Farzad Kheirabadi
CYB 555
UNIT 7

TACAS+

• TACACS+ (Terminal Access Controller Access System) is a Cisco proprietary protocol for communication between the Cisco client and the Cisco ACS server. It uses the TCP port 49, which makes it dependable.

• TACACS+ separates authentication, authorization, and accounting.

• All AAA packets are encrypted and should be used for ACS.

• It allows for more granular control, such as specifying the authorization command.

• TACACS+ provides multiprotocol support for device administration • TACACS+ is more dependable than RADIUS since it leverages TCP.

• TACACS+ allows for additional control over command authorization, whereas RADIUS does not allow for external command authorization.

• TACACS+ encrypts all AAA packets, whereas RADIUS encrypts only the credentials, making it safer.

RADIUS

• Remote Access Dial-In User Service (RADIUS) is an open standard protocol that allows any vendor AAA client to communicate with an ACS server.

• If one of the clients or servers is from a different vendor, we must use RADIUS.

• For authentication and permission, it utilizes port 1812, and for accounting, it uses port 1813.

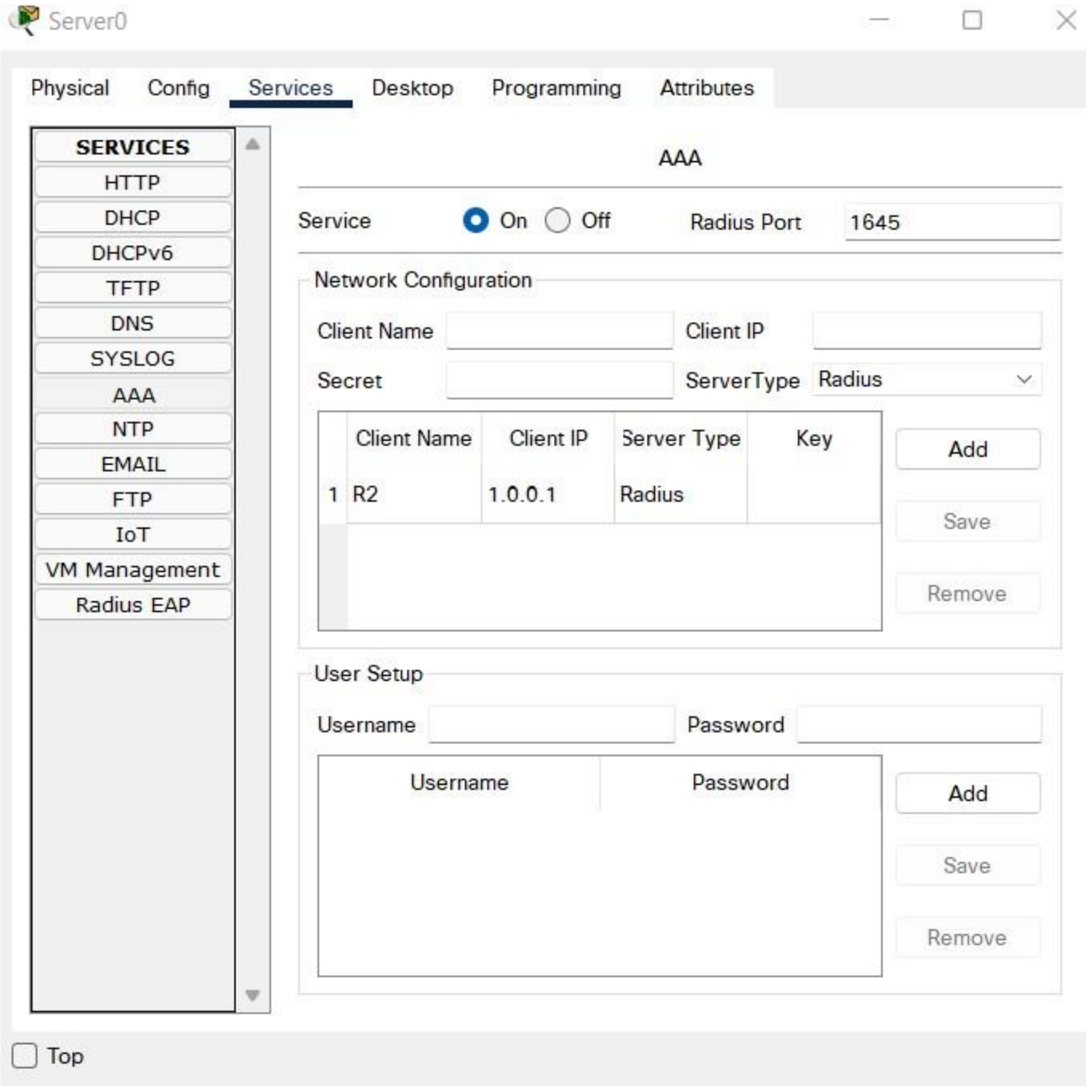
• Because RADIUS is an open standard, it may be used with devices from various vendors, whereas TACACS+ is proprietary to Cisco and can only be used with Cisco equipment.

• It's used to connect to the internet.

• Does not allow multi-protocol • Does not provide external command authorization

Farzad Kheirabadi
CYB 555
UNIT 7

• Only the password is encrypted, whereas other information such as usernames, accounting information, and so on is not encrypted.



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name

Client IP

Secret

ServerType Radius

	Client Name	Client IP	Server Type	Key
1	R2	1.0.0.1	Radius	

User Setup

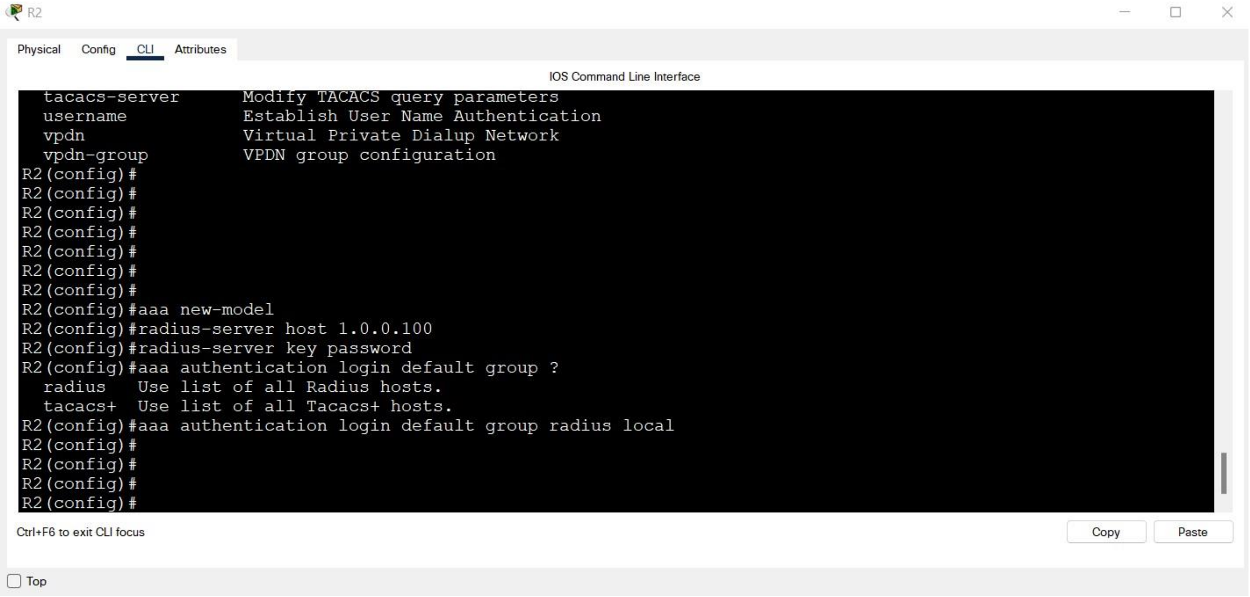
Username

Password

Username	Password

□ Top

Farzad Kheirabadi
CYB 555
UNIT 7



```
  tacacs-server      Modify TACACS query parameters
  username           Establish User Name Authentication
  vpdn               Virtual Private Dialup Network
  vpdn-group         VPDN group configuration
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#aaa new-model
R2(config)#radius-server host 1.0.0.100
R2(config)#radius-server key password
R2(config)#aaa authentication login default group ?
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
R2(config)#aaa authentication login default group radius local
R2(config)#
R2(config)#
R2(config)#
R2(config)#
```

ACL

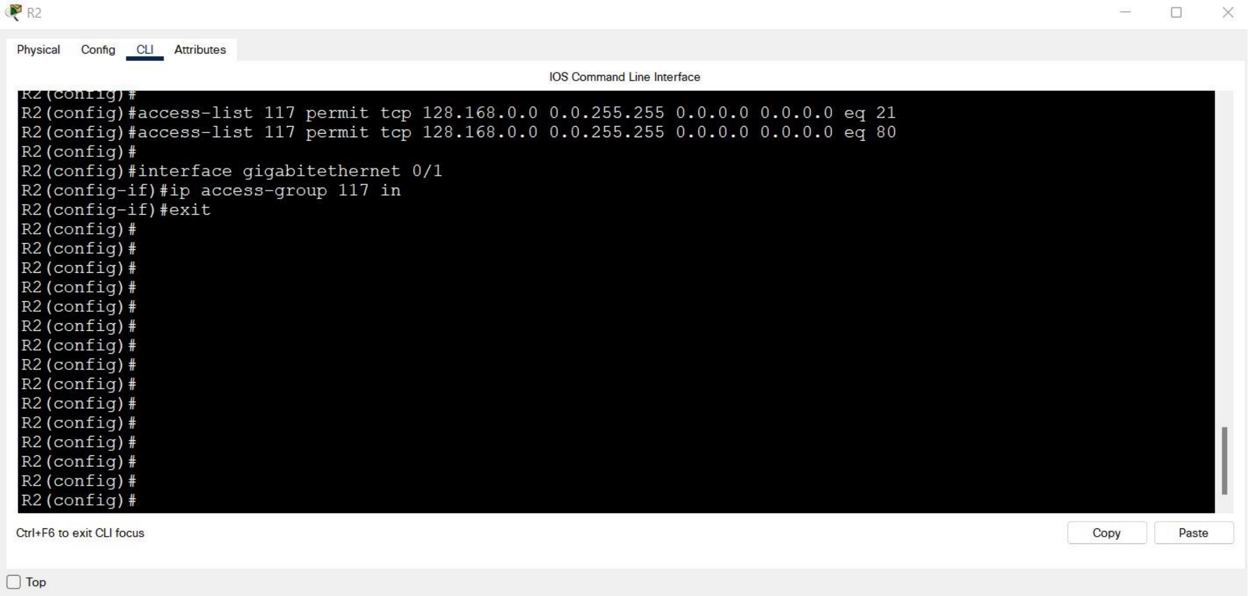
An access control list (ACL) is a set of rules that determines whether users or systems have access to a certain item or system resource. Enter control lists are filters that are implemented in routers or switches that manage which traffic can access the network. A security characteristic on each system resource identifies the access control list. Each user that has access to the system has an entry in the list. The ability to read a file or all of the files in a directory, write to the file or files, and execute the file if it's an executable file or program are the most frequent privileges for a filing system ACL. Network interfaces and operating systems (OSes), such as Linux and Windows, have ACLs. Access control lists are commonly used on networks to prevent or allow specific types of traffic. They frequently censor traffic based on its origin and destination.

Access control lists can be installed on almost any security or routing device, and having many ACLs in different regions of the network might be advantageous. ACLs have a similar temperament to network endpoints that require high speed, performance, and security, such as apps or servers. According to the specification, network administrators may prefer to install an access control list at various places throughout the network. Because they border the general public internet, ACLs are frequently set on a network's sting routers. The ACL can then use this information to filter traffic before it reaches the rest of the network. Edge routers with ACLs can be deployed in the DMZ (dedicated network zone) between the public internet and the rest of the network. A DMZ could be a buffer zone with an outward-facing router that provides general network security. It also has an indoor router that divides the secured network from the DMZ.

ACLs are divided into two types: 1. system of classification ACLs control who has access to which files and directories. They provide OSes with the instructions for establishing user access permissions and privileges for the system once it has been accessed.

2. Networking ACLs control network access by instructing network switches and routers on which types of traffic are permitted to communicate with the network. Once inside the network, these ACLs also define user permissions. The networking ACL rules are predefined by the network administrator. They act as a firewall throughout this time.

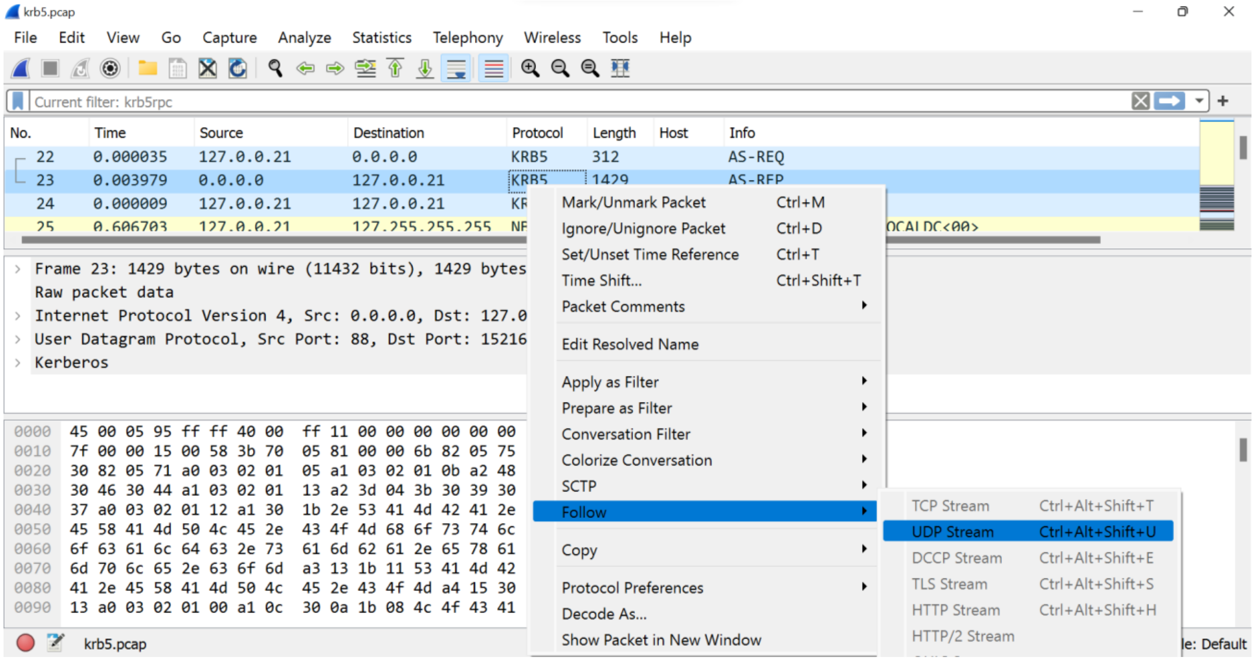
Each ACL contains one or more access control entries (ACEs), each of which contains the name of a user or group of users. A job title, such as programmer or tester, might be used as the user. The access privileges for each of those users, groups, or roles are specified in an access mask, which is a string of bits. The access control list for an object is usually created by the computer user or the item owner.



```
R2(config)#
R2(config)#access-list 117 permit tcp 128.168.0.0 0.0.255.255 0.0.0.0 0.0.0.0 eq 21
R2(config)#access-list 117 permit tcp 128.168.0.0 0.0.255.255 0.0.0.0 0.0.0.0 eq 80
R2(config)#
R2(config)#interface gigabitethernet 0/1
R2(config-if)#ip access-group 117 in
R2(config-if)#exit
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
```

KERBEROS

Farzad Kheirabadi
CYB 555
UNIT 7

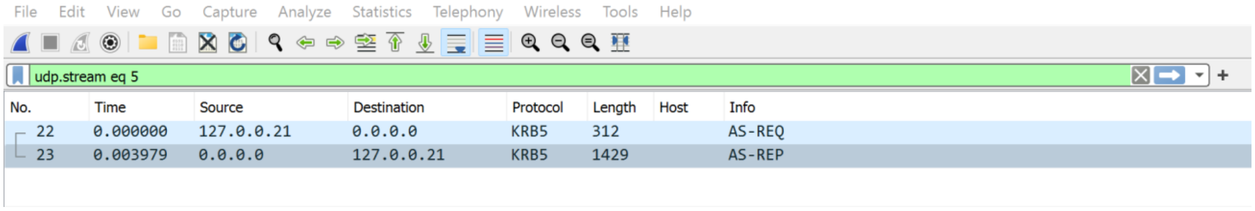

krb5.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
krb5.pcap
le: Default

Current filter: krb5rpc

```
No.  Time      Source      Destination      Protocol  Length  Host  Info
22   0.000035  127.0.0.21  0.0.0.0          KRB5      312           AS-REQ
23   0.003979  0.0.0.0     127.0.0.21       KRB5      1429          AS-REP
24   0.000009  127.0.0.21  127.0.0.21       KR
25   0.606703  127.0.0.21  127.255.255.255  NE                      OCALDC<00>
```

```
> Frame 23: 1429 bytes on wire (11432 bits), 1429 bytes
  Raw packet data
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 127.0
> User Datagram Protocol, Src Port: 88, Dst Port: 15216
> Kerberos
```

```
0000  45 00 05 95 ff ff 40 00  ff 11 00 00 00 00 00 00
0010  7f 00 00 15 00 58 3b 70  05 81 00 00 6b 82 05 75
0020  30 82 05 71 a0 03 02 01  05 a1 03 02 01 0b a2 48
0030  30 46 30 44 a1 03 02 01  13 a2 3d 04 3b 30 39 30
0040  37 a0 03 02 01 12 a1 30  1b 2e 53 41 4d 42 41 2e
0050  45 58 41 4d 50 4c 45 2e  43 4f 4d 68 6f 73 74 6c
0060  6f 63 61 6c 64 63 2e 73  61 6d 62 61 2e 65 78 61
0070  6d 70 6c 65 2e 63 6f 6d  a3 13 1b 11 53 41 4d 42
0080  41 2e 45 58 41 4d 50 4c  45 2e 43 4f 4d a4 15 30
0090  13 a0 03 02 01 00 a1 0c  30 0a 1b 08 4c 4f 43 41
```

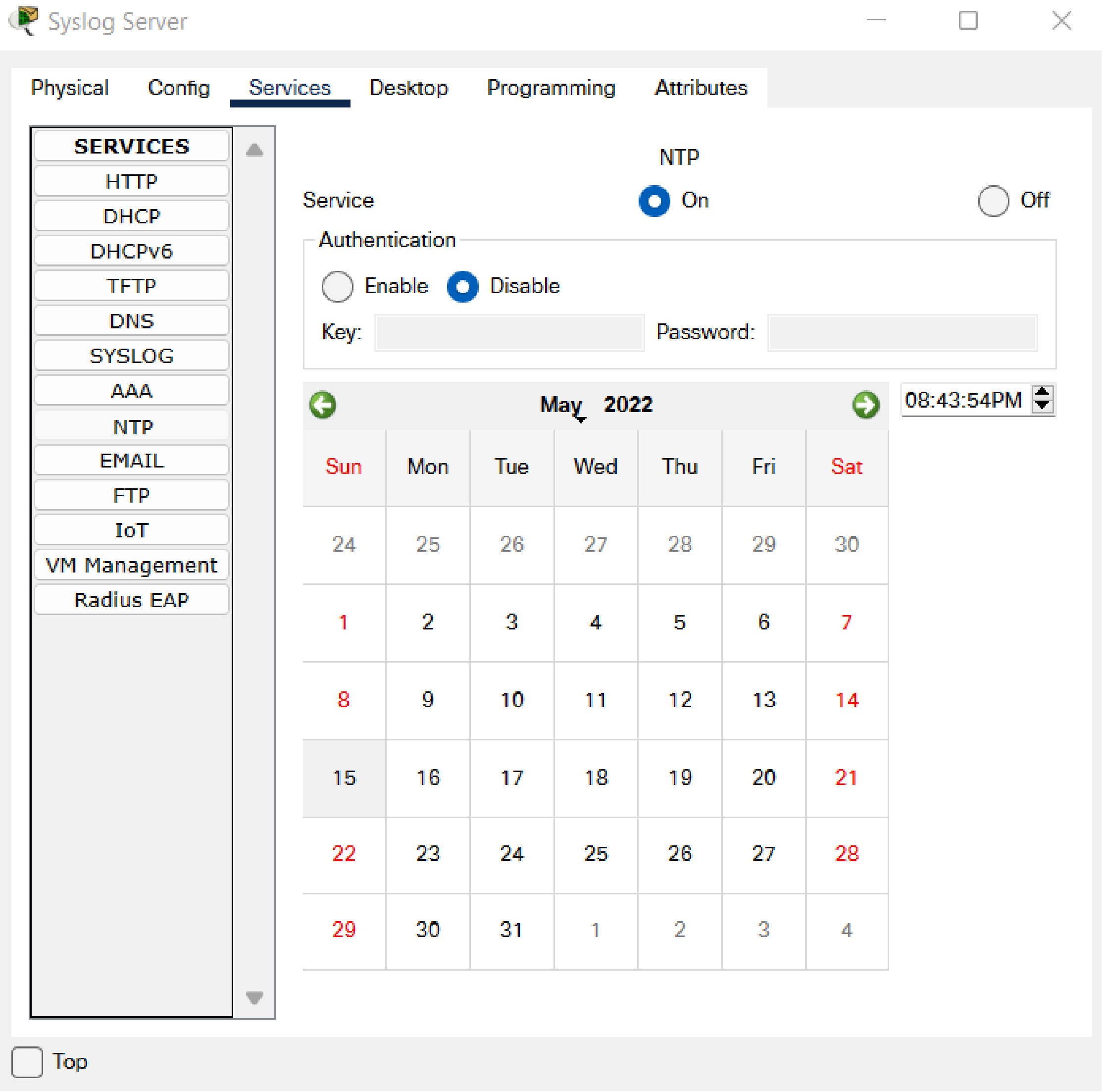

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 5

```
No.  Time      Source      Destination  Protocol  Length  Host  Info
22   0.000000  127.0.0.21  0.0.0.0      KRB5      312           AS-REQ
23   0.003979  0.0.0.0     127.0.0.21   KRB5      1429          AS-REP
```

SYSLOG and NTP

Farzad Kheirabadi
CYB 555
UNIT 7



NTP

Service ● On ○ Off

Authentication

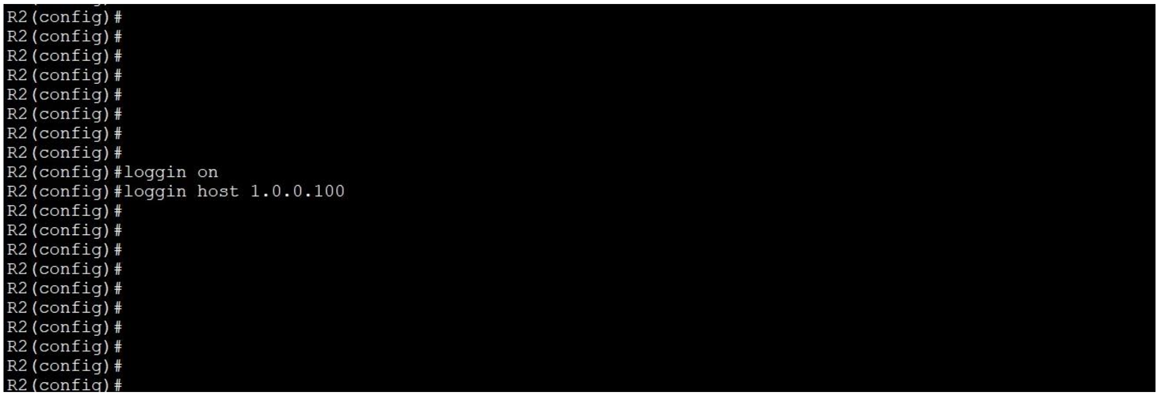
○ Enable ● Disable

Key: Password:

May 2022 08:43:54PM

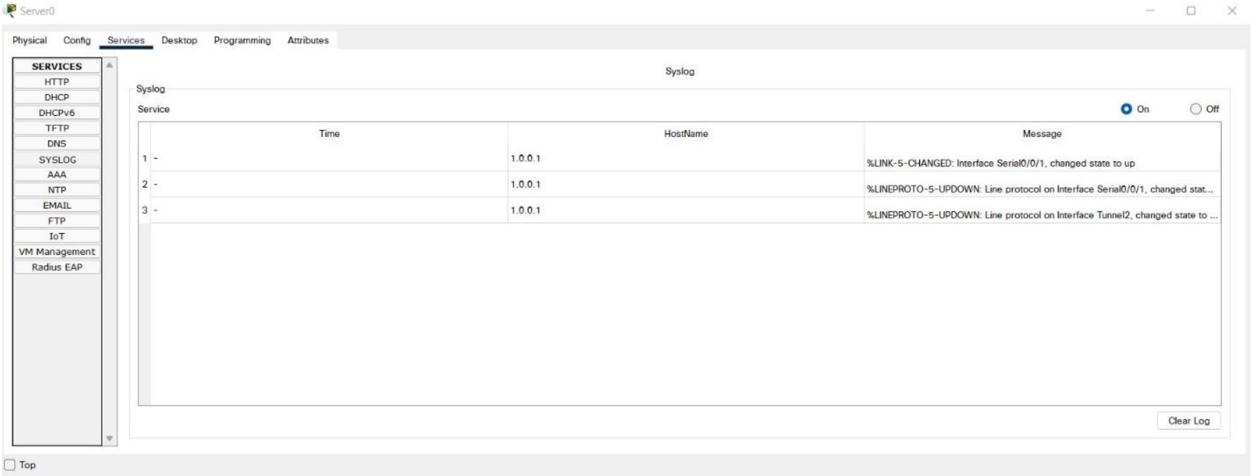
Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

☐ Top



```
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#loggin on
R2(config)#loggin host 1.0.0.100
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
```

Farzad Kheirabadi
CYB 555
UNIT 7



Syslog

Syslog

Service ● On ○ Off

	Time	HostName	Message
1	-	1.0.0.1	%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
2	-	1.0.0.1	%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed stat...
3	-	1.0.0.1	%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to ...