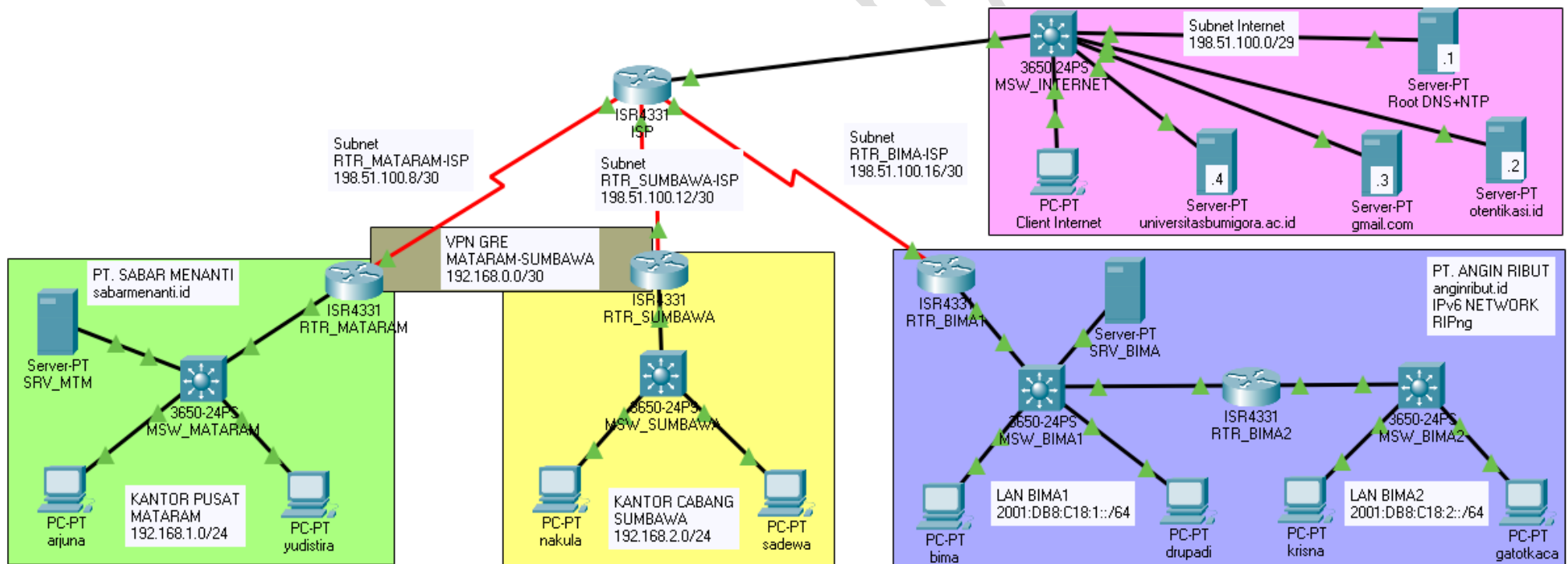


PEMBAHASAN SOLUSI SOAL UJIAN AKHIR SEMESTER (UAS)
PRAKTIKUM TROUBLESHOOTING & MAINTAINING COMPUTER NETWORK (TSHOOT)
SEMESTER GANJIL TAHUN AKADEMIK 2021/2022 UNIVERSITAS BUMIGORA

Oleh I Putu Hariyadi (putu.hariyadi@universitasbumigora.ac.id)

SOAL:

Lakukan **troubleshooting** terhadap 5 (lima) permasalahan yang terdapat pada topologi jaringan berikut:



1. Keseluruhan *host* pada **KANTOR PUSAT MATARAM PT. SABAR MENANTI** tidak dapat berkomunikasi ke **KANTOR CABANG SUMBAWA** dan sebaliknya. Namun koneksi Internet dari setiap **KANTOR** tersebut ke Internet berhasil dilakukan (Point: 20).
2. Keseluruhan *host* pada **KANTOR CABANG SUMBAWA** dari **PT. Sabar Menanti** tidak dapat mengakses layanan **HTTP** dan **HTTPS** serta **FTP** yang terdapat pada **Server SRV_MTM** yang terdapat di **KANTOR PUSAT MATARAM** menggunakan alamat **IP 192.168.1.1** (Point: 20).
3. *Router RTR_MATARAM, RTR_SUMBAWA* dan *RTR_BIMA* gagal melakukan sinkronisasi waktu dengan **server Network Time Protocol (NTP)** di **Internet** (Point: 20).
4. Network administrator tidak dapat melakukan **remote access via SSH** dari *hosts* pada **KANTOR PUSAT MATARAM** ke *Router RTR_MATARAM* menggunakan **TACACS+ Account** yaitu **username sabarX** dengan **password sabarX**. Ganti nilai **X** menjadi **1** sampai dengan **6**, sebagai contoh menggunakan **X** bernilai **1** sehingga **username** dan **password**-nya adalah **sabar1**. Sebagai informasi Network administrator telah mengatur skema otentikasi berbasis **TACACS+ menggunakan eksternal Authentication, Authorization & Accounting (AAA)** dari **provider otentikasi.id** di **Internet** untuk *Router RTR_MATARAM* (Point: 20).
5. Network administrator tidak dapat melakukan **remote access via SSH** dari *hosts* pada **LAN BIMA1** ke *Router RTR_BIMA* menggunakan **Radius Account username sabarX** dengan **password sabarX**. Akses **SSH** ke *router RTR_BIMA* dapat menggunakan alamat **IPv6 2001:db8:c18:1::1**. Ganti nilai **X** menjadi **1** sampai dengan **6**, sebagai contoh menggunakan **X** bernilai **1** sehingga **username** dan **password**-nya adalah **sabar1**. Sebagai informasi Network administrator telah mengatur skema otentikasi berbasis **Radius menggunakan eksternal Authentication, Authorization & Accounting (AAA)** dari **provider otentikasi.id** di **Internet** untuk *Router RTR_BIMA* (Point: 20).

Template file Cisco Packet Tracer dapat diunduh melalui [Google Drive](#).

Jelaskan penyebab dari setiap permasalahan tersebut dan *screenshot* solusi penyelesaian pada setiap perangkat yang memerlukan perbaikan. Selain itu lampirkan *screenshot* verifikasi keberhasilan pengaksesan dari perangkat terkait setelah diperbaiki.

Username dan **Password local user account** yang terdapat pada setiap database dari *router* dan *multilayer switch* sehingga menjembatani akses ke perangkat tersebut adalah:

- **Console** dan **SSH** menggunakan **username: netadmin** dan **password: netadmin**
- **Privilege mode: menanti**

Apabila terkendala ketika mengakses **CLI** dari perangkat maka pilih tab **Config** dan tekan tombol **Save**. Setelah itu pilih kembali tab **CLI** sehingga akan dibawa ke prompt **privilege mode**.

SOLUSI:

1. a. Penyebab Permasalahan

Kesalahan konfigurasi di **router RTR_MATARAM** meliputi argumen dari perintah **Tunnel Destination GRE** pada **interface tunnel 0** dan argumen perintah **network** pada **routing protocol OSPF**.

```
RTR_MATARAM#show run | section interface Tunnel0
interface Tunnel0
  ip address 192.168.0.1 255.255.255.252
  mtu 1476
  tunnel source Serial0/1/0
  tunnel destination 198.51.100.14
RTR_MATARAM#show run | section router ospf
router ospf 1
  log-adjacency-changes
  network 192.168.1.254 0.0.0.0 area 0
  network 192.168.0.0 0.0.0.0 area 0
```

b. Solusi Penyelesaian

Mengubah argumen dari perintah **tunnel destination** pada **RTR_MATARAM** dari **198.51.100.14** ke **198.51.100.13**.

```

RTR_MATARAM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RTR_MATARAM(config)#int tunnel0
RTR_MATARAM(config-if)#tunnel destination 198.51.100.13
RTR_MATARAM(config-if)#do show run | section interface Tunnel0
interface Tunnel0
  ip address 192.168.0.1 255.255.255.252
  mtu 1476
  tunnel source Serial0/1/0
  tunnel destination 198.51.100.13

```

Mengubah argumen dari perintah **network** pada **routing ospf** dari **192.168.0.0 0.0.0.0 area 0** menjadi **192.168.0.1 0.0.0.0 area 0**.

```

RTR_MATARAM(config-if)#exit
RTR_MATARAM(config)#router ospf 1
RTR_MATARAM(config-router)#no network 192.168.0.0 0.0.0.0 area 0
RTR_MATARAM(config-router)#network 192.168.0.1 0.0.0.0 area 0
RTR_MATARAM(config-router)#do show run | section router ospf
router ospf 1
  log-adjacency-changes
  network 192.168.1.254 0.0.0.0 area 0
  network 192.168.0.1 0.0.0.0 area 0

```

c. Verifikasi

Memverifikasi koneksi menggunakan Simple PDU dari PC arjuna di LAN Kantor Pusat Mataram dari PT. Sabar Menanti ke seluruh hosts di LAN Kantor Cabang Sumbawa.

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	arjuna	nakula	ICMP		0.000	N	0	(edit)	
	Successful	arjuna	sadewa	ICMP		0.000	N	1	(edit)	

Terlihat koneksi berhasil dilakukan.

2. a. Penyebab Permasalahan

Service HTTP dan HTTPS pada Server SRV_MTM yang terdapat di LAN Kantor Pusat Mataram dari PT. Sabar Menanti belum aktif.

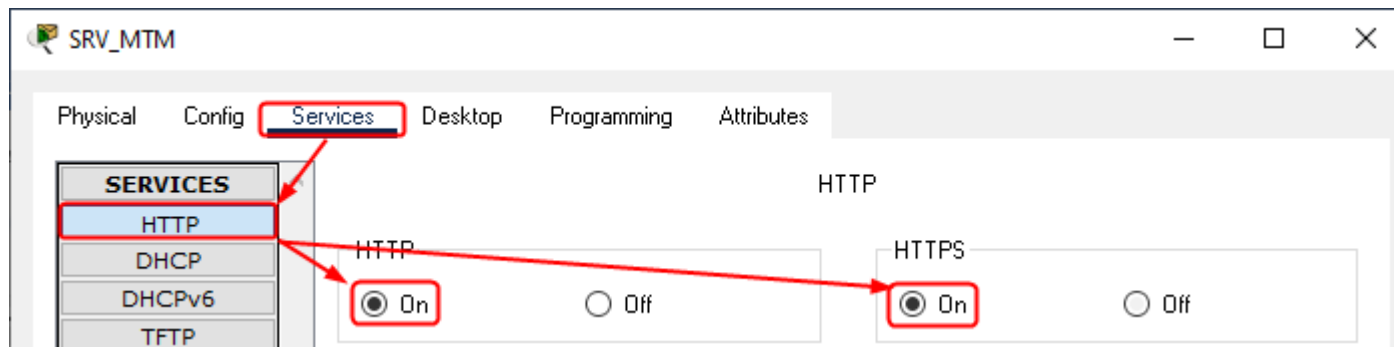


Selain itu kesalahan konfigurasi ACL pada router RTR_MATARAM yang hanya mengijinkan trafik ICMP dari LAN MATARAM ke LAN SUMBAWA.

```
RTR_MATARAM#show access-list
Standard IP access list 1
 10 permit 192.168.1.0 0.0.0.255 (2 match(es))
Extended IP access list 101
 10 permit icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
 20 permit gre host 198.51.100.9 host 198.51.100.13
```

b. Solusi Penyelesaian

Mengaktifkan service HTTP dan HTTPS pada Server SRV_MTM.



Mengatur ulang Numbered ACL 101 dengan agar mengijinkan trafik terkait protocol ip dari dari **LAN MATARAM** ke **LAN SUMBAWA**.

RTR_MATARAM#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RTR_MATARAM(config)#no access-list 101

RTR_MATARAM(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

RTR_MATARAM(config)#access-list 101 permit gre host 198.51.100.9 host 198.51.100.13

RTR_MATARAM(config)#do show access-list

Standard IP access list 1

10 permit 192.168.1.0 0.0.0.255 (2 match(es))

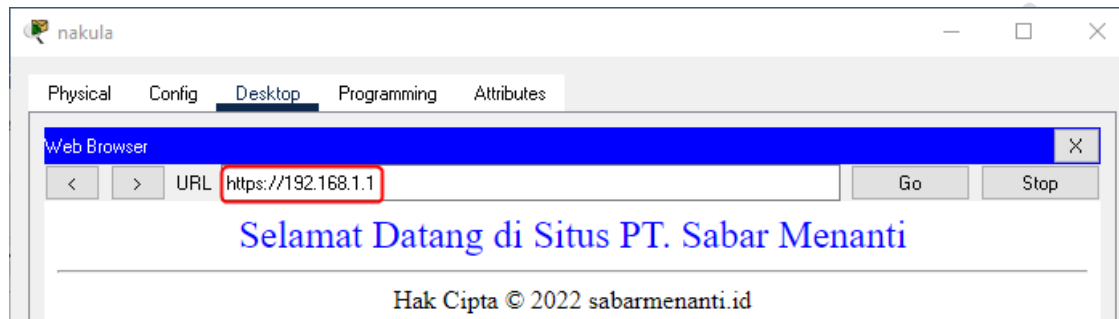
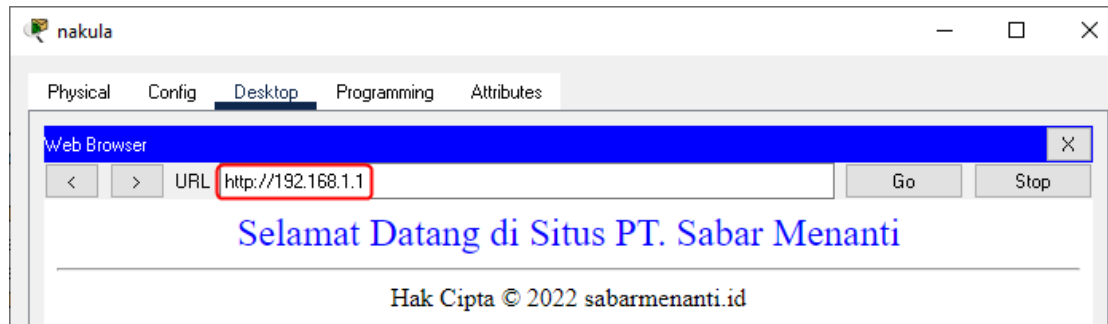
Extended IP access list 101

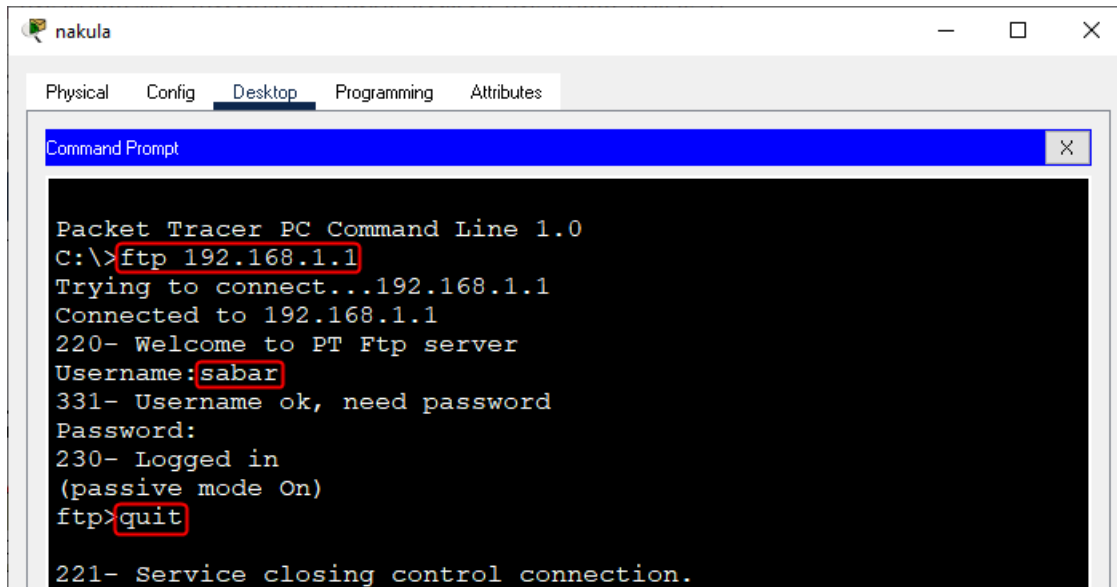
10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

20 permit gre host 198.51.100.9 host 198.51.100.13 (1 match(es))

c. Verifikasi

Mengakses layanan **HTTP** dan **HTTPS** serta **FTP** dari **PC nakula** yang terdapat di LAN SUMBAWA ke Server SRV_MTM.





```

Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.1
Trying to connect...192.168.1.1
Connected to 192.168.1.1
220- Welcome to PT Ftp server
Username:sabar
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit
221- Service closing control connection.

```

Terlihat akses HTTP dan HTTPS serta FTP berhasil dilakukan.

3. a. Penyebab Permasalahan

Kesalahan konfigurasi alamat IP dari Server NTP pada router RTR_MATARAM.

```

RTR_MATARAM#show run | include ntp
ntp authentication-key 46 md5 082C49400817111E 7
ntp trusted-key 46
ntp server 198.51.100.111 key 46

```

Kesalahan konfigurasi sandi untuk otentikasi ke Server NTP pada router RTR_SUMBAWA.

```

RTR_SUMBAWA#show run | include ntp
ntp authentication-key 46 md5 082C494008171146 7
ntp trusted-key 46
ntp server 198.51.100.1 key 46

```

Kesalahan konfigurasi pada router RTR_BIMA1 yang belum menerapkan otentikasi NTP.

```

RTR_BIMA1#show run | include ntp
ntp server 198.51.100.1

```

b. Solusi Penyelesaian

Mengubah alamat IP dari Server NTP pada argumen dari perintah **ntp server** di router **RTR_MATARAM**.

```
RTR_MATARAM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RTR_MATARAM(config)#ntp server 198.51.100.1 key 46
RTR_MATARAM(config)#end
RTR_MATARAM#
%SYS-5-CONFIG_I: Configured from console by console

RTR_MATARAM#show run | include ntp
ntp authentication-key 46 md5 082C49400817111E 7
ntp trusted-key 46
ntp server 198.51.100.1 key 46
```

Mengubah sandi untuk otentikasi ke Server NTP pada argumen perintah **ntp authentication-key** di router **RTR_SUMBAWA**.

```
RTR_SUMBAWA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RTR_SUMBAWA(config)#ntp authentication-key 46 md5 menanti
RTR_SUMBAWA(config)#end
RTR_SUMBAWA#
%SYS-5-CONFIG_I: Configured from console by console

RTR_SUMBAWA#show run | include ntp
ntp authentication-key 46 md5 082C49400817111E 7
ntp trusted-key 46
ntp server 198.51.100.1 key 46
```

Menambahkan pengaturan otentikasi **NTP** pada router **RTR_BIMA1**.

```
RTR_BIMA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RTR_BIMA1(config)#ntp server 198.51.100.1 key 46
RTR_BIMA1(config)#ntp authentication-key 46 md5 menanti
RTR_BIMA1(config)#ntp trusted-key 46
RTR_BIMA1(config)#end
RTR_BIMA1#
%SYS-5-CONFIG_I: Configured from console by console

RTR_BIMA1#show run | include ntp
ntp authentication-key 46 md5 082C49400817111E 7
ntp trusted-key 46
ntp server 198.51.100.1 key 46
```

c. Verifikasi

Hasil verifikasi waktu dan tanggal di **router RTR_MATARAM**.

```
RTR_MATARAM#show clock
*21:49:57.139 UTC Wed Jan 12 2022
```

Hasil verifikasi waktu dan tanggal di **router RTR_SUMBAWA**.

```
RTR_SUMBAWA#show clock
20:36:53.523 UTC Wed Jan 12 2022
```

Hasil verifikasi waktu dan tanggal di **router RTR_BIMA1**.

```
RTR_BIMA1#show clock
20:36:48.761 UTC Wed Jan 12 2022
```

Terlihat ketiga router telah berhasil melakukan sinkronisasi waktu dengan Server NTP.

4. a. Penyebab Permasalahan

Alamat IP dari **TACACS Server** yang dirujuk pada **router RTR_MATARAM** kurang tepat yaitu **198.51.100.1** seharusnya **198.51.100.2**. Begitu pula key yang digunakan kurang tepat yaitu **menanti** seharusnya **menanti**.

```
RTR_MATARAM#show run | include tacacs-server  
tacacs-server host 198.51.100.2 key menanti
```

b. Solusi Penyelesaian

Mengatur ulang konfigurasi **tacacs-server** pada **router RTR_MATARAM**.

```
RTR_MATARAM#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
RTR_MATARAM(config)#no tacacs-server host 198.51.100.2 key menanti  
RTR_MATARAM(config)#tacacs-server host 198.51.100.2 key menanti  
RTR_MATARAM(config)#end  
RTR_MATARAM#  
%SYS-5-CONFIG_I: Configured from console by console  
  
RTR_MATARAM#show run | include tacacs-server  
tacacs-server host 198.51.100.2 key menanti
```

c. Verifikasi

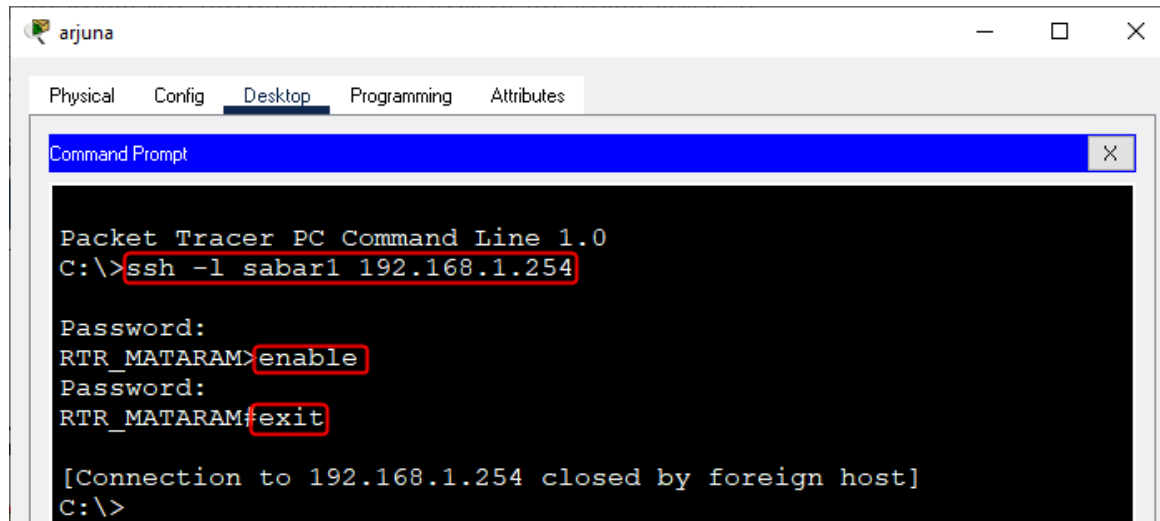
Hasil ujicoba login melalui **console** dari **router RTR_MATARAM** menggunakan akun TACACS berupa username **sabar1** dengan password **sabar1** dan berpindah ke mode **privilege** menggunakan password **menanti**.

User Access Verification

```
Username: sabar1  
Password:  
RTR_MATARAM>enable  
Password:  
RTR_MATARAM#
```

Terlihat otentikasi berhasil dilakukan.

Hasil ujicoba akses **SSH** ke **router RTR_MATARAM** melalui **Command Prompt** dari **PC arjuna**.



```

Packet Tracer PC Command Line 1.0
C:\>ssh -l sabar1 192.168.1.254

Password:
RTR_MATARAM>enable
Password:
RTR_MATARAM#exit

[Connection to 192.168.1.254 closed by foreign host]
C:\>

```

Terlihat akses SSH berhasil dilakukan.

5. a. Penyebab Permasalahan

Kesalahan konfigurasi **radius-server** di **router RTR_BIMA1** yang masih menggunakan default port yaitu 1645. Sedangkan di Server Radius menggunakan nomor port 1654.

```

RTR_BIMA1#show run | include radius-server
radius-server host 198.51.100.2 auth-port 1645 key menanti

```

b. Solusi Penyelesaian

Mengubah nilai dari parameter **authentication-port** dari perintah **radius-server** agar menggunakan nomor port RADIUS **1654**.

```
RTR_BIMA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RTR_BIMA1(config)#no radius-server host 198.51.100.2 auth-port 1645 key menanti
RTR_BIMA1(config)#radius-server host 198.51.100.2 auth-port 1654 key menanti
RTR_BIMA1(config)#end
RTR_BIMA1#
%SYS-5-CONFIG_I: Configured from console by console

RTR_BIMA1#show run | include radius-server
radius-server host 198.51.100.2 auth-port 1654 key menanti
```

c. Verifikasi

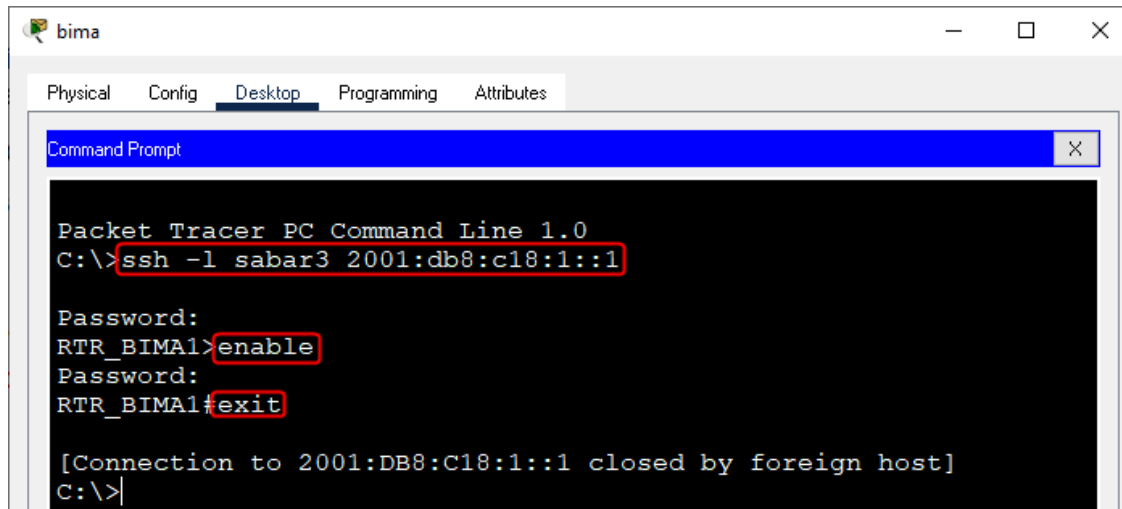
Hasil ujicoba login melalui **console** dari **router RTR_BIMA1** menggunakan akun **RADIUS** berupa username **sabar3** dengan password **sabar3** dan berpindah ke mode **privilege** menggunakan password **menanti**.

User Access Verification

```
Username: sabar3
Password:
RTR_BIMA1>enable
Password:
RTR_BIMA1#
```

Terlihat otentikasi berhasil dilakukan.

Hasil ujicoba akses **SSH** ke **router RTR_BIMA1** melalui **Command Prompt** dari **PC bima**.



The screenshot shows a Packet Tracer PC Command Line window titled 'bima'. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the following text: 'Packet Tracer PC Command Line 1.0', 'C:\>ssh -l sabar3 2001:db8:c18:1::1', 'Password:', 'RTR_BIMAl>enable', 'Password:', 'RTR_BIMAl#exit', '[Connection to 2001:DB8:C18:1::1 closed by foreign host]', and 'C:\>'. The commands 'ssh -l sabar3 2001:db8:c18:1::1', 'enable', and 'exit' are highlighted with red boxes.

Terlihat akses SSH berhasil dilakukan.

Selamat Menguji coba. Semoga Sukses.