Welcome @ XTG

XTG
XPERT TRAINING GROUP

Wij trainen met plezier. En dàt merkt u!

Welkom !

- Xpert in virtualization technology, knowledge Center for virtualization: VMware, Citrix, Linux...
- Biggest independent VMware Authorized Training Centre (VATC) in Benelux
- LPI and Gurulabs training center

Introduction

Frederik Vos

- Almost 6 years senior technical trainer @ XTG
- VMware Certified Instructor

  o.a. ICM, FastTrack, Optimize & Scale
- Citrix Certified Instructor

  XenServer, Netscaler & Provisioning Server
- LPI Certified Instructor & Open Source Specialist

  LPI 1, 2 and 3 certified, Linux & Solaris background
  Novell Certified Linux Administrator

Agenda

- Your network...
- Network utilities
- Network configuration: Ubuntu Server
- Network configuration: Ubuntu Desktop
- Network monitoring
- Firewall (optional)

Goal

- Identify network
- Basic troubleshooting
- Monitoring network
- Firewall setup

Your network....

Your network

- More and more complex, even in home environments
- More different devices: routers from internet providers, wireless routers, mobile devices, Ethernet over Power
- Virtual Environments: even with solutions like VirtualBox

Points of interests

- IP adress
- DHCP
  - DHCP out-of-the-box
  - One dhcp server
- DNS
- Next-Hop

Your network: addressing

- 10.0.0.0/8 (255.0.0.0)
- 172.16.0.0/12 (255.240.0.0)
- 192.168.0.0/16 (255.255.0.0)

Network utilities

Netwerk interfaces

- Network cards: eth*X*
- Wireless cards: eth*X* or wlan*X*
- Other other possibilities:
  - Motherboard embedded network interfaces: em*X*
  - PCI addon interfaces: p<slot number>p<port number> Example: p3p1
- Other interfaces: tunnels, bridges and bonds

Identify Network interfaces

- ls /sys/class/net
- cat /sys/class/net/eth0/device/vendor
  cat /sys/class/net/eth0/device/device
  → http://www.pcidatabase.com
- udevadm info --query=all
  --path=/sys/class/net/eth0
- lspci

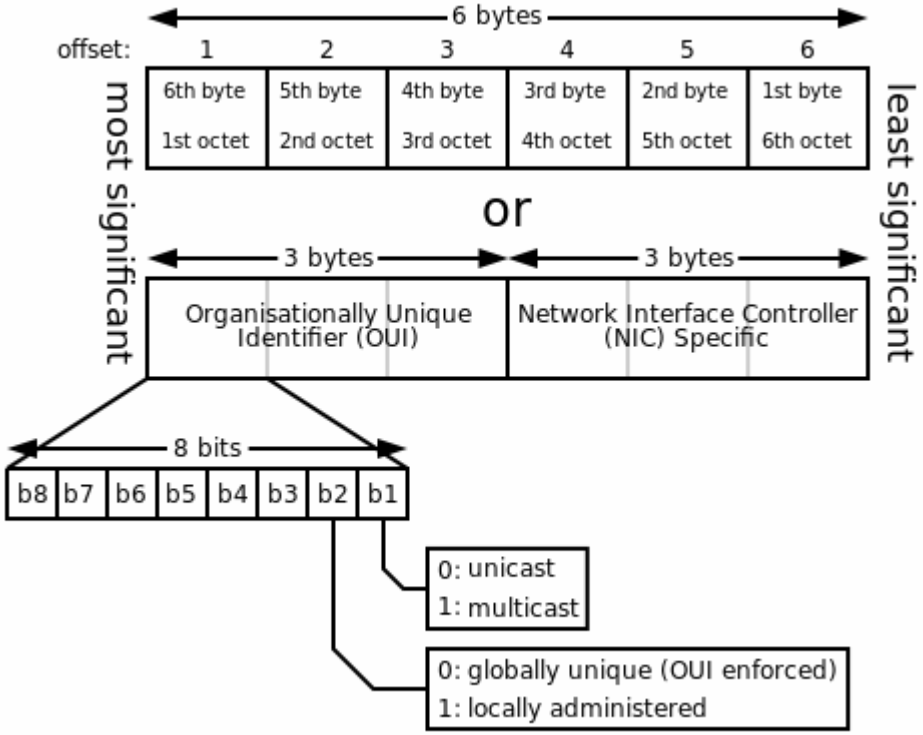
Iproute2

- ifconfig, route, arp, netstat etc. are deprecated
- New set of commands: ip, ss, rtmon, tc, lnstat
- Identification, monitoring, troubleshoot, **non-persistent** configuration
- TIP: use zsh grml for auto-completion

Layer 1: physical device

- ethtool -s eth0 speed 100 duplex full
- ethtool -s eth0 speed 100 duplex full autoneg on
- ethtool -S eth0
- lot of other possibilities: support for hardware features, like wake-on-lan, ring-parameters..

Layer 1: mac address



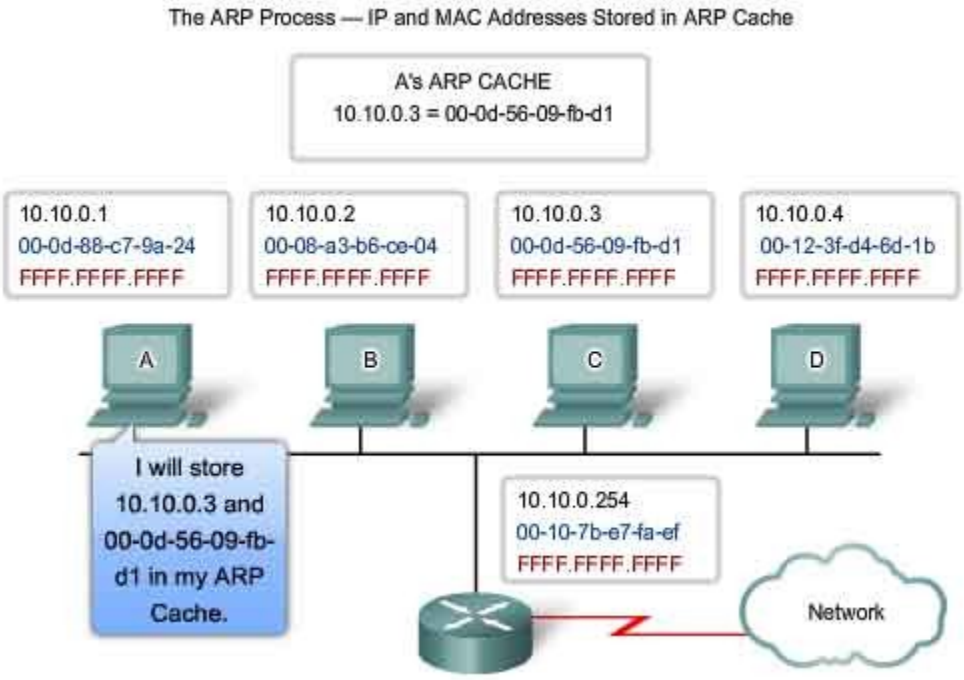
Layer 1: link status

- ip link show
- ip link show dev eth0
- ip link set dev eth0 up | down
- ip link set dev eth0 mtu ...
- ip monitor all

Layer 1: wireless

- Discovery:
  - iwlist, iwgetid
- Monitoring:
  - iwspy, iwevent
- Configuration:
  - iwconfig, iwpriv, iwrename

Layer 2: arp

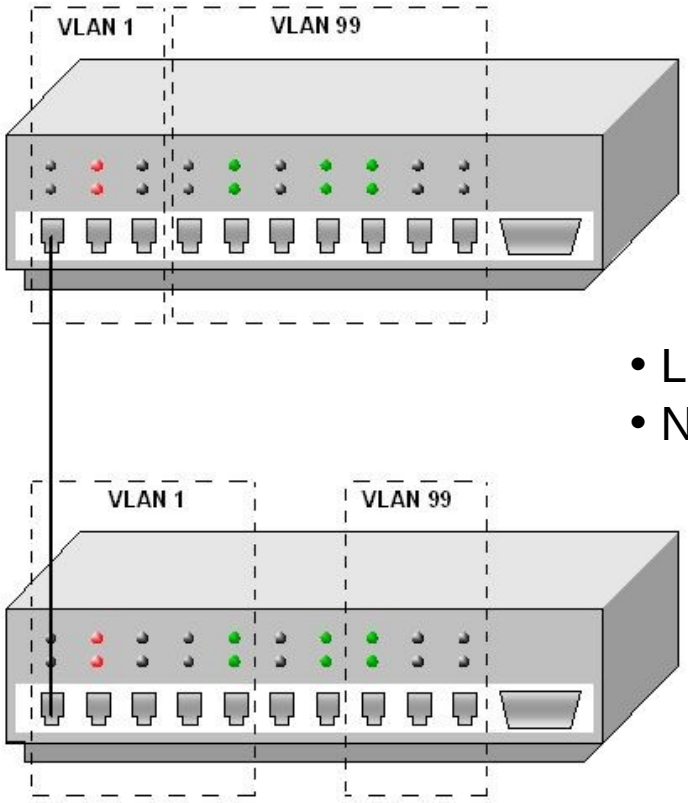


arp: convert ip address into hardware address

Layer 2: arp table

- ip neigh show
- ip neigh show dev eth0
- ip neigh flush

Layer 2: VLAN



- Logical networks
- Network isolation

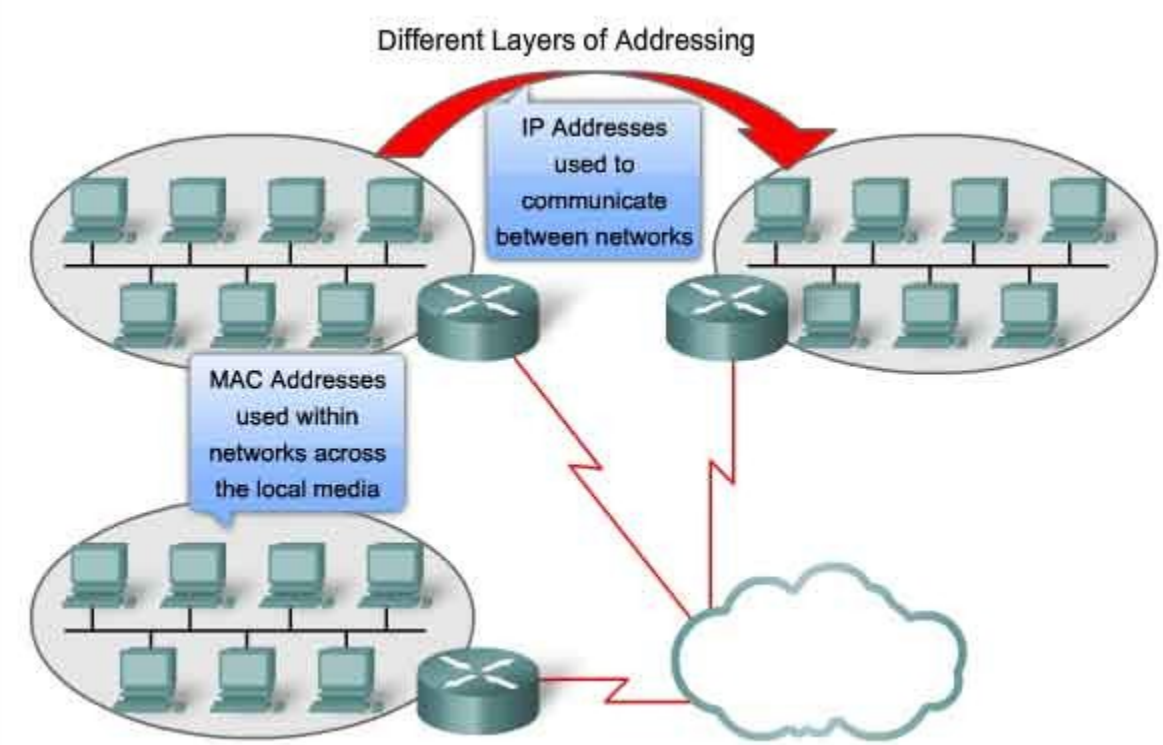
Layer 2: VLAN configuration

- Configure VLAN ID:
  - ip link add link eth0 name eth0.10 type vlan id 10
  - ip link set dev eth0.10 up
- Remove VLAN ID:
  - ip link set dev eth0.10 down
  - ip link delete dev eth0.10
- Show configuration:
  - ip link show dev eth0.10

Layer 3: IP address

- ip addr show
- ip addr show dev eth0
- ip addr add 192.168.1.1/24 dev eth0
- ip addr add 192.168.1.1/24 label eth0.test dev eth0
- ip addr show label eth0.test

Layer 3: IP communication



Layer 3: Route

- ip route show
- ip route show dev eth0
- ip route add 0/0 via 192.168.1.1 dev eth0
- ip route del 0/0 via 192.168.1.1 dev eth0

Layer 4: open ports

- ss = show socket
- ss -nl
- ss -A inet | tcp | udp
- ss -o state established '(dport = :ssh or sport = :ssh)'

Troubleshooting

- ping
- traceroute / tracepath
- mtr
- tcpdump
- wireshark
- firewall: iptables -n --list

tcpdump

- tcpdump 192.168.1.180
- tcpdump src 192.168.1.180 and dst 192.168.1.1
- tcpdump host 192.168.1.180 and port 21
- tcpdump host 192.168.1.180 and not port 21
- tcpdump dst 192.168.0.2 and src net 172.16.0.0/16 and not ssh
- tcpdump -c2 icmp

DNS

- hostname ...
- hostname --long
- cat /etc/resolv.conf
- host www.google.com
- dig @dns host -t type

Ubuntu Server

Persistent configuration

- ip, gateway, dns configuration: /etc/network/interfaces
- hostname: /etc/hostname
- /etc/hosts

/etc/network/interfaces: static

```
auto eth0
iface eth0 inet static
network 192.168.0.0
address 192.168.1.1
netmask 255.255.255.0
broadcast 192.168.0.255
gateway 192.168.1.2
dns-nameservers 8.8.4.4*
dns-search example.org
```

*) install resolvconf

/etc/network/interface: dhcp

auto eth0

iface eth0 inet dhcp

TIP: remove /etc/hostname
(receive hostname via dhcp)

Activate interface

- restart networking
- ifup | ifdown eth0*

*) install ifplugd

hostname & /etc/hosts

- /etc/hostname
- /etc/hosts:

```
127.0.0.1 localhost.localdomain localhost
127.0.1.1 fqdn-long shortname
```

Ubuntu desktop

Differences with Ubuntu Server

- networkmanager
- dnsmasq

Network Manager

- Easy configuration
- Ethernet and wireless cards
- Plugins, e.g. VPN
- Policykit
- Customize with hooks

Disable NetworkManager

- /etc/NetworkManager/NetworkManager.conf
  →
  [ifupdown]
  managed=true

DNSMASQ-BASE

- Faster browsing
- VPN
- Handling dns failures

Disable dnsmasq-base

- No need to remove it, only if you want 'full dnsmasq' !
- Disable it, if you have your own dns server
- /etc/NetworkManager/NetworkManager.conf

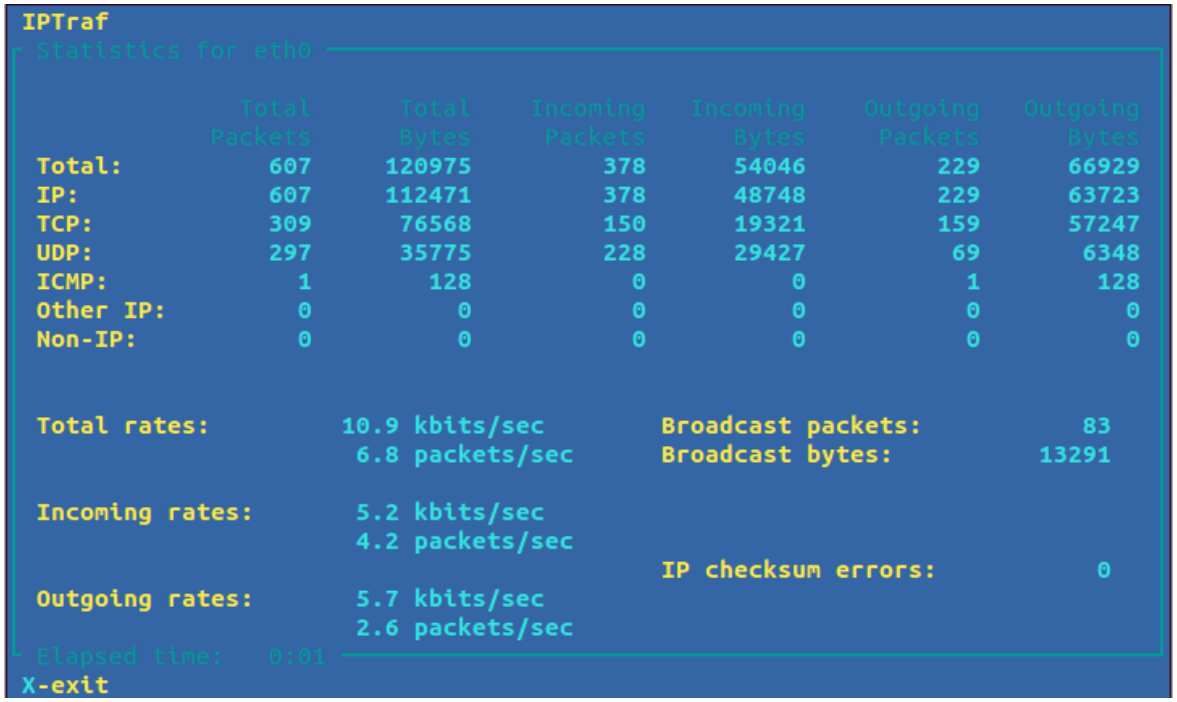
  → #dns=dnsmasq
- restart networkmanager

Network monitoring

iproute2 & ethtool

- nstat
- ss -n
- ethtool -S
- ip monitor

iptraf


IPTraf
Statistics for eth0
Total Packets
Total Bytes
Incoming Packets
Incoming Bytes
Outgoing Packets
Outgoing Bytes
Total: 607 120975 378 54046 229 66929
IP: 607 112471 378 48748 229 63723
TCP: 309 76568 150 19321 159 57247
UDP: 297 35775 228 29427 69 6348
ICMP: 1 128 0 0 1 128
Other IP: 0 0 0 0 0 0
Non-IP: 0 0 0 0 0 0
Total rates: 10.9 kbits/sec
6.8 packets/sec
Broadcast packets: 83
Broadcast bytes: 13291
Incoming rates: 5.2 kbits/sec
4.2 packets/sec
IP checksum errors: 0
Outgoing rates: 5.7 kbits/sec
2.6 packets/sec
Elapsed time: 0:01
X-exit

iftop

```
             1.91Mb          3.81Mb          5.72Mb          7.63Mb    9.54Mb
└──────────────┴───────────────┴───────────────┴───────────────┴─────────┘
xd-productie-07.xtg.local   => papeda.canonical.com          0b    3.29kb  2.46kb
                            <=                             0b     101kb  91.6kb
xd-productie-07.xtg.local   => viewcs01.xtg.local       6.81kb    5.18kb  5.17kb
                            <=                          15.8kb    17.8kb  9.40kb
192.168.0.255               => pc-melanie.xtg.local        0b       0b     0b
                            <=                           936b     749b    397b
255.255.255.255             => 192.168.0.63                0b       0b     0b
                            <=                          1.25kb    256b     80b
xd-productie-07.xtg.local   => inside-fw1.xtg.local      284b      57b    490b
                            <=                           484b      97b   1.09kb
192.168.0.255               => 192.168.0.63                0b       0b     0b
                            <=                           640b     128b     40b
xd-productie-07.xtg.local   => 224.0.0.251               568b     114b    358b
                            <=                             0b       0b     0b
xd-productie-07.xtg.local   => 4.27.28.254                 0b      42b    593b
                            <=                             0b      42b   19.3kb
255.255.255.255             => 192.168.0.200               0b       0b     0b
                            <=                             0b      61b     57b
─────────────────────────────────────────────────────────────────────────────
TX:             cum:   56.2kB   peak:   50.2kb  rates:   7.64kb  8.68kb  14.1kb
RX:                    1.31MB           2.45Mb           19.1kb   121kb   334kb
TOTAL:                 1.36MB           2.50Mb           26.7kb   129kb   348kb
```

Firewall

UFW

- Easy configuration
  - command-line
  - gufw
- Basic firewall → @home solution

Basic configuration (1)

- ufw enable | disable
- ufw status

Basic configuration (2)

- ufw app list
- ufw allow OpenSSH
- ufw allow 25/tcp
- ufw allow from 10.0.0.0/8
- ufw allow in on eth0 to any port 80 proto tcp
- ufw allow proto tcp from any to any port 22
- ufw allow from 192.168.0.0/16 to any app OpenSSH

NAT

- Network Address Translation: private ip address → public
- S(ource) NAT / Masquerading

NAT router

- /etc/default/ufw → DEFAULT_FORWARD_POLICY="ACCEPT"
- /etc/ufw/sysctl.conf → net.ipv4.ip_forward=1
- /etc/ufw/before.rules →

```
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 192.168.1.0/24 -o eth0
-j MASQUERADE

COMMIT
```

The other way around

- Home usage:
  - ip route add
- Advanced:
  - portforwarding in /etc/ufw/before.rules

Vragen ?