Computer Networking Advanced – Course Summary

Lecture 11

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Table of Contents

Have a Question?

Software University

sli.do

#CNA

Spanning Tree Protocol Advanced (1)

The STP algorithm

1. Elect the **Root** switch (Root bridge)
   - This is the switch with the lowest BID (Bridge ID)
   - BID = Switch Priority and MAC
2. Select the **root ports**
   - They have the best cost (lowest) to the Root
   - Selected per switch
3. Select the **designated ports**
   - They have the best cost (lowest) to the Root
   - Selected per segment (connection)
4. All other ports go to **blocking** state

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

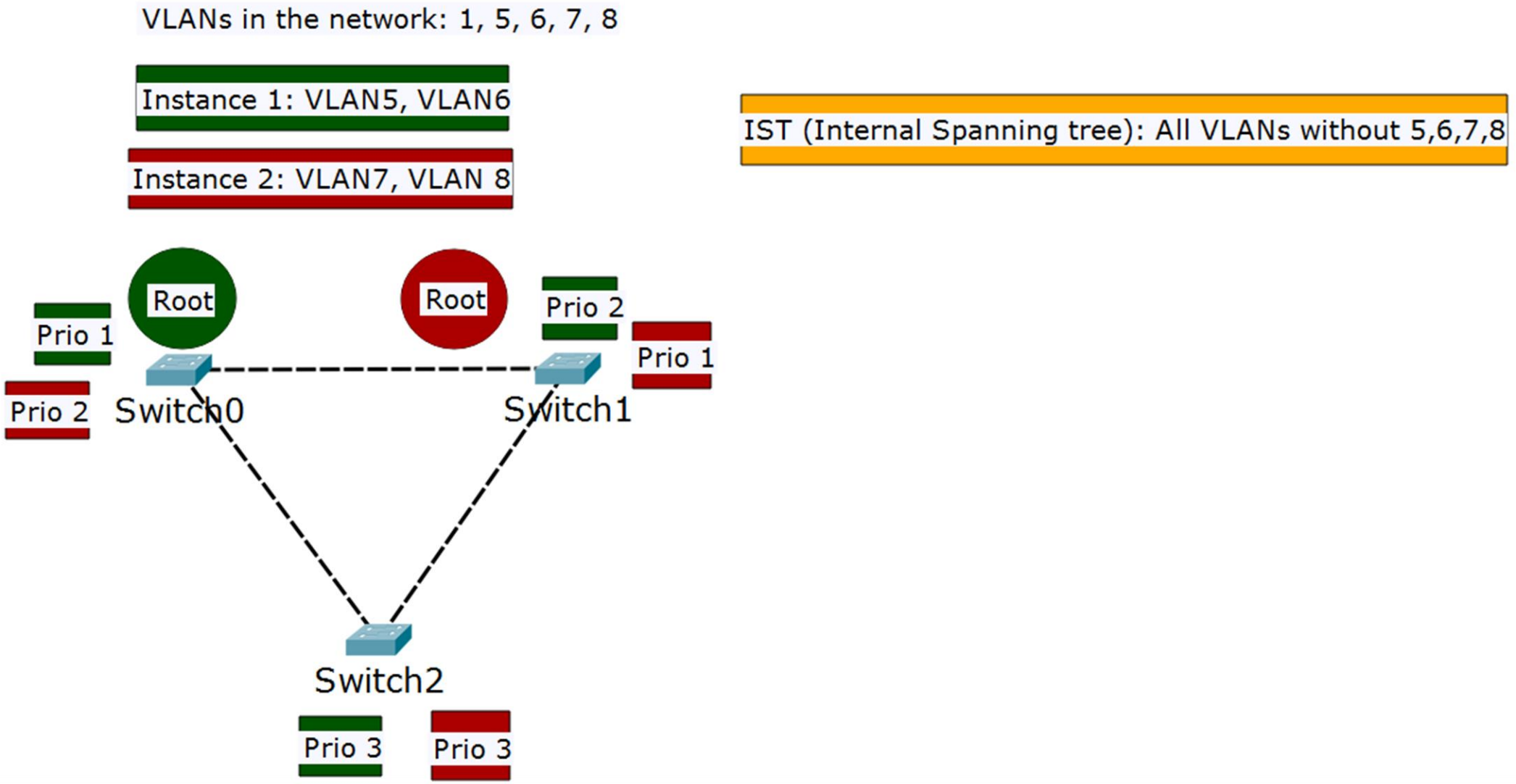
Spanning Tree Protocol – main flavors

- **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

MSTP

- Multiple Spanning Tree Protocol
- Creates multiple instances of the physical STP topology
- Can have **different Root** switches - one for each instance
- Provides **load-sharing** because of the multiple Roots
- It is also "rapid"
- One instance is mapped to one or multiple VLANs
- Needs additional configuration

MSTP: multiple roots



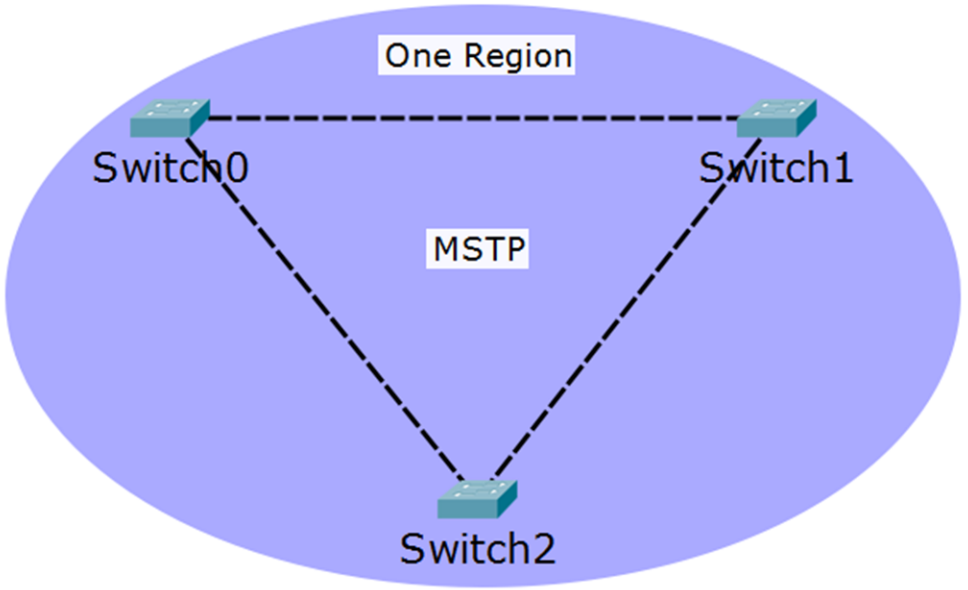
MSTP configuration

- All switches in the MSTP domain must be in the **same region**
- Three parameters should be configured equally on all switches:
  - Configuration Name (region name)
  - Revision number
  - VLAN-to-instance mappings
- The priorities are configured on a **per instance** basis

MSTP: all switches in the same region

Switch0:

1. Configuration name: SoftUni
2. Revision: 1
3. Instance 1 = vlan 5 and vlan 6
   Instance 2 = vlan 7 and vlan 8



Switch1:

1. Configuration name: SoftUni
2. Revision: 1
3. Instance 1 = vlan 5 and vlan 6
   Instance 2 = vlan 7 and vlan 8

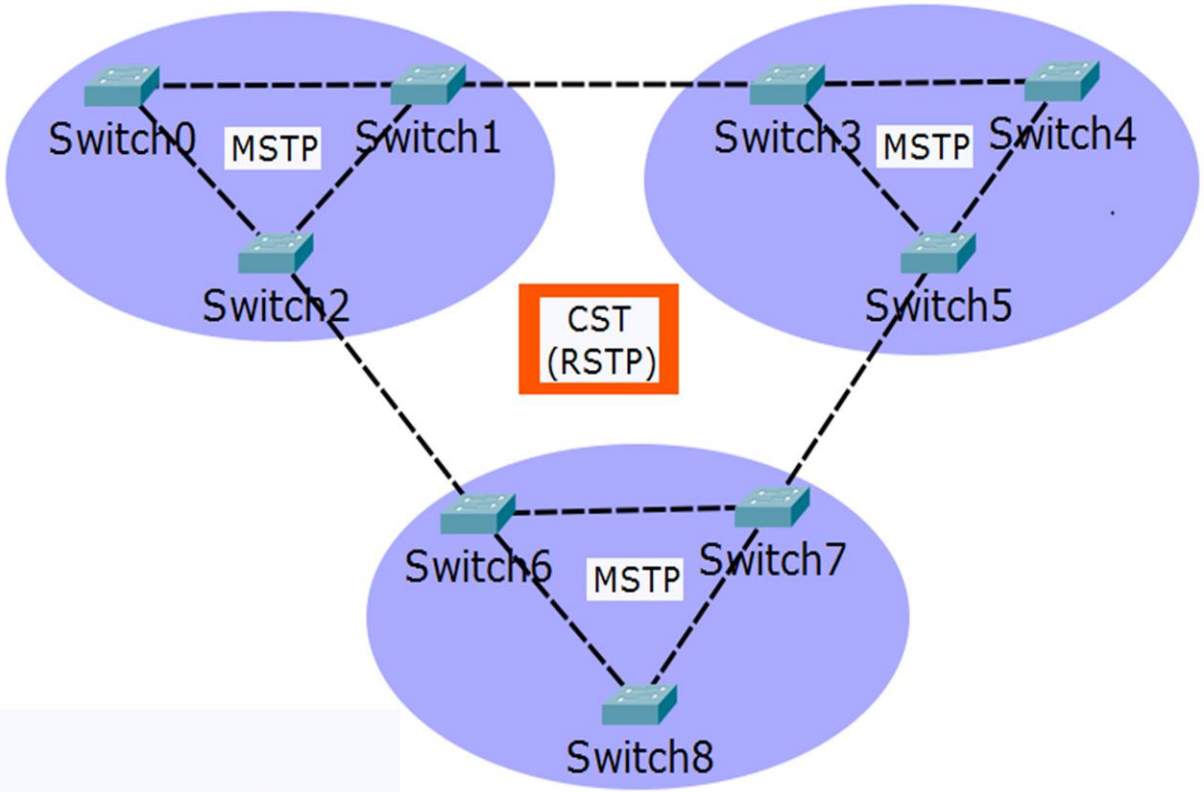
Switch2:

1. Configuration name: SoftUni
2. Revision: 1
3. Instance 1 = vlan 5 and vlan 6
   Instance 2 = vlan 7 and vlan 8

MSTP: multiple regions

Region1:

1. Configuration name: SoftUni
2. Revision: 1
3. Instance 1 = vlan 5 and vlan 6
   Instance 2 = vlan 7 and vlan 8



Region2:

1. Configuration name: Region2
2. Revision: 1
3. Instance 1 = vlan 5 and vlan 6
   Instance 2 = vlan 7 and vlan 8

Region3:

1. Configuration name: Test
2. Revision: 5
3. Instance 1 = vlan 15 and vlan 16
   Instance 2 = vlan 98 and vlan 3

MSTP vs PVST+

Software University

- Two similar protocols, which one is better?
- 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

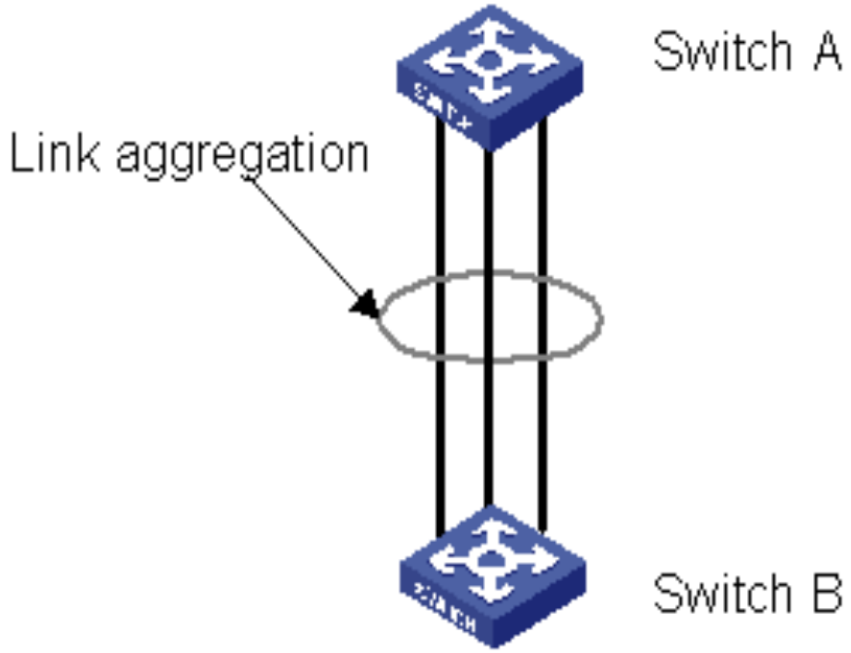
MSTP vs PVST+ (2)

- MSTP advantages:
  - uses **less BPDUs** and generates less overhead
  - open standard
- MSTP disadvantages:
  - **not VLAN aware** (does not look which VLANs are on the trunk ports)
  - Harder to configure
- Recommendation: use MSTP if you have more than 100 VLANs

Link Aggregation (1)

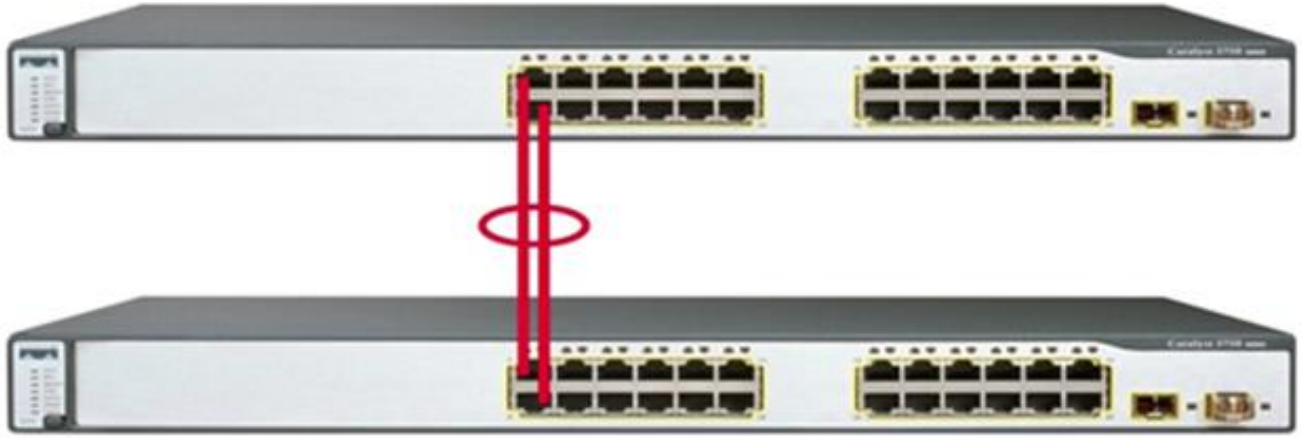
What is link aggregation?

- Combination of two or more physical interfaces to create one logical link or port
- Other terms with the same meanin
  - Port trunking (HPE Provision)
  - EtherChannel (Cisco)
  - Link bundling
  - NIC bonding/teaming
  - Etc.



Why to use link aggregation?

- To increase the bandwidth
- To provide redundancy



Load sharing modes

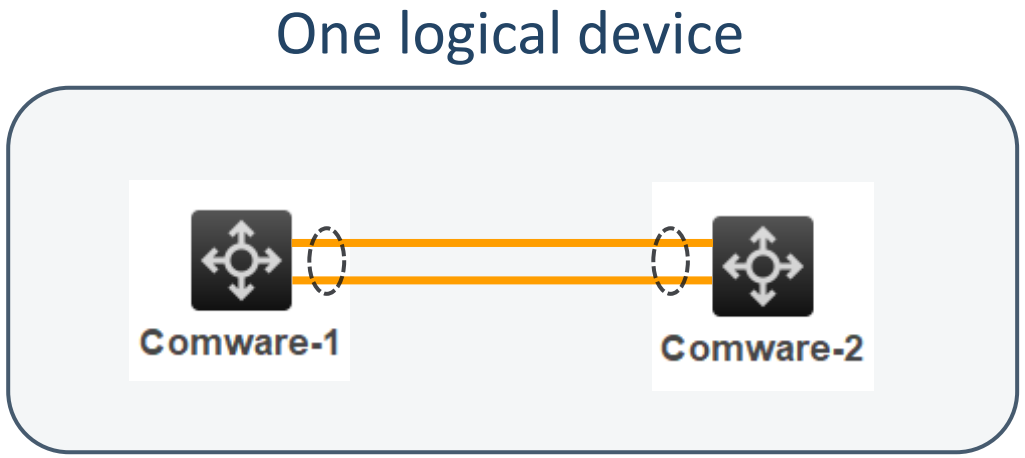
- Multiple physical links form one logical but at the end the traffic uses the physical links
- Which exact link to use - random decision based on the conversations
- Conversations depend on the load sharing mode

```
Switch(config)#port-channel load-balance ?
  dst-ip        Dst IP Addr
  dst-mac       Dst Mac Addr
  src-dst-ip    Src XOR Dst IP Addr
  src-dst-mac   Src XOR Dst Mac Addr
  src-ip        Src IP Addr
  src-mac       Src Mac Addr
```

Device Stacking – IRF (1)

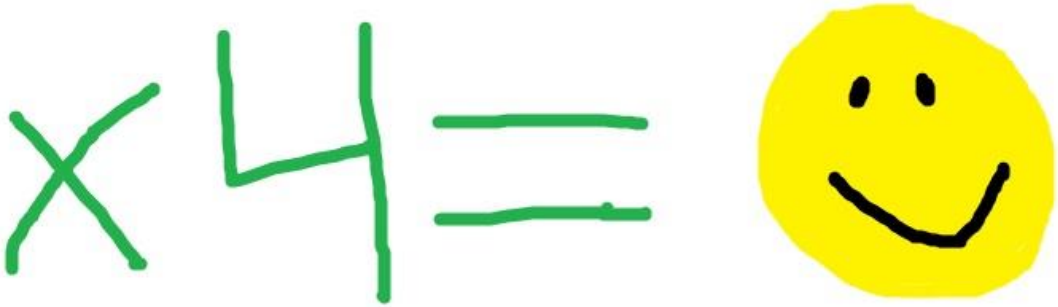
What is device stacking?

- Combination of two or more physical devices to form one logical



Why device stacking?

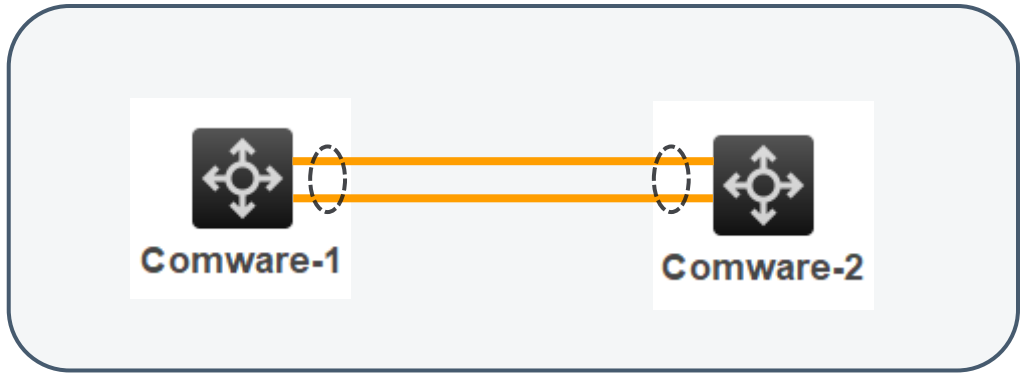
- More resilient
- Does not block ports (like STP)
- Simple management
- Simple design



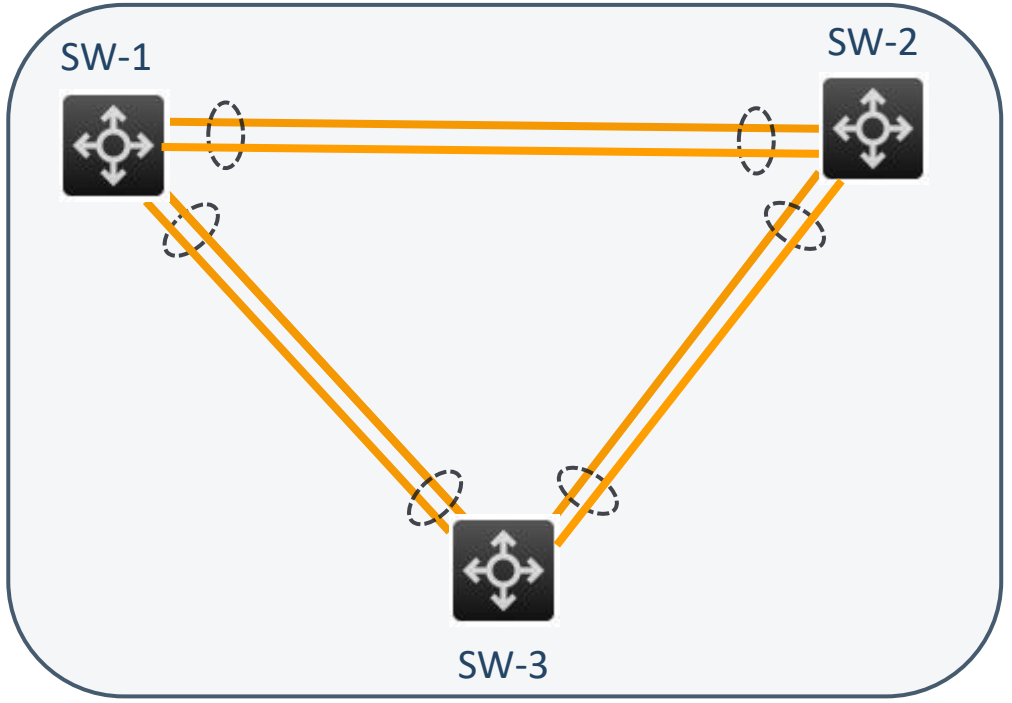
IRF topologies

Software University

Daisy chain:



Ring:



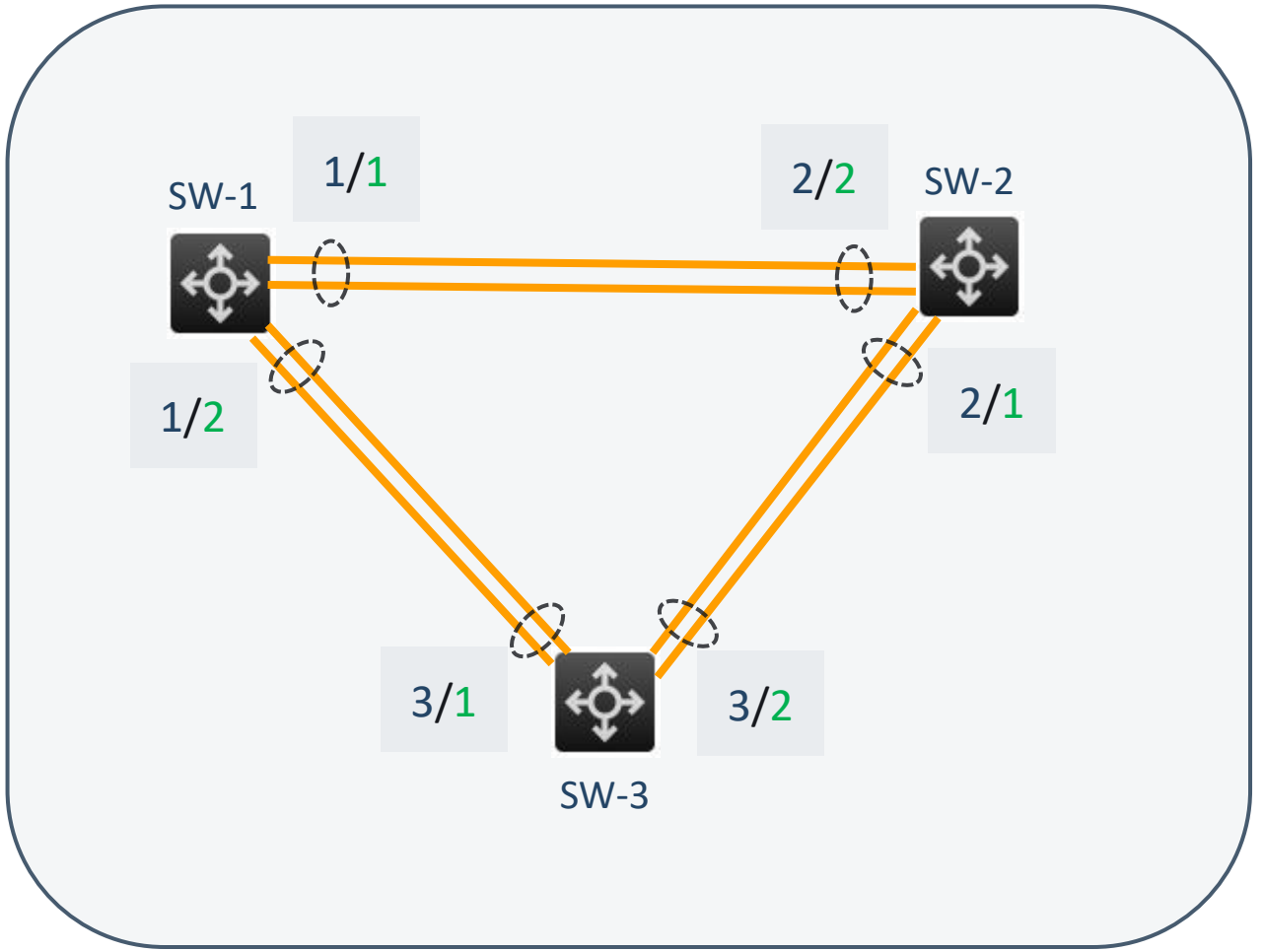
IRF ports and connections

Single physical cable
Must be at least 10Gbps

x/y IRF port – memberID/port

Only connect IRF port 1 to IRF port 2!

Possible connections	**1/1 -> 2/2**	**1/2 -> 2/1**
Not possible connections	1/1 -> 2/1	1/2 -> 2/2



Master election

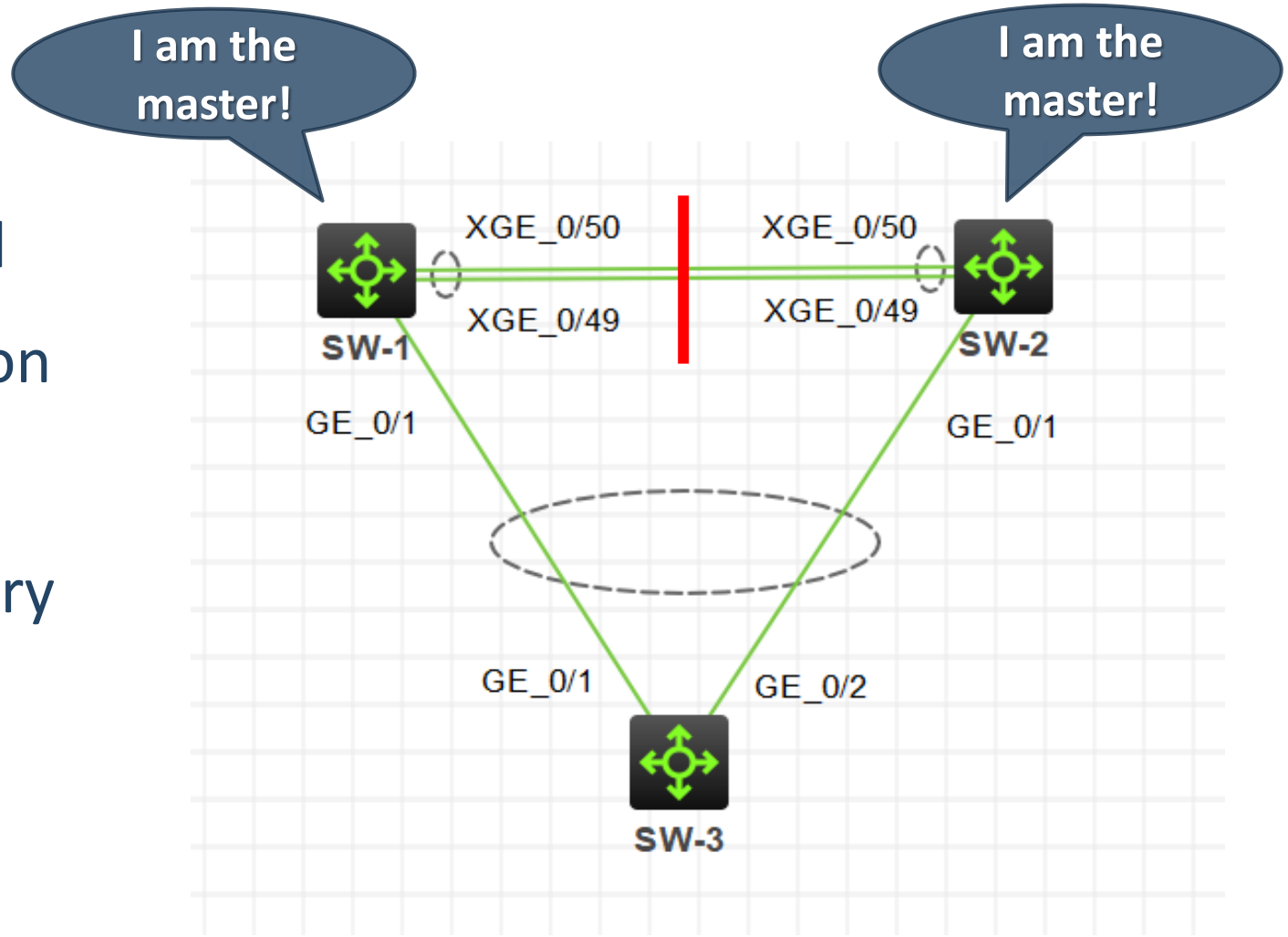
- When creating the IRF stack:
  - The member with highest priority wins
  - If no member has a higher priority, the member with the longest system up-time wins (rounded to 10 minutes)
  - If no member has a longer up-time, the member with the lowest bridge MAC address wins
- When joining another device to existing IRF stack:
  - The current master wins

IRF split stack

- When there is a split stack situation, each of the two parts assumes "I am the new master"
- This can create problems
- Additional Multi Active Detection (MAD) algorithm needs to be configured:
  - LACP MAD
  - BFD MAD
  - ARP MAD

Detect IRF split stack with LACP MAD

- Additional Comware switch is required
- Extended LACPDU are exchanged
- If split stack, MAD triggers election
- Smaller member ID wins
- The other device(s) put in recovery state (shuts down the ports)

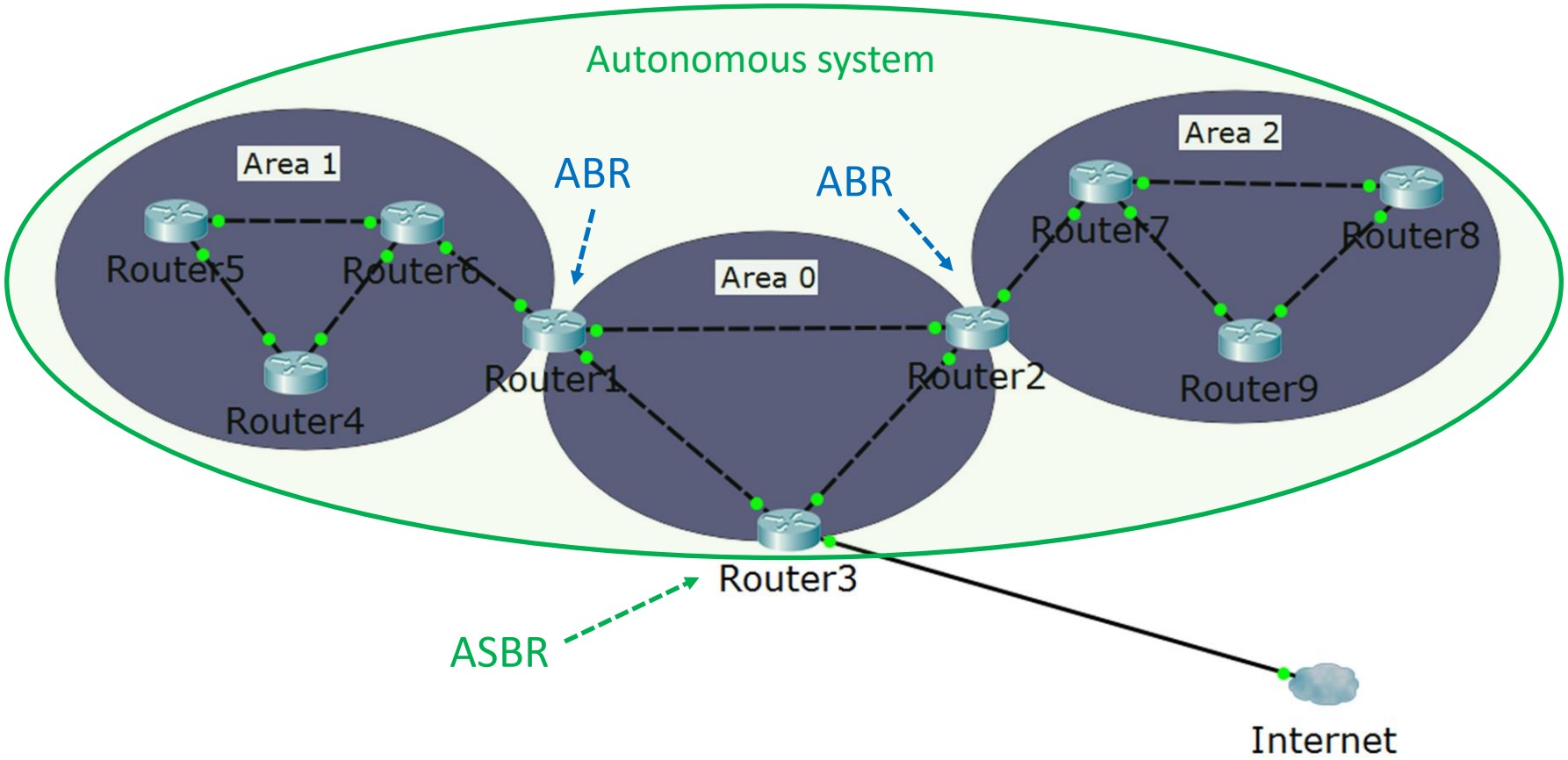


OSPF advanced - general concepts (2)

OSPF terms

- LSA – Link state advertisement
- LSDB – Link state database
- Router ID
- Area
- ABR – Area border router
- Autonomous system
- ASBR – Autonomous system boundary router

OSPF terms (2)



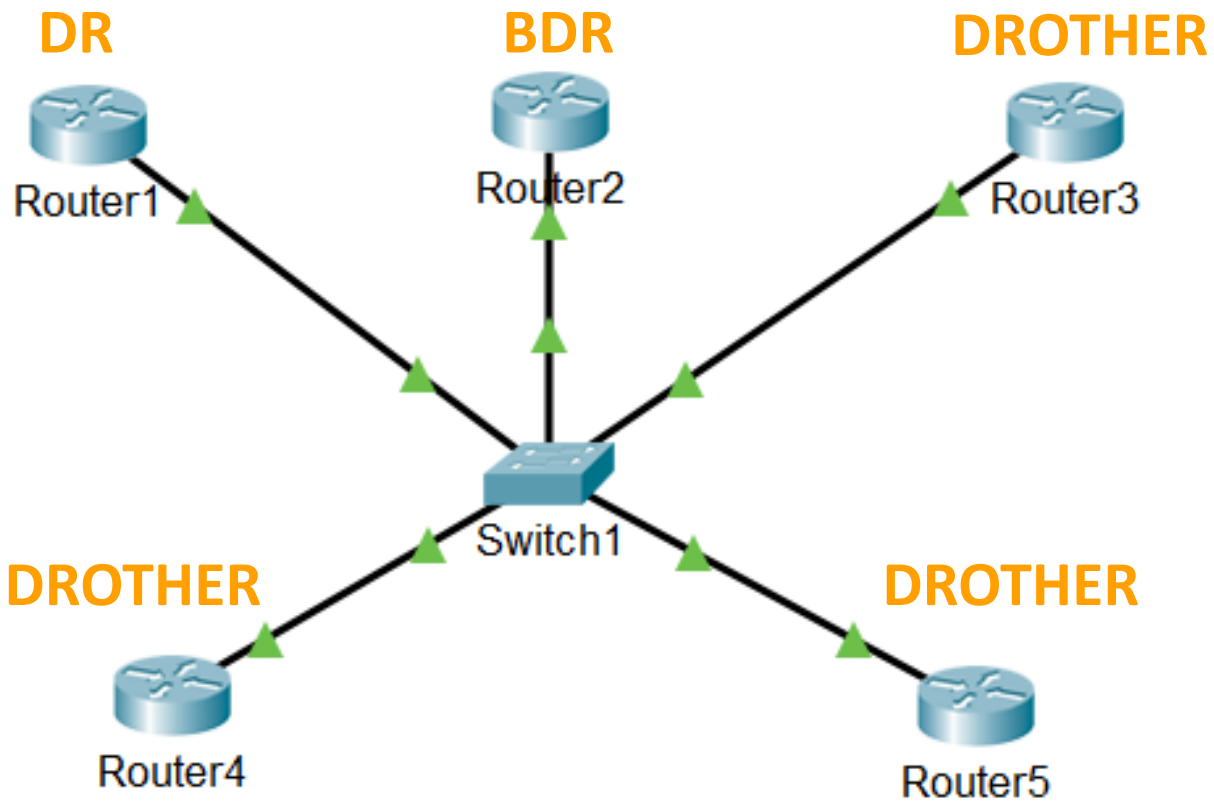
Area 0 = the backbone area

Neighbor relationships

- If multiple routers are connected to a switch, we use designated router (DR) and backup designated router (BDR)
- This minimizes LSA traffic
- Other routers are referred to as DROTHER (DR other)
- The DR and the BDR ensure that all routers receive all of the required updates

Neighbor relationships (2)

The **DR**, the **BDR** and the **DROTHER**s



DR/BDR election process

- The first router that is active on the link becomes the DR
- The second router that is active on the link becomes the BDR
- Link/interface priority is used for a re-election if the DR/BDR fails
- Default priority is 1
- Highest priority is elected; if a tie, the highest router ID (not IP address on the interface) is elected
- A priority of **0** prevents a router from becoming a DR or BDR

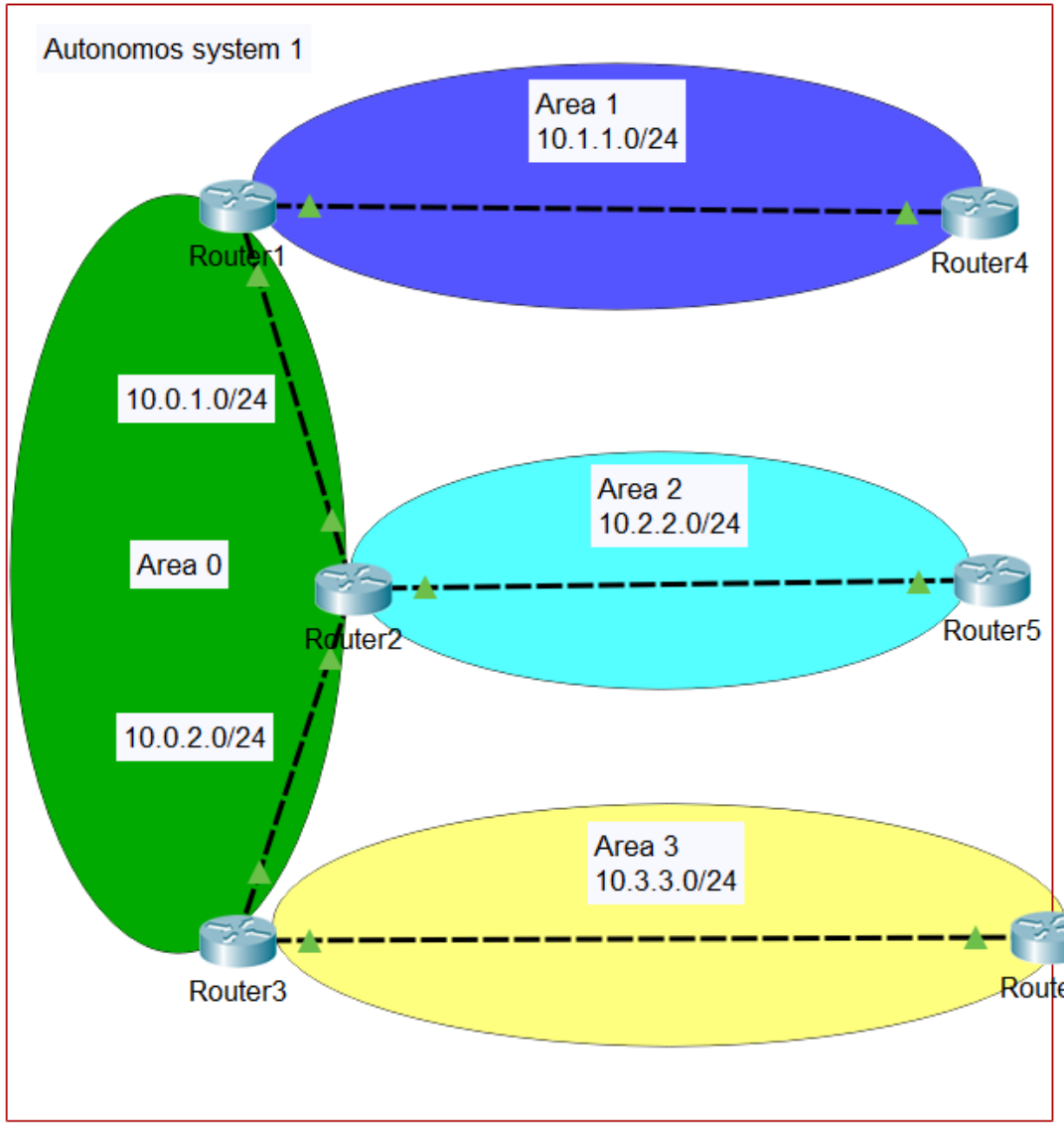
OSPF Advanced – Multi Area (2)

Why multiple areas?

Software University

- When the OSPF domain is segmented to areas:
  - Inter-area routes can be summarized
  - Router's LSDBs are not too big
  - The protocol is faster
  - Stability and control is increased

Multiple areas example

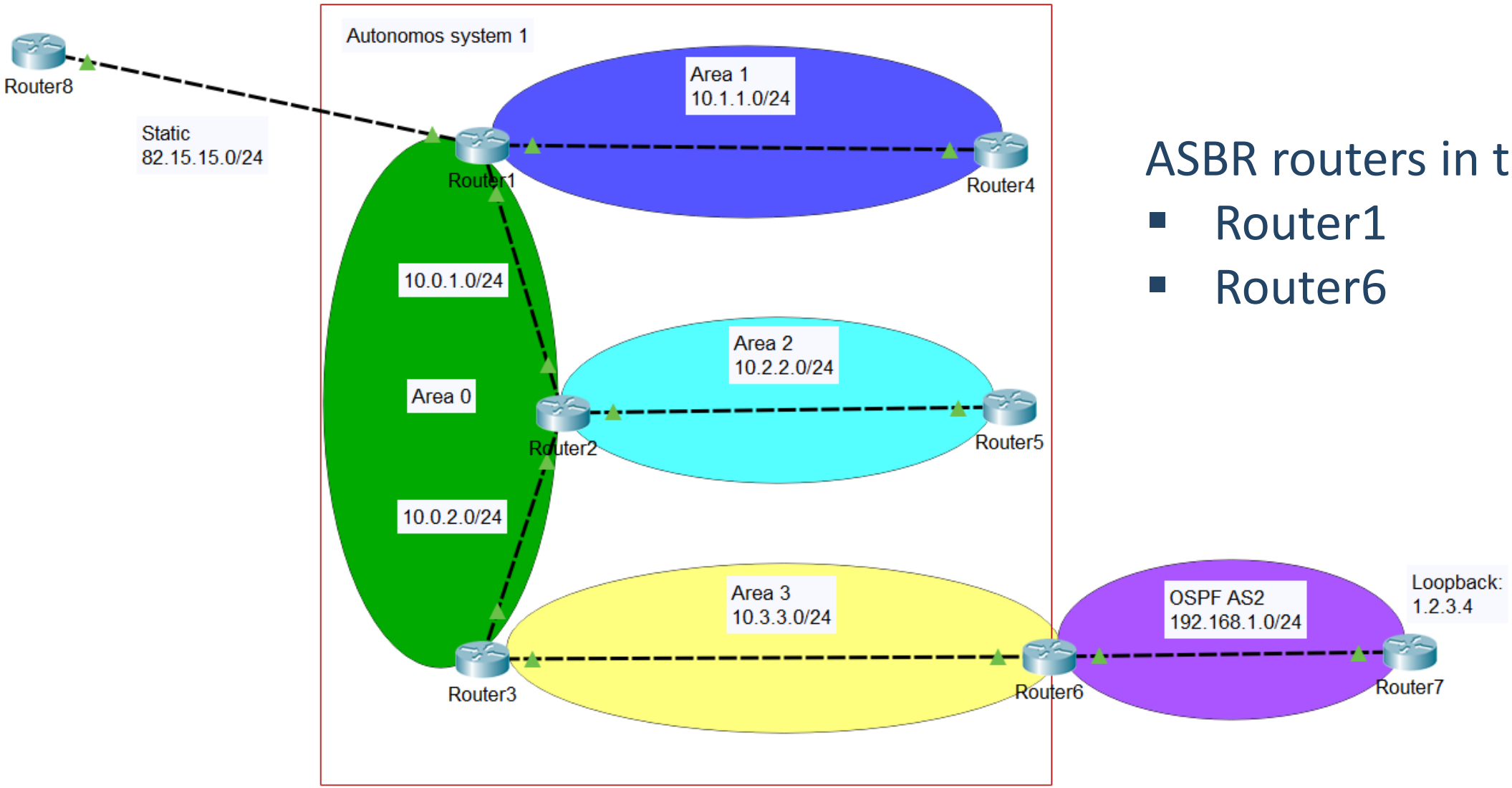


- All other areas connect to Area 0 (the backbone area)

- ABR routers in the example:
  - Router1
  - Router2
  - Router3

OSPF advanced - connect to external networks (2)

OSPF autonomous system and external networks



ASBR routers in the example:

- Router1
- Router6

Redistribute between protocols

- You need to import or redistribute routes to your AS
- Some options for redistribution:
  - **redistribute RIP**
  - **redistribute ospf [process_id]**
  - **redistribute static**
  - **redistribute connected [subnets]**

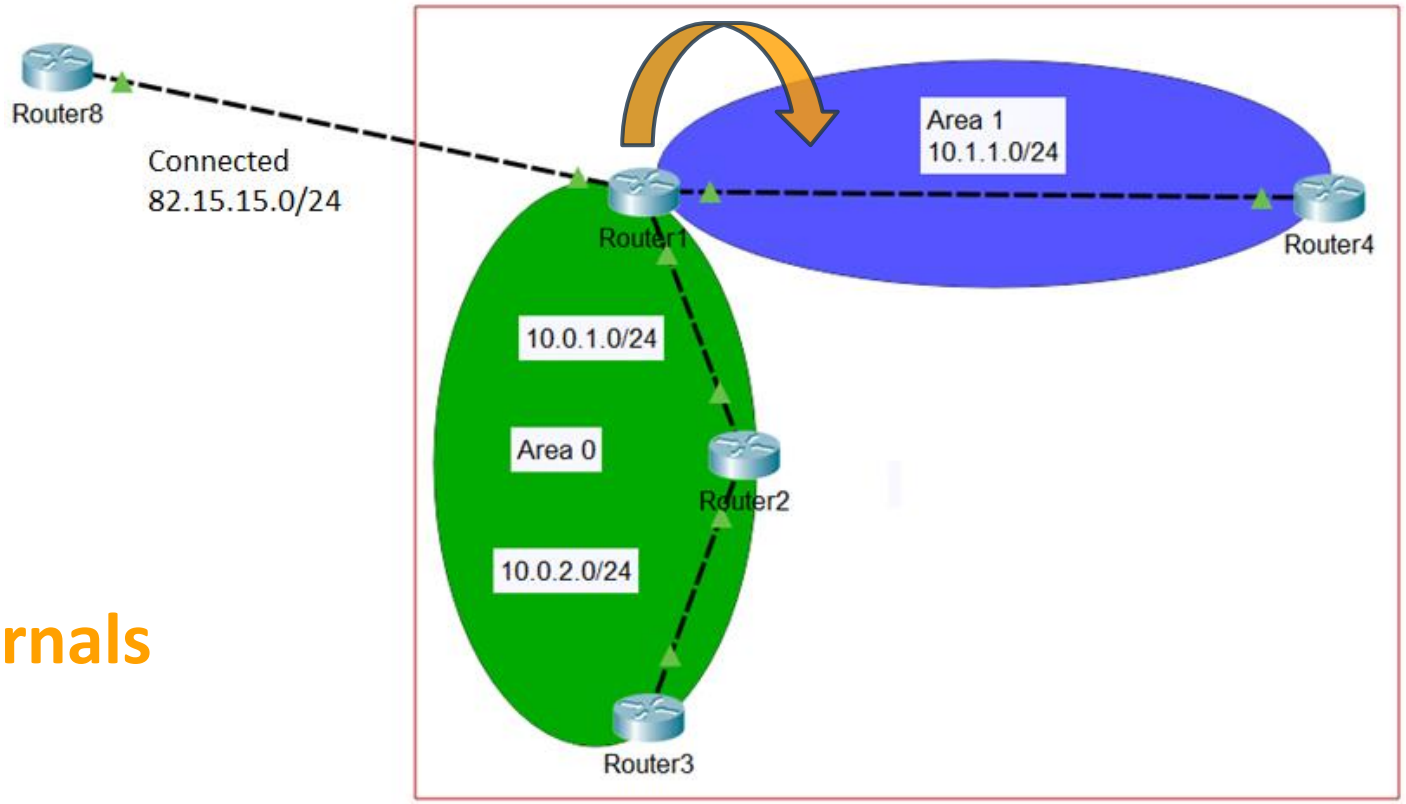
OSPF advanced – LSA and area types (2)

OSPF LSA types

- LSA type 1: Router
- LSA type 2: Network
- LSA type 3: Summary
- LSA type 4: ASBR summary
- LSA type 5: ASBR external
- ~~LSA type 6: Multicast OSPF~~
- LSA type 7: Not-so-stubby area LSA

OSPF stub area

- Uses LSA types 1, 2, 3 + default route (for external networks)
- Blocks LSA types 4 and 5



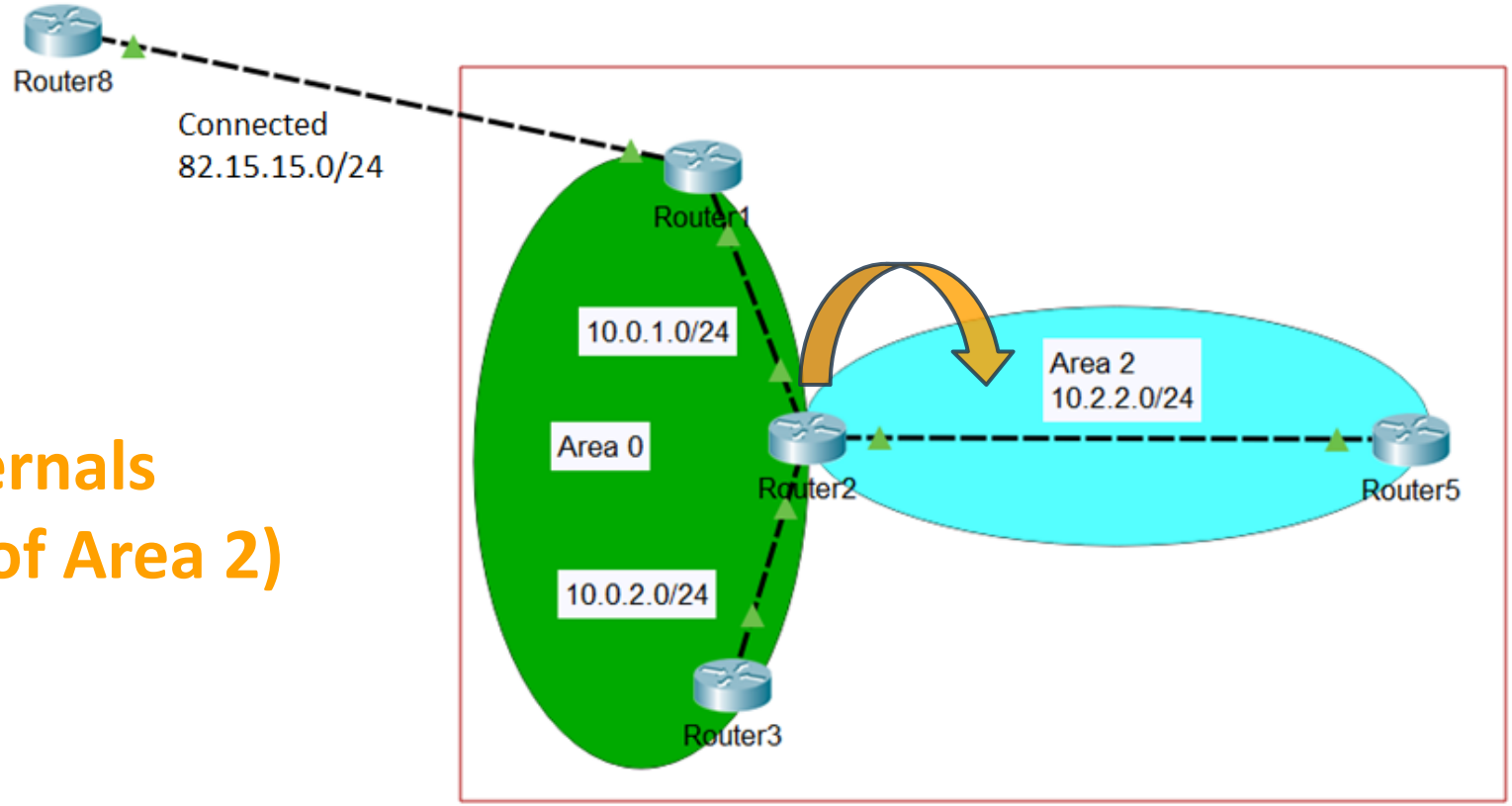
Area 1 is stub

Router1 injects:

- **Routes from area 0**
- **Default route to externals**

OSPF totally stubby area

- Uses LSA types 1 and 2 + default route (for the other areas and external networks)
- Blocks LSA types 3, 4 and 5



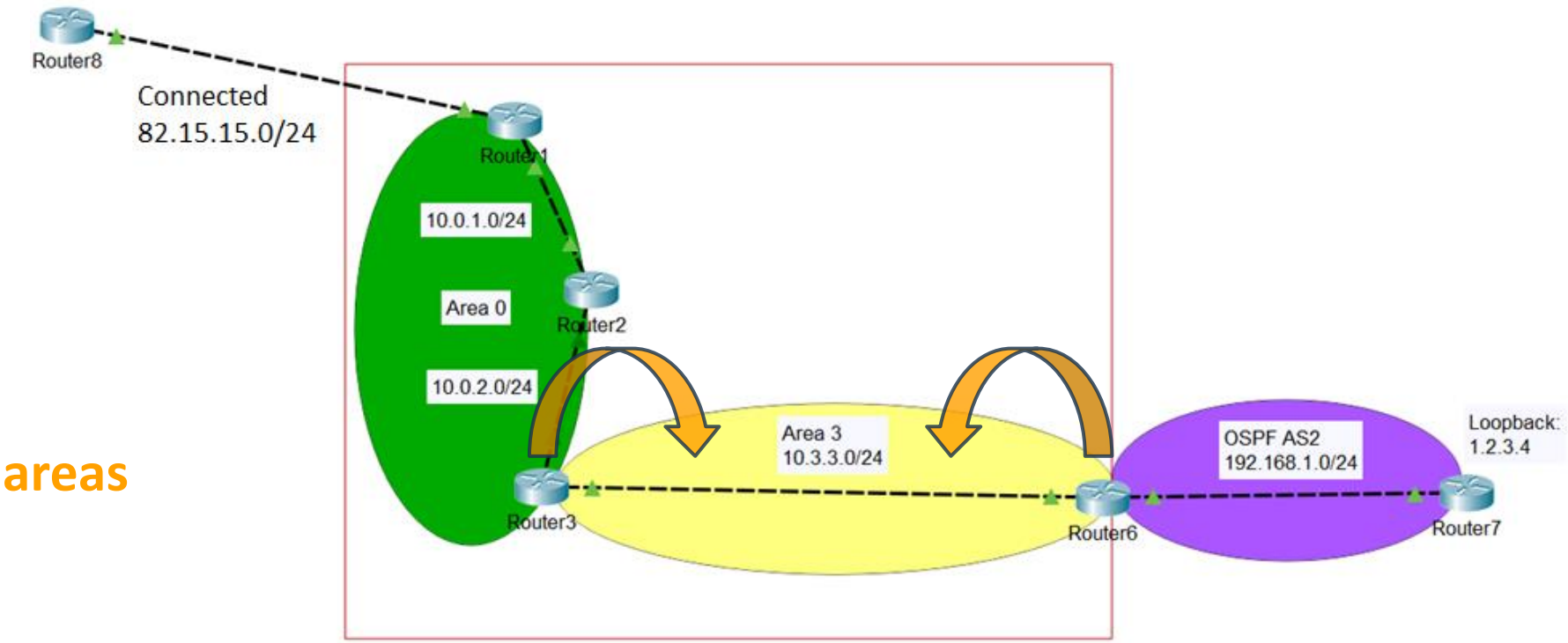
Area 2 is totally stubby

Router2 injects:

- **Default route to externals (everything outside of Area 2)**

OSPF not-so-stubby area (NSSA)

- Uses LSA types 1, 2, 3 and 7
- Blocks LSA types 4 and 5



Area 3 is NSSA

Router6 injects:

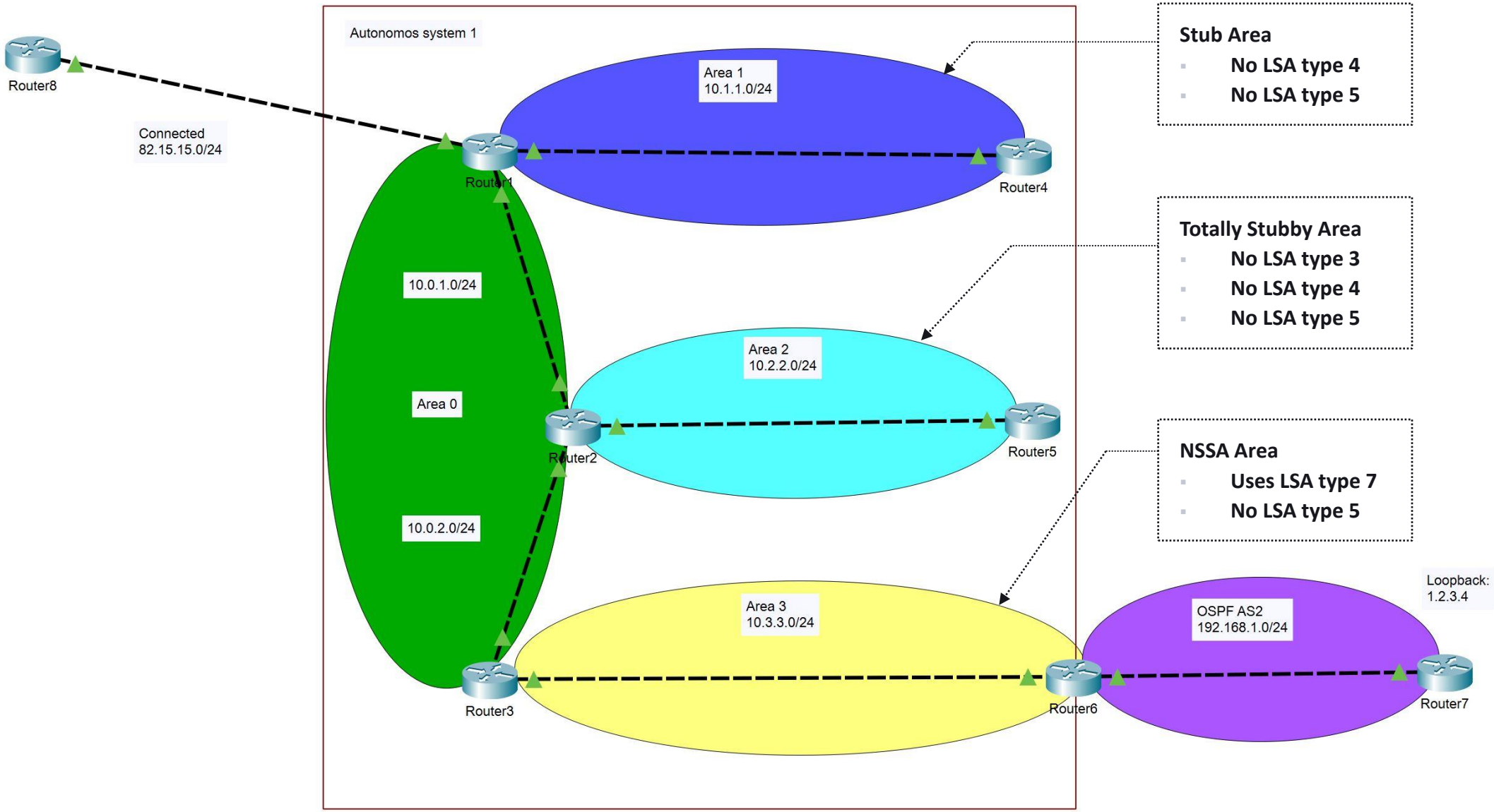
- **Routes in AS2**

Router3 injects:

- **Routes from other areas**

(Route to 82.15.15.0/24 not advertised)

Common area types and LSAs



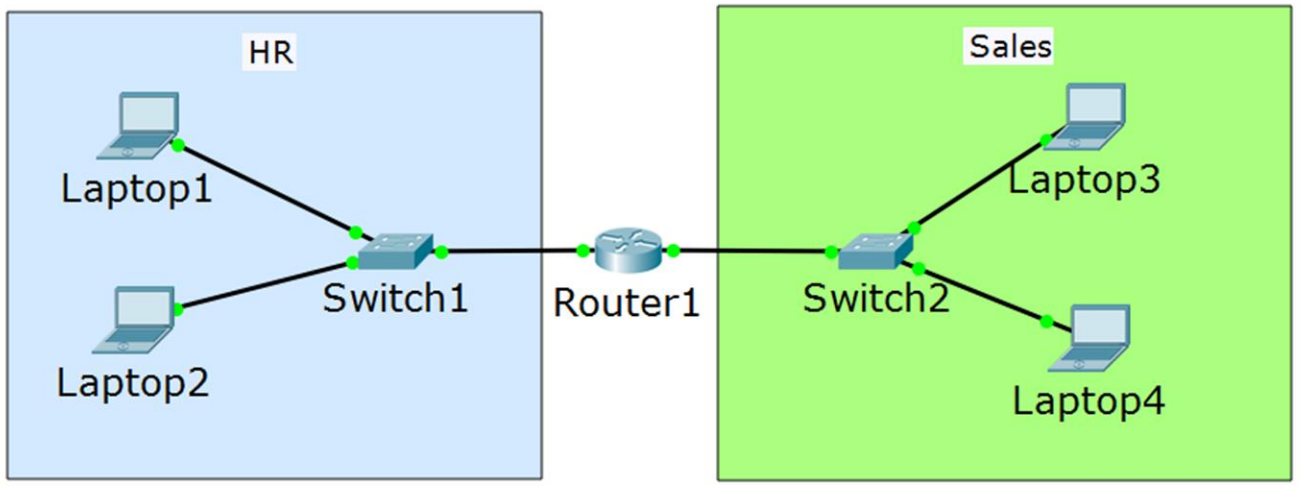
Access Control Lists – overview (3)

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?

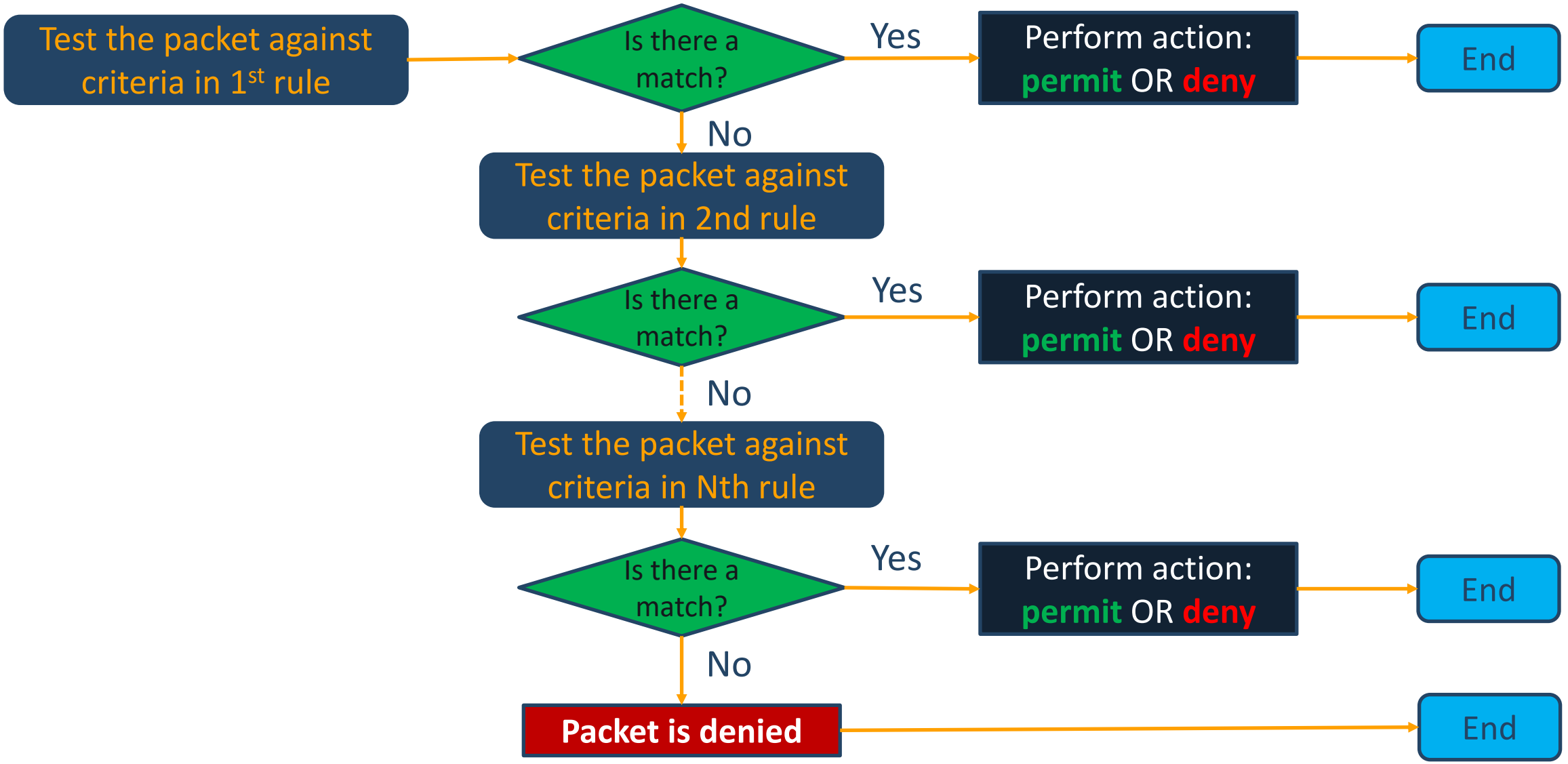
- ACLs filter the network traffic
  - Better security
  - Can increase the overall network performance
- ACLs may just select traffic for other reasons:
  - Applying QoS
  - NAT
  - Traffic mirroring



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



Access Control Lists - creating (3)

Standard ACLs configuration

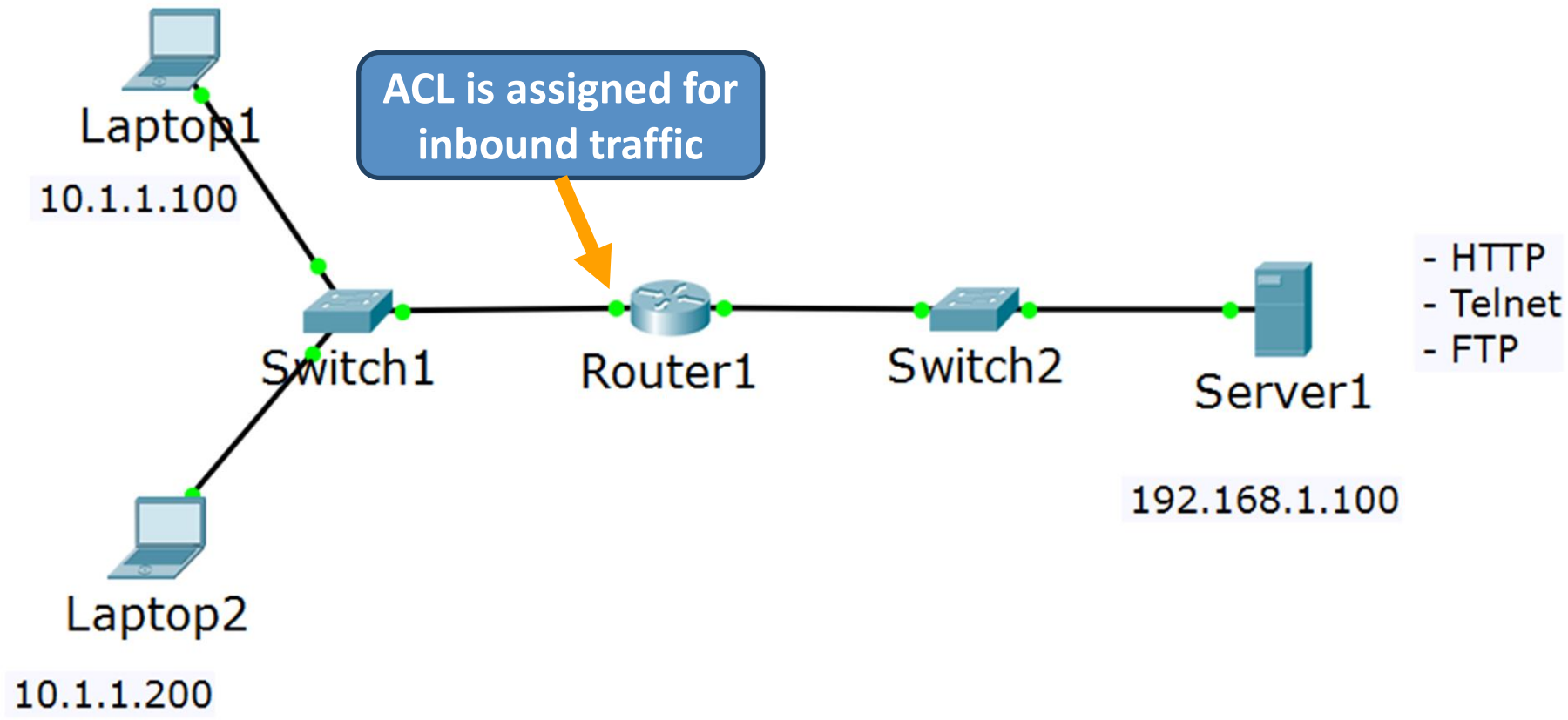
- **ip access-list standard** [<***1-99***> or ***name***]
- [**permit** or **deny**] ***network*** [wildcard mask] or **any** or **host**
- **Example: ip access-list standard test_standard**
  - **permit 192.168.1.0 0.0.0.255** (the whole 192.168.1.X network)
  - **deny host 10.1.1.1** (only the host 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!)

Extended ACLs configuration

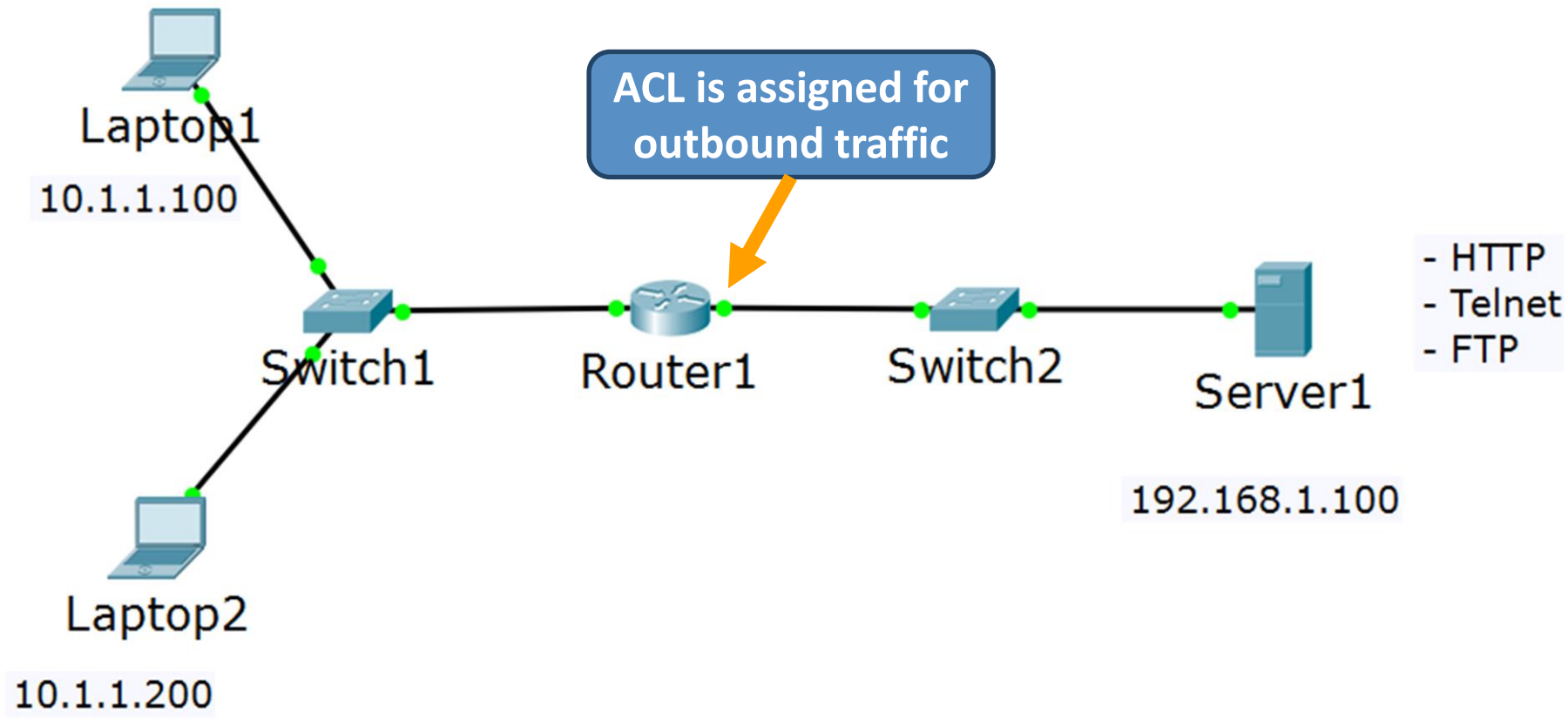
- **ip access-list extended** [<***100-199***> or ***name***]
- [**permit** or **deny**] ***protocol*** [source] ***network*** or **any** or **host** [destination] ***network*** or **any** or **host**
- **Examples: ip access-list extended test_extended**
  - **deny ip host 10.1.1.1 host 20.2.2.2**
  - **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)

Access Control Lists - assigning (3)

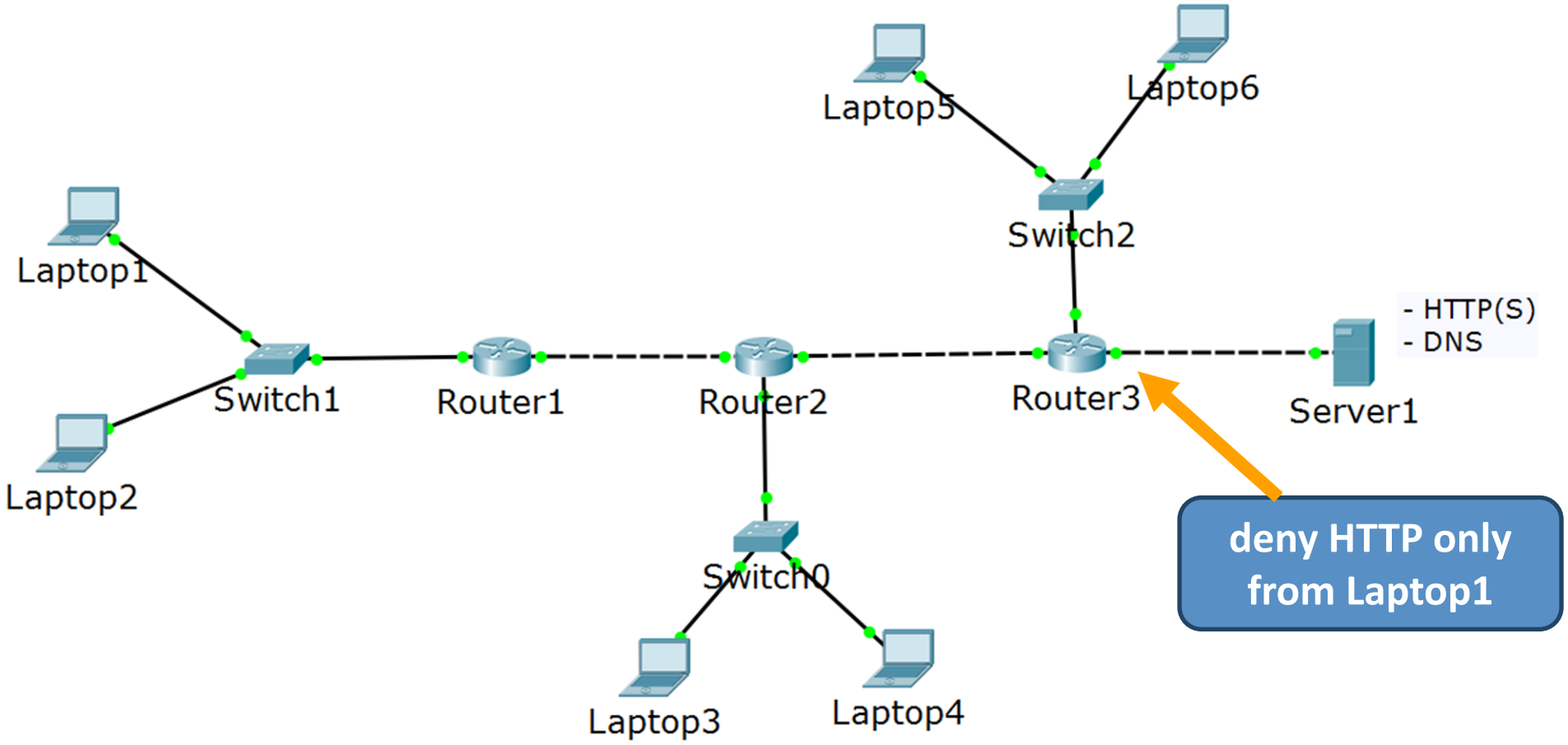
Assigning ACLs - inbound



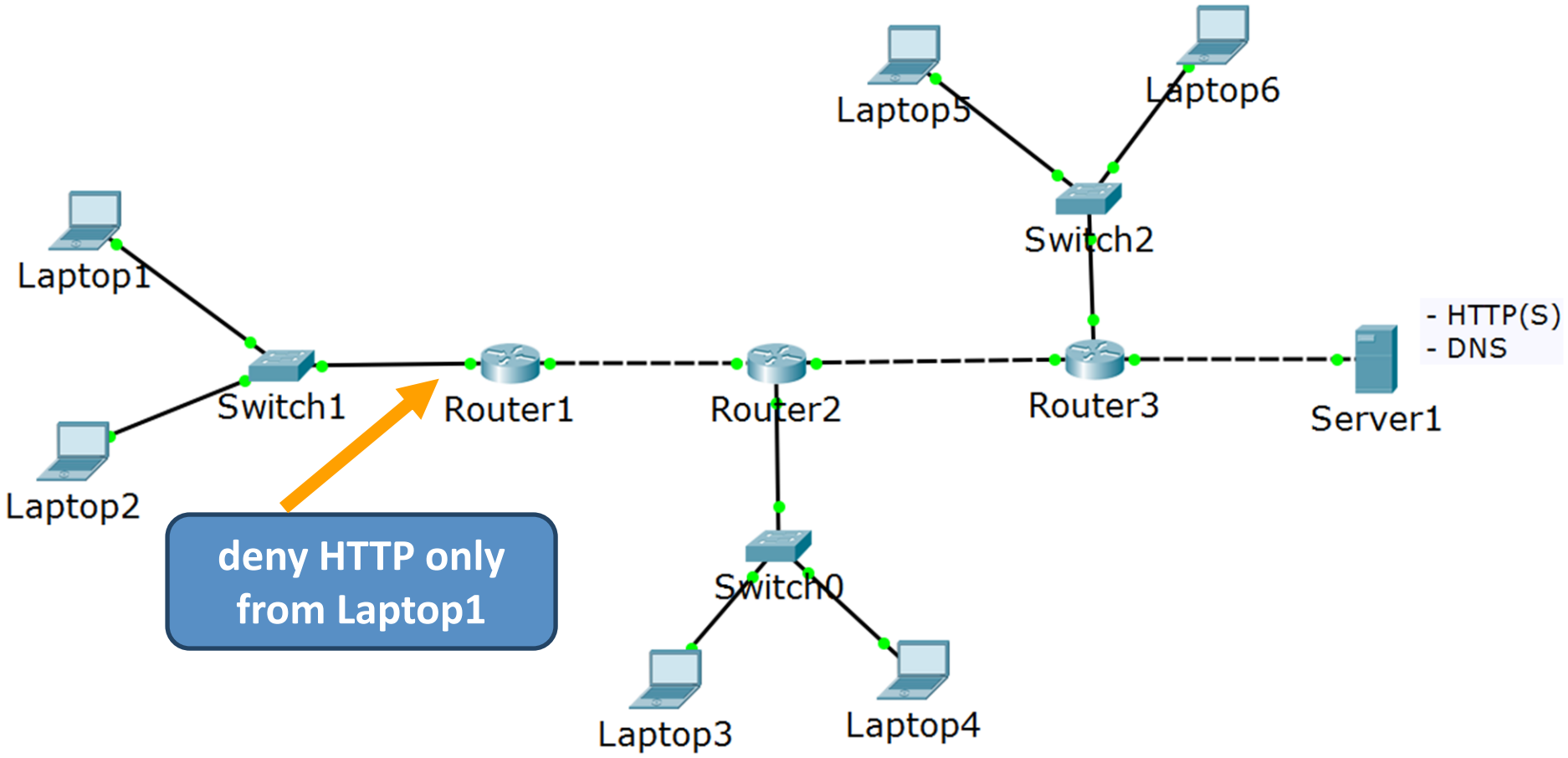
Assigning ACLs - outbound



Assigning ACLs – best practice for standard ACLs



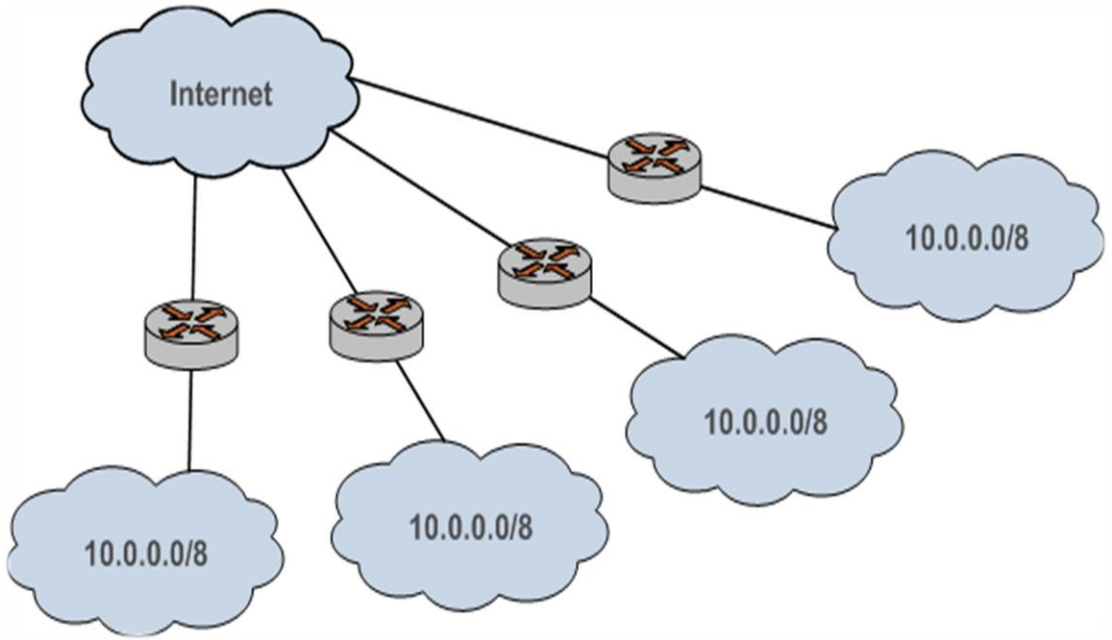
Assigning ACLs – best practice for extended ACLs



Network Address Translation (3)

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



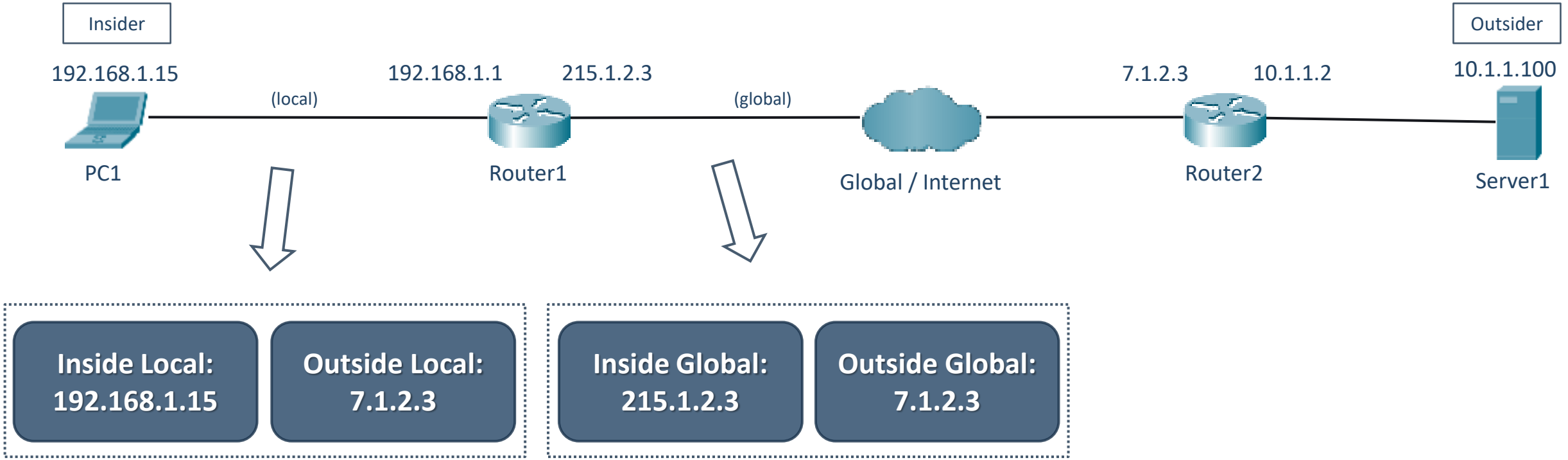
Types of NAT

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

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



- 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

Domain Name System (4)

DNS structure

- DNS is hierarchical and distributed system
- At the top there is the root domain or "."
  - One level below are the TLD (top level domains, i.e. ".com")
    - One level below are the second level domains, i.e. "yahoo"
      - Possible third level domains, etc.
- DNS Zone – part of the DNS namespace, managed by specific organization

Resource Records (in a DNS zone)

Software University

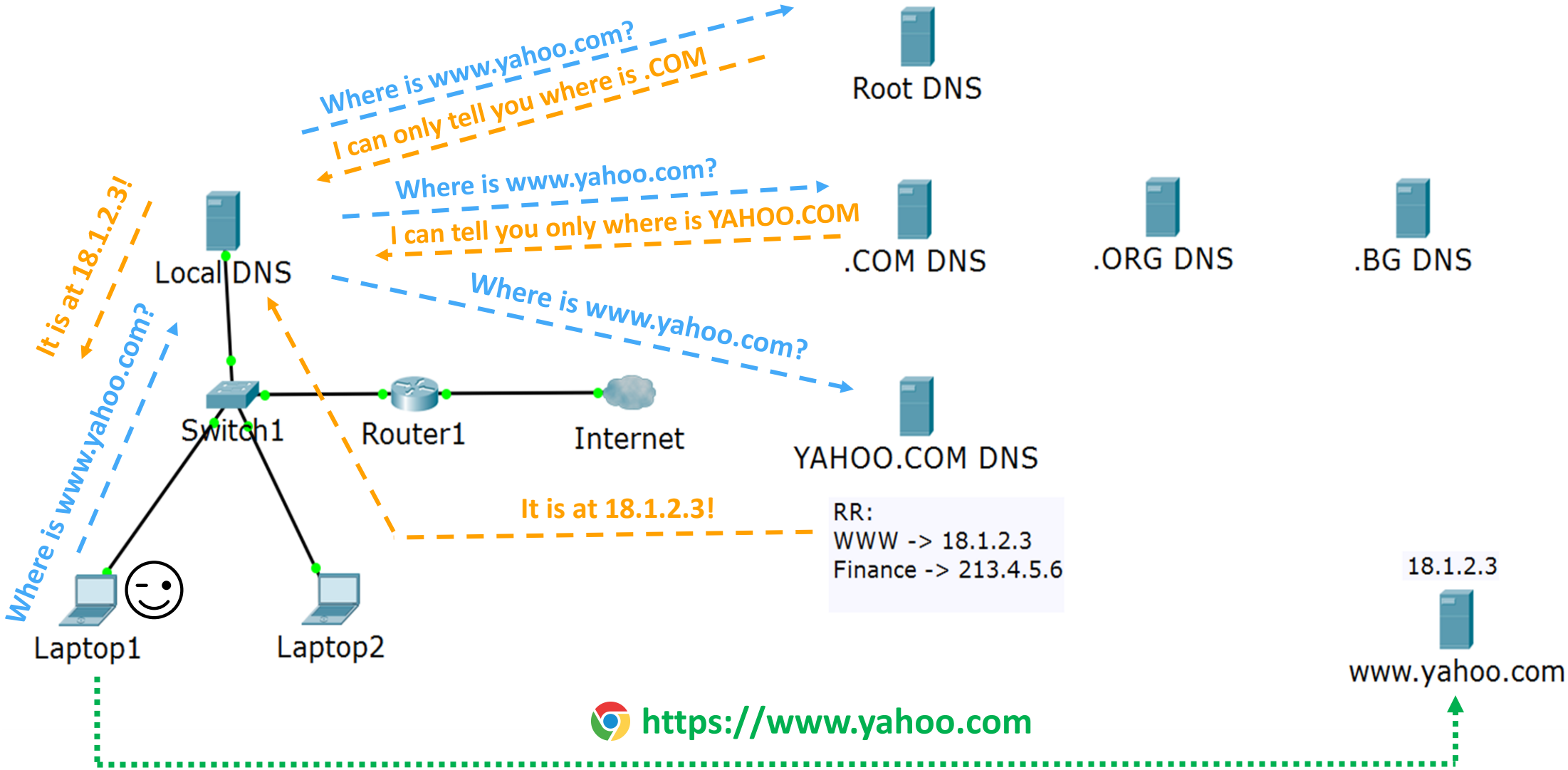
- Common resource records and their purposes:
  - **A** record: a name which points to a IPv4 address
  - **AAAA** record: a name which points to a IPv6 address
  - **CNAME** record (alias): a name which points to another name
    (Canonical Name)
  - **MX** record: shows who is the mail server for that domain
    (Mail EXchanger)
  - **TXT** record: text entry, usually used for domain verification and anti-spam
    (TeXT)
  - **NS** record: shows which are the name servers for the zone
    (Name Server)
  - **SOA** record: contains administrative information about the zone
    (Start Of Authority)

Windows client local DNS cache

Software University

- Resolved DNS queries stay in the local cache for a time period determined by the zone TTL value on the server
- The **hosts** file
  - Alternative name resolution mechanism
  - Usually located in **%systemroot%\system32\drivers\etc** folder
  - Not distributed and scalable but can serve as a backup DNS method
  - It has **higher priority** than DNS resolution
  - The content of the hosts file is constantly copied in the DNS cache

DNS query process



The NSLOOKUP command

Software University

- To check a DNS resolution, one can use **ping** or **nslookup**
  - ping - intuitive to use but can have older and inaccurate info
    the purpose of ping is not to troubleshoot DNS
  - **nslookup** - useful tool designed for troubleshooting DNS
- Demo: how to use **nslookup** on Windows

IPv6 (4)

IPv4 vs IPv6

- Much (much…) larger address space in IPv6
- A lot of the IP concepts and upper layer protocols remain the same or similar
- In the OSI model, only L3 is different
- No broadcast, no subnetting and no NAT in IPv6!

IPv6 address format

- IPv6 address is represented as eight groups of four hexadecimal digits
- Example:

  2001:0db8:0000:0000:0000:ff00:0042:8132

- Each of this groups has 16 bits and is separated from the others with ":"

Abbreviations

- One option - remove the long string with zeros (allowed only once)
  - Original: 2041:0000:140F:0000:0000:0000:875B:031B
  - Short: 2041:0000:140F::875B:031B
- Another option - replace four zeros with one
  - Short: 2041:0000:140F::875B:031B
  - Shorter: 2041:0:140F::875B:031B
- Also, another leading zero can be removed: 031B --> 31B
- The result from the above options:
  2041:0000:140F:0000:0000:0000:875B:031B --> 2041:0:140F::875B:31B

Abbreviations - other examples

Software University

- FF02:0000:0000:0000:0000:0000:0000:0001
  - FF02:0:0:0:0:0:0:1
  - FF02::0:0:0:1
  - FF02:0:0::1
  - FF02::1
- 1234:0000:0000:5678:0000:0000:4321:001
  - 1234::5678:0:0:4321:1
  - 1234:0:0:5678::4321:1
- 0000:0000:0000:0000:0000:0000:0000:0001 (the loopback address)
  - ::1

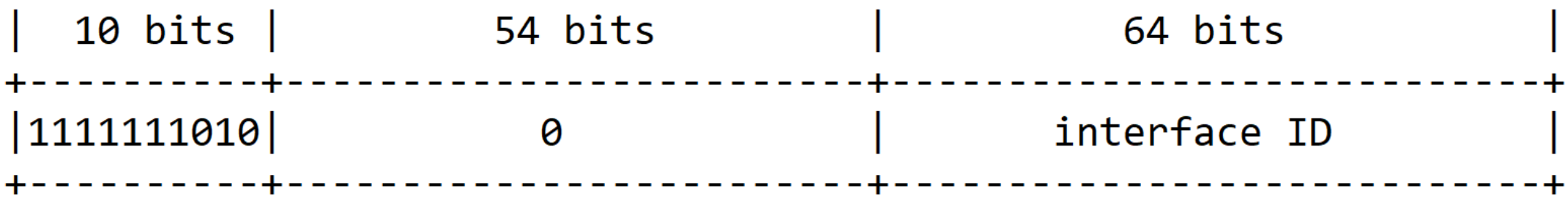
IPv6 address types

- Unicast - a packet is delivered to one interface
  - Global
  - Reserved
  - Link local (something like APIPA in IPv4)
  - Site local (something like the RFC 1918 private addresses in IPv4, deprecated)
- Multicast - a packet is delivered to multiple interfaces
- Anycast - a packet is delivered to the nearest of multiple interfaces (as defined by the routing protocols in use)

*no more Broadcast in IPv6

IPv6 scopes (unicast)

- Link-local (similar to APIPA in IPv4)
  - Prefix is FE80::/10 ...(or FE80::/64?)

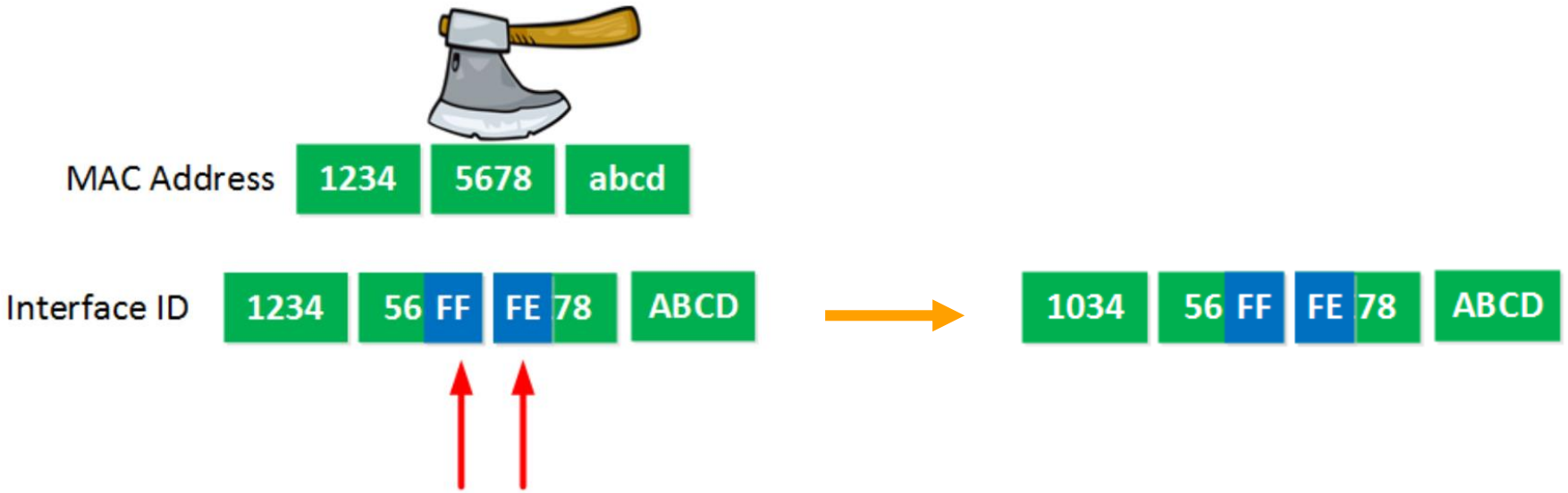


- Global (similar to IPv4 public addresses)
  - Typical prefix is 2000::/3

::1/128 - the loopback address is a unicast localhost address

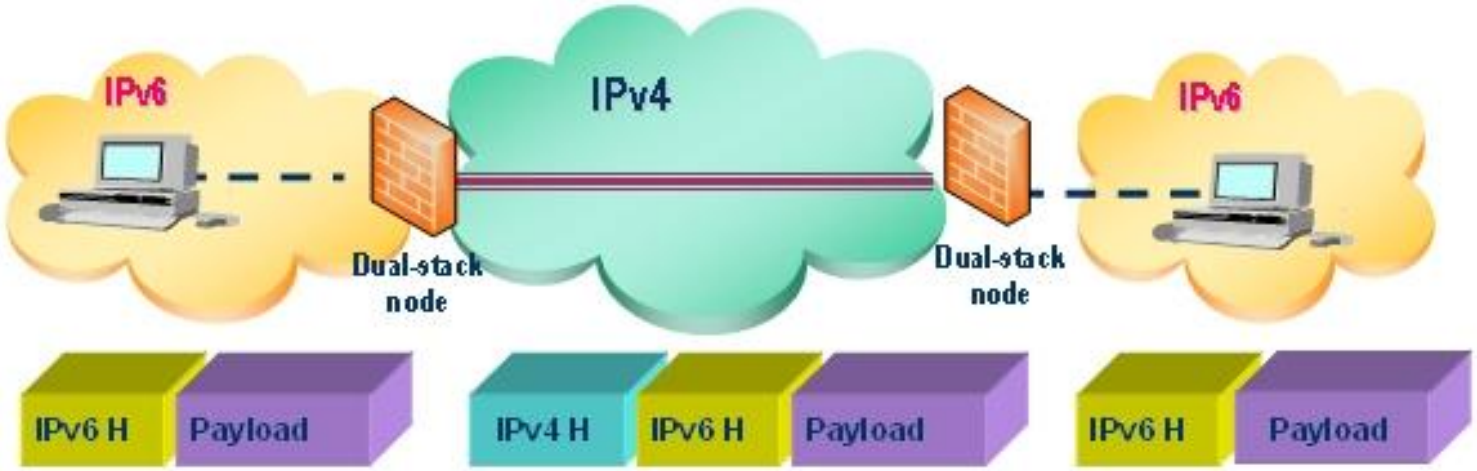
IPv6 EUI-64 bit address (2)

- How the IPv6 EUI-64 address is automatically configured:
  - ✓ Split the MAC address of the interface into two pieces
  - ✓ Insert **FFEE** between the two pieces (to achieve 64 bits)
  - ✓ Invert the 7th bit of the interface ID



IPv6 tunneling

- Encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure
- Different methods exist – 6to4, 6rd, Teredo, ISATAP, etc.



IPv6 SLAAC

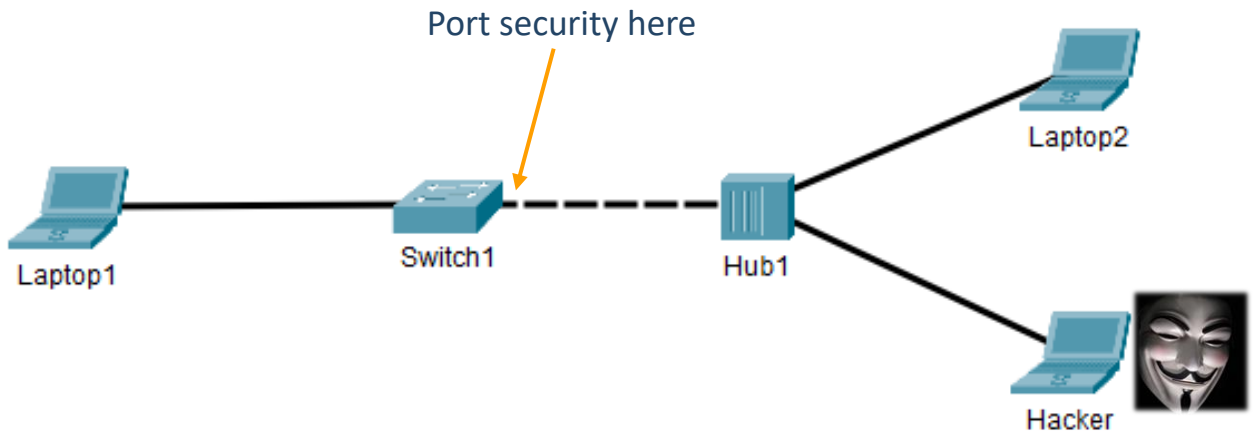
Software University

- SLAAC = StateLess Address Auto Configuration
- Designed to be fast and easy alternative to DHCPv6
- IPv6 Neighbor Discovery Protocol (NDP) is like ARP in IPv4
- With SLAAC and NDP, nodes on the network can easily autoconfigure IPv6 address from the correct subnet/prefix
- The problem: with SLAAC there is no assignment for DNS
- SLAAC and DHCPv6 can be used together:
  - the M flag (Managed) specifies if DHCPv6 is needed for IPv6 address
  - the O flag (Other) specifies if DHCPv6 is needed for DNS information

Port security (5)

What is port security?

- Without port security, any device can connect to any port in the network
- With port security, the switch looks at the source MAC address of the received frames



Note: This is not a user authentication (802.1X, discussed later in the course)

Configuration options

- Static
  - Manually configure the allowed MAC addresses on a port
  - Better control, but requires manual configuration
- Dynamic learning
  - Specify a number of allowed MAC address on a port (let's say "n")
  - Only the first "n" dynamically learned MAC addresses are allowed
  - When the switch is rebooted, the learning process starts over! (not in the config)
- Combination of static and dynamic learning
  - Specify a number of allowed MAC address on a port, let's say 5
  - Manually configure only some of them, let's say 2
  - The other 3 MAC addresses will be dynamically learned

Violation actions

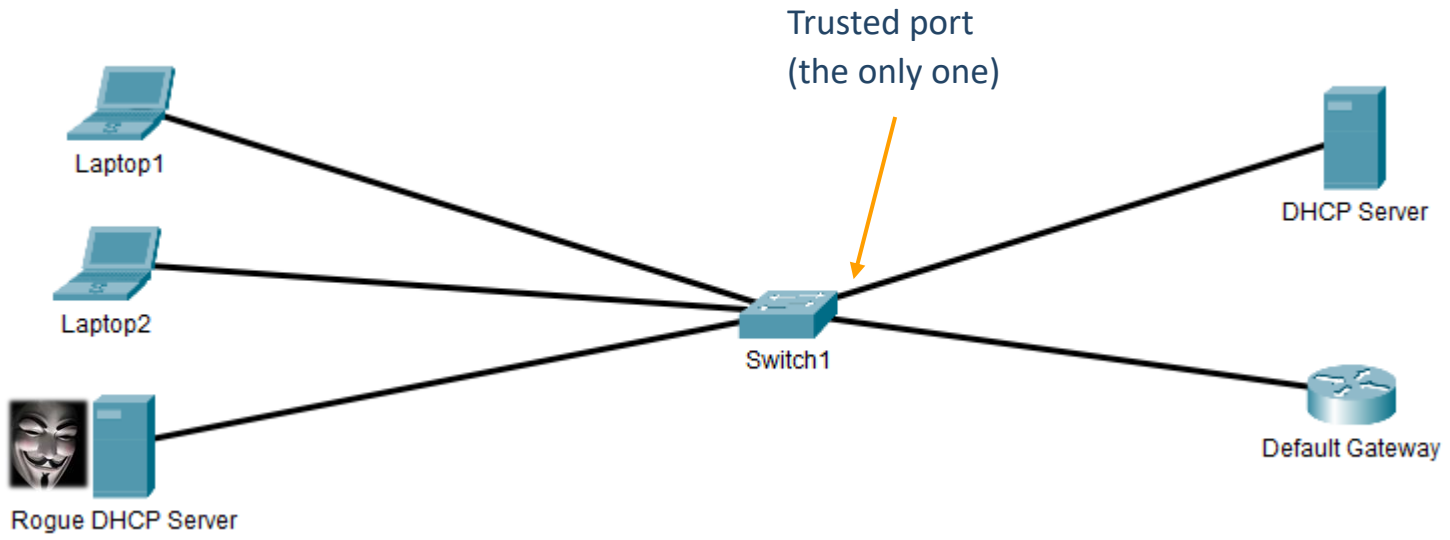
- What happens when a device with not allowed MAC address tries to access the switch port?
  - **Protect** - drops packets with unknown source MAC when the allowed maximum is reached
  - **Restrict** - same as Protect + logging (counters will increment)
  - **Shutdown** (default) - puts the port into Error disable mode and sends SNMP trap notification

```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

DHCP snooping (5)

What is DHCP snooping?

- Without DHCP snooping, anyone can act as a DHCP server in the segment (VLAN), intentionally or not
- This can lead to security problems (point users to a wrong DNS or gateway, for example) or simply Denial Of Service
- DHCP snooping does not allow server messages on “untrusted” ports



Trusted and untrusted ports

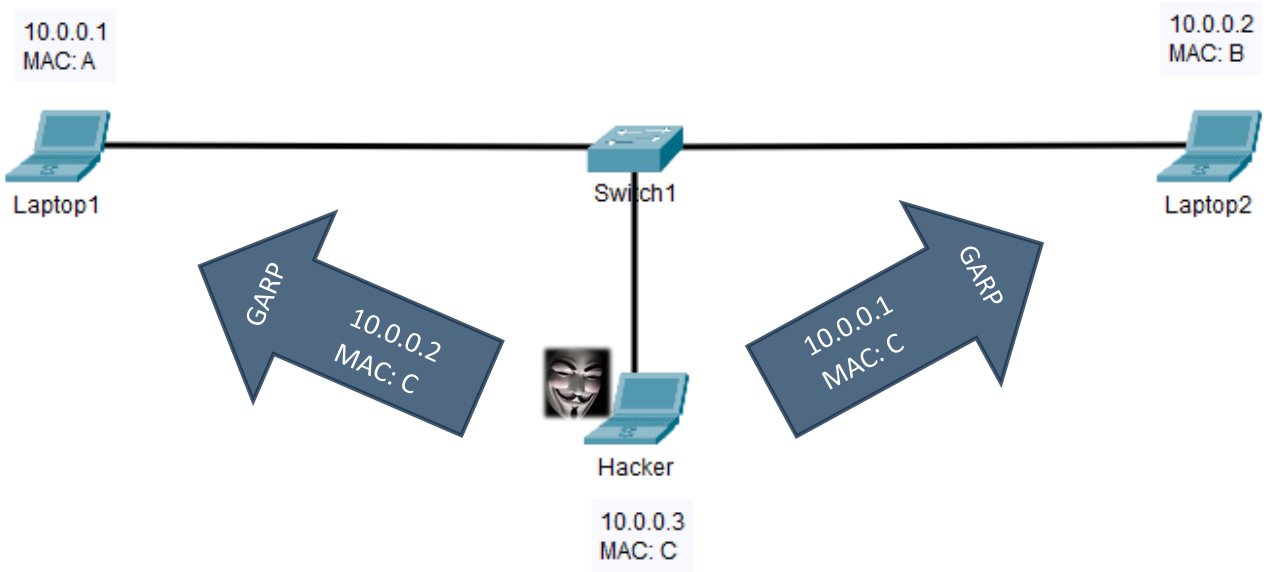
- When DHCP snooping is enabled, all ports by default are “untrusted”
- DHCP “offer” and “acknowledge” messages are not allowed on untrusted ports
- The port going to the **real** DHCP server should be configured as trusted

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted    Rate limit (pps)
-----------------------  -------    ----------------
FastEthernet0/4          no         unlimited
FastEthernet0/24         yes        unlimited
FastEthernet0/1          no         unlimited
FastEthernet0/2          no         unlimited
```

Dynamic ARP inspection (5)

What is dynamic ARP inspection?

- Without dynamic ARP inspection (DAI), a malicious user can insert himself between the communicating devices and perform “man in the middle” attacks
- An attacker can poison the ARP cache tables of the hosts with gratuitous ARP
- The result: traffic between the laptops goes through the “Hacker” device



What is dynamic ARP inspection (2)?

Software University

- With dynamic ARP inspection (DAI), the switch will check the MAC-to-IP entries in the ARP messages and verify if they are correct
- How does the switch verify these entries:
  - Via DHCP snooping (1)
  - Via manually created access list (2)

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type            VLAN  Interface
------------------  ---------------  ----------  --------------  ----  --------------------
00:0D:BD:56:20:00   10.1.1.3         86400       dhcp-snooping   1     FastEthernet0/1
22:22:22:22:22:22   10.1.1.1         86400       dhcp-snooping   1     FastEthernet0/2
Total number of bindings: 2
```

(1)

```
Switch#show arp access-list
ARP access list List1
    permit ip 1.2.3.4 0.0.0.255 mac host 2222.2222.2222
    permit response ip host 4.3.2.1 any mac any any
```

(2)

Authentication with 802.1X (6)

Who can connect to the network?

- By default, anyone with physical access can connect to our wired network
- Two common protection mechanisms:
  - Port security - simple authentication based on MAC addresses
    - Only frames from specific MAC addresses are allowed
    - Limited number of MAC addresses are permitted
  - User authentication with 802.1X

AAA

- AAA: Authentication, Authorization and Accounting
  - **Authentication** – "Who are you? Prove it!"
  - **Authorization** – "This is where you have access and where you do not"
  - **Accounting** – "I am recording all (un)successful login attempts"
- Often a single server plays the three roles but can be multiple servers as well

Why 802.1X?

- The switches and access points do not need to know how to authenticate the client
- They (authenticators) simply pass the authentication information between the client and the authentication server
- That is why it is easier for 802.1X to support many authentication methods

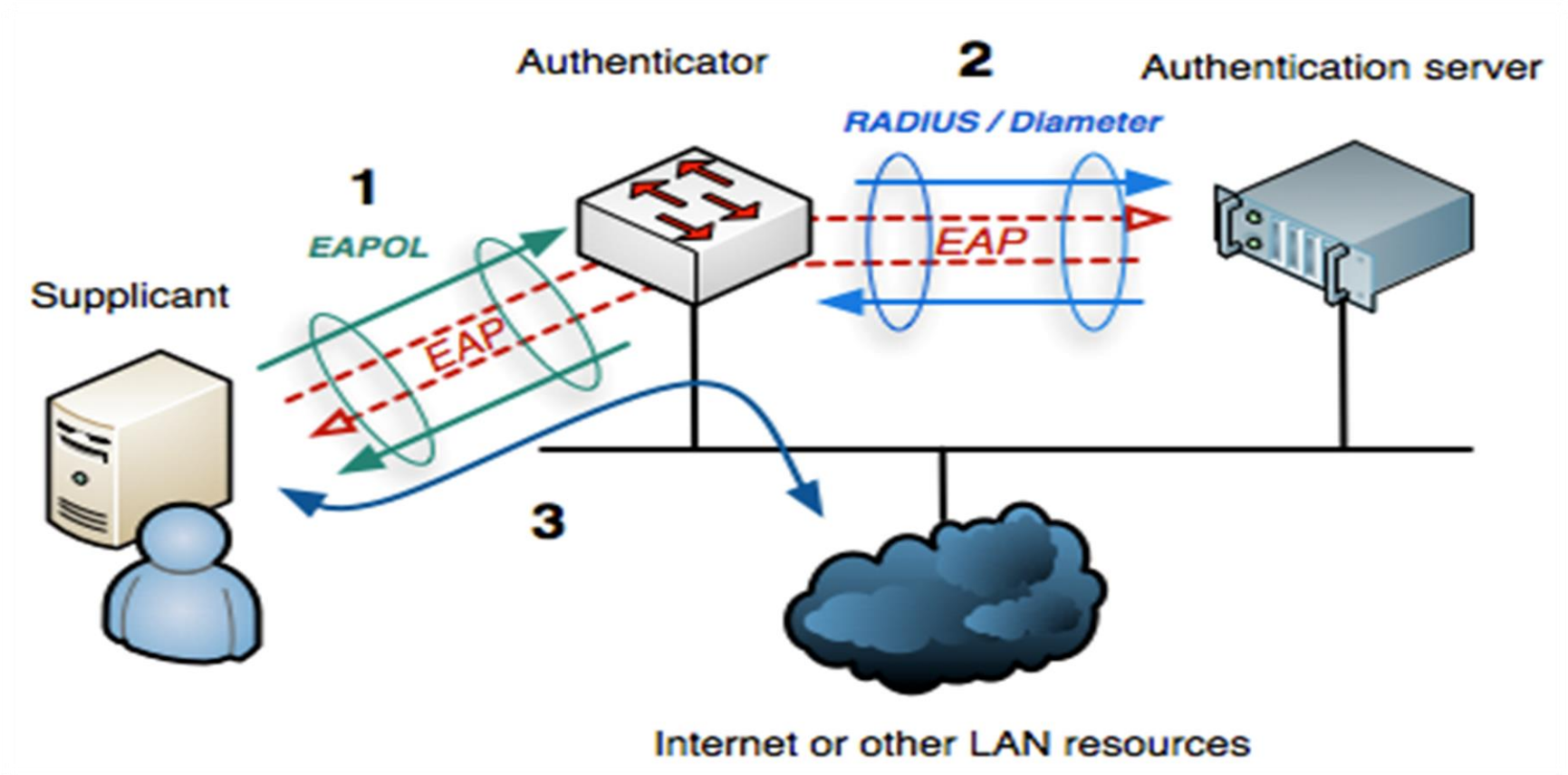
802.1X

- IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC)
- Part of the IEEE 802.1 group of networking protocols
- Provides authentication mechanism to devices asking to attach to a LAN or a WLAN
- Uses Extensible Authentication Protocol (EAP) over LAN – known as EAPOL

The participants in 802.1X

1. **Supplicant** - the end device requesting access
2. **Authenticator** – usually a switch or AP which is to provide access
3. **Authentication Server** - the device which makes the decision (grant/deny access). Usually, RADIUS server

802.1X


Authenticator
2
Authentication server
RADIUS / Diameter
1
EAPOL
EAP
Supplicant
EAP
3
Internet or other LAN resources

802.1X and EAP

Software University

- 802.1x uses EAP to facilitate the communications between the participants
- Common EAP authentication types:
  - **EAP-MD5** - minimal security, one-way authentication
  - **EAP-TLS** - mutual authentication, secure but no very easy to adopt
  - **EAP-TTLS** - mutual authentication (optional client certificate)
  - **EAP-PEAP** - most popular method, has an "outer" and "inner" methods, developed by Cisco, Microsoft and RSA Security

Wireless Networking Concepts (6)

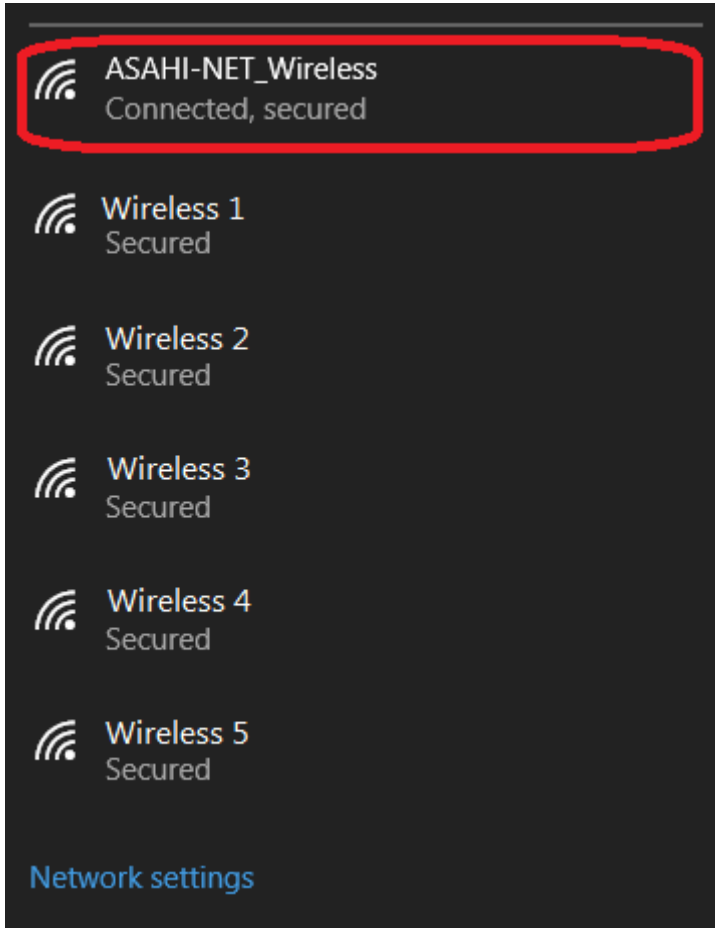
Some 802.11 standards

Software University

IEEE Standard	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Friendly name	WiFi 1	WiFi 2	WiFi 3	WiFi 4	WiFi 5	WiFi 6
Year adopted	1999	1999	2003	2009	2014	2019
Frequency	2.4 Ghz	5 Ghz	2.4 Ghz	2.4/5 Ghz	5 Ghz	2.4/5 Ghz
Max data rate	11 Mbps	54 Mbps	54 Mbps	450 Mbps	1.7 Gbps	2.4 Gbps
Typical range indoors*	35 m	35 m	38 m	70 m	35 m	-
Typical range outdoors*	140 m	120 m	140 m	250 m	250 m	250 m

SSID

- SSID: Service Set Identifier
- This is the name of the wireless network (not the Access Point name)
- It is up to 32 characters in length
- A single AP can broadcast multiple SSIDs
- Should you hide your SSID?



Wireless security

- Hiding the SSID ("not the best" security)
- MAC ID filtering
- Static client IP addressing
- 802.11 security (next slide)

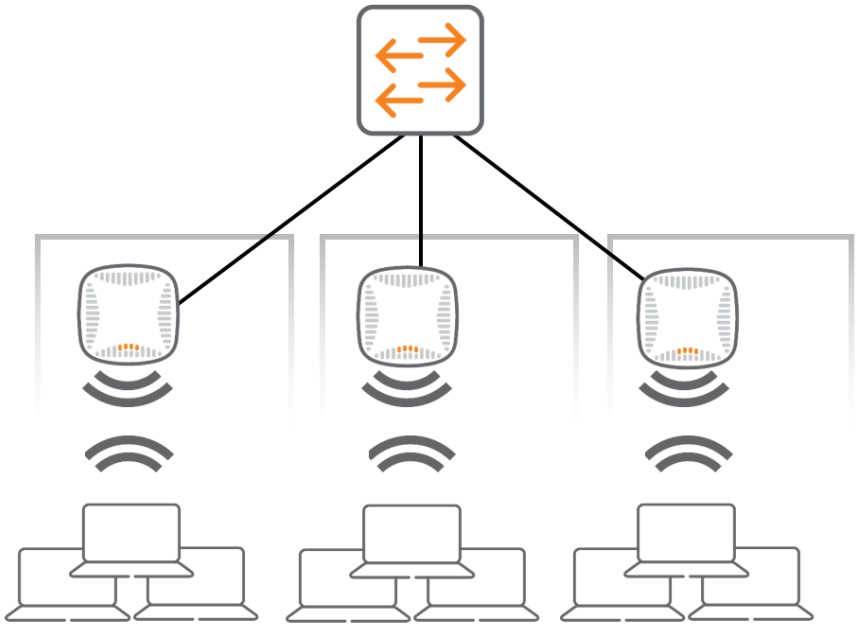
802.11 security

- **WEP** - very weak, deprecated
- **WPA** - better than WEP, still risky
- **WPA2** - the de facto standard
  - WPA2 (TKIP) - risky
  - WPA2 (AES)
  - WPA2-PSK vs WPA2-Enterprise (which uses EAP)
- **WPA3** - improved general Wi-Fi encryption
  - WPA3 - personal
    (uses Simultaneous Authentication of Equals (SAE) vs PSK)
  - WPA3 - enterprise
    (targets large-scale Wi-Fi with optional 192-bit security)

Wireless Devices Management

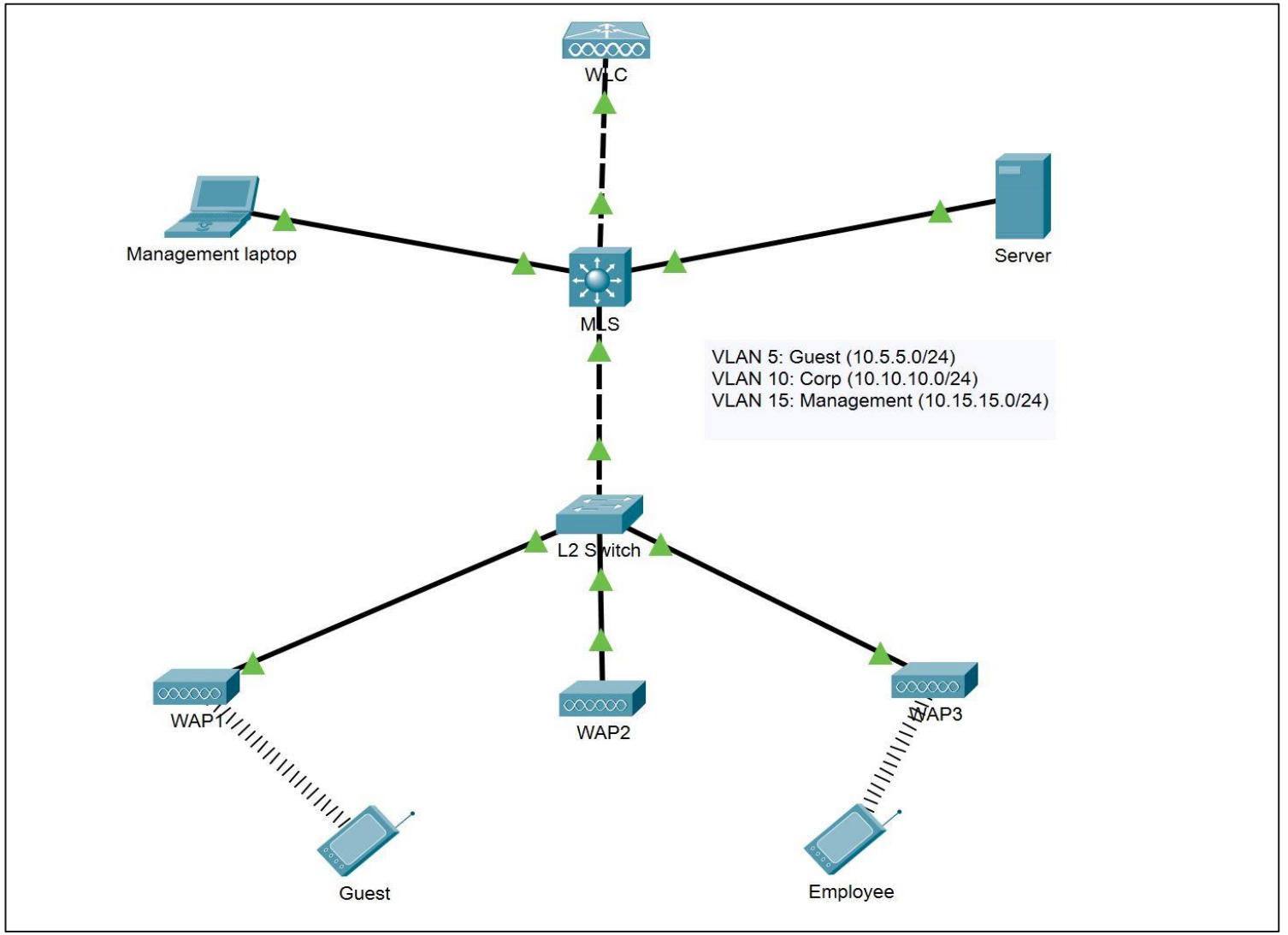
APs in standalone mode

APs controlled by a controller



Software University

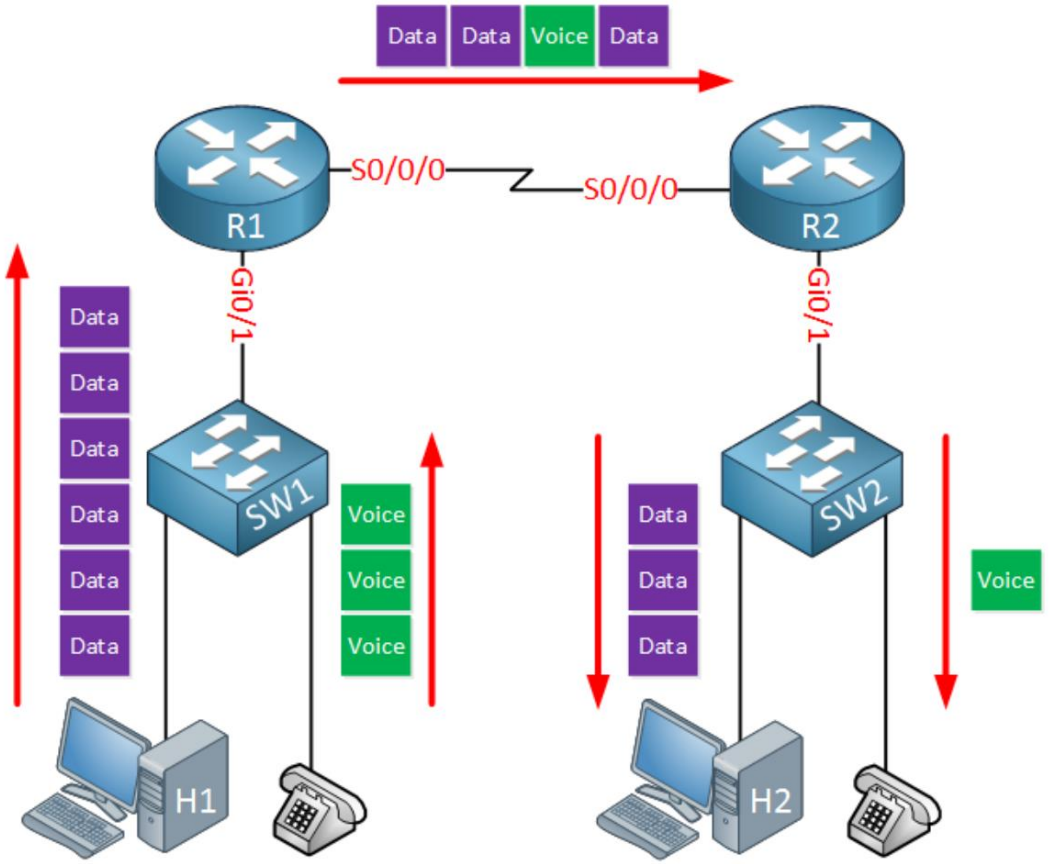
Wireless Lan Controller Lab



Quality of Service (7)

What is QoS?

- Network devices do NOT care about the type of traffic, they need to forward:
  - Switches use destination MAC
  - Routers use routing tables
- The logic in forwarding is simply I
- **QoS** is a way to prioritize



Characteristics of network traffic

- **Bandwidth** - the speed of the link
- **Delay** - the time it takes for a packet to get from the source to the destination (a.k.a. one-way delay)
- **Jitter** - the variation of the delay for each packet
- **Loss** - the amount of the lost data

QoS tools

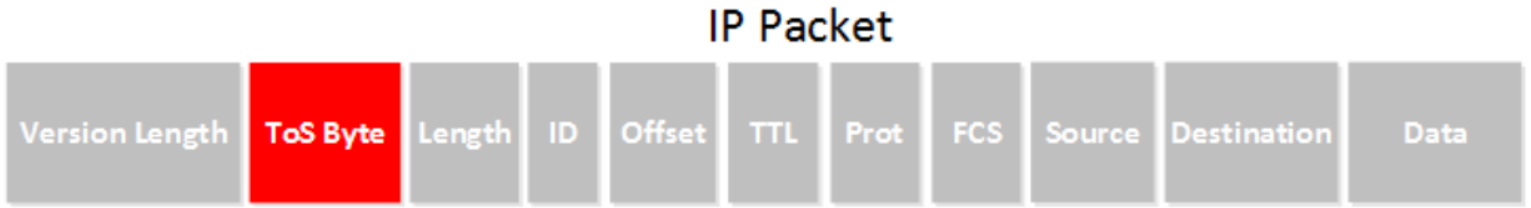
- Classification and marking
- Queuing
- Policing and shaping
- Congestion avoidance

Classification and marking

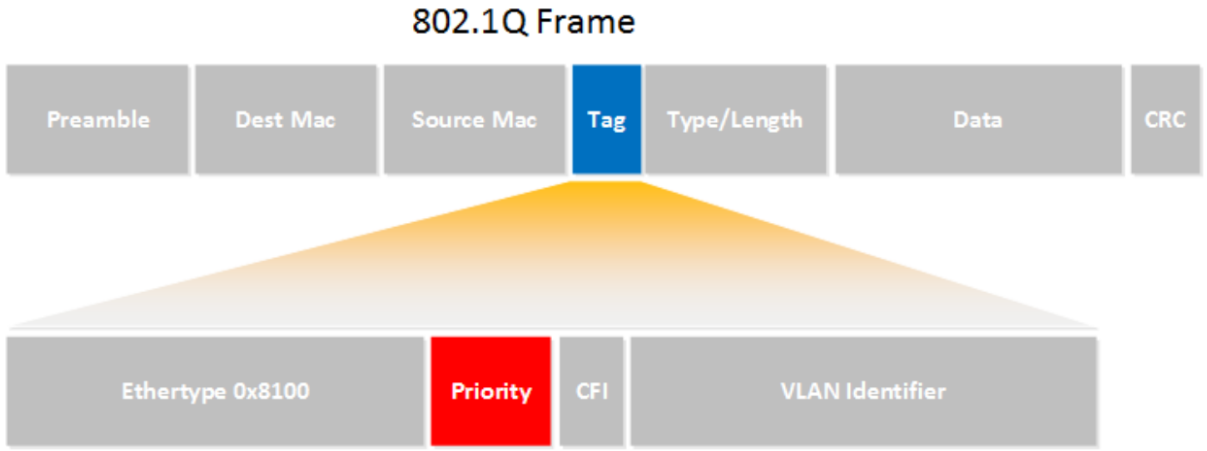
- For each packet to have different treatment, we have to first identify and mark them
- There are different methods to classify a packet:
  - Header inspection - looks for MAC, IP, port numbers
  - Payload inspection - looks inside the packet, making deep packet inspection.
  - On Cisco routers, this is done with **NBAR** (**N**etwork-**B**ased **A**pplication **R**ecognition)

Classification and marking (2)

- Once classified, we need to mark the packet or frame
  - For L3 packets, we modify the ToS field:

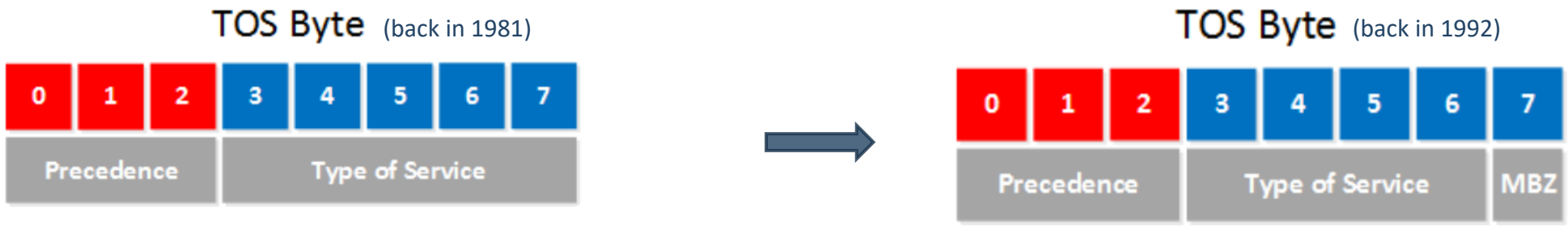


  - For L2 frames, we modify the Priority field (for trunks only):



IP precedence

- Originally, only the precedence in the ToS byte was used:

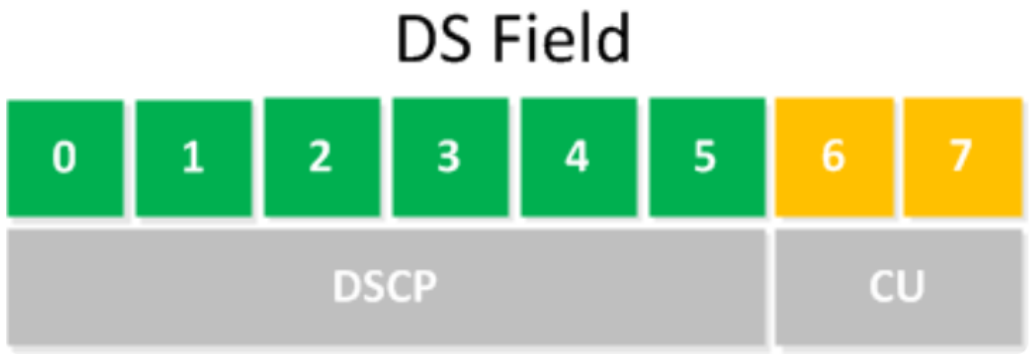


- The possible values for precedence:

IP Precedence	Decimal value	Bit pattern
Routine	0	000
Priority	1	001
Immediate	2	010
Flash	3	011
Flash Override	4	100
Critical	5	101
Internetwork Control	6	110
Network Control	7	111

Differentiated Services

- In 1998, the ToS filed gets a new name: DS field
- The first 6 bits set a **code point** which affects the Per Hop Behavior
- **DSCP**: **D**ifferentiated **S**ervices **C**ode **P**oint
- DSCP PHB (Per Hop Behavior) options:
  - Default PHB
  - Class-Selector PHB
  - Assured Forwarding PHB
  - Expedited Forwarding PHB

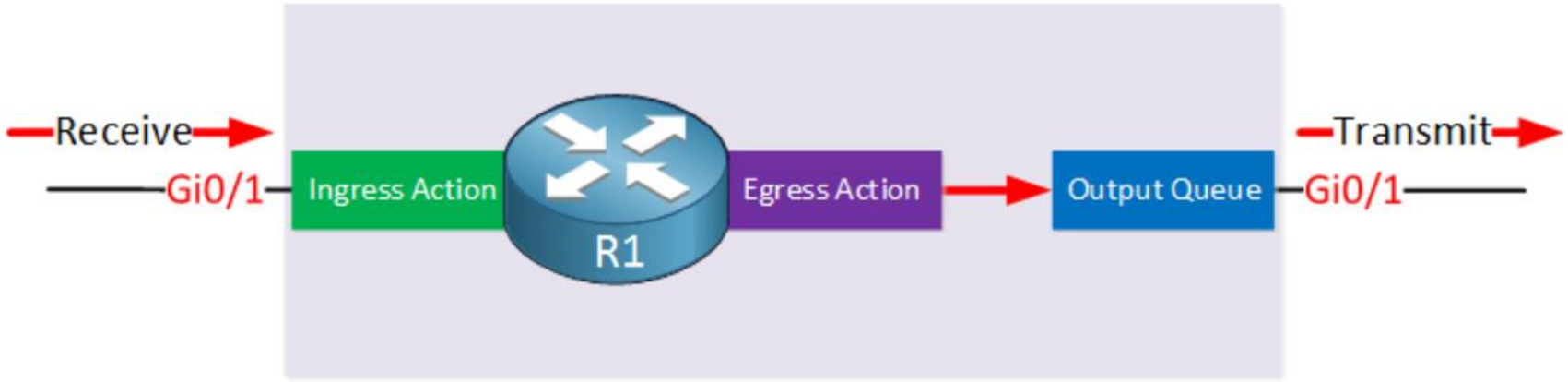


QoS tools

- Classification and marking
- Queuing
- Policing and shaping
- Congestion avoidance

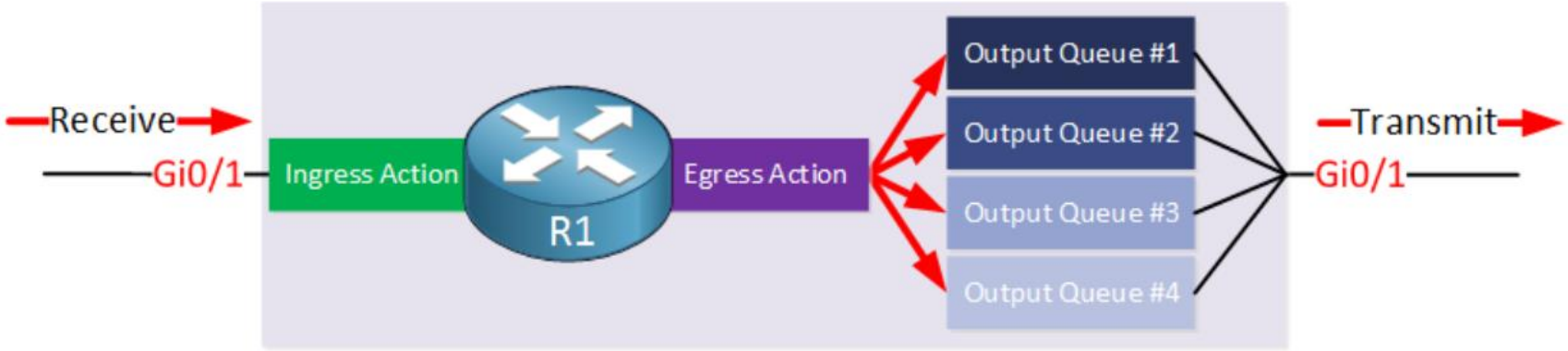
Queuing/congestion management

- In a router, after consulting with the routing table, the router will put a packet in an interface's queue
  (same applies for a switch, with frames)
- Queuing is needed only if there is congestion



Queuing/congestion management (2)

- Most network devices has multiple output queues



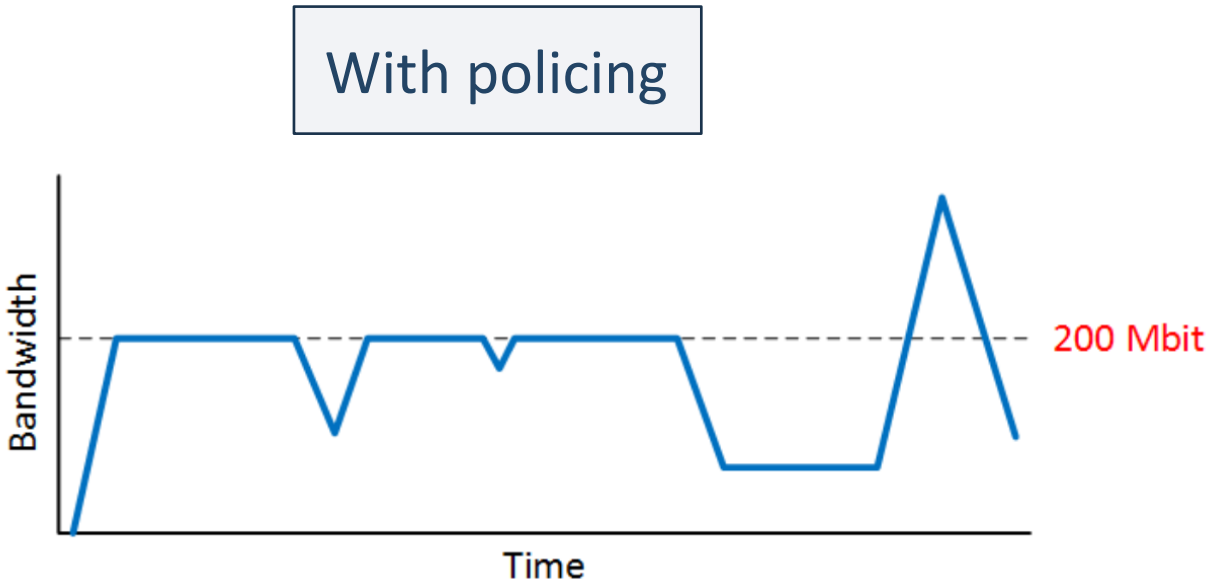
- Different **scheduling** options exist, for example:
  - FIFO (First In First Out)
  - Priority Queuing
  - Custom Queuing
  - WFQ (Weighted Fair Queuing)
  - CBWFQ (Class Based Weighted Fair Queuing)

QoS tools

- Classification and marking
- Queuing
- Policing and shaping
- Congestion avoidance

Policing

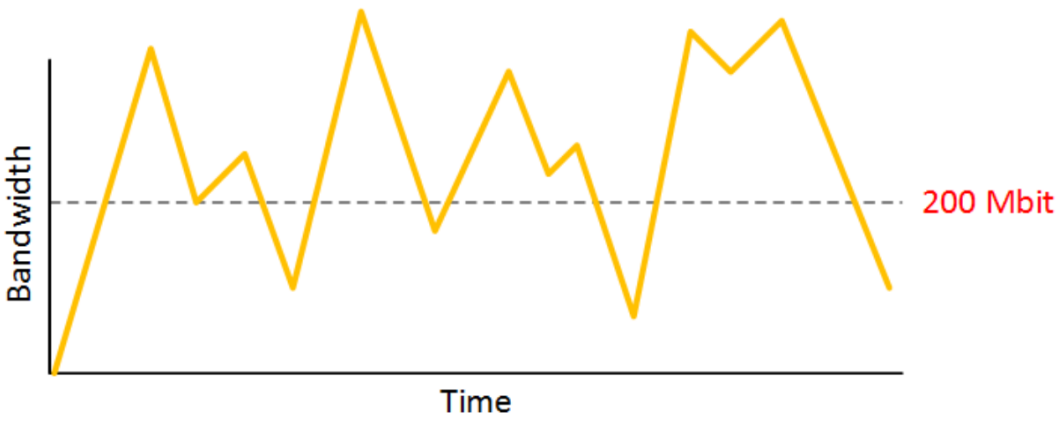
- Policers discard traffic in order to meet the CIR (Committed Information Rate)



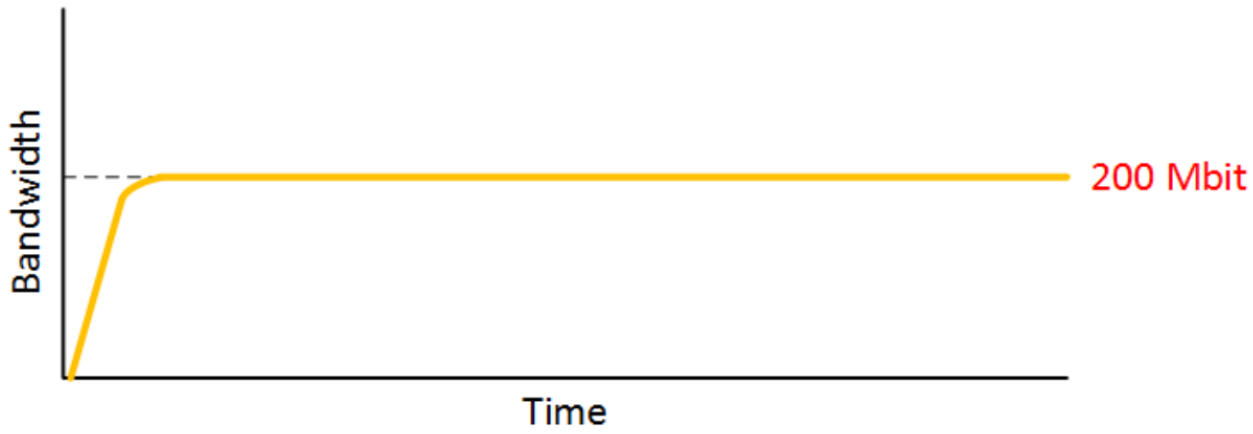
Shaping

- Shapers hold packets in a queue, causing delay
- This prevents the traffic from getting dropped at the other end

Before



After

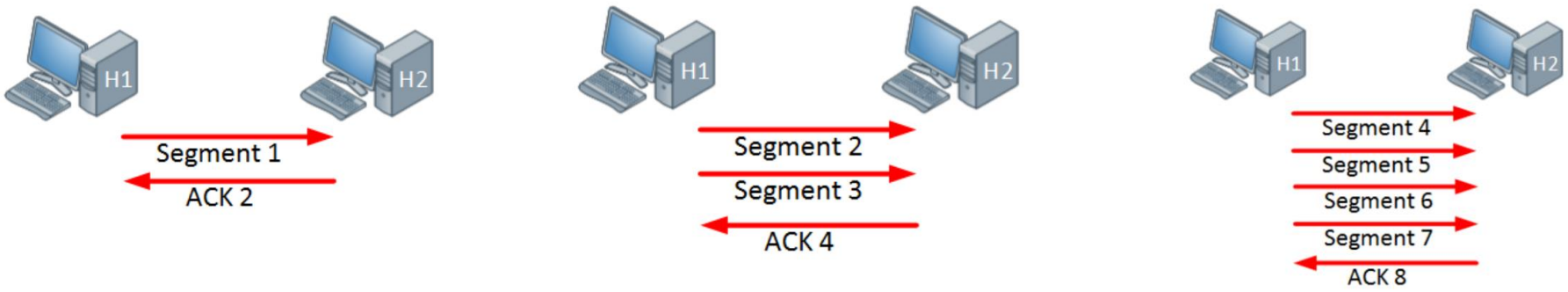


QoS tools

- Classification and marking
- Queuing
- Shaping and policing
- Congestion avoidance

Congestion avoidance

- Remember the TCP windowing?

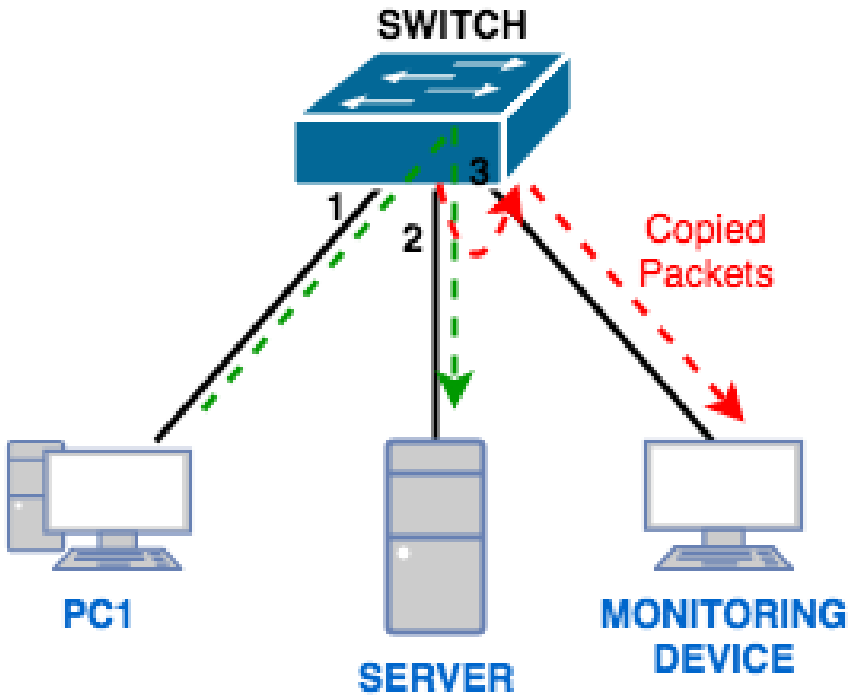


  - Tail drop – when congestion occurs, all packets at the end are dropped
  - This causes **TCP global synchronization**
- With congestion avoidance mechanisms, once the output queue is at certain level, it will drop TCP segments in order to reduce the window size
  - Example: WRED (Weighted Random Early Detection)

Port mirroring (7)

What is port mirroring?

- Also called port monitor or SPAN (Switch Port Analyzer) in Cisco
- Lets you copy all traffic from a source port or source VLAN to a destination interface

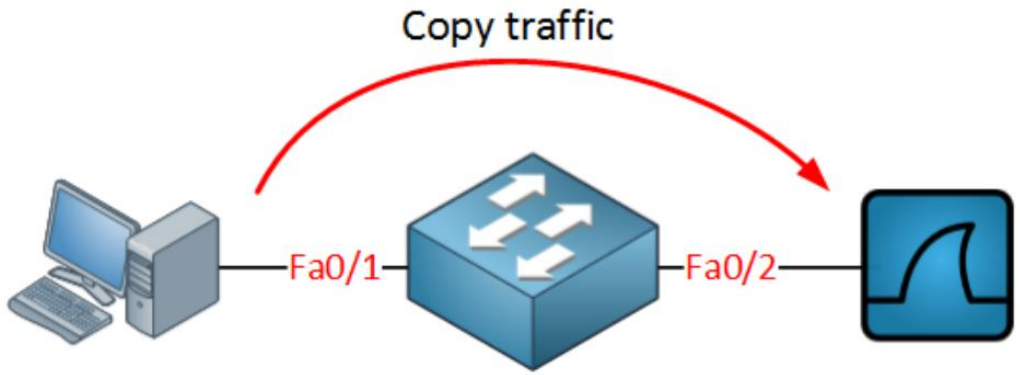


Why port mirroring?

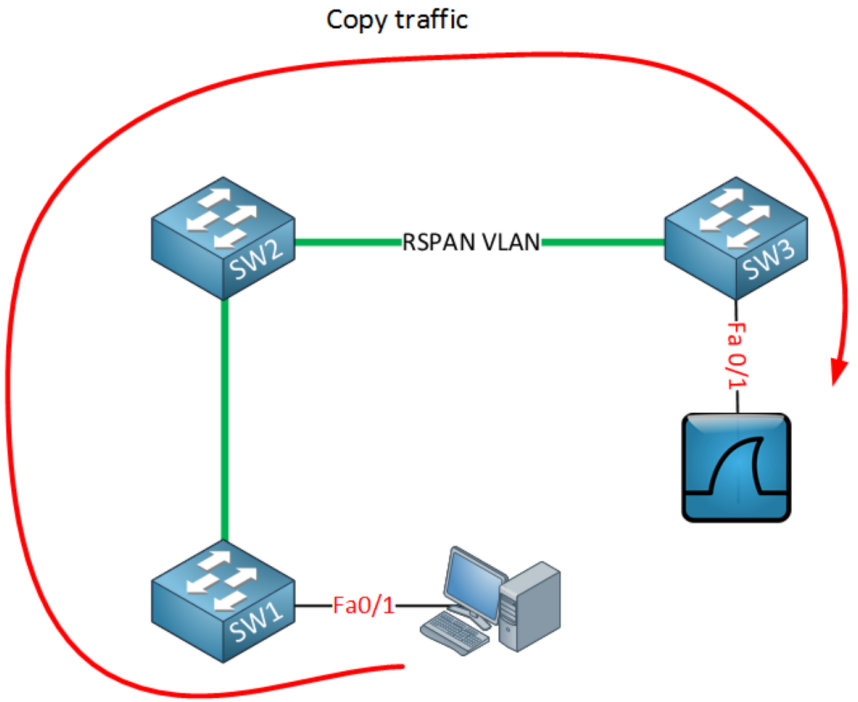
- SPAN can be useful for a number of reasons:
  - If you want to use Wireshark to capture a communication, you need to sniff
  - To redirect all traffic from a VLAN to an IDS/IPS
  - Redirect all VoIP calls from a VLAN so you can record the calls

Types of SPAN

- Local SPAN



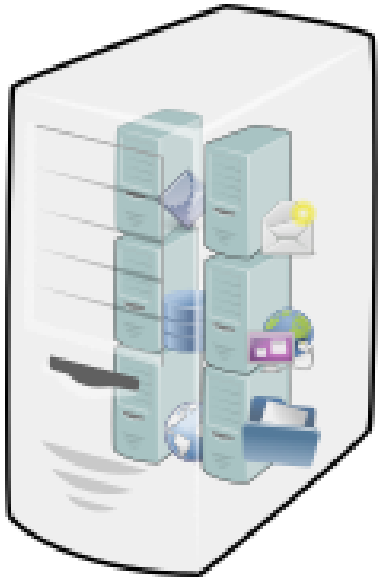
- Remote SPAN (RSPAN)



OS virtualization and networking (8)

Why virtualization?

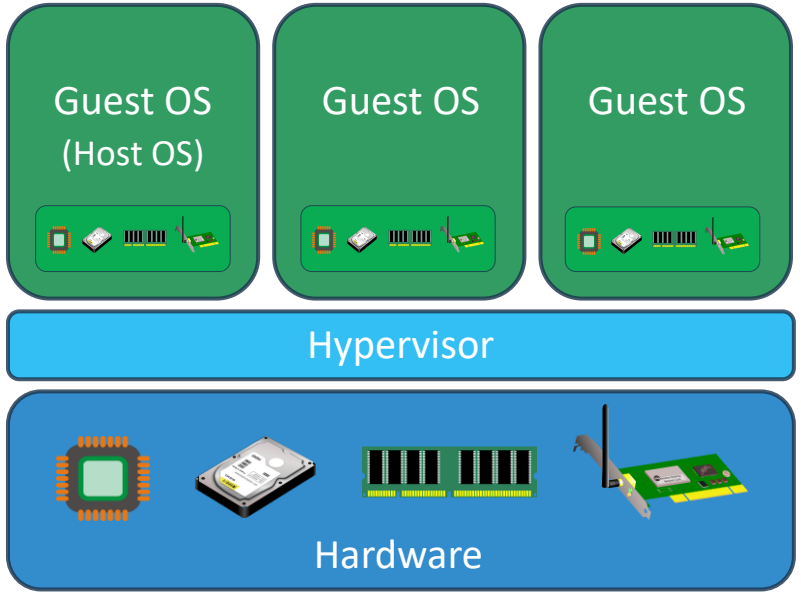
- You get the most out of your server hardware
- Easier configuration for redundancy and backup
- Simplified management
- Fast provisioning of new machines
- Saves energy and costs



OS virtualization types

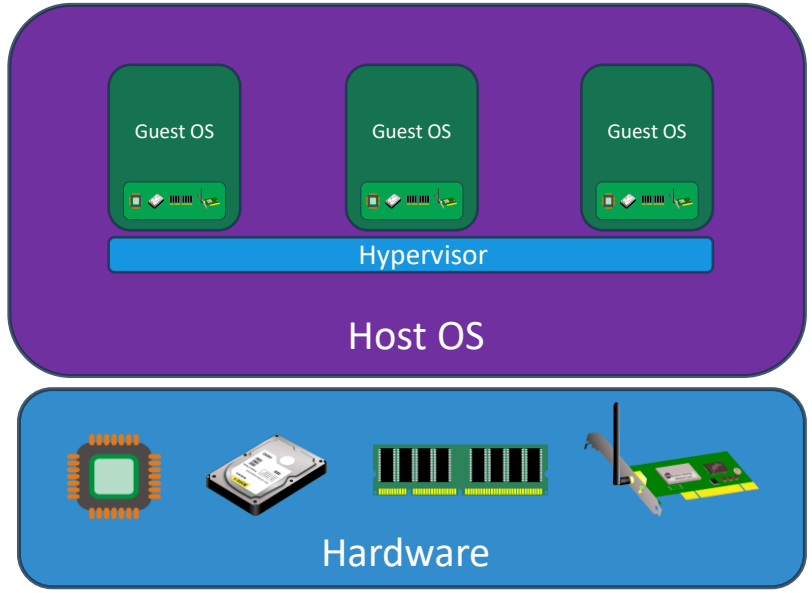
Software University

Type 1 - Bare Metal hypervisor



- Very fast access to the hardware
- Examples:
  - VMware ESXi
  - Microsoft Hyper-V
  - Citrix XenServer
  - KVM (Kernel-based Virtual Machine)

Type 2 - Hosted hypervisor



- Slower access to the hardware
- Examples:
  - VMware Workstation (Player)
  - Oracle VirtualBox
  - Microsoft Virtual PC
  - Parallels Desktop for MAC
  - QEMU (Quick Emulator)

Hyper-V and virtual networks

- In Hyper-V, when you create a new network, you create a new virtual switch
- You can create different types of networking (switches), depending on your needs:
  - Private
  - Internal
  - External

VMware workstation and virtual networks

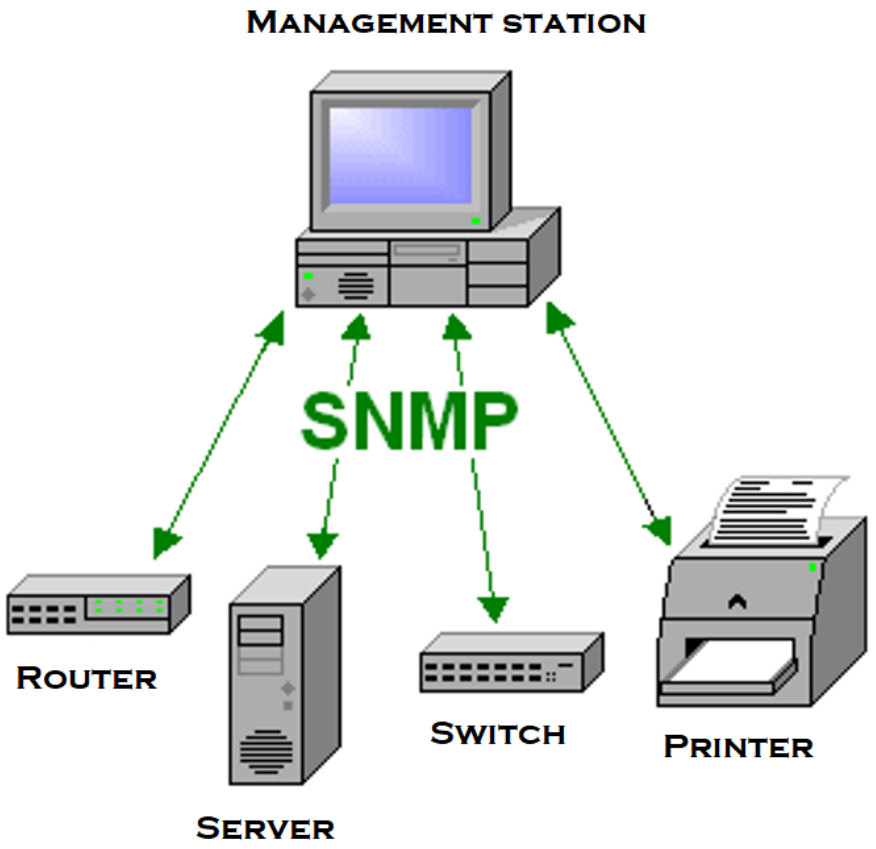
Software University

- In VMware Workstation (Player), several virtual adapters can be added to the host OS and they represent connections to different virtual switches (or networks):
  - **VMnet0** – represents a bridge. You can decide and manually assign the exact physical interface to be bridged
  - **VMnet1** – represents the host-only switch
  - **VMnet8** – represents NAT, which is performed by the host
- Custom connections/networks can also be created

Network Management Systems (8)

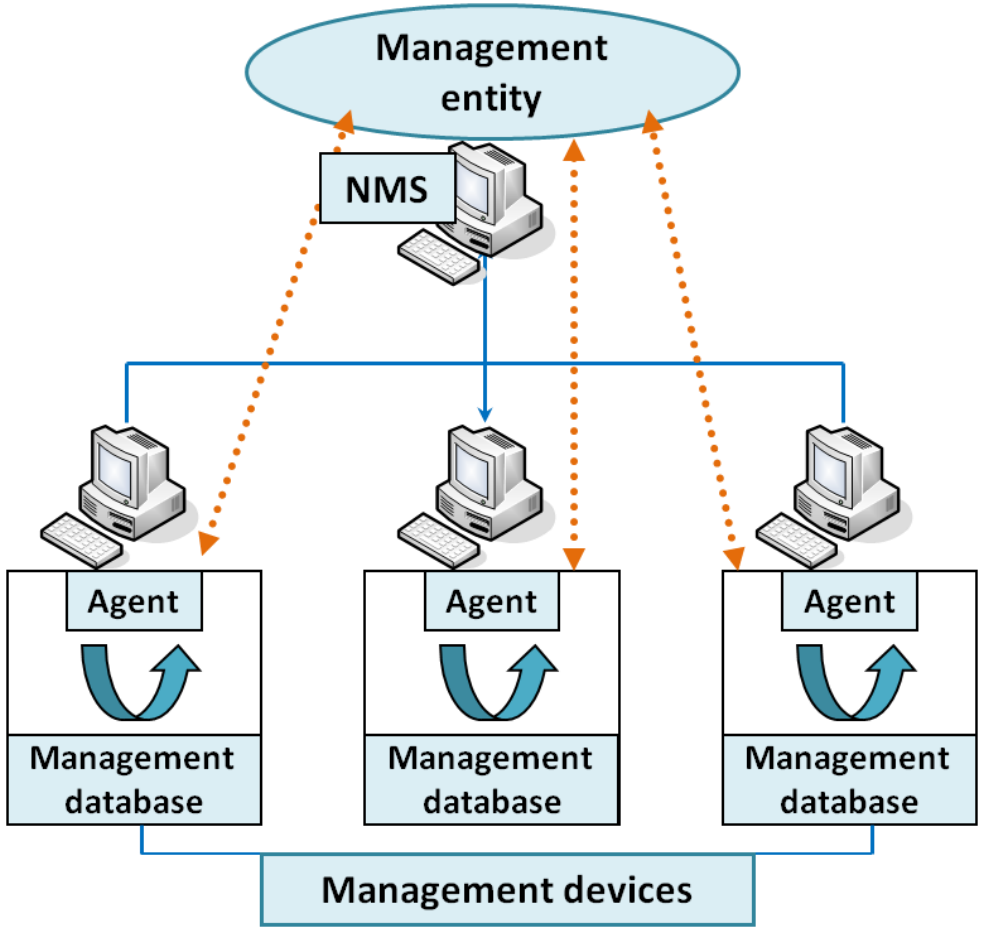
What is a Network Management System?

- A central "hub" to monitor and manage multiple devices
- Advantages:
  - Easy to manage your network
  - Saves time
  - Cost effective
  - Decreases downtime
  - …more?



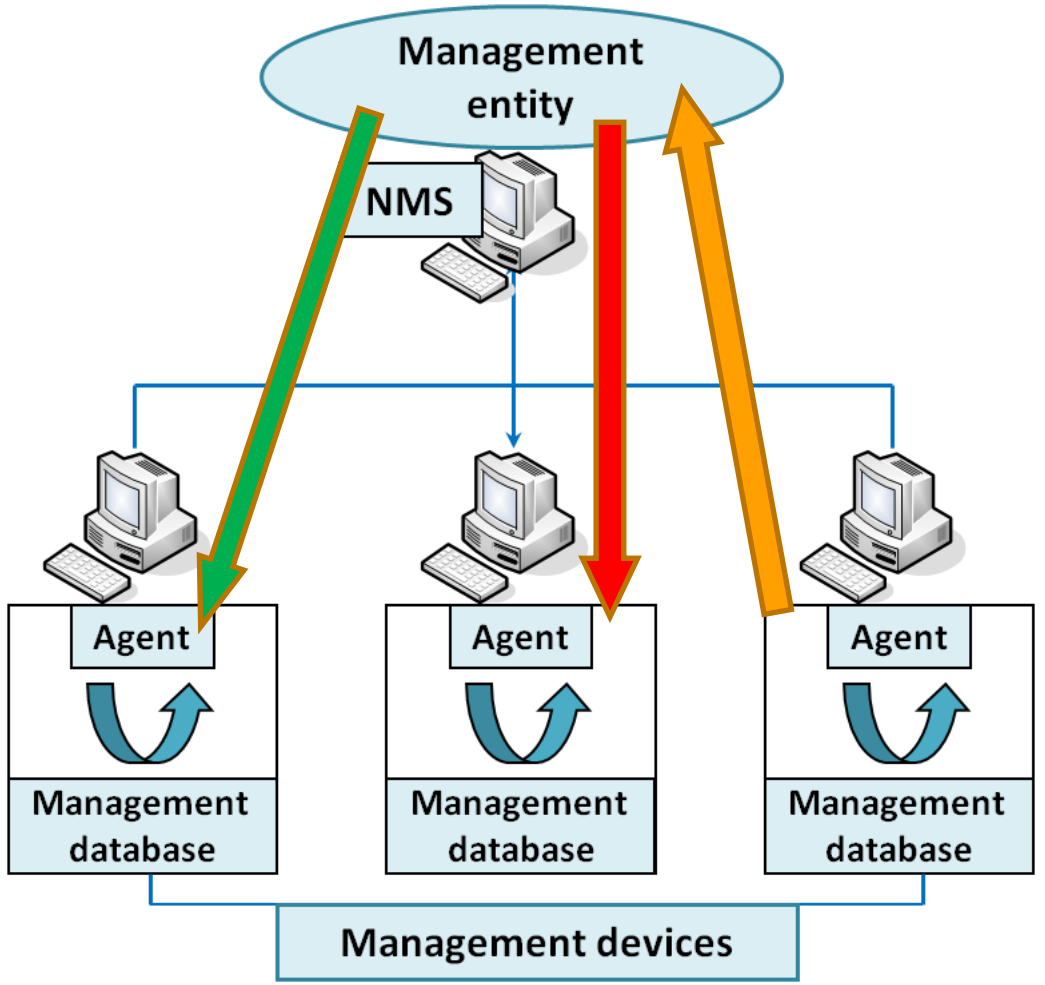
SNMP components

- Agent
- Management station (NMS)
- SNMP messages
- Management information base (MIB)



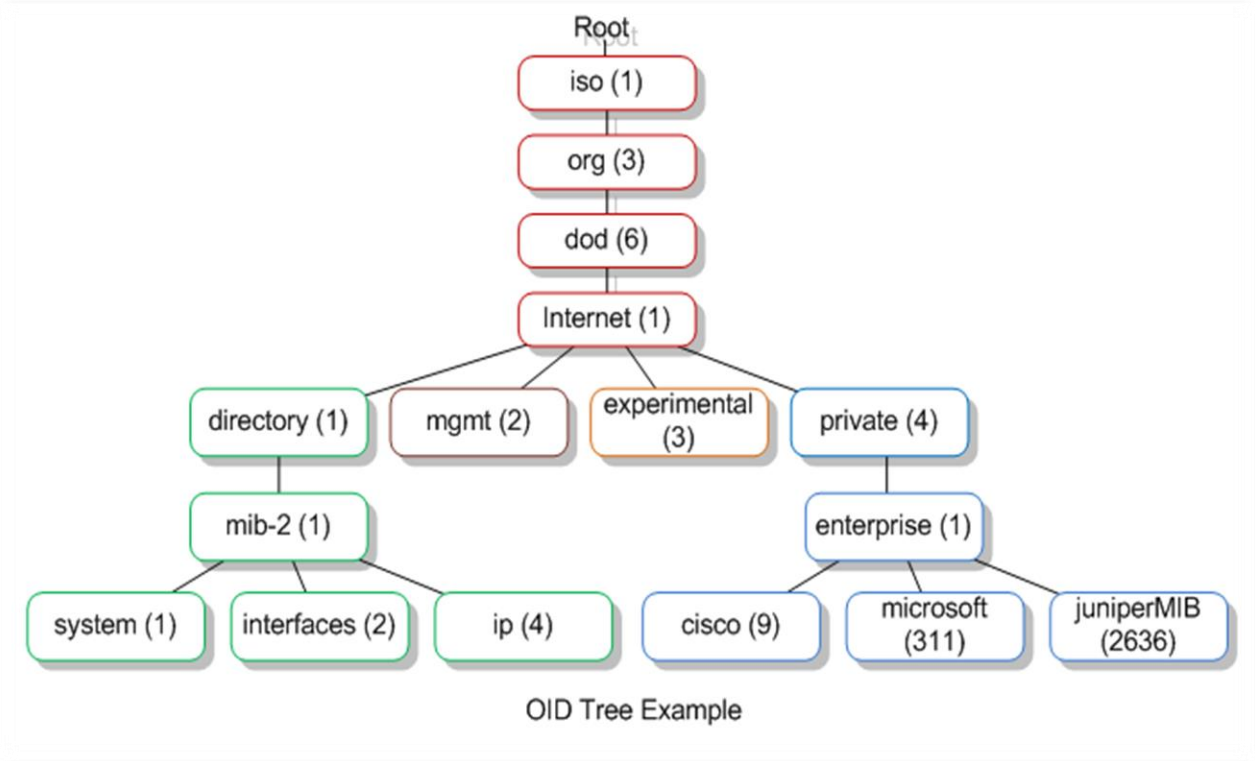
SNMP message types

- **Get** - Read only
- **Set** - Read/Write
- **Trap** - generated by the agent



SNMP MIB

- MIB: Management Information Base
- Collection of information organized hierarchically
- Each entry in MIB is addressed through OID (object ID)
- MIB structure must be known by the NMS and the agents

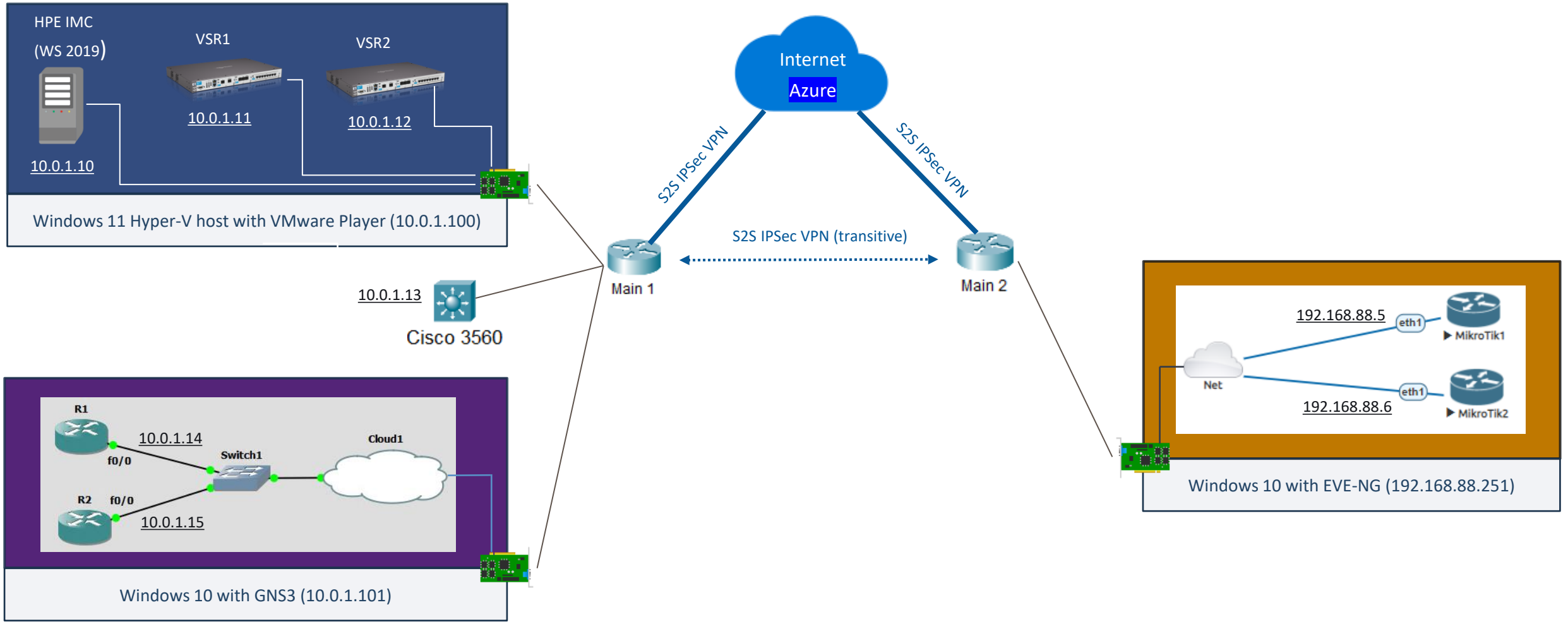


OID Tree Example

SNMP versions

- SNMP v1
  - poor security
  - not very good performance
- SNMP v2c
  - poor security
  - better performance
- SNMP v3
  - Secure and with good performance
  - More difficult to configure

Demo



* All masks are /24

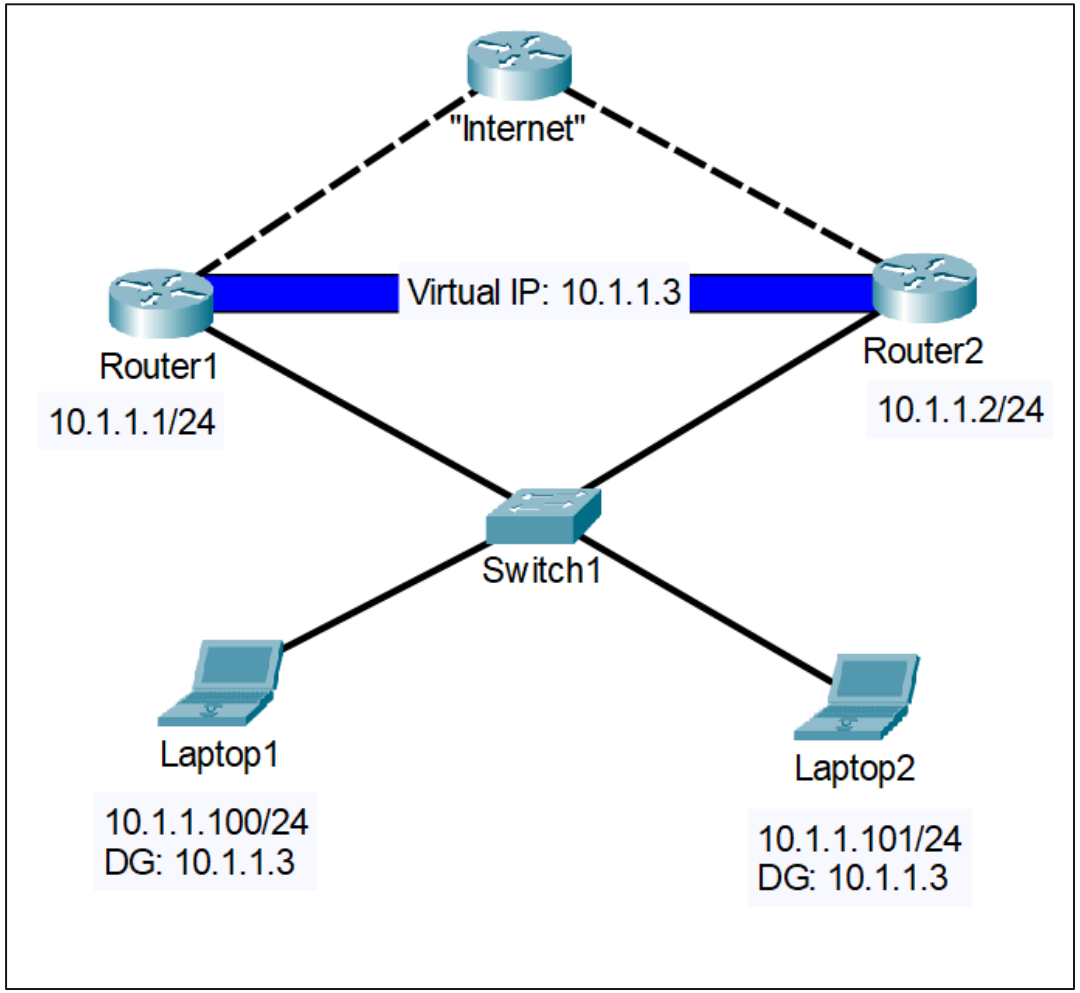
Hot Standby Routing Protocol (9)

Default gateway redundancy

- The end devices (hosts, servers) need a default gateway to reach remote networks or Internet
- If the default gateway is not reachable, the end devices can no longer exit their local segment
- A secondary / backup default gateway option is needed to provide fault tolerance. There are two options:
  - On the client / OS side - causes problems and is not recommended
  - On the router side – usually one IP address is shared between multiple routers and it acts as a default gateway

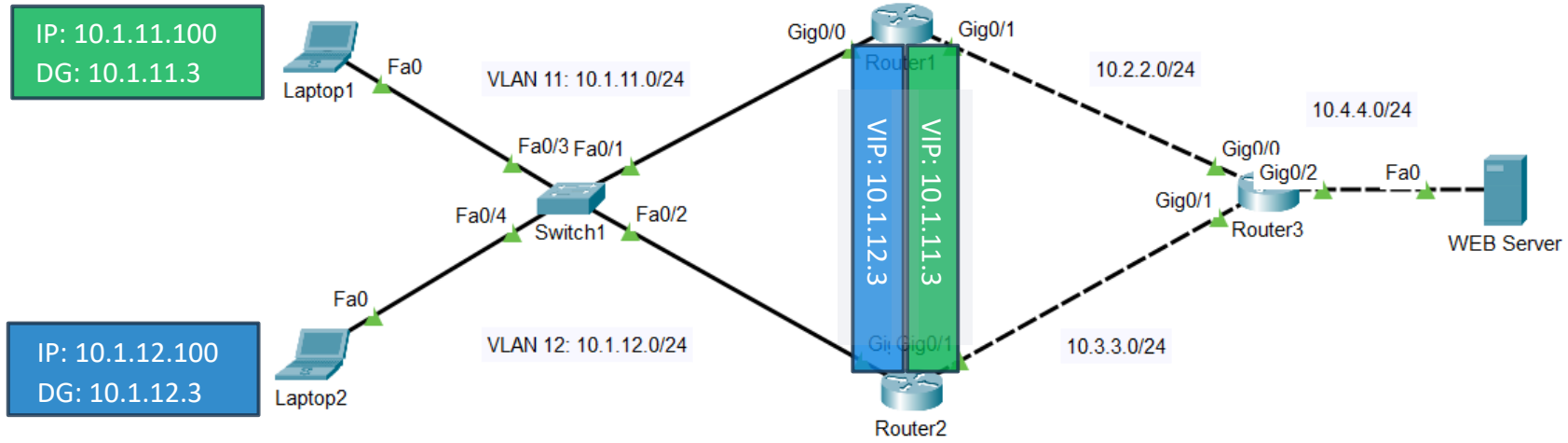
HSRP overview

- HSRP = **H**ot **S**tandby **R**outer **P**rotocol
- Two (or more) routers share one virtual IP (and MAC) address, which is used as default gateway for the clients



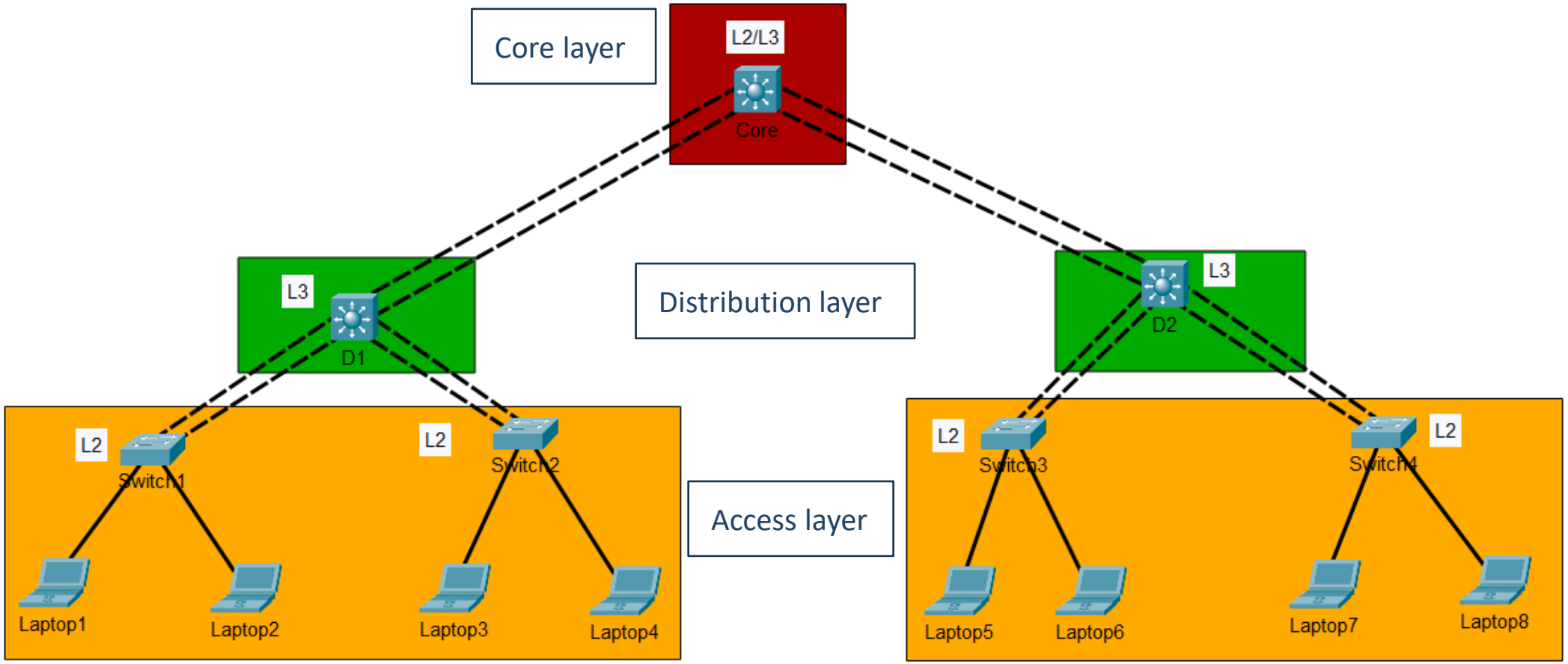
HSRP load balancing

- Load balancing is possible with **different HSRP groups**
- In the example below:
  - one HSRP group is configured with Virtual IP of 10.1.11.3 and the active router R1
  - another HSRP group is configured with Virtual IP of 10.1.12.3 and active router R2
- In case of one of the routers goes down, the other will handle all the traffic

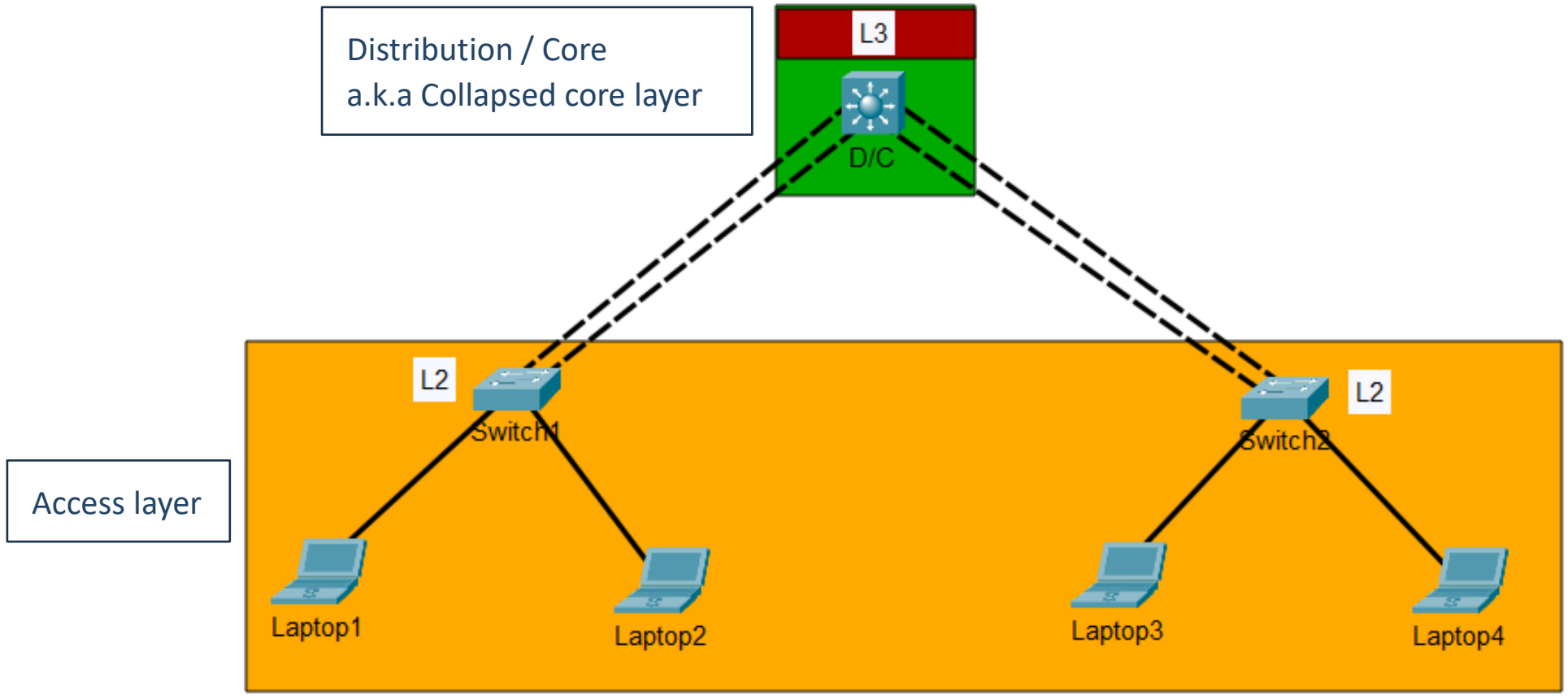


Hierarchical design models (9)

3-tier hierarchical model

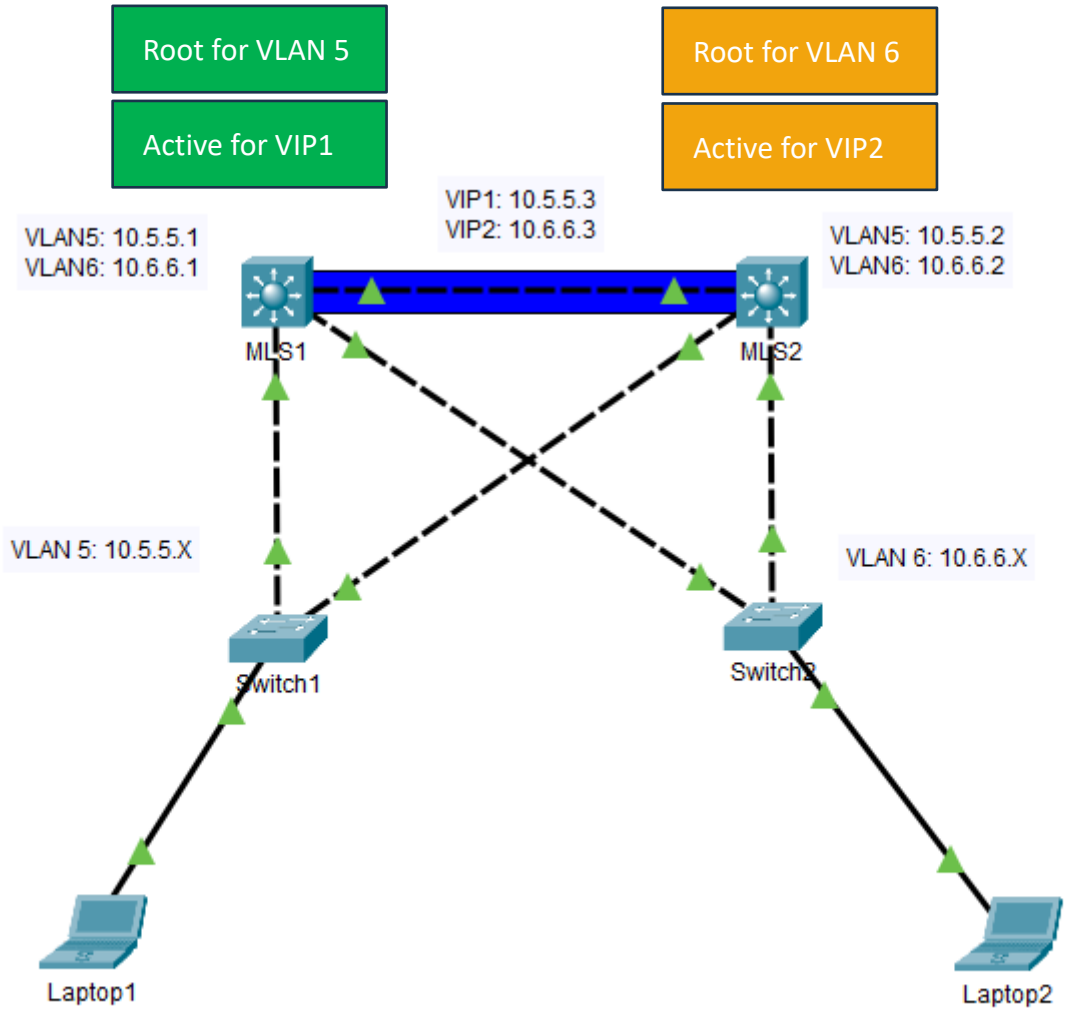


2-tier hierarchical model



HSRP and STP (9)

HSRP and STP



- Load balancing at L2 and L3 during normal operations
- Failover at L2 and L3 during failure of links or distribution devices

Software Defined Networking (10)

The old (current) way of doing networking

Software University

- Networking vendors sell proprietary hardware
- Hardware can be different, but devices talk to each other using protocols
- These protocols are built in the OS/image in each device
- We need to separately configure the logic for each “box” by using:
  - Command Line Interface (CLI)
  - Some kind of Network Management System (NMS)

How network devices make forwarding decisions

Software University

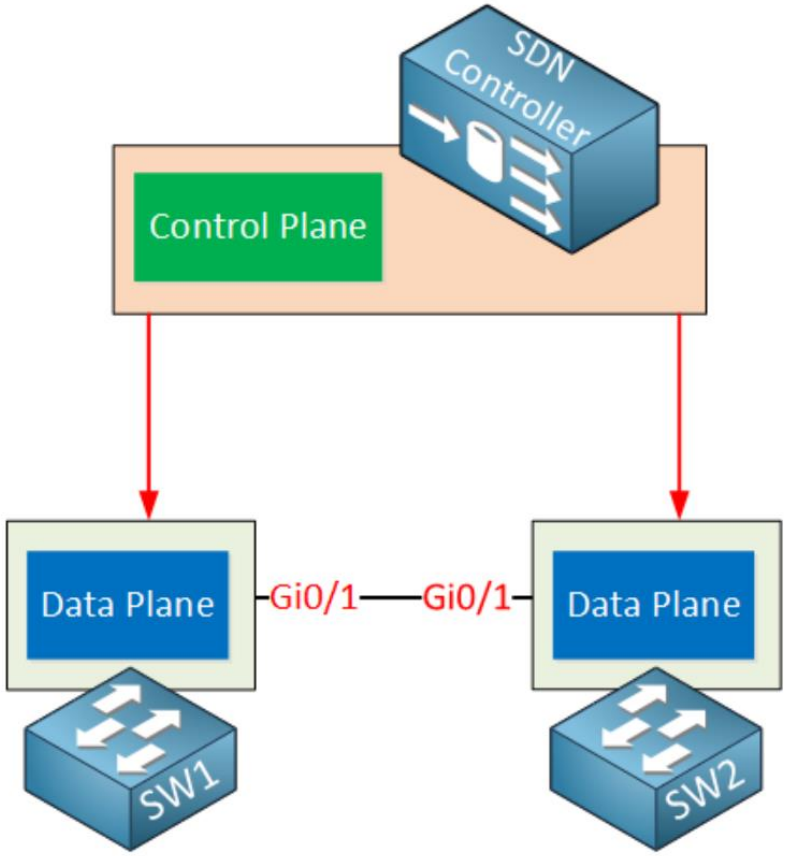
- Switches and routers should decide where to send a particular packet so each device may need to consider, build or change:
  - MAC address tables
  - Routing tables
  - Use ARP to find the destination MAC
  - Decrease the TTL of each packet
- Different **planes** are responsible for the different tasks: **control** plane, **data** plane and **management** plane

Devices and planes

- **Control plane** (the brain). Responsible for:
  - Building ARP tables
  - Building routing tables
  - Running STP to avoid loops
- **Data plane** (the muscles). Responsible for:
  - Encapsulation/decapsulation
  - Adding or removing headers (802.1Q for example)
  - Replace source/destination address (if there is NAT)
- **Management plane** - used for accessing and managing the devices. Examples - Telnet, SSH

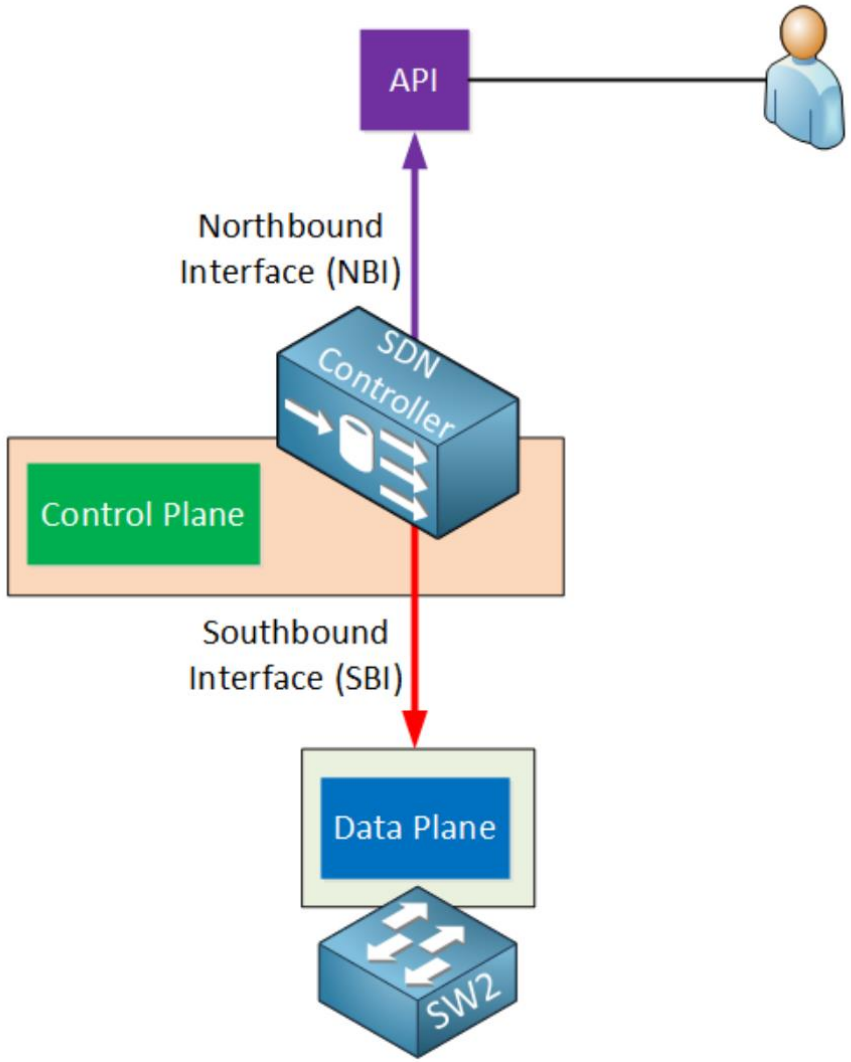
What is SDN?

- SDN - Software Defined Networking
- SDN uses a centralized control plane - SDN controller



SDN controller interfaces

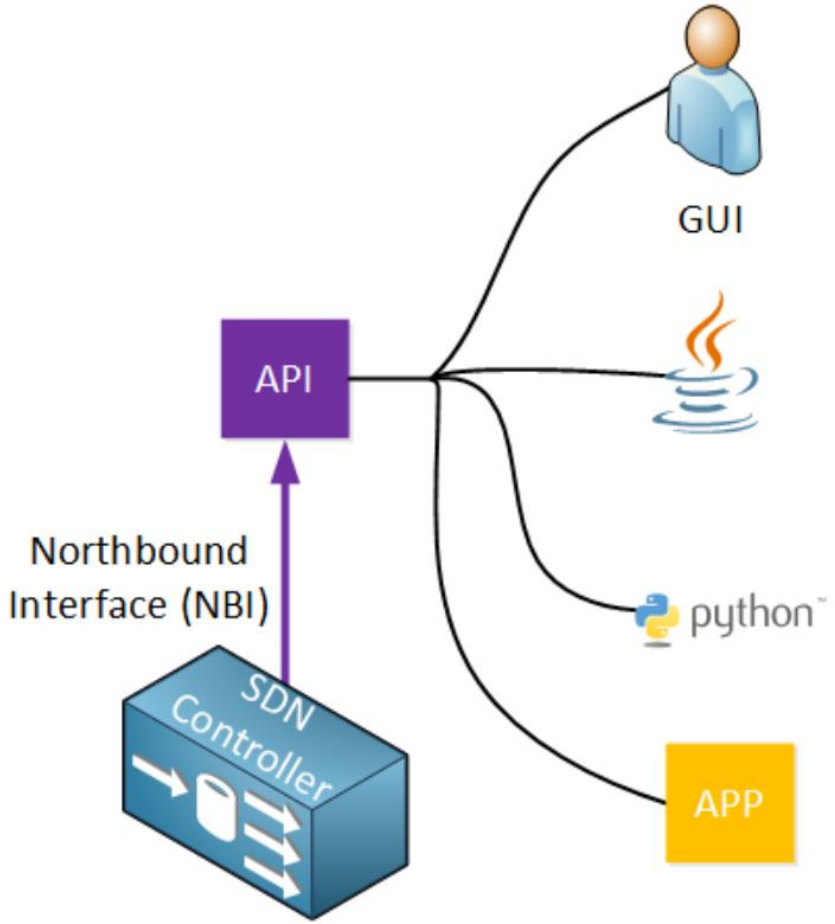
- Northbound Interface (NBI)
  - Used to access and program the controller
  - Can have GUI, CLI and API
  - You can write scripts for automation
- Southbound Interface (SBI)
  - The controller's communication with the "dumb" devices
  - It is a software interface, often API



SDN northbound interface

- The interface allows multiple applications to access the controller:
  - GUI
  - Java/Python or other scripts
  - 3rd party apps

- REST API and JSON (next slide) are typically used



JSON

- JSON = JavaScript Object Notation
- Why?
  - User vs machine languages and **information formatting**
  - Easy to read collection of key-value pairs
  - Uses **declarative** ("what") rather than imperative ("how") syntax

```
    "contentVersion": "1.0.0.0",
    "parameters": {
        "location": {
            "value": "westeurope"
        },
        "networkInterfaceName": {
            "value": "vm1903"
        },
        "enableAcceleratedNetworking": {
            "value": true
        },
        "networkSecurityGroupName": {
            "value": "VM1-nsg"
        },
        "networkSecurityGroupRules": {
            "value": [
                {
                    "name": "RDP",
                    "properties": {
                        "priority": 300,
                        "protocol": "TCP",
                        "access": "Allow",
                        "direction": "Inbound",
                        "sourceAddressPrefix": "*",
                        "sourcePortRange": "*",
                        "destinationAddressPrefix": "*",
                        "destinationPortRange": "3389"
                    }
                }
            ]
        },
```

SDN southbound interface

- This is the controller's communication with the "dumb" hardware
- It specifies a software (not a physical) interface
- Some popular southbound interfaces:
  - OpenFlow
  - Cisco OpFlex
  - The good old CLI - SNMP/Telnet/SSH

Simulators and labs for SDN

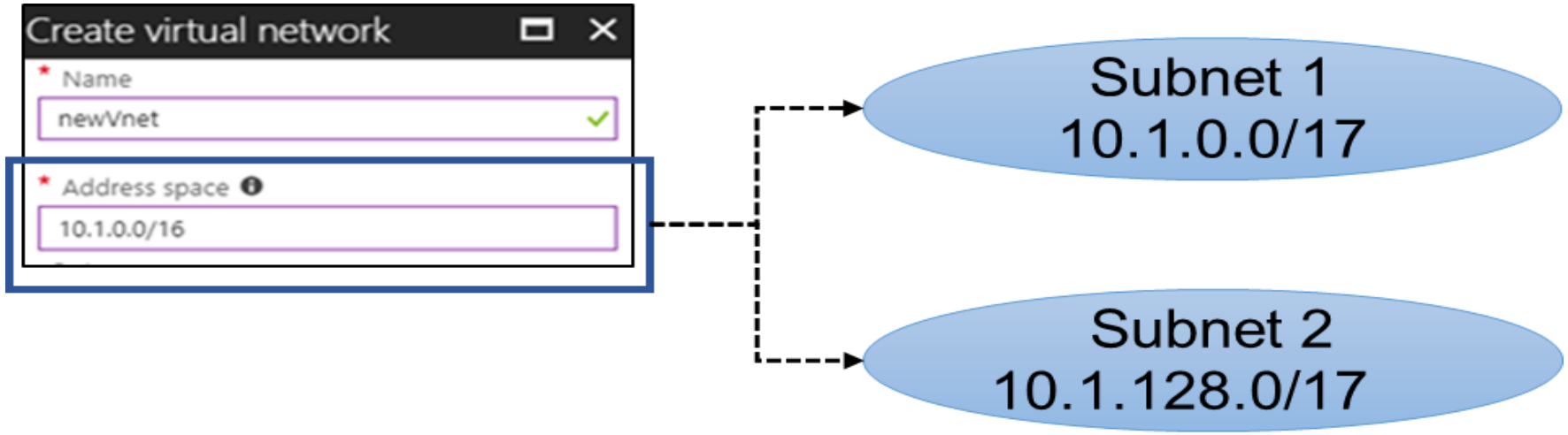
- Mininet and Miniedit
- HPE VAN SDN controller (with Mininet)
- Cisco APIC-EM
- VMWare NSX
- Cisco DNA center
- Cisco Packet Tracer

Course Summary (11)

Cloud Networking with Microsoft Azure (12)

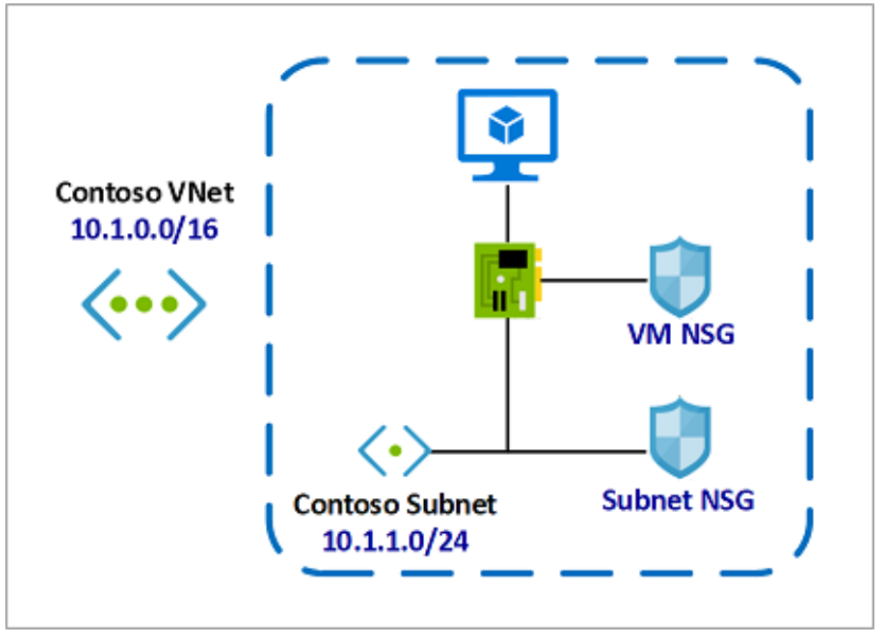
Subnets

- A virtual network can be segmented into one or more subnets
- Subnets provide logical divisions within your network
- Benefits of subnetting a virtual network include security and performance
- Each subnet must have a unique address range - cannot overlap with other subnets in the virtual network in the subscription



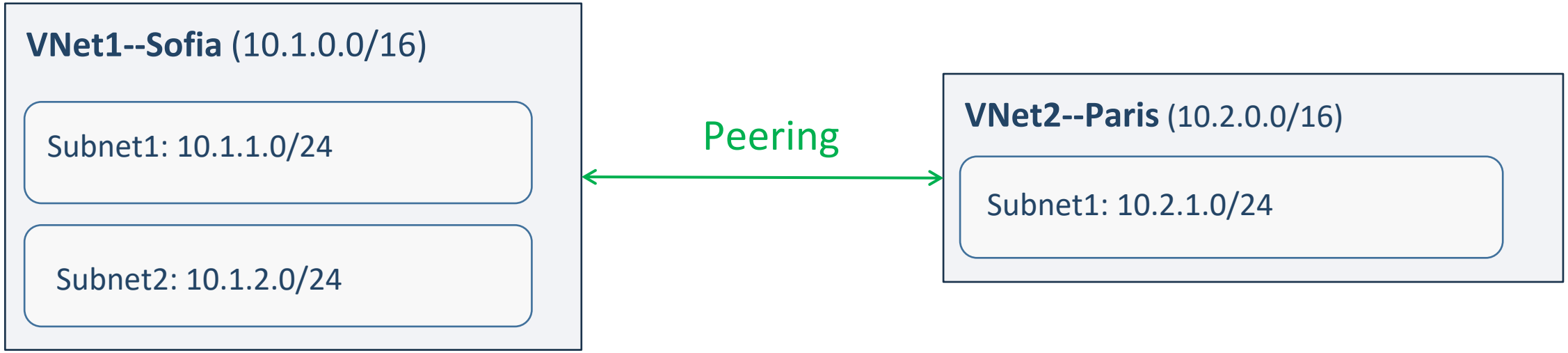
Network Security Groups (NSG)

- You can limit network traffic to resources in a virtual network
- An NSG contains a list of security rules that allow or deny inbound or outbound network traffic
- An NSG can be associated to a subnet or a network interface
- Similar to Access Control Lists discussed before



Virtual Network Peering

- VNet peering connects two Azure virtual networks
- Peered networks use the Azure backbone for privacy and isolation
- Easy to setup, seamless data transfer and great performance



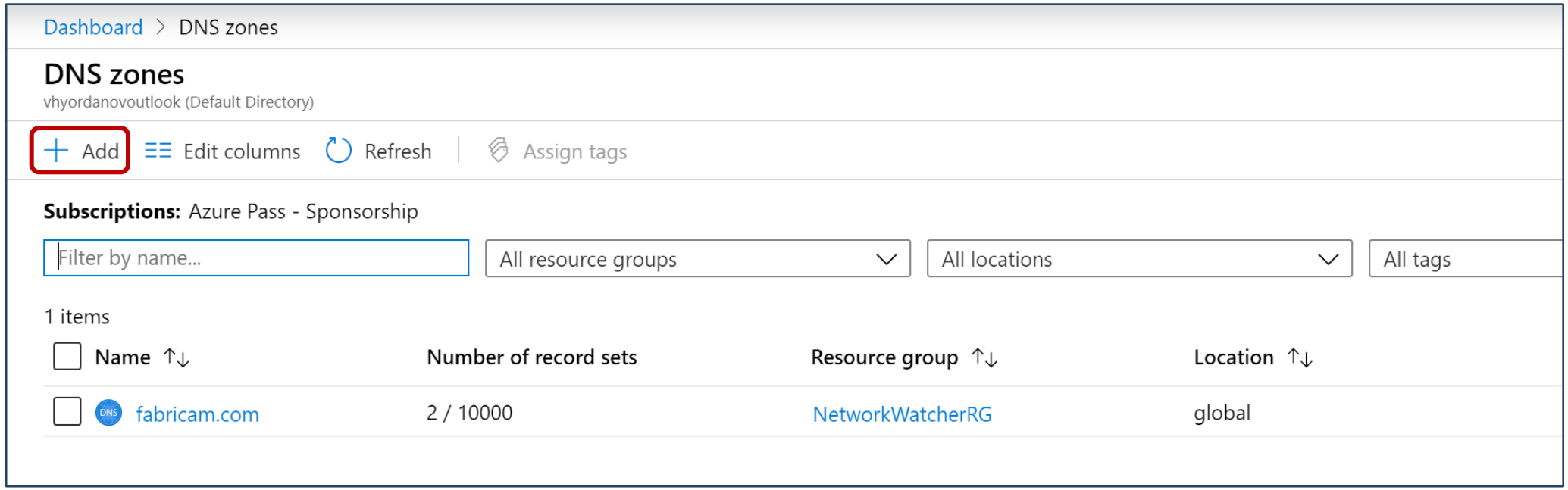
VPN Gateway

Software University

- Used to send encrypted traffic between Azure and on-premise
- Can also create tunnels between Azure virtual networks
- Is able to accept multiple connections
- Each VNet can have only one VPN gateway
- Special VNet subnet is required before creating the VPN gateway
- Different connection topology diagrams are supported – site-to-site, multi-site, point-to-site, VNet-to-VNet

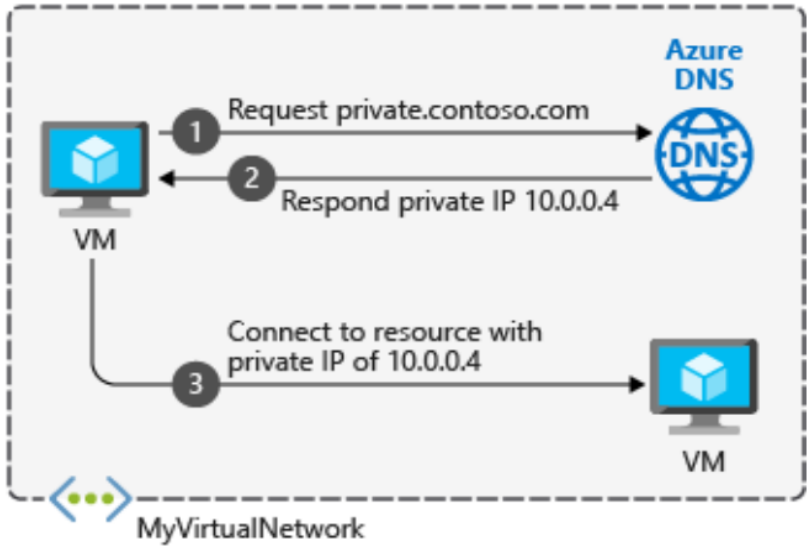
Azure DNS Zones

- Azure offers a DNS service where you can host your DNS zones
- You do not have to own the domain to create a DNS zone with that domain name in Azure
- But…if you want the records in your domain to be resolved by everyone in Internet, then:
  - You must own the domain
  - You must change the name servers in your domain register to point to your Azure DNS zone



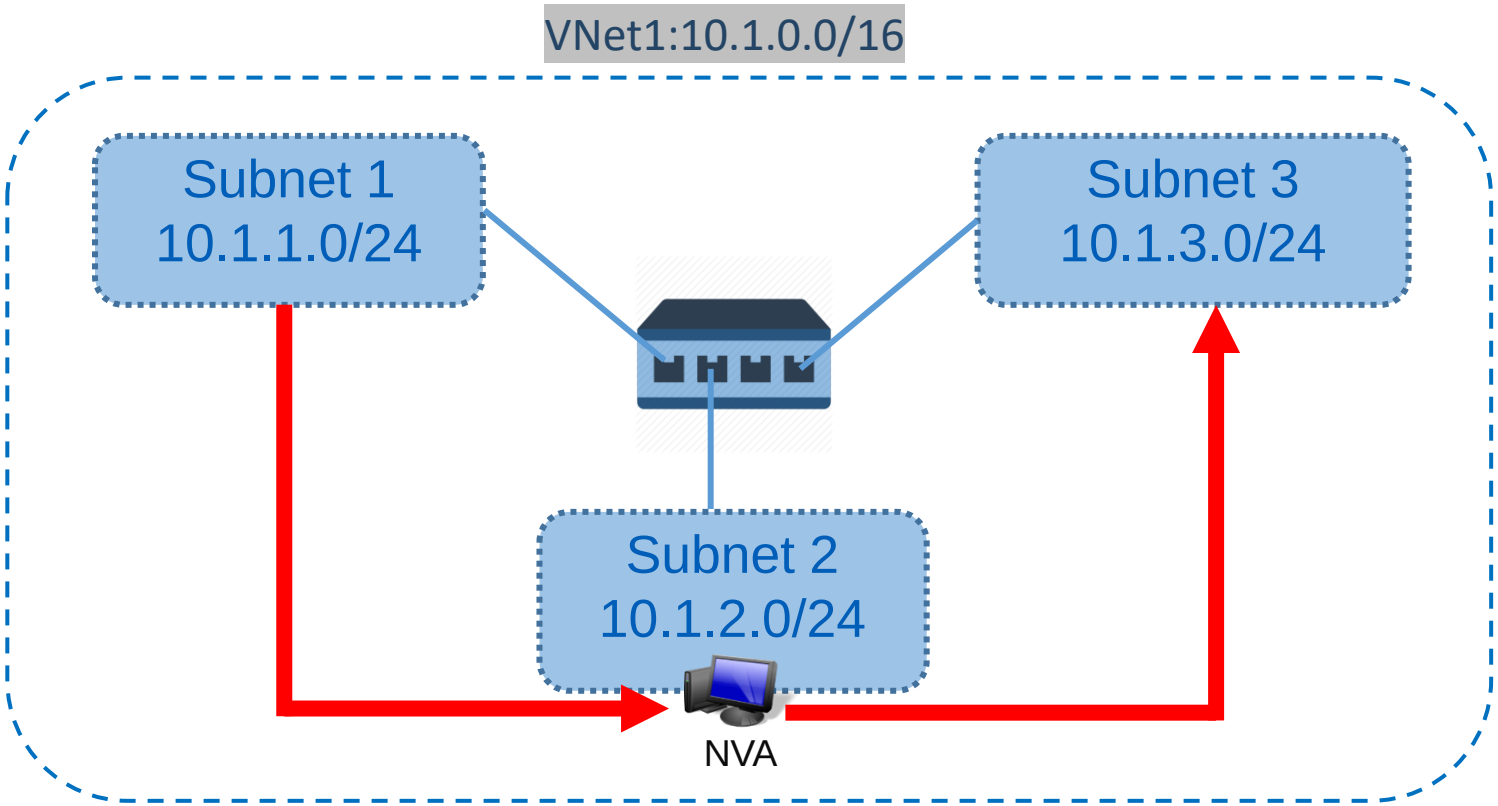
Private DNS Zones

- Private DNS zones provide name resolution in virtual networks without the need to add a custom DNS solution
- Not accessible over the Internet
- Capabilities and benefits:
  - All common DNS records types are supported
  - Hostname resolution between virtual networks
  - Automatic hostname record management
  - Available in all Azure regions
- When you create a Private DNS zone, you need to link it with one or more virtual networks

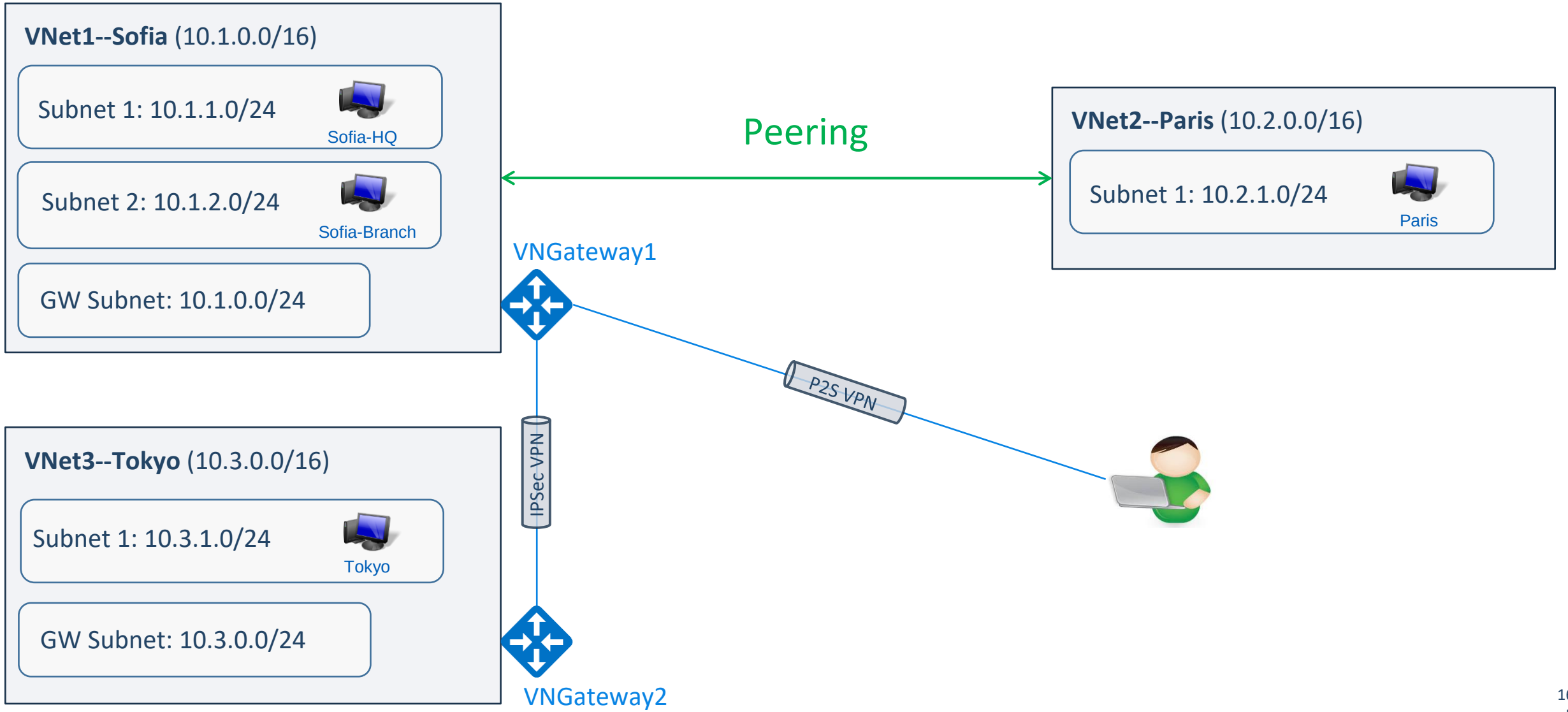


System and User-defined Routes (UDR)

- Before the UDR, system routes connects VMs from each subnet directly
- After a UDR is created, the routing table for Subnet 1 is updated so the traffic goes via the Virtual appliance in Subnet 2



Demonstration



Knowledge Check

Question 1

- **What is an advantage of MSTP over PVST+?**

a. It uses more BPDUs and therefore calculates the topology faster

b. It is easier to configure than PVST+

c. It uses less BPDUs and therefore creates less overhead

d. It is VLAN aware

Question 2

- **What is an advantage of PVST+ over MSTP?**

a. It is VLAN aware and triggers STP calculation for each VLAN individually

b. It is more difficult to configure than MSTP

c. It uses less BPDUs and therefore creates less overhead

d. It is VLAN unaware which simplifies the creation of the VLANs across the network

Question 3

- **Which of the following in terms of link aggregation is false?**

a. The physical interfaces which participate in a link aggregation group should have the same speed and duplex settings

b. There is static and dynamic LACP

c. Link aggregation load balances on a per-packet basis and ensures equally distributed traffic across the physical links

d. Link aggregation benefits include higher bandwidth and better redundancy

Question 4

- **Which of the following in terms of IRF is wrong?**

a. You can only have Ring or Daisy chain topologies

b. The member ID of each device may be the same, but the priorities must be different

c. An IRF stack must consist of Comware devices only

d. The priorities of each device may be the same, but the member IDs must be different

Question 5

- **What is the difference between NAT and PAT? (select multiple)**

a. NAT translates one private to one public IP address

b. NAT translates multiple private to one public IP address

c. PAT translates one private to multiple public IP address

d. PAT translates multiple private to one public IP address

Question 6

- **Which of the following determines how long a DNS entry will stay in the client's cache?**

a. The operating system of the client

b. The TTL value

c. Your ISP

d. The operating system of the DNS server

Question 7

- **What is the best way to secure a wireless network?**

a. Make the SSID hidden, so the clients must know it in order to connect

b. Implement MAC ID filtering to allow only known devices to the network

c. Disable the DHCP server on your wireless router

d. Implement WPA3/WPA2

Question 8

- **Which are the main components of an SNMP system?**

a. Agent, messages, network management system and MIB

b. Get, set and trap

c. Community strings

d. IMC, authentication protocol and SNMP enabled devices

Question 9

- **Which of the following in terms of SDN is false?**

a. It uses Northbound interface and Southbound interface

b. It has a decentralized control plane

c. You may use REST API to communicate with the controller

d. OpenFlow is a typical SDN protocol

Question 10

- **Two possible options to connect between two VNets in Azure are:**

a. Point-to-site VPN and ExpressRoute

b. Virtual network peering and VPN

c. System routes and user-defined routes (UDR)

d. Using NSG and NAT

Questions?

SoftUni

Software University

SoftUni Creative

SoftUni Digital

SoftUni Foundation

SoftUni Kids

Finance Academy

SoftUni Diamond Partners

Software University

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