Linux Servers

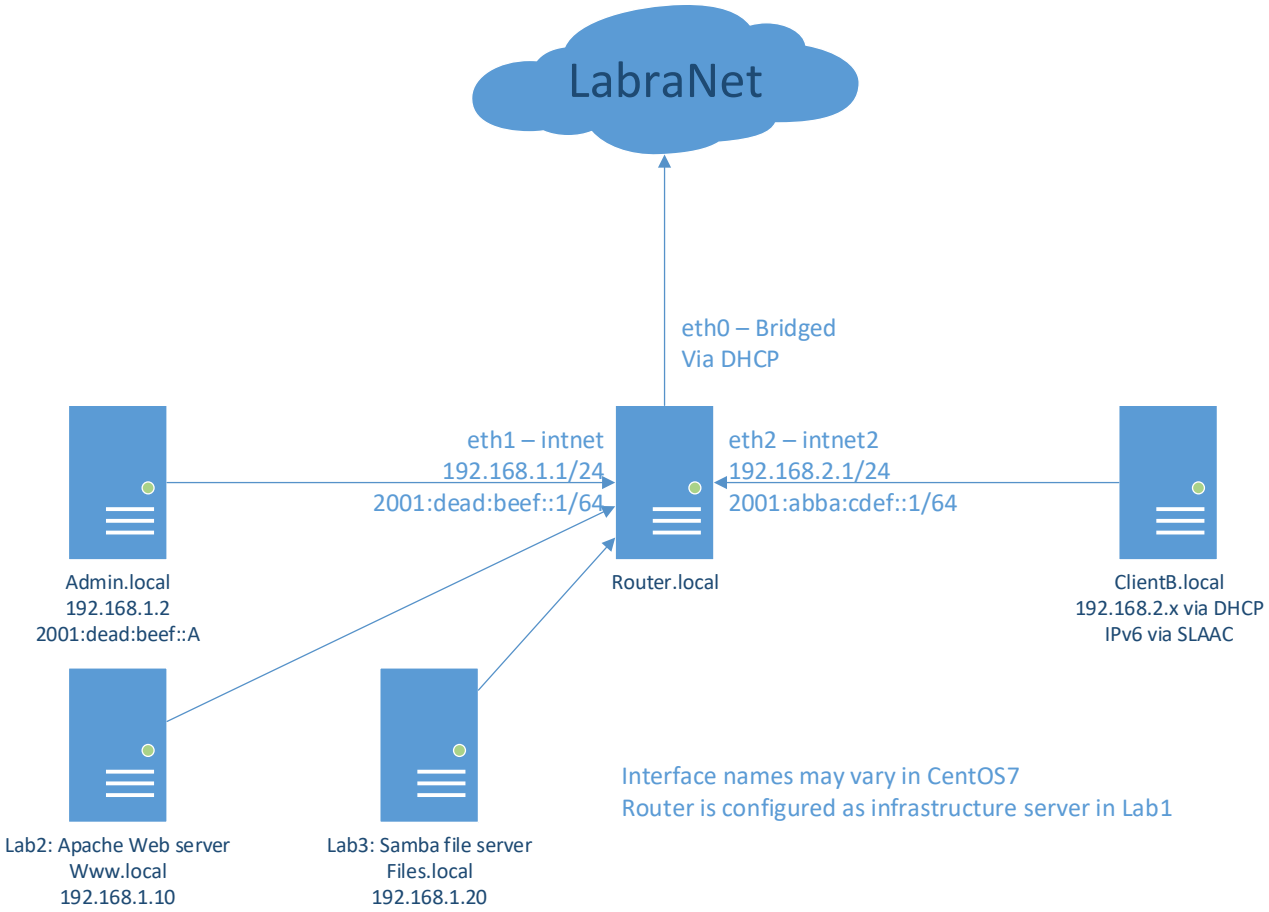
Lab1 – Infrastructure Server

Mikael Romanov

Document your commands or take screenshots. Answer questions in english or finnish.

All configuration must be persistent (survive a reboot). You may use your own notes and Internet resources for your aid. You may consult the teacher or other students.

The labs use the following topology:



- **Generic routing and firewalling (1p)**

Configure IP and IPv6 forwarding in Router.local. (/etc/sysctl.conf)

I conifgured inside /etc/sysctl.conf file ipv6 forwardingin on, as shown in the snip below the command is net.ipv6.conf.all.forwarding=1

```
  GNU nano 2.3.1            File: /etc/sysctl.conf

# System default settings live in /usr/lib/sysctl.d/00-syst
# To override those settings, enter new settings here, or i
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward =1
net.ipv6.conf.all.forwarding =1
```

And added a line in /etc/sysconfig/network file:

```
  GNU nano 2.3.1          File: /etc/sysconfig/network

# Created by anaconda
IPV6FORWARDING=yes
```

Then I restarted the services again and tested that the ipv6 forwading is on. The service was on.

```
[admin@router ~]$ sudo sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
```

Configure firewall (either FirewallD or iptables): Both internal networks must be allowed access to internet. NAT (masquerade) must be used on the outgoing interface. intnet network is considered as trusted and may access intnet2 but not the other way around.

Added firewall rules to the router so it can reach internet which was done with command firewall-cmd –direct –add-rule ipv4 nat POSTROUTING 0 -o enp0s3 -j MASQUERADE:

Routerilla firewall sääntö, että pääsee nettiin, joka tehty komennolla firewall-cmd –direct –add-rule ipv4 nat POSTROUTING 0 –o enp0s3 –j MASQUERADE:

```
[admin@router ~]$ sudo firewall-cmd --direct --get-all-rules
ipv4 nat POSTROUTING 0 -o enp0s3 -j MASQUERADE
ipv4 filter FORWARD 0 -j ACCEPT
```

Määrätään intnet1 trusted zone:ksi /etc/sysconfig/network-scripts kansiosta:

The

```
  GNU nano 2.3.1         File: ifcfg-Wired_connection_1

TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=intnet1
UUID=b4ef05f5-ad34-43ce-bd6f-d087041105b4
ONBOOT=yes
IPV6ADDR=2001:dead:beef::1/64
DEVICE=enp0s8
IPADDR=192.168.1.1
PREFIX=24
ZONE=trusted_
```

nano

Määritetään intnet2 internal zoneksi samasta kansiosta:

```
  GNU nano 2.3.1              File: ifcfg-intnet2

HWADDR=08:00:27:39:FF:31
TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=intnet2
UUID=39d30f78-85cc-467d-91d9-0f728f7a927b
ONBOOT=yes
IPADDR=192.168.2.1
PREFIX=24
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
ZONE=internal_
```

```
[root@router network-scripts]# firewall-cmd --get-active-zones
internal
  interfaces: enp0s9
external
  interfaces: enp0s3
trusted
  interfaces: enp0s8
```

The following services/ports need to be allowed in internal zone: dns/udp53, ping/icmp

Lisäsin firewall sääntöihin ensin dns palvelun:

```
[admin@router network-scripts]$ sudo firewall-cmd --permanent --zone=internal --
add-service=dns
success
```

Tälle avasin portin 53 udp:

```
[admin@router network-scripts]$ sudo firewall-cmd --permanent --zone=internal --
add-port=53/udp
success
```

ICMP-block ei ollut oletuksena päällä internal zonessa, joten ping toimii:

```
[admin@router network-scripts]$ sudo firewall-cmd --zone=internal --list-all
internal
  interfaces:
  sources:
  services: dhcpv6-client dns ipp-client mdns samba-client ssh
  ports: 53/udp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

Zones to be used if configuring with firewallD: external, trusted, internal. (Use network-scripts to configure zones, ZONE=xxx). DO NOT use firewall-cmd --change-zone or --change-interface, it will NOT work.

- **Name resolution (1p)**

Install BIND on Router.local as a resolving name server. Listen at all interfaces but allow queries from internal networks only.

Asennetaan BIND:

```
[admin@router network-scripts]$ sudo yum install bind bind-utils -y
```

Muokataan BINDin conffia /etc/named.conf ja laitetaan se kuuntelemaan kaikkia rajapintoja ja sallitaan kyselyt vain internal networkista:

```
  GNU nano 2.3.1            File: /etc/named.conf

//
// named.conf
//
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { 192.168.1.0/24;192.168.2.0/24;_};
```

- **Local names (1p)**

Create a .local –zone and corresponding reverse zone in BIND (example zones can be found in Optima) and add the following name-IP mappings in them:

- router.local – 192.168.1.1
- admin.local – 192.168.1.2
- www.local – 192.168.1.10
- files.local – 192.168.1.20

muokkasin /etc/named.conf
tiedostoa

```
 GNU nano 2.3.1            File: /etc/named.conf                    Modified


        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recur$
         - If you are building a RECURSIVE (caching) DNS server, you need to en$
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enabl$
           control to limit queries to your legitimate users. Failing to do so $
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable no;
        dnssec-validation no;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
```

```
zone ".local"{
        type master;
        file "local.fwd";
        allow-update {none;};
};

zone "1.168.192.in-addr.arpa"{
        type master;
        file "local.rr";
        allow-update {none;};
```

```
[root@router named]# cp -p named.localhost local.forward.zone
[root@router named]# cp -p named.loopback local.reverse.zone
[root@router named]# ls -l
total 24
drwxrwx---. 2 named named   22 Nov  4 09:37 data
drwxrwx---. 2 named named   58 Nov  4 09:38 dynamic
-rw-r-----. 1 root  named  152 Jun 21  2007 local.forward.zone
-rw-r-----. 1 root  named  168 Dec 15  2009 local.reverse.zone
-rw-r-----. 1 root  named 2076 Jan 28  2013 named.ca
-rw-r-----. 1 root  named  152 Dec 15  2009 named.empty
-rw-r-----. 1 root  named  152 Jun 21  2007 named.localhost
-rw-r-----. 1 root  named  168 Dec 15  2009 named.loopback
drwxrwx---. 2 named named    6 Sep 28 16:14 slaves
```

```
$ORIGIN local.
@       IN SOA  @ local.(
                2016100000
                28800
                7200
                604800
                85400 )

        IN      NS      router.local.
router.local.   IN      A       192.168.1.1
admin   IN      A       192.168.1.2
client  IN      A       192.168.2.3
files   IN      A       192.168.1.20
www     IN      CNAME   192.168.1.10
```

```
$ORIGIN 1.168.192.in-addr.arpa.
@       IN SOA  @ local.(
        2016100000
        28800
        7200
        604800
        85400)

        IN      NS      router.local.
1       IN      PTR     router.local.
2       IN      PTR     admin
10      IN      PTR     www
20      IN      PTR     files
```

```
[root@router named]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service t
o /usr/lib/systemd/system/named.service.
```

- **DHCP (1p)**

Install isc-dhcp –server (or dhcp3) and set it to serve addresses to 192.168.2.0/24 with it. Serve 192.168.2.1 as the gateway and also as the DNS server in the network. See /usr/share/doc/dhcp-4.2.5 for config examples.

Dhcp:n asennus:

```
[admin@router var]$ sudo yum install dhcp_
```

Kopioin esimerkin /usr/share/doc/dhcp-4.2.5 kansiosta /etc/dhcp/dhcpd.conffiin, kommentoin muut kohdat ja lisäsin jakamaan osoitteita välillä 192.168.2.0 – 192.168.2.254, default gatewayksi 192.168.2.1 ja nimipalvelimeksi 192.168.2.1:

```
  GNU nano 2.3.1          File: /etc/dhcp/dhcpd.conf

# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "local";
option domain-name-servers local;

default-lease-time 600;
max-lease-time 7200;
```

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
authorative;
_
subnet  192.168.2.0 netmask 255.255.255.0 {
        range 192.168.2.0 192.168.2.254;
        option routers 192.168.2.1;
        option domain-name-servers 192.168.2.1;
}
```

IPv6 & SLAAC (1p)

Set the IPv6 addressing as shown in the topology. Install radvd-package and set it to serve IPv6 addresses from 2001:abba:cdef::/64 network to intnet2. Default settings in /etc/radvd.conf will be mostly correct.

I installed radvd.

```
[admin@router var]$ sudo yum install radvd
```

Muokkasin radvd.conf tiedostoon interfacen enp0s9, joka on intnet2 ja laitoin ipv6 osoitteen prefix:ksi 2001:abba…jne

```
interface enp0s8_
{
        AdvSendAdvert on;
        MinRtrAdvInterval 30;
        MaxRtrAdvInterval 100;
        prefix 2001:abba:cdef::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
        };

};
```

```
[root@router named]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service t
o /usr/lib/systemd/system/named.service.
[root@router named]# systemctl enable radvd
Created symlink from /etc/systemd/system/multi-user.target.wants/radvd.service t
o /usr/lib/systemd/system/radvd.service.
[root@router named]# systemctl enable dhcpd
Created symlink from /etc/systemd/system/multi-user.target.wants/dhcpd.service t
o /usr/lib/systemd/system/dhcpd.service.
You have new mail in /var/spool/mail/root
[root@router named]# systemctl enable httpd
```

Testing

Reboot router.local and admin/client and verify that your configuration persists. Test that you can access Internet from Admin.local and ClientB.local. Test that you can ping and ping6 ClientB from Admin.local.

Checklist for screenshots/documentation:

- Services are running after a reboot (systemctl status service) and firewall-rules are in effect (firewall-cmd --list-all or iptables -nvL)
- ClientB gets both IPv4 and IPv6 address, gateway and a DNS server (ifconfig, /etc/resolv.conf, route -n, route -6 -n)

  ClientB saa IPv4 ja IPv6 osoitteet:

```
[admin@clientb ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.3  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 2001:abba:cdef:0:a00:27ff:fe2e:de9f  prefixlen 64  scopeid 0x0<glo
bal>
```

  Route –n tuloste:

```
[admin@clientb ~]$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.1     0.0.0.0         UG    100    0        0 enp0s3
192.168.2.0     0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
```

  Route -6 –n tuloste:

```
::1/128                     ::                          U     256 0        0 lo
::/96                       ::                          !n    1024 0       0 lo
0.0.0.0/96                  ::                          !n    1024 0       0 lo
2001:abba:cdef::/64         ::                          U     100 0        2 enp0s
3
2002:a00::/24               ::                          !n    1024 0       0 lo
2002:7f00::/24              ::                          !n    1024 0       0 lo
2002:a9fe::/32              ::                          !n    1024 0       0 lo
2002:ac10::/28              ::                          !n    1024 0       0 lo
2002:c0a8::/32              ::                          !n    1024 0       0 lo
2002:e000::/19              ::                          !n    1024 0       0 lo
3ffe:ffff::/32              ::                          !n    1024 0       0 lo
fe80::/64                   ::                          U     256 0        2 enp0s
3
::/0                        fe80::a00:27ff:fe39:ff31    UG    100 0        0 enp0s
3
::/0                        ::                          !n    -1  1       29 lo
::1/128                     ::                          Un    0   1       33 lo
2001:abba:cdef:0:a00:27ff:fe2e:de9f/128 ::                          Un    0   1
  8 lo
fe80::a00:27ff:fe2e:de9f/128 ::                         Un    0   1        3 lo
ff00::/8                    ::                          U     256 1        0 enp0s
3
::/0                        ::                          !n    -1  1       29 lo
[admin@clientb ~]$ _
```

- ClientB can resolve www.google.com and router.local or any other names (dig/nsloookup)
- Admin can ping and ping6 ClientB, ClientB can ping gateway and www.google.com, Admin can ping www.google.com

  Adminin ping clientB:lle:

```
[admin@admin ~]$ ping 192.168.2.3
PING 192.168.2.3 (192.168.2.3) 56(84) bytes of data.
64 bytes from 192.168.2.3: icmp_seq=1 ttl=63 time=0.506 ms
64 bytes from 192.168.2.3: icmp_seq=2 ttl=63 time=0.490 ms
```

- wget www.google.com loads index.html