# 12.1.3 IPv4 Addressing

Click one of the buttons to take you to that part of the video.

### IPv4 Addressing 0:00-0:31

In this lesson, we're going to discuss how IP version 4 addressing works. One of the key things that you need to understand is the fact that for communications to occur between hosts on an IP-based network, each one of these hosts has to have a unique IP address assigned to it. Without IP addresses being assigned, the network hosts will not be able to talk to each other.

An IP address is a network layer 3 address that is logically assigned to a network host.

### How IPv4 Addressing Works 0:26-2:19

Because it's a logical address, it's not a permanent assignment. You can actually change it at any time.

In this example, I have two workstations. Workstation 1 has been assigned an IP address of 192.168.1.1.

This second workstation has been assigned an IP address of 192.168.1.2. Because these are logical addresses, I could actually swap these, and I could assign this system an address of 192.168.1.2, and this one an IP address of 192.168.1.1.

Understand that each IP host on the network actually has two addresses assigned to it that come into play. The first one is the IPv4 address that we just looked at, but each host also has a MAC address assigned to it. This MAC address is totally and completely different from the IP address.

The MAC layer address is a data link layer 2 address, and it is not logically assigned to the host. Instead, that address, which we sometimes call the hardware address, is burned into the ROM chip of the network board itself.

Every single network board sold in the world has a unique MAC address burned into it. And because this address is hardcoded on the network board itself, it can't be changed. The only way you can reassign a network host with a different MAC address would be to actually take the network board out and put it in a different system, because the MAC address travels with the network board itself.

You know, if for whatever reason I wanted to swap MAC addresses between these hosts, I would have to actually take the network boards out of each one and move them around.

Again, the MAC address follows the network board, but the IP address is logically assigned. You can change that any time you want.

### How IPv4 Addresses are Constructed 2:18-8:59

During the host addressing process, basically what we have to do is map the MAC address that is hardcoded in the workstation to whatever logical IPv4 address that host is currently using.

In this example, we would say that 192.168.1.1 maps to this MAC address, while 192.168.1.2 maps to this MAC address. And because these IPv4 addresses are logically assigned, and therefore could change at any time, we have to use a special protocol called ARP to map these logical IP addresses to their hardcoded MAC addresses.

A valid IPv4 address consists of four numbers, and they're separated by periods. A couple of examples of valid IP addresses are shown here. 12.34.181.78. 192.168.1.1. 246.70.3.8.

Because IPv4 addresses have four parts to them-- one, two, three, four-- and because these portions are separated by periods, you will sometimes hear IPv4 addresses referred to as dotted quad addresses.

Here's a very important thing that you need to understand. In decimal notation, each number between periods in an IPv4 address has to be between 0 and 255. For example, 192.168.1.1 is a valid IP address because each of these numbers-- 192, 168, 1, and 1-- are all within this range between 0 and 255.

Here are some invalid IP addresses over here. Can you tell me why they are invalid? Let's take a look at the first one. Why is that an invalid IP address? The first part of the address contains the number 356. Well, that violates this rule. It can't be higher than 255.

How about this address? Why is it invalid? Well, 10 is okay, 3 is okay, 4 is okay, so we didn't violate this rule. What's wrong with it? It's too short; it needs to have another period, and then another number, like a 5 or something like that.

How about this number--why is it invalid? The 192 is okay. Ah, 258. It's not. 258 exceeds 255.

You might be asking, why can't a number in an IP address exceed 255? Why can't it be 256 or 384 or something like that? That's because each number within this IP address is actually an 8-bit binary number, and we call each one of these 8-bit binary numbers an octet.

"Oct" means eight. There are eight binary numbers, hence the term octet. Think of octagon, eight-sided shape. Because each octet is a binary number, that means each number within it can be represented by only one of two numbers: a 0 or a 1.

In this example, 192.168.1.1 in decimal up here can be represented as this number down here in binary. 192 equals 11000000 168 can be represented as 10101000. The number one is just 00000001, and the same for the last number.

You might be asking, "How do I convert between the two? How do I convert a binary IP address to decimal? And the other direction, decimal to binary?" The math for doing so is not very difficult.

Basically, what you need to understand is that each value of each bit in a binary number has a decimal equivalent.

The first bit in an 8-bit binary number has a decimal value of 128. The second bit in an 8-bit binary number has a value of 64. Bit number three has a value of 32. Bit four has a value of 16. Bit five has a value of 8. Bit six has a value of 4. Bit seven has a value of 2. Bit eight has a value of 1.

If you look very carefully, you notice that there's a pattern. Bit eight is 1; bit seven is 2, which is twice the value of 1; bit six is 4, which is twice the value of 2; bit five is 8, which is twice the value of 4; and so on, all the way up to the top.

Each bit basically doubles. Start at 1, and then just double it for each bit moving from right to left.

With that in mind, let's break down just the first octet of this decimal IP address, 192. In order to convert 192 to its binary equivalent, we need to look through the various bits over here and see which numbers add up to 192. And then we put a 1 wherever that bit that we picked resides. If we don't use one of those bits, we just use a 0. Okay, so let's think about it.

How can we come up with 192? Well, actually, all we have to do-- it's really simple-- is add 128 and 64 together. If we add 128 and 64, we get a value of 192. Therefore, we know that we need to have a 1 in bit one and in bit two, and all the rest can be zeros.

192 in binary would be 11, and because there are eight bits in an octet, the remaining six bits have to be 0. One, two, three, four, five, six. Pretty easy. Let's do the same thing for the last octet. It's a decimal value of 1, so how would you represent that in binary?

Pretty easy. Right there. We need a 1 in the bit eight position. All the rest can be 0. Remember, there are eight bits in an octet, so the first seven have to be zeros. One, two, three, four, five, six, seven, and then a 1. That's the binary equivalent of decimal 1. You can do the same thing for 168.

Remember I said earlier that the value of an octet in a valid IP address can be between 0 and 255. That's sort of true.

There are actually some IP addresses that are reserved for special purposes, and they can't actually be assigned to a host. They are still valid IP addresses, but you can't assign them to a particular computer.

For example, you cannot have a 0 in the last octet of a host IP address. Let's say we have 192.168.1.0. Well, that is not a valid address that we can assign to a computer on the network, because this is actually what we call the network address.

This is the IP address of the network itself, not the hosts on the network, but the IP address of the entire network segment.

---

How to Conserve Registered IPv4 Addresses 8:59-14:29

In addition, the last octet of an IP address can't end in a 255 either-- for example, 192.168.1.255. That's because 255 is reserved for sending broadcast messages to all the hosts on the segment. By default, when we send communications between hosts on an IP network, we use what's called unicast communications, meaning one host sends a message to one other host.

There are times, however, when we need to send messages to everybody and we don't want to have to actually enumerate each single host that we want to send the message to. In which case, we just use a 255 and that allows the message to be received by everybody on the network.

It's very important that you understand that every single host on an IP-based network must have a unique IP address assigned to it. That means no two hosts on the same IP network can have the same IP address assigned.

This is particularly true if the host resides on a public network. What's a good example of a public network? The internet. If your computer hosts are connected to the internet, then each host has to have a globally unique IP address.

That means the IP address that it uses cannot be used by anybody else anywhere in the world. You can apply to the Internet Assigned Numbers Authority, IANA, for a block of registered IP addresses. Once that IP address is assigned to you, then nobody else in the world can use it on that public network.

This actually introduces a very important problem with IPv4. IPv4 uses a 32-bit addressing scheme, and that allows for a maximum of four billion possible unique IP addresses. Back when IPv4 was first defined, that seemed like a lot of addresses. We thought, "How in the world would we ever use that many addresses?"

Well, today, we've used them all. This finite amount of available IP addresses has been completely allocated. Few, if any, registered IPv4 addresses are currently available for assignment.

One way to get around this shortage of IPv4 addresses is to use private networks with network address translation, which we just affectionately refer to as NAT. NAT has been widely implemented around the world to conserve IP addresses.

Essentially, with network address translation, you implement a NAT router, and this NAT router uses one single globally unique registered IP address, and it's connected to a public network, like the internet. On the other side of the NAT router, on our local network here, we use a non-globally unique IP addressing scheme.

Notice here we've assigned an IP address of 192.168.1.254 to this router, and this host has an IP address of 192.168.1.1, and this host has an IP address of 192.168.1.2. Because these are non-globally unique addresses, it's very likely--in fact I can almost guarantee it-- that there are other computers in the world that have those very same IP addresses assigned to them.

This violates the rule that we specified earlier, right? That each host has to have a globally unique IP address. Well, how does this work?

Basically, what happens is this router translates these addresses into this one address right here, so no matter what computer is accessing the internet, from the internet's perspective it's all coming from just this one IP address. The NAT router takes care of translating the addresses back and forth.

Using a NAT router has many advantages. Probably the most important advantage is you can hide a huge private organization, with thousands and thousands of computers, behind this public interface on the NAT router, and this allows a huge organization to implement its network and need only a very limited number of these scarce globally unique IP addresses.

There have been three ranges of IP addresses defined that are called private IP addresses. Sometimes they're called reserved IP addresses. These addresses are unallocated. They have not been registered to anybody in the world. And because they're unregistered, anybody who wants to use them can, as long as you use a NAT router to convert those unregistered addresses into registered ones on the internet.

This allows you to use tons of these unregistered addresses on your local network and still be able to connect to a public network like the internet, even though somebody else in the world is probably using those very same addresses that you're using.

If you want to use unregistered addresses on your network with a NAT router, you can use this range of addresses here, or this one, or this one.

The important thing you need to remember about these addresses is that they are non-routable addresses. Which means if you tried to use an address in any of these three address ranges out on the public network, out on the internet, the routers out on the internet will not forward this data to or from them.

That's why we have to use a network address translation router to convert these unregistered addresses into proper, registered addresses out on the internet.

---

Summary 14:30-14:40

That's it for this lesson. In this lesson, we discussed how IPv4 addressing works, we looked at how IPv4 addresses are constructed, and then we talked about how you can use a NAT router to conserve registered IPv4 addresses.

---