

## 9. Troubleshooting in networks

If troubleshooting by experience fails, then you need a systematic way to identify the source of the problem. A good way to do this is the bottom up method. The correct function of every OSI layer is checked one by one from bottom to the top.

### 9.1 Checking the physical layer

Ethernet:

Check the link and activity LED next to the Ethernet socket. If no LED is on or flashing then check the cables and connectors to the switch or change components until you identify the origin.

WLAN:

Check with a WLAN Host if you capture the WLAN signal and if you can connect to it. If this fails even though you are close enough to capture it, then check the configuration of the access point.

### 9.2 Checking the data link layer

Its not easy to identify a problem on the data link layer as there is no way to manually generate a frame only. Troubleshooting on the data link layer is more or less limited to checking if the ARP table is filling after clearing it (ARP -d \*). If this is not the case check the configuration of the switch if it is managed. MAC address filtering or VLAN settings (see CORE2) in the switch might be the origin of the problem.

### 9.3 Checking the network layer

To check the network layer use the PING command. If a ping to a local host fails, check the IP configuration with the IPCONFIG command. The settings shown in the GUI (graphical user interface) of the operating system might not be reliable.

If a ping to an IP address outside of the local network fails, check the routing table of the router.

## 9.4 Checking the transport layer

With the NETSTAT command you can check if an application is successfully creating a socket pair with the port numbers and IP addresses you are expecting.

If the PING works but an application that did work before fails to connect, then the firewall settings might be the origin of the problem as it blocks traffic based on port numbers.

## 9.5 Checking the application layer

Beside bugs in the programming of the used application there could be problems with the DNS system. Check correct DNS resolving by using the NSLOOKUP command.

**Exercise 1:**

You are engaged at the helpdesk of “Duck enterprises”. Help the following users with their troubles. However the company owner Dagobert Duck wants to know every day what you have been working on, so document your work.

**Network information:**

company LAN	172.16.0.0 / 16
default gateway	172.16.255.254
DNS	12.168.254.254
No DHCP server	

User at PC#	trouble description
PC0	Help I have deleted the internet!
PC3	I can access the shared files of PC2 but I have no access to the enterprise websites.
PC1	I can access the shared files of PC0 but I have no access to the public enterprise website.
PC3	I can access the public enterprise website but not the intranet site.
PC2	I can ping the public enterprise webserver but still cannot access the website.
PC4	I can access the intranet enterprise website but not the public site.