TIM PENYUSUN

MODUL
JARINGAN KOMPUTER

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS NUSANTARA PGRI
KEDIRI

Lembar Pengesahan
Modul Praktikum Jaringan Komputer

Telah disetujui dan di sahkan sebagai Modul Jaringan Komputer
Tahun Akademik 2013/2014

Di sahkan Di : Kediri

Mengesahkan,
Kepala Program Studi
Teknik Informatika.

Ahmad Bagus Setiawan, S.T., M.M

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Kuasa, yang telah memberikan rahmat-Nya sehingga Modul Praktikum Jaringan Komputer untuk mahasiswa/i Jurusan Teknik Informatika Fakultas Teknik Universitas Nusantara PGRI Kediri ini dapat diselesaikan dengan sebaik-baiknya.

Modul praktikum ini dibuat sebagai pedoman dalam melakukan kegiatan praktikum Jaringan Komputer yang merupakan kegiatan penunjang mata kuliah jaringan komputer pada Jurusan Teknik Informatika Universitas Nusantara PGRI Kediri. Modul praktikum ini diharapkan dapat membantu mahasiswa/i dalam mempersiapkan dan melaksanakan praktikum dengan lebih baik, terarah, dan terencana. Pada setiap topik telah ditetapkan tujuan pelaksanaan praktikum dan semua kegiatan yang harus dilakukan oleh mahasiswa/i serta teori singkat untuk memperdalam pemahaman mahasiswa/i mengenai materi yang dibahas.

Penyusun menyakini bahwa dalam pembuatan Modul Praktikum Jaringan Komputer ini masih jauh dari sempurna. Oleh karena itu penyusun mengharapkan kritik dan saran yang membangun guna penyempurnaan modul praktikum ini dimasa yang akan datang.

Akhir kata, penyusun mengucapkan banyak terima kasih kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung.

Kediri, September 2013

Penyusun

DAFTAR ISI

BAB I
NETWORK TOPOLOGI AND EQUIPMENT

I. Tujuan

1. Mahasiswa mengenal dan mengetahui peralatan yang dibutuhkan untuk membuat suatu jaringan lokal (Local Area Network/LAN).
2. Mahasiswa mengerti dan mampu menyiapkan alat pembangun jaringan dan testing koneksi alat yang ada untuk membangun suatu jaringan.
3. Mahasiswa memahami topologi jaringan yang ada.
4. Mahasiswa mampu melakukan konfigurasi jaringan pada sistem operasi Linux
5. Mahasiswa mengerti perbedaan konfigurasi jaringan yang sifatnya sementara dan yang bersifat permanen
6. Mahasiswa mampu melakukan tes koneksi pada komputer

II. Peralatan Yang Dibutuhkan

1. Beberapa PC untuk konfigurasi jaringan
2. Hub/Switch
3. NIC yang tertancap pada setiap PC
4. Kabel jaringan secukupnya
5. Konektor RJ 45
6. Tang Crimper
7. Alat Testing koneksi kabel

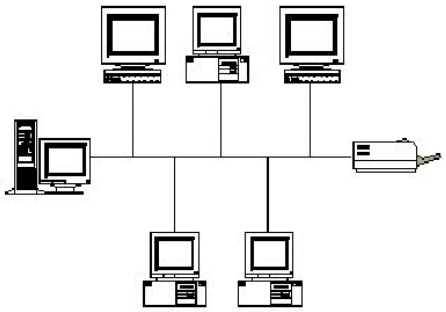
III. Dasar Teori

Jaringan komputer adalah kumpulan dua atau lebih dari komputer yang saling berhubungan satu sama lain. Produktifitas dan efisiensi merupakan bentuk keuntungan yang kita dapat dari jaringan komputer. Sebagai misal dengan adanya jaringan komputer memungkinkan pemakaian printer secara bersama-sama, memungkinkan pengkopian dile antar PC dsb.

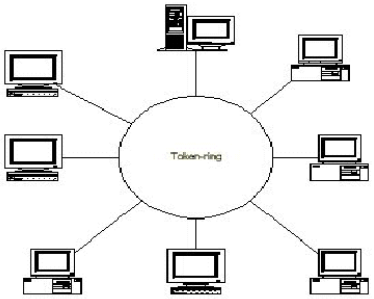
Arsitektur Fisik Jaringan

Arsitektur Fisik jaringan biasa disebut sebagai topologi, yang merupakan suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Yang saat ini banyak digunakan adalah *bus, token-ring, star dan peer-to-peer network.* Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri.

1. Topologi BUS
   Bentuk topologi BUS terlihat pada gambar di bawah ini :

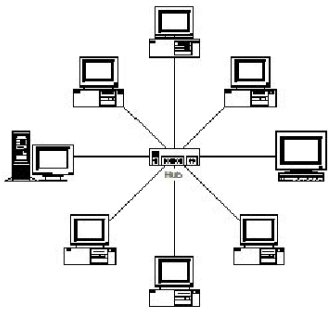


2. Topologi TokenRing
   Metode token-ring (sering disebut ring saja) adalah cara menghubungkan komputer sehingga berbentuk ring (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.
   Bentuk Topologi TokeRing terlihat pada gambar di bawah ini :



3. Topologi STAR
   Kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasium primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server.

   Bentuk Topologi Star terlihat pada gambar di bawah ini :



4. Topologi Peer To Peer
   Peer artinya rekan sekerja. *Peer-to-peer network* adalah jaringan komputer yang terdiri dari beberapa komputer (biasanya tidak lebih dari 10 komputer dengan 1-2 printer).

Dalam sistem jaringan ini yang diutamakan adalah penggunaan program, data dan printer secara bersama-sama.

Arsitektur Logik Jaringan

Arsitektur logik jaringan ada beberapa yang dikenal yaitu :

1. Arsitektur Ethernet
2. Arsitektur Token Ring
3. Arsitektur FDDI
4. Arsitektur ATM
5. ArsitekturArcNet

Perangkat Jaringan

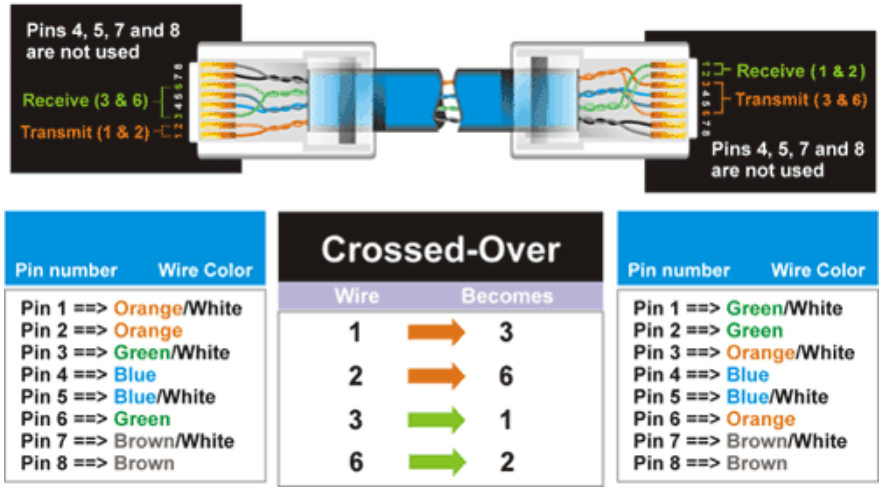
Supaya beberepa komputer saling terhubung, maka diperlukan perangkat yang menghubungkan 2 komputer atau lebih. Perangkat – perangkat tersebut adalah sbb :

1. Network Interface Carad (NIC)
   Merupakan suatu card yang ditanam di komputer yang berguna untuk menghubungkan dengan komputer lain.

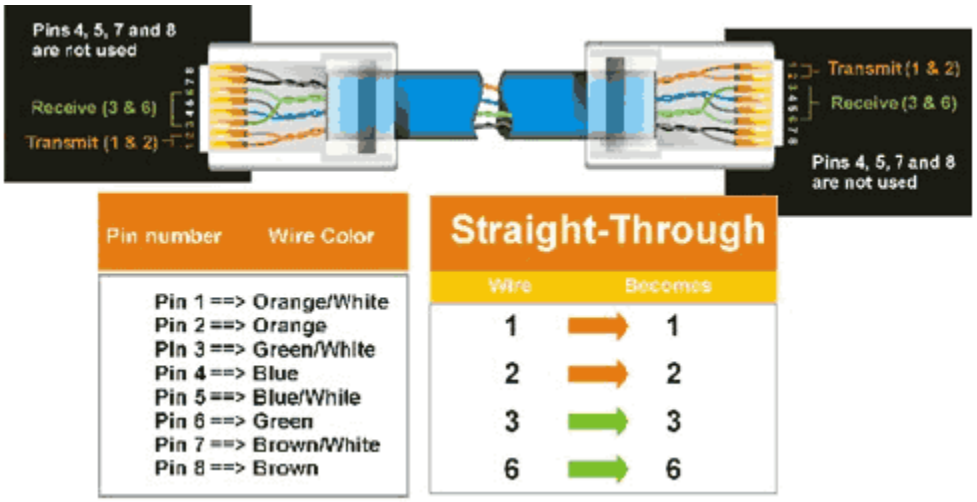
   Pada komputer biasanya ada slot(tempat menancap card) yang disebut expansion slot. Slot ini saat membeli komputer baru banyak yang kosong. Yang biasa terpasang adalah untuk menancapkan VGA Card untuk menghubungkan antara CPU dan monitor. Dan salah satu dari slot itu bisa dipakai untuk menancapkan NIC Card supaya bisa komputer kita bisa terhubung dengan jaringan. Kadang-kadang sekarang NIC Card sudah termasuk dalam fasilitas Motherboard kita (onboard)(sehingga kita tidak perlu lagi susah-susah memasangnya.
   Ada 2 tipe yaitu ISA dan PCI. Slot PCI lebih pendek dari ISA tapi meskipun lebih pendek mendukung kecepatan I/O yang lebih cepat.
   Dari sisi protokol, yang paling banyak dipakai adalah ethernet dan fast ethernet. Ada beberapa protokol lain, tapi kurang populer yaitu Token Ring, FDDI dan ATM (dua protokol terakhir dipakai untuk jaringan besar). Ethernet mendukung kecepatan transfer 10/100 Mbps bahkan ada yang sudah 1Giga bps.
   Untuk Laptop dikenal PCMCIA Card, mirip kartu kredit sedikit tebal.

2. Kabel
   Ada beberapa jenis kabel untuk jaringan :
   - UTP (Unshielded twisted pair)
     Kabel paling murah berbentuk mirip kabel telepon. Bentuk kabel UTP dan konektornya sbb :

Penampang untuk koneksi langsung 2 komputer (Peer To Peer) biasanya diberi nama cross cabel dgn penampang sbb :

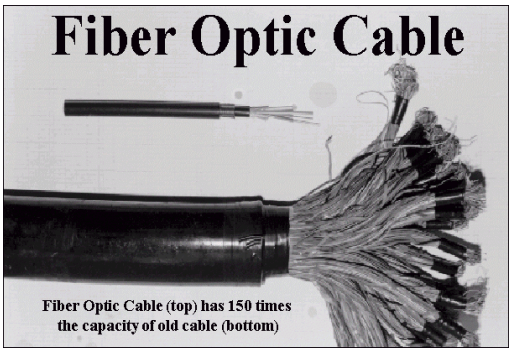


Dan untuk koneksi 2 buah komputer atau lebih dengan memakai sambungan hub/switch disebut sebagai straight kabel. Bentuk penampangnya adalah sbb :



- Coaxial
  Mirip dengan kabel televisi, dulu banyak digunakan, tapi sekarang jarang sekali digunakan.

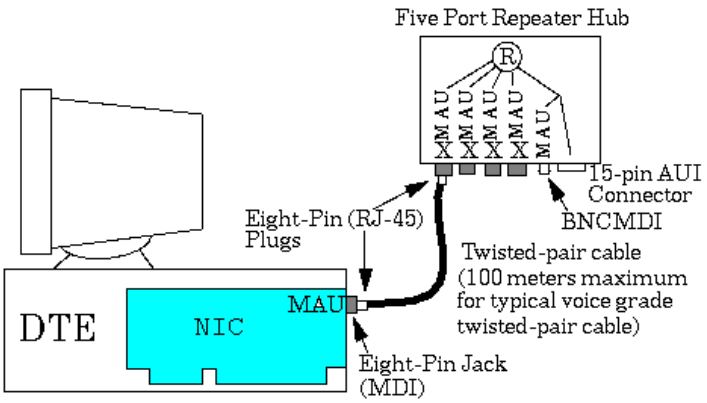
- Fiber Optik
  Kabel termahal, tapi mendukung kecepatan transfer terbagus.



Dalam memilih kabel disesuaikan dengan jenis NIC dan bentuk jaringan yang akan kita bentuk. Untuk UTP, portnya dikenal dengan nama RJ45.

3. Hub atau switch atau router
   Hub adalah perangkat penghubung. Pada jaringan bertopologi star, hub adalah perangkat dengan banyak port yang memungkinkan beberapa titik (dalam hal ini komputer yang sudah memasang NIC Card) bergabung menjadi satu jaringan dengan memakai kabel yang ada.

Contoh sederhana hubungan perangkat bisa dilihat pada gambar di bawah ini.

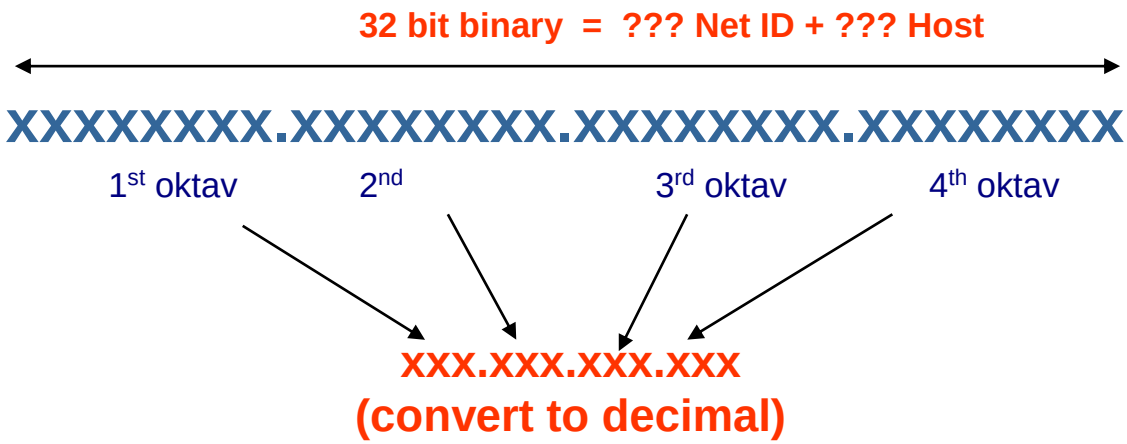


IP Address

Supaya komputer bisa terhubung dengan benar memerlukan adanya IP Address di setiap komputer.

IP Address terdiri dari bilangan biner sepanjang 32 bit yang dibagi atas 4 segmen. Tiap segmen terdiri atas 8 bit yang berarti memiliki nilai desimal dari 0 - 255. Range address yang bisa digunakan adalah dari 00000000.00000000.00000000.00000000 sampai dengan

11111111.11111111.11111111.11111111. Jadi, ada sebanyak 2^{32} kombinasi address yang bisa dipakai diseluruh dunia (walaupun pada kenyataannya ada sejumlah IP Address yang digunakan untuk keperluan khusus). Jadi, jaringan TCP/IP dengan 32 bit address ini mampu menampung sebanyak 2^{32} atau lebih dari 4 milyar host.

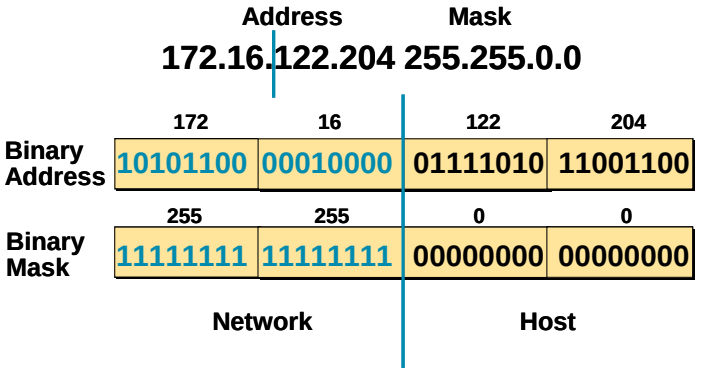


Konversi dari biner ke desimal

Untuk memudahkan pembacaan dan penulisan, IP Address biasanya direpresentasikan dalam bilangan desimal. Jadi, range address di atas dapat diubah menjadi address 0.0.0.0 sampai address 255.255.255.255. Nilai desimal dari IP Address inilah yang dikenal dalam pemakaian sehari-hari. Beberapa contoh IP Address adalah :

202.95.151.129
202.58.201.211
172.16.122.204

Ilustrasi IP Addres dalam desimal dan biner dapat dilihat pada gambar 1 berikut:



IP Address dalam Bilangan Desimal dan Biner

IP Address dapat dipisahkan menjadi 2 bagian, yakni :

1. Bagian network (bit-bit network/*network bit*) dan bagian host (bit-bit host/*host bit*). Bit network berperan dalam identifikasi suatu network dari network yang lain,
2. Bagian host, yang berperan dalam identifikasi host dalam suatu network. Jadi, seluruh ***host yang tersambung dalam jaringan yang sama memiliki bit network yang sama***.

Sebagian dari bit-bit bagian awal dari IP Address merupakan *network bit/network number*, sedangkan sisanya untuk host. ***Garis pemisah antara bagian network dan host tidak tetap, bergantung kepada kelas network***.

Ada 3 kelas address yang utama dalam TCP/IP, yakni :

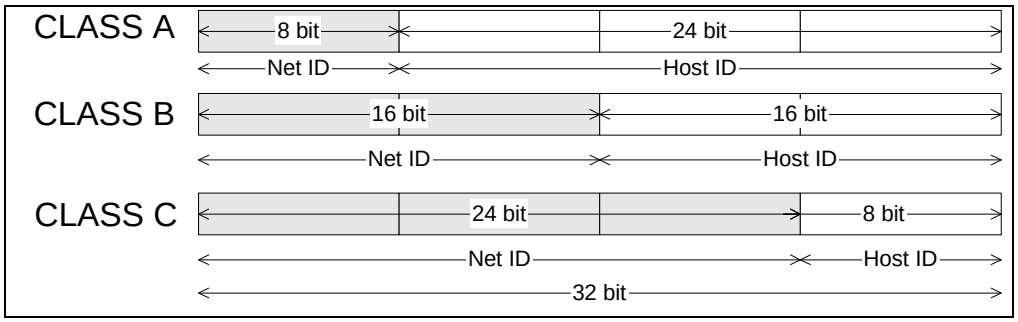
1. Kelas A
   8 bit pertama merupakan bit network sedangkan 24 bit terakhir merupakan bit host.

2. Kelas B
   16 bit pertama merupakan bit network sedangkan 16 bit terakhir merupakan bit host.

3. Kelas C

24 bit pertama) merupakan bit network sedangkan 8 bit terakhir merupakan bit host.

Secara garis besar berikut inilah pembagian kelas IP



Netmask

Selain NetID yang menentukan suatu jaringan dalam satu net(jaringan) adalah netmask.
Default netmask adalah sbb :

Class	Netmask	Jumlah Komputer (IP) dalam range
A	255.0.0.0	16.777.216
B	255.255.0.0	65.536
C	255.255.255.0	256

Ketika kita berhubungan dengan komputer lain pada suatu jaringan, selain IP yang dibutuhkan adalah netmask. Misal kita pada IP 10.252.102.12 ingin berkirim data pada 10.252.102.135 bagaimana komputer kita memutuskan apakah ia berada pada satu jaringan atau lain jaringan? Maka yang dilakukan adalah mengecek dulu netmask komputer kita karena kombinasi IP dan netmask menentukan range jaringan kita.
Jika netmask kita 255.255.255.0 maka range terdiri dari atas semua IP yang memiliki 3 byte pertama yang sama. Misal jika IP kita 10.252.102.12 dan netmask saya 255.255.255.0 maka range jaringan kita adalah **10.252.102**.0-**10.252.102**.255 sehingga kita bisa secara langsung berkomunukasi pada mesin yang diantara itu jadi **10.252.102**.135 berada pada jaringan yang sama yaitu **10.252.102** (lihat yang angka-angka tercetak tebal menunjukkan dalam satu jaringan karena semua sama).

Selain ke tiga kelas di atas, ada 2 kelas lagi yang ditujukan untuk pemakaian khusus, yakni kelas D dan kelas E. Jika 4 bit pertama adalah 1110, IP Address merupakan **kelas D** yang digunakan untuk **multicast address**, yakni sejumlah komputer yang memakai bersama suatu aplikasi (bedakan dengan pengertian network address yang mengacu kepada sejumlah komputer yang memakai bersama suatu network). Salah satu penggunaan multicast address

yang sedang berkembang saat ini di Internet adalah untuk aplikasi real-time video conference yang melibatkan lebih dari dua host (multipoint), menggunakan **Multicast Backbone (MBone).** Kelas terakhir adalah **kelas E** (4 bit pertama adalah 1111 atau sisa dari seluruh kelas). Pemakaiannya dicadangkan untuk kegiatan eksperimental.

Jenis kelas address yang diberikan oleh kooordinator IP Address bergantung kepada kebutuhan instansi yang meminta, yakni jumlah host yang akan diintegrasikan dalam network dan rencana pengembangan untuk beberapa tahun mendatang. Untuk perusahaan, kantor pemerintah atau universitas besar yang memiliki puluhan ribu komputer dan sangat berpotensi untuk tumbuh menjadi jutaan komputer, koordinator IP Address akan mempertimbangkan untuk memberikan kelas A. Contoh IP Address kelas A yang dipakai di Internet adalah untuk amatir paket radio seluruh dunia, mendapat IP nomor 44.xxx.xxx.xxx. Untuk kelas B, contohnya adalah nomor 167.205.xxx.xxx yang dialokasikan untuk ITB dan jaringan yang terkait ke ITB dibawah koordinator Onno W. Purbo.

Address Khusus

Selain address yang dipergunakan untuk pengenal host, ada beberapa jenis address yang digunakan untuk keperluan khusus dan tidak boleh digunakan untuk pengenal host. Address tersebut adalah :

Broadcast Address. Address ini digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh host yang ada pada suatu network. Seperti diketahui, setiap paket IP memiliki *header* alamat tujuan berupa IP Address dari host yang akan dituju oleh paket tersebut. Dengan adanya alamat ini, maka hanya host tujuan saja yang memproses paket tersebut, sedangkan host lain akan mengabaikannya. Bagaimana jika suatu host ingin mengirim paket kepada seluruh host yang ada pada networknya ? Tidak efisien jika ia harus membuat replikasi paket sebanyak jumlah host tujuan. Pemakaian bandwidth akan meningkat dan beban kerja host pengirim bertambah, padahal isi paket-paket tersebut sama. Oleh karena itu, dibuat konsep broadcast address. Host cukup mengirim ke alamat broadcast, maka seluruh host yang ada pada network akan menerima paket tersebut. Konsekuensinya, seluruh host pada network yang sama harus memiliki address broadcast yang sama dan address tersebut tidak boleh digunakan sebagai IP Address untuk host tertentu. Jadi, sebenarnya setiap host memiliki 2 address untuk menerima paket : pertama adalah IP Addressnya yang bersifat unik dan kedua adalah broadcast address pada network tempat host tersebut berada. Address broadcast diperoleh dengan membuat seluruh bit host pada IP Address menjadi 1. Jadi, untuk host dengan IP address 167.205.9.35 atau 167.205.240.2, broadcast addressnya adalah 167.205.255.255 (2 segmen terakhir dari IP Address tersebut dibuat berharga 11111111.11111111, sehingga secara desimal terbaca 255.255). Jenis informasi yang dibroadcast biasanya adalah **informasi routing.**

Perintah – Perintah Baru

perintah untuk mengecek ethernet card

```
[root@WSC204-11 root]# dmesg | grep eth
```

perintah untuk melakukan konfigurasi jaringan secara manual

```
[root@WSC204-11 root]# ifconfig eth0 10.252.105.111 netmask 255.255.255.0 up
```

perintah untuk mengecek hasil konfigurasi jaringan

[root@WSC204-11 root]# ifconfig

perintah untuk mengecek koneksifitas dengan komputer lain

[root@WSC204-11 root]# ping 10.252.105.110

perintah untuk melihat isi cache ARP(memetakan IP Address ke MAC Address)

[root@WSC204-11 root]# arp –a

perintah untuk menambahkan informasi gateway

[root@WSC204-11 root]# route add default gw 10.252.105.1

perintah untuk melakukan konfigurasi jaringan secara permanen

[root@WSC204-11 root]# netconfig

IV. Tugas Pendahuluan

1. Gambar diagram penampang kabel straight kabel dan cross kabel
2. Jelaskan pembagian kelas address di dalam TCP/IP
3. Apa yang dimaksud dengan Network Address, Broadcast Address dan Netmask, jelaskan secara singkat.
4. Apakah kegunaan perintah *dmesg* dan *grep* di linux dan bagaimana sintax secara lengkapnya di linux
5. Apa kegunaan perintah ifconfig di linux dan bagaiman sintaxnya secara lengkap
6. Apa kegunaan perintah ping di linux dan bagaimana sintaxnya secara lengkap

V. Percobaan

1. Dengan memakai peralatan yang ada buatlah kabel UTP dengan bentuk penampang straight cable dan cross cable, selanjutnya lakukan pengetesan koneksi terhadap kabel yang anda buat
2. Hubungkan peralatan hub/switch, kabel dan CPU sehingga membentuk suatu jaringan STAR.
3. Untuk sebagian yang lain hubungkan 2 komputer dengan memakai topologi Peer To Peer
4. Lakukan setting jaringan di bawah ini.
   a. Masuklah ke sistem komputer yang memiliki sistem operasi Linux
   b. Login sebagai root
   c. Buka terminal dengan mengklik pada Start Menu -> System Tools -> terminal
   d. Ceklah ethernet card yang ada pada komputer anda dengan megetikkan perintah
      [root@WSC204-11 root]# dmesg | grep eth
      Analisa hasilnya.
   e. Lakukan konfigurasi jaringan secara manual dengan menggunakan perintah *ifconfig*
      [root@WSC204-11 root]# ifconfig eth0 10.252.105.111 netmask 255.255.255.0 up

   f. Setelah melakukan konfigurasi untuk melihat hasilnya ketikkan perintah di bawah dan lihat pesan yang keluar
      [root@WSC204-11 root]# ifconfig

   Analisa hasilnya

5. Selanjutnya lakukan tes konektifitas dengan menggunakan perintah *ping no_address* dengan komputer lain yang berada pada 1 jaringan.
   Untuk menghentikan tekan Ctrl + C dan Analisa Hasilnya.
   Analisa hasilnya.

6. Lakukan lagi cek koneksifitas tetapi kali ini lakukan dengan komputer lain yang berbeda subnet
   Apa maksud pesan yang timbul ?
   Untuk menghentikan tekan Ctrl + C dan Analisa Hasilnya.
7. Tambahkan informasi gateway dengan mengetikkan perintah di bawah ini
   [root@WSC204-11 root]# route add default gw 10.252.105.1
8. Lakukan lagi cek koneksifitas tetapi kali ini lakukan dengan komputer lain yang berbeda subnet
   Untuk menghentikan tekan Ctrl + C dan Analisa Hasilnya.
   Bagaimana hasilnya ?
9. Lakukan pengubahan konfigurasi jaringan secara permanen dengan menggunakan perintah *netconfig*
   [root@WSC204-25 root]# netconfig
   mengubah setting jaringan secara permanen dengan menngunakan netconfig
   maka akan ditanyakan

   Apakah Anda benar ingin mengubah setting jaringan?
   Jika ya, maka isikan :
   IP Address : 10.252.105.111
   Netmask : 255.255.255.0
   Gateway : 10.252.105.1
   Primary name server : 202.154.59.178

   Setelah selesai mengisi pilih OK
10. File – file yang diupdate pada waktu pengubahan konfigurasi jaringan secara permanen adalah
    etc/sysconfig/networking/devices/ifcfg-eth0
    etc/sysconfig/networking/profiles/default/ifcfg-eth0
    etc/sysconfig/network-scripts/ifcfg-eth0
    *File yang diupdate IP Address, Netmask dan Gateway

11. Hasil konfigurasi jaringan secara permanen tidak dapat dilihat secara langsung tetapi harus diadakan *restart* terlebih dahulu
    [root@WSC204-11 root]# service network restart
    Shutting down interface eth0: [OK]
    Shutting down loopback interface: [OK]
    Setting network parameters: [OK]
    Bringing up loopback interface: [OK]
    Bringing up interface eth0: [OK]
12. Melihat konfigurasi jaringan hasil dari pengubahan secara permanen
    [root@WSC204-11 root]# ifconfig

VI. Laporan Resmi

1. Tulis hasil percobaan dan analisa hasilnya.

BAB II
PING, ARP, RARP, TCPDUMP DAN ETHEREAL

I. Tujuan

1. Mahasiswa mengenal ARP dan RARP
2. Mahasiswa mampu menganalisa mapping IP memakai ARP
3. Mahasiswa mampu mengcapture permintaan packet ARP memakai Tcpdump dan ethereal.

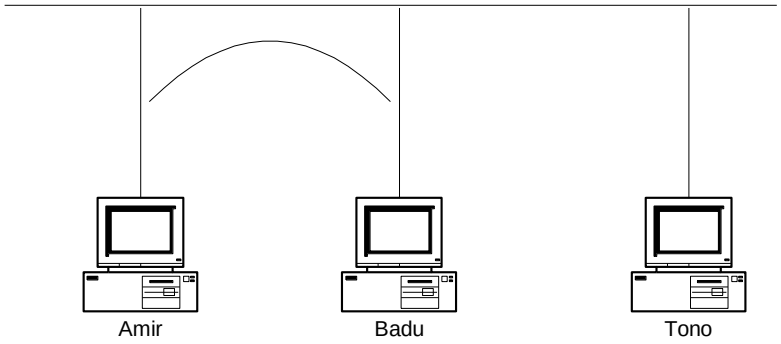
II. Peralatan Yang Dibutuhkan

a. Beberapa PC yang akan dihubungkan secara serial
b. Kabel Serial secukupnya

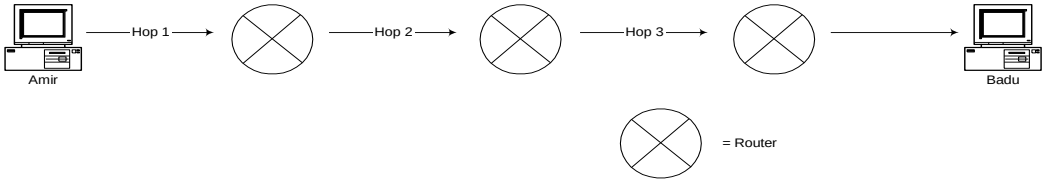
III. Dasar Teori

IP Addreass adalah 32 bit address yang diperlukan oleh software untuk mengidentifikasi host pada jaringan, namun nomor identitas yang sebenarnya adalah diatur oleh NIC (Network Interface Card)/Card Jaringan yang juga mempunyai address tunggal.
Ethernet address terdiri atas 48 bit, 24 bit ID dari pabrik pembuat sedangkan 24 bit sisanya adalah nomor urut/sequence number. Oleh karena itu setiap Ethernet Card (nama lain NIC Card) selalu mempunyai address tunggal yang berlaku untuk seluruh dunia.

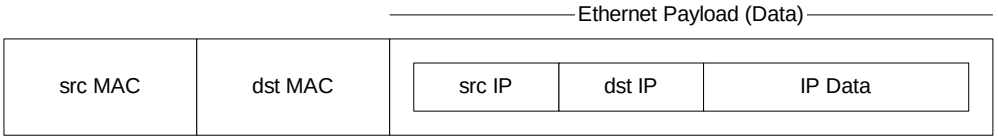
Pada dasarnya untuk komunikasi terjadi antara dua komputer. Misal Amir berkomunikasi dengan Badu dalam satu jaringan, bisa digambar sbb :



Jika terjadi komunikasi antara Amir dan Badu di internet, maka paket berjalan melompat dari satu jaringan dengan jaringan yang lain sampai tujuan. Penghubung antara satu jaringan dengan jaringan yang lain disebut sebagai router. Jadi bisa saja dari Amir ke Router, dari router ke router, dan akhirnya dari router ke Badu. Tapi secara garis besar bisa dianggap komunikasi tetap antara dua komputer (bisa komp-komp, komp-router, router-router)



TCP/IP merupakan standar software yang menentukan apa yang harus dilakukan oleh suatu bagian dari software jaringan pada sebuah mesin untuk dapat berkomunikasi dengan software jaringan pada mesin yang lain. Agar dapat bekerja maka TCP/IP membutuhkan hardware jaringan dalam hal ini adalah Ethernet meskipun ethernet bukan bagian dari TCP/IP, TCP/IP hanya berinteraksi untuk menggunakan fasilitasnya menggerakkan paket. Pengalamatan ethernet sudah dijelaskan di atas.
Untuk mengirim data ke komputer lain, maka software menyusun paket ethernet dalam memori sbb :



jadi referensi IP ke MAC addressnya shg data terkirim ke komputer yang benar sesuai phisical addressnya. Berdasarkan mapping IP dengan phisical addressnya.
Dalam hal ini mungkin Amir tahu nomor IP Badu tapi tidak tahu MACnya. TCP/IP memecahkan masalah ini dengan menggunakan ARP (Address Resolution Protocol) .

ARP
Secara internal ARP melakukan resolusi address tersebut dan ARP berhubungan langsung dengan Data Link Layer. ARP mengolah sebuah tabel yang berisi IP-address dan Ethernet Card. Dan tabel ini diisi setelah ARP melakukan request (broadcast) ke seluruh jaringan.

Misal user host tertentu menjalankan command ping dengan host foghorn ($telnet foghorn) . Setelah user menjalankan command telnet, maka sistem akan mengecek ARP cache untuk menentukan phisical addres yang dimaksud. Jika informasi ini adalah tidak ditemukan, kemudian host akan mengeluarkan suatu ARP khusus meminta paket. ARP Request dikapsulkan dengan semua informasi yang dibutuhkan kecuali physical addrees tujuan karena memang host tidak tahu tujuannya dimana. Untuk phisical address host akan broadcast ke jaringan, karena broadcast maka semua system pada local network akan menguji resuest tersebut. Paket ARP request/Reply mempunyai format yang sama. Informasi ini bisa ditangkap oleh *software sniffer ethereal*.

ARP Cache
Tadi sedikit disinggung, bahwa setelah menjalankan command ping maka host akan mengecek ARP Cache. ARP cache bisa dikatakan sebagai tabel IP dan host serta phisical adrees komputer. ARP cache akan bertambah jika ARP Request mendapat jawaban. ARP Cache ini diatur secara dinamik oleh kernel. Untuk melihat bisa pakai command arp –a.
Manipulasi ARP Cache
Kita bisa melakukan penghapusan sebuah entry ARP dengan arp –d hostname

RARP
RARP digunakan oleh komputer yang tidak mempunyai nomor IP. Pada saat komputer dihidupkan (power on) maka komputer melakukan broadcast ke jaringan untuk menanyakan apakah ada server (DHCP Server) yang dapat memberikan nomor IP untuk dirinya. Paket Broadcast tersebut dikirim beserta dengan Ethernet Addressnya (bisa disebut MAC

Address). Server yang mendengar request akan menjawab dan memberikan nomor IP dan waktu pinjam (lease time). Bila lease time habis atau komputer dimatikan maka IP tersebut akan diambil kembali dan diberikan ke komputer lain.

TCPDump

Jaringan TCP/IP terdiri atas keseluruhan paket dan cara terbaik untuk mendebug jaringan adalah dengan cara melacak paket. Dengan demikian kita dapat menentukan informasi yang tepat dari sumber yang benar. Untuk melacak paket kita dapat menggunakan TCPDump, yang tersedia gratis. Dengan memakai ini seumpama kita berada di web maka kita bisa memakainya untuk mencari penyebab sesuatu tidak beres/gagal sumber penyebabnya dimana dengan tracing tersebut.

Dengan menjalankan TCPDump, kita bisa melihat semua traffic yang masuk atau meninggalkan NIC dan bisa melihat aktifitas jaringan.

Dengan TCPDump bisa juga dipakai untuk menganalisa seumpama terjadi kelambatan aplikasi, kita bisa menganalisanya mulai dari ini.

Kemampaun TCPDump akan berkurang jika kita menggunakan switch, jadi untuk mempelajari paket jaringan secara detail dengan memakai TCPDump sebaiknya memakai hub sebab jika memakai switch yang dapat diketahui dari TCPDump hanya traffic ke dan dari komputer.

TCPDump akan berjalan dengan menjalankan command tcpdump [-n|-t|-e] dst.

Dengan TCPDump kita bisa : Memilih paket yang diminati,Memilih paket berdasarkan alamat host], Memilih paket berdasarkan tipe traffic.

Ethereal

Ethereal merupakan software sniffer gratis yang sudah berbentuk Graphical User Interface(GUI). Software ini berjalan baik di linux. Dengan grafiknya mempermudah melihat setiap detail sebuah paket dan frame ethernet.

Software Sniffer lain

Selain dua software di atas ada juga seperti ngrep, ngrep ini mencetak paket sebagai teks ascii. Untuk windows tersedia pula windump yang juga merupakan free software. Selain itu ada pulan Windows Netwrok Monitor, yang mirip dengan ethereal tapi bekerja di windows.

IV. Tugas Pendahuluan

a. Apa kegunaan ARP
b. Gambarkan dan jelaskan format datagram ARP Request/Reply
c. Berada dimanakah tabel ARP cache itu (di directory apa?)
d. Tuliskan option command arp (misal arp –a, arp -??), dan jelaskan maksud dan kegunaannya.
e. Apa yang dimaksud dengan RARP
f. Cari informasi tentang software sniffer tcpdump berikut command – command yang ada pada tcpdump dan apa kegunaannya
g. Cari pula software sniffer ngrep berikut command-command tambahan yang ada pada ngrep dan apa kegunaannya.

V. Percobaan

a. Jalankan command arp –a pada host anda masing-masing, catat dan amati hasilnya. Apa maksud output yang dihasilkan command arp –a
b. Jalankan software sniffer ethereal
c. lakukan command ping no_ip , pilih no_ip yang tidak terdaftar pada percobaan 1 tapi masih dalam satu jaringan.
d. Lihat display yang ada pada software sniffer ethereal, catat dan amati hasilnya. Apa maksud display yang ada pada software ethereal tersebut.
e. Setelah menjalankan perintah ping, lakukan proses 6
f. Jalankan perintah arp –a sekali lagi. Amati pada perbedaan output dibanding waktu percobaan no 1.
g. Lakukan command ping no_ip , pilih no_ip yang sudah terdaftar pada percobaan no 1.
h. Lihat display di ethereal bandingkan dengan display percobaan no 4, tulis perbedaannya.
i. Jawab pertanyaan berikut ini : Kenapa bisa terjadi perbedaan hasil percobaan meskipun kita memakai command yang sama, jelaskan secara singkat.
j. Kita bisa melakukan pengurangan ARP Cache atau disable ARP Cache, lakukan percobaan di bawah ini :
    1. Jalankan command arp –d hostname (pakai salah satu hostname yang terdaftar pada Arp cache). Amati hasilnya dengan menjalankan command arp –a.
    2. Jalankan command berikut :
       ifconfig eth0 down
       ifconfig eth0 –arp up

       Apa maksud 2 perintah di atas ?
k. Selain melakukan pengurangan juga bisa melakukan penambahan Arp Cache , lakukan command berikut :
   arp –s hostname phisical_address
   arp -a
   Sebelum anda mengetik no phisical_address cari dulu di komputer teman anda dengan command ifconfig. Amati hasil percobaan, berikan kesimpulanmu.
l. Jalankan command insmod rarp
m. jalankan command cat /etc/ethers
n. jalankan command rarp –f
o. jalankan command rarp –a
p. Amati percobaan 12-15 apa maksud percobaan di atas dan tulis hasil percobaan
q. Untuk melakukan pengintaian kita bisa juga memakai tcpdump. Ganti software sniffer ethereal pada percobaan di atas dengan software tcpdump dan tulis hasil percobaan anda.
r. Pakailah command-command tambahan di tcpdump untuk mengintai paket yang lewat, misal tcpdump –n, tcpdump –n –t, tcpdump -n –t, tcpdump –n –t –e.
s. Tulis hasil percobaan anda pada no 18 dan analisa hasilnya apa maksud output yang dihasilkannya.

VI. Laporan Resmi

a. Tulis hasil percobaan dan analisa hasilnya.

BAB III
SUBNETTING DAN NETMASK

I. Tujuan

1. Siswa mengenal dan mengetahui peralatan yang dibutuhkan untuk membuat suatu jaringan lokal (Local Area Network/LAN).
2. Siswa memahami topologi jaringan yang ada.
3. Siswa mampu membangun jaringan sederhana

II. Peralatan Yang Dibutuhkan

a. PC yang dianggap sebagai server
b. Beberapa PC sebagai client
c. Hub/Switch
d. NIC yang tertancap pada setiap PC
e. Kabel jaringan secukupnya

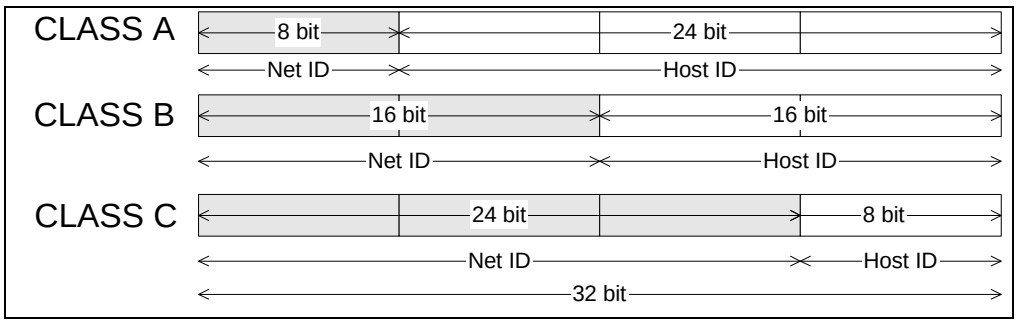
III. Dasar Teori

Masih ingat dengan konsep IP addres ? IP Address terdiri dari 32 bit yang didalamnya terdapat bit untuk NETWORK ID (NetID) dan HOST ID (HostID).

Pemetaan bit NetID dan HostID untuk masing-masing kelas

Kelas IP	Range	Subnet Mask	NetID (bit)	HostID (bit)
A	1-126	255.0.0.0	8	24
B	128-191	255.255.0.0	16	16
C	192-223	255.255.255.0	24	8

Secara garis besar berikut inilah pembagian kelas IP



Netmask

Selain NetID yang menentukan suatu jaringan dalam satu net(jaringan) adalah netmask.

Default netmask adalah sbb :

Class	Netmask	Jumlah Komputer (IP) dalam range
A	255.0.0.0	16.777.216
B	255.255.0.0	65.536
C	255.255.255.0	256

Ketika kita berhubungan dengan komputer lain pada suatu jaringan, selain IP yang dibutuhkan adalah netmask. Misal kita pada IP 10.252.102.12 ingin berkirim data pada 10.252.102.135 bagaimana komputer kita memutuskan apakah ia berada pada satu jaringan atau lain jaringan? Maka yang dilakukan adalah mengecek dulu netmask komputer kita karena kombinasi IP dan netmask menentukan range jaringan kita.
Jika netmask kita 255.255.255.0 maka range terdiri dari atas semua IP yang memiliki 3 byte pertama yang sama. Misal jika IP kita 10.252.102.12 dan netmask saya 255.255.255.0 maka range jaringan kita adalah **10.252.102**.0-**10.252.102**.255 sehingga kita bisa secara langsung berkomunukasi pada mesin yang diantara itu jadi **10.252.102**.135 berada pada jaringan yang sama yaitu **10.252.102** (lihat yang angka-angka tercetak tebal menunjukkan dalam satu jaringan karena semua sama).

Dalam suatu organisasi komersial biasanya terdiri dari beberapa bagian, misalnya bagian personalia/HRD, Marketing, Produksi, Keuangan, IT dsb. Setiap bagian di perusahaan tentunya mempunyai kepentingan yang berbeda-beda. Dengan beberapa alasan maka setiap bagian bisa dibuatkan jaringan lokal sendiri – sendiri dan antar bagian bisa pula digabungkan jaringannya dengan bagian yang lain. ***Pembagian jaringan besar ke dalam jaringan yang kecil-kecil inilah yang disebut sebagai subnetting.***

Ada beberapa alasan yang menyebabkan satu organisasi membutuhkan lebih dari satu jaringan lokal (LAN) agar dapat mencakup seluruh organisasi :

- Teknologi yang berbeda. Dalam suatu organisasi dimungkinkan menggunakan bermacam teknologi dalam jaringannya. Semisal teknologi ethernet akan mempunyai LAN yang berbeda dengan teknologi FDDI.
- Kongesti pada jaringan. Sebuah LAN dengan 254 host akan memiliki performansi yang kurang baik dibandingkan dengan LAN yang hanya mempunyai 62 host. Semakin banyak host yang terhubung dalam satu media akan menurunkan performasi dari jaringan. Pemecahan yang paling sedherhana adalah memecah menjadi 2 LAN.
- Departemen tertentu membutuhkan keamanan khusus sehingga solusinya memecah menjadi jaringan sendiri.

Pemecehan menggunakan konsep ***subnetting***. Membagi jaringan besar tunggal ke dalam sunet-subnet (sub-sub jaringan). ***Setiap subnet ditentukan dengan menggunakan subnet mask bersama-sama dengan no IP.***

Misal jika jaringan kita adalah 20.0.0.0 (class A memberikan range 20.0.0.0 – 20.255.255.255). Ingat class A berarti 8 bit pertama menjadi NetID yang dalam satu jaringan tidak berubah (dalam hal ini adalah 20) dan bit selanjutya sebagai Host ID (yang merupakan no komputer yang terhubung ke jaringan dengan id 10 dan setiap komputer mempunyai no unik mulai dari 0.0.0 – 255.255.255). Dimana netmasknya/subnetmasknya adalah 255.0.0.0

Kita dapat membagi menjadi subnet sbb :

Nama	NetID	Subnet mask	Range Jaringan
P	20.1.1.0	255.255.255.0	20.1.1.0-20.1.1.255
Q	20.1.2.0	255.255.255.0	20.1.2.0-20.1.2.255

R	20.201.0.0	255.255.0.0	20.201.1.0-20.201.255.255
S	20.202.77.0	255.255.0.0	20.202.77.0-20.202.77.255
Dan seterusnya pembagian sesuai kebutuhan			

Sekarang yang jadi masalah ada bagaimana kita dapat mengalokasikan class B yang seharusnya 65.536 IP tapi sebenarnya kita hanya butuh 16 Class B saja. Karena jika kita tetap memakai default class B mungkin terlalu besar jaringan kita.

Rumusan cara menentukan Subnet (NetID dan Netmask)

1. **Langkah 1 :**

   Pada dasarnya solusi sebuah subnet dimulai dengan mengenal class dari alamat IP lebih dahulu.

   Class A 1 - 126 (127 reserved)
   Class B 128 - 191
   Class C 192 - 223

   Ketiganya (A,B,C) bisa dikatakan subjaringan/subnet sendiri-sendiri. Tapi kita akan berusahan membuat subjaringan dari jaringan yang sudah ada. Misal membuat beberapa sub jaringan lagi di class A, jadi class A yang seharusnya 1 jaringan besar dipecah menjadi jaringan yang lebih kecil.

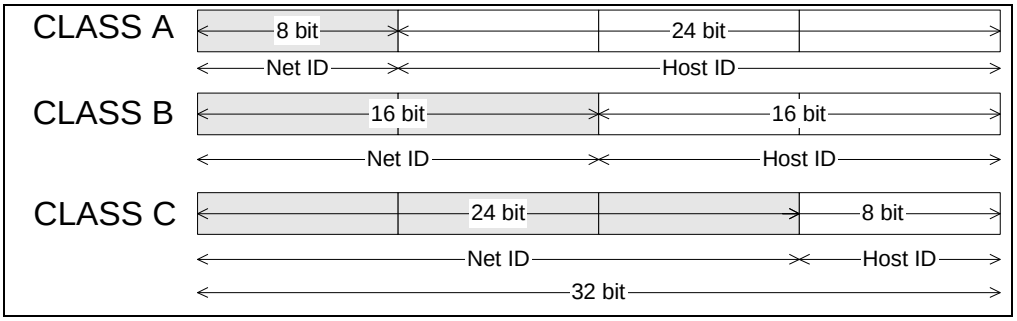
   Tidak disertakan pada Subnetting;
   Class D 224 – 239 (multicast)
   Class E 240 – 254 (experimental)

2. **Langkah 2 :**

   Untuk membuat subnet dalam suatu class adalah dengan cara melihat bit hostnya dikurangi 2 bit untuk network address dan broadcast address

Class	Host bits	Yang Dapat Diambil (Yang dpt dipakai subnet)
A	24	22
B	16	14
C	8	6

Perhitungan host bits berasal dari perhitungan berikut :



Jumlah subnets yang terkecil yang dapat dibuat :

$2^2 - 2 = 4 - 2 = 2$ subnets.

Jumlah Subnet yang dapat dibuat $= 2^N - 2$

Jumlah Host yang dapat dibuat $= 2^n - 2$

N = jumlah bit dari bit host yang dipinjam

n = sisa bit dari bit host yang di pinjam

Contoh :

Misal kita ingin membuat 50 subnet pada class C, dengan masing- masing subnet mempunyai 4 hosts. Berapa subnet-bits yang dibutuhkan ?

Jawab :

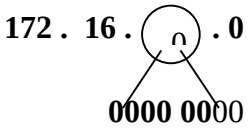
Untuk mendapatkan 50 subnet, maka nilai pangkat 2 yang paling dekat adalah 64, yang berarti $2^6 - 2 = 62$ subnets. Sehingga subnets bits yang dibutuhkan untuk membuat 50 subnet adalah 6.

Pada Class C host bitnya ada 8 (lihat gambar di atas), sehingga :

Sisa $8 - 6 = 2$ bits untuk Hosts, sehingga jumlah Hosts yang dapat dibuat hanya $2^2 - 2 = 2$. Karena itu permintaan tersebut tidak dapat dipenuhi.

Bagaimana dengan **Class B** ?. Misalnya **172.16.0.0** Hosts-Bits pada class B adalah 16 bits, sehingga bila diambil 6, maka sisa adalah 10 bits yang berarti setiap subnets dapat mempunyai $2^{10} - 2$ Hosts = 1044 Hosts (memenuhi).

Untuk membentuk subnets, maka octet ke-3 dari **172.16.0.0** diambil 6 bit sebagai nomor sub-jaringan yang baru.



3. **Langkah 3 :**

Tentukan subnets-mask. Karena yang diambil adalah 6 bits, maka komposisi biner 1 adalah 0.

Class B tanpa subnet :

10xxxxxx.xxxxxxxx	xxxxxxxx.xxxxxxxx
11111111.1111111	00000000.00000000
255 . 255	.0 .0

B dengan subnet :

10xxxxxx.xxxxxxxx	xxxxxxxx.xxxxxxxx
11111111. 11111111	**11111100.00000000**
255 .255	.252 .0

Subnetmask = 255.255.252.0

Gunakan tabel berikut untuk menghitung nilai desimal dari subnet :

1	0	0	0	0	0	0	0	= 128
1	1	0	0	0	0	0	0	= 192
1	1	1	0	0	0	0	0	= 224

1	1	1	1	0	0	0	0	= 240
1	1	1	1	1	0	0	0	= 248
1	1	1	1	1	1	0	0	= 252
1	1	1	1	1	1	1	0	= 254
1	1	1	1	1	1	1	1	= 255

Catatan :
Bila hosts bits yang diambil melebihi 8 bits, maka netmask berlanjut.

9 bits	- > 255 . 128
10 bits	- > 255 . 192
11 bits	- > 255 . 224
12 bits	- > 255 . 240
13 bits	- > 255 . 248
14 bits	- > 255 . 252

Dan seterusnya.....

4. Langkah 4 :

Tentukan nomor subnet :
Dari 6 bits subnet address yang ada terperinci sebagai berikut (total 2^6 = 64 address)/ buat kombinasinya:

000000 00 = 0
000001 00 = 4
000010 00 = 8
000011 00 = 12
.....
111110 00 = 248
111111 00 = 252

Perhatikan bahwa baris pertama disebut sebagai **subnet-zeroes**, karena network-id seluruhnya terdiri atas angka biner 0, sedangkan baris terakhir disebut sebagai **subnet-ones.**
Karena alamat tersebut rancu dengan network-id yang asli (tanpa subnet), sedangkan subnet-ones rancu dengan alamat broadcast network tersebut, maka penggunaan subnet-zeroes dan ones tidak dimengerti oleh routers. Oleh karena itu penggunaannya dihindari dan dianggap sebagai alamat jaringan yang **tidak valid**.

~~**000000** 00 = 0~~
000001 00 = 4
000010 00 = 8
....
111110 10 = 248
~~**111111** 00 = 252~~

Dengan demikian nomor sub-jaringan yang didapat adalah :

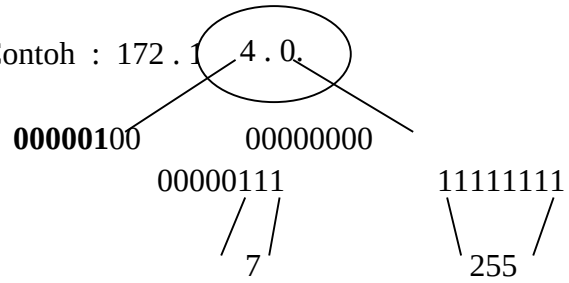
Subnet	Subnet – Id	Keterangan
1	172 . 16 . 0 . 0	invalid, subnet zeroes
2	172 . 16 . 4 . 0	
3	172 . 16 . 8 . 0	
4	172 . 16 . 12 . 0	
.....		
63	172 . 16 . 248 . 0	
64	172 . 16 . 252 . 0	invalid, subnet ones

NB: Subnet yang digunakan dari subnet nomor 2 sampai dengan 63.

5. Langkah 5 :

Setiap subnet mempunyai alamat broadcast, yaitu alamat yang ditujukan untuk seluruh simpul di sub jaringan tersebut.

Untuk menentukan alamat broadcast, maka seluruh bits pada bagian Host dibuat menjadi biner 1.



Hasil : alamat broadcast adalah **172. 16. 7. 255**

Sebuah formula yang dapat diaplikasikan untuk mendapatkan broadcast secara cepat adalah :

alamat broadcast = subnet id berikut – 1

Artinya, untuk mendapatkan alamat broadcast dari subnet 172. 16. 4. 0 adalah subnet 172. 16. 8. 0 dikurang 1, menjadi 172. 16. 7. 255 (ingat bahwa setiap octet terdiri atas 8 bit dengan nilai 0 sampai dengan 255).

Subnet	Subnet - Id	Broadcast	Keterangan
1	172. 16. 0. 0	172. 16. 3. 255	invalid, subnet zeroes
2	172. 16. 7. 0	172. 16. 7. 255	
3	172. 16. 11. 0	172. 16. 11. 255	
4	172. 16. 15. 0	172. 16. 15. 255	
...			
63	172. 16.251. 0	172. 16. 251. 255	
64	172. 16. 252. 0	172. 16. 255. 255	invalid, subnet ones

6. Langkah 6 :

Setelah mendapatkan subnet id dan broadcast id, maka nomor IP yang dapat diberikan pada subnet tersebut adalah network id + 1, sedangkan nomor IP terakhir yang dapat diberikan adalah broadcastid dikurangi 1.

Subnet Address : 172. 16. 4. 0 / 22
IP-Address 1 : 172. 16. 4. 1 / 22

IP – Address terakhir 172. 16. 7. 254 /22
Broadcast : 172. 16. 7. 255 /22

Perhatikan bahwa /22 adalah bitcount (jumlah angka biner 1) dari netmask 255. 255. 252.0

IV. Tugas Pendahuluan

Lengkapilah tabel berikut ini :

Subnet	Subnet - Id	Broadcast	Keterangan
1	172. 16. 0. 0		invalid
2	172. 16. 4. 0	172. 16. 4. 1	172. 16. 7. 254
3	172. 16. 8. 0		
4	172. 16. 12. 0		
...			
62	172. 16. 244. 0		
63	172. 16. 248. 0		
64	172. 16. 252. 0		invalid

V. Percobaan

a. Dengan memakai 3 subnet di tugas pendahuluan (subnet 2,3 dan 4) lakukan langkah percobaan.
b. Lakukan setting jaringan berikut ini (bagi dalam 3 kelompok besar sesuai subnetnya dan pilih IP untuk setiap kelompok sesuai subnetnya) untuk setiap subnet lakukan langkah berikut:
   g. Masuklah ke sistem komputer yang memiliki sistem operasi Linux
   h. Login sebagai root
   i. Buka terminal dengan mengklik pada Start Menu -> System Tools -> terminal
   j. Ceklah ethernet card yang ada pada komputer anda dengan megetikkan perintah
      [root@WSC204-11 root]# dmesg | grep eth
      Analisa hasilnya.
   k. Lakukan konfigurasi jaringan secara manual dengan menggunakan perintah *ifconfig*
      [root@WSC204-11 root]# ifconfig eth0 no_ip netmask no_netmask up

   l. Setelah melakukan konfigurasi untuk melihat hasilnya ketikkan perintah di bawah dan lihat pesan yang keluar
      [root@WSC204-11 root]# ifconfig

      Analisa hasilnya
c. Selanjutnya lakukan tes konektifitas dengan menggunakan perintah *ping* dengan komputer lain yang berada pada 1 jaringan dengan memakai perintah *ping*.
   Untuk menghentikan tekan Ctrl + C dan Analisa Hasilnya.
d. Lakukan koneksi lain subnet dengan melakukan perintah ping
   Analisa apa yang terjadi, kenapa bisa seperti itu?

VI. Laporan Resmi

a. Tulis hasil percobaan dan analisa hasilnya.

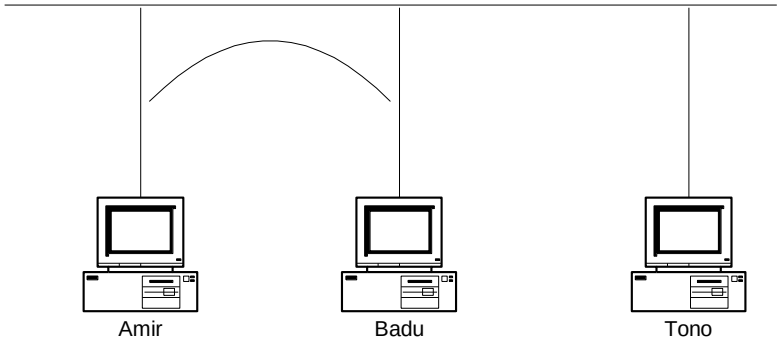
BAB IV
LINUX ROUTER

I. Tujuan

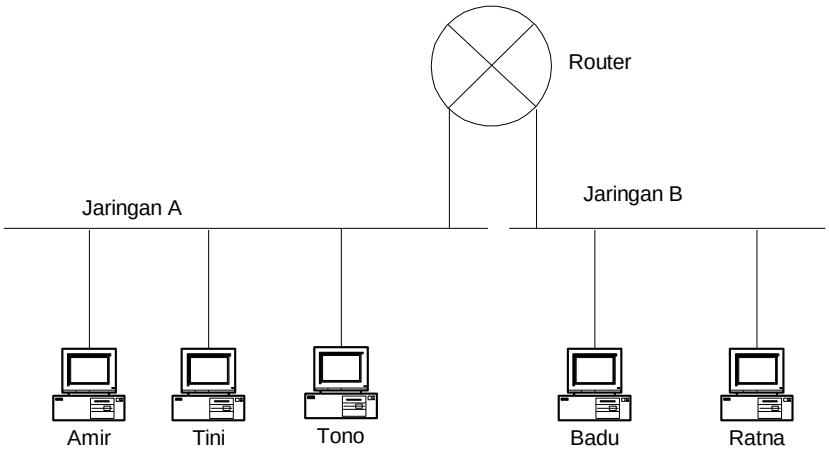
1. Mahasiswa memahami konsep routing
2. Mahasiswa mampu melakukan konfigurasi static routing

II. Dasar Teori

Pada dasarnya untuk komunikasi terjadi antara dua komputer. Misal Amir berkomunikasi dengan Badu dalam satu jaringan, bisa digambar sbb :



Jika terjadi komunikasi antara Amir dan Badu di jaringan yang lebih besar dimana bisa saja antara keduanya tidak berada pada jaringan sama, maka perlu penghubung diantara keduanya sehingga berhasil berhubungan.

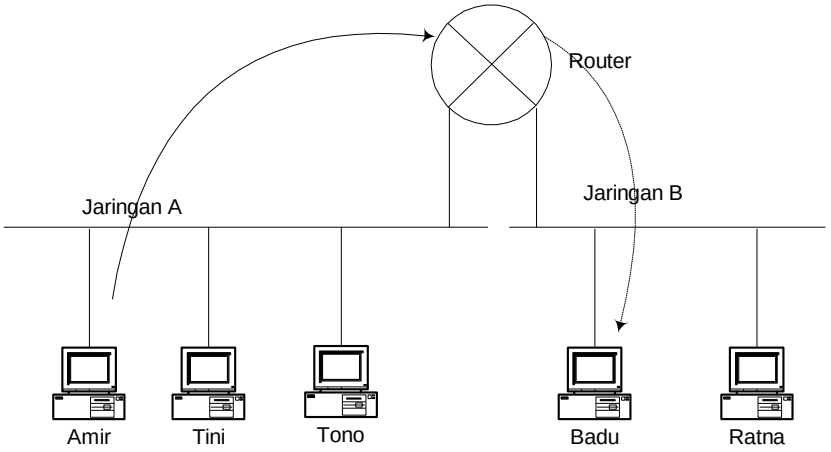


Penghubung antara satu jaringan dengan jaringan yang lain disebut sebagai router.

Konsepnya pengirim paket akan menguji tujuan dari paket apakah tujuan IP berada pada jaringan lokal ? Jika tidak pengirim akan mengirimkan paket akan meminta bantuan ke router yang terhubung dengan pengirim dan paket diberikan ke router untuk diteruskan. Router yang diberi paket pada prinsipnya juga bekerja seperti pengirim paket tadi. Setiap router mengulangi cara yang sama sampai paket berada pada router yang mempunyai koneksi lokal dengan penerima.

Router bertugas untuk menyampaikan paket data dari satu jaringan ke jaringan lainnya, jaringan pengirim hanya tahu bahwa tujuan jauh dari router. Dan routerlah yang mengatur

mekanisme pengiriman selain itu router juga memilih "jalan terbaik" untuk mencapai tujuan. Diberikan ilustrasi sederhana berikut :



Meneruskan sebuah paket via router sangatlah sederhana. Router dikoneksi langsung ke Amir sehingga dapat mengirim sebuah paket Ethernet ke Badu dengan menentukan alamat ethernetnya sebagai tujuan. Akan tetapi pada tingkat IP, tujuan akhir dari paket adalah Badu, bukan router. Dengan demikian Amir menset alamat tujuan IP ke IP Badu. Hasilnya adalah paket dengan pengalamatan sbb :

	Src	Dst
MAC	Ethernet Address Amir	Ethernet Address Router
IP	IP Address Amir	IP Address Badu

Koneksi Via Router

	src	Dst
MAC	Ethernet Address Amir	Ethernet Address Badu
IP	IP Address Amir	IP Address Badu

Koneksi langsung

Dari tabel diatas ada beberapa hal yang perlu diperhatikan :

- Source address : baik ethernet dan IP terhubung ke Amir.
- Alamt tujuan : Ethernet ke Router sedangkan IP tujuan ke Amir. Ethernet tujuan dalam paket hanya terkait dengan hop, sedangkan IP tujuan adalah tujuan paket.
- Ketika sebuah router menerima paket dengan IP address yang bukan miliknya, maka ini menjadi permintaan implisit untuk meneruskan paket ke tujuan.
- Sebuah mesin hanya bisa meneruskan paket ke router yang terkoneksi langsung dengannya. Dan digunakan mekanisme yang sama untuk mengirim ke sebuah router. Jika tidak ada router pada jaringan Amir, maka amir tidak dapat mengirim ke semua komputer diluar jaringannya.
- Router juga dapat melewatkan paket hanya ke host/router yang ada pada jaringan yang terkoneksi langsung kepadanya. Dengan demikian supaya router berfungsi, ia harus dikoneksikan langsung ke lebih dari satu jaringan.

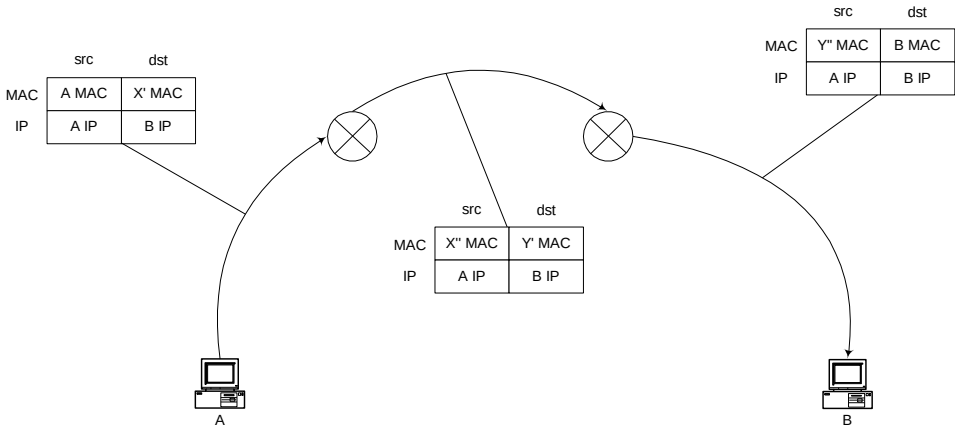
Perjalanan melintasi jaringan ke banyak hop

- Setiap hop yang berubah adalah segmet ethernet dari tujuan

- Setiap hop adalah source ke router, router ke router atau router ke tujuan

Kita dapat mendiagnosa memakai tcpdump atau ethereal. Sehingga kita dapat memeriksa jalannya jaringan dan jika ada masalah bisa mengetahui masalah ada pada hop yang mana.

Berikut ini adalah ilustrasi perubahan alamat paket dari hop ke hop sampai data ke tujuan :



Jadi yang berubah hanya MAC Address, sedangkan nomor IP selalu sama.

Default Gateway

Router adalah komputer general purpose dengan dua atau lebih interface jaringan di dalamnya yang berfungsi hubungan 2 jaringan atau lebih, sehingga dia bisa meneruskan paket dari satu jaringan ke jaringan yang lain.

Untuk jaringan kecil interfacenya adalah NIC Card, sehingga router mempunyai 2 NIC atau lebih yang bisa menghubungkan dengan jaringan lain. Untuk LAN kecil yang terhubung internet, salah satu interface adalah NIC card, dan interface yang lain adalah sembarang hardware jaringan leased line atau ISDN atau koneksi internet ADSL yang digunakan.

Router bisa dibuat dari komputer yang difungsikan sebagai router, jadi tidak harus hardware.

Defaukt gateway dari mesin merupakan sebuah router yang digunakan untuk meneruskan paket-paket ke jaringan yang lain.

Biasanya LAN dikonfigurasi hanya mengetahui LAN miliknya dan default gatewaynya. Jika dalam suatu LAN tidak ada default gatewaynya maka LAN tersebut tidak bisa terkoneksi dengan jaringan lainnya.

Jadi supaya dapat melakukan routing maka setting jaringan perlu ditambahkan satu lagi yaitu default gateway.

Sekarang ada tiga parameter yang penting pada setting jaringan yaitu :

1. IP Address
2. Netmask
3. Default Gateway.

Tabel Routing

Supaya router bisa melayani permintaan untuk meneruskan pengiriman data, maka router harus mempunyai tabel yang dipakai sebagai patokan data ini harus saya kirim ke jaringan

yang mana? Tabel yang dipunyai oleh router disebut sebagai tabel routing yang berisi NETID dan Default gatewaynya.

Berikut ini adalah skenario pengiriman data dari komputer 192.168.1.5 ke komputer 192.168.2.36 :

a. Komputer 192.168.1.5 ingin mengirim data ke 192.168.2.36, menyadari bahwa alamat tujuan tidak berada di jaringan lokal, maka komputer mencari daftar "default gateway" pada property TCP/IP yaitu 192.168.1.13. Paket data kemudian dikirim ke Gateway tersebut.
b. Pada komputer 192.168.1.13 paket data tersebut kembali diperiksa, dan ditemukan pada tabel routing bahwa paket tersebut dapat dikirim ke jaringan 192.168.2 lewat IP 192.168.2.43
c. Via IP 192.168.2.43 akhirnya data dapat ditransmisi ke tujuan yaitu 192.168.2.36

Router yang mempunyai tabel routing yang dikelalo secara manual disebut sebagai static routing. Tabel tersebut berisi daftar jaringan yang dapat dicapai oleh router tersebut.

Static routing dapat mempelajari jaringan yang berada disekelilingnya secara terbatas (bila hanya 2 jaringan), tapi bila terdapat banyak jaringan, maka administrator harus mengelola tabel routing tersebut secara cermat.

Dynamic routing adalah fungsi dari routing protocol yang berkomunikasi dengan router yang lain untuk saling meremajakan (update) tabel routing yang ada. Dengan demikian, administrator tidak perlu melakukan updating jalur (path) jika terjadi perubahan jalur transmisi (path). Dynamic routing umumnya digunakan untuk jaringan komputer yang besar dan lebih kompleks.

Konfigurasi Static Routing

Tabel routing biasanya berada pada /sbin/route dan command /bin/netstat –r. Sedangkan untuk melihat tabel routing bisa memakai command route atau netstat -r.

Untuk mendefinisikan/setting default gateway, jalankan perintah command : route add default gw 192.0.2.1

Untuk mendaftarkan jaringan pada tabel routing, maka sintaxnya adalah sbb:

Route add –net 10.0.0.0 192.168.1.11

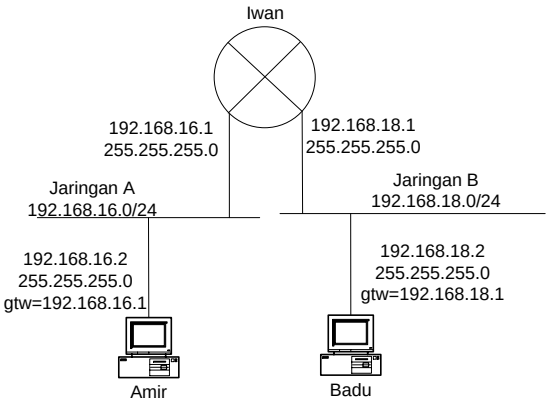
Dalam percobaan kali ini kita akan mencoba mengkonfigurasi routing antara dua jaringan.

III. Tugas Pendahuluan

a. Jelaskan apa yang dimaksud dengan router
b. Jelaskan secara singkat bagaimana komputer bisa mengirim data antar jaringan.
c. Apa saja setting jaringan yang diperlukan jika kita perlu berkomunikasi dengan jaringan yang lain
d. Jelaskan secara singkat apa itu tabel routing
e. Bagaimana care mengkonfigurasi static routing
f. Tuliskan kembali command route secara lengkap
g. Jelaskan secara singkat apa kegunaan command traceroute dan tuliskan kembali command traceroute beserta parameternya

IV. Percobaan

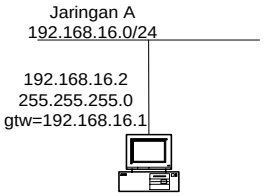
a. Bangunlah jaringan sederhana seperti pada gambar :



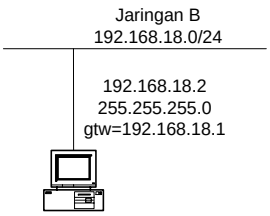
b. Konfigurasi salah satu komputer sebagai router, dengan cara menambah NIC Card menjadi 2 buah dan pasangkan pada komputer.

c. Siapkan 2 hub/switch, buat 2 subnet komputer yang ada di laboratorium. Hubungkan setiap subnet dengan Hub/switch. Lihat 2 buah subnet berikut :

Subnet A



dan Subnet B



d. Konfigurasi komputer yang ada di tiap subnet. Berundinglah dengan teman anda dalam 1 subnet untuk memberi nomor IP (Lihat praktikum 1 dan praktikum 2 untuk setting IP) **NB. Jangan memakai IP 192.168.16.1 dan 192.168.18.1 karena akan dipakai untuk keperluan lain**

e. Lakukan koneksi di tiap subnet dan yakinkan komputer tiap subnet terhubung satu sama lain

f. Setting Router untuk menghubungkan dua buah jaringan tersebut.
Pada komputer yang NICnya kita pasang dua, tancapkan dua kabel untuk NIC tersebut, satu dihubungkan dengan subnet satu (kabel dihubungkan dengan hub yang satu)dan NIC yang lain dihubungkan dengan subnet yang lain (kabel yang satunya dihubungkan dengan hub yang lain).
Pastikan untuk NIC dengan label eth0 dihubungkan dengan NetID 192.168.16 dan NIC dengan label eth1 dihubungkan dengan NetID 192.168.18. Selanjutnya lakukan konfigurasi berikut pada komputer router tersebut :

i. Konfigurasi eth0
   # ifconfig eth0 192.168.16.1 broadcast 192.168.16.255 netmask 255.255.255.0 up
ii. Cek hasil configurasi kita dengan command
   # ifconfig eth0
iii. Tambahkan tabel routing dengan command :
   # route add – net 192.168.16.0 netmask 255.255.255.0 eth0
iv. Konfigurasi eth1
   # ifconfig eth1 192.168.18.1 broadcast 192.168.18.255 netmask 255.255.255.0 up
v. Cek hasil konfigurasi dengan command
   # ifconfig eth1
vi. Tambahkan tabel routing pada eth1 dengan command :
   # route add – net 192.168.18.0 netmask 255.255.255.0 eth1

g. Untuk setiap workstation di subnet A, lakukan perintah berikut untuk menghubungkan dengan router
   # route add – net default gw 192.168.16.1 metric 1
h. Untuk setiap workstation di subnet B, lakukan perintah berikut untuk menghubungkan dengan router Setting jaringan anda
   # route add – net default gw 192.168.18.1 metric 1
i. Untuk semua komputer yang ada tidak terkecuali router juga, set ip_forward menjadi 1, caranya jalankan command berikut :
   # echo “1”>/proc/sys/net/ipv4/ip_forward
j. Lakukan perintah ping ke satu jaringan dan lain jaringan, jika bisa maka percobaan anda berhasil
k. Ketika menjalankan command ping, tangkap paket yang lewat memakai tcpdump dan ethereal. Analisa apa hasilnya
l. Lakukan command traceroute, dan analisa hasilnya.
m. Tulis percobaan anda dan Analisa hasilnya.

V. Laporan Resmi

Tulis hasil percobaan dan analisa hasilnya.

BAB V
ROUTING TINGKAT LANJUT

I. Tujuan

1. Mahasiswa memahami konsep routing.
2. Mahasiswa memahami konsep IP-Aliasing untuk Multinetting
3. Mahasiswa mampu mengimplementasikan IP aliasing untuk Multinetting
4. Mahasiswa memahami konsep routing di inter-networking
5. Mahasiswa mampu membangun router-router di inter-networking (lebih dari 2 subnet)

II. Dasar Teori

Inter-Network

Internet adalah inter-network dari banyak jaringan yang terpisah. Jaringan ini dikoneksikan ke jaringan yang lain dengan router. Ketika kita berkomunikasi dengan internet , paket dari PC kita berjalan hop demi hop melewati semua jaringan yang menghadangnya sampai ke tempat tujuan. Pada setiap hop, sebuah router meneruskan paket menuju tujuan. Paket yang ada hanya berisi IP tujuan tidak berisi routing apapun (dia harus kemana/melewati jalan mana source tidak tahu) routerlah yang harus memutuskan paket ini harus melewati router mana saja menggunakan tabel routing, yang merupakan sekumpulan aturan yang memberitahu router mengenai hop berikutnya untuk melanjutkan paket sampai ke tujuan.

Di dalam internet, diperlukan router yang canggih dimana secara otomatis bisa melakukan routing secara otomatis. Di sini router menemukan dari router lainnya bagaimana mengirim ke berbagai tujuan, dan menginformasikan ke router lain ketika koneksi terhenti sehingga paket dapat dikirim dengan jalur yang berbeda.

Akan tetapi untuk sekarang kita mencoba memakai router yang statis. Untuk melihat table routing kita memakai command :

```
route –n
netstat  -router –n
```

Untuk menambah sebuah route pada sebuah jaringan memakai command :

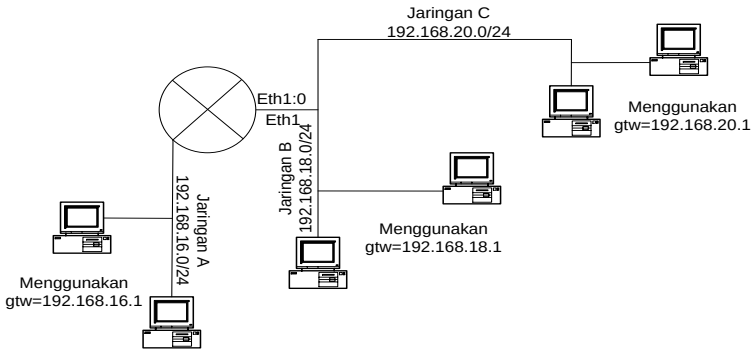
```
route add –net destaddr netmask x.x.x.x gw routeaddr
```

Untuk membuat setting permanen maka pada command route ditambahkan opsi –**p**.

Untuk menghapus pakai command route delete destaddr

IP Aliasing untuk Multi-Netting

IP Aliasing adalah adalah mapping single MAC Address untuk multiple IP address, satu NIC bisa diberi nomor IP lebih dari satu. Contoh penggunaan IP Aliasing bisa dilihat pada gambar di bawah ini.



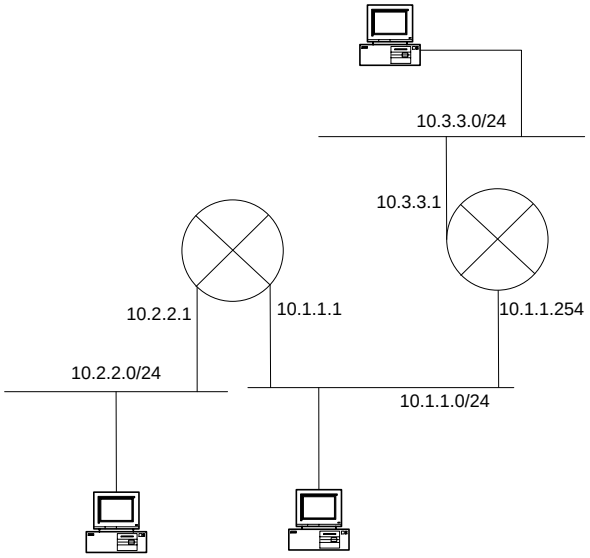
Dengan 2 NIC bisa menghubungkan 3 subnet yang berbeda. Dimana salah satu NIC router diberi 2 IP adrees.

III. Tugas Pendahuluan

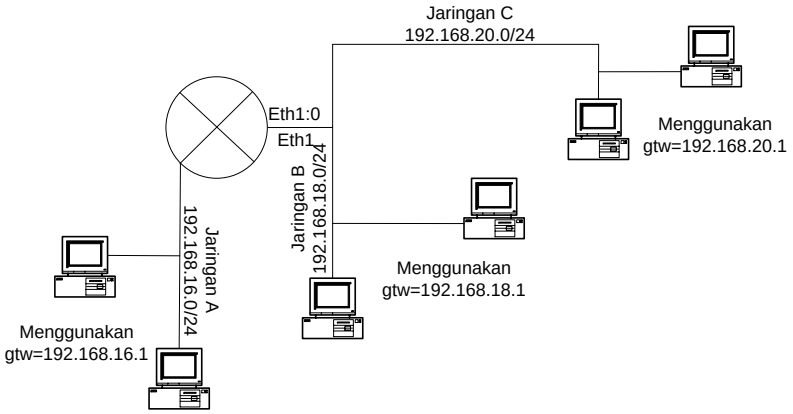
a. Jelaskan apa perbedaan command router memakai –n dan tidak
b. Jelaskan tentang IP Aliasing

IV. Percobaan

a. Buatlah percobaan seperti pada gambar berikut :



b. Lakukan berkelompok setting per subnet untuk percobaan ini siapkan beberapa komputer untuk tiap subnet, sesuaikan no IP sesuai range di gambar.
c. Lakukan testing jaringan tiap subnet, semua komputer persubnet pastikan sudah terhubung.
d. Siapkan beberapa komputer bertindak sebagai router antar jaringan.
e. Setting router itu dengan memakai cara pada praktikum sebelumnya.
f. Lakukan koneksi antar jaringan dengan memakai command ping.
g. Tangkap hasil ping dengan tcpdump atau ethereal, sehingga kita akan mengetahui rute jaringan dan jika ada error kita bisa tahu penyebab error berada dimana.
h. Setelah praktikum di atas selesai, cobalah analisa hasilnya.
i. Buat pula percobaan IP Aliasing seperti pada gambar berikut



j. Caranya lakukan seperti pada percobaan ke 4.
k. Buatlah pula satu subnet lagi dan konfigurasi IP yang masuk ke dalam subnet C.
l. Lakukan setting router tambahan sbb :

    # ifconfig eth1:0 192.168.20.1 broadcast 192.168.20.255 netmask 255.255.255.0 up

m. Cek memakai perintah ifconfig eth1:0
n. Tambah ke dalam routing tabelnya sbb :

    # route add – net 192.168.20.0 netmask 255.255.255.0 eth1

o. Lakukan perintah ping ke satu jaringan dan lain jaringan, jika bisa maka percobaan anda berhasil
p. Ketika menjalankan command ping, tangkap paket yang lewat memakai tcpdump dan ethereal. Analisa apa hasilnya
q. Lakukan command traceroute, dan analisa hasilnya.

V. Laporan Resmi

a. Tulis hasil percobaan dan analisa hasilnya.

BAB VI
TELNET DAN FTP

I. Tujuan

1. Siswa Memahami konsep telnet dan FTP
2. Siswa mampu membangun telnet dan FTP

II. Dasar Teori

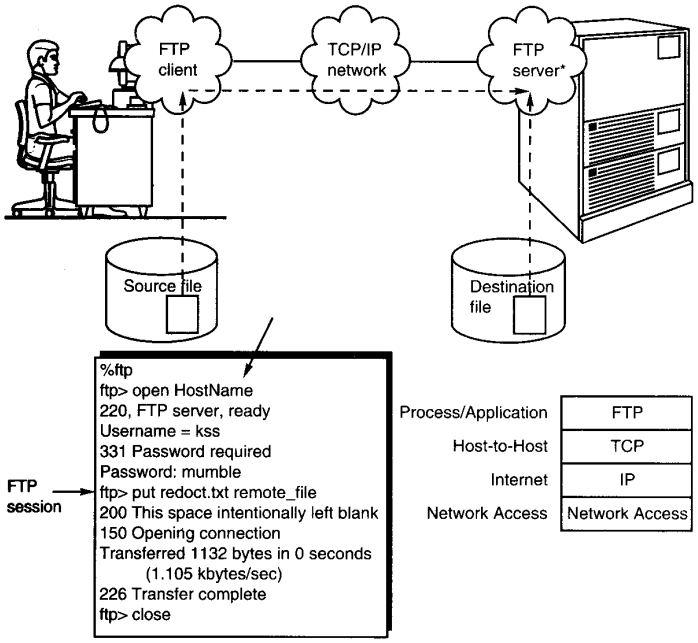
FTP menggunakan protokol transport TCP untuk mengirimkan file. TCP dipakai sebagai protokol transport karena protokol ini memberikan garansi pengiriman dengan FTP yang dapat memungkinkan user mengakses file dan direktory secara interaktif, diantaranya :

- Melihat daftar file pada direktory remote dan lokal.
- Menganti nama dan menghapus file
- Transfer file dari host remote ke lokal (download)
- Transfer file dari host lokal ke remote (upload)

Pada gambar dibawah menunjukkan mekanisme transfer file dari host lokal ke remote, proses transfer file seperti ditunjukkan dengan tanda panah pada gambar tersebut. Tahapan FTP dimulai dari client memasuki jaringan TCP/IP, komputer remote yang akan dituju disebut host FTP, dan host FTP ini harus memiliki software FTP server yang telah diinstall agar dapat berinteraksi dengan sistem file pada host. Untuk memulai melakukan FTP, maka berikan perintah seperti berikut :

%ftp [hostname]

tanda % adalah prompt default pada OS Unix, *hostname* merupakan nama secara simbolik atau IP address dari host yang akan dituju. Bila sudah dapat tersambung maka akan ditanyakan nama *user* dan *password*, isian nama *user* dan *password* sesuai dengan *account* yang diberikan seperti yang digunakan bila user akan menggunakan server tersebut, tetapi pada FTP server yang umum, untuk nama user dapat digunakan *ftp* atau *anonymous* dengan menggunakan *password* yaitu alamat *e-mail*, akan tetapi memiliki hak akses yang terbatas sesuai yang ditetapkan administrator FTP server.



Gambar 2. Mekanisme FTP

III. Tugas Pendahuluan

1. Apa perbedaan fungsi telnet dan ftp ?
2. Klasifikasikan jenis ftp server berdasarkan tipe usernya!
3. Pada Linux Redhat versi 8.0 keatas, program ftp server telah menggunakan vsftpd, setelah sebelumnya digunakan wu-ftpd. Sebutkan beberapa keunggulan dari program vsftpd dibandingkan dengan wu-ftpd.

IV. Percobaan

1. Login ke sistem Linux sebagai root
2. Cek apakah konfigurasi alamat IP untuk host.
   a. Jalankan perintah **ifconfig**, tulis konfigurasi IP host anda.
      Interface : _____
      IP Address : _____
      Subnet mask : _____
   b. Jalankan perintah netstat –r, tuliskan default gateway host anda.
      Default Gateway :

3. Catatlah berapa nomer port yang digunakan oleh telnet dan ftp

```
# cat /etc/services | grep ftp
# cat /etc/services | grep telnet
```

   Apakah protokol yang digunakan oleh ftp dan telnet ?

4. Cek apakah program vsftpd sudah terinstall atau belum. Jika sudah, langsung kerjakan langkah nomer 8.
   - Jalankan perintah **rpm –qa | grep telnet**, tulis hasilnya

- Ada berapa banyak program telnet yang terinstall ?
- Apakah sudah ada program telnet-server ?
- Jalankan perintah **rpm –qa | grep telnet-server** , tulis hasilnya
- Jalankan perintah **rpm –qa | grep vsftpd**, tulis hasilnya.
- Versi dari vsftpd : _____

5. Jika program telnet-server dan vsftpd belum ada, installah dengan cara sbb.
   Masukkan CD Rom Redhat dan ketiklah perintah berikut ini.

```
# mount  /dev/cdrom  /mnt/cdrom
# cd /mnt/cdrom
# ls –l
# cd RedHat
# ls –l
# cd RPMS
# ls –l telnet*
# ls –l vsftpd*
```

6. Jika tidak ditemukan telnet-server-xxxx.rpm atau vsftpd-xxxx.rpm (xxx = nomer versi) gantilah dengan CD yang lain, jika ditemukan installah program tersebut dengan cara

```
# rpm –ivh telnet-server*.rpm
# rpm –ivh vsftpd*.rpm
```

7. Catatlah di direktori mana saja kedua program tersebut diinstall.

```
# rpm –ql telnet-server
# rpm –ql vsftpd
```

   Catatlah :
   - Direktori yang berisi executable file untuk program telnet dan vsftpd
   - Nama file konfigurasi :_____
   - Direktori yang menyimpan manual dan dokumentasi kedua program tersebut

8. Mengaktifkan vsftp server
   Amati file-file yang berhubungan dengan program vsftpd

```
# rpm –ql vsftpd
```

   Baca dan pelajari file konfigurasi vsftpd

```
# vi /etc/vsftpd/vsftpd.conf
```

   Baca dan pelajari file script vsftpd

```
# vi /etc/rc.d/init.d/vsftpd
```

   Untuk menjalankan program vsftpd ketiklah

```
# vi /etc/rc.d/init.d/vsftpd start
```

9. Menghapus rule firewall

Redhat Linux versi 8 atau yang lebih baru, akan mengaktifkan firewall secara default sehingga semua akses dari luar akan ditolak. Untuk kepentingan percobaan ini, ada baiknya untuk sementar semua rule firewall dihapus. Gunakan perintah :

```
# iptables -F
```

10. Uji coba dari localhost

Untuk menguji coba apakah telnet & ftp server sudah berjalan dengan baik atau tidak jalankan perintah sbb. :

```
# telnet localhost
# ftp localhost
```

Jika terdapat pesan sbb. berarti kedua service tersebut belum berhasil.

```
# telnet localhost
Trying 127.0.0.1…
telnet : unable to connect to remote host
Connection Refused
```

Jika proses instalasi berhasil akan ada pesan sbb.

```
# telnet localhost
Red Hat Linux release 9 (Shrike)
login: student
Password: ******
```

11. Telnet dan ftp dari komputer client ke server

Pertama-tama, buatkan user baru di komputer anda (sekarang berfungsi sebagai telnet dan ftp server) untuk rekan-rekan anda yang berada di sebelah kanan, kiri, depan dan belakang. Misalnya rekan yang duduk disekitar anda bernama agus dan budi, buatkan user dengan cara sbb.

```
# groupadd temanku
# useradd agus –g temanku
# passwd agus
# useradd budi –g temanku
# passwd budi
```

Berikan teman anda informasi tentang IP PC anda, username dan password untuk login ke komputer anda. Misalkan PC anda mempunyai IP 10.252.108.100, maka dari PC teman anda lakukan perintah sbb.

```
# ping 10.252.108.100   ---- cek konektivitas
```

```
# telnet 10.252.108.100
$ username : agus
$ passwd : ********
$ hostname            ---- catat hostnamenya
$ whoami
$ pwd                 ---- catat home direktorinya
$ finger              ---- catat siapa saja yang login
$ finger > dataku     ---- cek : boleh write ?
$ hostname > namapc
$ pwd
$ exit                ---- kembali ke PC client
```

Untuk melakukan ftp ke PC anda dari PC rekan anda, gunakan perintah .

```
# ping 10.252.108.100   ---- cek konektivitas
# telnet 10.252.108.100
$ username : budi
$ passwd : ********
```

12. Cek kerja dari ftp server anda dengan melakukan koneksi ftp ke server anda sendiri (localhost/hostname dari server anda) dengan menjalankan perintah :
#ftp localhost atau **#ftp** *nama_host_server.* Tuliskan pesan yang muncul.
_____
_____
_____

13. Login sebagai user yang telah anda buat/ nama user anda. Setelah itu ketikkan perintah >**help.** Tuliskan perintah-perintah tersebut.
Catatan: untuk melihat deskripsi perintah ftp jalankan perintah >help nama_perintah

14. Berdiskusilah dengan rekan-rekan disebelah anda, perintahkan rekan-rekan anda untuk melakukan telnet dan ftp ke PC anda.

    Misalkan PC anda mempunyai IP 10.252.108.100, maka perintahkan teman anda untuk mengupload filenya ke PC anda.

```
$ hostname          ---- catat namahostnya
$ cd                ---- kembali ke HOME
$ touch dataku datague mydata   --- buat filebaru
$ ls -l
$ ftp 10.252.108.100
ftp> username : agus
ftp> passwd : ********
ftp> hostname        ---- ada error ?
ftp> whoami          ---- ada error ?
ftp> pwd             ---- catat home direktorinya
ftp> finger          ---- ada error ?
ftp> mput *          ---- mengupload semua file
ftp> ls
```

```
ftp> bye              ---- kembali ke client
$ hostname
```

Jelaskan, mengapa perintah-perintah seperti hostname, whoami, finger, dll dapat berjalan di service telnet tetapi tidak dapat berfungsi di service ftp

15. Amatilah proses-proses yang terjadi di PC anda (server)

Ajaklah rekan anda untuk telnet dan ftp ke PC anda, dan amati dengan perintah :

```
# finger                --- amati hasilnya
# netstat
# netstat –a |grep telnet  --- amati hasilnya
# netstat –a |grep ftp     --- amati hasilnya
# cat /var/log/secure
```

Jelaskan apa fungsi dari perintah netstat ?
Informasi apa saja yang didapat dari file /var/log/secure ?

16. Lakukan beberapa kali percobaan dengan perintah telnet dan ftp, kemudian jelaskan secara detail, apa perbedaan antara telnet dan ftp

17. Mencoba anonymous ftp

Isilah direktori /var/ftp/pub dengan beberapa file agar dapat di-download oleh anonymous ftp user yang sedang terhubung ke PC anda.

```
# cd /var/ftp/pub
# echo “Ini komputerku, namanya” `hostname` > namapcku
# ifconfig > ip.komputerku
# touch filekosong1 filekosong2 filekosong3
# ls -l
```

Perintahkan rekan-rekan anda untuk ftp ke PC anda menggunakan account anonymous, kemudian download semua file di direktory pub

```
$ hostname          ---- catat namahostnya
$ cd                ---- kembali ke HOME
$ $ ls -l
$ ftp 10.252.108.100
ftp> username : anonymous
ftp> passwd : ********  --- masukkan email anda
ftp> hostname         ---- ada error ?
ftp> whoami           ---- ada error ?
ftp> pwd
ftp> ls
ftp> cd pub
ftp> ls
```

```
ftp> mget *      -- download semua file di direktori pub
ftp> bye              ---- kembali ke client
$ ls –l    --- apakah file sukses terdownload ?
$
```

Jelaskan secara detail, apa perbedaan antara user ftp dan anonymous ftp !

V. Laporan Resmi

Tulis hasil percobaan dan analisa hasilnya.

BAB VII
REMOTE ACCESS

I. Tujuan

1. Mahasiswa mampu melakukan konfigurasi SSH Server pada Linux
2. Mahasiswa mampu melakukan remote access berbasis text-mode dengan SSH menggunakan Windows dan Linux
3. Mahasiswa mampu melakukan konfigurasi Telnet Server pada Windows
4. Mahasiswa mampu melakukan remote access berbasis text-mode dengan Telnet menggunakan Windows dan Linux
5. Mahasiswa mampu melakukan konfigurasi Windows Remote Desktop Connection (RDC) pada Windows
6. Mahasiswa mampu melakukan remote access berbasis GUI dengan Windows RDC menggunakan Windows
7. Mahasiswa mampu melakukan konfigurasi Virtual Network Computing (VNC) pada Linux dan Windows
8. Mahasiswa mampu melakukan remote access berbasis GUI dengan VNC menggunakan Linux dan Windows

II. Perangkat yang digunakan

1. CD Linux Ubuntu 8.10
2. OpenSSH Server (openssh-server_5.1p1-3ubuntu1_i386.deb)
3. Putty (SSH-client pada windows)
4. Windows XP (dengan service RDC dan Telnet)
5. RealVNC (install pada Windows)
6. Kabel UTP Straight atau Cross
7. Switch

III. Dasar Teori

Remote access service (layanan akses jarah jauh) yaitu kombinasi perangkat keras dan lunak yang memungkinkan mengakses secara jarak jauh ke informasi atau perkakas yang berada pada suatu jaringan. RAS bekerja dengan beberapa protokol jaringan diantaranya TCP/IP, IPX, dan NBF. Untuk menggunakan RAS dari sebuah node jarak jauh, diperlukan sebuah program RAS untuk client misalnya yang ada disemua versi Windows atau di beberapa PPP client software.

Sejarah Perkembangan Remote Access

Di pertengahan tahun 1980 ketika PC mulai populer, banyak orang menyadari bahwa kemampuan untuk bertukar informasi antara satu komputer dengan komputer lain adalah sangat penting. Oleh karena itu lahirlah Local Area Network (LAN). Segera banyak perusahaan yang membuat LAN dengan kabel penghubung. Di sisi lain banyak perusahaan yang memiliki kantor cabang di tempat yang berjauhan sejak tahun 1990. Mereka pun

memikirkan bagaimana mereka dapat menghubungkan kantor-kantor tersebut menjadi satu agar dapat bertukar informasi. Seiring dengan PC yang semakin kecil dan mudah dikendalikan maka konsep untuk membawa PC ke rumah atau jalan menjadi kenyataan. Kemudian para pengguna PC itupun ingin agar saat bekerja dengan PC di rumah atau di jalan tetap memiliki berbagai kemampuan akses informasi seperti saat bekerja di kantor. Keinginan inilah yang didorong oleh implementasi LAN yang mulai baik menyebabkan lahirnya Remote Access.

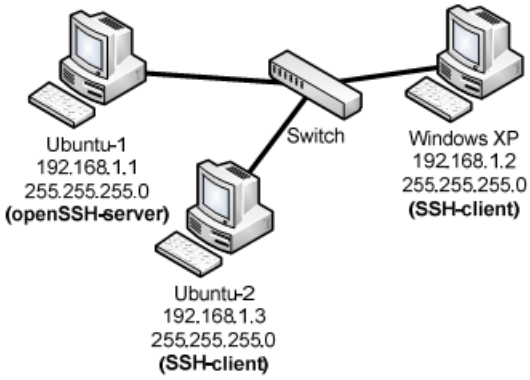
Siapa Yang Membutuhkan Remote Access.
Mengapa banyak perusahaan yang menerapkan Remote Access ? Ini semata-mata karena alasan bisnis.

- Perusahaan yang menerapkan Remote Access ini memiliki keunggulan kompetitif yakni dengan memberikan kemudahan bagi karyawan untuk mengakses informasi yang dianggap penting untuk kelancaran pekerjaan
- Remote Access memungkinkan karyawan bekerja di rumah. Ini membuat produktivitas meningkat karena dengan bekerja di rumah para karyawan merasa senang dan tenteram.
- Remote Access membuat karyawan memanfaatkan waktu kerjanya dengan optimal karena mereka tetap dapat bekerja meski di dalam mobil.
- Remote Access juga membuat karyawan lebih loyal karena mereka merasa lebih bebas dan tidak dipaksa bekerja di kantor.
- Remote Access menghemat ruang di kantor sehingga perusahaan dapat menghemat biaya pembangunan gedung.

IV. Percobaan

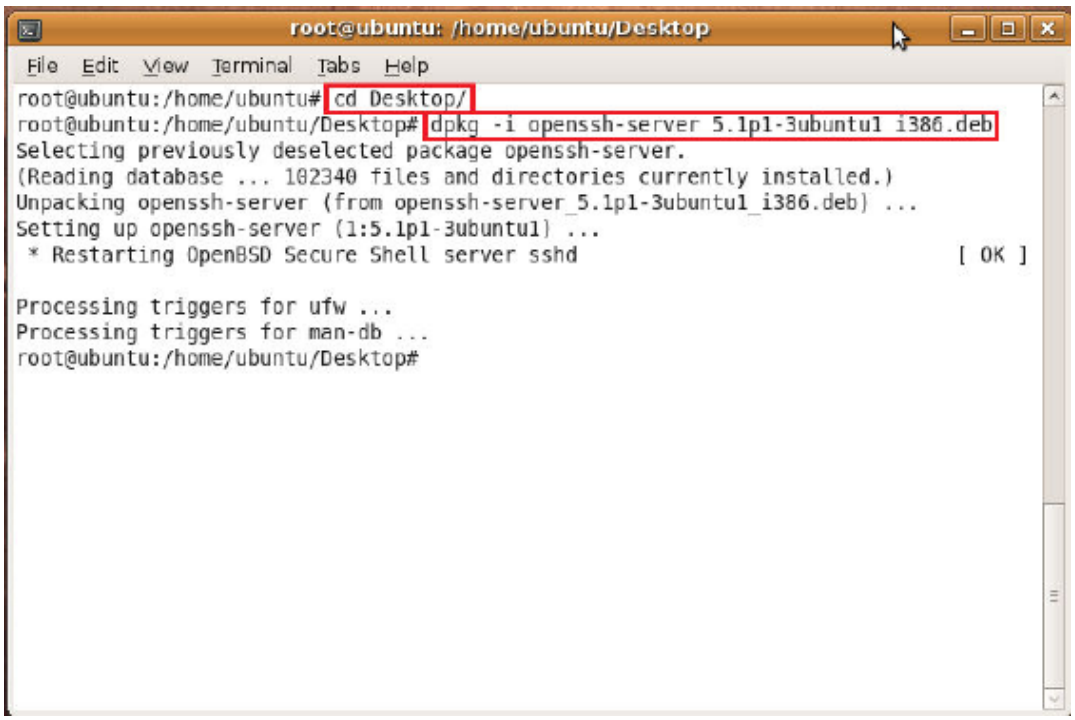
Melakukan konfigurasi SSH Server pada Linux (serta melakukan remote access berbasis text-mode dengan SSH menggunakan Windows dan Linux)

a. Berikut topologi yang akan dibuat

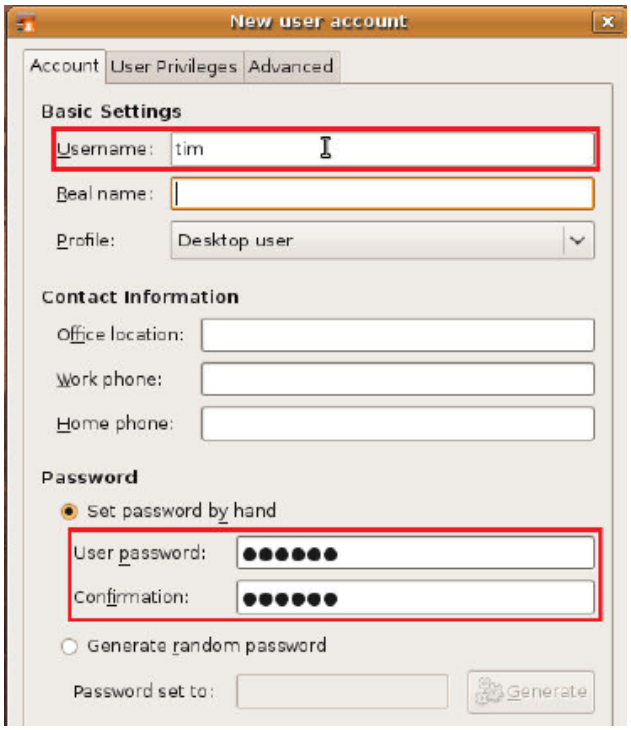


b. Salin file openssh-server_5.1p1-3ubuntu1_i386.deb pada Desktop di Ubuntu-1

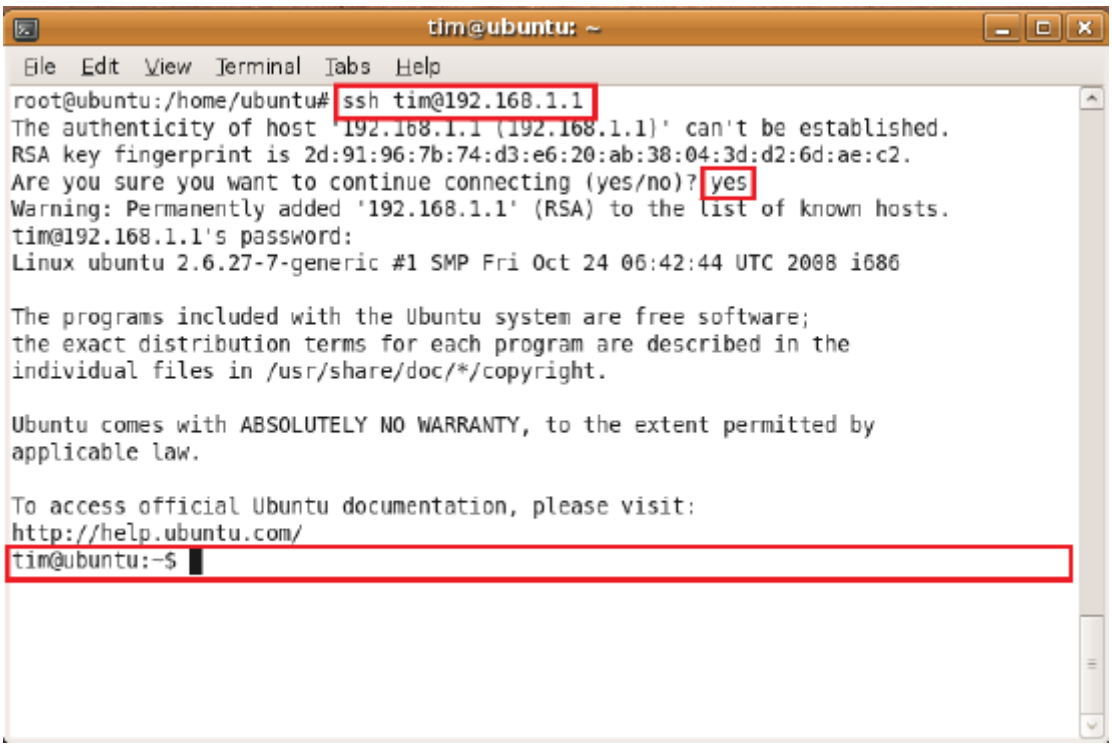
c. Lakukan proses instalasi openssh-server dengan menggunakan perintah “dpkg –i”



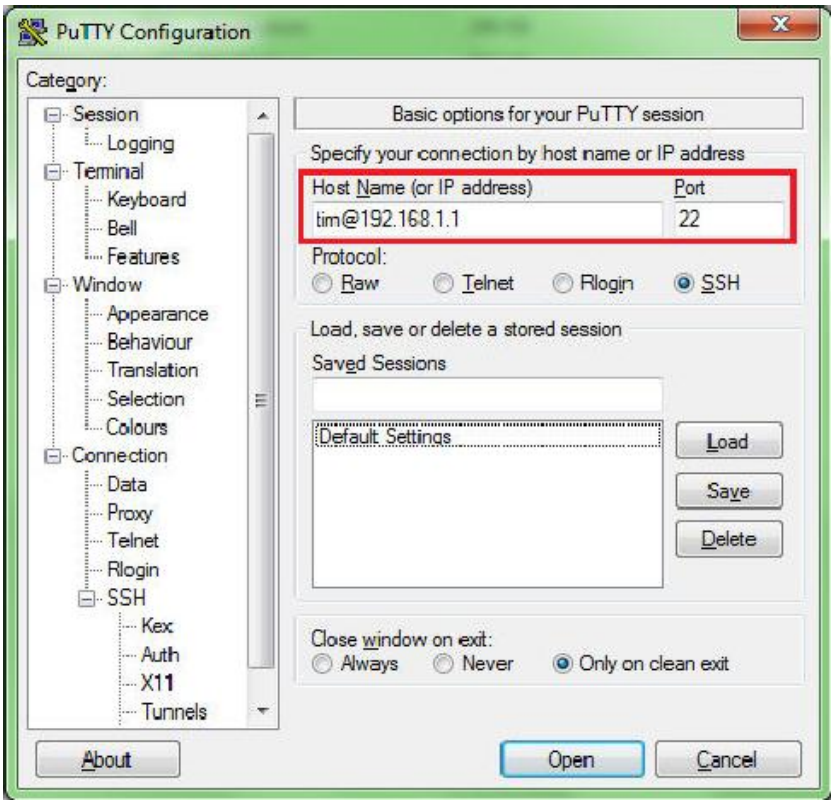
d. Tambahkan user untuk akses pada SSH-server

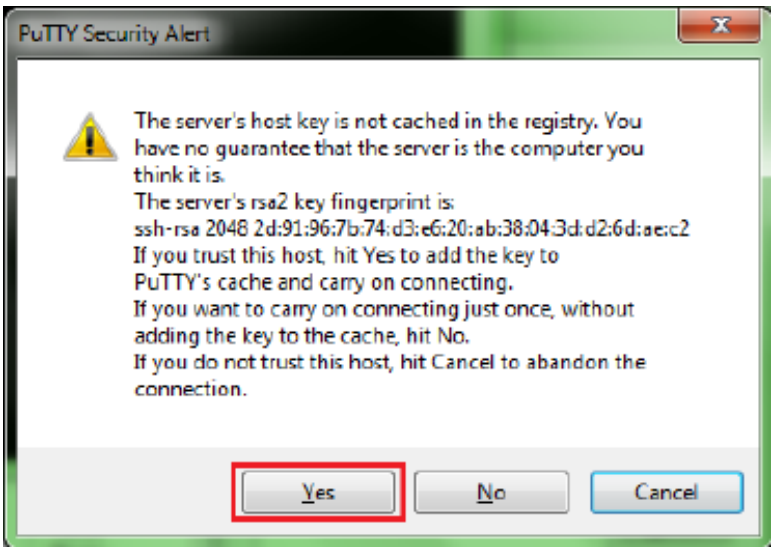


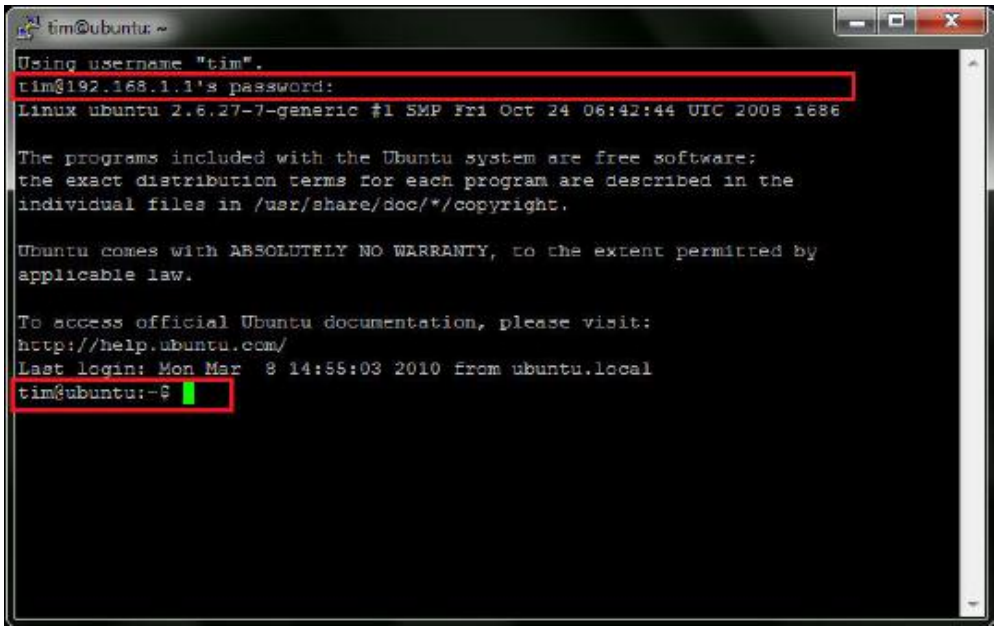
e. Akses SSH menggunakan Linux-client menggunakan perintah “ssh user@hostname/ip



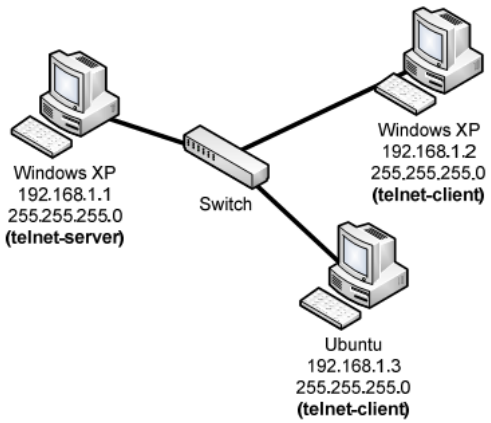
f. Akses SSH menggunakan putty di Windows-client



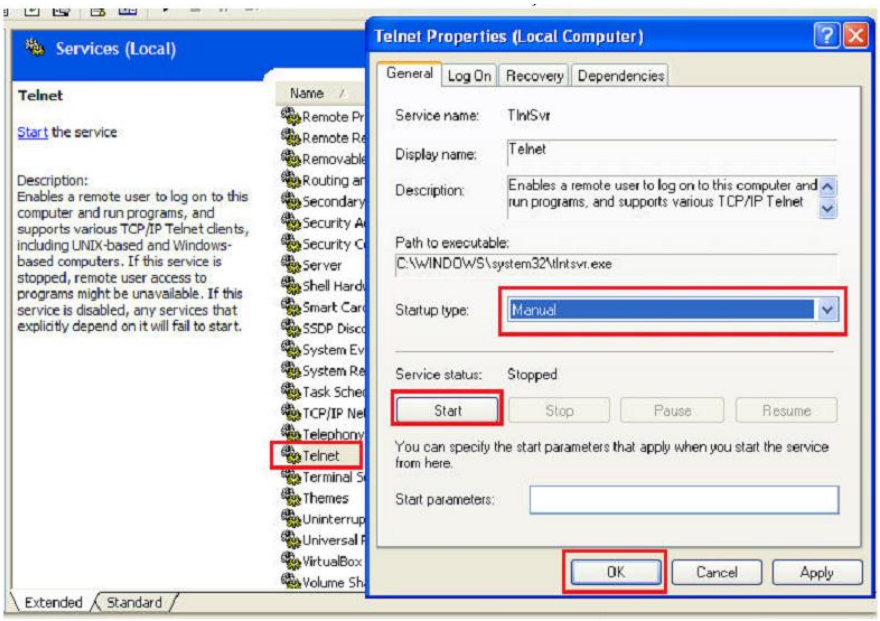




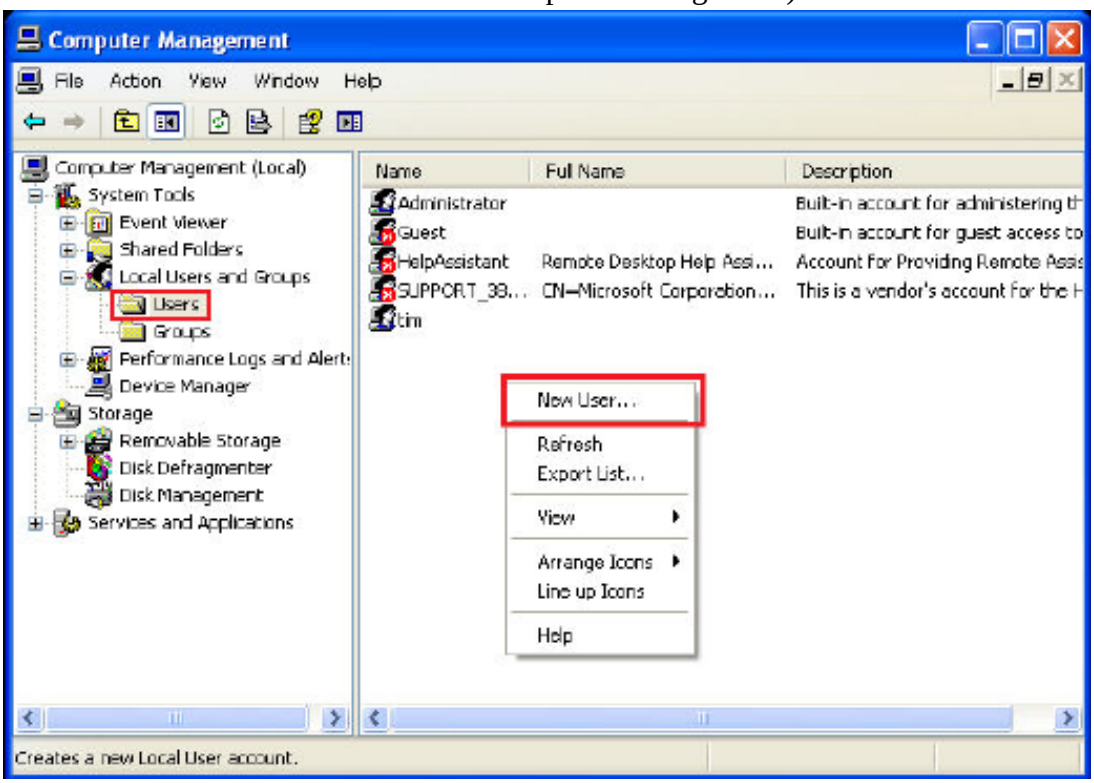
2. Melakukan konfigurasi Telnet Server pada Windows (serta melakukan remote access berbasis text-mode dengan Telnet menggunakan Windows dan Linux)
   a. Berikut topologi yang akan dibuat

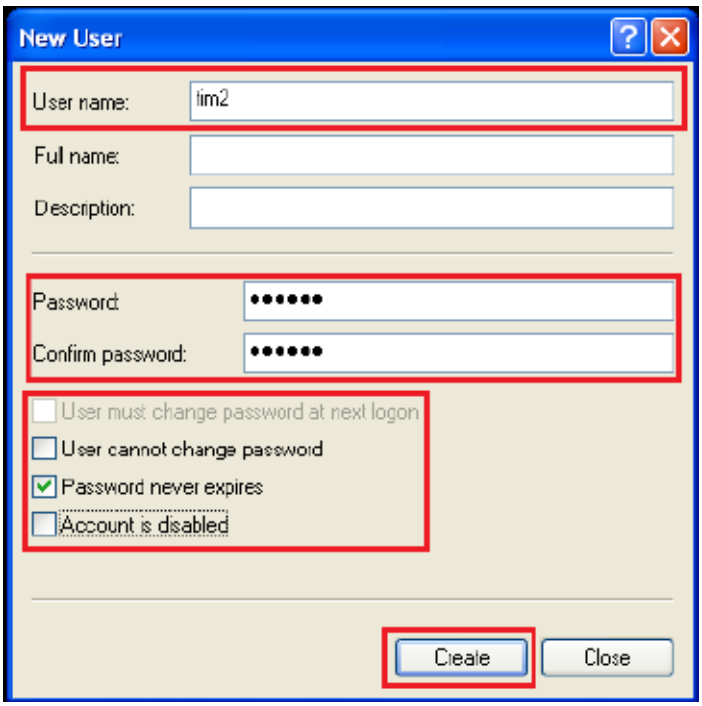


   b. Jalankan servis telnet pada telnet-server (untuk menjalankan service telnet dapat dilakukan melalui Start – Control Panel – Administrative Tools – Services)

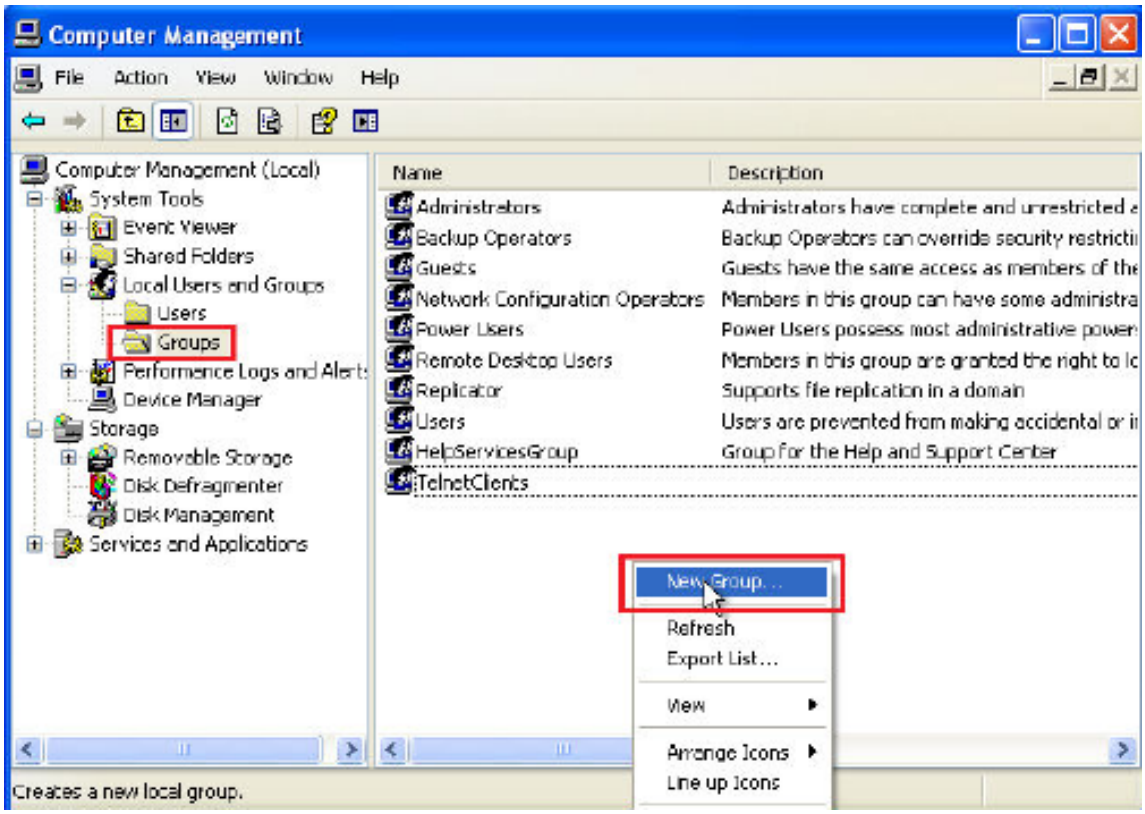


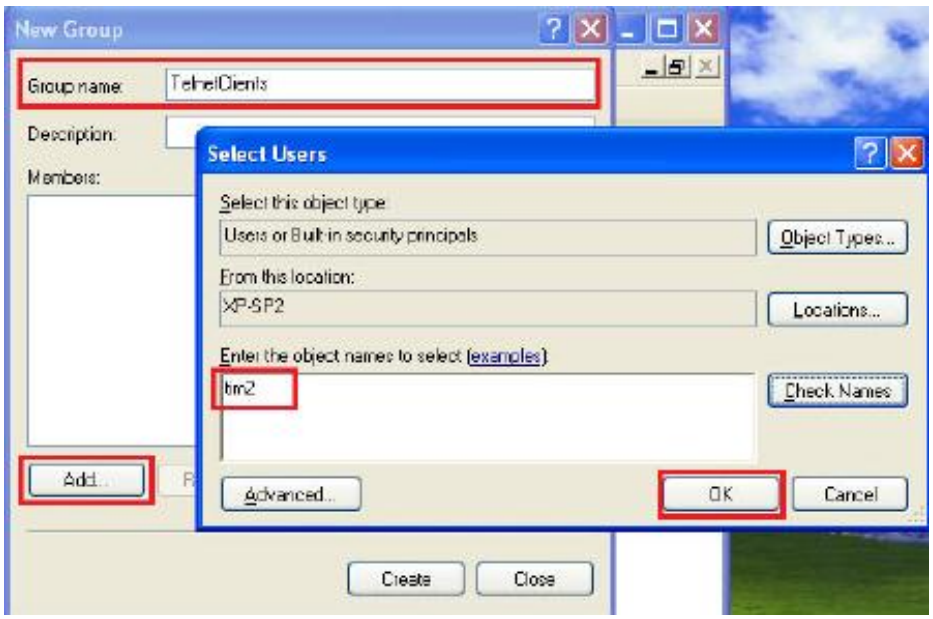
c. Tambahkan user baru pada Local Users and Groups (dapat diakses dari Start – Control Panel – Administrative Tools – Computer Management)



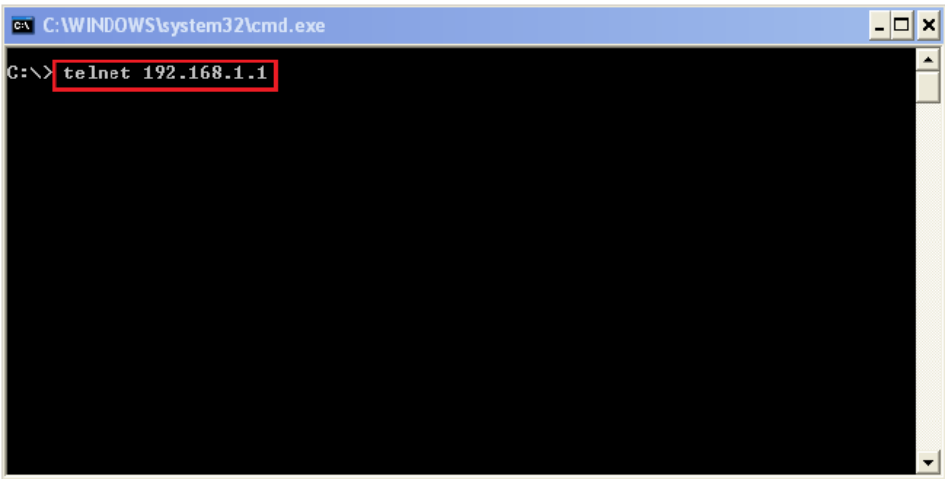


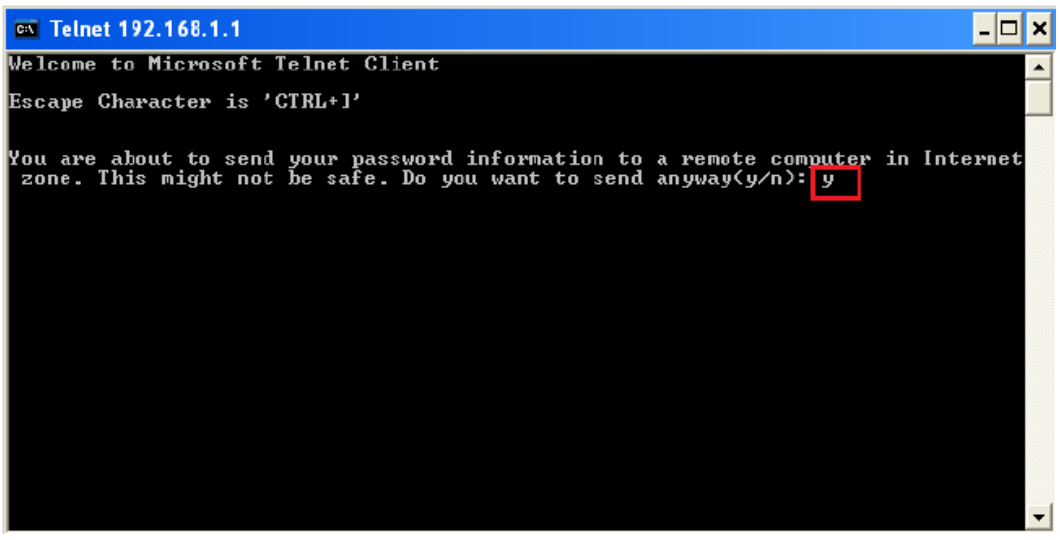
d. Tambahkan Group “TelnetClients” pada Local Users and Groups dan daftarkan user yang baru dibuat dalam group TelnetClients

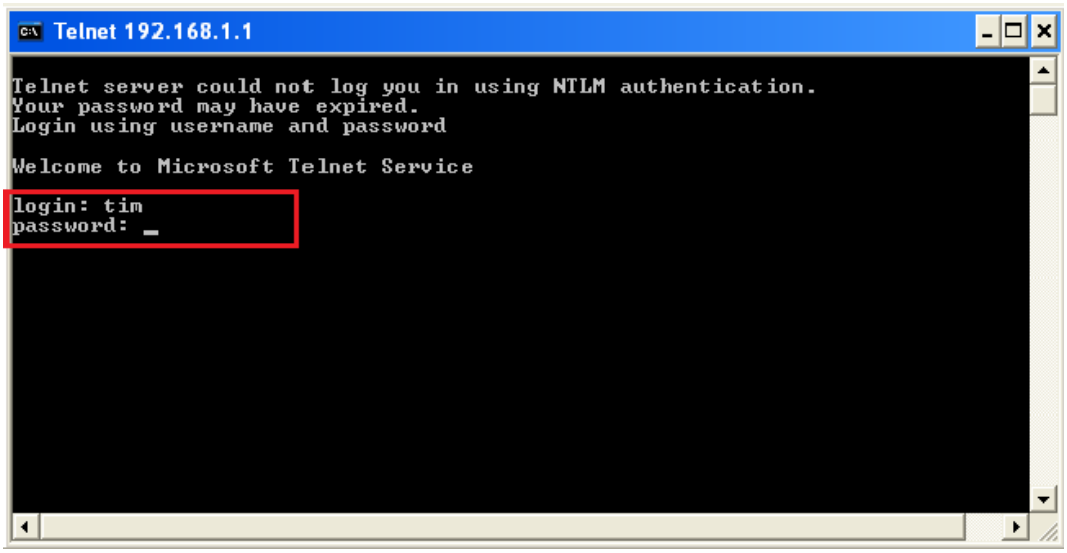


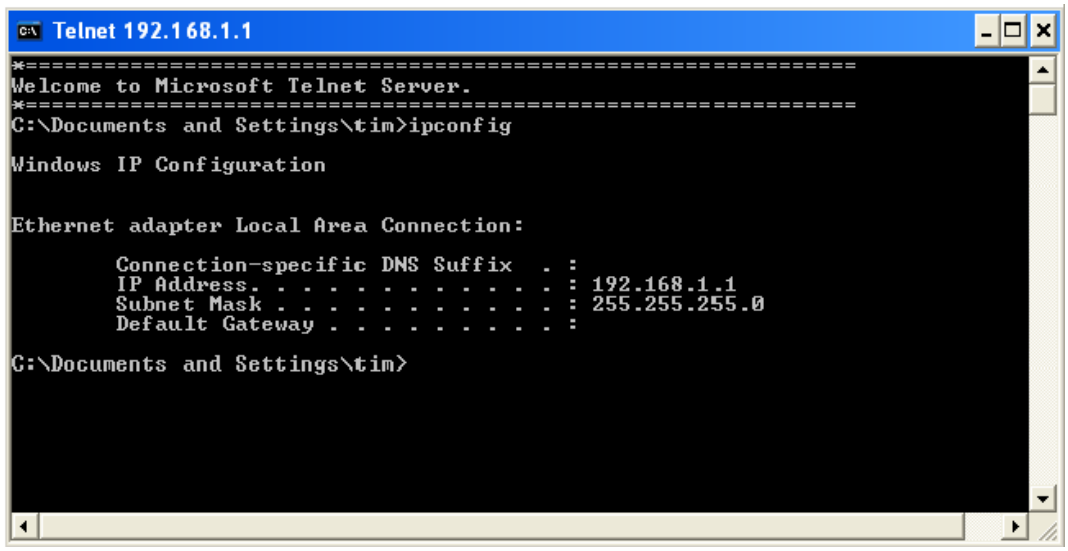


e. Akses telnet menggunakan telnet client pada Windows-client (akses telnet client melalui command prompt menggunakan perintah “telnet hostname/ip”)

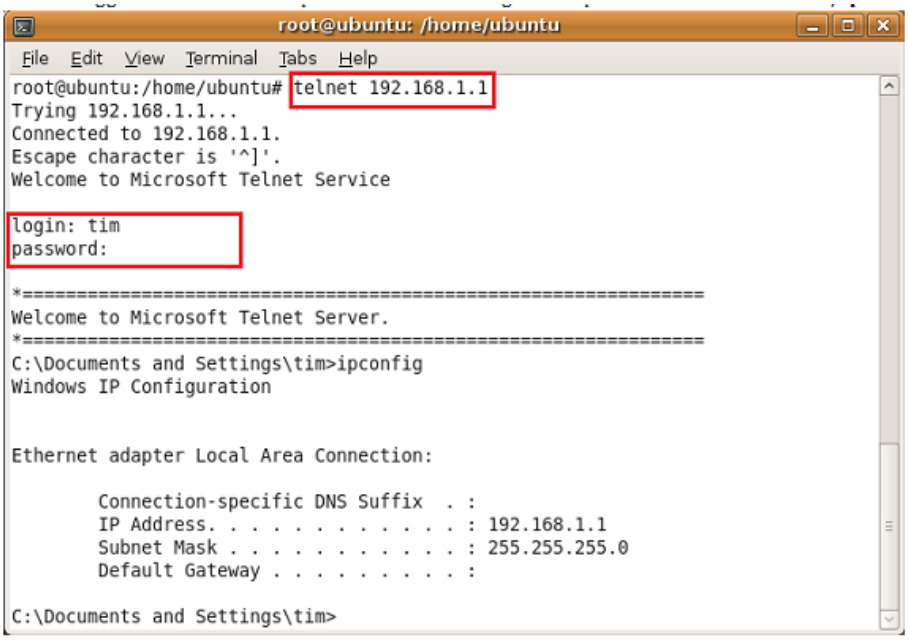






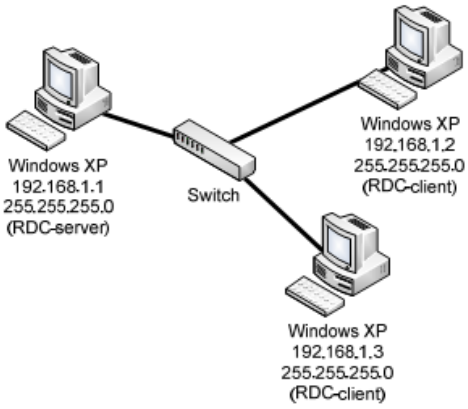


f. Akses menggunakan telnet client pada Linux-client mengunakan perintah “telnet hostname/ip”

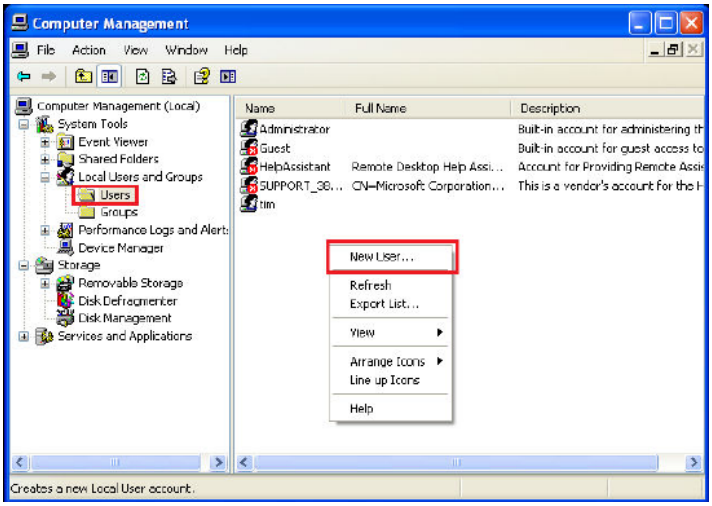


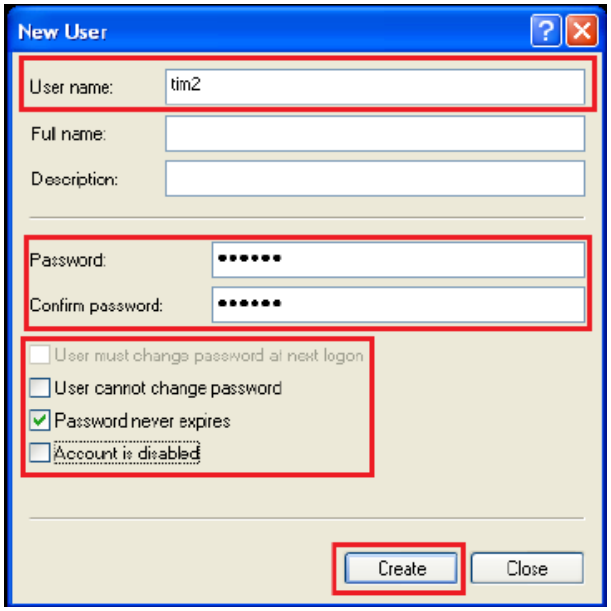
3. Melakukan konfigurasi RDC pada Windows (serta melakukan remote access berbasis GUI dengan RDC menggunakan Windows)

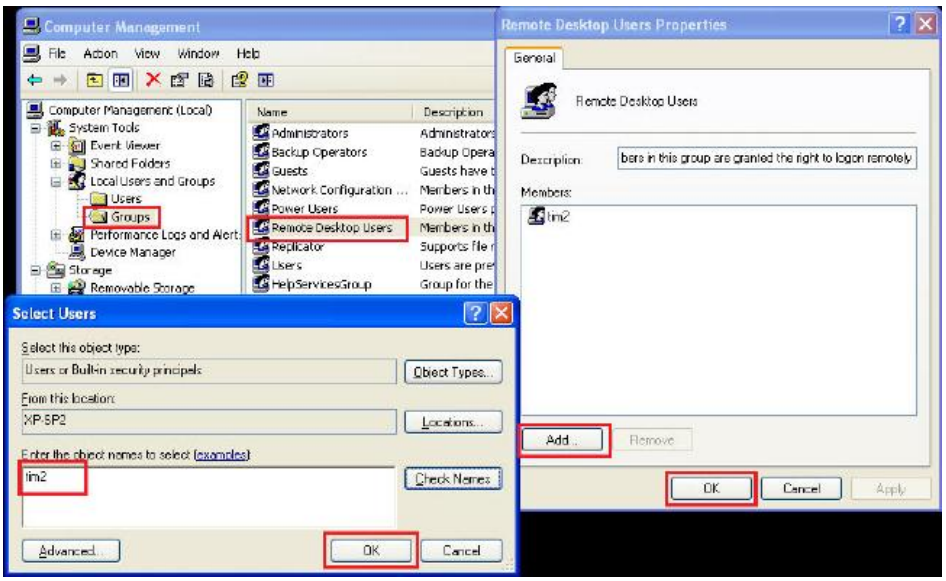
a. Berikut topologi yang akan dibuat



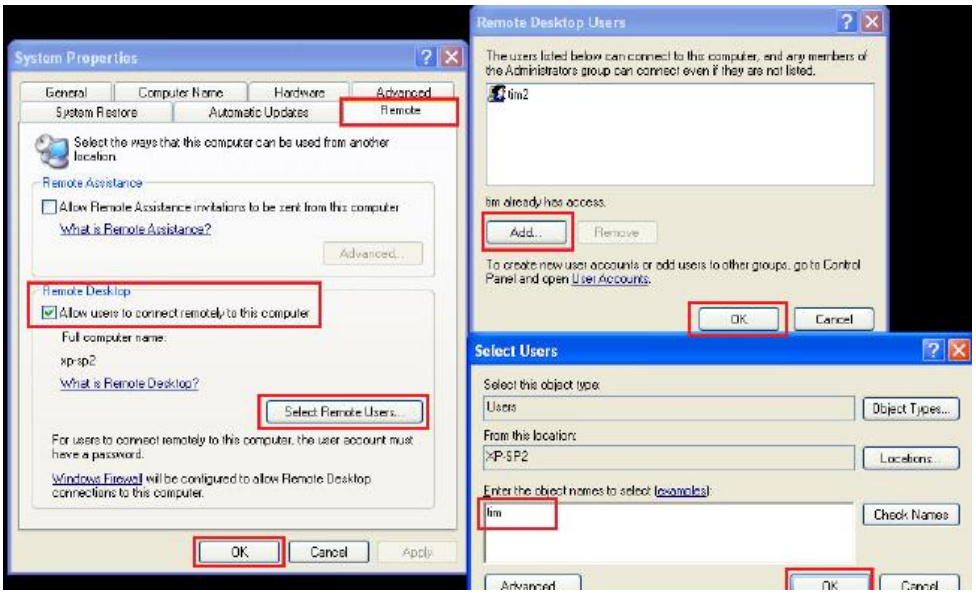
b. Tambahkan user baru untuk dimasukkan ke dalam group "Remote Desktop Users



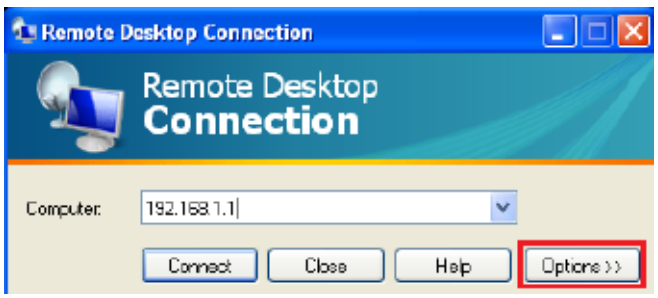


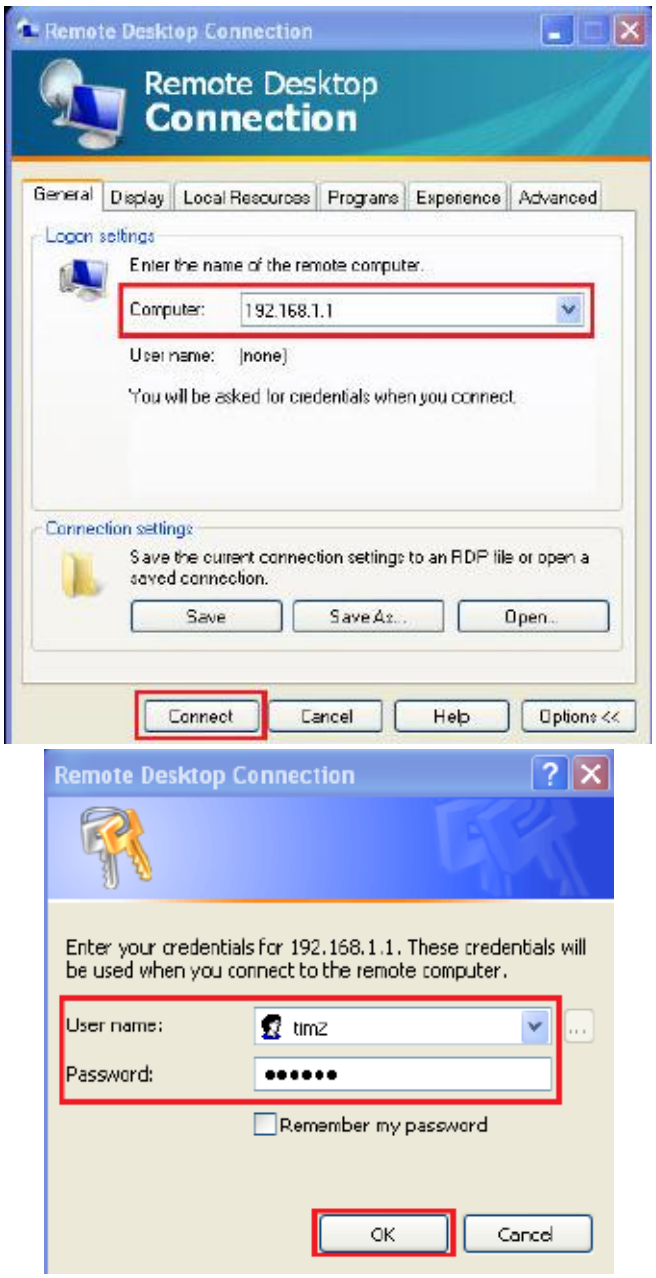


c. Aktifkan RDC dan tambahkan user yang ada dalam group Remote Desktop Users

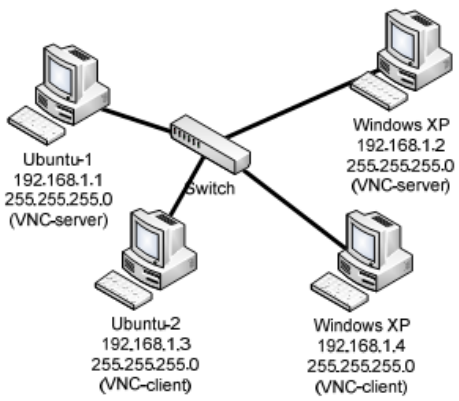


c. Akses RDC lewat windows-client (Remote Desktop Connection bisa diakses dari Start – All Programs – Accessories – Communications – Remote Desktop Connection)



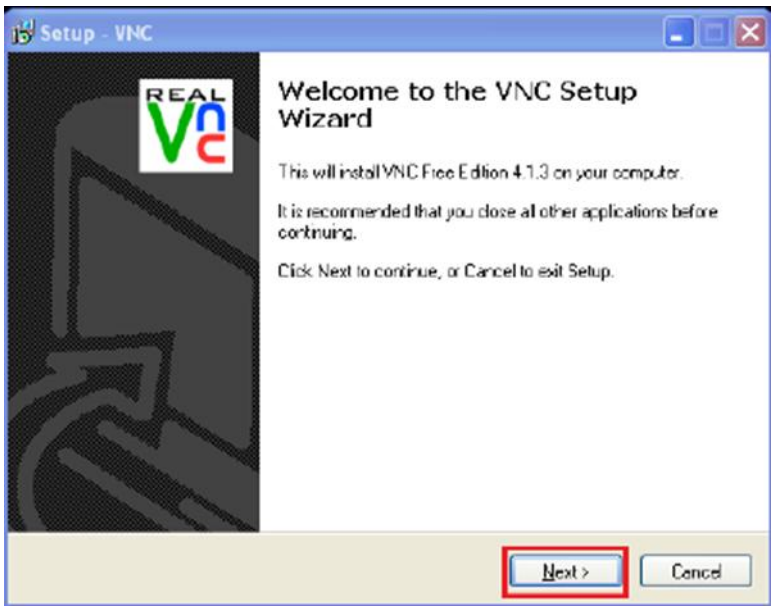


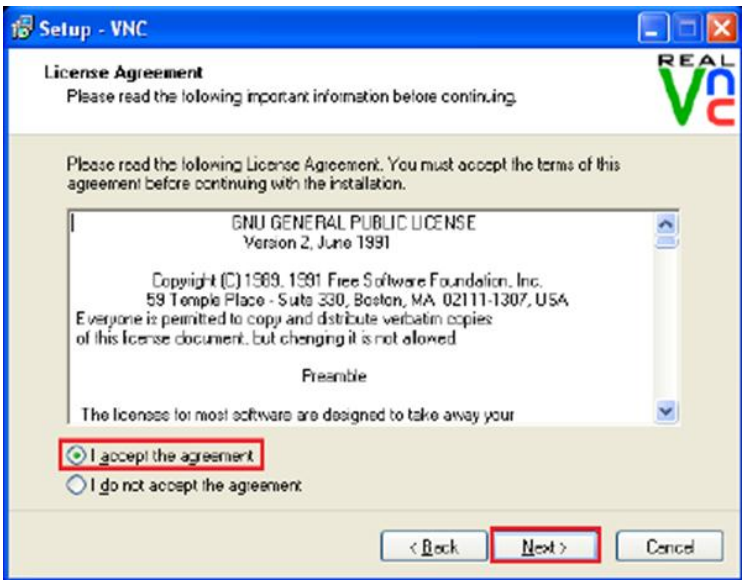
4. Melakukan konfigurasi VNC pada Windows dan Linux (serta melakukan remote access berbasis GUI dengan VNC menggunakan Windows)
   a. Berikut topologi yang akan dibuat

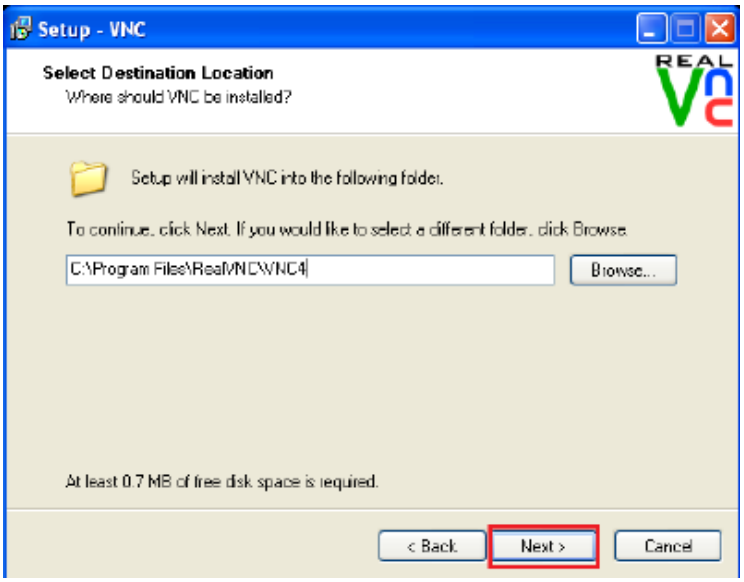


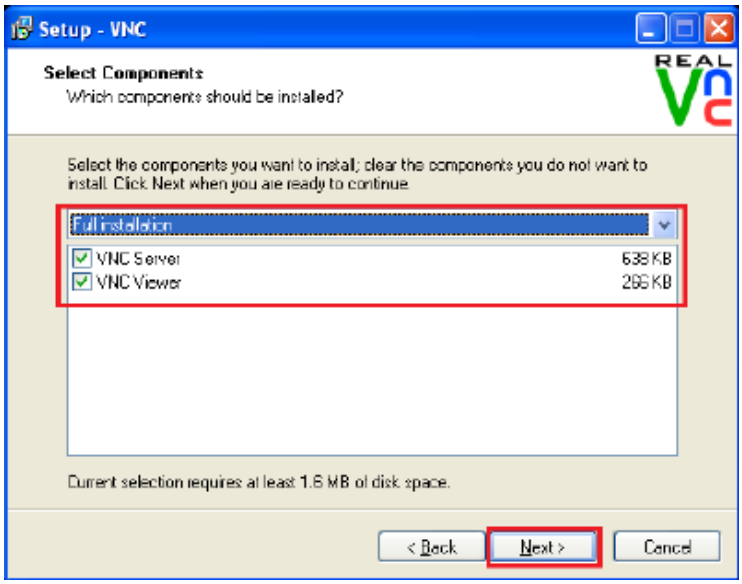
b. Aktifkan VNC Server pada Ubuntu (Remote Desktop Preferences dapat diakses dari System – Preferences – Remote Desktop)

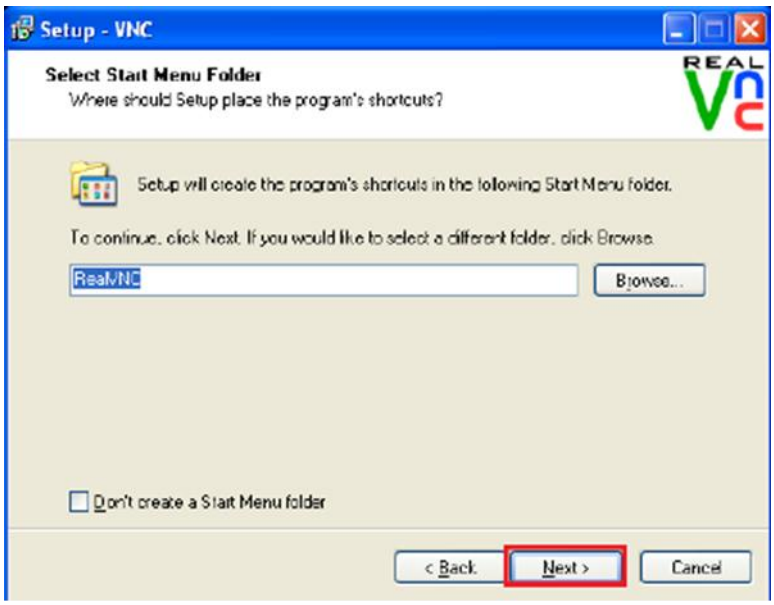
c. Aktifkan VNC Server pada Windows

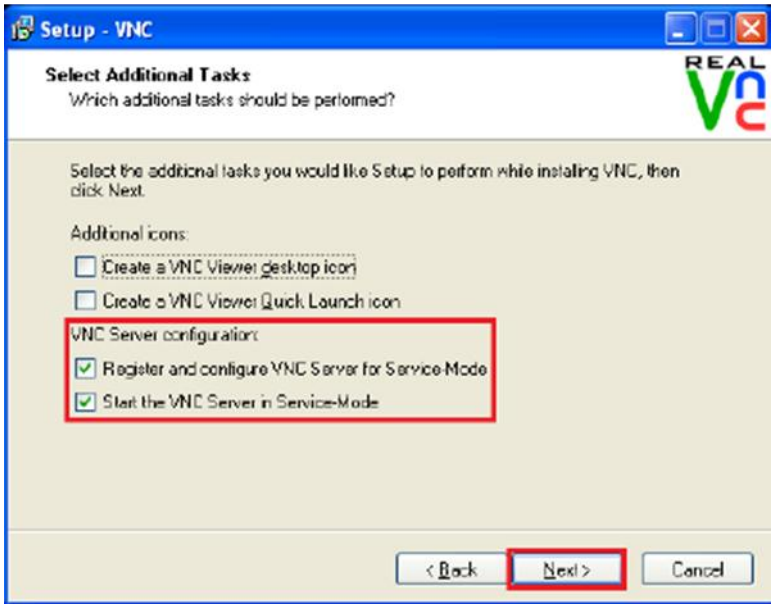


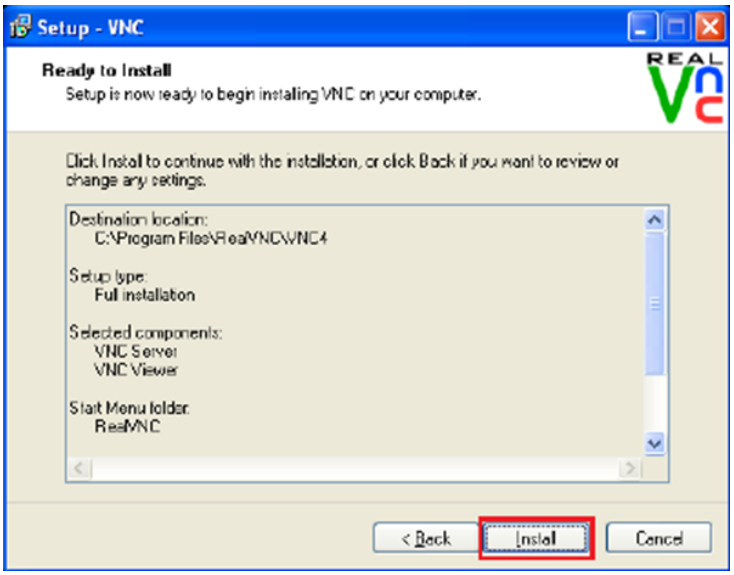

Setup - VNC
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

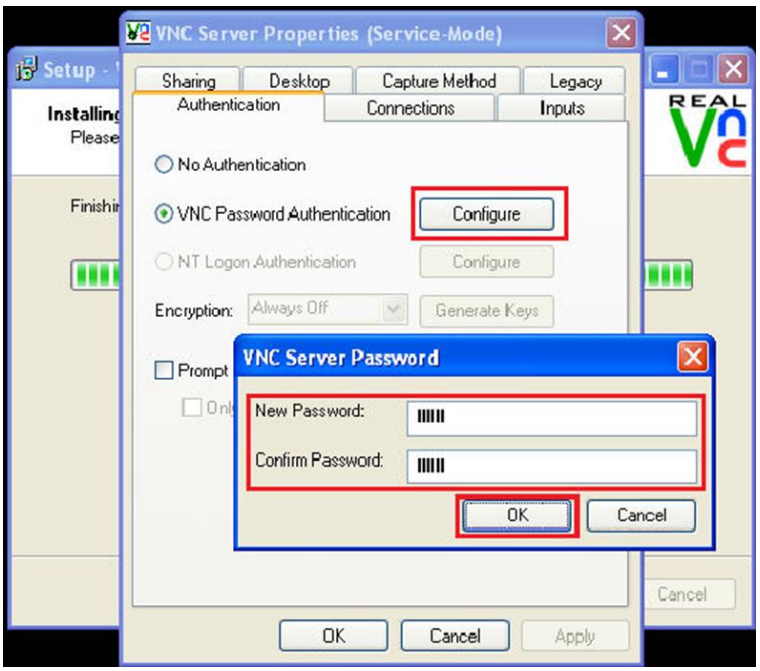

Setup - VNC
Select Destination Location
Where should VNC be installed?
Setup will install VNC into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\RealVNC\VNC4
Browse...
At least 0.7 MB of free disk space is required.
< Back
Next >
Cancel

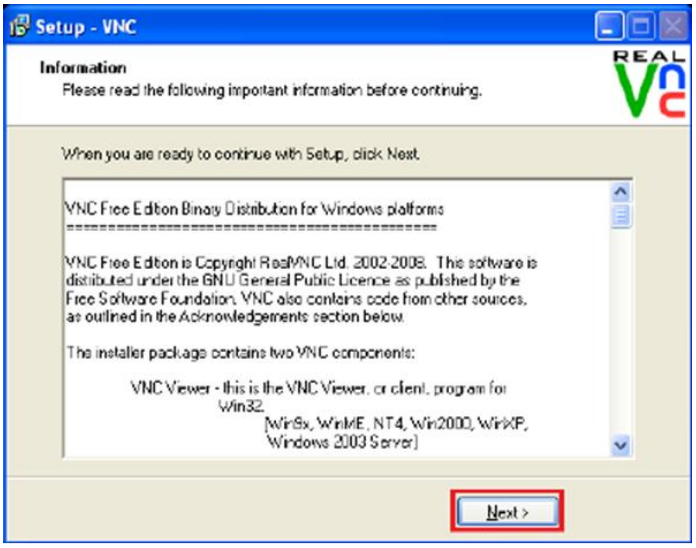

Setup - VNC
Select Components
Which components should be installed?
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Full installation
VNC Server 638 KB
VNC Viewer 266 KB
Current selection requires at least 1.6 MB of disk space.
< Back
Next >
Cancel

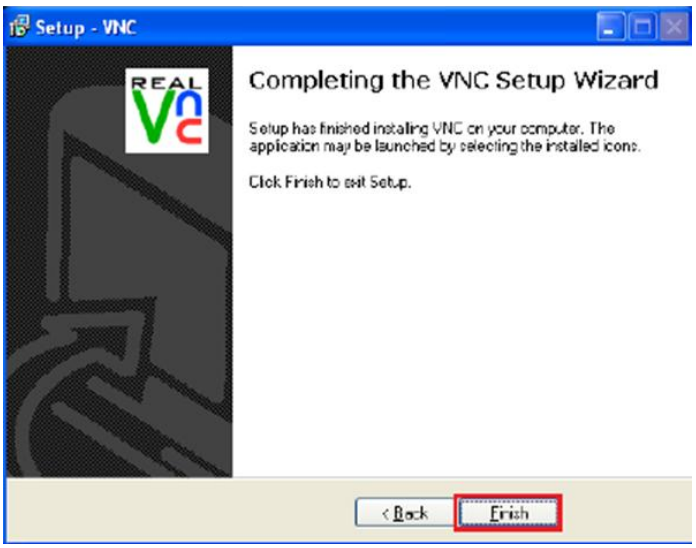

Setup - VNC
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
RealVNC
Browse...
Don't create a Start Menu folder
< Back
Next >
Cancel


Setup - VNC
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing VNC, then click Next.
Additional icons:
Create a VNC Viewer desktop icon
Create a VNC Viewer Quick Launch icon
VNC Server configuration:
Register and configure VNC Server for Service Mode
Start the VNC Server in Service Mode
< Back
Next >
Cancel

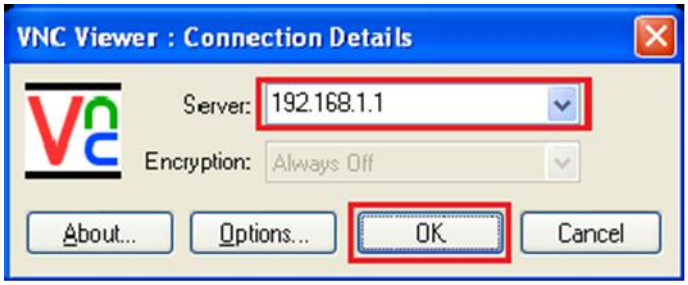

Setup - VNC
Ready to Install
Setup is now ready to begin installing VNC on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\RealVNC\VNC4
Setup type:
Full installation
Selected components:
VNC Server
VNC Viewer
Start Menu folder:
RealVNC
< Back
Install
Cancel

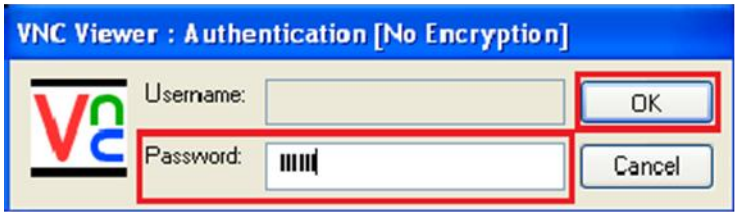


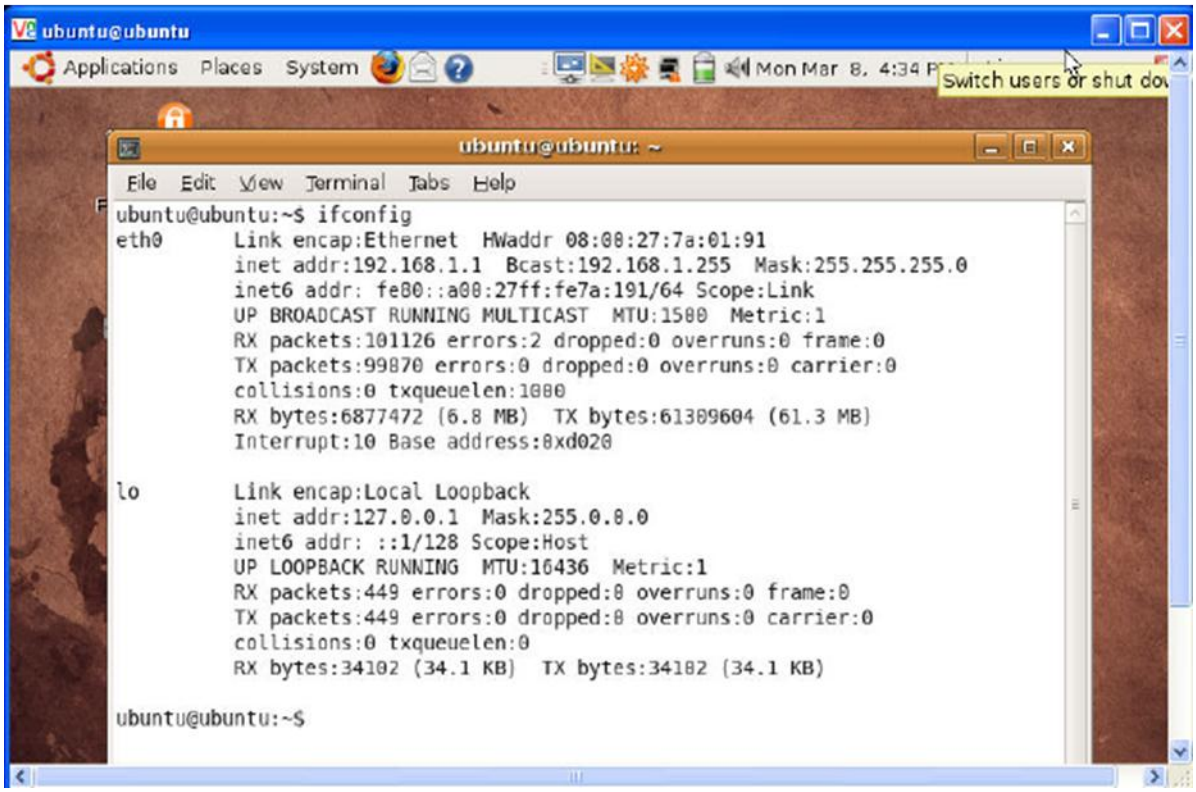




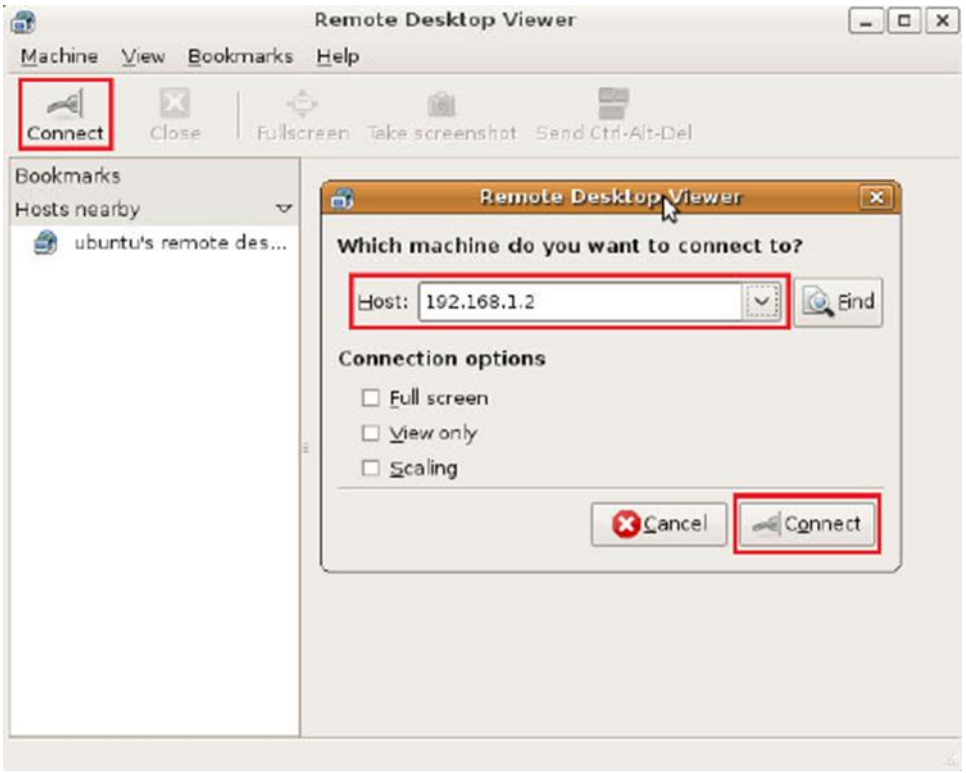
d. Akses melalui VNC Viewer pada windows-client (VNC Viewer dapat diakses dari Start – All Programs – RealVNC – VNC Viewer 4 – Run VNC Viewer)

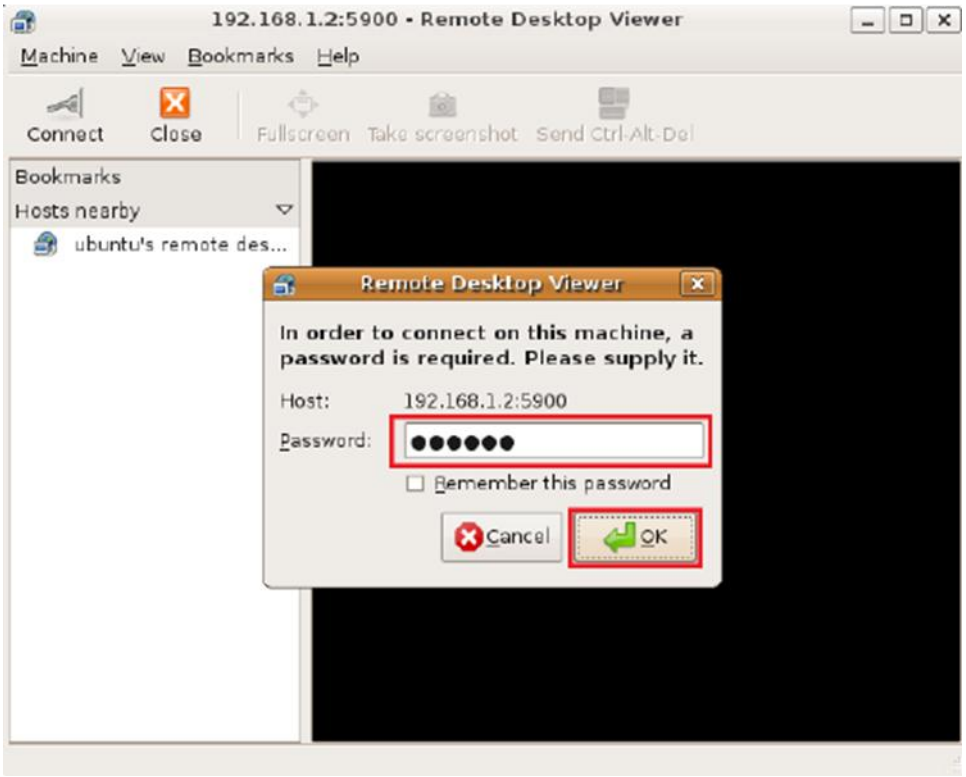

VNC Viewer : Connection Details
Server:
192.168.1.1
Encryption:
Always Off
About...
Options...
OK
Cancel

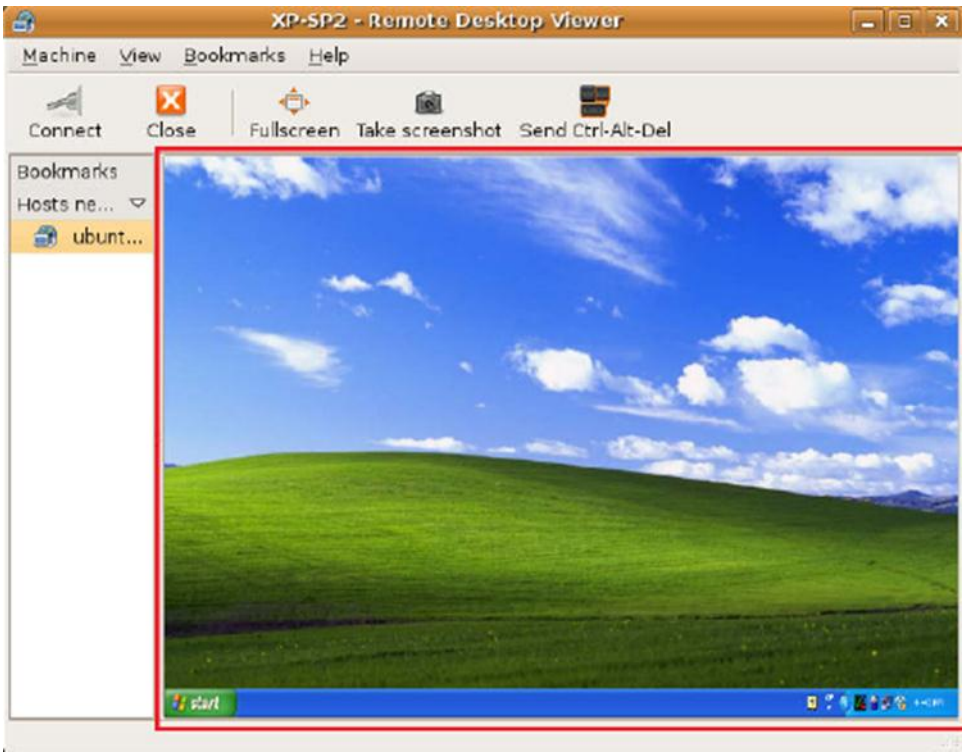

VNC Viewer : Authentication [No Encryption]
Username:
Password:
OK
Cancel


ubuntu@ubuntu
Applications
Places
System
Mon Mar 8, 4:34
Switch users or shut do
ubuntu@ubuntu: ~
File Edit View Terminal Tabs Help
ubuntu@ubuntu:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:7a:01:91
inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe7a:191/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:101126 errors:2 dropped:0 overruns:0 frame:0
TX packets:99870 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6877472 (6.8 MB) TX bytes:61309604 (61.3 MB)
Interrupt:10 Base address:0xd020
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:449 errors:0 dropped:0 overruns:0 frame:0
TX packets:449 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:34102 (34.1 KB) TX bytes:34102 (34.1 KB)
ubuntu@ubuntu:~$

e. Akses melalui Remote Desktop Viewer pada Linux (Remote Desktop Viewer dapat diakses pada Applications – Internet – Remote Desktop Viewer)







V. Laporan Resmi

a. Tulis hasil percobaan dan analisa hasilnya.

BAB VIII
SECURE SHELL, SECURE COPY DAN SECURE FTP

I. Tujuan

1. Mahasiswa dapat memahami penggunaan service secure shell, secure copy dan secure ftp pada sistem operasi unix/linux
2. Mahasiswa mampu melakukan instalasi dan konfigurasi ssh untuk meningkatkan keamanan data
3. Mahasiswa memahami kelebihan penggunaan secure shell dibanding service telnet, ftp dan perintah remote lainnya

II. Dasar Teori

Secure Shell & Secure FTP

Secure Shell (ssh) adalah suatu protokol yang memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur client/server, serta memungkinkan seorang user untuk login ke server secara remote. Berbeda dengan telnet dan ftp yang menggunakan plain text, SSH meng-enkripsi data selama proses komunikasi sehingga menyulitkan intruder yang mencoba mendapatkan password yang tidak dienkripsi. Fungsi utama aplikasi ini adalah untuk mengakses mesin secara remote. Bentuk akses remote yang bisa diperoleh adalah akses pada mode teks maupun mode grafis/X apabila konfigurasinya mengijinkan

SSH dirancang untuk menggantikan service-service di sistem unix/linux yang menggunakan sistem plain-text seperti telnet, ftp, rlogin, rsh, rcp, dll). Untuk menggantikan fungsi ftp dapat digunakan sftp (secure ftp), sedangkan untuk menggantikan rcp (remote copy) dapat digunakan scp (secure copy).

Dengan SSH, semua percakapan antara server dan klien di-enkripsi. Artinya, apabila percakapan tersebut disadap, penyadap tidak mungkin memahami isinya. Bayangkan seandainya Anda sedang melakukan maintenance server dari jauh, tentunya dengan account yang punya hak khusus, tanpa setahu Anda, account dan password tersebut disadap orang lain, kemudian server Anda dirusak setelahnya.

Implementasi SSH yang banyak dipakai saat ini adalah OpenSSH, aplikasi ini telah dimasukkan kedalam berbagai macam distribusi linux. Redhat Linux versi 9 sudah menyediakan program tersebut dalam format RPM.

Fitur-fitur SSH

Protokol SSH menyediakan layanan sbb.:

- Pada saat awal terjadinya koneksi, client melakukan pengecekan apakah host yang dihubungi sudah terdaftar pada client atau tidak

- Client mengirimkan proses autentifikasi ke server menggunakan teknik enkrisp 128 bit
- Semua data yang dikirimkan dan diterima menggunakan teknik enkripsi 128 bit sehingga sangat sulit u dibaca tanpa mengetahui kode enkripsinya
- Client dapat memforward aplikasi Xwindows / X11 ke server, layanan ini disebuat

III. Tugas Pendahuluan

1. Apa kelebihan secure shell dibanding perintah telnet, ftp dan perintah remote lainnya
2. Sistem enkripsi apa yang digunakan oleh program ssh pada Redhat Linux 9
3. Jelaskan bagaimana program ssh bekerja pada sistem jaringan client/server

IV. Percobaan

1. Login ke sistem Linux sebagai root
2. Cek apakah konfigurasi alamat IP untuk host.
   a. Jalankan perintah **ifconfig**, tulis konfigurasi IP host anda.
      Interface : _____
      IP Address : _____
      Subnet mask : _____
   b. Jalankan perintah netstat –r, tuliskan default gateway host anda.
      Default Gateway :

3. Untuk menjalankan service ssh pada server diperlukan paket program yang bernama openssh-server-xxx.rpm, sedangkan pada PC client diperlukan program openssh-clients-xxx.rpm.
   Cek apakah program kedua program tersebut sudah terinstall atau belum. Jika sudah, langsung kerjakan langkah nomer 8.
   a. Jalankan perintah **rpm –qa | grep openssh**, tulis hasilnya
   b. Ada berapa banyak program openssh yang terinstall di PC anda ?
   c. Apakah sudah ada program openssh-server ?
      Jalankan perintah **rpm –qa | grep openssh-server** , tulis hasilnya

4. Jika program openssh-server dan openssl-client belum ada, installah dengan cara sbb. Masukkan CD Rom Redhat dan ketiklah perintah berikut ini.

```
# mount  /dev/cdrom  /mnt/cdrom
# cd /mnt/cdrom
# ls –l
# cd RedHat
# ls –l
# cd RPMS
# ls –l openssh*
```

5. Jika tidak ditemukan openssh-server-xxxx.rpm atau openssh-client.rpm (xxx = nomer versi) gantilah dengan CD yang lain. Jika anda tidak membawa CD Redhat Linux, anda bisa mendownloadnya di ftp server.

```
# cd                    -- ke home direktori
# ping 10.252.105.101       -- cek konektivitas
# ftp 10.252.105.101
Connected to host8.
220 (vsFTPd 1.1.3)
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (localhost:root): anonymous
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
ftp> cd pub
ftp> ls                -- lihat isi direktori pub
ftp> bin               -- mode binary file
ftp> mget openssh*       -- ketik yes untuk download
ftp> bye               -- keluar dari ftp server
#
```

6. Instalasi program ssh

```
# rpm –ivh openssh-server*.rpm
# rpm –ivh openssh-clients*.rpm
```

7. Catatlah di direktori mana saja program openssh-server diinstall.

```
# rpm –ql openssh-server
```

   a. Dimana binary/executeble file program shh berada ?
   b. Dimana file konfigurasi ssh berada ?
   c. Bacalah manual dari program ssh server

```
# man sshd
```

   d. Bacalah semua informasi yang ada di file konfigurasi ssh server

```
# more /etc/ssh/sshd_config
# man sshd_config
```

8. Catatlah di direktori mana saja program openssh-clients diinstall.

```
# rpm –ql openssh-clients
```

   a. Catatlah semua binary/executable file yang terinstall
   b. Dimana file konfigurasi ssh client berada ?
   c. Baca dan pahamilah manual dari program-program ssh client berikut ini

```
# man ssh
# man scp
# man sftp
# man slogin
```

   Jelaskan apa fungsi atau kegunaan dari masing-masing service ssh, scp, sftp dan slogin

   d. Bacalah semua informasi yang ada di file konfigurasi ssh client

```
# more /etc/ssh/ssh_config
# man ssh_config
```

9. Mengaktifkan service ssh server

   Untuk menjalankan service ssh service gunakan perintah

   ```
   # /etc/rc.d/init.d/sshd start
   ```

   Untuk mematikan services gunakan perintah :

   ```
   # /etc/rc.d/init.d/sshd stop
   ```

   Untuk menjalankan ulang services gunakan perintah :

   ```
   # /etc/rc.d/init.d/sshd restart
   ```

10. Memeriksa proses sshd

    Setelah program sshd (ssh daemon) dijalankan, periksalah apakah sshd sudah aktif di memory.

    ```
    # ps –aux | grep sshd
    ```

    Catatlah, berapa nomer proses sshd di pc anda.

    ```
    # netstat –a | grep ssh
    ```

    Protokol apa yang digunakan oleh program ssh ?

11. Catatlah berapa nomer port yang digunakan oleh service ssh

    ```
    # cat /etc/services | grep ssh
    ```

    Berapa nomer port yang digunakan oleh service ssh ?

12. Menghapus rule firewall

    Redhat Linux versi 8 atau yang lebih baru, akan mengaktifkan firewall secara default sehingga semua akses dari luar akan ditolak. Untuk kepentingan percobaan ini, ada baiknya untuk sementar semua rule firewall dihapus. Gunakan perintah :

    ```
    # iptables -F
    ```

13. Uji coba dari localhost

    Untuk menguji coba apakah ssh server sudah berfungsi dengan baik gunakan perintah :

    ```
    # ssh localhost
    The authenticity of host 'localhost (127.0.0.1)' can't be established.
    RSA key fingerprint is 82:0a:7f:f3:f3:5c:cf:87:db:a0:4d:b6:ce:20:26:1c.
    Are you sure you want to continue connecting (yes/no)? yes
    Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
    root@localhost's password: *******
    Last login: Wed May  5 08:46:13 2004
    #
    ```

    Jika anda ssh ke localhost dan terdapat pesan seperti diatas, maka ssh server sudah dapat berfungsi dengan baik.

Misalkan sshd sedang dalam keadaan tidak aktif, maka jika ada permintaan service ssh akan ditolak oleh server.

```
# /etc/rc.d/init.d/sshd stop      -- mematikan service
Stopping sshd:  OK  ]
# ssh localhost
ssh: connect to host localhost port 22: Connection refused          -- koneksi ssh ditolak
#
# /etc/rc.d/init.d/sshd start
```

14. Percobaan kelompok

Percobaan-percobaan yang ada dibawah ini dilakukan secara berpasangan (2 orang). Sebelum memulai percobaan, buatlah user baru sbb. :

```
# useradd userkiri
# passwd userkiri
# useradd userkanan
# passwd userkanan
```

Keterangan : userkiri digunakan untuk user yang duduk di sebelah kiri, dan userkanan untuk user yang duduk di sebelah kanan. Jangan lupa beritahu pasangan anda password yang sudah anda tentukan.

Setelah itu editlah file /etc/hosts sbb. :

```
# cp /etc/hosts /etc/hosts.asli    -- backup file
# vi /etc/hosts                    -- edit file
----- tambahkan di baris paling akhir

127.0.0.1       localhost.localdomain   localhost
ip_pc_anda      nama_pc_anda
ip_pc_sebelah   nama_pc_sebelah
```

Contoh : Misalkan ip anda 10.252.105.111 dan anda duduk dikiri maka anda dapat mengisi file /etc/hsts sbb. :

```
# vi /etc/hosts                    -- edit file
----- tambahkan di baris paling akhir
127.0.0.1       localhost.localdomain   localhost
10.252.105.111  pckiri
10.252.105.112  pckanan
```

Setelah itu lakukan pengecekan konektifitas

```
# ping 10.252.105.111   ---- cek konektivitas
# ping pckiri
# ping 10.252.105.112   ---- cek konektivitas
# ping pckanan
```

15. Mencoba ssh server

Jika anda duduk di kiri, ketiklah perintah berikut ini. Jika anda duduk sebelah kanan, sesuaikan dengan perintah sejenis.

```
# hostname                -- catat nama hostnya
# ssh pckanan –l userkiri
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is 82:0a:7f:f3:f3:5c:cf:87:db:a0:4d:b6:ce:20:26:1c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
userkiri@pckanan's password: *******
Last login: Wed May  5 08:46:13 2004
$ whoami
$ finger          -- ada berapa orang yang login ?
$ hostname        -- skr anda ada dimana ?
$ pwd             -- dimana home direktory anda ?
$ exit
# hostaname       -- kembali ke pc asal
```

Setiap anda melakukan ssh ke remote PC, dimanakah home direktori anda ?

Apakah anda dapat berpindah atau masuk ke direktori /etc, /var, /bin, /usr, /home ?

Direktori apa saja yang tidak dapat anda masuki ?

16. Mencoba service sftp

Perintah-perintah berikut ini akan berhubungan dengan service sftp. Jika anda duduk di kiri, ketiklah perintah berikut ini. Jika anda duduk sebelah kanan, sesuaikan dengan perintah sejenis.

```
# hostname                -- catat nama hostnya
# su –l userkiri          -- mengganti user
$ pwd                     -- home dir. userkiri
$ whoami
# sftp pckanan
  userkiri@pckanan's password: *******
  Last login: Wed May  5 08:46:13 2004
sftp> whoami
sftp> finger          -- ada berapa orang yang login ?
sftp> hostname        -- skr anda ada dimana ?
sftp> pwd             -- dimana home direktory anda ?
sftp> exit
$ hostname        -- kembali ke pc asal
```

17. Mencoba upload dan download file

Pertama buatlah beberapa file di pc anda, lalu upload ke pc sebelah menggunakan perintah sftp.

```
$ cd
$ hostname >namapcku
$ whoami > loginku
$ echo $HOME > homedirku
```

```
$ mkdir dataku
$ cp /etc/g* /home/dataku
$ ls –l
# sftp pckanan
  userkiri@pckanan's password: *******
sftp> ?          -- baca & pelajari helpnya
sftp> mput *     -- upload file
sftp> lpwd       -- local dir.
sftp> lls        -- local ls
sftp> lcd dataku  -- cd dataku di local pc
sftp> lpwd        -- local pwd
sftp> mkdir datakuremote  -- buar dir baru di remote pc
sftp> cd datakuremote
sftp> mput *    --upload semua file di dataku (local pc)
              --ke datakuremote (remote pc)
sftp> ls         -- ls di remote pc
sftp> pwd        -- pwd di remote pc
sftp> lls        -- ls di local pc
sftp> lpwd       -- pwd local pc
sftp> cd /etc
sftp> ls
sftp> lmkdir hasildownload
sftp> lcd hasildownload
sftp> mget passwd*  -- download file
sftp> mget group*
sftp> mget host*
sftp> ls
sftp> lls
sftp> bye
$ hostname        -- kembali ke pc asal
```

V. Laporan Resmi

b. Tulis hasil percobaan dan analisa hasilnya.

Daftar Pustaka

Hermanto, Syamsudin M. 2013. *Tip Dan Trik Otomatis Perangkat Jaringan (Shell Script)*. Yogyakarta : ANDI

Irawan. 2013. *Jaringan Komputer Untuk Orang Awam Edisi-2 + Cd*. Palembang : MAXIKOM

Madcoms. 2013. *Cepat Dan Mudah Membangun Sistem Jaringan Komputer*. Yogyakarta : ANDI

Sofana, Iwan. 2013. *Membangun Jaringan Computer (Mudah Membuat Jaringan Computer Wire&Wireless Untuk Pengguna Windows dan Linux)+DVD*. Bandung : INFORMATIKA