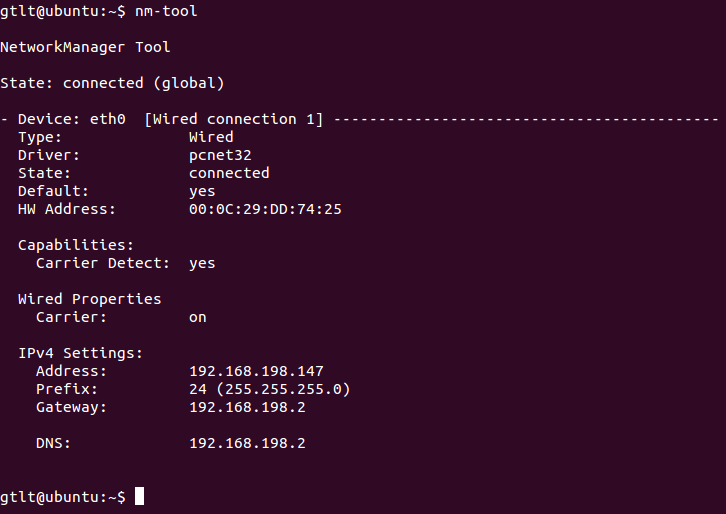
**DNS fundamentals**

1. In Linux, run the commands hostname and nm-tool and investigate the output. In Windows, run the command ipconfig /all and investigate the output.

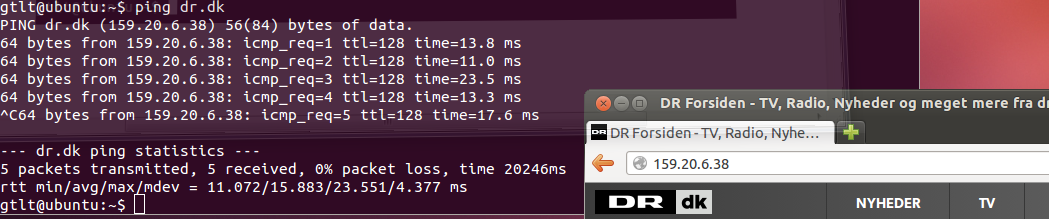
* nm-tool output: What does the Address field tell us?   
  **Tells us about the current internal IP-address for the device. The internal IP is an IP assigned for the device that is connected to a router.**
* nm-tool output: What does the Prefix field tell us?   
  **The prefix tells us, that the 24 first bits of IP address indicates the network and subnet. The subnet mask is 255.255.255.0**
* nm-tool output: What does the Gateway field tell us? **Tells us about the IP-address for the current host router.**
* nm-tool output: What does the DNS fields tell us? **Tells us which IP-address it connects to and makes a lookup when accessing the internet.**



1. In Linux or Windows, ping a webserver

* Try browsing the net by IP number and name using your browsers address field.

**Ping dr.dk, and you get IP 159.20.6.38.**



1. Host Lookup Table (HLT)

* Edit your HLT and redirect the name of a web server to IP address of another
* Is the HLT looked through before your primary DNS server is queried?
* Who first proposed the HLT? **Peggy Karp**
* When was the HLT proposed? **In 1971-1972**

1. What does TLD stand for? **TLD stands for “Top Level Domain”. TLD is like .com (dot com). The TLD names are installed in the root-zone of the name space.**
2. Why does a FQDN end with a dot, “.”? **Fully Qualified Domain Name is ended with a dot to show that it is a root server. Also to distinguish between relative and absolute domain.**
3. What is a DNS "A" record and what is it used for? **Used to control location of resources in the internet. Maps the domain name to the server IP-address.**
4. What is a DNS zone and what it is used for? [**http://en.wikipedia.org/wiki/DNS\_zone**](http://en.wikipedia.org/wiki/DNS_zone)

**Name resolution**

1. What is recursive and iterative name resolution? [**http://technet.microsoft.com/en-us/library/cc961401.aspx**](http://technet.microsoft.com/en-us/library/cc961401.aspx)
2. How may DNS caching be more effective in recursive vs. iterative resolution?
3. Why are client-side communication costs reduced in recursive name resolution?
4. Why does recursive resolution put higher performance demands on each name server?

**DNS security extensions**

1. What is DNSSEC and why is it needed? **DNSSEC (Domain Name System Security) is an extension to the existing DNS and makes the DNS more reliable. Purpose: make the authenticity of DNS records verifiable. Check the response, so it actually originates from the wished source.**
2. What is a signed zone? **Adding a digital signature to resource records in the zone file (RRSIGs).**
3. What common types of security vulnerabilities are hindered by DNSSEC?

**BIND DNS server**

1. Install BIND on a Linux machine and check the installation. **Follow the steps in the PDF Fischer\_ITONK\_BIND\_Setup.pdf.**
2. Configure a caching name server and forwarder
3. Use Google’s Name Bench to find a suitable public DNS server to forward to
4. Test and document that forwarding works as intended
5. Test and document whether the DNS lookup time is reduced by caching

**Prototype**

* Consider a concrete case, e.g. home, school, office, or hospital, where employing a caching name server and forwarder serves a realistic purpose
* How would you set up BIND in your case?
* What functionalities in BIND would you use?