VLAN SWITCH REPORT



VLAN SWITCH REPORT

[Student’s signature]

­­­­­­­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Student’s name, date]

**Tabl****e of Contents**

[Introduction 4](#_Toc420418942)

[Problem description 4](#_Toc420418943)

[The ProCurve switch\* 5](#_Toc420418944)

[General description 5](#_Toc420418945)

[Implementation of Trunk Ports 5](#_Toc420418946)

[Possible Network Security measures 5](#_Toc420418947)

[Configuration of the switch and configuration procedure 6](#_Toc420418948)

[Accessing via console port and Telnet 6](#_Toc420418949)

[The different interfaces and setup possibilities (HyperTerminal, Telnet, CLI, Setup and Menu) 12](#_Toc420418950)

[Accessing via WEB-interface 17](#_Toc420418951)

[Test the function of the complete configuration 20](#_Toc420418952)

[Motivation and function of VLAN 20](#_Toc420418953)

[Motivation of VLAN 20](#_Toc420418954)

[Function of VLAN 21](#_Toc420418955)

[Motivation and function of a trunk port 21](#_Toc420418956)

[Motivation for trunk port 21](#_Toc420418957)

[Function of trunk port 21](#_Toc420418958)

[VLAN Tagging 22](#_Toc420418959)

[Conclusion 23](#_Toc420418960)

# Introduction

This report is the documentation of project work made for networking, IT-technology AP-program, first semester on KEA 2015. A group of four students is contributing to this assignment. Groups were preassigned according to unknown, for students, pedagogical parameters. The project works as an exam to show that knowledge and skills acquired in networking are sufficient to pass on to second semester. Knowledge must be practically applied in configuration of a switch and documented according to academic standards as described in the subject known as “com.doc”. The purpose, of the project, is to simulate a – somewhat - realistic scenario, like one a student might meet in the wild but with a difficulty level fitting a first semester student.

# Problem description

The project have multiple tasks including understanding theoretical information, understanding never previously seen hardware, applying theory into practice and configuring a switch to work optimally in the given scenario. Overall, this breaks down to the following tasks:

* Demonstrate a general knowledge on how local area networks work
* Demonstrate a knowledge on how the supplied ProCurve switch work
* Demonstrate a knowledge on how subnetting and VLANs work
* Demonstrate how to configure the supplied ProCurve switch from all 3 interfaces
  + In particularly setting up VLANs – with and without “trunking”
* Demonstrate how to test configurations and interpretate results
* Demonstrate a theoretical knowledge and understanding of VLANs and trunk ports, including “tagging”
* Demonstrate knowledge of the motivation for *and* function of VLANs and trunk ports

These tasks are dependent on each other obviously, without the theoretical knowledge, it will be impossible to configure the switch and without practical understanding about configuring the switch, it will be impossible to create VLANs, trunk ports and so on. This means that both theory and practice must be observed equally.

# The ProCurve switch\*

(\* This chapter is from HP website: <http://h17007.www1.hp.com/us/en/networking/products/switches/HP_2510_Switch_Series/index.aspx#.VWNLcrmqqko>)

The HP 2510 series are designed to provide essential solutions to businesses of small and medium sizes. The HP 2510 Switch Series consists of two Layer 2- managed switches that provide reliable 10/100 connectivity. Building off of the popularity of the HP 2510-24 Switch, a 24-port 10/100 switch with two dual-personality ports, the 2510 switch series has expanded to include a higher-density HP 2510-48 Switch, with 48 10/100 ports and four Gigabit Ethernet uplinks.

## General description

* **IEEE 802.1p prioritization:** delivers data to devices based on the priority and type of traffic Implementation of Trunk ports
* **10/100 and 10/100/1000 connectivity:** provides customers with the choice of selecting the network connectivity speed that best meets their needs, with a consistent user experience
* **Ports:** the 2510-24 switch has two dual-personality ports for either 10/100/1000 or mini-GBIC connectivity
* **HP Auto-MDIX:** automatically adjusts for straight-through or crossover cables on all 10/100 and 10/100/1000 copper ports

## Implementation of Trunk Ports

* **IEEE 802.1s Multiple Spanning Tree:** provides high link availability in multiple VLAN environments by allowing multiple spanning trees; provides legacy support for IEEE 802.1d and IEEE 802.1w
* **IEEE 802.3ad Link Aggregation Control Protocol (LACP) and HP trunking:**
* 2510-24 switch supports up to two 10/100 trunks each with four links/ports plus one Gigabit Ethernet trunk

## Possible Network Security measures

* **Protected ports:** provides increased security by allowing specified ports to be isolated from all other ports on the switch; the protected port or ports can communicate only with the uplinks or shared resources
* **Multiple user authentication methods:**
* **IEEE 802.1X:** is an industry-standard method of user authentication using an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server
* **Web-based authentication:** similar to IEEE 802.1X, it provides a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant
* **MAC-based authentication:** client is authenticated with the RADIUS server based on the client's MAC address
* **Guest VLAN:** isolates guest and unauthorized user traffic to a separate VLAN
* **Port security:** allows access only to specified MAC addresses, which can be learned or specified by the administrator
* **MAC address lockout:** prevents particular configured MAC addresses from connecting to the network
* **Multiple IEEE 802.1X users per port:** provides authentication of up to two IEEE 802.1X users per port; prevents user "piggybacking" on another user's IEEE 802.1X authentication
* **STP BPDU port protection:** blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks
* **Secure management access:** securely encrypts all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3
* **TACACS+:** eases switch management security administration by using a password authentication server

# Configuration of the switch and configuration procedure

The ProCurve 2510 switch is equipped with triple interface access possibility i.e. SSH, telnet and WEB (HTTP via browser). Each are accessed through different applications and settings. Each interface is explained in separate sub chapters below.

## Accessing via console port and Telnet

Both secure shell (SSH) and telnet can be accessed through the switch’ console port, located in the lower left part of the switch. It is an RJ45 to serial interface that with a serial to USB adapter cable can be accessed from a regular USB port. With the program HyperTerminal (HT) both SSH and telnet can be used to access the switch interface when configure with the correct settings from the manual. Figure 1 shows the settings as provided from the manual.

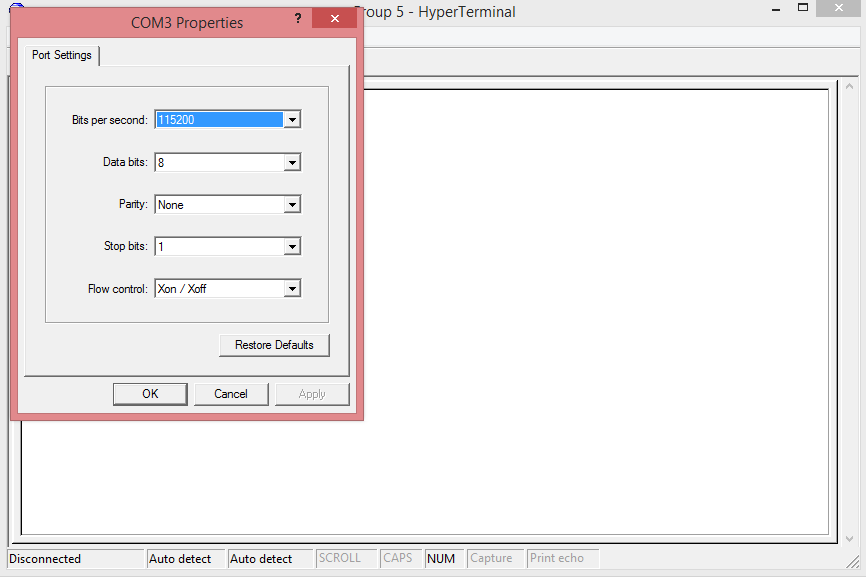


Figure 1.

After log-in a DOS/BIOS like interface appears that can simply be navigated with the keyboard, see figure 2.

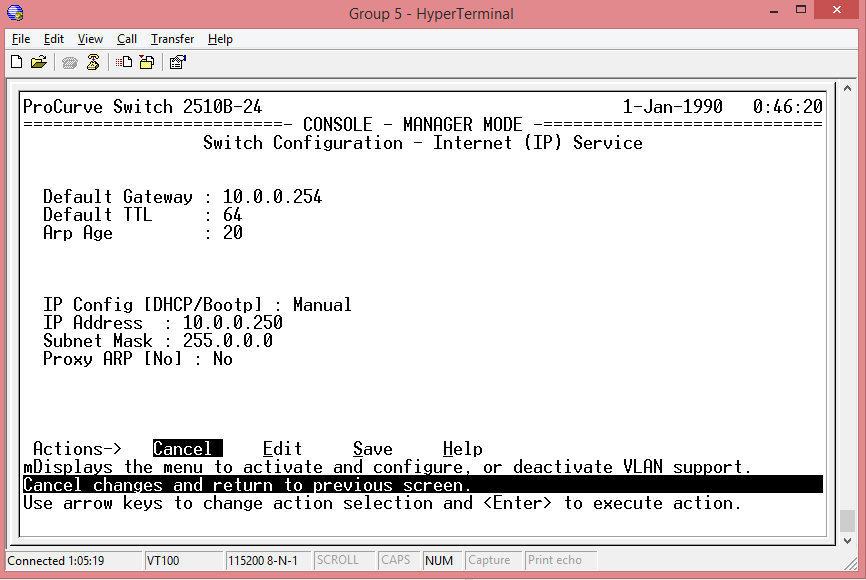


Figure 2.

Now in the console, it is possible to configure VLANs using the VLAN port assignment menu. There is already, by default, a VLAN named “DEFAULT\_VLAN” and ports are as default set to “no”. The two departments “Dep. A” and “Dep. B” needs each a separate VLANs with each six ports. Each port therefore has to be set to “untagged”. Other port options are tagged and forbid. Tagged is used for trunking and is explained in a subsequent chapter and forbid is not relevant for solving the assignment at hand. Figure 3 shows configuration of switch with the two VLANs for Dep. A & B.

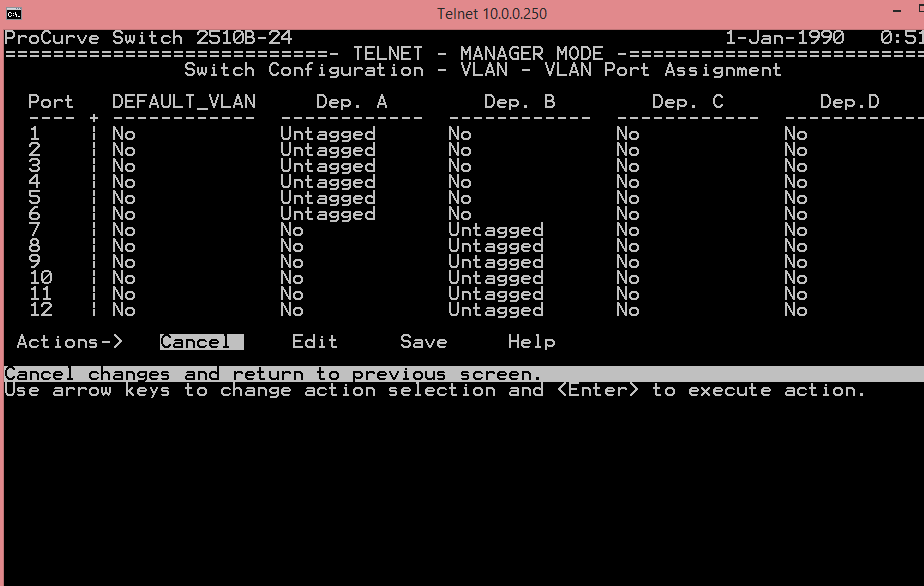


Figure 3.

Obviously, for a VLAN to work each department needs to be on its own subnet, this is known as multinetting or subnetting. This must be set up manually on the ProCurve for instance using the command line interface (CLI), still trough HT. A VLAN can be chosen by using the command “vlan #”. The VLAN 1 is the default VLAN so DEP. A & B are VLAN 2 and 3 respectively. Figure 4 shows configuration procedure and command in a before / after view. Other commands are “ip address” that works to configure IP, and subnet, and “show ip” that shows current IP configuration.

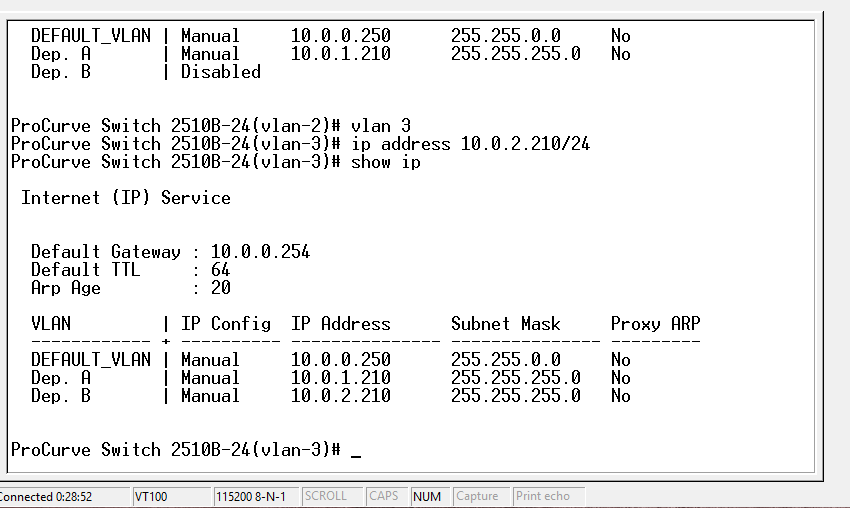


Figure 4.

The IP-configuration is in the format 10.0.0.xxx/24, subnet mask 255.255.255.0, which means that 24 bits out of the 32-bit IP4 address is allocated for network prefix and the remaining 8 bits are used to uniquely identifying hosts. The host part (10.0.x.210) is somewhat arbitrarily chosen but easy to remember. The IP network part is a class A network range and even though a class C network would be sufficient, in this case, it is the prerogative of the system administrator to choose IP network class. An online IP calculator (<http://jodies.de/>) illustrates the configuration in figure 5.

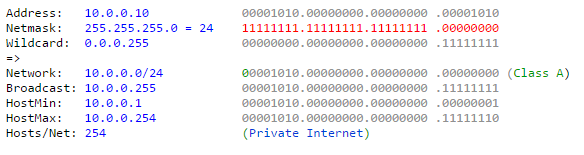


Figure 5.

In a DHCP enabled network, IP’s will be auto assigned to hosts however, with this lab setup hosts needs to be configured manually (see figure 6).

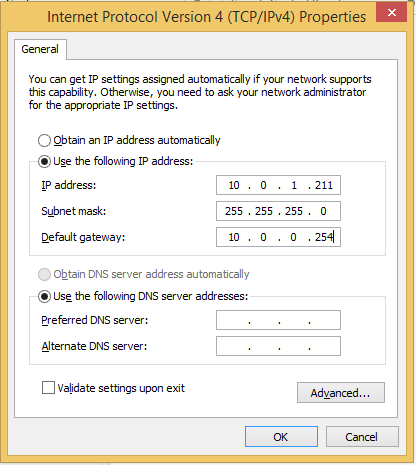


Figure 6.

The shows configuration is for a host that connects to VLAN A. As there is no DNS on this network, it needs not to be configured.

Switch and host configuration can be tested by pinging between to hosts on same subnet.

### The different interfaces and setup possibilities (HyperTerminal, Telnet, CLI, Setup and Menu)

As mentioned earlier the switch can be accessed through both terminal and telnet. Terminal is accessed by using the special terminal port and HT or putty, figure 7 shows the console port.

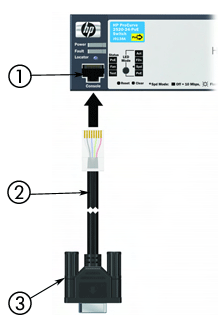


Figure 7.

Another possibility for accessing the switches setup / configuration interface is telnet. Unlike HT telnet needs requires a host and switch that is configured to connect via LAN (RJ45) interface and have valid IP addresses i.e. LAN configuration. This explains the need for both a console and telnet option for the switch. Telnet is accessed from the command prompt typing “telnet o switch ip address” e.g. in figure 8.

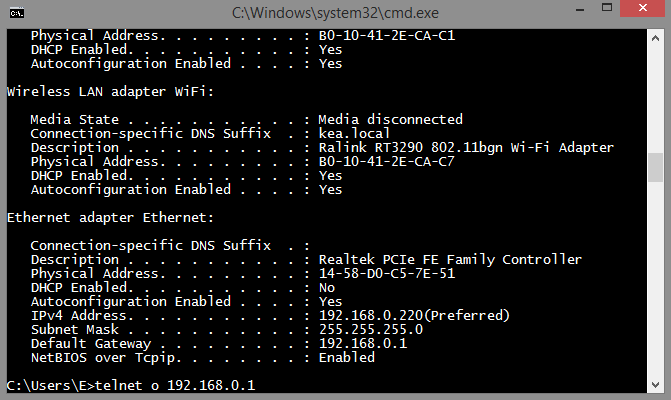


Figure 8.

No matter the connection, console or telnet, the menu structure and navigation is identical. At the command line, “setup” or “menu” starts the interface. “Setup” has some basic option while “menu” gives the full number of configuration possibilities. Figure 9 shows the basic “setup” menu options.

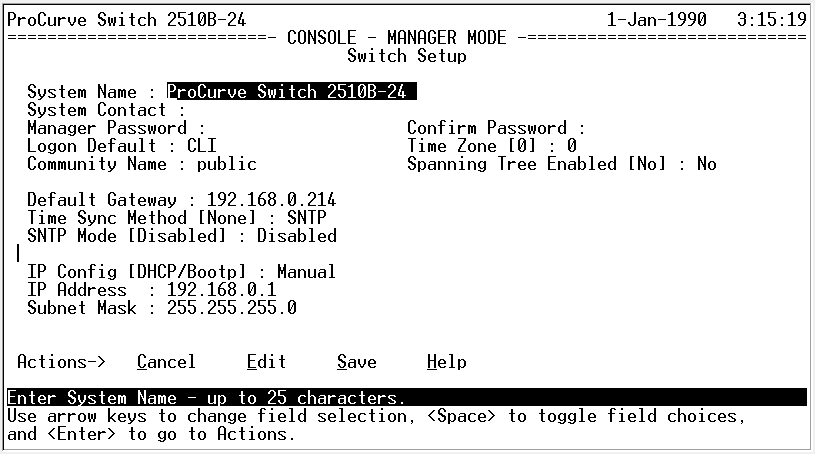


Figure 9.

To access more options the “menu” command must be used and starts up the full configuration menu, see figure 10.

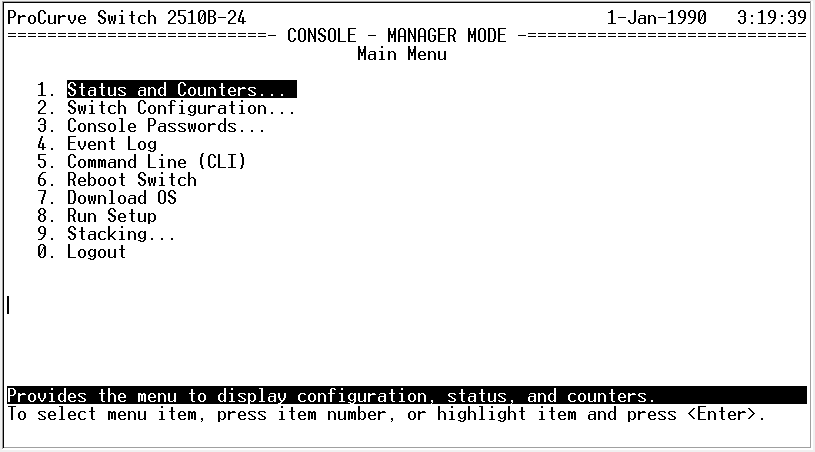


Figure 10.

Several points are of interest. This includes the “Status and Counters” that holds several sub menu points to give quick overview of different settings such as “Switch Management Address Information”, see figure 11.

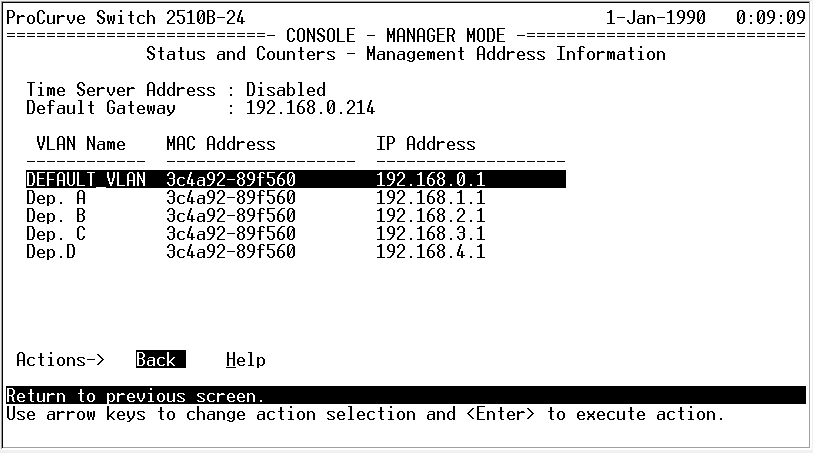


Figure 11.

Note: Unlike earlier figures, the switch in figure 11 is configured for a class C network (earlier A). The change was made so the configuration matched another switch from different group, which makes double switch trunking possible.

The most important menu point is the “VLAN menu” under “Switch Configuration” where VLANs can be named (added) and ports assigned. Figure 12 shows the “VLAN names” menu.

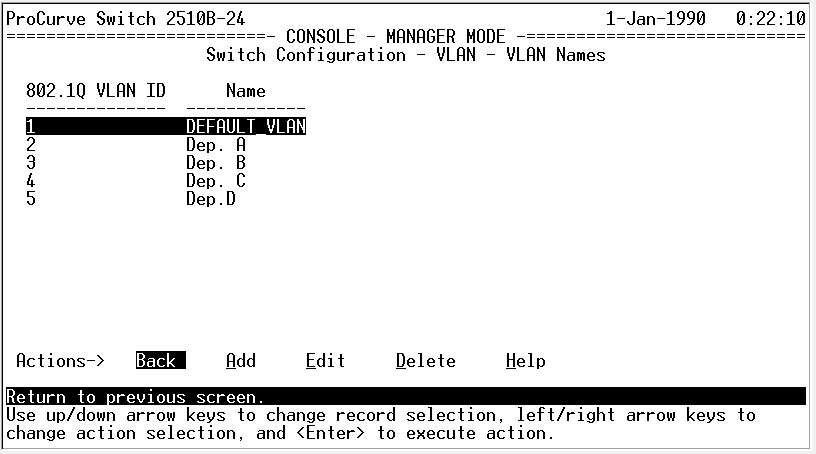


Figure 12.

A graphical user interface (GUI) is nice but the switch can be fully configured using only the command line (CLI). For the experience user this could also be faster than throttling through various menus. Besides the previously mentioned commands other notable commands are “show run”, that shows current configuration (including VLAN setup), and “telnet” that makes it possible to telnet locals host and others.

## Accessing via WEB-interface

In order to be able to access the WEB-interface a simple browser is needed (Simple Browser Two), which is a simple Browser, without any in-built add-ons. Furthermore, java have to be set to not blocking the switches configuration page (Note: this step has to be done only if the switch driver is out of date).

In the WEB-interface, there is a variety of configuration possibilities:

* **Device View:** Here we could see which ports were being in use, and we could deny the access to them if we needed to.

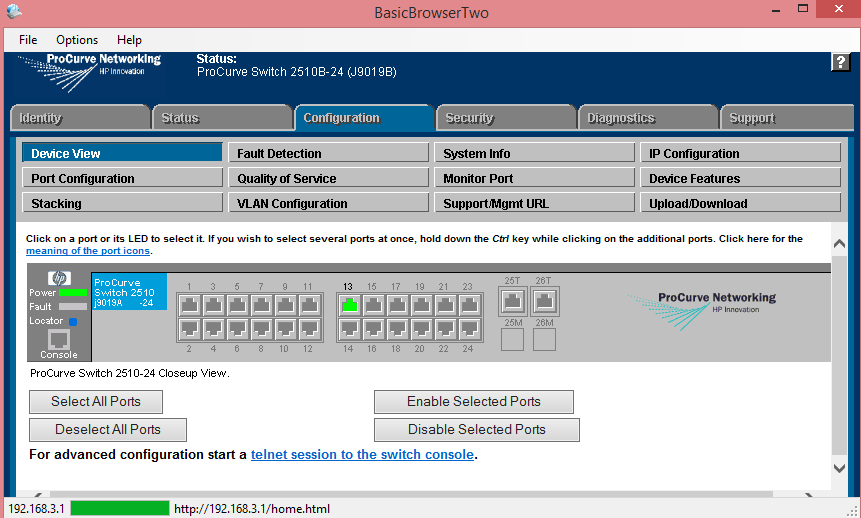


Figure 13.

* **IP Configuration:** Here we can configure the Default Gateway, and also the VLAN’s IP Address and Subnet Mask

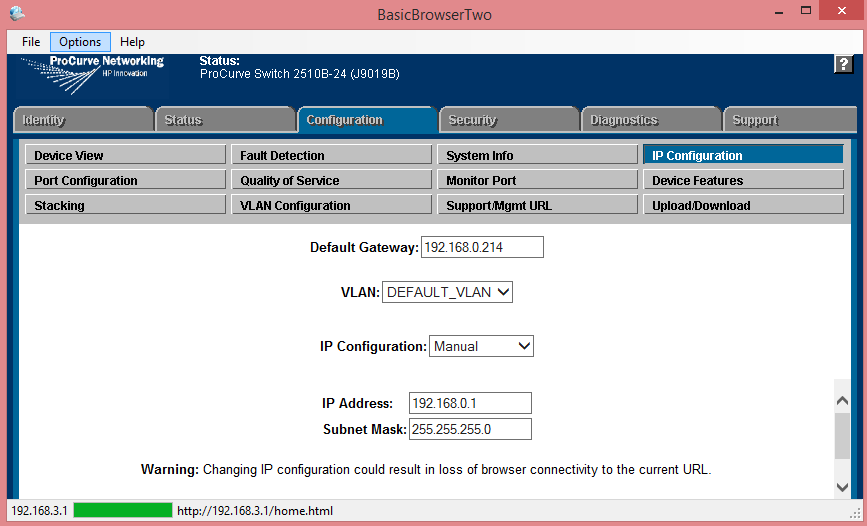


Figure 14.

* **VLAN Configuration:** Here we had the possibility to configure the VLANs with their assigned ports, names and IDs

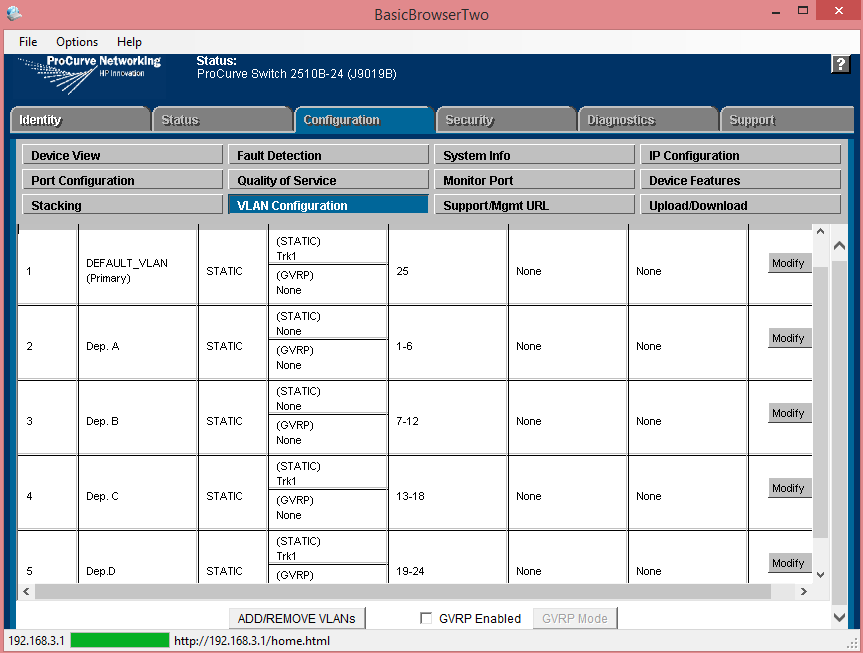


Figure 15.

* **Security:** Here we went under **Port Security** in order to configure the ports to be used by 1 and 3 devices only

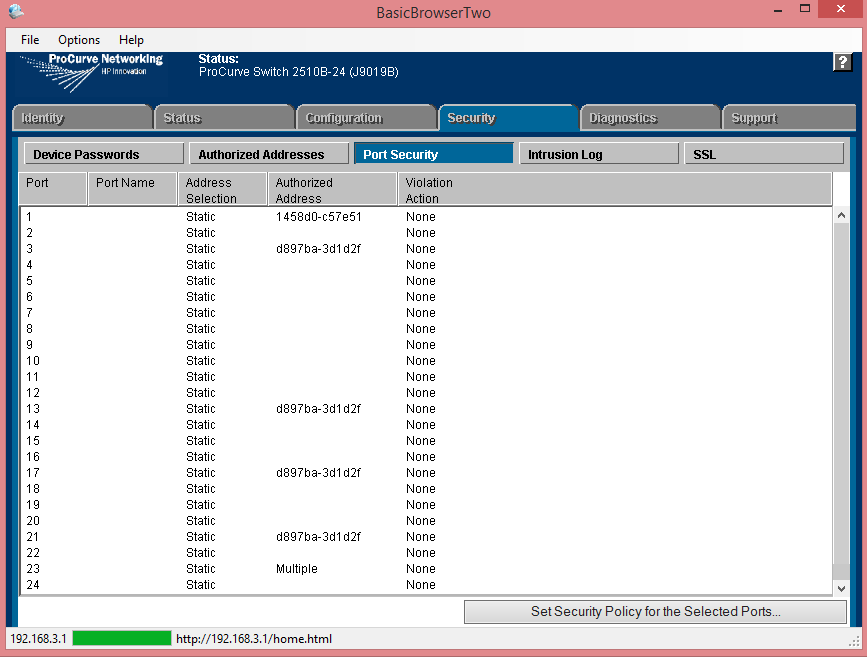


Figure 16.

## Test the function of the complete configuration

After we have finished the configurations, we had to make sure everything was actually working in a perfect manner. First of all we tested that the departments worked properly with their assigned ports, so we tried to connect 2 devices on the same VLAN and see if they could ping each other, and then we tried to connect the same 2 devices but from different VLANs, which gave positive results. After that, we tried to see if the security worked properly so we tried to connect two devices to the same port that had a limit of only one address, and then we tried to connect the same 2 devices to a port that had a limit of 3 addresses, likewise the results were positive. Then last but not the least, in order to see if all the settings were made correctly, we tried to connect two switches to each other via trunk ports, and see if we could ping two devices that were connected to different switches, which of course they did.

# Motivation and function of VLAN

## Motivation of VLAN

Briefly, a VLAN gives us three major benefits: traffic control by prioritizing traffic in particular VLANs or reducing broadcast traffic by making the broadcast domains smaller; security, by controlling traffic between different VLANs (subnets); and flexibility in network design without extra equipment.

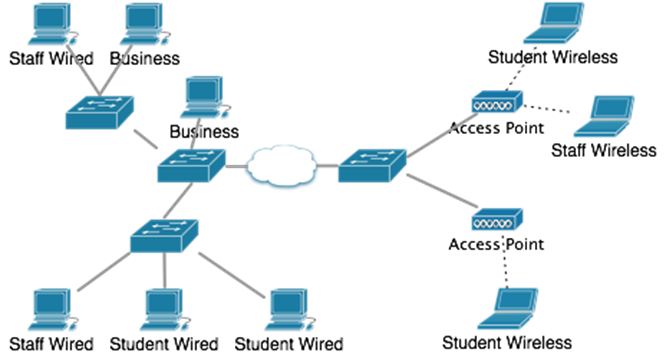


Figure 17.

With the use of VLANs in this network, it is possible to have machines in different subnets that are physically dispersed within the network. That is something that would otherwise be quite impractical.

There is more to be said about VLAN management, most notably, about how a VLAN database mapping between VLAN identifiers and a name can be shared amongst the various switches, using the VLAN Trunking Protocol (VTP). More difficult is how you can automatically assign a VLAN based on protocols such as 802.1X, but that is outside the scope of this lab.

## Function of VLAN

VLANs can also help create multiple layer 3 networks on a single physical infrastructure. For example, if a DHCP server is plugged into a switch it will serve any host on that switch that is configured for DHCP. By using VLANs, the network can be easily split up so some hosts will not use that DHCP server and will obtain link-local addresses, or obtain an address from a different DHCP server.

VLANs are layer 2 constructs, compared with IP subnets, which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent layer 2 and layer 3 constructs that map to one another and this correspondence is useful during the network design process.

By using VLANs, one can control traffic patterns and react quickly to relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.

# Motivation and function of a trunk port

## Motivation for trunk port

Trunks are used to interconnect switches to form networks, and to interconnect local area networks (LANs) to form wide area networks (WANs) or virtual LANs (VLANs). A trunk often consists of multiple wires, cables, or fiber optic strands to maximize the available bandwidth and the number of channels that can be accommodated. A trunk can also be a broadband wireless link. The use and management of trunks in a communications system is known as trunking. It minimizes the number of physical signal paths, and thus the total amount of cable hardware, required to serve a given number of subscribers in a network.

## Function of trunk port

A trunk is a line or link designed to handle many signals simultaneously, and that connects major switching centers or nodes in a communications system. The transmitted data can be voice (as in the conventional telephone system) data, computer programs, images, video or control signals.

In Cisco networks, trunking is a special function that can be assigned to a port, making that port capable of carrying traffic for any or all of the VLANs accessible by a particular switch. Such a port is called a trunk port, in contrast to an access port, which carries traffic only to and from the specific VLAN assigned to it.

## VLAN Tagging

When VLANs span multiple switches, VLAN Tagging is required. A VLAN is a method of creating independent logical networks within a physical network. VLAN Tagging is the practice of inserting a VLAN ID into a packet header in order to identify which VLAN (Virtual Local Area Network) the packet belongs to. More specifically, switches use the VLAN ID to determine which port(s), or interface(s), to send a broadcast packet too. VLAN Tagging support allows administrators to deploy Proxy SG appliances in line with switches that are routing VLAN traffic without the risk of losing VLAN ID information.

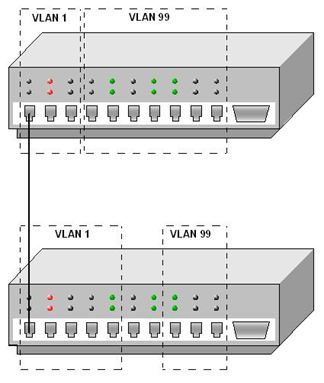


Figure 18.

# Conclusion

The scope of the project ‘’VLAN-Switch ‘’ was to put in practice all the theory learned during the first semester in networking. The project has theory on many points:

* The ProCurve switch
* Implementation of Trunk Ports
* Possible Network Security measures
* Configuration of the switch and configuration procedure
* Accessing via console port and Telnet
* Explain about CLI, Setup and Menu
* Accessing via WEB-interface
* Adding VLANs and ports/interfaces to individual VLANs
* Adding “security” to selected interfaces
* Test the function of the complete configuration
* Motivation and function of VLAN
* Motivation and function of a trunk port
* VLAN Tagging

Things that been learned during the task list :

1 . To ping two computers the firewall and virtual machines must be closed . After that check the antivirus\* ( if you have one on your computer and deactivate or disable the protection , if it doesn’t work you need to uninstall the antivirus from your computer ) .

2. Creating virtual networks using VLANs : - Things that need to be known : -

- VLANs can be trunked by a single cable.

- Connect the primary and secondary lines to separate switches when possible

.