COMP311
Linux OS Laboratory
Lab12. Security and Networking Concepts

By

Alaa’ Omar

جامعة بيرزيت

BIRZEIT UNIVERSITY

Objectives

1

Understand through example the importance and usage of set user id (suid) and set group id (permissions) in Linux

2

Set and modify suid and sgid values on Linux files.

3

Identify and learn some Linux networking tool basics..

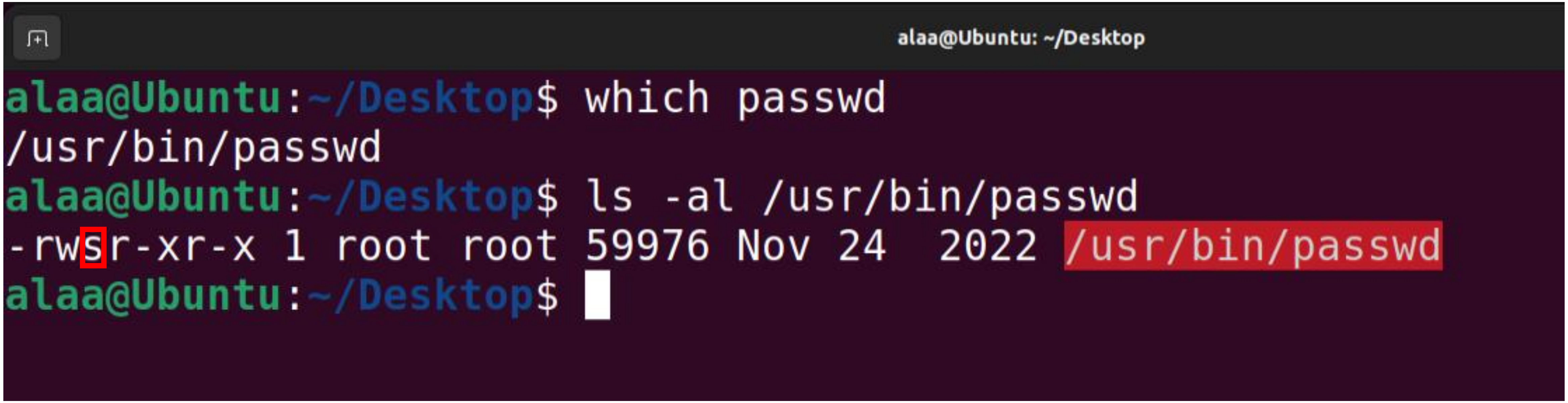
Suid and Sgid

- Linux systems are very secure and have multiple levels of security that takes volumes to discuss. We have already talked about a part of one of those security levels which is **file security** where we explained the permissions (mode) and how they are used to control who can access and use files and directories.
- The permissions we talked about were the **read (r), write (w), and execute (x)**. In this lab we will present a less obvious, but very powerful permission called the **setuid (set user id) and setgid (set group id)** permission usually referenced with an (s) permission.

Source: Learning bash shell book

Set User Id (suid) Permission

To understand how the suid permission is used let’s take an example based on the passwd command which we use to change our passwords. Run the following commads



```
alaa@Ubuntu:~/Desktop$ which passwd
/usr/bin/passwd
alaa@Ubuntu:~/Desktop$ ls -al /usr/bin/passwd
-rwsr-xr-x 1 root root 59976 Nov 24  2022 /usr/bin/passwd
alaa@Ubuntu:~/Desktop$ 
```

The (s) on the user part of the mode is the suid. This (s) is very important and without it a user will not be able to change his/her password.

Set User Id (suid) Permission

When a command such as passwd is executed, a process is created as explained in lab 6. That process has many properties. Four of those are:

- real uid (real user id)
- real gid (real group id)
- effective uid (effective user id)
- effective gid (effective group id)

- The real uid and gid are the same as the username and group of the user executing that command. The effective uid is the same as the real uid and the effective gid is the same as the real gid except when there is an (s) permission. In this case the effective uid will be same as the owner of the file and the effective gid will be same as the group name on the file.

Set User Id (suid) Permission

- The process resulting from running the passwd command has an effective uid as root (owner of the file passwd) which is why this command is able to open and modify files (e.g. /etc/passwd and /etc/shadow files) which the user running the command is not allowed to.
- This gives great flexibility by giving regular users the ability to access files through running commands which they cannot access normally.

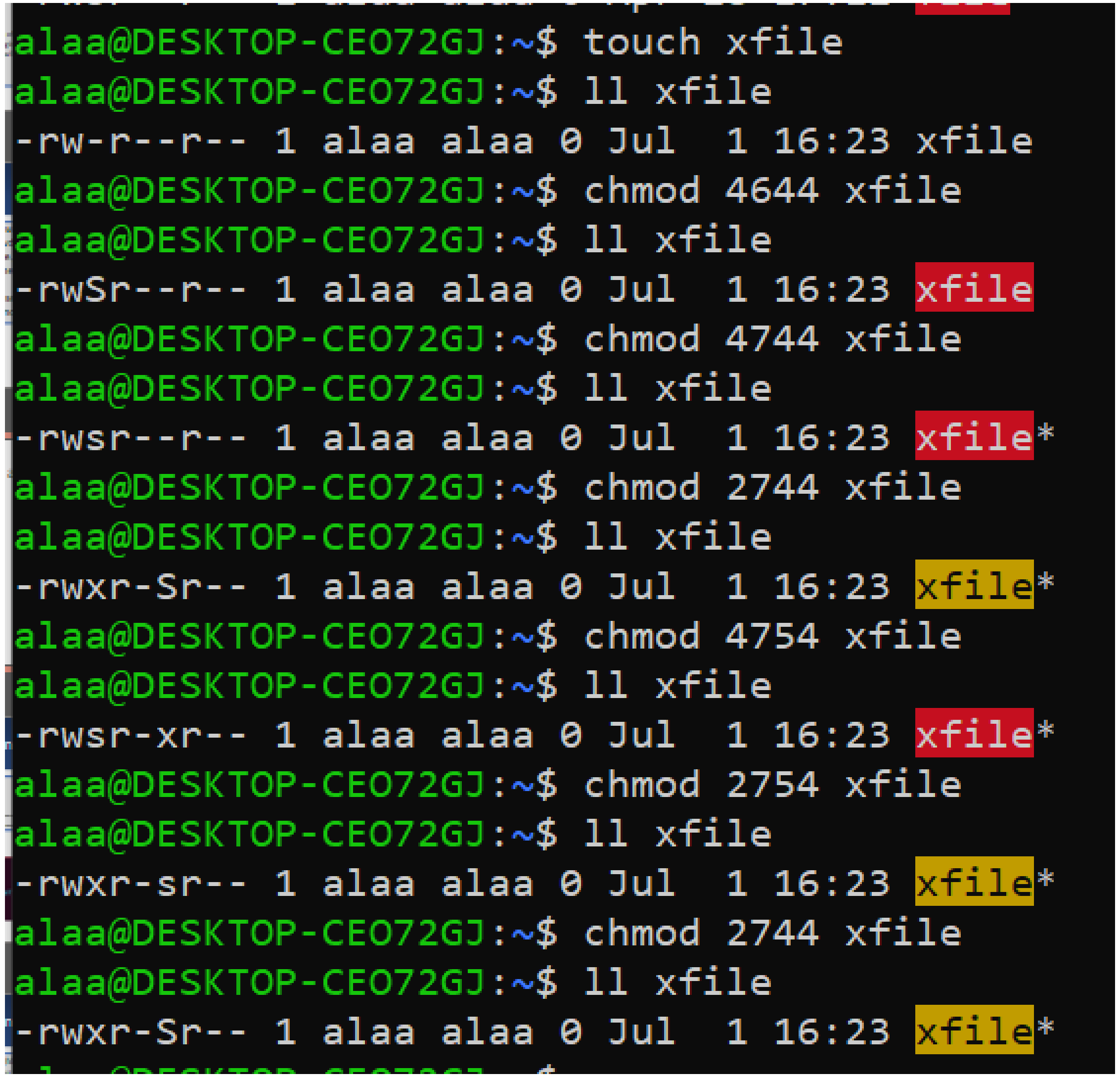
Methods of setting the suid, and guid bit

- Numeric method

Special permission	Number
suid	4
guid	2
Suid+guid	6

- Permissions values

symbole	Number
read	4
write	2
execute	1

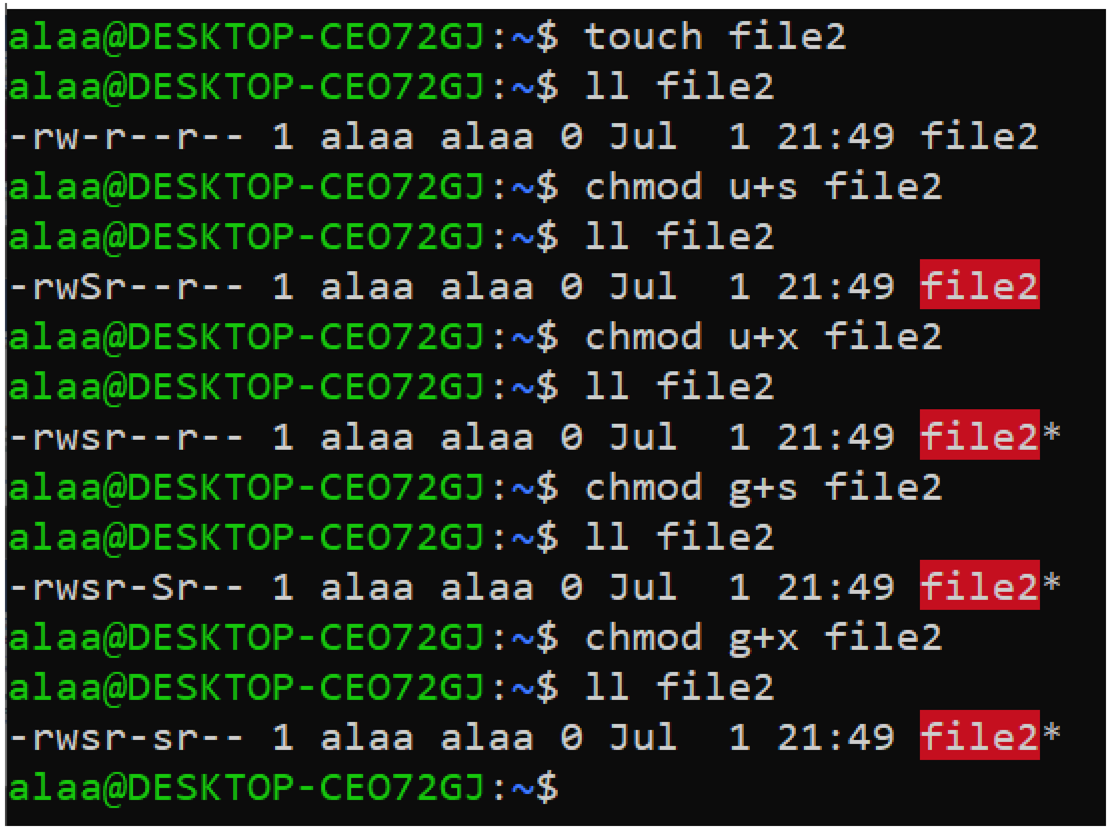


```
alaa@DESKTOP-CEO72GJ:~$ touch xfile
alaa@DESKTOP-CEO72GJ:~$ ll xfile
-rw-r--r-- 1 alaa alaa 0 Jul  1 16:23 xfile
alaa@DESKTOP-CEO72GJ:~$ chmod 4644 xfile
alaa@DESKTOP-CEO72GJ:~$ ll xfile
-rwSr--r-- 1 alaa alaa 0 Jul  1 16:23 xfile
alaa@DESKTOP-CEO72GJ:~$ chmod 4744 xfile
alaa@DESKTOP-CEO72GJ:~$ ll xfile
-rwsr--r-- 1 alaa alaa 0 Jul  1 16:23 xfile*
alaa@DESKTOP-CEO72GJ:~$ chmod 2744 xfile
alaa@DESKTOP-CEO72GJ:~$ ll xfile
-rwxr-Sr-- 1 alaa alaa 0 Jul  1 16:23 xfile*
alaa@DESKTOP-CEO72GJ:~$ chmod 4754 xfile
alaa@DESKTOP-CEO72GJ:~$ ll xfile
-rwsr-xr-- 1 alaa alaa 0 Jul  1 16:23 xfile*
alaa@DESKTOP-CEO72GJ:~$ chmod 2754 xfile
alaa@DESKTOP-CEO72GJ:~$ ll xfile
-rwxr-sr-- 1 alaa alaa 0 Jul  1 16:23 xfile*
alaa@DESKTOP-CEO72GJ:~$ chmod 2744 xfile
alaa@DESKTOP-CEO72GJ:~$ ll xfile
-rwxr-Sr-- 1 alaa alaa 0 Jul  1 16:23 xfile*
```

Methods of setting the suid, and guid bit

- For knowledge only
- Don’t use in exams

- Relative method

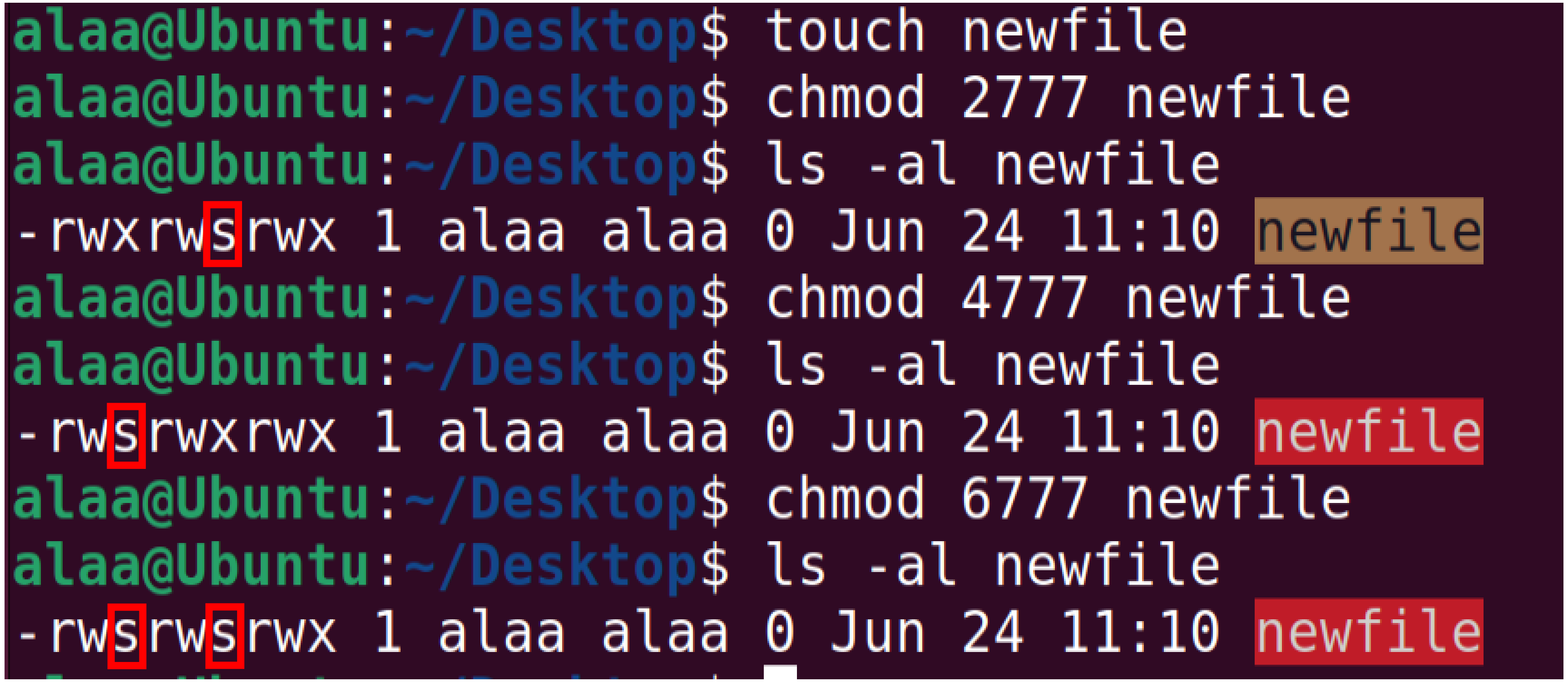


```
alaa@DESKTOP-CEO72GJ:~$ touch file2
alaa@DESKTOP-CEO72GJ:~$ ll file2
-rw-r--r-- 1 alaa alaa 0 Jul  1 21:49 file2
alaa@DESKTOP-CEO72GJ:~$ chmod u+s file2
alaa@DESKTOP-CEO72GJ:~$ ll file2
-rwSr--r-- 1 alaa alaa 0 Jul  1 21:49 file2
alaa@DESKTOP-CEO72GJ:~$ chmod u+x file2
alaa@DESKTOP-CEO72GJ:~$ ll file2
-rwsr--r-- 1 alaa alaa 0 Jul  1 21:49 file2*
alaa@DESKTOP-CEO72GJ:~$ chmod g+s file2
alaa@DESKTOP-CEO72GJ:~$ ll file2
-rwsr-Sr-- 1 alaa alaa 0 Jul  1 21:49 file2*
alaa@DESKTOP-CEO72GJ:~$ chmod g+x file2
alaa@DESKTOP-CEO72GJ:~$ ll file2
-rwsr-sr-- 1 alaa alaa 0 Jul  1 21:49 file2*
alaa@DESKTOP-CEO72GJ:~$
```

Adding (s) Permission

To add the s permission to your files, use the chmod command with four digits instead of three as before, for example:
create a file called newfile (touch newfile).
chmod 2777 newfile
What permissions are now on file newfile? ___________________________________.
chmod 4777 newfile
What permissions are now on file newfile? ___________________________________
chmod 6777 newfile
What permissions are now on file newfile? ___________________________________
As you can see adding an even digit (2 or 4 or 6) will put (s) on group, user, or both respectively.

Adding (s) Permission



```
alaa@Ubuntu:~/Desktop$ touch newfile
alaa@Ubuntu:~/Desktop$ chmod 2777 newfile
alaa@Ubuntu:~/Desktop$ ls -al newfile
-rwxrwsrwx 1 alaa alaa 0 Jun 24 11:10 newfile
alaa@Ubuntu:~/Desktop$ chmod 4777 newfile
alaa@Ubuntu:~/Desktop$ ls -al newfile
-rwsrwxrwx 1 alaa alaa 0 Jun 24 11:10 newfile
alaa@Ubuntu:~/Desktop$ chmod 6777 newfile
alaa@Ubuntu:~/Desktop$ ls -al newfile
-rwsrwsrwx 1 alaa alaa 0 Jun 24 11:10 newfile
```

Adding (s) Permission

What command would you use to set the permissions on newfile to:

1. r_s_wxrwx ____

2. r_xrwsr___ ____

3. rwSrwsr___ ____

Networking

As users we are not allowed to modify network setups, but we can view some information on how networks are configured on Linux.

Run the command:

/sbin/ifconfig

What is the ip address (inet) of your machine?

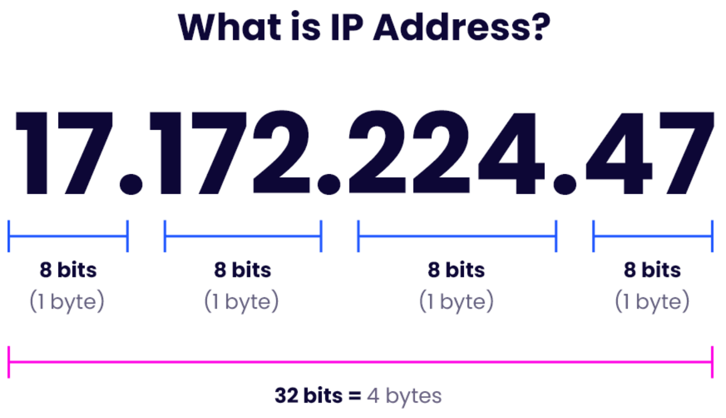
____

What is the MAC (HWaddr) address of your machine?

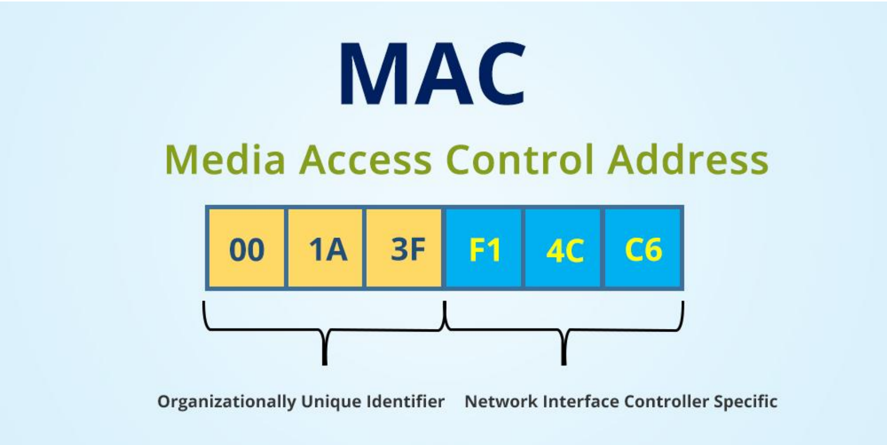
____

What is the netmask used by your machine?

____



https://www.ipxo.com/blog/what-is-an-ip-address/


MAC
Media Access Control Address
00
1A
3F
F1
4C
C6
Organizationally Unique Identifier
Network Interface Controller Specific

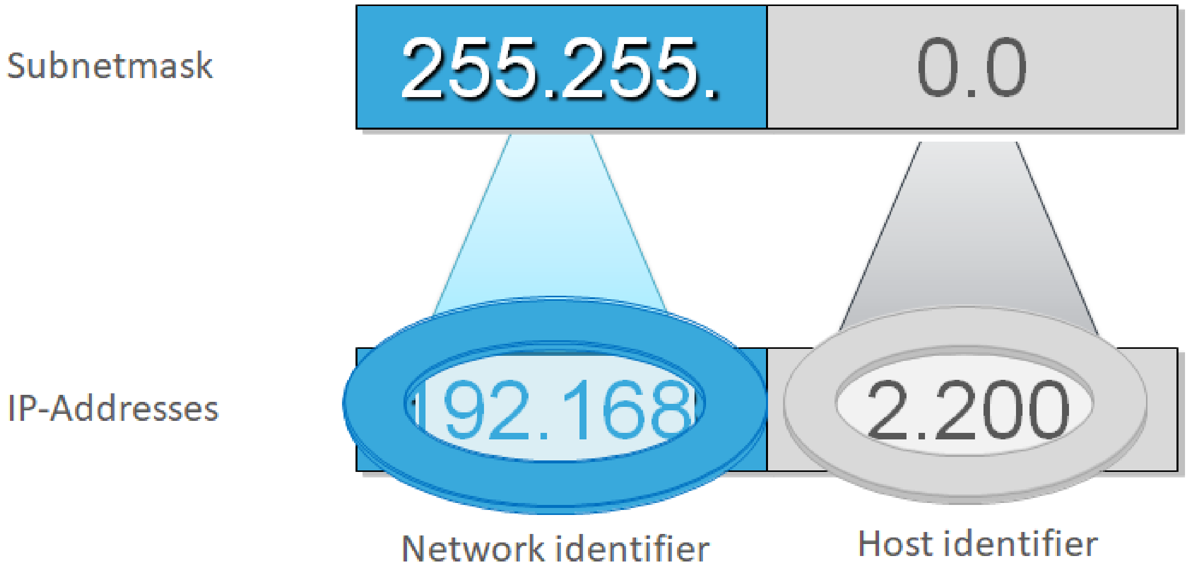
https://community.fs.com/blog/switch-mac-address-whats-it-and-how-does-it-work.html

Networking

Run the command

/sbin/route

What is the default gateway?



https://service.snom.com/display/wiki/Subnet+Masks

Networking

Run the command:

```
/bin/netstat -n | grep 23
```

This will give information about the telnet connections made to/from the system.

List the quad (Socket Connection) for your telnet connection:

____.

The End