Computer Network Settings

- Basic terms
- Network interface settings
- DNS settings
- Routing
- Network services
- Firewall

Computer Networks

- Used for communication between computers, sharing their resources and information.
- Different sizes
- Different topologies
- Different protocols
- This material is aimed at TCP/IP networks.

Network Interfaces (1)

- Interface names can differ based on the distribution and system settings.
- Network interfaces are usually managed by a system service or a network manager (on systems with GUI).
- Ethernet interfaces
  - `eth0, eth1, eth2, ...`
- Wireless interfaces
  - `wlan0, wlan1, wlan2, ...`
-

Network Interfaces (2)

- USB interfaces
  - `usb0, usb1, usb2, ...`
- Bluetooth interfaces
  - `bnep0, bnep1, bnep2, ...`
- Point-to-point interfaces
  - `ppp0, ppp1, ppp2, ...`
- Serial interfaces
  - `ttyS0, ttyS1, ttyS2, ...`

Network Interface Settings – by Script

- Configuration file
  - `/etc/sysconfig/network-scripts/ifcfg-eth0`
- `DEVICE=eth0` # device name
- `USERCTL=no` # do not allow non-root users to control the interface
- `ONBOOT=yes` # bring up the interface on boot
- `BOOTPROTO=dhcp` # run DHCP protocol, or ‘none’ for manual addr.
- `IPADDR=` # IP address
- `NETWORK=` # network address
- `NETMASK=` # network mask
- `BROADCAST=` # broadcast address

Network Interface Settings – by Script

- Configuration file
  - `/etc/sysconfig/network-scripts/ifcfg-eth0`
- Start / stop / restart networking
  - `/etc/init.d/network {start,stop,restart}`
  - `service network {start,stop,restart}`
  - `systemctl {start,stop,restart} network`
- Networking service can be named differently, e.g. ‘networking’, ‘NetworkManager’, ...
- Start / stop network interface based on config. file
  - `ifup eth0, ifdown eth0`

Network Interface Settings – Manual

- Show IP address
  - `ip addr, ip add, ip a`
- Add static IP address to network interface
  - `ip addr add 192.168.1.1/24 dev eth0`
- Remove IP address from network interface
  - `ip addr del 192.168.1.1/24 dev eth0`
- Start / stop network interface
  - `ip link set eth0 up`
  - `ip link set eth0 down`
- Change MAC address
  - `ip link set dev eth0 address XX:XX:XX:XX:XX:XX`
- Start network interface with dynamic IP address
  - `dhcpclient eth0, dhclient eth0`

Network Interface Settings – Manual

- Older systems use command ‘ifconfig’
  - `ifconfig`
  - `ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up`
  - `ifconfig eth0 down`
  - `ifconfig eth0 hw ether XX:XX:XX:XX:XX:XX`

Further Configuration Options

- Configuration file
  - `/etc/sysconfig/network`
- Enable networking
  - `NETWORKING=yes`
- Hostname
  - `HOSTNAME=`
- Allow packet forwarding
  - `FORWARD_IPV4=yes`
- Default gateway settings
  - `GATEWAYDEV=`
  - `GATEWAY=`

Routing

- View routing tables
  - `/sbin/route`
  - `netstat –r`
  - `ip route`
  - `cat /proc/net/route`
- Add route
  - `route add net 192.168.1.0 netmask 255.255.255.0 eth0`
  - `route add default gw 192.168.1.1 eth0`
- Using ‘ip’ command
  - `ip route add 192.168.1.0/24 dev eth0`
  - `ip route add default via 192.168.1.1 dev eth0`

Host Name

- Unambiguous name that identifies host in a network
  - `hostname`
  - `hostname –f (full name including domain)`
- A host can have multiple hostnames (aliases)
  - `hostname –a`
- Change hostname
  - `hostname computer`
  - `/etc/hostname`
  - `/etc/hosts`
- Custom names for other hosts (without DNS lookup)
  - `/etc/hosts`

DNS Settings

- Configuration file `/etc/resolv.conf`
- DNS servers
  - `nameserver 1.2.3.4`
- Domain. If not specified, string after the first dot in the host name
  - `domain mydomain.local`
- DNS suffix, that should be searched when doing DNS lookups
  - `search fiit.stuba.sk`
  - `host www`

DNS Search Settings

- Configuration file `/etc/host.conf`
- Set search order.
  - `order hosts, bind, nis`
- Allow multiple IP addresses for one host. If ‘off’, resolv library returns the first record.
  - `multi off`
- Other options
  - `trim, spoof, nospoof, spoofalert, reorder`

Proxy Settings

- (HTTP) Proxy server is an intermediate server that sits between a client and an HTTP server.
- The client sends web requests to the proxy which in turn forwards it to the destination HTTP server and delivers the response.
- Multiple use-cases, including Internet access policy, web caching, web traffic monitoring.
- Environment variables in */etc/environment:*
  - `export http_proxy="192.168.1.10:8080"`
  - `export no_proxy="localhost,192.168.1.1"`

System Databases Settings

- Information such as users list, their passwords, etc. can be stored in different databases:
  - e.g. `files, dns, nis, ldap`
- Configuration file that specifies allowed sources and their order.
  - `/etc/nsswitch.conf`
- Compat is similar to files but allows special characters +/- for sources like passwd and group (`man nsswitch.conf`).
  - `passwd: compat`
  - `hosts: ldap dns files`

TCP/IP Network Sevices and IP Protocols

- List of well known and most used services based on TCP and UDP
  - /etc/services
- List of well known and most used IP protocols
  - `/etc/protocols`

Netstat

- View network connections, routing tables and statistics.
- View all TCP sockets that are in listening state and list the respective program:
  - `netstat -tlp`
- View all network connections in numeric form (no DNS resolving):
  - `netstat -an`

Nmap

- Tool for network reconnaissance and auditing.
- Host discovery – hosts that are “up” on the network.
  - `nmap -sn 192.168.1.0/24 (ping scan)`
- Port scan – determine state of ports.
  - `nmap -sS -p1-100 1.2.3.4 (SYN scan)`
- Service detection – services that listen on open ports and their versions
  - `nmap -sV 1.2.3.4`
- OS detection – determine host OS
  - `nmap -O 1.2.3.4`
- Vulnerabilities, scripts, ...

Netcat (1)

- “Swiss-knife for TCP/IP network”
- Wide usage in computer networks
- TCP and UDP connection to specified port
  - `nc [-u] hostname port`
- Online chat.
  - `nc -l -p 1234  // server, -l opens listening port`
  - `nc hostname 1234 // client`

Netcat (2)

- Simple file transfer. Connection is closed after EOF is read.
  - `nc -l -p 1234 > outfile`
  - `cat infile | nc hostname 1234 -q 0`
- Remote access.
  - `nc -l -p 1234 -e /bin/bash`
  - `nc hostname 1234`

ARP

- View and set kernel ARP entries.
- View ARP table
  - `arp, arp -n`
- Set static ARP entry (protection against ARP Spoofing Man in the Middle attack in switched network)
  - `arp -s xx:xx:xx:xx:xx:xx`
- Clear ARP cache
  - `arp -d 192.168.1.1`
  - `ip -s -s neigh flush all`

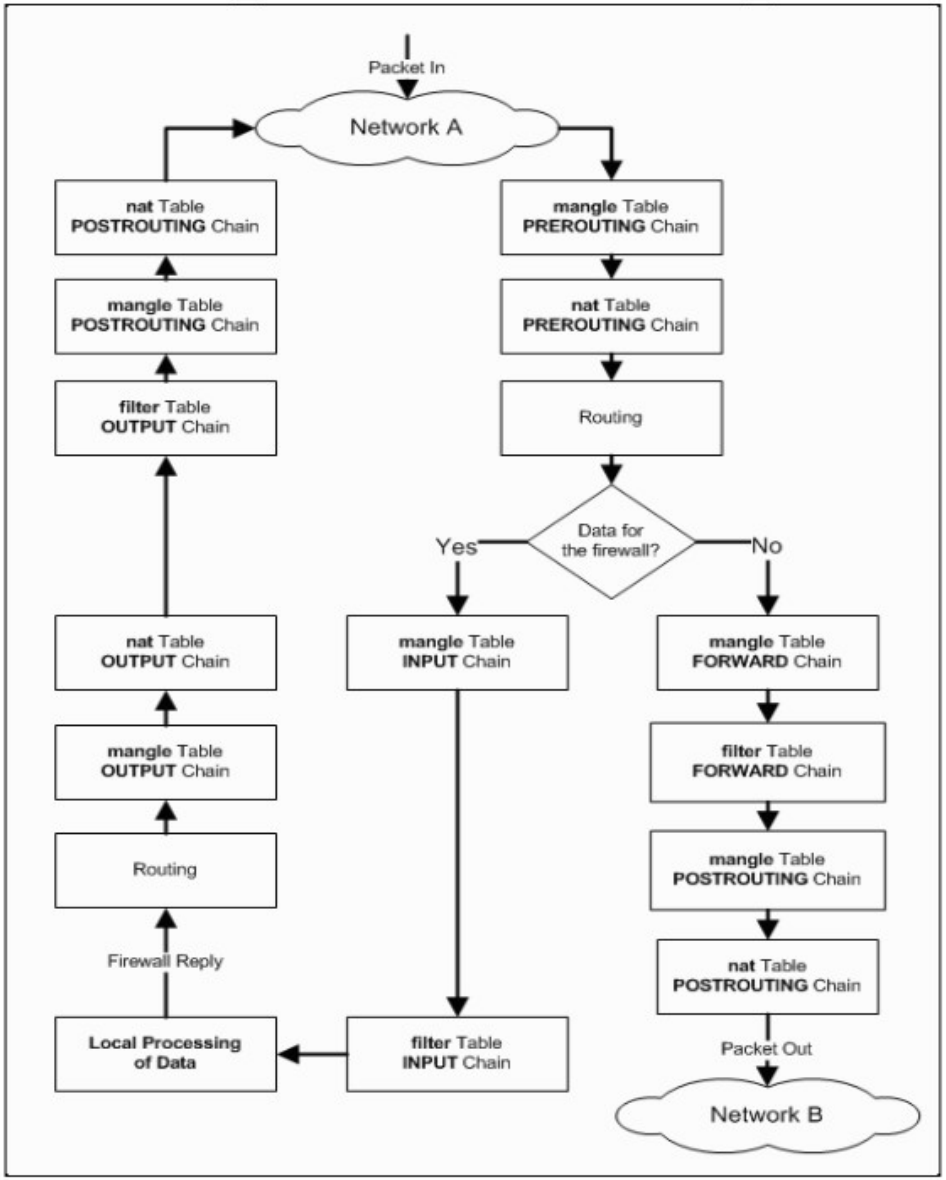
Firewall

- Firewall built-in in Linux kernel – iptables. Loading kernel module (if needed):
  - `modprobe ip_tables`
- Three tables for rules.
  - `filter` – used for packet filtering based on defined rules.
  - `nat` – used for IP address translation (NAT).
  - `mangle` – used for changing TCP headers, mainly for QoS
- Packet is processed by the first rule that matches the condition.

iptables - Chains

- Each table has multiple rule chains.
- NAT:
  - `PREROUTING` – applied before routing,
  - `POSTROUTING` – applied after routing,
  - `OUTPUT` – applied to outgoing packets.
- FILTER:
  - `INPUT` – incoming packets for this host,
  - `OUTPUT` – outgoing packets from this host,
  - `FORWARD` – packets routed to other interface (flowing through the host).
- MANGLE: same as the preceding. Always applied before entering specific chain in NAT and FILTER table.
- Possibility to create custom chain.

Packet route through iptables



iptables - Targets

- ACCEPT – packet passed.
- DROP – packet dropped.
- REJECT – similar to DROP but sends response to the sending node that the packet was rejected. By default:
  - `--reject-with icmp-port-unreachable`
- LOG – packet is logged in syslog (evaluation continues to the next rule)
- RETURN – return to the parent chain (used with custom chains).

iptables – NAT Table

- Actions for chains in NAT table.
- DNAT – translation of destination address.
  - `--to-destination <address>[:port]`
- SNAT – translation of source address.
  - `--to-source <address>[:port]`
- MASQUERADE – translation of source address. The source address is set to the address of the interface where the rule has been applied, i.e. the source is “hidden” behind the IP of the firewall. Appropriate for dynamic IPs.

iptables – important options (1)

- `-t table` – table that is edited.
- `-P target` – set default policy.
- `-j target` – action to be executed (jump)
- `-A chain` – append the rule to the end of the chain.
- `-I chain` – insert the rule to the beginning of the chain.
- `-F chain` – delete all rules in the chain (flush).

iptables – important options (2)

- `-p protocol` – match protocol.
- `-s source_ip` – match source IP.
- `-d destination_ip` – match destination IP.
- `-i in_interface` – match input interface.
- `-o out_interface` – match output interface.
- `--sport src_port` – match source port.
- `--dport dst_port` – match destination port.

iptables – Usage

- `iptables -P INPUT DROP`
- `iptables -A INPUT -i eth0 -s \ 147.175.92.1 -p TCP --dport 22 \`

  `-j ACCEPT`
- `iptables -A INPUT -i eth0 -p ICMP \`

  `--icmp-type echo-request -j ACCEPT`
- `iptables -A INPUT -i eth0 -m state \`

  `--state ESTABLISHED,RELATED -j ACCEPT`
- `iptables -A INPUT -j LOG`

iptables – Explanation of the Previous Example

- Set default policy for incoming packets to ‘DROP’. Packets that did not match any allow rule will be dropped.
- Allow SSH only from IP address 147.175.92.1
- Allow ICMP echo-requests (ping)
- Allow packets that are responses to existing connections initiated from the host (otherwise we could not communicate in outbound direction).
- All other traffic is logged and dropped.
- `dmesg | tail` – view last 10 system messages (logs).

iptables – Management

- Show current rules
  - `iptables –vnL [–t table]`
- Delete rules (beware of default policy!)
  - `iptables –F INPUT`
- Save state
  - `service iptables save`
- Load saved state
  - `service iptables reload`

Other Useful Tools

- Network testing
  - `ping, traceroute, arping`
- Packet sniffing
  - `tcpdump, wireshark, ettercap`
  - `iftop, nettop`
- Intrusion Detection System
  - `snort, suricata`

References

- Manual pages
- https://linux.die.net/man/
- ip command cheat sheet
- https://access.redhat.com/articles/ip-command-cheat-sheet
- Linux Networking HOWTO
- https://tldp.org/HOWTO/NET3-4-HOWTO-5.html
- iptables HOWTO
- https://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO-7.html