AURIZA AKBAR

PRAKTIKUM KOMUNIKASI DATA & JARINGAN KOMPUTER

ILMU KOMPUTER IPB

Daftar Isi

Daftar Tabel

Daftar Gambar

Bagian I

Layer Jaringan Komputer

1

Instalasi Web Server Virtual

Tujuan: mahasiswa dapat menginstal aplikasi web pada *virtual private server* (VPS) berbasis Linux.

VPS menyediakan fleksibilitas untuk menginstal aplikasi server apa saja, tidak terbatas hanya pada aplikasi web berbasis PHP. Layanan VPS banyak tersedia (misal: Niagahoster, DigitalOcean, dan Amazon) dengan harga yang bervariasi sesuai dengan spesifikasi server yang ditawarkan.

Membuat VM Ubuntu Server

Telah tersedia *virtual disk image* (VDI) instalasi Ubuntu Server 16.04 di direktori `/opt/vm`. Salin *file* `ubuntu-server.vdi` tersebut ke direktori *home* anda. Kemudian, buat VM baru pada VirtualBox dengan tipe "Ubuntu 64-bit". Gunakan *virtual disk* yang sudah disalin tadi.[1]

[1] bagi yang ingin mencoba instalasi Ubuntu Server dari awal, silahkan unduh Ubuntu Server dan ikuti petunjuknya di sini

Setting port-forwarding *VM*

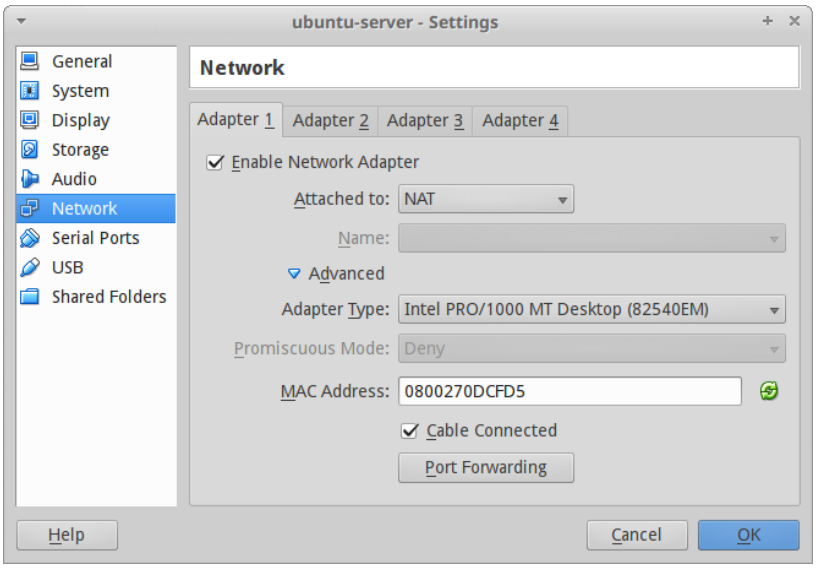
Tujuannya adalah agar VM bisa diakses dari luar melalui alamat IP *host* (*localhost*). Masuk ke '*Settings -> Network -> Advanced -> Port Forwarding*' dan tambahkan dua aturan berikut.

Tabel 1.1: Aturan *port forwarding*

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
http	TCP		8888		80
ssh	TCP		2222		22

Dengan demikian, jika kita mengakses `localhost:8888` di *host*, maka akan diteruskan ke `localhost:80` di *guest* (VM).

Setelah semuanya beres, jalankan VM dengan login *username* `student` dan *password* `student`.



Gambar 1.1: *Port forwarding* pada NAT VirtualBox

Instalasi LAMP (Linux Apache MySQL PHP)

```
# instal SSH
sudo apt update
sudo apt install ssh
```

Setelah terinstal SSH, kita bisa mengakses VM secara *remote*. Buka terminal di *host* untuk login *remote* ke *port* 2222.

```
# akses remote dari host
ssh student@localhost -p 2222

# instal Apache, MySQL, PHP
sudo apt install apache2
sudo apt install mysql-server
sudo apt install php
sudo apt install libapache2-mod-php
sudo apt install php-mysql
sudo apt install php-gd php-mcrypt php-mbstring php-xml php-ssh2
sudo service apache2 restart
```

Cek instalasi Apache dengan membuka laman http://localhost:8888.

Instalasi aplikasi web Wordpress

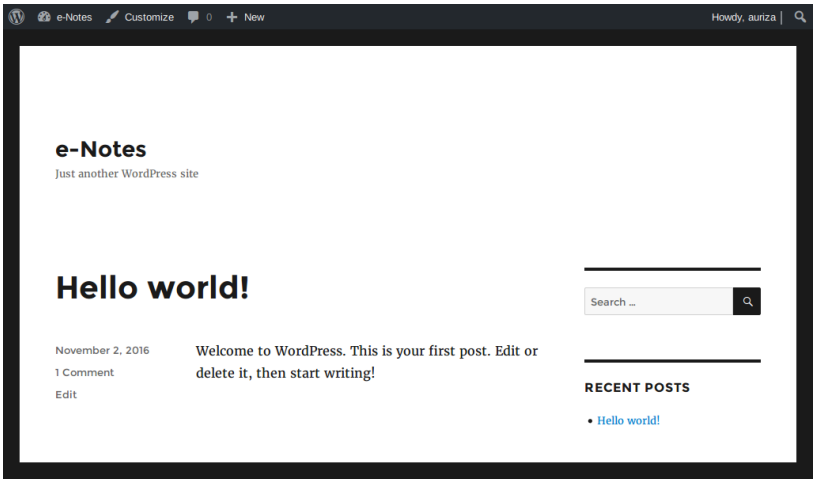
```
# buat database dan user untuk Wordpress
mysql -u root -p -v -e "
  CREATE DATABASE wordpress;
  CREATE USER wordpress IDENTIFIED BY 'password';
  GRANT ALL PRIVILEGES ON wordpress.* TO wordpress;"

# download Wordpress
wget "https://wordpress.org/latest.tar.gz"
```

```
# ekstrak ke direktori web
sudo tar -xzf latest.tar.gz -C /var/www/html

# ubah kepemilikan ke user www-data (webserver)
sudo chown -R www-data:www-data /var/www/html/wordpress
```

Buka laman http://localhost:8888/wordpress untuk meneruskan instalasi.



Gambar 1.2: Halaman utama Wordpress

Praktikum pekan depan: cabling

Setiap praktikan membawa:

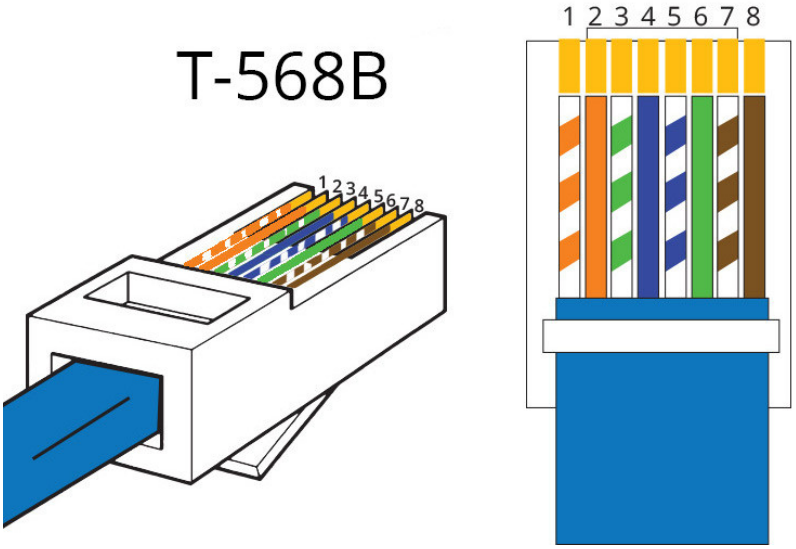
- kabel LAN Cat5E minimal 1 meter[2]
- konektor RJ-45 4 buah
- gunting
- *crimping tool* (jika ada)

[2] bagi yang mau kabel LAN bekas gratis, silahkan ke lab NCC

2
Cabling Jaringan LAN

Tujuan: mahasiswa dapat melakukan terminasi kabel UTP untuk infrastruktur jaringan kabel.

Standar LAN



Gambar 2.1: Standar T568B

Cabling

Alat dan Bahan

- Kabel UTP Cat5E
- *Crimping tool*
- Pengupas kabel atau gunting
- Konektor RJ-45 4 buah
- *Cable tester*

Langkah

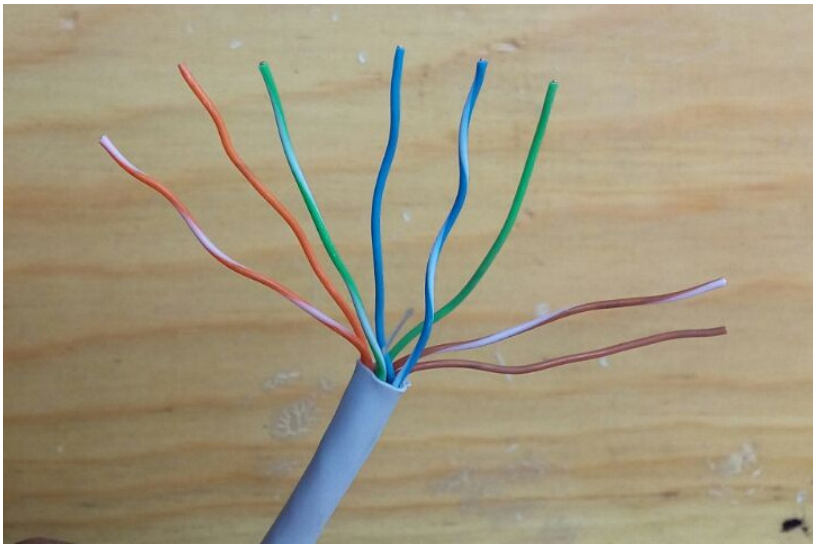
- Kelupas sarung kabel sepanjang kurang lebih 4 cm.
- Lepaskan pilinan dan susun kabel dengan standar T568B
- Luruskan semua kabel

Gambar 2.2: Alat dan bahan

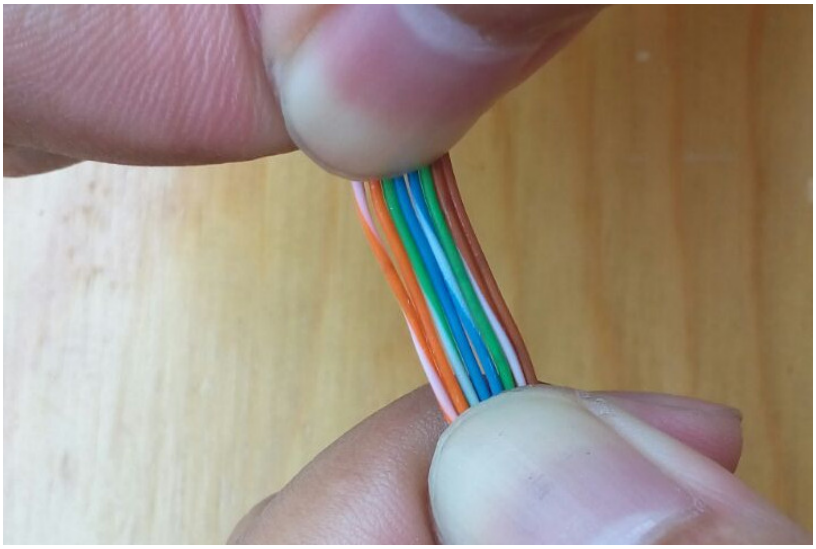
Gambar 2.3: Kabel UTP kategori 5E

Gambar 2.4: Kelupas sarung kabel

Gambar 2.5: Kabel yang telah dikelupas

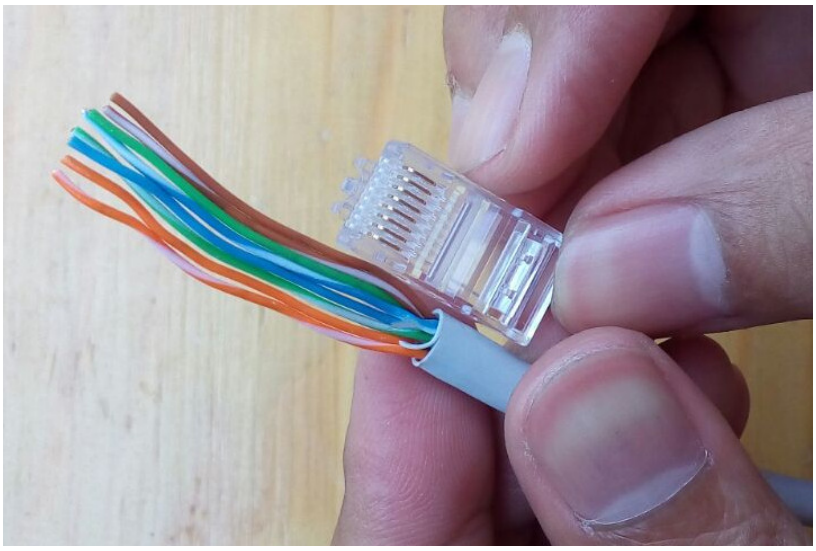


Gambar 2.6: Susunan kabel T568B

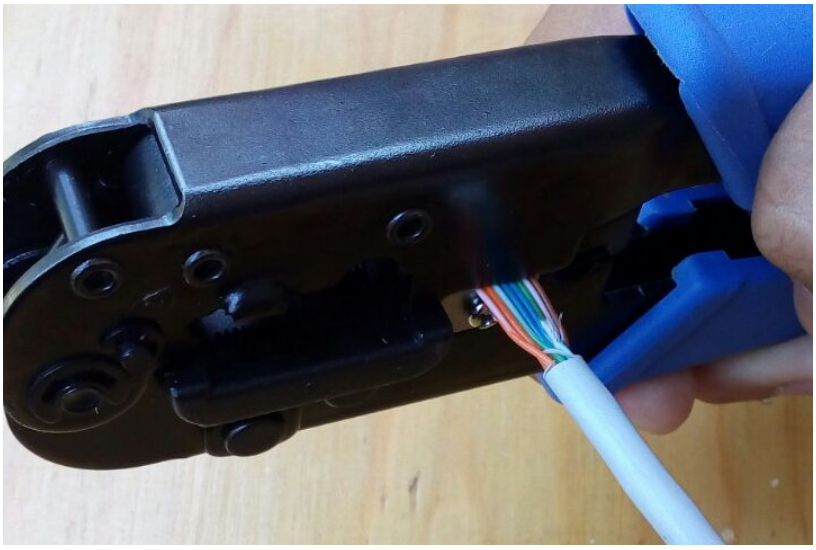


Gambar 2.7: Kabel yang sudah diluruskan

- Potong ujungnya, sesuaikan dengan panjang konektor. Jaket kabel harus masuk dan terjepit oleh konektor.



Gambar 2.8: Sesuaikan dengan panjang konektor



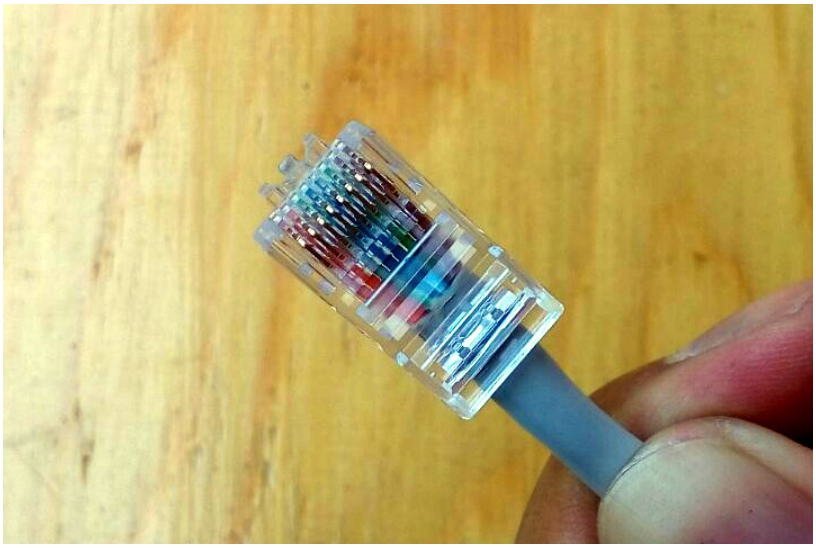
Gambar 2.9: Potong kabel dengan *crimping tool*

- Masukkan semua kabel ke dalam konektor
  - pastikan ujung kabel masuk sampai ujung konektor
  - pastikan jaket kabel terjepit oleh konektor
- *Crimp* dengan *crimping tool*
- Ulangi lagi pada ujung satunya
- Tes dengan *cable tester*

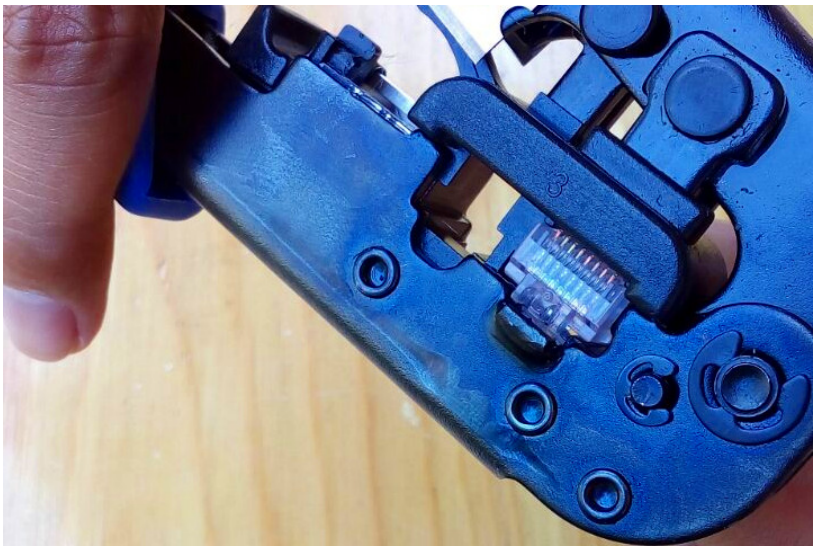
Penilaian

- *Crimping* rapi dan semua kabel tersambung: **100**
- *Crimping* tidak rapi: **-10** per konektor
- Kabel tidak tersambung: **-10** per kabel
- Kabel nomor 1, 2, 3, atau 6 [1] tidak tersambung: **ulang**

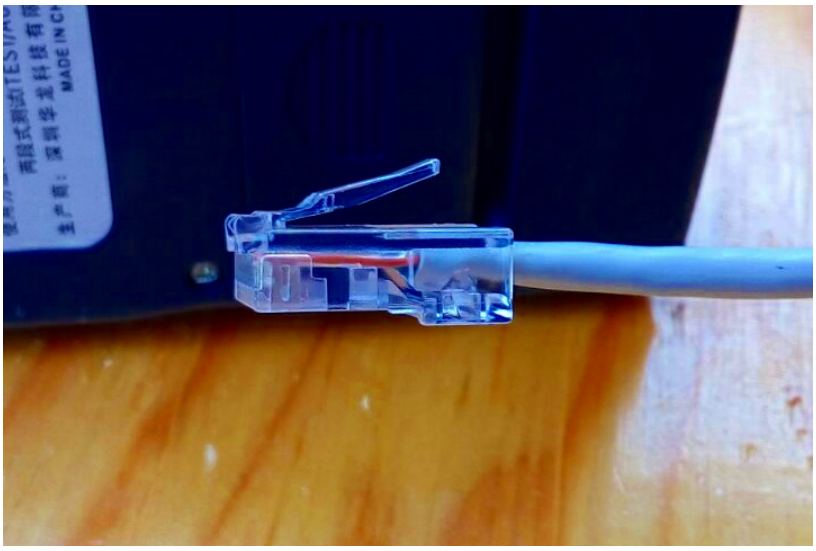
[1] Fast Ethernet hanya memakai 4 kabel, yaitu kabel nomor 1, 2, 3, dan 6. Sedangkan, Gigabit Ethernet memakai semuanya, yaitu 8 kabel.



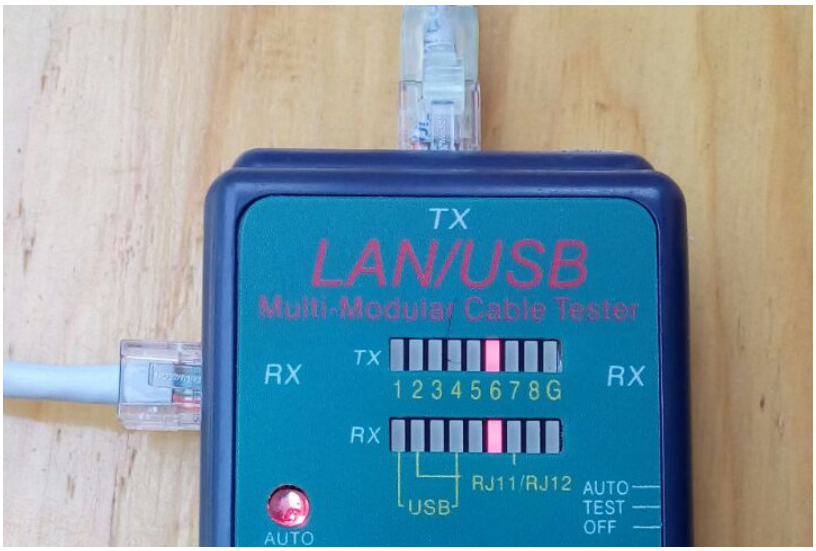
Gambar 2.10: Masukkan kabel ke konektor, pastikan ujung kabel masuk hingga ke dalam



Gambar 2.11: *Crimp* sampai kabel terjepit oleh konektor



Gambar 2.12: Kabel yang sudah di-*crimp*



Gambar 2.13: Tes dengan *cable tester*

Praktikum pekan depan: infrastruktur wireless

Setiap kelompok membawa:

- kabel LAN (*straight*) yang dibuat hari ini
- laptop untuk setting *access point*

Bahan Bacaan Lanjut

- Terrible Terminations[2]: How even perfectly good Ethernet cable and connectors, put together badly, can result in lousy performance.

[2] http://www.bluejeanscable.com/articles/terrible-terminations.htm

3
Infrastruktur Wireless

Tujuan: mahasiswa dapat membuat infrastruktur jaringan *wireless*.

Standar *wireless* LAN yang paling banyak dipakai adalah standar IEEE 802.11 (Wi-Fi). Wi-Fi beroperasi pada pita frekuensi 2.4 GHz dan 5 GHz. Standar Wi-Fi yang banyak dipakai adalah 802.11n yang mendukung *dual band* dan antena *multiple-input multiple-output* (MIMO) hingga 4 buah. Standar Wi-Fi terbaru di pasaran adalah 802.11ac yang mendukung MIMO hingga 8 buah.

Tabel 3.1: Standar *wireless* IEEE 802.11

802.11	Frekuensi (GHz)	*Bandwidth* (MHz)	*Data rate* (Mbps)	MIMO	*Range* (m)
–	2.4	22	1–2	–	20
a	5.0	20	6–54	–	35
b	2.4	22	1–11	–	35
g	2.4	20	6–54	–	38
n	2.4/5.0	20,40	7.2–150	4	70
ac	5.0	20,40,80,160	7.2–867	8	35

Frekuensi 2.4 GHz

Standar 802.11b/g/n menggunakan frekuensi 2.4 GHz pada rentang spektrum 2400–2500 MHz. Rentang tersebut dibagi menjadi 14 *channel* dengan lebar tiap *channel* 20 MHz. Pusat tiap *channel* terpisah 5 MHz, dimulai dari *channel* 1 dengan pusat 2412 MHz. Untuk instalasi beberapa perangkat WiFi, perlu dipilih *channel* yang tidak *overlap* untuk meminimalkan interferensi. Contoh *non-overlap channel* yang banyak dipakai adalah *channel* 1, 6, dan 11[1].

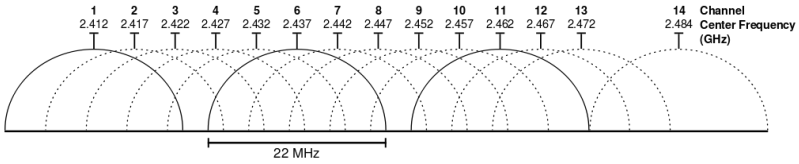
[1] http://www.metageek.com/training/resources/why-channels-1-6-11.html

Lebar *channel* dapat diubah menjadi 40 MHz untuk meningkatkan *data rate* dua kali lipat. Namun penggunaannya tidak disarankan pada jaringan bersama, karena akan sulit menghindari *overlap* dengan *channel* lainnya.

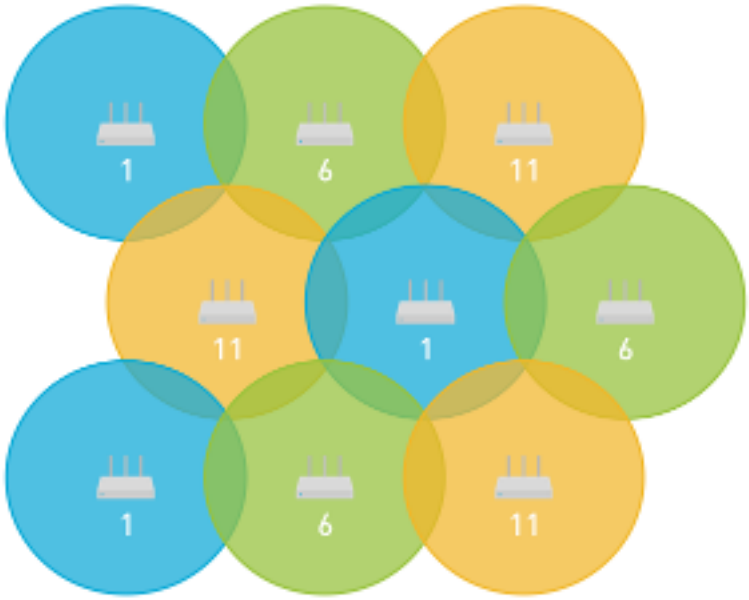
Berikut adalah contoh instalasi beberapa perangkat WiFi pada jaringan bersama. Pemilihan *channel* perlu diperhatikan untuk menghindari interferensi yang menyebabkan penurunan kinerja. Untuk memilih *channel*, kita harus melihat *channel* mana saja yang masih kosong dan tidak terlalu *crowded*. Gunakan aplikasi inSSIDer[2] pada Windows atau Wifi Analyzer[3] pada Android.

[2] http://www.metageek.com/support/downloads/

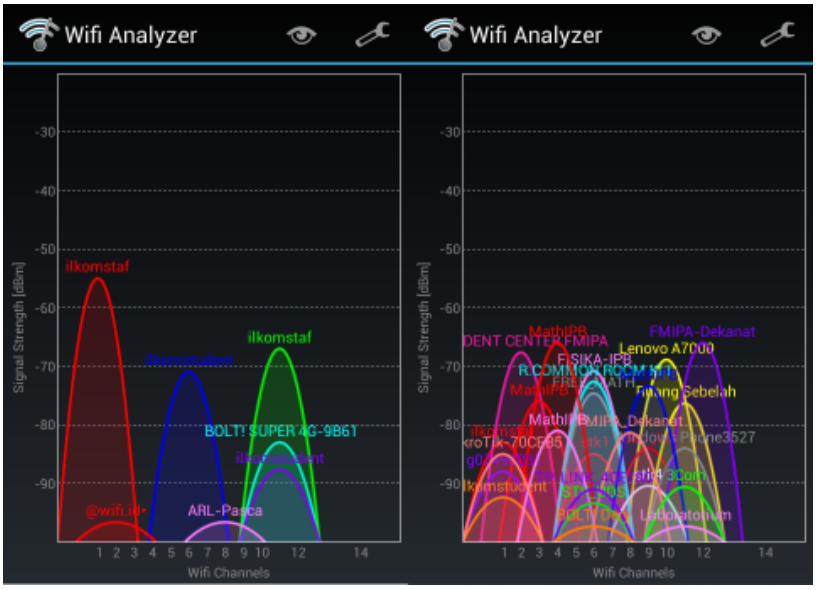
[3] https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer



Gambar 3.1: *Channel* 2.4 GHz (sumber: Wikipedia)



Gambar 3.2: Contoh pemilihan *channel* 2.4 GHz (sumber: MetaGeek)



Gambar 3.3: Contoh pengaturan *channel* yang baik dan buruk

Keamanan Data

Berikut jenis enkripsi yang bisa dipakai untuk melindungi data yang dikirim via *wireless*:

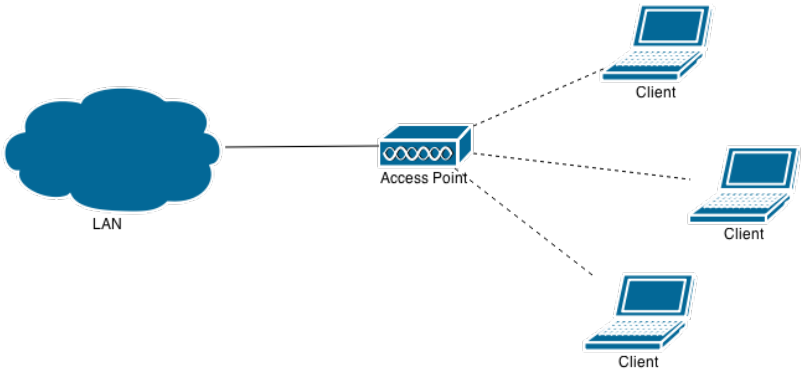
- *Unsecured*
- WEP: ARC4
- WPA: TKIP
- WPA2: AES

Keamanan terbaik adalah dengan WPA2 dan menonaktifkan fitur WPS[4].

[4] http://www.metageek.com/training/resources/wireless-security-basics.html

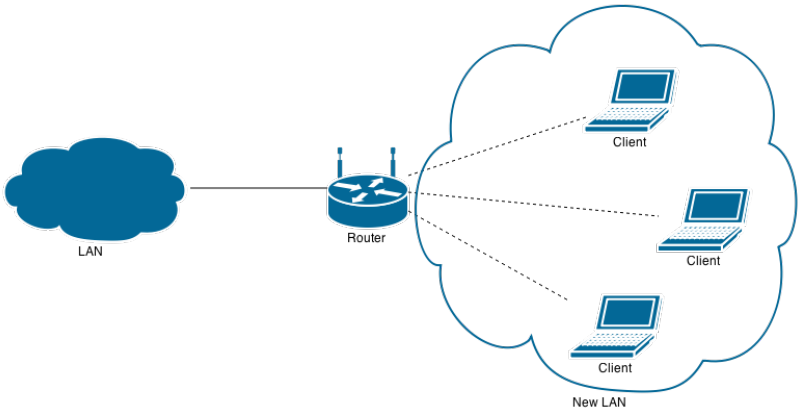
Mode Kerja

- *Access Point* (AP): untuk memperluas jaringan LAN yang sudah ada untuk klien *wireless*.



Gambar 3.4: *Wireless access point*

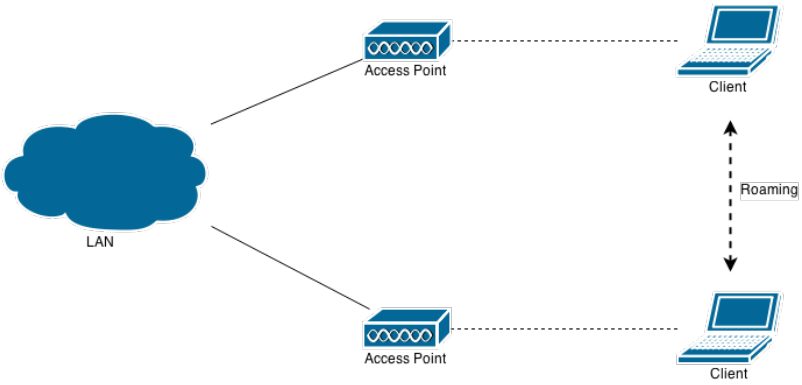
- *Router*: untuk membuat jaringan *wireless* baru



Gambar 3.5: *Wireless router*

Roaming *pada* Multiple *AP*

Untuk memanfaatkan fitur *roaming*, gunakan SSID dan pengaturan keamanan yang sama pada setiap AP yang dipasang. Jika klien berpindah tempat dan sinyal AP lemah, klien dapat berpindah ke AP lain secara otomatis tanpa melakukan koneksi ulang.



Gambar 3.6: *Wireless roaming*

Pengaturan Router *TL-WR1043ND*

Simulator: http://static.tp-link.com/resources/simulator/TL-WR1043ND_UN_2.0/Index.htm atau https://www.dd-wrt.com/demo/.

- Nyalakan *device* lalu tekan tombol *reset* sampai semua lampu menyala (~ 10 detik)
- Colokkan kabel *straight* dari komputer ke *port* LAN (kuning)
- Colokkan kabel *straight* dari jaringan ke *port* WAN (biru)
- Akses ke http://192.168.0.1 dengan *user*:`admin` dan *password*:`admin`
- "Quick Setup"
  - Network Name (SSID): **.....**
  - Region: **Indonesia**
  - Security: **WPA2-PSK**
  - Password: **.....**
  - More Advanced:
    - Width: **20 MHz**
    - Channel: **1, 6, atau 11**
- "System Tools"
  - Time setting
    - Time zone: **GMT +7**
    - Klik **Get GMT**
  - Password
    - Ganti *username* dan *password*

Pengaturan Access Point *TL-WA901ND*

Simulator: http://static.tp-link.com/resources/simulator/TL-WA901ND_V3/Index.htm

- Nyalakan *device* lalu tekan tombol *reset* sampai semua lampu menyala (~ 10 detik)
- Colokkan kabel *straight* dari komputer ke port LAN
- Akses ke http://192.168.0.254 dengan *user*:`admin` dan *password*:`admin`
- "Quick Setup"

  - Country/Region: **Indonesia**
  - Change the login account: **Yes**
    * Ganti *username* dan *password*
  - Mode: **Access Point**
  - Wireless
    * SSID: **. . . . . .**
    * Channel: **1, 6, atau 11**
    * Security: **WPA2-PSK**
    * Password: **. . . . . .**
  - Network type: **Smart IP (DHCP)**
  - Finish
- "Wireless"
  - Channel width: **20 MHz**
- Colokkan kabel *straight* dari jaringan ke port LAN

4
Pemrograman Soket TCP

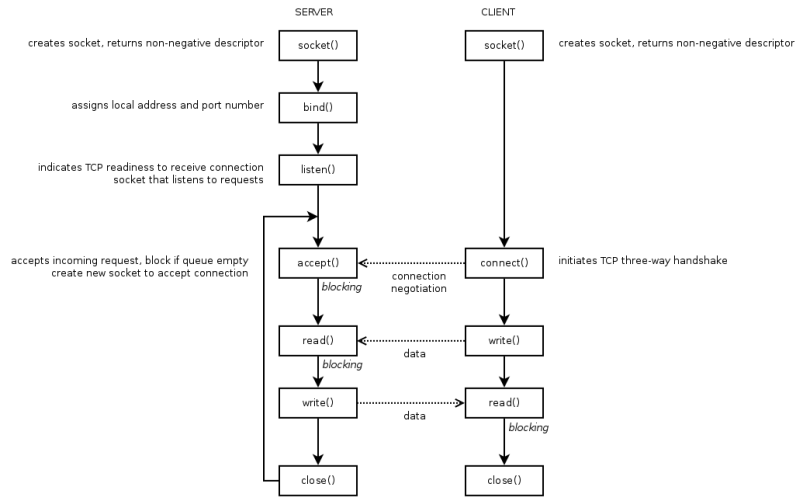
Tujuan: mahasiswa dapat membuat program server/klien TCP.

Soket adalah abstraksi untuk komunikasi jaringan. Pada sistem operasi UNIX, semua *resource*, termasuk komunikasi jaringan, diabstraksikan sebagai *file*. Jadi, anggap saja soket adalah sebuah *file* yang bisa dibuka, ditutup, dibaca, dan ditulis. Soket diidentifikasi dengan sebuah *integer* yang disebut *socket descriptor* (*pointer* ke struktur data yang berisi deskripsi soket). Struktur data tersebut berisi: jenis soket, alamat dan port lokal yang dipakai, dan alamat dan port *remote* yang akan menerima komunikasi dari soket.

Penggunaan soket terbagi menjadi dua:

- Soket pasif: server, menunggu koneksi masuk
- Soket aktif: klien, memulai koneksi ke server

Alur Penggunaan Soket TCP



Gambar 4.1: TCP socket call

Program Server TCP

`server.c`

```c
#include <stdio.h>
#include <string.h>
#include <unistd.h>
#include <arpa/inet.h>

#define PORT    2000
#define QUEUE   5

int main()
{
    int                 server;
    int                 client;
    struct sockaddr_in  sv_addr = {AF_INET, htons(PORT), {INADDR_ANY}};
    struct sockaddr_in  cl_addr;
    char                welcome[] = "+OK Welcome, type your message:\n";
    char                goodbye[] = "+OK Message accepted, goodbye!\n";
    char                data[80]  = {0};

    server = socket(AF_INET, SOCK_STREAM, 0);
    setsockopt(server, SOL_SOCKET, SO_REUSEADDR, &(int){1}, sizeof (int));
    bind(server, (struct sockaddr*)&sv_addr, sizeof sv_addr);
    if (listen(server, QUEUE) == 0)
        puts("listening...");

    while (1) {
        client = accept(server, (struct sockaddr*)&cl_addr, &(socklen_t){sizeof cl_addr});

        write(client, welcome, sizeof welcome);

        memset(data, 0, sizeof data);
        read(client, data, sizeof data);
        printf("[%s:%d]: %s", inet_ntoa(cl_addr.sin_addr), ntohs(cl_addr.sin_port), data);

        write(client, goodbye, sizeof goodbye);

        close(client);
    }

    close(server);
    return 0;
}
```

Jalankan program `server`, lalu gunakan `nc` sebagai klien untuk melakukan koneksi ke server.

```
nc localhost 2000
```

Coba buat dua sesi klien yang mengakses server secara bersamaan, apa yang terjadi? Mengapa demikian? Bagaimana agar server bisa melayani banyak klien sekaligus?

Dengan membuat program server menjadi *multithreaded*, server bisa melayani beberapa klien sekaligus. Tambahkan

direktif OpenMP berikut di atas blok `while`. Kompilasi dengan menambahkan *flag* `-fopenmp`.

```
#pragma omp parallel private(client, cl_addr, data) num_threads(16)
```

Program Klien TCP

`client.c`

```
#include <stdio.h>
#include <unistd.h>
#include <arpa/inet.h>

#define HOST    "127.0.0.1"
#define PORT    2000

int main()
{
    int                 server;
    struct sockaddr_in  sv_addr = {AF_INET, htons(PORT), {inet_addr(HOST)}};
    char                mesg[80];
    char                data[80];

    server = socket(AF_INET, SOCK_STREAM, 0);
    connect(server, (struct sockaddr*)&sv_addr, sizeof sv_addr);

    read(server, mesg, sizeof mesg);
    printf("%s", mesg);

    fgets(data, sizeof data, stdin);
    write(server, data, sizeof data);

    read(server, mesg, sizeof mesg);
    printf("%s", mesg);

    close(server);
    return 0;
}
```

Jalankan program `server`, lalu jalankan program `client` di atas.

Tugas

Buat program klien untuk koneksi ke server web http://xubuntu.org (`162.213.33.66`) dan menampilkan keluarannya ke layar.

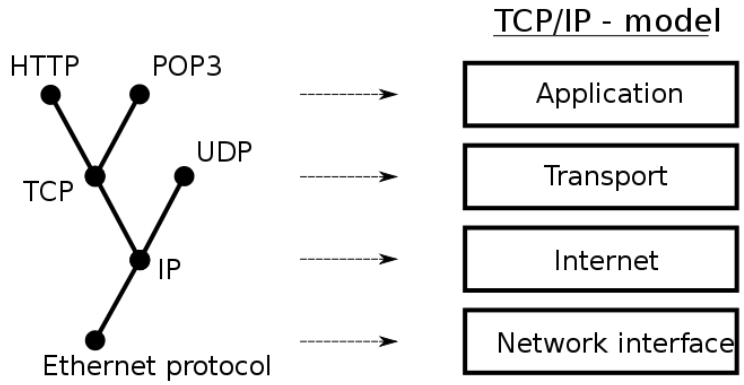
Petunjuk: kirimkan *request* HTTP berikut ke server dan tampilkan balasannya.

```
GET / HTTP/1.0
Host: xubuntu.org
```

5
Protokol Layer Aplikasi

Tujuan: mahasiswa dapat memahami cara kerja protokol *layer* aplikasi berbasis teks.

Protokol komunikasi adalah prosedur dan aturan standar dalam berkomunikasi. Klien yang ingin berkomunikasi dengan server harus mengikuti protokol tersebut. Misalnya klien untuk web seperti Firefox, harus menggunakan protokol HTTP untuk berkomunikasi dengan server. Namun, mekanisme protokol sangat jarang diperlihatkan pada aplikasi berbasis GUI. Untuk melihatnya, kita akan menggunakan program `netcat` dan `openssl s_client`. Umumnya protokol pada layer aplikasi ini berbasis teks, sehingga mudah dipahami.



Gambar 5.1: Layer jaringan TCP/IP (sumber: Wikipedia)

HTTP

Hypertext transfer protocol (HTTP) adalah dasar komunikasi pada *world wide web*. Server HTTP menggunakan *transport layer* TCP pada *port* 80. Spesifikasi HTTP versi 1.1 didefinisikan pada RFC 2616.

Jenis request

- `GET`: mengambil data

- `HEAD`: mengambil *header*-nya saja
- `POST`: menambahkan data, misalnya *form submission*
- ...

Status respon

- `100 Continue`
- `200 OK`
- `206 Partial Content`
- `301 Moved Permanently`
- `400 Bad Request`
- `401 Unauthorized`
- `403 Forbidden`
- `404 Not Found`
- ...

Header HTTP dapat diamati menggunakan 'Network Monitor' (`Ctrl+Shift+Q`) pada Firefox.

Contoh `GET`

```
$ netcat ipb.ac.id 80
GET / HTTP/1.0
Host: ipb.ac.id

HTTP/1.1 200 OK
Date: Wed, 15 Mar 2017 09:48:03 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.19
...
```

Contoh `POST` ke form

```
$ netcat 172.18.12.13 80
POST /pesan.php HTTP/1.0
Host: 172.18.12.13
Content-type: application/x-www-form-urlencoded
Content-length: 51

nama=Adam&email=adam@earth&pesan=Hola&tambah=Tambah
```

FTP

File transfer protocol (FTP) adalah protokol standar untuk transfer *file* via jaringan. FTP menggunakan *transport layer* TCP. Server menerima perintah melalui *port* 21. Server mengirimkan data ke port 20 (mode aktif) atau port *ephemeral* (mode pasif). Mode pasif lebih banyak dipakai oleh klien FTP karena tidak terhalang oleh *firewall*[1]. Spesifikasi FTP didefinisikan pada RFC 959.

[1] *lihat* http://slacksite.com/other/ftp.html

Perintah FTP

- `USER`: otentikasi nama pengguna
- `PASS`: otentikasi *password*
- `STAT`: status koneksi
- `CWD`: ganti direktori
- `PWD`: cetak nama direktori
- `PASV`: masuk ke mode pasif (dilakukan sebelum transfer data)
- `LIST`: list isi direktori
- `RETR`: mengunduh *file*
- `STOR`: mengunggah *file*
- `QUIT`: memutus koneksi

Contoh komunikasi dengan server FTP

```
$ netcat ftp.debian.org 21
220 ftp.debian.org FTP server
USER anonymous
331 Please specify the password.
PASS
230 Login successful.
STAT
211-FTP server status:
     ...
211 End of status
CWD debian
250 Directory successfully changed.
PWD
257 "/debian"
PASV
227 Entering Passive Mode (130,89,148,12,147,101).
LIST
150 Here comes the directory listing.
226 Directory send OK.
PASV
227 Entering Passive Mode (130,89,148,12,179,98).
RETR README
150 Opening BINARY mode data connection for README (1060 bytes).
226 Transfer complete.
QUIT
221 Goodbye.
```

Setelah masuk mode `PASV`, buka satu klien lain ke alamat yang dikembalikan mode tersebut untuk menangkap transfer data dari server.

```
(130,89,148,12,147,101) -> 130.89.148.12 $((147*256+101))

$ netcat 130.89.148.12 $((147*256+101))
-rw-rw-r--    1 1176     1176         1060 Jan 14 10:44 README
-rw-rw-r--    1 1176     1176         1290 Jun 26  2010 README.CD-manufacture
-rw-rw-r--    1 1176     1176         2588 Jan 14 10:44 README.html
```

```
-rw-r--r--    1 1176     1176           291 Mar 04 20:08 README.mirrors.html
-rw-r--r--    1 1176     1176            86 Mar 04 20:08 README.mirrors.txt
...
```

Gambar 5.2: Protokol untuk email: SMTP dan POP3/IMAP (sumber: Jscape)

SMTP

Simple mail transfer protocol (SMTP) adalah standar untuk pengiriman email melalui Internet. SMTP menggunakan *transport layer* TCP port 25, 465 (SSL), atau 587 (TLS). SSL atau TLS digunakan oleh SMTPS untuk mengenkripsi pesan. Spesifikasi SMTP didefinisikan pada RFC 5321.

Perintah SMTP

- `HELO`: intro ke server
- `AUTH`: otentikasi
- `MAIL`: alamat pengirim
- `RCPT`: alamat penerima
- `DATA`: isi pesan, diakhiri dengan sebaris yang berisi satu titik
- `QUIT`: mengakhiri sesi

Enkode username *dan* password *untuk otentikasi*

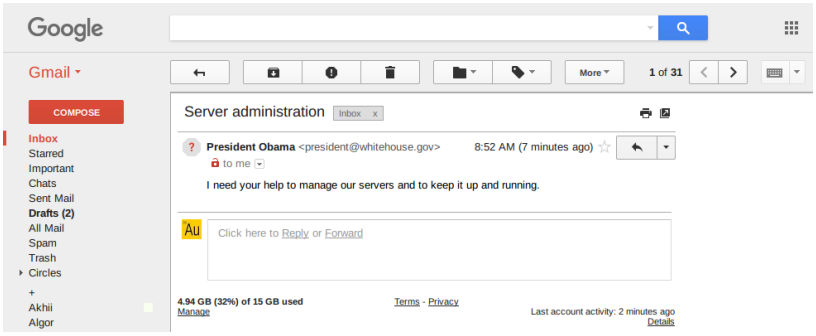
```
$ printf "\0komdatjarkom2@gmail.com\0ilkomerz2" | base64
AGtvbWRhdGphcmtvbTJAZ21haWwuY29tAGlsa29tZXJ6Mg==
```

Contoh komunikasi dengan server SMTPS

```
$ openssl s_client -connect smtp.gmail.com:465 -crlf -ign_eof -quiet
...
220 smtp.google.com ESMTP
HELO localhost
250 smtp.google.com at your service
AUTH PLAIN AGtvbWRhdGphcmtvbTJAZ21haWwuY29tAGlsa29tZXJ6Mg==
235 2.7.0 Accepted
MAIL FROM: <komdatjarkom2@gmail.com>
250 2.1.0 OK
```

```
RCPT TO: <auriza.akbar@gmail.com>
250 2.1.5 OK
DATA
354  Go ahead
Subject: SMTP test
From: "Komdat Jarkom" <komdatjarkom2@gmail.com>
To: "Auriza Akbar" <auriza.akbar@gmail.com>

Hello, this mail is sent from my terminal.
.
250 2.0.0 OK 1489590573
QUIT
221 2.0.0 closing connection
```



Gambar 5.3: Email telah terkirim

POP3

Post office protocol versi 3 (POP3) digunakan oleh klien untuk mengambil email dari server. POP3 menggunakan *transport layer* TCP port 110 atau 995 (POP3S). POP3S menggunakan SSL/TLS untuk mengenkripsi pesan. Spesifikasi POP3 didefinisikan pada RFC 1939.

Perintah POP3

- `USER`: nama pengguna
- `PASS`: *password*
- `STAT`: status inbox
- `LIST`: list inbox
- `RETR`: membaca surat
- `DELE`: menghapus surat
- `RSET`: reset, batalkan semua modifikasi
- `QUIT`: mengakhiri sesi

Contoh komunikasi dengan server POP3S

```
$ openssl s_client -connect pop.gmail.com:995 -crlf -ign_eof -quiet
...
+OK Gpop ready
```

```
USER komdatjarkom2@gmail.com
+OK send PASS
PASS ilkomerz2
+OK Welcome.
STAT
+OK 4 22204
LIST
+OK 4 messages (22204 bytes)
1 6920
2 4836
...
.
RETR 4
+OK message follows
...
Subject: New Email
From: Auriza Akbar <auriza.akbar@gmail.com>
To: komdatjarkom2@gmail.com

Test.
.
DELE 4
+OK marked for deletion
RSET
+OK
QUIT
+OK Farewell.
```

IMAP

Internet message access protocol (IMAP) digunakan oleh klien untuk mengambil email dari server. IMAP menggunakan *transport layer* TCP port 143 atau melalui SSL pada port 993 (IMAPS). Spesifikasi IMAP didefinisikan pada RFC 3501. IMAP memiliki fitur yang lebih canggih dan kompleks daripada POP3.

Perintah IMAP

- `LOGIN`: nama dan *password* pengguna
- `LIST`: list mailbox
- `SELECT`: memilih mailbox
- `FETCH`: membaca surat
- `STORE`: mengubah atribut surat
- `LOGOUT`: mengakhiri sesi

Contoh komunikasi dengan server IMAPS

```
$ openssl s_client -connect imap.gmail.com:993 -crlf -ign_eof -quiet
...
* OK Gimap ready
```

```
t1 LOGIN komdatjarkom2@gmail.com ilkomerz2
...
t1 OK komdatjarkom2@gmail.com authenticated (Success)
t2 LIST "" "*"
...
t2 OK Success
t3 SELECT INBOX
...
t3 OK [READ-WRITE] INBOX selected. (Success)
t4 FETCH 311 ALL
* 311 FETCH (ENVELOPE
                ("Tue, 21 Mar 2017 21:04:17 -0700 (PDT)" "SMTP G64130108"
                    (("Mastur Fatullah" NIL "masturfatullah808" "gmail.com")) ...
                    (("Komdat Jarkom" NIL "komdatjarkom2" "gmail.com")) ...
                )
                FLAGS (\Seen) ...
            )
t4 OK Success
t5 FETCH 311 BODY[TEXT]
* 311 FETCH (BODY[TEXT] {44}
                Hello, this mail is sent from my terminal.
            )
t5 OK Success
t6 STORE 311 +FLAGS \Flagged
* 311 FETCH (FLAGS (\Seen \Flagged))
t6 OK Success
t7 LOGOUT
* BYE LOGOUT Requested
t7 OK 73 good day (Success)
```

Tugas

Gunakan protokol SMTP langsung untuk mengirim email dari akun email kalian masing-masing ke komdatjarkom2@gmail.com dengan isi sebagai berikut (sesuaikan dengan nama dan NIM kalian):

```
Subject: SMTP G6...
From: ...
To: komdatjarkom2@gmail.com

Hello, ...

.
```

6
Aplikasi Jaringan

Tujuan: mahasiswa dapat menggunakan berbagai aplikasi jaringan untuk mengecek koneksi, konfigurasi, dan monitoring jaringan.

Koneksi

ping

- untuk mengecek koneksi ke suatu *host*
- mengirimkan paket ICMP `ECHO_REQUEST` ke *host* tujuan dan menunggu balasannya
- digunakan untuk memberikan gambaran awal di mana letak masalah pada jaringan

```
ping <dest>
```

traceroute

- untuk menelusuri rute menuju *host* tujuan, serta waktu latensinya
- digunakan untuk mengetahui di mana letak masalah pada jaringan
- `traceroute` bekerja dengan mengatur nilai *time-to-live* (TTL) paket
  - setiap paket melewati *gateway*, TTL berkurang satu
  - jika TTL bernilai 0, paket tersebut dibuang dan *gateway* mengirimkan pesan *error* ICMP "time exceeded" ke *host* pengirim

```
traceroute <dest>
```

host

- untuk mendapatkan alamat IP dari nama domain yang diberikan
- memakai protokol DNS untuk menerjemahkan nama domain menjadi alamat IP
- konfigurasi server DNS terletak pada *file* `/etc/resolv.conf`

```
host <domain>
```

```
host -a <domain>
```

whois

- untuk melihat info registrasi pemilik suatu domain

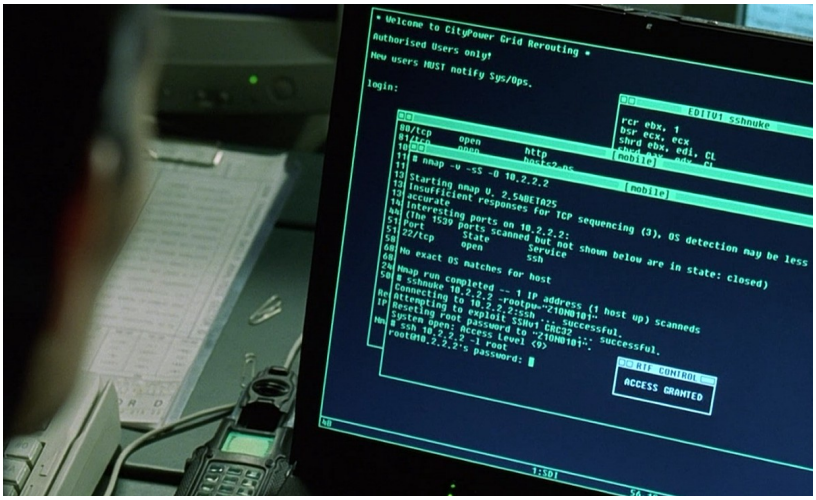
```
whois <domain>
```

nmap

- untuk mengetahui *port* yang terbuka pada suatu *host*
- juga informasi versi aplikasi dan sistem operasi yang digunakan

```
nmap <host>
```

```
nmap -A <host>
```



Gambar 6.1: nmap

Latihan:

- cari tahu alamat IP, nama admin, dan alamat admin domain `ipb.ac.id`
- cek *port* apa saja yang terbuka pada server `ipb.ac.id`
- cek jenis dan versi aplikasi server yang dipakai pada server `ipb.ac.id`
- dari data di atas, cari tahu apakah ada celah keamanan pada server tersebut

Konfigurasi

ifconfig

- untuk mengetahui konfigurasi *interface* jaringan pada host
- satu host memiliki lebih dari satu *interface*: *loopback*, ethernet, *wireless*, *point-to-point*
- konfigurasi *interface* jaringan terletak pada *file* `/etc/network/interfaces`

```
ifconfig
```

arp

- untuk menampilkan tabel ARP
- tabel ARP berisi pasangan MAC address dan alamat IP

- MAC address dipakai untuk mengirim paket dalam satu jaringan (*layer* 2: *link*)

`arp`

netstat

- menampilkan koneksi jaringan, tabel *routing*, statistik *interface*, dan sebagainya.

```
# menampilkan koneksi internet yang sedang aktif (kecuali server)
netstat

# menampilkan koneksi internet yang sedang listening (server)
netstat -l

# menampilkan statistik interface
netstat -i

# menampilkan tabel routing
netstat -r

# menampilkan statistik tiap protokol
netstat -s
```

route

- untuk menampilkan, menambah, atau mengurangi aturan pada tabel *routing*
- penting jika sebuah *host* memiliki banyak *interface* dan *gateway* (misal: PC router)
- *flag*: U (*up*), G (*gateway*), H (*host*), D (*dynamic*), ! (*reject*)

```
# menampilkan tabel routing
route

# mengatur default gateway, misalnya 192.168.1.1
route add default gw 192.168.1.1

# paket ke jaringan 192.168.3.0/24 akan di-forward ke interface 192.168.3.1
route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.3.1

# memblok paket dari jaringan 192.168.3.0/24
route add -net 192.168.3.0 netmask 255.255.255.0 reject

# memblok paket dari host 192.168.4.1
route add -host 192.168.4.1 reject

# menghapus konfigurasi routing sebelumnya
route del -host 192.168.4.1 reject
```

Monitoring

tcpdump

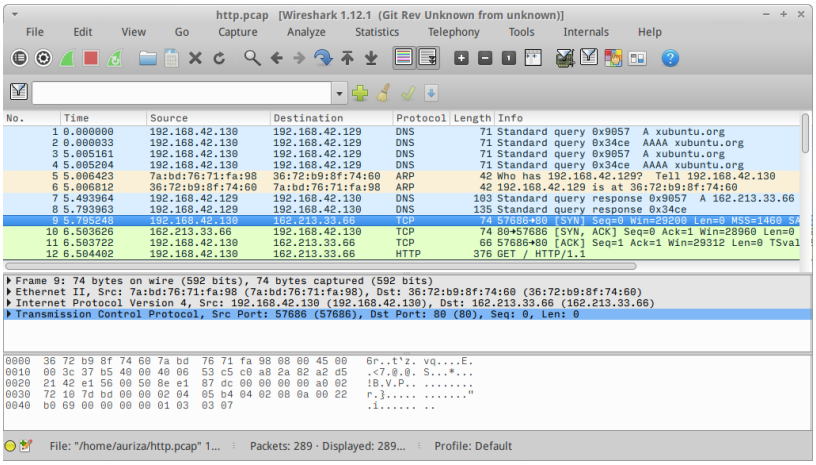
- menampilkan semua *traffic* paket pada sebuah *interface* jaringan
- hasil keluarannya (.pcap) dapat dianalisis lebih lanjut

```
tcpdump -i <interface>
```

```
tcpdump -i <interface> -w <file.pcap>
```

Wireshark

- versi GUI dari `tcpdump`
- digunakan untuk analisis jaringan



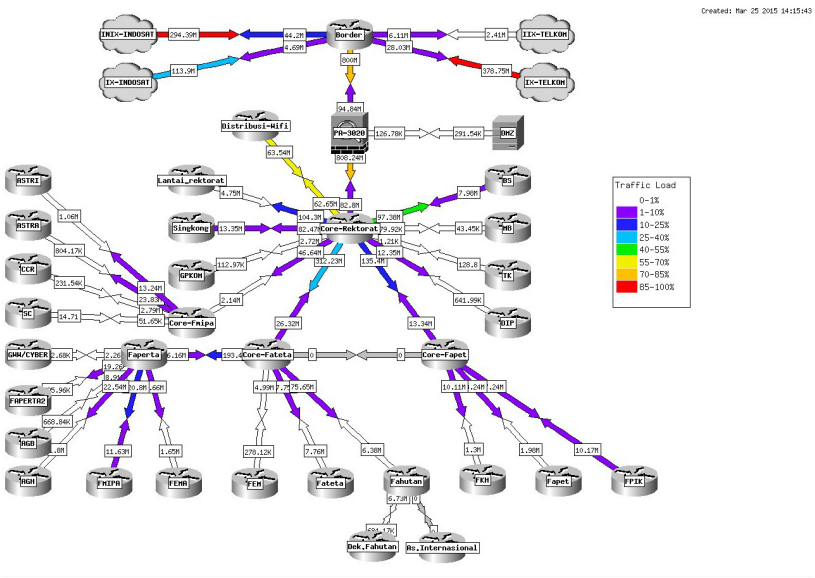
Gambar 6.2: Wireshark

Latihan:

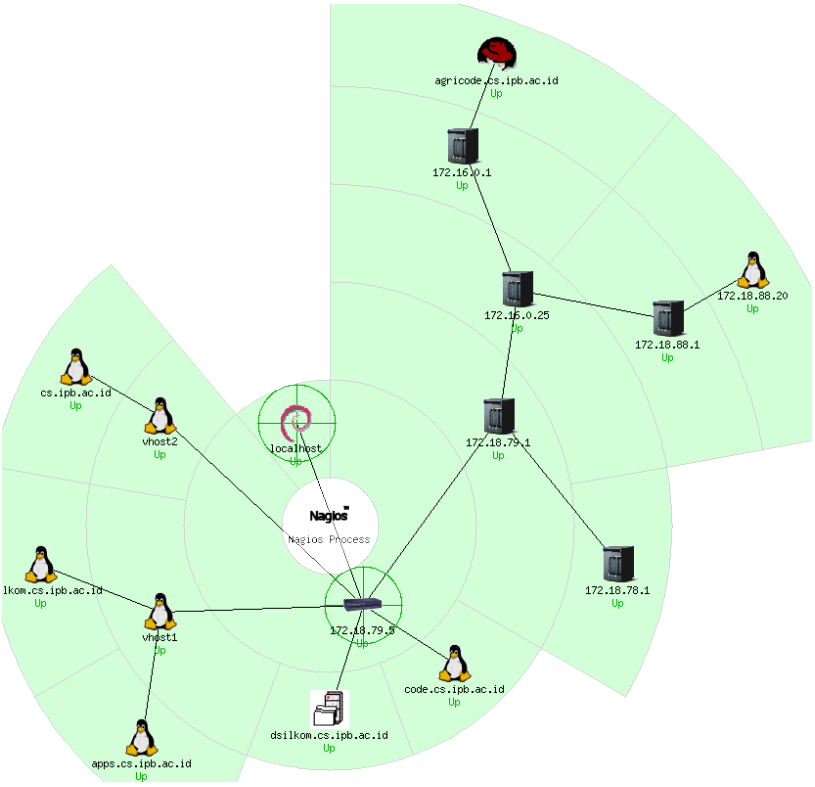
- *capture* semua paket HTTP saat membuka laman web http://xubuntu.org:
  - buka Wireshark dan mulai *capture* paket di *interface* Ethernet
  - buka *browser* dan akses ke laman http://xubuntu.org
  - tunggu sampai semua halaman termuat
  - stop *capture* paket
- filter semua paket dari/ke server web tersebut
- amati dan analisis
  - TCP *handshake*
  - HTTP *request* dan *response*
  - struktur *header* frame Ethernet, paket IP, segmen TCP, dan data HTTP
- simpan hasil *capture* dengan ekstensi `.pcap`

Web-based

- Cacti http://www.cacti.net/
- MRTG http://oss.oetiker.ch/mrtg/
- SmokePing http://oss.oetiker.ch/smokeping/
- Nagios http://www.nagios.org/



Gambar 6.3: Cacti



Gambar 6.4: Nagios

Bonus Film

```
telnet towel.blinkenlights.nl
```

Tugas

Ulangi analisis paket dengan Wireshark untuk kasus aplikasi FTP!

Bagian II

Simulasi Packet Tracer

7
Pengenalan Packet Tracer

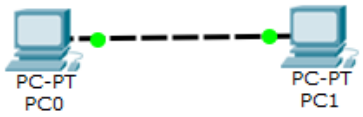
Packet Tracer adalah simulator protokol yang dikembangkan oleh Cisco. Silahkan unduh di https://www.netacad.com/about-networking-academy/packet-tracer/.

Operasi Dasar

- Menambahkan *device* (PC, *switch*, *hub*, dll)
- Membuat koneksi antar *device*
  - jika *port* berwarna hijau, berarti *device* sudah terkoneksi
- Konfigurasi *device* bisa melalui *command prompt* atau GUI
- Verifikasi koneksi
  - mode *realtime*: dengan perintah `ping`
  - mode simulasi: dengan membuat *protocol data unit* (PDU) untuk mengamati jalannya paket secara visual

Koneksi Point-to-Point

- Dua PC dengan IP statis dihubungkan dengan kabel LAN *crossover*
- Setting IP statis untuk tiap PC melalui *command prompt*, misal: `ipconfig 192.168.0.1 255.255.255.0`
- Coba ganti dengan kabel *straight*, apa yang terjadi?
- Bagaimana kalau kita ingin menghubungkan 3 PC atau lebih?

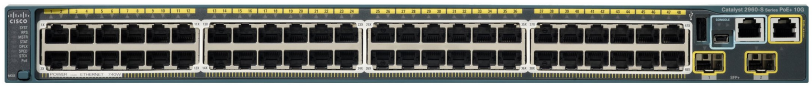


Gambar 7.1: *Point-to-point*

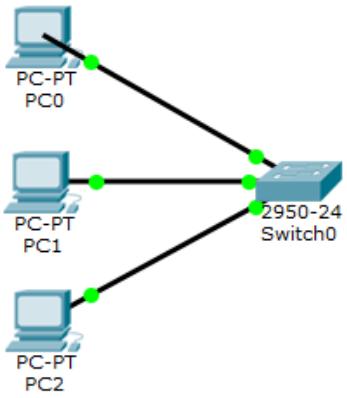
Switch *dan* Hub

- Tiga PC dengan IP statis dihubungkan dengan *switch*
  - Cek tabel ARP pada tiap PC dan tabel MAC pada *switch* dengan tombol “Inspect”
- Kemudian coba juga dengan memakai *hub*
  - *hub* jarang dipakai karena cara kerjanya *broadcast*: membuat jaringan lebih sibuk

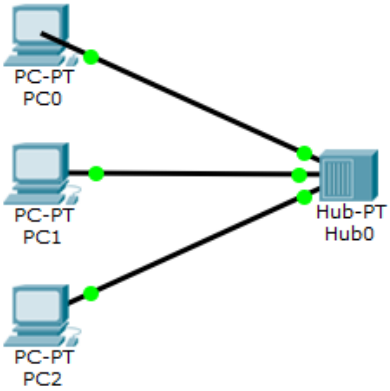
- Amati perbedaan cara kerja *hub* vs *switch* (pakai mode simulasi)



Gambar 7.2: *Switch Cisco 2960*



Gambar 7.3: Simulasi *switch*



Gambar 7.4: Simulasi *hub*

Broadcast

- Coba ping *broadcast* untuk jaringan `192.168.0.0/24`
  - `ping 192.168.0.255`
  - `ping 255.255.255.255` (jika alamat jaringan tidak diketahui)
- Jalankan pada mode simulasi, amati jalannya paket ICMP

Catatan

- Jaringan `192.168.0.0/24`:
  - Alamat jaringan: `192.168.0.0`
  - Alamat untuk *host*: `192.168.0.[1-254]` –> maksimal 254 *host* dalam jaringan ini
  - Alamat *broadcast*: `192.168.0.255`
  - Prefiks jaringan: `24` –> Subnet mask: `255.255.255.0`
- Alamat jaringan: digunakan untuk *routing*

- Alamat *broadcast*: digunakan untuk mengetahui siapa saja *host* lain yang berada dalam satu jaringan

Tugas

- Jenis protokol apa saja yang dipakai saat mengirim `ping` pertama kali?
- Jelaskan dengan singkat kegunaan protokol tersebut?

8
Aplikasi Server dan Wireless

- Hubungkan 3 PC dengan menggunakan *switch*
- alamat jaringan LAN yang akan dipakai: `192.168.0.0/24`

DHCP

- DHCP digunakan untuk memberikan konfigurasi alamat IP secara dinamis kepada klien
- Tambahkan satu server, hubungkan ke *switch*
  - set alamat IP server statis: `192.168.0.2/24`
  - aktifkan servis DHCP: `Services > DHCP`
    - *range* alamat IP yang akan dialokasikan secara dinamis: `192.168.0.[101-250]/24`
    - *gateway* adalah alamat *router* yang akan digunakan untuk ke luar jaringan
    - klik **Save**, lalu aktifkan servis DHCP

      ```
      Default gateway: 192.168.0.1
      DNS server     : 192.168.0.2
      Start IP addres: 192.168.0.101
      Subnet mask    : 255.255.255.0
      Max num of user: 150
      ```
  - set konfigurasi IP semua PC menjadi dinamis: `Desktop > IP Configuration > DHCP`
  - pastikan PC telah mendapatkan alamat IP dari server DHCP
  - cek konektivitas dengan ping *broadcast*

Multiple Switch

- Tambahkan satu *switch* baru dan beberapa PC
  - contoh kasus: kita ingin menambahkan PC baru ke dalam jaringan, tetapi port pada *switch* pertama sudah terpakai semua, maka perlu *switch* tambahan untuk memperluas jaringan LAN.
  - hubungkan *switch* baru ke *switch* pertama dengan kabel *crossover*
  - pastikan PC yang terhubung pada *switch* baru sudah mendapat alamat IP dari server DHCP
  - cek konektivitas dengan ping *broadcast*, amati juga simulasi

berjalannya paket DHCP, ARP, dan ICMP (gunakan filter paket)
  - **penting**: jangan memasang *switch* membentuk *cycle*, karena akan membuat jaringan *looping*

Wireless AP

- Tambahkan satu *wireless* AP dan beberapa *laptop* atau *smartphone*
  - contoh kasus: kita ingin perangkat *mobile* juga dapat terhubung ke jaringan
  - set SSID, *channel*, dan *security* pada AP
  - matikan *laptop*, ganti *network interface* ethernet menjadi *wireless* (`PT-LAPTOP-NM-1W`), hidupkan *laptop* kembali
  - set koneksi wifi ke AP jaringan LAN pada *laptop*

Servis lainnya

- Cobakan servis HTTP pada server
  - modifikasi isi halaman web pada server
  - akses alamat IP server dari *browser* salah satu PC di jaringan
- Cobakan servis DNS pada server
  - DNS: menerjemahkan nama domain menjadi alamat IP
  - berikan nama domain untuk server ini, misal: `komdat.id`
  - akses alamat domain di atas dari *browser* salah satu PC di jaringan

Tugas

Lengkapi tabel berikut ini! Kumpulkan pada selembar kertas!

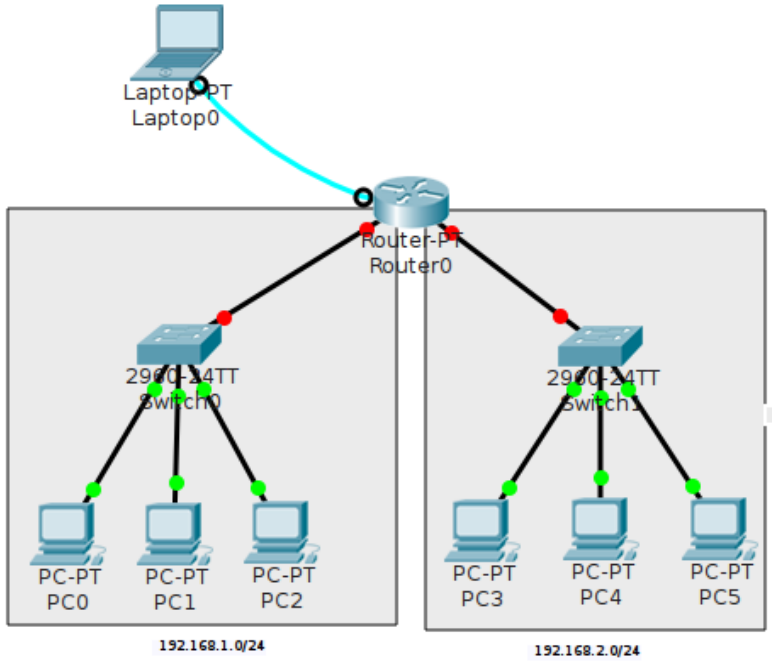
Atribut	HTTP	DHCP	DNS
Kepanjangan	Hypertext Transfer Protocol	.....	.....
Standar	RFC 2616	.....	.....
Layer	Aplikasi	.....	.....
Transport	TCP	.....	.....
Port	80	.....	.....
Fungsi	komunikasi data pada WWW	.....	.....
Jenis request	GET, POST, HEAD, PUT, ...	.....	.....
Aplikasi server	Apache, Nginx, IIS	.....	.....
Aplikasi klien	Firefox, Chrome, Opera	.....	.....

9
Router Jaringan Lokal

Router: bekerja hingga *layer* 3 (*network*), memiliki lebih dari satu alamat IP, dan bertugas mengarahkan paket ke jaringan yang lebih dekat ke tujuan.

Gambar 9.1: *Router* Cisco 1921

Konfigurasi Router *untuk Menghubungkan Dua Jaringan Lokal*



Gambar 9.2: *Router* LAN

- Diberikan dua jaringan: `192.168.1.0/24` dan `192.168.2.0/24`
  - untuk menghubungkan jaringan yang berbeda, dibutuhkan *router*

  - siapkan beberapa PC dan *switch* untuk dua jaringan lokal tersebut
- Tambahkan satu *router* untuk menghubungkan kedua jaringan tersebut
- Siapkan satu laptop untuk mengkonfigurasi *router*, hubungkan dengan kabel *console*
  - buka Terminal pada laptop untuk menampilkan CLI *router*
- Set alamat IP *router* dengan mengikuti perintah berikut
  - set *hostname* dan *password router*
  - set alamat IP *router* dan mengaktifkan *interface*-nya
  - biasanya *router* diberikan nomor *host* paling awal (`.1`)

```
enable
configure terminal
  hostname R0
  enable secret *****

  interface FastEthernet 0/0
    ip address 192.168.1.1 255.255.255.0
    no shutdown
    exit

  interface FastEthernet 1/0
    ip address 192.168.2.1 255.255.255.0
    no shutdown
    exit

  exit
show running-config
disable
```

- Setelah itu, atur layanan DHCP pada *router* dengan membuat *pool* untuk tiap jaringan

```
enable
configure terminal

  ip dhcp pool NET1
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
    exit
  ip dhcp excluded-address 192.168.1.1 192.168.1.100

  ip dhcp pool NET2
    network 192.168.2.0 255.255.255.0
    default-router 192.168.2.1
    exit
  ip dhcp excluded-address 192.168.2.1 192.168.2.100

  exit
disable
```

- Atur konfigurasi IP semua PC dengan DHCP

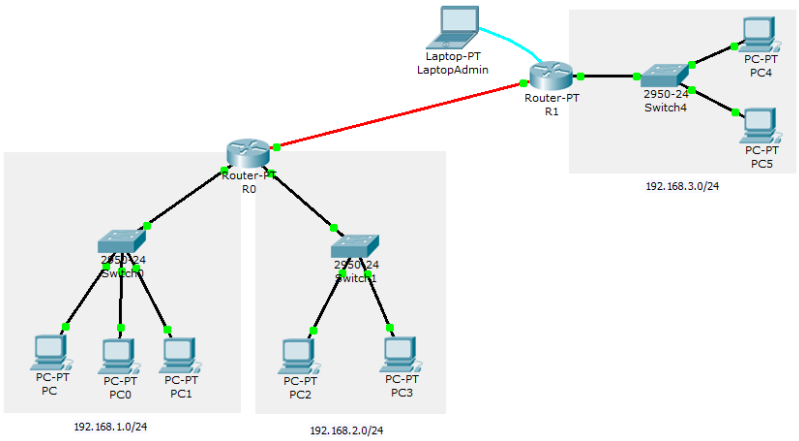
- Cek koneksi tiap PC antara dua jaringan
- Untuk mengecek daftar klien DHCP, gunakan perintah `show ip dhcp binding`
- **Penting**: simpan ke *file* `.pkt` untuk bahan praktikum pekan depan

Tugas

Setting *router* untuk menghubungkan tiga jaringan lokal yang berbeda, yaitu jaringan untuk `STAFF`, `STUDENT`, dan `NCC`. Berikan alamat IP privat dengan *subnet* masing-masing `172.18.15.0/24`, `172.18.16.0/24`, dan `172.18.12.0/24`.

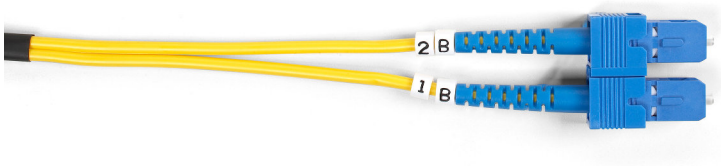
10
Routing Statis

Menghubungkan Jaringan yang Lokasinya Berjauhan



Gambar 10.1: *Router* untuk menghubungkan jaringan dengan lokasi yang berjauhan

- Lanjutkan dari praktikum sebelumnya, tambahkan jaringan baru `192.168.3.0/24`
  - jaringan baru ini jaraknya 5 km dari jaringan yang sudah ada
  - perlu memakai kabel *fiber optic* (FO)



Gambar 10.2: Kabel *fiber optic single-mode*

- Tambahkan satu *router* baru `R1`
  - hubungkan *router* lama `R0` dengan *router* `R1` ini memakai kabel FO
  - hubungkan router `R1` dengan jaringan baru tersebut
- Hubungkan antara *router* `R0` dengan `R1`
  - antara *router* `R0` dan `R1` adalah jaringan baru, misalnya `192.168.0.0/24`
  - konfigurasi alamat IP *interface* di *router* lama `R0`

```
enable
```

```
configure terminal
  interface FastEthernet4/0
    ip address 192.168.0.1 255.255.255.0
    no shutdown
    exit
  exit
disable
```

– konfigurasi alamat IP *interface* di *router* baru `R1`

```
enable
configure terminal
  hostname R1
  enable secret *****

  interface FastEthernet4/0
    ip address 192.168.0.2 255.255.255.0
    no shutdown
    exit

  exit
disable
```

- Hubungkan *router* `R1` dengan jaringan `192.168.3.0/24` dan set *pool* DHCP untuk jaringan tersebut

```
enable
configure terminal

  interface FastEthernet0/0
    ip address 192.168.3.1 255.255.255.0
    no shutdown
    exit

  ip dhcp pool NET3
    network 192.168.3.0 255.255.255.0
    default-router 192.168.3.1
    exit
  ip dhcp excluded-address 192.168.3.1 192.168.3.100

  exit
disable
```

- Konfigurasi *routing* statik di `R0`
  – rute ke jaringan `192.168.3.0/24`: *forward* ke `192.168.0.2` (`R1`)

```
enable
configure terminal

  ip route 192.168.3.0 255.255.255.0 192.168.0.2

  exit
show ip route
disable
```

- Konfigurasi *routing* statik di `R1`
  - rute ke jaringan `192.168.1.0/24`: *forward* ke `192.168.0.1` (`R0`)
  - rute ke jaringan `192.168.2.0/24`: *forward* ke `192.168.0.1` (`R0`)

```
enable
configure terminal

  ip route 192.168.1.0 255.255.255.0 192.168.0.1
  ip route 192.168.2.0 255.255.255.0 192.168.0.1

end
show ip route
disable
```

- Set konfigurasi IP semua PC yang baru dengan DHCP
- Cek koneksi antara jaringan baru dengan jaringan lama

Tugas

Tambahkan *router* baru `R2` dengan jarak 5 km dari `R0` dan `R1`. *Router* `R2` ini menghubungkan ke dua jaringan baru, yaitu `192.168.4.0/24` dan `192.168.5.0/24`.

11
Routing Dinamis: RIPv2

Routing *Statis vs Dinamis*

Dua metode dasar untuk membangun tabel *routing*: statis dan dinamis[1].

[1] http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=5

Routing statis:

- tabel *routing* disusun secara manual oleh administrator jaringan
- rute statis untuk tiap jaringan harus dikonfigurasi pada setiap *router*
- menyediakan kontrol penuh pada konfigurasi *routing*, namun tidak praktis untuk jaringan yang besar
- jika ada *link* yang terputus, maka harus *update* tabel *routing* secara manual

Routing dinamis:

- tabel *routing* disusun oleh protokol *routing* yang berjalan pada *router*
- *router* berbagi informasi *routing* dengan *router* lainnya secara berkala
- mampu memilih jalur yang berbeda secara dinamis jika ada *link* yang terputus
- contoh: *routing information protocol* (RIP), *open shortest path first* (OSPF), dan *border gateway protocol* (BGP).

Routing Information Protocol *(RIP)*

RIP didefinisikan dalam RFC 1058 pada tahun 1988. RIP adalah protokol vektor-jarak sederhana yang menggunakan jumlah *hop* sebagai ukuran jarak. RIP didesain untuk jaringan kecil dengan jumlah *hop* maksimum 15.

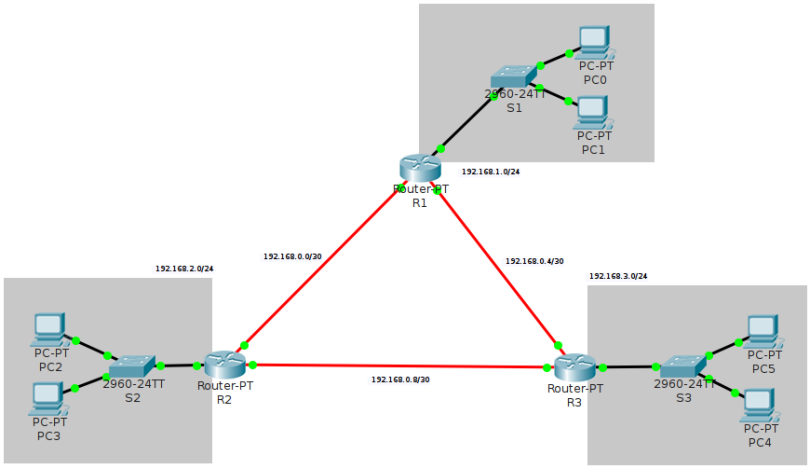
Terdapat tiga versi RIP[2]:

[2] Nemeth *et al.* 2011, https://goo.gl/RicmLf

- RIPv1 hanya mendukung *classful routing*
- RIPv2 menambahkan dukungan *subnet* dan *classless inter-domain routing* (CIDR)
- RIPng adalah ekstensi dari RIPv2 untuk jaringan IPv6

Walaupun terkesan ketinggalan zaman, namun RIP masih digunakan karena sederhana, mudah dikonfigurasi, dan bekerja dengan baik pada jaringan berkompleksitas rendah.

Routing *Dinamis dengan RIPv2*



Gambar 11.1: *Routing* dinamis dengan RIPv2

- siapkan tiga *router*: R1, R2, dan R3, hubungkan dengan kabel fiber
- siapkan jaringan lokal untuk tiap *router*: `192.168.1.0/24`, `192.168.2.0/24`, dan `192.168.3.0/24`

Konfigurasi router *R1*

- set IP *router* R1 yang terhubung ke LAN dan set servis DHCP

```
enable
configure terminal
  hostname R1

  interface FastEthernet 0/0
    ip address 192.168.1.1 255.255.255.0
    no shutdown
    exit

  ip dhcp pool NET1
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
    exit
  ip dhcp excluded-address 192.168.1.1 192.168.1.20
```

- set IP router R1 yang terhubung dengan *router* lainnya

```
  interface FastEthernet 4/0
    ip address 192.168.0.1 255.255.255.252
    no shutdown
    exit

  interface FastEthernet 5/0
    ip address 192.168.0.5 255.255.255.252
    no shutdown
    exit
```

- konfigurasi RIP untuk *routing*, tambahkan **semua jaringan yang terhubung langsung** dengan *router* R1 dalam notasi *classful*

```
router rip
  version 2
  network 192.168.0.0
  network 192.168.1.0
  no auto-summary
  exit
```

- jangan kirim *update* RIP ke *interface* untuk LAN, kirimkan ke sesama *router* saja

```
router rip
  passive-interface FastEthernet 0/0
  exit
```

- lanjutkan dengan konfigurasi R2 dan R3

Konfigurasi router *R2*

```
enable
configure terminal
  hostname R2

  interface FastEthernet 0/0
    ip address 192.168.2.1 255.255.255.0
    no shutdown
    exit

  ip dhcp pool NET2
    network 192.168.2.0 255.255.255.0
    default-router 192.168.2.1
    exit
  ip dhcp excluded-address 192.168.2.1 192.168.2.20

  interface FastEthernet 5/0
    ip address 192.168.0.2 255.255.255.252
    no shutdown
    exit

  interface FastEthernet 4/0
    ip address 192.168.0.9 255.255.255.252
    no shutdown
    exit

  router rip
    version 2
    passive-interface FastEthernet 0/0
    network 192.168.0.0
    network 192.168.2.0
    no auto-summary
```

```
    exit

  exit
disable
```

Konfigurasi router *R3*

```
enable
configure terminal
  hostname R3

  interface FastEthernet 0/0
    ip address 192.168.3.1 255.255.255.0
    no shutdown
    exit

  ip dhcp pool NET3
    network 192.168.3.0 255.255.255.0
    default-router 192.168.3.1
    exit
  ip dhcp excluded-address 192.168.3.1 192.168.3.20

  interface FastEthernet 4/0
    no ip address
    ip address 192.168.0.6 255.255.255.252
    no shutdown
    exit

  interface FastEthernet 5/0
    ip address 192.168.0.10 255.255.255.252
    no shutdown
    exit

  router rip
    version 2
    passive-interface FastEthernet 0/0
    network 192.168.0.0
    network 192.168.3.0
    no auto-summary
    exit

  exit
disable
```

Pengujian

- Cek koneksi antara ketiga jaringan tersebut (mode *realtime* dan simulasi)
- Cek isi tabel *routing* tiap *router* dengan perintah `show ip route`
- Cek detail protokol dengan perintah `show ip protocols`

Tugas

Tambahkan satu *router* baru R4 yang tersambung ke R2, R3, dan jaringan baru NET4 `192.168.4.0/24`. Gunakan *routing* dinamis RIPv2 dan pastikan semua jaringan tersambung.

Referensi

Lihat dokumentasi lengkapnya di halaman berikut: *RIP and RIPng routing*[3] dan *configuring RIP*[4].

[3] http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=10

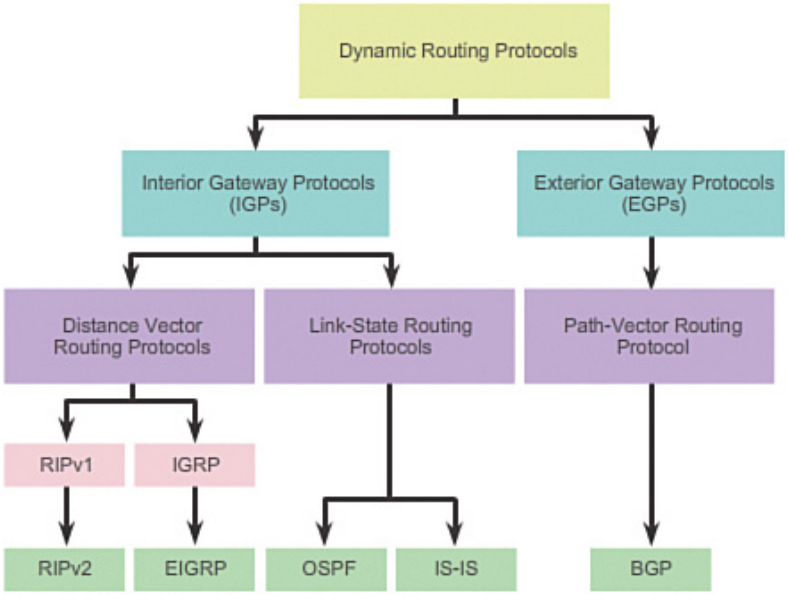
[4] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/12-4t/irr-12-4t-book/irr-cfg-info-prot.html

12
Routing Dinamis: OSPF

Ada dua cara bagaimana algoritme *routing* dinamis bekerja, yaitu *distance-vector* (contoh: RIP, EIGRP) dan *link-state* (contoh: OSPF, IS-IS). Perbedaan antara keduanya dapat dibaca lebih lanjut pada halaman berikut:

- Jenis protokol *routing*[1]
- Protokol *distance vector* dan *link state*[2]

[1] http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7
[2] https://www.youtube.com/watch?v=ygxBBMztT4U



Gambar 12.1: Protokol *routing* dinamis (sumber: Cisco)

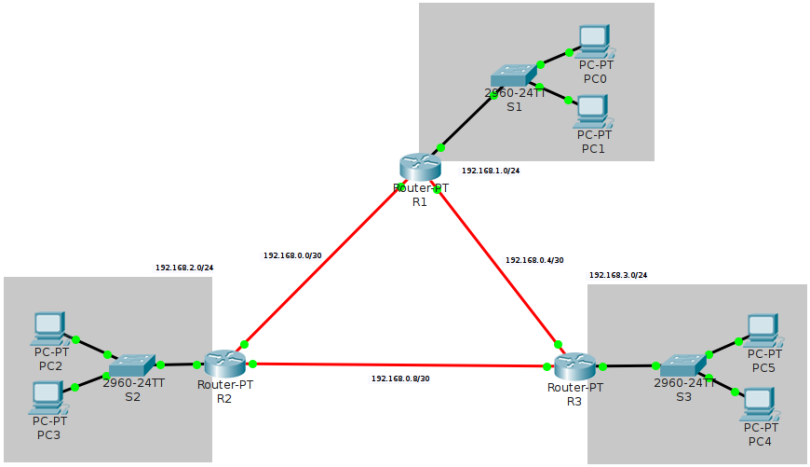
Open Shortest Path First *(OSPF)*

OSPF adalah protokol berbasis *link-state* yang paling populer. "*Shortest path first*" mengacu pada nama algoritme yang dipakai dalam menghitung rute; sedangkan "*open*" menandakan bahwa protokol ini bersifat terbuka. RFC2328 mendefinisikan protokol dasar (OSPFv2) dan RFC5340 menambahkan dukungan untuk IPv6 (OSPFv3). OSPF adalah protokol handal yang baik untuk topologi yang besar dan kompleks. Keunggulannya dibandingkan dengan RIP antara lain kemampuan mengatur beberapa jalur ke satu tujuan dan kemampuan mempartisi jaringan menjadi bagian (*area*) untuk

mengurangi beban *router* dalam meng-*update* tabel *routing* (Nemeth *et al.* 2011).

Routing *Dinamis dengan OSPF*

Routing dengan OSPF dapat dibagi menjadi beberapa area. Pada contoh berikut, hanya digunakan satu area, yaitu `area 0`.



Gambar 12.2: Routing dinamis dengan OSPF

- siapkan tiga *router*: R1, R2, dan R3, hubungkan dengan kabel fiber
- siapkan jaringan lokal untuk tiap *router*: `192.168.1.0/24`, `192.168.2.0/24`, dan `192.168.3.0/24`

Konfigurasi router *R1*

- set IP *router* R1 yang terhubung ke LAN dan set servis DHCP

```
enable
configure terminal
  hostname R1

  interface FastEthernet 0/0
    ip address 192.168.1.1 255.255.255.0
    no shutdown
    exit

  ip dhcp pool NET1
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
    exit
  ip dhcp excluded-address 192.168.1.1 192.168.1.20
```

- set IP router R1 yang terhubung dengan *router* lainnya

```
  interface FastEthernet 4/0
    ip address 192.168.0.1 255.255.255.252
    no shutdown
    exit
```

```
interface FastEthernet 5/0
  ip address 192.168.0.5 255.255.255.252
  no shutdown
  exit
```

- konfigurasi OSPF pada tabel *routing*, tambahkan **semua jaringan dalam satu area** *routing* yang R1 terlibat di dalamnya, misalnya `192.168.0.0/16`

```
router ospf 1
  network 192.168.0.0 0.0.255.255  area 0
  exit
```

- lanjutkan dengan konfigurasi R2 dan R3

Konfigurasi router *R2*

```
enable
configure terminal
  hostname R2

  interface FastEthernet 0/0
    ip address 192.168.2.1 255.255.255.0
    no shutdown
    exit

  ip dhcp pool NET2
    network 192.168.2.0 255.255.255.0
    default-router 192.168.2.1
    exit
  ip dhcp excluded-address 192.168.2.1 192.168.2.20

  interface FastEthernet 5/0
    ip address 192.168.0.2 255.255.255.252
    no shutdown
    exit

  interface FastEthernet 4/0
    ip address 192.168.0.9 255.255.255.252
    no shutdown
    exit

  router ospf 1
    network 192.168.0.0 0.0.255.255  area 0
    exit

  exit
disable
```

Konfigurasi router *R3*

```
enable
```

```
configure terminal
  hostname R3

  interface FastEthernet 0/0
    ip address 192.168.3.1 255.255.255.0
    no shutdown
    exit

  ip dhcp pool NET3
    network 192.168.3.0 255.255.255.0
    default-router 192.168.3.1
    exit
  ip dhcp excluded-address 192.168.3.1 192.168.3.20

  interface FastEthernet 4/0
    no ip address
    ip address 192.168.0.6 255.255.255.252
    no shutdown
    exit

  interface FastEthernet 5/0
    ip address 192.168.0.10 255.255.255.252
    no shutdown
    exit

  router ospf 1
    network 192.168.0.0 0.0.255.255  area 0
    exit

  exit
disable
```

Pengujian

- Cek koneksi antara ketiga jaringan tersebut (mode *realtime* dan simulasi)
- Cek isi tabel *routing* tiap *router* dengan perintah `show ip route`
- Cek detail protokol dengan perintah `show ip protocols`
- Cek tetangga *router* dengan perintah `show ip ospf neighbor`

Tugas

Tambahkan satu *router* baru R4 yang tersambung ke R2, R3, dan jaringan baru NET4 `192.168.4.0/24`. Gunakan *routing* dinamis OSPF dan pastikan semua jaringan tersambung.

Referensi

Lihat dokumentasi lengkapnya di halaman berikut: *configuring OSPF*[3].

[3] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro-cfg.html