

VLAN tag based configuration examples (Legacy Firmware)

□

Contents

- [1 Summary](#)
- [2 Configuration in Router's web interface](#)
 - [2.1 Creating new LAN's](#)
 - [2.2 Assigning LAN networks](#)
- [3 Configuration in Ubuntu terminal](#)
- [4 Testing VLAN](#)

Summary

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic. VLANs work by applying tags to network packets and handling these tags in networking systems - creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labor of relocating nodes or rewiring data links. It also has benefits in allowing networks and devices that must be kept separate to share the same physical cabling without interacting, for reasons of simplicity, security, traffic management, or economy. For example, a VLAN could be used to separate traffic within a business due to users, and due to network administrators, or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network's functioning. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their datacenter. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.

This chapter is an overview of the **VLAN** function of **RUT** devices.

Configuration in Router's web interface

You should secure your wiki.

Creating new LAN's

Go to Network>>VLAN



Go to LAN Networks



Create 2 new LAN's by typing LAN name and pressing Add New



When configuration window appears, fill in the LAN's IP addresses and IP broadcasts and click Save button.



LAN1 and LAN2 has to be with different subnets (for example 192.168.21.1 and 192.168.22.1)



Assigning LAN networks

Go to Network >> VLAN >> VLAN Networks and select VLAN mode "Tag based" and click Save



Default section appears



Create 2 new VLAN network interfaces by clicking "Add". Assign created LAN networks to a different LAN ID and click "Save"



Configuration in Ubuntu terminal

Install vlan with command "**sudo apt-get install vlan**" and then run command "**ifconfig**" to see your devices network interfaces

For example, we have to use router's interface, so the network interface is "**enp2s0**"



In order to use VLAN feature in Ubuntu, we have to let kernel support 802.1q by loading 8021q module. Load the 8021q kernel module with command **"sudo modprobe 8021q"**.

Add VLAN interfaces with **"sudo vconfig add network_interface VLAN_ID"** (for example **"sudo vconfig add enp2s0 2"**)

Enable added network interfaces by typing **"sudo ifconfig network_interface.VLAN_ID up"**. (for example **"sudo ifconfig enp2s0.2 up"**)

Get IP address for your VLAN's with **"sudo dhclient network_interface.VLAN_ID"**. (for example **"sudo dhclient enp2s0.2"**)



Testing VLAN

1. In Ubuntu terminal run the command **"ifconfig"** and you should see your VLAN interfaces with IP addresses from correct subnets (example **"enp2s0.2"**)



2. Run ping on your VLAN IP (for example 192.168.21.1)

