TECHNICAL REPORT

PRAKTIKUM JARINGAN KOMPUTER

MODUL 12

Disusun Oleh :

TGL. PRAKTIKUM	:	Kamis, 04 Juni 2021
NAMA	:	Achmad Farid Alfa Waid
NIM	:	190411100073
KELOMPOK	:	1
DOSEN	:	Yoga Dwitya Pramudita, S.Kom
ASPRAK	:	Rizal Abul Fata

LABORATORIUM COMMON COMPUTING

JURUSAN TEKNIK INFORMATIKA

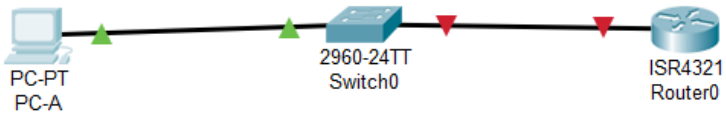
FAKULTAS TEKNIK

UNIVERSITAS TRUNOJOYO MADURA

2020

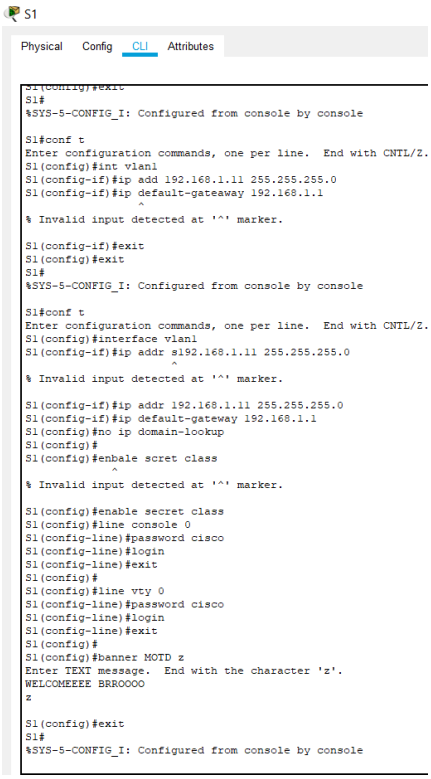
I. Latihan 1: Mengkonfigurasi Perangkat Dasar

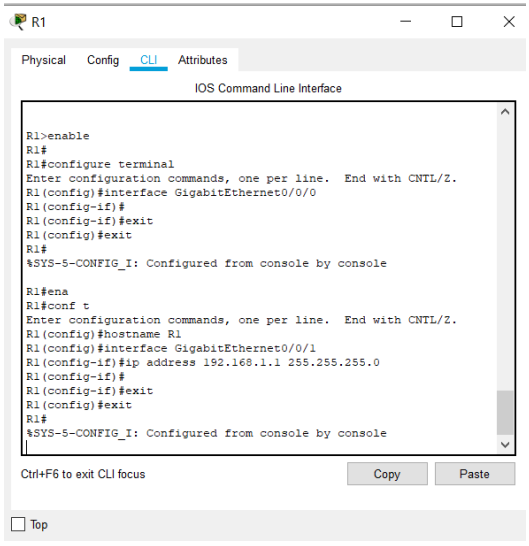
1. Langkah 1: Kabelkan jaringan mengikuti gambaran topologi

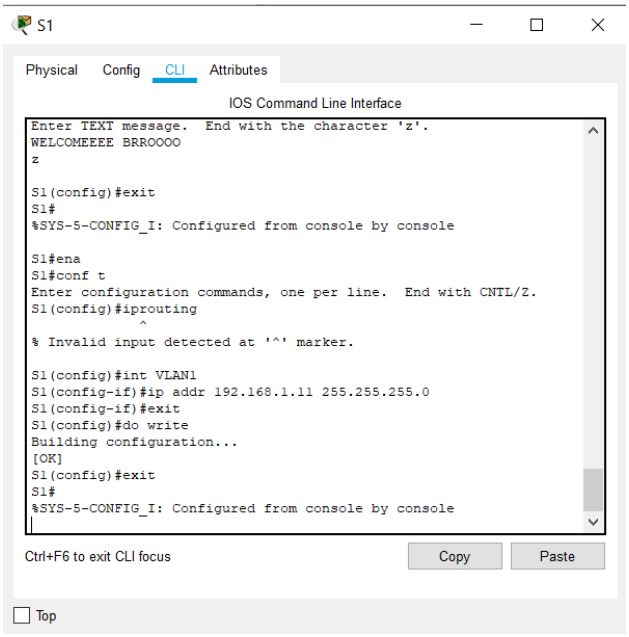


2. Langkah 2: Inisialisasi dan muat-ulang router dan switch

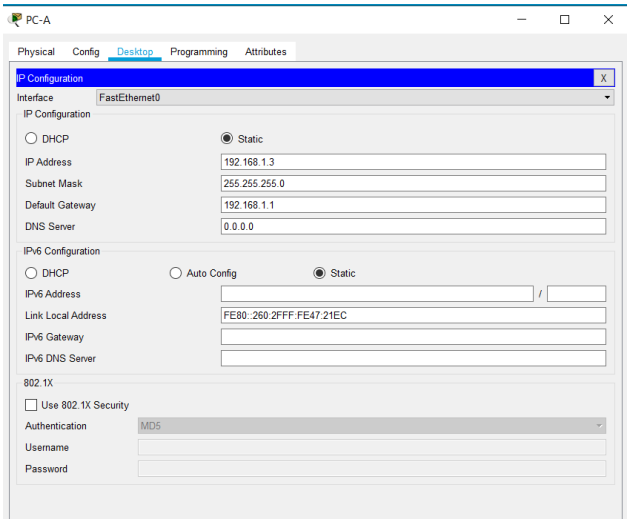
3. Langkah 3: Konfigurasikan router dan switch



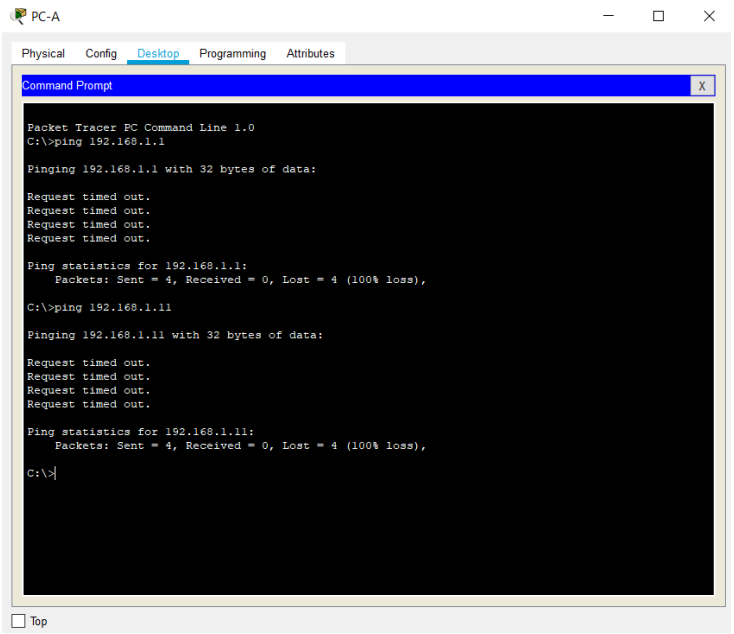




4. Konfigurasi PC-A

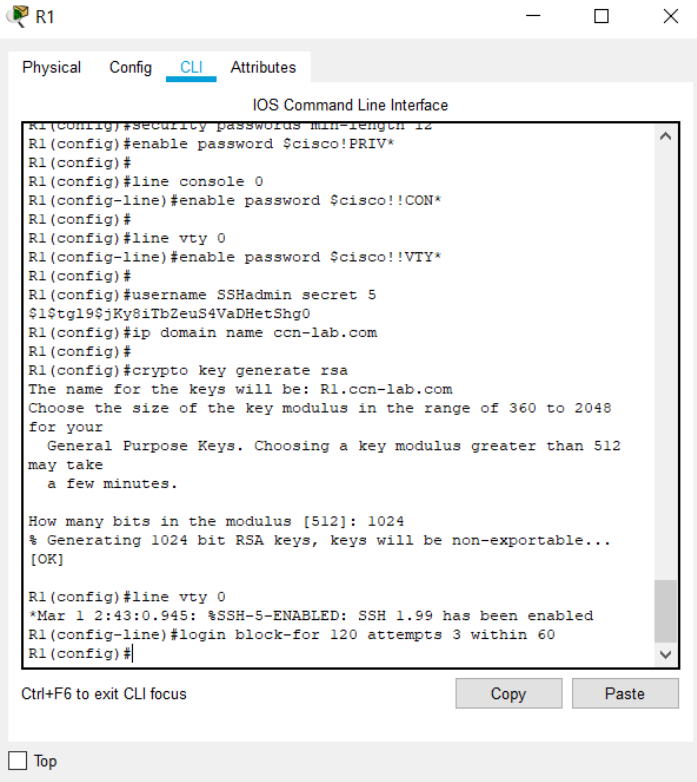


5. Pastikan konektivitas jaringan



II. Latihan 2: Mengkonfigurasi Ukuran Keamanan Dasar Pada Router

1. Langkah 1: Konfigurasikan ukuran keamanan

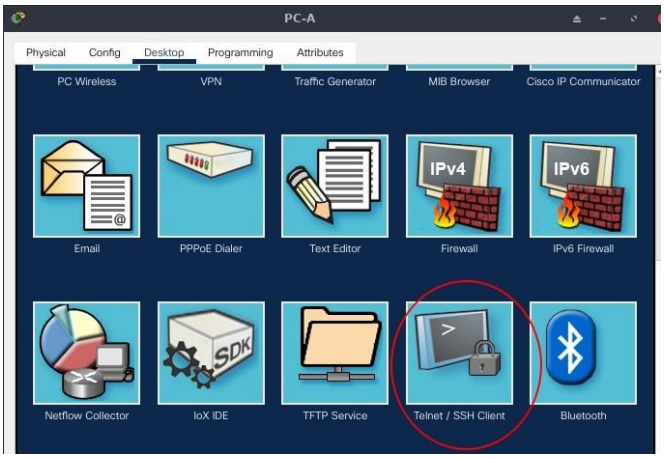


2. Langkah 2: Pastikan semua port yang tidak digunakan dimatikan

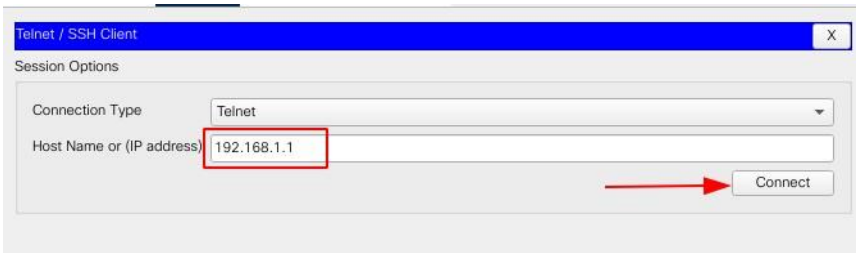
```
R1>ena
Password:
R1#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.1.1     YES manual administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface GigabitEthernet0/0/0
R1(config-if)#no ip addr
R1(config-if)#shutdown
R1(config-if)#negotiation auto
                 ^
% Invalid input detected at '^' marker.

R1(config-if)#!negotiation auto
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

3. Langkah 3: Pastikan ukuran keamanan telah diimplementasi dengan benar



Gunakan Tera Term pada PC-A untuk melakukan telnet ke R1.



Telnet ke R1

Pertanyaan:

Apakah R1 menerima koneksi Telnet? Jelaskan.

Jawab :

Tidak, koneksi ditolak karena Telnet dinonaktifkan dengan perintah ssh input transport.

2. Gunakan Tera Term pada PC-A untuk melakukan SSH ke R1.

   Pertanyaan:

   Apakah R1 menerima koneksi SSH?

   Jawab :

   Ya

3. Cobalah berikan informasi user dan password yang sengaja salah untuk melihatapakah akses login diblok setelah dua percobaan.

   Pertanyaan:

   Apa yang terjadi setelah anda gagal login kali kedua?

   Jawab :

   Sambungan ke R1 terputus. Jika tetap mencoba menyambung kembali dalam waktu 30 detik, sambungan akan ditolak.

4. Dari sesi console anda pada router, jalankan perintah show login untukmenampilkan status login. Dalam contoh berikut, perintah show login telah dijalankan di dalam 120 detik periode login blocking dan menampilkan bahwa router berada dalam Quiet-Mode. Router tidak akan menerima percobaan login selama 111 detik lagi.

```
R1>ena
Password:
R1#show login
    A default login delay of 1 seconds is applied.
    No Quiet-Mode access list has been configured.
    All successful login is logged.

    Router enabled to watch for login Attacks.
    If more than 3 login failures occur in 60 seconds or less,
    logins will be disabled for 120 seconds.

    Router presently in Normal-Mode.
    Current Watch Window
        Time remaining: 0 seconds.
        Login failures for current window: 0.
    Total login failures: 0.

R1#
```

5. Setelah 120 detik kadaluarsa, SSH ke R1 lagi dan login menggunakan usernameSSHadmin dan password 55HAdm!n2020.

   Pertanyaan:

   Setelah anda berhasil login, apa yang ditampilkan?

   Jawab :

   Banner MOTD R1

6. Masuklah ke modus privileged EXEC dan gunakan $cisco!PRIV* sebagai passwordnya.

   Pertanyaan:

   Jika anda salah ketik password ini, apakah anda didiskoneksi dai sesi SSH anda setelah tiga usaha gagal dalam rentang 60 detik? Jelaskan.

   Jawab :

   Tidak, Blok login-untuk 120 (2 menit) detik upaya 3x dalam 60detik (1 menit) perintah hanya memantau upaya login sesi pada jalur VTY.

7. Jalankan perintah show running-config pada prompt privileged EXEC untuk menampilkan setingan keamanan yang telah diterapkan

```
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

III. Latihan 3: Mengkonfigurasi Ukuran Keamanan Dasar Pada Switch

1. Langkah 1: Kondigurasi ukuran keamanan

```
User Access Verification

Password:

Switch>ena
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password $cisco!PRIV*
Switch(config)#
Switch(config)#line console 0
Switch(config-line)#enable password $cisco!!CON*
Switch(config)#
Switch(config)#line vty 0
Switch(config-line)#enable password $cisco!!VTY*
Switch(config)#
Switch(config)#username SSHadmin secret 5 $1$2ens$10nrX3Vj14Ofk.oMKtTrQ1
Switch(config)#ip domain-name ccna-lab.com
```

2. Langkah 2: Pastikan semua port yang tidak digunakan didisable

```
Switch#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.11    YES manual administratively down down
```

Melakukan shutdown pada interface yang tidak aktif

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
Switch(config-if)#interface FastEthernet0/2
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
Switch(config-if)#interface FastEthernet0/3
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
Switch(config-if)#interface FastEthernet0/4
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
Switch(config-if)#interface FastEthernet0/7
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
Switch(config-if)#interface FastEthernet0/8
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
Switch(config-if)#interface FastEthernet0/9
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
Switch(config-if)#interface FastEthernet0/10
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
```

3. **Langkah 3: Pastikan ukuran keamanan telah diimplementasikan dengan benar**

1. Pastikan bahwa Telnet telah didisable pada switch.

2. SSH ke switch dan sengajalah salah ketik informasi user dan password untukmelihat apakah akses login diblokir.

3. Setelah 30 detik kadaluarsa, SSH ke S1 lagi dan log in menggunakan usernameSSHadmin dan password 55HAdm!n2020.

   Pertanyaan:
   Banner apakah yang tampil setelah anda berhasil login?
   Jawab :
   Iya

4. Masuklah ke modus privileged EXEC menggunakan password $cisco!PRIV*.User Access Verification

   Password: Switch>ena
   Password:
   Switch#

5. Jalankan perintah show running-config pada prompt privileged EXEC untukmenampilkan setingan keamanan yang telah diterapkan

Pertanyaan:

1. Perintah **password cisco** telah disematkan untuk console dan VTY lines saat konfigurasi dasar dalam Latihan 1. Kapankah password ini digunakan setelah ukuran keamanan best practice diterapkan?

   Jawab:

   Kata sandi ini tidak digunakan lagi, karena sudah dinonaktifkan setelah perintah login lokal dimasukkan untuk baris tersebut.

2. Apakah password preconfigured yang lebih pendek dari 10 karakter terpengaruh oleh perintah security passwords min-length 12?

   Jawab:

   Tidak. Perintah keamanan kata sandi min-length hanya berlaku pada kata sandi yang dimasukkan setelah perintah ini dikeluarkan. Untuk kata sandi sebelumnya masih bisa digunakan dan aktif. Namun jika dilakukan perubahan kata sandi, panjangnya minimal harus 12 karakter.