NAMA: mohammad fathor rosi
NIM: 1310651037

KELAS: b

PRELIMINARY
The goal of access control is to allow authorized users to access the appropriate data and deny access to unauthorized users. Access control to protect against threats such as unauthorized access, inappropriate modification of data, and loss of confidentiality
CORNERSTONE CONCEPT OF INFORMATION SECURITY
Before we could explain access control, we must define the foundation of information security concept. These concepts provide the basis upon which the domain 10
General body of knowledge built
Confidentiality, integrity, and availability secrecy

ntegrity
Integrity seeks to prevent unauthorized modification of information. In other words, integrity trying to prevent unauthorized write access to data.
There are two types of integrity: the integrity of the data and the integrity of the system. Data integrity trying to
protecting information against unauthorized modification; seeks to protect the integrity of the system systems, such as Windows server operating system in 2012, from unauthorized modification.
destruction
(DAD). Disclosure is unauthorized disclosure of information; alter-
ASI is unauthorized modification of data, and the destruction was making system not available. While the acronym CIA sometimes change, acronym DAD is displayed in that order.

Identity and Authentication
Identity is the claim: if your name is "Person X," you identify yourself by saying "I People X. "Identities be weak because there is no evidence. You can also identify themselves by saying "I Person Y."
Authorization describes the actions that you can do on the system after you have identified and confirmed.
Accountability
Accountability hold users accountable for their actions. This is usually accomplished by logging and analyzing audit data. Enforcing accountability helps keep "Honest people honest.
nonrepudiation
nonrepudiationberarti users can not deny (reject) after a transac-tion.

Subject and object
A subject
is an active entity in the system data. Most examples involve lessons

accessing the data file. However, a computer program that is running is the subject as well.

object
is a passive data into the system. Objects can range from database to a text file. The important thing to remember about objects is that they are passive in the system. They do not manipulate other objects.
Defense-in-depth

(also called defense in depth) apply some protection (also called control:
control may fail; to exert some control, you increase the confidentiality, integrity, and availability of data.
ACCESS CONTROL MODEL
Now that we have reviewed the concept of access control foundation, we can discuss different access control model: the main model is Discretionary Access Control (DAC), Mandatory Access Control (MAC), and nondiscretionary access control.

Discretionary access control
Discretionary Access Control
(DAC) Provides full control subjects from the objects they own has been given access to, including share objects with other subjects. subject empowered and in control of their data.

Mandatory access control
Mandatory Access Control
Is enforced by the access control system sub ject and object permissions label.
ubjects and objects have a license and label, respectively, as a secret, secret and confidential. A subject may access the object only if permission subject is equal to or greater than object label.
Nondiscretionary access control
Role-Based Access Control
Defines how information is accessed on the system based on the role of the subject. A role can be a nurse, backup administrator, help desk technician, etc. The subjects are grouped into roles and their respective roles defined to have access permissions based on roles, not individuals.
RBAC is jeniskontrol nondiscretionary access because the user does not have wisdom of the group of objects they are allowed to access and can not afford to transfer an object for other subjects.

Rule-based access control
AN
rule-based access control system uses a set of defined rules, restrictions, and filters to access the object in a system. The rules in the form of "If / then" statement.
Centralized access control
Terpusatberkonsentrasi access control access control in one logical point for system or organization.

Access control list
Used throughout many IT security policies, proce-
dures, and technology. Access control list is a list of objects; each entry describes the subjects that can access the object. Subject attempts to access an object which does not have a matching entry in the ACL will be rejected.
Access the procurement lifecycle
After proper access control model has been selected and used, the access pro-
the vision of the life cycle must be maintained and secured. While many organizations fol-
Low best practices for issuing access, many shortcomings formal process to ensure lifetime is kept secure access as employees and contractors engaged dalamsebuah organization. IBM describes the life cycle of identity following rules:
• Password policy compliance checks
• Notifying users to change their passwords before they expire
• Identify life cycle changes such as accounts that are inactive for more than 30 consecutive days
• Identify new account that has not been used for more than 10 days after their creation is to identify accounts that candidates for removal because they have suspended for more than 30 days
• When the contract expires, identifies all accounts belonging to business partners or employees of contractors and revoke their access rights "

Remote Authentication Dial-In User Service

Protocol is a third-party authentication system. RADIUS uses the User Datagram Protocol (UDP) port 1812 (authentication) and 1813 (accounting).

1. It System Terminal Access Controller Access Control
(TACACS) is focused
access control system that requires users to send ID and static (reusable) password for authentication. TACACS uses UDP port 49 (and possibly also using TCP). Reusable password has security vulnerabilities
2. PAP and CHAP
ItuPassword Authentication Protocol
(PAP) is not safe: the user enters the password
and it is sent over the network in clear text. When received by the server PAP, it is confirmed and validated. Sniffing the network can reveal the plaintext

password.
It Challenge-Handshake Authentication Protocol
(CHAP) Provide protection
against playback attacks.
It uses challenging locations remote users. As
stated in RFC 1994, "CHAP depending on the 'secret' known only to the authenticator and peer.
3. ACCESS CONTROL AND TYPE defensive CATEGORIES
To understand and apply appropriate access control, understanding
what are the benefits of each control can increase security is very important. In this section, every kind
Access control will be determined on the basis of how to add security system.
There are six types of access control:
• Abatement
• Detective
• Repairs
• Recovery
• Abatement
• Compensation
1.Administratif
(Also called a directive) controls implemented by creating and following
organizational policies, procedures, or regulations. User training and awareness also fall into this
dalamkategori.
2.Teknis
control is implemented using software, hardware, or firmware that restrict logical access to the
information technology system. Examples include firewalls, routers,
and encryption.
3.Fisik
control is implemented with a physical device, such as locks, fences, gates, and security guards.
PencegahKontrol preventive
prevents the action from occurring. This applies to any restrictions
Potential users, whether authorized or unauthorized, can be done.
Detective
Detective controls
is the standby control during or after a successful attack. Intrusion
signal detection system after a successful attack, closed circuit television cameras
(CCTV) which guards against an intruder alert, and building systems that are triggered alarm

by intruders are examples of detective controls.
Recovery
After a security incident has occurred, control recovery
dalammemesan may need to be taken to restore the functioning of the system and organization.
Deterrent
Control preventer
prevent users from performingactions on the system. Examples include

"Beware of Dog" sign: thieves face two buildings, one with a guard dog and one without, are more likely to attack a building without a guard dog. Large fines for speeding are deterrent to drivers not to speed up.

METHOD OF AUTHENTICATION

A key concept to implement proper control access control
authentication subjects in IT systems. Subject A first identify himself or
himself; This identification can not be trusted. Subjects were then authenticate by promasi assurance that the identity of the claimed effect.

Personal Identification Number
(Password number-based). This is the easiest form, and often weak, the authentication.
Access control methods.
There are four types of passwords to be considered when implementing access control: static password, passphrase, one-time passwords, and dynamic password.
Static passwords
is a reusable passwords that may or may not end. They
usually user-generated and work well when combined with other authentication
type, such as a smart card or biometric controls.
Passphrases
is a static password length, made up of words in a phrase or sentence. Examples passphrase is: "I will pass the CISSP
valid only for one time use.
Dynamic Passwords
change periodically. RSA Security makes synchronized with
The device is called nous sign SecurID token that generates a new code every 60 seconds.
Static PIN users combine them with dynamic RSA token code to create a
dynamic password that changes every time it is used. One disadvantage when using dynamic password token own expense.

Password hashes and password cracking
In most cases, the clear text password is not stored in the IT system; only
output hash of their stored passwords.
Hashing
is a one-way encryption uses
algorithm and no buttons. When the user tries to login, passwords they type is
hash, and hash are compared against the hash that is stored on the system. Hash
Function can not be reversed: it is impossible to reverse the algorithm and generates
password from the hash. While the hash can not be reversed, the attacker can run
advanced hash algorithms many times, choosing a variety of possible passwords and comparing output to the desired hash, hoping to find a match (and to get the original
password). This is called password cracking.
Dictionary attack
AN
dictionary attack
using a list of words: a standard list of words, and then run each

said through a hash algorithm. If the software is cracked in accordance with the output of
Password hash output dictionary attack, the attacker will be able to identify
The original password.
AN
Hybrid attack
adding, prepends, or change characters in the words of the dictionary
before hashing, to try fastest slit complex password brute-force attack
s take more time but is more effective. Attackers counting
output hash for every possible password. Just a few years ago, the speed of basic computer
still slow enough to make a daunting task. However, with advances in
CPU speed and parallel computing, the time required to brute-force pass complex
the word has been much reduced.
Table rainbow
A rainbow table is precomputed compilation of plaintext and ciphertext matching
(Usually passwords and their hashes match). Greatly accelerate the rainbow table
many types of password cracking attacks, often take minutes to solve another where
methods (such as dictionary, hybrid and brute force password cracking attempts)
may take longer.
Although the rainbow table acts as a database, they are more complex under the hood,
relying on a time / memory trade-off to represent and recover passwords and hash.
Most of rainbow tables can solve most, but not all, possible hashes.
Salt
AN
salt
allows a password to hash some way. Some systems (such as modern
Systems UNIX / Linux) combining the salt with the password before hashing: "The
designer of the UNIX operating system is increased in this method by using random

do not use salt (such as Microsoft LAN Manager hash), thousands, millions, billions,
or more rainbow tables would be required for systems that use salt, depending on the
Long salt.
Type 2 authentication (something you have) requires users to have something,
such as tokens, which proves they are authenticated users. Token is an object that helps prove the
identity claim.
Synchronous dynamic tokens, using the time or counter to synchronize sign displayed
code with the code expected by the server authentication: the synchronized code.
Token-based dynamic synchronous time code display dynamic marks
change frequently, such as every 60 seconds.

Asynchronous dynamic token, not synchronized with a central server. most
Various public is a challenge-response token. Challenge-response authentica- mark
tion system generates a challenge or input to the mark. Then the user credentials

ually entering information into the device along with their PIN, and devices generating output. This output is then sent to the system.

3 types of authentication (something you are) is biometrics, which uses physical acteristics acteristics as a means of identification or authentication. Biometrics can be used to establish identity or to authenticate (prove a claim of identity).

registration
describes the process of registration with biometric systems: creating account for the first time. Users typically provide their name (identity), pass a word or PIN, and then provide biometric information, such as fingerprints on swiping fingerprint reader or after a photo taken of their iris. Registration is a one-on-one a process that should take 2 minutes or less.

The accuracy of biometric systems
The accuracy of a biometric system should be considered before implementing a bio control program metrics. Three metrics used to assess the accuracy of biometrics: the False Reject Rate

One level of rejects
False rejection occurs when the subject is authorized rejected by systemic biometrics tem as invalid. Also called a false rejection
Type I error
, false rejection
One received a rate

A false acceptance occurs when the subject is not legitimately accepted as valid. If the biometric control organization produces many false rejection, overall control may have to lower the accuracy of the system by reducing the amount of data collected when authenticating the subject. When the data points derived, organizations risk of false acceptance rate increases. , an organization that is nization risk of unauthorized users gaining access. This type of error is also called a
Type II error
CRUNCH TIME
A false accept is worse than false rejects: most organizations would prefer to reject authentic subject to receiving a fraud. Fars (Type II error) is worse than FRRS (Type I error).

system
As the sensitivity of biometric systems increases, FRRS will rise and will Fars drop. Conversely, as the sensitivity is lowered, will go down and Fars FRRS will rise.

Type of biometric control
There are a number of biometric controls in use today. Here are the main implementations and their specific pros and cons associated with access control security.
fingerprint
prints jariadalah most widely used biometric controls available today. smartcard may bring fingerprint information. Many office buildings rely on the US Government fingerprint authentication for physical access to facilities. Examples include smart keyboard, which requires the user to present the fingerprint to unlock the computer screen saver.

Retinal scanning
Is a retinal scan laser scan capillaries that feed the retina from the back eye. It can interfere with personal because the rays must be straight enter the pupil, and users typically need to press their eyes to the laser scanner eyecup. Laser scanning map blood vessels of the retina. Health Information TIN CAN users by scanning the retina:
TEST WARNING
Retinal scans are rarely used because of health risks and invasion-of-privacy issues. Alternatives should be considered to control the exchange of biometric risks or bodily fluids increase the legitimate privacy concerns.

Iris Scan

An iris scan is passive biometric controls. A camera takes a picture of the iris (the the colored portion of the eye) and then compare the images in the authentication database. It also works through contact lenses and eyeglasses. Everyone is two slices iris is unique, even twins'.

hand geometry
biometric control, measurements were taken of the specific points on hand the subject: "The device uses a simple concept to measure and record Hand geometry devices are fairly simple and can store information in time as 9 bytes

Keyboard dynamics
refers to how hard a person presses any key and the rhythm by the key is pressed. Surprisingly, inexpensive access control for implement and can be effective. As people learn how to type and use a computer keyboard, they developed certain habits that are difficult to replicate, although it is not impossible.
Dynamic Signature

Dynamic signature
measuring process where a person signs his name.

Voiceprint
A voiceprint
measuring tone of voice subjects while stating specific sentence or
phrases. The type of access control is vulnerable to replay attacks (repeating a
sound recording), so that other access control should be implemented along with the voicemail
print. One such control requires the subject to express random words, protect against
Attackers play certain phrases recorded. Another problem is the people's voice can be
substantially changed due to illness, so the false rejection.
Facial scan
Facial scan
technology has greatly improved over the last few years. Scan- face
ning (also called face recognition) is a passive process of taking a picture of
the subject's face and compares that image to the list stored in the database. Although not
often used for biometric authentication control due to high costs, legal
enforcement agencies and security using face recognition and scanning technology
for biometric identification to improve the security of high-value, which is publicly accessible
targets.

Your Place
You describe the place of location-based access control using technologies such as
as the global positioning system (GPS), IP address geolocation-based, or physical
location to the point-of-sale purchases. These controls can deny access if the subject
in the wrong location
ACCESS CONTROL TECHNOLOGIES
There are several technologies that are used to implement access control.
Since every technology presented, it is important to identify what is unique about each
technical solutions.
Single sign-on
Single Sign-On (SSO) allows multiple systems to use a central authentication server
(US). This allows users to authenticate once and then access multiple, distinct systemic
tems. It also allows the security administrator to add, modify, or revoke user privileges
in one central system.
The main disadvantage to the SSO allows an attacker to gain access to
some sources after sacrificing any of the authentication methods, such as pass
said. SSO should always be used with multifactor authentication for this reason.
Federated identity management
Identity federation Management
(FIdM) applies Single Sign-On in the wider
scale: from cross-organization for Internet scale. Sometimes simply called
Identity Management (IDM). FIdM can use OpenID or SAML (Security Association
Markup Language).

According to EDUCAUSE, "Identity management refers to the policies, pro-
processes and technologies that build user identity and enforce rules on access
to digital resources. In a campus setting, many systems-such as e-mail information,
learning management systems, library databases, and grid computing applica-
require users to authenticate themselves (usually with a username and password).
An authorization process and then determine the system that the user is authenticated PER
mitted to access. With the company's identity management system, rather than having
separate credentials for each system, users can use a single digital identity to
to access all of the resources that the user is entitled. Per-federated identity management
mits extend this approach at the top level of the company, creating a trusted authority
for digital identities across multiple organizations. In a federated system, participat-
ing stock identity attributes based on agreed standards institutions, facilitating
authentication of another member of the federation and give appropriate access
for online resources. This approach flows access to digital assets while protecting it
ing limited resources. "
Kerberos
Kerberos
is a third-party authentication service that can be used to support
Single Sign-On. Kerberos (
http://www.kerberos.org/
) Kerberos uses symmetric encryption and mutual authentication provides a second
client and server. It protects against network sniffing and replay attacks.

QUICK FACTS
Kerberos has the following components:
•
School Principal
: Client (user) or service
•
nature
: A logical Kerberos network
•
ticket
: The data that authenticates the identity of the principal
•
credentials
: A ticket and key services
•
KDC
: Key Distribution Center, which authenticates principals
•
TGS
: Ticket-Granting Service
•
SESAME
SESAME is a European System Safe to A

pplication in a multivendor environment
ment, single sign-on system that supports heterogeneous environments.
SESAME can be considered as a sequel of sorts to Kerberos, "adds SESAME
Kerberos: heterogeneity, sophisticated
access control fea
tures, scalability
public key system, either managea
bility, auditing and delegation.
A penetration tester is a white hat hacker who receive authorization to download
entered into an electronic or physical perimeter organizations (and sometimes both).
Penetration test
(Called "pen test" for short) is designed to determine whether
black hat hacker can do the same thing. They are narrow, but often useful, tests, espe-
officially if the penetration tester successfully.
Penetration tests may include the following tests:
• Network (Internet)
• Network (internal or DMZ)
• Call war
• Wireless
• Physical (attempt to gain entry to the center or chamber)
• Wireless
Network attack can take advantage of client-side attacks, server-side attacks, or web appli
cation attacks. See

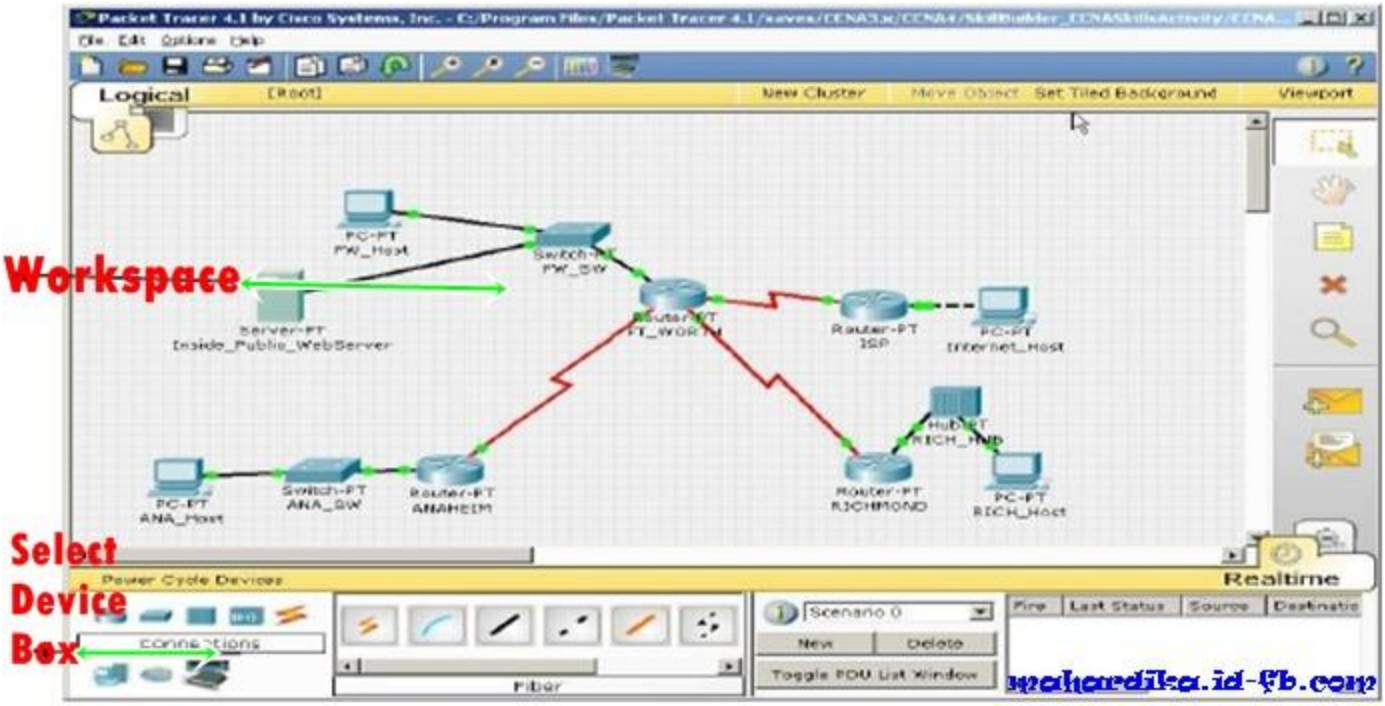
Call war
using the modem dial a phone series
number, look for an answering modem carrier tone (penetration tester later
trying to access the answering system); The name is derived from the 1983 movie
WarGames.
Social engineering
using the human mind to pass through security controls. Engineered social
neering can be used in combination with various types of attacks, particularly client
side attacks or physical tests. Examples of social engineering attacks combined
with a client-side attacks malware e-mail with the subject line "Category 5 Hur-
ricane is to hit Florida! "
AN
zero-knowledge
test "blind"; without external penetration tester starts
or reliable information and launch attacks with public information only.
Partial knowledge
test between zero and full knowledge:
penetration tester received some reliable information is limited.
Susceptibility testing

Vulnerability scanning
(Also called susceptibility testing) scan the network or system
for a list of vulnerabilities that have been defined as a system misconfiguration, obsolete
software, or lack of patches.
Security audit
Sebua security Haudit

is a test of the standard is published. Organizations can be audited
to PCI-DSS (Payment Card Industry Data Security Standard) compliance, for-example
ple. PCI-DSS includes many necessary controls, such as firewalls, certain access con-
control models, and wireless encryption.
Safety assessment
Security Assessment is a holistic approach to assess the effectiveness of access
control. Instead of looking at the narrow penetration test or vulnerability assessment,
security assessment has a broader scope.
SUMMARY PURPOSE EXAM
If one thinks about the castle analogy to security, access control will ditch and
the walls of the fort. Access control ensures that the border protection mechanisms, in the second
logical and physical standpoint, guaranteed. The goal of access control is to allow
authorized users access to the appropriate data and deny access to unauthorized users-
This is also known as the subject of restricting access to objects. Although this task is
complex and involved one, it is possible to implement strong access control pro
gram without burdening users who rely on access to the system.
Protecting the CIA triad is another key aspect to implement access control.
Confidentiality, integrity, and availability is very important.
Maintain security during the CIA of the system means enact special procedures
to access the data. This procedure will change depending on the function
users require and sensitivity of the data that is stored on the syste

2. **Packet Tracer**

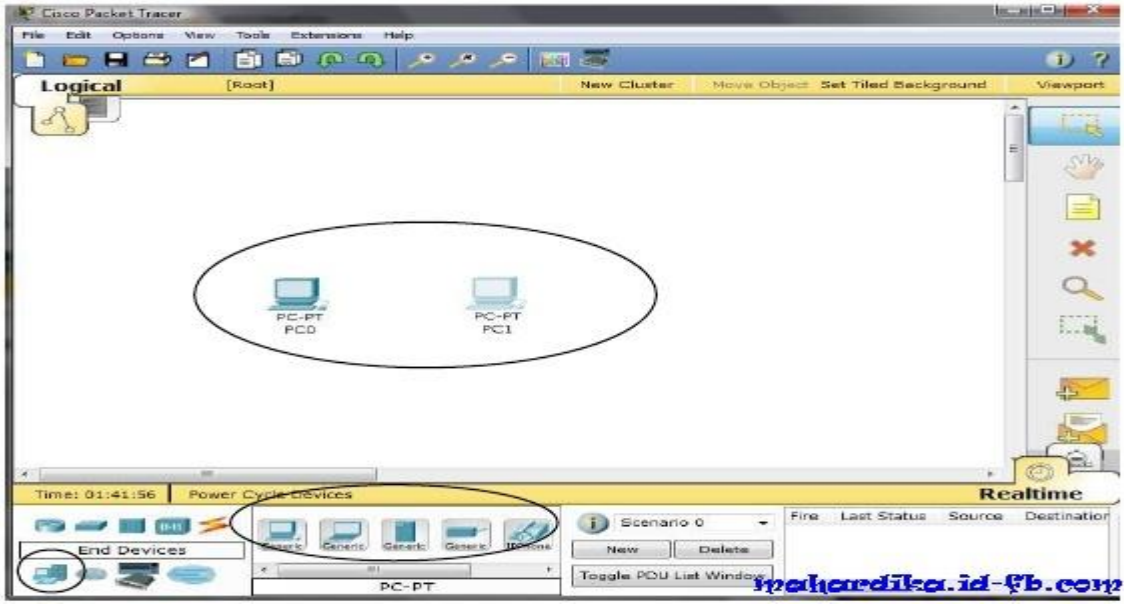
Packet tracer adalah sebuah simulator protocol jaringan yang dikembangkan oleh Cisco System. Paket Tracer dapat mensimulasikan berbagai macam protocol yg digunakan pada jaringan baik secara realtime maupun dengan mode simulasi.



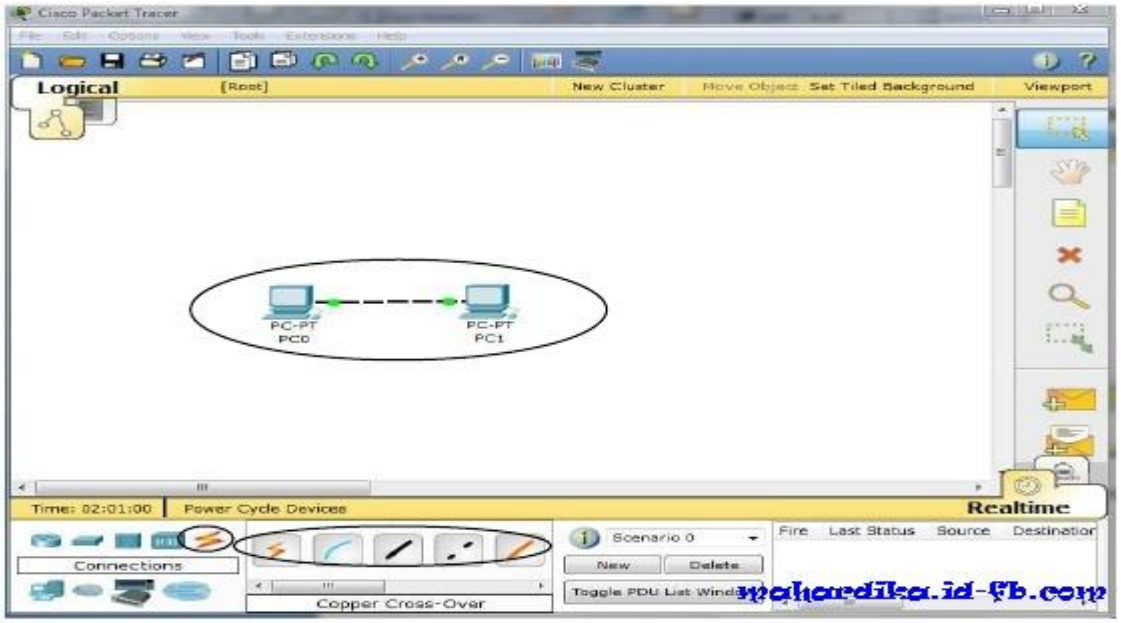
Gambar.1 Tampilan Packet Tracer

Membuat jaringan peer-to-peer menggunakan packet tracer :

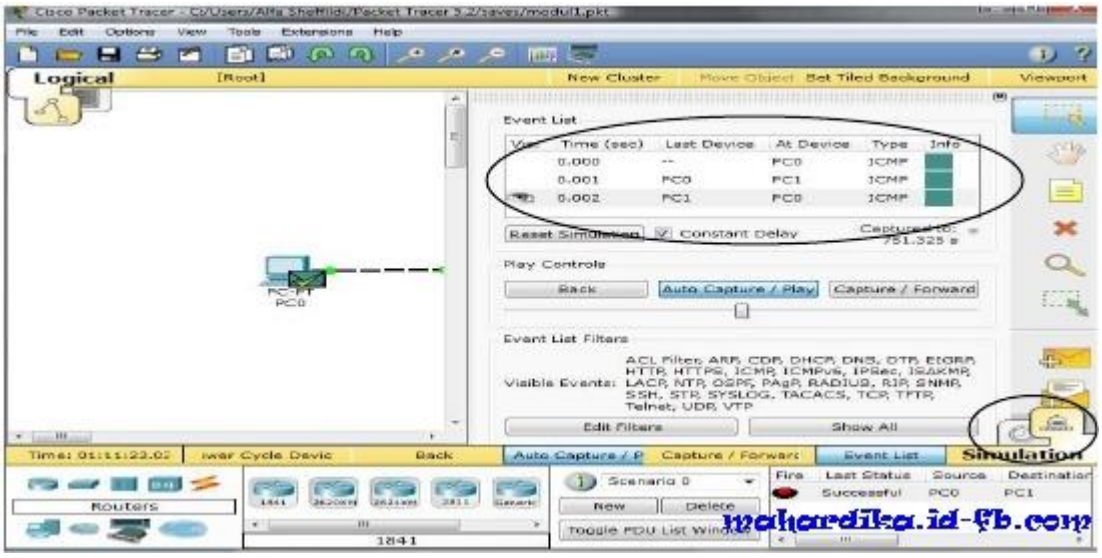
1.Ambil 2 buah PC dari select device box pada bagian end devices ke logical workspace seperti terlihat pada gambar dibawah ini :



2.Hubungkan 2 PC tadi dengan kabel yang sesuai (kabel cross) pada masing-masing port Ethernet



3.Selain mode realtime kita juga dapat memilih mode simulation, dimana pada saat kita melakukan perintah, kita dapat mengetahui prorokol yang digunakan dan apa yang sebenarnya terjadi pada setiap layer. Contohnya pada saat perintah ping pada gambar dibawah ini.

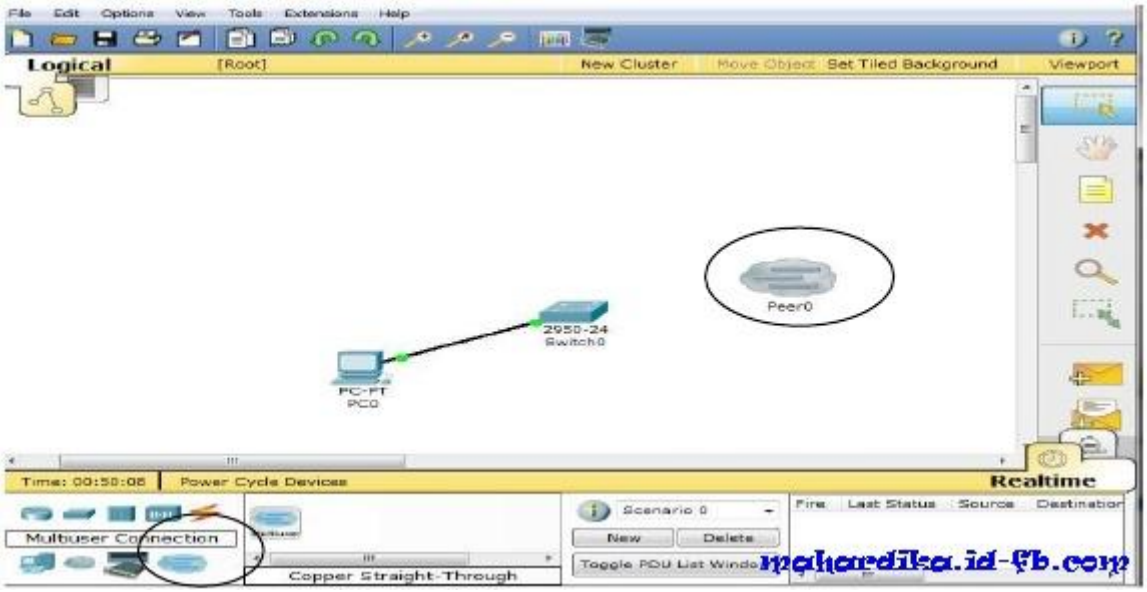


Membuat jaringan sederhana dengan menggunakan fitur multi user pada packet tracer :

Pada aplikasi packet tracer kita dimungkinkan untuk membuat simulasi jaringan gabungan antara simulasi jaringan menggunakan packet

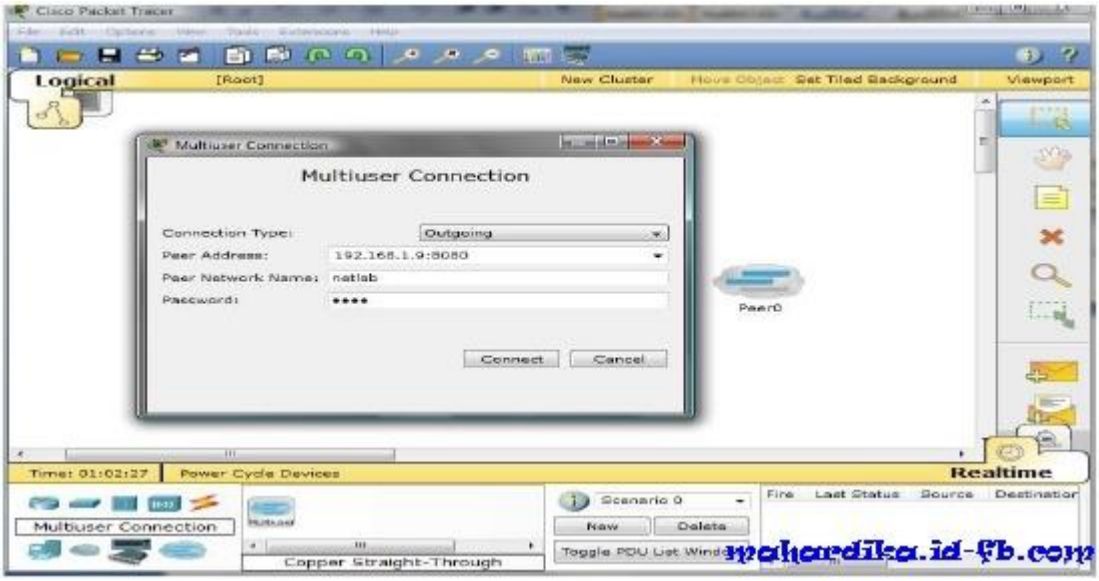
tracer di 2 atau lebih PC yang saling terhubung dalam satu network. Contoh penggunaan :

1.Buat jaringan sederhana lalu masukkan awan multiuser :



2.Klik pada awan multi user peer0, lalu set mode ke outgoing, dan ip address PC lain dimana terdapat simulasi jaringan yang akan dikoneksikan, set peer network name dan password

3.Tekan tombol connect dan tunggu konfirmasi koneksi (mode incoming) di PC yang dituju muncul. Setelah terkoneksi, kita langsung dapat menjalankan 2 simulasi di PC yang berbeda.



Network Analysis Tool

1.Network Analysis Tool

Wireshark merupakan salah satu network analysis tool, atau disebut juga dengan protocol analysis tool atau packet sniffer. Wireshark dapat digunakan untuk troubleshooting jaringan, analisis, pengembangan software dan protocol, serta untuk keperluan edukasi. Wireshark merupakan software gratis, sebelumnya,Wireshark dikenal dengan nama Ethereal.Packet sniffer sendiri diartikan sebagai sebuah program atau tool yang memiliki kemampuan untuk ﷺencegat dan melakukan pencatatan terhadap traffic data dalam jaringan. Selama terjadi aliran data dalam, packet sniffer dapat menangkap protocol data unit (PDU), melakukan dekoding serta melakukan analisis terhadap isi paket berdasarkan spesifikasi RFC atau spesifikasi-spesifikasi yang lain.Wireshark sebagai salah satu packet sniffer diprogram sedemikian rupa untuk mengenali berbagai macam protokol jaringan. Wireshark mampu menampilkan hasil enkapsulasi dan field yang ada dalam PDU.

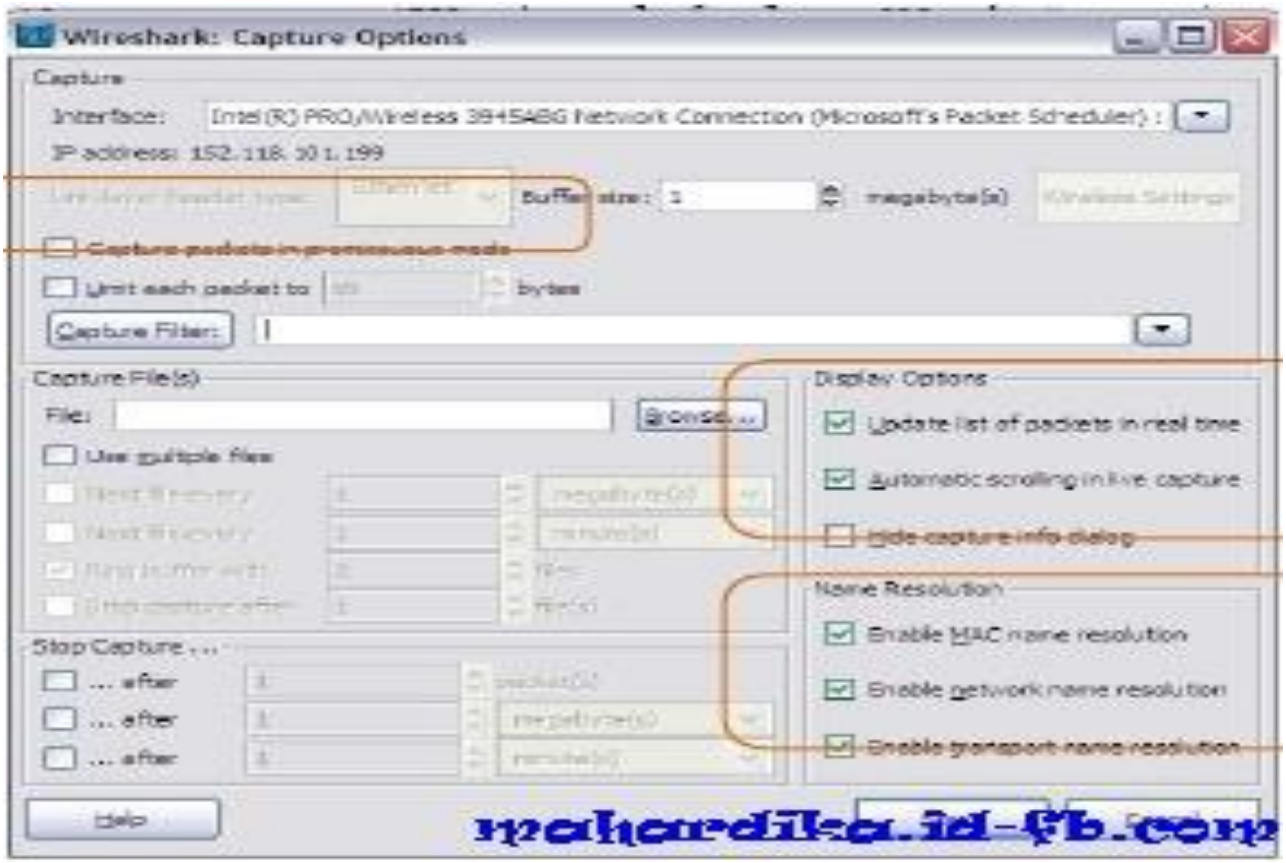
Prosedur

Pada bagian ini akan diberikan bagaimana menggunakan Wireshark serta contoh melakukan capture PDU.

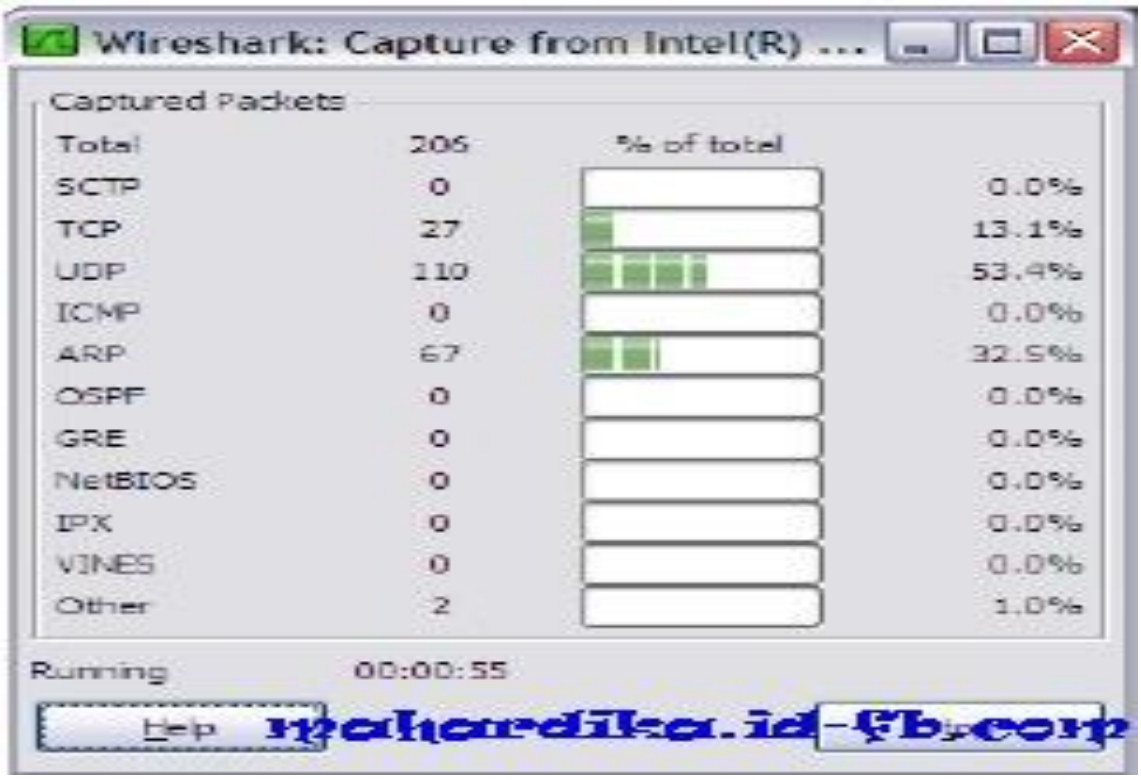
1)Jalankan Wireshark

2)Untuk melakukan capture dengan memilih pilihan yang tersedia, pilih menu

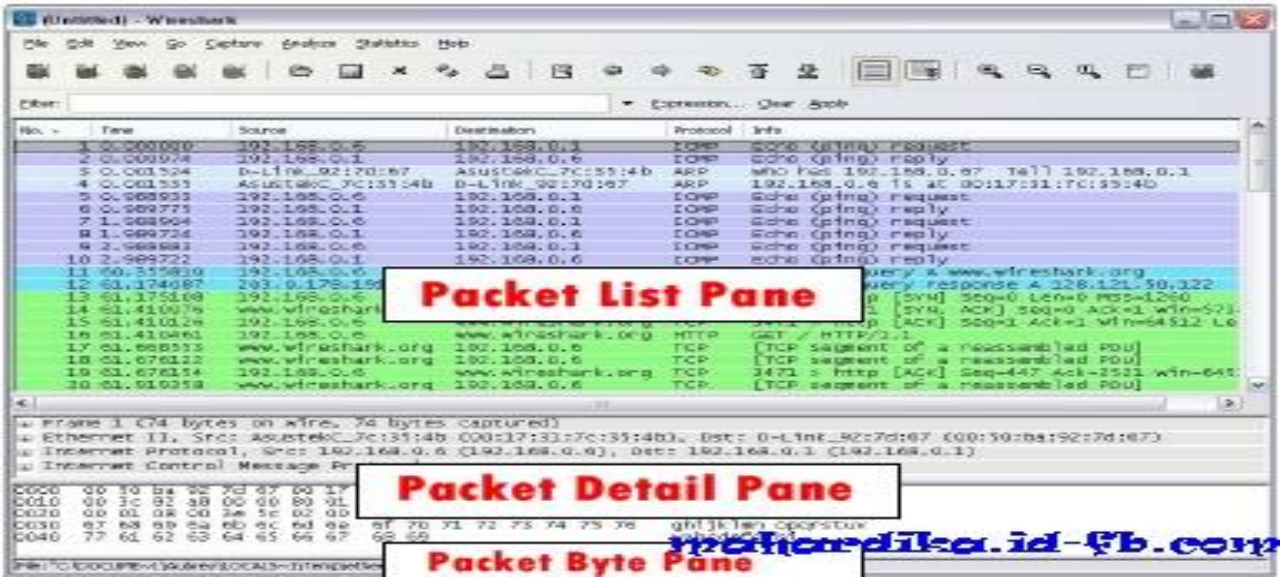
Capture > Options... akan tampil jendela semacam ini:



3.Pada jendela Capture Option, pilihlah interface Ethernet yang akan di-capture. Terlihat pada screenshot di atas terdapat 3 buah highlight. Highlight paling atas menunjukkan pilihan untuk melakukan capture pada Promiscuous Mode. Jika pilihan ini diaktifkan, maka Wireshark akan melakukan capture terhadap paket-paket yang ditujukan untuk komputer ini dan paket-paket yang terdeteksi oleh NIC dari komputer-komputer dalam satu segmen jaringan.Highlight kedua menunjukkan pilihan-pilihan untuk mengatur tampilan atau informasi yang akan ditampilkan oleh Wireshark. Jika pilihan hide capture dialog info dinonaktifkan, ketika kita memulai capture, Wireshark akan menampilkan jendela tambahan yang memberikan statistik persentase protokol yang ter-capture sebagai berikut:



Highlight ketiga memberikan pilihan bahwa Wireshark akan menerjemahakan alamat jaringan dalam PDU menjadi nama.Mengaktifkan pilihan ini akan menambah PDU ekstra ke dalam data yang ter-capture.Jendela Wireshark terdiri atas tiga bagian, seperti ditunjukkan pada screenshot berikut:



Packet List Pane menampilkan ringkasan dari paket-paket yang tertangkap oleh Wireshark.Memilih salah satu paket yang tampil pada bagian ini akan memperlihatkan detail dari paket tersebut pada dua panel di bawahnya.Packet Detail Pane menampilkan detail dari paket yang dipiliha pada Packet List Pane.Packet Byte Pane menunjukkan isi data dari sebuah paket dalam heksadesimal serta menunjukkan detail dari field yang dipilih pada Packet Detail Pane.Untuk memulai proses capture, klik pada tombol Start.

4)Buka command prompt dengan cara klik Start > Run... > ketikkan cmd >
klik OK. Lakukan ping ke komputer sebelah anda dengan mengetikkan perintah ping IPkomputerDiSebelahAnda.
5)Aktivitas ping tersebut akan terekam oleh Wireshark, simpan hasil capture dengan memilih menu File > Save As... pada Wireshark.
6)Berdasarkan hasil capture Wireshark tersebut, isikan informasi yang diminta pada borang yang disediakan.