Linux Administration

Networking

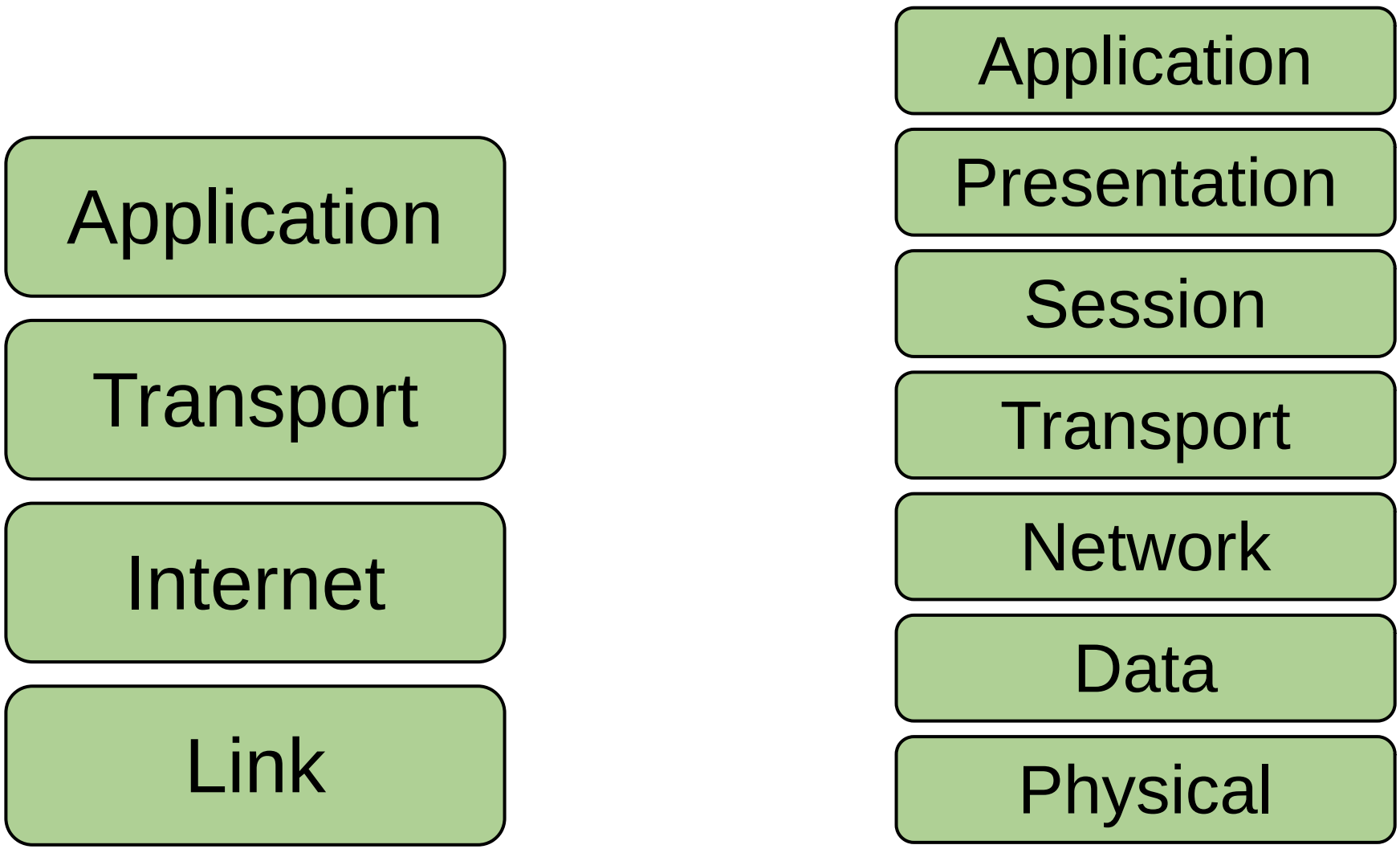
Xavier Belanger

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



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}), and that limit has been reached.
- IPv6 was created in 1995. It's using a larger address space (2^{128}).
- 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 another computer, a subnet mask is needed. This defines 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 common notation (CIDR - Classless Inter-Domain Routing)is to list the first address of the network, followed with a slash and the number of bytes used by the netmask. For instance, 192.168.5.0/24.
- 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

Example #1

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

Example #2

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

Special IPv4 networks

127.0.0.0 - 127.255.255.255	loopback
192.168.0.0 - 192.168.255.255	private networks
172.16.0.0 - 172.31.255.255	private networks
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”

IPv6 addressing

An IPv6 address is a 128-bit value, grouped in four hexadecimal blocks, separated by colons.

2001:0db8:85a3:0000:0000:8a2e:0370:7334

There is way to compress the representation. (Removing leading zeros, suppressing zero fields, etc. Specific rules applies.)

The CIDR notation is also used to specify the size of the networks.

IPv6 addresses scope

- IPv6 addresses are assigned to a specific scope:
  - Unicast, that is divided between local and global.
  - Anycast, that allows an address to be used by multiple devices.
  - Multicast to be used between a group of devices.
- It is possible for a network interface to have multiple IPv6 addresses with different scopes.

TCP and UDP

Two main protocols are use to transmit information:

- **TCP**: Transmission Control Protocol, that is connection-oriented, using handshakes, re-transmission and error checking.
- **UDP**: User Datagram Protocol, that is connection-less 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 the /etc/services file.

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/389	Lightweight Directory Access Protocol (LDAP)
TCP/443	Hyper Text Transfer Protocol over SSL (HTTPS)
TCP/636	Lightweight Directory Access Protocol over SSL (LDAPS)
TCP/993	Internet Message Access Protocol over SSL (IMAPS)
TCP/995	Post Office Protocol over SSL (POPS)

Network interfaces

- The loopback interface is named “lo”.
- The classic naming 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, interface names are based on the hardware, such as “ens34” (“Ethernet interface, PCI slot 34”).

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
- Displaying the routing table:
  ip route
  ip -6 route
- To add an IP address to an interface:
  ip address add <address>/<mask> dev <interface>

Name and name resolution

- The *hostname* command can be used to define the system fully qualify domain name (FQDN). See also the /etc/hostname file.
- The */etc/resolv.conf* file will contain the list of domain name servers to use.

NetworkManager

- The NetworkManager package is used by many Linux distributions 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.
- You can list all UDP and TCP processes in numerical form with the following options:
  ss -anutp

The lsof command

- The lsof (list opened files) command can also be used to list all existing network connections:

  lsof -i -P

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 uses 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 or name as an argument. Specific options requires root privileges.

The wget and curl commands

- *wget* can be used to download files over HTTP and HTTPS. It can even be used to copy an entire website.
- *curl* is a similar tool, and support more protocols (including SCP, SMB, various mail protocols, etc.).