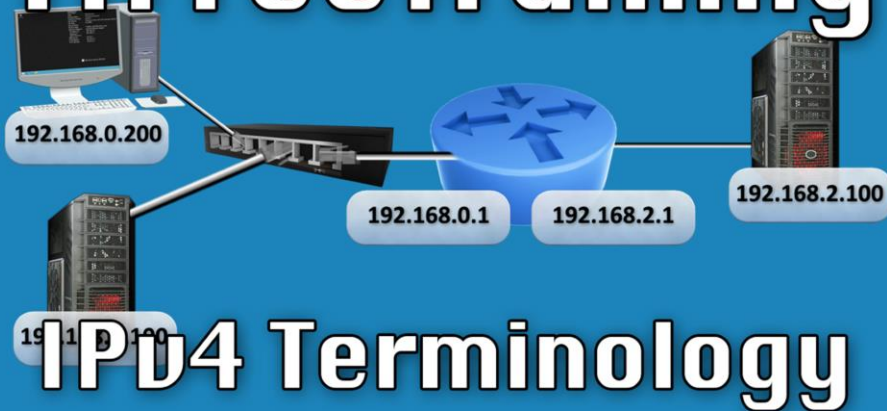


ITFreeTraining



IPv4 Terminology

For the free video please see
<http://itfreetraining.com/ipv4/terminology>

In this video from ITFreeTraining, we'll take a look at the terminology and components that are used with IPv4. Having an understanding of these concepts is very crucial as they comprise the building blocks of modern networks.

Access the rest of the course <http://ITFreeTraining.com/ipv4>

Download the PDF handout <http://ITFreeTraining.com/handouts/ipv4/terminology.pdf>

What is an IP Address?

- A unique identifier for devices on a network



Each phone has a unique number
e.g. 555-2368



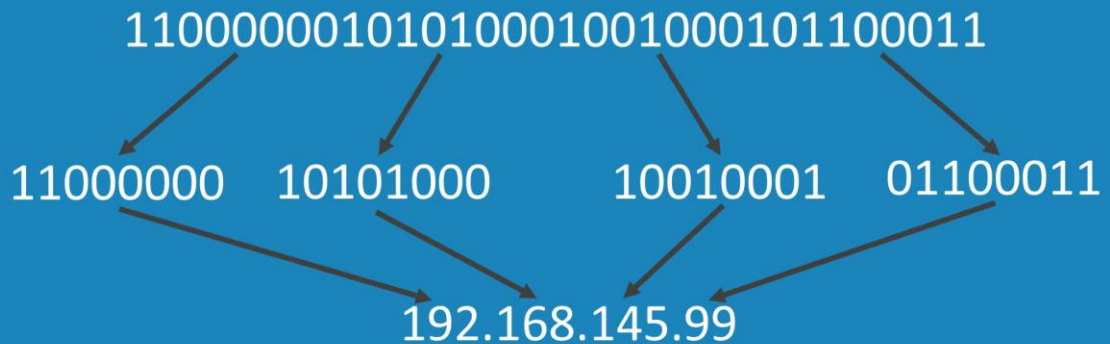
Each network device has unique IP Address
e.g. 8.8.4.4

What is an IP Address?

0:14 – To begin, we'll define what an IP Address is. An IP Address is simply a unique identifier for the devices on a network. To relate this to the real world, a common example would be to consider a telephone. Every telephone would have a unique, public number assigned to it. Due to this unique number, it allows anyone who knows that public number to call it. Just like a phone, all the devices on the network can receive a unique, individual identifier called an IP Address. If you wanted to contact a device on the internet, you'd only need to know the IP Address of the device. Let's have a closer look at an IP Address.

IP Address

- IPv4 Addresses are 32bits long
- Divided into 4 parts called Octets
- Written in dot-decimal notation

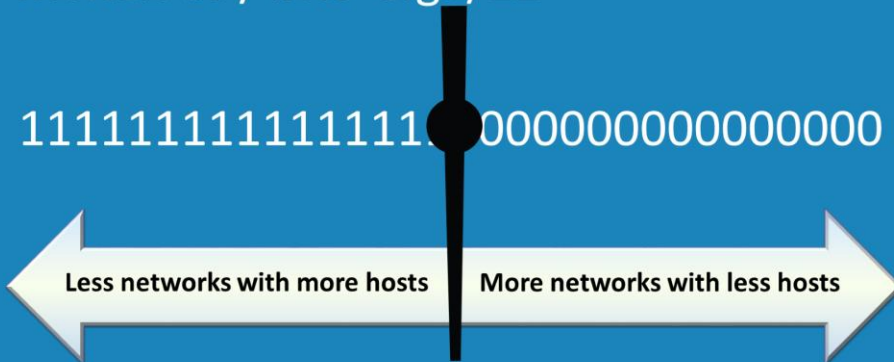


IP Address

0:57 – An IPv4 address is 32-bits long. If you were to look at it as a 32 bit binary string it would be difficult to make sense of. For this reason a 32 bit address is divided up into 4 parts called 'Octets'. If you look at this, in binary it is still hard to read. For this reason, IP Version 4 addresses are often written in dot-decimal notation. Dot-decimal notation of an IP Address is a lot easier to read and use. If this format is so easy to read, the question to be asked would be why you would ever even look at it in binary? This brings us to the next topic of the subnet mask.

Subnet Mask

- Divides an IP Address into networks and hosts
- 1's on the left, 0's on the right
- E.g. 255.255.252.0
- Or written as / bits e.g. /22

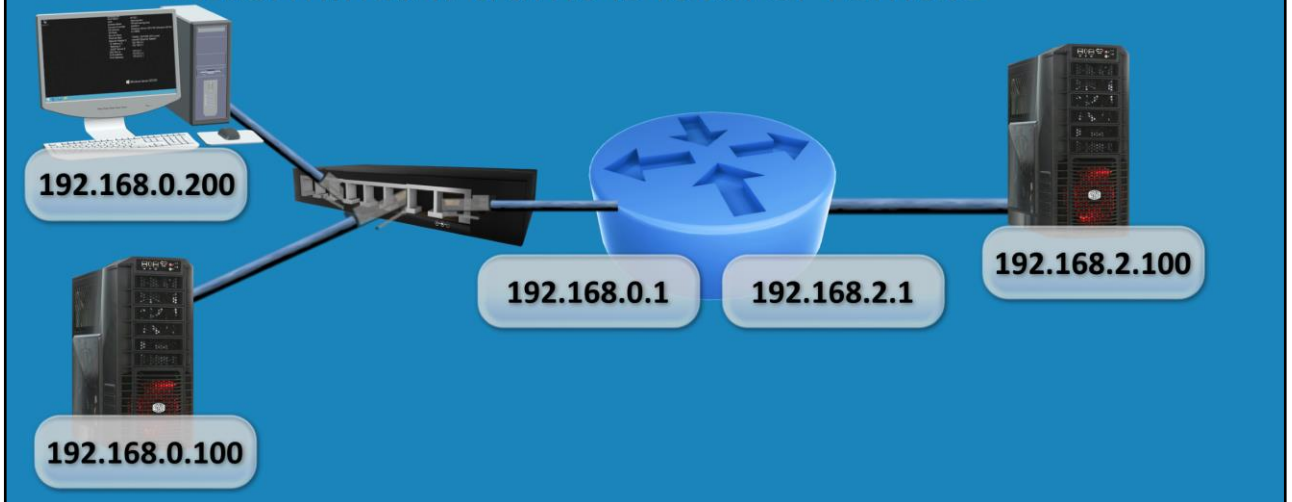


Subnet Mask

1:42 – A subnet mask divides an IP address into networks and hosts. The left hand side consists of ones and the right side has only zeros. There are actually two ways that subnet masks are represented. The first way is the familiar dot-decimal notation, the same way as an IP Address is written. The second method is called Classless Inter-domain Routing (CIDR), also called slash notation, and is represented as a slash followed by the number of 1 bits that are used in the subnet mask. In a later video, we will cover subnetting in far more detail, but essentially what occurs is that the fewer 1 bits there are in the subnet mask, the fewer individual networks can be created. However, fewer networks means more hosts or devices that can be placed on that network. The opposite is also true, if you were to increase the number of 1 bits that are used in the subnet, you would be able to allocate more individual networks. The drawback to remember is that if you can create more networks, you cannot have as many hosts on the network. Particular subnet masks are easier to use than other subnet masks. However, you can see that depending on what your organization's needs are for devices they require on each network, this may mean that the decision of which subnet mask to be used will be made for you. The next point to consider is how the subnet mask is used in an IP network.

How the Subnet Mask is used?

- Subnet mask used for traffic routing
 - Determines if traffic is local or remote



How the Subnet Mask is used?

3:01 – The subnet mask is used in our device's basic routing to determine if network traffic is for the local or remote network. Let's consider that you have a computer that is connected to a network and on that network is also a server and a router all connected to the same network switch. Adding to this, there is also a server on a remote network connected to the router. The question is, how does traffic move around and reach the appropriate areas of the network? The first step is to assign each an IP Address. Once the IP Address has been assigned, decisions can be made on where to send traffic to ensure that it gets to its destination. This is because the left part of the IP Address is the network and the right part is the host. If the desktop wants to send network traffic to a device on the same network, it will send it directly to the device. If it wants to send it to a remote network, the data will be directed to the local router which is referred to as the gateway. This begs the question, how is the decision made on where to send the data?

AND Operator







- Operator that works at the binary level
- Same result as multiplication of bits

Bit 1	Bit 2	Result
1	1	1
1	0	0
0	1	0
0	0	0

AND Operator

4:05 –The 'AND' operator is a mathematical calculation that works at the binary level. When the 'AND' operator is applied to bits, it gives the same result as multiplying them together. To understand how it works, consider this table. The 'AND' operator takes 2 bits, looks at their values in order to achieve a result. If I consider the first case, if the first bit and second bit are both 1, the result will be 1. This is the same result as multiplying bit 1 and bit 2 together. 1 times 1 gives 1. If I consider the next case, the first bit is 1 and the second bit is 0. This gives a result of 0. If I were to multiply 1 by 0, this would give 0. The next case is the first bit is a 0 and the second bit is a 1 which just like before yields a result of 0. The last case is when both bits are 0. When this occurs the result will be 0. So you can see that the 'AND' operator is easy to remember. All you need to remember is that if both bits are 1 the result is 1, whereas all other results are zeros. The next question is, how is the 'AND' operator used to route traffic?

Basic Routing

Source	Destination	And Operator	Result
 192.168.0.200	 192.168.0.100 local Network	Source IP 11000000101010000000000011001000 Subnet mask 11111111111111111111111110000000 Result 11000000101010000000000000000000 Destination IP 11000000101010000000000001100100 Subnet mask 11111111111111111111111110000000 Result 11000000101010000000000000000000 Compare 11000000101010000000000000000000	 Sent direct
 192.168.0.200	 192.168.2.100 Remote Network	Source IP 11000000101010000000000011001000 Subnet mask 11111111111111111111111110000000 Result 11000000101010000000000000000000 Destination IP 11000000101010000000001001100100 Subnet mask 11111111111111111111111110000000 Result 11000000101010000000001000000000 Compare 11000000101010000000000000000000	 Sent to gateway

Basic Routing

5:21 – Any device on the network when sending traffic needs to make a decision if the traffic will be sent directly to the local network or to a router to get routed to its destination. Let's first begin to understand how traffic would be routed if the final destination was on the same network as the sender. Consider a computer on the network. In this example it will communicate with a server on the same network. So a computer will send data directly to the server. The next question is how does the computer make a decision if the data should be sent locally or remotely via a router? To do this, the 'AND' operator is used. To perform this calculation, a bitwise 'AND' operation is performed between the source IP Address and the subnet mask. The result of this will be recorded. Since the result is a long string of binary numbers, it is hard to tell what has happened. Essentially what has happened is the network part of the IP Address has been separated. This now means that the network of the source computer has been calculated and determined.

The next step is to work out the network of the destination IP Address. The same process is followed. The 'AND' operator is used with the destination IP Address and the subnet mask. The result will give the network that the destination IP Address is on. Now that the source network and destination have been found, they can be compared. In this case, both the networks are the same. So this means that the source IP Address is on the same network as the destination host's network. So the result is that the traffic will be sent directly to the server. Whenever the networks match, the traffic will be sent directly to the destination. Let's consider another example. If the same computer this time, attempts to send data to a remote network, the following will happen. Like before, the source IP Address and the subnet mask have the 'AND' operator applied to them and the result recorded. The next step is to apply the 'AND' operator

on the destination IP Address and the subnet mask and record the result. Notice, however, that when the results are compared, they do not match. The source network and the destination network are different. Only 1 bit is different, but that is enough. When this happens, the network traffic will be sent to the default gateway, which is typically the local router.

See <http://YouTube.com/ITFreeTraining> or <http://itfreetraining.com> for our always free training videos. This is only one video from the many free courses available on YouTube.

References

“IP Address” https://en.wikipedia.org/wiki/IP_address

Credits

Trainer: Austin Mason <http://ITFreeTraining.com>

Voice Talent: HP Lewis <http://hplewis.com>

Companion Document: Phillip Guld <https://philguld.com>

Video Production: Kevin Luttman <http://www.KevinLuttman.com>

Quality Assurance: Brett Batson <http://www.pbb-proofreading.uk>