**18. tétel Virtual LANs (**Local Area Networks)- Virtuális helyi hálózatok

I work as an IT engineer for a system integration company. Our task is to improve the network performance of a small/medium-sized enterprise. I would like to explain how the new network with virtual LANs works. I would also speak about the advantages of the new system.

A **virtual LAN** is a logical subnetwork that can group together a collection of devices from different physical LANs. Larger business computer networks often set up VLANs to re-partition their network for improved traffic management. Several different kinds of physical networks support virtual LANs including both Ethernet and WI- Fi.

-**VLANs** allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device.

-**VLANs** enable the implementation of access and security policies according to specific groupings of users.

-A VLAN is a logical partition of a Layer 2 network.

-Multiple partitions can be created, allowing for multiple VLANs to co-exist.

-Each VLAN is a broadcast domain, usually with its own IP network.

-VLANs are mutually isolated, and packets can only pass between them via a router.

-The partitioning of the Layer 2 network takes place inside a Layer 2 device, (usually) via a switch.

**Benefits of VLANs** are the following:

-**Improved security; Reduced cost; Better performance; Smaller broadcast domains; IT Efficiency; Management Efficiency; Simpler Project and Application Management**

-When set up correctly, virtual LANs can improve the overall performance of busy networks.

-VLANs are intended **to group together client devices** that communicate with each other most frequently. The traffic between devices split across two or more physical networks ordinarily needs to be handled by a network's core routers, but with a VLAN that traffic can be handled more efficiently by network switches instead.

-VLANs also bring additional **security benefits** on larger networks by allowing greater control over which devices have local access to each other. Wi-Fi guest networks are often implemented using wireless access points that support VLANs.

**VLAN Trunks**

-A VLAN trunk is a point-to-point link that carries more than one VLAN.

-A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.

-A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.

-Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol.

**Tagging Ethernet Frames for VLAN Identification**

-Frame tagging is the process of adding a VLAN identification header to the frame.

-It is used to properly transmit multiple VLAN frames through a trunk link.

-Switches tag frames to identify the VLAN to which they belong.

-Different tagging protocol exist; IEEE 802.1Q is a very popular example.

-The protocol defines the structure of the tagging header added to the frame.

-Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before frames through non-trunk ports.

-When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.

**(Setting up a VLAN-** At a high level, network administrators set up new VLANs as follows:

1. Choose a valid VLAN number.
2. Choose a private IP address range for devices on that VLAN to use.
3. Configure the switch device with either static or dynamic settings.  Static configurations require the administrator to assign a VLAN number to each switch port while dynamic configurations require assigning a list of MAC addresses or user names to a VLAN number.
4. Configure routing between VLANs as needed. Configuring two or more VLANs to communicate with each other requires the use of either a VLAN-aware router or a [Layer 3 switch](https://www.lifewire.com/layer-3-switch-817583).)