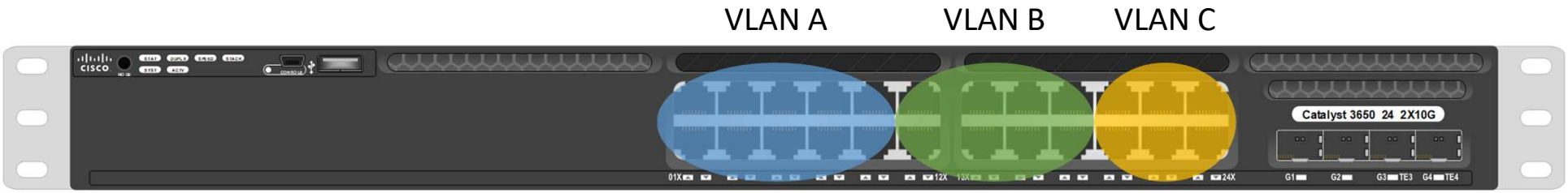
VLANs

Virtual Local Area Networks – VLANs

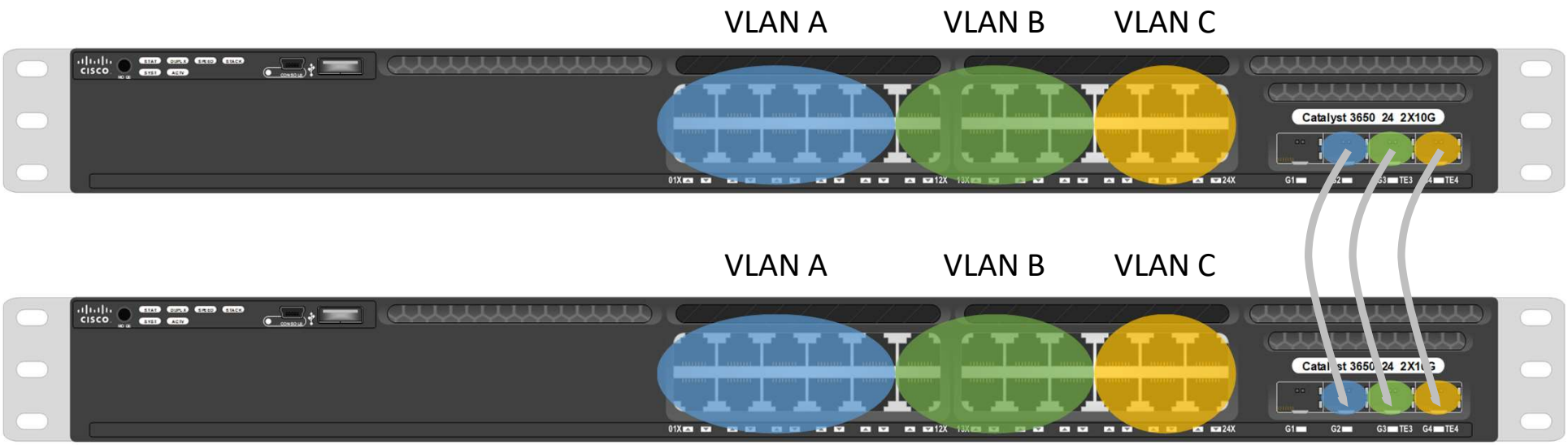
- One of the most common managed-switch feature.
- Allows the creation of many separate LAN networks on the same physical infrastructure.
- One VLAN – one broadcast domain.

- A relatively simple task on a single switch
  - a complex one in a multi-switch system.

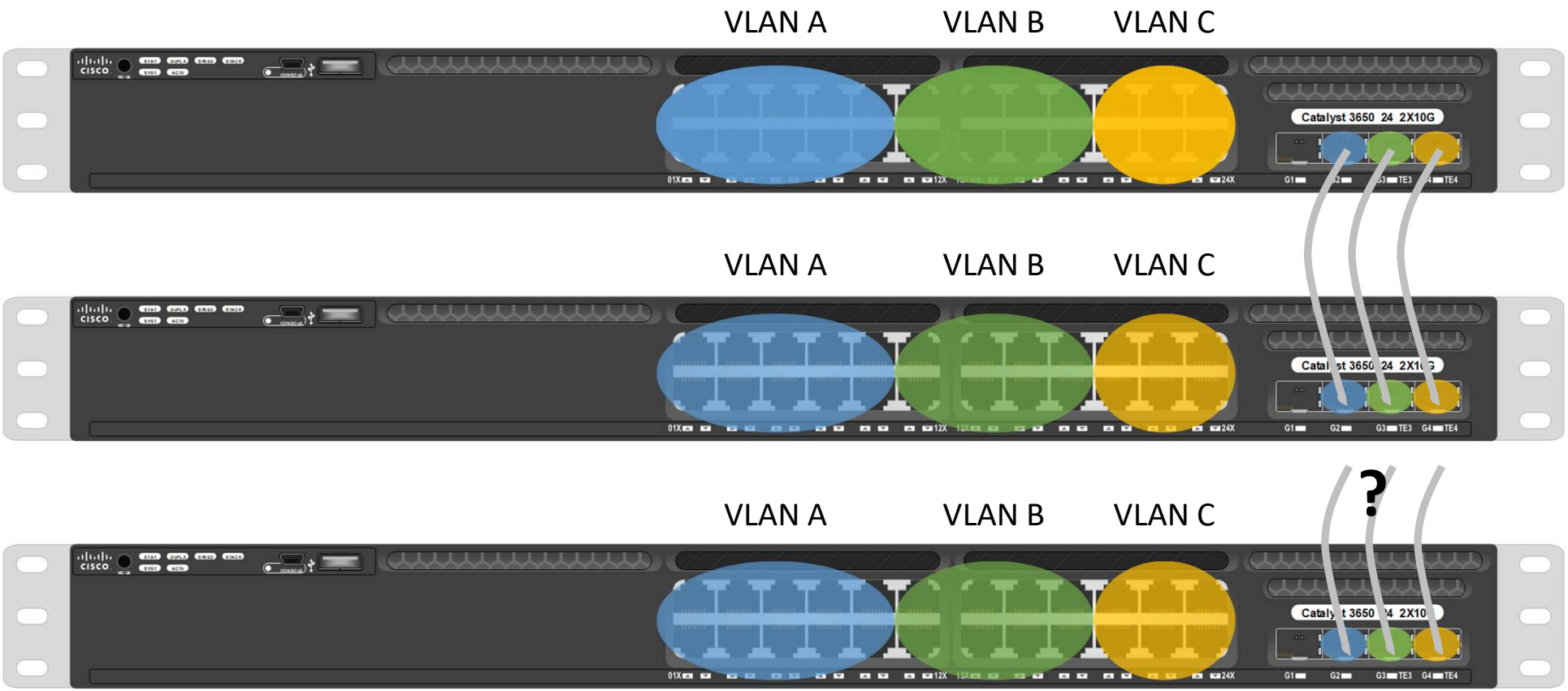
Port-based Virtual LANs



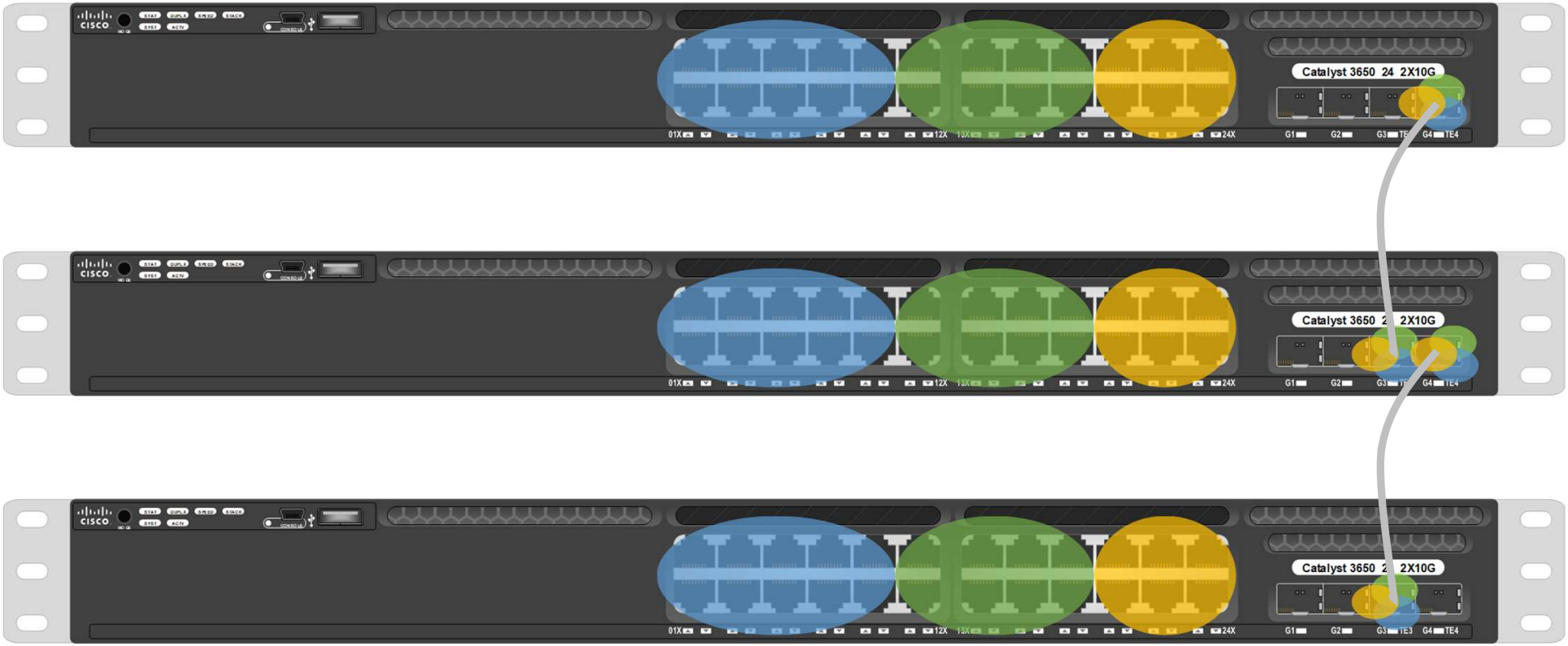
VLANs – the connection problem



With the number of switches scale problem arises



Single link to send multiple VLANs



Single link multiple VLANs solutions

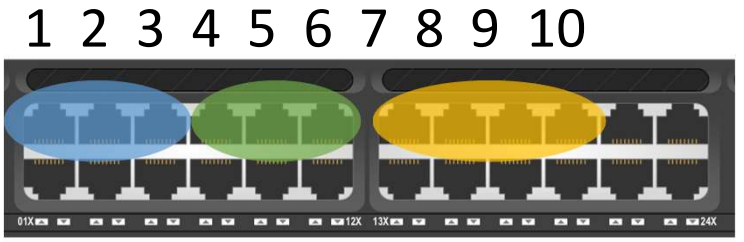
- Time-based division of link bandwidth
- ISL – Cisco proprietary concept of adding tags to frames
- IEEE 802.1Q – standard for frame tagging

Switching matrix

output port

input port

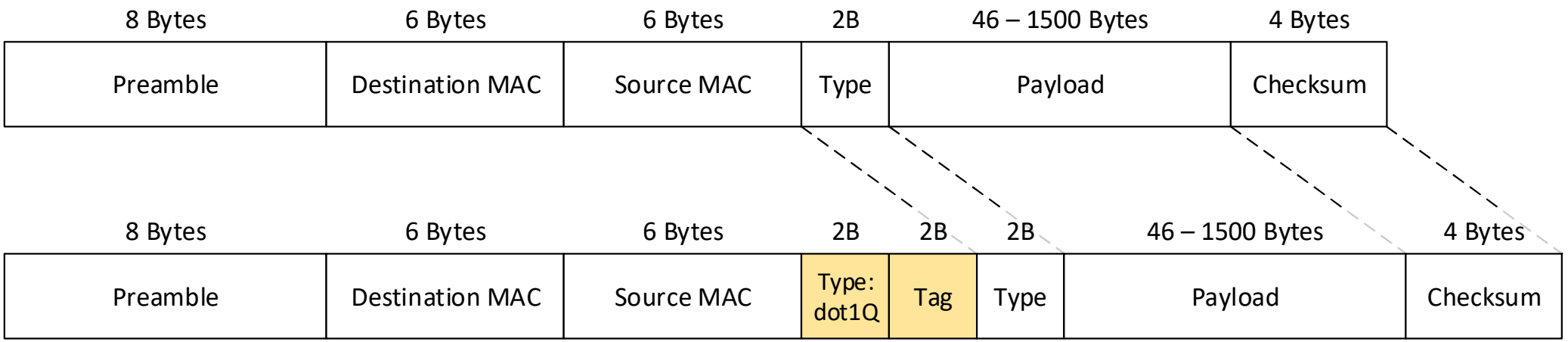
	1	2	3	4	5	6	7	8	9	10
1	0	1	1							
2	1	0	1							
3	1	1	0							
4				0	1	1				
5				1	0	1				
6				1	1	0				
7							0	1	1	1
8							1	0	1	1
9							1	1	0	1
10							1	1	1	0



VLAN tagging

- IEEE 802.1Q standard
- tags are added to each transmitted frame
- tagged frames are longer by 4 bytes (2x2 bytes)
- the tag contains VLAN ID (number) allowing to identify which broadcast domain (VLAN) a frame belongs
- the maximum of 4096 VLAN IDs (12 bits numbering) can be carried in the tag

VLAN tag


8 Bytes
6 Bytes
6 Bytes
2B
46 – 1500 Bytes
4 Bytes
Preamble
Destination MAC
Source MAC
Type
Payload
Checksum
8 Bytes
6 Bytes
6 Bytes
2B
2B
2B
46 – 1500 Bytes
4 Bytes
Preamble
Destination MAC
Source MAC
Type: dot1Q
Tag
Type
Payload
Checksum

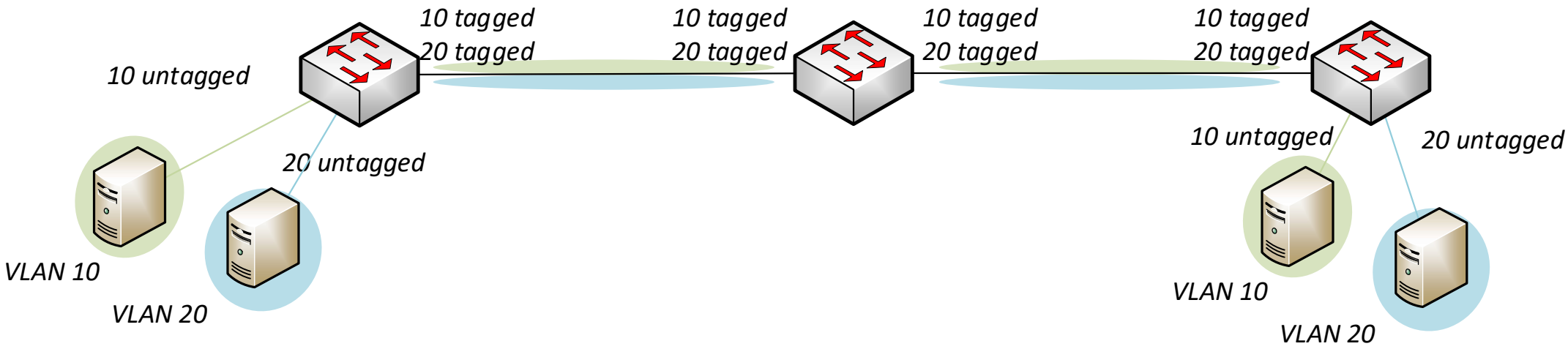
Typical configuration of VLANs on switches

- Multiple distinct broadcast domains
  - following logical enterprise structure,
  - following geographical structure,
- in any case total broadcast traffic volume is significantly reduced.

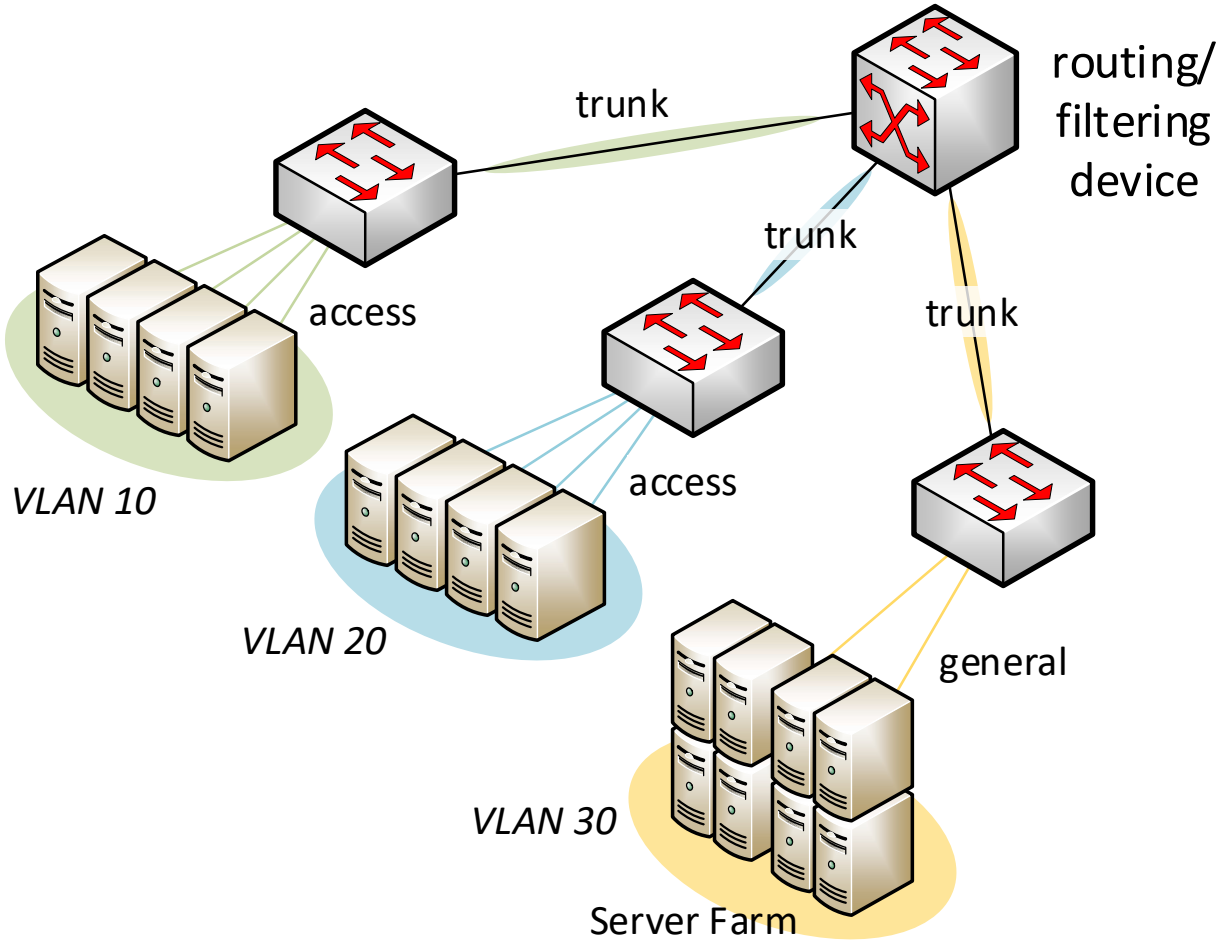
- Three types of VLAN links/ports:
  - access port – no tags, typical workstation port,
  - trunk port – all frames tagged, typically connects two switches,
  - general/hybrid port – multiple tagged VLANs and a SINGLE VLAN untagged.
- Native VLAN – the only untagged VLAN on port:
  - If untagged frame arrives on port – it is assigned to a Native VLAN.
  - If a frame from a Native VLAN is to be sent on (non-trunk) port – it will be sent without a tag.
- Untagged traffic may be assigned to just one VLAN.

Frame tagging

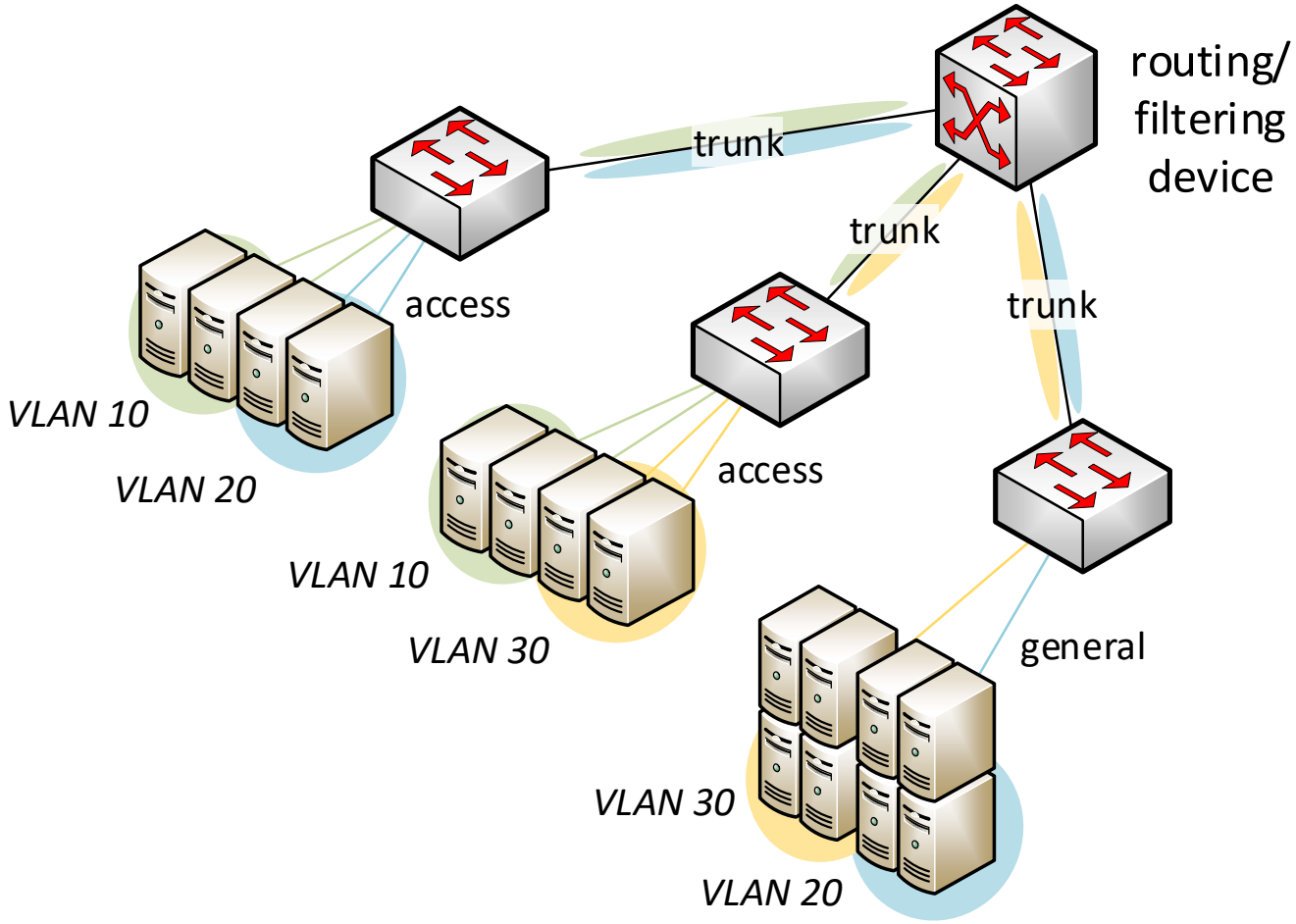
- Property of a port for specified VLAN.
- Switching inside VLAN occurs on the same manner as inside a separate, physical switch.



Example VLAN configuration



Example VLAN configuration



Example port configurations

- Example configurations from real-life switches:

Trunk port configured to support VLANs 10, 20, 30, 181

```
interface te1/0/2
 switchport mode trunk
 switchport trunk allowed vlan add 10,20,30,181 tagged
```

Access port configured as belonging to VLAN 10

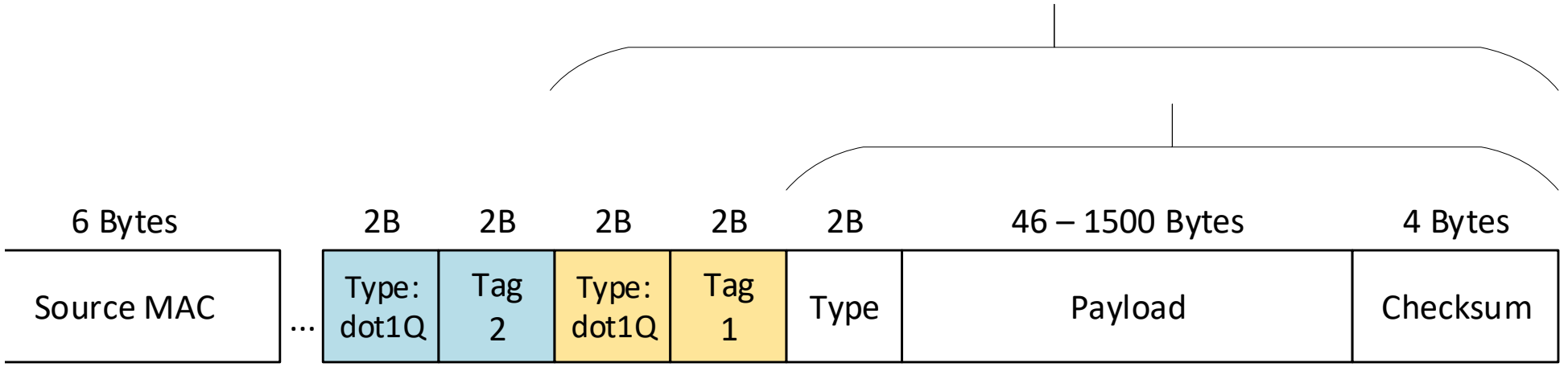
```
interface Gi1/0/14
 switchport access vlan 10
```

VLAN 20 configured to span a list of ports

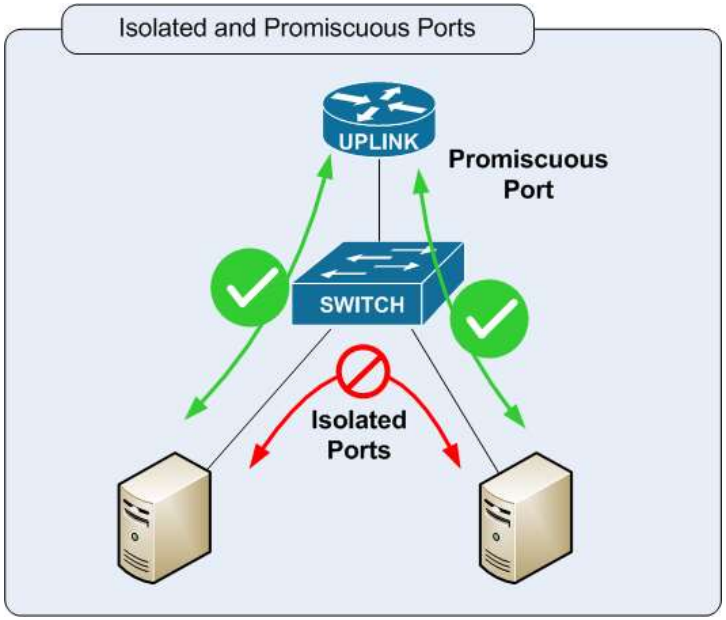
```
interface Vlan 20
 no ip address
 tagged TenGigabitEthernet 0/2-5,9,11-12
```

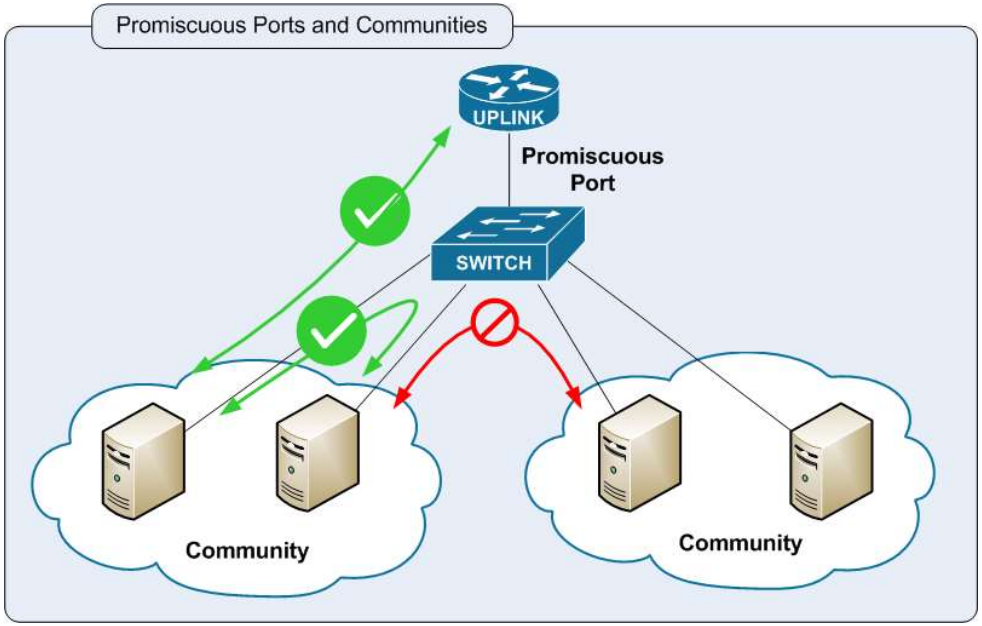
Q-in-Q tagging

- IEEE 802.1ad standard amendment
- Allows multiple tags to be added to Ethernet frames
- Each new tag encapsulates all previous tags and payload



Private VLANs



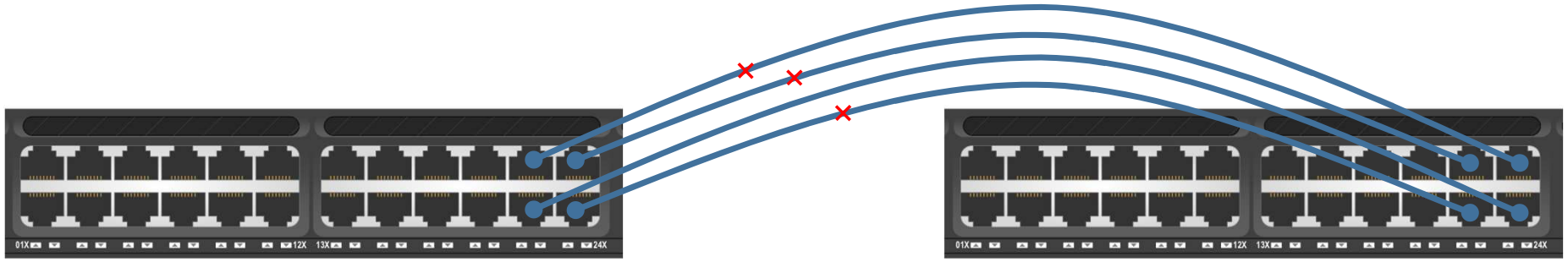


- Promiscuous port (P-Port) – can communicate with any other port
- Isolated port (I-Port) – can communicate only with P-Ports
- Community port (C-Port) – can communicate with C-Ports in the same community and with P-Ports

High-availability: link aggregation

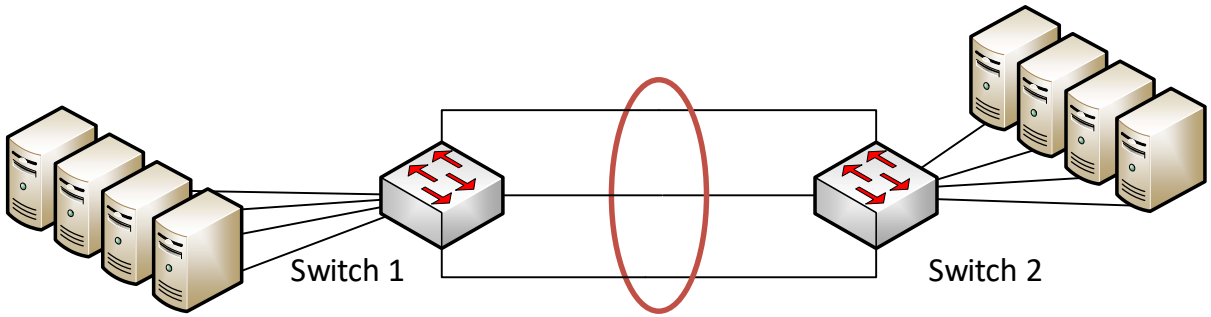
Link aggregation

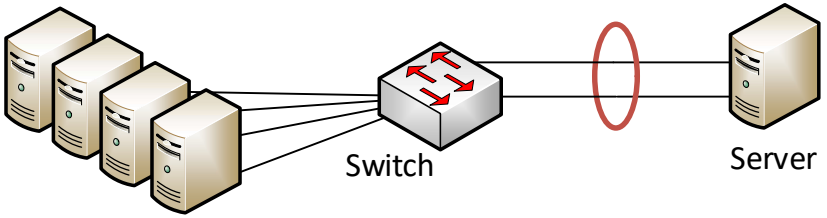
- IEEE 802.3ad – standard amendment
- Allows to aggregate Ethernet links into a composite one called LAG – Link Aggregation Group
- Provides resiliency to link failures
  - in case of e.g. four aggregated links up to three may fail and the link still remains accessible



Link aggregation

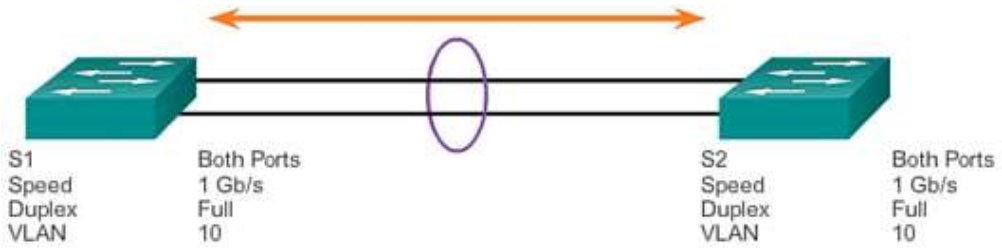
- Provides load balancing
  - the throughput of LAG is equal to sum of throughputs of aggregated links: 4 links of 1 Gbps may offer up to 4 Gbps,
  - preserves packet order,
  - depends on MAC address pairs of traffic flows.
- LAG is a point-to-point link – the group cannot span devices.

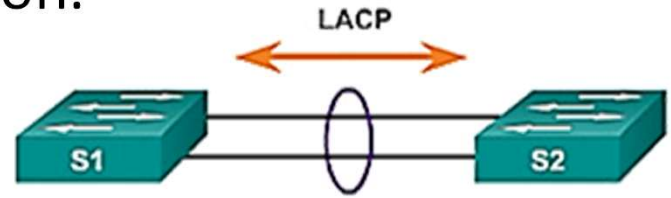




Link Aggregation Control Protocol (LACP)

- Link parameters on both devices have to match:
  - speed and duplex,
  - VLAN configuration.
- Different physical medium links can be aggregated – copper and fiber.
- LACP can be used to negotiate configuration.

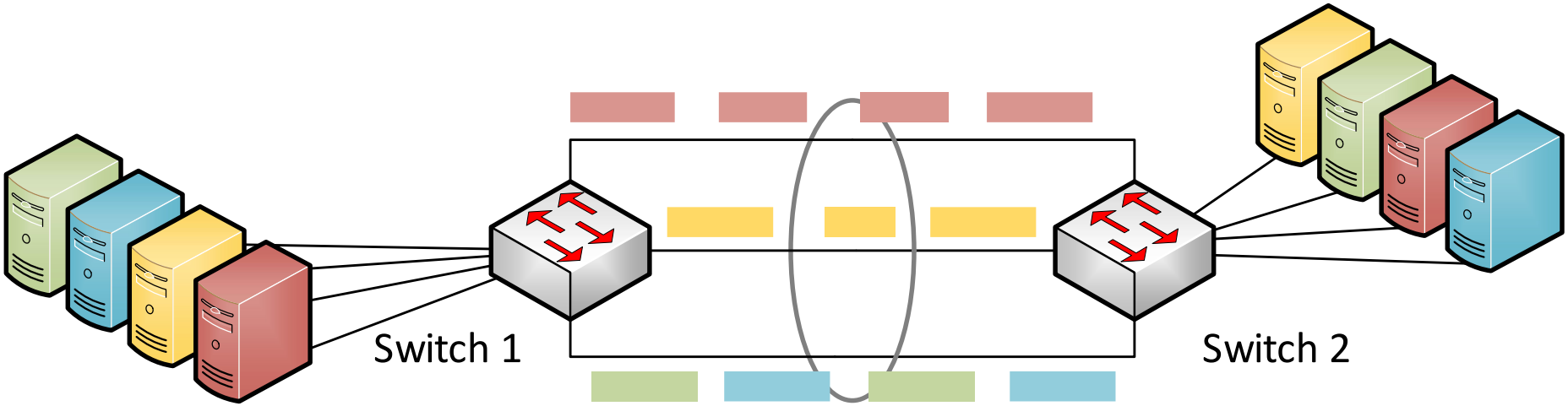




S1	S2	Channel Establishment
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	Not Configured	No
On	Active	No
Passive/On	Passive	No

LAG – frame ordering

- LAG preserves frame order
- Frames between MAC-pairs are being sent over the same physical links



Additional switch functions

- Statistics monitoring
  - a number of standards in use, mainly Simple Network Management Protocol (SNMP).
- Port-mirroring (SPAN, Switch Port Analyzer)
  - allows configurable traffic forwarding to an analysis device.
- Test Access Point (TAP)
  - forwards L1 or L2 traffic to an analysis device.