Lab 04: DHCP

💡Have you ever had to manually configure an IP address when connecting to a wifi or cellular network? Of course not! Behind the scenes, DHCP has been taking care of you. This lab will illustrate how DHCP works and why it is a core service in any network with clients.

Objectives:

Install and configure Linux DHCP service on dhcp01.yourname.local.

Prerequisites:

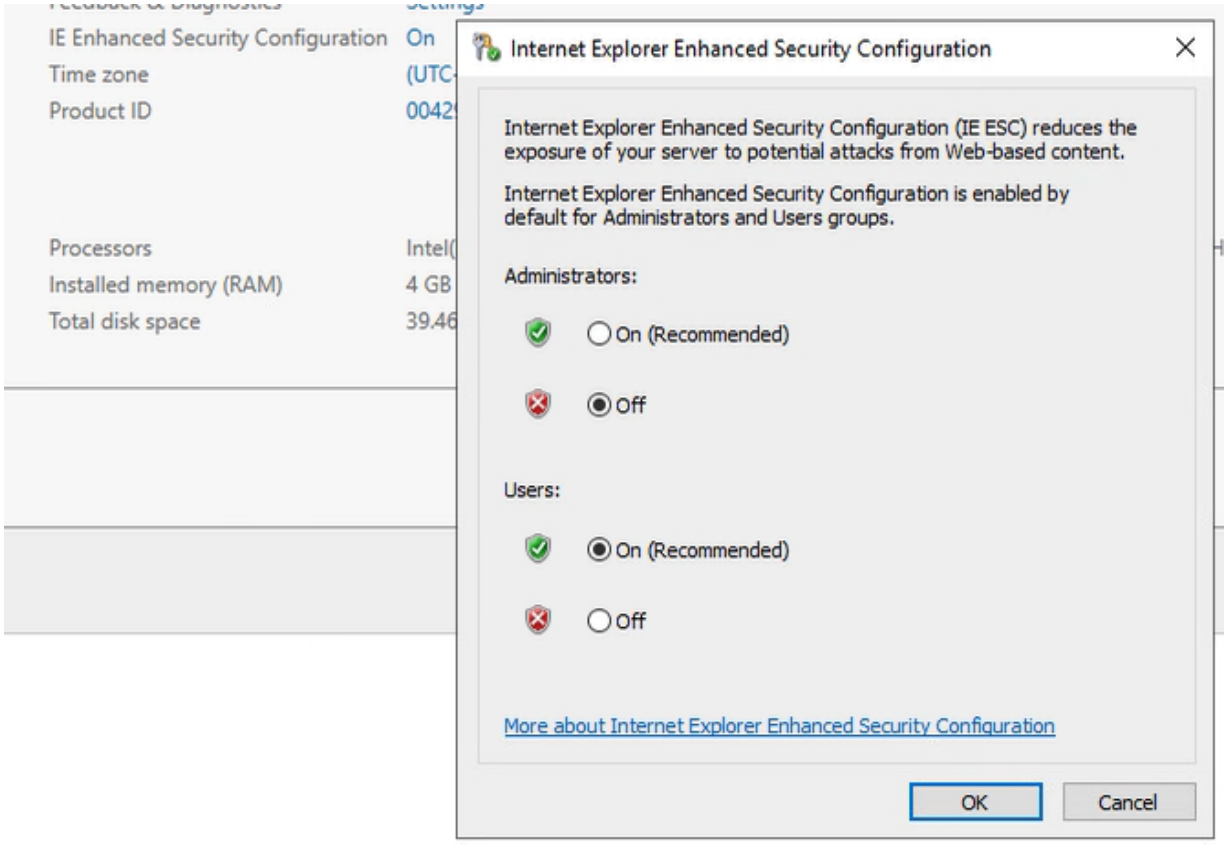
Lab 3 is complete, and the environment is in a happy state.

SSH from AD01 -> DHCP01

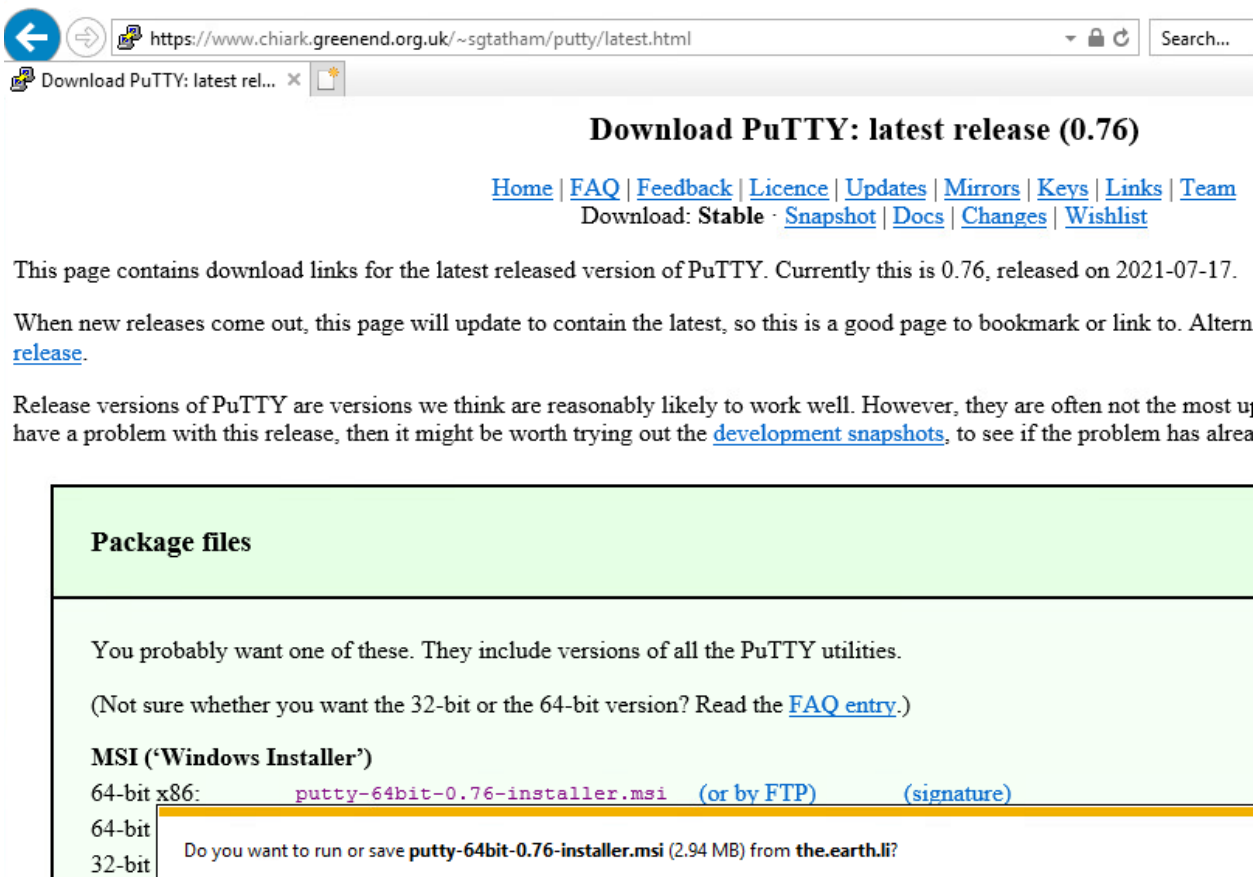
Disable IE Enhanced Security Configuration

💡Use either PuTTY (which you download + install) **or** Powershell SSH from AD01 to access your CentOS server from now on! This allows you to copy/paste from your Windows system (you can login into Canvas from here). You can open up multiple windows should you wish.

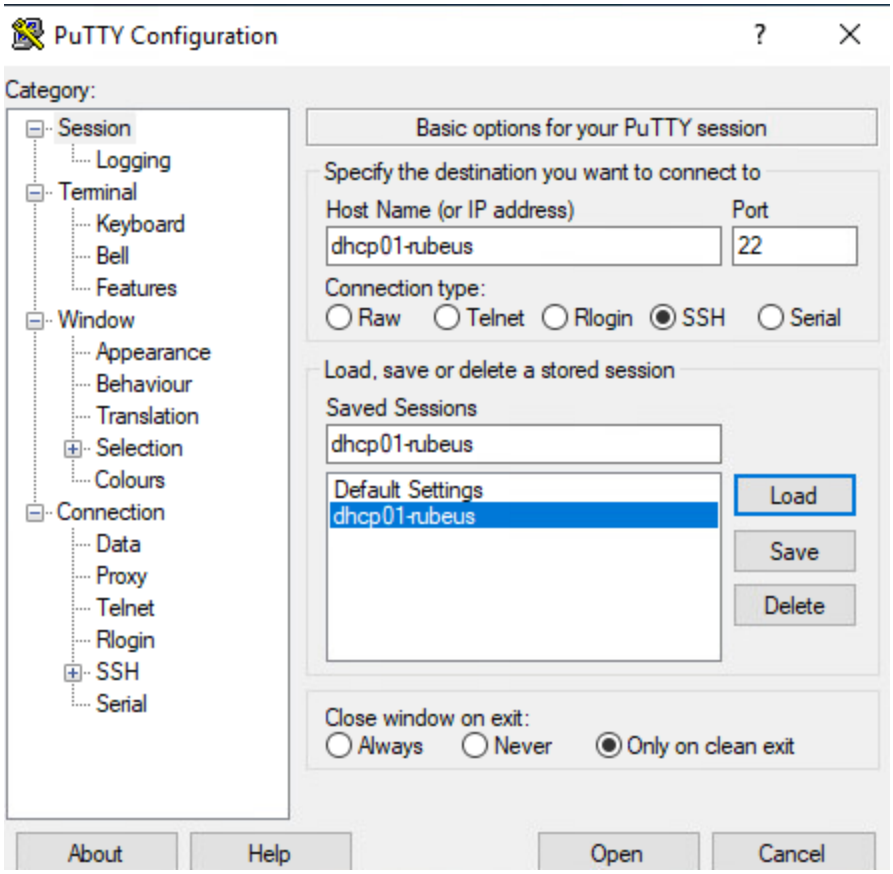
Note: Powershell SSH is somewhat newer, and you may experience occasional keyboard issues. If this is the case, move to PuTTY. In order to pull down PuTTY from the internet, you will want to disable IE Enhanced Security Configuration on Server Manager as shown below:

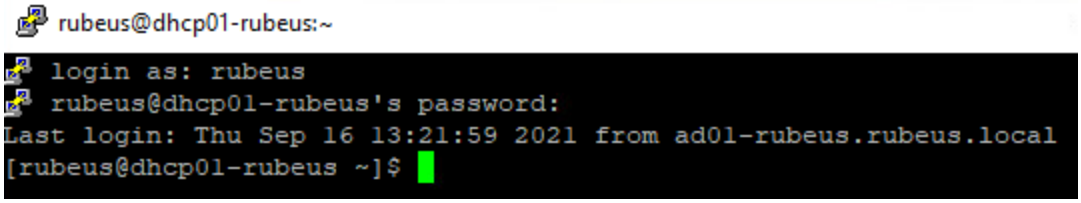


Install PuTTY


https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
Search...
Download PuTTY: latest rel...
Download PuTTY: latest release (0.76)
Home | FAQ | Feedback | Licence | Updates | Mirrors | Keys | Links | Team
Download: Stable · Snapshot | Docs | Changes | Wishlist
This page contains download links for the latest released version of PuTTY. Currently this is 0.76, released on 2021-07-17.
When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Altern
release.
Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most u
have a problem with this release, then it might be worth trying out the development snapshots, to see if the problem has alrea
Package files
You probably want one of these. They include versions of all the PuTTY utilities.
(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)
MSI ('Windows Installer')
64-bit x86: putty-64bit-0.76-installer.msi (or by FTP) (signature)
64-bit
32-bit
Do you want to run or save putty-64bit-0.76-installer.msi (2.94 MB) from the.earth.li?

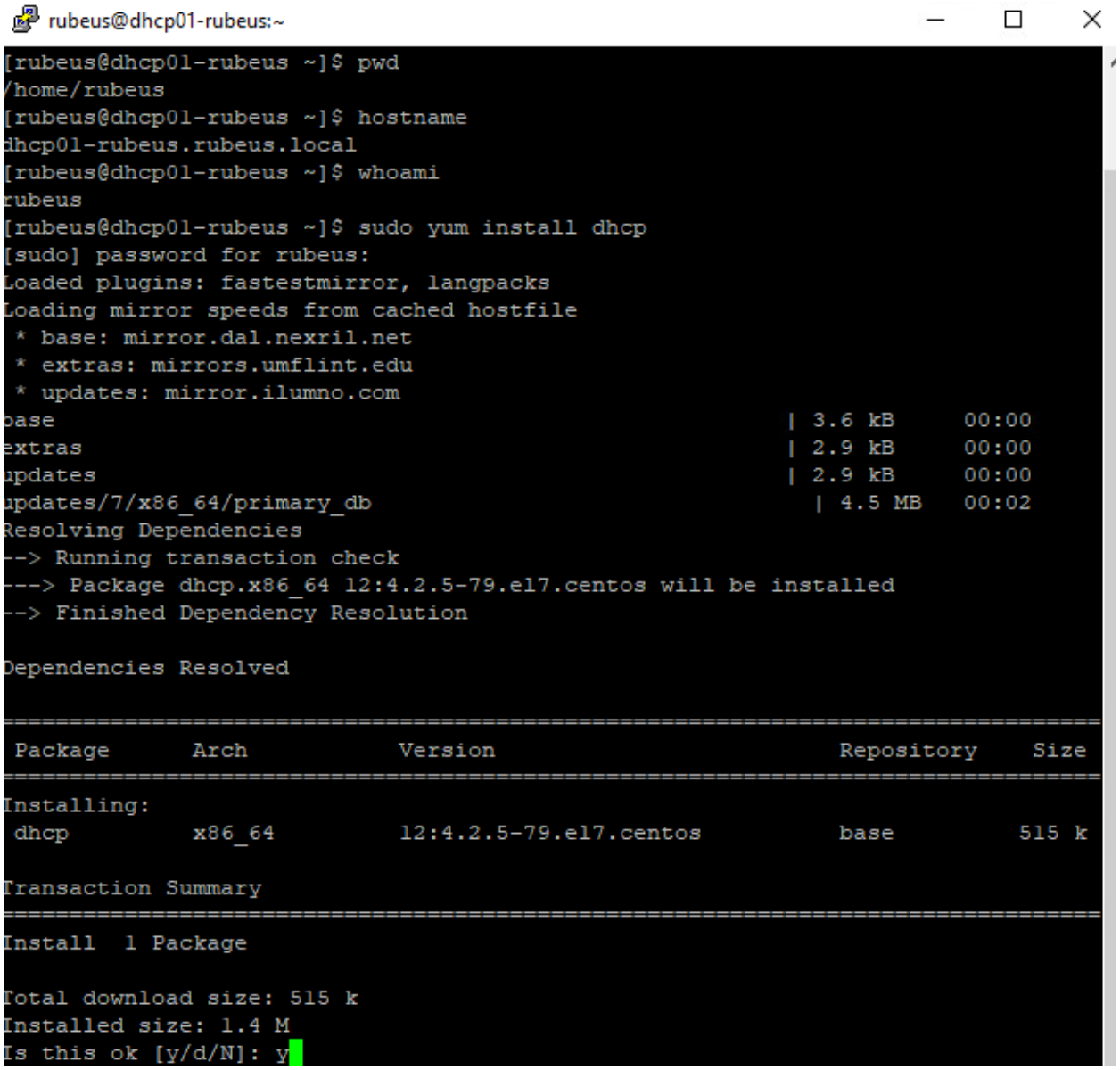
Connect via PuTTY





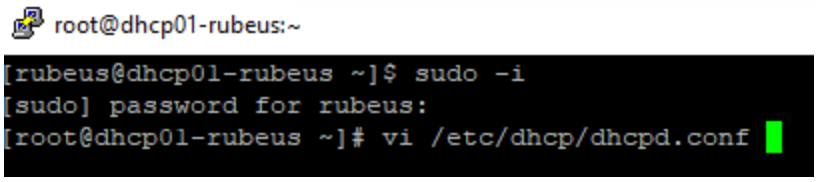
Install DHCP Services

We are going to use the yum update manager to install DHCP on this server with your elevated user.



Configuring DHCP Services

Become the system user for a brief period of time using the sudo -i command, and then open the dhcp configuration file using the vi or nano text editor (nano may be easier, but at some point you will need to learn vim so we will use it).



Typing very carefully, enter the following into your new file below the comments (# denotes a comment). Change the domain-name to yourname.local.

root@dhcp01-rubeus:~

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
subnet 10.0.5.0 netmask 255.255.255.0 {
        option routers 10.0.5.2;
        option subnet-mask 255.255.255.0;
        option domain-name "hermione.local";
        option domain-name-servers 10.0.5.5;
        range 10.0.5.100 10.0.5.150;
}
```

When you think you are done, write changes to save and quit vi.

Starting DHCP Services

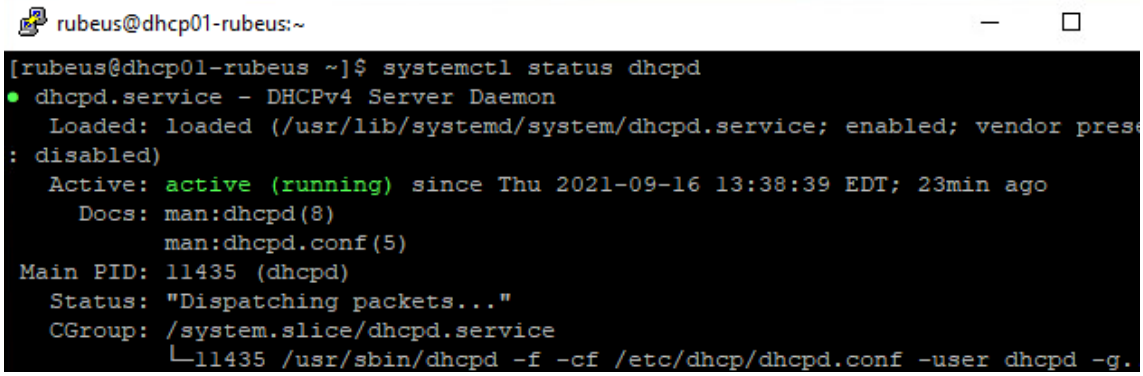
💣Whenever you change or create a service configuration file, you generally need to start or restart the service involved. This fact trips up many Linux administrators!

The systemd control program systemctl is how you start, stop and status services.

To start dhcp, type the following as root:

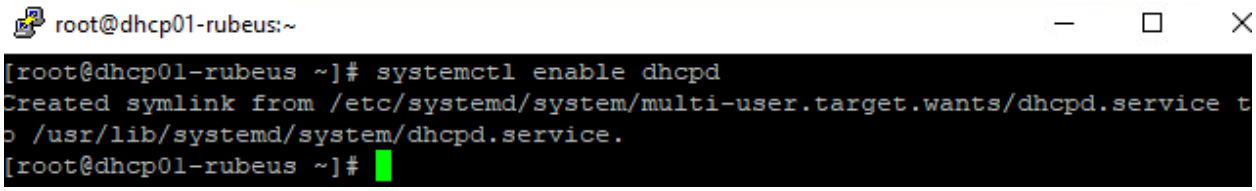
```
systemctl start dhcpd
```

Start dhcpd and check its status (Fun fact: the dhcp**D** means it's a Daemon, which is Linux speak for Service). Note any errors and check the syntax of dhcpd.conf accordingly.



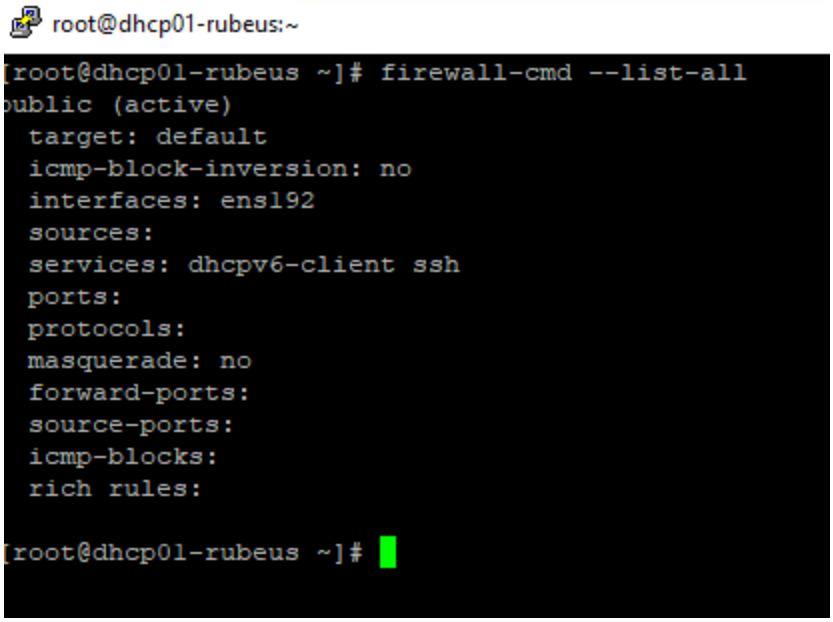
Enabling the service to start at boot.

💣Forgetting to enable a service to start on boot will cause the service to fail when the system is rebooted. Remember this if a service worked fine one day and does not after a reboot.



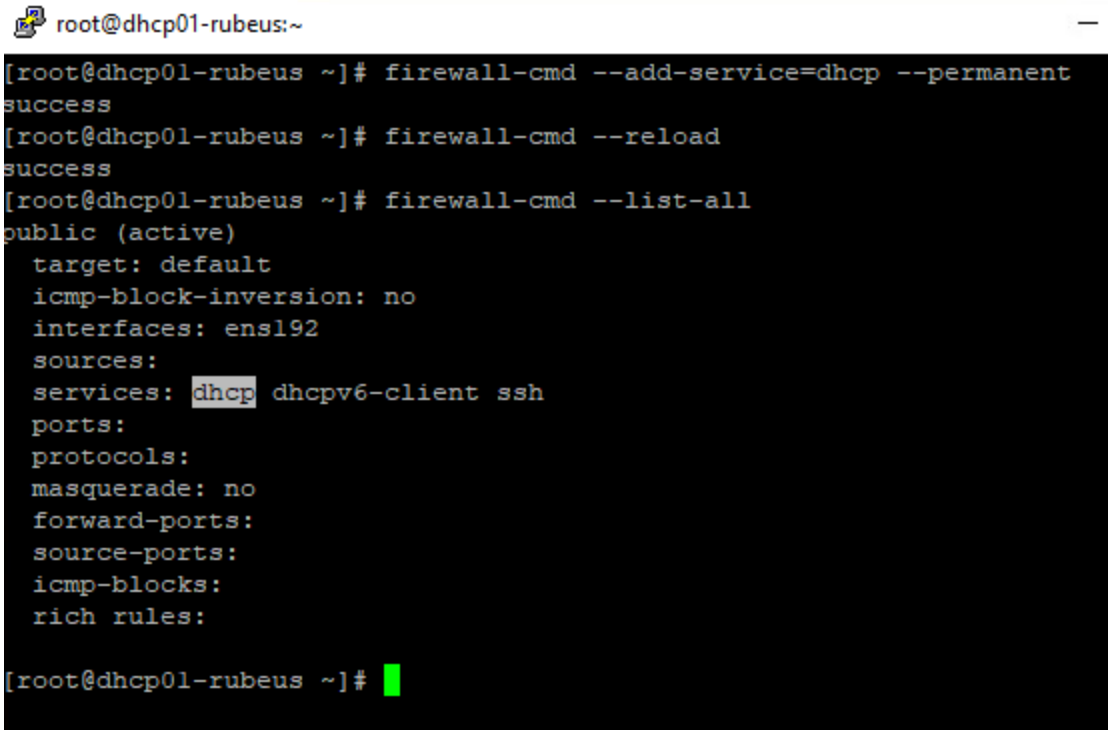
Configuring the Firewall to allow incoming DHCP requests

The default configuration on CentOS is to enable the firewall and allow both ICMP and SSH requests in. The DHCP server will not work until we enable the firewall. We will be using firewalld and the firewall-cmd utility to make this happen. The “firewall-cmd --list-all” option shows the default firewall that allows dhcpv6-client (not to be confused with dhcp server) and ssh. We will add the dhcp service (as opposed to its ports).

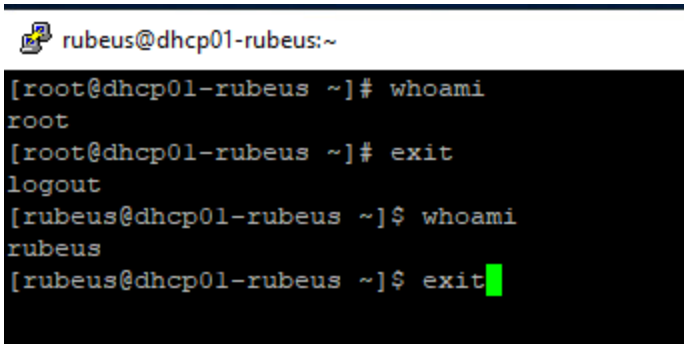


The following syntax adds the ports associated with dhcp permanently. The --permanent flag is important. If you fail to add this, the next time you reboot, your changes will be lost. Make sure you reload the firewall to invoke the change. List all the rules and make sure your dhcp service has been added.

💣Don't forget the --permanent flag, nor forget to reload the firewall!

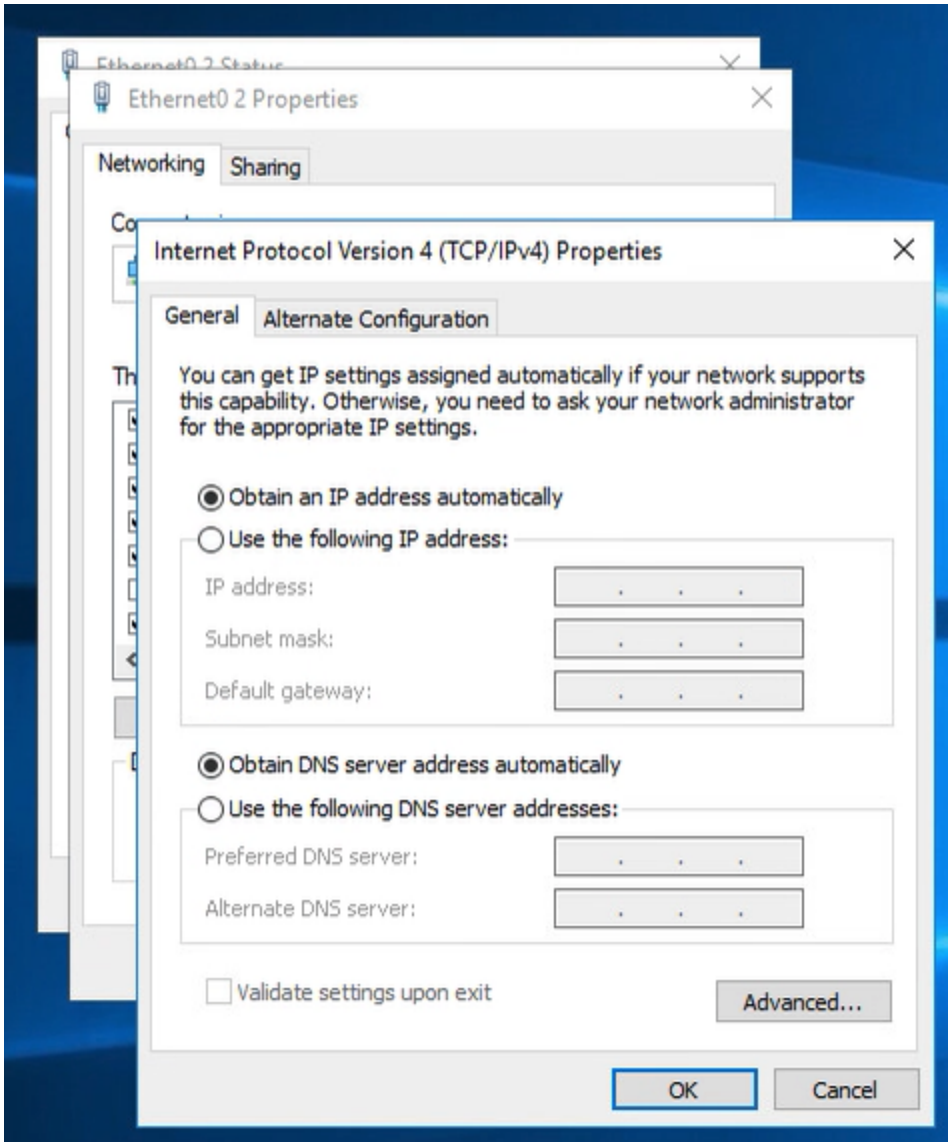


Type exit to leave your elevated state and exit again to exit PuTTY.



Windows 10 DHCP Client

As a privileged user, you will now re-configure networking on WKS01 to use dynamic addressing rather than static addresses.

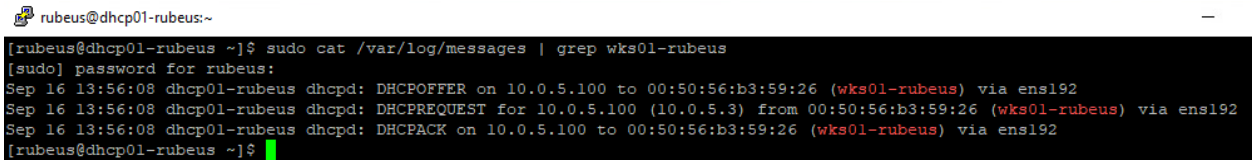

Ethernet0 2 Properties
Networking
Sharing
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Deliverable 1. Take a snapshot of the results of ipconfig /all. Note the DHCP server of 10.0.5.3 should be there, your IP address should be the first IP address in the scope you set earlier. Your domain name, netmask and gateway should also be set correctly.

```
PS C:\Users\rubeus.hagrid-adm> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : wks01-rubeus
   Primary Dns Suffix  . . . . . . . : rubeus.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : rubeus.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : rubeus.local
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B3-59-26
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.5.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, September 16, 2021 1:55:57 PM
   Lease Expires . . . . . . . . . . : Friday, September 17, 2021 1:55:57 AM
   Default Gateway . . . . . . . . . : 10.0.5.2
   DHCP Server . . . . . . . . . . . : 10.0.5.3
   DNS Servers . . . . . . . . . . . : 10.0.5.5
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Users\rubeus.hagrid-adm>
```

Deliverable 2. Log back into dhcp01 and find the DHCP log associated with wks01's request for DHCP information. Take a snapshot similar to the one below. The IP address, the workstation name, the layer 2 address should all match between deliverables 1 and 2.

The following command below looks complex, but let's break it down:
sudo = raises our privileges because /var/log/messages is owned by the root user.
cat = writes the file /var/log/messages to the screen
| = Called 'pipe', & sends the output of the previous command to the next command
grep wks01-yourname = filters input for the string 'wks01-yourname'.



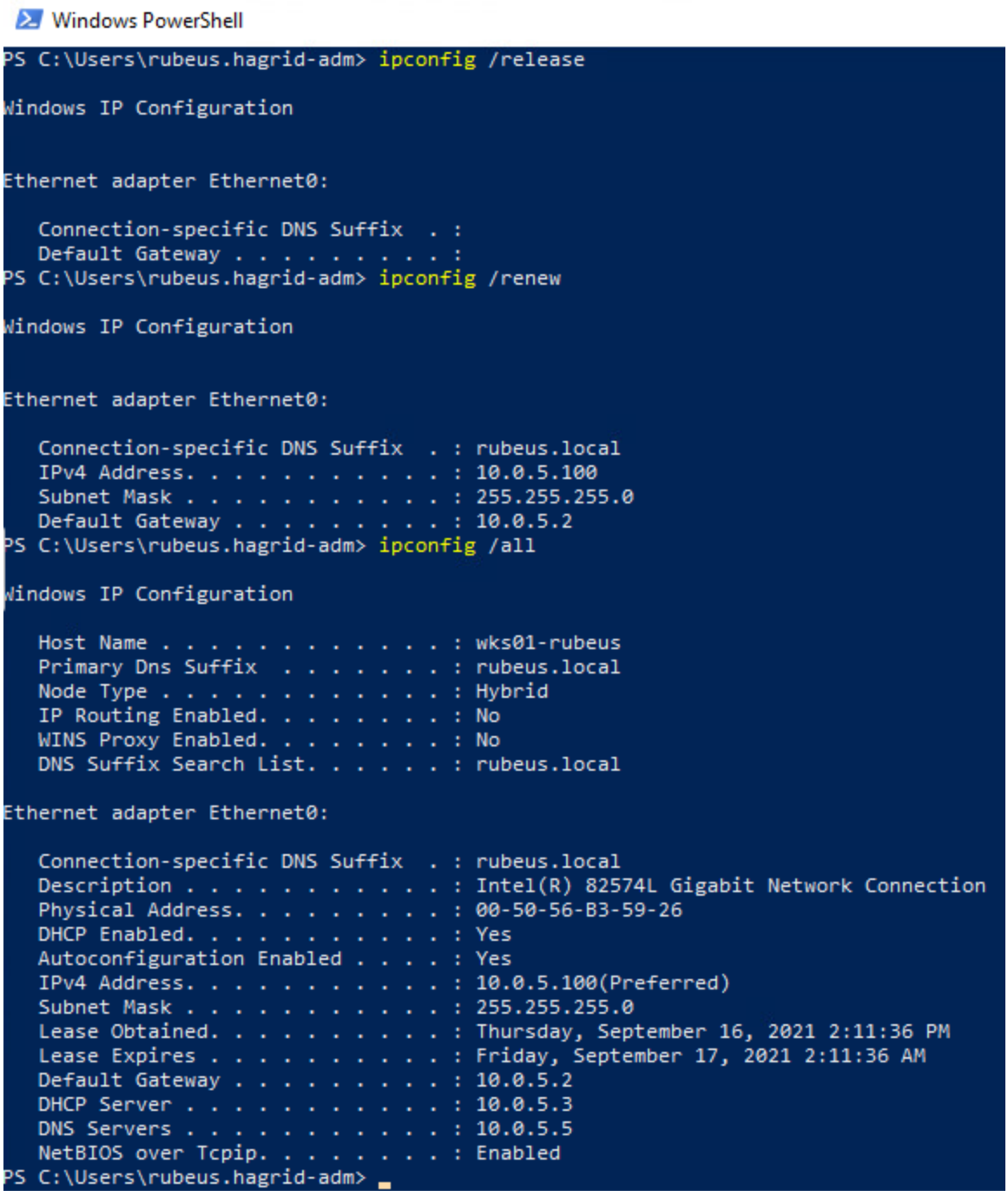
Wireshark

Run a capture session against WKS01's Ethernet0 adapter.

As an administrative power user (-adm), release the current DHCP release and then renew it on WKS01. Your objective: Capture the four DHCP messages between client and server.

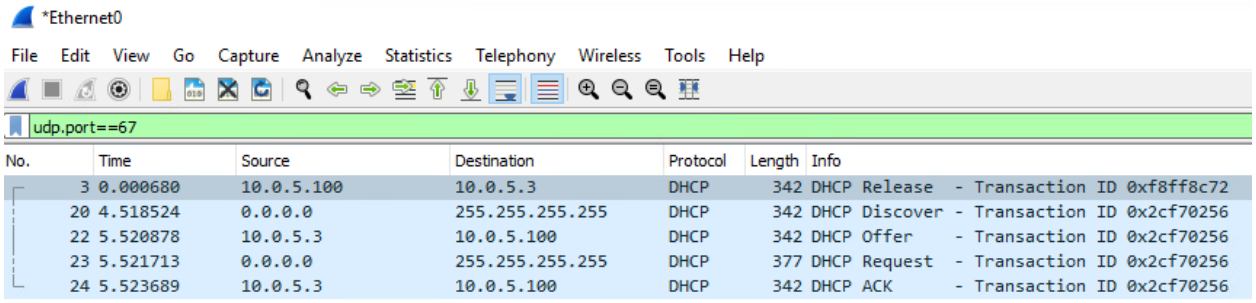
You release your current DHCP release using the following command:

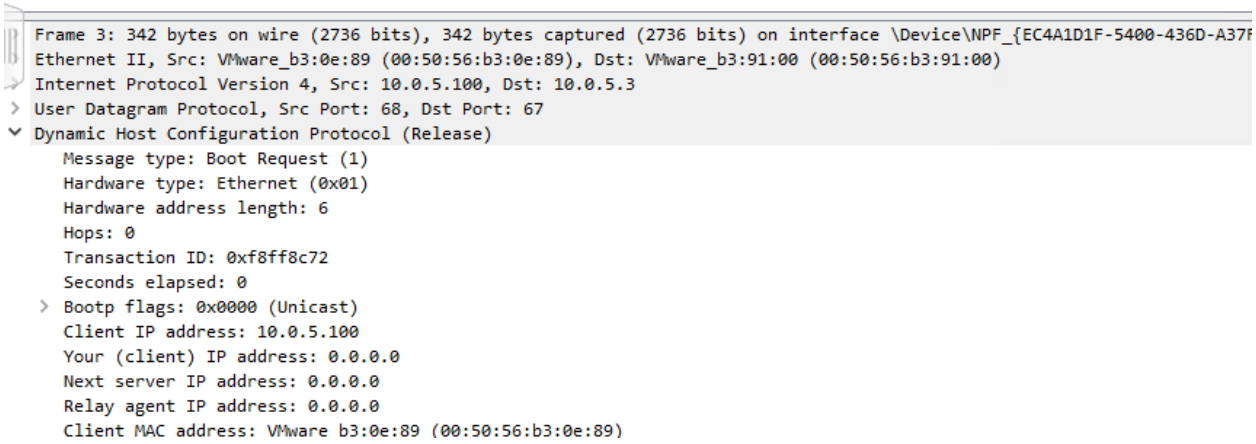
```
ipconfig /release
```



Stop the capture and create a Wireshark display filter that shows UDP traffic sourced or destined to port 67. Browse each of the four messages to get a handle on source, destination addresses (layer 2 & layer 3) and ports and the sequence of messages used to provide WKS01 another leased IP address.

Deliverable 3. Provide a screenshot similar to the one below that shows the 4 Key DHCP Messages.





Leveling Up

Deliverable 4. Figure out how to change the default lease time given to dhcp clients to 1 hour with a max lease time of four hours. Provide a screenshot displaying the new configuration, along with the shot confirming the change.

Deliverable 5. Tech Journal Entry - Explore 3 other items related to DHCP, and dig into their related Wireshark captured packets.