

Advanced Linux System Administration

Topic 11. Network administration (Introduction).



Pablo Abad Fidalgo
José Ángel Herrero Velasco

Departamento de Ingeniería Informática y Electrónica

Este tema se publica bajo Licencia:

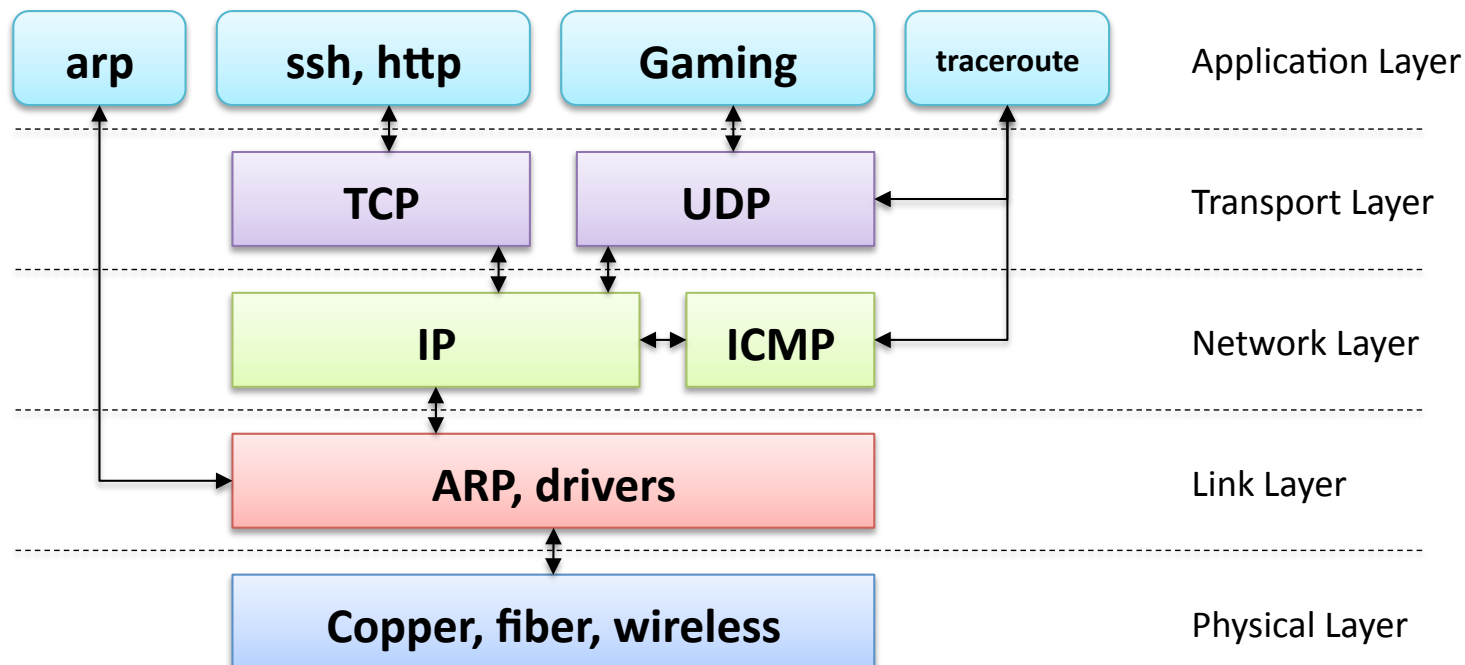
[Creative Commons BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Index

- **Introduction (TCP/IP).**
- **Network Interface.**
- **Link Layer.**
- **Network Layer.**
- **Monitoring/Test.**

Introduction (TCP/IP)

- Protocol “Suite”, a set of protocols designed to implement interconnection networks:
 - Origin: research project of the USA defense department (ARPANET).
- Multiple components, arranged hierarchically (stack).



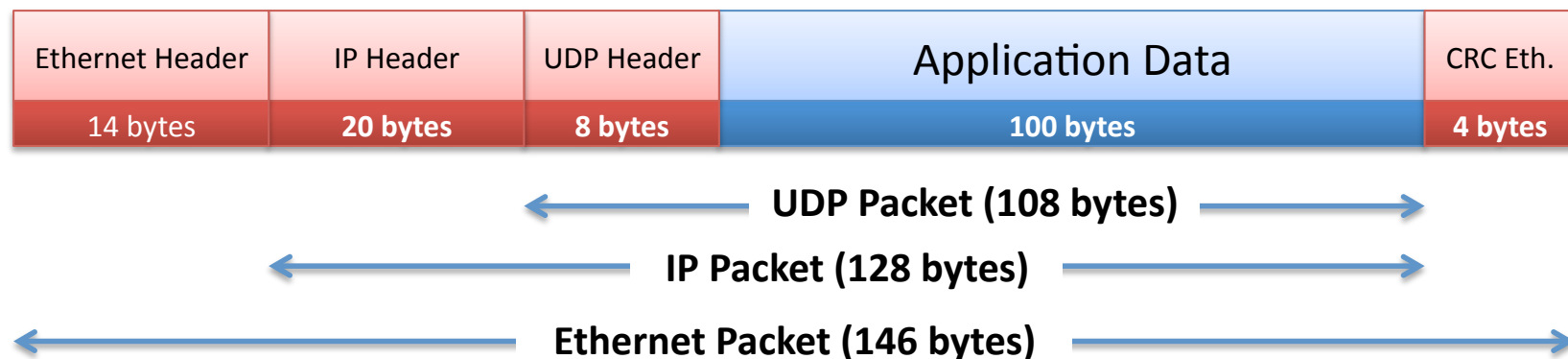
Introduction (TCP/IP)

- Protocol “Suite”, a set of protocols designed to implement interconnection networks:
 - Origin: research project of the USA defense department (ARPANET).
- Multiple components, arranged hierarchically (stack):
 - **UDP**, User Datagram Protocol, unverified, one-way data delivery.
 - **TCP**, Transmission Control Protocol, reliable, full duplex, flow controlled, error corrected conversations.
 - **IP**, the Internet Protocol, routes data packets from one machine to another.
 - **ICMP**, the Internet Control Message Protocol, provides low level support for IP: error messages, routing assistance, debugging.
 - **ARP**, Address Resolution Protocol, translates IP addresses into HW address (MAC).

Introduction (TCP/IP)

- **Encapsulation:**

- Data travels on the network in the form of packets, bursts of data with a maximum length imposed by the link layer.
- Each packet consists of a header and a payload:
 - Header: includes Source-Destination and protocol information.
 - Payload: the information (Data).
- As a packet travels down the TCP/IP protocol stack, each protocol adds its own header information.



Introduction (TCP/IP)

- **Packet Addressing:** multiple addressing schemes (at different layers):
 - HW Addressing (link layer):
 - Each net interface has one MAC addr that distinguishes it in the physical network.
 - Ethernet Network: 6 byte direction (2-digit hex bytes: 00:50:8D:9A:3B:DF).
 - IP Addressing (IPv4: 216.58.211.196):
 - Identifies the network interface in Internet. Unique at global level* (NAT & private addr).
 - Physical Address – IP address mapping: ARP protocol.
 - Hostname Addressing:
 - Number-based directions hard to remember (216.58.211.196 ??). Name mapping.
 - File mapping (/etc/hosts) or DNS (world-wide Domain Name Server).
 - Ports:
 - IP identifies the interface, How to identify active services? (multiple connections).
 - Extend IP address with port number: 16 bits identifying a communication channel.
 - Standard services (ssh, ftp, http) are associated to pre-established ports (/etc/services).

Introduction (TCP/IP)

- **IP Addressing:**

- **IPv4 vs IPv6:** IPv4 limitations (3 february 2011 no more addresses available):

- <https://www.google.com/intl/en/ipv6/statistics.html> (may 2017, below 20%).

- **Types** of IPv4 addresses: (32 bits divided into 4 8-bit fields a.b.c.d):

- Determines which portion identifies the network and which one the host.
 - Class A: (N.H.H.H) 1.x.x.x – 127.x.x.x (Apple, AT&T, Ford, US DoD...):
 - Network part=a, 126 nets.
 - Host part=b.c.d, +16 million hosts at each net.
 - Class B: (N.N.H.H) 128.x.x.x – 191.x.x.x:
 - +16K nets, 65K hosts per net.
 - Class C: (N.N.N.H) 192.x.x.x – 233.x.x.x.
 - Classes D and E: 234.0.0.0 – 255.x.x.x:
 - Experimental networks and multicast addressing.

0.0.0.0: My own Host (NO net connection)
0.x.x.x: One machine in our network
127.0.0.1: Loopback. Does not reach the NIC.
255.255.255.255: Bcast in local network.
x.x.x.255: Bcast in specified network.

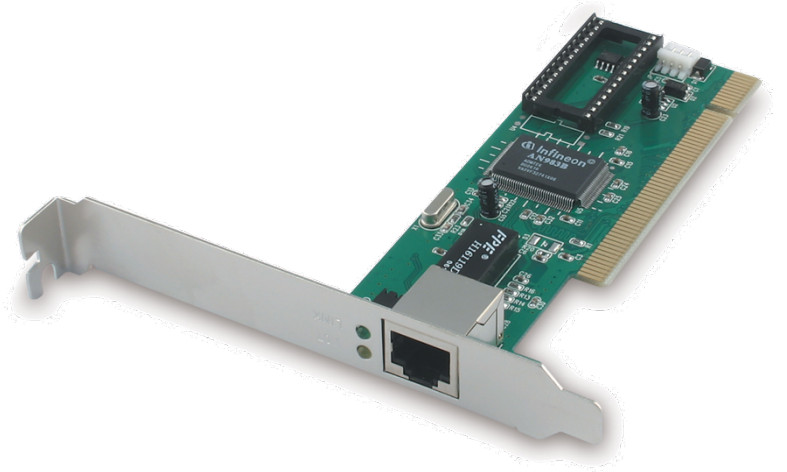
- **Subnetting:** A & B oversized, break classes into subclasses:

- Part of the host identifier is employed to identify the network.
 - Through the network mask (mapping).

Index

- Introduction (TCP/IP).
- **Network Interface.**
- Link Layer.
- Network Layer.
- Monitoring/Test.

Network Interface



- **Host / Interface:**
 - Hosts are computers/individual systems.
 - Each host can have one or more network interfaces (NICs) (Cable + WIFI):
 - Each interface represents a connection to a different network (different IP).
- **Basic network equipment:**
 - Hubs (level OSI-1): Only interconnects wires.
 - Switches (level OSI-2): Ethernet level management (ARP, MAC, etc.).
 - Routers (level OSI-3): IP packet management, network level.
 - Others: traffic balancing, firewalls...
- **Linux *does not* perform net management through *device files*:**
 - ethX has no device file associated (/dev/ethX not found).
 - NICs are managed through kernel modules (drivers).

Network Interface

- Configuration (Debian): file **/etc/network/interfaces**:
 - Establishes the configuration of network interfaces.
 - Allows additional functionality: routes*, alias, pre/post operations...
 - Fields:
 - auto <interface>: activates the interface when the system boots up.
 - iface <interface> <ip_addressing> <method>: interface configuration:
 - ip_addressing: inet (IPv4) / inet6 (IPv6).
 - method: dhcp (automatic) / static (manual, requires additional lines for configuration).
 - *Loopback interface:
 - Communication of network apps hosted in the same system.
 - auth lo.

```
auto eth0
iface eth0 inet static
    address 192.168.1.132
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
```

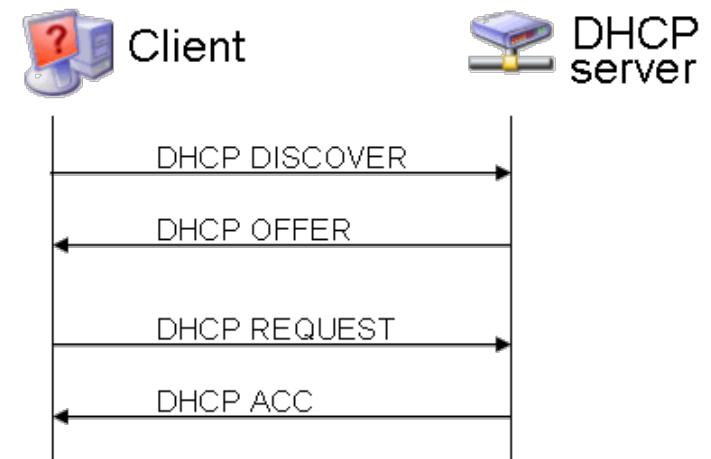
Network Interface

- Configuration (Debian):
 - Interface configuration can be modified in a “running” system:
 - STEP 1. Modification. Edit the file (/etc/network/interfaces or command ifconfig).
 - STEP 2. Re-start. ifdown/ifup or reboot the service (/etc/init.d/networking restart).
 - Commands **ifup/ifdown**: power on/off a network interface:
 - Syntax: ifdown eth0 (power off eth0 card).
 - Command **ifconfig**: net parameter configuration:
 - Syntax: ifconfig <interface> <address> <options>:
 - Example: ifconfig eth0 192.168.1.13 netmask 255.255.255.198 broadcast 192.168.1.191 up.
 - ifconfig -a prints information about available interfaces.
 - Caution!! Changes made with ifconfig are not permanent (do not modify interfaces file).
- Graphic tools: network-admin, webmin...

Network Interface

- **DHCP** (Dynamic Host Configuration Protocol):
 - The DHCP service performs **automatic network configuration** for the system:
 - “Renting” parameters from a server: IP, Gateway, DNS, etc.
 - “Safe”: allows forcing network configuration based on MAC address.
 - Easier: centralized management of the whole network.
 - Dynamic: information is only valid temporally.
 - Requires a “client” service at each host.
 - How to specify we want to use DHCP:
 - In /etc/network/interfaces:

```
iface ethX inet dhcp
```
 - `man dhclient`.
 - `ifconfig eth0 up`.



Index

- Introduction (TCP/IP).
- Network Interface.
- **Link Layer.**
- Network Layer.
- Monitoring/Test.

Link Layer

- The physical level in TCP/IP, almost always a ethernet network:
 - Each interface (NIC) has a unique MAC address.
 - Layer in charge of IP Frame <—> Ethernet Frame conversion:
 - Need to map IP address and MAC Address: ARP (Address Resolution Protocol).
 - **ARP Protocol:**
 - Search @MAC corresponding to a @IP in the local ARP table (translated address cache).
 - If not in the table, it performs a broadcast and the receiver informs. ARP table is updated for future connections.
 - When destination is not in local network, the IP route tables are employed, sending the message through the gateway MAC.
 - Command **arp**: manipulation/display of ARP table.
 - Configuration/Modification of @MAC:
 - # ifconfig eth0 **hw ether** 00:02:B3:19:C8:21.

Index

- Introduction (TCP/IP).
- Network Interface.
- Link Layer.
- **Network Layer.**
- Monitoring/Test.

Network Layer

- Through ARP only hosts in my net segment can be reached:
 - Cannot reach further than my hub/switch/router.
 - IP routes must be established for external addresses.
- **Route Tables:** information about how to reach IP destinations:
 - **Destination:** identifies destination network.
 - **Gateway:** how to reach to Destination (* means no forwarding is required, the packet is already in that network).
 - **Genmask:** network mask (identifies the subnetwork).
 - **Iface:** network interface to reach destination network.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.10.0	*	255.255.255.0	U	0	0	0	eth1
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.10.1	0.0.0.0	UG	0	0	0	eth1

Network Layer

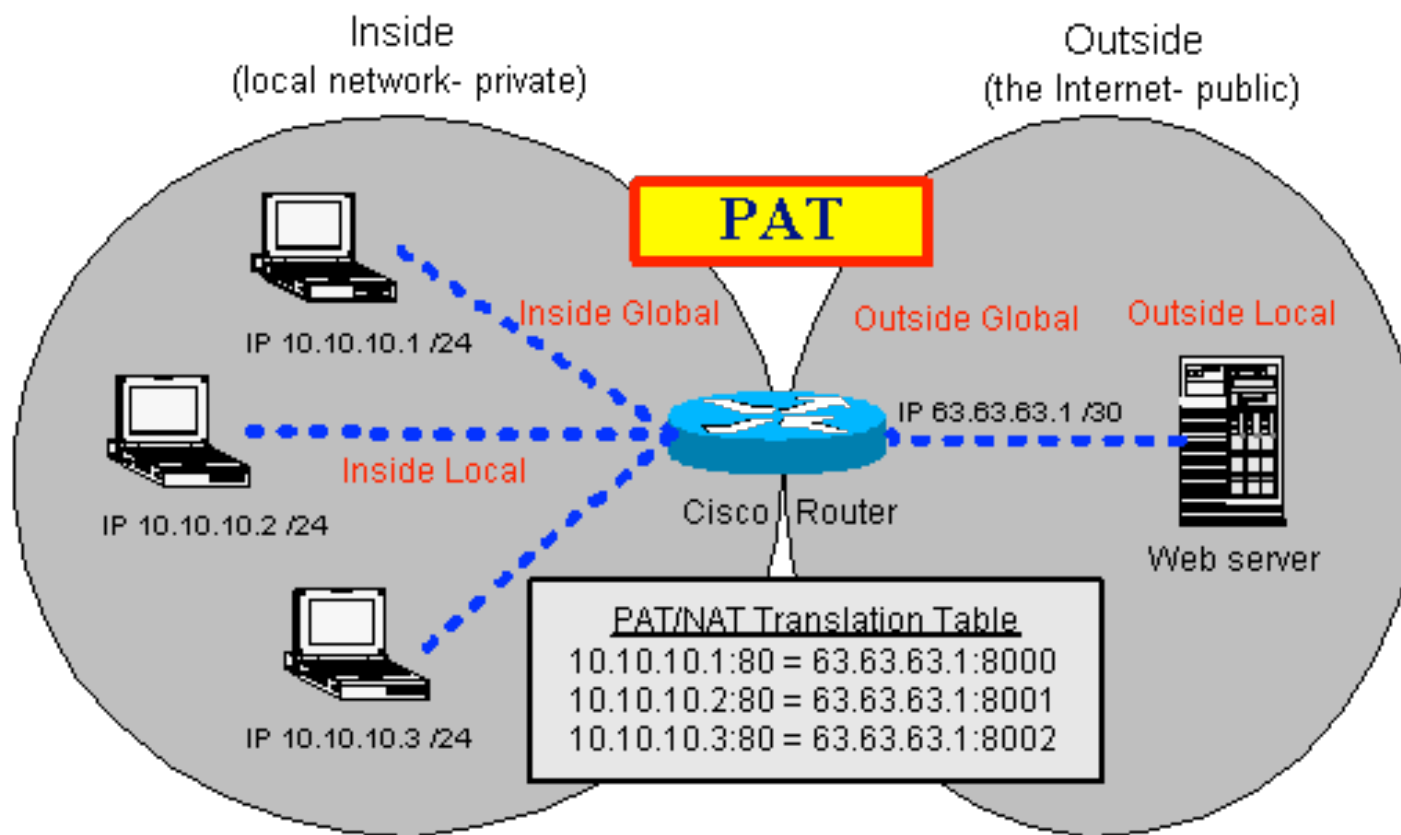
- Manual configuration of route tables:
 - Command **route**: modify/show tables:
 - #route -n: shows route tables.
 - Add a route for a network segment:
 - # route add -net 192.168.1.0 netmask 255.255.255.0 eth0.
 - Add the link element to other subnetworks (default route):
 - # route add default gw 192.168.1.1 eth0.
- Dynamic routes (automatic):
 - Static configuration of tables limits their functionality:
 - Valid for stable networks (not very large...).
 - Requires knowledge about network topology.
 - Complex environments: Dynamic Routes:
 - Daemon “routed” or “gated”. OSFP, RIP, BGP...
 - Maybe one of the most complex aspects concerning network administration.

Network Layer

- **Network Address Translation (NAT):**
 - Routing mechanism for packet exchange between incompatible networks (Public-Private address):
 - Allows a private IP to maintain internet connectivity.
 - For outgoing connections, the router translates the private IP as its own IP.
 - Router keeps information about all outgoing connections, relating them with incoming ones:
 - Outgoing connection: 192.168.1.25(1085) -> 212.106.192.142(1085).
 - Inbound communication: 212.106.192.142(1085) -> 192.168.1.125(1085).
 - NAT Types:
 - **Static NAT:** one-to-one mapping, each private IP is assigned a dedicated public IP.
 - **Dynamic NAT:** the router has a pool of public IPS assigned dynamically to the private IPs making a request.
 - **Port Address Translation (PAT):** single public IP. The port identifies the private IP.

Network Layer

- Network Address Translation (NAT):



Network Layer

- **Name Resolution:**
 - Name <-> IP translation, the network phonebook.
 - Option 1. Through the file **/etc/hosts**:
 - Conventional way, editing the file manually or through the command `addhost`.
 - Reasonable for small and private networks. Not useful for the rest of cases:
 - Adding a new host requires modifying all the `/etc/hosts` files in the network.
 - Usually employed only for the values required during boot process (`localhost`, `hostname...`).
 - Can add the IPs of relevant network servers or those providing essential network services.
 - Option 2. **Domain Name Service (DNS)**:
 - Dedicated server in charge of performing the conversion.
 - Each host must be configured to make use of its corresponding name server.
 - The client is configured through the file `/etc/resolv.conf`.

Network Layer

- **Name Resolution:** the file `/etc/resolv.conf`:
 - **search:** domain search order:
 - When we try to connect to a host without suffix, it auto-completes.
 - `ssh si -> ssh si.localdomain`.
 - Priority from left to right (first `atc.unican.es`, then `unican.es`).
 - **nameserver:** name server:
 - Try to resolve with the first one.
 - If it fails, keep on descending to lower lines.

```
search localdomain
search atc.unican.es unican.es

nameserver 193.144.193.11
nameserver 193.144.193.22
nameserver 192.168.0.105
```

Index

- Introduction (TCP/IP).
- Network Interface.
- Link Layer.
- Network Layer.
- **Monitoring/Test.**

Monitoring/Test

- Test Command:
 - Command **netstat**: shows network status:
 - Route table (-r), active connections (-a). Also sockets (TCP).
 - Command **ping**: packet ECHO_REQUEST (ICMP) to a host:
 - Check if a destination is reachable (warning, firewall & ICMP).
 - Command **tracert**: route followed by a packet towards destination:
 - Collects the IP at each gateway traversed.
- Command/Tools for monitoring:
 - Command **iptraf**: traffic statistics at network interfaces.
 - **tcpdump/Wireshark/...**: monitoring sent/received data for each connection.
 - **netperf**: performance measurement for links.
 - More sophisticated ones: MRTG, SAINT, Ganglia-monitor...