fhs

Fachhochschule
Salzburg

Laboratory I

Binna, Reschenhofer, Schörghofer

Course: Internet Infrastructure and Security

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

22.11.2016

Table of Contents

List of Abbreviations

MAC	Media Access Control
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
DHCP	Dynamic Host Configuration Protocol

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.

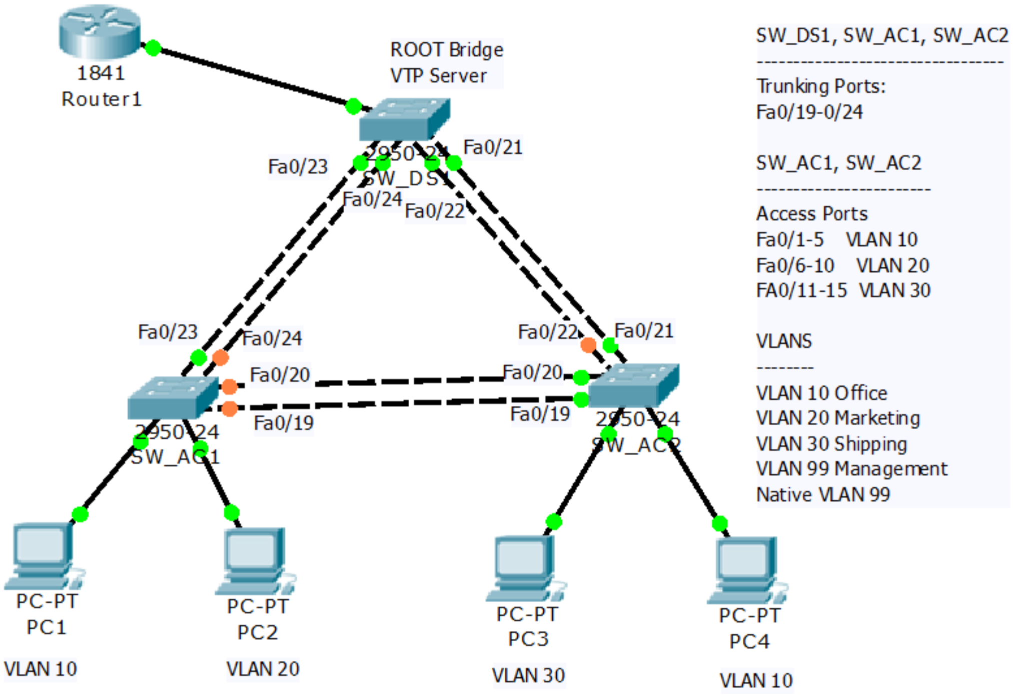

Figure 2.1: Topology (Moodle)

2.1 Basic configuration

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

```
enable
conf terminal
hostname SW_AC1
banner motd # Unauthorized access prohibited! #
enable secret cisco
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.

```
conf terminal
spanning-tree mode pvst
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.

```
vlan 10 name Office
vlan 20 name Marketing
vlan 30 name Shipping
vlan 99 name Management

vtp mode server
vtp version 2
vtp lab
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.

```
vtp mode client
vtp version 2
vtp lab
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

```
int range fa0/1 - 5
switchport mode access
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`.

```
int fa0/21
switchport mode trunk
switchport trunk allowed vlan 10,20,30,99
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 where 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.

```
conf terminal
int Gig0/0.10
encapsulation dot1q 10
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.

```
conf terminal
interface Vlan99
 ip address 192.168.1.226 255.255.255.240
 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.

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

Listing 6.2: SSH and user creation

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.

7 Layer 2 Security

In this chapter Layer 2 security was applied to the switches.

First, unused switchport were shut down, as can be seen in listing ??.

```
conf terminal
ip range fa0/3 - 20
shutdown
```

Listing 7.1: Shutdown unused ports

This command has been adopted on the switches, this example was applied on `SW_DS1`.

Another security feature is to allow only a certain amount of Media Access Control (MAC) addresses per switchport and deactivate the port if more addresses are seen from it.

```
conf terminal
ip range fa0/11 - 15
 switchport port-security
 switchport port-security mac-address sticky 1
 switchport port-security violation shutdown
```

Listing 7.2: Sticky MAC addresses

In listing 7.2 such a configuration can be seen. The maximum allowed MAC addresses is set to 1. Meaning only one device is allowed on that port, if a violation of that rule should occur the port will be shut down and has to be reactivate manually.

8 DHCP

Dynamic Host Configuration Protocol (DHCP) is a method to distribute IP addresses in a network automatically. DHCP clients are available on nearly every operating system.

The router was configured to act as DHCP server, distributing IP addresses to clients in the VLANs.

```
ip dhcp pool VLAN10
 network 192.168.1.0 255.255.255.128
 domain-name VLAN10
 default-router 192.168.1.1
```

Listing 8.1: DHCP

With these commands (8.1) the router will act as a DHCP server and will distribute IP addresses in the `192.168.1.0/25` subnet. Those commands were also entered for the other VLANs.

8.1 DHCP Snooping

DHCP Snooping is a method to block rogue DHCP servers which can handle out wrong IP addresses. It can also be used to limit the amount of IP addresses a port can request in a given amount of time, to counter IP address shortage. DHCP responses may also be only allowed from certain ports, not access ports where clients are connected. As DHCP has no authentication method this must be used if security is important.

```
ip dhcp snooping vlan 10,20,30,99
ip dhcp snooping database flash
ip dhcp snooping

int fa0/21
ip dhcp snooping trust
```

Listing 8.2: DHCP Snooping

The access switches have been configured for DHCP snooping, as can be seen in listing 8.2. The trunk ports have been configured as trusted DHCP interfaces.

To test this setup, we removed the trust from one of the interfaces, and tried to get an IP from the router, which then failed.

However, a rogue DHCP server in the same subnet was still possible. We could not determine what caused this, as the binding table remained empty, even if a DHCP lease was given out to a valid client.

Most likely the `no ip dhcp snooping trust` and `ip dhcp snooping limit rate 10` had to be used on the access ports, but we did not use this command, so this might be the reason it did not work as expected. The last command would have limited the amount of DHCP packets to 10 per minute.