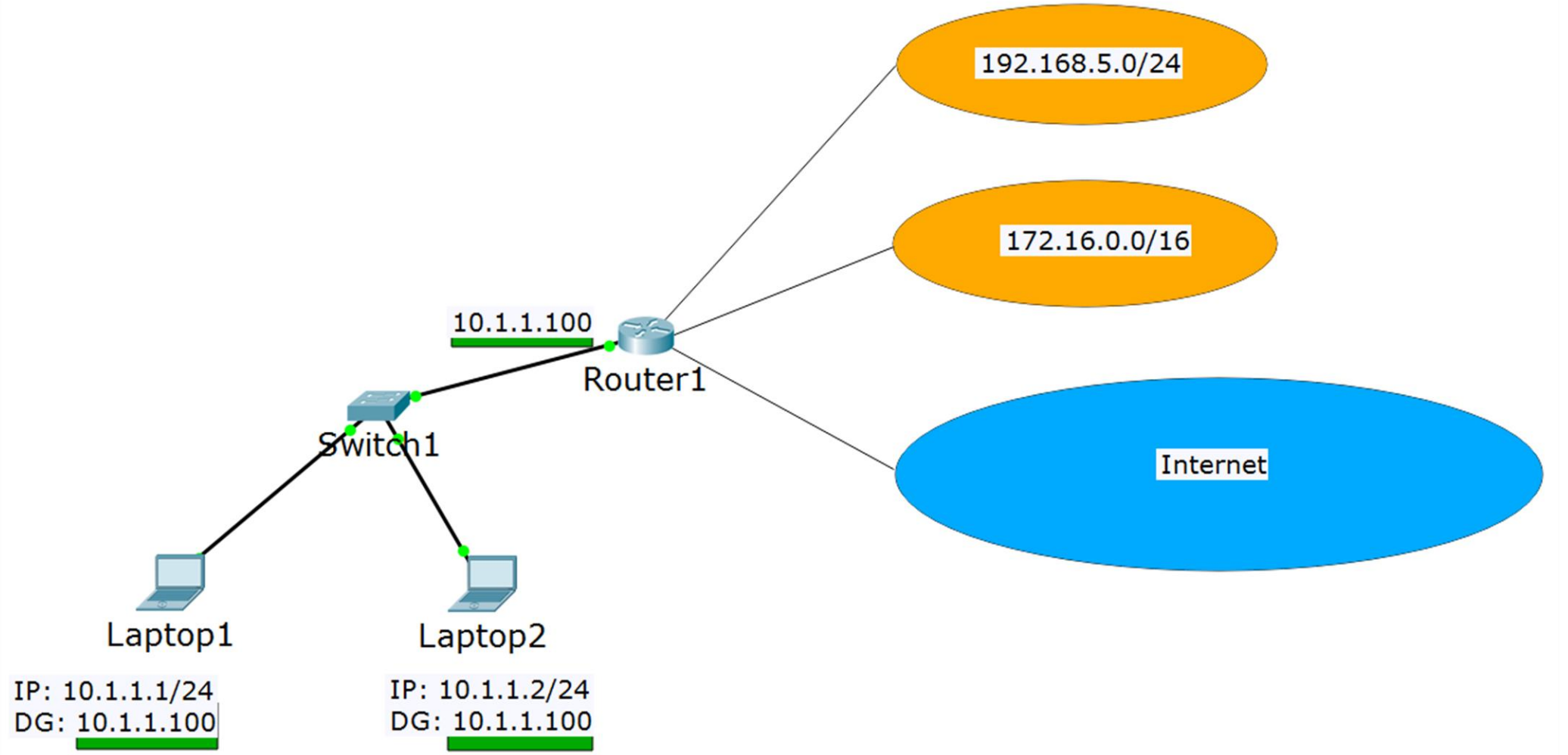
All masks are /24

My routing table:

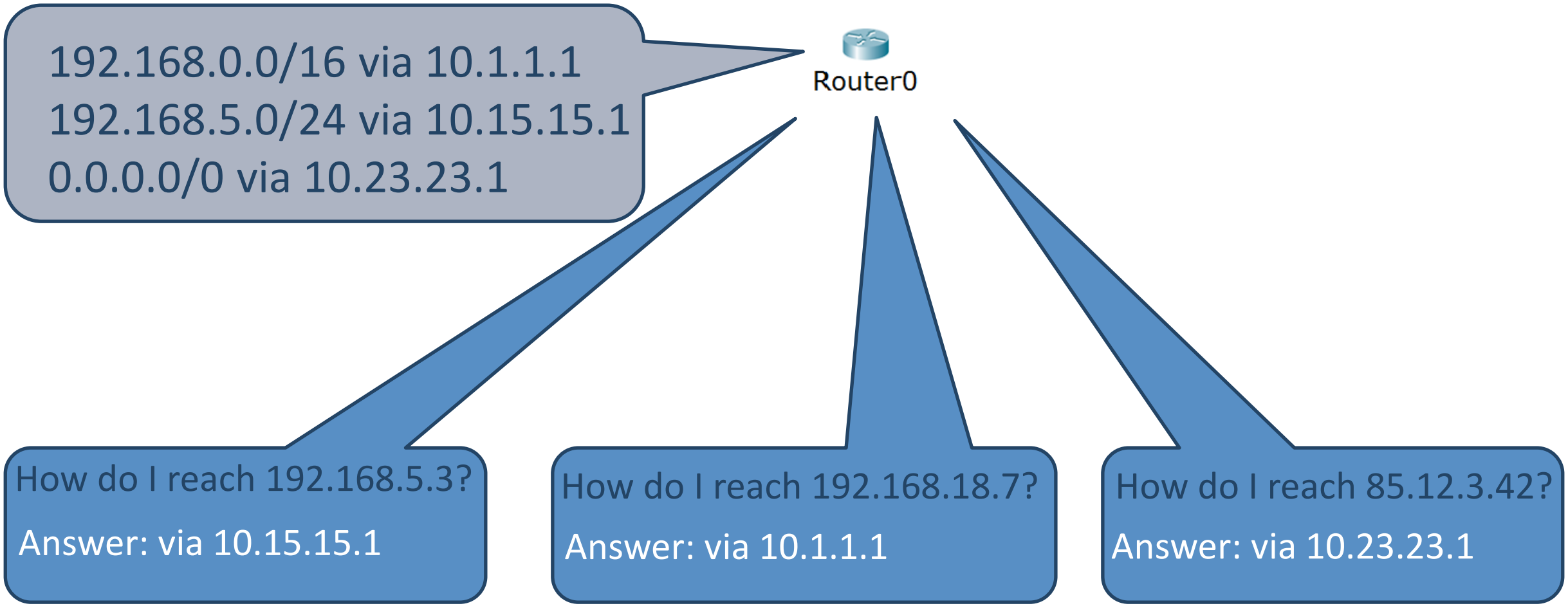
192.168.5.0/24 via 10.1.1.1
172.16.0.0/16 via 10.15.15.1
87.15.23.0/24 via 10.23.23.1
10.1.1.0/24 is connected
10.15.15.0/24 is connected
10.23.23.0/24 is connected

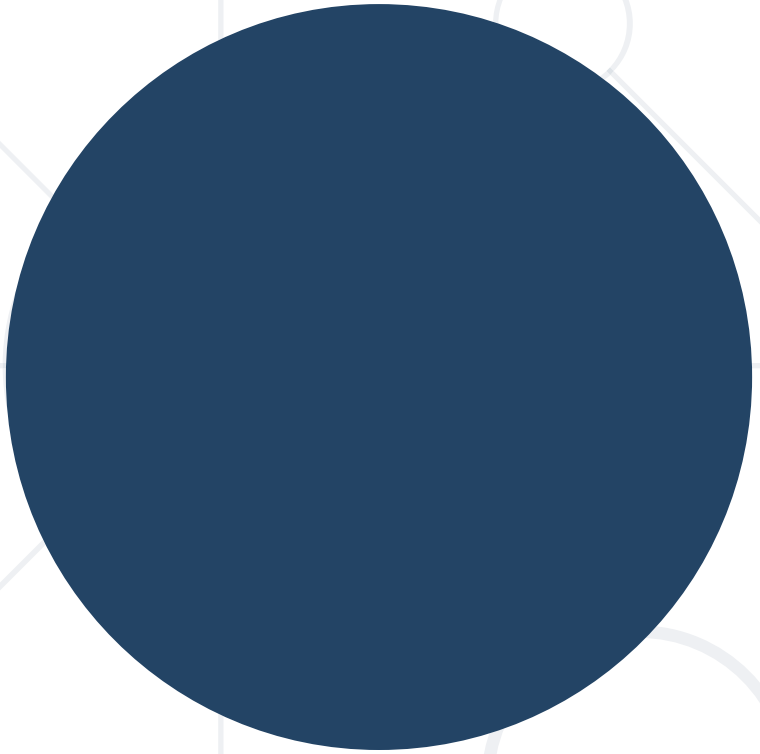


Default Gateway



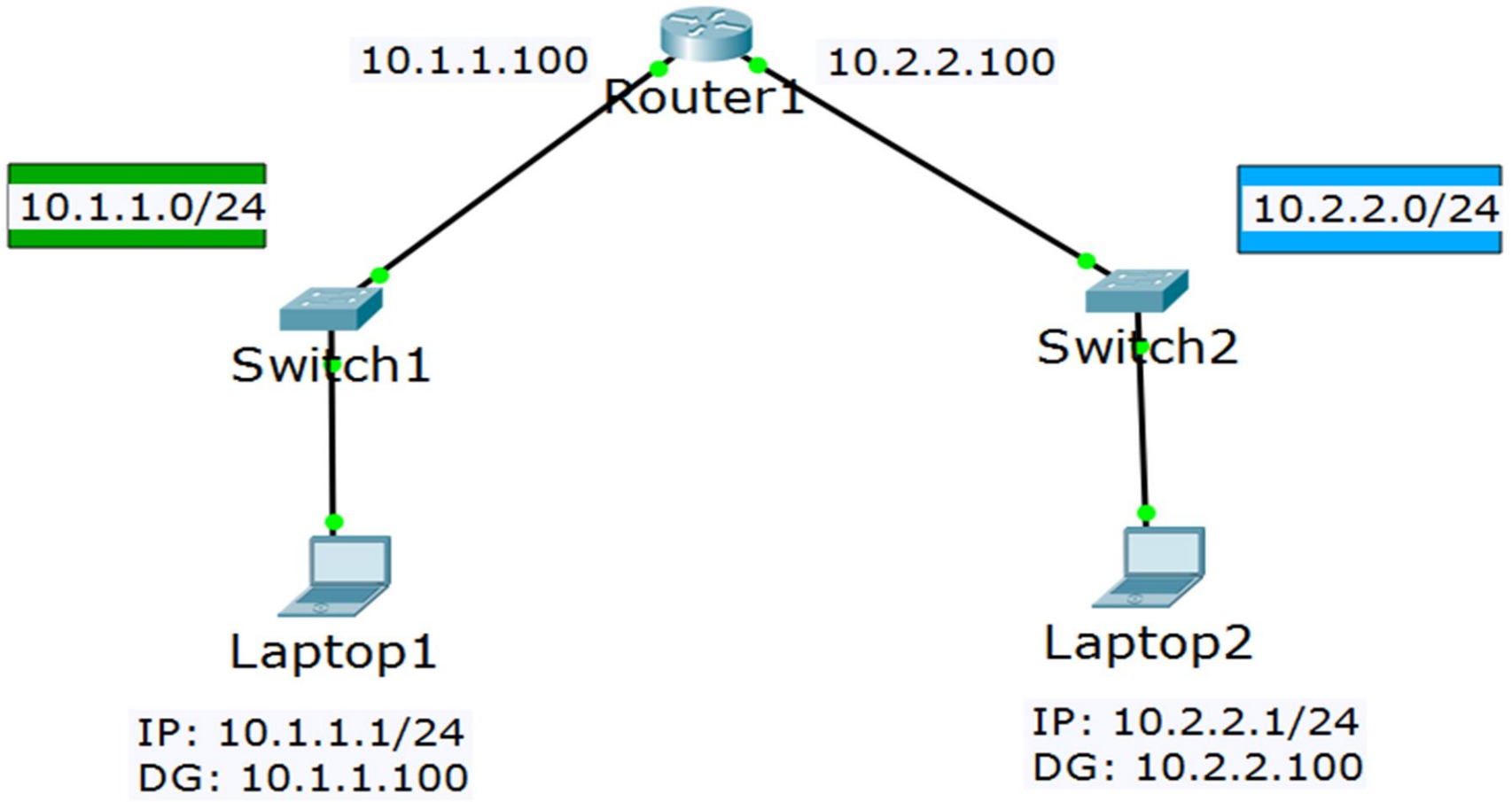
The Rule of the Longest Match

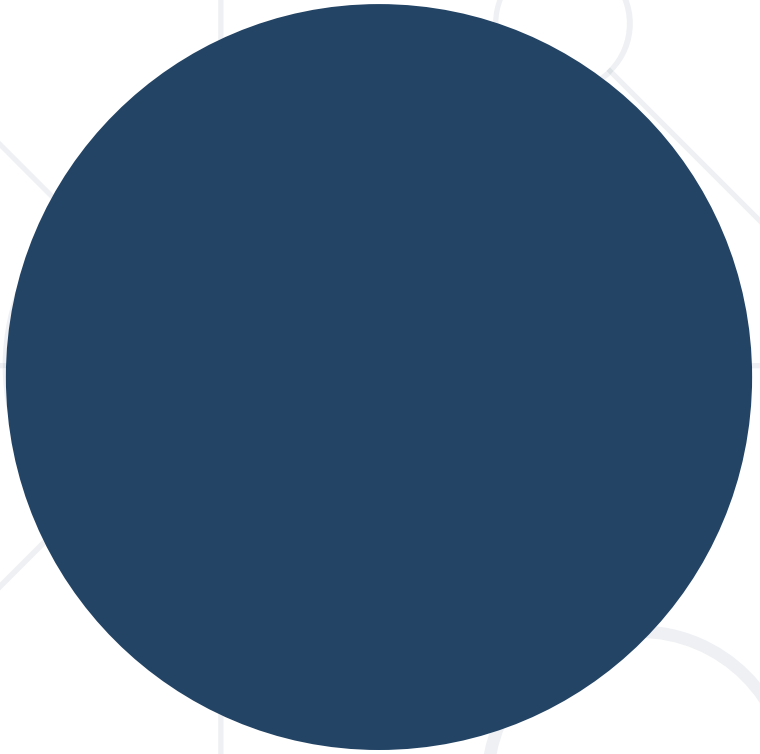




Direct routing

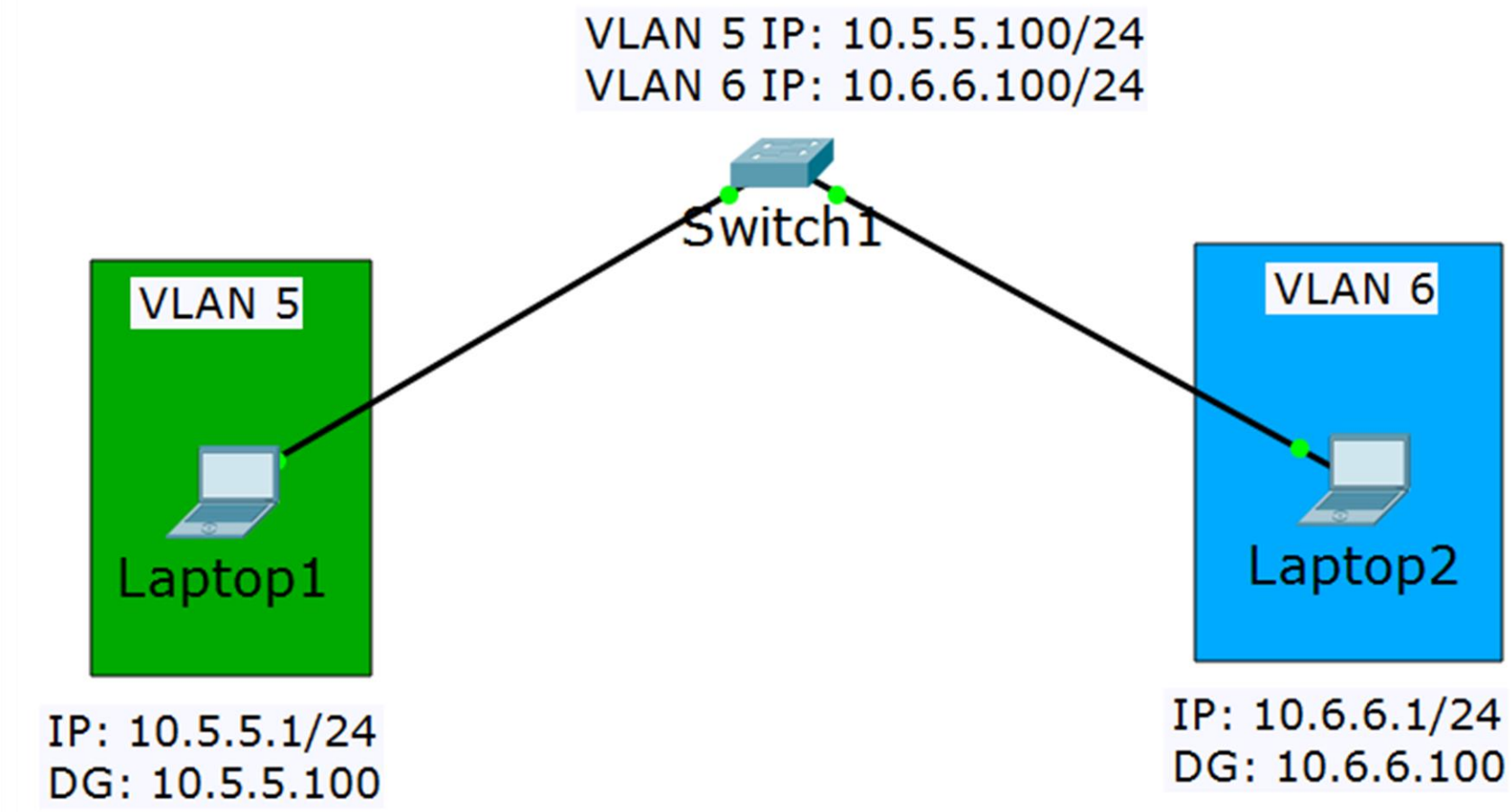
Direct routing



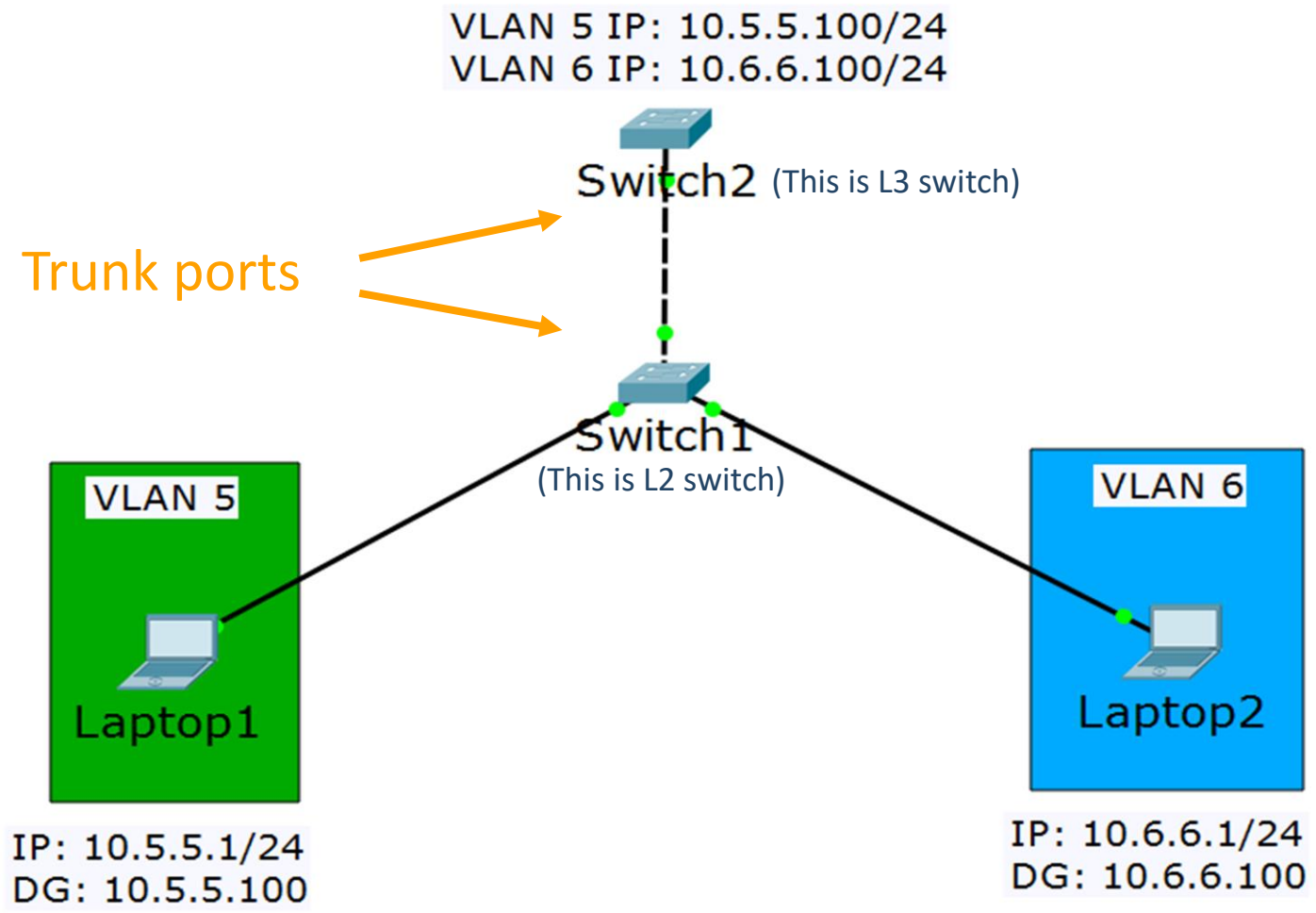


Inter-VLAN routing

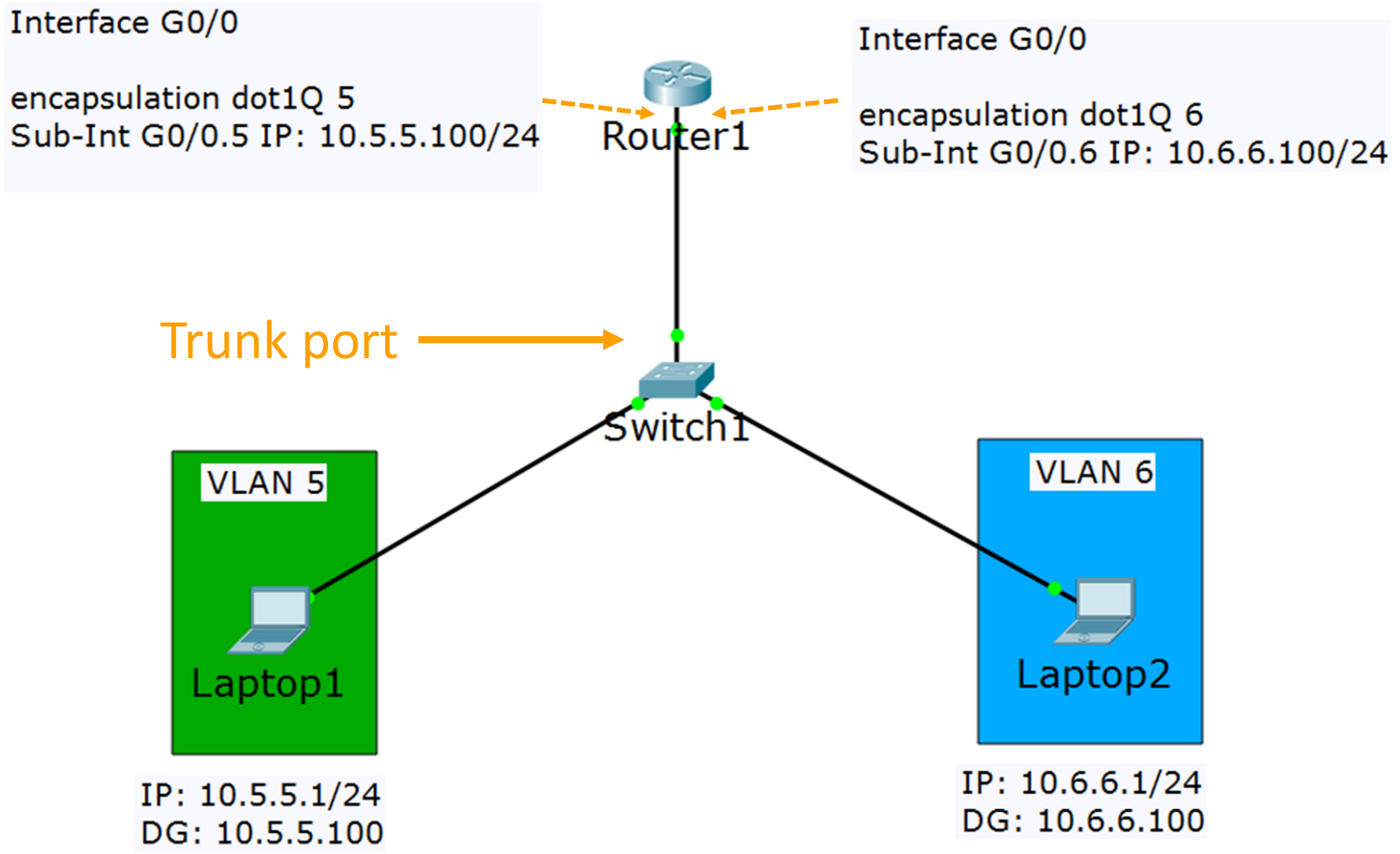
Inter-VLAN Routing Using the Same Switch

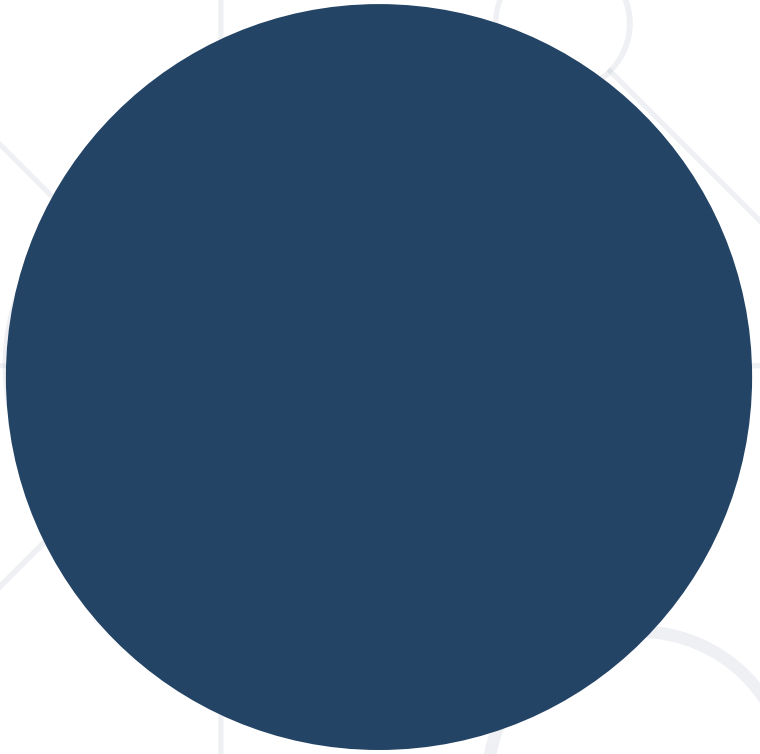


Inter-VLAN Routing Using External Switch



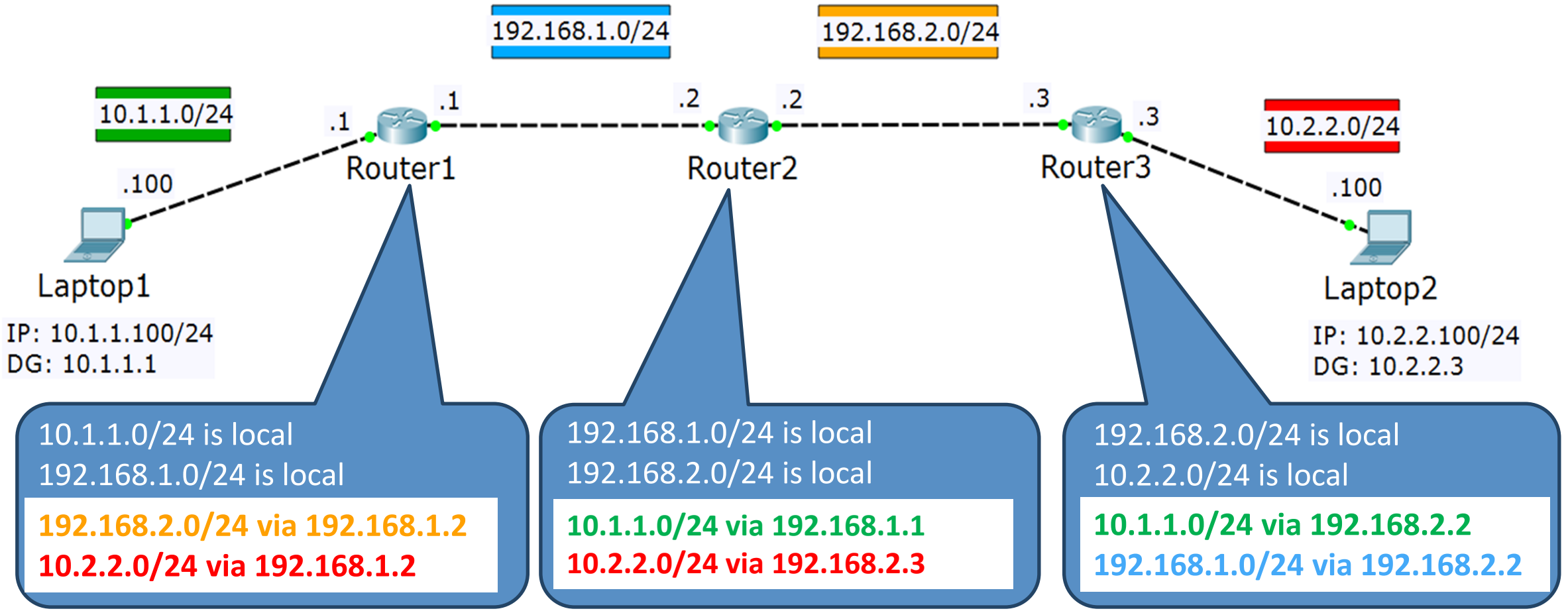
Inter-VLAN Routing Using External Router (2)

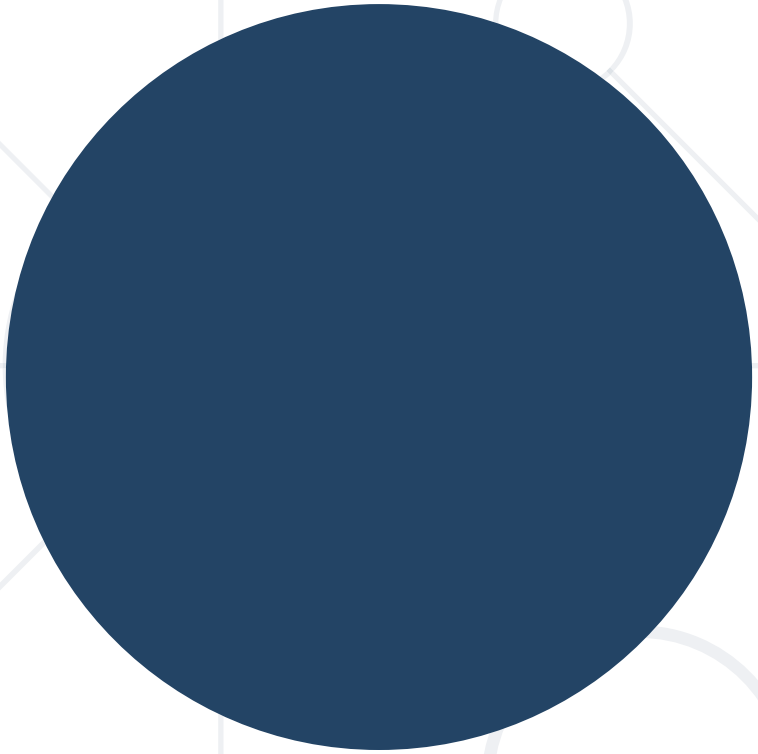




Static routing

Static Routes



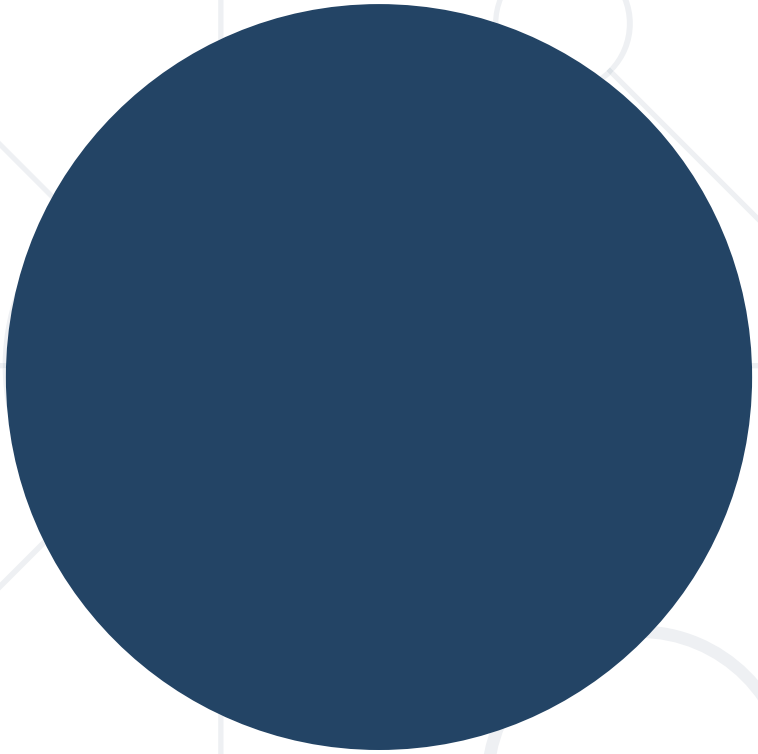


Routing demonstrations

Back to ToC

Practice

- Wireshark demonstration
- Packet Tracer demonstrations:
  - Static routing
  - The rule of the longest match
  - SVI (Switch Virtual Interface) vs. IP address on a physical port
  - L2 vs L3 (**no switchport**) interface on a Layer 3 switch
  - **ip route 0.0.0.0 0.0.0.0** vs. **ip default-gateway**
  - Static routing and administrative distance
  - ECMP (Equal Cost MultiPath)
  - Administrative distance vs. the rule of the longest match



Introduction to dynamic routing

Back to ToC

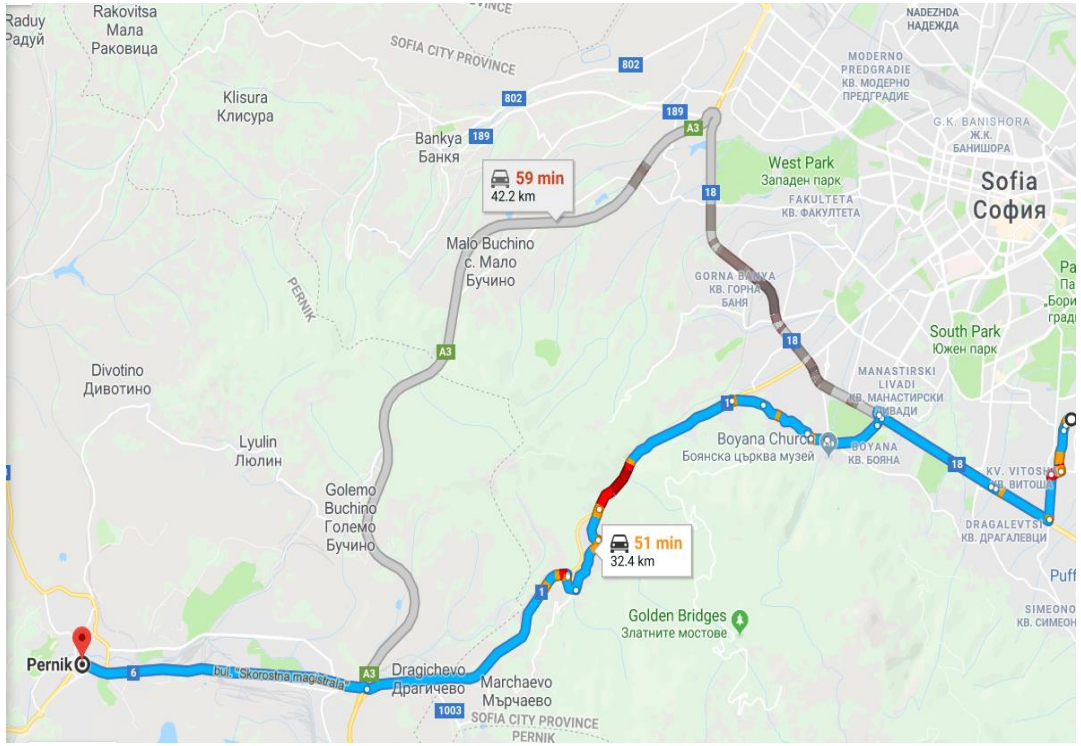
Static vs dynamic routing

- **Static routing**:
  - Routes to destination networks configured manually
  - Routing tables not updated if there is better route or lost network
  - Big administrative overhead, hard to manage
- **Dynamic routing**:
  - Routers dynamically exchange the networks they know about
  - Routing tables are created with the best routes to destinations
  - Routing tables dynamically create or remove entries

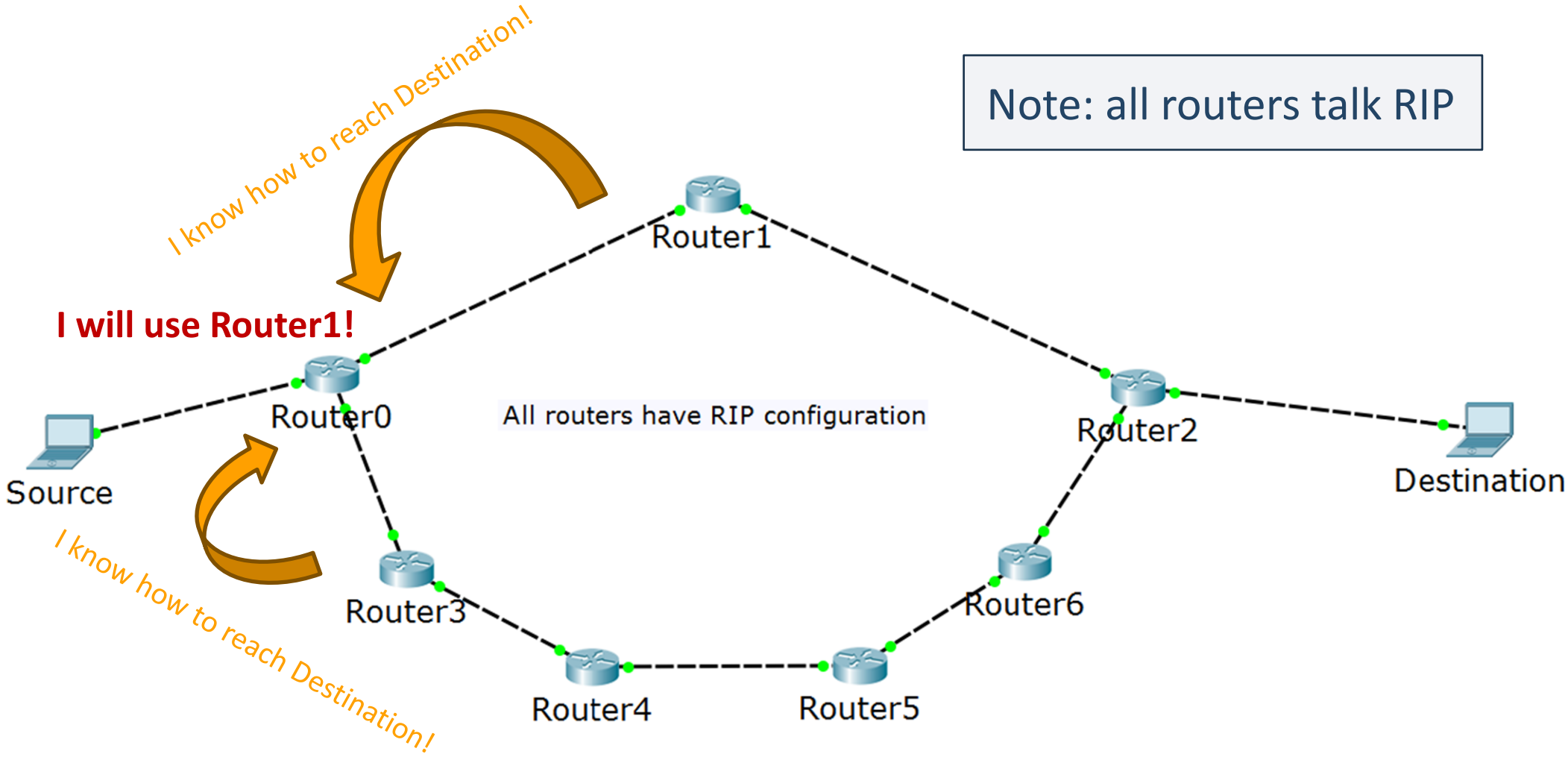
Distance-vector vs link-state protocols

- Distance-vector protocols

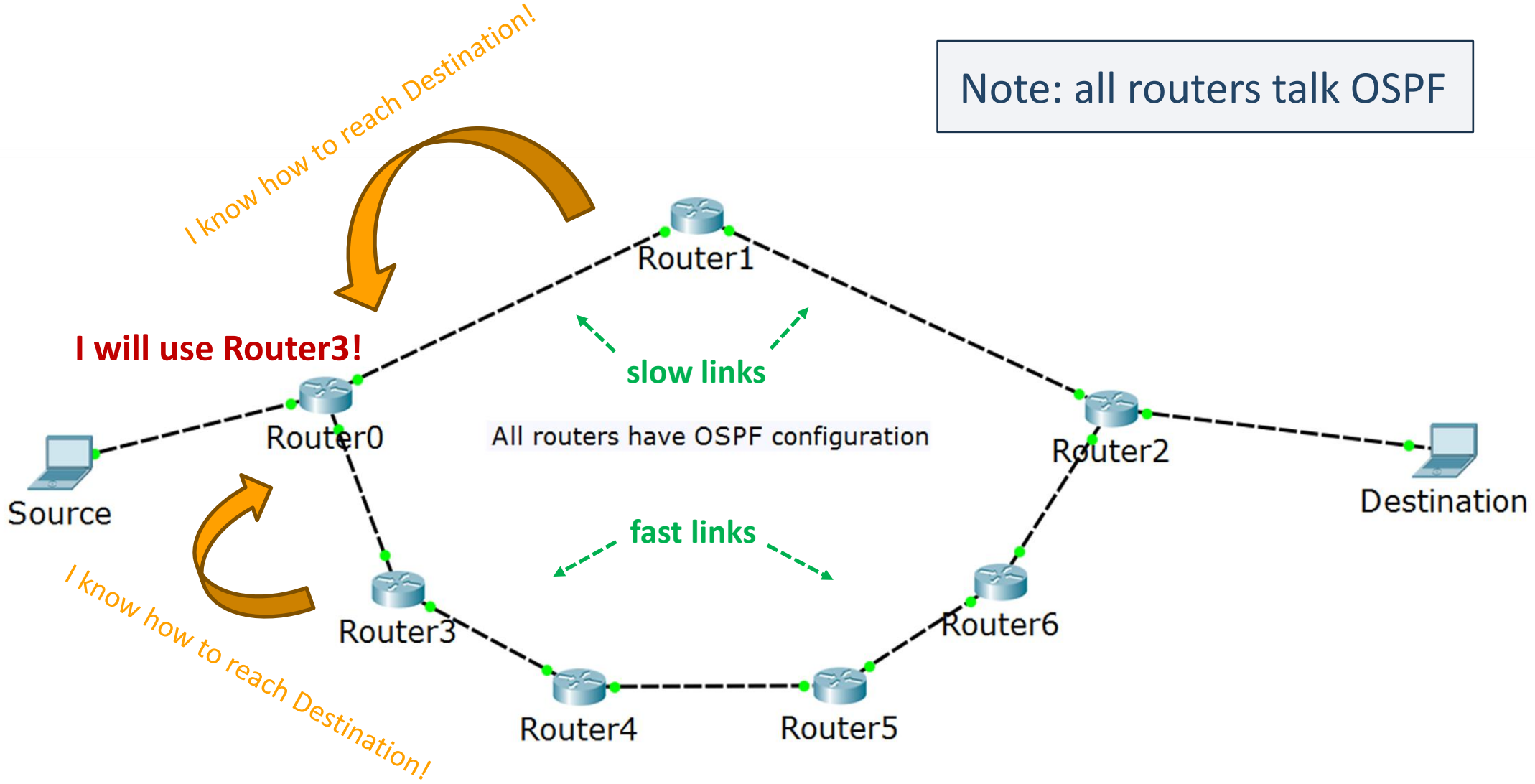
- Link-state protocols



RIP Metric: hop count



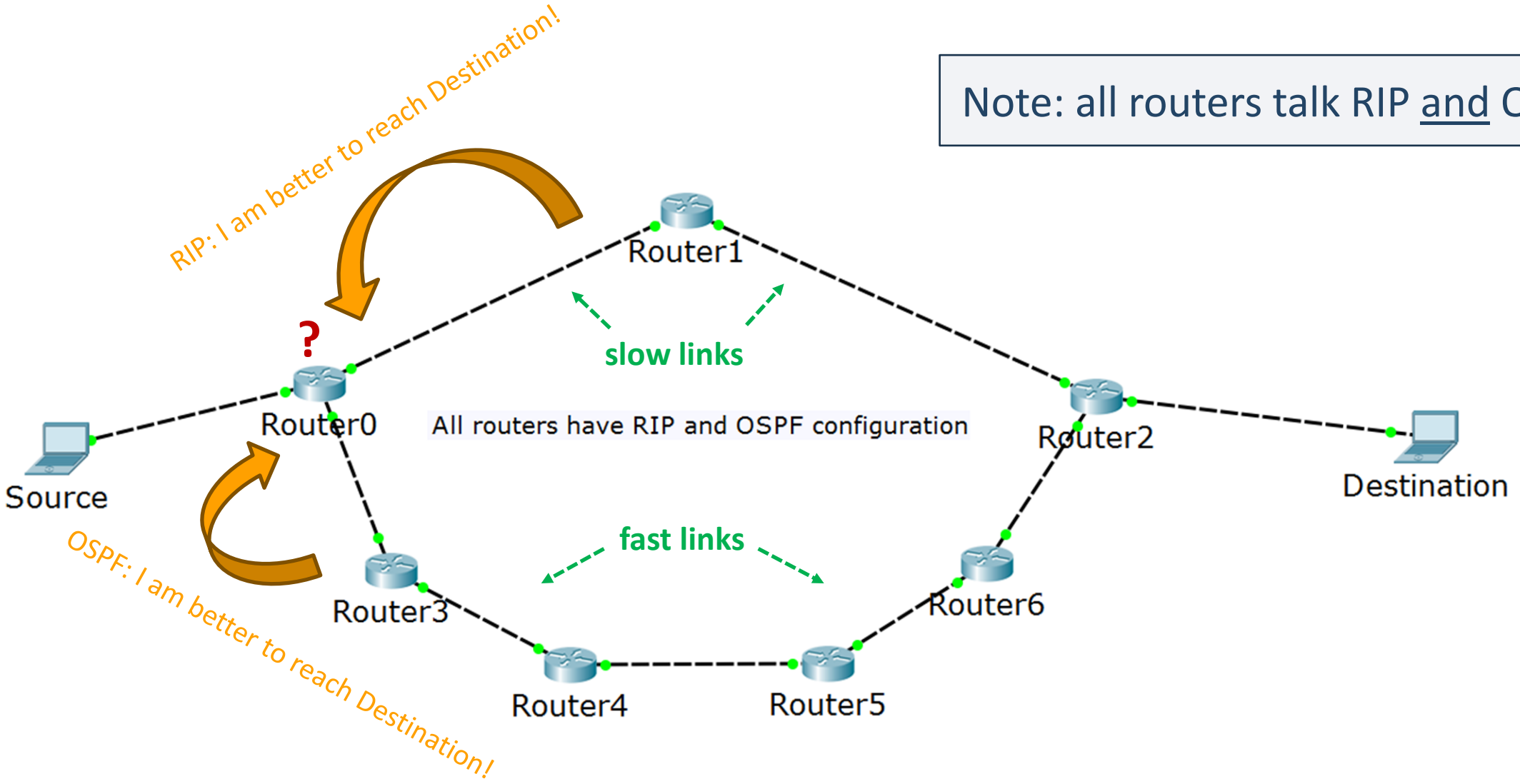
OSPF Metric: cost



Multiple protocols in the same network

Software University

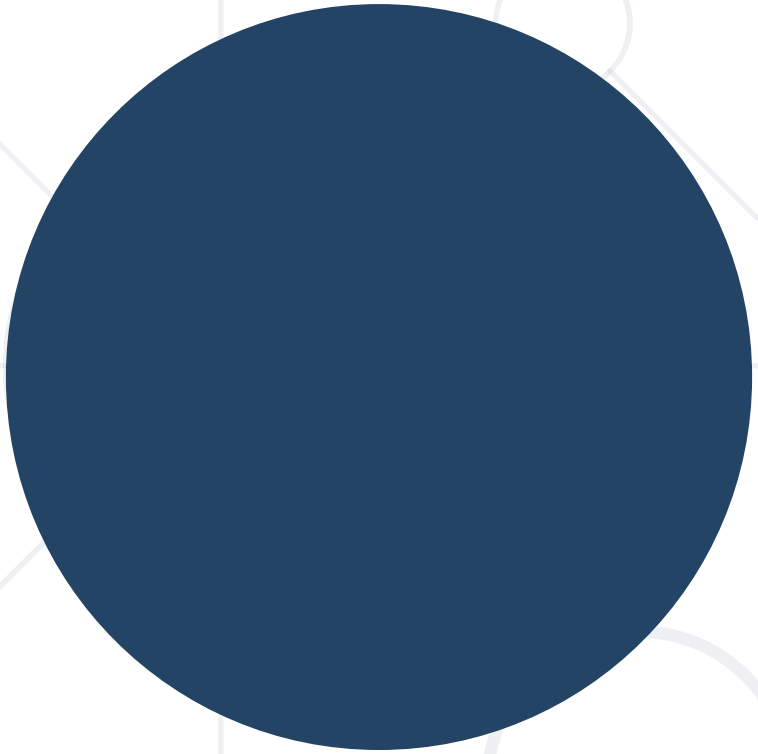
Note: all routers talk RIP and OSPF



Administrative distance

Software University

Route Source	Default Distance	Routing Table Entry
Connected interface	0	C
Static route out an interface	0	S
Static route to a next-hop address	1	S
EIGRP summary route	5	D
External BGP	20	B
Internal EIGRP	90	D
IGRP	100	I
OSPF	110	O
IS-IS	115	i
RIPv1, RIPv2	120	R
Exterior Gateway Protocol (EGP)	140	E
ODR	160	O
External EIGRP	170	D EX
Internal BGP	200	B
Unknown	255	



OSPF introduction

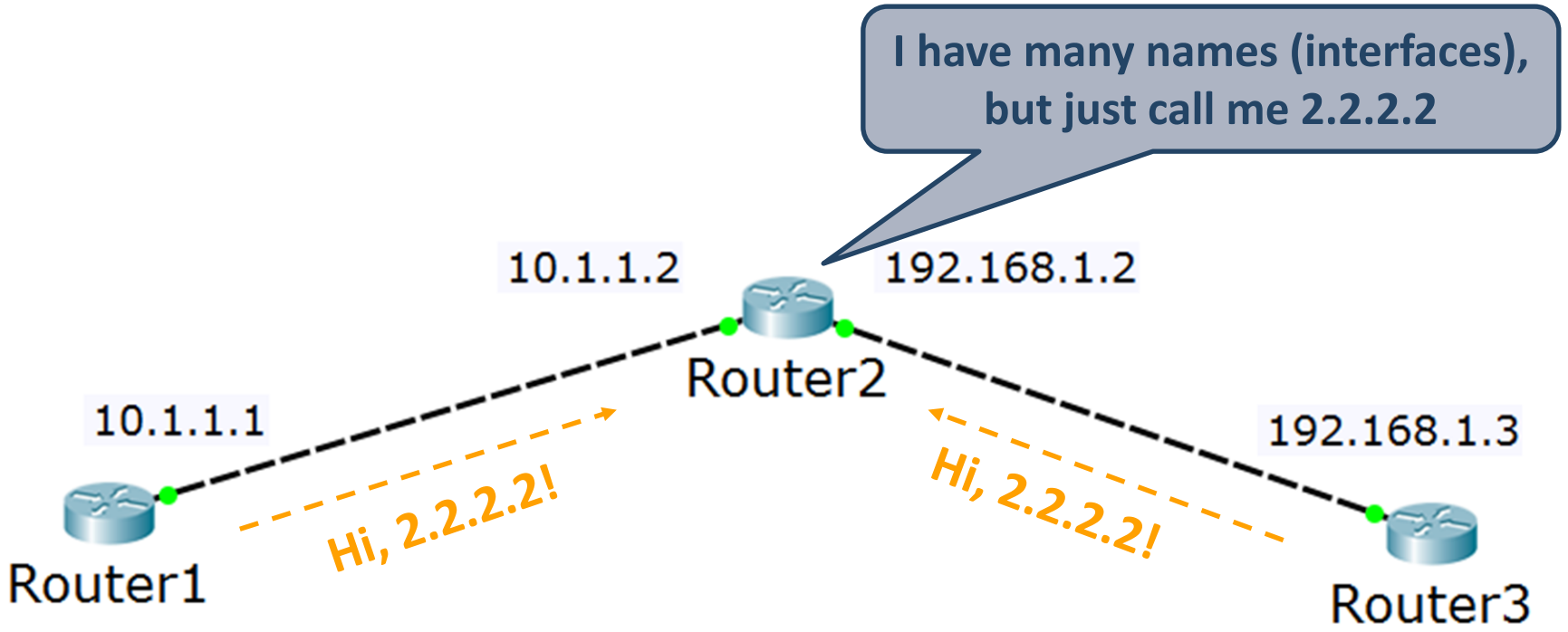
OSPF advantages

- Fast convergence with triggered updates
- Hierarchical structure (areas)
- VLSM support (classless protocol)
- Efficient communication with neighbors
- Uses intelligent metric (cost)
- Open standard

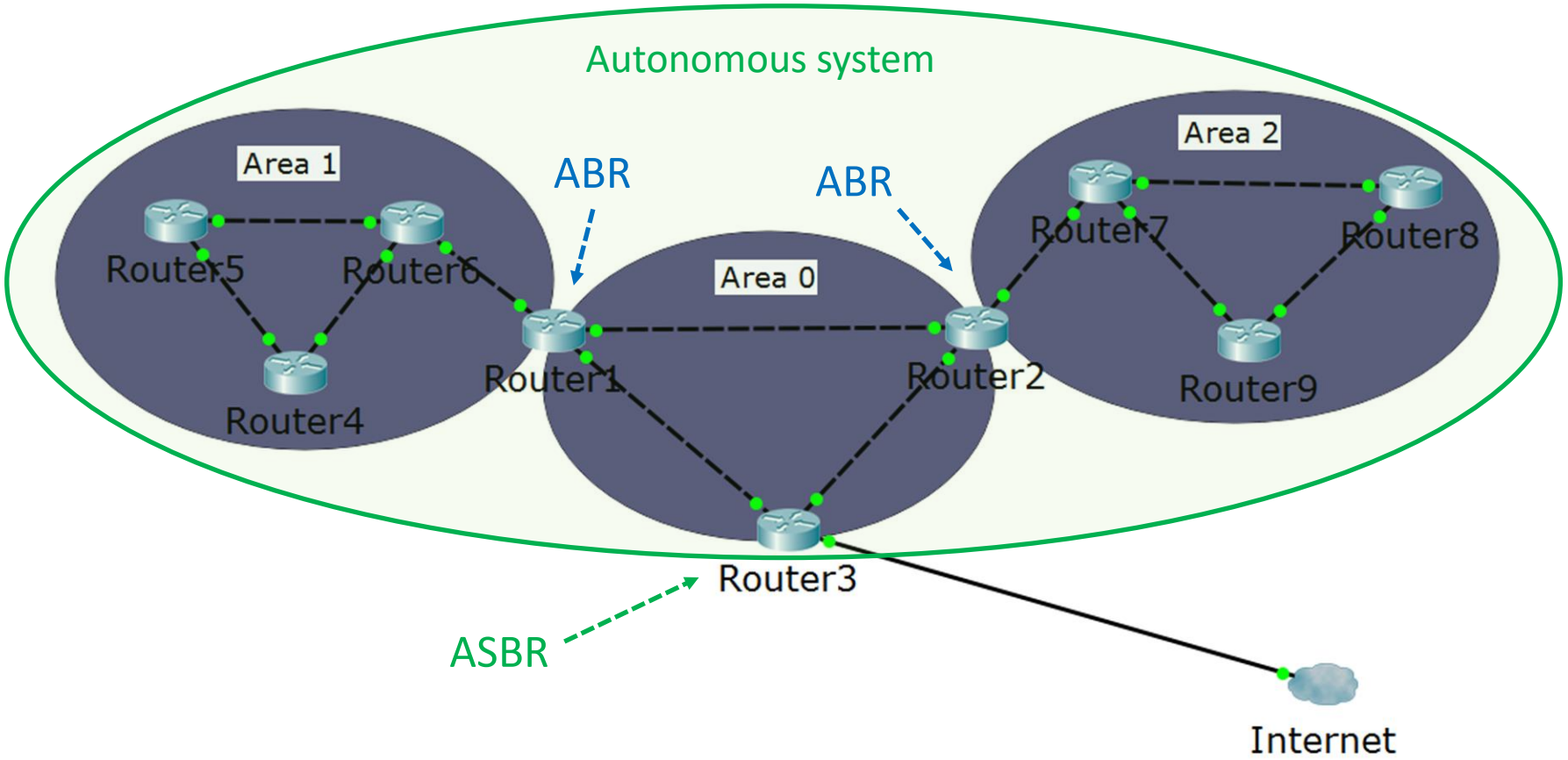
Wildcard masks

- In the subnet masks, 1 means “do care” and 0 means “don’t care”
- Examples:
  - 192.168.1.0 255.255.255.0 -> refers to 192.168.1.0 network
  - Loopback address: 10.1.1.1 255.255.255.255 -> exact IP address
- In the wildcard masks, 0 means “do care” and 1 means “don’t care”
- Examples:
  - 192.168.1.0 0.0.0.255 -> refers to 192.168.1.0 network
  - Loopback address: 10.1.1.1 0.0.0.0 -> exact IP address

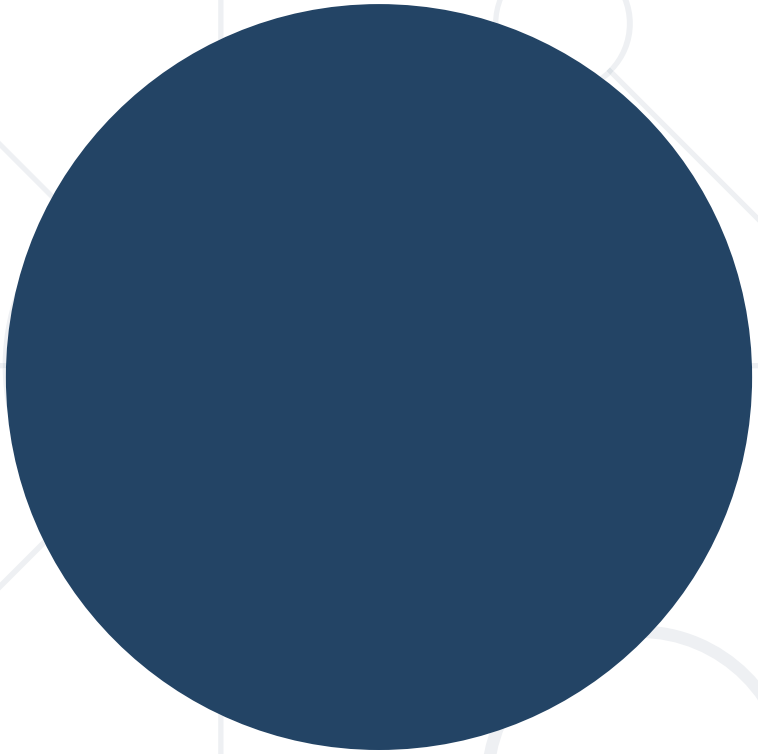
OSPF terms: router ID



OSPF terms



Area 0 = the backbone area



Single area OSPF configuration

Single area OSPF configuration

- Minimum configuration:
  - **router ospf *process_id***
  - **router-id *number*** (optional)
  - **network A.B.C.D *wildcard_mask* area *number***
- Example:
  - **router ospf 1**
  - **router-id 1.1.1.1** (optional)
  - **network 192.168.1.0 0.0.0.255 area 0**
  - **network 10.0.0.0 0.0.0.255 area 0**

OSPF passive interface

Software University

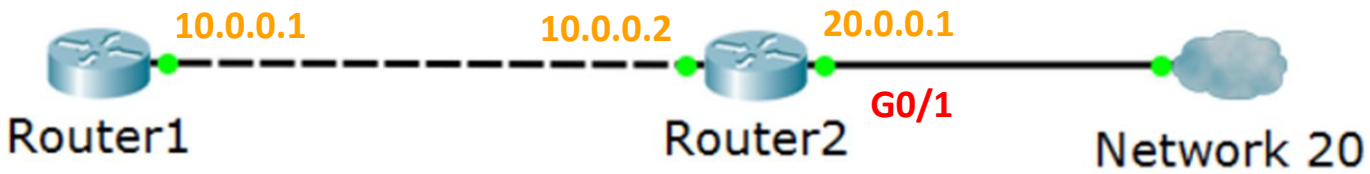
- The “network” command advertises the network AND sends hello messages out of the interface
- What if there is non-OSPF device on the other end of the link?
  - The Hello packets will be useless
  - Represents security issues
- One solution: use passive interfaces

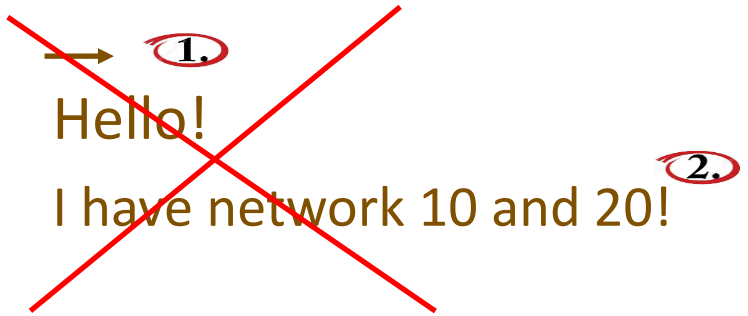
OSPF passive interface (2)

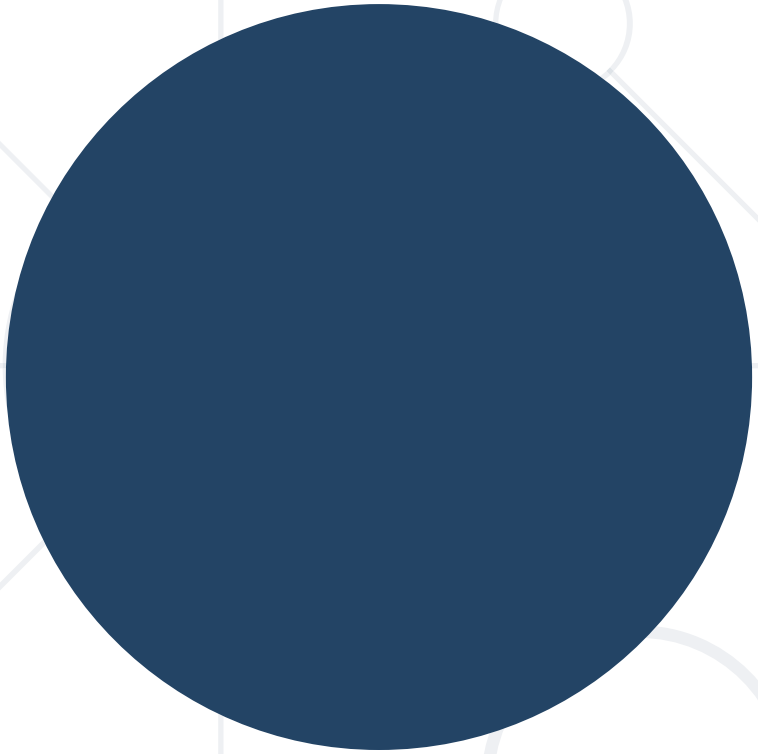
R1:
network 10.0.0.0 0.0.0.255

R2:
network 10.0.0.0 0.0.0.255
network 20.0.0.0 0.0.0.255

passive-interface G0/1

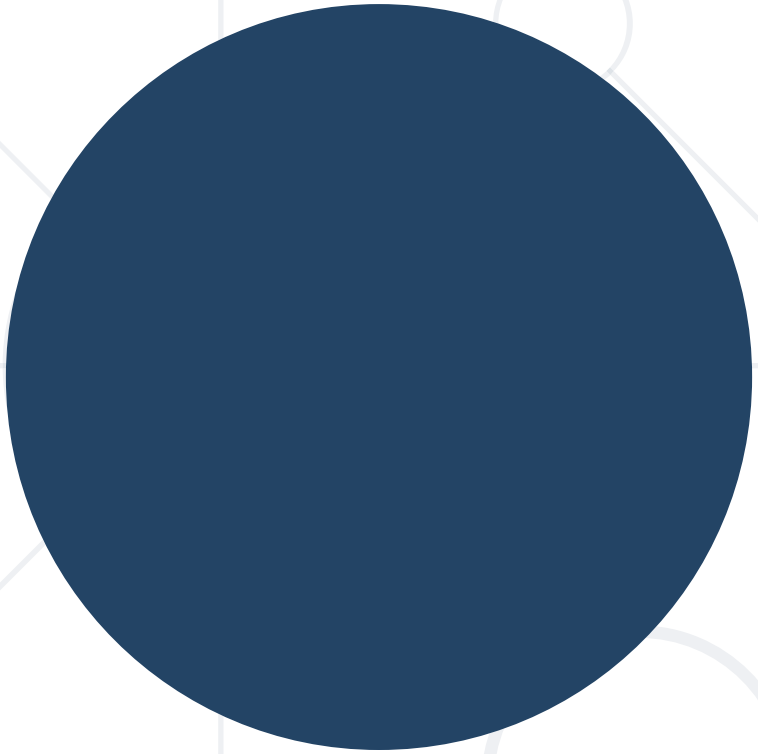






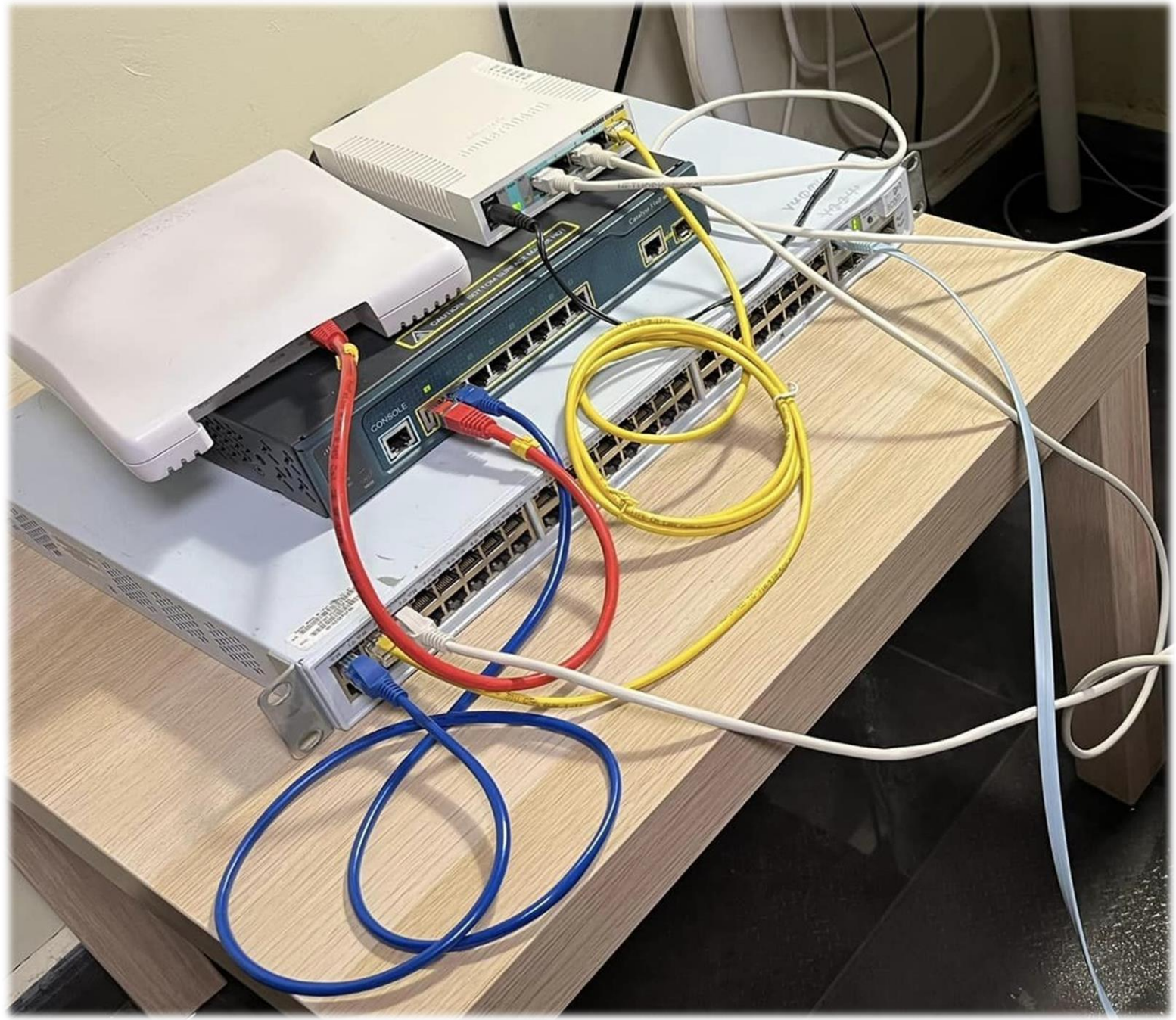
Course summary and exam preparation

Back to ToC



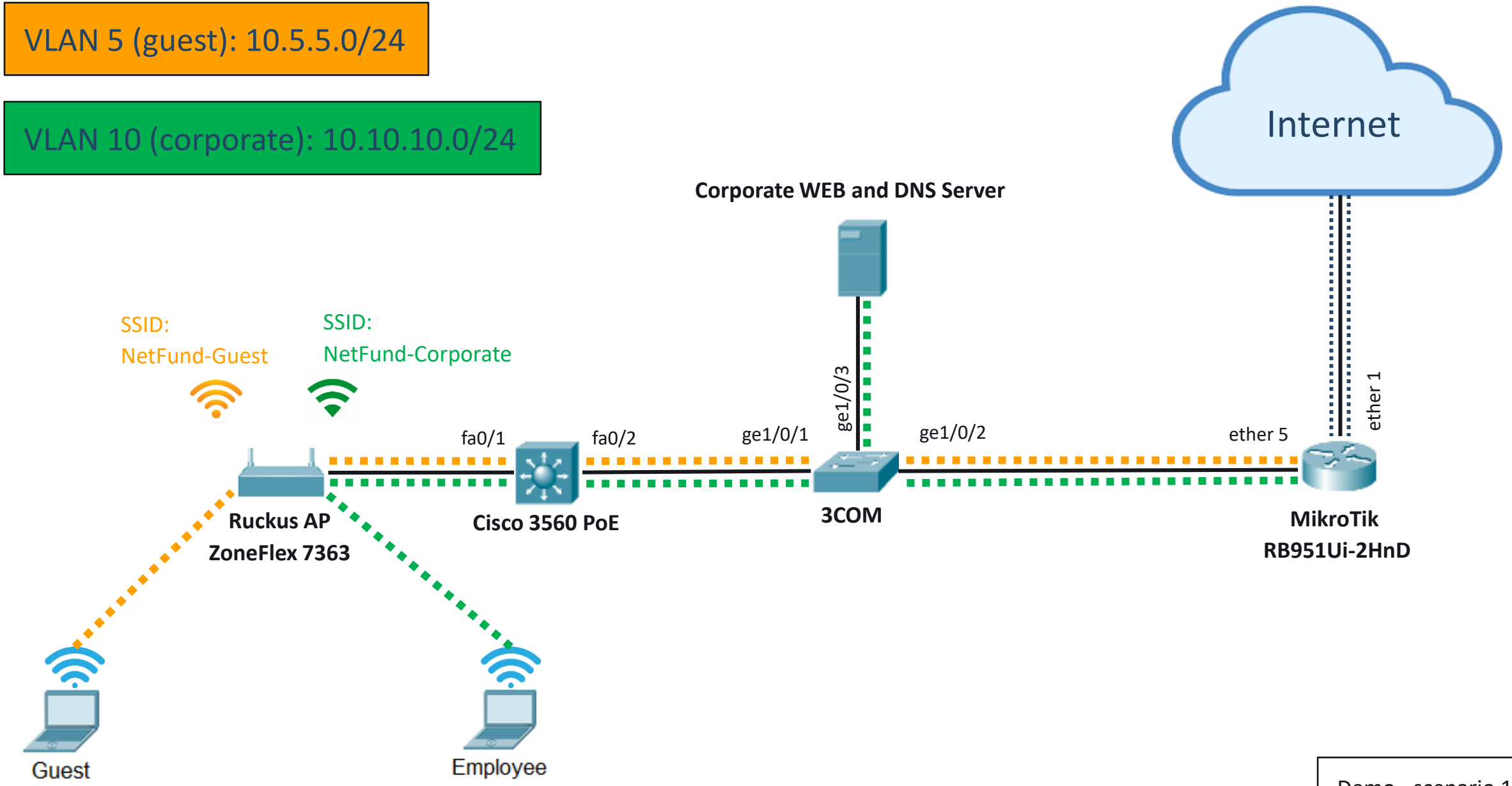
Building LAB with physical devices - scenario 1

Back to ToC


CONSOLE

VLAN 5 (guest): 10.5.5.0/24

VLAN 10 (corporate): 10.10.10.0/24



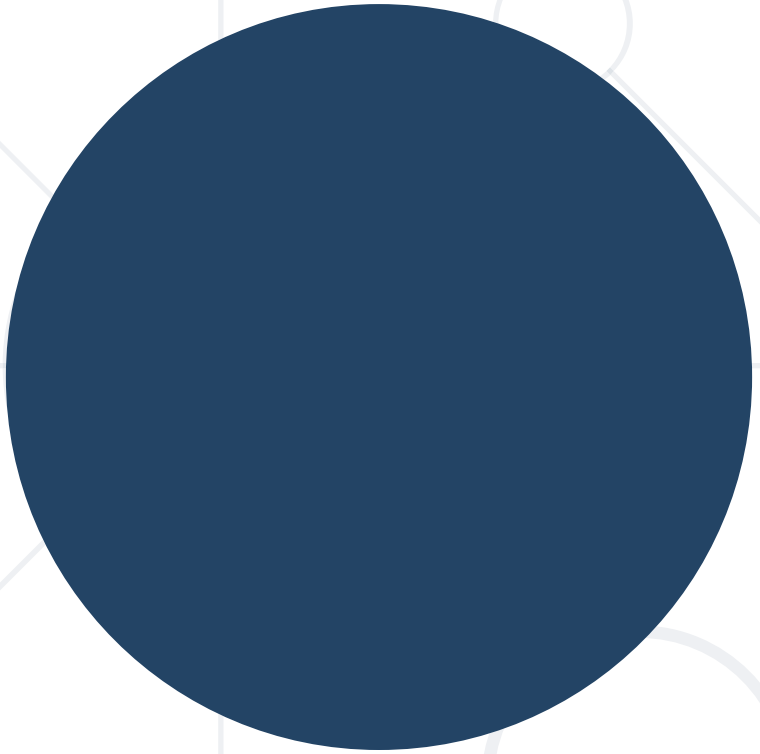
Demo - scenario 1

Topology details – scenario 1

Software University

- DHCP server for both VLANs is the Cisco device
- MikroTik is routing the VLANs and making NAT to “outside”

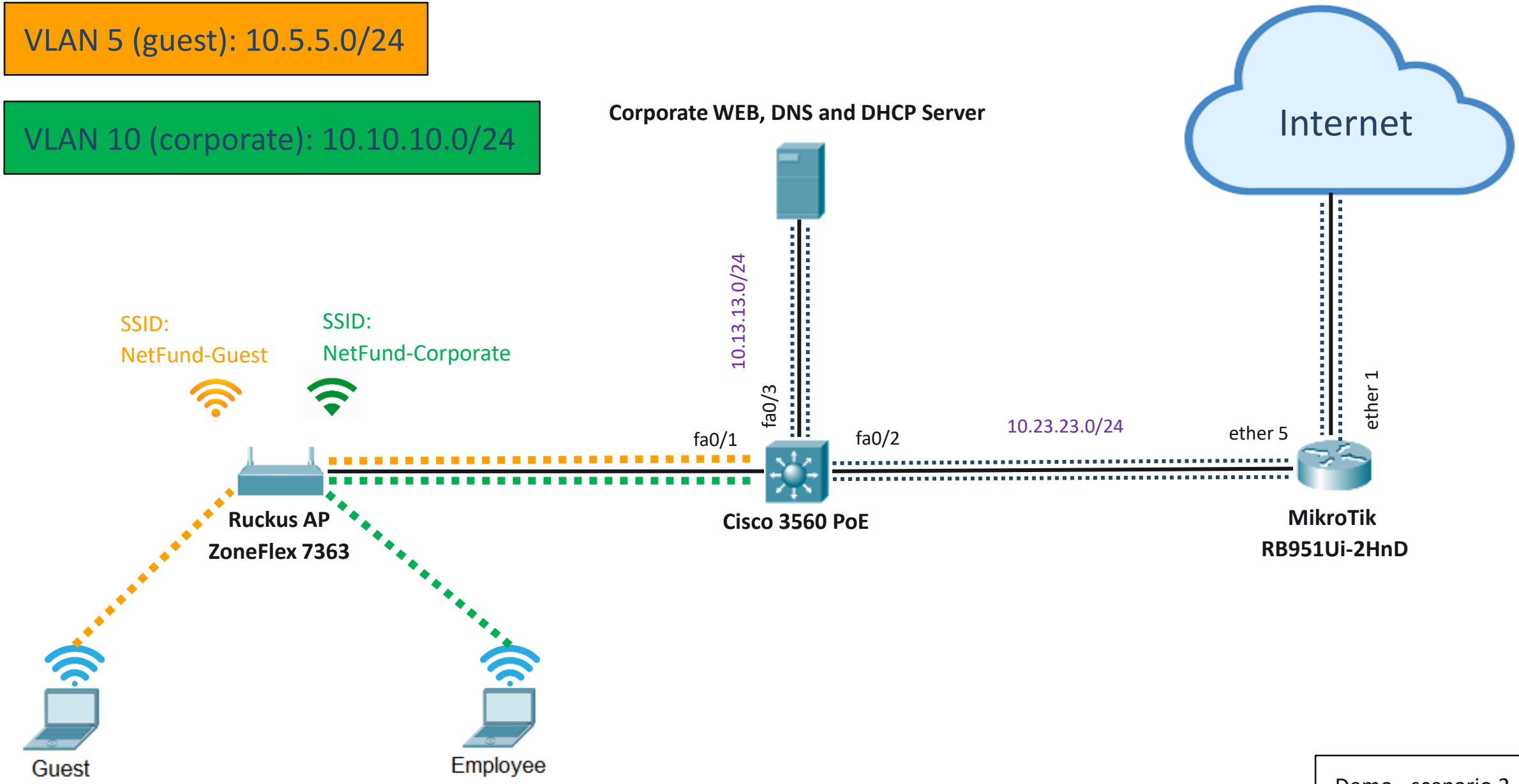
Device, interface	IP address
Cisco, VLAN 5	10.5.5.3
Cisco, VLAN 10	10.10.10.3
HP, VLAN 5	(10.5.5.2)
HP, VLAN 10	(10.10.10.2)
Corporate server (Web and DNS)	10.10.10.101
MikroTik, VLAN 5	10.5.5.1
MikroTik, VLAN 10	10.10.10.1



Building LAB with physical devices - scenario 2

VLAN 5 (guest): 10.5.5.0/24

VLAN 10 (corporate): 10.10.10.0/24



Demo - scenario 2

Topology details – scenario 2

- DHCP server for both VLANs is the (Windows) Server
- Cisco is routing the VLANs, MikroTik is making NAT to “outside”

Device, interface	IP address
Cisco, VLAN 5	10.5.5.3
Cisco, VLAN 10	10.10.10.3
Cisco, fa0/3	10.13.13.3
Cisco, fa0/2	10.23.23.3
Corporate server (Web and DNS)	10.13.13.101
MikroTik, ether 5	10.23.23.1

Summary

1. Introduction to networking
2. IP addresses and host-to-host communication – part 1
3. IP addresses and host-to-host communication – part 2
4. Network access, security and VLANS
5. Layer 2 redundancy – Spanning Tree Protocol
6. IP services and basic routing
7. Routing demonstrations
8. Dynamic routing with OSPF
9. Course summary and exam preparation
10. Building LAB with physical devices

SoftUni Diamond Partners

Software University

SUPER HOSTING .BG

Coca-Cola HBC Bulgaria

Flutter™ International

INDEAVR
Serving the high achievers

AMBITIONED

DRAFT KINGS

SOFTWARE GROUP

BOSCH

Postbank
Решения за твоето утре

PHAR VISION

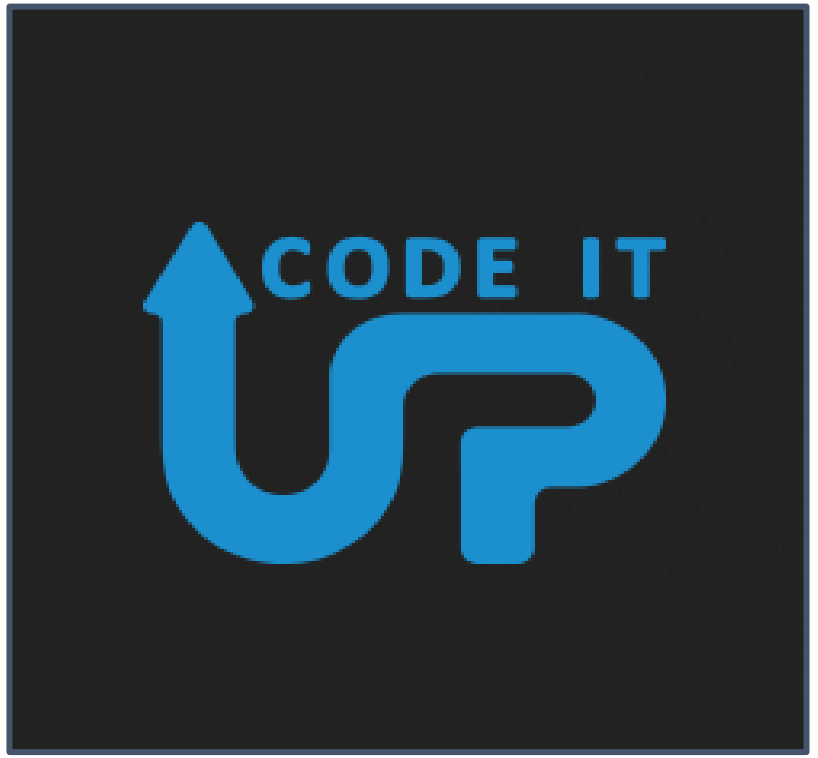
SmartIT

DXC TECHNOLOGY

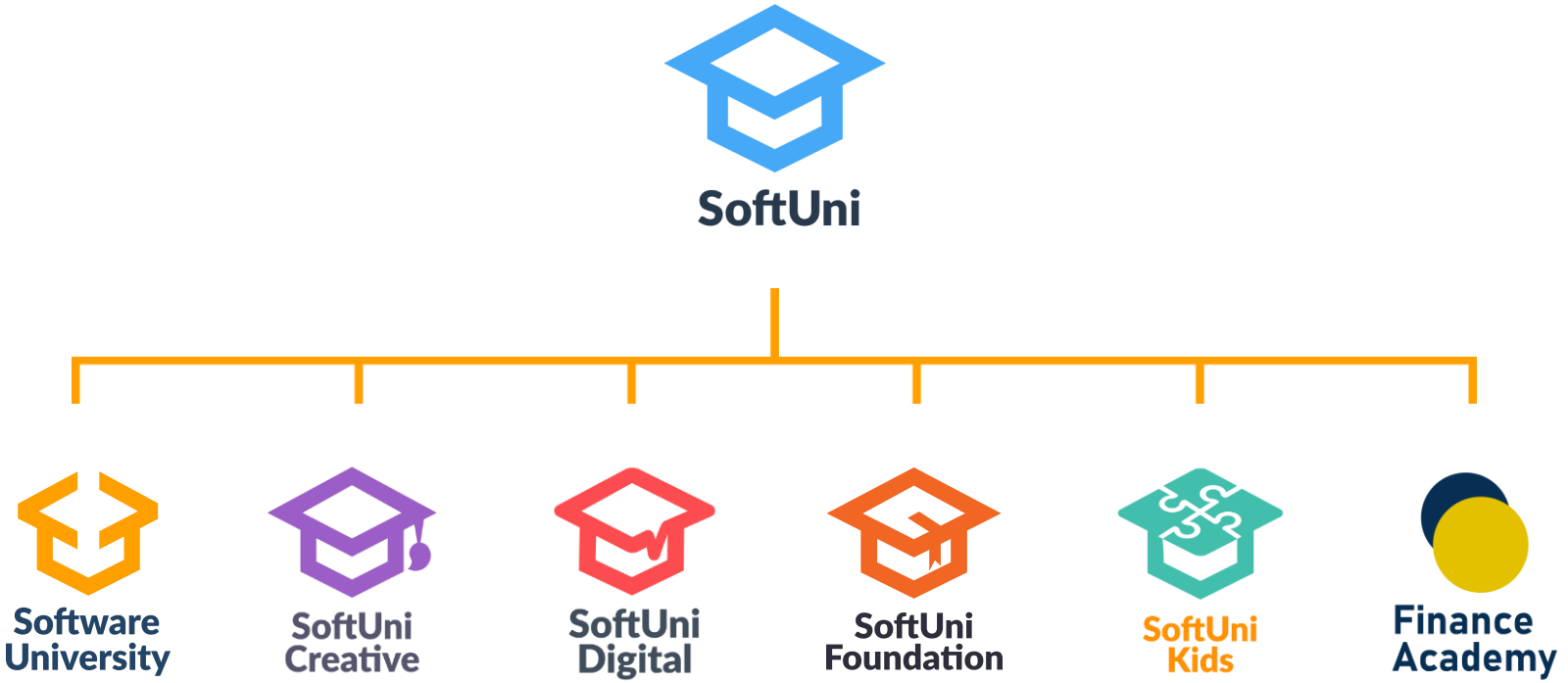
createX

Educational Partners

Software University



Questions?



Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Pr ofession 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

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://about.softuni.bg
- © Software University – https://softuni.bg