<epam>

Virtual Networks

TRAINING

CENTER

<epam>

Aliaksandr Ramanovich

<epam>

Agenda

- WHAT IS IT?
- 802.11Q
- EXAMPLES

VLAN

- A virtual LAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer.
- In other words it is a logical subnetwork that groups a collection of devices from different physical LANs.
- VLANs can group client devices that communicate frequently with each other. The traffic among devices split across two or more physical networks is usually handled by a network's core routers. But with a VLAN, that traffic is handled more efficiently by network switches.
- VLANs also bring security benefits to larger networks by allowing greater control over which devices have local access to each other.

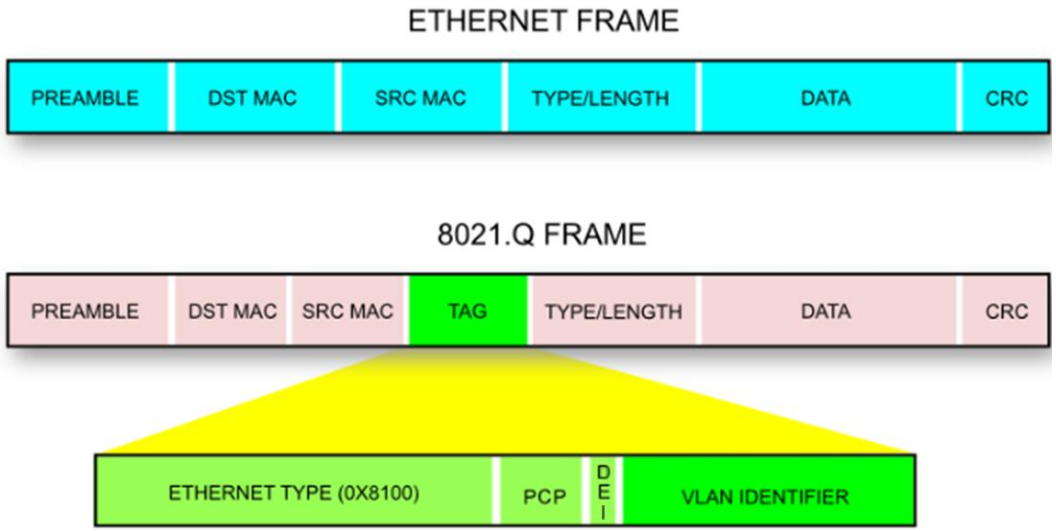
VLAN Membership

- Static VLANs are also referred to as port-based VLANs. Static VLAN assignments are created by assigning ports to a VLAN. As a device enters the network, the device automatically assumes the VLAN of the port. If the user changes ports and needs access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.

- Dynamic VLANs are created using software or by protocol. With a VLAN Management Policy Server (VMPS), an administrator can assign switch ports to VLANs dynamically based on information such as the source MAC address of the device connected to the port or the username used to log onto that device. As a device enters the network, the switch queries a database for the VLAN membership of the port that device is connected to.

IEEE 802.1Q

- IEEE 802.1Q, often referred to as Dot1q, is the networking standard that supports VLANs in Ethernet.
- It defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames.



VLAN Tag

A 16-bit field set to a value of 0x8100. This field is located at the same position as the EtherType field in untagged frames, and is thus used to distinguish the frame from untagged frames.

Priority code point - 3-bit field which refers to the IEEE 802.1p class of service and maps to the frame priority level.

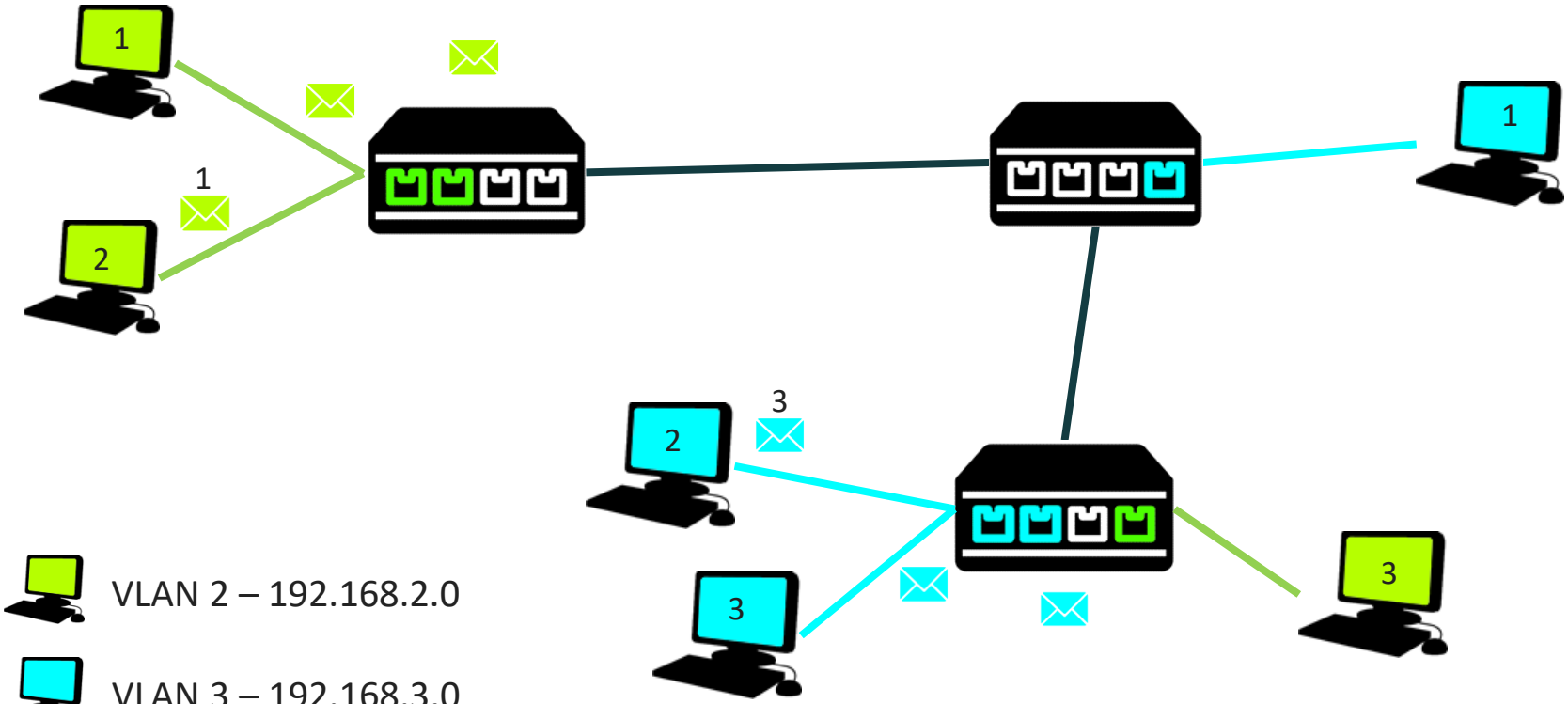
Drop eligible indicator - may be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion

VID - a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 (default VLAN) and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs.

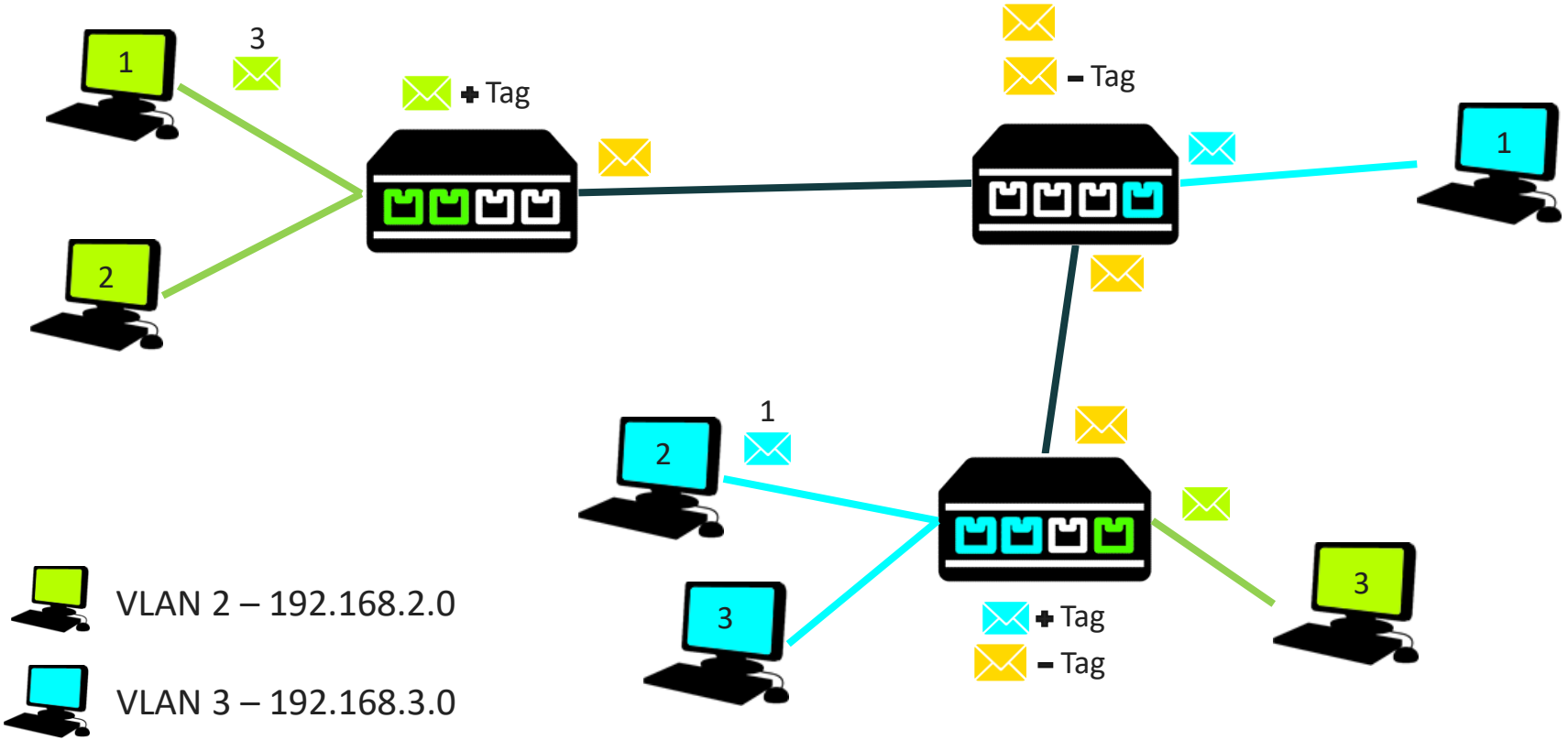
VLAN Ports

- Access port works with untagged traffic. Used to connect end devices that do not support VLAN technology
- When a switch receives data from the device connected to access port, it will add a common tag with the specified subnet identifier to all Ethernet frames and then operate with the already tagged packet. When data send to the device from the main network, the switch will compare the VLAN ID of the received packet with the VLAN subnet number of this port. If they match, the tag ill be removed and data will be successfully transmitted to the port.
- If VLAN IDs don’t match packet will be ignored.
- Trunk-port carries tagged data packets. Used to connect network devices with VLAN support, most often to connect switches together.
- In addition to specifying the operating mode and VLAN identifier it is possible to create a list of allowed VLANs for transmission, and the switch will check it receiving packets on that trunk port. This allows packets from multiple VLAN subnets to be transmitted through trunk ports.

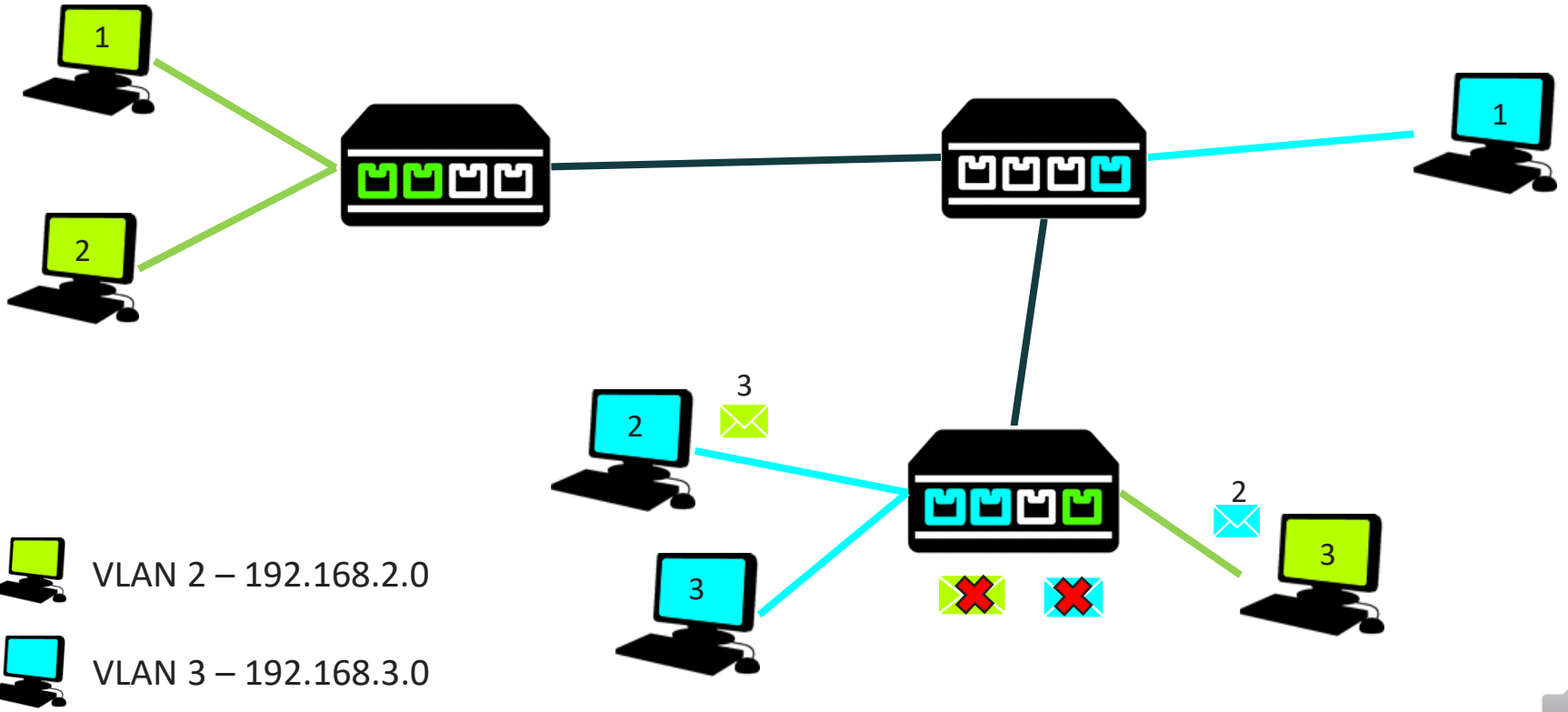
VLAN



VLAN



VLAN



VLAN Advantages

- Reducing the number of broadcast requests that reduce network bandwidth.
- Increase the security of each virtual network. Employees of one department in the office will not be able to monitor the traffic of departments that are not included in their VLAN, and will not have access to their resources.
- The ability to divide or combine departments or users, geographically distant from each other. This makes it possible to involve specialists outside the office building in the work process.
- Simplification of network administration. When a VLAN user moves to another room or building, the network administrator does not need to reconnect the cables; it is enough to reconfigure the network equipment from his workplace. And in the case of using dynamic VLANs, the user will be registered in his “own” VLAN at the new location automatically.

THANK YOU