



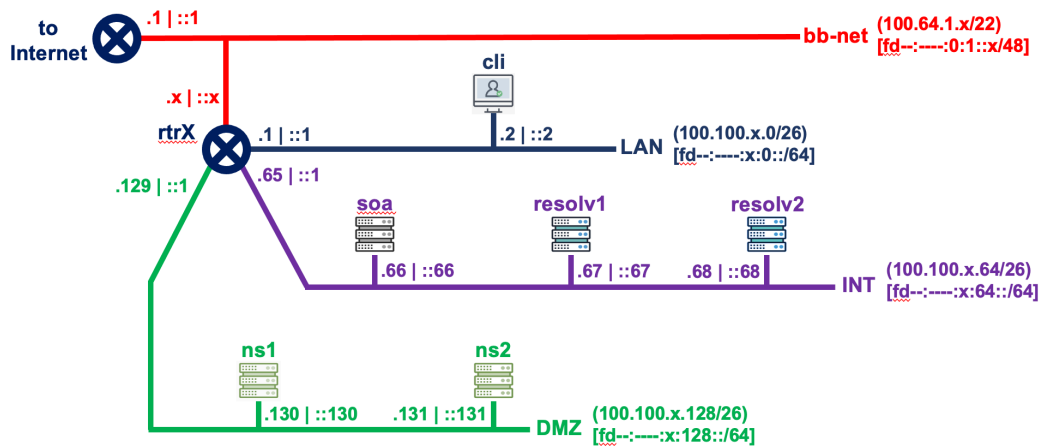
ICANN

**DNS/DNSSEC Workshop in conjunction with
Lanka Network Operators Group (LKNOG) Conference
12-16 August 2024**

Lab Exercises

**Champika Wijayatunga
Technical Engagement Sr. Manager - Asia Pacific
<champika.wijayatunga@icann.org>**

grpX network topology



Lab address space: (100.64.0.0/10)
[fd--:--:0:32]

Click on selected device to
access its terminal

Reverse DNS

During this practice we are only going to access the following equipment:

- **grpX-cli** : client
- **grpX-soa** : hidden authoritative servers (primary)
- **grpX-ns1** & **grpX-ns2** : secondary authoritative servers

NOTE: In all this lab, be careful to always replace **X** by your Group number in IP addresses, server name and any other place where required. Same for `<lab_domain>` to be replaced by the domain name registered for the class.

Configure primary authoritative server (BIND)

Introduction to reverse DNS

To map your IP address to your domain name, we'll need to setup a reverse zone. We are going to configure a hidden authoritative server for your reverse zone and create the authoritative zone `reverse_grpX.<lab_domain>.te-labs.training`.

```
# nano /etc/bind/zones/reverse_grpX.<lab_domain>.te-labs.training.
```

```
$TTL      300
@         IN      SOA      soa.grpX.<lab_domain>.te-labs.training. dnsadmin
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        86400 )    ; Negative Cache TTL
;

                        IN      NS       ns1.grp1.rw.te-labs.traini
                        IN      NS       ns2.grp1.rw.te-labs.traini
66        IN      PTR      soa.grpX.<lab_domain>.te-labs.training.
67        IN      PTR      resolv1.grpX.<lab_domain>.te-labs.training.
68        IN      PTR      resolv2.grpX.<lab_domain>.te-labs.training.
130       IN      PTR      ns1.grpX.<lab_domain>.te-labs.training.
131       IN      PTR      ns2.grpX.<lab_domain>.te-labs.training.
```

Save and exit.

Next, edit the `/etc/bind/named.conf.local` file and add the following lines:

```
zone "X.100.100.in-addr.arpa" {
    type primary;
    file "/etc/bind/zones/reverse_grpX.<lab_domain>.te-labs.training.";
};
allow-transfer { any; };
also-notify {100.100.1.130; 100.100.1.131; };
```

Save and exit.

Run the following command to check for any errors in your setup:

```
# named-checkconf
```

Restart Bind 9 and test your reverse DNS using dig

```
# dig -x 100.100.X.66 @127.0.0.1
```

Or

```
# dig 66.X.100.100.in-addr.arpa. PTR @100.100.X.66
```

Question: Do you get a DNS response with the PTR record in the answer section?

Configure secondary authoritative servers (ns1 and ns2)

These servers are the ones that expose our zone publicly (so they will be open-to-all servers).

You should now know how to configure the secondary NS. If you forgot, go back to the lab where you created the forward zone for your grp and follow the instructions to do this new configuration for your reverse zone.

Once you are done with configuration, test your reverse zone propagation.

Test your zone configuration and propagation.

Use dig tool to test the domain

We will now use *dig* tool to verify our own zone configuration and propagation, then do the same for one or two other groups in the class and share comments. From your client, run the following dig queries. All should return answer otherwise you should review your configurations before continuing:

1. `dig -x 100.100.X.66 @100.100.X.66`
2. `dig -x 100.100.X.66 @100.100.X.130`
3. `dig -x 100.100.X.66 @100.100.X.131`
4. `dig -x 100.100.X.67 @100.100.X.130`
5. `dig -x 100.100.X.68 @100.100.X.130`