University of Rome Tor Vergata
ICT and Internet Engineering

Network and System Defense

Alessandro Pellegrini, Angelo Tulumello

A.A. 2023/2024

Virtual LANs

Angelo Tulumello

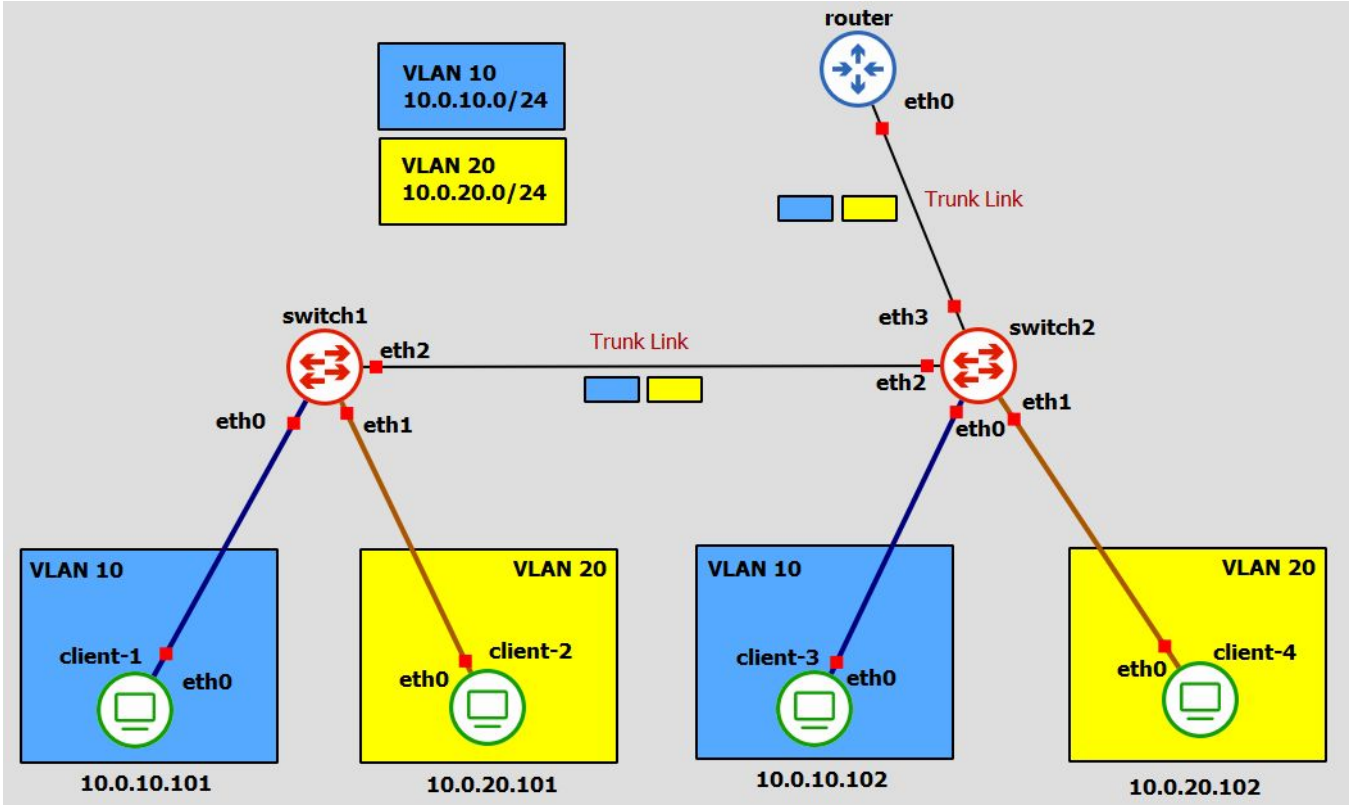
Slides by Prof. Marco Bonola

Other Slides Set

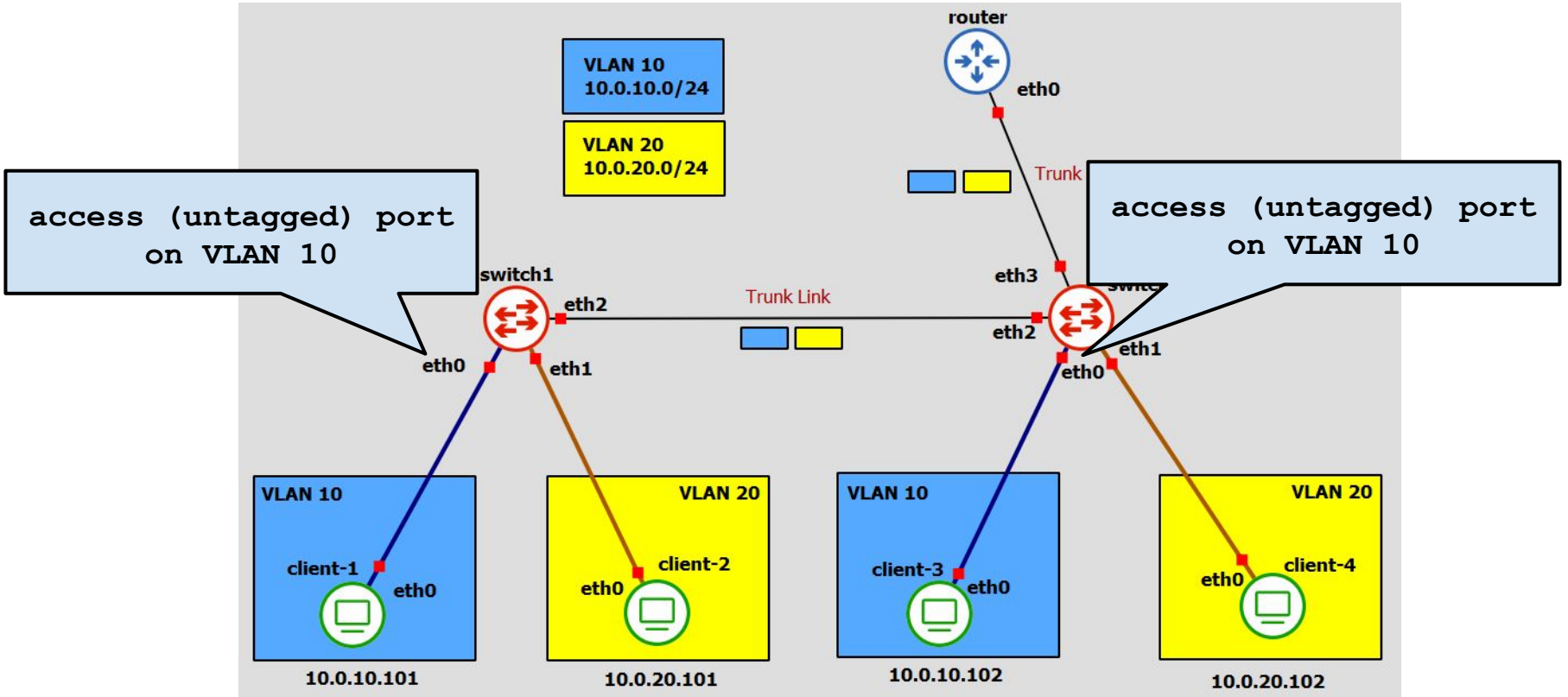
from Prof Salsano's ITP Course

Lab3: 2 VLANs, 2 switch, 1 Router

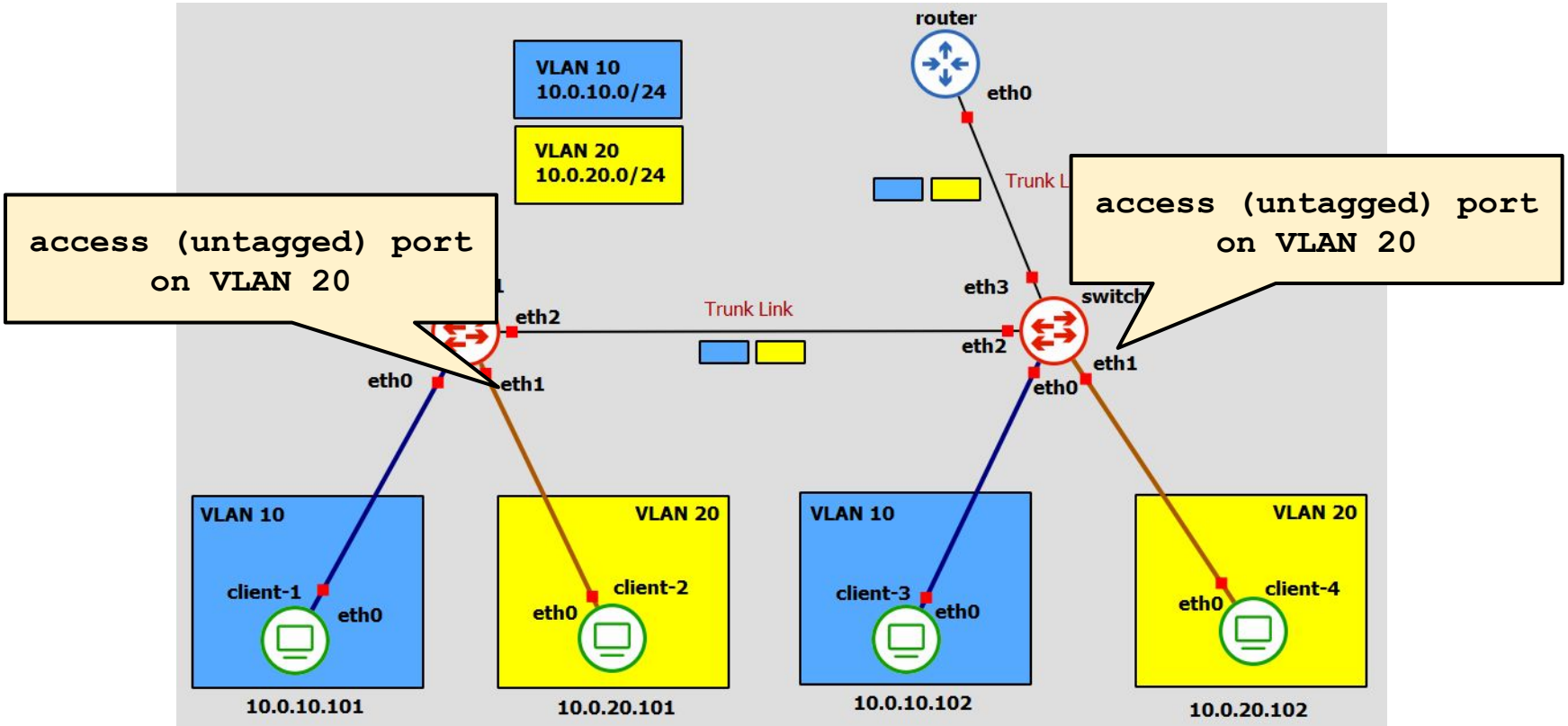
Topology


router
VLAN 10
10.0.10.0/24
VLAN 20
10.0.20.0/24
eth0
Trunk Link
switch1
eth2
Trunk Link
eth3
switch2
eth2
eth0
eth1
eth0
eth1
VLAN 10
client-1
eth0
VLAN 20
client-2
eth0
VLAN 10
client-3
eth0
VLAN 20
client-4
eth0
10.0.10.101
10.0.20.101
10.0.10.102
10.0.20.102

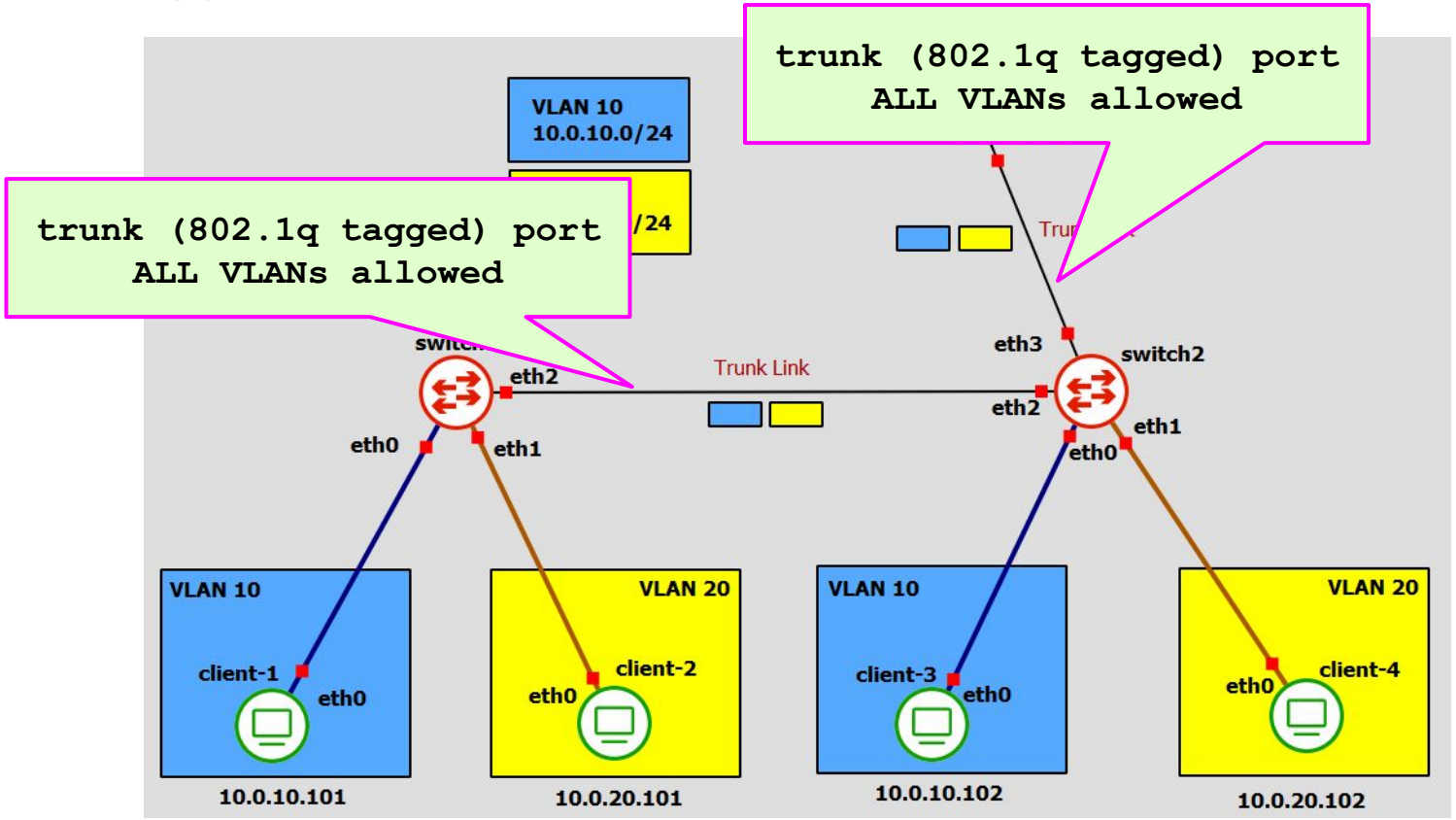
Topology


router
VLAN 10
10.0.10.0/24
VLAN 20
10.0.20.0/24
eth0
Trunk
access (untagged) port
on VLAN 10
access (untagged) port
on VLAN 10
switch1
eth2
Trunk Link
eth3
eth2
eth0
eth1
eth0
eth1
VLAN 10
client-1
eth0
VLAN 20
client-2
eth0
VLAN 10
client-3
eth0
VLAN 20
client-4
eth0
10.0.10.101
10.0.20.101
10.0.10.102
10.0.20.102

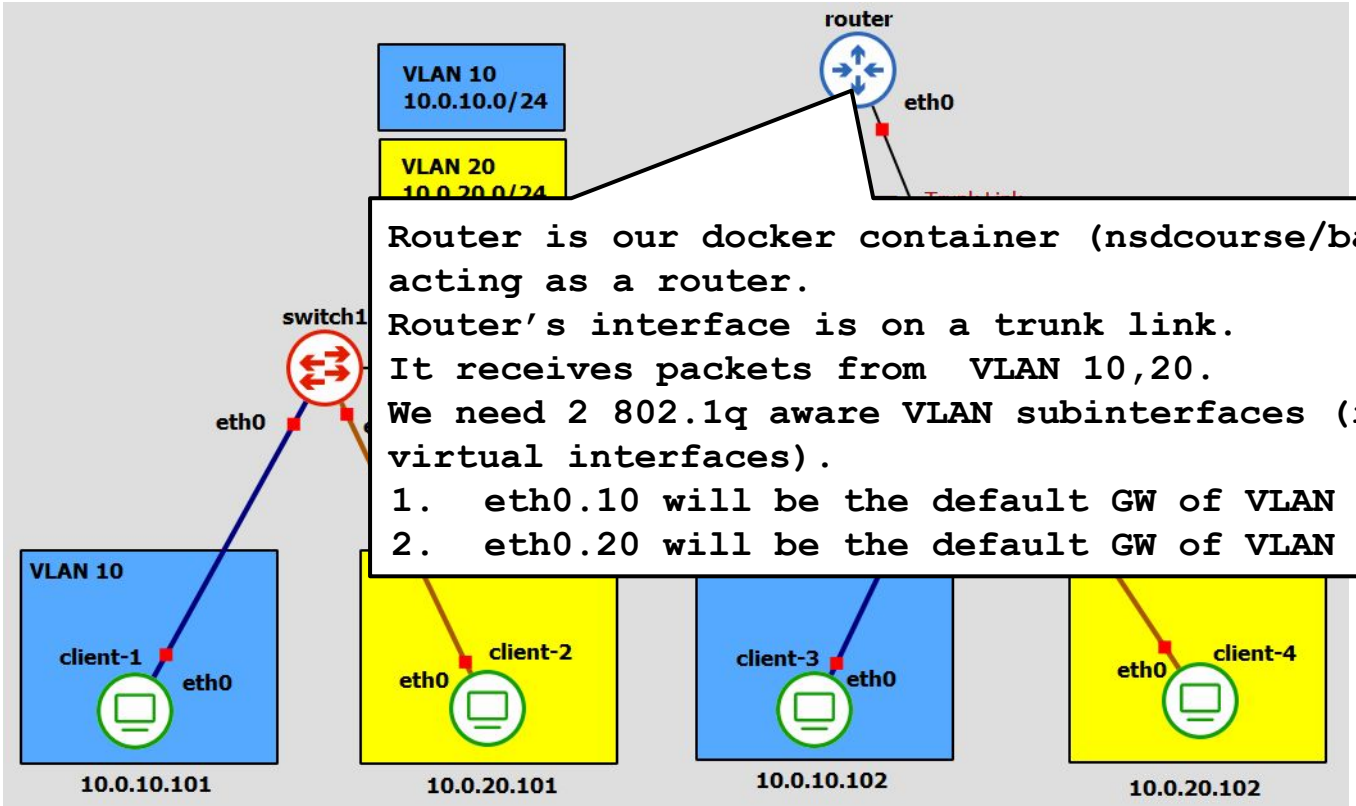
Topology


router
VLAN 10
10.0.10.0/24
VLAN 20
10.0.20.0/24
eth0
Trunk L
access (untagged) port
on VLAN 20
access (untagged) port
on VLAN 20
eth3
switch
eth2
Trunk Link
eth2
eth1
eth0
eth0
VLAN 10
client-1
eth0
10.0.10.101
VLAN 20
client-2
eth0
10.0.20.101
VLAN 10
client-3
eth0
10.0.10.102
VLAN 20
client-4
eth0
10.0.20.102

Topology


trunk (802.1q tagged) port
ALL VLANs allowed
trunk (802.1q tagged) port
ALL VLANs allowed
VLAN 10
10.0.10.0/24
/24
Trunk Link
eth2
eth0
eth1
eth3
switch2
eth2
eth0
eth1
VLAN 10
client-1
eth0
10.0.10.101
VLAN 20
client-2
eth0
10.0.20.101
VLAN 10
client-3
eth0
10.0.10.102
VLAN 20
client-4
eth0
10.0.20.102

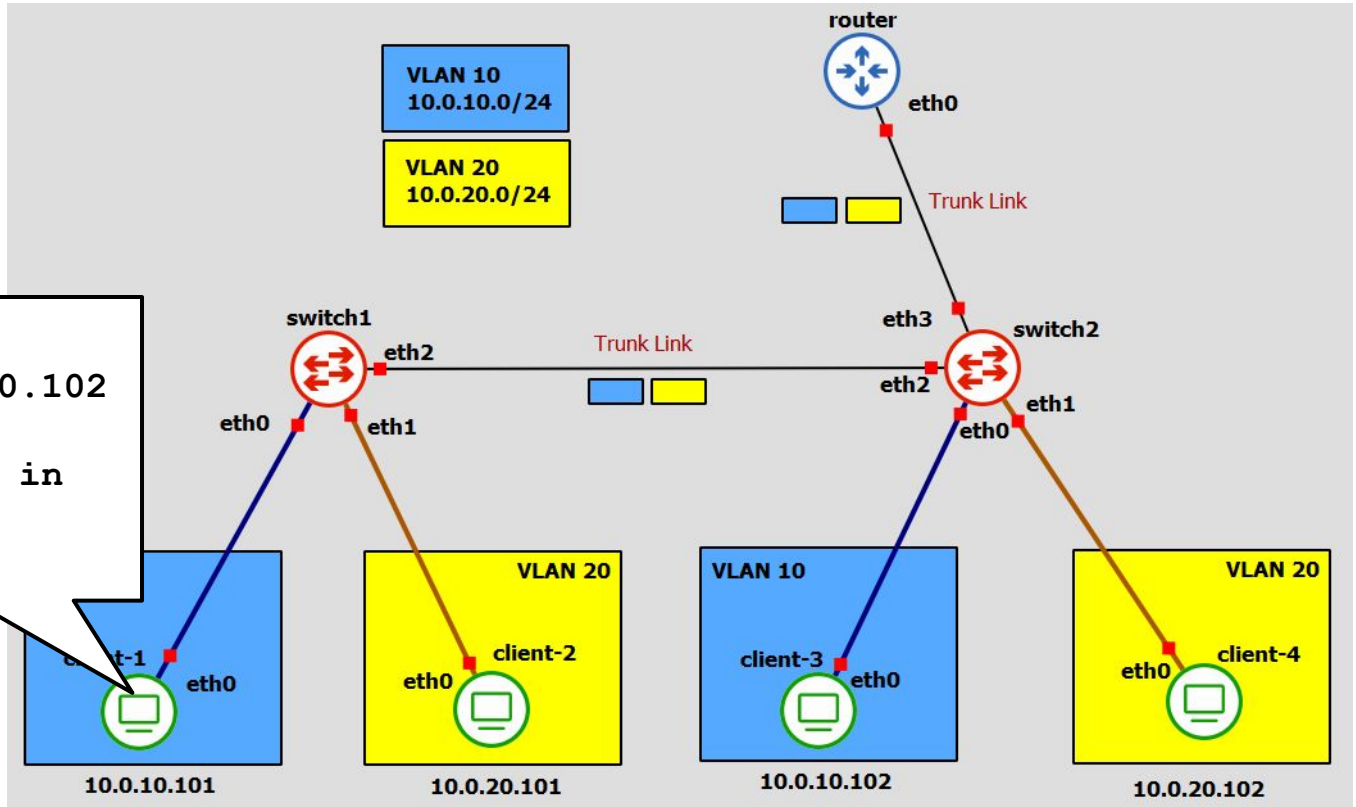
Topology



Router is our docker container (nsdcourse/basenet) acting as a router.
Router's interface is on a trunk link.
It receives packets from VLAN 10,20.
We need 2 802.1q aware VLAN subinterfaces (i.e. virtual interfaces).

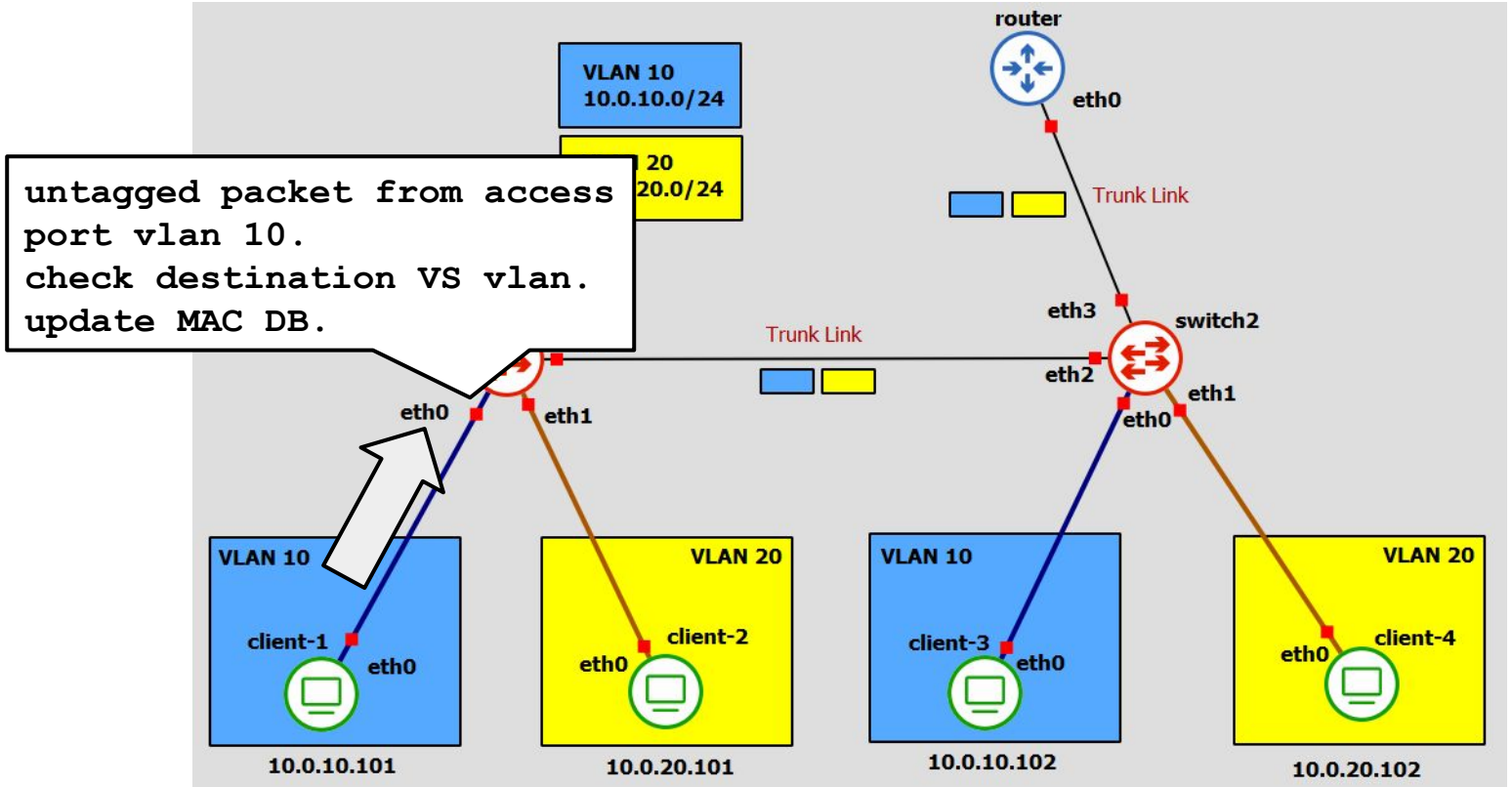
1. eth0.10 will be the default GW of VLAN 10
2. eth0.20 will be the default GW of VLAN 20

Forwarding Operations

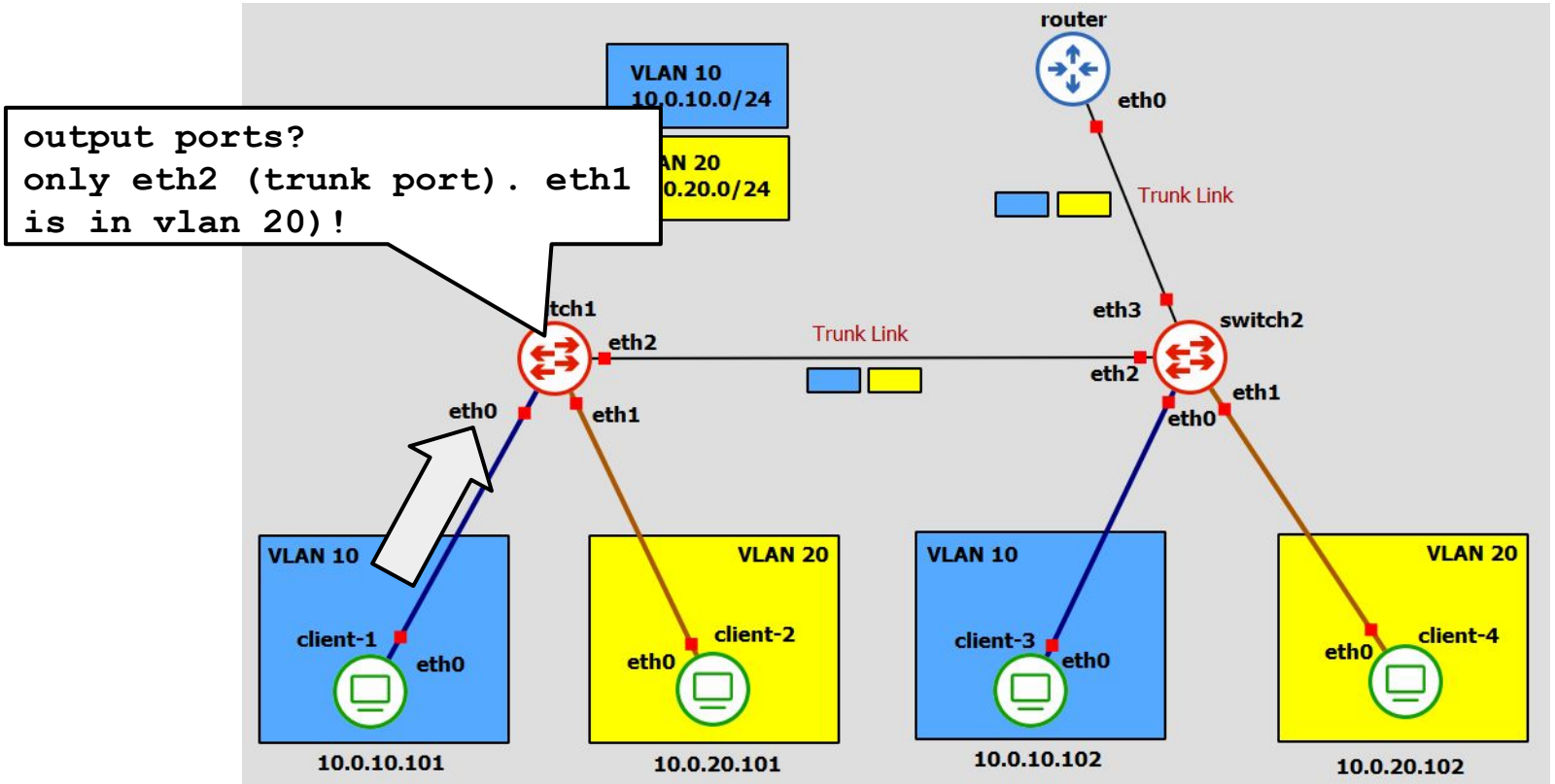



```
ping 10.0.10.102
(assuming
destination in
ARP cache)
```

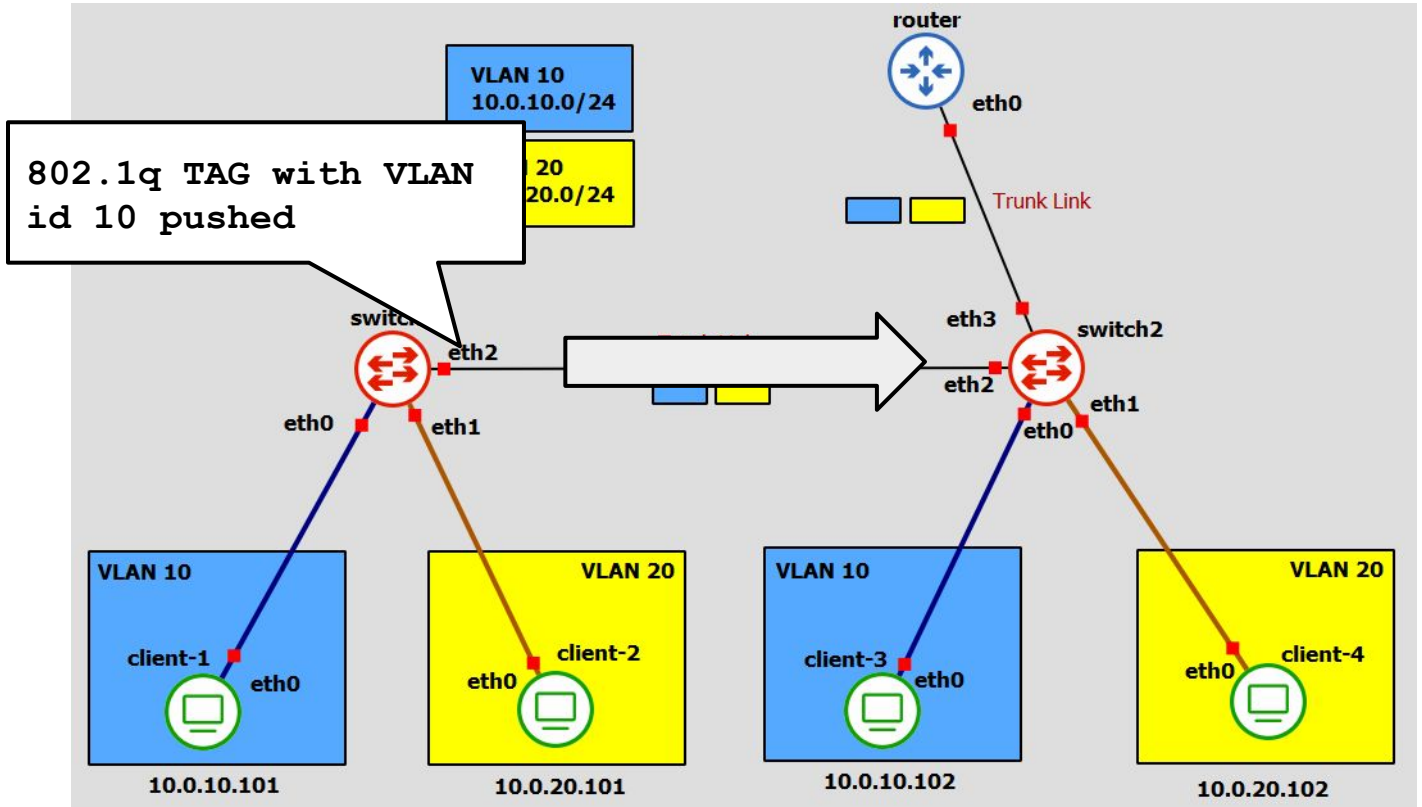
Forwarding Operations



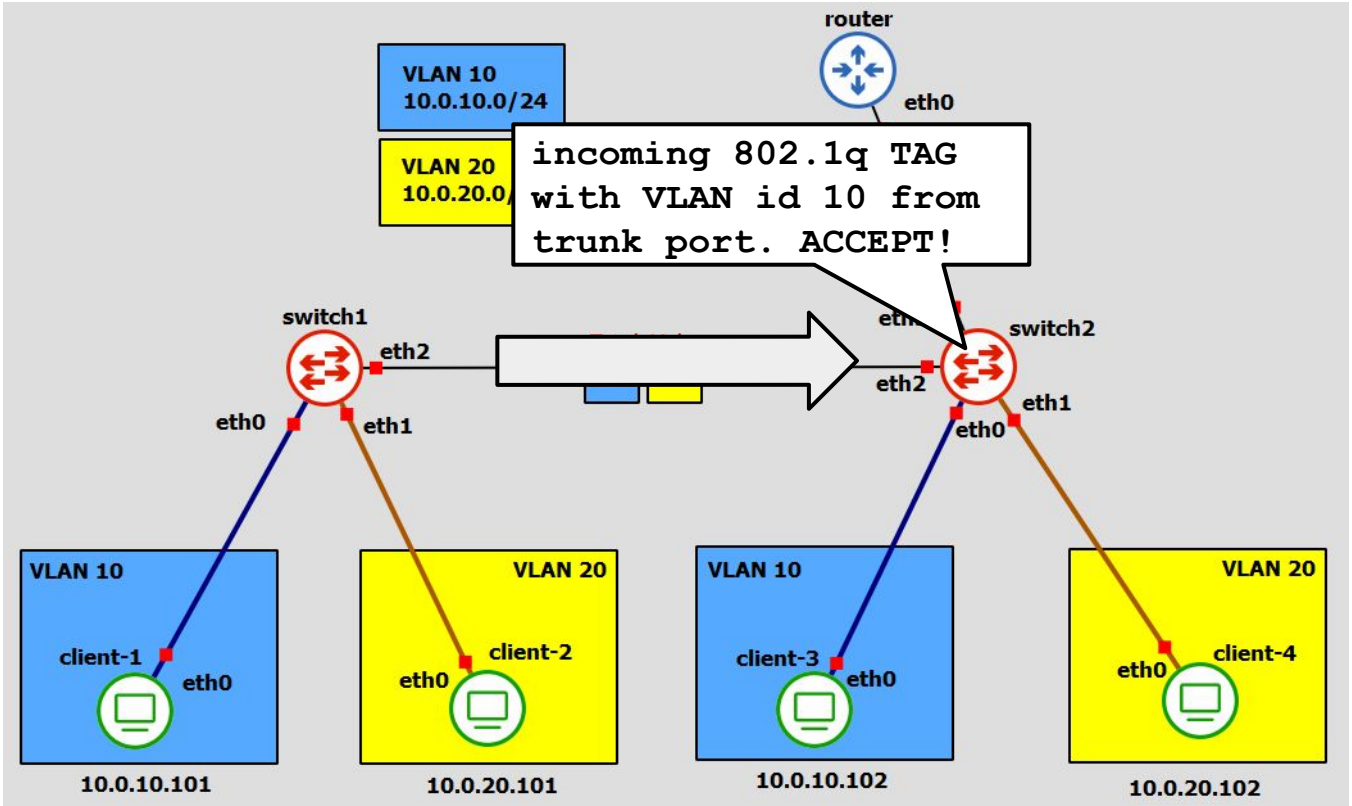
Forwarding Operations



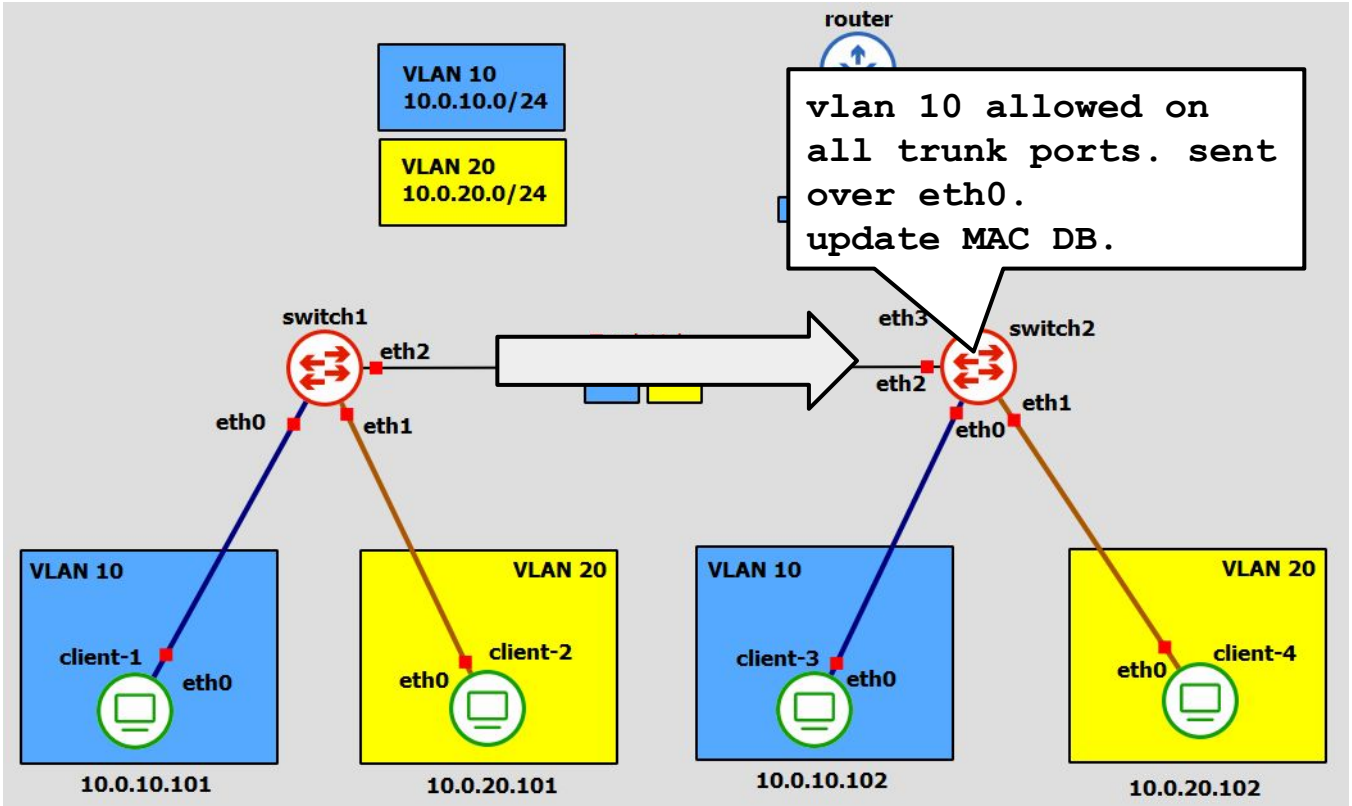
Forwarding Operations



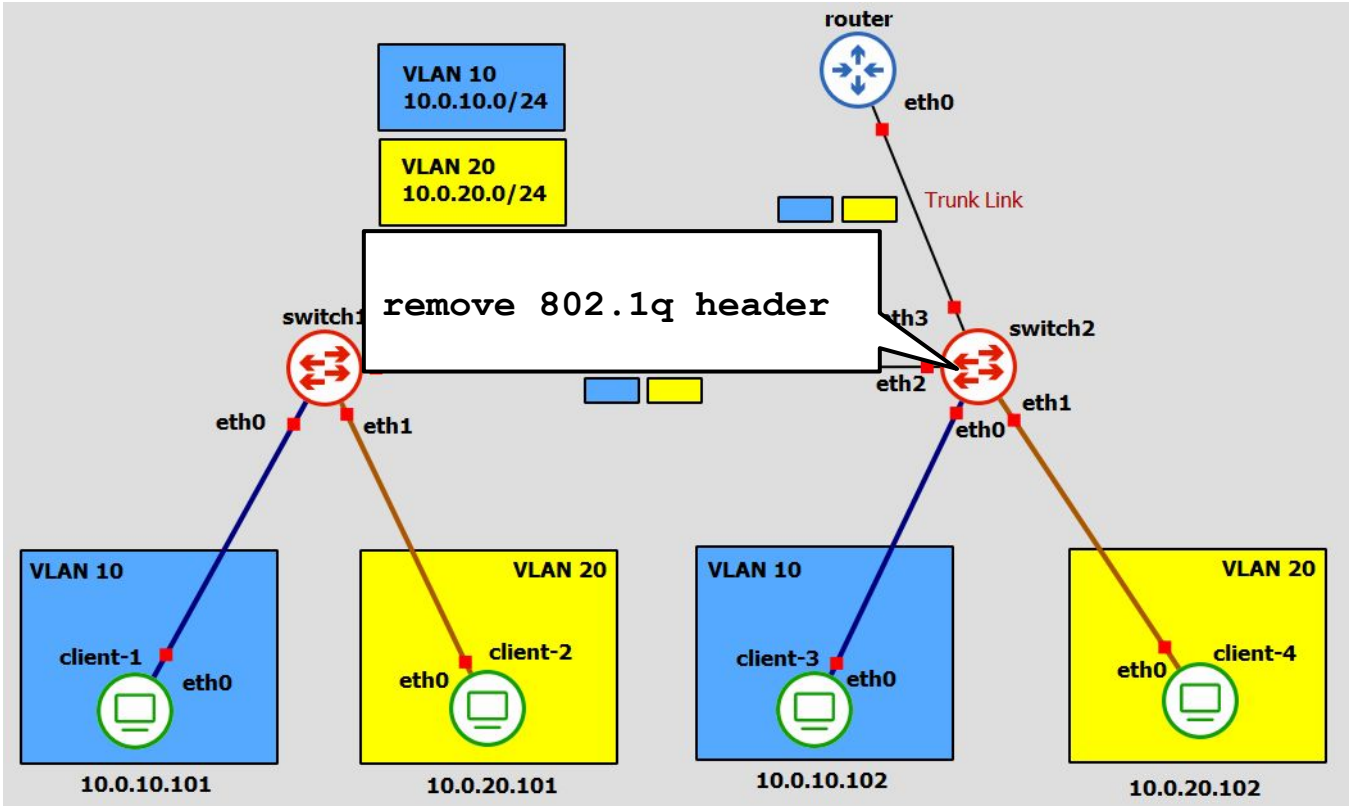
Forwarding Operations



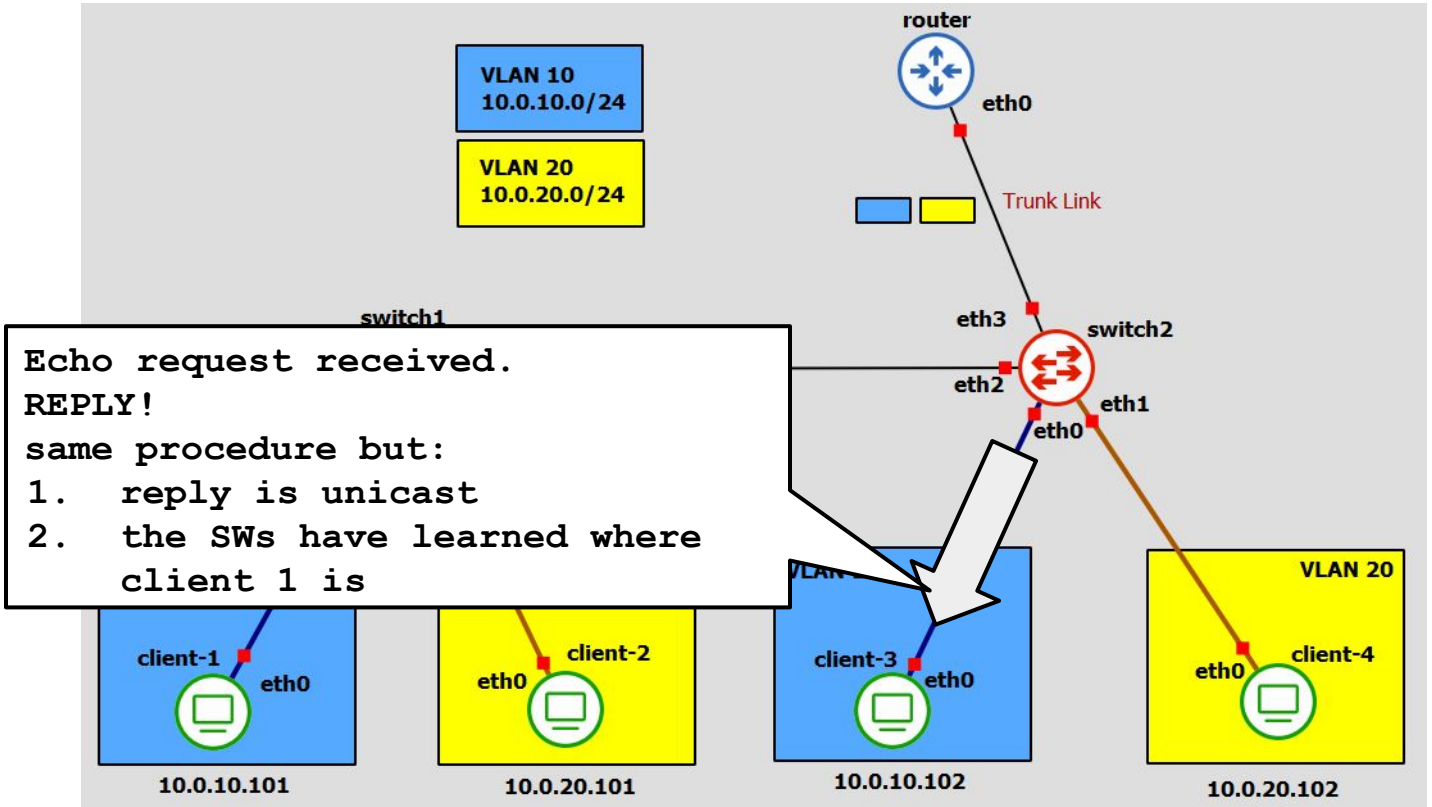
Forwarding Operations



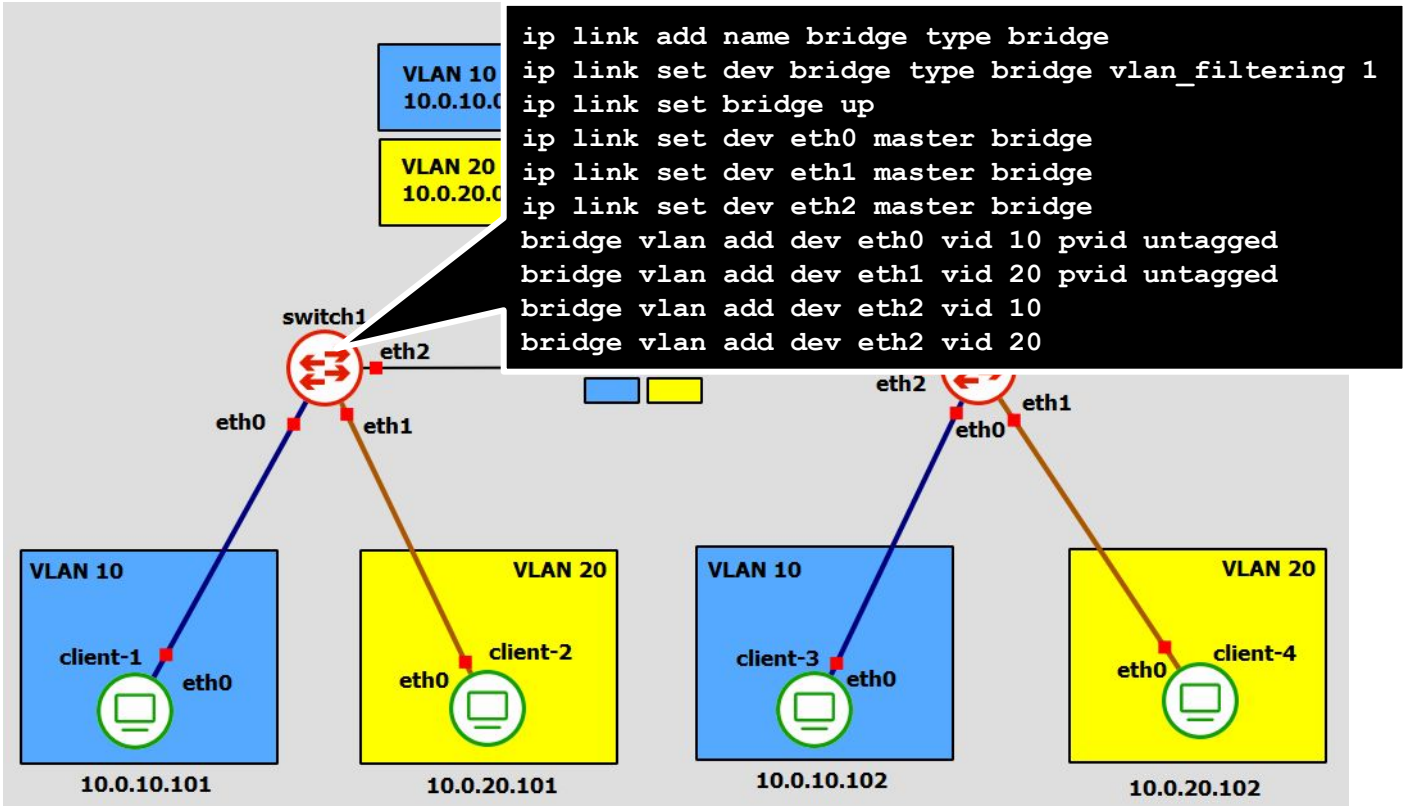
Forwarding Operations



Forwarding Operations

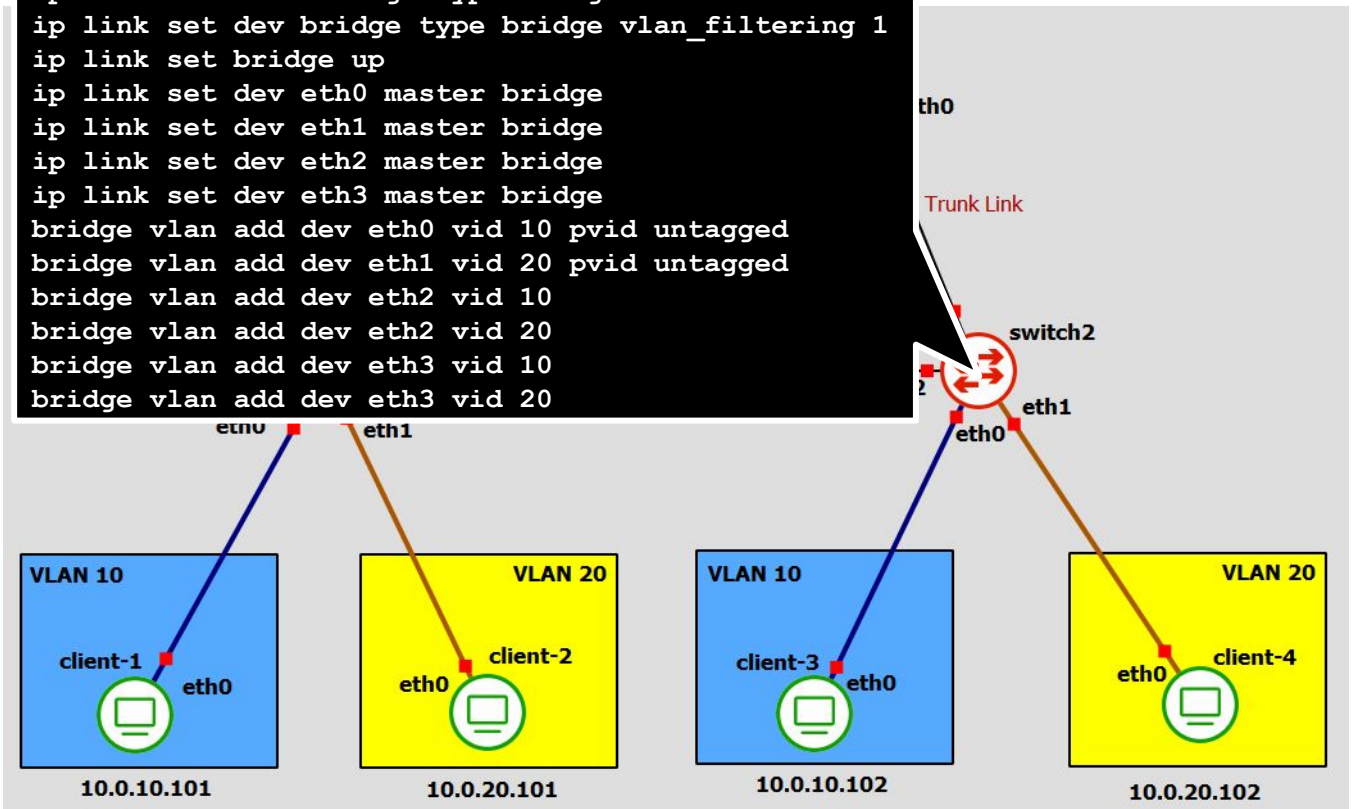


Configuration

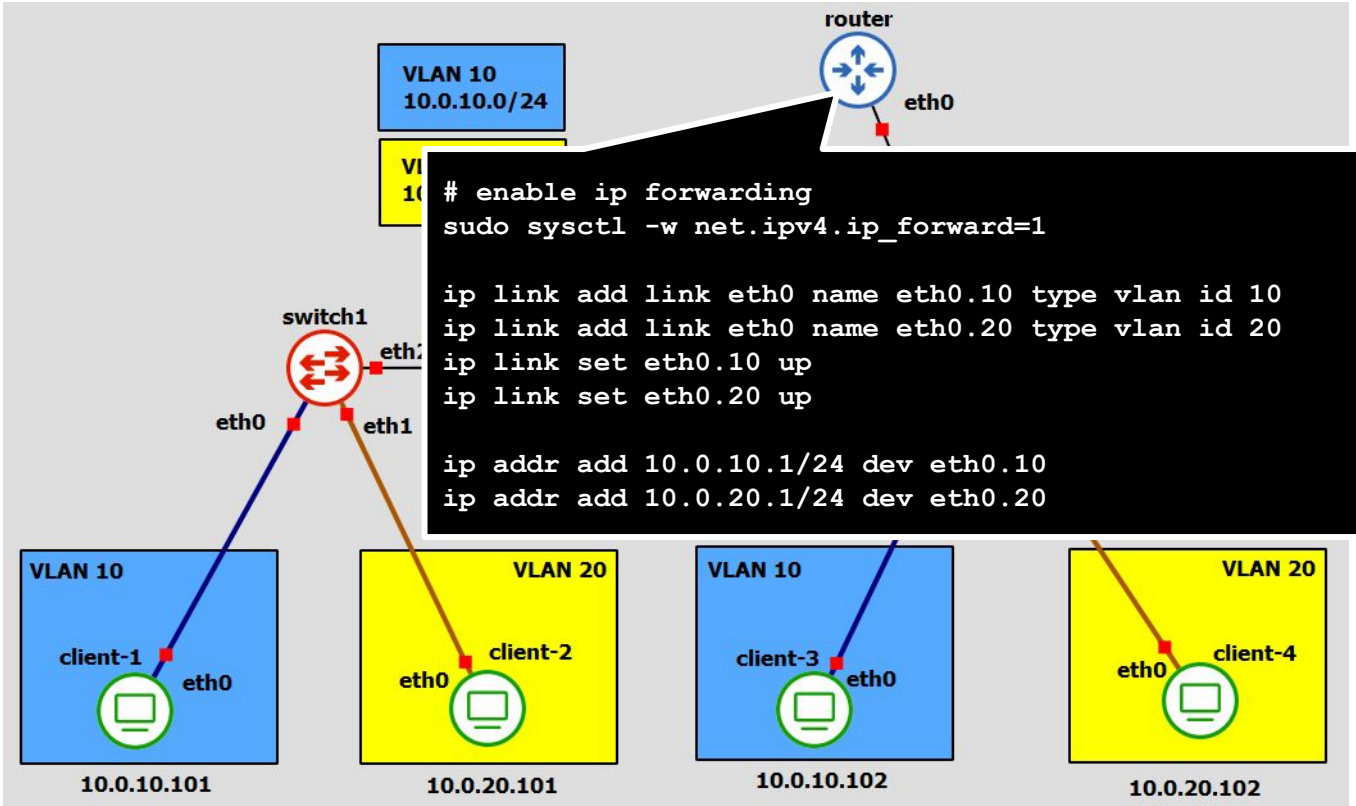


Configuration

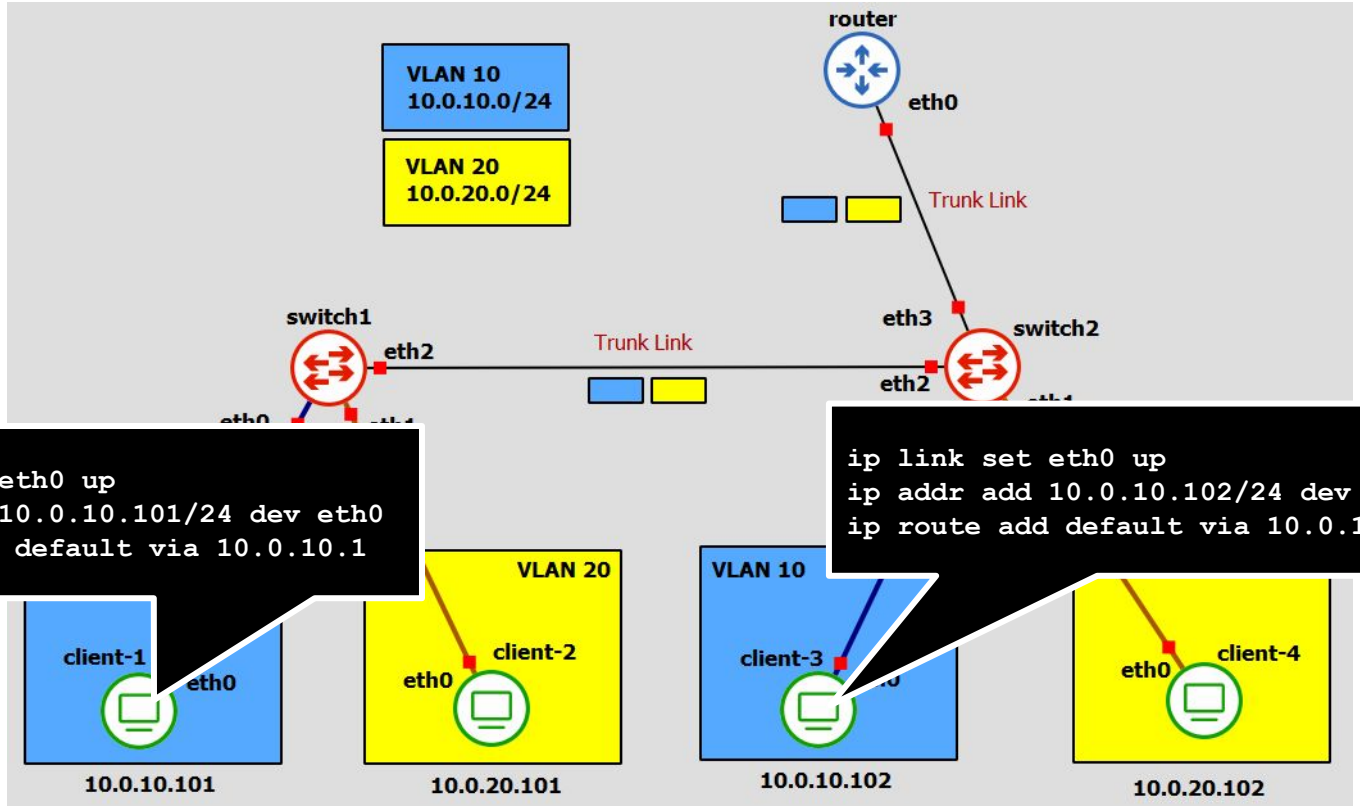
```
ip link add name bridge type bridge
ip link set dev bridge type bridge vlan_filtering 1
ip link set bridge up
ip link set dev eth0 master bridge
ip link set dev eth1 master bridge
ip link set dev eth2 master bridge
ip link set dev eth3 master bridge
bridge vlan add dev eth0 vid 10 pvid untagged
bridge vlan add dev eth1 vid 20 pvid untagged
bridge vlan add dev eth2 vid 10
bridge vlan add dev eth2 vid 20
bridge vlan add dev eth3 vid 10
bridge vlan add dev eth3 vid 20
```



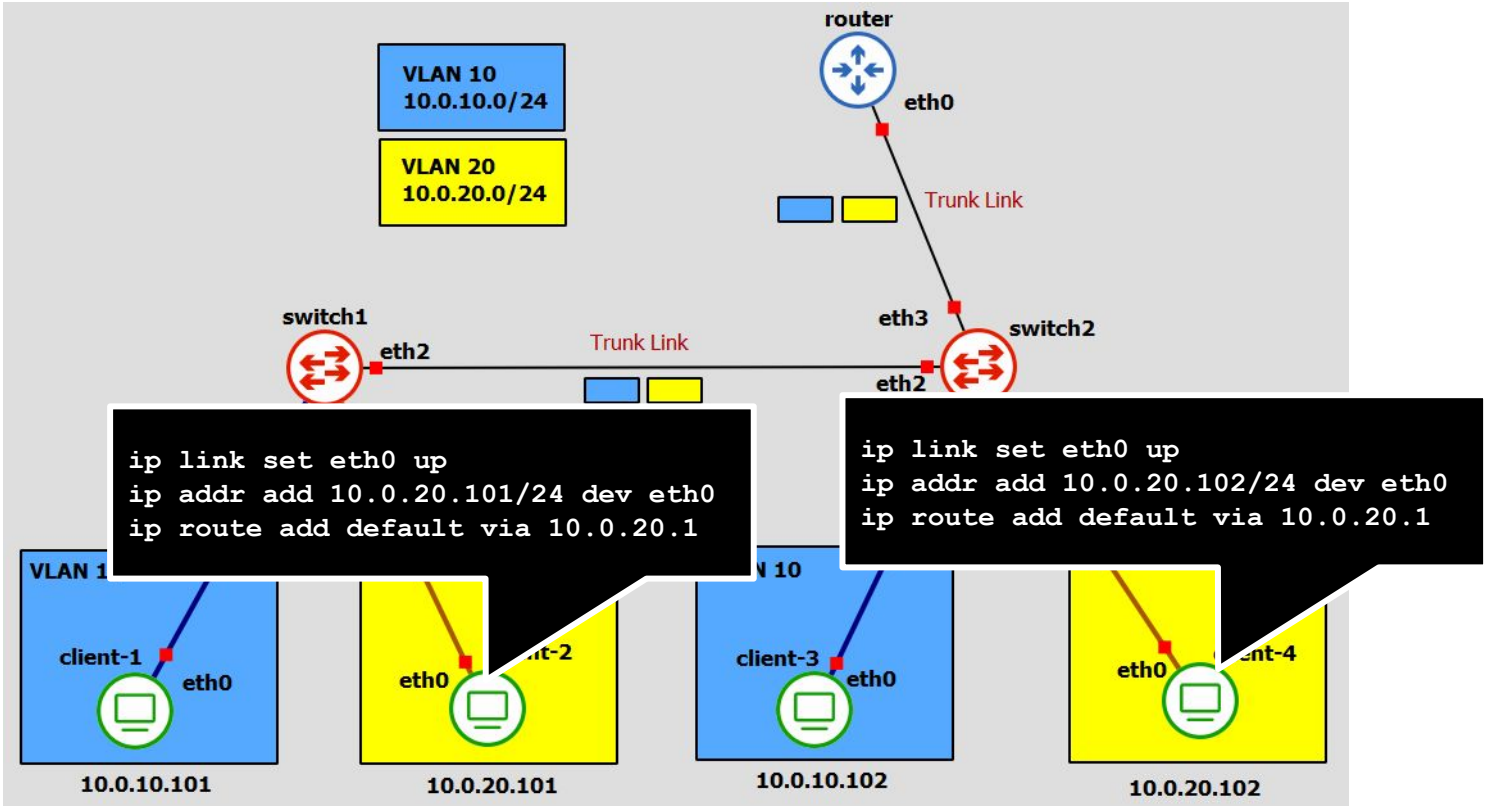
Configuration



Configuration



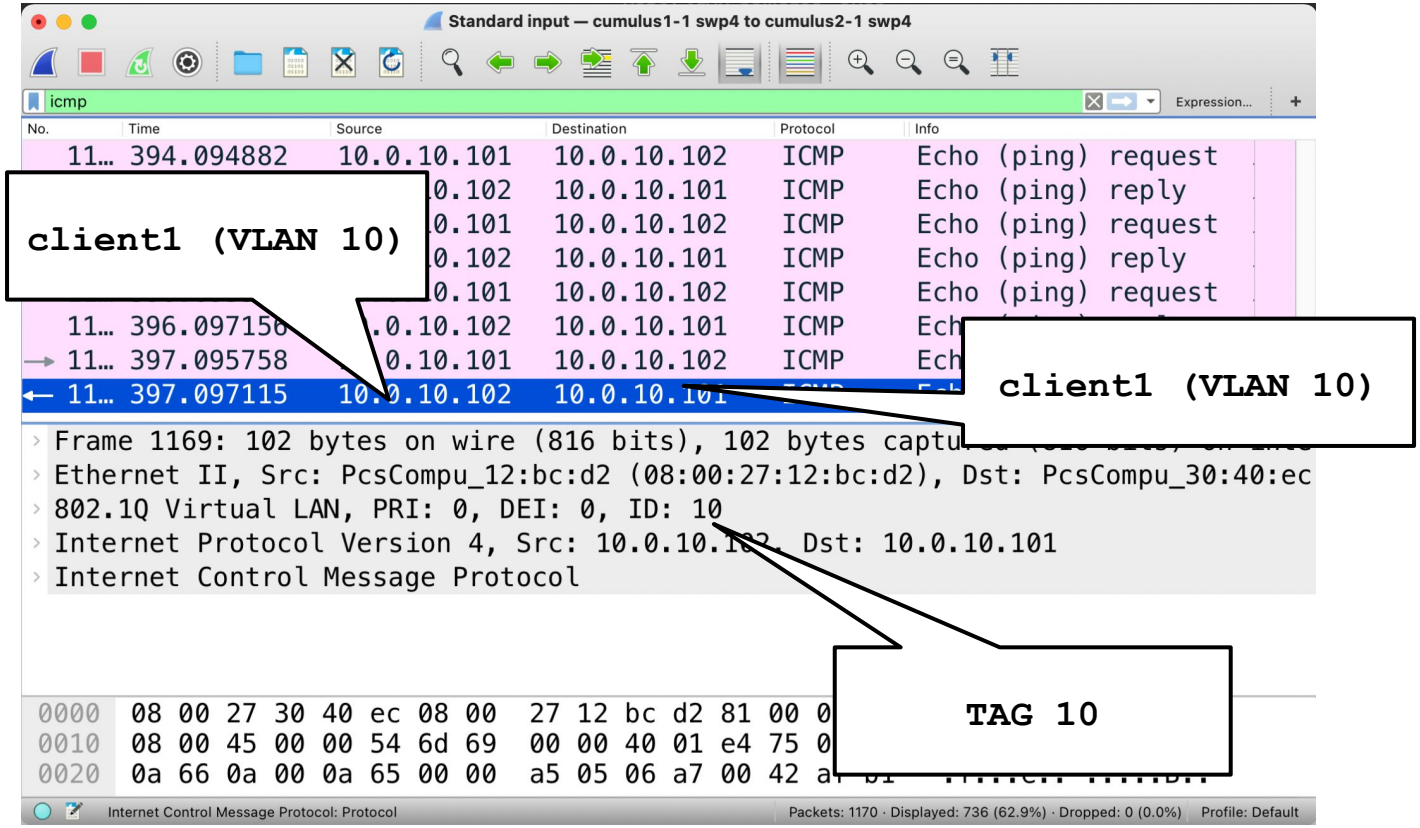
Configuration



Check the actual VLAN separation

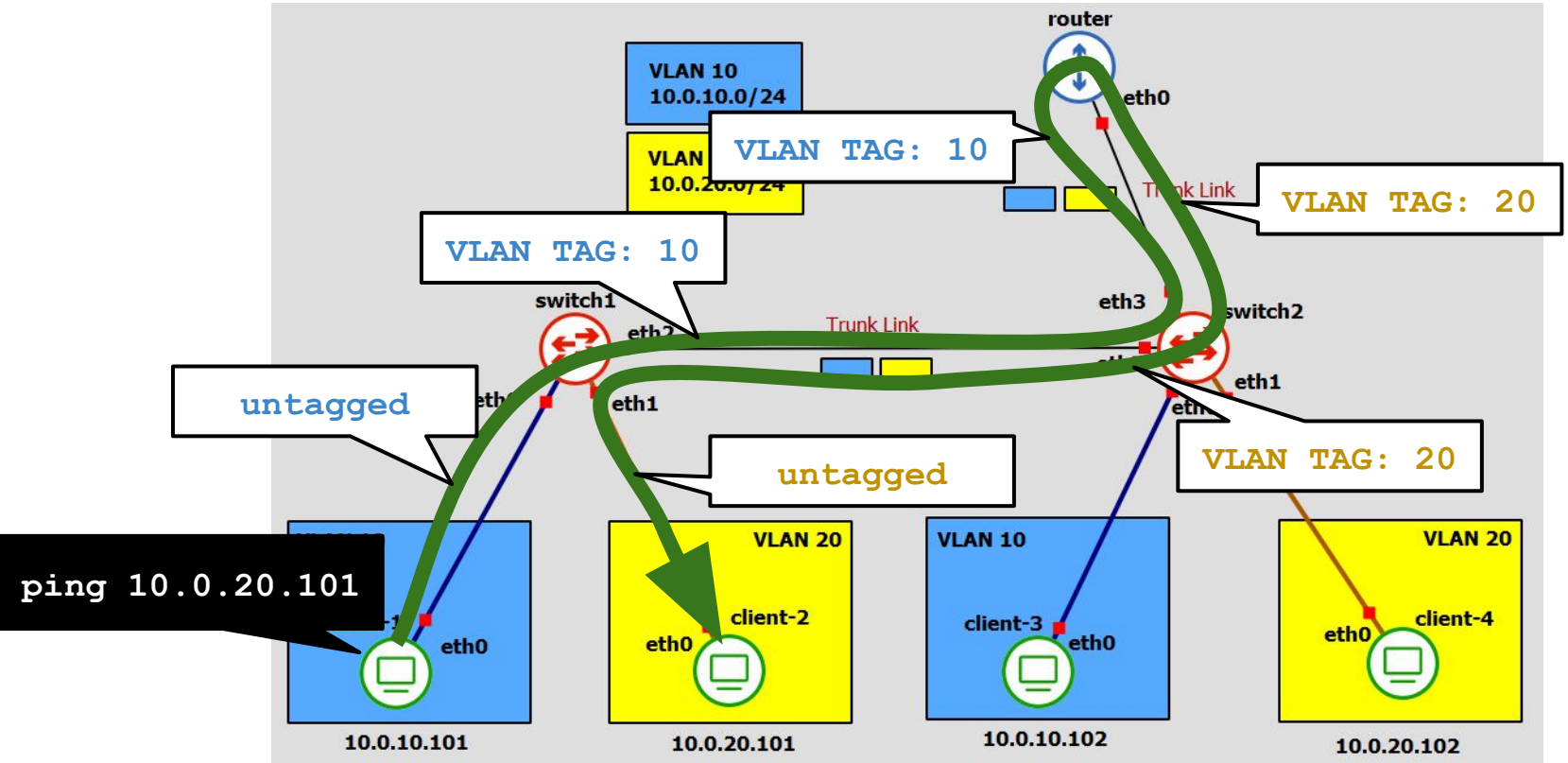
1. broadcast packets from client1 only visible by client3
2. trunk link correctly tag the packet from client1 to client2
3. for inter-VLAN communication we need IP forwarding!

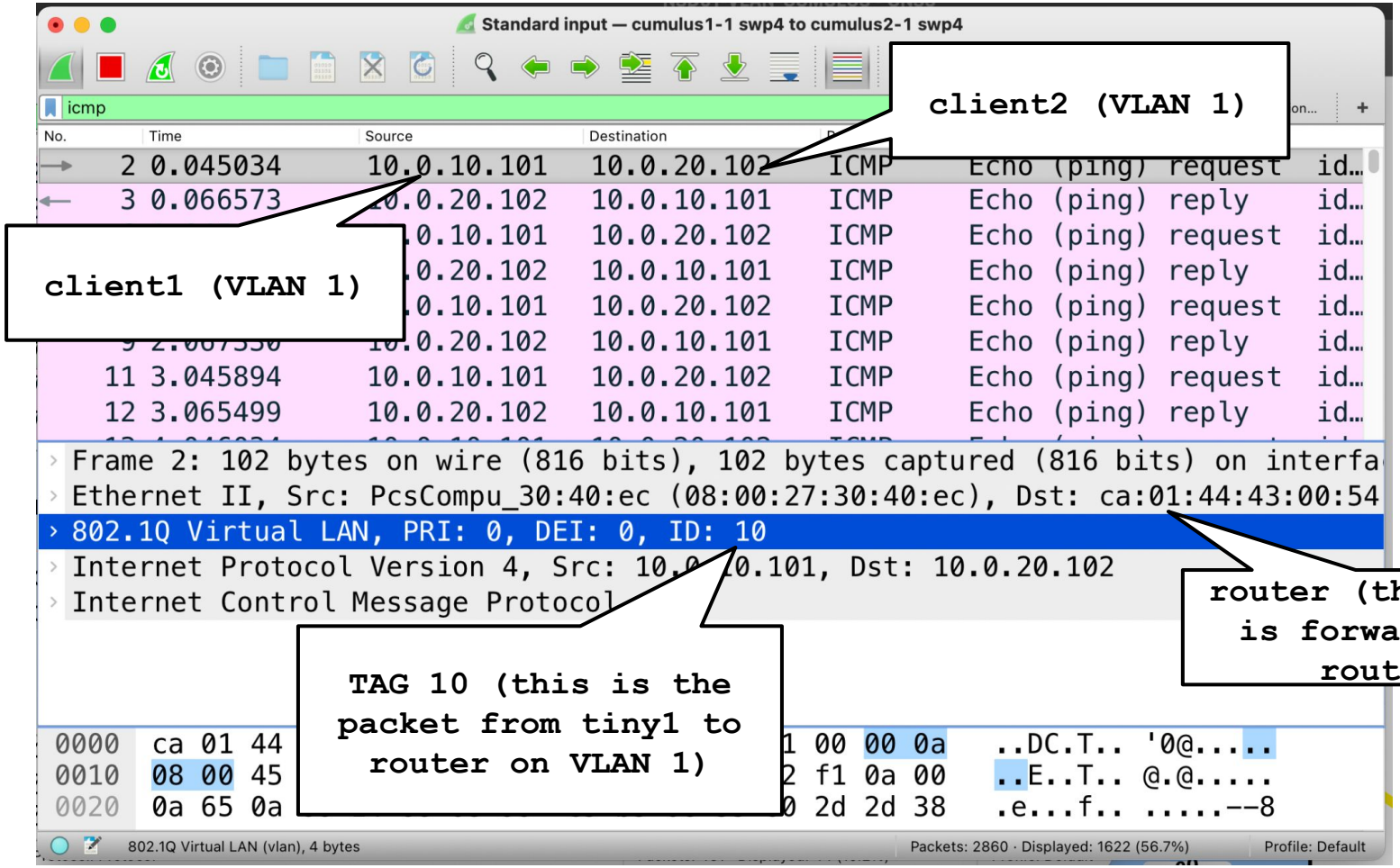
further check: statically bind an IP in VLAN 10 to client2 MAC address. ping this IP address. You will see packets in the link between switch1 and client2



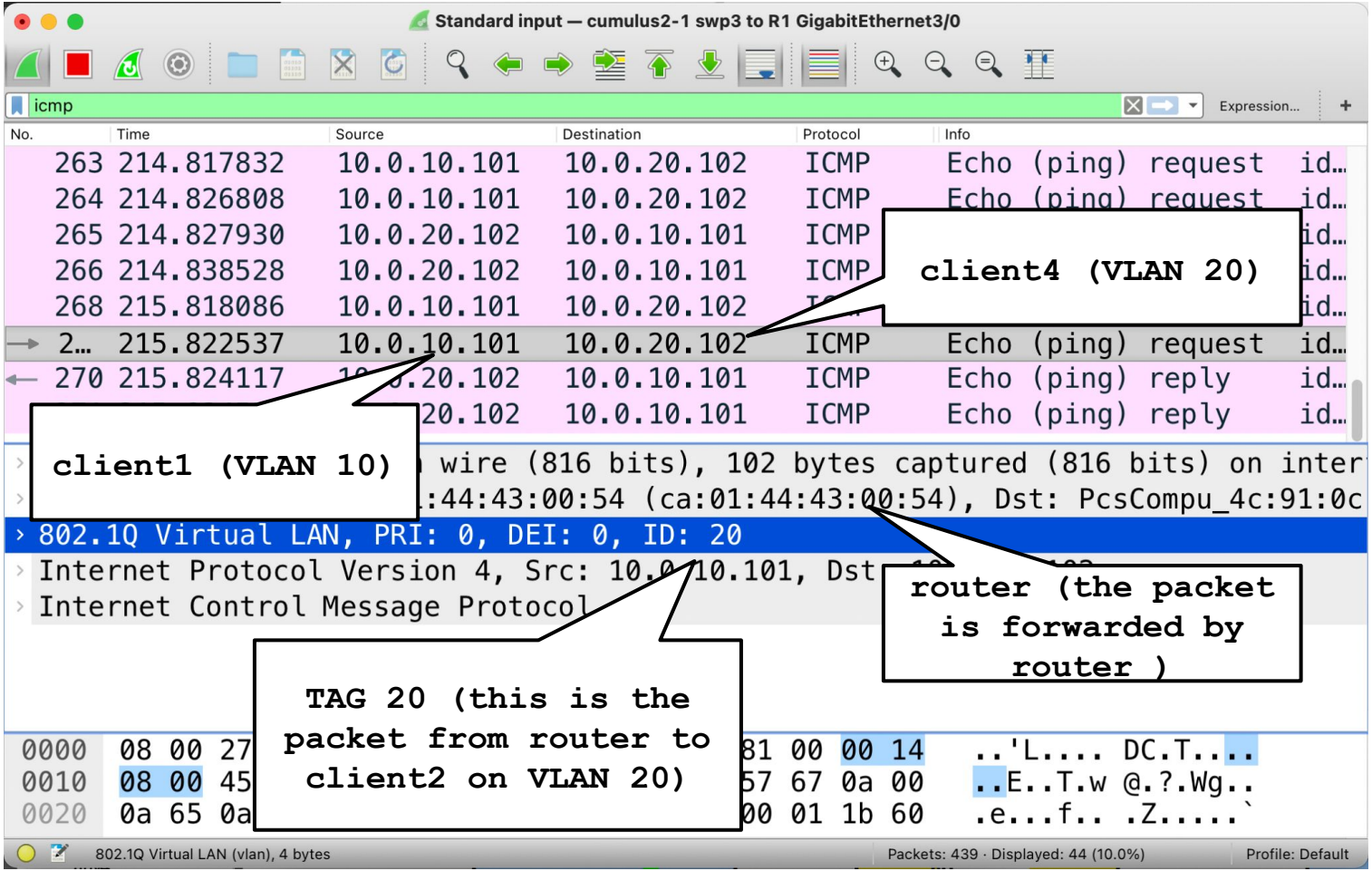
tagged packet on the trunk link between switch1 and switch2

Communicating between VLANs? Only via R1!!!





tagged packet on the trunk link between switch1 and switch2



tagged packet on the trunk link between router and switch2

VLAN Security

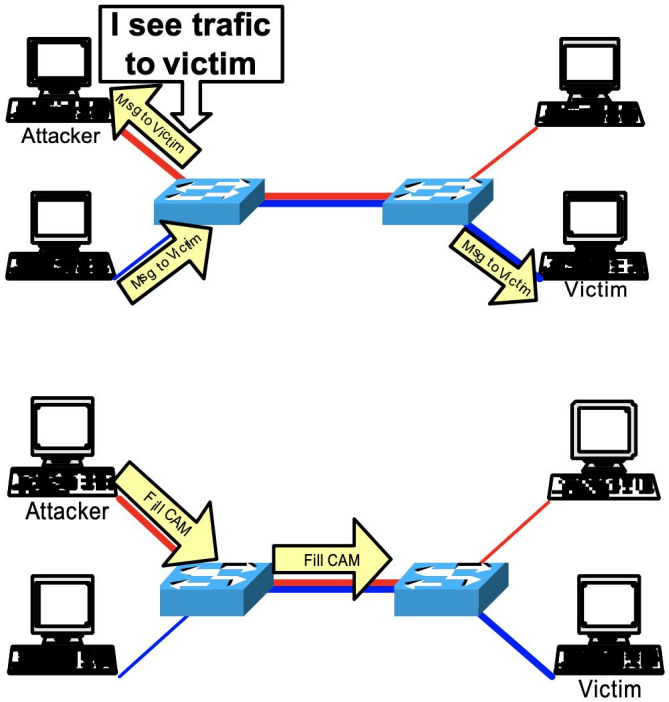
Based on “Rouiller, Steve A. "Virtual LAN Security: weaknesses and countermeasures” URL:
https://www.sans.org/reading-room/whitepapers/networkdevs/virtual-lan-security-weaknesses-countermeasures-1090

LAYER 2 attacks landscape

- ❏ Media Access Control (MAC) attack ***(same as with no VLANs)***
- ❏ BASIC VLAN Hopping attack
- ❏ Double Encapsulation VLAN Hopping attack
- ❏ Address Resolution Protocol (ARP) attack ***(same as with no VLANs)***
- ❏ Spanning Tree Attack ***(same as with no VLANs)***
- ❏ VLAN Trunking Protocol attack
- ❏ Cisco Discovery Protocol (CDP) Attack
- ❏ Private VLAN (PVLAN) attack

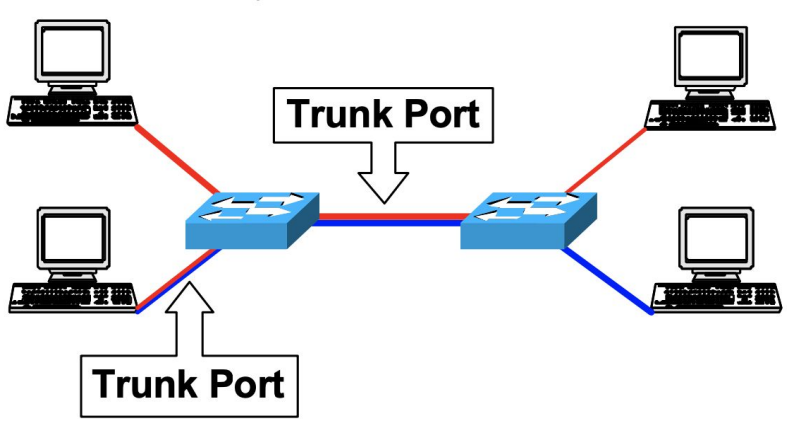
Media Access Control (MAC) Attack

- This attack is based on ***Content Addressable Memory (CAM) Overflow***
- The CAM Table stores information such as MAC addresses available on physical ports with their associated VLAN parameters.
- CAM Tables have fixed size.
- Once the table is full, the traffic without CAM entry, floods on the local VLAN
- The MAC flooding attack can be mitigated by using the ***port-security*** features.
  - This allows to specify MAC addresses for each port or to learn a certain number of MAC addresses per port.



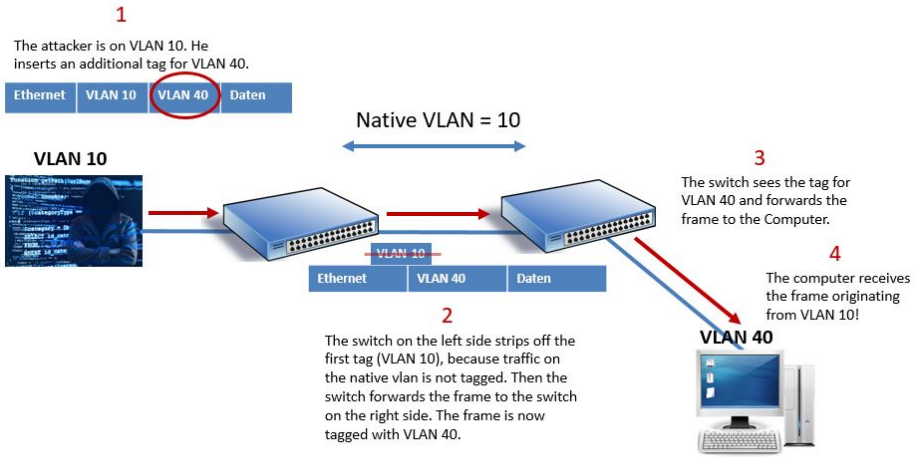
Basic VLAN Hopping attack

- This attack is based on ***Dynamic Trunk Protocol*** (DTP) DTP is used for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q) to be used.
- Cisco has fixed this with the new version of IOS and CATOS.
- As shown in the Figure, a station can spoof as a switch with 802.1Q signalling (using a rogue DTP frame). The station is then member of all VLANs.
- It requires a trunking favorable setting on the port
  - DTP enabled on the port
  - or in general it assumes an enabled trunk port



Double Encapsulation VLAN Hopping attack

- ***Double Tagging*** can only be exploited on switch ports configured to use native VLANs. Trunk ports configured with a native VLAN don't apply a VLAN tag when sending these frames.
- An attacker sends a double encapsulated 802.1Q frame with ***first TAG = native VLAN TAG***
- The first switch strips off the first encapsulation and then sends it back out
- The second switch strips off the second encapsulation and sends the frame to another VLAN ID.
- With this attack, the attacker can only send packets, and not receive them (***Unidirectional traffic only)***.
- As the attacker requires a trunking favorable setting on the port
  - on some implementations it also works with the attacker connected to an access port



to defeat this attack:

1. the administrator should disable Auto-trunking
2. use dedicated VLANID for all trunk ports. The administrator mustn't use VLAN 1 for anything

Address Resolution Protocol (ARP) attack

- We already talked about this…
  - this attack affects also VLAN environments
- A way to mitigate the attack is to use the ***port-security*** features
- Administrators have to consider static ARP for critical routers and hosts
- IDS systems could be tuned to watch for unusually high amounts of ARP traffic
- There are also tools which track IP/MAC address pairing (e.g. ARPWatch)

Spanning Tree Attack

- STP is used to maintain loop-free topologies in a redundant Layer 2 infrastructure
- Messages are sent using ***Bridge Protocol Data Units (BPDUs)***
- The attacker sends BPDUs which can force a Root bridge change and thus create a DoS condition on the network.
- The attacker also has the possibility to see frames he shouldn't.
- There are tools to replay this attack. The tool requires that the attacker be dual homed on two different switches
- A bad idea, in order to protect switches against this attack, is to disable STP, introducing loops would become another source of attack.
- There are two features on switches which are called ***BPDU Guard*** and ***Root Guard***.
  - BPDU Guard disables interfaces using portfast upon detection of a BPDU message on the interface (spanning-tree portfast bpduguard).
  - Root Guard disables interfaces who become the root bridge due to their BPDU advertisement (spanning-tree guard root).

VLAN Trunking Protocol attack (DoS)

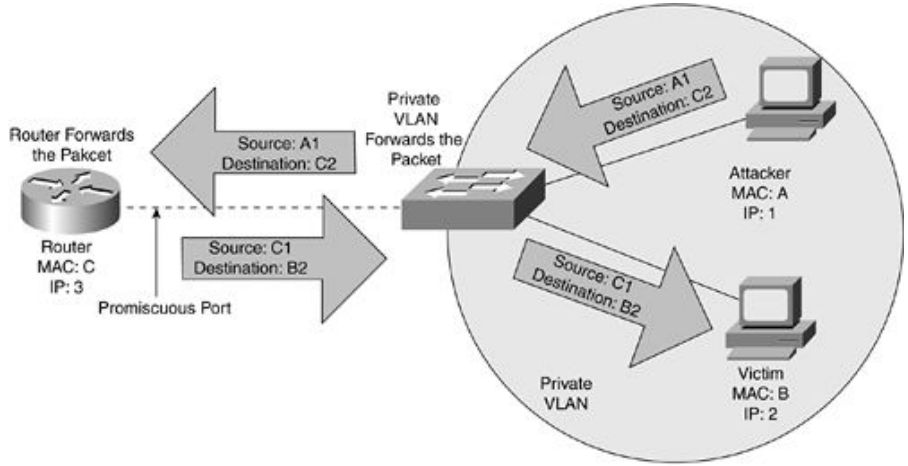
- VTP reduces administration in a switched network. When configuring a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain.
- VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst family products
- After negotiating a trunk port, an attacker could send VTP messages as a server with no VLANs configured
  - ***All VLANs would be deleted across the entire VTP domain***
- In order to avoid this, disable VTP (**`vtp mode transparent`**), or at least to use MD5 authentication (**`vtp domain <vtp.domain> password <password>`**)

Cisco Discovery Protocol (CDP) Attack

- ***Cisco Discovery Protocol*** allows Cisco devices to chat among one another. It can be used to learn possibly sensitive information (IP address, software version, router model,...). CDP is in cleartext and unauthenticated.
- Besides the information gathering benefit, CDP offers even more to an attacker; there was a vulnerability in CDP that allowed Cisco devices to run out of memory and potentially crash, if the attacker sends tons of bogus CDP packets to it.
- In order to mitigate this attack, consider disabling CDP (no cdp enable), or being very selective in its use in security sensitive environments (backbone vs. user interface may be a good distinction).

Private VLAN (PVLAN) attack

- ***PVLANs*** (also called protected ports) are used to isolated traffic in specific communities, to create distinct “networks” within a normal VLAN.
- Some applications require that no traffic is forwarded by the Layer 2 protocol between interfaces on the same switch.
  - In such an environment, there is no exchange of unicast, broadcast, or multicast traffic between interfaces on the switch, and traffic between interfaces on the same switch is forwarded through a Layer 3 device such as a router
- The attacker sends a frame with a rogue MAC address (the one of the Layer 3 device) but with the IP address of the victim. Thus the router will forward the packet to the victim. ***Intended PVLAN security is bypassed.***
  - With this attack, the attacker can only send packets, and not receive them
- In order to mitigate this attack, the administrator could setup an ingress ACL on the router interface, or use VLAN ACL



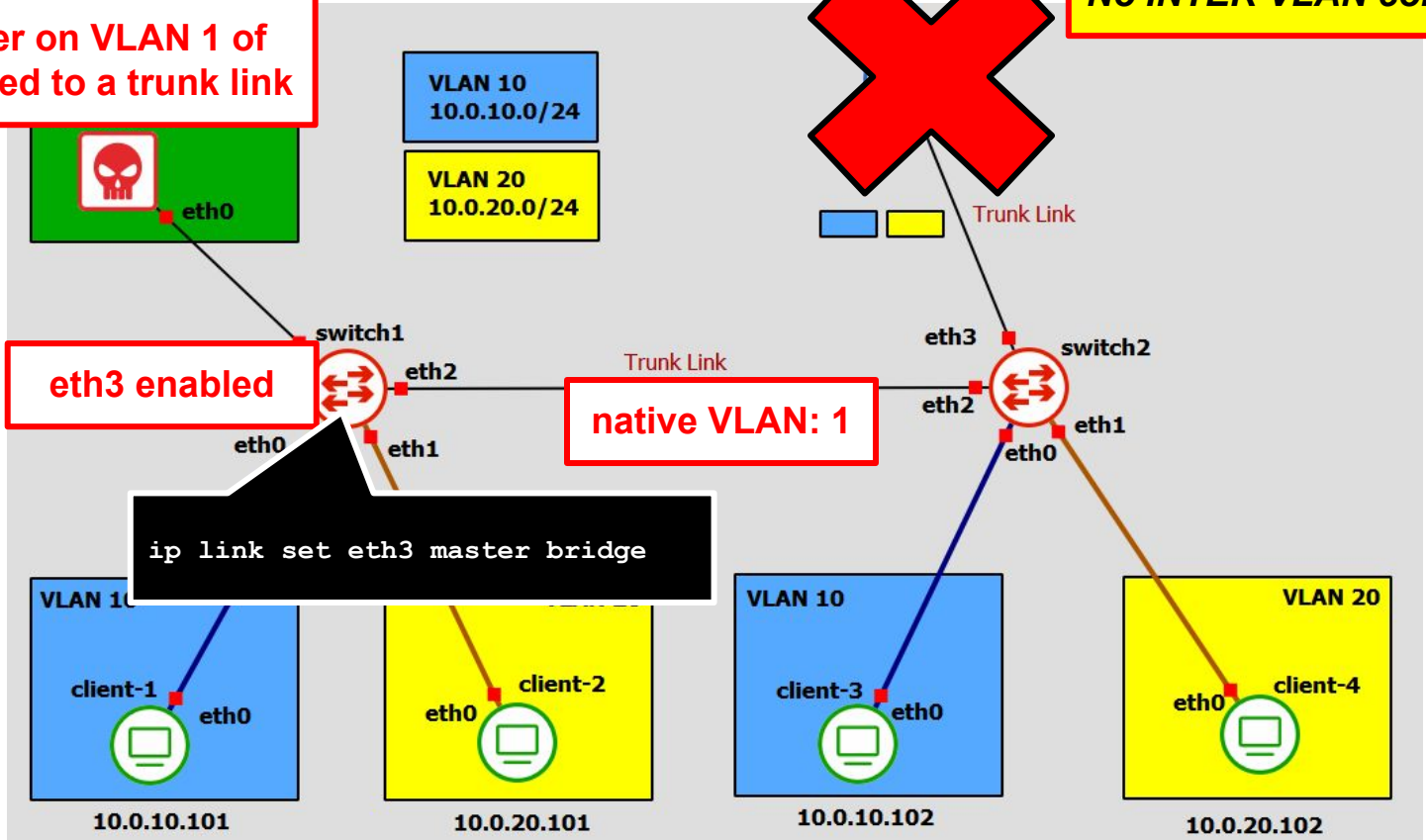
private VLAN further reading:
https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/private-vlans.html

Lab4: Double Tagging Attack

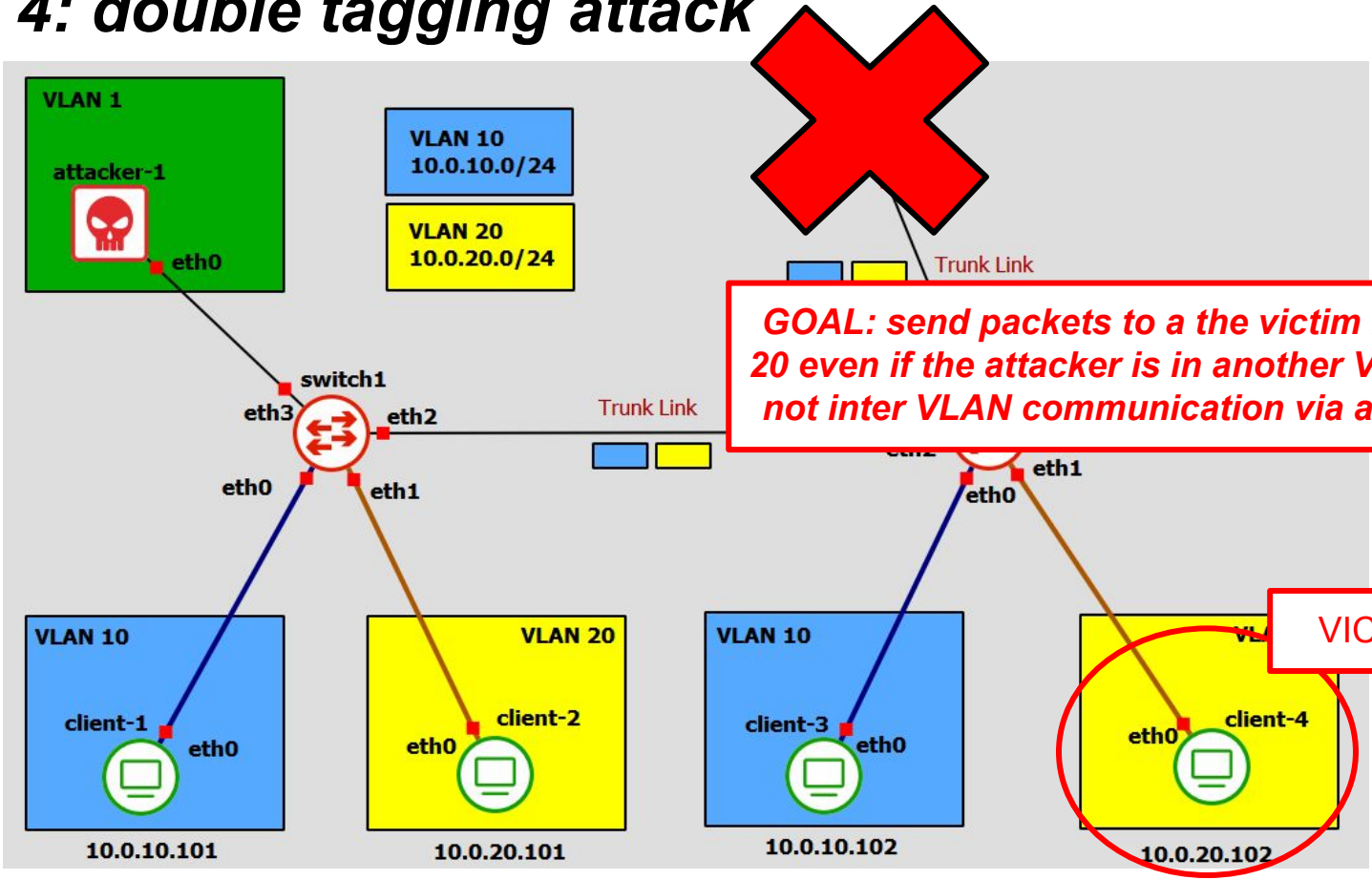
Lab 4: topology

attacker on VLAN 1 of connected to a trunk link

from lab 3 remove the router.
No INTER VLAN communication

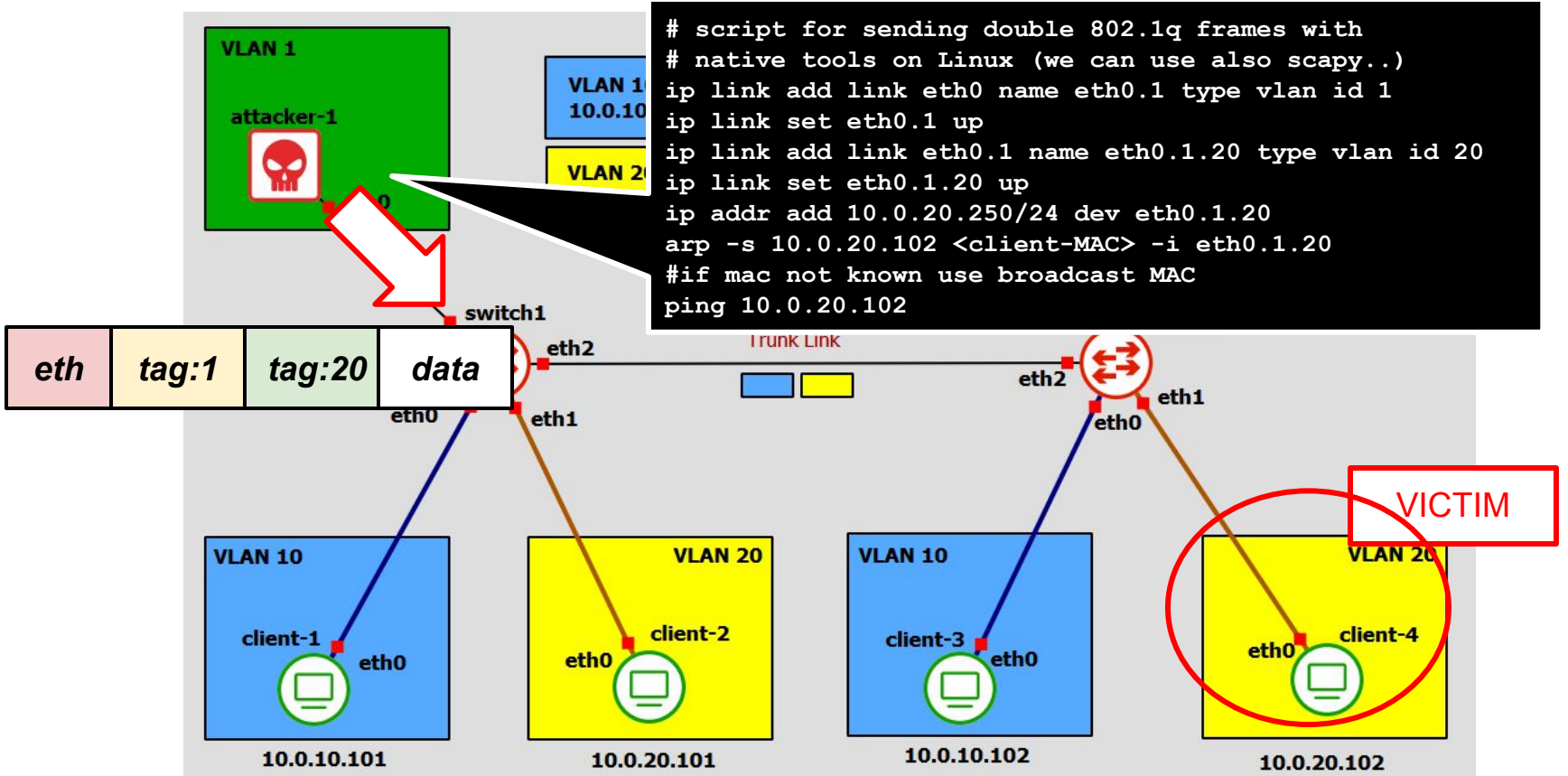


Lab 4: double tagging attack

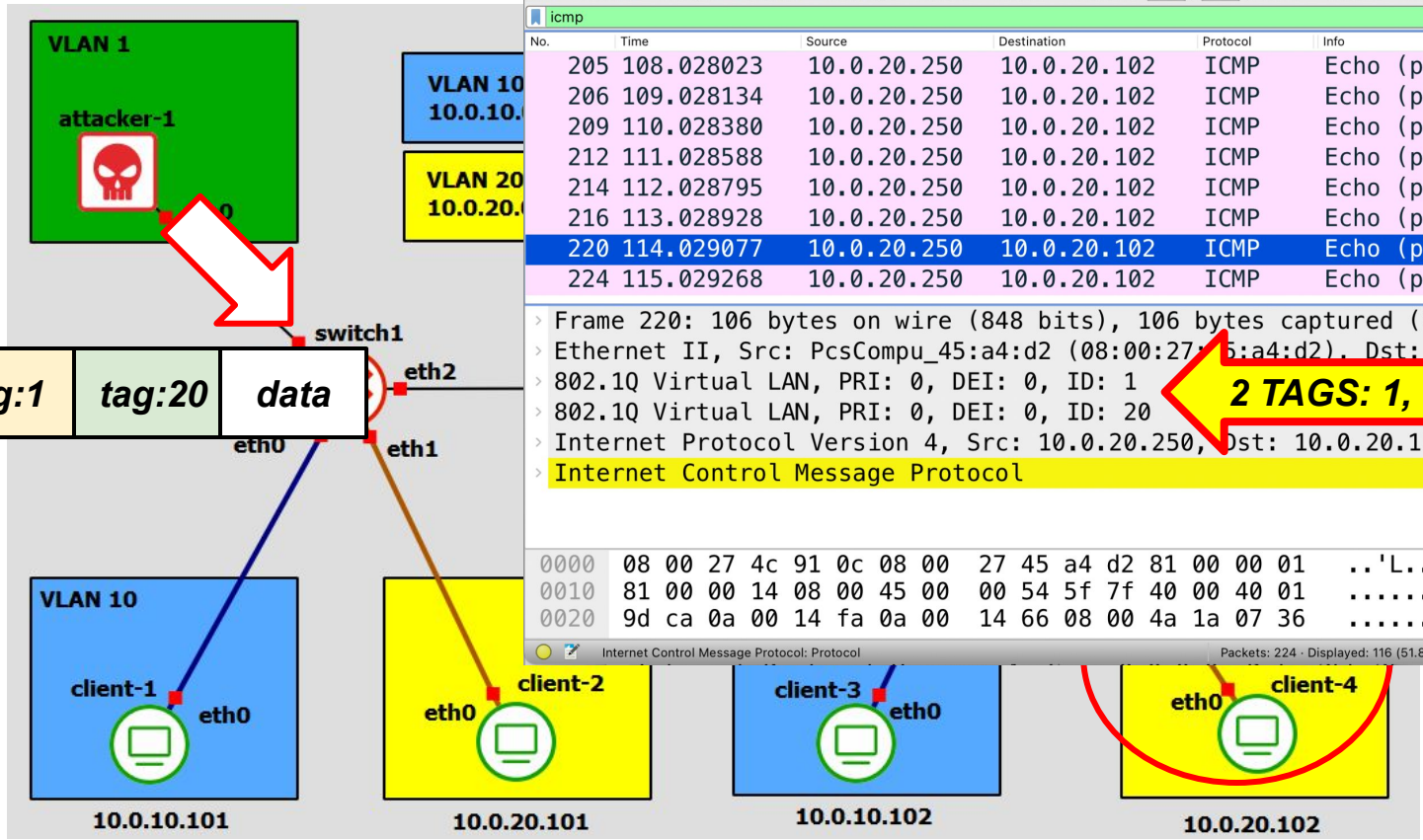


Lab 4: double tagging attack

```
# script for sending double 802.1q frames with
# native tools on Linux (we can use also scapy..)
ip link add link eth0 name eth0.1 type vlan id 1
ip link set eth0.1 up
ip link add link eth0.1 name eth0.1.20 type vlan id 20
ip link set eth0.1.20 up
ip addr add 10.0.20.250/24 dev eth0.1.20
arp -s 10.0.20.102 <client-MAC> -i eth0.1.20
#if mac not known use broadcast MAC
ping 10.0.20.102
```



Lab 4: double taggin



eth	tag:1	tag:20	data

Standard input — cumulus1-1 swp3 to tiny5-1 Ethernet0

icmp

No.	Time	Source	Destination	Protocol	Info
205	108.028023	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request
206	109.028134	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request
209	110.028380	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request
212	111.028588	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request
214	112.028795	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request
216	113.028928	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request
220	114.029077	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request
224	115.029268	10.0.20.250	10.0.20.102	ICMP	Echo (ping) request

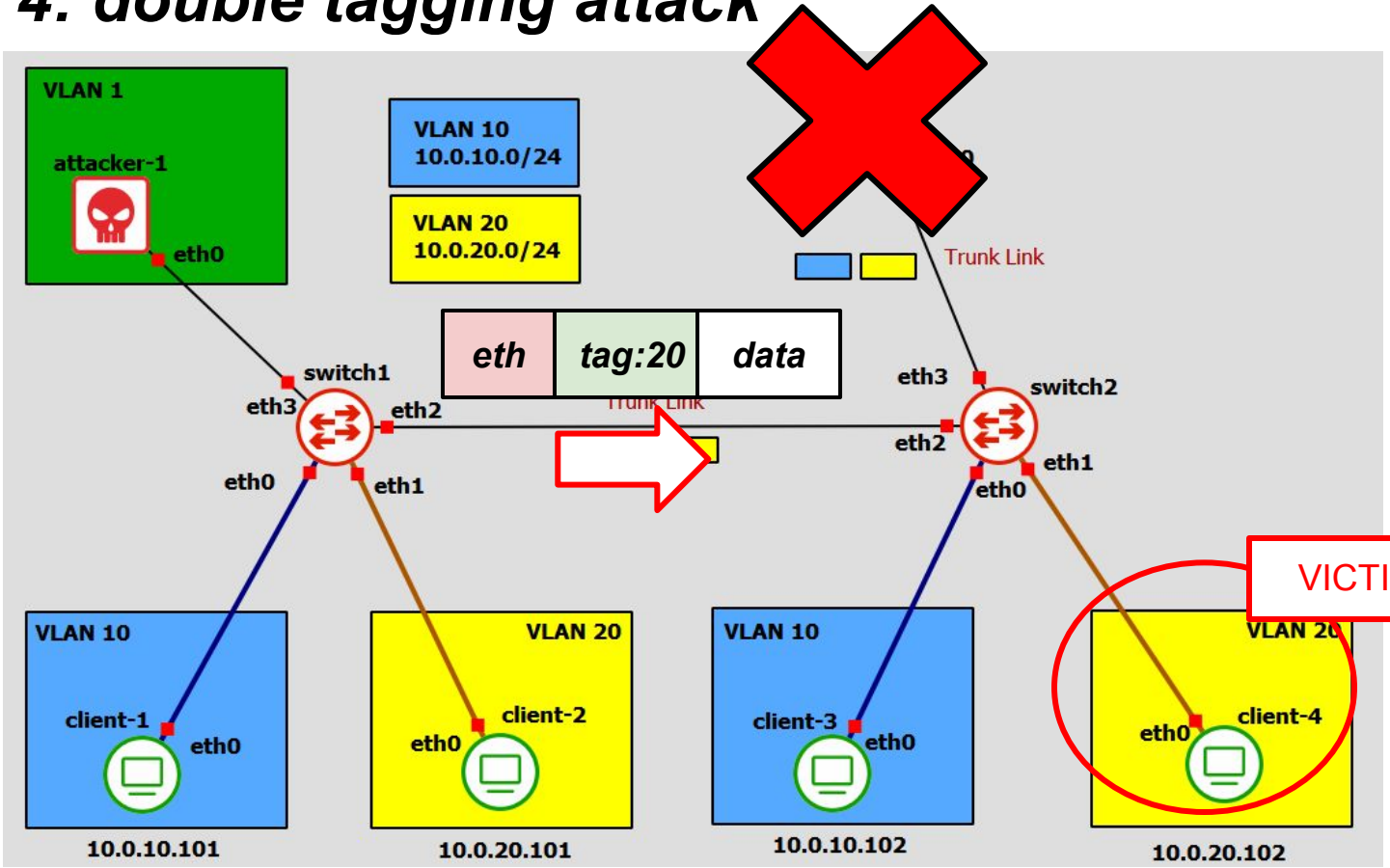
```
Frame 220: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on inter
Ethernet II, Src: PcsCompu_45:a4:d2 (08:00:27:45:a4:d2), Dst: PcsCompu_4c:91:0c
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 20
Internet Protocol Version 4, Src: 10.0.20.250, Dst: 10.0.20.102
Internet Control Message Protocol
```

2 TAGS: 1, 20

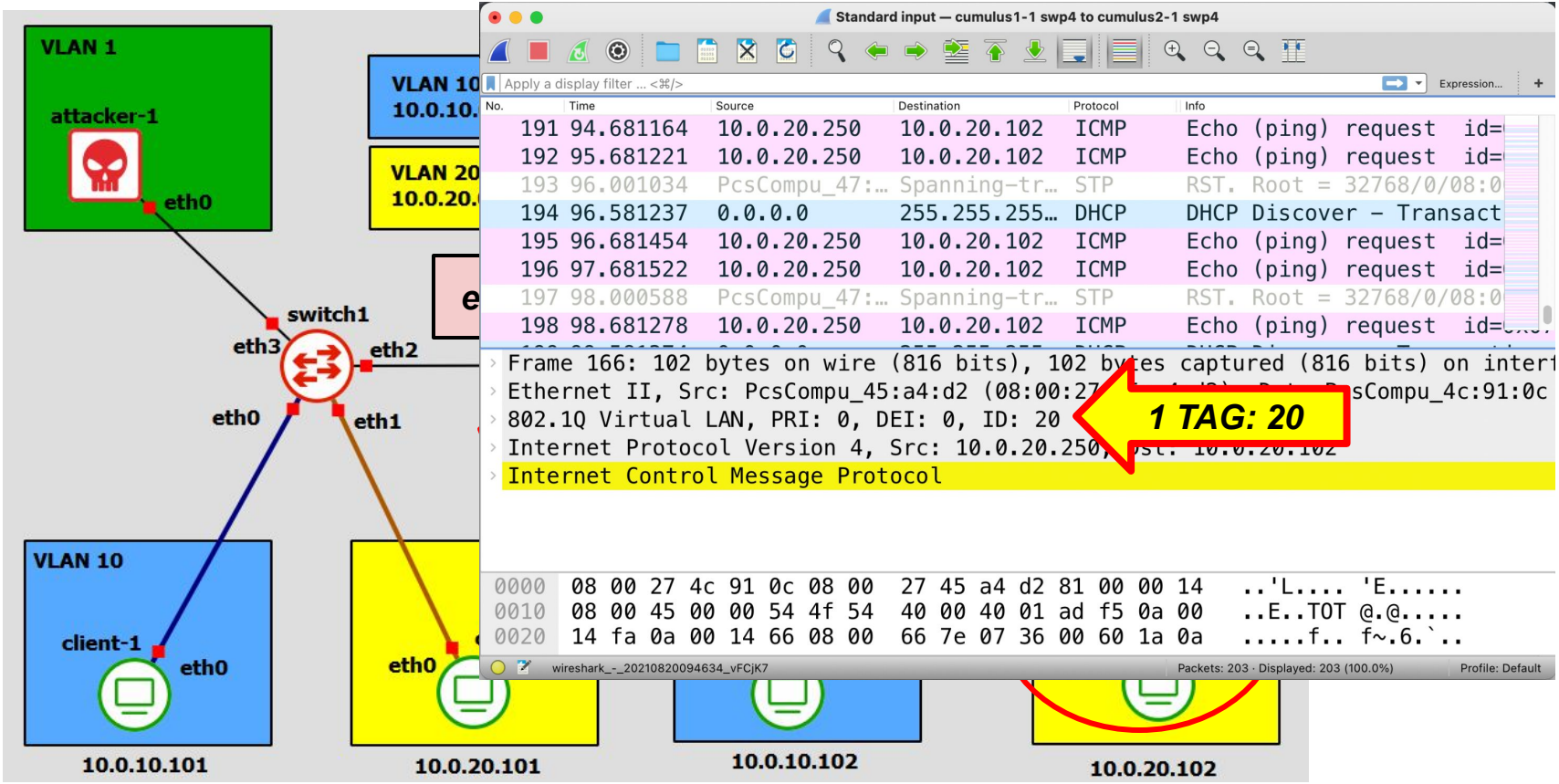
```
0000  08 00 27 4c 91 0c 08 00  27 45 a4 d2 81 00 00 01   ..'L.... 'E......
0010  81 00 00 14 08 00 45 00  00 54 5f 7f 40 00 40 01   ......E. .T_.@.@.
0020  9d ca 0a 00 14 fa 0a 00  14 66 08 00 4a 1a 07 36   ........ .f..J..6
```

Internet Control Message Protocol: Protocol — Packets: 224 · Displayed: 116 (51.8%) · Dropped: 0 (0.0%) — Profile: Default

Lab 4: double tagging attack



Lab 4: double tagging attack



Lab 4: double tagging attack