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 6: Tunneling & VPN

Network tunnels play a crucial role in logically isolating Internet traffic. Tunnel-based traffic isolation enables many important mechanisms such as customer access accounting, secure private networks, generic protocol encapsulation, and incremental deployment of IPv6. In this worksheet, we will look at a few different types of tunnels to get a better appreciation for how they may be used.

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		fd00:470:525b: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: (15 Points) *Secure Virtual Private Networking (Theory)*

Virtual Private Networks (VPNs) play an essential role in the largely insecure Internet, allowing authenticated, confidential communication between trusted parties. Many different types of VPNs exist, implemented at different layers in the protocol stack, intended for use at different points within the network. In this section, we will consider Layer 2 and Layer 3 VPNs.
Please answer each of the following questions in 2-3 sentences.

(a) What are the advantages of VPN solutions (like IPSec and OpenVPN) compared to just using SSL/TLS directly below the application layer?

(b) What are the two modes of operation supported by IPSec and what purpose does each serve? How many additional bytes of packet overhead are introduced by the two operational modes, assuming IP as the encapsulated protocol?

(c) Which IPSec mode of operation would you choose to setup a secure tunnel from end-host to end-host? Give a brief explanation.

(d) Can IPSec be run without encryption, but with authentication support? Which protocols of IPSec are responsible for which task in that respect?

(e) Describe the conceptional differences between SSL VPN solutions like OpenVPN and IPSec. At which layer do they operate? When used in tunnelling mode how do you configure which traffic should go through the tunnel in the respective implementations?

(f) Describe the differences between TUN and TAP mode of operation in OpenVPN. Which mode would one use to bridge two LANs across a layer 3 network?

(g) As IP is inherently a connectionless protocol, what mechanism of the IPSec protocol suite is used to ensure data origin authenticity and to protect against replay attacks? What mechanism provides confidentiality?

(h) Does the term "Virtual Private Network" necessarily imply security through encryption and authentication of the traffic? Hint: Look at tunneling technologies like PPPoE and MPLS.

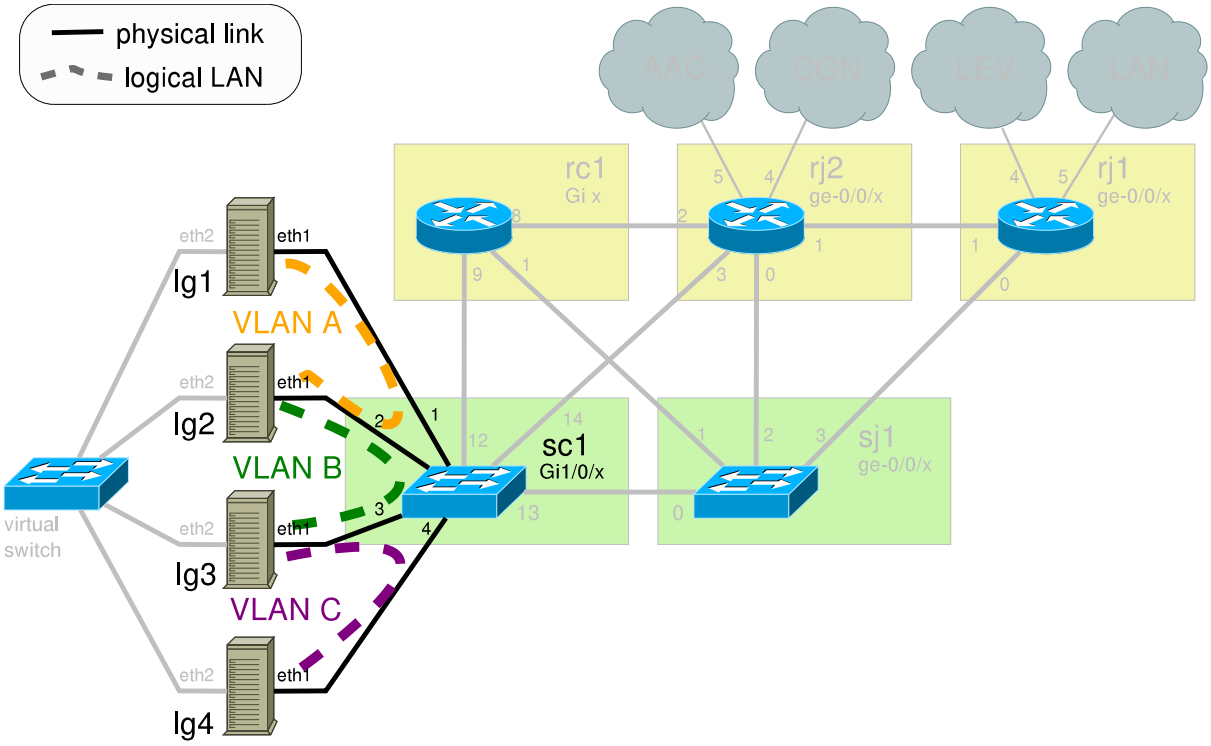

Figure 1: Topology for OpenVPN question

Question 2: (20 Points) *Deploying OpenVPN*

In this section, you will create a VPN tunnel to interconnect two networks in two different physical locations of two cooperating business partners. Take a look at Figure 1. In this topology, imagine that one business partner controls groupX-lg1 and groupX-lg2 and the other one controls groupX-lg3 and groupX-lg4. Your task will be to interconnect both networks with a TUN tunnel via the link that connects groupX-lg2 and groupX-lg3 (which will represent the public Internet).

Please remember to delete routes/configurations in your loadgens (power-cycle them). In addition, make sure that the current configuration in aac-sc1 (cgn-sc1 / lev-sc1) does not contain lines from previous exercises. In the following, remember to substitute `X` with your group number.

(a) Configure the loadgens and the aac-sc1 (cgn-sc1 / lev-sc1) switch using the specified address and appropriate VLAN ranges (e.g., VLAN A: 101, VLAN B: 103, VLAN C: 102). Note that you will have to configure the interfaces in groupX-lg2 and groupX-lg3 to operate with VLAN tags. Configure two different subnets and VLANs, one for groupX-lg1 and groupX-lg2 (`10.X.1.0/24`) and another for groupX-lg3 and groupX-lg4 (`10.X.2.0/24`).

(b) Configure the switch and interfaces of groupX-lg2 and groupX-lg3 so that the latter two can communicate. Use the address range `10.X.100.0/24`.

(c) Install the OpenVPN package on groupX-lg2 and groupX-lg3. You will now have to configure groupX-lg2 as the VPN server end-point and groupX-lg3 as the client end-point with a static key. You can follow the instructions in the OpenVPN static key mini-HOWTO [1]. Create the two config files and include them in your answer. Remember to configure end-points within the LANs of both partners. To create the tunnel run:

```
openvpn --config <configfile>
```

(d) Perform on groupX-lg2 a few *ping* measurements to the interfaces of groupX-lg3 so that you can observe both ICMP and OpenVPN packets simultaneously. Provide the tcpdump output on the corresponding interface(s) of groupX-lg3 and explain in 2-3 sentences what you see.

[1] http://openvpn.net/index.php/open-source/documentation/miscellaneous/78-static-key-mini-howto.html

(e) Now that you successfully established a tunnel between groupX-lg2 and groupX-lg3, the business partners want that the other loadgens in their networks, i.e., groupX-lg1 and groupX-lg4 can also make use of this tunnel. First enable packet forwarding. Try pinging groupX-lg4 from groupX-lg1. Does it work? As you probably anticipated, you have first to configure routes on these loadgens. Make sure that you assign the right gateways to them. Show us that both groupX-lg1 and groupX-lg4 communicate via the tunnel with a few *ping* measurements and *traceroutes*. Include a few relevant lines from dumps in groupX-lg1 and groupX-lg3.

(f) Use `tcpdump` to demonstrate that no un-encrypted traffic is passing the vlan between groupX-lg2 and groupX-lg3 and provide us with a few lines of output or a screenshot.

Question 3: (25 Points) *Deploying IPSec*

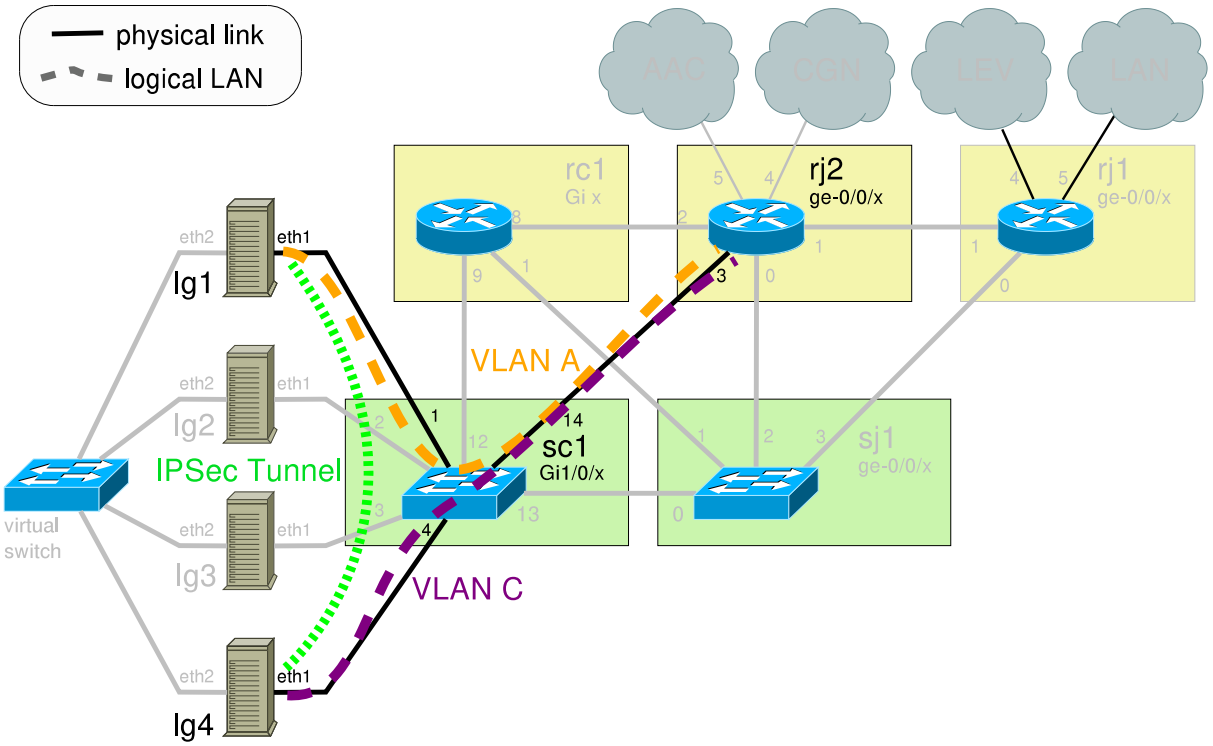

Figure 2: Topology for IPSec question

In this assignment you will connect two end hosts via IPSec in transport mode. All communication between both hosts will be encrypted as well as authenticated. Remember to quit openvpn.

(a) Configure two VLANs on aac-sc1 (cgn-sc1 / lev-sc1) using access or trunk mode where necessary. VLAN A connects groupX-lg1 with aac-rj2 (cgn-rj2 / lev-rj2) and VLAN B connects groupX-lg4 with aac-rj2 (cgn-rj2 / lev-rj2). Consult Figure 2 for the VLAN setup. **Hint:** Make sure that groupX-lg1 and groupX-lg4 can communicate (You need to setup routing on aac-rj2 (cgn-rj2 / lev-rj2). keyword: l3-interface), and also update the routes.

(b) Install the strongswan package on groupX-lg1 and groupX-lg4 by
`apt-get install strongswan`.
Visit http://wiki.strongswan.org/projects/strongswan and familiarize yourself with the strongswan IPSec implementation.
On http://strongswan.org/uml/testresults4/ikev2/host2host-transport/index.html you find an example configuration for the scenario you will be working on. Have a look at the different configuration files and give a brief description of what the following configuration files do:

- `/etc/ipsec.conf`
- `/etc/ipsec.secrets`
- `/etc/strongswan.conf`

Additionally explain on a general level what information you can gather from the following commands:

- `ipsec statusall`
- `ipsec listall`
- `ip -s xfrm policy`
- `(ipsec up <conection-name>)`
- `(service ipsec restart)`

Hint: Besides looking into the log files in `/var/log/*`, the commands listed above help you a great deal while debugging IPSec connections.

(c) Have a look at the topology above and configure an IPSec Security Association between groupX-lg1 and groupX-lg4. Use the transport mode to connect both end hosts via IPSec.

It is easier to work with PSKs (pre-shared keys), but you are free to use X.509 certificate based authentication. The example given on the strongswan page uses certificate based authentication. In order to use certificates, you need to generate the appropriate OpenSSL certificates and put them into the according directories under `/etc/ipsec.d/` on the communicating hosts. For an overview over PSK authentication see: https://strongswan.org/uml/testresults4/ikev2/net2net-psk/index.html.

If you want to use PSK authentication add
`authby=secret`
to the section which corresponds to your connection in
`/etc/ipsec.conf`.

Again, have a look at the example under http://strongswan.org/uml/testresults4/ikev2/net2net-psk/index.html to find out how your `/etc/ipsec.secrets` has to look like to utilize PSK authentication.

(d) Ping groupX-lg4 from groupX-lg1 and capture the connection between groupX-lg1 and groupX-lg4 on aac-rj2 (cgn-rj2 / lev-rj2). What can be observed, and what can *not* be observed?

(e) Do a `traceroute` from groupX-lg4 to groupX-lg1 and compare its output to the `traceroute` you did in the previous question. How to they differ?

Question 4: (10 Points) *6to4 Tunneling (Theory)*

This exercise gives you an idea how tunnelling technologies can be used to try to simplify adaption of new protocols. In this case you will tunnel IPv6 traffic from the loadgens in your IPv6-enabled "home-network" through the network of your IPv4-only ISP to the IPv6 Internet.

In order to do so, you will configure the router aac-rc1 (cgn-rc1 / lev-rc1) within the network as a 6to4 relay, which in the real world would be provided by a network operator. You will then set up your "home router" groupX-lg4 to provide a tunnel to the IPv6 gateway, and finally allow the "client" groupX-lg3 in the home network access, thus enabling it to use IPv6.

We'll refer to the groupX-lg4 interface connecting to aac-rj1 (cgn-rj1 / lev-rj1) as 'exterior' interface, and the one connecting to groupX-lg3 via the virtual switch as 'interior' interface.

(a) Search the web and briefly explain each of the following concepts in 2 or 3 sentences:

- Tunneling IPv6 over IPv4
- Automatic Tunneling, 6to4
- Configured Tunneling, tunnel brokers, 6in4

(b) Generally, it is possible to manually configure static tunnels. What would be the disadvantage in common uplink scenarios, where a home router is connected via DSL and assigned a dynamic IP address?

(c) Explain how 6to4 IPv6 addresses are derived from IPv4 addresses (see RFC 3056 Section 2).

(d) Read RFC 6343. What is the default anycast 6to4 address that is reserved for 6to4 relays, and what are the problems with it?

Question 5: (25 Points) *6to4 Tunneling (Practice)*

In this part, we'll prepare the networks for the subsequent IPv6-over-IPv4 tunnel experiment. We'll create a set of 5 logical LANs, two of which will be running IPv4, two of which will be running IPv6, and one of which will (in the end) run both. In this setup, aac-rc1 (cgn-rc1 / lev-rc1) and aac-rj1 (cgn-rj1 / lev-rj1) will represent the IPv4 infrastructure and an IPv6 relay run by your local ISP.

groupX-lg4 will represent your home router, connected to the ISP, while groupX-lg3 will represent your local client. groupX-lg1 represents an IPv6 only machine you'd like to connect to. The Home Network and IPv6 Internet are IPv6 enabled, the ISP Network as well as the IPv4 Network are IPv4 only.
Remember to write '1' into /proc/sys/net/ipv{4/6}/ip_forward on the appropriate loadgen to enable packet forwarding (routing) on the device; (a value of 0 disables the routing). The virtual switch connecting the interfaces eth2 of the loadgens needs no configuration and is always connected to all your loadgens.

Remember: Remove all old configurations that can potential break things for the new task.

(a) Setup the VLANs, as indicated in Figure 3. Draw a topology map, in which you will fill in the IPv4-, and IPv6-addresses as you assign them to the devices, along with the used VLAN IDs. This topology map is part of the documents to be submitted.

Hint: Be careful whether you set a port to access or trunk mode. (The distinction is **not** just "one or multiple vlans").

Hint: To get a better overview, it can be helpful to draw an additional diagram with just the logical LANs as a line topology. This can help you understand the path from the home network via the IPv4 network to the relay and IPv6 network.

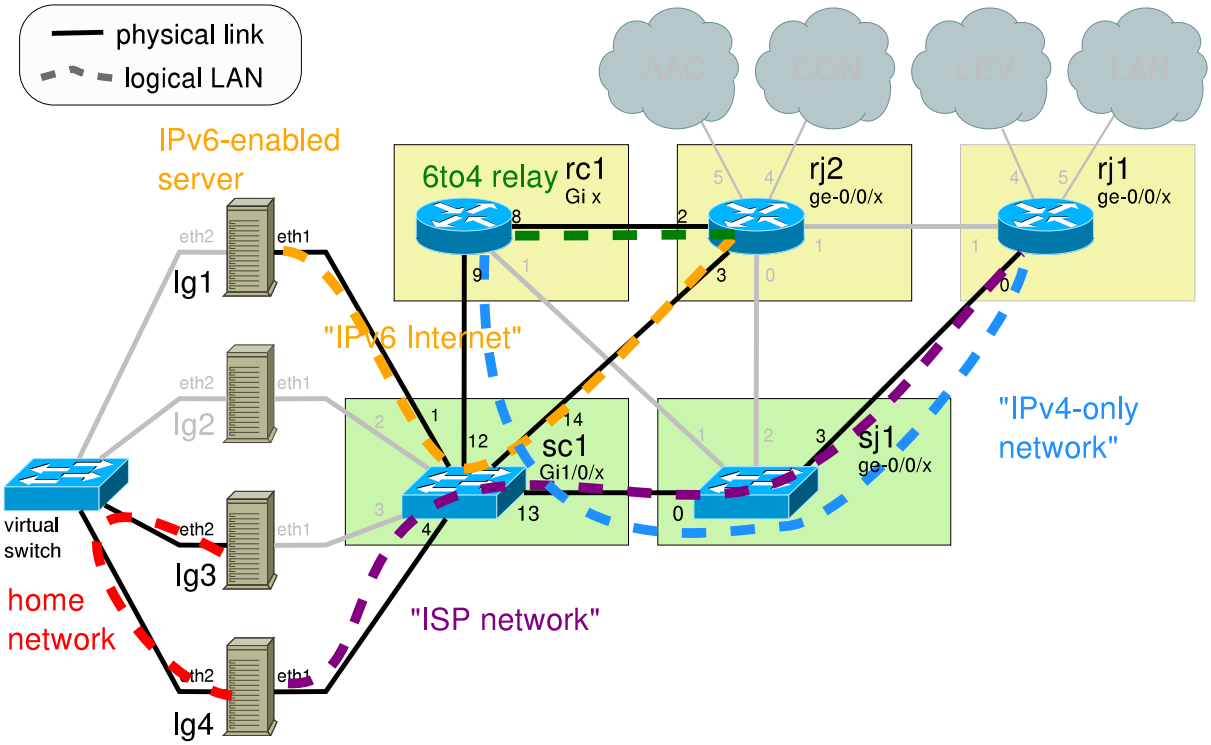

Figure 3: Topology for 6to4 question

(b) Log on to groupX-lg3 and ping the **link local** address of groupX-lg4. Use the appropriate home-network interface. You can find that address using the `ip addr` command on groupX-lg4. Show us the output. (One ping only, please![2])

Hint: Just providing ping with the IP address is not enough here - you also need the interface name.

(c) Configure an IPv4 network between groupX-lg4 and aac-rc1 (cgn-rc1 / lev-rc1) by configuring IP addresses, gateways, and routing where needed. Traceroute aac-rc1 (cgn-rc1 / lev-rc1) from groupX-lg4 to verify that it works and show it to us.

(d) Set up IPv6 connectivity between aac-rc1 (cgn-rc1 / lev-rc1) and groupX-lg1. Use traceroute to verify it works and show us its output (from groupX-lg1 to aac-rc1 (cgn-rc1 / lev-rc1)). As a reminder, the commands to configure static routes begin as follows: `ipv6 route` (Cisco), `set routing-options rib inet6.0` (Juniper).

[2] http://www.youtube.com/watch?v=70398Ubx-Gs

(e) Before we start with the configuration of the *6to4 gateway*, think about the IP address mapping you learned about in 4 (c). What are appropriate 6to4 addresses for the tunnel endpoint ('exterior' interface, TUNNEL-6to4) and LAN interface ('interior' interface, LAN-6to4) of the groupX-lg4? To find out you may use the following shell script, make it executable (chmod) and finally execute it, using the WAN interface's IP address as parameter:

```
#!/bin/bash

WANIP=$1
echo "IPv4 address: $WANIP"
V6PREFIX=$(printf "2002:%02x%02x:%02x%02x" $(echo $WANIP | tr . " "))
TUNNEL6to4=$V6PREFIX:0::1/16
LAN6to4=$V6PREFIX:1::1/64
echo "Tunnel6to4: $TUNNEL6to4, LAN6to4: $LAN6to4"
```

Try to understand the script from above (check manpages if necessary). Explain in a few sentences what the script does and add the calculated IPv6 addresses to your topology map. For more information we refer to RFC 3056 (Section 2) or other sources in the web.

(f) Now configure aac-rc1 (cgn-rc1 / lev-rc1) as a *6to4* relay. Assign both appropriate IPv4 and IPv6 addresses and netmask (/32, /128) to a Loopback device, based on your answer to question 4 (d)[3].

The loopback interface will serve as tunnel endpoint. The tunnel will decapsulate packets received on this address, and forward them to the correct host in the IPv6 network. In the reverse direction, it will accept IPv6 packets with address `2002::/16`, encapsulate them, and send them to the appropriate IPv4 address.

In order to receive packets on the loopback device, it needs to be associated to an appropriate tunnel by the following commands:

```
interface Tunnel0
    no ip address
    no ip redirects
    ipv6 unnumbered Loopback <interface number>
    tunnel source Loopback <interface number>
    tunnel mode ipv6ip 6to4
    tunnel path-mtu-discovery
!
ipv6 route 2002::/16 Tunnel0
```

The last above command adds an appropriate route for all IPv6to4 packets to the tunnel device. Since IPv6 routing is by default disabled on Cisco routers, you probably will have to enable ipv6 routing with the command: `ipv6 unicast-routing`

Configure routing on rj2 and lg1 so they can reach the tunnel endpoint's IPv6 address and so that they know the route to the mapped IPv4 addresses. Configure routing on rj1 and lg4 to they can reach the tunnel endpoint's IPv4 address.

(g) Now configure the 6to4 tunnel, IP addresses and routing on your home router groupX-lg4, i.e. the 6to4 gateway. To do this manually, you need the following commands:

```
ip tunnel add tun6to4 mode sit ttl 255 remote any local <IPv4 address of 'exterior' interface>
ip link set tun6to4 mtu 1280
ip link set tun6to4 up
ip addr add <TUNNEL6to4 address/netmask> dev tun6to4
ip addr add <LAN6to4 address/netmask> dev <'interior' interface>
ip -6 route add ::/96 dev tun6to4 metric 256
ip -6 route add ::/0 via ::<IPv4 relay address>
```

Explain what each *individual* command does. Check with ip tunnel show tun6to4 and ip a whether the tunnel has been created and if the IPv6 addresses have been assigned.

(h) Make sure that the tunnel endpoint is reachable from both groupX-lg4 and groupX-lg1, and then show that IPv6 packets get through the tunnel between groupX-lg4 and groupX-lg1. Log on to groupX-lg4 and ping first aac-rc1 (cgn-rc1 / lev-rc1), then aac-rj1 (cgn-rj1 / lev-rj1), and finally groupX-lg1. Provide the output of one ping for each of these, in order to show us that the tunnel and routing is working!

(i) Finally we want to have IPv6 connectivity from groupX-lg3 as well. Remember: groupX-lg4 represents our 'home router' and groupX-lg3 is supposed to be a client. Assign an address from

[3] You may also use different addresses, but make sure they work. In particular, the addresses you assign here need to be different from the addresses you assigned to the IPv4 and IPv6 subnets you configured before.

your `LAN6to4` range to the home-network interface (eth2) of groupX-lg3 and configure groupX-lg4 appropriately. Show us, that you can reach groupX-lg1 via IPv6 from groupX-lg3 using ping. Note: normally you would assign the address of groupX-lg3 using SLAAC / DHCPv6 but for the sake of simplicity we assign them manually.

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, June 14th, 23:55