DHCP, TCP Transmission, Common Port Numbers

May 2018 — Apr 18 — Monday — 09 — WK 15 (099-266)

Dynamic Host Configuration Protocol —

This protocol is used to configure IP address to hosts dynamically.

So, when we click on Internet Protocol Version 4 Properties, we find there option Obtain an IP address automatically. This option literally searches for a DHCP server that is configured in the same subnet and it sends different packets and requests for an IP address.

DHCP has 6 messages —

first 4 messages are critical for assigning an IP address.

(a) DHCP Discovery
(b) DHCP Offer
(c) DHCP Request
(d) DHCP Ack

} Critical for assigning IP address.

(e) DHCP Information
(f) DHCP Release

Notes

The DHCP DISCOVERY — message like a hello packet. When a new device comes onto the network, the device literally asks or shouts out in the network asking if there is a DHCP server around. So, it's like a broadcast or it is a shout to the DHCP server. So, all the devices in the network hears this broadcast. Now, if there is a DHCP server, it sends back a DHCP offer packet. Now, DHCP offer packet is the reply to the DHCP Discovery by the DHCP server. This reply tells that the client sent by telling the DHCP client to take a certain IP address. Now what the DHCP Server does is it reserves an IP address. Let it reserves an ip. address :— 192.168.1.50,

Now, if there are more than one DHCP servers configured in this network, even the other DHCP server would have got the broadcast from the client and he too would offer an IP address like 192.168.1.50 and it would tell the Server's IP address is :— 192.168.1.200.

Now, ideally we would not configure 2 DHCP Servers in the same network

Notes

but sometimes it happens.

(b) DHCP Offer - So, when this DHCP offer is sent back to the client, the client gets 2 DHCP offers. Now, its upto the client to decide which DHCP offer it wants to accept.

So, let us assume it wants to accept the first one, so, what it does is it sends a DHCP request packet.

(c) DHCP Request - Now, the DHCP Request packet says "OK, I will take 192.168.1.2 offered by DHCP Server 192.168.1.1. Now, that is again sent back to the network and the DHCP Server hears that.

Now, when the DHCP Server at 192.168.1.1 hears that, he says "Al right, I acknowledge that". So, he sends a

(d) DHCP Ack - DHCP Ack to that. The other DHCP Server, what it does is, it had reserved the IP address — 192.168.1.50.

So, what it would do is that it would put that IP Address back to the pool so it could assign that IP address

Notes

to another client if there is another request. So, there are 4 critical messages that a DHCP exchanges in the critical DHCP IP Address assignment.

(e) **DHCP Information** Now, DHCP also has 2 more messages that is DHCP information message. The information message is issued by the client if it needs more information than the information that is provided by the DHCP offer, that was the second step. So in the DHCP offer, if the server had not given enough information or if the client needs more information than the information that was there in the offer packet, the DHCP information is what is sent to obtain those extra information.

(f) **DHCP Release** There is last message named — DHCP Release. Now, DHCP Release is the message sent by the client to the server to tell that it wants to release the IP address that it already has. But most of the time what happens is the user just disconnects before the client can send that message to the server.

Notes

So, before the client can even send that message, the computer is shut down or the computer is disconnected.

TCP transmission →

TCP transmission can also be possible when there is a connection that needs to be established before the real transmission can start. Now like we discussed in our previous topics, TCP is a connection-oriented transmission, whereas UDP is a connection-less transmission.

TCP actually builds a connection, then it starts doing the real transmission. In technical term it is known as 3 way Hand Shake —

It is initiated by the sending device. Now, it does that by creating a SYN packet.

Suppose two communication points established a connection — A and B. A sends SYN packet to B for starting communication. B sends back SYN/ACK a combination of Syn with Acknowledgement.

Notes

Apr'18

14 Saturday
WK 15 (104-261)

Mar 2018

M	T	W	T	F	S	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Now device A sends back the ACK to the device B. At this point of time device A and device B both have a SYN/ACK combination. This is the stage where connection has been established. or this is the basic 3-way Handshake in a TCP transmission.

TCP transmission windowing technique

If you tried transfering a big file from one drive to another drive. Initially it would come back and say "Alright, this transmission is going to take about one year or some days. And a few seconds after it would say "Oh wait a minute, I think it's about 6 months. After some time it's going to say "Wait a minute, I think may be I can do this in 10 minutes.

Apr'18

15 Sunday
WK 15 (105-260)

Notes

Initially when your device tried to communicate with the other device, it sends one packet. Now it

sends one packet and it waits for acknowledgement; Now, it ~~end~~ sends that packet and it waits for a long time for the acknowledgement and it says "Ok, if at this speed I have to complete this entire data (suppose 2GB), it is going to take about one year. Now after sometime it receives the ACK, and it thinks "Alright, I have sent one, I have received ~~one~~ the ACK. That means its perfectly fine, the receiving device is capable of receiving 1. Ok, let me try sending 10 instead of 1". So it sends 10; after sometime it sends the ACK for 11. So that's how it works. If it receives 10, then the receiving device will send the next message. So lets say if it has sent the 10th packet, then it says ACK 11 which means that it's expecting the 11th packet. Now the sending device says - "Fine". He sends maybe 100 packets this time. And the receiving device says "I received it's I am expecting 101 now".

So, as time goes by, it increases the number of packets that it's sending. Now that is exactly why you see that time dropping from 1 year to 6 month. Because every time its increasing its capacity of how much it is transferring. Now it will reach a point where let's say it would have send 10,000 but the receiver device buffer can only take about 9000. So, it would say "Alright, I received 9000. Now I am waiting for the 9001 packet. At that point, the sending device realises that "Alright, the receiving device buffer capacity is only 9000." It will constantly start sending 9000 packets and that is about the time when the time like in the example 10 minutes because, both of them have established and realized what is the capacity. That is actually

Notes

What windowing is. It is one of those flow control mechanisms where both of them, gradually by doing this, it realizes what is the capacity of the transmission.

Since, there are various types of devices on the network, so you will have an IPad, may be of capacity different with other devices or may be you have a very old Computer. So, everybody has got different capacity of network transmission. So depending on that, when they do this, when they start doing windowing technique, so they start with the small number, then they keep increasing that window so you send 1 packet, 5 packet, 10 packet, 100 packet, 10,000 packet, you are slowly sliding that window bigger and bigger until it reaches your device's maximum buffer capacity they can send at any point of time.

Notes

Apr'18 COMMON PORT NUMBER

19 Thursday
WK 16 (109-256)

Mar 2018: S M T W T F S — 1 2 3 4 5 6 7 8 9 10 11 — 12 13 14 15 16 17 18 19 20 21 22 23 24 25 — 26 27 28 29 30 31

In a wide area network or internet network, there are many File Servers, Web Servers, Email Servers and DHCP Servers.

Now, if a device communicating with that server, like for instance, a data traffic was going, that was the file server traffic, so that was going to a particular port or particular application or particular server.

Now how did that server know which server this traffic was supposed to go to? It knows by looking at the port number (destination port No).

So, there is standard port numbers, in every transmission if you look at the frame, there is a place where it mentions the destination port number. It also has the source port number. Now source port number

Notes

is required for it to send back.

Now, there is another traffic signal to/from web server. Now both of them go to the same server or same physical server which has different servers installed in that. So may be it is a data centre, it is virtualized, so virtual servers. So how did it know that the traffic of file server had to return back to this IP address.

They know this by making use of port numbers. If you go to this website of Wikipedia, you will get all the standard port numbers for communication. Some important port numbers that we must have to remember for networking interviews.

Notes

Port numbers can go through

1 — 65,565

Apr'18
21
WK 16 (111-254)
Saturday

Mar 2018
M T W T F S S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

The port numbers from 1 to 1024 are known as well-known port.

Some Std. Port Nos used :-

21 — TCP, FTP (File Transfer Protocol / Transmission Control Protocol)
22 — ssh
23 — telnet
80 — http
443 — https (secure version of http)

Apr'18
22
WK 16 (112-253)
Sunday

Some of the port numbers used in TCP and UDP data transmission is same but some are different.

When a device wants to communicate with any server, first like we know, part of 3-way handshake, it has to send a SYN. So it creates a SYN, it puts a port number;

Notes

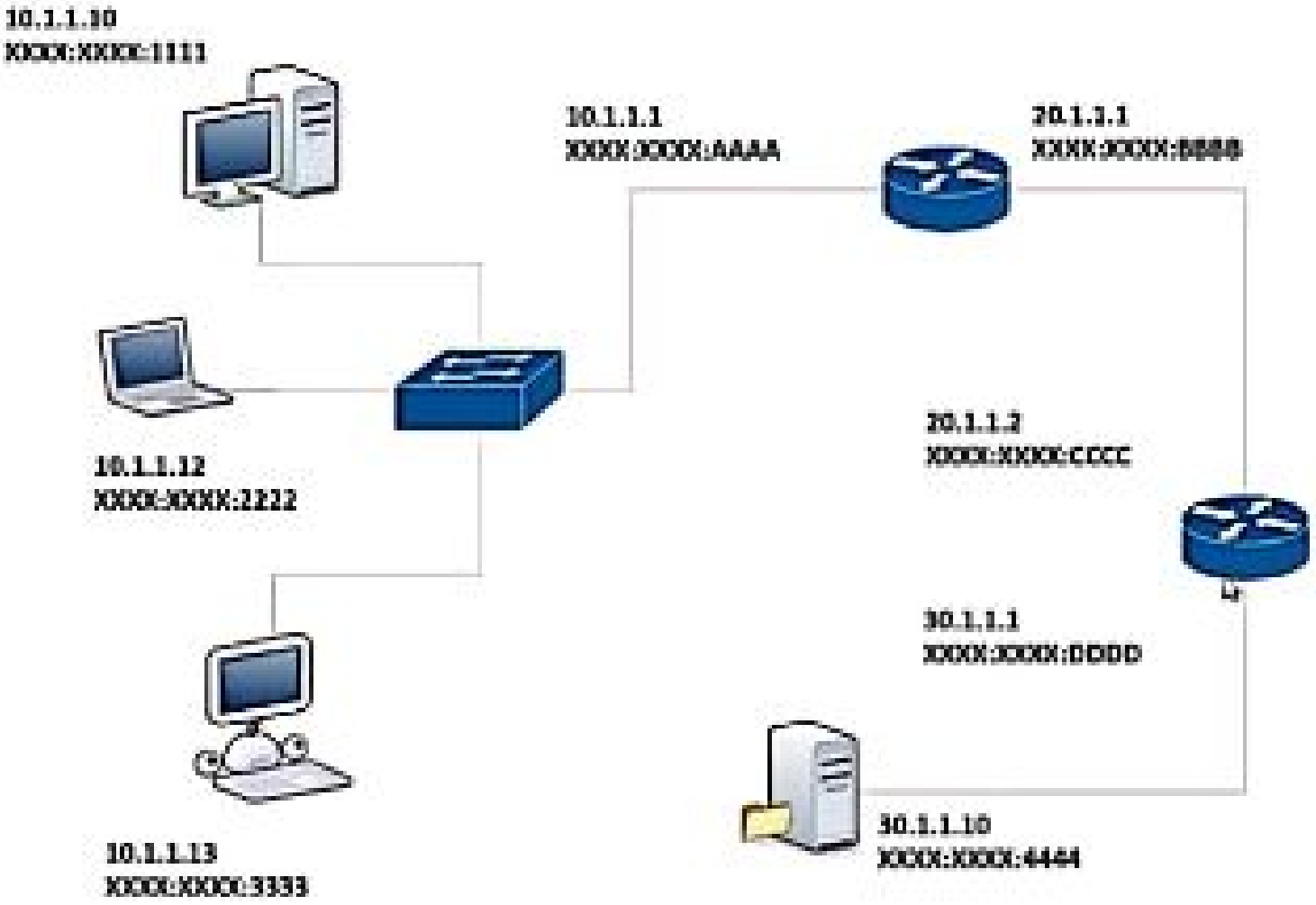
this is source port number generated ~~by wind~~ dynamically by Windows. Now windows will just randomly take a port number between 25000 ~~and~~ 65000.

After that, it puts a destination port number. In this case the application is trying to connect to FTP server. So, it says that port number is port 21.

Now, it says "Okay, my IP address is 10.1.1.10 (supposed), I need to go to an IP address of 30.1.1.10". This forms the packet, now this packet does not change until it reaches the end of this communication.

Notes

So, when this computer sees the source IP address and the destination IP address, it realises one



thing that this IP address is not in this local network. 10.1.1.10 and 30.1.1.10 is not in the same network. So, it realises that for it to go out of this network, it needs to go to 10.1.1.1, which is the gateway and which is configured at one of the interfaces of the router. So, it knows it has to go to 10.1.1.1. So it knows that its MAC address is something at 111, but it does not know the MAC address for 10.1.1.1. What does it do? It sends an ARP Request. Now ARP goes on a broadcast, everybody in the network receives, but only the router with the IP Address 10.1.1.1 would reply. Now he replies with his MAC addres

Notes

Which is Suppose AAAA. What- this device would do is put that in that frame. Once that frame is ready, just- before it goes out of the network, it would do something called as the frame check sequence or CRC, it is just an error checking, error detection mechanism. So, what it literally does is it takes this entire thing, from SYN to this MAC address, puts it through a hashing algorithm, it let us say MD5 hash, so it just puts it through a hashing algorithm, it gets a hash value. What it does is it just attaches that- hash value to the start of the frame. So, you have FCS, FCS is frame check sequence or CRC which is cyclic Redundancy Check both is indicating the same but there must- be a hash value, that is all CRC or FCS. It is there to make sure that whatever

Notes

data is coming through the network, is error free. So, when this data or frame goes through and reaches the router, the first thing it will do is — it will take this FCS or CRC value, take whatever is remaining, but it through the same hashing algorithm and see if the hash that is generated by it is the same that came with this frame. Now if this FCS matches the FCS generated by this router's interface card, that means that there was no error induced during transmission.

The next it looks at the MAC address, it says - MAC address AAAA. that means it is addressed to me, and it strips that away. Next it looks at the IP address, of the destination 30.1.1.10, it realises

Notes

that this packet is not to the router but it is going through the router.

So, Routers have a routing table where all network's entries are present. Network 30.1.1.0 is not the host IP address that is going to be there but it is going to be the network ID. So it would say 30.1.1.0/24 is reachable by going to 20.1.1.2;

Now, how does it know that? Just know for now that it knows, either it could be automatically learnt by using routing protocols or maybe as an administrator, you configured it there, a static route.

But either way, this router's routing table will have that entry there. It knows that it has to send this packet to 20.1.1.2.

Now assuming that this packet already knows the MAC address,

Apr'18

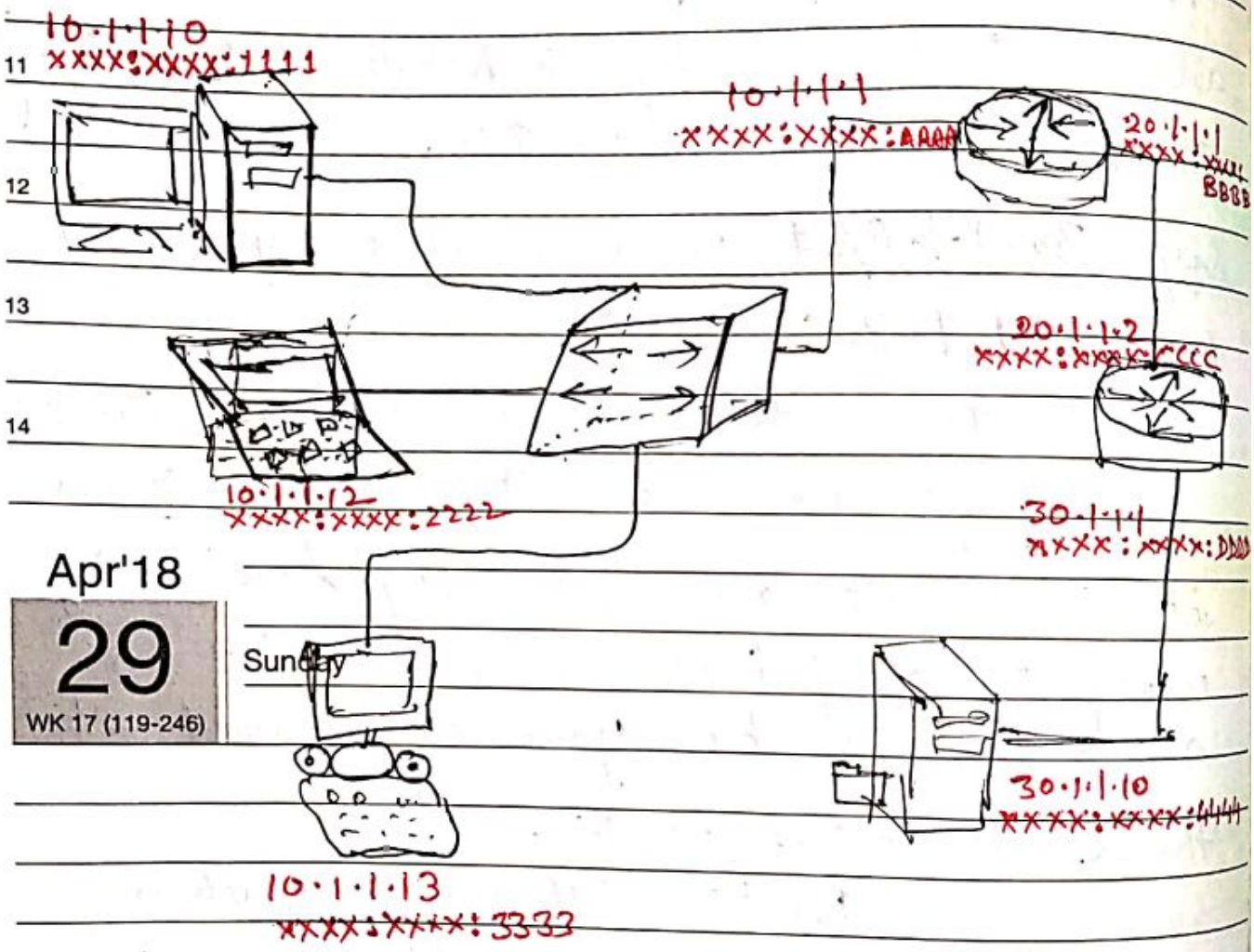
28 Saturday

WK 17 (118-247)

Mar 2018

M	T	W	T	F	S	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

We will continue from here but even if it doesn't know, it will run an ARP again, it will try to get the MAC address of 20.1.1.2



Apr'18

29 Sunday

WK 17 (119-246)

Notes and then it will continue. So, we are assuming that it already knows the MAC address, so it will put the Source MAC Address as BBBB,

destination MAC address as ECC. It again does same computation of hashing algorithm with this entire packet and puts the hash value at the start of the packet. Then it sends that frame across the network, it goes to the device, it again removes the FCS value, it checks, it does hashing and it checks if whatever data it received, is not corrupt. When the FCS matches with the hash that the device generates, it deduces that the data is good. Then it removes the MAC address again and it looks at the destination, it sees that it is 30.1.1.10 and it knows that 30.1.1.10 is connected to its interface. So, the same process continues, it finds out the MAC address, it puts those MAC addresses, does the hashing, attaches the hash

Notes

to the frame and sends it across the network. So, when the receiving device receives that, it again does the same thing, it checks if the hash is matching and if the hash is matching, it knows it did not have any error that was induced. Next it will remove the MAC address from the table, it will remove this protective cover which I put there for reference to tell you that it never changes throughout the journey, from the start till the end, it looks at the IP address and it realises that it is the destination. So it can strip out the IP address information which is layer 3 information, then it looks at the port numbers. It says that it has to go to port no 21

Notes

and it knows that it is an FTP traffic and also it looks at SYN. So, it realises that somebody is trying to establish a connection, so what it has to do according to what we know? It creates a SYN/ACK packet, it will reverse this whole process, it will send back to 10.1.1.10. This device 10.1.1.10 will create an ACK, will follow the same process as we did in earlier notes and send that to this device.

Once that happens, the connection is established.

Now one thing you need to know is that all this happens in less than a second. So, it's very very fast, it is just that we have tried to slow this process to show you exactly how it works.

This is something that we have learnt and I think it has been really useful.

Notes