Southeast Europe Journal of Soft Computing
Available online: http://scjournal.ius.edu.ba

ISSN 2233 – 1859

Vol 11, No. 2, September 2022, pp. 01-05

Practical Assignment for CCNA7 part 3, Enterprise Network Security and Automation

[1*]Galymzada Alin, [1]Viktor Pyagay

[1] Department of Computer Engineering and Information Security
of the International University of Information Technologies,
050040, 34/1 Manas Str., suite 409
Kazakhstan, Almaty
**Corresponding Author*: g.alin@iitu.edu.kz, v.pyagai@iitu.edu.kz

Article Info

Article history:

Article received on 12 April 2022

Received in revised form 01 August 2022

ABSTRACT: This article continues the discussion of the general requirements of new Cisco CCNA7 course and particularly provides the ideas of practical assignments for this course based on the Packet Tracer (PT). This article adds some corrections to previously provided approaches in [8] to managing and automation of the student practical skills assessments. The article also demonstrates the option of point distribution in assignment management and discusses the possible potholes and issues.

Keywords:

CCNA7 course, packet tracer assignment, networking, assessment of students' knowledge

1. INTRODUCTION

CCNA course version 7 proposed numbers of practical assignment for networking skills in [5]. The advantages of Cisco Packet Tracer were perfectly reviewed in [4] as comparing to GNS3 [3] Cisco PT provides various methods to automate the process of grading of students' level of assignment completion. Of course, if we need to conduct the education for CCNP course [6] GNS3 tool is more preferable due to the comprehensive functions and features covered in CCNP materials. However, the migration to CCNA v7 still requires to develop some non-standard and complicated assignments for new version. This article considers the new assignment specifically developed to cover the main topics of CCNA v7 course materials.

2. PACKET TRACER PROJECT DESCRIPTION

The topology of the PT project is presented in the picture 1 and it consists of Head Quarter and Branch offices connected by routers R1 / R2 correspondingly via two internet service providers ISP1 and ISP2. ISP2 connection is used to setup IPsec tunnel between two offices while ISP1 connection is used to install PAT on R1 / R2 and then check the internet access from office PCs to ISP server. R1 has also been configured by static NAT to provide the access to the internal server of Head Quarter office – HQ TFTP/HTTP server. The switching topology of both offices consists of one core switch HQ-CS / BR-CS and two switches of access level HQ-AS1 / BR-AS1 and HQ-AS2 / BR-AS2 connected by two uplinks configured into Ether Channel ports to provide the required redundancy and load balancing.

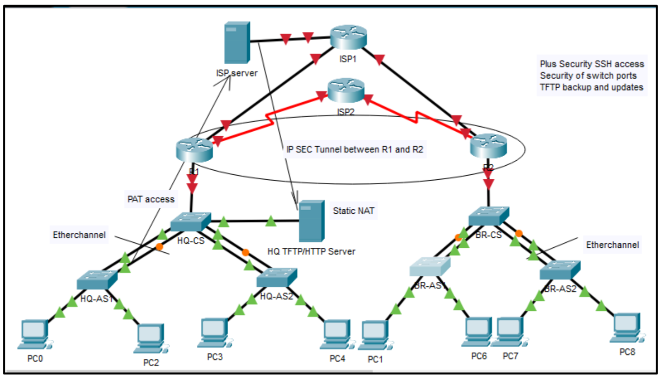
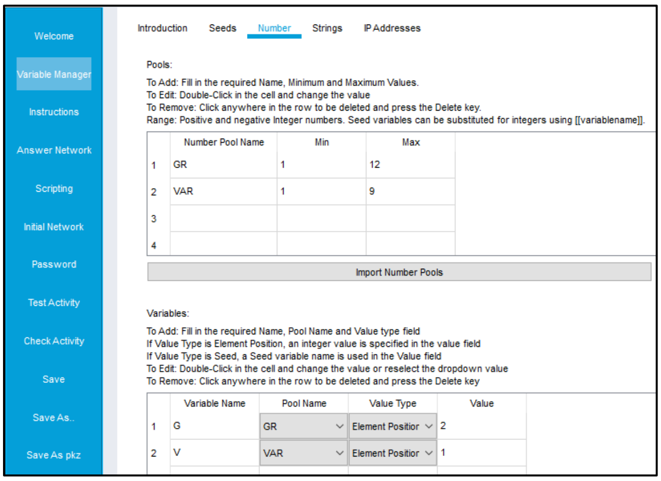


Figure 1: Network topology

The Variable Manager was set to use two numeric variables G (group number) and V (variant number) – see the Figure 2:



Pools:

To Add: Fill in the required Name, Minimum and Maximum Values.
To Edit: Double-Click in the cell and change the value
To Remove: Click anywhere in the row to be deleted and press the Delete key.
Range: Positive and negative Integer numbers. Seed variables can be substituted for integers using [[variablename]].

	Number Pool Name	Min	Max
1	GR	1	12
2	VAR	1	9
3			
4			

Variables:

To Add: Fill in the required Name, Pool Name and Value type field
If Value Type is Element Position, an integer value is specified in the value field
If Value Type is Seed, a Seed variable name is used in the Value field
To Edit: Double-Click in the cell and change the value or reselect the dropdown value
To Remove: Click anywhere in the row to be deleted and press the Delete key

	Variable Name	Pool Name	Value Type	Value
1	G	GR	Element Positior	2
2	V	VAR	Element Positior	1

Figure 2: Variable manager

The instruction Table 1 (part 1 and 2) represents the main instruction of the PT project where [[G]] and [[V]] are used to generate various IP addresses.

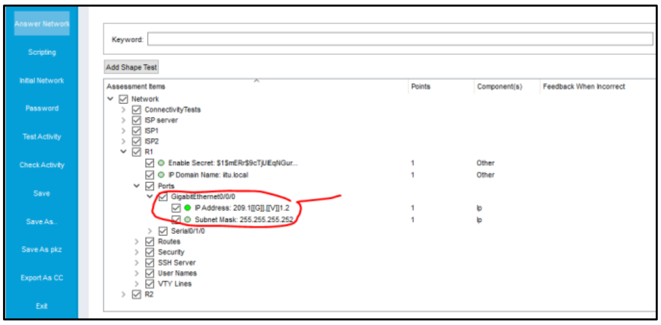
Table 1, part 1 Istruction table: device names, models, port and VLANs

Device name	**Model**	**Port**	**VLAN**
ISP1	2911	G0/0	-
		G0/1	-
		G0/2	-
ISP2	2911	S0/3/0	-
		S0/3/1	-
ISP server		Fa0	-
R1	ISR4321	G0/0/0	-
		S0/1/0	-
		G0/0/1	TR
		G0/0/1.10	10
		G0/0/1.20	20
		G0/0/1.40	40
HQ-CS	2960	Fa0/23-24	TR
		Fa0/21-22	TR
		Fa0/1	10
		G0/1	TR
		VLAN40	
HQ-AS1	2960	Fa0/23-24	TR
		Fa0/1	10
		Fa0/2	20
		VLAN40	
HQ-AS2	2960	Fa0/23-24	TR
		Fa0/1	10
		Fa0/2	20
		VLAN40	
PC0/PC2		Fa0	10
PC3/PC4		Fa0	20
HQ TFTP / HTTP Server		Fa0	
R2	ISR4321	G0/0/0	-
		S0/1/0	-
		G0/0/0	TR
		G0/0/0.30	30
		G0/0/0.50	50
		G0/0/0.40	40
BR-CS	2960	Fa0/23-24	TR
		Fa0/21-22	TR
		G0/1	TR
		VLAN40	
BR-AS1	2960	Fa0/23-24	TR
		Fa0/1	30
		Fa0/2	50
		VLAN40	
BR-AS2	2960	Fa0/23-24	TR
		Fa0/1	30
		Fa0/2	50
		VLAN40	
PC1/PC6		Fa0	30
PC7/PC8		Fa0	50

Table 2, part 2 Istruction table: ip addresses, subnet mask, default gateway and comments

IP address	Subnet mask	Default Gateway	Comments
209.1[[G]].[[V]]1.1	/30	-	to R1
209.1[[G]].[[V]]2.1	/30	-	to R2
209.1[[G]].[[V]]3.1	/30	-	to ISP server
209.2[[G]].[[V]]1.1	/30	-	to R1
209.2[[G]].[[V]]2.1	/30	-	to R2
?.?.?.?	/30	?.?.?.?	to ISP1
?.?.?.?	/30	?.?.?.?	to ISP1
?.?.?.?	/30	?.?.?.?	to ISP2
			to HQ-CS
10.[[G]].1[[V]].1	/24	-	to HQ-CS
10.[[G]].2[[V]].1	/24	-	to HQ-CS
10.[[G]].4[[V]].1	/24	-	to HQ-CS
Ether channel			to HQ-AS1
Ether channel			to HQ-AS2
			to HQ TFTP / HTTP Server
			to R1
10.[[G]].4[[V]].2	/24	10.[[G]].4[[V]].1	Manage-ment
Ether channel			to HQ-CS
			to PC0
			to PC2
10.[[G]].4[[V]].3	/24	10.[[G]].4[[V]].1	Manage-ment
Ether channel			to HQ-CS
			to PC3
			to PC4
10.[[G]].4[[V]].4	/24	10.[[G]].4[[V]].1	Manage-ment
DHCP VLAN10			to HQ-AS1
DHCP VLAN20			to HQ-AS2
			to HQ-CS
?.?.?.?	/30	?.?.?.?	to ISP1
?.?.?.?	/30	?.?.?.?	to ISP2
			to BR-CS
10.[[G]].3[[V]].1	/24	-	to BR-CS
10.[[G]].5[[V]].1	/24	-	to BR-CS
10.[[G]].4[[V]].1	/24	-	to BR-CS
Ether channel			to BR-AS1
Ether channel			to BR-AS2
			to R2
10.[[G]].4[[V]].2	/24	10.[[G]].4[[V]].1	Manage-ment
Ether channel			to BR-CS
			to PC1
			to PC7
10.[[G]].4[[V]].3	/24	10.[[G]].4[[V]].1	Manage-ment
Ether channel			to BR-CS
			to PC6
			to PC8
10.[[G]].4[[V]].4	/24	10.[[G]].4[[V]].1	Manage-ment
DHCP VLAN30			to BR-AS1
DHCP VLAN50			to BR-AS2

All corresponding variables are configured in Answer Network (see the figure 3) to support the collection of required grades:



Assessment Items	Points	Component(s)	Feedback When Incorrect
☑ Network			
☑ ConnectivityTests			
☑ ISP server			
☑ ISP1			
☑ ISP2			
☑ R1			
☑ ○ Enable Secret: $1$mERr$9cTjUEqNGur...	1	Other	
☑ ○ IP Domain Name: iitu.local	1	Other	
☑ Ports			
☑ GigabitEthernet0/0/0			
☑ ● IP Address: 209.1[[G]].[[V]]1.2	1	Ip	
☑ ○ Subnet Mask: 255.255.255.252	1	Ip	
☑ Serial0/1/0			
☑ Routes			
☑ Security			
☑ SSH Server			
☑ User Names			
☑ VTY Lines			
☑ R2			

Figure 3: Answer Network

3. ASSIGNMENT CONTENT

3.1. The first part of the project:

This part was developed to check the basic knowledge of IP configuration, securing the router management access and routing [1], [2].

- Complete the missed information '?.?.?.?' in the instruction table and then configure IP addresses of ISP1, ISP2, R1, R2 and ISP Server;
- Make sure that you can ping IP addresses of ISP1, ISP2 from R1, R2 and ISP Server from R1, R2;
- On the router R1, R2 please also configure the enable secret password 'class', security account 'user ' (privilege level 0) and 'admin' (privilege level 15) with passwords 'cisco'.
- Setup the remote connection via SSH only, the encryption key size is 1024, ip domain is 'iitu.local'.
- Configure the default static routes on R1, R2 over ISP2 and the static routes on R1, R2 to ISP Server via ISP1

Instead of configuring default static routes there is another option depending on different needs:

- Configure standard ACL#99 to allow the remote connection to R1, R2 via SSH from RCom only.
- Configure OSPF process 1 on R1, R2 and RCom (include networks of VLANs 10, 20, 30, 50 accordingly): make sure you can ping R1 from R2 or back.
- Configure OSPF so that routing updates are not sent into networks where they are not required.
- Configure the static routes on R1 and R2 to ISP server over ISP1 and make sure you can ping it.

3.2. The second part of the project:

This part was developed to check the basic knowledge of switch access and trunk ports configuration, securing the switch management access and EtherChannel technology[1], [2].

Setup and configure the switches of Head Quarter (HQ-CS, HQ-AS1, HQ-AS2) and Branch office (BR-CS, BR-AS1, BR-AS2):

- Protect the access to the privileged exec mode on all switches using encrypted password 'class', as well as security account 'user ' (privelege level 0) and 'admin' (privelege level 15), both with ecnrypted passwords 'cisco'.
- Setup the remote connection via SSH only, the encryption key size is 1024, ip domain is 'iitu.local'.
- Configure the port-security settings on active access ports:
    - Maximum MAC is 2
    - Dynamic learning of MACs
    - BPDU protection and Portfast are enabled

- Configure the required VLANs 10, 20, 30, 40, 50 where 40 is Management VLAN
- Disable all unused ports
- Configure the Etherchannels between Core switches and switches of Access level:
    - HQ-CS and HQ-AS1: Group #1 mode ON
    - HQ-CS and HQ-AS2: Group #2 mode ON
    - and the same in Branch office (BR-CS and BR-AS1 / BR-CS and BR-AS2)

- Turn off the negotiation on trunk ports
- Make sure that native VLAN 99 on all trunk and list of allowed VLAN includes only required ones.

3.3. The third part of the project:

This part was developed to check the basic knowledge of VLAN configuration, DHCP configuration, inter-vlan routing and SVI configuration [1], [2].

Restore the configuration done in the previous parts of assignment and then setup the Management VLAN 40 on all switches and DHCP for PCs:

- Configure the required IP addresses and subnet mask of VLAN 40 (Management VLAN) on all switches;
- Configure Router on stick (subinterfaces) in R1 and R2 in order to provide the connectivity among VLANs; Setup the Management VLAN 40 (description 'Management') on all switches and DHCP for PCs:
- Configure the required IP addresses and subnet mask of VLAN 40 (Management VLAN) on all switches

- Configure Router on stick (subinterfaces) in R1 and R2 in order to provide the connectivity among VLANs (description of subinterfaces 'VLAN XX')
- Configure DHCP range on R1 and R2 for VLAN 10,20,30,50 (pool name VlanXX) and make sure that PC1-PC8 can obtain the required IP addresses
- Exclude the gateway IP addresses and IP address of HQ TFTP/HTTP Server (X.X.X.200-254)
- Configure formal DNS server 8.8.8.8. in each pool.

3.4. The fourth part of the project:

This part was developed to check the basic knowledge of PAT and static NAT configuration, static routing [1], [2].

Restore the configuration done in the previous parts of assignment and then configure the Network Address Translation on R1 and R2 routers:
- Make sure that all PCs of HQ and BR can open the web-site of ISP Server via PAT (source ACL #1);
- Configure static NAT on R1 to access the HQ TFTP/HTTP server via external IP address 64.1[[G]].5[[V]].1;
- Make sure that you can open the web-site on HQ TFTP/HTTP server from ISP Server. In order to achieve the web-site of internal HQ TFTP/HTTP server from ISP server please provide the proper static route on ISP1.

3.5. The fifth part of the project:

This part was developed to check the basic knowledge of IPSec tunnel configuration [1], [2].

Restore the configuration done in the previous parts of assignment and then configure the IPSEC tunnel between R1 and R2 routers:
- Make sure that you use policy 10 with encryption AES 256, authentication pre-share key "secretkey" and group 5;
- Transform-set with ESP-AES 256 ESP-SHA-MAC and names R1->R2, R2->R1 correspondingly
- Configure crypto map IPSEC-MAP (Source ACL #100);
- Make sure that you can open the web-site on HQ HTTP/HTTP server from PC7 and PC1.

3.6. The sixth part of the project:

This part was developed to check the basic knowledge of Cisco devices IOS and configuration maintenance by using TFTP server [1], [2].

Restore the configuration done in the previous parts of assignment and then backup all active equipment configuration in HQ on HQ TFTP/HTTP server:
- Make sure that you can ping HQ TFTP/HTTP server from all switches and router of HQ;
- Copy the configuration files to HQ TFTP/HTTP server: R1-confg, HQ-CS-confg, HQ-AS1-confg, HQ-AS2-confg;
- Make sure that you can copy the configuration of HQ equipment from HQ TFTP/HTTP server to the flash: R1-confg.text, HQ-CS-confg.text, HQ-AS1-confg.text, HQ-AS2-confg.text
- Upgrade IOS of HQ switches from HQ TFTP server up to version: c2960-lanbasek9-mz.150-2.SE4.bin

3.7. Additional task (bonus)

- Radius authentication

Please review the topology of your project (see the figure 4) and the table with additional instructions (see the figure 5)

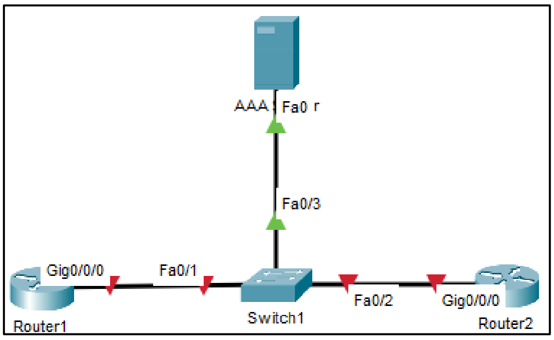
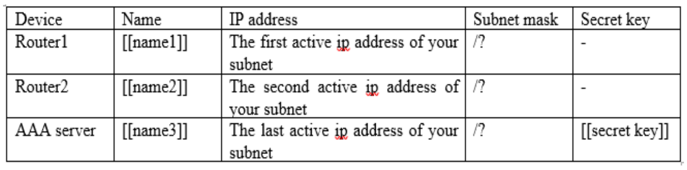


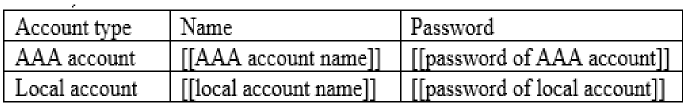
Figure 4: Network topology of additional assignment



Device	Name	IP address	Subnet mask	Secret key
Router1	[[name1]]	The first active ip address of your subnet	/?	-
Router2	[[name2]]	The second active ip address of your subnet	/?	-
AAA server	[[name3]]	The last active ip address of your subnet	/?	[[secret key]]

Figure 5. Instruction table of additional assignment (all variables in [[…]] are setup via Variable Manager)

Please configure both Routers for Radius Server authentication:
1) Split the network 200.100.4.0/24 into 32 subnets and take the ([[V]]+1)-subnet
2) VTY access
- Setup the remote connection via SSH only, the encryption key size is 1024, ip domain is 'iitu.local'.
3) Console, VTY access and enable mode via Radius authentication and local authentication as a backup method (see the figure 6).
- Make sure that you can login to both routers with AAA server online and offline (over backup account).

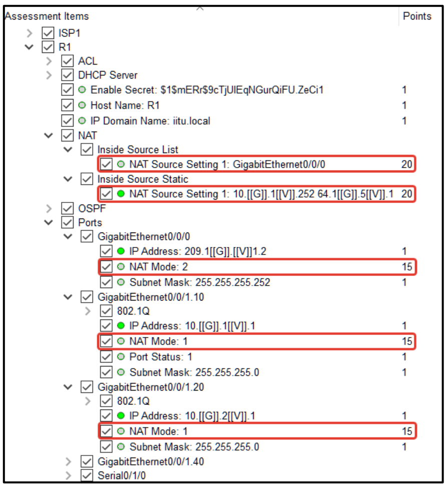


Account type	Name	Password
AAA account	[[AAA account name]]	[[password of AAA account]]
Local account	[[local account name]]	[[password of local account]]

Figure 6. Instruction table of additional assignment (all variables in [[…]] are setup via Variable Manager)

3.8. Assessment managing. Points distribution

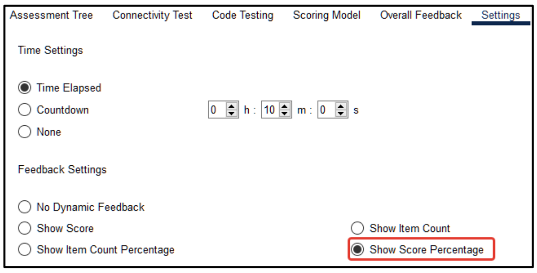
It is also a good practice to redistribute points in each part of the project according to the main task. For example, in part four put more points for configurations related to the NAT protocol. As it represented in the figure 7.



```
Assessment Items                                                       Points
  > ☑ ISP1
  ⌄ ☑ R1
    > ☑ ACL
    > ☑ DHCP Server
      ☑ ○ Enable Secret: $1$mERr$9cTjUlEqNGurQiFU.ZeCi1                  1
      ☑ ○ Host Name: R1                                                   1
      ☑ ○ IP Domain Name: iitu.local                                      1
    ⌄ ☑ NAT
      ⌄ ☑ Inside Source List
          ☑ ○ NAT Source Setting 1: GigabitEthernet0/0/0                  20
      ⌄ ☑ Inside Source Static
          ☑ ● NAT Source Setting 1: 10.[[G]].1[[V]].252 64.1[[G]].5[[V]].1 20
    > ☑ OSPF
    ⌄ ☑ Ports
      ⌄ ☑ GigabitEthernet0/0/0
          ☑ ● IP Address: 209.1[[G]].[[V]]1.2                             1
          ☑ ○ NAT Mode: 2                                                 15
          ☑ ○ Subnet Mask: 255.255.255.252                                1
      ⌄ ☑ GigabitEthernet0/0/1.10
        > ☑ 802.1Q
          ☑ ● IP Address: 10.[[G]].1[[V]].1                               1
          ☑ ○ NAT Mode: 1                                                 15
          ☑ ○ Port Status: 1                                              1
          ☑ ○ Subnet Mask: 255.255.255.0                                  1
      ⌄ ☑ GigabitEthernet0/0/1.20
        > ☑ 802.1Q
          ☑ ● IP Address: 10.[[G]].2[[V]].1                               1
          ☑ ○ NAT Mode: 1                                                 15
          ☑ ○ Subnet Mask: 255.255.255.0                                  1
      > ☑ GigabitEthernet0/0/1.40
      > ☑ Serial0/1/0
```

Figure 7. Example of points redistribution

In order to represent this in dynamic completion feedback during the task, the "Show Score Percentage" option should be selected, as it is demonstrated on figure 8.



Time Settings

● Time Elapsed
○ Countdown　0 h : 10 m : 0 s
○ None

Feedback Settings

○ No Dynamic Feedback
○ Show Score
○ Show Item Count Percentage
○ Show Item Count
● Show Score Percentage

Figure 8. Show Score Percentage

4. CONCLUSION

The considered PT assignment consists of 6 main tasks which encompassed the previously completed tasks and covered all main modules of CCNA version 7 course [5]: static routing, ACLs, NATs, IPSec and IOS maintenance. However, there are several opportunities and recommendations were identified:

- The variable manager of PT can give you enough flexibility to create the group assignment for different variants of IP addresses and other configuration settings

- To harden the completion of the assignment it is recommended to include the connectivity tests and hide the "Check results" or "Assessment tree"

- The formal check of PT completion does not mean that the configured network is working properly. Therefore, some comprehensive check is required

- Activity grader does not work properly in several cases: for instance, when the total size of one pka-file archive exceeded 6Mb or the pka-file inside of archive is not converged properly.

Overall it is a good automation tool for student skills assessment in addition to recommended assignments in [7].

REFERENCES

[1] Lammle, T. Cisco CCNA Certification, 2 Volume Set: Exam 200-301, 1st Edition, Sybex Publishing, 2020.

[2] Odom W. CCNA 200-301 Official Cert Guide, Volume 2, 1st Edition, Cisco Press, 2020.

[3] Gil, P., Garcia, G. J., Delgado, A., Medina, R. M., Calderon, A., & Marti, P. (2015). Computer networks virtualization with GNS3: Evaluating a solution to optimize resources and achieve a distance learning. In Proceedings - Frontiers in Education Conference, FIE (Vol. 2015–Febru, pp. 1–4). IEEE. https://doi.org/10.1109/fie.2014.7044343.

[4] Javid, S. R. (2014). Role of Packet Tracer in learning Computer Networks. International Journal of Advanced Research in Computer and Communication Engineering, 3(5), 6508– 6511.

[5] Mark Taub, Editor-in-Chief. Enterprise Networking, Security, and Automation Companion Guide (CCNAv7) Cisco Networking Academy Copyright© 2020 Cisco Systems, Inc. Published by Cisco Press 2020.

[6] Brad Edgeworth, Ramiro Garza Rios, David Hucaby, Jason Gooley CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide Copyright © 2020 Cisco Systems, Inc. Published by: Cisco Press.

[7] CCNAv7 Enterprise Networking, Security, and Automation (ENSA). Student Lab Manual (online UML modeling and system architecture for agent based information retrieval D. Muhammad Noorul Mubarak, Philomina Simon. International Journal of Computer Science & Information Technology (IJCSIT) Vol 7, No 6, December 2015.

[8] G. Alin, T. Nurlybayev CCNA7 Cisco networking course: Practical assignment. Southeast Europe Journal of Soft Computing, Vol 10, No. 1, March 2021, pp. 49-54.