

VERSI 1.0

Agustus 2025



KOMUNIKASI DATA

MODUL 3 - IDENTIFY MAC AND IP ADDRESSES

DISUSUN OLEH:

Luqman Hakim, S.Kom., M.Kom.

Moh. Khairul Umam

Fatahillah Al-Fatih

**TIM LABORATORIUM INFORMATIKA
UNIVERSITAS MUHAMMADIYAH MALANG**

PENDAHULUAN

TUJUAN

1. Membedakan fungsi dan karakteristik antara alamat MAC (Layer 2) dengan alamat IP (Layer 3) dalam komunikasi jaringan.
2. Mengidentifikasi alamat MAC, alamat IP, *subnet mask*, dan *default gateway* pada berbagai sistem operasi seperti Windows, macOS, Linux, dan perangkat mobile.
3. Memahami mekanisme kerja *Address Resolution Protocol* (ARP) dalam memetakan alamat IP ke alamat MAC di jaringan lokal.
4. Menganalisis proses enkapsulasi dan informasi PDU (*Protocol Data Unit*) pada komunikasi jaringan lokal dan *remote* menggunakan mode simulasi di Cisco Packet Tracer.

TARGET MODUL

1. Menjelaskan secara konseptual perbedaan fundamental antara alamat fisik (MAC) dan alamat logis (IP) beserta perannya masing-masing.
2. Mendemonstrasikan cara menemukan informasi pengalamatan jaringan pada perangkat yang berbeda menggunakan perintah yang sesuai (*command line interface*).
3. Mencatat dan membandingkan informasi PDU, khususnya alamat MAC dan IP sumber serta tujuan, pada saat komunikasi terjadi di dalam jaringan lokal (antar *host* dalam satu segmen) dan saat menuju jaringan *remote* (melalui *gateway*).

PERSIAPAN

Praktikan diharapkan mempelajari Group Exam Modules 8 - 10 : Communicating Between Networks Exam yang terdiri dari beberapa chapter serta mendownload software :

1. Software [Packet Tracer 8.2.2](#)
2. Komputer/Laptop
3. Sistem Operasi Windows/ Linux / Mac OS

KEYWORDS

MAC Address, IP Address (IPv4, IPv6), ARP (Address Resolution Protocol), PDU (Protocol Data Unit), Packet Tracer, Unicast, Broadcast, OSI Model (Layer 2, Layer 3), Default Gateway



TABLE OF CONTENTS

PENDAHULUAN.....	2
TUJUAN.....	2
TARGET MODUL.....	2
PERSIAPAN.....	2
KEYWORDS.....	2
TABLE OF CONTENTS.....	3
Materi.....	4
1. Mengidentifikasi Alamat MAC dan IP.....	4
1.1. Pengenalan Alamat Jaringan.....	4
1.2. Sinergi Alamat Fisik dan Logis.....	4
2. Alamat MAC (Media Access Control).....	5
2.1. Definisi dan Karakteristik Alamat MAC.....	5
2.2. Struktur dan Format Alamat MAC.....	5
2.3. Jenis Komunikasi Berbasis Alamat MAC.....	5
3. Alamat IP (Internet Protocol).....	6
3.1. Definisi dan Karakteristik Alamat IP.....	6
3.2. Evolusi Alamat IP: IPv4 dan IPv6.....	6
3.3. Struktur Alamat IPv4.....	7
3.4. Jenis Alamat IP: Publik dan Privat.....	7
4. Address Resolution Protocol (ARP).....	7
4.1. Fungsi dan Kebutuhan ARP.....	7
4.2. Mekanisme Kerja ARP dan ARP Cache.....	8
Latihan & Tugas.....	9
Praktik.....	9
Identifikasi pada Sistem Operasi Windows.....	9
Identifikasi pada Sistem Operasi macOS dan Linux.....	10
Identifikasi pada Perangkat Mobile.....	10
Pertanyaan Praktek.....	10
Codelab.....	11
PERTANYAAN TUGAS.....	15
Penilaian.....	15
Rubrik Penilaian.....	15
Skala Penilaian.....	16



Materi

1. Mengidentifikasi Alamat MAC dan IP

1.1. Pengenalan Alamat Jaringan

Dalam arsitektur jaringan, setiap perangkat atau *host* yang terhubung memerlukan sistem pengalamatan yang terstruktur agar komunikasi data dapat berlangsung secara efisien dan akurat. Sistem ini diatur oleh model referensi **OSI (Open Systems Interconnection)**, yang membagi fungsi jaringan ke dalam tujuh lapisan. Pada konteks ini, dua jenis pengalamatan fundamental menjadi krusial:

- **Alamat MAC (Media Access Control):** Beroperasi pada **Layer 2 (Data Link Layer)**, berfungsi sebagai alamat fisik untuk pengiriman *frame* dalam segmen jaringan lokal yang sama.
- **Alamat IP (Internet Protocol):** Beroperasi pada **Layer 3 (Network Layer)**, berfungsi sebagai alamat logis untuk perutean *paket* antarjaringan yang berbeda.

Meskipun beroperasi pada lapisan yang berbeda, kedua alamat ini harus bekerja secara sinergis untuk memungkinkan komunikasi *end-to-end* yang sukses, mulai dari pengiriman data di LAN hingga melintasi internet global.

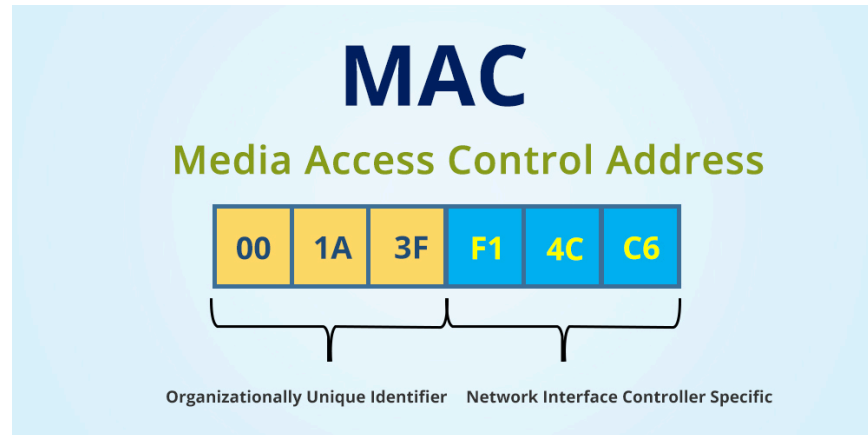
1.2. Sinergi Alamat Fisik dan Logis

Meskipun beroperasi pada lapisan yang berbeda, kedua alamat ini harus bekerja secara sinergis untuk memungkinkan komunikasi *end-to-end* yang sukses. Alamat IP mengarahkan paket ke jaringan tujuan yang benar, sementara alamat MAC memastikan *frame* sampai ke perangkat yang tepat di dalam jaringan lokal tersebut.



2. Alamat MAC (Media Access Control)

2.1. Definisi dan Karakteristik Alamat MAC



Alamat MAC merupakan sebuah pengidentifikasi unik yang ditanamkan secara permanen (*burned-in*) oleh pabrik ke dalam *chip* perangkat keras jaringan, seperti *Network Interface Card* (NIC). Karena sifatnya yang permanen dan melekat pada perangkat keras, alamat ini sering disebut sebagai **alamat fisik** (*physical address*) atau **alamat perangkat keras** (*hardware address*).

2.2. Struktur dan Format Alamat MAC

Alamat MAC memiliki panjang **48 bit (6 byte)** dan umumnya ditulis dalam 12 digit heksadesimal. Struktur 48-bit ini terbagi menjadi dua bagian utama:

- **Organizationally Unique Identifier (OUI):** 24 bit pertama adalah kode unik yang ditetapkan oleh IEEE kepada setiap pabrik. Ini berfungsi untuk mengidentifikasi vendor perangkat keras (misalnya, Cisco, Intel, Realtek).
- **Network Interface Controller (NIC) Specific:** 24 bit terakhir adalah nomor seri yang ditetapkan pabrik untuk setiap perangkat, memastikan keunikan alamat di seluruh dunia.

2.3. Jenis Komunikasi Berbasis Alamat MAC

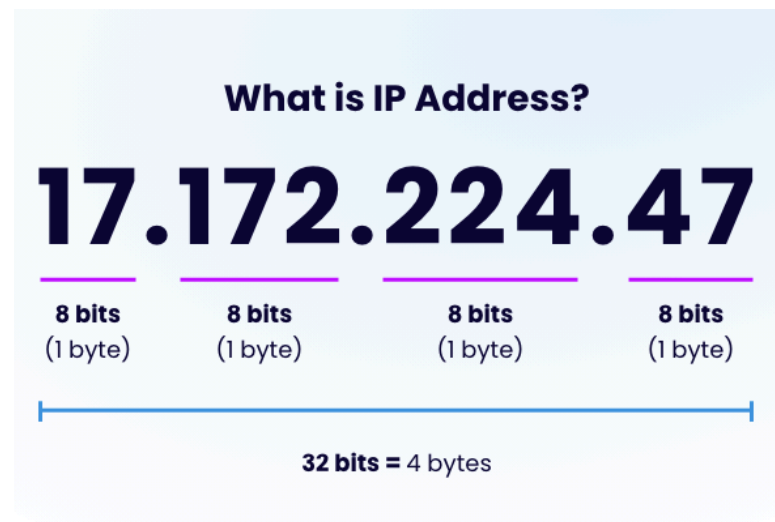
Berdasarkan alamat MAC tujuan, pengiriman *frame* di jaringan lokal dapat dibedakan menjadi tiga jenis:



- **Unicast:** Komunikasi satu-ke-satu. Alamat MAC tujuan adalah alamat spesifik dari satu perangkat penerima.
- **Broadcast:** Komunikasi satu-ke-semua. *Frame* dikirim ke semua perangkat dalam segmen jaringan dengan menggunakan alamat MAC tujuan FF:FF:FF:FF:FF:FF.
- **Multicast:** Komunikasi satu-ke-kelompok. *Frame* dikirim ke sekelompok perangkat tertentu yang tergabung dalam grup *multicast*.

3. Alamat IP (Internet Protocol)

3.1. Definisi dan Karakteristik Alamat IP



Alamat IP adalah sebuah pengidentifikasi logis yang dikonfigurasi pada antarmuka jaringan setiap perangkat. Disebut "logis" karena tidak terikat secara permanen pada perangkat keras dan dapat diubah sesuai dengan topologi atau lokasi perangkat dalam jaringan. Alamat ini berfungsi untuk mengidentifikasi *host* dan lokasi jaringannya.

3.2. Evolusi Alamat IP: IPv4 dan IPv6

- **IPv4 (Internet Protocol version 4):** Merupakan versi yang paling luas digunakan. Dengan panjang 32 bit, IPv4 menyediakan sekitar 4.3 miliar alamat. Namun, jumlah ini sudah hampir habis karena pertumbuhan pesat internet.
- **IPv6 (Internet Protocol version 6):** Dikembangkan untuk mengatasi keterbatasan IPv4. Dengan panjang 128 bit, IPv6 menyediakan jumlah alamat yang masif (3.4×10^{38}) untuk kebutuhan internet di masa depan.



3.3. Struktur Alamat IPv4

Alamat IPv4 ditulis dalam format desimal bertitik (contoh: **192.168.1.1**) dan terdiri dari dua bagian yang pemisahannya ditentukan oleh **Subnet Mask**:

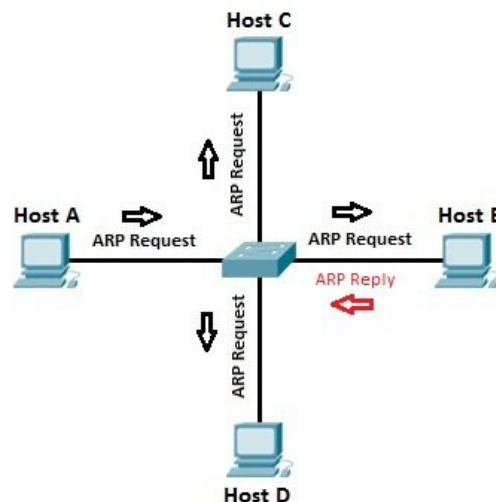
- **Network ID:** Bagian yang mengidentifikasi alamat suatu jaringan.
- **Host ID:** Bagian yang mengidentifikasi perangkat unik dalam jaringan tersebut.

3.4. Jenis Alamat IP: Publik dan Privat

- **Alamat IP Publik:** Alamat yang unik secara global dan dapat dirutekan di internet. Alamat ini ditetapkan oleh Internet Service Provider (ISP).
- **Alamat IP Privat:** Alamat yang digunakan dalam jaringan lokal (LAN) dan tidak dapat dirutekan di internet (contoh: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Untuk berkomunikasi dengan internet, perangkat dengan IP privat memerlukan NAT (Network Address Translation) pada router.

4. Address Resolution Protocol (ARP)

4.1. Fungsi dan Kebutuhan ARP



ARP adalah protokol komunikasi krusial yang berfungsi untuk memetakan alamat Layer 3 (Alamat IP) ke alamat Layer 2 (Alamat MAC) dalam sebuah jaringan lokal. Proses ini mutlak diperlukan karena transmisi data secara



fisik melalui media seperti kabel Ethernet membutuhkan alamat MAC tujuan untuk enkapsulasi *frame*.

4.2. Mekanisme Kerja ARP dan ARP Cache

Ketika sebuah *host* sumber ingin mengirim paket ke *host* tujuan di jaringan yang sama, ia akan memeriksa **ARP Cache**-nya. *ARP Cache* adalah tabel dinamis berisi pemetaan alamat IP ke MAC yang baru ditemukan.

1. Jika pemetaan **ditemukan**, alamat MAC langsung digunakan.
2. Jika **tidak ditemukan**, *host* sumber akan mengirimkan **ARP Request** (broadcast) untuk menanyakan alamat MAC dari IP tujuan.
3. *Host* tujuan akan merespons dengan **ARP Reply** (unicast) yang berisi alamat MAC-nya.
4. Pemetaan ini kemudian disimpan di *ARP Cache* milik *host* sumber untuk mempercepat komunikasi selanjutnya.



Latihan & Tugas

Praktik

Langkah-Langkah Praktik

Identifikasi pada Sistem Operasi Windows

```
Microsoft Windows [Version 10.0.22631.5624]
(c) Microsoft Corporation. All rights reserved.

C:\Users\narut>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : Hush
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : umm.ac.id
    Description . . . . . : Realtek PCIe GbE Family Controller
    Physical Address. . . . . : D8-BB-C1-77-EA-32
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix . :
    Description . . . . . : VirtualBox Host-Only Ethernet Adapter
    Physical Address. . . . . : 0A-00-27-00-00-0F
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-Local IPv6 Address . . . . . : fe80::b30d:42c4:97d1:9cae%15(Preferred)
    IPv4 Address. . . . . : 192.168.56.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
    DHCPv6 IAID . . . . . : 1107951655
    DHCPv6 Client DUID. . . . . : 00-01-00-01-29-E2-53-26-D8-BB-C1-77-EA-32
    NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 14-85-7F-7D-BF-23
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
```

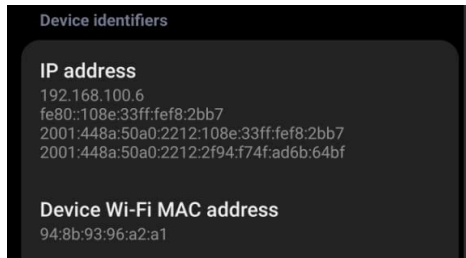
1. Buka **Command Prompt** (ketik **cmd** di menu Start).
2. Gunakan perintah **ipconfig /all**.
3. Perhatikan output pada adapter yang aktif:
 - **IPv4 Address:** Alamat IP perangkat.
 - **Physical Address:** Alamat MAC perangkat.
 - **Subnet Mask:** Penentu segmen jaringan.
 - **Default Gateway:** Alamat IP *router*.



Identifikasi pada Sistem Operasi macOS dan Linux

1. Buka aplikasi **Terminal**.
2. Gunakan perintah **ip addr** atau **ifconfig**.
3. Cari antarmuka jaringan yang aktif (misalnya eth0 atau wlan0):
 - o **inet**: Menunjukkan alamat IPv4.
 - o **ether** atau **link/ether**: Menunjukkan alamat MAC.

Identifikasi pada Perangkat Mobile



- **Android**: Buka *Settings* > *About Phone* > *Status*.
- **iOS (iPhone/iPad)**: Buka *Settings* > *General* > *About* untuk melihat *Wi-Fi Address* (MAC). Untuk Alamat IP, buka *Settings* > *Wi-Fi* dan ketuk ikon informasi (i) di sebelah jaringan yang terhubung.

Pertanyaan Praktek

1. Pada contoh output ipconfig /all, Subnet Mask untuk "Ethernet adapter Ethernet 3" adalah 255.255.255.0. Apa fungsi utama dari Subnet Mask dalam menentukan segmen jaringan sebuah perangkat?
2. Mengacu pada hasil ipconfig /all yang ditampilkan, "Ethernet adapter Ethernet" menunjukkan status Media State: Media disconnected. Apa kemungkinan penyebab status ini dan apa dampaknya terhadap koneksi perangkat ke jaringan melalui adapter tersebut?
3. Seorang pengguna ingin menemukan alamat IP dan alamat MAC pada ponsel Android-nya untuk keperluan pendaftaran jaringan. Berdasarkan panduan diatas manakah kedua informasi tersebut dapat ditemukan?
4. Praktik diatas menyebutkan perintah ip addr atau ifconfig untuk sistem operasi Linux dan macOS. Dalam output dari perintah tersebut, kata kunci apa yang biasanya menandakan alamat IPv4 dan alamat MAC?
5. Lihat pada bagian "Ethernet adapter Ethernet 3" di pada output Windows. Apa deskripsi dari adapter tersebut dan berapa alamat IPv4 yang digunakannya?



Codelab

Silakan unduh terlebih dahulu file resource Packet Tracer pada link berikut:

[Module-3-CL.pka](#)

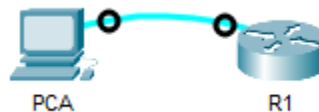
Bagian 1 : Verify the Default Router Configuration

A. Establish a console connection to R1.

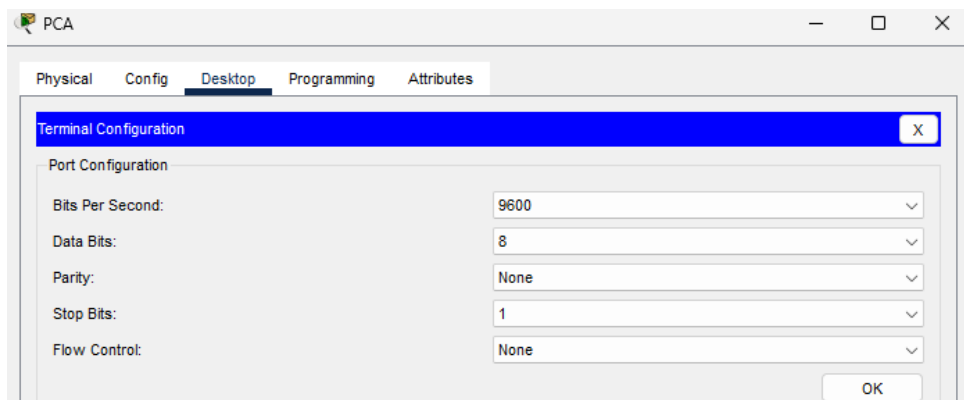
1. Pilih kabel **Console** dari koneksi yang tersedia.



2. Klik **PCA** dan pilih port **RS-232**, kemudian klik **R1** dan pilih **Console**.



3. Klik **PCA**, lalu masuk ke **Terminal** pada tab **Desktop**.



4. Klik **OK** dan tekan **ENTER**. Sekarang **R1** sudah dapat dikonfigurasi.



```

PCA
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 49
bytes of memory.
Processor board ID FTX152400KS
4 FastEthernet interface(s)
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network in
DRAM configuration is 64 bits wide with p
disabled.
255K bytes of non-volatile configuration
249856K bytes of ATA System CompactFlash
Write)

Press RETURN to get started!

Router>
  
```

B. Enter privileged mode and examine the current configuration.

Semua perintah router dapat diakses dari mode privileged EXEC. Namun, karena banyak perintah privileged yang mengonfigurasi parameter operasi, akses privileged harus dilindungi dengan kata sandi untuk mencegah penggunaan yang tidak sah.

1. Masuk ke mode **EXEC** dengan memasukkan perintah **enable**. Pastikan prompt sudah berubah ke **privileged/EXEC mode**.

```

Router>enable
Router#
  
```

2. Masukkan perintah **show running-config** untuk menampilkan konfigurasi saat ini (**running configuration**).

```

Router#show running-config
  
```

3. Tampilkan konten **NVRAM** menggunakan perintah **show startup-config**.

```

Router#show startup-config
  
```

Bagian 2 : Configure and Verify the Initial Router Configuration

A. Configure the initial settings on R1.

1. Konfigurasi R1 sebagai nama host.
2. Konfigurasi **banner MOTD: \$Unauthorized access is strictly prohibited.\$**

```

R1(config)#banner motd $Unauthorized access is strictly prohibited.$
  
```

3. Enkripsi semua kata sandi dengan teks. Gunakan kata sandi berikut:



- Privileged EXEC, unencrypted : cisco
- Privileged EXEC, encrypted : itsasecret
- Console : letmein

Ikuti Langkah ini:

```
R1(config)#enable password ?
7       Specifies a HIDDEN password will follow
LINE    The UNENCRYPTED (cleartext) 'enable' password
level   Set exec level password
R1(config)#enable password cisco
R1(config)#enable secret itsasecret
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

A. Configure the initial settings on R1.

1. Verifikasi pengaturan awal dengan melihat konfigurasi untuk R1.

```
R1#show running-config
```

2. Keluar dari sesi console (petunjuk: **exit**) hingga muncul pesan.

```
R1#exit
R1 con0 is now available
Press RETURN to get started.
```

3. Tekan ENTER; Anda akan melihat pesan berikut.

```
Unauthorized access is strictly prohibited.
User Access Verification
Password:
```

4. Masukkan kata sandi untuk kembali ke mode privileged (petunjuk: **letmein**, **itsasecret**).

Bagian 3 : Save the Running Configuration File

Setelah mengonfigurasi pengaturan awal untuk R1, lakukan backup file konfigurasi yang sedang berjalan ke NVRAM dengan menggunakan perintah **copy running-config startup-config**, dan sebagai opsi tambahan, Anda juga dapat menyimpan konfigurasi



startup ke flash dengan perintah **copy startup-config flash** untuk memastikan bahwa perubahan yang dilakukan tidak hilang jika sistem di-reboot atau jika NVRAM mengalami kerusakan, kemudian verifikasi bahwa konfigurasi telah tersimpan dengan benar menggunakan perintah **show flash**.

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```



PERTANYAAN TUGAS

1. Apa arti pesan *startup-config is not present* pada NVRAM, dan apa dampaknya pada operasi router setelah *reboot*?
2. Mengapa setiap perangkat jaringan seperti router atau switch sebaiknya memiliki MOTD, dan bagaimana hal ini mendukung kebijakan keamanan jaringan perusahaan?
3. Apa perbedaan utama antara perintah `enable secret` dan `enable password` terkait keamanan dan tampilan kata sandi di konfigurasi router?
4. Bagaimana cara menyimpan konfigurasi router secara permanen, dan perintah apa yang digunakan untuk memverifikasi bahwa penyimpanan berhasil?
5. Jelaskan cara kerja protokol *routing* dinamis (RIP/OSPF), dan apa peran router dalam proses penerusan paket data menggunakan protokol tersebut?

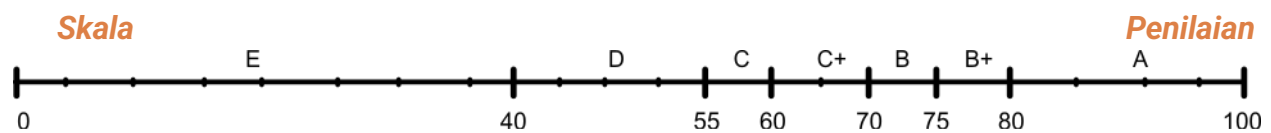
Penilaian

Rubrik Penilaian

Aspek Penilaian	Poin (Total 100%)
Praktik	Total 10%
Kesesuaian Prosedur Pengerjaan	5%
Ketepatan Menjawab Pertanyaan	5%
Codelab	Total 20%
Komunikasi & Presentasi	10%
Penguasaan Materi	10%



Demo	Total 70%
Komunikasi & Presentasi	20%
Kesesuaian Prosedur Pengerjaan	25%
Penguasaan Materi	25%



A = (81 - 100) → Sepuh

B+ = (75 - 80) → Sangat baik

B = (70 - 74) → Baik

C+ = (60 - 69) → Cukup baik

C = (55 - 59) → Cukup

D = (41 - 54) → Kurang

E = (0 - 40) → Bro really...

