CSCI 5010 – Fundamentals of Data Communications

Lab 7

Applications:

DHCP and DNS

University of Colorado Boulder

Department of Computer Science

Network Engineering

Levi Perigo, Ph.D.

# Objectives

* Learn DHCP configuration and concepts.
* Learn DNS basic configuration and concepts.

Summary:

As networks scale, we need applications to help manage our IP addresses and configuration of devices. Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) are applications used for better network management. You will use GNS3 in this lab to implement these protocols. You will be examining the messages on Wireshark at the packet level to get a deeper understanding about the protocol mechanics. This lab covers many interview questions that you will be asked when you’re applying for internships and jobs. The main goal of the lab is to help you gain protocol knowledge and basic implementation skills to be able to configure these services on networking devices.

Objective-1: Getting started with DHCP

1. Startup GNS3 and initialize the following topology:

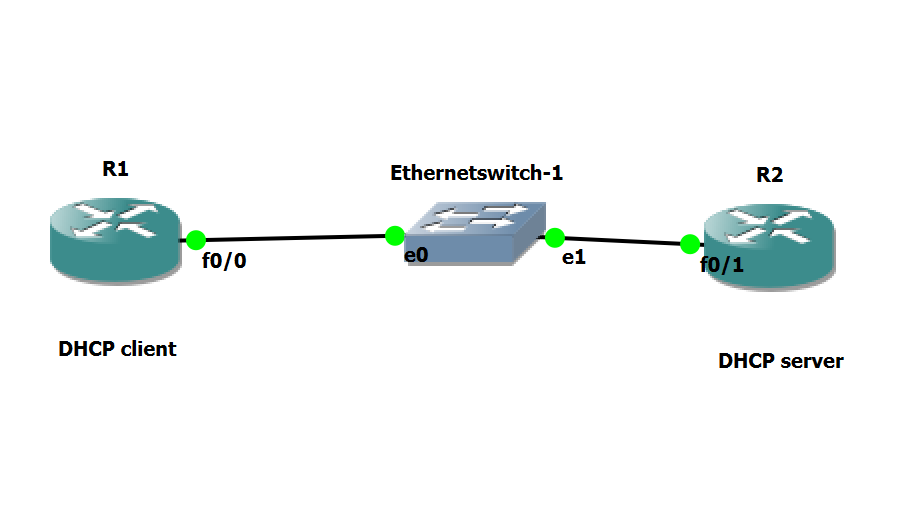


Fig.1

1. Configure R1’s f0/0 interface to obtain its IP address from DHCP. Paste a screenshot of the interface configuration. **[3 points]**

A computer screen shot of white text

Description automatically generated

1. Start a Wireshark capture in this step to capture all DHCP messages that will be exchanged in the next step. In the above topology, where would you initiate a Wireshark capture? **[1 point]**

I would initiate a Wireshark capture between R1 and the switch.

(Hint: To start a capture on Wireshark, right click on an interface and click start capture)

1. If R2 is only a DHCP server, do you need any other basic configuration on R2 besides the configuration of a DHCP pool? Explain if the f0/1 interface of R2 needs to have an IP address. Justify your answer. **[5 points]**

I would think that f0/1 interface would not have to have an IP address. It is not routing any IPs and for a device to get an IP, it would be sending discover request to the specified DHCP port.

1. Having made sure you started Wireshark capture in Step 3, now configure R2 to be a DHCP server. Paste a screenshot of the configuration you made on R2. **[5 points]**

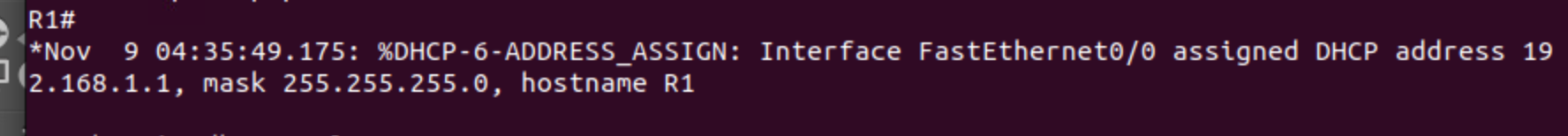
A screenshot of a computer

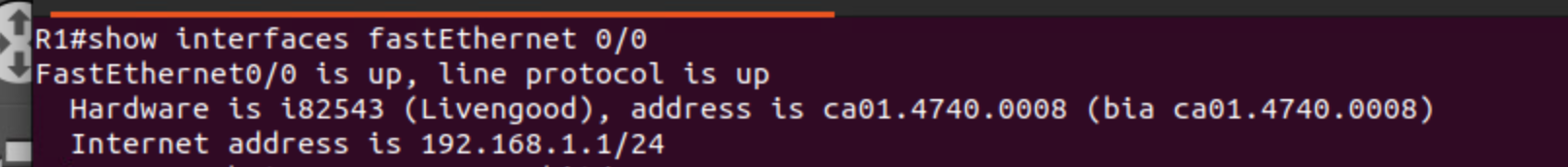
Description automatically generated

A computer screen with white text

Description automatically generated

1. Did you get an IP address on R1? Indicate from its CLI that it got a DHCP address. How do you know this? **[2 points]**





Yes, I know this by the message and by typing show interfaces fastEthernet 0/0

1. In the above step, capture the DHCP messages that were exchanged. Explain in detail the four messages. For each of these messages, mention the Source IP, Destination IP, Source MAC and Destination MAC that you see. **[10 points]**

Discover: R1 sends a broadcast to the network trying to find a DHCP server

* Source IP: 0.0.0.0
* Dest IP: 255.255.255.255
* Source MAC: Source MAC of R1
* Dest MAC: FF::FF

Offer: DHCP server gets discover and sends information of the wanted IP address.

* Source IP: 192.168.1.100
* Dest IP: 255.255.255.255
* Source MAC: Source MAC of R2
* Dest MAC: MAC of R1

Request: R1 gets the offer, and sends a broadcast request saying it accepts the IP

* Source IP: 0.0.0.0
* Dest IP: 255.255.255.255
* Source MAC: Source MAC of R1
* Dest MAC: MAC of R2

Acknowledge: The server will now send back the rest of the needed IP info like subnet, dns ,etc.

* Source IP: 192.168.1.100
* Dest IP: 255.255.255.255
* Source MAC: Source MAC of R2
* Dest MAC: MAC of R1

1. Which of the DHCP messages are broadcast at Layer 3? Which of the DHCP messages are broadcast at Layer 2? **[2 points]**

Discover: Layer 2 & 3

Offer: Layer 3

Request: Layer 3

Acknowledge: Layer 3

1. Are there any other messages you expect to see during the above process except DHCP messages? (Eg: From your theoretical knowledge of DHCP, postulate if you would see any ARP, ICMP or any other messages. Now verify the same on Wireshark)

Explain if you see any of these messages. Why or why not? **[5 points]**

I could expect to see ARP request for the discover and offer request.

I could expect to see ICMP requests for discover and offer requests to check reachability.

I only see ARP requests which makes to resolve the MACs of both client and server.

Objective-2: DHCP server with multiple clients

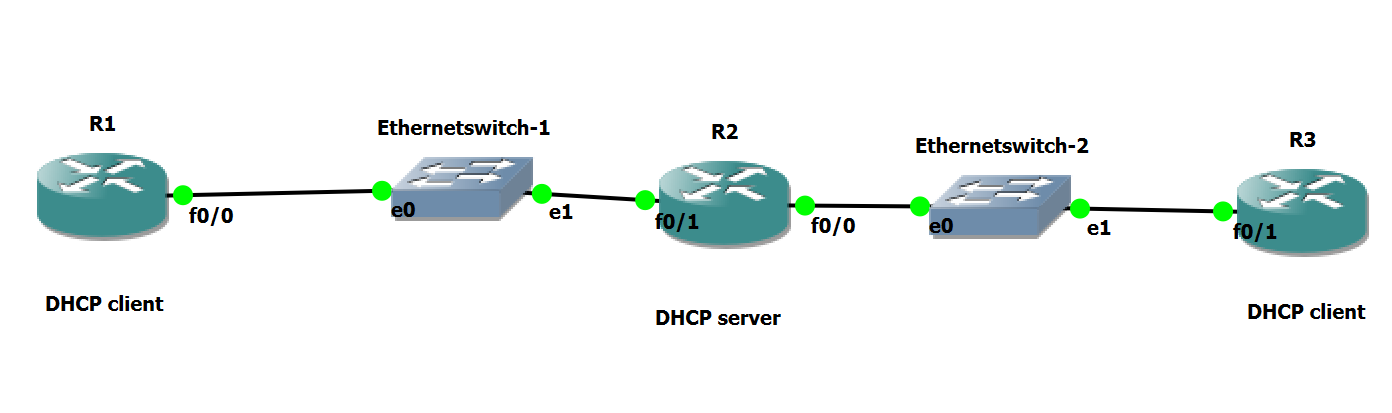


Fig.2

1. Refer to figure 2. Could this network design work? Can a single DHCP server serve two different DHCP clients as shown in the figure? If yes, explain what configuration changes you will need to do on R2 to make this work, and why you would have to make these modifications. Paste the configuration change you made on R2 to make it work.

**[10 points]**

Yes this is possible. You will have to bridge the two interfaces by using the bridge command. I have to do this so it allows both ports to have the same IP and allowing DHCP serving out both ports. The config will speak for itself:

A computer screen shot of a program

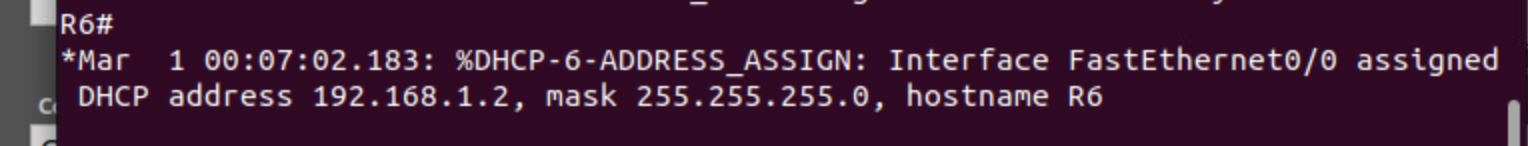
Description automatically generated

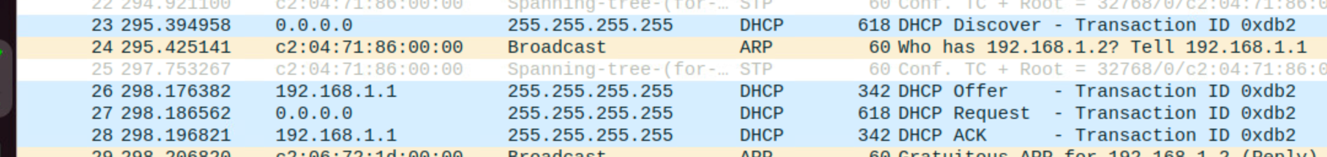
A purple background with white text

Description automatically generated

1. Now configure R3 as a DHCP client and R2 configured to also be the DHCP server for R3. Paste screenshots of DHCP messages exchanged and R3 getting the IP via DHCP.

**[10 points]**





1. When R1 and R3 sent DHCP DISCOVER packets, how did R2 choose which IP to assign? How does R2 know which DHCP pool to use to loan IPs, if there are multiple pools configured on R2. **[10 points]**

It’s basically a first come first serve basis. In my case, R3 was first to send out the Discover packet, so it got a .2 instead of a .3 like R1 got. If there are multiple pools configured on R2, the interface that is configured with an address within the pool’s network will then use that associated pool.

1. Explain excluded DHCP addresses are and why you would use them. Did you configure this on R2? If so, what are some of the DHCP excluded addresses on R2 in your topology? **[3 points]**

Excluded addresses is a set of Ips that a DHCP server will not be allowed to serve. For example, I can exclude the first 100 Ips from a /24 on a network and the first IP served will be .101. I did not configure this.

1. Can R1’s f0/0 interface communicate with R3’s f0/1 interface? If yes, how? Make this work without adding any static routes on any of the routers. Paste screenshots of what you did to make it work and the successful ping. **[3 points]**

I could not get it to work, so no.

1. Explain four differences between TCP and UDP. Mention two advantages and disadvantages of both. **[5 points]**

Differences:

* TCP connection based, UDP connectionless.
* TCP slower, UDP faster
* TCP error checking, UDP no error checking
* TCP reliable, UDP unreliable

TCP Advantages:

* Error checking to make sure packets got to dest.
* Data recovery to make sure all packets got to dest.

TCP Disadvantages:

* High overhead, lots going on in the background.
* Slow, needs 3-way handshake and constant error checking

UDP Advantages:

* Faster, sends packets regardless of if it gets there 100%.
* Low overhead, no need for errorchecking.

UDP Disadvantages:

* Unreliable
* No data recovery

1. Release the DHCP IP from the client R1. What command did you use? Paste the screenshot of the packet capture on Wireshark where these DHCP messages are captured. **[5 points]**

Release dhcp fastethernet 0/0

A screenshot of a computer

Description automatically generated

1. Can the server also retrieve the DHCP IP back from the client before the lease time is over? If yes, what command can you use on the server to do this? **[5 points]**

Yes, clear ip dhcp binding ‘IP’, then to get the IP back, do this command:

Renew dhcp fastethernet 0/0

1. Now turn on DHCP debugging on R1 and R3. What commands did you use? **[3 points]**

Debug ip dhcp server events

debug ip dhcp server packet

1. Update the configuration on R2 to provide extra DHCP option for DNS. The DNS server you are using should be R2 itself. Include the appropriate IP address(es) to use in the DHCP configuration. Paste a screenshot of updated DHCP configuration on R2.

**[10 points]**

A screenshot of a computer

Description automatically generated

1. After DHCP is successful, paste screenshots of debug messages you captured on R1 and R3 indicating the success. **[10 points]**

A screenshot of a computer program

Description automatically generated

Objective-3: Getting started with DNS

1. Now configure R2 as the DNS server. Below are the mappings you will add on the DNS server:

**Hostname IP address**

R1 R1’s interface IP

R2 R2’s interface IP

Paste a screenshot of the configuration on R2 indicating the hostname configurations. **[10 points]**

A screenshot of a computer screen

Description automatically generated

1. To implement DNS, do you need any additional configuration on R1 and R3? If yes, explain and paste screenshots. If not, explain. **[5 points]**

Yes, all you need to input to R1 and R3 in their configs are “ip domain lookup” then it will allow dns resolution. I looked through the config and it didn’t explicitly show this command in it, but knowing that DHCP gave all the info that it needed to R1 and R3, dns resolution does work.

A computer screen with white text

Description automatically generated

My router is named R5, but it acts as R1 according to the topology.

1. If DNS is successfully configured, from R1 you should be able to issue the command “ping R2” and on R2 use the command “ping R1”. Show screenshots of the ping working. **[10 points]**

R5 is R1 in my case. R4 is R2 in my case as well.

A screenshot of a computer program

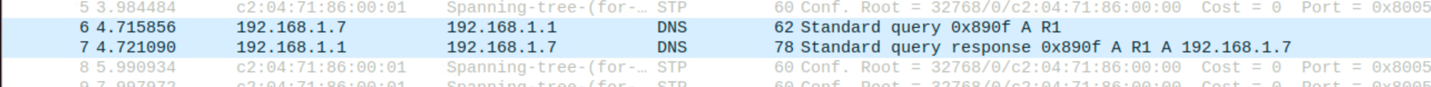
Description automatically generated

A screenshot of a computer code

Description automatically generated

1. Initiate a Wireshark capture in your topology. Where would you initiate the capture? Paste a screenshot of the Wireshark capture of the DNS messages that are exchanged when you issue either “ping R1” or “ping R2” command. **[10 points]**

I would initiate the capture between R1 and R2.



1. Explain in detail the sequence of DNS messages that are exchanged. **[8 points]**

According to the sequence of DNS messages from above, R1 is requesting a name resolution of the name ‘R1’. R2 receives this message because R2 is the dns-server of R1 and resolve the IP of the domain name ‘R1’. R2 receives this message and it can now ping the IP of ‘R1’.

1. Did DNS use UDP or TCP as the transport layer protocol in this case? Will it ever use the other protocol? If yes, when? **[3 points]**

It used UDP. It can use TCP if data transfer fails on UDP. It can also use TCP if the dns data exceeds the packet size of a UDP packet.

Objective-4: Report Questions

1. Run Wireshark on your laptop and start the capture on the interface going to the Internet. Ping [www.google.com](http://www.google.com)
2. What IP is your laptop using as the DNS server? How do you know this? **[2 points]**

DNS is 192.168.1.1 or my DG. I know in the request packet for DNS in my Wireshark capture. To my best knowledge, my computer goes to my DG for the DNS request and my DG actually has public DNS servers set to it where it can then request a resolution.

1. For a DNS query, what is the source and destination port numbers? **[2 points]**

Src: 65255, Dest: 53

1. For a DNS response what is the source and destination port numbers? **[2 points]**

Src: 53, Dest: 65255

1. Clear any DNS cache on your laptop. How did you do this? Paste screenshot. **[2 points]**

On my mac, I used the command:

sudo dscacheutil -flushcache

sudo killall -HUP mDNSResponder

1. Paste a screenshot of the DNS messages exchanged in this case. Did DNS use UDP or TCP in this case? **[2 points]**

A screenshot of a computer

Description automatically generated

It used UDP.

1. You had your DNS cache cleared. Assume all DNS nameservers in the world have their DNS cache cleared. Now explain in theory how your DNS query is resolved. Assuming no caches exist, what levels of the hierarchy does the query need to propagate through to get resolved? Explain the sequence of events and the flow. **[10 points]**

In theory, if I were to first ping google.com, it would go to my default gateway as a DNS request, and my DG would create a connection with its set DNS server, being 1.1.1.1. I would expect it to create a either a UDP or TCP connection based on the size of the packets. It would send it to the DNS server and the DNS would then send the resolved IP of google.com back. To get this resolved domain name, the hierarchy of DNS servers that it would have to traverse first starts with the root DNS, then TLD and finally the authoritative DNS server. To get back to the sender, it will go back through backwards.

1. Explain briefly the different type of DNS records. **[5 points]**

Type a: has name and value

Type ns: also has name and value but value is of the authoritative name server

Type cname: has name which is an alias for the real name. and the value is the real name.

Type mx: value is name of mail server.

1. What are the different types of DNS nameservers? Could you configure your laptop to be a DNS server too? If yes, explain what type of DNS nameserver or nameservers it can be. **[5 points]**

Root DNS Server

Top Level Domain Server

Authoritative DNS Server

Recursive DNS Server

Caching DNS Server

Forwarding DNS Server

I could configure my laptop to be a DNS server too. Technically I could expect my laptop to be configured as any type of DNS server, but for my usability in my network, I would set it as a Caching DNS Server. This means I could use the cache information from the server to resolve domain name’s much faster.

1. Explain briefly the HTTP Error Messages with their status code. **[2 points]**

200 OK: request succeeded

301 Moved Permanently: requested object moved

400 Bad Request: request msg not understood by server

404 Not Found: document not found on server

505 HTTP: Version not supported

1. Explain briefly the different types of HTTP requests. **[2 points]**

GET: retireve data from server

POST: submit data to specified resource

1. What is a proxy web server? Mention any four advantages of using a proxy webserver.

**[3 points]**

A proxy server is basically a caching server that allows clients to request data without involving the original server

* Reduce response time to client
* Reduce traffic on servers network
* Can filter content for malicious traffic
* Proxy servers provide anonymity by masking clients IP

1. You are trying to connect to [www.bbc.com](http://www.bbc.com) but the page does not load and keeps buffering. So now you try to connect to [www.cnn.com](http://www.cnn.com) and the page loads relatively faster. Brainstorm four possible reasons that could have led to this scenario. Mention the steps you will follow to troubleshoot this. **[10 points]**

Four Possible Reasons:

* CNN has a proxy server and BBC does not
* Possible DNS resolution issues
* Possible packet loss for BBC and not CNN
* Higher than usual traffic on BBC

Troubleshoot steps:

1. First, I would determine if this had every happened before and has it worked in the past.
2. From this scenario, it either seems we can get to the internet or that CNN has been cached at some point allowing us to load the webpage faster. I would try a traceroute to both BBC and CNN and see where there is increased latency.
3. I would then make sure our set DNS servers are up and not experiencing any unusual traffic by checking the ping latency to those servers.
4. From there I would hope that would figure out where the latency issues are happening.
5. What is a major disadvantage in using HTTP? What is another protocol that would solve this issue? **[2 points]**

A major disadvantage of using HTTP is that it is insecure and transfers data in plain text. Another protocol that would solve this problem is HTTPS as it uses TLS which is a protocol that encrypts HTTP traffic.

Objective-5: DHCP Relay- Extra Credit [+20]

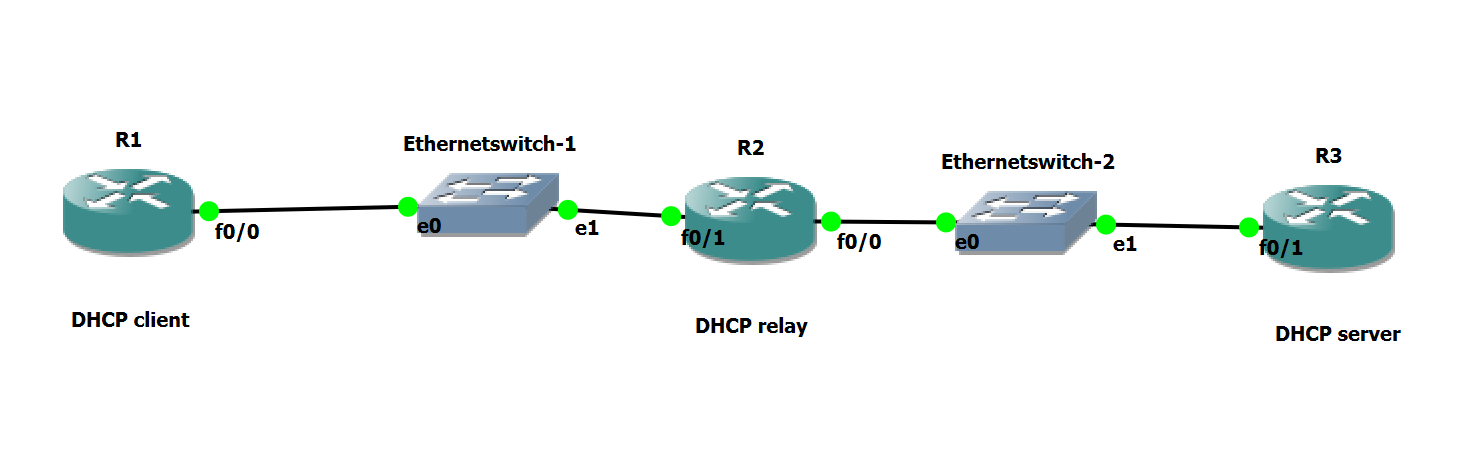


Fig.3

1. What is a DHCP relay? When would you use one? **[2 points]**
2. Clear any previous configurations on your topology. Setup the topology shown in Fig3. Initiate a Wireshark capture on Switch-1 and a simultaneous Wireshark capture on Switch-2.
3. In this case, R1 should be configured as a DHCP client to get its IP from R3 which is the DHCP server. R2 is the DHCP relay.
4. Paste screenshot of DHCP and interface configurations on R1, R2 and R3 that will work.

(Hint: show run | begin ip dhcp and sh ip int br) **[5 points]**

1. Is the configuration on DHCP server and DHCP client same as before? Or did you have to do anything extra in this case? If yes, mention the extra configuration you had to do.

**[3 points]**

1. After successful DHCP, examine the Wireshark capture.

Mention Source IP, Dest IP, Source MAC and Dest MAC of all 4 DHCP messages for the capture on the Ethernet-1 switch interface. Also note if each individual message is a broadcast or unicast message at Layer-2 and Layer-3. **[5 points]**

1. Mention Source IP, Dest IP, Source MAC and Dest MAC of all 4 DHCP messages for the capture on the Ethernet-2 switch interface. Also note if each individual message is a broadcast or unicast message at Layer-2 and Layer-3. **[5 points]**

Format:

Src IP Dest IP Src MAC Dest MAC L2 L3

DHCP Discover XXXX YYYY abcd efgh uni/broadcast uni/broadcast

…… ….. …… ……….. …… …… …..

Score: \_\_\_\_\_ / 200 points [+20 points]