Systems Advanced II
Linux

Routing

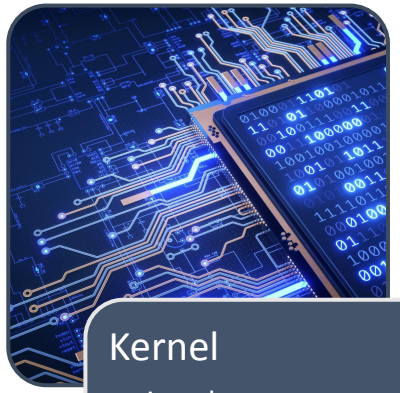
DE HOGESCHOOL MET HET NETWERK

Elfde-Liniestraat 24, 3500 Hasselt, www.pxl.be

Doelstellingen

- De student:
  - De student kan Netwerk-services installeren, configureren en onderhouden.
  - De student kan microservices-infrastructuur opzetten en beheren.
  - De student kan een (eigen) cloud systeem opzetten a.d.h.v. opgelegde voorwaarden.
  - De student kan een systeem beveiligen.

Systems Advanced II - Linux



Kernel

- virtual memory
- user space and kernel space
- processes and threads
- sockets & pipes
- systemd
- Docker

Networking

- routing
- firewall
- eBPF
- certificates
- ssh
- latency
- bandwidth

Services

- nfs
- load balancers and reverse proxies
- databases
- logging

Clusters

- Storage
- Kubernetes

Licensing & open-source software

Systems Advanced II - Linux

kernel

- virtual memory
- user space and kernel space
- processes and threads
- sockets & pipes
- systemd
- Docker

Networking

- routing
- firewall
- eBPF
- certificates
- ssh
- latency
- bandwidth

Services

- nfs (rook)
- load balancers and reverse proxies
- databases
- logging

Clusters

- Storage
- Kubernetes

Systems Advanced II - Linux

kernel

- virtual memory
- user space and kernel space
- processes and threads
- sockets & pipes
- systemd
- Docker

Networking

- routing
- firewall
- eBPF
- certificates
- ssh
- latency
- bandwidth

Services

- nfs (rook)
- load balancers and reverse proxies
- databases
- logging

Clusters

- Storage
- Kubernetes

Agenda

- Routing definitie
- Example Centos network environment met Vagrant
  - Extra Vagrant uitleg
- Routing
  - Add routes in de routing table
  - Configure router en NAT
- Verschil Centos en Ubuntu
- Oefening 1: nu met Ubuntu!
- Oefening 2: extra hop

Routing

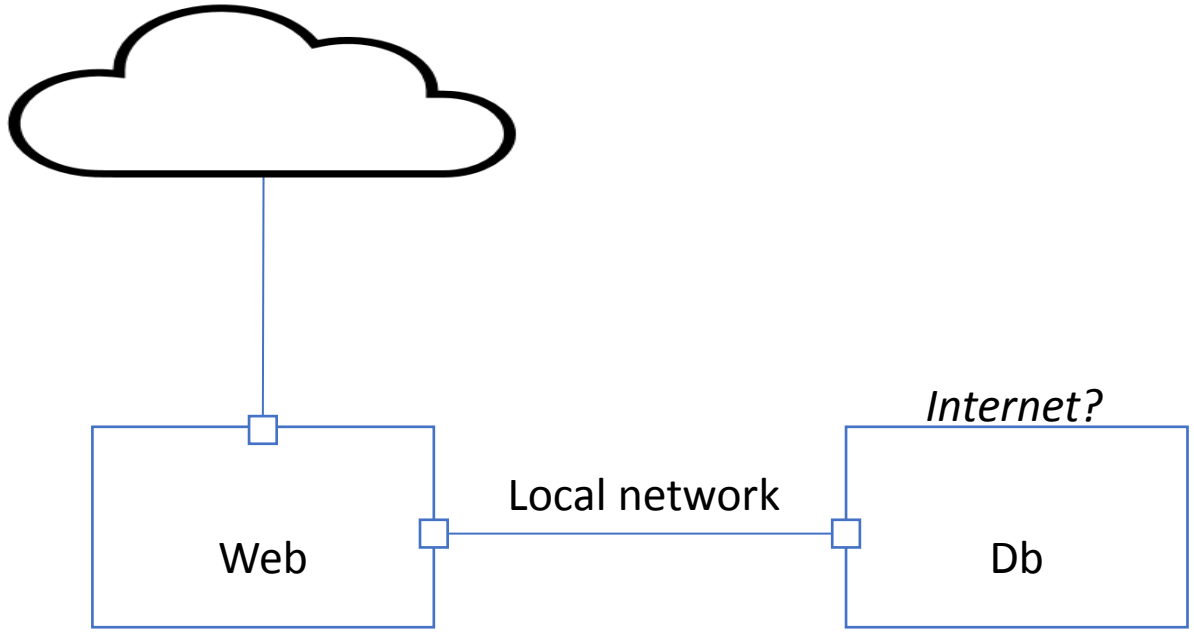
- **Routing** is the process of selecting a path for traffic in a network or between or across multiple networks.
- **Packet forwarding** is the transit of network packets from one network interface to another.
- The routing process usually directs forwarding on the basis of **routing tables.** Routing tables maintain a record of the routes to various network destinations.
- **IP routing** assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices.
- *Routing has become the dominant form of addressing on the Internet.*

Environment prerequisites

- Linux
  - vagrant, git installed

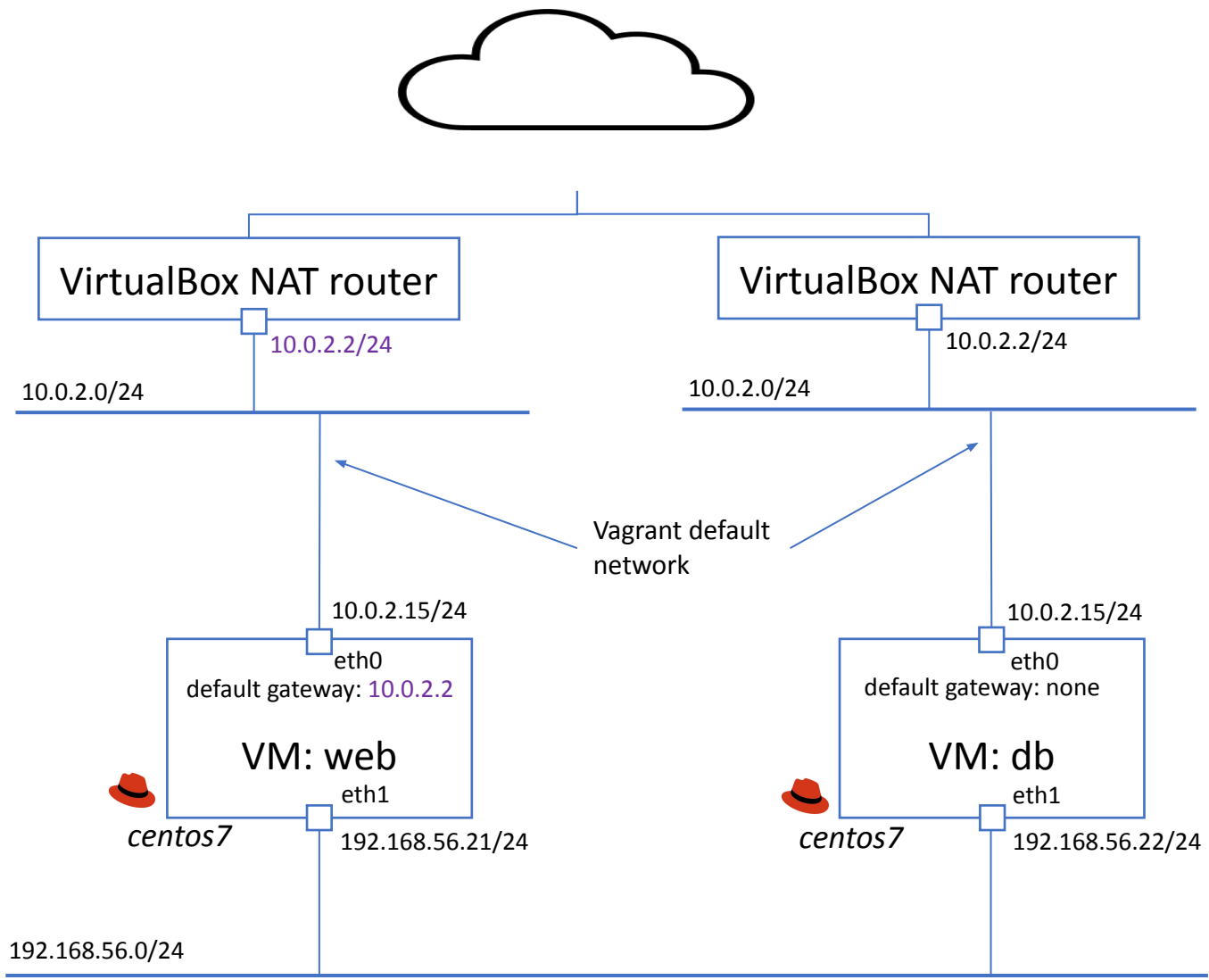
Problem case: router nodig voor Internet connectivity

- 2 machines
  - Web
  - Db
- Web is verbonden aan het Internet
- Db heeft internet connectivity nodig



Vagrant Environment

- Clone environment
  - git clone https://github.com/PXLSystemsAdvancedII/sysadv2-2223.git
- cd sysadv2-2223/routing
- Check config
  - code Vagrantfile *of* vim Vagrantfile
- Start VMs
  - vagrant up
- Check ssh ports
  - vagrant ssh-config web
  - vagrant ssh-config db
- Login vms en check ip, route table
  - vagrant ssh web en vagrant ssh db
  - ip a
  - ip r
  - exit



Vagrantfile

https://github.com/PXLSystemsAdvancedII/sysadv2-2223/blob/main/routing/Vagrantfile

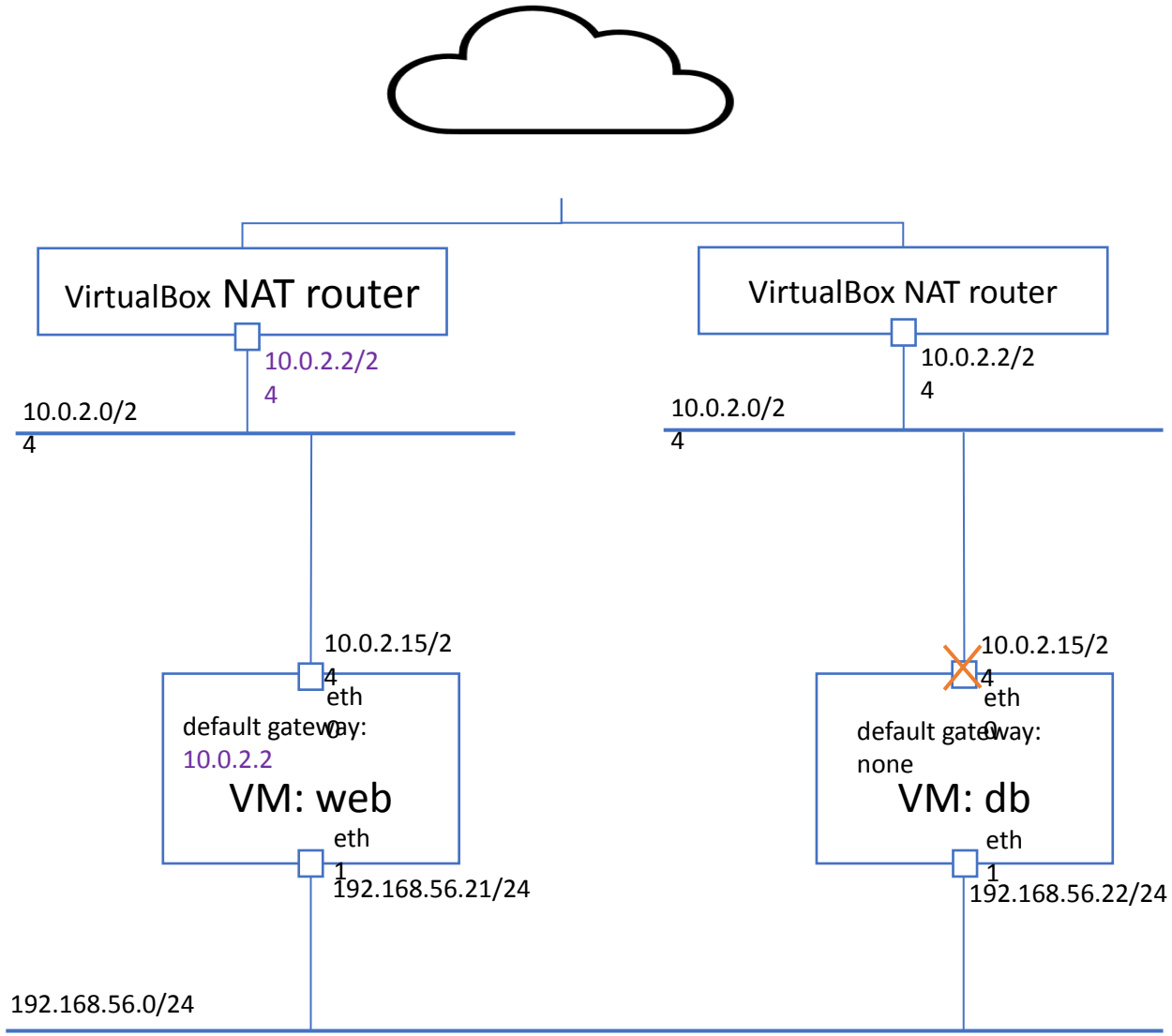
- Vagrant.configure("2") do |config|
  - Versie 2 van de config syntax
- config.vm.define "web" do |web|
  - Definieer vm
- web.vm.hostname = "web.local“
  - Set hostname
- web.vm.box = "centos/7“
  - Gebruik voorgedefineerde vm box centos, 7
    Vagrant box centos/7 - Vagrant Cloud (vagrantup.com)
- web.vm.network "private_network", ip: "192.168.10.21", hostname: true
  - Voeg n/w adapter toe met static ip address en ken hostname toe aan dit ip address
  - Private Networks - Networking | Vagrant by HashiCorp (vagrantup.com)
- web.vm.network "forwarded_port", guest: 80, host: 8888
  - Forward ports
- web.vm.provider :virtualbox do |vb|
  - Virtual box specifieke settings
- web.vm.provision "shell", inline: <<-SHELL

  ...

  SHELL
  - Shell installatie commando’s

Environment: remove eth0 van db

- Login naar db via local host forwarded port, via 10.0.2.15
  - vagrant ssh db
- Open password access sshd
  - sudo sed -re 's/^(PasswordAuthentication)([[:space:]]+)no/\1\2yes/' -i.`date -I` /etc/ssh/sshd_config
    - sudo vi /etc/ssh/sshd_config -> PasswordAuthentication yes
  - sudo systemctl restart sshd
  - exit
- Login naar web, vanaf web naar db
  - vagrant ssh web
  - ssh db
    - Password ‘vagrant’
- db: disable eth0
  - ping 10.0.2.15
  - sudo bash
    - echo "DEVICE=eth0" > /etc/sysconfig/network-scripts/ifcfg-eth0
    - service network restart
    - ifdown eth0
    - exit
  - ping 10.0.2.15



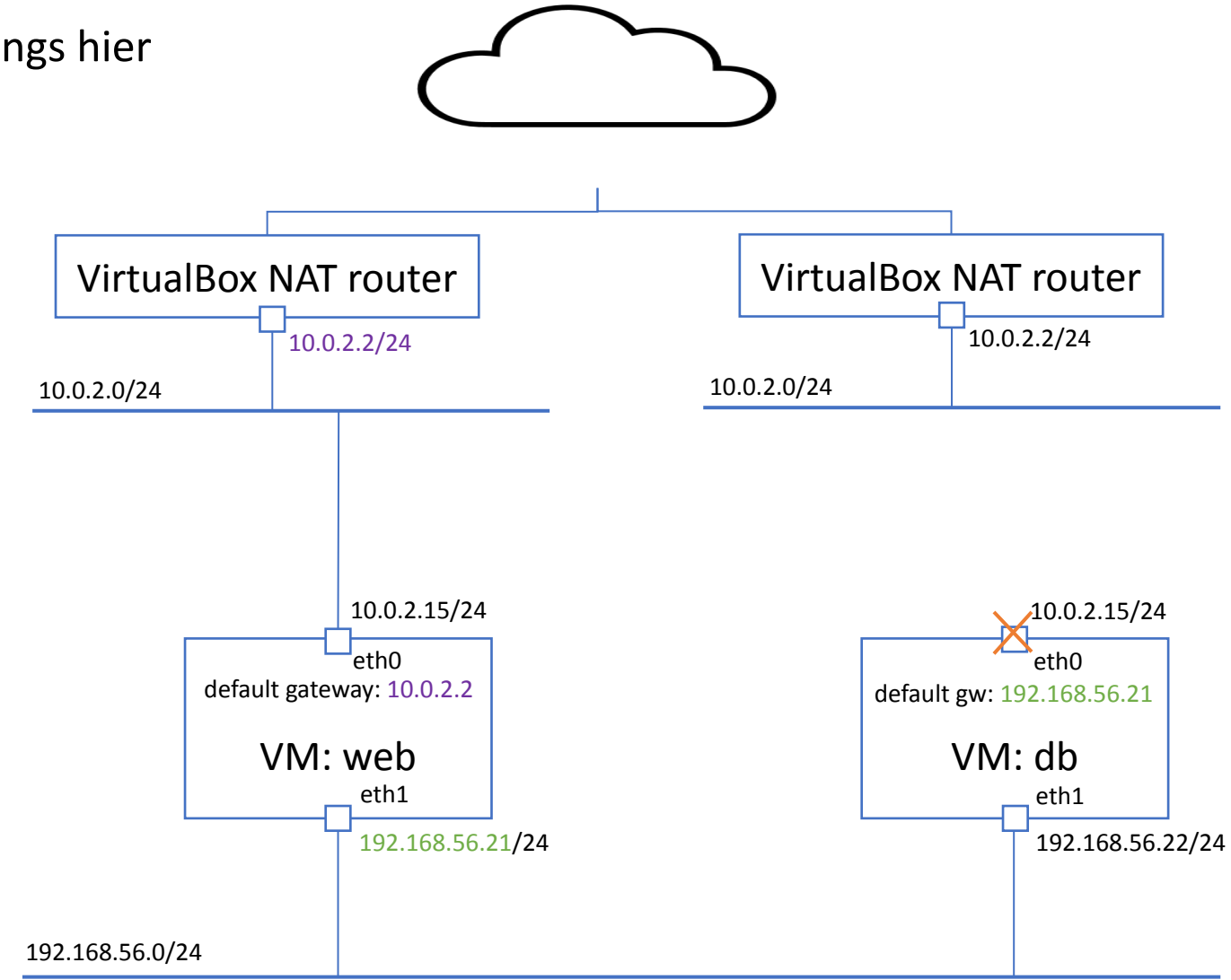
Add routes

Traditional (RHEL, centos)	Netplan (Ubuntu)
/etc/resolve.conf /etc/network/interfaces /etc/sysconfig/network-scripts/	/etc/netplan/*.yaml config files Netplan | Backend-agnostic network configuration in YAML sudo netplan apply

- default route: alle onbekende network access langs hier

db:

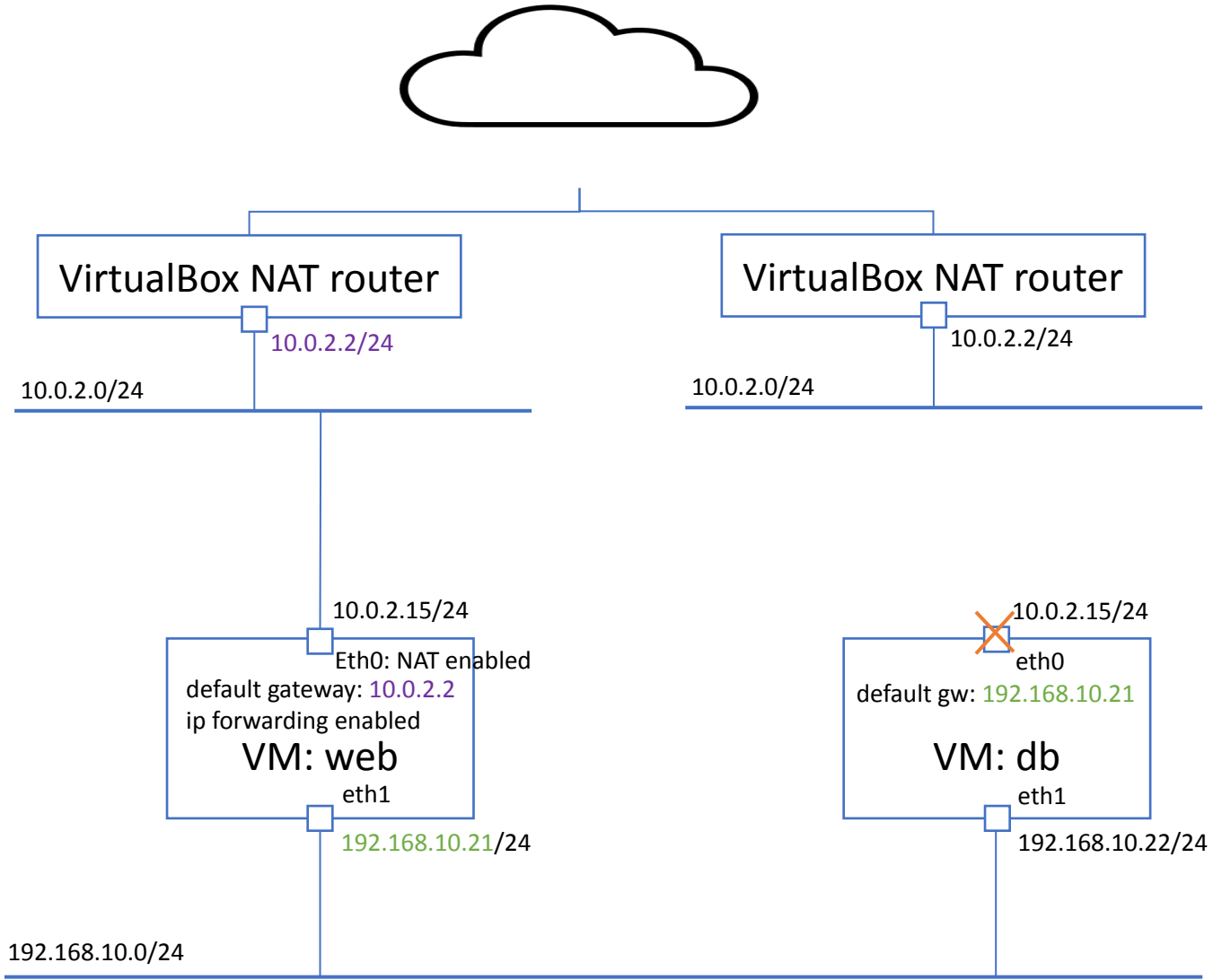
- vagrant ssh web
- ssh db
- ping 10.0.2.15
- ip r
- **Add default gateway**
  - **sudo ip route add default via 192.168.56.21**
  - ip r
- ping 10.0.2.15
- Make change permanent
  - cd /etc/sysconfig/network-scripts
  - sudo vi ifcfg-eth1
    - DEFROUTE=yes
    - GATEWAY=192.168.56.21
- ping 10.0.2.15
- exit



Enable DNS

Traditional (RHEL, centos)	Netplan (Ubuntu)
/etc/resolve.conf /etc/network/interfaces /etc/sysconfig/network-scripts/	/etc/netplan/*.yaml config files Netplan | Backend-agnostic network configuration in YAML sudo netplan apply

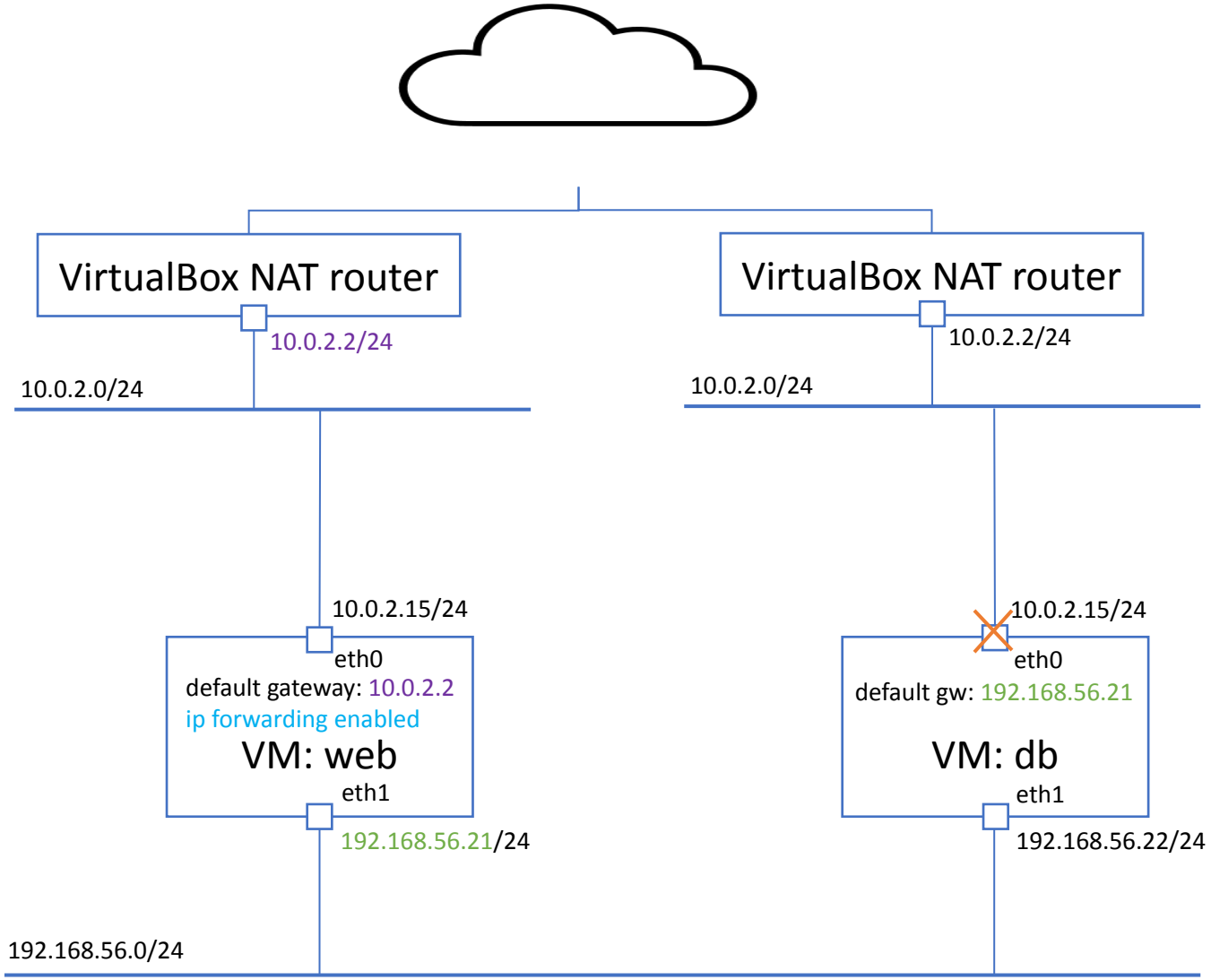
- **Db**: enable DNS
  - ping google.com
  - cat /etc/resolve.conf
  - cd /etc/sysconfig/network-scripts
  - sudo vi ifcfg-eth1
    - PEERDNS=yes
    - DNS1=8.8.8.8
  - sudo ifdown eth1 && sudo ifup eth1



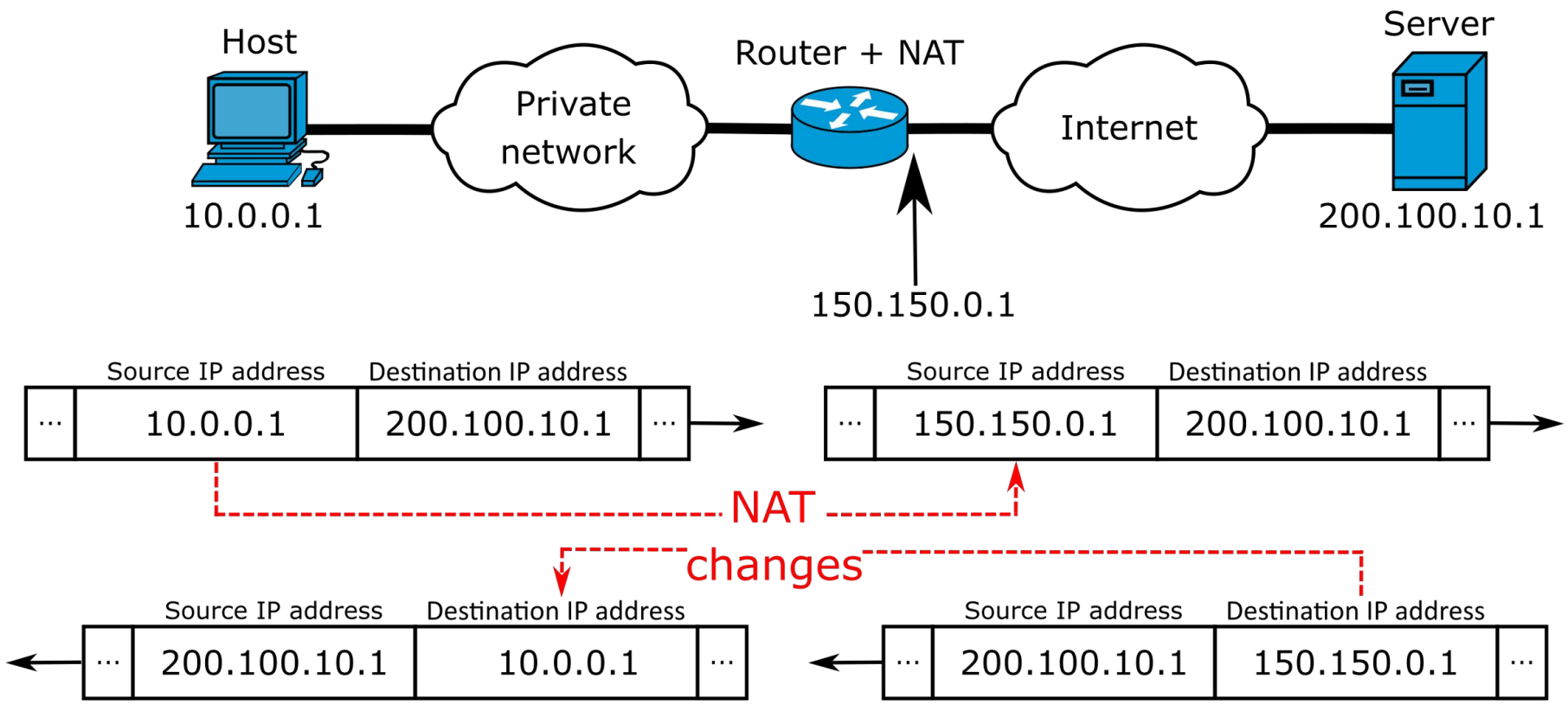
Configure router

- Web: **enable routing**
  - vagrant ssh web
  - cat /proc/sys/net/ipv4/ip_forward
  - sysctl net.ipv4.ip_forward
  - sysctl -w net.ipv4.ip_forward=1
  - **echo "net.ipv4.ip_forward=1" | \ sudo tee -a /etc/sysctl.conf**
  - **sudo sysctl -p**
- Db: test routing
  - ssh db
  - ping 8.8.8.8
    - Packetjes geraken niet terug van het 10.0.2.0/24 netwerk naar 192.168.56.22
  - exit

ip forwarding: ability for an operating system to accept incoming network packets on one interface, identifying that it is not meant for the system itself, but it should be forwarded on to another network



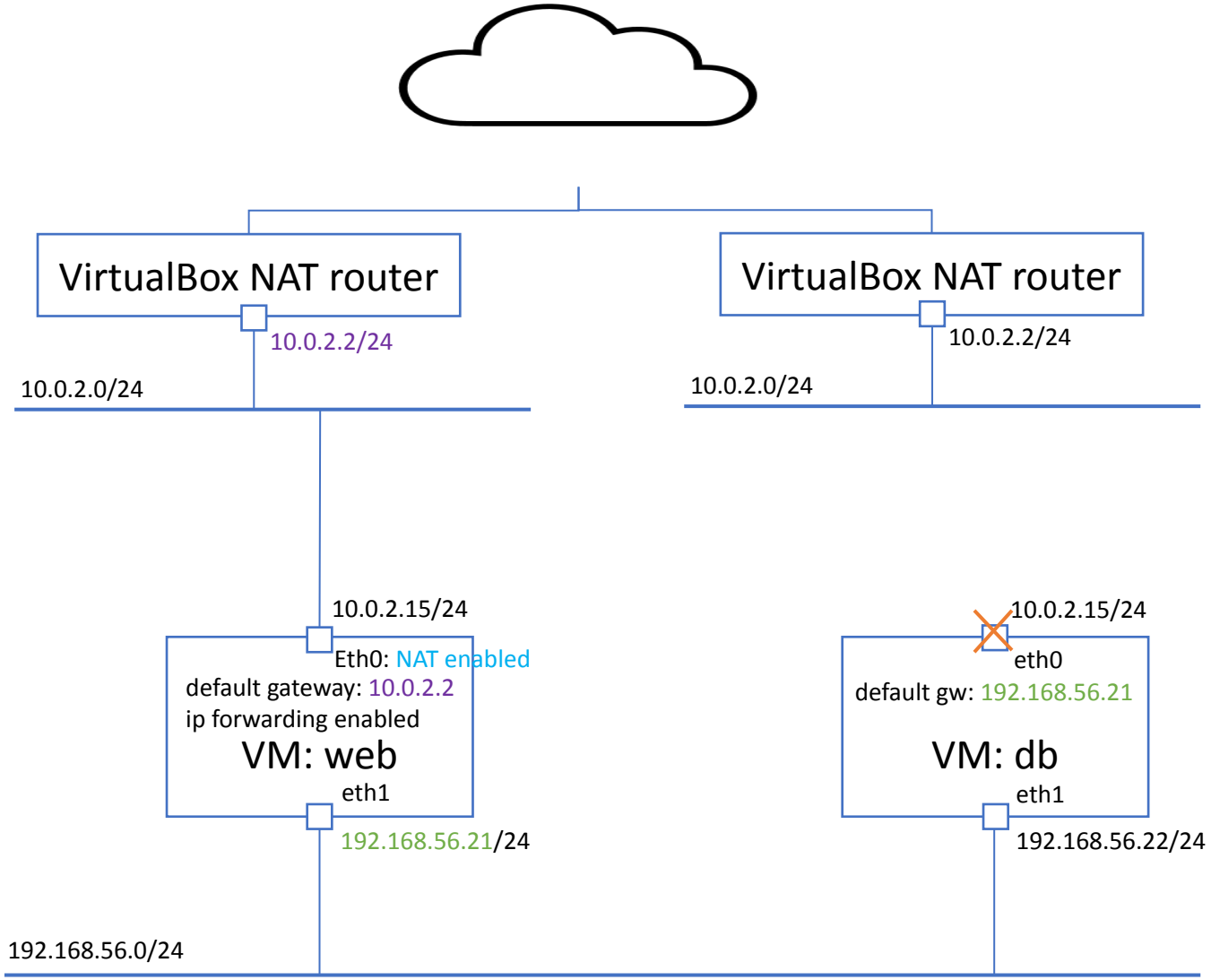
Network Address Translation



Enable NAT

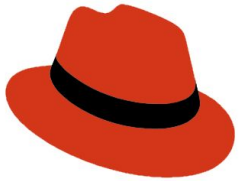
IP masquerading is a technique that hides an entire IP address space, usually consisting of private IP addresses, **behind a single IP (public) address** in another, usually public address space. The hidden addresses are changed into a single IP address as the source address of the outgoing IP packets so they appear as originating not from the hidden host but from the routing device itself.

- web:
  - Stop firewalld
    - sudo iptables -L
    - sudo systemctl stop firewalld
    - sudo iptables -L
  - **NAT**
    - sudo iptables -t nat -L
    - **sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**
    - sudo iptables -t nat -L
- Db: test nat routing
  - ssh db
  - ping 10.0.2.2
  - ping google.com
  - sudo yum install traceroute
  - traceroute pxl.be

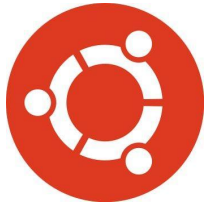


Summary: Add routes

- Temporary:
  - ip route add default via <ip>

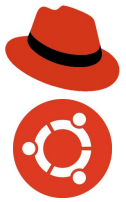


- Traditional Linux (RHEL, centos)
  - /etc/sysconfig/network-scripts/ifcfg-<nic>
    - DEFROUTE=yes
    - GATEWAY=<ip>
    - PEERDNS=yes
    - DNS1=<dns_ip1>
    - DNS2=<dns_ip2>
  - ifdown <nic> && ifup <nic>



- Ubuntu-based
  - /etc/netplan/*.yaml config files
    - `gateway4: <ip>`
    - `nameservers:`
    - `addresses:`
    - `- <dns_ip1>`
    - `- <dns_ip2>`
  - sudo netplan apply
  - Netplan | Backend-agnostic network configuration in YAML

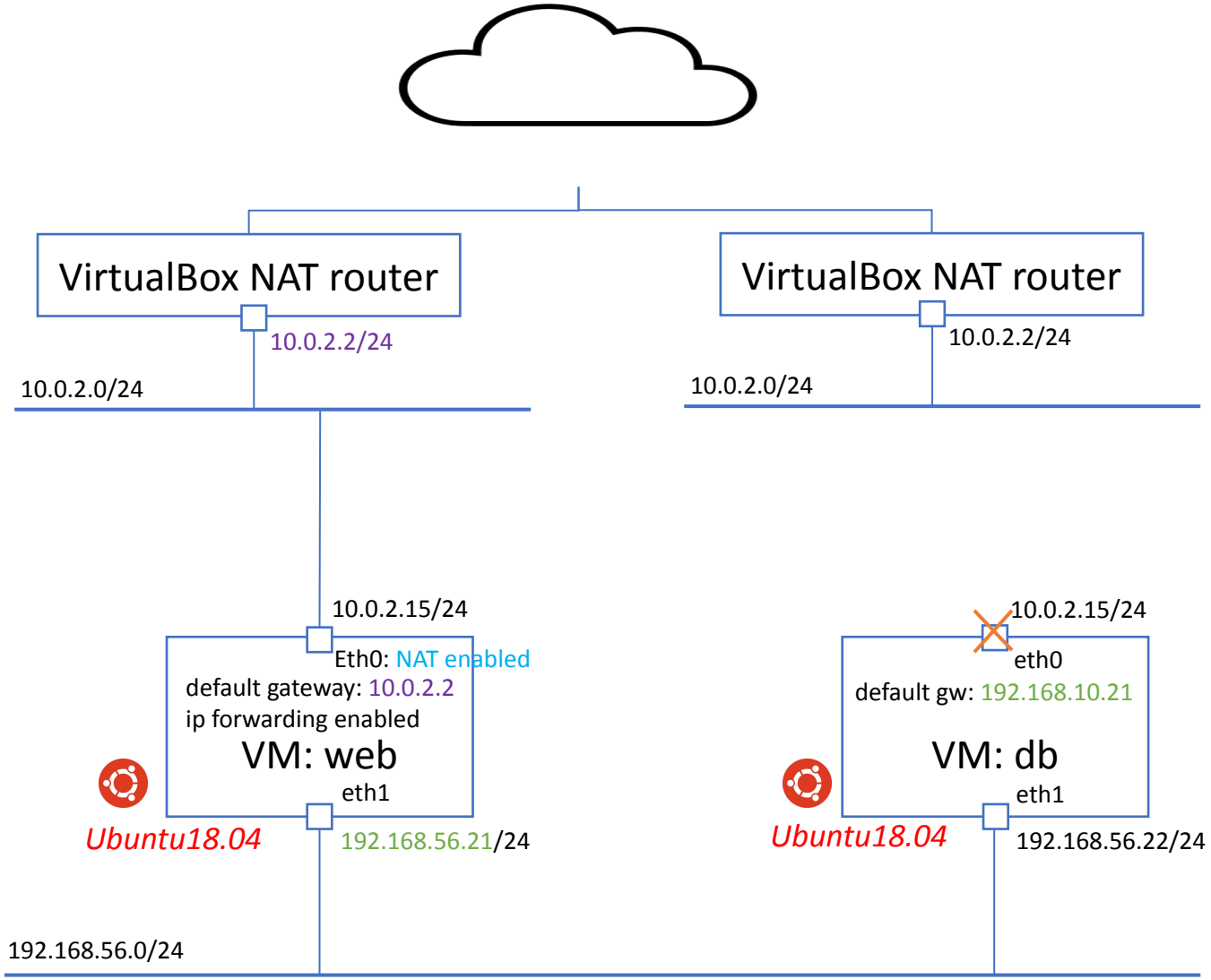
Summary: Router config



- Enable IP-forwarding
  - cat /proc/sys/net/ipv4/ip_forward
  - sysctl -w net.ipv4.ip_forward=1
  - vi /etc/sysctl.conf
    - net.ipv4.ip_forward=1
  - sysctl -p
- Enable NAT
  - iptables -t nat -A POSTROUTING -o <NIC> -j MASQUERADE

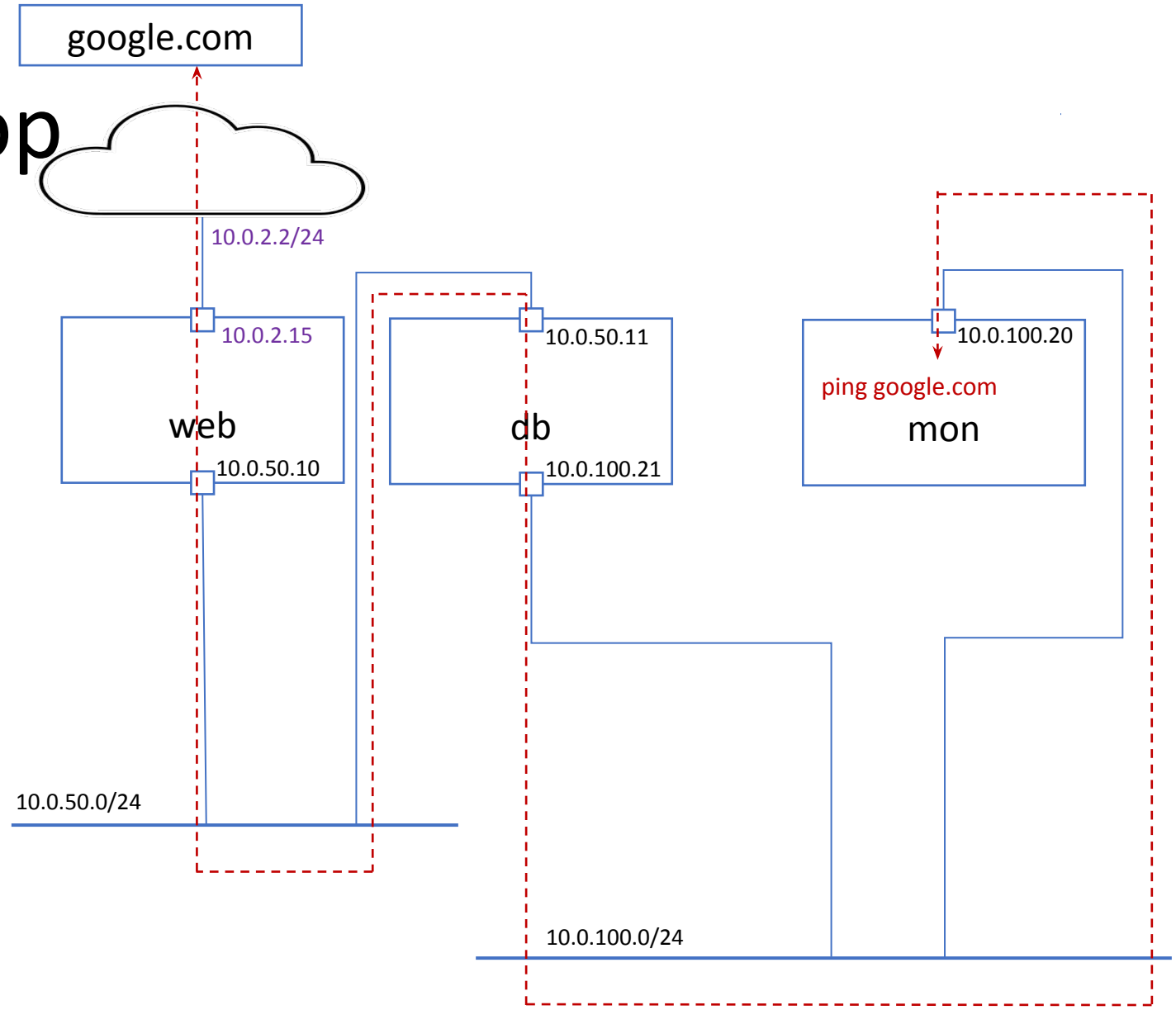
Oefening 1: nu met Ubuntu!

- Check vagrant config in sysadv2223/routing_ubuntu
- Pas de configuratie aan zodat het routing diagram automatisch mee provisioned wordt door vagrant



Oefening 2: extra hop

- Maak een nieuwe set-up gebaseerd op het diagram hiernaast
- Gebruik ubuntu de hosts
- De host mon heeft Internet connectiviteit via db naar web naar het Internet
- Check traffic naar google.com met traceroute



end