Debian/GNU Linux Networking

Basics of the Networking

Károly Erdei

5. November 2008

Agenda

Agenda

Computer Networks
Transmission Principles

Broadcasting networks

- transmission medium shared by all network participants (hosts)
- one machine sends short messages (packet)
- Broadcasting: all other machines receive the package sent
- Example: Radio, television, GSM, Ethernet

Point-to-point networks

- Multiple connections between individual pairs of machines
- Message from one machine to another
- Message must be routed from source to destination
- Example: Telephone system, Internet

Range of Networks

Ranges

- LAN - Local Area Network: Room (10 m), building (100 m), campus (1000 m)
- MAN - Metropolitan Area Network: City (10 km) Metronet-Hgb
- WAN - Wide Area Network: Country (100 km), continent (1000 km)
- Internetwork - Combination or network of networks: Planet (10K km)
- PAN - Personal Area Networks 1-10 m, (using Bluetooth units)

LAN

- Private network within building or complex of buildings
- Connection based on cables (hosts are attached via network cards)
- Transmission speed 0.1–1 Gbps
- Various topologies: Bus-based (Ethernet), Wireless (WLAN)

Range of Networks

Internetwork

Internetwork:

- Connects multiple WANs/LANs across the globe
- LANs/WANs connected to Internetworks by routers or gateways
- Each attached network may have different protocol
  - Protocol = language spoken by computers on network
- Any computer in any network can communicate with any other computer in any other network independently of physical network technologies
- Communication based on higher level protocols

Agenda

The Internet

The Internet

- A worldwide internetwork that uses the TCP/IP protocol suite
- It is a packet switching network (data will be splitted in packets)

Various groups of networks

- Backbones: large networks for connecting other networks (GEANT2)
- Regional networks: e.g. connecting universities (ACOnet)
- Commercial networks: privately owned for paying users (LIWEST)

Lot of services

- Application level: World Wide Web, eMail, file transfer, remote login
- Network level: connectionless packet delivery (UDP), reliable stream transport (TCP)

History of the Internet

From The Beginnings till Today

- Late 60s: numerous networks based on different technologies
- Early 70s: DARPA (US Defense Advanced Research Proj. Agency)
  - 1978: TCP/IP in its current form
  - 1983: ARPANET is the backbone of the Internet (research sites)
- 1983: TCP/IP for the operating system BSD Unix
  - Berkeley Software Distribution (University of California at Berkeley)
  - TCP/IP spreads among universities and research centers
- 1986: NSFNET - connection with ARPANET and EBONE (Europe)
- 1993: World Wide Web, Service on top of the Internet
- 1995: Commercialization of the Internet
- 2000: Internet as a universal medium (Internet Access trough ISPs)

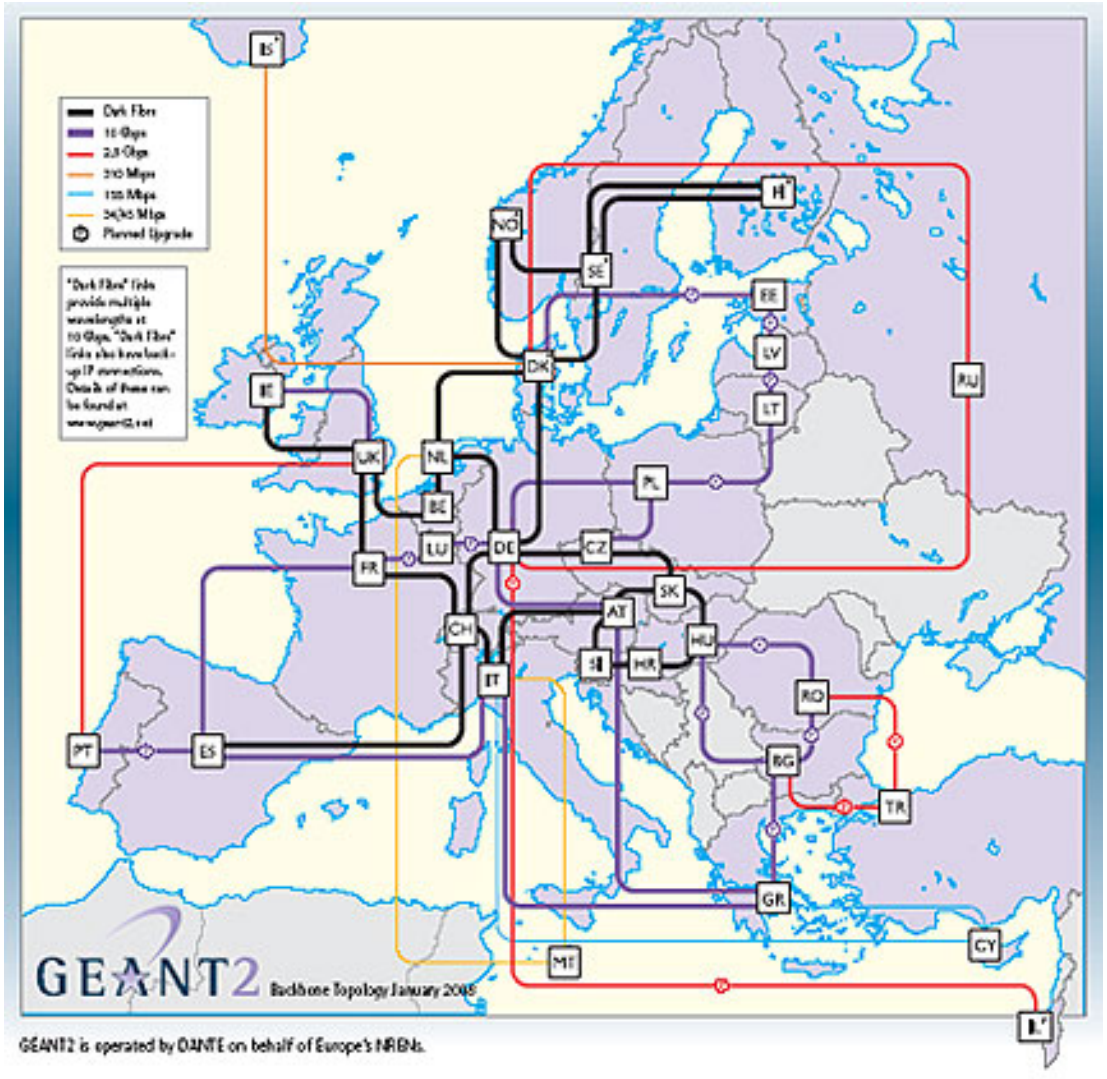
Today the Internet is a collection of commercial networks

Organisation of the Internet

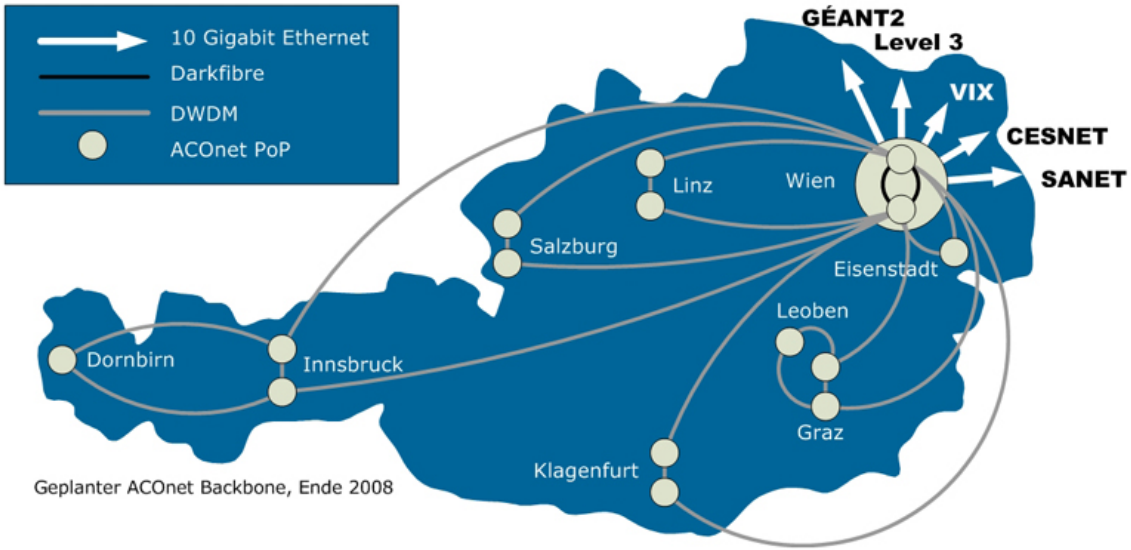
Internet Architecture Board (IAB)

- Internet Engineering Task Force (IETF)
  - Decisions about protocols, procedures, conventions
- Request for Comments (RFCs)
  - Series of reports that defines the (history of) Internet protocols
- Internet Standards
  - Defines the official Internet protocols
  - References the RFCs that define a current standard
  - Update of standards: other RFCs will be referenced
- Examples of Internet Standards:
  - IP - Internet Protocol: STD 5
  - TCP - Transmission Control Protocol: STD 7
  - DNS - Domain Name System: STD 13
  - SMTP - Simple Mail Transfer Protocol: STD 10

GEANT2 - Pan-European Education/Research Network



ACOnet - Austrian Academic Computer Network



Agenda

Ethernet

The communications medium

Ethernet

- is a family of frame-based computer networking technologies for local area networks (LANs)
  - a data packet on the wire is called a frame
- defines a number of wiring and signaling standards for the Physical Layer (OSI model)
- uses the Media Access Control (MAC) address to identify nodes
- allows communication of computers over a shared coaxial cable acting as a broadcast transmission medium
- all generations of Ethernet share the same frame formats
  - the same interface for higher layers
  - and can be readily interconnected

Ethernet

MAC addresses

MAC / physical / hardware Address

- each Ethernet station is given a single 48-bit unique MAC address
- is used both to specify the destination and the source of each data packet
- is six groups of two hexadecimal digits, separated by - or :
  - first three octets identify the organization
  - arbitrary but unique next three octets assigned by the organisation
- is used/valid only in LAN (network segment)

technologies which use MAC address

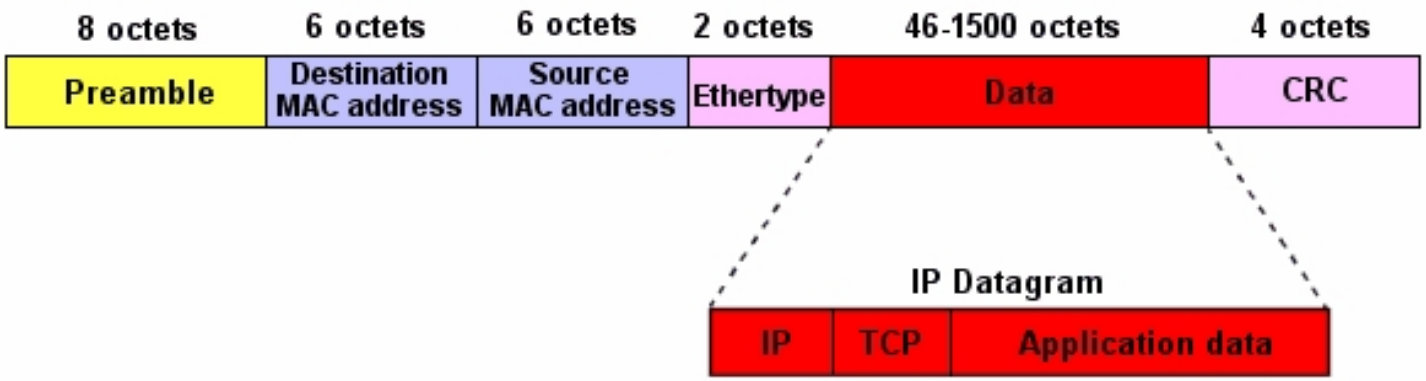
- Ethernet, 802.11 wireless networks, Bluetooth

Special MAC addresses:

- broadcast address: ff:ff:ff:ff:ff:ff
  - packets sent to this address are received by all stations on the local network

Ethernet

The frame structure



Ethernet - MAC address

How to find a local MAC addresses

Linux - command line with /sbin/ifconfig

```
uhu:~> /sbin/ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:16:41:16:6D:5D
          inet addr:192.168.1.115  Bcast:192.168.1.255  Mask:255.255.25
 ....
uhu:~> /sbin/ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:16:6F:BA:3E:01
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
 ....
```

MS Windows - fastest way

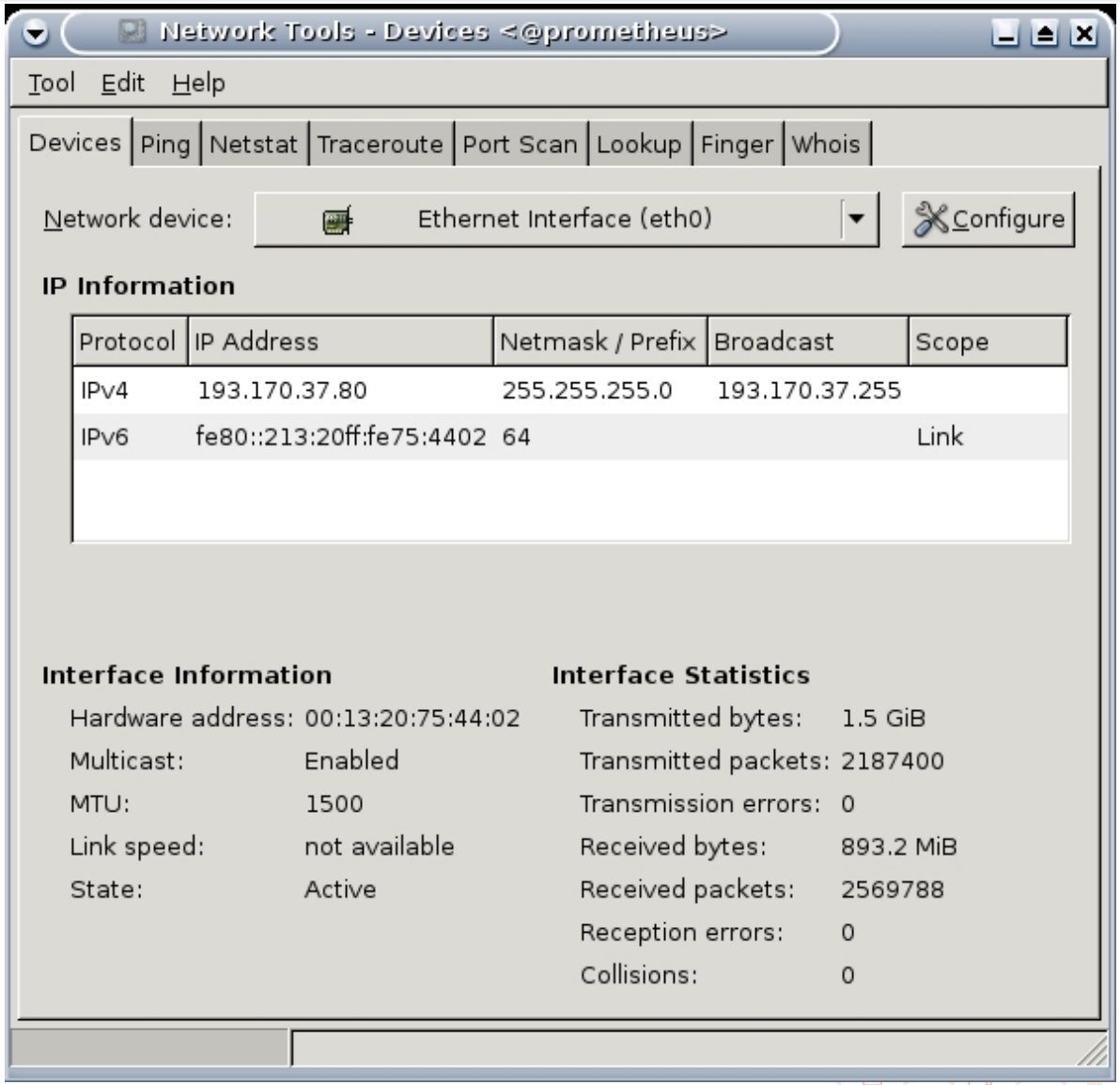
- in DOS Window by means of ipconfig /all

Linux - all units in the network segment

- arp -a (only one line listed as example):
  - crutch.risc.uni-linz.ac.at (193.170.37.76) at 00:16:35:37:5C:EC [ether] on eth0

Ethernet - MAC address

How to find a local MAC addresses - Linux with gnome-nettool



Agenda

Internet Protocols

Connectionless and Connection-oriented protocols

Connectionless protocol

- communication between two network point in which message can be sent without prior arrangement
- the transmitting device sending the message:
  - does not ensures first recipient is available and ready to receive data
  - simply sends the message to the recipient address
- often problems with transmission
- examples: IP, UDP, ICMP, IPX

Connection-oriented protocol

- delivers a stream of data in the same order as it was sent
  - first a communication section will be established
  - data stream will be send by handshaking
  - packet retransmission by error, data lost, etc.
- examples: TCP
  - phone call: user must dial first and get answer before transmitting data

IP - The Internet Protocol

Features of IP

- A standard protocol (STD 5)
  - Includes ICMP - Internet Control Message Protocol (used by `ping`)
- No delivery guarantuees
  - Connection-less
  - Unreliable: packets may be lost, duplicated, reordered
  - Best-effort: however, we do our best to deliver a packet
  - packets oriented
- Data from an upper layer protocol is encapsulated inside one or more packets
- IP can be used over a heterogeneous network
  - Ethernet, ATM, FDDI, Wi-Fi, token ring, etc.
- Core functionality
  - defines IP addresses und subnetting
  - defines routing in the network

IP Addressing

RFC 1166: Internet Numbers

- An IP address is a 32 bit unsigned integer
  - There exist $2^{32} \approx 4$ billion IP addresses
- Representation in dotted decimal notation
  - $X.X.X.X$; Each X is a decimal number, a byte of the address
- Example: 128.10.2.30: 10000000 00001010 00000010 0011110
- Each Internet host has (at least) one Internet address
- IP addresses are divided in classes: Class A, B, C
  - IP address splitted in network and host part (bytes:1/3;2/2;3/1)

Class	Lowest Address	Highest Address
A	1.0.0.0	126.0.0.0
B	128.1.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0

Reserved IP Addresses

Special addresses

Some addresses are reserved for special purposes

- net.0: the "network" address (not a particular host) 193.170.37.0
- default gateway: an address in this network: 193.170.37.1
- broadcast address: net.255
  - `B-net`.255.255: broadcast in class B network: 140.78.255.255
  - `C-net`.255: broadcast in class C network: 193.170.37.255
- 0.0.0.0: "this" host
- 127.0.0.1: loopback (not sent across network, for testing local IP setup)

The original IP class scheme became too unflexible

- For each physical network, an address range has to be allocated;
- The address range is badly utilized; not all IP is assigned to hosts

IP Subnets

Solution: IP subnetting

- Entire network appears as single IP network to the outside world
- Idea: host address -> subnet address: host address
- IP address: network address: subnet address: host address

Implementation by subnet masks

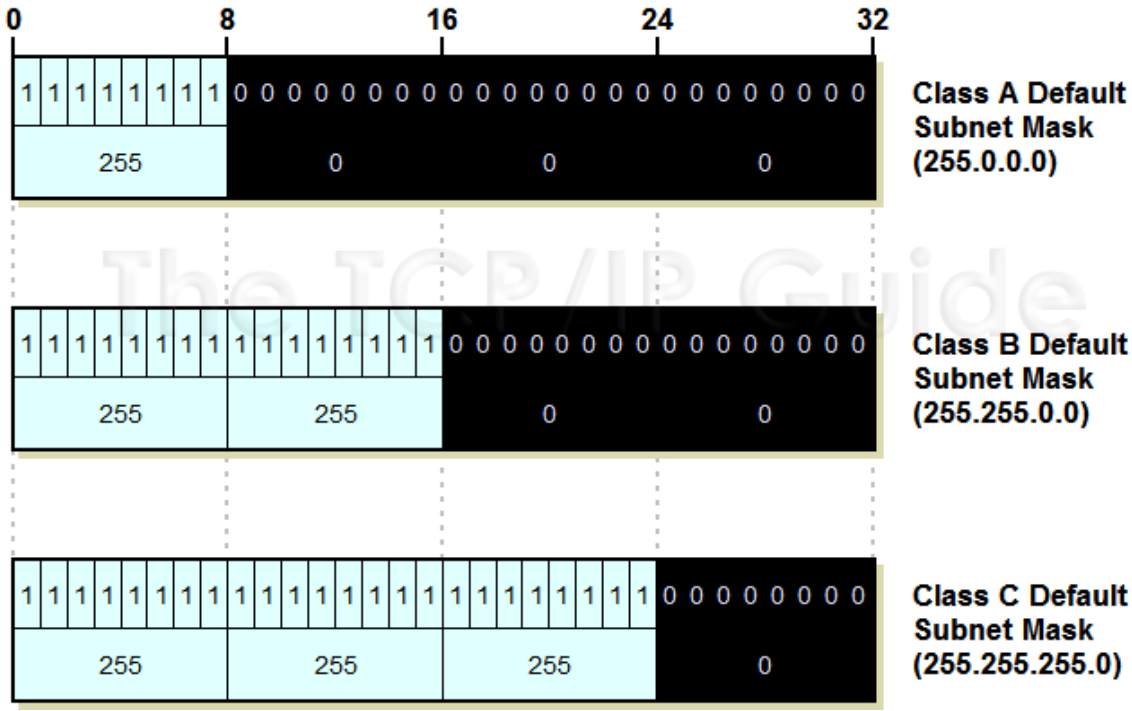
- For each subnet, a 32 bit subnet mask is chosen
  - Bit 1 in mask: corresponding bit in address is part of (sub)network address
  - Bit 0 in mask: corresponding bit in address is part of host address

Routers route today subnets with netmasks

- IP network classes are obsolete

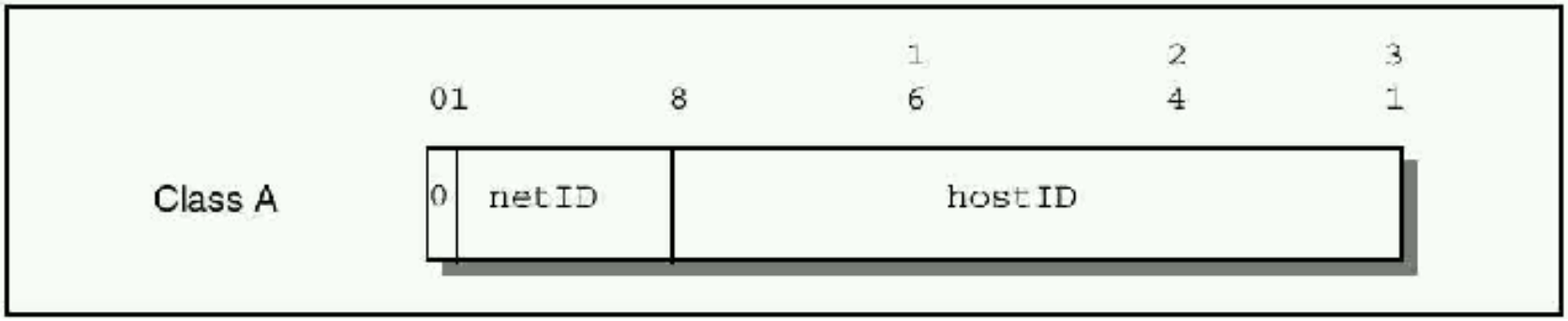
Default Subnet Mask

Graphical representation

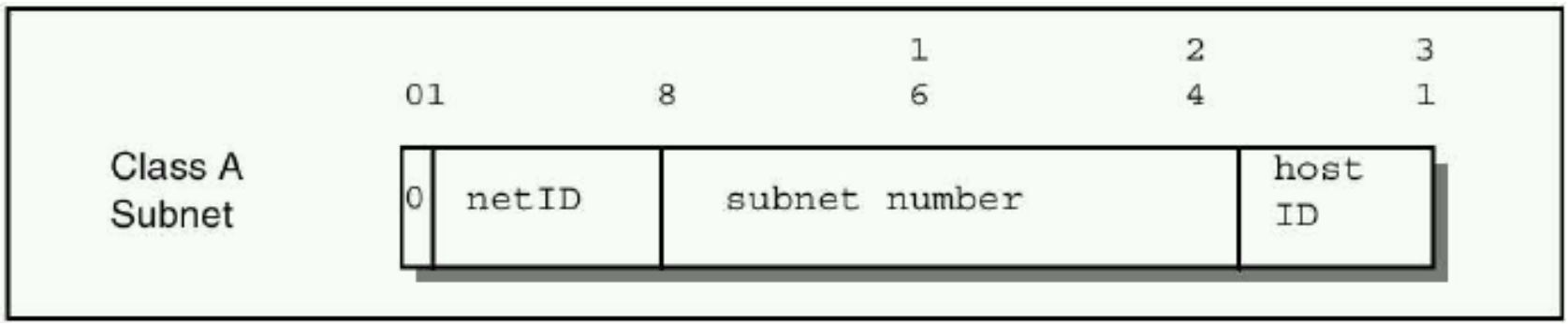


IP Addresses with Subnets

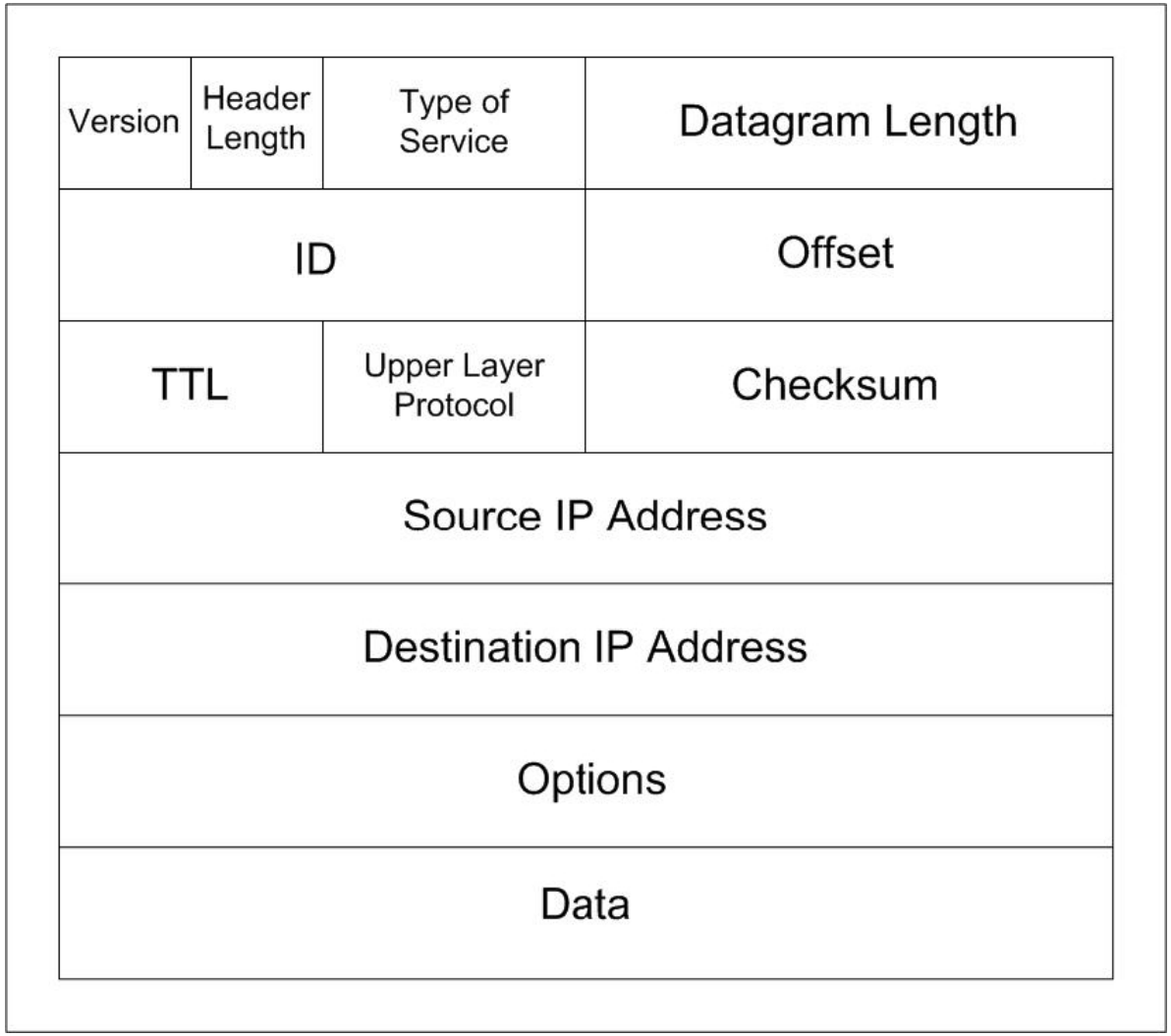
Without subnet:



With subnet:



IP Datagram Structure



Routers

Features

Router: a networking device

- a computer whose software and hardware are usually tailored to the tasks of routing and forwarding packets
- transfers packets only across networks using similar protocols
- contains a specialized operating system (e.g. Cisco's IOS)
- has multiple network connections
  - multiple physical networks are connected to a router
  - from the point of view of each network, the router is part of this network
- Types of routers
  - inside enterprises; enterprises and Internet; ISP - enterpise; SOHO: small office home office
  - small units (DSL router) - ISPs big multiprocessor unit

Node in a network that serves as access point to another network

Routers and Gateways

How they works

How Routing works

- IP packet routing based on routing tables
  - hard-coded static routes
  - by exchanging routing protocol information with other routers
- protocols
  - BGP - Border Gateway Protocol; eBGP
- Standard PC can act as a router with appropriate software

Gateway

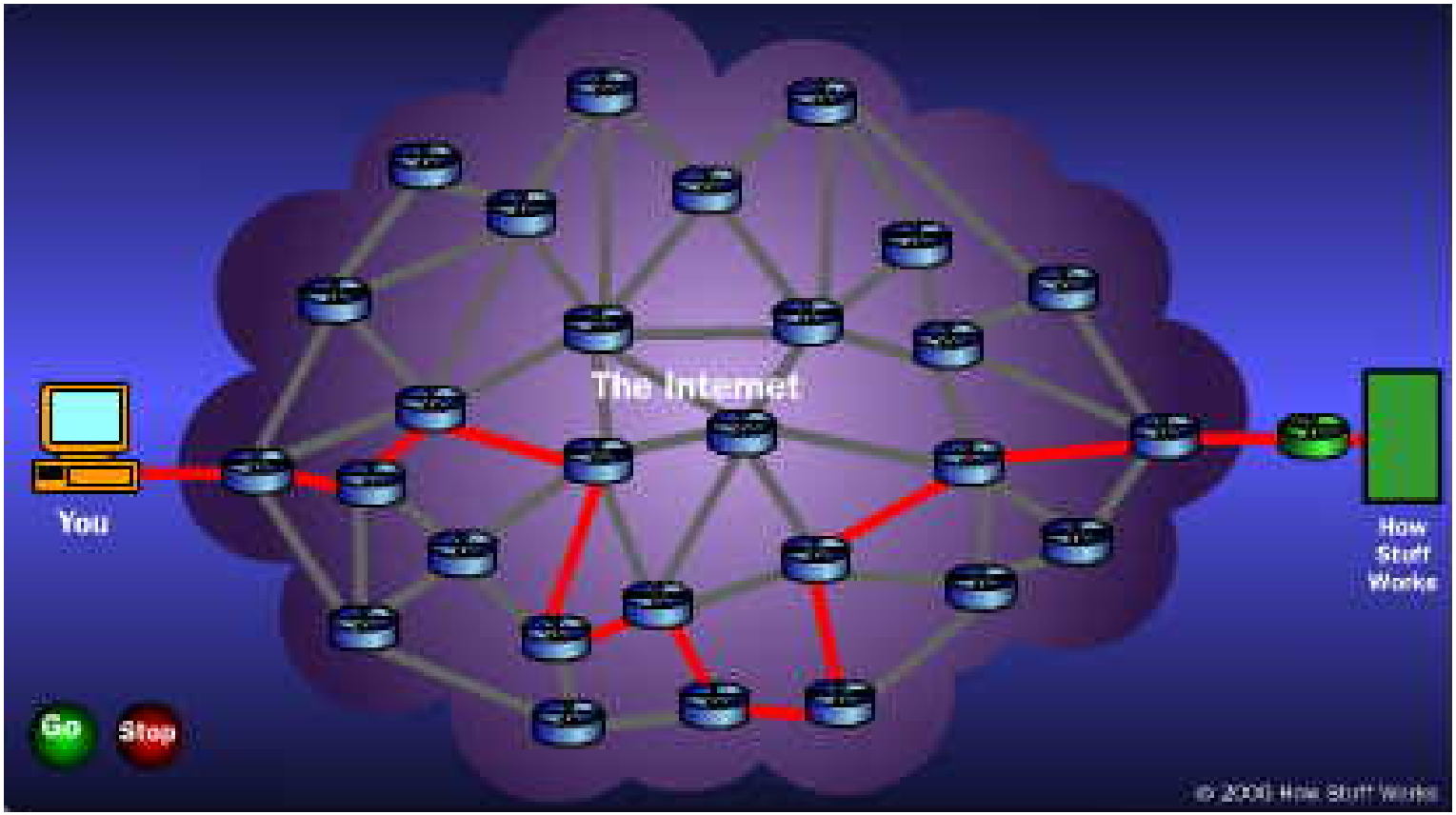
- a networking device that converts protocols among networks
- accepts a packet formatted for one protocol (AppleTalk) and converts it to a packet formatted to another protocol (TPC/IP)

Default gateway

- node in a network that is choosen when the IP address not in the routing table of the host

Routers, packets

A route of a packet in the Internet



Private Networks - Private IP Addresses

The addresses, which can be used by everyone

Private Internet Addresses

- RFC 1918: address allocation for private Internets
  - May be used internally in any organization
  - routers have to discard any packets with a private IP address in the IP header
  - gives security for private networks they are not available from the Internet

Examples

- private class A network: 10.0.0.0 - 10.255.255.255
  - Huge address range for communication within an organization
- Home network: 192.168.0.0 - 192.168.255.255
  - Cable/DSL router: 192.168.1.1

How to connect network with private addresses to the Internet?

Internet Protocol - ICMP based applications

Ping and Traceroute

ping

- simplest version: ping hostname

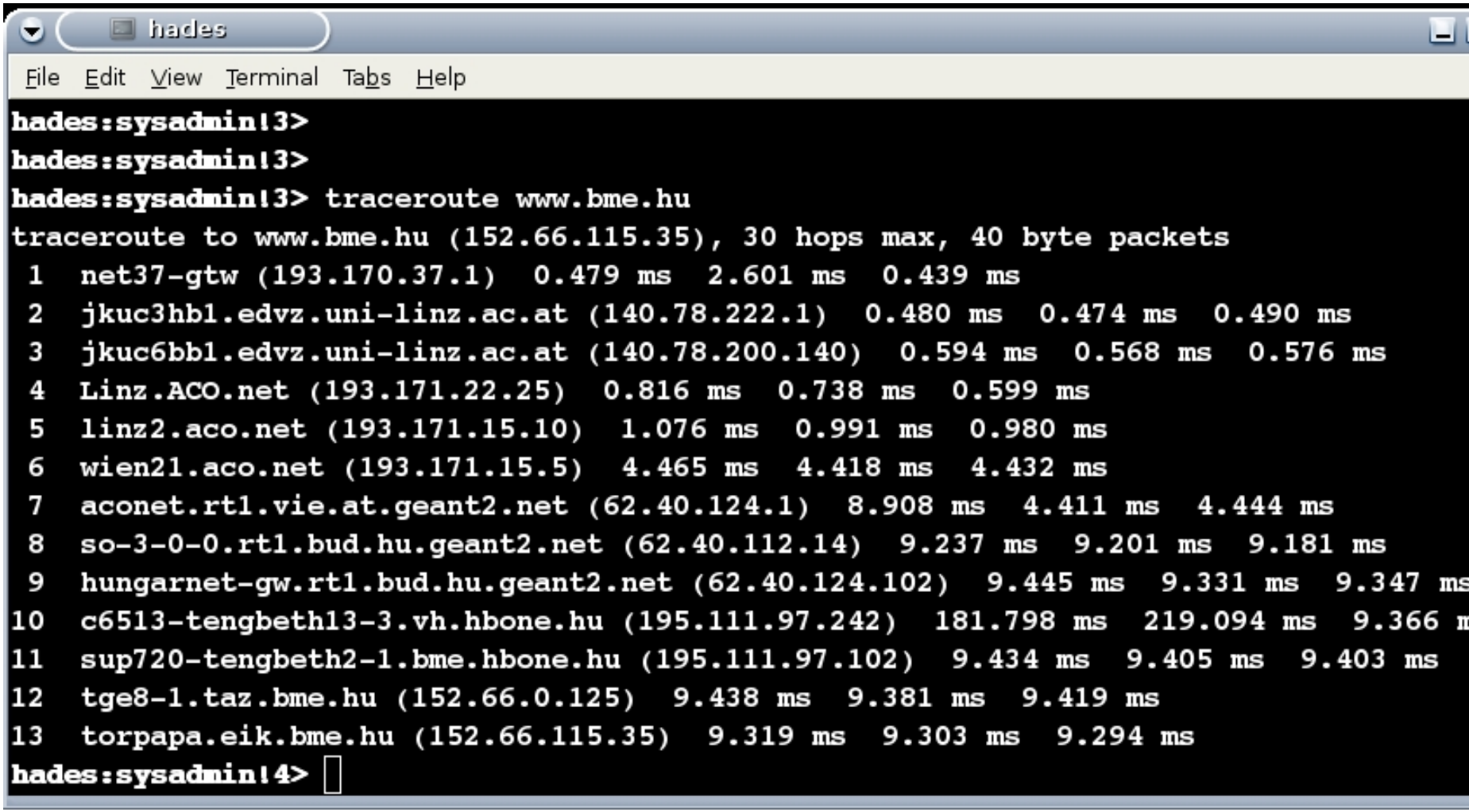
```
PING kernel.risc.uni-linz.ac.at (193.170.37.225) 56(84) bytes of da
64 bytes from kernel.risc.uni-linz.ac.at (193.170.37.225):
icmp_seq=1 ttl=245 time=25.0 ms
64 bytes from kernel.risc.uni-linz.ac.at (193.170.37.225):
icmp_seq=2 ttl=245 time=26.3 ms
--- kernel.risc.uni-linz.ac.at ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 25.021/25.705/26.389/0.684 ms
```

traceroute

- simplest version: traceroute hostname
- try it yourself this command

Internet Protocol - ICMP based applications

Traceroute



Agenda

OSI Model - TCP/IP Model

OSI: 7 layers – TCP/IP: 4 levels

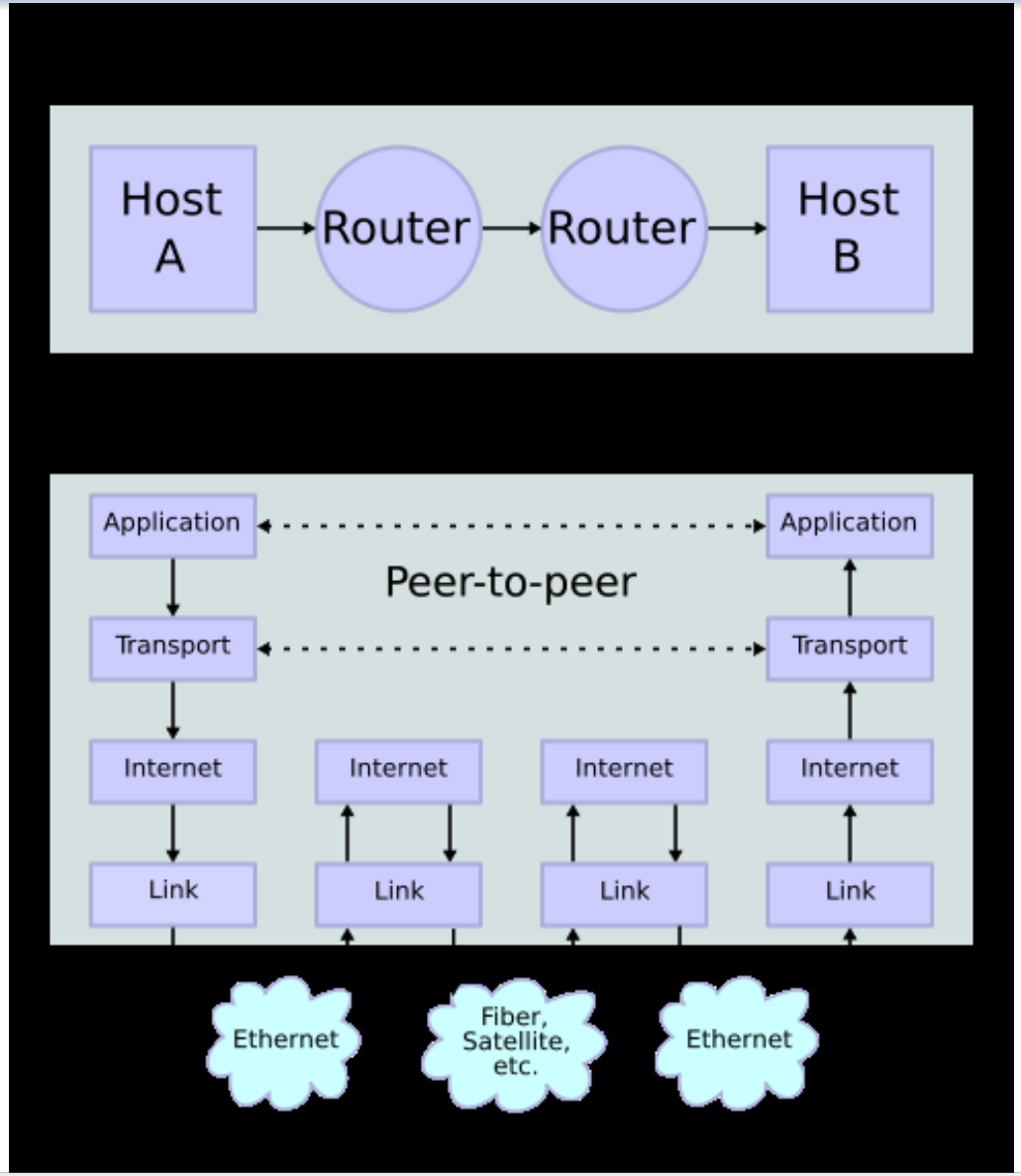
OSI - Open System Interconnect (general networking)

- 1: Physical Layer: sending raw bits
  - bit by bits delivery, how a bit as a signal looks like
- 2: Data Link Layer: transfers data between network nodes
  - Ethernet protocol; MAC address; local network delivery
- 3: Network Layer: transfer data packets from source to destination
  - via one or more networks using unique addresses and routing (IP - level)
- 4: Transport Layer: delivering data to the applications on hosts
  - forming data packets, adding source, destination ports (TCP, UDP)
- 7: Application Layer: running programs on host

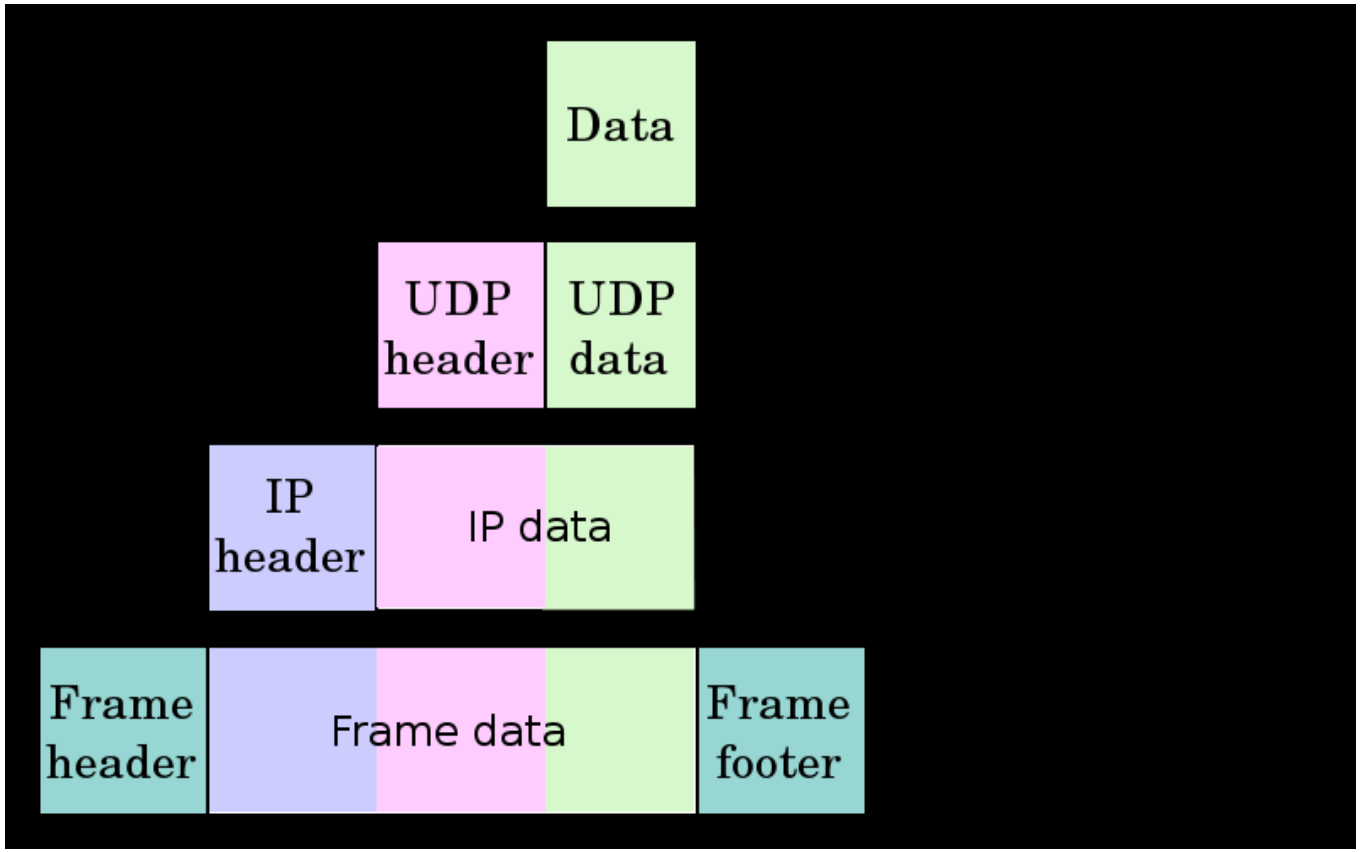
TCP/IP Model - 4 layers

- Link, Internet, Transport, Application Layers

TCP Model - packets route

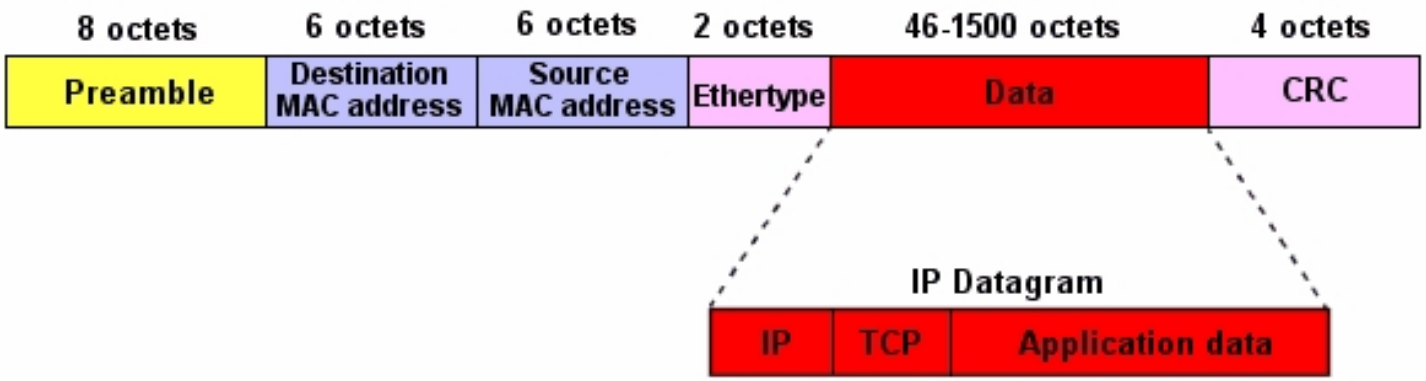


TCP Model - packets encapsulation



TCP Model - encapsulatioin

The Ethernet frame structure



Agenda

TCP - Transmission Control Protocol

Transport layer services

- Connection oriented
  - for data delivery first a connection must be established
- Same Order Delivery
  - data will arrive in the same order it has been sent
- Reliable data transmission
  - retransmit corrupted packages; error detection code, packet acknowledgement
- Byte orientation: not packages, but stream of byte sent
- Introducing the term port
  - port addresses multiple entities on the same location

TCP - Ports

The problem of the applications on a host to communicate

- more programs run on a computer
  - sendmail, webserver, name server, ftp-, pop server, etc.
- the computer has one unique IP address
- how to deal with the application, how to differ them
- introducing ports is the solution
  - analogy: postal address as IP address; appartement number or name is the port number

Ports

- to each services in the Internet/Computer a port is assigned
  - ports are identified by the port number
  - see in Linux the /etc/services file for numbers/services allocation
  - port number is a part of TCP packets header
- a program implement a service
  - the program LISTEN on the port for a communication

TCP - Ports

Unix port in /etc/services

```
ftp-data        20/tcp
ftp             21/tcp
ssh             22/tcp                          # SSH Remote Login Prot
telnet          23/tcp
smtp            25/tcp          mail
whois           43/tcp          nicname
domain          53/tcp                          # name-domain server
domain          53/udp
finger          79/tcp
www             80/tcp          http            # WorldWideWeb HTTP
www             80/udp                          # HyperText Transfer Pr
pop3            110/tcp         pop-3           # POP version 3
imap2           143/tcp         imap            # Interim Mail Access P
https           443/tcp                         # http protocol over TL
https           443/udp
ftps            990/tcp
telnets         992/tcp                         # Telnet over SSL
imaps           993/tcp                         # IMAP over SSL
pop3s           995/tcp                         # POP-3 over SSL
```

TCP - Transmission Control Protocol

Example: Sending email per smtp port (1)

```
hu:~> telnet bullfinch 25
Trying 193.170.37.222...
Connected to bullfinch.risc.uni-linz.ac.at.
Escape character is '^]'.
220 bullfinch.risc.uni-linz.ac.at ESMTP Sendmail 8.13.8/8.13.8/Debian-3
Mon, 3 Nov 2008 15:19:26 +0100; (No UCE/UBE) logging access from: i
uhu37.risc.uni-linz.ac.at(OK)-ke@uhu37.risc.uni-linz.ac.at [193.170.37.
helo ich-bin-s
250 bullfinch.risc.uni-linz.ac.at Hello ke@uhu37.risc.uni-linz.ac.at
[193.170.37.115], pleased to meet you
mail from: k.erdei@risc.uni-linz.ac.at
250 2.1.0 k.erdei@risc.uni-linz.ac.at... Sender ok
rcpt to: karoly.erdei@jku.at
250 2.1.5 karoly.erdei@jku.at... Recipient ok
```

TCP - Transmission Control Protocol

Example: Sending email per smtp port (2)

```
data
354 Enter mail, end with "." on a line by itself
this is an email sent by telnet 25 command from the laptop to the mail
server bullfinch.risc...  demonstrating how smtp works
.
250 2.0.0 mA3EJQr4014077 Message accepted for delivery
quit
221 2.0.0 bullfinch.risc.uni-linz.ac.at closing connection
Connection closed by foreign host.
uhu:~>
```

TCP - Transmission Control Protocol

Example: Downloading file from the WWW server

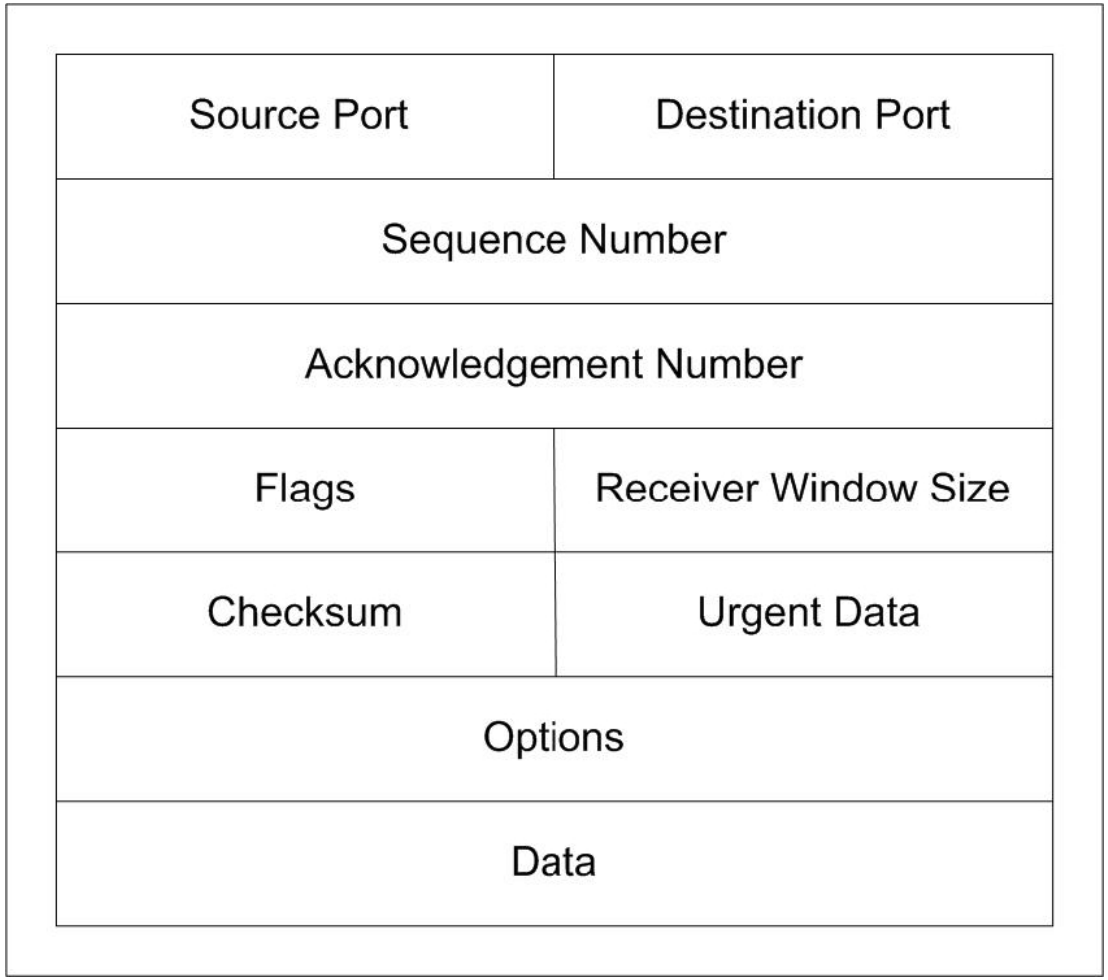
Telnet to port 80 on the Web server

```
hades:www!11> telnet www 80
Trying 193.170.37.138...
Connected to crow.risc.uni-linz.ac.at.
Escape character is '^]'.
GET http://www/proba.txt

Hello! This is a test file. To get it per port access with telnet.
It succeeded to get this file per port access from the web server.
Great!

Connection closed by foreign host.
hades:www!12>
```

TCP Datagram Structure



Agenda

UDP - User Datagramm Protocol

UDP what is it

- UDP is a minimal message-oriented Transport Layer protocol
- main features
  - unreliable; not ordered; lightweight; datagrams
  - urreliable: data may be lost, arrive duplicated, etc.
- comparing to TCP, which is:
  - reliable; ordered; heavyweight; streaming
- faster and more efficient as TCP for some application
- services using UDP:
  - DNS (Domain Name System); IPTV
  - VoIP (Voice over IP) - the internet telephony
- data structure
  - source port; destination port; length; checksum; data

DHCP - Dynamic Host Control Protocol

Client - Server application

DHCP protocol is used to obtain parameters necessary for IP networking

DHCP Client - Server communication flow

- client: broadcasts a DHCPDISCOVER request
  - Asks for a DHCP server on the network segment
  - Asks for a lease and for an IP address
  - Lease: the length of time for the allocation is valid
- server: sends a DHCPOFFER message
  - Checks if the MAC of client is registered
  - Marks an IP from the spool
- client: broadcasts a DHCPREQUEST on the network
  - The IP of the server is in the packet
- server: sends the client the data
  - Reservers the IP for the time of the lease
  - Other servers delete the mark for the IP

DHCP - Dynamic Host Control Protocol

DHCP server

- has a pool of IP addresses
- manages other network parameters for networking by client
  - options are widely configurable
- checks the MAC of the client, if configured
- lease time is configurable (max;min)

Client requests periodically

- Client has to request again before lease time is over
  - a new IP or request the same IP
- By booting must suspend other processes
  - without IP no network connection

DHCP - Dynamic Host Control Protocol

ct DHCP Server data table

Assigned data by DHCP server at RISC

- Network configurations parameter at RISC
  - IP Address
  - Lease
  - Domain Name (risc.uni-linz.ac.at)
  - Default Gateway address (193.170.38.1)
  - Name server IP address (193.170.37.225)
  - Name server IP address (193.170.37.224)
  - WINS servers (phoebe.risc.uni-linz.ac.at)
  - WINS servers (samba-dc1.risc.uni-linz.ac.at)
  - NTP servers (time.risc.uni-linz.ac.at)
  - SMTP server (mail.risc.uni-linz.ac.at)
  - POP server (pop.risc.uni-linz.ac.at)

NAT - Network Address Translation

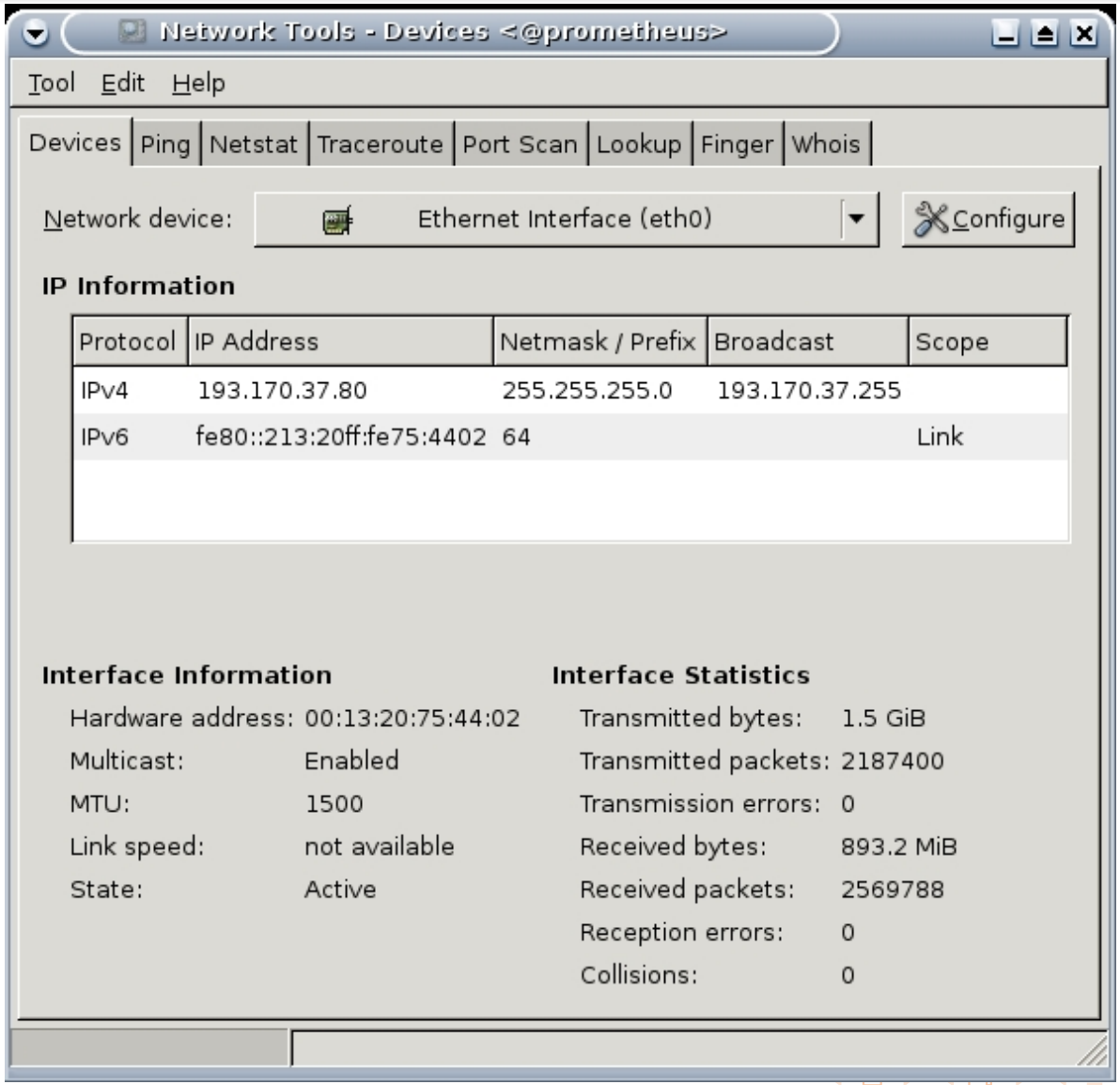
How NAT works

- general definition
  - a technique that hides an entire address space, usually consisting of private network addresses (RFC 1918), behind a single IP address in another, (often) public address space.
- implemented in a router - connected to private/public network
  - uses translation tables to map/remap the addresses
  - translation table are created by the outgoing requests
  - rewrites the outgoing IP packets as sent from the router
  - Assigns to each connection a different source port
- NAT introduces complications in communication, performance
  - it has to rewrite checksum, reassemble packets, fragment them again, etc.
- The NAT box - the Internet router
  - for SOHO Network (Small Office Home Office)
  - Cable/DSL router: a firewall is always integrated

Agenda

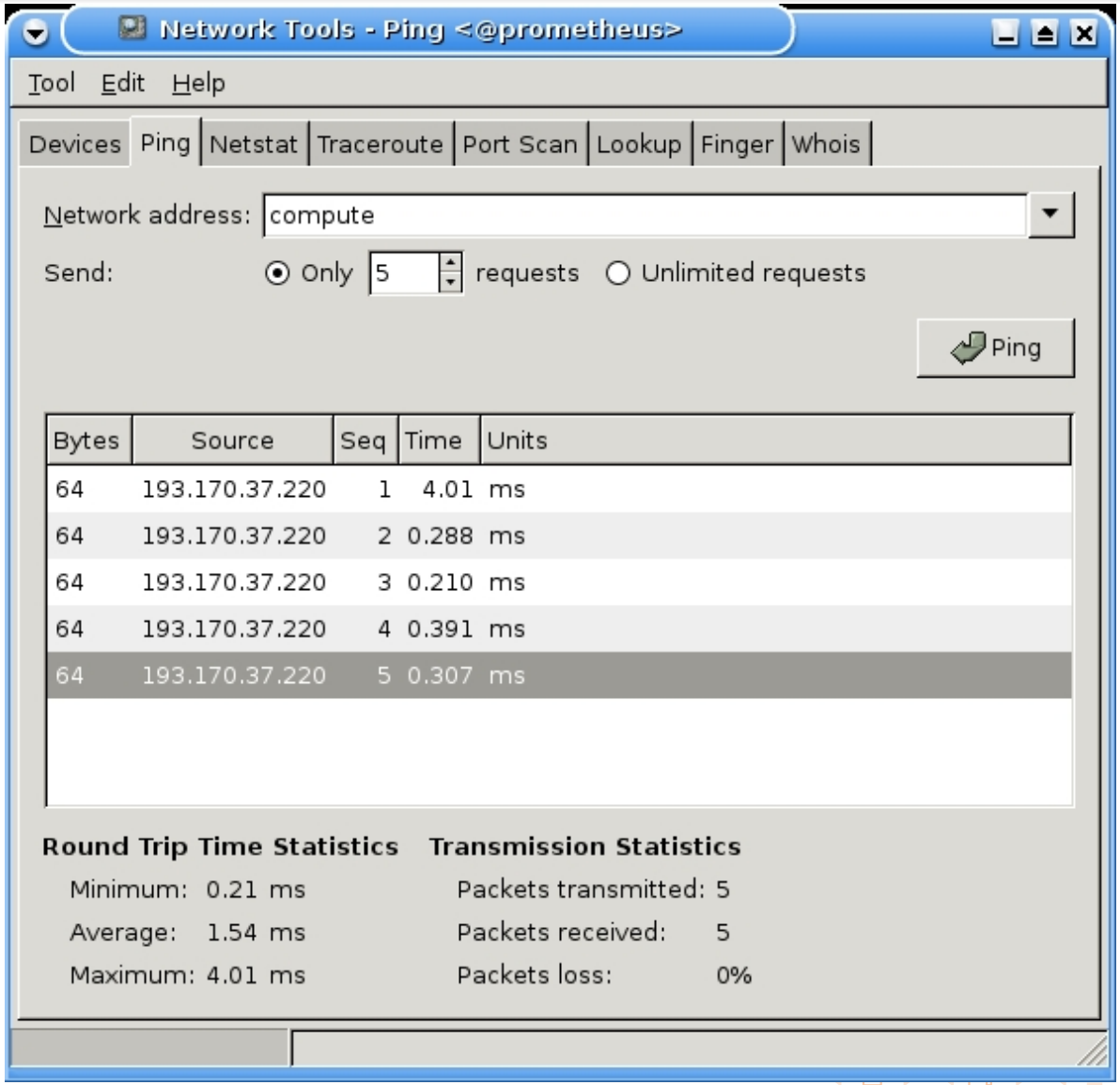
Checking Network Connections

gnome-nettool, devices



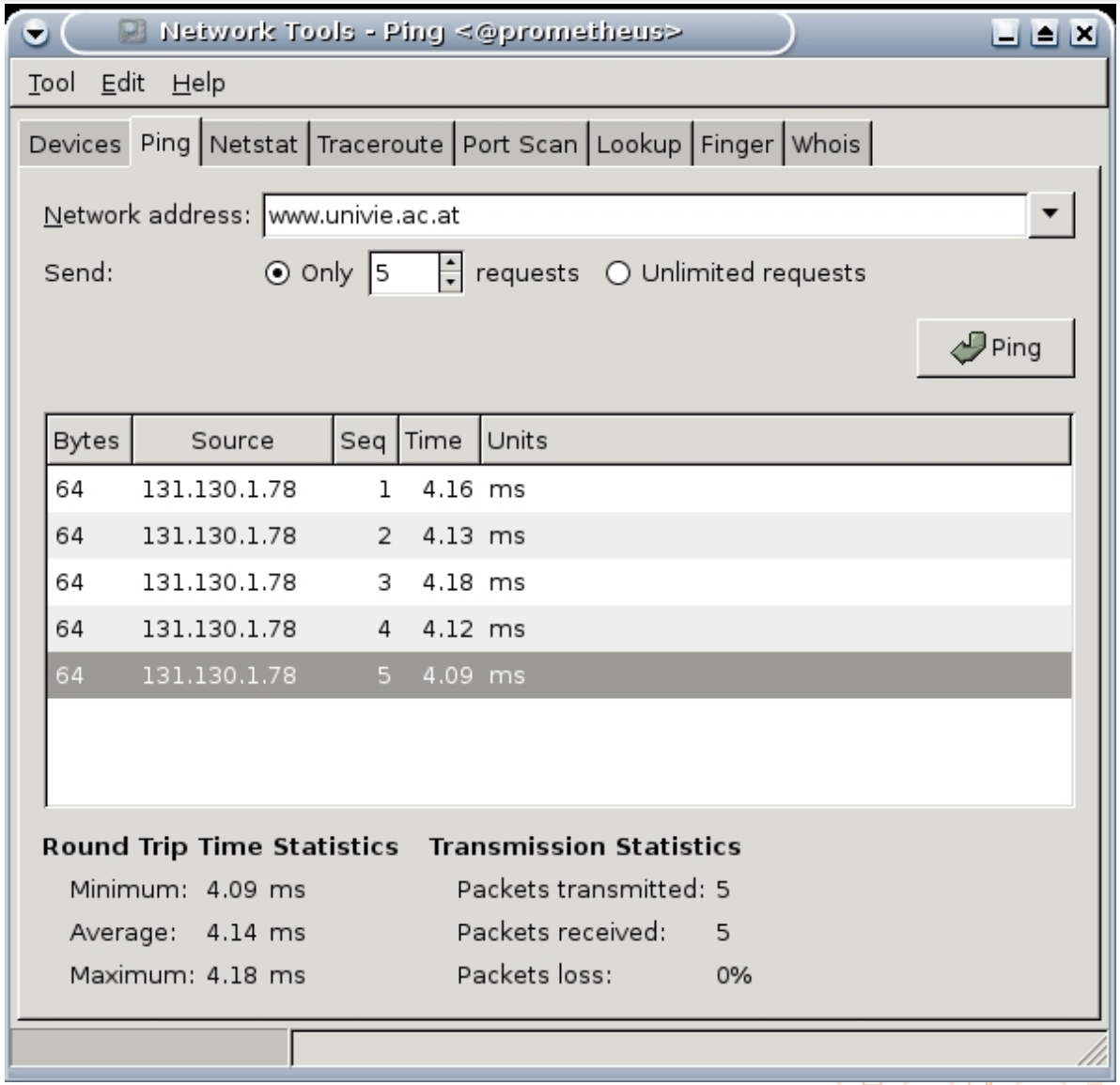
Checking Network Connections

gnome-nettool, ping, LAN



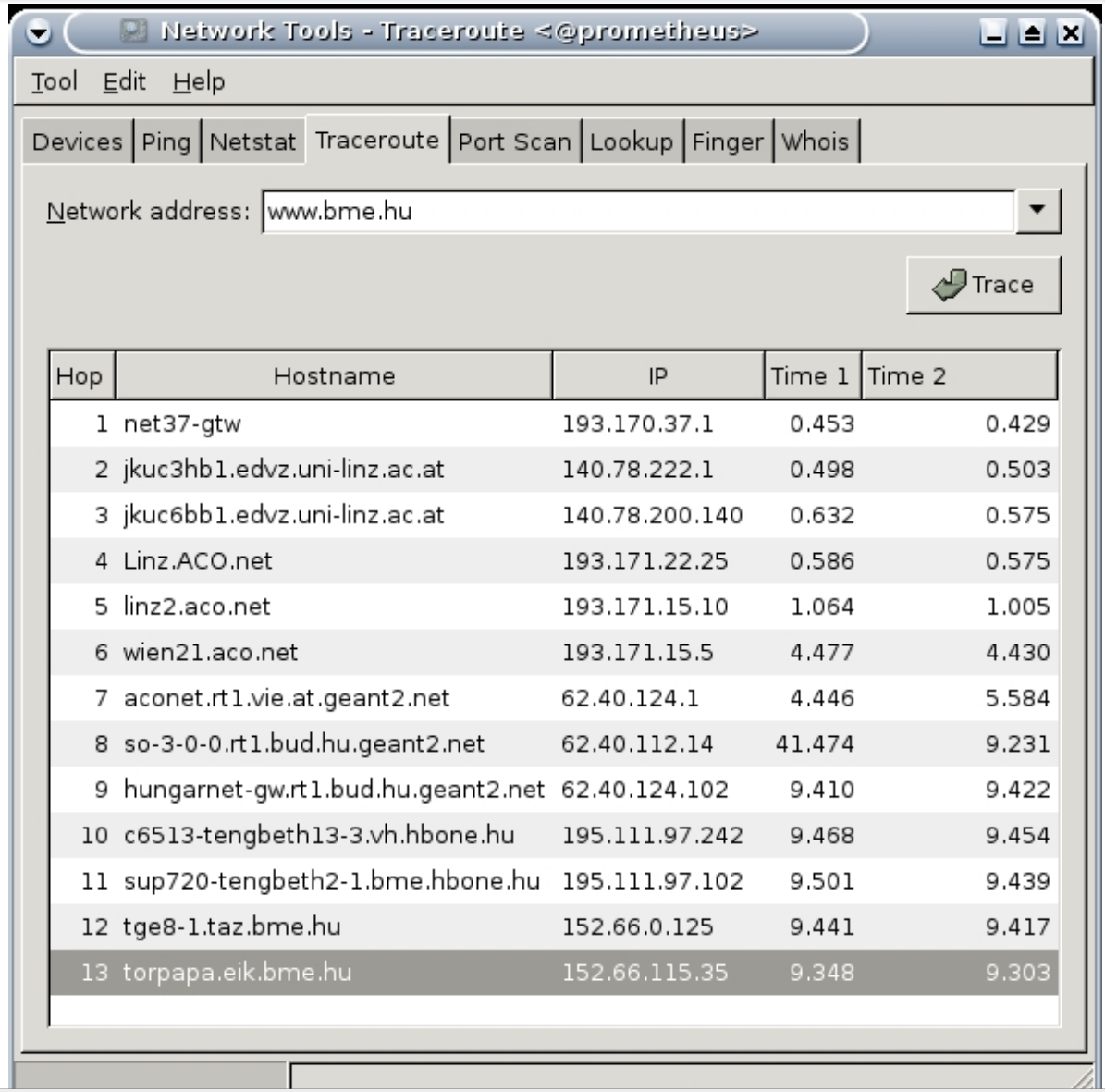
Checking Network Connections

gnome-nettool, ping, remote



Checking Network Connections

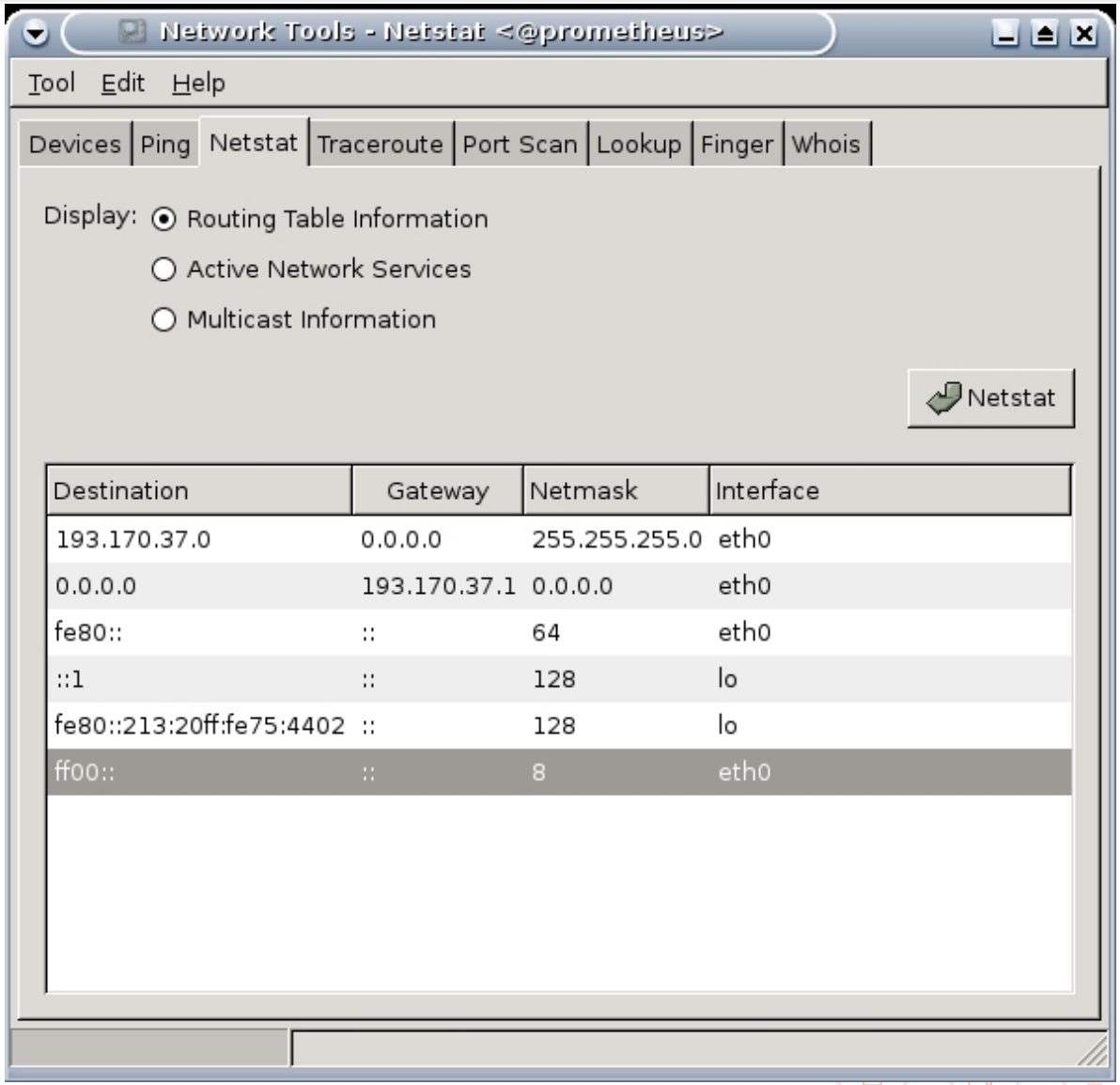
gnome-nettool, traceroute



Hop	Hostname	IP	Time 1	Time 2
1	net37-gtw	193.170.37.1	0.453	0.429
2	jkuc3hb1.edvz.uni-linz.ac.at	140.78.222.1	0.498	0.503
3	jkuc6bb1.edvz.uni-linz.ac.at	140.78.200.140	0.632	0.575
4	Linz.ACO.net	193.171.22.25	0.586	0.575
5	linz2.aco.net	193.171.15.10	1.064	1.005
6	wien21.aco.net	193.171.15.5	4.477	4.430
7	aconet.rt1.vie.at.geant2.net	62.40.124.1	4.446	5.584
8	so-3-0-0.rt1.bud.hu.geant2.net	62.40.112.14	41.474	9.231
9	hungarnet-gw.rt1.bud.hu.geant2.net	62.40.124.102	9.410	9.422
10	c6513-tengbeth13-3.vh.hbone.hu	195.111.97.242	9.468	9.454
11	sup720-tengbeth2-1.bme.hbone.hu	195.111.97.102	9.501	9.439
12	tge8-1.taz.bme.hu	152.66.0.125	9.441	9.417
13	torpapa.eik.bme.hu	152.66.115.35	9.348	9.303

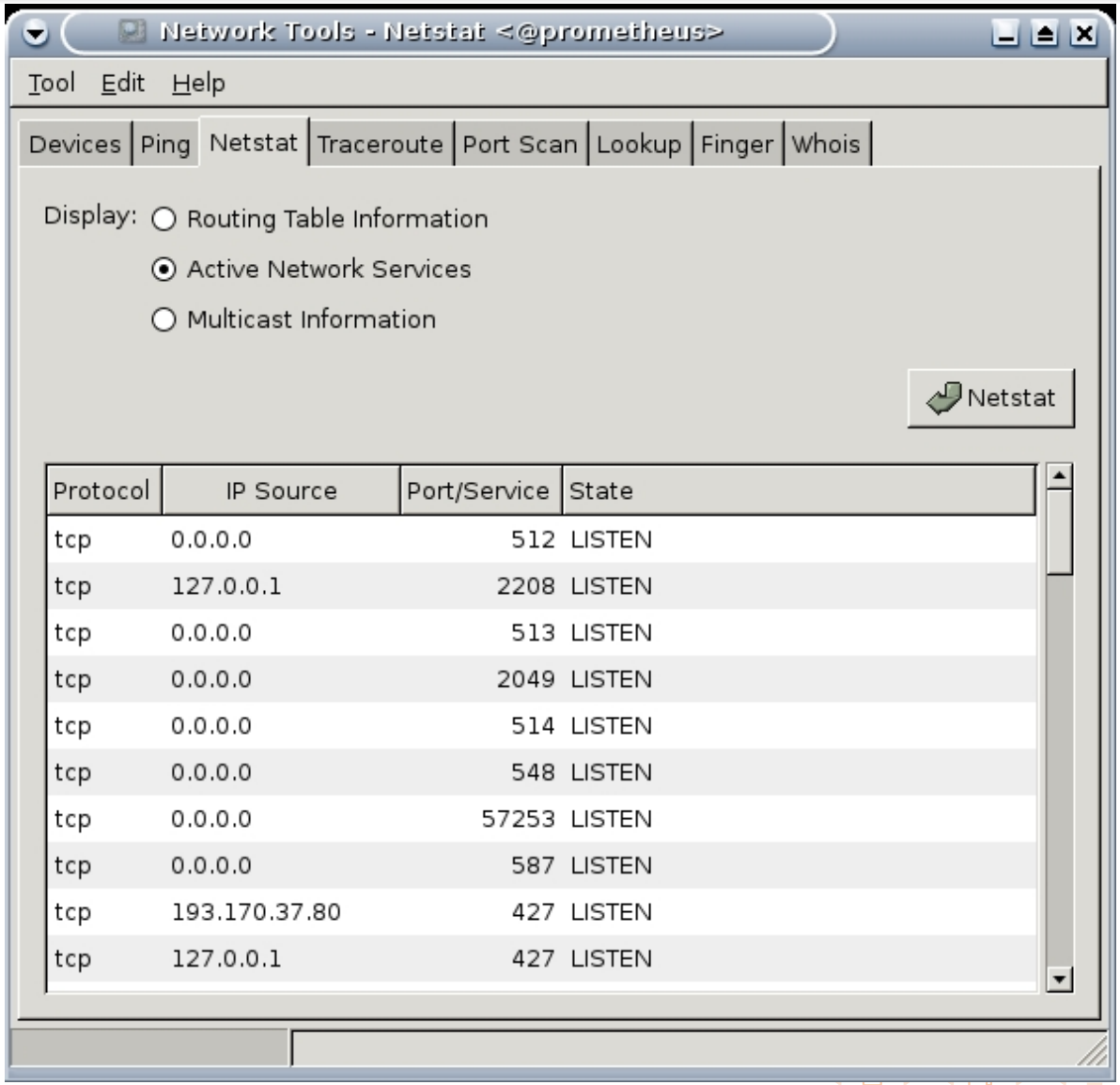
Network Connections - Routing

gnome-nettool, netstat



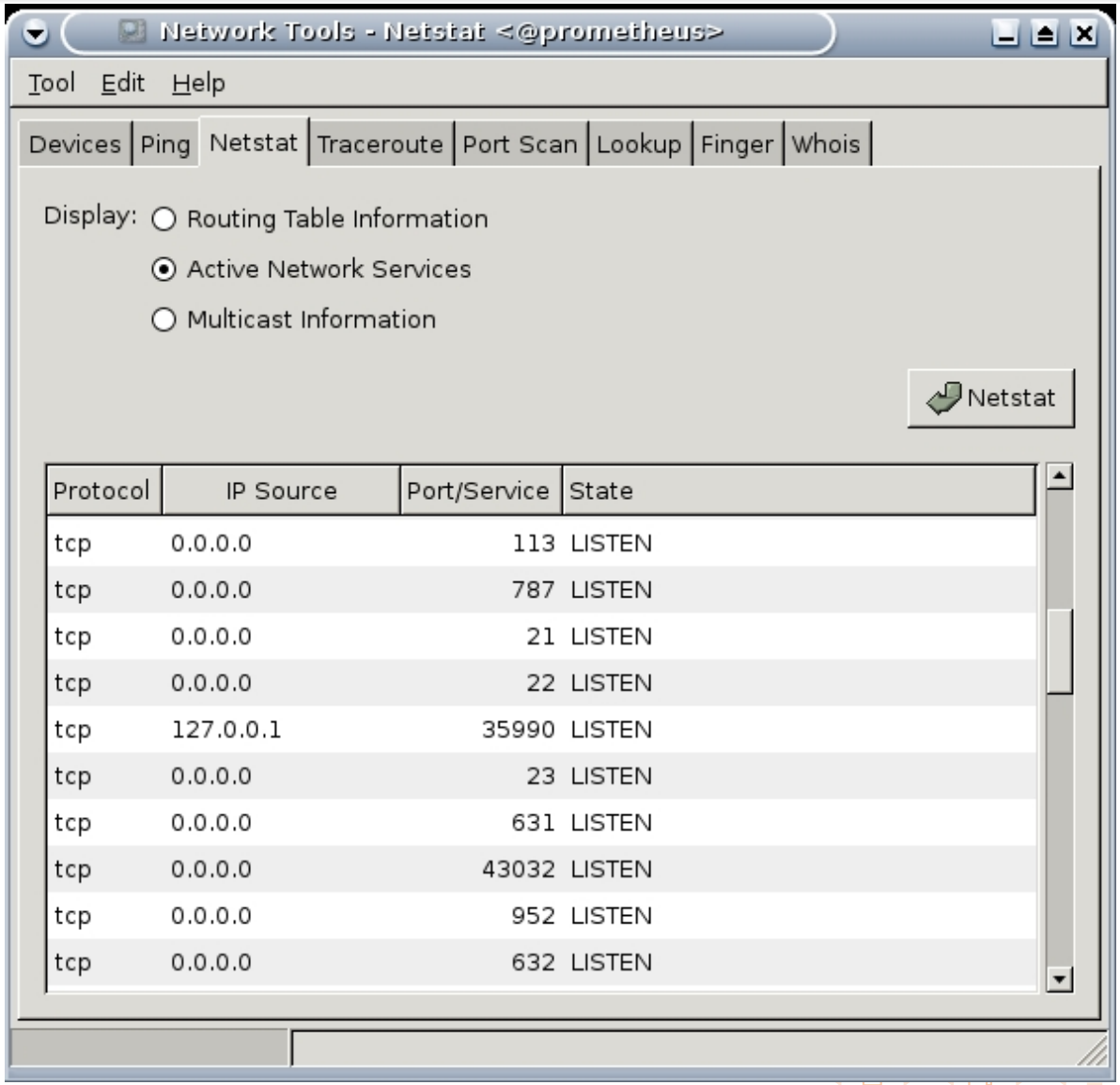
Network Connections - Active Services

gnome-nettool, netstat



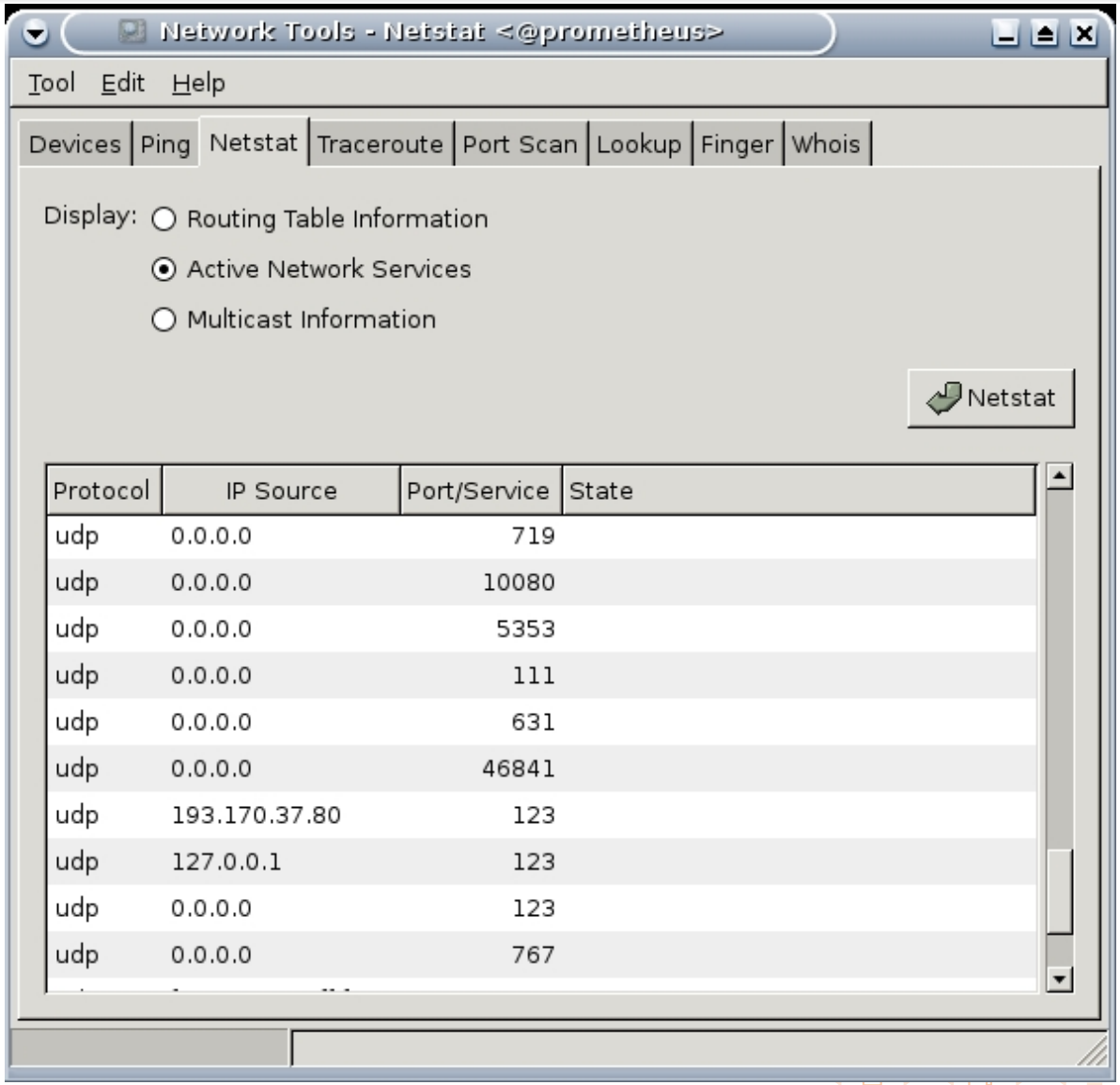
Network Connections - Active Services

gnome-nettool, netstat



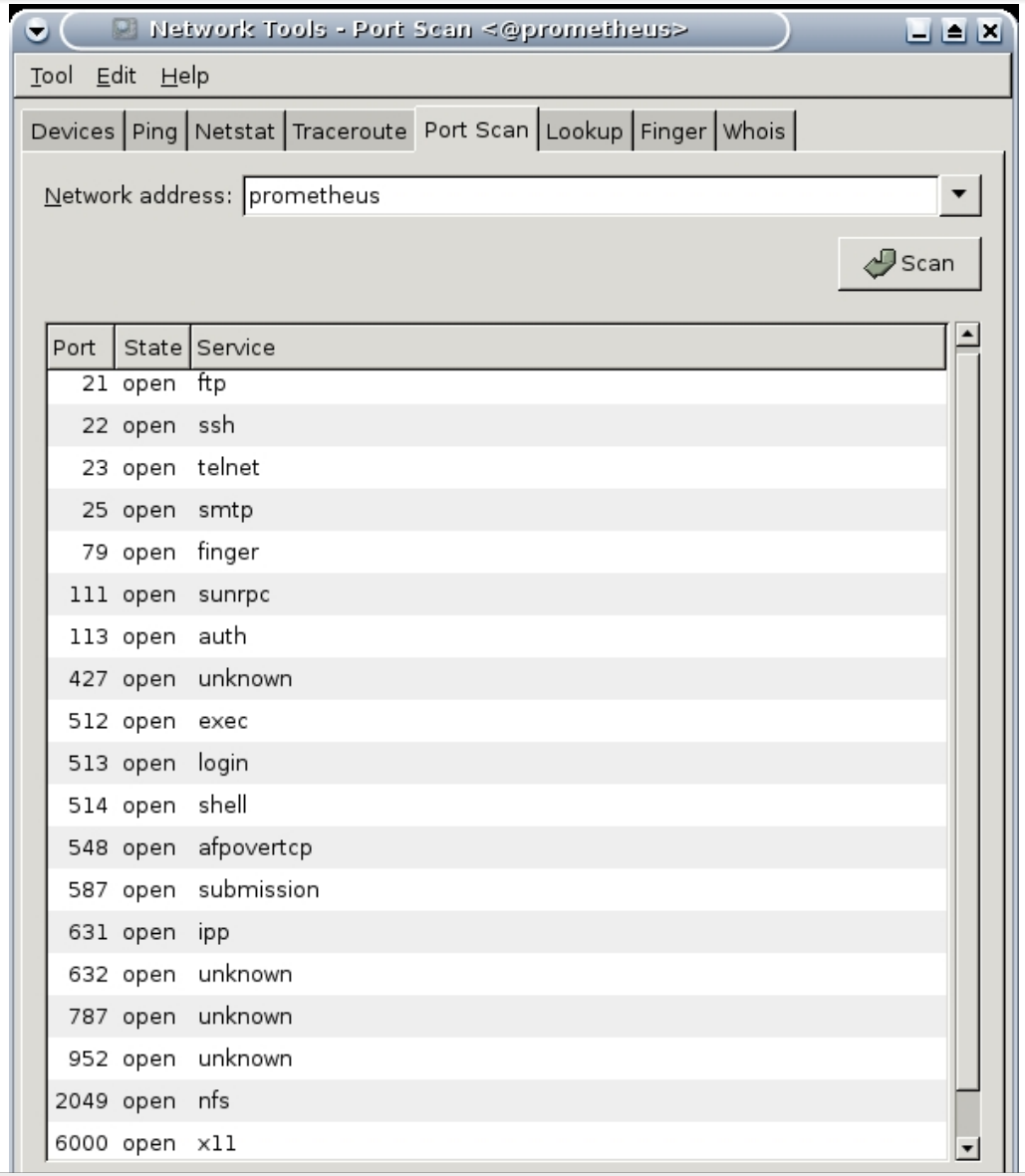
Network Connections - Active Services

gnome-nettool, netstat



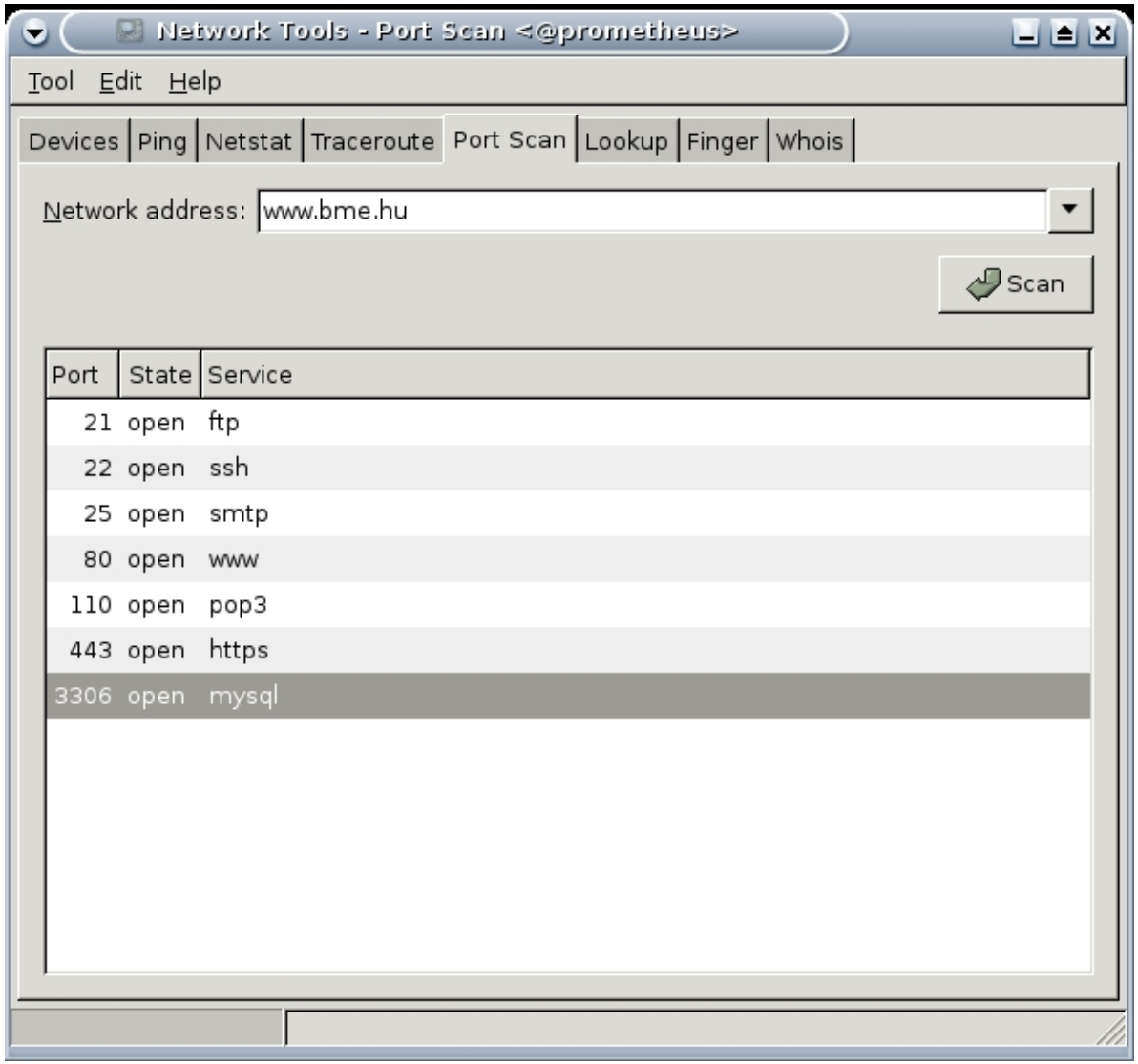
Network Connections - portscan

gnome-nettool, local



Network Connections- portscan

gnome-nettool, remote



Agenda

Connecting Computers to the Network

General remarks

Connecting automatically by DHCP

- the most confortable solution
  - if DHCP server is available for the domain, for the LAN segment
  - if the DHCP server is not restricted to known hosts
  - the hardware address (MAC address) of ethernet/wireless interface needed for access

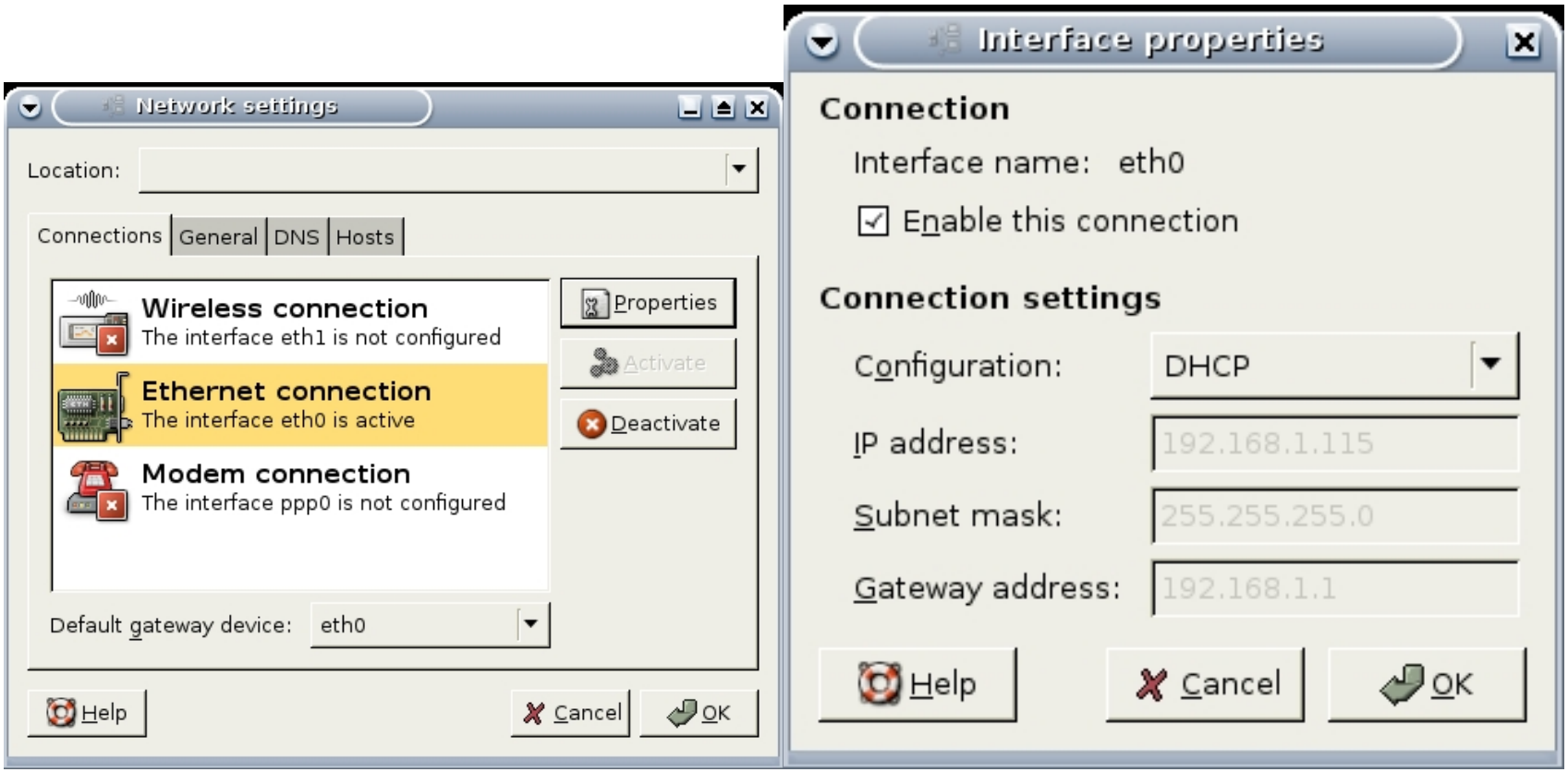
Connecting manually with fixed IP address

- this solution always works (local help (IP) needed)
- needs more knowledge about the OS, configuration files, etc.
- the only possibility if no DCHP server available

Connecting Computers to the Network

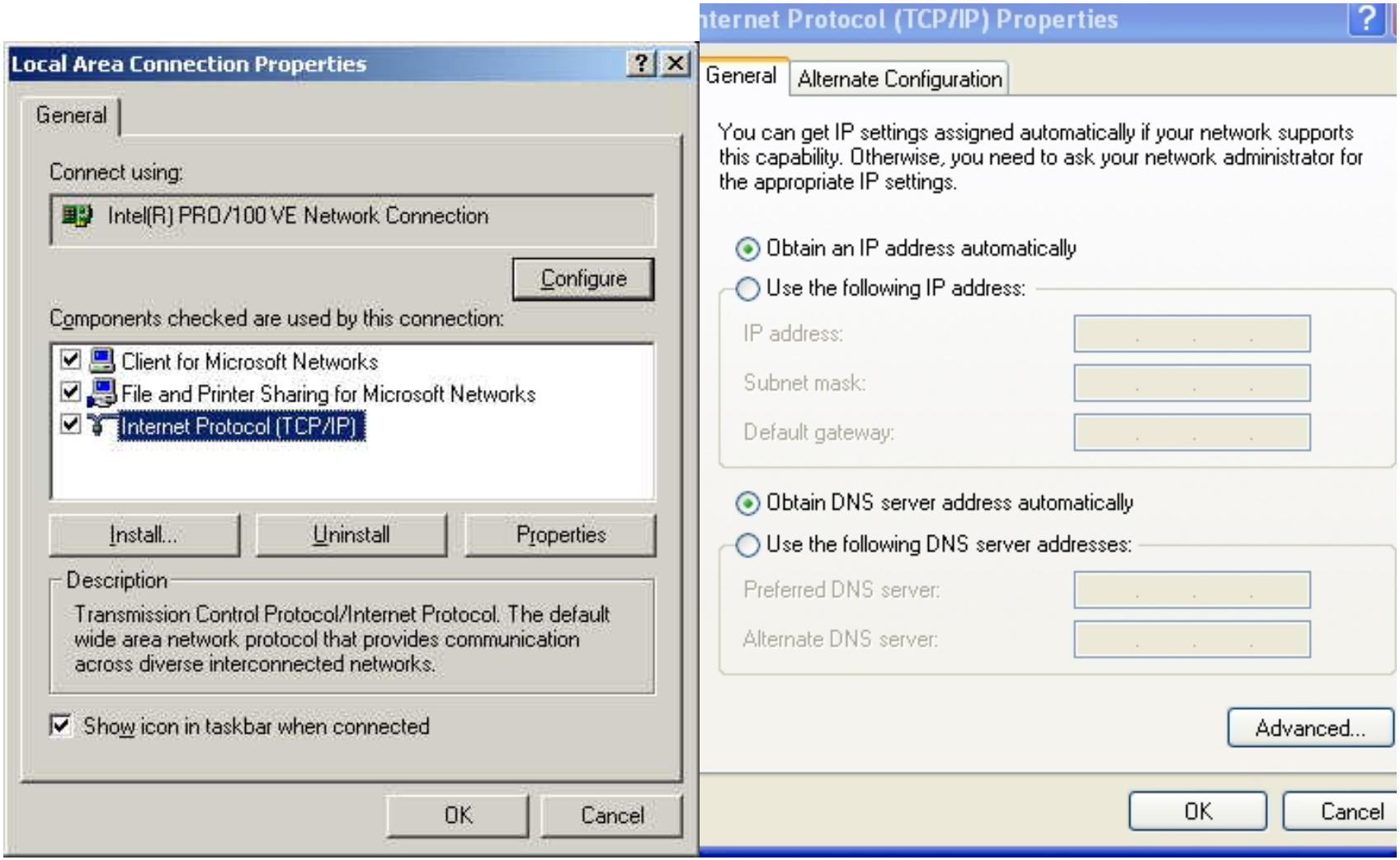
Using DHCP

Linux Configuration with network-admin



Connecting Computers to the Network

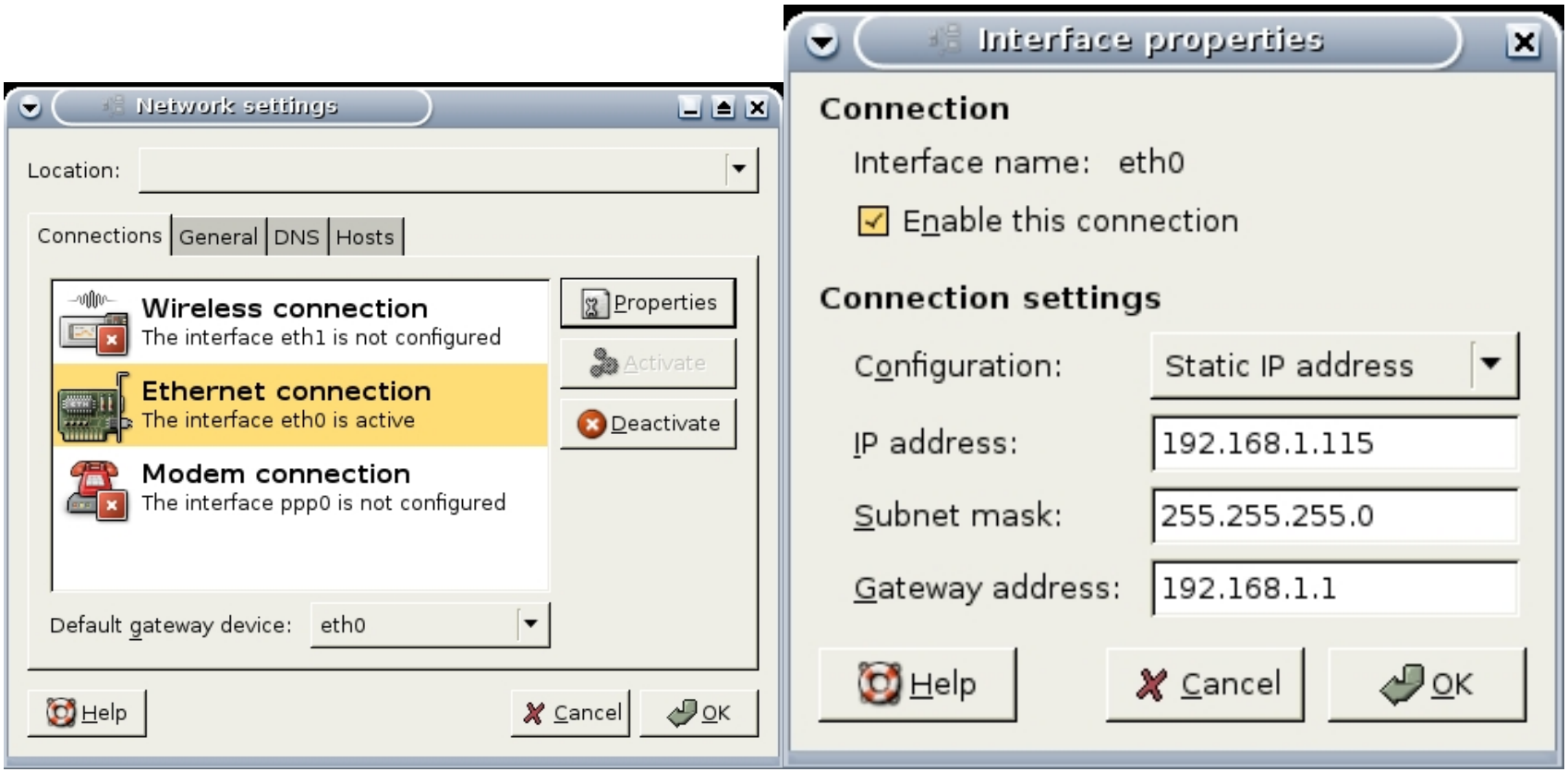
by DHCP for MS Windows



Connecting Computers to the Network

Using fixed IP addresses

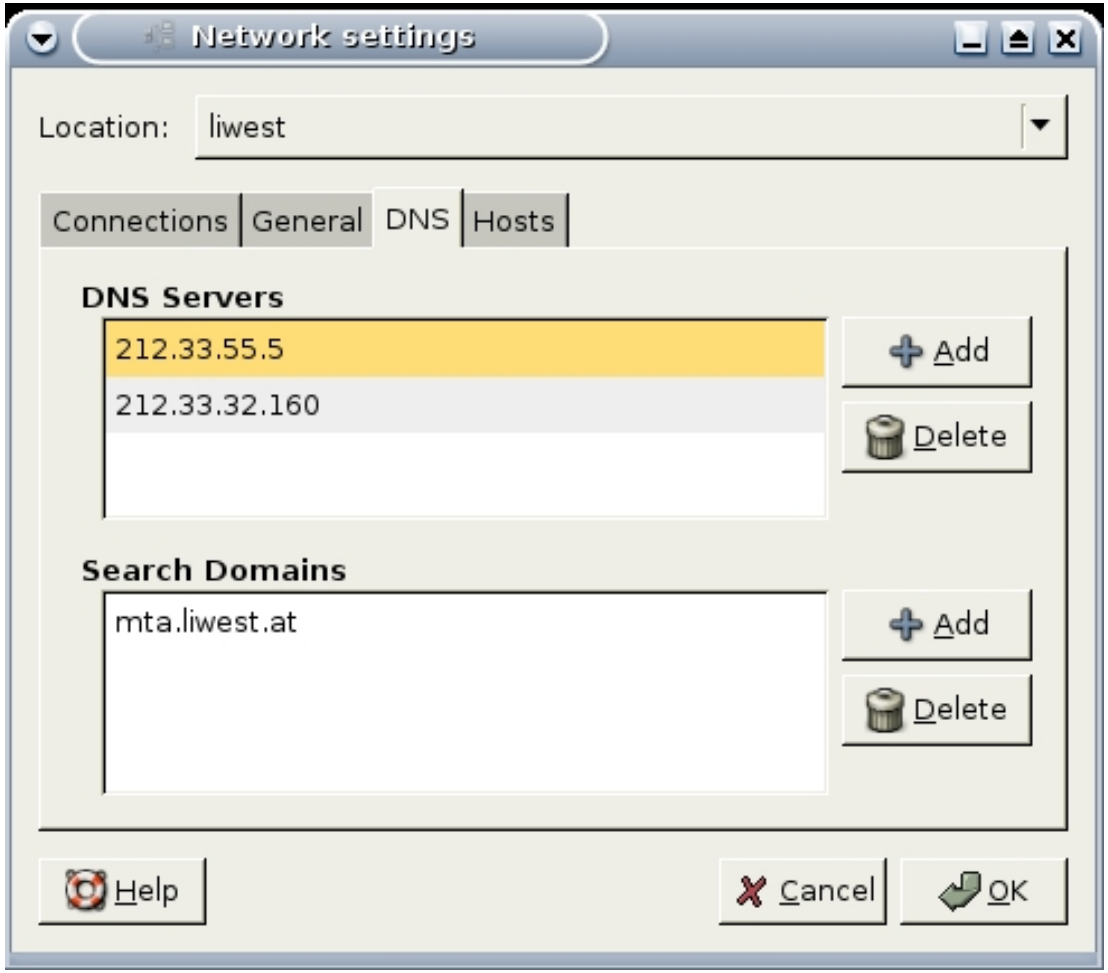
Linux Configuration with network-admin



Connecting Computers to the Network

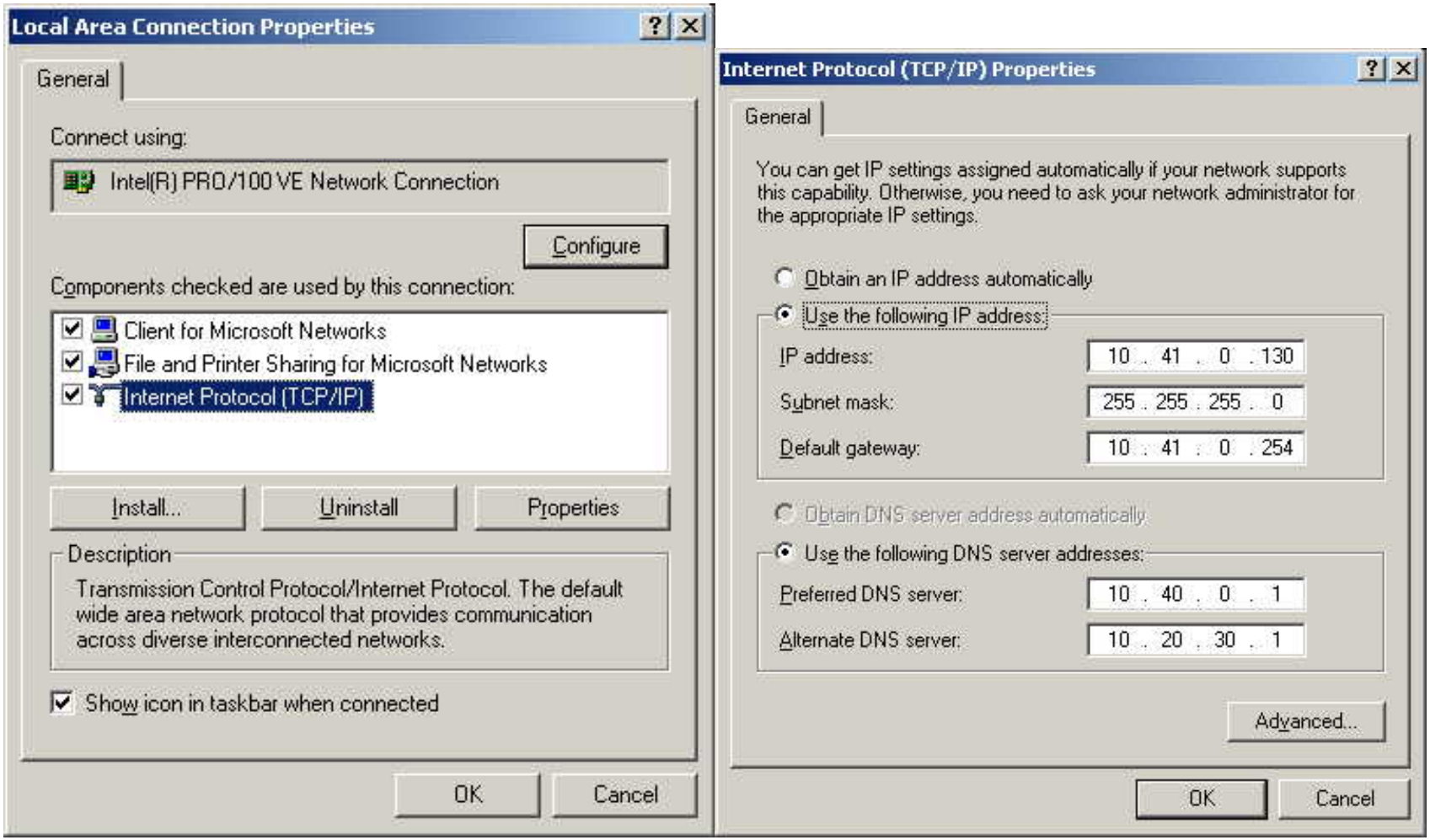
The Name Server

Configuration in Linux with network-admin



Connecting Computers to the Network

by static IP for MS Windows



Connecting Computers to the Network

Linux computer with Fixed IP addresses

Manual (command line) solution

- Changing the appropriate files
- Files responsible for connection:
  - /etc/network/interfaces
  - /etc/hosts
  - /etc/resolv.conf
- Other files for the host configuration
  - /etc/hostname
- File /etc/hosts

```
127.0.0.1       localhost
193.170.37.225          kernel.risc.uni-linz.ac.at      kernel
```

- File /etc/hostname
  - kernel

Connecting Computers to the Network

By fixed IP address

File /etc/network/interfaces for fixed IP address

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# allow-hotplug eth0
auto eth0
iface eth0 inet static

address 193.170.37.115
netmask  255.255.255.0
broadcast  193.170.37.255
network  193.170.37.0
gateway 193.170.37.1
```

Connecting Computers to the Network

Using DHCP

File /etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# allow-hotplug eth0
auto eth0
iface eth0 inet dhcp
```

Linux Configuration, on Command line

- change the /etc/network/interfaces file
- stop and start the interface: ifdown eth0; ifup eth0
- you will see the messages in the command line from `ifup` command

Connecting Computers to the Network

Using DHCP

File /etc/resolv.conf

- for fixed IP configuration it consist the nameservers and domain name

```
search risc.uni-linz.ac.at
# nameserver 193.170.37.224
nameserver 193.170.37.222
nameserver 193.170.37.138
```

- for DHCP connection it will be created by DHCP
- the contents is the same as above

Firewall

slide will be added later!

End of Network Basics

Thanks for your attention !