



Laboratory I

Binna, Reschenhofer, Schörghofer

Course: Internet Infrastructure and Security

Lecturer: FH-Prof. DI Mag. Dr. Dominik Engel

22.11.2016

Table of Contents

Table of Contents	i
List of Abbreviations	1
1 VLANs and Subnetting	2
2 Topology	3
2.1 Basic configuration	3
2.2 Spanning Tree	4
3 VTP	5
4 Virtual Local Area Network (VLAN) setup	6
5 Inter-VLAN Routing	7
6 Remote Administraion	8
6.1 SSH	8

List of Abbreviations

STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network
MOTD	Message of the Day
PVST	Per-VLAN Spanning Tree
VTP	VLAN Trunking Protocol
SSH	Secure Shell

1 VLANs and Subnetting

The given network was a 192.168.1.0/24 network, which had to be divided into 4 subnets. Each subnet had its own VLAN.

VLAN	Hosts	Network ID/Subnet	First usable IP	Broadcast IP
10	120	192.168.1.0/25	192.168.1.1	192.168.1.127
20	60	192.168.1.128/26	192.168.1.129	192.168.1.191
30	30	192.168.1.192/27	192.168.1.193	192.168.1.223
99	10	192.168.1.224/28	192.168.1.224	192.168.1.239

Table 1.1: VLANs and Subnets

The final subnetting that was used in the lab can be seen in table 1.1.

The first usable IP address in each subnet was given to the router to that subnet.

2 Topology

The following topology (Figure 2.1, taken from the Moodle instructions, had to be recreated in the lab.

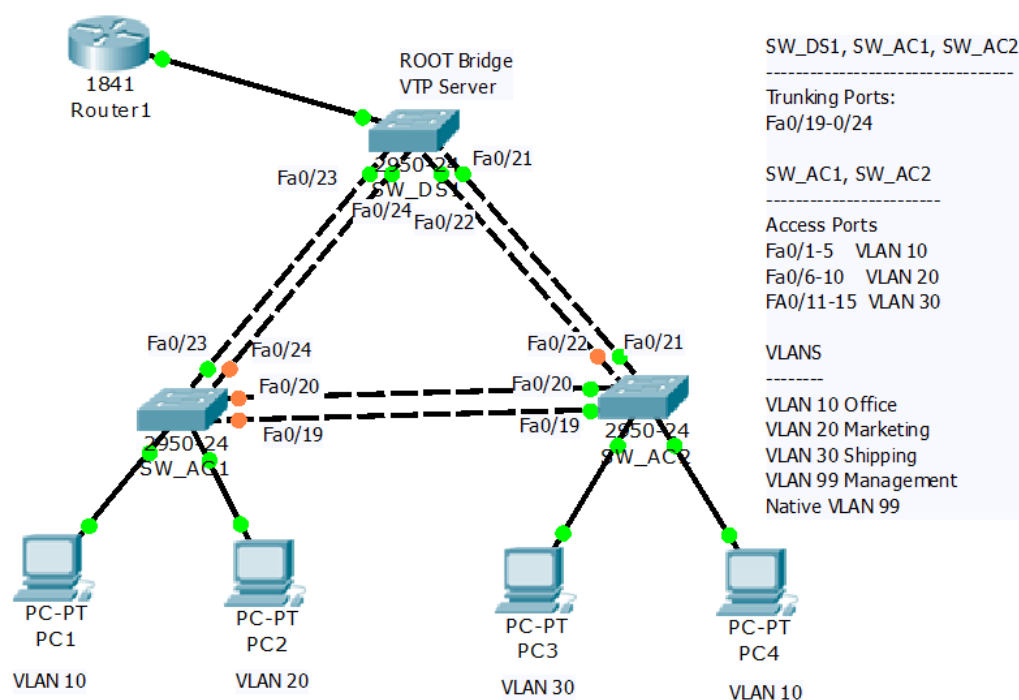


Figure 2.1: Topology (Moodle)

2.1 Basic configuration

Each device was configured with basic settings like Hostname, Message of the Day (MOTD) and a password.

```

1 enable
2 conf terminal
3 hostname SW_AC1
4 banner motd # Unauthorized access prohibited! #
5 enable secret cisco
6 service password-encryption

```

Listing 2.1: Basic configuration

These few lines would set hostname and the MOTD and encrypt the configured password 'cisco'.

These settings were applied onto every device, with the hostname changed.

2.2 Spanning Tree

The use of the Spanning Tree Protocol (STP) allows to detect loops in the network and creates a first redundancy layer. STP uses a tree structure in which every Switch (bridge) in the network knows the best path to the root bridge. Redundant paths to the root bridge will be blocked for normal traffic.

SW_DS1 had to be configured as root bridge.

```
1 conf terminal
2 spanning-tree mode pvst
3 spanning-tree vlan 1,10,20,30,99 priority 4096
```

Listing 2.2: STP configuration root

This is the configuration for the root bridge. The bridge with the lowest bridge ID will become root bridge. In this configuration the ID is 4096, the other switches in the network have been set to a higher bridge ID to ensure that SW_DS1 becomes root.

The Per-VLAN Spanning Tree (PVST) mode has been used to spawn a STP instance per VLAN. This would allow to load balance certain VLANs to different paths, but this was not used in this lab. The PVST mode was used for all configured VLANs.

3 VTP

The VLAN Trunking Protocol (VTP) allows the distribution of configured VLANs to all switches in the VTP domain. This allows easier reconfiguration of VLANs. For this one switch has to act as the VTP server, while the other ones get the configuration from the server.

Similar to the STP root bridge, SW_DS1 had to be configured as VTP server.

```
1 vlan 10 name Office
2 vlan 20 name Marketing
3 vlan 30 name Shipping
4 vlan 99 name Management
5
6 vtp mode server
7 vtp version 2
8 vtp lab
9 vtp cisco
```

Listing 3.1: VTP and VLAN

Those commands created the 4 VLANs and the VTP server on SW_DS1.

Version 2 had to be used, as we encountered some problems with VTP version 3.

The client configuration for the switches can be seen in 3.2.

```
1 vtp mode client
2 vtp version 2
3 vtp lab
4 vtp cisco
```

Listing 3.2: VTP client

4 VLAN setup

In this chapter, the ports on the switch had to be configured as either VLAN access ports, or trunk ports for the uplinks to the other switches.

The assignment from VLAN to port can be seen in table 4.1.

Ports	VLANs
Fa0/1-5	10
Fa0/6-10	20
Fa0/11-15	30
Fa0/19-24	Trunk ports
everything else	1

Table 4.1: VLANs to ports

```

1 int range fa0/1 - 5
2 switchport mode access
3 switchport access vlan 10

```

Listing 4.1: Access port configuration

The commands in 4.2 have been adapted for the different VLANs. The access ports have been configured on both SW_AC1 and SW_AC2.

```

1 int fa0/21
2 switchport mode trunk
3 switchport trunk allowed vlan 10,20,30,99
4 switchport trunk native vlan 99

```

Listing 4.2: Trunk port configuration

The native VLAN is 99, which is also the management VLAN, which may not be wise from a security point of view. The native VLAN will not be tagged (802.1Q) when transmitted through the trunk port. For ease of configuration some unused ports were assigned to the Management VLAN.

To test this configuration we put a PC in each VLAN on each switch and used the ‘ping’ tool, which showed a successful configuration.

5 Inter-VLAN Routing

To make communication between the VLANs possible a router needs to be used. The router has an IP address (see table 1.1) in each subnet. All PCs can therefore reach the router.

```
1 conf terminal
2 int Gig0/0.10
3 encapsulation dot1q 10
4 ip address 192.168.1.1 255.255.255.128
```

Listing 5.1: Router configuration

The commands in listing 5.1 will create a subinterface on gig0/1 and set the encapsulation to the IEEE 802.1Q standard. Then an IP address is assigned to that interface. This commands have been adopted for every VLAN.

For the native VLAN, the encapsulation line had been changed to:

```
encapsulation dot1Q 99 native
```

to mark VLAN 99 as the native VLAN.

6 Remote Administraion

In this chapter remote access via Secure Shell (SSH) had to be configured for each switch and the router.

The management interface on the switches was created in the management VLAN.

```
1 conf terminal
2 interface Vlan99
3   ip address 192.168.1.226 255.255.255.240
4   no shutdown
```

Listing 6.1: Management interface

The IP addresses were assigned beginning with 192.168.1.225 for the router and ending with 192.168.228 for SW_AC2.

6.1 SSH

SSH(v2) is a protocol for a secure connection to another device which should be used instead of insecure protocols like Telnet. For SSH access a domain name and a user had to be created.

```
1 conf terminal
2 ip domain-name its.its
3 crypto key generate rsa 1024
4 username admin secret cisco
5 line vty 0 4
6 login local
7 transport input ssh
```

Listing 6.2: SSH

The commands from listing 6.2 will create this. The key length has been set to 1024 bit for convenience, as it would take more time to create a key with a length of 2048 bit.