Linux Administration

Networking

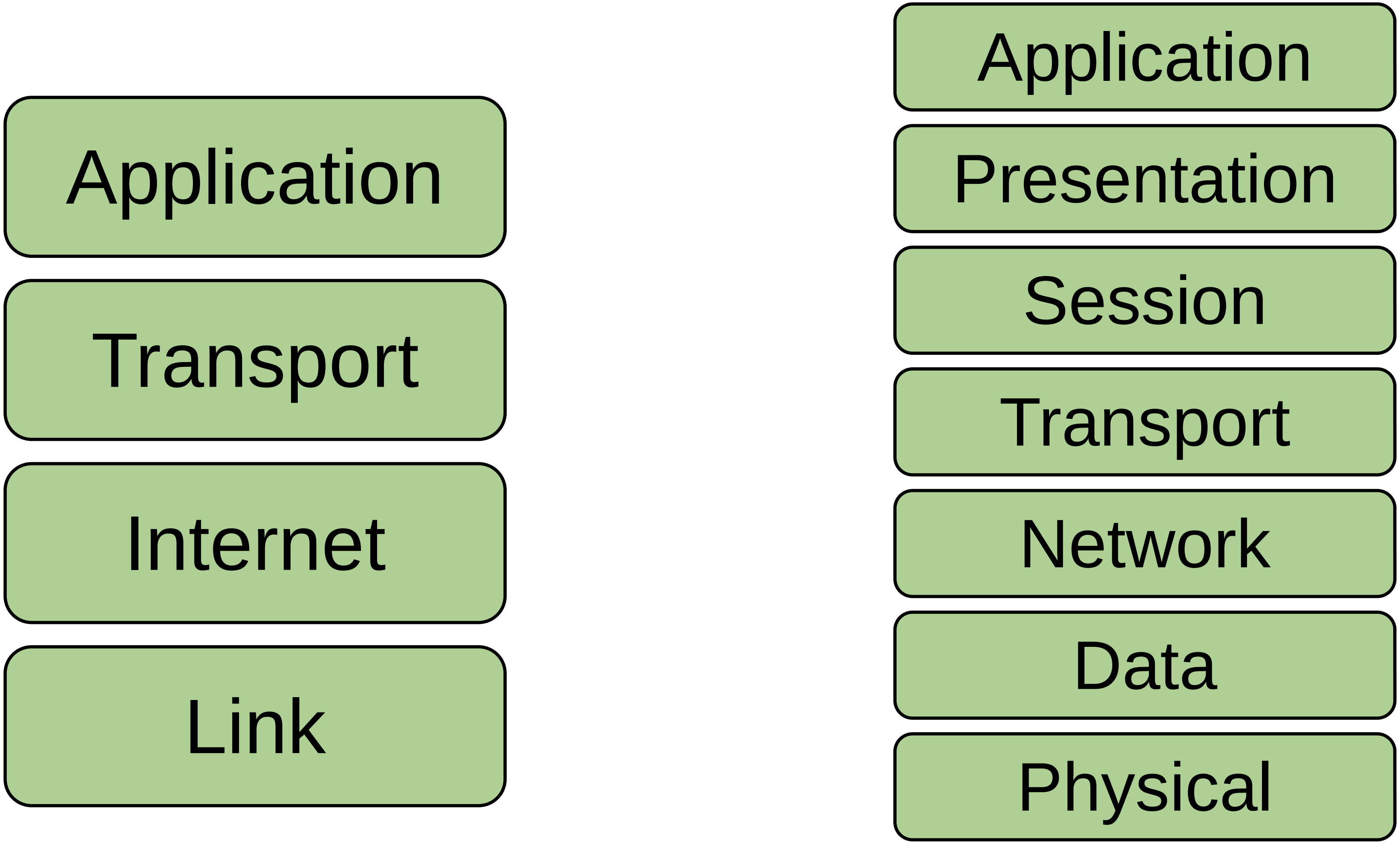
Xavier Belanger

Networking models

Two models are used to define the concepts used in networking:

- The OSI model. OSI stands for “Open Systems Interconnection” and is an ISO standard (International Organization for Standardization).
- The TCP model. TCP stands for Transmission Control Protocol, and is used as part of the Internet Protocol (IP). This model is older, and doesn’t go into as much details as the OSI one.

TCP model and OSI model



Application

Transport

Internet

Link

Application

Presentation

Session

Transport

Network

Data

Physical

IPv4 and IPv6

- IPv4 is the main protocol used on the Internet, it was created in the early 80s.
- There is a limit of 4,294,967,296 addresses (2^{32} - 32-bit addresses), and that limit has been reached.
- IPv6 was created in 1995. It’s using a larger address space (2^{128} - 128-bit addresses).
- IPv6 deployment is slow and may not be available everywhere.

IPv4 addressing

An IPv4 address is a 32-bit integer value, grouped by four octets represented in decimal.

0-255 . 0-255 . 0-255 . 0-255

1 octet . 1 octet . 1 octet . 1 octet
32-bit

IPv4 networks

- In itself, an IPv4 address is not sufficient to reach out another computer, a subnet mask is needed. This will define the size of the network.
- The subnet mask is a 32-bit integer value. A bitwise AND operation is used to get the network prefix.
- The first address of a network is reserved for identifying the network itself; the last address is used for broadcast.
- An address should be reserved for a router, in order to connect to other networks. Usually the first or last address available is used for this.

Subnet mask calculation

- 192.168.35.18/24
- 192.168.35.18
  255.255.255.0
- 192.168.35.0 - Number of hosts: 254 (.1 to .254)

- 172.20.79.125/26
- 172.20.79.125
  255.255.255.192
- 172.20.79.64 - Number of hosts: 62 (.65 to .126)

Special IPv4 networks

- 127.0.0.0 - 127.255.255.255: loopback
- 192.168.0.0 - 192.168.255.255, 172.16.0.0 - 172.31.255.255, 10.0.0.0 - 10.255.255.255: private networks
- 169.254.0.0 - 169.254.255.255:
  link-local addresses
- 224.0.0.0 - 239.255.255.255: multicast
- 240.0.0.0 - 255.255.255.254: “future use”

TCP and UDP

Two main protocols are use to transmit information:

- TCP: Transmission Control Protocol, that is connection-oriented, using handshakes, restransmission and error checking.
- UDP: User Datagram Protocol, that is connectionless with no overhead, and no guaranteed delivery.

TCP and UDP ports

- Applications using the network are using one or more TCP and/or UDP ports.
- Port numbers are ranging from 0 to 65535.
- Ports up to 1024 are usually called “well-known”, since most of those have historically been used for specific applications and standardized.
- On a Linux system, running an application using a port lower than 1024 requires root privileges.
- Port assignments are listed in /etc/services.

Few common ports

- TCP/21: File Transfer Protocol (FTP)
- TCP/22: Secure Shell (SSH)
- TCP/23: Telnet
- TCP/25: Simple Mail Transfer Protocol (SMTP)
- UDP/53 and TCP/53: Domain Name System (DNS)
- UDP/67 and UDP/68: Dynamic Host Configuration Protocol (DHCP)
- TCP/80: Hyper Text Transfer Protocol (HTTP)
- UDP/123: Network Time Protocol (NTP)
- UDP/161: Simple Network Management Protocol (SNMP)
- TCP/443: Hyper Text Transfer Protocol over SSL (HTTPS)
- TCP/993: Internet Message Access Protocol over SSL (IMAPS)
- TCP/995: Post Office Protocol over SSL (POPS)

Network interfaces

- The classic network scheme used on Linux for Ethernet interfaces is to use eth0 for the first interface, eth1 for the second one, etc.
- Wireless interfaces are usually named wlan0, wlan1, etc.
- In more recent years and depending on the distribution, interface names may be based on the network driver name, and could vary from one system to the other.
- The loopback interface is usually named “lo”.

The ip command

- The ip command can be used to configure and display settings related to network interfaces.
- Listing all network interfaces:
  ```
  ip addr show
  ```
- Add an IP address to an interface:
  ```
  ip address add <address>/<mask> dev <interface>
  ```

NetworkManager

- The NetworkManager package is used (or available) on various Linux distributions and can be used to configure the system network configuration.
- Three interfaces are available: command line (nmcli), text-based (nmtui) or via a graphical interface.

The ss command

- The ss (socket statistics) command can provide details on network connections.
- For a quick view of all networks connections use the following syntax:
  ss -anutp
  (all, numerical, UDP, TCP, processes)

The ping command

- You can check if a target device is reachable with the ping command.
- Note: this could be disabled on the target or somewhere on the network path.
- ping doesn’t rely on TCP or UDP, but on ICMP (Internet Control Message Protocol).
- The ping command doesn’t stop by default (you will need to use ctrl + c). You can use the -c option to limit the number of packets.

The traceroute command

- traceroute sends a series of three packets with short TTL (time to live) to each node (usually routers) on the path to the final target.
- By default, you can use the command with only the target IP address as an argument. Specific options requires root privileges.