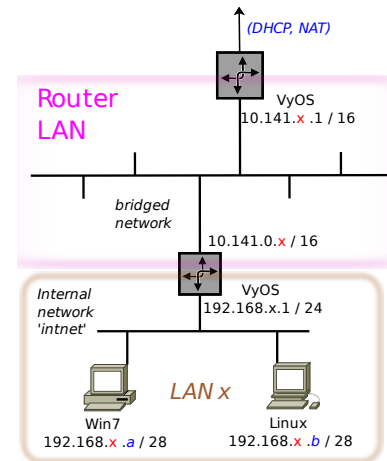


## Networking VyOS Internet Router Worksheet

# Route the LAN to the Internet

In this worksheet you will add another router to your installation. This router will indirectly connect your LAN to the Internet. It serves as a "border router" for the "autonomous system" formed by the virtual subnets.



## Reconfigure your current VyOS VM

Make sure that your VyOS router is powered off. Then do these steps:

1. Select "Settings" for the VyOS router.
2. Select "Network"; click on the tab for Adapter 1.
3. Set to be attached to "Internal Network". Enter the **"routernet"** as the name of the network.
4. Click on the tab for Adapter 2.
5. Set it to be attached to "Internal Network", name **"intnet"**.
6. Click on "Okay".

Now start your router, and do the following:

1. Start the configuration:

```
configure
```

2. Configure the internal LAN interface:

```
del interfaces ethernet eth1 address
del interfaces ethernet eth1 description
set interfaces ethernet eth1 address '192.168.x.1/24'
set interfaces ethernet eth1 description 'LAN'
```

3. Configure the interface to other routers:

```
del interfaces ethernet eth0 address
del interfaces ethernet eth0 description
set interfaces ethernet eth0 address '10.141.0.x/16'
set interfaces ethernet eth0 description 'ROUTERNET'
```

4. Check your work with the command:

```
show interfaces
```

5. Commit your changes, save them, and exit:

```
commit
save
exit
```

Leave this VM running while you do the next steps.

---

## Install another VyOS Router VM

Repeat these steps from the VyOS worksheet:

1. Run the command **virtualbox** from the command line, or find the link from the start menu.
2. Click on "New" from the VM manager window. Name this machine "border-**<number>**", where "**<number>**" is the last number of your physical host's IP address (*e.g.* 106 or 118). Set the "Type" and "Version" as Linux, Debian 64-bit, and click on "Next >".
3. Set the Memory at 512 MB, and click on "Next".

Check "Create a virtual hard drive now", and click on "Create".

Check "VDI (VirtualBox Disk Image)", and click on "Next".

Check "Dynamically allocated", and click on "Next".

Set the virtual hard drive size to about 2 GB, and click on "Create".

4. Select your VyOS VM in the VM manager, and click on the "Settings" icon.

Choose the "Network" item in the dialog box.

5. You should see a tab labeled "Adapter 1"

Verify that it is enabled, and attached to NAT.

6. Click the tab labeled "Adapter 2".

- Check the "Enable Network Adapter" box.
- Set it to be Attached to: "Internal Network". Enter "**routernet**" for the network name.

7. Choose the "Storage" item on the left.

8. Choose the "Empty" item under "Controller: IDE".

- Click on the "CD" icon under the Attributes section on the right. Select "Choose a virtual CD/DVD disk file..."
- Browse to where you saved the vyos .iso file. Double-click on it.

9. Click on "OK".

10. Select your new VM in the VM manager, and click on "Start".

You should see a basic text-mode login. Login with username "vyos" and password "vyos" (sense a pattern here?)

11. Run the command "install image". Accept defaults, but enter "yes" when asked to "Continue?"

Name the image "router-**x**" (replace **x** with the last part of your physical host's IP address).

Re-enter the password "vyos" twice.

12. Enter the command "poweroff".

13. Click on the "Settings" menu in the VM manager.

Choose "Storage", and select the vyos .iso line.

Click on the round "CD" icon in the Attributes panel on the right.

Click on "Remove disk from virtual drive".

Click on "OK".

---

### Configure VyOS to route between your LAN and the campus network.

**In the following steps, replace the value "x" with the last part of your physical host's IP address.**

Restart your vyos VM. Press "Enter" twice, to boot the VM, or just wait for it.

Login to the router, using account "vyos" and password "vyos".

Enter these commands:

1. Start the configuration:

```
configure
```

2. (Get rid of an error message:)

```
delete system console device ttyS0
```

3. Configure the router's interface to the outside world:

```
set interfaces ethernet eth0 address dhcp  
set interfaces ethernet eth0 description 'World'
```

Configure the interface to other routers:

```
set interfaces ethernet eth1 address '10.141.x.1/16'  
set interfaces ethernet eth1 description 'ROUTERNET'
```

Check your settings with the command:

```
show interfaces
```

4. Set up RIPv2 routing. This will share routing information with the other routers that are specified as neighbors.

For this you will need your "neighbor" LAN network addresses — these will be the LAN numbers one less than, and one greater than, your own. For example, if your LAN number is 103, then your neighbors will be 102 and 104. (The instructor machine, LAN number 119, has neighbors 118 and 120.)

```
#-----  
# Configure RIPv2 on gateway router.  
# (If necessary, change "148.137.141.1" to an upstream router,  
#   such as the Hardware Lab's gateway router.)  
# Change "10.141.0.." to the router subnet.  
# Configure a couple of neighbors, .y and .z  
# 2016-10-22  
#-----  
  
# This appears to prevent duplicated ping responses?  
set interfaces loopback lo address 1.1.1.x/32  
  
# Set default route.  
delete protocols static route 0.0.0.0/0  
set protocols static route 0.0.0.0/0 next-hop 148.137.141.1 distance '3'  
  
# Configure RIP on connected networks  
# .y and .z are one number larger and smaller than the local subnet number.  
set protocols rip redistribute connected  
set protocols rip network 10.141.0.0/16  
set protocols rip neighbor 10.141.0.y  
set protocols rip neighbor 10.141.0.z  
# Shortcut route to the border router...  
#set protocols rip neighbor 10.141.0.1  
  
show protocols  
#-----
```

Replace the *y* and *z* with values for two of your neighbors' LANs.

Check your work again with the command:

```
show protocols
```

5. Configure Network Address Translation (NAT):

```
set nat source rule 100 outbound-interface 'eth0'  
set nat source rule 100 translation address masquerade  
set nat source rule 100 source address '192.168.x.0/24'
```

6. Allow remote connection (more convenient than the console shell):

```
set service ssh port '22'
```

7. Apply a firewall to the outward-facing network interface. This firewall contains rules to prevent packets with spoofed IP addresses from escaping to the Internet. It also repeats the firewall on the gateway router.

```
#-----  
# Set firewall on border router.  
# Block outbound packets that don't claim to be from a LAN.  
# 2016-10-22  
#-----  
  
# Block packets with invalid source addresses:  
set firewall name 'Hosts-to-World' default-action 'drop'  
  
# Accept packets from the routers?:  
#set firewall name 'Hosts-to-World' rule 10 action 'accept'  
#set firewall name 'Hosts-to-World' rule 10 source address 10.141.0.0/16  
#  
# Accept packets from LAN hosts:  
set firewall name 'Hosts-to-World' rule 20 action 'accept'  
set firewall name 'Hosts-to-World' rule 20 source address 172.16.0.0/16  
  
# bind firewall rulesets to an interface  
set interfaces ethernet eth0 firewall out name 'Hosts-to-World'  
#-----  
  
#-----  
# Set firewall on gateway router.  
# Two sets of rules: world-inbound-to-LAN,  
# and world-to-router.  
# No rules for packets outbound from LAN (let the fur fly).  
# 2016-10-22  
#-----  
  
set firewall name 'World-to-LAN' default-action 'drop'  
# allow established and related packets,  
# but no inbound connection requests except pings  
set firewall name 'World-to-LAN' rule 10 action 'accept'  
set firewall name 'World-to-LAN' rule 10 state established 'enable'  
set firewall name 'World-to-LAN' rule 10 state related 'enable'  
set firewall name 'World-to-LAN' rule 10 description 'Allow established and related'  
# allow inbound pings to LAN:  
set firewall name 'World-to-LAN' rule 20 action 'accept'  
set firewall name 'World-to-LAN' rule 20 icmp type-name 'echo-request'  
set firewall name 'World-to-LAN' rule 20 protocol 'icmp'  
set firewall name 'World-to-LAN' rule 20 state new 'enable'  
set firewall name 'World-to-LAN' rule 20 description 'Allow inbound pings'
```

Check your firewall with the command:

```
show firewall
```

---

## Finish up.

1. Apply the configuration:

```
commit
```

2. Save the configuration for future reboots:

```
save
```

3. ... and quit:

exit

---

## Test your Router

In the following steps, replace the value "x" with the last part of your physical host's IP address.

1. First verify that your new router is connected to the Internet: run the command **ping 4.2.2.2**.

You should get a reply from an Internet host. After a few pings, enter a <Ctrl>-C to end the pings.

2. Use either your Linux or Windows VM to run the command **ping 192.168.x.1**. This will test your new router installation.
3. Also run the command **ping 10.141.0.x**. This tests the router's ability to route to its external interface.
4. Try pinging one of the VMs on your neighbor's physical host. You should still be able to ping other people in the class, including the instructor.

**Congratulations! You've set up your LAN's router.**

Homepage: [montcs.bloomu.edu](https://montcs.bloomu.edu/) (URL: <https://montcs.bloomu.edu/>)

© 2004-2016 Robert Montante unless otherwise indicated. All rights reserved.

File last modified 11/02/2016 08:05:27

[Valid XHTML 1.0!](https://validator.w3.org/check?uri=referer) (URL: <https://validator.w3.org/check?uri=referer>)  
[Valid CSS!](https://jigsaw.w3.org/css-validator/check/referer) (URL: <https://jigsaw.w3.org/css-validator/check/referer>)