

SE 4455 – Cloud Computing

Linux Containers with LXC

Dr. Jagath Samarabandu

jagath@uwo.ca

TEB 351

519-661-2111 x80058

LXC Setup with Debian 8.7 (Jessie)

- Each VM has a minimal Debian 8.7 install
 - LXC 2.0 packages installed from "jessie-backports" (backported from Debian 9)
- Guide: wiki.debian.org/LXC
 - Be careful with online guides that may be obsolete due to rapid development of LXC
 - Due diligence: Understand purpose of each command as well as all the parameters
 - Note: "sudo" - running commands that need super-user privileges from a normal shell

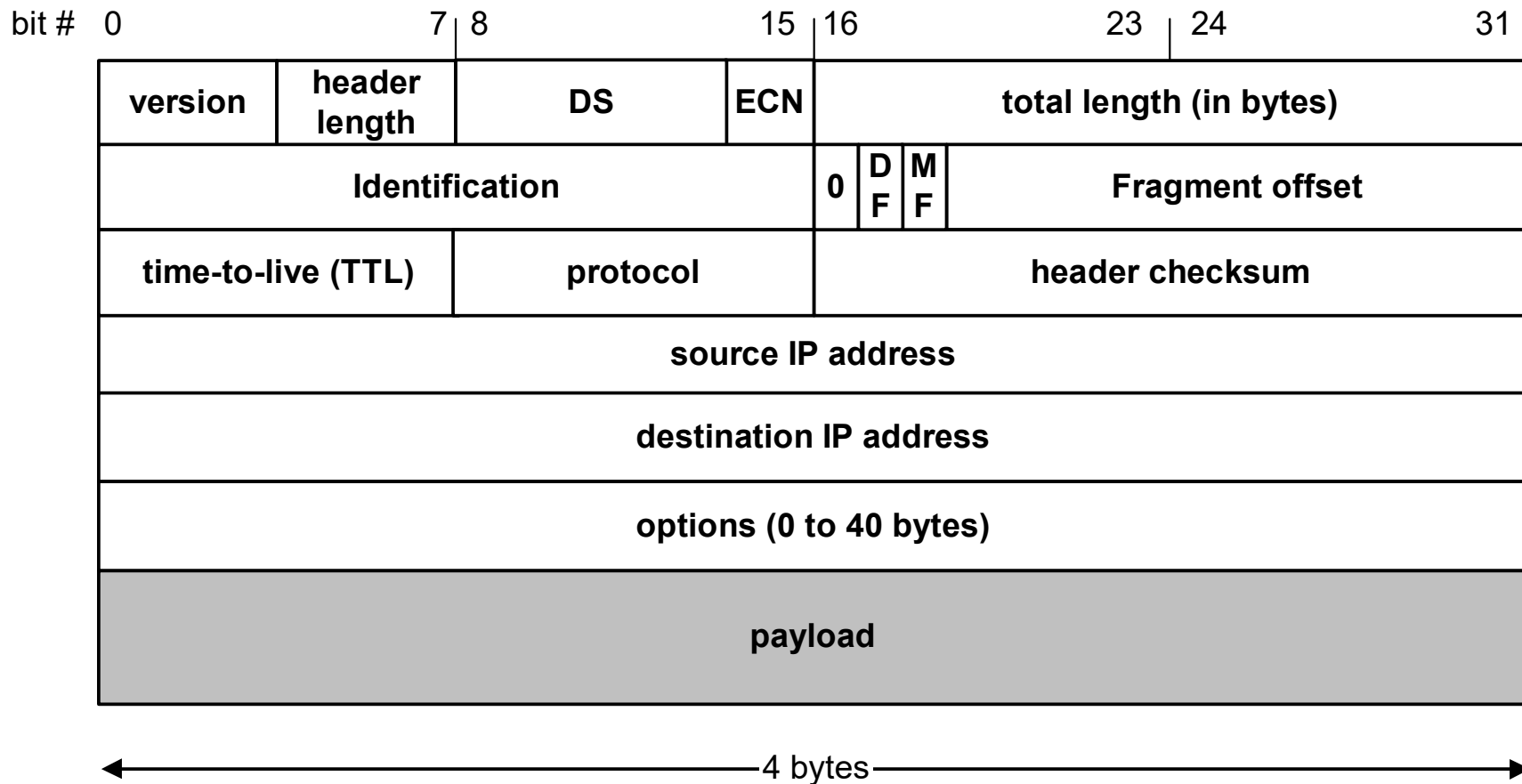
Tips for Troubleshooting LXC

- Man pages: 'lxc', 'lxc-container.conf'
- LXC commands: Type 'lxc' and press 'tab' key twice
- Each 'lxc-*' command has a man page
- Configuration files (for Debian):
 - /etc/default/lxc
 - /etc/default/lxc-net
 - /etc/lxc/default.conf
 - /etc/lxc/lxc-usernet

Troubleshooting Network Issues

- Use 'ping' command to check if a packet can reach from host to the given destination
 - E.g. 'ping google.com'
- Use 'ip' command to query and configure network devices ('man ip')
 - Show all network devices: 'ip link'
 - Show all network routes: 'ip route'
- Use 'iptables' command to query and configure rules for network filtering ('man iptables')
 - List rules for 'nat' table: 'iptables -L -n -d nat'
 - List rules for 'filter' table: 'iptables -L -n'

Networking Review – IP Datagram



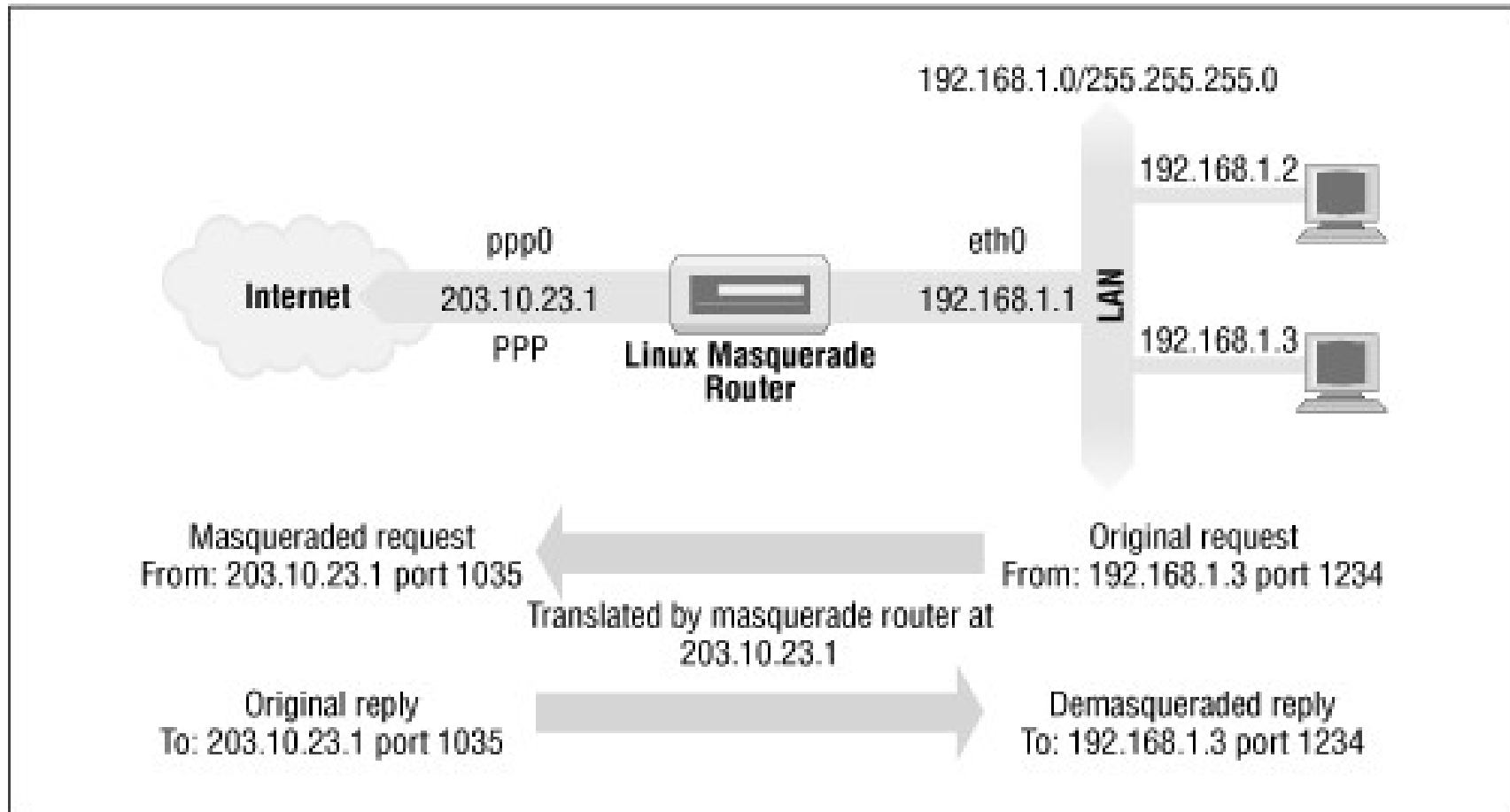
Networking Review – Private IP

- Address ranges reserved by IANA for private use (not publicly routable)
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- Devices with a private IP cannot send/receive datagrams directly to devices with a public IP
 - Network Address Translation solves this

Networking Review - NAT

- Network Address Translation (NAT)
 - Modifying source/destination addresses in a datagram while in transit
- Masquerading – type of NAT
 - Modifying all datagrams on a private network
 - By router that connects internal private network to public network
 - Change source IP to that of router (public)
 - Track replies (destination is now router IP)
 - Change destination IP back to private IP

Networking Review - Masquerading



Source: *Linux Network Administrator's Guide, 2nd Edition* by Olaf Kirch & Terry Dawson; Orielly

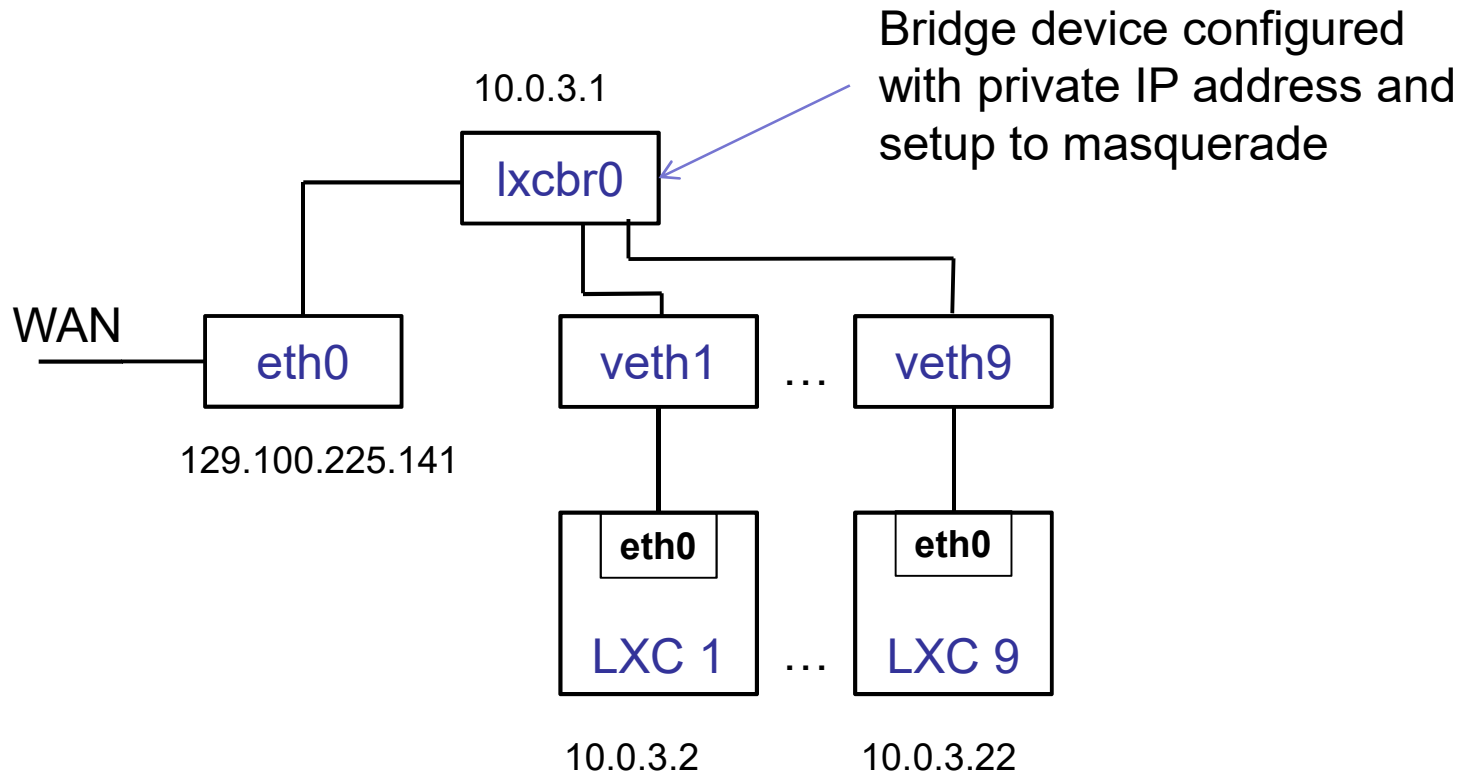
Port Forwarding

- NAT cannot handle datagrams originating from internet to private IP addresses
 - E.g. request for a web server
- Port forwarding helps mitigate this
 - Requests to a particular port on the router gets forwarded to an internal IP+port
 - E.g. datagram with destination 129.100.225.141:8080 gets forwarded to 192.168.1.5:80 which has the actual web server

IP Masquerading in Software

- Linux provides IP packet manipulation
 - Kernel space: "netfilter" module
 - User space: "iptables"
 - Used by most home routers
- Use "**iptables**" command to manipulate rules for packet filtering and manipulation
- E.g. "**iptables -L -t nat**" shows all rules in 'nat' table

LXC Networking Setup



Setting Up LXC – Overview

1. Use a kernel version that supports LXC
2. Install LXC tools and dependencies
3. Setup networking configuration
4. Setup subuid/subgid for unprivileged containers
5. Setup a template for containers
6. Create container
7. Start container
8. Attach a terminal to running container

Container Locations

- Privileged containers
 - /var/lib/lxc and /var/lib/lxcfs
- Unprivileged containers
 - /etc/lxc/lxc.conf => ~/.config/lxc/lxc.conf
 - /etc/lxc/default.conf => ~/.config/lxc/default.conf
 - /var/lib/lxc => ~/.local/share/lxc
 - /var/cache/lxc => ~/.cache/lxc

Referenes

- Debian LXC guides
 - <https://wiki.debian.org/LXC>
 - wiki.debian.org/LXC/SimpleBridge
 - wiki.debian.org/LXC/MasqueradedBridge
- Orielly Linux Network Admin guide
 - <http://www.oreilly.com/openbook/linag2/book/ch11.html>
- Stéphane Graber's articles on LXC
 - <https://www.stgraber.org/2013/12/20/lxc-1-0-blog-post-series/>