VERSION 2.1

23 NOVEMBER, 2021

[PRAKTIKUM KOMUNIKASI DATA]

MODUL 6 TUGAS– BUILDING AND SECURING A SMALL NETWORK

DISUSUN OLEH :

SALSABILA AULIA RAMADHAN
WAHYU BUDI UTOMO

DIAUDIT OLEH : MAHAR FAIQURAHMAN, S.KOM., M.T.
FAUZI DWI SETIAWAN SUMADI, S.T., M.CompSc.

PRESENTED BY: TIM LAB-IT

UNIVERSITAS MUHAMMADIYAH MALANG

[PRAKTIKUM KOMUNIKASI DATA]

PERSIAPAN MATERI

Praktikan diharapkan mempelajari Group Exam Modules 16 - 17 : Building And Securing A Small Network Exam yangterdiri dari beberapa chapter berikut :

1. Network Security Fundamentals (Chapter 16)
2. Build a Small Network (Chapter 17)

TUJUAN PRAKTIKUM

1. Bagian 1: Mengkonfigurasikan Pengaturan Perangkat Dasar
2. Bagian 2: Mengkonfigurasikan Router untuk Akses SSH
3. Bagian 3: Mengkonfigurasikan Switch untuk Akses SSH
4. Bagian 4: SSH dari CLI di Switch

PERSIAPAN SOFTWARE/APLIKASI

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell(SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands. However, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs.Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

MATERI POKOK

Part 1: Mengkonfigurasikan Pengaturan Perangkat Dasar

1. Kabel jaringan seperti yang ditunjukkan pada topologi

2. Inisialisasi dan memuat ulang router dan switch

3. Mengkonfigurasikan router

    a. Lakukan koneksi console ke router dan aktifkan privileged EXEC mode
    b. Masuk ke mode konfigurasi
    c. Menon-aktifkan pencarian DNS untuk mencegah router mencoba menerjemahkan perintah yang dimasukkan secara salah seolah – olah itu adalah nama host
    d. Menetapkan **class** sebagai kata sandi terenkripsi privileged EXEC
    e. Menetapkan **cisco** sebagai kata sandi console dan aktifkan login
    f. Menetapkan **cisco** sebagai kata sandi VTY dan aktifkan login
    g. Enkripsi kata sandi plaintext
    h. Membuat pemberitahuan untuk memperingatkan siapa pun yang mengakses perangkat bahwa akses tidak sah dilarang
    i. Mengkonfigurasikan dan mengaktifkan interface G0/0/1 pada router menggunakan informasi yang terdapat pada Tabel Pengalamatan
    j. Simpan hasil konfigurasi yang sedang berjalan ke file konfigurasi startup

4. Mengkonfigurasikan PC-A
    a. Mengkonfigurasikan PC-A dengan alamat IP dan subnet mask
    b. Mengkonfigurasikan gateway default untuk PC-A

5. Verifikasi konektivitas jaringan

Ping R1 dari PC-A. Jika ping gagal, pecahkan masalah koneksi

Part 2: Mengkonfigurasikan Router untuk Akses SSH

1. Mengkonfigurasikan otentikasi perangkat
   a. Mengkonfigurasikan nama perangkat
   b. Mengkonfigurasikan domain untuk perangkat

2. Mengkonfigurasikan metode kunci enkripsi

3. Mengkonfigurasikan nama pengguna basis data lokal

   Note : Konfigurasikan nama pengguna menggunakan **admin** sebagai nama pengguna dan **Adm1nP@55** sebagai kata sandi

4. Aktifkan SSH pada baris VTY
   a. Aktifkan Telnet dan SSH pada jalur VTY masuk menggunakan perintah **input transport**
   b. Ubah metode login untuk menggunakan database lokal untuk verifikasi pengguna

5. Menyimpan konfigurasi yang sedang berjalan ke file konfigurasi startup
6. Membuat koneksi SSH ke router
   a. Mulailah Tera Term dari PC-A
   b. Menetapkan sesi SSH ke R1. Gunakan username **admin** dan password **Adm1Np@55.** Diharapkan dapat membuat sesi SSH dengan R1

Part 3: Mengkonfigurasikan Switch untuk Akses SSH

1. Mengkonfigurasikan pengaturan dasar pada switch
a. Lakukan koneksi console ke switch dan aktifkan mode privileged EXEC
b. Masuk ke mode konfigurasi
c. Menonaktifkan pencarian DNS untuk mencegah router mencoba menerjemahkan perintah yang dimasukkan secara salah seolah-olah itu adalah nama host
d. Menetapkan **class** sebagai kata sandi terenkripsi privileged EXEC
e. Menetapkan **cisco** sebagai kata sandi konsol dan mengaktifkan login
f. Menetapkan **cisco** sebagai kata sandi VTY dan aktifkan login
g. Enkripsi kata sandi teks biasa
h. Buat banner yang akan memperingatkan siapa pun yang mengakses perangkat bahwa akses tidak sah dilarang
i. Mengkonfigurasikan dan mengaktifkan antarmuka VLAN 1 pada switch sesuai dengan Tabel Pengalamatan
j. Menyimpan konfigurasi yang sedang berjalan ke file konfigurasi startup

2. Mengkonfigurasikan switch untuk konektivitas SSH
a. Mengkonfigurasikan nama perangkat seperti yang tercantum dalam Tabel Pengalamatan
b. Mengkonfigurasikan domain untuk perangkat
c. Mengkonfigurasikan metode kunci enkripsi
d. Mengkonfigurasikan nama pengguna basis data lokal
e. Mengaktifkan Telnet dan SSH di jalur VTY
f. Mengubah metode login untuk menggunakan database lokal untuk verifikasi pengguna

3. Membuat suatu koneksi SSH ke sakelar

Part 4: SSH From the CLI on the Switch

1. Lihatlah parameter yang tersedia untuk klien Cisco IOS SSH
   Gunakan tanda Tanya (?) untuk menampilkan opsi parameter yang tersedia dengan perintah SSH

```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

2. SSH ke R1 dari S1
   a. Diharuskan menggunakan opsi -**–l admin** saat melakukan SSH ke R1. Sehingga memungkinkan untuk masuk sebagai **admin** pengguna. Saat diminta, masukkan **Adm1Np@55** untuk kata sandi.

```
S1# ssh -l admin 192.168.1.1
Password:
Authorized Users Only!
R1>
```

   b. Kembali ke S1 tanpa menutup sesi SSH ke R1 dengan menekan **Ctrl + Shift + 6**. Lepaskan tombol **Ctrl + Shift + 6** dan tekan **x.** Tampilan prompt privileged EXEC switch

```
R1>
S1#
```

   c. Untuk kembali ke sesi SSH di R1, tekan Enter pada baris CLI kosong. Tekan Enter untuk kedua kalinya untuk melihat prompt CLI router

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]


R1>
```

   d. Untuk mengakhiri sesi SSH pada R1, ketik **exit** pada prompt router

```
R1# exit


[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

PERTANYAAN TUGAS

1. Apakah anda dapat mengkonfigurasikan SSH pada switch?
2. Jelaskan mengenai kegiatan konfigurasi SSH pada soal no 1!

CATATAN

Tugas :

Batas maksimal dikerjakan H-1 praktikum dan dikumpulkan di i-Lab dengan format [Nama_Nim_Modul6] .rar

Praktek :

Didemokan kepada asisten masing – masing pada hari H

praktikum Netacad :

Batas maksimal pengerjaan netacad adalah 1 minggu setelah jadwal praktikum

KRITERIA PENILAIAN TUGAS

>81 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas dengan benar 70 – 40 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas namun kurang maksimal.

KRITERIA PENILAIAN PRAKTEK

>81 : Praktikan mampu memahami, menjawab dan menjelaskan materi praktek kepada asisten. 70 – 80 : Praktikan mampu memahami, menjawab dan menjelaskan materi praktek kepada asisten namun kurang maksimal.

55 – 69 : Praktikan mampu menjawab soal yang ada di materi praktek kepada asisten namun tidak bisa menjelaskan proses yang terjadi.

<55 : Praktikan tidak memahami, menjawab dan menjelaskan materi praktek kepada asisten.

DETAIL PENILAIAN PRAKTIKUM

TUGAS	20%
PRAKTEK	80%