

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/350049012>

MODUL PRAKTIKUM JARKOM DASAR & MEDIUM

Article · March 2021

CITATIONS

0

READS

1,411

1 author:



Muhamajir - Syamsu

Institut Teknologi dan Bisnis Ahmad Dahlan

3 PUBLICATIONS 0 CITATIONS

[SEE PROFILE](#)

MODUL PRAKTIKUM JARINGAN KOMPUTER (BASIC & MEDIUM)



Fakultas Tehnik & Desain
Jurusan : Teknologi Informasi & Sistem Informasi
Institut Teknologi & Bisnis Ahmad Dahlan

January 31,
th 2021

Penyusun :
Muhajir Syamsu



ITB AHMAD DAHLAN
Socio Technopreneur University

Muhajir Syamsu

Modul Praktikum Jaringan Komputer **(BASIC & MEDIUM)**

January 31, 2021



Kata Pengantar

Puji syukur penulis panjatkan kehadapan Tuhan Yang Maha Esa, karena atas berkat rahmatnya maka Modul Praktikum Jaringan Komputer (*Basic & Medium*) dapat diselesaikan.

Modul ini bertujuan sebagai panduan mahasiswa dalam mengikuti praktikum Jaringan Komputer. Modul ini dibagi menjadi beberapa sub modul yang akan dibahas pada setiap pertemuan dalam praktikum.

Penulis meminta maaf, jika dalam penulisan ini terdapat kesalahan baik yang disengaja atau tidak disengaja. Untuk itu, penulis terbuka terhadap saran dan pesan untuk menyempurnakan modul praktikum ini.

Ciputat,..... Januari 2021

Penulis



Daftar Isi

Kata Pengantar
Daftar Isi
1 MODUL I PENGANTAR JARINGAN KOMPUTER
1.1 Tujuan Praktikum
1.2 Indikator Pencapaian.....
1.3 Materi.....
1.3.1. Sejarah Jaringan Komputer
1.3.2. Evolusi Jaringan.....
1.3.2.1. Mainframe Pada Era 1960-1970 an.....
1.3.2.2. LAN (Local Area Network) pada era 1970-1980 an..
1.3.2.3. WAN (Wide Area Network) Pada Era 1980-1990 an.
1.3.3.4. Internet Pada Era 1990 an.....
1.3.2.5. Konsep Jaringan Komputer.....
1.3.3. Tujuan Jaringan Komputer.....
1.3.4. Kriteria Jaringan Komputer
1.3.4.1. Berdasarkan Distribusi Sumber Informasi/Data
1.3.4.2. Berdasarkan Jangkauan Geografis Dibedakan Menjadi
1.3.4.3. Berdasarkan Peranan Dan Hubungan Tiap Komputer Dalam Memproses Data.....
1.3.4.4. Berdasarkan Media Transmisi Data
1.3.5. Perangkat Keras Jaringan.....
1.3.5.1. Network Interface Cards (NIC) atau Kartu Jaringan
1.3.5.2. Ethernet Card / Kartu Jaringan Ethernet
1.3.5.3. Media (kabel, Gelombang Radio)
1.3.6. Hub/Konsentrator
1.3.7. Swicth/Hub
1.3.8. Repeaters.....
1.3.9. Bridges / Jembatan
1.3.10. Routers.....
1.3.11. Printer Dan Peripheral Lain
1.3.12. Model Open System Interconnection (OSI).....
1.3.12.1. Sejarah Model OSI Layer.....
1.3.12.2. Model Layer OSI.....
1.3.12.3. Kegunaan Model OSI.....
1.3.12.4. Enkapsulasi OSI Layer.....
1.3.12.5. Cara Kerja OSI Layer
1.4 Alat dan Bahan
1.5 Praktikum
1.6 Referensi
1.7 Tugas
1.8 Laporan.....



2 MODUL II PENGALAMATAN JARINGAN

2.1	Tujuan Praktikum
2.2	Indikator Pencapaian.....
2.3	Materi.....
2.3.1.	Protokol TCP/IP.....
2.3.2.	Arsitektur TCP/IP
2.3.2.1.	Protokol Lapisan Application.....
2.3.2.2.	Protokol Lapisan Transport
2.3.2.3.	Protokol Lapisan Internet.....
2.3.2.4.	Protokol Lapisan Network Access
2.3.3.	Layanan Pada TCP/IP
2.3.4.	Port TCP
2.3.5.	IP Address
2.3.5.1.	IP Address Versi 4
2.3.5.3.	IP Address Versi 6.....
2.3.6.	Pengalokasikan IP Address
2.3.6.1.	Network ID
2.3.6.2.	Host ID
2.3.7.	Range IP Address
2.3.8.	MAC Address
2.3.9.	Pengertian Topologi.....
2.3.9.1.	Topologi Bus
2.3.9.2.	Topologi Ring (Cincin)
2.3.9.3.	Topologi Star (Bintang).....
2.3.9.4.	Topologi Tree (Pohon)
2.3.9.5.	Topologi Mesh (Tak beraturan)
2.4	Alat dan Bahan
2.5	Praktikum
2.6	Referensi
2.7	Tugas
2.8	Laporan.....

3 MODUL III PENGANTAR SUBNETTING

3.1	Tujuan Praktikum
3.2	Indikator Pencapaian.....
3.3	Materi.....
3.3.1.	Pengertian subnetting.....
3.3.2.	Pengertian Subnet Mask
3.3.3.	Representasi Subnet Mask.....
3.3.4.	Perhitungan Subnetting
3.3.5.	CIDR (Classless Inter-Domain Routing)
3.3.5.1.	Perhitungan Subnetting CIDR.....
3.3.5.2.	Subnetting Pada Kelas C
3.3.5.3.	Subnetting Pada Kelas B.....



3.3.5.4.	Subnetting Pada Kelas A
3.3.6.	VLSM (Variable Length Subnet Mask)
3.3.6.1.	Perhitungan Subnetting VLSM
3.4	Alat dan Bahan
3.5	Praktikum
3.6	Referensi
3.7	Tugas
3.8	Laporan.....

4 MODUL IV PENGENALAN PENGKABELAN

4.1	Tujuan Praktikum
4.2	Indikator Pencapaian.....
4.3	Materi.....
4.3.1.	Kabel LAN.....
4.3.2.	Arsitektur Jaringan
4.3.3.	10Base2
4.3.4.	10Base5
4.3.5.	10BaseT
4.3.6.	10BaseF
4.3.7.	100BaseT
4.3.8.	100VG-AnyLAN.....
4.3.9.	Jenis – Jenis Kabel LAN
4.3.9.1.	Twisted Pair
4.3.9.1.1.	Kabel Unshielded Twisted Pair (UTP)
4.3.9.1.2.	Kabel Shielded Twisted Pair (STP)
4.3.9.2.	Kabel Coaxial.....
4.3.9.3.	Thick coaxial cable (Kabel Coaxial “gemuk”)
4.3.9.4.	Thin coaxial cable (Kabel Coaxial “Kurus”)
4.3.9.5.	Kabel Serat Optik (Fiber Optik)
4.3.10.	Proses Penyambungan FO
4.3.11.	Pemasangan Connector FO
4.3.12.	Jenis-Jenis Kabel Fo
4.3.12.1.	Single Mode
4.3.12.2.	Multi Mode Step Index
4.3.12.3.	Multimode Grade Index.....
4.3.13.	Crimping
4.4	Alat dan Bahan
4.5	Praktikum
4.6	Referensi
4.7	Tugas
4.8	Laporan.....



5 MODUL V PENGANTAR LAN (LOCAL AREA NETWORK)

5.1	Tujuan Praktikum
5.2	Indikator Pencapaian.....
5.3	Materi.....
5.3.1.	Pengertian LAN
5.3.2.	Jaringan Peer To Peer
5.3.3.	Jaringan Client – Server.....
5.3.4.	Konfigurasi Jaringan pada Windows 10
5.3.4.1.	Mengkonfigurasi TCP/IP
5.3.4.2.	Konfigurasi Jaringan Peer To Peer.....
5.3.4.3.	Konfigurasi Jaringan Client – Server
5.3.5.	Pengenalan VLAN (Virtual Local Area Network)
5.3.5.1.	Bagaimana VLAN Bekerja
5.3.5.2.	Tipe - Tipe Vlan.....
5.3.5.3.	Konfigurasi Jaringan VLAN
5.3.5.4.	Konfigurasi Jaringan Asymmetric VLAN & Port Management.....
5.3.6.	Pengertian Wireless LAN (WLAN)
5.3.7.	Standarisasi Wireless LAN
5.3.8.	Frekuensi yang Digunakan pada WLAN
5.3.9.	Mode pada WLAN.....
5.3.9.1.	Mode Ad-Hoc
5.3.9.2.	Mode Infrastruktur
5.3.10.	Komponen-komponen pada WLAN
5.3.10.1.	Access Point.....
5.3.10.2.	WLAN Interface
5.3.10.3.	Mobile/Desktop PC
5.3.10.4.	Antena
5.3.11.	Konfigurasi Komponen WLAN
5.3.12.	Konfigurasi WLAN Mode Ad-Hoc
5.4	Alat dan Bahan
5.5	Praktikum
5.6	Referensi
5.7	Tugas
5.8	Laporan.....

6 MODUL VI ROUTER DASAR

6.1	Tujuan Praktikum
6.2	Indikator Pencapaian.....
6.3	Materi.....
6.3.1.	DHCP
6.3.1.1.	DHCP Scope
6.3.1.2.	DHCP Lease.....



6.3.1.3. DHCP Options
6.3.2. Cara Kerja DHCP
6.3.2.1. DHCP Server.....
6.3.2.2. DHCP Client
6.3.3. Router
6.3.4. Jenis - Jenis Router.....
6.3.5. Konfigurasi Jaringan Pada Router.....
6.3.5.1. Konfigurasi Jaringan Pada Router Menggunakan DHCP Dinamis
6.3.5.2. Konfigurasi Jaringan Pada Router Menggunakan DHCP Static
6.4 Alat dan Bahan
6.5 Praktikum
6.6 Referensi
6.7 Tugas
6.8 Laporan.....

7 MODUL VII MONITORING DAN REMOTE PC

7.1 Tujuan Praktikum
7.2 Indikator Pencapaian.....
7.3 Materi.....
7.3.1. Monitoring dan Remote PC.....
7.3.2. Network Management
7.3.2.1. Konsep Dasar SNMP
7.3.3 Langkah-langkah Instalasi Aplikasi The Dude.....
7.3.4. Langkah-langkah Untuk Menemukan Jaringan
7.3.5. Radmin.....
7.3.5.1. Prinsip Operasi Radmin
7.3.6. Sejarah Radmin
7.3.7. Fitur-Fitur Pada Radmin.....
7.3.8. Tahap Instalasi Pada Penggunaan.....
7.3.9. Tahap Instalasi Pada Server.....
7.4 Alat dan Bahan
7.5 Praktikum
7.6 Referensi
7.7 Tugas
7.8 Laporan.....



8 MODUL VIII WINDOWS SERVER 2016

8.1	Tujuan Praktikum
8.2	Indikator Pencapaian.....
8.3	Materi..... 8.3.1. Pengenalan Windows Server 2016..... 8.3.2. Edisi Windows Server 2016..... 8.3.3. Active Directory
	8.3.4. DNS Server
	8.3.5. DHCP Server..... 8.3.5.1. Cara Kerja DHCP Server
	8.3.5.2. DHCP Scope
	8.3.5.3. DHCP Lease.....
	8.3.5.4. DHCP Options
	8.3.6. Virtual Box
	8.3.7. Proses Installasi Windows Server 2016 DiVirtualBox.....
	8.3.8. Proses Instalasi dan Konfigurasi Active Directory Domain Service..... 8.3.8.1. Konfigurasi pada client Windows
	8.3.8.2. Konfigurasi pada client Linux
	8.3.9. Active Directory User and Computer (Membuat User Account)
	8.3.10. Instalasi dan Konfigurasi DHCP Server
	8.3.11. Menghubungkan Client dengan Komputer Server
	8.3.12. Membuat Sharing Folder.....
	8.3.13. Membuka drive sharing
8.4	Alat dan Bahan
8.5	Praktikum
8.6	Referensi
8.7	Tugas
8.8	Laporan.....

STUDI KASUS (PROJECT MAHASISWA).....

1.	Studi Kasus I.....
2.	Studi Kasus II.....
3.	Studi Kasus III.....
4.	Studi Kasus IV
5.	Studi Kasus V.....



MODUL I

PENGANTAR JARINGAN KOMPUTER

1.1 Tujuan Praktikum

1. Untuk mengenal awal mula jaringan komputer
2. Untuk mengetahui konsep proses distribusi (Distributed Processing)
3. Untuk mengetahui evolusi jaringan
4. Untuk mengetahui konsep kerja jaringan komputer
5. Untuk mengetahui perangkat kerja jaringan komputer

1.2 Indikator Pencapaian

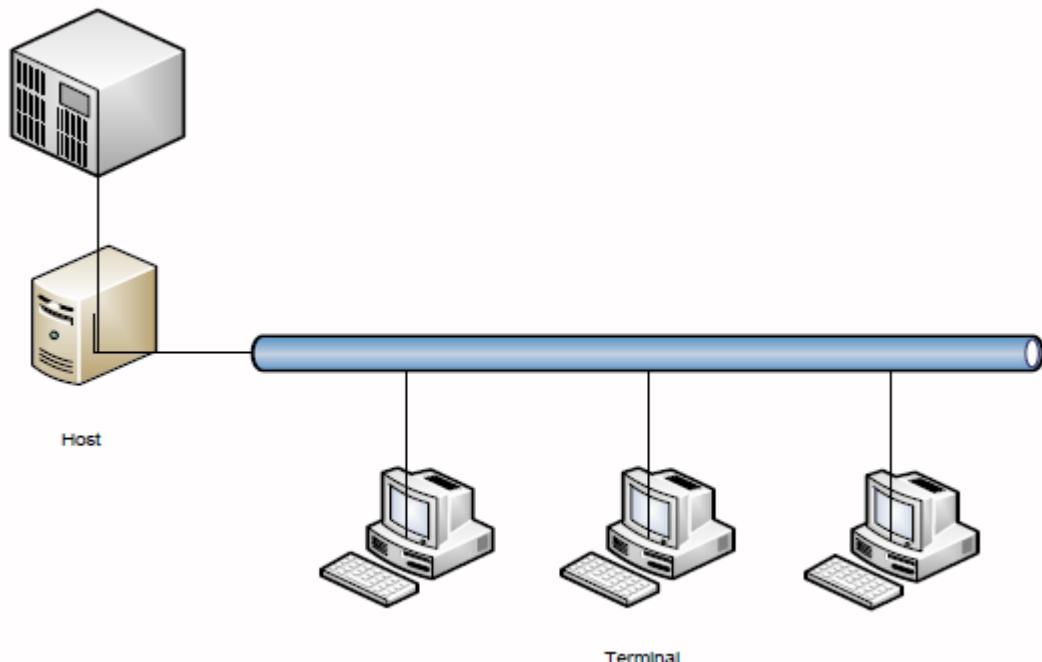
1. Mampu memahami konsep jaringan dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University.
2. Mampu memahami Jaringan Komputer Model TSS
3. Mampu mengembangkan Jaringan Komputer Model Distributed Processing
4. Mampu membedakan evolusi jaringan
5. Mampu menerapkan sebuah konsep dan manfaat jaringan komputer
6. Mampu membedakan kriteria dari jaringan komputer

1.3 Materi

1.3 1. Sejarah Jaringan Komputer

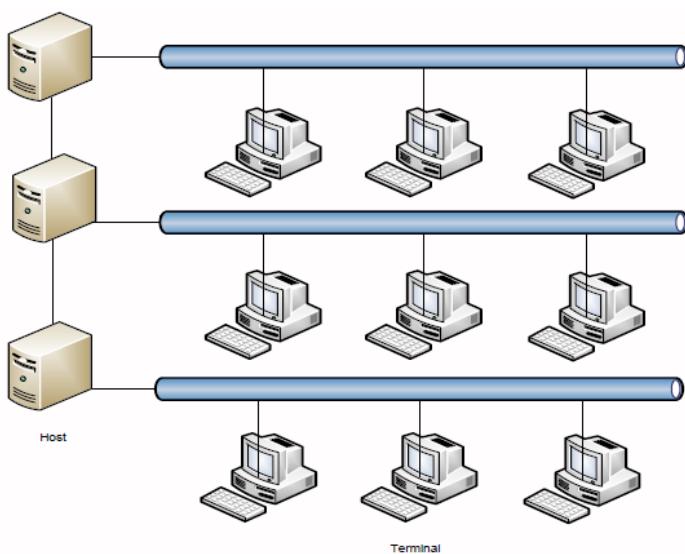
Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (Batch Processing), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan dengan kaidah antrian.

Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. (Lihat Gambar 1.1) Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar 1.1 Jaringan Komputer Model TSS

Memasuki tahun 1970-an, setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (Distributed Processing). Seperti pada (Gambar 1.2). dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer. Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.



Gambar 1.2 Jaringan Komputer Model Distributed Processing



Selanjutnya ketika harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam dari mulai menangani proses bersama maupun komunikasi antar komputer (Peer to Peer System) saja tanpa melalui komputer pusat.

Untuk itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN. Demikian pula ketika Internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa WAN.

1.3.2. Evolusi Jaringan

1.3.2.1. Mainframe Pada Era 1960-1970 an

Pada tahun 1940-an komputer adalah suatu alat dengan ukuran besar yang sangat rentan terhadap kesalahan. Pada tahun 1947, ditemukannya transistor semikonduktor membuat banyak kemungkinan untuk membuat komputer dengan ukuran lebih kecil dan tentunya lebih handal.

Pada tahun 1950-an institusi-institusi besar mulai menggunakan komputer-komputer mainframe, dimana dijalankan dengan program-program punched card. Pada akhir tahun 1950-an, Integrated circuit (IC) yang mengembangkan beberapa dan sekarang jutaan, transistor pada satu semikonduktor yang kecil telah ditemukan. pada tahun 1960-an, mainframe dengan terminal dan IC telah banyak digunakan.

1.3.2.2. LAN (Local Area Network) pada era 1970-1980 an

Pada akhir 1960-an dan 1970-an komputer-komputer yang lebih kecil dengan sebutan minikomputer telah diciptakan. Walau bagaimana-pun, minikomputer- minikomputer masih dalam ukuran yang sangat besar dibanding dengan standar modern saat ini. Pada tahun 1977, Apple Computer Company memperkenalkan mikrokomputer, dimana dikenal dengan sebutan MAC.

Pada tahun 1981 IBM memperkenalkan PC pertamanya. Mac yang user-friendly, IBM PC yang open-archetecture, dan langkah lebih jauh dari proses "micro-minisasi" dari IC membawahi penyebaran luas dari PC baik di rumah maupun di kantor-kantor. Pada masa ini jaringan-jaringan local mulai dibuat dikembangkan dengan berbagai macam teknologi.

1.3.2.3. WAN (Wide Area Network) Pada Era 1980-1990 an

Pada pertengahan 1980 pengguna PC mulai menggunakan modem untuk berbagi file dengan komputer lain. Hal ini dikenal sebagai point-to-point, atau komunikasi dial-up. Konsep ini disebar oleh penggunaan komputer yang merupakan pusat dari komunikasi dalam koneksi dial-up. Komputer-komputer ini disebut bulletin boards.

Para pengguna akan terhubung ke bulletin boards, meninggalkan dan mengambil pesan sebagaimana upload dan download file. Kekurangan



dari tipe ini adalah sangat sedikitnya komunikasi langgung dan selanjutnya hanya orang-orang tertentu yang tahu mengenai bulletin board. Pembatasan lain dari bulleting board adalah satu modem per satu koneksi. Jika lima orang terhubung secara simultan, hal ini akan memerlukan lima modem terkoneksi ke lima jalur telepon terpisah. Jumlah orang yang ingin menggunakan sistem ini berkembang, sistem ini selanjutnya tidak dapat meng-handle kebutuhan yang terus meningkat. Sebagai contoh, bayangkan jika 500 orang ingin terhubung dalam waktu yang bersamaan.

1.3.3.4. Internet Pada Era 1990 an

Dari tahun 1960-an ke tahun 1990-an Departemen Pertahanan Amerika Serikat (DoD) mengembangkan Wide-Area Networks (WANs) yang besar, dapat diandalkan untuk militer dan alasan-alasan sains. Teknologi ini berbeda dari komunikasi point-to-point yang digunakan dalam bulletin boards. Hal ini memungkinkan beberapa komputer untuk terhubung secara bersamaan melalui beberapa jalur berbeda.

Jaringan itu sendiri akan bisa membedakan bagaimana memindahkan data dari komputer satu ke komputer lain. Satu koneksi dapat digunakan untuk berhubungan dengan banyak komputer pada saat yang bersamaan. Jaringan yang diterapkan DoD nantinya akan menjadi jaringan yang mendunia pada saat ini yang disebut Internet.

1.3.2.5. Konsep Jaringan Komputer

Dalam ilmu komputer dan teknologi informasi, dikenal istilah jaringan komputer. Jaringan komputer adalah sekumpulan komputer yang dapat saling berhubungan antara satu dengan lainnya dengan menggunakan media komunikasi, sehingga dapat saling berbagi data, informasi, program, dan perangkat keras (printer, harddisk, webcam, dsb).

Berbeda dengan konsep jaringan dalam ilmu biologi –yaitu kumpulan sel yang fungsinya sejenis komputer-komputer yang terhubung dalam jaringan komputer tidak harus sejenis. Komputer-komputer tersebut bisa saja memiliki tipe yang berbeda-beda, menggunakan sistem operasi yang berbeda, dan menggunakan program/aplikasi yang berbeda pula.

Tetapi komputer-komputer yang terhubung dalam jaringan komputer harus memakai aturan komunikasi (protokol) yang sama. Hal ini dimaksudkan agar masing-masing komputer dapat berkomunikasi yang baik dengan komputer lainnya. Protokol yang menjadi Standar Internasional adalah TCP/IP (Transmission Control Protocol / Internet Protocol).



1.3.3. Tujuan Jaringan Komputer

Dibandingkan dengan komputer yang berdiri sendiri (stand-alone), jaringan komputer memiliki beberapa keunggulan antara lain:

1. Berbagi peralatan dan sumber daya
Beberapa komputer dimungkinkan untuk saling memanfaatkan sumber daya yang ada, seperti printer, harddisk, serta perangkat lunak bersama, seperti aplikasi perkantoran, basis data (database), dan sistem informasi. Penggunaan perangkat secara bersama ini akan menghemat biaya dan meningkatkan efektivitas peralatan tersebut.
2. Integrasi data
Jaringan komputer memungkinkan pengintegrasian data dari atau ke semua komputer yang terhubung dalam jaringan tersebut.
3. Komunikasi
Jaringan komputer memungkinkan komunikasi antar pemakai komputer, baik melalui e-mail, teleconference dsb.
4. Keamanan (Security)
Jaringan komputer mempermudah dalam pemberian perlindungan terhadap data. Meskipun data pada sebuah komputer dapat diakses oleh komputer lain, tetapi kita dapat membatasi akses orang lain terhadap data tersebut. Selain itu kita juga bisa melakukan pengamanan terpusat atas seluruh komputer yang terhubung ke jaringan.

1.3.4. Kriteria Jaringan Komputer

1.3.4.1. Berdasarkan Distribusi Sumber Informasi/Data

1. Jaringan terpusat
Jaringan ini terdiri dari komputer client dan server yang mana komputer klien yang berfungsi sebagai perantara untuk mengakses sumber informasi/data yang berasal dari satu komputer server.
2. Jaringan terdistribusi
Merupakan perpaduan beberapa jaringan terpusat sehingga terdapat beberapa komputer server yang saling berhubungan dengan klien membentuk sistem jaringan tertentu.



1.3.4.2. Berdasarkan Jangkauan Geografis Dibedakan Menjadi

1. Jaringan LAN

Merupakan jaringan yang menghubungkan 2 komputer atau lebih dalam cakupan seperti laboratorium, kantor, serta dalam 1 warnet.

2. Jaringan MAN

Merupakan jaringan yang mencakup satu kota besar beserta daerah setempat. Contohnya jaringan telepon lokal, sistem telepon seluler, serta jaringan relay beberapa ISP internet.

3. Jaringan WAN

Merupakan jaringan dengan cakupan seluruh dunia. Contohnya jaringan PT. Telkom, PT. Indosat, serta jaringan GSM Seluler seperti Satelindo, Telkomsel, dan masih banyak lagi.

1.3.4.3. Berdasarkan Peranan Dan Hubungan Tiap Komputer Dalam Memproses Data

1. Jaringan Client-Server

Pada jaringan ini terdapat 1 atau beberapa komputer server dan komputer client. Komputer yang akan menjadi komputer server maupun menjadi komputer client dan diubah-ubah melalui software jaringan pada protokolnya. Komputer client sebagai perantara untuk dapat mengakses data pada komputer server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer client.

2. Jaringan Peer-to-peer

Pada jaringan ini tidak ada komputer client maupun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi sehingga semua komputer berfungsi sebagai client sekaligus sebagai server.

1.3.4.4. Berdasarkan Media Transmisi Data

1. Jaringan Berkabel (Wired Network)

Pada jaringan ini, untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar komputer jaringan.

2. Jaringan Nirkabel (Wireless Network)

Merupakan jaringan dengan medium berupa gelombang elektromagnetik. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan



1.3.5. Perangkat Keras Jaringan

1.3.5.1. Network Interface Cards (NIC) atau Kartu Jaringan

Kartu Jaringan (NIC) merupakan perangkat yang menyediakan media untuk menghubungkan antara komputer, kebanyakan kartu jaringan adalah kartu internal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer. Beberapa komputer seperti komputer MAC, menggunakan sebuah kotak khusus yang ditancapkan ke port serial atau SCSI port komputernya.

Pada computer notebook ada slot untuk kartu jaringan yang biasa disebut PCMCIA slot. Kartu jaringan yang banyak terpakai saat ini adalah : kartu jaringan Ethernet, LocalTalk konektor, dan kartu jaringan Token Ring. Yang saat ini populer digunakan adalah Ethernet, lalu diikuti oleh Token Ring, dan LocalTalk.

1.3.5.2. Ethernet Card / Kartu Jaringan Ethernet

Kartu jaringan Ethernet biasanya dibeli terpisah dengan komputer, kecuali seperti komputer Macintosh yang sudah mengikutkan kartu jaringan Ethernet didalamnya. kartu Jaringan ethernet umumnya telah menyediakan port koneksi untuk kabel Koaksial ataupun kabel twisted pair, jika didesain untuk kabel koaksial konenektorya adalah BNC, dan apabila didesain untuk kabel twisted pair maka akan punya konektor RJ-45. Beberapa kartu jaringan ethernet kadang juga punya konektor AUI. Semua itu di koneksi dengan koaksial, twisted pair, ataupun dengan kabel fiber optik.



Gambar 1.3 Kartu Jaringan Ethernet

1. LocalTalk Connectors/Konektor LocalTalk

LocalTalk adalah peralatan jaringan untuk komputer macintosh, ini menggunakan sebuah kotak adapter khusus dan kabel yang terpasang ke Port untuk printer. Kekurangan dari LocalTalk dibandingkan Ethernet adalah kecepatan laju transfer datanya, Ethernet di Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perusahaan

tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan jaringan komputer yang terhubungan dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah pengguna jaringan komputer yang tergabung dalam Internet berlipat ganda. asanya dapat sampai 10 Mbps, sedangkan LocalTalk hanya dapat beroperasi pada kecepatan 230 Kbps atau setara dengan 0.23 Mbps.

2. Token Ring Cards

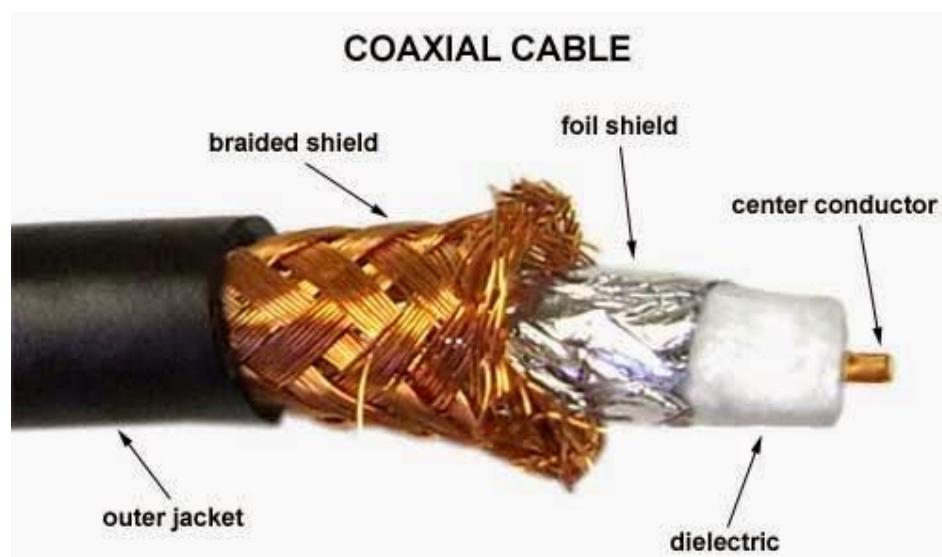
Kartu jaringan Token Ring terlihat hampir sama dengan Kartu jaringan Ethernet. Satu perbedaannya adalah tipe konektor di belakang Kartu jaringannya, Token Ring umumnya mempunyai tipe konektor 9 Pin DIN yang menyambung Kartu jaringan ke Kabel Network

1.3.5.3. Media (kabel, Gelombang Radio)

Empat jenis kabel jaringan yang umum digunakan saat ini yaitu :

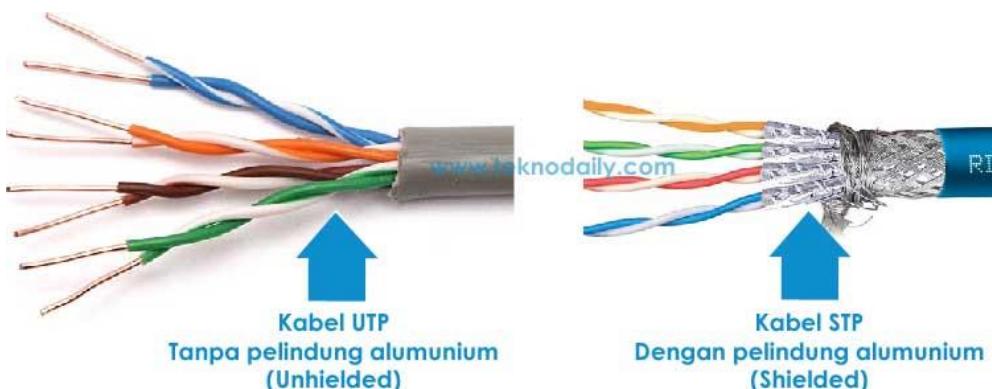
1. Kabel Coaxial

Terdiri atas dua kabel yang diselubungi oleh dua tingkat isolasi. Tingkat isolasi pertama adalah yang paling dekat dengan kawat konduktor tembaga. Tingkat pertama ini dilindungi oleh serabut konduktor yang menutup bagian atasnya yang melindungi dari pengaruh elektromagnetik. Sedangkan bagian inti yang digunakan untuk transfer data adalah bagian tengahnya yang selanjutnya ditutup atau dilindungi dengan plastik sebagai pelindung akhir untuk menghindari dari goresan kabel. Beberapa jenis kabel coaxial lebih besar dari pada yang lain. Makin besar kabel, makin besar kapasitas datanya, lebih jauh jarak jangkauannya dan tidak begitu sensitif terhadap interferensi listrik.



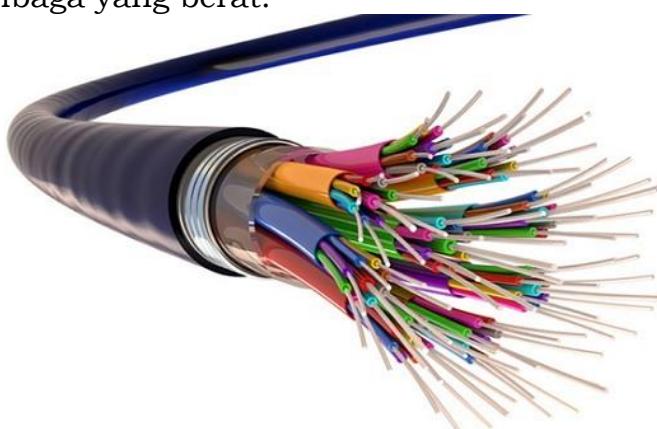
Gambar 1.4 Kabel Coxial

2. Kabel Unshielded Twisted Pair (UTP)
Kabel twisted pair terjadi dari dua kabel yang diputar enam kali per-inchi untuk memberikan perlindungan terhadap interferensi listrik ditambah dengan impedensi, atau tahanan listrik yang konsisten. Nama yang umum digunakan untuk kawat ini adalah IBM jenis/kategori 3. Secara singkat kabel UTP adalah murah dan mudah dipasang, dan bisa bekerja untuk jaringan skala kecil.
3. Kabel Shielded Twisted Pair (STP)
Kabel STP sama dengan kabel UTP, tetapi kawatnya lebih besar dan diselubungi dengan lapisan pelindung isolasi untuk mencegah gangguan interferensi. Jenis kabel STP yang paling umum digunakan pada LAN ialah IBM jenis/kategori 1.



Gambar 1.5 Contoh Kabel UTP dan STP

4. Kabel Serat Optik (Fiber Optik)
Kabel serat optik mengirim data sebagai pulsa cahaya melalui kabel serat optik. Kabel serat optik mempunyai keuntungan yang menonjol dibandingkan dengan semua pilihan kabel tembaga. Kabel serat optik memberikan kecepatan transmisi data tercepat dan lebih reliable, karena jarang terjadi kehilangan data yang disebabkan oleh interferensi listrik. Kabel serat optik juga sangat tipis dan fleksibel sehingga lebih mudah dipindahkan dari pada kabel tembaga yang berat.



Gambar 1.6 Kabel Fiber Optik

1.3.6. Hub/Konsentrator



Gambar 1.7 Hub/Konsentrator

Sebuah Konsentrator/Hub adalah sebuah perangkat yang menyatukan kabel-kabel network dari tiap-tiap workstation, server atau perangkat lain. Dalam topologi Bintang, kabel twisted pair datang dari sebuah workstation masuk kedalam hub. Hub mempunyai banyak slot concentrator yang mana dapat dipasang menurut nomor port dari card yang dituju. Ciri-ciri yang dimiliki Konsentrator adalah :

1. Biasanya terdiri dari 8, 12, atau 24 port RJ-45
 2. Digunakan pada topologi Bintang/Star
 3. Biasanya di jual dengan aplikasi khusus yaitu aplikasi yang mengatur manajemen port tersebut.
 4. Biasanya disebut hub
- Biasanya di pasang pada rak khusus, yang didalamnya ada Bridges, router

1.3.7. Swicth/Hub



Gambar 1.8 Hub/Switch



Switch jaringan (atau switch untuk singkatnya) adalah sebuah alat jaringan yang melakukan bridging transparan (penghubung segementasi banyak jaringan dengan forwarding berdasarkan alamat MAC).

Switch dapat dikatakan sebagai multi-port bridge karena mempunyai collision domain dan broadcast domain tersendiri, dapat mengatur lalu lintas paket yang melalui switch jaringan.

Cara menghubungkan komputer ke switch sangat mirip dengan cara menghubungkan komputer atau router ke hub. Switch dapat digunakan langsung untuk menggantikan hub yang sudah terpasang pada jaringan.

Switch jaringan dapat digunakan sebagai penghubung komputer atau router pada satu area yang terbatas, switch juga bekerja pada lapisan data link, cara kerja switch hampir sama seperti bridge, tetapi switch memiliki sejumlah port sehingga sering dinamakan multi-port bridge

1.3.8. Repeaters



Gambar 1.9 Repeaters

Contoh yang paling mudah adalah pada sebuah LAN menggunakan topologi Bintang dengan menggunakan kabel unshielded twisted pair. Dimana diketahui panjang maksimal untuk sebuah kabel unshielded twisted pair adalah 100 meter, maka untuk menguatkan sinyal dari kabel tersebut dipasanglah sebuah repeater pada jaringan tersebut.

1.3.9. Bridges / Jembatan

Adalah sebuah perangkat yang membagi satu buah jaringan kedalam dua buah jaringan, ini digunakan untuk mendapatkan jaringan yang efisien, dimana kadang pertumbuhan network sangat cepat makanya perlukan jembatan untuk itu.

Kebanyakan Bridges dapat mengetahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan sebelahnya dan juga pada jaringan yang lain di sebelahnya pula. Diibaratkan bahwa Bridges ini seperti polisi lalu lintas yang mengatur di persimpangan jalan pada saat jam-jam sibuk.



Dia mengatur agar informasi di antara kedua sisi network tetap jalan dengan baik dan teratur. Bridges juga dapat di gunakan untuk mengkoneksi diantara network yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.



Gambar 1.10 Bridges

1.3.10. Routers

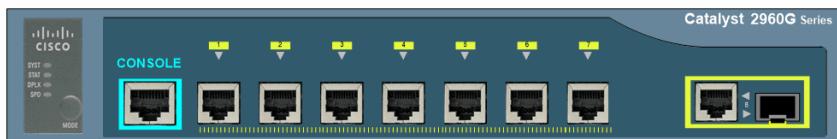
Sebuah Router mengartikan informasi dari satu jaringan ke jaringan yang lain, dia hampir sama dengan Bridge namun lebih pintar, router akan mencari jalur yang terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal. Sementara Bridges dapat mengetahui alamat masing-masing komputer dimasing- masing sisi jaringan, router mengetahui alamat komputerr, bridges dan router lainnya. router dapat mengetahui keseluruhan jaringan melihat sisi manayang paling sibuk dan dia bisa menarik data dari sisi yang sibuk tersebut sampaisisi tersebut bersih.

Jika sebuah perusahaan mempunyai LAN dan menginginkan terkoneksi keInternet, mereka harus membeli router. Ini berarti sebuah router dapatmenyerahkan informasi diantara LAN anda dan Internet. ini juga berartimencarikan alternatif jalur yang terbaik untuk mengirimkan data melewatiinternet.Ini berarti Router itu :

1. Mengatur jalur sinyal secara effisien
2. Mengatur Pesan diantara dua buah protocol
3. Mengatur Pesan diantara topologi jaringan linear Bus dan Bintang(star)

Mengatur Pesan diantara melewati Kabel Fiber optic, kabel koaksial atau kabel twisted pair

Catalyst 2960 Front



outer 1921 Rear



Gambar 1.11 Router Tampak Depan dan Belakang

1.3.11. Printer Dan Peripheral Lain



Gambar 1.12 Printer

Printer adalah salah satu alasan utama kenapa ada network. Karena printer tidak selalu digunakan oleh setiap pemakai, akan lebih ekonomis jika memakai satu printer bersama-sama. Printer bisa dihubungkan langsung pada workstation atau ke server. kalian juga bisa memasang scanner, CD-ROM eksternal dan peralatan lain yang berguna dan dapat digunakan secara bersama-sama pada network. Sama seperti yang lainnya, hal ini membutuhkan perangkat lunak dan perangkat keras yang tepat.



1.3.12. Model Open System Interconnection (OSI)

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetujui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/interpreter atau satu bahasa yang dimengerti kedua belah pihak.

Dalam dunia komputer dan telekomunikasi interpreter identik dengan protokol. Untuk itu maka pada tahun 1977 di Eropa sebuah badan dunia yang menangani masalah standarisasi ISO (International Standardization Organization) membuat aturan baku sebuah model arsitektural jaringan.

1.3.12.1. Sejarah Model OSI Layer

Dahulu pada era 70-an, banyak perusahaan software maupun hardware yang membuat System Network Architektur (SNA), yang antara lain IBM, Digital, Sperry, Burrough dsb. Tentunya masing – masing perusahaan tersebut membuat aturan – aturan sendiri yang satu sama lain tidak sama, misalkan IBM mengembangkan SNA yang hanya memenuhi kebutuhan komputer – komputer IBM.

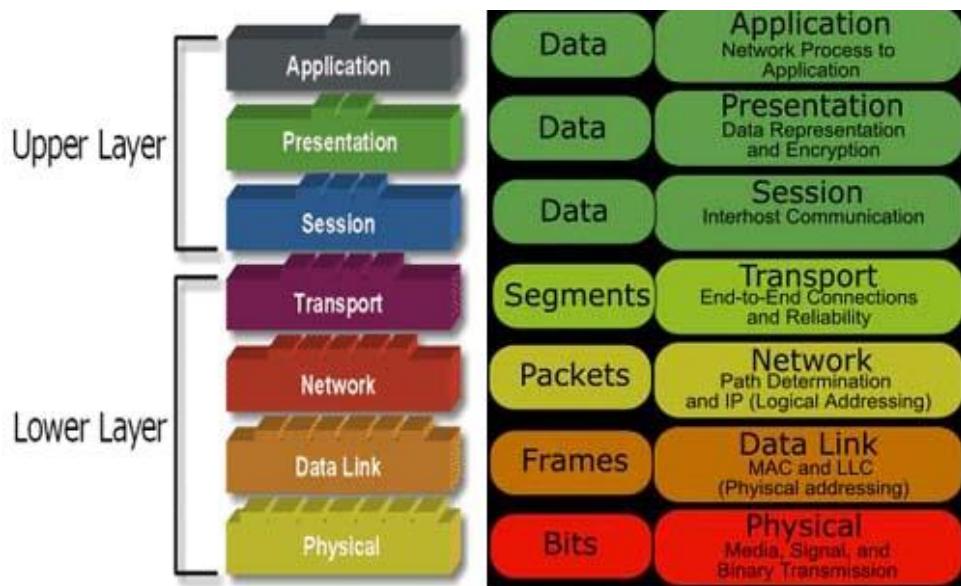
Dari sini kemudian timbul masalah misalkan jaringan komputer menggunakan SNA produk IBM ingin dihubungkan dengan SNA produk Digital tentunya tidak bisa, hal ini disebabkan protokolnya tidak sama.

Analoginya, misalkan anda berbicara dengan bahasa jawa, tentunya akan dimengerti pula orang lain yang juga bisa berbahasa Jawa, misalkan anda berbicara dengan orang Sunda apakah bahasa anda bisa diterima oleh orang tersebut? tentunya tidak? Masalah ini bisa diselesaikan jika anda berbicara menggunakan bahasa standar yang tentunya bisa dimengerti lawan bicara anda.

Menghadapi kenyataan ini, kemudian The International Standard Organization (ISO) pada sekitar tahun 1980-an, meluncurkan sebuah standar model referensi yang berisi cara kerja serangkaian protokol SNA. Model referensi ini selanjutnya dinamakan Open System Interconnection (OSI).

Model Referensi OSI terdiri dari 7 buah bagian (layer), yang masing – masing layer mempunyai tugas sendiri – sendiri. Dikarenakan OSI terdiri dari 7 macam layer, maka model referensi OSI seringkali disebut 7 OSI layer

1.3.12.2. Model Layer OSI



Gambar 1.13 Model OSI Layer

Terdapat 7 layer pada model OSI. Setiap layer bertanggungjawab secara khusus pada proses komunikasi data. Misal, satu layer bertanggungjawab untuk membentuk koneksi antar perangkat, sementara layer lainnya bertanggungjawab untuk mengoreksi terjadinya “error” selama proses transfer data berlangsung.

Model Layer OSI dibagi dalam dua group: “upper layer” dan “lower layer”. “Upper layer” fokus pada aplikasi pengguna dan bagaimana file direpresentasikan di komputer. Untuk Network Engineer, bagian utama yang menjadi perhatiannya adalah pada “lower layer”. Lower layer adalah intisari komunikasi data melalui jaringan aktual.

1.3.12.3. Kegunaan Model OSI

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. Termasuk jenis-jenis protokol jaringan dan metode transmisi.

Model dibagi menjadi 7 layer, dengan karakteristik dan fungsinya masing-masing. Tiap layer harus dapat berkomunikasi dengan layer di atasnya maupun dibawahnya secara langsung melalui serentetan protokol dan standard

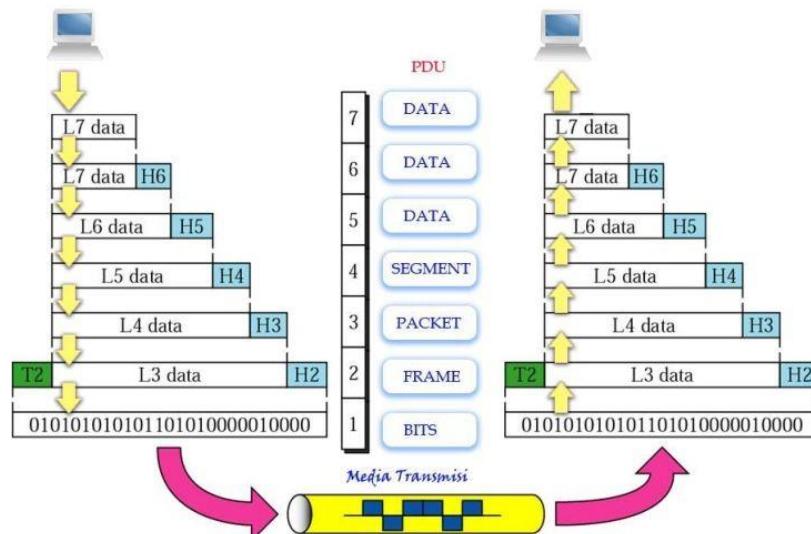


Tabel 1.1 Lapisan OSI Layer

Lapisan Ke-	Nama Lapisan	Keterangan
7	Application layer	Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.
6	Presentation layer	Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (redirection software), seperti layanan Workstation (dalam Windows NT) dan juga Network shell (semacam Virtual Network Computing (VNC) atau Remote Desktop Protocol (RDP)).
5	Session layer	Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.
4	Transport layer	Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.
3	Network layer	Berfungsi untuk mendefinisikan alamat-alamat IP, membuat header untuk paket-paket, dan kemudian melakukan routing melalui internetworking dengan menggunakan router dan switch layer-3.
2	Data-link layer	Berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, flow control, pengalamanan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menentukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan Logical Link Control (LLC) dan lapisan Media Access Control (MAC).
1	Physical layer	Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana Network Interface Card (NIC) dapat berinteraksi dengan media kabel atau radio.

1.3.12.4. Enkapsulasi OSI Layer

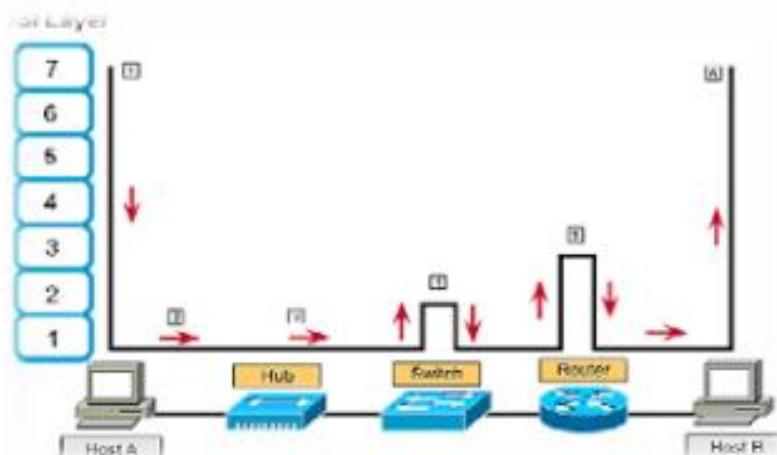
Agar sebuah data dapat terkirim dengan baik perlu dilakukan enkapsulasi terhadap data tersebut. Enkapsulasi adalah sebuah proses menambahkan header dan trailer atau melakukan pemaketan pada sebuah data. Dengan enkapsulasi data menjadi memiliki identitas. Bayangkan sebuah surat yang akan dikirim tetapi tanpa amplop, alamat dan perangko. Tentu saja surat tidak akan sampai ke tujuan. Amplop dengan alamat dan perangko adalah sama dengan enkapsulasi pada data.



Gambar 1.14 Enkapsulasi 7 OSI Layer

1.3.12.5. Cara Kerja OSI Layer

Cara Kerja yang dimaksud adalah proses berjalannya sebuah data dari sumber ke tujuan melalui OSI layer. Jadi untuk mencapai tujuan sebuah data harus melalui lapisan-lapisan OSI terlebih dahulu.



Gambar 1.15 Cara Kerja OSI Layer Pada Jaringan



Berikut akan dijelaskan bagaimana jalannya data dari host A menuju host B sesuai dengan nomor pada gambar.

1. Pertama-tama data dibuat oleh Host A. Kemudian data tersebut turun dari Application layer sampai ke physical layer (dalam proses ini data akan ditambahkan header setiap turun 1 lapisan kecuali pada Physical layer, sehingga terjadi enkapsulasi sempurna).
2. Data keluar dari host A menuju kabel dalam bentuk bit (kabel bekerja pada Physical layer).
3. Data masuk ke hub, tetapi data dalam bentuk bit tersebut tidak mengalami proses apa-apa karena hub bekerja pada Physical layer.
4. Setelah data keluar dari hub, data masuk ke switch. Karena switch bekerja pada Datalink layer/ layer 2, maka data akan naik sampai layer 2 kemudian dilakukan proses, setelah itu data turun dari layer 2 kembali ke layer 1 / phisical layer.
5. Setelah data keluar dari switch, data masuk ke router. Karena router bekerja pada layer 3/ Network layer, maka data naik sampai layer 3 kemudian dilakukan proses, setelah itu data turun dari layer 3 kembali ke layer 1 , dan data keluar dari router menuju kabel dalam bentuk bit.
6. Pada akhirnya data sampai pada host B. Data dalam bentuk bit naik dari layer 1 sampai layer 7. Dalam proses ini data yang dibungkus oleh header-header layer OSI mulai dilepas satu persatu sesuai dengan lapisannya (berlawanan dengan proses no 1). Setalah data sampai di layer 7 maka data siap dipakai oleh host B.

1.3 Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
3. Crimpping Tools
4. Kabel
5. Multi Tester
6. Router
7. Switch
8. Hub
9. Aplikasi Packet Tracer
10. Software virtualisasi (VMware)

1.4 Praktikum

1. Instalasi OS Windows/linux
2. Mengerjakan Jobsheet Praktikum



1.5 Referensi

1. Micro, Andi. 2012. Dasar-dasar Jaringan Komputer. Banjarbaru: Andi Micro.
2. Digital Equipment Corporation; Intel Corporation; Xerox Corporation (September 1980). "The Ethernet: A Local Area Network". ACM SIGCOMM Computer Communication Review. 11 (3): 20. doi:10.1145/1015591.1015594. Version 1.0 of the DIX specification.
3. "Ethernet Technologies". Internetworking Technology Handbook. Cisco Systems. Diakses tanggal April 11, 2011.
4. Charles E. Spurgeon (2000). Ethernet: The Definitive Guide. O'Reilly Media. ISBN 978-1565-9266-08.

1.6 Tugas

Buatlah sebuah makalah dengan tema “PENGGUNAAN JARINGAN KOMPUTER DALAM KEHIDUPAN SEHARI” dan untuk judul silahkan ditentukan sendiri

1.7 Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, MODUL I PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Bottom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



MODUL II

PENGALAMATAN JARINGAN

2.1 Tujuan Praktikum

1. Untuk mengetahui cara kerja protokol TCP/IP (Transmission Control Protocol/Internet Protocol)
2. Untuk mengetahui protokol – protokol utama pada TCP/IP
3. Untuk mengetahui layanan – layanan pada TCP/IP
4. Untuk menerapkan berbagai macam topologi jaringan

2.2 Indikator Pencapaian

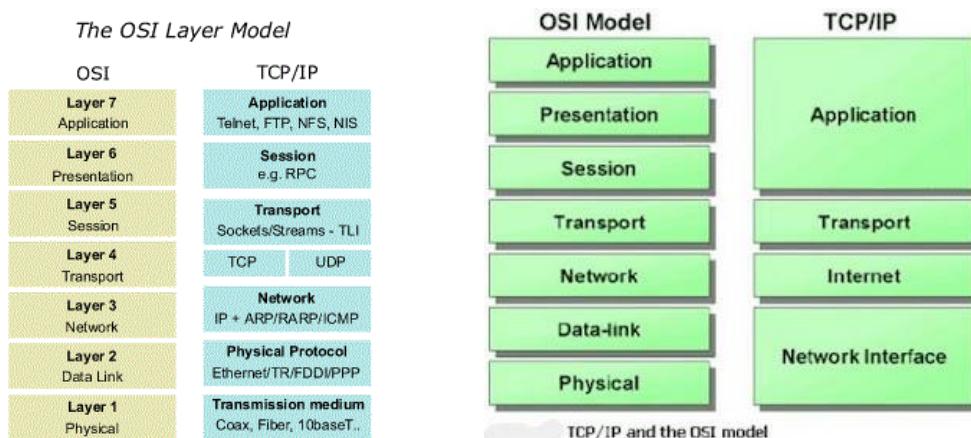
1. Mampu mengaosiasikan protokol – protokol utama pada TCP/IP
2. Mampu menggunakan port dalam berbagai macam konfigurasi jaringan
3. Mampu menerapkan IPv4 dan IPv6 dalam jaringan komputer

2.3 Materi

2.3.1. Protokol TCP/IP

Protokol Jaringan yang banyak digunakan saat ini adalah protokol TCP/IP (Transmission Control Protocol/Internet Protocol) yang merupakan sekelompok protokol yang mengatur komunikasi data komputer di internet. Komputer-komputer yang terhubung ke internet berkomunikasi dengan TCP/IP, karena menggunakan bahasa yang sama perbedaan jenis komputer dan sistem operasi tidak menjadi masalah. Jadi jika sebuah komputer menggunakan protocol TCP/IP dan terhubung langsung ke internet, maka komputer tersebut dapat berhubungan dengan komputer manapun yang terhubung dengan internet.

2.3.2. Arsitektur TCP/IP



Gambar 2.1 Perbandingan Model OSI dengan TCP/IP



Arsitektur TCP/IP tidaklah berbasis model referensi tujuh lapis OSI, tetapi menggunakan model referensi DARPA. Seperti diperlihatkan dalam diagram, TCP/IP mewujudkan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini, dapat dipetakan (meski tidak secara langsung) terhadap model referensi OSI. Empat lapis ini kadang-kadang disebut sebagai DARPA Model, Internet Model, atau DoD Model, mengingat TCP/IP merupakan protokol yang awalnya dikembangkan dari proyek ARPANET yang dimulai oleh Departemen Pertahanan Amerika Serikat. Setiap lapisan yang dimiliki oleh kumpulan protokol (protocol suite) TCP/IP diasosiasikan dengan protokolnya masing-masing

2.3.2.1. Protokol Lapisan Application

Bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), dan masih banyak protokol lainnya. Dalam beberapa implementasi stack protokol, seperti halnya Microsoft TCP/IP, protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka Windows Sockets (Winsock) atau NetBIOS over TCP/IP (NetBT).

2.3.2.2. Protokol Lapisan Transport

Berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat connection-oriented atau broadcast yang bersifat connectionless. Protokol dalam lapisan ini adalah Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP).

2.3.2.3. Protokol Lapisan Internet

Bertanggung jawab untuk melakukan pemetaan (routing) dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), dan Internet Group Management Protocol (IGMP).

3.3.2.4. Protokol Lapisan Network Access

Bertanggung jawab untuk meletakkan frame-frame jaringan di atas media jaringan yang digunakan. TCP/IP dapat bekerja dengan banyak teknologi transport, mulai dari teknologi transport dalam LAN (seperti halnya Ethernet dan Token Ring), MAN dan WAN (seperti halnya dial-up modem yang berjalan di atas Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), serta Asynchronous Transfer Mode (ATM)).



2.3.3. Layanan Pada TCP/IP

- a. Pengiriman file (File Transfer)
File Transfer Protokol (FTP) memungkinkan user dapat mengirim atau menerima file dari komputer jaringan.
- b. Remote Login
Network Terminal Protokol (telnet). Memungkinkan user untuk melakukan login ke dalam suatu komputer di dalam jaringan.
- c. Computer Mail
Digunakan untuk menerapkan sistem e-mail, Protokol yang digunakan:
 - SMTP (Simple Mail Transport Protokol) untuk pengiriman email
 - POP (Post Office Protokol) dan IMAP (Internet Message Access Control) untuk menerima email
 - MIME (Multipurpose Internet Mail Extensions) untuk mengirimkan data selain teks
- d. Network File System (NFS)
Pelayanan akses file jarak jauh yang memungkinkan klien untuk mengakses file pada komputer jaringan jarak jauh walaupun file tersebut disimpan lokal.
- e. Remote Execution
Memungkinkan user untuk menjalankan suatu program dari komputer yang berbeda.
- f. Name Servers
Nama database alamat yang digunakan pada internet.
- g. IRC (Internet Relay Chat)
Memberikan layanan chat
- h. Streaming (Layanan audio dan video)
Jenis layanan yang langsung mengolah data yang diterima tanpa menunggu mengolah data selesai dikirim.

2.3.4. Port TCP

Port TCP mampu mengindikasikan sebuah lokasi tertentu untuk menyampaikan segmen-semen TCP yang dikirimkan yang diidentifikasi dengan TCP Port Number. Nomor-nomor di bawah angka 1024 merupakan port yang umum digunakan dan ditetapkan oleh IANA (Internet Assigned Number Authority). Tabel berikut ini menyebutkan beberapa port TCP yang telah umum digunakan.

Tabel 2.1 Port TCP

Nomor TCP	Keterangan
20	File Transfer Protocol/FTP (digunakan untuk saluran data)



Nomor TCP	Keterangan
21	File Transfer Protocol/FTP (digunakan untuk saluran kontrol)
23	Simple Mail Transfer Protocol/SMP yang digunakan untuk mengirim e-mail
25	Telnet
80	Hypertext Transfer Protocol/HTTP yang digunakan untuk World Wide Web.
110	Post Office Protocol 3/POP3 yang digunakan untuk menerima e-mail.
139	NetBIOS over TCP session service

Port TCP merupakan hal yang berbeda dibandingkan dengan port UDP, meskipun mereka memiliki nomor port yang sama. Port TCP merepresentasikan satu sisi dari sebuah koneksi TCP untuk protokol lapisan aplikasi, sementara port UDP merepresentasikan sebuah antrean pesan UDP untuk protokol lapisan aplikasi. Selain itu, protokol lapisan aplikasi yang menggunakan port TCP dan port UDP dalam nomor yang sama juga tidak harus sama.

Sebagai contoh protokol Extended Filenam Server (EFS) menggunakan port TCP dengan nomor 520, dan protokol Routing Information Protocol (RIP) menggunakan port UDP juga dengan nomor 520. Jelas, dua protokol tersebut sangatlah berbeda! Karenanya, untuk menyebutkan sebuah nomor port, sebutkan juga jenis port yang digunakannya, karena hal tersebut mampu membingungkan (ambigu).

2.3.5. IP Address

2.3.5.1. IP Address Versi 4

Sebuah jenis pengalaman jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan secara teoritis dapat mengalami hingga 4 miliar host komputer atau lebih tepatnya $4.294.967.296$ host di seluruh dunia, jumlah host tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4(karena terdapat 4 oktet) sehingga nilai maksimal dari alamat IP versi 4 tersebut adalah 255.255.255.255 dimana nilai dihitung dari nol sehingga nilai nilai host yang dapat ditampung adalah $256 \times 256 \times 256 \times 256 = 4.294.967.296$ host

2.3.5.3. IP Address Versi 6

Sebuah jenis pengalaman jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 6. Panjang



totalnya adalah 128-bit, dan secara teoritis dapat mengalami hingga $2^{128} = 3,4 \times 10^{38}$ host komputer di seluruh dunia. Contoh alamat IP versi 6 sebagai berikut : 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.

2.3.6. Pengalokasikan IP Address

2.3.6.1. Network ID

Bagian dari IP address yang digunakan untuk menunjuk jaringan tempat komputer ini berada.

2.3.6.2. Host ID

Class A	Network	Host		
Octet	1	2	3	4
Class B	Network	Host		
Octet	1	2	3	4
Class C	Network			Host
Octet	1	2	3	4
Class D	Host			
Octet	1	2	3	4

Gambar 2.2 Network & Host ID Pada Tiap Class IP Address

2.3.7. Range IP Address

Tabel 2. 2 : Tabel Range IP Address

IP Adress Class	High Orders Bits	Fist Octet Address Range	Number Of Bits In The Network Address
Class A	0	0 – 126 (00000001 – 01111110)	8
Class B	10	128 – 191 (10000000 – 10111111)	16
Class C	110	192 – 223 (11000000 – 11011111)	24
Class D	1110	224 – 239 (11100000 – 11101111)	28
Class E	1111	240 – 255 (11110000 – 11111111)	32



ITB AHMAD DAHLAN
Socio Technopreneur University

127 adalah kelas yang dicadangkan untuk alamat loopback, digunakan untuk pengujian dan tidak dapat diberikan ke jaringan.

ITB-AHMAD DAHLAN CIPUTAT

Jl. Ir. H. Juanda No.77 Cirendeu, Ciputat Tangerang Selatan

ITB-AHMAD DAHLAN KARAWACIH

Jl. Imam Bonjol No.4/9, RT.001/RW.009, Panunggangan Bar
Kec. Cibodas, Kota Tangerang Banten 15138



2.3.8. MAC Address

MAC Address (Media Access Control Address) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasi sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address.

MAC Address mengizinkan perangkat-perangkat dalam jaringan agar dapat berkomunikasi antara satu dengan yang lainnya. Sebagai contoh, dalam sebuah jaringan berbasis teknologi Ethernet, setiap header dalam frame Ethernet mengandung informasi mengenai MAC address dari komputer sumber (source) dan MAC address dari komputer tujuan (destination). Beberapa perangkat, seperti halnya bridge dan switch Layer-2 akan melihat pada informasi MAC address dari komputer sumber dari setiap frame yang ia terima dan menggunakan informasi MAC address ini untuk membuat "tabel routing" internal secara dinamis. Perangkat-perangkat tersebut pun kemudian menggunakan tabel yang baru dibuat itu untuk meneruskan frame yang ia terima ke sebuah port atau segmen jaringan tertentu di mana komputer atau node yang memiliki MAC address tujuan berada.

Dalam sebuah komputer, MAC address ditetapkan ke sebuah kartu jaringan (network interface card/NIC) yang digunakan untuk menghubungkan komputer yang bersangkutan ke jaringan. MAC Address umumnya tidak dapat diubah karena telah dimasukkan ke dalam ROM. Beberapa kartu jaringan menyediakan utilitas yang mengizinkan pengguna untuk mengubah MAC address, meski hal ini kurang disarankan. Jika dalam sebuah jaringan terdapat dua kartu jaringan yang memiliki MAC address yang sama, maka akan terjadi konflik alamat dan komputer pun tidak dapat saling berkomunikasi antara satu dengan lainnya. Beberapa kartu jaringan, seperti halnya kartu Token Ring mengharuskan pengguna untuk mengatur MAC address (tidak dimasukkan ke dalam ROM) sebelum dapat digunakan.

MAC address memang harus unik dan untuk itulah, Institute of Electrical and Electronics Engineers (IEEE) mengalokasikan blok-blok dalam MAC address. 24 bit pertama dari MAC address merepresentasikan siapa pembuat kartu tersebut dan 24 bit sisanya merepresentasikan nomor kartu tersebut. Setiap kelompok 24 bit tersebut dapat direpresentasikan dengan menggunakan enam digit bilangan heksadesimal, sehingga menjadikan total 12 digit bilangan heksadesimal yang merepresentasikan keseluruhan MAC address. Berikut merupakan tabel beberapa pembuat kartu jaringan populer dan nomor identifikasi dalam MAC Address.



<i>Nama Vendor</i>	<i>Alamat MAC</i>
<i>Cisco Systems</i>	00 00 0C
<i>Cabletron Systems</i>	00 00 1D
<i>International Business Machine Corporation</i>	00 04 AC
<i>3Com Corporation</i>	00 20 AF
<i>GVC Corporation</i>	00 C0 A8
<i>Apple Computer</i>	08 00 07
<i>Hewlett-Packard Company</i>	08 00 09

Tabel 2. 3 : MAC Address Yang Umum Digunakan

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Server 03>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : server-02
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : Yes
    WINS Proxy Enabled. . . . . : No

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : VMware Virtual Ethernet Adapter for
                           VMnet8
    Physical Address . . . . . : 00-50-56-C0-00-08
    Dhcp Enabled. . . . . : No
    IP Address . . . . . : 192.168.37.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Gambar 2. 3: Tampilan Untuk Melihat MAC Address
Pada Command Prompt

2.3.9. Pengertian Topologi

Topologi (dari bahasa Yunani *topos*, "tempat", dan *logos*, "ilmu") merupakan cabang matematika yang bersangkutan dengan tata ruang yang tidak berubah dalam deformasi dwikontinu (yaitu ruang yang dapat ditekuk, dilipat, disusut, direntangkan, dan dipilin tetapi tidak diperkenankan untuk dipotong, dirobek, ditusuk atau dilekatkan). Ia muncul melalui pengembangan konsep dari geometri dan teori himpunan, seperti ruang, dimensi, bentuk, transformasi.

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan / keuntungan dan kekurangan / kerugian dari masing - masing topologi berdasarkan kateristiknya.

Topologi pada dasarnya adalah peta dari sebuah jaringan. Topologi jaringan terbagi lagi menjadi dua yaitu topologi secara fisik (physical topology) dan topologi secara logika (logical topology). Topologi secara fisik menjelaskan bagaimana susunan dari label, komputer dan lokasi



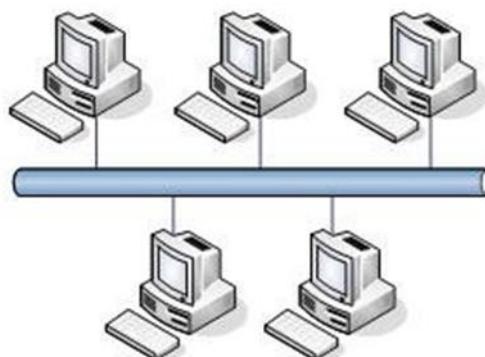
dari semua komponen jaringan. Sedangkan topologi secara logika menetapkan bagaimana informasi atau aliran data dalam jaringan. Arsitektur topologi merupakan bentuk koneksi fisik untuk menghubungkan setiap node pada sebuah jaringan. Pada sistem LAN terdapat tiga topologi utama yang paling sering digunakan, yaitu : Bus, Star, dan Ring. Topologi jaringan ini kemudian berkembang menjadi Topologi Tree dan Mesh yang merupakan kombinasi dari Star, Mesh, dan Bus. Berikut jenis-jenis topologi Topologi :

1. Topologi Bus
2. Topologi Ring (Cincin)
3. Topologi Star (Bintang)
4. Topologi Tree (Pohon)
5. Topologi Mesh (Tak Beraturan)

2.3.9.1. Topologi Bus

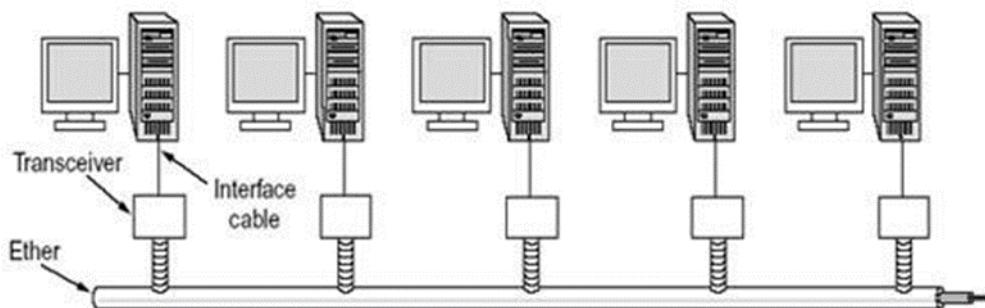
Topologi bus ini sering juga disebut sebagai topologi backbone, dimana ada sebuah kabel coaxial yang dibentang kemudian beberapa komputer dihubungkan pada kabel tersebut.

Secara sederhana pada topologi bus, satu kabel media transmisi dibentang dari ujung ke ujung, kemudian kedua ujung ditutup dengan “terminator” atau terminating-resistance (biasanya berupa tahanan listrik sekitar 60 ohm).



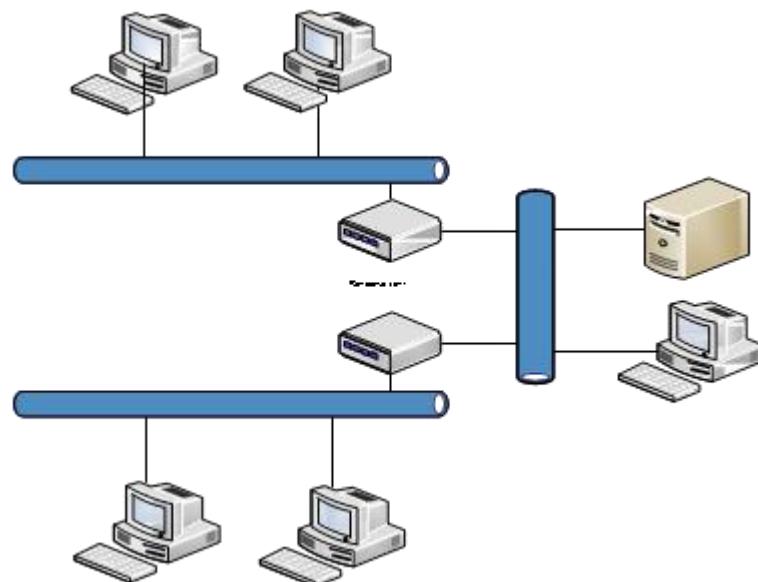
Gambar 2.4 Topologi Bus

1. Pada titik tertentu diadakan sambungan (tap) untuk setiap terminal.
2. Wujud dari tap ini bisa berupa kabel transceiver bila digunakan thick coax sebagai media transmisi.
3. Atau berupa BNC T-connector bila digunakan thin coax sebagai media transmisi.
4. Atau berupa konektor RJ-45 dan Hub bila digunakan kabel UTP.
5. Transmisi data dalam kabel bersifat full duplex, dan sifatnya broadcast, semua terminal bisa menerima transmisi data.



Gambar 2.5 Koneksi Kabel-Transceiver Pada Topologi Bus

6. Suatu protokol akan mengatur transmisi dan penerimaan data, yaitu Protokol Ethernet atau CSMA/CD.
7. Melihat bahwa pada setiap segmen (bentang) kabel ada batasnya maka diperlukan “Repeater” untuk menyambungkan segmen-segmen kabel.



Gambar 2.6 Perluasan Topologi Bus Menggunakan Repeater

Kelebihan Topologi Bus

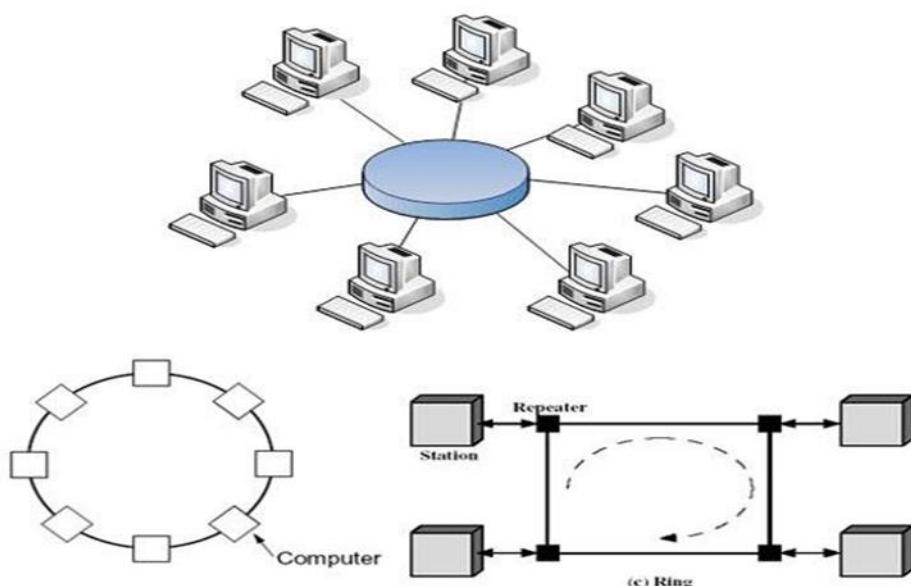
1. Instalasi relatif lebih murah
2. Kerusakan satu komputer client tidak akan mempengaruhi komunikasi antar client lainnya
3. Biaya relatif lebih murah

Kelemahan Topologi Bus

1. Jika kabel utama (bus) atau backbone putus maka komunikasi gagal
2. Bila kabel utama sangat panjang maka pencarian gangguan menjadi sulit. Kemungkinan akan terjadi tabrakan data (data collision) apabila banyak client yang mengirim pesan dan ini akan menurunkan kecepatan komunikasi.

2.3.9.2. Topologi Ring (Cincin)

Topologi ring biasa juga disebut sebagai topologi cincin karena bentuknya seperti cincin yang melingkar. Semua komputer dalam jaringan akan dihubungkan pada sebuah cincin. Cincin ini hampir sama fungsinya dengan concentrator pada topologi star yang menjadi pusat berkumpulnya ujung kabel dari setiap komputer yang terhubung. Secara lebih sederhana lagi topologi cincin merupakan untaian media transmisi dari satu terminal ke terminal lainnya hingga membentuk suatu lingkaran, dimana jalur transmisi hanya “satu arah”. Tiga fungsi yang diperlukan dalam topologi cincin : penyelipan data, penerimaan data, dan pemindahan data.



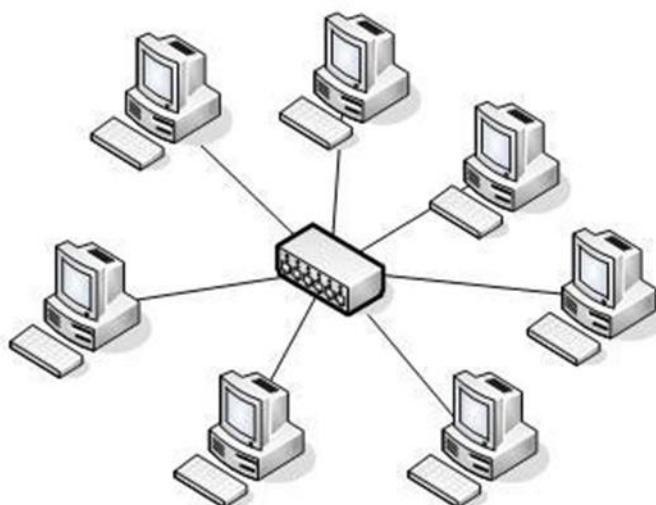
Gambar 2.7 Prinsip Koneksi Topologi Ring

1. Penyelipan data adalah proses dimana data dimasukkan kedalam saluran transmisi oleh terminal pengirim setelah diberi alamat dan bit-bit tambahan lainnya.
2. Penerimaan data adalah proses ketika terminal yang dituju telah mengambil data dari saluran, yaitu dengan cara membandingkan alamat yang ada pada paket data dengan alamat terminal itu sendiri. Apabila alamat tersebut sama maka data kiriman disalin.
3. Pemindahan data adalah proses dimana kiriman data diambil kembali oleh terminal pengirim karena tidak ada terminal yang menerimanya (mungkin akibat salah alamat). Jika data tidak diambil kembali maka data ini akan berputar-putar dalam saluran. Pada jaringan bus hal ini tidak akan terjadi karena kiriman akan diserap oleh “terminator”.
4. Pada hakikatnya setiap terminal dalam jaringan cincin adalah “repeater”, dan mampu melakukan ketiga fungsi dari topologi cincin.



5. Sistem yang mengatur bagaimana komunikasi data berlangsung pada jaringan cincin sering disebut token-ring.
6. Tiap komputer dapat diberi repeater (transceiver) yang berfungsi sebagai:
 - Listen State
Tiap bit dikirim dengan mengalami delay waktu
 - Transmit State
Bila bit berasal dari paket lebih besar dari ring maka repeater dapat mengembalikan ke pengirim. Bila terdapat beberapa paket dalam ring, repeater yang tengah memancarkan, menerima bit dari paket yang tidak dikirimnya harus menampung dan memancarkan kembali.
 - Bypass State
Berfungsi menghilangkan delay waktu dari stasiun yang tidak aktif.
 - a. Keuntungan :
 - Kegagalan koneksi akibat gangguan media dapat diatasi lewat jalur lain yang masih terhubung.
 - Penggunaan sambungan point to point membuat transmission error dapat diperkecil
 - b. Kerugian :
Data yang dikirim, bila melalui banyak komputer, transfer menjadi lambat.

2.3.9.3. Topologi Star (Bintang)



Gambar 2.8 Prinsip Koneksi Topologi Star

Disebut topologi star karena bentuknya seperti bintang, sebuah alat yang disebut concentrator bisa berupa hub atau switch menjadi pusat, dimana semua komputer dalam jaringan dihubungkan ke concentrator ini.



1. Pada topologi Bintang (Star) sebuah terminal pusat bertindak sebagai pengatur dan pengendali semua komunikasi yang terjadi. Terminal-terminal lainnya melalukan komunikasi melalui terminal pusat ini.
2. Terminal kontrol pusat bisa berupa sebuah komputer yang difungsikan sebagai pengendali tetapi bisa juga berupa "HUB" atau "MAU" (Multi Access Unit).
3. Terdapat dua alternatif untuk operasi simpul pusat.
 - Simpul pusat beroperasi secara "broadcast" yang menyalurkan data ke seluruh arah. Pada operasi ini walaupun secara fisik kelihatan sebagai bintang namun secara logik sebenarnya beroperasi seperti bus. Alternatif ini menggunakan HUB.
 - Simpul pusat beroperasi sebagai "switch", data kiriman diterima oleh simpul kemudian dikirim hanya ke terminal tujuan (bersifat point-to-point), akternatif ini menggunakan MAU sebagai pengendali.
4. Bila menggunakan HUB maka secara fisik sebenarnya jaringan berbentuk topologi Bintang namun secara logis bertopologi Bus. Bila menggunakan MAU maka baik fisik maupun logis bertopologi Bintang.

Kelebihan Topologi Bintang

1. Karena setiap komponen dihubungkan langsung ke simpul pusat maka pengelolaan menjadi mudah, kegagalan komunikasi mudah ditelusuri.
2. Kegagalan pada satu komponen/terminal tidak mempengaruhi komunikasi terminal lain.

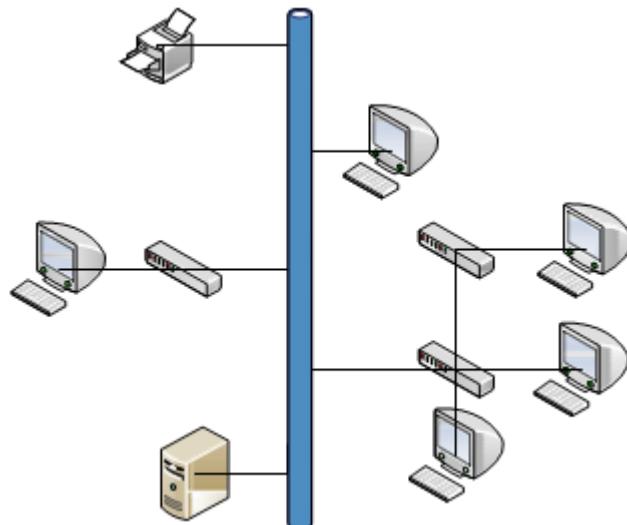
Kelemahan Topologi Bintang

1. Kegagalan pusat kontrol (simpul pusat) memutuskan semua komunikasi
2. Bila yang digunakan sebagai pusat kontrol adalah HUB maka kecepatan akan berkurang sesuai dengan penambahan komputer, semakin banyak semakin lambat.

2.3.9.4. Topologi Tree (Pohon)

Topologi pohon adalah pengembangan atau generalisasi topologi bus. Media transmisi merupakan satu kabel yang bercabang namun loop tidak tertutup.

Topologi pohon dimulai dari suatu titik yang disebut "headend". Dari headend beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung beberapa terminal dalam bentuk bus, atau dicabang lagi hingga menjadi rumit.

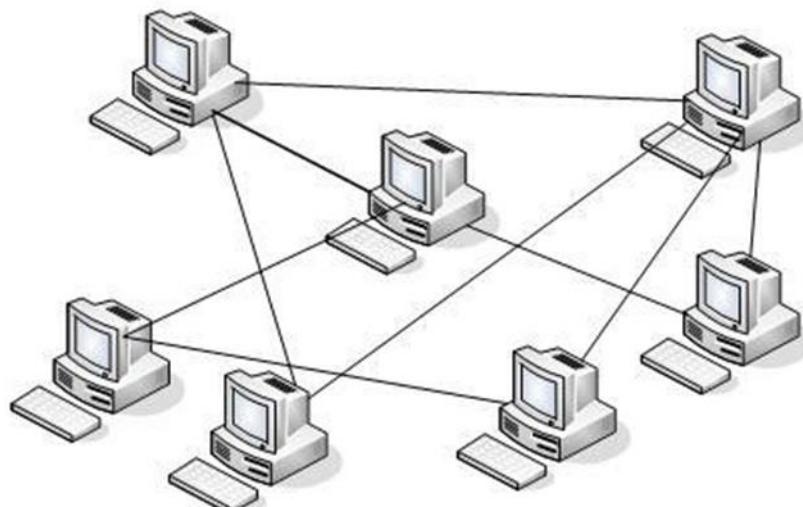


Gambar 2.9 Prinsip Koneksi Topologi Tree

Ada dua kesulitan pada topologi ini:

- Karena bercabang maka diperlukan cara untuk menunjukkan kemana data dikirim, atau kepada siapa transmisi data ditujukan.
- Perlu suatu mekanisme untuk mengatur transmisi dari terminal terminal dalam jaringan

2.3.9.5. Topologi Mesh (Tak beraturan)



Gambar 2.10 Prinsip Koneksi Topologi Mesh

1. Topologi Mesh adalah topologi yang tidak memiliki aturan dalam koneksi. Topologi ini biasanya timbul akibat tidak adanya perencanaan awal ketika membangun suatu jaringan.
2. Karena tidak teratur maka kegagalan komunikasi menjadi sulit dideteksi, dan ada kemungkinan boros dalam pemakaian media transmisi.



3. Topologi ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran yang harus disediakan untuk membentuk jaringan Mesh adalah jumlah sentral dikurangi 1.
4. Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang.
5. Disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.
6. Topologi ini merupakan teknologi khusus yang tidak dapat dibuat dengan pengkabelan, karena sistem yang rumit. Namun dengan teknologi wireless, topologi ini sangat memungkinkan untuk diwujudkan.

2.4 Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
3. Kabel
4. Multi Tester
5. Router
6. Switch
7. Hub
8. Aplikasi Packet Tracer
9. Software virtualisasi (VMware)

2.5 Praktikum

Percobaan - I - Pengalamatan IPv4

1. Buat Jaringan seperti gambar dibawah ini



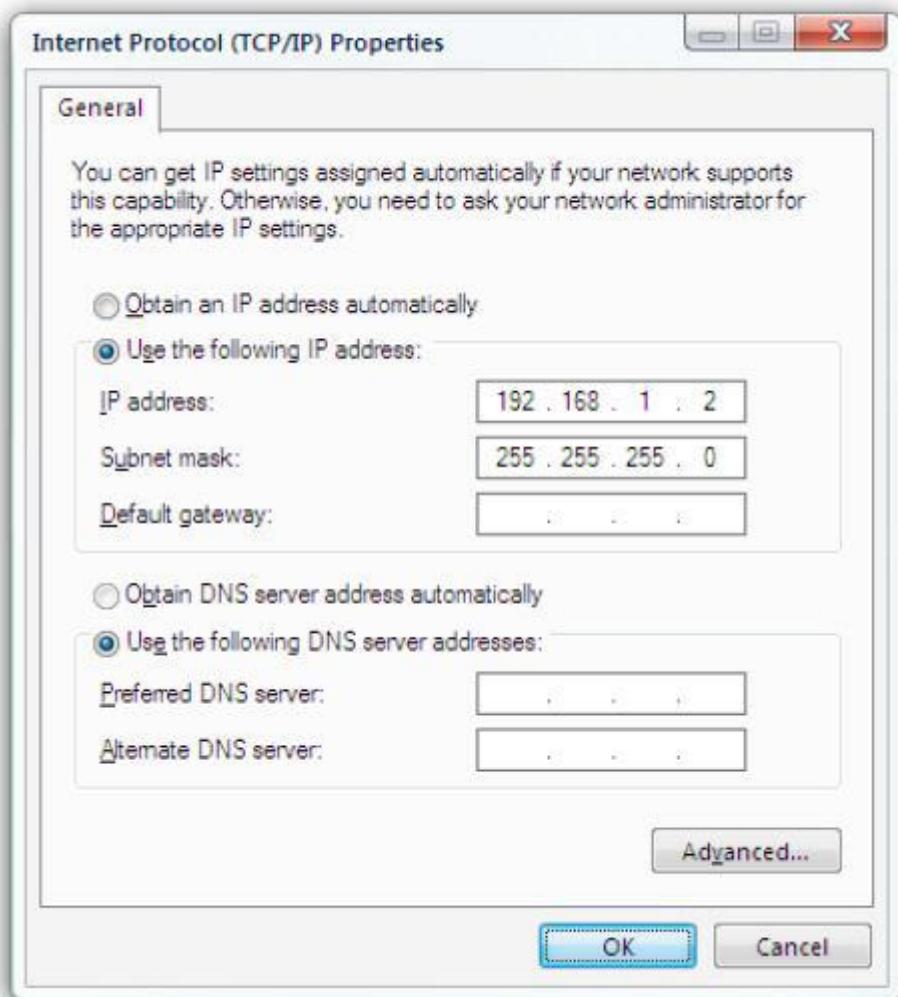
2. Hubungkan dua computer dengan kabel cross kemudian berikan alamat private dikelas C
3. Masukan IP di computer A dengan (misal IPnya adalah 192.168.1.2/24 dan Komputer B dengan IP 192.168.1.254/24)
 - Pilih Control Panel kemudian pilih Network Adapter dan pilih Local Area Connection.



- Klik 2 X bagian Local Area Connections kemudian pilih Internet Protocol (TCP/IP) kemudian Propertise



- Isikan Alamat di Komputer A dengan IP 192.168.1.2 dan untuk Komputer B dengan IP 192.168.1.254 dengan subnetmask 255.255.255.0



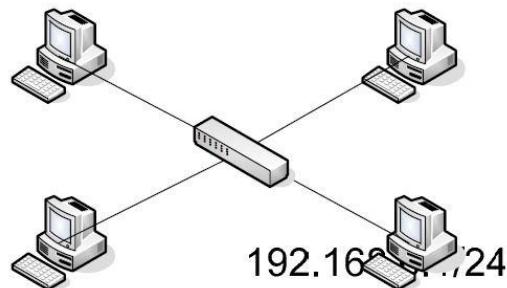
4. Pada komputer A klik menu Start kemudian ambil RUN ketikan CMD
5. Ping ke komputer B dengan cara sbb ping 192.168.1.254

Tuliskan hasil yang didapat ! _____



PERCOBAAN – 2 – Pengalamatan IPv4

1. Hubungkan dua komputer atau lebih dengan menggunakan switch atau hub kabel straight kemudian berikan alamat private dikelas C: (IP Addres 192.168.2.0/24)



2. Masukan IP address di setiap komputer (A,B,C dan D), komputer A 192.168.1.1/24, Komputer B192.168.1.10/24, Komputer C 192.168.1.20/24 dan komputer C 192.168.1.50/24
3. Dari komputer A ping ke komputer B , C dan D, hasil yang di dapat
4. Hasil Ping Ke Komputer B

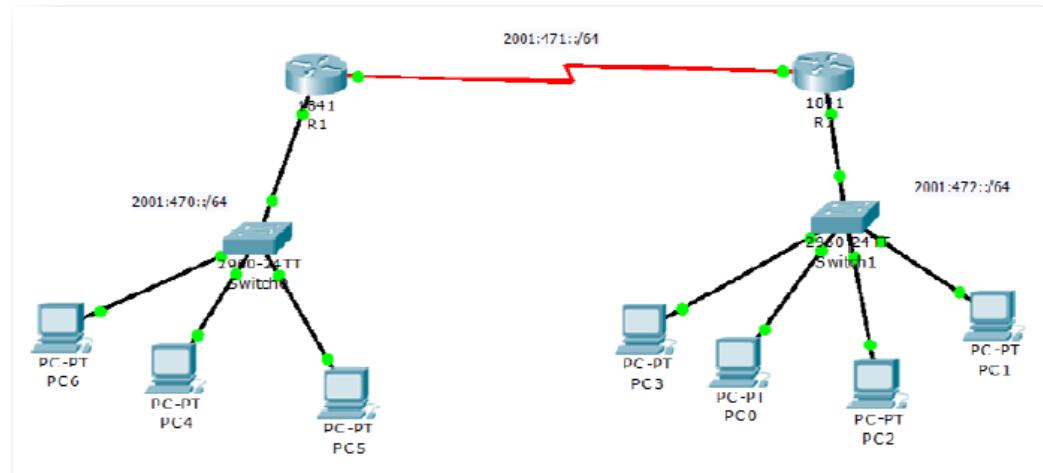
Hasil Ping Ke Komputer C

Hasil Ping Ke Komputer D

PERCOBAAN – 3 – Pengalamatan IPv6

Untuk membangun simulasi ini ada beberapa langkah yang harus dilakukan untuk mendisain beberapa subnet jaringan yang saling terhubung dalam satu jaringan melalui IPv6.

1. Desain jaringan seperti gambar berikut:



Gambar 1. Desain Jaringan dengan IPv6

Keterangan skenario gambar:

- Pada gambar sekenario menunjukkan 3 subnet jaringan yang berbeda yaitu:
2001:470::/64 ==> Jaringan 1
2001:471::/64 ==> Jaringan 2
2001:472::/64 ==> Jaringan 3
- Masing-masing host jaringan 1 terhubung ke switch melalui port Fast Ethernet dan kemudian melalui gateway port Fast Ethernet 0/0 pada router R1 dengan IPv6 2001:470::1/64 untuk terhubung ke jaringan 2 dan jaringan 3.
- Pada jaringan 3 dilakukan konfigurasi yang sama untuk dapat terhubung ke jaringan 2 dan jaringan 1, akan tetapi port gateway yang digunakan adalah Fast Ethernet 0/0 Router R2 dengan IPv6 2001:472::1/64.
- Masing-masing Router R1 dan R2 terhubung melalui kabel serial.
- Port serial 0/1/0 pada Router R1 ber-IPv6 2001:471::1/64 sedangkan pada Serial 0/1/0 Router R2 2001:471::2/64.
- Local link yang digunakan pad tiap Router adalah fe80::1/64.
- Pada masing masing PC client akan dilakukan konfigurasi IPv6 secara Auto Config sehingga tiap PC Client akan mendapat IP Local link dan Global Unicast secara otomatis. Selain itu juga akan disetting secara manual.



Konfigurasi pada Cisco Router

- a. Lakukan konfigurasi pada Router 1 dengan mengetikkan perintah berikut pada CLI:

```
R1> enable  
R1# configure terminal  
R1(config)#ipv6 unicast-routing  
R1(config)#interface fastethernet0/0  
R1(config-if)#ipv6 enable  
R1(config-if)#ipv6 address 2001:470::1/64  
R1(config-if)#ipv6 address fe80::1 link-local  
R1(config-if)#no shutdown  
R1(config-if)#exit
```

- b. Untuk melihat hasil konfigurasi :

```
R1#show ipv6 interface brief
```

Amati dan catat hasil perintah di atas.

- c. Kemudian lakukan pemberian IPv6 pada port serial 0/1/0 pada Router R1

```
R1(config)#interface serial0/1/0  
R1(config-if)#ipv6 enable  
R1(config-if)#ipv6 address 2001:471::1/64  
R1(config-if)#no shutdown  
R1(config-if)#exit
```

- d. Lakukan hal yang sama pada Router 2:

```
R2> enable  
R2#configure terminal R  
2(config)#ipv6 unicast-routing  
R2(config)#interface fastethernet0/0  
R2(config)#ipv6 enable  
R2(config-if)#ipv6 address 2001:472::1/64  
R2(config-if)#ipv6 address fe80::1 link-local  
R2(config-if)#no shutdown  
R2(config-if)#exit
```

- e. Untuk melihat hasil konfigurasi ketikan sebagai berikut:

```
R2# show ipv6 interface brief
```

Amati dan catat hasil perintah di atas.

- f. Kemudian lakukan pemberian IPv6 pada port serial 0/1/0 pada Router R2

```
R2(config)#interface serial0/1/0  
R2(config-if)#ipv6 enable  
R2(config-if)#ipv6 address 2001:471::2/64  
R2(config-if)#clock rate 64000  
R2(config-if)#no shutdown  
R2(config-if)#exit
```



- g. Untuk melakukan routing agar dapat terhubung dari satu jaringan ke jaringan lain maka akan dilakukan routing dinamis menggunakan Routing RIP.

Untuk melakukannya lakukan langkah sebagai berikut pad CLI:

- Pada Router 1:

R1> enable

R1#configure terminal

R1(config)#ipv6 router rip ciscorip => ciscorip adalah nama jaringannya

R1(config-rtr)#exit

R1(config)#interface fastethernet0/0

R1(config-if)#ipv6 rip ciscorip enable

R1(config-if)#exit

R1(config)#interface serial0/1/0

R1(config-if)#ipv6 rip ciscorip enable

R1(config-if)#exit

R1(config)#end

- h. Pada Router 2:

R2> enable

R2#configure terminal

R2(config)#ipv6 router rip ciscorip

R2(config-rtr)#exit

R2(config)#interface fastethernet0/0

R2(config-if)#ipv6 rip ciscorip enable

R2(config-if)#exit R2(config)#interface serial0/1/0

R2(config-if)#ipv6 rip ciscorip enable

R2(config-if)#exit

R2(config)#end

- i. Untuk menunjukkan table routing yang telah terbentuk secara otomatis, ketikkan sebagai berikut:

R2#show ipv6 route

Amati dan catat hasilnya pada masing-masing router.



j. Konfigurasi pada PC Client

Lakukan konfigurasi pada PC Client agar mendapat IPv6 secara otomatis

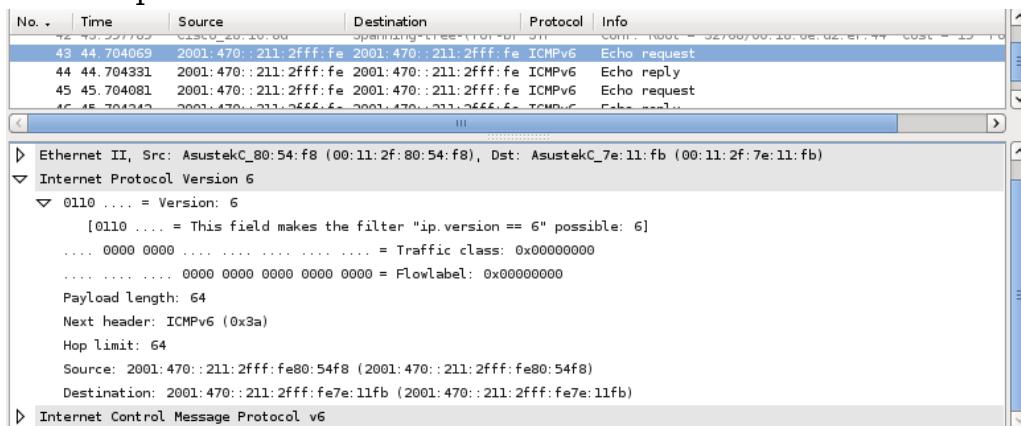
Ketikkan perintah berikut pada kedua PC Client

ifconfig

```
debian:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:11:2f:80:54:f8
          inet addr:192.168.50.89 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: 2001:472::211:2fff:fe80:54f8/64 Scope:Global
                   inet6 addr: fe80::211:2fff:fe80:54f8/64 Scope:Link
          RX packets:363 errors:0 dropped:0 overruns:0 frame:0
          TX packets:296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:447773 (437.2 KiB) TX bytes:32327 (31.5 KiB)
```

Amati dan catat hasilnya.

- Jalankan wireshark
- Lakukan tes ping dari Client pada subnet 1 ke client pada subnet 3.
- Amati dan catat hasil dari ping.
- Amati dan catat hasil wireshark, amati perbedaannya dengan format ipv4.



k. Lakukan setting secara manual pada PC Client.

Setting IPv6 dengan nomor 2001:470::2/64 pada jaringan 1

ip -6 address add 2001:470::2/64 dev eth0

* Dimana dengan menambahkan -6 artinya menggunakan ipv6, pada perangkat jaringan eth0 (dev eth0)

Cek ipv6 dan catat di laporan

ip -6 address show

Lakukan setting juga pada client pada jaringan 3 yaitu 2001:472::2/64

ip -6 address add 2001:472::2/64 dev eth0

Lakukan ping6 dari jaringan 1 ke jaringan 3

ping6 2001:472::2



Amati dan catat hasilnya dari hasil ping dan wireshark.

NB:

Untuk menghapus alamat IPv6 :

```
# ip -6 address del 2001:5c0:948c::10/64 dev eth0
```

LAPORAN RESMI

Berikan kesimpulan hasil praktikum yang anda lakukan.

2.6 Referensi

1. Rafiudin Rahmat, Panduan membangun jaringan Komputer untuk pemula, Jakarta: PT. Elex Media Competindo,2006.
2. Enterprise Jubilee, Membuat Jaringan Komputer Tanpa Bantuan Teknisi, Jakarta : PT. Elex Media Competindo,2008.
3. Yani Ahmad, Panduan Menjadi Teknisi Jaringan Komputer, Jakarta : PT Kawan Pustaka, 2008.
4. Sofana Iwan (2013). "CISCO CCNA & Jaringan Komputer,(Edisi Revisi)." Bandung: Informatika.
5. Wikipedia Ensiklopedia Bebas (22 Juni 2016) "Jaringan komputer" https://id.wikipedia.org/wiki/Jaringan_komputer diakses pada 31 Januari 2021

2.7 Tugas

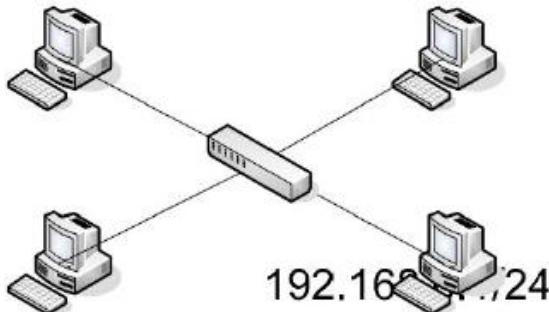
Bagian – 1



Host IP Address	172.30.1.33
Network Mask	255.255.0.0
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	
IP Computer A	
IP Computer B	



Bagian – 2



Host IP Address	172.30.1.33
Network Mask	255.255.255.0
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	
IP Computer A	
IP Computer B	
IP Computer C	
IP Computer D	

2.8 Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, MODUL I PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Bottom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



MODUL III

PENGANTAR SUBNETTING

3.1 Tujuan Praktikum

1. Untuk mengetahui cara kerja Subnetting
2. Untuk dapat merepresentasi pada Subnet Mask
3. Untuk mengetahui perhitungan Subnetting

3.2 Indikator Pencapaian

1. Mampu melakukan perhitungan Subnetting
2. Mampu melalukan perhitungan subnetting menggunakan metode desimal bertitik
3. Mampu melakukan Perhitungan Subnetting CIDR
4. Mampu melakukan Subnetting Kelas C, B, dan A
5. Mampu mengembangkan VLSM (Variable Length Subnet Mask)
6. Mampu melakukan perhitungan Subnetting VLSM

3.3 Materi

3.3.1. Pengertian subnetting

Subnetting adalah upaya / proses untuk memecah sebuah network dengan jumlah host yang cukup banyak, menjadi beberapa network dengan jumlah host yang lebih sedikit. Teknik subnetting membuat skala jaringan lebih luas dan tidak dibatas oleh kelas-kelas IP (IP Classes) A, B, dan C yang sudah diatur. Dengan subnetting, anda bisa membuat network dengan batasan host yang lebih realistik sesuai kebutuhan

3.3.2. Pengertian Subnet Mask

Subnet mask adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka biner 32 bit yang digunakan untuk membedakan network ID dengan host ID, menunjukkan letak suatu host, apakah berada di jaringan lokal atau jaringan luar.

RFC 950 mendefinisikan penggunaan sebuah subnet mask yang disebut juga sebagai sebuah address mask sebagai sebuah nilai 32-bit yang digunakan untuk membedakan network identifier dari host identifier di dalam sebuah alamat IP. Bit-bit subnet mask yang didefinisikan, adalah sebagai berikut:

- Semua bit yang ditujukan agar digunakan oleh network identifier diset ke nilai 1.
- Semua bit yang ditujukan agar digunakan oleh host identifier diset ke nilai 0.



3.3.3. Representasi Subnet Mask

Ada dua metode yang dapat digunakan untuk merepresentasikan subnet mask, yakni:

- Desimal bertitik
- Prefix length

Tabel 3. 1 : Format Notasi Desimal bertitik dan Prefix Length

Kelas Alamat	Subnet Mask (Biner)	Subnet Mask (Desimal)	Prefix Length
Kelas A	11111111.00000000.00000000.00000000	255.0.0.0	/8
Kelas B	11111111.11111111.00000000.00000000	255.255.0.0	/16
Kelas C	11111111.11111111.11111111.00000000	255.255.255.0	/24

3.3.4. Perhitungan Subnetting

Selain dengan melihat tabel-tabel diatas, untuk menghitung jumlah subnet atau pun jumlah host dapat menggunakan rumus sebagai berikut :

- a. Menentukan Jumlah Subnet

$$2^x - 2 \geq \text{Jumlah Subnet}$$

Dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask. Sedangkan untuk kelas B binari 1 pada 2 oktet terakhir, kelas A binari pada 3 oktet terakhir.

- b. Menentukan Jumlah Host Per Subnet

$$2^y - 2 \geq \text{Jumlah Host Per Subnet}$$

Dimana y adalah kebalikan dari x yaitu banyaknya binari 0 pada oktet terakhir subnet mask. Untuk kelas B pada 2 oktet terakhir dan kelas A pada 3 oktet terakhir.

- c. Menentukan Blok Subnet

$$\begin{aligned} &256 - \text{Nilai Oktet Terakhir} \\ &\text{Subnet Mask} \end{aligned}$$

Nilai oktet terakhir subnet mask adalah angka yang ada dibelakang subnet mask, misalnya 255.255.255.192, maka $256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.

Hasil dari pengurangan ditambahkan dengan bilangan itu sendiri sampai berjumlah sama dengan angka belakang subnet mask $64 + 64 = 128$, dan $128 + 64 = 192$. Jadi total subnetnya adalah 0,64,128,192.

- d. Menentukan Subnet, Host dan Broadcast Yang Valid

Pertama kali kita membuat sebuah table atau subnet mapnya kemudian dari table atau subnet map tersebut dapat kita ambil subnet yang valid berdasarkan perhitungan subnetting menggunakan rumus menentukan jumlah subnet. Begitu juga dengan range host yang valid berdasarkan perhitungan subnetting



menggunakan rumus menentukan jumlah host per subnet. Untuk alamat broadcast merupakan alamat ip address terakhir setelah alamat untuk range host sudah terpenuhi baru alamat broadcast diberikan. Dengan ketentuan alamat broadcast tidak boleh sama dengan alamat subnet blok berikutnya atau alamat host terakhir pada blok subnet yang sedang dikerjakan.

Contoh perhitungan subnetting menggunakan metode desimal bertitik
Diketahui sebuah network address 88.2.65.192 dengan subnet mask 255.192.0.0

- a. Menentukan jumlah subnet $2^x - 2 \geq$ Jumlah Subnet
Nilai tiga oktet terakhir dari subnet mask adalah 192.0.0, kemudian dikonversi kan ke biner maka didapatkan hasil 11000000.00000000.00000000, Jadi x adalah 2 (banyaknya binari 1 pada tiga oktet terakhir subnet mask), maka $2^2 - 2 \geq 2$ subnet
- b. Menentukan jumlah host per subnet $2^y - 2 \geq$ Jumlah Host Per Subnet
Jadi y adalah 22 (banyaknya binari 0 pada dua oktet terakhir subnet mask), maka $2^{22} - 2 \geq 4194302$ host per subnet
- c. Menentukan Blok Subnet
256 – Nilai Oktet Terakhir Subnet Mask
Nilai tiga octet terakhir dari subnet mask adalah 254, kemudian $256 - 192 = 64$, subnet berikutnya $64 + 64 = 128$ dan $128 + 64 = 192$. Jadi total subnetnya adalah 0, 64, 128, 192.
- d. Menentukan Subnet, Host dan Broadcast yang valid

Blok Subnet	Network	Range Host	Broadcast
1	88.0.0.0	88.0.0.1 – 88.63.255.254	88.63.255.255
2	88.64.0.0	88.64.0.1 – 88.127.255.254	88.127.255.255
3	88.128.0.0	88.128.0.1 – 88.191.255.254	88.191.255.255
4	88.192.0.0	88.192.0.1 – 88.255.255.254	88.255.255.255

Blok subnet 2 dan 3 merupakan subnet yang valid, berdasarkan rumus menentukan jumlah subnet, menghasilkan 2 subnet, mengapa diambil subnet ke 2 dan 3, dilihat lagi dari blok subnetnya berdasarkan perhitungan itu mulai di ambil dari hasil yang dikurangi dari 256 adalah 64 dan sampai dengan batas nilai octet terakhir dari subnet mask, jadi host & broadcast yang valid berada pada blok subnet 2 dan 3.



Contoh perhitungan subnetting menggunakan metode desimal bertitik
Diketahui sebuah network address 143.212.17.189 dengan subnet
mask 255.255.240.0

- a. Menentukan jumlah subnet

$$2x - 2 \geq \text{Jumlah Subnet}$$

Nilai dua oktet terakhir dari subnet mask adalah 240.0, kemudian dikonversi ke biner maka didapatkan hasil 11110000.00000000, Jadi x adalah 4 (banyaknya binari 1 pada dua oktet terakhir subnet mask), maka $2^4 - 2 \geq 14$ subnet

- b. Menentukan jumlah host per subnet

$$2y - 2 \geq \text{Jumlah Host Per Subnet}$$

Jadi y adalah 12 (banyaknya binari 0 pada dua oktet terakhir subnet mask), maka $2^{12} - 2 \geq 4094$ host per subnet

- c. Menentukan Blok Subnet

256 – Nilai Oktet Terakhir Subnet Mask

Nilai dua oktet terakhir dari subnet mask adalah 240, kemudian $256 - 240 = 16$, subnet berikutnya $16 + 16 = 32$, $32 + 16 = 48$, $48 + 16 = 64$, $64 + 16 = 80$, $80 + 16 = 96$, $96 + 16 = 112$, $112 + 16 = 128$, $128 + 16 = 144$, $144 + 16 = 160$, $160 + 16 = 176$, $176 + 16 = 192$, $192 + 16 = 208$, $208 + 16 = 224$ dan $224 + 16 = 240$. Jadi total, subnetnya adalah 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.

- c. Menentukan Subnet, Host dan Broadcast yang valid

Blok Subnet	Network	Range Host	Broadcast
1	143.212.0.0	143.212.0.1 – 143.212.15.254	143.212.15.255
2	143.212.16.0	143.212.16.1 – 143.212.31.254	143.212.31.255
3	143.212.32.0	143.212.32.1 – 143.212.47.254	143.212.47.255
4	143.212.48.0	143.212.48.1 – 143.212.63.254	143.212.63.255
5	143.212.64.0	143.212.64.1 – 143.212.79.254	143.212.79.255
6	143.212.80.0	143.212.80.1 – 143.212.95.254	143.212.95.255
7	143.212.96.0	143.212.96.1 – 143.212.111.254	143.212.111.255
8	143.212.112.0	143.212.112.1 – 143.212.127.254	143.212.127.255
9	143.212.128.0	143.212.128.1 – 143.212.143.254	143.212.143.255
10	143.212.144.0	143.212.144.1 – 143.212.159.254	143.212.159.255
11	143.212.160.0	143.212.160.1 – 143.212.175.254	143.212.175.255
12	143.212.176.0	143.212.176.1 – 143.212.191.254	143.212.191.255
13	143.212.192.0	143.212.192.1 – 143.212.207.254	143.212.207.255



14	143.212.208.0	143.212.208.1 – 143.212.223.254	143.212.223.255
15	143.212.224.0	143.212.224.1 – 143.212.239.254	143.212.239.255
16	143.212.240.0	143.212.240.1 – 143.212.255.254	143.212.225.255

Blok subnet 2 sampai dengan 15 merupakan subnet yang valid, berdasarkan rumus menentukan jumlah subnet, menghasilkan 14 subnet, mengapa diambil subnet ke 2 hingga 15, dilihat lagi dari blok subnetnya berdasarkan perhitungan itu mulai di ambil dari hasil yang dikurangi dari 256 adalah 16 dan sampai dengan batas nilai octet terakhir dari subnet mask, jadi host & broadcast yang valid berada pada blok subnet 2 hingga 15.

Contoh perhitungan subnetting menggunakan metode desimal bertitik Diketahui sebuah network address 192.168.2.122 255.255.255.224

- a. Menentukan jumlah subnet $2x - 2 \geq$ Jumlah Subnet
Nilai oktet terakhir dari subnet mask adalah 224, kemudian dikonversi kan ke biner maka didapatkan hasil 11100000, Jadi x adalah 3 (banyaknya binari 1 pada oktet terakhir subnet mask), maka $2^3 - 2 \geq 6$ subnet
- b. Menentukan jumlah host per subnet $2y - 2 \geq$ Jumlah Host Per Subnet
Jadi y adalah 5 (banyaknya binari 0 pada oktet terakhir subnet mask), maka $2^5 - 2 \geq 30$ host per subnet
- c. Menentukan Blok Subnet
 $256 - \text{Nilai Oktet Terakhir Subnet Mask}$
Nilai octet terakhir dari subnet mask adalah 224, kemudian $256 - 224 = 32$, subnet berikutnya $32 + 32 = 64$, $64 + 32 = 96$, $96 + 32 = 128$, $128 + 32 = 160$, $160 + 32 = 192$, dan $192 + 32 = 224$. Jadi total subnetnya adalah 0, 32, 64, 96, 128, 160, 192, 224
- d. Menentukan Subnet, Host dan Broadcast yang valid

Blok Subnet	Network	Range Host	Broadcast
1	192.168.2.0	192.168.2.1 – 192.168.2.30	192.168.2.31
2	192.168.2.32	192.168.2.33 – 192.168.2.62	192.168.2.63
3	192.168.2.64	192.168.2.65 – 192.168.2.94	192.168.2.95
4	192.168.2.96	192.168.2.97 – 192.168.2.126	192.168.2.127
5	192.168.2.128	192.168.2.129 – 192.168.2.158	192.168.2.159
6	192.168.2.160	192.168.2.161 – 192.168.2.190	192.168.2.191
7	192.168.2.192	192.168.2.193 – 192.168.2.222	192.168.2.223
8	192.168.2.224	192.168.2.225 – 192.168.2.254	192.168.2.255



Blok subnet 2 sampai dengan 7 merupakan subnet yang valid, berdasarkan rumus menentukan jumlah subnet, menghasilkan 6 subnet, mengapa diambil subnet ke 2 hingga 7, dilihat lagi dari blok subnetnya berdasarkan perhitungan itu mulai di ambil dari hasil yang dikurangi dari 256 adalah 32 dan sampai dengan batas nilai octet terakhir dari subnet mask, jadi host & broadcast yang valid berada pada blok subnet 2 hingga 7.

3.3.5. CIDR (Classless Inter-Domain Routing)

Classless Inter-Domain Routing (disingkat menjadi CIDR) yang diperkenalkan pertama kali tahun 1992 oleh IEFT adalah sebuah cara alternatif untuk mengklasifikasikan alamat- alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai supernetting. CIDR merupakan mekanisme routing yang lebih efisien dibandingkan dengan cara yang asli, yakni dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C. Metode ini menggunakan notasi prefix dengan panjang notasi tertentu sebagai network prefix, panjang notasi prefix ini menentukan jumlah bit sebelah kiri yang digunakan sebagai Network ID, metode CIDR dengan notasi prefix dapat diterapkan pada semua kelas IP Address sehingga hal ini memudahkan dan lebih efektif. Menggunakan metode CIDR kita dapat melakukan pembagian IP address yang tidak berkelas sesukanya tergantung dari kebutuhan pemakai.

3.3.5.1. Perhitungan Subnetting CIDR

- Menentukan Jumlah Subnet

$$2^N \geq \text{JumlahSubnet}$$

Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask. Sedangkan untuk kelas B binari 1 pada 2 oktet terakhir, kelas A binari pada 3 oktet terakhir.

- Menentukan Jumlah Host Per Subnet

$$2^n - 2 \geq \text{Jumlah Host Per Subnet}$$

Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask. Untuk kelas B pada 2 oktet terakhir dan kelas A pada 3 oktet terakhir.

- Menentukan Blok Subnet

$$256 - \text{Nilai Oktet Terakhir Subnet Mask}$$



Nilai oktet terakhir subnet mask adalah angka yang ada dibelakang subnet mask, misalnya 255.255.255.192, maka $256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.

Hasil dari pengurangan ditambahkan dengan bilangan itu sendiri sampai berjumlah sama dengan angka belakang subnet mask $64 + 64 = 128$, dan $128 + 64 = 192$. Jadi total subnetnya adalah 0,64,128,192.

d. Menentukan Alamat Broadcast

Yaitu mengambil alamat IP address yang terletak paling akhir. Dengan ketentuan alamat broadcast tidak boleh sama dengan alamat subnet blok berikutnya atau alamat host terakhir pada blok subnet yang sedang dikerjakan. Bit-bit dari Network ID maupun Host ID tidak boleh.

Semuanya berupa angka binary 0 semua atau 1 semua, jika hal tersebut terjadi maka disebut flooded broadcast sebagai contoh 255.255.255.255.

3.3.5.2. Subnetting Pada Kelas C

Penulisan IP Address pada umumnya adalah 192.168.1.2. namun adakalanya ditulis dengan 192.168.1.2/24, maksud dari penulisan IP Address tersebut adalah bahwa IP Address 192.168.1.2 dengan subnet mask 255.255.255.0 . Mengapa demikian, karena /24 diambil dari perhitungan bahwa 24 bit subnet mask diselubungkan dengan binary 1, atau dengan kata lain subnet masknya adalah 11111111.11111111.11111111.00000000 (255.255.255.0)

Tabel 3.2 CIDR Pada Kelas C

Subnet Mask	Nilai CIDR
255.255.225.128	/25
255.255.225.192	/26
255.255.225.224	/27
255.255.225.240	/28
255.255.225.248	/29
255.255.225.252	/30

Contoh soal jika diketahui network address 192.168.1.3/26?

Analisa 192.168.1.3 berarti kelas C dengan subnet mask /26 maka 1111111.11111111.11111111.11000000 (255.255.255.192)

Jumlah Subnet

$$2N \geq \text{Jumlah Subnet} \rightarrow 2^2 \geq 4 \text{ subnet}$$



Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask

Jumlah Host per subnet

$$2n - 2 \geq \text{Jumlah Host Per Subnet} \rightarrow 26 - 2 \geq 62 \text{ host}$$

Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask.

Jumlah Blok Subnet

$$256 - 192 \text{ (nilai terakhir oktet subnet mask)} = 64 \text{ subnet.}$$

Berikutnya adalah $64+64=128$, dan $128+64=192$, jadi total subnetnya $0,64,128,192$.

Subnet Map & Alamat Broadcast

Blok Subnet	Subnet	Range Host	Broadcast
1	192.168.1.0	192.168.1.1 – 192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65 – 192.168.1.126	192.168.1.127
3	192.168.1.128	192.168.1.129 – 192.168.1.190	192.168.1.191
4	192.168.1.192	192.168.1.193 – 192.168.1.254	192.168.1.255

3.3.5.3. Subnetting Pada Kelas B

Tabel 3.3 CIDR Pada Kelas B

Subnet Mask	Nilai CIDR
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23

Tabel 3.4 CIDR Pada Kelas B

Subnet Mask	Nilai CIDR
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28



255.255.255.248	/29
255.255.255.252	/30

Contoh soal jika diketahui network address 172.16.1.8/18?

Analisa 172.16.1.8 berarti kelas B dengan subnet mask /18 maka
11111111.11111111.1100000.00000000 (255.255.192.0)

Jumlah Subnet

$2N \geq$ Jumlah Subnet $\rightarrow 2^2 \geq 4$ subnet

Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask

Jumlah Host per subnet

$2n - 2 \geq$ Jumlah Host Per Subnet $\rightarrow 2^{14} - 2 \geq 16382$ host

Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask.

Jumlah Blok Subnet

256 – 192 (nilai terakhir oktet subnet mask) = 64 subnet.

Berikutnya adalah $64+64=128$, dan $128+64=192$, jadi total subnetnya 0,64,128,192.

Subnet Map & Alamat Broadcast

Blok Subnet	Subnet	Range Host	Broadcast
1	172.16.0.0	172.16.0.1 – 172.16.63.254	172.16.63.255
2	172.16.64.0	172.16.64.1 – 172.16.127.254	172.16.127.255
3	172.16.128.0	172.16.128.1 – 172.16.191.254	172.16.191.255
4	172.16.192.0	172.16.192.1 – 172.16.255.254	172.16.255.255

3.3.5.4. Subnetting Pada Kelas A

Tabel 3.5 CIDR Pada Kelas A

Subnet Mask	Nilai CIDR
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14



255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19



Tabel 3.6 CIDR Pada Kelas A

Subnet Mask	Nilai CIDR
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Contoh soal jika diketahui network address 10.17.0.0 /10?

Analisa 10.17.0.0 berarti kelas A dengan subnet mask /10 maka
11111111.1100000.00000000.00000000 (255.192.0.0)

Jumlah Subnet

$2^N \geq$ Jumlah Subnet $\rightarrow 2^2 \geq 4$ subnet

Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask

Jumlah Host per subnet

$2^n - 2 \geq$ Jumlah Host Per Subnet $\rightarrow 2^{22} - 2 \geq 4194304$ host

Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask.

Jumlah Blok Subnet

$256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.

Berikutnya adalah $64+64=128$, dan $128+64=192$, jadi total subnetnya 0,64,128,192.

Subnet Map & Alamat Broadcast

Blok Subnet	Subnet	Range Host	Broadcast
1	10.0.0.0	10.0.0.1 – 10.63.255.254	10.63.255.255
2	10.64.0.0	10.64.0.1 – 10.127.255.254	10.127.255.255



ITB AHMAD DAHLAN
Socio Technopreneur University

3	10.128.0.0	10.128.0.1 – 10.191.255.254	10.191.255.255
4	10.192.0.0	10.192.0.1 – 10.255.255.254	10.255.255.255



3.3.6. VLSM (Variable Length Subnet Mask)

VLSM adalah pengembangan mekanisme subnetting, dimana dalam vlsm dilakukan peningkatan dari kelemahan subnetting klasik, yang mana dalam clasik subnetting, subnet zeroes, dan subnet ones tidak bisa digunakan. selain itu, dalam subnet classic, lokasi nomor IP tidak efisien. VLSM juga dapat diartikan sebagai teknologi kunci pada jaringan skala besar. Mastering konsep VLSM tidak mudah, namun VLSM adalah sangat penting dan bermanfaat untuk merancang jaringan.

Metode VLSM hampir serupa dengan CIDR hanya blok subnet hasil dari CIDR dapat kita bagi lagi menjadi sejumlah Blok subnet dan blok IP address yang lebih banyak dan lebih kecil lagi.

Dalam penerapan IP Address menggunakan metode VLSM agar tetap dapat berkomunikasi kedalam jaringan internet sebaiknya pengelolaan networknya dapat memenuhi persyaratan :

1. Routing protocol yang digunakan harus mampu membawa informasi mengenai notasi prefix untuk setiap rute broadcastnya (routing protocol :RIP, IGRP, EIGRP, OSPF dan lainnya, bahan bacaan lanjut protocol routing :CNAP 1-2),
2. Semua perangkat router yang digunakan dalam jaringan harus mendukung metode VLSM yang menggunakan algoritma penerus paket informasi.

Manfaat dari VLSM adalah:

1. Efisien menggunakan alamat IP, alamat IP yang dialokasikan sesuai dengan kebutuhan ruang host setiap subnet.
2. VLSM mendukung hierarkis menangani desain sehingga dapat secara efektif
3. mendukung rute agregasi, juga disebut route summarization.

Yang terakhir dapat berhasil mengurangi jumlah rute di routingtable oleh berbagai jaringan subnets dalam satu ringkasan alamat. Misalnya subnets 192.168.10.0/24, 192.168.11.0/24 dan 192.168.12.0/24 semua akan dapat diringkas menjadi 192.168.8.0/21.

3.3.6.1. Perhitungan Subnetting VLSM

Pada pembahasan sebelumnya, suatu network ID hanya memiliki satu subnet mask. VLSM menggunakan metode yang berbeda dengan memberikan suatu network address lebih dari satu subnet mask. Network address yang menggunakan lebih dari satu subnet mask disebut Variable Length Subnet Mask (VLSM). Untuk jelasnya perhatikan contoh berikut ini.

- Diberikan Class C network 204.24.93.0/27, mempunyai subnet dengan kebutuhan berdasarkan jumlah host: netA=14 host, netB=28 host, netC=2 host, netD=7 host, netE=28 host.



- Analisa 204.24.93.0 berarti kelas C dengan subnet mask /27 maka $11111111.11111111.11111111.11100000$ (255.255.255.224)
Secara keseluruhan terlihat untuk melakukan hal tersebut di butuhkan 5 bit host $\rightarrow 2n - 2 \geq$ Jumlah Host Per Subnet ($25 - \geq 30$ host) sehingga ;
 $netA = 14$ host : $204.24.93.0/27 \rightarrow$ ada 30 host, tidak terpakai 16 host
 $netB = 28$ host : $204.24.93.32/27 \rightarrow$ ada 30 host, tidak terpakai 2 host
 $netC = 2$ host : $204.24.93.64/27 \rightarrow$ ada 30 host, tidak terpakai 28 host
 $netD = 7$ host : $204.24.93.96/27 \rightarrow$ ada 30 host, tidak terpakai 23 host
 $netE = 28$ host : $204.24.93.128/27 \rightarrow$ ada 30 host, tidak terpakai 2 host
- Buat Urutan Berdasarkan Penggunaan Jumlah Host Terbanyak
 $netB = 28$ host
 $netE = 28$ host
 $netA = 14$ host
 $netD = 7$ host
 $netC = 2$ host
- Menentukan Range Host Berdasarkan Kebutuhan Host
 $netB = 28$ host : $2n - 2 \geq 28$ host $\rightarrow 25 - 2 \geq 30$ host $\rightarrow 32 \geq 28$ host
 $netE = 28$ host : $2n - 2 \geq 28$ host $\rightarrow 25 - 2 \geq 30$ host $\rightarrow 32 \geq 28$ host
 $netA = 14$ host : $2n - 2 \geq 14$ host $\rightarrow 24 - 2 \geq 14$ host $\rightarrow 14 \geq 14$ host
 $netD = 7$ host : $2n - 2 \geq 7$ host $\rightarrow 24 - 2 \geq 14$ host $\rightarrow 14 \geq 7$ host
 $netC = 2$ host : $2n - 2 \geq 2$ host $\rightarrow 22 - 2 \geq 2$ host $\rightarrow 2 \geq 2$ host
- Menentukan Bit Net
 $netB = 28$ host : $32 - n \rightarrow 32 - 5 = /27$
 $netE = 28$ host : $32 - n \rightarrow 32 - 5 = /27$
 $netA = 14$ host : $32 - n \rightarrow 32 - 4 = /28$
 $netD = 7$ host : $32 - n \rightarrow 32 - 4 = /28$
 $netC = 2$ host : $32 - n \rightarrow 32 - 2 = /30$
- Menentukan Blok Subnet
 $netB = 28$ host : $256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$
 $netE = 28$ host : $256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$
 $netA = 14$ host : $256 - \text{Bit Net} \rightarrow 256 - (/28) \rightarrow 256 - 240 = 16$
 $netD = 7$ host : $256 - \text{Bit Net} \rightarrow 256 - (/28) \rightarrow 256 - 240 = 16$
 $netC = 2$ host : $256 - \text{Bit Net} \rightarrow 256 - (/30) \rightarrow 256 - 252 = 4$
Sehingga Blok Subnetnya Menjadi
 $netB = 28$ host : $204.24.93.0/27 \rightarrow$ ada 30 host, tidak terpakai 2 host
 $netE = 28$ host : $204.24.93.32/27 \rightarrow$ ada 30 host, tidak terpakai 2 host
 $netA = 14$ host : $204.24.93.64/28 \rightarrow$ ada 14 host, tidak terpakai 0 host
 $netD = 7$ host : $204.24.93.80/28 \rightarrow$ ada 14 host, tidak terpakai 7 host
 $netC = 2$ host : $204.24.93.96/30 \rightarrow$ ada 2 host, tidak terpakai 0 host



- Subnet Map

Subnet Name	Subnet	Range Host	Broadcast
netB	204.24.93.0	204.24.93.1 - 204.24.93.30	204.24.93.31
netE	204.24.93.32	204.24.93.33 - 204.24.93.62	204.24.93.63
net A	204.24.93.64	204.24.93.65 - 204.24.93.78	204.24.93.79
netD	204.24.93.80	204.24.93.81 - 204.24.93.94	204.24.93.95
netC	204.24.93.96	204.24.93.97 - 204.24.93.98	204.24.93.99

- Diberikan Class B network 185.14.0.2/19, mempunyai subnet dengan kebutuhan berdasarkan jumlah host:
netA=30 host, netB=14 host, netC=62 host, netD=25 host, netE=32 host.
- Analisa 185.14.0.2 berarti kelas C dengan subnet mask /19 maka 11111111.11111111.11100000.00000000 (255.255.224.0)

Secara keseluruhan terlihat untuk melakukan hal tersebut dibutuhkan 13 bit host

→ $2n - 2 \geq$ Jumlah Host Per Subnet ($2^{13} - 2 \geq 8190$ host) sehingga

netA = 30 host : 185.14.0.0/19 → ada 8190 host, tidak terpakai 8160 host

netB = 14 host : 185.14.32.0/19 → ada 8190 host, tidak terpakai 8176 host

netC = 62 host : 185.14.64.0/19 → ada 8190 host, tidak terpakai 8128 host

netD = 25 host : 185.14.96.0/19 → ada 8190 host, tidak terpakai 8165 host

netE = 32 host : 185.14.128.0/19 → ada 8190 host, tidak terpakai 8158 host

- Buat Urutan Berdasarkan Penggunaan Jumlah Host Terbanyak
netC = 62 host
netE = 32 host
netA = 30 host
netD = 25 host
netB = 14 host
- Menentukan Range Host Berdasarkan Kebutuhan Host
netC = 62 host : $2n - 2 \geq 62$ host → $2^{13} - 2 \geq 62$ host → $62 \geq 62$ host
netE = 32 host : $2n - 2 \geq 32$ host → $2^{13} - 2 \geq 32$ host → $62 \geq 32$ host
netA = 30 host : $2n - 2 \geq 30$ host → $2^{13} - 2 \geq 30$ host → $30 \geq 30$ host
netD = 25 host : $2n - 2 \geq 25$ host → $2^{13} - 2 \geq 25$ host → $30 \geq 25$ host
netB = 14 host : $2n - 2 \geq 14$ host → $2^{13} - 2 \geq 14$ host → $14 \geq 14$ host
- Menentukan Bit Net
netC = 62 host : $32 - n \rightarrow 32 - 6 = /26$
netE = 32 host : $32 - n \rightarrow 32 - 6 = /26$
netA = 30 host : $32 - n \rightarrow 32 - 5 = /27$
netD = 25 host : $32 - n \rightarrow 32 - 5 = /27$
netB = 14 host : $32 - n \rightarrow 32 - 4 = /28$



- Menentukan Blok Subnet

$$\text{netC} = 62 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$$

$$\text{netE} = 32 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$$

$$\text{netA} = 30 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$$

$$\text{netD} = 25 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$$

$$\text{netB} = 14 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/28) \rightarrow 256 - 240 = 16$$

Sehingga Blok Subnetnya Menjadi

$$\text{netC} = 62 \text{ host : } 185.14.0.0/26 \rightarrow \text{ada 62 host, tidak terpakai 0 host}$$

$$\text{netE} = 32 \text{ host : } 185.14.0.64/26 \rightarrow \text{ada 62 host, tidak terpakai 30 host}$$

$$\text{netA} = 30 \text{ host : } 185.14.0.128/27 \rightarrow \text{ada 30 host, tidak terpakai 0 host}$$

$$\text{netD} = 25 \text{ host : } 185.14.0.160/27 \rightarrow \text{ada 30 host, tidak terpakai 5 host}$$

$$\text{netB} = 14 \text{ host : } 185.14.0.192/28 \rightarrow \text{ada 14 host, tidak terpakai 0 host}$$

Subnet Map

Subnet Name	Subnet	Range Host	Broadcast
netC	185.14.0.0	185.14.0.1 – 185.14.0.62	185.14.0.63
netE	185.14.0.64	185.14.0.65 – 185.14.0.126	185.14.0.127
net A	185.14.0.128	185.14.0.129 – 185.14.0.158	185.14.0.159
netD	185.14.0.160	185.14.0.161 – 185.14.0.190	185.14.0.191
netB	185.14.0.192	185.14.0.193 – 185.14.0.206	185.14.0.207

- Diberikan Class A network 20.30.10.5/14, mempunyai subnet dengan kebutuhan berdasarkan jumlah host: netA=10 host, netB=18 host, netC=54 host, netD=34 host, netE=2 host.
Analisa 20.30.10.5 berarti kelas A dengan subnet mask /14 maka 11111111.11111100.00000000.00000000 (255.255.255.252)

Secara keseluruhan terlihat untuk melakukan hal tersebut dibutuhkan 18 bit host

$$\rightarrow 2n - 2 \geq \text{Jumlah Host Per Subnet} (2^{18} - \geq 262142 \text{ host}) \text{ sehingga}$$

$$\text{netA} = 10 \text{ host : } 20.0.0.0/14 \rightarrow \text{ada 262142 host, tidak terpakai 262132 host}$$

$$\text{netB} = 18 \text{ host : } 20.4.0.0/14 \rightarrow \text{ada 262142 host, tidak terpakai 262124 host}$$

$$\text{netC} = 54 \text{ host : } 20.8.0.0/14 \rightarrow \text{ada 262142 host, tidak terpakai 262088 host}$$

$$\text{netD} = 34 \text{ host : } 20.12.0.0/14 \rightarrow \text{ada 262142 host, tidak terpakai 262108 host}$$

$$\text{netE} = 2 \text{ host : } 20.16.0.0/14 \rightarrow \text{ada 262142 host, tidak terpakai 262140 host}$$

- Buat Urutan Berdasarkan Penggunaan Jumlah Host Terbanyak
 $\text{netC} = 54 \text{ host}$
 $\text{netD} = 34 \text{ host}$
 $\text{netB} = 18 \text{ host}$
 $\text{netA} = 10 \text{ host}$
 $\text{netE} = 2 \text{ host}$



- Menentukan Range Host Berdasarkan Kebutuhan Host

netC = 54 host : $2n - 2 \geq 62$ host $\rightarrow 26 - 2 \geq 62$ host $\rightarrow 62 \geq 54$ host

netD = 34 host : $2n - 2 \geq 62$ host $\rightarrow 26 - 2 \geq 62$ host $\rightarrow 62 \geq 34$ host

netB = 18 host : $2n - 2 \geq 30$ host $\rightarrow 25 - 2 \geq 30$ host $\rightarrow 30 \geq 18$ host

netA = 10 host : $2n - 2 \geq 14$ host $\rightarrow 24 - 2 \geq 14$ host $\rightarrow 14 \geq 10$ host

netE = 2 host : $2n - 2 \geq 2$ host $\rightarrow 22 - 2 \geq 2$ host $\rightarrow 2 \geq 2$ host

- Menentukan Bit Net

netC = 54 host : $32 - n \rightarrow 32 - 6 = /26$

netD = 34 host : $32 - n \rightarrow 32 - 6 = /26$

netB = 18 host : $32 - n \rightarrow 32 - 5 = /27$

netA = 10 host : $32 - n \rightarrow 32 - 4 = /28$

netE = 2 host : $32 - n \rightarrow 32 - 2 = /30$

- Menentukan Blok Subnet

netC = 54 host : $256 - \text{Bit Net} \rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$

netE = 34 host : $256 - \text{Bit Net} \rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$

netA = 18 host : $256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$

netD = 10 host : $256 - \text{Bit Net} \rightarrow 256 - (/28) \rightarrow 256 - 224 = 16$

netB = 2 host : $256 - \text{Bit Net} \rightarrow 256 - (/30) \rightarrow 256 - 240 = 8$

Sehingga Blok Subnetnya Menjadi

netC = 54 host : $20.0.0.0 /26 \rightarrow$ ada 62 host, tidak terpakai 0 host

netE = 34 host : $20.0.0.64 /26 \rightarrow$ ada 62 host, tidak terpakai 30 host

netA = 18 host : $20.0.0.128 /27 \rightarrow$ ada 30 host, tidak terpakai 12 host

netD = 10 host : $20.0.0.160 /28 \rightarrow$ ada 14 host, tidak terpakai 4 host

netB = 2 host : $20.0.0.176 /30 \rightarrow$ ada 2 host, tidak terpakai 0 host

Subnet Map

Subnet Name	Subnet	Range Host	Broadcast
netC	20.0.0.0	20.0.0.1 - 20.0.0.62	20.0.0.63
netE	20.0.0.64	20.0.0.65 - 20.0.0.126	20.0.0.127
net A	20.0.0.128	20.0.0.129 - 20.0.0.158	20.0.0.159
netD	20.0.0.160	20.0.0.161 - 20.0.0.174	20.0.0.175
netB	20.0.0.176	20.0.0.177 - 20.0.0.178	20.0.0.179

Terlihat adanya ip address yang tidak terpakai dalam jumlah yang cukup besar. Hal ini mungkin tidak akan menjadi masalah pada ip private akan tetapi jika ini di alokasikan pada ip public(seperti contoh ini) maka terjadi pemborosan dalam pengalokasian ip public tersebut. Untuk mengatasi hal ini (efisiensi) dapat digunakan metode VLSM.

Jika kita perhatikan, CIDR dan metode VLSM mirip satu sama lain, yaitu blok network address dapat dibagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil. Perbedaannya adalah CIDR merupakan sebuah konsep untuk pembagian blok IP Public

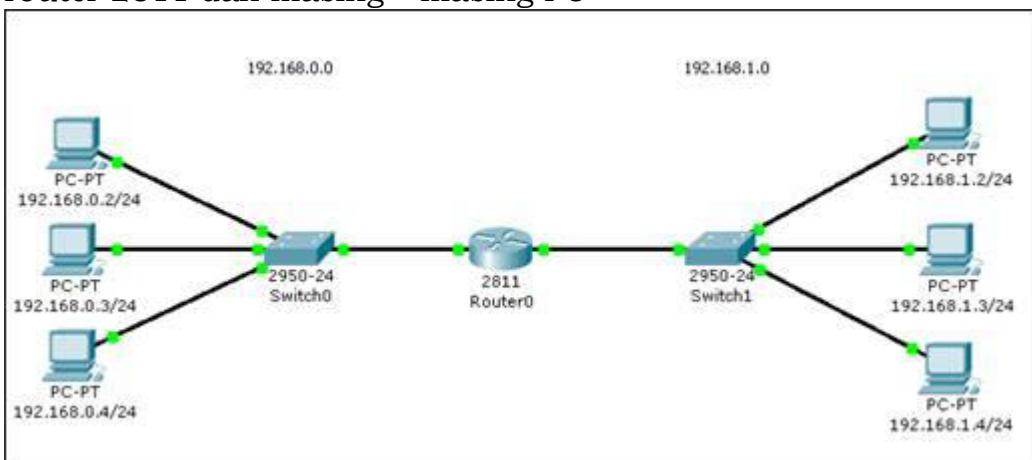
yang telah didistribusikan dari IANA, sedangkan VLSM merupakan implementasi pengalokasian blok IP yang dilakukan oleh pemilik network (network administrator) dari blok IP yang telah diberikan padanya (sifatnya lokal dan tidak dikenal di internet).

3.4 Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
3. Aplikasi Packet Tracer
4. Software virtualisasi (VMware)

3.5 Praktikum

Rancanglah skema jaringan di bawah ini, berikut dengan konfigurasi router 2811 dan masing – masing PC



Langkah kerja:

1. Siapkan 1 router 2811, 2 switch 2950-24, 6 PC-PT kemudian susun seperti gambar .
2. Hubungkan device seperti pada gambar 3 dengan menggunakan automatic connection.
3. Kelas IPv4 yang akan digunakan adalah kelas C dengan subnetmask ‘255.255.255.0’. Kita akan menghubungkan 2 network yang berbeda dengan menggunakan router. Network yang kita gunakan adalah ‘192.168.0.0/24’ dan ‘192.168.1.0/24’. Sekedar informasi, ‘/24’ setelah IP menandakan bit masking-nya adalah 24-bit (11111111.11111111.11111111.00000000 atau 255.255.255.0).
4. Konfigurasi IP masing-masing PC pada masing-masing jaringan. Gunakan default gateway ‘192.168.0.1’ dan ‘192.168.1.1’ pada masing-masing PC dengan network yang tepat. Gunakan subnetmask ‘255.255.255.0’.
5. Konfigurasi IP masing-masing interface router sesuai dengan default gateway dari network yang terhubung pada masing-masing interface router.



6. Lakukan perintah ‘ping’ antar PC dan pastikan semua PC saling terhubung dengan baik. Jika terhubung dengan baik, maka konfigurasi jaringan sudah benar.
7. Sekarang kita akan menguji penggunaan address pada host dimana kelompok bit terakhir bernilai ‘0’ (Network ID) dan ‘255’ (Broadcast). Pilih salah satu PC misalnya PC yang IP Address-nya ‘192.168.0.2/24’. Coba ubah IP Address-nya menjadi ‘192.168.0.0’ atau ‘192.168.0.255’
8. Amati kejadian di simulator, ketika anda memasuki langkah nomor 7, akan terdapat pesan error, apa yang menyebabkannya?

3.6 Referensi

1. Graziani, Rick and Johnson, Allan, Routing Protocols and Concepts, CISCO Press, 2007.
2. Lewis, LAN Switching and Wireless, CISCO Press, 2007.
3. Graziani, Rick, Accessing the WAN, CISCO Press, 2007.\
4. Heywood, D.1998. Networking with Microsoft TCP/IP 3rdEdition. USA : New Riders Publishing
5. Mogul, J. , "Internet Subnets",RFC 917, <http://asg2.web.cmu.edu/rfc/rfc917.html>, diakses tanggal 28 Januari 2021
6. Mogul, J. , and J. Postel, "Internet Standard Subnetting Procedure", RFC 950,<http://www.faqs.org/rfcs/rfc950.html>, diakses tanggal 29 Januari 2021
7. Pummill, T. , and B. Manning, "Variable Length Subnet Table For IPv4", RFC 1878<http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1878.html>, diakses tanggal 30 Januari 2021

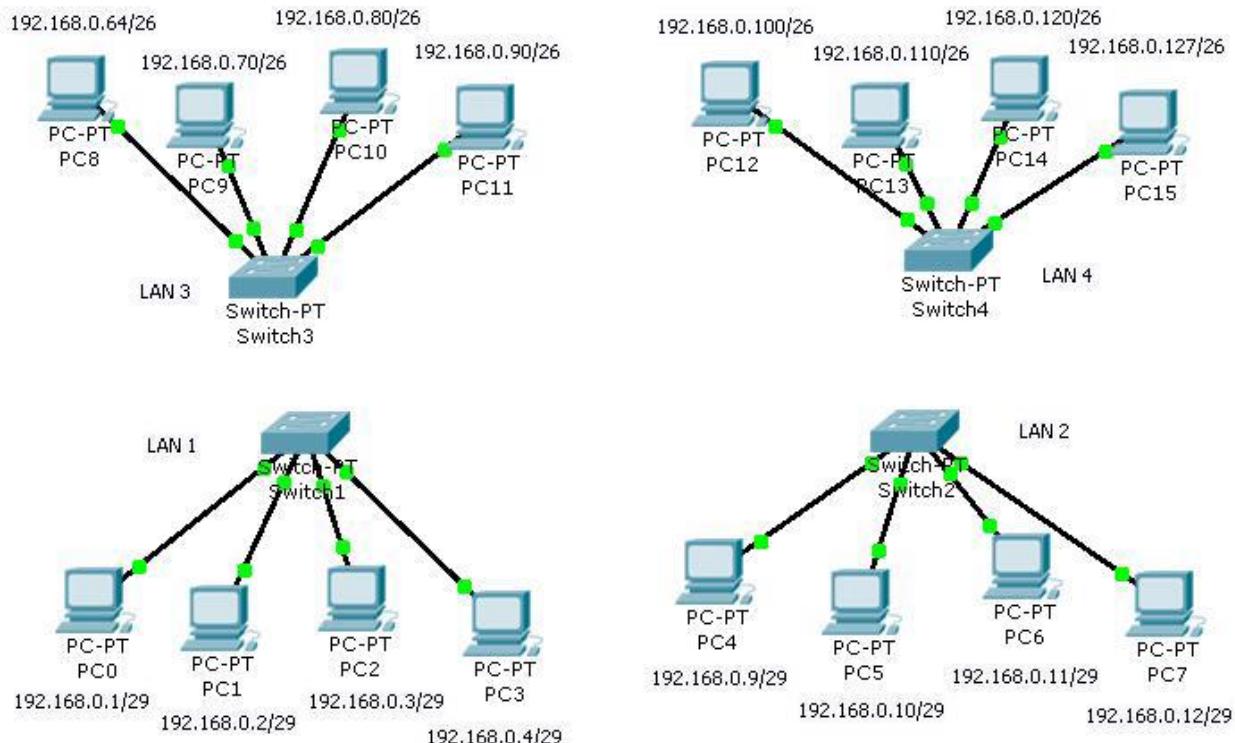
3.7 Tugas

Latihan – 1

1. kerjakan beberapa soal di bawah ini :
 - a) diketahui IP Address sebagai berikut :
 - (1)10.24.36.27/8 ,
 - (2)10.24.36 / 12 ,
 - (3)10.24.36.2 / 16 ,
 - (4)10.24.36.2 / 23cari berapakah subnet mask untuk masing-masing IP Address
 - b) cari prefix mask untuk IP Address dan Subnet Mask di bawah ini :
 - (1) 10.24.36.2 - 255.255.24.0
 - (2) 10.24.36.2 - 255.255.255.192
 - (3) 10.24.36.2 - 255.255.255.242
 - (4) 10.24.36.2 - 255.254.0.0
 - (5) 10.24.36.2 - 255.255.240.0



2. Buatlah skema jaringan seperti di bawah ini :



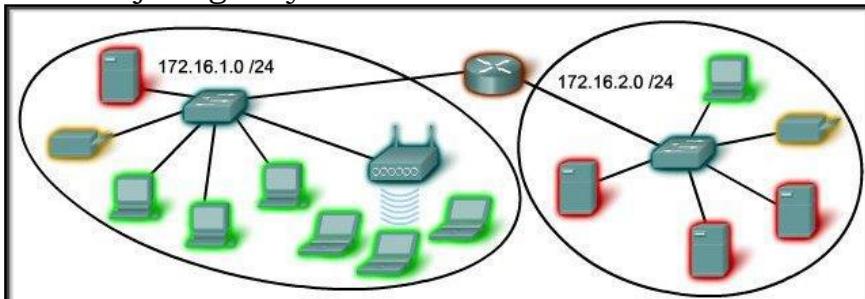
- Apakah semua PC dapat dikonfigurasi sesuai gambar
- Bila ada PC yang tidak dapat dikonfigurasi sesuai gambar, PC berapa yang tidak dapat dikonfigurasi, jelaskan kenapa?
- Rubah konfigurasi IP Address PC yang keliru agar dapat menjadi bagian dari subnet
- Berapa konfigurasi IP Address dan netmask yang semestinya
- Berapa range IP untuk LAN 1, 2 dan 3

Menguji koneksi antar PC tiap subnet

- Hubungkan switch 1 dengan switch 2, switch 3 dengan switch 4
- Dapatkan PC di LAN 1 dikoneksikan dengan PC di LAN 2, jelaskan
- Dapatkah PC di LAN 3 dikoneksikan dengan PC di LAN 4, Jelaskan
- Bagaimana caranya agar PC di LAN 1 dapat terkoneksi dengan PC di LAN
- Berikan solusi dalam topologi tersebut agar semua PC di tiap-tiap subnet (LAN) dapat terhubung satu sama lain, lampirkan gambar hasilnya dengan packet tracer.

Latihan - 2

Anda diberikan kasus untuk membangun sebuah server, berikut koneksi jaringannya :



Diberikan pula beberapa aturan penomoran IP Address nya, sebagai berikut. Buatlah dengan menggunakan software packet tracer

Use	FirstAddress	LastAddress
Network Address	172.16.x.0	
User Hosts (DHCP Pool)	172.16.x.1	172.16.x.127
Servers	172.16.x.128	172.16.x.191
Peripherals	172.16.x.192	172.16.x.223
Networking Devices	172.16.x.224	172.16.x.253
Router	172.16.x.254	
Broadcast	172.16.x.255	

Setelah koneksi berhasil, dan sesuai dengan koneksi diatas, laporan konfigurasi yang anda buat dan tuliskan konfigurasi ke empat server yang anda rancang dan lakukan analisis penomoran IP Address yang anda lakukan ?

3.8 Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, MODUL I PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Bottom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



MODUL IV

PENGENALAN PENGKABELAN

4.1 Tujuan Praktikum

1. Untuk mengetahui jenis – jenis kabel LAN
2. Untuk mengetahui arsitektur jaringan LAN
3. Untuk mengidentifikasi kabel jaringan LAN

4.2 Indikator Pencapaian

1. Mampu melakukan crimping pada kabel jaringan LAN
2. Mampu menerapkan jenis – jenis kabel pada jaringan LAN

4.3 Materi

4.3.1. Kabel LAN

Merupakan media transmisi Ethernet yang menghubungkan piranti-2 jaringan dalam jaringan komputer kita. Adalah sangat bermanfaat jika kita mengenal lebih baik mengenai kabel LAN sebelum kita membuat design jaringan. Design kabel jaringan yang bagus, merupakan unsur pendukung yang membuat jaringan komputer LAN kita nantinya mudah dipelihara dan bisa dikitalkan.

Jadi kabel LAN sangat bermanfaat sekali dalam realitas jaringan. Pertama kali LAN menggunakan kabel “coaxial”. Kemudian, kabel “twisted pair” yang digunakan dalam sistem telepon telah mampu membawa frekuensi yang lebih tinggi dan dapat mendukung trafik LAN. Dan saat ini, kabel fiber optik telah tampil sebagai pilhan kabel berkecepatan sangat tinggi. Local Area Network menggunakan tiga tipe kabel :

- a. Twisted Pair
- b. Coaxial
- c. Fiber Optik

4.3.2. Arsitektur Jaringan

Ada beberapa macam tipe Ethernet yang secara umum terbagi atas dua bagian yaitu yang mempunyai kecepatan 10 MBps dan Fast Ethernet yaitu yang mempunyai kecepatan 100 MBps atau lebih. Ethernet 10 MBps yang sering digunakan adalah 10Base2, 10Base5, 10BaseT dan 10BaseF. Sedangkan untuk kategori Fast Ethernet adalah 100BaseT dan 100VG-AnyLAN.



4.3.3. 10Base2

10Base2 disebut juga Thin Ethernet karena menggunakan kabel Coaxial jenis Thin atau disebut sebagai Cheapernet. 10Base2 menggunakan topologi Bus. Spesifikasi 10Base2 adalah sebagai berikut:

- Panjang kabel per-segmen adalah 185 m
- Total segmen kabel adalah 5 buah
- Maksimum Repeater adalah 4 buah
- Maksimum jumlah segmen yang terdapat node (station) adalah 3 buah
- Jarak terdekat antar station minimum 0,5 m
- Maksimum jumlah station dalam satu segmen kabel adalah 30
- Maksimum panjang keseluruhan dengan Repeater adalah 925 m
- Awal dan akhir kabel diberi Terminator 50 ohm
- Jenis kabel yang digunakan RG-58A/U atau RG-58C/U

4.3.4. 10Base5

10Base5 disebut juga Thick Ethernet karena menggunakan kabel Coaxial jenis Thick. Topologi pada 10Base5 sama seperti 10Base2 yaitu Topologi Bus. Spesifikasi dari 10Base5 adalah sebagai berikut:

- Panjang kabel per-segmen adalah 500 m
- Total segmen kabel adalah 4 buah
- Maksimum jumlah segmen yang terdapat node adalah 3
- Jarak terdekat antar station minimum adalah 2,5 m
- Maksimum jumlah station dalam satu segmen kabel adalah 100
- Maksimum panjang kabel AUI ke node 50 m
- Maksimum panjang keseluruhan dengan Repeater 2500 m
- Awal dan akhir kabel diberi Terminator 50 ohm
- Jenis kabel Coaxial RG-8 atau RG-11

4.3.5. 10BaseT

Berbeda dengan 10Base2 atau 10Base5 yang menggunakan topologi Bus, pada ethernet TbaseT menggunakan topologi Star. Ethernet dengan topologi Star ini paling banyak digunakan, karena mudah pemasangannya serta melakukan pengecekan jika ada kerusakan pada jaringan. Pada 10BaseT kabel yang dipakai bukan Coaxial tapi kabel UTP. Spesifikasi dari 10BaseT adalah sebagai berikut:

- Panjang kabel per-segmen maksimum 100 m
- Maksimum jumlah segmen adalah 1024
- Maksimum jumlah node per-jaringan 1024
- Menggunakan Hub dengan jumlah maksimum 4 buah dalam bentuk hubungan chain
- Kabel yang digunakan UTP Category-3 atau lebih



4.3.6. 10BaseF

10BaseF menggunakan kabel serat optik, ini jarang digunakan karena biasanya mahal dan pemasangannya tidak semudah ethernet tipe lain. Umumnya jenis ini dipakai untuk penghubung (link) antar segmen karena jaraknya bisa mencapai 2000 m serta kabel yang digunakan adalah serat optik.

4.3.7. 100BaseT

100BaseT disebut juga Fast Ethernet atau 100BaseX, adalah ethernet yang mempunyai kecepatan 100 Mbps. Ada beberapa tipe 100BaseT berdasarkan kabel yang dipakai, yaitu:

- 100BaseT4, memakai kabel UTP Category-5 dan kabel yang dipakai adalah 4 pasang
- 100BaseTX, memakai kabel UTP Category-5 dan kabel yang dipakai hanya 2 pasang
- 100BaseTX, memakai kabel serat optic

Pada 100BaseT yang menggunakan kabel Coaxial maksimum total kabelnya dengan menggunakan Hub Class II adalah 205 m, dengan perincian 100 m untuk panjang segmen dan 5 m untuk hubungan Hubke Hub. Sedangkan untuk 100BaseFX dengan menggunakan dua Repeater bisa mencapai 412 m, dan panjang segmen dengan serat optik bisa mencapai 2000 m.

4.3.8. 100VG-AnyLAN

100VG-AnyLAN bukan merupakan ethernet umum murni karena metode akses medianya berdasarkan demand priority. 100VG-AnyLAN bisa digunakan dengan sistem Frame Ethernet ataupun dengan Frame Token Ring.

Kabel yang digunakan adalah kabel UTP Category-3 atau 5. Tidak seperti ethernet biasa yang menggunakan kabel UTP dengan panjang maksimum segmen 100 m, maka pada 100VG-AnyLAN jika yang dipakai adalah UTP Category-5 maka panjang maksimum segmen- nya bisa mencapai 150 m, sedangkan yang memakai serat optik panjang maksimum segmen-nya adalah 2000 m.

4.3.9. Jenis – Jenis Kabel LAN

4.3.9.1. Twisted Pair

KabelTwisted pair (pasangan berpilin) adalah sebuah bentuk kabel di mana dua konduktor digabungkan dengan tujuan untuk mengurangi atau meniadakan interferensi elektromagnetik dari luar seperti radiasi elektromagnetik dari kabel unshielded twisted pair (UTP) cables, dan crosstalk di antara pasangan kabel yang berdekatan.



4.3.9.1.1. Kabel Unshielded Twisted Pair (UTP)

Unshielded twisted-pair (disingkat UTP) adalah sebuah jenis kabel jaringan yang menggunakan bahan dasar tembaga, yang tidak dilengkapi dengan shield internal. UTP merupakan jenis kabel yang paling umum yang sering digunakan di dalam jaringan lokal (LAN), karena memang harganya yang rendah, fleksibel dan kinerja yang ditunjukannya relatif bagus. Dalam kabel UTP, terdapat insulasi satu lapis yang melindungi kabel dari ketegangan fisik atau kerusakan tapi, tidak seperti kabel Shielded Twisted-pair (STP), insulasi tersebut tidak melindungi kabel dari interferensi elektromagnetik.

Kabel UTP memiliki impedansi kira-kira 100 Ohm dan tersedia dalam beberapa kategori yang ditentukan dari kemampuan transmisi data yang dimilikinya seperti tertulis dalam tabel berikut.

Tabel 4.1 Kategori Kabel UTP

Kategori	Type	Kegunaan
Category 1 (Cat1)	UTP	Kualitas suara analog
Category 2 (Cat2)	UTP	Transmisi suara digital hingga 4 Megabit per detik
Category 3 (Cat3)	UTP / STP	Transmisi data digital hingga 10 Megabit per detik
Category 4 (Cat4)	UTP, STP	Transmisi data digital hingga 16 Megabit per detik
Category 5 (Cat5)	UTP, STP hingga 100MHz	Transmisi data digital hingga 100 Megabit per detik
Enhanced Category 5 (Cat5e)	UTP, STP hingga 100MHz	Transmisi data digital hingga 1 Gigabit per detik
Category 6 (Cat6)	Hingga 155MHz atau 250MHz	Transmisi data digital hingga 2Gigabit per detik
Category 7 (Cat7)	Hingga 200MHz atau 700MHz	Transmisi data digital hingga Giga Ethernet

Di antara semua kabel di atas, kabel Enhanced Category 5 (Cat5e) dan Category 5 (Cat5) merupakan kabel UTP yang paling populer yang banyak digunakan dalam jaringan berbasis teknologi Ethernet.

1. Category 1



Kabel LAN UTP Cat 1 adalah kabel UTP dengan kualitas transmisi terendah, yang didesain untuk mendukung komunikasi suara analog saja. Kabel Cat1 digunakan sebelum tahun 1983 untuk menghubungkan telepon analog Plain Old Telephone Service (POTS).

Karakteristik kelistrikan dari kabel Cat1 membuatnya kurang sesuai untuk digunakan sebagai kabel untuk mentransmisikan data digital di dalam jaringan komputer, dan karena itulah tidak pernah digunakan untuk tujuan tersebut.

2. Category 2

Kabel LAN UTP Cat 2 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 1 (Cat1), yang didesain untuk mendukung komunikasi data dan suara digital. Kabel ini dapat mentransmisikan data hingga 4 megabit per detik. Seringnya, kabel ini digunakan untuk menghubungkan node-node dalam jaringan dengan teknologi Token Ring dari IBM. Karakteristik kelistrikan dari kabel Cat2 kurang cocok jika digunakan sebagai kabel jaringan masa kini. aslinya dimaksudkan untuk mendukung Token Ring lewat UTP.

3. Category 3

Kabel LAN Cat 3 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 2 (Cat2), yang didesain untuk mendukung komunikasi data dan suara pada kecepatan hingga 10 megabit per detik. Kabel UTP Cat3 menggunakan kawat-kawat tembaga 24-gauge dalam konfigurasi 4 pasang kawat yang dipilin (twisted-pair) yang dilindungi oleh isolasi. Cat3 merupakan kabel yang memiliki kemampuan terendah (jika dilihat dari perkembangan teknologi Ethernet), karena memang hanya mendukung jaringan 10BaseT saja Kabel LAN ini bisa dipakai untuk jaringan telpon dan merupakan pilihan kabel LAN UTP masa silam.

Tabel berikut menyebutkan beberapa karakteristik yang dimiliki oleh kabel UTP Category 3 pada beberapa frekuensi.

Table 4.2 Karakteristik Kabel UTP Category 3

Karakteristik	Nilai Pada Frekuensi	
	10 Mhz	16 Mhz
Attenuation (pelemahan sinyal)	27 dB/1000 kaki	36 dB/1000 kaki
Near-end Cross-Talk (NEXT)	26 dB/1000 kaki	23 dB/1000 kaki
Resistansi	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki



ITB AHMAD DAHLAN
Socio Technopreneur University

Kapasitansi

18 picoFarad/kaki

18 icoFarad/kaki



4. Category 4

Kabel LAN UTP Cat 4 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 3 (Cat3), yang didesain untuk mendukung komunikasi data dan suara hingga kecepatan 16 megabit per detik. Kabel ini menggunakan kawat tembaga 22-gauge atau 24-gauge dalam konfigurasi empat pasang kawat yang dipilin (twisted pair) yang dilindungi oleh insulasi. Kabel ini dapat mendukung jaringan Ethernet 10BaseT, tapi seringnya digunakan pada jaringan IBM Token Ring 16 megabit per detik., umum dipakai jaringan versi cepat Token Ring.

Tabel berikut menyebutkan beberapa karakteristik yang dimiliki oleh kabel UTP Category 4 pada beberapa frekuensi.

Table 4.3 Karakteristik Kabel UTP Category 4

Karakteristik	Nilai Pada Frekuensi 10 Mhz	Nilai Pada Frekuensi 20 Mhz
Attenuation	20 dB/1000 kaki	31 dB/1000 kaki
Near-end Cross-Talk	41 dB/1000 kaki	36 dB/1000 kaki
Resistansi	28.6 Ohm/1000kaki	28.6 Ohm/1000kaki
Impedansi	100 Ohm ($\pm 15\%$)	100 Ohm ($\pm 15\%$)
Kapasitansi	18 picoFarad/kaki	18 icoFarad/kaki

5. Category 5

Kabel LAN Cat 5 kabel dengan kualitas transmisi yang jauh lebih baik dibandingkan dengan kabel UTP Category 4 (Cat4), yang didesain untuk mendukung komunikasi data serta suara pada kecepatan hingga 100 megabit per detik. Kabel ini menggunakan kawat tembaga dalam konfigurasi empat pasang kawat yang dipilin (twisted pair) yang dilindungi oleh insulasi. Kabel ini telah distandardisasi oleh Electronic Industries Alliance (EIA) dan Telecommunication Industry Association (TIA).

Kabel Cat5 dapat mendukung jaringan Ethernet (10BaseT), Fast Ethernet (100BaseT), hingga Gigabit Ethereret (1000BaseT). Kabel ini adalah kabel paling populer, mengingat kabel serat optik yang lebih baik harganya hampir dua kali lipat lebih mahal dibandingkan dengan kabel Cat5. Karena memiliki karakteristik kelistrikan yang lebih baik, kabel Cat5 adalah kabel yang disarankan untuk semua instalasi jaringan. kecepatan maksimum 1 Gigabps, sangat popular untuk kabel LAN desktop



Table 4.4 Karakteristik Kabel UTP Category 5

Karakteristik	Nilai Pada Frekuensi 10 Mhz	Nilai Pada Frekuensi 100 Mhz
Attenuation	20 dB/1000 kaki	22 dB/1000 kaki
Near-end Cross-talk	47 dB/1000 kaki	32.3 dB/1000 kaki
Resistansi	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki
Impendansi	100 Ohm ($\pm 15\%$)	100 Ohm ($\pm 15\%$)
Kapasitansi	18 picoFarad/kaki	18 picoFarad/kaki
Structural return loss	16 dB	16 dB
Delay skew	45 nanodetik/100 meter	45 anodetik/100meter

6. Category 5e

Kabel LAN UTP Cat 5e, Kabel ini merupakan versi perbaikan dari kabel UTP Cat5, yang menawarkan kemampuan yang lebih baik dibandingkan dengan Cat5 biasa. Kabel ini mampu mendukung frekuensi hingga 250 MHz, yang direkomendasikan untuk penggunaan dalam jaringan Gigabit Ethernet, dengan kecepatan maksimum 1 Gigabps, tingkat emisi lebih rendah, lebih mahal dari Cat 5 akan tetapi lebih bagus untuk jaringan Gigabit.

7. Category 6

Kabel LAN UTP Cat 6, kecepatan maksimum adalah 1 Gigabps+, dimaksudkan sebagai pengganti Cat 5e dengan kemampuan mendukung kecepatan-2 multigigabit.

→ Identifikasi UTP

Kita harus terbiasa dengan baik untuk bisa mengidentifikasi kabel ini dengan memeriksa pin-2 nya. Sebenarnya ada dua macam standart yaitu:

1. T568-A adalah kabel LAN UTP jenis straight through, kedua ujung penempatan kabel pada pin-2 konektor RJ-45 adalah sama.
2. T568-B adalah kabel LAN UTP jenis cross-over. Kita bisa perhatikan dengan seksama pada kabel cross-over ini, pasangan pin 2 dan 6 dan pasangan pin 1 dan 3 bertukar tempat.

→ Straight Trough Cable

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat yang berbeda, contoh PC To Switch, Switch To Router, PC To Hub. Kabel ini menghubungkan ujung satu dengan ujung lain dengan satu warna, dalam artinya ujung nomor satu merupakan ujung nomor dua di ujung lain. Sebenarnya urutan warna dari masing-masing kabel tidak menjadi masalah, namun ada standard secara internasional yang digunakan untuk straight trough cable ini, yaitu : Untuk kabel dengan konfigurasi memiliki susunan warna sebagai berikut (T568-A) :



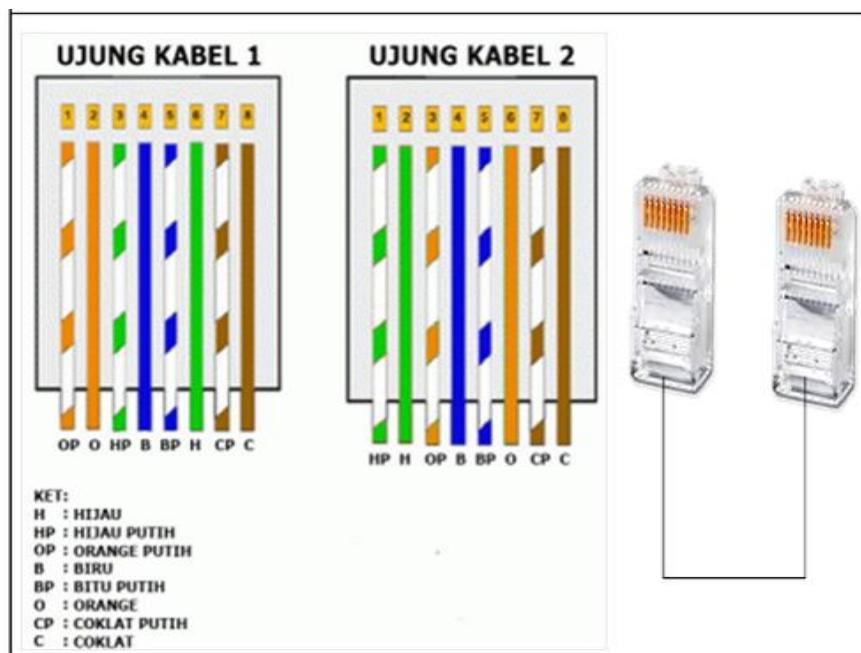
Gambar 4.1 Warna Kabel Straight Trough

Table 4.5 Konfigurasi Warna Kabel Straight Trough

No.	T568-A	T568-B
1	Putih Orange	Putih Orange
2	Orange	Orange
3	Putih Hijau	Putih Hijau
4	Biru	Biru
5	Putih Biru	Putih Biru
6	Hijau	Hijau
7	Putih Coklat	Putih Coklat
8	Coklat	Coklat

→ Cross Over Cable

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat setingkat, sebagai contoh koneksi antara PC to PC, atau PC ke AP Radio, Router to router. Berikut konfigurasi pengkabelan/pemasangan konektor RJ-45: untuk cross memiliki konfigurasi kabel dengan ujung – ujung A-B atau B-A , maksudnya jika salah satu ujung nya seperti ini :



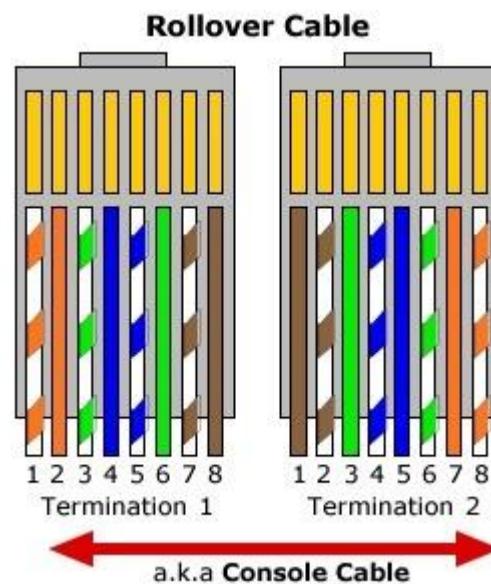
Gambar 4.2 Warna Kabel Cross Over

Table 4.6 Konfigurasi Warna Kabel Cross Over

	T568-A	T568-B	Keterangan
1	Putih Orange	Putih Hijau	Tukar dengan 3
2	Orange	Hijau	Tukar dengan 6
3	Putih Hijau	Putih Orange	Tukar dengan 1
4	Biru	Biru	Tetap
5	Putih Biru	Putih Biru	Tetap
6	Hijau	Orange	Tukar dengan 2
7	Putih Coklat	Putih Coklat	Tetap
8	Coklat	Coklat	Tetap

→ Roll Over Cable

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat yang berbeda, hampir sama pengertiannya dengan straight trough namun jenis kabel ini lebih menghubungkan perangkat yang memiliki konsole sebagai contoh koneksi antara Switch To Printer, atau Switch To Infocus. Berikut konfigurasi pengkabelan/pemasangan konektor RJ-45: untuk roll memiliki konfigurasi kabel dengan ujung – ujung A dan ujung satunya kebalikan warna A , maksudnya jika salah satu ujung nya seperti ini :



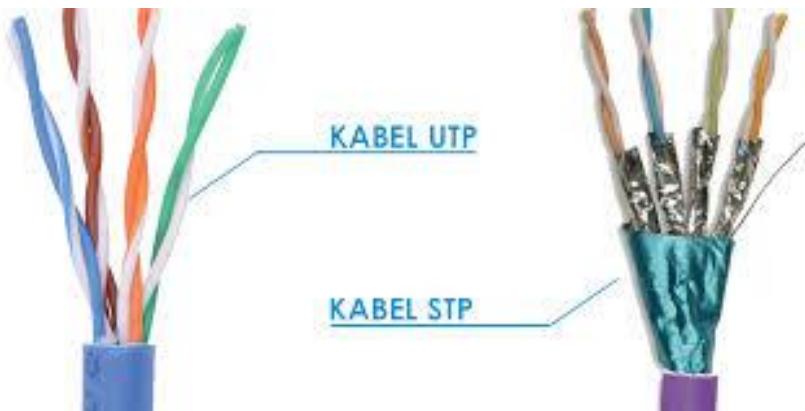
Gambar 4.3 Warna Kabel Cross Over

Table 4.7 Konfigurasi Warna Kabel Roll Over

	T568-A	T568-A	Keterangan
1	Putih Orange	Coklat	Tukar dengan 8
2	Orange	Putih Coklat	Tukar dengan 7
3	Putih Hijau	Hijau	Tukar dengan 6
4	Biru	Putih Biru	Tukar dengan 5
5	Putih Biru	Biru	Tukar dengan 4
6	Hijau	Putih Hijau	Tukar dengan 3
7	Putih Coklat	Orange	Tukar dengan 2
8	Coklat	Putih Orange	Tukar dengan 1

4.3.9.1.2. Kabel Shielded Twisted Pair (STP)

Kabel STP sama dengan kabel UTP, tetapi kawatnya lebih besar dan diselubungi dengan lapisan pelindung isolasi untuk mencegah gangguan interferensi. Jenis kabel STP yang paling umum digunakan pada LAN ialah IBM jenis/kategori 1.



Gambar 4.4 Contoh Kabel UTP dan STP

4.3.9.2. Kabel Coaxial

Terdiri atas dua kabel yang diselubungi oleh dua tingkat isolasi. Tingkat isolasi pertama adalah yang paling dekat dengan kawat konduktor tembaga. Tingkat pertama ini dilindungi oleh serabut konduktor yang menutup bagian atasnya yang melindungi dari pengaruh elektromagnetik. Sedangkan bagian inti yang digunakan untuk transfer data adalah bagian tengahnya yang selanjutnya ditutup atau dilindungi dengan plastik sebagai pelindung akhir untuk menghindari dari goresan kabel.

Penggunaan kabel coaxial pada LAN memiliki beberapa keuntungan. Penguatannya dari repeater tidak sebesar kabel STP atau UTP. Kabel coaxial lebih murah dari kabel fiber optic dan teknologinya juga tidak asing lagi. Kabel coaxial sudah digunakan selama puluhan tahun untuk berbagai jenis komunikasi data. Ketika bekerja dengan kabel, adalah penting untuk mempertimbangkan ukurannya.

Seiring dengan pertambahan ketebalan atau diameter kabel, maka tingkat kesulitan penggerjaannya pun akan semakin tinggi. Kita harus ingat pula bahwa kabel ini harus ditarik melalui pipa saluran yang ada dan pipa ini ukurannya terbatas.

Kabel coaxial memiliki ukuran yang bervariasi. Diameter yang terbesar ditujukan untuk penggunaan kabel backbone Ethernet karena secara historis memiliki panjang transmisi dan penolakan noise yang lebih besar. Kabel coaxial ini seringkali dikenal sebagai thicknet. Seperti namanya, jenis kabel ini, karena ukurannya yang besar, pada beberapa situasi tertentu dapat sulit diinstall. Suatu petunjuk praktis menyatakan bahwa semakin sulit media jaringan diinstall. Suatu petunjuk praktis menyatakan bahwa semakin sulit media jaringan



diinstall, maka semakin mahal media tersebut diinstall. Kabel coaxial memiliki biaya instalasi yang lebih mahal dari kabel twisted pair. Kabel thicknet hampir tidak pernah digunakan lagi, kecuali untuk kepentingan khusus.

Beberapa jenis kabel coaxial lebih besar dari pada yang lain. Makin besar kabel, makin besar kapasitas datanya, lebih jauh jarak jangkauannya dan tidak begitu sensitif terhadap interferensi listrik.

Table 4.8 Tipe Kabel Coxial

Tipe Kabel Coxial	Arsitektur	Terminator Yang Dipakai
RG-8	Ethernet 10Base5	50 Ω
RG-11	Ethernet 10Base5	50 Ω
RG-51A/U	Ethernet 10Base5	50 Ω
RG-59/U	ARCnet, CATV	75 Ω
RG-62A/U	ARCnet	93 Ω

4.3.9.3. Thick coaxial cable (Kabel Coaxial “gemuk”)

Kabel Coaxial ini (RG-6) jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut:

- Setiap ujung harus diterminasi dengan terminator 50-ohm (dianjurkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah resistor 50-ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar).
- Maksimum 3 segment dengan peralatan terhubung (attached devices) atau berupa populated segments.
- Setiap kartu jaringan mempunyai pemancar tambahan (external transceiver).
- Setiap segment maksimum berisi 100 perangkat jaringan, termasuk dalam hal ini repeaters.
- Maksimum panjang kabel per segment adalah 1.640 feet (atau sekitar 500 meter).
- Maksimum jarak antar segment adalah 4.920 feet (atau sekitar 1500 meter).
- Setiap segment harus diberi ground.
- Jarang maksimum antara tap atau pencabang dari kabel utama ke perangkat (device) adalah 16 feet (sekitar 5 meter).
- Jarang minimum antar tap adalah 8 feet (sekitar 2,5 meter).

4.3.9.4. Thin coaxial cable (Kabel Coaxial “Kurus”)

Kabel coaxial jenis ini banyak dipergunakan di kaLANgan radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang

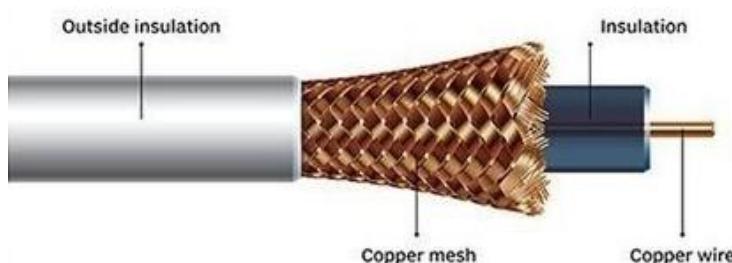
besar. Untuk digunakan sebagai perangkat jaringan, kabel coaxial jenis ini harus memenuhi standart IEEE 802.3 10BASE2,

dimana diameter rata-rata berkisar 5mm dan biasanya berwarna hitam atau warna gelap lainnya. Setiap perangkat (device) dihubungkan dengan BNC T-connector. Kabel jenis ini juga dikenal sebagai thin Ethernet atau ThinNet.

Kabel coaxial jenis ini, misalnya jenis RG-58 A/U atau C/U, jika diimplementasikan dengan T-Connector dan terminator dalam sebuah jaringan, harus mengikuti aturan sebagai berikut:

- Setiap ujung kabel diberi terminator 50-ohm.
- Panjang maksimal kabel adalah 1,000 feet (185 meter) per segment.
- Setiap segment maksimum terkoneksi sebanyak 30 perangkat jaringan (devices)
- Kartu jaringan cukup menggunakan transceiver yang onboard, tidak perlu tambahan transceiver, kecuali untuk repeater.
- Maksimum ada 3 segment terhubung satu sama lain (populated segment).
- Setiap segment sebaiknya dilengkapi dengan satu ground.
- Panjang minimum antar T-Connector adalah 1,5 feet (0.5 meter).
- Maksimum panjang kabel dalam satu segment adalah 1,818 feet (555 meter).
- Setiap segment maksimum mempunyai 30 perangkat terkoneksi.

Coaxial cable



Gambar 4.5 Kabel Coaxial

4.3.9.5. Kabel Serat Optik (Fiber Optik)

Kabel fiber optic merupakan kabel jaringan yang dapat mentransmisi cahaya. Dibandingkan dengan jenis kabel lainnya, kabel ini lebih mahal. Namun, fiber optic memiliki jangkauan yang lebih jauh dari 550 meter sampai ratusan kilometer, tahan terhadap interferensi elektromagnetik dan dapat mengirim data pada kecepatan yang lebih tinggi dari jenis kabel lainnya. Kabel fiber optic tidak membawa sinyal elektrik, seperti kabel lainnya yang menggunakan kabel tembaga. Sebagai gantinya,



sinyal yang mewakili bit tersebut diubah ke bentuk cahaya. biasanya fiber optic digunakan pada jaringan backbone (TuLANG Punggung) karena dibutuhkan kecepatan yang lebih dalam jaringan ini,namun pada saat ini sudah banyak yang menggunakan fiber optic untuk jaringan biasa baik LAN, WAN maupun MAN karena dapat memberikan dampak yang lebih pada kecepatan dan bandwith karena fiber optic ini menggunakan bias cahaya untuk mentransfer data yang melewatinya dan sudah barang tentu kecepatan cahaya tidak diragukan lagi namun untuk membangun jaringan dengan fiber optic dibutuhkan biaya yang cukup mahal dikarenakan dibutuhkan alat khusus dalam pembangunannya.

4.3.10. Proses Penyambungan FO

Biasanya kabel fiber optic digulung pada haspel. Panjang kabel fiber optic dalam sebuah haspel bergantung pada besarnya kabel dan haspelnya. Ada haspel yang dapat menampung 2000 m kabel fiber optic. Karena kabel fiber optic digelar untuk jarak jauh (dapat mencapai puluhan atau ratusan kilometer) maka diperlukan proses penyambungan yang disebut proses splicing. Alat untuk melakukan proses penyambungan kabel fiber optic disebut FUSION SPLICE.

Alat ini yang digunakan untuk menyambung dua ujung fiber optic dengan menggunakan panas, alat ini butuh ketelitian yang sangat tinggi, alat ini dilengkapi dengan alat pengukur karena setiap ingin menyambung dua sisi fiber optic harus diukur terlebih dahulu dan ukurannya harus sama antara ujung A dan ujung B dan kedua ujung fiber optic harus benar-benar bersih (biasanya digunakan alcohol 95% dan tisu untuk membersihkan ujung fiber optic yang sudah dikupas) karena apabila ada kotoran sedikit saja maka fusion splicer tidak akan bisa digunakan, alias menolak untuk melakukan penyambungan.

4.3.11. Pemasangan Connector FO

Terminasi adalah proses pemasangan connector pada fiber optic. Proses ini tidak dapat dilakukan secara sembarangan, mengingat diameter kabel fiber optic adalah sedemikian kecil, jauh lebih kecil daripada rambut manusia.Connector yang selalu digunakan untuk menyambung kabel fiber optik ialah SC connector yang menyerupai BNC connector. Namun SC connector akan menjadi lebih popular karena mudah digunakan.

Untuk melakukan terminasi diperlukan tool kit yang disebut termination kit. Proses terminasi connector fiber optic dimulai dengan mengupas jaket kabel dengan suatu alat yang dikenal sebagai stripper, lalu core fiber optic dipotong dengan alat scribe. Selanjutnya core fiber optic dimasukkan ke dalam connector, yang selanjutnya direkat dengan lem epoxy. Setelah kering, epoxy ini akan dipanaskan dalam oven, untuk selanjutnya fiber optic dipoles dengan lapping film.



ITB AHMAD DAHLAN
Socio Technopreneur University

Untuk mengerjakan terminasi, seorang terminator perlu bekerja dengan presisi dan teliti, mengingat yang ditangani adalah kabel fiber optic yang sangat kecil.

ITB-AHMAD DAHLAN CIPUTAT

Jl. Ir. H. Juanda No.77 Cirendeu, Ciputat Tangerang Selatan

ITB-AHMAD DAHLAN KARAWACIH

Jl. Imam Bonjol No.4/9, RT.001/RW.009, Panunggangan Bar
Kec. Cibodas, Kota Tangerang Banten 15138

4.3.12. Jenis-Jenis Kabel Fo

4.3.12.1. Single Mode

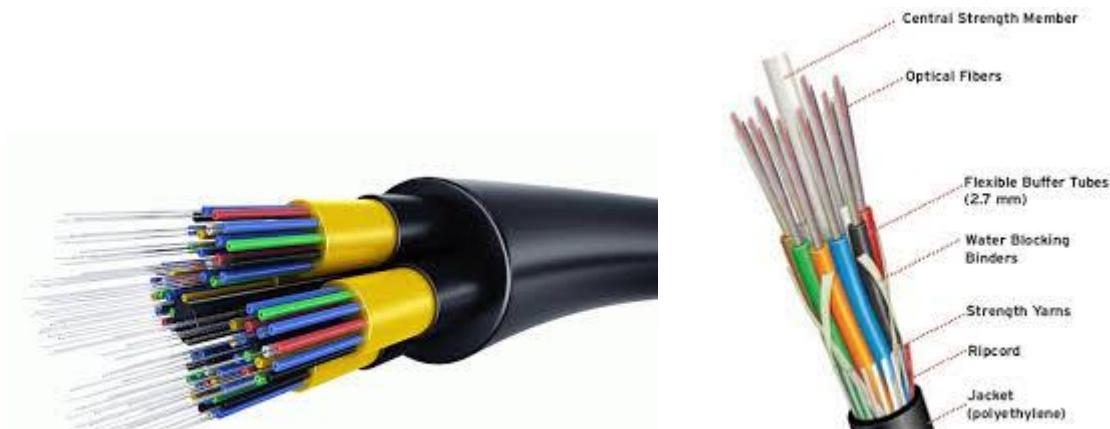
Yaitu serat optic dengan core yang sangat kecil, sekitar 8 mikro meter. Besar diameternya mendekati panjang gelombang, sehingga cahaya yang masuk ke dalamnya tidak terpantul-pantul ke dinding cladding. Kabel single mode dapat menjangkau jarak yang lebih jauh. Ia hanya mengirim satu sinyal pada waktu yang sama. Pulsa cahaya yang ditembakkan pada single mode adalah cahaya dengan panjang gelombang 1310-1550nm.

4.3.12.2. Multi Mode Step Index

Yaitu serat optic dengan diameter core yang sedikit lebih besar dibanding single mode, sekitar 10 mikro meter. Ukuran tersebut membuat laser di dalamnya terpantul didinding cladding, yang dapat menyebabkan berkurangnya bandwidth dari serat optic jenis ini. Kabel jenis ini dapat mengirimkan data yang berbeda pada saat yang bersamaan. Namun, jika kabel single mode dapat menjangkau ratusan kilometer, kabel multi mode hanya mampu menjangkau kurang dari 550 meter.

4.3.12.3. Multimode Grade Index

Yaitu serat optic dengan diameter core yang terbesar, dibanding dua jenis serat optic lainnya. Jenis yang satu ini tidak terlalu banyak digunakan.



Gambar 4.6 Kabel Fiber Optik

4.3.13. Crimping

Crimping adalah istilah dalam bidang teknisi komputer yang digunakan untuk pemasangan kable LAN ke konektornya atau dapat disebut juga sebuah teknik dalam pembuatan kabel jaringan. Namun pada modul ini kita hanya akan membahas teknik crimping pada kabel UTP, peralatan dan media yang dibutuhkan dalam crimping ini adalah sebagai berikut :

4.3.13.1. Peralatan dan Bahan



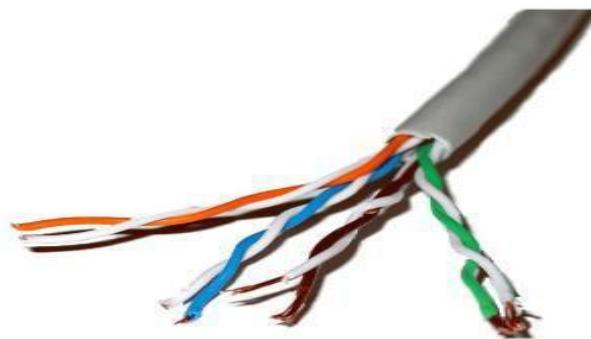
Gambar 4.7 Tang Crimping



Gambar 4.8 Gunting



Gambar 4.9 LAN Tester



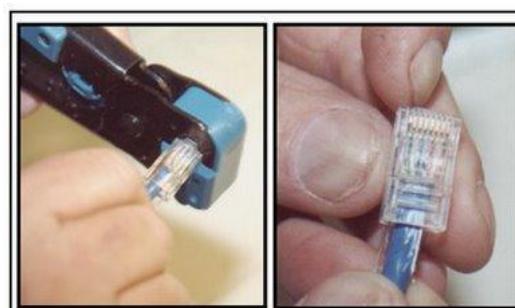
Gambar 4.10 Kabel UTP



Gambar 4.11 Konektor RJ-45

4.3.13.2. Cara Kerja

1. Kupas lapisan luar kabel UTP sepanjang \pm 1 cm dari ujung, sehingga 8 urat kabel terlihat dari luar.
2. Susun urutan warna kabel sesuai jenis kabel yang akan kita buat berdasarkan standard internasional.
3. Rapikan 8 urat kabel hingga sama rata, pada masing ujung-ujungnya.
4. Kemudian masukkan ujung kabel UTP yang telah disusun menurut urutan internasional, pastikan ekor konektor menghadap keluar, kemudian jepit dengan menggunakan crimping tool (Tang Crimping) sampai berbunyi “klik”



Gambar 4.12 Cara Menggunakan Tang Crimping



5. Ikuti caranya untuk ujung kedua sama dengan langkah pertama. Agar tidak terjadi kesalahan, pastikan kabel yang akan kita buat
6. Masukkan ujung kedua kabel kedalam LAN-tester lalu periksa, jika semua lampu indicator pada masing-masing ujung kabel dari 1 – 8 terhubung maka kabel ini sudah siap kita pakai.
7. Perhatian : penyusunan salah atau penjepitan yang salah menyebabkan RJ-45 Connector tidak bisa dipakai lagi.

4.4 Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
3. Crimpping Tools
4. Kabel
5. Multi Tester

4.5 Praktikum

Langkah Percobaan

- a. Siapkan semua peralatannya, terutama kabel, koneksi RJ-45 dan Crimping Tool
- b. Kupas bagian luar kabel kira-kira 1 cm dengan menggunakan pengupas kabel yang biasanya ada pada crimping tool.
- c. Susunlah kabel sesuai dengan keperluan (straight atau cross)
- d. Rapikan kabel kemudian potong ujung-ujung kabel yang tidak rata dengan pemotong kabel sampai rapi. Usahakan jarak antara pembungkus kabel sampai ujung kabel tidak lebih dari 1cm.
- e. Dengan tetap menekan perbatasan antara kabel yang terbungkus dan kabel yang tidak terbungkus, masukan kabel ke konektor RJ-45 sampai ujung-ujung kabel terlihat di bagian depan konektor RJ-45.
- f. Setelah yakin posisi kabel tidak berubah dan kabel sudah masuk dengan baik ke konektor RJ-45, selanjutnya masukan konektor RJ-45 tersebut ke tang crimping kemudian di-press.

Analisis

- a. Pemasangan kabel ke konektor RJ-45 dengan cara STRAIGHT DAN CROSS itu tidak lah mudah , harus sesuai dengan susunan warna yang telah di tentukan
- b. Pemotongan kabel kita merasa kesulitan karena baru pertama kali memotong kabel menggunakan Tang Crimping
- c. Pada pemasangan / pematenan RJ-45 harus secara hati-hati agar RJ-45 nya tidak pecah atau rusak.
- d. Proses akhir untuk mengetahui kabel RJ-45 yang telah di buat tadi kita menggunakan LAN/USB (cable transfer) , dan alhamdulillah pada percobaan dengan kabel SRTX dan CROS berhasil



4.6 Referensi

1. Micro, Andi. 2012. Dasar-dasar Jaringan Komputer. Banjarbaru: Andi Micro.
2. Arifin. 2011. Jaringan Komputer dan Internet. Jakarta: Mediakom.
3. Listanto, Virgiawan. 2011. Teknik Jaringan Komputer. Jakarta: PT. prestasi Pustakaraya.
4. RuangIT. 2013. Tentang Kabel UTP. Diambil dari : <http://ruang-it.com/tentang-kabel-utp/index.php> (diakses tanggal 15 Januari 2021)
5. Siswapedia. 2013. Jenis-jenis Kabel Jaringan. Diambil dari : <http://www.siswapedia.com/jenis-kabel-jaringan/#sthash.dNcaeJxh.dpuf> (diakses tanggal, 15 Januari 2021)
6. Vicky. 2010. Pengenalan Jaringan Local Komputer Local Area Network (LAN).
7. Diambil dari : <http://belajar-komputer-mu.com/artikel-pengenalan-jaringan-local-komputer-local-area-network-lan/> (diakses tanggal 21 Januari 2021)

4.7 Tugas

Membuat Jaringan Sederhana dengan Cisco Packet Tracer, disini saya akan memberikan membuat sebuah jaringan computer yang terdiri dari;

- 21 komputer + 3 switch + 1 server

Tugas Anda adalah menghubungkan ke 21 komputer ke server tersebut dengan perantara switch

4.8 Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, MODUL I PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Bottom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



MODUL V

PENGANTAR LAN (LOCAL AREA NETWORK)

5.1 Tujuan Praktikum

1. Untuk memahami jaringan Peer to Peer dan jaringan Client-Server
2. Untuk mengetahui beberapa elemen dasar pada LAN
3. Untuk memahami VLAN (Virtual Local Area Network)
4. Untuk memahami cara kerja Wireless LAN (WLAN)
5. Untuk mengetahui komponen-komponen pada WLAN

5.2 Indikator Pencapaian

1. Mampu mengkonfigurasi jaringan Peer to Peer dan jaringan Client-Server.
2. Mampu menentukan komponen fisik dan komponen software yang digunakan didalam jaringan
3. Mampu mengkonfigurasi jaringan pada Windows 10
4. Mampu mengkonfigurasi TCP/IP
5. Mampu mengkonfigurasi jaringan VLAN (Virtual Local Area Network)
6. Mampu mengkonfigurasi jaringan Asymmetric VLAN & Port Management
7. Mampu mengkonfigurasi jaringan WLAN

5.3. Materi

5.3.1. Pengertian LAN

Local Area Network (LAN) adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung. Secara garis besar terdapat dua tipe jaringan atau LAN, yaitu jaringan Peer to Peer dan jaringan Client-Server.

Pada jaringan peer to peer, setiap komputer yang terhubung ke jaringan dapat bertindak baik sebagai workstation maupun server. Sedangkan pada jaringan Client-Server, hanya satu komputer yang bertugas sebagai server dan komputer lain berperan sebagai workstation. Antara dua tipe jaringan tersebut masing-masing memiliki keunggulan dan kelemahan, di mana masing-masing akan dijelaskan.

LAN tersusun dari beberapa elemen dasar yang meliputi komponen hardware dan software, yaitu :

- a. Komponen Fisik
Personal Computer (PC), Network Interface Card (NIC), Kabel, Topologi Jaringan
- b. Komponen Software
Sistem Operasi Jaringan, Network Adapter Driver, Protokol Jaringan.



5.3.2. Jaringan Peer To Peer

Peer To Peer adalah sebuah aplikasi yang menghandle resource dari sejumlah autonomous participant atau user yang terkoneksi secara mandiri, artinya user dapat mengakses dirinya sesuai dengan keinginannya, tidak terikat oleh struktur jaringan secara fisik. Peer-to-peer menjadi sebuah alternatif aplikasi untuk mencari resource tertentu yang tidak ada di website ataupun alternatif untuk berbagi resouce tanpa sebuah web server yang harganya masih tergolong mahal. Bila ditinjau dari peran server di kedua tipe jaringan tersebut, maka server di jaringan tipe peer to peer diistilahkan non-dedicated server, karena server tidak berperan sebagai server murni melainkan sekaligus dapat berperan sebagai workstation.

→ Keunggulan

1. Antar komputer dalam jaringan dapat saling berbagi-pakai fasilitas yang dimilikinya seperti : harddisk, drive, fax/modem, printer.
2. Biaya operasional relatif lebih murah dibandingkan dengan tipe jaringan client-server, salah satunya karena tidak memerlukan adanya server yang memiliki kemampuan khusus untuk mengorganisasikan dan menyediakan fasilitas jaringan.
3. Kelangsungan kerja jaringan tidak tergantung pada satu server. Sehingga bila salah satu komputer/peer mati atau rusak, jaringan secara keseluruhan tidak akan mengalami gangguan.

→ Kelemahan

1. Troubleshooting jaringan relatif lebih sulit, karena pada jaringan tipe peer to peer setiap komputer dimungkinkan untuk terlibat dalam komunikasi yang ada. Di jaringan client-server, komunikasi adalah antara server dengan workstation.
2. Unjuk kerja lebih rendah dibandingkan dengan jaringan client-server, karena setiap komputer/peer disamping harus mengelola pemakaian fasilitas jaringan juga harus mengelola pekerjaan atau aplikasi sendiri.
3. Sistem keamanan jaringan ditentukan oleh masing-masing user dengan mengatur keamanan masing-masing fasilitas yang dimiliki.

Karena data jaringan tersebar di masing-masing komputer dalam jaringan, maka backup harus dilakukan oleh masing-masing komputer tersebut.

5.3.3. Jaringan Client – Server

Server adalah komputer yang menyediakan fasilitas bagi komputer-komputer lain didalam jaringan dan client adalah komputer-komputer yang menerima atau menggunakan fasilitas yang disediakan oleh server. Server di jaringan tipe client-server disebut dengan Dedicated Server karena murni berperan sebagai server yang menyediakan fasilitas



kepada workstation dan server tersebut tidak dapat berperan sebagai workstation.

→ Keunggulan

- 1 Kecepatan akses lebih tinggi karena penyediaan fasilitas jaringan dan pengelolaannya dilakukan secara khusus oleh satu komputer (server) yang tidak dibebani dengan tugas lain sebagai workstation.
- 2 Sistem keamanan dan administrasi jaringan lebih baik, karena terdapat seorang pemakai yang bertugas sebagai administrator jaringan, yang mengelola administrasi dan sistem keamanan jaringan.
- 3 Sistem backup data lebih baik, karena pada jaringan client-server backup dilakukan terpusat di server, yang akan membackup seluruh data yang digunakan di dalam jaringan.

→ Kelemahan

- 1 Biaya operasional relatif lebih mahal.
- 2 Diperlukan adanya satu komputer khusus yang berkemampuan lebih untuk ditugaskan sebagai server.
- 3 Kelangsungan jaringan sangat tergantung pada server. Bila server mengalami gangguan maka secara keseluruhan jaringan akan terganggu.

5.3.4. Konfigurasi Jaringan pada Windows 10

Untuk menggunakan fasilitas dan komponen jaringan yang ada pada Windows 10, harus terlebih dahulu menginstall dan mengkonfigurasinya. Pada bagian ini akan mendiskusikan bagaimana cara untuk menginstall dan mengkonfigurasi komponen-komponen jaringan. Proses pertama memberi nama komputer (unik) untuk memastikan bahwa komputer yang dipakai dapat dikenali oleh pemakai komputer lain yang terhubung di dalam jaringan komputer. Menginstall hardware, software untuk membuat komputer terhubung ke dalam jaringan, dan kemudian mengkonfigurasi protokol yang digunakan komputer untuk “berkomunikasi” dengan komputer lain.

→ Konfigurasi ini bertujuan untuk :

- 1 Mengidentifikasi komputer di dalam jaringan
Berikan nama komputer yang unik untuk mengidentifikasi komputer yang akan digunakan agar dapat “berkomunikasi” dengan komputer lain di dalam jaringan.
- 2 Memberi nama komputer
Komputer dengan sistem operasi Windows 10 di dalam jaringan komputer harus menggunakan nama yang unik untuk menghindari adanya tumpang-tindih (konflik) dengan komputer lain.

Note : Pemberian nama computer bisa mencapai 15 karakter dan tidak disertai dengan spasi

3. Computer Description

Anda bisa saja mengabaikan deskripsi komputer yang dipakai. Deskripsi komputer akan terlihat oleh orang lain pada saat browsing di jaringan, bila Anda ingin mengisi computer descriptor, ikuti prosedur dibawah sekaligus untuk memberikan nama untuk komputer. Saat proses installasi sistem operasi, entah itu Windows 10 dan Windows 7, user memungkinkan untuk memberi nama pada komputer mereka. Semua orang sudah pasti pernah melakukan ini. Tapi untuk Windows 10, user tidak akan diminta untuk memberi nama pada komputer mereka.

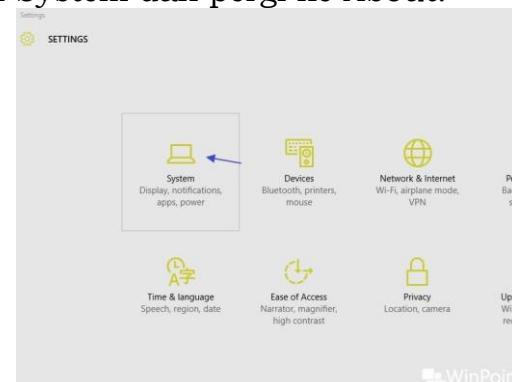
Mungkin ini diperlukan untuk mempercepat proses installasi, Windows 10 secara random akan memberi nama pada komputer anda, menggunakan nama anda sendiri. Pada versi Windows sebelumnya, anda bisa mengganti nama di System Properties>Control Panel. Di Windows 10 pun cara ini masih bisa digunakan. Sistem operasi terbaru buatan Microsoft ini juga memiliki aplikasi Settings, tempat pengaturan yang berbeda dengan Control Panel. Sebagian besar pengaturan di aplikasi Settings diperuntukkan untuk Windows 10.

1. Buka aplikasi Settings dengan klik Start Menu dan klik Settings, atau gunakan shortcut keyboard Win+I untuk membuka aplikasi Settings.

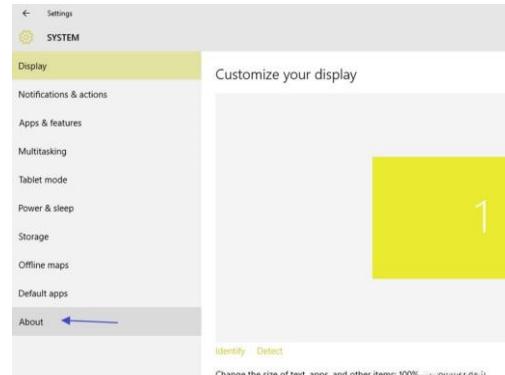


Gambar 5.1 tampilan Windows 10

2. Setelah itu klik System dan pergi ke About.

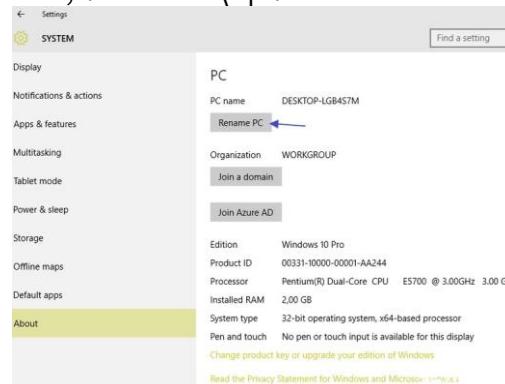


Gambar 5.2 tampilan settings



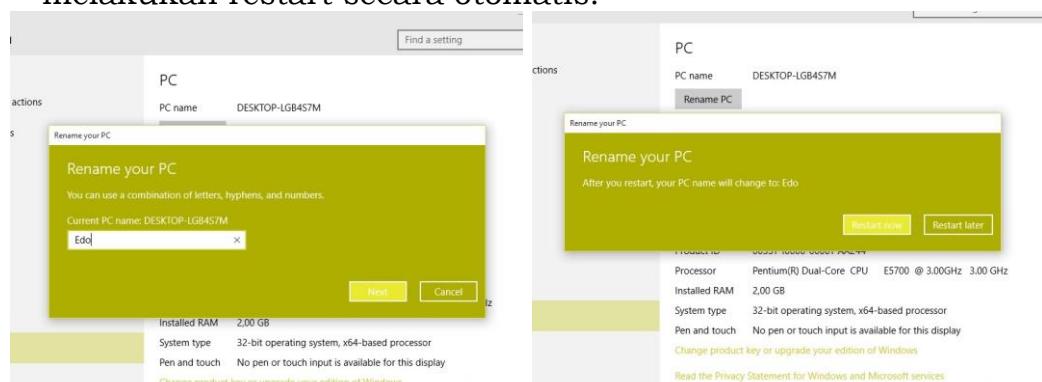
Gambar 5.3 tampilan about

3. Ketika sudah di About maka tampilannya seperti di System info di Control Panel. Kamu akan melihat nama komputer, versi sistem operasi, arsitektur, processor, memori RAM dan informasi lainnya. Untuk merubah nama komputer di Windows 10, kamu tinggal klik Rename PC. Setelah itu masukkan nama komputer yang kamu inginkan, hindari penggunaan karakter khusus seperti < > ; : " * + = \ | ?



Gambar 5.4 tampilan about

4. Lalu setelah memasukan nama klik Next, komputer akan melakukan restart secara otomatis.



Gambar 5.5 rename your pc

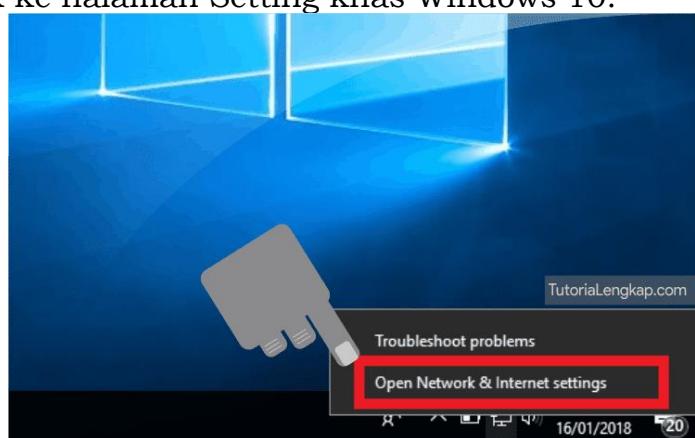
Catatan: Jika kamu upgrade ke Windows 10 dari versi sebelumnya, secara otomatis nama komputer akan menggunakan nama komputer pada versi Windows sebelumnya.

5.3.4.1. Mengkonfigurasi TCP/IP

Seperti yang kita tau bahwa untuk melakukan konfigurasi atau setting IP Address pada windows 10 ada sedikit perbedaan dimana biasanya pada windows 7, ketika anda melakukan klik kanan pada icon jaringan pada taskbar dan kita memilih option Open network & internet settings maka secara langsung anda akan dibawa masuk ke control panel.

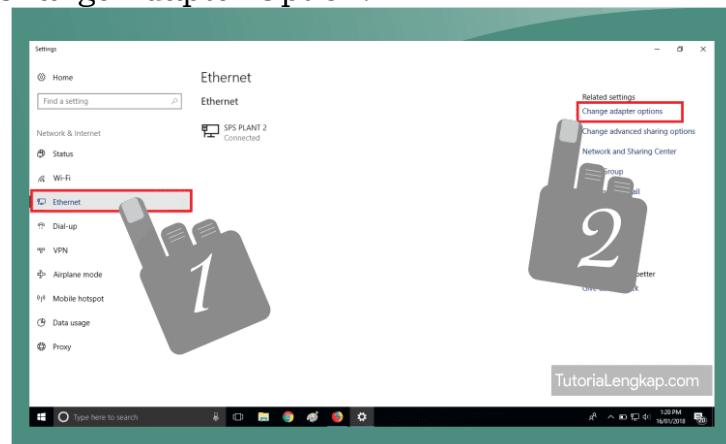
Namun berbeda dengan system operasi windows 10, ketika anda melakukan klik kanan pada icon jaringan pada taskbar dan memilih pilihan open network & internet settings maka anda akan dibawa masuk ke halaman Setting dengan tampilan baru windows 10.

1. Klik kanan pada icon jaringan pada taskbar windows 10 milik anda, kemudian pilih Open Network & Internet Settings, sehingga anda akan masuk ke halaman Setting khas Windows 10.



Gambar 5.6 Open Network & Internet Settings

2. Pada halaman settings sebalah kiri, silahkan pilih Wi-Fi jika anda ingin melakukan konfigurasi IP Address pada koneksi jaringan Wi-fi, atau pilih Ethernet jika anda ingin melakukan konfigurasi IP Address pada koneksi jaringan Ethernet atau LAN dengan menggunakan kabel sebagai koneksi ke jaringan. (Sebagai contoh disini admin akan melakukan konfigurasi pada jaringan Ethernet maka ang admin pilih adalah Ethernet) Kemudian pada halaman sebelah kanan, silahkan anda pilih Change Adapter Option.

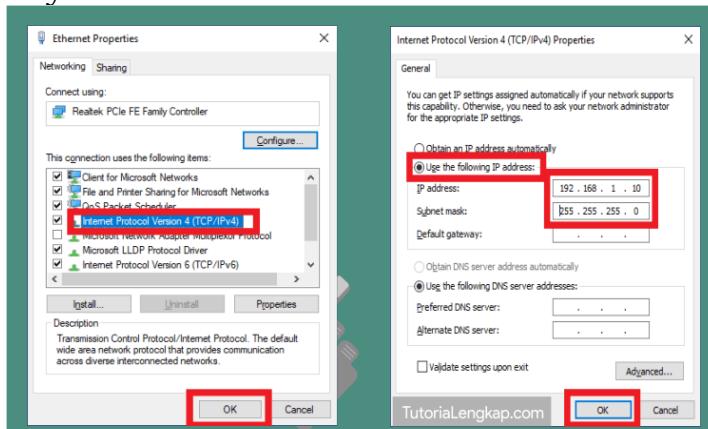


Gambar 5.7 jaringan Ethernet



3. Langkah selanjutnya, anda akan masuk ke halaman Network Connection, Klik kanan pada icon ethernet jika ingin melakukan konfigurasi pada ethernet, atau klik kanan pada icon wi-fi jika anda ingin melakukan konfigurasi pada jaringan wi-fi, kemudian pilih properties.
4. Langkah berikutnya, kita telah masuk ke halaman Ethernet Properties, nah untuk melakukan konfigurasi atau setting IP Address secara manual (Static IP Address) silahkan anda double click pada pilihan Internet Protocol Version 4 (TPC/IPv4).
5. Kemudian pada tahap berikutnya, kita akan masuk ke halaman Internet Protocol Version 4 (TPC/IPv4) Properties, silahkan masukkan IP Address sesuai dengan yang anda inginkan (sesuaikan dengan kelas IP yang digunakan pada jaringan yang ingin anda sambung). Jika anda telah selesai mengisikan IP Address, subnet mask, Default Gateway dan juga DNS Server, silahkan klik pada tombol OK untuk menerapkan perubahan
6. Klik kanan pada Internet Protocol (TCP/IP), kemudian pilih Properties.
7. Klik pada Use the following IP address, kemudian isikan :
 - IP address komputer Anda (ingat harus unik, tak boleh sama dalam satu jaringan)
 - Subnet mask
 - Default gateway (harus sama dalam satu jaringan)
8. Klik pada Use the following DNS server address, kemudian isikan
 - Preferred DNS server (alamat yang menghubungkan jaringan Anda dengan jaringan server yang terhubung ke internet)
 - Alternate DNS server (pilihan alamat lain yang menghubungkan jaringan Anda dengan jaringan server yang terhubung ke internet)

Pengisian DNS server tergantung dari alamat yang diberikan oleh layanan koneksi internet (ISP) Anda. Anda akan diberi alamat ini oleh ISP. Jika alamat DNS server lebih dari dua Anda harus mengisikan dengan klik tombol Advanced, kemudian klik DNS dan pilih Add untuk menambahkannya.



Gambar 5.8 Tampilan Local Area Properties & Internet Protokol Properties

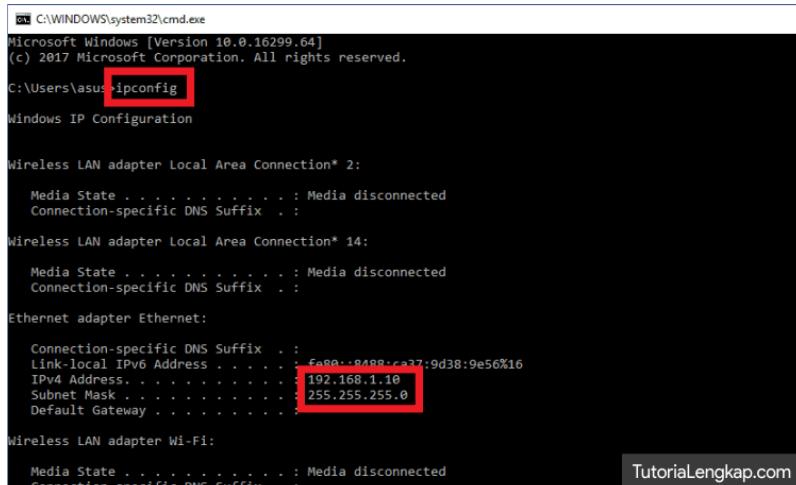
Cara melakukan pengecekan IP Address melalui CMD (command prompt)

Tekan tombol Windows atau start dan tombol R secara bersamaan pada tombol keyboard computer, sehingga terbuka halaman RUN, kemudian ketik CMD, lalu tekan tombol Enter pada keyboard.

how to setting static ip address windows 7, 8 and windows 10, cara konfigurasi ip address manual, network configuration on windows, how to setting LAN, cara setting jaringan windows, network setup on windows easily

Jika halaman cmd telah terbuka, silahkan ketik ipconfig pada halaman cmd tersebut lalu tekan tombol enter pada keyboard.

Setelah anda menekan tombol Enter pada keyboard, maka pada halaman cmd akan menampilkan informasi IP Address beserta subnet mask dan juga default gateway yang telah terpasang atau tersetting pada computer anda.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\asus>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 14:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . . . . . : F880-8488-ca27-9d38:9e56%16
  Link-local IPv6 Address . . . . . : fe80::8488:ca27%9d38:9e56%16
  IPv4 Address. . . . . : 192.168.1.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
```

Gambar 5.9 CMD (command prompt)

5.3.4.2. Konfigurasi Jaringan Peer To Peer

Cara mengkonfigurasi Jaringan Peer To Peer tidak jauh berbeda dengan penjelasan konfigurasi pada Windows 10, agar menghasilkan jaringan seperti dibawah ini maka langkah – langkah yang perlu dilakukan adalah sebagai berikut :

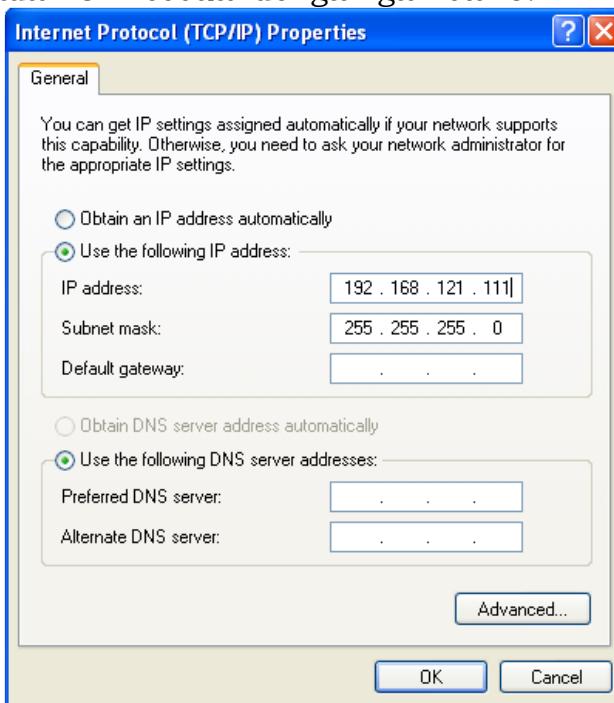


Gambar 5.10 Bentuk Jaringan Peer To Peer

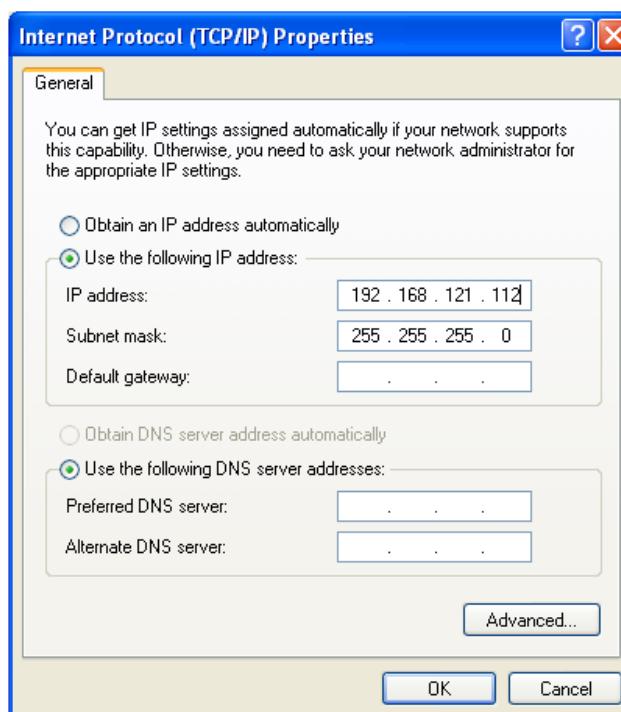
1. Diperlukan 2 buah PC, pada PC pertama kita beri nama PC A dan PC kedua kita beri nama PC B (Lihat Konfigurasi Pada Windows 10, Tentang Memberi Nama Komputer)



2. Kemudian baik pada PC A maupun PC B dihubung dengan menggunakan kabel Cross Over, setelah dihubungankan, pada masing-masing PC dilakukan konfigurasi yang sama seperti Konfigurasi Jaringan Pada Windows 10
3. Kemudian pada saat melakukan konfigurasi TCP/IP yang perlu dilakukan adalah untuk PC A diberikan IP Address sesuai gambar 6.6 dan pada PC B sesuai dengan gambar 6.7

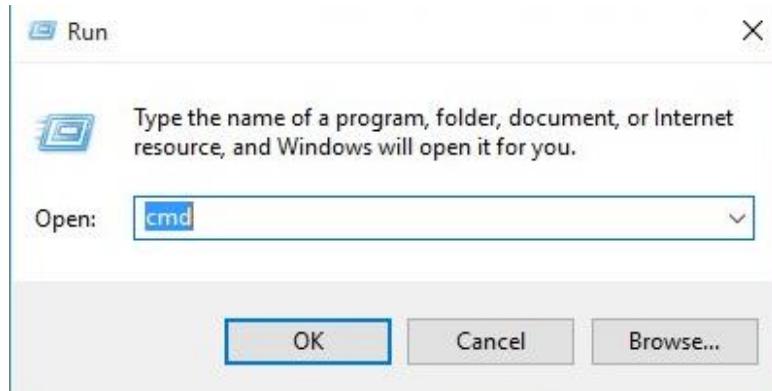


Gambar 5.11 Internet Protokol Properties Pada PC A



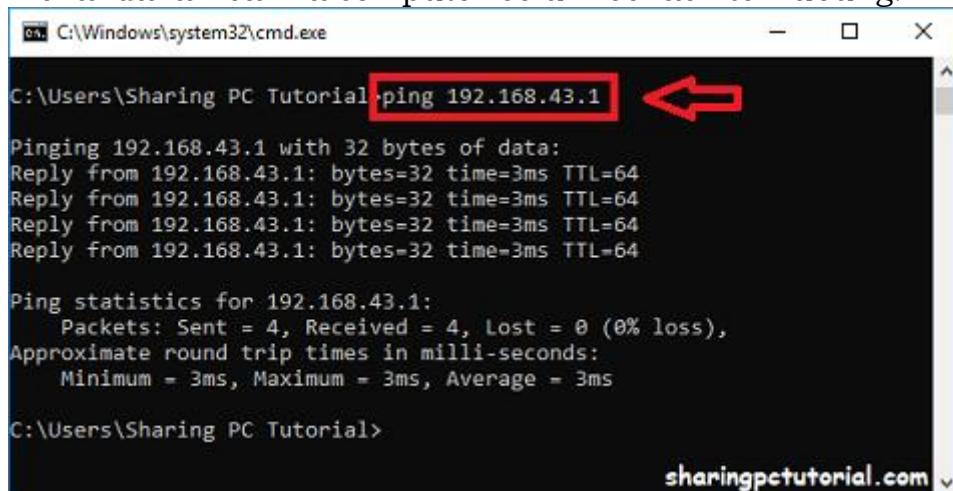
Gambar 5.12 Internet Protokol Properties Pada PC B

4. Setelah memberi IP Address pada masing-masing PC, langkah terakhir adalah memastikan apakah kedua komputer dapat terhubung / berkomunikasi satu sama lain, dengan cara PING <nomor IP Address> pada salah satu PC, contoh kita melakukan ping pada PC A yang ditujukan ke PC B
5. Caranya dengan klik Start, kemudian pilih Run, setelah muncul tampilan Run ketikan cmd klik OK.



Gambar 5.12 Tampilan Run

6. Setelah ditampilkan layar cmd, ketik PING dengan format ping <spasi> nomor IP Address PC tujuan, jika hasil ping menunjukkan Reply itu menandakan bahwa komputer ini terhubung jika menunjukkan Time Out atau Destination Host Unreachable menandakan bahwa computer belum berhasil terhubung.



```
C:\Windows\system32\cmd.exe
C:\Users\Sharing PC Tutorial>ping 192.168.43.1 ←
Pinging 192.168.43.1 with 32 bytes of data:
Reply from 192.168.43.1: bytes=32 time=3ms TTL=64

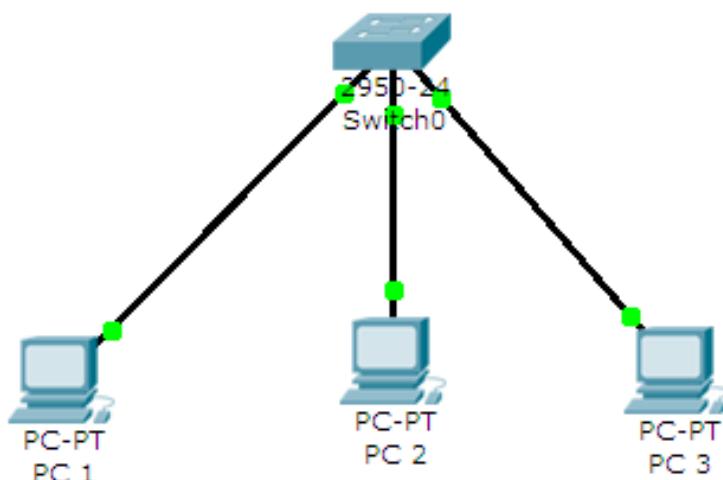
Ping statistics for 192.168.43.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Users\Sharing PC Tutorial>
```

Gambar 5.13 Tampilan cmd

5.3.4.3. Konfigurasi Jaringan Client – Server

Cara mengkonfigurasi Jaringan Client - Server tidak jauh berbeda dengan Jaringan Peer To Peer perbedaannya adalah dibutuhkannya lagi perangkat pendukung jaringan yaitu Switch/Hub, agar menghasilkan jaringan seperti dibawah ini maka langkah – langkah yang perlu dilakukan adalah sebagai berikut :



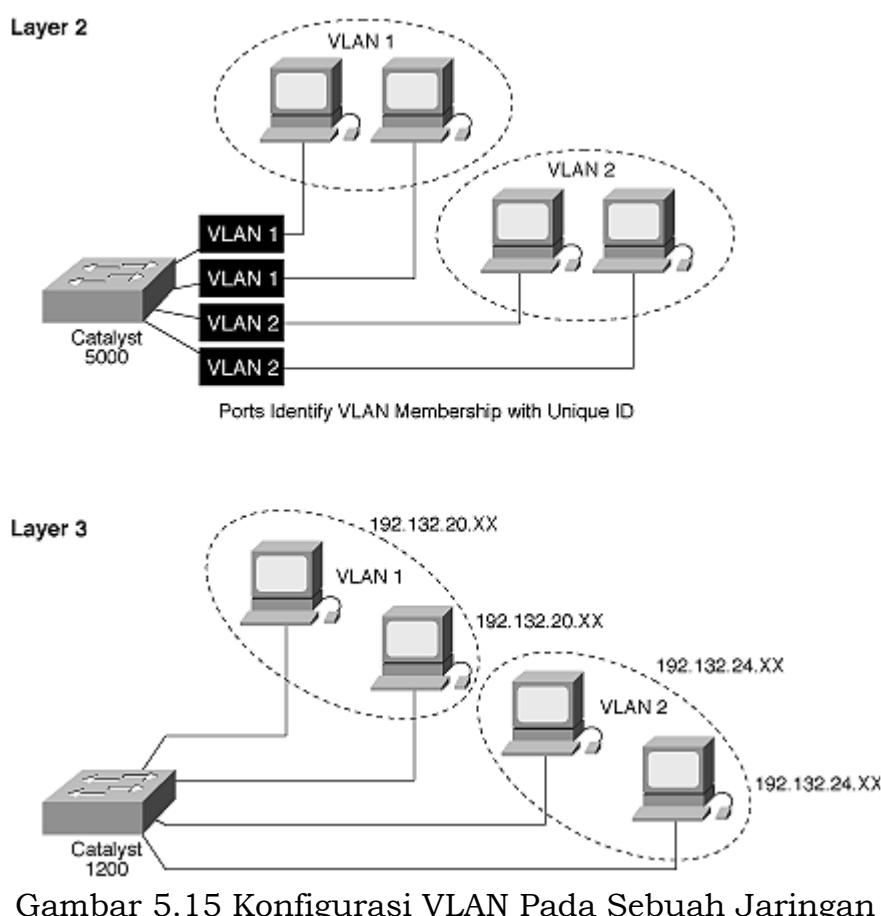
Gambar 5.14 Bentuk Jaringan Client – Server

1. Jaringan Client – Server ini terhubungan dengan menggunakan jenis kabel Straight Trough
2. Langkah – langkah konfigurasi pada jaringan ini hampir sama dengan konfigurasi pada jaringan Peer To Peer perbedaan terletak pada saat melakukan pengaturan TCP/IP atau pemberian IP Address pada masing-masing PC dengan ketentuan sebagai berikut
 - a. PC 1 diberikan IP Address 192.168.121.16 dengan Subnet Mask 255.255.255.0
 - b. PC 2 diberikan IP Address 192.168.121.17 dengan Subnet Mask 255.255.255.0
 - c. Dan terakhir pada PC 3 diberikan IP Address 192.168.121.18 dengan Subnet Mask 255.255.255.0
3. Setelah memberi IP Address pada masing-masing PC, langkah terakhir adalah memastikan apakah kedua komputer dapat terhubung / berkomunikasi satu sama lain, dengan cara PING <nomor IP Address> pada salah satu PC, ping dilakukan pada masing-masing PC, untuk mengetahui apakah masing-masing PC dapat terhubung satu sama lain.
4. Caranya dengan klik Start, kemudian pilih Run, setelah muncul tampilan Run ketikan cmd klik OK.

Setelah ditampilkan layar cmd, ketik PING dengan format ping <spasi> nomor IP Address PC tujuan, jika hasil ping menunjukan Reply itu menandakan bahwa komputer ini terhubung jika menunjukan Time Out atau Destination Host Unreacable menandakan bahwa computer belum berhasil terhubung.

5.3.5. Pengenalan VLAN (Virtual Local Area Network)

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN , hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi workstation seperti pada gambar dibawah ini



Gambar 5.15 Konfigurasi VLAN Pada Sebuah Jaringan



5.3.5.1. Bagaimana VLAN Bekerja

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik menggunakan port, MAC addresses dsb. Semua informasi yang mengandung penandaan/pengalaman suatu vlan (tagging) di simpan dalam suatu database (tabel), jika penandaannya berdasarkan port yang digunakan maka database harus mengindikasikan port-port yang digunakan oleh VLAN. Untuk mengaturnya maka biasanya digunakan switch/bridge yang manageable atau yang bisa di atur. Switch/bridge inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua switch/bridge memiliki informasi yang sama.

Switch akan menentukan kemana data-data akan diteruskan dan sebagainya. Atau dapat pula digunakan suatu software pengalaman (bridging software) yang berfungsi mencatat/menandai suatu VLAN beserta workstation yang didalamnya.untuk menghubungkan antar VLAN dibutuhkan router.

5.3.5.2. Tipe - Tipe Vlan

Keanggotaan dalam suatu VLAN dapat di klasifikasikan berdasarkan port yang di gunakan , MAC address, tipe protokol.

1. Berdasarkan Port

Keanggotaan pada suatu VLAN dapat di dasarkan pada port yang di gunakan oleh VLAN tersebut. Sebagai contoh, pada bridge/switch dengan 4 port, port 1, 2, dan 4 merupakan VLAN 1 sedang port 3 dimiliki oleh VLAN 2, lihat tabel :

Tabel 5.1 Port dan VLAN

Port	1	2	3	4
VLAN	2	2	1	2

Kelemahan : user tidak bisa untuk berpindah pindah, apabila harus berpindah maka Network administrator harus mengkonfigurasikan ulang.

2. Berdasarkan MAC Address

Keanggotaan suatu VLAN didasarkan pada MAC address dari setiap workstation/komputer yang dimiliki oleh user. Switch mendekripsi/mencatat semua MAC address yang dimiliki oleh setiap Virtual LAN. MAC address merupakan suatu bagian yang dimiliki oleh NIC (Network Interface Card) disetiap workstation.

Kelebihan : Apabila user berpindah pindah maka dia akan tetap terkonfigurasi sebagai anggota dari VLAN tersebut

Kekurangan : Bahwa setiap mesin harus di konfigurasikan secara manual , dan untuk jaringan yang memiliki ratusan workstation maka tipe ini kurang efisien untuk dilakukan.



Tabel 5.2 MAC address dan VLAN

MAC Address	132516617738	272389579355	536666337777	24444125556
VLAN	1	2	2	1

3. Berdasarkan tipe protokol yang digunakan
Keanggotaan VLAN juga bisa berdasarkan protocol yang digunakan, lihat table

Tabel 5.3 Protokol dan VLAN

Protokol	IP	IPX
VLAN	1	2

4. Berdasarkan Alamat Subnet IP
Subnet IP address pada suatu jaringan juga dapat digunakan untuk mengklasifikasi suatu VLAN

Tabel 5.4 IP Subnet dan VLAN

IP Subnet	22.3.24	46.20.45
VLAN	1	2

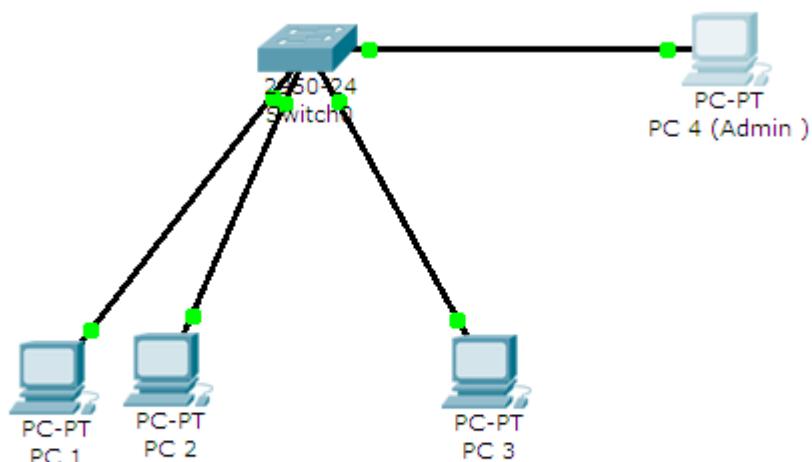
Konfigurasi ini tidak berhubungan dengan routing pada jaringan dan juga tidak mempermasalahkan fungsi router. IP address digunakan untuk memetakan keanggotaan VLAN.

Keuntungannya : seorang user tidak perlu mengkonfigurasikan ulang alamatnya di jaringan apabila berpindah tempat, hanya saja karena bekerja di layer yang lebih tinggi maka akan sedikit lebih lambat untuk meneruskan paket di banding menggunakan MAC addresses.

5. Berdasarkan aplikasi atau kombinasi lain
Sangat dimungkinkan untuk menentukan suatu VLAN berdasarkan aplikasi yang dijalankan, atau kombinasi dari semua tipe di atas untuk diterapkan pada suatu jaringan. Misalkan: aplikasi FTP (file transfer protocol) hanya bias digunakan oleh VLAN 1 dan Telnet hanya bisa digunakan pada VLAN 2.

5.3.5.3. Konfigurasi Jaringan VLAN

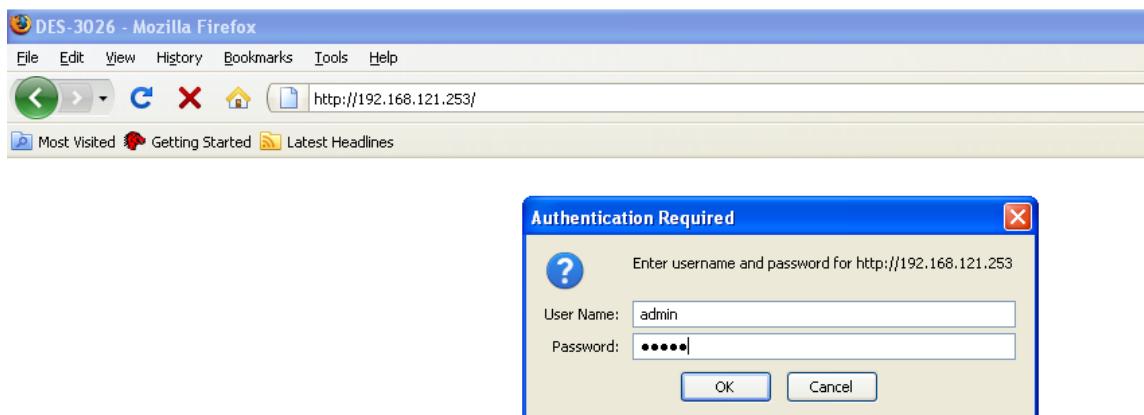
Cara mengkonfigurasi Jaringan VLAN tidak jauh berbeda dengan Jaringan Client – Server karena sama-sama menggunakan perangkat pendukung jaringan Switch/Hub, perbedaanya hanya terletak pada konfigurasi pengaturan VLAN nantinya, cara mengkonfigurasi VLAN dengan menggunakan Switch D-Link DCS - 3026. Tidak semua switch mempunyai fasilitas VLAN hanya switch manageable saja yang memiliki fasilitas ini, salah satunya yaitu Switch D-Link DCS - 3026, agar menghasilkan jaringan seperti dibawah ini maka langkah – langkah yang perlu dilakukan adalah sebagai berikut :



Gambar 5.16 Bentuk Jaringan VLAN

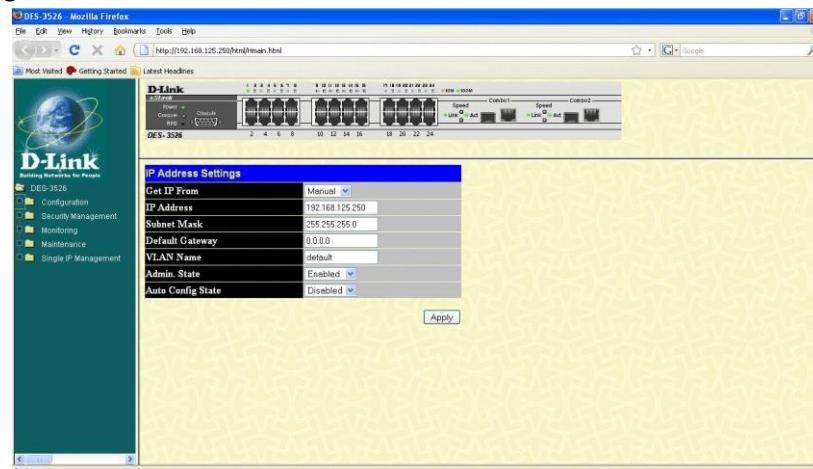
1. Jaringan VLAN ini terhubungan dengan menggunakan jenis kabel Straight Trough dengan ketentuan untuk masing-masing PC sebagai berikut :
 - a. PC 1 dipasang ke Switch pada Port 1
 - b. PC 2 dipasang ke Switch pada Port 2
 - c. PC 3 dipasang ke Switch pada Port 3
 - d. PC 4 dipasang ke Switch pada Port 4
2. Langkah – langkah konfigurasi pada jaringan ini hampir sama dengan konfigurasi pada jaringan Client – Server perbedaan terletak pada saat melakukan konfigurasi VLAN menggunakan GUI (Graphic User Interface) sebelum sampai pada langkah itu langkah selanjut adalah melakukan pengaturan TCP/IP atau pemberian IP Address pada masing-masing PC dengan ketentuan sebagai berikut
 - a. PC 1 diberikan IP Address 192.168.121.16 dengan Subnet Mask 255.255.255.0
 - b. PC 2 diberikan IP Address 192.168.121.17 dengan Subnet Mask 255.255.255.0
 - c. PC 3 diberikan IP Address 192.168.121.11 dengan Subnet Mask 255.255.255.0
 - d. Dan terakhir pada PC 4 diberikan IP Address 192.168.121.12 dengan Subnet Mask 255.255.255.0

3. Setelah memberi IP Address pada masing-masing PC, langkah terakhir adalah memastikan apakah kedua komputer dapat terhubung / berkomunikasi satu sama lain, dengan cara PING <nomor IP Address> pada salah satu PC, ping dilakukan pada masing-masing PC, untuk mengetahui apakah masing-masing PC dapat terhubung satu sama lain.
4. Setelah semua PC berhasil terhubung dengan baik, maka langkah selanjutnya konfigurasi VLAN menggunakan GUI, pada gambar 6.11 terdapat 4 buah PC, 3 buah PC sebagai Client dan 1 PC digunakan sebagai Admin, pada PC yang digunakan sebagai Admin, akan kita lakukan konfigurasi dari PC tersebut, PC yang digunakan sebagai Admin adalah PC 4,
5. Konfigurasi VLAN pada PC 4 klik web browser(mozilla/IE) yang ada pada PC, setelah ditampilkan browser ketikan IP Address Switch yang kita gunakan pada alamat URL, dengan IP Address 192.168.125.250 (Cek IP Address Switch Pada Switch)
6. Kemudian akan muncul tampilan Authentication Required, masukan Usernamanya admin dan Passwordnya admin klik OK



Gambar 5.17 Tampilan Authentication Required Pada Web Browser

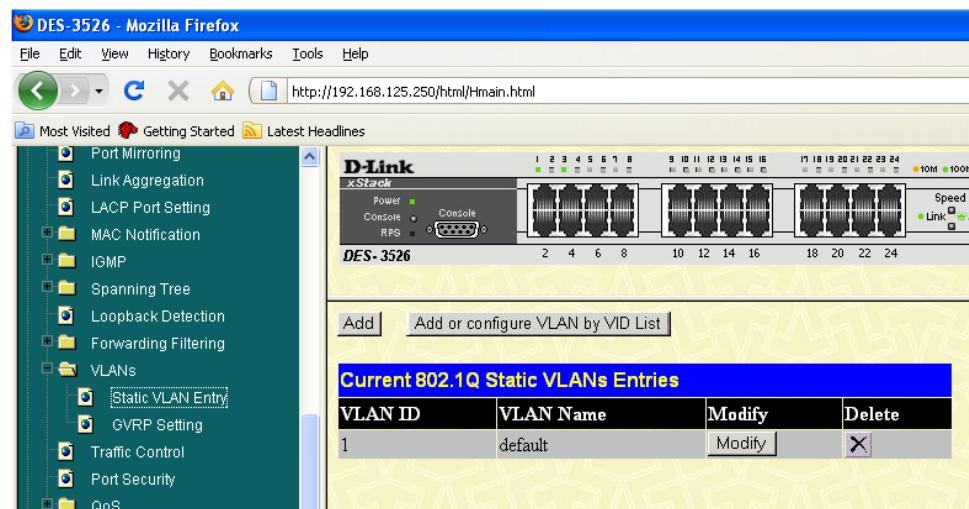
7. Kemudian ditampilkan tampilan awal dari Switch D-Link DES - 3526



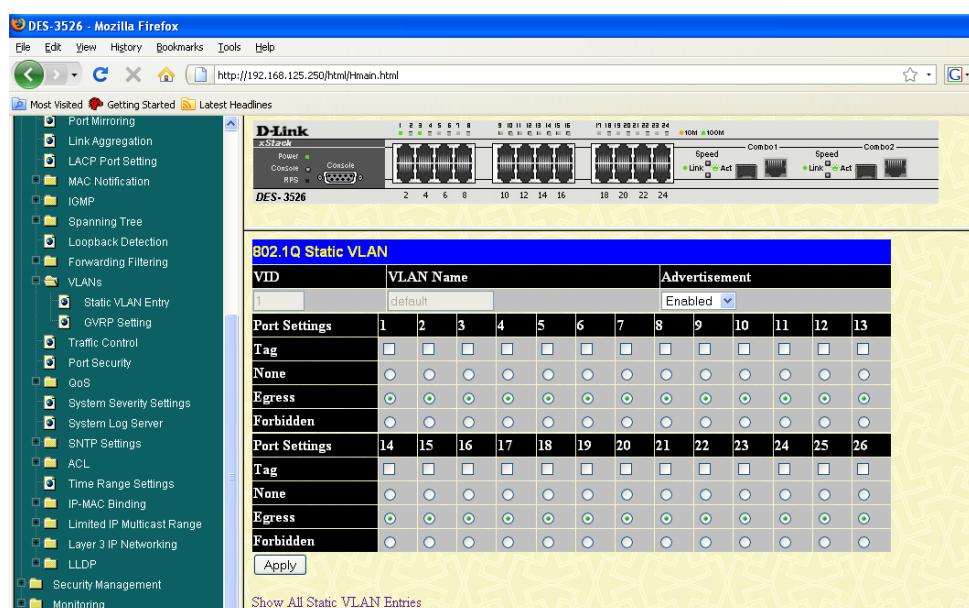
Gambar 5.18 Tampilan Halaman Depan Web Switch D-Link DES-3526



8. Klik Tanda + pada Configuration yang terdapat di Menu Pilihan Sebelah Kiri, kemudian pilih Submenu dari VLAN's yaitu klik Static VLAN Entry
9. Kemudian ditampilkan halaman submenu yaitu Static VLAN Entry. Setelah itu klik Modify pada VLAN Name Default
10. Kemudian akan ditampilkan halaman pengaturan pada VLAN Name Default, pada VLAN ini akan didaftarkan anggota LAN yang ingin diberi VLAN, perlu di ingin yang didaftarkan hanya PC Client sedang PC Admin tidak didaftarkan dengan cara klik TAG dan NONE pada Port yang terhubung dengan masing-masing PC Client yang akan didaftarkan. Pada konfigurasi awal telah ditentukan Port yang digunakan adalah Port 1 – 4 tapi yang kita gunakan hanya Port 2-4 karena pada Port 1 merupakan Port PC Admin, kemudian klik OK

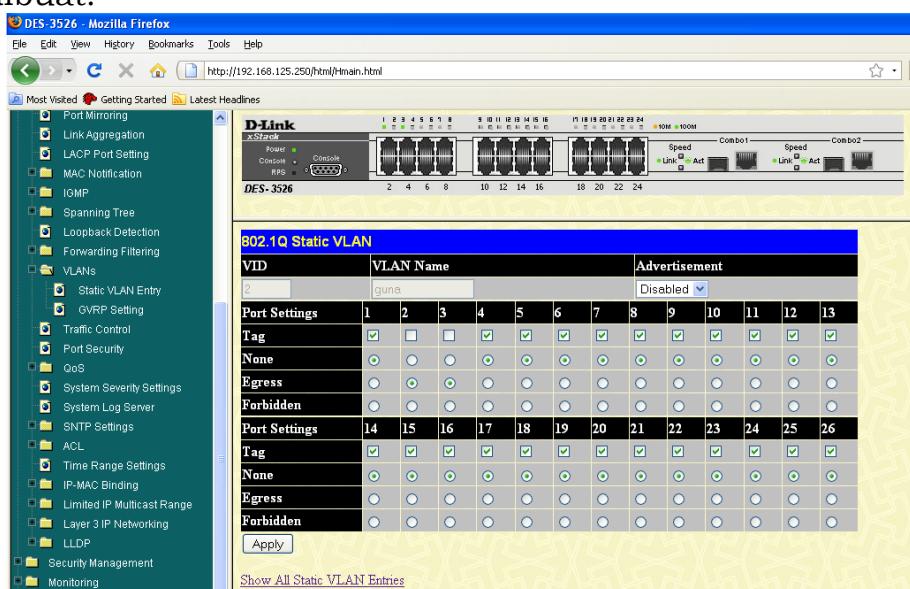


Gambar 5.19 Tampilan Halaman Submenu Static VLAN Entry



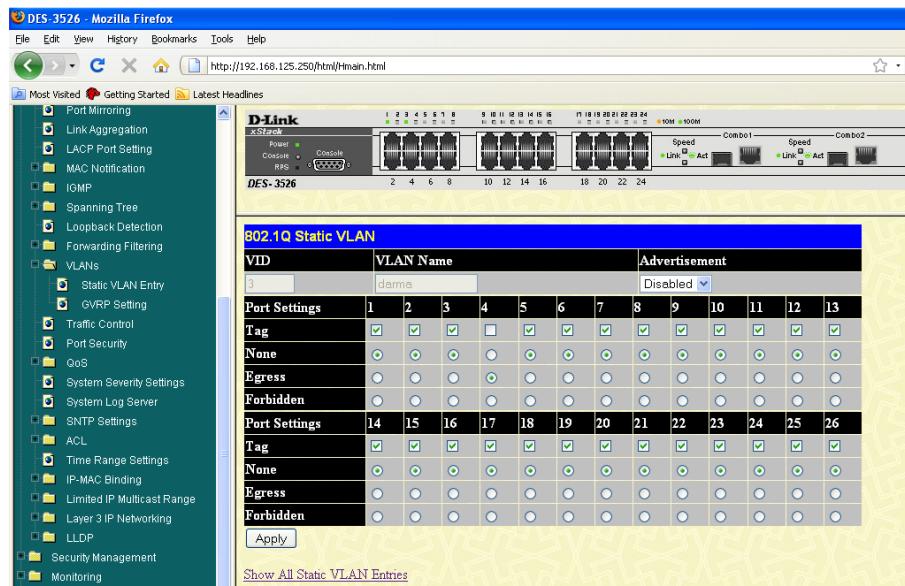
Gambar 5.20 Tampilan Pengaturan VLAN Name Default

11. Klik Show All Static VLAN Entry yang terdapat pada halaman pengaturan VLAN Name Default
12. Kemudian ditampilkan tampilan halaman submenu Static VLAN Entry, langkah selanjutnya adalah membuat VLAN dimana pada gambar 6.11 terdapat 2 buah VLAN, yaitu GUNA dan DARMA
13. Cara untuk membuat VLAN baru dengan klik ADD pada Kolom ADD New Entry VLAN. Kemudian ditampilkan konfigurasi VLAN baru yang akan dibuat, Masukan VLAN ID nya 2 dan VLAN Name nya Guna.
14. Setelah itu daftarkan anggota PC Client yang terdaftar pada VLAN Guna, pada gambar 5.21
- 6.11 yaitu PC 2 dan PC 3, maka pada Port 2 dan Port 3 klik Egress, klik OK, kemudian akan muncul konfirmasi bahwa VLAN Success dibuat.



Gambar 5.21 Tampilan Pengaturan VLAN Name GUNA

15. Klik Show All Static VLAN Entry yang terdapat pada halaman pengaturan VLAN Name GUNA
16. Kemudian ditampilkan tampilan halaman submenu Static VLAN Entry, langkah selanjutnya adalah membuat VLAN DARMA
17. Cara untuk membuat VLAN DARMA sama dengan membuat VLAN GUNA, masukan VLAN ID 3 dan VLAN Name Darma
18. Setelah itu daftarkan anggota PC Client yang terdaftar pada VLAN Guna, pada gambar 5.22
- 6.12 yaitu PC 4 maka pada Port 4 klik Egress, klik OK, kemudian akan muncul konfirmasi bahwa VLAN Success dibuat.



Gambar 5.22 Tampilan Pengaturan VLAN Name DARMA

19. Langkah terakhir memastikan apakan VLAN yang kita buat berhasil apa tidak dengan melakukan PING pada masing-masing PC, VLAN dikatakan berhasil apabila PC dapat terhubung hanya dengan PC yang memiliki VLAN Name sama dengan PC yang yang dituju dan tidak ada berkomunikasi/terhubung dengan PC yang tidak memiliki VLAN Name sama dengan dituju atau tidak terdapat VLAN pada PC dituju.

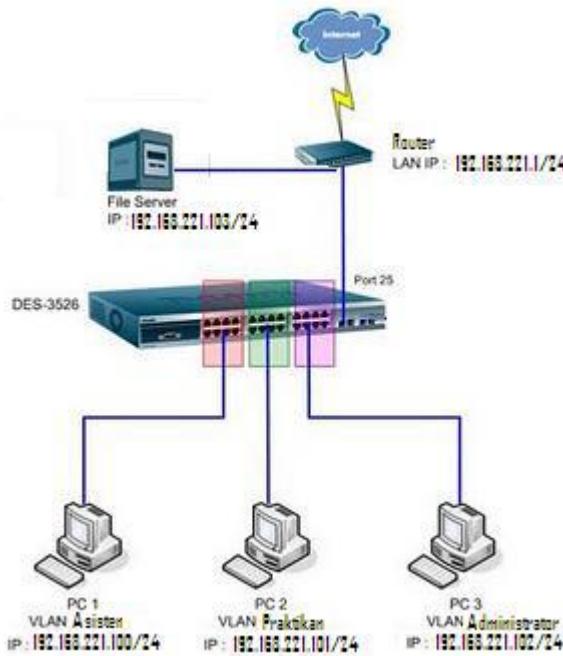
5.3.5.4. Konfigurasi Jaringan Asymmetric VLAN & Port Management

Asymmetric VLAN merupakan salah satu kelebihan yang diberikan oleh produk D-Link dalam mengatasi jaringan dengan mode VLAN supaya segmentasi antar port dalam pembagian IP serta routing lebih mudah serta mengijinkan sebuah port menjadi anggota 1 VLAN atau lebih.

Terdapat beberapa kelebihan yang diberikan oleh produk D-Link yakni switch D-Link xStack Managed Switch DES-3526 yang akan dilakukan percobaan menggunakan Asymmetric VLAN serta Port Bandwidth.

Port Bandwidth digunakan untuk melakukan pembatasan bandwidth terhadap PC yang terhubung pada port, dimana port tersebut sudah dikonfigurasikan dalam pembatasan bandwidth yang diinginkan. Beberapa kelebihan dari Asymmetric VLAN terdapat pada seri DES-3028/52 Series (DES- 3028/3028P/3052/3052P), DES-3500 Series (DES-3526/3526DC/3550) dan DES-3528/52 Series (DES-3528/3528P/3528DC/3552).

Gambar di 5.23 merupakan salah satu contoh topologi yang akan dikonfigurasikan menggunakan Asymmetric VLAN serta Port Bandwidth.

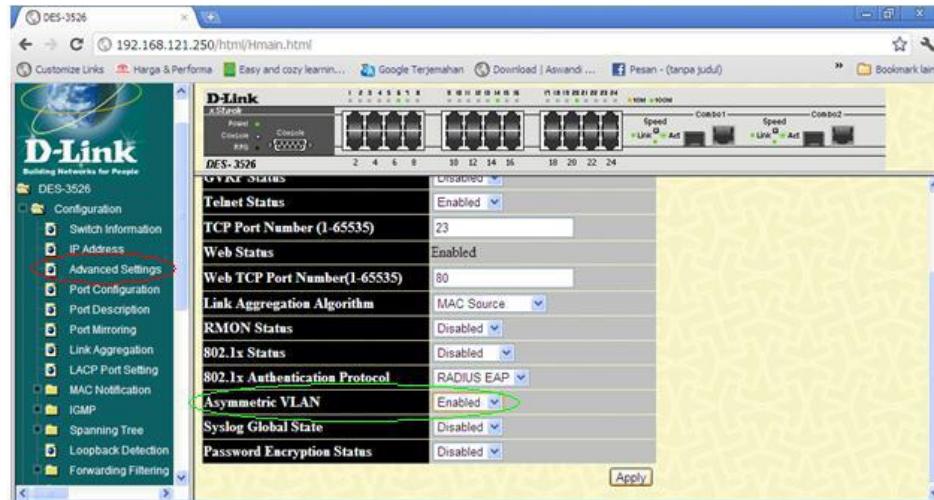


Gambar 5.23 Topologi Asymmetric VLAN & Port Management

Terdapat 3 buah PC yang akan disegmentasi antar port sehingga antar komputer tersebut tidak dapat saling akses namun 3 PC tersebut dapat akses ke internet serta dapat akses ke file server. Ke-3 PC tersebut akan mendapatkan IP secara otomatis (DHCP client) dari router yang telah diaktifkan DHCP servernya. Dengan menggunakan Switch D-Link xStack Managed Switch DES-3526, akan dilakukan pembagian port sebagai berikut :

- Port 1 – 8 untuk VLAN Asisten dengan batasan bandwidth 1 Mbps (Download & Upload)
- Port 9 – 16 untuk VLAN Praktikan dengan batasan bandwidth 2 Mbps (Download & Upload)
- Port 17 – 24 untuk VLAN Administrator dengan batasan bandwidth 3 Mbps (Download & Upload)
- Port 25 untuk router yang terhubung dengan internet dan file server

Pertama untuk mengkonfigurasikan Asymmetric VLAN menggunakan Switch D-Link xStack Managed Switch DES-3526 (kondisi sudah masuk pada web konfigurasi seperti pada percobaan VLAN sebelumnya), pilih menu “configuration” selanjutnya pilih kembali submenu “Advance Settings”. Pada layar kanan akan tampil lembaran konfigurasi yang dapat kita pilih dan isi, kemudian arahkan pada “Asymmetric VLAN” yang awal (default) konfigurasi besifat disabled diubah menjadi enabled. Setelah semua konfigurasi yang diinginkan untuk berubah maka kita harus menekan atau mengklik “Apply”. Hasil konfigurasi pengaktifan Asymmetric VLAN dapat dilihat seperti pada gambar 5.24



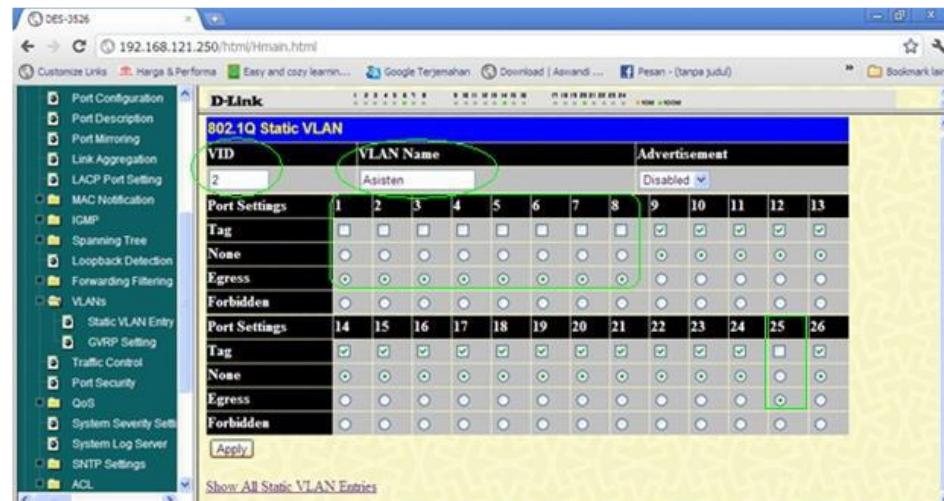
Gambar 5.24 Konfigurasi Awal Untuk Mengaktifkan Asymmetric VLAN

Langkah yang kedua, pilih submenu “VLANs” dari menu yang sama seperti pada langkah awal. Kemudian dari submenu tersebut pilih kembali “Static VLAN Entry”, maka akan tampil lembaran konfigurasi pada layar kanan komputer. Tekan atau klik “Add” untuk membuat dan mengkonfigurasikan port pada VLAN. Hasil yang akan di dapat setelah kita buat dan konfigurasi dari vlan maka akan tampil pada lembaran konfigurasi seperti pada gambar 5.25 Kita dapat mengkonfigurasikan kembali hasil dari VLAN yang sudah dibuat dengan menekan atau mengklik “Modify” pada pilihan VLAN ID serta VLAN Name yang ingin kita konfigurasikan.



Gambar 5.25 Hasil Pembuatan dan Konfigurasi Port Pada VLAN

Pada Gambar 5.25 – 5.27 menampilkan lembaran konfigurasi VLAN yang akan kita buat dengan mengisikan “VID” (selain dari angka 1 karena default), “VLAN Name”, serta memilih port yang akan dijadikan grup dari vlan tersebut (hilangkan tanda ceklist pada Tag dan ceklist pada Egress). Setelah semua konfigurasi yang diinginkan sudah diubah maka tekan atau klik “Apply”.



Gambar 5.25 Konfigurasi Grup VLAN (VID 2, VLAN Name Asisten, Port 1-8 & 25)

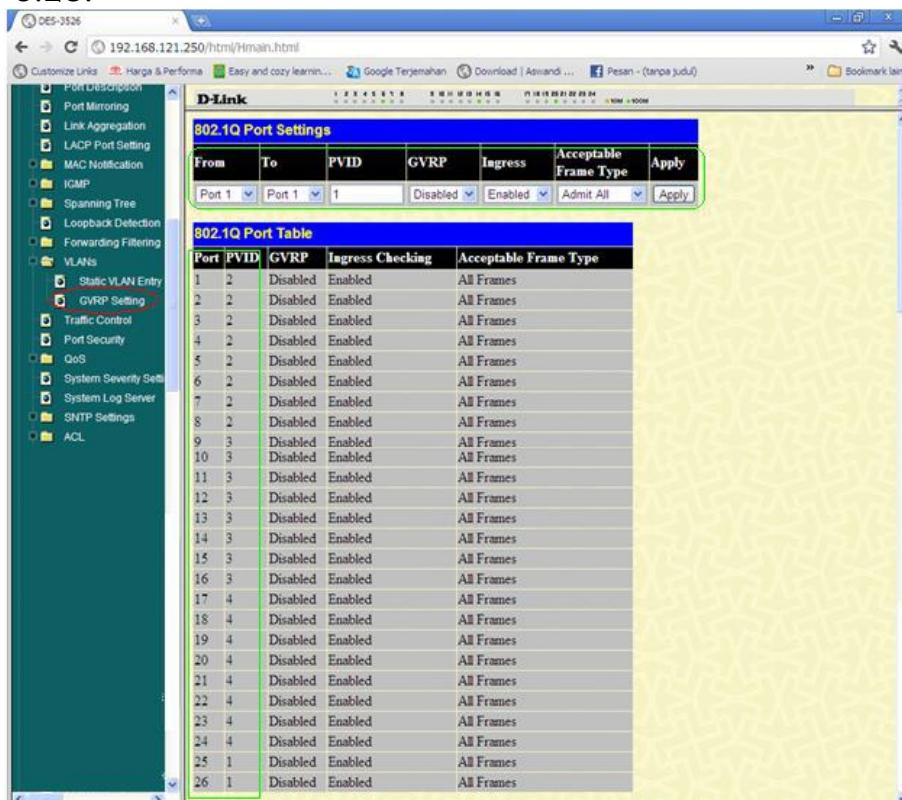


Gambar 5.26 Konfigurasi Grup VLAN (VID 3, VLAN Name Praktikan, Port 9-16 & 25)



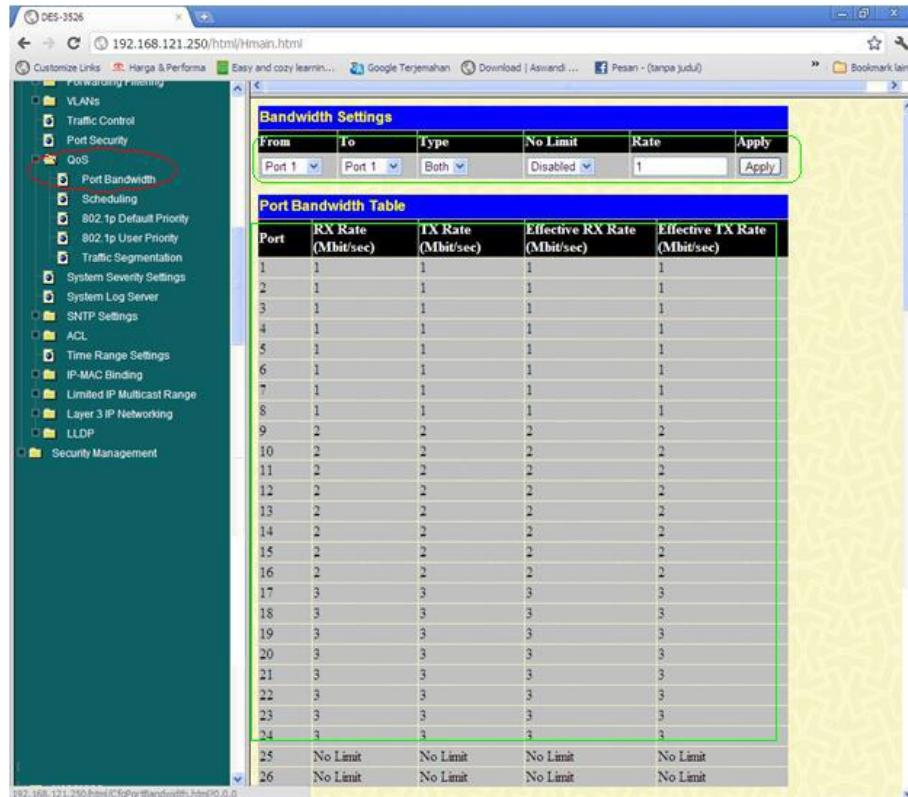
Gambar 5.27 Konfigurasi Grup VLAN (VID 4, VLAN Name Administrator, Port 17-24 & 25)

Langkah yang keempat, pilih “GVRP Setting” pada submenu “VLANs”, untuk mengaktifkan PVID (Port Vlan ID), masukkan banyaknya port yang akan diaktifkan dengan memilih port awal “From”, port akhir “To”, serta isi PVID sesuai grup dari VLAN yang sudah dibentuk, kemudian aktifkan “Ingress Checking” dengan memilih “Enabled”. Untuk port 25 serta 26 kita tidak ubah, biarkan konfigurasi tersebut bersifat default yaitu PVID 1. Setelah semua konfigurasi diubah, jangan lupa untuk menekan atau mengklik “Apply” untuk melihat hasil dari perubahan konfigurasi. Hasil dari konfigurasi yang dilakukan dapat dilihat pada gambar 5.28.



Gambar 5.28 Hasil Pengaktifan PVID Setiap Grup VLAN

Konfigurasi dari Asymmetric VLAN telah selesai, langkah kemudian membatasi bandwidth dari setiap port yang diinginkan. Langkah pertama untuk membatasi bandwidth dari setiap port yakni, pilih submenu “QOS”, kemudian masukkan banyaknya port yang akan dibatasi bandwidthnya dengan memilih port awal “From”, port akhir “To”, jenis pembatasan (upload & download) “Type” serta isi nilai batasan “Rate” yang diinginkan (mulai dari 1 Mbps). Hasil konfigurasi dari pembatasan bandwidth berdasarkan port dapat dilihat pada gambar 5.29



Gambar 5.29 Konfigurasi Pembatasan Bandwidth Berdasarkan Port

Penggunaan dari Asymmetric VLAN serta pembatasan Bandwidth berdasarkan port selesai, silahkan dilakukan pengujian terhadap PC yang terdapat pada setiap grup VLAN dimana telah menerima IP secara otomatis (DHCP Client) dengan melakukan ping ke setiap PC yang ada, ping ke router serta ping ke PC file server. Jika hasil ping antar pc dalam grup VLAN menunjukkan tidak saling terkoneksi serta hasil ping dari PC yang ada dalam grup VLAN ke router dan PC file server menunjukkan saling terkoneksi maka konfigurasi Asymmeric VLAN telah berhasil. Untuk melakukan pengujian pembatasan bandwidth berdasarkan port yang telah dikonfigurasikan dapat dilakukan download file dari PC yang menjadi file server, jika terdapat perbedaan dalam kecepatan download dari masing-masing PC yang ditempatkan pada port dengan pembatasan bandwidth maka pembatasan bandwidth berdasarkan port telah berhasil.

5.3.6. Pengertian Wireless LAN (WLAN)

Teknologi Wireless LAN menjadi sangat popular saat ini di banyak aplikasi. Setelah evaluasi terhadap teknologi tersebut dilakukan, menjadikan para pengguna merasa puas dan meyakini reliability teknologi ini dan siap untuk digunakan dalam skala luas dan komplek pada jaringan tanpa kabel. Wireless LAN bekerja dengan menggunakan gelombang radio. Sinyal radio menjalar dari pengirim ke penerima melalui free space, pantulan, difraksi,



Line of Sight. Ini berarti sinyal radio tiba di penerima melalui banyak jalur (Multipath), dimana tiap sinyal (pada jalur yang berbeda-beda) memiliki level kekuatan, delay dan fasa yang berbeda-beda. Awalnya teknologi ini didesain untuk aplikasi perkantoran dalam ruangan, namun sekarang Wireless LAN dapat digunakan pada jaringan peer to peer dalam ruangan dan juga point to point diluar ruangan maupun point to multipoint pada aplikasi bridge Wireless LAN di desain sangat modular dan fleksibel. Jaringan ini juga bisa di optimalkan pada lingkungan yang berbeda. Dapat mengatasi kendala geografis dan rumitnya instalasi kabel.

5.3.7. Standarisasi Wireless LAN

Karena wireless LAN mengirim menggunakan frekuensi radio, wireless LAN diatur oleh jenis hukum yang sama dan digunakan untuk mengatur hal-hal seperti AM/FM radio. Federal Communications Commission (FCC) mengatur penggunaan alat dari wireless LAN. Dalam pemasaran wireless LAN sekarang, menerima beberapa standar operasional dan syarat dalam Amerika Serikat yang diciptakan dan dirawat oleh Institute of Electrical Electronic Engineers (IEEE). Beberapa Standar wireless LAN :

Tabel 5.5 Standarisasi WLAN

STANDAR KETERANGAN	
IEEE 802.11	Standar asli wireless LAN menetapkan tingkat perpindahan data yang paling lambat dalam teknologi transmisi light-based dan RF.
IEEE 802.11b	Menggambarkan tentang beberapa transfer data yang lebih cepat dan lebih bersifat terbatas dalam lingkup teknologi transmisi.
IEEE 802.11a	Gambaran tentang pengiriman data lebih cepat dibandingkan (tetapi kurang sesuai dengan) IEEE 802.11b, dan menggunakan 5 GHZ frekuensi band UNII.
IEEE 802.11g	Syarat yang paling terbaru berdasar pada 802.11 standar yang menguraikan transfer data sama dengan cepatnya seperti IEEE 802.11a, dan sesuai dengan 802.11b yang memungkinkan untuk lebih murah.

5.3.8. Frekuensi yang Digunakan pada WLAN

Frekuensi adalah banyaknya getaran per detik dalam arus listrik yang terus berubah. Satuan frekuensi adalah Hertz disingkat Hz. Jika arus



bergerak lengkap satu getaran per detik, maka frekuensinya 1Hz Satuan frekuensi lain :

Kilohertz (kHz), Megahertz (MHz), Gigahertz (GHz), Terahertz (THz).

Frekuensi yang dipakai adalah 2.4 Ghz atau 5 Ghz yakni frekuensi yang tergolong pada ISM (Industrial, Scientific, dan Medial). Dalam teknologi WLAN ada dua standar yang digunakan yakni :

Tabel 5.6 Standarisasi Frekuensi Pada WLAN

802.11 STANDAR INDOOR

Jenis Standar	Frekuensi	Kecepatan
802.11	2,4 GHz	2 Mbps
802.11a	5 GHz	54 Mbps
802.11a 2X	5 GHz	108 Mbps
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 GHz	54 Mbps
802.11n	2,4 GHz	120 Mbps

Sedangkan untuk 802.16 Standar Outdoor salah satunya adalah WIMAX (World Interoperability for Microwave Access) yang sedang digalangkan penggunaanya di Indonesia.

5.3.9. Mode pada WLAN

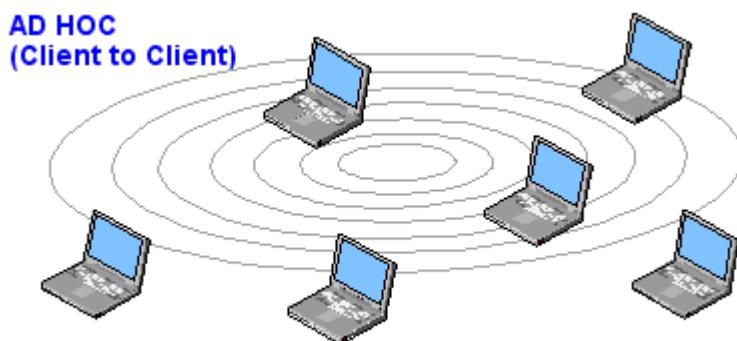
Wireless Local Area Network sebenarnya hampir sama dengan jaringan LAN, akan tetapi setiap node pada WLAN menggunakan wireless device untuk berhubungan dengan jaringan. Node pada WLAN menggunakan channel frekuensi yang sama dan SSID yang menunjukkan identitas dari wireless device. Tidak seperti jaringan kabel, jaringan wireless memiliki dua mode yang dapat digunakan yaitu Mode infrastruktur dan Mode Ad-Hoc.

Konfigurasi infrastruktur adalah komunikasi antar masing-masing PC melalui sebuah access point pada WLAN atau LAN. Komunikasi Ad-Hoc adalah komunikasi secara langsung antara masing-masing computer dengan menggunakan piranti wireless. Penggunaan kedua mode ini tergantung dari kebutuhan untuk berbagi data atau kebutuhan yang lain dengan jaringan berkabel.

5.3.9.1. Mode Ad-Hoc

Ad-Hoc merupakan mode jaringan WLAN yang sangat sederhana, karena pada ad-hoc ini tidak memerlukan access point untuk host dapat saling berinteraksi. Setiap host cukup memiliki transmitter dan receiver wireless untuk berkomunikasi secara langsung satu sama lain

seperti tampak pada gambar dibawah ini. Kekurangan dari mode ini adalah komputer tidak bisa berkomunikasi dengan komputer pada jaringan yang menggunakan kabel. Selain itu, daerah jangkauan pada mode ini terbatas pada jarak antara kedua komputer tersebut.



Gambar 5.30 Mode Ad-Hoc

5.3.9.2. Mode Infrastruktur

Jika komputer pada jaringan wireless ingin mengakses jaringan kabel atau berbagi printer misalnya, maka jaringan wireless tersebut harus menggunakan mode Infrastruktur. Pada mode infrastruktur access point berfungsi untuk melayani komunikasi utama pada jaringan wireless. Access point mentransmisikan data pada PC dengan jangkauan tertentu pada suatu daerah. Penambahan dan pengaturan letak access point dapat memperluas jangkauan dari WLAN. Mode infrastruktur dapat dikatakan seperti keterangan dibawah ini :

- 1 Terdapat 1 buah Access Point (AP) yang terhubung jaringan LAN kabel dan router untuk koneksi internet
- 2 PC pada jaringan LAN kabel (wired LAN) berkomunikasi dengan PC wireless LAN melalui Access Point, demikian pula komunikasi antar PC wireless LAN
- 3 PC wireless LAN memerlukan wireless LAN berupa PCI, PCMCIA atau USB adapter, bisa juga menggunakan AP yang diset pd mode Client Infrastructure / Station Infrastructure
- 4 PC dalam jaringan wired & wireless bersama-sama mengakses internet melalui router

Kualitas Saluran (Link Quality) antara AP ke wireless Client ditetukan oleh kuat sinyal (signal strength) yang diterima oleh wireless adapter pd PC Client



Gambar 5.31 Mode Jaringan Wireless Infrastruktur

5.3.10. Komponen-komponen pada WLAN

5.3.10.1. Access Point

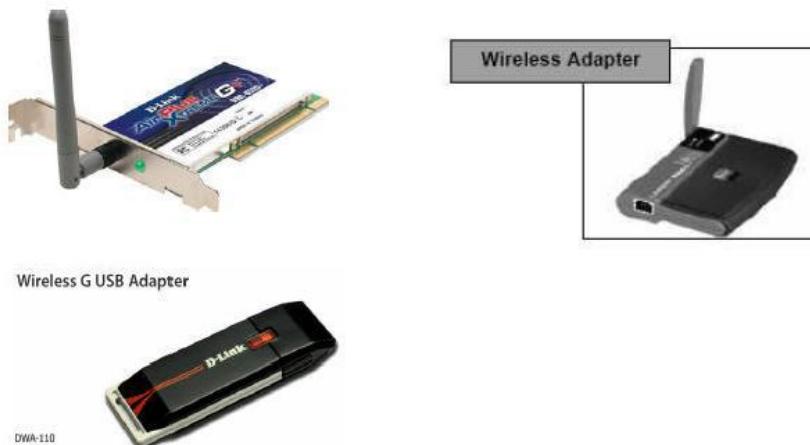
Merupakan perangkat yang menjadi sentral koneksi dari pengguna (user) ke ISP (Internet Service Provider), atau dari kantor cabang ke kantor pusat jika jaringannya adalah milik sebuah perusahaan. Access-Point berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.



Gambar 5.32 Contoh Access Point

5.3.10.2. WLAN Interface

Merupakan peralatan yang dipasang di Mobile/desktop pc, peralatan yang dikembangkan secara massal adalah Dalam bentuk PCMCIA (Personal Computer Memory Card International Association) card, pci card maupun melalui port usb (universal serial bus).



Gambar 5.33 WLAN Interface

5.3.10.3. Mobile/Desktop PC

Merupakan perangkat akses untuk pengguna, mobile PC pada umumnya sudah terpasang port PCMCIA. Sedangkan Desktop PC harus ditambahkan Wireless Adapter melalui PCI (Peripheral Componentinterconnect) Card atau USB (Universal Serial Bus).



Gambar 5.34 Mobile/Desktop PC

5.3.10.4. Antena

Antena external (optional) digunakan untuk memperkuat daya pancar. Antena ini dapat dirakit sendiri oleh user. contoh : antena kaleng, wajan bolic maupun antena komersil yang banyak dijual bebas di pasaran



Gambar 5.35 Antena Eksternal



1. Antena Omni – Directional

Yaitu jenis antena yang memiliki pola pancaran sinyal ke segala arah dengan daya yang sama. Untuk menghasilkan cakupan area yang luas, gain dari antena omni-directional harus memfokuskan dayanya secara horizontal (mendatar), dengan mengabaikan pola pemancaran ke atas dan kebawah, sehingga antena dapat diletakkan ditengah-tengah base station. Dengan demikian keuntungan dari antenna jenis ini adalah dapat melayani jumlah pengguna yang lebih banyak. Namun, kesulitannya adalah pada pengalokasian frekuensi untuk setiap sel agar tidak terjadi interferensi.

2. Antena Directional

Yaitu antena yang mempunyai pola pemancaran sinyal dengan satu arah tertentu. Antena ini idealnya digunakan sebagai penghubung antar gedung atau untuk daerah yang mempunyai konfigurasi cakupan area yang kecil seperti pada lorong – lorong yang panjang.

5.3.11. Konfigurasi Komponen WLAN

Untuk menggunakan fasilitas dan komponen jaringan pada WLAN, harus terlebih dahulu menginstall dan mengkonfigurasinya. Pada bagian ini akan mendiskusikan bagaimana cara untuk menginstall dan mengkonfigurasi komponen-komponen jaringan.

Periksa perangkat pendukung WLAN untuk memastikan bahwa perangkat ini dapat terhubung ke jaringan. Menginstall hardware, software untuk membuat komputer terhubung ke dalam jaringan, dan kemudian mengkonfigurasi protokol yang digunakan komputer untuk “berkomunikasi” dengan komputer lain. Perangkatpendukung yang kita gunakan adalah Access Point Router Linksys Cisco WRT54G2.

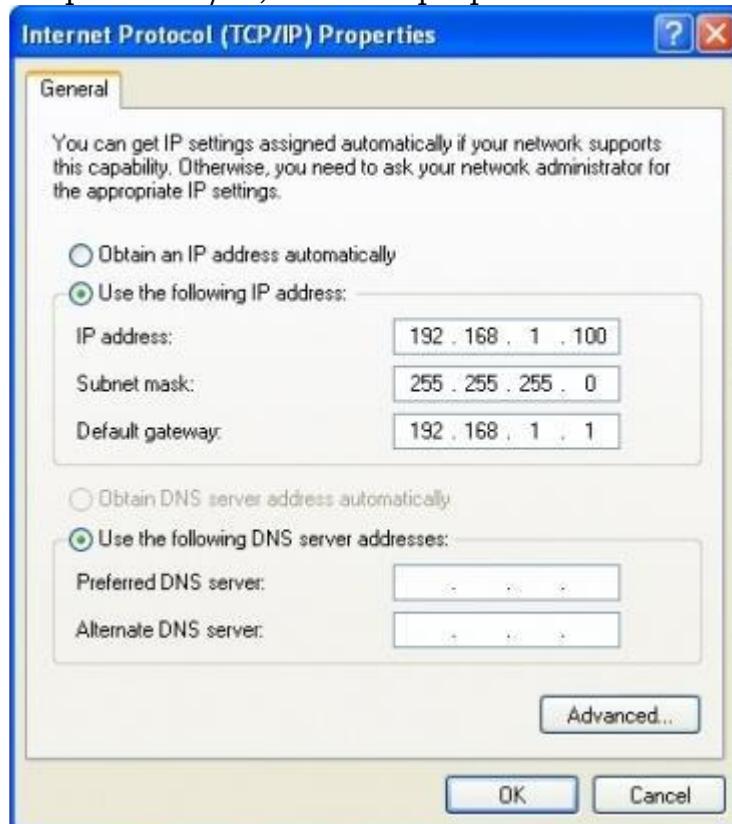


Gambar 5.36 Access Point Router Linksys Cisco WRT54G2

Langkah Konfigurasi Access Point Router Linksys Cisco

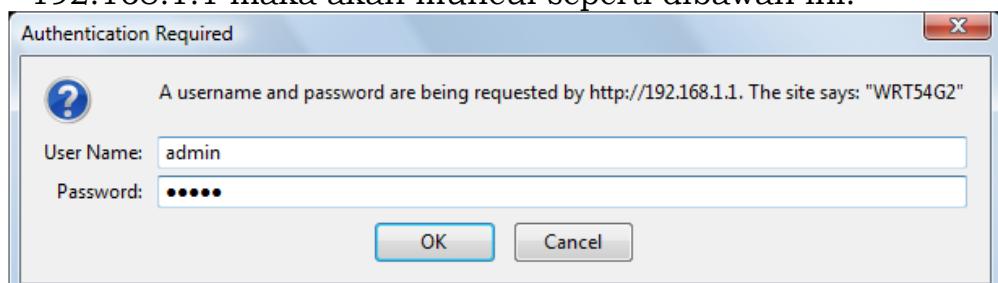
1. Buka kotaknya, terdapat Access Point Router broadband, CD, Adapter, Kabel.
2. Dibagian belakang terlihat terdapat beberapa konektor RJ 45, adapun fungsinya adalah ;
 - a. Konektor RJ 45 dari ISP
 - b. Terdapat konektor 1-4,ini dikoneksikan ke PC-PC / ke Switch
 - c. Ke Adapter Listrik
3. Koneksikan kabel Adapter ke lubang koneksi power lalu hubungkan ke listrik
4. Untuk mengkonfigurasinya, maka yang kita persiapkan adalah :
 - a. Tancapkan kabel warna biru yang disertakan didalam kotak ke port di belakang router dan tancapkan ujung kabel ke Ethernet (port RJ45) di laptop / PC,

- b. Set IP PC / Laptop dengan cara,
- c. Klik dua kali icon Network Connection/ masuk ke Control Panel, klik NetworkConnection, klik Local Area Connection, lalu pilih TCP/IP, lalu klik properties



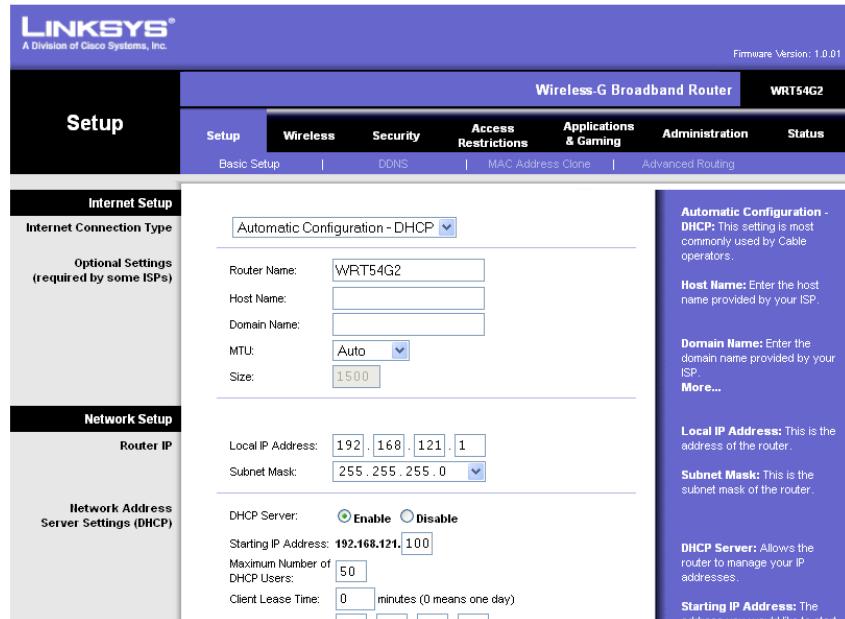
Gambar 5.37 : Tampilan Internet Protokol TCP/IP Properties

5. Masukan IP diatas, lalu klik OK. Setelah IP address di laptop / PC kita diganti seperti langkah sebelumnya Buka Browser, ketikan 192.168.1.1 maka akan muncul seperti dibawah ini.

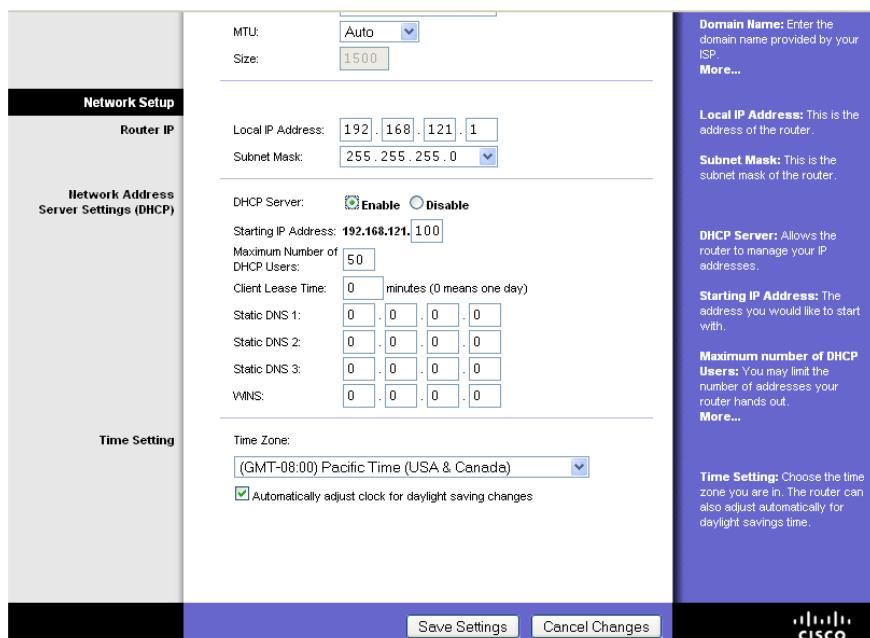


Gambar 5.38 Tampilan Authentication Required

6. Ketikan usernya : admin& passwordnya : admin, kemudian akan muncul halaman depan web Access Point Router.



Gambar 5.39 Tampilan Halaman Depan Access Point Router



Gambar 5.40 Tampilan Lanjutan Halaman Depan Access Point Router

7. Setting tab Setup seperti dibawah ini :

Internet Setup

- a. Internet Connection type : Pilih Automatic Configuration – DHCP Digunakan untuk menentukan tipe koneksi, terdapat 6 pilihan yaitu:
- Automatic Configuration – DHCP
 - Static IP
 - PPPoE
 - PPTP
 - L2TP



- Telstra Cable
- b. Optional Setting
 - Router Name : WRT54G2
Merupakan tipe router digunakan sebagai nama router
 - Host Name : Ketikan Lab Lanjut SK
Merupakan nama alat access point ini yang akan dibaca oleh PC Client
 - Domain Name : <kosong>default
Merupakan nama protocol di internet berdasarkan DNS (Domain Name System)
 - MTU : Pilih Auto
Merupakan ukuran paket data yang dapat di transmisikan terdapat 2 pilihan yaitu :
 - Auto
 - Manual
 - Size :<Auto>
Merupakan nilai besaran dari MTU dalam satuan bit
- c. Network Setup
 - Router IP
 - Local IP Address : Masukkan IP Address 192.168.121.1 Digunakan untuk pemberian IP Address pada jaringan local
 - Subnet Mask : Masukan 255.255.255.0 <Kelas C>
 - Network Address Server Setting (DHCP)
 - DHCP Server : Pilih Enable
Digunakan untuk mengaktifkan DHCP Server terdapat 2 pilihan yaitu :
 1. Enable
 2. Disable
 - Starting IP Address : Masukkan 100
Digunakan untuk pemberian awalan IP Address kepada PC Client
 - Maximum Number DHCPUser : Masukkan 50
Digunakan untuk menentukan jumlah PC Client yang dapat terkoneksi dengan Access Point Router
 - Client Lease Time : Masukkan 0
Digunakan untuk memberikan lama waktu koneksi, misal 10 minute, maka dalam 1 hari PC Client akan mengkonfirmasi ulang koneksi setiap 10 menit
 - Static DNS 1 : Masukan <kosong> default
Digunakan untuk pemberian IP Address secara manual untuk DNS 1
 - Static DNS 2 : Masukan <kosong> default
Digunakan untuk pemberian IP Address secara manual untuk DNS 2
 - Static DNS 3 : Masukan <kosong> default



Digunakan untuk pemberian IP Address secara manual untuk DNS 3

- WINS : Masukan <kosong> default

Digunakan untuk pemberian IP Address pada layanan untuk nama komputer NetBIOS

d. Time Setting

- Time Zone : (GMT+07.00 Thailand, Rusia)
Digunakan untuk melakukan pengaturan waktu pada Access Point Router, terdapat pilihan waktu dari setiap Negara atau posisi dimana wilayah dimana kita berada.
- Automatically adjust check for daylight saving changes : Cek List

e. Klik Save Setting untuk menyimpan hasil konfigurasi

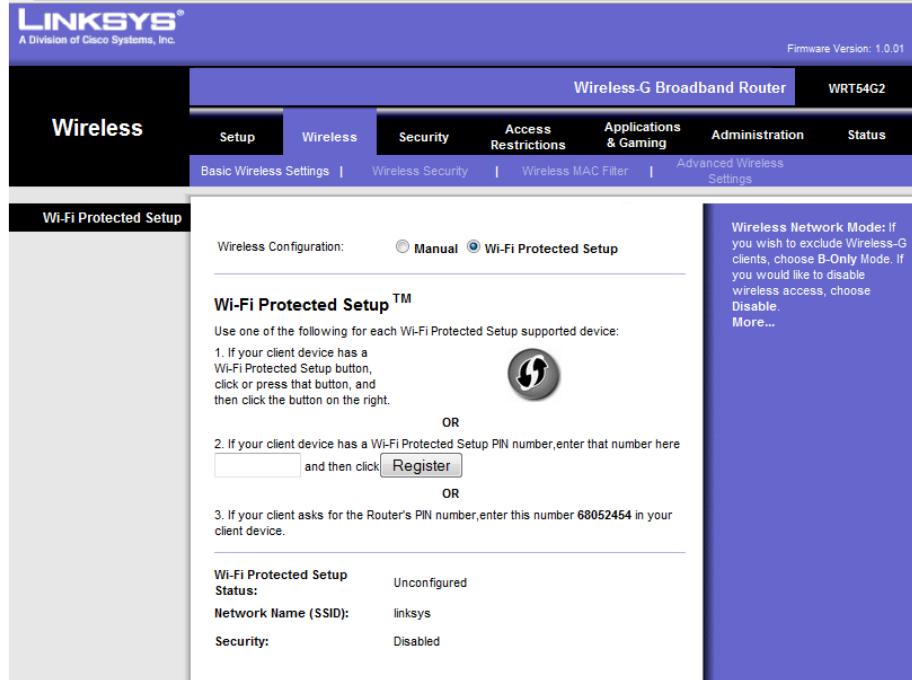
8. Agar supaya hanya PC/ Notebook tertentu yang terdaftar di router ini dan tidak semua PC/Notebook dapat terkoneksi ke internet, maka aturlah sistem keamanan wirelessnya, klik tab Wireless, maka akan muncul Basic Wireless Setup konfigurasi seperti berikut :

a. Wireless Network

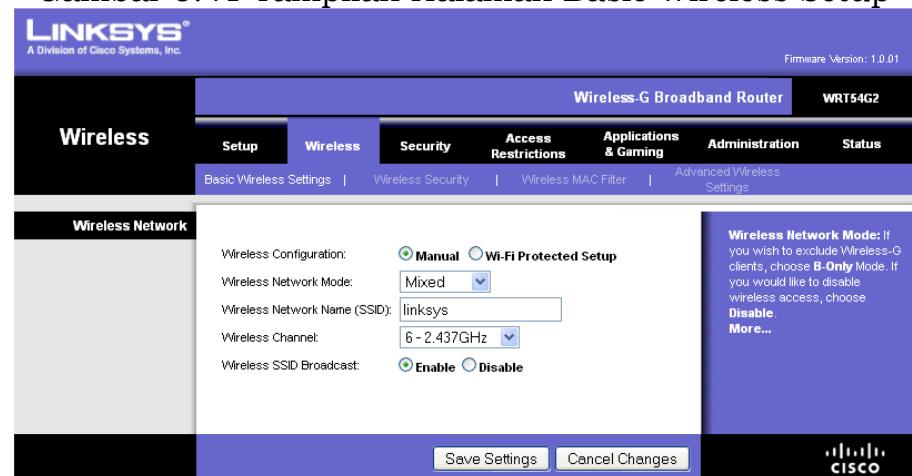
- Wireless Configuration : Pilih Manual
Digunakan untuk mengatur keamanan pada Access Point Router, terdapat 2 buah pilihan yaitu :
 - Manual
 - Wi-Fi Protected Setup
- Wireless Network Mode : Pilih Mixed (default Access Point yang akan support pada standar 802.11b dan 82.11g)
Digunakan untuk menentukan model jaringan yang akan digunakan terdapat 4 pilihan yaitu :
 - Disable
 - Mixed
 - B-Only
 - G-Only
- Wireless Network Name (SSID) : Ketikan linksys
Digunakan untuk pemberian nama Access Point yang akan terdeteksi di jaringan wireless.
- Wireless Channel : Pilih 6-2.437 GHz (default channel yang digunakan) Digunakan untuk menentukan channel frekuensi jaringan ini berada, terdapat 11 pilihan yaitu :
 - 1-2.437 GHz
 - 2-2.412 GHz
 - 3-2.442 GHz
 - 4-2.427 GHz
 - 5-2.432 GHz
 - 6-2.437 GHz

- g. 7-2.442 GHz
- h. 8-2.447 GHz
- i. 9-2.452 GHz
- j. 10-2.457 GHz
- k. 11-2.462 GHz
- Wireless SSID Broadcast : Pilih Enable
Digunakan untuk SSID akan dibroadcast ke jaringan wireless.

b. Klik Save Setting untuk menyimpan hasil konfigurasi



Gambar 5.41 Tampilan Halaman Basic Wireless Setup

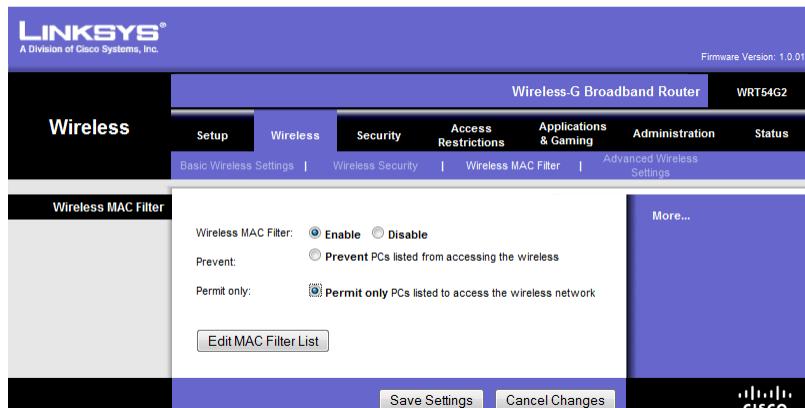


Gambar 5.42 Tampilan Konfigurasi Wireless Network Secara Manual

9. Agar dapat membatasi pengguna, maka Laptop atau PC yang akan terhubung ke Access Point Router kita ataur dengan menggunakan MAC Address Filter, Lalu pilih Wireless, kemudian klik tab Wireless Mac Filter dengan konfigurasi sebagai berikut:
- Wireless MAC Filter



- Wireless MAC Filter : Pilih Enable
Digunakan untuk mengaktifkan MAC Filter, terdapat 2 pilihan yaitu :
 - a. Enable
 - b. Disable
- Prevent : Default
Digunakan untuk mencegah PC/Notebook yang akan masuk ke dalam Acces Point Router / jaringan.
- Permit Only : Pilih Permit Only PCs Listed To Access The Wireless Network Digunakan untuk memberikan ijin kepada PC/Notebook yang terdaftar pada jaringan/Access Point Router ini.



Gambar 5.43 Tampilan Halaman Wireless MAC Filter

10. Pada kolom MAC 01 sampai dengan 40 adalah nomor MAC Address Filter List setiap laptop yang kita daftarkan ke router ini, jika MAC PC/Notebook tersebut kita tidak masukan maka Notebook/PC tersebut tidak dapat terkoneksi ke Internet. Bagaimana kita tahu alamat MAC address setiap laptop yang akan kita masukan ke kolom MAC address ini, maka pada laptop yang akan terkoneksi kita lakukan:



Gambar 5.44 Tampilan Pengaturan MAC Filter



11. Klik Start, pilih Run, setelah muncul tampilan Run maka ketikan cmd, kemudian ditampilkan cmd, ketikan ipconfig /all maka akan muncul, seperti gambar dibawah ini. Diperhatikan pada Ethernet Adapter Wireless Network Connection, perhatikan Physical Address, misalnya : 00-15-00-4F-48-E3

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Deris&Rini>IPCONFIG /ALL
Windows IP Configuration

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

Ethernet adapter Wireless Network Connection:

Connection-specific DNS Suffix . : intel(R) PRO/Wireless 2200BG Network
Description . . . . . : Intel(R) PRO/Wireless 2200BG Network
Connection
Physical Address. . . . . : 00-15-00-4F-48-E3
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 202.146.178.4
                           202.146.180.4
Lease Obtained. . . . . : Sunday, June 24, 2007 8:18:24 AM
Lease Expires . . . . . : Monday, June 25, 2007 8:18:24 AM

Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
Description . . . . . : Realtek RTL8139/810x Family Fast Eth
ernet NIC
Physical Address. . . . . : 00-16-36-18-23-18

C:\Documents and Settings\Deris&Rini>
```

Gambar 5.45 Tampilan cmd Untuk Mengetahui Nomor MAC Address Pada Laptop / PC

12. Lakukan langkah ke 14 untuk Laptop/PC yang lain juga.
13. Setelah mendapatkan alamat MAC nya masukan alamat tadi pada kolom MAC Router seperti pada langkah diatas tadi. Klik Save Settinguntuk simpan,
14. Perhatikan pada saat menyalin nomor MAC Address Laptop/PC ke MAC di Access Point Router menggunakan : bukan –
15. Setelah dilakukan langkah 16 sebelumnya, maka cobalah di Laptop/PC yang telah didaftarkan tadi dengan mengetikan PING 192.168.1 untuk mengetahui apakah Laptop/PC tersebut mendapatkan respon dari Access Point Router, seperti dibawah ini

```
C:\WINDOWS\system32\cmd.exe
Lease Obtained. . . . . : Tuesday, June 26, 2007 5:31:40 PM
Lease Expires . . . . . : Wednesday, June 27, 2007 5:31:40 PM

Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
Description . . . . . : Realtek RTL8139/810x Family Fast Eth
ernet NIC
Physical Address. . . . . : 00-16-36-18-23-18

C:\Documents and Settings\Deris&Rini>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Documents and Settings\Deris&Rini>
```

Gambar 5.46 Tampilan cmd Pada Saat Melakukan PING

5.3.12. Konfigurasi WLAN Mode Ad-Hoc

Jaringan Ad Hoc adalah salah satu jenis dari jaringan nirkabel yang terdiri dari sekumpulan node-node yang berkomunikasi antara satu dengan yang lainnya secara langsung tanpa melibatkan node perantara seperti router atau access point.

Disebut sebagai jaringannya ad hoc karena jaringan ini tidak bergantung pada infrastruktur yang sudah ada sebelumnya, seperti router di jaringan kabel atau akses point di jaringan nirkabel.

- Pastikan driver WLAN anda mendukung jaringan Ad Hoc

Caranya mengeceknya :

Buka CMD pada mode Administrator : ketik CMD pada kotak pencarian (search), klik kanan pilih run administrator dan ketik : **netsh wlan show driver**.



Gambar 5.47 mengecek Driver WLAN mendukung jaringan Ad-Hoc

Cek pada bagian : **Hosted Network Supported** kalau **YES** berarti komputer anda bisa disetting jaringan ad hoc tapi kalau **NO** berarti komputer anda tidak support.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh wlan show driver

Interface name: Wi-Fi

Driver : Qualcomm Atheros AR9485 Wireless Network Adapter
Vendor : Qualcomm Atheros Communications Inc.
Provider : Qualcomm Atheros Communications Inc.
Date : 26/03/2016
Version : 3.0.2.201
INF file : athw8x.inf
Type : Native Wi-Fi Driver
Radio types supported : 802.11b 802.11g 802.11n
FIPS_140-2 mode supported : Yes
802.11w Management Frame Protection supported : Yes
Hosted network supported : Yes
Authentication and cipher supported in infrastructure mode:
    Open      None
    Open      WEP-40bit
    Open      WEP-104bit
    Open      WEP
    WPA-Enterprise  TKIP
    WPA-Personal   TKIP
```

Gambar 5.48 Hosted Network Supported

2. Masih pada mode CMD administrator
ketik : `netsh wlan set hostednetwork mode=allow ssid=wireless-rizky key=secretpassword`

```
C:\Windows\system32>netsh wlan set hostednetwork mode=allow ssid=wireless-rizky key=secretpassword
The hosted network mode has been set to allow.
The SSID of the hosted network has been successfully changed.
The user key passphrase of the hosted network has been successfully changed.
```

gambar 5.49 set hostednetwork

Maksud command diatas yaitu kita membuat jaringan AdHoc menggunakan WLAN dan di set hostednetwork, dan diberi nama SSID yaitu wireless-rizky dan password login secretpassword
Jika sudah muncul keterangan successfully seperti diatas, sekarang silakan di start hostednetwork tersebut, jalankan command berikut ini ; `netsh wlan start hostednetwork`

```
C:\Windows\system32>netsh wlan start hostednetwork
The hosted network started.
```

Gambar 5.50 start hostednewok

3. Pastikan muncul keterangan hosted network started yang berarti jaringan tersebut sudah dibuat, sekarang coba cek di Network and Sharing Center, semestinya muncul koneksi baru tersebut.



Gambar 5.51 jaringan Ad-Hoc yang dibuat

4. Sekarang silakan koneksikan laptop kamu yang lain agar terhubung ke jaringan AdHoc tersebut,



Gambar 5.52 koneksi di laptop



5.4. Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
3. Kabel
4. Multi Tester
5. Access Point
6. Switch
7. Hub
8. Aplikasi Packet Tracer
9. Software virtualisasi (VMware)

5.5. Praktikum

1. Simulasi konfigurasi jaringan Peer to Peer
2. Simulasi konfigurasi jaringan client – Server
3. Simulasi Setting Access Point (AP)
4. Simulasi konfigurasi membuat jaringan Ad-Hoc

5.6. Referensi

1. Athailah, 2013. Panduan Singkat Menguasai Router Mikrotik Untuk Pemula. Mediakita.
2. Sofana, Iwan 2009. Cisco CCNA & Jaringan Komputer. Informatika Bandung.
3. Sofana, Iwan 2012. Cisco CCNP dan Jaringan Komputer (Materi Route, Switch & Troubleshooting). Informatika Bandung.
4. Wahyono, Teguh 2007. Building & Maintenance PC Server. Elex Media Komputindo.
5. Andi, (2005) "Penanganan Jaringan Komputer" Penerbit :Andi Yogyakarta.
6. Andi, (2004) "Wireless Atasi Keterbatasan Jangkauan" Penerbit : ANDI, Yogyakarta.
7. Goldman, James E. dan Rawles, Phillip T. (2001). "Applied Data Communications A Business Oriented Approach, 3th Edition". Penerbit John Wiley & Sons, Inc.
8. Gunadi Dwi Hantoro, (2009) "Wifi (Wireless LAN) Jaringan Tanpa Kabel" Penerbit : Informatika, Jakarta.
9. Heriadi, Dodi. Priyambodo, Tri Kuntoro. (2005) "Jaringan Wi-Fi Teori dan Implementasi" Penerbit ANDI Yogyakarta.
10. Hartono, Jogiyanto. (2000) "Pengenalan Komputer" Penerbit : Andi Yogyakarta.
11. Jim Gieir, (2005). "Wireless Network First Step". Penerbit : Andi Yogyakarta
12. Setiawan, Deris. (2009)."Internetworking Development & Design Life Cycle"
13. http://deris.unsri.ac.id/materi/jarkom/network_development_cycles.pdf Diakses tanggal 29 Januari 2021 Pukul 18:00 WIB.
14. Sopandi, Dede. (2008). "Instalasi dan Konfigurasi Jaringan komputer" Penerbit : Informatika.



5.7. Tugas

1. Menghubungkan 2 Komputer Secara Peer-to-Peer (bisa live atau menggunakan packet tracer)
2. Menghubungkan 6 Komputer Secara Client - Server (bisa live atau menggunakan packet tracer)
3. Membuat jaringan sharing data dan sharing printer
4. Melakukan pengamatan di tempat kerja, ditempat lain atau dikampus mengenai jaringan WLAN dengan point pengamatan ;
 - a. Topologi
 - b. Tipe & merk alat yang digunakan (indoor or outdoor)
 - c. Jangkauan
 - d. Bandwidt yang digunakan
5. Membuat video (model mahasiswa) tentang setting Wireless Router atau Access Point

Bahan Diskusi

- a. Bilamana dan mengapa LAN perlu dibangun dalam instansi dewasa ini. Jelaskan tentang kelebihan dan kekurangan dari pemakaian LAN.
- b. Bagaimana caranya dan apa saja yang diperlukan untuk menghubungkan dua atau lebih komputer dengan menggunakan kartu jaringan (membuat LAN sederhana)
- c. Apakah yang dimaksud dengan sharing periperal itu? Jelaskan tentang kelebihan dan kekurangannya.
- d. Apa kelebihan dan kekurangan topologi jaringan bintang dibandingkan dengan yang lain?
- e. Apakah yang dimaksud dengan protokol itu?
- f. Apakah bisa dilakukan instruksi ping dengan sintak:
ping <nama komputer tujuan>? Contoh: ping komputer-2
Cobalah anda praktekan!

5.8. Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, MODUL I PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Buttom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



MODUL VI

DHCP & ROUTER DASAR

6.1 Tujuan Praktikum

1. Untuk mengetahui cara kerja DHCP
2. Untuk mengetahui DHCP Server dan DHCP client
3. Untuk mengetahui dasar – dasar ROUTER

6.2 Indikator Pencapaian

1. Mampu mengkonfigurasi / mensetting DHCP Server dan DHCP Client
2. Mampu mengkonfigurasi jaringan pada router dasar
3. Mampu mengkonfigurasi Jaringan Pada Router Menggunakan DHCP Dinamis
4. Mampy mengkonfigurasi Jaringan Pada Router Menggunakan DHCP Static

6.3 Materi

6.3.1. DHCP

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan secara otomatis. Selain pengalokasian IP secara otomatis DHCP juga memberikan parameter jaringan seperti default gateway dan DNS server

6.3.1.1. DHCP Scope

DHCP Scope adalah alamat-alamat IP yang dapat disewakan kepada DHCP client. Ini juga dapat dikonfigurasikan oleh seorang administrator dengan menggunakan peralatan konfigurasi DHCP server. Biasanya, sebuah alamat IP disewakan dalam jangka waktu tertentu, yang disebut sebagai DHCP Lease, yang umumnya bernilai tiga hari.

Informasi mengenai DHCP Scope dan alamat IP yang telah disewakan kemudian disimpan di dalam basis data DHCP dalam DHCP server. Nilai alamat-alamat IP yang dapat disewakan harus diambil dari DHCP Pool yang tersedia yang dialokasikan dalam jaringan. Kesalahan yang sering terjadi dalam konfigurasi DHCP Server adalah kesalahan dalam konfigurasi DHCP Scope.

6.3.1.2. DHCP Lease

DHCP Lease adalah batas waktu penyewaan alamat IP yang diberikan kepada DHCP client oleh DHCP Server. Umumnya, hal ini dapat dikonfigurasikan sedemikian rupa oleh seorang administrator dengan menggunakan beberapa peralatan konfigurasi (dalam Windows NT Server dapat menggunakan DHCP Manager atau dalam Windows 2000



ke atas dapat menggunakan Microsoft Management Console [MMC]). DHCP Lease juga sering disebut sebagai Reservation.

6.3.1.3. DHCP Options

DHCP Options adalah tambahan pengaturan alamat IP yang diberikan oleh DHCP ke DHCP client. Ketika sebuah klien meminta alamat IP kepada server, server akan memberikan paling tidak sebuah alamat IP dan alamat subnet jaringan.

DHCP server juga dapat dikonfigurasikan sedemikian rupa agar memberikan tambahan informasi kepada klien, yang tentunya dapat dilakukan oleh seorang administrator. DHCP Options ini dapat diaplikasikan kepada semua klien, DHCP Scope tertentu, atau kepada sebuah host tertentu dalam jaringan.

6.3.2. Cara Kerja DHCP

Karena DHCP merupakan sebuah protokol yang menggunakan arsitektur client/server, maka dalam DHCP terdapat dua pihak yang terlibat, yakni DHCP Server dan DHCP Client.

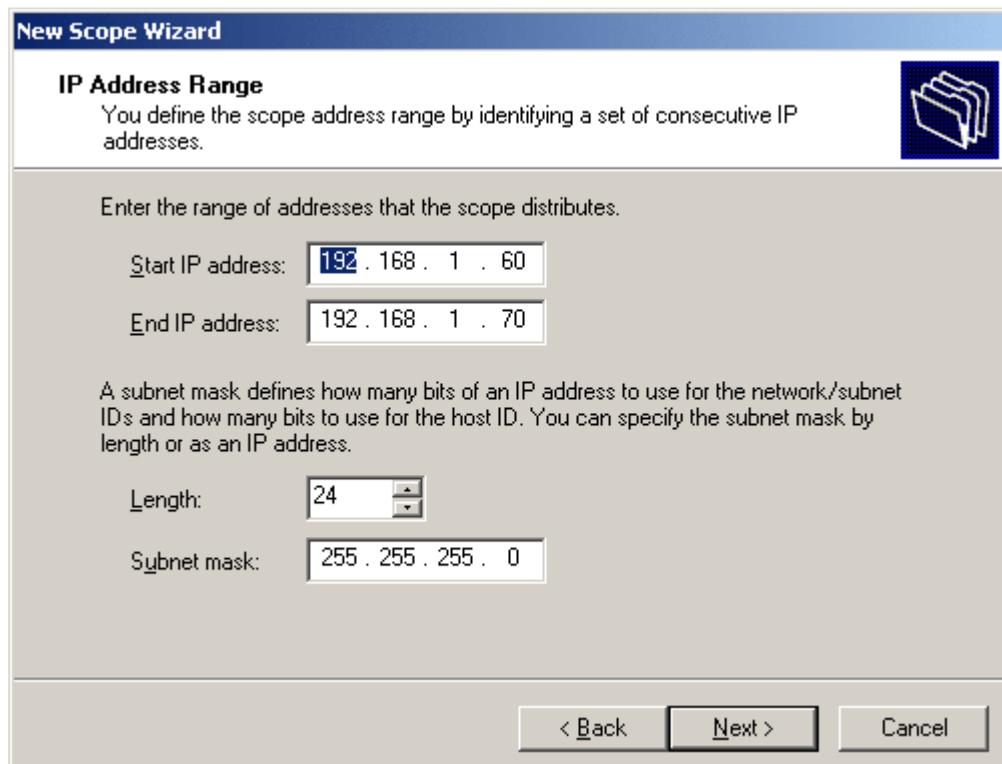
6.3.2.1. DHCP Server

Merupakan sebuah mesin yang menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. Beberapa sistem operasi jaringan seperti ;

- a. Windows NT Server
- b. Windows Server 2000
- c. Windows Server 2003
- d. Windows Server 2008
- e. Windows Server 2012
- f. Windows Server 2016
- g. Windows Small Business Server
- h. Windows Essential Business Server
- i. Windows Server Home Server
- j. Windows Server 2019 (Update)atau GNU/Linux

Memiliki layanan seperti ini. DHCP server umumnya memiliki sekumpulan alamat yang diizinkan untuk didistribusikan kepada klien, yang disebut sebagai DHCP Pool.

Setiap klien kemudian akan menyewa alamat IP dari DHCP Pool ini untuk waktu yang ditentukan oleh DHCP, biasanya hingga beberapa hari. Manakala waktu penyewaan alamat IP tersebut habis masanya, klien akan meminta kepada server untuk memberikan alamat IP yang baru atau memperpanjangnya.



Gambar 6.1 Tampilan DHCP Server

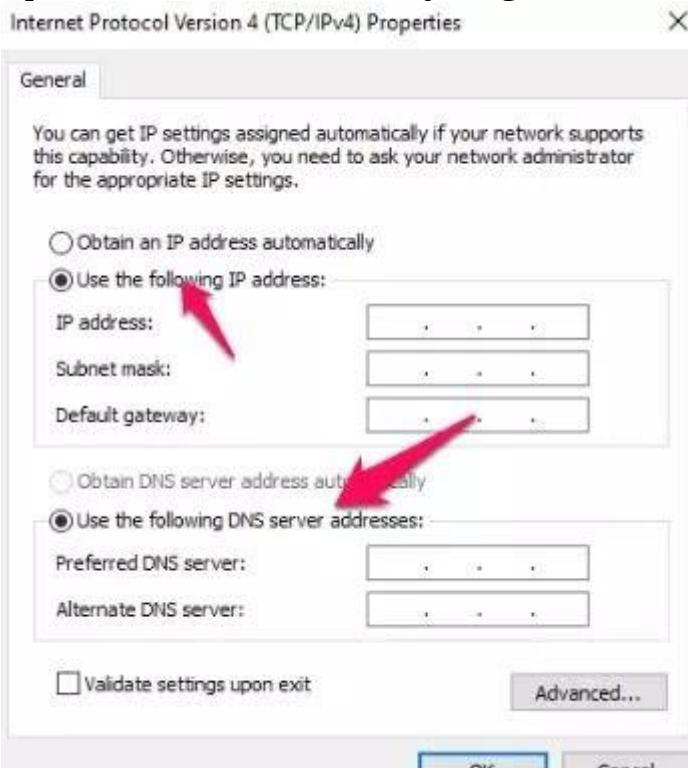
6.3.2.2. DHCP Client

Merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server. Sebagian besar sistem operasi klien jaringan (Windows NT Workstation, Windows 2000 Professional, Windows XP, Windows Vista, atau GNU/Linux) memiliki perangkat lunak seperti ini. DHCP Client akan mencoba untuk mendapatkan "penyewaan" alamat IP dari sebuah DHCP server dalam proses empat langkah berikut:

1. **DHCPDISCOVER**
DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.
2. **DHCPOFFER**
Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.
3. **DHCPREQUEST**
Client meminta DCHP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.
4. **DHCPACK**
DHCP server akan merespons permintaan dari klien dengan mengirimkan paket acknowledgment. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP lainnya) kepada klien, dan memperbarui basis data database miliknya. Klien selanjutnya akan memulai proses binding dengan



tumpukan protokol TCP/IP dan karena telah memiliki alamat IP, klien pun dapat memulai komunikasi jaringan.



Gambar 6.2 Tampilan DHCP Pada Client

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\CSAL 02>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:
      Connection-specific DNS Suffix  . : 
      IP Address. . . . . : 192.168.121.102
      Subnet Mask . . . . . : 255.255.255.0
      Default Gateway . . . . . : 192.168.121.1

C:\Documents and Settings\CSAL 02>
```

Gambar 6.3 Tampilan Untuk Mengetahui IP Yang Diberikan Server

Empat tahap di atas hanya berlaku bagi klien yang belum memiliki alamat. Untuk klien yang sebelumnya pernah meminta alamat kepada DHCP server yang sama, hanya tahap 3 dan tahap 4 yang dilakukan, yakni tahap pembaruan alamat (address renewal), yang jelas lebih cepat prosesnya.

DHCP bersifat stand-alone, sehingga jika dalam sebuah jaringan terdapat beberapa DHCP server, basis data alamat IP dalam sebuah DHCP Server tidak akan direplikasi ke DHCP server lainnya. Hal ini dapat menjadi masalah jika konfigurasi antara



dua DHCP server tersebut berbenturan, karena protokol IP tidak mengizinkan dua host memiliki alamat yang sama. Selain dapat menyediakan alamat dinamis kepada klien, DHCP Server juga dapat menetapkan sebuah alamat statik kepada klien, sehingga alamat klien akan tetap dari waktu ke waktu.

6.3.3. Router

Router merupakan perangkat jaringan yang berada di layer 3 dari OSI Layer. Fungsi dari router adalah untuk memisahkan atau mensegmentasi satu jaringan ke jaringan lainnya. Router juga bertujuan untuk memeriksa paket data yang masuk dan memilih jalur yang terbaik.

Router menghubungkan teknologi layer 2 yang berbeda, seperti Ethernet, Token-Ring dan berbagai teknologi komunikasi serial lainnya seperti ISDN, PPP dll. Router seperti halnya PC memiliki sebuah RAM, ROM, CPU, Flash Memory, NVRAM dan Operating System yang dikenal dengan Cisco Internetwork Operating System atau IOS.

6.3.4. Jenis - Jenis Router

Secara umum, router dibagi menjadi dua buah jenis, yakni:

1. Static Router (router statis): adalah sebuah router yang memiliki tabel routing statis yang diset secara manual oleh para administrator jaringan.
2. Dynamic Router (router dinamis): adalah sebuah router yang memiliki table routing dinamis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan dengan router lainnya.

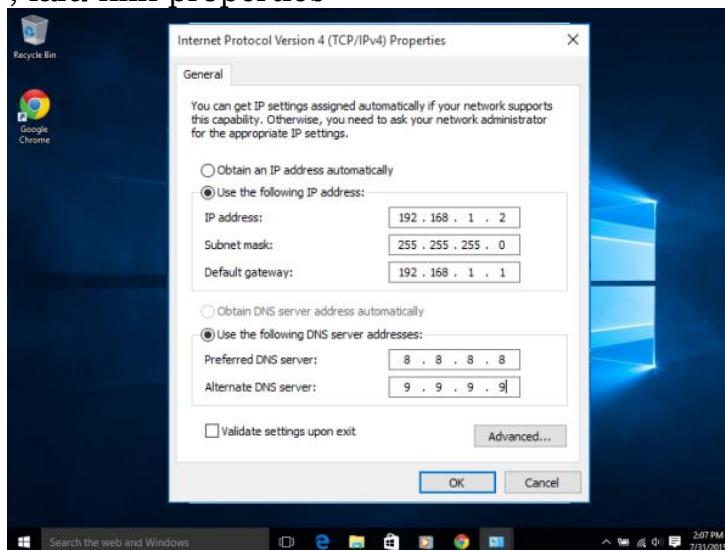
6.3.5. Konfigurasi Jaringan Pada Router

Sebelum dapat menggunakan router pada jaringan, ada baiknya dilakukan konfigurasi awal untuk mempermudah dalam melakukan koneksi sebuah jaringan, perangkat pendukung yang kita gunakan adalah VPN Router Linksys RV042, dengan konfigurasi sebagai berikut :



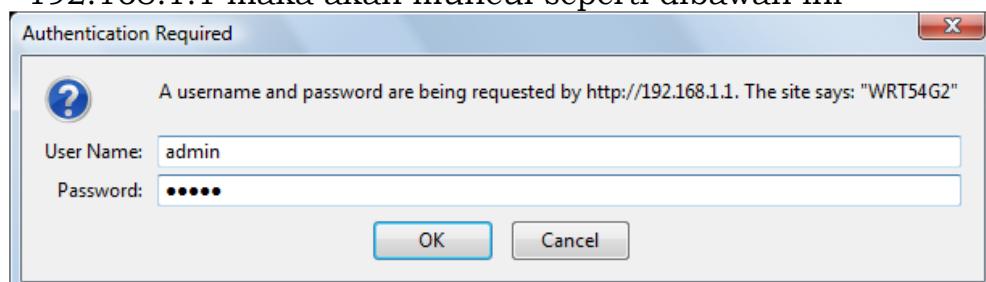
Gambar 6.4 VPN Router Linksys LRT224

1. Sebelum kita mulai, pastikan bahwa semua hardware kita dimatikan, termasuk Router, PC, Hub, Switches, dan kabel atau DSL Modem
2. Menghubungkan salah satu ujung kabel jaringan ethernet ke salah satu port bernomor di belakang router. hubungkan ujung lainnya ke port ethernet pada perangkat jaringan, ulangi langkah ini untuk menghubungkan PC atau perangkat lebih jaringan lainnya ke router
3. Hubungkan kabel listrik termasuk power AC pada sisi router, dan kemudian pasang ujung kabel daya ke stop kontak listrik
4. Klik dua kali icon Network Connection/ masuk ke Control Panel, klik NetworkConnection, klik Local Area Connection, lalu pilih TCP/IP, lalu klik properties



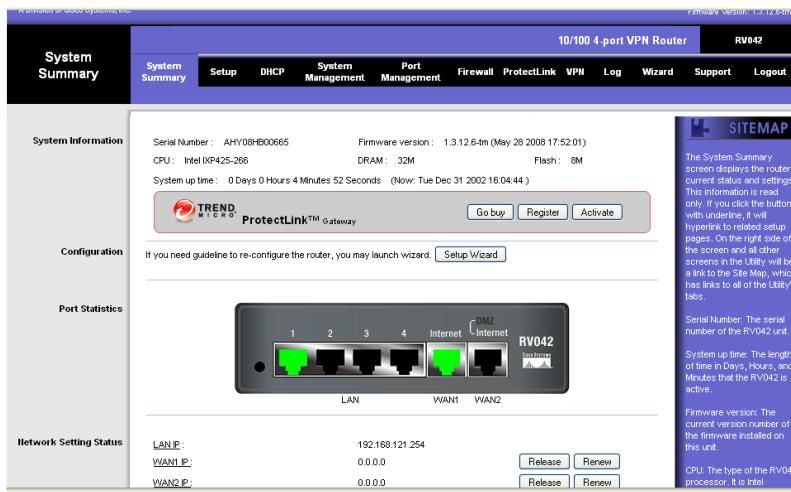
Gambar 6.5 Tampilan Internet Protokol TCP/IP Properties

5. Masukan IP diatas, lalu klik OK. Setelah IP address di laptop / PC kita diganti seperti langkah sebelumnya Buka Browser, ketikan 192.168.1.1 maka akan muncul seperti dibawah ini



Gambar 6.6 Tampilan Authentication Required

6. Ketikan usernya : admin& passwordnya : admin, kemudian akan muncul halaman depan web VPN Router



Gambar 6.7 Tampilan Halaman Depan Web VPN Router

7. Setting tab Setup seperti dibawah ini :
 - Network
 - LAN Setting
 - Host Name : Ketikan Lab SK Lanjut
Digunakan untuk memberikan nama alat access point ini yang akan dibaca oleh PC Client
 - Domain Name : Ketikan Lab SK Lanjut
Digunakan untuk memberikan nama protocol di internet berdasarkan DNS (Domain Name System)
 - Device IP Address : Masukan IP Address 192.168.121.254
Digunakan untuk memberikan pengalaman IP Address pada router
 - Subnet Mask : 255.255.255.0
Digunakan untuk memberikan Subnet Mask yang sesuai dengan pengalaman IP Address yang diberikan
 - Multiple Subnet Setting : Default
Digunakan untuk memberikan kombinasi pengalaman pada banyak host
 - Dual WAN / DMZ Setting
 - Dual WAN : Pilih atau di aktifkan
Digunakan untuk menghubungkan LAN dan jenis-jenis jaringan bersama-sama dan terkoneksi dengan internet
 - DMZ : Non Aktif
DMZ adalah subnetwork fisik atau logis yang berisi dan paparan layanan eksternal organisasi jaringan yang lebih besar untuk dipercaya, biasanya Internet
 - WAN Connection Type
 - WAN 1 : Pilih Obtain an IP Automatically
Terdapat 4 pilihan koneksi jaringan pada router yaitu :
 - a. Obtain an IP Automatically Static IP
Jika ISP Kita mengatakan bahwa koneksi kita terhubung melalui DHCP atau dinamis Alamat IP dari ISP. Maka pilih Obtain an IP Automatically Static IP sebagai WAN



Connection Type. Jika juga memilih untuk menggunakan alamat server DNS. Maka cek list Use The Following DNS Server Addresses masukan pengalamatan DNS Server 1 dan DNS Server 2

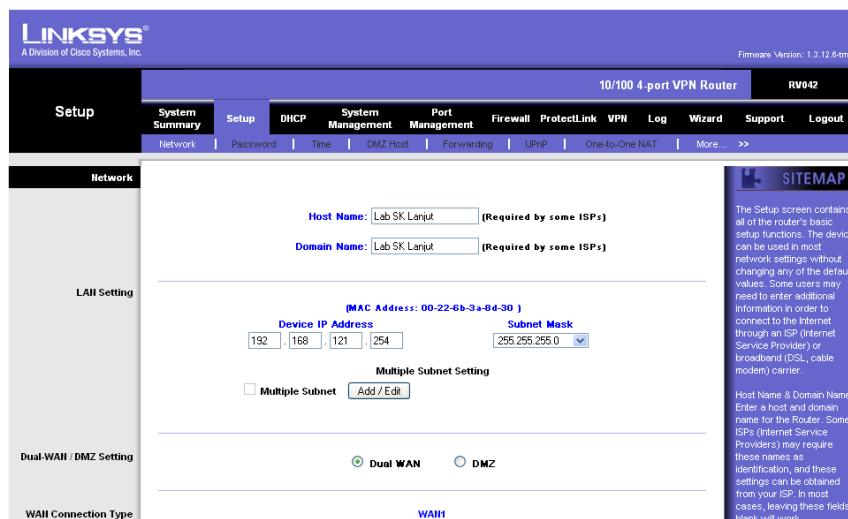
b. Static IP

Jika ISP Kita mengatakan bahwa koneksi kita terhubung melalui alamat IP Statis atau tetap dari ISP, Maka pilih Static IP sebagai WAN Connection Type, masukkan alamat IP WAN pada Specify WAN IP Address, Subnet Mask, Default Gateway dan DNS Server Address disediakan oleh ISP, pada kolom DNS Server Address, masukkan alamat DNS yang diberikan oleh ISP Kita, setidaknya satu alamat DNS Server

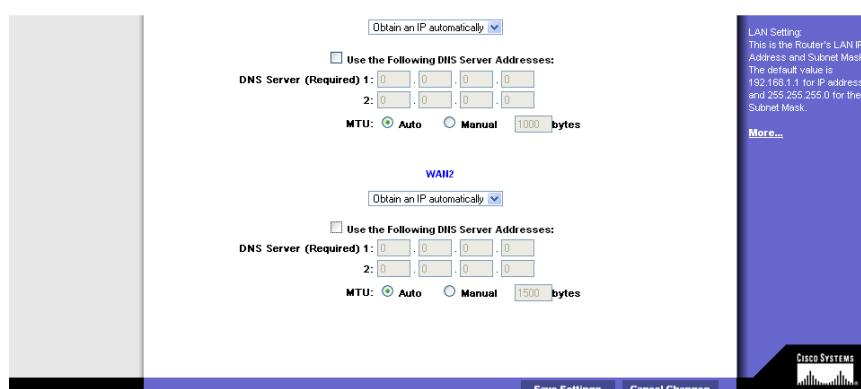
c. PPPoE

d. PPTP

→ Klik Save Setting untuk menyimpan hasil konfigurasi



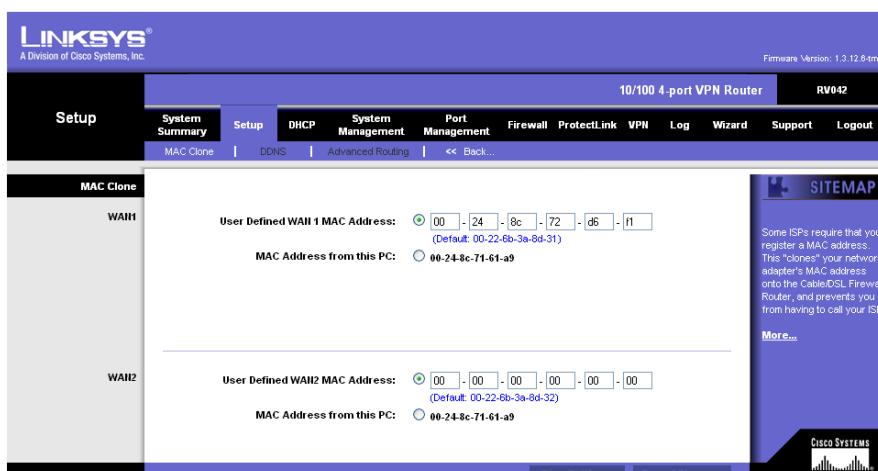
Gambar Gambar 6.8 Tampilan Setup Setting



Gambar 6.9 Tampilan Setup Lanjutan Setting



8. Terdapat 1 PC yang sudah terkoneksi internet, saat PC/Notebook ingin menggunakan jaringan yang sama agar bias terkoneksi, ternyata harus mendaftarkan MAC Address dari PC/Notebook yang ingin dikoneksikan, agar semua PC/Notebook yang ada bias terhubung ke internet tanpa mendaftarkan MAC Address dengan cara menduplikat MAC Address pada PC terhubung ke dalam router. Masih pada Setup namun pilih tab MAC Clone berikut konfigurasinya :
 - MAC Clone
 - WAN 1
 - User Defined WAN 1 MAC Address : Pilih (Aktif / Enable) Masukkan MAC Address 00-24-8C-72-D6-F1
Digunakan untuk memberikan MAC Address dari komputer lain yang terkoneksi dengan internet
 - MAC Address From This PC : Non Aktif
Digunakan untuk memberikan MAC Address dari computer yang terhubung langsung dengan router
 - WAN 2
 - Klik Save Setting untuk menyimpan hasil konfigurasi



Gambar 5.10 Tampilan Settingan MAC Clone

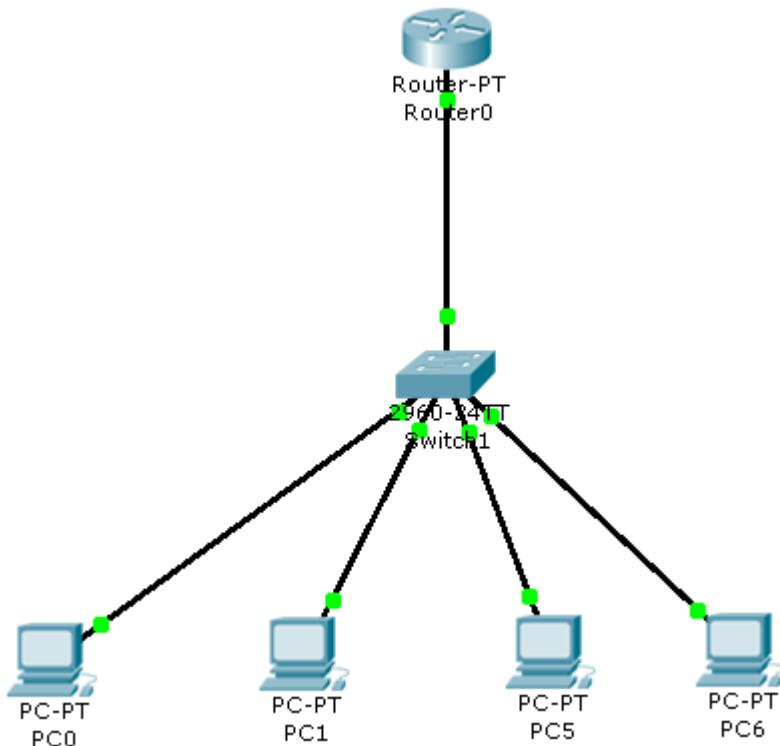
6.3.5.1. Konfigurasi Jaringan Pada Router Menggunakan DHCP Dinamis

DHCP server memberikan configurasi IP secara dinamis kepada hosts yang ada dalam jaringan kita agar bisa saling berkomunikasi satu sama lain. Seperti yang telah dibahas sebelumnya Modul Panduan Pertemuan 1 “Pengalamatan Jaringan”, untuk bisa berkomunikasi pada suatu jaringan private ataupun pada jaringan public Internet, setiap host pada jaringan harus diidentifikasi oleh suatu IP address.

Buat apa sich sebenarnya DHCP server ini? DHCP sangat dibutuhkan untuk mengurangi kompleksitas konfigurasi IP pada computer. Bayangkan saja kalau kita sebagai administrator jaringan dalam suatu business yang mempunyai sekitar 1000 computer dan kita tahu bahwa setiap computer tersebut membutuhkan konfigurasi IP yang unik.

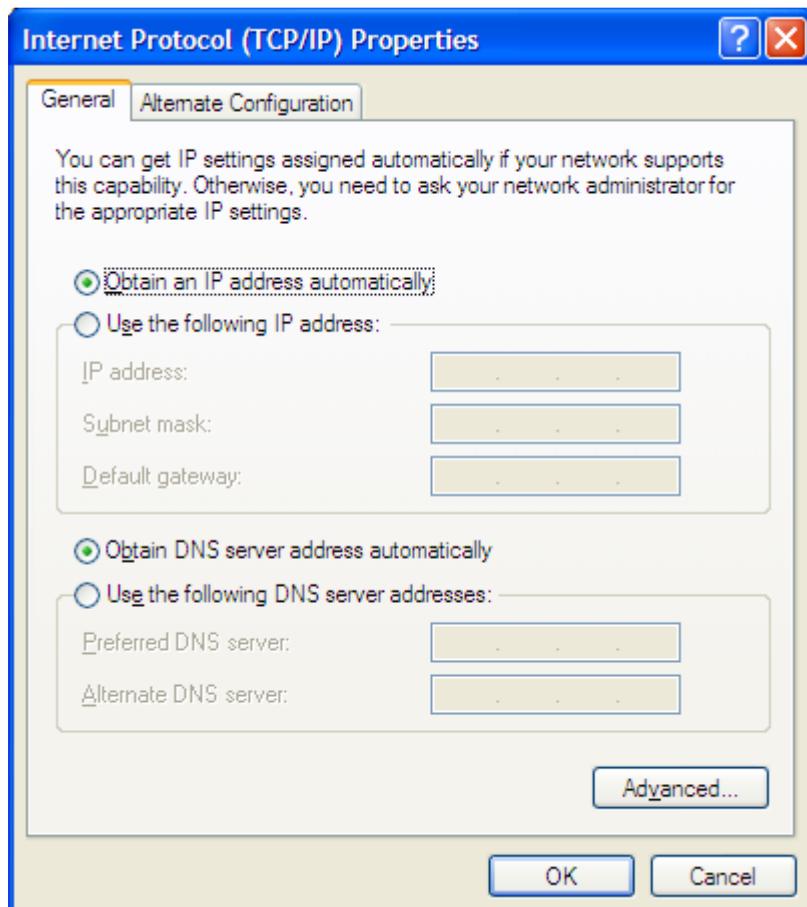
Kalau kita harus melakukannya manual satu persatu ...wah bakal keriting tuch jari, tapi jangan khawatir bisa direbonding kok tuch jari. Belum lagi kalau ada perubahan konfigurasi missal perubahan IP pada DNS atau WINS, atau perubahawan gateway address; maka kitapun harus mengubahnya satu persatu lagi.

Itu pun kalau berjalan mulus kalau salah ketik saja dan terjadi IP yang sama maka IP conflict tak terhindarkan dan kita harus mencarinya dan mengubahnya. Berikut dijelaskan konfigurasi DHCP Dinamis sesuai dengan gambar dibawah ini :



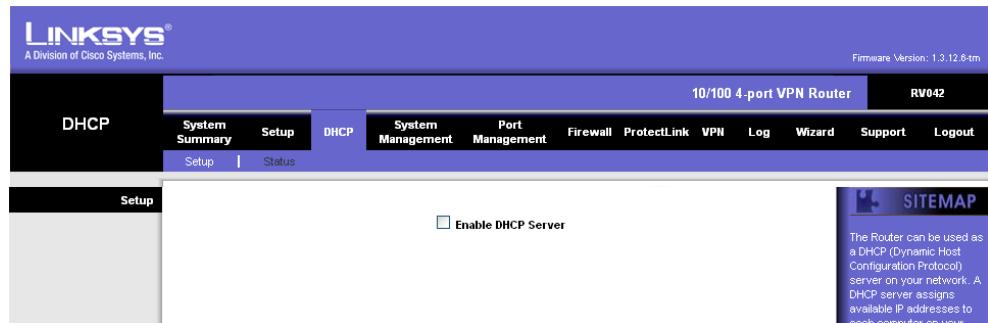
Gambar 6.11 Tampilan Jaringan Menggunakan DHCP Dinamis

1. Langkah – langkah konfigurasi DHCP Dinamis pada router sama saja dengan langkah – langkah konfigurasi pada router di atas, sampai dengan langkah ke 7. Perlu di ingat, karena kita menggunakan DHCP Dinamis dari server maka pada protocol TCP/IP dipilih Obtain an IP Address Automatically

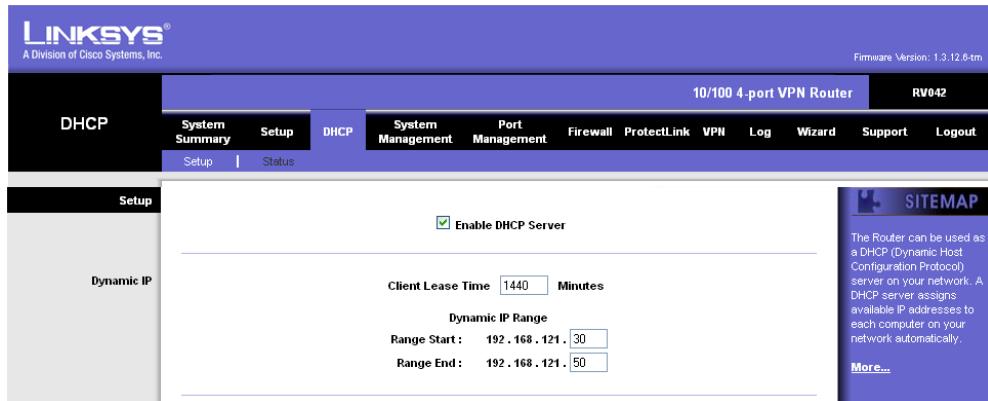


Gambar 6.12 Tampilan Internet Protokol TCP/IP Properties

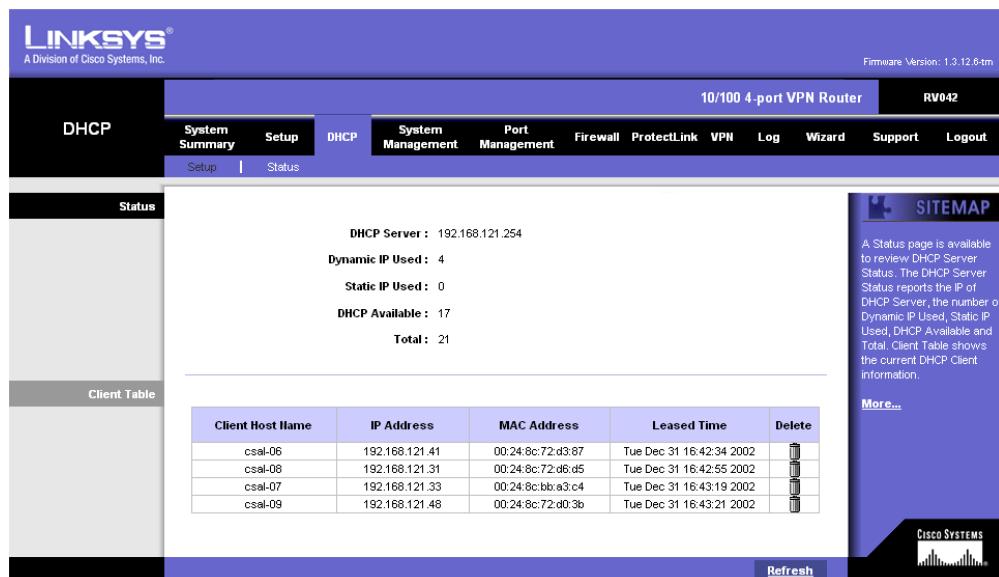
2. Selanjutnya mengatur DHCP Server dengan cara memilih tab DHCP, dengan settingan pada tab sebagai berikut :
→ Setup
 - Enable DHCP Server : Cek list
Digunakan untuk mengaktifkan fungsi DHCP Server pada router
 - Dynamic IP
 - Client Lease Time : Masukkan 1440 Minutes
Digunakan untuk memberikan lama waktu koneksi dari PC Client ke Server
 - Dynamic IP Range
 - 1. Range Start : Masukan 30
 - 2. Range End : Masukan 50Digunakan untuk memberikan batas awal dan batas akhir dari pengalamatan IP Address secara dinamis



Gambar 6.13 Tampilan Setup Settingan Awalan



Gambar 6.14 Tampilan Setup Settingan Setelah Dilakukan Konfigurasi



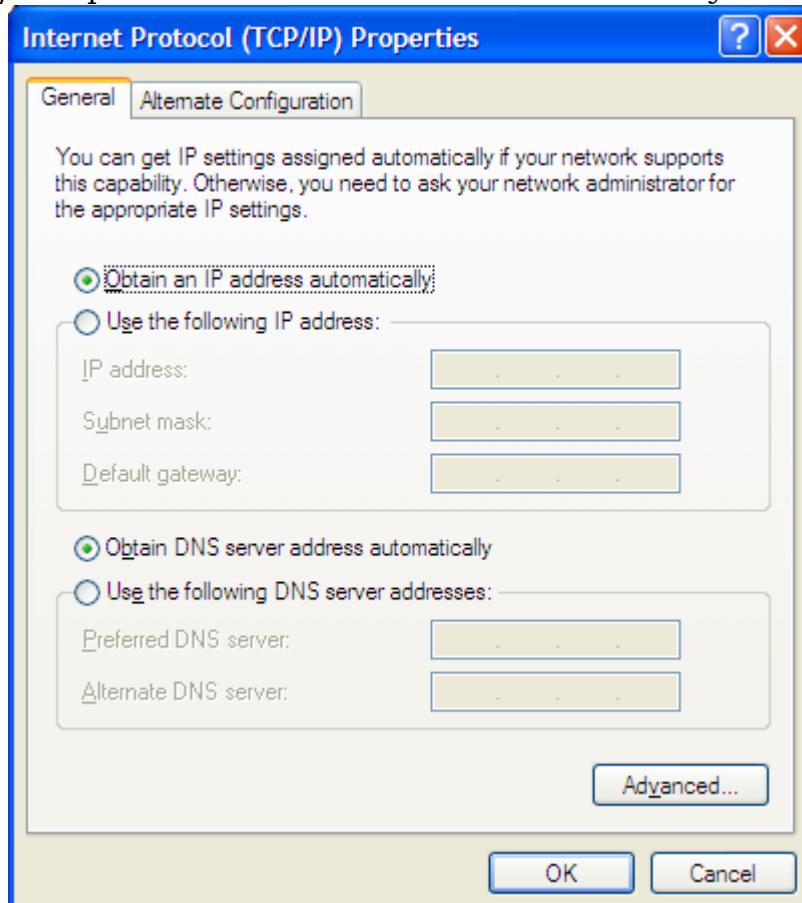
Gambar 6.15 Tampilan Status Traffic Jaringan DHCP Dinamis

3. Kemudian langkah selanjutnya untuk mengetahui traffic jaringan PC Client yang terhubung dengan router masih pada DHCP pliih tab Status, maka akan tampil gambar seperti di atas.



6.3.5.2. Konfigurasi Jaringan Pada Router Menggunakan DHCP Static

1. Langkah – langkah konfigurasi DHCP Static pada router sama saja dengan langkah – langkah konfigurasi Dinamis pada router di atas, sampai dengan langkah ke 2. Perlu di ingat, karena kita menggunakan DHCP Dinamis dari server maka pada protocol TCP/IP dipilih Obtain an IP Address Automatically

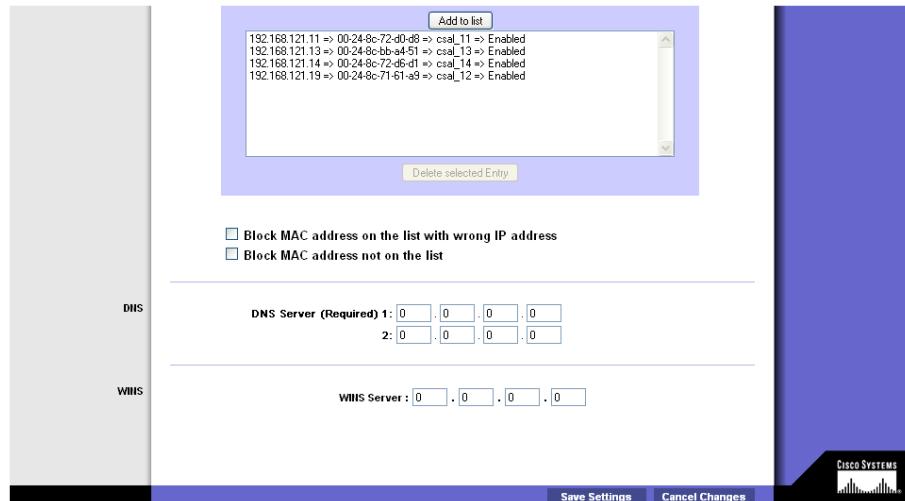


Gambar 5.17 Tampilan Internet Protokol TCP/IP Properties

2. Selanjutnya mengatur DHCP Server dengan cara memilih tab DHCP, dengan settingan pada tab sebagai berikut :
→ Setup
 - Enable DHCP Server : Cek list
Digunakan untuk mengaktifkan fungsi DHCP Server pada router
 - Static IP
 - Static IP Address : Masukkan IP Address 192.168.121.19
Digunakan untuk memberikan IP Address secara manual kepada PC yang akan didaftarkan, agar saat terkoneksi, PC tersebut akan mendapatkan IP yang sama.
 - MAC Address : Masukkan 00-8C-9D-48-79-D8
Digunakan untuk mendaftarkan PC Client pada router agar mendapatkan IP Static

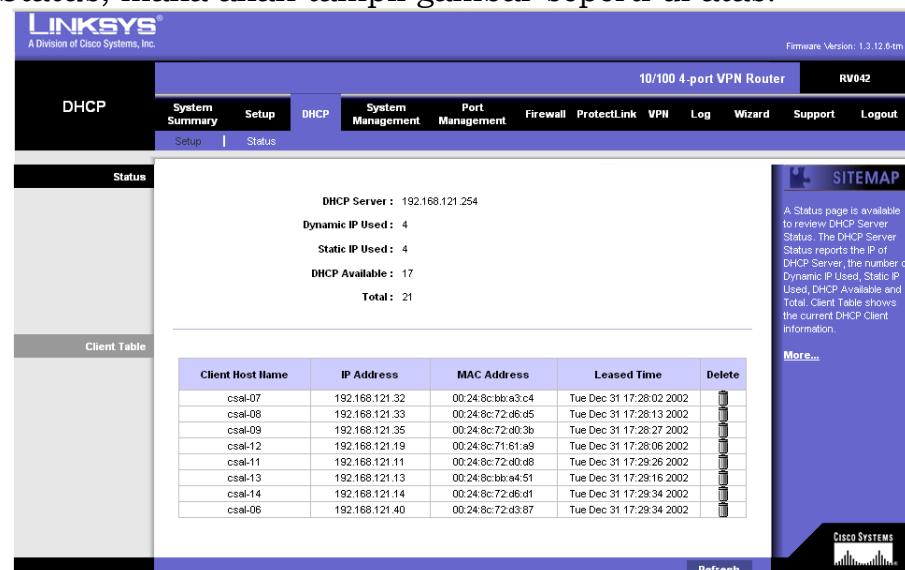


- Name : Masukkan csla 12
Digunakan untuk memberikan nama computer kepada PC Client yang terdaftar
 - Enable : Cek List
Digunakan untuk mengaktifkan DHCP Static pada PC Client terdaftar
 - Klik Add To List
3. Ulang langkah 2 untuk menambahkan PC Client yang ingin di berikan IP Static



Gambar 6.17 Tampilan Setup Konfigurasi DHCP Static

4. Kemudian langkah selanjutnya untuk mengetahui traffic jaringan PC Client yang terhubung dengan router masih pada DHCP pliih tab Status, maka akan tampil gambar seperti di atas.



Gambar 6.18 Tampilan Status Traffic Jaringan DHCP Static



6.4 Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
3. Router Linksys LRT224
4. Kabel
5. Multi Tester
6. Router
7. Switch
8. Hub
9. Aplikasi Packet Tracer
9. Software virtualisasi (VMware)

6.5 Praktikum

1. Simulasi DHCP Server
2. Simulasi DHCP Client
3. Simulasi konfigurasi jaringan Router Linksys LRT224
4. Simulasi konfigurasi Jaringan Pada Router Menggunakan DHCP Dinamis
5. Simulasi konfigurasi Jaringan Pada Router Menggunakan DHCP Static

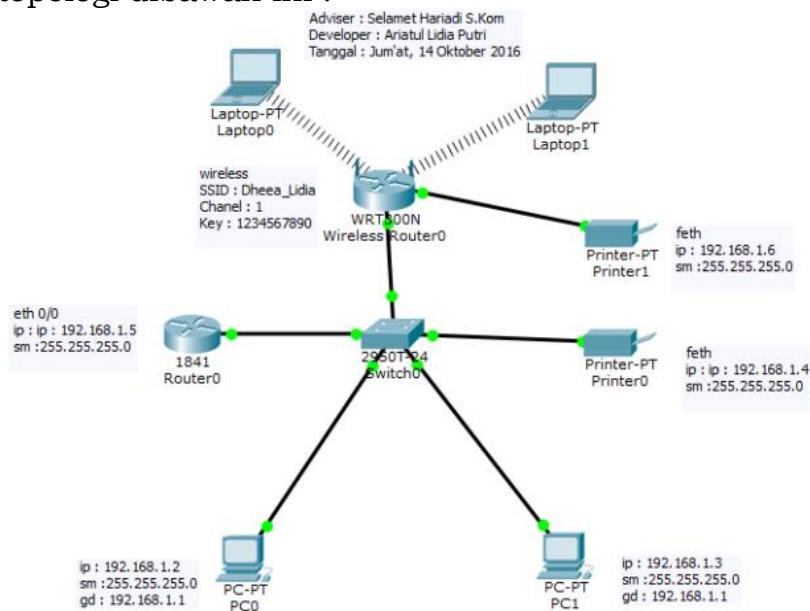
6.6 Referensi

1. bangpahmi.com. (2015, September 23). Pengertian DHCP Server, Fungsi dan Cara Kerjanya. <https://bangpahmi.com/pengertian-dhcp-server-fungsi-dan-cara-kerjanya/> (diakses tanggal, 28 Januari 2021)
2. Sofana, Iwan, Membangun Jaringan Komputer (Mudah membuat Jaringan Komputer Wire&Wireless untuk Pengguna Windows dan Linux) +DVD. Bandung: Informatika, 2013.
3. Sukmaaji, Anjik dan Rianto, Jaringan Komputer: Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan. Yogyakarta: Andi, 2008.
4. Rajab, Muis, Analisa Dan Perancangan Wireless LAN Security Menggunakan WPA2-Radius, Jurnal Skripsi Fakultas Sains Dan Teknologi Universitas UIN Syarief Hidayatullah, 2010.
5. Waloeya Yohan Jati, Computer Networking. Yogyakarta: Andi Publisher, 2012.
6. Enterprise Jubilee, 100 Tip & Trik WiFi. Jakarta: PT.Elex Media Komputindo, 2009.
7. Baihaqi, dkk. Implementasi Sistem Keamanan WPA 2-PSK Pada Jaringan Wifi. Serambi Engineering, Vol III : 248-254, Jan 2018.
8. Ariyadi, Tamsir. Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN). Jusikom, Vol 2 : 28-36, Jun 2017.
9. Y, Peisong and Guangxue Yue. Security Research on WEP of WLAN. Proceedings of the Second International Symposium on

- Networking and Network Security (ISNNS '10) Jinggangshan, P. R. China, 2-4, April. 2010, pp. 039-042.
10. Park, S.Joon and Derrick Dicoi. Wlan Security : Current and Future. IEEE Internet Computing. 1089-7801/03/\$17.00©2003 IEEE. September-Oktober 2003.

6.7 Tugas

Buatlah topologi dibawah ini !



Konfigurasi WIRELESS ROUTER Linksys Cisco tersebut agar bisa diakses !

6.8 Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, MODUL I PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Buttom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



MODUL VII

MONITORING DAN REMOTE PC

7.1 Tujuan Praktikum

1. Untuk dapat mengamati layanan dari alat atau komputer dan memberitahu jika ada masalah
2. Untuk mengetahui cara kerja network management
3. Untuk mengetahui konsep dasar SNMP

7.2 Indikator Pencapaian

1. Mampu mengoperasikan mikrotik sebagai network management
2. Mampu mengelola perangkat lunak jaringan system manajemen
3. Mampu menginstalasi aplikasi the DEDU
4. Mampu mengelola remote administrator (Radmin)

7.3 Materi

7.3 1. Monitoring dan Remote PC

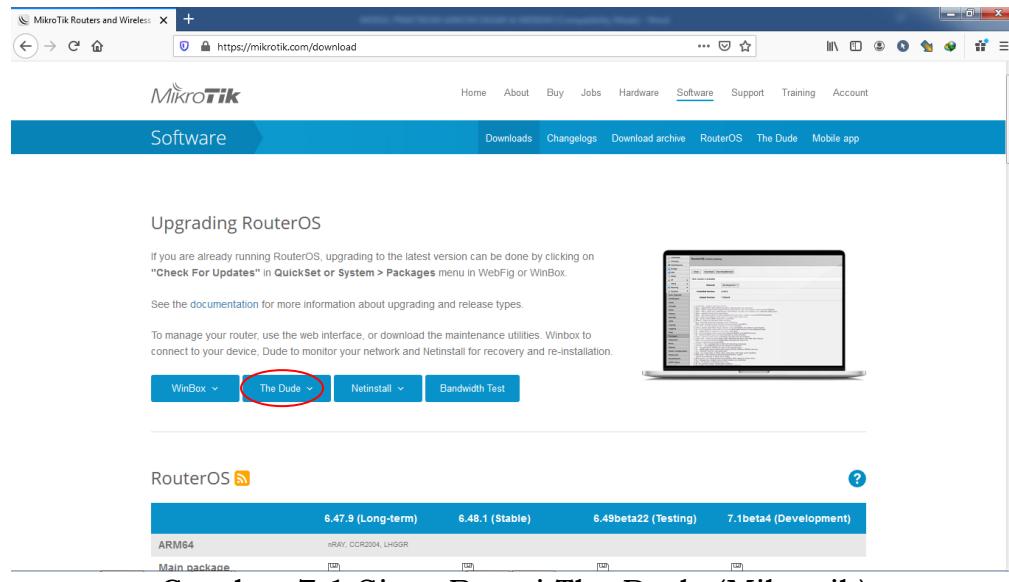
The Dude Network monitor adalah aplikasi baru dari mikrotik yang mana dapat menjadi sebuah jalan anda untuk mengatur lingkungan jaringan anda, the dude akan otomatis membaca dengan cepat semua alat/komputer yang terhubung dalam jaringan dalam satu jaringan lokal, menggambar dari rancangan peta dari jaringan lokal anda, mengamati layanan dari alat atau komputer dan memberitahu jika ada masalah servis dari alat/komputer dalam jaringan lokal anda. Beberapa fitur yang tersedia dalam program the dude adalah :

1. Dude bersifat gratis.
2. Instalasi dan pemakaian mudah.
3. Penemuan jaringan otomatis dan pengaturan tata letak jaringan.
4. Mengizinkan anda untuk menyusun peta-peta sendiri dan menambahkan alat-alat sendiri.
5. Dukungan untuk mengamati servis yang berjalan pada alat/komputer tersebut.

Uraian tersebut diatas adalah sedikit penjelasan tentang the dude network monitor dan beberapa fitur yang ada dalam the dude network monitor meskipun masih banyak lagi fasilitas yang di berikan oleh the dude, akan tetapi penulis akan mencoba memberikan sedikit tentang the dude network monitor yang sesuai dengan fitur yang ada.

The Dude bersifat gratis karena dapat di download di website milik mikrotik, pada saat artikel ini di buat penulis mendownload aplikasi the dude di alamat milik mikrotik yaitu

<http://www.mikrotik.com/download.html>



Gambar 7.1 Situs Resmi The Dude (Mikrotik)

Keberadaan dude sangat penting bagi seorang administrator jaringan untuk memantau (monitoring) jaringan di lingkungannya. Dengan menggunakan dude, maka akan dapat segera diketahui perangkat mana saja yang sedang mengalami gangguan. Sehingga harapannya setelah gangguan ditemukan, maka permasalahan yang ada dapat dengan segera diatasi.

7.3.2. Network Management

Network Management Protocol (SNMP) adalah sebuah "internet-protokol standar untuk mengelola perangkat pada jaringan IP Perangkat yang biasanya mendukung SNMP termasuk router, switch, server, workstation, printer, modem rak, dan banyak lagi.

Hal ini digunakan sebagian besar dalam sistem manajemen jaringan untuk memonitor jaringan terpasang perangkat untuk kondisi yang menjamin perhatian administratif. SNMP adalah komponen dari Internet Protocol Suite seperti yang didefinisikan oleh Internet Engineering Task Force (IETF).

Ini terdiri dari satu set standar untuk manajemen jaringan, termasuk protokol layer aplikasi, skema database, dan satu set objek data. SNMP memaparkan pengelolaan data dalam bentuk variabel pada sistem yang dikelola, yang menggambarkan konfigurasi sistem. Variabel ini kemudian dapat bertanya (dan kadang-kadang ditetapkan) oleh aplikasi mengelola.

7.3.2.1. Konsep Dasar SNMP

Dalam menggunakan SNMP khas, satu atau lebih komputer administrasi, manajer disebut, memiliki tugas pemantauan atau mengelola sebuah kelompok host atau perangkat pada jaringan komputer. Setiap sistem dikelola mengeksekusi, setiap saat, sebuah komponen perangkat lunak yang disebut agen yang melaporkan

informasi melalui SNMP untuk manajer. Pada dasarnya, agen SNMP manajemen mengekspos data pada sistem yang dikelola sebagai variabel. Protokol ini juga memungkinkan tugas-tugas manajemen aktif, seperti memodifikasi dan menerapkan konfigurasi baru melalui modifikasi terpencil variabel-variabel ini.

Variabel-variabel dapat diakses melalui SNMP diatur dalam hirarki. Ini hirarki, dan metadata lainnya (seperti tipe dan deskripsi variabel), yang dijelaskan oleh Basis Informasi Manajemen (MIBs). Sebuah jaringan SNMP dikelola terdiri dari tiga komponen utama:

- a. dikelola perangkat
- b. Agen - perangkat lunak yang berjalan pada perangkat dikelola
- c. Jaringan sistem manajemen (NMS) - perangkat lunak yang berjalan pada manajer

Sebuah perangkat dikelola adalah node jaringan yang mengimplementasikan interface SNMP yang memungkinkan searah (read-only) atau akses dua arah ke node informasi spesifik. Dikelola perangkat pertukaran simpul-spesifik informasi dengan NMSs tersebut. Kadang-kadang disebut elemen jaringan, perangkat dikelola dapat menjadi semua jenis perangkat, termasuk, namun tidak terbatas pada, router, server akses, switch, jembatan, hub, telepon IP, kamera video IP, host computer dan printer. Agen adalah manajemen jaringan-modul perangkat lunak yang berada pada perangkat dikelola. Agen memiliki pengetahuan lokal dari informasi manajemen dan menterjemahkan informasi ke atau dari bentuk spesifik SNMP.

Sebuah sistem manajemen jaringan (NMS) mengeksekusi aplikasi yang memantau dan mengontrol perangkat dikelola. NMSs menyediakan sebagian besar sumber daya

7.3.3 Langkah-langkah Instalasi Aplikasi The Dude

Langkah-langkah dalam instalasi aplikasi the dude adalah sebagai berikut :

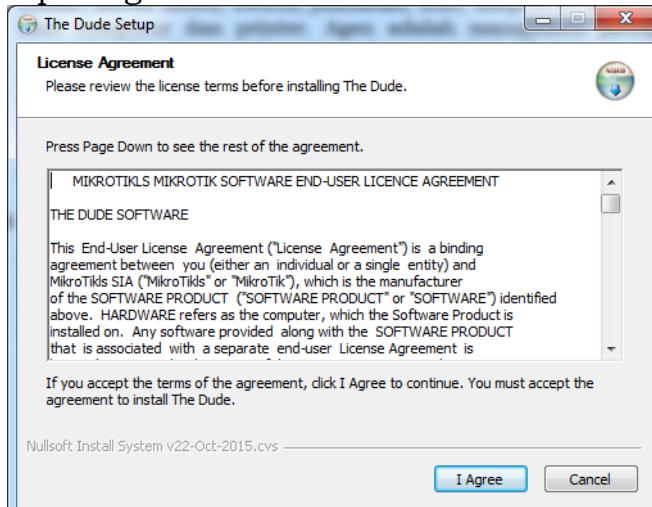
1. Download aplikasi the dude dari official website mikrotik.
2. Setelah proses download selesai, jalankan proses instalasi seperti pada gambar dibawah ini :



Gambar 7.2 The Dude Setup Wizard

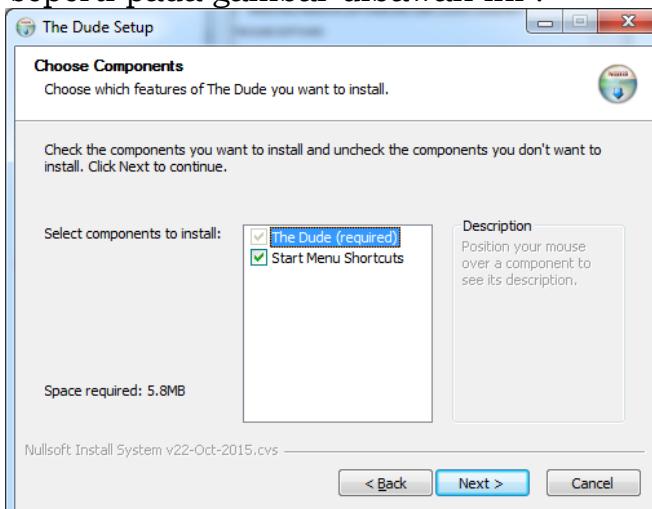


3. Setelah tampil seperti gambar diatas maka klik next, mka akan tampil seperti pada gambar dibawah ini :



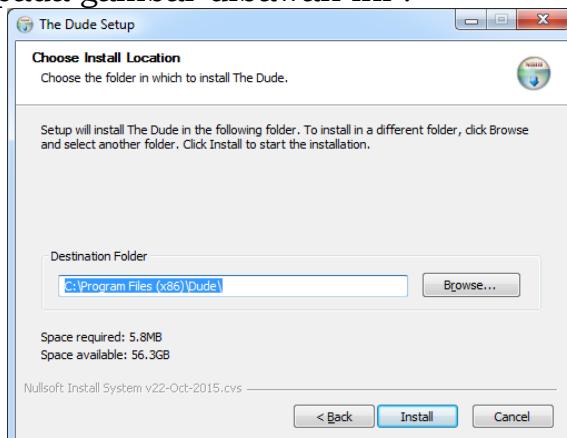
Gambar 6.3 License Agreement The Dude

4. Klik tombol I Agree untuk melanjutkan proses instalasi, kemudian akan tampil seperti pada gambar dibawah ini :



Gambar 7.4 Choose Component

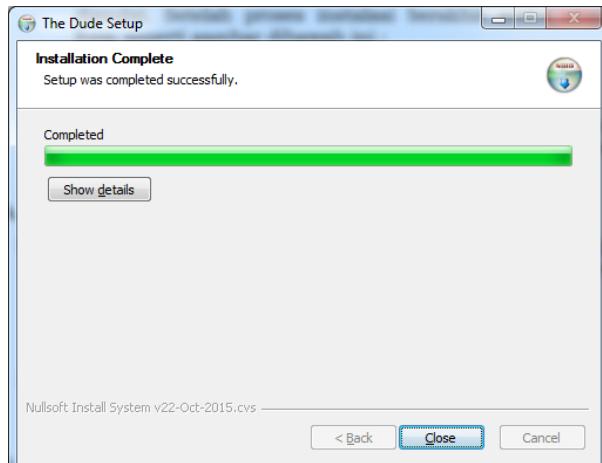
5. Pilih component yang akan digunakan, klik Next maka akan tampil seperti pada gambar dibawah ini :



Gambar 7.5 Pemilihan Lokasi Instalasi



6. Setelah anda klik next kemudian pilih dimana aplikasi tersebut akan diinstal, kemudian klik install dan proses instalasi akan dimulai. Setelah proses instalasi berakhir maka akan muncul form seperti gambar dibawah ini :



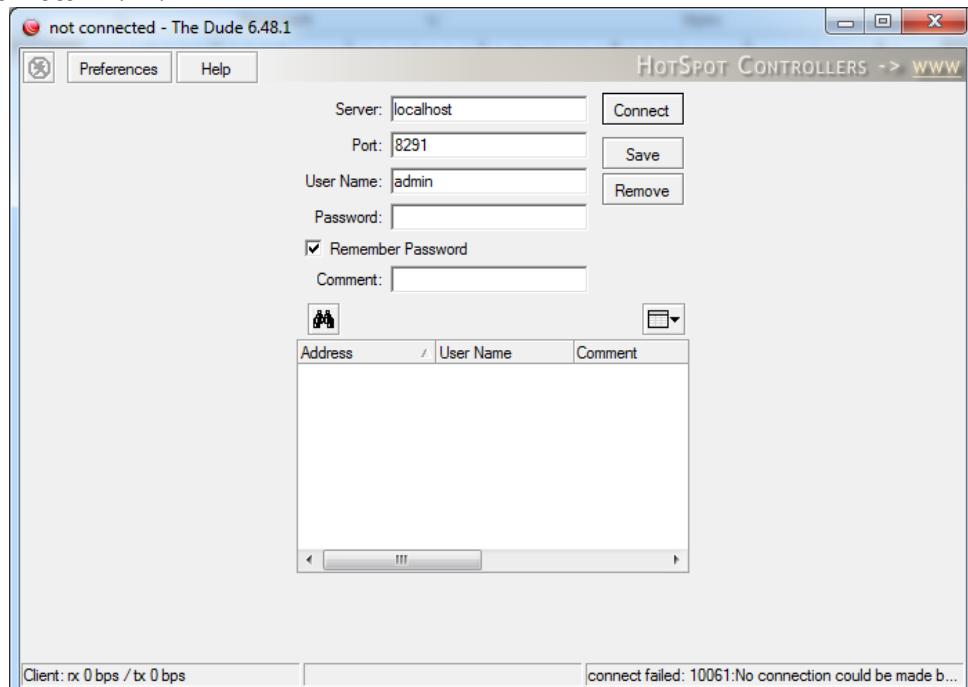
Gambar 7.6 Proses Instalasi Selesai

7. Proses instalasi the dude telah berakhir, jika anda ingin menjalankan the dude setelah proses instalasi maka pilih tanda centang pada Run The Dude. Klik Close/Finish.

7.3.4. Langkah-langkah Untuk Menemukan Jaringan

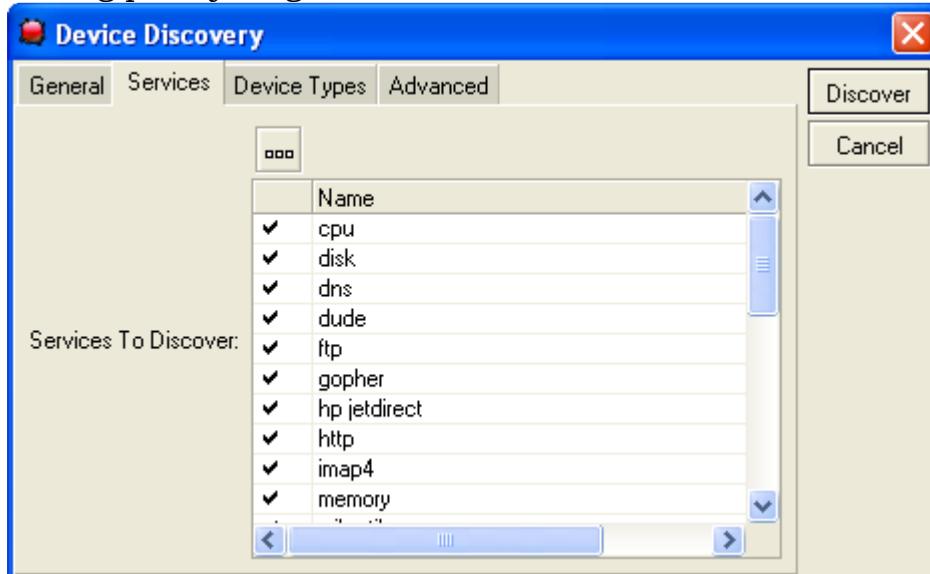
Langkah-langkah untuk menemukan jaringan adalah sebagai berikut :

1. Setelah kita menjalankan aplikasi maka akan muncul form seperti gambar 7.7 :



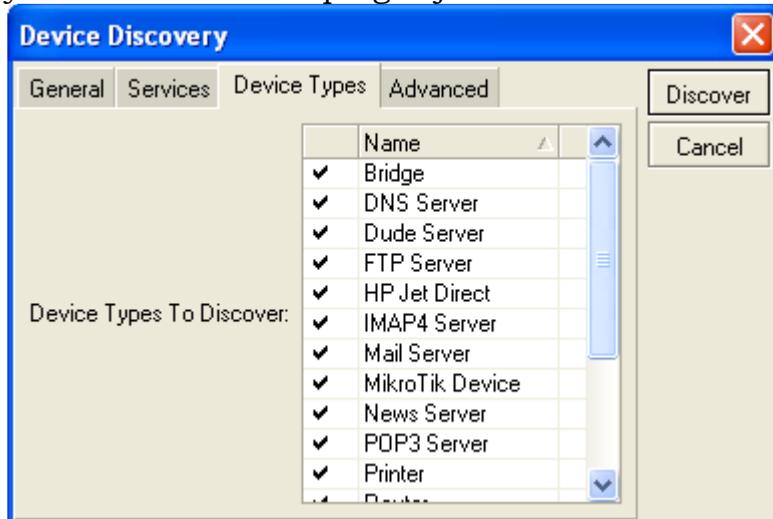
Gambar 7.7 The Dude 6.48.1

2. Dapat dilihat saat kita menjalankan the dude, akan muncul sebuah form (gambar 6.7) Device Discovery form inilah yang akan mencari sebuah alat/komputer pada jaringan yang terhubung dalam satu subnet yaitu 192.168.2.0/24. Range IP yang dicari adalah 192.168.2.1-192.168.2.255. pada “Add Networks to Auto Scan” beri tanda (✓) untuk menampilkan semua network yang terhubung pada jaringan.



Gambar 7.8 Servis Pada Device Discovery

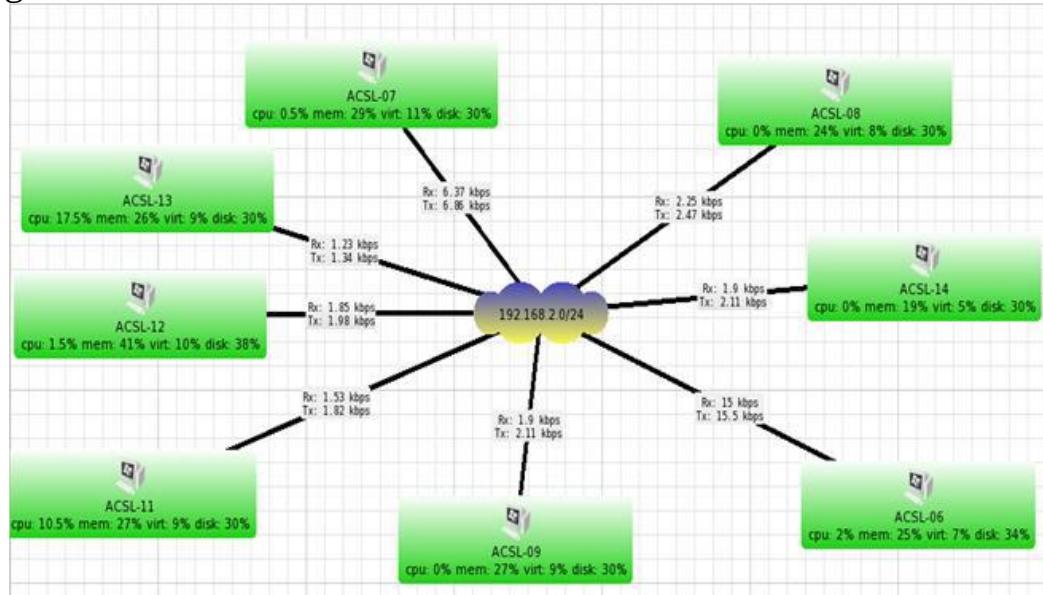
3. Kemudian pada tab services dapat kita lihat apa saja yang bias kita scan servisnya akan tetapi jika kita memakai fast scan maka kita hanya akan scan servis ping saja.



Gambar 7.9 Device Type

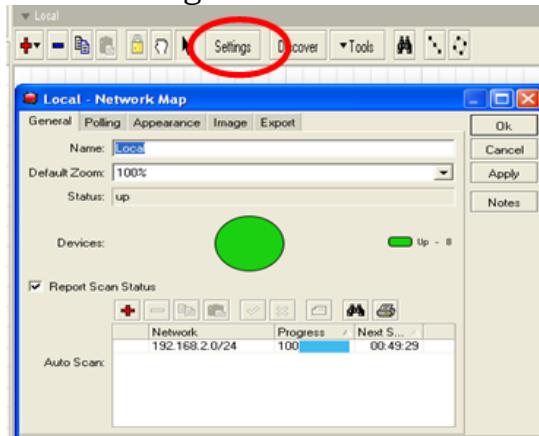
4. Pada tab Device type dapat kita lihat alat/komputer apa saja yang akan discan diantaranya Bridge, FTP Server, Mikrotik Device, Mail Server dan lain-lain. Silakan di pelajari untuk yang lain. Klik discover untuk mulai pencarian alat/komputer.

5. Setelah selesai pencarian alat/komputer maka akan muncul jaringan dalam satu subnet yang kita cari yaitu seperti pada gambar dibawah ini :



Gambar 7.10 Hasil Pencarian The Dude

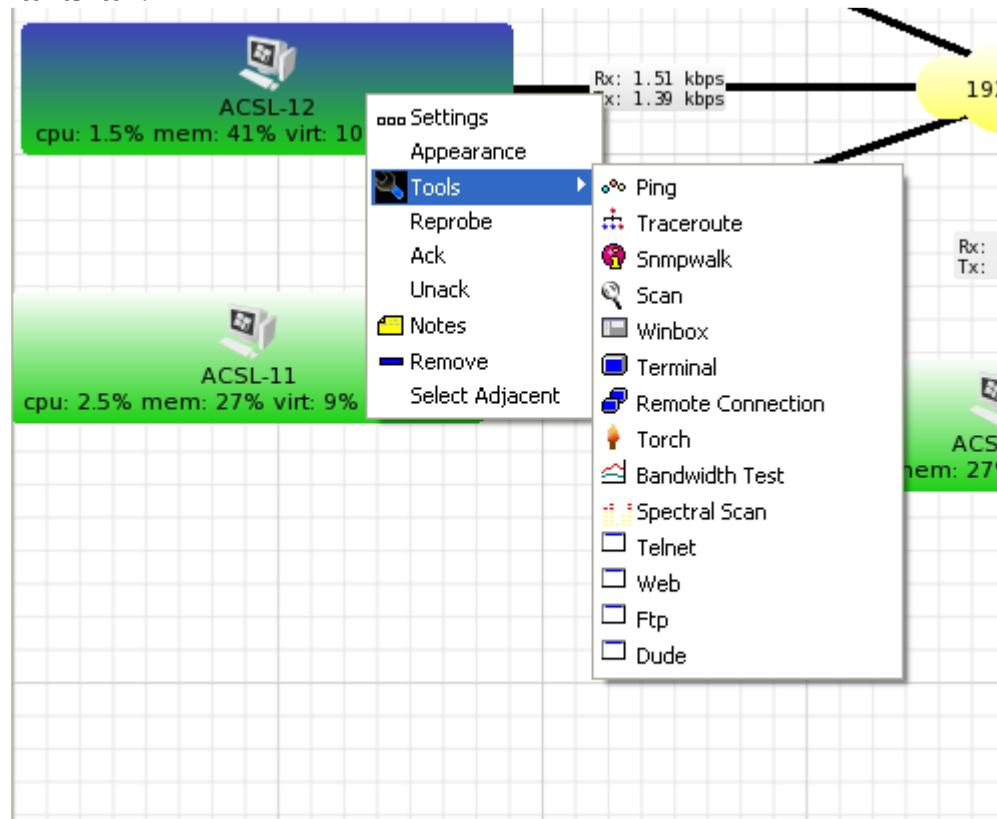
6. Setelah proses pencarian selesai maka akan muncul seperti pada gambar diatas. Sebagai catatan jika komputer dalam sebuah jaringan firewall nya hidup dan icmp echo request nya tidak dihidupkan maka komputer tersebut tidak dapat discan oleh the dude. Pada gambar diatas dapat dilihat seluruh alat/komputer yang terhubung dalam satu jaringan secara otomatis akan termonitoring sehingga kita dapat dengan mudah mengetahui informasi dari setiap PC dengan jaringan mulai dari pengiriman dan penerimaan paket – paket data dan mengetahui device yang ada pada setiap PC. Jika salah satu layanan atau device pada PC mengalami gangguan atau mengalami kerusakan akan terlihat dalam gambar akan berwarna merah, jika semua layanan dan device dalam kondisi baik maka setiap PC akan berwarna hijau seperti yang terlihat dalam gambar.



Gambar 7.11 Local Network-Map

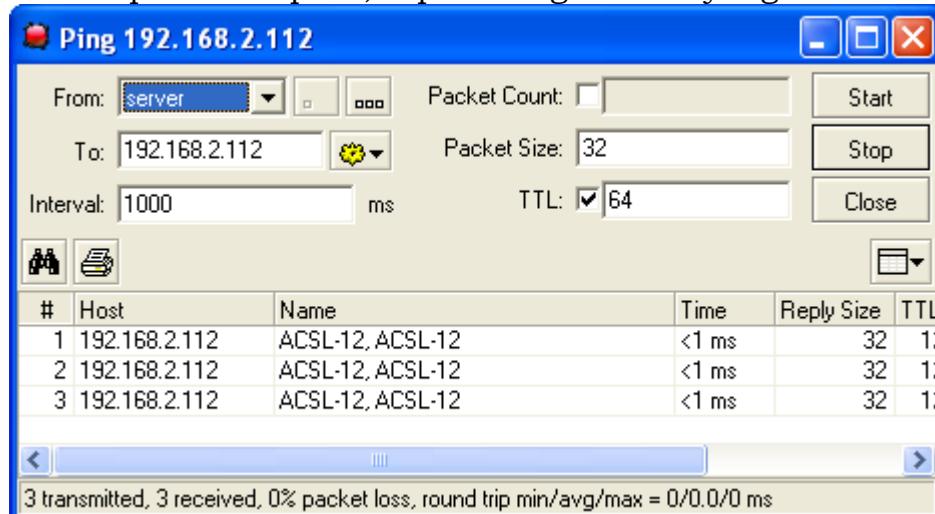


Pada Tab “Settings” akan menampilkan form diatas dimana form tersebut berisi tentang informasi hasil dari scan status yang telah dilakukan.



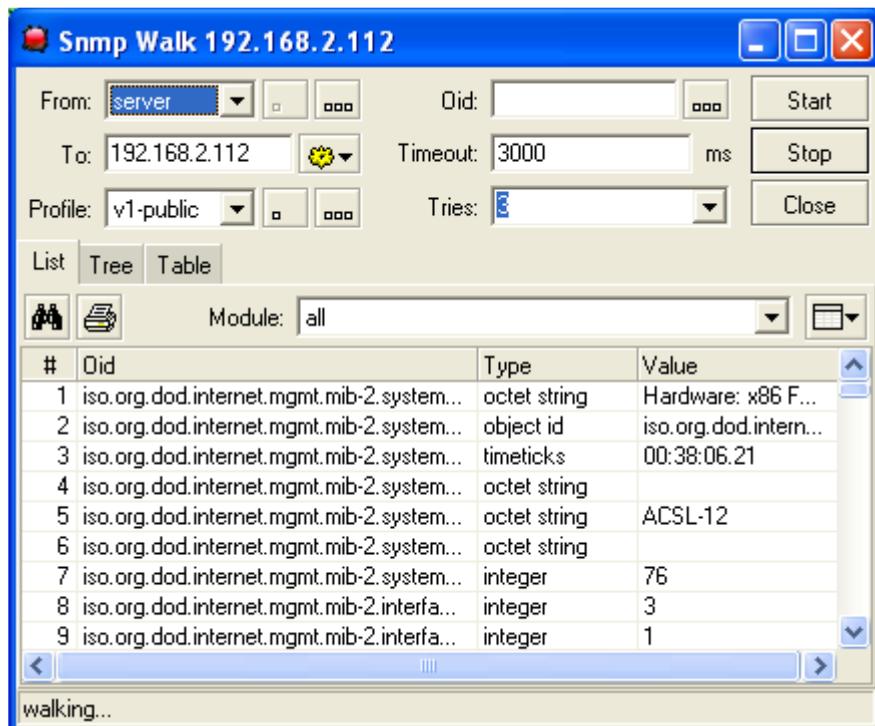
Gambar 6.12 Tools Pada PC

7. Pada gambar diatas menampilkan beberapa tools yang bisa digunakan pada setiap PC, seperti Ping dari PC yang dimonitoring;

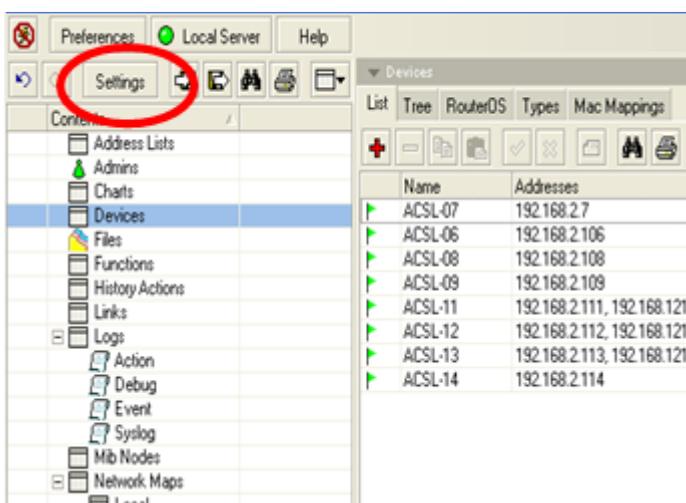


Gambar 7.13 Tes Ping

Snmp Walk : untuk mendapatkan atau memperoleh informasi snmp yang sudah ada dalam masing – masing perangkat didalam jaringan, Snmp Walk merupakan utilitas yang terintegrasi dari snmp.

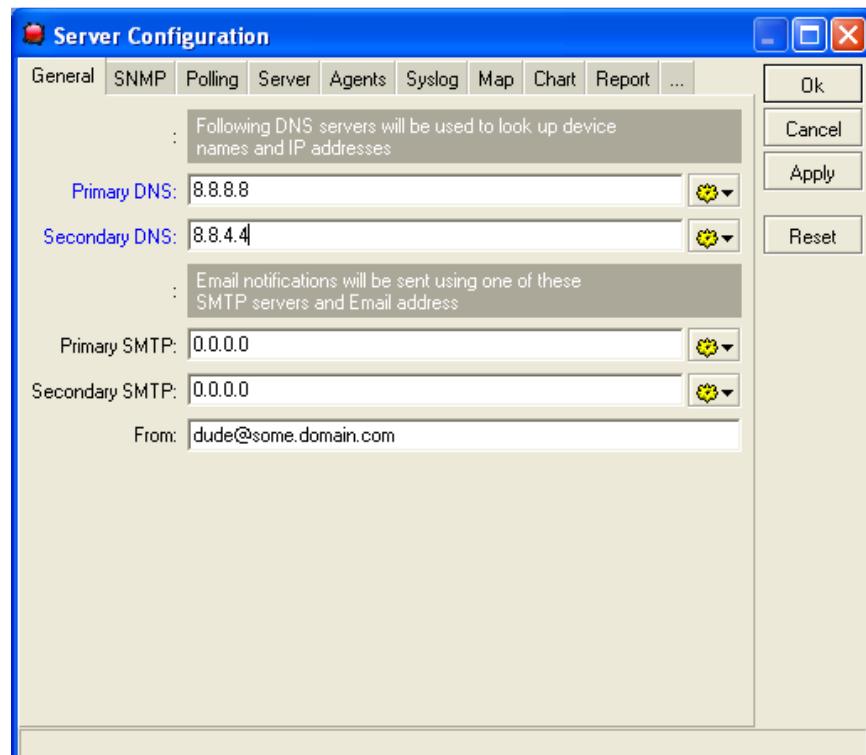


Gambar 7.14 SNMP Walk



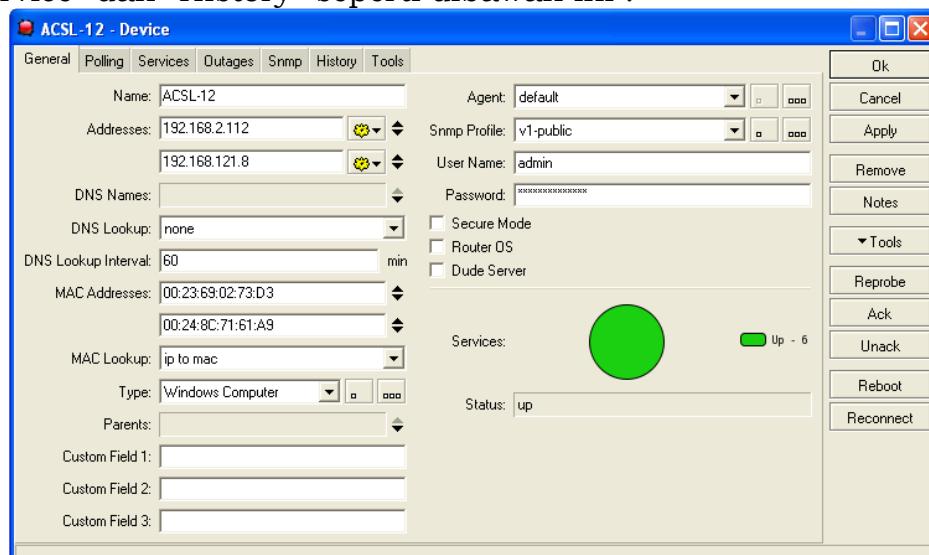
Gambar 7.15 The Dude 6.48.1

Dapat juga dilihat informasi device melalui content yang tersedia dari The Dude dengan melihatnya pada Tab "Device", pada tab "Setting" akan menampilkan beberapa informasi pada Server configuration, seperti dibawah ini :

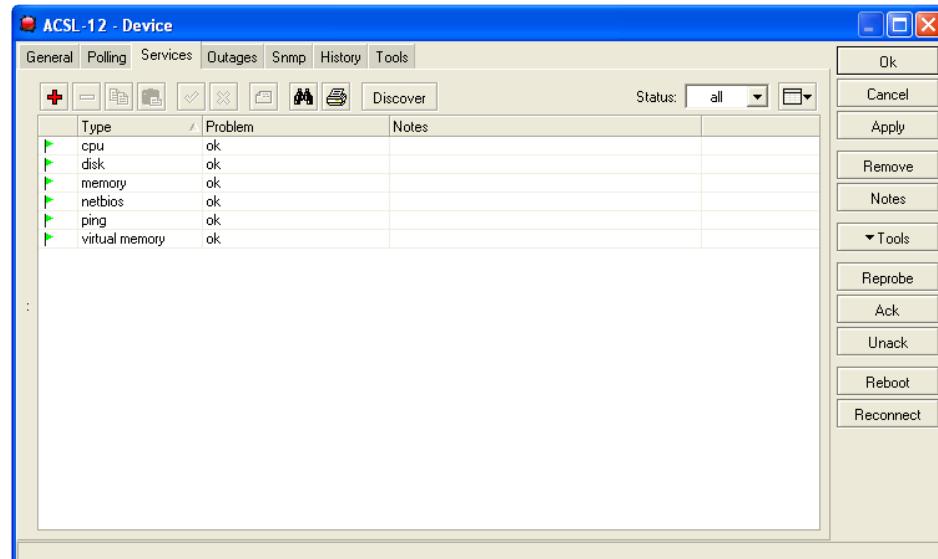


Gambar 7. 16 Server Configuration

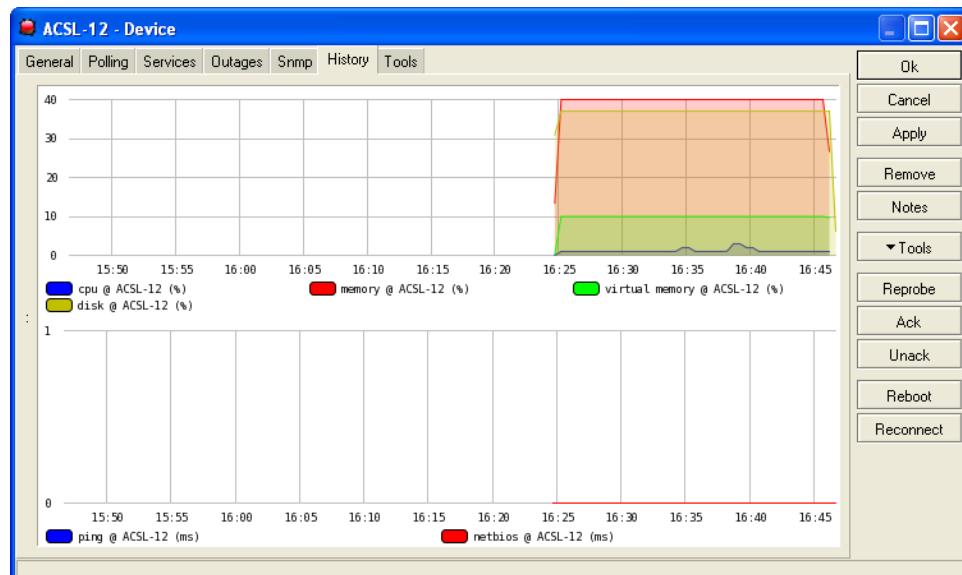
Pada setiap device bisa dilihat informasi – informasi yang terdapat dalam setiap device tersebut, yang terlihat pada Tab “general”, “Service” dan “History” seperti dibawah ini :



Gambar 7.17 Device Pada salah satu PC

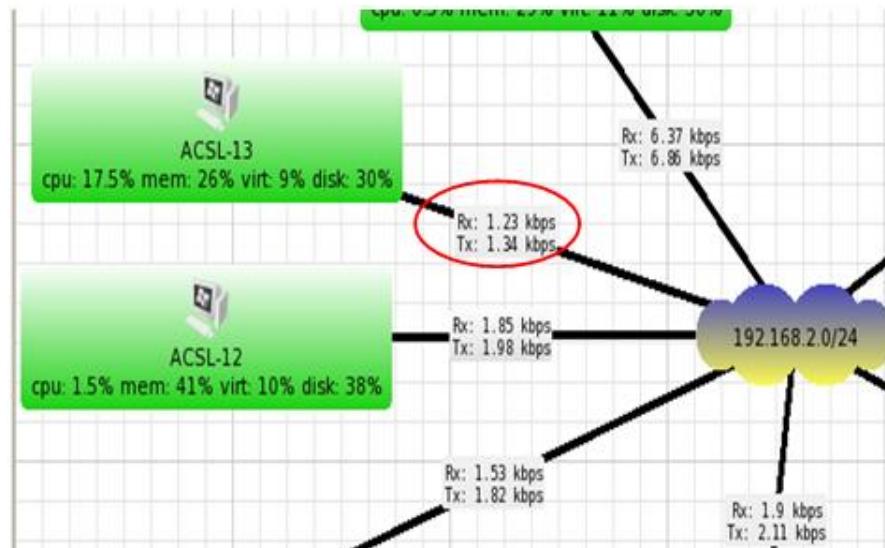


Gambar 7.18 Sevices Pada salah satu PC



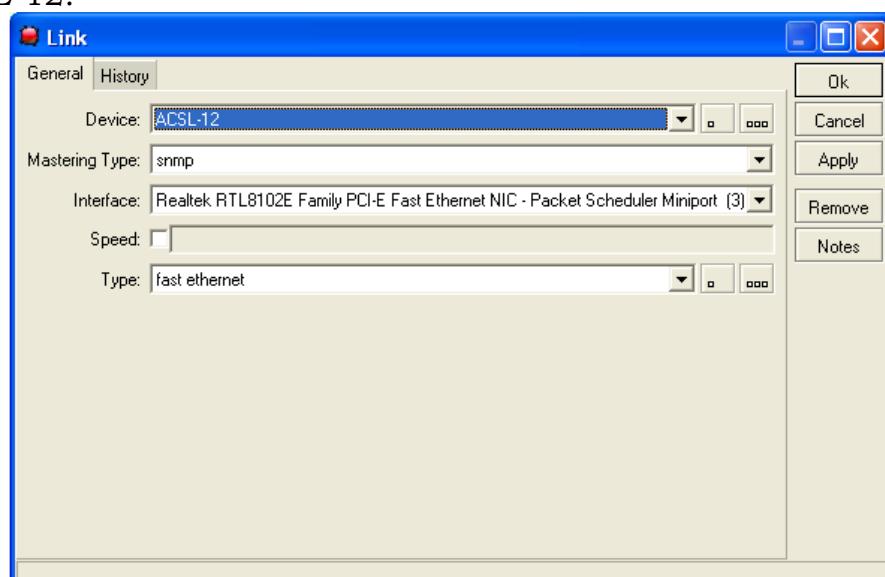
Gambar 7.19 History Pada Salah Satu PC

Pada gambar dibawah, akan menghasilkan informasi tentang interface yang digunakan dan kecepatan dari setiap penerimaan dan pengiriman paket – paket data.



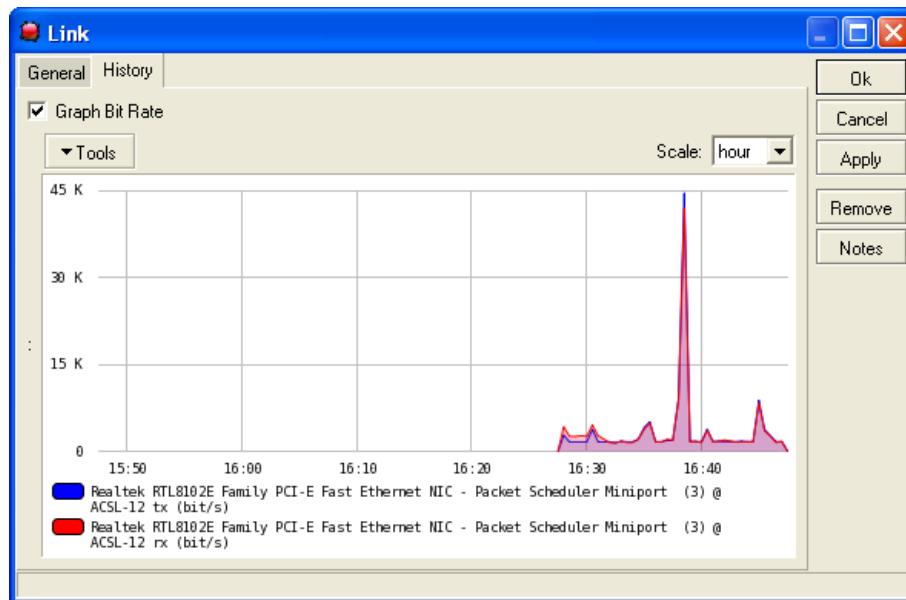
Gambar 7.20 Kecepatan Pda Interface Yang Digunakan

Pada form dibawah menampilkan interface yang terdapat pada ACSL-12.



Gambar 7.21 Interface Pada ACSL-12

Pada Tab "History" akan menampilkan kecepatan pada penerimaan dan pengiriman setiap paket – paket data, seperti dibawah ini :



Gambar 7.22 Kecepatan Pada Pengiriman dan Penerimaan Paket Data

7.3.5. Radmin

Radmin (Remote Administrator) remote control dan akses remote perangkat lunak yang memungkinkan Anda bekerja pada komputer remote seolah-olah Anda sedang duduk tepat di depannya dan mengaksesnya dari beberapa tempat. Radmin menggunakan yang selalu hadir TCP / IP protokol – protokol yang paling luas digunakan di LAN, WAN dan Internet. Ini berarti Anda dapat mengakses komputer remote dari mana saja di dunia. Radmin ditempatkan pada PC ribuan perusahaan di seluruh dunia dan aplikasi Radmin juga dijadikan materi praktikum ITB Ahmad Dahlan Jakarta.

7.3.5.1. Prinsip Operasi Radmin

Radmin terdiri dari dua modul terpisah:

- ➔ Modul Server (Radmin Server): harus diinstal pada komputer yang ingin Anda akses dari jarak jauh.
- ➔ Modul Klien (Radmin Viewer): harus diinstal pada komputer yang ingin Anda gunakan untuk mengakses komputer remote. Namun, isi folder dari modul Klien dipasang dapat disalin dan ditempatkan pada setiap folder lain dan/atau komputer dan komputer ini tidak perlu modul Client diinstal.
- ➔ Semua gerakan mouse dan keyboard sinyal ditransfer dari komputer lokal langsung ke komputer remote melalui jaringan (melalui LAN atau Internet), menyampaikan layar grafis update kembali ke arah lain. Radmin Server menggunakan Driver Cermin (juga dikenal sebagai driver video hook) untuk membaca layar Controller Tampilan Video melewati jarak jauh. Supir cermin memungkinkan untuk hanya membaca bagian mengubah layar.



- Teknologi Direct Screen Transfer baru itu diterapkan pada versi terbaru dari Radmin. Pengembang perangkat lunak yang klaim adaptasi dari driver video baru memungkinkan Radmin untuk secara dramatis meningkatkan tingkat update layar dengan utilisasi CPU minimal. Fitur keamanan dapat ditambahkan seperti user prompt dan keterbatasan pada apa yang pengguna dapat dilakukan. Beberapa account pengguna dapat menciptakan segala dengan hak akses yang berbeda.

7.3.6. Sejarah Radmin

Remote Administrator pada awalnya dikembangkan oleh Dmitry Znosko pada tahun 1999. Saat ini ia adalah CEO Famatech. Administrator terpencil 2.2 dirilis 16 Juni 2004. Para pengguna dan pengembang memperpendek nama perangkat lunak untuk Radmin. Versi saat ini resmi disebut Radmin 3 dan dirilis 13 Februari 2007.

Minor update Radmin 3.01 dirilis 3 Juli 2007. Versi Radmin 3.1 dengan 64-bit versi mendukung Windows dirilis pada 2 November 2007. Versi Radmin 3.2 keluar 25 April 2008 dan mendukung Windows Vista SP1 kedua edisi 32-bit dan 64-bit dan Windows Server 2008.

Dalam Radmin 3.3. dirilis 19 November 2008 dukungan untuk fitur Intel AMT diperkenalkan. Versi saat ini Radmin 3.4 yang mendukung Windows 7 (32 - dan 64-bit) dan Windows Server 2008 R2. Versi Sebelumnya kompatibilitas : Para penampil Radmin 3.x dapat beroperasi dengan perangkat lunak server yang sebelumnya 2.2, meskipun beberapa fitur baru seperti chatting tidak akan tersedia.

Tabel 7.1 Versi Radmin 2.x dan 3.x

-	Radmin Server 3.x	Radmin Server 2.x
Radmin Viewer 3.x	Yes	Yes
Radmin Viewer 2.x	No	Yes

Operasi sistem pendukung (32-bit dan 64-bit edisi, versi 3.2

Tabel 7.2 Versi Radmin 3.4

-	Windows 7	Windows Vista	Windows 2008	Windows XP	Windows 2003
Radmin Server 3.4	Yes	Yes	Yes	Yes	Yes
Radmin Server 2.x	No	No	No	Yes	Yes
Radmin Viewer 3.4	Yes	Yes	Yes	Yes	Yes
Radmin Viewer 2.x	No	No	No	Yes	Yes



7.3.7. Fitur-Fitur Pada Radmin

Beberapa fiturnya

- a. Penemuan dan tata letak jaringan otomatis
- b. Menemukan semua jenis atau merek perangkat
- c. Perangkat, Pemantauan tautan, dan pemberitahuan
- d. Termasuk ikon SVG untuk perangkat, dan mendukung ikon dan latar belakang khusus
- e. Instalasi dan penggunaan yang mudah
- f. Memungkinkan Anda menggambar peta Anda sendiri dan menambahkan perangkat khusus
- g. Mendukung pemantauan SNMP, ICMP, DNS dan TCP untuk perangkat yang mendukungnya
- h. Pemantauan dan grafik penggunaan Tautan Individu
- i. Akses langsung ke alat kendali jarak jauh untuk manajemen perangkat
- j. Mendukung server Dude jarak jauh dan klien lokal
- k. Berjalan di lingkungan Linux Wine, MacOS Darwine, dan Windows

Secara teknologi Radmin mampu memberikan sebuah layanan dimana Radmin adalah salah satu yang paling aman, solusi tercepat dan paling populer akses remote perangkat lunak yang dirancang untuk Windows. Sebuah layar komputer remote dapat dilihat pada monitor lokal baik jendela atau tampilan layar penuh. Semua gerakan mouse dan penekanan tombol akan ditransfer langsung ke komputer remote. File dapat ditransfer ke dan dari komputer remote, dan komunikasi dengan pengguna komputer remote dimungkinkan dengan baik Text Obrolan atau Voice Chat ;

- a. Kecepatan kerja tinggi

Radmin adalah software remote control tercepat yang tersedia. Teknologi baru DirectScreenTransfer™ yang menggunakan video hook kernel mode driver untuk meningkatkan tingkat capture untuk ratusan update layar per detik. Khusus optimasi bandwidth rendah memungkinkan Anda mengontrol komputer remote nyaman bahkan pada modem dial-up dan koneksi GPRS.

- b. Tingkat Keamanan Tertinggi

Radmin bekerja dalam modus terenkripsi dimana semua data, gambar layar, gerakan mouse dan keyboard sinyal yang dienkripsi menggunakan 256-Bit AES enkripsi yang kuat dengan kunci yang dihasilkan secara acak untuk setiap koneksi ke komputer remote. Untuk otentifikasi pengguna Radmin dapat menggunakan Windows keamanan dengan Active Directory dan dukungan Kerberos, atau keamanan sendiri dengan izin pengguna individu dan aman otentifikasi login / password. Keamanan Radmin menggunakan Diffie-Hellman berbasis pertukaran kunci dengan 2048-bit ukuran kunci. filter IP tambahan membatasi akses ke host dan jaringan tertentu.



- c. Hardware remote control dengan dukungan Intel® AMT
Versi baru dari Radmin 3.5 mendukung Intel® AMT (Active Manajemen Teknologi) dan memungkinkan untuk mengontrol komputer remote bahkan jika itu dimatikan atau Anda tidak dapat memulai sistem operasi. Menggunakan Radmin Viewer Anda dapat mengaktifkan, restart dan mematikan komputer remote. Hal ini juga memungkinkan pengguna untuk melihat dan mengubah pengaturan BIOS dari komputer remote dan untuk boot dari CD atau disk file gambar lokal.
- d. Kompatibilitas penuh dengan Windows 10
Radmin 3.5 mendukung sepenuhnya Windows 10 32-bit dan 64-bit, termasuk User Account Control dan Fast User Switching. Radmin Server 3.5 mendukung Windows 10/8/7 / Vista / XP / 2012/2008/2003/2000 (32-bit) dan Windows 10/8/7 / Vista / XP / 2012/2008/2003 (64-bit) operasi sistem. Radmin Viewer 3.5 mendukung Windows 10 / 8 / 7 / Vista / XP / 2012 / 2008 / 2003 / 2000 / ME / 98/95 / NT4.0 (32-bit) dan Windows 10 / 8 / 7 / Vista / XP / 2012 / 2008 / 2003 (64-bit) sistem operasi.
- e. Teks dan Voice Chat
Teks Chat, Voice Chat dan Send Message, yang baru untuk Radmin versi 3, semua dikembangkan untuk membantu Anda berkomunikasi dengan orang yang mengoperasikan komputer remote yang terhubung dengan Anda.
- f. Mudah digunakan
Radmin adalah sangat user-friendly. Sebagian besar pengguna kami setuju bahwa keunggulan Radmin adalah kesederhanaannya. Semua melaporkan bahwa antarmuka yang intuitif dan program ini sangat mudah digunakan. Tidak seperti bloatware, Radmin tidak sia-sia 'nilai tambah' fitur yang membuatnya sulit untuk bekerja dengan, kompleks untuk belajar, atau yang meremukkan kinerjanya. Mengontrol komputer remote dengan mudah dengan Radmin!
- g. Mengamankan "Drag and Drop" file transfer dengan fitur "Delta Copy"
Dengan Radmin Anda dapat men-drag and drop file melalui antarmuka Explorer seperti untuk atau dari komputer remote dalam mode terenkripsi. Radmin memiliki fitur menggunakan ketika menyalin file yang memungkinkan memperbarui hanya bagian dari sebuah file yang berbeda pada kedua mesin. Fitur ini disebut "Delta Copy" karena hanya perbedaan antara file ('delta') disalin. Ini memungkinkan Anda terus menyalin setelah kesalahan jaringan dari tempat di mana kesalahan terjadi bukan dari awal. Fitur ini digunakan secara otomatis ketika ada file yang disalin ke atau dari mesin remote.
- h. Beberapa Koneksi Dukungan
Radmin mendukung beberapa koneksi simultan ke layar remote yang sama. Ini berarti bahwa Anda dapat mengundang teman atau kolega untuk melihat layar Anda dari jarak jauh (sangat



berguna untuk konferensi) atau Anda dapat melihat atau mengontrol beberapa komputer jauh dari layar komputer Anda sendiri (sangat berguna untuk helpdesk terpencil atau mengajar).

7.3.8. Tahap Instalasi Pada Penggunaan

1. Bagi yang belum punya aplikasi RAdmin 3.5, silahkan download terlebih dahulu di situs resminya www.radmin.com.
2. Jika sudah selesai didownload, maka akan terdapat dua file **rserv35** dan **rview35**.
 - Untuk **rserv35** di install di komputer server yang akan mengontrol dan meremote komputer client dari jarak jauh.
 - Untuk **rview35** di install di komputer client yang akan dikontrol dan diremote.

Radmin Server 3.5

1. Untuk memulai proses Install **Radmin Server 3.5**, double klik pada **rserv35**.



Gambar 7.23 Instalasi Radmin

2. Lalu akan muncul jendela **Welcome to the InstallShield Wizard for Radmin Server 3.5**, lalu klik **Next**.



Gambar 7.24 InstalShield Wizard



- Selanjutnya, pilih **I accept the terms in the license agreement**, dan klik **Next**.



Gambar 7.25 I Accept the Tems

- Pada tampilan **Ready to Install the Program** seperti di bawah ini, klik **Install**.



Gambar 7.26 Ready to Install

- Selanjutnya ketika di klik **Install** akan muncul proses seperti di bawah ini.



Gambar 7.27 proses install

6. Tunggu sampai proses selesai dan klik **Finish**.



Gambar 7.28 Instalasi Finish

7.3.9. Tahap Instalasi Pada Server

Lakukan setting pada Radmin Server :

1. Klik **Permissions ...**



Gambar 7.29 Radmin Server

2. Pada tampilan **Radmin Server Security Mode**, default **Set user/password verification mode** adalah pada **Radmin security**, kemudian klik tombol **Permissions**.



Gambar 7.30 Radmin Server Security

3. Tambahkan **Radmin Users** dengan cara klik **Add User**



Gambar 7.31 Radmin Users

4. Masukkan **User name**, **Password**, dan juga **Confirm password**, lalu klik **OK**.



Gambar 7.32 User name dan Password

5. Setelah **Radmin Users** ditambahkan, centang pada **All Access** maka secara otomatis semua **Allow** akan tercenteng. Klik **OK**.

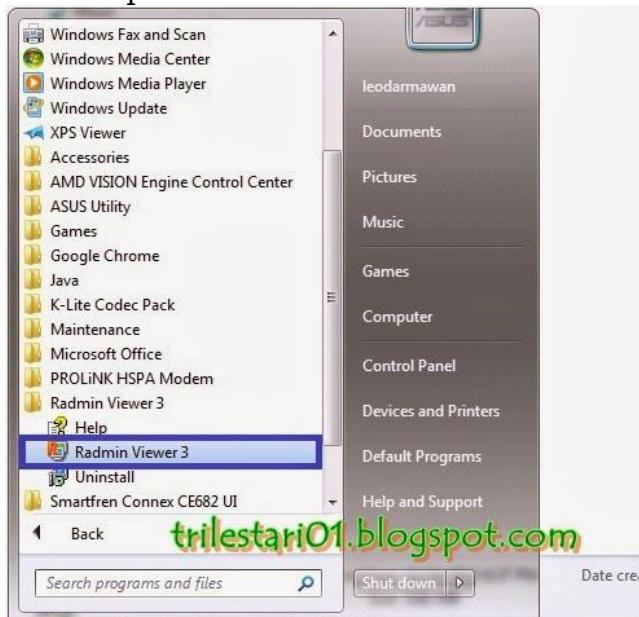


Gambar 7.33 Radmin Users



Langkah Me-remote Komputer :

- Untuk mulai me-remote komputer client, buka software **RAdmin Viewer** pada komputer client.



Gambar 7.34 remote compute client

- Koneksikan komputer server ke komputer client dengan mengklik menu **Connection** dan memilih opsi **Connect to**.



Gambar 7.35 Connection

- Klik kotak kombo **Connection type** dan pilih jenis koneksi **Full Control** untuk mengontrol atau dan meremote komputer client. Lalu ketikkan IP Address atau DNS Name komputer client yang akan diremote. Jika sudah, klik tombol **OK**.



Gambar 7.36 Connect to Client

4. Setelah memasukkan IP Address, maka komputer client dapat diremote oleh komputer server.

7.4 Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
3. Kabel
4. Router
5. Switch
6. Hub
7. Aplikasi Packet Tracer
8. Software virtualisasi (VMware)
9. Software The Dude
10. Software Radmin

7.5 Praktikum

1. Simulasi Network Management The Dude by Mikrotik
2. Simulasi network Management The Radmin

7.6 Referensi

1. Ariyus, Dony & Rum Andri K.R, Komunikasi Data. 2008. Yogyakarta : Penerbit Andi. Kurniawan, Wiharsono, Jaringan Komputer. 200. Yogyakarta : Penerbit Andi.
2. Nurjaman, Yoga. Pengembangan Sistem Remote Access Jaringan Berbasis Client Server. 2012. Jurnal Algoritma, Sekolah Tinggi
3. Soetedjo Dharma Oetomo, Budi, dkk. 2006. Konsep & Aplikasi Pemrograman Client Server dan Sistem Terdistribusi. Penerbit



- Andi. Sutisna, Nia. 2008. E-Learning Makalah Inovasi Pendidikan, Prodi Pasca Sarjana Pendidikan Luar Sekolah, Universitas Pendidikan Indonesia, Bandung,
4. Tittel, Ed. 2004. Computer Networking. Jakarta : Erlangga.
 - Wahana Komputer. 2005. Pintar Menjadi Administrator Jaringan Komputer. Yogyakarta : Penerbit Andi.
 5. Enterprise, Jubilee. 2010. Teknik Mengendalikan PC dari Jarak Jauh. Jakarta: PT Elex Media Komputindo

7.7 Tugas

Download link berikut ini !

<https://www.mediafire.com/file/x6rfo20c0sx1nbb/MONITORING+NETWORK+DENGAN+THE+DUDE.doc/file>

Kemudian ikuti setiap langkah – langkah yang diberikan dalam panduan tugas tersebut !

7.8 Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, MODUL I PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Bottom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



MODUL VIII

WINDOWS SERVER 2016

8.1 Tujuan Praktikum

1. Dapat mengetahui cara – cara menginstall Windows Server 2016 dengan benar
2. Dapat mengetahui cara menambah user
3. Dapat mengetahui cara mengganti hostname
4. Dapat mengetahui cara mengatur partisi harddisk
5. Dapat mengetahui cara mengubah IP address pada Windows Server 2016

8.2 Indikator Pencapaian

1. Mampu menginstalasi Windows Server 2016
2. Mampu mengonfigurasi DNS dan DHCP Server
3. Mampu mengkonfgurasi Windows Server 2016 pada Virtual Box

8.3 Materi

8.3.1. Pengenalan Windows Server 2016

Windows server 2016 adalah system operasi terbaru dari Microsoft yang didesain untuk memenuhi kebutuhan komputasi yang mutakhir. Dimana memiliki fitur dan service sebagai server dalam mengelola client di suatu jaringan. Beberapa service yang biasa digunakan adalah : DNS, DHCP server, Active Directory, Fileserver, maupun sebagai printer server.

Dimana untuk windows server 2016 mengusung slogan: Aman, Berkembang dan Menginovasi. Dengan masih memegang konsep yang sama dengan versi 2012, windows server 2016 hadir dengan versi GUI dan core.

Beberapa fitur di Windows Server 2016:

1. Server Core dan Desktop Experience
Masih menggunakan fitur yang ada di windows server sebelumnya dimana, dapat diinstall sebagai Server Core dan GUI.
2. Virtualisasi
Hyper-V yang berfungsi sebagai virtualisasi, dimana kita dapat memasang beberapa server yang terpisah. Terbaru, format konfigurasi mesin virtual biner lebih efisien (*.VMCX untuk data konfigurasi mesin virtual dan *.VMRS untuk data status durasi)
3. Internet Information Services 10 (IIS 10)
Dilengkapi dengan Internet Information Service 10 dan .NET Framework 4.6 yang mendukung HTTP/2. Tingkat keamanan yang tinggi Windows Server 2016 mengklaim aman dari serangan dan adanya pencegahan kegagalan system.



Berikut minimum spesifikasi hardware yang dibutuhkan oleh windows server 2016:

Tabel 8.1 Kebutuhan System

Komponen	Kebutuhan
Prosesor	1.4GHz 64-bit processor
Memori	512 MB (2GB untuk Desktop Experience)
Ruang Hardisk	32GB
Drive	DVD
Display	VGA (1024x768)
Lainnya	Keyboard dan Mouse

Windows Server 2016 merupakan rilis terbaru dari sistem operasi Windows Server dari Microsoft yang secara umum dirilis pada tanggal 12 Oktober 2016. Tujuan Microsoft dengan Windows Server 2016 adalah untuk lebih mengasimilasi resource lokal dengan infrastruktur public cloud dan private cloud untuk memberikan tingkat pengelolaan yang lebih tinggi terhadap berbagai lingkungan komputasi baik fisik maupun virtual. Sekaligus menjaga agar bisnis dan pengguna menjadi lebih produktif.

Windows Server 2016 hadir dengan beberapa perubahan penting pada intinya dan banyak fitur baru dalam upaya meningkatkan keamanannya. Beberapa fitur diantaranya:

1. Nano Server: Serupa dengan mode Windows Server Core, Nano Server harus dikelola secara remote, karena tidak menyediakan kemampuan logon lokal dan hanya mendukung aplikasi 64-bit. Nano Server dioptimalkan untuk penggunaan di private cloud dan data center, serta menjalankan web service, seperti DNS atau IIS.
2. Windows Containers: Tidak seperti virtual machine, container memungkinkan virtualisasi pada system-level dengan menyediakan cukup akses ke OS, library, dan resource untuk meng-host aplikasi di dalam user-space yang terisolasi.
3. Active Directory Domain Services: Privileged Access Management (PAM) membantu untuk mengatasi pencurian informasi kredensial dengan menggunakan Microsoft Identity Manager (MIM) untuk melindungi Active Directory (AD) dari akun dengan hak privileged access.
4. Active Directory Federation Services (ADFS): Terus menyediakan gabungan identitas yang simpel, aman dan Single Sign-On (SSO) antara ADFS-secured enterprises dan organisasi mitra. Di versi 2016 memiliki kemampuan untuk mengotentikasi pengguna yang tersimpan di LDAP atau cloud-based providers.
5. Hyper-V: Memperkenalkan manajemen dari virtual networking adapter dan memori untuk virtual machine. Versi 2016 juga memasukan shielded virtual machine untuk meminimalkan gangguan atau pencurian data dan status virtual machine dengan mengenkripsi keduanya dan mencegah pemeriksaan sinyal video dan disk.



6. Windows Defender: Aplikasi Windows Server Antimalware terinstal secara default pada Windows Server 2016, untuk mendeteksi dan menetralkan ancaman malware secara real time dengan update otomatis.
7. Storage Spaces Direct: Memungkinkan membangun penyimpanan dengan ketersedian yang tinggi dari sistem local storage.
8. PowerShell 5.0: Terdiri dengan memperkenalkan cmdlets baru, dan module untuk remote management dan scripting dari client, server dan applications.

Sebagai tambahan fitur baru, metode instalasi juga telah dimodifikasi sedemikian rupa. Sehingga secara default versi Server Core dari OS akan terinstal. Hal ini untuk meminimalkan serangan dengan menghapus GUI dan pilihan instalasi yang tidak perlu.

Untuk percobaan Lab , ISO Microsoft bisa di download pada :

<https://www.microsoft.com/en-us/evalcenter>

8.3.2. Edisi Windows Server 2016

Versi Windows Server 2016, terbagi atas 3 versi:

1. Windows Server 2016 Datacenter , Edisi ini ditujukan untuk Enterprise yang menggunakan high Virtualisasi data center atau cloud provider.
2. Windows Server 2016 Standard , Edisi ini ditujukan untuk perusahaan kelas menengah yang menggunakan server en-premises untuk menjalankan network services mereka.
3. Windows Server 2016 Essentials , Edisi ini ditujukan untuk perusahaan kecil yang hanya menggunakan single server dalam usahanya.

Feature	Datacenter	Standard
Core functionality of Windows Server	yes	yes
OSes / Hyper-V containers	unlimited	2
Windows Server containers	unlimited	unlimited
Host Guardian Service	yes	yes
Nano Server installation option	yes	yes
Storage features including Storage Spaces Direct and Storage Replica	yes	no
Shielded Virtual Machines	yes	no
Software Defined Networking Infrastructure (Network Controller, Software Load Balancer, and Multi-tenant Gateway)	yes	no

Gambar 8.1 Versi Windows Server 2016



8.3.3. Active Directory

Active Directory adalah directory service yang menyimpan konfigurasi jaringan baik user, group, komputer, hardware, serta berbagai policy keamanan dalam satu database terpusat. Peranan Active Directory dalam jaringan dapat diumpamakan sebagai buketelepon, yang menyimpan daftar alamat dalam informasi penting untuk mengenali berbagai obyek dalam jaringan ;

1. Active Directory adalah layanan direktori yang dimiliki oleh sistem operasi jaringan Microsoft Windows 2000, Windows XP, Windows Vista dan Windows Server 2008 2012 dan 2016.
2. Active Directory terdiri atas basis data dan layanan direktori,, Basis data yang dimiliki oleh Active Directory yaitu menyimpan segala sumber daya yang terdapat dalam jaringan dan dalam satu domain.
3. DNS (Domain Name System) merupakan komponen utama yang harus ada dalam domain windows. Tanpa DNS kita tidak bisa membuat Domain. Domain bisa diartikan sebagai kumpulan dari komputer dalam satu grup yang sama dan saling berbagi resource dengan management terpusat melalui DC.

Fasilitas Active Directory Domain Services berperan penting pada system operasi windows server 2008, juga dapat memberikan sebuah keamanan akses security yang dikelola secara infrastruktur yang canggih. ADDS menyediakan distribusi database yang menyimpan dan mengelola informasi tentang jaringan serta aplikasi yang digunakan.

Fasilitas Active Directory User and Computer berperan untuk memberikan hak akses sumber daya jaringan kepada para pengguna, maka harus dibuat user dan grup untuk tiap – tiap pengguna. Windows server 2016 mengenali seorang pengguna serta hak yang dimilikinya berdasarkan user dan grup yang telah dibuat.

Secara default, computer akan menyediakan dua buah account user serta beberapa grup account. User account yang disediakan adalah user administrator dan user guest. Beberapa account dapat digabungkan dalam satu grup yang berfungsi mengelompokkan account ke dalam suatu kelompok tertentu sesuai dengan hak yang diberikan.

8.3.4. DNS Server

DNS (Domain Name System) adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surel (email) untuk setiap domain. DNS menyediakan servis yang cukup penting untuk Internet, bilamana perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalamatan dan penjaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan



alamat surel. Analogi yang umum digunakan untuk menjelaskan fungsinya adalah DNS bisa dianggap seperti buku telepon internet dimana saat pengguna mengetikkan www.indosat.net.id di peramban web maka pengguna akan diarahkan ke alamat IP 124.81.92.144 (IPv4) dan 2001:e00:d:10:3:140::83 (IPv6).

8.3.5. DHCP Server

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti default gateway dan DNS server.

8.3.5.1. Cara Kerja DHCP Server

Karena DHCP merupakan sebuah protokol yang menggunakan arsitektur client/server, maka dalam DHCP terdapat dua pihak yang terlibat, yakni DHCP Server dan DHCP Client. DHCP server merupakan sebuah mesin yang menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. DHCP client merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server.

DHCP server umumnya memiliki sekumpulan alamat yang diizinkan untuk didistribusikan kepada klien, yang disebut sebagai DHCP Pool. Setiap klien kemudian akan menyewa alamat IP dari DHCP Pool ini untuk waktu yang ditentukan oleh DHCP, biasanya hingga beberapa hari.

Manakala waktu penyewaan alamat IP tersebut habis masanya, klien akan meminta kepada server untuk memberikan alamat IP yang baru atau memperpanjangnya. DHCP Client akan mencoba untuk mendapatkan "penyewaan" alamat IP dari sebuah DHCP server dalam proses empat langkah berikut:

1. **DHCPDISCOVER:** DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.
2. **DHCPOFFER:** Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.
3. **DHCPREQUEST:** Client meminta DCHP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.
4. **DCHPACK:** DHCP server akan merespons permintaan dari klien dengan mengirimkan paket acknowledgment. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP



lainnya) kepada klien, dan memperbarui basis data database miliknya. Klien selanjutnya akan memulai proses binding dengan tumpukan protokol TCP/IP dan karena telah memiliki alamat IP, klien pun dapat memulai komunikasi jaringan.

Empat tahap di atas hanya berlaku bagi klien yang belum memiliki alamat. Untuk klien yang sebelumnya pernah meminta alamat kepada DHCP server yang sama, hanya tahap 3 dan tahap 4 yang dilakukan, yakni tahap pembaruan alamat (address renewal), yang jelas lebih cepat prosesnya.

Berbeda dengan sistem DNS yang terdistribusi, DHCP bersifat stand-alone, sehingga jika dalam sebuah jaringan terdapat beberapa DHCP server, basis data alamat IP dalam sebuah DHCP Server tidak akan direplikasi ke DHCP server lainnya. Hal ini dapat menjadi masalah jika konfigurasi antara dua DHCP server tersebut berbenturan, karena protokol IP tidak mengizinkan dua host memiliki alamat yang sama.

Selain dapat menyediakan alamat dinamis kepada klien, DHCP Server juga dapat menetapkan sebuah alamat statik kepada klien, sehingga alamat klien akan tetap dari waktu ke waktu.

Catatan: DHCP server harus memiliki alamat IP yang statis.

8.3.5.2. DHCP Scope

DHCP Scope adalah alamat-alamat IP yang dapat disewakan kepada DHCP client. Ini juga dapat dikonfigurasikan oleh seorang administrator dengan menggunakan peralatan konfigurasi DHCP server. Biasanya, sebuah alamat IP disewakan dalam jangka waktu tertentu, yang disebut sebagai DHCP Lease, yang umumnya bernilai tiga hari.

Informasi mengenai DHCP Scope dan alamat IP yang telah disewakan kemudian disimpan di dalam basis data DHCP dalam DHCP server. Nilai alamat-alamat IP yang dapat disewakan harus diambil dari DHCP Pool yang tersedia yang dialokasikan dalam jaringan. Kesalahan yang sering terjadi dalam konfigurasi DHCP Server adalah kesalahan dalam konfigurasi DHCP Scope.

8.3.5.3. DHCP Lease

DHCP Lease adalah batas waktu penyewaan alamat IP yang diberikan kepada DHCP client oleh DHCP Server. Umumnya, hal ini dapat dikonfigurasikan sedemikian rupa oleh seorang administrator dengan menggunakan beberapa peralatan konfigurasi. DHCP Lease juga sering disebut sebagai Reservation.

8.3.5.4. DHCP Options

DHCP Options adalah tambahan pengaturan alamat IP yang diberikan oleh DHCP ke DHCP client. Ketika sebuah klien meminta alamat IP kepada server, server akan memberikan paling tidak sebuah alamat IP dan alamat subnet jaringan. DHCP server juga dapat dikonfigurasikan sedemikian rupa agar memberikan tambahan informasi kepada klien,



yang tentunya dapat dilakukan oleh seorang administrator. DHCP Options ini dapat diaplikasikan kepada semua klien, DHCP Scope tertentu, atau kepada sebuah host tertentu dalam jaringan.

8.3.6. Virtual Box

Oracle VM VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Sebagai contoh, jika seseorang mempunyai sistem operasi MS Windows yang terpasang di komputernya, maka seseorang tersebut dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi MS Windows.

Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada.

8.3.7. Proses Instalasi Windows Server 2016 DiVirtualBox

Proses instalasi windows server 2016 cukup mudah dibandingkan dengan versi sebelumnya. Proses instalasi windows server 2016 hampir sama dengan instalasi windows vista, meskipun ada beberapa konfigurasi yang membedakan. Pilihan Tipe Instalasi

Pada proses instalasi windows server 2016 terdapat dua pilihan tipe, pilihan tersebut merupakan fasilitas yang dapat digunakan untuk memaksimalkan fitur yang ada di dalamnya sesuai dengan kebutuhan yang diperlukan, pilihan tersebut adalah :

1. Full Installation

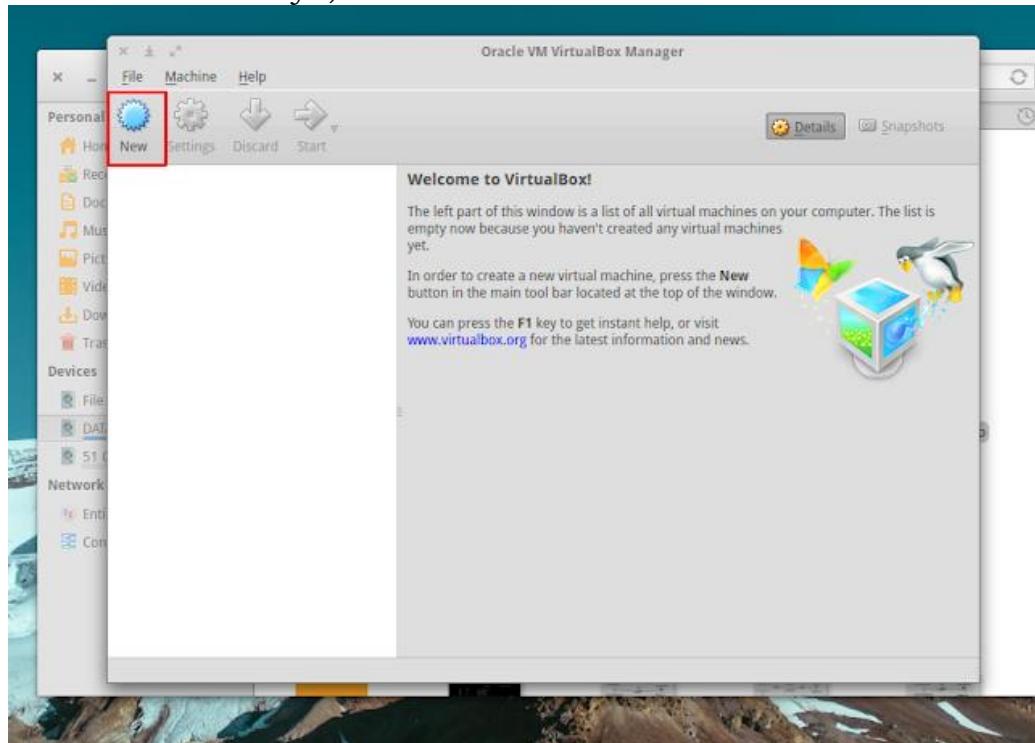
Merupakan pilihan untuk melakukan instalasi secara normal dan lengkap dengan fasilitas –fasilitas serta fitur – fitur yang dimiliki oleh windows server 2008

2. Server Core Installation

Merupakan jenis pilihan, dimana proses instalasi berfokus pada role dan meminimalkan komponen yang digunakan. Diantara komponen yang tidak dilakukan instalasi adalah desktop shell (tanpa wallpaper, screensever), windows explorer, .NET Framework, MMC Console (tanpa Administrative tools dalam start menu), control panel, internet explorer, windows mail, dan search windows.

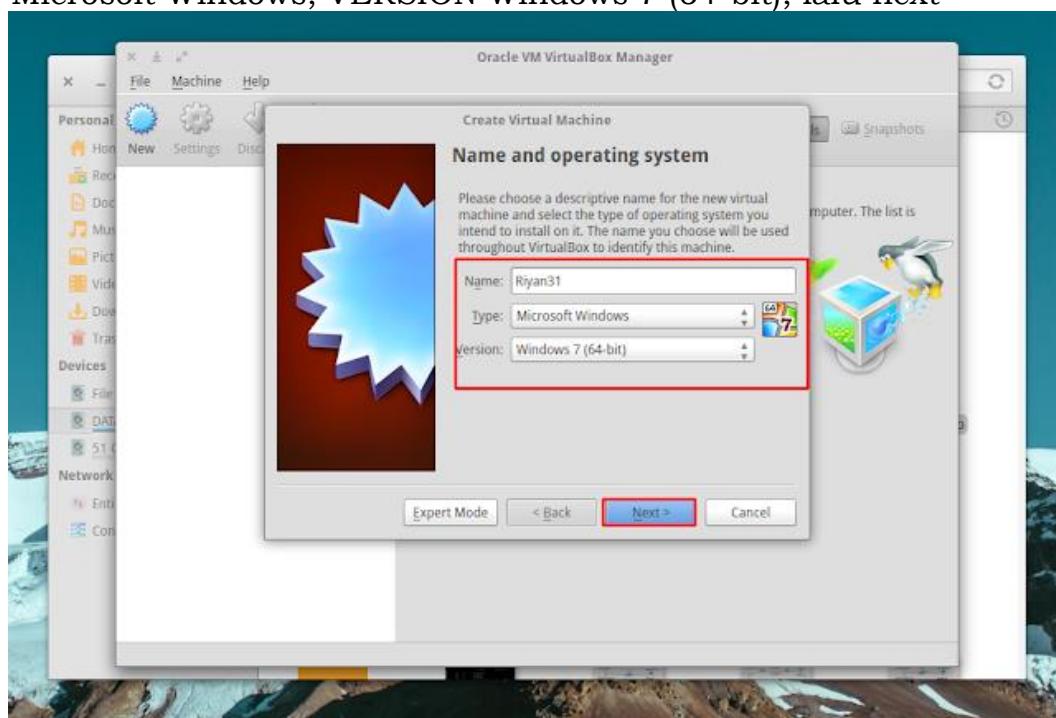
Proses instalasi Windows Server 2016 via Virtual Box

- Buka Virtual Boxnya, Lalu klik New



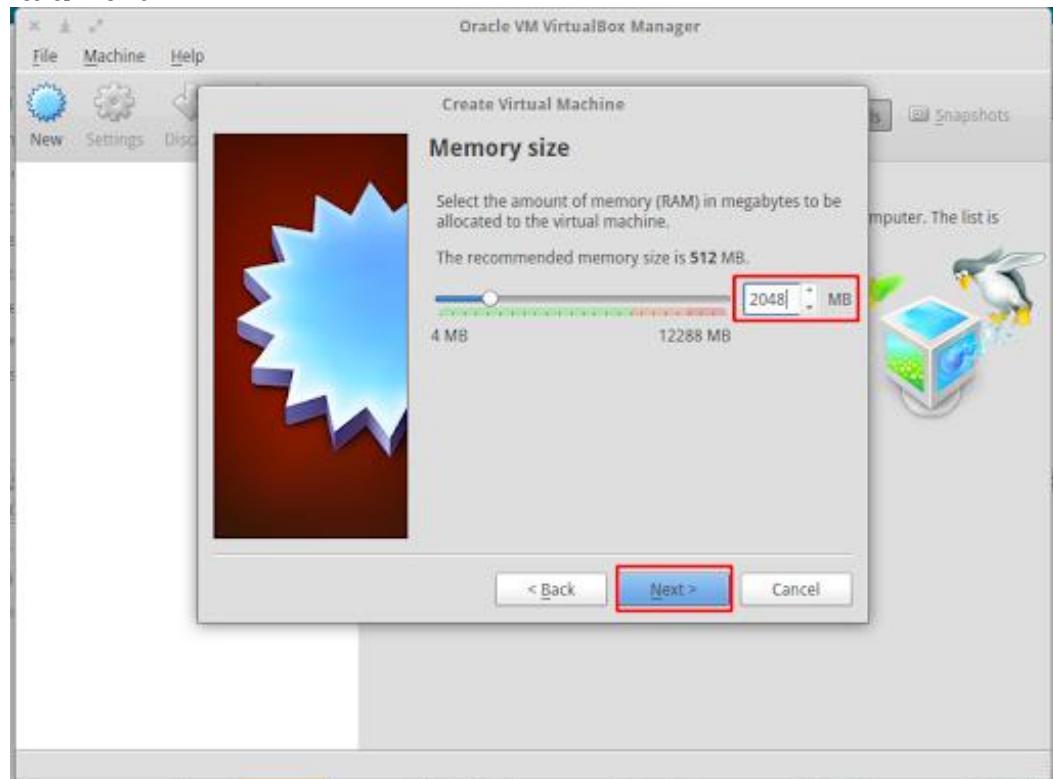
Gambar 8.1 Tampilan Awal Winbox

- Lalu isi kolom NAME susai dengan nama anda, TYPE pilihlah Microsoft Windows, VERSION Windows 7 (64-bit), lalu next



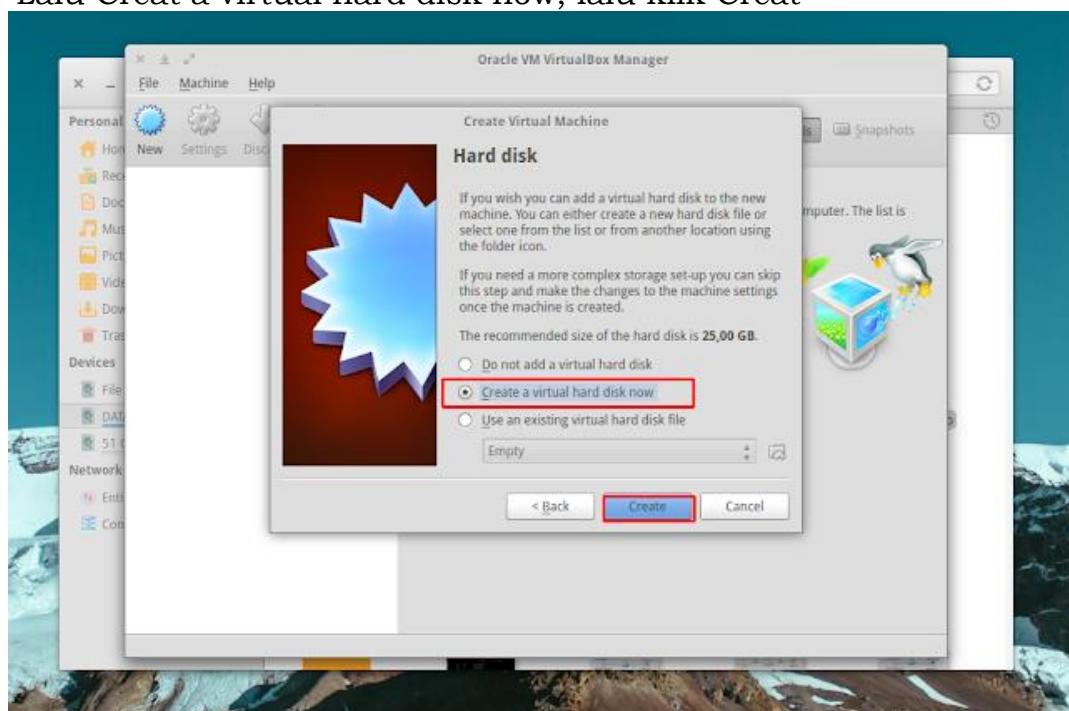
Gambar 8.2. memilih version windows

- Pada Memory Size atau RAM, kita ubah menjadi 2 GB (2048 MB), lalu next



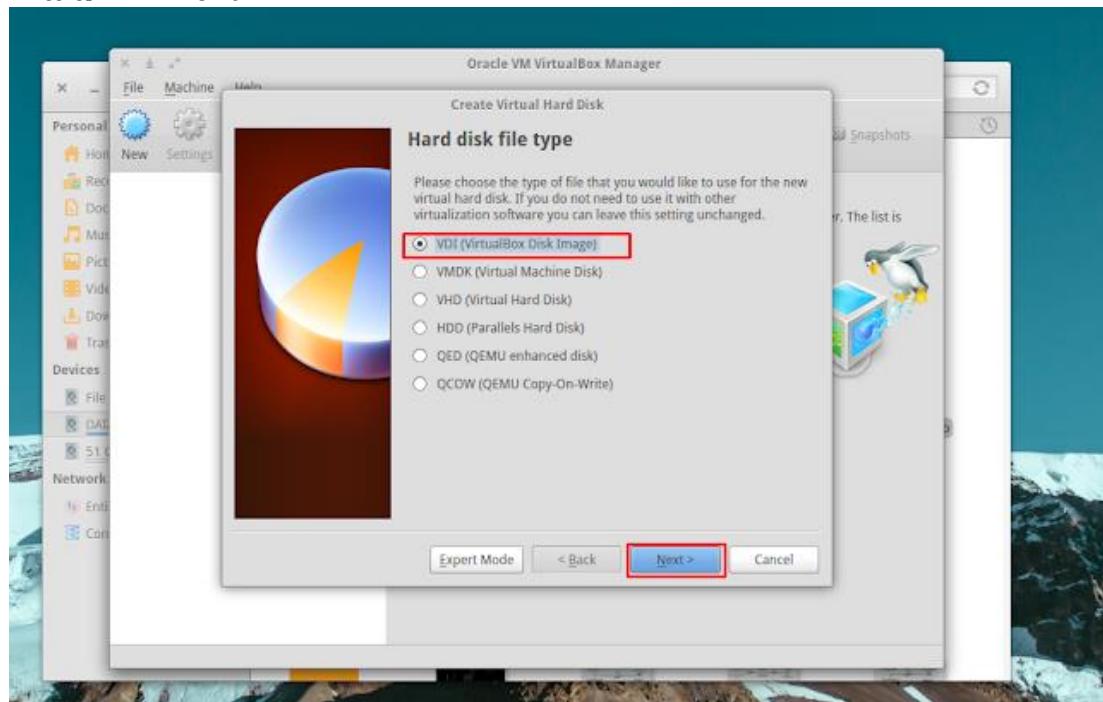
Gambar 8.3 memilih memori size

- Lalu Creat a virtual hard disk now, lalu klik Creat



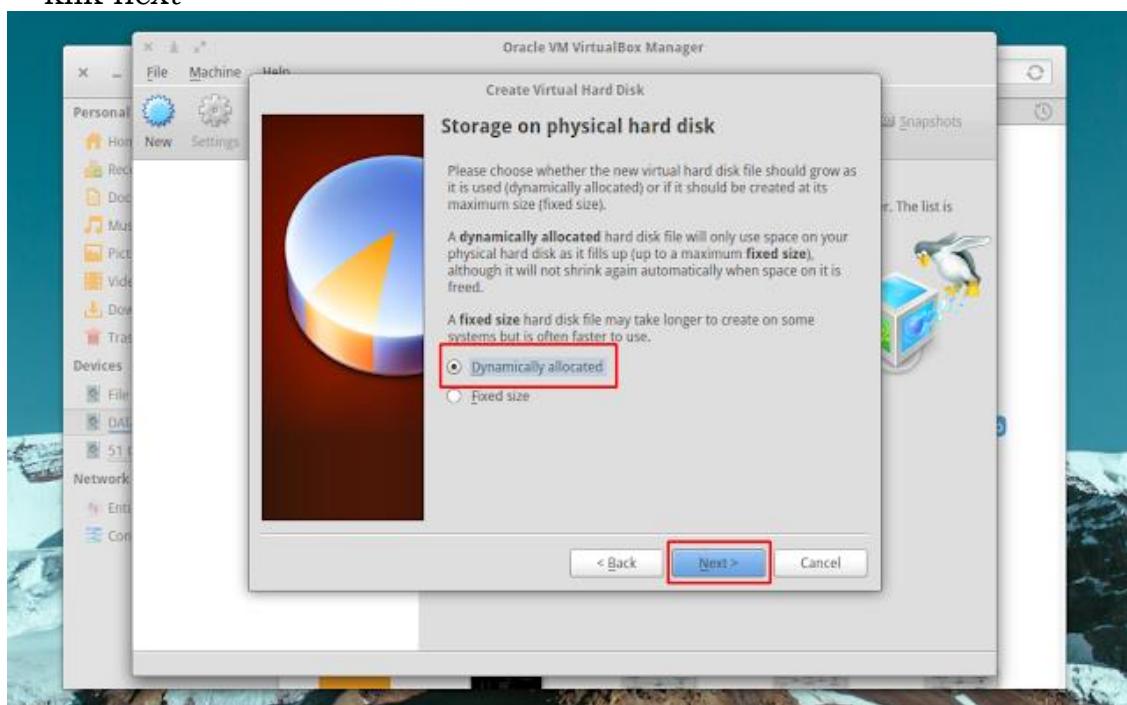
Gambar 8.4 Create Virtual

- Pada Hard Disk File Type, pilih yang VDI (VirtualBox Disk Image), lalu klik next



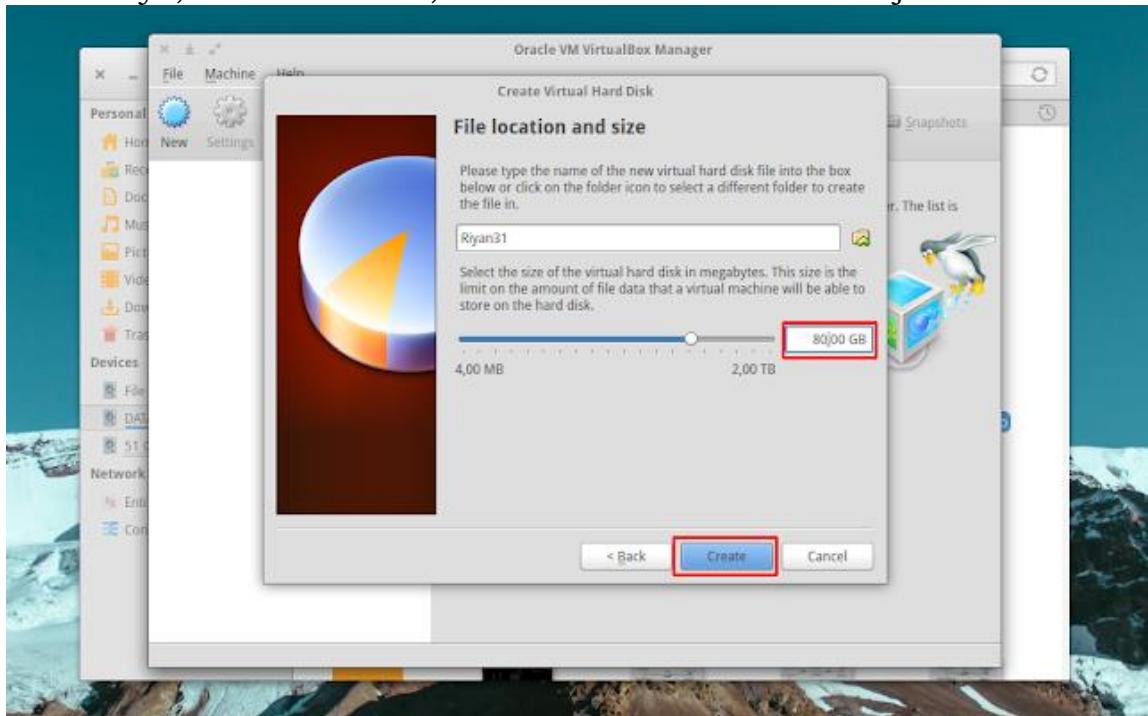
Gambar 8.5 memilih hard disk file type

- Pada Storage On Physical Hard Disk, pilih Dynamically allocated, lalu klik next



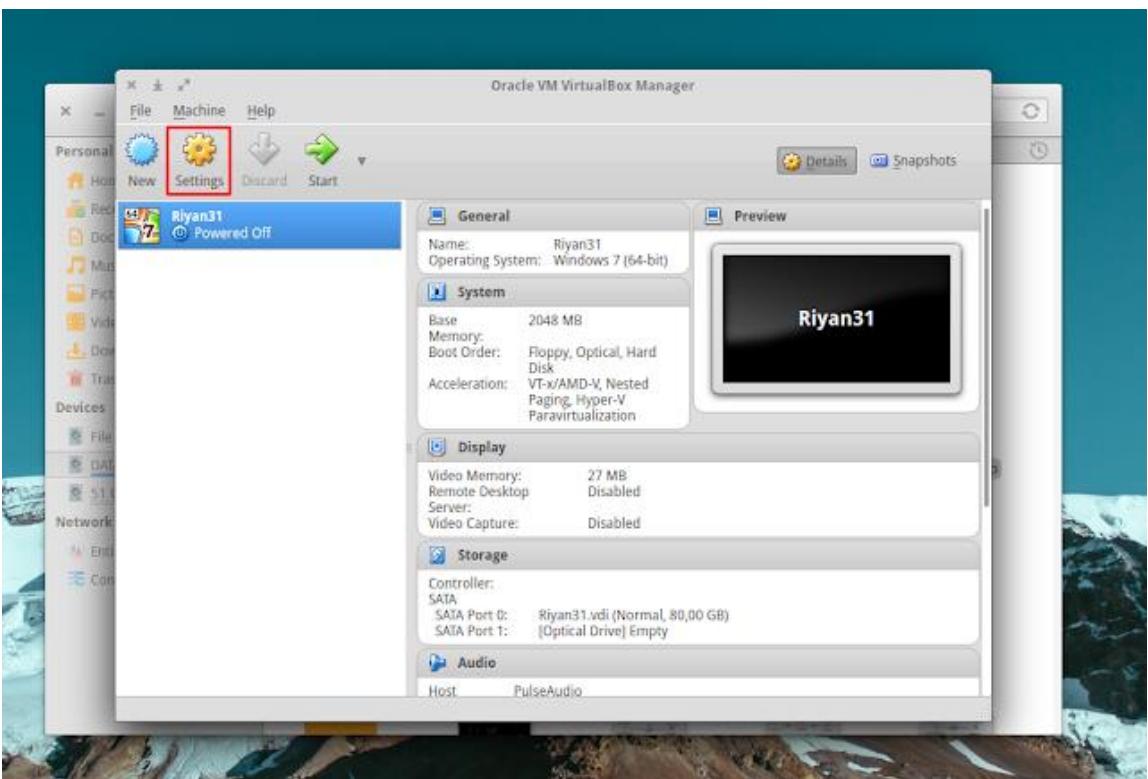
Gambar 8.6 dynamically allocated

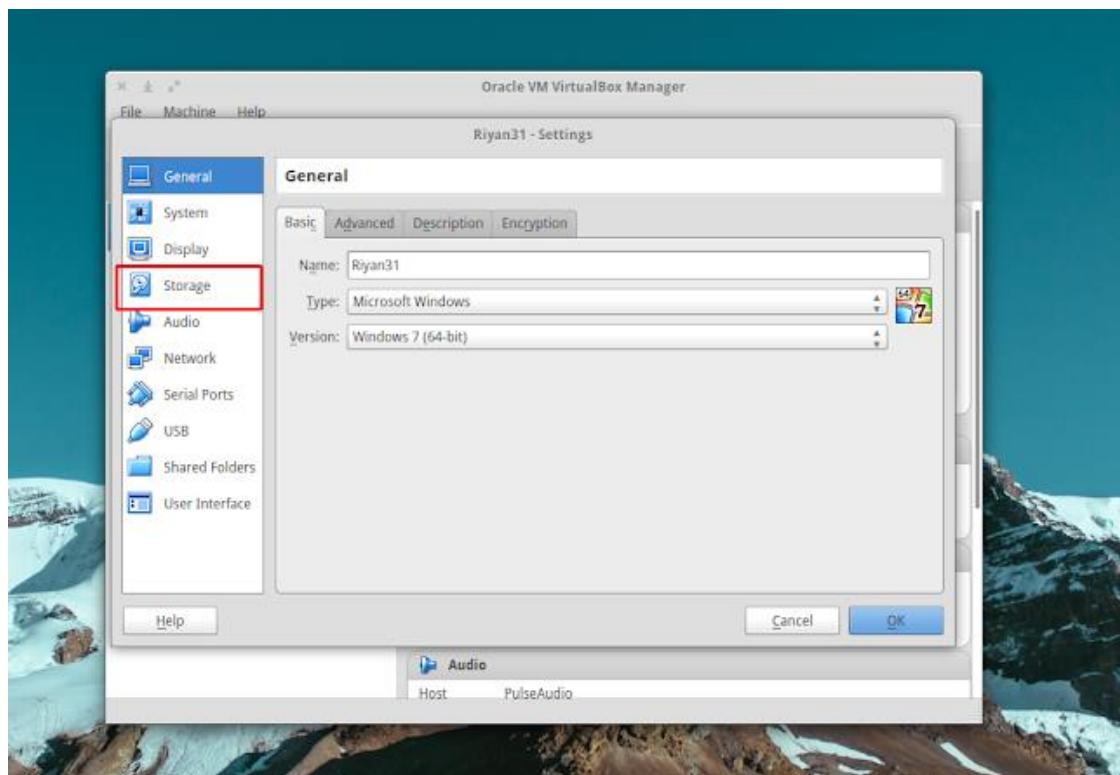
- Pada File Location And Size, isi kolom menjadi 80 GB untuk hard disknya, lalu klik create, lalu virtual box anda sudah jadi



Gambar 8.7 file location and size

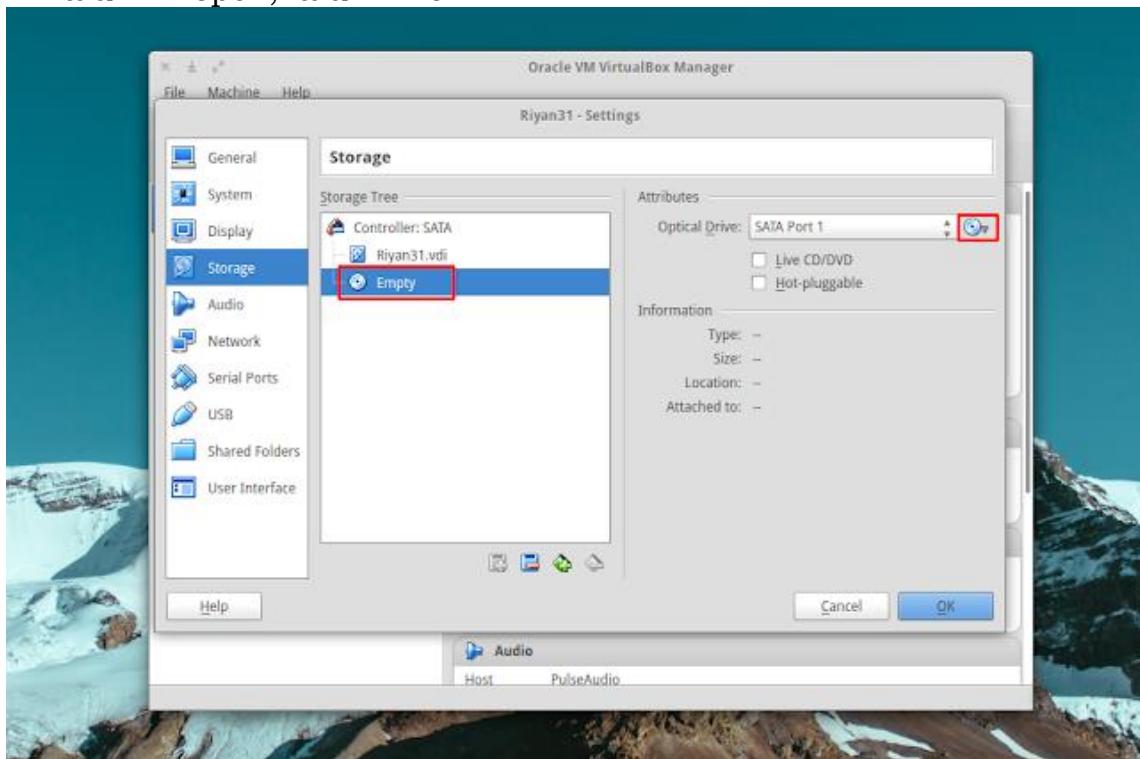
- Sebelum mulai kita setting dulu, lalu pilih Storage





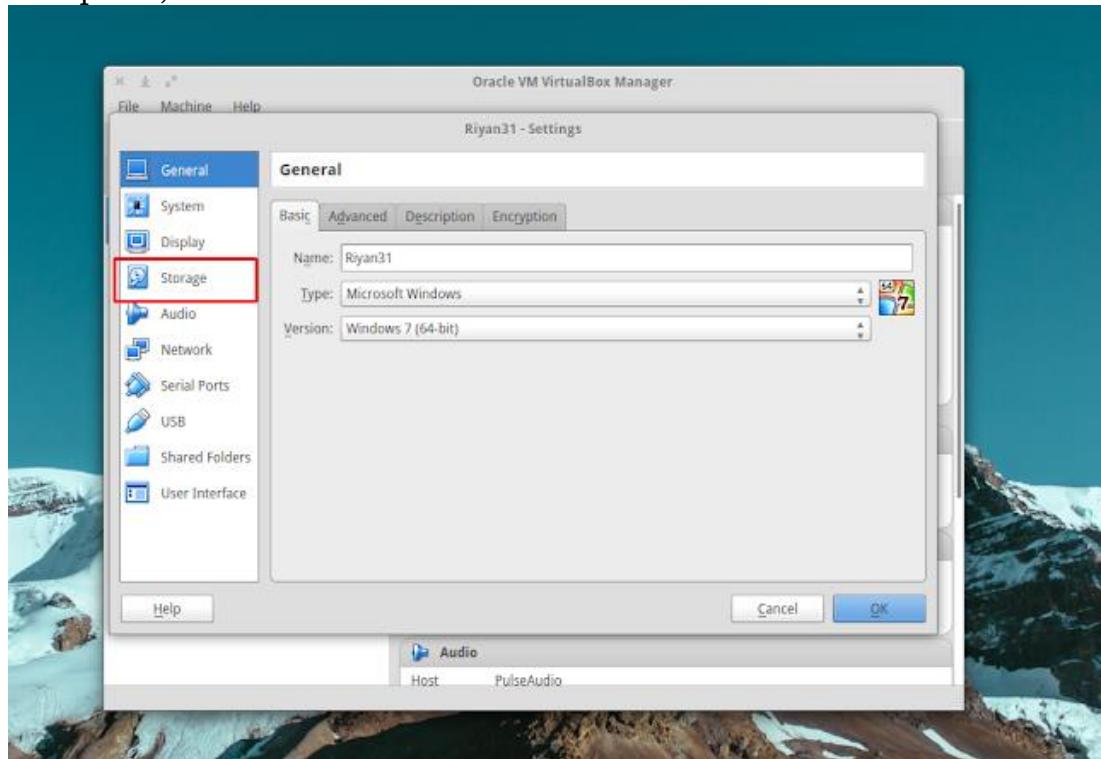
Gambar 8.8 memilih storage

- Pada Storage, pilih yang empty lalu klik yang bergambar kaset, lalu pilih Choose A Virtual Optical Disk File, untuk mencari file isonya, lalu klik open, lalu klik ok



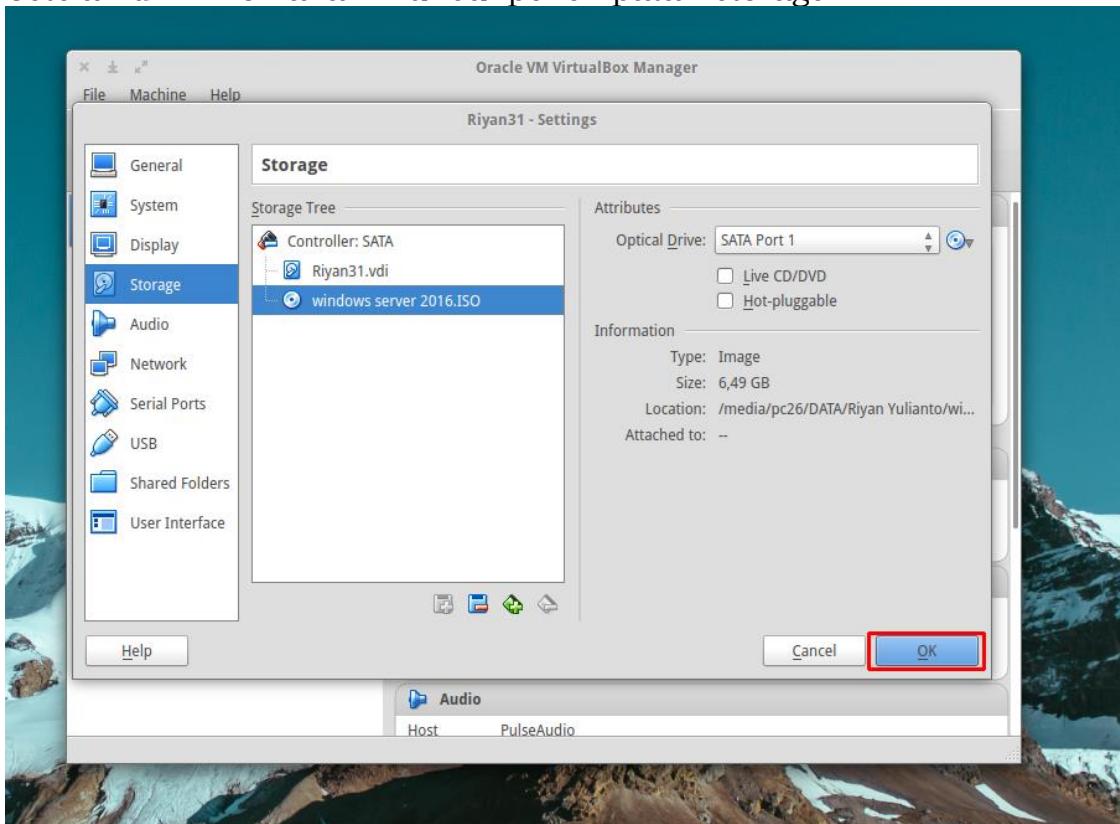
Gambar 8.9 memilih virtual optccal disk file

- Pada pilihan virtual optical disk pilih iso windows 2016 yang telah disiapkan, kemudian klik oke



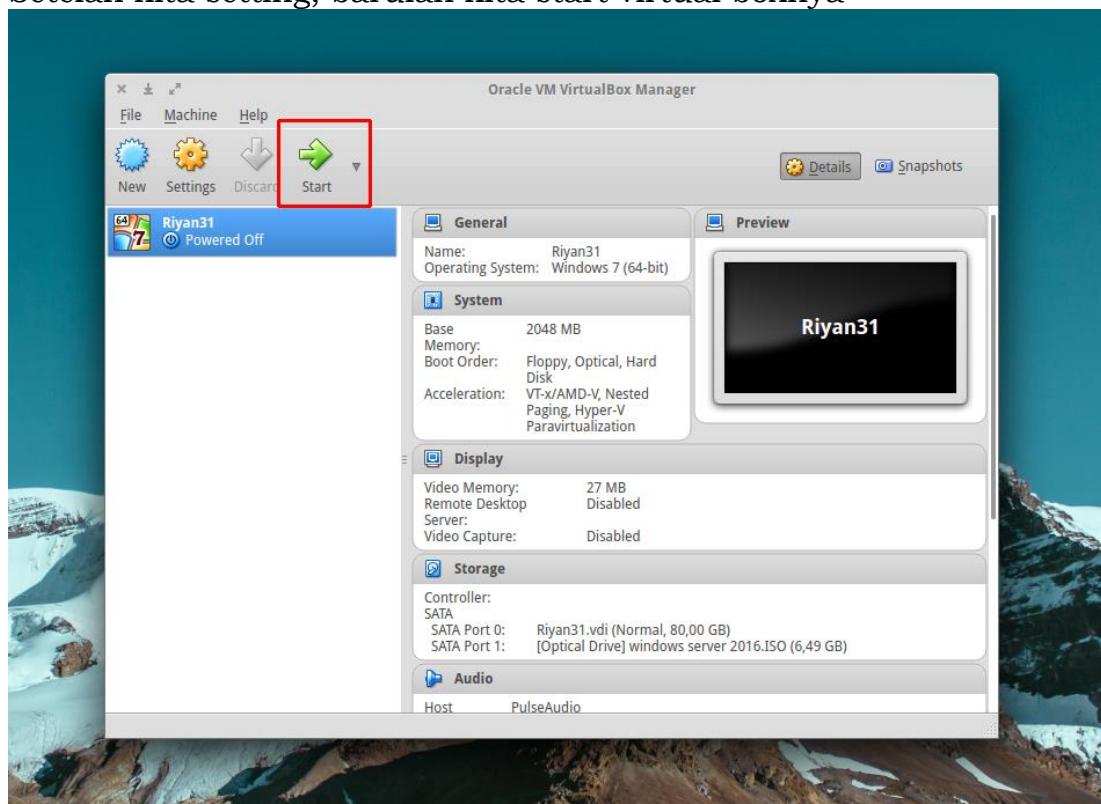
Gambar 8.10 choose virtual optical

- Setelah di klik ok akan muncul penempatan storage



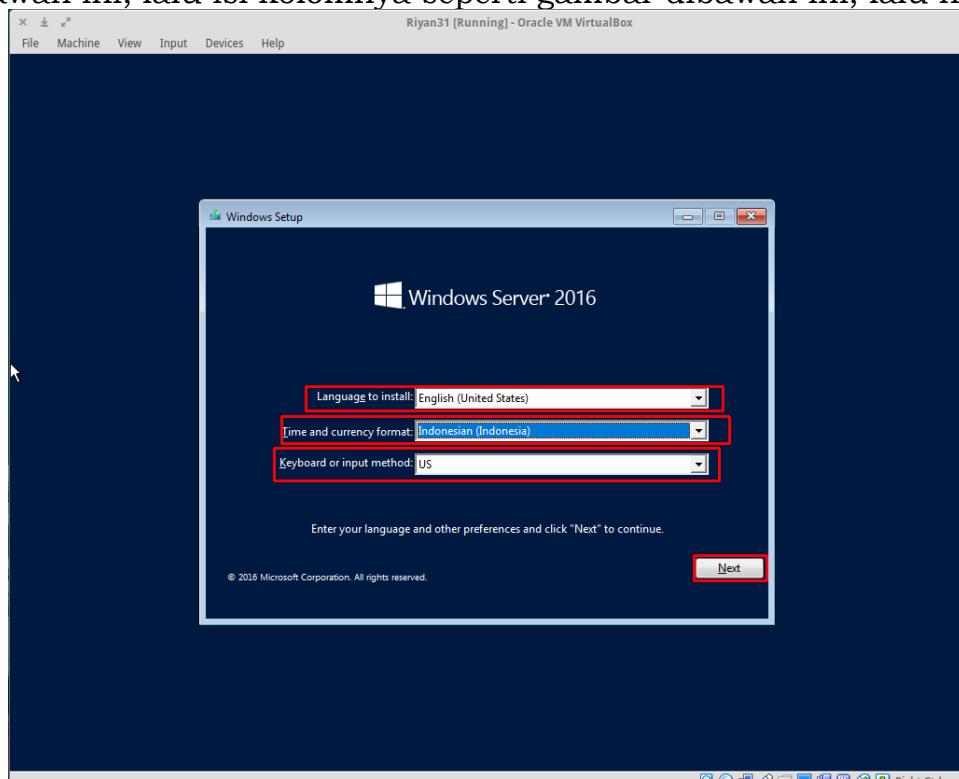
Gambar 8.11 penempatan storage

- Setelah kita setting, barulah kita start virtual boxnya



Gambar 8.12 startn virtual box

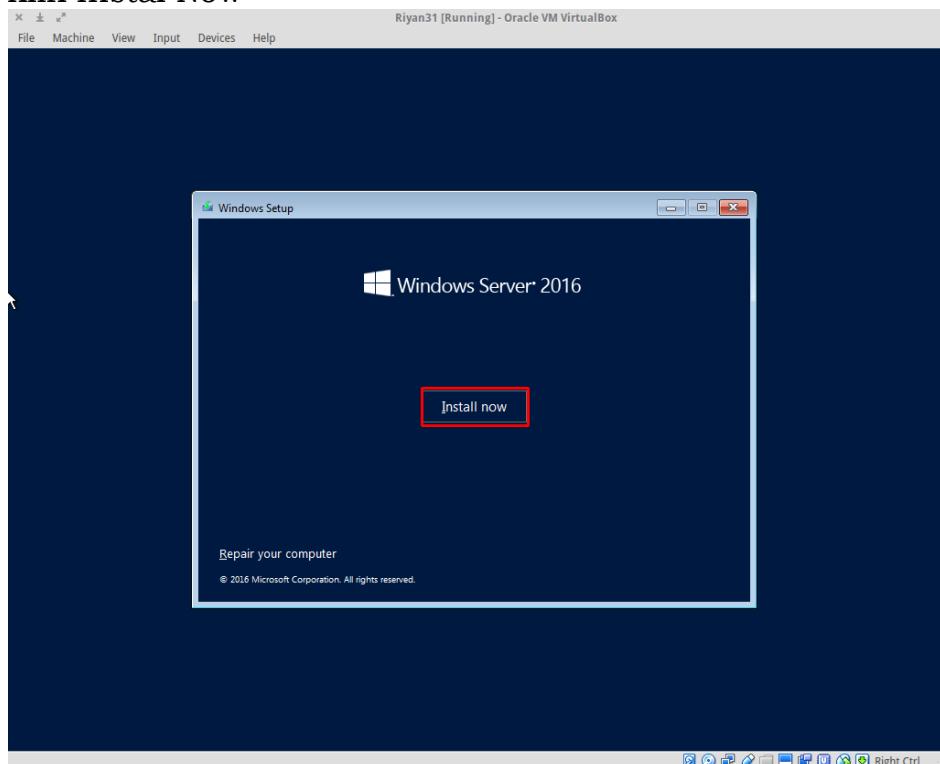
- Setelah kita start virtual boxnya, akan muncul tampilan seperti dibawah ini, lalu isi kolomnya seperti gambar dibawah ini, lalu next



Gambar 8.13 tampilan awal instalasi windows server 2016

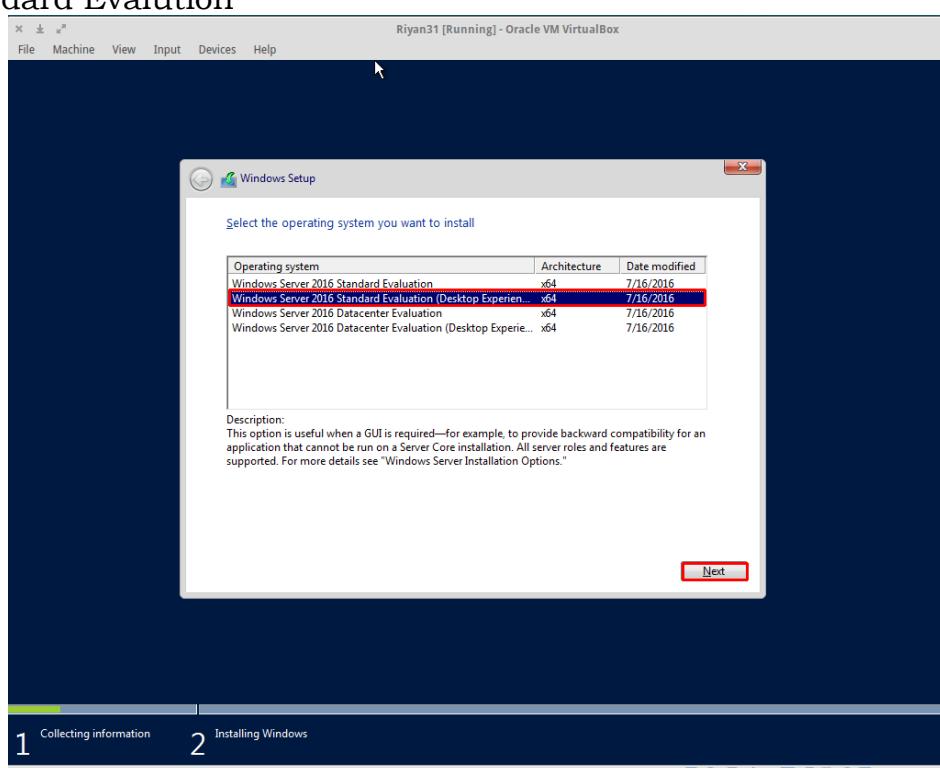


- Lalu klik Instal Now



Gambar 8.14 windows setup

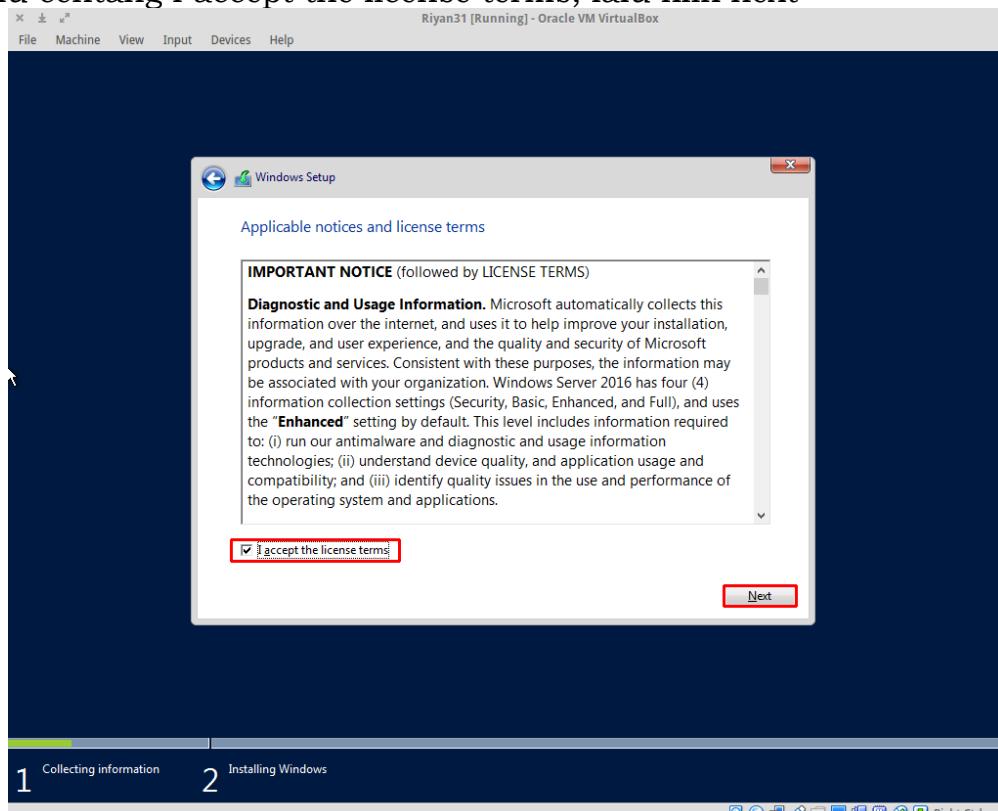
- Setelah itu pilih Operating Systemnya Windows Server 2016 Standard Evaluation



Gambar 8.15 memilih operating windows

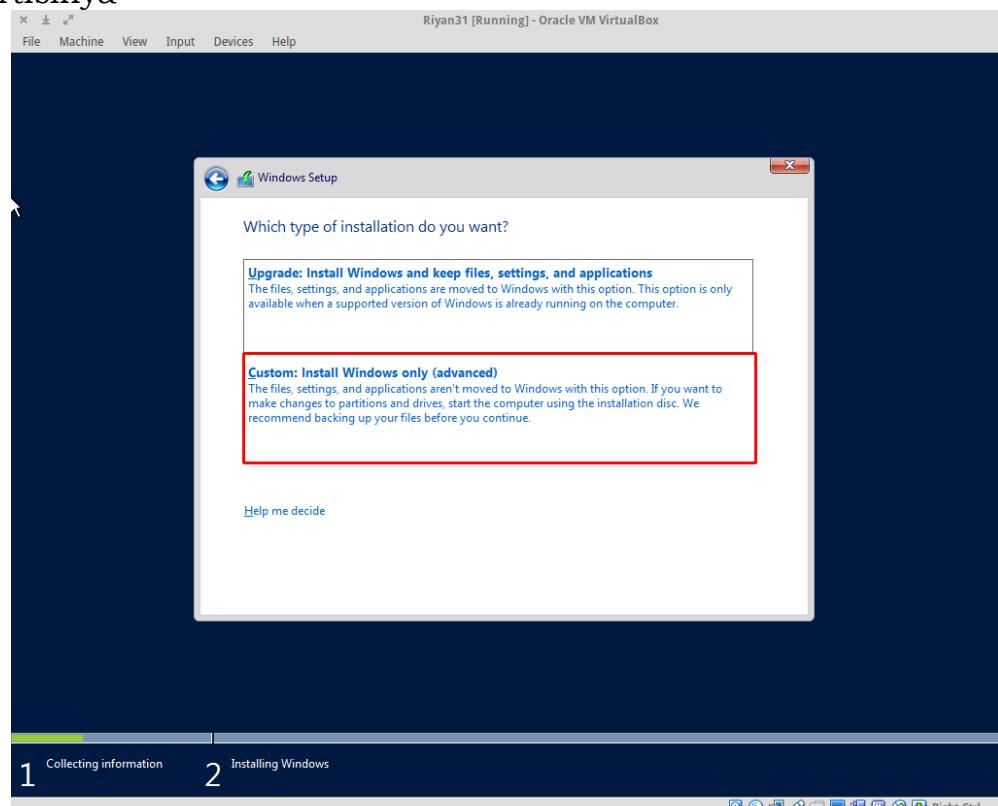


- Lalu centang I accept the license terms, lalu klik next



Gambar 8.19 memilih license

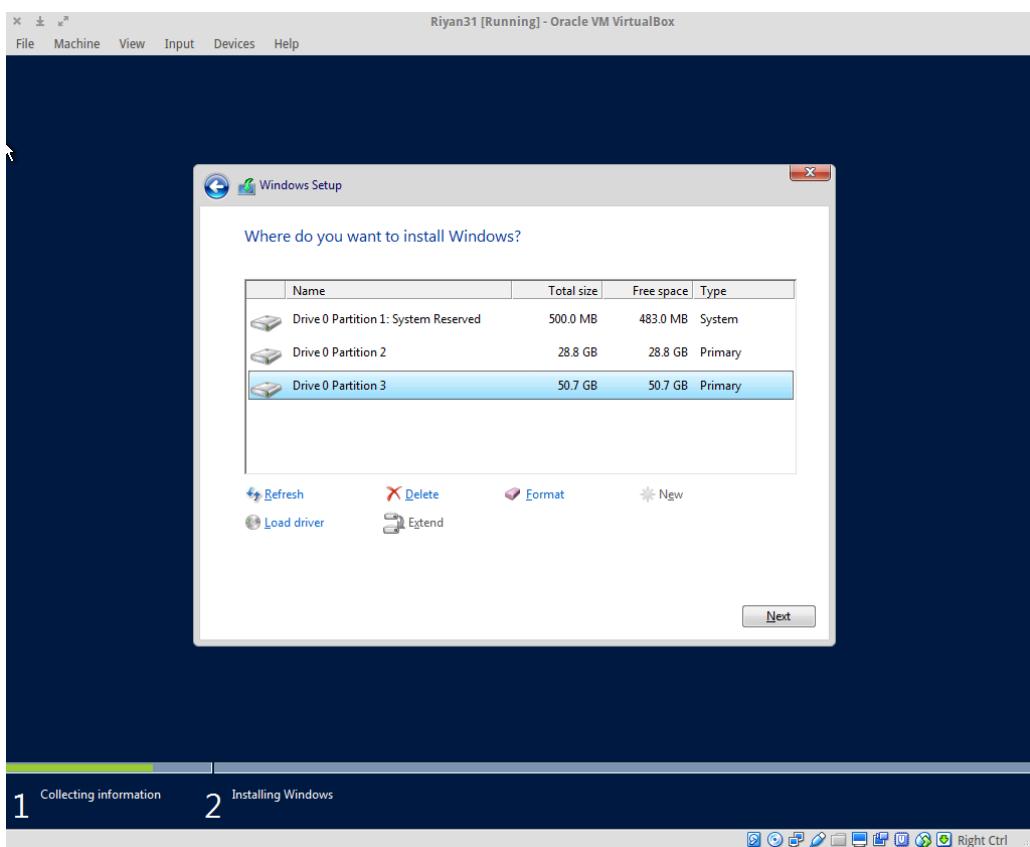
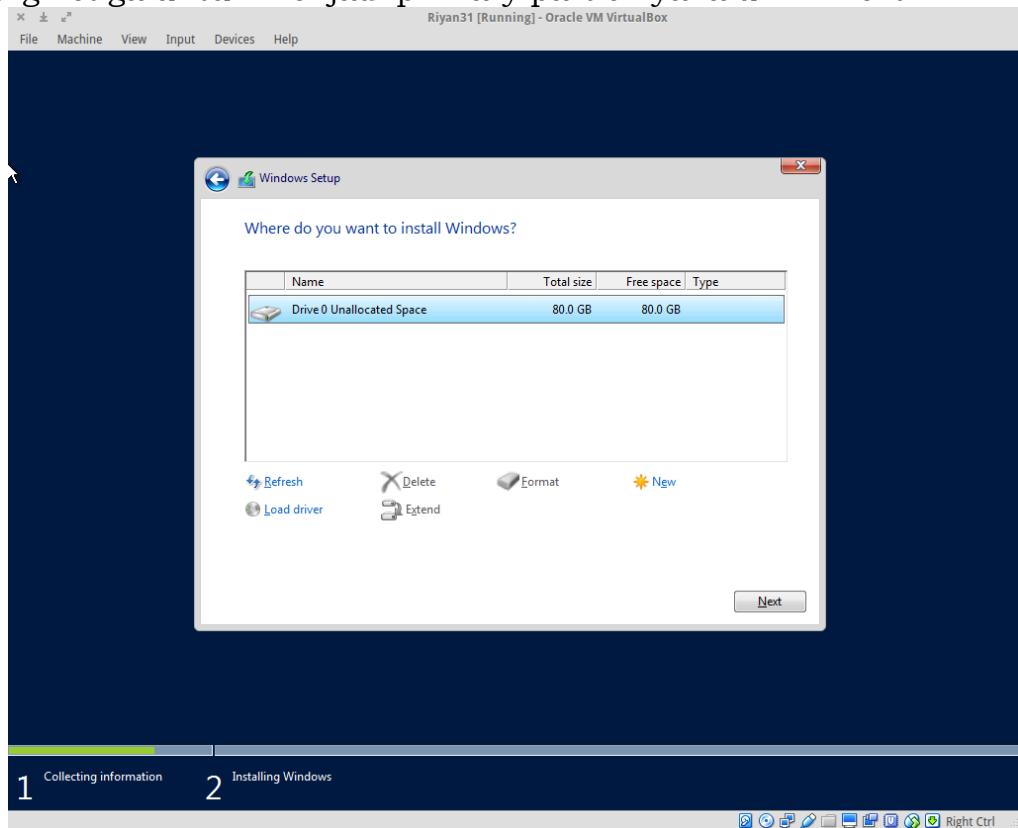
- Setelah itu kita pilih Custom Install Windows Only, untuk custom partisinya

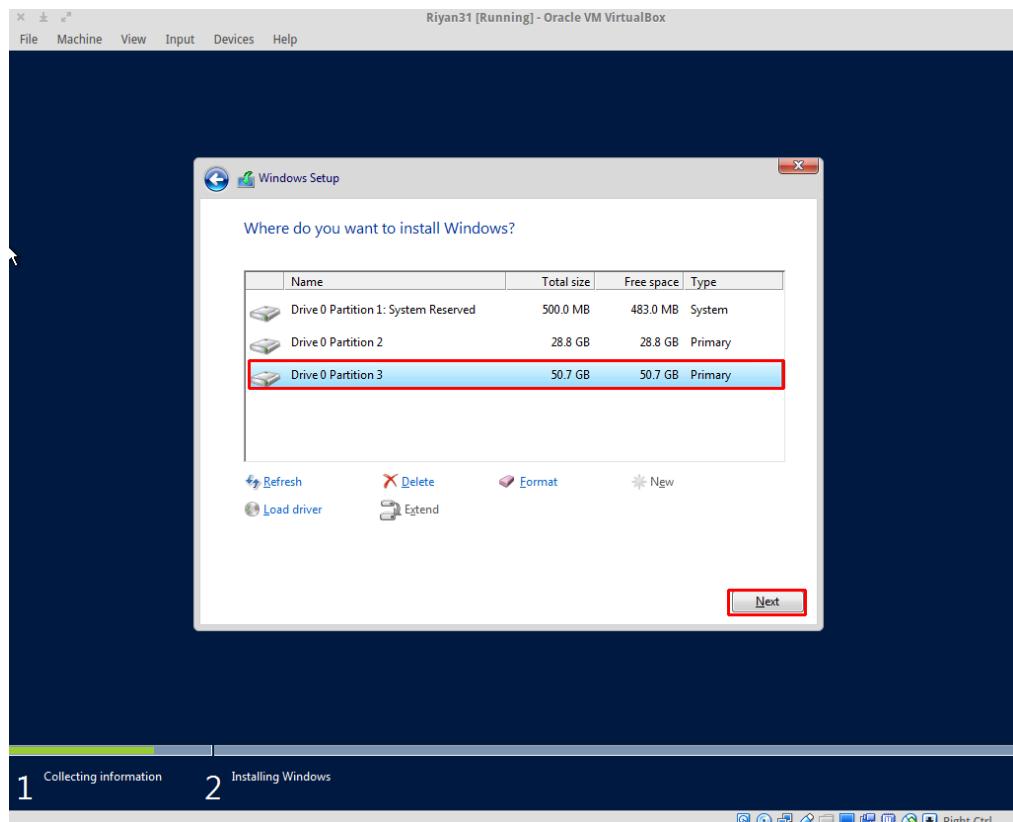


Gambar 8.16 custom install windows



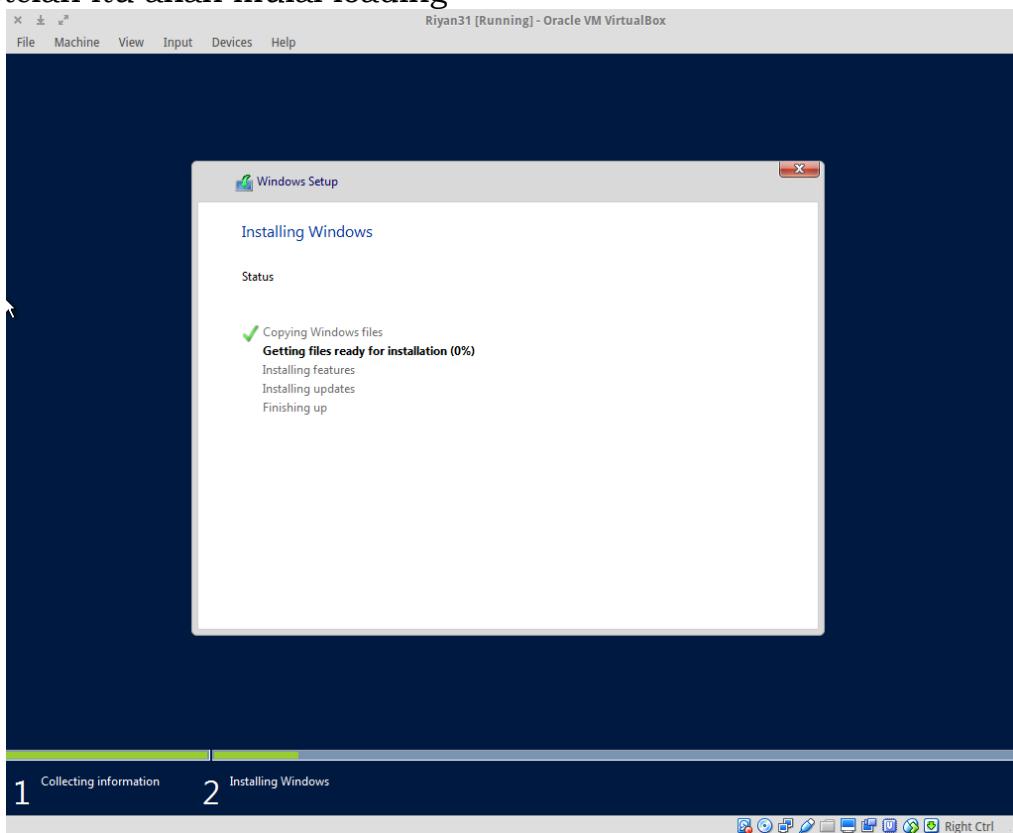
- Lalu kita buat partisinya seperti dibawah ini, setelah itu pilih partisi yang ketiga untuk menjadi primary partisinya lalu klik next

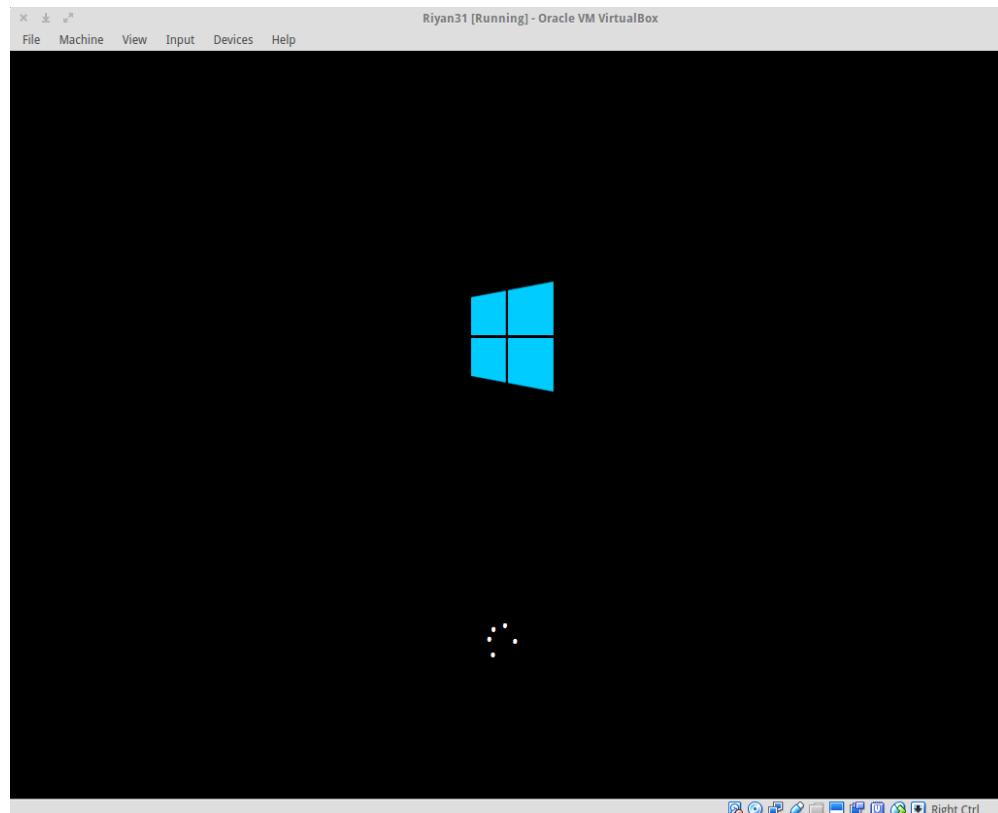




Gambar 8.17 Pengaturan partisi

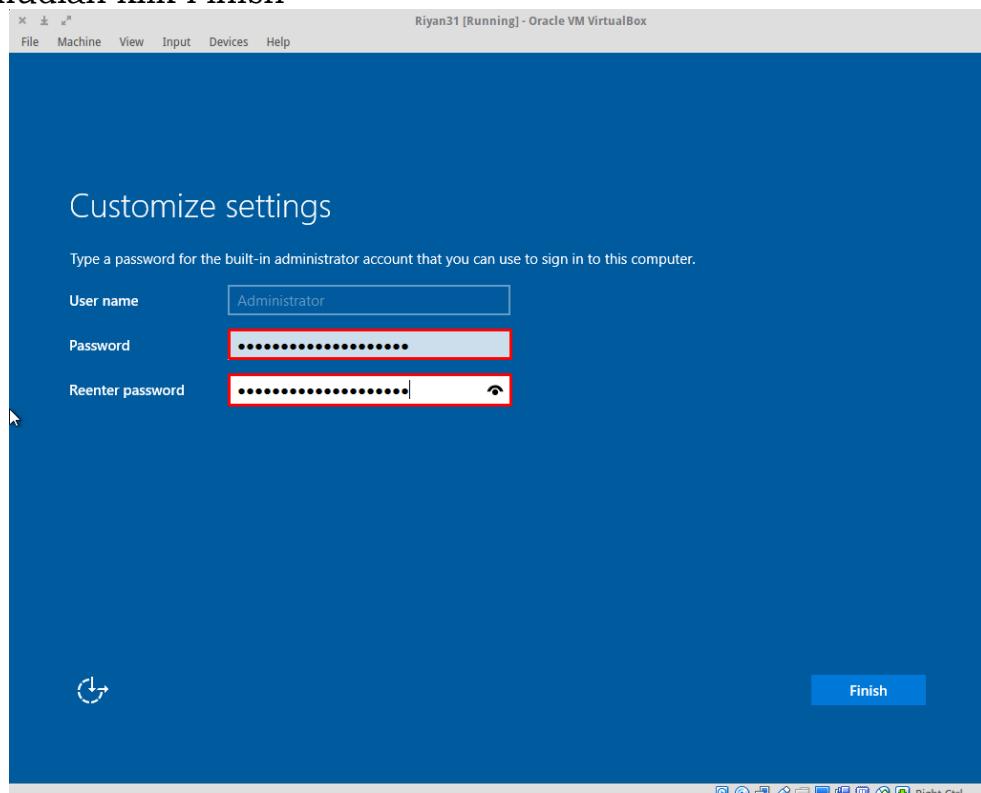
- Setelah itu akan mulai loading





Gambar 8.18 proses instalas windows

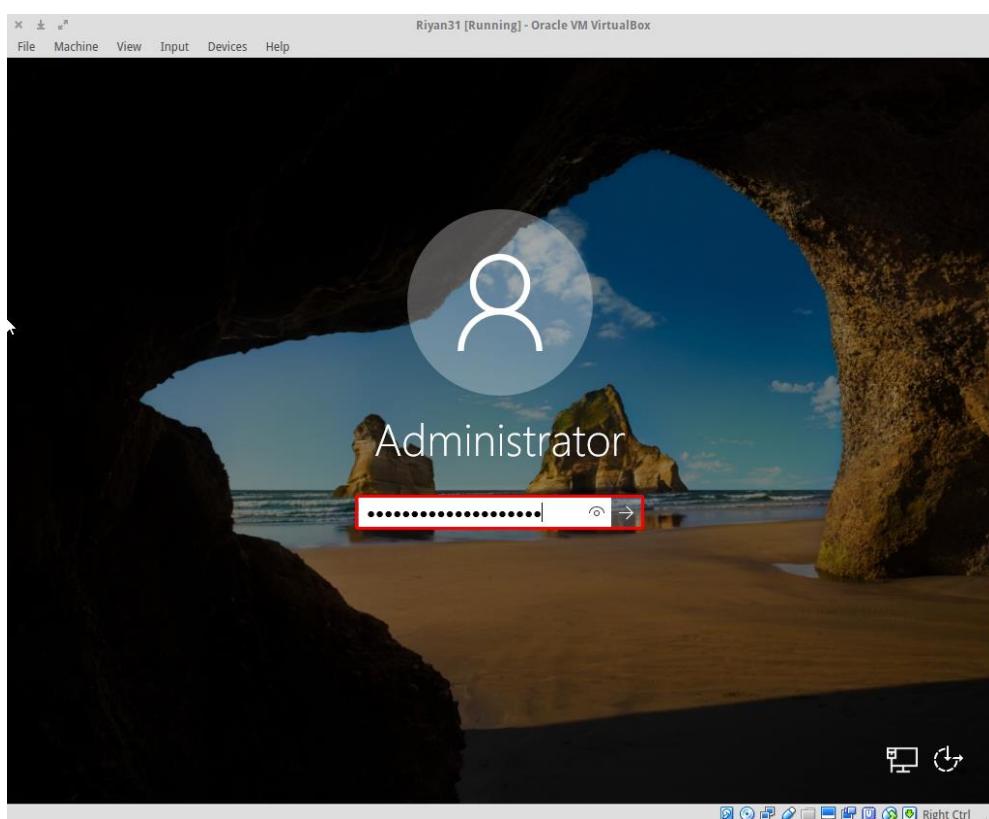
- Setelah itu, isi kolom password, contoh(!@#\$%^&*()_+riyan123), kemudian klik Finish



Gambar 8.19 kolom password



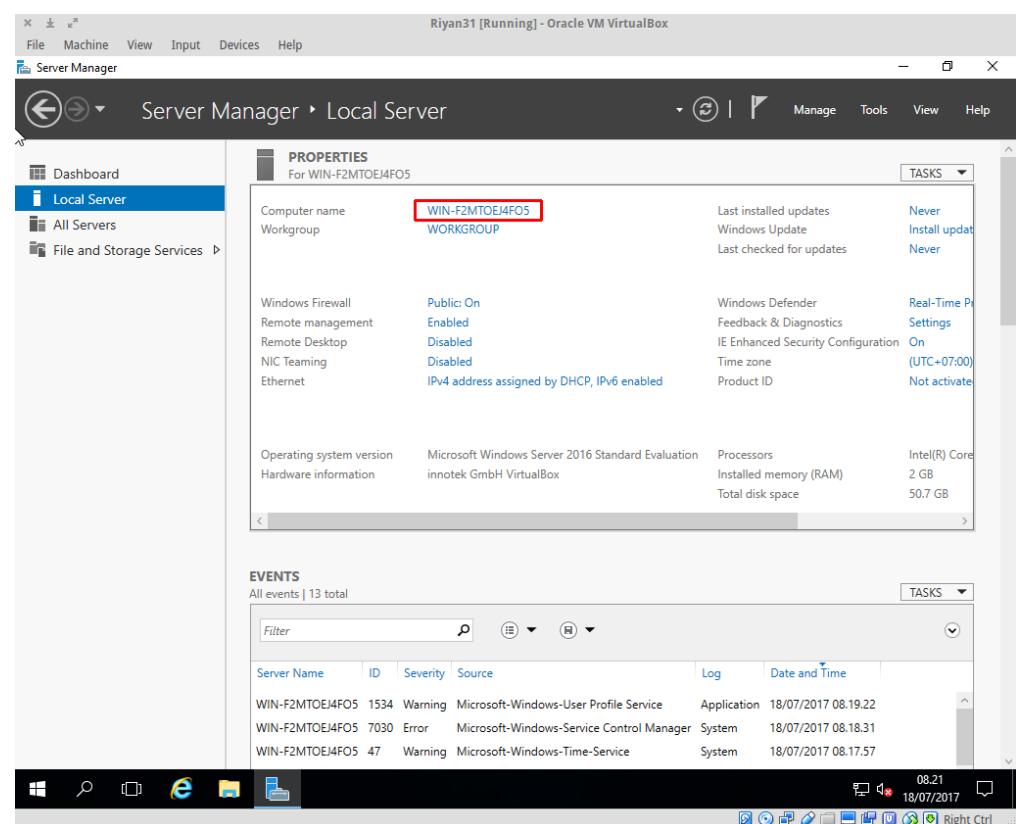
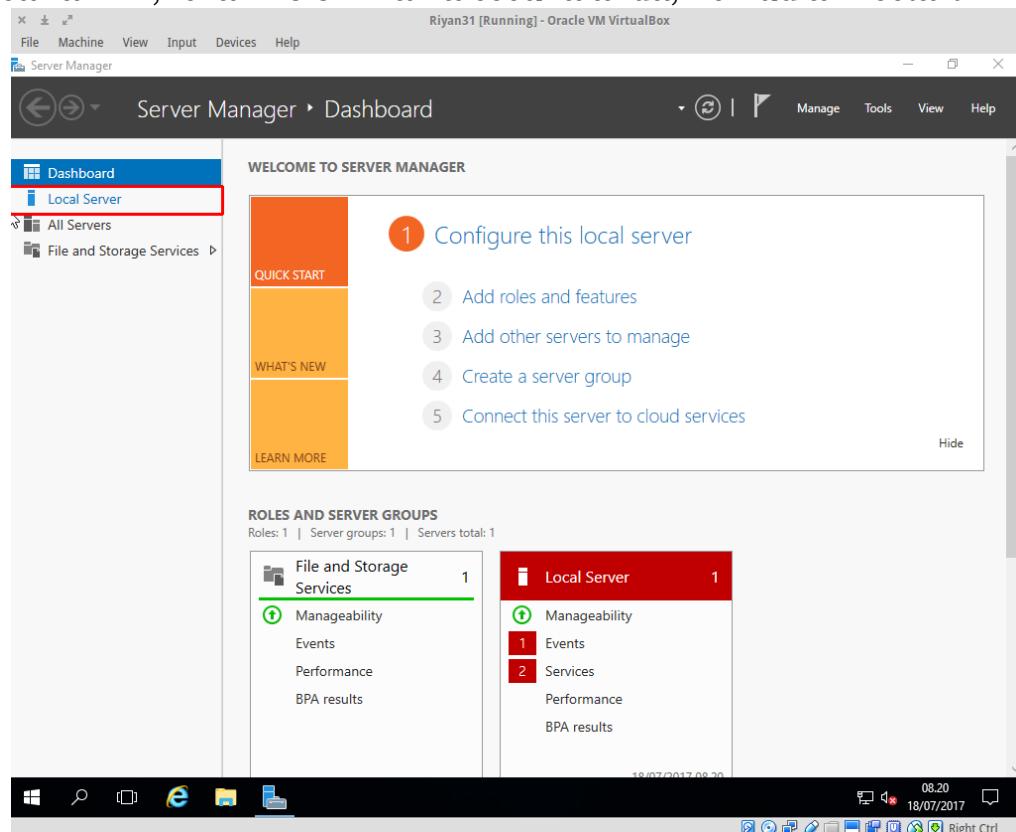
- Setelah itu akan muncul tampilan seperti ini, kemudian klik input pada virtual boxnya, pilih keyboard, lalu insert Ctrl-Alt-Del untuk ke langkah selanjutnya, lalu isi password yang tadi telah disetel

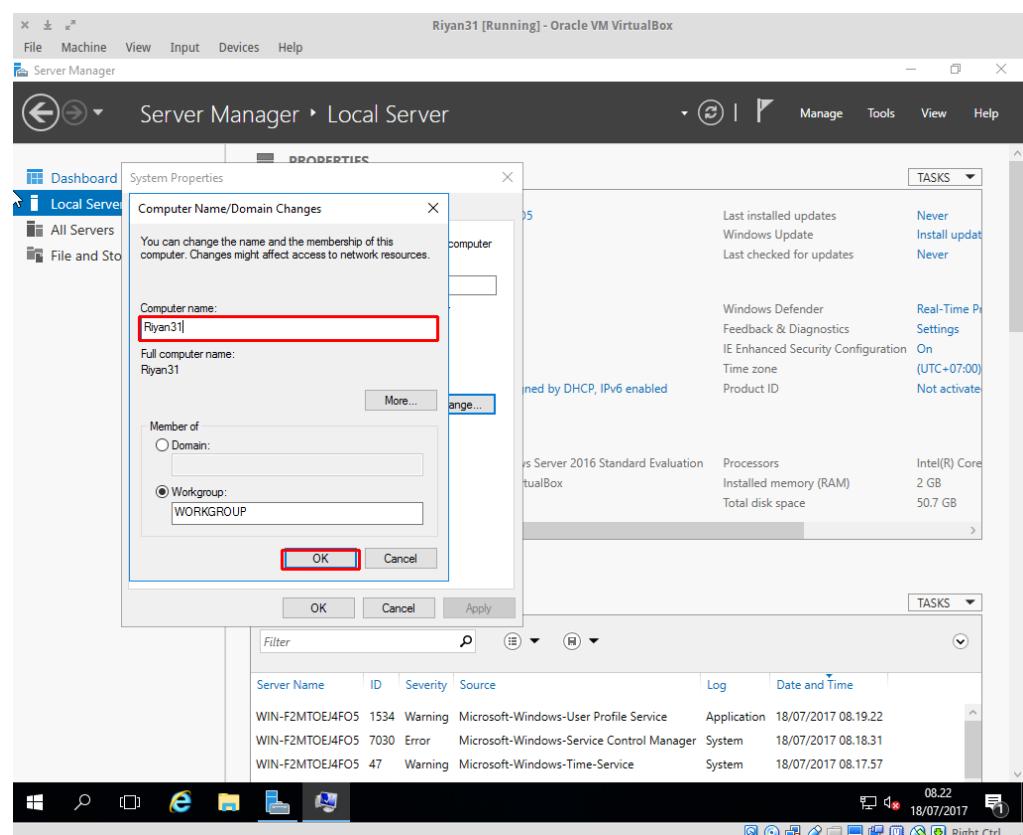
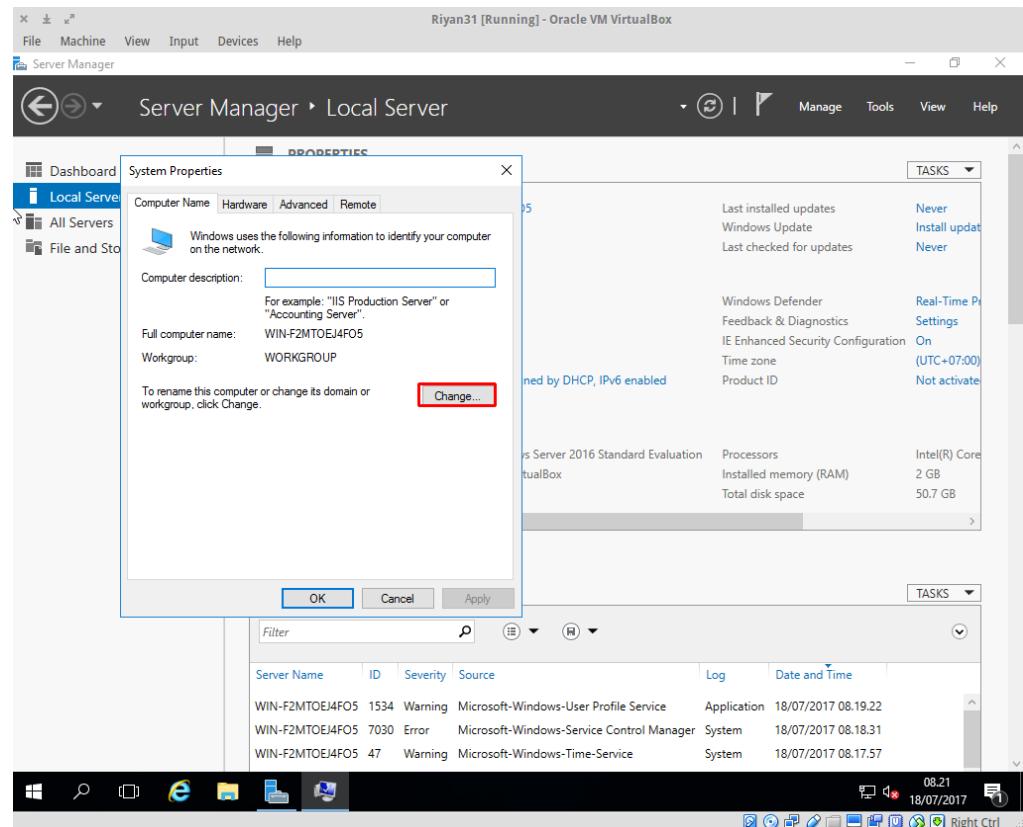


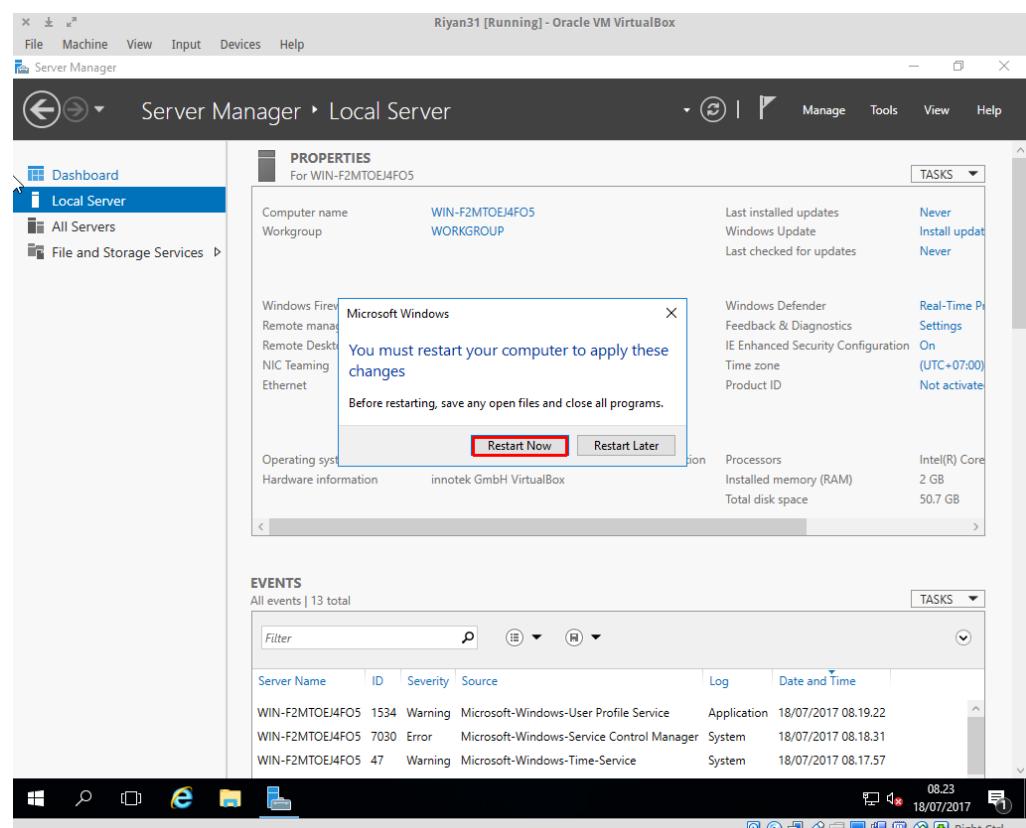
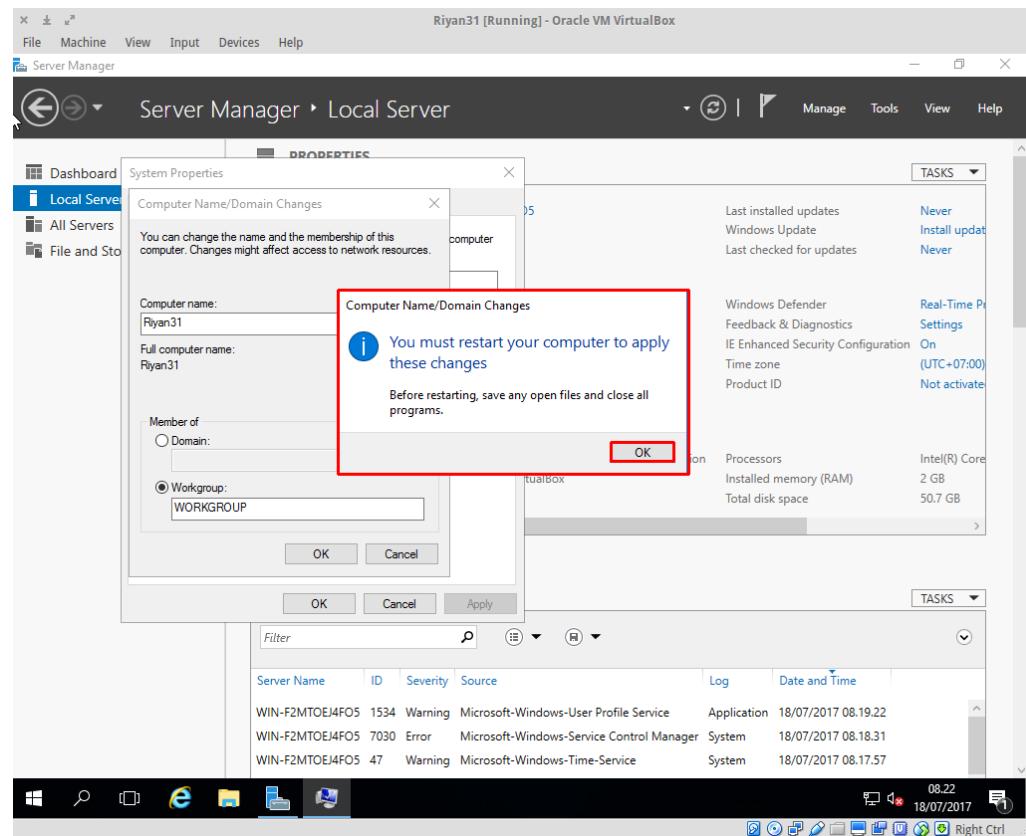
Gambar 8.20 klik input pada virtual box



- Setelah itu kita pilih Local Server untuk mengubah computer seperti dibawah ini, isilah kolom nama sesuka anda, kemudian restart



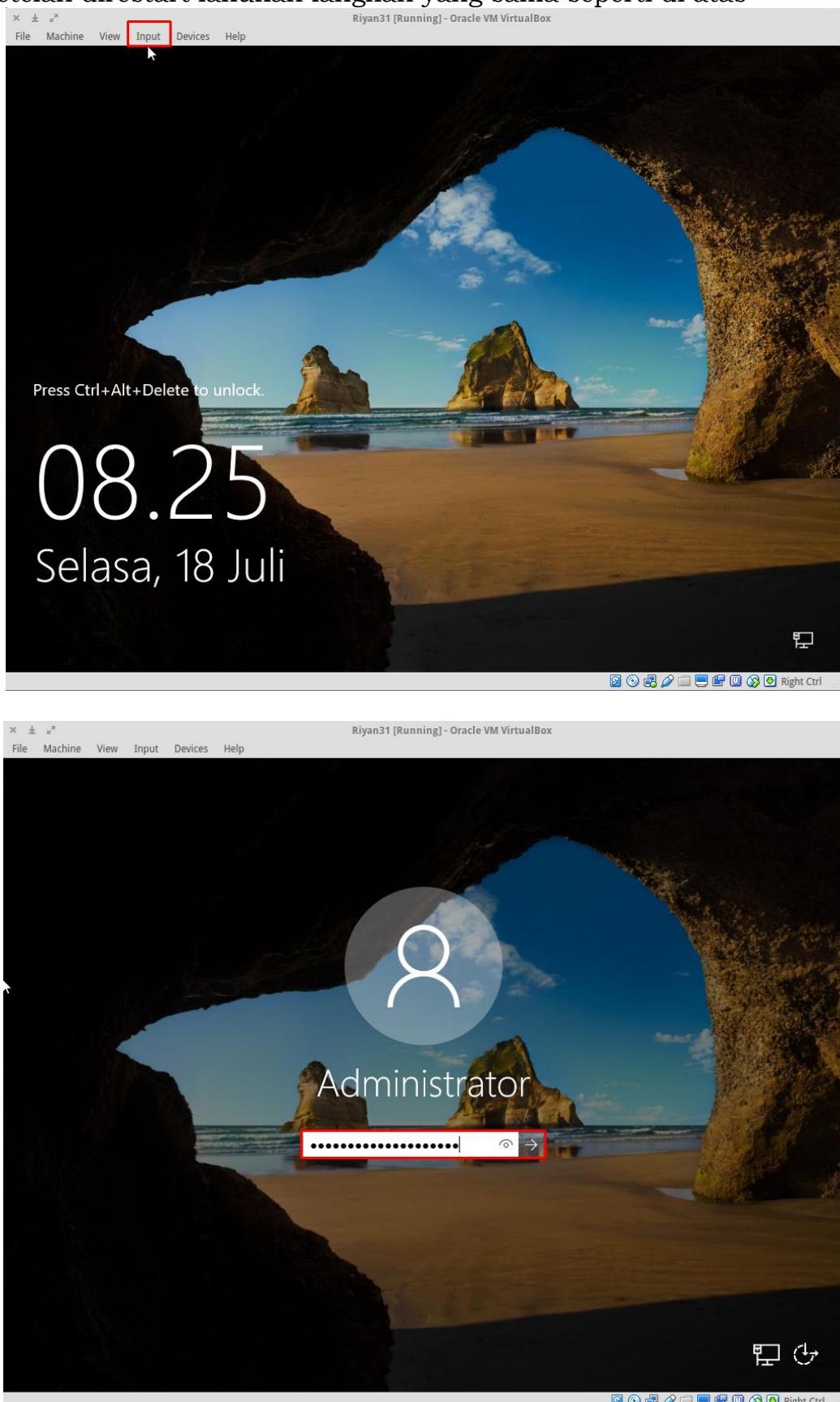




Gambar 8.21 Local Server untuk mengubah computer



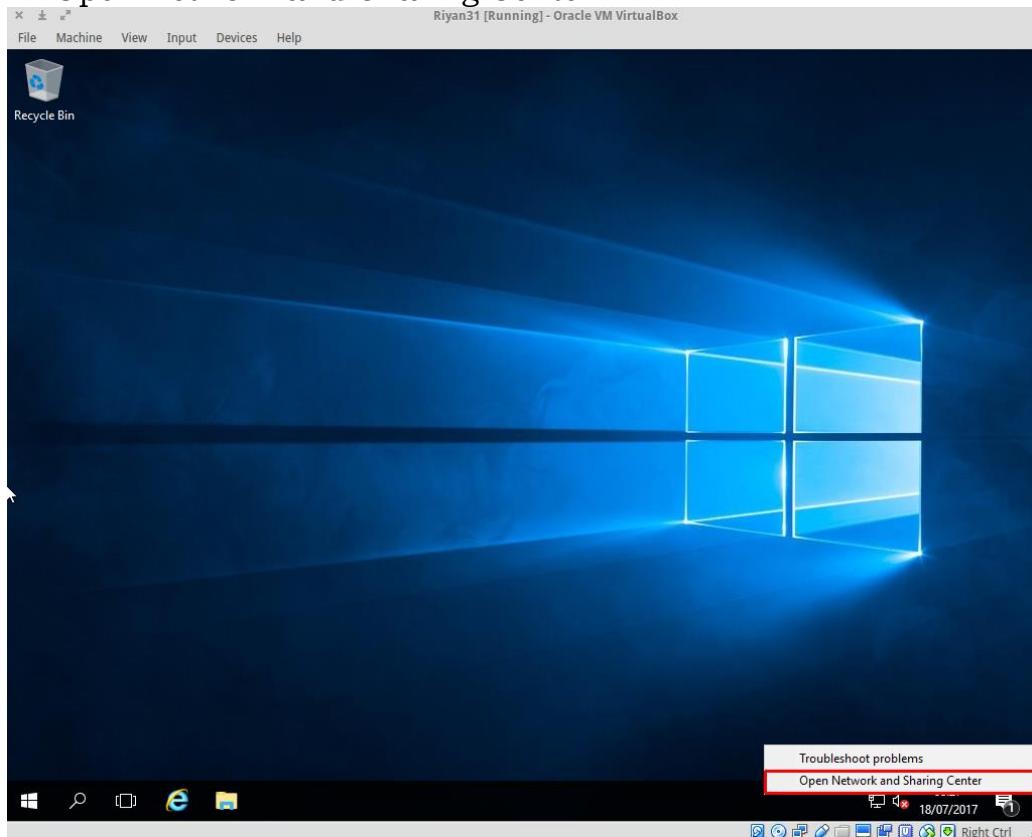
- Setelah direstart lakukan langkah yang sama seperti di atas



Gambar 8.22 hasil restart

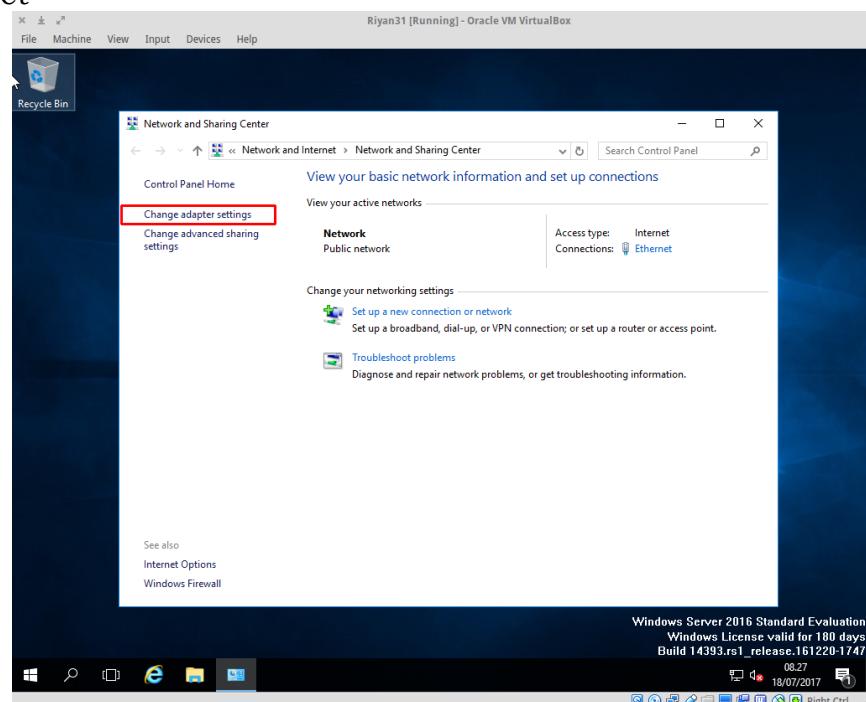


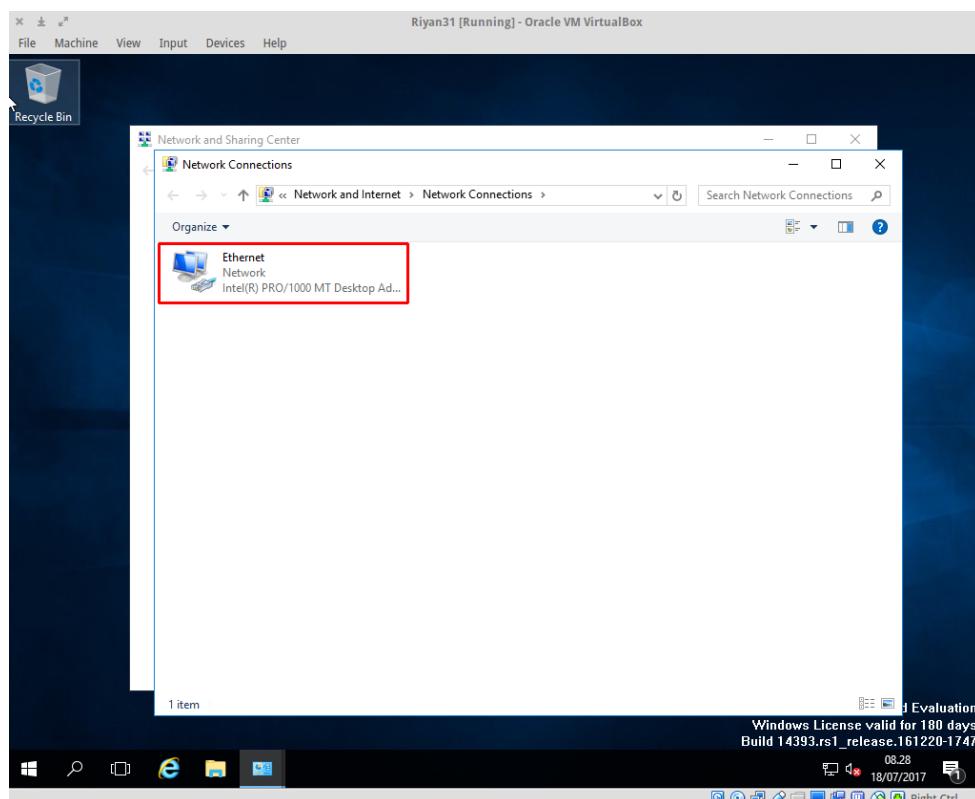
- Setelah itu anda akan masuk ke tampilan desktop, lalu klik kanan pada gambar pc yang ada di bagian pojok kanan bawah, kemudian pilih Open Network and Sharing Center



Gambar 8.23 Network and Sharing Center

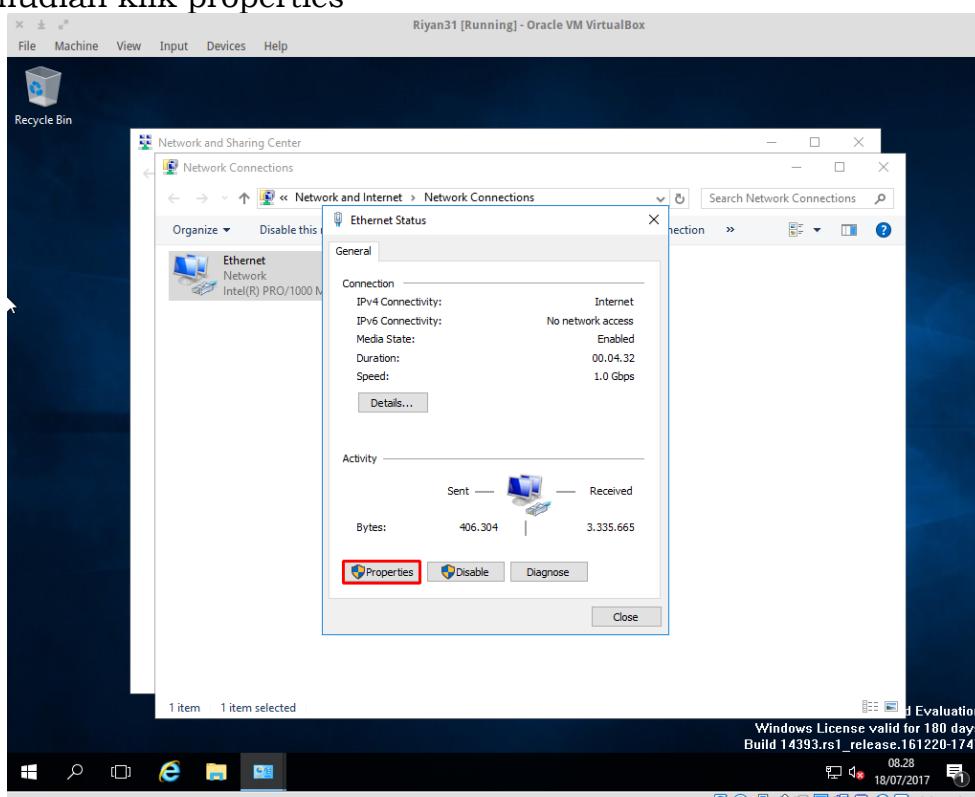
- Kemudian pilih Change adapter settings, kemudian pilih yang Ethernet





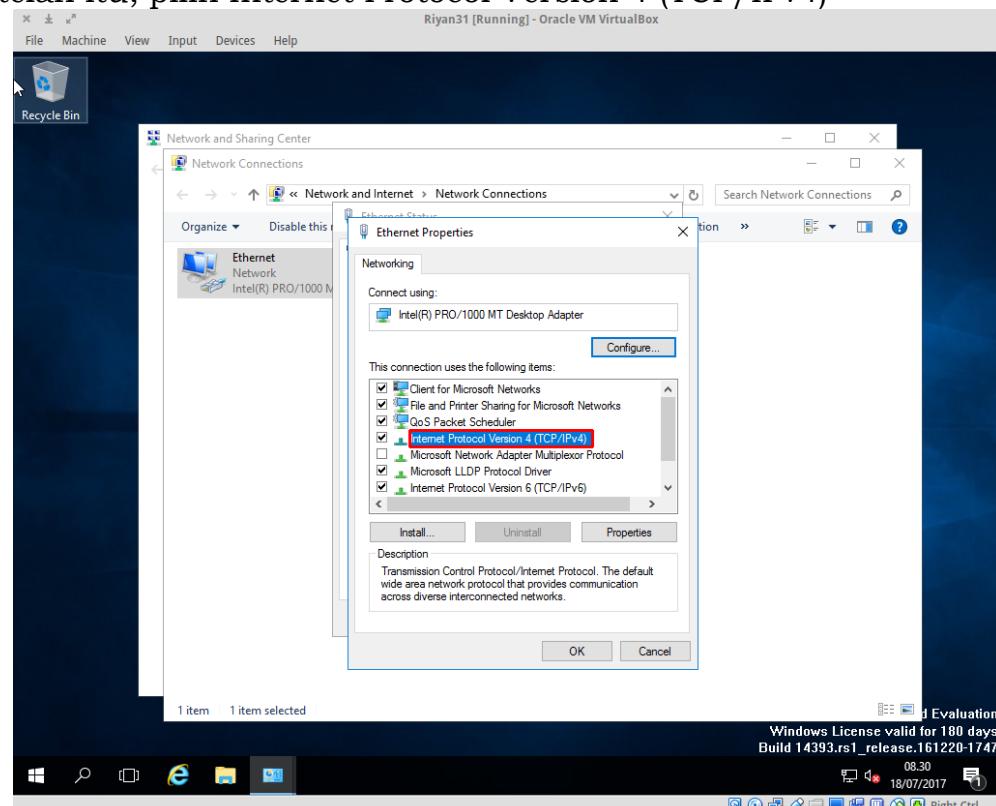
Gambar 8.24 change adapter settings

- Kemudian klik properties



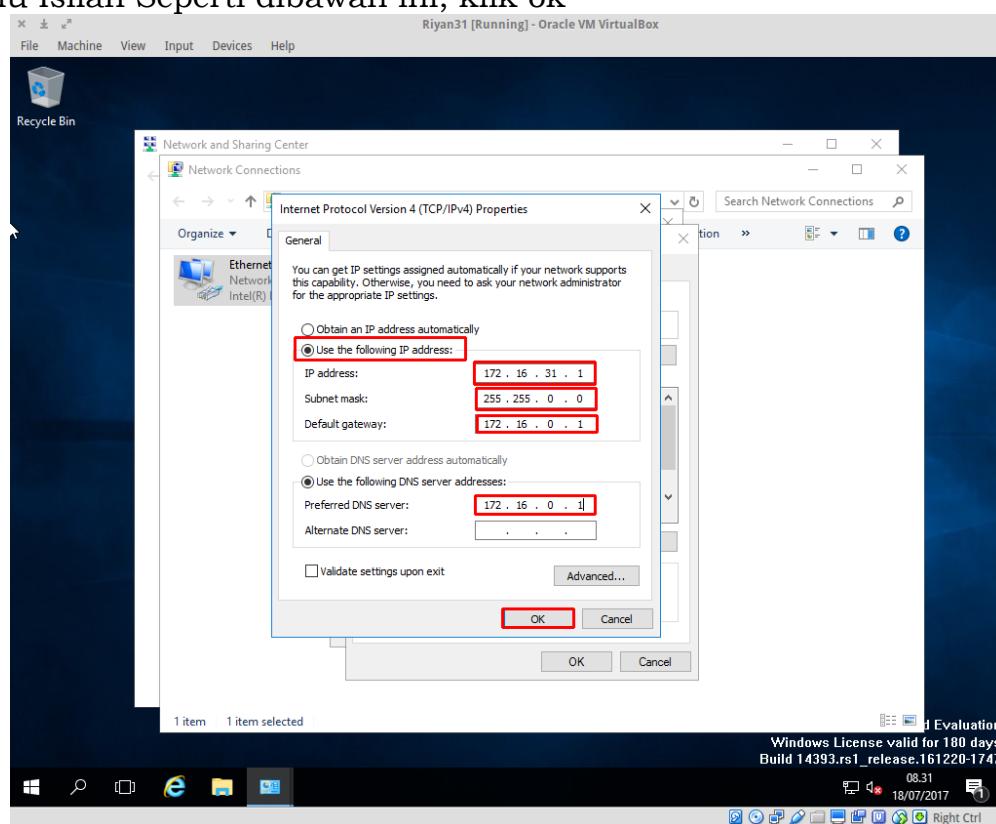
Gambar 8.25 pemilihan properties

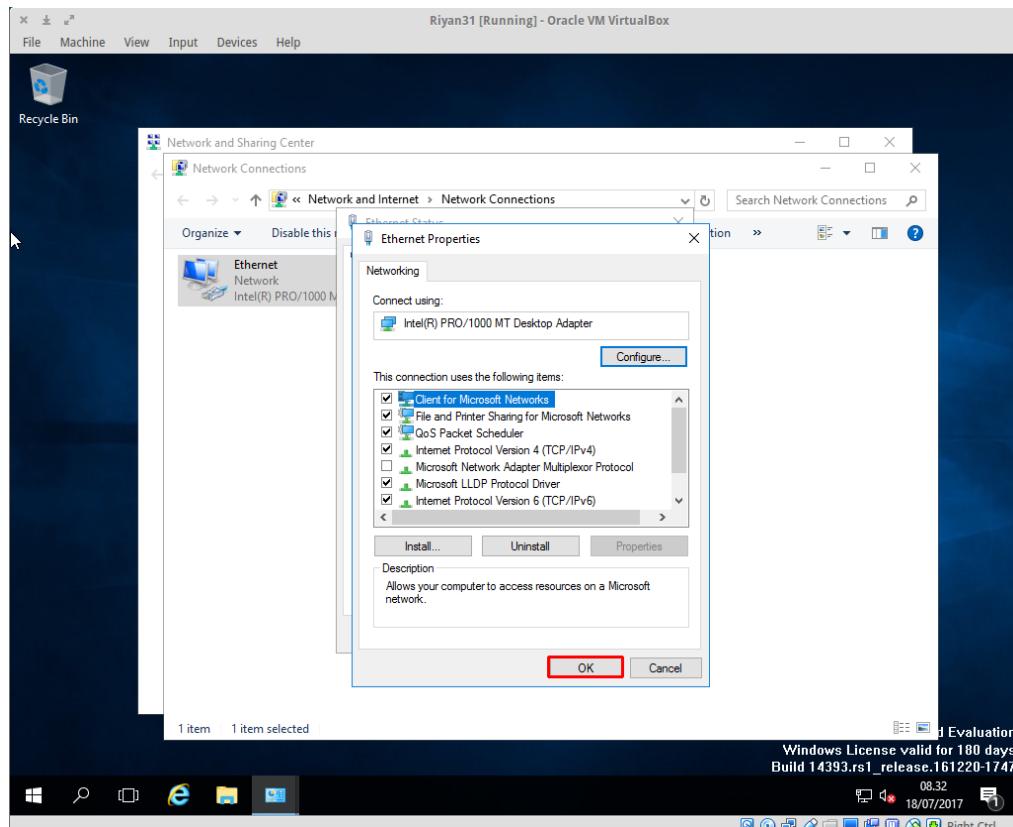
- Setelah itu, pilih Internet Protocol Version 4 (TCP/IPv4)



Gambar 8.26 Internet Protocol Version 4 (TCP/IPv4)

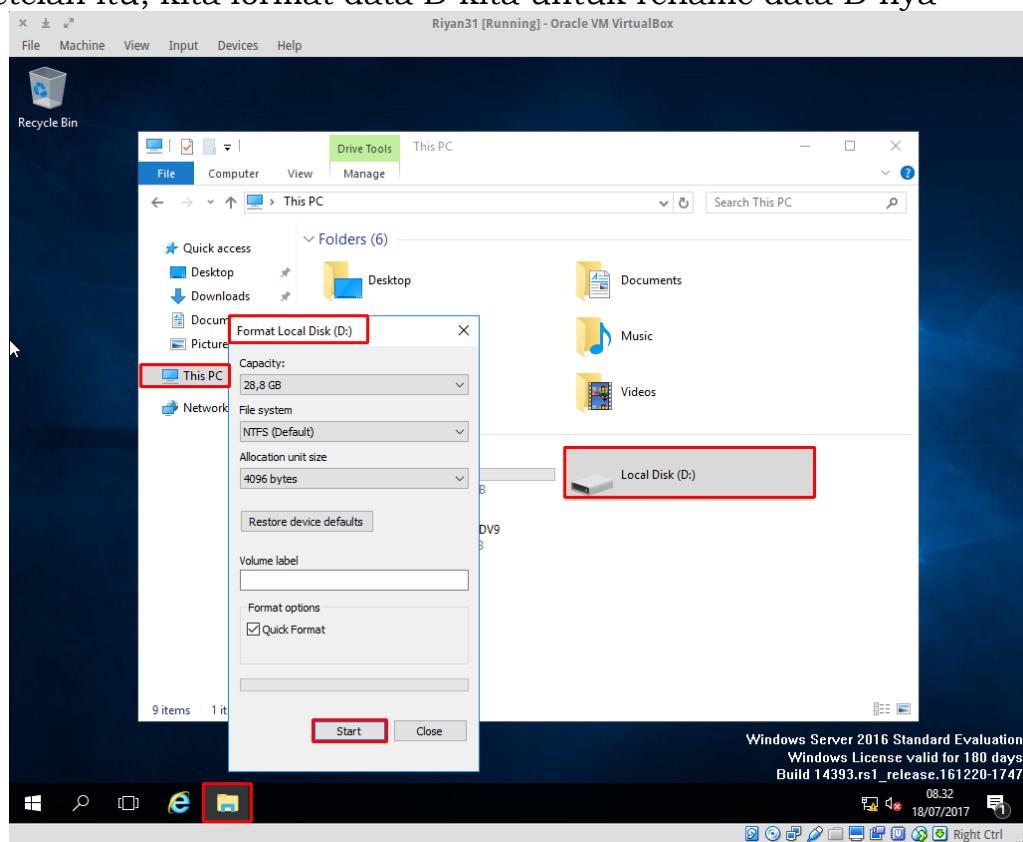
- Lalu Isilah Seperti dibawah ini, klik ok

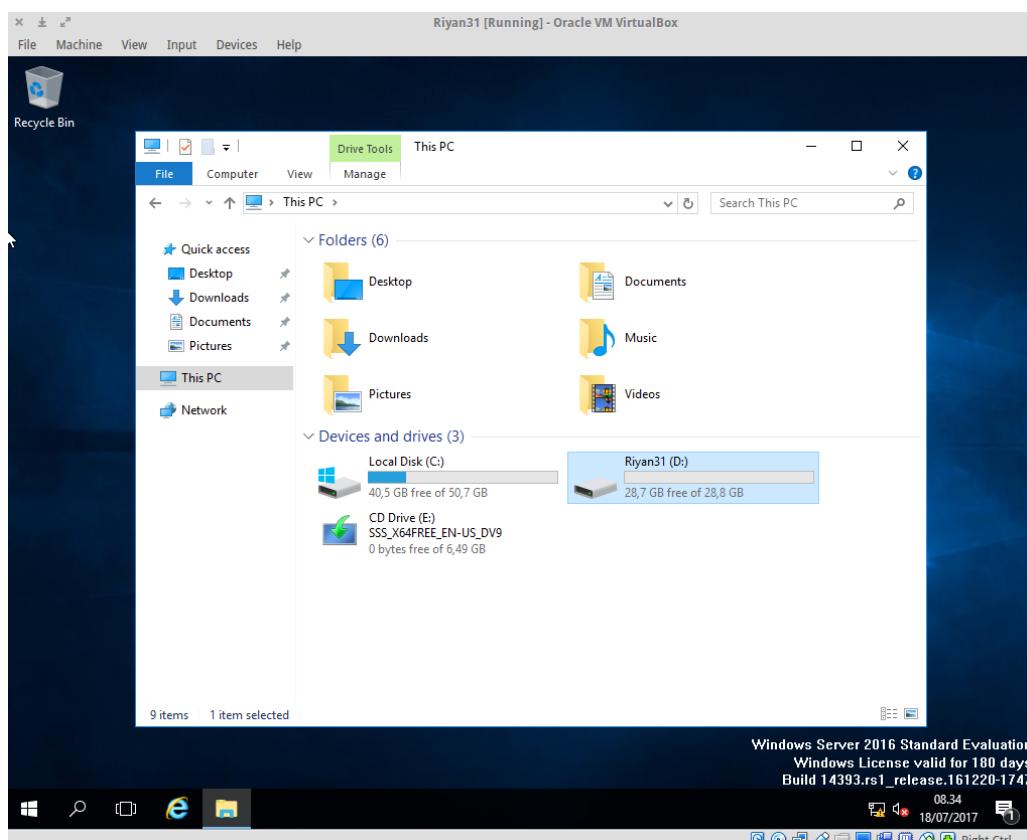
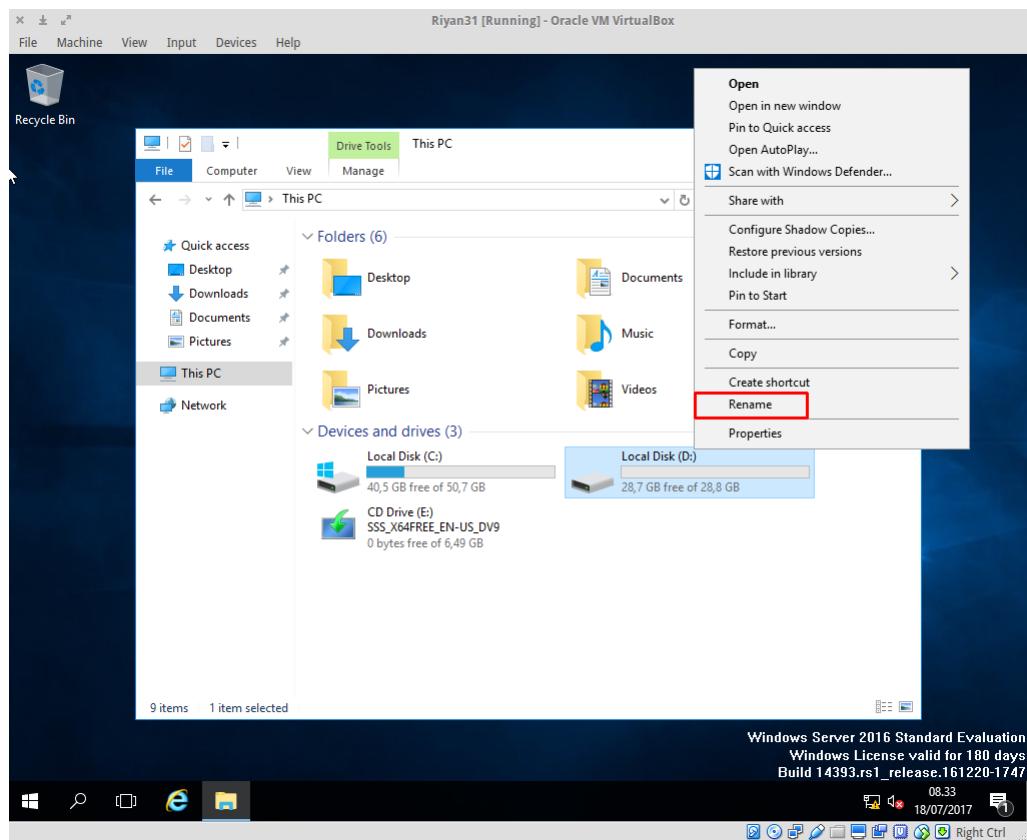




Gambar 8.27 pengisian IP dan DNS

- Setelah itu, kita format data D kita untuk rename data D nya



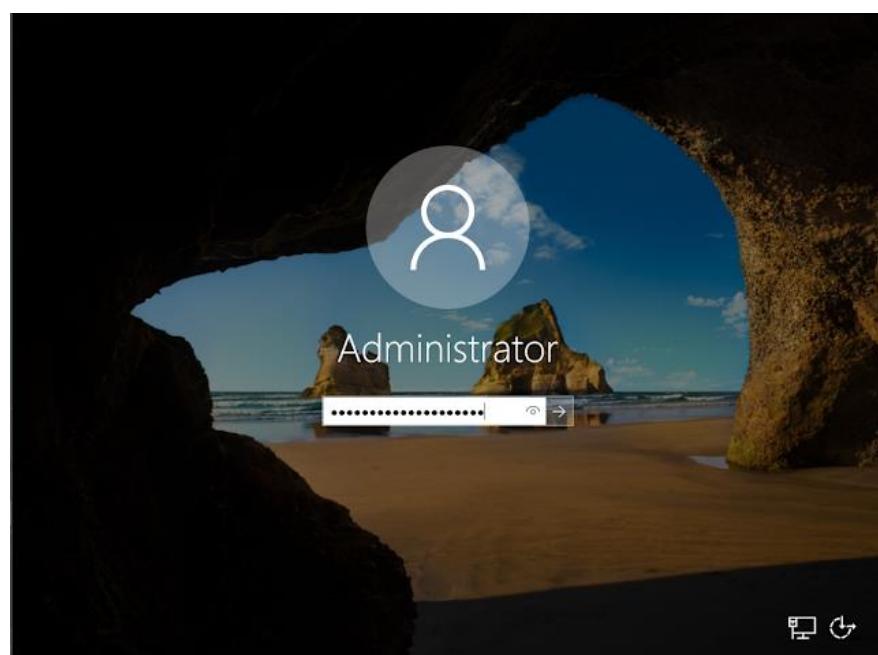


Gambar 8.28 melakukan format pada localdisk

8.3.8. Proses Instalasi dan Konfigurasi Active Directory Domain Service

Active Directory (AD) adalah layanan direktori yang dikembangkan Microsoft untuk domain Windows. Ini termasuk dalam kebanyakan sistem operasi Windows Server sebagai satu set proses dan layanan. Awalnya, Active Directory hanya bertanggung jawab atas pengelolaan domain terpusat. Dimulai dengan Windows Server 2016 , Active Directory menjadi judul payung untuk berbagai layanan berbasis identitas berbasis direktori.

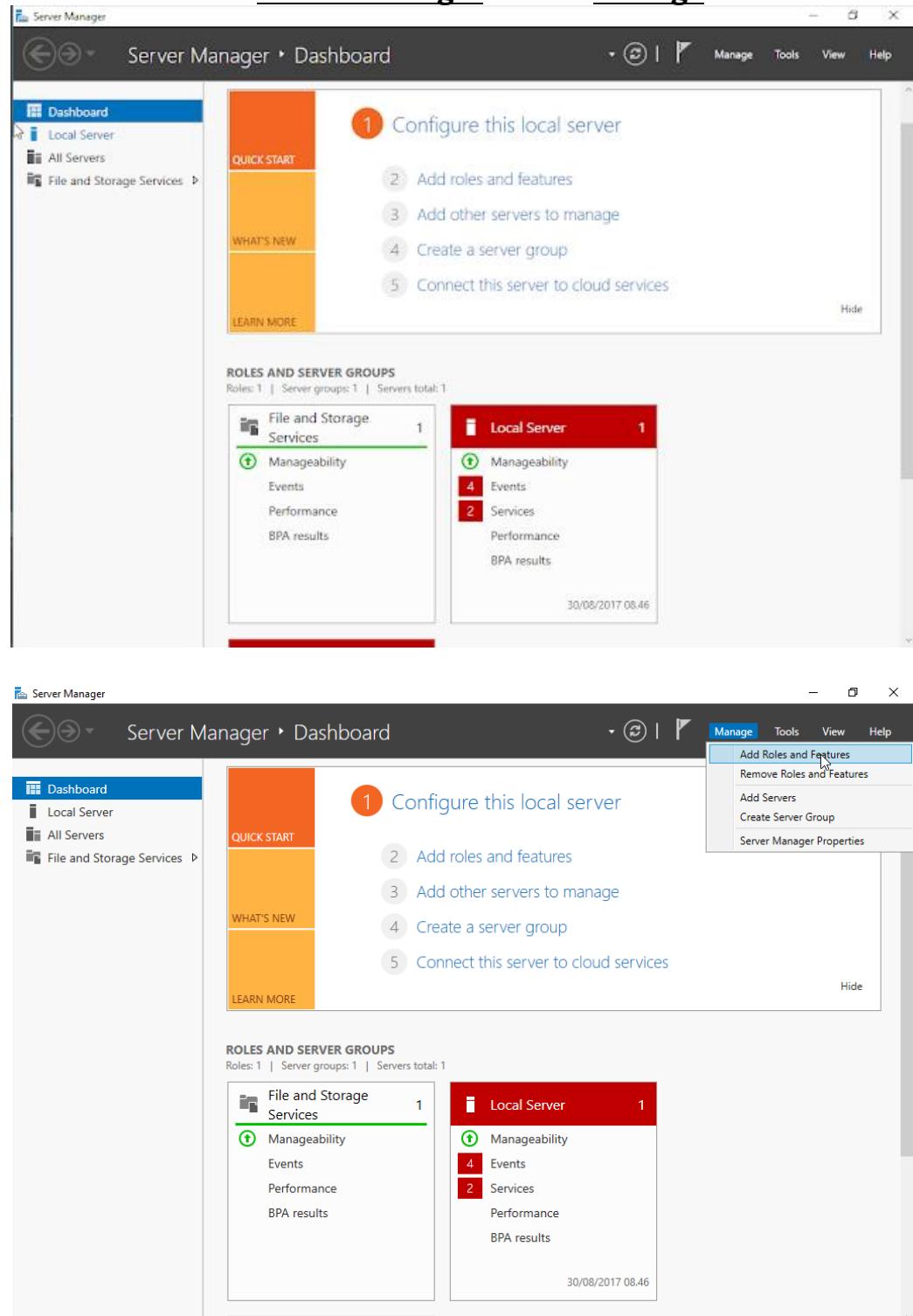
1. Klik Start → Administrative Tools → Server Manager, maka tampilan server manager, merupakan fasilitas yang digunakan untuk pengaturan dan konfigurasi windows server 2016.



Gambar 8.28 Administrative Tools



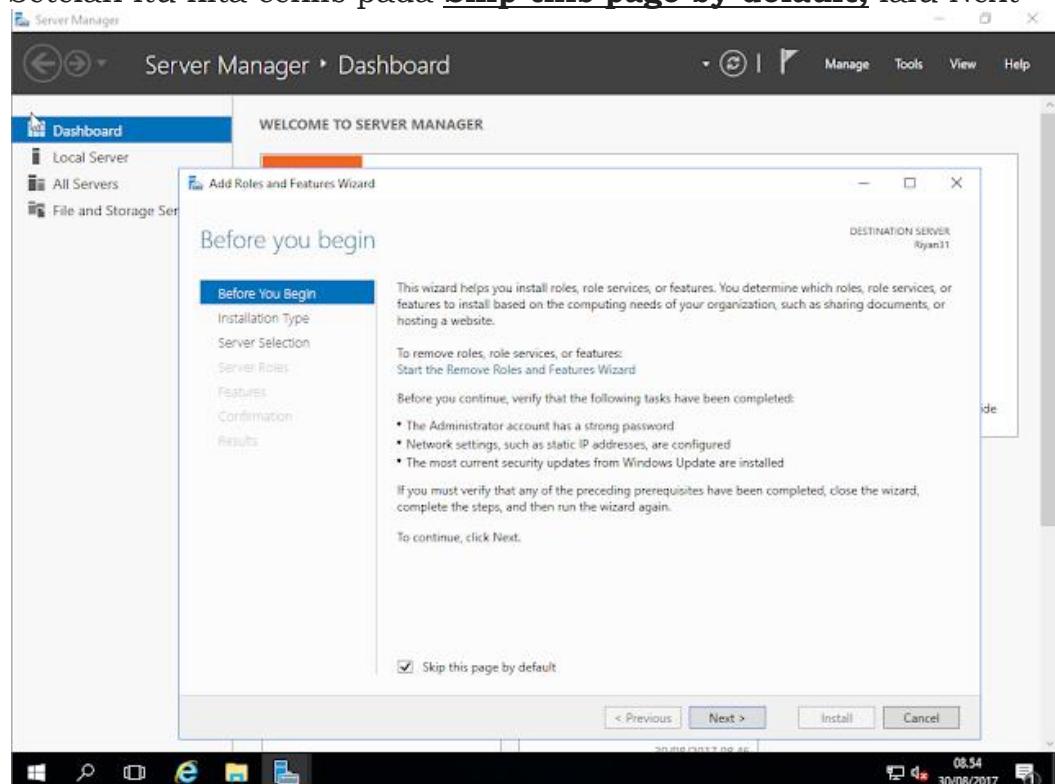
- Setelah itu kita ke **Server Manager** lalu ke **Manage**



Gambar 8.29 Server Manager

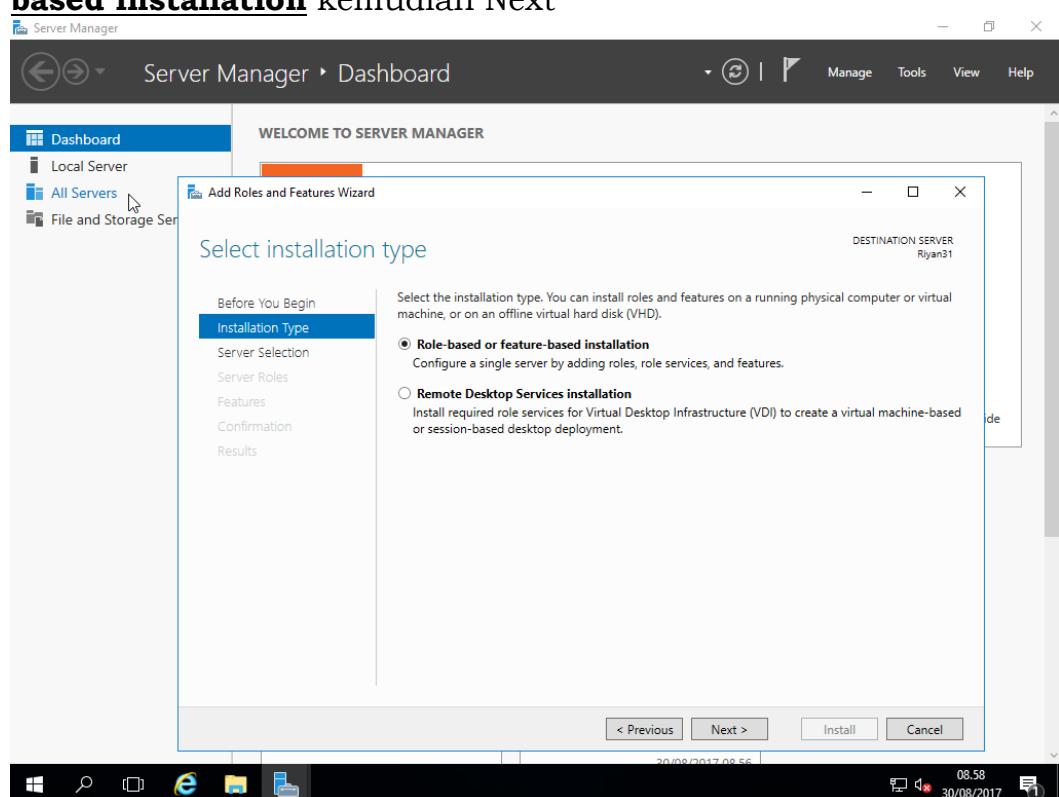


- Setelah itu kita ceklis pada Skip this page by default, lalu Next



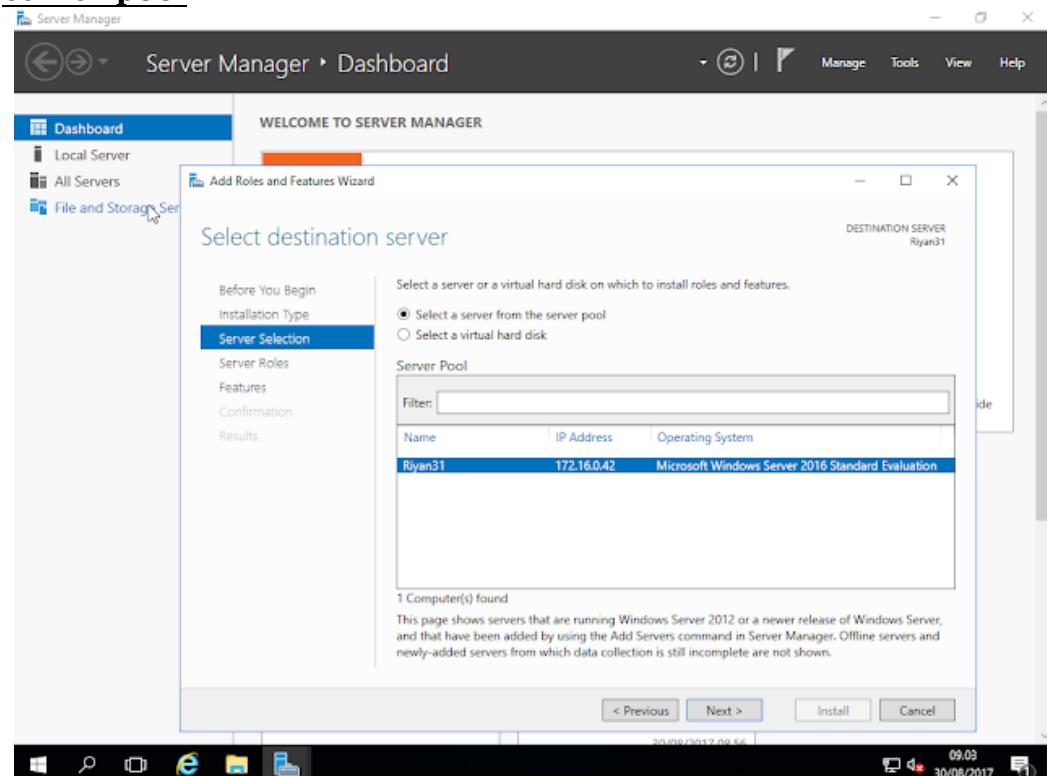
Gambar 8.30 Skip this page by default

- Lalu pada bagian **Installation Type** pilih **Role-based or feature-based installation** kemudian Next



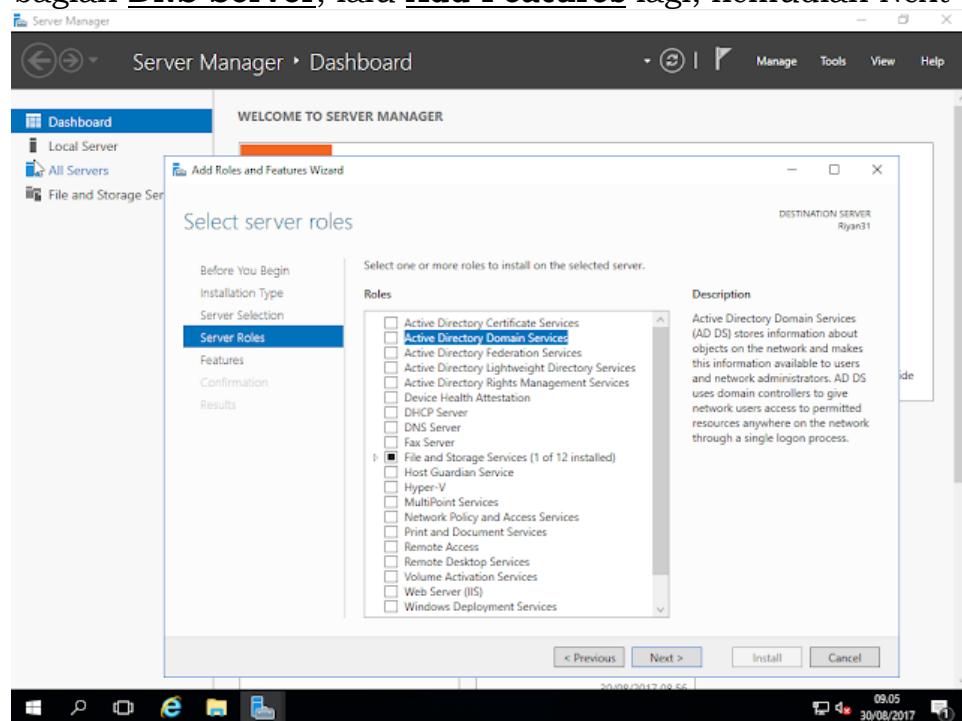
Gambar 8.31 Installation Type

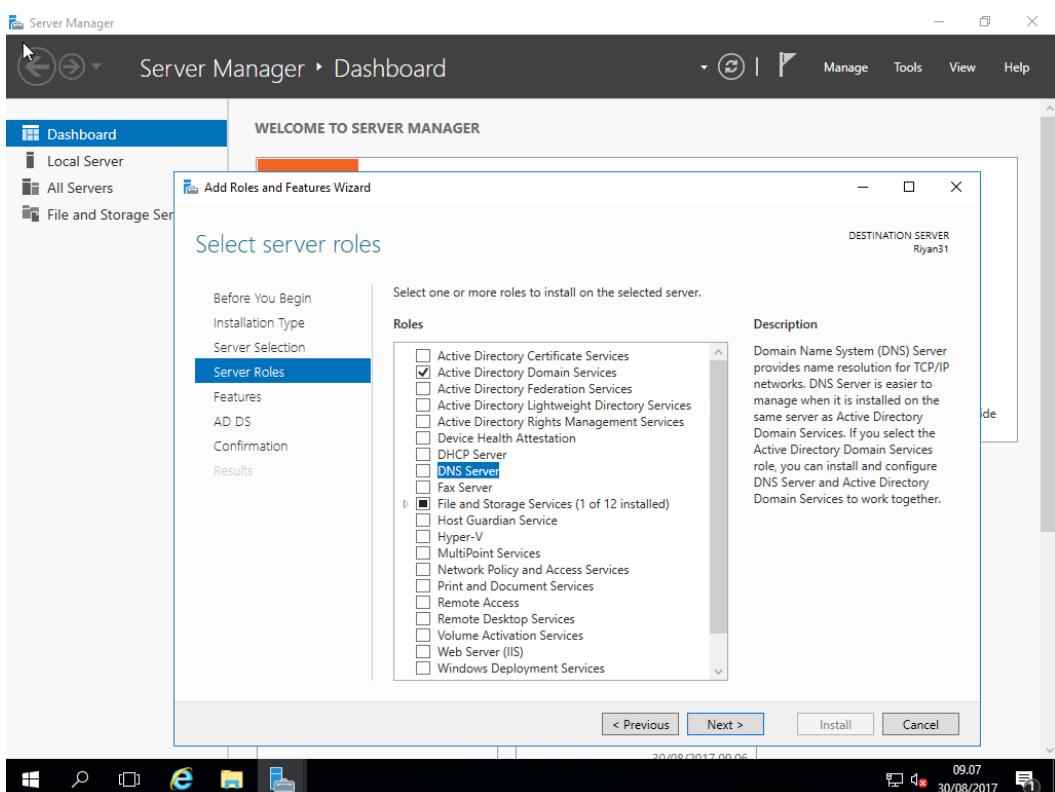
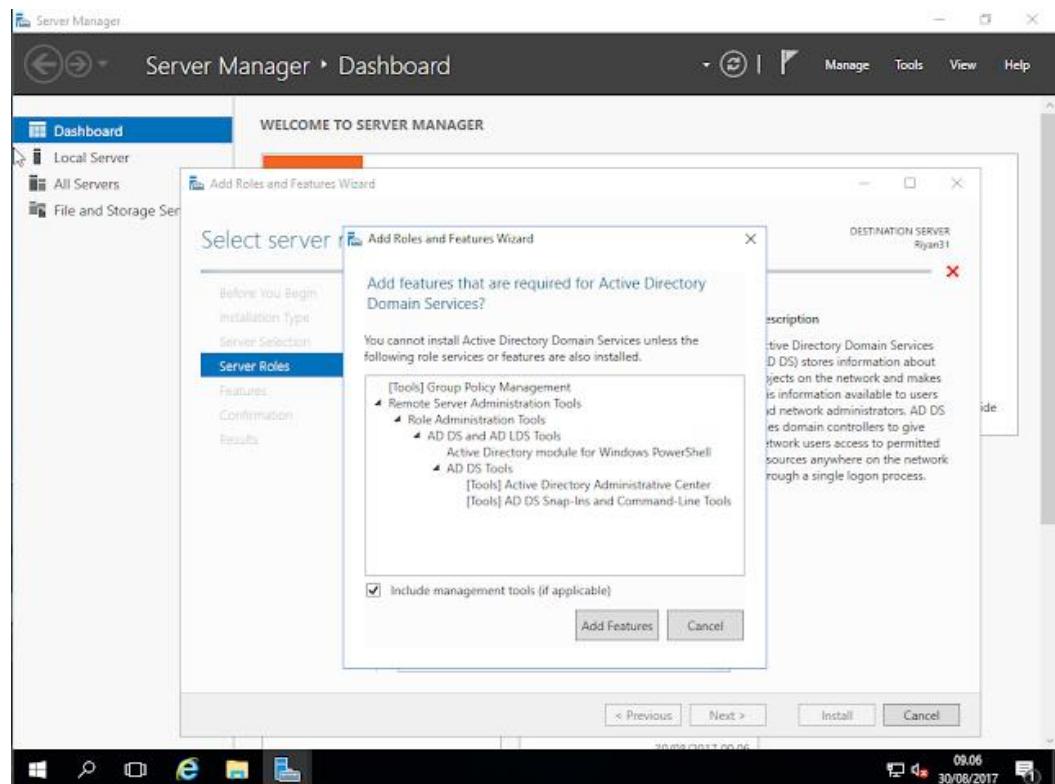
- Pada **Server Selection**, pilih yang **Select a server from the server pool**

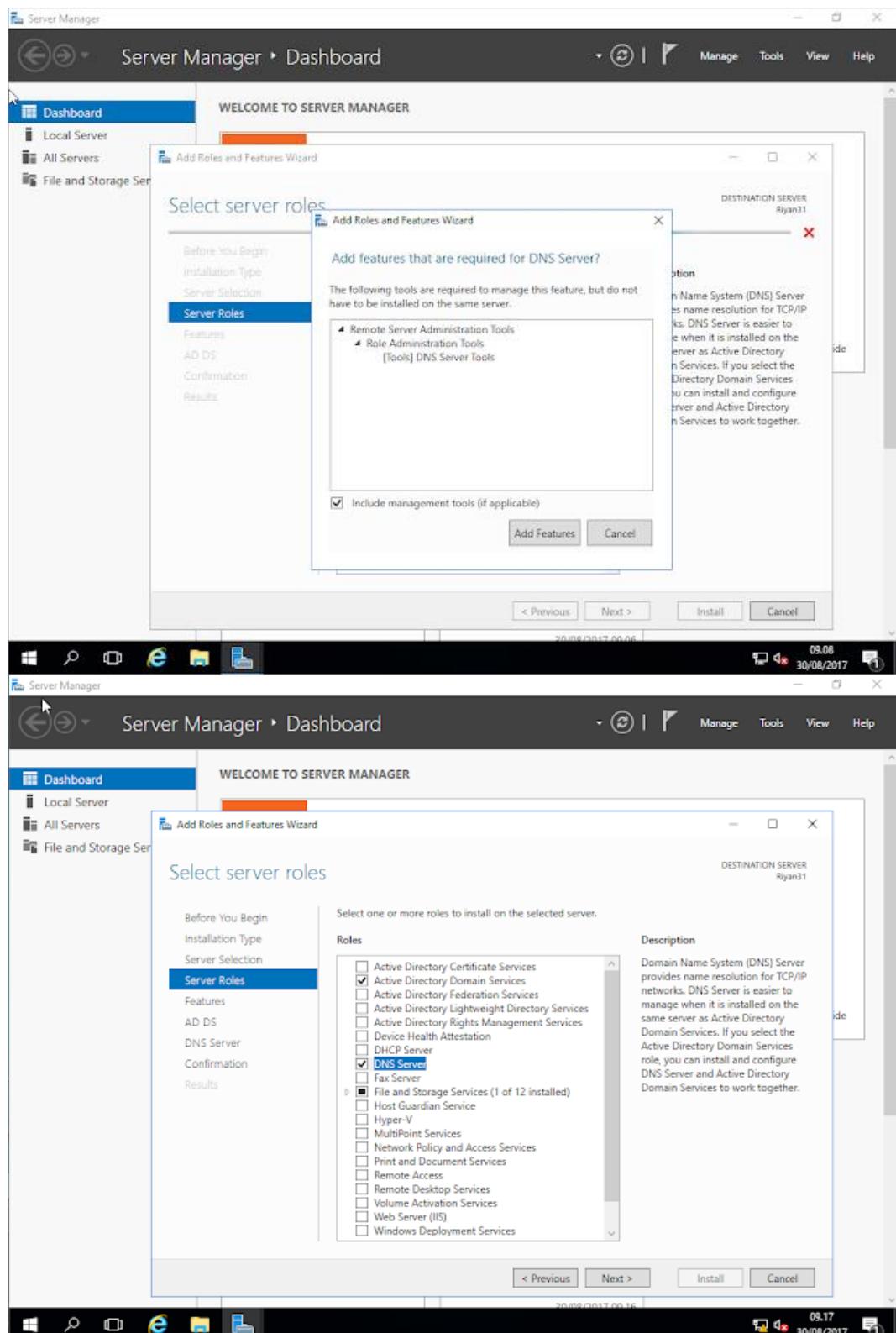


Gambar 8.32 select a server

- Kemudian pada **Server Roles**, ceklis pada bagian **Active Directory Domain Services**, lalu **Add Features**, kemudian ceklis bagian **DNS Server**, lalu **Add Features** lagi, kemudian Next



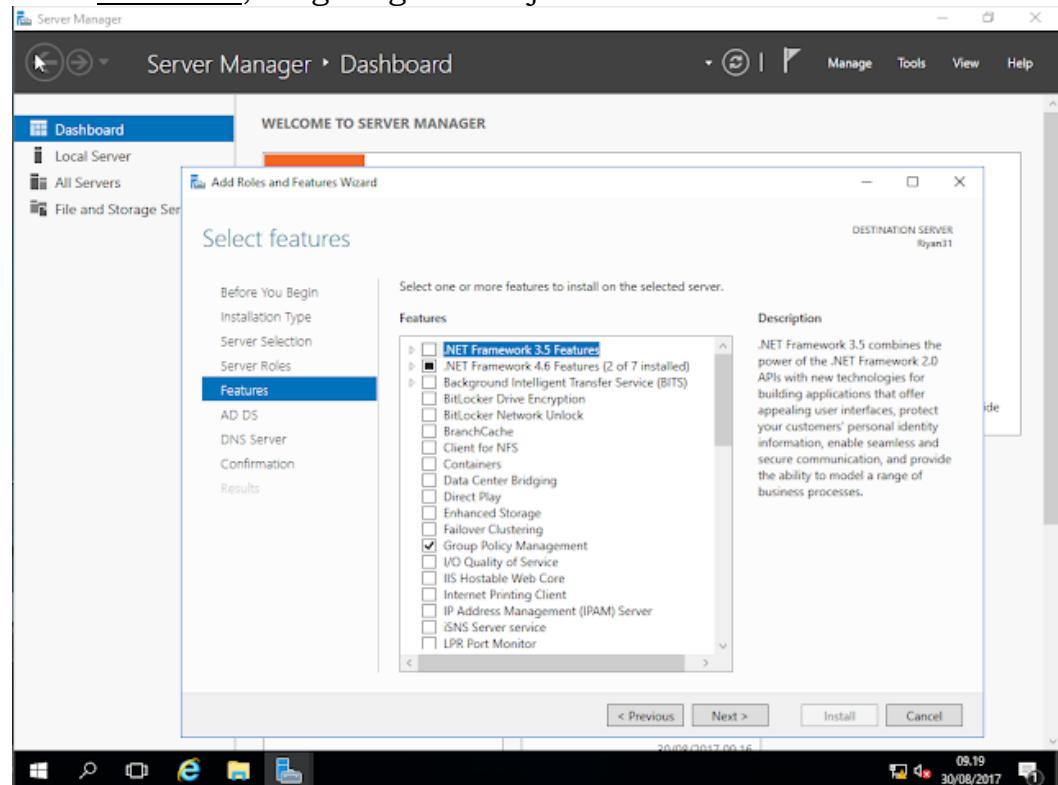




Gambar 8.33 server roles

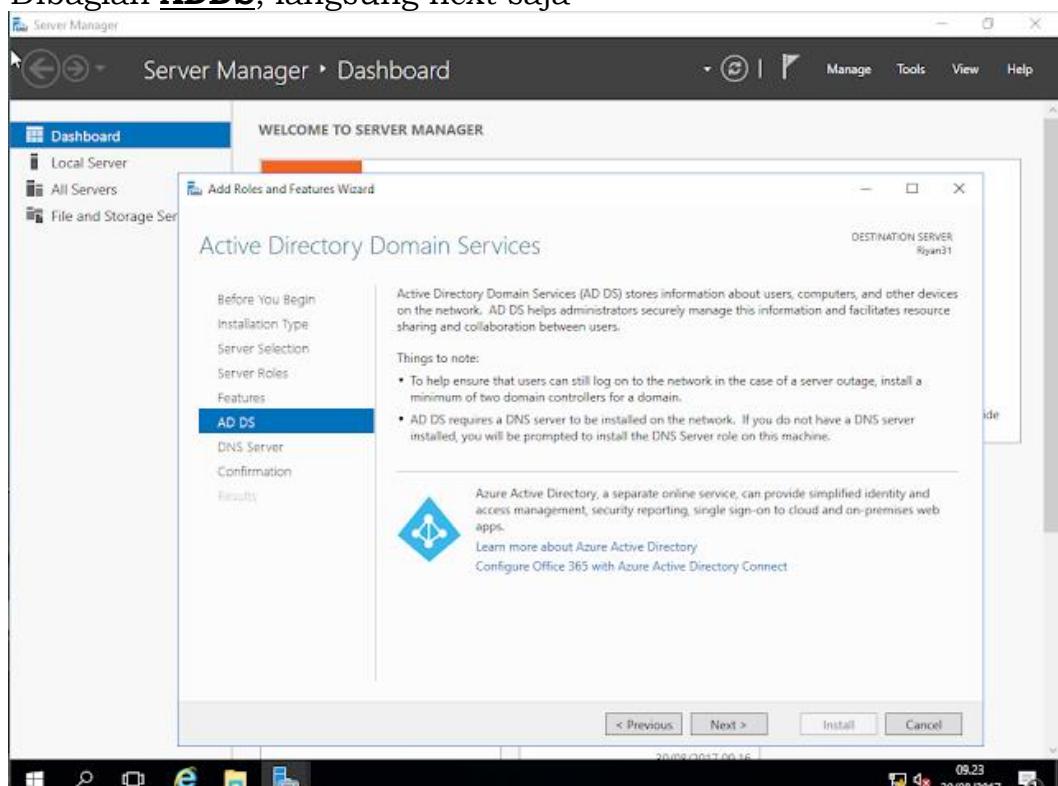


- Pada **Features**, langsung next saja



Gambar 8.34 features

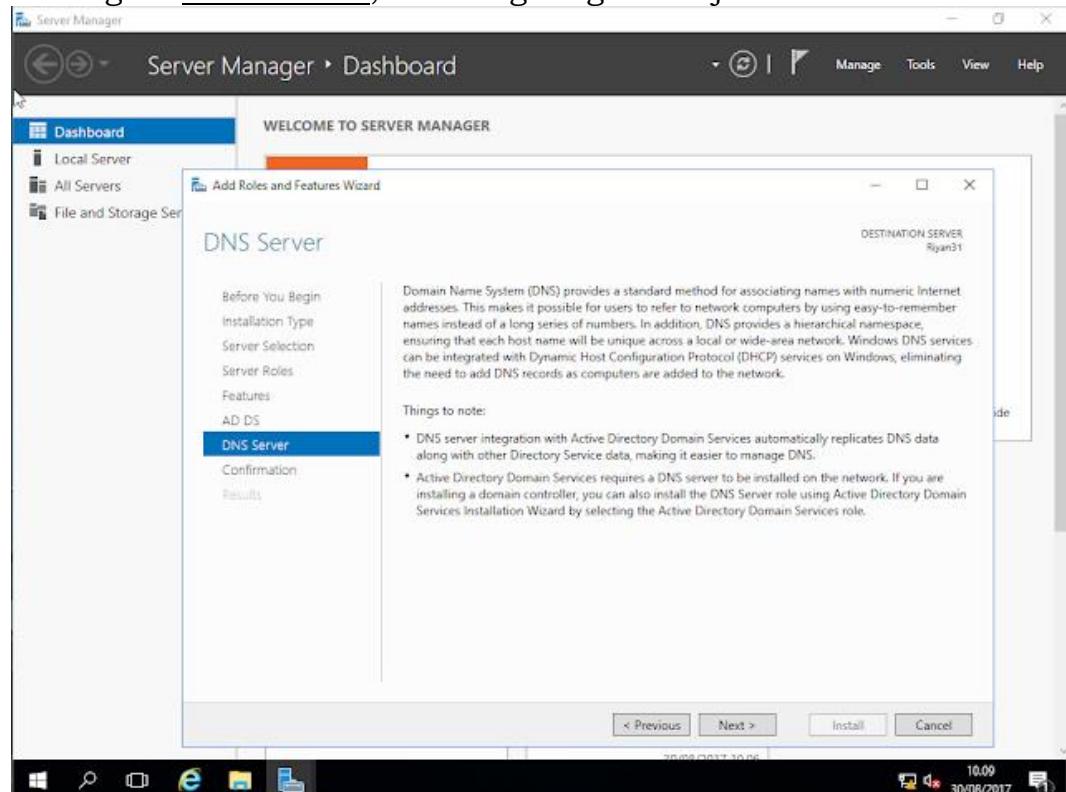
- Dibagian **ADDS**, langsung next saja



Gambar 8.35 bagian Active Directory Domain Services

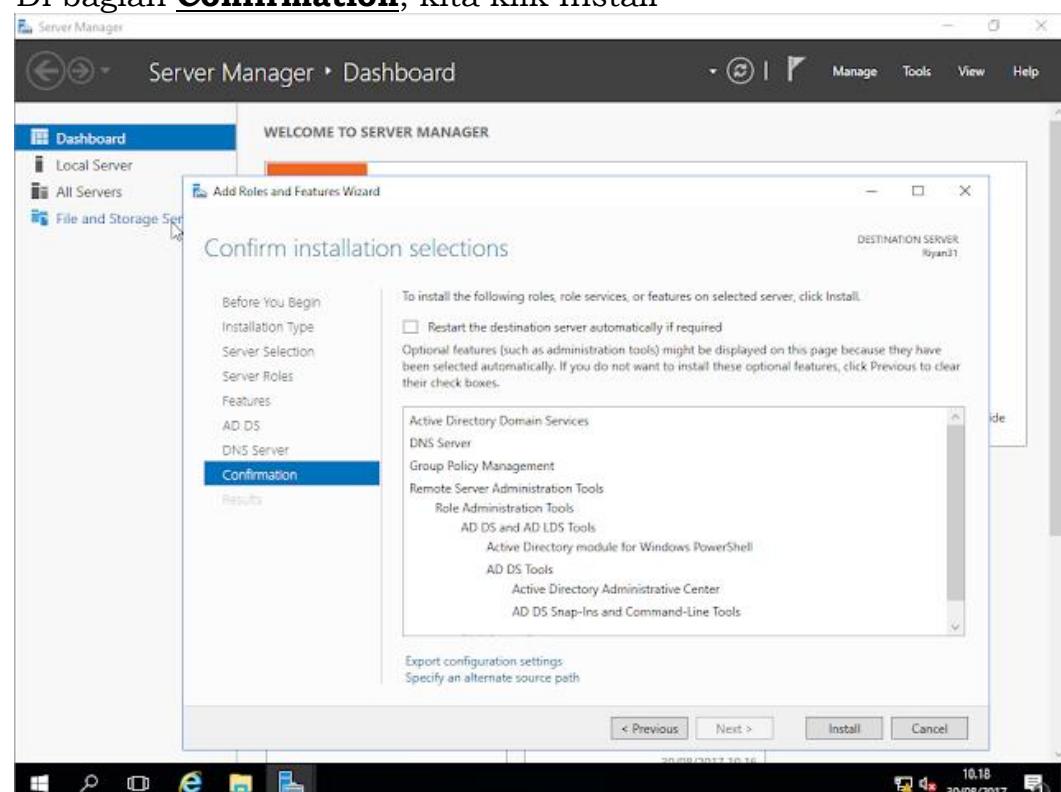


- Di bagian **DNS Server**, kita langsung Next aja



Gambar 8.36 DNS Server

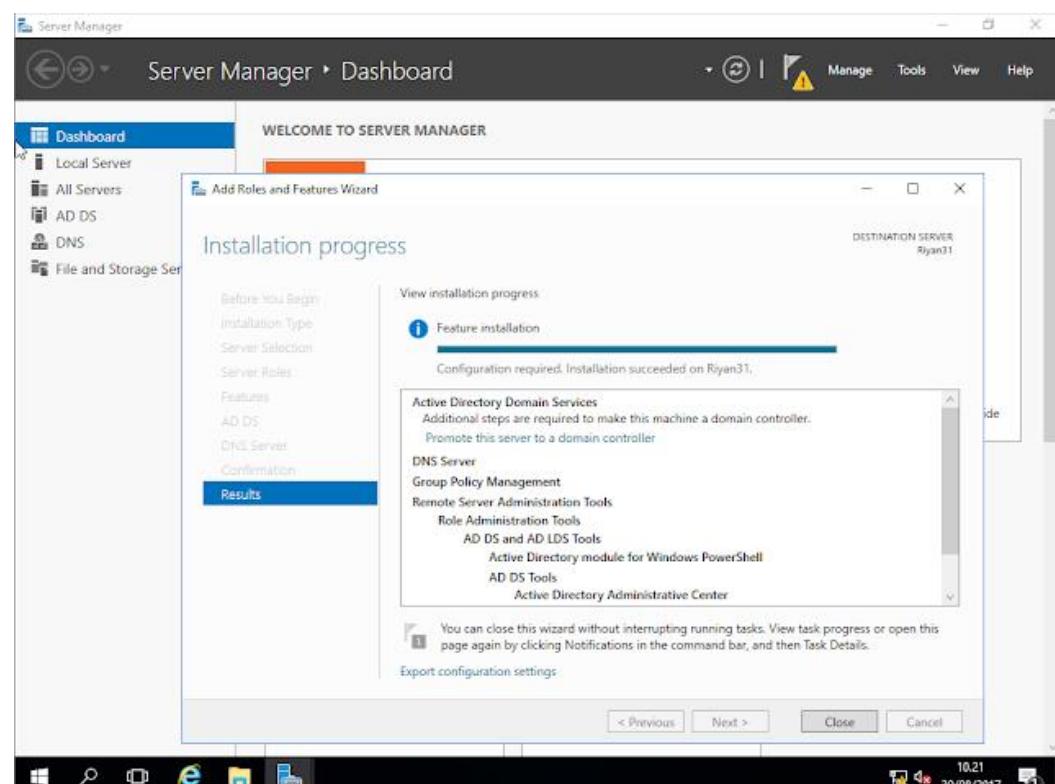
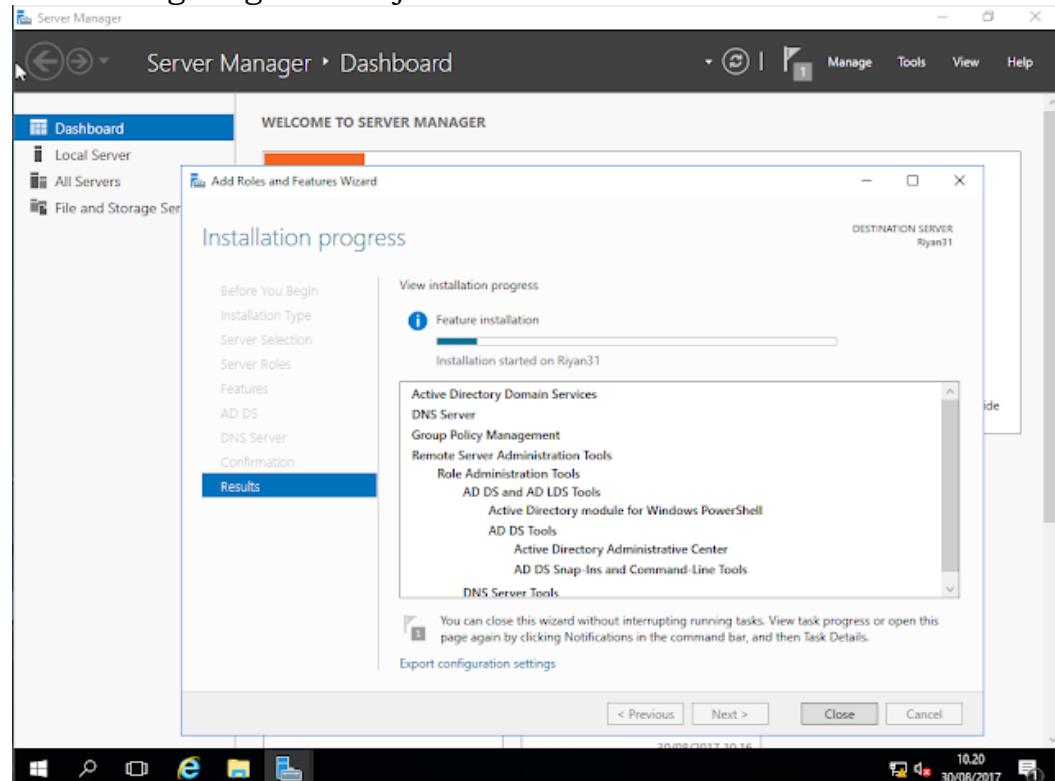
- Di bagian **Confirmation**, kita klik Install



Gambar 8.37 Confirmation



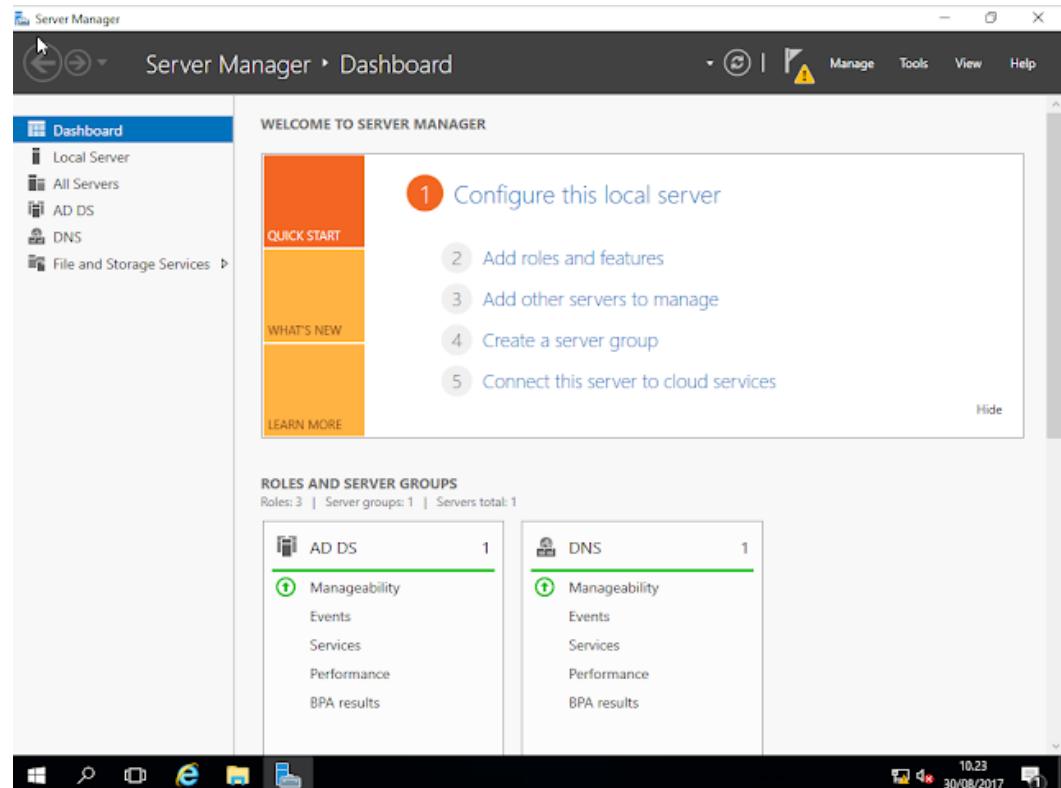
- Dibagian **Results** ini kita tunggu sampai prosesnya selesai, bila sudah langsung close saja



Gambar 8.38 proses selesai

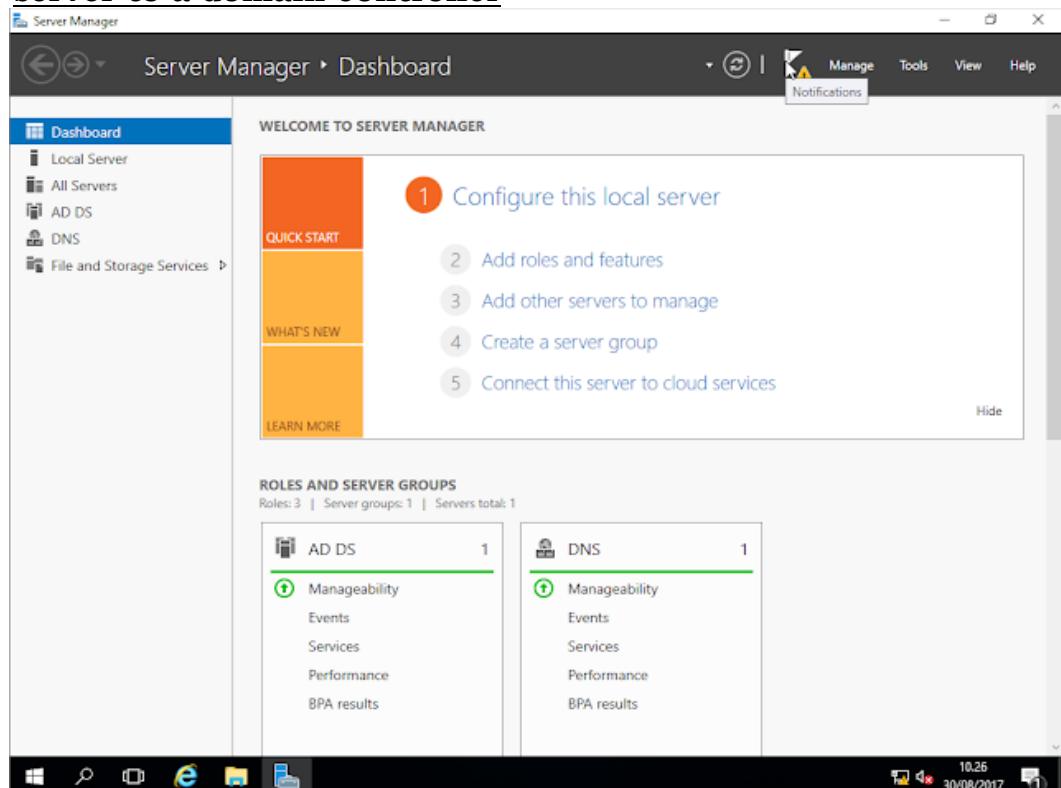


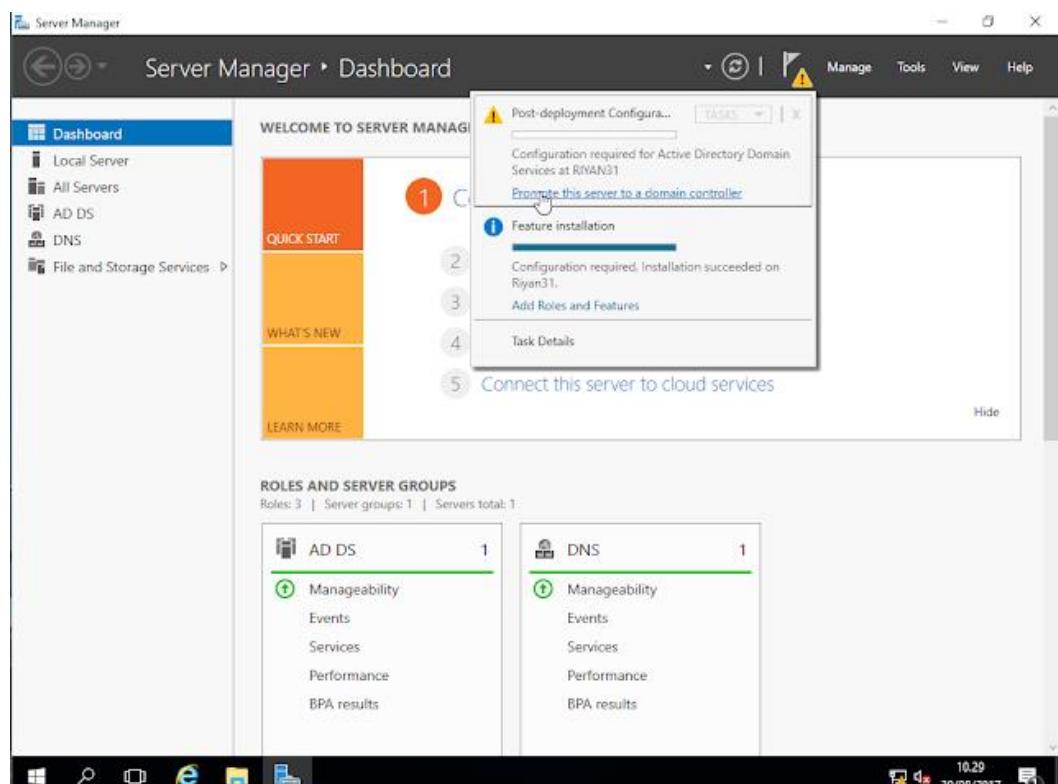
- Nahh disini kita bisa lihat ada tambahan **ADDS** dan **DNS**



Gambar 8.39 ADDS & DNS

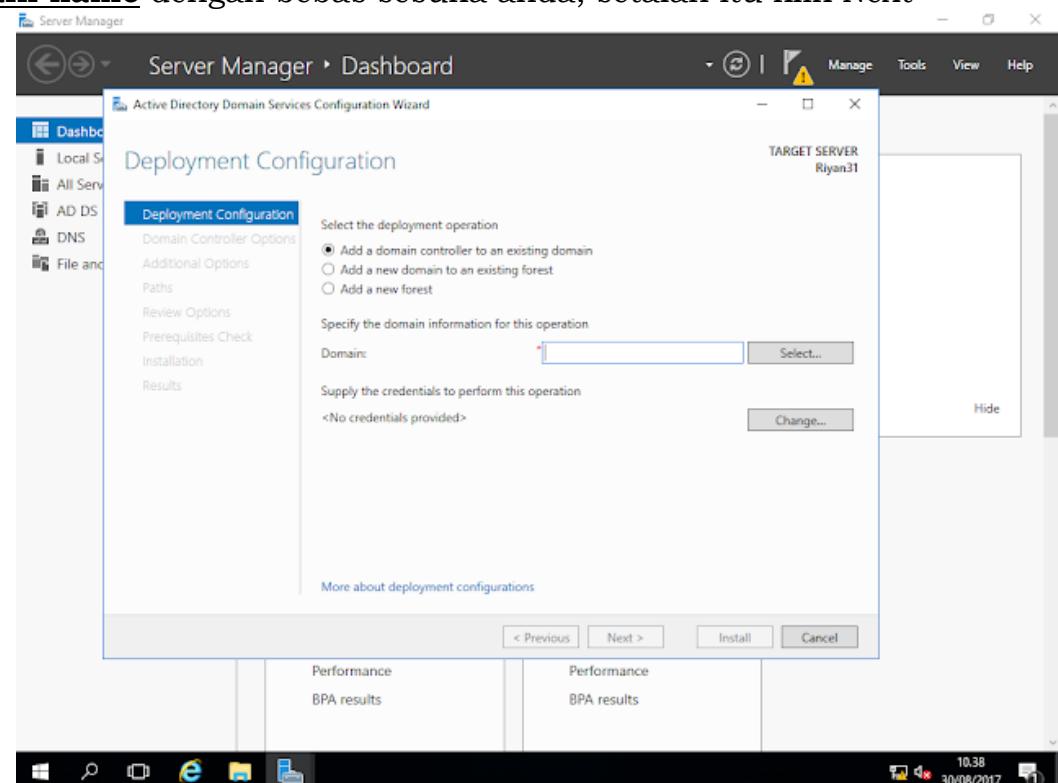
- Setelah itu kita klik icon yang bergambar bendera dan tanda seru, ini adalah bagian **Notification**, lalu kita klik pada **Promote this server to a domain controller**

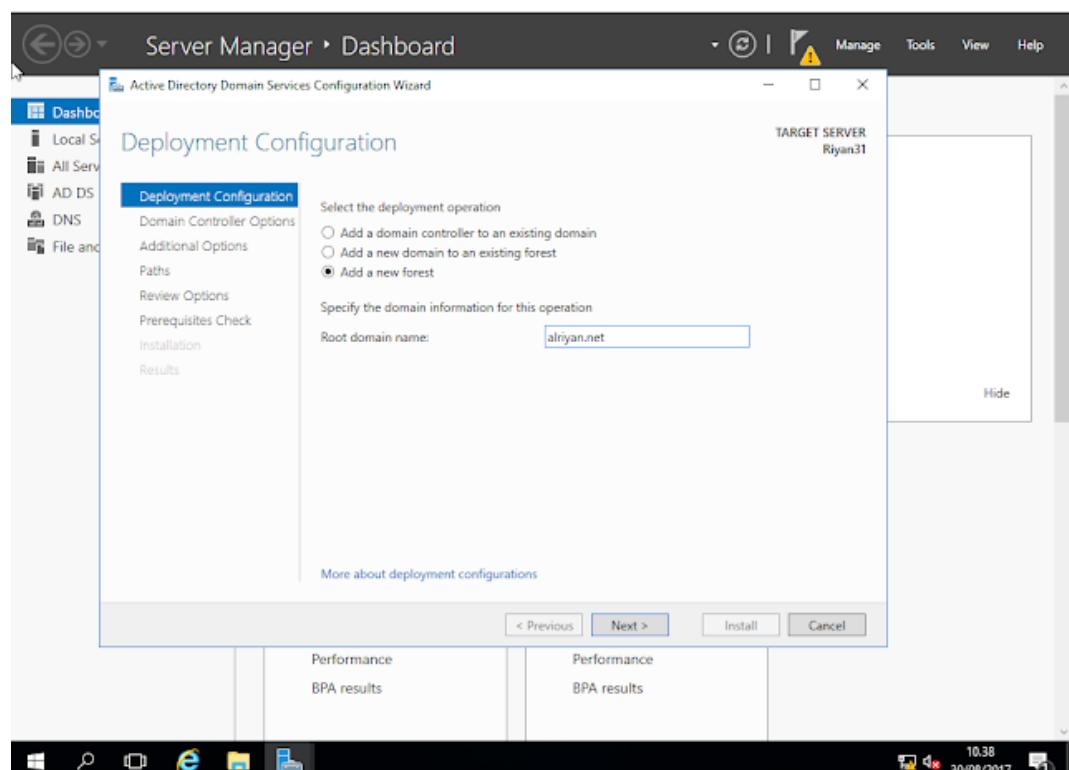




Gambar 8.40 Notification

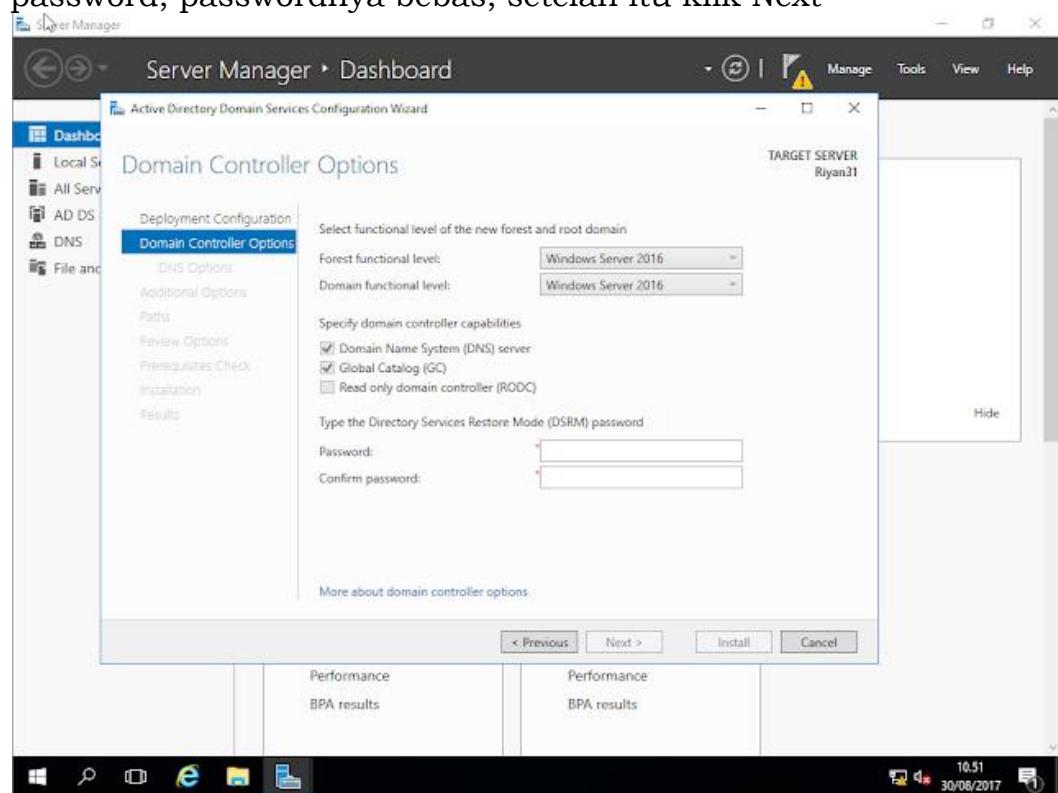
- Setelah itu akan muncul Bagan **Deployment Configuration**, nah setelah itu kita pilih yang **Add a new forest**, setelah itu kita isi **Root domain name** dengan bebas sesuka anda, setalah itu klik Next

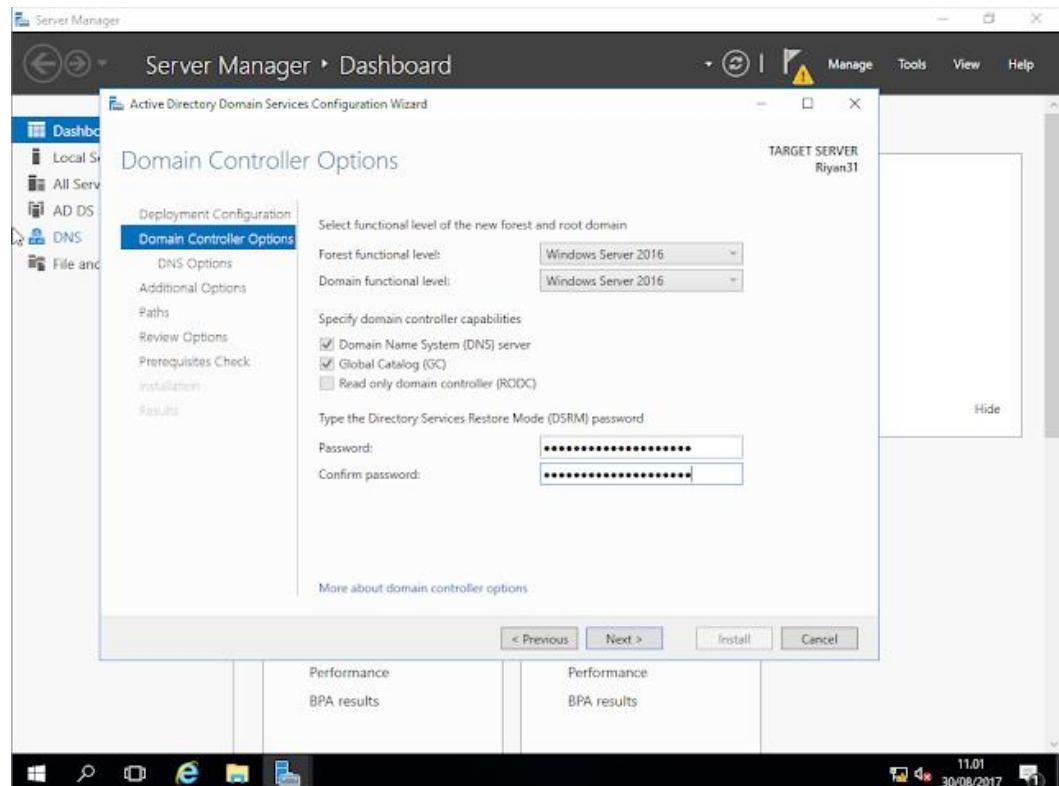




Gambar 8.41 Deployment Configuration

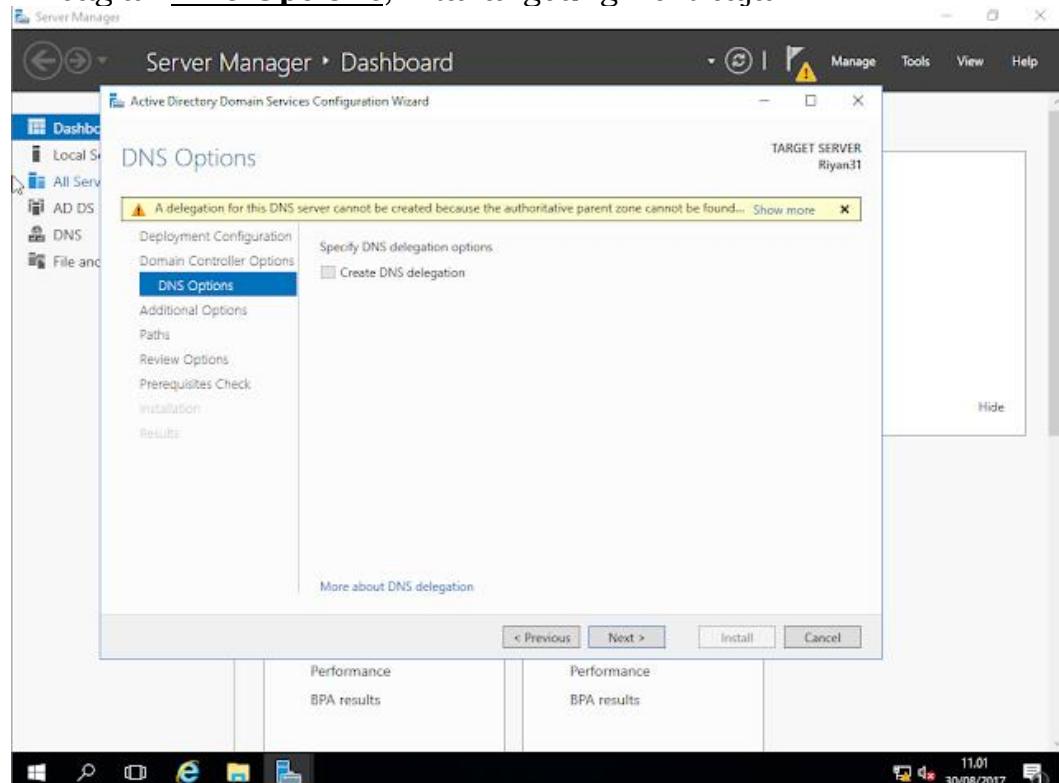
- Pada **Domain Controller Options**, kita harus memasukkan password, passwordnya bebas, setelah itu klik Next





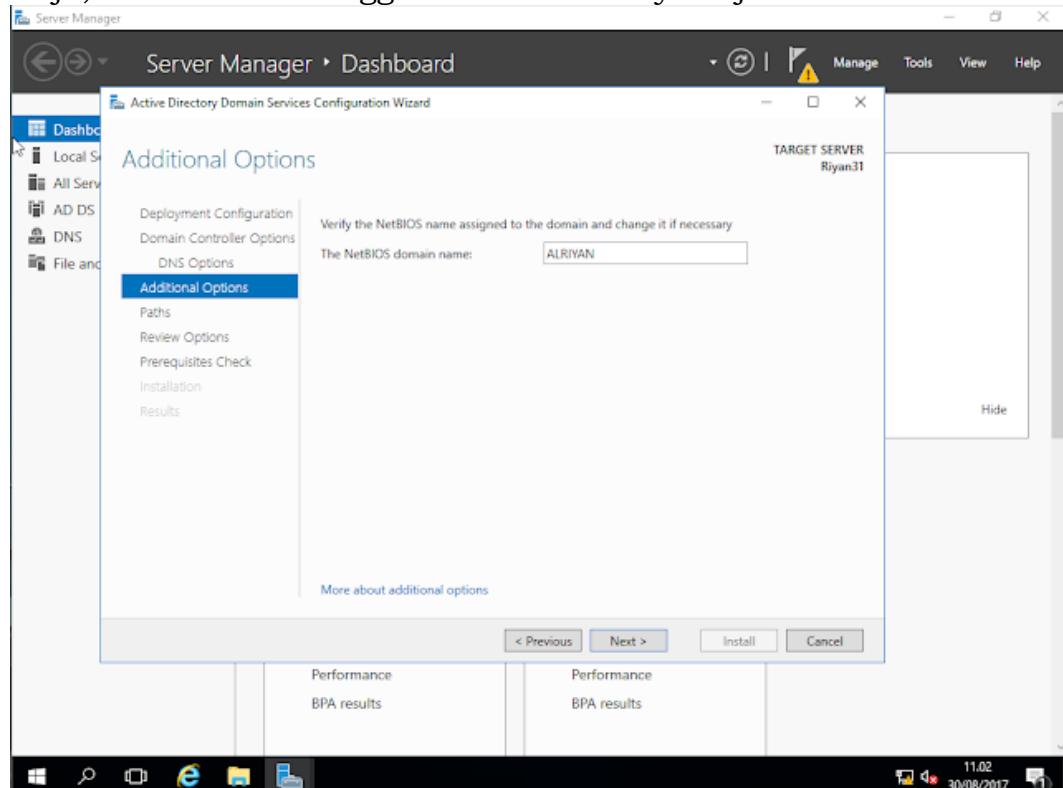
Gambar 8.42 Domain Controller Options

- Di bagian **DNS Options**, kita langsung Next saja



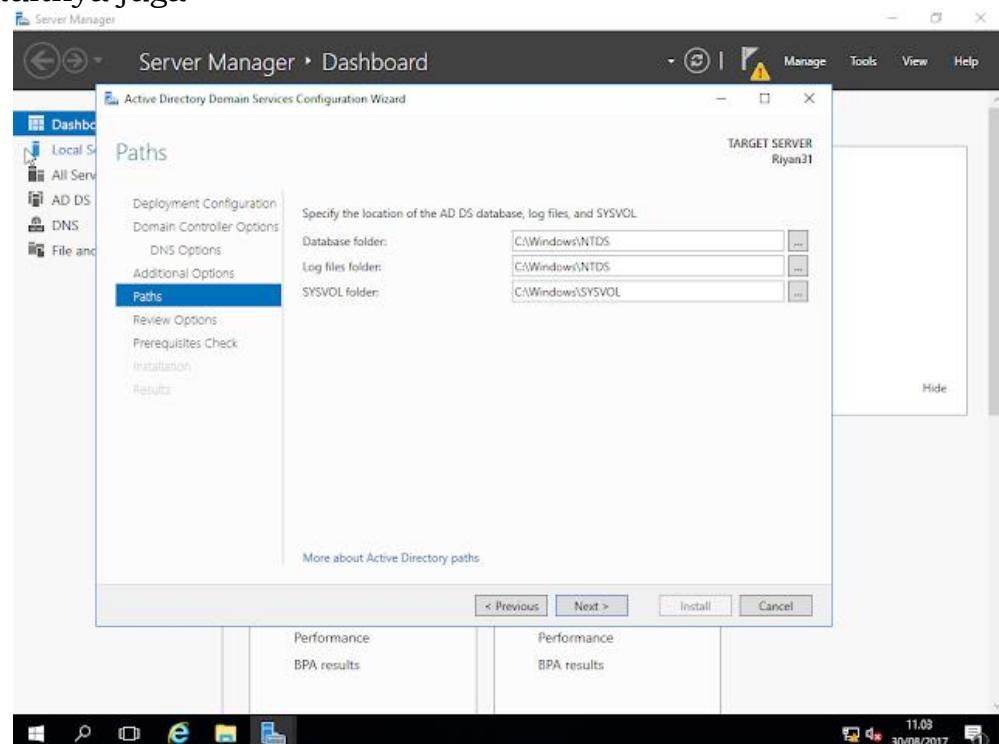
Gambar 8.43 DNS Options

- Setelah itu, di bagian **Additional Options**, kita langsung Next saja, karena kita menggunakan defaultnya saja



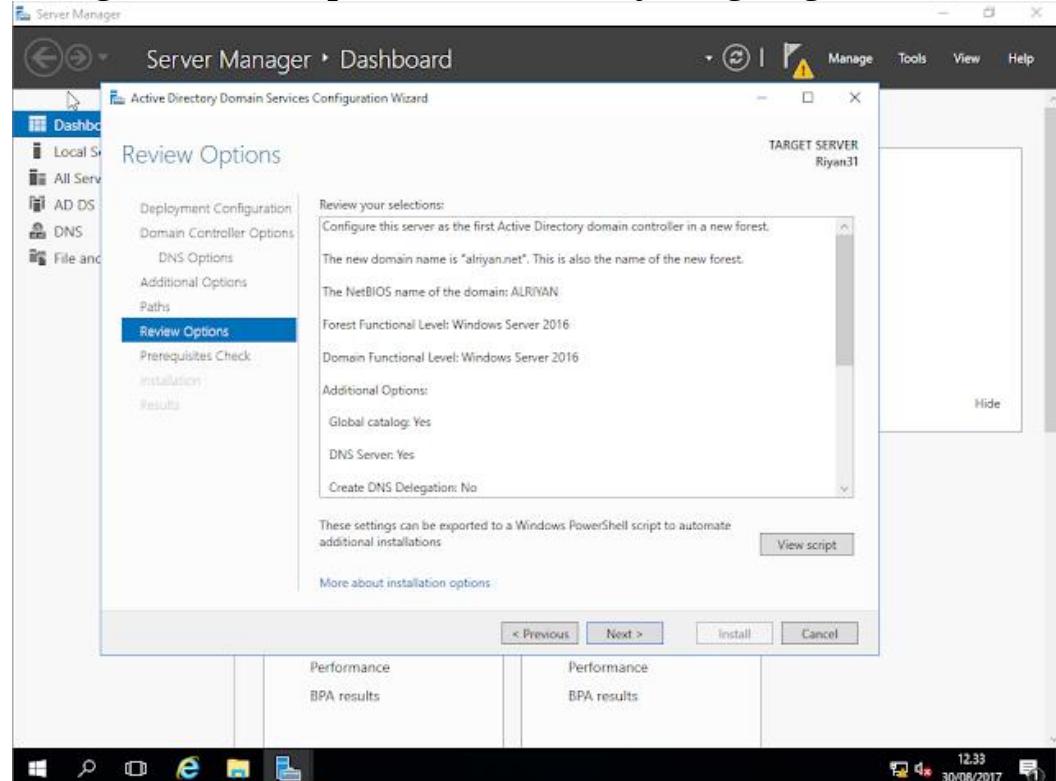
Gambar 8.44 Additional Options

- Di bagian **Paths** juga langsung kita Next saja karena kita menggunakan yang defaultnya juga



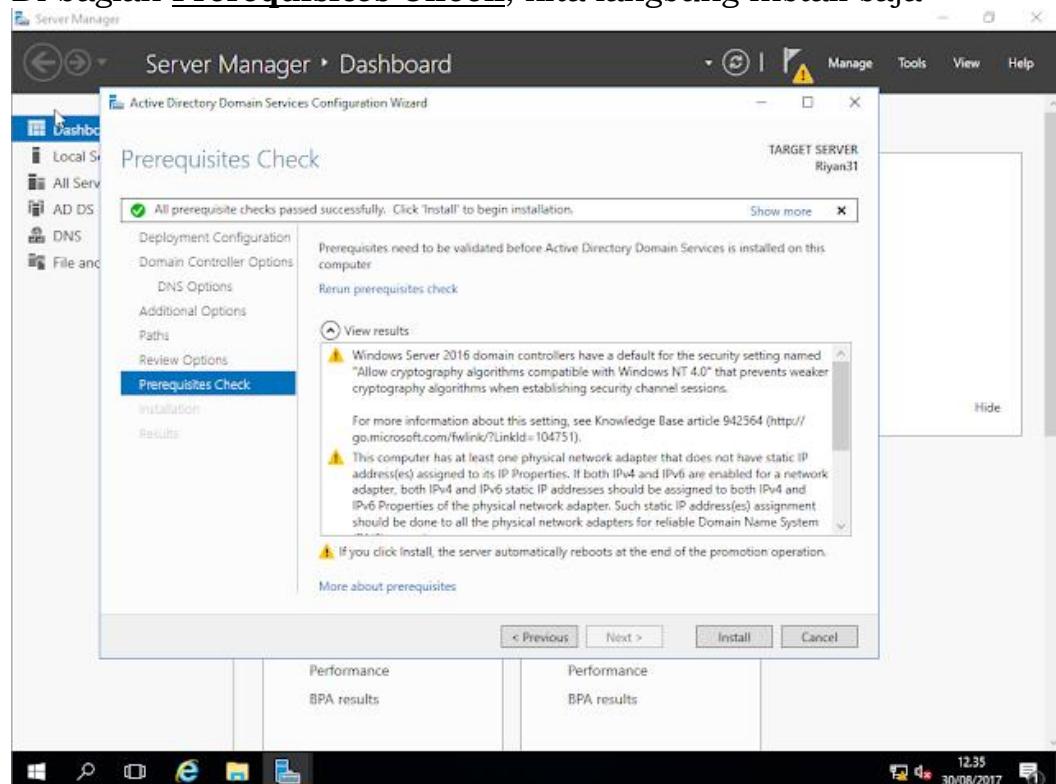
Gambar 8.45 Paths

- Di bagian **Review Options**, kita Next saja langsung



Gambar 8.46 Review Options

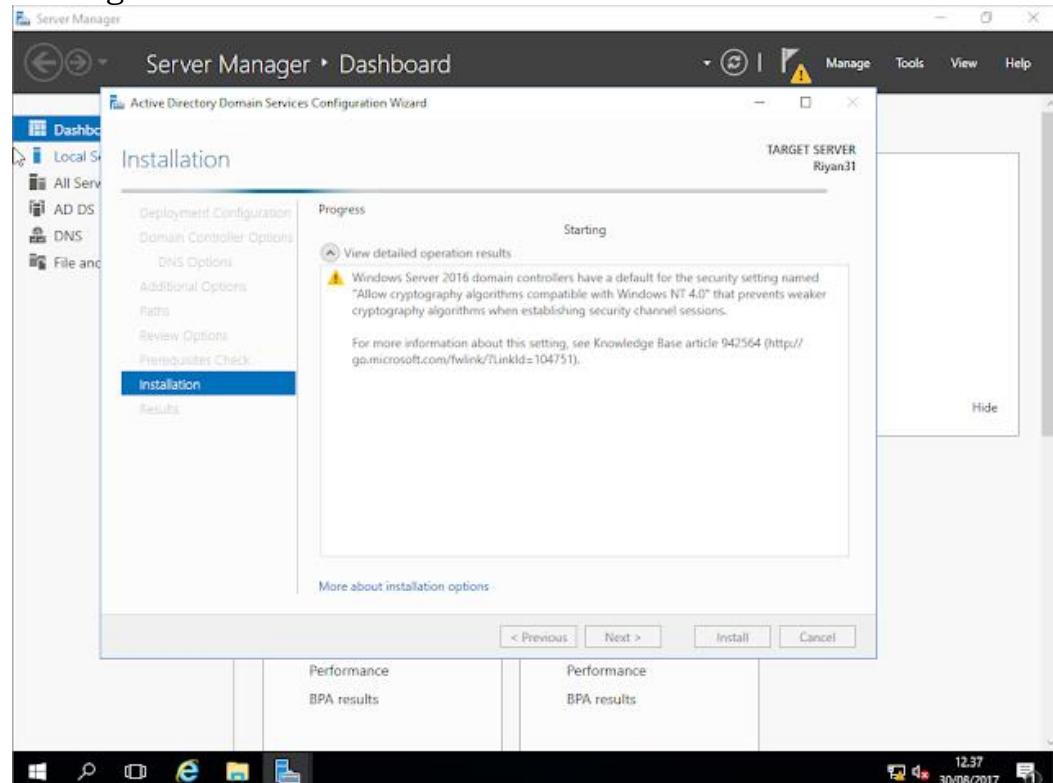
- Di bagian **Prerequisites Check**, kita langsung Install saja

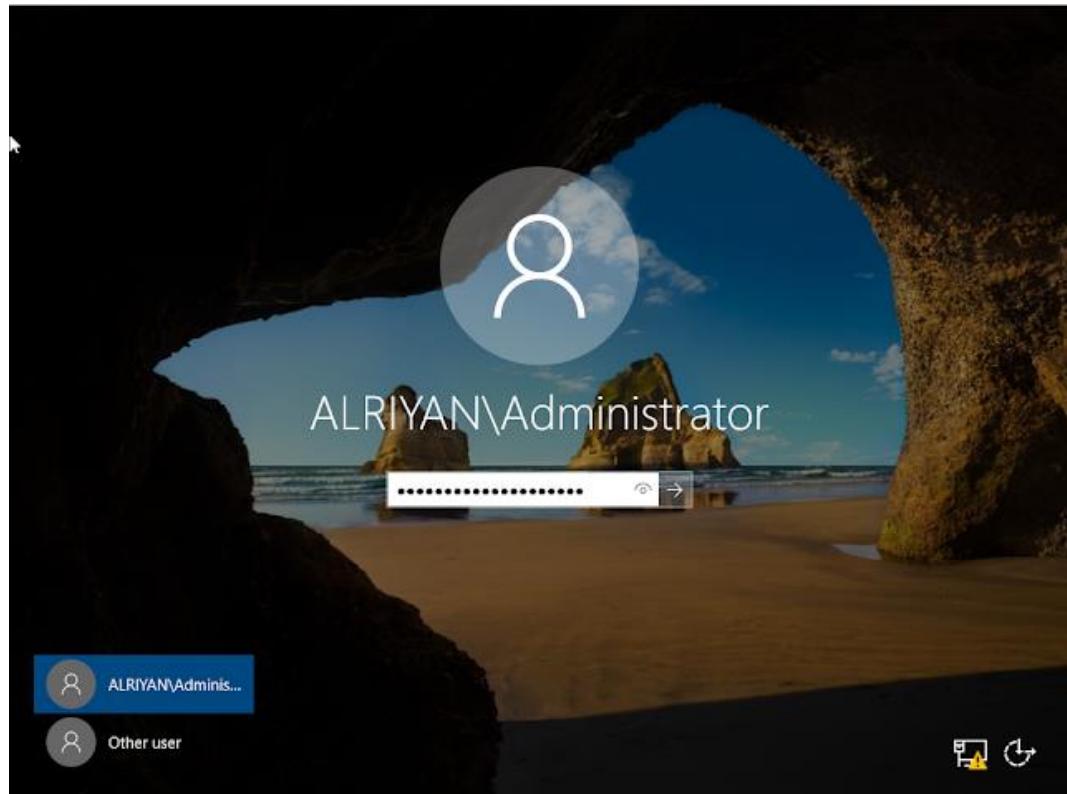


Gambar 8.47 Prerequisites Check



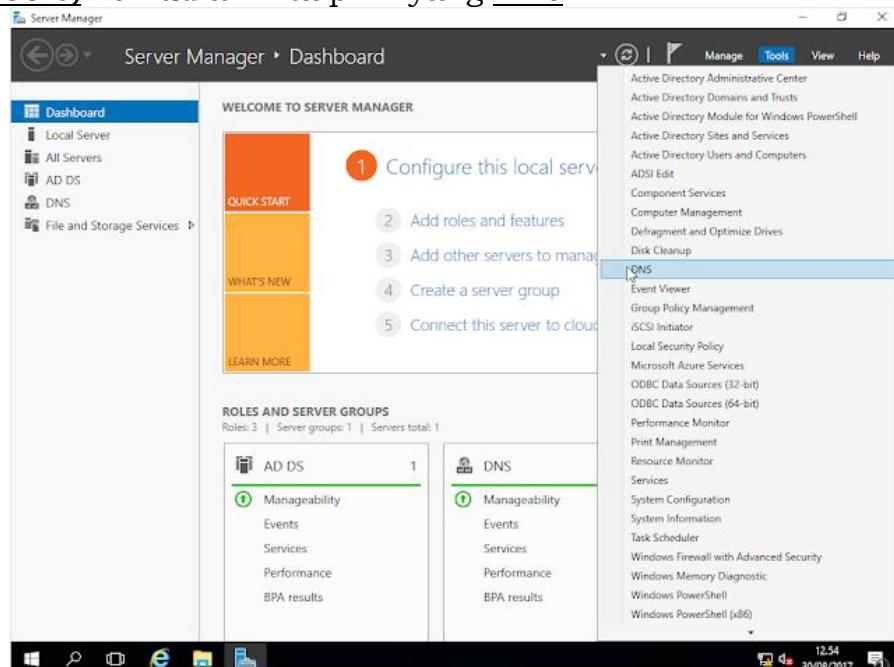
- Di bagian **Installation** ini kita tunggu sampai prosesnya selesai, setelah itu akan anda akan merestart ulang OS anda, setelah itu kita login kembali





Gambar 8.48 Installation / Finish

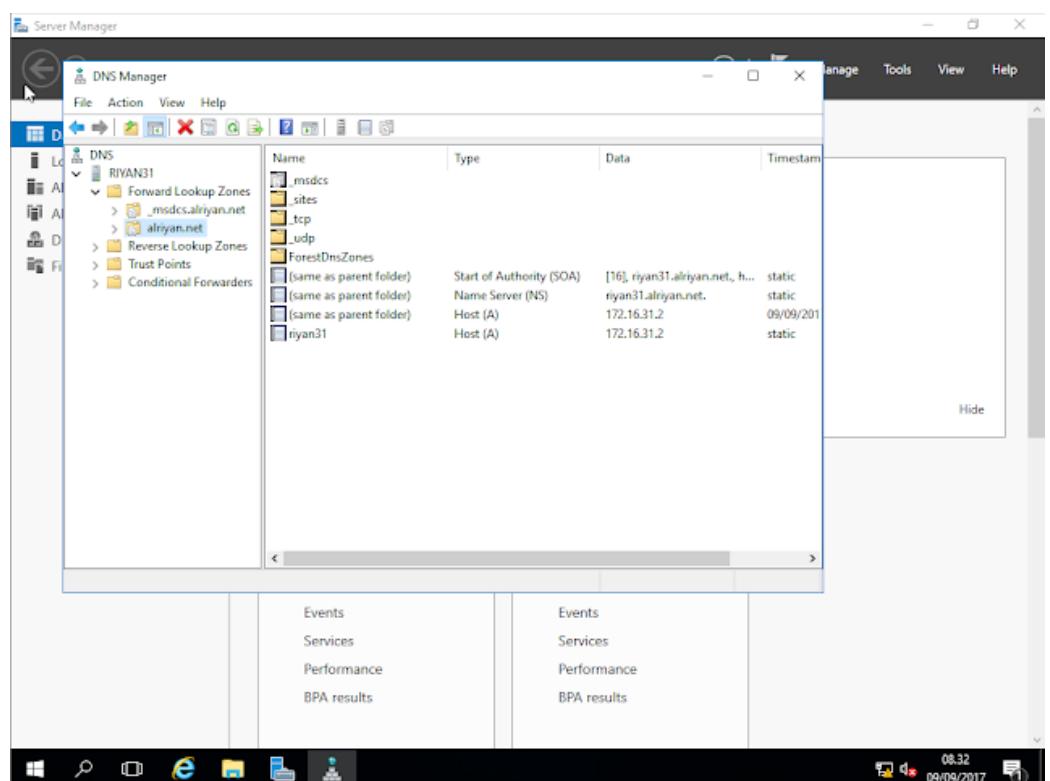
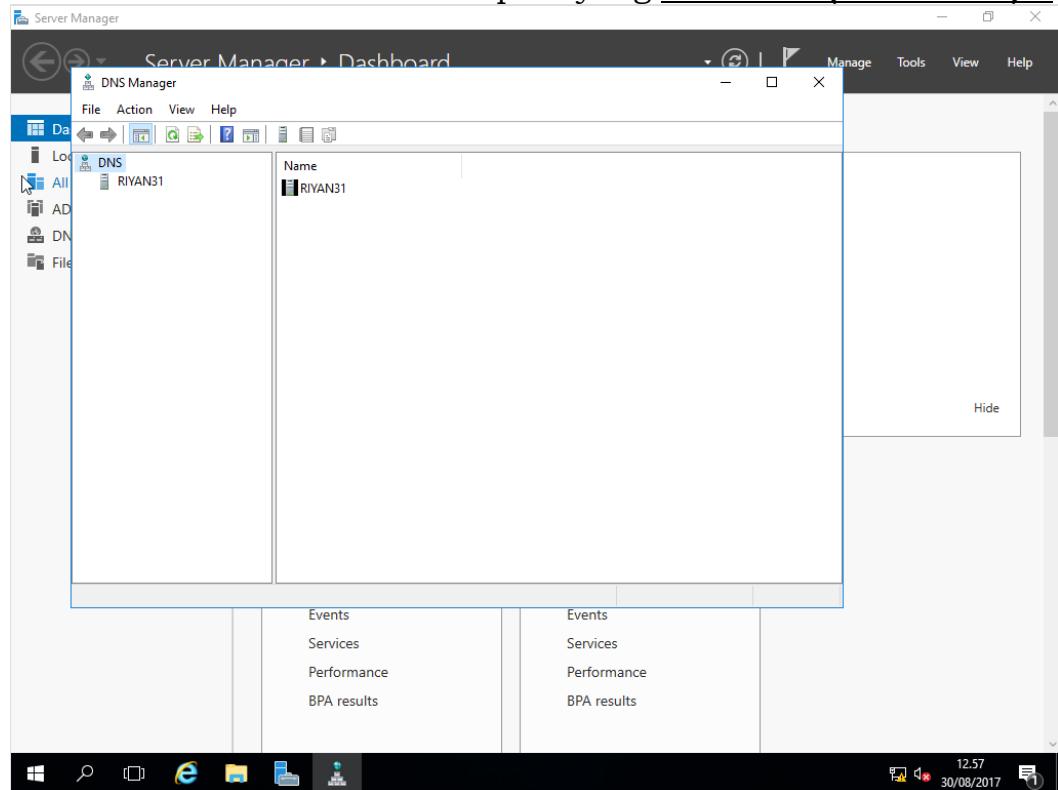
- Sekarang kita akan mengkonfigurasi agar client kita bisa menggunakan domain server yang kita buat tadi
- Pertama saya menggunakan Windows 10 terlebih dahulu untuk clientnya
- Ok kita kembali lagi ke **Server Manager**, lalu kita klik di bagian **Tools**, kemudian kita pilih yang **DNS**

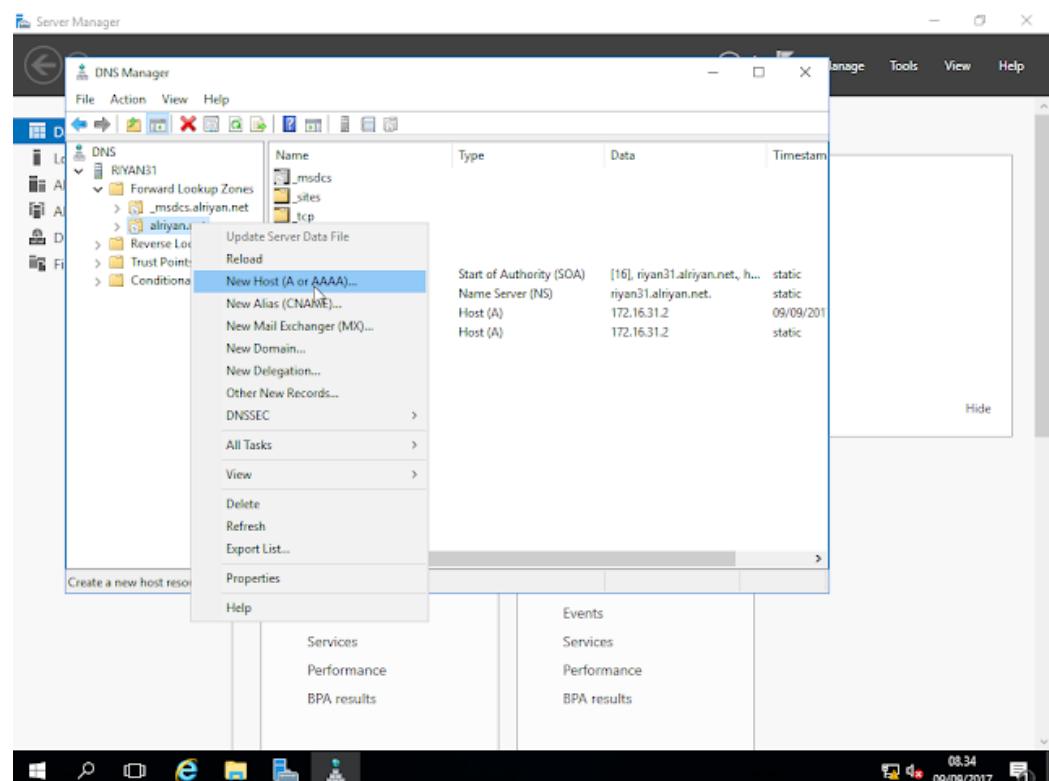


Gambar 8.49 server manager



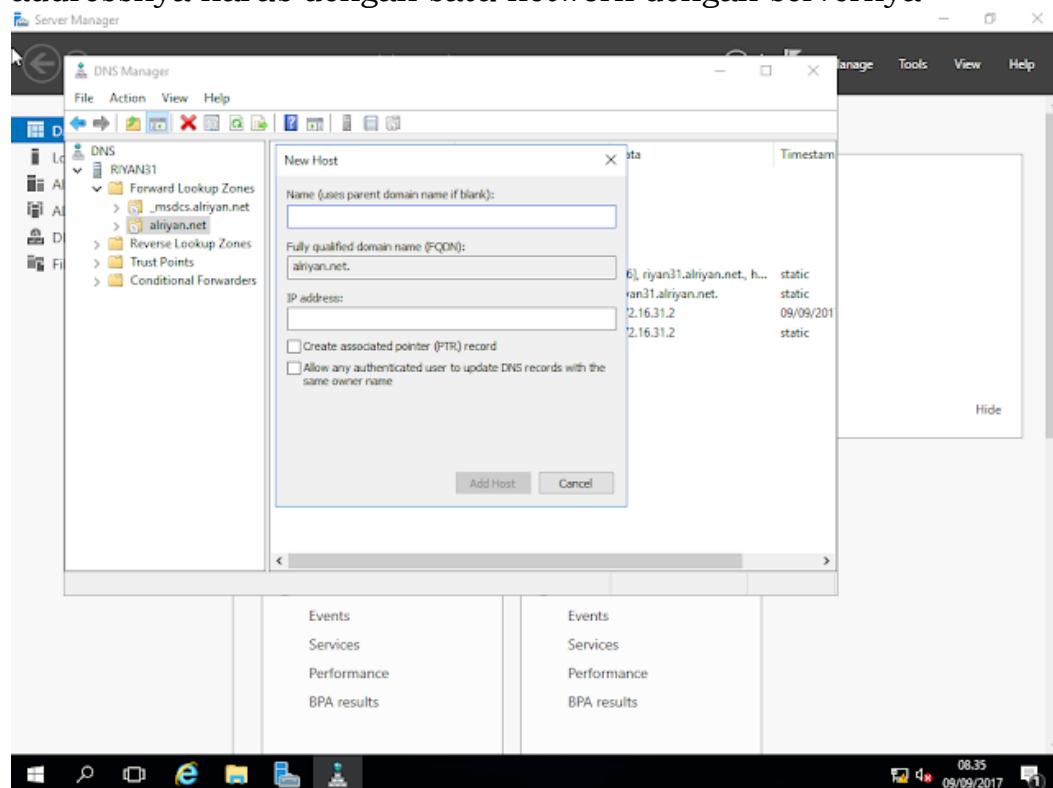
- Setelah itu kita bisa lihat seperti gamabar dibawah ini, lalu kita klik host pc kita, kemudian kita klik **Forward Loockup Zones**, kemudian kita klik domain yang kita buat tadi (alriyan.net), kemudian kita klik kanan lalu pilih yang **New Host (A or AAAA)...**

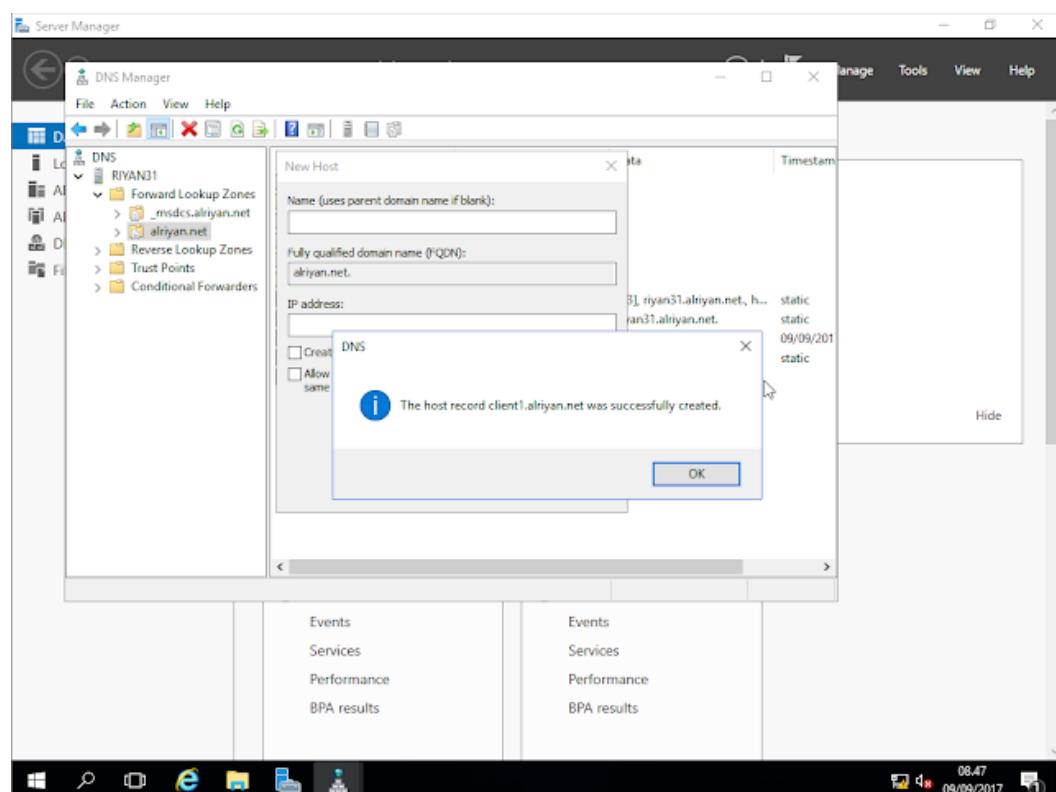
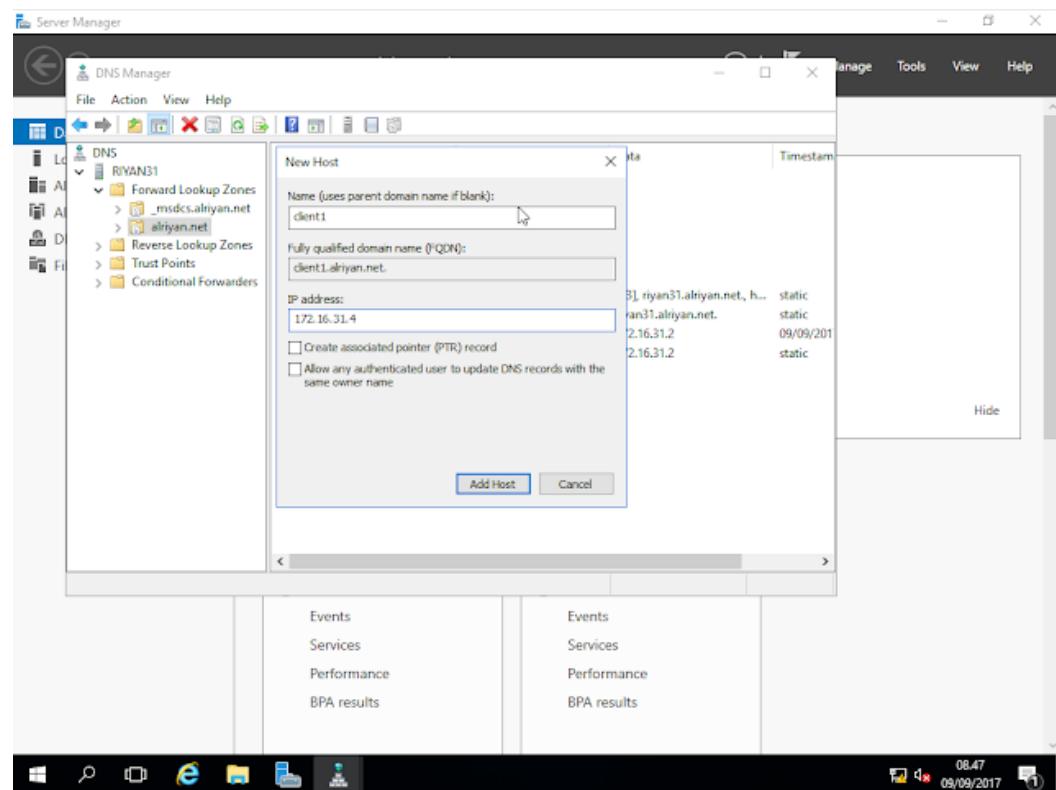




Gambar 8.50 Forward Loockup Zones

- Kemudian disini kita diminta untuk memasukkan nama clientnya dan ip addressnya, kita isinya dengan nama bebas dan ip addressnya harus dengan satu network dengan servernya





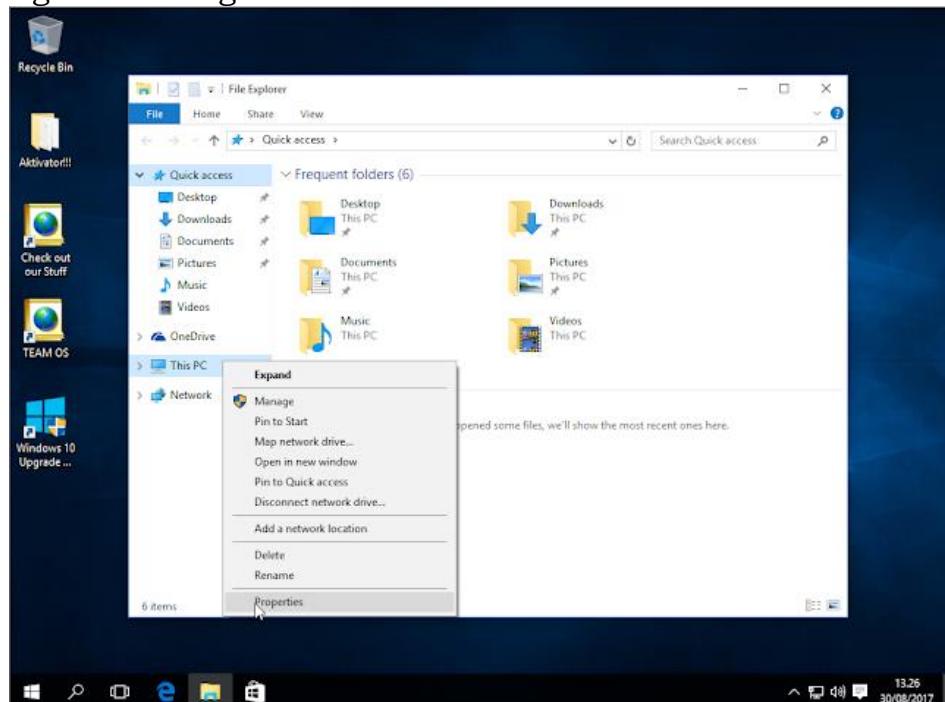
Gambar 8.51 memasukkan nama client

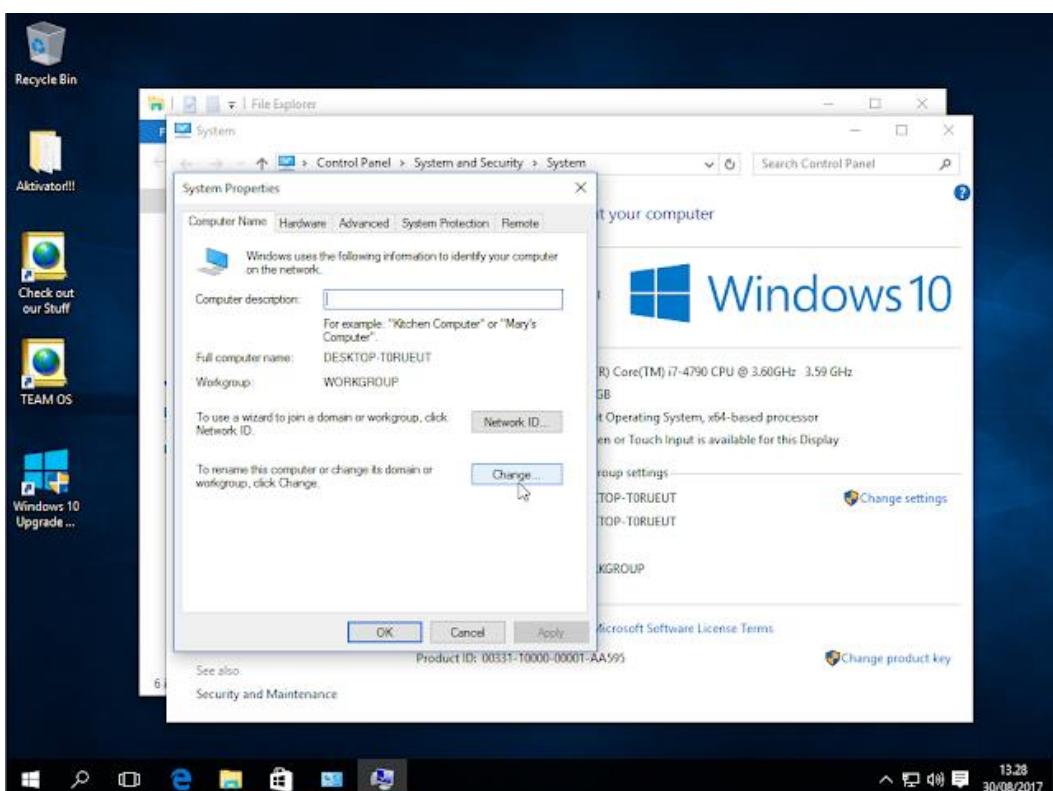
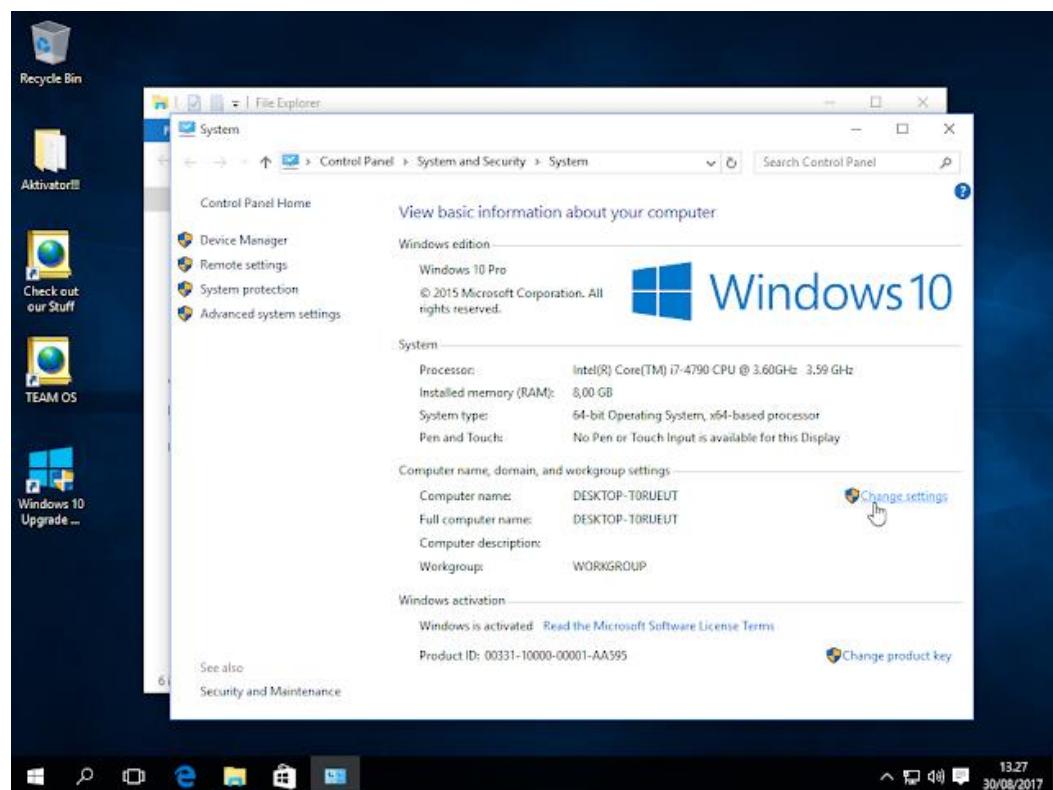
- Ok sekarang kita ke Client windowsnya

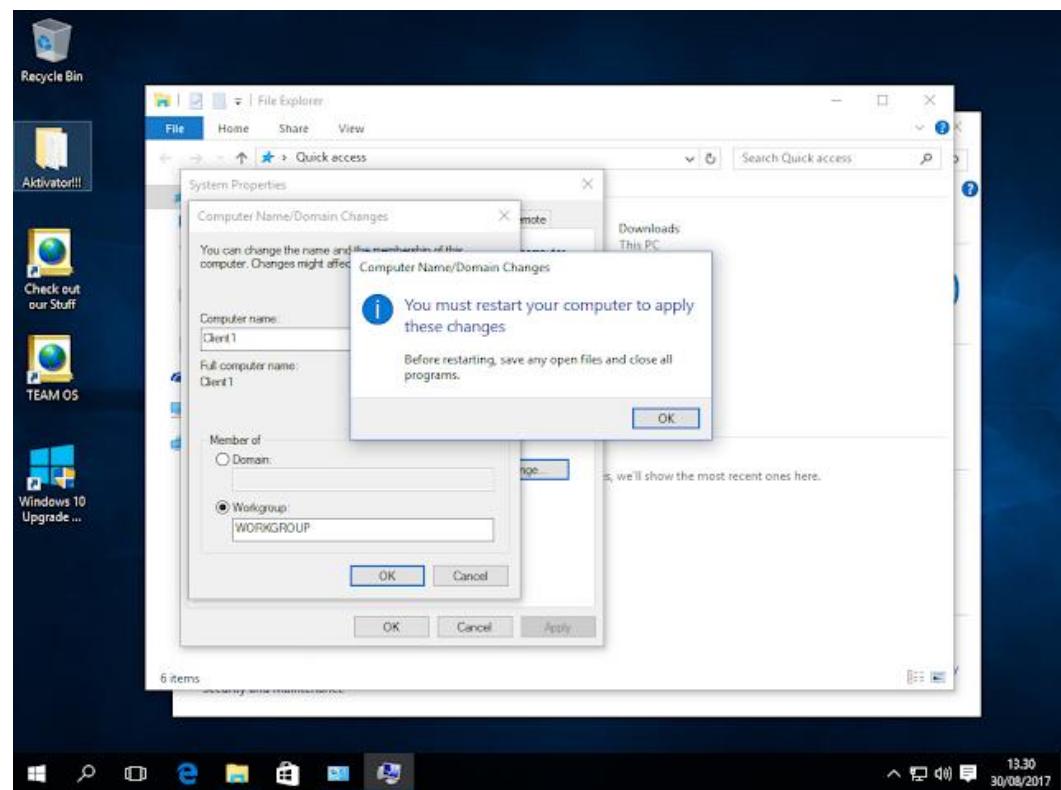
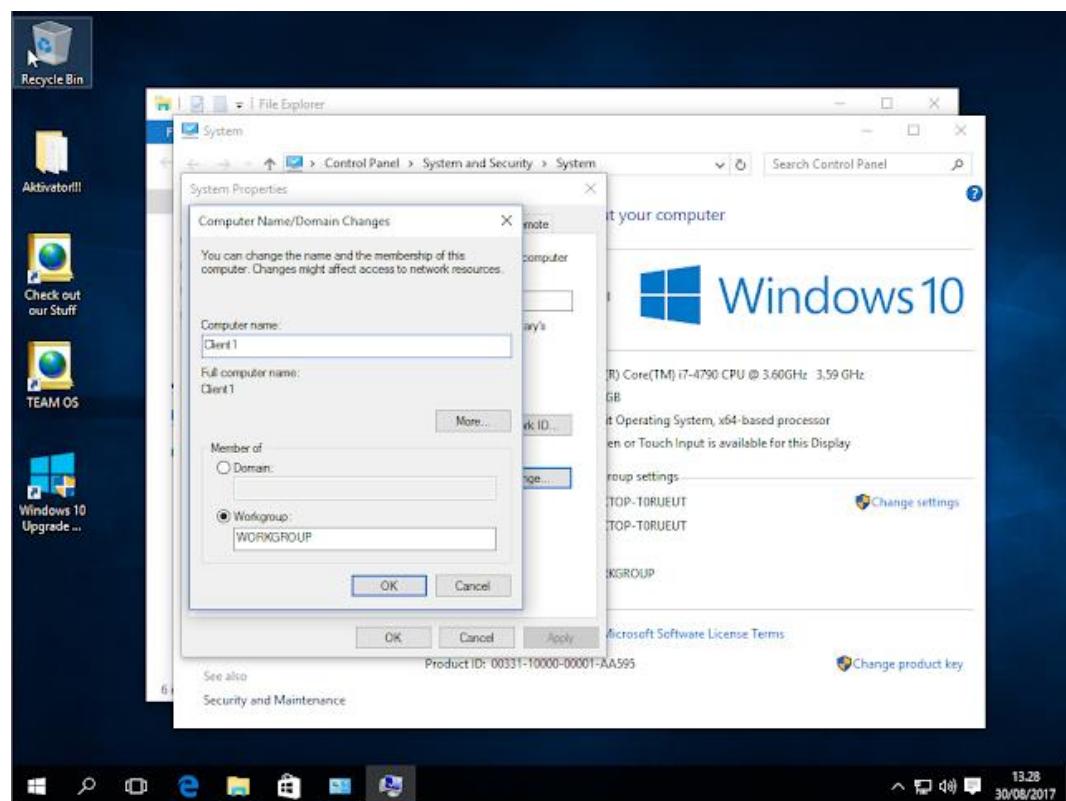


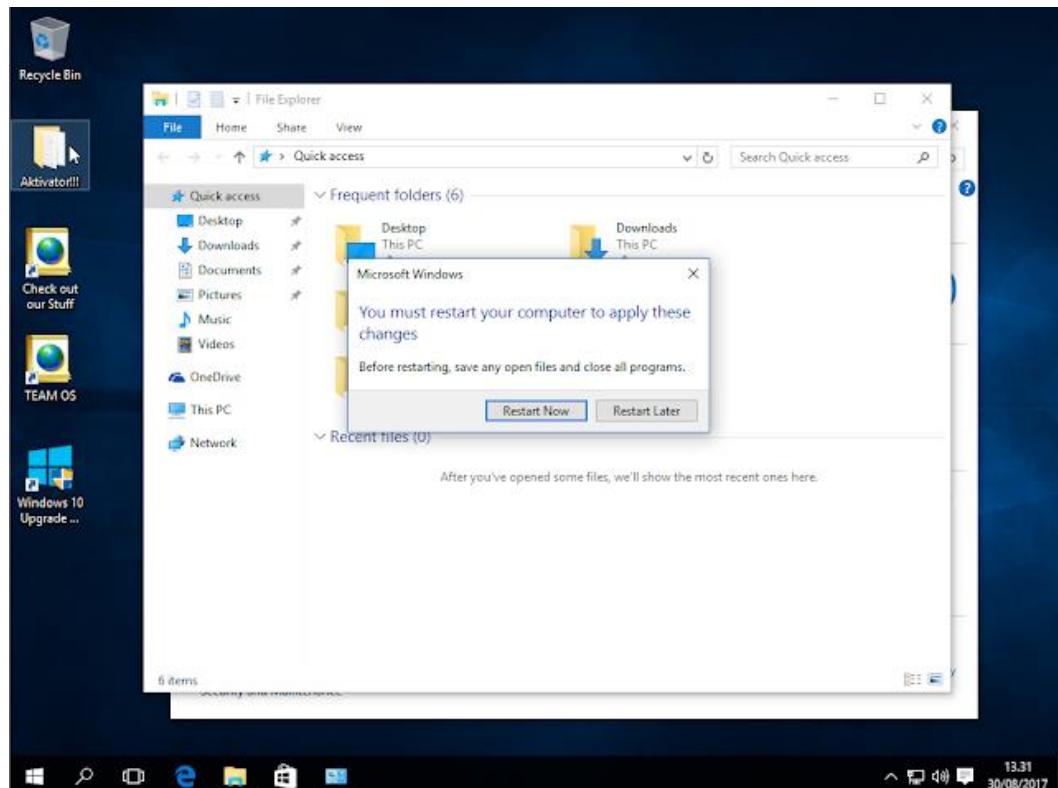
Gambar 8.52 client windows

- Setelah itu kita ke **Properties**, kemudian kita **Change settings**, kemudian pilih **Changes...**, setelah itu kita ganti **Computer name** dengan nama yang kita tambahkan di server tadi, lalu klik Ok, setelah itu anda akan disarankan untuk merestart OS anda agar host yang kita setting tadi berubah



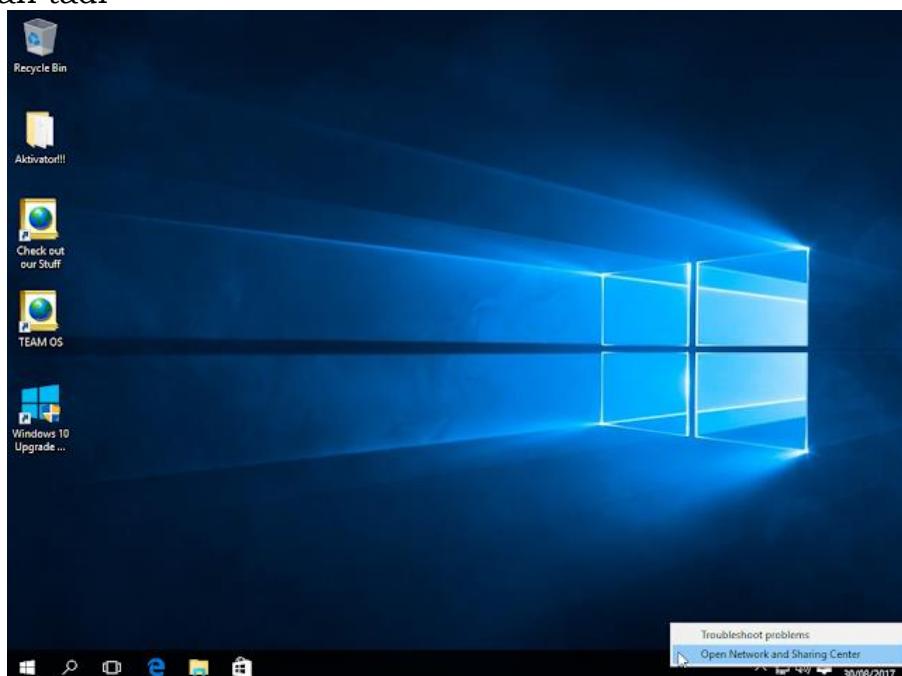


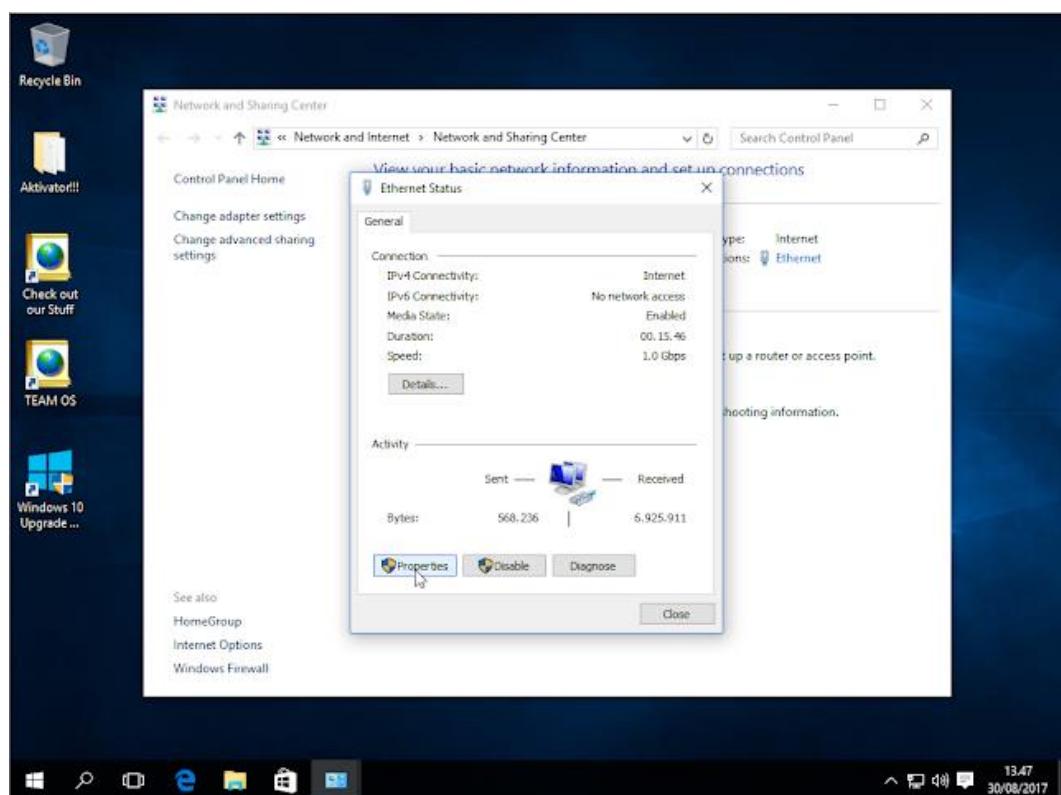
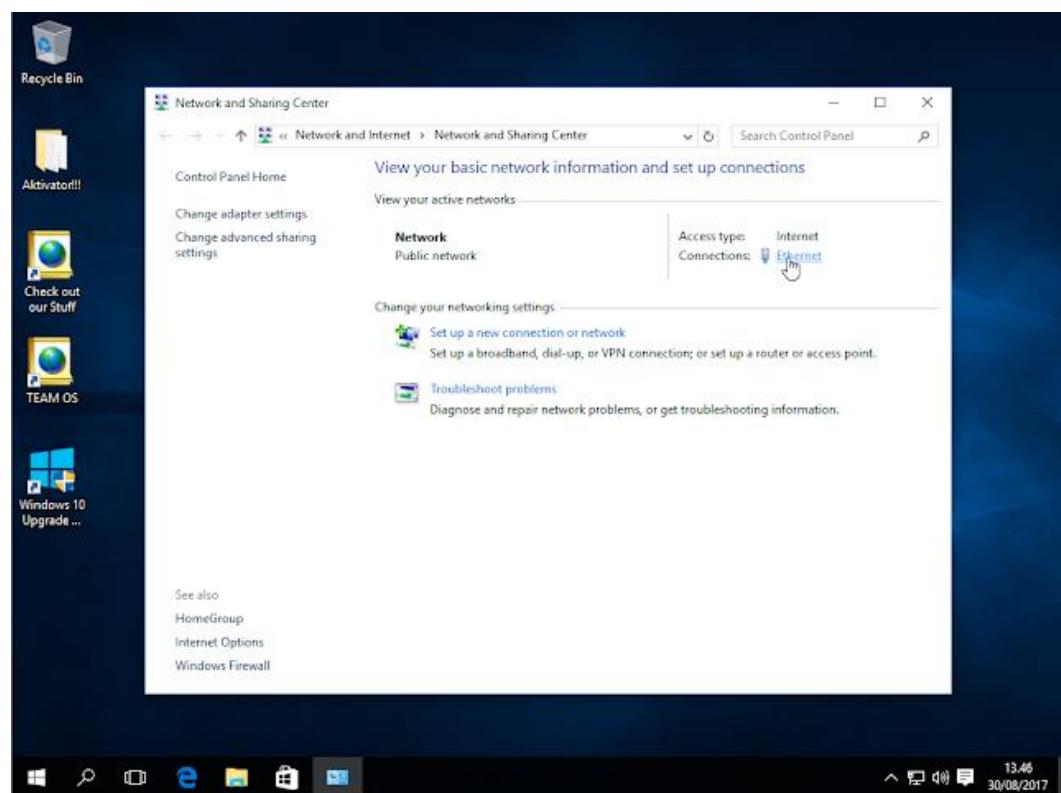


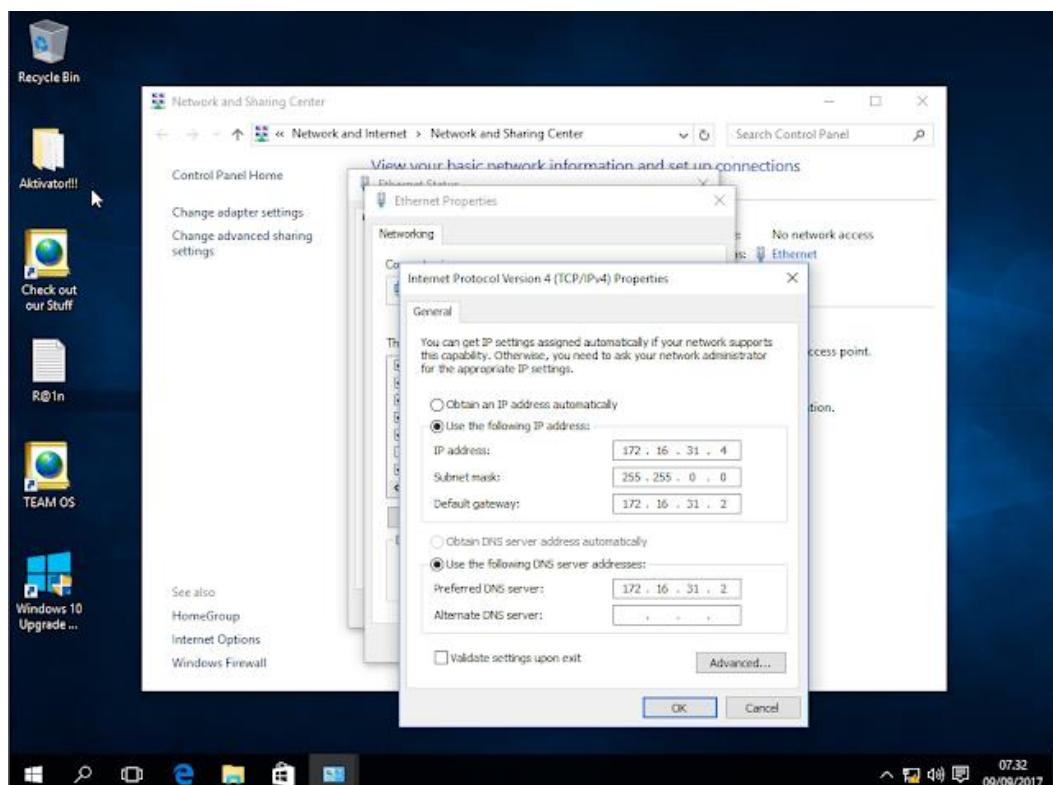
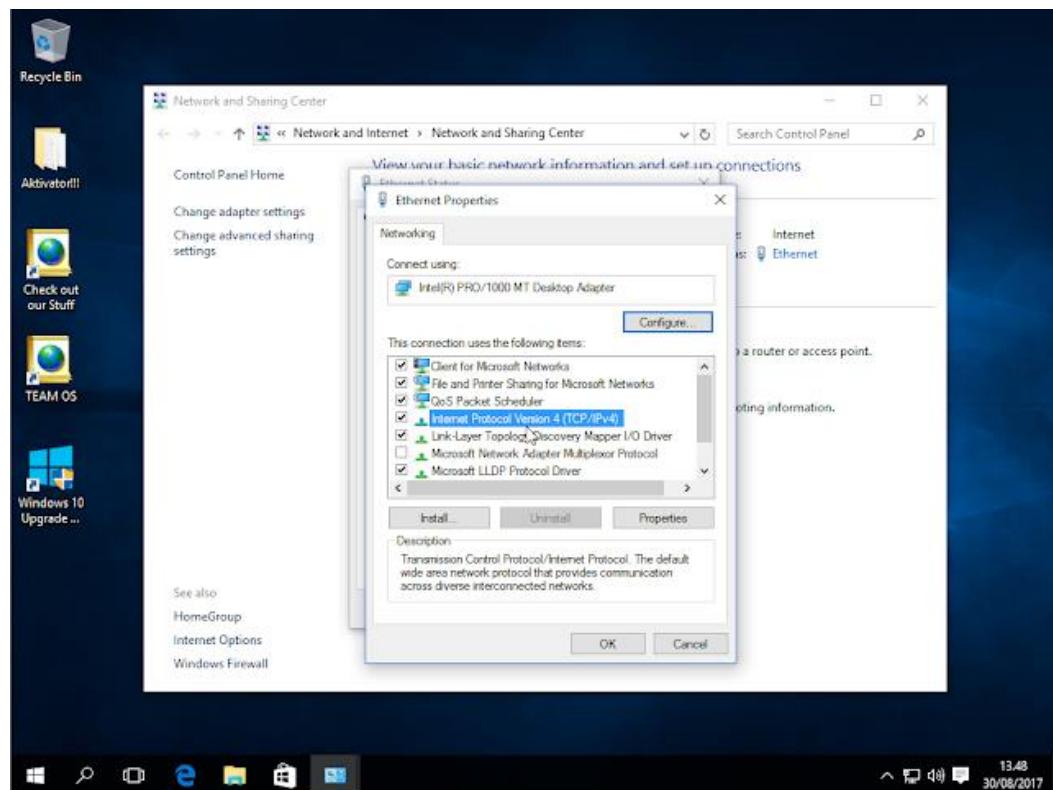


Gambar 8.53 change settings

- Setelah itu kita setting ip addressnya, kita ganti sama dengan yang kita tambahkan di server tadi, pertama kita klik kanan pada icon yang bergambar pc yaaitu icon network, lalu pilih yang **Open Network and Sharing Center**, kemudian klik tulisan **ethernet**, lalu klik **properties**, setelah itu kita pilih yang **Internet Protocol Version 4 (TCP/IPv4)**, lalu isilah ip addressnya sesuai yang kita tambahkan tadi





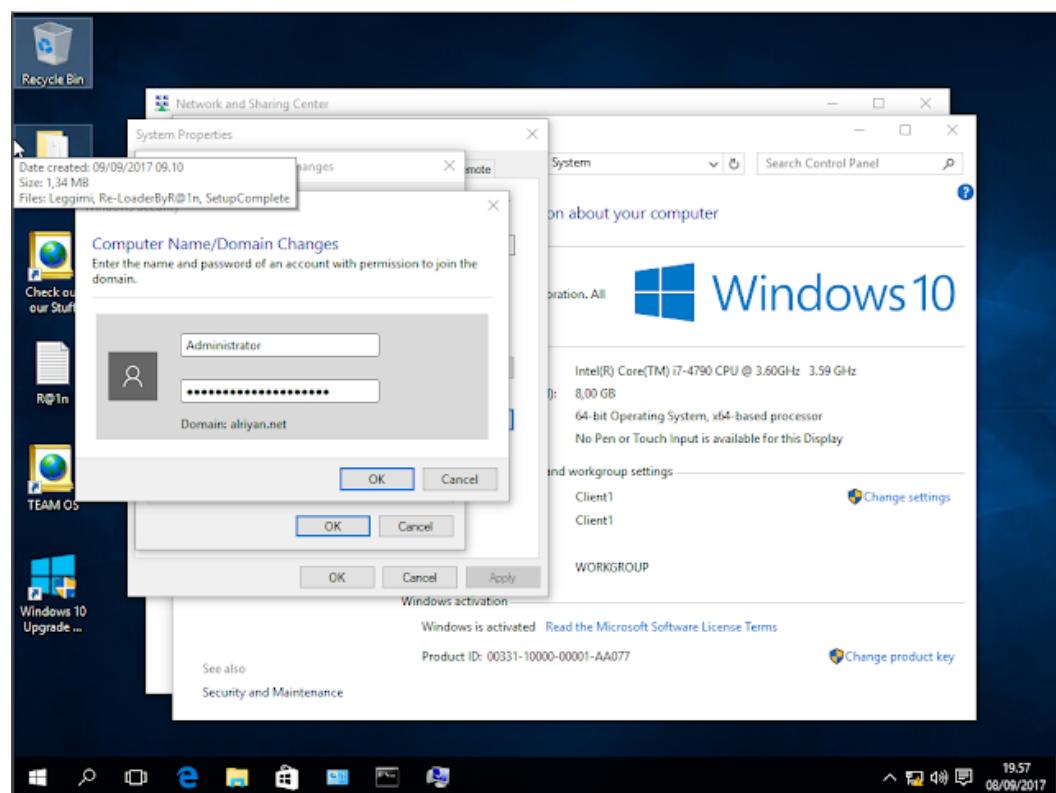
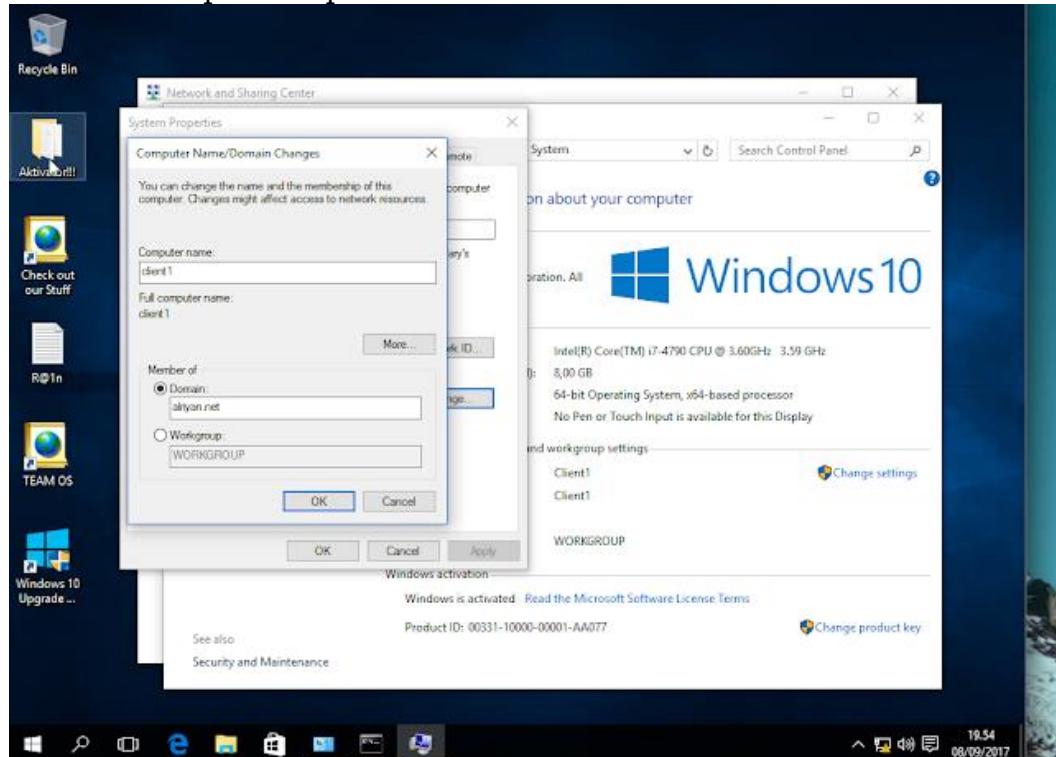


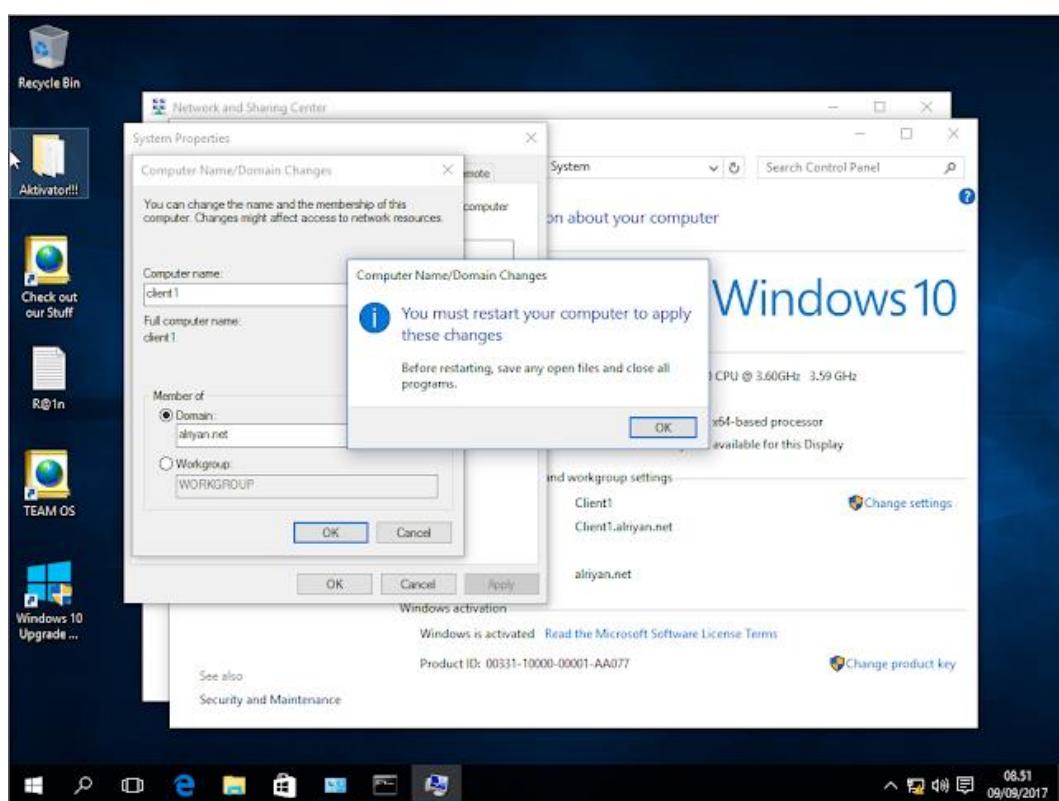
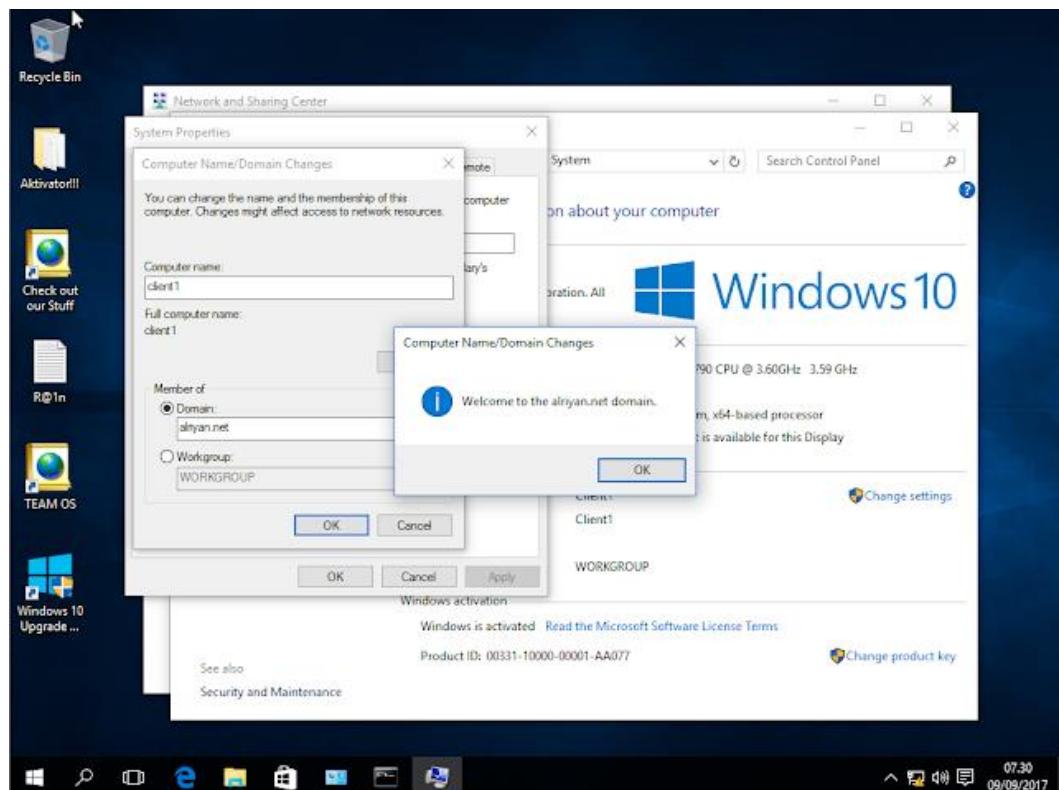
Gambar 8.54 Open Network and Sharing Center

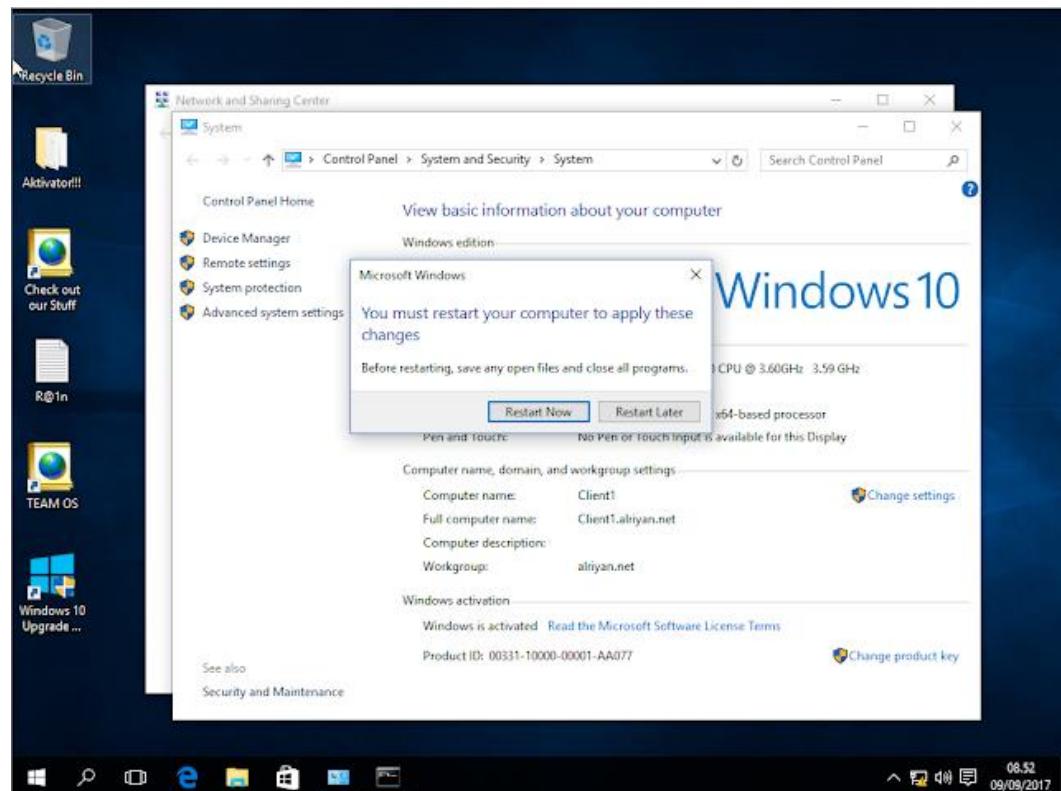
- Setelah itu kita akan join domain yang kita buat tadi, caranya sama seperti tadi kita ke **Properties**, kemudian kita **Change settings**, kemudian pilih **Changes...**, setelah itu kita rubah dari



Workgroup ke **Domain**, lalu kita isi dengan domain yang kita buat tadi (alriyan.net) kemudian ok, kemudian anda masukkan **Username** dan **Password** sesuai dengan server, setelah itu akan ada perintah restart, nahh kita restart aja langsung, lalu akan muncul tampilan seperti dibawah

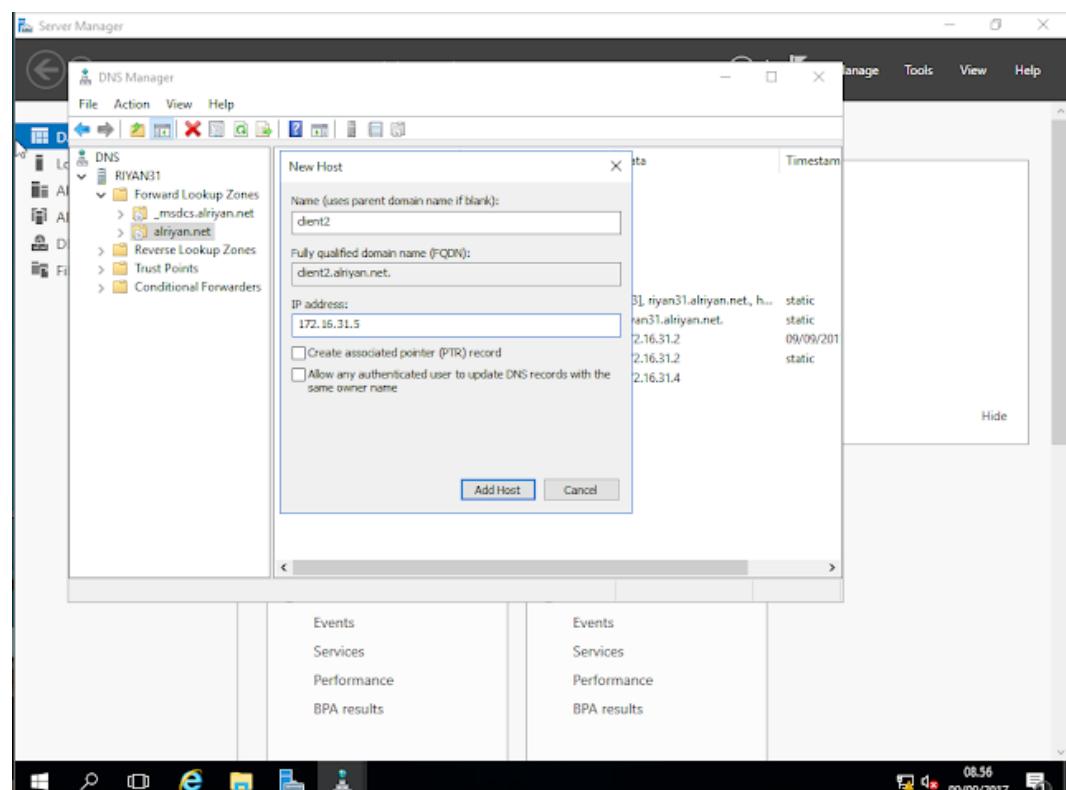
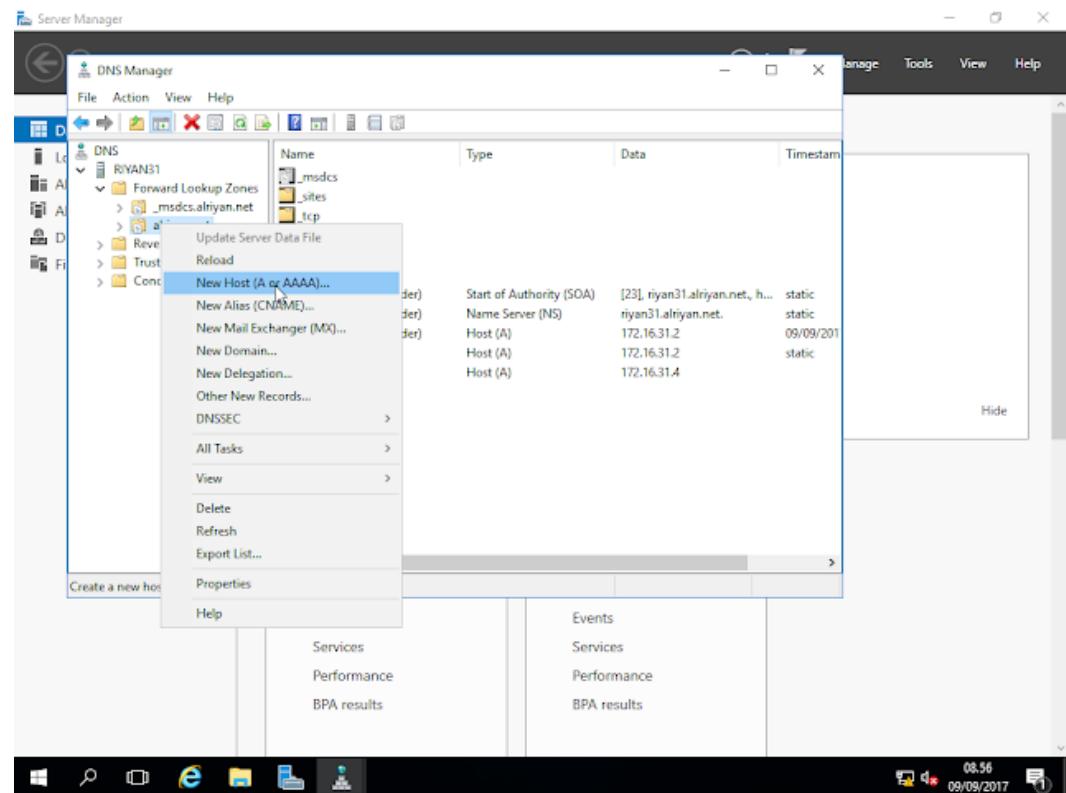






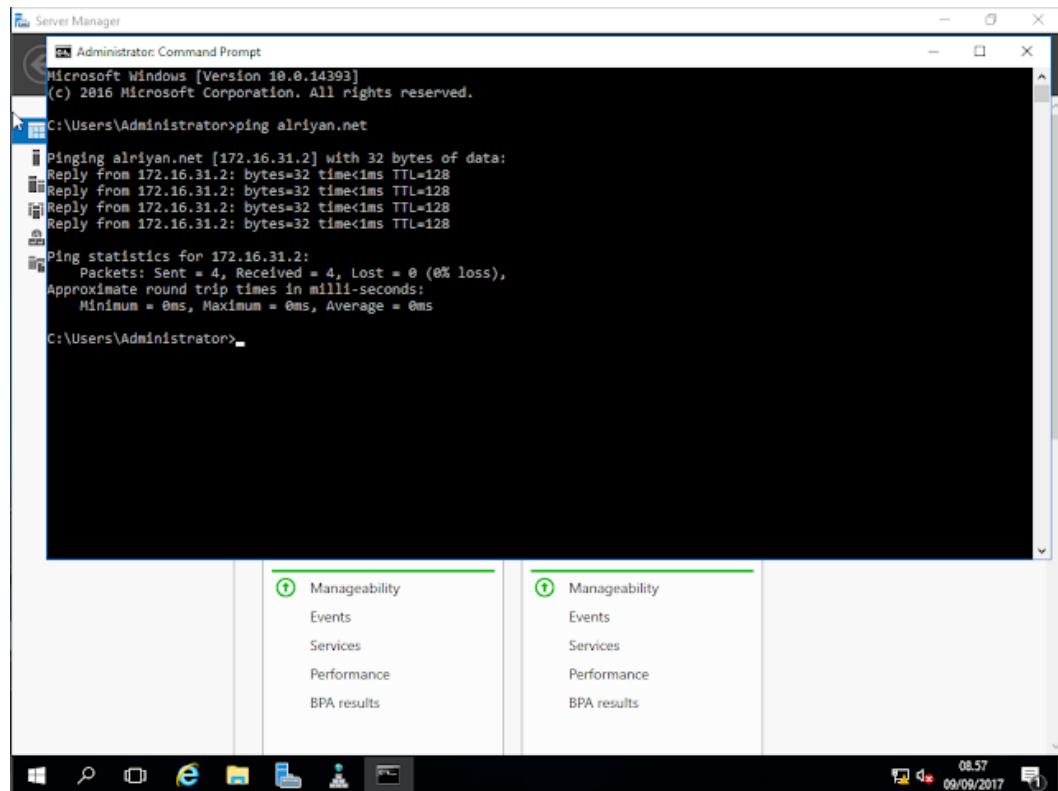
Gambar 8.55 computer domain change

- Ok sekarang client linuxnya, kita buat new host lagi pada severnya untuk client linuxnya



Gambar 8.56 client linux

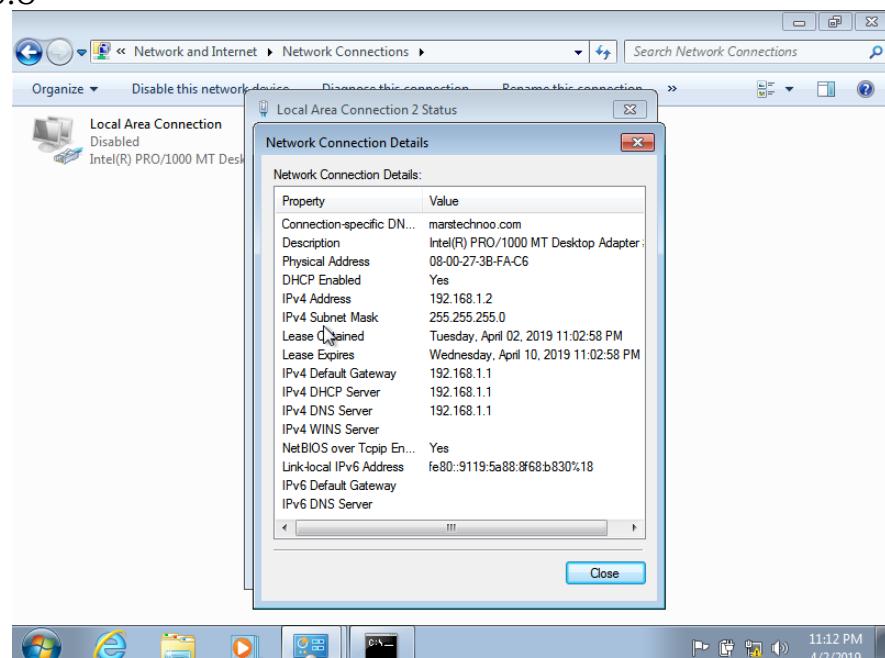
- Dan ini saya ping ke domainnya dan reply



Gambar 8.57 ping ke client

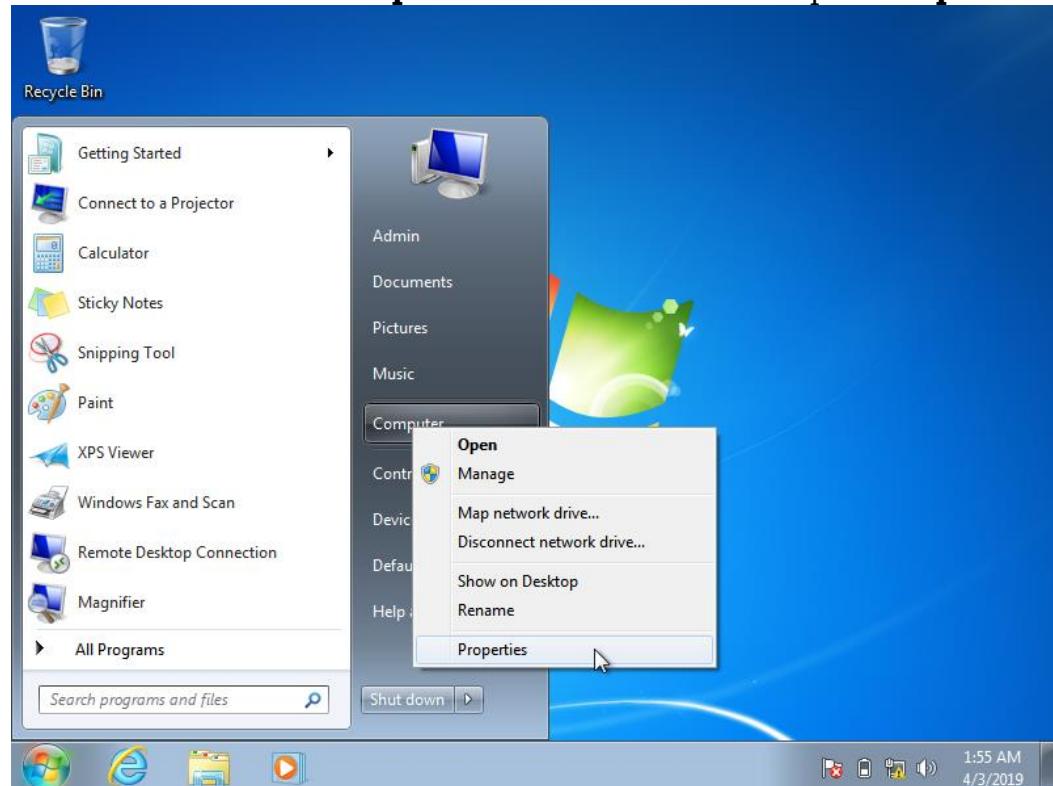
8.3.8.1. Konfigurasi pada client Windows

- Setting IP Address **TCP/IPv4** menjadi DHCP karena sebelumnya saya sudah buat [DHCP Server](#) silahkan dibaca juga. Jika belum dibuat static sesuai dengan range IP Server. Jangan lupa juga DNS Server itu IP Address Server nya jangan memakai DNS 8.8.8.8



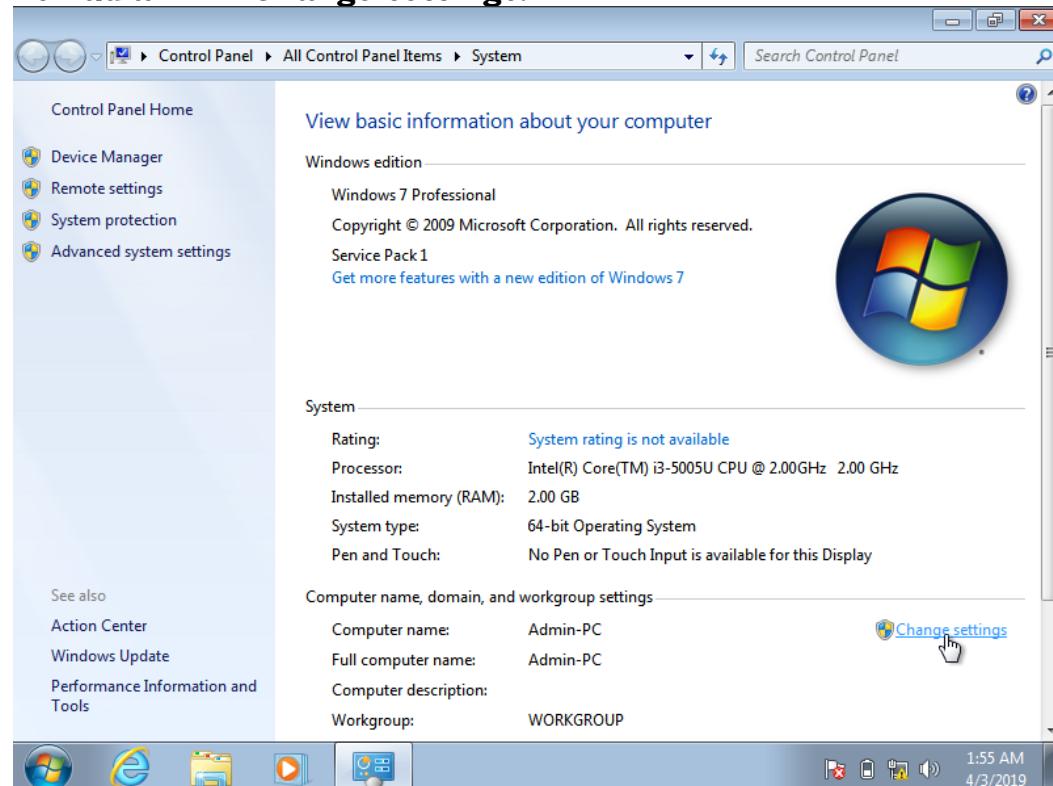
Gambar 8.58 Setting IP Address **TCP/IPv4**

2. Pilih menu **Start > Computer** lalu klik kanan dan pilih**Properties**.



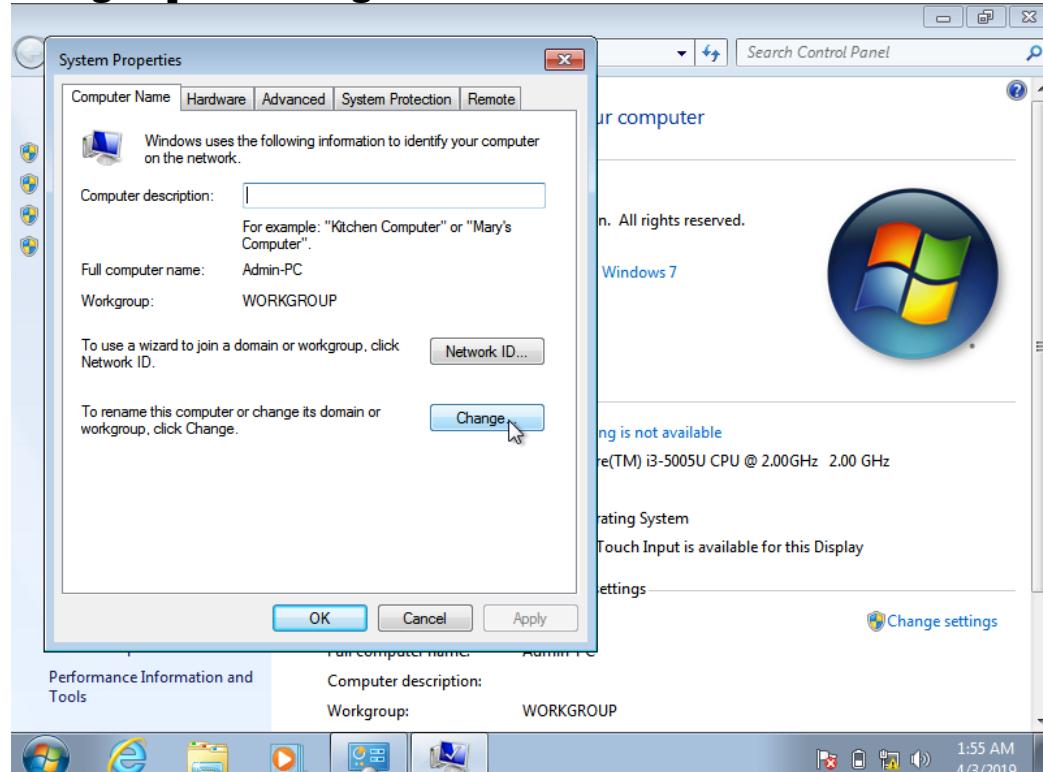
Gambar 8.59 properties

3. Kemudian klik **Change settings**.



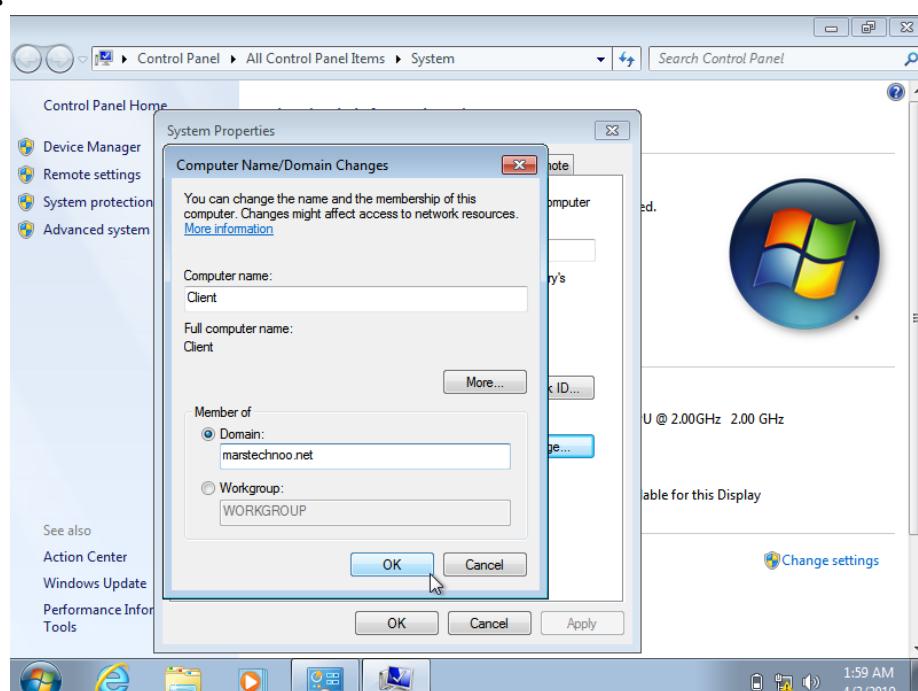
Gambar 8.60 change settings

4. Setelah itu **To rename this computer or change its domain or workgroup** klik **Change**.



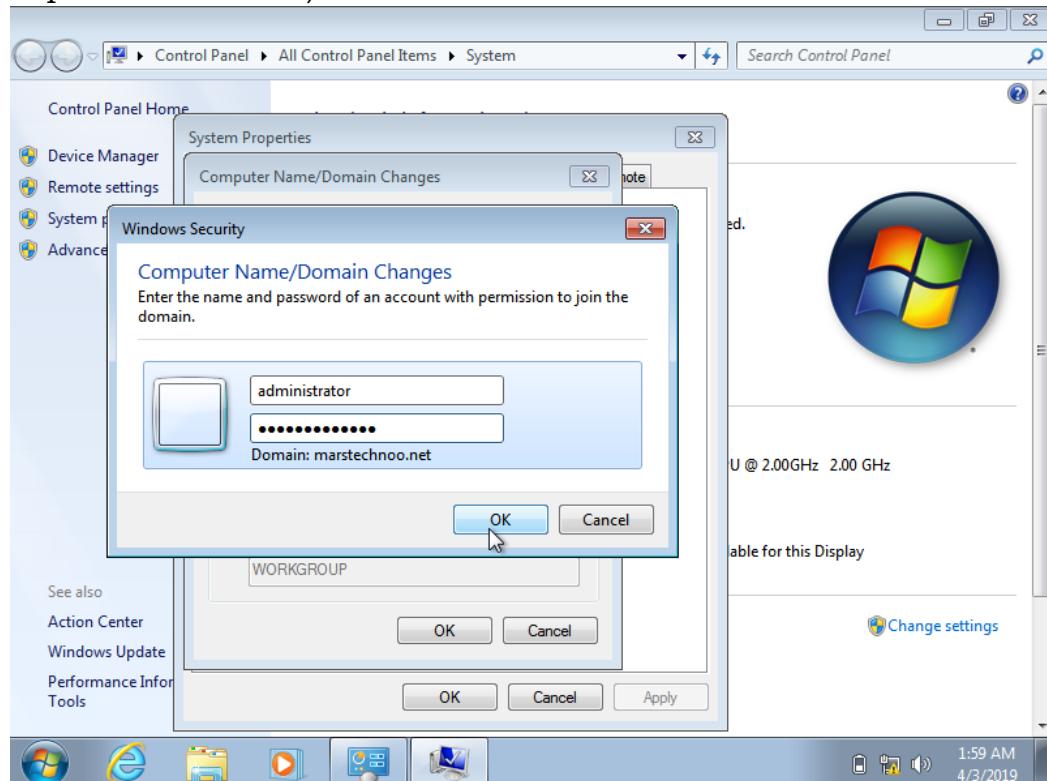
Gambar 8.61 rename this computer

5. Pada jendelan **Computer Name/Domain Changes**, masukkan : Computer name : (sesuai host yang dibuat oleh server) Domain : (sesuai domain yang dibuat oleh server). Kemudian klik **OK**.



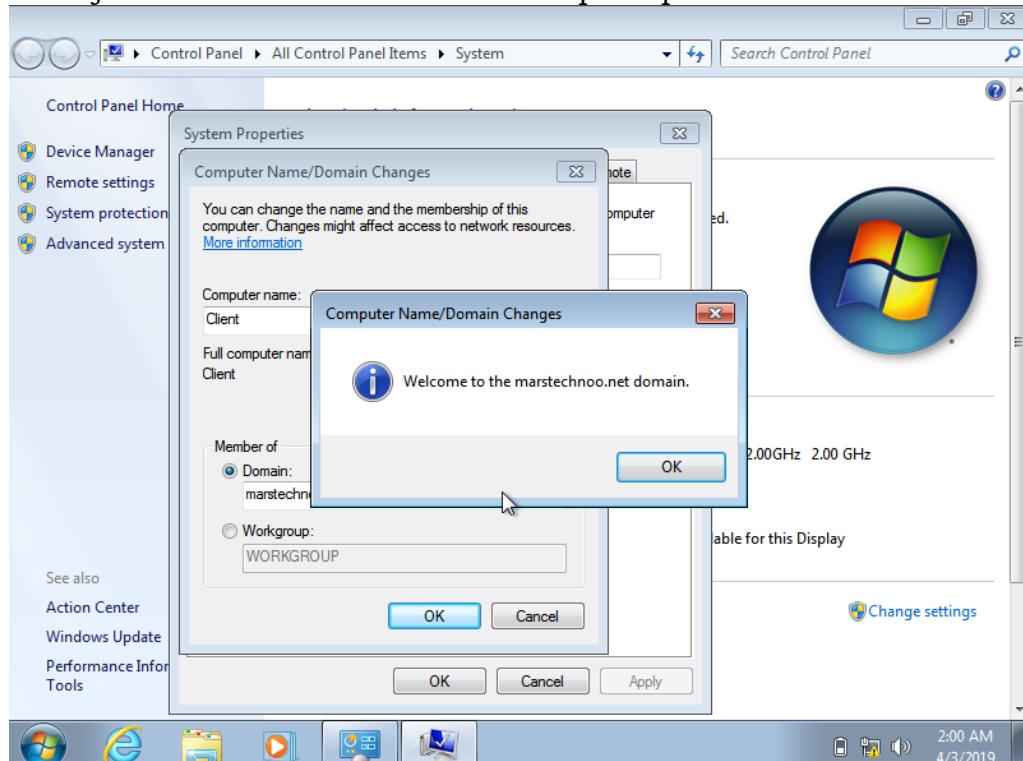
Gambar 8.62 computer name

6. Jika berhasil akan muncul pop-up seperti ini, masukkan **Username** dan **Password** (sesuai username dan password kepemilikan server). Klik **OK**.



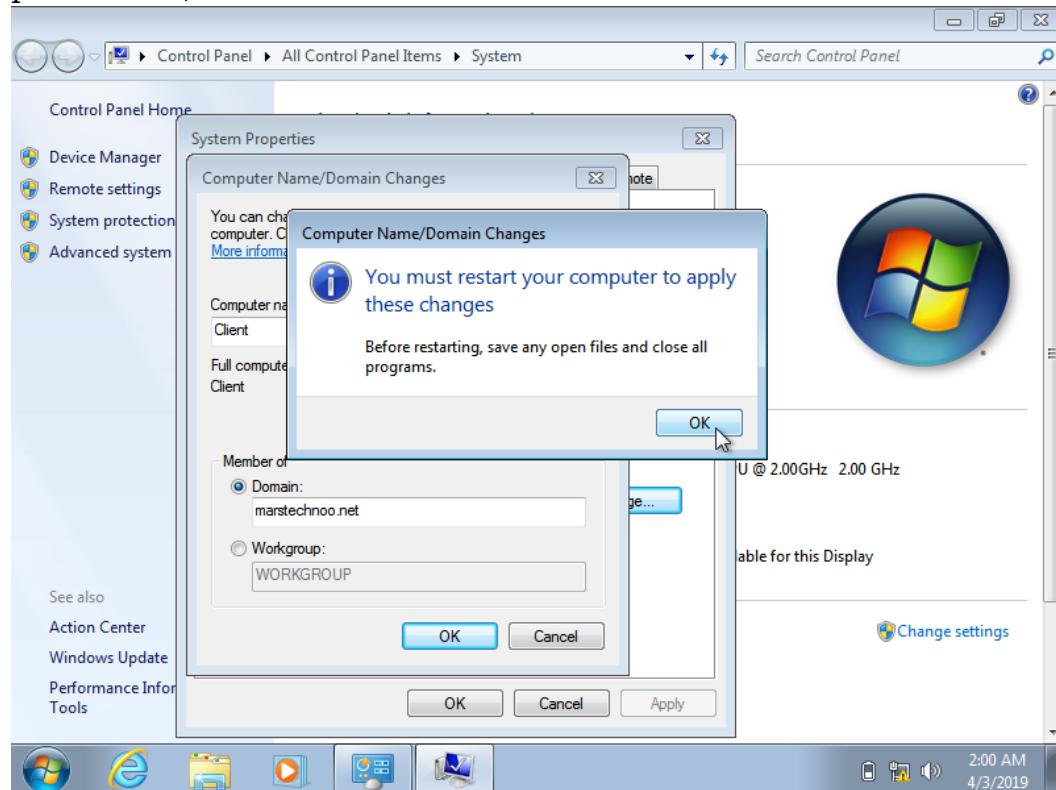
Gambar 8.63 Username dan Password

7. Dan jika berhasil akan muncul tampil seperti ini.



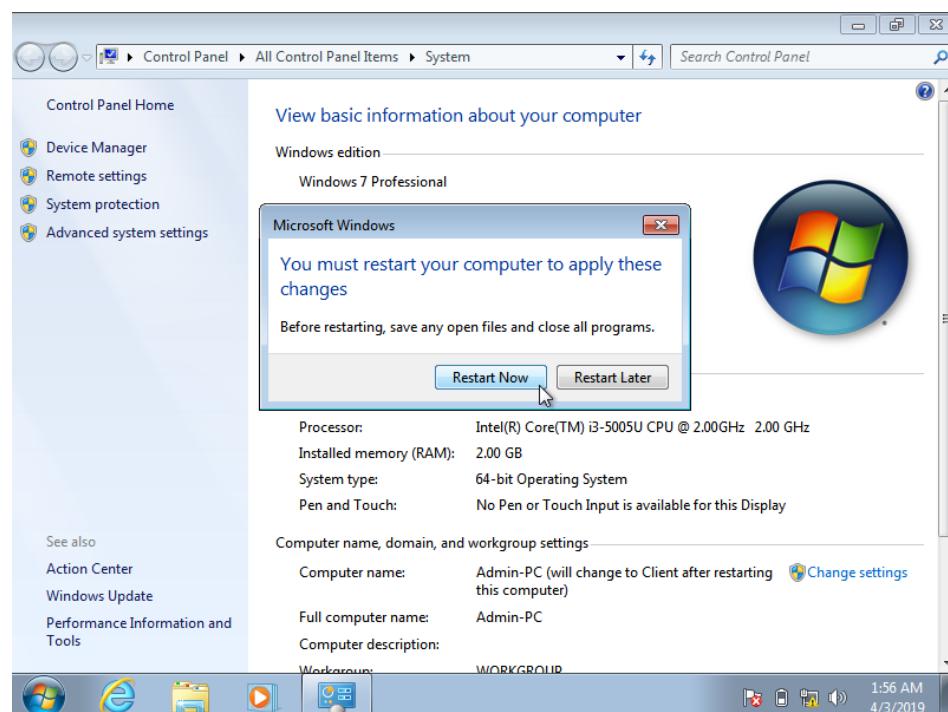
Gambar 8.64 welcome the name

- 8 Lalu kita diminta me-restart windows untuk menyimpan perubahan, klik **OK**.



gambar 8.65 restart computer

9. Kemudian **Restart Now.**



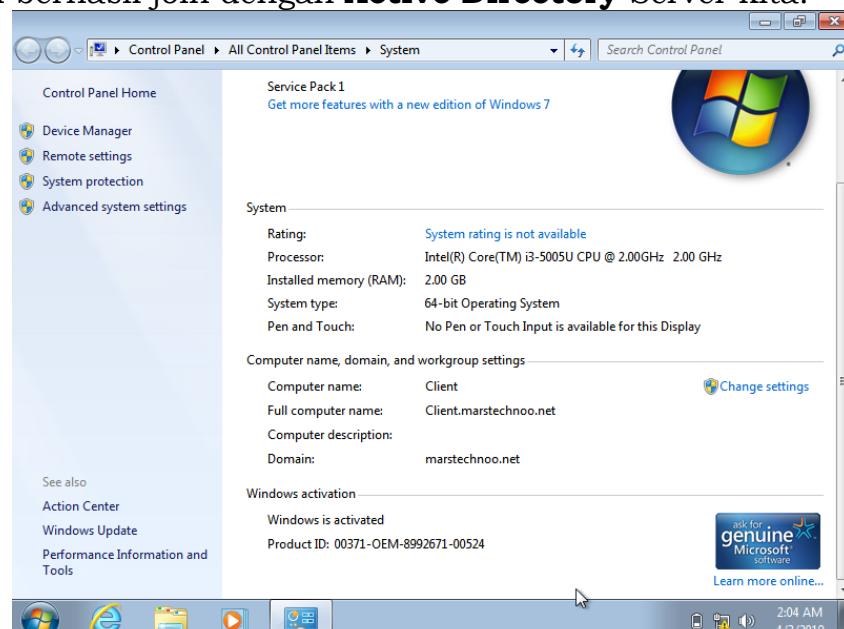
Gambar 8.66 restart

10. Setelah proses restart selesai, akan muncul tampilan log on seperti ini dan masukkan password kita sebelumnya. Dijelaskan **CLIENT** ini ada **Active Directory** nya Server.



Gambar 8.67 client admin

11. Untuk mengeceknya buka **Control Panel > All Control Panel Items > System**. Dapat dilihat **Full computer name** di sisi Client sudah berhasil join dengan **Active Directory** Server kita.

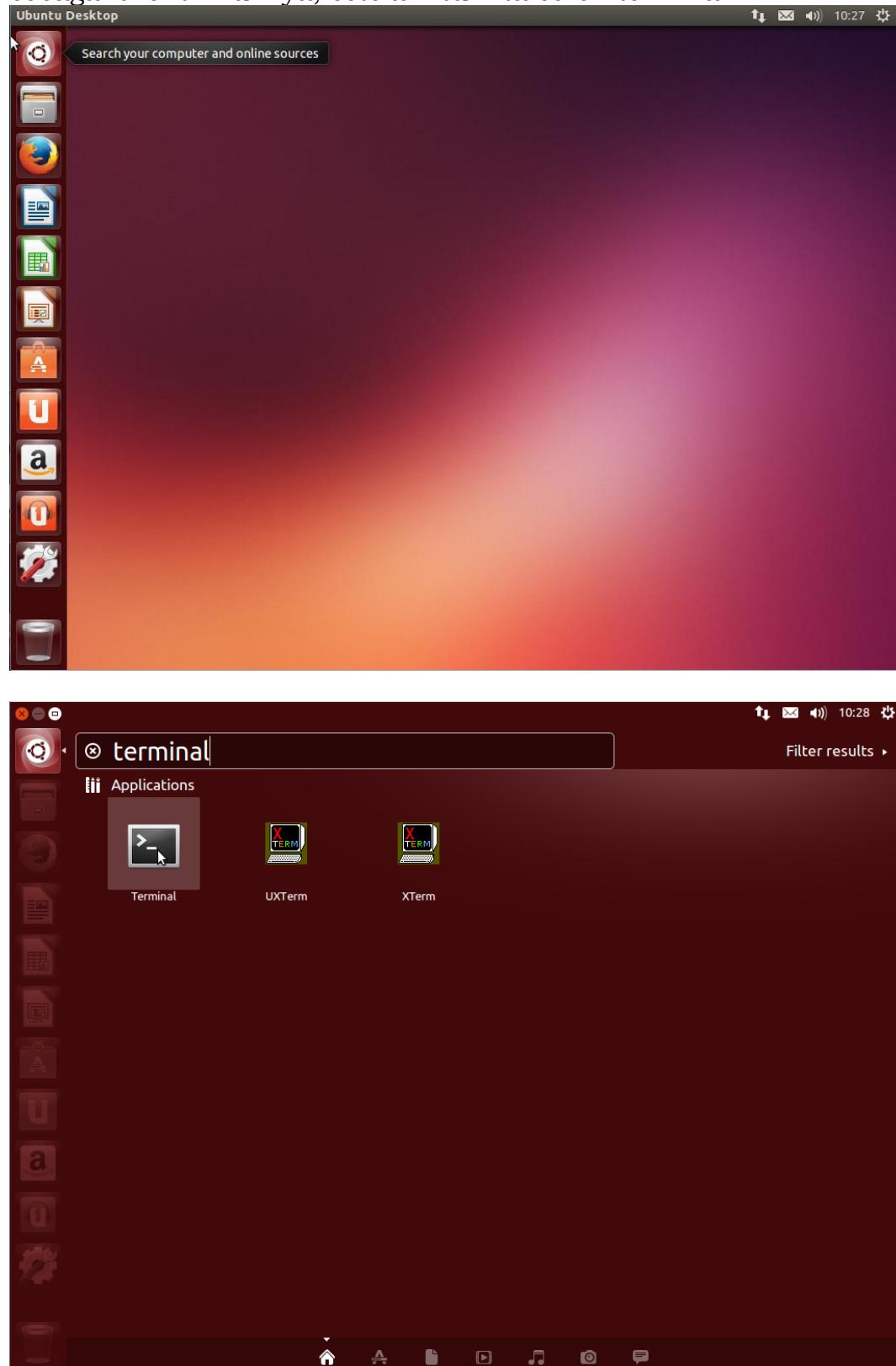


Gambar 8.68 control panel



8.3.8.2. Konfigurasi pada client Linux

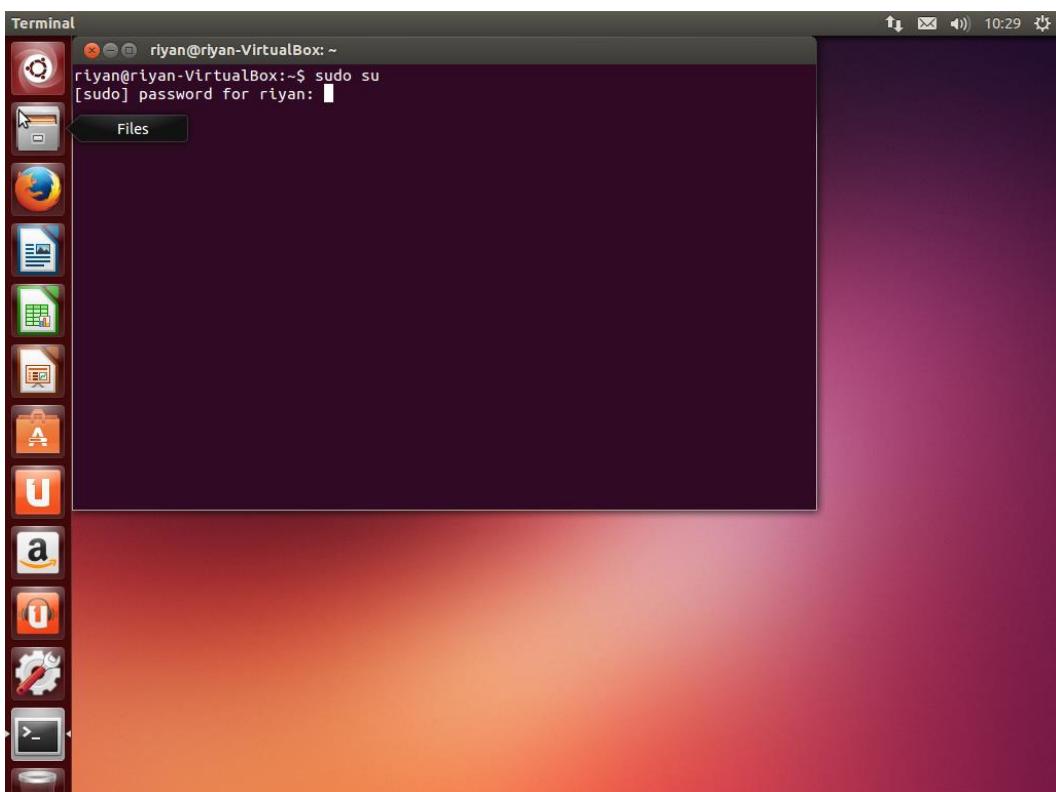
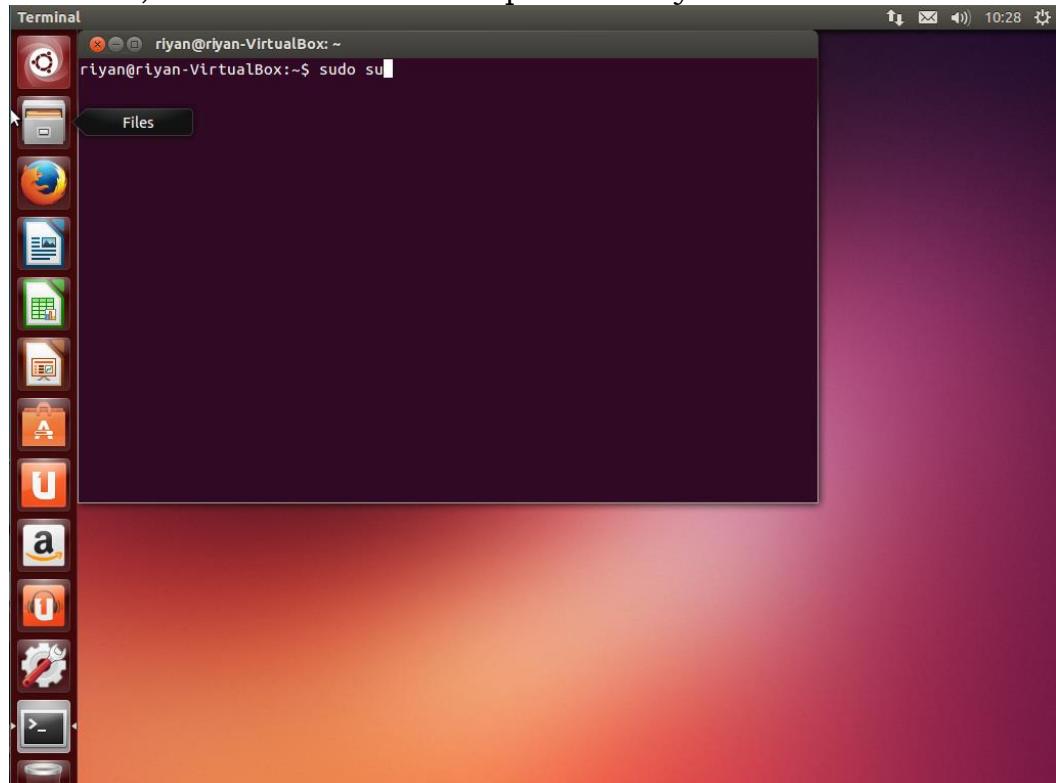
- Ke Client linuxnya, disini saya menggunakan ubuntu desktop sebagai client linuxnya, setelah itu kita serch terminal



Gambar 8.69 ubuntu desktop



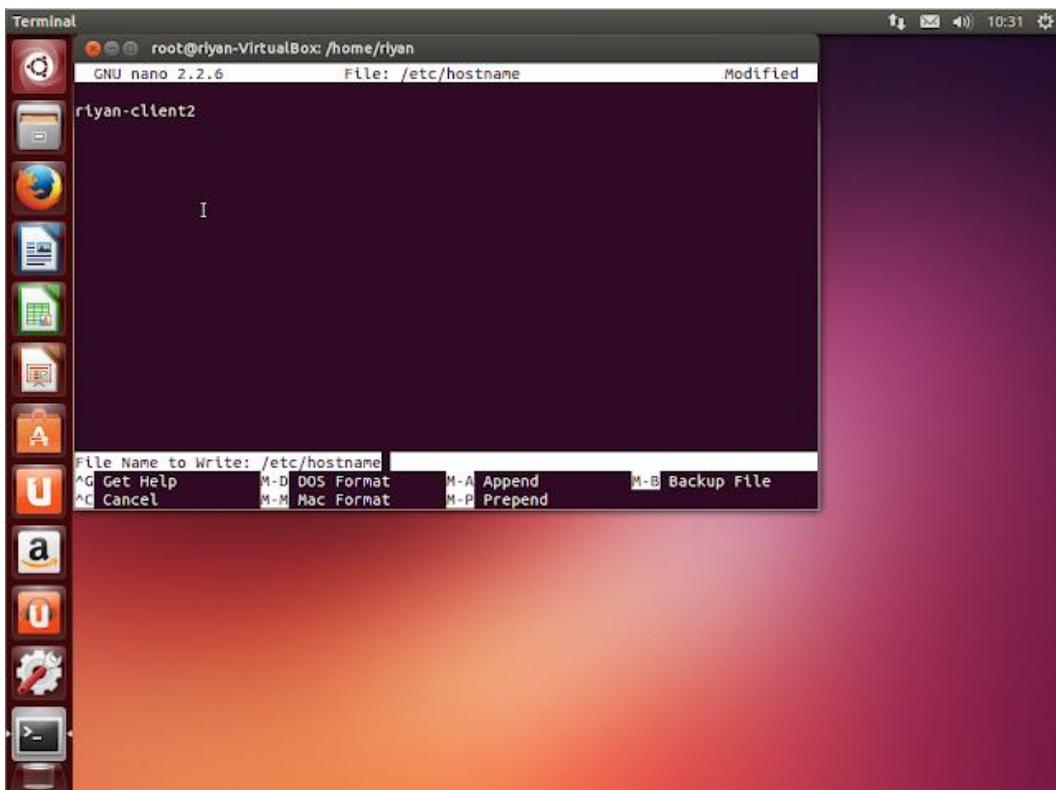
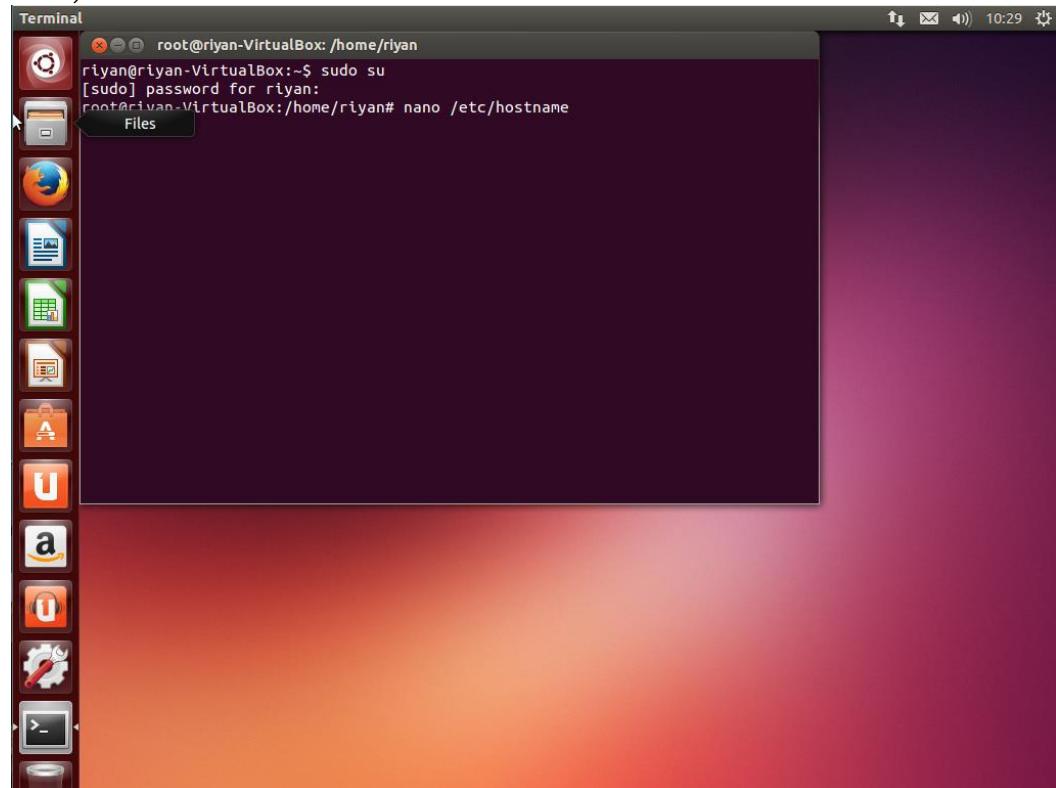
- Setelah itu kita masuk ke rootnya, ketikkan **sudo su** pada terminal, kemudian masukkan passwordnya

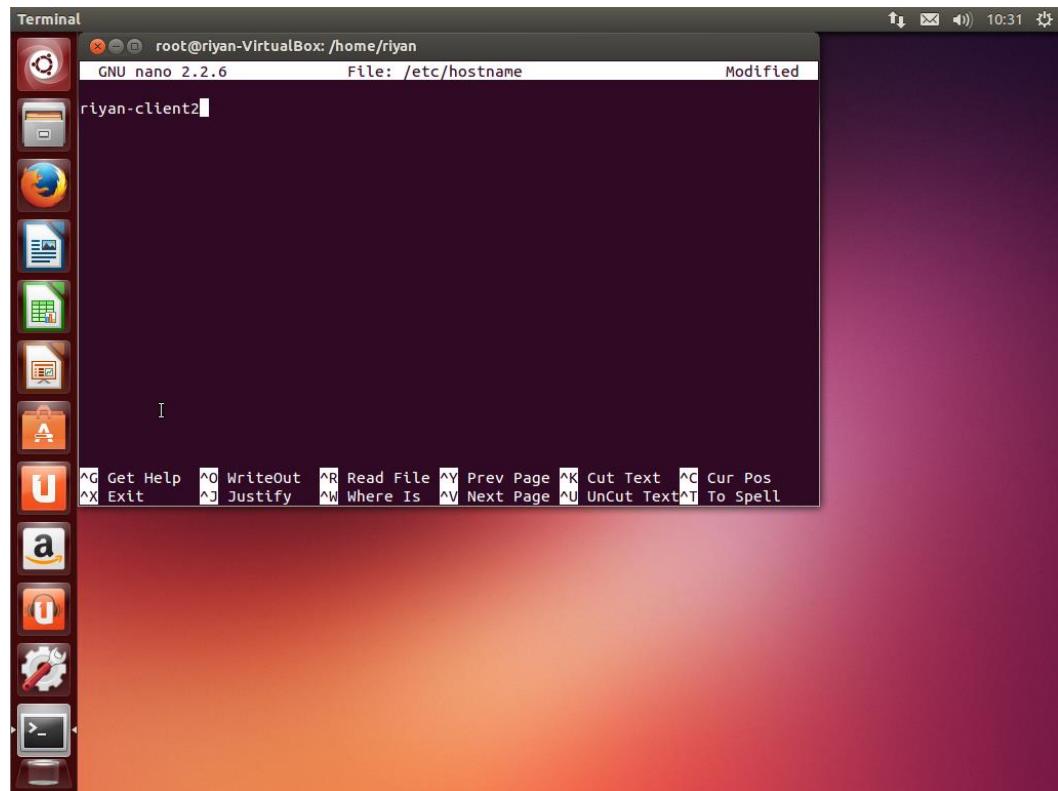


Gambar 8.70 login Ubuntu



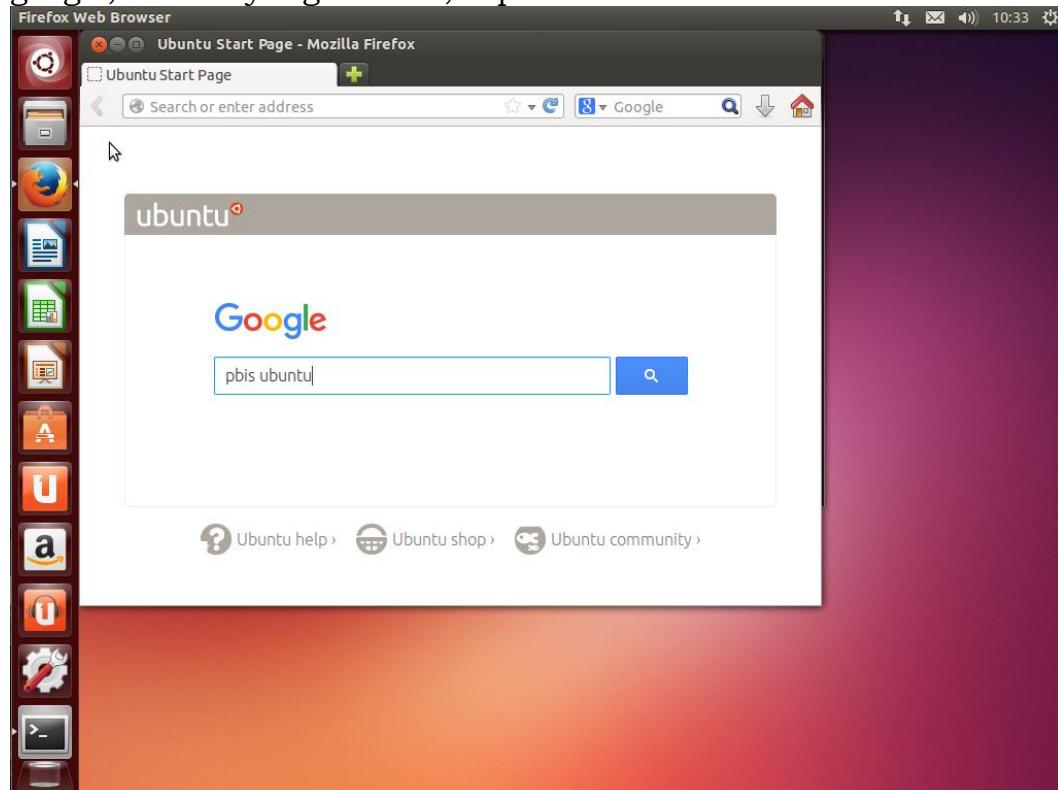
- Dan sekarang kita ganti hostnamenya, perintahnya **nano /etc/hostname**, ketiklah sesuai dengan yang dibuat pada server tadi, kemudian save

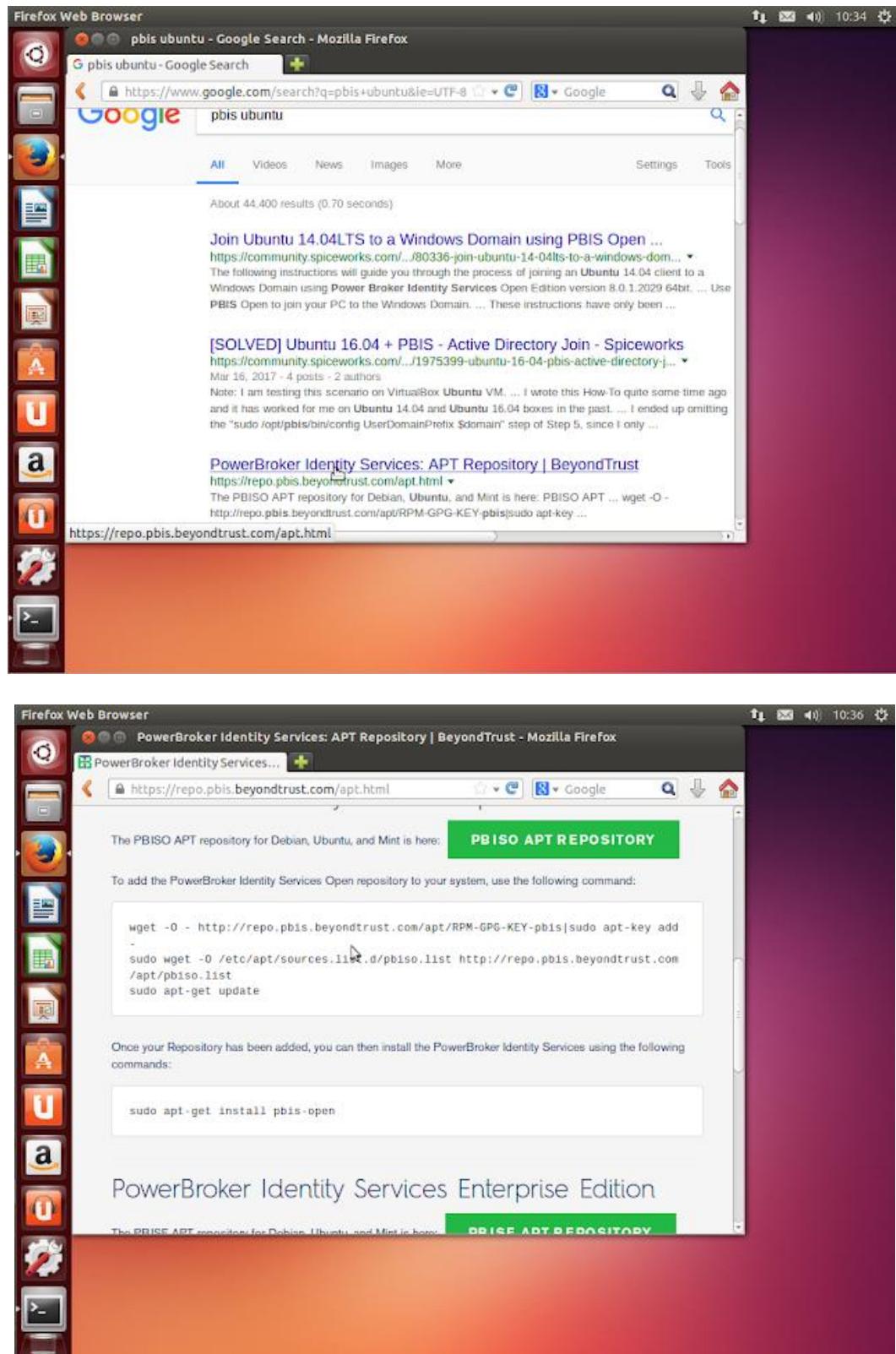




Gambar 8.71 hostname

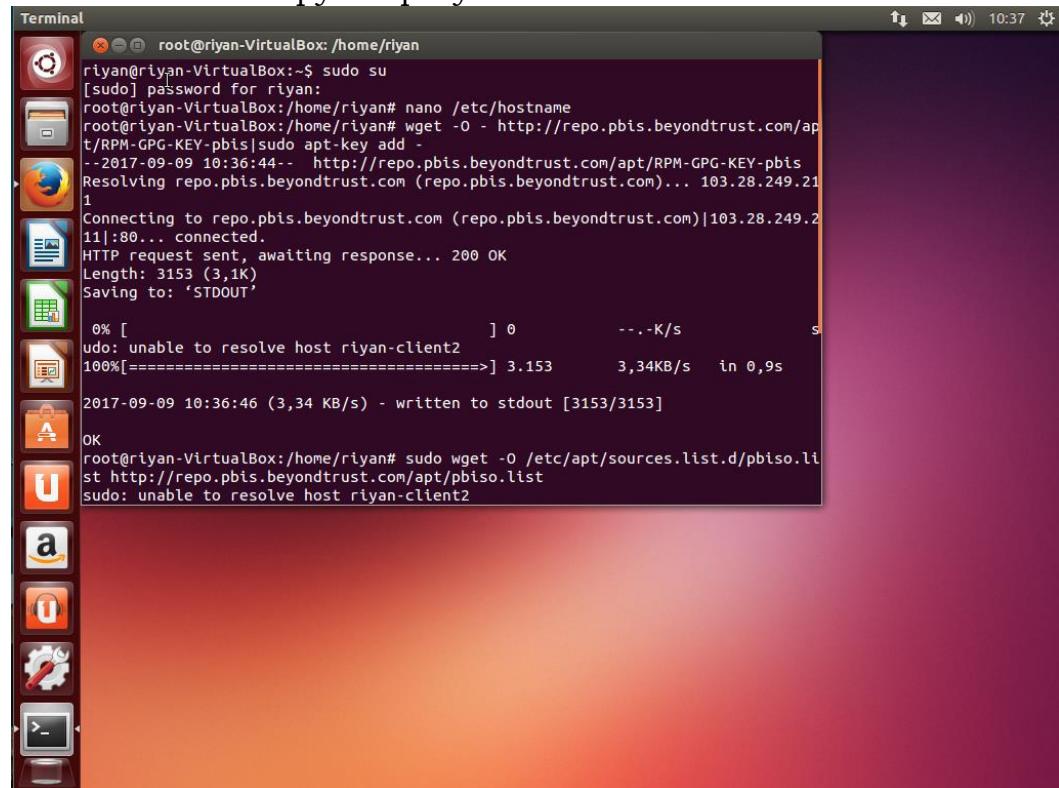
- Sekarang kita harus menginstall pbis ubuntu, kita bisa cari di google, carilah yang trusted, seperti di bawah





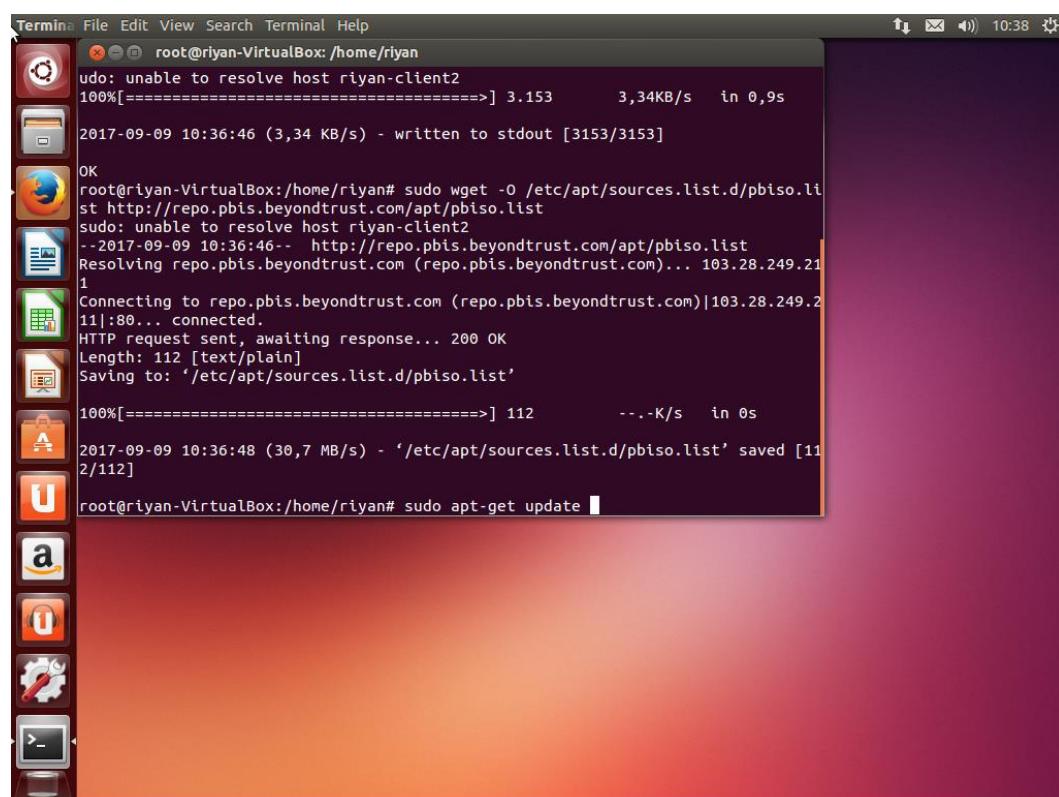
Gambar 8.72 menginstall PBIS Ubuntu

- Setelah itu kita copy scirptnya di terminal tadi



```
root@riyan-VirtualBox: /home/riyan
root@riyan-VirtualBox:~$ sudo su
[sudo] password for rryan:
root@riyan-VirtualBox:/home/riyan# nano /etc/hostname
root@riyan-VirtualBox:/home/riyan# wget -O - http://repo.pbis.beyondtrust.com/apt/RPM-GPG-KEY-pbis | sudo apt-key add -
--2017-09-09 10:36:44-- http://repo.pbis.beyondtrust.com/apt/RPM-GPG-KEY-pbis
Resolving repo.pbis.beyondtrust.com (repo.pbis.beyondtrust.com)... 103.28.249.21
1
Connecting to repo.pbis.beyondtrust.com (repo.pbis.beyondtrust.com)|103.28.249.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3153 (3,1K)
Saving to: 'STDOUT'

0% [=====] 0          --.-K/s
100%[=====] 3.153      3,34KB/s  in 0,9s
2017-09-09 10:36:46 (3,34 KB/s) - written to stdout [3153/3153]
OK
root@riyan-VirtualBox:/home/riyan# sudo wget -O /etc/apt/sources.list.d/pbis.list http://repo.pbis.beyondtrust.com/apt/pbis.list
sudo: unable to resolve host rryan-client2
```



```
root@riyan-VirtualBox: /home/riyan
udo: unable to resolve host rryan-client2
100%[=====] 3.153      3,34KB/s  in 0,9s
2017-09-09 10:36:46 (3,34 KB/s) - written to stdout [3153/3153]
OK
root@riyan-VirtualBox:/home/riyan# sudo wget -O /etc/apt/sources.list.d/pbis.list http://repo.pbis.beyondtrust.com/apt/pbis.list
sudo: unable to resolve host rryan-client2
--2017-09-09 10:36:46-- http://repo.pbis.beyondtrust.com/apt/pbis.list
Resolving repo.pbis.beyondtrust.com (repo.pbis.beyondtrust.com)... 103.28.249.21
1
Connecting to repo.pbis.beyondtrust.com (repo.pbis.beyondtrust.com)|103.28.249.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 112 [text/plain]
Saving to: '/etc/apt/sources.list.d/pbis.list'

100%[=====] 112          --.-K/s  in 0s
2017-09-09 10:36:48 (30,7 MB/s) - '/etc/apt/sources.list.d/pbis.list' saved [112/112]
root@riyan-VirtualBox:/home/riyan# sudo apt-get update
```

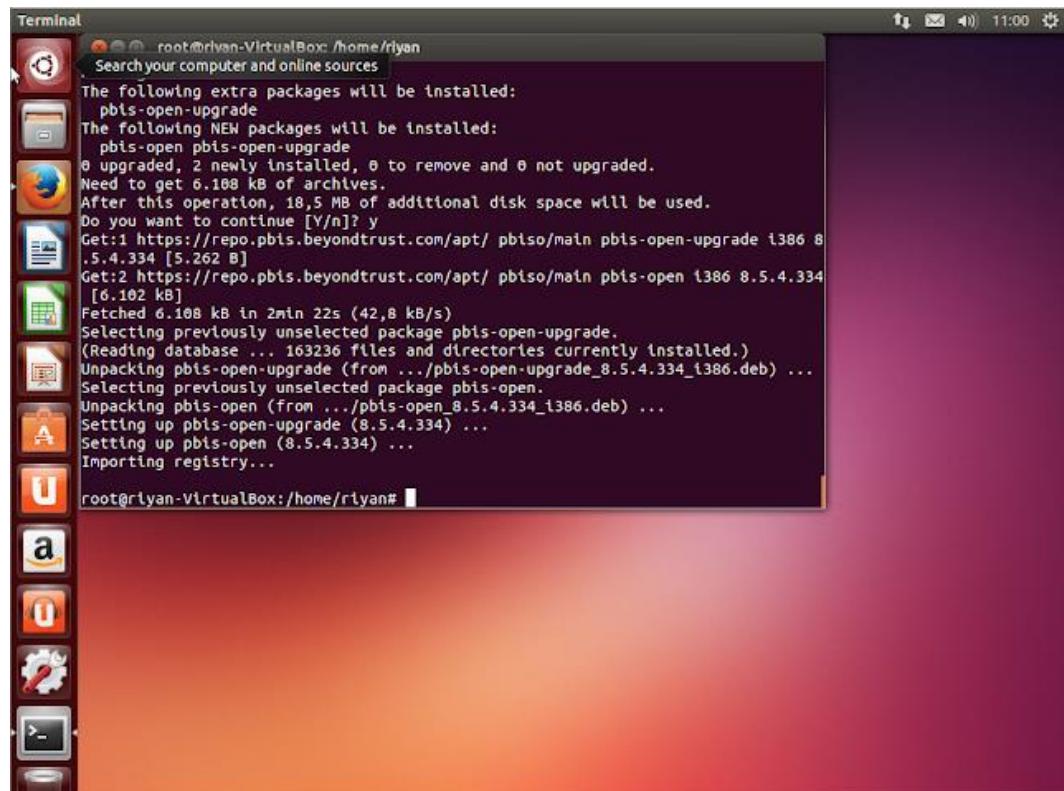
Gambar 8.73 copy script



- Kemudian masukkan script yang bawahnya pada terminal, lalu ketik y untuk yes

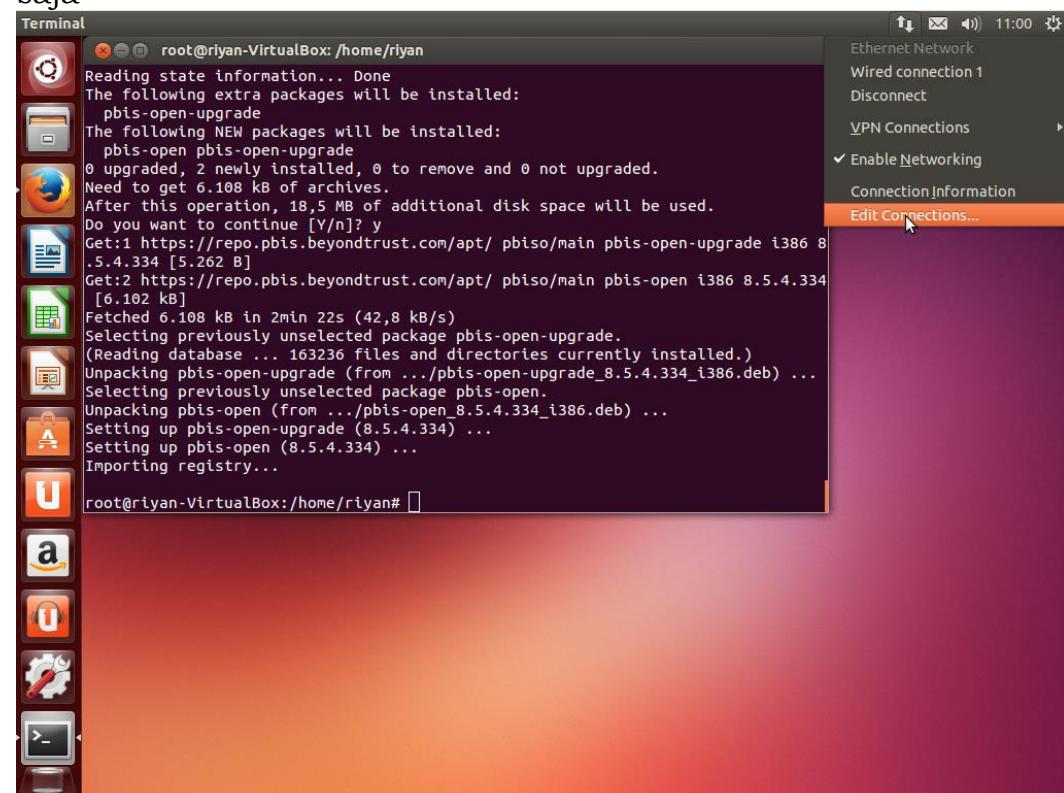
```
root@riyan-VirtualBox: /home/riyan
. Search your computer and online sources lve.ubuntu.com/ubuntu/dists/saucy-backports/restricted/source/Sources 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/universe/source/Sources 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/multiverse/source/Sources 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/main/binary-i386/Packages 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/restricted/binary-i386/Packages 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/universe/binary-i386/Packages 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/multiverse/binary-i386/Packages 404 Not Found [IP: 91.189.91.26 80]
E: Some index files failed to download. They have been ignored, or old ones used instead.
root@riyan-VirtualBox:/home/riyan# sudo apt-get install pbis-open
```

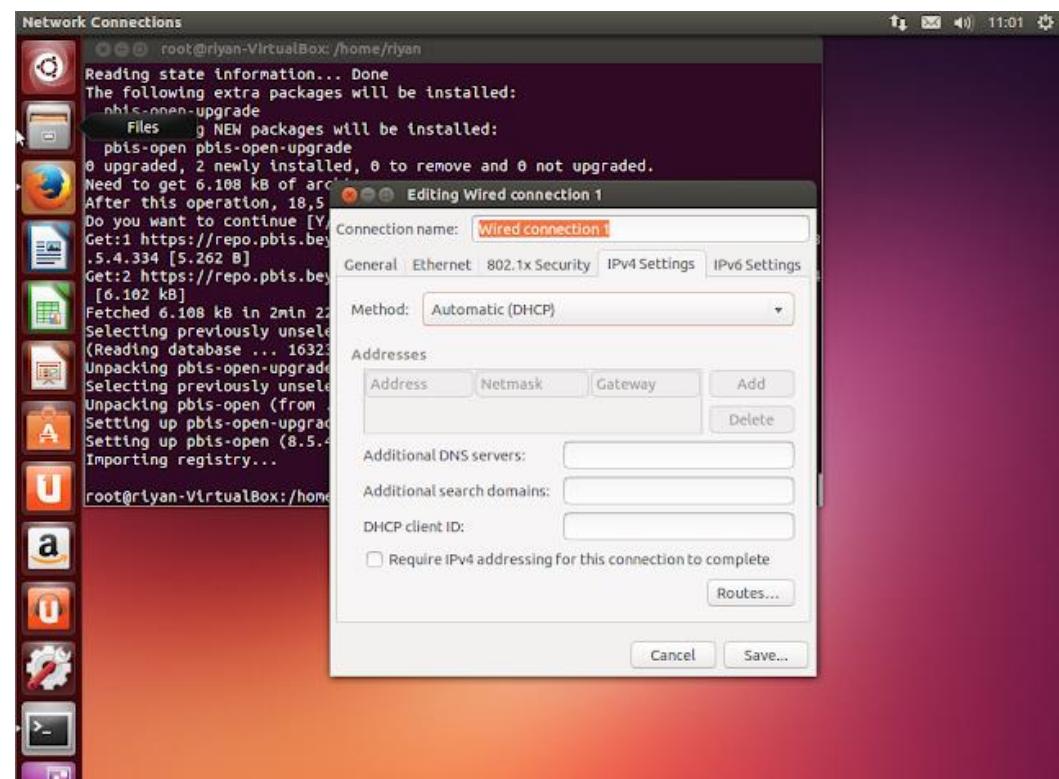
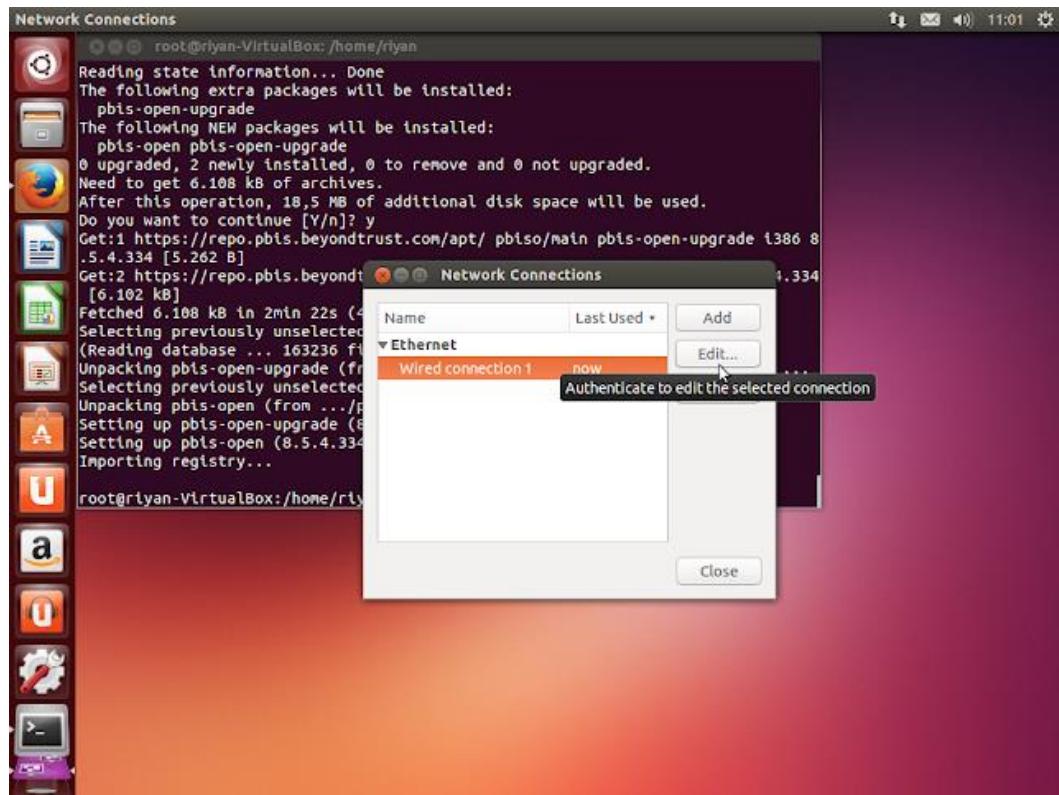
```
root@riyan-VirtualBox: /home/riyan
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/restricted/binary-i386/Packages 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/universe/binary-i386/Packages 404 Not Found [IP: 91.189.91.26 80]
W: Failed to fetch http://id.archive.ubuntu.com/ubuntu/dists/saucy-backports/multiverse/binary-i386/Packages 404 Not Found [IP: 91.189.91.26 80]
E: Some index files failed to download. They have been ignored, or old ones used instead.
root@riyan-VirtualBox:/home/riyan# sudo apt-get install pbis-open
sudo: unable to resolve host rryan-client2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  pbis-open-upgrade
The following NEW packages will be installed:
  pbis-open pbis-open-upgrade
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 6.108 kB of archives.
After this operation, 18.5 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

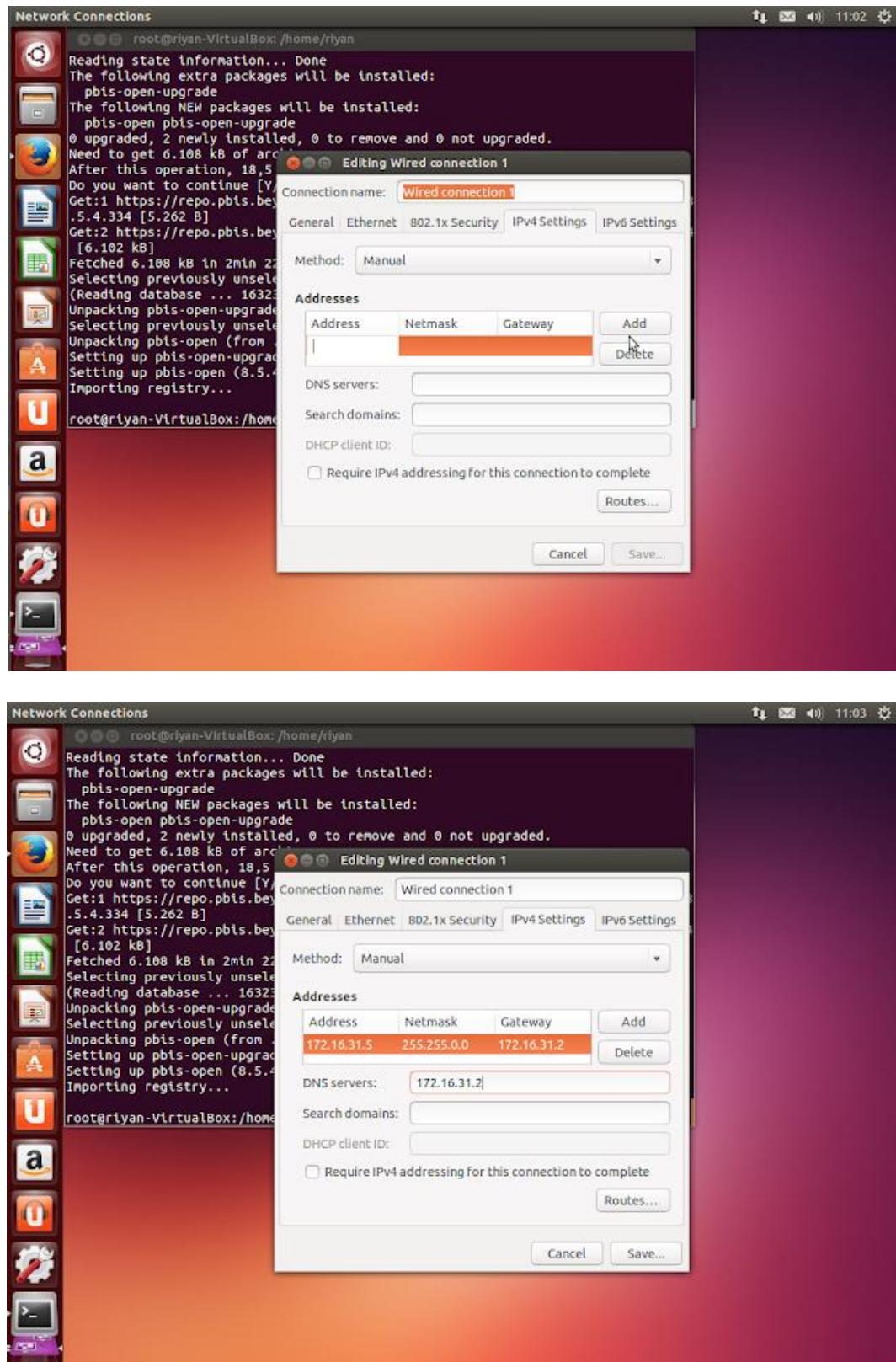


Gambar 8.74 masukkan script pada terminal

- Setting ip addressnya, kita setting sesai dengan yang kita tambahkan pada server tadi, bila sudah save dan langsung close saja





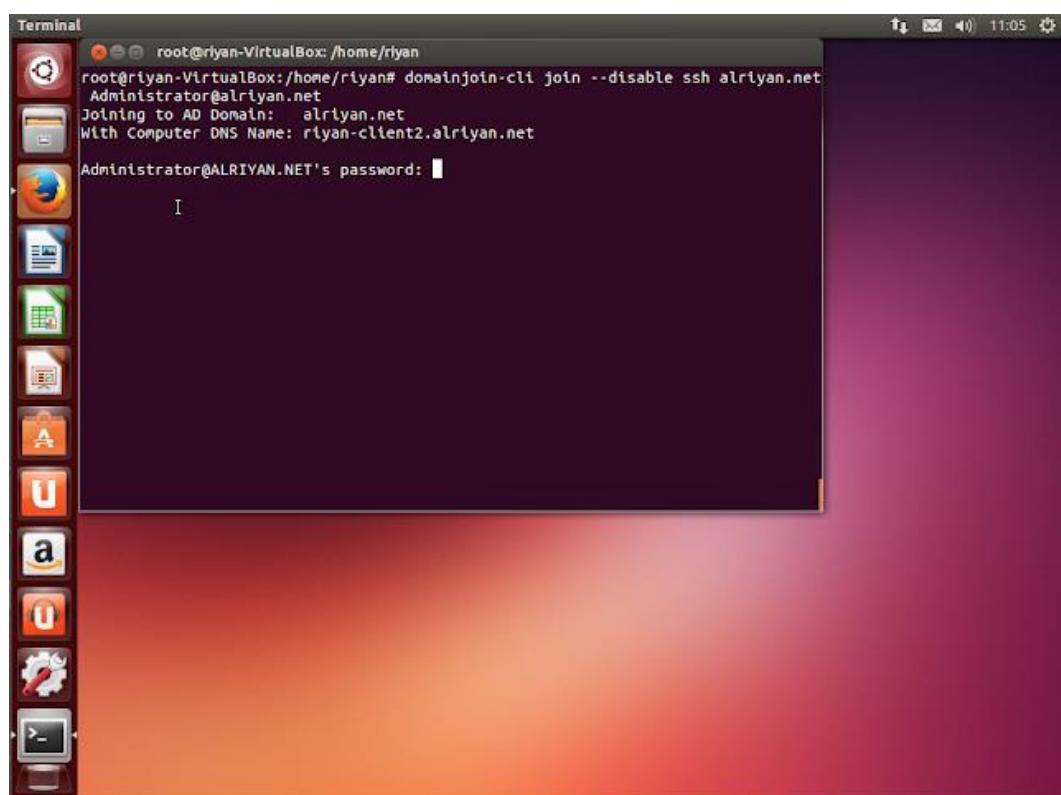
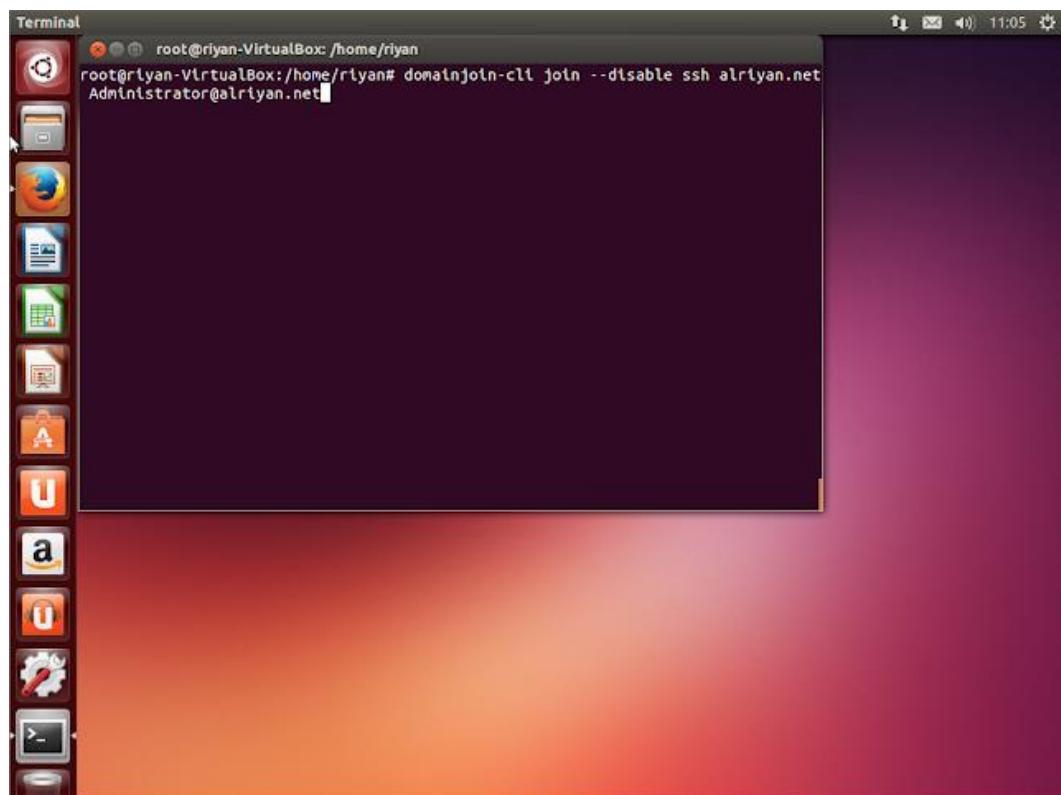


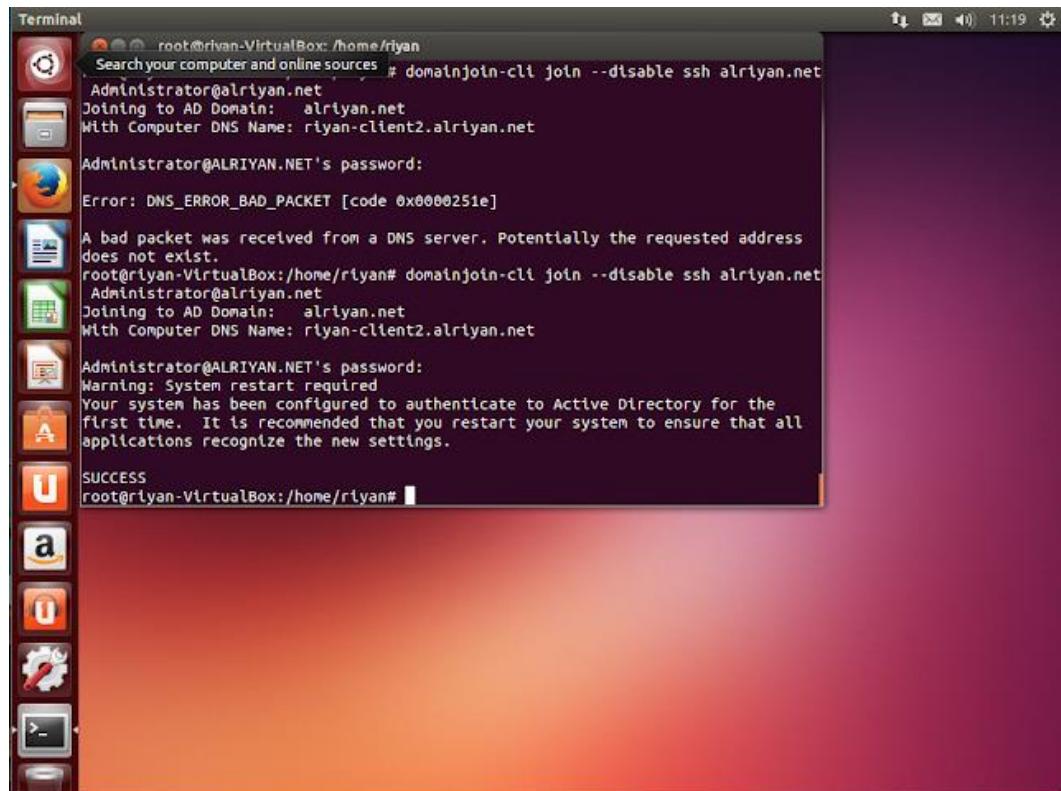
Gambar 8.75 Setting ip address

- Join domainnya, perintahnya **domainjoin-cli join --disable ssh alriyan.net Administrator@alriyan.net**, setelah itu masukkan



passwordnya, jika sudah berhasil akan terdapat tulisan **SUCCESS**, seperti gambar dibawah





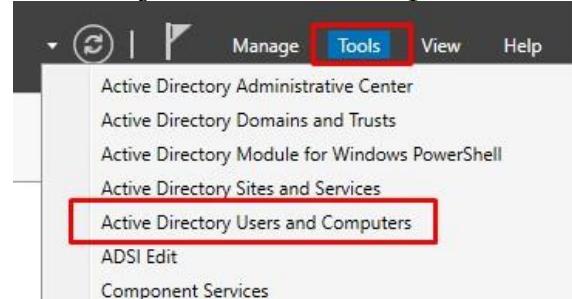
Gambar 8.76 Joint Domain

8.3.9. Active Directory User and Computer (Membuat User Account)

Pada konfigurasi kali ini, menggunakan Windows Server Standard 2016 dan Windows 7 sebagai Client. Sebelum teman-teman konfigurasi GPO ini, teman-teman harus install feature Active Directory terlebih dahulu dan Windows 7 harus join domain ke dalam Active Directorynya. Untuk teman-teman yang belum tahu bagaimana cara install Windows Server GPO sendiri merupakan kepanjangan dari Group Policy Object, yaitu sebuah fitur yang terdapat pada Active Directory Windows Server, yang berfungsi untuk memanage konfigurasi sistem operasi komputer client secara terpusat. Contohnya user active directory bisa dikonfigurasikan tidak dapat membuka control panel, tidak dapat membuka browser dan masih banyak lagi. Namun, Pada konfigurasi kali ini, TechnoBoard akan membuat Tampilan Text ketika user Active Directory login.

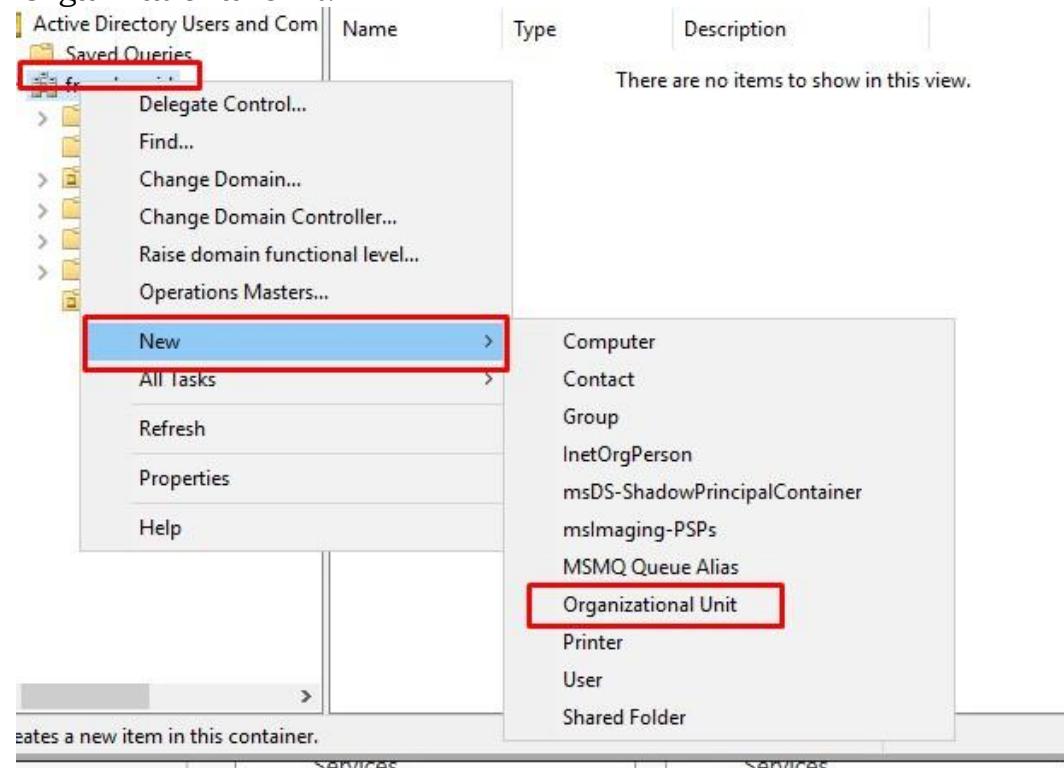
Konfigurasi GPO Pada Windows Server 2016

1. Bukalah server manager, lalu klik tools, kemudian pilih Active Directory Users and Computers.



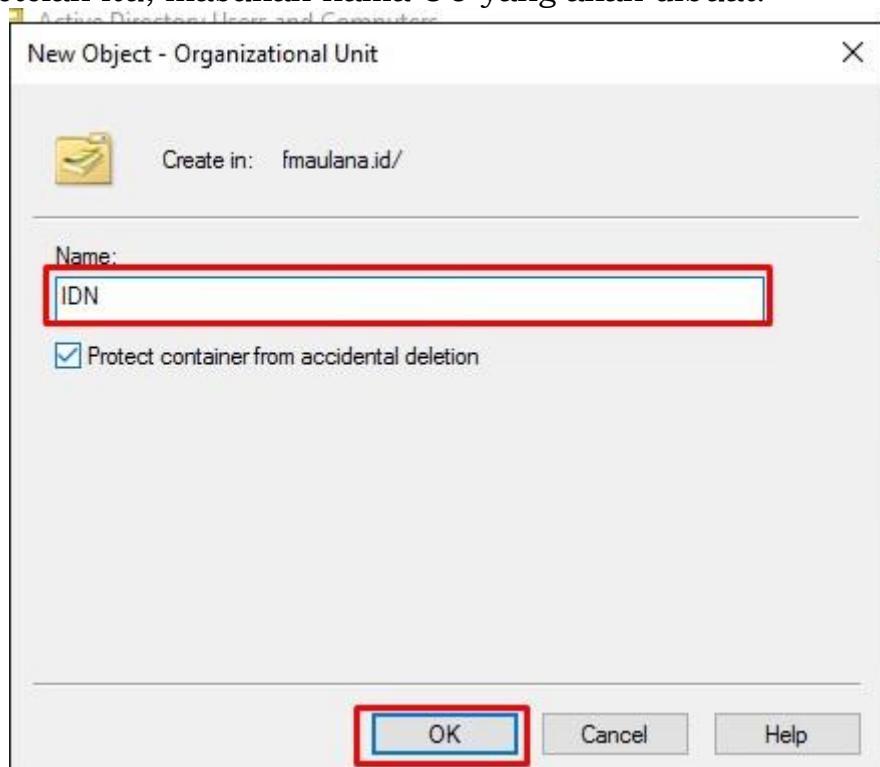
gambar 8.77 server manager

2. Kemudian, klik kanan pada domain, lalu pilih new, kemudian klik Organizational Unit.



Gambar 8.78 membuat organizational unit

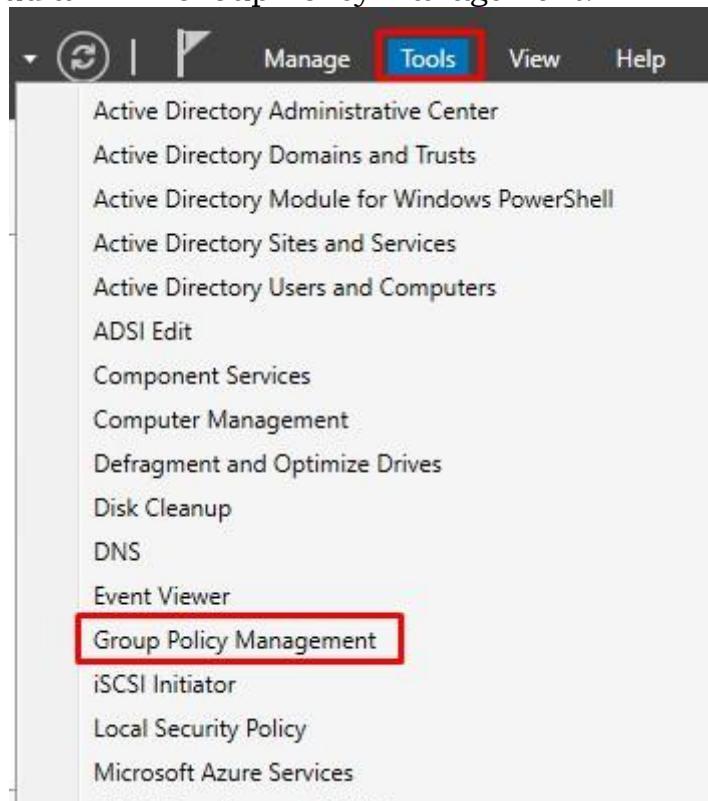
3. Setelah itu, masukan nama OU yang akan dibuat.



Gambar 8.79 memasukkan nama OU

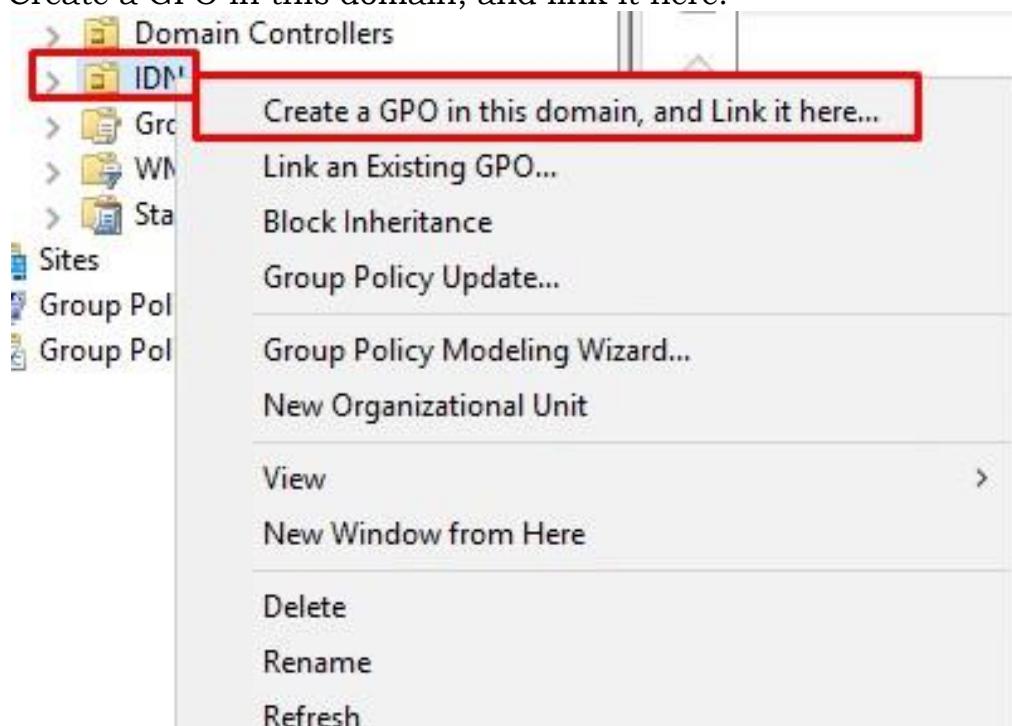


4. Berikutnya, buka kembali server manager, lalu pilih tools, kemudian klik Group Policy Management.



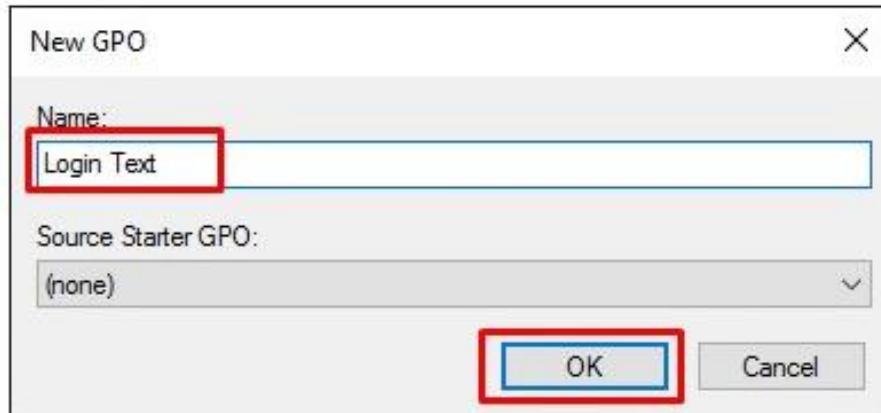
Gambar 8.80 group policy management

5. Selanjutnya klik kanan pada OU yang telah kita buat, lalu klik Create a GPO in this domain, and link it here.



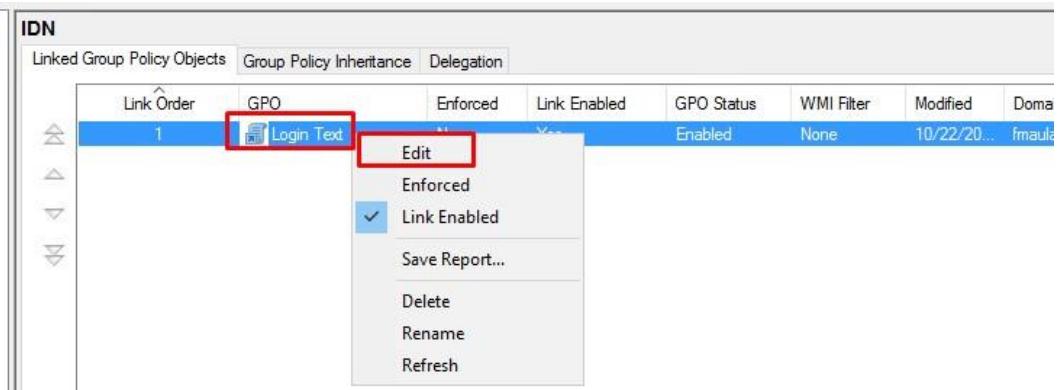
Gambar 8.81 create GPO

6. Pada bagian ini, silahkan beri nama untuk GPO yang akan kita buat, setelah itu, klik OK.



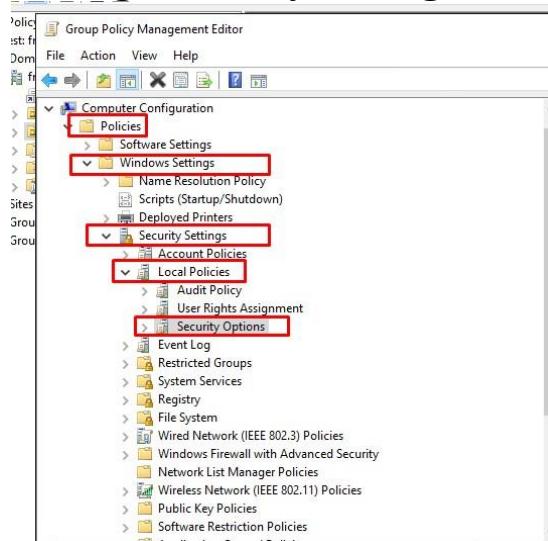
Gambar 8.82 New GPO

7. Kemudian klik kanan pada GPO yang tadi telah dibuat. Lalu pilih Edit.



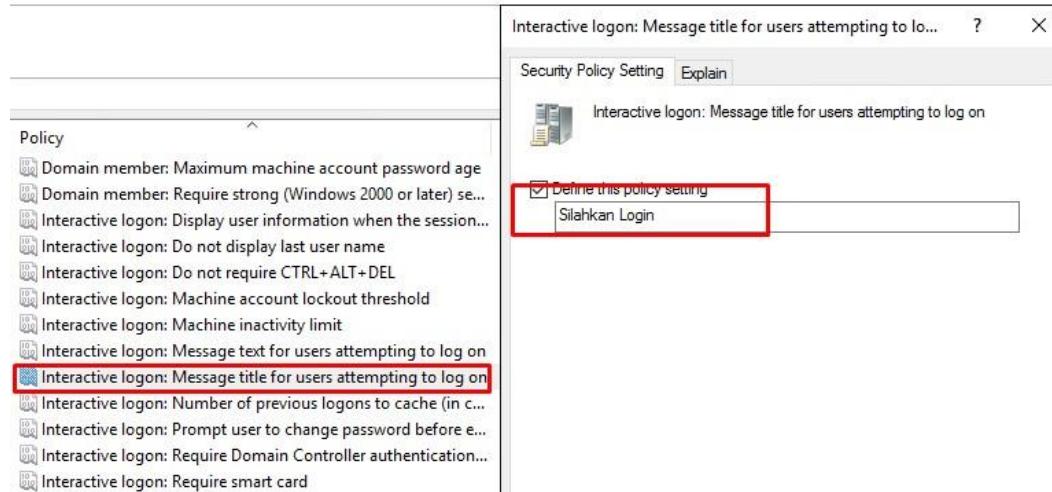
Gambar 8.83 mengedit GPO

8. Setelah itu, kita akan membuat tulisan login pada client, pada bagian ini pilih Computer **Configuration>Policies>Windows Settings>Security Settings>Local Policies>Security Options**.



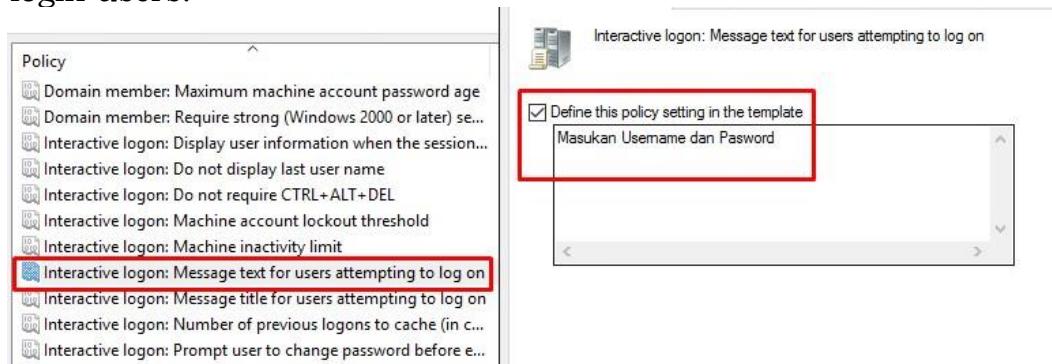
Gambar 8.84 Configuration

9. Pada bagian ini, carilah **Interactive logon : Message title users attempting to log on**, lalu klik 2 kali , kemudian masukan Title untuk tampilan login users.



Gambar 8.85 Message title users

10. Setelah itu, klik 2 kali pada **Interactive logon : Message text for users attempting to log on**. Lalu masukan text untuk tampilan login users.



Gambar 8.86 Message text for users

11. Terakhir, pada windows 7 cobalah restart, lalu nanti akan muncul text yang tadi kita buat sebelumnya.



Gambar 8.87 restart

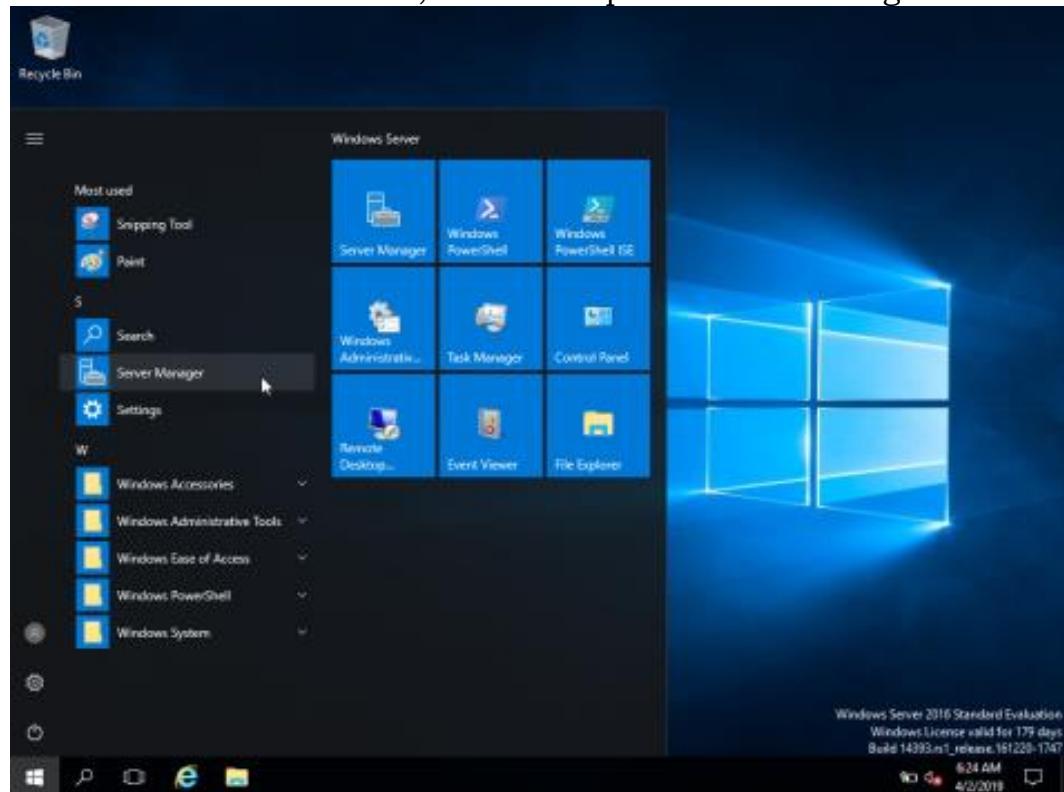
8.3.10. Instalasi dan Konfigurasi DHCP Server

Dynamic Host Configuration Protocol (DHCP) adalah protokol klien / server yang secara otomatis menyediakan host IP (Internet Protocol) dengan alamat IP dan informasi konfigurasi terkait lainnya seperti subnet mask dan gateway default.

RFCs 2131 dan 2132 mendefinisikan DHCP sebagai standar Internet Engineering Task Force (IETF) berdasarkan Bootstrap Protocol (BOOTP), sebuah protokol yang mana DHCP berbagi banyak detail implementasi. DHCP memungkinkan host untuk mendapatkan informasi konfigurasi TCP / IP yang diperlukan dari server DHCP.

Sedikit catatan: Pastikan anda tidak mensetup lebih dari satu server DHCP di jaringan yang sama (akan dianggap bahwa Anda akan memiliki server DHCP jahat di jaringan), jadi pastikan Anda menonaktifkan peran di Virtualbox (dengan asumsi Anda menggunakan Virtualbox seperti saya di sini dalam tutorial ini). Tentu, Anda dapat melakukan beberapa hal lanjut seperti memiliki server DHCP cadangan, tetapi hanya untuk memulainya, tetap gunakan satu. Disini karena sebelumnya saya sudah menginstall Windows Server 2016 di Virtual Box jadi langsung saja ke pembahasannya yaa dan jangan lupa dibaca artikel Install Windows Server 2016 di Virtual Box

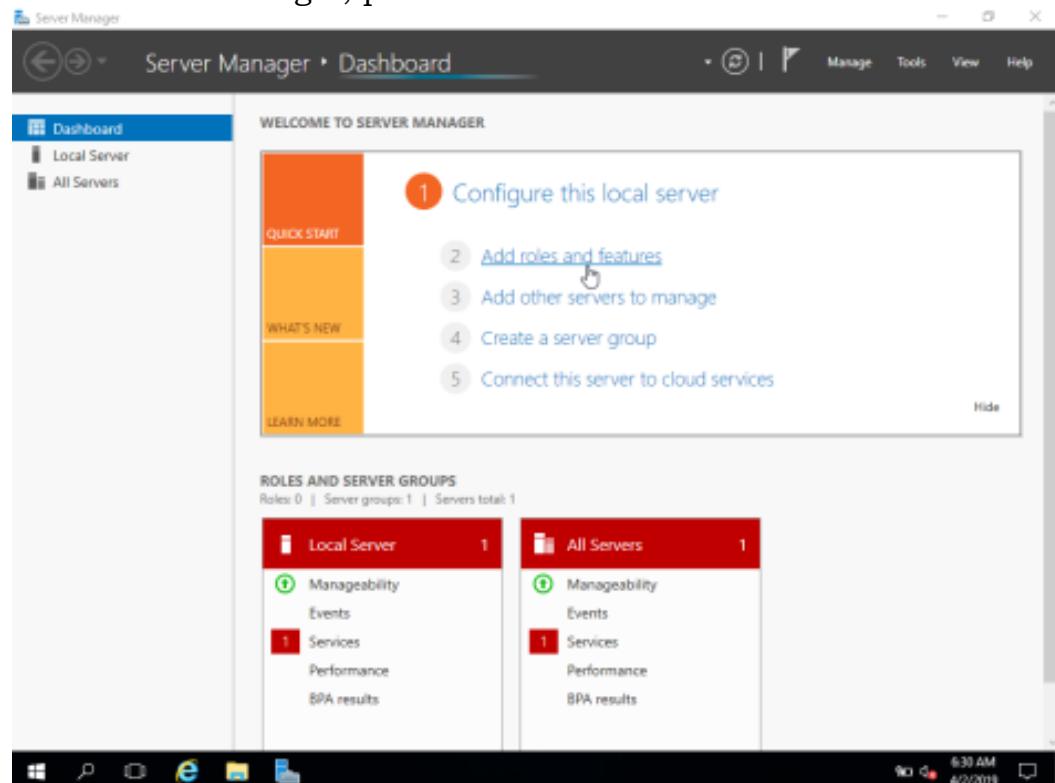
1. Klik menu Windows Start, kemudian pilih Server Manager



Gambar 8.88 server manager

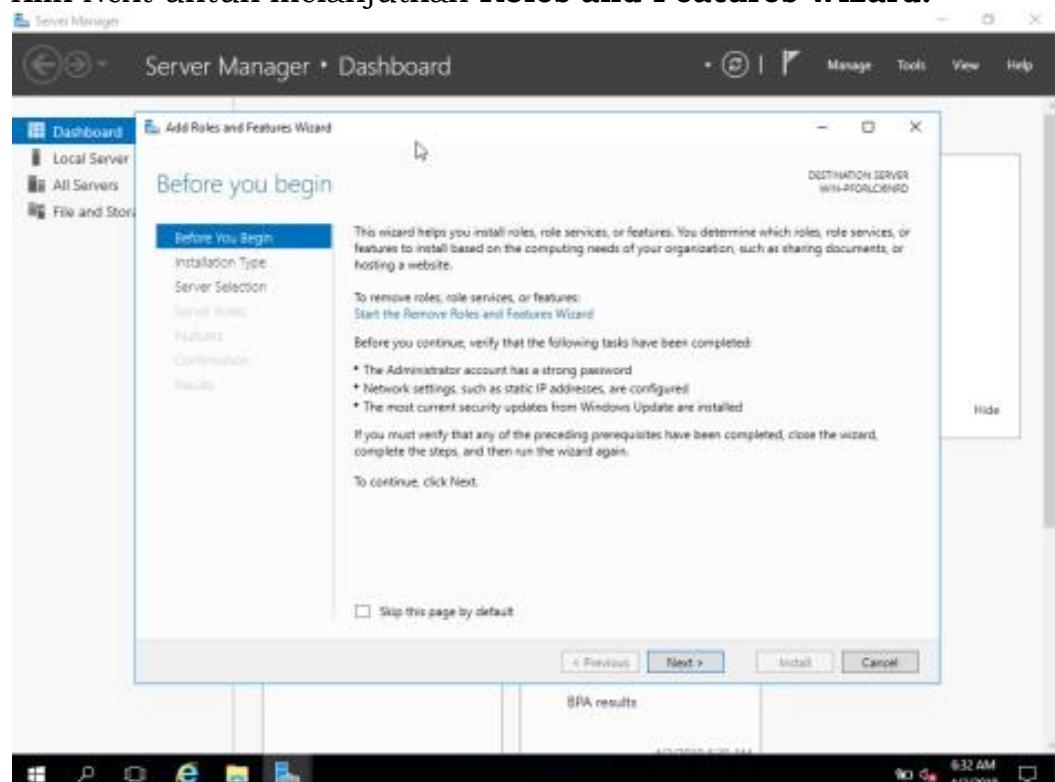


2. Pada Server Manager, pilih Add roles and features



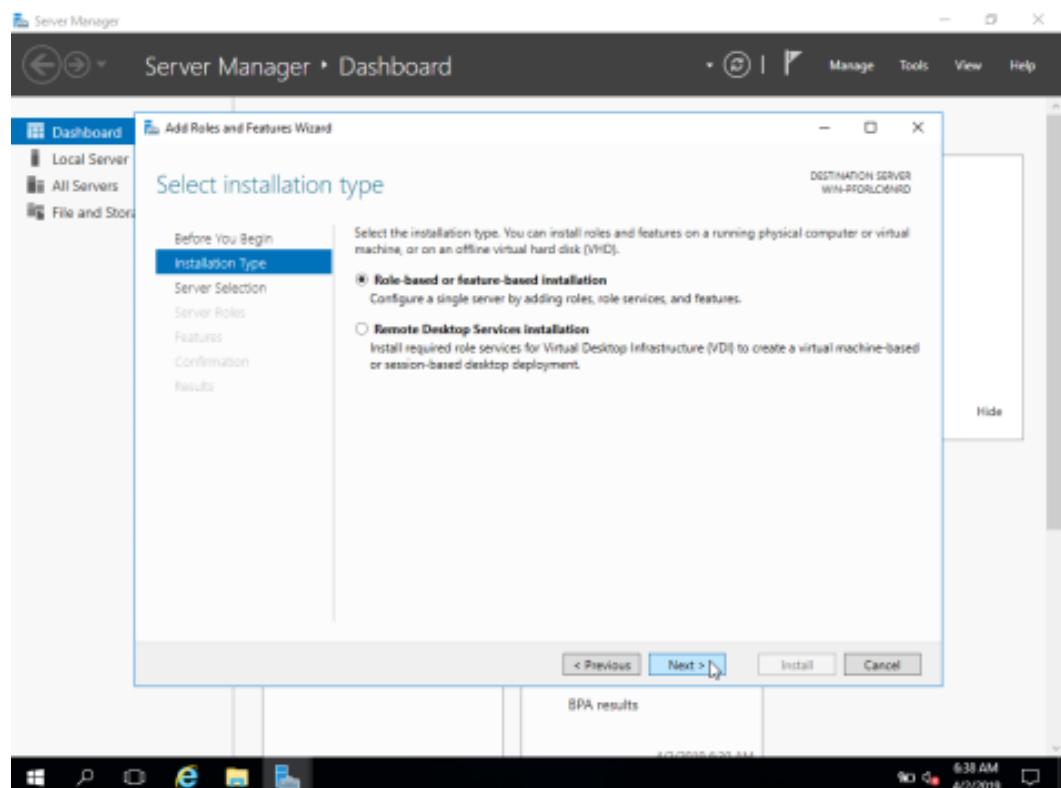
Gambar 8.89 Add roles and features

3. Klik Next untuk melanjutkan **Roles and Features Wizard**.



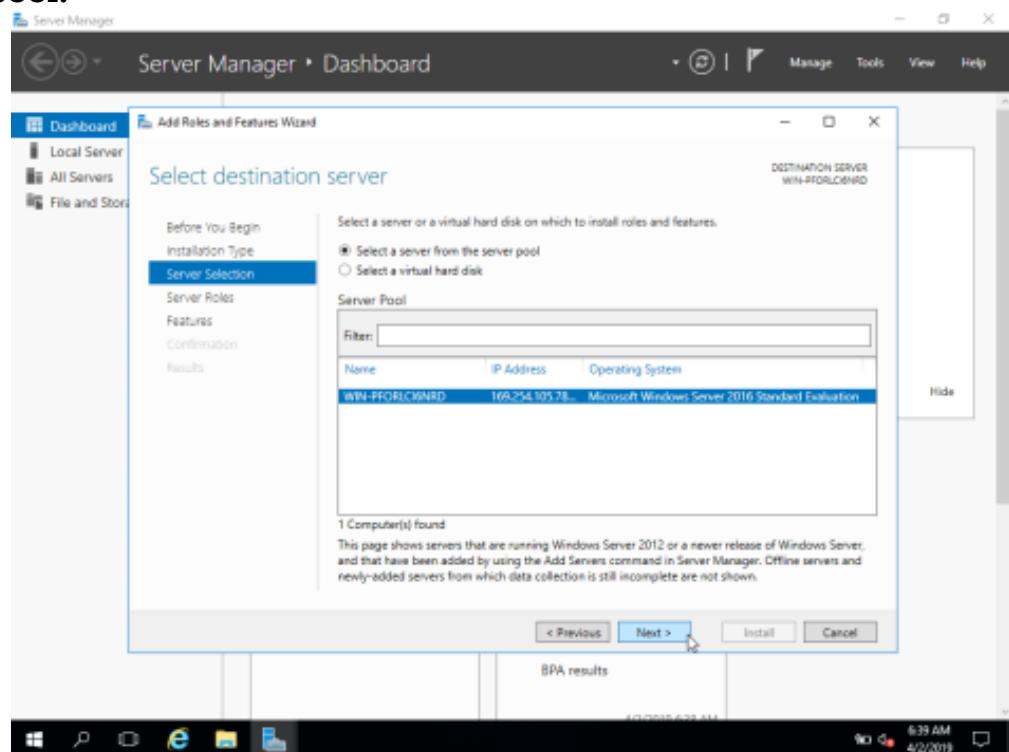
Gambar 8.89 roels and features wizard

4. Pilih **Role-based or feature-based installation** dan klik Next.



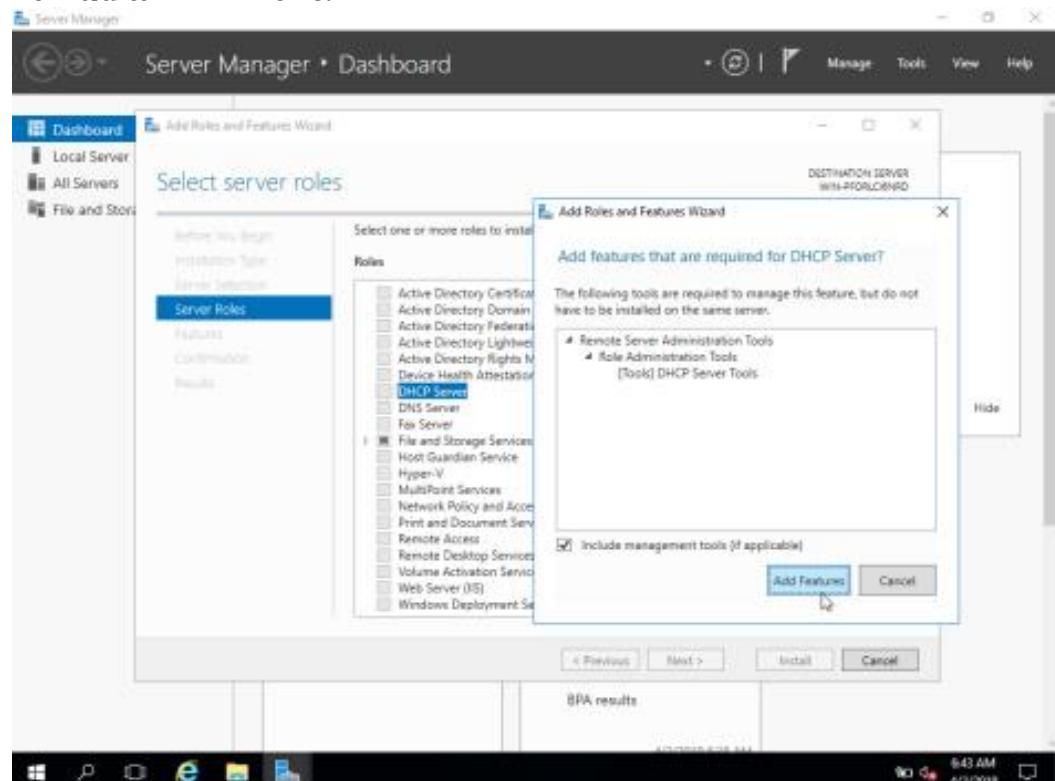
Gambar 8.90 Role-based or feature-based installation

5. Pilih server tempat Anda ingin mengkonfigurasi DHCP dan klik **Next**. Disini saya memilih **Select the server from server pool**.



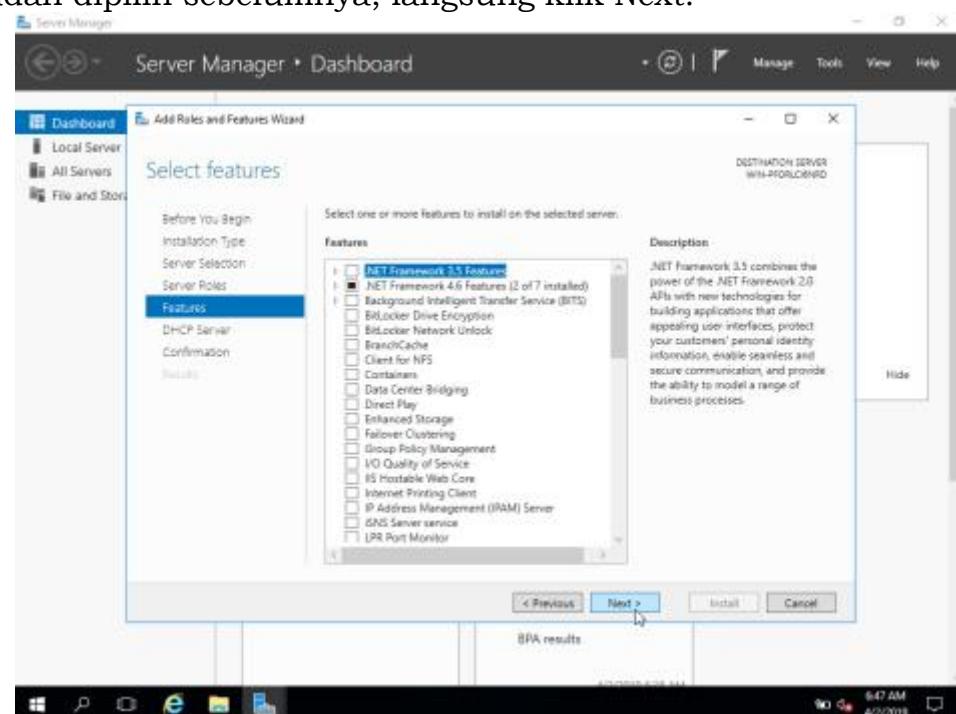
Gambar 8.91 select the server from server pool

- Pilih **DHCP Server** dari Server Roles. Setelah Anda memilih DHCP Server, jendela baru akan muncul. Klik **Add Features**, dan kemudian klik **Next**.



Gambar 8.92 DHCP Server

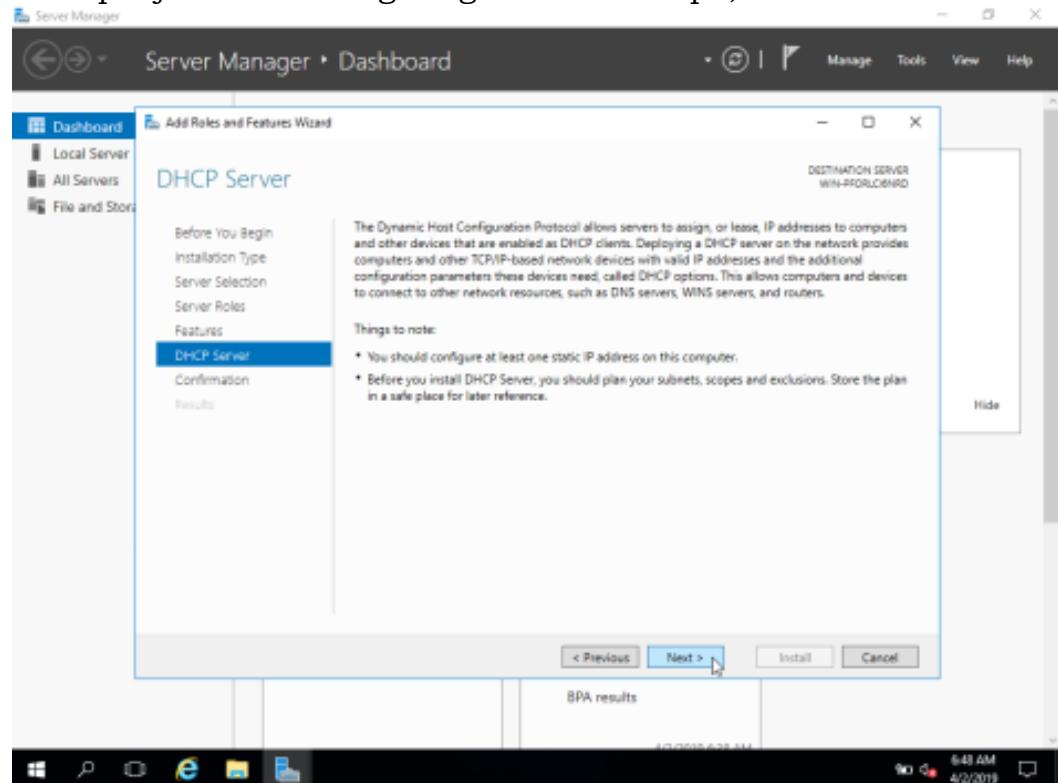
- Karena NET Frameworks yang diperlukan untuk server DHCP sudah dipilih sebelumnya, langsung klik Next.



Gambar 8.93 Net Frameworks

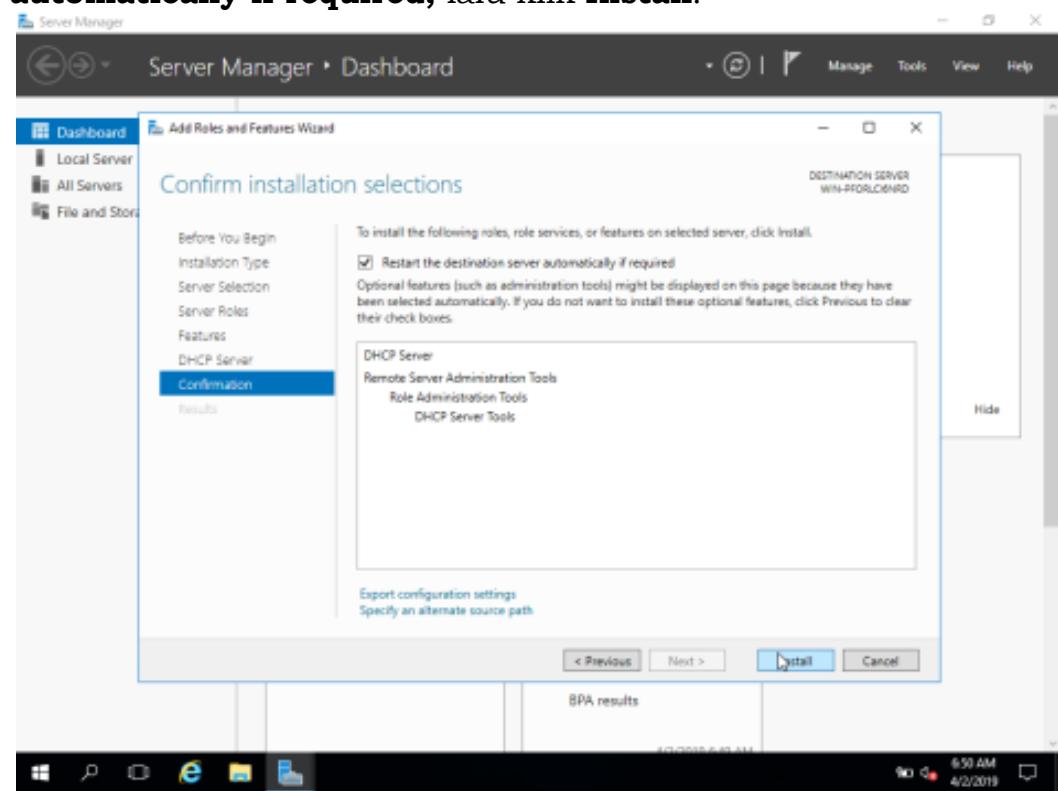


8. Baca penjelasan tentang fungsi DHCP itu apa, lalu klik **Next**.



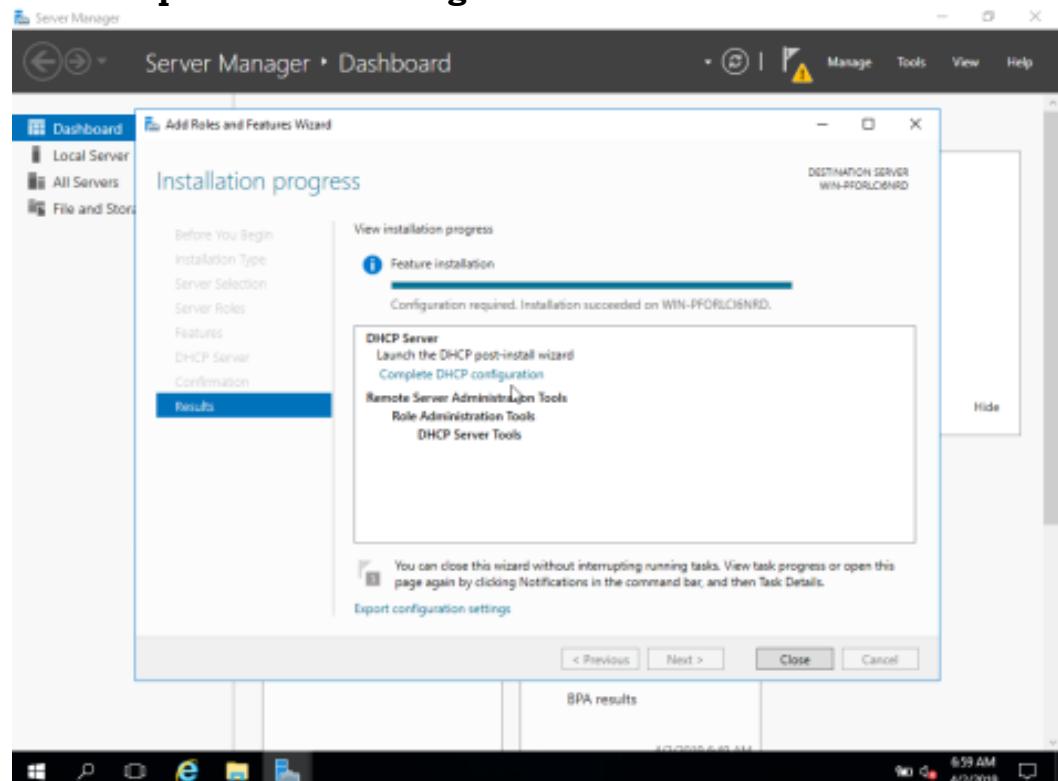
Gambar 8.94 penjelasan about DHCP

9. Pastikan untuk mencentang **Restart the destination server automatically if required**, lalu klik **Install**.



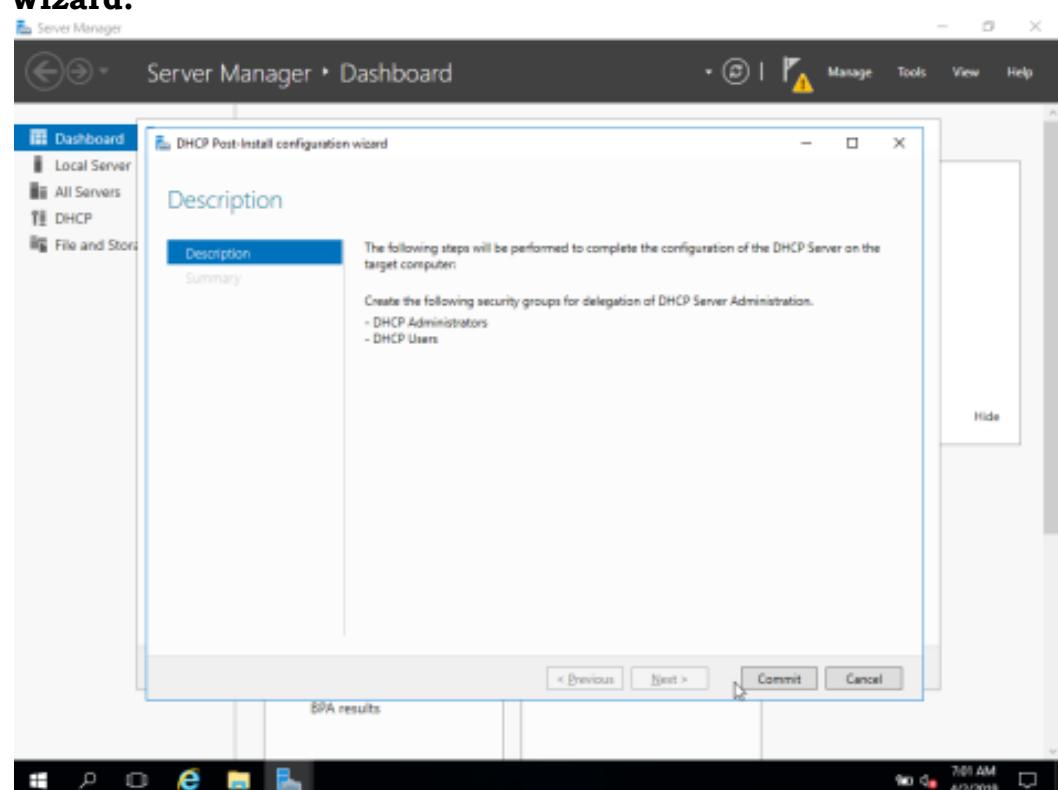
Gambar 8.95 restart the destination

10. Klik Complete DHCP Configuration.



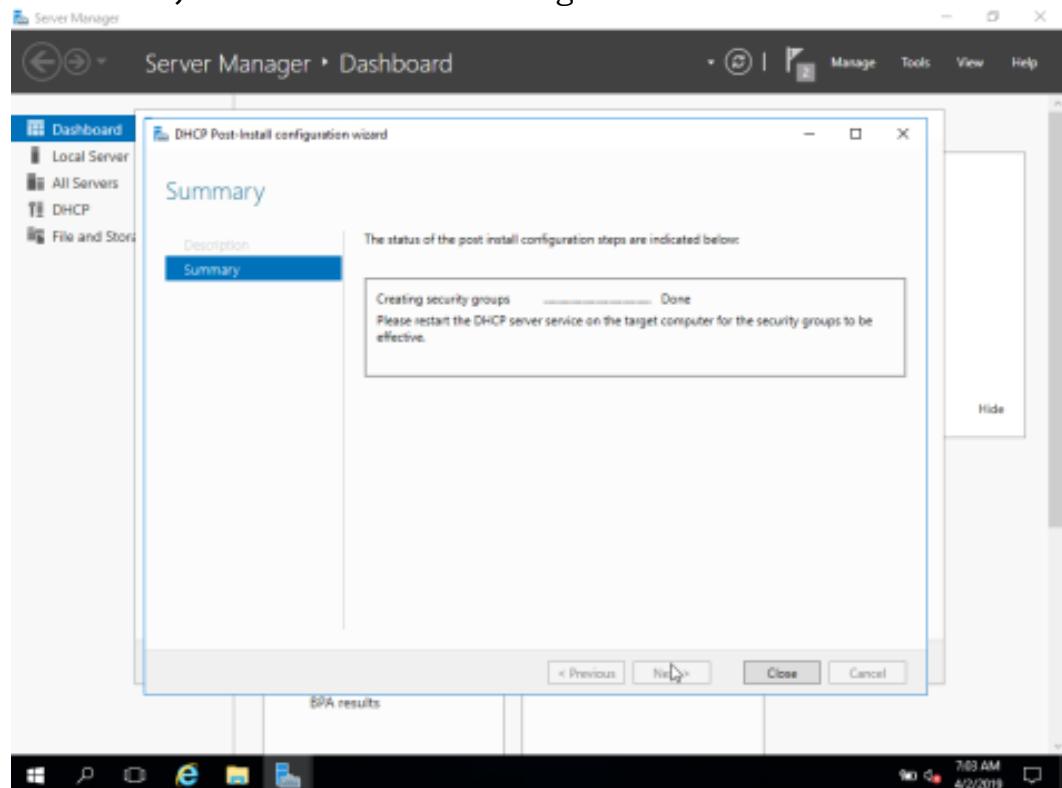
Gambar 8.96 Complete DHCP Configuration

11. Klik Commit, untuk melanjutkan proses **DHCP Post-Install Wizard.**



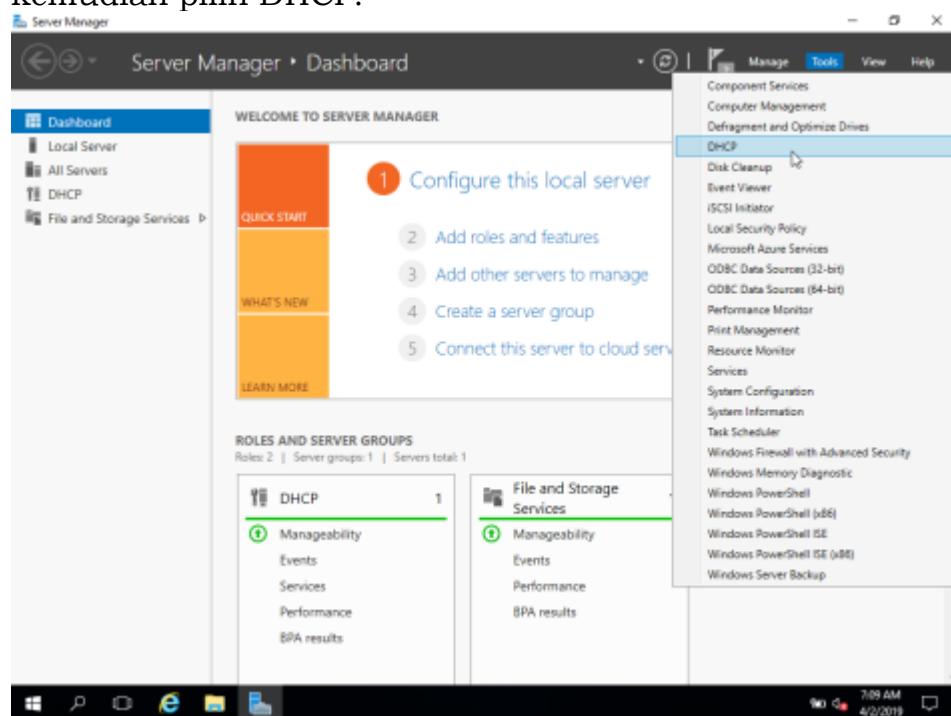
Gambar 8.97 DHCP Post-Install Wizard

12. Klik **Close**, kita sudah selesai mengInstall fitur **DHCP Server**.



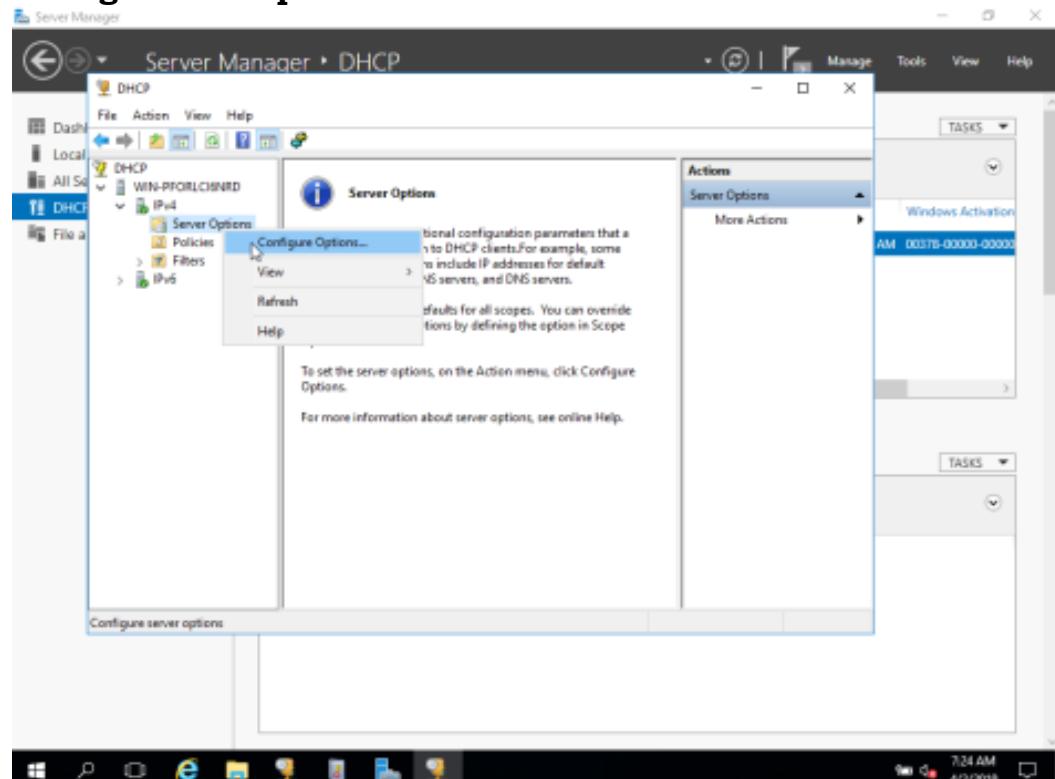
Gambar 8.98 Finish Installation DHCP Server

13. Pada Server Manager > Dashboard , klik Tools di kanan atas, kemudian pilih DHCP.



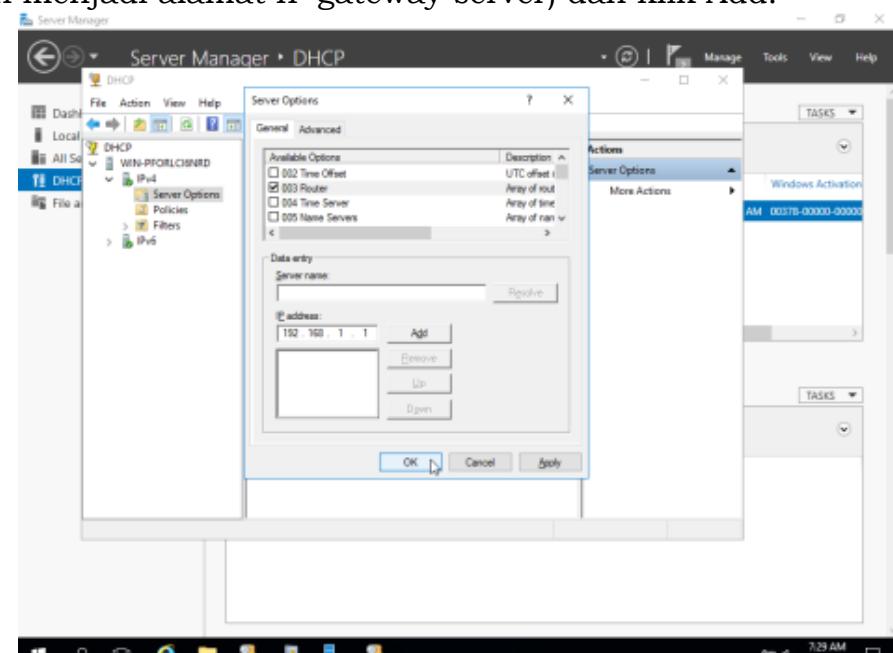
Gambar 8.99

14. Kemudian expand pada “**Server Name**” yang telah dibuat > expand **IPv4** > klik kanan pada **Server Options** dan pilih **Configuration Options**.



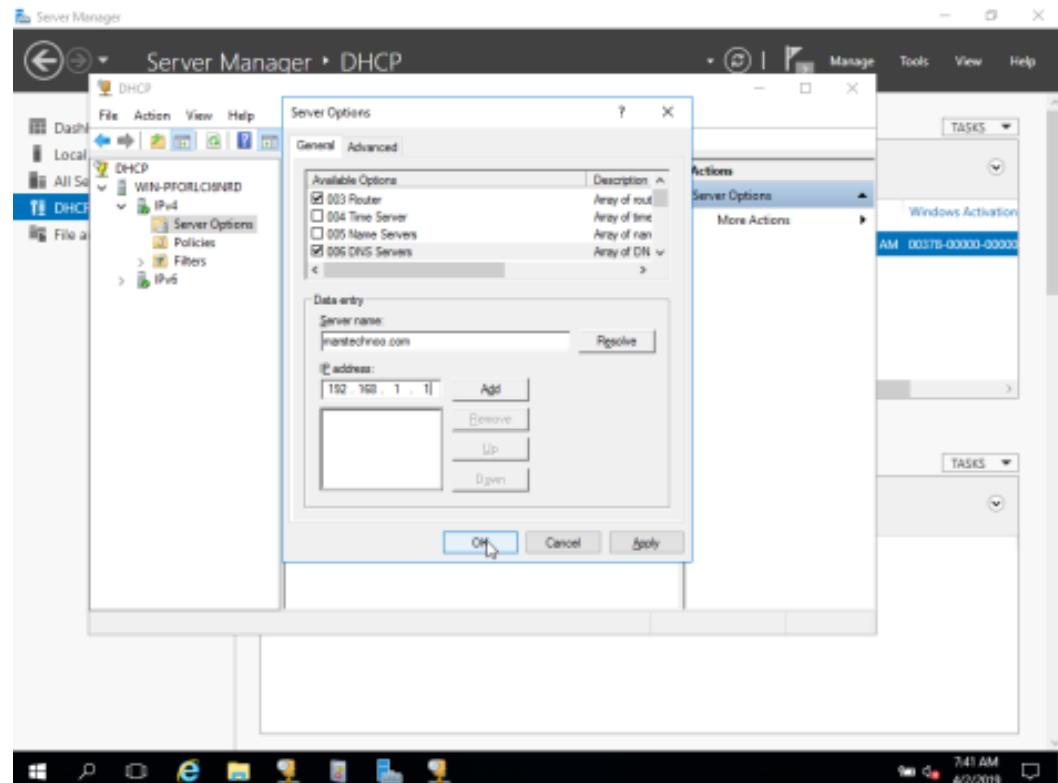
Gambar 8.100 server name

15. Centang 003 Router, dan ketikkan Router IP Address (karena saya menggunakan Jaringan NAT di dalam Virtualbox, alamat IP ini akan menjadi alamat IP gateway server) dan klik Add.



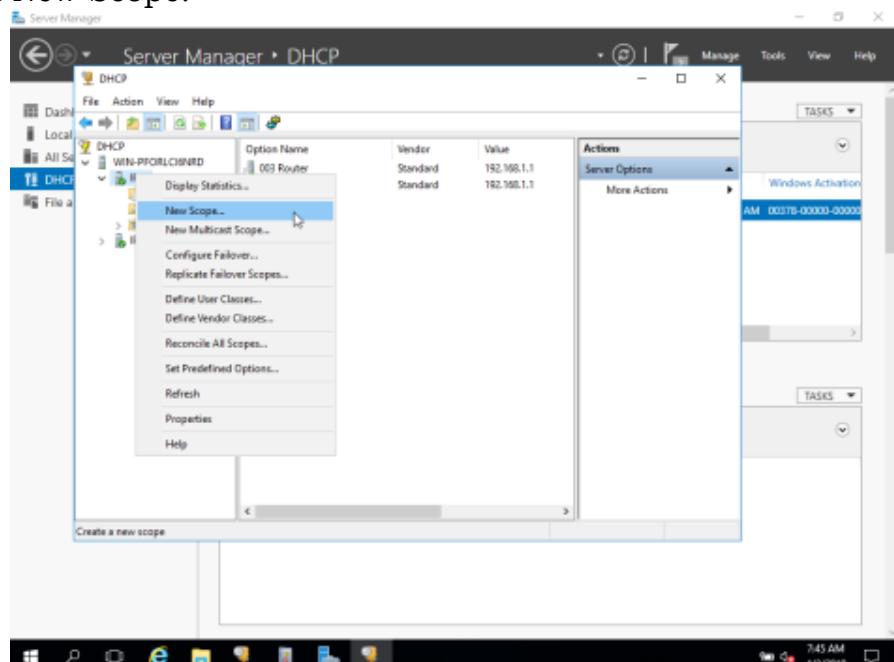
Gambar 8.101 Pemilihan Router 003

16. Centang DNS Server, dan ketik Server name yang telah diatur sebagai Domain dan juga alamat IP nya, klik Add, dan kemudian OK.



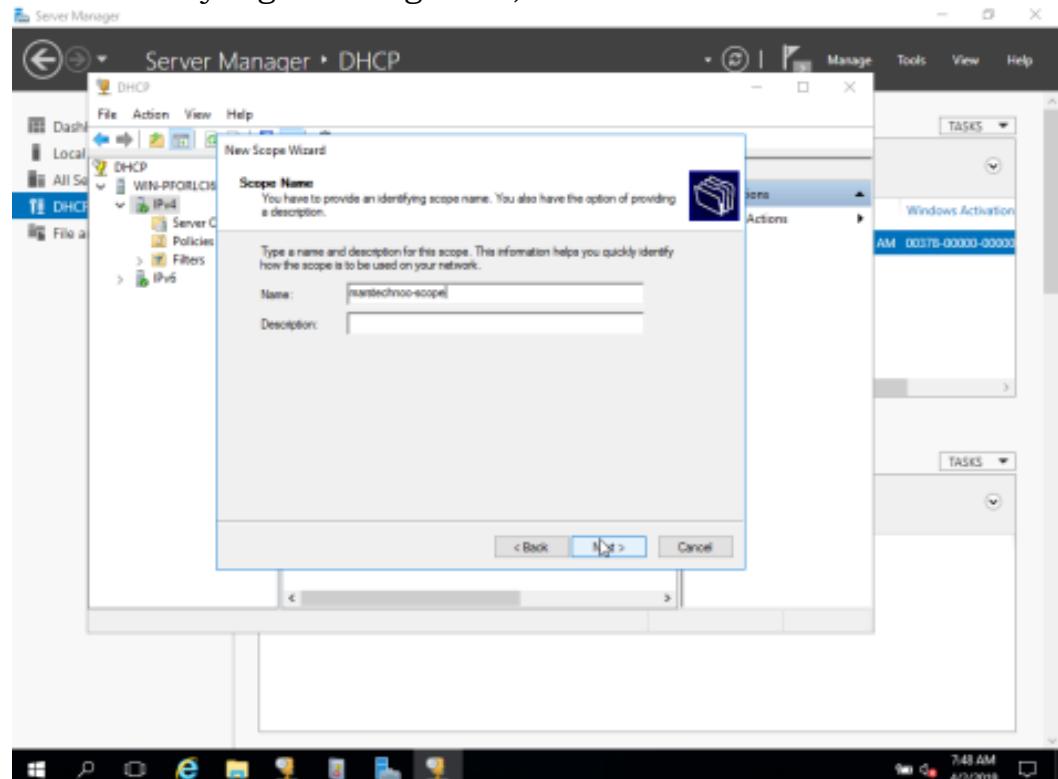
Gambar 8.102 DNS Server

17. Setelah selesai mengkonfig pengaturan IPnya, selanjutnya kita buat New Scope.



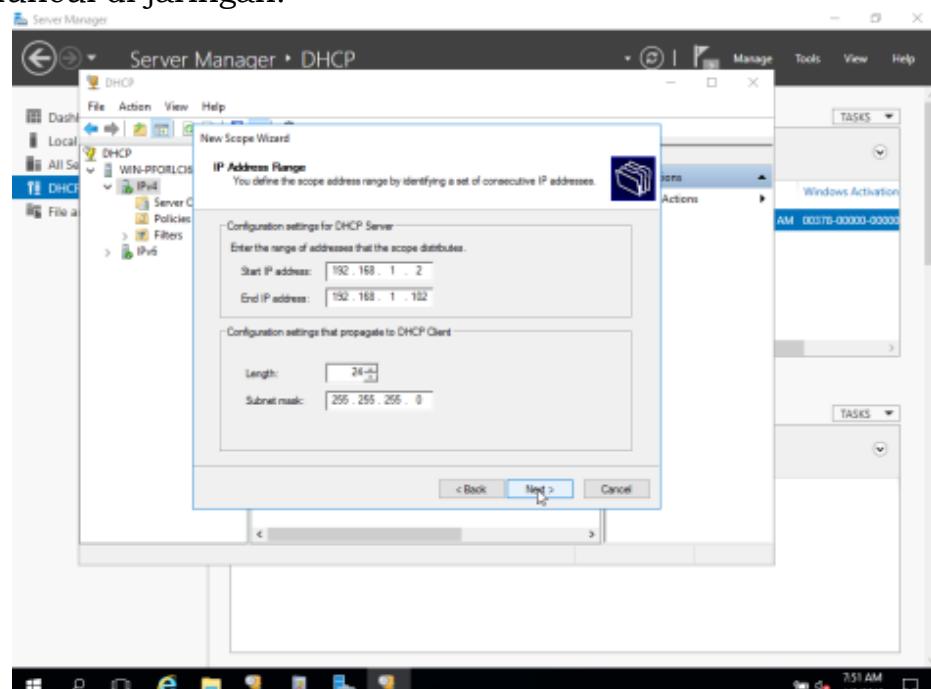
Gambar 8.103 pengaturan IP

18. Ketik Name yang anda inginkan, kemudian klik Next.



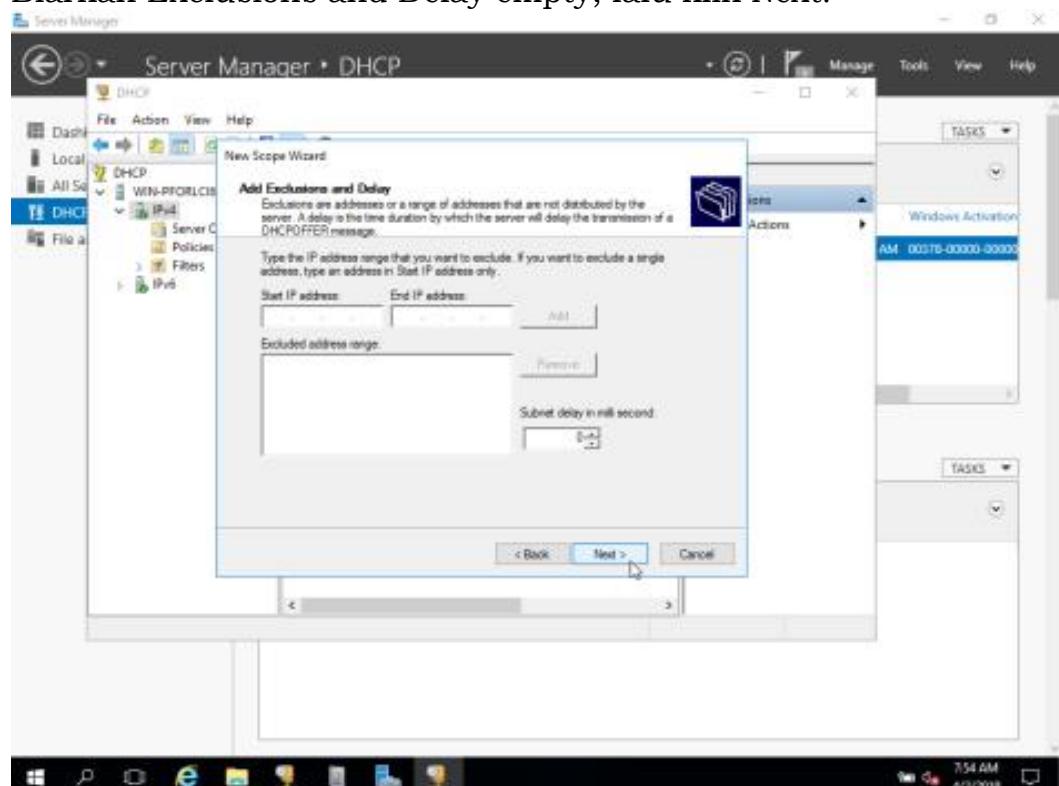
Gambar 8.104 memasukkan nama yang diinginkan

19. Kemudian masukkan Rentang/Range Alamat IP (mulai dan akhir) dan subnet mask yang sesuai, lalu klik **Next**. Rentang alamat IP yang akan dibagikan server kepada DHCP client ini yang akan muncul di jaringan.



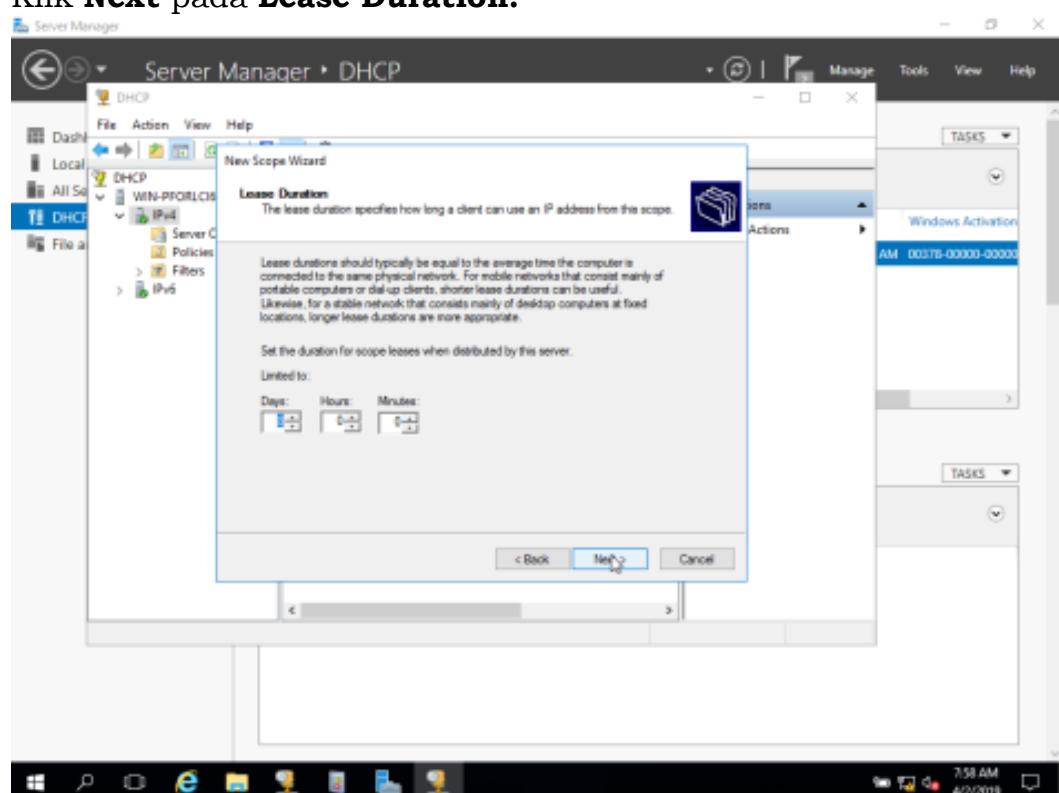
Gambar 8.105 memasukkan rentang/range alamat IP

20. Biarkan Exclusions and Delay empty, lalu klik Next.



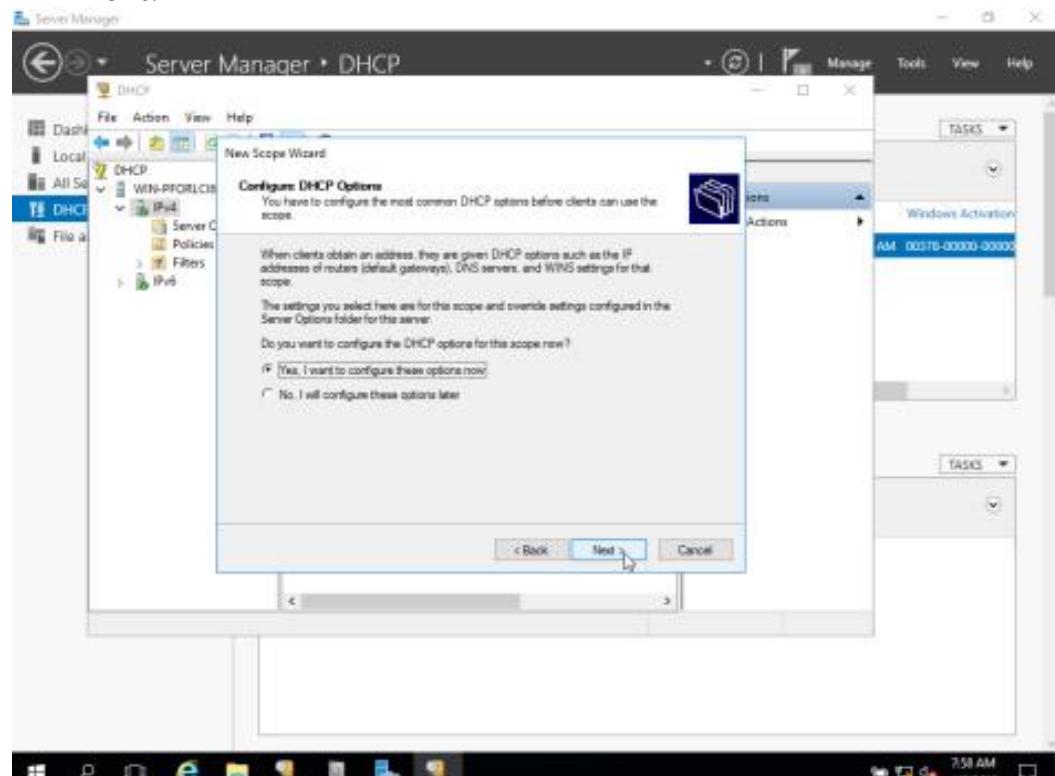
Gambar 8.106 exclusions and delay empty

21. Klik Next pada Lease Duration.



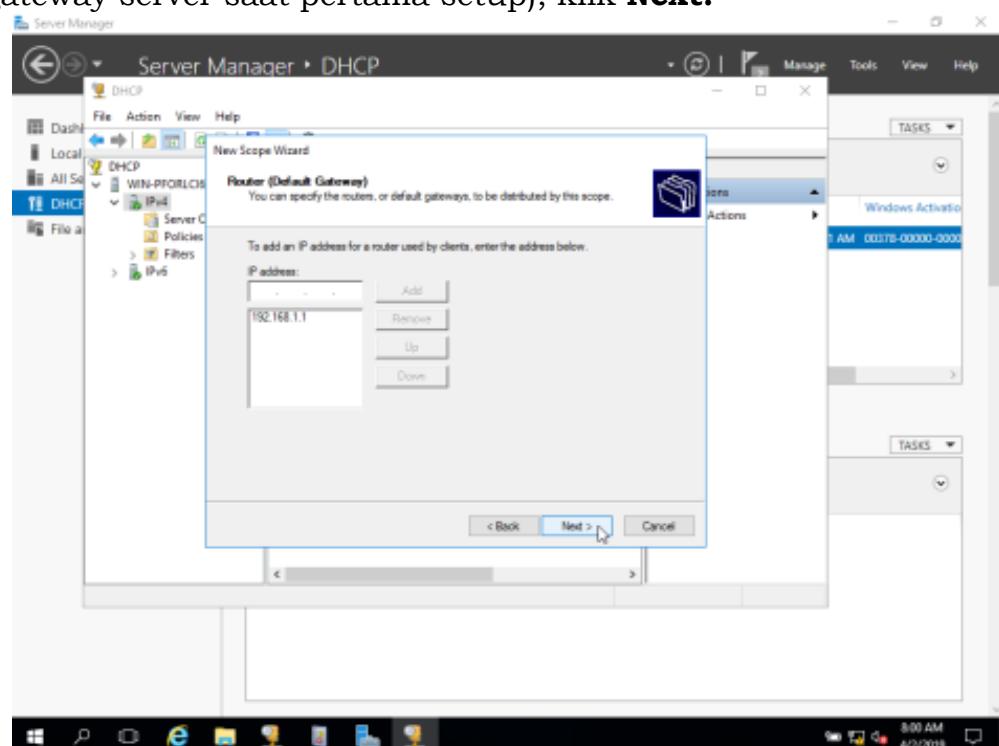
Gambar 8.107 lease duration

22. Pilih Yes, I want to configure these options now, kemudian klik Next.



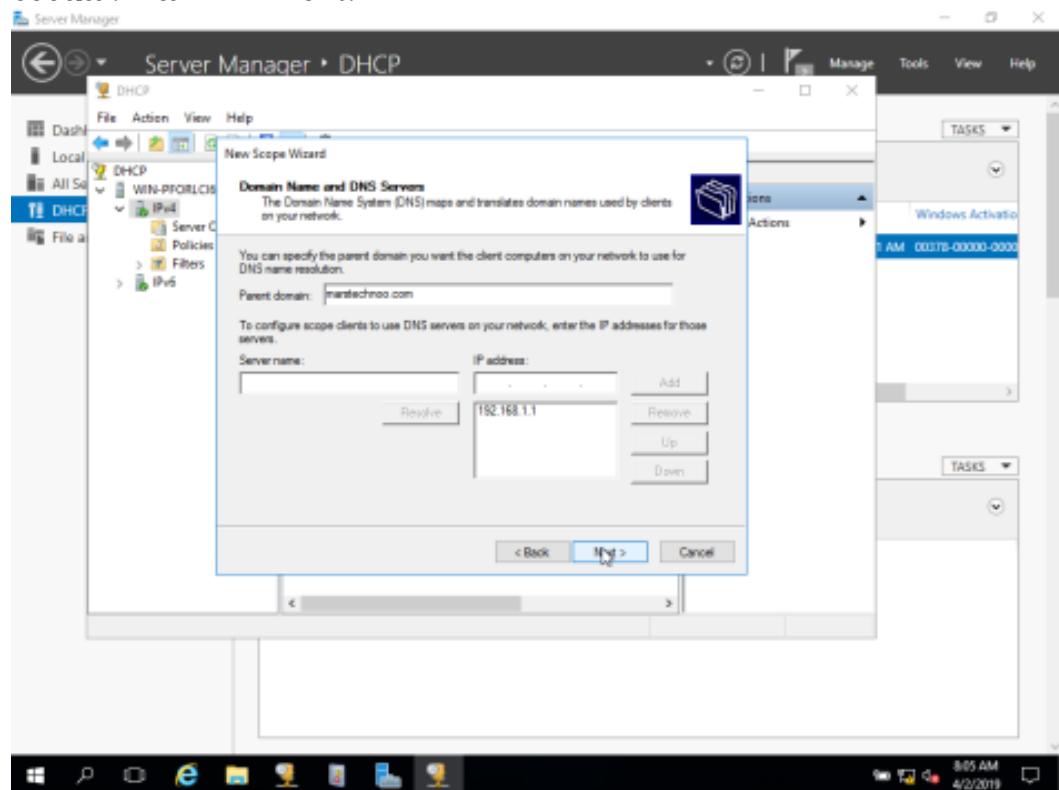
Gambar 8.108 memilih configuration

23. Ketikkan lagi alamat IP Router (ingat, ini sama dengan alamat gateway server saat pertama setup), klik **Next**.

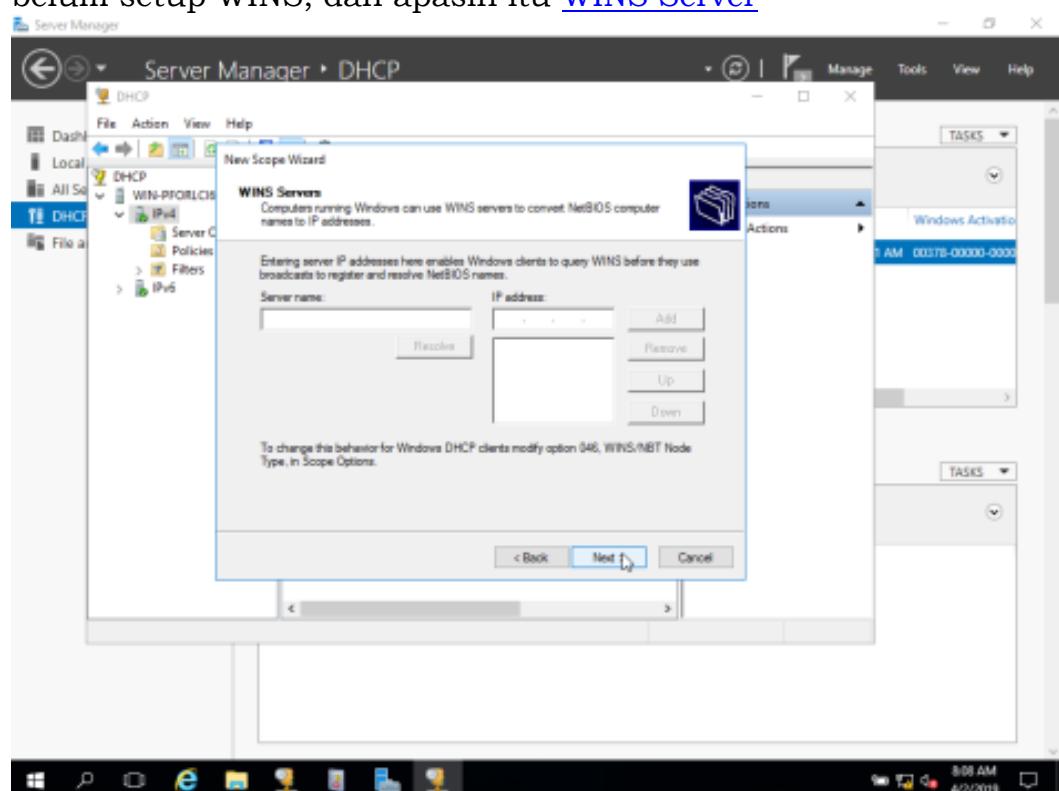


Gambar 8.109 alamat IP Router

24. Selanjutnya isi Parent Domain, dan pastikan alamat IP nya sudah sesuai. Dan klik Next.

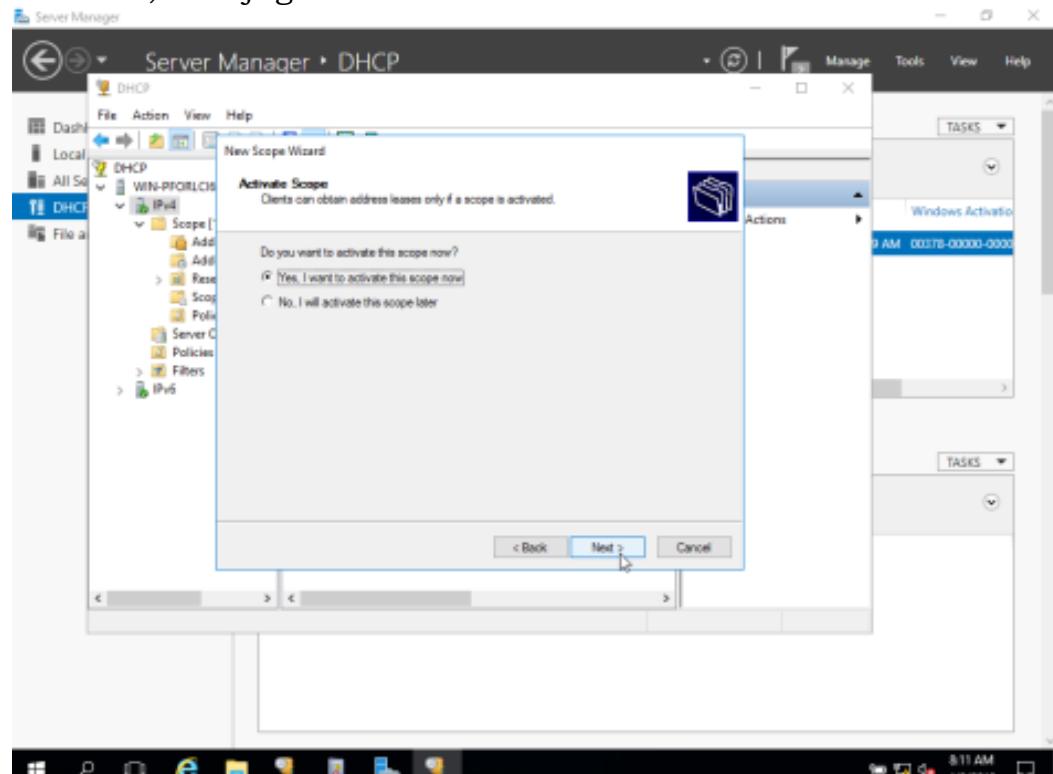


Langsung saja klik **Next**, kenapa? karena untuk saat ini kita belum setup WINS, dan apasih itu [WINS Server](#)



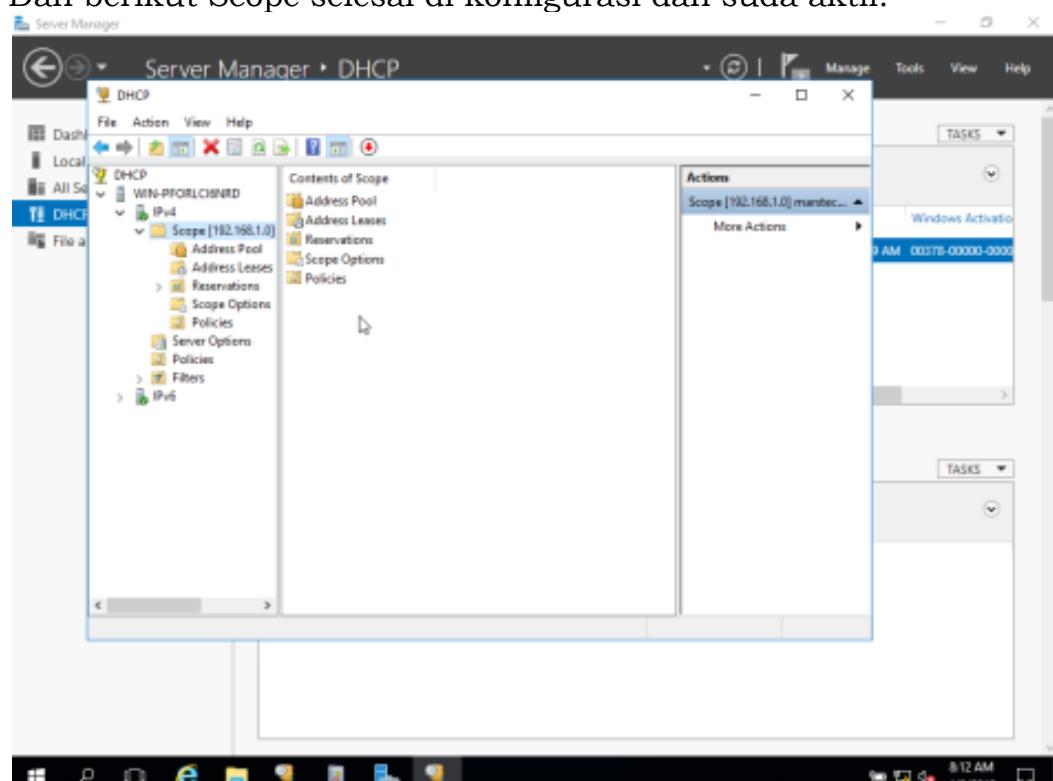
Gambar 8.110 parent domain

25. Pilih Yes, I want to activate this scope now, kemudian klik Next, Dan juga Finish.



Gambar 8.111 activate this scope

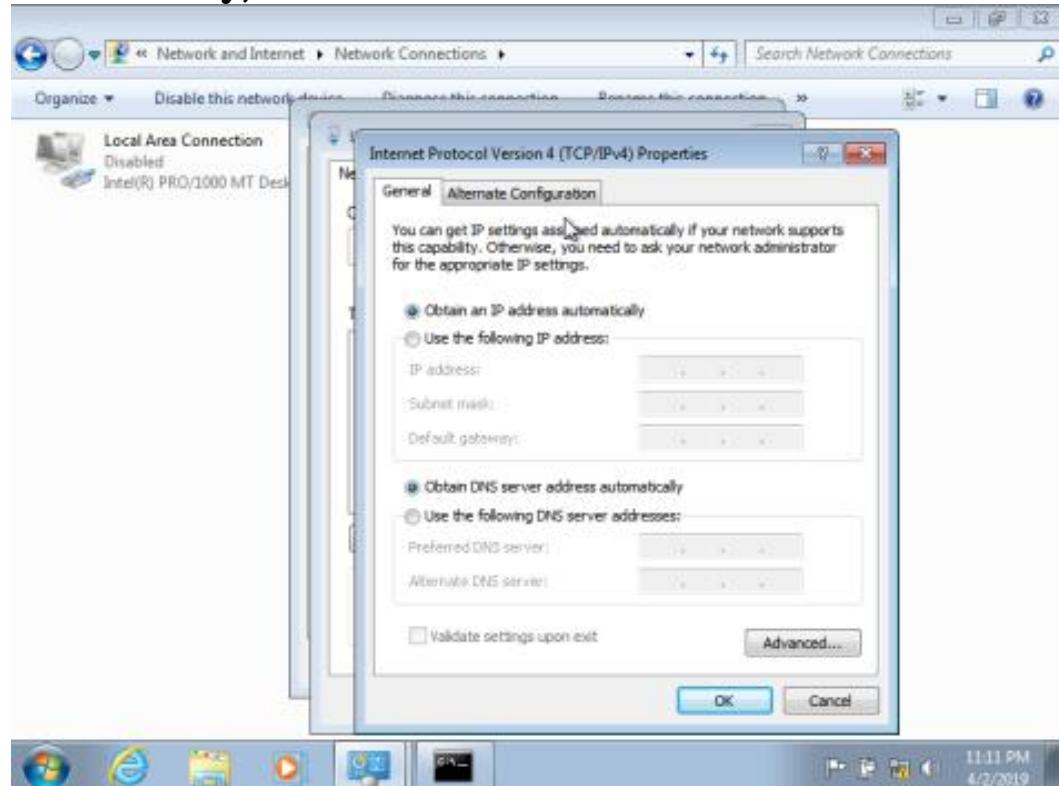
26. Dan berikut Scope selesai di konfigurasi dan suda aktif.



Gambar 8.112 finish scope installation

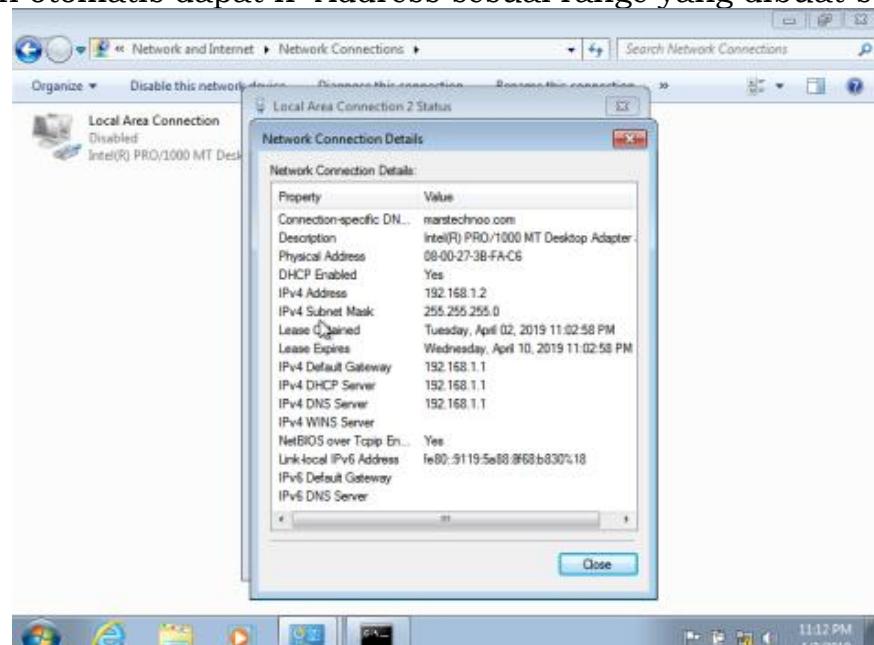
Konfigurasi pada Client Windows

1. Sekarang cek konfigurasi di sisi Client, dan disini saya menggunakan Client Windows 7 di Virtual Box juga. Ubah settingan TCP / IPv4 menjadi **Obtain an IP address automatically**, Klik **OK**.



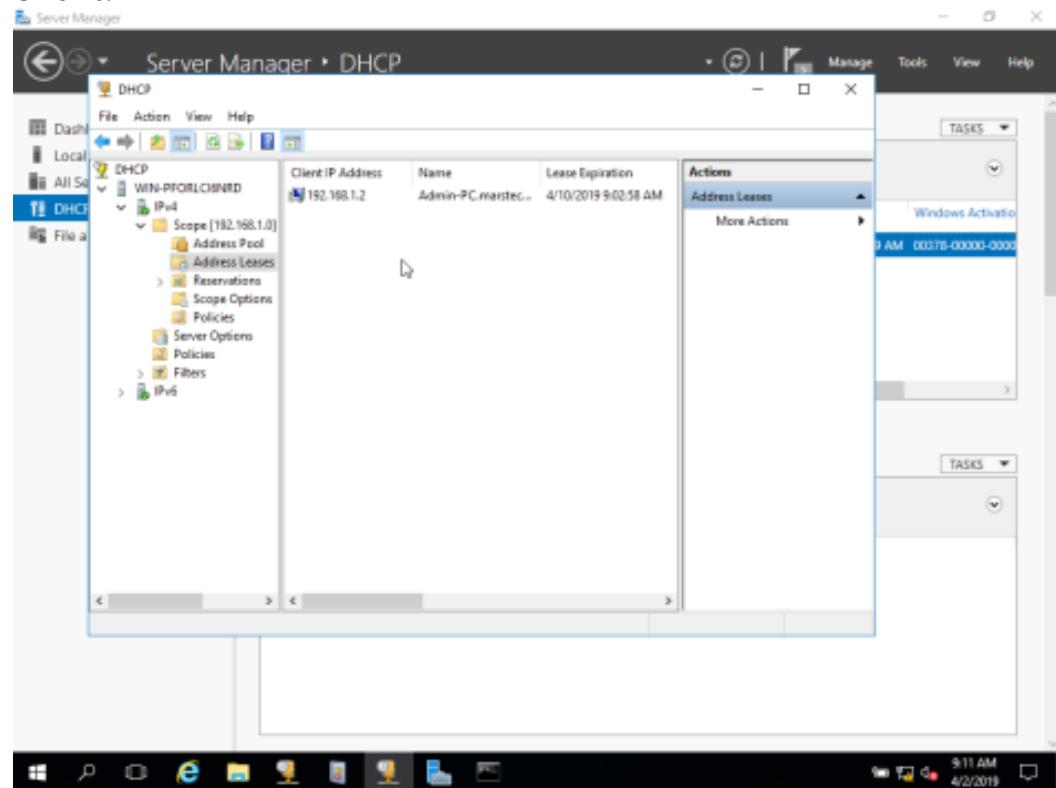
Gambar 8.113 setting TCP/IP di Client

2. Lalu lihat di sisi **Network Connection Details**, client windows sudah otomatis dapat IP Address sesuai range yang dibuat server.



Gambar 8.114 network connection details

3. Jika kita lihat di sisi Windows Server 2016, tepat di **Scope > Address Leases** terdapat IP Address yang sudah digunakan oleh Client.



Gambar 8.115 scope address leases

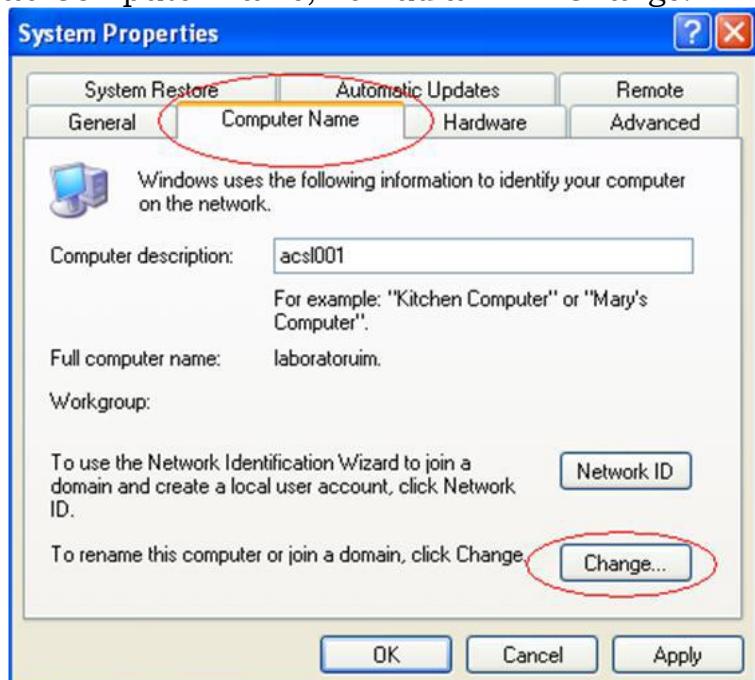
4. Kemudian kita coba test ICMP sisi Client apa dapat respond dari Server, dan ternyata success



Gambar 8.116 test ICMP sisi client

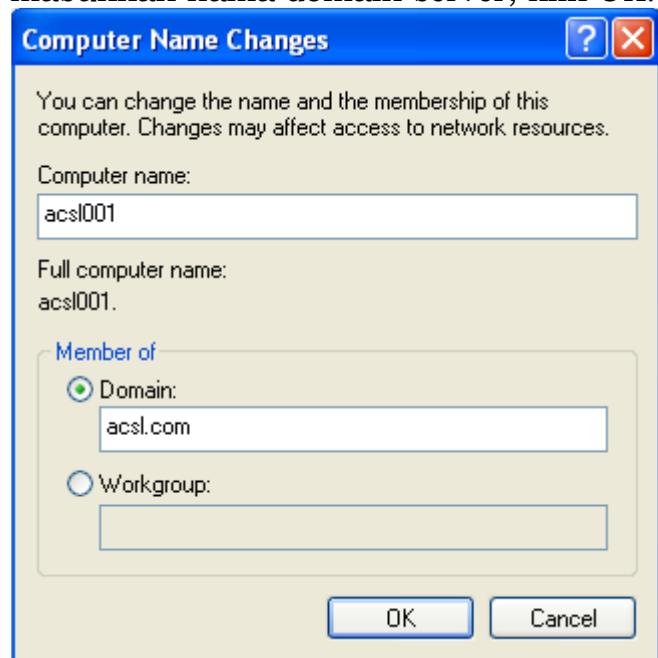
8.3.11. Menghubungkan Client dengan Komputer Server.

1. Pilih Start □ Setting □ Control Panel. Di dalam Control Panel pilih ikon System dan klik ganda pada ikon tersebut.
2. Pilih tab Computer Name, kemudian klik Change.



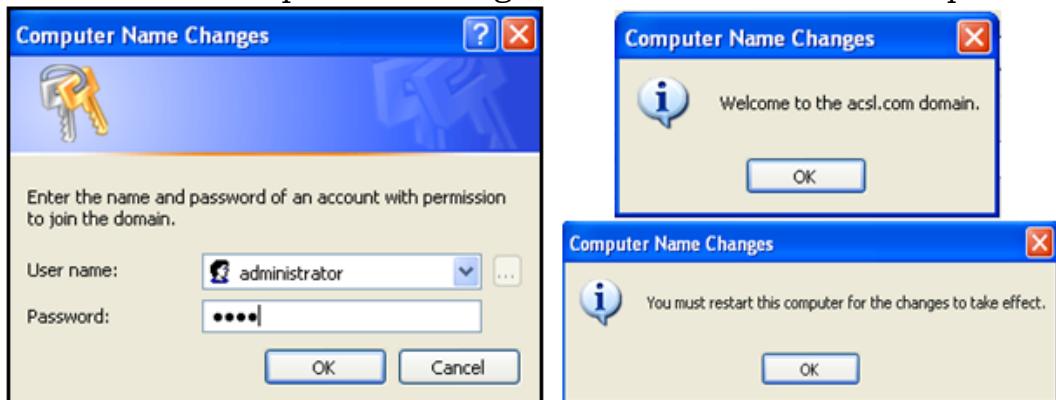
Gambar 8.117 Pemilihan Properties

3. Di dalam Tab Computer Name □ change terdapat dua pilihan, Domain dan Workgrup yang terdapat pada frame member of , pilih domain lalu masukkan nama domain server, klik OK.



Gambar 8.118 Memasukkan Computer Name & Domain

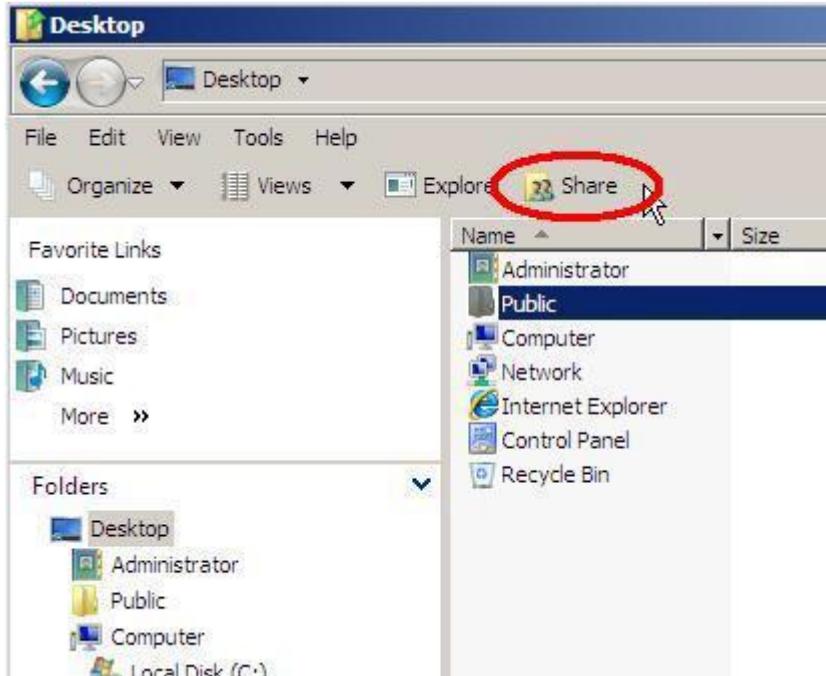
4. Kemudian masukkan username dan password administrator, klik OK. Jika username dan passwordnya valid maka tampil informasi bahwa nama computer telah diganti. Kemudian restart komputer.



Gambar 8.119 Tampilan Akhir

8.3.12. Membuat Sharing Folder

1. Dicontohkan folder public akan dishare, masuk ke direktori yang di dalamnya terdapat folder Public, seperti gambar. Kemudian pilih Share.



Gambar 8.120 Konfigurasi Sharing

2. Maka muncul jendela public properties, klik Advance Sharing dan centang share this folder, Dan OK. Semua folder yang berada di dalam Public otomatis dapat diakses oleh semua client.



Gambar 8.121 Public Properties

8.3.13. Membuka drive sharing.

1. Buka windows explore.
2. Pilih tools map network drive.



Gambar 8.122 Letak Map Network Drive

3. Maka tampil jendela Map Network Drive, pilih different user name.



Gambar 8.123 Tampilan Map Network Drive



4. Masukkan username dan password account client yang telah dibuat. Klik OK. Dan pilih folder yang dishare.



Gambar 8.124 Tampilan Otentikasi

8.4 Alat dan Bahan

1. Manual Book/Guide
2. PC dengan system operasi windows/linux
2. Kabel
3. Multi Tester
4. Router
5. Switch
6. Hub
7. Aplikasi Packet Tracer
8. Software virtualisasi (VMware)
9. Software Windows Server 2016/OSI

8.5 Praktikum

1. Simulasi Installasi Windows Server 2016 DiVirtualBox
2. Simulasi Instalasi dan Konfigurasi Active Directory Domain Service
3. Simulasi Konfigurasi pada client Windows
4. Simulasi Konfigurasi pada client Linux
5. Simulasi Active Directory User and Computer (Membuat User Account)
6. Simulasi Instalasi dan Konfigurasi DHCP Server
7. Simulasi Menghubungkan Client dengan Komputer Server
8. Simulasi Membuat Sharing Folder
9. Simulasi Membuka drive sharing



8.6 Referensi

1. Arief, A. (2015). "Analisa Keamanan Jaringan Wireless menggunakan Radius Server pada Mikrotik". Skripsi. Program Studi Teknik Informatika Universitas Gadjah Mada. Yogyakarta.
2. Behrouz A. (2003). Data Communications and Networking, Third Edition. McGraw-Hill. New York.
3. [3] Chaffey, D. (2011). E-Business and E-Commerce Management Strategy, Implementation and Practice 5th Edition. London: Prentice hall Financial Times.
4. Esabella, S. (2016). Perancangan Infrastruktur Jaringan Komputer Untuk Mendukung Implementasi Sistem Informasi Pada Universitas Teknologi Sumbawa, JurnalMatrik, vol. 16, no.1, pp. 1-2.
5. Gufron. (2013). Perbaikan Perangkat Komputer. Bung Hatta University Press. Padang.
6. Kurni, Asmunim. (2017) :Membangun Privileges Pada Jaringan Komputer SMA Negeri 2 Boyolali Berbasis Active Directory Dengan Windows Server 2016 Enterprise. Laporan Tugas Akhir. Jurusan Teknik Elektro. Surakarta :Universitas Muhammadiyah Surakarta.
7. Rainer Jr, R. Kelly & Casey G. Cegielski. (2013). Introduction to Information Systems- fourt edition. Singapore: John Wiley and Sons Singapore pte. ltd.
8. Sukaridhoto, Sritrusta. (2014). Jaringan Komputer, Edisi Pertama. Surabaya: Politeknik Elektronika Negeri Surabaya.
9. Uji Muryanto, Prasetyo. (2011). "Implementasi Sistem Wireless Security dan Bandwdith Berbasis Radius Server dengan Mikrotik". Skripsi. Jakarta: Jurusan Teknik Informatika Universitas Islam Negeri Syarif Hidayatullah.
10. <https://marstechnoo.wordpress.com/2019/04/11/konfigurasi-web-server-di-windows-server-2016/> diakses tanggal, 28 Januari 2021

8.7 Tugas

Tugas Kelompok

Kelompok terdiri dari 3 s.d 5 orang, kemudian lakukan pembagian tugas untuk mendemostrasikan studi kasus dibawah ini !

1. Cara Instalasi Windows Server 2016
2. Konfigurasi dasar untuk Windows Server 2016
3. Konfigurasi DHCP Server | Pada Windows Server 2016
4. Cara MengKonfigurasi DNS Server di Windows Server 2016
5. Konfigurasi Mail Server pada Windows Server 2016



8.8 Laporan

Laporan Praktikum terdiri dari (Cover, Kata Pengantar, Daftar Isi, PENUTUP (Simpulan dan Saran), DAFTAR PUSTAKA).

Format Penulisan Laporan :

1. Margin, Paper = A4
 - a. Top = 3 cm
 - b. Bottom = 3 cm
 - c. Left = 4 cm
 - d. Right = 3 cm
2. Font : Times New Roman
 - a. Judul MODUL = 14 pt, Bold
 - b. Sub Modul dan Paragraph = 12 pt
3. Page :
 - a. Cover = tanpa halaman
 - b. Kata Pengantar s/d sebelum MODUL I = Center Bottom, angka romawi kecil (i,ii,iii)
 - c. MODUL = Center Bottom, angka arab (1,2,3) d. Bagian MODUL = Top Right, angka arab (1,2,3)
4. Laporan dikumpulkan dalam 1 file (tanggal & waktu ditentukan kemudian).



STUDI KASUS (PROJECT MAHASISWA)

1. Studi Kasus I

Sebuah Koperasi ACSL ingin membuat suatu jaringan sederhana, peralatan jaringan yang tersedia sebuah Access Point Linksys 4 port, serta beberapa komputer yang digunakan sebagai server dan client. System operasi yang digunakan pada komputer server berupa windows server 2008 enterprise, serta system operasi dari computer client (Virtual Box) yakni windows xp. Gambarkan serta rancanglah jaringan tersebut dengan ketentuan :

5. SSID Access Point dengan nama "KOPERASI_ACSL", dengan key protection, serta dilakukan MAC filtering terhadap user yang hanya diijinkan terkoneksi ke Access Point.
6. Setiap client terdaftar sebagai user pada server serta dapat terkoneksi ke internet.
7. User1 bagian Keuangan membuat storage dari folder "Data_Keuangan" yang telah di share oleh server.
8. User2 bagian Barang membuat storage dari folder "Data_Barang" yang telah di share oleh server.
9. User3 bagian Keanggotaan membuat storage dari folder "Data_Anggota" yang telah di share oleh server.



2. Studi Kasus II

Perusahaan kontraktor alat-alat berat ingin membangun jaringan pada kantor cabangnya dengan mensegmentasi setiap bagian : Bagian Keuangan, HRD, serta Staff. Perlengkapan jaringan yang tersedia berupa Access Point serta Switch DLINK DES-3526. Seluruh perlengkapan jaringan ditempatkan di lantai 1. Bagian Keuangan dan HRD berada di lantai 1 yang terhubung pada jaringan melalui kabel, sedangkan bagian Staff berada di lantai 2 yang terhubung pada jaringan melalui Wireless. Setiap bagian tersebut dapat terkoneksi ke internet melalui modem router yang disediakan oleh ISP, namun antar bagian tidak dapat melakukan pengambilan file maupun data yang di-share oleh bagian tertentu. File dapat diambil / diprint pada setiap bagian hanya melalui file server. Seorang administrator memonitoring setiap computer client yang terhubung pada jaringan menggunakan The Dude dan mereMOTE komputer setiap client menggunakan Radmin. Gambarkan perancangan topologi jaringan serta implementasikan hasil perancangan tersebut dengan ketentuan :

- a. Port 5 pada switch untuk bagian keuangan dengan pembatasan bandwidth sebesar 1 Mbps.
- b. Port 7 pada switch untuk bagian HRD dengan pembatasan bandwidth sebesar 2Mbps.
- c. Port 9 pada switch untuk bagian Staff dengan pembatasan bandwidth sebesar 3 Mbps.
- d. Port 1 pada switch terkoneksi dengan modem router internet dari ISP.
- e. Port 3 pada switch terkoneksi dengan computer administrator sebagai monitoring serta konfigurasi setiap perangkat jaringan yang digunakan.
- f. SSID Access Point router “ACSL_KONTRAKTOR”, dengan key protection.

3. Studi Kasus III

Suatu Laboratorium Jaringan ingin melakukan uji coba terhadap beberapa perangkat jaringan seperti switch, AP Router, serta Router dalam mengkomunikasikan data melalui jaringan yang luas (internet). Uji coba tersebut diharapkan dari setiap PC client yang terhubung melalui Router maupun AP Router dapat terkoneksi dengan internet, gambarkan rancangan tersebut serta implementasikan dengan ketentuan :

- a. Port 1 switch terhubung dengan Modem internet dari ISP.
- b. Port 3 switch terhubung dengan router.
- c. Port 5 switch terhubung dengan AP Router.
- d. DHCP Router dikonfigurasikan secara dinamis dan statis.
- e. Client yang terhubung dengan AP Router dikonfigurasikan secara obtain dan manual.



4. Studi Kasus IV

Sebuah Perusahaan “Big ACSL” mendapatkan IP dari ISP 172.110.23.12/26 ingin membagi ke dalam 5 divisi di perusahaan tersebut. Kebutuhan computer dari masing-masing divisi :

- Divisi A = 14 Komputer
- Divisi B = 7 Komputer
- Divisi C = 5 Komputer Divisi
- D = 4 Komputer
- Divisi E = 12 Komputer

Sebagai seorang Network Administrator akan membagi dari Ip yang diterima oleh ISP tersebut menjadi beberapa bagian untuk mempermudah pengelolan dan mengoptimalkan efisiensi kerja jaringan sehingga jaringan tidak terpusat pada satu network. Bagaimana perhitungan pembagian network agar efisien dengan menampilkan hasil bentuk table yang terdiri atas Divisi (Subnet), Jumlah Komputer yang digunakan (Jumlah Host), Alokasi yang tersedia pada 1 network (Alokasi Ketersediaan), Address dari 1 Network tersebut (Address), Subnet Mask (Prefix & Desimal Bertitik), Range IP Address, serta Broadcast.

5. Studi Kasus V

1. Seorang pengusaha ingin menginvestasikan uangnya melalui usaha warnet yang memiliki cabang sebanyak 10 warnet. Setiap warnet tersedia 12 komputer.
2. Sebagai seorang administrator jaringan akan dilakukan pembagian IP Address dari warnet pusat 192.168.221.5 terhadap seluruh computer yang ada di setiap warnet.
3. Pembagian alamat jaringan tersebut dilakukan supaya mudah dalam pengelolaan serta mengoptimalkan kerja jaringan sehingga tidak memberatkan pada satu network.
4. Bagaimana administrator memperhitungkan pembagian alamat tersebut kepada setiap computer agar dapat terhubung dalam jaringan.
5. Tampilkan hasil perhitungan dalam bentuk table yang terdiri atas blok subnet, alamat jaringan (IP Address), Range dari IP Address, serta Broadcast (Analisa cabang dari warnet serta banyaknya computer dari setiap warnet untuk mendapatkan subnet mask).