

# BAB 14

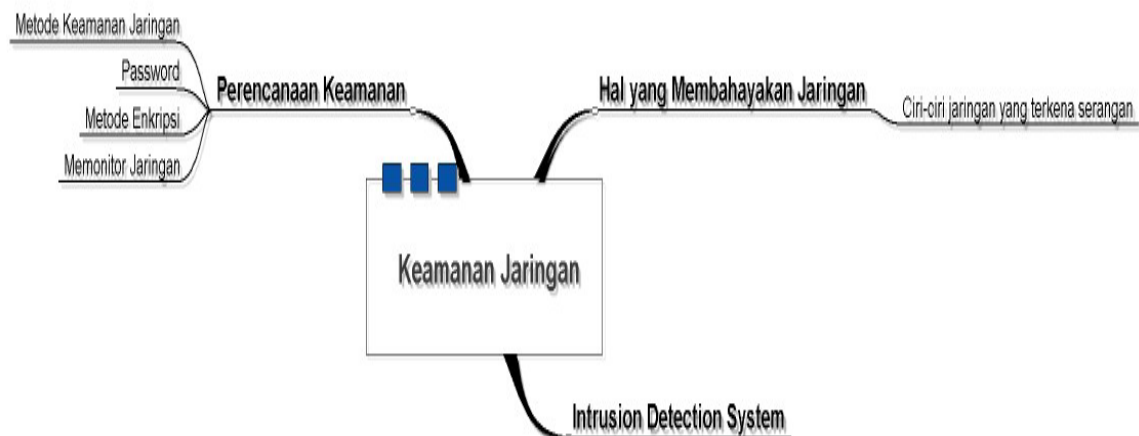
## KEAMANAN JARINGAN

### Tujuan Instruksional Umum

- Siswa mampu menjelaskan bagaimana cara mengamankan suatu jaringan

### Tujuan Instruksional Khusus

- Siswa mampu menyebutkan hal-hal yang membahayakan sebuah jaringan
- Siswa mampu menyebutkan ciri-ciri jaringan yang terkena serangan
- Siswa mampu merencanakan sebuah keamanan jaringan dengan baik
- Siswa mampu menjelaskan secara umum mengenai enkripsi
- Siswa mampu melakukan enkripsi secara sederhana
- Siswa mampu menyebutkan hal-hal yang perlu dimonitor dalam jaringan.
- Siswa mampu menjelaskan mengenai Intrusion Detection System.



Gambar 14.1. Rincian Pembelajaran Bab 14

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini

Perkembangan teknologi komputer, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke Internet. Sebagai akibat dari serangan itu, banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan kita.

Dalam perkembangan teknologi dewasa ini, sebuah informasi menjadi sangat penting bagi sebuah organisasi. Informasi tersebut biasanya dapat diakses oleh para penggunanya. Akan tetapi, ada masalah baru yang berakibat dari keterbukaan akses tersebut. Masalah-masalah tersebut antara lain adalah sebagai berikut:

- Pemeliharaan validitas dan integritas data atau informasi tersebut
- Jaminan ketersediaan informasi bagi pengguna yang berhak
- Pencegahan akses sistem dari yang tidak berhak
- Pencegahan akses informasi dari yang tidak berhak

## Hal yang Membahayakan Jaringan

Kegiatan dan hal-hal yang membahayakan keamanan jaringan antara lain adalah hal-hal sebagai berikut:

- Probe  
Probe atau yang biasa disebut probing adalah suatu usaha untuk mengakses sistem atau mendapatkan informasi tentang sistem. Contoh sederhana dari probing adalah percobaan log in ke suatu account yang tidak digunakan. Probing dapat dianalogikan dengan menguji kenop-kenop pintu untuk mencari pintu yang

tidak dikunci sehingga dapat masuk dengan mudah. Probing tidak begitu berbahaya bagi sistem jaringan kita namun biasanya diikuti oleh tindakan lain yang lebih membahayakan keamanan.

- Scan

Scan adalah probing dalam jumlah besar menggunakan suatu tool. Scan biasanya merupakan awal dari serangan langsung terhadap sistem yang oleh pelakunya ditemukan mudah diserang.

- Account Compromise

- Root Compromise

- Packet Sniffer

Packet sniffer adalah sebuah program yang menangkap (capture) data dari paket yang lewat di jaringan. Data tersebut bisa termasuk user name, password, dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk text. Paket yang dapat ditangkap tidak hanya satu paket tapi bisa berjumlah ratusan bahkan ribuan, yang berarti pelaku mendapatkan ribuan user name dan password. Dengan password itu pelaku dapat mengirimkan serangan besar-besaran ke sistem.

- Denial of Service

Denial of service (DoS) bertujuan untuk mencegah pengguna mendapatkan layanan dari sistem. Serangan DoS dapat terjadi dalam banyak bentuk. Penyerang dapat membanjiri (flood) jaringan dengan data yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, seperti process control block (PCB) atau pending network connection. Penyerang juga mungkin saja mengacaukan komponen fisik dari jaringan atau memanipulasi data yang sedang dikirim termasuk data yang terenkripsi.

- Exploitation of Trust

- Malicious Code

- Internet Infrastructure Attacks

## Perencanaan Keamanan

Untuk menjamin keamanan dalam jaringan, perlu dilakukan perencanaan keamanan yang matang berdasarkan prosedur dan kebijakan dalam keamanan jaringan. Perencanaan tersebut akan membantu dalam hal-hal berikut ini:

- Menentukan data atau informasi apa saja yang harus dilindungi
- Menentukan berapa besar biaya yang harus ditanamkan dalam melindunginya
- Menentukan siapa yang bertanggung jawab untuk menjalankan langkah-langkah yang diperlukan untuk melindungi bagian tersebut

### Metode Keamanan Jaringan

Dalam merencanakan suatu keamanan jaringan, ada beberapa metode yang dapat diterapkan. Metode-metode tersebut adalah sebagai berikut:

- Pembatasan akses pada suatu jaringan

Ada 3 beberapa konsep yang ada dalam pembatasan akses jaringan, yakni sebagai berikut:

- ✦ Internal Password Authentication

Password yang baik menjadi penting dan sederhana dalam keamanan suatu jaringan. Kebanyakan masalah dalam keamanan jaringan disebabkan karena password yang buruk. Cara yang tepat antara lain dengan menggunakan shadow password dan menonaktifkan TFTP.

- ✦ Server-based password authentication

- ✦ Firewall dan Routing Control

Untuk firewall akan dijelaskan pada bagian selanjutnya.

- Menggunakan metode enkripsi tertentu

Dasar enkripsi cukup sederhana. Pengirim menjalankan fungsi enkripsi pada pesan plaintext, ciphertext yang dihasilkan kemudian dikirimkan lewat jaringan, dan penerima menjalankan fungsi dekripsi (decryption) untuk mendapatkan plaintext semula. Proses enkripsi/dekripsi tergantung pada kunci (key) rahasia yang hanya diketahui oleh pengirim dan penerima. Ketika kunci dan enkripsi ini digunakan, sulit bagi penyadap untuk mematahkan ciphertext, sehingga komunikasi data antara pengirim dan penerima aman.


Lebih lanjut mengenai enkripsi akan dijelaskan pada bagian selanjutnya.

- Pemonitoran terjadwal terhadap jaringan

Proses memonitor dan melakukan administrasi terhadap keamanan jaringan akan dibahas pada bagian lain.

## **Password**

Akun administrator pada suatu server sebaiknya diubah namanya dan sebaiknya hanya satu akun saja yang dapat mengakses. Pada sistem operasi Windows, cara membuat password adalah sebagai berikut:

- Tekan tombol  **Start** pada start menu
- Klik **Control Panel**
- Klik **User Account**
- klik **create a password**
- Masukkan password
- Tekan **tombol create password**

Pemberian password yang tepat dengan kebijakan keamanan dalam akun admin, password itu harus memiliki suatu karakter yang unik dan sukar ditebak. Ada beberapa karakter yang dapat digunakan agar password sukar untuk ditebak, antara lain adalah sebagai berikut:

- Karakter #

- Karakter %
- Karakter \$
- Dll

Untuk melakukan pengujian terhadap password yang dibuat. Ada utilitas yang dapat digunakan untuk mengetes kehandalan password, yaitu dengan menggunakan software seperti avior yang bertujuan untuk melakukan brute-force password.

Kewenangan akses bagi user lain dalam satu perusahaan perlu didokumentasikan, hal ini dilakukan untuk memenuhi kebutuhan klien. Kewenangan user selain administrator antara lain adalah memasukkan data-data terbaru sesuai dengan tujuan tertentu untuk memenuhi kebutuhan klien.

## **Metode Enkripsi**

Kriptografi macam ini dirancang untuk menjamin privacy, mencegah informasi menyebar luas tanpa izin. Akan tetapi, privacy bukan satu-satunya layanan yang disediakan kriptografi. Kriptografi dapat juga digunakan untuk mendukung authentication (memverifikasi identitas user) dan integritas (memastikan bahwa pesan belum diubah).

Kriptografi digunakan untuk mencegah orang yang tidak berhak untuk memasuki komunikasi, sehingga kerahasiaan data dapat dilindungi. Secara garis besar, kriptografi digunakan untuk mengirim dan menerima pesan. Kriptografi pada dasarnya berpatokan pada key yang secara selektif telah disebar pada komputer-komputer yang berada dalam satu jaringan dan digunakan untuk memproses suatu pesan.

Ada beberapa jenis metode enkripsi, sebagai berikut:

### ⊕ DES

DES adalah mekanisme enkripsi data yang sangat populer dan banyak digunakan. Ada banyak implementasi perangkat lunak maupun perangkat keras DES. DES melakukan transformasi informasi dalam bentuk plain text ke dalam bentuk data terenkripsi yang disebut dengan ciphertext melalui algoritma khusus

dan seed value yang disebut dengan kunci. Bila kunci tersebut diketahui oleh penerima, maka dapat dilakukan proses konversi dari ciphertext ke dalam bentuk aslinya.

Kelemahan potensial yang dimiliki oleh semua sistem enkripsi adalah kunci yang harus diingat, sebagaimana sebuah password harus diingat. Bila kunci ditulis dan menjadi diketahui oleh pihak lain yang tidak diinginkan, maka pihak lain tersebut dapat membaca data asli. Bila kunci terlupakan, maka pemegang kunci tidak akan dapat membaca data asli.

Banyak sistem yang mendukung perintah DES, atau utility-utility dan library yang dapat digunakan untuk DES.

#### ✦ PGP (Pretty Food Privacy)

PGP dibuat oleh Phil Zimmerman, menyediakan bentuk proteksi kriptografi yang sebelumnya belum ada. PGP digunakan untuk melindungi file, email, dan dokumen-dokumen yang mempunyai tanda digital dan tersedia dalam versi komersial maupun freeware.

#### ✦ SSL

SSL singkatan dari Secure Socket Layer adalah metode enkripsi yang dikembangkan oleh Netscape untuk keamanan Internet. SSL mendukung beberapa protokol enkripsi yang berbeda, dan menyediakan autentifikasi client dan server. SSL beroperasi pada layer transport, membuat sebuah kanal data yang terenskripsi sehingga aman, dan dapat mengenkrip berbagai tipe data. Penggunaan SSL sering dijumpai pada saat berkunjung ke sebuah secure site untuk menampilkan sebuah secure document dengan Communicator.

#### ✦ SSH

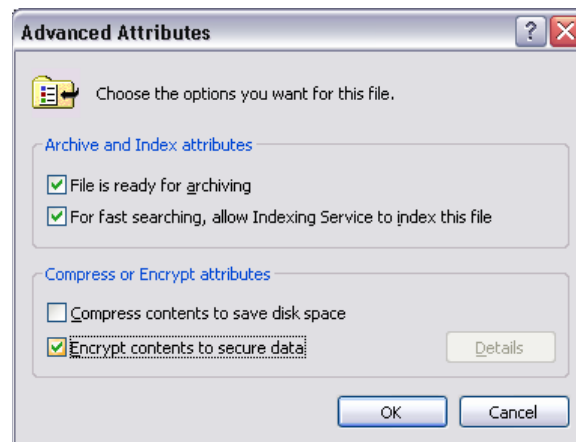
SSH adalah program yang menyediakan koneksi terenskripsi pada saat melakukan login ke suatu remote system. SSH merupakan suatu set program

yang digunakan sebagai pengganti rlogin, rsh, dan rcp dalam segi keamanan. SSH menggunakan kriptografi kunci public untuk mengenkrip komunikasi antara dua host, sehingga juga melakukan autentikasi terhadap user. SSH dapat digunakan untuk mengamankan proses login ke suatu remote system atau menyalin data antar host, karena mencegah terjadinya pembajakan sesi. SSH melakukan kompresi data [ada koneksi yang terjadi, dan mengamankan komunikasi X11 (untuk sistem berbasis Unix) antar host.

SSH dapat digunakan dari workstation dengan sistem windows dengan server berbasis unix.

Berikut ini adalah cara-cara yang dapat dilakukan dalam mengenkripsi sebuah file di sistem operasi Microsoft Windows:

- Klik kanan pada file yang ingin dienkripsi
- Klik **Properties**
- Klik tab **General**
- Tekan tombol **Advanced**
- Beri tanda check pada **Encrypt contents to secure data**



- Kemudian tekan tombol **OK**

Jika file hasil enkripsi tersebut disalin dan dibuka oleh user lain, maka akan muncul pesan error seperti

- Username does not have access privileges, atau
- Error copying file or folder

## **Memonitor Jaringan**

Ancaman pada jaringan yang perlu dimonitoring dan diwaspadai oleh administrator jaringan antara lain adalah sebagai berikut:

- Program perusak seperti virus, trojan, worm, dsb.

Virus dan program perusak lain memiliki kemungkinan yang besar untuk dapat membahayakan keamanan suatu jaringan. Salah satu hal yang dapat dilakukan oleh administrator jaringan adalah melakukan instalasi program antivirus pada workstation.

Perangkat anti virus memiliki fungsi untuk mendefinisikan dan membasmi virus, worm, trojan yang akan masuk ke dalam suatu workstation. Perangkat anti virus yang dapat digunakan oleh suatu workstation adalah sebagai berikut:

- ✦ Norton AV ([www.norman.com](http://www.norman.com))
- ✦ Kaspersky AV
- ✦ McAfee AV

Akan tetapi, antivirus tidak akan menjadi suatu penangkal yang berguna jika administrator tidak melakukan pembaharuan *virus definition* pada anti virus yang telah diinstal pada workstation.

- Denial of service

Pengertian dari denial of service telah dibahas pada bagian sebelumnya.

- Scanning

Pengertian dari scanning telah dibahas pada bagian sebelumnya.

Untuk meminimalisir penyerangan terhadap keamanan jaringan, hal yang dapat dilakukan administrator dalam memonitoring jaringan sebaiknya adalah dengan membatasi user yang dapat melakukan full-access ke dalam suatu server. Cara paling sederhana adalah dengan memberlakukan wewenang *read only* untuk semua user. Cara lain adalah dengan melakukan pembatasan berdasarkan hal berikut ini:

- MAC Address

Contohnya, user yang dapat melakukan akses secara penuh adalah user yang memiliki alamat `abcd:1020:fa02:1:2:3`.

- IP Address

Contohnya, user yang dapat melakukan akses secara penuh adalah user yang memiliki alamat `192.168.2.1`.

Pemantauan juga dapat dilakukan dengan melakukan pengauditan sistem Log pada server tertentu oleh administrator jaringan. Tujuannya adalah mengidentifikasi gangguan dan ancaman keamanan yang akan terjadi pada jaringan.

Administrator dapat juga menggunakan software seperti NSauditor yang bertujuan untuk mengevaluasi keamanan jaringan dan dapat melakukan audit untuk penanggulangan kesalahan.

Selain NSauditor, ada pula tools yang lain yang dapat digunakan untuk mendiagnosis seperti:

- GFI Network Server Monitoring

- MRTG

Selain perangkat lunak, perangkat keras pun perlu dilakukan monitoring. Hal apakah yang perlu diperhatikan dalam monitoring perangkat keras antara lain adalah sebagai berikut:

- Waktu respon perangkat keras

- Kompatibilitas dengan perangkat lunak

Pada sistem operasi tertentu perlu dirancang sistem monitoring yang bersifat user friendly, seperti merancang sistem monitoring berbasis web (misalnya menggunakan PHP dan Apache, dengan browser dan Linux kernel 2.4.xx). Untuk dapat menerapkan sistem monitoring berbasis web ada dua hal yang perlu diperhatikan, sebagai berikut:

- ✦ Koneksi ke internet atau intranet
- ✦ Kompatibilitas dengan browser

Metode pemantauan melalui web ini dapat dilakukan melalui protokol HTTP. Akan tetapi protokol ini tidak dijamin keamanannya, karena itu perlu dilakukan pengenkripsian informasi yang dikirim melalui browser dengan menggunakan sebuah enkripsi yang dinamakan dengan SSH.

## Intrusion Detection System

Intrusion Detection System (IDS) adalah sebuah sistem untuk mendeteksi penyalahgunaan jaringan dan sumber daya komputer. IDS memiliki sejumlah sensor yang digunakan untuk mendeteksi penyusupan. Contoh sensor meliputi:

- Sebuah sensor untuk memonitor TCP request
- Log file monitor
- File integrity checker

IDS memiliki diagram blok yang terdiri dari 3 buah modul, sebagai berikut:

- Modul sensor (sensor modul)
- Modul analisis (analyzer modul)
- Modul basis data (database modul)

Sistem IDS bertanggung jawab untuk mengumpulkan data-data dari sensor dan kemudian menganalisisnya untuk diberikan kepada administrator keamanan

jaringan. Tujuannya adalah untuk memberikan peringatan terhadap gangguan pada jaringan.

Teknologi IDS secara umum terbagi menjadi NIDS (Network Intrusion Detection System) dan HIDS (Host Intrusion Detection System). Snort adalah salah satu open source yang baik untuk NIDS. Sistem deteksi Snort terdiri dari sensor dan analyzer.

AIRIDS (Automatic Interactive Reactive Intrusion Detection System) adalah suatu metode keamanan jaringan yang bertujuan untuk membentuk suatu arsitektur sistem keamanan yang terintegrasi. Untuk mewujudkan AIRIDS perlu dirancang komponen-komponen sistem jaringan sebagai berikut:

- IDS
- Sistem firewall
- Sistem basis data

## Latihan

1. Dalam era teknologi informasi saat ini, hampir seluruh informasi yang penting bagi suatu institusi dapat diakses oleh para penggunanya. Akan tetapi keterbukaan akses akan memunculkan berbagai masalah baru. Masalah apa sajakah itu?
  - a. Pemeliharaan validitas dan integritas data/informasi tersebut
  - b. Jaminan ketersediaan informasi bagi pengguna yang berhak
  - c. Pencegahan akses informasi dari yang tidak berhak
  - d. Pencegahan akses sistem dari yang tidak berhak
  - e. Pencegahan akses sistem dan informasi kepada seluruh user
2. Di bawah ini adalah hal-hal yang membahayakan jaringan, kecuali...
  - a. Probe
  - b. Scan

- c. Nsauditor
  - d. Packet Sniffer
  - e. Denial of Service
3. Berikut ini yang tidak termasuk jenis-jenis ancaman pada jaringan yang perlu dimonitoring dan diwaspadai oleh administrator jaringan adalah sebagai berikut, kecuali..
- a. Denial of service
  - b. Scanning
  - c. Intranet
  - d. Trojan
  - e. Virus
4. AIRIDS merupakan suatu metode kewanaman jaringan yang bertujuan untuk membentuk suatu arsitektur sistem keamanan yang terintegrasi. Apakah kepanjangan dari AIRIDS yang tepat?
- a. Autorecovery Interactive Reactive Intrusion Detection System
  - b. Autorecovery Interoperability Reactive Intrusion Detection System
  - c. Automatic Interactive Reactive Intrusion Detection System
  - d. Automatic Interoperability Reactive Intrusion Detection System
  - e. Automatic Interoperability Reactive Intrusion Detection System
5. IDS mempunyai diagram blok yang terdiri dari beberapa modul. Pilihlah modul-modul yang tepat berkaitan dengan hal ini?
- a. Sensor modul
  - b. Unlock modul
  - c. Analyzer modul
  - d. Database modul
  - e. Firewall modul
6. Hal yang dapat dilakukan administrator dalam memonitoring jaringan sebaik dibatasi user yang dapat melakukan full-access ke dalam suatu server. Cara membatasi itu dapat dilakukan berdasarkan apa saja?
- a. Full address
  - b. MAC address

- c. Blank address
  - d. IP address
  - e. Semua pilihan jawaban benar
7. Dalam melakukan pembatasan akses pada jaringan dibagi menjadi beberapa konsep. Sebutkan konsep tersebut dengan tepat?
- a. Internal password authentication
  - b. Server-based password authentication
  - c. Open source password authentication
  - d. Firewall dan Routing Control
  - e. Wonderwall dan Routing Control
8. Password yang baik menjadi bagian yang paling penting namun sederhana dalam keamanan jaringan. Sebagian besar dari masalah network security disebabkan password yang buruk. Untuk cara-cara dalam internal password authentication yang tepat antara lain adalah..
- a. Menonaktifkan TFTP
  - b. Menonaktifkan HTTP
  - c. Dictionary Guessing
  - d. Menggunakan shadow password
  - e. Error logging
9. Perangkat anti virus memiliki fungsi untuk mendefinisikan dan membasami virus yang akan masuk ke dalam suatu workstation. Perangkat anti virus yang dapat digunakan oleh suatu workstation adalah...
- a. Kaspersky
  - b. Norman AV
  - c. Norton AV
  - d. Mandor AV
  - e. Hydro AV
10. Pada OS tertentu perlu dirancang sistem monitoring yang bersifat user friendly, seperti merancang sistem monitoring berbasis web. Memerlukan hal apa saja untuk dapat melakukan monitoring dari web ini?
- a. Kompatibilitas dengan browser

- b. Spesifikasi komputer berteknologi terbaru dengan harga mahal
- c. Koneksi ke internet atau intranet
- d. 1 dan 2 benar
- e. 2 dan 3 benar

# BAB 15

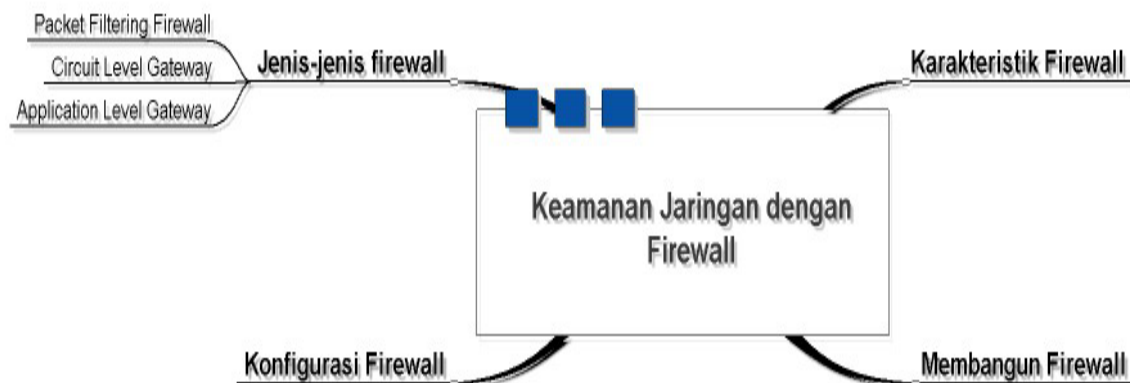
## KEAMANAN JARINGAN DENGAN FIREWALL

### Tujuan Instruksional Umum

- Siswa mampu menjelaskan mengenai firewall

### Tujuan Instruksional Khusus

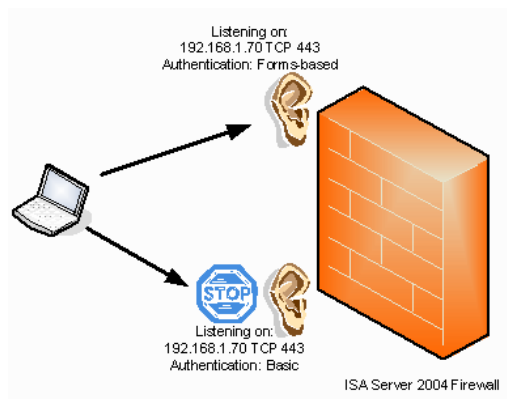
- Siswa mampu menjelaskan secara umum apa itu firewall
- Siswa mampu menyebutkan karakteristik sebuah firewall
- Siswa mampu menyebutkan jenis-jenis firewall
- Siswa mampu menyebutkan metode penyaringan firewall
- Siswa mampu menjelaskan beberapa konfigurasi firewall
- Siswa mampu menjelaskan tahapan dalam membangun sebuah firewall



Gambar 15.1. Rincian Pembelajaran Bab 15

Keamanan adalah hal yang penting dalam segala hal. Selayaknya sebuah rumah memiliki pagar, *server* kita pun membutuhkan 'pagar'. Apalagi *server* selalu terhubung dengan internet. Isu keamanan sangat penting untuk melindungi *server* dan data yang tersimpan di dalamnya. 'Pagar' tersebut bernama "*firewall*" atau "Tembok Api".

*Firewall* merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya. Segmen tersebut dapat merupakan sebuah *workstation*, *server*, *router*, atau *local area network* (LAN) anda.



Gambar 15.2. Firewall

## Karakteristik Firewall

Berikut ini adalah karakteristik dari sebuah firewall:

- Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati *firewall*. Hal ini dapat dilakukan dengan cara memblokir/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati *firewall*. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
- Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan

hubungan, hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis *firewall* yang dapat dipilih sekaligus berbagai jenis *policy* yang ditawarkan.

- *Firewall* itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

## Jenis-jenis Firewall

Ada beberapa jenis firewall, antara lain sebagai berikut:

- *Software Firewall*

*Software Firewall* adalah program yang berjalan pada background komputer. *Software* ini mengevaluasi setiap *request* dari jaringan dan menentukan apakah *request* itu valid atau tidak.

Kelebihan yang dimiliki *software firewall*:

- ⊕ Harganya murah.
- ⊕ Mudah dikonfigurasi.

Kekurangan *software firewall*:

- ⊕ Memakan sumber daya dari komputer (CPU, memory, ruang disk) sehingga dapat menyebabkan inkompatibilitas pada sistem operasi.
- ⊕ Terdapat versi yang berbeda untuk sistem operasi yang berbeda, jadi harus dipastikan bahwa *software firewall* yang diinstall adalah versi yang sesuai dengan sistem operasi Anda.
- ⊕ Dibutuhkan beberapa *copy* yang berbeda untuk tiap sistem dalam jaringan Anda.

- *Hardware Firewall*

*Hardware firewall* adalah *firewall* yang dipasang pada komputer, yang menghubungkan komputer dengan modem.

Kelebihan *hardware firewall*:

- ✦ Menyediakan perlindungan yang lebih banyak dibandingkan dengan *software firewall*. Sebuah *hardware firewall* dapat melindungi keseluruhan jaringan.
- ✦ *Hardware firewall* beroperasi secara independen terhadap sistem operasi dan aplikasi perangkat lunak sehingga kinerja sistem tidak akan terganggu.

Kekurangan *hardware firewall*:

- ✦ Cenderung lebih mahal dari *software firewall*. Namun, jika Anda memiliki beberapa mesin yang harus dilindungi akan lebih murah untuk membeli satu *hardware firewall* dibandingkan membeli beberapa *copy* dari sebuah *software firewall*.
- ✦ Karena tidak berjalan independen, konfigurasi *hardware firewall* cukup sulit.

Untuk metode yang digunakan dalam penyaringan, ada beberapa metode pemfilteran yang dapat dilakukan oleh sebuah firewall, antara lain sebagai berikut:

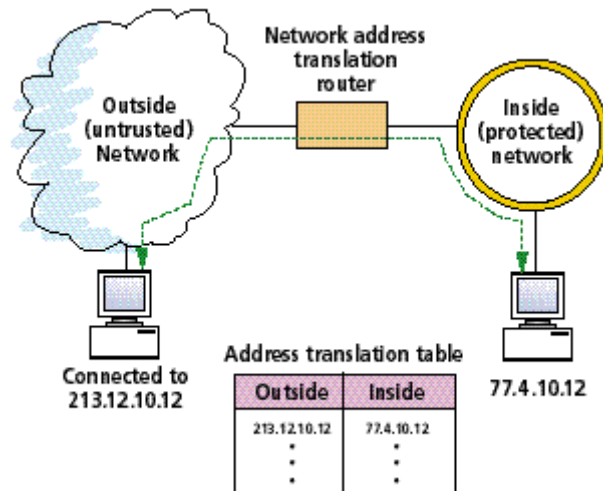
- Circuit level gateway
- Application level gateway
- Packet filtering firewall
- Stateful Multilayer Inspection Firewall

## **Packet Filtering Firewall**

Dalam packet filtering firewall, firewall menguji lima karakteristik dari sebuah paket, yaitu:

- Alamat IP sumber
- Port sumber
- Alamat IP tujuan

- Port tujuan
- Protokol IP (TCP atau UDP)



Gambar 15.3. Packet Filtering Firewall

Berdasarkan aturan yang telah dikonfigurasi ke dalam firewall, paket akan diizinkan untuk lewat atau ditolak. Jika firewall menolak paket, maka firewall akan mengirimkan pesan ke pengirim untuk memberi tahu bahwa paketnya telah ditolak. Routers adalah bentuk yang paling umum dari metode packet filtering firewall ini.

### Circuit Level Gateway

Circuit Level gateway memonitor TCP handshaking antar paket dari klien atau server yang dipercaya ke host yang tidak dipercaya dan sebaliknya, untuk mengetahui apakah session yang diminta itu sah. Dalam menyaring paket dengan menggunakan cara ini, circuit level gateway bergantung kepada data yang terkandung pada header paket.

Untuk menentukan apakah session yang diminta itu sah, circuit level gateway menggunakan proses sebagai berikut:

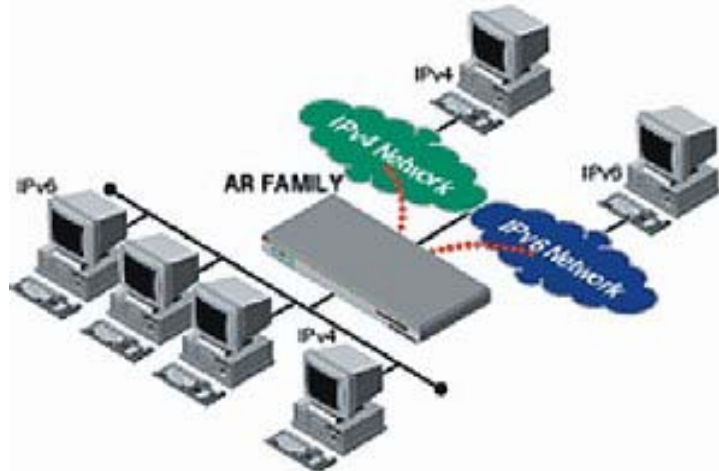
- Client yang dipercaya meminta sebuah servis

- Gateway menerima servis tersebut dengan asumsi bahwa client memenuhi criteria dasar penyaringan
- Gateway membuka sebuah koneksi ke host yang tidak dipercaya
- Gateway memonitor TCP handshaking yang terjadi
- Request session dinyatakan sah hanya pada kondisi tertentu pada session
- Setelah gateway menyatakan sah, gateway akan membangun sebuah koneksi.
- Dari sini, circuit level gateway tinggal menyalin dan meneruskan paket tanpa melakukan penyaringan kembali.

Gateway memiliki sebuah tabel yang mencatat koneksi yang sedang terbangun, yang akan mengizinkan data untuk diteruskan jika informasi sessionnya berada dalam tabel. Ketika session selesai, gateway akan menghilangkan informasi tersebut pada tabel.

### **Application Level Gateway**

Application-level gateway (gateway yang bekerja pada layer aplikasi pada layer-layer OSI) dapat menangani proses store-and-forward- terhadap lalu lintas jaringan. Application level gateway deprogram untuk mengerti lalu lintas pada layer 7 model OSI, sehingga application level gateway ini menyediakan control terhadap akses pada level user dan level protocol aplikasi. Lebih jauh lagi, application-level gateway ini dapat digunakan untuk mengelola secara cerdas semua penggunaan aplikasi. Kemampuan untuk melakukan log dan control terhadap semua lalu lintas yang keluar atau masuk adalah salah satu kelebihan utama dari application-level gateway. Gateway tersebut memiliki sistem keamanan tambahan di dalamnya yang dibangun sesuai dengan kebutuhan.



Gambar 15.4. Application Level Gateway

Untuk tiap aplikasi yang di relay, application level gateay menggunakan kode khusus. Karena kode khusus inilah application-level gateway menyediakan level keamanan yang tinggi, Untuk tiap jenis aplikasi yang ditambahkan ke jaringan (dan membutuhkan proteksi), maka dibutuhkan kode khusus yang baru untuk aplikasi tersebut. Sehingga, kebanyakan application level gateway menyediakan suatu subset yang terbatas untuk aplikasi-apliaksi dan servis-servis dasar.

## Konfigurasi Firewall

Ada beberapa konfigurasi firewall, sebagai berikut:

### ■ *Screened Host Firewall system (single-homed bastion)*

Pada konfigurasi ini, fungsi *firewall* akan dilakukan oleh *packet filtering router* dan *bastion host*<sup>1</sup>). *Router* ini dikonfigurasi sedemikian rupa sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju *bastion host* yang diijinkan. Sedangkan untuk arus data (*traffic*) dari jaringan internal, hanya paket IP dari *bastion host* yang diijinkan untuk keluar.

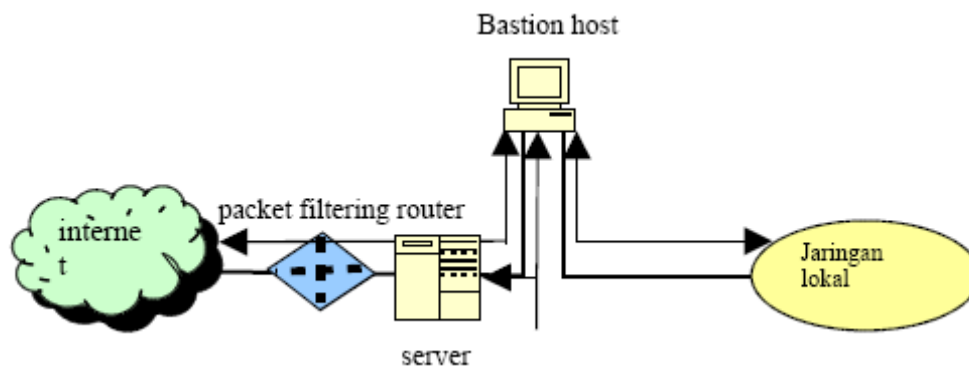
Konfigurasi ini mendukung fleksibilitas dalam akses internet secara langsung, sebagai contoh apabila terdapat *web server* pada jaringan ini maka dapat dikonfigurasi agar *web server* dapat diakses langsung dari internet.

*Bastion host*<sup>8</sup> melakukan fungsi autentikasi dan fungsi sebagai *proxy*. Konfigurasi ini memberikan

tingkat keamanan yang lebih baik daripada *packet-filtering router* atau *application-level gateway* secara terpisah.

#### ■ *Screened Host Firewall system (Dual-homed bastion)*

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya dibanding konfigurasi pertama, adapun untuk server-server yang memerlukan direct access (akses dengan adanya dua jalur yang memisahkan secara fisik maka akan lebih meningkatkan keamanan langsung) maka dapat diletakkan di tempat/segment yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (*network interface card*) pada *bastion host*.



Gambar 15.5. Screened Host Firewall System (Dual-homed Bastion)

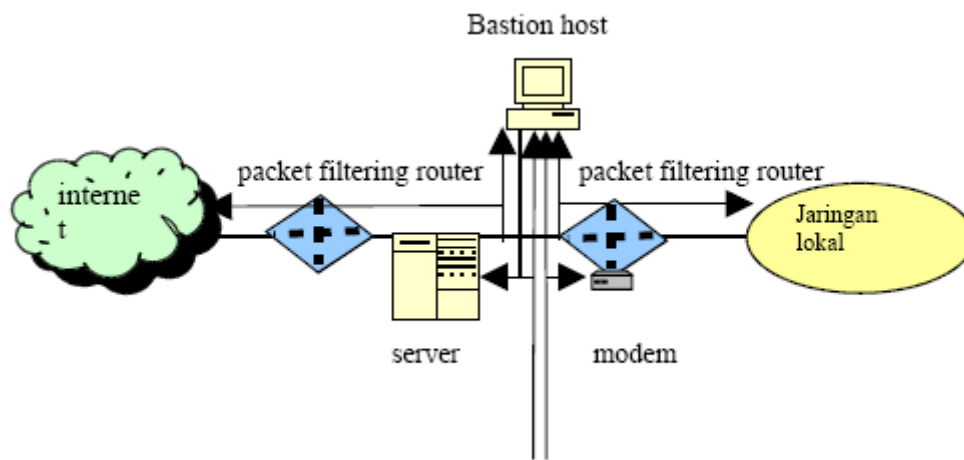
#### ■ *Screened subnet firewall*

Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. Karena pada konfigurasi ini digunakan 2 buah *packet filtering router*, salah satunya terletak di

---

<sup>8</sup>Bastion Host adalah sistem/bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator atau dapat disebut bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen *firewall* atau bagian terluar sistem publik. Umumnya *bastion host* akan menggunakan sistem operasi yang dapat menangani semua kebutuhan (misal, Unix, linux, NT).

antara internet dan *bastion host*, sedangkan sisanya terletak di antara *bastion host* dan jaringan lokal. Konfigurasi ini membentuk *subnet* yang terisolasi.



Gambar 15.6. Screened Subnet Firewall

Adapun kelebihanannya adalah :

- ✦ Terdapat 3 lapisan/tingkat pertahanan terhadap penyusup/*intruder* .
- ✦ *Router* luar hanya melayani hubungan antara internet dan *bastion host* sehingga jaringan lokal menjadi tak terlihat (*invisible*)
- ✦ Jaringan lokal tidak dapat mengkonstruksi *routing* langsung ke internet, atau dengan kata lain, internet menjadi *invisible* (bukan berarti tidak bisa melakukan koneksi internet).

## Membangun Firewall

Ada beberapa langkah yang dilakukan dalam membangun sebuah firewall. Caranya adalah dengan melakukan tahapan sebagai berikut:

- Mengidentifikasi bentuk jaringan yang dimiliki

Mengetahui bentuk jaringan yang dimiliki khususnya topologi yang digunakan serta protokol jaringan, akan memudahkan dalam mendesain sebuah firewall

- Menentukan *Policy* atau kebijakan

Penentuan kebijakan atau *policy* merupakan hal yang harus dilakukan. Baik atau buruknya sebuah *firewall* yang dibangun sangat ditentukan oleh *policy*/kebijakan yang diterapkan. Diantaranya adalah sebagai berikut:

- ✦ Menentukan apa saja yang perlu dilayani. Artinya, apa saja yang akan dikenai *policy* atau kebijakan yang akan kita buat
- ✦ Menentukan individu atau kelompok-kelompok yang akan dikenakan *policy* atau kebijakan tersebut
- ✦ Menentukan layanan-layanan yang dibutuhkan oleh setiap individu atau kelompok yang menggunakan jaringan
- ✦ Berdasarkan setiap layanan yang digunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
- ✦ Menerapkan semua *policy* atau kebijakan tersebut

#### ■ Menyiapkan Software atau Hardware yang akan digunakan

Baik itu sistem operasi yang mendukung atau perangkat lunak khusus pendukung *firewall* seperti *ipchains*, atau *iptables* pada linux, dsb. Serta konfigurasi *hardware* yang akan mendukung *firewall* tersebut.

Sistem operasi yang dapat mendukung firewall antara lain adalah sebagai berikut:

- ✦ Windows XP
- ✦ FreeBSD 5.2
- ✦ Fedora 9.0

#### ■ Melakukan test konfigurasi

Pengujian terhadap *firewall* yang telah selesai dibangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan *tools* yang biasa dilakukan untuk mengaudit seperti *nmap*.

## Latihan

1. Di bawah ini yang bukan metode pemfilteran yang dapat dilakukan oleh Firewall adalah..
  - a. Circuit level gateway
  - b. Application level gateway
  - c. Packet filtering firewall
  - d. Open source password authentication
  - e. Stateful Multilayer Inspection Firewall
  
2. **Benar atau salah**, seluruh hubungan/kegiatan dari dalam ke luar, harus melewati *firewall*
  
3. Program yang berjalan pada background komputer, yang bertugas mengevaluasi setiap *request* dari jaringan dan menentukan apakah *request* itu valid atau tidak. Program tersebut disebut dengan..
  - a. Hardware Firewall
  - b. Software Firewall
  - c. Circuit level gateway
  - d. Packet filtering firewall
  
4. Berikut ini adalah jenis Operating System yang dapat digunakan untuk mengendalikan Firewall yang telah dibuat antara lain..
  - a. Windows XP
  - b. FreeBSD 5.2
  - c. AMD Sempron
  - d. Fedora 9.0
  - e. SQUID

5. Di bawah ini yang merupakan jenis konfigurasi firewall adalah..
- a. *Screened Host Firewall system (single-homed bastion)*
  - b. *Screened Host Firewall system (Dual-homed bastion)*
  - c. *Screened subnet firewall*
  - d. Semua Benar
  - e. Semua Salah

# **BAB 16**

## **PERAWATAN DAN PEMELIHARAAN JARINGAN**

### **Tujuan Instruksional Umum**

- Siswa mampu melakukan perawatan dan pemeliharaan jaringan

### **Tujuan Instruksional Khusus**

- Siswa mampu menentukan strategi perawatan
- Siswa mampu menjelaskan mengenai SLA
- Siswa mampu menyebutkan metode identifikasi masalah
- Siswa mampu melakukan perawatan perangkat keras jaringan
- Siswa mampu melakukan perawatan lunak jaringan
- Siswa mampu menjelaskan latar belakang tentang modifikasi sistem
- Siswa mampu menyebutkan langkah-langkah dalam koreksi kesalahan sistem
- Siswa mampu menyebutkan langkah-langkah dalam pengembangan sistem
- Siswa mampu menjelaskan dampak dari pengembangan sistem



Gambar 16.1. Rincian Pembelajaran Bab 16

Memiliki sebuah jaringan bukanlah suatu hal yang murah. Banyak komponen-komponen jaringan yang harus dibeli dengan biaya yang cukup besar. Semakin luas jaringan, semakin banyak komponen jaringan dan semakin besar biaya yang dibutuhkan.

Bagi sebuah perusahaan, koneksi Internet menjadi sebuah bagian yang penting dalam bisnis. Terputusnya koneksi Internet dapat mengakibatkan kerugian, sebagai berikut:

- Terhambatnya proses pelaksanaan bisnis suatu perusahaan
- Tertundanya beberapa pekerjaan yang dapat mengakibatkan kerugian materi

Dari penjelasan di atas, dapat diambil sebuah kesimpulan bahwa jaringan adalah suatu asset yang berharga. Oleh karena itu, diperlukan suatu perawatan dan pemeliharaan jaringan. Tujuannya adalah agar komponen-komponen jaringan tidak cepat rusak, dan dapat bertahan cukup lama. Selain itu perawatan dan pemeliharaan juga dilakukan agar jaringan dapat terus digunakan sebagaimana mestinya.

## Menentukan Strategi Perawatan

Seperti yang telah dijelaskan di atas, perawatan jaringan perlu dilakukan. Mengaudit suatu peralatan jaringan perlu dilakukan jika informasi tentang itu belum tersedia. Peralatan jaringan yang diaudit meliputi Ethernet Card, Hub, Switch, Router, dan peralatan jaringan lainnya.

Suatu strategi-strategi perawatan untuk menjaga kontinuitas operasi IT dan fungsi bisnis diidentifikasi berdasarkan faktor, faktor tersebut antara lain adalah sebagai berikut:

- Anggaran
- Kebutuhan bisnis
- Persyaratan SLA

Untuk itu dalam menguji suatu strategi perawatan perlu mempertimbangkan beberapa faktor di atas. Jadwal perawatan komponen jaringan juga harus dilakukan dan dipertimbangkan berdasarkan faktor-faktor di atas.

Dalam strategi perawatan jaringan, suatu dokumentasi arsitektur dan konfigurasi sistem jaringan juga perlu ditinjau kembali. Tujuan dilakukan pemberian informasi ini adalah untuk menyediakan suatu informasi terbaru sehingga dapat dilakukan suatu penanganan yang mudah jika terjadi suatu kerusakan atau kesalahan dalam jaringan.

### **SLA**

SLA atau yang dikenal dengan perjanjian tingkat layanan adalah perjanjian formal antara Service Provider dengan pelanggan untuk menetapkan suatu level pelayanan (QoS) tertentu. SLA disiapkan untuk mencocokkan pengguna dengan persyaratan bisnis.

SLA perlu dipersiapkan untuk sesuai dengan parameter yang berlaku. Beberapa parameter yang dapat mempengaruhi SLA untuk layanan voice adalah sebagai berikut :

- Paket loss
- Delay
- Jitter
- Throughput

## Help Desk

Help desk dan fungsi dukungan lain diatur menurut prosedur dan standar yang disetujui dan sesuai dengan praktek terbaik yang ada di industri. Help Desk adalah suatu sistem pendukung yang didesain untuk menuntun pelanggan dengan jawaban teknis dan fungsional. Help Desk sangat membantu bagi pelanggan yang ingin mengadakan suatu kerusakan pada jaringan.

## Metode Identifikasi Masalah

Ada 2 cara yang dapat dilakukan untuk mengidentifikasi masalah dalam sistem jaringan, sebagai berikut:

- Metode Penelusuran Kesalahan

Metode ini melakukan pelacakan hal-hal yang menyebabkan terjadinya kesalahan pada sistem jaringan hingga dapat menemukan solusi yang tepat.

- Metode *Try and Error*

Metode ini melakukan percobaan dan mencatat hasil yang dikeluarkan untuk menemukan pemecahan dalam menangani masalah yang timbul.

Berikut ini adalah contoh-contoh kasus pada jaringan dan tindakan yang harus dilakukan.

Kasus	Tindakan
Suatu server yang berfungsi untuk melakukan resolver dari nama domain ke IP address pada jaringan sedang mati atau down	Merestart kembali daemon DNS untuk diaktifkan
Suatu server pada jaringan sedang mati atau down sehingga para klien tidak dapat mendapatkan IP dinamis dari server tersebut	Merestart kembali daemon DHCP untuk diaktifkan
Suatu server yang berfungsi untuk mengelola halaman suatu situs pada jaringan sedang mati atau down	Merestart kembali daemon APACHE untuk diaktifkan

## Perawatan Perangkat Jaringan

Seperti yang telah dijelaskan di atas, ada dua buah perangkat dalam jaringan:

- Perangkat Keras
- Perangkat Lunak

### Perawatan Perangkat Keras

Berikut ini adalah cara-cara dalam melakukan perawatan perangkat keras jaringan agar jaringan dapat beroperasi dengan baik:

- Membersihkan setiap perangkat keras jaringan dari debu yang menumpuk
- Melakukan penyusunan kabel LAN secara teratur untuk mudah dalam melakukan penelusuran kesalahan. Oleh karena itu kabel LAN biasanya diberikan sebuah label.
- Memastikan antena yang terhubung ke ISP tidak berubah posisi dari posisi semula dan berada pada kondisi Line Of Sight.

Apabila terjadi kesalahan dalam pengkabelan, dapat digunakan alat yang bernama LAN tester. Fungsi dari alat ini adalah untuk menguji redaman suatu kabel LAN, maupun struktur kabel tersebut.



Gambar 16.2. LAN Tester

Apabila diketahui bahwa kesalahan disebabkan oleh rusaknya hub sehingga beberapa user terganggu aktifitasnya. Komponen Switch dapat digunakan sementara untuk mengatasi hal tersebut. Sedangkan apabila diketahui bahwa kesalahan disebabkan oleh rusaknya router pinjaman dari ISP sehingga semua user yang tergabung dalam jaringan tersebut terganggu aktifitasnya, maka PC Router dapat digunakan sementara untuk meminimalkan gangguan tersebut.

Sementara itu untuk dapat menguji konektifitas dan kinerja access point sehingga dapat memonitor sedang dalam kondisi apa AP tersebut, dapat menggunakan sebuah software yang bernama netstumbler.

Akan tetapi ada keterbatasan dalam melakukan perawatan dan pemeliharaan jaringan. Ada prosedur-prosedur perawatan yang tidak dapat dilakukan oleh internal, contohnya antara lain sebagai berikut:

- Penginstallan Antena AP yang dipinjamkan oleh pihak ISP yang terletak pada kantor ISP tersebut
- Penginstallan kabel serat optik yang akan digunakan sebagai media penghubung dari ISP ke pelanggan

Sedangkan prosedur perawatan yang dapat dilakukan secara internal contohnya antara lain adalah sebagai berikut:

- Pembersihan komponen jaringan dari debu dan kotoran lainnya
- Pembuatan dan penjagaan firewall untuk kepentingan perusahaan

## **Perawatan Perangkat Lunak**

Berikut ini adalah cara-cara dalam melakukan perawatan perangkat lunak jaringan agar jaringan dapat beroperasi dengan baik:

- Tidak melakukan perangkat lunak yang memakan memori besar pada komputer yang berfungsi untuk memonitoring kondisi jaringan. Perangkat lunak yang memakan memori besar antara lain adalah game.
- Selalu memperbaharui kompatibilitas perangkat lunak dengan perangkat keras

Rekomendasi pencegahan atau deteksi dini dari masalah-masalah yang sama pada peralatan dan perangkat lunak di buat. Hal ini bertujuan agar penyelesaian untuk masalah-masalah yang sama dapat dilakukan dengan cepat.

## **Dokumentasi Perawatan**

Dokumentasi hasil perawatan perangkat keras dan lunak dibuat untuk melengkapi persyaratan standar proyek. Seiring dengan perkembangan teknologi, dokumentasi yang dibuat secara digital memiliki kelebihan dibandingkan dokumentasi secara manual. Contoh dari format digital adalah dengan membuat dokumen berformat .txt, .doc, atau .pdf.

Tujuan dari digitalisasi tersebut antara lain adalah sebagai berikut:

- Untuk melancarkan pengembangan yang sistematis tentang cara mengumpulkan, menyimpan, dan mengorganisasi informasi dan pengetahuan dalam format digital
- Untuk mengembangkan pengiriman informasi yang hemat dan efisien di semua sektor
- Untuk mendorong upaya kerjasama yang sangat mempengaruhi investasi pada sumber-sumber penelitian dan jaringan komunikasi

Laporan kesalahan dalam bentuk digital tersebut sebaiknya juga dicetak dan ditempatkan pada dekat komponen jaringan sehingga dapat meminimalisasi waktu yang terbuang akibat kecelakaan atau kerusakan pada jaringan.

## Pembaharuan Jaringan

Seiring dengan berkembangnya teknologi, banyak komponen jaringan yang muncul dengan tujuan untuk meningkatkan kinerja jaringan menjadi lebih baik lagi. Agar dapat bersaing, terkadang perusahaan harus selalu melakukan pembaharuan dalam teknologi jaringan, baik komponen maupun sistemnya.

Pembaharuan juga dibutuhkan ketika sistem yang lama sudah dinilai tidak layak lagi. Ketidaklayakan tersebut dapat dipandang dari segi kesalahan yang terjadi akibat sistem lama tersebut, maupun ketidaksesuaian dengan kebutuhan bisnis perusahaan saat ini dan di masa yang akan datang. Hal ini tentu membutuhkan suatu perubahan sistem. Untuk dapat memenuhi permintaan perubahan suatu sistem, laporan kesalahan dan laporan help desk perlu dikumpulkan dan ditinjau terlebih dahulu. Tujuannya adalah sebagai berikut:

- Untuk dijadikan sebagai bahan pertimbangan dalam proses pengerjaan permintaan perubahan sistem
- Agar dapat menjalankan permintaan secara terstruktur sesuai dengan laporan dan permintaan yang ada

### **Modifikasi Sistem**

Yang merupakan modifikasi suatu sistem antara lain sebagai berikut:

- Koreksi kesalahan sistem
- Perbaikan sistem
- Pengembangan sistem

Staf yang tepat ditugasi dalam pelaksanaan modifikasi sistem jaringan adalah sebagai berikut:

- Administrator
- IT technical support
- Provider jaringan

Sedangkan jika ingin melakukan modifikasi pada sistem operasi jaringan, tugas tersebut lebih tepat diserahkan pada administrator atau programmer.

## **Koreksi Kesalahan Sistem**

Berikut ini adalah langkah-langkah yang dapat dilakukan dalam melakukan koreksi sistem komputer.

- Memeriksa log sistem

Biasanya sistem melakukan pencatatan ke dalam log jika sistem mengalami error. Selain agar dapat dikoreksi, laporan kesalahan juga diperlukan untuk mengidentifikasi perubahan sistem jaringan.

- Melakukan pencarian kesalahan

- Membenahi dan membetulkan sistem yang salah

## **Pengembangan Sistem**

Langkah-langkah yang dilakukan dalam pengembangan sistem adalah sebagai berikut:

- Menilai kelayakan sistem

- Memperbaharui seluruh komponen dalam sistem

- Menyelaraskan dengan standarisasi teknologi yang baru

## **Dampak**

Ketika implementasi baru dilakukan dengan tujuan untuk pembaharuan jaringan, tentu akan membawa dampak sementara bagi jaringan. Contoh dampak terhadap basis pengguna antara lain adalah sebagai berikut:

- Pemadaman jaringan sementara waktu

- User akan off-line sementara waktu

Sedangkan perubahan yang terjadi ketika terjadi migrasi dari jaringan kabel ke jaringan nirkabel antara lain adalah sebagai berikut:

- Perubahan perangkat jaringan
- Perubahan kecepatan data

Sementara itu, suatu perubahan dalam bentuk apapun termasuk topologi jaringan perlu dilakukan klarifikasi kepada para pengguna jaringan agar tidak mengganggu kinerja perusahaan.

Ada beberapa hal yang harus dilakukan sebagai tindak lanjut dari perubahan sistem jaringan, sebagai berikut:

- Dokumentasi

Apabila suatu perubahan desain jaringan telah terbentuk maka perlu dibuatkan suatu dokumen teknis atau dokumen pemakaian. Tujuannya adalah menjadi pedoman tuntunan penjelasan perubahan suatu sistem jaringan. Format dari dokumentasi ini adalah sebagai berikut:

- ⊕ Menjabarkan topologi jaringan dan penjelasannya dengan bahasa yang mudah dimengerti
- ⊕ Cara-cara standar seperti merubah IP komputer klien sesuai dengan topologi jaringan didefinisikan

- Pelatihan

Pelatihan disiapkan untuk memenuhi kebutuhan pelatihan klien terhadap permintaan perubahan sistem. Contoh bahan-bahan yang perlu dipersiapkan dalam suatu pelatihan tersebut antara lain adalah sebagai berikut:

- ⊕ Pengenalan dasar topologi jaringan
- ⊕ Cara memberikan IP ke komputer masing-masing
- ⊕ Troubleshooting apabila komputer klien tidak dapat terhubung ke jaringan

Suatu pelatihan kepada klien tidak dapat dilakukan secara bersamaan untuk seluruh bagian-bagian dalam perusahaan karena itu dalam pelaksanaannya perlu dibuatkan jadwal untuk tiap-tiap bagian sesuai dengan materi yang akan diberikan.

## Latihan

1. Cara apakah yang digunakan untuk merawat perangkat keras sistem jaringan yang benar agar dapat tetap beroperasi?
  - a. Membersihkan setiap perangkat keras jaringan dari debu yang menumpuk
  - b. Menjual perangkat keras yang sudah berdebu tebal dengan harga mahal
  - c. Melakukan penyusunan kabel LAN secara teratur untuk mudah dalam melakukan penelusuran kesalahan
  - d. Memastikan antena yang terhubung ke ISP tidak berubah posisi dari posisi semula dan berada pada kondisi Line Of Sight
  - e. Tidak ada pilihan jawaban yang benar
  
2. Cara apakah yang digunakan untuk merawat perangkat lunak sistem jaringan yang benar agar dapat tetap beroperasi?
  - a. Menjual perangkat lunak kepada masyarakat umum untuk mendapatkan keuntungan tambahan
  - b. Selalu meng-update kompatibilitas perangkat lunak dengan perangkat keras
  - c. Diizinkan menginstall perangkat lunak seperti game yang memakan memori besar pada komputer yang berfungsi untuk memonitoring kondisi jaringan
  - d. Dilarang menginstall perangkat lunak seperti game yang memakan memori besar pada komputer yang berfungsi untuk memonitoring kondisi jaringan
  - e. Semua pilihan jawaban benar
  
3. Berikut ini manakah suatu prosedur yang dapat ditangani pihak internal perusahaan dalam merawat dan menjaga sistem jaringan?

- a. Penginstallan Antena AP yang dipinjamkan oleh pihak ISP yang terletak pada kantor ISP tersebut
  - b. Pembersihan komponen jaringan dari debu dan kotoran lainnya
  - c. Pembuatan dan penjagaan firewall untuk kepentingan perusahaan
  - d. Penginstallan kabel serat optik yang akan digunakan sebagai media penghubung dari ISP ke pelanggan
  - e. Perawatan kebersihan kantor beserta seluruh isinya
4. Langkah-langkah dalam melakukan koreksi kesalahan dalam sistem komputer adalah..
- a. Menginterogasi user
  - b. Memeriksa log sistim
  - c. Melakukan pencarian kesalahan
  - d. Memformat seluruh sistem
  - e. Membenahi dan membetulkan sistem yang salah
5. Dampak yang akan berpengaruh terhadap jaringan ketika terjadi perubahan letak storage adalah..
- a. Alamat dari storage akan dikonfigurasi ulang
  - b. Jaringan di konfigurasi ulang
  - c. User akan kebingungan
  - d. Jaringan akan down dalam beberapa saat
  - e. Perubahan topologi jaringan
6. Dokumentasi hasil perawatan perangkat keras dan lunak dibuat untuk melengkapi persyaratan standar proyek. Karena perkembangan teknologi format pembuatan itu dapat dilakukan secara digital. Tujuan dari digitalisasi ini adalah..
- a. Untuk formalitas prosedur kerja yang berlaku pada era teknologi modern saat ini

- b. Untuk melancarkan pengembangan yang sistematis tentang cara mengumpulkan, menyimpan, dan mengorganisasi informasi dan pengetahuan dalam format digital
  - c. Untuk mengembangkan pengiriman informasi yang hemat dan efisien di semua sektor
  - d. Untuk menciptakan sistem yang membutuhkan tingkat pengeluaran dana yang besar
  - e. Untuk mendorong upaya kerjasama yang sangat mempengaruhi investasi pada sumber-sumber penelitian dan jaringan komunikasi
7. Berikut ini adalah suatu metode yang dapat digunakan untuk mengidentifikasi masalah dalam sistem jaringan antara lain..
- a. Metode try and error
  - b. Metode penelusuran kesalahan sistem
  - c. Metode born to cook
  - d. Metode Chatting online
  - e. Metode Menanam bunga

# BAB 17

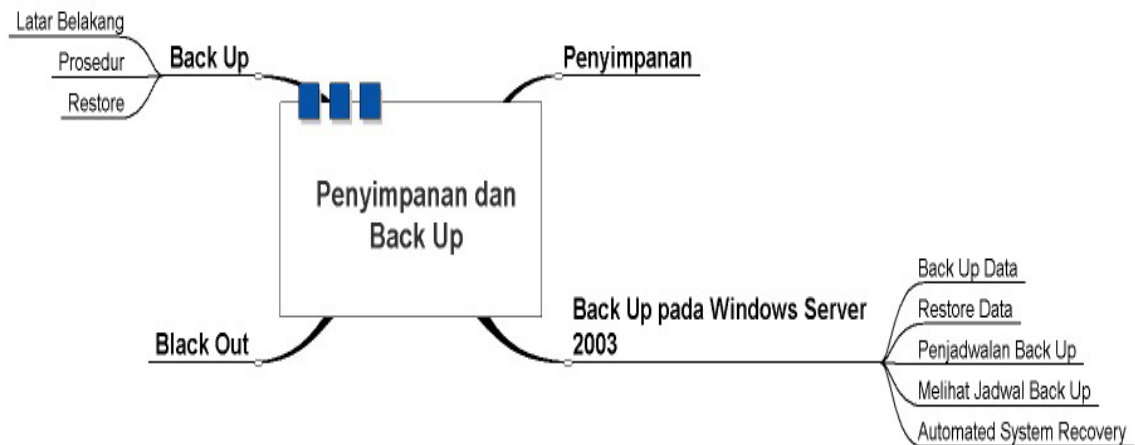
## PENYIMPANAN DAN BACK UP

### Tujuan Instruksional Umum

- Siswa mampu menjelaskan tentang penyimpanan dan back-up.

### Tujuan Instruksional Khusus

- Siswa mampu menjelaskan tentang penyimpanan
- Siswa mampu menjelaskan latar belakang back-up
- Siswa mampu menyebutkan prosedur back-up
- Siswa mampu menjelaskan mengenai restore
- Siswa mampu melakukan back-up data pada Windows Server 2003
- Siswa mampu melakukan restore data pada Windows Server 2003
- Siswa mampu melakukan penjadwalan back-up pada Windows Server 2003
- Siswa mampu menjelaskan automated system recovery
- Siswa mampu menjelaskan mengenai black out



Gambar 17.1. Rincian Pembelajaran Bab 17

Pengaturan penyimpanan dan back up juga termasuk dalam upaya perawatan dan pemeliharaan sistem jaringan. Pada bab ini akan dibahas secara lebih dalam mengenai hal tersebut, khususnya back up pada sistem operasi Windows Server 2003.

## Penyimpanan

Keberadaan tempat penyimpanan (storage) pada sistem komputer sangat berguna dalam proses penanganan kesalahan sistem. Dengan adanya penyimpanan, terkadang dapat diketahui jenis kesalahan yang terjadi atau bagaimana cara menangani suatu kesalahan. Penyimpanan tersebut meliputi hal-hal sebagai berikut:

- Penyimpanan dokumentasi tiap user
- Penyimpanan data
- Penyimpanan program
- Penyimpanan komponen dari sistem

Dalam perawatan jaringan, perubahan atau pengembangan dapat terjadi pada penyimpanan. Perubahan tersebut antara lain adalah sebagai berikut:

- Perubahan kapasitas dari storage tersebut
- Perubahan letak dari storage tersebut

Sementara itu dampak dari perubahan storage terhadap jaringan antara lain adalah sebagai berikut:

- Jaringan akan dimatikan dan down dalam beberapa saat
- Alamat dari storage akan dikonfigurasi ulang (untuk perubahan letak storage)

Penyimpanan juga dapat dilakukan melalui jaringan berbasis IP. Salah satu keuntungan dari network storage berbasis IP adalah membuat pelanggan dapat memilih arsitektur penyimpanan baik tersebar (distributed), maupun terpusat (centralized).

## Back-Up

## Latar Belakang

Penyimpanan (storage) saat ini merupakan hal yang sangat penting, terutama di dunia bisnis. Dalam sebuah media penyimpanan, dapat berisi data dan informasi yang penting.

Suatu media penyimpanan suatu ketika dapat dikatakan menjadi suatu bencana jika:

- Data dan informasi yang berada di dalamnya mengalami perubahan yang tidak dapat dipertanggungjawabkan kebenarannya (mis: kesalahan perubahan data yang sangat fatal).
- Data dan informasi yang berada di dalamnya rusak karena bencana, seperti berikut:
  - ⊕ Virus
  - ⊕ Bencana Alam (mis: Tsunami, Kebakaran, Banjir, dll)
  - ⊕ Sistem downtime

Karena alasan tersebut, suatu sistem back-up data mutlak diperlukan. Hal ini bertujuan agar data dan informasi lama dapat dikembalikan seperti keadaan semula.

## Prosedur Back-up

Prosedur back-up digunakan oleh perusahaan untuk mengantisipasi terjadinya perubahan yang terjadi pada storage. Caranya adalah dengan membuat salinan atau copy terhadap data dan informasi yang terdapat pada storage ke media tertentu. Media tersebut antara lain sebagai berikut:

- Hard Disk Eksternal
- Flash Disk
- CD / DVD
- Floppy Disk
- Lain-lain

Proses yang terjadi pada saat back-up sistem jaringan adalah sebagai berikut:

- Memilih data yang akan di back-up

- Menghubungkan dengan media penyimpanan (storage)
- Pemilihan media penyimpanan untuk back-up

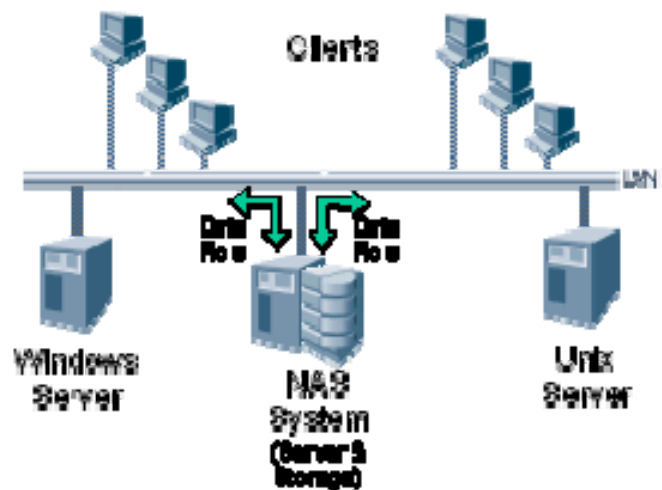
Prosedur back-up baru yang dikembangkan dalam mengantisipasi perubahan yang terjadi pada storage ialah sebagai berikut:

- Melakukan perubahan address storage pada saat menyimpan
- Melakukan koneksi kembali pada storage yang telah berpindah tempat

Back-up dapat pula dilakukan secara online melalui jaringan. Jaringan yang mampu menangani proses tersebut antara lain adalah sebagai berikut:

- Network Attached Storage

Network Attached Storage adalah suatu jaringan yang akan digunakan untuk membackup file-file yang sedang on-line, dimana jaringan tersebut diletakkan diantara server dan klien



Gambar 17.2. Network Attached Storage

- Storage Area Network

Storage Area Network adalah tipe jaringan dimana proses backup data dilakukan secara terpisah dari LAN. Tujuannya adalah agar kemampuan LAN tetap terjaga.

## Restore

Sistem restore data adalah suatu sistem yang berguna untuk mengembalikan suatu komputer ke suatu keadaan sebelumnya tanpa kehilangan data-data penting (seperti dokumen word,email dll) sesuai dengan restore point yang ditandai.

Dalam sistem restore terdapat sesuatu yang dikenal dengan restore point. Restore point adalah Representasi kondisi waktu data tertentu dari suatu komputer

Selain proses back-up, restore juga mutlak diperlukan pada suatu perusahaan. Tujuannya adalah agar jika terjadi suatu kesalahan, data yang lama masih dapat diperoleh kembali dengan cara me-restore-nya.

## Back-Up pada Windows Server 2003

Utilitas Back-up pada sistem operasi Windows Server 2003 memiliki tiga buah pilihan sebagai berikut:

- Back-up

Untuk menyimpan file yang ada ke lokasi lain

- Restore

Untuk mengembalikan file yang disimpan. Proses ini dilakukan jika file aslinya mengalami kerusakan.


- Automated System Recovery

Fitur ini merupakan pengganti dari fitur emergency repair disk dari sistem operasi Windows versi sebelumnya.

## Back-up Data

Selain Administrator atau group Administrator, group Server Operator<sup>9</sup> atau group Backup Operators dapat juga menggunakan utiliti back-up ini.

Untuk melakukan back-up dapat menggunakan wizard atau tanpa wizard. Jika ingin melakukan back-up dengan wizard, ikuti langkah-langkah berikut ini:

- Tekan tombol  **Start** pada start menu
- Klik **All Programs**
- Klik **Accessories**
- Klik **System Tools**
- Klik **Backup**
- Akan tampil wizard, kemudian tekan tombol **Next**.
- Pilih opsi **back-up files and settings**, kemudian tekan tombol **Next**.
- Pilih opsi **Let me choose what to back up**, kemudian tekan tombol **Next**.
- Cari lokasi file yang akan diback-up kemudian beri tanda check. Setelah itu tekan tombol **Next**.
- Tampil kotak isian untuk letak atau lokasi file hasil back-up, kemudian ketik nama file hasil back-up. File ini biasanya akan memiliki format .bkf.
- Setelah itu tekan tombol **Save**.
- Tekan tombol **Next**.
- Tekan tombol **Finish**.
- Biarkan komputer melakukan **back-up**. Jika telah selesai, sistem back-up akan menampilkan informasi back-up. Tekan tombol **report** atau **close**.


---

<sup>9</sup> Untuk jenis group seperti ini dapat dibaca pada modul Windows XP dan Server 2003

## Restore Data

Jika file atau data pada disk mengalami kerusakan dan user telah melakukan back-up, maka dapat dilakukan pengembalian file atau data tersebut ke asalnya, sehingga tidak perlu melakukan instalasi dan memasukkan data tersebut dari awal.

Cara melakukan restore data aslah sebagai berikut:

- Tekan tombol  **Start** pada start menu
- Klik **All Programs**
- Klik **Accessories**
- Klik **System Tools**
- Klik **Backup**
- Akan tampil wizard, kemudian tekan tombol **Next**.
- Pilih opsi **restore files and settings**, kemudian tekan tombol **Next**.
- Cari tanggal dan lokasi media yang telah diback-up untuk di-restore kembali dengan memberi tanda check pada folder yang akan di-restore.
- Setelah itu tekan tombol Next dan **Finish**. Sistem akan melakukan proses restore. Jika file yang di-back-up dipindahkan ke sebuah media penyimpanan bergerak (removable disk) seperti CD, disket, dsb, maka jangan lupa untuk memasukkan media yang berisi file yang akan di-restore tersebut.
- Tekan tombol **Report** atau **Close**.

## Penjadwalan Back-Up

Pada sistem operasi Microsoft Windows Server 2003, proses back-up dapat dijadwalkan, sehingga proses tersebut akan dilakukan secara otomatis.

Untuk melakukan penjadwalan back-up, lakukan langkah-langkah berikut:

- Lakukan proses back-up seperti yang telah dijelaskan sebelumnya.
- Setelah wizard back-up selesai, tekan tombol **Advanced**.
- Akan ada beberapa jenis back-up, sebagai berikut:
  - ⊕ Normal

Back-up jenis ini akan mem-back-up semua folder dan file dan menggunakan archive bit. Normal back-up sering disebut juga dengan full back-up

✦ Copy

Back-up jenis ini sama seperti normal back-up. Perbedaannya adalah copy back-up tidak mengubah status archive bit.

✦ Incremental

Back-up jenis ini hanya melakukan back-up file-file yang berubah setelah back-up terakhir, menggunakan archive bit.

✦ Differential

Sama seperti proses incremental, bedanya differential tidak akan menghapus status dari archive bit setelah proses back-up selesai.

✦ Daily


Back-up jenis ini akan memeriksa atribut tanggal file yang akan di-back-up, jadi hanya mem-back-up file-file yang dibuat atau diubah pada hari proses back-up dibuat.

- Pilih salah satu jenis back-up seperti yang telah dijelaskan di atas. Setelah itu tekan tombol **Next**. Akan tampil pilihan apakah ingin verify datanya setelah back-up. Beri tanda check pada pilihan tersebut. Setelah itu tekan tombol **Next**.
- Akan muncul pilihan apakah data ingin ditambahkan ke data back-up sebelumnya, atau data akan menggantikan data back-up yang lama. Setelah memilih, tekan tombol **Next**.
- Akan tampil pilihan waktu back-up, pilih opsi **Later**. Setelah itu akan muncul nama job-nya, ketik nama job-nya kemudian tekan tombol **Set Schedule**.
- Pada **Schedule Task**, pilih jadwal back-up, apakah hanya sekali (**Once**), setiap minggu (**Weekly**), atau yang lainnya. Untuk jam mulai back-up, isi pada kotak isian **Start time** dan tanggal pelaksanaannya.

- Setelah selesai tekan tombol **OK**. Akan tampil kotak isian sebagai account-nya, biarkan sesuai default-nya. Kemudian pada isian password ketik password-nya dan ulangi pada **Confirm password**, lalu tekan tombol **OK**.
- Setelah itu tekan tombol **Next**. Akan tampil kembali isian account-nya, setelah diisi tekan tombol **OK**.
- Tekan tombol **Finish**.


## Melihat Jadwal Back-up

Untuk dapat melihat jadwal proses back-up dengan menggunakan Advanced Mode, lakukan langkah-langkah berikut ini:

- Tekan tombol  **Start** pada start menu
- Klik **Accessories**
- Klik **System Tools**
- Klik **Backup**
- Akan muncul wizard, klik **Advanced Mode**.
- Klik tab **Schedule Jobs**.
- Akan tampil jadwal back-up yang ada.

## Automated System Recovery

Pada sistem operasi Windows Server 2003, back-up ini merupakan pengganti dari emergency repair disk yang berfungsi untuk mengembalikan atau memulihkan jika konfigurasi sistem mengalami kerusakan. Setiap melakukan perubahan konfigurasi sistem sebaiknya lakukan proses ini. Caranya adalah dengan melakukan sederetan langkah-langkah berikut:

- Tekan tombol  **Start** pada start menu
- Klik **All Programs**
- Klik **Accessories**

- Klik **System Tools**
- Klik **Backup**
- Akan muncul wizard, klik **Advanced Mode**.
- Klik tombol **Automated System Recovery Wizard**, kemudian tekan tombol **Next**.
- Lokasikan hasil back-up-nya, kemudian tekan tombol **Next**.
- Tekan tombol **Finish**.
- Akan terjadi proses back-up. Setelah terjadi back-up maka akan diminta memasukkan disket kosong pada drive A untuk menyimpan recovery informasi yang di-back-up.
- Tekan tombol **OK**.
- Tekan tombol **Close**.

## Black Out

Black out adalah menghapus salinan/copy untuk data-data penting perusahaan yang ada pada komputer.

Proses yang terjadi pada strategi dalam sistem jaringan ialah sebagai berikut:

- Pengkoneksian dengan storage
- Pemilihan data yang akan di black-out
- Penghapusan data dari storage

## Latihan

1. Suatu sistem backup dan restore data bersifat mutlak diperlukan dalam suatu perusahaan. Apakah maksud dari sistem backup data itu?
  - a. Suatu sistem yang berguna untuk menservice suatu komputer sehingga kondisi komputer dapat berjalan pulih seperti biasanya

- b. Suatu sistem yang berguna untuk mengembalikan suatu komputer ke suatu keadaan sebelumnya tanpa kehilangan data-data penting (seperti dokumen word,email dll) sesuai dengan restore point yang ditandai
  - c. Suatu sistem yang membantu menyalin informasi dari suatu harddisk ke suatu media penyimpanan tertentu
  - d. Suatu sistem yang berguna untuk merusak suatu data-data penting (seperti dokumen word,email dll) pada komputer sesuai dengan restore point yang ditandai
  - e. Suatu sistem yang berguna untuk menggantikan suatu komputer dengan komputer yang baru tanpa kehilangan data-data penting (seperti dokumen word,email dll) sesuai dengan restore point yang ditandai
2. Proses backup dapat juga dilakukan secara on-line atau melewati suatu jaringan tertentu. Manakah jaringan berikut ini yang menangani proses tersebut?
- a. Wide Area Network
  - b. Metropolitan Area Network
  - c. Storage Area Network
  - d. Local Area Network
  - e. Personel Area Network
3. Suatu sistem backup dan restore data bersifat mutlak diperlukan dalam suatu perusahaan. Apakah maksud dari sistem restore data itu?
- a. Suatu sistem yang berguna untuk menggantikan suatu komputer dengan komputer yang baru tanpa kehilangan data-data penting (seperti dokumen word,email dll) sesuai dengan restore point yang ditandai
  - b. Suatu sistem yang berguna untuk menservice suatu komputer sehingga kondisi komputer dapat berjalan pulih seperti biasanya
  - c. Suatu sistem yang berguna untuk mengembalikan suatu komputer ke suatu keadaan sebelumnya tanpa kehilangan data-data penting (seperti dokumen word,email dll) sesuai dengan restore point yang ditandai

- d. Suatu sistem yang berguna untuk merusak suatu data-data penting (seperti dokumen word,email dll) pada komputer sesuai dengan restore point yang ditandai
  - e. Suatu sistem yang dimiliki oleh pemerintah pusat saja
4. Apa yang dimaksud dengan black-out?
- a. Menghapus salinan/copy untuk data-data penting perusahaan yang ada pada komputer.
  - b. Defragmentasi data, membuang sampah-sampah yang ada pada komputer, memperbaiki kesalahan setting
  - c. Membangun dan menata ulang kembali sistem yang rusak oleh faktor yang tidak disengaja, supaya sistem dapat bekerja kembali seperti semula
  - d. Menambah fungsi, memperbaharui sistem yang ada sesuai dengan permintaan pelanggan, testing stabilitas untuk hardware dan software
  - e. Melacak dan membersihkan virus dari komputer dan jaringan
5. Di bawah ini yang merupakan proses yang terjadi pada strategi back-up di dalam sistem jaringan ialah
- a. Pemilihan harga storage
  - b. Pemilihan data yang akan di back-up
  - c. Pemeliharaan jaringan
  - d. Pengkoneksian dengan storage
  - e. Pemilihan media back-up

## Soal Praktek

6. Bagaimana cara melakukan back-up pada Windows Server 2003?



# BAB 18

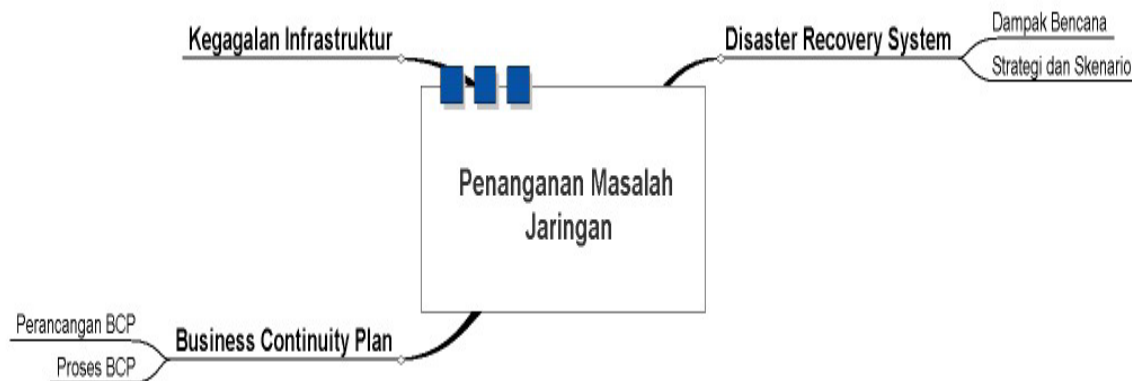
## PENANGANAN MASALAH JARINGAN

### Tujuan Instruksional Umum

- Siswa mampu menjelaskan hal-hal yang dilakukan dalam menangani masalah pada jaringan

### Tujuan Instruksional Khusus

- Siswa mampu menjelaskan secara singkat mengenai Disaster Recovery System
- Siswa mampu menjelaskan dampak bencana pada perusahaan
- Siswa mampu menjelaskan strategi dan skenario dalam mencegah terjadinya kerusakan akibat bencana
- Siswa mampu melakukan beberapa penanganan akibat kegagalan infrastruktur
- Siswa mampu menjelaskan mengenai Business Continuity Plan
- Siswa mampu menjelaskan tahapan dalam Business Continuity Plan
- Siswa mampu menerapkan Business Continuity Plan



Gambar 18.1. Rincian Pembelajaran Bab 18

Selain dari segi keamanan, masalah kerusakan jaringan dapat terjadi karena bermacam hal, seperti bencana alam ataupun komponen yang sudah usang. Pada

bagian ini akan dibahas mengenai bagaimana menanggulangi masalah-masalah yang ada pada jaringan.

## Disaster Recovery System

Disaster Recovery System adalah sebuah sistem yang dijalankan ketika terjadi masalah yang disebabkan oleh suatu bencana alam. Contoh bencana alam yang dapat merusak jaringan antara lain adalah sebagai berikut:

- Gempa
- Tsunami
- Banjir
- Kebakaran
- Dan Lain Lain

### Dampak Bencana

Kegagalan potensial yang akan diterima oleh perusahaan akibat bencana adalah sebagai berikut:

- Semakin memperbesar keterlambatan suatu perusahaan dalam menyediakan jasa. Hal ini tentu saja akan membuat perusahaan kehilangan keuntungan yang tidak sedikit jumlahnya.
- Hilangnya data-data pelanggan dan perusahaan yang akan berdampak serius pada kelangsungan bisnis perusahaan ke depannya.
- Runtuhnya infrastruktur jaringan yang telah dibangun dengan biaya yang tidak sedikit.

### Strategi dan Skenario Disaster Recovery Plan

Strategi yang dilakukan perusahaan dalam mencegah terjadinya kerusakan akibat bencana antara lain adalah sebagai berikut:

- Memastikan keamanan para pekerja dan pengunjung atau pelanggan
- Menata dan mem-back-up data-data perusahaan dengan baik
- Melakukan pelatihan pada para pekerja secara periodik yang meliputi berbagai aspek.

Untuk sebuah perusahaan yang memiliki pengelolaan yang baik, biasanya terdapat suatu skenario, yang dikenal dengan Disaster Recovery Plan, yang harus dilakukan untuk melakukan pemulihan akibat bencana. Contoh dari skenario tersebut adalah sebagai berikut:

- Pengiriman data dari Authorized User Data dan Software archived dalam bentuk off-site storage ke Disaster Recovery Center
- Menghubungkan network lines ke Disaster Recovery Center
- Menyediakan Critical Coverage pada Disaster Recovery Center
- Menyediakan workspace dan peralatan yang dibutuhkan

Yang harus diingat adalah penyimpanan kembali data-data dari critical coverage (tempat data-data dari pusat komputer di-backup) ke pusat komputer dilakukan setelah pusat komputer itu beroperasi dengan baik.

Selain itu, strategi yang ada perlu ditinjau kembali dan dievaluasi. Tujuannya adalah agar dapat meminimalisasi resiko yang mungkin dapat terjadi, dan sesuai dengan batasan-batasan yang dimiliki oleh perusahaan. Salah satu batasan tersebut adalah dana.

## **Kegagalan Infrastruktur**

Selain bencana yang disebabkan oleh alam, ada masalah yang lebih dikarenakan oleh ulah manusia seperti halnya sebagai berikut:

- Sabotase dari pihak yang tidak bertanggung jawab
- Kegagalan infrastruktur
- Serangan para cracker ganas

Poin pertama dan ketiga menyangkut mengenai keamanan jaringan. Hal tersebut telah dibahas pada bagian-bagian terdahulu.

Ada beberapa tahap yang dapat dilakukan untuk menangani suatu sistem yang crash. Tahap tersebut antara lain adalah sebagai berikut:

- Memeriksa letak kesalahan
- Mengidentifikasi jenis kesalahan
- Membetulkan kesalahan sesuai jenisnya
- Membetulkan kesalahan sesuai jenisnya

Untuk kegagalan infrastruktur, ada beberapa kasus yang menjadi masalah dalam jaringan. Beberapa kasus tersebut dan cara penanggulangannya dapat dilihat pada tabel di bawah ini.

Tabel 18.1: Beberapa kasus dan cara penanggulangannya

Kasus	Tindakan
Suatu server yang berfungsi untuk melakukan resolver dari nama domain ke IP address pada jaringan sedang mati atau down	Merestart kembali daemon DNS untuk diaktifkan
Suatu server pada jaringan sedang mati atau down sehingga para klien tidak dapat mendapatkan IP dinamis dari server tersebut	Merestart kembali daemon DHCP untuk diaktifkan
Suatu server yang berfungsi untuk mengelola halaman suatu situs pada jaringan sedang mati atau down	Merestart kembali daemon APACHE untuk diaktifkan
Diketahui bahwa kesalahan disebabkan oleh rusaknya Hub sehingga beberapa user terganggu aktifitasnya.	Menggunakan komponen switch, untuk meminimalkan gangguan tersebut.
Apabila diketahui bahwa kesalahan disebabkan oleh rusaknya Router pinjaman dari ISP sehingga semua user yang tergabung dalam jaringan tersebut terganggu aktifitasnya	Mengadakan komponen PC Router secara sementara, untuk meminimalkan gangguan tersebut.
Apabila diketahui bahwa kesalahan disebabkan oleh rusaknya AP pinjaman dari ISP sehingga semua user yang tergabung dalam jaringan tersebut terganggu aktifitasnya.	Mengadakan komponen Access Point secara sementara, untuk meminimalkan gangguan tersebut.
Apabila terjadi kesalahan dalam pengkabelan dapat mengakibatkan tidak dapat terhubung ke suatu jaringan.	Menggunakan LAN tester untuk menguji redaman suatu kabel LAN, maupun struktur kabel.
Jika suatu server proxy mengalami kerusakan fatal atau	Kerusakan terjadi pada perangkat

Kasus	Tindakan
tidak dapat beroperasi yang diakibatkan oleh manusia yang tidak bertanggung jawab. Akan tetapi perangkat keras tetap berfungsi sebagai mana mestinya.	lunak. Instal dan konfigurasi ulang perangkat lunak, seperti squid.

Untuk kerusakan pada kabel, pencarian kerusakan pada jaringan kabel dilakukan antara lain pada:

- Kabel UTP
- Koneksi pada switch dan router
- Konektor RJ-45
- Pemasangan LAN card

## Business Continuity Plan

Business Continuity Plan adalah sebuah rencana yang diambil suatu perusahaan untuk meneruskan bisnisnya, jika terjadi suatu kekacauan. Proses perencanaan suatu business continuity plan akan memungkinkan suatu perusahaan untuk melakukan hal-hal sebagai berikut (4R):

- Mengurangi ancaman-ancaman yang mungkin terjadi (Reduce),
- Merespon suatu peristiwa dengan baik (Respon),
- Memulihkan dari dampak langsung suatu peristiwa (Recover),
- Mengembalikan ke kondisi semula (Restore).

### Perancangan BCP

Sebelum melakukan perancangan perlu dilakukan pengamatan pada semua area pengolahan informasi kritis perusahaan. Area tersebut antara lain sebagai berikut:

- LAN, WAN, Server, workstation
- Telekomunikasi dan link komunikasi data
- Perangkat keras, perangkat lunak dan data

- Media dan penyimpanan arsip
- Tugas-tugas staf dan proses produksi

## **Proses BCP**

Proses BCP memiliki 4 unsur utama, antara lain sebagai berikut:

- **Proses Inisiasi Lingkup dan Rencana**

Pada tahap ini meliputi pembuatan lingkup dan unsur-unsur lain yang diperlukan untuk menentukan parameter-parameter rencana

- **Proses Business Impact Assessment**

Business Impact Assessment adalah suatu proses yang dilaksanakan untuk membantu unit-unit bisnis memahami dampak suatu peristiwa yang mengganggu yang meliputi pelaksanaan vulnerability assessment.

- **Proses Persetujuan Rencana dan implementasi**

Pada proses ini melibatkan pengambilan keputusan akhir manajemen senior, menciptakan kesadaran terhadap rencana tersebut ke seluruh personil perusahaan, dan menerapkan suatu prosedur pemeliharaan untuk membaharui rencana jika dibutuhkan.

- **Proses Pengembangan BCP**

Proses ini meliputi area dari implementasi rencana, pengujian rencana, dan pemeliharaan rencana berkelanjutan

## **Latihan**

1. Kegagalan potensial yang dapat disebabkan suatu disaster dapat meliputi beberapa hal, kecuali...
  - a. Memperkecil resiko keterlambatan suatu perusahaan dalam menyediakan jasa

- b. Semakin memperbesar keterlambatan suatu perusahaan dalam menyediakan jasa
  - c. Hilangnya data-data pelanggan dan perusahaan yang berdampak serius
  - d. Terciptanya pembackupan data penting yang menjamin kelangsungan bisnis perusahaan
  - e. Runtuhnya infrastruktur jaringan yang telah dibangun dengan biaya yang tidak sedikit
2. Berikut ini adalah contoh-contoh peristiwa yang dapat mengganggu kesinambungan bisnis perusahaan : 1.Gempa Bumi, 2.Sabotase dari pihak yang tidak bertanggung jawab, 3.Banjir dan badai, 4.Kegagalan infrastruktur komunikasi, 5.Serangan para cracker ganas. Dari contoh di atas peristiwa manakah yang tidak diakibatkan oleh ulah manusia?
- a. 1 dan 2
  - b. 2 dan 3
  - c. 3 dan 4
  - d. 4 dan 5
  - e. 1 dan 3
  - f. 2 dan 5
3. Strategi yang dilakukan untuk mencegah terjadinya disaster oleh suatu perusahaan antara lain adalah..
- a. Memastikan rekening pemilik perusahaan telah terisi penuh untuk persiapan melarikan diri saat terjadi bencana
  - b. Memastikan keamanan para pekerja dan pengunjung atau pelanggan
  - c. Data-data perusahaan ditata dan dibackup dengan baik
  - d. Training para pekerja dilakukan secara periodik yang meliputi berbagai aspek
  - e. Menghilangkan data-data pelanggan karena menambah beban kerja perusahaan

4. Proses perencanaan suatu business continuity plan akan memungkinkan suatu perusahaan untuk melakukan : 1.Mengurangi ancaman-ancaman yang mungkin terjadi, 2.Merespon suatu peristiwa dengan baik, 3.Memulihkan dari dampak langsung suatu peristiwa, 4.Mengembalikan ke kondisi semula. Manakah yang hal-hal yang dapat dihasilkan jika perencanaan bisnis tersebut disiapkan?
- a. 1 dan 2
  - b. 1 dan 3
  - c. 2 dan 3
  - d. 2 dan 4
  - e. 2,3 dan 4
  - f. 1,2 dan 3
  - g. 1,2,3 dan 4
6. Business Continuity Plan (BCP) perlu disampaikan kepada pihak yang berwenang. Tujuan dari direncanakan BCP ini adalah 4 R. Pilihlah yang termasuk 4 R?
- a. Ratio
  - b. Respect
  - c. Reduce
  - d. Recover

# **BAB 19**

## **CISCO**

### **Tujuan Instruksional Umum**

- Siswa mampu menjelaskan mengenai CISCO

### **Tujuan Instruksional Khusus**

- Siswa mampu menjelaskan secara singkat apa itu CISCO
- Siswa mampu menjelaskan tentang CISCO Networking Academy

### **CISCO**

Cisco adalah perusahaan peralatan komunikasi yang berbasis di California, Amerika Serikat. Perusahaan ini awalnya hanya membuat peralatan routing, akan tetapi sekarang menjual bermacam peralatan-peralatan komunikasi seperti berikut:

- Ethernet switches
- Branch office routers and CPE (Customer Premises Equipment)
- IP Telephony products such as IP PBXes (CallManager), VoIP gateways and IP phones
- Network security devices such as Firewalls, VPN concentrators, Network and Host Intrusion Prevention and Software
- Metro optical switching platforms
- Large carrier grade core and edge routers / MPLS switches
- Carrier and enterprise ATM switches
- Cable Modem Termination Systems (CMTSes)
- DSL subscriber aggregation / concentration equipment

- Remote access and universal gateways
- Storage Area Network (SAN) switches and appliances
- Network management software and appliances
- Wireless
- Home networking products (via the Linksys division)

## CISCO Networking Academy

Cisco juga menjalankan kursus networking yang dikenal dengan Cisco Networking Academy, dimana menggunakan kampus dan sekolah untuk belajar. Kursus yang ditawarkan pada Cisco Networking Academy antara lain adalah sebagai berikut:

- CCNA

Ekivalen dengan 280 jam instruksi, memberikan siswa dengan pelajaran dasar dalam jaringan. Siswa yang menyelesaikan bagian ini akan mendapatkan Cisco Certified Network Associate (CCNA™) certification.

- CCNP

Juga ekivalen dengan 280 jam instruksi, dan lebih advanced. Siswa belajar lebih kompleks mengenai konfigurasi jaringan dan bagaimana mendiagnosa dan memperbaiki masalah jaringan. Siswa yang menyelesaikan bagian ini akan mendapatkan Cisco Certified Network Professional (CCNP™) certification.

- Hp IT Essentials I

Disponsori oleh Hewlett-Packard Company, melakukan penggalan dalam pada hardware komputer dan sistem operasi. Siswa belajar fungsionalitas hardware dan software serta langkah-langkah terbaik dalam pemeliharaan dan keamanan. Kursus ini membantu siswa untuk mendapatkan CompTIA's A+ certification."

- Hp IT Essentials II

Disponsori oleh Hewlett-Packard Company, pengenalan intensif terhadap multi-user, multi-tasking network operating systems. Karakteristik sistem operasi jaringan Linux, Windows 2000, NT, and XP akan dibahas . Siswa akan menggali banyak topik, antara lain prosedur instalasi, keamanan, back up, dan remote access.

#### ■ JAVA

70-jam kursus yang akan memberikan pengertian konsep dari pemrograman berorientasi objek. Kursus juga akan mengajarkan siswa bagaimana menggunakan bahasa JAVA untuk menyelesaikan masalah bisnis. Siswa akan belajar cara membuat class, object, dan aplikasi.

#### ■ Network Security

Kursus ini akan mengajarkan siswa merancang dan mengimplementasi solusi keamanan yang akan mengurangi resiko kehilangan keuntungan.

#### ■ UNIX

Mengajarkan bagaimana menggunakan UNIX® operating system dan mengenalkan CDE, GNOME, and KDE graphical user interfaces (GUI).

#### ■ Web Design

Disponsori oleh Adobe Systems akan menitikberatkan pada proses produksi sebuah Web. Kursus Web Design exercises akan diajari dengan Adobe® Photoshop®, Adobe Illustrator®, Adobe GoLive™, Adobe LiveMotion™, dan Adobe Premiere®.

#### ■ Wireless LAN

Kursus pengenalan yang akan menitikberatkan pada perancangan, perencanaan, implementasi, operasi, dan penanganan masalah pada jaringan wireless.

## Latihan

1. Di bawah ini adalah contoh produk CISCO, kecuali..
  - a. Branch office routers and CPE (Customer Premises Equipment)
  - b. Storage Area Network (SAN) switches and appliances
  - c. Cable Modem Termination Systems (CMTSes)
  - d. Network management software and appliances
  - e. Semua Benar

2. Di bawah ini yang termasuk kursus yang ditawarkan pada CISCO Networking Academy, kecuali..
- a. Microsoft Office
  - b. JAVA
  - c. Hp IT Essentials I
  - d. Semua Benar
  - e. Semua Salah

# KUNCI JAWABAN

## BAB 1

- |                 |       |
|-----------------|-------|
| 8. e            | 11. d |
| 9. c.           | 12. a |
| 10. a, b, dan d |       |

## BAB 2

- |            |            |
|------------|------------|
| 1. a       | 6. b       |
| 2. b dan d | 7. a dan b |
| 3. a       | 8. d       |
| 4. b       | 9. a       |
| 5. a       |            |

10. Ikuti langkah-langkah berikut ini:

- Buka casing komputer, baik untuk Server maupun untuk workstation
- Setelah casing terbuka, pasang (tancapkan) kartu jaringan ke soket atau slot PCI di komputer.
- Pasang mur di bagian atas sehingga kartu jaringan kokoh dan tidak goyang.
- Setelah selesai tutup casing dan rapikan letak komputer yang sudah dipasang kartu jaringan
- Tancapkan kabel yang telah dipasang konektor RJ45 ke port di Hub dan di komputer.

## BAB 3

1. e
2. b

## BAB 4

1. d
2. e
3. b
4. a
5. c

6. Ikuti langkah-langkah berikut ini:

- Sediakan WLAN card usb
- Install driver sesuai dengan sistem operasi yang digunakan
- Masukkan perangkat ke dalam PC
- Lakukan Setting SSID dan IP
- Lakukan uji coba keberhasilan konektivitas. Pengujian dapat dilakukan dengan menggunakan PING.

## BAB 5

1. Benar
2. d.
3. a.
4. b.
5. c.
6. Lihat cara instalasi Active Directory pada bab 5

## BAB 6

1. a dan c
2. a, d, dan e.
3. d.
4. d
5. c.
6. Ikuti langkah-langkah berikut:
  - Tekan tombol start pada start menu
  - Klik **Run**.
  - Ketikkan **cmd** pada bagian **Open:** kemudian tekan tombol **OK**.
  - Ketik **ipconfig/all** kemudian tekan **enter**.

## BAB 7

1. b dan e
2. a
3. c
4. a dan d
5. b dan d
6. Ikuti langkah-langkah berikut ini:
  - Matikan semua perangkat yang terhubung ke jaringan.
  - Gunakan kabel Ethernet Kategori V yang cukup panjang untuk menghubungkan access point dengan hub atau switch.
  - Pasangkan salah satu ujung kabel ke port Ethernet berlabel LAN yang berada di belakang access point.
  - Pasangkan ujung kabel yang lain ke port Ethernet manapun pada hub atau switch, kecuali yang berlabel UPLINK.
  - Pasangkan kabel Ethernet Kategori V yang kedua ke port berlabel UPLINK di belakang router.

- Pasangkan ujung lain dari kabel kedua ke port manapun di router, kecuali yang berlabel WAN.
- Pasangkan kabel Ethernet Kategori V yang ketiga ke port berlabel WAN di belakang router.
- Pasangkan ujung lain dari kabel ketiga ke port LAN di belakang perangkat untuk mengakses Internet (bisa berupa modem kabel atau modem DSL).
- Nyalakan semua perangkat, dalam urutan: modem kabel/DSL, router, hub, access point, kemudian semua komputer.

## BAB 8


1. DNS server melakukan penerjemahan nama host yang user sediakan ke alamat IP sebenarnya.
2. DNS akan memetakan nama domain ke alamat IP. Reverse Lookup Zone adalah proses sebaliknya, yaitu memetakan alamat IP ke nama domain.
3. D
4. D
5. A dan C
6. Ikuti langkah-langkah berikut:
  - Tekan tombol start pada start menu
  - Klik **Control Panel**.
  - Klik dua kali **Add or Remove Program**
  - Tekan tombol **Add/Remove Windows Components**
  - Akan tampil sebuah wizard, pilih **Networking Services**.
  - Tekan tombol **Details**. Kemudian akan tampil subkomponennya.
  - Beri tanda check pada **Domain Name System (DNS)**,
  - Tekan tombol **OK**.
  - Masukkan CD Windows Server 2003, dan tekan tombol **Next**.

- Tekan **Finish**.

## BAB 9

1. Benar
2. Ikuti langkah-langkah berikut:
  - Tekan tombol start dari start menu.
  - Klik **Control Panel**.
  - Klik 2 kali **Add/Remove Programs**.
  - Klik **Add/Remove Windows Components**.
  - Klik **Networking Services**.
  - Tekan tombol **Details**.
  - Beri tanda check pada **Dynamic Host Configuration Protocol (DHCP)**.
  - Tekan tombol **OK**.
  - Tekan tombol **Next**.
  - Biarkan program bekerja. Jika sistem meminta user memasukkan master Windows Server 2003, masukkan CD ke drive CD.
  - Setelah selesai tekan tombol **Finish**.

## BAB 10

1. d
2. c
3. d
4. c
5. Ikuti langkah-langkah berikut ini:
  - Tekan tombol  **Start** pada start menu
  - Klik **Control Panel**.
  - Klik 2 kali **Add/Remove Programs**.
  - Klik **Add/Remove Windows Component**.

- Pilih **Internet Information Services (IIS)**, tekan tombol **Details**.
- Beri tanda check pada **IIS Manager**, **Common Files** dan **FTP Service**.
- Tekan tombol **OK**.
- Tekan tombol **OK**.
- Tekan tombol **Next** dan masukkan Windows Server 2003.
- Tekan tombol **Finish**.

## BAB 11


1. Salah.
2. C.
3. Ikuti langkah-langkah berikut:
  - Tekan tombol start pada start menu.
  - Klik **All Programs**.
  - Klik **Administrative Tools**.
  - Klik **Manage Your Server**.
  - Klik **Add Printer**.
  - Akan muncul wizard, tekan tombol **Next**.
  - Pilih opsi **Local Printer Attached to this computer** dan beri tanda check pada **Automatically detect and install my Plug and Play Printer**, jika user telah memasang printer dan dalam keadaan ON. Setelah itu tekan tombol **Next**.
  - Ikuti petunjuk yang ada. Masukkan CD instalasi printer yang biasanya disertakan bersama dengan printer dalam kemasan, jika diperlukan.
  - Tekan tombol **Finish** jika selesai.
3. Ikuti langkah-langkah berikut
  - Tekan tombol start pada Windows.
  - Klik **Printer and Faxes**.
  - Klik **File** pada menubar.

- Klik **Add a printer**.
- Akan muncul wizard, kemudian tekan tombol **Next**.
- Pilih **Network Printer or a printer attached to another computer** kemudian tekan tombol **Next**.
- Spesifikasikan nama printer atau alamat printer jaringan. User juga dapat melakukan pencarian printer yang dimaksud. Pilih salah satu opsi (sebaiknya pilih **Browse for a printer**) tombol **Next**.
- Ikuti langkah selanjutnya.


## BAB 12

1. a dan b
2. b, d, dan e
3. e
4. d
5. c

6. Ikuti langkah-langkah berikut:

- Tekan tombol  **Start** pada start menu
- Klik **Control Panel**.
- Klik 2 kali **Add/Remove Programs**.
- Klik **Add/Remove Window Components**.
- Beri tanda check pada komponen **Email Services**
- Masukkan CD Windows kemudian tekan tombol **Next**.
- Ikuti instruksi selanjutnya hingga selesai.

Setelah itu lakukan pengaturan terhadap servis POP3 dengan melakukan langkah-langkah berikut ini:

- Tekan tombol  **Start** pada start menu
- Klik **All Programs**
- Klik **Administrative Tools**

- Klik **POP3 Service**
- Klik **Server Properties**
- Beri tanda check pada opsi **Require Secure Password Authentication (SPA)** for all client connections dan **Always create an associated user for new mailbox.**
- Jika sudah, tekan tombol **OK.**

## BAB 13

1. c.
2. a dan c
3. d dan e
4. b
5. e
6. Ikuti langkah-langkah berikut ini:
  - Buka Query Analyzer pada SQL Server. Jika sedang berada pada Enterprise Manager, dapat melalui menu **Tools** dan kemudian mengklik **SQL Query Analyzer.**
  - Fitur Query Analyzer akan tampak seperti gambar di bawah ini.
  - Pilih database tempat DDL atau DML akan diimplementasikan.
  - Ketikkan DDL maupun DML pada tempat yang disediakan.
  - Tekan ikon ✓ untuk melakukan pemeriksaan terhadap syntax DDL atau DML yang ditulis. Jika benar akan tampil pesan **The command(s) completed successfully.**
  - Tekan ikon ▶ untuk menjalankan DDL atau DML yang telah ditulis tersebut.

## BAB 14

1. a, b, c, dan d
2. c
3. c
4. c
5. a, c, dan d
6. b dan d
7. a, b, dan d
8. a dan d
9. a, b, dan c
10. a dan c

## BAB 15

1. d
2. benar
3. b
4. a, b, dan d
5. d


## BAB 16

1. a, c, dan d
2. b dan d
3. b dan c
4. b, c, dan e
5. a dan d
6. b, c, dan e
7. a dan b

## BAB 17

1. c
2. c
3. c
4. a
5. b, d, dan e

6. Ikuti langkah-langkah berikut:

- Tekan tombol  **Start** pada start menu
- Klik **All Programs**
- Klik **Accessories**
- Klik **System Tools**
- Klik **Backup**
- Akan tampil wizard, kemudian tekan tombol **Next**.
- Pilih opsi **back-up files and settings**, kemudian tekan tombol **Next**.
- Pilih opsi **Let me choose what to back up**, kemudian tekan tombol **Next**.
- Cari lokasi file yang akan diback-up kemudian beri tanda check. Setelah itu tekan tombol **Next**.
- Tampil kotak isian untuk letak atau lokasi file hasil back-up, kemudian ketik nama file hasil back-up. File ini biasanya akan memiliki format .bkf.
- Setelah itu tekan tombol **Save**.
- Tekan tombol **Next**.
- Tekan tombol **Finish**.
- Biarkan komputer melakukan **back-up**. Jika telah selesai, sistem back-up akan menampilkan informasi back-up. Tekan tombol **report** atau **close**.

## BAB 18

1. a dan d
2. e
3. b, c, dan d
4. g
5. c dan d

## BAB 19

1. e
2. a



## DAFTAR PUSTAKA

- . *Expand Your Wireless Network*. Information Technology Services.  
[http://www.utexas.edu/its/wireless/install/install\\_extender.html](http://www.utexas.edu/its/wireless/install/install_extender.html). 2003.
- . *Glossary: Decoding the Jargon*. Cable News Network LP, LLLP.  
<http://edition.cnn.com/2004/TECH/internet/10/25/glossary/>. 2004.
- . *Hotspot (wifi)*. [http://en.wikipedia.org/wiki/Hotspot\\_\(wifi\)](http://en.wikipedia.org/wiki/Hotspot_(wifi)). 2006.
- . *Install an Access Point*. Information Technology Services.  
[http://www.utexas.edu/its/wireless/install/install\\_ap.html](http://www.utexas.edu/its/wireless/install/install_ap.html). 2003.
- . *Setting Up a Secure Wireless Network*. <http://www.wifiplanet.com/tutorials/article.php/2233511>. 2003
- . *Sharing a Single IP Address Using a Router*. Information Technology Services. [http://www.utexas.edu/its/wireless/install/install\\_router.html](http://www.utexas.edu/its/wireless/install/install_router.html). 2003.
- . *SKN Jaringan Komputer dan Sistem Administrasi Versi 0.1*. LSP Telematika
- . *Wireless and Mobility – Set Up a Wireless Network*. Hewlett-Packard Development Company, L.P.  
[http://www.hp.com/sbso/wireless/setup\\_wireless\\_network.html](http://www.hp.com/sbso/wireless/setup_wireless_network.html). 2003
- Kelik, Wahyu. *Pengantar Pengkabelan dan Jaringan*.  
<http://ilmukomputer.com/umum/kelik-kabel.php>. 2003.
- Lowe, Jr, Richard. *Installing A Firewall*. <http://www.rlrouse.com/install-firewall.html>. 2006.
- Microsoft Cooperation. *SQL Server Book Online*. 2000.

Prihanto, Harry. Membangun Jaringan Komputer: Mengenal Hardware dan Topologi Jaringan. <http://ilmukomputer.com/umum/harry-jaringan.php>. 2003.

Petri, Daniel. How can I install Windows Server 2003 on my server? <http://www.petri.co.il>. 1998.

W. K., Ahmad Muammar. *FireWall*. <http://ilmukomputer.com/umum/ammam-firewall.php>. 2004.

Tutang. 2005. *Mendesain dan Mengimplementasikan Jaringan Modern Berbasis Microsoft Windows Server 2003*. Jakarta: Datakom Lintas Buana.

W. Purbo, Onno. *Keamanan Jaringan Internet*. PT. Elex Media Komputindo. Jakarta. 2001.

Wheat, Jeffrey, et.al. *Designing a Wireless Network*. Syngress Publishing, Inc. 2001. ([http://www.ssuet.edu.pk/~amkhan/cisco/wan\\_book.pdf](http://www.ssuet.edu.pk/~amkhan/cisco/wan_book.pdf)).

Wirija, Sudantha. 2005. *Microsoft Windows Server 2003*. Jakarta: PT. Elex Media Komputindo.

