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 192.168.1.0/24, which had to be divided into 4 subnets. Each subnet corresponded to a specific 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 subnets that were used in the lab can be seen in table 1.1.

The first usable IP address in each subnet was assigned to the subinterface of that network at the router.

2 Topology

The following topology (figure 2.1, taken from the moodle instructions) had to be recreated in the lab.

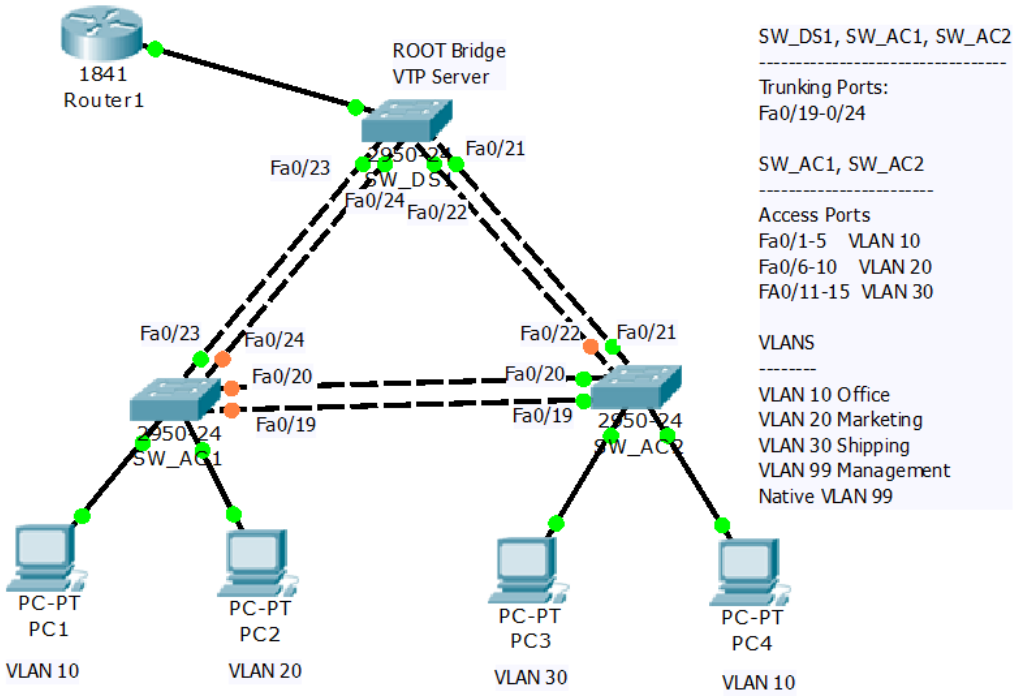

Figure 2.1: Topology (Moodle)

2.1 Basic configuration

Each device was configured with basic settings like hostname, Message of the Day (MOTD), a secret enable password, disabled IP domain lookup, synchronous logging on line console 0 and the service password-encryption, which prevents passwords from being displayed in cleartext in the start-up and running configuration.

```
enable
conf terminal
hostname SW_AC1
banner motd # Unauthorized access prohibited! #
enable secret cisco
service password-encryption
no ip domain-lookup
line con 0
```

```
9       synchronous logging
```

Listing 2.1: Basic configuration

These settings were applied to every device, with a respectively different hostname.

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 left at the default priority which is higher and enables `SW_DS1` to become root.

The Per-VLAN Spanning Tree (PVST) mode has been used to spawn a STP instance per VLAN. This would allow load balancing of 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 VTP to work one switch has to act as the VTP server and the switches that need to receive the configuration have to be set as VTP clients.

Similar to the STP root bridge, `SW_DS1` had to be configured to act 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 domain lab
vtp password cisco
```

Listing 3.1: VTP and VLAN

The commands listed above create the 4 VLANs and the VTP server on `SW_DS1`.

Version 2 had to be used, as we encountered the following problem when using VTP V3:

VTP V3 rejected the deletion of VLANs on the VTP server as well as on the VTP clients. The following error message appeared when trying to delete VLANs:
VTP VLAN configuration not allowed when device is not the primary server for vlan database.

Moreover important was to explicitly set a VTP password, otherwise the following message may appear:
**** MD5 digest checksum mismatch on trunk: Fa0/xx ****

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

```
vtp mode client
vtp version 2
vtp domain lab
vtp password 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 port VLAN assignment 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

```
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 commands in listing 4.2 have been adapted to match the different VLANs. The access ports have been configured on both `SW_AC1` and `SW_AC2`.

The native VLAN is 99, which is also the management VLAN. From a security point of view it's not recommended to set the native VLAN to the same as the management VLAN.
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 for verification, which showed a successful configuration.

5 Inter-VLAN Routing

To make communication between the VLANs possible a router needs to be used. This type of setup is normally known as router on a stick. Subinterfaces with IP addresses for each subnets (see table 1.1) have been configured. Thus all PCs are able to communicate with the router and also with PCs on different subnets (when the default gateway on the PCs is correctly set to the IP address of the subinterface on 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 subinterface.

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 Administration

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, a user and certificates have 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 configure SSH on the device. 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. Moreover, the virtual terminal line has been configured to only allow ssh input and use the local database for authentication.

7 Layer 2 Security

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

First, unused switchports were shut down, as seen in listing 7.1.

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

Listing 7.1: Shutdown unused ports

This command has been adopted to all switches, the example was applied to `SW_DS1`.

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

```
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

Listing 7.2 shows such a configuration. The maximum allowed MAC addresses is set to 1, which means that only one device is allowed on that port. If a second device with a different MAC address connects to the port a violation will be thrown and the port will shut down. In order to reactivate the port it has to be manually shut down and enabled again.

8 DHCP

Dynamic Host Configuration Protocol (DHCP) is a method to distribute IP addresses (in form of DHCP leases) in a network automatically. Almost all operating systems have available DHCP clients.

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 set for the other VLANs.

8.1 DHCP Snooping

DHCP Snooping is a method to block rogue DHCP server 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 in order to counterfeit IP address shortage. DHCP responses may also be restricted to certain ports. In example an access port, where a client computer is connected, should nit issue DHCP responses. As DHCP has no authentication mechanism DHCP snooping should be implemented if security is from importance.

```
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 seen in listing 8.2. The trunk ports have been configured as trusted DHCP interfaces.

To test this setup, the trust from one of the uplink interfaces to the router was removed, thus the client computer wasn't able to get a DHCP lease from the router anymore.

However, a rogue DHCP server in the same subnet would still be possible. We could not determine the root of this problem, because the binding table always remained empty, even if a DHCP lease was sent 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.