TECHNISCHE UNIVERSITÄT BERLIN
Fakultät IV – Elektrotechnik und Informatik
FG INET
Prof. Dr. Thomas Zinner
Theresa Enghardt, Apoorv Shukla, Damien Foucard, Thomas Krenc

Routerlab SoSe 2018
Worksheet 2: Static Routing and VLANs

In this worksheet, we will learn how to configure Virtual LANs (VLANs) which enable logical layer-2 networks to be configured upon a fixed physical topology. After configuring VLANs, we will set up routing between all the involved devices to create a fully routed network setup.

Table 1: Device and Address Overview

Cloud	Aachen	Köln	Leverkusen
Router	aac-rc1, aac-rj1, aac-rj2	cgn-rc1, cgn-rj1, cgn-rj2	lev-rc1, lev-rj1, lev-rj2
Switches	aac-sc1, aac-sj1	cgn-sc1, cgn-sj1	lev-sc1, lev-sj1
IPv4 range		10.Z.0.0/16	
IPv6 range		fc00:470:525b:fY00::/56	
Loadgens		groupX-lg1,2,3,4	

Note: Replace X with the number of your group with leading zero, e.g. $X = 03$ for group 3. Replace Y with the number of your group without leading zero and use hex encoding, eg $Y = 3$ for group 3 and $Y = a$ for group 10. Finally replace Z with the decimal group number without leading zero, e.g. $Z = 3$ for group 3.

Question 1: (18 (5+5+2+3+3) Points) *Virtual LANs (VLANs) in Theory*

Let's start by getting acquainted with what VLANs are, how they work, how they are used in practice and what the IEEE 802.1q standard is. To answer the following questions, please have a look through the following sources:

- http://en.wikipedia.org/wiki/Virtual_LAN
- The article *A Survey of Virtual LAN Usage in Campus Networks*, see ISIS please.

(a) What are some motivations for using VLANs? Pick two use-cases and explain briefly (2-4 sentences each) how VLANs can solve the problem.

(b) What is the difference between *Port-based VLANs* and *VLAN Trunks* and what mechanism is used to distinguish between Ethernet frames of different VLANs on a trunk?

(c) How many VLANs (802.1q) could exist simultaneously in a network? Explain.

(d) Are there ways to overcome the limits of 802.1q? List at least two or explain why this is not possible.

(e) VLANs are often (ab)used to realize security, access-control, or mobility solutions. Briefly explain some problems and limitations that arise from using VLANs to achieve these more complex network management goals.

Question 2: (42 (5+10+2+5+20) Points) *Virtual LANs (VLANs) in Practice*

This section motivates some practical applications of VLANs. We start with a configuration without separating VLANs, then add VLAN configuration and take a look at what changed.

For this purpose, please have a look at Figure 1. It shows adjacencies between hosts and routers as thick dashed lines (one separate virtual LAN is characterized by a specific color and line style).

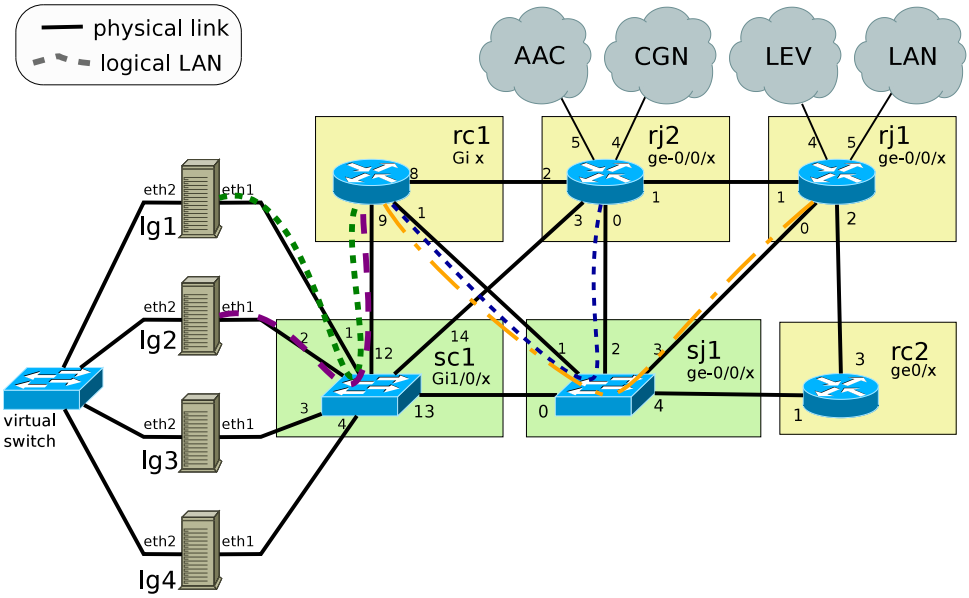

Figure 1: Topology: Mapping of VLANs to physical links.

(a) As in our previous worksheet, create a topology map (see Figure 1)[1] that shows your IPv4 and IPv6 address assignment.

Your address assignment must satisfy the following conditions:

- If two hosts/routers are interconnected with a dashed line ("logical LAN"), then the interfaces of these two routers must be able to reach each other.
- For IPv4, use /31 subnets between the routers and /29 subnets between the loadgens and the routers (see Q4).
- For IPv6, use a /64 for all subnets.
- Assign IP addresses to devices in a way such that there is no overlap in IP address space for any pairs of "logical LANs" shown in Figure 1 as each dashed arc will be configured as a separate "logical LAN" using a VLAN later on. Therefore, in other words, the IP address ranges used for different "logical LANs" must be disjoint.

Give a short explanation.

(b) Enable IP connectivity between adjacent routers and hosts by configuring IP addresses according to your topology map and check that ping/ping6 works between all device pairs for both IP versions (this will require 8 invocations of the ping/ping6 command).

Hint: It is possible to assign multiple IP addresses to a router interface. For now, assign two IP addresses to each of Gi9 and Vlan1[2] aac-rc1 (cgn-rc1 / lev-rc1).

(c) Assume that sj1 is replaced by an Ethernet hub. Which routers would see Ethernet frames that are sent from rc1 to rj2? Please be reminded that port from rc1 to sj1 is a Layer2 port. Feel free to google on how to configure ip address on Layer2 ports. Hint: Harness the power of VLANs.

(d) Do a ping from rc1 to rj2. Check with tcpdump on rj1 if it sees the ICMP Echo Request or other related packets and explain.

Note: tcpdump on Juniper routers is available in the UNIX shell.

[1] You're welcome to use our topology map as a starting point. The dia sources will be provided in the ISIS.
[2] See hints of e) for explanation why you have to use `Vlan1` instead of `Gi 1`.

(e) Configure a separate VLAN for each "logical LAN" in Figure 1, and add the used VLAN IDs to your topology map. Make sure that adjacent routers can ping each other. Your setup must satisfy the following conditions:

- Only use VLAN IDs in the range $x0 - x9$ where x is your team number.
- Whenever possible, use `access` mode on the switches.
- Altogether you will need to configure four separate VLANs.

From groupX-lg1 and groupX-lg2 use ping/ping6 to the interfaces of devices in the same VLAN to verify they are interconnected. Do the same between rj1 and rc1

Some hints for configuring the switches:

- First create the VLANs you need using `vlan <vlan-id>` on cisco or `set vlans <vlan name> vlan-id <vlan id>` on Juniper.
- Figure out whether to use trunk mode for each switch port and configure the port accordingly:
  On the Cisco switch enter the interface context and use `switchport mode <access|trunk>`.
  On the Juniper switch, edit the interface and use `set unit 0 family ethernet-switching port-mode <access|trunk>`.
- For trunk port: Set the allowed VLANs of a trunk use.
  On the Cisco switch use `switchport trunk allowed vlan add <vlan id>` in interface context.
  For Juniper, you have two ways to configure this — choose one and do not mix as this will lead to great confusion:
  Either edit the VLAN and use `set interface <interface>` or
  edit the interface and use `set unit 0 family ethernet-switching vlan members <vlan name>`.

Some hints for configuring the routers:

- Figure out where you need *subinterfaces* (Cisco) or new *units* (Juniper).
- Whenever possible, avoid configuring unnecessary subinterfaces or extra units.
- The router aac-rc1 (cgn-rc1 / lev-rc1) has two kinds of interfaces:
  `Gi 0-7` are switch interfaces and do not support subinterfaces or setting IP addresses, if you have to use them, configure them like a switch and then add ip addresses to the VLAN interface like `vlan42`.
  `Gi 8-9` are real route interfaces. VLANs are configured through subinterfaces and interfaces `vlan42` do not influence them.
- To create a subinterface on Cisco, e.g. `Gi 9.<id>`, just invoke the context and use `encapsulation dot1Q <vlan id>`.
- On the routers aac-rj1 (cgn-rj1 / lev-rj1) and aac-rj2 (cgn-rj2 / lev-rj2), each port can either be configured as router interface or as switch interface.
- To enable VLAN tagging on a Juniper router's interface in router mode, use `set int ge-x/x/x vlan-tagging` and then create a `unit` using `set int ge-x/x/x unit <id> vlan-id <vlan id>` and configure the ip address in the unit's context. Matching the unit id with the vlan id makes the config neat. Just in case you don't know, to ping from a Juniper router, you need to deactivate the firewall, which you do with `set security zones security-zone anywhere host-inbound-traffic system-services ping`

For more information on how to configure VLANs on switches on routers, please check the resources or additional material in the ISIS.

Question 3: (20 Points) *Static Routing*

Now all device interfaces within each logical LAN should be able to communicate with each other on layer two, while device interfaces of other VLANs should be unreachable. In this part of the exercise, we will establish connectivity across this set of networks to bind them together in one contiguous network, allowing for arbitrary connections between all your assigned components. This will be done by configuring static routes between these networks.

(a) On which OSI layer are we realizing the connectivity between the VLANs?

(b) Answer the following questions for every loadgen of your cloud:

1. In which network[s] (prefix/netmask) does the loadgen participate directly?
2. Specify a next hop (IP address) for each network that needs to be routed for this loadgen. Choose a next hop providing the shortest path to the respective network.

(c) Which devices (aside from the loadgens) need to be configured with additional routes in order to communicate with the loadgens of the cloud?

(d) Add the respective static routes to the loadgens and to the additional devices identified in the previous question.

(e) For each loadgen: traceroute every other configured interface (the ones *you* have given IP addresses) of your assigned routers and loadgens to verify that they are all reachable. Check which paths the packets are taking. Provide us with the traceroute output from lg1.

Question 4: (10 (2+3+5) Points) *Linux VLAN Trunking*

We will now add groupX-lg3 to the two VLANs connecting groupX-lg1 and groupX-lg2 with aac-rc1 (cgn-rc1 / lev-rc1) (see Figure 2) to demonstrate how Linux supports VLAN trunking.

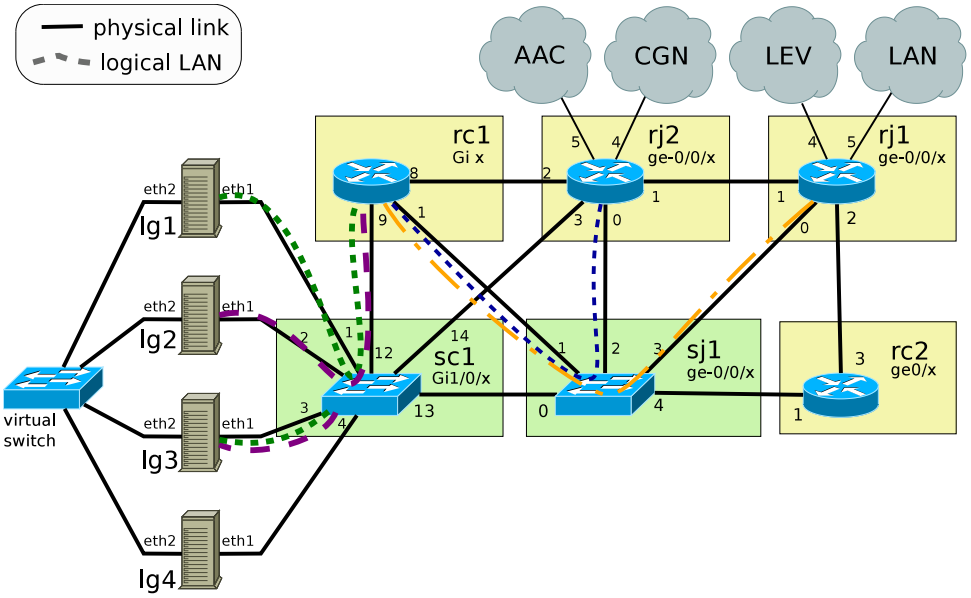

Figure 2: Topology: Mapping of VLANs to physical links.

(a) Choose two appropriate IPv4/IPv6 addresses for groupX-lg3 and add them to the two new dotted links in your topology diagram.

(b) On aac-sc1 (cgn-sc1 / lev-sc1), configure the switch port to groupX-lg3 to enable trunking and include the VLANs already going to groupX-lg1 and groupX-lg2

(c) Now that you've configured switchport vlan trunking on sc1, you must also configure the network interfaces on groupX-lg3 to support VLAN trunking. The end result will be that groupX-lg3 will have two subinterfaces. One subinterface will have an IP in the same subnet as that of groupX-lg1. The other subinterface will have an IP in the same subnet as that of groupX-lg2.

- The Debian system on the loadgens will require that you install the vlan package and load the 8021q kernel module. This can be achieved via the commands: `apt install vlan`
- The following example illustrates how to set up a subinterface such that all outgoing Ethernet frames are tagged with a VLAN ID[3]:

```
root@loadgenxxx:~# ip link set up dev ethX
root@loadgenxxx:~# vconfig add ethX <vlan-id>
root@loadgenxxx:~# ifconfig ethX.<vlan-id> <ip-address> netmask <netmask>
```

Finally, assign two new IPv4 addresses from the same new subnet to each of the new subinterfaces on lg1 and lg2 respectively. Show a traceroute from groupX-lg3 toward groupX-lg1 and groupX-lg2.

[3]subinterfaces can be removed with vconfig rem, see man vconfig

Question 5: (10 (2+3+5) Points) *Spanning Tree in Theory*

The *Spanning Tree Protocol (STP)* is one of the essential protocols needed to maintain switched ethernet networks. As our topology only has two switches, using STP makes not much sense in our topology and we will only take a brief look at it.

(a) Imagine we have configured the switches without STP, LACP and VLANs. We add a link between aac-sc1 (cgn-sc1 / lev-sc1) Gi1/0/14 and aac-sj1 (cgn-sj1 / lev-sj1) ge-0/0/7 and enable it (hypothetical scenario in which those interfaces would exist and a link were added). What would happen?

(b) Describe briefly how STP mitigates this problem.

(c) Assume we added rSTP to the config and now configure VLAN 23 as access VLAN on the link aac-sc1 (cgn-sc1 / lev-sc1) Gi1/0/14 and aac-sj1 (cgn-sj1 / lev-sj1) ge-0/0/7 and VLAN 42 as access VLAN on aac-sc1 (cgn-sc1 / lev-sc1) Gi1/0/13 and aac-sj1 (cgn-sj1 / lev-sj1) ge-0/0/0. What would happen? Explain how PVSTP+ and MSTP can solve that problem.

Submission details (more in ISIS):
Please submit an archive (.tar.gz or .zip) containing *a directory*, which contains all files you want to submit. Please have *your group number* in the file name and the directory name.
A report (one single PDF file, named *worksheet(num)-group(num).pdf*) containing the following elements is mandatory:

- Your group number on the first page
- Topology map with relevant routers, switches, *loadgens*, and interfaces, IPs and subnet masks (CIDR).
- For each question, the written answers with the **relevant** portions of output from all commands such as ping, tcpdump, etc in a text format. **No** screenshots of terminal windows are accepted. For ping 3-4 lines of ping requests are usually sufficient.
- For each question all commands needed to configure the *loadgens*.
- For each question all **changed parts** in the configuration of routers and switches (differences to the default config).
- **Never** include the full verbatim switch or router configuration in the pdf report.
- For all questions, state your assumptions, say what you did, describe what you observed, explain your conclusions.

Additionally, please include your config files in the archive.
For each question, please provide the full switch and router configuration in a separate text file named after the device and question, e.g.: *q01-config-sc1.txt*. This makes it easier for us to reproduce your configuration and understand what you did.
We can only grade what we find in your submission and what we understand. Please state your assumptions and observations as clearly as possible.
Due Date: Thursday, May 10, 23:55 PM[4]

[4] We will not accept any solutions submitted after this allowed time.