
Computing Systems Worksheet 7

Introduction to TCP/IP utilities in Linux

Roz Wyatt-Millington

12th November 2021

This worksheet looks at some basics of TCP/IP based networks and how to determine information about the network connections within Ubuntu (Linux) as installed on the ARM Server and then runs the same experiments on the IMS PC to see the impact of being behind a proxy server.

Note that we use both the legacy IP tools (from net-tools package) but also the replacement commands from the ip tool which is the modern set of tools. This is best explained in Vitale 2011 which is a very good overview of the deprecated tools and the replacement commands. We use the legacy IP tools as they are either identical to or have close equivalent commands in Windows.

Directed Reading

The directed reading for this week can be found in Chapter 1 Tanenbaum & Wetherall (2013, pp. 1–88).

Tanenbaum, A. S. & Wetherall, D. J. (2013) **Computer Networks**. 5th. Pearson International Edition.

Vitale, D. (2011) **Deprecated Linux networking commands and their replacements**. URL: <https://dougvitale.wordpress.com/2011/12/21/deprecated-linux-networking-commands-and-their-replacements/>. (accessed: 17/01/2020).

Document conventions

Reminder of the conventions

- Information for you to read and understand is in this font.
- Information output by the PC or when discussing commands is shown in `this font`.
- Commands that you need to type into terminal is shown in **this font**.
- A control Character is indicated by prefixing a ^ character e.g. ^C means Control-C. To generate this on keyboard, hold down "Ctrl" and press "c".

1 Introduction

In this lab, you will learn about some of the TCP-IP diagnostic tools/utilities and some aspects of TCP/IP networks. We assume our network uses Ethernet at the lowest level with a unique Physical or Medium Access Control (MAC) address. If you change the network interface hardware, the MAC address changes which is unusable for maintainable communication. The number that is used to identify machines on the internet is the IP address. This is not very user friendly either. What everyone uses is the HOST name. Clearly translation is required:

HOST NAME → IP Address → MAC Address

HOST Name / IP Number mappings (pairs) are maintained by a file called HOSTS and/or by a Domain Name Server. The translation to MAC addresses is handled by the OS using the Address Resolution Protocol (ARP).

We are going to do the exercises twice to compare the differences between the ARM server and the IMS PC so you can see the impact of a proxy server on the way a network works.

2 Tasks - ARM Server

2.1 Network configuration

Task 1. Access ARM Server & look at legacy command

Login to the remote servers (if on bottom PC in IMS Lab or a Leeds Beckett PC on campus go to <https://guac.aet.leedsbeckett.ac.uk/guacamole/#/>). Refer to Worksheet 3 if you are unsure. Then go into the Linux ARM Desktop.

In this first set of exercise we will look at the use of the legacy command `ifconfig` and what it can tell us about the machine's connection to the network locally. Login to the Linux access from the link and go into the Linux ARM Desktop. Open a terminal window. In the terminal type in:

```
ifconfig
```

From the information returned by this command can you find the IPv4 address which will be in the dot decimal format and labelled `inet` for the main interface (probably labelled `eno1`). Write this down below:

Use the available “help” – i.e. `man ifconfig` to determine the optional argument to get `ifconfig` to display the information only for the main Ethernet interface. Then use it to fill in the following information about the ARM Desktop you connected to and its MAC address:

My PC's IPv4 Address: _____

IPv4 Subnet mask: _____

IPv4 broadcast address: _____

My PC's MAC address: _____

TX Queue Length: _____

Task 2. Using ip commands

Run the following command (replace `eno1` with your Ethernet interface name if it differs).

```
ip address show dev eno1
```

What information does this give? This command `ip` is the replacement for `ifconfig` – use `man ip` and `man ip address` to find out more. Note that `address` could be `addr` or `a` in command.

To find your default gateway in Linux you need to look at the routing table via the following command and find the line that starts default (the result of this command is to output the routing table for the PC to the terminal):

```
ip route show
```

Run this and record your default gateway IP address

Default Gateway Address: _____

2.2 IP & ICMP

The Internet Protocol(IP) is the base protocol on which the Internet rests – ALL information is conveyed in IP packets. There are a number of reasons why IP packets may not reach their intended destination. The designers of TCP/IP decided that some mechanism should provide feedback to the sender regarding non-delivery of IP packets – and other diagnostic information.

These facilities are provided by the Internet Control Message Protocol (ICMP). This protocol defines

a number of messages. ICMP is a user of IP — ICMP messages are conveyed directly in IP packets — but it is very closely linked with IP. In fact, implementations of TCP/IP are required to include ICMP in order to be compliant with Internet standards.

Task 3. Research on ICMP/IP packets

One ICMP message is the “echo-request” message. If this message arrives at the destination, the receiving ICMP protocol entity is required to return an ICMP “echo-reply” message to the originating ICMP protocol entity – both are carried inside IP packets.

Find out the “message type” and “code” of ICMP echo request and echo reply. You will find out the answer by searching online for IP and ICMP format.

IP packets contain a “time-to-live” (TTL) field. This can contain a maximum value of 255 as the field size is 8 bits, but is 64 by default in Linux. Every router on the Internet decrements the TTL value before forwarding an IP packet. If it decrements this to zero, it actually discards the packet rather than routing it. This avoids IP packets wandering around the Internet forever. When a router discards a packet for this reason it will also return an ICMP message meaning “TTL expired in transit” to the originating IP address to indicate that it did discard the packet. Find the message type and code for this:

2.3 Ping

This is a very useful tool. It works by sending ICMP “echo request” messages to a host (or hosts) and listening for the responses. Basic usage of this utility involves one of the following 2 routines:

- Pinging an IP address and verifying that the destination specified is responding – a response will confirm that IP packets can be sent to the destination.
- Pinging a host specified by its domain name ¹. This will also confirm the reachability (or otherwise) of the host as well as providing its IP number and confirming that the DNS database (or the local HOSTS file) contains appropriate entries.

PING displays on screen messages regarding the results. To communicate with another PC, both PCs need to be using the same network or be connected via the Internet. This is the theory, at least!

Unfortunately, System administrators sometimes switch off the ability to receive ICMP messages. This sad fact is a reflection of the need to protect networks from bombardment by malicious software. This means that you might find that a PING is unsuccessful because ICMP is blocked at the firewall

¹You will learn more about domain name subsystem (DNS) when you do more on networks in a later module

and NOT because the destination is unreachable. A common if crude method of DDoS attacks is to flood the IP address with ICMP messages

Task 4. Ping localhost

IPv4 address 127.0.0.1 provides a local loopback facility. You should always try pinging this first if you are using ping to investigate and isolate a network problem. A response confirms that the local (internal) network interface and TCP/IP protocol stack is operational.

In a terminal window type:

```
ping 127.0.0.1
```

This should effectively ping the PC you are on. In Linux (unlike Windows) the ping command goes on forever until stopped by using `^C` — in Windows only 4 pings are sent. What are the values for the average round trip time (RTT) and time-to-live (TTL) for this set of pings:

Average RTT:

Average TTL:

To send a default number of pings (for instance 4 as in Windows) you can use the following command - note here we use the domain name localhost as opposed to the IP address 127.0.0.1:

```
ping -c 4 localhost
```

What is the average RTT and TTL for this set of pings?

Average RTT:

Average TTL:

Task 5. Ping external addresses Now let us try pinging some computers external to the ARM server. Ping the following addresses 10 times and record the response:

- `www.leedsbeckett.ac.uk`

IP address:

Average RTT:

Average TTL:

- `www.bbc.co.uk`

IP address:

Average RTT:

Average TTL:

- `www.uni-bremen.de` University of Bremen in Germany

IP address:

Average RTT:

Average TTL:

- `www.ucla.edu` University of California, Los Angeles

IP address:

Average RTT:

Average TTL:

- `www.usu.edu` Utah State University

IP address:

Average RTT:

Average TTL:

What do you notice about the average round trip times? What is the reason for this variation in RTTs? What about the two US universities — how do they differ? Do you know what is happening?

Task 6. Questions to research and answer

Do these at end if you have time or outside of the timetabled session You will need the manual page for ping which can be obtained by typing:

`man ping`

Once you have worked out the commands try them to see what happens.

1. What is the default timeout — that is the time ping will wait for a reply? Using the manual page for ping can you work out how to change this value to 5 sec?

2. What is the default data field size in an echo request message? Using the manual page for ping can you work out how to change this value to give a total packet size of 128 bytes?

3. What is the default interval between echo requests being sent? Using the manual page for ping can you work out how to change this value to send pings every 2 seconds to an external address? How about to send 11 pings over a minute to an external address?

4. Using the manual page for ping can you work out how to change the TTL option? Now try tracing the route to `www.leedsbeckett.ac.uk` from the ARM Server by incrementing the TTL field by one each time and sending three pings each time until you get the response from the server at Leeds Beckett. Record the route and the RTT below:

The final question above shows how the principles of how the next command that you are going to use works - that is traceroute.

2.4 Traceroute

This is a command that enables you to trace the route between you and the server (IP address or domain name) and see where any possible issues are. It works literally by initially sending UDP datagrams (with an unlikely port number to prevent processing of datagrams) with a TTL of 1 — these generate a "time to live exceed" message from the first router between your PC and the target server. `traceroute` will print out to the terminal window the RTT for each echo reply along with the

server IP address and name (if found). Then three echo requests with a TTL of 2 are sent out to find the next router - and so on till the reply comes from the target server or the number of hops (default is 30) is exceeded. A lot of modern systems reject the UDP packets so can use other methods such as ICMP (-I flag) or TCP (tcptraceroute). However the Ubuntu installation on the ARM server only allows us to set the ICMP flag.

```
P:\>tracert 160.9.56.211

Tracing route to 160.9.56.211 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    10.81.2.3
  2     1 ms     1 ms     1 ms    172.29.36.10
  3     1 ms    <1 ms    <1 ms    160.9.56.211

Trace complete.
```

Figure 1: Traceroute Example

A typical trace route (on Windows not Ubuntu) that was sent from a lab PC (in JG207) to the university main website external IP address (in 2019-20) is shown in Figure 1. The first 2 addresses are private IP addresses – that is IPv4 addresses that are private to the Intranet and are therefore reused in many internal networks by companies etc. We know this as private addresses are in ranges:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

Private addresses are used so that the university does not need to have an IP address for each computer – just the DHCP routers that handle the address translation from the public address to private address. Something similar happens with a network inside a house where typically your ISP router has a 192.168.xxx.xxx address and acts as a dynamic host control protocol (DHCP) server within the home — the external IP address is given to the external interface of the router. DHCP is the TCP/IP protocol that can allocate IP addresses from the range given to the server to clients when they attach to the network.

It is common that some intermediate routers discard packets whose TTL has decremented to zero and don't return an ICMP message. This affects both ping and traceroute. Normally traceroute prints a line displaying information gleaned from the "TTL expired" messages it receives. Where it doesn't get one, it times out, prints a line with * * * filled fields and then carries on with an incremented TTL field in the next IP packet it sends.

Task 7. Internal traceroute example

Try running `traceroute -I 172.26.190.20` which uses ICMP requests to trace the route to the private (internal) IP address matching to `www.leedsbeckett.ac.uk` — if you found a different address when pinging above please use it. Record the route below

The switch `-I` tells the server to use ICMP messages rather than the default UDP messages of `traceroute` which are blocked at various points in Internet. What happens if you run the command `traceroute 172.26.190.20`?

Task 8. External traceroute examples We take fast internet for granted but you may reflect on how far you can reach and how quickly – USA (try `traceroute -I wm.edu`) Australia (try `traceroute -I uq.edu.au`) and Japan (try `traceroute -I www.hju.ac.jp`). Can you draw any conclusions about the routes messages take across the globe? Hint: screenshot the routes using Screenshot app in Ubuntu



2.5 Identifying PCs in LAN

Within a local area network (LAN), the individual machines are identified using their Ethernet address (more about this next week) which is also often called the physical address or MAC address. This is a 48 bit address which uniquely identifies a network interface card (NIC). The protocol that translates IP addresses to MAC addresses is the address resolution protocol (arp).

The basic idea is that if a computer (X) can connect directly to another computer (Y) on the LAN, it will keep both the IP Address and the MAC Address of Y in a table. To allow for the probability of Y becoming unavailable, the ARP table is refreshed frequently and unused entries are deleted. The host first uses the destination IP address to determine whether it can use the MAC address of the destination or must use that of a router directly connected to this subnet. If the required MAC address is not present in the arp table, the arp protocol is used to broadcast a request for the mac address corresponding to the appropriate IP address. The machine (router or host) with that IP address responds with its MAC address. All other machines on the subnet ignore the request. Note

that when a packet is being forwarded to a router, the Ethernet frame has the destination MAC address of the router but the IP packet has the final destination IP address not that of the router.

Task 9. ARP research questions

In which layer of the TCP/IP stack does ARP work?

As mentioned above ARP discovers the MAC address of a computer by sending a broadcast message (i.e. request sent to all computers). What is the “physical address” for a broadcast message?

Task 10. ARP basics

In a terminal type:

```
arp -a
```

Make a note of the number of computers listed in the table.

arp is another deprecated command in Linux and has been replaced by options to the ip command. Try:

```
ip n show
```

What do you see and how does it compare to the results of the arp -a command

Task 11. Network statistics

There are a number of commands in Linux (and Windows) that allow you to gather useful information about your PC's usage of the network. The first of these is the deprecated command `netstat`.

In a terminal type:

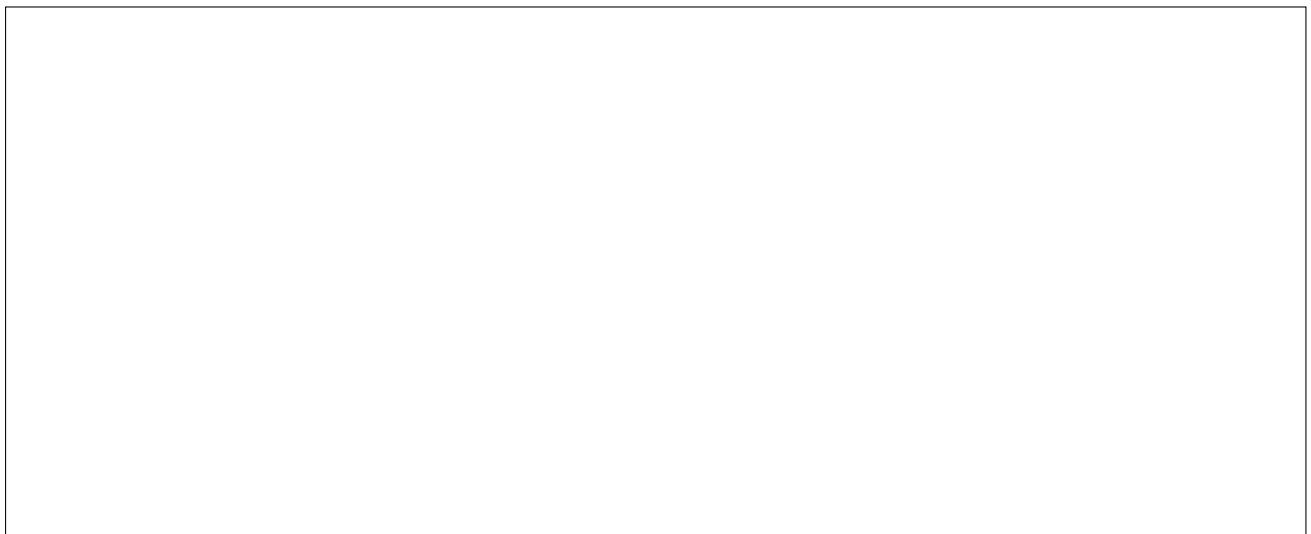
```
netstat -s
```

You will see counts of the number of packets sent and received by your PC using IP, ICMP, TCP, UDP, etc.

In order to look at this data it is easier to put the output to file which we do by using command:

```
netstat -s > /Documents/netstat.txt
```

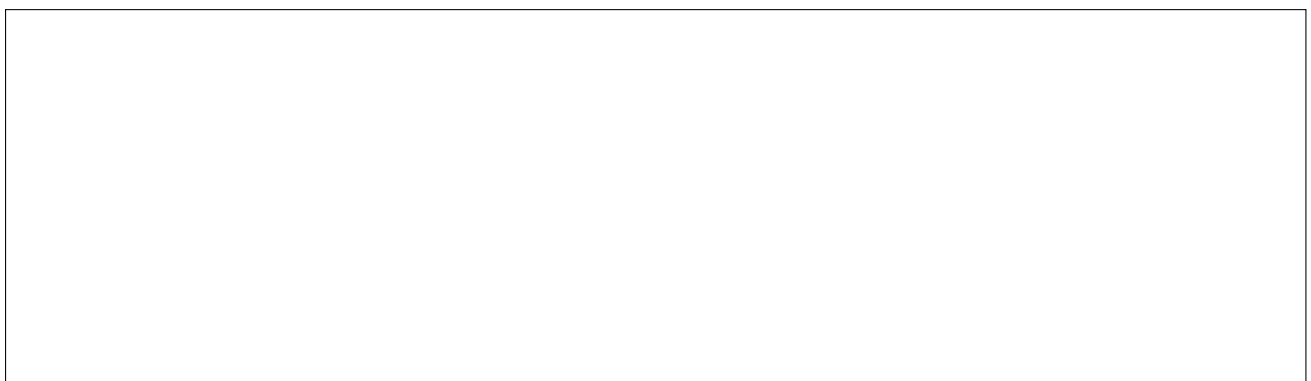
This puts the output of `netstat` into a file in your Documents folder called `netstat.txt`. Now look at this output in notepad and make notes on what you see:



In modern Linux `netstat` has been deprecated and replaced by `ss` which looks at the sockets active in the system. Try the command

```
ss -s
```

What is the response and how does it differ from the previous response from `netstat`? Look at the help file on `ss` (`man ss`) to learn more about this command.



We can also look at the data about what has been sent on a specific link. Type the following into a terminal (replace `eno1` by the name of your Ethernet link if different)

```
ip -s link show dev eno1
```

What are the results you see? Do you know what do they mean?

3 Summary

In this lab we have looked some basic utilities in Linux that can be used to investigate how the PC is connected to the network and routes that traffic takes. There are very similar commands that can be run in Windows (`ipconfig` for `ifconfig` and `tracert` for `traceroute`) to investigate the network links there. It may be beneficial to repeat this lab in Windows at some point. These utilities are very useful when you are trying to work out why a connection is not working or where it is losing data (`traceroute` is particularly useful here). If you run the commands as a super user in Linux or an Administrator in Windows you have much more flexibility and can use other methods than UDP or ICMP for `traceroute`.

With the IMS PC we saw the impact the proxy server has on accessing the external Internet — basically you cannot ping or `traceroute` to any computer outside of the IMS set-up