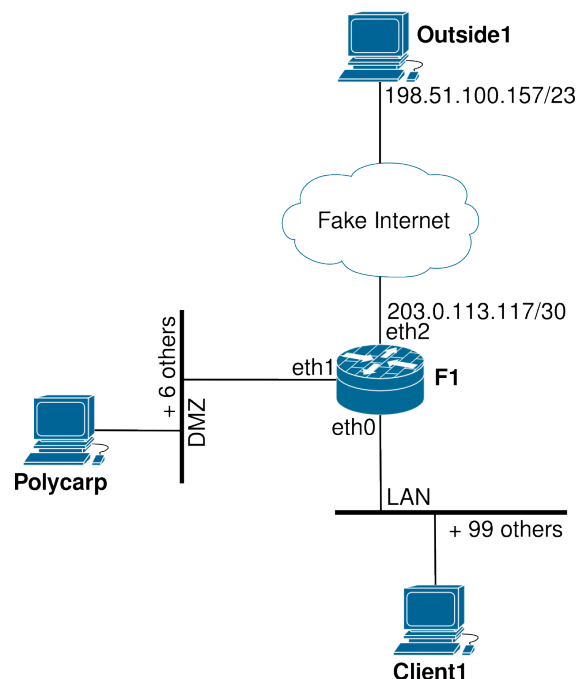# Subnetting

COSC301 Laboratory Manual

This lab is actually run as a class-tutorial. Thus, when we come to do this tutorial, everyone should do it at the same time. In this tutorial, we shall learn about subnetting, mostly in IPv4, but we shall also cover IPv6, which is easier. IPv4 is a bit more challenging, largely because we have to deal with conversions between decimal and binary a lot, but the concepts are otherwise identical.

As part of this tutorial, you will be given a set of questions. These questions are very similar in style to what you would find in any networking examination, whether it be a professional certification (such as a Cisco CCNA), or for this paper. The content of this tutorial is vendor inspecific: everyone in the networking field needs to know this.

This tutorial and the following firewall lab will use the IPv4 addressing scheme you have developed in this tutorial. The (quite small) network we shall be addressing is shown in Figure 1, "Network Map for this Laboratory".

Figure 1. Network Map for this Laboratory

The network that we shall be subnetting. You shall later use the addressing scheme when we implement this network in a the next lab.

The external network will be similar to the Internet, but several orders of magnitude smaller and not as complete. There is a single host on the external network, with a very different public IP address (as you would expect with a distant host on the Internet.) As we are modelling the Internet (and we use the term "model" very loosely here,) the hosts are not using RFC1918 private "non-routeable" addresses. Generally, you should never make up addresses in this way; we just want you to have some experience working with other address ranges and subnet sizes.

Speaking of subnet sizes, you will not be using the /24 addresses we have become accustomed to in this lab. To make it more interesting, the DMZ and internal networks will not use /24 (previously called "Class C" networks). Instead, we shall use CIDR (pronounced "cider") addressing and use subnets.

F1, which is a router/firewall, will have a single public IP address (203.0.113.117), and the internal and DMZ networks will use two subnets, each appropriately sized, which you will split out from 10.8.2.0/24 yourself, which for the purposes of this exercise you must use sparingly.

You will only have one machine in your DMZ in this lab, but you should pretend that in the real network that you *currently* have 7 hosts in the DMZ, and you must allow for some growth. **What is the smallest practical subnet size for the DMZ network?** Don't forget the very first address (subnet address) and very last address (broadcast address) are reserved, and the router will need an address for each subnet it has an interface on. For the internal network, consider your needs to be 100 hosts, which is considered a small business. As a point of comparison, a medium sized network would have about 500 hosts.

For the DMZ network, to make it a little more educational, do not use the first available subnet, but choose the second or third available subnet instead. [In an exam situation, you should be able to handle any subnet.] When you have designed your subnets, write them down, including the following information:

• network address,

• netmask in dotted decimal format, and corresponding prefix-length in CIDR notation,

• gateway address,

• broadcast address,

• first and last usable host address,

• and current number of host addresses unused in each subnet.

For your benefit, Figure 2, "Subnetting a /24" shows a chart to help you understand the relationship between prefix-length and address-space. Using this chart will help you check for overlapping allocations, and to visualise "holes" in the address-space. You should not, however, depend on it because it will be unavailable in the examination.

Figure 2. Subnetting a /24
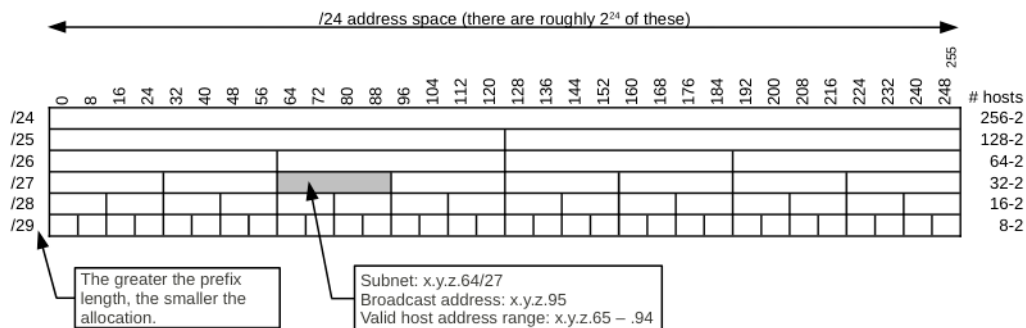
This chart shows the relationship between prefix-length and allocation size. You can use it for visualising your address space and checking your subnetting calculations.

In production networks, you generally need to have some tool to assist you in managing your address space. In many networks, one simple solution is to use a spreadsheet. A nicely designed spreadsheet can show you your address space very nicely. You can drill down to arbitrary levels of detail, even down to individual addresses. This sort of spreadsheet could be useful for adding things like DNS names, MAC addresses, and accounting data. However, for larger networks with more IT staff, this rapidly becomes unmanagable. One sample spreadsheet is available in the `Lab Resources/Subnetting` folder. It spans a few pages, so is not included in this text, but Figure 3, "1000-foot View of an Example Address Management Spreadsheet" shows a "1000-foot" view of it.

Figure 3. 1000-foot View of an Example Address Management Spreadsheet
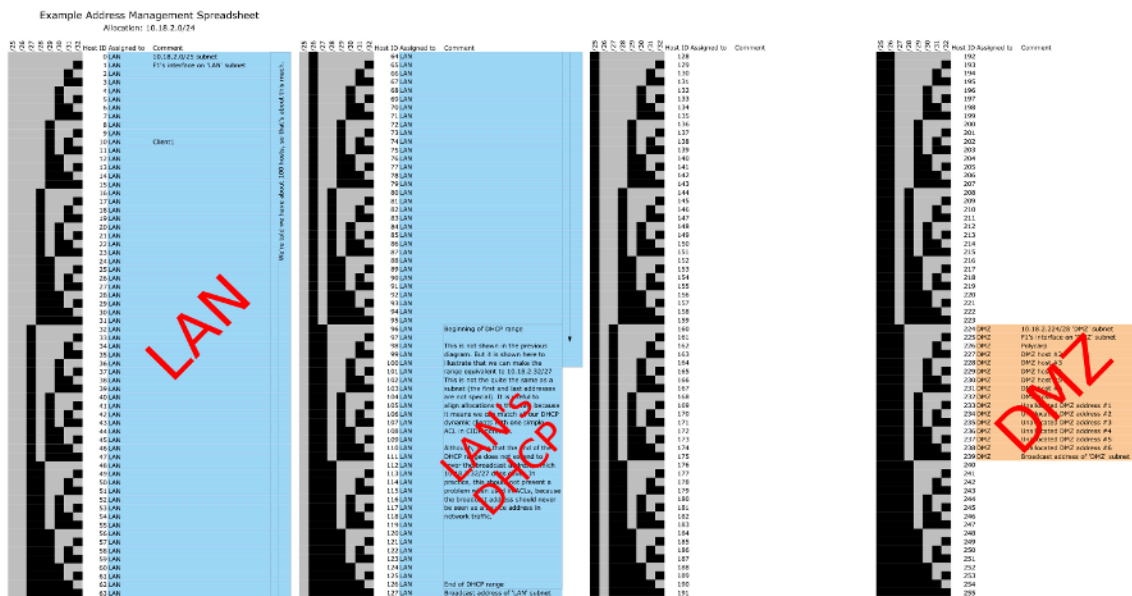
1000-foot view of a example address management spreadsheet. The spreadsheet is very long, so it has been split into four pages. Each page covers a /26 exactly.

Note that a visual device has been included to help you see the size of various allocations. Colour is used to delineate different allocations; here there are two subnets shown, one for the LAN, and another for the DMZ. There is still ample empty space. Inside the LAN subnet, a particular allocation has been set aside for a dynamic DHCP range of addresses.

1. In-Class Exercises

Most of these questions were sourced from SubnettingQuestions.com [http://subnettingquestions.com/], which is a very useful resource for practicing these skills; recommended for your exam study. The last question is another style of question you could expect in any subnetting examination.

1. Which subnet does host 192.168.77.108/28 belong to?

2. What valid host range is the IP address 172.21.71.219/20 a part of?

3. What is the first valid host on the subnetwork that the node 172.16.139.35/26 belongs to?

4. What is the broadcast address of the network 172.30.134.0/23?

5. How many subnets and hosts can you get from the network 172.20.0.0 if you want to partition it into subnets like 172.20.0.0/255.255.254.0?

Sometimes you need to know the class of an address, for example, to answer a question such as this one. The class of an address, and therefore its network mask, can be determined by the first few bits of the address, as shown below.

```
Class A  ≤127  0nnn nnnn  hhhh hhhh  hhhh hhhh  hhhh hhhh
Class B        10nn nnnn  nnnn nnnn  hhhh hhhh  hhhh hhhh
Class C  >192  110n nnnn  nnnn nnnn  nnnn nnnn  hhhh hhhh
```

6. Given the following address allocations, create two further allocations, a /29 ("Test Network") and a /27 ("Sensor Network"), such that fragmentation of the address space is minimised. The "Test Network" can be a subnet of the Engineering subnet.

```
172.16.20.0/24      Complete allocation
172.16.20.0/27      DMZ
172.16.20.64/26     Engineering
172.16.20.192/26    Main Office
```

2. Subnetting in IPv6

Subnetting in IPv6 is much easier than in IPv4, largely for two reasons. The first is that because the address-space is much larger, we can take a much more structured/readable approach, and also because working with hexadecimal is much easier than decimal, when it comes to subnetting. You will come to appreciate that in this section.

In case students have not already done it, the IPv6 routing for the lab on Interior Routing will be discussed as a class exercise. Even if you haven't done, or don't have time to implement the network, all students should understand the basic strategy behind the addressing scheme.

Students should watch the 20-minute IPv6 Subnetting video in the Lab Resources before the tutorial.