Exercise Series - DNS & WWW

Please consider the footnotes in the exercises!

For the following exercises, the "router" VM must be configured and running according to the "Exercise Series - Routing & DHCP".

Exercise 1 DNS Server Connectivity

1. Use the VM "server01" as with Debian as DNS server.
   Start the VM and log in.
2. The DNS server must now be configured to the specified static IP address.
   See "S22.L2 - Lab Networks and Names" → "Routing and DHCP information".
   Use the "webmin" administration tool for the configuration.
   "webmin" is also accessible on this VM using the address https://localhost:10000[1].
   Log in with the user "root".
3. Under "Networking → Network Configuration → Network Interfaces", reconfigure the network interface "ens192" according to the guidelines and save the settings with (`Save and Apply`).
4. Now configure the "Default Route" of the DNS server to the IP address of your router on the "servers" network. Set the correct "Gateway" (interface "ens192") for your server under "Networking → Network Configuration → Routing and Gateways" in the tab "Boot time configuration".
   Save the changes you have made with (`Save`).
5. In order for your server to resolve hosts by name, you must next configure its DNS resolvers.
   To do this, open "Networking → Network Configuration → Hostname and DNS Client".
   Enter the host name "ns".
   Leave the entry for the "Resolution order" as it is[2].
   Now configure the "DNS servers" with the IP addresses according to the guidelines for your group. Since your DNS server is not yet configured, you should enter the address of the laboratory DNS server `147.87.80.2` ("paris.bfh.ch") as the first address and `127.0.0.1` ("localhost", local DNS-Server) as the second address.
   You can/must change this order as soon as your DNS server is working.
   At "Search domains" enter your forward domain/zone according to the guidelines.
   Save the changes you have made with (`Save`).
6. You should now be back on the "Networking → Network Configuration" page.
   Apply the configurations you have made by pressing (`Apply Configuration`).
   Your server should now be correctly configured and working.
   Test the internet connectivity of the "server01".
   Does the "servers" network work as expected?
   Does the connectivity between "servers" network and "clients" network[3] work?
   Does the "server01" VM work after a reboot?
   Restart in the operating system ("ON/OFF" icon at the top right) or in "webmin" under "System → Bootup and Shutdown" using the button (`Reboot System`).

[1] Ignore the security warning and accept the insecure/self-signed certificate.
[2] This sets the order of name resolution: local host file "/etc/hosts" and then DNS.
[3] Keep in mind that Windows computers do not respond to "ICMP Echo Requests" by default.
Instructions for modifying the "Windows Defender Firewall" can be found here:
https://www.howtogeek.com/howto/windows-vista/allow-pings-icmp-echo-request-through-your-windows-vista-firewall/
https://tunecomp.net/allow-incoming-ping-echo-request-without-disabling-windows-10-firewall/

Exercise 2 DNS Server - Base Configuration

1. The reference implementation ISC "BIND" is used as DNS server software.
   (see also https://www.isc.org/bind/).
   The preconfiguration of this software on the Debian system is sufficient for our purposes and can be used directly. However, it is limited so that the name server only listens for and responds to requests on the local address `127.0.0.1` ("localhost").
   This is sufficient for the use by the local server computer.
   In "webmin", start the DNS server (if it is not already running).
   Under "Servers → BIND DNS Server" click on the "Play" icon ("Start bind") in the upper right corner. Now change the order of the "DNS Servers" under
   "Networking → Network Configuration → Hostname and DNS Client".
   Enter `127.0.0.1` ("localhost") as the first address and `147.87.80.2` ("paris.bfh.ch") as the second address. Apply the change: (`Save`) and (`Apply Configuration`).
   Test in a terminal window or in "webmin" ("Tools → Command Shell") with the utility "dig" whether the DNS server on "localhost" can be queried.
   Does the command "`dig www.bfh.ch`" return the address of the BFH web server without delay? Does the answer come from the local server `127.0.0.1`?

2. If this works, configure the DNS server so that it is started automatically when the system is booted.
   Under "System → Bootup and Shutdown" in the "Service name" column, check the box at the "named" .
   Click at the bottom (`Start On Boot`).
   Go back to the "Bootup and Shutdown" page and verify that "named" service is set to "Yes" in the "Start at boot?" column.

3. The next step is to reconfigure the DHCP server on the "router" system so that the local DNS server is set first on the DHCP clients.
   Log in to the"router"VM and start "webmin".
   Alternatively, you can access "webmin" on the "router" VM directly from the "server01/ns" VM:
   Under "Webmin → Webmin Servers Index" click on (`Broadcast for servers`), the "webmin" server on the "router" VM should be found[4].
   Select "Return to servers", click on the found "webmin" server and log in.
   Select "Servers → DHCP Server" (`Edit Client Options`).
   Change the order of the DNS servers so that your DNS server (IP address according to guidelines) is entered first and only then the laboratory DNS server `147.87.80.2` ("paris.bfh.ch").
   Click (`Save`) and (`Apply Changes`).

4. Now start the Windows 10 Client VM "client02".
   Open a command line: Click the "Start" button, type "`cmd`" in the search field, press the `<RETURN>` key, a command line window should open.
   In the command window, use the command "`ipconfig /all`" to check the interface configuration of the Ethernet adapter and especially the DNS servers.
   The first IP address listed should be the one of your DNS server[5].
   Now enter the command "`nslookup www.bfh.ch`".
   What do you find? Can the name be resolved?

[4] If this does not work right away, click on (`Broadcast for servers`) again.
[5] You may have to use "`ipconfig /renew`" to get the new configuration if "client02" was already started before the DHCP server was changed.

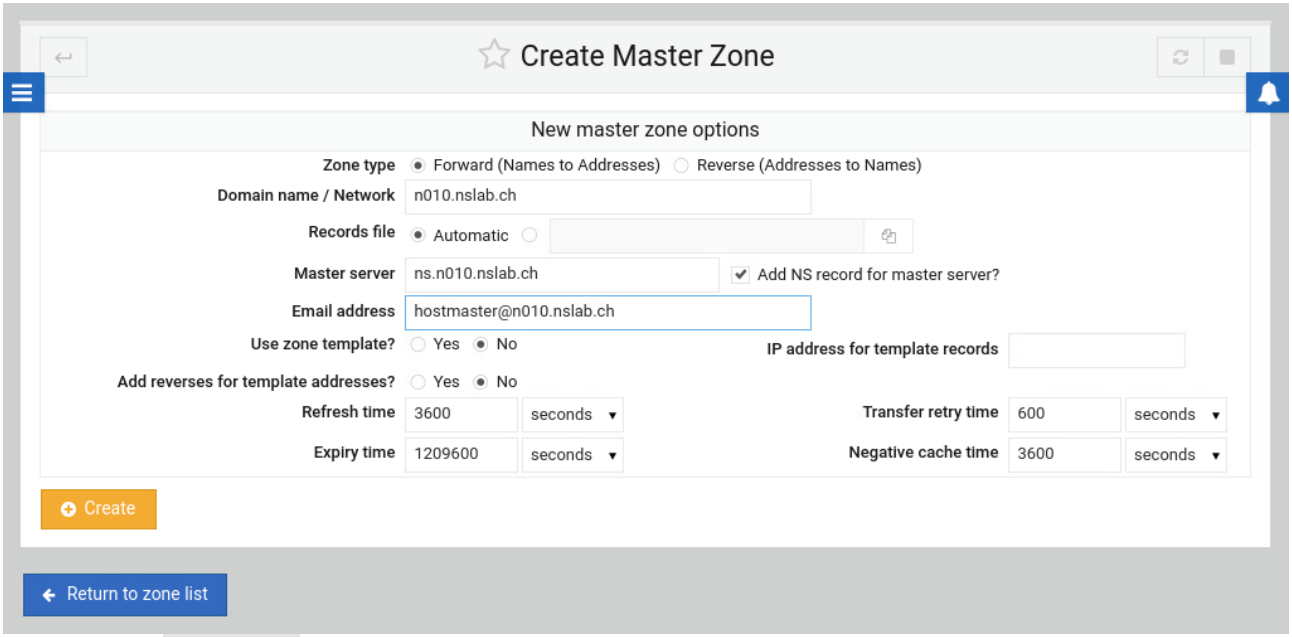
5. Apparently, the DNS server does not answer queries from your networks.
   The DNS server must now be changed so that it also listens to and answers queries on interfaces other than the "localhost" interface.
   Go to the "webmin" interface of the DNS server and there to "Servers → BIND DNS Server".
   Under "Addresses and Topology" → "Ports and addresses to listen on" set the top entry to "Default" instead of "Listed below…".
   (Save) and klick the "Reload" icon on the top right ("Apply configuration").
   The server should now listen to requests from the outside on the interface "ens192".
   What happens now if you enter the command "`nslookup www.bfh.ch`" on the "client02"?
   Do you get the expected response?

6. Obviously, the (recursive) request of the client is (still) rejected by the server.
   The next step is to configure ACLs (Access Control Lists) that allow the networks in your setup to access the DNS server.
   Go to the "webmin" interface of the DNS server again and then to "Servers → BIND DNS Server".
   Under "Access Control Lists" create the entry with the "ACL Name": "servers" and the "Matching addresses" for your server network (e.g. `147.87.82.32/28`) and click (Save).
   Then create the entry with the "ACL Name": "clients" for your client network.
   You can then combine these two entries in a new entry with the "ACL Name": "mynets" and the "Matching ACLs" "servers" and "clients" (one entry per line). Click on (Save).

7. Now set the entry under "Addresses and Topology" → "Allow recursive queries from" to "Listed .." and enter "mynets" in the text field.
   (Save) and click the "Reload" icon in the upper right corner ("Apply configuration").
   This should allow the computers on your networks to access the DNS server.
   Verify this on the "client02" using "nslookup", the request should now return the address of the BFH web server.

Exercise 3 DNS Server - Zones

1. Now try to configure the DNS zones for your lab setup.
   On the "webmin" interface of the DNS server, go to "Servers → BIND DNS Server".
   Now create a new forward zone with "Create master zone" according to the guidelines with entries analogous to the following example (for "n010.nslab.ch"):



   Click on (`Create`) to create the zone.
   Now add the "Address" records with the correct addresses for your DNS server and the router interfaces to the zone (e.g. "ns" with the address `147.87.82.34`),
   "Time-To-Live": Default, "Update reverse?": No → (`Create`)
   With "Return to record types" you go back to "Edit Master Zone".
   Under "Edit Zone Records File" you can display the zone file created using the Web-GUI in the default zone format. Do not change anything and go back with "Return to record types".

2. Now the zone options must be adjusted with "Edit Zone Options".
   Under "Allow queries from.." enter "any" to allow all DNS servers on the Internet to query the data of your zone (using iterative queries).
   Save the configuration with (`Save`) and apply it with "Apply zone" icon (top right) and "Apply configuration" icon (top right).

3. Now try to query the address of your name server using "dig" or "nslookup".
   E.g. "`dig ns.n010.nslab.ch`" or "`nslookup ns.n010.nslab.ch`".
   Does this work?
   Then test the function of your zone from the internet with a DNS check tool e.g. with https://www.nslookup.io/dns-checker/.
   Enter your zone name (e.g. `n010.nslab.ch`) or the name of the name server (e.g. `ns.n010.nslab.ch`) under "Domain name" and start the test.
   Do you get any error messages or warnings?
   Show the results of this test to the lecturer.

4. To find out the hostnames of your servers using their IP addresses you need entries (PTR records) in the reverse zone of your network. Since the subnets used for the lab are (/28), but the "smallest" IPv4 DNS reverse zone can only be made elegant by a C-class network (/24)[6], you must enter these PTR record entries using Dynamic DNS DDNS update into the IPv4 reverse zone specified for your lab setup.
   This could be done using the utility "nsupdate" and the corresponding security key "DHCP_UPDATER"[7].
   To make this easier for you, the lab-specific shell script "nsupdate-nslab" is available (on the name server VM).
   Use the "nsupdate-nslab" script to add the PTR records of your servers to the corresponding reverse zone (at least the one of the name server must be entered).
   E.g.: "`nsupdate-nslab add ns.n010.nslab.ch 147.87.82.34`".
5. Then try to query the names for an address (PTR records) using "dig" or "nslookup".
   (e.g. "`dig -x 147.87.82.34`" or "`nslookup 147.87.82.34`").
   Does this work?

Exercise 4 DNS Queries - Captures

1. Now capture some DNS queries and lookups using "wireshark".
2. Try to capture the "priming" (querying of the root name servers) immediately after the DNS server is started.
3. Try to capture a clients recursive query to the local DNS server and the resulting queries to name servers on the Internet (iterative queries) immediately after the local DNS server starts up.
4. Capture more DNS queries and try to make visible the optimizations by the caching of the local DNS server.

[6]Delegation via CNAMEs according to BCP20 / RFC2317 "Classless IN-ADDR.ARPA delegation" would be possible, but is beyond the scope of this lab exercise.

[7]
```
key DHCP_UPDATER {
          algorithm hmac-md5;
          secret H6ZUGGZLq1pj0r9tdjZsgCUqEkaAZUz3o0XjbPVsRermdUO436KZUkX8XevE;
};
```

Exercise 5 Web Server

1. This exercise is about configuring a web server which is then reachable via the name "www". Use the server VM "server02" and configure the system in the same way as "server01" in Exercise 1. Use the next free address from your "servers" network, keep the hostname "server02". Now check the internet connectivity of "server02".
2. Go to the "webmin" interface of "server02" and start the preconfigured web server under "Servers → Apache Webserver" using "Start Apache" ("Play" icon on the top right).
   You should now be able to access the web server using http://localhost, a test page should be displayed.
3. Now enter the name "www" for your web server in the DNS.
   Make an address entry for "server02" in your DNS forward zone.
   Then add a "Name Alias" with the "Name" "www" to the "Real Name" "server02" and apply the changes with "Apply Zone".
   You should now be able to access your web server (from anywhere on the BFH network `147.87.0.0/16`) using the "Fully Qualified Domain Name" FQDN (e.g. http://www.n010.nslab.ch). Test it out! Capture an HTTP access using "wireshark".
4. In a next step, the communication to your web server shall be secured by "Transport Layer Security TLS". Certificates from the Let's Encrypt CA[8] are to be used to check the authenticity of the web server.
   In the "webmin" interface of the "server02", go to "Servers → Apache Web Server" to the "Existing virtual hosts" tab.
   Click on the globe of the server listening on port 80
   (entry with "**Address** Any" und "**Port** 80").
   For "Server Name" (at the bottom of the page), enter the FQDN of your web server.
   (e.g. "www.n010.nslab.ch").
   You can leave the rest of the entries at the defaults.
   Click on "Save" and then apply the changes ("Apply changes" icon at the top right).
   Check that your web server is still accessible (e.g. using http://www.n010.nslab.ch).
5. Now create and fetch a certificate from the Let's Encrypt CA using the pre-installed tool "certbot"[9]: e.g. "`sudo certbot --apache -d www.n010.nslab.ch`".
   Enter "certmaster@nslab.ch"[10] as the mail address,
   accept the "Terms of Service" by entering "Y",
   do not share the mail address with the Electronic Frontier Foundation EFF[11] ("N").
   Now access your web server again using "http" (e.g. using http://www.n010.nslab.ch).
   The access should now be redirected to "https" and your LE certificate should be valid and correct and accepted by the browser without any security message.
6. Check the TLS/SSL configuration of your web server at https://www.ssllabs.com/ssltest/ and document the results.
7. In a further step you can now try to create your own content on the web server (e.g. "/var/www/html/index.html").

Congratulation! You made it!

[8] Let's Encrypt Certificate Authority: https://letsencrypt.org/
[9] The installation of "certbot" was done according to https://certbot.eff.org/instructions?ws=apache&os=debiantesting.
[10] Mails to this address go to the person responsible for the lab. For own installations you should enter your own mail address!
[11] https://www.eff.org/