

BUKU PRAKTIS

# Teknik Jaringan Komputer



Yang Agita Rindri

**BUKU PRAKTIS**  
**TEKNIK JARINGAN KOMPUTER**

## **UU No 28 tahun 2014 tentang Hak Cipta**

### **Fungsi dan sifat hak cipta Pasal 4**

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

### **Pembatasan Perlindungan Pasal 26**

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

- i. Penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
- ii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
- iii. Penggandaan Ciptaan dan/atau produk Hak Terkait untuk keperluan pengajaran, kecuali pertunjukkan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
- iv. Penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

### **Sanksi Pelanggaran Pasal 113**

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp 100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah).

**BUKU PRAKTIS  
TEKNIK JARINGAN KOMPUTER**

**Yang Agita Rindri**

**POLITEKNIK MANUFAKTUR NEGERI  
BANGKA BELITUNG  
2022**

## **BUKU PRAKTIS TEKNIK JARINGAN KOMPUTER**

*Penulis* : Yang Agita Rindri

*Pengarah* : I Made Andik Setiawan

*Editor* : Mardiyah Ayu

*Proofreader* : Sidhiq Andriyanto

*Desain Isi* : Subkhan

*Desain Cover* : Muhammad Zenda Rud

*Jumlah halaman* : xi, 99 halaman

*Ukuran buku* : 18 x 25 cm

*Cetakan Pertama* : 2022

*ISBN* : 978-623-97870-7-3

*Penerbit*

***Politeknik Manufaktur Negeri Bangka Belitung***

*Kawasan Industri Air Kantung, Sungailiat, Bangka*

*polmanbabelpress@polman-babel.ac.id*

*Telp/Faks: (0717) 93586*

© Hak Cipta 2022 pada penulis

*Hak Cipta dilindungi undang-undang. Dilarang memperbanyak sebagian atau seluruh buku ini dalam bentuk apapun, baik secara elektronik maupun mekanik, termasuk memfotokopi, merekam, atau dengan system penyimpanan lainnya, tanpa izin tertulis dari penerbit.*

*Perpustakaan Nasional : Katalog Dalam Terbitan (KDT)*

Rindri, Yang Agita

Buku Praktis Teknik Jaringan Komputer/Yang Agita Rindri-  
Sungailiat Bangka: Politeknik Manufaktur Negeri Bangka Belitung, 2022  
110 hlm, 18 x 25 cm

ISBN : 978-623-97870-7-3

1. Komputer

I. Judul

II. Yang Agita Rindri

004.03

## KATA PENGANTAR

---

---

Segala puji syukur penulis panjatkan atas rahmat dan karunia dari Allah S.W.T sehingga dapat menyelesaikan Buku Praktis Teknik Jaringan Komputer ini. Buku ini disusun untuk memudahkan mahasiswa dalam mempelajari teknik jaringan komputer.

Selesainya penyusunan buku ini tidak terlepas dari bantuan dan dukungan dari banyak pihak. Dalam kesempatan ini pula, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu dan mendukung penulis dalam proses penyusunan buku ini.

Penulis menyadari, masih banyak kekurangan yang terdapat dalam buku ini. Oleh karena itu, penulis menerima saran dan masukan dari seluruh pembaca untuk perbaikan buku ini selanjutnya. Penulis mengharapkan buku ini dapat memberikan manfaat bagi seluruh pembaca.

Sungailiat, Juni 2022

Penulis



## **DAFTAR ISI**

---

---

KATA PENGANTAR.....	v
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	x
DESKRIPSI UMUM.....	1
A. Pendahuluan.....	1
B. Teori Jaringan Komputer Dan Komunikasi Data.....	3
MATERI PRAKTIK.....	6
A. Materi Praktik.....	6
MATERI 1 MENGENAL PERANGKAT KERAS JARINGAN.....	7
A. Tujuan Praktik.....	7
B. Dasar Teori.....	7
C. Tugas.....	9
MATERI 2 PENGKABELAN.....	10
A. Tujuan Praktik.....	10
B. Dasar Teori.....	10
C. Tugas.....	13
MATERI 3 INSTALASI SOFTWARE PENDUKUNG praktik.....	14
A. Tujuan Praktik.....	14
B. Dasar Teori.....	14
C. Kegiatan Praktik.....	14
D. Tugas.....	26
MATERI 4 MENGANALISA PROTOKOL JARINGAN DENGAN TOOLS WIRESHARK.....	27
A. Tujuan Praktik.....	27
B. Dasar Teori.....	27
C. Kegiatan Praktik.....	33
D. Tugas.....	38
MATERI 5 MERANCANG PENGALAMATAN JARINGAN.....	39
A. Tujuan Praktik.....	39
B. Dasar Teori.....	39
C. Kegiatan Praktik.....	51
MATERI 6 MEMBUAT LAN SEDERHANA.....	54
A. Tujuan.....	54
B. Dasar Teori.....	54



C. Kegiatan Praktik.....	56
D. Tugas.....	60
MATERI 7 SIMULASI MEMBANGUN VLAN PADA PACKET TRACER.....	61
A. Tujuan Praktik.....	61
B. Dasar Teori.....	61
C. Kegiatan Praktik.....	61
D. Tugas.....	65
MATERI 8 MEMBANGUN JARINGAN LAN DENGAN BEBERAPA SEGMENT JARINGAN (ROUTING).....	67
A. Tujuan Praktik.....	67
B. Dasar Teori.....	67
C. Kegiatan Praktik.....	68
D. Tugas.....	73
MATERI 9 MEMBANGUN JARINGAN LAN WIRELESS.....	75
A. Tujuan Praktik.....	75
B. Dasar Teori.....	75
C. Kegiatan Praktik.....	75
D. Tugas.....	77
MATERI 10 MENGHUBUNGKAN LAN KE INTERNET PADA CISCO PACKET TRACER.....	79
A. Tujuan Praktik.....	79
B. Dasar Teori.....	79
C. Kegiatan Praktik.....	79
D. Tugas.....	84
MATERI 11 NETWORK ADDRESS TRANSLATION.....	85
A. Tujuan Praktik.....	85
B. Dasar Teori.....	85
C. Kegiatan Praktik.....	89
D. Tugas.....	94
DAFTAR PUSTAKA.....	95
GLOSARIUM.....	97
BIOGRAFI PENULIS.....	99

## DAFTAR GAMBAR

---

---

Gambar 1 Topologi Jaringan .....	4
Gambar 2 Topologi Mesh Fully Connected .....	4
Gambar 3 Topologi Star .....	4
Gambar 4 Topologi Ring .....	5
Gambar 5 Perangkat Modem .....	8
Gambar 6 Unshielded Twisted Pair .....	11
Gambar 7 Folded Twisted Pair .....	11
Gambar 8 Shielded Twisted Pair .....	11
Gambar 9 License Agreement Packet Tracer .....	15
Gambar 10 Memilih lokasi Cisco Packet Tracer .....	16
Gambar 11 Memilih lokasi shortcut Cisco Packet Tracer .....	16
Gambar 12 Memilih Additional Task .....	17
Gambar 13 Jendela Informasi tentang proses instalasi .....	17
Gambar 14 Progres instalasi berjalan .....	18
Gambar 15 Tombol finish saat instalasi sudah selesai .....	18
Gambar 16 Halaman registrasi Cisco Packet Tracer .....	19
Gambar 17 Ruang kerja Cisco Packet Tracer .....	19
Gambar 18 Jendela Installer Wireshark .....	20
Gambar 19 Licence agreement Wireshark .....	21
Gambar 20 Memilih fitur Wireshark yang akan di- <i>install</i> .....	21
Gambar 21 Membuat shortcut Wireshark .....	22
Gambar 22 Memilih lokasi instalasi Wireshark .....	22
Gambar 23 Memilih tool penangkap paket data .....	23
Gambar 24 Memilih apakah akan memasang USBCap .....	23
Gambar 25 Progres instalasi Wireshark .....	24
Gambar 26 Licence agreement NpCap .....	24
Gambar 27 Opsi-opsi sebelum instalasi Npcap .....	25
Gambar 28 Proses instalasi Npcap .....	25
Gambar 29 Tujuh layer OSI .....	28
Gambar 30 Lima layer TCP/IP .....	29
Gambar 31 Perbandingan model OSI dan TCP/IP .....	30
Gambar 32 Implementasi ICMP pada proses ping .....	32
Gambar 33 Ruang kerja Wireshark .....	33
Gambar 34 Antarmuka Wireshark .....	34
Gambar 35 Memilih tombol Manage Interface .....	34

Gambar 36 Memilih interface yang akan dianalisa .....	35
Gambar 37 Wireshark menangkap data .....	35
Gambar 38 Melakukan uji ping .....	36
Gambar 39 Memilih frame HTTP yang telah ditangkap .....	36
Gambar 40 Memilih frame ICMP yang telah ditangkap .....	36
Gambar 41 Melihat detil frame HTTP yang ditangkap .....	37
Gambar 42 Topologi Peer to Peer membuat LAN sederhana .....	56
Gambar 43 Langkah percobaan modul 6 memilih device .....	56
Gambar 44 Percobaan modul 6 menguji jaringan P2P .....	57
Gambar 45 Percobaan modul 6 topologi DHCP Server .....	58
Gambar 46 Percobaan modul 6 memilih tab DHCP .....	58
Gambar 47 Percobaan modul 6 menyalakan service DHCP .....	59
Gambar 48 Percobaan modul 6 mengisi start IP .....	59
Gambar 49 Percobaan modul 6 mengkonfigurasi IP Address .....	59
Gambar 50 Percobaan modul 6 cek IP PC .....	60
Gambar 51 Tugas modul 6 .....	60
Gambar 52 praktik modul 7 topologi VLAN .....	62
Gambar 53 Praktik modul 7 memilih VLAN Database .....	63
Gambar 54 Praktik modul 8 topologi LAN 1 router .....	69
Gambar 55 Praktik modul 8 topologi LAN 2 router .....	70
Gambar 56 Praktik modul 9 topologi jaringan WLAN .....	75
Gambar 57 Langkah percobaan modul 9 .....	76
Gambar 58 Praktik modul 9 konfigurasi Port 1 AP .....	76
Gambar 59 Praktik modul 9 cek IP dari Server DHCP .....	77
Gambar 60 Topologi LAN terhubung internet .....	80
Gambar 61 praktik modul 10 mengkonfigurasi DSL .....	81
Gambar 62 Praktik modul 10 konfigurasi PC 1 .....	81
Gambar 63 Praktik modul 10 konfigurasi PC 2 .....	82
Gambar 64 Konfigurasi GigabitEthernet00/0 .....	82
Gambar 65 Konfigurasi GigabitEthernet00/1 .....	82
Gambar 66 praktik modul 10 konfigurasi server .....	83
Gambar 67 praktik modul 10 menguji koneksi .....	83
Gambar 68 Network Address Translation [6] .....	85
Gambar 69 NAT Statis .....	86
Gambar 70 NAT Dinamis [6] .....	87
Gambar 71 Tugas membuat topologi dengan NAT .....	89
Gambar 72 Konfigurasi DNS di PC .....	90
Gambar 73 Membuat topologi dengan PAT .....	92

## **DAFTAR TABEL**

---

---

Tabel 1 Modul-modul praktik JKKD .....	6
Tabel 2 Hubungan kabel pada kabel straight .....	12
Tabel 3 Hubungan kabel pada kabel crossover .....	12
Tabel 4 Fungsi dan PDU Model OSI .....	28
Tabel 5 Layer Model TCP/IP dan PDU .....	30
Tabel 6 Ciri IP versi 4 kelas A .....	40
Tabel 7 Ciri IP versi 4 kelas B .....	40
Tabel 8 Ciri IP versi 4 kelas C .....	41
Tabel 9 Private Address .....	42
Tabel 10 CIDR angka biner kelas C .....	43
Tabel 11 Subnet mask kelas C .....	43
Tabel 12 Subnet mask kelas B .....	43
Tabel 13 Subnet mask kelas A .....	44
Tabel 14 Contoh 1 blok subnet kelas C .....	45
Tabel 15 Contoh 2 blok subnet kelas C .....	46
Tabel 16 Contoh 1 blok subnet kelas B .....	47
Tabel 17 Contoh 2 blok subnet kelas B .....	47
Tabel 18 Contoh 1 blok subnet kelas A .....	48
Tabel 19 Jumlah host subnet mask kelas C .....	49
Tabel 20 Contoh VLSM .....	50
Tabel 21 Praktik modul 8 konfigurasi PC 0 .....	69
Tabel 22 Praktik modul 8 konfigurasi PC 1 .....	69
Tabel 23 praktik modul 10 alamat IP perangkat keras .....	80
Tabel 24 praktik modul 10 jenis kabel yang digunakan .....	81
Tabel 25 Tugas modul 10 kebutuhan alamat IP .....	84

## DESKRIPSI UMUM

### A. Pendahuluan

praktik Jaringan Komputer dan Komunikasi Data (JKKD) merupakan salah satu mata kuliah wajib pada Program Studi D4 Teknologi Rekayasa Perangkat Lunak dengan beban SKS sebanyak 2 sks per minggu setara dengan 340 menit kegiatan laboratorium per minggu.

praktik JKKD pada pedoman praktik ini disusun berdasarkan Silabus dan RPS Tahun Akademik 2020/2021 dengan CPL-PRODI yang dibebankan pada mata kuliah yang meliputi :

1. S9 : Menunjukkan sikap bertanggung jawab atas pekerjaan di bidang keahliannya secara mandiri
2. KU1 : Mampu menerapkan pemikiran logis, kritis, inovatif, bermutu, dan terukur dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan
3. KK1 : Mampu menganalisa permasalahan, mengidentifikasi, dan mendefinisikan kebutuhan dan persyaratan (*requirements*) untuk membangun perangkat lunak di bidang teknologi informasi
4. P3 : Menguasai pengetahuan teoritis yang berkenaan dengan desain algoritma dan analisis kompleksitas algoritma, yang berkaitan dengan struktur data dan manipulasinya, bahasa-bahasa pemrograman, arsitektur dan organisasi komputer, sistem operasi komputer, dan jaringan komputer untuk digunakan dalam menyelesaikan permasalahan dalam rekayasa perangkat lunak

Capaian Pembelajaran Mata Kuliah (CPMK) JKKD antara lain sebagai berikut:

1. CPMK-1: Mahasiswa mampu menganalisis konsep jaringan komputer dan komunikasi data [C4]
2. CPMK-2: Mahasiswa mampu memecahkan studi kasus pengalamatan jaringan. [C4]
3. CPMK-3: Mahasiswa mampu merancang Local Area Network yang mendukung komunikasi data melalui intranet maupun internet. [C6]

Sedangkan Sub- CPMK yang dicapai berdasarkan tiap CPMK meliputi:

#### CPMK-1

1. Mampu menganalisis konsep jaringan komputer dan komunikasi data
2. Mampu menganalisis konsep model jaringan osi dan tcp/ip
3. Mampu menelaah berbagai protokol jaringan tcp/ip
4. Mampu menganalisis perangkat keras jaringan komputer yang sesuai dengan kebutuhan organisasi
5. Mampu merangkai berbagai jenis kabel UTP

#### CPMK-2

1. Mampu mengimplementasikan IP Address Versi 4 pada jaringan komputer
2. Mampu menganalisis konsep subnetting kelas A, B, C
3. Mampu memecahkan permasalahan yang berkaitan dengan subnetting

#### CPMK-3

1. Mampu merancang dan membangun wired LAN Sederhana dengan menggunakan berbagai perangkat keras switch
2. Mampu merancang dan membangun wireless LAN
3. Mampu mengimplementasikan server di LAN
4. Mampu merancang dan membangun LAN dengan menggunakan CSMACD, Switching, and vlans
5. Mampu mengimplementasikan router dalam rancangan LAN/wireless LAN
6. Mampu mengimplementasikan NAT ke dalam rancangan LAN
7. Mampu membuat rancangan LAN berdasarkan studi kasus yang diberikan

Untuk mencapai kompetensi-kompetensi di atas, maka Kegiatan Praktik JKCD dilaksanakan melalui kegiatan-kegiatan praktik yang dibagi menjadi modul-modul praktik berdasarkan CPL yang diharapkan. Setiap modul yang disusun terdiri dari beberapa bagian, antara lain:

1. Tujuan Praktik  
Tujuan Praktik merangkum garis besar Tujuan Praktik pada modul tertentu.
2. Dasar Teori  
Bagian berisi tentang teori Jaringan Komputer dan Komunikasi Data yang berkaitan dengan modul praktik yang dilaksanakan.

### 3. Kegiatan Praktik

Kegiatan Praktik merupakan langkah-langkah percobaan yang dilakukan selama Kegiatan Praktik untuk menjamin bahwa mahasiswa dapat mencapai CPL pada modul praktik tersebut.

### 4. Tugas

Tugas adalah penugasan yang diberikan kepada mahasiswa berkaitan dengan Kegiatan Praktik yang telah dilaksanakan.

praktik JKKD ini menggunakan beberapa tool pendukung antara lain:

#### 1. Packet Tracer

Packet Tracer adalah sebuah software simulator untuk perangkat keras jaringan yang dikeluarkan oleh Vendor Cisco yang dapat digunakan sebagai media pembelajaran dalam bidang Jaringan Komputer [1].

#### 2. Wireshark

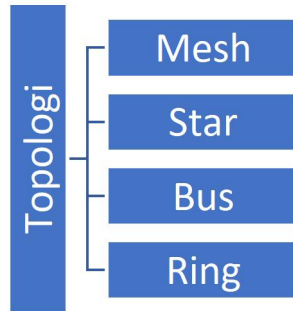
Wireshark merupakan sebuah software open source yang dapat menganalisa paket data yang lewat pada interface jaringan [2].

## **B. Teori Jaringan Komputer Dan Komunikasi Data**

Jaringan Komputer dan Komunikasi Data merupakan dua istilah yang saling berkaitan satu dengan lainnya. Jaringan komputer memungkinkan proses komunikasi data dapat terjadi karena data dikirim dari satu perangkat ke perangkat yang lain melalui jaringan komputer. Sedangkan, komunikasi data merupakan proses pertukaran data yang terjadi antara dua atau lebih perangkat melalui media transmisi seperti media kabel ataupun non kabel [4].

Meskipun memiliki konsep yang hampir sama, akan tetapi jaringan komputer secara lebih spesifik berfokus pada pertukaran data antar komputer dibandingkan dengan komunikasi data yang pertukaran datanya melibatkan perangkat yang lebih luas selain komputer, seperti satelit, telepon dan media telekomunikasi lainnya.

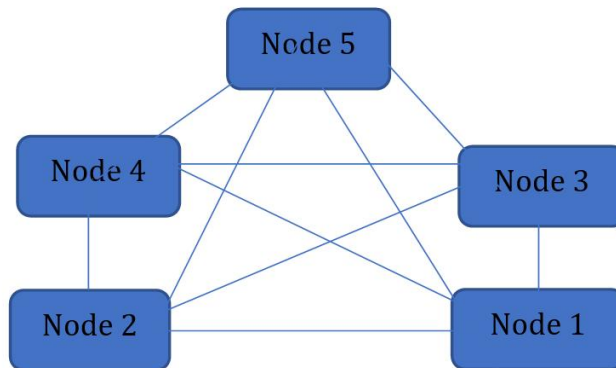
Pada jaringan computer dan komunikasi data dikenal beberapa jenis topologi jaringan. Topologi jaringan merupakan cara perangkat-perangkat pada jaringan komunikasi data saling terhubung satu dengan lainnya. Kategori topologi jaringan digambarkan pada Gambar 1.1.



Gambar 1 Topologi Jaringan

a. Topologi Mesh

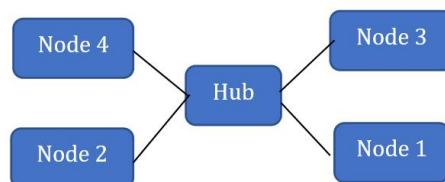
Topologi Mesh merupakan topologi jaringan di mana setiap node saling terhubung dengan semua node yang ada di jaringan secara langsung dengan menggunakan kabel.



Gambar 2 Topologi Mesh Fully Connected

b. Topologi Star

Topologi Star merupakan topologi jaringan di mana setiap node terhubung dengan node lainnya menyerupai bentuk bintang. Semua node yang ada terkoneksi ke 1 buah node utama yang terletak di tengah-tengah jaringan.



Gambar 3 Topologi Star

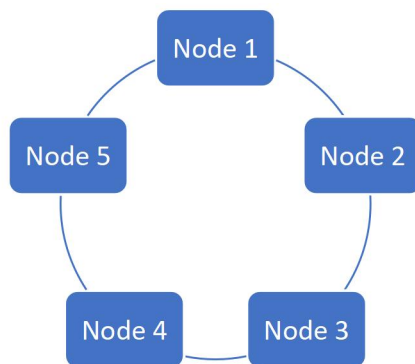


c. Topologi Bus

Topologi Bus menggunakan kabel utama sebagai pusat lalu lintas jaringan. Semua node pada topologi bus terhubung secara serial pada kabel utama tersebut.

d. Topologi Ring

Topologi Ring merupakan topologi yang berbentuk cincin dimana setiap node terhubung ke dua node disebelahnya sedemikian rupa sehingga membentuk cincin.



Gambar 4 Topologi Ring

Berdasarkan cakupan wilayahnya, jaringan terdiri dari kategori-kategori sebagai berikut:

1. Local Area Network

Local Area Network (LAN) merupakan jaringan yang meliputi cakupan wilayah yang kecil, seperti lingkungan kampus, sekolah, atau 1 gedung.

2. Metropolitan Area Network

Metropolitan Area Network (LAN) merupakan jaringan yang meliputi cakupan wilayah dalam 1 kota.

3. Wide Area Network

Local Area Network (LAN) merupakan jaringan yang meliputi cakupan wilayah yang luas, seperti antarnegara.

## MATERI PRAKTIK

### A. Materi Praktik

Materi praktik Jaringan Komputer dan Komunikasi Data (JKKD) terdiri dari 11 modul praktik yang setiap modul terdiri dari percobaan praktik dan Tugas. Alokasi waktu pelaksanaan praktik tiap modul antara 1 hingga 2 minggu (masing-masing minggu 370 menit) dengan rincian sebagai berikut:

Tabel 1 Modul-modul praktik JKKD

<b>Nama Materi</b>	<b>Alokasi Waktu</b>
Materi 1 mengenal perangkat keras jaringan	1 Minggu
Materi 2 Pengkabelan	1 Minggu
Materi 3 Instalasi Software Pendukung praktik	1 Minggu
Materi 4 Menganalisa Protokol Jaringan Dengan Tools Wireshark	1 Minggu
Materi 5 Merancang Pengalamatan Jaringan	2 Minggu
Materi 6 Membuat Lan Sederhana	1 Minggu
Materi 7 Simulasi Membangun Vlan Pada Packet Tracer	1 Minggu
Materi 8 Membangun Jaringan Lan Dengan Beberapa Segmen Jaringan (Routing)	2 Minggu
Materi 9 Membangun Jaringan Lan Wireless	1 Minggu
Materi 10 Menghubungkan Lan Ke Internet Pada Cisco Packet Tracer	1 Minggu
Materi Network Address Translation	1 Minggu

# MATERI 1 MENGENAL PERANGKAT KERAS JARINGAN

## A. Tujuan Praktik

- Agar mahasiswa dapat mengidentifikasi berbagai perangkat keras jaringan
- Agar mahasiswa dapat memahami fungsi dari berbagai perangkat keras jaringan

## B. Dasar Teori

Salah satu komponen penting dari jaringan komputer adalah perangkat keras jaringan komputer. Perangkat keras jaringan komputer adalah perangkat yang digunakan dalam membangun jaringan komputer. Jaringan komputer yang paling sederhana adalah jaringan komputer yang terdiri dari dua buah komputer yang dihubungkan melalui sebuah kabel. Semakin banyak perangkat keras yang digunakan, maka semakin besar jaringan yang dapat terbentuk. Perangkat keras jaringan komputer berfungsi agar jaringan komputer dapat beroperasi dengan baik.

Setiap perangkat keras jaringan memiliki fungsi dan kegunaan masing-masing. Adapun perangkat keras jaringan komputer adalah sebagai berikut:

### a. Modem

Modem merupakan perangkat keras yang berperan sebagai modulator dan demodulator yang mengubah sinyal digital menjadi sinyal analog dan sebaliknya. Sinyal yang keluar dari komputer adalah sinyal digital dengan data biner. Modem mengubah data biner tersebut menjadi analog sehingga dapat ditransmisikan, sebaliknya sinyal analog yang diterima akan diubah terlebih dahulu menjadi sinyal digital sehingga dapat dibaca oleh komputer.



Gambar 5 Perangkat Modem

*Sumber Gambar : <https://cworld.id/product/huawei-modem-e8372/>*

b. Hub

Hub adalah perangkat keras yang dapat menghubungkan dua atau lebih komputer agar dapat saling berkomunikasi dalam 1 subnet jaringan. Komputer-komputer yang terhubung pada satu hub memiliki collision domain yang sama, artinya transmisi data pada hub dapat menyebabkan terjadinya collision atau tabrakan data. Oleh karena itu, saat ini hub sudah tidak digunakan lagi dan diganti dengan perangkat switch.

c. Switch

Switch memiliki fungsi yang sama dengan hub, yakni menghubungkan beberapa komputer dalam 1 jaringan. Berbeda dengan hub, switch memecah collision domain sehingga dapat meminimalisir terjadinya tabrakan data. Akan tetapi, komputer-komputer yang terhubung ke switch memiliki broadcast domain yang sama sehingga semua komputer yang terhubung ke switch dapat mengirim dan menerima broadcast ke semua komputer. Switch yang terhubung ke komputer dalam jumlah yang besar dapat menyebabkan performa jaringan menurun karena banyaknya broadcast yang terjadi.

d. Kabel

e. LAN CARD

f. Access Point

g. Bridge

h. Repeater

### **C. Tugas**

1. Dari poin 2 materi praktik, carilah literatur tentang perangkat keras tersebut lalu jelaskan berbagai perangkat keras jaringan tersebut dalam file presentasi!
2. Identifikasikan perangkat-perangkat keras jaringan yang ada di sekitar Anda, foto dan tampilkan dalam file presentasi Anda!

## MATERI 2 PENGKABELAN

### A. Tujuan Praktik

- Agar mahasiswa dapat mengidentifikasi berbagai jenis kabel yang digunakan dalam jaringan komputer
- Agar mahasiswa dapat membuat berbagai susunan kabel UTP

### B. Dasar Teori

Jaringan komputer dapat dibedakan berdasarkan media transmisinya, yaitu

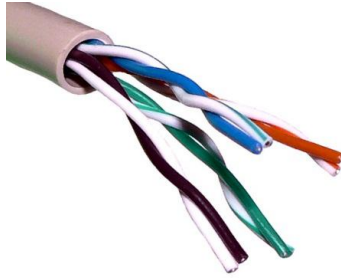
1. Jaringan Berkabel merupakan jaringan yang media transmisinya menggunakan kabel.
2. Jaringan Nirkabel merupakan jaringan yang media transmisinya tidak menggunakan kabel.

Pada jaringan komputer berkabel, terdapat beberapa jenis kabel yang digunakan sebagai media transmisi, antara lain:

1. Fiber Optic yang merupakan kabel yang terbuat dari serat optik, seperti kaca dan plastik yang ukurannya sangat halus.
2. Kabel Coaxial merupakan kabel yang mempunyai 2 konduktor yakni copper pada bagian tengahnya atau pusat inti yang terbuat dari tembaga bertekstur keras dan dilapisi dengan isolator
3. Kabel Twisted Pair merupakan kabel yang biasanya digunakan pada jaringan computer untuk menghubungkan 1 perangkat jaringan computer tertentu dengan perangkat jaringan computer lainnya, seperti menghubungkan computer dengan switch atau menghubungkan switch dengan switch.

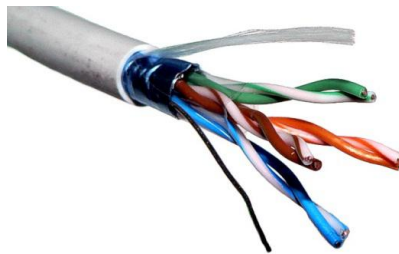
Twisted Pair terdiri dari 3 jenis kabel, yaitu

1. Unshielded Twisted Pair, yakni kabel yang umum digunakan pada LAN yang tidak dilengkapi dengan shield internal, yang disebut unshielded twisted pair (UTP).



Gambar 6 Unshielded Twisted Pair

2. Folded Twisted Pair (FTP) merupakan kabel twisted pair yang menggunakan aluminium foil sebagai selimut yang melindungi lapisan terluar (dibawah karet luar), gunanya untuk mengurangi interferensi elektromagnetik dari luar



Gambar 7 Folded Twisted Pair

3. Shielded Twisted Pair (STP) merupakan kabel twisted pair yang menggunakan aluminium foil untuk melindungi lapisan terluar dan bagian dalam yang melindungi setiap pasangan kabel.



Gambar 8 Shielded Twisted Pair

Dalam praktik ini, jenis kabel yang digunakan adalah dari jenis UTP karena kabel UTP merupakan kabel yang umum digunakan untuk jaringan LAN.

### **Beberapa jenis sambungan kabel UTP**

Kabel UTP memiliki beberapa jenis sambungan yang digunakan untuk koneksi perangkat keras jaringan. Sambungan tersebut antara lain:

1. Kabel Straight adalah jenis sambungan kabel UTP yang digunakan untuk menghubungkan perangkat keras jaringan yang berbeda jenis, misalnya menghubungkan *PC* ke hub atau router.

Tabel 2 Hubungan kabel pada kabel straight

Sisi pertama		Sisi kedua	
Nomor Pin	Warna Kabel	Nomor Pin	Warna Kabel
1	Putih Jingga	1	Putih Jingga
2	Jingga	2	Jingga
3	Putih Hijau	3	Putih Hijau
4	Biru	4	Biru
5	Putih Biru	5	Putih Biru
6	Hijau	6	Hijau
7	Putih Cokelat	7	Putih Cokelat
8	Cokelat	8	Cokelat

Beberapa penggunaan kabel straight antara lain sebagai berikut.

- Menghubungkan PC dengan hub
  - Menghubungkan PC dengan modem
  - Menghubungkan router dengan modem
  - Menghubungkan switch dengan router
  - Menghubungkan hub dengan router
2. Kabel Crossover adalah jenis sambungan kabel UTP yang digunakan untuk menghubungkan perangkat jaringan yang sejenis.

Tabel 3 Hubungan kabel pada kabel crossover

Sisi pertama		Sisi kedua	
Nomor Pin	Warna Kabel	Nomor Pin	Warna Kabel



1	Putih Jingga	1	Putih Hijau
2	Jingga	2	Hijau
3	Putih Hijau	3	Putih Jingga
4	Biru	4	Biru
5	Putih Biru	5	Putih Biru
6	Hijau	6	Jingga
7	Putih Cokelat	7	Putih Cokelat
8	Cokelat	8	Cokelat

Selanjutnya, kedua ujung kabel dihubungkan dengan connector RJ45. Beberapa penggunaan kabel crossover antara lain sebagai berikut.

- Menghubungkan PC dengan PC
- Menghubungkan switch dengan switch
- Menghubungkan hub dengan hub
- Menghubungkan switch dengan hub
- Menghubungkan PC dengan router

### **C. Tugas**

1. Buatlah masing-masing 1 buah kabel straight dan kabel crossover, lalu ujilah dengan menggunakan tester!

## **MATERI 3 INSTALASI SOFTWARE PENDUKUNG praktik**

### **A. Tujuan Praktik**

- Agar mahasiswa mampu menginstal software pendukung praktik

### **B. Dasar Teori**

Dalam praktik Jaringan Komputer dan Komunikasi Data, terdapat 3 buah aplikasi yang digunakan sebagai software pendukung praktik, yaitu:

#### 1. Packet Tracer

Packet Tracer merupakan perangkat lunak simulator untuk mensimulasikan perangkat keras jaringan. Packet Tracer dikeluarkan oleh Vendor Cisco yang dapat digunakan sebagai media pembelajaran dalam bidang Jaringan Komputer [1].

#### 2. Wireshark

Wireshark merupakan sebuah perangkat lunak open source yang dapat menganalisa paket data yang lewat pada antarmuka jaringan [2].

Pada pedoman praktik ini, software-software pendukung diinstal pada Sistem Operasi Windows 10-64 Bit. Software-software pendukung ini dapat diinstal di sistem operasi yang lain, seperti Linux dan macOS dengan terlebih dahulu mendownload installer software yang sesuai dengan sistem operasi yang digunakan.

### **C. Kegiatan Praktik**

#### **C.1 Instalasi Cisco Packet Tracer**

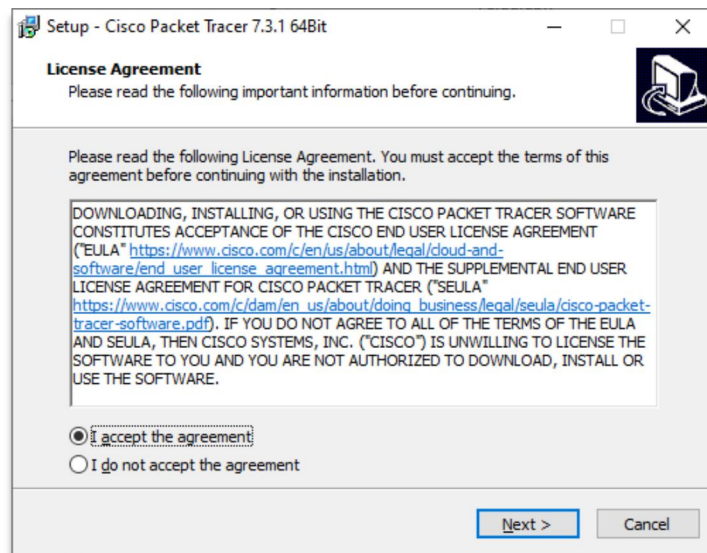
Pada saat panduan praktik ini disusun, Installer Cisco Packet Tracer yang digunakan pada praktik Jaringan Komputer adalah Packet Tracer Versi 7.3.0 Sistem Operasi Windows 64 bit. Mahasiswa dapat mengunduh versi terbaru Packet Tracer dari situs resminya.

Cisco Packet Tracer juga dapat diinstal di sistem operasi lain, seperti Linux, Android 4.2+, iOS 8+ and Microsoft Windows, macOS.

Packet Tracer digunakan sebagai software simulator yang dapat digunakan untuk mendesain jaringan LAN dan WAN dengan menggunakan simulasi perangkat keras jaringan dari Vendor Cisco, seperti PC, Switch, Server, Router, kabel, dan perangkat keras jaringan lainnya.

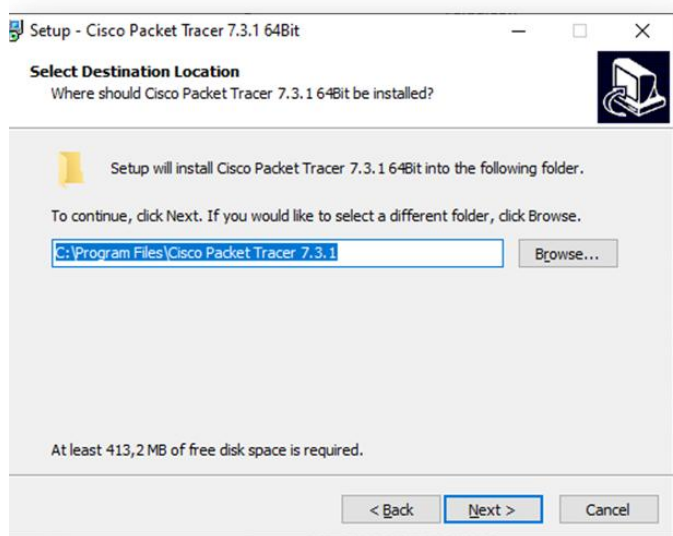
Langkah-langkah instalasi Cisco Packet Tracer Versi 7.3.0 Sistem Operasi Windows 64 bit

1. Download Cisco Packet Tracer Versi 7.3.0 Sistem Operasi Windows 64 bit di situs resmi Cisco lalu simpan di *local drive* pada komputer masing-masing.
2. Klik 2 kali pada file *installer* sehingga akan muncul jendela *License Agreement*. Pilih Radio Button "*I accept the agreement*" untuk menyetujui persetujuan lisensi, lalu tekan tombol *next* untuk melanjutkan instalasi.



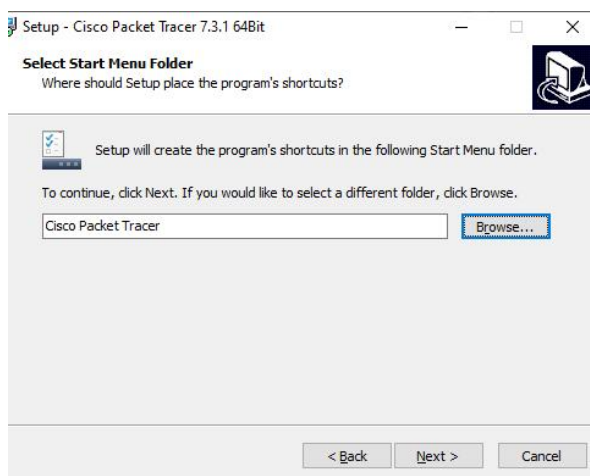
Gambar 9 License Agreement Packet Tracer

3. Pilih lokasi instalasi Cisco Packet Tracer pada local drive komputer, misalnya pada drive C:\Program Files\Cisco Packet Tracer 7.3.1 dengan menekan browse pada jendela Select Destination Location seperti pada Gambar x. Lalu tekan tombol Next untuk melanjutkan instalasi.



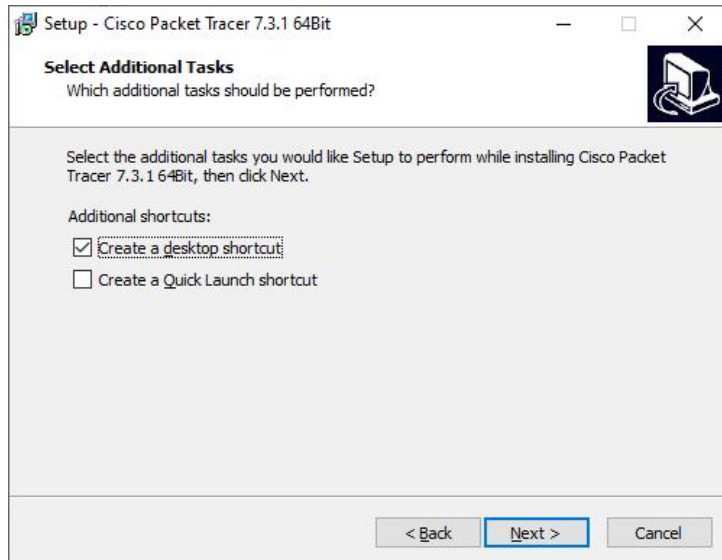
Gambar 10 Memilih lokasi Cisco Packet Tracer

- Langkah selanjutnya adalah memilih lokasi di mana shortcut Packet Tracer akan diletakkan. Tekan tombol Next untuk melanjutkan instalasi.



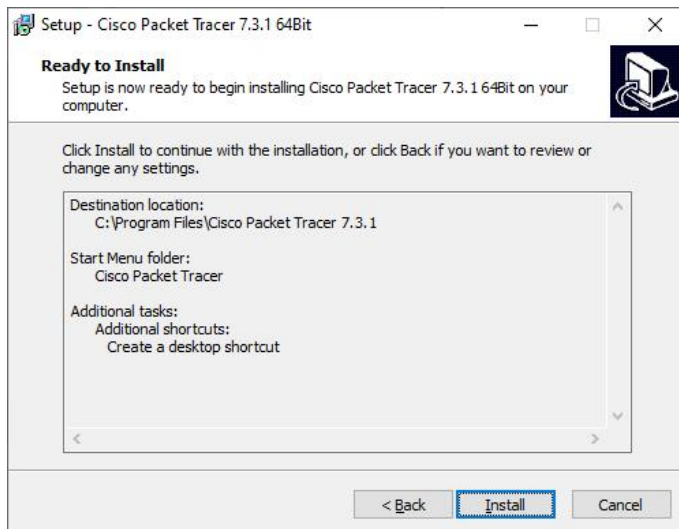
Gambar 11 Memilih lokasi shortcut Cisco Packet Tracer

- Memilih task lain yang dilakukan saat proses instalasi sedang berjalan. Terdapat dua check box yang dapat dipilih, yaitu membuat shortcut di desktop dan/ atau membuat shortcut untuk mempercepat launch Packet Tracer saat akan dibuka dan digunakan. Selanjutnya tekan tombol next untuk melanjutkan instalasi.



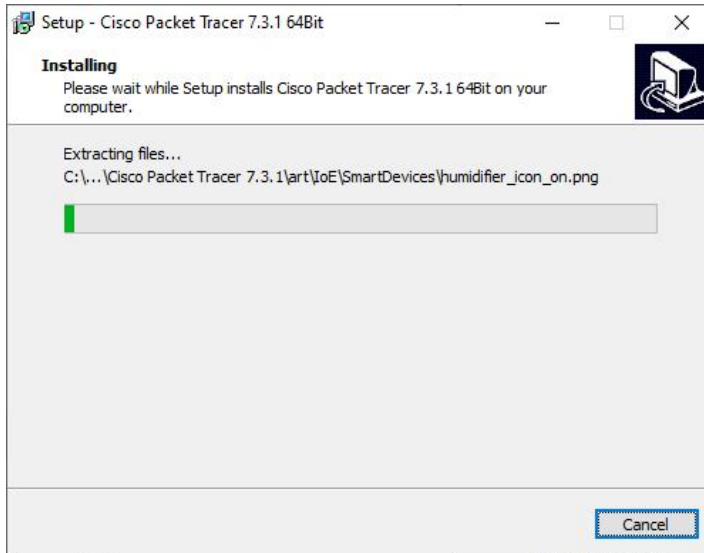
Gambar 12 Memilih Additional Task

6. Proses instalasi sudah hampir siap. Jendela informasi tentang proses instalasi sudah muncul. Jika sudah sesuai, tekan tombol Install.



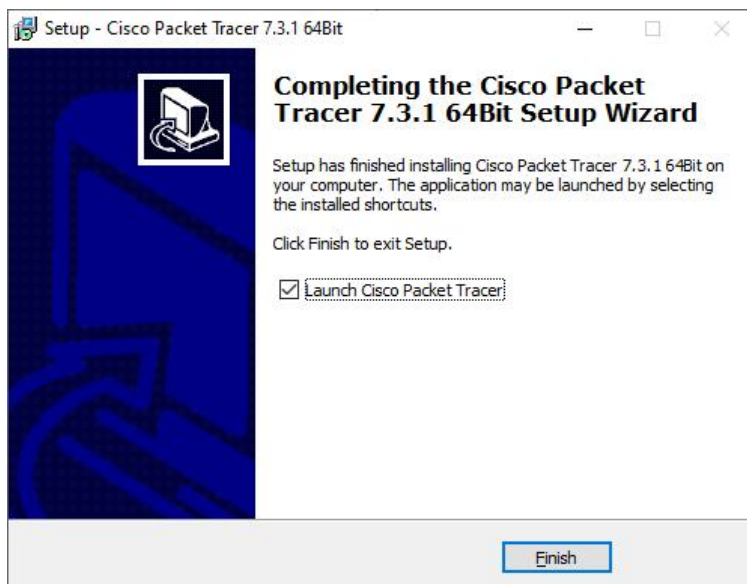
Gambar 13 Jendela Informasi tentang proses instalasi

7. Proses instalasi pun berjalan. Tunggu hingga proses instalasi selesai.



Gambar 14 Progres instalasi berjalan

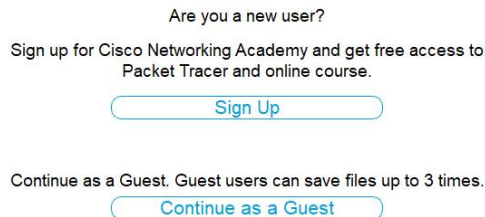
8. Apabila proses instalasi selesai, akan muncul jendela yang menginformasikan bahwa proses instalasi packet Tracer sudah selesai. Tekan tombol Finish.



Gambar 15 Tombol finish saat instalasi sudah selesai

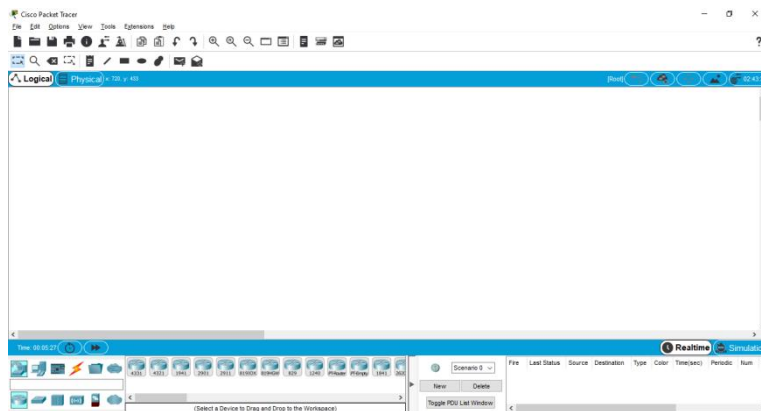
9. Selanjutnya, Cisco Packet Tracer akan meminta user untuk melakukan registrasi apabila user belum memiliki akun di Cisco

Networking Academy atau user dapat menggunakan Packet Tracer dengan akun guest. Jika user sudah memiliki akun, maka login terlebih dahulu agar dapat menggunakan Packet Tracer.



Gambar 16 Halaman registrasi Cisco Packet Tracer

10. Jika sudah berhasil login, maka ruang kerja Packet Tracer dapat digunakan.



Gambar 17 Ruang kerja Cisco Packet Tracer

## C.2 Instalasi Wireshark

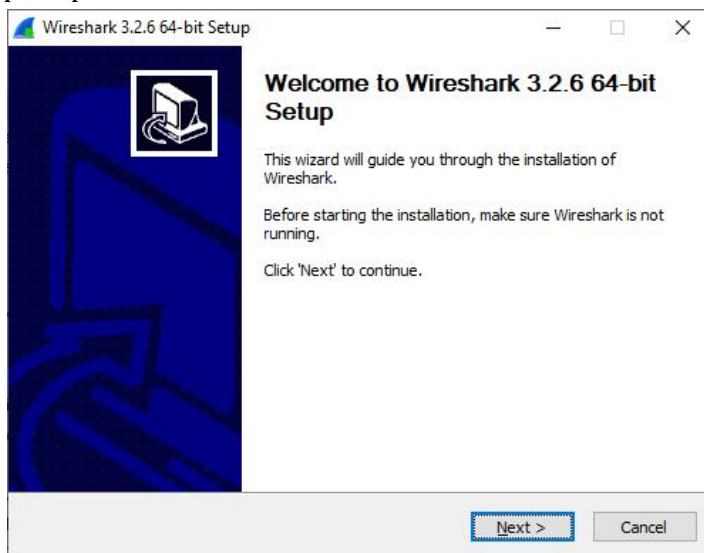
Pada saat panduan praktik ini disusun, Installer Wireshark yang digunakan pada praktik Jaringan Komputer adalah Winshark 3.2.4 Sistem Operasi Windows 64 bit. Mahasiswa dapat mengunduh versi terbaru Wireshark dari situs resminya <https://www.wireshark.org/download.html>. Menurut situs resminya,

wireshark memiliki beberapa installer yang bisa dijalankan di berbagai sistem operasi, seperti Windows Installer (64-bit), Windows Installer (32-bit), Windows PortableApps® (32-bit), dan macOS Intel 64-bit .dmg. Wireshark berjalan pada sistem operasi Windows, Unix/Linux, dan macOS [4].

Wireshark merupakan tool untuk menganalisa paket jaringan. Wireshark mencoba paket jaringan yang lewat dan menampilkan paket data tersebut sedetil mungkin ke dalam GUI Wireshark [5]. Pada praktik Jaringan Komputer, Wireshark digunakan untuk mempelajari berbagai protokol jaringan yang melewati jaringan beserta dengan PDU pada setiap layer jaringan.

Langkah-langkah instalasi Wireshark.

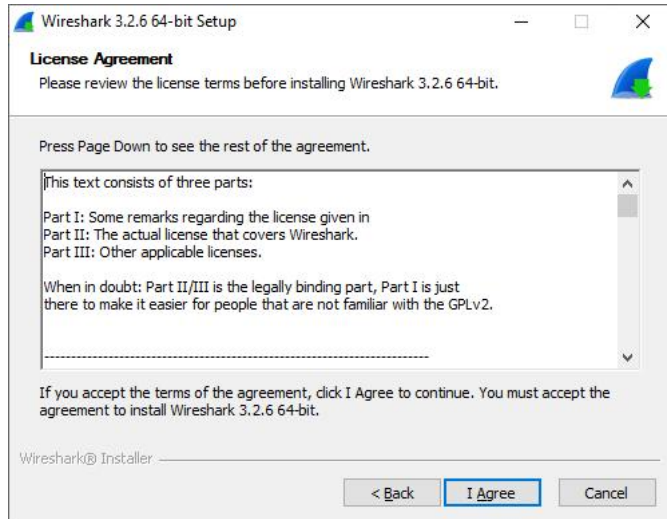
1. Download installer Wireshark dari situs <https://www.wireshark.org/download.html>.
2. Klik 2 kali pada installer Wireshark hingga muncul jendela installer seperti pada Gambar ini. Tekan tombol Next untuk memulai instalasi.



Gambar 18 Jendela Installer Wireshark

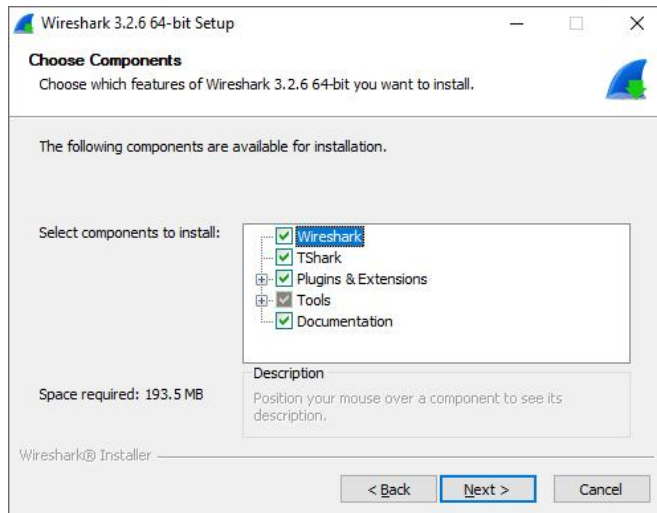
3. Selanjutnya muncul jendela License Agreement. Jika user menyetujui, maka tekan tombol *I Agree*.





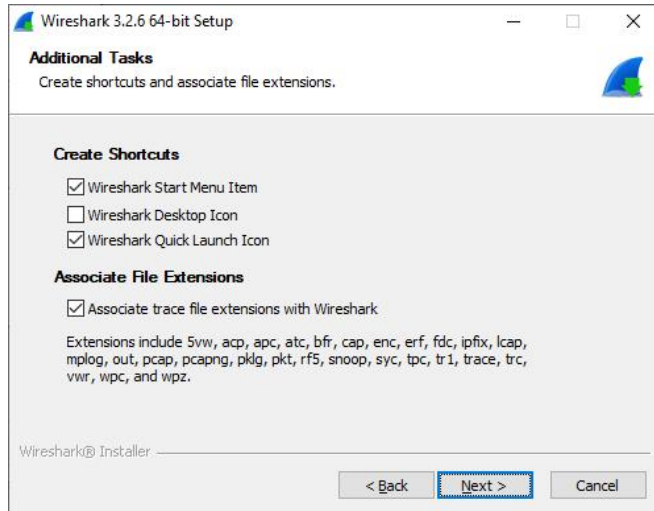
Gambar 19 Licence agreement Wireshark

4. Setelah menyetujui licence agreement, tahap selanjutnya adalah memilih komponen yang akan diinstal. Berilah cek untuk semua check box yang tersedia. Setelah itu tekan tombol Next.



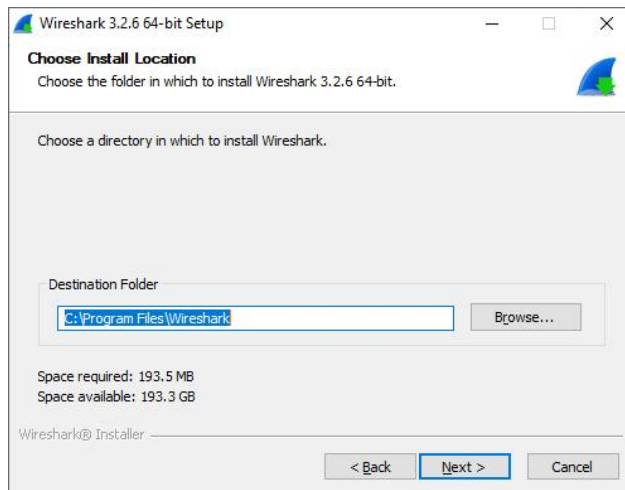
Gambar 20 Memilih fitur Wireshark yang akan di-install

5. Jendela selanjutnya adalah jendela untuk membuat jalan pintas/ shortcut beserta file extention yang diinginkan. Beri tanda check pada checkbox yang diinginkan lalu tekan tombol Next.



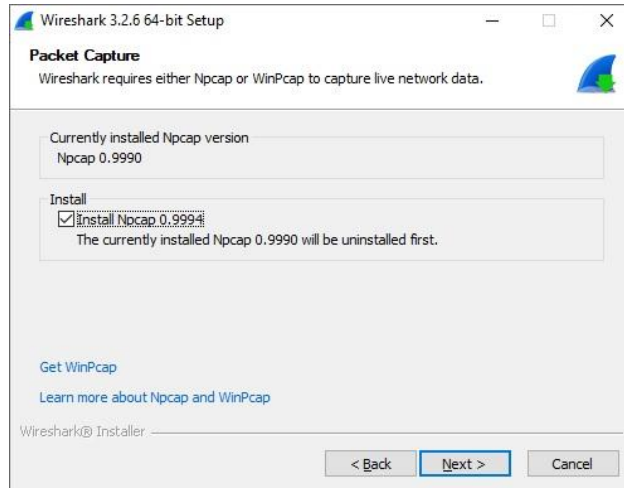
Gambar 21 Membuat shortcut Wireshark

- Langkah selanjutnya adalah memilih lokasi instalasi dengan cara memilih direktori tempat Wireshark diinstal. Tekan tombol Next.



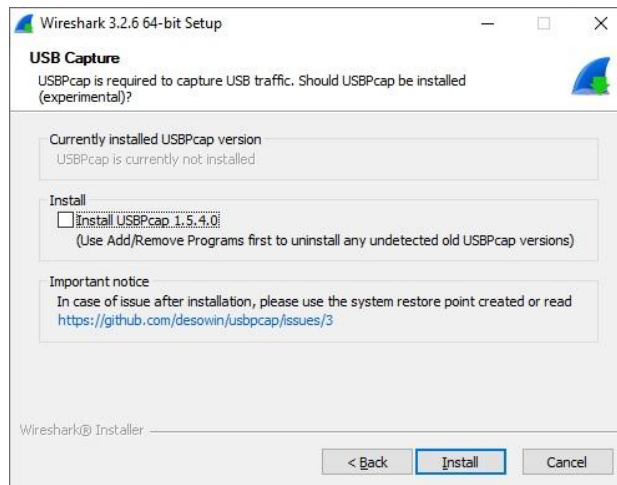
Gambar 22 Memilih lokasi instalasi Wireshark

- Memilih tool penangkap paket data untuk menangkap lalu lintas data secara live. Beri tanda centang pada check box Install Npcap. Klik tombol Next.



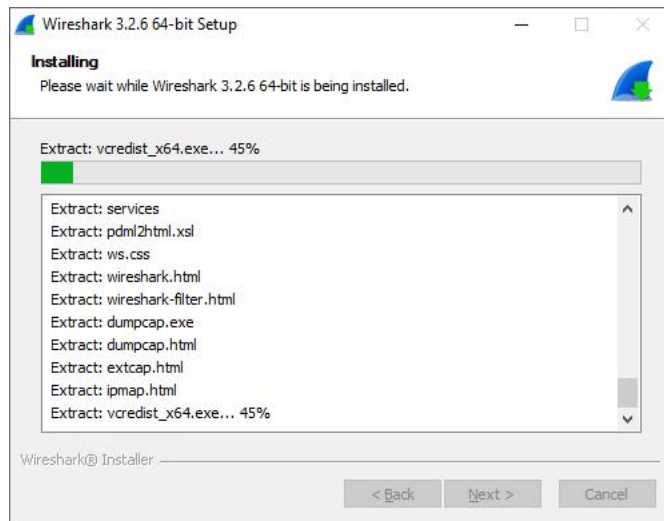
Gambar 23 Memilih tool penangkap paket data

- Langkah selanjutnya adalah memilih apakah akan menginstal USBCap untuk menangkap lalu lintas pada USB. Jika akan memilih, maka beri tanda cek pada checkbox Install USBCap. Setelah itu tekan tombol Install.



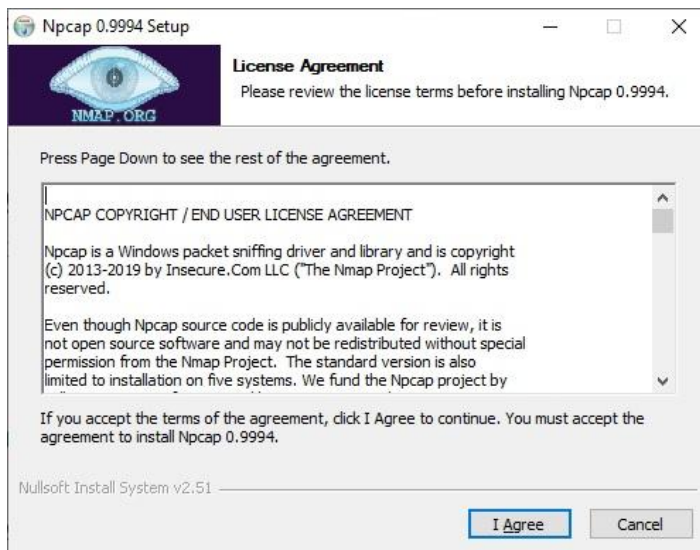
Gambar 24 Memilih apakah akan memasang USBCap

9. Proses instalasi pun berjalan.



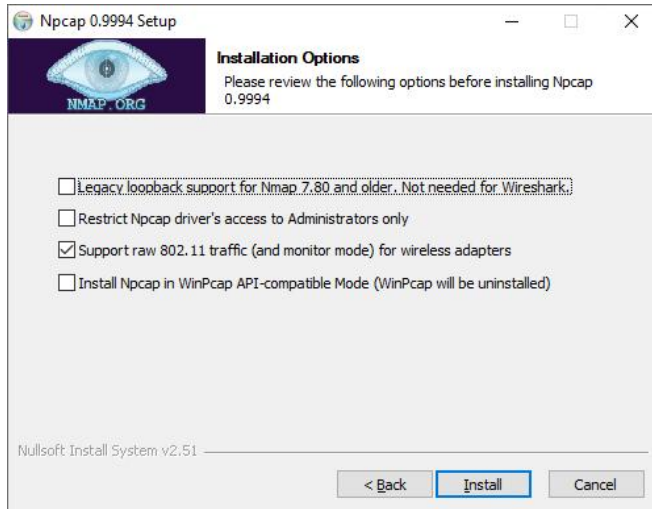
Gambar 25 Progres instalasi Wireshark

10. Saat proses instalasi sedang berjalan, sistem akan meminta konfirmasi apakah akan menyetujui kesepakatan lisensi tool Npcap. Jika menyetujui, tekan tombol "I Agree".



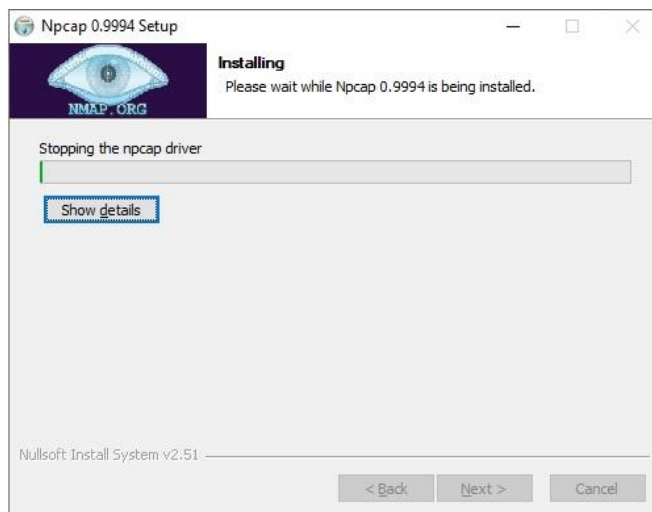
Gambar 26 Licence agreement NpCap

11. Selanjutnya akan muncul jendela untuk memilih opsi-opsi sebelum instalasi Npcap. Tekan tombol Install untuk menginstal Npcap.



Gambar 27 Opsi-opsi sebelum instalasi Npcap

## 12. Npcap mulai dipasang



Gambar 28 Proses instalasi Npcap

13. Jika proses instalasi sempurna, tekanlah tombol Next dan tombol Finish. Proses instalasi Npcap telah selesai dan kita kembali ke jendela instalasi Wireshark.
14. Jika proses instalasi Wireshark sudah sempurna, maka klik tombol Next dan tombol Finish. Kita akan diminta untuk memilih apakah komputer akan segera dinyalakan ulang (reboot) atau komputer akan dinyalakan ulang secara manual nanti.

## **D. Tugas**

1. Buatlah laporan praktik yang telah dilakukan pada Modul 3 ini. Laporan dikumpulkan dalam bentuk PDF dengan format nama file adalah nim\_namamahasiswa.pdf.

# MATERI 4 MENGANALISA PROTOKOL JARINGAN DENGAN TOOLS WIRESHARK

## A. Tujuan Praktik

- Agar mahasiswa mampu menganalisa paket data yang melewati jaringan dengan menggunakan *tool* Wireshark

## B. Dasar Teori

Pada jaringan komputer, berbagai data dan informasi ditransmisikan dari komputer sumber menuju komputer tujuan. Sebagai administrator jaringan, kita perlu mengetahui berbagai data yang melewati jaringan LAN kita untuk menjamin bahwa data yang melewati jaringan adalah data yang aman dengan cara menganalisa data tersebut. Salah satu tool yang dapat digunakan oleh administrator jaringan adalah Wireshark dan NetworMiner.

Wireshark adalah salah satu software yang dapat menangkap informasi paket data yang melewati interface jaringan. Informasi yang berhasil ditangkap melalui Wireshark dapat digunakan untuk:

- Untuk melakukan troubleshooting masalah di jaringan
- Untuk memeriksa keamanan jaringan
- Untuk melakukan sniffing data-data privasi di jaringan

Wireshark dapat digunakan pada jaringan kabel maupun jaringan nirkabel. Wireshark dapat membaca:

- Ethernet yang merupakan bagian dari teknologi jaringan berkabel pada LAN berbasis pada CSMA/CD
- Token-Ring yang merupakan teknologi LAN berbasis pada token
- FDDI yang merupakan metode transmisi data berbasis fiber optic.
- Serial (PPP dan SLIP) yang merupakan protokol bekerja di port serial
- 802.11 wireless LAN yang merupakan teknik transmisi data tanpa kabel
- Koneksi ATM
- Mengetahui IP seseorang

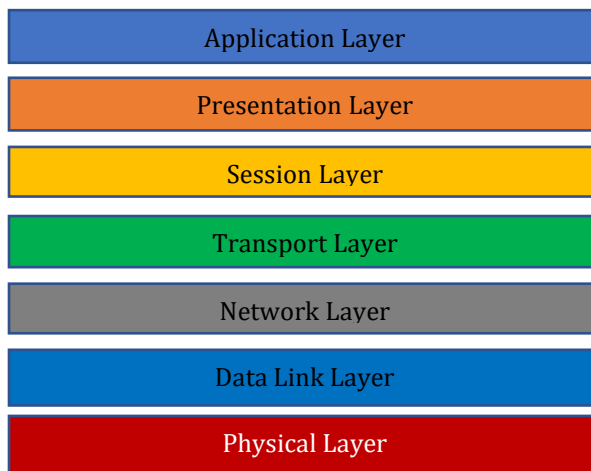
- Transmisi data antar komputer

### B.1 Model Jaringan

Model jaringan pada jaringan komputer adalah sebuah standar yang harus diikuti vendor dalam mengembangkan perangkat keras jaringan [6]. Terdapat 2 model jaringan yang umum digunakan, yaitu:

#### 1. Model OSI

Model OSI terdiri dari 7 layer, yaitu:



Gambar 29 Tujuh layer OSI

Fungsi dan PDU atau Protocol dari Model OSI menurut Forrouzan [6].

Tabel 4 Fungsi dan PDU Model OSI

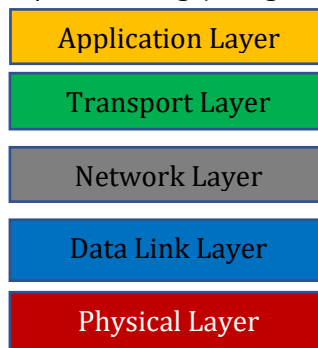
Nama Layer	Fungsi	Contoh
Application layer	Berkaitan dengan layanan terhadap user	HTTP, FTP, Telnet
Presentation layer	Bertanggung jawab terhadap kompresi, enkripsi, dan translasi data.	JPEG, MPEG, MIDI, MP3, GIF, TIFF
Session layer	Bertanggung jawab terhadap kontrol dan sinkronisasi data	RPC, NFS
Transport layer	Bertanggung jawab terhadap pengantaran pesan dari satu proses ke	TCP, SCTP and



	proses yang lain (pengalamatan, dan routing)	UDP
Network layer	Berkaitan dengan transmisi paket dari satu titik ke titik yang lain	IP, ARP, RARP, ICMP, IGMP
Data link layer	Berkaitan dengan transmisi frame dari satu titik ke titik lain	ATM, Frame Relay, FDDI
Physical layer	Berkaitan dengan fisik media transmisi, seperti nilai tegangan, konektor, jumlah pin, dst. Mengatur transmisi bit-bit data pada media transmisi.	RJ45, Ethernet

## 2. Model TCP

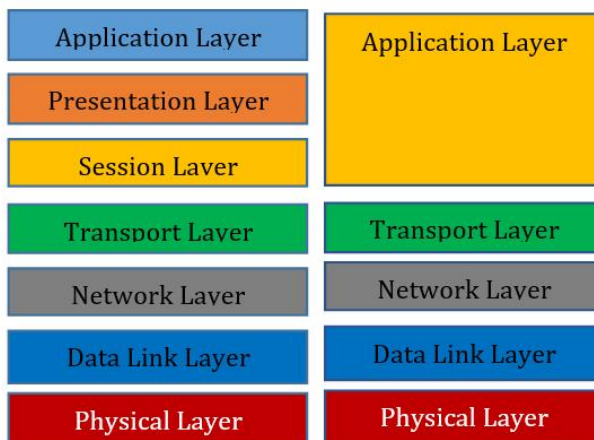
Model TCP/ IP merupakan model jaringan yang saat ini paling banyak digunakan oleh vendor sebagai standar pengembangan perangkat keras jaringan. Model TCP/IP membagi jaringan ke dalam 5 layer.



Gambar 30 Lima layer TCP/IP

### B.2 Model OSI versus TCP/IP

Pada TCP/IP, layer aplikasi merupakan gabungan 3 layer teratas pada Model OSI.



Gambar 31 Perbandingan model OSI dan TCP/IP

Model TCP/IP memiliki lima layer dengan PDU sebagai berikut:

Tabel 5 Layer Model TCP/IP dan PDU

Layer	Data Unit
Layer aplikasi	
Layer transport	Segment
Layer network	Packet
Layer data link	Frame
Layer fisik	Bit

### B.3 Berbagai Protocol TCP/IP

Protokol adalah aturan atau standar yang harus diikuti. Protokol jaringan berarti aturan atau standar yang harus diikuti oleh pengirim dan penerima agar pertukaran data dapat berjalan dengan baik.

Pada TCP/IP terdapat berbagai protokol yang digunakan. Protokol – protokol tersebut dijelaskan sebagai berikut [7].

#### 1. Internet Protocol (IP)

Internet Protocol berjalan pada layer network TCP/IP yang bertanggung jawab untuk mentransmisi paket dari satu titik ke titik lain. IP menggunakan alamat IP agar paket dapat sampai sesuai dengan alamat pengirim dan penerimanya. IP bersifat connectionless artinya IP tidak bertanggung jawab terhadap kesalahan yang terjadi saat pengiriman data. Pada layer network,

tidak perlu membuat dan memelihara koneksi karena yang bertugas melakukan connection oriented adalah layer transport.

2. Transmission Control Protocol (TCP)

Protokol TCP berjalan pada layer transport. Berbeda dengan IP, TCP menyediakan layanan yang connection-oriented sehingga untuk melakukan pengiriman paket perlu untuk membuat dan memelihara koneksi (handshaking). Beberapa fungsi dari TCP adalah menyediakan kontrol data, error detection, dan sequencing. TCP menjamin pengiriman yang reliable. Beberapa aplikasi yang cocok menggunakan TCP antara lain FTP, web browsing, dan email.

3. User Datagram Protocol (UDP)

Protokol UDP yang beroperasi pada layer transport. Berbeda dengan TCP, UDP bersifat connectionless. UDP mengirim paket tanpa mengetahui apakah paket berhasil sampai ke tujuan atau tidak. UDP digunakan untuk aplikasi game online, video streaming, dan voIP.

4. File Transfer Protocol (FTP)

Protokol ini beroperasi pada layer aplikasi dan membutuhkan pengiriman data secara handal. FTP digunakan untuk transportasi data jarak jauh antara 2 titik secara handal.

5. Trivial File Transfer Protocol (TFTP)

TFTP juga merupakan protokol untuk transportasi data antara dua titik. TFTP tidak sehandal FTP karena bersifat connectionless yang menggunakan port UDP 69.

6. Simple Mail Transfer Protocol (SMTP)

SMTP merupakan protokol untuk mengirimkan email dari email server ke penerima. SMTP menggunakan port TCP 25.

7. Hyper Text Transfer Protocol (HTTP)

Protokol HTTP beroperasi pada layer aplikasi menggunakan port TCP 80. HTTP digunakan untuk pengiriman data dari server website ke browser.

8. Internet Control Message Protocol (ICMP)

Protokol ICMP digunakan untuk mengecek transmisi paket dari satu titik ke titik lain untuk mendapatkan informasi terkait masalah yang muncul dalam pengiriman paket. Salah satu implementasi ICMP adalah proses ping ke host tujuan dengan menggunakan command prompt.

```

C:\Users\YANG AGITA RINDRI>ping www.youtube.com

Pinging youtube-ui.l.google.com [172.217.194.91] with 32 bytes of data:
Reply from 172.217.194.91: bytes=32 time=8ms TTL=58
Reply from 172.217.194.91: bytes=32 time=8ms TTL=58
Reply from 172.217.194.91: bytes=32 time=8ms TTL=58
Reply from 172.217.194.91: bytes=32 time=8ms TTL=58

Ping statistics for 172.217.194.91:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 8ms, Average = 8ms

```

Gambar 32 Implementasi ICMP pada proses ping

#### 9. Address Resolution Protocol (ARP)

ARP merupakan protokol yang menterjemahkan alamat IP pada layer network menjadi alamat lokal komputer (MAC Address) pada layer data link. Dalam proses transmisi paket, perlu diketahui MAC Address masing-masing pengirim dan penerima.

#### 10. Reverse Address Resolution Protocol (RARP)

RARP merupakan protokol yang menterjemahkan MAC Address menjadi alamat IP.

#### 11. Simple Network Management Protocol (SNMP)

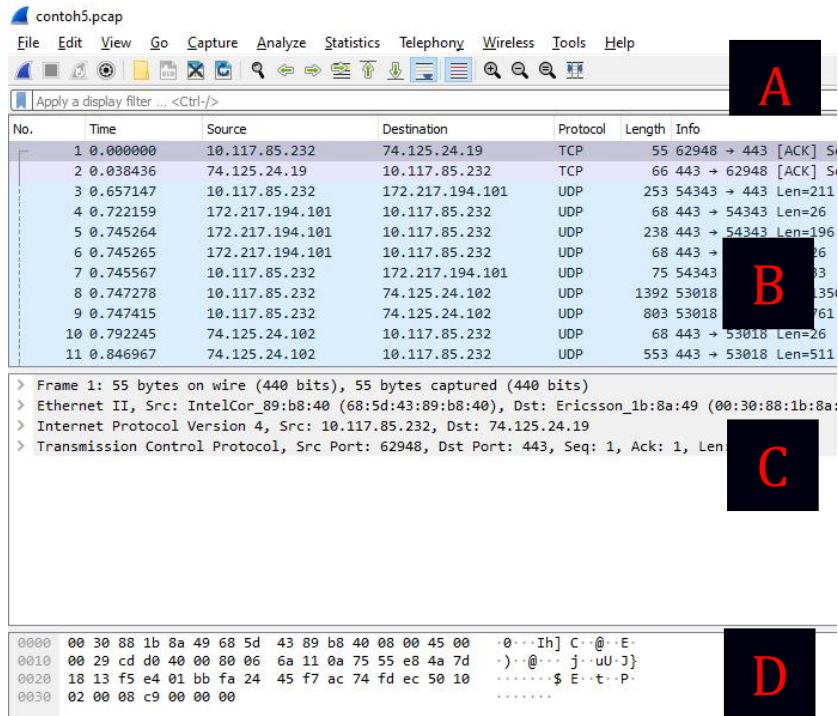
SNMP merupakan protokol untuk manajemen peralatan jaringan, seperti router, switch, server, komputer, dan modem

#### 12. Hyper Text Transfer Protocol Secure (HTTPS)

HTTPs merupakan protokol HTTP yang menerapkan TLS/SSL untuk pertukaran data yang lebih aman.

### B.4 Tool Wireshark

Tool wireshark digunakan untuk menganalisis paket yang melewati jaringan. Untuk melakukan analisis paket yang melewati jaringan terlebih dahulu perlu menginstal tool wireshark. Apabila sudah berhasil melakukan instalasi Wireshark, selanjutnya adalah membuka Wireshark. Saat membuka tool wireshark, akan muncul workspace seperti pada Gambar 1.



Gambar 33 Ruang kerja Wireshark

Bagian-bagian pada workspace Wireshark antara lain:

- Bagian A adalah menu bar dan Tool bar yang menyediakan fitur-fitur penting pada Wireshark
- Bagian B adalah daftar frame yang ditangkap oleh Wireshark yang berisi informasi tentang alamat IP host sumber, alamat IP host tujuan, jenis protokol yang digunakan oleh frame, panjang frame, dan informasi yang berkaitan dengan frame.
- Bagian C menampilkan detail setiap frame yang ditangkap. Untuk menampilkan detail frame yang ingin dilihat, pengguna perlu untuk memilih atau menekan 1 frame pada bagian B.
- Bagian D menampilkan detail frame dalam bentuk hexa

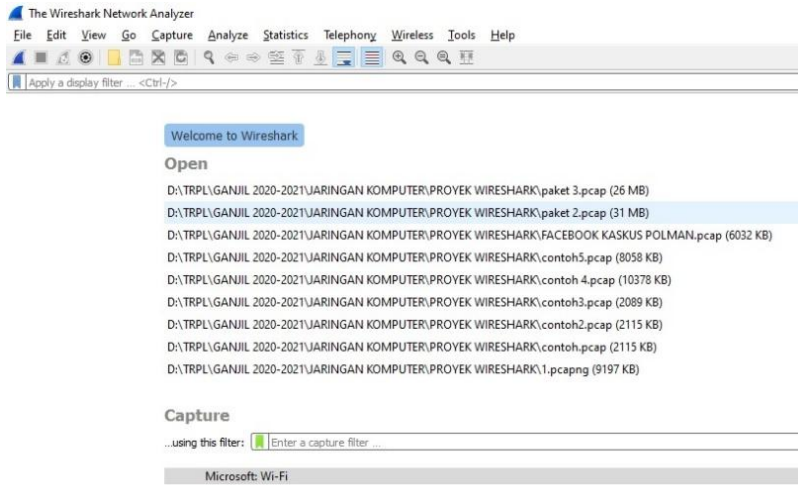
### C. Kegiatan Praktik

praktik modul 4 mendemokan percobaan dalam menangkap dan menganalisa paket data dengan menggunakan tool Wireshark.

#### Percobaan 1 : Melakukan capture jaringan

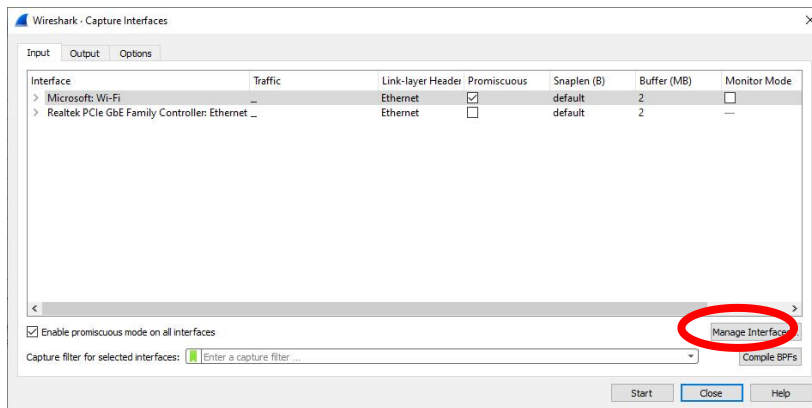
Langkah Percobaan:

1. Bukalah aplikasi Wireshark sehingga muncul halaman awal seperti Gambar 2.32.



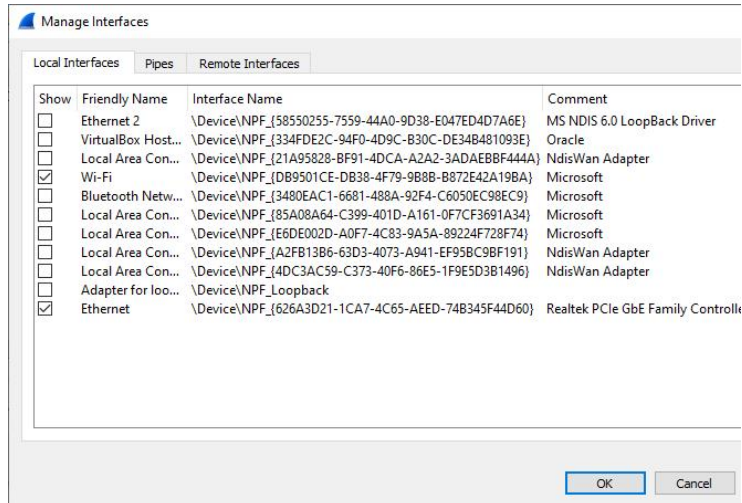
Gambar 34 Antarmuka Wireshark

2. Memilih menu Capture pada tab menu, lalu memilih submenu Option sehingga muncul jendela Capture Interface seperti pada Gambar 2.31.



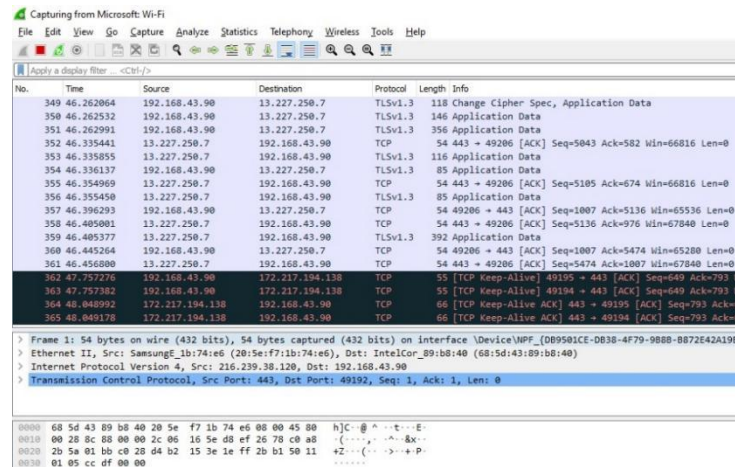
Gambar 35 Memilih tombol Manage Interface

3. Pilih *Button* Manage Interface untuk mengatur interface lokal yang akan ditangkap lalu lintas datanya. Pada contoh ini karena menggunakan Wifi, maka interface yang akan dipilih adalah interface Wi-Fi. Beri tanda centang pada check box Wi-Fi lalu klik OK



Gambar 36 Memilih interface yang akan dianalisa

4. Mulai meng-capture lalu lintas jaringan dengan menekan tombol Start atau memilih menu Capture → Start. Wireshark mulai menangkap paket yang melewati interface.



Gambar 37 Wireshark menangkap data

5. Saat Wireshark mulai menangkap lalu lintas data, bukalah browser lalu ketikkan URL- URL ini.

- <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>
- [www.kaskus.com](http://www.kaskus.com)

dan URL-URL lain

- Lakukan pula ping dari command prompt ke beberapa URL, misalnya ke URL [www.polman-babel.ac.id](http://www.polman-babel.ac.id) dan [www.kaskus.com](http://www.kaskus.com)

```

C:\Command Prompt
Request timed out.

Ping statistics for 27.126.217.137:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\YANG AGITA RINDRI>ping www.kaskus.com

Pinging kaskus.com [27.126.217.137] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 27.126.217.137:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\YANG AGITA RINDRI>ping www.polman-babel.ac.id

Pinging polman-babel.ac.id [103.29.212.240] with 32 bytes of data:
Reply from 103.29.212.240: bytes=32 time=26ms TTL=57
Reply from 103.29.212.240: bytes=32 time=9ms TTL=57
Reply from 103.29.212.240: bytes=32 time=10ms TTL=57
Reply from 103.29.212.240: bytes=32 time=13ms TTL=57

Ping statistics for 103.29.212.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 26ms, Average = 14ms

C:\Users\YANG AGITA RINDRI>

```

Gambar 38 Melakukan uji ping

- Lalu stop Wireshark
- Perhatikan pada List/ daftar frame yang ditangkap. Pada bagian filter, isilah dengan http. Artinya kita akan menampilkan daftar frame HTTP yang telah ditangkap.

No.	Time	Source	Destination	Protocol	Length	Info
627	47.117153	10.10.116.171	128.119.245.12	HTTP	616	GET /wireshark-labs/INTRO-wire
640	47.364194	128.119.245.12	10.10.116.171	HTTP	293	HTTP/1.1 304 Not Modified

Gambar 39 Memilih frame HTTP yang telah ditangkap

- Setelah itu, gantilah filter dengan ICMP, perhatikan daftar frame yang muncul.

Time	Source	Destination	Protocol	Length	Info
1389	108.345617	10.10.116.171	27.126.217.137	ICMP	74 Echo (ping) request id=0x0001, seq=246/62976,
1416	113.165268	10.10.116.171	27.126.217.137	ICMP	74 Echo (ping) request id=0x0001, seq=247/63232,
1453	118.166376	10.10.116.171	27.126.217.137	ICMP	74 Echo (ping) request id=0x0001, seq=248/63488,
1486	123.165883	10.10.116.171	27.126.217.137	ICMP	74 Echo (ping) request id=0x0001, seq=249/63744,
1528	129.349242	10.10.116.171	103.29.212.240	ICMP	74 Echo (ping) request id=0x0001, seq=250/64000,
1529	129.375656	103.29.212.240	10.10.116.171	ICMP	74 Echo (ping) reply id=0x0001, seq=250/64000,
1537	130.353473	10.10.116.171	103.29.212.240	ICMP	74 Echo (ping) request id=0x0001, seq=251/64256,
1538	130.362734	103.29.212.240	10.10.116.171	ICMP	74 Echo (ping) reply id=0x0001, seq=251/64256,
1546	131.356791	10.10.116.171	103.29.212.240	ICMP	74 Echo (ping) request id=0x0001, seq=252/64512,
1547	131.367661	103.29.212.240	10.10.116.171	ICMP	74 Echo (ping) reply id=0x0001, seq=252/64512,
1564	132.360974	10.10.116.171	103.29.212.240	ICMP	74 Echo (ping) request id=0x0001, seq=253/64768,
1565	132.374398	103.29.212.240	10.10.116.171	ICMP	74 Echo (ping) reply id=0x0001, seq=253/64768,

Gambar 40 Memilih frame ICMP yang telah ditangkap



10. Selanjutnya pada langkah ke 8, coba klik pada frame HTTP yang paling atas. Perhatikan bagian detil frame seperti Gambar 2.37.

```
> Frame 627: 616 bytes on wire (4928 bits), 616 bytes captured (4928 bits) on interface \Device\NPF_{DB9501CE-D838-4F...}
> Ethernet II, Src: IntelCor_89:b8:40 (68:5d:43:89:b8:40), Dst: Routerbo_48:52:ca (c4:ad:34:48:52:ca)
> Internet Protocol Version 4, Src: 10.10.116.171, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54048, Dst Port: 80, Seq: 1, Ack: 1, Len: 562
> Hypertext Transfer Protocol
```

Gambar 41 Melihat detil frame HTTP yang ditangkap

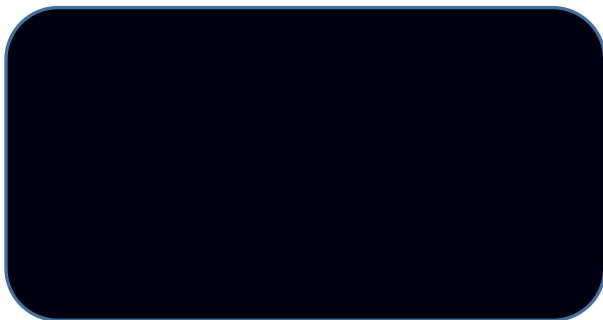
11. Selanjutnya, pada langkah ke 9, klik frame ICMP yang paling atas. Perhatikan bagian detil framenya.

## D. Tugas

1. Dari kegiatan percobaan mengcapture HTTP di atas, catatlah detail frame yang ditangkap oleh wireshark
  - a. Data Link Layer/Ethernet frame



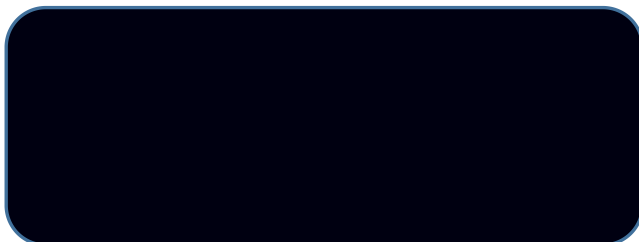
- b. Network Layer/ IP datagram



- c. Transport Layer/TCP segment



- d. Application Layer / HTTP message



## MATERI 5 MERANCANG PENGALAMATAN JARINGAN

### A. Tujuan Praktik

- Agar mahasiswa mampu memahami alamat IP dan dapat merancang pengalamatan komputer sehingga jaringan komputer berfungsi dengan baik

### B. Dasar Teori

#### B.1 Alamat IP

Menurut Behrouz A. Forrouzan, alamat IP merupakan alamat logik yang berjalan pada layer Network di protokol TCP/IP [6]. Terdapat dua jenis alamat IP, yaitu IP Versi 4 atau disebut dengan Ipv4 dan IP Versi 6 atau Ipv6. Alamat IP bersifat unik artinya satu alamat IP hanya boleh digunakan oleh 1 host saja dan tidak boleh digunakan oleh host yang lain. Satu host mengacu kepada 1 buah perangkat keras komputer. Lembaga yang berwenang mengatur penggunaan alamat IP di seluruh dunia adalah IANA yang merupakan singkatan dari *Internet Assigned Numbers Authority*. IP versi 4 (IPv4) menggunakan 32 bit untuk alamatnya, sementara IP versi 6 (IPv6) menggunakan 128 bit.

Saat ini, Ipv4 masih digunakan secara luas dalam membangun jaringan LAN dan WAN sehingga untuk praktik Jaringan Komputer ini, Ipv4 masih digunakan. Adapun alamat IP versi 4 dibagi menjadi 2 bagian, yakni:

1. Bagian bit network yang merupakan alamat suatu network.
2. Bagian bit host yang merupakan alamat host dalam suatu jaringan.

Sehingga host yang terhubung ke dalam jaringan yang sama memiliki bit network yang sama, tetapi memiliki bit host yang berbeda. Apabila beberapa host berada pada jaringan yang berbeda, maka host-host tersebut memiliki bit network yang berbeda.

Ipv4 memiliki beberapa jenis alamat yang dibedakan berdasarkan bit pertamanya, yaitu kelas A, kelas B, dan kelas C.

- Kelas A memiliki ciri:
  - Bit pertama adalah angka 0
  - Oktet pertama merupakan bit yang mengidentifikasikan alamat network dan 3 oktet selanjutnya mengidentifikasikan alamat host.

- Karena bit pertama pada octet pertama adalah 0, maka bentuk decimal dari octet pertama adalah dalam rentang 0 sampai 127 sehingga Jumlah network pada kelas A sebanyak 128
- Karena 3 oktet terakhir merupakan kombinasi angka 0 dan angka 1 sehingga jumlah host yang mungkin terbentuk dari kelas A sebanyak  $256 \times 256 \times 256$  menjadi 16.777.216 host.

Tabel 6 Ciri IP versi 4 kelas A

0NNNNNNN	HHHHHHHH	HHHHHHHH	HHHHHHHH
0 - 127	0 - 255	0 - 255	0 - 255

- Kelas B

Ciri IP Kelas B :

- Dua bit pertama pada oktet pertama alamat IP kelas B adalah 10.
- Dua Oktet pertama merupakan bit yang mengidentifikasi alamat network dan 2 oktet selanjutnya mengidentifikasi alamat host.
- Karena dua bit pertama pada octet pertama adalah 10, maka bentuk decimal dari octet pertama adalah dalam rentang 128 sampai 191 sehingga jumlah network pada kelas B adalah  $64 \times 256$  yakni sebanyak 16.384 network.
- Karena 2 oktet terakhir merupakan kombinasi angka 0 dan angka 1 sehingga jumlah host yang mungkin terbentuk dari kelas B sebanyak  $256 \times 256$  yakni sebanyak 65.536 host.

Tabel 7 Ciri IP versi 4 kelas B

110NNNNN	NNNNNNNN	NNNNNNNN	HHHHHHHH
192 - 223	0 - 255	0 - 255	0 - 255

- Kelas C

Ciri IP Kelas C :

- Tiga bit pertama pada oktet pertama alamat IP kelas C adalah 110
- Tiga oktet pertama merupakan bit yang mengidentifikasi alamat network dan 1 oktet selanjutnya mengidentifikasi alamat host.

- Karena tiga bit pertama pada octet pertama adalah 110, maka bentuk decimal dari octet pertama adalah dalam rentang 192 sampai 223 sehingga jumlah network pada kelas C adalah  $32 \times 256 \times 256$  yakni sebanyak 2.097.152 network.
- Karena 1 oktet terakhir merupakan kombinasi angka 0 dan angka 1 sehingga jumlah host yang mungkin terbentuk dari kelas B sebanyak 254 host

Tabel 8 Ciri IP versi 4 kelas C

10NNNNNN	NNNNNNNN	HHHHHHHH	HHHHHHHH
128 - 191	0 - 255	0 - 255	0 - 255

Selain kelas A, kelas B, dan kelas C, Ipv4 juga memiliki alamat khusus yaitu alamat yang tidak boleh digunakan sebagai alamat pada host. Alamat khusus tersebut adalah

1. Network Address atau alamat jaringan

Network address merupakan alamat yang digunakan untuk mengidentifikasi alamat jaringan. Network Address diperoleh dengan membuat bit host menjadi 0. Dengan membuat bit host menjadi 0, informasi routing pada internet menjadi lebih sederhana sehingga perangkat router hanya melihat alamat jaringan saja dalam mengirimkan paket data.

Salah satu contoh network address adalah pada kelas A dengan alamat 10.10.1.5 memiliki network address 10.0.0.0. Sedangkan pada kelas C, alamat IP 192.168.1.10 memiliki network address 192.168.1.0.

2. Broadcast Address

Broadcast address merupakan alamat untuk mengirimkan informasi-informasi yang diterima oleh seluruh host yang ada pada jaringan tertentu. Sebagai contoh, host A dan host B dengan alamat IP masing-masing 192.168.1.2 dan 192.168.1.3 berada dalam satu jaringan yang sama, yaitu 192.168.1.0. Agar kedua host ini dapat mengirim/ menerima informasi yang harus diketahui oleh seluruh host pada jaringan 192.168.1.0, maka membutuhkan alamat broadcast yang digunakan untuk mengirimkan informasi broadcast. Alamat broadcast didapat dengan mengubah seluruh bit pada bit

terakhir menjadi 1. Dengan demikian alamat broadcast host A dan host B adalah 192.168.1.255.

Selain alamat IP yang disebutkan di atas, masih ada 1 jenis alamat IP lagi, yaitu Private Address yang digunakan untuk memberi alamat host pada jaringan lokal/ Local Area Network, seperti warnet, kampus, dan perkantoran. Private Address tidak bisa digunakan untuk mengakses internet karena tidak dirouting ke internet sehingga tidak dapat dijadikan alamat pengenal di internet. Untuk menggunakan private address, kita tidak perlu mendaftarkannya ke IANA.

Private Address tersebut terdiri dari 3 kelas yang dapat dipilih sesuai dengan kebutuhan host yang ada di masing-masing organisasi.

Tabel 9 Private Address

KELAS A	10.0.0.0 – 10.255.255.255	16.777.216 hosts
KELAS B	172.16.0.0 – 172.31.255.255	1.048.576 hosts
KELAS C	192.168.0.0 – 192.168.255.255	65.536 hosts

## B.2 Subnetting

Pengalamatan berdasarkan kelas memungkinkan organisasi memiliki jumlah host yang besar dalam 1 segmen jaringan terutama untuk kelas A dan kelas B. Jika dalam 1 segmen jaringan memiliki jumlah host yang besar, maka memungkinkan terjadinya hal-hal berikut:

1. Meningkatkan jumlah broadcast sehingga dapat menurunkan performa jaringan
2. LAN menjadi kurang fleksibel
3. Keamanan LAN menjadi kurang baik

Subnetting menjadi solusi terhadap masalah di atas. Subnetting memungkinkan network administrator membagi-bagi jaringan ke dalam sub jaringan. Masing-masing sub jaringan memiliki blok jaringan dengan alamat yang berbeda antar satu sub jaringan dengan sub jaringan yang lain sehingga tiap-tiap sub jaringan memiliki lalu lintas sendiri dan tidak mengganggu lalu lintas keseluruhan jaringan.

Setiap sub jaringan memiliki alamat network (Network ID) dan Host ID yang berbeda-beda. Perbedaan antara alamat network dan alamat host disebut dengan **subnet mask**. Subnet mask ditulis dengan 2 cara, yaitu:

1. Subnet mask susunan IP Address

Contoh penulisan subnet mask susunan IP address  
192.168.2.5/255.255.255.0

2. Subnet mask susunan CIDR (Classless Inter-Domain Routing)

Contoh penulisan subnet mask susunan CIDR 192.168.2.5/24.  
/24 diperoleh dari banyaknya jumlah angka biner 1 pada alamat IP.

Tabel 10 CIDR angka biner kelas C

11111111	11111111	11111111	00000000
----------	----------	----------	----------

Subnet mask kelas C ditunjukkan pada Tabel 11.

Tabel 11 Subnet mask kelas C

Subnet Mask	Nilai CIDR			
255.255.255.128	/25			
<table border="1"> <tr> <td>255</td> <td>255</td> <td>255</td> <td>0</td> </tr> </table>		255	255	255
255	255	255	0	
255.255.255.192	/26			
255.255.255.224	/27			
255.255.255.240	/28			
255.255.255.248	/29			
255.255.255.252	/30			

Beberapa subnet mask pada Kelas B ditunjukkan pada Tabel 12.

Tabel 12 Subnet mask kelas B

Subnet Mask	Nilai CIDR	Subnet Mask	Nilai CIDR
255.255.128.0	/17	255.255.255.0	/24
255.255.192.0	/18	255.255.255.128	/25
255.255.224.0	/19	255.255.255.192	/26

255.255.240.0	/20	255.255.255.224	/27
255.255.248.0	/21	255.255.255.240	/28
255.255.252.0	/22	255.255.255.248	/29
255.255.254.0	/23	255.255.255.252	/30

Sedangkan subnet mask pada Kelas A ditunjukkan pada Tabel 13.

Tabel 13 Subnet mask kelas A

<b>Subnet Mask</b>	<b>Nilai CIDR</b>	<b>Subnet Mask</b>	<b>Nilai CIDR</b>
255.0.0.0	/8	255.255.240.0	/20
255.128.0.0	/9	255.255.248.0	/21
255.192.0.0	/10	255.255.252.0	/22
255.224.0.0	/11	255.255.254.0	/23
255.240.0.0	/12	255.255.255.0	/24
255.248.0.0	/13	255.255.255.128	/25
255.252.0.0	/14	255.255.255.192	/26
255.254.0.0	/15	255.255.255.224	/27
255.255.0.0	/16	255.255.255.240	/28
255.255.128.0	/17	255.255.255.248	/29
255.255.192.0	/18	255.255.255.252	/30
255.255.224.0	/19		

### 2.2.1 Subnetting Kelas C

Contoh 1 subnetting kelas C:

1. Buatlah subnetting untuk alamat IP 192.168.5.12/26!

Penyelesaian:

CIDR /26 artinya subnet mask 255.255.255.192



Angka 192 pada octet terakhir alamat IP tersebut didapat dari angka biner 1 sejumlah 26-digit sehingga menjadi apabila 255.255.255.192 diubah ke bentuk biner menjadi *11111111.11111111.11111111.11000000*.

Berdasarkan contoh di atas, dapat diperoleh informasi yang berkaitan dengan subnetting kelas C, yaitu:

1. Jumlah Subnet atau subjaringan dari kasus diatas adalah sebanyak 4 subnet. Jumlah subnet diperoleh dengan cara menghitung banyaknya angka biner pada octet terakhir subnet mask yaitu 11000000. Dari octet terakhir ini diketahui bahwa angka biner 1 berjumlah 2 buah. Selanjutnya, angka biner 1 yang berjumlah 2 buah menjadi nilai pangkat terhadap 2, yakni  $2^x$  atau  $2^2$  sehingga jumlah subnet mas adalah 4.
2. Jumlah Host per Subnet diperoleh dengan cara memangkatkan banyaknya angka biner 0 pada octet terakhir lalu mengurangkannya dengan angka 2 atau dengan menggunakan rumus  $2^y - 2$ . Pada kasus di atas yaitu 11000000, maka jumlah angka biner 0 sebanyak 6 buah sehingga diperoleh jumlah host per subnet adalah  $2^6 - 2$  yakni 62 host.
3. Blok Subnet merupakan rentang alamat IP yang dapat digunakan pada sebuah subnet. Blok subnet didapat dengan cara mengurangkan 256 dengan nilai octet terakhir pada subnet mask. Pada kasus di atas, subnet masknya adalah 11000000, artinya nilai octet terakhir subnet mask tersebut adalah 192. Hasil pengurangan  $256 - 192$  diperoleh nilai 64.

Sehingga blok subnetnya adalah setiap kelipatan 64, yakni 0, 64, 128, 192.

Tabel 14 Contoh 1 blok subnet kelas C

Subnet	192.168.5.0	192.168.5.64	192.168.5.128	192.168.5.192
Host Pertama	192.168.5.1	192.168.5.65	192.168.5.129	192.168.5.193
Host Terakhir	192.168.5.62	192.168.5.126	192.168.5.190	192.168.5.254

Broadcast	192.168.5.63	192.168.5.127	192.168.5.191	192.168.5.255
-----------	--------------	---------------	---------------	---------------

Contoh 2:

2. Tentukan subnetting dari 192.168.5.12/24

Penyelesaian:

CIDR /24 artinya 11111111.11111111.11111111.00000000

- Jumlah Subnet =  $2^x = 2^0$
- Jumlah Host per Subnet =  $2^y - 2 = 2^8 - 2 = 256 - 2 = 254$
- Blok Subnet  $256 - 0 = 256$

Tabel 15 Contoh 2 blok subnet kelas C

Subnet	192.168.5.0
Host Pertama	192.168.5.1
Host Terakhir	192.168.5.254
Broadcast	192.168.5.255

### 2.2.2 Subnetting Kelas B

Pada subnetting kelas B, cara subnetting CIDR /17 sampai /24 persis dengan subnetting Class C. Akan tetapi blok subnetnya dilakukan pada oktet ketiga, tidak seperti Class C yang dilakukan di oktet ke empat. Sedangkan CIDR /25 sampai /30 blok subnet dilakukan di oktet keempat, tapi setelah selesai oktet ketiga berjalan maju (counter) dari 0, 1, 2, 3, dst.

Contoh 1:

Tentukan subnetting dari 172.16.0.0/18

CIDR /18 memiliki bilangan biner 11111111.11111111.11000000.00000000 yang nilainya sama dengan bentuk desimal 255.255.192.0. Hasil subnetting contoh tersebut adalah sebagai berikut.

- Jumlah Subnet =  $2^2 = 4$

- Jumlah Host per Subnet =  $2^{14} - 2 = 16.382$  host
- Blok Subnet  $256 - 192 = 64$
- Jadi blok subnet lengkapnya adalah 0, 64, 128, 192.

Tabel 16 Contoh 1 blok subnet kelas B

<b>Subnet</b>	172.16.0.0	172.16.64.0	172.16.128.0	172.16.192.0
<b>Host Pertama</b>	172.16.0.1	172.16.64.1	172.16.128.1	172.16.192.1
<b>Host Terakhir</b>	172.16.63.254	172.16.127.254	172.16.191.254	172.16.255.254
<b>Broadcast</b>	172.16.63.255	172.16.127.255	172.16.191.255	172.16..255.255

### Contoh 2

Tentukan subnetting dari 172.16.0.0/25

CIDR /25 jika diubah ke dalam angka biner 11111111.11111111.11111111.10000000 memiliki nilai yang sama dengan 255.255.255.128.

Dari informasi di atas, maka subnettingnya adalah sebagai berikut.

- Jumlah Subnet =  $2^9 = 512$
- Jumlah Host per Subnet =  $2^7 - 2 = 126$  host
- Blok Subnet  $256 - 128 = 128$
- Jadi subnet lengkapnya adalah 0, 128.

Tabel 17 Contoh 2 blok subnet kelas B

Subnet	172.16.0.0	172.16.0.128	172.16.1.0	...	172.16.255.128
Host Pertama	172.16.0.1	172.16.0.129	172.16.1.1	...	172.16.255.129
Host Terakhir	172.16.0.126	172.16.0.254	172.16.1.126	...	172.16.255.254
Broadcast	172.16.0.127	172.16.0.255	172.16.1.127	...	172.16.255.255

### 2.2.3 Subnetting Kelas A

Subnetting Class A dilakukan pada 3 oktet terakhir, yaitu oktet 2, 3, dan 4. Subnet mask yang bisa digunakan untuk subnetting class A adalah semua subnet mask dari CIDR /8 sampai /30.

### Contoh 1

Lakukan subnetting untuk alamat IP 10.0.0.0/16!

Alamat IP 10.0.0.0 berarti alamat IP kelas A. Subnet Mask /16 jika ditulis ke dalam angka biner adalah

11111111.11111111.00000000.00000000 sedangkan jika ditulis dalam angka desimal menjadi 255.255.0.0.

- Jumlah Subnet =  $2^8 = 256$  subnet
- Jumlah Host per Subnet =  $2^{16} - 2 = 65534$  host
- Blok Subnet =  $256 - 255 = 1$ . Jadi subnet lengkapnya: 0,1,2,3,4, etc.

Dari informasi di atas diperoleh blok subnet untuk contoh 1 seperti pada Tabel 18.

Tabel 18 Contoh 1 blok subnet kelas A

Subnet	10.0.0.0	10.1.0.0	...	10.254.0.0	10.255.0.0
Host Pertama	10.0.0.1	10.1.0.1	...	10.254.0.1	10.255.0.1
Host Terakhir	10.0.255.254	10.1.255.254	...	10.254.255.254	10.255.255.254
Broadcast	10.0.255.255	10.1.255.255	...	10.254.255.255	10.255.255.255

Jika 2 atau lebih jaringan berbeda subnet, maka kedua jaringan tersebut tidak bisa melakukan koneksi secara langsung, namun perlu menggunakan perangkat tambahan, seperti router (bukan switch).

### B.3 Variable Length Subnet Masking - VLSM

Subnetting pada sub bab 2.2 di atas merupakan metode subnetting yang membagi jaringan menjadi subnet-subnet dengan jumlah host yang sama. Misalkan saja kita menggunakan 192.168.1.0/26, maka jumlah subnet adalah 4 buah subnet dengan masing-masing 62 host. Bagaimana apabila jumlah host pada jaringan yang dimiliki bervariasi, misalnya hanya 8 host saja? Maka terdapat 54 alamat yang tidak digunakan.

Oleh karena itu, administrator jaringan dapat menggunakan metode VLSM yang membagi jaringan menjadi subnet-subnet dengan jumlah host

yang berbeda sesuai dengan kebutuhan organisasi. VLSM dilakukan dengan membentuk subnet yang dimulai dari kebutuhan host yang paling banyak.



**Contoh kasus dengan VLSM**

Sebuah perusahaan terdiri dari 4 departemen, yaitu departemen penjualan, departemen SDM, departemen logistik, dan departemen akuntansi. Departemen penjualan memiliki karyawan 60 orang, departemen SDM memiliki karyawan 30 orang, departemen logistik, administrasi, dan umum 121 orang, dan departemen akuntansi 10 orang. Dengan metode VLSM tentukan subnet yang memungkinkan.

Langkah penyelesaian:

1. Rincian jumlah host per departemen

Departemen penjualan = 60

Departemen SDM = 30

Departemen logistik, administrasi, dan umum = 121

Departmen akuntansi = 10

2. Perhatikan subnet pada kelas C

Tabel 19 Jumlah host subnet mask kelas C

CIDR	Jumlah Host
/24	254
/25	126
/26	62
/27	30
/28	14
/29	6
/30	2

3. Untuk metode VLSM dimulai dari jumlah host terbesar, yaitu Departemen logistik, administrasi, dan umum sebanyak 121. Karena jumlah host sebanyak 101, maka dipilih subnet dengan jumlah host yang relevan, yaitu /25 dengan jumlah host maksimum 126 host dengan subnet mask 255.255.255.128. Alamat IP yang dapat digunakan

dari rentang 192.168.1.1 hingga 192.168.1.126 dengan alamat network 192.168.1.0 dan alamat broadcast 192.168.1.127

4. Langkah selanjutnya adalah memilih departemen dengan jumlah host terbanyak kedua, yaitu Departemen Penjualan dengan 60 host. Perhatikan Tabel 19 di atas untuk menentukan subnet mask yang sesuai, yakni /26 dengan jumlah host sebanyak 62 sehingga alamat IP untuk Departemen Penjualan adalah 192.168.1.128 / 26 dengan rentang alamat yang dapat digunakan adalah 192.168.1.129 hingga 192.168.1.190 dengan alamat network 192.168.1.128 dan alamat broadcast 192.168.1.191.
5. Langkah selanjutnya adalah memilih departemen dengan jumlah host terbanyak ketiga, yaitu Departemen SDM 30 host. Sama seperti langkah ke empat, maka subnet mask yang dipilih adalah 192.168.1.192 / 27 dengan rentang alamat yang dapat digunakan adalah 192.168.1.193 hingga 192.168.1.222 dengan alamat network 192.168.1.192 dan alamat broadcast 192.168.1.223. Terdapat 30 host yang memungkinkan untuk digunakan pada subnet mask / 27.
6. Departmen dengan jumlah host paling sedikit adalah Departemen Akuntansi dengan jumlah host sebanyak 10 host. Subnet yang dapat digunakan adalah 192.168.1.224 /28 dengan rentang alamat yang dapat digunakan sebagai alamat host adalah 192.168.1.225 hingga 192.168.1.238 dengan alamat network 192.168.1.224 dan alamat broadcast 192.168.1.239. Terdapat 14 host yang memungkinkan unuk digunakan pada subnet mask /28.
7. Kesimpulan subnet VLSM yang mungkin dibuat dari contoh kasus di atas.

Tabel 20 Contoh VLSM

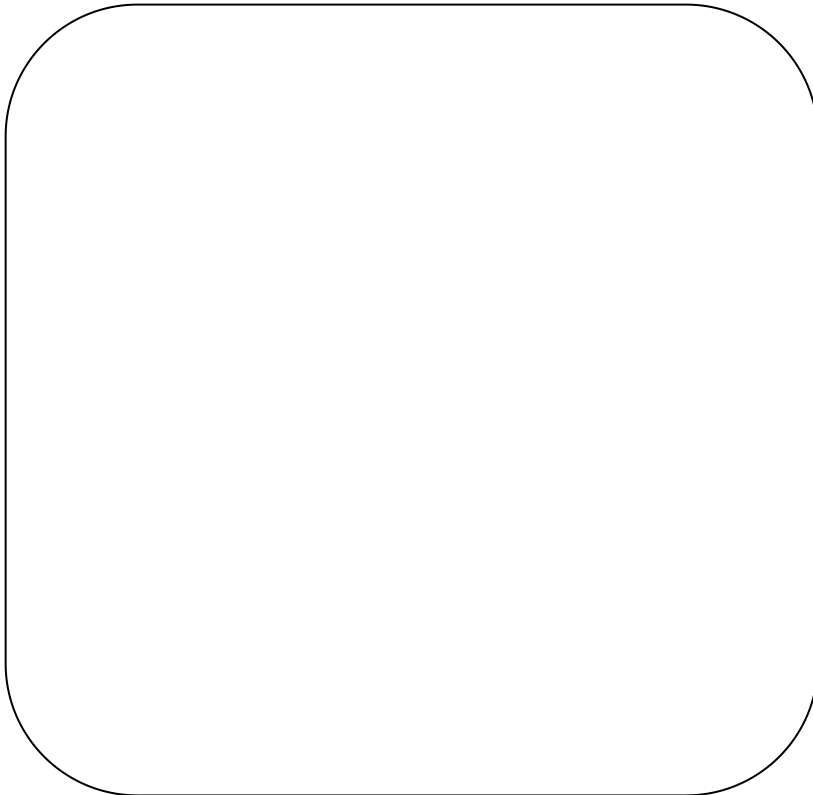
Nama Departemen	Alamat Network	Alamat Host	Alamat Broadcast
Departemen logistik, administrasi, dan umum	192.168.1.0	192.168.1.1 hingga 192.168.1.126	192.168.1.127
Departemen penjualan	192.168.1.128	192.168.1.129 hingga 192.168.1.190	192.168.1.191
Departemen SDM	192.168.1.192	192.168.1.193 hingga	192.168.1.223

		192.168.1.222	
Departemen Akuntansi	192.168.1.224	192.168.1.225 hingga 192.168.1.238	192.168.1.239

### C. Kegiatan Praktik

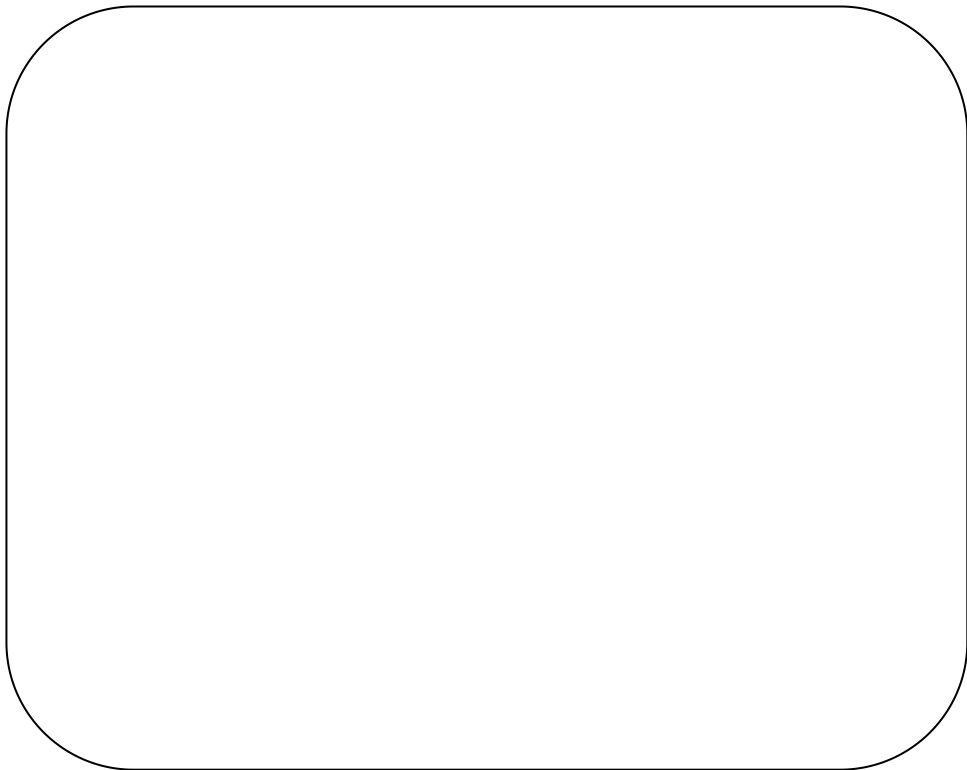
1. Tentukan subnetting dari alamat berikut ini:

- a. 192.168.5.12/25
- b. 192.168.5.12/27
- c. 192.168.5.12/28
- d. 192.168.5.12/29
- e. 192.168.5.12/30



2. Tentukan subnetting dari alamat berikut ini:

- a. 172.16.0.0/19
- b. 172.16.0.0/20
- c. 172.16.0.0/21
- d. 172.16.0.0/26
- e. 172.16.0.0/27

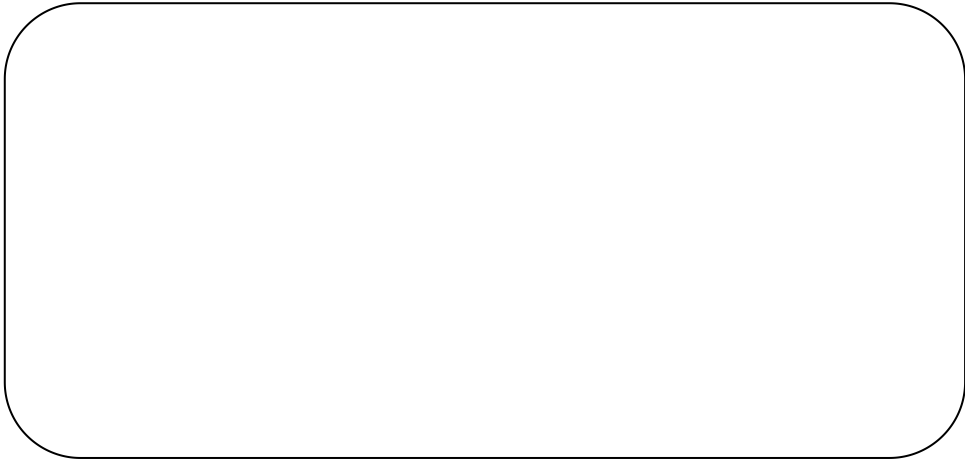




3. Sebuah program studi memiliki 5 laboratorium dengan masing-masing user sebagai berikut:

- Lab Sistem Cerdas memiliki 14 komputer
- Lab Pemrograman memiliki 28 komputer
- Lab Jaringan Komputer memiliki 18 komputer
- Lab Dasar Komputer memiliki 90 komputer
- Lab Multimedia 20 komputer

Buatlah desain alamat IP dengan menggunakan metode VLSM!



## MATERI 6 MEMBUAT LAN SEDERHANA

### A. Tujuan

Tujuan dari praktik ini adalah

- Agar mahasiswa dapat memahami bagaimana membangun jaringan LAN sederhana dengan menggunakan software simulasi Cisco Packet Tracer

### B. Dasar Teori

Local Area Network (LAN) adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung.

Lan terdiri dari 2 jenis, yaitu

1. Peer to Peer : Local Area Network (LAN) adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung.
2. Client Server : hanya satu komputer yang bertugas sebagai server dan komputer lain berperan sebagai workstation

Sebuah komputer biasanya memiliki 1 buah port ethernet untuk mendukung koneksi dalam jaringan LAN. Port ini akan terhubung dengan media transmisi yang berupa kabel UTP. Karena komputer hanya memiliki 1 port, maka satu komputer tidak dapat dihubungkan ke beberapa komputer.

Untuk mengatasi hal tersebut, maka digunakan switch atau hub. Satu buah switch dapat menghubungkan lebih dari 1 komputer sehingga switch umum digunakan untuk membentuk satu segmen jaringan. Satu segmen jaringan ditandai dengan 1 broadcast domain yang artinya seluruh komputer yang terhubung ke switch akan menerima broadcast dari setiap komputer yang terhubung ke switch. Satu segmen jaringan juga ditandai dengan alamat IP yang berada dalam 1 segmen yang sama.

Untuk membangun jaringan LAN lokal, setiap PC atau mode yang terhubung ke jaringan LAN harus memiliki alamat IP sebagai alamat logik pengiriman paket data. Oleh karena itu, perlu untuk mengatur konfigurasi alamat IP pada setiap PC. Dalam memberikan alamat IP pada setiap PC pada jaringan lokal, terdapat 2 metode pemberian alamat IP, yaitu

1. Statik
2. Dinamik

Alamat IP yang bersifat statik harus ditetapkan di PC masing-masing. Alamat IP tersebut akan bersifat tetap meskipun PC dimatikan.

Sedangkan alamat IP dinamik ditetapkan dengan menggunakan layanan DHCP yang disediakan oleh server DHCP. Untuk menetapkan IP dinamik, perlu disiapkan sebuah server DHCP. Server DHCP dapat dibangun pada sebuah dedicated server atau ditetapkan di router. Server DHCP akan memberikan alamat IP kepada setiap PC yang terhubung ke server sehingga pengguna PC tidak perlu menetapkan alamat IP di PC masing-masing. Server DHCP menyediakan range IP yang digunakan oleh PC klien. Dengan menggunakan Server DHCP, setiap PC mendapatkan IP yang dinamik, artinya alamat IP tersebut akan berubah-ubah setiap kali pengguna menyalakan PC.

## C. Kegiatan Praktik

Pada praktik ini, kita akan membuat topologi jaringan peer to peer dan client server untuk membangun simulasi satu segmen jaringan.

### **Percobaan 1: Membuat jaringan LAN Peer to Peer yang terdiri dari 2 PC**

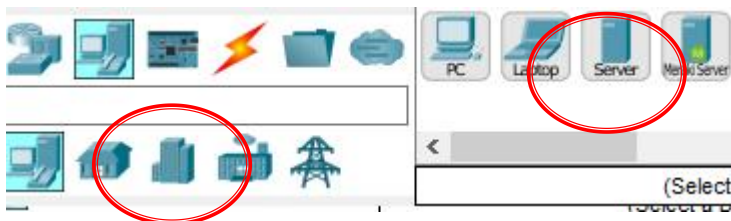
Pada percobaan 1, kita akan membuat topologi jaringan sebagai berikut:



Gambar 42 Topologi Peer to Peer membuat LAN sederhana

Langkah percobaan:

1. Drag 2 buah komputer dengan memilih pilihan device di pojok kanan bawah workspace



Gambar 43 Langkah percobaan modul 6 memilih device

2. Pilih kabel crossover lalu hubungkan kedua komputer
3. Konfigurasi alamat ip setiap PC dengan klik pada PC → tab desktop → IP Configuration
4. Isi IP address dan subnet mask
5. Lakukan pengujian dengan cara ping, pilih tab desktop → command promp

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<lms TTL=128
Reply from 192.168.1.2: bytes=32 time<lms TTL=128
Reply from 192.168.1.2: bytes=32 time<lms TTL=128
Reply from 192.168.1.2: bytes=32 time<lms TTL=128

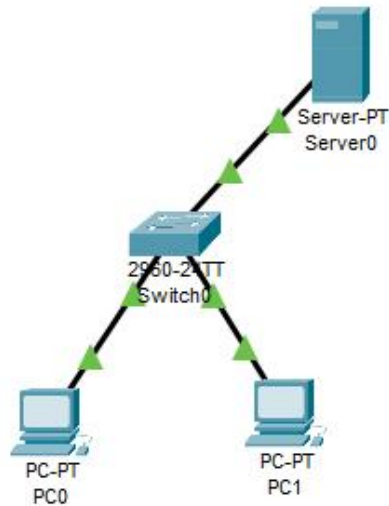
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Gambar 44 Percobaan modul 6 menguji jaringan P2P

### **Percobaan 2: Membuat jaringan LAN Peer to Peer yang terdiri dari beberapa komputer**

1. Drag and drop 5 buah PC ke workspace Packet Tracer
2. Drag and drop 1 buah switch 2960 ke workspace Packet Tracer
3. Set masing-masing komputer dengan IP sebagai berikut  
PC 1 > 10.10.10.1  
PC 1 > 10.10.10.2  
PC 1 > 10.10.10.3  
PC 1 > 10.10.10.4  
PC 1 > 10.10.10.5
4. Hubungkan semua komputer ke switch dengan menggunakan kabel straight-through
5. Lakukan pengujian pada PC

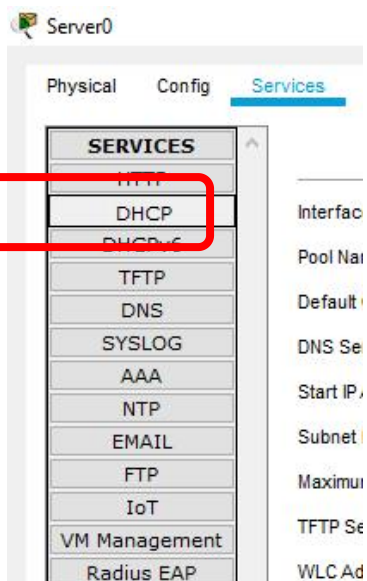
### Percobaan 3: Membuat DHCP Server



Gambar 45 Percobaan modul 6 topologi DHCP Server

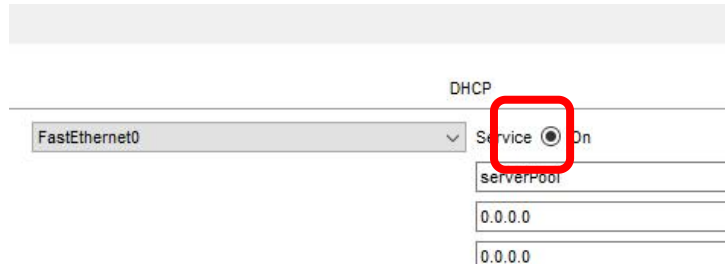
Langkah percobaan:

1. Drag and drop 2 buah PC, 1 buah switch, dan 1 buah server ke workspace Cisco Packet Tracer
2. Hubungkan setiap node dengan kabel straight through
3. Lakukan konfigurasi server dengan klik pada server
4. Pada Tab Service pilih DHCP



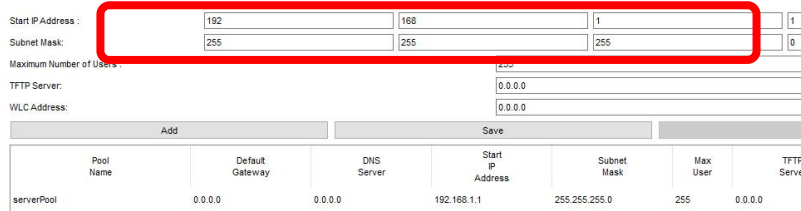
Gambar 46 Percobaan modul 6 memilih tab DHCP

5. Nyalakan service dengan memilih ON



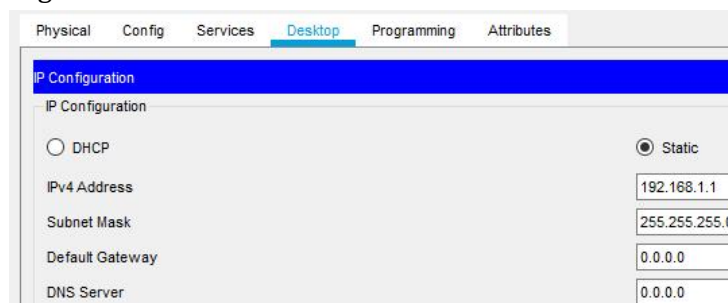
Gambar 47 Percobaan modul 6 menyalakan service DHCP

6. Isi Start IP address dengan alamat IP pertama dalam range DHCP. Misalnya kita gunakan Start IP address 192.168.1.1/24 dengan subnet mask 255.255.255.0 → lalu tekan save



Gambar 48 Percobaan modul 6 mengisi start IP

7. Pada Tab Desktop pilih IP configuration, isilah IP addressnya, misalnya IP untuk server kita pilih Start IP Address 192.168.1.1 dengan subnet mask 255.255.255.0



Gambar 49 Percobaan modul 6 mengkonfigurasi IP Address

8. Cek di masing-masing PC. Secara otomatis, setiap PC akan mendapatkan alamat IP dari Server DHCP.

```
C:\>ipconfig

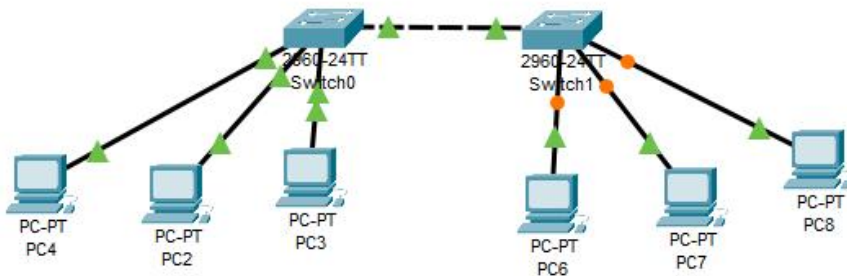
FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . . : FE80::201:96FF:FE5E:4A16
IPv6 Address . . . . . :
IPv4 Address. . . . . : 192.168.1.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
                                0.0.0.0
```

Gambar 50 Percobaan modul 6 cek IP PC

## D. Tugas

1. Buatlah sebuah topologi jaringan dengan alamat 192.168.1.0/26 seperti gambar berikut ini:



Gambar 51 Tugas modul 6

2. Pada sebuah gedung yang terdiri dari 10 komputer akan dibangun jaringan LAN dengan menggunakan IP dinamik dengan alamat IP 10.10.10.0/24. Buatlah rancangan desain jaringan tersebut



## MATERI 7 SIMULASI MEMBANGUN VLAN PADA PACKET TRACER

### A. Tujuan Praktik

- Agar mahasiswa mampu memahami konsep VLAN
- Agar mahasiswa dapat membangun VLAN pada Packet Tracer

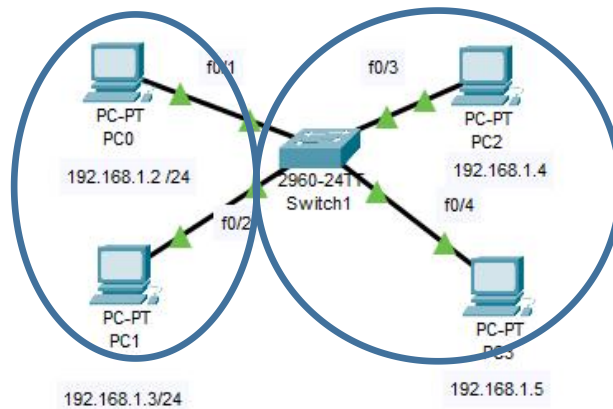
### B. Dasar Teori

Secara default, setiap komputer (host) yang terhubung ke switch yang sama akan memiliki broadcast domain yang sama atau dengan kata lain komputer-komputer tersebut akan berada pada segmen jaringan yang sama. Untuk memecah broadcast domain tersebut dibutuhkan perangkat router.

Alternatif lain yang lebih mudah dan murah adalah dengan menggunakan VLAN. VLAN dapat memecah broadcast domain meskipun tanpa menggunakan router. Komputer-komputer yang terhubung ke switch yang sama secara logic dapat dipisah-pisah menjadi VLAN-VLAN yang berbeda. Dengan memisah-misah komputer ke dalam VLAN, maka komputer-komputer yang berbeda VLAN meskipun berada pada switch yang sama akan dianggap segmen jaringan yang berbeda dan tidak dapat saling menerima broadcast karena komputer-komputer tersebut sudah berada pada broadcast domain yang berbeda.

### C. Kegiatan Praktik

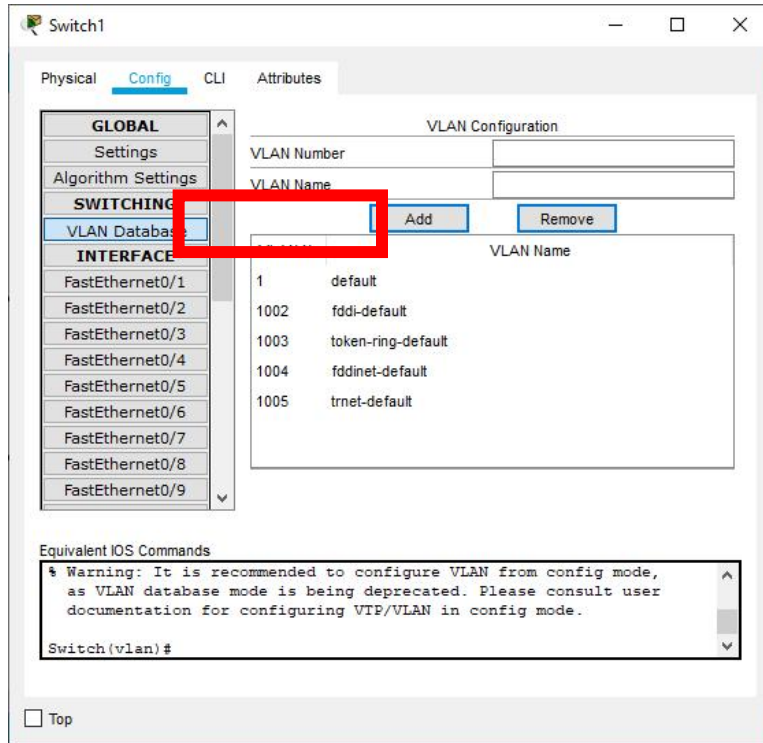
Pada praktik Simulasi Membangun Vlan, kita akan mensimulasikan bagaimana membangun VLAN dengan menggunakan Packet Tracer. Topologi jaringan yang akan dibangun adalah seperti gambar di bawah ini.



Gambar 52 praktik modul 7 topologi VLAN

Langkah praktik:

1. Buatlah topologi seperti pada gambar di atas
2. Untuk PC 0 – Hubungkan port PC 0 ke port FastEthernet0/1 di switch, untuk PC 1 – Hubungkan port PC 1 ke port FastEthernet0/2 di switch
3. Untuk PC 2 – Hubungkan port PC 2 ke port FastEthernet0/2 di switch, untuk PC 1 – Hubungkan port PC 3 ke port FastEthernet0/3 di switch
4. Vlan yang akan dibuat terdiri dari 2 Vlan, yaitu Vlan nomor 2 dengan nama Vlan ruang A dan Vlan nomor 3 dengan nama Vlan ruang B.
5. Beri alamat IP untuk setiap PC sesuai dengan gambar
6. Lakukan konfigurasi pada switch dengan klik switch → tab config → pilih vlan database



Gambar 53 Praktikum modul 7 memilih VLAN Database

7. Klik tab CLI ketikkan command di bawah ini.

- Membuat atau mendefinisikan VLAN nomor 2 dengan nama VLAN ruang A dan VLAN nomor 3 dengan nama VLAN ruang B

```
Switch(vlan)#vlan 2 name ruangA
```

```
VLAN 2 added:
```

```
Name: ruangA
```

```
Switch(vlan)#vlan 3 name ruangB
```

```
VLAN 3 added:
```

```
Name: ruangB
```

```
Switch(vlan)#exit|
```

- Memasukkan PC-PC ke masing-masing VLAN dimulai dari PC 0 dan PC 1 dimasukkan sebagai VLAN 2

```

Switch#conf t
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit

```

- Memasukkan PC 2 dan PC 3 dimasukkan sebagai VLAN 3

```

Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#exit
Switch#write

```

- Cek untuk melihat daftar VLAN yang tersedia

```
Switch>show Vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
2 ruangA	active	Fa0/1, Fa0/2
3 ruangB	active	Fa0/3, Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0

- Uji VLAN dengan melakukan ping antara PC 1 dan PC 3

#### **D. Tugas**

1. Apa mode dari port switch pada Kegiatan Praktik di atas?
2. Jelaskan alasan Anda!
3. Di sebuah gedung yang terdiri dari 20 PC akan dibuat 4 buah VLAN. VLAN dibuat untuk bidang perencanaan, bidang administrasi, bidang keuangan, dan bidang logistik. Bagaimana Anda akan mendesain jaringan internal pada gedung tersebut agar PC-PC yang terdapat di gedung tersebut dapat dikelompokkan berdasarkan bidangnya.



## **MATERI 8 MEMBANGUN JARINGAN LAN DENGAN BEBERAPA SEGMENT JARINGAN (ROUTING)**

### **A. Tujuan Praktik**

Tujuan dari praktik ini adalah

1. Agar mahasiswa dapat memahami bagaimana membangun jaringan LAN yang terdiri dari beberapa segmen jaringan

### **B. Dasar Teori**

Komputer dapat berkomunikasi dengan komputer lain yang memiliki broadcast domain yang sama. Artinya, komputer dapat saling berkomunikasi apabila komputer-komputer tersebut berada pada segmen jaringan yang sama. Komputer secara default tidak dapat berkomunikasi dengan komputer lain yang berbeda jaringan.

Akan tetapi, interkoneksi antar banyak komputer dibutuhkan agar komputer dapat berkomunikasi dengan komputer lain di seluruh dunia. Untuk mengatasi masalah tersebut, maka digunakan routing.

Routing adalah proses untuk menentukan jalur yang akan dilalui paket data sehingga paket data yang dikirim dari host sumber dapat diterima oleh host tujuan. Perangkat keras yang melakukan proses routing disebut dengan router.

Routing dibagi menjadi 2 jenis, yaitu

1. Routing statik
2. Routing dinamik

Routing statik dilakukan secara manual, artinya administrator jaringan harus mengkonfigurasi satu per satu perangkat jaringan untuk memasukkan atau menghapus informasi routing. Routing statik memiliki kelebihan antara lain jaringan menjadi lebih aman, sumber daya lebih sedikit karena tidak perlu menjalankan algoritma routing. Apabila terjadi perubahan pada topologi jaringan, maka administrator jaringan harus melakukan konfigurasi lagi secara manual. Routing statik cocok digunakan untuk jaringan berskala kecil hingga sedang.

Cara kerja routing statis dapat dibagi menjadi 3 bagian :

- Administrator jaringan yang mengkonfigurasi router

- Router melakukan routing berdasarkan informasi dalam tabel routing
- Routing statis digunakan untuk melewatkan paket data. Seorang administrator harus menggunakan perintah ip route secara manual untuk mengkonfigurasi router dengan routing statis.

Pada cisco perintah untuk mengkonfigurasi routing pada perangkat router adalah seperti command di bawah ini:

```
Router(config)# ip route [IP tujuan] [subnet mask] [IP
Next Hop]
```

Keterangan :

- Ip route : perintah untuk membuat static routing
- Destination : network tujuan yang hendak ditambahkan
- Subnet Mask : subnet mask yang digunakan dalam network
- Next hop address : alamat dari router yang menghubungkan router dan router atau router tujuan

Contoh command static routing:

```
Router(config)#ip route 172.110.0.0 255.255.0.0
10.10.10.0
```

Command di atas artinya proses routing menuju alamat jaringan 172.110.0.0 dengan subnet mask 255.255.0.0 yang mana alamat IP hope selanjutnya adalah 10.10.10.0.

Sedangkan routing dinamik berkerja menggunakan protokol routing dan memiliki algoritma dalam menentukan jalur pengiriman paket data. Routing dinamik membutuhkan sumber daya yang lebih besar dan terkadang dapat membebani kinerja jaringan.

## C. Kegiatan Praktik

### Percobaan 1:

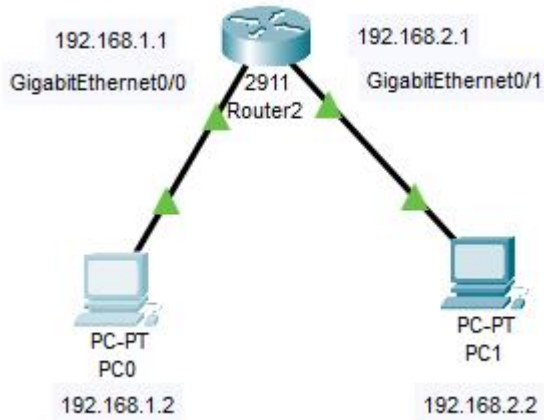
Pada praktik ini, kita akan menerapkan proses routing pada sebuah jaringan sederhana. Perangkat yang dibutuhkan adalah sebagai berikut:

1. Satu buah router
2. Dua buah PC

Langkah praktik:



1. Buatlah topologi seperti gambar di bawah ini



Gambar 54 Praktik modul 8 topologi LAN 1 router

2. Beri alamat IP pada PC 0 dan PC 1 dengan ketentuan sebagai berikut

- PC 0

Tabel 21 Praktik modul 8 konfigurasi PC 0

Alamat IP	192.168.1.2
Subnet Mask	255.255.255.0
Gateway	192.168.1.1

- PC 1

Tabel 22 Praktik modul 8 konfigurasi PC 1

Alamat IP	192.168.2.2
Subnet Mask	255.255.255.0
Gateway	192.168.2.1

3. Port router yang terhubung ke PC 0 adalah port GigabitEthernet0/0 dengan alamat IP 192.168.1.1
4. Port Router yang terhubung ke PC 1 adalah port GigabitEtherneer 0/1 dengan alamat IP 192.168.2.1
5. Lakukan konfigurasi pada router dengan klik router lalu pilih tab CLI
6. Lalu ketikkan command untuk memberikan alamat IP pada interface pertama dari Router

```

Router>enable
Router#conf t
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#ex

```

7. Ketikkan command untuk memberikan alamat IP pada interface kedua dari Router

```

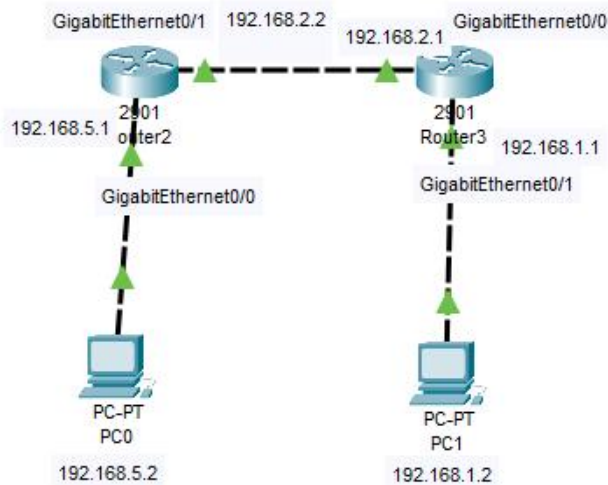
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ex
Router#write

```

8. Cek koneksi antara PC 0 dengan interface GigabitEthernet0/0, PC 1 dengan interface GigabitEthernet0/1, dan PC 1

### **Percobaan 2: Jaringan dengan lebih dari 1 buah router**

Buatlah desain jaringan dengan topologi sebagai berikut:



Gambar 55 Praktikum modul 8 topologi LAN 2 router

Perangkat yang dibutuhkan antara lain:

- a. Dua buah PC
- b. Dua buah Router

- c. PC 0 dengan alamat IP 192.168.5.2/24 terhubung ke interface GigabitEthernet0/0 router 1 dengan alamat IP 192.168.5.1/24
- d. PC 1 dengan alamat IP 192.168.1.2/24 terhubung ke interface GigabitEthernet0/1 router 2 dengan alamat IP 192.168.1.1/24
- e. Kedua router terhubung melalui interface GigabitEthernet0/1 pada router 1 dengan alamat IP 192.168.2.2/24 ke interface GigabitEthernet0/0 pada router 2 dengan alamat IP 192.168.2.1

Langkah Percobaan:

- a. Atur alamat IP untuk setiap PC dengan ketentuan seperti dijelaskan di atas
- b. Memberi alamat IP pada setiap interface router 1 dengan perintah:  
Pada interface GigabitEthernet0/0 yang terhubung ke PC 0

```
Router>enable
Router#conf t
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Pada interface GigabitEthernet0/1 yang terhubung ke router 2

```
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

- c. Memberi alamat IP pada setiap interface router 2 dengan perintah:  
Pada interface GigabitEthernet0/1 yang terhubung ke PC 1

```
Router>enable
Router#conf t
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#ex
```

Pada interface GigabitEthernet0/0 yang terhubung ke Router 1

```

Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config)#ex
Router#write

```

d. Cek koneksi pada PC 1, isilah tabel di bawah ini:

	PC 1
Router 2 GigabitEthernet0/1	.....
Router 2 GigabitEthernet0/0	.....
Router 1 GigabitEthernet0/1	.....
Router 1 GigabitEthernet0/0	.....
PC 0	.....

e. Apa yang dapat disimpulkan dari langkah percobaan d

f. Buatlah routing pada setiap router

Pada Router 1:

```

Router#conf t
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
Router(config)#exit
Router#write

```

Pada Router 2:

```

Router#conf t
Router(config)#ip route 192.168.5.0 255.255.255.0 192.168.2.2
Router(config)#ex
Router#write

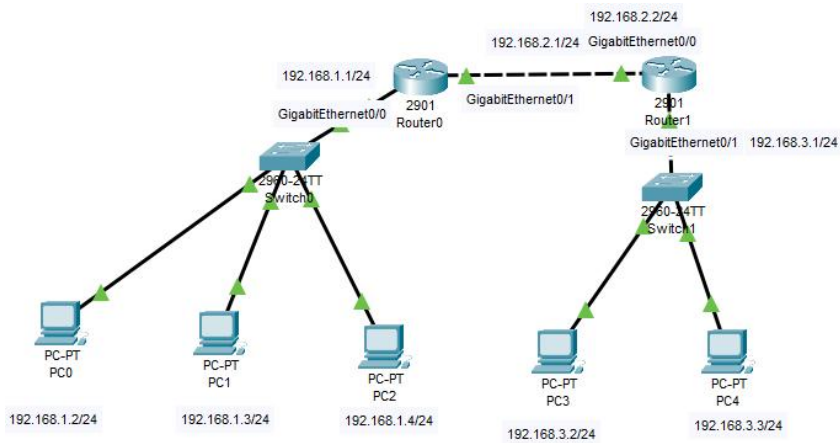
```

g. Cek koneksi pada PC 1, isilah tabel di bawah ini:

	PC 1
Router 2 GigabitEthernet0/1	.....
Router 2 GigabitEthernet0/0	.....
Router 1 GigabitEthernet0/1	.....
Router 1 GigabitEthernet0/0	.....
PC 0	.....

## D. Tugas

- Perintah untuk mengaktifkan router \_\_\_\_\_
- Perintah untuk mengaktifkan interface router \_\_\_\_\_
- Apa tujuan dari perintah no shutdown \_\_\_\_\_
- Mengapa pada PC 0 dan PC1 harus mengisi IP Gateway?
- Apa kegunaan dari Gateway?
- Pada sebuah sekolah terdapat 2 buah lantai, yaitu lantai 1 dan lantai 2. Lantai 1 terdiri dari 10 PC dan lantai 2 terdiri dari 10 PC. Kedua lantai tersebut berbeda segmen jaringan, di mana lantai 1 memiliki alamat jaringan 10.10.10.0/24 dan lantai 2 memiliki alamat jaringan 192.168.10.0/24. Buatlah desain jaringan agar komputer pada kedua lantai dapat berkomunikasi!
- Buatlah desain jaringan dengan topologi berikut ini:





## MATERI 9 MEMBANGUN JARINGAN LAN WIRELESS

### A. Tujuan Praktik

Tujuan dari praktik ini adalah

- Agar mahasiswa dapat memahami bagaimana membangun jaringan LAN tanpa kabel

### B. Dasar Teori

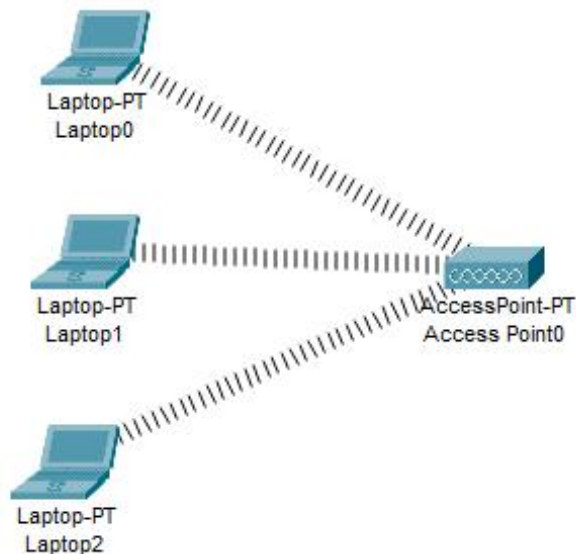
Jaringan lokal Lan terdiri dari 2 jenis, yaitu

1. Jaringan LAN dengan kabel
2. Jaringan LAN tanpa kabel

Untuk membangun jaringan LAN tanpa kabel, kita membutuhkan perangkat keras wireless, seperti Access Point (AP). Biasanya jaringan LAN tanpa kabel menggunakan alamat IP dinamik sehingga kita membutuhkan server DHCP yang menyediakan layanan IP dinamik.

### C. Kegiatan Praktik

Topologi jaringan tanpa kabel pada modul 9 adalah seperti yang tampak pada Gambar 2.54.



Gambar 56 Praktik modul 9 topologi jaringan WLAN

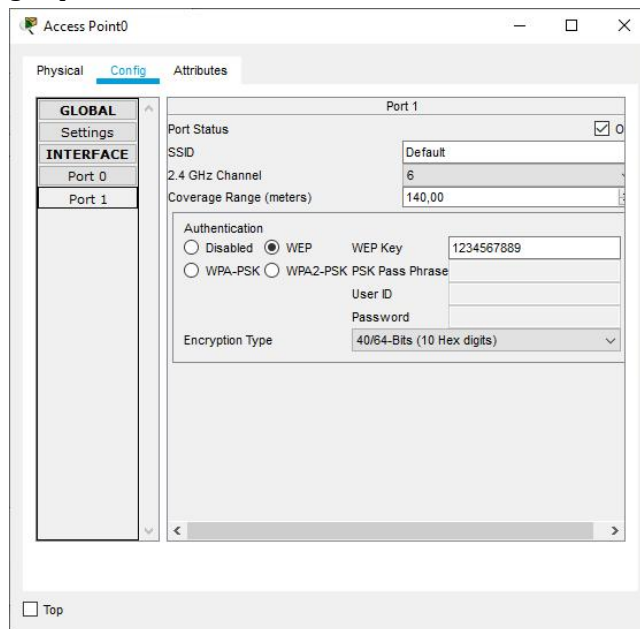
### Langkah percobaan:

1. Sediakan 3 buah laptop dan 1 buah Access Point (AP-PT)
2. Mengubah interface jaringan dari Ethernet ke interface wireless dengan cara klik pada laptop → tab Physical → interface wireless (misalnya WPC300N)
3. Turn off laptop, drag interface Ethernet keluar dari laptop, lalu ganti dengan interface wireless (WPC300N)



Gambar 57 Langkah percobaan modul 9

4. Setelah itu, nyalakan laptop
5. Selanjutnya lakukan konfigurasi pada AP dengan cara klik AP → tab config → port1



Gambar 58 Praktik modul 9 konfigurasi Port 1 AP

6. Isi otentikasi dengan memasukkan kata sandi yang terdiri dari minimal 10 digit hexa
7. Close AP



8. Lalu konfigurasi setiap PC dengan cara klik laptop → desktop → PC Wireless → tab connect → pilih wireless network name → tekan tombol connect → masukkan kata sandi
9. Jika berhasil, maka laptop dan switch akan tampak terhubung oleh sinyal
10. Selanjutnya beri alamat IP untuk semua PC yang ada dengan IP statik.
11. Cek koneksi dengan melakukan ping antar PC
12. Cek di masing-masing PC. Secara otomatis, setiap PC akan mendapatkan alamat IP dari Server DHCP.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:96FF:FE5E:4A16
    IPv6 Address . . . . . : ::
    IPv4 Address. . . . . : 192.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : ::
                                0.0.0.0
```

Gambar 59 Praktik modul 9 cek IP dari Server DHCP

#### D. Tugas

1. Sebuah kantor terdiri dari 2 buah PC yang terhubung melalui switch. Akan tetapi, di kantor tersebut terdapat beberapa karyawan yang membawa laptop. Bagaimana Anda mendesain jaringan LAN agar seluruh PC dan laptop di kantor tersebut dapat saling terhubung melalui alamat IP yang statik?
2. Dari soal nomor 1, bagaimana mendesain jaringan LAN tersebut agar seluruh laptop mendapatkan IP dinamik, tetapi seluruh PC masih menggunakan kabel sebagai konektornya? Buatlah desain jaringannya!



# MATERI 10 MENGHUBUNGKAN LAN KE INTERNET PADA CISCO PACKET TRACER

## A. Tujuan Praktik

Tujuan dari praktik ini adalah

- Agar mahasiswa dapat memahami bagaimana membangun jaringan LAN yang dapat terhubung ke internet dengan menggunakan software simulasi Cisco Packet Tracer

## B. Dasar Teori

Untuk menghubungkan jaringan lokal ke internet, maka dibutuhkan perangkat keras router yang terhubung ke modem dan ke ISP. Router berperan sebagai gateway yang menghubungkan 2 segmen jaringan yang berbeda. Pada interface yang menghadap jaringan lokal, maka interface tersebut akan mendapatkan alamat IP sesuai segmen jaringan lokal. Sedangkan, pada interface yang menghadap ke jaringan global, maka perlu diberi IP sesuai dengan segmen jaringan global.

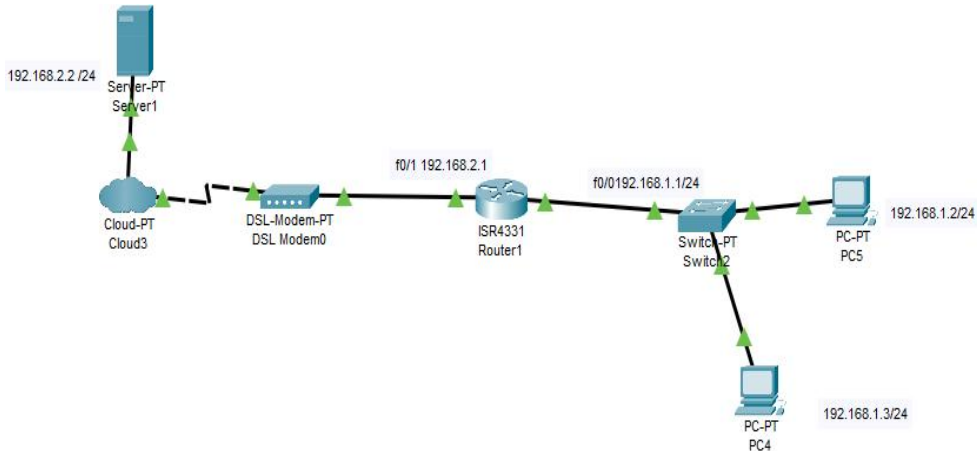
Pada praktik ini, kita masih belum menerapkan Network Address Translation sehingga dalam mengkoneksikan 2 host pada jaringan lokal dan jaringan global masih menggunakan alamat IP.

Yang perlu diingat adalah saat menghubungkan router ke jaringan global, dibutuhkan perangkat keras modem, yaitu sebuah perangkat keras yang mengubah sinyal digital menjadi sinyal analog dan sebaliknya.

Tidak seperti pada GNS3 yang dapat langsung menggunakan share internet dengan real komputer, maka pada Packet Tracer kita perlu membuat server yang terhubung ke node cloud pada Packet Tracer. Server ini akan bertindak sebagai host di jaringan eksternal yang akan diakses dari jaringan lokal.

## C. Kegiatan Praktik

Pada praktik ini, kita akan membuat topologi jaringan seperti yang ditampilkan pada gambar ini.



Gambar 60 Topologi LAN terhubung internet

Gambar 2.58 menggambarkan sebuah jaringan lokal yang terdiri dari :

1. Dua buah PC
2. Satu buah switch
3. Satu buah router
4. Satu buah modem DSL
5. Satu buah node cloud yang menandai jaringan eksternal
6. Satu buah server eksternal yang akan diakses dari jaringan lokal.

Pada dunia nyata, server tersebut dapat berupa server-server yang dapat diakses melalui internet, seperti web server Facebook, Amazone, Google, dll

Adapun alamat IP yang akan ditetapkan pada interface di perangkat keras jaringan adalah sebagai berikut:

Tabel 23 praktik modul 10 alamat IP perangkat keras

Nama Perangkat Keras	Alamat IP
PC 1	192.168.1.2/24
PC 2	192.168.1.3/24
Router (GigabitEthernet0/0)	192.168.1.1
Router (GigabitEthernet0/1)	192.168.2.1
Server	192.168.2.2

Jenis kabel yang digunakan setiap perangkat keras juga berbeda. Adapun jenis kabel yang digunakan adalah sebagai berikut:

Tabel 24 praktik modul 10 jenis kabel yang digunakan

Node	Jenis Kabel
PC 1 - Switch	Straight-through
PC 2 - Switch	Straight-through
Switch- router	Straight-through
Router - Modem DSL	Straight-through
Modem DSL - node cloud	Kabel Telepon
Node Cloud - Server	Straight-through

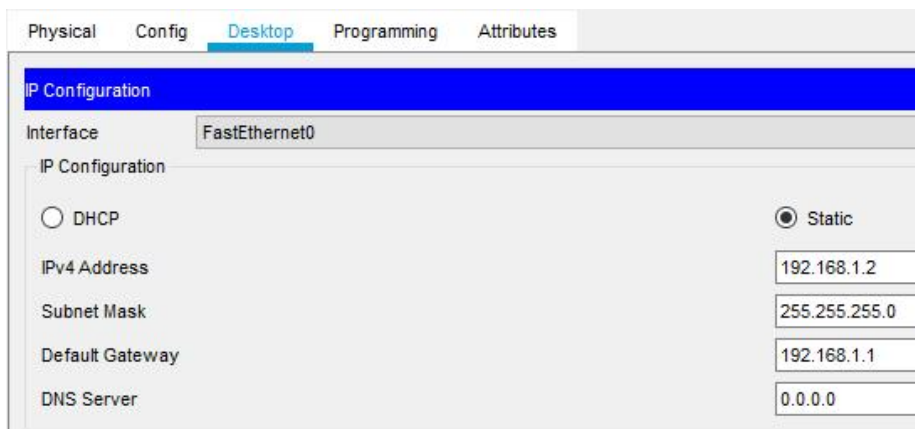
Kita perlu mengkonfigurasi jenis koneksi pada node cloud dengan klik node cloud → tab config → DSL → Pada dropdown box pilih port tempat kita menghubungkan kabel (misalnya port modem 4 atau modem 4) lalu pilih juga dihubungkan ke port mana pada cloud, misalnya pada port Ethernet6.



Gambar 61 praktik modul 10 mengkonfigurasi DSL

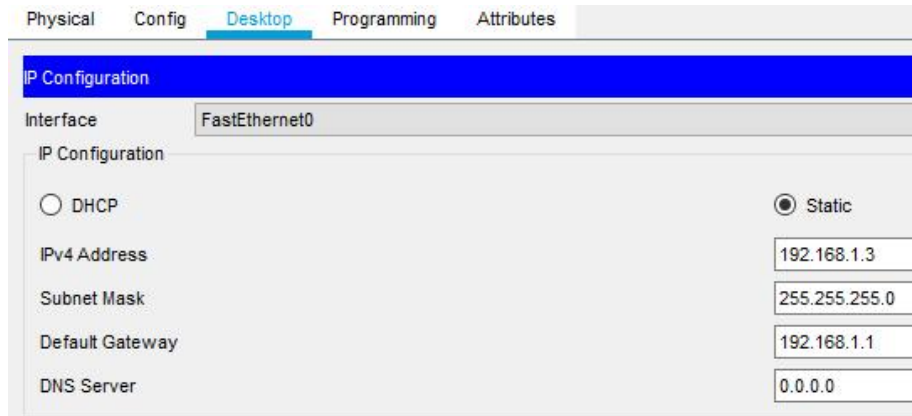
Langkah selanjutnya adalah melakukan konfigurasi pada perangkat keras.

a. Pada PC 1



Gambar 62 Praktik modul 10 konfigurasi PC 1

b. Pada PC 2



Gambar 63 Praktik modul 10 konfigurasi PC 2

c. Pada Router

Konfigurasi pada GigabitEthernet0/0/0 yang menuju jaringan lokal



Gambar 64 Konfigurasi GigabitEthernet0/0/0

Konfigurasi pada GigabitEthernet0/0/1 yang menuju jaringan global



Gambar 65 Konfigurasi GigabitEthernet0/0/1

Dengan command

Router>enable

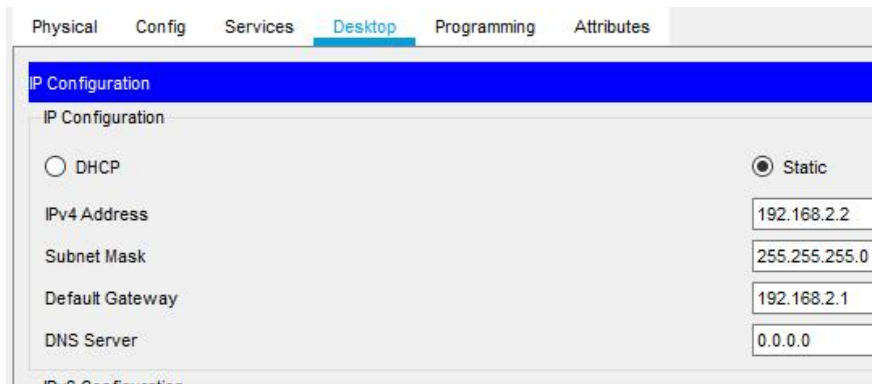
Router#configure terminal

```

Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.1.1
255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 192.168.2.1
255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

```

d. Pada Server



Gambar 66 praktik modul 10 konfigurasi server

Setelah melakukan konfigurasi pada masing-masing perangkat, selanjutnya adalah menguji koneksi dari PC ke server yang dituju, misalnya dari PC dengan IP 192.168.1.2 ke server 192.168.2.2

```

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=63ms TTL=127
Reply from 192.168.2.2: bytes=32 time=61ms TTL=127
Reply from 192.168.2.2: bytes=32 time=61ms TTL=127
Reply from 192.168.2.2: bytes=32 time=62ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 63ms, Average = 61ms

```

Gambar 67 praktik modul 10 menguji koneksi

## D. Tugas

Buatlah desain jaringan untuk topologi di bawah ini!

Kebutuhan perangkat keras:

- Satu buah modem DSL, router, node cloud dan server
- Dua buah switch
- Enam buah PC

Kebutuhan alamat IP terdapat pada Tabel 25.

Tabel 25 Tugas modul 10 kebutuhan alamat IP

Nama Perangkat Keras	Alamat IP
PC 1 (Jaringan 1)	192.168.1.2/24
PC 2 (Jaringan 1)	192.168.1.3/24
PC 3 (Jaringan 1)	192.168.1.3/24
PC 4 (Jaringan 2)	192.168.2.2/24
PC 5 (Jaringan 2)	192.168.2.3/24
PC 6 (Jaringan 2)	192.168.2.4/24
Router (GigabitEthernet0/0) ke Jaringan 1	192.168.1.1
Router (GigabitEthernet0/1) ke jaringan global	192.168.4.1
Router (GigabitEthernet0/2) ke jaringan 2	192.168.2.1
Server	192.168.4.2



# MATERI 11 NETWORK ADDRESS TRANSLATION

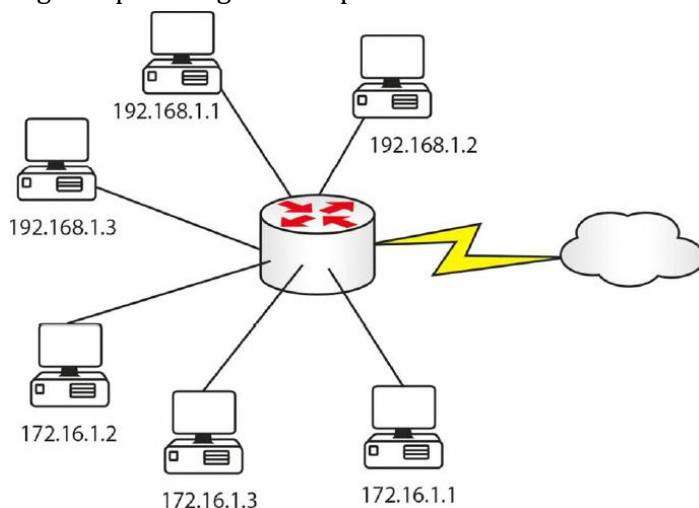
## A. Tujuan Praktik

Tujuan dari praktik ini adalah

- Agar mahasiswa mampu memahami konsep NAT
- Agar mahasiswa dapat mengimplementasikan NAT pada LAN

## B. Dasar Teori

NAT adalah sebuah sistem untuk menggabungkan beberapa komputer ke dalam jaringan komputer menggunakan 1 alamat IP saja [6]. Hal ini menyebabkan seluruh komputer di dalam 1 NAT akan memiliki 1 alamat IP saja. Dengan kata lain sebuah komputer yang memiliki alamat IP pada jaringan lokal akan terlebih dulu diterjemahkan oleh NAT agar dapat mengakses IP publik.



Gambar 68 Network Address Translation [6]

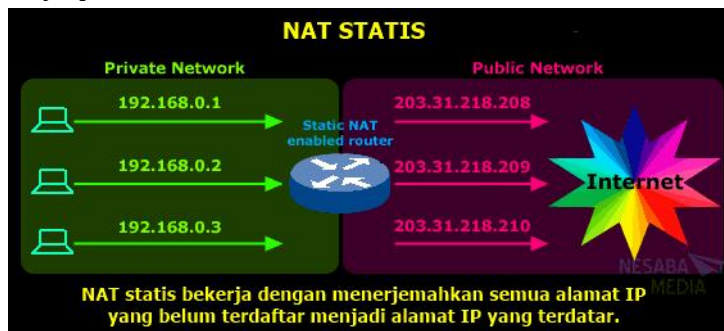
Dari gambar di atas, NAT membutuhkan inside address dan outside address. Inside address untuk mendefinisikan alamat-alamat jaringan lokal, sementara outside address mendefinisikan alamat ke jaringan internet. Saat mengkonfigurasi NAT, kita harus memberi tahu user interface mana yang merupakan inside NAT dan outside NAT.

Beberapa istilah pada NAT antara lain:

1. The NAT inside interface → interface yang handle komputer di jaringan lokal
2. Inside local address → IP address pada komputer-komputer yang terdapat pada jaringan lokal
3. Inside global address → IP internal pada jaringan lokal yang terlihat dari jaringan global. Setelah alamat IP inside diterjemahkan, akan muncul sebagai alamat global ke Internet atau jaringan atau host eksternal lainnya.
4. The NAT outside interface → interface di luar jaringan lokal (yang tidak dikontrol oleh organisasi, yang terhubung ke internet atau jaringan eksternal)
5. Outside local address → alamat IP host pada jaringan eksternal yang terlihat di jaringan lokal
6. Outside global address → alamat yang digunakan pada internet

Jenis-jenis NAT antara lain:

1. NAT Statis : Bekerja dengan menerjemahkan satu buah alamat IP lokal menjadi 1 buah IP Public. NAT Statis banyak digunakan untuk komputer yang ingin dapat diakses dari luar/ internet, contoh email dan FTP. Pada NAT Statis, 1 komputer pada jaringan lokal didaftarkan akan mendapatkan 1 IP terdaftar. Hal ini menyebabkan terjadinya pemborosan alamat IP.

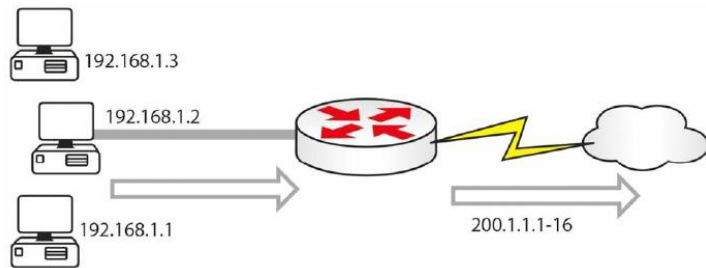


Gambar 69 NAT Statis

Sumber: <https://www.nesabamedia.com/>

2. NAT Dinamis : bekerja dengan cara mendaftarkan beberapa computer ke dalam satu buah kelompok alamat IP yang terdaftar yang sama. Oleh karena itu, akan ada beberapa computer yang

memiliki alamat IP yang sama dengan computer yang lain yang terdaftar.



Gambar 70 NAT Dinamis [6]

Perhatikan gambar di atas, komputer dengan IP address lokal dapat menggunakan kelompok IP Publik dengan range dari 200.1.1.1 sampai denan 200.1.1.16. IP publik ini akan berubah-ubah karena bersifat dinamis sehingga setiap komputer di jaringan lokal juga mendapatkan IP publik yang dinamis. IP Dinamis memiliki rentang waktu tertentu. Jika sudah melewati batas waktu, maka alamat IP akan dihapus dan dapat digunakan oleh komputer yang lain.

Kelemahan : Jika IP publik sudah terpakai semua, maka komputer lain tidak bisa menggunakan alamat IP lagi sehingga harus menunggu komputer lain berhenti menggunakan IP tersebut.

3. Overloading NAT atau Port Address Translation adalah metode NAT yang menerjemahkan banyak IP address lokal ke satu IP Public

### Mengkonfigurasi NAT

Untuk melihat konfigurasi NAT yang ada pada router Cisco

```
R1#show ip nat translations
```

Hasil yang muncul adalah

```
Pro Inside global Inside local Outside local
Outside global
icmp 150.1.1.4:4 10.5.5.1:4 200.1.1.1:4 200.1.1.1:4
icmp 150.1.1.3:1 10.5.5.2:1 200.1.1.1:1 200.1.1.1:1
tcp 150.1.1.5:159 10.5.5.3:159 200.1.1.1:23
200.1.1.1:23
```

Untuk melakukan konfigurasi NAT static yang ada pada router Cisco menggunakan commad berikut.

```
Router(config)#interface f0/0
Router(config-if)#ip          address          192.168.1.1
255.255.255.0
Router(config-if)#ip nat inside
Router(config)#interface f0/1
Router(config-if)#ip          address          192.168.2.1
255.255.255.0
Router(config-if)#ip nat inside
Router(config)#interface s0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip  nat    inside    source    static
192.168.1.1 200.1.1.1
Router(config)#ip  nat    inside    source    static
192.168.2.1 200.1.1.2
```

Untuk melakukan konfigurasi NAT dinamis yang ada pada router Cisco menggunakan commad berikut.

```
Router(config)#interface f0/0
Router(config-if)#ip nat inside
Router(config)#interface s0/1
Router(config-if)#ip nat outside
Router(config)#ip  nat  pool  poolname  200.1.1.1
200.1.1.16 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool
poolname
Router(config)#access-list 1 permit 192.168.1.0
0.0.0.255
```

Untuk melakukan konfigurasi NAT PAT yang ada pada router cisco

```
Router(config)#interface f0/0
Router(config-if)#ip nat inside
Router(config)#interface s0/1
Router(config-if)#ip nat outside
Router(config)#ip  nat  pool  poolname  200.1.1.1
200.1.1.1 netmask 255.255.255.0
```

```

Router(config)#ip nat inside source list 1 pool
poolname overload
Router(config)#access-list 1 permit 192.168.1.0
0.0.0.255

```

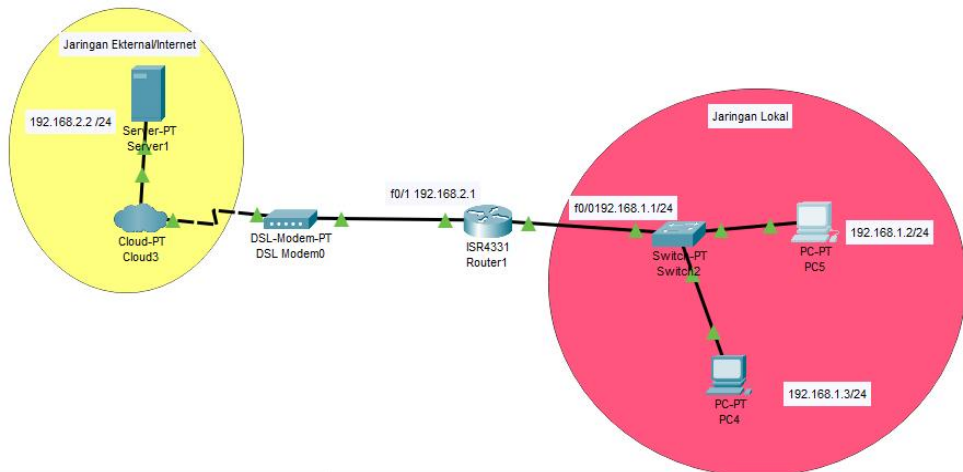
### C. Kegiatan Praktik

Pada praktik ini, mahasiswa akan melakukan percobaan bagaimana NAT diimplementasikan pada router.

#### Percobaan 1 : NAT Statik

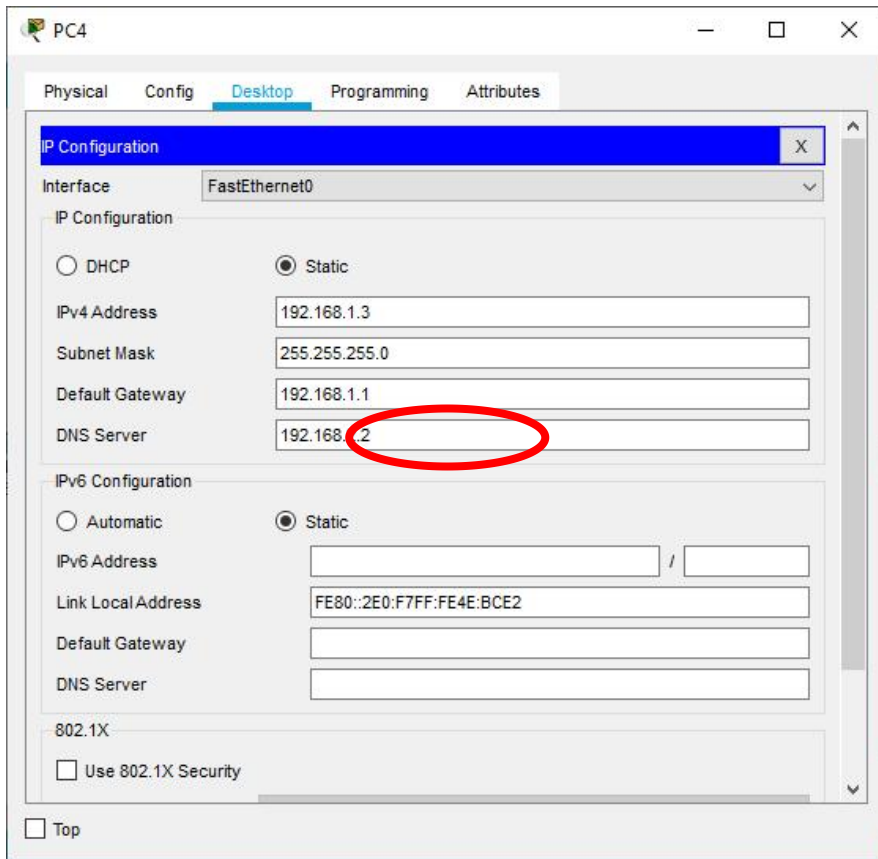
Langkah praktik:

- Buatlah topologi jaringan seperti gambar di bawah ini dengan menggunakan topologi jaringan yang sudah di buat pada praktik menghubungkan LAN ke Internet sebelumnya.



Gambar 71 Tugas membuat topologi dengan NAT

- Untuk setiap PC, yaitu PC 1 dan PC 2, tambahkan IP DNS menggunakan alamat IP server di internet. Pada topologi di atas, server di internet memiliki alamat IP 192.168.2.2 sehingga konfigurasi DNS di PC adalah seperti gambar di bawah ini.



Gambar 72 Konfigurasi DNS di PC

- Karena pada praktik sebelumnya kita sudah mengkonfigurasi alamat IP di router sehingga selanjutnya kita hanya perlu mengkonfigurasi NAT Static di router dengan masuk ke CLI router, lalu mengetikkan perintah berikut ini.

```

Router#conf t
Router(config)#ip nat inside source static 192.168.1.3
192.168.2.3
Router(config)#ip nat inside source static 192.168.1.2
192.168.2.4
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip nat outside
Router(config-if)#ex
Router(config)#ex
Router#write

```

Perhatikan perintah pada baris ke dua! Perintah pada baris kedua artinya memberikan IP Public 192.168.2.3 untuk IP lokal 192.168.1.3. Perhatikan perintah baris ketiga! Perintah baris ketiga artinya memberikan ip public 192.168.2.4 untuk IP lokal 192.168.1.2 Dari contoh di atas, kita dapat memahami bahwa setiap PC di komputer jaringan lokal akan diberikan IP Publik satu persatu.

- Cek apakah konfigurasi NAT telah berhasil dengan mengetikkan perintah show ip nat translations

```

Router#show ip nat translations
Pro  Inside global    Inside local      Outside local     Outside global
---  192.168.2.3      192.168.1.3     ---              ---
---  192.168.2.4      192.168.1.2     ---              ---

```

Dari gambar dapat dilihat bahwa IP inside local berisi tentang alamat IP PC di jaringan lokal, sedangkan inside global adalah alamat IP PC jaringan lokal yang terlihat dari jaringan global. Sedangkan IP Outside local dan Ouside Global belum muncul karena server di internet belum melakukan pengiriman data ke jaringan lokal kita.

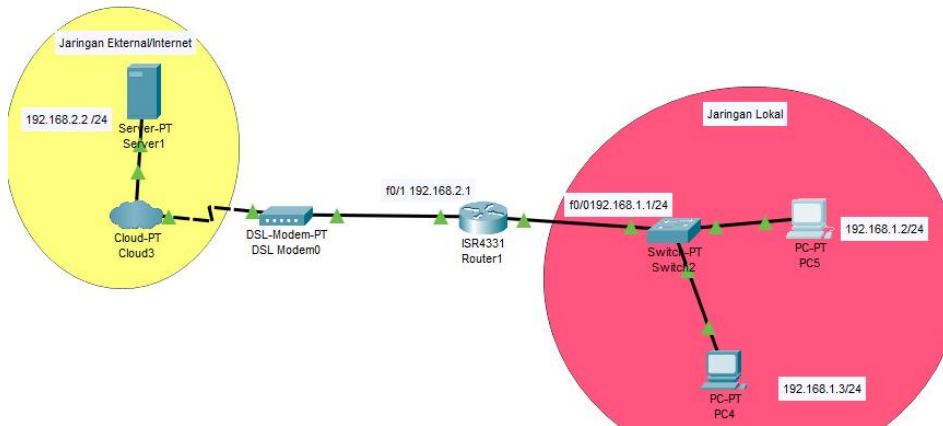
- Untuk melihat outside local dan outside global, lakukan uji ping dari PC lokal ke server di internet sehingga Server di internet memberikan reply ke jaringan lokal kita

- Lalu cek lagi NAT dengan mengetikkan perintah show ip nat translations

```
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 192.168.2.4:1      192.168.1.2:1    192.168.2.2:1    192.168.2.2:1
icmp 192.168.2.4:2      192.168.1.2:2    192.168.2.2:2    192.168.2.2:2
icmp 192.168.2.4:3      192.168.1.2:3    192.168.2.2:3    192.168.2.2:3
icmp 192.168.2.4:4      192.168.1.2:4    192.168.2.2:4    192.168.2.2:4
---  192.168.2.3        192.168.1.3      ---               ---
---  192.168.2.4        192.168.1.2      ---               ---
```

**Percobaan 2 : PAT**

- Buatlah topologi jaringan seperti gambar di bawah ini dengan menggunakan topologi jaringan yang sudah di buat pada praktik menghubungkan LAN ke Internet sebelumnya.



Gambar 73 Membuat topologi dengan PAT

- Buatlah topologi jaringan seperti gambar di bawah ini dengan menggunakan topologi jaringan yang sudah di buat pada praktik menghubungkan LAN ke Internet sebelumnya.
- Karena pada praktik sebelumnya kita sudah mengkonfigurasi alamat IP di router sehingga selanjutnya kita hanya perlu mengkonfigurasi NAT PAT di router dengan masuk ke CLI router, lalu mengetikkan perintah berikut ini.



```

Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip nat outside
Router(config-if)#ex

```

Perhatikan perintah di atas! Kita mengkonfigurasi interface GigabitEthernet 0/0 yang menghadap ke jaringan lokal sebagai IP NAT inside. Sedangkan interface GigabitEthernet0/1, kita tetapkan sebagai ip nat outside karena berhadapan langsung dengan jaringan global.

```

Router(config)#ip nat pool publik1 192.168.2.5 192.168.2.5
netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool publik1
overload
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ex
Router#write

```

Perintah di atas artinya kita memberi IP Publik / inside global 192.168.2.5 untuk seluruh alamat IP yang ada di jaringan lokal. Artinya seluruh komputer pada jaringan lokal mendapatkan IP 192.168.2.5 untuk mengakses jaringan global/ terhubung ke internet.

- Cek PC 1 dan PC 2 untuk melakukan ping ke server global
- Setelah itu jalankan perintah show ip nat translations pada router untuk melihat NAT yang telah dibuat.

### Cek PC 1

```

Router(config)#do sh ip nat translations

```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	192.168.2.5:1	192.168.1.2:1	192.168.2.2:1	192.168.2.2:1
icmp	192.168.2.5:2	192.168.1.2:2	192.168.2.2:2	192.168.2.2:2
icmp	192.168.2.5:3	192.168.1.2:3	192.168.2.2:3	192.168.2.2:3
icmp	192.168.2.5:4	192.168.1.2:4	192.168.2.2:4	192.168.2.2:4

Perhatikan perintah di atas! PC 1 dengan alamat IP (inside local) 192.168.1.2 akan terlihat dari jaringan global memiliki IP 192.168.2.5. Hal ini sesuai dengan konfigurasi NAT PAT yang telah kita lakukan sebelumnya

### Cek PC 2

```
Router(config)#do sh ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 192.168.2.5:5       192.168.1.3:5    192.168.2.2:5    192.168.2.2:5
icmp 192.168.2.5:6       192.168.1.3:6    192.168.2.2:6    192.168.2.2:6
icmp 192.168.2.5:7       192.168.1.3:7    192.168.2.2:7    192.168.2.2:7
icmp 192.168.2.5:8       192.168.1.3:8    192.168.2.2:8    192.168.2.2:8
```

Perhatikan perintah di atas! PC 2 dengan alamat IP (inside local) 192.168.1.3 juga terlihat dari jaringan global memiliki IP 192.168.2.5. Hal ini disebabkan karena metode NAT yang digunakan adalah metode overload sehingga seluruh alamat IP pada jaringan lokal akan dipetakan dengan alamat IP publik yang sama.

## D. Tugas

1. Mengapa alamat inside global menggunakan alamat 192.168.2.0/24?
2. Apa yang akan terjadi jika kita tidak membuat NAT pada jaringan lokal?
3. Dari dasar teori dan Kegiatan Praktik di atas, buatlah NAT dengan metode dinamik menggunakan topologi di atas dengan rentang alamat IP inside global 192.168.2.10 sampai dengan 192.168.2.20.
4. Dari soal nomor 3, apa kesimpulan yang dapat diambil?

## **DAFTAR PUSTAKA**

---

---

- [1] Wikipedia, "Wikipedia," Wikipedia, 14 Juni 2019. [Online]. Available: [https://id.wikipedia.org/wiki/Packet\\_Tracer](https://id.wikipedia.org/wiki/Packet_Tracer). [Diakses 1 2 2021].
- [2] Wikipedia, "Wikipedia," 20 11 2019. [Online]. Available: <https://id.wikipedia.org/wiki/Wireshark>. [Diakses 1 2 2021].
- [3] B. A. Forrouzan, Data Communications and Networking Fourth Edition, New York: McGraw-Hill, 2007.
- [4] W. Web, "Wireshark," Wireshark , [Online]. Available: <https://www.wireshark.org/>. [Diakses 2 2 2021].
- [5] U. Lamping, R. Sharpe dan E. Warnicke, "Wireshark User's Guide v1.11.4-rc1-54-g9496733 for Wireshark 1.11," 2013.
- [6] P. Browning, F. Tafa, D. Gheorghe dan D. Barinic, Cisco CCNA in 60 Days, Milton Keynes: Reality Press Ltd., 2014.



## GLOSARIUM

---

---

Collision	Tabrakan sinyal yang terjadi pada jaringan ethernet
Digital	Sinyal data yang bersifat diskrit
Fiber Optic	Kabel yang terbuat dari serat optik
Nirkabel	Tanpa kabel
PC	Komputer personal
PDU	<i>Protokol Data Unit</i> yang merupakan data pada tiap layer
Router	Perangkat keras jaringan yang berguna untuk menghubungkan komputer-komputer segmen jaringan yang berbeda
Server	Komputer yang menyediakan layanan tertentu untuk komputer yang lain
Sinyal Analog	Sinyal data yang berbentuk gelombang kontinyu
Switch	Perangkat keras jaringan yang berguna untuk menghubungkan komputer-komputer dalam 1 segmen jaringan
Topologi	Cara komponen-komponen jaringan saling terhubung
<i>Troubleshooting</i>	Pendekatan sistematis guna mencari penyelesaian atas masalah yang muncul pada perangkat keras, perangkat lunak, dan sistem komputer



## **BIOGRAFI PENULIS**

---

---

Nama : Yang Agita Rindri  
Pekerjaan : Dosen Prodi Teknologi Rekayasa Perangkat Lunak  
Polman Negeri Babel  
Pendidikan : S1 Sistem Informasi Institut Teknologi Sepuluh  
Nopember  
S2 Teknologi Informasi Universitas Gadjah Mada

**B**uku ini disusun untuk memudahkan mahasiswa dalam mempelajari teknik jaringan komputer. Buku ini berisi langkah-langkah praktis dalam pengaturan jaringan komputer. Langkah-langkah yang disajikan sangat jelas dan mudah untuk diterapkan. Selain itu buku ini disediakan gambar hasil tangkapan layar sehingga dapat memberikan visualisasi yang tepat. Bacalah buku ini untuk memahami lebih jauh tentang Jaringan Komputer.



Penerbit Politeknik Manufaktur Negeri  
Bangka Belitung (POLMANBABEL PRESS)  
Kawasan Industri Air Kantung, Sungailiat,  
Bangka 33211  
Telp: 0717 93586  
E-Mail: polman@polman-babel.ac.id

ISBN 978-623-97870-7-3

