Practical Computer Networks and Applications

Exercise 3 – DHCP and VLAN

Prof. Dr. Baun, Prof. Dr. Ebinger, Prof. Dr. Hahm, Prof. Dr. Kappes, Dipl. Inf. (FH) Maurizio Petrozziello

{baun,cocos,peter.ebinger,oliver.hahm,kappes,petrozziello}@fb2.fra-uas.de

Frankfurt University of Applied Sciences
Faculty of Computer Science and Engineering
Nibelungenplatz 1
60318 Frankfurt am Main

Contents

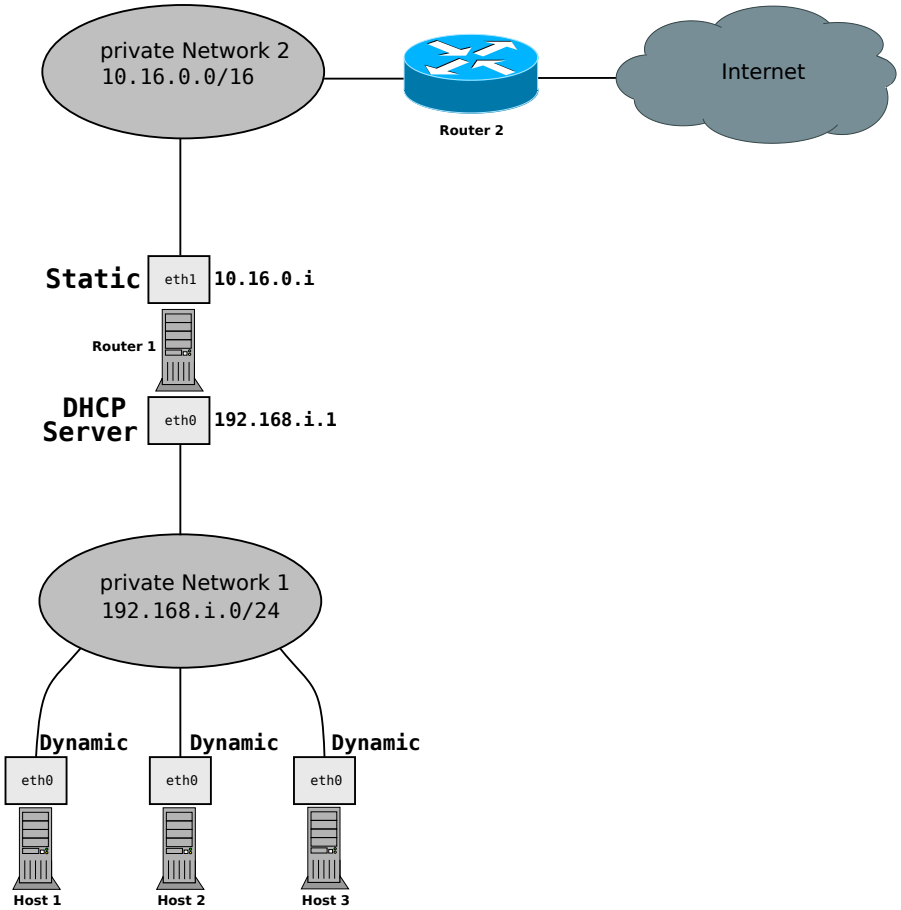
Exercise 3

DHCP

VLAN

TP-Link TL-SG108E - Managed Switch

Network Topology – Exercise 3 – DHCP



Network Topology of lab exercise 3 – DHCP

Private Network 1:

`192.168.i.0/24`

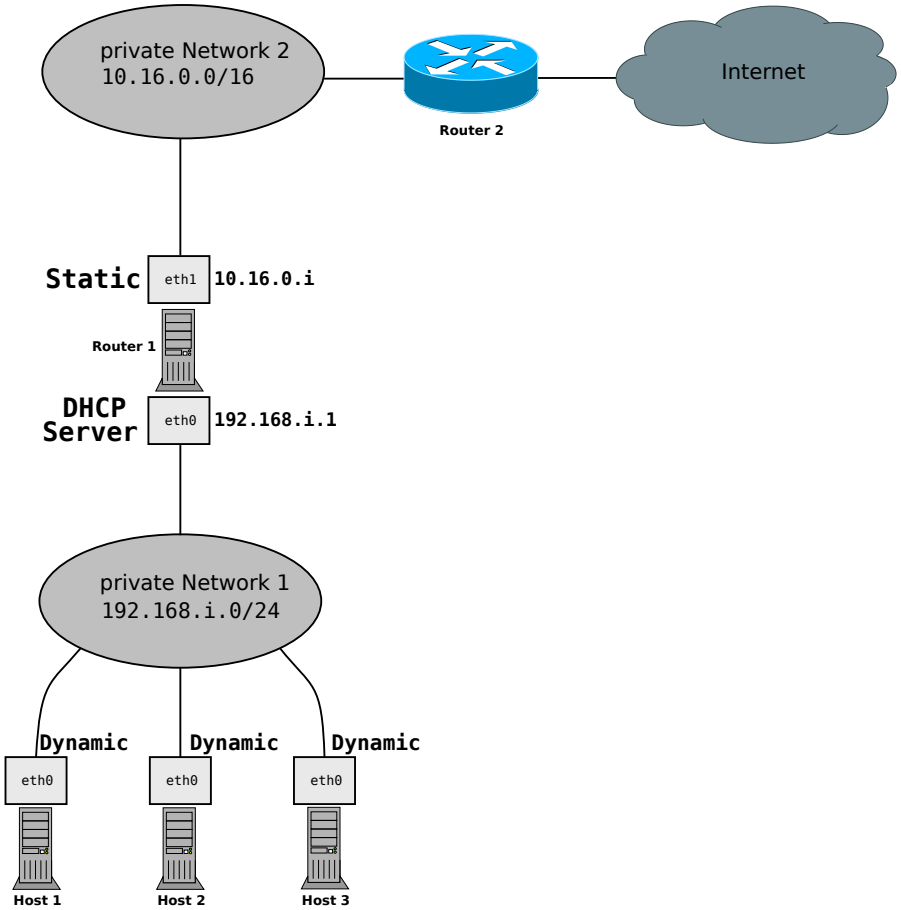
Private Network for host machines and router

Private Network 2:

`10.16.0.i/16`

Private Network spanning all networks

Network Topology – Private Network 2



Network Topology of lab exercise 3 – DHCP

Private Network 2:

`10.16.0.i/16`

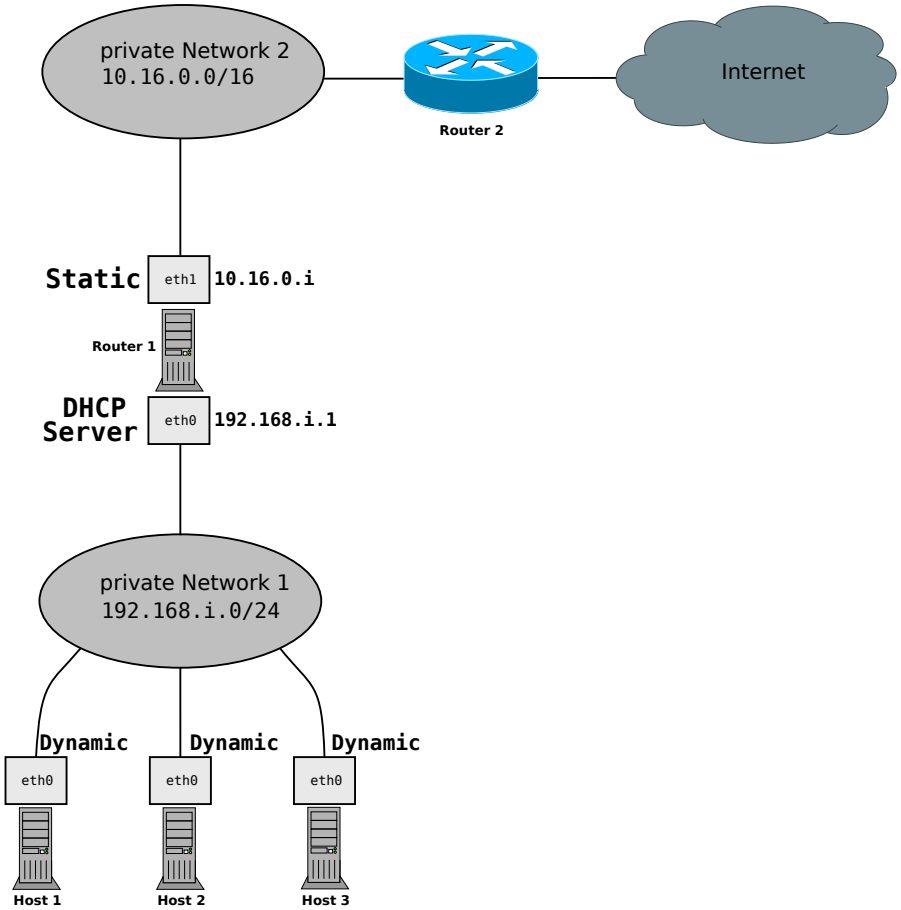
Router 2:

`10.16.0.200`

Router 2 is the gateway for all routers in private network 1!

The route to **Router 2** needs to be configured on **Router 1**!

Network Topology – Private Network 1



Network Topology of lab exercise 3 – DHCP

Private Network 1:

`192.168.i.1`

Running `isc-dhcp-server`

Configures Hosts dynamically

Router 1:

1. `eth0` – `192.168.i.1`
2. `eth1` – `10.16.0.i`

Host Network:

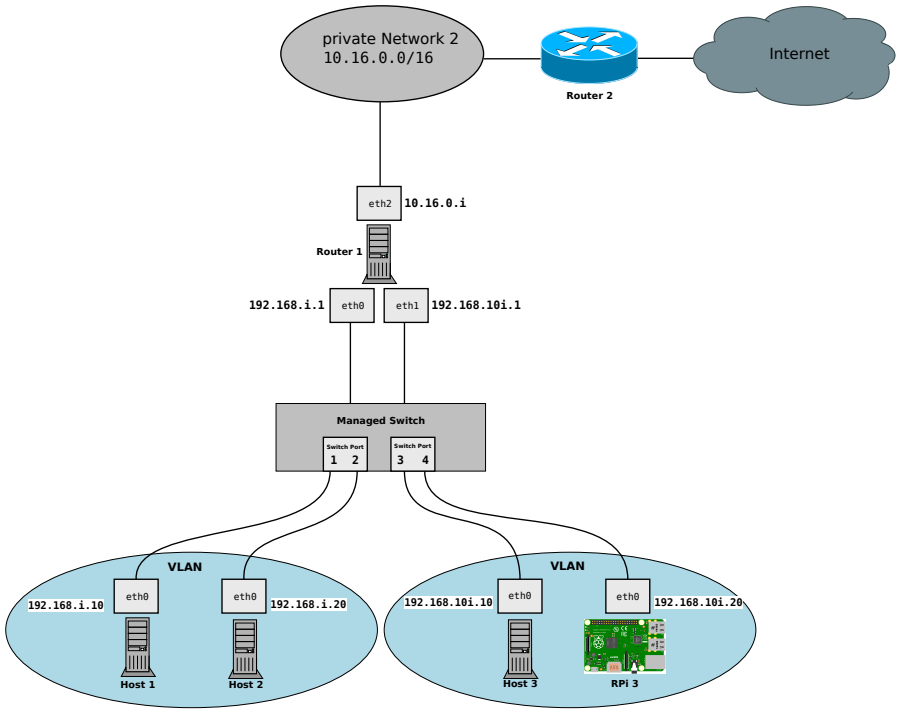
Router 1 – `192.168.i.1`

Host 1 – `DHCP`

Host 2 – `DHCP`

Host 3 – `DHCP`

Network Topology – Exercise 3 – VLAN



Network Topology of lab exercise 3 – VLAN

Private Network 1:

`10.16.0.0/16`

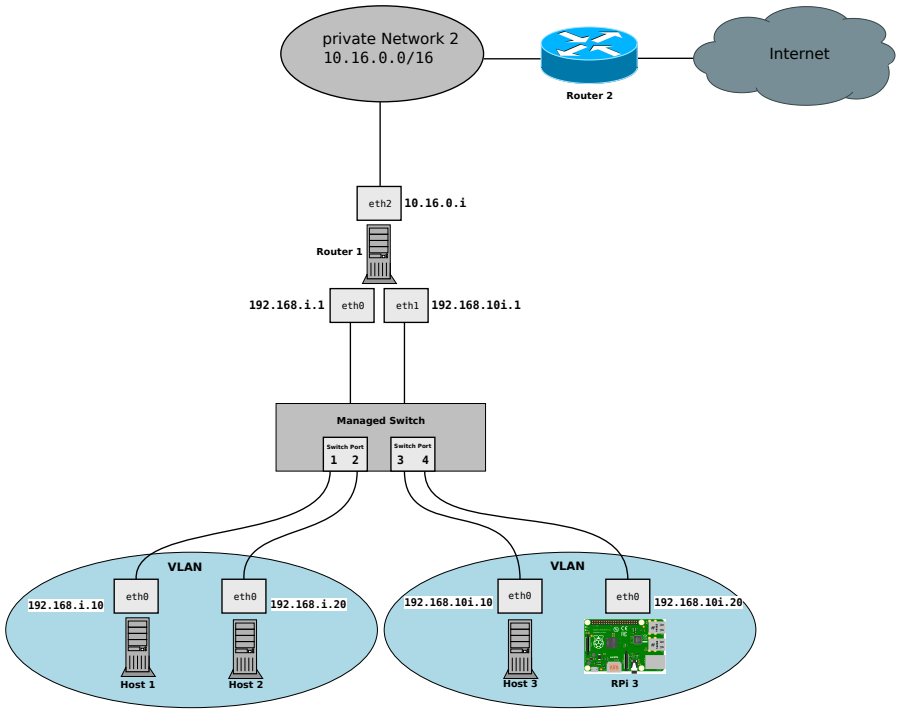
Private Network for host machines and router

Private Network 2:

`192.168.i.0/24`

Private Network spanning all networks

Network Topology – Private Network 1



Network Topology of lab exercise 3 – VLAN

Private Network 1:

`192.168.i.1`

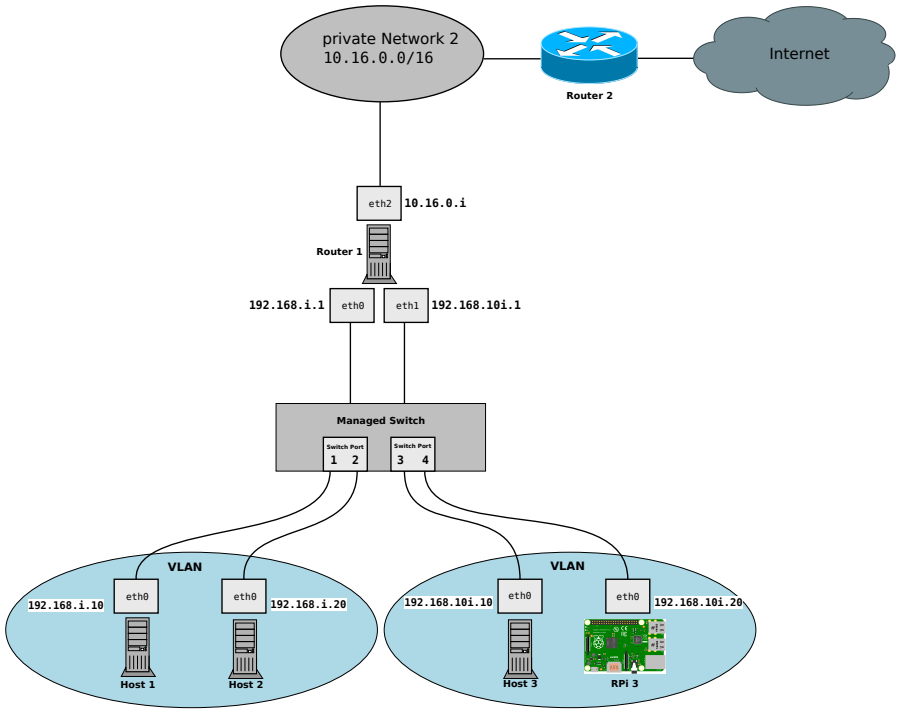
Router 1:

1. Interface `eth0` – `192.168.i.1`
2. Interface `eth1` – `10.16.0.i`

Host VLAN:

1. **VLAN 10**
2. **VLAN 20**

Network Topology – Private Network 1



Network Topology of lab exercise 3 – VLAN

Private Network 1:

`eth0` – `192.168.i.1`

`eth1` – `192.168.10i.1`

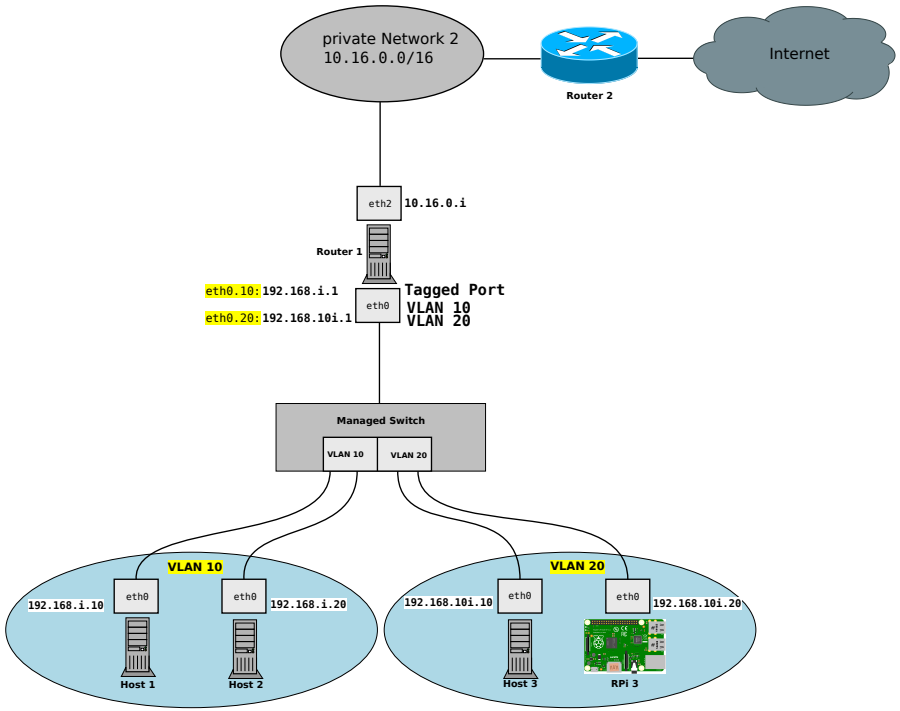
VLAN 10:

1. **Host 1** – `192.168.i.10`
2. **Host 2** – `192.168.i.20`

VLAN 20:

1. **Host 3** – `192.168.10i.10`
2. **RPi 3** – `192.168.10i.20`

Network Topology – Private Network 1



Network Topology of lab exercise 3 – VLAN 802.1.Q

Private Network 1:

`eth0.10` – `192.168.i.1`

`eth0.20` – `192.168.10i.1`

VLAN 10:

1. **Host 1** – `192.168.i.10`
2. **Host 2** – `192.168.i.20`

VLAN 20:

1. **Host 3** – `192.168.10i.10`
2. **RPi 3** – `192.168.10i.20`

Network Topology – Exercise 3 – Objectives

In the lab exercise you need to accomplish...

- ✓ a successful dynamic configuration of the machines!
- ✓ successful configuration of `isc-dhcp-server`!
- ✓ successful configuration of port-based VLAN!
- ✓ successful configuration of 802.1Q VLAN!
- ✓ successful configuration of Quality of Service!
- ✓ reachability of all machines (all hosts including **Router 1** and **2**)!

Contents

Exercise 3

DHCP

VLAN

TP-Link TL-SG108E - Managed Switch

Dynamic Host Configuration Protocol – DHCP

The Dynamic Host Configuration Protocol (DHCP) is used to control the assignement of IP-Adresses

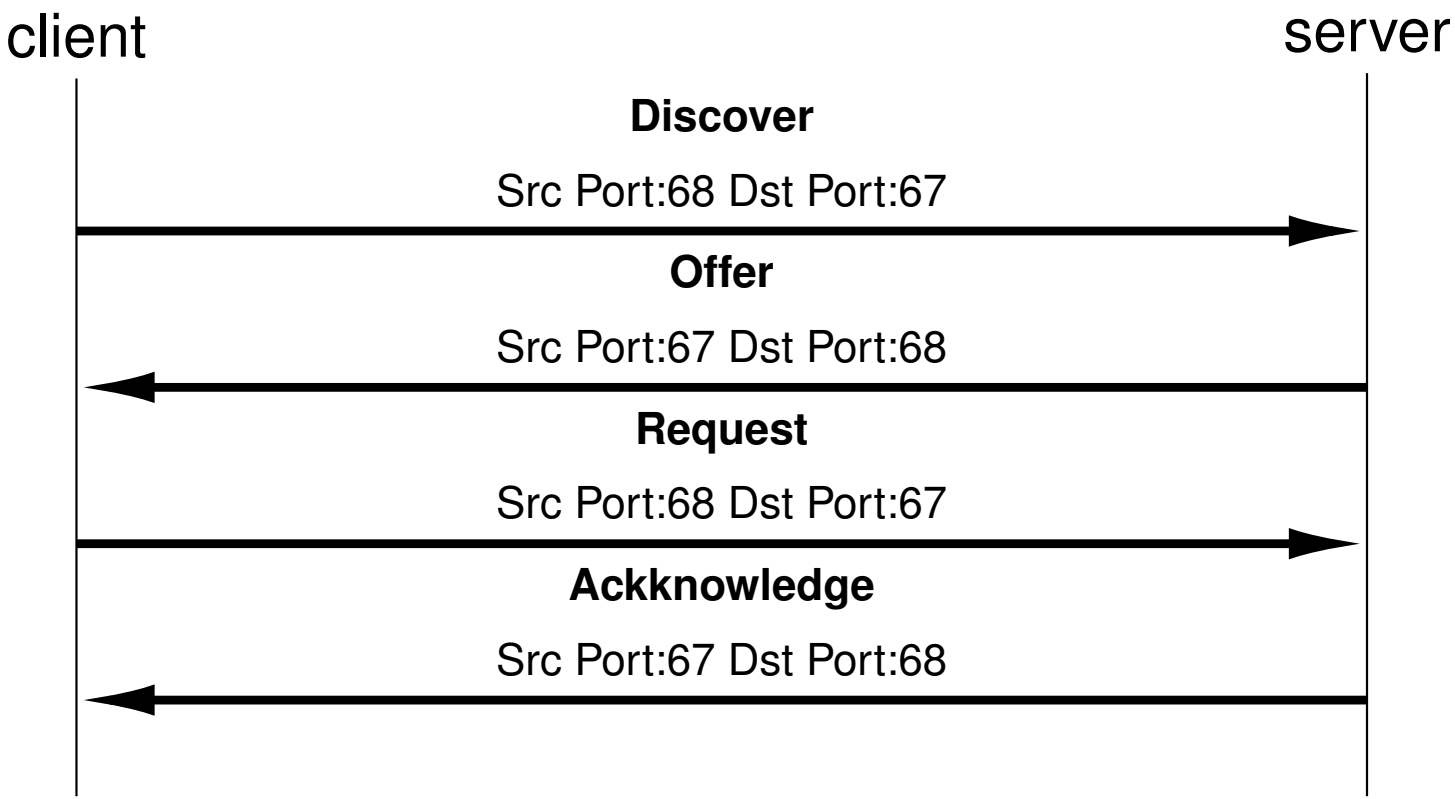
The assignment of IP-Addresses and network configurations is managed by a DHCP-Server

The DHCP-Server in a private network is usually the Router/Gateway

DHCP vs `bootp`

The Bootstrap Protocol `bootp` (RFC 951) is the core protocol for dynamically assigning IP-Addresses, netmasks, and gateways. However in large private networks additional information is needed. Therefore DHCP (RFC 1541) was invented which is an extension of the Bootstrap Protocol. The flow of `bootp` is shown in the next slide.

Dynamic Host Configuration Protocol – Bootstrap Protocol



Message Sequence Diagramm for DHCP

DHCP Server – Linux

In Linux the DHCP Server `isc-dhcp-server` can be used to configure DHCP on a Router

The DHCP Server is configured in the two configuration files `/etc/default/isc-dhcp-server` and `/etc/dhcp/dhcpd.conf`

In these files the parameters for the gateway of the network are defined

Configurations in `/etc/dhcp/dhcpd.conf`

Among others defined are...

- IP addresses, subnet masks,
- DNS servers,
- Lease times,...

DHCP Client – Linux

In Linux the DHCP Client `dhclient` can be used to configure DHCP on a Client

The DHCP Client is configured in the configuration file `/etc/dhcp/dhclient.conf`

In these files the parameters for the client are defined

Dynamic Host Configuration Protocol – Wireshark

In Wireshark the exchange ot DHCP messages can be displayed with the filter `bootp`

The behaviour of `dhclient` DHCP message exchange can be changed by adjusting the configuration file `/etc/dhcp/dhclient.conf`

The option `bootp-broadcast-always` changes the behaviour of `dhclient`

`dhclient` option

By setting the option `bootp-broadcast-always` the DHCP client can be adjusted to use broadcast messages instead of unicast messages. This option is important since older clients do not support unicast messages in DHCP.

Contents

Exercise 3

DHCP

VLAN

TP-Link TL-SG108E - Managed Switch

Virtual Local Area Network – VLAN

VLAN is used to subdivide physical networks on Layer 2 (Data-Link Layer)!

For the definition of VLANs **managed switches** are needed

There are two types of VLAN definitions:

Port-based VLAN – Definition of Ports in a Switch

802.1Q – Definition of **Tagged VLAN ID** in the Switch and/or NIC (Network interface card)

Port-based vs. 802.1Q

Port-based VLAN was invented in order to obtain backward compability for older NICs. In Port-based VLAN definitions the VLAN is transparent for the clients NIC and managed by the Switch. In 802.1Q VLAN the Ethernet frame is extended by a VLAN ID inside of the frame header.

Virtual Local Area Network – Port-based VLAN

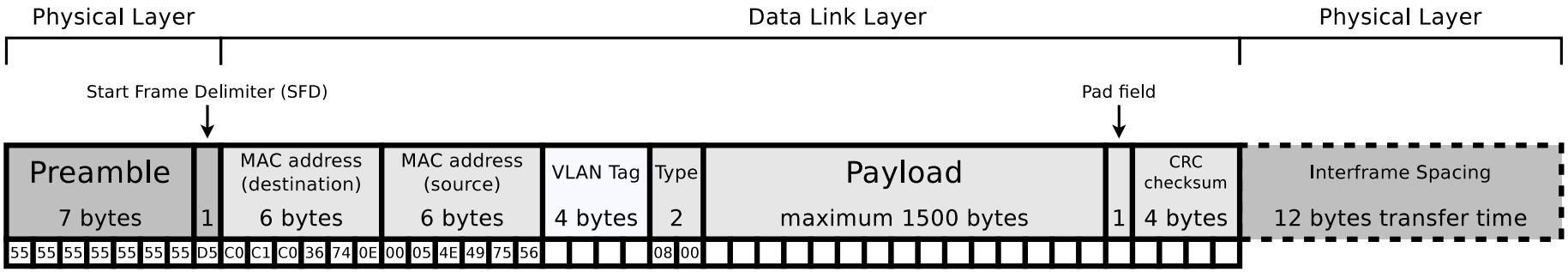
Port-based VLAN works in the following way:

- Each Port is assigned to a VLAN and the physical network is subdivided by the Switch!
- Only frames defined for a specific VLAN can be accessed by hosts in this VLAN!
- Tags in a frame are extracted by the Switch and the frame is forwarded without the tag!

Port-based VLAN

Port-based were the first edition of VLANs and are suitable for all hosts connected to a Switch, since the VLAN tags are managed by the Switch. In the past only servergrade NICs were capable of identifying VLAN tags.

Virtual Local Area Network – VLAN 802.1Q



The fields for the physical addresses (MAC addresses) of sender and destination are 6 bytes long each

The 4 bytes long optional VLAN tag contains, among others. . .

VID a 12 bits long VLAN ID

PCP a 3 bits long field for the priority information

VLAN

With 12 bits for the VLAN ID 4094 VLANs can be addressed (ID 0 and 4095 are reserved)! The 3 bits for priority information is used for the definition of Quality of Service (QoS) in Ethernet!

Virtual Local Area Network – Linux

In Linux the `ip` command can be used to configure VLAN IDs:

`ip link add link eth0 name eth0.X type vlan id X`[1] – adds a VLAN tag to an interface

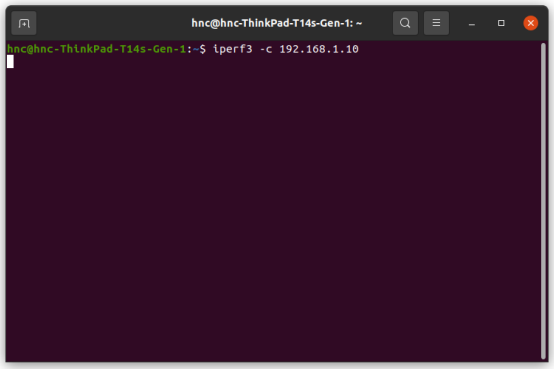
`ip addr add <IP ADDRESS> dev eth0.X` – adds an IP address to a tagged interface

Tagged interfaces

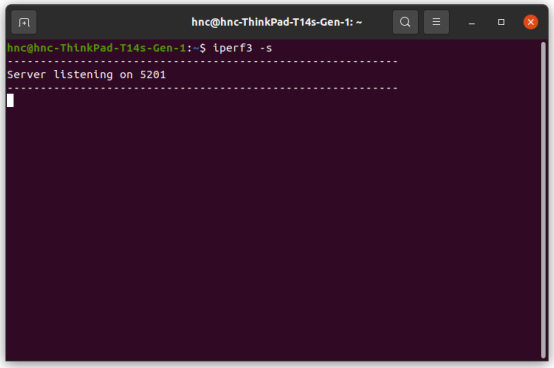
By using tagged interfaces in Linux multiple IP addresses and physical networks can be assigned to a single NIC. This way multiple services can be logicallly and physically seperated from each other on host side!

[1] `X` corresponds to the VLAN ID! `eth0` corresponds to the interfaces!

iperf3



(a) `iperf3` on clientside



(b) `iperf3` on serverside

Functionality:

Measurements of the maximum achievable bandwidth on IP networks.

Used for metrics in a network and optimization

One host is started as server (`-s` option)

One host is started as client (`-c` option)

Contents

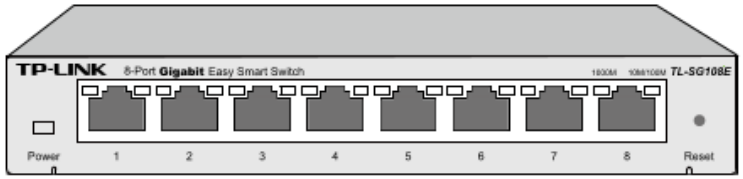
Exercise 3

DHCP

VLAN

TP-Link TL-SG108E - Managed Switch

TP-Link TL-SG108E - Managed Switch



TP-Link TL-SG108E - Front

Functionality:

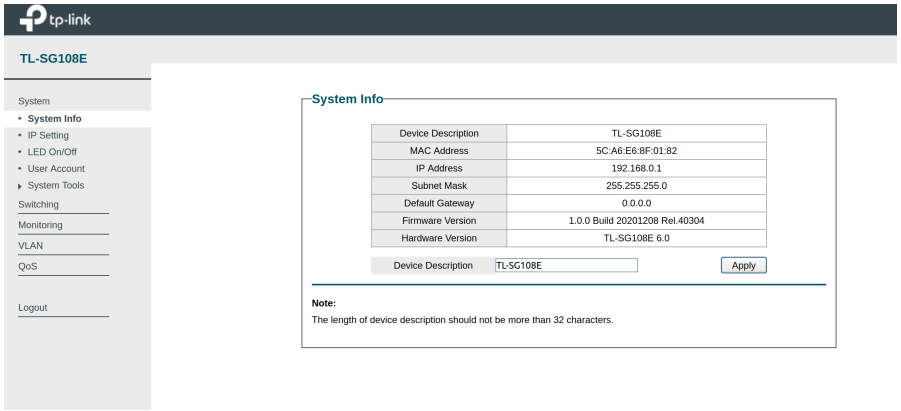
8-port Switch 1GBit/s

Port-based and 802.1Q VLAN

Quality of Service 802.1p and DSCP

Loop Prevention

TP-Link TL-SG108E - System Panel



TP-Link TL-SG108E - Management Panel

Login:

IP: `192.168.0.1`

User: **admin**

PW: **admin**

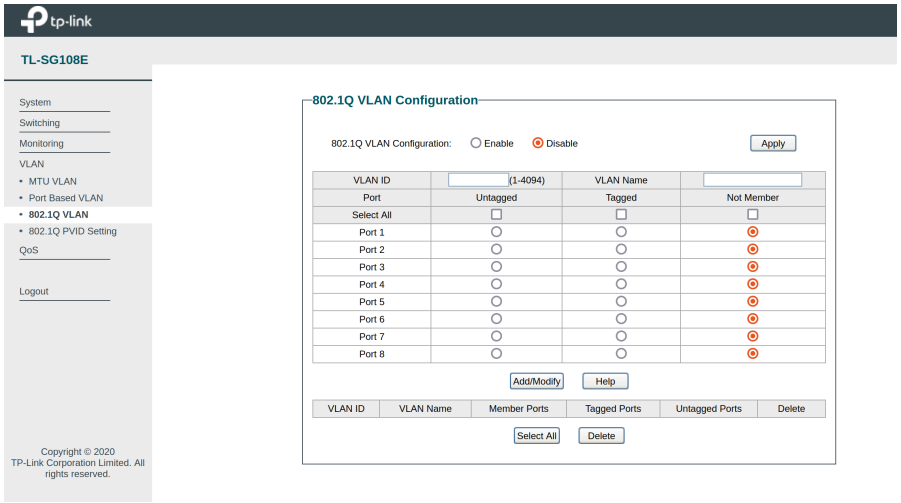
Needs to be changed after login!

System Panel

The managed Switch has a build in DHCP Server and is capable of dynamic network configurations. There is also a funtionality called *Loop Prevention* implemented, which periodically sends frames in the local network for loop detection[a]

[a] Further details: `https://en.wikipedia.org/wiki/Switching_loop`

TP-Link TL-SG108E - VLAN



TP-Link TL-SG108E - 802.1Q VLAN settings

VLAN functionality:

Port-based and 802.1Q (Tagged) VLAN

Port-based: Assign port to desired VLAN ID

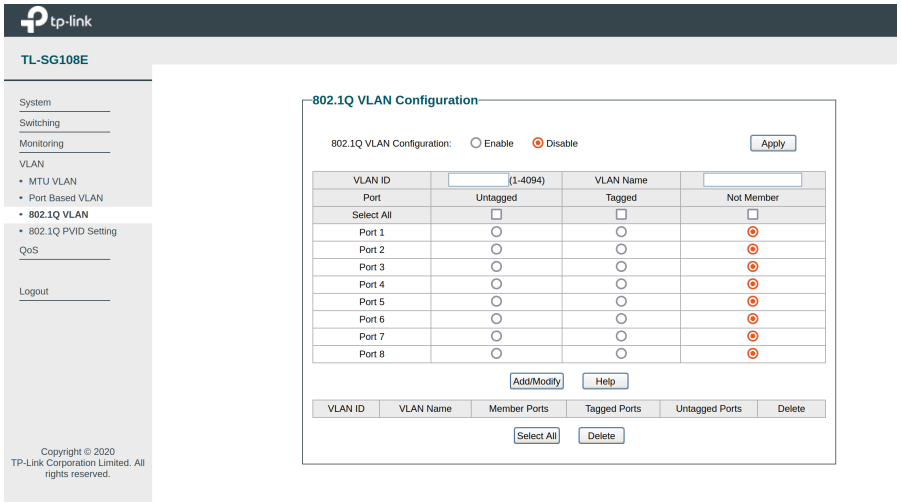
802.1Q: Assign a VLAN ID to a physical network

Default VLAN ID: Always 1!

Port-based vs 802.1Q VLAN

In contrast to 802.1Q VLAN the Port-based settings only assign a VLAN to a port, whereas 802.1Q assigns one or multiple VLAN tags to a port and can assign multiple physical networks to one port making it more flexible!

TP-Link TL-SG108E - VLAN - Ingress/Egress



TP-Link TL-SG108E - 802.1Q VLAN settings

Ingress vs Egress

Ingress → the incomming traffic

Egress → the outgoing traffic

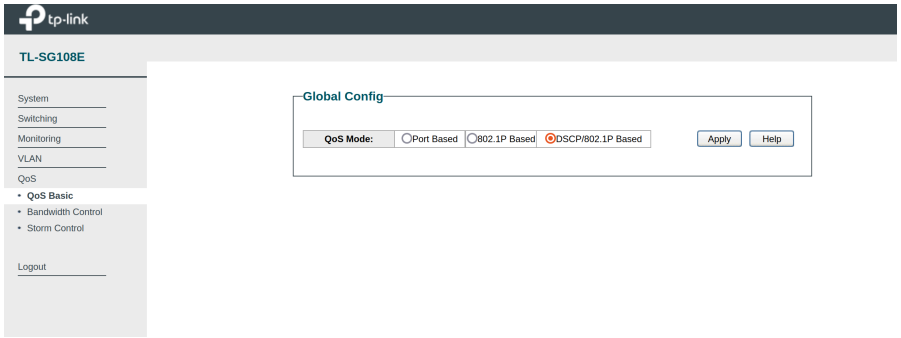
For untagged frames a default VLAN ID needs to be specified

Default VLAN ID: Always 1!

Configure Ingrees and Egress

In the Switch the Ingress rule needs to be specified in the *802.1Q VLAN* menu. The VLAN ID for Egress of the Ports need to be configured in the *802.1Q PVID Setting* menu! The default PVID is always 1!

TP-Link TL-SG108E - Quality of Service



TP-Link TL-SG108E - Quality of Service

QoS functionality:

Manage priority for traffic

Port-based: manages four different priority queues

802.1Q: Assigns a value for the 3-bit *802.1p* parameter in the frame (value between 0-7)

DSCP: Sets the ToS Byte in the IP Header (value between 0-63)

802.1p vs DSCP

802.1p is defined with 802.1Q Tagged VLANs and specifies 3-bit for the definition of priority in the traffic (see slide 19!). DSCP (Differentiated Services Code Point) is defined in the IP header and therefore applied on the network layer. Aforementioned 802.1p value is applied on the data-link layer.

Configuration of the machines

Please follow these rules:

Make your configurations statically! Use the tool `ip` exclusively!

Save your configuration on file! Use an USB-Drive for the extraction!

Test your setup and document it accurately! Demonstrate it in the lab exercise!

Make slides of your configurations! Use the command-line snippets, screenshots and Wireshark captures for your documentation!

Non persistent configuration on machines

Please be aware, that the configurations on the machines are static and will be deleted after a reboot! Make sure to save your progress on an external drive!