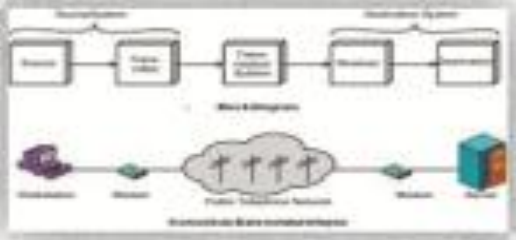
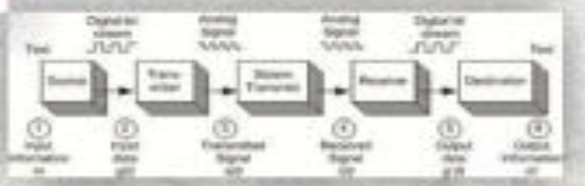
Kementrian Pendidikan dan Kebudayaan
Republik Indonesia
2014





KOMUNIKASI DATA

Paket Keahlian Teknik Komputer dan Jaringan

SMK/MAK Kelas XI
Semester 2

HAK CIPTA

Penulis : **Gladly C. Rorimpandey, ST, MISD**

Editor Materi : **Feldy Tumimomor, S.Pd**

Editor Bahasa :

Ilustrasi Sampul :

Desain & Ilustrasi Buku : **Mareska P. Jacobis, S.Pd**

Pusat Pengembangan & Pemberdayaan Pendidik

Jl. Teluk Mandar, Arjosari Tromol Pos 5, Malang 65102, Telp. (0341) 491239, (0341) 495849, Fax. (0341) 491342, Surel: vedcmalang@vedcmalang.or.id, Laman: www.vedcmalang.com

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan yang Maha Esa atas tersusunnya buku teks ini, dengan harapan dapat digunakan sebagai buku teks untuk siswa Sekolah Menengah Kejuruan (SMK) Bidang Studi Keahlian Teknologi Informasi dan Komunikasi, Program Keahlian Teknik Komputer dan Informatika.

Penerapan kurikulum 2013 mengacu pada paradigma belajar kurikulum abad 21 menyebabkan terjadinya perubahan, yakni dari pengajaran (teaching) menjadi BELAJAR (learning), dari pembelajaran yang berpusat kepada guru (teachers-centered) menjadi pembelajaran yang berpusat kepada peserta didik (student-centered), dari pembelajaran pasif (pasive learning) ke cara belajar peserta didik aktif (active learning-CBSA) atau Student Active Learning-SAL.

Buku teks Komunikasi Data ini disusun berdasarkan tuntutan paradigma pengajaran dan pembelajaran kurikulum 2013 diselaraskan berdasarkan pendekatan model pembelajaran yang sesuai dengan kebutuhan belajar kurikulum abad 21, yaitu pendekatan model pembelajaran berbasis peningkatan keterampilan proses sains.

Penyajian buku teks untuk Mata Pelajaran Komunikasi Data ini disusun dengan tujuan agar supaya peserta didik dapat melakukan proses pencarian pengetahuan berkenaan dengan materi pelajaran melalui berbagai aktivitas proses sains sebagaimana dilakukan oleh para ilmuwan dalam melakukan eksperimen ilmiah (penerapan scientifik), dengan demikian peserta didik diarahkan untuk menemukan sendiri berbagai fakta, membangun konsep, dan nilai-nilai baru secara mandiri.

Jakarta, November 2013
Menteri Pendidikan dan Kebudayaan

DAFTAR ISI

DAFTAR GAMBAR

Bagian 1 Pendahuluan

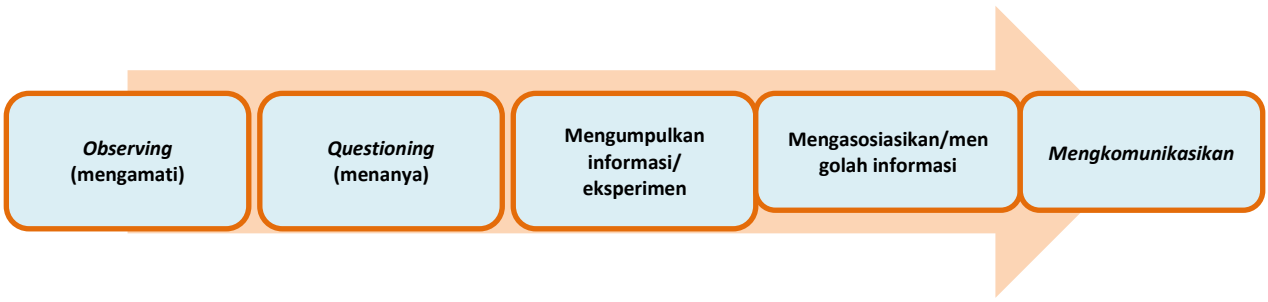
BAGIAN 1 : PENDAHULUAN

1. Deskripsi

Komunikasi Data merupakan salah satu mata pelajaran paket Teknik Komputer dan Jaringan (TKJ pada program keahlian Teknik Komputer dan Informatika (TKI) Berdasarkan struktur kurikulum 2013, mata pelajaran Komunikasi Data disampaikan di kelas XI semester 1 dan 2, masing-masing 4 jam pelajaran untuk setiap pertemuan kelas.

Perkembangan dunia komputer menjadikan informasi merupakan hal yang sangat berharga dalam komputer. Setiap saat dibutuhkan pemindahan informasi dari satu tempat ke tempat yang lain. Hal ini dikenal dengan komunikasi data. Data akan ditransmisikan dari satu tempat ke tempat yang lain yang membutuhkan. Selain itu, komunikasi data berkaitan dengan pengiriman sinyal yang handal dan efisien melalui kanal komunikasi. Hal-hal tersebut mendorong akan pemahaman terhadap komunikasi data dan keterampilan dalam membangun berbagai arsitektur komunikasi data sangat dibutuhkan sejalan dengan kebutuhan teknologi informasi dan komunikasi.

Pembelajaran komunikasi data ini menggunakan metode pendekatan *scientific*. Dalam pendekatan ini praktikum atau eksperimen berbasis sains meripakan bidang pendekatan ilmiah dengan tujuan dan aturan khusus, dimana tujuan utamanya adalah untuk memberikan bekal keterampilan yang kuat dengan disertai landasan teori yang realistis mengenai fenomena yang akan diamati. Ketika suatu permasalahan yang hendak diamati menimbulkan pertanyaan-pertanyaan yang tidak dapat terjawab, maka metode eksperimen ilmiah hendaklah dapat memberikan jawaban melalui proses yang logis. Proses-proses pendekatan *scientific* meliputi beberapa tahapan yaitu: mengamati, hipotesis atau menanya, mengumpulkan informasi atau eksperimen, mengasosiasikan atau mengolah informasi dan mengkomunikasikan.



Gambar 1.1 Pendekatan ScientifikPrasyarat

2. Prasyarat

Untuk kelancaran pencapaian kompetensi dalam mata pelajaran Komunikasi Data pada semester 2 ini, dibutuhkan beberapa persyaratan baik pengetahuan maupun keterampilan dasar. Persyaratan tersebut antara lain: Komunikasi Data semester 1, sistem komputer dan jaringan dasar. Selain itu, siswa harus mempunyai kompetensi dalam hal pemanfaatan teknologi informasi seperti mengoperasikan perangkat keras dan perangkat lunak komputer. Perangkat lunak tersebut antara lain adalah pengolah data untuk menganalisis data hasi eksperimen, pengolah kata untuk membuat laporan dan aplikasi presentasi untuk mengkomunikasikan dan mempresentasikan hasil laporan.

3. Petunjuk Penggunaan

Buku pedoman siswa ini disusun berdasarkan kurikulum 2013 yang mempunyai ciri khas penggunaan metode scientifik. Buku ini terdiri dari 2 bab yaitu bab satu pendahuluan dan bab dua pembelajaran. Dalam bab pendahuluan beberapa haris dipelajari oleh siswa adalah deskripsi mata pelajaran yang berisi informasi umum, rasionalitas dan penggunaan metode scientifik. Selanjutnya pengetahuan tentang persyaratan, tujuan yang diharapkan, kompetensi inti dan dasar yang akan dicapai serta peta kompetensi dari mata pelajaran ini.

Pada bab dua menuntun siswa untuk memahami deskripsi umu topik yang akan dipelajari dan rincian kegiatan belajar sesuai dengan kompetensi dan tujuan yang dicapai. Setiap kegiatan belajar terdiri dari tujuan yang akan dicapai, aktifitas belajar siswa, tugas dan tes formatif. Aktifitas belajar siswa mengacu pada 5 tahap pendekatan scientifik.

Tugas yang harus dikerjakan oleh siswa dapat berupa tugas praktek, eksperimen atau pendalaman materi pembelajaran. Setiap tugas yang dilakukan melalui beberapa tahapan scientifik yaitu:

1) Melakukan pengamatan setiap tahapan untuk kerja
2) Melakukan praktek sesuai dengan unjuk kerja
3) Mengumpulkan data yang dihasilkan setiap tahapan
4) Menganalisa hasil data menggunakan analisa deskriptif
5) Mengasosiasikan beberapa pengetahuan dalam uraian materi pembelajaran untuk membentuk suatu kesimpulan
6) Mengkomunikasikan hasil dengan membuat laporan portofolio. Laporan ini akan dijadikan sebagai salah satu referensi penilaian.

4. Tujuan Akhir

Setelah melewati semua aktifitas belajar dalam bab pembelajaran, maka siswa diharapkan dapat memiliki kompetensi sikap, pengetahuan dan keterampilan yang berkaitan dengan materi:

- Prosedur Instalasi Server Softswitch berbasis SIP
- Konfigurasi Ekstensi dan Dial-Plan Server Softswitch
- Fungsi Firewall pada Jaringan VoIP
- Prinsip Kerja Subscriber pada Internet Telepon
- Konfigurasi Subscriber pada Internet Telepon
- Prosedur Pengamatan Kerja

5. Kompetensi Inti Dan Kompetensi Dasar

Kompetensi Inti dan Kompetensi Dasar untuk Mata Kuliah Komunikasi Data ini adalah sebagai berikut:

Kompetensi Inti	Kompetensi Dasar
Menghayati dan mengamalkan ajaran agama yang dianutnya	1.1. Memahami nilai-nilai keimanan dengan menyadari hubungan keteraturan dan kompleksitas alam dan jagad raya terhadap kebesaran Tuhan yang menciptakannya. 1.2. Mendiskripsikan kebesaran Tuhan yang menciptakan berbagai sumber energi di alam. 1.3. Mengamalkan nilai-nilai keimanan sesuai dengan ajaran agamanya dalam kehidupan sehari-hari. 1.4. Meningkatkan nilai-nilai keimanan

	dalam upaya untuk mencegah pengaruh negatif perkembangan teknologi informasi dan komunikasi.
2.Menghayati dan Mengamalkan perilaku jujur, disiplin, tanggung jawab, peduli (gotong royong, kerjasama, toleran, damai), santun, responsif dan proaktif dan menunjukan sikap sebagai bagian dari solusi atas berbagai permasalahan dalam berinteraksi secara efektif dengan lingkungan sosial dan alam serta dalam menempatkan diri sebagai cerminan bangsa dalam pergaulan dunia.	2.1. Menunjukkan perilaku ilmiah (memiliki rasa ingin tahu; objektif; jujur; teliti; cermat; tekun; hati-hati; bertanggung jawab; terbuka; kritis; kreatif; inovatif dan peduli lingkungan) dalam aktivitas sehari-hari sebagai wujud implementasi sikap dalam melakukan percobaan dan berdiskusi 2.2. Menghargai kerja individu dan kelompok dalam aktivitas sehari-hari sebagai wujud implementasi melaksanakan percobaan dan melaporkan hasil percobaan

3. Memahami, menerapkan, dan menjelaskan pengetahuan faktual, konseptual, prosedural, dan metakognitif dalam ilmu pengetahuan, teknologi, seni, budaya, dan humaniora dengan wawasan kemanusiaan, kebangsaan, kenegaraan, dan peradaban terkait penyebab fenomena dan kejadian, serta menerapkan pengetahuan prosedural pada bidang kajian yang spesifik sesuai dengan bakat dan minatnya untuk memecahkan masalah	3.1. Memahami ragam aplikasi komunikasi data. 3.2. Menganalisis berbagai standar komunikasi data. 3.3. Menganalisis proses komunikasi data dalam jaringan. 3.4. Memahami aspek-aspek teknologi komunikasi data dan suara. 3.5. Menganalisis kebutuhan telekomunikasi dalam jaringan. 3.6. Menganalisis kebutuhan beban / bandwidth jaringan. 3.7. Memahami konsep kerja protokoler server softswitch. 3.8. Memahami diagram rangkaian operasi komunikasi VoIP 3.9. Memahami bagan dan konsep kerja server softswitch berkaitan dengan PBX. 3.10. Menjelaskan konfigurasi ekstensi dan

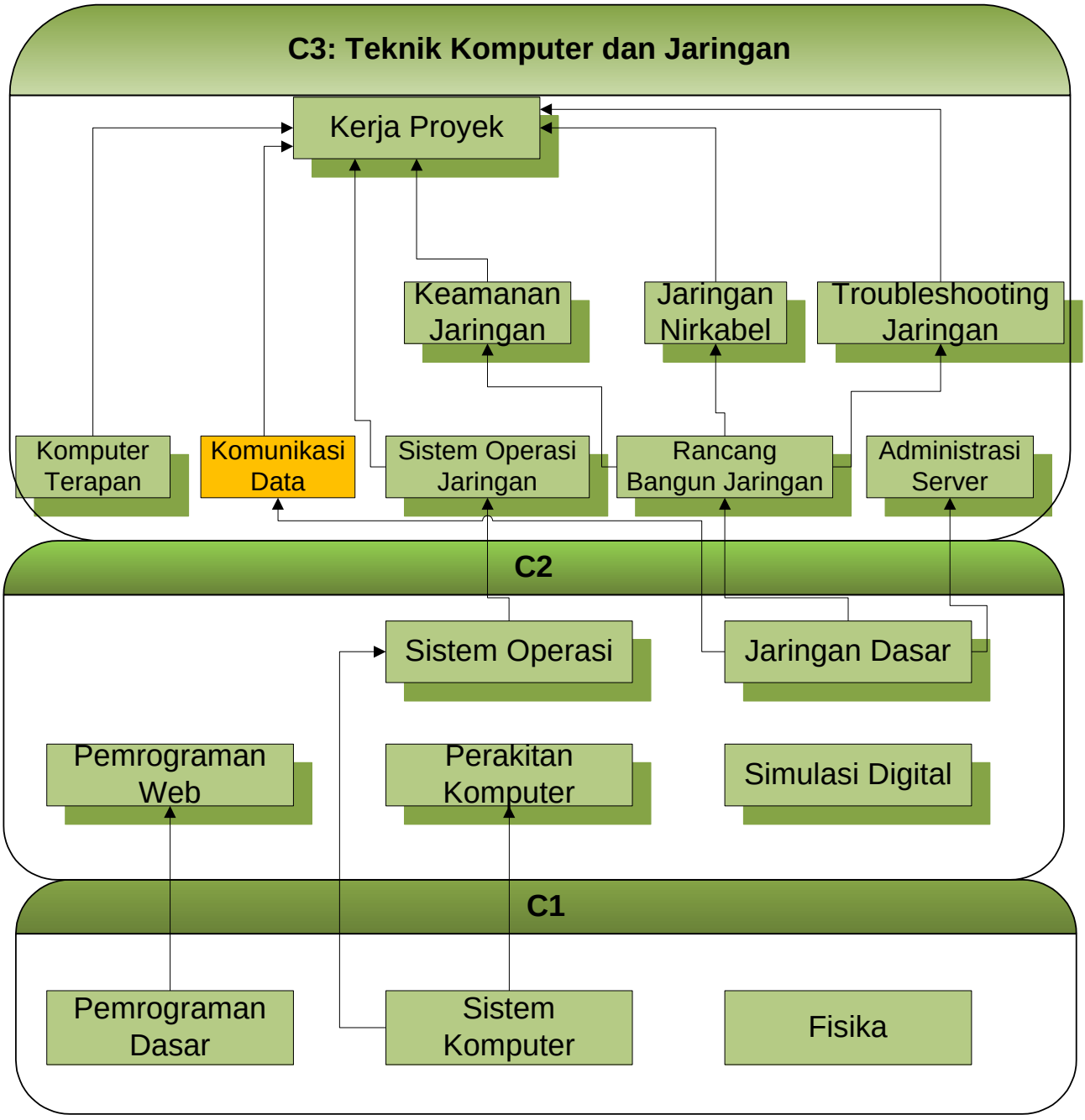
	dial-plan server softswitch. 3.11. Memahami prosedur instalasi server softswitch berbasis session initial protocol (SIP). 3.12. Memahami konfigurasi ekstensi dan dial-plan server softswitch 3.13. Memahami fungsi firewall pada jaringan VoIP 3.14. Memahami prinsip kerja subscriber internet telepon 3.15. Memahami konfigurasi pada subscriber internet telepon 3.16. Memahami prosedur pengamatan kerja system komunikasi VoIP
4. Mencoba, mengolah, dan menyaji dalam ranah konkret dan ranah abstrak terkait dengan pengembangan dari yang dipelajarinya di sekolah secara mandiri, bertindak secara	4.1. Menyajikan karakteristik ragam aplikasi komunikasi data 4.2. Menyajikan berbagai standar komunikasi data 4.3. Menyajikan hasil analisis proses

efektif dan kreatif, serta mampu menggunakan metoda sesuai kaidah keilmuan	komunikasi data 4.4. Menalar aspek-aspek teknologi komunikasi data dan suara 4.5. Menyajikan hasil analisis kebutuhan telekomunikasi dalam jaringan 4.6. Menyajikan hasil analisis kebutuhan beban/bandwidth jaringan 4.7. Menalar konsep kerja protokoler server softswitch 4.8. Menalar diagram rangkaian operasi komunikasi VoIP 4.9. Menyajikan bagan dan konsep kerja server softswitch berkaitan dengan PBX. 4.10. Menerapkan konfigurasi ekstensi dan dial-plan server softswitch 4.11. Menyajikan hasil instalasi server softswitch berbasis session initial protocol (SIP). 4.12. Menyajikan hasil konfigurasi

	eksistensi dan dial-plan server softswitch. 4.13. Menalar fungsi firewall pada jaringan VoIP 4.14. Menalar prinsip kerja subscriber internet telepon 4.15. Menyajikan hasil instalasi dan konfigurasi subscriber internet telepon. 4.16. Menyajikan hasil analisa prosedur pengamatan kerja system komunikasi VoIP

6. Peta Konsep

Peta konsep atau kedudukan bahan ajar merupakan suatu diagram yang menjelaskan struktur mata pelajaran dan keterkaitan antar mata kuliah dalam satu bidang studi keahlian.



Gambar 6.1 Peta Kedudukan Mata Pelajaran

BAGIAN 2 : PEMBELAJARAN

BAB I

1.1 Kegiatan Belajar 1: Prosedur Instalasi Server Softswitch berbasis SIP

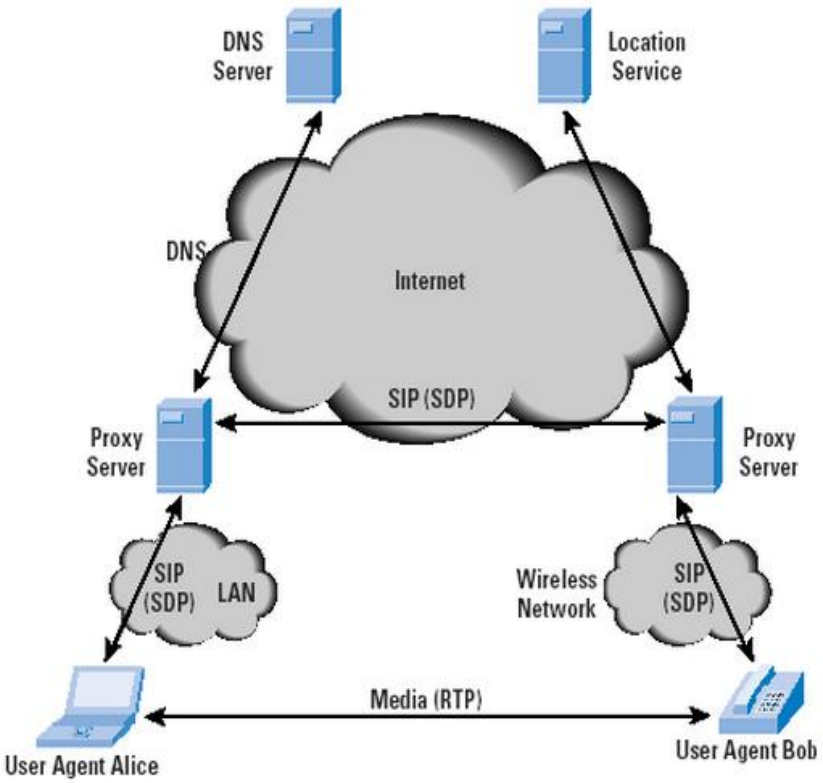
1.1.1 Tujuan Pembelajaran

Setelah mempelajari kegiatan belajar 1 ini, siswa diharapkan dapat:

1) Memahami prosedur instalasi server softswitch berbasis Session Initial Protocol (SIP)
2) Menyajikan hasil instalasi server Softswitch berbasis Session Initial Protocol (SIP)

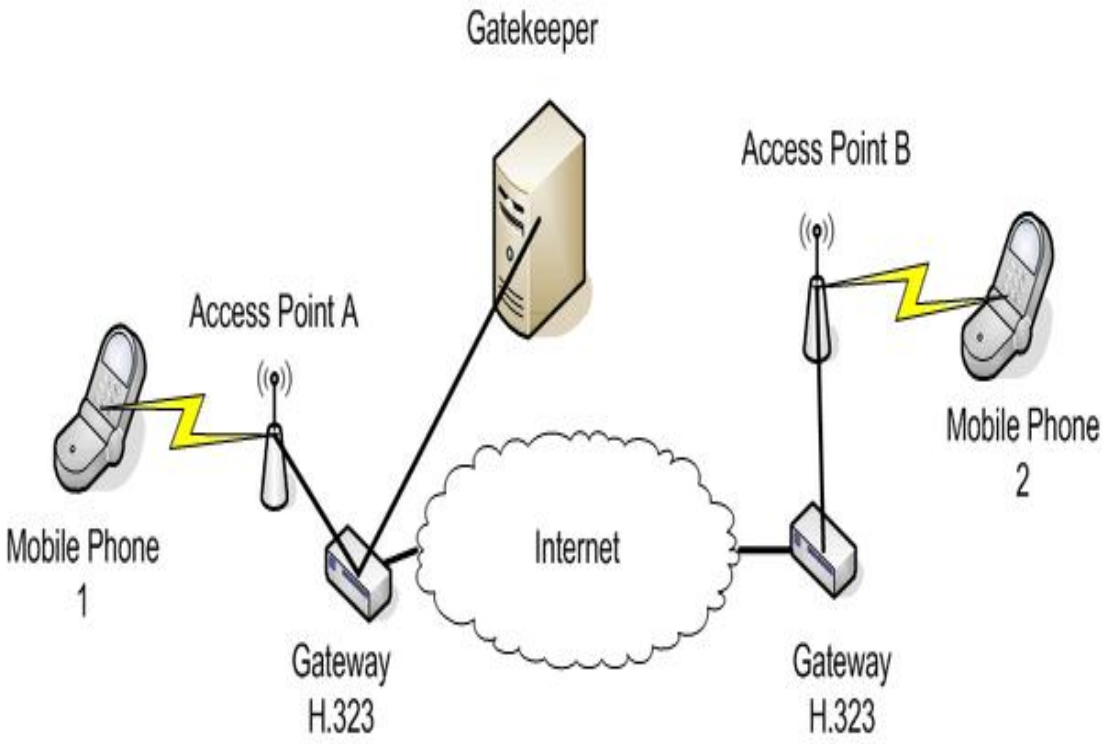
1.1.2 Aktifitas Belajar Siswa

1.1.2.1 Mengamati/Observasi



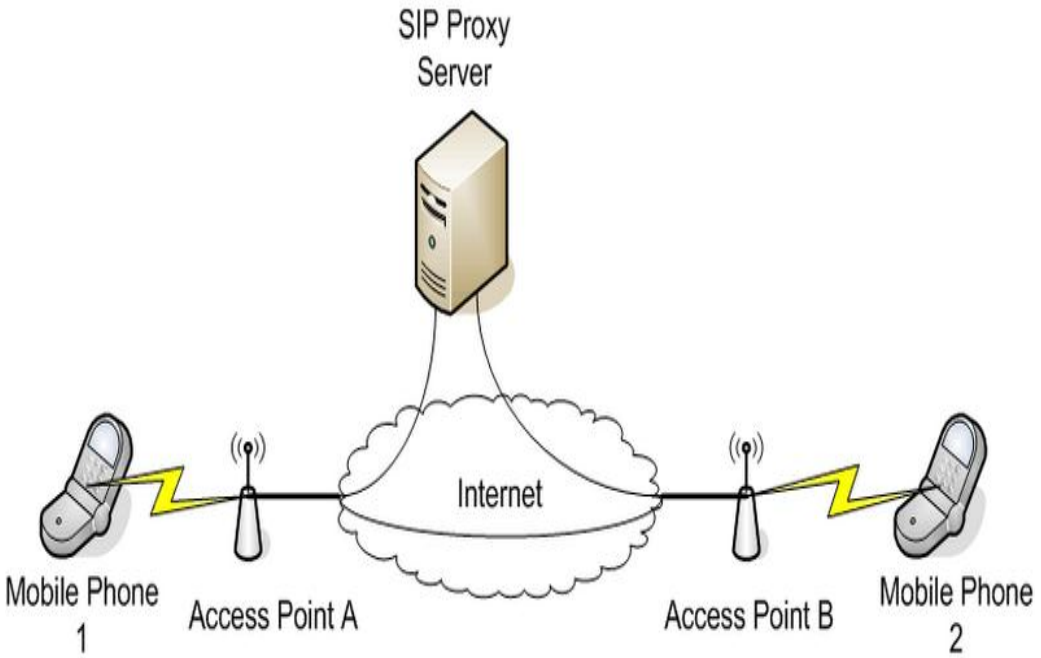
Sumber: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/sip.html

Gambar 1.1 Komponen dan Protokol SIP



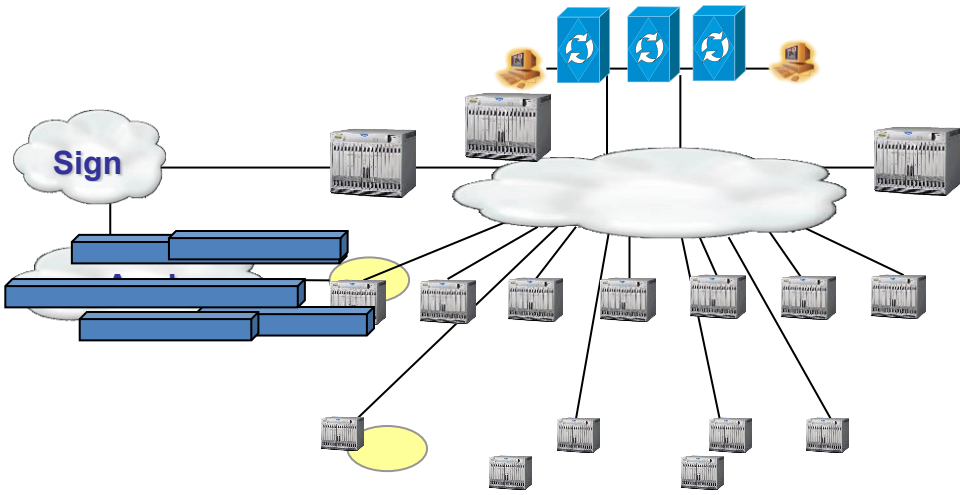
Sumber: http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_voip/

Gambar 1.2 Contoh Jaringan H.323 dengan Gatekeeper



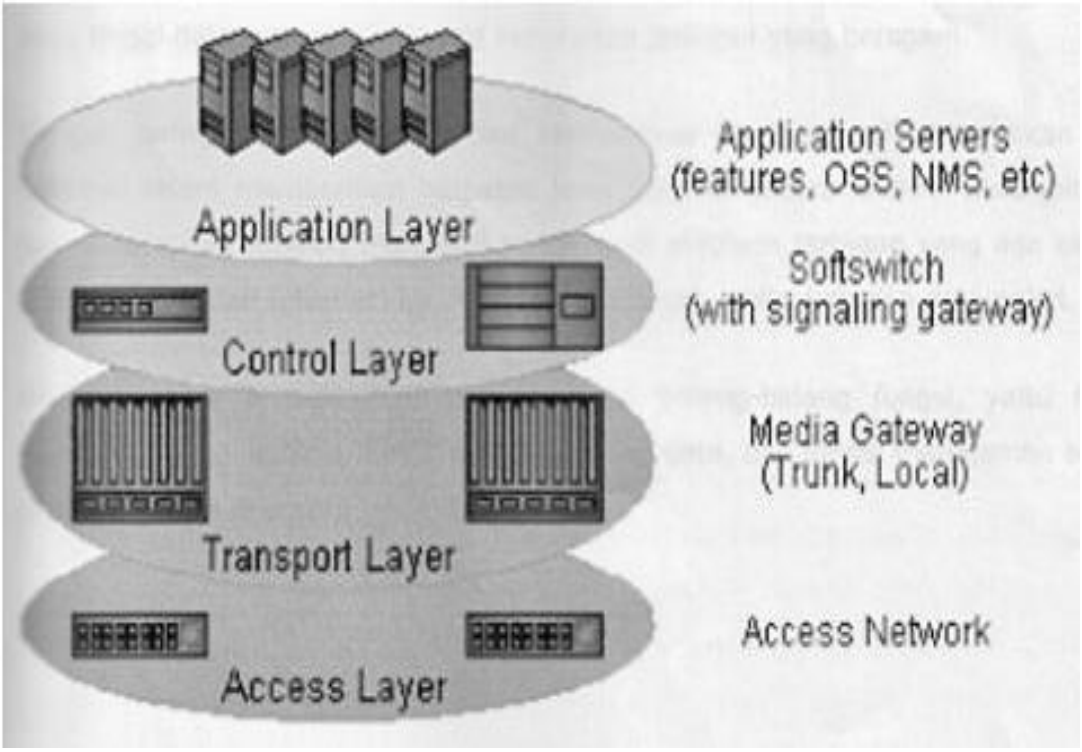
Sumber: http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_voip/

Gambar 1.3 Contoh SIP pada *Voice Over Wireless*



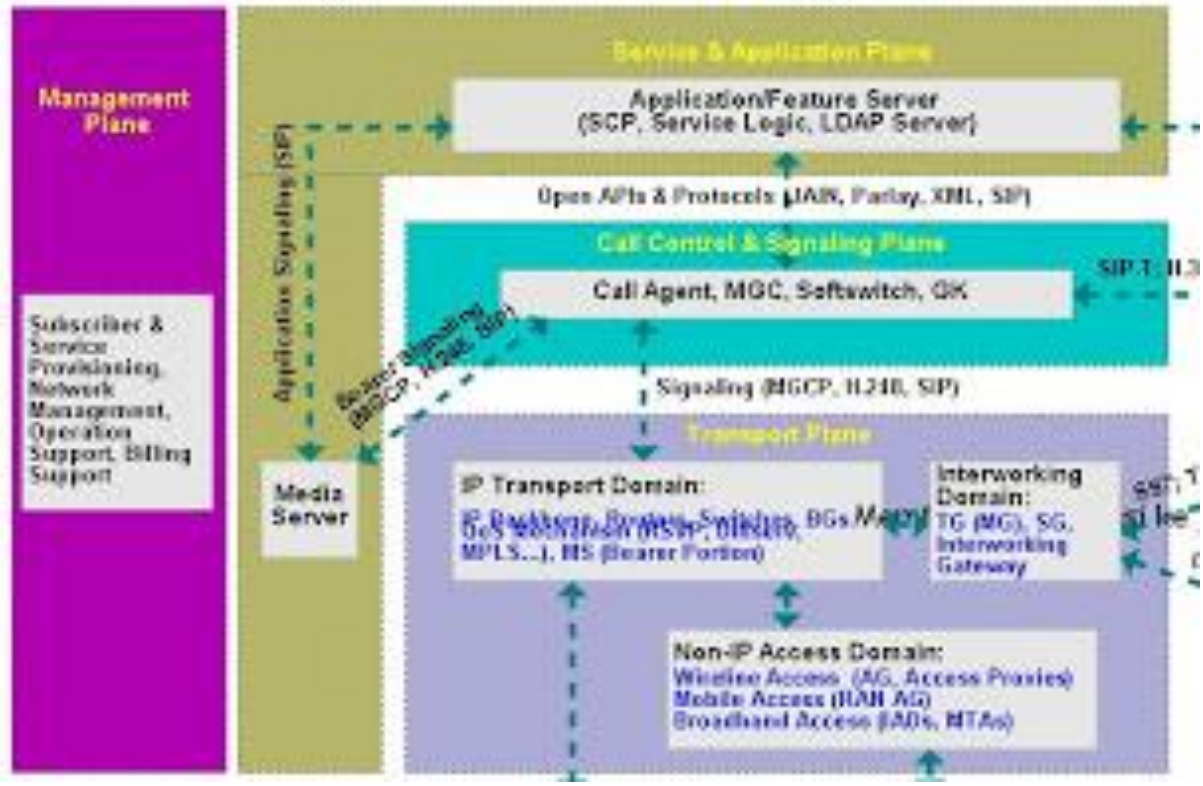
Sumber : Dokumen Kemendikbud

Gambar 1.4 Arsitektur Softswitch



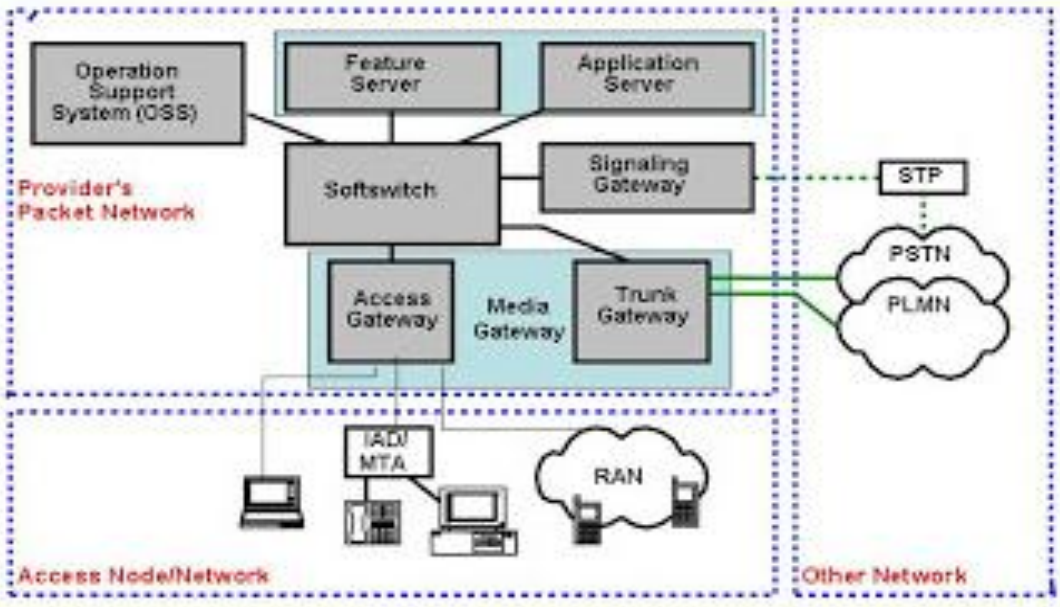
Sumber : http://elektro-unesa.blogspot.com/2011/06/jaringan-telekomunikasi-masa-depan-next.html

Gambar 1.5 Arsitektur Layer Softswitch



Sumber : http://smktelkomzone.blogspot.com/2012/03/mengapa-softswitch-dibutuhkan.html

Gambar 1.6 Arsitektur Fungsional Softswitch



Sumber : http://elektro-unesa.blogspot.com/2011/06/jaringan-telekomunikasi-masa-depan-next.html

Gambar 1.7 Fungsional Elemen Softswitch

1.1.2.2 Menanya

Dengan mengamati gambar yang ada pada bagian observasi, menurut anda:

1) Apakah yang dimaksud dengan SIP (*Session Initial Protocol*)?

2) Bagaimanakah instalasi server softswitch berbasis SIP?

1.1.2.3 Mencoba/Mengumpulkan Informasi

1.1.2.3.1 Konsep SIP (Session Initial Protocol)

SIP atau *Session Initial Protocol* merupakan protokol jaringan komunikasi yang digunakan untuk memberikan signal bagi VoIP. Dalam jaringan VoIP, SIP merupakan pendekatan alternatif untuk mengirimkan sinyal dengan menggunakan standar protokol H.323 (Mitchell, 2014). H.323 adalah protokol *International Telecommunication Unit* (ITU) untuk membangun koneksi VoIP. Protokol ini merupakan standar pertama yang memecahkan masalah VoIP dalam jaringan. Standar ini terdiri dari tiga komponen utama: *Call Processing Server, Media Gateways, dan Gatekeeper*. *Call Processing Server* menangani panggilan routing juga memungkinkan untuk komunikasi ke gateway VoIP dan perangkat pengguna akhir. *Media Gateways* menyediakan antarmuka dengan jaringan non-H.323 selain menjadi simpul protokol terminasi. *Gatekeeper* (meskipun tidak diperlukan) menyediakan fungsi kontrol masuk panggilan, pemanggilan signal dan manajemen bandwidth sebagai lokasi kerjasama unit. *Gatekeeper* memungkinkan protokol menjadi sangat terukur dengan mengambil kontrol panggilan dan manajemen dari gerbang. Perhatikan Gambar 1.2 sebagai contoh jaringan H.323 dengan *Gatekeeper.*

SIP merupakan sebuah protokol dalam level aplikasi yang membuat, mengatur dan menterminasikan setiap sesi pada sebuah jaringan berbasis IP. Suatu sesi yang dimaksud dapat berupa komunikasi telepon dua arah ataupun komunikasi yang berupa kolaborasi konferensi sesi multi-media (perhatikan Gambar 1.3). Hal ini memungkinkan untuk mengimplementasikan layanan seperti E-commerce dengan suara, halaman Web dengan Koneksi Dial-Up atau Instant Messanger dengan gratis. SIP merupakan standar (RFC 3261) yang diajukan oleh *Internet Engineering Task Force* (IETF) pada tahun 1999 yang awalnya merupakan RFC 2543. SIP masih terus dikembangkan dan dimodifikasi untuk memenuhi semua fitur yang relevan sebagai sebuah teknologi yang dinamis. Tapi perlu diingat bahwa tugas SIP hanya sebatas pada pengaturan dan pengendalian sesi. Rincian pertukaran data dalam sesi misalnya pengkodean atau codec yang berhubungan dengan media audio/video tidak dikontrol oleh SIP tapi diatur oleh protokol lain.

Sistem telepon berbasis saklar tradisional adalah awal media utama untuk transmisi pesan. Namun dengan munculnya Internet, kebutuhan dirasakan untuk membuat sebuah sistem yang menghubungkan orang melalui jaringan berbasis IP. Komunitas yang berbeda mengajukan solusi yang berbeda namun solusi yang disajikan oleh IETF akhirnya diterima sebagai yang paling umum. Namun pengembangan SIP di IETF bukan proses satu langkah. Pada Februari 1996, Draft Internet awal diproduksi dalam bentuk - Session Undangan Protocol (SIP) -

M.Handley, E.Schooler. Sederhana Konferensi Undangan Protocol (Scip) - H.Schulzrinne. SIP pada awalnya ditujukan untuk menciptakan mekanisme untuk mengundang orang untuk konferensi multipoint besar-besaran pada Backbone Internet Multicast (Mbone). Pada tahap ini, IP telephony tidak benar-benar ada. Draft pertama dikenal sebagai "draft-IETF-mmusic-sip-00". Ini termasuk satu jenis permintaan, yang merupakan permintaan call setup. Pada Desember 1996, sebuah versi yang lebih baru "draft-IETF-mmusic-sip-01" diusulkan sebagai modifikasi SIP-0. Namun itu belum mengambil bentuk SIP seperti yang kita kenal sekarang. Dan selanjutnya pada Januari 1999, IETF menerbitkan rancangan yang disebut "draft-IETF-mmusic-sip-12". Isinya enam permintaan yang SIP hari ini. Sehingga Maret 1999 IETF menetapkan standar SIP. (Banerjee, 2005).

SIP mendukung lima aspek membangun dan mengakhiri komunikasi multimedia (Stallings, 2003). Lima aspek tersebut adalah sebagai berikut:

1) Lokasi Pengguna: Pengguna dapat pindah ke lokasi lain dan mengakses telepon atau fitur aplikasi lainnya dari lokasi terpencil.
2) Ketersediaan Pengguna: Langkah ini melibatkan penentuan kesediaan pihak yang dipanggil untuk terlibat dalam komunikasi.
3) Kemampuan Pengguna: Pada langkah ini, media dan parameter media yang akan digunakan ditentukan.
4) Pengaturan sesi: Point-to-point dan panggilan multipartai ditetapkan, dengan parameter sesi disepakati.
5) Manajemen sesi: Langkah ini termasuk mutasi dan pemutusan sesi, memodifikasi parameter sesi, dan layanan memohon.

SIP menggunakan elemen desain yang dikembangkan untuk protokol sebelumnya. SIP didasarkan pada HTTP seperti model transaksi request/respon. Setiap transaksi terdiri dari permintaan klien yang memanggil metode tertentu, atau fungsi, pada server dan setidaknya satu respon. SIP menggunakan sebagian besar field header, aturan encoding, dan kode status HTTP. Ini menyediakan format berbasis teks yang dapat dibaca untuk menampilkan informasi. SIP menggabungkan penggunaan Session Description Protocol (SDP), yang mendefinisikan konten sesi menggunakan satu set jenis yang sama dengan yang digunakan di Multipurpose Internet Mail Extensions (MIME). RFC 2327 mendefinisikan Session Description Protocol (SDP) yaitu konten yang menggambarkan isi dari sesi, termasuk telepon, radio internet, dan aplikasi multimedia. SDP mencakup informasi tentang:

- Media stream: Sesi yang dapat mencakup beberapa aliran konten yang berbeda. SDP saat mendefinisikan audio, video, data, kontrol, dan aplikasi sebagai jenis aliran, mirip dengan jenis MIME digunakan untuk Internet mail.

- Alamat: SDP menunjukkan alamat tujuan, yang mungkin alamat multicast, untuk media stream.
- Ports: Untuk setiap aliran, nomor port UDP untuk mengirim dan menerima ditentukan.
- Jenis muatan: Untuk setiap jenis media stream yang digunakan (misalnya, telepon), tipe payload menunjukkan format media yang dapat digunakan selama sesi.
- Memulai dan menghentikan waktu: ini berlaku untuk menyiarkan sesi, misalnya, sebuah program televisi atau radio. Start, stop, dan ulangi kali sesi ditunjukkan.
- Originator: Untuk sesi siaran, originator ditentukan, dengan informasi kontak. Ini mungkin berguna jika penerima bertemu kesulitan teknis.

Meskipun SDP menyediakan kemampuan untuk menggambarkan konten multimedia, tetapi SDP tidak memiliki mekanisme yang kedua belah pihak menyepakati parameter yang akan digunakan. RFC 3264 memperbaiki kekurangannya dengan mendefinisikan sebuah tawaran model/jawaban yang sederhana, dimana dua pihak bertukar pesan SDP untuk mencapai kesepakatan tentang sifat konten multimedia yang akan dikirim.

Komponen dan Protokol SIP

Sebuah sistem berbasis SIP dapat diidentifikasi dengan komponen yang dimilikinya, yaitu elemen client / server dan jaringan individu. RFC 3261 mendefinisikan klien dan server sebagai berikut: Klien adalah setiap elemen jaringan yang mengirim permintaan SIP dan menerima tanggapan SIP. Klien mungkin atau mungkin tidak berinteraksi langsung dengan pengguna manusia. Pengguna agen klien dan proxy adalah klien. Sedangkan Server adalah sebuah elemen jaringan yang menerima permintaan untuk layanan mereka dan mengirimkan kembali tanggapan terhadap permintaan tersebut. Contoh server proxy, server user agent, refirect server, dan panitera.

Unsur-unsur individual dari konfigurasi SIP standar meliputi berikut ini:

- User Agent: Agen pengguna berada di setiap stasiun akhir SIP. Kerjanya di dua peran:
  - User Agent Client (UAC): permintaan Isu SIP
  - User Agent Server (UAS): Menerima permintaan SIP dan menghasilkan respon yang menerima, menolak, atau pengalihan permintaan.
- Redirect Server digunakan selama inisiasi sesi untuk menentukan alamat yang disebut perangkat. Redirect Server kembali informasi ini ke perangkat memanggil, mengarahkan UAC untuk menghubungi alternatif Universal Resource Identifier (URI). Sebuah URI adalah identifier generik yang digunakan untuk menyebutkan nama sumber daya di Internet. URL yang digunakan untuk alamat Web

adalah jenis URI. Lihat RFC 2396 untuk lebih detail.

- Proxy Server adalah entitas perantara yang bertindak baik sebagai server dan klien untuk tujuan membuat permintaan atas nama klien lainnya. Sebuah server proxy terutama memainkan peran routing, yang berarti bahwa tugasnya adalah untuk memastikan bahwa permintaan dikirim ke entitas lain lebih dekat ke pengguna yang ditargetkan. Proxy juga berguna untuk menegakkan kebijakan (misalnya, memastikan pengguna diperbolehkan untuk membuat panggilan). Sebuah proxy menafsirkan, dan, jika perlu, penulisan ulang bagian-bagian tertentu dari pesan permintaan sebelum meneruskan itu.
- Paniter adalah sebuah server yang menerima permintaan REGISTER dan menempatkan informasi yang diterimanya (alamat SIP dan terkait alamat IP dari perangkat mendaftar) di permintaan tersebut ke layanan lokasi untuk domain menangani.
- Lokasi Layanan: Layanan lokasi digunakan oleh redirect SIP atau server proxy untuk mendapatkan informasi tentang kemungkinan lokasi yang dituju. Untuk tujuan ini, layanan lokasi memelihara sebuah database pemetaan SIP-address / IP-address.

Sumber:
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/sip.html

Gambar 1.1 pada bagian mengamati menunjukkan bagaimana beberapa komponen SIP berhubungan satu sama lain dan protokol yang digunakan. Seorang agen pengguna bertindak sebagai klien (dalam hal ini UAC Alice) menggunakan SIP untuk mengatur sesi dengan agen pengguna yang bertindak sebagai server (dalam hal ini UAS Bob). Dialog inisiasi sesi menggunakan SIP dan melibatkan satu atau lebih server proxy untuk meneruskan permintaan dan tanggapan antara dua agen pengguna. Para agen pengguna juga memanfaatkan SDP, yang digunakan untuk menggambarkan sesi media.

Proxy server juga dapat bertindak sebagai redirect server yang diperlukan. Jika pengalihan dilakukan, proxy server perlu berkonsultasi dengan database layanan lokasi, yang mungkin atau tidak berlokasi dengan proxy server. Komunikasi antara proxy server dan layanan lokasi di luar lingkup standar SIP.

Domain Name System (DNS) juga merupakan bagian penting dari operasi SIP. Biasanya, sebuah UAC membuat permintaan menggunakan nama domain dari UAS, bukan alamat IP. Sebuah server proxy perlu berkonsultasi server DNS untuk menemukan server proxy untuk target domain. SIP sering berjalan di atas *User Datagram Protocol* (UDP) untuk alasan kinerja, dan menyediakan mekanisme kehandalan sendiri, tetapi juga dapat menggunakan TCP. Jika, mekanisme transportasi terenkripsi yang aman yang diinginkan, pesan SIP dapat alternatif

dilakukan selama *Transport Layer Security* (TLS) protokol.

Terkait dengan SIP adalah SDP, didefinisikan dalam RFC 2327. SIP digunakan untuk mengundang satu atau lebih peserta untuk sesi, sementara tubuh SDP-dikodekan pesan SIP berisi informasi tentang pengkodean media (misalnya, suara, video) para pihak dapat dan akan menggunakan. Setelah informasi ini ditukarkan dan diakui, semua peserta menyadari alamat peserta IP, kapasitas transmisi yang tersedia, dan jenis media. Kemudian, transmisi data dimulai, menggunakan protokol transport yang sesuai. Biasanya, RTP digunakan. Sepanjang sesi, peserta dapat membuat perubahan parameter sesi, seperti jenis media baru atau partai baru untuk sesi, menggunakan pesan SIP.

Sebuah sumber daya dalam konfigurasi SIP diidentifikasi oleh URI. Contoh sumber daya komunikasi meliputi berikut ini:

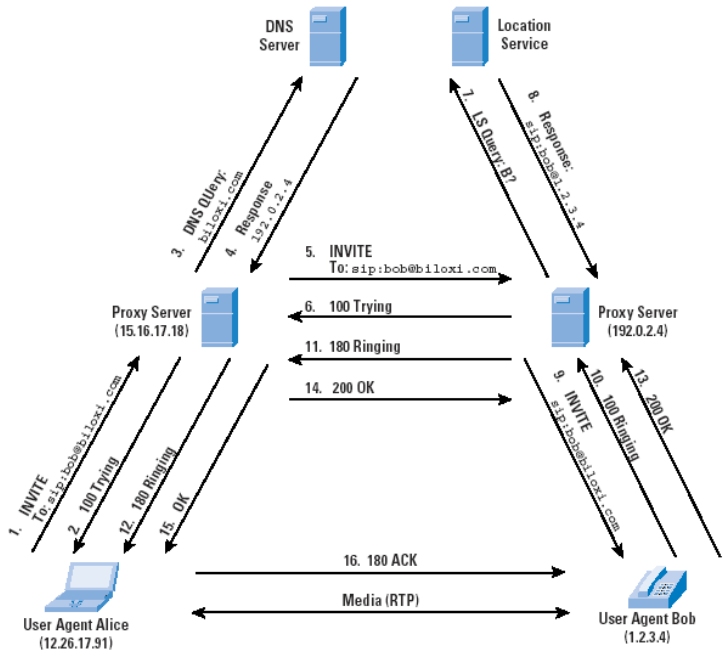
- Seorang pengguna dari layanan online
- Sebuah penampilan di telepon multiline
- Sebuah kotak pada sistem pesan
- Sebuah nomor telepon di layanan gerbang
- Sebuah kelompok (seperti "penjualan" atau "help desk") dalam sebuah organisasi

Perintah pada SIP

Perintah yang digunakan dalam SIP adalah sebagai berikut:

- INVITE merupakan perintah untuk mengundang pengguna untuk panggilan.
- ACK atau Acknowledgement merupakan perintah yang digunakan untuk memfasilitasi pertukaran pesan pada perintah INVITE.
- BYE merupakan perintah untuk menghentikan hubungan antara pengguna.
- CANCEL merupakan perintah untuk menghentikan permintaan atau mencari permintaan untuk seorang pengguna. Perintah ini digunakan jika klien mengirimkan perintah INVITE dan merubah keputusannya untuk memanggil penerima.
- OPTION merupakan perintah untuk mengumpulkan sejumlah informasi tentang kemampuan sebuah server.
- REGISTER merupakan perintah untuk register lokasi pengguna saat ini.
- INFO merupakan perintah yang digunakan pada pertengahan sesi signaling.

Seperti contoh berikut ini:



Sumber: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/sip.html

Gambar 1.8 Pengaturan Panggilan SIP yang Sukses

Perintah pada Gambar 1.8 untuk pesan Header (1) adalah sebagai berikut (Stallings, 2003):

INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP 12.26.17.91:5060
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com
From: Alice <sip:alice@atlanta.com;tag=1928301774
Call-ID: a84b4c76e66710@12.26.17.91
CSeq: 314159 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 142

Baris pertama berisi nama metode (INVITE) yang merupakan SIP URI, dan nomor versi SIP yang digunakan. Garis yang mengikuti adalah daftar *field header*. Contoh ini berisi minimum yang diperlukan ditetapkan. Via header menunjukkan jalan permintaan yang telah diambil dalam konfigurasi SIP (sumber dan intervensi proxy), dan digunakan untuk respon rute di sepanjang jalan yang sama. Sebagai pesan turunan INVITE, hanya ada header dimasukkan oleh Alice. Garis koneksi berisi alamat IP (12.26.17.91), nomor port (5060), dan protokol transport (UDP) bahwa Alice ingin Bob untuk digunakan dalam tanggapannya.

Max-Forward header membatasi jumlah hop dengan permintaan dapat dibuat dalam perjalanan ke tujuannya. Ini terdiri dari integer yang dikurangi oleh satu disetiap masing-masing proxy yang meneruskan permintaan. Jika nilai Max-Forward mencapai 0 sebelum permintaan mencapai tujuannya, ia ditolak dengan 483 (Terlalu Banyak Hops) respon kesalahan. Daerah To Header berisi nama tampilan (Bob) dan SIP atau SIPS URI (sip: bob@biloxi.com) ke arah mana permintaan awalnya diarahkan. Daerah From Header juga berisi nama tampilan (Alice) dan SIP atau SIPS URI (sip: alice@atlanta.com) yang menunjukkan pencetus permintaan. Daerah

header ini juga memiliki parameter tag yang berisi string acak (1928301774) yang ditambahkan ke URI oleh UAC yang digunakan untuk mengidentifikasi sesi.

Daerah Call-ID header berisi pengenal unik global untuk panggilan ini, yang dihasilkan oleh kombinasi string acak dan nama host atau alamat IP. Kombinasi dari To Tag, From Tag, dan Call-ID benar mendefinisikan hubungan SIP peer-to-peer antara Alice dan Bob dan disebut sebagai dialog. Bagian CSeq atau *Command Sequence header* berisi integer dan nama metode. Jumlah CSeq diinisialisasi pada awal panggilan (314.159 dalam contoh ini), bertambah untuk setiap permintaan baru dalam dialog, dan merupakan nomor urut tradisional. Bagian CSeq ini digunakan untuk membedakan transmisi dari permintaan baru. Bagian *Contact field header* berisi SIP URI untuk komunikasi langsung antara pengguna. Sedangkan *Via field header* mengatakan unsur-unsur lain di mana untuk mengirim tanggapan (respon), *Contact field header* mengatakan unsur-unsur lain di mana untuk mengirim permintaan masa depan untuk dialog ini. Bagian *Content-Type field header* menunjukkan jenis badan pesan. Bagian *Content-Type field header* ini memberikan panjang dalam oktet tubuh pesan.

Contoh yang lain yaitu pesan header (13) pada Gambar 1.8 dapat dilihat seperti berikut ini:

SIP/2.0 200 OK
Via: SIP/2.0/UDP server10.biloxi.com
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com
Via: SIP/2.0/UDP 12.26.17.91:5060
To: Bob <sip:bob@biloxi.com;tag=a6c85cf
From: Alice <sip:alice@atlanta.com;tag=1928301774
Call-ID: a84b4c76e66710@12.26.17.91
CSeq: 314159 INVITE
Contact: <sip:bob@biloxi.com>
Content-Type: application/sdp
Content-Length: 131

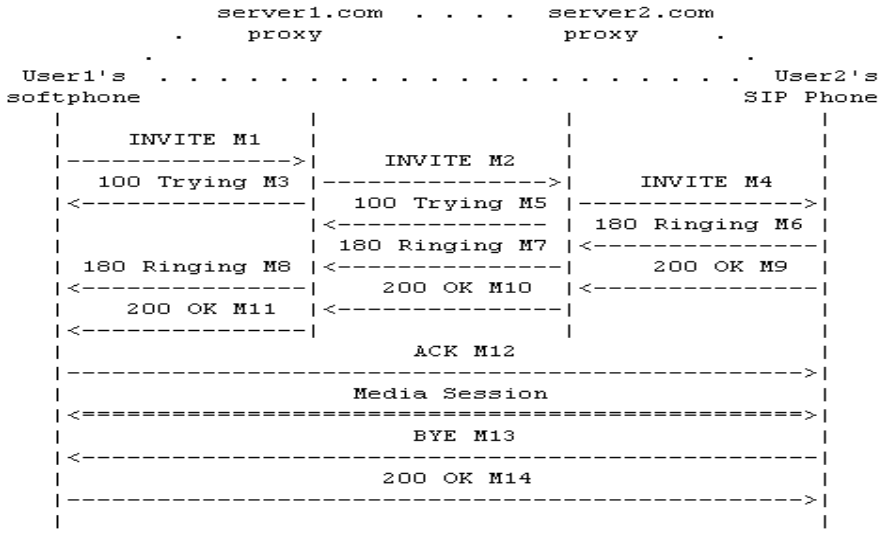
Baris pertama berisi nomor versi SIP yang digunakan dan kode respon serta nama. Garis yang mengikuti adalah daftar field header. Via, To, From, Call-ID dan CSeq field header disalin dari INVITE request. Ada tiga Via kolom header nilai-satu ditambah Alice SIP UAC, satu ditambah proxy atlanta.com, dan satunya lagi ditambah proxy biloxi.com. Telepon SIP Bob telah menambahkan sebuah parameter tag ke To field header. Tag ini dimasukkan oleh kedua endpoint ke dialog juga termasuk dengan semua permintaan masa depan dan tanggapan dalam panggilan ini.

RFC 3261 mendefinisikan jenis respon SIP dalam kategori berikut (Stallings, 2003):

- *Provisional* (1xx): Permintaan itu dikirim dan sedang diproses.
- *Success* (2xx): Aksi ini berhasil dikirim, dipahami, dan diterima.
- *Redirection* (3xx): Tindakan selanjutnya perlu diambil untuk menyelesaikan permintaan.
- *Client Error* (4xx): Permintaan berisi sintaks yang buruk atau tidak dapat dipenuhi di server ini.
- *Server Error* (5xx): Server gagal untuk memenuhi permintaan yang berlaku.
- *Global Failure* (6xx): Permintaan tidak dapat dipenuhi pada server apapun.

Digit pertama dari Status-Code mendefinisikan kategori respon. Jadi tanggapan antara 100 dan 199 disebut sebagai "1xx" respon dan dilakukan untuk jenis lainnya. Jika respon yang diterima memiliki bentuk Status-Code seperti YXX yang tidak dipahami oleh pihak penerima, maka respon tersebut diberlakukan sebagai respon y00. Seperti contoh jika klien menerima respon 345 yang tidak diketahui, maka respon tersebut diperlakukan sebagai 300 respon. Sebuah 1xx diketahui diperlakukan sebagai 183 (Session di Progress). Jadi setiap *user-agent* harus tahu bagaimana bereaksi terhadap 100.183.200.300.400.500 dan 600.

Contoh yang lain, perhatikan gambar berikut:



Sumber : http://www.siptutorial.net/SIP/example.html

Gambar 1.9 Contoh SIP dengan Trapezoid

Pada Gambar 1.9 menerangkan bahwa user1 menggunakan softphone untuk berhubungan dengan telepon SIP dari user2. Server1 dan server2 membantu untuk mengatur sesi pengguna. Pengaturan umum kedua proxy ini dan pengguna akhir disebut "SIP Trapezoid" seperti yang digambarkan oleh garis putus-putus pada gambar tersebut. Pesan muncul secara vertikal dalam urutan mereka sebagai contoh yaitu pesan yang pertama muncul (INVITE M1) diikuti oleh pesan selanjutnya. Arah panah menunjukkan pengirim dan penerima masing-masing pesan. Setiap pesan berisi 3 digit nomor yang diikuti dengan nama dan masing-masing diberi label dengan 'M' dan nomor seri. 3-digit nomor adalah kode numerik pesan terkait dipahami dengan mudah oleh mesin seperti yang sudah dijelaskan pada bagian kategori respon SIP. Pengguna, dalam hal ini manusia, menggunakan nama untuk mengidentifikasi pesan.

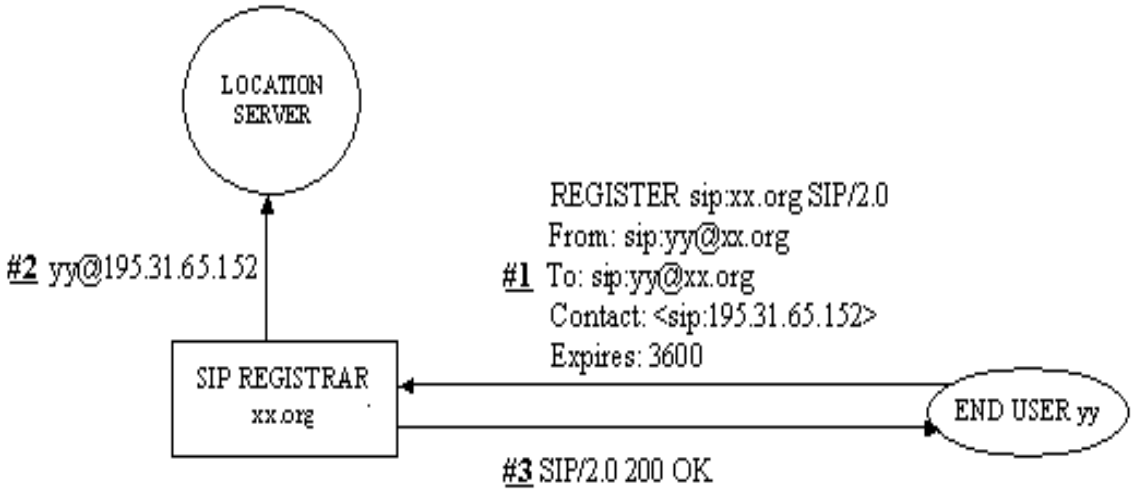
Transaksi dimulai dengan user1 membuat INVITE permintaan user2. Tapi user1 tidak tahu lokasi yang tepat dari user2 di jaringan IP. Jadi mengirim permintaan ke server1. Server1 atas nama user1 meneruskan permintaan INVITE untuk user2 ke server2. Server2 mengirimkan respon

TRYING kepada user1 memberitahukan bahwa server2 berusaha untuk mencapai user2. Server2 akan mengetahui lokasi user1 dengan REGISTRAR proxy seperti contoh sebelumnya, karena setiap user pasti sudah terdaftar pada REGISTRAR proxy yang ada (lihat Gambar 1.10).

Penerimaan INVITE M2 dari server1, server2 bekerja dengan cara yang sama dengan server1. Server2 meneruskan sebuah INVITE request untuk user2 (catatan: saat ini server2 sudah mengetahui lokasi user2, Jika tidak tahu lokasi, itu akan diteruskan ke server proxy lain sehingga INVITE request dapat melakukan perjalanan melalui beberapa proxy sebelum mencapai user2). Setelah meneruskan INVITE M3 server2 mengeluarkan respon TRYING ke server1.

Saat menerima pesan INVITE, Telepon SIP mulai berdering menginformasikan user2 bahwa permintaan panggilan telah datang. Ini mengirimkan respon RINGING kembali ke server2 yang mencapai user1 melalui server1. Jadi user1 mendapat umpan balik dari user2 yang telah menerima INVITE request. User2 pada saat ini memiliki pilihan untuk menerima atau menolak panggilan. Mari kita berasumsi bahwa dia memutuskan untuk menerimanya. Segera setelah ia menerima panggilan, OK respon dengan kode 200 dikirim oleh telepon ke server2. Menapak jalur INVITE, mencapai user1. The softphone dari user1 mengirim pesan ACK untuk mengkonfirmasi pengaturan panggilan. 3 jalan (INVITE + OK + ACK) ini digunakan untuk pengaturan call yang dapat diandalkan. Perhatikan bahwa pesan ACK tidak menggunakan proxy untuk mencapai user2 seperti sekarang user1 tahu lokasi yang tepat dari user2.

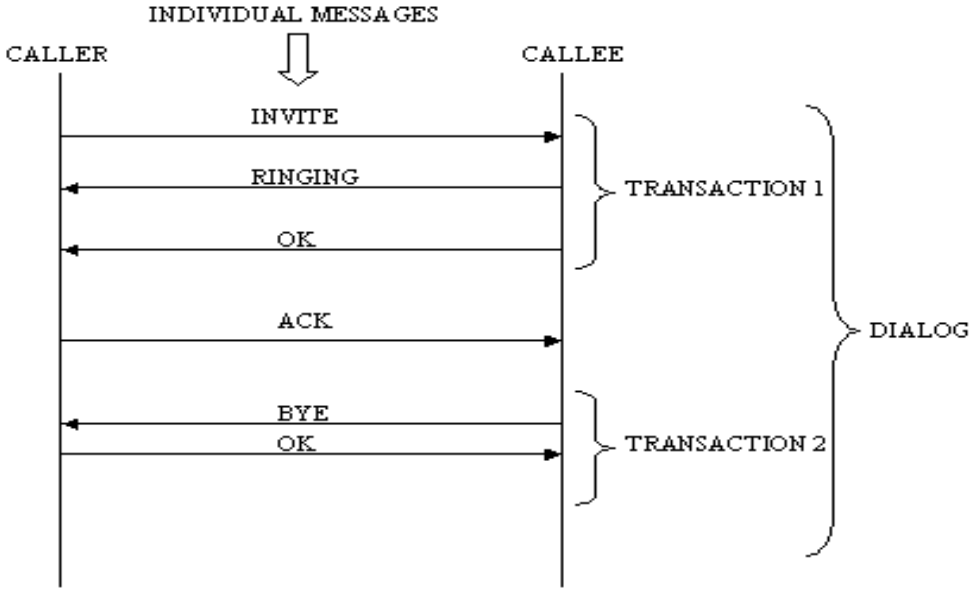
Setelah sambungan telah diatur, media mengalir antara dua endpoint. Aliran Media dikontrol menggunakan protokol yang berbeda dari SIP misalnya RTP. Ketika salah satu pihak dalam sesi memutuskan hubungan/panggilan (user2 dalam kasus ini), maka user2 mengirim pesan BYE ke user1 dan user1 mengirimkan 200 pesan OK untuk mengkonfirmasi pemutusan sesi.



Sumber : http://www.siptutorial.net/SIP/registration.html

Gambar 1.10 Registrasi pada SIP

Apabila masih terdapat kekeliruan dalam pemahaman akan hubungan antara *Call, Dialog, Transaction* dan *Message*, berikut ini penjelasan tambahan untuk ke-4 hal tersebut.



Sumber : http://www.siptutorial.net/SIP/relation.html

Gambar 1.11 Relasi antara Call, Dialog, Transaction and Messages

- *Message* adalah badan tekstual individu dipertukarkan antara server dan klien. Ada dua jenis pesan yaitu *Requests* dan *Responses*.
- *Transaction* terjadi antara klien dan server dan terdiri dari semua pesan dari permintaan pertama yang dikirim dari klien ke server sampai akhir (non-1xx) respon yang dikirim dari server ke klien. Jika permintaan tersebut INVITE dan respon akhir adalah non-2xx, *transaction* juga mencakup ACK untuk respon. ACK untuk respon 2xx ke INVITE request adalah *transaction* yang terpisah.
- *Dialog* adalah hubungan SIP peer-to-peer antara dua UA yang berlangsung selama beberapa waktu. Sebuah *dialog* diidentifikasi oleh Call-ID, *local tag* dan *remote tag*. Sebuah *dialog* biasanya disebut juga '*call leg*'.
- *Call* dari tujuan penelpon terdiri dari semua dialog yang terlibat. Beberapa pakar juga berpendapat bahwa sebuah *call* sama dengan sebuah sesi.

Perhatikan gambar 1.11 relasi antara *Call, Dialog, Transaction* dan *Message* digambarkan dengan jelas. RINGING merupakan sebuah respon dengan kode 1xx sedangkan OK merupakan respon dengan kode 2xx. Seorang penelepon (*Caller*) mungkin memiliki koneksi dengan sejumlah tujuan penelepon (*Callee*).

1.1.2.3.2 Intalasi Server Softswitch berbasis SIP

Sebelum melakukan instalasi Server softswitch berbasis SIP perlu mengenal

softswitch itu sendiri. *Apa yang dimaksud dengan softswitch?* Pertanyaan ini pasti akan tersirat dalam pikiran kita pada saat membaca bab ini. Softswitch secara harafiah merupakan 1 kata yang terdiri dari 2 kata, yaitu *software dan switch*. Softswitch merupakan switching berbasis software. Secara umum sistem softswitch merupakan suatu sistem komunikasi yang menggunakan elemen jaringan berupa software sebagai pusat mengendalian panggilannya. Softswitch juga sering disamakan dengan Call Agent, Call Server, atau Media Gateway Controller. Softswitch merupakan konsep komunikasi masa depan yang dikembangkan dari pendekatan PSTN, VoIP dan jaringan data. Sistem komunikasi ini dirancang untuk dapat memberikan layanan VoIP, data dan multimedia, disamping dirancang juga untuk melakukan penetrasi terhadap PSTN dalam bermigrasi ke jaringan data. Softswich dikembangkan oleh International Softswitch Consortium (ISC) yang berdiri pada bulan Mei 1999 dan berpusat San Ramon, California USA. ISC mempromosikan Softswitch sebagai arsitektur terbuka dan terdistribusi yang memungkinkan jaringan mendukung layanan voice, data dan multimedia dari perangkat pelanggan ke jaringan core, dan mendukung *interworking* jaringan dengan aplikasi yang dapat menyediakan kombinasi layanan voice, data dan multimedia tersebut (Fauzy & Suherman, 2006). Ada beberapa keuntungan dari software softswitch, yaitu sebagai berikut:

- Mengaktifkan dan mempercepat layanan NGN (*Next Generation Network*).
- Meningkatkan fleksibilitas jaringan dan menyediakan dukungan untuk beberapa aplikasi dari platform tunggal.
- Menyederhanakan *upgrade* infrastruktur dengan terbuka dan memusatkan fitur layanan.
- Menyediakan operator dengan berbagai pilihan, yang memungkinkan untuk membangun '*best of breed*' atau perkembangan jaringan terbaik dengan produk dari beberapa vendor.

Selain beberapa keuntungan tersebut, server softswitch juga menyediakan fungsionalitas kontrol pemanggilan, yaitu sebagai berikut:

- Menjaga kondisi panggilan
- Menyediakan layanan yang akan mengubah panggilan
- Berkomunikasi dengan fungsi control pemanggilan untuk pembentukan dan pelepasan panggilan
- Permintaan layanan dari fungsi dalam layer fungsionalitas *service control*
- Permintaan penentuan, alokasi, dan pelepasan sumber dari pembawa fungsi control.
- Menerapkan serangkaian kebijakan dan mekanisme untuk satu set (IP) sumber transportasi untuk memastikan bahwa sumber daya yang dialokasikan cukup untuk memungkinkan standar QoS (*Quality of Services*) melewati control domainnya.

Perhatikan Gambar 1.4 arsitektur dari softswitch digambarkan dengan memiliki 8 arsitektur utama, yaitu sebagai berikut:

1) **Application Server** adalah elemen jaringan yang menyediakan aplikasi tambahan di luar fitur teleponi yang membutuhkan server tersendiri, misalnya voice mail, prepaid call, fixed-SMS, dll.
2) **Feature Server** adalah elemen jaringan yang berfungsi sebagai penyedia aplikasi fitur teleponi.
3) **Media Gateway** adalah elemen jaringan yang berfungsi sebagai elemen transport untuk merutekan trafik dalam jaringan softswitch dan juga mengirim atau menerima trafik dari jaringan lain yang berbeda, seperti PSTN, PLMN dan jaringan akses pelanggan.
4) **Signaling Gateway** adalah elemen jaringan yang berfungsi sebagai interface pensinyalan dari jaringan sofswitch ke SS7 PSTN atau PLMN.
5) **Media Server** adalah elemen jaringan berfungsi membantu Softswitch untuk melakukan pemprosesan panggilan yang terjadi pada media stream, seperti penyediaan dial-tone, sarana conference, announcement, dll.
6) **Operating Support System** (OSS) adalah elemen jaringan yang berfungsi untuk mendukung operasi dan pemeliharaan jaringan, seperti manajemen jaringan, provisioning, billing, monitoring, statistik, dll.
7) ***Media akses*** adalah media yang digunakan oleh jaringan softswitch untuk menjangkau pelanggan. Media akses dapat menggunakan cable modem, leased circuit, V5.2, DSL, HFC, FTTH/FTTC dan radio access.
8) ***Perangkat akses*** adalah perangkat yang digunakan di sisi pelanggan (CPE) untuk melakukan akses ke jaringan softswitch. Perangkat akses dapat berupa node berbasis paket IP, terminal analog, dan perangkat terpadu yang memiliki port analog dan data paket (IAD, MTA, dll).

Sedangkan untuk arsitektur fungsional softswitch yang digambarkan pada Gambar 1.6 memiliki 4 layer (Munadi, Softswitch Layanan dan Aplikasi, 2009), yaitu sebagai berikut:

1) ***Call Control & Signaling Plane*** merupakan bagian jaringan yang berfungsi sebagai pengendali proses pembangunan dan pemutusan hubungan yang melibatkan elemen-elemen jaringan pada layer yang lain berdasarkan *signaling message* yang diterima dari *Transport Plane*. Elemen utama bidang ini adalah *Softswitch* (*call agent* atau *Media Gateway Controler*).
2) ***Service/Application Plane*** merupakan bagian jaringan yang menyediakan dan mengeksekusi satu atau beberapa aplikasi layanan di dalam jaringan softswitch. Di dalam layer ini termasuk juga Application server dan Feature server. Service/Application Plane juga mengontrol Media Server yang

memberikan fungsi seperti *conference, IVR, tone processing*, dll.

3) ***Transport Plane*** merupakan bagian jaringan yang berfungsi sebagai media transport bagi semua *message* di jaringan, seperti: *call signaling, call & media setup* atau *informasi voice atau datanya sendiri*. *Transport Plane* dibagi dalam tiga domain, yaitu;

   a. *IP Transport Domain*, yaitu fungsi transport pada layer IP. Domain ini merupakan backbone IP yang dilengkapi dengan border gateway, mekanisme ruting dan QoS *(Router, switches, dll),*

   b. *Interworking Domain (Trunk Gateway, Signaling Gateway),*

   c. *Non-IP Access Domain (Access Gateway (wireline, mobile), Integrated Access Device, Cable modem/MM Terminal Adaptor-MTA, dll)*.

4) ***Manajemen Plane*** merupakan bagian jaringan yang berfungsi untuk memberikan fungsi-fungsi dari *Operation System Support* (OSS) yaitu; fungsi sistem operasi dan pemeliharaan jaringan, *provisioning* layanan dan pelanggan, *network management* serta sistem *billing*.

Setelah semua komponen SIP dan arsitektur server softswitch dipahami, maka selanjutnya pada bagian ini akan membahas instalasi server softswitch secara *step-by-step* dengan mengacu pada petunjuk yang diberikan melalui pakar Telekomunikasi Indonesia, yaitu Onno W. Purbo (Purbo, 2007).

Bagi mereka yang ingin membuat sendiri sentral telepon Internet berbasis Session Initiation Protocol (SIP) seperti yang di kembangkan oleh VoIP Rakyat di http://www.voiprakyat.or.id, maka berikut ini adalah beberapa tip singkat untuk membangunnya. Teknologi SIP ini yang akan di adopsi oleh para operator telekomunikasi di Indonesia. Tampaknya yang mulai siap salah satunya adalah XL, yang mungkin akan di ikuti oleh Indosat.

Sebetulnya tidak banyak yang harus di instalasi untuk menjalankan Asterisk secara minimal sekali, yang hanya mempunyai fungsi untuk

- Authentikasi user dengan nomor telepon & password.
- Dial plan, untuk mengatur apa yang harus dilakukan untuk call ke sebuah nomor tertentu.
- ENUM, agar Asterisk nantinya mengenali nomor +62XXX

Peralatan yang dibutuhkan adalah

- Sebuah PC Linux, saya sendiri menggunakan Fedora Core 6.
- Sambungan LAN
- Sambungan Internet

Instalasi Asterisk

Teknik Instalasi yang perlu dikerjakan adalah

- Ambil software asterisk & asterisk sound dari http://www.asterisk.org.

Pada saat tulisan ini ditulis oleh bapak Onno W. Purbo ada dua (2) jenis / versi asterisk, yaitu,

asterisk-1.4.0.tar.gz

asterisk-1.2.15.tar.gz

Anda harus memilih versi asterisk mana yang ingin di install. Mungkin yang agak aman pada hari ini adalah versi 1.2, kecuali nanti pada saat 1.4 sudah mulaistabil. Semetara suara operator wanita yang dibutuhkan adalah

asterisk-sounds-1.2.1.tar.gz

- Sesuai petunjuk, bapak Onno W.Purbo biasanya akan mengcopykan semua file yang dia butuhkan tersebut ke folder /usr/local/src, melalui perintah

cp asterisk-1.4.0.tar.gz /usr/local/src/

cp asterisk-1.2.15.tar.gz /usr/local/src/

cp asterisk-sounds-1.2.1.tar.gz /usr/local/src/

- Menginstalasi asterisk tidak sukar, cara yang perlu dilakukan untuk asterisk-1.4 agak berbeda dengan asterisk-1.2 sebelumnya dengan menambahkan ./configure, yaitu

cd /usr/local/src

tar zxvf asterisk-1.4.0.tar.gz

cd asterisk-1.4.0

./configure

make

make install

make samples

- Asterisk-1.2.15 merupakan versi terakhir dari asterisk-1.2 pada saat naskah ini ditulis, perintah yang perlu dijalankan untuk menginstalasi adalah

cd /usr/local/src

tar zxvf asterisk-1.2.15.tar.gz

cd asterisk-1.2.15

make

make install

make samples

- Selanjutnya install suara operator asterisk, melalui perintah

cd /usr/local/src

tar zxvf asterisk-sounds-1.2.1.tar.gz

cd asterisk-sounds-1.2.1

make install

Seleai sudah proses instalasi asterisk. Langsung selanjutnya yang perlu dilakukan adalah mengkonfigurasi agar sesuai dengan apa yang kita inginkan.

Konfigurasi Asterisk Minimal Sekali

Konfigurasi Asterisk yang aman sangat minimal dengan misi untuk meng-authentikasi user, mengkonfigurasi dial-plan dan

mengenalkan ENUM tidak banyak yang harus dilakukan. Seluruh proses konfigurasi merupakan proses editing file-file yang ada di folder

/etc/asterisk

File yang perlu diperhatikan tidak banyak, hanya,

sip.conf - untuk authentikasi user dengan nomor telepon dan password.

extensions.conf - untuk mengatur dialplan.

enum.conf - untuk memperkenalkan nomor +62XX.

Masih banyak file-file konfigurasi lainnya, sangat di sarankan bagi anda yang ingin secara serius mempelajari asterisk untuk membaca-baca file-file konfigurasi yang ada di /etc/asterisk/

Konfigurasi ENUM.CONF

Tidak banyak yang harus di ubah di /etc/asterisk/enum.conf, hanya pastikan bahwa ada entry

search => e164.arpa

search => e164.org

search => e164.id

Dengan cara itu, kita dapat pastikan bahwa informasi ENUM yang ada di e164.arpa, e164.org dan e164.id akan dapat di ketahui dengan baik oleh asterisk kita.

Konfigurasi SIP.CONF

Pada file /etc/asterisk/sip.conf, untuk sebuah account dengan nomor telepon 2099, password 123456, IP address dinamis menggunakan DHCP maka entry yang digunakan adalah:

[2099]

context=default

type=friend

username=2099

secret=123456

host=dynamic

dtmfmode=rfc2833

mailbox=2099@default

Untuk asterisk-1.4, agar dial tone dapat di handel dengan baik maka perlu ditambahkan di tambahan entry berikut:

rfc2833compensate=yes

Masukan entry di atas untuk masing-masing user.

Sampai titik ini maka masing-masing user dapat meregistrasikan diri ke asterisk dan dapat menelepon satu sama lain dengan mereka yang terdaftar di asterisk server yang kita operasikan. Agar asterisk server kita dapat berbicara dengan user lain di XL. Indosat, VoIP Rakyat, di Pulver atau di SIP Proxy yang banyak bertebaran di Internet, kita perlu meregistrasikan diri ke SIP Proxy server tersebut. Perintah yang digunakan adalah

register => 2345:password@sip_proxy/1234

yang artinya, user 1234 di asterisk server yang kita operasikan merupakan user 2345 di sip_proxy yang login ke sana menggunakan password "password". Misalnya seseorang user 2000 mempunyai account 20345 di server voiprakyat.or,id dengan password "rahasia" maka format yang digunakan adalah

register => 20345:rahasia@voiprakyat.or,id/2000

Dengan cara ini, maka ada panggilan di VoIP Rakyat ke nomor 20345 akan langsung di forward ke nomor 2000 di SIP server yang kita gunakan.

Konfigurasi EXTENSIONS.CONF

Pada file /etc/asterisk/extensions.conf kita dapat mengatur apa yang harus dilakukan oleh asterisk jika menerima sebuah panggilan ke nomor extension tertentu, yang sering digunakan adalah

exten => _20XX,1,Dial(SIP/${EXTEN},20,rt)

exten => _20XX,2,HangUp

Cara membaca perintah di atas adalah sebagai berikut

Jika ada orang yang menelepon ke extension 20XX maka langkah 1 yang harus di kerjakan adalah DIAL EXTENsiontersebut mengunakan teknologi SIP, tunggu 20 detik, jika tidak di angkat maka time out (rt). Langkah ke 2 yang harus dilakukan adalah HangUp. Tentunya anda perlu mengatur sedikit-sedikit perintah ini agar sesuai dengan kondisi yang anda gunakan di SIP Server anda.

Beberapa perintah berbahaya yang sering dicari orang adalah sebagai berikut

exten => _0711X.,1,Dial(SIP/${EXTEN:4}@2031,20.rt)

Cara membaca-nya adalah,

Jika ada orang yang menelepon ke 0711X. Perhatikan titik sesudah X, berarti berapapun dibelakang X tidak di perdulikan. DIAL menggunakan teknologi SIP ke nomor 2031. Perhatikan baik-baik kode {EXTEN:4} ini harus di baca - buang empat (4) digit di depan nomor EXTENsion sebelum dimasukan ke 2031 - jadi 07115551234 menjadi 5551234.

Jika kita menggunakan PABX antara ATA dengan Telkom, maka perintah yang digunakan menjadi

exten => _021X.,1,Dial(SIP/9${EXTEN:3}@2031,20.rt)

Cara membaca-nya adalah

Jika ada orang yang menelepon ke 021X. Perhatikan titik sesudah X, berarti berapapun dibelakang X tidak di perdulikan. DIAL menggunakan teknologi SIP ke nomor 2031. Perhatikan baik-baik kode 9{EXTEN:3} ini harus di baca buang tiga (3) digit di depan nomor EXTENsion yang di dial kemudian tambahkan 9 - jadi 0215551234 menjadi 95551234. Artinya jika nomor 2031 merupakan sebuah Analog Telepon Adapter (ATA) seperti SPA3000 yang berada di jakarta dan sambungkan ke PABX di Jakarta.

Maka siapapun yang berada di jaringan VoIP Tersebut akan dapat menelepon Jakarta tanpa perlu membayar SLJII maupun SLI. Orang yang mempunyai ATA tetap harus membayar pulsa lokal untuk menelelpon ke nomor ang di tuju.

Cara yang sama dapat di kembangkan untuk menelepon selular dengan cara menyambungkan ATA yang kita gunakan ke telkom. Perintah yang digunakan adalah sebagai berikut

exten => _08X.,1,Dial(SIP/${EXTEN}@2031,20.rt)

Tentunya untuk sebuah kantor yang tersambung ke jaringan VoIP Publik tidak akan mau membuka akses agar semua orang dapat menelepon semua nomor selular atau Telkom, oleh karenanya biasanya kita tidak menggunakan kode-kode 021X., atau 08X. Tapi kita akan memasukan satu per satu nomor-nomor yang di ijinkan di telepon melalui VoIP, misalnya,

exten => _0811567854,1,Dial(SIP/${EXTEN}@2031,20.rt)

exten => _0216575675,1,Dial(SIP/${EXTEN}@2031,20.rt)

exten => _0216755675,1,Dial(SIP/${EXTEN}@2031,20.rt)

Artinya hanya nomor 0811567854, 0216575675 dan 0216755675 yang dapat dihubungi melalui VoIP nomor selain nomor-nomor ini tidak dapat dihubungi.

Untuk mengadopsi nomor telepon +62XXX maupun nomor telepon lainnya kita dapat memasukan ENUMLOOKUP menggunakan perintah

exten => _62X.,1,ENUMLOOKUP(${EXTEN},sip,,1,e164.id)

exten => _62X.,2,Dial(${ENUM})

exten => _62X.,102,Playback(im-sorry)

atau

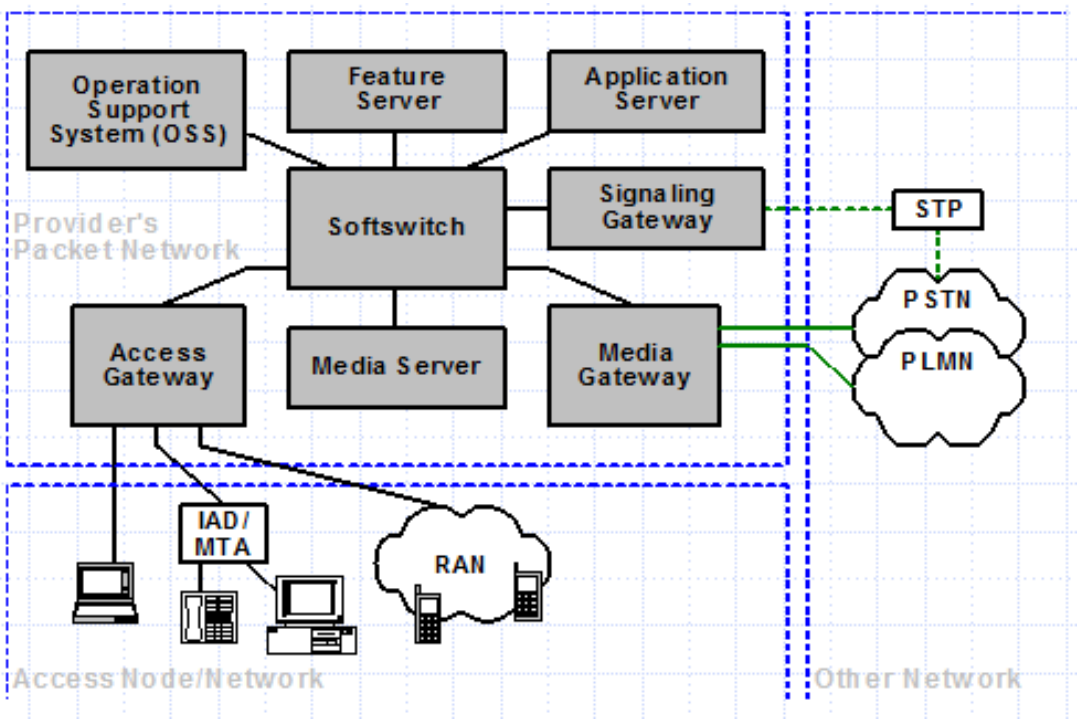
exten => _+X.,1,ENUMLOOKUP(${EXTEN},sip,,1,e164.id)

exten => _+X.,2,Dial(${ENUM})

exten => _+X.,102,Playback(im-sorry)

1.1.2.4 Mengasosiasi/Menalar

Dari informasi yang didapat pada bagian mencoba/mengumpulkan informasi dan gambar yang diamati pada bagian observasi, konfigurasi jaringan untuk instalasi server softswitch berbasis SIP dapat digambarkan seperti berikut:



Sumber : Dokumen Kemendikbud

Gambar 1.11 Konfigurasi Jaringan Softswitch

Dari konfigurasi jaringan tersebut maka jaringan softswitch dapat dilihat terbentuk dari elemen-elemen fungsi jaringan sebagai berikut:

- Softswitch (disebut juga dengan Call Agent (CA), Media Gateway Controller (MGC)),
- Feature Server,
- Application Server (AS),
- Media Gateway (MG),
- Signaling Gateway (SG),
- Media Server (MS), dan
- Operation Support System (OSS)

Elemen-elemen di atas saling berinteraksi membentuk fungsi sistem jaringan softswitch dalam menyediakan layanan kepada pelanggan.

1.1.3 Rangkuman

Konsep dasar layanan yang dapat diberikan oleh softswitch berbasis SIP adalah untuk mendukung kebutuhan konvergensi layanan masa depan (*Next Generation Network – NGN)* , yaitu terintegrasinya layanan suara dan data dalam satu platform jaringan. Oleh karena itu implementasi jaringan berbasis softswitch didesain untuk menyediakan layanan berupa teleponi, data, Internet, dan multimedia.

Konsep dasar penyediaan layanan teleponi oleh softswitch adalah harus mampu menyediakan layanan teleponi minimal setingkat dengan layanan yang sudah diberikan oleh PSTN dengan berbagai kelengkapan fiturnya. Layanan teleponi yang diberikan juga hendaknya mengakomodasi jenis-jenis layanan yang sudah diberikan

kepada pelanggan selama ini, diantaranya sebagai berikut:

- Komunikasi lokal,
- Komunikasi jarak jauh,
- Komunikasi internasional,
- Emergency services,
- Number portability,
- Televoting,
- Prepaid dan postpaid,
- Service class
- Voice VPN
- Toll free

Berdasarkan konfigurasi jaringan yang telah dipaparkan pada bagian sebelumnya, beberapa komponen yang ada dalam server sofswitch adalah sebagai berikut:

- *Feature Server* adalah elemen jaringan yang berfungsi sebagai penyedia aplikasi fitur teleponi.
- *Application Server* adalah elemen jaringan yang menyediakan aplikasi tambahan di luar fitur teleponi yang membutuhkan server tersendiri, misalnya voice mail, prepaid call, fixed-SMS, voice VPN, dll.
- *Media Gateway* adalah elemen jaringan yang berfungsi sebagai elemen transport untuk merutekan trafik dalam jaringan softswitch dan juga mengirim atau menerima trafik dari jaringan lain yang berbeda, seperti PSTN, PLMN, dan jaringan akses pelanggan.
- *Signaling Gateway* adalah elemen jaringan yang berfungsi sebagai interface pensinyalan dari jaringan sofswitch ke SS7 PSTN atau PLMN.
- *Media Server* adalah elemen jaringan berfungsi membantu Softswitch untuk mendukung layanan/aplikasi seperti messaging, audio dan video conferencing, music on hold, announcement, dll.
- *Operating Support System (OSS)* adalah elemen jaringan yang berfungsi untuk mendukung operasi dan pemeliharaan jaringan, seperti manajemen jaringan, provisioning, billing, monitoring, statistik, dll.

Dengan mempelajari informasi-informasi yang ada, ditarik kesimpulan bahwa untuk menjadi seorang ahli dalam pengembangan dan instalasi jaringan softswitch berbasis SIP diperlukan pemahaman tetapi juga praktikum dengan intensitas yang cukup.

1.1.4 Tugas

Tugas

Mengamati instalasi server softswitch berbasis SIP yang sudah cukup banyak diterapkan. Buatlah laporan berisi pengamatan dan pendapat anda akan server softswitch berbasis SIP!

Langkah Kerja

1. Buatlah kelompok dengan anggota 3 – 4 orang.
2. Uraikan pengamatan kelompok tentang SIP!
3. Uraikan pengamatan kelompok tentang server softswitch!
4. Uraikan pengamatan kelompok tentang instalasi server softswitch berbasis SIP!
5. Uraikan pengamatan kelompok tentang komponen server softswitch berbasis SIP dan fungsinya!
6. Buat laporan dan diskusikan dengan teman sekelompok.

Bandingkan dan Simpulkan

Presentasikan hasil kerja kelompok anda di depan kelas dan bandingkan hasil kerja kelompok Anda dengan kelompok lain.

Berdasarkan hasil perbandingan tersebut hal penting apa yang harus dirumuskan secara bersama.

1.1.5 Penilaian Diri

Dalam test ini setiap siswa harus membaca dengan cermat dan teliti setiap butir soal berikut ini. Kemudian berdasarkan aktifitas belajar siswa tulislah jawaban untuk setiap butir soal pada lembar jawaban test penilaian diri yang telah disediakan.

1. Sebutkan dan jelaskan komponen/unsure-unsur standar pada SIP!
2. Jelaskan 7 perintah pada SIP!
3. Jelaskan keuntungan menggunakan server softswitch!
4. Bagaimanakah fungsionalitas layanan yang disediakan oleh softswitch?

5. Jelaskan arsitektur utama dari server softswitch!

Lembar Kerja Penilaian Diri

LJ- 01: Sebutkan dan jelaskan komponen/unsur-unsur standar pada SIP!

……
……
……
……
……

LJ- 02: Jelaskan 7 perintah pada SIP!

……
……
……
……
……
……
……
……

LJ- 03: Jelaskan keuntungan menggunakan server softswitch!

……
……
……
……
……
……
……

LJ- 04: Bagaimanakah fungsionalitas layanan yang disediakan oleh softswitch?

……
……
……
……
……
……

LJ- 05: Jelaskan arsitektur utama dari server softswitch!

……

……

……

……

……

……

BAB II

2.1 Kegiatan Belajar 2: Konfigurasi Ekstensi dan Dial plan Server Softwitch.

2.1.1. Tujuan Pembelajaran

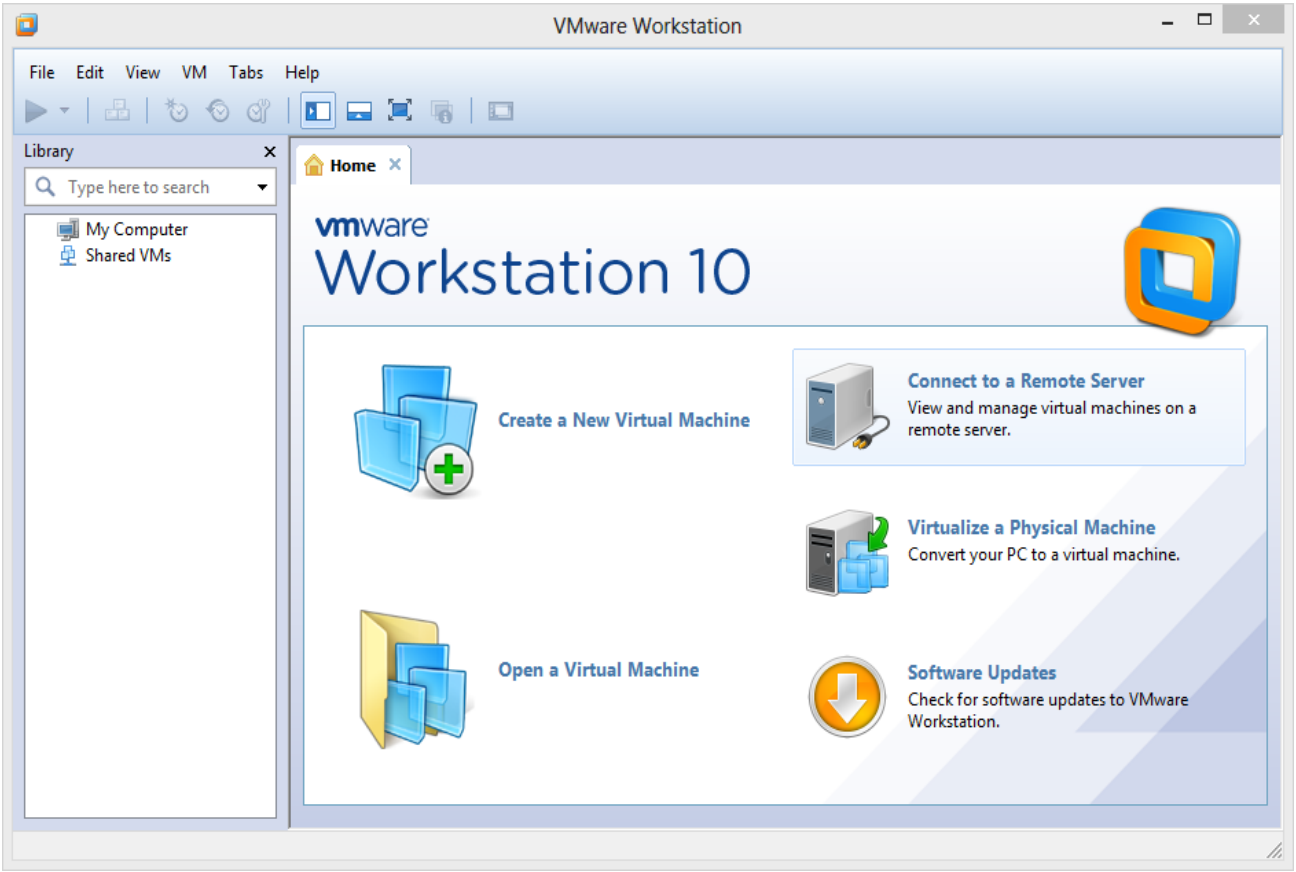
Setelah mempelajari kegiatan belajar 2 ini, diharapakan siswa dapat:

1) Memahami konfigurasi ekstensi dan dial plan server Softswitch
2) Menyajikan hasil konfigurasi ekstensi dan dial plan serber Softswitch

2.1.2 Aktifitas Belajar Siswa

2.1.2.1 Mengamati/Observasi

Amatilah proses konfigurasi ekstensi dan dial-plan server softswitch berikut:



Sumber : Dokumen Kemendikbud

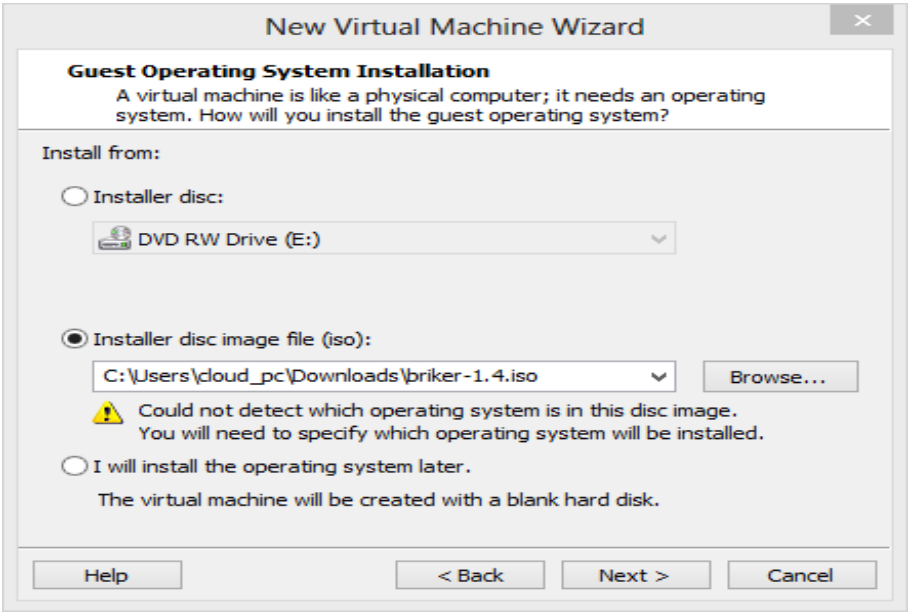
Gambar 2.1 Tampilan Awal Konfigurasi VMWare

Tampilan awal konfigurasi VMWare untuk instalasi Briker. Pada gambar 2.1, klik icon atau pada tulisan *Create a New Virtual Machine*. Kemudian akan muncul tampilan seperti gambar berikut.

Sumber : Dokumen Kemendikbud

Gambar 2.2 Tampilan tipe konfigurasi VMWare

Pada gambar 2.2, pilih atau klik option *Typical (recommended)* kemudian klik tombol Next.

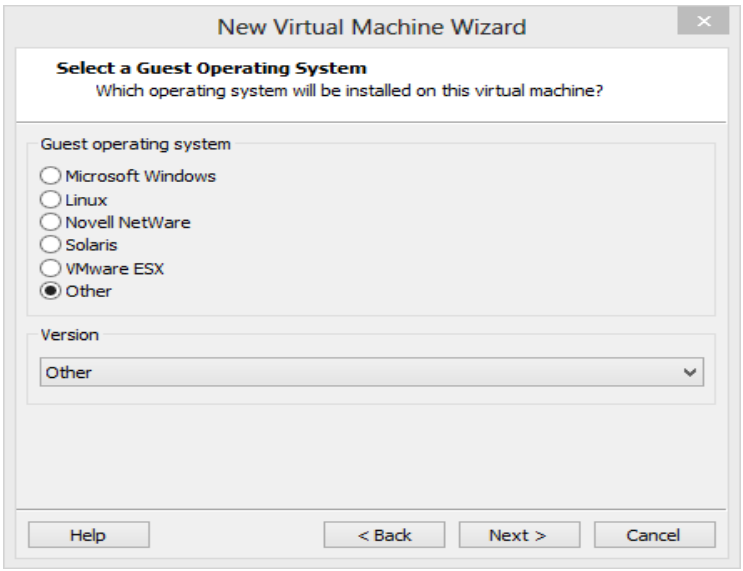


Sumber : Dokumen Kemendikbud

Gambar 2.3 Sumber Konfigurasi Briker

Kemudian pada Sumber : Dokumen Kemendikbud

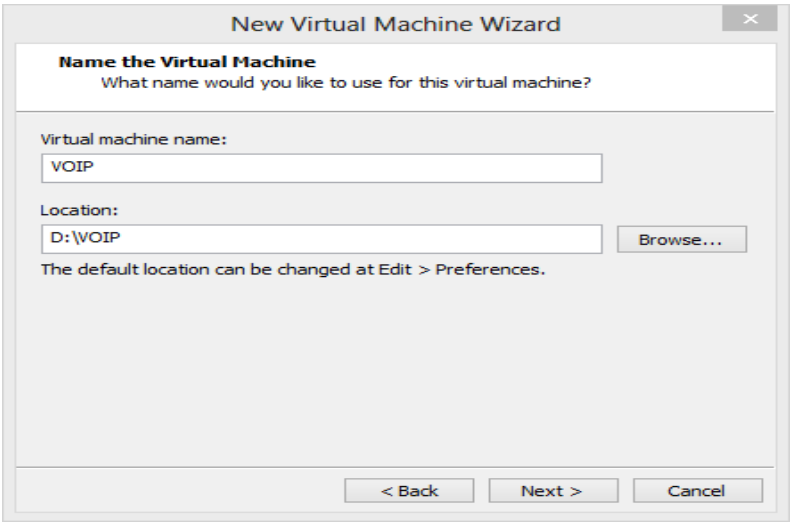
, klik/pilih option Installer disc image file (iso) lalu klik Browse dan cari file image dari Sistem Briker yang telah didownload, seperti pada gambar di atas file image system briker tersimpan di drive C:\Users\cloud_pc\Downloads\briker-1.4.iso. Kemudian klik Next



Sumber : Dokumen Kemendikbud

Gambar 2.4 Tampilan Pemilihan Jenis Sistem Operasi

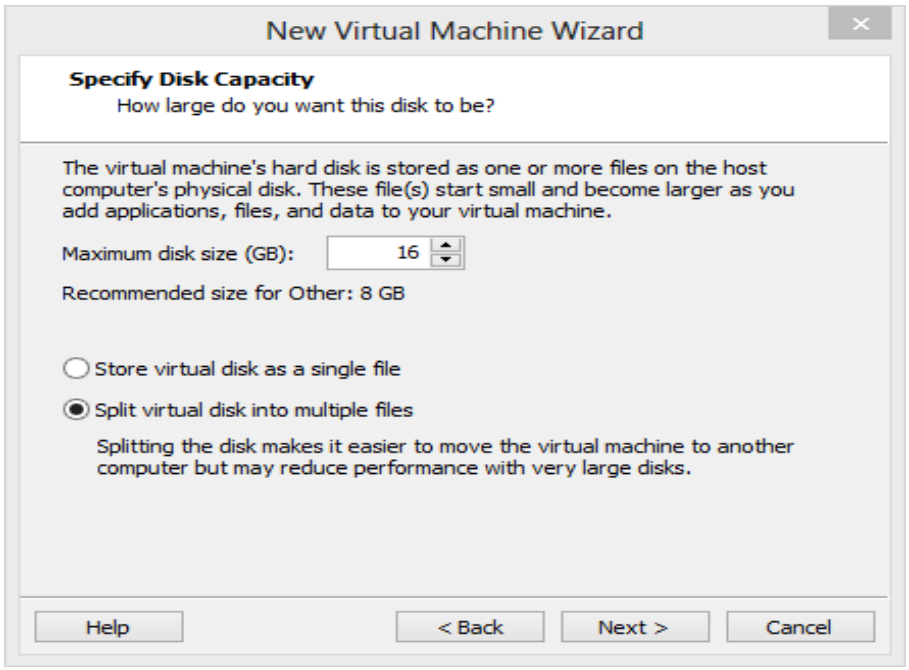
Kemudian muncul tampilan seperti pada gambar 2.4, pilih option guest operating system other dengan versi other juga. Lalu klik tombol Next.



Sumber : Dokumen Kemendikbud

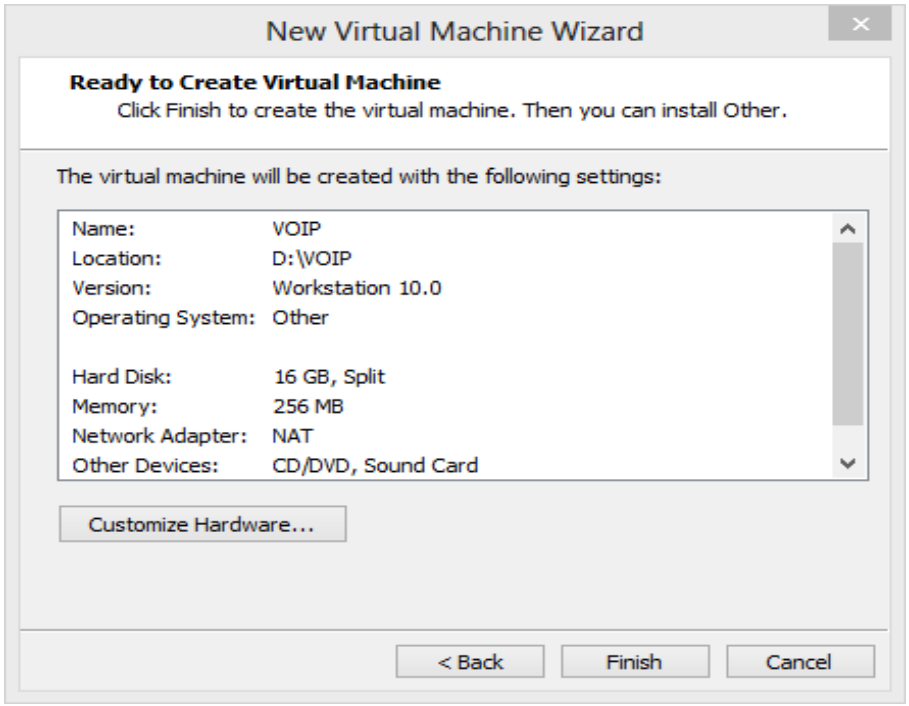
Gambar 2.5 Tampilan Simpan Nama File

Simpan nama Virtual Machine dengan menggunakan nama apa saja dan lokasi penyimpanan biasa ditentukan sendiri.



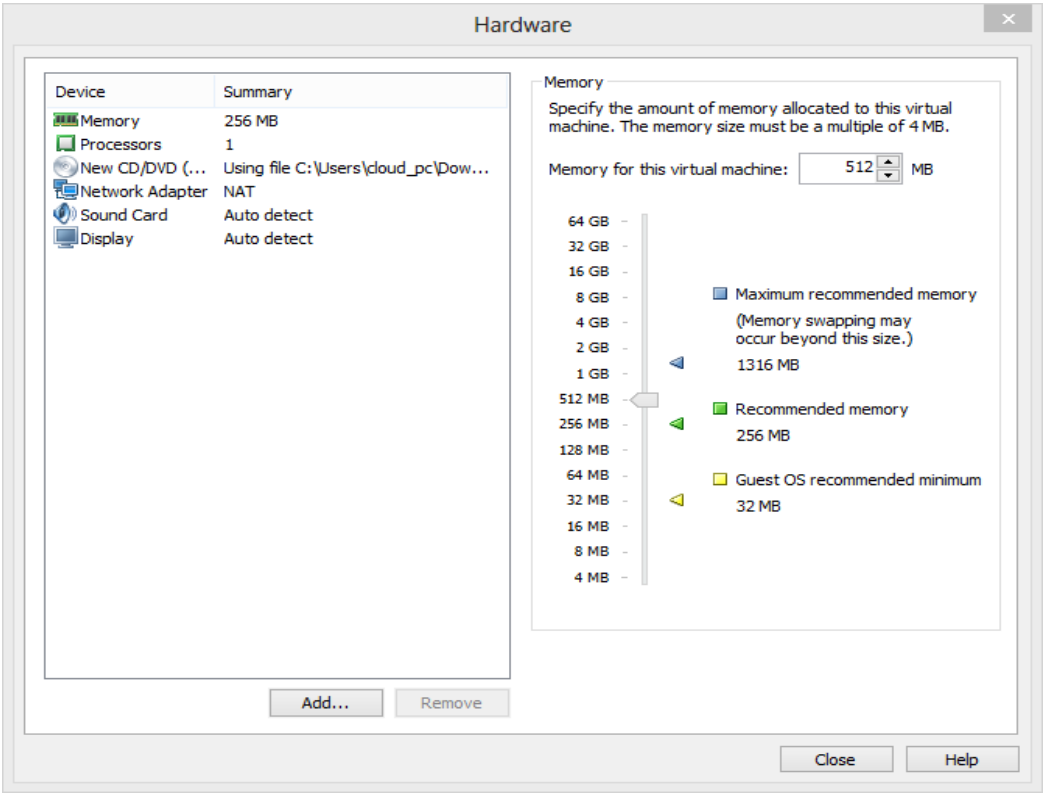
Sumber : Dokumen Kemendikbud

Gambar 2.6 Tampilan Ukuran Disk VMWare



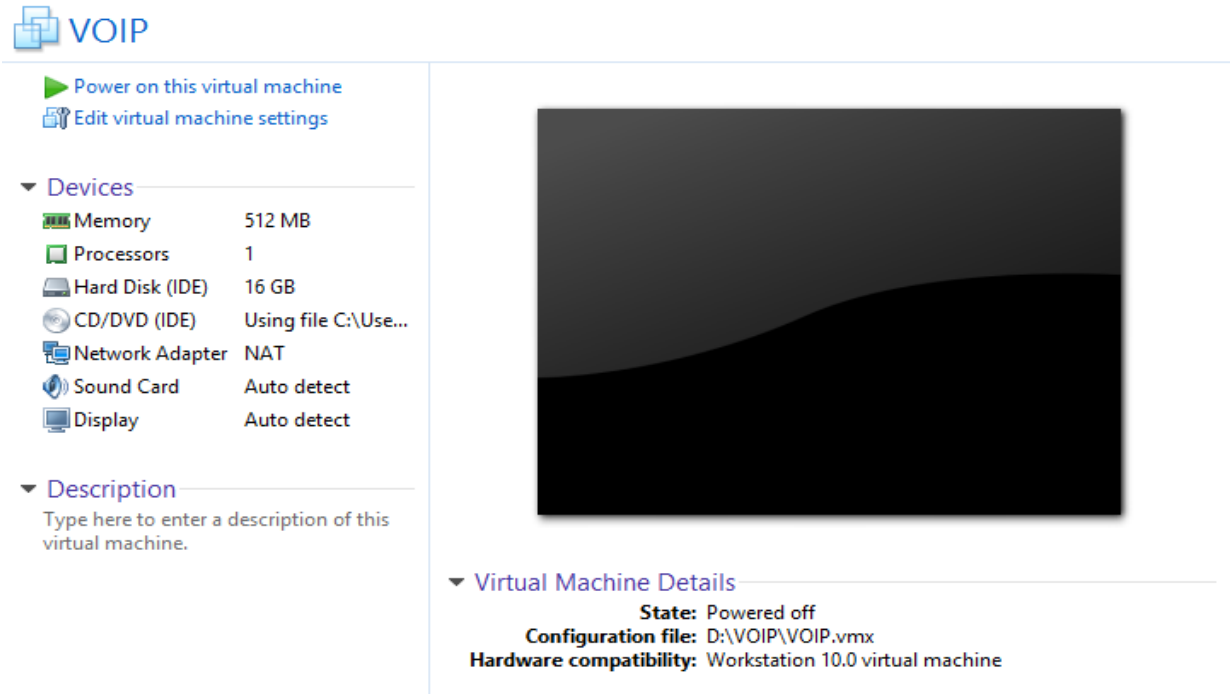
Sumber : Dokumen Kemendikbud

Gambar 2.7 Tampilan Akhir Konfigurasi VMWare



Sumber : Dokumen Kemendikbud

Gambar 2.8 Tampilan Pengaturan Hardware

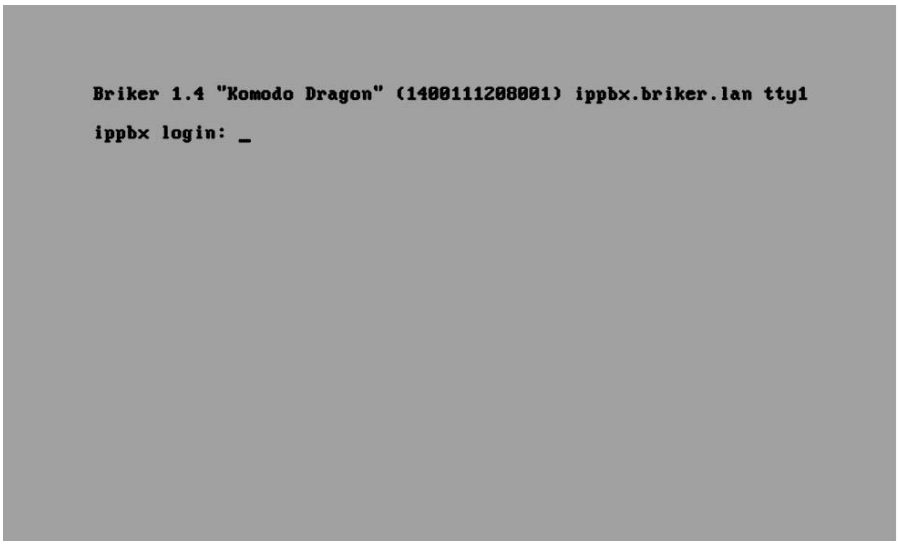


Sumber : Dokumen Kemendikbud

Gambar 2.9 Tampilan Siap Menjalankan Instalasi Briker

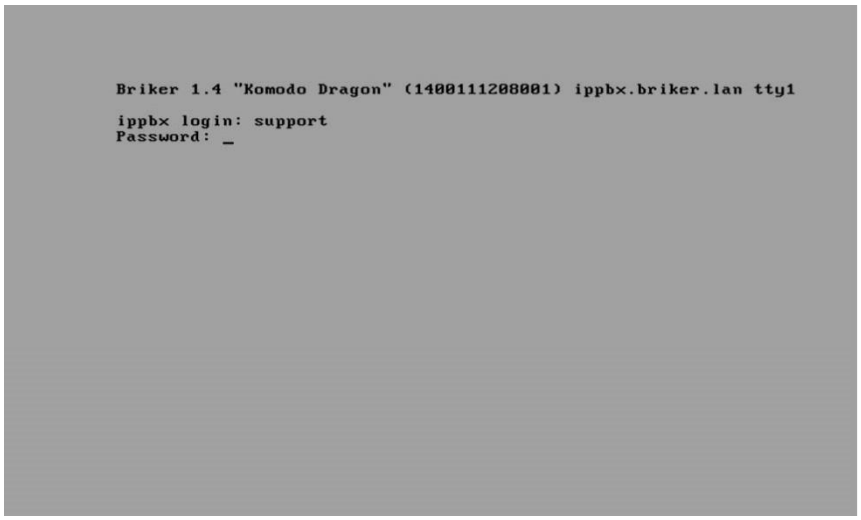
Sumber : Dokumen Kemendikbud

Gambar 2.10 Tampilan Awal Instalasi Briker



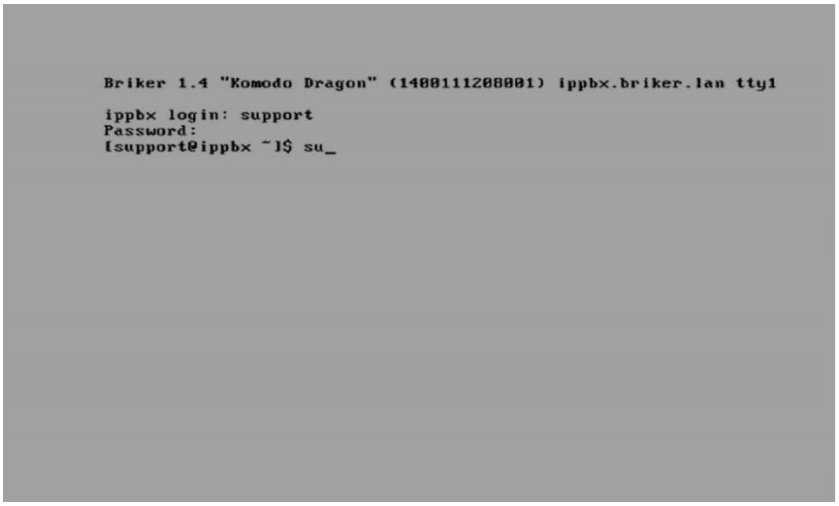
Sumber : Dokumen Kemendikbud

Gambar 2.11 Tampilan Briker berhasil Diinstal



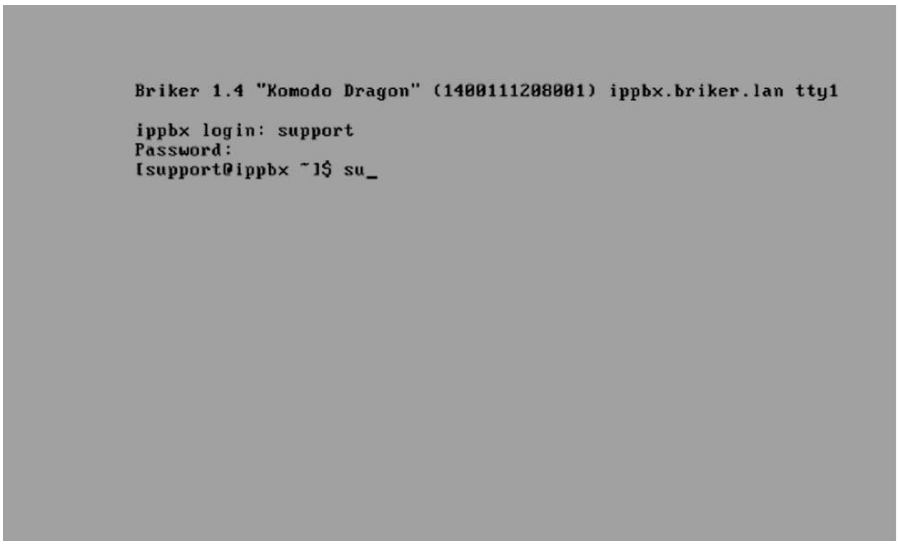
Sumber : Dokumen Kemendikbud

Gambar 2.12 Tampilan Awal Konfigurasi Briker



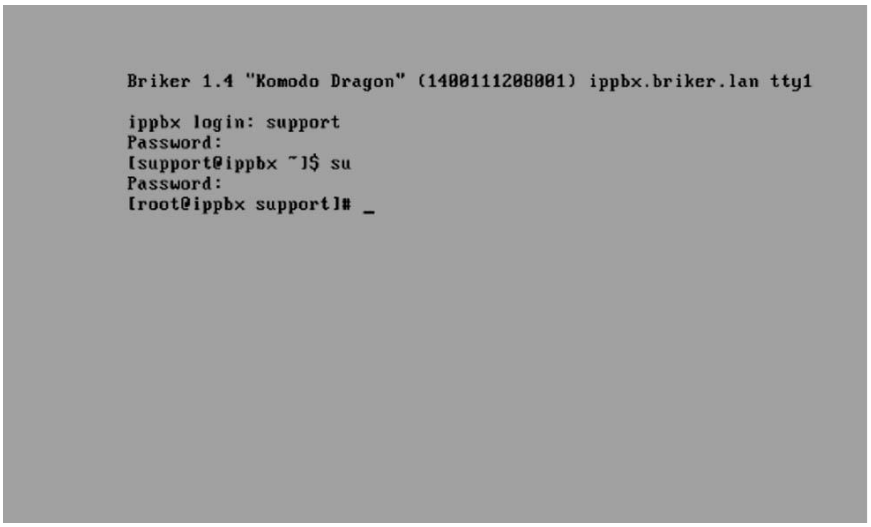
Sumber : Dokumen Kemendikbud

Gambar 2.13 Tampilan Konfigurasi 1 Briker



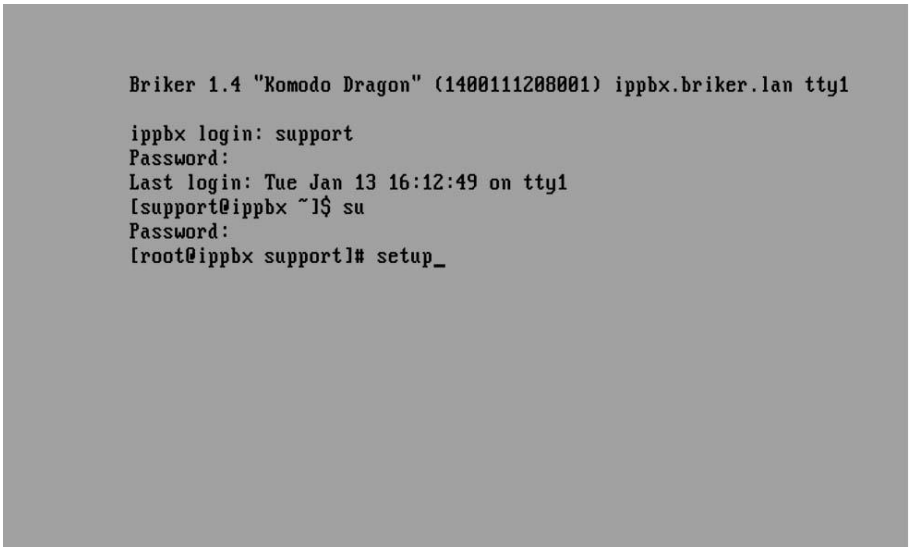
Sumber : Dokumen Kemendikbud

Gambar 2.14 Tampilan Konfigurasi 2 Briker



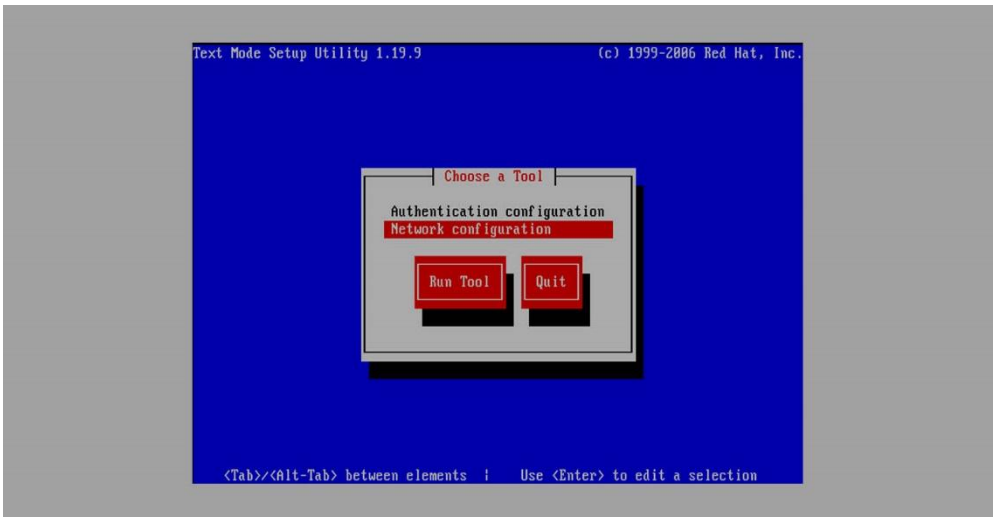
Sumber : Dokumen Kemendikbud

Gambar 2.15 Tampilan Konfigurasi 4 Briker



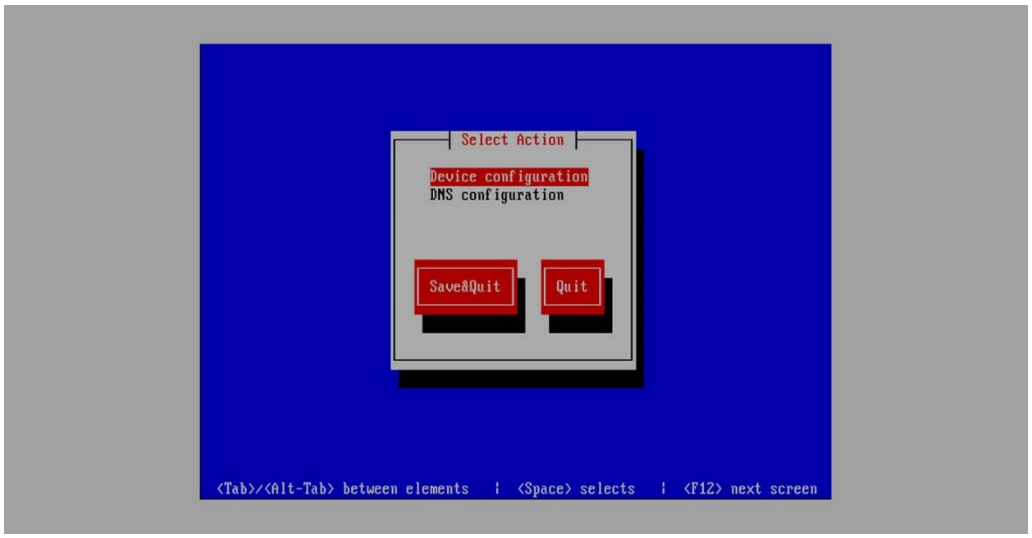
Sumber : Dokumen Kemendikbud

Gambar 2.16 Tampilan Konfigurasi 5 Briker



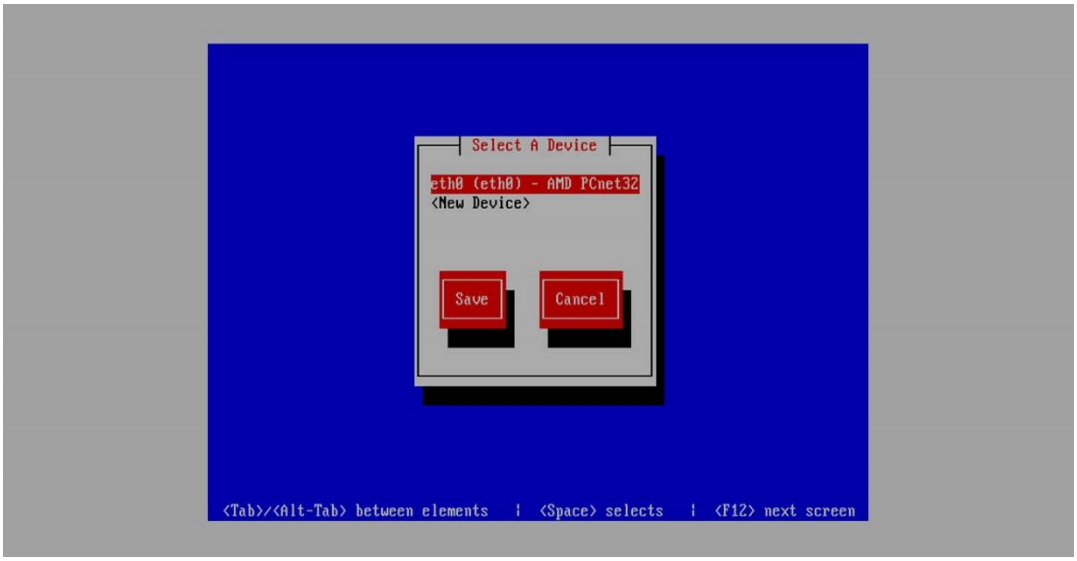
Sumber : Dokumen Kemendikbud

Gambar 2.17 Tampilan Konfigurasi 1 Alamat IP Briker



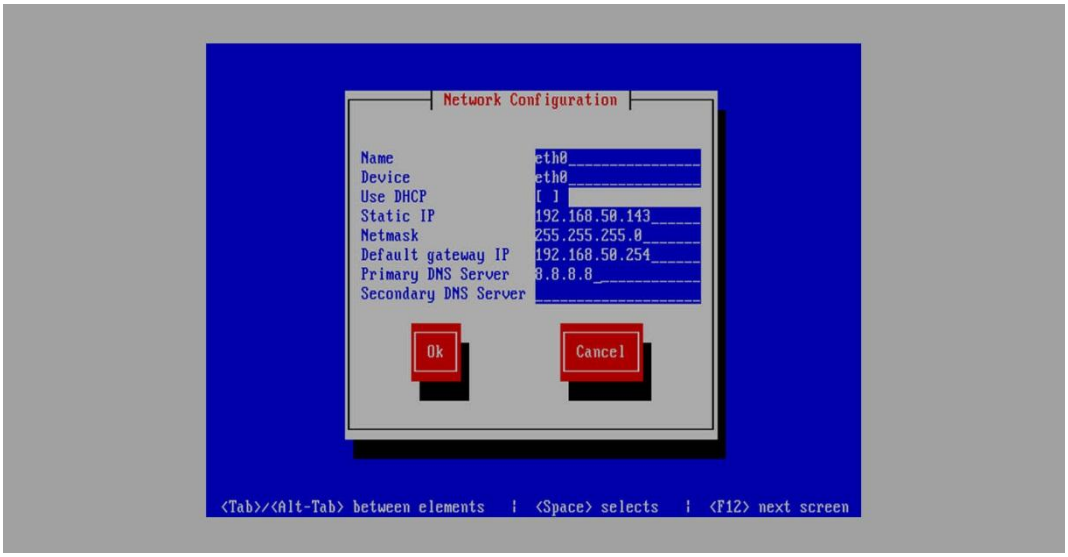
Sumber : Dokumen Kemendikbud

Gambar 2.18 Tampilan Konfigurasi 2 Alamat IP Briker



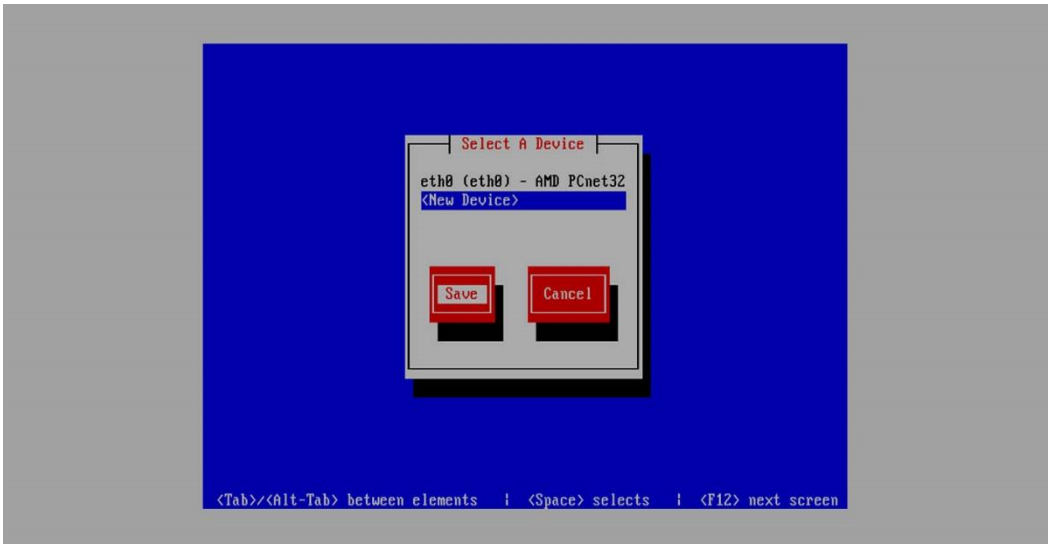
Sumber : Dokumen Kemendikbud

Gambar 2.19 Tampilan Konfigurasi 3 Alamat IP Briker



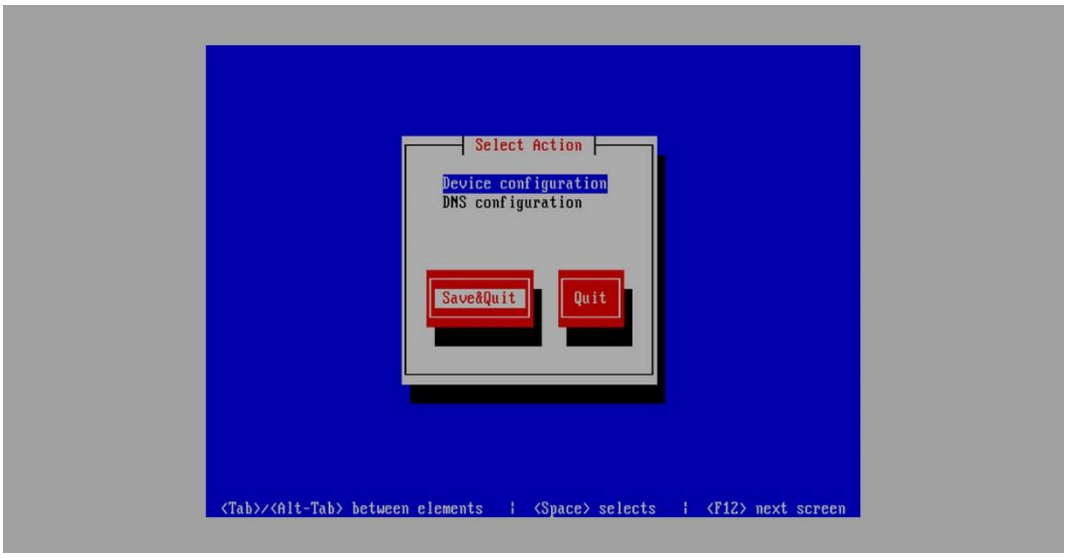
Sumber : Dokumen Kemendikbud

Gambar 2.20 Tampilan Konfigurasi 4 Alamat IP Briker



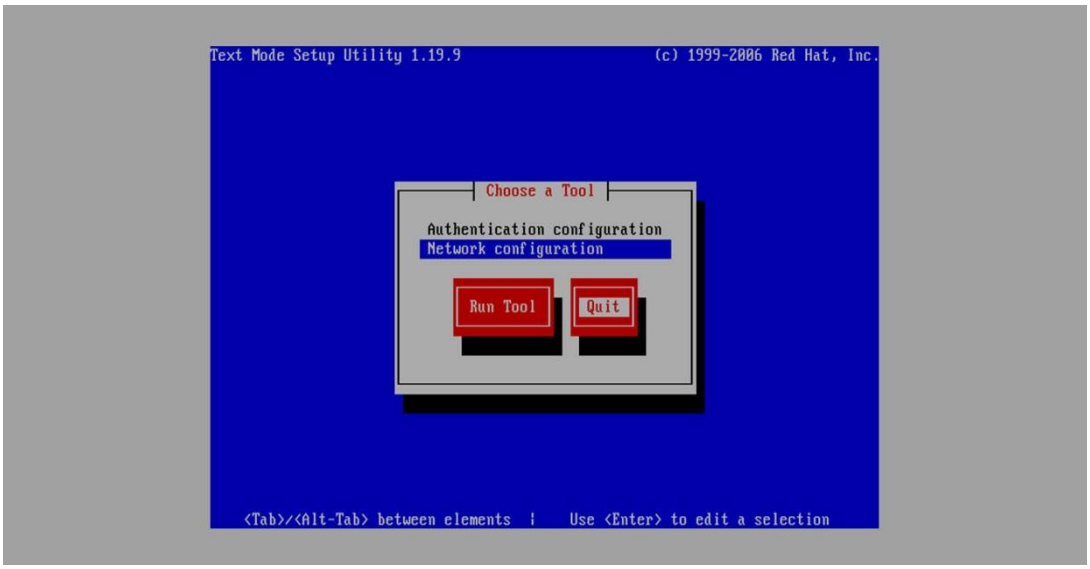
Sumber : Dokumen Kemendikbud

Gambar 2.21 Tampilan Konfigurasi 5 Alamat IP Briker



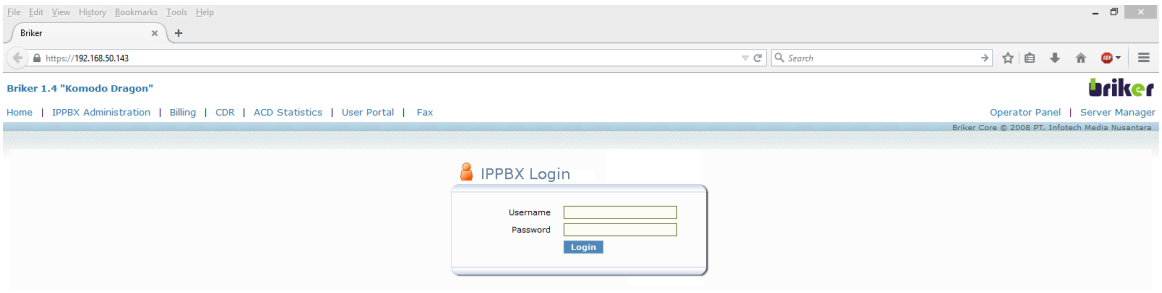
Sumber : Dokumen Kemendikbud

Gambar 2.22 Tampilan Konfigurasi 6 Alamat IP Briker



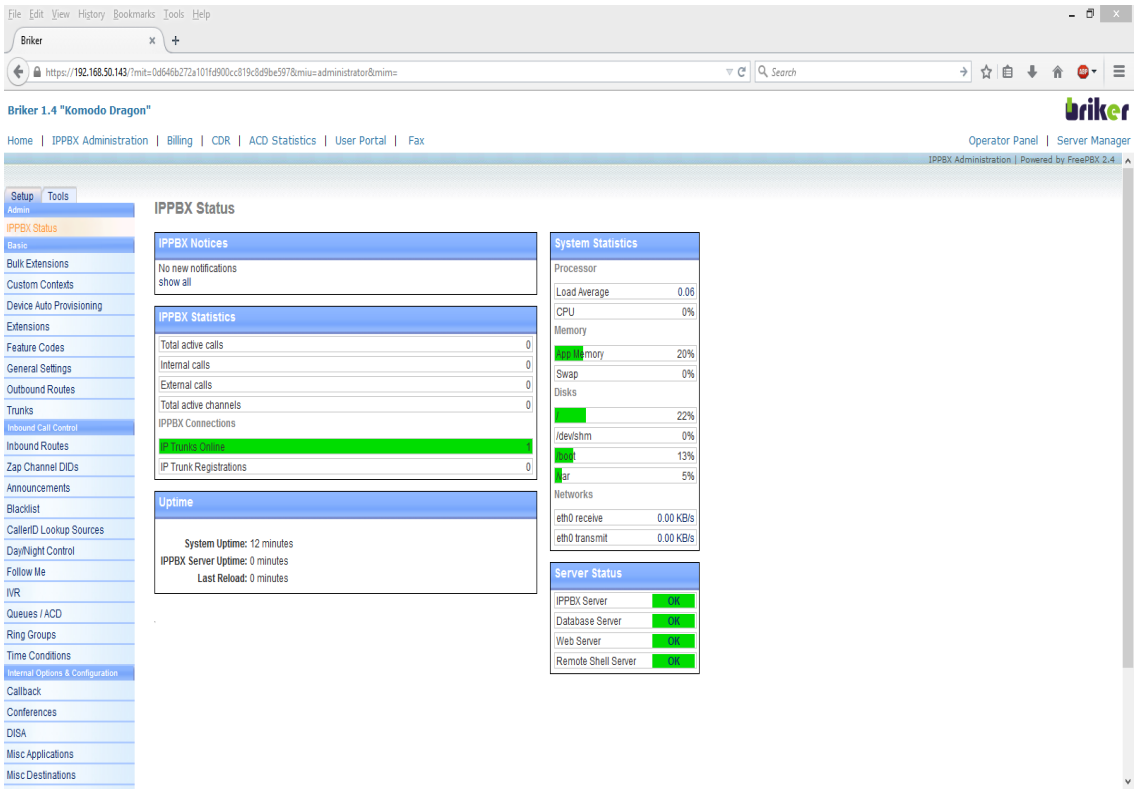
Sumber : Dokumen Kemendikbud

Gambar 2.23 Tampilan Konfigurasi 7 Alamat IP Briker



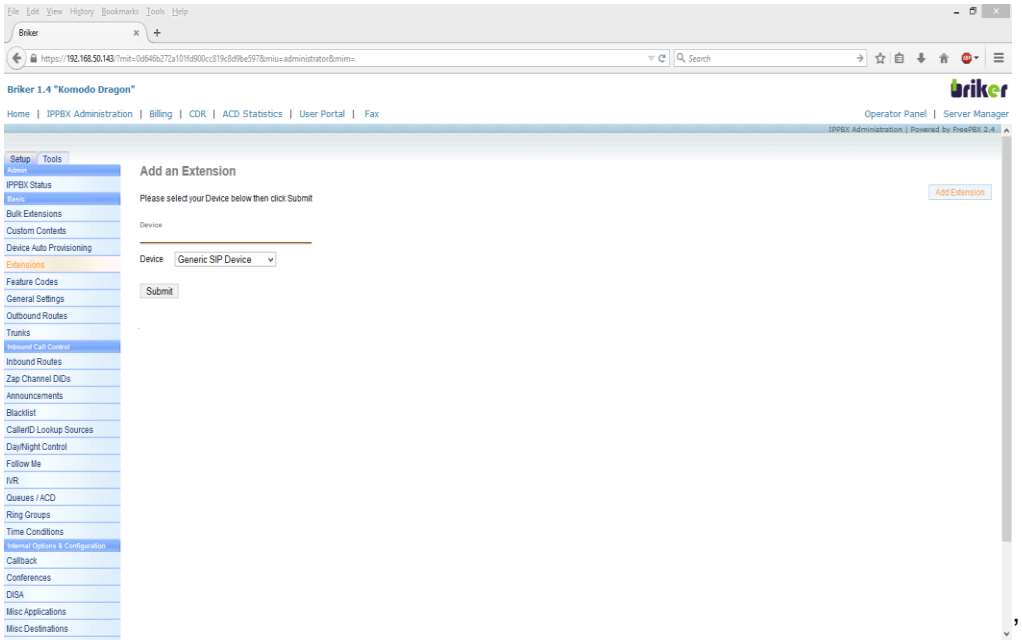
Sumber : Dokumen Kemendikbud

Gambar 2.24 Tampilan Login Halaman Operator



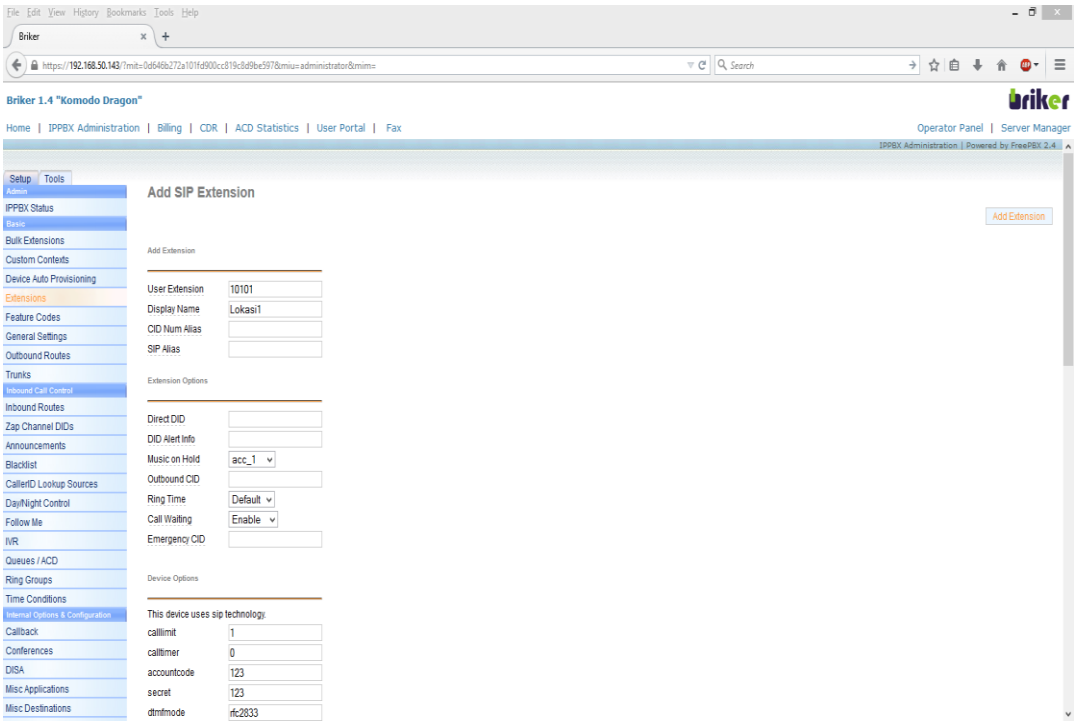
Sumber : Dokumen Kemendikbud

Gambar 2.25 Tampilan IPPBX Administration



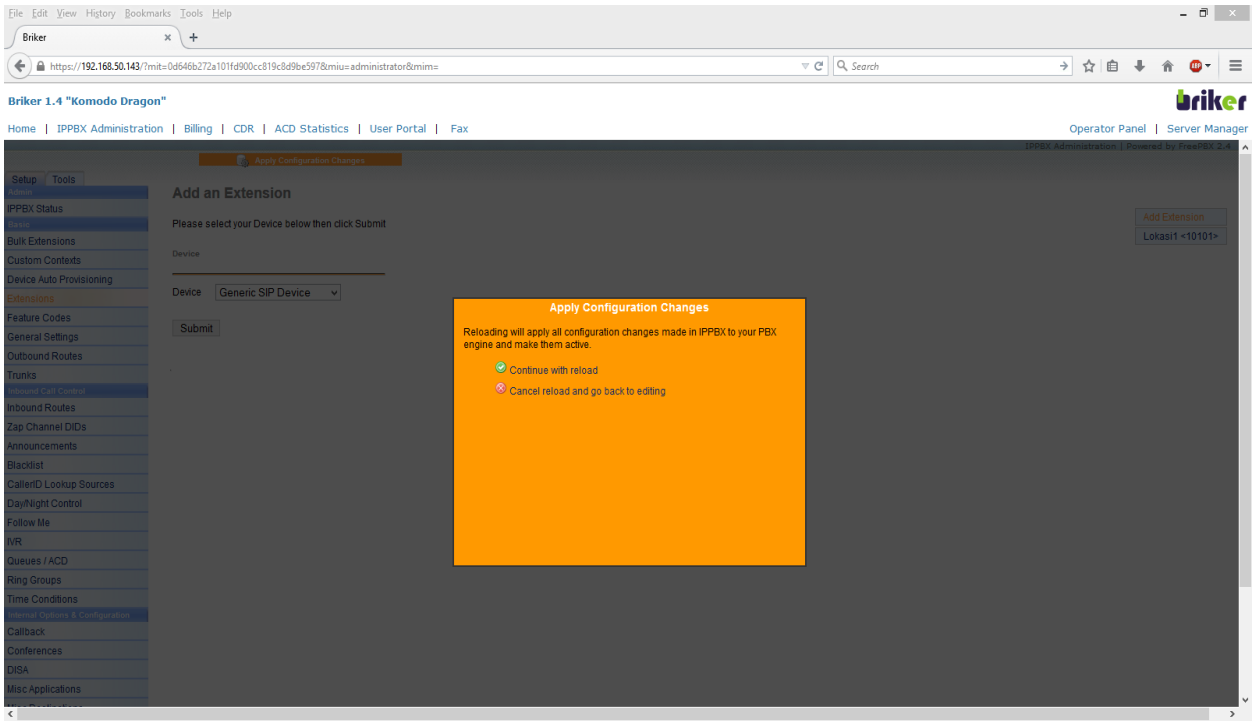
Sumber : Dokumen Kemendikbud

Gambar 2.26 Tampilan Add Extension



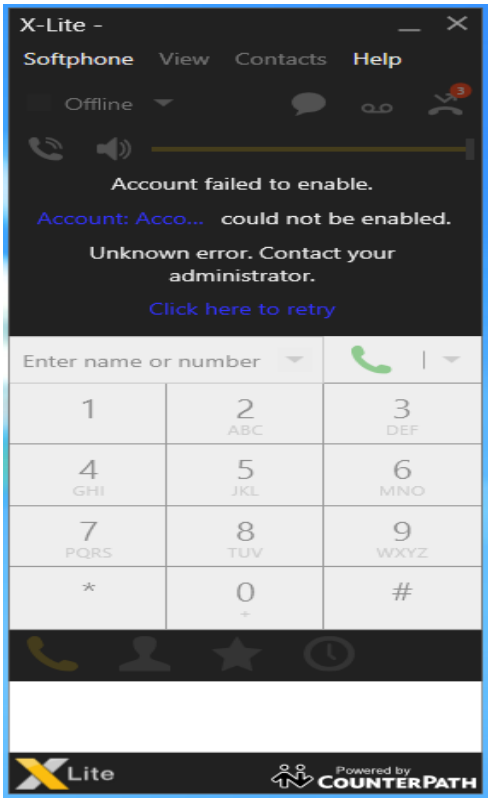
Sumber : Dokumen Kemendikbud

Gambar 2.27 Tampilan SIP Extension



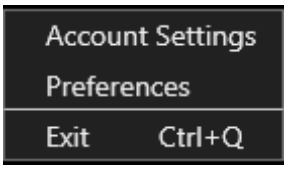
Sumber : Dokumen Kemendikbud

Gambar 2.28 Tampilan Apply Configuration Change



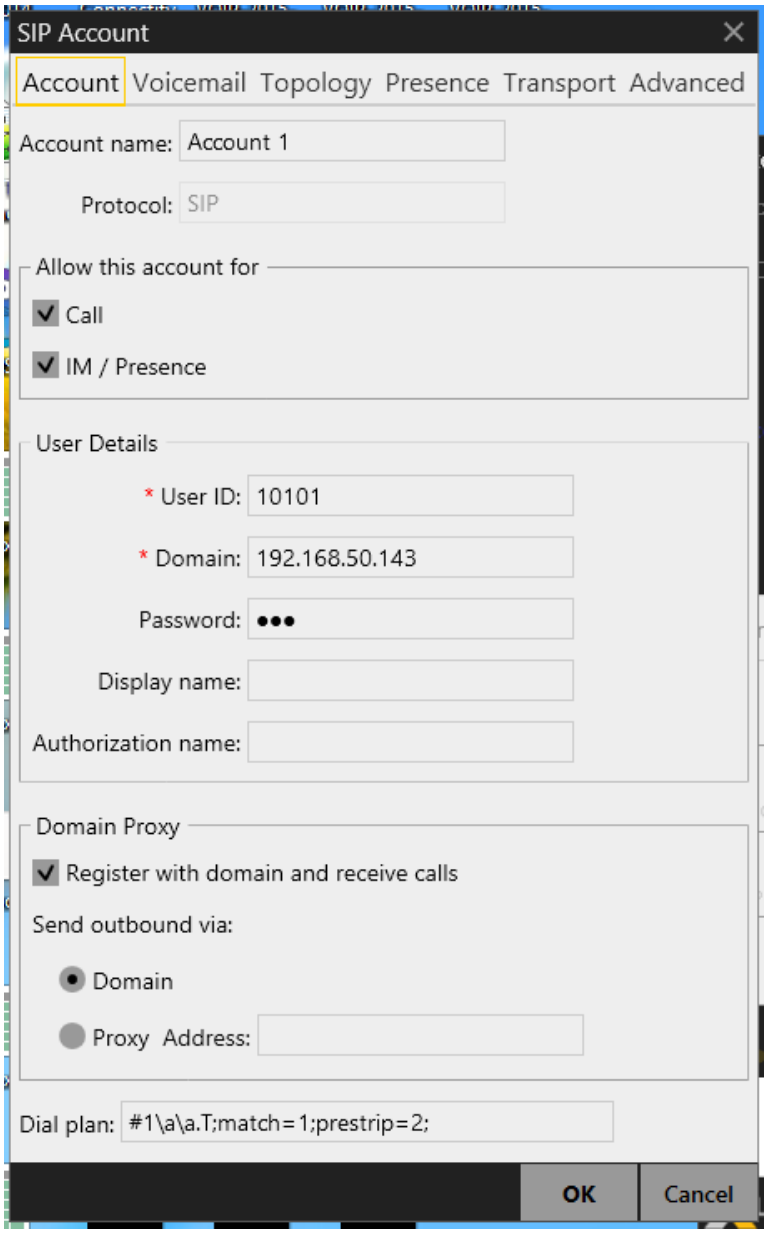
Sumber : Dokumen Kemendikbud

Gambar 2.29 Tampilan X-Lite Softphone



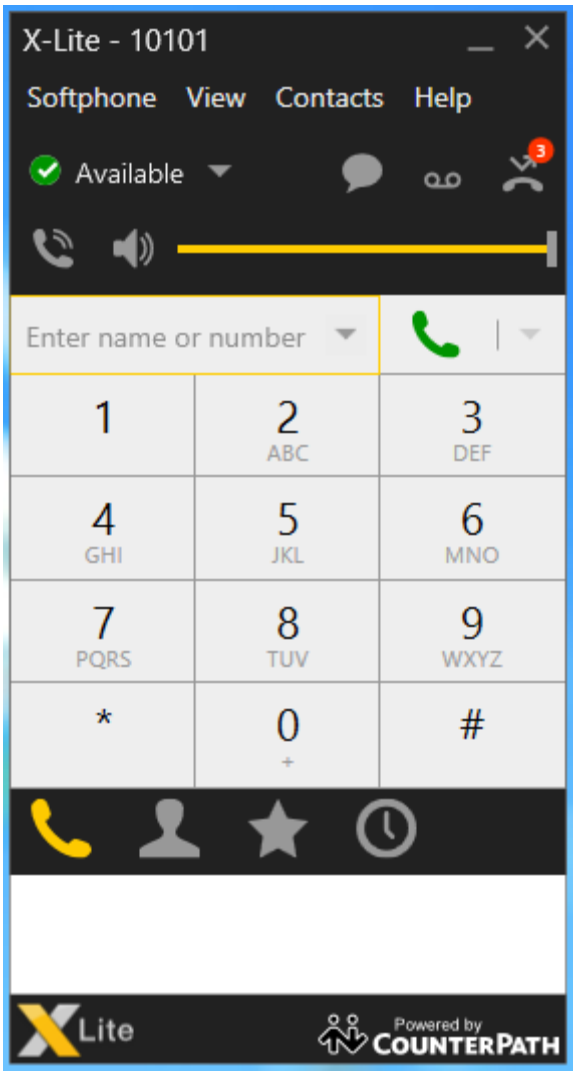
Sumber : Dokumen Kemendikbud

Gambar 2.30 Tampilan Setting X-Lite



Sumber : Dokumen Kemendikbud

Gambar 2.31 Tampilan Setting Akun Briker di X-Lite



Sumber : Dokumen Kemendikbud

Gambar 2.32Tampilan IPPBX Softphone Diap Digunakan

2.1.2.2 Menanya

Dengan mengamati gambar yang ada pada bagian observasi, menurut anda:

1) Bagimanakah konfigurasi ekstensi dan dial plan server Softswitch?
2) Dapatkah anda menjelaskan hasil konfigurasi ekstensi dan dial plan server Softswitch menurut pemahaman anda?

2.1.2.3 Mencoba/Mengumpulkan Informasi

Softswitch merupakan teknologi baru dalam switching yang didalamnya menyangkut istilah Call Control dan Call Prosesing. Definsi softswitch adalah suatu sisitem komunikasi NGN yang menggunakan standar terbuka untuk membuat jaringan terintegrasi dengan memadukan kemampuan layanan yang intelegence dalam menangani Traffic Voice data dan multimedia secara lebih efisien dan dengan potensi nilai tambah layanan yang jauh lebih besar dari pada PSTN. Softswitch lebih dikenal sebagai IP-PBX.

Data Account

- Extension

Merupakan data account yang akan digunakan oleh extension agar terhubung dengan IP PBX ini. Extension disini adalah sebuah nama atau nomor yang merepresentasikan user dari IP PBX ini.

- Trunk

Merupakan data account yang akan digunakan IP PBX untuk menghubungi trunk. Trunk adalah sebuah nama atau nomor yang merepresentasikan server lain atau IP PBX lain yang akan dihubungi oleh IP PBX ini.

- Dial Plan

Merupakan aturan dial yang akan dimanfaatkan oleh extension untuk menghubungi sesama extension atau trunk dan sebaliknya.

Perangkat dalam sofswitch yaitu :

- Media gateway controller (MGC) yang sering disebut dengan perangkat call agent
- Aplication/fitur server
- Media server

Selain memiliki berbagai perangkat, softswitch juga memiliki kapsitas yaitu harus mampu trafik panggilan minimal 4 juta BHC dan dapat pula ditambah kapasitasnya sesuai kebutuhan. Kapasitas sistem ini juga harus didesain secara modular.

Perangkat dalam softswitch harus mampu menjamin kualitas layanan dengan batas batas nilai seperti pada dibawah ini :

- one way delay
- delay fariation
- information loss
- MOS (mean opition socore)
- echo cancelation
- post dial delay

Fitur fitur softswitch adalah :

- abreviated dialing
- call forwading
- call waiting
- cancel call waiting
- calling line indetification presentasi (ccip)
- clip on call waiting
- conterence call
- confrex

Server dari ip-pbx yaitu :

- Elastix

Elastix merupakan sumber Bersatu terbuka Communications Server perangkat lunak yang menyatukan IP PBX, email, IM, fax dan fungsionalitas kolaborasi. Memiliki antar muka web dan mencakup kemampuan seperti software Call Center dengan panggilan prediktif.

Fungsi Elastix didasarkan pada proyek open source termasuk Asterisk, HylaFax, Openfire dan Postfix. Mereka menawarkan paket PBX, faks, instant messaging dan

fungsi email, masing-masing. Dukungan untuk hardware telepon

Elastix memiliki dukungan yang baik untuk hardware telepon [1]. Ini mencakup driver untuk produsen besar seperti Dinstar, OpenVox, Digium, Sangoma, Peralatan Rhino, Xorcom, dan Yeastar. Yang sebagian besar driver didukung melalui proyek zaptel atau versi yang dimodifikasi dari itu. Driver lain yang didukung oleh proyek mIDSN dan proyek lainnya.

Elastix juga mendukung merek berkat telepon ke protokol SIP dan IAX bahwa Asterisk mengimplementasikan lainnya. Protokol ini didasarkan pada standar yang tersedia publik. Untuk alasan ini setiap produsen dapat membangun sebuah produk yang mendukung mereka. Beberapa produsen yang didukung adalah Polycom, ATCOM, Aastra, Linksys, SNOM, dan Cisco.

Sebuah hardware Elastix kompatibilitas list, dikelola oleh masyarakat dapat ditemukan di sini Panggil modul center

Elastix adalah distribusi pertama yang termasuk modul call center dengan dialer prediktif, dirilis seluruhnya sebagai perangkat lunak bebas. Modul ini dapat diinstal dari antarmuka berbasis web yang sama Elastix melalui loader modul. Modul call center dapat menangani kampanye yang masuk dan keluar. Pada Maret 2009 fungsi ini berada dalam tahap awal pengembangan, dan belum sepenuhnya fungsional. Sejarah proyek.

- Briker adalah IPPBX berbentuk software atau operasi linux yang dikhususkan untuk melayani Voip. Komputer akan berubah menjadi mesin PBX (Private Branch Exchange) dengan kemampuan telekomunikasi melalui jaringan atau IP.

Tahap-tahap konfigurasi pada sistem operasi Briker supaya dapat bekerja dengan baik, meliputi Konfigurasi Administration, Konfigurasi Trunk, Konfigurasi Outbound Routes, Konfigurasi Video Call, Konfigurasi SIP Account dan Management User.

2.1.1.1.1 Instalasi Server

Konfigurasi BIOS agar melakukan booting pertama kali dari CDROM, kemudian CD Briker IPPBX dimasukan ke CDROM Install Briker IPPBX ke harddisk, ketik install lalu tekan enter. Setelah proses instalasi selesai, sistem akan membuat password default untuk console login dan web login, serta mengkonfigurasi alamat IP default.

Default console login (SSH port 22):

- Username : support
- Password : Briker

Default web login (HTTP port 80):

- Username : administrator
- Password : Briker

Alamat IP default:

- IP address : 192.168.2.2

- Subnet mask : 255.255.255.0

Namun pada buku ini, untuk IP address Briker menggunakan konfigurasi IP manual sehingga alamat IP menjadi 192.168.50.143.

Pada proses instlasi Briker otomatis memeriksa hardware yang terpasang dengan pertama kali memeriksa CDROM.

Briker otomatis memeriksa perangkat keras jaringan, lalu mengkonfigurasi alamat IP secara otomatis. Briker otomatis menghapus (format) hardisk dan menggunakan semua isi hardisk. Terakhir, Briker akan install GRUB boot loader.

Instalasi sistem selesai, CD Briker akan otomatis keluar dari CDROM dan komputer akan restart. Setelah instalasi selesai, dapat memulai melakukan konfigurasi dari console seperti mengganti alamat IP, konfigurasi tanggal dan jam dan lainnya.

Alamat IP default Briker adalah 192.168.2.2, pada banyak kondisi sudah dipastikan perlu merubahnya, misal untuk menyesuaikan dengan topologi jaringan dan pengalamatan IP yang ada. Untuk mengganti alamat IP dan informasi lainnya berkenaan dengan network address berada pada directory server pada pasisi /etc/network/interfaces.

Konfigurasi Administration (WebBase)

Konfigurasi Administration pada browser dengan cara memanggil alamat IP Briker melalui web browser dengan IP 192.168.50.143 yaitu IP yang didaftarkan pada server, setelah itu akan muncul halaman untuk login. Sebagai username default yaitu administrator dan password default yaitu Briker. Pada menu home ini dapat dilakukan penambahan account sehingga mudah dilakukan Management User dan dapat diberikan hak yang dapat dilakukan user baik sebagai administartor atau sebagai user biasa tetapi tidak dapat membuat SIP acoount, trunk, inbount, outbount, IVR, dan bisa melihat Operator panel.

Konfigurasi pada IPPBX Administration

Pada halaman ini tersedia menu untuk mengatur fitur IPPBX dari Briker, antara lain pengaturan extensions, trunks dan routes. IPPBX Administration dapat diamati pada pada gambar 2.25.

IPPBX Status menampilkan System Statistics yang menunjukkan persentasi Load Average, CPU, Memory dan Swap yang terpakai, penggunaan ruang harddisk dan kecepatan Receive dan Transmit Ethernet. Terdapat pula IPPBX Statistics yang menampilkan Total Active Calls, Internal Calls, External Calls, Total Active Channels, serta informasi Uptime Briker.

Karena proses pengambilan datanya realtime dan menggunakan CPU resource yang tidak sedikit maka tidak disarankan untuk terus menerus membuka halaman ini. Konfigurasi utama fitur-fitur IPPBX dapat ditemui pada menu di sisi kiri. Ada 3 (tiga) fitur menu yang akan dikonfigurasikan pada IPPBX Administration, yaitu sebagai berikut.

1. Menu Extensions

Fitur ini berkaitan dengan account pada IPPBX. Penambahan, penghapusan dan pergantian data account dapat dilakukan pada menu ini. Setiap account yang ditambahkan berlaku sebagai extension IPPBX. Bisa dikatakan bahwa extension adalah user yang akan menggunakan layanan Briker.

Untuk melakukan konfigurasi Extensions pilih Extensions pada menu IPPBX Administration, Add Extensions, lalu pilih protocol SIP yaitu protocol VoIP yang menggunakan port 5060 UDP.

Ada beberapa hal yang wajib harus didaftarkan dalam membuat account VoIP yaitu:

- User Extensions: Nomor extension, misal 10101. Biasanya hanya numeric.
- Display Name: Nama yang akan digunakan sebagai Caller ID ketika melakukan panggilan
- Secret: Password yang digunakan user untuk proses otentikasi saat registrasi extension pada User Agent

2. Konfigurasi Trunk

Trunking dalam jaringan telekomunikasi berarti menghubungkan satu sentral dengan sentral telepon lainnya. Pada Briker hal tersebut tidak jauh berbeda, selain itu Briker dapat saling berhubungan secara IP Trunking dengan protokol SIP atau secara konvensional melalui jalur analog dan digital dengan bantuan perangkat keras teleponi seperti Digium seri TDM untuk analog dan seri TE untuk digital atau dengan bantuan Internet Telephony Gateway (ITG). Untuk melakukan konfigurasi pada menu menu IPPBX Administration, pilih menu Trunks lalu pilih Add SIP Trunk.

3. Konfigurasi Outbound Routes

Outbound routes digunakan untuk mengatur tujuan panggilan, yang keluar melalui trunk. Outbound routes inilah yang mendefinisikan untuk semua panggilan keluar, contoh Briker dihubungkan ke VoIP server yang lain, maka untuk panggilan ke VoIP rakyat, diatur dial rules-nya misal 9. Yang berarti ketika akan melakukan panggilan ke VoIP rakyat harus menggunakan prefix 9 diikuti nomor tujuan. Berikut contoh konfigurasinya.

Dalam menu IPPBX Administration pilih menu Outbound Routes, lalu pilih Add Route.

Ada beberapa hal yang wajib harus didaftarkan dalam konfigurasi Outbound Routes, yaitu:

- Route Name : Merupakan nama route
- Dial Patterns : Kode awal untuk menghubungi ke server lain
- Trunk Sequence : Trunk yang digunakan, lihat pada bagian Trunks

Konfigurasi Video Call

Agar antar client dapat melakukan video call, maka perlu penambahan konfigurasi pada server dibagian #/etc/asterisk/sip.conf, hal ini dapat dilakukan dengan mengetikkan perintah pada konsole Briker sebagai berikut #vi /etc/asterisk/sip.conf.

Konfigurasi pada sisi Client

Konfigurasi pada sisi client meliputi penambah user account dan instalasi softphone. Jenis sistem operasi yang digunakan oleh client yaitu system operasi Windows dimana system operasi Windows menggunakan softphone x-lite atau zoiper. Proses instalasi pada client windows dan pada handphone relatif mudah karena tersedianya source software yang telah siap untuk di install.

Beberapa cara konfigurasi softphone pada client VoIP sebagai berikut:

1. Konfigurasi Aplikasi X-lite pada OS Windows.

Konfigurasi client pada aplikasi X-lite dilakukan pada menu softphone lalu pada tab SIP Account. Pada pengaturan ini yang diisi yaitu account name, user ID, domain, password dan desplay name.

2. Konfigurasi pada Handphone

Konfigurasi VoIP client pada handphone pada dasarnya sama seperti konfigurasi pada VoIP client untuk komputer, konfigurasi ini juga meliputi pengisian account name, user ID, domain dan password yang sebelumnya sudah didaftarkan pada server VoIP. Akan tetapi tidak semua softphone dapat berjalan pada setiap handphone, karena tidak semua handphone dapat menggunakan fasilitas VoIP ini.

2.1.2.4 Mengasosiasi/Menalar

Konfigurasi yang dilakukan, maka beberapa hasil analisis dapat disampaikan yaitu:

1) Softswitch adalah suatu sistem komunikasi NGN yang menggunakan standar terbuka untuk membuat jaringan terintegrasi dengan memadukan kemampuan layanan yang intelegence dalam menangani Traffic Voice data dan multimedia secara lebih efisien dan dengan potensi nilai tambah layanan yang jauh lebih besar dari pada PSTN.
2) Softswitch lebih dikenal sebagai IP-PBX
3) Extension merupakan data account yang akan digunakan oleh extension agar terhubung dengan IP PBX ini.
4) Extension juga adalah sebuah nama atau nomor yang merepresentasikan user dari IP PBX ini.
5) Trunk merupakan data account yang akan digunakan IP PBX untuk menghubungi trunk.
6) Trunk adalah sebuah nama atau nomor yang merepresentasikan server lain atau IP PBX lain yang akan dihubungi oleh IP PBX ini.
7) Dial Plan merupakan aturan dial yang akan dimanfaatkan oleh extension untuk menghubungi sesama extension atau trunk dan sebaliknya.
8) Server dari ip-pbx yaitu :
    a. Elastix merupakan sumber Bersatu terbuka Communications Server perangkat lunak yang menyatukan IP PBX, email, IM, fax dan fungsionalitas kolaborasi. Sebuah hardware Elastix kompatibilitas list,

dikelola oleh masyarakat dapat ditemukan di sini Panggil modul center.

b. Briker adalah IPPBX berbentuk software atau operasi linux yang dikhususkan untuk melayani Voip. Komputer akan berubah menjadi mesin PBX (Private Branch Exchange) dengan kemampuan telekomunikasi melalui jaringan atau IP.

9) Ada 3 (tiga) fitur menu yang akan dikonfigurasikan pada IPPBX Administration, yaitu menu Extensions, konfigurasi Trunk dan konfigurasi Outbound Routes
10) Fitur yang berkaitan dengan account pada IPPBX adalah menu Exstensions
11) Penambahan, penghapusan dan pergantian data account dapat dilakukan pada menu Exstensions
12) Setiap account yang ditambahkan berlaku sebagai extension IPPBX.
13) Extension juga adalah user yang akan menggunakan layanan Briker.
14) Untuk melakukan konfigurasi Extensions pilih Extensions pada menu IPPBX Administration, Add Extensions, lalu pilih protocol SIP yaitu protocol VoIP yang menggunakan port 5060 UDP.
15) Ada beberapa hal yang wajib harus didaftarkan dalam membuat account VoIP yaitu:
    - User Extensions: Nomor extension, misal 10101. Biasanya hanya numeric.
    - Display Name: Nama yang akan digunakan sebagai Caller ID ketika melakukan panggilan
    - Secret: Password yang digunakan user untuk proses otentikasi saat registrasi extension pada User Agent
16) Trunking dalam jaringan telekomunikasi berarti menghubungkan satu sentral dengan sentral telepon lainnya.
17) Untuk melakukan konfigurasi pada menu menu IPPBX Administration, pilih menu Trunks lalu pilih Add SIP Trunk.
18) Outbound routes digunakan untuk mengatur tujuan panggilan, yang keluar melalui trunk.
19) Outbound routes inilah yang mendefinisikan untuk semua panggilan keluar, contoh Briker dihubungkan ke VoIP server yang lain, maka untuk panggilan ke VoIP rakyat, diatur dial rules-nya
20) Untuk melakukan konfigurasi pada menu IPPBX Administration pilih menu Outbound Routes, lalu pilih Add Route.
21) Ada beberapa hal yang wajib harus didaftarkan dalam konfigurasi Outbound Routes, yaitu:
    - Route Name : Merupakan nama route

- Dial Patterns : Kode awal untuk menghubungi ke server lain
- Trunk Sequence : Trunk yang digunakan, lihat pada bagian Trunks

2.1.3 Rangkuman

Dari pembahasan dan konfigurasi yang dilakukan maka dapat disimpulkan bahwa Softswitch merupakan teknologi baru dalam switching yang didalamnya menyangkut istilah Call Control dan Call Prosesing. Softswitch lebih dikenal sebagai IP-PBX. Perangkat dalam softswitch harus mampu menjamin kualitas layanan dengan batas batas nilai seperti pada dibawah ini :

- one way delay
- delay fariation
- information loss
- MOS (mean opition socore)
- echo cancelation
- post dial delay

Fitur fitur softswitch adalah :

- abreviated dialing
- call forwading
- call waiting
- cancel call waiting
- calling line indetification presentasi (ccip)
- clip on call waiting
- conterence call
- confrex

Briker adalah jenis softswitch yang dibahas pada buku ini. Briker merupakan IPPBX yang berbentuk software atau sistem operasi Linux yang dikhususkan untuk layanan VoIP. Tahap-tahap konfigurasi pada sistem operasi Briker supaya dapat bekerja dengan baik, meliputi Konfigurasi Administration, Konfigurasi Trunk, Konfigurasi Outbound Routes, Konfigurasi Video Call, Konfigurasi SIP Account dan Management User.

2.1.4 Tugas

Tugas

Lakukan proses pengamatan langkah-langkah konfigurasi ekstensi dan dial plan server softswitch serta menyajikan hasil konfigurasi esktensi dan dial plan server softswitch.

Langkah Kerja

1. Buatlah kelompok dengan anggota 3 – 4 orang.
2. Uraikan pengamatan kelompok tentang konfigurasi ekstensi server softswitch!
3. Uraikan pengamatan kelompok tentang konfigurasi dial-plan server softswitch!
4. Uraikan pengamatan kelompok tentang konfigurasi administration (WebBase)!
5. Uraikan pengamatan kelompok tentang konfigurasi administration IPPBX Administration!
6. Buat laporan dan diskusikan dengan teman sekelompok.

Bandingkan dan Simpulkan

Presentasikan hasil kerja kelompok anda di depan kelas dan bandingkan hasil kerja kelompok Anda dengan kelompok lain.

Berdasarkan hasil perbandingan tersebut hal penting apa yang harus dirumuskan secara bersama.

2.1.5 Penilaian Diri

Dalam test ini setiap anda harus membaca dengan cermat dan teliti setiap butir soal dibawah ini. Kemudian berdasarkan uraian materi diatas tulislah jawabannya pada lembar jawaban penilaian diri yang telah disediakan.

1. Tuliskan tahap-tahap konfigurasi pada sistem operasi Briker!
2. Jelaskan yang dimaksud dengan

a. Extension
b. Trunk
c. Dial Plan

3. Berikan penjelasan bagaimanakah keterkaitan antara IP-PBX dengan Sistem Operasi Briker!
4. Tuliskan beberapa hal yang wajib harus didaftarkan dalam membuat account VoIP!

Lembar Kerja penilaian Diri

LJ- 01: Tuliskan tahap-tahap konfigurasi pada sistem operasi Briker!

……
……
……
……
……
……

LJ- 02.a: Jelaskan yang dimaksud dengan Extension!

……
……
……
……
……
……
……
……

LJ- 02.b: Jelaskan yang dimaksud dengan Trunk!

……
……
……
……
……
……
……
……

LJ- 02.c: Jelaskan yang dimaksud dengan Dial Plan!

……
……
……
……
……
……
……

LJ- 03: Berikan penjelasan bagaimanakah keterkaitan antara IP-PBX dengan Sistem Operasi Briker!

……
……
……
……
……
……
……
……

LJ- 04: Tuliskan beberapa hal yang wajib harus didaftarkan dalam membuat account VoIP!

……
……
……
……
……
……
……

BAB III

3.1 Kegiatan Belajar 3: Fungsi Firewall pada Jaringan VoIP

3.1.1 Tujuan Pembelajaran

Setelah mempelajari kegiatan belajar 3, maka diharapkan siswa dapat:

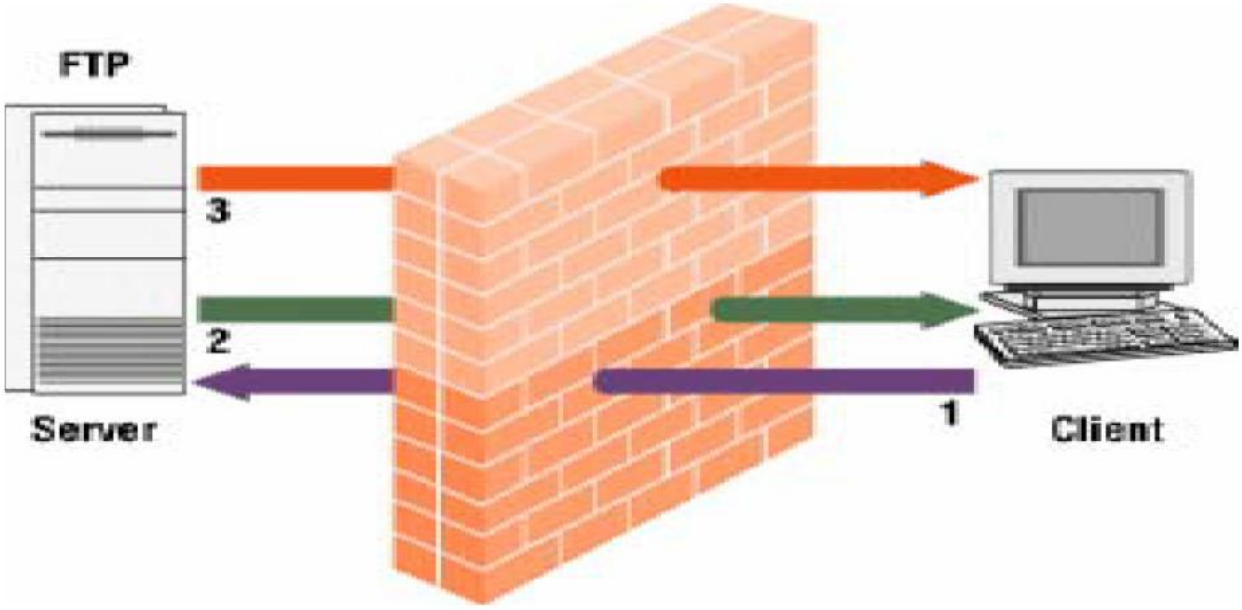
a) Memahami fungsi Firewall pada jaringan VoIP.
b) Menalar fungsi Firewall pada jaringan VoIP.

3.1.2 Aktifitas Belajar Siswa

Pada bagian ini, siswa akan mengamati, menanya, mengumpulkan informasi dan menalar fungsi firewall pada jaringan VoIP.

3.1.2.1 Mengamati/Observasi

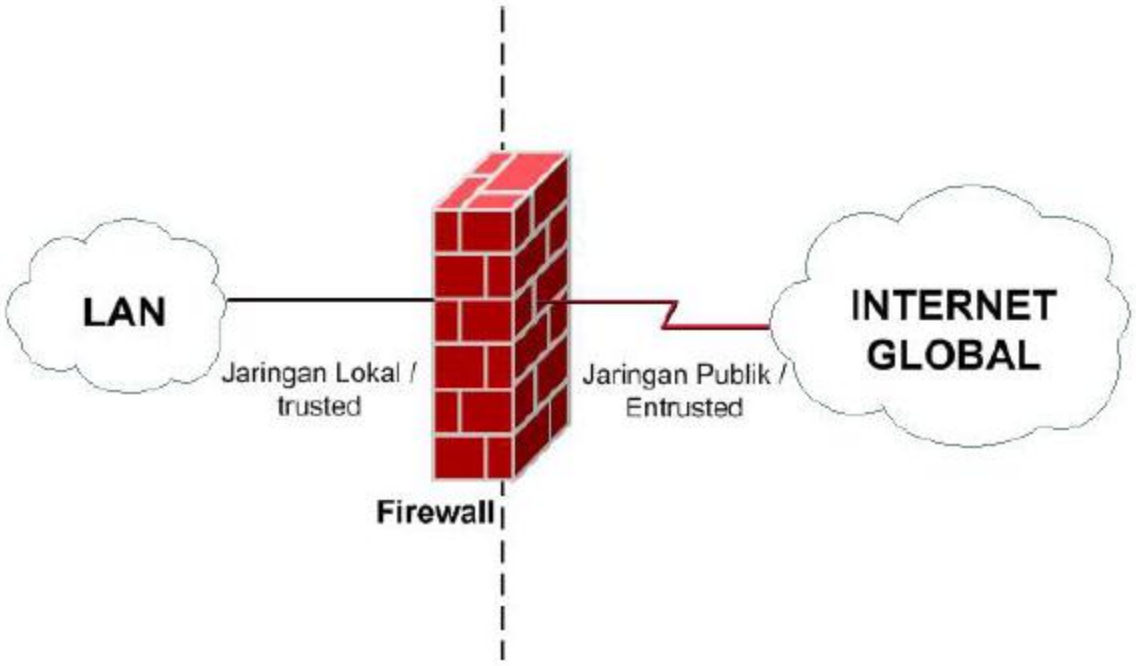
Perhatikan gambar berikut ini:



Sumber : Dokumen Kemendikbud

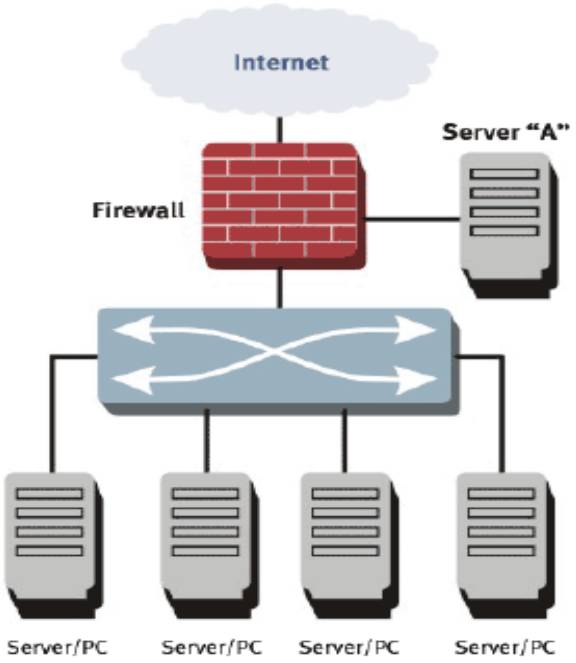
Gambar 3.1 Ilustrasi Penerapan Firewall

FTP (File Transfer Protocol) merupakan sebuah protokol internet yang berjalan di dalam level aplikasi yang merupakan standart untuk proses transfer file antar mesin komputer dalam sebuah framework. Fungsi utama FTP sebagai protokol yang melakukan transfer file dalam suatu network yang mendukung TCP/IP Protokol. Seperti gambar 3.1, FTP digunakan untuk arsitektur jaringan computer Client-Server.



Sumber : Dokumen Kemendikbud

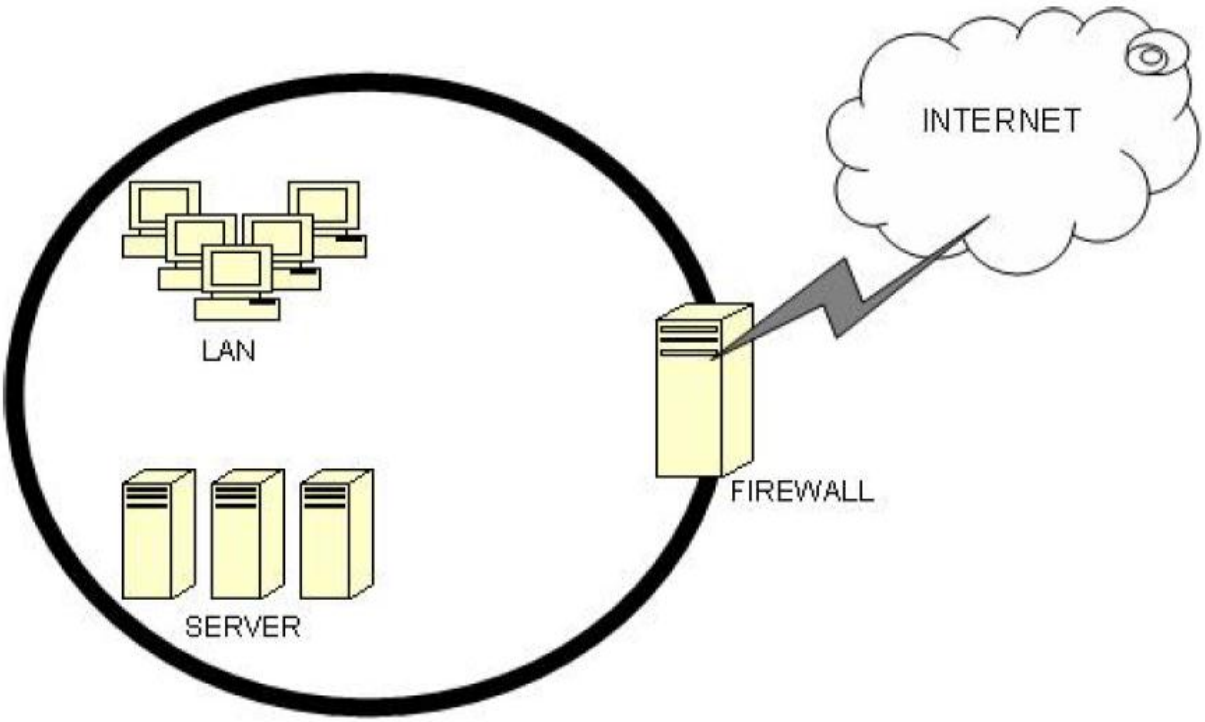
Gambar 3.2 Fundamental Firewall, memisahkan jaringan publik dan lokal.



Sumber : Dokumen Kemendikbud

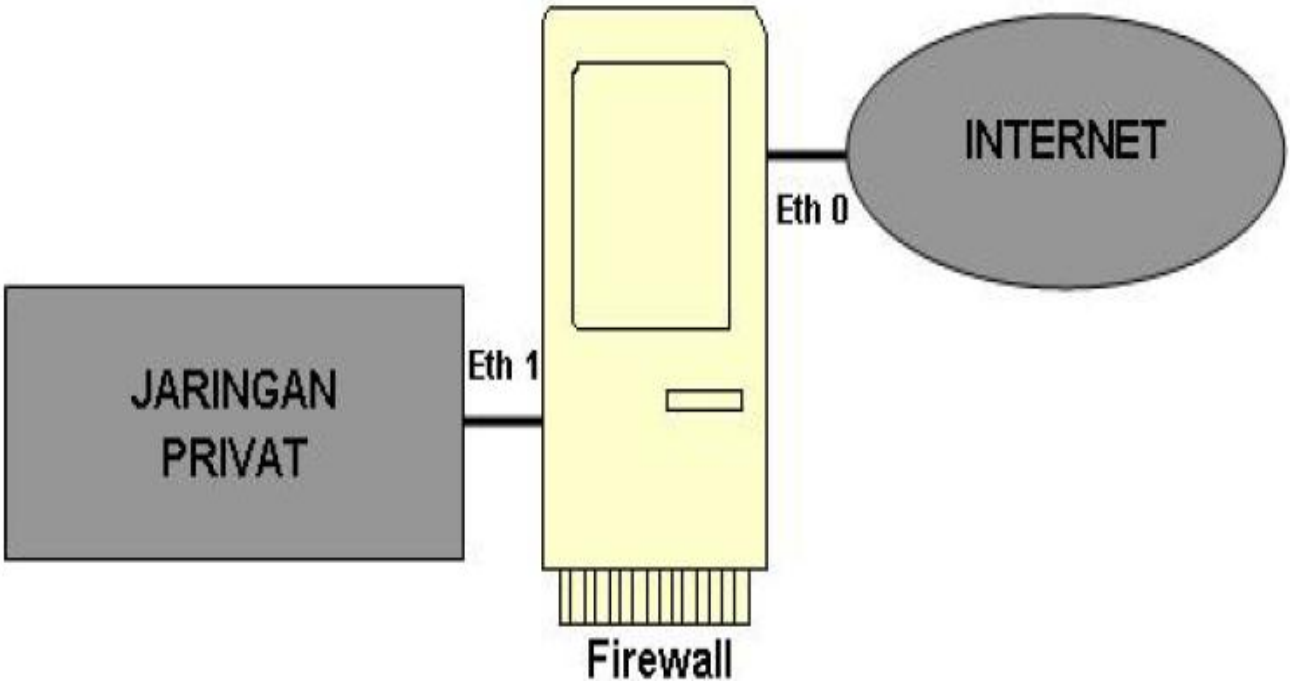
Gambar 3.3 Contoh Firewall dalam Jaringan Komputer

Selanjutnya gambar 3.3 juga mengilustrasikan cara kerja firewall dalam jaringan Komputer.



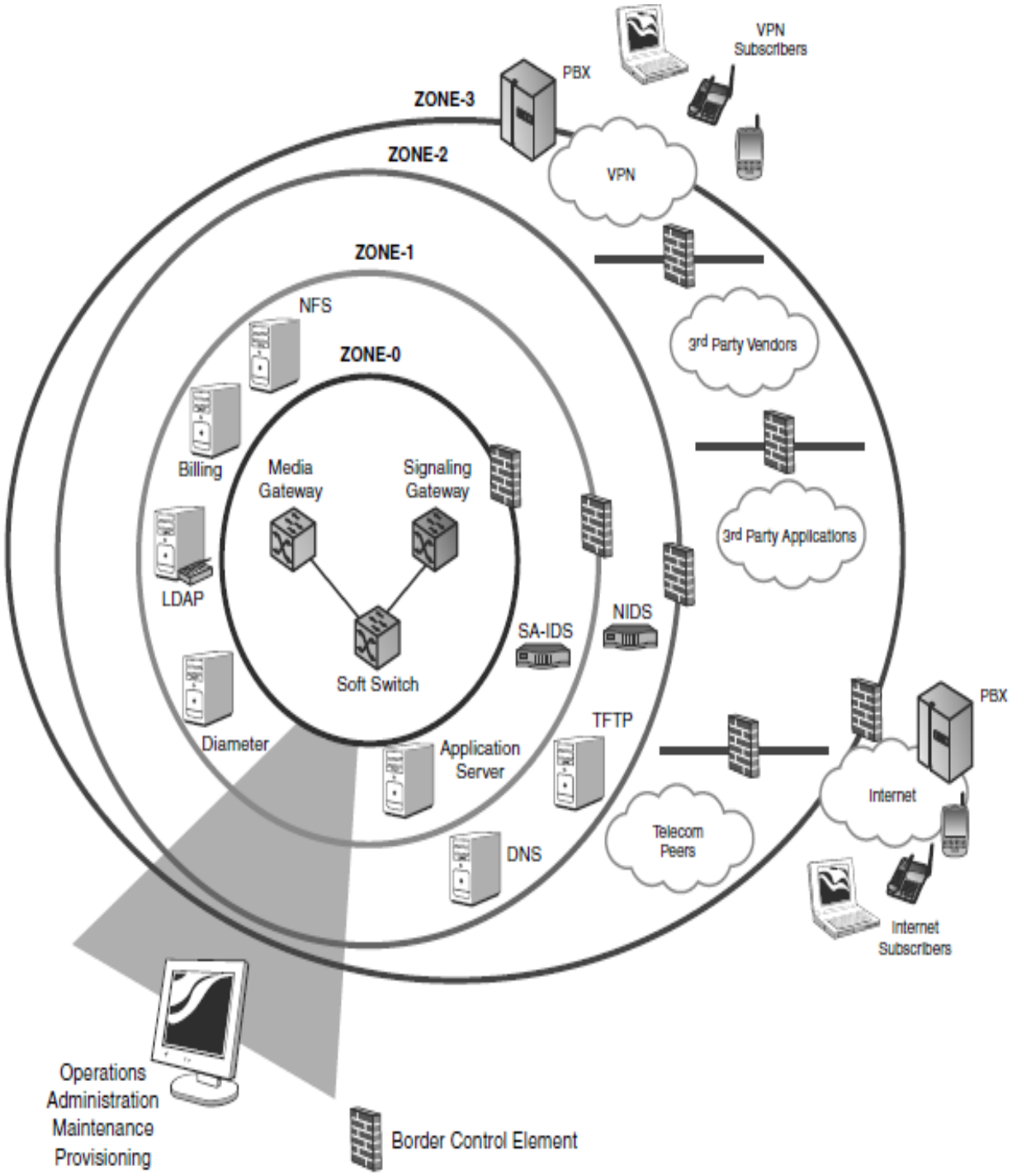
Sumber : Dokumen Kemendikbud

Gambar 3.4 Arsitektur Firewall pada Jaringan Komputer



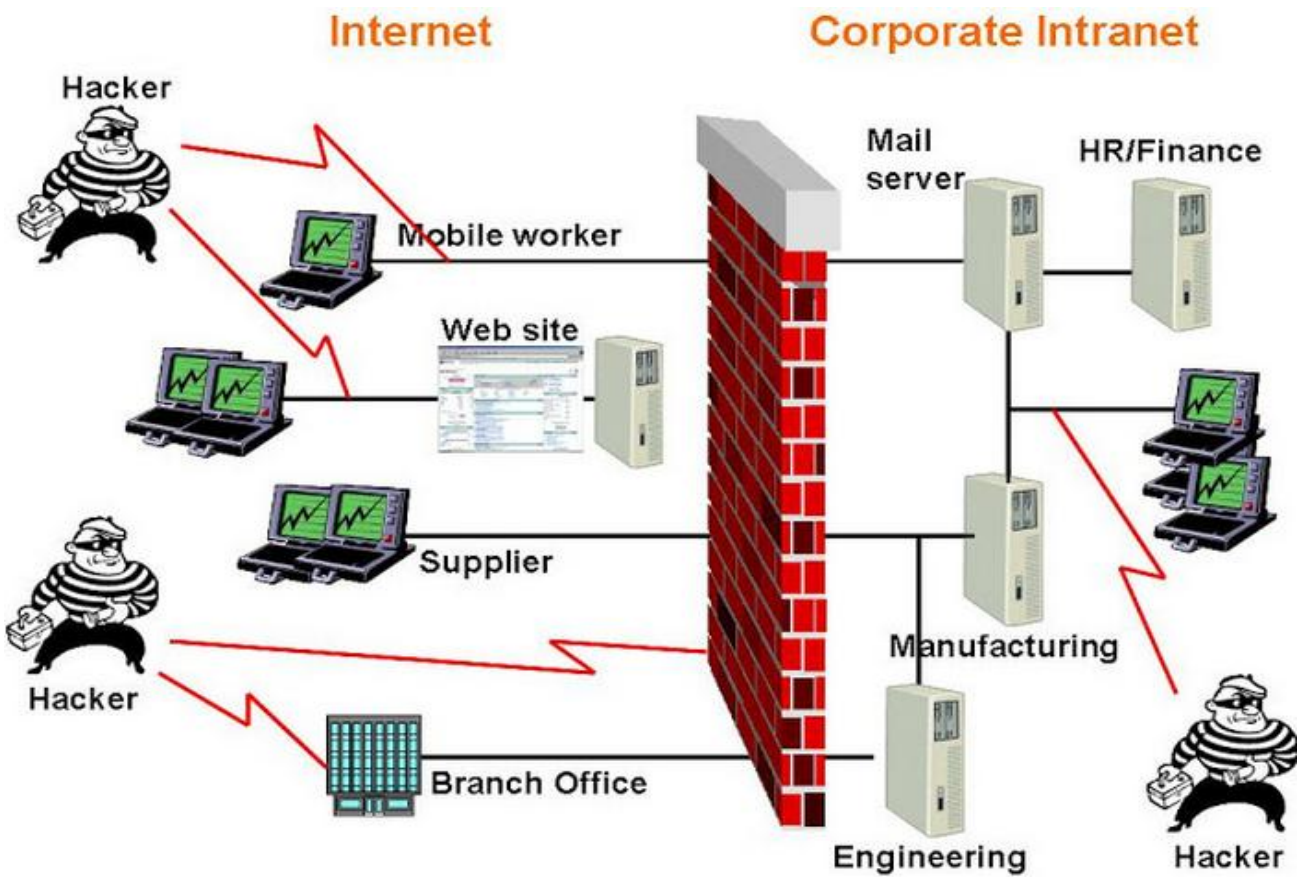
Sumber : Dokumen Kemendikbud

Gambar 3.5 Skema Firewall dalam Jaringan



Sumber : Securing VoIP Network

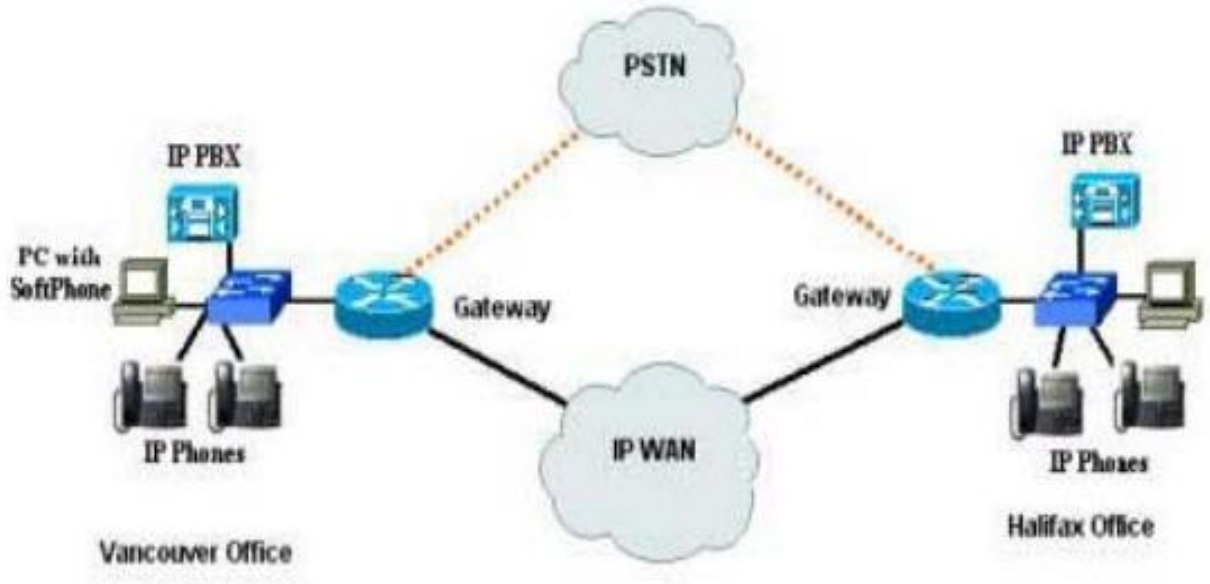
Gambar 3.6 Contoh Layer Sekuritas NGN



Sumber : http://ecgalery.blogspot.com/2010_06_01_archive.html

Ilustrasi Penyerangan Keamanan Jaringan

Berikut perhatikan gambar berikut ini:

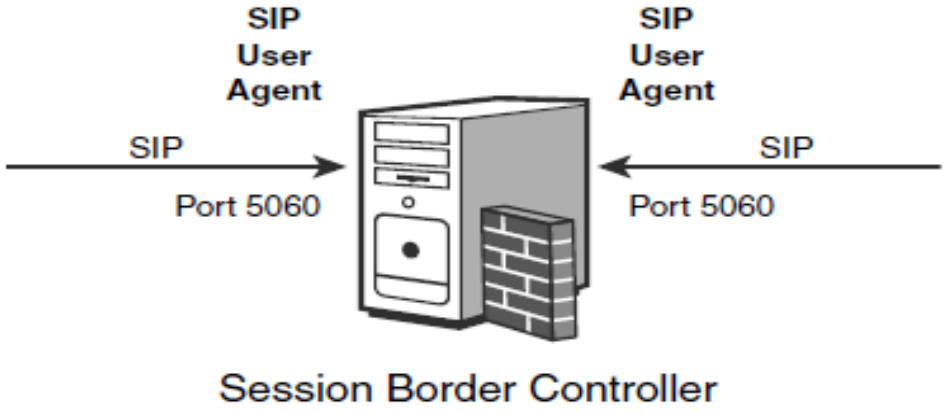


Sumber : http://digilib.tes.telkomuniversity.ac.id

Gambar 3.7 Diagram VoIP

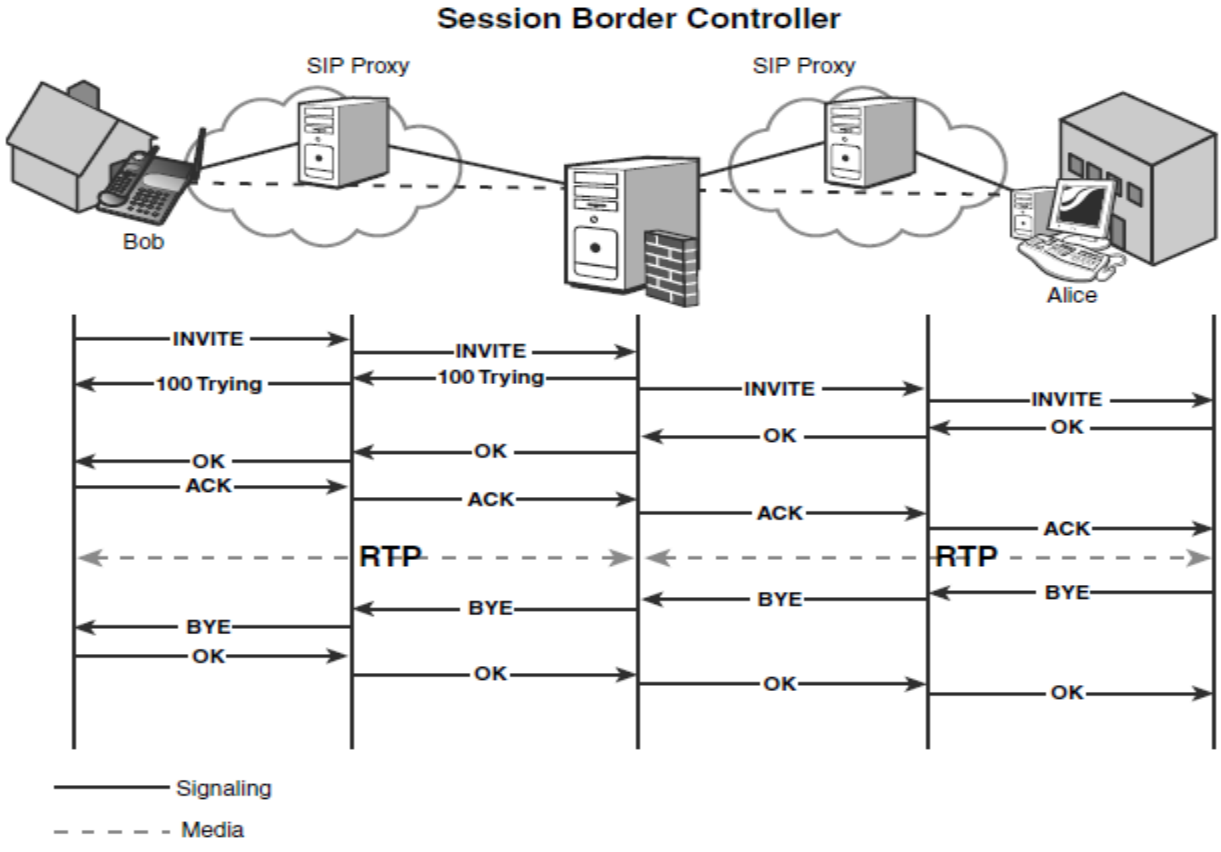
Gambar 3.7 menggambarkan bentuk arsitektur atau diagram VoIP (Voice over Internet Protocol). VoIP dikenal juga dengan IP Telephony. VoIP didefinisikan sebagai

suatu sistem yang menggunakan jaringan internet untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol IP (Tharom, 2002).



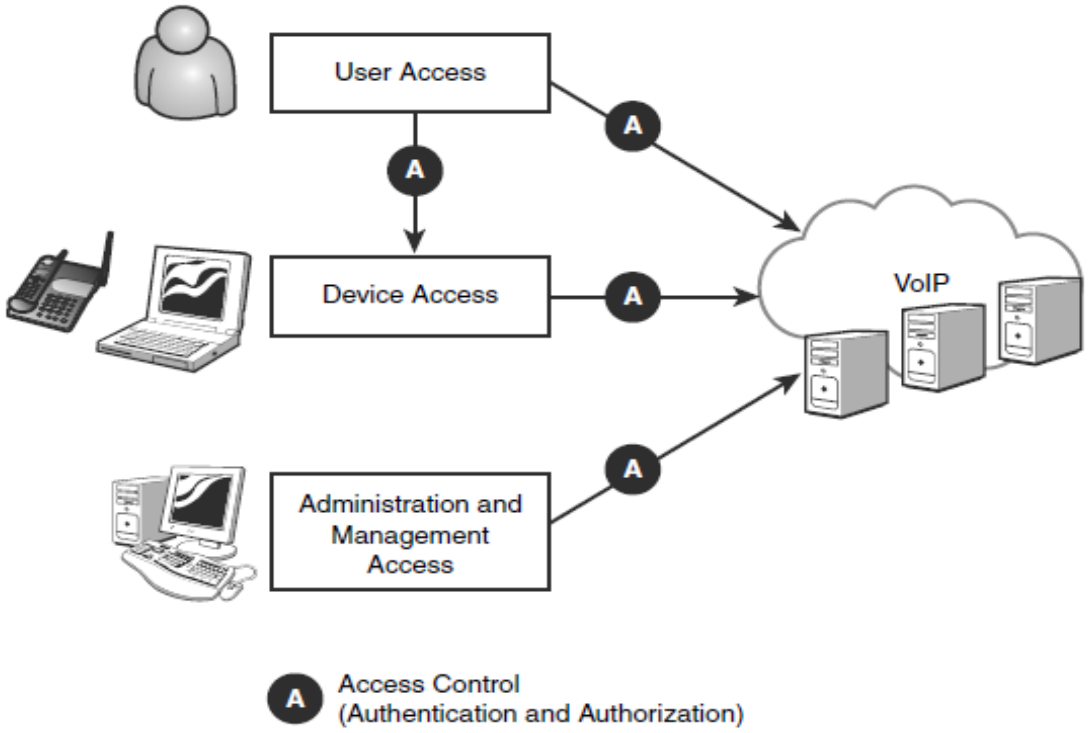
Sumber : Securing VoIP Network

Gambar 3.8 Contoh Sekuritas Keamanan pada VoIP yang disebut SBC (Session Border Control).



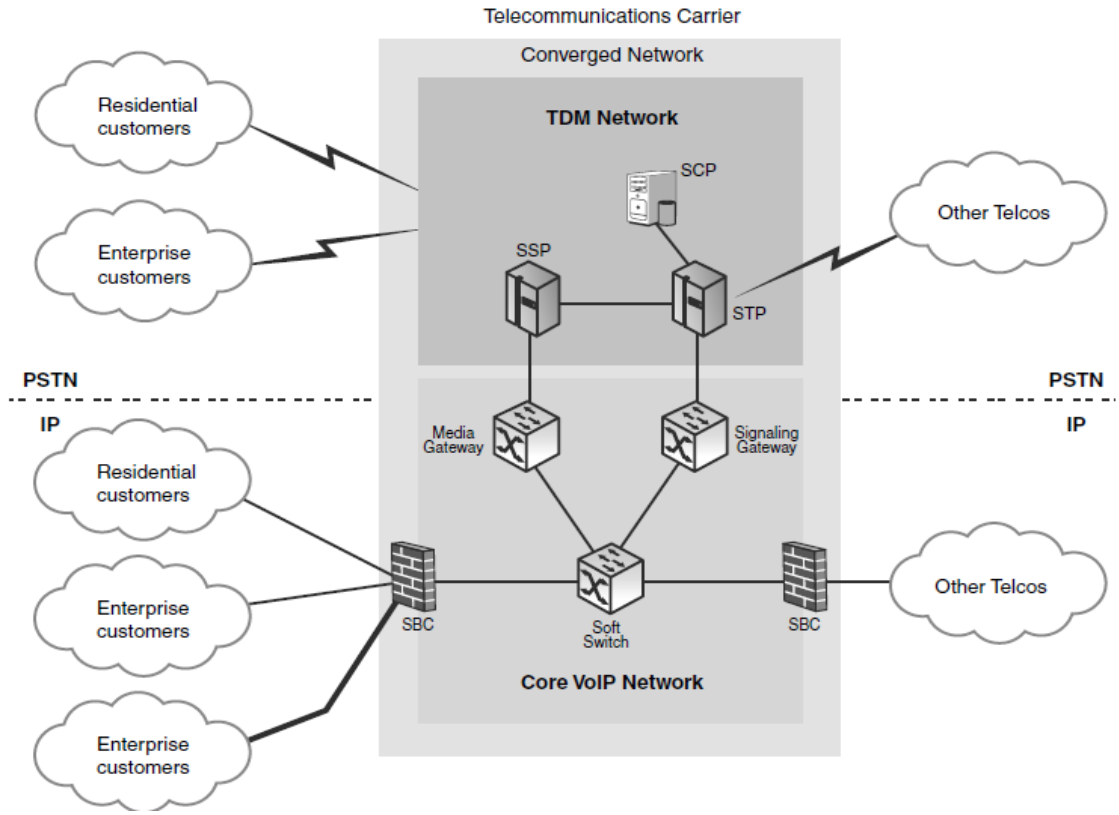
Sumber : Securing VoIP Network

Gambar 3.9 Contoh Aliran Panggilan dengan SBC



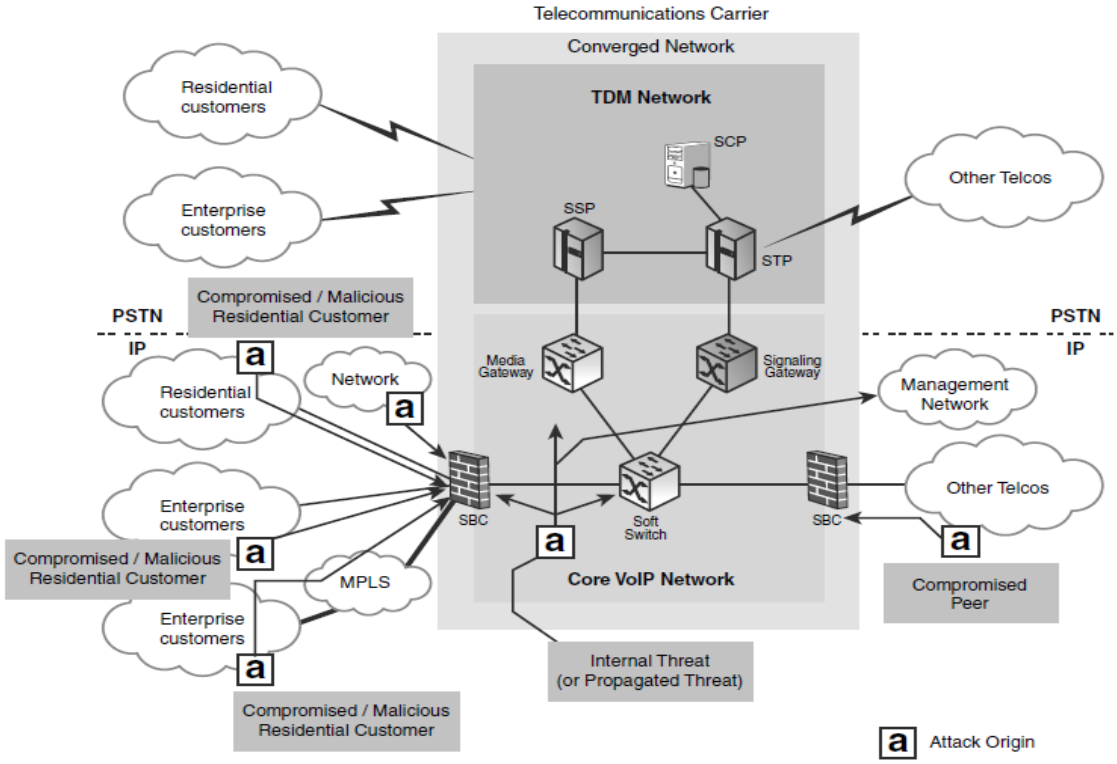
Sumber : Securing VoIP Network

Gambar 3.10 Logika Layer Kontrol Akses pada Jaringan VoIP



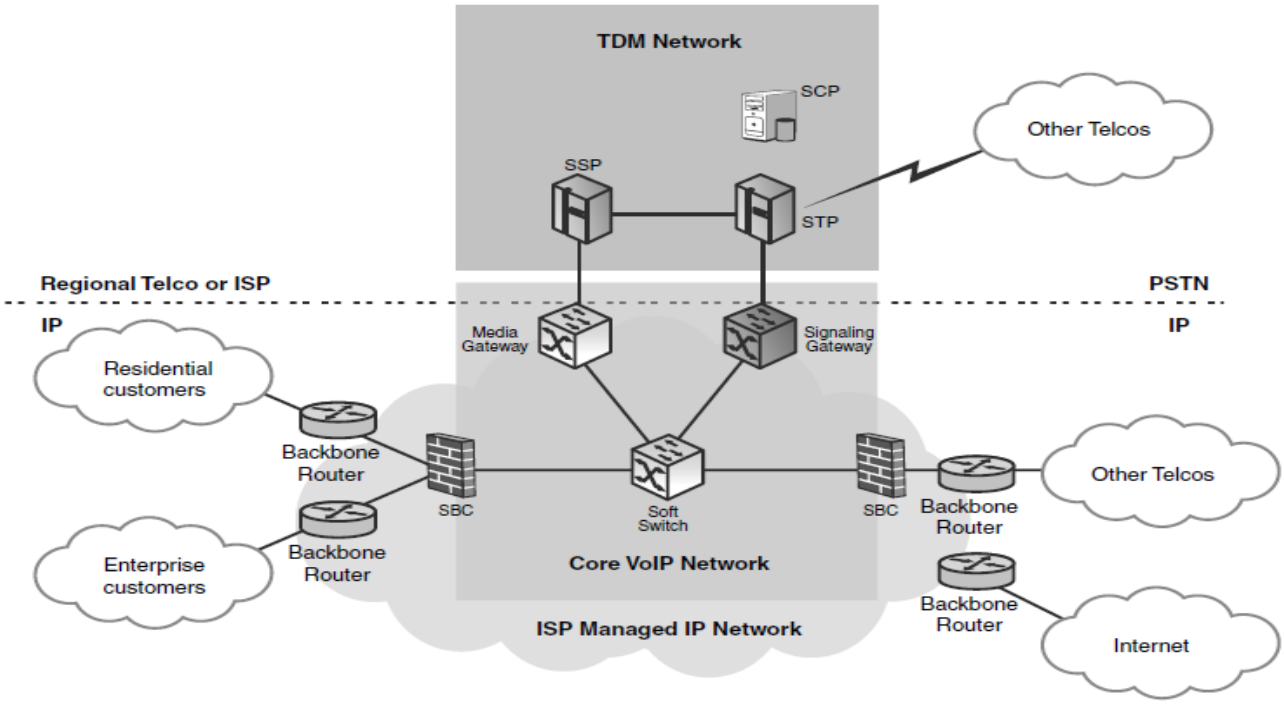
Sumber : Securing VoIP Network

Gambar 3.11 Contoh Arsitektur VoIP (Converged Telco)



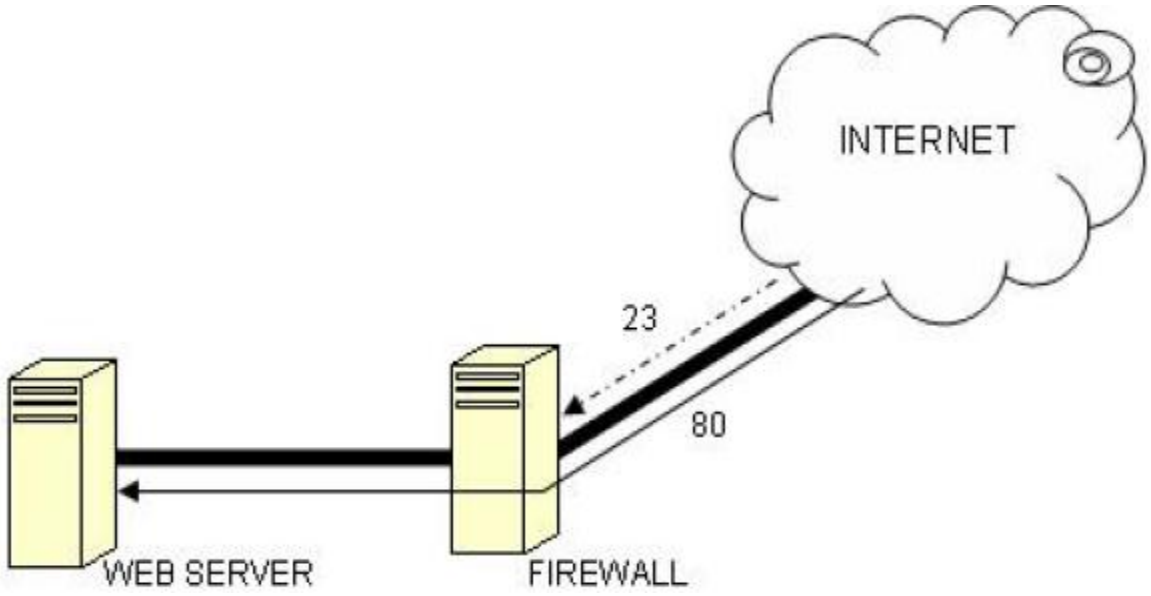
Sumber : Securing Network VoIP

Gambar 3.12 Contoh Penyerangan Jaringan VoIP pada Converged Telco



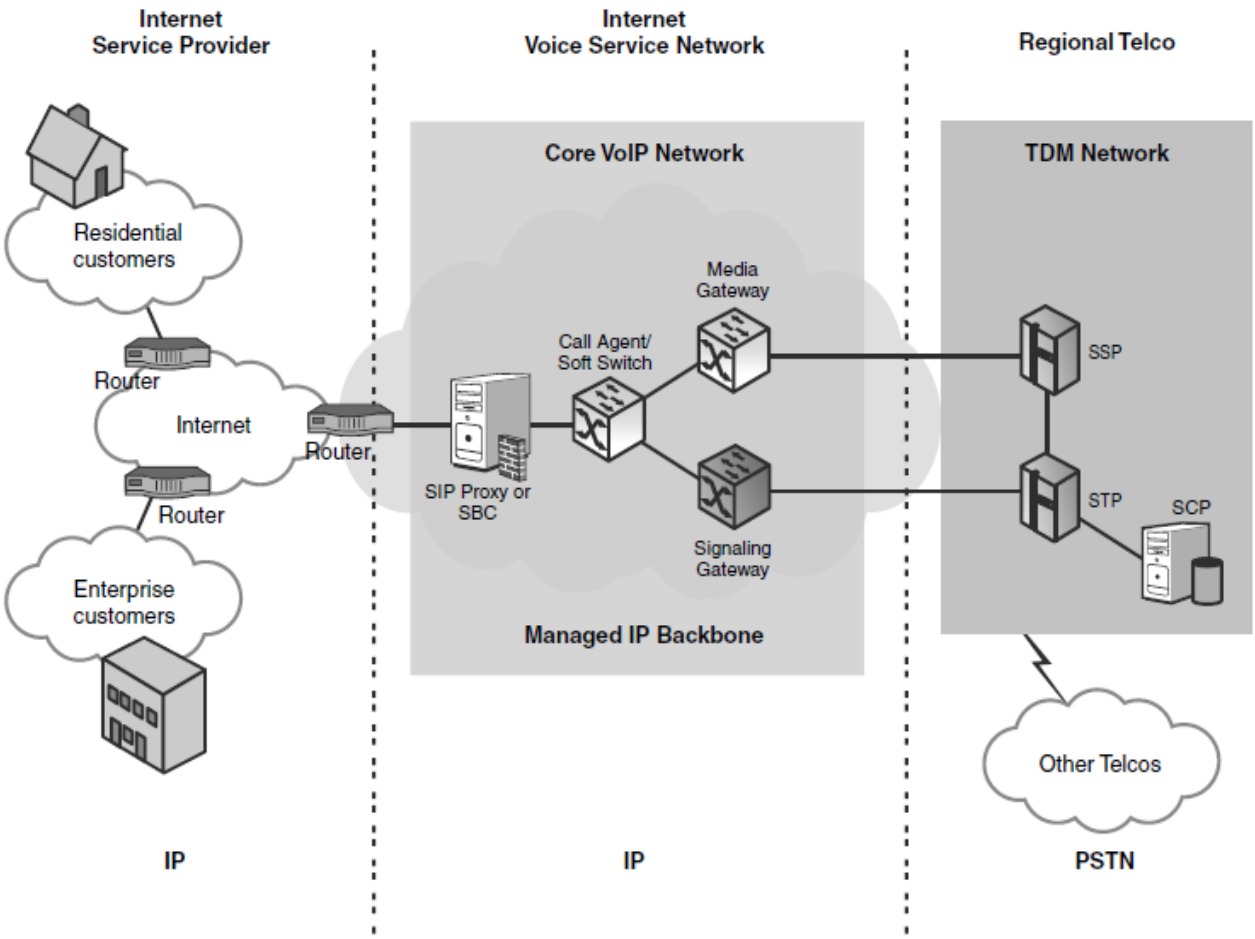
Sumber : Securing Network VoIP

Gambar 3.13 Arsitektur VoIP dengan VSP



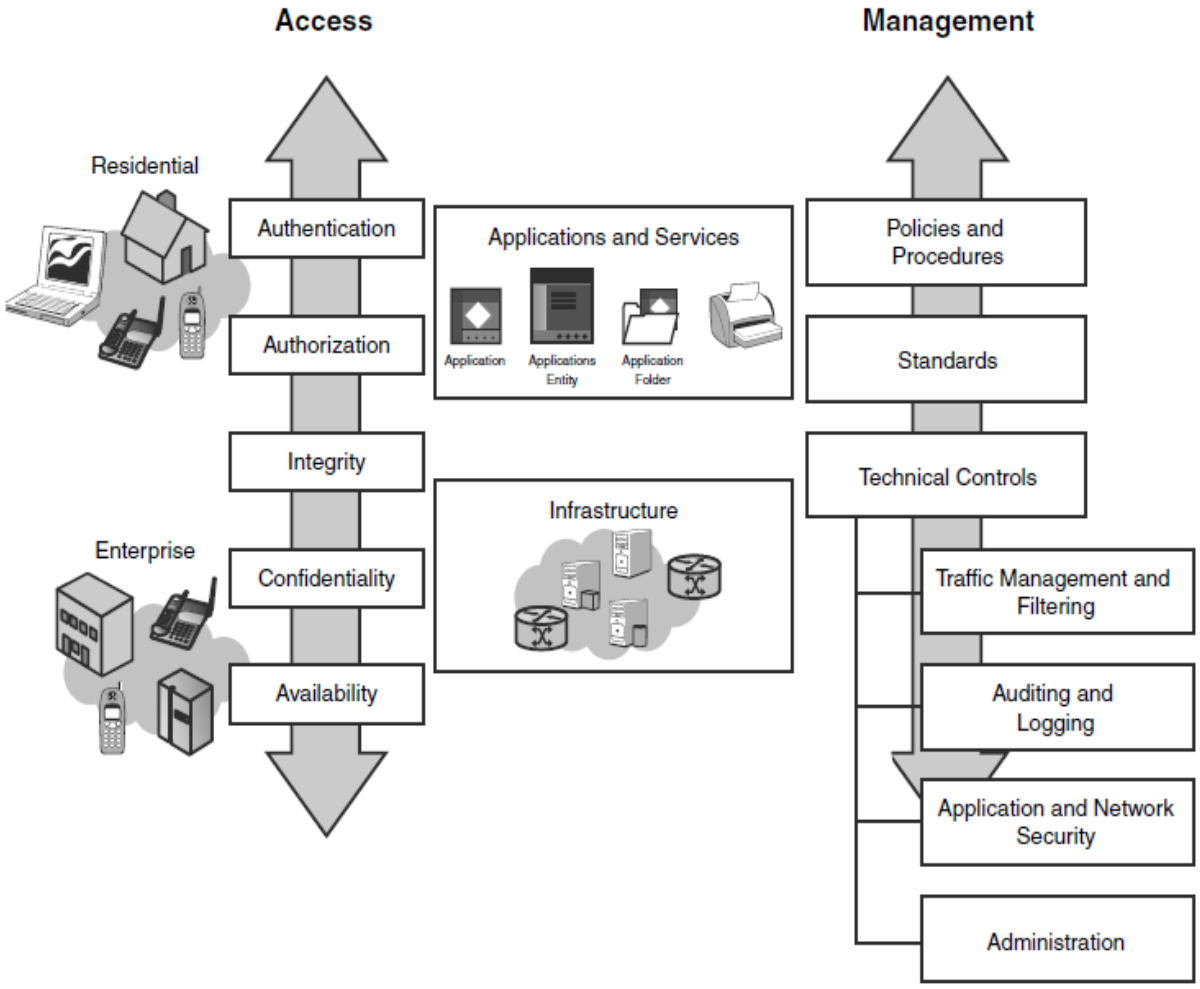
Sumber : Dokumen Kemendikbud

Gambar 3.14 WebServer dengan Firewall



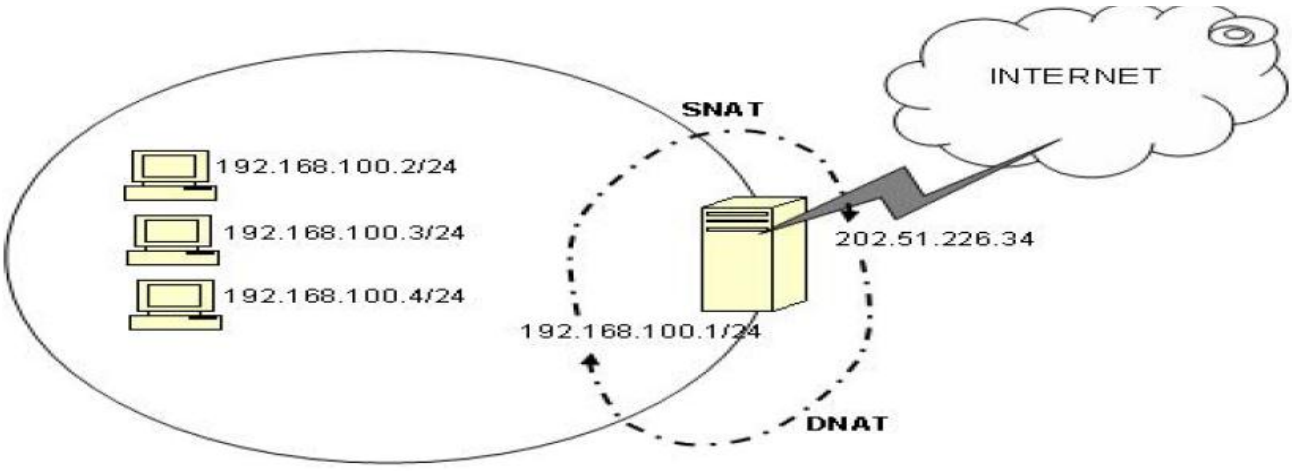
Sumber : Securing Network VoIP

Gambar 3.15 Arsitektur VSP berbasis Internet dengan Firewall



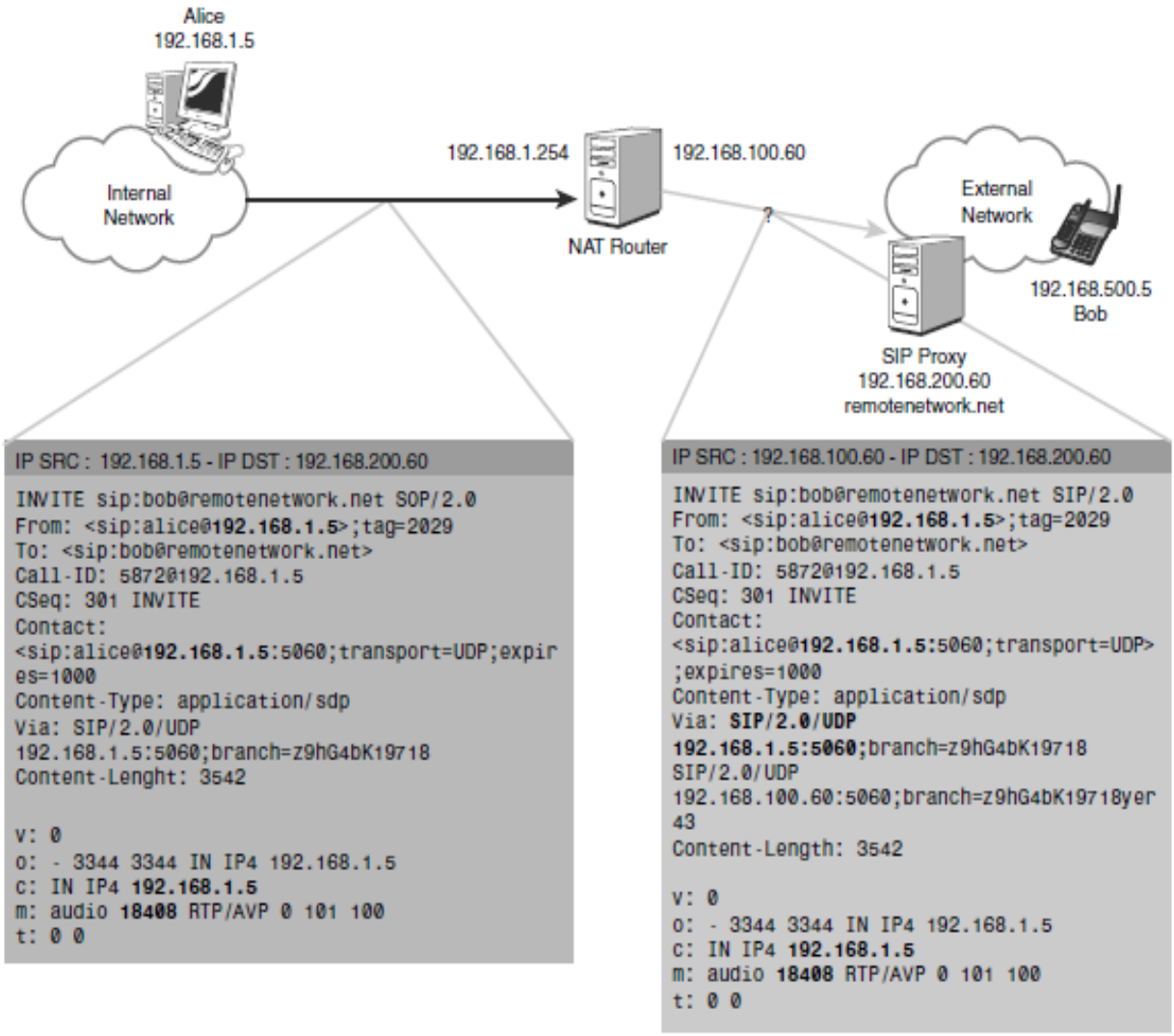
Sumber : Securing Network VoIP

Gambar 3.16 Contoh Framework Proteksi



Sumber : Dokumen Kemendikbud

Gambar 3.17 SNAT yang digunakan untuk mengubah IP pengirim sedangakn DNAT merupakan alamat IP yang belum diubah (pre Routing).



Sumber : Securing Network VoIP

Gambar 3.18 Contoh Kesalahan NAT pada SIP terjadi karena remote telepon diletakkan diluar Firewall NAT.

3.1.2.2 Menanya

Dari tayangan gambar yang dilihat pada bagian 3.1.2.1 Mengamati/Observasi, menurut anda:

1) Bagaimanakah fungsi firewall pada jaringan Komputer?
2) Bagaimanakah fungsi firewall pada jaringan VoIP?

3.1.2.3 Mencoba/Mengumpulkan Informasi

Pada bagian ini, kita akan membahas konsep firewall yang diterapkan pada jaringan komputer dan jaringan VoIP.

1.1.1.1.1 Konsep Firewall pada Jaringan Komputer

Dalam jaringan komputer, khususnya yang berkaitan dengan aplikasi yang melibatkan berbagai kepentingan, akan banyak terjadi hal yang dapat mengganggu kestabilan koneksi jaringan komputer tersebut, baik yang berkaitan dengan hardware

(pengamanan fisik, sumber daya listrik) maupun yang berkaitan dengan software (sistem, konfigurasi, sistem akses, dll).

Internet merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus di tanggung adalah tidak ada jaminan keamanan bagi jaringan yang terkait ke Internet. Artinya jika administrator jaringan tidak hati-hati dalam mengatur sistemnya, maka kemungkinan besar jaringan yang terkait ke Internet akan dengan mudah dimasuki orang yang tidak di undang dari luar. Administrator jaringan yang bersangkutan bertugas untuk menekan resiko tersebut seminimal mungkin. Pemilihan strategi dan kecakapan administrator jaringan ini, akan sangat membedakan apakah suatu jaringan mudah ditembus atau tidak.

Keamanan pada jaringan didefinisikan pada lima kategori berikut:

1. *Confidentiality,* memberi persyaratan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
2. *Integrity*, memberi persyaratan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
3. *Availability*, memberi persyaratan bahwa informasi yang tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
4. *Authentication*, memberi persyaratan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
5. *Nonrepidiation,* memberi persyaratan bahwa baik pengirim maupun penerima pesan informasi tidak dapat menyangkal pengiriman pesan.

Gangguan pada sistem dapat terjadi karena faktor ketidaksengajaan yang dilakukan oleh administrator jaringan (human error), akan tetapi tidak sedikit pula yang disebabkan oleh pihak ketiga. Gangguan dapat berupa perusakan, penyusupan, pencurian hak akses, penyalahgunaan data maupun sistem, sampai tindakan kriminal melalui aplikasi jaringan komputer. Berikut ini merupakan 4 kategori utama bentuk gangguan (serangan) pada sistem:

1. *Interruption* merupakan suatu aset dari suatu sistem diserang sehingga tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan
2. *Interception* merupakan suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud dapat berupa orang, program atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.
3. *Modification* merupakan suatu pihak yang tidak berwenang tapi dapat melakukan perubahan terhadap suatu aset. Contohnya

adalah perubahan nilai pada file data, modifikasi pesan yang sedang ditransmisikan dalam jaringan.

4. *Fabrication* merupakan suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.

Selain empat kategori gangguan tersebut diatas, dalam internetworking dikenal ada beberapa istilah gangguan yaitu sebagai berikut:

1. *Hacking,* berupa pengrusakan pada infrastruktur jaringan yang sudah ada, misalnya pengrusakan pada sistem dari suatu server
2. *Physing*, berupa pemalsuan terhadap data resmi dilakukan untuk hal berkaitan dengan pemanfaatannya.
3. *Deface,* perubahan terhadap tampilan suatu website secara illegal.
4. *Carding,* pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.

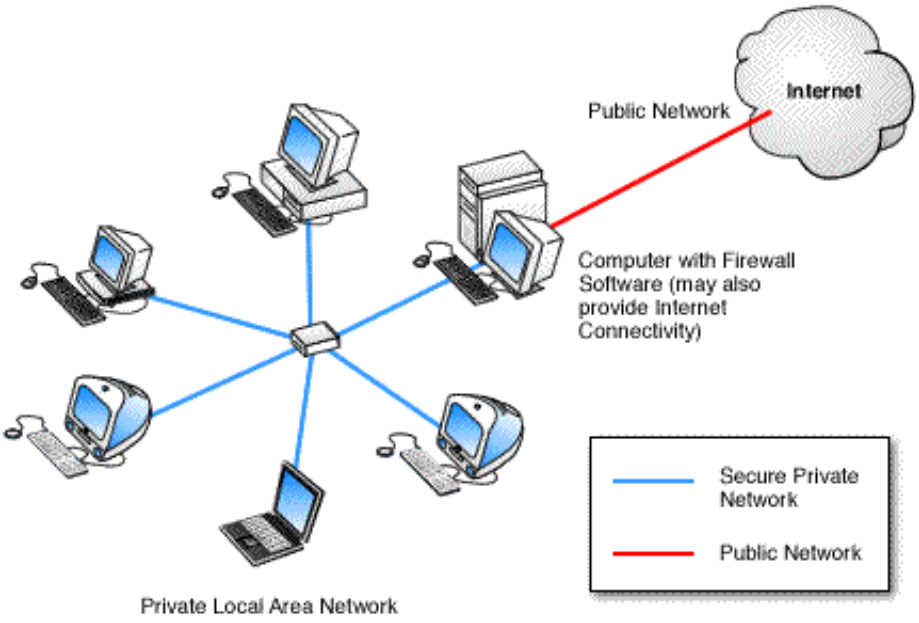
Pengamanan terhadap sistem hendaknya dilakukan sebelum sistem tersebut difungsikan. Percobaan koneksi (*trial*) sebaiknya dilakukan sebelum sistem yang sebenarnya difungsikan. Dalam melakukan persiapan fungsi sistem hendaknya disiapkan pengamanan dalam bentuk:

1. Memisahkan terminal yang difungsikan sebagai pengendali jaringan atau titik pusat akses (server) pada suatu area yang digunakan untuk aplikasi tertentu.
2. Menyediakan pengamanan fisik ruangan khusus untuk pengamanan perangkat yang dimaksud pada point 1. Ruangan tersebut dapat diberikan label Network Operating Center (NOC) dengan membatasi personil yang diperbolehkan masuk.
3. Memisahkan sumber daya listrik untuk NOC dari pemakaian yang lain. Hal ini untuk menjaga kestabilan fungsi sistem. Perlu juga difungsikan Uninteruptable Power Supply (UPS) dan Stabilizer untuk menjaga kestabilan supply listrik yang diperlukan perangkat pada NOC.
4. Merapikan wiring ruangan dan memberikan label serta pengklasifikasian kabel.
5. Memberikan Soft Security berupa Sistem Firewall pada perangkat yang difungsikan di jaringan.
6. Merencanakan maintenance dan menyiapkan Back Up sistem.

Firewall merupakan alat untuk mengimplementasikan kebijakan security (security policy). Sedangkan kebijakan security, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan

implikasi security-nya. Semakin ketat kebijakan security, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau sedemikian sederhananya konfigurasi yang diterapkan, maka semakin mudah orang orang 'usil' dari luar masuk ke dalam sistem (akibat langsung dari lemahnya kebijakan security).

Firewall tersusun dari aturan-aturan yang diterapkan baik terhadap *hardware, software* ataupun sistem itu sendiri dengan tujuan untuk melindungi jaringan, baik dengan melakukan filterisasi, membatasi ataupun menolak suatu permintaan koneksi dari jaringan luar lainnya seperti internet.



Sumber : Dokumen Kemendikbud

Gambar 3.19 Firewall pada Jaringan Komputer

Firewall juga berfungsi sebagai pintu penyangga antara jaringan yang dilindunginya dengan dengan jaringan lainnya atau biasa disebut *gateway*. Gambar 3.4 menunjukkan firewall yang melindungi jaringan lokal dengan cara mengendalikan aliran paket yang melewatinya. Firewall dirancang untuk mengendalikan aliran paket berdasarkan asal, tujuan, port dan informasi tipe paket.Firewall berisi sederet daftar aturan yang digunakan untuk menentukan nasib paket data yang datang atau pergi dari firewall menurut kriteria dan parameter tertentu. Semua paket yang diperiksa firewall akan melakukan mengalami perlakuan yang diterapkan pada *rule* atau *policy* yang diterapkan pada *chains firewall*. Masing-masing tabel dikenakan untuk tipe aktivitas paket tertentu dan dikendalikan oleh rantai aturan filter paket yang sesuai. Rantai (*chains*) adalah daftar aturan yang dibuat untuk mengendalikan paket. Pada firewall terjadi beberapa proses yang memungkinkannya melindungi jaringan.

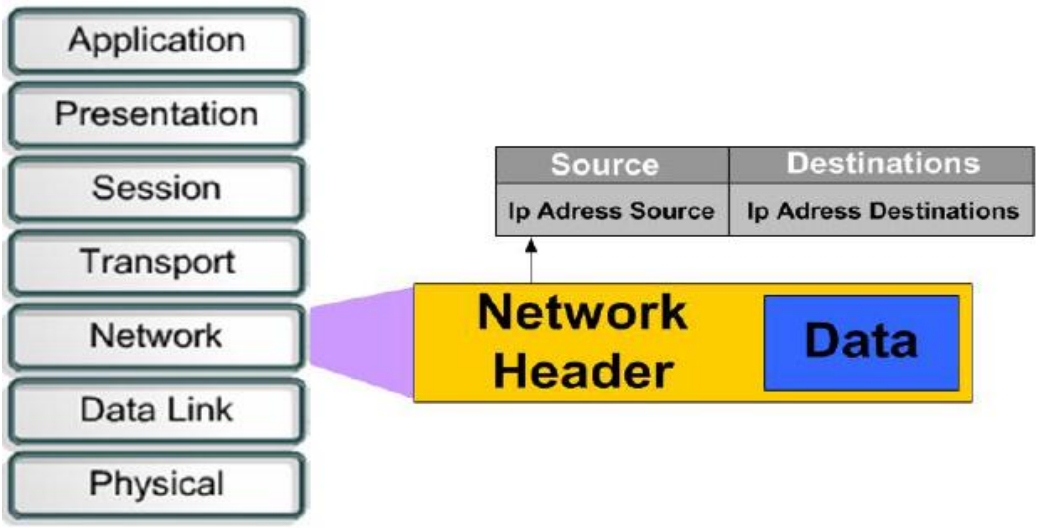
Proses yang terjadi pada firewall ada tiga macam yaitu:

1. Modifikasi header paket, digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing
2. Translasi alamat jaringan, translasi yang terjadi dapat berupa translasi satu ke satu (one to one), yaitu satu alamat IP privat dipetakan ke satu alamat IP public atau translasi banyak ke satu (many to one) yaitu beberapa alamat IP privat dipetakan kesatu alamat public.
3. Filter paket, digunakan untuk menentukan nasib paket apakah dapat diteruskan atau tidak.

Secara umum terdapat 4 jenis firewall yang dibedakan berdasarkan cara kerjanya. Jenis-jenis firewall tersebut adalah sebagai berikut:

1. Packet Filtering Gateway

Packet filtering gateway dapat diartikan sebagai firewall yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jarigan yang dilindunginya. Filterirasi paket ini hanya terbatas pada sumber paket, tujuan paket, dan atribut-atribut dari paket tersebut, misalnya paket tersebut bertujuan ke server kita yang menggunakan alamat IP 202.51.226.35 dengan port 80. Port 80 adalah atribut yang dimiliki oleh paket tersebut. Seperti yang terlihat pada gambar 3.14, firewall tersebut akan melewatkan paket dengan tujuan ke Web Server yang menggunakan port 80 dan menolak paket yang menuju Web Server dengan port 23. Bila kita lihat dari sisi arsitektur TCP/IP, firewall ini akan bekerja pada layer internet. Firewall ini biasanya merupakan bagian dari sebuah **router firewall.** Software yang dapat digunakan untuk implementasi packet filtering diantaranya adalah *iptables* dan *ipfw*.



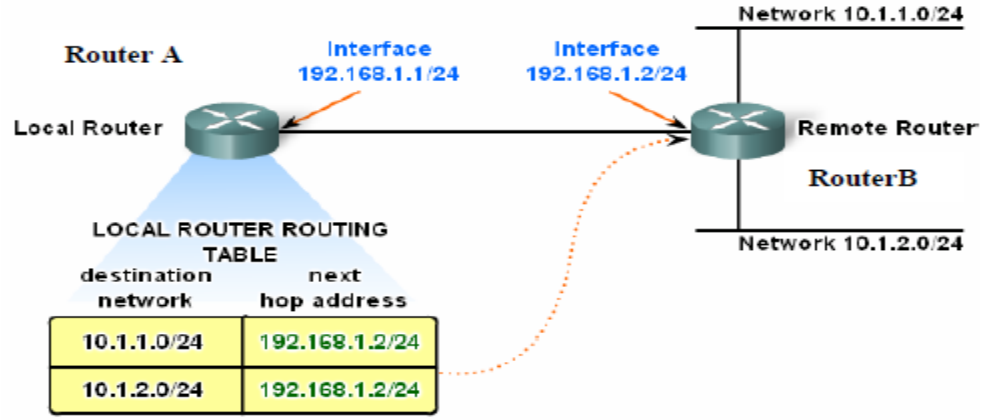
Sumber : Dokumen Kemendikbud

Gambar 3.20 Lapisan untuk Proses Packet Filtering Gateway

Pada Layer 3 yaitu Layer / lapisan network, contoh perangkat hardware yang digunakan delayer ini adalah router, di layer 3 yang diproses hanya IP Address Source dan IP Address Destinations. Encapsulation yang berasal dari Layer sebelumnya, yang akan dibaca adalah IP Address sumber dan tujuan paket tersebut, untuk diteruskan ke routing

yang lain. Pada layer 3 router tidak peduli dimana lokasi suatu host berada dan isi paket data yang dibawa, karena Layer 3 hanya peduli dengan network itu berada dan cara terbaik untuk mencapainya dan menentukan lokasi jaringan tersebut. Pada layer ini akan mengangkut lalu lintas antar peralatan yang tidak terhubung secara lokal.

Sebagai contoh paket diterima oleh interface router, dan mencek alamat IP tujuan, lalu Router mengecek alamat network tujuan pada routing table yang dimilikinya. Jika tidak ditemukan pada entri routing tablenya maka data akan di drop. Jika ditemukan, Interface router akan melewatkan paket data dengan dibungkus menjadi frame data dan dikirimkan ke jaringan lokal/ interface router tetangga untuk dibungkus di layer berikutnya. Jadi yang dibaca dilayer 3 ini hanya ip source dan tujuannya tanpa melihat paket data yang ada. Penggunaan Filtering di layer 3 ini dalam konfigurasinya tergantung dari command dan syntax dari perangkat yang kita gunakan, misalnya jika kita menggunakan router dari vendor cisco systems maka command line Interface yang digunakan disebut Access Control List (ACL). Dalam penggunaan perintah ACL selain kita bisa memfiltering alamat IP yang masuk dan keluar juga dapat memfiltering penggunaan port yang digunakan. ACL biasa digunakan oleh administrator untuk memfilter dan blocking IP Address, port number, dan protocol dari sumber dan tujuan di jaringan.



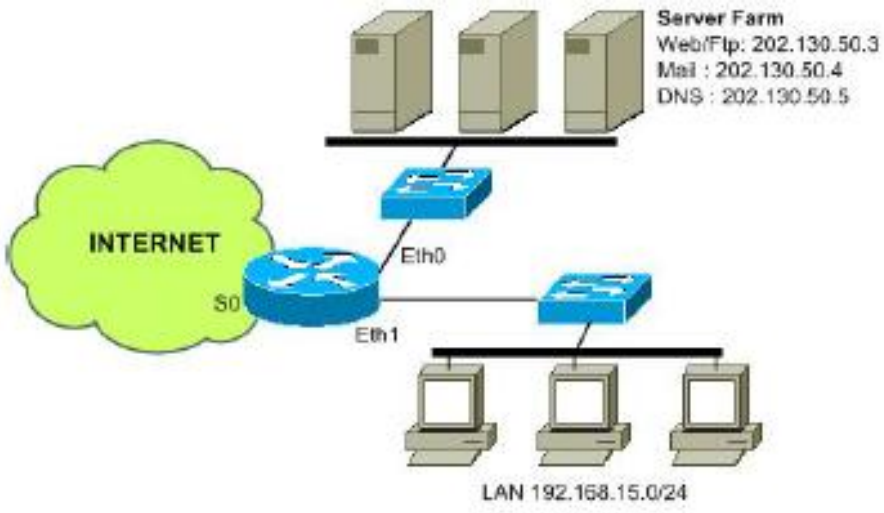

```
  10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

Sumber : http://www.cisco.neacad.net

Gambar 3.21 Routing di Layer Network

Sebagai contoh seperti pada gambar 3.21 , terlihat bahwa router hanya membaca IP Address sumbernya dan tujuannya, dari network header inilah paket data akan diteruskan. Di perangkat router koneksi terjalin ke interkoneksi lainnya lewat suatu interface bisa berupa interface Ethernet, fast Ethernet atau serial yang tergantung dari layanan yang disewa ke provider. Terlihat pada gambar 3.20 IP Address interkoneksi

interface antara router A dan router B adalah 192.168.1.1 dan 192.168.1.2. pada router A terdapat routing table yang menerangkan pengelamatan ke network yang berada di network router B melewati interface router A.



Sumber : http://www.cisco.neacad.net

Gambar 3.22 Router sebagai Packet Filtering

Contoh pada gambar 3.22 diatas dapat dibuat aturan dengan ACL untuk melakukan filtering, blocking terhadap akses. Pembuatan ACL dengan menggunakan Router salah satu vendor network sebagai Firewall yang akan menyaring semua paket data yang akan masuk dan keluar. Dalam contoh ini semua layanan seperti Web, Mail, DNS dan FTP server diletakkan di daerah DMZ (Demilitarized Zone).

Konfigurasi pada Router ;

```
Router(config)# int serial 0
Router(config)# ip access-group filterin in
Router(config)# ip access-group filterout out
Router(config)# no snmp
Router(config)# no ip direct-broadcast
Router(config)# no ip redirects
Router(config)# no ip unreachables
Router(config)# no cdp ena
```

Filter in :

```
Router(config)# ip access-list extended filtering
Router(config)# deny ip 192.0.0.0 0.0.0.255 any
Router(config)# deny ip 172.16.0.15 0.0.0.0.255 any
Router(config)# deny 224.0.0.0 15.255.255.255 any
Router(config)# deny ip host 0.0.0.0 any
Router(config)# permit tcp any host 202.130.0.3 eq 80
Router(config)# permit tcp any host 202.130.0.4 eq 25
Router(config)# permit tcp any host 202.130.0.5 eq 53
```

Filter Out

```
Router(config)# ip access-list extended filterout
Router(config)# permit tcp host 202.130.0.3 any gt 1023 est
Router(config)# permit tcp host 202.130.0.4 any gt 1023 est
Router(config)# permit tcp host 202.130.0.5 any gt 1023 est
Router(config)# permit tcp any any eq 21 reflect packets
Router(config)# permit tcp any any eq 25 reflect packets
Router(config)# permit tcp any any eq 80 reflect packets
```

Konfigurasi ke LAN ;

```
Router(config)# Interface eth0
Router(config)# ip access-group filterin1 in
Router(config)# ip access-list extended filterin 1
Router(config)# permit IP 192.168.0.0 0.0.0.255 any
Router(config)# Interface eth1
Router(config)# ip access-group filterout2 out
Router(config)# ip access-group filterin2 in
```

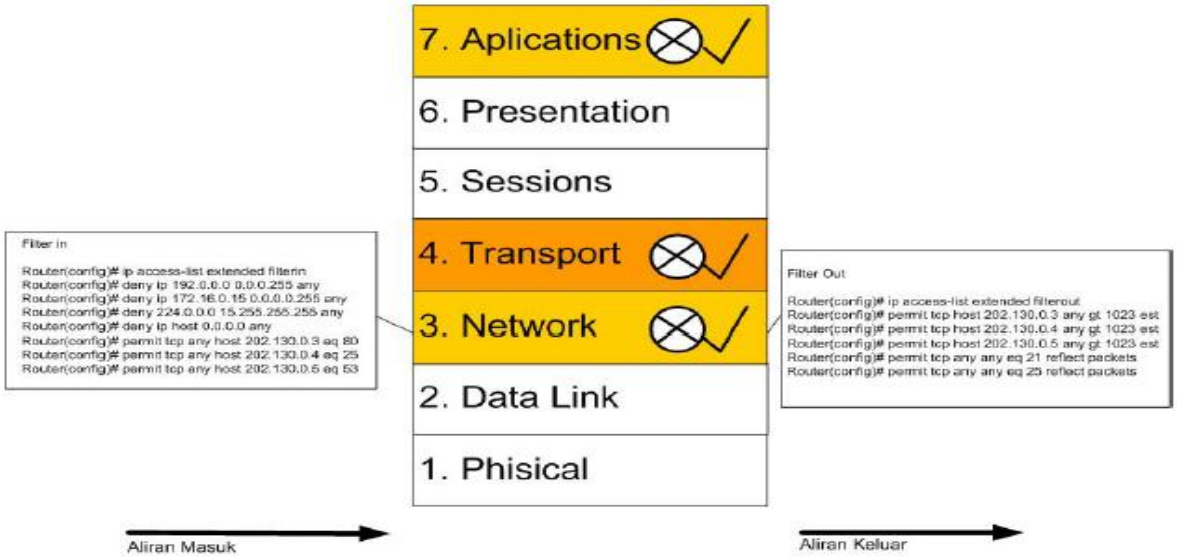
Filter-out 2

```
Router(config)# ip access-list extended filterout2
Router(config)#  permit tcp any host 202.130.50.3 eq 80
Router(config)#  permit tcp any host 202.130.50.4 eq 25
Router(config)#  permit tcp any host 202.130.50.5 eq 53
```

Filter-in 2

```
Router(config)#  ip access-list extended filter2
Router(config)#  permit tcp host 202.130.50.4 any eq 53
Router(config)#  permit udp host 202.130.50.4 any eq 53
Router(config)#  permit tcp host 202.130.50.3 any eq 53
```

Penggunaan Firewall di layer 3 ini untuk menyaring atau Filter Paket yang biasa disebut port based Firewall sangat baik dalam kecepatan membaca paket data namun kurang di aplikasi atau paket yang melewati protocol FTP.

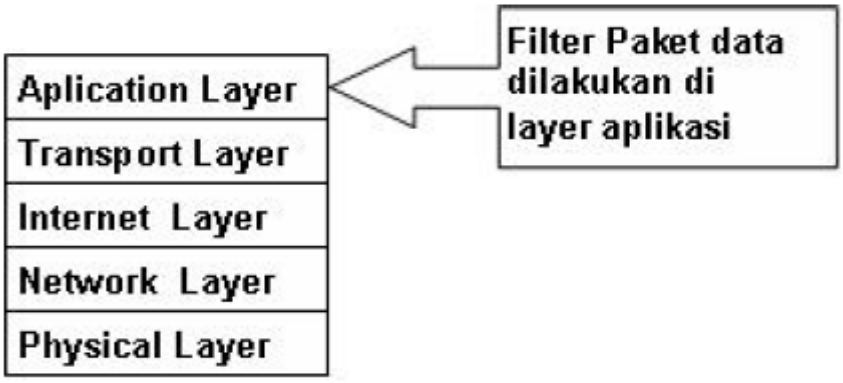


Sumber : Dokumen Kemendikbud

Gambar 3.23 Filter in dan Filter Out pada Network Layer

2. Application Layer Gateway

Model firewall ini juga dapat disebut Proxy Firewall. Mekanismenya tidak hanya berdasarkan sumber, tujuan dan atribut paket, tapi bisa mencapai isi (content) paket tersebut. Mekanisme lainnya yang terjadi adalah paket tersebut tidak akan secara langsung sampai ke server tujuan, akan tetapi hanya sampai firewall saja. Selebihnya firewall ini akan membuka koneksi baru ke server tujuan setelah paket tersebut diperiksa berdasarkan aturan yang berlaku. Bila kita melihat dari sisi layer TCP/IP, firewall jenis ini akan melakukan filterisasi pada layer aplikasi (Application Layer).

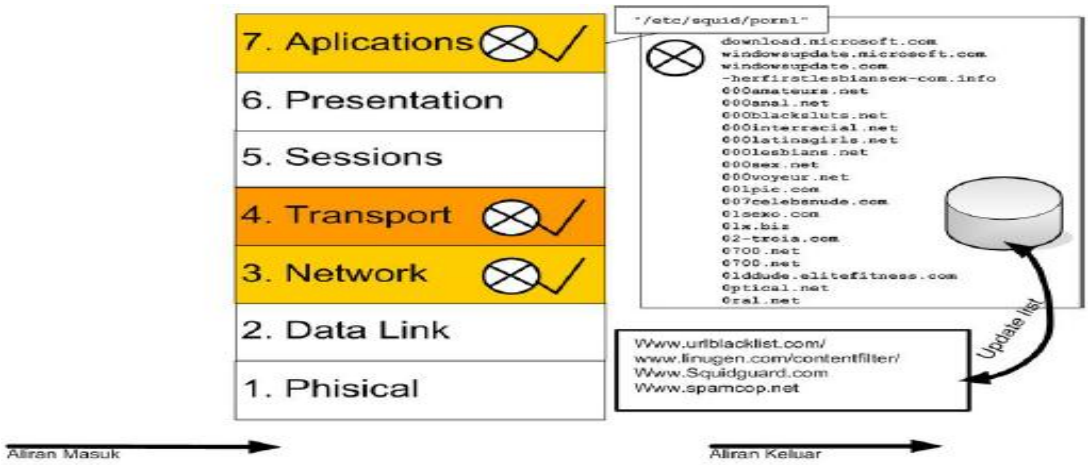


Sumber : Dokumen Kemendikbud

Gambar 3.24 Proxy Firewall dilihat pada Model TCP/IP

Pada Layer 7, Layer Applications berfungsi sebagai Interface antara jaringan dan software aplikasi, contohnya Telnet, HTTP, FTP, WWW Browser, SMTP Gateway atau Mail Client (eudora, outlook, thebat dan sebagainya) . Fungsi utama dari layer 7 adalah mengkomunikasikan service ke aplikasi dan sebagai Interface antara jaringan dengan aplikasi software yang ada. Penggunaan Proxy Server dapat dijadikan

solusi untuk melakukan screening dan blocking di Layer 7, dengan menggunakan proxy dapat menyaring paket-paket berdasarkan policy yang dibuat, misalnya berdasarkan alamat web tertentu.



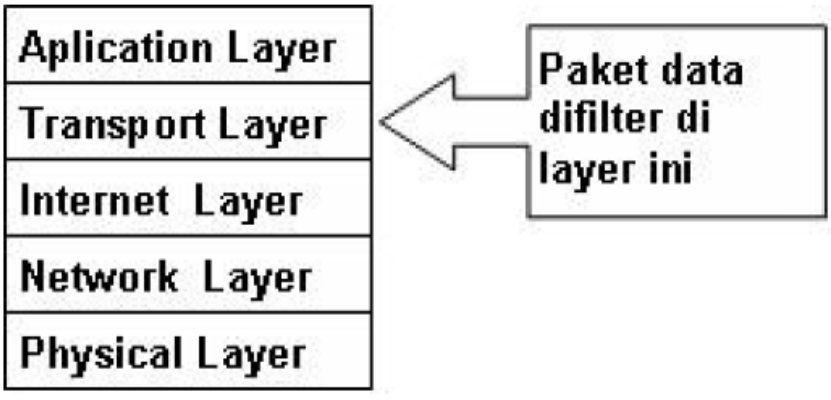
Sumber : Dokumen Kemendikbud

Gambar 3.25 Filtering Content Web

Blocking dengan proxy dapat dioptimalkan dengan menyaring alamat-alamat web yang mengandung content pornography, kekerasan, virus atau trojan, ilegal software dan sebagainya. Pada gambar 3.25 terlihat metode filtering di layer 7 bisa menyaring content website berdasarkan URL yang tidak diperbolehkan mengakses ke jaringan kita, baik paket data yang keluar atau paket data yang masuk. Ada banyak website yang memberikan layanan block alamat-alamat web seperti urlblacklist.org, squidguard.org, spamcop.net .

3. Circuit Level Gateway

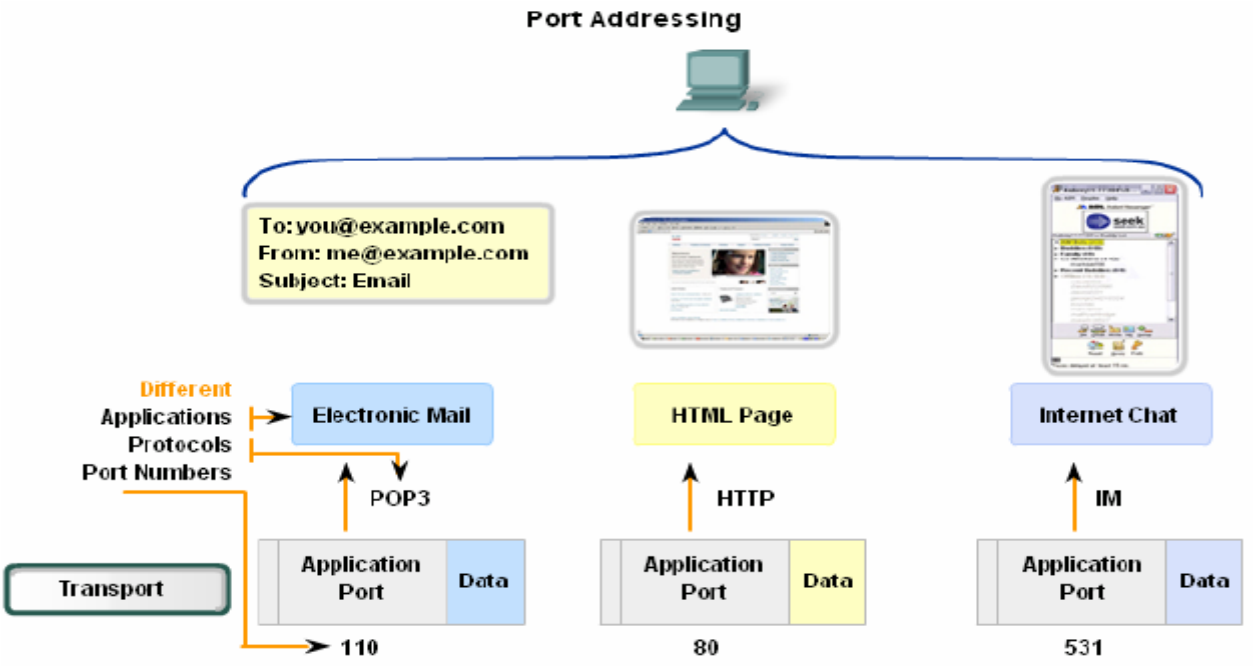
Model firewall ini bekerja pada bagian Lapisan Transport model referensi TCP/IP. Firewall ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Bentuknya hampir sama dengan Application Layer Gateway, hanya saja bagian yang difilter terdapat ada lapisan yang berbeda, yaitu berada pada layer Transport.



Sumber : Dokumen Kemendikbud

Gambar 3.26 Circuit Level Gateway dilihat pada TCP/IP

Pada Layer 4 Transport, prose terjadi melakukan segmentasi dan menyatukan kembali data yang tersegmentasi (reassembling) dari upper layer menjadi sebuah arus data yang sama dan menyediakan layanan tranportasi data ujung ke ujung serta membuat sebuah koneksi logikal antara host pengirim dan tujuan pada sebuah internetwork.



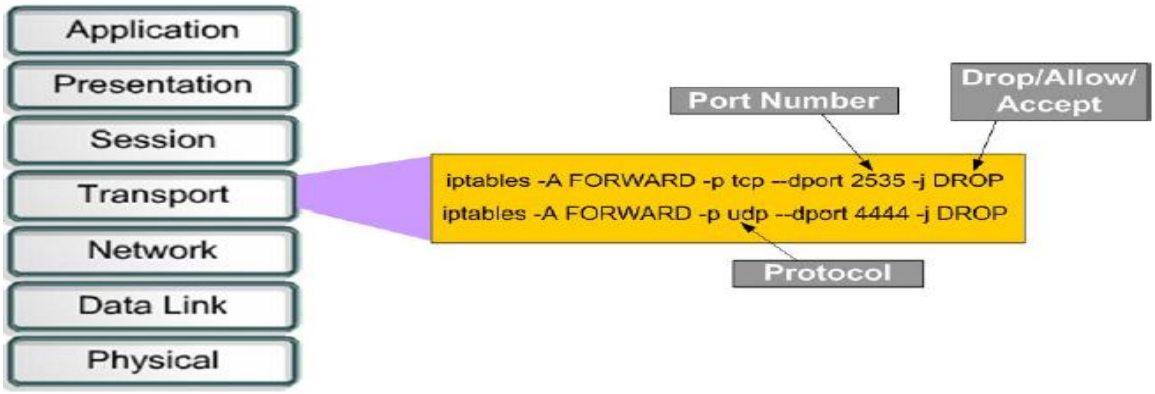
Sumber : http://www.cisco.neacad.net

Gambar 3.27 Multiflexing di Layer Transport

Pada layer 4 ini terjadi proses three-way handshake yang melakukan proses handshake antara sumber dan tujuan dengan menggunakan protocol TCP/UDP dan pengalamatan port number tertentu. Pada layer ini bisa terjadi lebih dari satu proses handshake dikarenakan terdapat bisa terjadi banyak proses komunikasi oleh aplikasi sistem yang disebut Multiflexing, yang memungkinkan bisa melakukan lebih dari satu proses komunikasi secara bersamaan misalnya sambil membuka e-mail dengan mail client juga membuka banyak halaman website pada browser, ditambah dengan melakukan chatting dengan melakukan panggilan VOIP/Video Streaming. Untuk membedakan banyak proses ini penggunaan Port Number adalah jawabannya, dimana setiap aplikasi yang dikembangkan oleh vendor atau pengembang perangkat lunak pasti menggunakan port number tertentu, begitu juga protocol-protocol lainnya. Misalnya pada contoh gambar 10 aplikasi-aplikasi Mail, browser, dan Internet Messaging (IM) koneksinya dapat dilakukan secara bersamaan, untuk membedakan banyak aplikasi yang dibuka ini digunakanlah port number yang sesuai dengan aplikasinya,

seperti untuk mengirim mail menggunakan port 110 untuk protocol POP3 (Post Office Protocol ver 3), port 80 untuk aplikasi browser, dan port 51 untuk aplikasi IM.

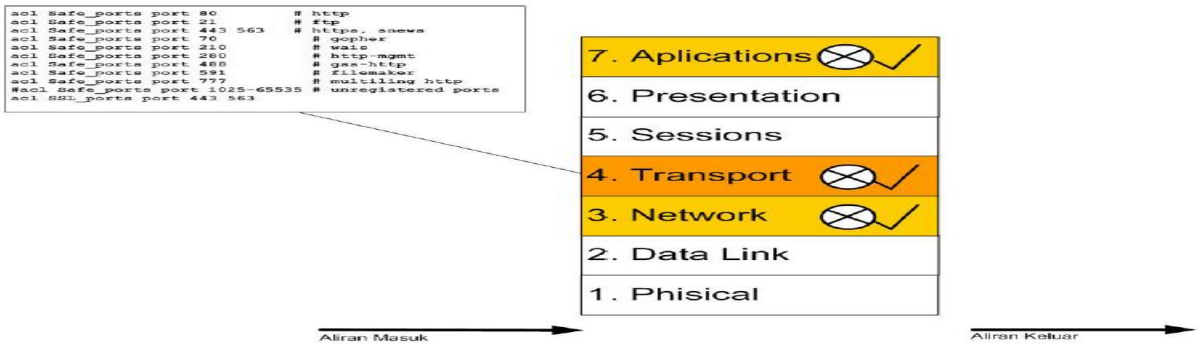
Pada gambar 3.27 terlihat sebuah komputer dapat melakukan banyak koneksi dengan aplikasi-aplikasi tertentu, dimana setiap aplikasi menggunakan port number untuk membedakan komunikasinya ke tujuan. Layer transport bersifat Connectionless atau Connection-oriented yang akan membuat komunikasi yang connection-oriented dengan membuat sesion pada peralatan remote lain. Perbedaan pada proses multiplexing diatas adalah protocol yang digunakan dan port number nya walaupun ada banyak aplikasi yang dibuka.



Sumber : Dokumen Kemendikbud

Gambar 3.28 Metode Filtering IPTABLES

Penggunaan Filtering, Screenning dan Blocking di layer 4 ini dapat dilakukan dengan memperhatikan penggunaan port number yang digunakan. Filtering dan blocking misalnya menyaring penggunaan Protocol tertentu, seperti TCP, UDP, IP, dan ICMP Penggunaan perintah dengan IP Tables adalah salah satu contoh filtering dan blocking di Layer 4 Transport. IP Tables merupakan program IP filter build-in yang disediakan oleh kernel Sistem Operasi Linux. Penggunaan IP Tables biasanya digunakan di sebuah mesin yang di fungsikan sebagai Firewall atau NAT (Network Address Translation) dan Server, contohnya Proxy Server.

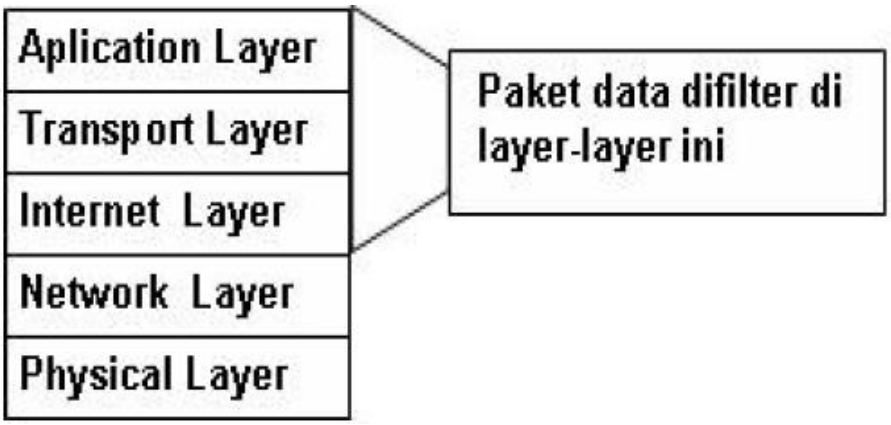


Sumber : Dokumen Kemendikbud

Gambar 3.29 Filtering pada Layer Transport

4. Statefull Multilayer Inspection Firewall

Model firewall ini merupakan penggabungan dari ketiga firewall sebelumnya. Firewall jenis ini akan bekerja pada lapisan Aplikasi, Transport dan Internet. Dengan penggabungan ketiga model firewall yaitu Packet Filtering Gateway, Application Layer Gateway dan Circuit Level Gateway, mungkin dapat dikatakan firewall jenis ini merupakan firewall yang,memberikan fitur terbanyak dan memberikan tingkat keamanan yang paling tinggi.



Sumber : Dokumen Kemendikbud

Gambar 3.30 Statefull Multilayer Inspection Firewall dilihat pada Model TCP/IP

1.1.1.1.2 Konsep Firewall pada Jaringan VoIP

Jaringan VoIP adalah jaringan yang menyediakan layanan multimedia internet aplikasi, memiliki struktur yang cukup rumit dibanding dengan jaringan komputer. Karena kerumitan protokol VoIP maka mekanisme sekuritas terhadap serangan yang mengambil keuntungan dari kelemahan jaringan VoIP perlu dikembangkan dengan baik. Menangkal ancaman dan serangan harus didefinisikan atau dibentuk dengan proses yang baik sehingga pendekatan yang berlapis untuk mempertahankan postur keamanan jaringan VoIP dapat terjamin. Proses tersebut harus dirancang untuk menggambungkan control yang dapat mengatasi hal-hal seperti berikut:

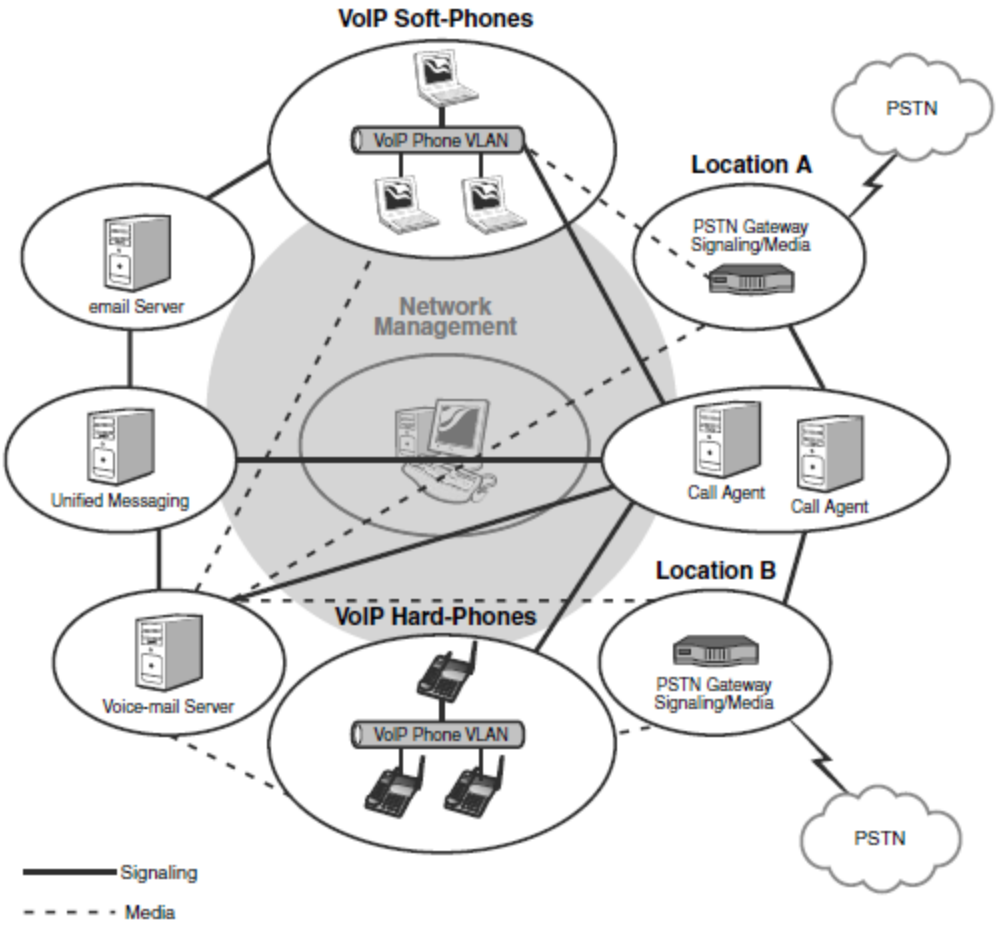
- Mengidentifikasi ancaman yang berlaku
- Mengidentifikasi serangan dan meminimalkan peluang untuk serangan
- Meminimalkan dampak dari serangan (jika terjadi)
- Mengelola dan mengurangi serangan yang sukses secara tepat waktu

Selain itu, control jaringan keamanan VoIP mencakup penggunaan kebijakan keamanan dan komponen yang digunakan untuk mengontrol akses ke sumber daya dan mencegah serangan. Hal yang paling fundamental untuk keamanan jaringan VoIP adalah arsitektur yang *well-defined*. Arsitektur VoIP harus memasukkan persyaratan untuk

keandalan, ketersediaan, kerahasiaan, otorisasi dan integritas. Untuk mendukung tujuan tersebut kita perlu mengidentifikasi, memprioritaskan dan mengkategorikan jenis data dan informasi yang dipertukarkan pada layanan jaringan VoIP. Selain itu, harus diidentifikasi persyaratan keamanan bahwa infrastruktur harus mendukung trujuan jaringan VoIP. Pengembangan persyaratan keamanan akan membantu untuk membangun arsitektur yang kuat dan dapat diukur yang menggabungkan keamanan dan ketersediaan selain QoS. Umumnya, keamanan jaringan VoIP yang ditinjau dari arsitekturnya mencakup Segmentasi jaringan yang tepat (*Network Segmentation*), *out-of-band network management*, dan *private addressing.*

1. Network Segmentation

   Network Segementation atau Sementasi Jaringan merupakan salah satu arsitektur yang perlu diperhatikan dalam layanan komunikasi VoIP. Pada perusahaan, segmentasi jaringan memberikan kemampuan untuk merampingkan dan mengontrol lalu lintas yang mengalir di antara komponen VoIP.



Sumber : Securing VoIP Network

Gambar 3.31 Contoh Arsitektur Segmentasi Jaringan pada Perusahaan

Gambar 3.31 menggambarkan konfigurasi jaringan perusahaan dengan VoIP tersegmentasi. Dalam arsitektur sampel ini, semua komponen kritis logis terisolasi. Penyaringan lalu lintas dapat ditegakkan oleh elemen jaringan pendukung seperti router dan switch atau penggunaan firewall VoIP atau perbatasan sesi controller (Session Border Controller - SBC).

Sebagai contoh, call Agent, PSTN gateways, server pesan suara, unified messaging server, email server, VoIP hard-Phone, dan VoIP soft-Phone, semua terletak di VLAN (Virtual LAN) yang berbeda. Sebagai tambahan signaling dan media lalu lintas antara VLAN dibatasi. Jika lalu lintas penyaringan diberlakukan oleh router atau switch, penggunaan daftar kontrol akses (ACL) adalah pilihan khas. Dalam contoh ini, sebagian besar lalu lintas sinyal akan mengalir antara VLAN yang rumah agen call dan semua VLAN lainnya. Oleh karena itu, ACL pada call agentsVLAN akan lebih panjang dibandingkan dengan VLAN lainnya. Karena lalu lintas sinyal dapat SIP, H.323, MGCP, atau sinyal lain. Oleh karena layanan pengiriman signal dapat berupa SIP, H.323, MGCP atau protokol pengiriman signal yang lain (contoh, Skinny), maka tambahan penyaringan dapat diterapkan untuk mencegah sinyal lain yang dapat mengalir antara VLAN. Tabel 3.1 menunjukkan contoh ACL yang memungkinkan SIP signaling antara VoIP telepon dan Call Agent VLAN.

Table 3.1 Contoh Penyaringan ACL untuk Distribusi Signal

Source	Destination	Transport	Port
Call Agent VLAN	VoIP phone VLAN	UDP	5060
VoIP phone VLAN	Call Agent VLAN	UDP	5060

3.2 menunjukkan contoh yang lain dari suatu ACL yang mengijinkan layanan signal MGCP diantara Call Agent dan Voice gateway VLAN.

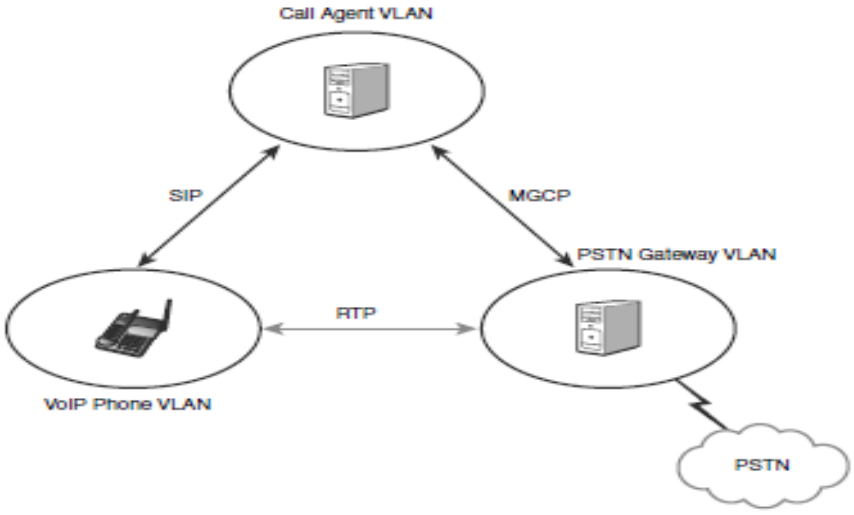
Table 3.2 Contoh 2 Penyaringan ACL untuk Distribusi Signal

Source	Destination	Transport	Port
Call Agent VLAN	Voice gateway VLAN	UDP	2427
Voice gateway VLAN	Call Agent VLAN	UDP	2427

Sebagai tambahan, Call Agent mungkin memiliki kemampuan untuk mengatur panggilan yang masuk (termasuk otentifikasi dan otorisasi)

berdasarkan pada kredensi, profil, manajemen, gudang dan aturan (contoh: menolak panggilan internasional atau sejumlah panggilan dari internal maupun eksternal) dari pengguna VoIP. Media lalu lintas jaringan mengijinkan layanan terjadi antara VLAN yang sudah terdaftar, seperti PSTN gateway VLAN, VoIP phone VLAN, dan Voicemail Server VLAN. Perlu diingat bawha jalur media bernegosiasi secara dinamis antara setiap titik akhir VLAN tersebut. Oleh karena itu, menggunakan ACL untuk membantasi lalu lintas RTP membutuhkan pendefinisian jarak antara port UDP yang diijinkan antara titik akhir. Biasanya, port antara 16.384 dan 32.767 digunakan untuk audio; port antara 49.152 dan 65.535 digunakan untuk video. Sebuah perusahaan penjual layanan VLAN mungkin menggunakan jarak yang berbeda, tetapi jarak yang digunakan seharusnya mungkin untuk mengidentifikasi nilai-nilai rendah dan tinggi dari jangkauan untuk menerapkan ACL yang sesuai.

Gambar 3.32 memperlihatkan contoh penyaringan ACL antara komponen VoIP dalam VLAN yang berbeda. Konfigurasi ini membatasi sinyal VoIP dan lalu lintas media mengalir hanya antara VLAN yang sesuai. Tambahan lagi, contoh tersebut juga memperlihatkan penyaringan ACL menyediakan lapisan pertahanan untuk signaling dan media dari serangan yang berasal dari jaringan selain VLAN yang ditunjuk. Sebagai contoh, sebuah serangan yang berasal dari titik lain dalam jaringan terhadap port signaling gateway suara akan gagal. Dalam kasus di mana lalu lintas sinyal yang dipertukarkan antara komponen VLAN, ACL dapat lebih disesuaikan untuk mengendalikan lalu lintas antara elemen jaringan berdasarkan alamat IP individu daripada seluruh subnet. Dengan kata lain, ACL dapat menegakkan pertukaran lalu lintas yang berasal sinyal dari panggilan agen alamat IP dan gateway IP suara alamat diport yang sesuai. Granularity tersebut jelas tergantung pada ukuran jaringan dan komponen terkait yang perlu dikelola. Untuk lingkungan perusahaan besar, konfigurasi ini mungkin tidak optimal.

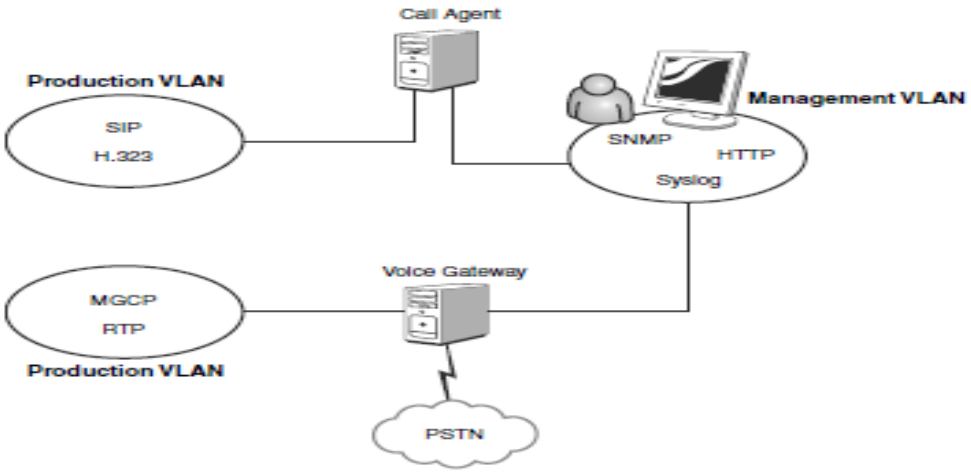


Sumber : Securing VoIP Network

gambar 3.32 Contoh Penyaringan ACL antara panggilan VoIP

2. Out-of-band Network Manajemen

Manajemen infrastruktur VoIP juga merupakan dimensi yang perlu dipertimbangkan dalam arsitektur VoIP. Manajemen jaringan VLAN memiliki visibilitas untuk semua VLAN dalam jaringan untuk memantau kesehatan semua komponen VoIP. Biasanya, komponen inti VoIP dikonfigurasi dengan dua antarmuka jaringan. Salah satu antarmuka ditugaskan untuk manajemen VLAN, dan lainnya ke VLAN produksi di mana sinyal dan media stream ditangani, seperti yang ditunjukkan pada gambar 3.33 berikut ini:



Sumber : Securing VoIP Network

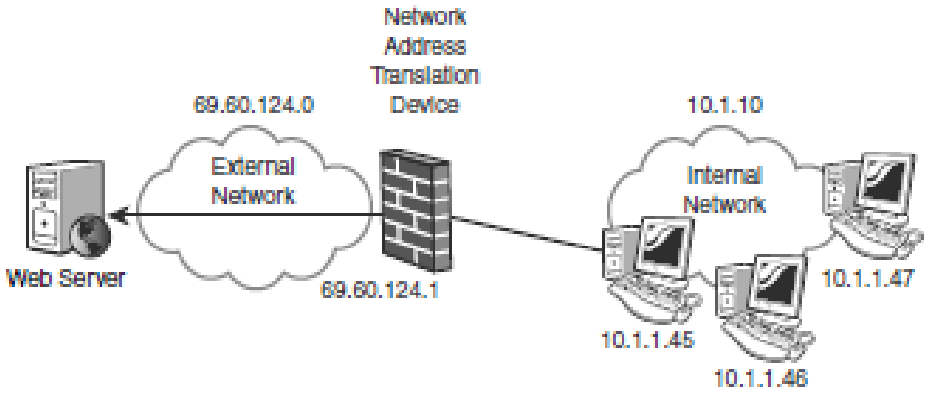
Gambar 3.33 Manajemen Jaringan

Konfigurasi arsitektur ini menyediakan out-of-band manajemen jaringan dan sistem administrasi yang menghilangkan risiko yang terkait dari serangan terhadap manajemen atau port administrasi (misalnya, SNMP, HTTP, Telnet). Hal ini merupakan konfigurasi khas untuk operator telekomunikasi,

penyedia layanan, dan jaringan perusahaan besar. Dalam kasus di mana sumber daya organisasi atau persyaratan tidak mengizinkan untuk konfigurasi antarmuka jaringan dual, lalu lintas manajemen telah dibatasi dengan ACL. Dan seperti sinyal dan protokol media, semua protokol manajemen jaringan secara eksplisit diijinkan antara VLAN dan manajemen jaringan VLAN. Pendekatan ini memungkinkan menegakkan granular penyaringan antara VLAN dan lalu lintas yang melintasi antara VLAN untuk menegakkan keamanan jaringan yang lebih kuat

3. Private Addressing

Private Addressing digunakan sebagai mekanisme lain untuk melindungi terhadap serangan eksternal. Pertumbuhan eksponensial dari internet di awal 1990-an mengisyaratkan menipisnya alamat IP yang unik secara global. IETF dipublikasikan RFC 1918, "Alamat Alokasi untuk Private Internets," dalam upaya untuk mendorong organisasi untuk menggunakan alamat IP nonroutable untuk sistem yang tidak dimaksudkan untuk langsung terhubung ke Internet. dengan mengkonfigurasi host internal organisasi dengan satu set alamat IP dan menggunakan hanya satu set kecil alamat IP untuk lalu lintas rute internet, penipisan Alamat IP routable-Internet telah melambat. Sebuah host internal akan mengirim semua lalu lintas melalui komponen yang bertanggung jawab untuk routing lalu lintas ke Internet dan juga melakukan Network Address Translation (NAT), sebagai digambarkan pada gambar 3.34 Perangkat NAT dapat melakukan address-to-address translation atau alamat dan terjemahan pelabuhan.



Sumber : Securing VoIP Network

Gambar 3.34 Private Addressing

Perangkat NAT mempertahankan tabel yang mengaitkan alamat IP dan port host internal dengan alamat IP dan port dari host eksternal (sumber dan tujuan). Opsi ini memberikan manfaat tambahan bagi keamanan jaringan internal organisasi. Lalu lintas eksternal yang berbahaya menargetkan sistem

internal dijatuhkan kecuali NAT telah membentuk asosiasi dalam tabel negaranya. Oleh karena itu, dianjurkan untuk menggunakan private addressing dalam penyebaran VoIP untuk memberikan lapisan perlindungan. Di saat yang sama, NAT telah memperkenalkan masalah dengan sinyal dan keamanan VoIP.

Firewall VoIP membantu melindungi terhadap berbagai serangan dengan menegakkan kebijakan lalu lintas inbound dan outbound lalu lintas dan mendukung Jaringan dan Alamat port Translation (Network and Port Address - NAPT). NAT menyediakan topologi jaringan internal tersembunyi dan menekan serangan eksternal terhadap host internal. Menyediakan NAT juga memperkenalkan hambatan untuk mengelolah dengan benar Sesi multimedia Internet. Salah satu isu penyebaran dengan VoIP dan firewall adalah manajemen sesi yang tepat. Ketika telepon VoIP yang berada di belakang firewall NAT memulai panggilan ke ponsel lain, sinyal tersebut mengirimkan pesan termasuk informasi yang mencerminkan sifat dari penyelenggara asal telepon. Informasi ini mencakup alamat IP lokal telepon dan port yang pesan itu dikirim dari dan port yang sinyal dan media pesan harus diterima. Jika telepon jarak jauh berada di luar Firewall NAT, informasi yang terkandung dalam pesan sinyal akan tidak sah karena mereka mencerminkan pengalamatan jaringan internal.

Gambar 3.18 pada bagian Mengamati/Observasi memberikan contoh di mana pesan sinyal dari host 192.168.1.5 dikirimkan ke telepon Bob di bob@remotenetwork.com dengan alamat 192.168.200.5. Catatan dua item penting di sini. Pertama, IP alamat pesan telah berubah dari 192.168.1.5 ke 192.168.100.60. Kedua, alamat IP yang diiklankan dalam pesan SIP dimana sinyal dan media pesan tersebut harus dikirim adalah 192.168.1.5, yang tidak benar.

Ketika Bob menjawab telepon, itu akan mulai mentransmisikan ke alamat IP 192.168.1.5 bukan 192.168.100.60, dan semua paket akan dibuang. Firewall NAT harus mampu untuk memeriksa pesan SIP dan membuat modifikasi yang diperlukan untuk header SIP / SDAP untuk mencerminkan sesuai Alamat IP dan port yang harus digunakan (dalam hal ini, firewall NAT alamat eksternal IP dan port dari mana permintaan itu dikirim). Selain itu, firewall NAT harus siap untuk menerima lalu lintas RTP dari Telepon Bob dengan memeriksa header SDP dan mengidentifikasi port telah dinegosiasikan antara dua titik akhir. IETF telah mengembangkan pendekatan untuk mengatasi masalah dengan SIP dan NAT'ing. Solusi ini didefinisikan dalam metodologi ICE dan termasuk STUN (Traversal Sederhana UDP melalui NAT, RFC 3489) protokol dan MENGHIDUPKAN (Traversal Menggunakan Relay NAT). Meskipun firewall VoIP memberikan perlindungan, seperti yang disebutkan sebelumnya, dan mereka dapat mengenali dan menangani komunikasi VoIP, mereka tidak bisa menawarkan skalabilitas

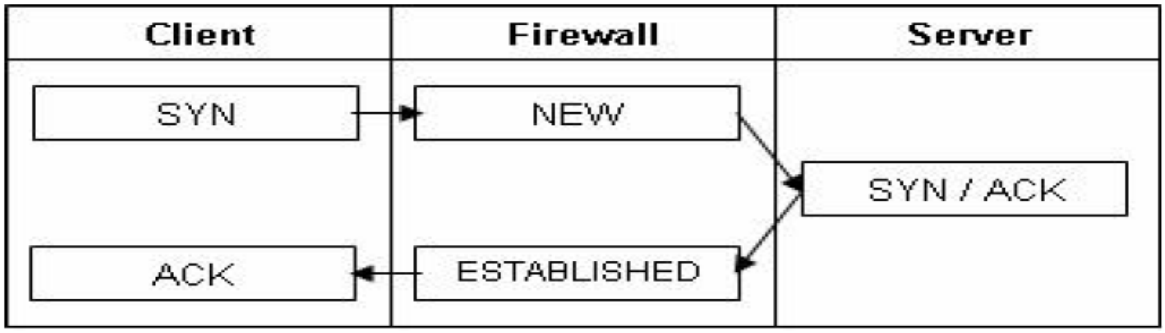
yang diperlukan yang diperlukan untuk mendukung IP multimedia komunikasi dalam lingkungan carrier-grade mana diperlukan untuk mengelola jutaan sesi multimedia simultan. Oleh karena itu, fungsi untuk mengelola sesi multimedia didedikasikan untuk perangkat seperti SBC (pengendali perbatasan sesi).

1.1.1.1.3 Pengendalian Jaringan

Dalam hal pengendalian jaringan dengan menggunakan firewall, ada dua hal yang harus diperhatikan yaitu koneksi firewall yang digunakan (dalam hal ini yang digunakan adalah koneksi TCP), dan konsep firewall yang diterapkan, yaitu IPTables. Dengan dua hal ini diharapkan firewall dapat mengenali apakah koneksi yang ada berupa koneksi baru (NEW), koneksi yang telah ada (ESTABLISH), koneksi yang memiliki relasi dengan koneksi lainnya (RELATED) atau koneksi yang tidak valid (INVALID). Keempat macam koneksi itulah yang membuat IPTables disebut Statefull Protocol.

1. Koneksi TCP

Sebuah koneksi TCP dikenal sebagai koneksi yang bersifat Connection Oriented, pada permulaan koneksi, sebuah klien akan mengirimkan sinyal SYN ke server tujuannya, selanjutnya proses pada firewall menganggap input ini sebagai paket baru yang akan di kirimkan ke server. Server akan mengolah masukan tersebut, dan akan meneruskan ke tujuannya apabila paket tersebut diperbolehkan untuk lewat atau diterima selanjutnya menjadi paket ACK bagi klien. Namun apabila perlakukan bagi paket tersebut adalah menolak atau membuangnya, maka paket tidak akan di perlakukan seperti yang diminta oleh aturan pada firewall.



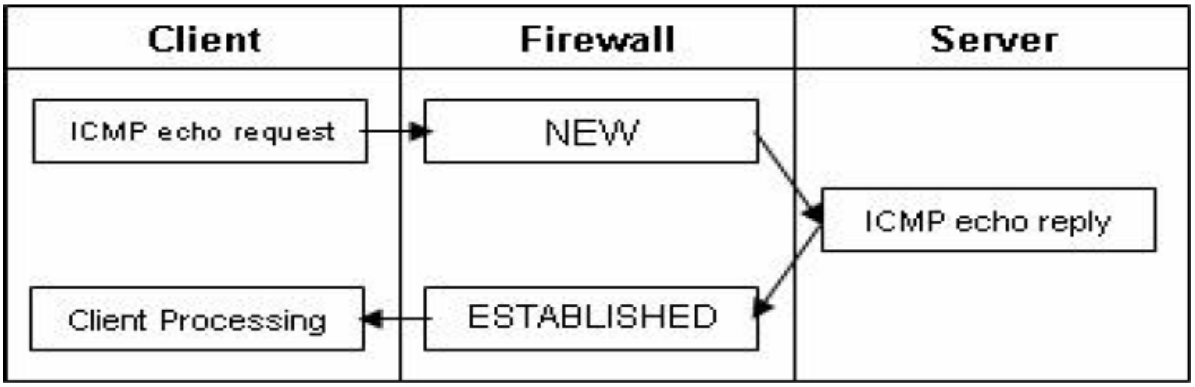
Sumber : Dokumen Kemendikbud

Gambar 3.35 Koneksi TCP pada Firewall

Setelah sinyal tersebut diterima, pada setiap koneksi yang terjadi klien juga akan mengirimkan sinyal ACK kepada server. Pengenalan koneksi oleh firewall seperti NEW, ESTABLISHED, dan RELATED dikenal dengan nama connection tracking. Koneksi TCP juga dikenal sebagai koneksi yang reliable dan menggunakan mekanisme byte stream service. Konsep reliable pada koneksi TCP berarti TCP akan mendeteksi error pada paket yang dikirim dan bila itu terjadi paket akan dikirim kembali. Konsep byte stream service berarti paket-paket dikirim ke tujuan secara urut. Setelah koneksi TCP selesai dilakukan, klien atau server akan mengirimkan signal FIN/ACK kepada mesin

tujuannya. Sinyal ini masih dianggap sebagai koneksi yang sudah terjadi (ESTASBLISHED). Setelah mesin tujuannya menerima sinyal FIN/ACK, mesin tersebut akan membalas dengan sinyal ACK kepada mesin itu kembali dan koneksi akan terputus. Protokol TCP mendominasi penggunaan aplikasi jaringan komputer, namun untuk penyelenggaraan jaringannya protocol IP yang memegang peranan. Dalam hal uji koneksi termasuk didalamnya monitoring jaringan, maka ICMP (Internet Control Message Protocol) diimplmentasikan untuk keperluan ini. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau. Salah satu aplikasi ICMP adalah tools ping yang digunakan untuk monitoring jaringan dengan mengirim pesan ICMP Echo Request (dan menerima Echo Reply) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan.

Sebuah koneksi ICMP hanyalah sebuah permintaan (request) echo dan balasannya (reply). Ada empat macam tipe echo yang akan mendapat paket balasan, yaitu echo request dan reply, timestamp request dan reply, infomation request dan reply, serta address mask request dan reply.



Sumber : Dokumen Kemendikbd

Gambar 3.36 Sebuah Koneksi ICMP

UDP (User Datagram Protocol), adalah salah satu protokol lapisan transport pada model referensi TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP. Protokol ini didefinisikan dalam RFC 768. UDP memiliki karakteristik-karakteristik berikut:

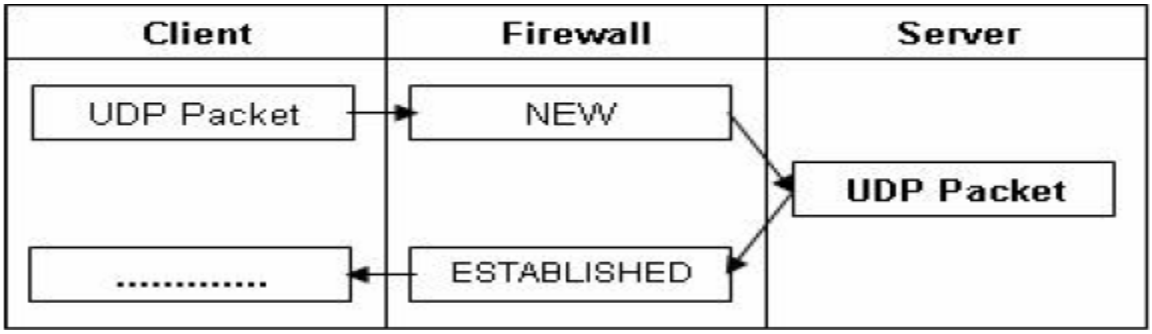
- Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.
- Unreliable (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan

terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.

- UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. Header UDP berisi field Source Process Identification dan Destination Process Identification.
- UDP menyediakan penghitungan checksum berukuran 16-bit terhadap keseluruhan pesan UDP.

Selain keempat karakteritik UPD tersebut, UDP juga diketahui tidak menyediakan layanan-layanan antar-host berikut:

- UDP tidak menyediakan mekanisme penyanggaan (buffering) dari data yang masuk ataupun data yang keluar. Tugas buffering merupakan tugas yang harus diimplementasikan oleh protokol lapisan aplikasi yang berjalan di atas UDP.
- UDP tidak me nyediakan mekanisme segmentasi data yang besar ke dalam segmen-segmen data, seperti yang terjadi dalam protokol TCP. Karena itulah, protokol lapisan aplikasi yang berjalan di atas UDP harus mengirimkan data yang berukuran kecil (tidak lebih besar dari nilai Maximum Transfer Unit/MTU) yang dimiliki oleh sebuah antarmuka di mana data tersebut dikirim. Karena, jika ukuran paket data yang dikirim lebih besar dibandingkan nilai MTU, paket data yang dikirimkan bisa saja terpecah menjadi beberapa fragmen yang akhirnya tidak jadi terkirim dengan benar.
- UDP tidak menyediakan mekanisme flow-control, seperti yang dimiliki oleh TCP.



Sumber : Dokumen Kemendikbud
Gambar 3.37 Koneksi UDP

Pada gambar 3.26 koneksi UDP bersifat connectionless. Sebuah mesin yang mengirimkan paket UDP tidak akan mendeteksi kesalahan terhadap pengiriman paket tersebut. Paket UDP tidak akan mengirimkan kembali paket-paket yang mengalami error. Model pengiriman paket ini

akan lebih efisien pada koneksi *broadcasting* atau *multicasting.*

Seperti halnya TCP, UDP juga memiliki saluran untuk mengirimkan informasi antar host, yang disebut dengan UDP Port. Untuk menggunakan protokol UDP, sebuah aplikasi harus menyediakan alamat IP dan nomor UDP Port dari host yang dituju. Sebuah UDP port berfungsi sebagai sebuah multiplexed message queue, yang berarti bahwa UDP port tersebut dapat menerima beberapa pesan secara sekaligus. Setiap port diidentifikasi dengan nomor yang unik, seperti halnya TCP, tetapi meskipun begitu, UDP Port berbeda dengan TCP Port meskipun memiliki nomor port yang sama. Tabel di bawah ini mendaftarkan beberapa UDP port yang telah dikenal secara luas.

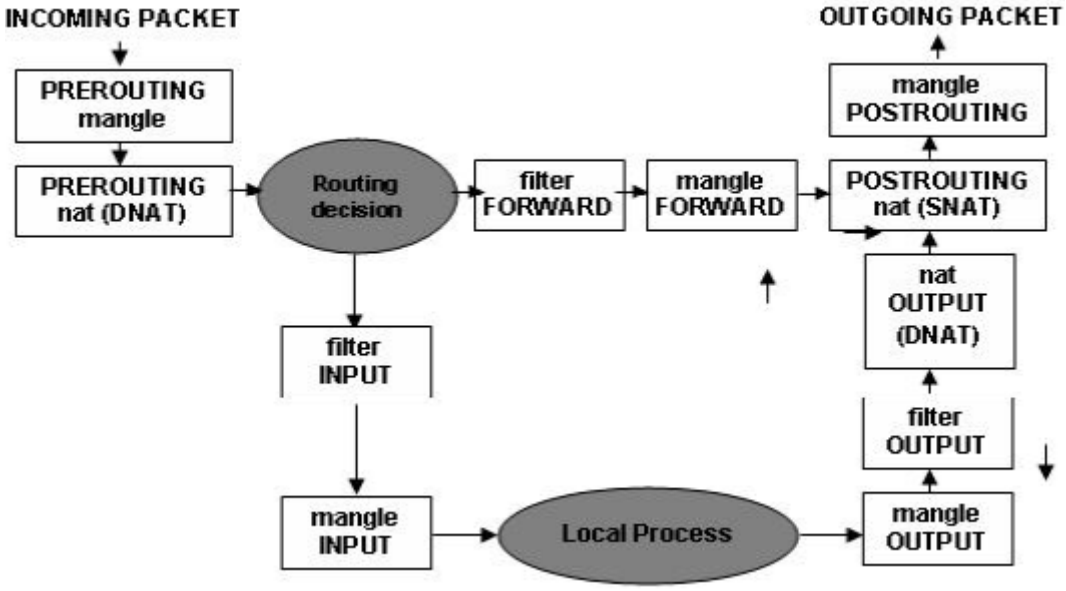
Table 3.3 Tabel Port UDP

Nomor Port UDP	Aplikasi
53	Domain Name System (DNS) Name Query
67	BOOTP klien (Dynamic Host Configuration Protocol [DHCP])
68	BOOTP server (DHCP)
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS Name Service
138	NetBIOS Datagram Service
161	Simple Network Management Protocol (SNMP)
445	Server Message Block (SMB)
520	Routing Information Protocol (RIP)
1812/1813	Remote Authentication Dial-In User Service (RADIUS)

2. Mata Rantai IPTables

Untuk membangun sebuah firewall, yang harus kita ketahui pertama-tama adalah bagaimana sebuah paket diproses oleh firewall, apakah paket-paket yang masuk akan di buang (DROP) atau diterima (ACCEPT), atau paket tersebut akan diteruskan (FORWARD) ke jaringan yang lain. Salah satu tool yang banyak digunakan untuk keperluan proses pada firewall adalah iptables. Program iptables adalah program administratif untuk Filter Paket dan NAT (Network Address Translation). Untuk menjalankan fungsinya, iptables dilengkapi dengan tabel mangle, nat dan filter.

Proses yang terjadi pada paket yang melewati suatu firewall dapat diperlihatkan pada gambar 3.27. Ketika paket dari suatu jaringan masuk pada firewall melalui kartu jaringan, pertama kali paket akan diperiksa oleh aturan rantai PREROUTING sebagai aksi yang dilakukan sebelum routing paket data dilakukan pada tabel mangle. Selanjutnya paket diperiksa oleh aturan rantai PREROUTING pada tabel nat, apakah paket akan memerlukan Tujuan yang terdapat pada aturan tujuan yang di NAT-kan (DNAT) atau tidak. Setelah itu paket mengalami routing. Di bagian ini paket tersebut akan ditentukan berdasarkan tujuan dari paket tersebut. Jika tujuan paket adalah jaringan lain, maka paket akan difilterkan oleh aturan rantai FORWARD pada tabel filter. Jika perlu, paket akan diperiksa oleh aturan rantai POSTROUTING pada tabel nat, apakah paket berasal dari sumber yang mempunyai aturan NAT, yang dalam istilah firewall dikenal dengan istilah SNAT (source NAT).



Sumber : Dokumen Kemendikbud

Gambar 3.38 Proses pada Paket yang Melewati Firewall

Jika tujuan paket adalah firewall, maka paket akan difilter oleh aturan rantai INPUT pada tabel filter. Selanjutnya paket akan mengalami proses lokal, paket tersebut akan di teruskan ke tabel INPUT untuk di proses firewall. Bila paket tersebut bertujuan untuk ke komputer lain yang berbeda jaringan, paket tersebut akan di teruskan ke kolom FORWARD. Proses lokal yang terjadi pada firewall dapat berupa pengiriman paket

kembali. Paket ini akan diperiksa oleh aturan rantai OUTPUT pada tabel MANGLE. Selanjutnya paket diperiksa oleh aturan rantai OUTPUT pada tabel NAT, apakah memerlukan DNAT. Sebelum routing, paket akan difilter oleh aturan rantai OUTPUT pada tabel filter. Setelah paket tersebut memasuki kolomnya (INPUT atau FORWARD) maka paket tersebut akan dicocokkan dengan aturan-aturan yang ada pada kolom tersebut. Paket diperiksa kecocokannya dengan aturan-aturan yang ada. Beberapa aturan yang ada pada urutan firewall akan dibaca oleh sistem secara berurut dari nomor teratas berdasarkan prioritas.

Sebagai contoh, ada paket dengan tujuan alamat IP komputer kita. Paket tersebut akan masuk ke tabel INPUT, kemudian paket tersebut akan di cocokkan dengan aturan no 1. Jika aturan tersebut tidak cocok dengan paket yang datang maka paket tersebut akan di cocokkan dengan aturan ke dua. Bila paket tidak cocok maka paket akan diteruskan ke aturan paket nomor 3. Jika sistem telah mencocokkan dengan aturan yang terakhir (aturan nomor n) tetapi tetap tidak ada kecocok\kan juga maka POLICY pada tabel yang akan berlaku, yaitu apakah paket tersebut akan di terima (ACCEPT) atau paket tersebut akan di buang (DROP). Salah satu kelebihan IPTABLES adalah untuk membuat komputer kita menjadi sebuah gateway menuju internet. Untuk keperluan tersebut, kita akan membutuhkan tabel lain pada IPTABLES selain ketiga tabel diatas. Tabel tersebut adalah tabel NAT (Network Address Translation).

Table 3.4 Tabel Filter pada IPTABLES

NO	INPUT	OUTPUT	FORWARD
1	Aturan no 1	Aturan no 1	Aturan no 1
2	Aturan no 2	Aturan no 2	Aturan no 2
3	Aturan no 3	Aturan no 3	Aturan no 3
N	Aturan no n	Aturan no n	Aturan no n
POLICY	ACCEPT/DROP	ACCEPT/DROP	ACCEPT/DROP

Perhatikan gambar 3.17 pada bagian Mengamati/Observasi SNAT digunakan untuk mengubah alamat IP pengirim (source IP address). Biasanya SNAT berguna untuk menjadikan komputer sebagai gateway menuju ke internet. Misalnya komputer kita menggunakan alamat IP 192.168.0.1. IP tersebut adalah IP lokal. SNAT akan mengubah IP lokal tersebut menjadi IP publik, misalnya 202.51.226.35. begitu juga sebaliknya, bila komputer lokal kita bisa di akses dari internet maka DNAT yang akan digunakan. Mangle pada IPTABLES banyak digunakan untuk menandai (marking) paket-paket untuk di gunakan di proses-proses selanjutnya. Mangle paling banyak di gunakan untuk bandwidth limiting atau pengaturan bandwidth. Fitur lain dari *mangle* adalah kemampuan untuk mengubah nilai

Time to Live (TTL) pada paket dan TOS (*type of service*).

Table 3.5 Table Mangle

NO	PRE ROUTING	INPUT	FORWARD	OUTPUT	POST ROUTING
1	Aturan no 1	Aturan no 1	Aturan no 1	Aturan no 1	Aturan no 1
2	Aturan no 2	Aturan no 2	Aturan no 2	Aturan no 2	Aturan no 2
3	Aturan no 3	Aturan no 3	Aturan no 3	Aturan no 3	Aturan no 3
N	Aturan no n	Aturan no n	Aturan no n	Aturan no n	Aturan no n
POLICY	ACCEPT/DROP	ACCEPT/DROP	ACCEPT/DROP	ACCEPT/DROP	ACCEPT/DROP

1.1.1.1.4 Mendesain Sistem Keamanan Jaringan

Berikut ini adalah langkah-langkah yang diperlukan dalam membangun sebuah firewall:

1. Menentukan topologi jaringan yang akan digunakan. Topologi dan kofigurasi jaringan akan menentukan bagaimana firewall akan dibangun.
2. Menentukan kebijakan atau policy. Kebijakan yang perlu di atur di sini adalah penentuan aturan-aturan yang akan diberlakukan.
3. Menentukan aplikasi– aplikasi atau servis-servis apa saja yang akan berjalan. Aplikasi dan servis yang akan berjalan harus kita ketahui agar kita dapat menentukan aturan-aturan yang lebih spesifik pada firewall kita.
4. Menentukan pengguna-pengguna mana saja yang akan dikenakan oleh satu atau lebih aturan firewall.
5. Menerapkan kebijakan, aturan, dan prosedur dalam implementasi firewall.
6. Sosialisasi kebijakan, aturan, dan prosedur yang sudah diterapkan. Batasi sosialisasi hanya kepada personil teknis yang diperlukan saja.

Dengan melakukan sosialisasi kepada pengguna-pengguna yang di kenai aturan-aturan firewall kita, di harapkan tidak terjadi kesalah-pahaman terhadap peraturan-peraturan yang diberlakukan. Berikut ini diberikan contoh penerapan iptables pada firewall. Konfigurasi network yang digunakan untuk contoh diilustrasikan pada gambar 3.5 pada bagian Mengamati/Observasi. Pada gambar tersebut terdapat suatu firewall yang mempunyai dua antar muka. Firewall berhubungan dengan jaringan internet melalui antar muka eth0 dan berhubungan dengan jaringan privat melalui antar muka eth1. Kadang-kadang firewall berhubungan dengan jaringan internet menggunakan modem, dalam hal ini antarmuka eth0 dapat diganti dengan ppp0. Kemampuan pertama yang harus di miliki firewall adalah melakukan forward IP Address dari antarmuka eth0 menuju antarmuka eth1 dan sebaliknya dari antarmuka eth1 menuju antarmuka eth0. Caranya adalah dengan memberi nilai 1 pada parameter ip_forward dengan perintah

```
# echo "1"
>/proc/sys/net/ipv4/ip_forward
```

Dalam beberapa variant Linux dilakukan dengan memberi baris konfigurasi pada file */etc/sysconfig/network*.

```
FORWARD_IPV4=yes
```

Untuk merancang sistem keamanan jaringan pada contoh tersebut perlu langkah-langkah sebagai berikut:

1. Membuat Inisialisasi

Inisialisasi aturan iptables digunakan untuk membuat kebijakan umum terhadap rantai iptables yang akan di terapkan pada firewall. Kebijakan ini akan di terapkan jika tidak ada aturan yang sesuai. Kebijakan umum yang diterapkan dalam suatu firewall umumnya adalah sebagai berikut:

- Kebijakan untuk membuang semua paket yang menuju, melintas dan keluar dari firewall. Kebijakan ini akan di terapkan pada paket apabila tidak ada satupun aturan yang sesuai dengan paket tersebut. Kebijakan ini di terapkan dengan memberikan status DROP untuk semua rantai pada tabel filter.

```
# iptables –p input DROP
# iptables –p forward DROP
# iptables –p output DROP
```

- Kebijakan untuk menerima semua paket yang menuju dan meninggalkan perangkat loopback. Kebijakan ini di terapkan dengan memberikan status ACCEPT pada semua paket yang masuk dan keluar perangkat loopback.

```
# iptables – A INPUT – i lo – j ACCEPT
# iptables – A OUTPUT– o lo – j ACCEPT
```

- Kebijakan menerima semua paket sebelum mengalami routing. Kebijakan ini diterapkan dengan memberikan status *ACCEPT* untuk rantai *POSTROUTING* dan *PREROUTING* pada tabel *NAT*.

```
# iptables - t nat - p POSTROUTING - j ACCEPT
# iptables - t nat - p PREROUTING - j ACCEPT
```

Tentu saja kebijakan umum yang di terapkan untuk suatu sistem sangat tergantung pada pengelolaan jaringan. Kebijakan tersebut tidak harus seperti di atas, tapi dapat disesuaikan dengan keperluan.

2. Mengijinkan Lalu Lintas Paket ICMP

Paket ICMP biasanya digunakan untuk menguji apakah suatu peralatan jaringan sudah terhubung secara benar dalam jaringan. Biasanya untuk menguji apakah suatu peralatan sudah terhubung secara benar dalam jaringan dapat dilakukan dengan perintah ping. Perintah ini akan mencoba mengirim paket ICMP ke alamat IP tujuan dan menggunakan tanggapan dari alamat IP tersebut. Untuk memberikan keleluasaan keluar, masuk dan melintasnya paket ICMP diterapkan dengan aturan tersebut.

```
# iptables – A INPUT –p icmp -j ACCEPT
# iptables – A FORWARD –p icmp -j ACCEPT
# iptables – A OUPUT –p icmp -j ACCEPT
```

Maksud perintah di atas adalah sebagai berikut:

- Firewall mengijinkan paket ICMP yang akan masuk.
- Firewall mengijinkan paket ICMP yang akan melintas.
- Firewall mengijinkan paket ICMP yang akan keluar.

Perintah ketiga ini memungkinkan firewall untuk mananggapi paket ICMP yang dikirim ke firewall. Jika perintah ketiga tidak diberikan, maka firewall tidak dapat mengirim keluar tanggapan paket ICMP.

Catatan: Kadang-kadang paket ICMP digunakan untuk tujuan yang tidak benar, sehingga kadang-kadang firewall ditutup untuk menerima lalu lintas paket tersebut. Jika firewall tidak diijinkan untuk menerima lalu lintas paket ICMP, maka perintah diatas tidak perlu dicantumkan.

3. Mengijinkan Paket SSH Masuk Firewall

Untuk mengkonfigurasi komputer dalam jaringan, biasanya dilakukan secara jarak jauh. Artinya pengelolaan tidak harus datang dengan berhadapan dengan komputer tersebut. Termasuk dalam hal ini untuk pengelolaan firewall. Untuk mengelola firewall dari jarak jauh, dapat digunakan program SSH. Program SSH menggunakan paket TCP dengan port 22 untuk menghubungkan antara dua komputer. Oleh sebab itu firewall harus mengijinkan paket dengan tujuan port 22 untuk masuk ke firewall. Firewall juga harus mengijinkan paket yang berasal dari port 22 untuk keluar dari firewall. Berikut ini perintah yang diterapkan untuk mengijinkan akses SSH melalui antarmuka eth1 yaitu dari jaringan privat.

```
# iptables – A INPUT –p tcp –dport 22 –i eth1 -j ACCEPT
# iptables – A OUTPUT –p tcp –sport 22 –o eth1 -j ACCEPT
```

Maksud dari perintah di atas adalah sebagai berikut:

- Firewall mengijinkan masuk untuk paket TCP yang punya tujuan port 22 melalui antarmuka eth1
- Firewall mengijinkan keluar untuk paket TCP yang berasal dari port 22 melalui antarmuka eth1

Aturan tersebut memungkinkan akses SSH hanya dari jaringan privat melalui antarmuka eth1. Untuk alasan keamanan, akses SSH dari jaringan privat dapat dibatasi untuk akses yang hanya berasal dari alamat jaringan tertentu atau bahkan dari komputer tertentu. Hal ini dilakukan dengan menambah opsi –s diikuti alamat jaringan atau alamat IP pada perintah pertama, contohnya diijinkan dari sumber yang mempunyai alamat IP hanya 192.168.0.1.

```
# iptables – A OUTPUT –s 192.168.0.1. –p tcp –sport 22 –o eth1 -j ACCEPT
```

4. Mengijinkan Akses HTTP Melintas Firewall

Akses http merupakan protokol yang paling banyak digunakan untuk berselancar di internet. Informasi yang disajikan pada internet umumnya menggunakan akses http ini. Akses http menggunakan port 80 dengan jenis paket TCP. Firewall biasanya mengijinkan akses http terutama yang melintas firewall baik yang keluar atau masuk jaringan privat. Akses http yang keluar jaringan privat digunakan untuk memberi akses http bagi komputer yang berada di jaringan privat. Sedangkan akses http dari internet terjadi apabila pada jaringan privat terdapat server web yang dapat diakses dari jaringan internet. Penerapan aturan iptables untuk mengijinkan akses http adalah sbb:

```
# iptables - A FORWARD -p tcp -dport 80 -i eth1 -j ACCEPT
# iptables - A FORWARD -p tcp -sport 80 -o eth1 -j ACCEPT
# iptables - A FORWARD -p tcp -dport 80 -i eth0 -j ACCEPT
# iptables - A FORWARD -p tcp -sport 80 -o eth0 -j ACCEPT
```

Maksud dari perintah di atas adalah sebagai berikut:

- Firewall mengijinkan melintas untuk paket TCP yang punya tujuan port 80 melalui antarmuka eth1
- Firewall mengijinkan melintas untuk paket TCP yang punya asal port 80 melalui antarmuka eth1
- Firewall mengijinkan melintas untuk paket TCP yang punya tujuan port 80 melalui antarmuka eth0
- Firewall mengijinkan melintas untuk paket TCP yang punya asal port 80 melalui antarmuka eth0.

Perintah pertama dan kedua digunakan untuk mengijinkan akses http yang berasal dari jaringan privat, sedangkan perintah ketiga dan keempat digunakan untuk mengijinkan akses http yang berasal dari internet. Keempat perintah tersebut dapat diganti dengan satu perintah menggunakan opsi multiport sebagai berikut:

```
# iptables – A FORWARD –p tcp –m multiport --port 80 -j ACCEPT
```

Perintah tersebut menyatakan bahwa firewall mengijinkan paket TCP yang punya port 80 (tujuan / asal) untuk melintas (dari *eth0* atau *eth1*).

5. Mengijinkan QUERY Server DNS

Firewall biasanya mempunyai minimal satu alamat IP untuk server DNS. Untuk query server DNS digunakan paket UDP melalui port 53. Firewall memerlukan query server DNS untuk menentukan alamat IP yang berhubungan dengan suatu nama host. Query server DNS pada firewall ini biasanya diijinkan untuk query server DNS keluar firewall (baik via eth0 atau eth1) dan query server DNS melintasi server firewall. Aturan iptables yang diterapkan untuk mengijinkan query sever DNS keluar dari firewall adalah sebagai berikut:

```
# iptables – A OUTPUT –p udp –dport 53 –o eth1 -j ACCEPT
# iptables – A INPUT –p udp –dport 53 –i eth1 -j ACCEPT
# iptables – A OUTPUT –p udp –dport 53 –o eth0 -j ACCEPT
# iptables – A INPUT –p udp –dport 53 –i eth0 -j ACCEPT
```

Maksudnya:

- Firewall mengijinkan keluar untuk paket UDP yang punya tujuan port 53 melalui antarmuka eth1.
- Firewall mengijinkan keluar untuk paket UDP yang punya asal port 53 melalui antarmuka eth1
- Firewall mengijinkan keluar untuk paket UDP yang punya tujuan port 53 melalui antarmuka eth0.
- Firewall mengijinkan keluar untuk paket UDP yang punya asal port 53 melalui antarmuka eth0

Perintah pertama dan kedua digunakan untuk query server DNS keluar melalui antarmuka eth1, sedangkan perintah ketiga dan keempat digunakan untuk mengijinkan query server DNS keluar melalui antarmuka eth0. Selanjutnya firewall akan mengijinkan query server DNS untuk melintas. Aturan iptables untuk mengijinkan query server DNS melintasi firewall adalah sebagai berikut:

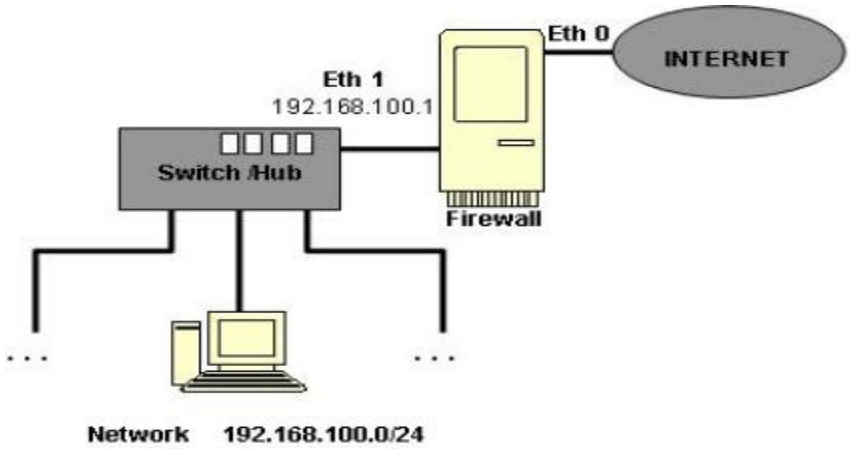
```
# iptables – A FORWARD –p udp –m multiport –ports 53 -j ACCEPT
```

Perintah tersebut menyatakan bahwa firewall mengijinkan paket UDP yang punya port 53 untuk melintas.

1.1.1.1.5 IP Masquerade

Alamat IP yang digunakan untuk menyusun jaringan lokal umumnya menggunakan alamat IP privat. Alamat IP ini tidak diroutingkan oleh jaringan publik, sehingga komputer yang ada pada jaringan lokal tidak dapat langsung berhubungan dengan internet. Hubungan antara komputer pada jaringan lokal dengan jaringan publik dilakukan dengan cara menyamarkan alamat IP privat dengan alamat IP yang dipunyai oleh kartu jaringan dengan alamat IP publik. Proses penyamaran alamat IP privat menjadi alamat IP publik ini disebut dengan IP MASQUERADE. Dengan cara yang diterapkan oleh konsep IP MASQUERADE, semua komputer pada jaringan lokal ketika berhubungan dengan jaringan publik seperti mempunyai alamat IP kartu jaringan yang punya alamat IP publik.

IP MASQUERADE adalah salah satu bentuk translasi alamat jaringan (NAT), yang memungkinkan bagi komputer-komputer yang terhubung dalam jaringan lokal yang menggunakan alamat IP privat untu berkomunikasi ke internet melalui firewall. Teknik IP MASQUERADE adalah cara yang biasanya digunakan untuk menghubungkan jaringan lokal dengan publik (internet). Bagi pelanggan internet yang hanya diberi satu alamat IP dinamis (dial up) menggunakan modem. Berikut ini diberikan contoh penerapan IP MASQUERADE (NAT).



Sumber : Dokumen Kemendikbud

Gambar 3.39 Jaringan untuk Penerapan IP MASQUERADE

Pada gambar 3.35 jaringan privat dengan alamat IP 192.168.100.0/24 berhubungan dengan internet melalui firewall. Pada komputer firewall terdapat dua antarmuka (eth0 dan eth1). Komputer firewall berhubungan dengan jaringan privat melalui eth1 yang diberi alamat IP 192.168.100.254. sedangkan dengan jaringan internet berhubungan melalui eth0 dengan alamat IP publik. Syarat utama supaya dapat menjalankan fungsi IP MASQUERADE, komputer firewall harus memiliki kebijakan untuk meneruskan paket yang akan dikirim melalui eth0 maupun paket yang diterima melalui eth1. Jenis paket dan nomor port yang akan diteruskan diatur melalui chains tertentu. Selanjutnya paket yang akan dikirim melalui antarmuka eth0 harus menjalani translasi alamat IP dengan proses IP MASQUERADE dengan perintah:

```
# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.100.0/24 -j MASQUERADE
```

Perintah tersebut menyatakan bahwa setelah mengalami routing, paket yang akan dikirim melalui antarmuka *eth0* yang berasal dari jaringan 192.168.100.0/24 akan mengalami proses *IP MASQUERADE*. Jika firewall berhubungan dengan internet adalah *ppp0*, sedangkan antarmuka untuk berhubungan dengan jaringan privat adalah *eth0*, dengan demikian harus diberikan perintah:

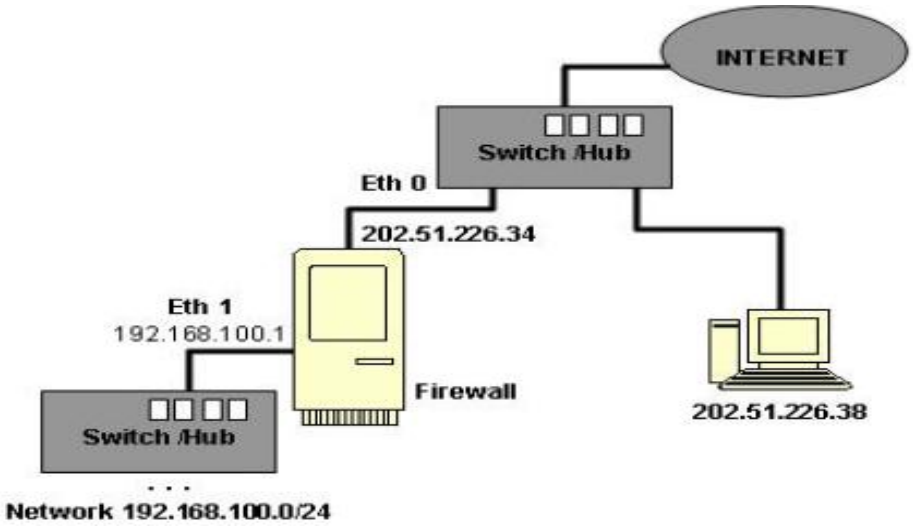
```
# iptables -t nat -A POSTROUTING -o ppp0 -s 192.168.100.0/24 -j MASQUERADE
```

IP MASQUERADE pada hubungan dial up dengan modem dapat juga diterapkan pada pelanggan rumah yang ingin membagi hubungan internet pada beberapa komputer. Translasi alamat IP secara statis dapat dilakukan dengan penerapan konsep subnetting pada pengalamatan jaringan privat. Begitu juga untuk penerapan alamat IP publik yang diberikan oleh Internet Service Provider (biasanya terbatas hanya dua

alamat IP), maka akses dari jaringan lokal dapat dilakukan dengan beberapa cara. Dua contoh yang dapat dilakukan adalah teknik hubungan langsung dan DMZ (De-Militarize Zone).

1. Teknik hubungan Langsung

Pada teknik hubungan langsung, komputer-komputer yang dirancang dapat untuk diakses melalui jaringan internet, diberi alamat IP publik dan langsung dihubungkan pada internet, tanpa melalui firewall. Sehingga komputer tersebut akan dirouting oleh jaringan publik. Contoh struktur nya:



Sumber : Dokumen Kemendikbud

Gambar 3.40 Jaringan Hubungan Langsung

Pada struktur diatas, komputer-komputer yang mempunyai alamat IP publik dihubungkan langsung dengan internet. Komputer dengan alamat IP 202.51.226.35 tidak diletakkan dibawah firewall, sehingga tidak diperlukan translasi alamat IP. Yang diletakkan di bawah firewall hanya komputer dengan alamat IP privat 192.168.100.0/24. Jaringan privat inilah yang memerlukan translasi alamat jaringan ketika berhubungan dengan jaringan public. Jaringan privat ini dapat dihubungkan ke interne dengan menggunakan teknik *IP Masquerade.* Karena alamat IP untuk *eth0* diketahui secara pasti, dapat juga digunakan opsi *–to-source* untuk menentukan asal alamat IP pada alamat publik. Dengan perintah pada firewall sebagai berikut:

```
# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.100.0/24 -j snat -to-source 202.51.226.34
```

Perintah ini menyatakan bahwa setelah mengalami routing, paket yang akan dikirim melalui antarmuka eth0 yang berasal dari jaringan 192.168.100.0/24 akan mengalami SNAT menjadi alamat IP 202.51.226.34.

2. DMZ (De-Militarized Zone)

Pada teknik ini, baik komputer yang dirancang untuk dapat diakses dari internet maupun yang tidak dapat diakses dari internet semuanya diberi alamat IP privat dan

diletakkan dibawah firewall. Alamat IP komputer yang dirancang dapat diakses dari internet dipetakan ke alamat IP publik yang diberikan pada firewall. Pemetaan yang terjadi adalah dari satu ke satu. Ada dua teknik DMZ yang dapat digunakan. Yang pertama adalah meletakkan komputer DMZ pada jaringan yang terpisah dari jaringan privat. Yang kedua adalah meletakkan komputer DMZ pada jaringan yang sama dengan jaringan privat.

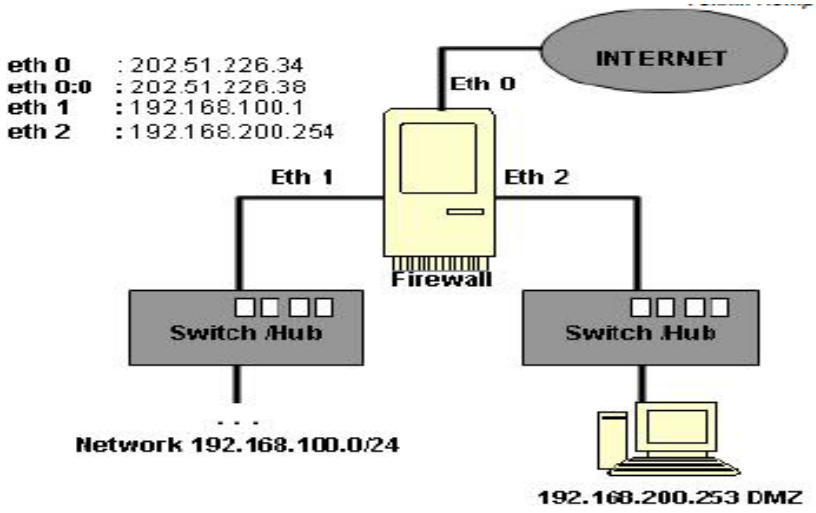
a. DMZ pada Jaringan Terpisah

Pada teknik ini, untuk komputer yang berada pada DMZ dibuatkan jaringan tersendiri yang terpisah dari jaringan privat lain. Komputer pada DMZ tetap menggunakan alamat IP privat. Dalam hal ini firewall memerlukan tiga kartu jaringan, yaitu:

- eth0 berhubungan dengan internet
- eth1 berhubungan dengan jaringan privat.
- eth2 berhubungan dengan DMZ.

```
# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.100.0/24 -j snat --to-source 202.51.226.34
```

Topologinya dapat digambar pada gambar 3.37 berikut:



Sumber : Dokumen Kemendikbud

Gambar 3.41 Jaringan DMZ Terpisah

Pada topologi diatas terdapat suatu firewall dengan tiga antarmuka, yaitu eth0, eth1 dan eth2. Kartu eth0 diberi dua alamat IP publik menggunakan teknik ip alias, yaitu 202.51.226.34 dan 202.51.226.38. Alamat IP 202.51.226.34 digunakan untuk memetakan alamat IP seluruh komputer pada jaringan 192.168.0.100/24, sehingga terjadi pemetaan banyak ke satu. Alamat IP 202.51.226.38 digunakan untuk memetakan satu komputer yang memiliki alamat 192.168.200.253, sehingga terjadi pemetaan satu ke satu. Untuk keperluan translasi alamat jaringan 192.168.0.100/24 dapat digunakan teknik yang sudah dibahas pada bagian sebelumnya.

```
# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.100.0/24 -j snat -to-source 202.51.226.34
```

Sedangkan untuk translasi alamat jaringan bagi komputer dengan alamat 192.168.200.253 dapat menggunakan pasangan perintah sebagai berikut:

```
# iptables -t nat -A POSTROUTING -i eth0 -d 202.51.226.38 -j DNAT --to-destination 192.168.200.253.
# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.200.253.-j SNAT --to-source 202.51.226.38.
```

Maksudnya:

- Perintah pertama menyatakan bahwa sebelum routing, paket yang masuk melalui antarmuka *eth0* dengan tujuan 202.51.226.38 akan mengalami proses *DNAT* menjadi alamat IP tujuan 192.168.200.253.
- Perintah kedua menyatakan bahwa setelah routing, paket yang akan dikirim melalui antarmuka *eth0* yang berasal dari alamat 192.168.200.253 akan mengalami proses *SNAT* menjadi alamat tujuan 202.51.226.38.

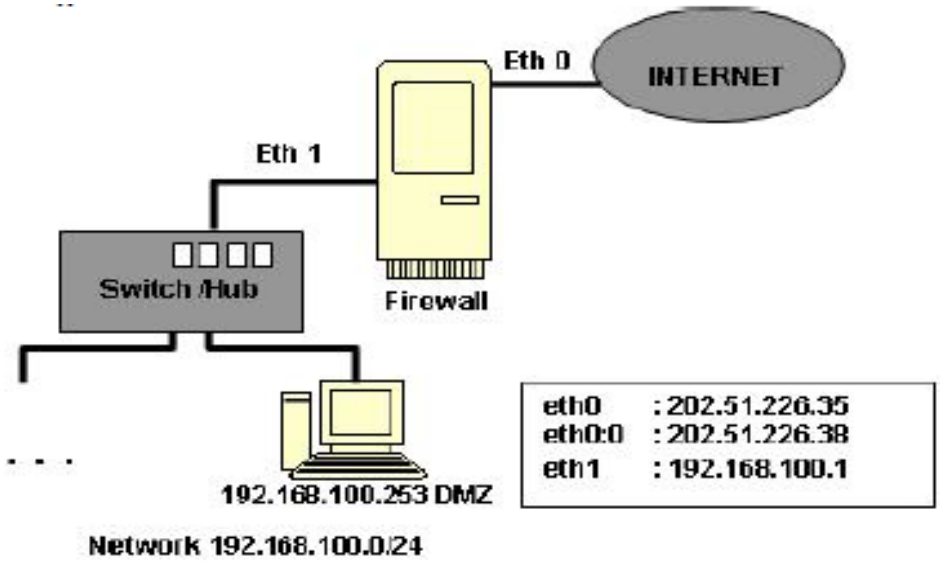
Pada teknik ini, hubungan antara alamat jaringan DMZ dengan alamat jaringan privat dilakukan secara routing.

b. DMZ pada Satu Jaringan

Pada teknik DMZ juga dimungkinkan untuk memasukkan komputer DMZ dengan alamat yang sama dengan alamat jaringan privat, Dalam hal ini komputer DMZ menggunakan alamat IP pada jaringan tersebut. Teknik ini akan menghemat penggunaan switch dan kartu jaringan. Pada teknik ini komputer firewall cukup menggunakan dua antar muka eth0 dan eth1. Eth0 digunakan untuk berhubungan dengan internet, sedangkan eth1 digunakan untuk berhubungan dengan jaringan privat.

```
# iptables -t nat -A POSTROUTING -i eth0 -d 202.51.226.38 -j DNAT --to-destination 192.168.200.253.
# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.200.253.-j SNAT --to-source 202.51.226.38.
```

Struktur DMZ pada satu jaringan dapat dilihat pada gambar berikut:



Sumber : Dokumen Kemendikbud

Gambar 3.42 Jaringan DMZ dalam Satu Jaringan

Pada struktur diatas terdapat satu firewall yang mempunyai dua antarmuka (*eth0* dan *eth1*). Antarmuka *eth0* diberi dua alamat IP publik menggunakan teknik IP Alias, yaitu 202.51.226.34 dan 202.51.226.38. Alamat IP 202.51.226.34 digunakan untuk memetakan alamat IP seluruh komputer pada jaringan 192.168.100.0/24, sehingga terjadi pemetaan banyak ke satu. Alamat IP 202.51.226.38 digunakan untuk memetakan satu komputer itu yang memiliki alamat IP 192.168.100.253, sehingga terjadi pemetaan satu ke satu. Alamat jaringan 192.168.100.0/24 dapat dianggap sebagai jaringan DMZ, tapi hanya ada satu komputer yang menggunakan pemetaan satu ke satu, sedangkan komputer yang lain menggunakan pemetaan banyak ke satu. Untuk translasi alamat jaringan 192.168.100.0/24 dapat digunakan teknik masquerade sebelumnya. Sedangkan untuk translasi alamat jaringan untuk komputer dengan alamat IP 192.168.100.253, dapat menggunakan pasangan perintah sebagai berikut:

```
# iptables -t nat -A PREROUTING -i eth0 -d 202.51.226.38 -j DNAT --to-destination 192.168.100.253
# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.100.253 -j SNAT --to-source 202.51.226.38
```

Maksud dari perintah tersebut adalah:

- Perintah pertama menyatakan bahwa sebelum routing, paket yang masuk melalui antarmuka eth0 dengan tujuan 202.51.226.38 akan mengalami DNAT menjadi alamat tujuan 192.168.100.253
- Perintah kedua menyatakan bahwa setelah routing, paket yang akan dikirim melalui antarmuka eth0 yang berasal dari alamat IP 192.168.100.253 akan mengalami proses SNAT menjadi alamat asal 202.51.226.38

Perlu dicatat bahwa komputer yang dirancang untuk berhubungan dengan internet dengan teknik DMZ tidak terbatas pada satu komputer.

c. Firewall dengan Hardware Khusus

Fungsi firewall seperti disebutkan diatas dapat juga dilakukan dengan menggunakan hardware khusus dari vendor yang telah didesain untuk keperluan pembuatan chains tertentu. Walaupun demikian, teknik dan penerapannya sama saja dengan menggunakan IP Tables. Pada hardware khusus Firewall penerapan chains-nya didesain sedemikian, agar memudahkan administrator dalam mengimplementasikan rule/policy firewall. Satu hal yang membedakan adalah perangkat firewall dari vendor hanya didesain khusus untuk keperluan chains tanpa fungsi lain, sementara PC Firewall dapat digunakan selain untuk Firewall juga untuk fungsi terminal jaringan yang lain.

1.1.1.2 Mengasosiasi/Menalar

Dari hasil pengamatan dan observasi, penalaran terhadap fungsi dari firewall pada jaringan komputer adalah sebagai berikut:

1) Mengontrol dan mengawasi paket data yang mengalir di jaringan, Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall;
2) Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat;
3) Melakukan autentifikasi terhadap akses;
4) Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi;
5) Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

Sedangkan fungsi firewall pada jaringan VoIP adalah sebagai berikut:

1) VoIP memiliki ribuan port yang dapat diakses untuk berbagai keperluan;
2) Firewall komputer bertugas menutup port-port tersebut kecuali beberapa port yang perlu tetap terbuka;
3) Firewall di VoIP bertindak sebagai garis pertahanan pertama dalam mencegah semua jenis hacking;
4) Menjaga informasi rahasia dan berharga agar tidak keluar tanpa diketahui oleh pengguna;
5) Untuk memodifikasi paket data yang datang melalui Firewall.

3.1.3 Rangkuman

Dengan mengikuti kegiatan belajar ini, dapat disimpulkan bahwa untuk membangun sebuah firewall pada jaringan komputer atau VoIP perlu dibangun arsitektur jaringan yang tepat dan aturan bisnis perusahaan yang jelas. Selain itu, dari kegiatan belajar ini dapat disimpulkan hal-hal berikut:

1) Pada jaringan komputer, firewall dapat dibedakan menjadi 4 jenis menurut cara kerjanya. $ jenis firewall tersebut adalah Packet Filtering Gateway, Application Layer Gateway, Circuit Level Gateway dan Statefull Multilayer Inspection Firewall.
2) Pada jaringan VoIP, firewall dibutuhkan untuk dapat mengatasi:
    - Mengidentifikasi ancaman yang berlaku
    - Mengidentifikasi serangan dan meminimalkan peluang untuk serangan
    - Meminimalkan dampak dari serangan (jika terjadi)
    - Mengelola dan mengurangi serangan yang sukses secara tepat waktu
3) Selain itu, keamanan pada jaringan VoIP ditinjau dari arsitektur jaringannya yang mencakup segmentasi jaringan, manajemen jaringan dan private addressing.
4) Dalam hal pengendalian jaringan dengan menggunakan firewall, ada dua hal yang harus diperhatikan yaitu koneksi firewall yang digunakan (dalam hal ini yang digunakan adalah koneksi TCP), dan konsep firewall yang diterapkan, yaitu IPTables. Dengan dua hal ini diharapkan firewall dapat mengenali apakah koneksi yang ada berupa koneksi baru (NEW), koneksi yang telah ada (ESTABLISH), koneksi yang memiliki relasi dengan koneksi lainnya (RELATED) atau koneksi yang tidak valid (INVALID). Keempat macam koneksi itulah yang membuat IPTables disebut Statefull Protocol.
5) Berikut ini adalah langkah-langkah yang diperlukan dalam membangun sebuah firewall:
    a. Menentukan topologi jaringan yang akan digunakan. Topologi dan kofigurasi jaringan akan menentukan bagaimana firewall akan dibangun.
    b. Menentukan kebijakan atau policy. Kebijakan yang perlu di atur di sini adalah penentuan aturan-aturan yang akan diberlakukan.
    c. Menentukan aplikasi– aplikasi atau servis-servis apa saja yang akan berjalan. Aplikasi dan servis yang akan berjalan harus kita ketahui agar kita dapat menentukan aturan-aturan yang lebih spesifik pada firewall kita.
    d. Menentukan pengguna-pengguna mana saja yang akan dikenakan oleh satu atau lebih aturan firewall.
    e. Menerapkan kebijakan, aturan, dan prosedur dalam implementasi firewall.
    f. Sosialisasi kebijakan, aturan, dan prosedur yang sudah diterapkan. Batasi sosialisasi hanya kepada personil teknis yang diperlukan saja.

3.1.4 Tugas

Tugas

Melakukan pengamatan terhadap Firewall pada jaringan Komputer dan VoIP!

Langkah Kerja

1. Buatlah kelompok dengan anggota 3 – 4 orang.
2. Uraikan pengamatan kelompok tentang Firewall pada jaringan Komputer!
3. Uraikan pengamatan kelompok tentang Firewall pada jaringan VoIP!
4. Buat laporan dan diskusikan dengan teman sekelompok.

Bandingkan dan Simpulkan

Presentasikan hasil kerja kelompok anda di depan kelas dan bandingkan hasil kerja kelompok Anda dengan kelompok lain.

Berdasarkan hasil perbandingan tersebut hal penting apa yang harus dirumuskan secara bersama.

3.1.5 Penilaian Diri

Dalam test ini setiap anda harus membaca dengan cermat dan teliti setiap butir soal dibawah ini. Kemudian berdasarkan uraian materi diatas tulislah jawabannya pada lembar jawaban penilaian diri yang telah disediakan.

1. Tuliskan tahap-tahap konfigurasi pada sistem operasi Briker!
2. Jelaskan jenis-jenis firewall berikut:
    a. Packet Filtering Gateway
    b. Application Layer Gateway
    c. Circuit Level Gateway
3. Jelaskan maksud dari perintah berikut:

```
# iptables – A FORWARD –p tcp –dport 80 –i eth1 –j ACCEPT
# iptables – A FORWARD –p tcp –sport 80 –o eth1 –j ACCEPT
# iptables – A FORWARD –p tcp –dport 80 –i eth0 –j ACCEPT
# iptables – A FORWARD –p tcp –sport 80 –o eth0 –j ACCEPT
```

4. Jelaskan apa yang dimaksud dengan IP Masquerade

Lembar Kerja penilaian Diri

LJ- 01: Jelaskan 3 macam proses yang terjadi pada Firewall

……
……
……
……
……

LJ- 02.a: Jelaskan yang dimaksud dengan Extension!

……
……
……
……
……
……
……

LJ- 02.b: Jelaskan yang dimaksud dengan Trunk!

……
……
……
……
……
……
……

LJ- 02.c: Jelaskan yang dimaksud dengan Dial Plan!

……
……
……
……
……
……

LJ- 03: Berikan penjelasan bagaimanakah keterkaitan antara IP-PBX dengan Sistem Operasi Briker!

……
……
……
……
……
……
……

LJ- 04: Tuliskan beberapa hal yang wajib harus didaftarkan dalam membuat account VoIP!

……

……

……

……

……

……

BAB IV

4.1 Kegiatan Belajar 4: Prinsip Kerja Subcriber Internet Telepon

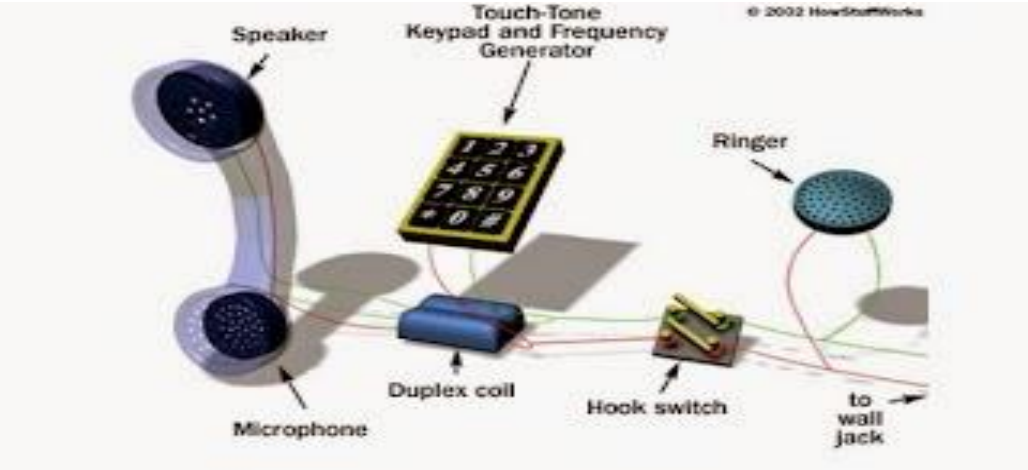
4.1.1 Tujuan Pembelajaran

Setelah mempelajari kegiatan belajar 4 ini, diharapkan siswa dapat:

1) Memahami prinsip kerja subscriber internet telepon
2) Menalar prinsip kerja subscriber internet telepon

4.1.2 Aktifitas Belajar Siswa

4.1.2.1 Mengamati/Observasi

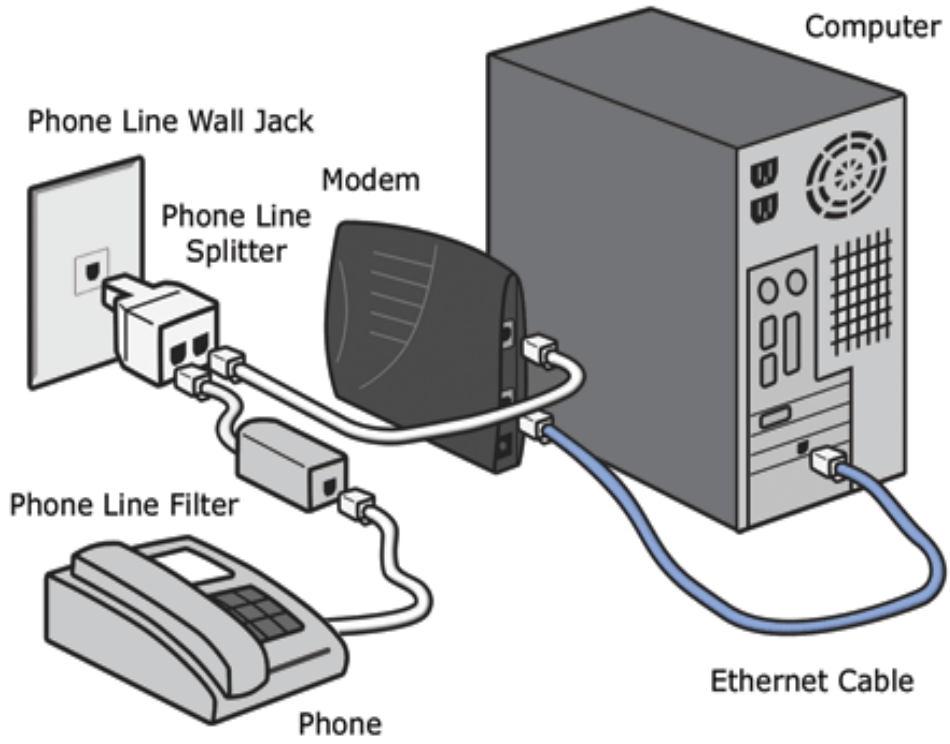


Sumber : Dokumen Kemendikbud

Gambar 4.1 Contoh Koneksi Telepon

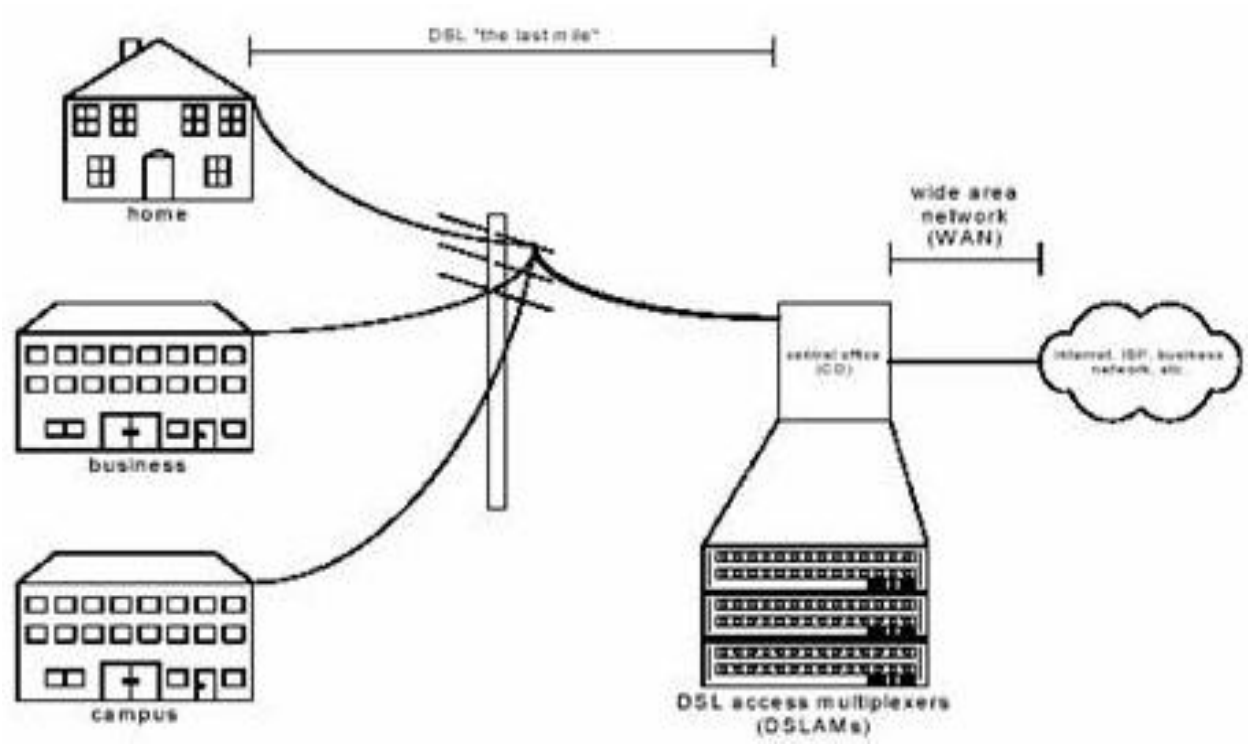
Sumber : http://inginberbagiilmu.blogspot.com/2009/01/cara-seting-koneksi-internet-dengan.html

Gambar 4.2 Contoh Telepon dengan Modem



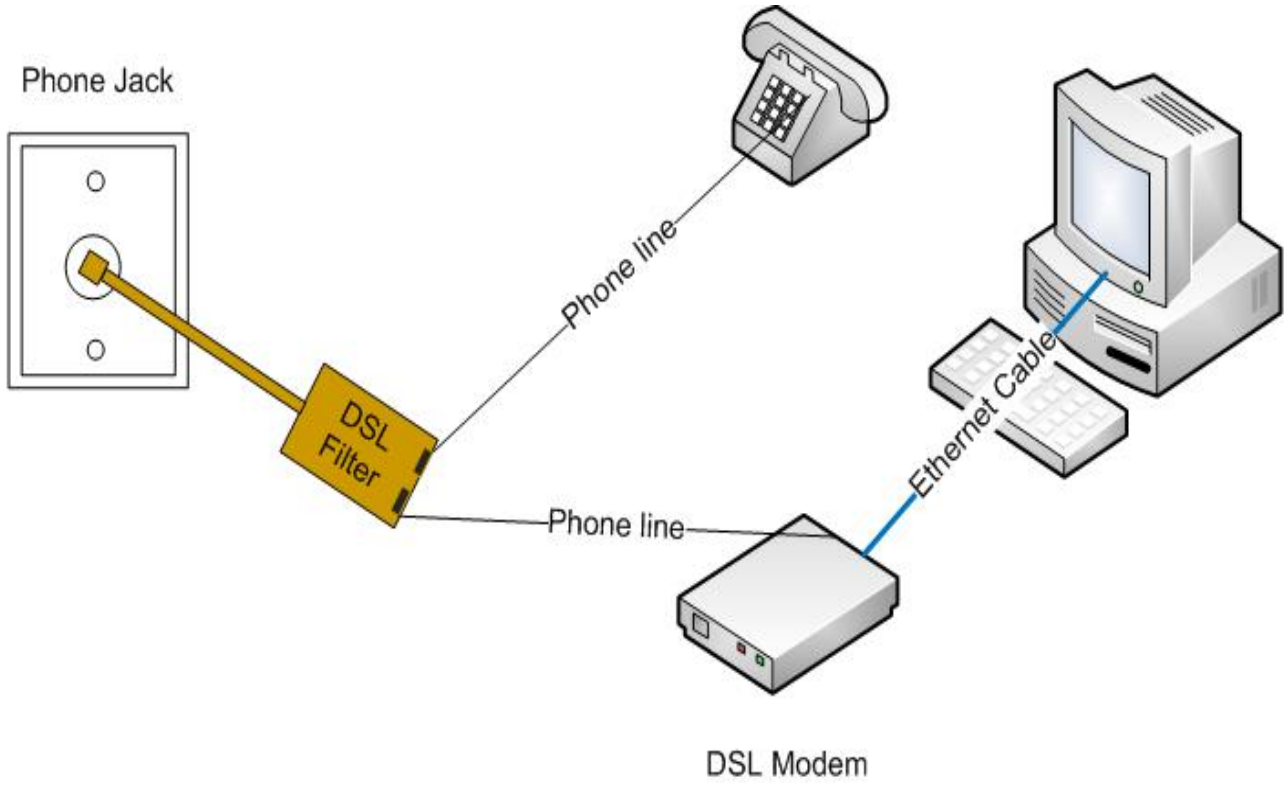
Sumber : http://www.cio.com/article/2371202/internet/dsl-connection-too-slow--here-s-how-to-speed-it-up.html

Gambar 4.3 Arsitektur dan Komponen Internet Telepon



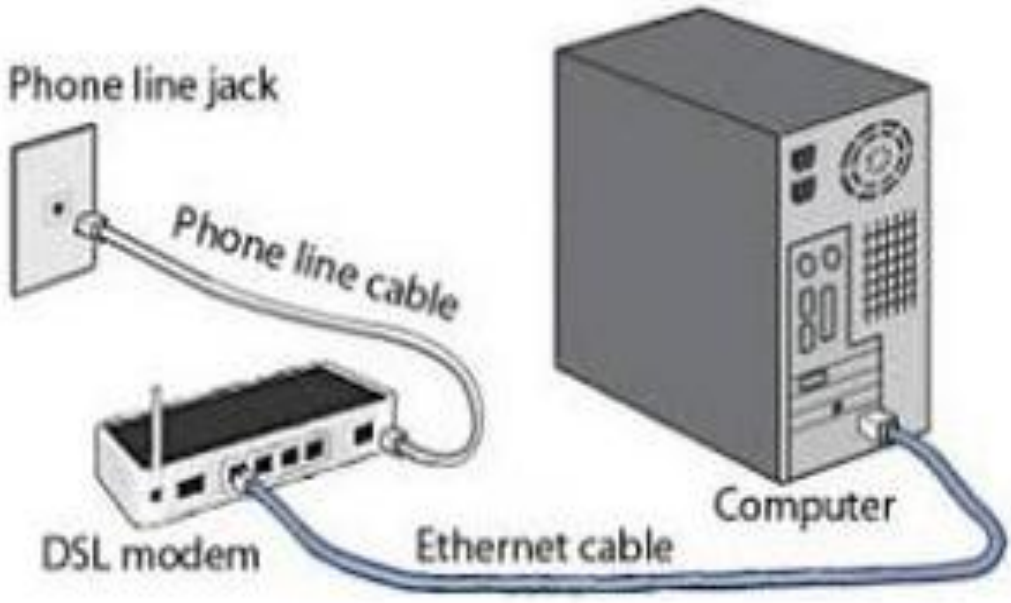
Sumber : http://sinauonline.50webs.com/Artikel/DSL.html

Gambar 4.4 Konfigurasi DSL Sistem



Sumber : http://tranquility.net/2012/standard-dsl-setup/

Gambar 4.5 Standar Pengaturan DSL



Sumber : http://www.lostintechnology.com/internet-tools/dsl-mean/

Gambar 4.6 Koneksi Modem DSL dengan Komputer

Sumber : http://www.lostintechnology.com/internet-tools/dsl-mean/

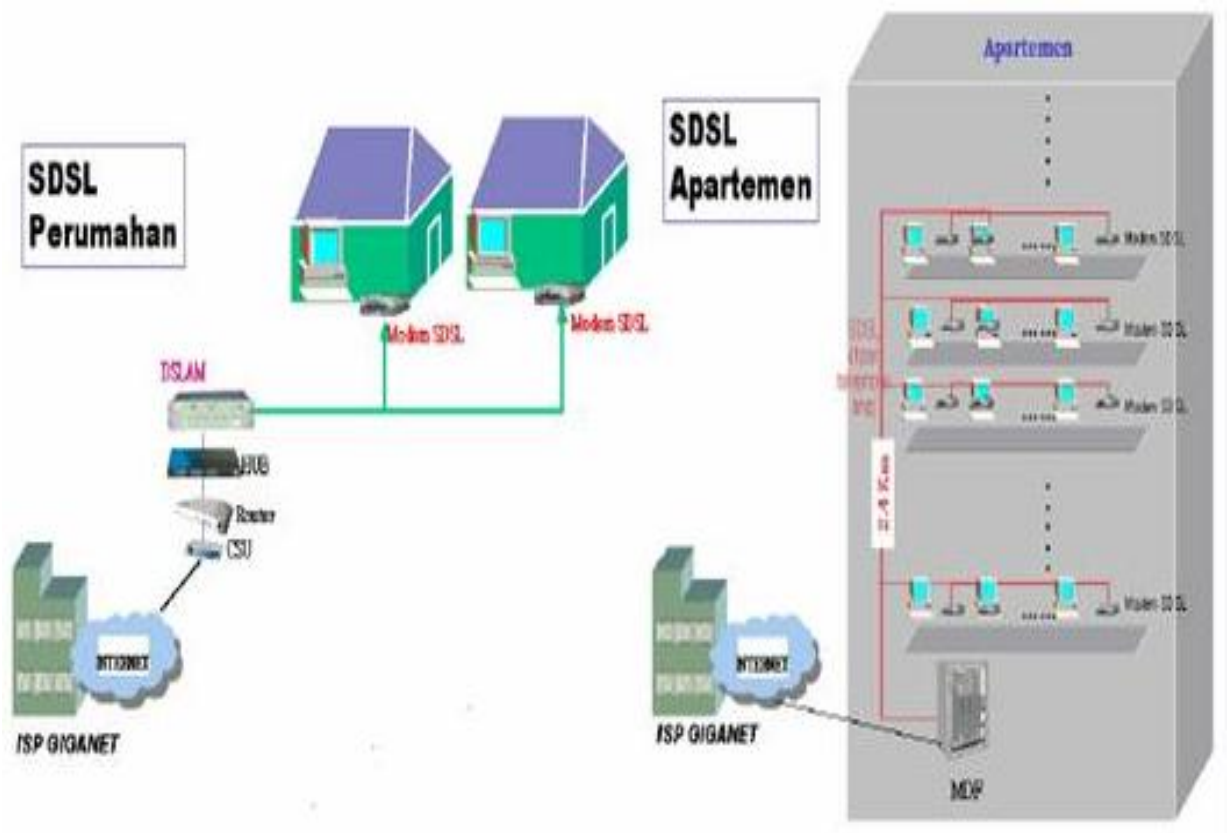
Gambar 4.7 Contoh Router DSL

Sumber : Dokumen Kemendikbud

Gambar 4.8 Contoh 1 Modem SDSL

Sumber : Dokumen Kemendikbud

gambar 4.9 Contoh 2 Modem SDSL

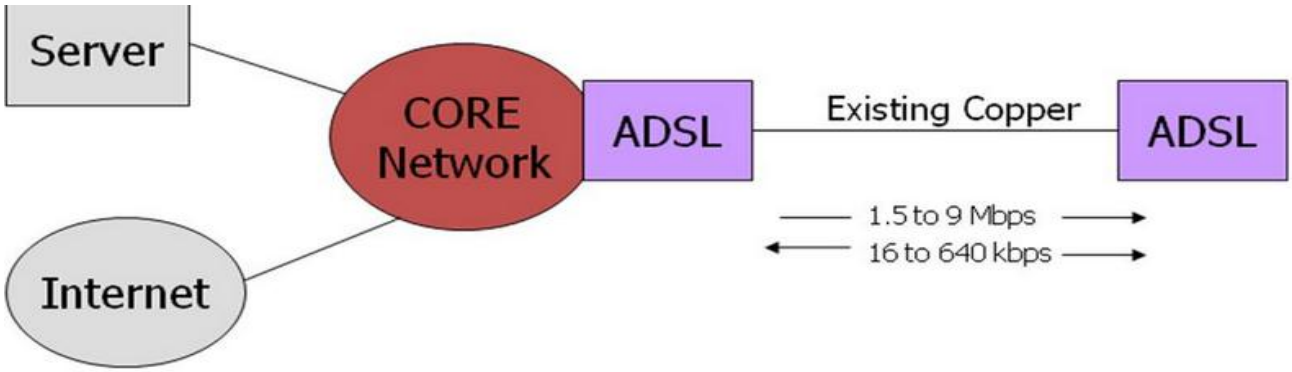


sumber : http://sinauonline.50webs.com/Artikel/DSL.html

gambar 4.10 Konfigurasi Koneksi SDSL

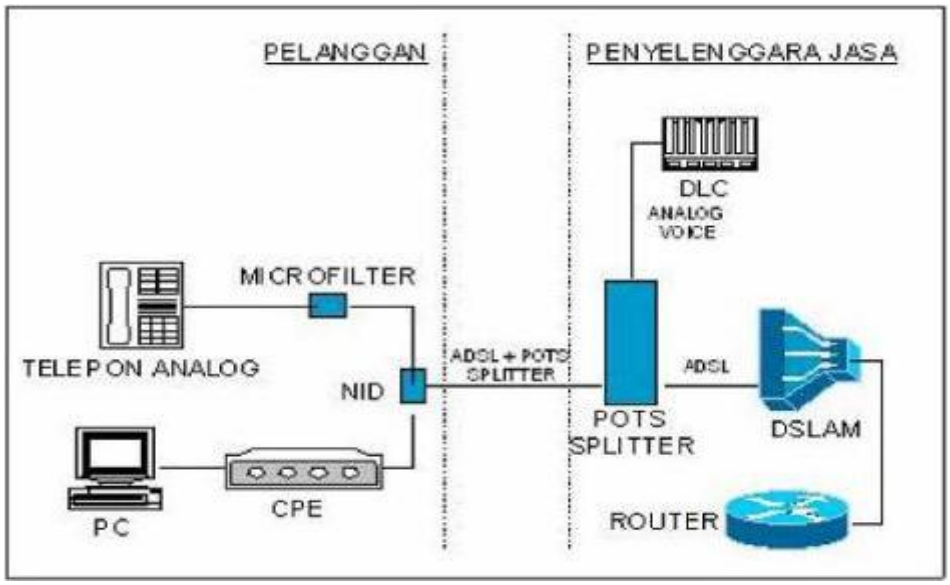
Sumber : http://www.asus.com/Networking/DSLN55U_Annex_A/

Gambar 4.11 Contoh Modem ADSL dengan dilengkapi Router Wifi dari produk ASUS.



Sumber : http://lecturer.eepis-its.edu/~nonot/KuliahTelefoni/ADSL.ppt

Gambar 4.12 Koneksi ADSL

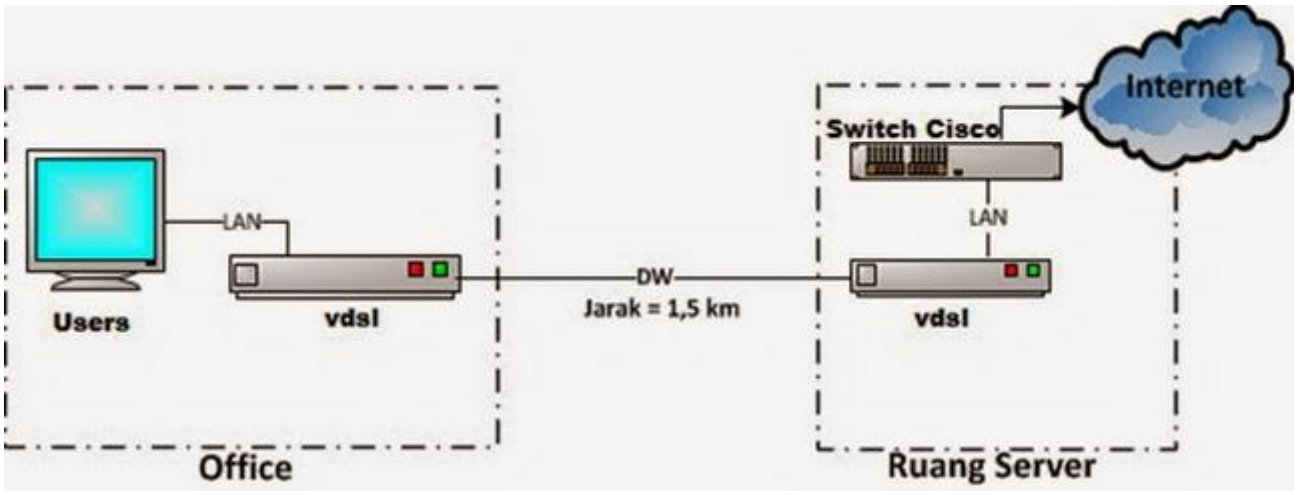


Sumber : http://i-networking.net/wp-content/uploads/2007/07/adsl.pdf

Gambar 4.13 Konfigurasi Umum ADSL

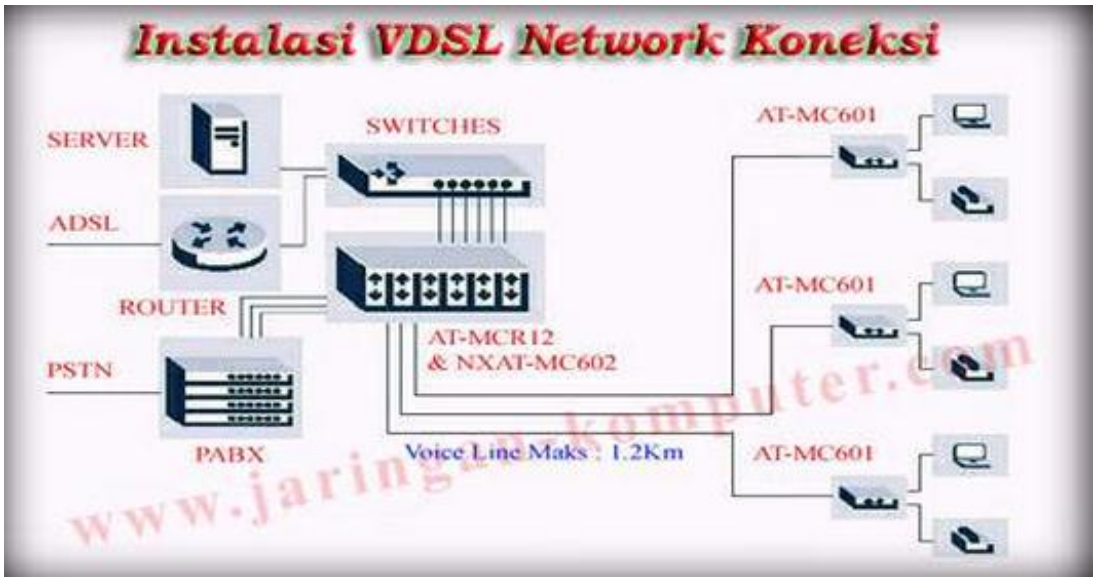
Sumber : http://en.wikipedia.org/wiki/Very-high-bit-rate_digital_subscriber_line#mediaviewer/File:VDSL_Modem.jpg

Gambar 4.14 Contoh Modem VDSL



Sumber : http://myconfigure.blogspot.com/2014/05/konfigurasi-modem-zyxel-sebagai-bridge.html

Gambar 4.15 Konfigurasi Jaringan Modem VDSL Zyxel

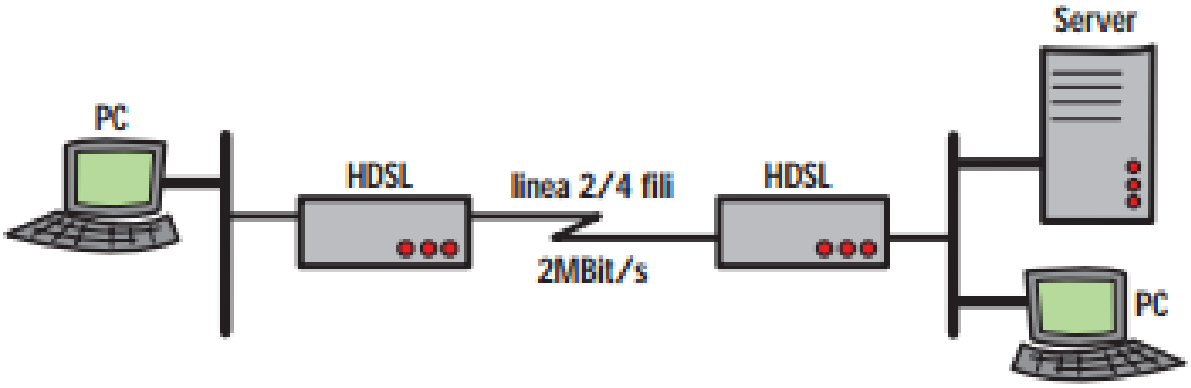


Sumber : www.jaringan-komputer.com

Gambar 4.16 Instalasi Koneksi Jaringan VDSL

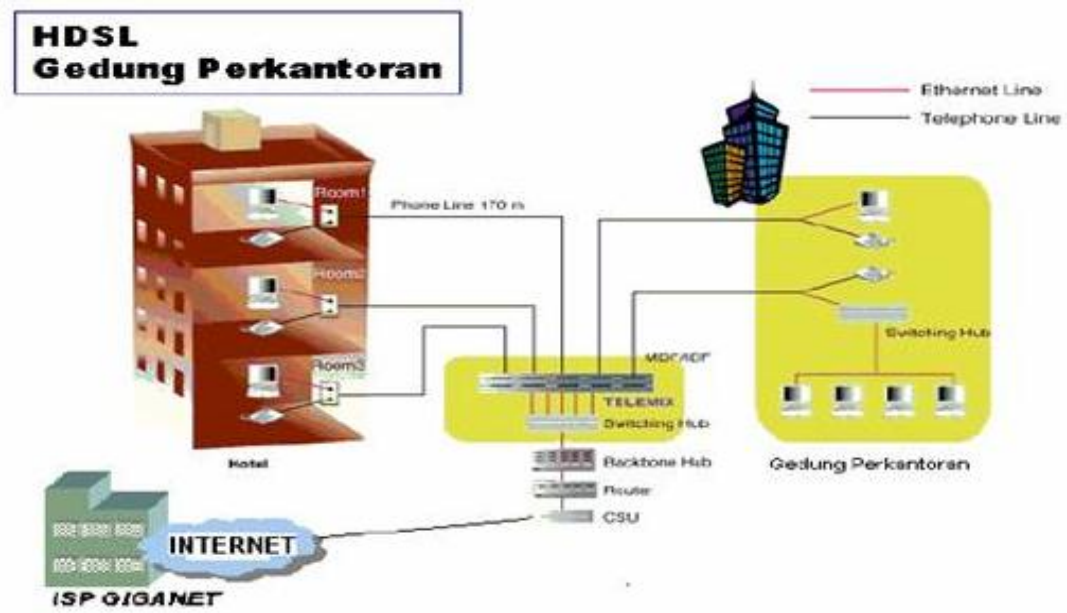
Sumber : http://www.digicom.it/digisit/pdffiles.nsf/ENDepPdfIDX/ModemHDSL2m/$file/ModemHDSL2m.pdf

Gambar 4.17 Contoh Modem HDSL



Sumber : http://www.digicom.it/digisit/pdffiles.nsf/ENDepPdfIDX/ModemHDSL2m/$file/ModemHDSL2m.pdf

Gambar 4.18 Konfigurasi Umum HDSL



Sumber : http://sinauonline.50webs.com/Artikel/DSL.html

Gambar 4.19 Contoh Konfigurasi Jaringan HDSL

4.1.2.2 Menanya

Dari tayangan gambar pada bagian 4.1.2.1 Mengamati/Observasi, menurut anda :

1) Apakah yang dimaksud dengan subscriber internet telepon?
2) Bagaimanakah prinsip kerja subscriber internet telepon?

4.1.2.3 Mencoba/Mengumpulkan Informasi

Perkembangan internet yang sangat cepat sejak adanya World Wide Web tidak saja membawa perubahan terhadap penyebaran informasi tetapi juga membawa perubahan terhadap infrastruktur telekomunikasi. Tetapi kecepatan pertambahan jumlah pengguna internet serta jumlah aliran data (informasi) lebih cepat dibandingkan dengan perkembangan infrastruktur telekomunikasi. Dengan semakin banyaknya informasi dan data yang akan diakses apalagi dengan

bentuk multimedia semakin memunculkan tuntutan akan kecepatan akses data dan informsi tersebut. Bagi suatu perusahaan kecepatan akan komunikasi data yang tinggi sangat diperlukan untuk implementasi pada aplikasi multimedia real-time seperti konferensi video, hubungan dengan kantor cabang, dan jasa layanan informasi lainnya. Untuk mendapatkan kualitas yang lebih baik maka ditawarkanlah solusi dengan ISDN (*Integrated Service Digital Network*). Dengan teknologi digital kecepatan pengiriman data dapat dilakukan sampai dengan 64kbps untuk setiap kanal, karena basic ISDN dapat menyediakan dua kanal maka secara keseluruhan bisa didapatkan kecepatan akses sampai 128kbps. Akan tetapi kendala utama dari teknologi ISDN ini adalah diperlukannya jaringan telekomunikasi baru. Sehingga tidak semua orang dapat menikmati keunggulan teknologi ini. Di Indonesia terdapat layanan jasa telekomunikasi yang menggunakan teknologi ini, yaitu pasopati tetapi layanan jasa ini baru terbatas di bebrapa kota besar. Banyak ragam yang digunakan oleh operator telekomunikasi untuk memberikan layanan broadband akses ke pelanggan. Dari sisi media yang digunakan dapat dibedakan menjadi dua yaitu teknologi wireline (kabel) dan teknologi wireless (tanpa kabel). Dari kategori teknologi wireline dapat digunakan teknologi DSL (Digital Subscriber Line), kabel modem, HFC ,maupun optik. Sedangkan dari kategori wireless dapat memanfaatkan teknologi wireless LAN, BWA (Broadband Wireless Access) maupun teknologi terbaru WiMAX (Worldwide Interoperability for Microwave Access).

Dengan berbagai solusi di atas, sebagian operator memanfaatkan teknologi DSL (kabel) dan BWA (untukwireless). Bagi operator telekomunikasi yang incumbent di suatu negara, contoh TELKOM untuk Indonesia dimana telah menggelar kabel sekitar 6 juta line maka akan memanfaatkan teknologi DSL guna meng-enhanced jaringan fisiknya untuk menyalurkan data kecepatan tinggi ke pelanggan. Sedangkan bagi operator baru tentunya sangat sulit dan mahal bila menggelar jaringan broadband dengan DSL. Alternatifnya memanfaatkan teknologi wireless (BWA). Dengan lahirnya teknologi wireless terbaru (WiMAX) maka dapat dijadikan sebagai pengganti atau alternatif untuk menyalurkan layanan broadband ke pelanggan.

Bila dilihat dari segmen pasarnya, maka antara WiMAX dan DSL memiliki kesamaan yaitu sama-sama ditujukan untuk MAN (Metro Area Network) dimana jarak ke pelanggan sekitar 10 km. Kemudian muncul pemikiran untuk tetap menggunakan infrastruktur yang ada guna membangun sambungan kecepatan tinggi, ini didasari dengan mahalnya investasi baru dan besarnya permintaan kebutuhan akan akses yang cepat. Salah satu solusinya adalah dengan teknologi DSL (Digital Subscriber Line) yang merupakan teknologi baru.

4.1.2.3.1 Konsep dasar DSL

Digital Subscriber Line (DSL) merupakan teknologi modem yang menggunakan jalur

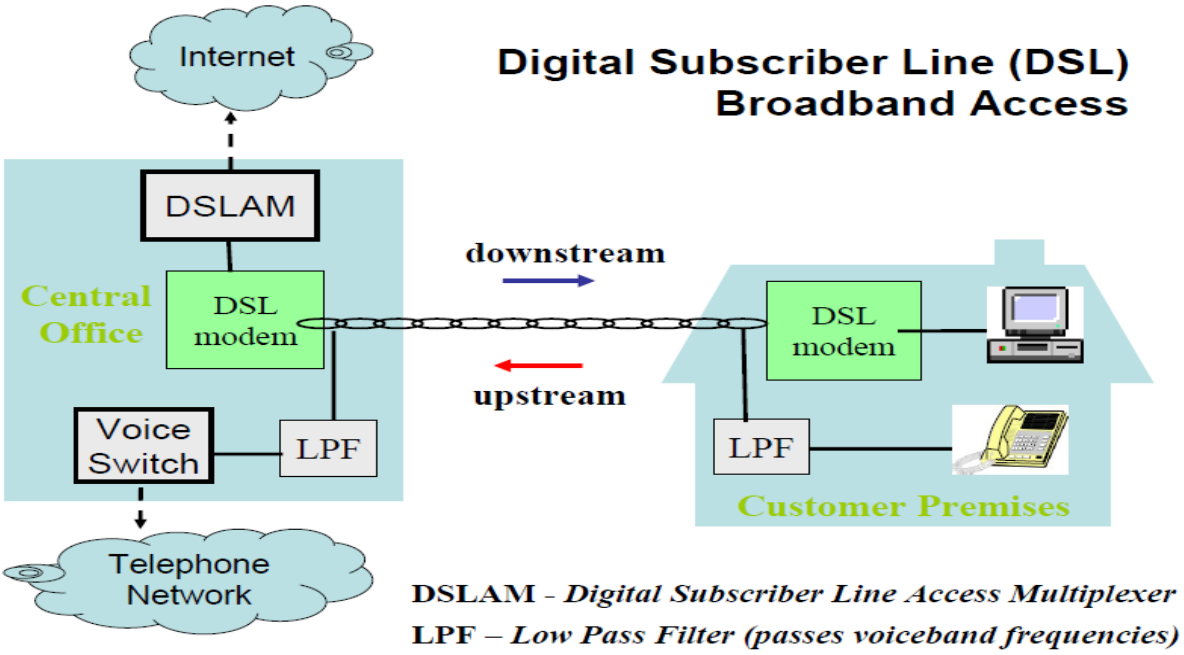
telepon yang sudah ada untuk menyalurkan data dengan bandwidth lebar, seperti multimedia dan video. Teknologi ini memerlukan perangkat khusus pada *central office* dan pelanggan yang memungkinkan transmisi broadband melalui kabel tembaga. Hal ini sering disebut juga dengan istilah teknologi suntikan atau *injection technology*. Dengan teknologi suntikan ini kabel telepon biasa yang telah ada dapat digunakan untuk menghantar data dalam jumlah yang besar dan dengan kecepatan yang tinggi. Jika PSTN hanya menggunakan sebagian frekuensi yang mampu dihantarkan oleh kabel tembaga, DSL memanfaatkan lebih banyak frekuensi dengan membaginya (*splitting),* frekuensi yang lebih tinggi untuk data dan frekuensi yang lebih rendah untuk suara dan fax. Jarak pemakai ke CO menentukan kecepatan DSL. Makin jauh jarak pemakai, kecepatan makin rendah. Contoh operator yang menggelar DSL di Indonesia adalah PT. Telkom dengan produk yang diberi nama **SPEEDY**.

Dilihat dari sisi teknis teknologi DSL menggunakan basis data paket sementara komunikasi suara berbasis sambungan (circuit-switch). Untuk komunikasi data yang berbasis sambungan , sambungan dengan lebar bandwith tertentu harus tetap dipertahankan walaupun tidak ada data yang lewat. Untuk komunikasi suara yang singkat waktu yang tidak terpakai tidak begitu menimbulkan masalah, tetapi untuk komunikasi data yang lama akan memboroskan sumber daya yang dimiliki oleh PSTN. Sementara komunikasi data yang berbasis paket akan memungkinkan penggunaan bandwith yang optimum, karena bisa dimanfaatkan untuk lebih dari satu sambungan secara efisien dan ekonomis. Teknologi DSL yang menggunakan kabel tembaga, membawa kedua sinyal analog serta digital pada satu kabel. Sinyal digital untuk komunikasi data sementara sinyal analog untuk suara sperti halanya yang digunakn telepon sekarang yang disebut sebagai POTS (Plain Old Telephone System). Kemampuan untuk memisahkan sinyal suara dan data ini adalah merupakan suatu keuntungan. DSL akan mengkoneksikan dan membawa sinyal digital untuk komunikasi data dan bekerja dengan menggunakan modem khusus (disebut modem DSL) untuk membaca (encode) data tersebut dan kemudian mengirimkannya melalui frekuensi yang tidak terpakai pada kabel telepon tersebut. DSL menjadi penting dan menjadi pilihan, pada saat pengguna mulai mencari kecepatan akses untuk koneksi internet. Tanpa harus pusing dan bosan menunggu bermenit-menit hanya untuk membuka satu halaman internet apalagi dapat menikmati layanan multimedia melalui internet, seperti menyaksikan layanan video, konferensi melalui video (kamera) atau layanan online lainnya dan harganya bisa murah Jaringan PSTN (Public Switch Telephone Network) yang ada dirancang untuk komunikasi suara yang hanya berlngsung sebentar sekitar tiga sampai lima menit.

Karena hal ini maka sambungan yang sama bisa digunakan secara bergantian sehingga tidak diperlukan penyedian

sambungan telepon yang sama banyak denga jumlah saluran teleponnya. Tetapi untuk komunikasi data umumnya para pelanggan menggunakan waktu yang leih lama, terutama dengan adanya intrenet, maka akibatnya tingkat keberhasilan penyambungan mengalami penurunan karena sebagian besar saluran telepon terpakai dalam jangka waktu yang lama. Perkembangan lalu lintas data yang sangat cepat ini akan membebani jaringan telepon publik (PSTN) yang ada. Ada dua pilihan yang bisa diambil penyelenggara jasa telekomunikasi untuk mengatasi hal ini yang pertama adalah meningkatkan jaringan PSTN untuk menangani permintaan komunikaais data dan suara yang bertambah dan yang kedua memindahkan lalu litas data ke jaringan yang terpisah yang dirancang khusus untuk komunikasi data. Dilihat dari sisi teknis teknologi DSL menggunakan basis data paket sementara komunikasi suara berbasis sambungan (circuit-switch).

Untuk komunikasi data yang berbasis sambungan, sambungan dengan lebar bandwith tertentu harus tetap dipertahankan walaupun tidak ada data yang lewat. Untuk komunikasi suara yang singkat waktu yang tidak terpakai tidak begitu menimbulkan masalah, tetapi untuk komunikasi data yang lama akan memboroskan sumber daya yang dimiliki oleh PSTN. Sementara komunikasi data yang berbasis paket akan memungkinkan penggunaan bandwith yang optimum, karena bisa dimanfaatkan untuk lebih dari satu sambungan secar efisien dan ekonomis. Yang juga merupakan kelebihan lain dari teknologi DSL adalah pengguanan kabel tembaga yang sudah ada dimana jaringannya sudah mencapai kantor-kantor dan rumah-rumah sehingga pembangunan infrastruktur yang diperlukan menjadi tidak terlalu mahal. Tetapi penggunaan kabel yang sudah ada ini harus memperhatikan beberapa hal yang berhubungan dengan sinyal data. Seperti atenuasi, crosstalk, dan derau (noise). Atenuasi adalah melemahnya sinyal yang diakibatkan oleh adanya jarak yang semakin jauh yang harus ditempuh oleh suatu sinyal dan juga oleh karena makin tingginya frekuensi sinyal tersebut. Karena faktor jarak dan frekuensi ini maka jarak terjauh yang masih mungkin adalah sekitar 5,5 km dengan bandwith sekitar 1 MHz. Crosstalk akan mungkin dtimbulkan oleh adanya pasangan kabel telepon yang digunakan. Gangguan ini bisa timbul karena sinyal dengan kecepatan yang sama dari masing-masing kabel bisa saling mempengaruhi, bila gangguan ini lebih tinggi dibandingkan dengan sinyal data maka akan timbul banyak error yang memperlambat kecepatan aliran data. Untuk menghindari efek crosstalk dapat dibuat untuk setiap kabel satu arah, sehingga sinyal pada masing-masing kabel tidak saling mempengaruhi. Gambaran konfigurasi umum untuk DSL dapat dilihat pada gambar 4.4 pada bagian Mengamati/Observasi Pada gambar berikut ini dapat dilihat ilustrasi akses broadband dari DSL.

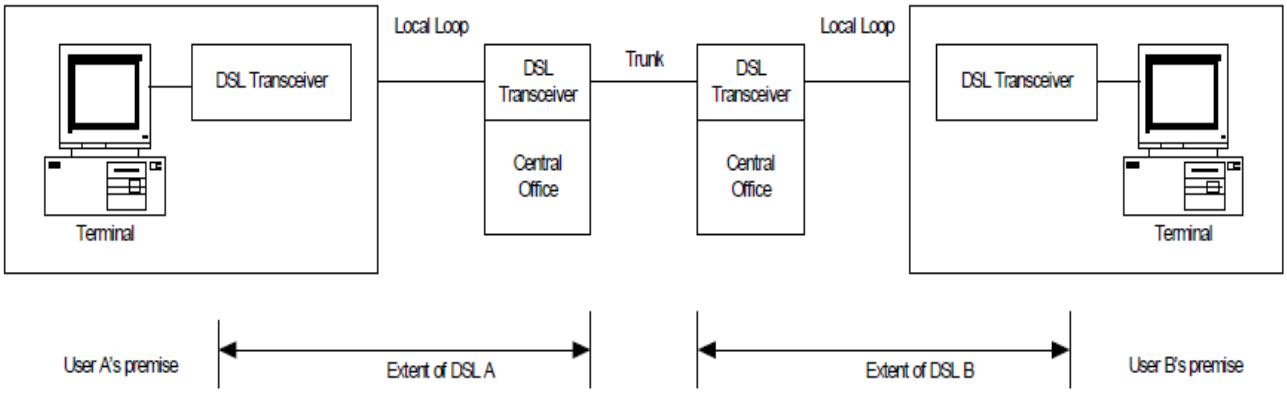


Sumber : Dokumen Kemendikbud

Gambar 4.20 Akses Broadband dari DSL

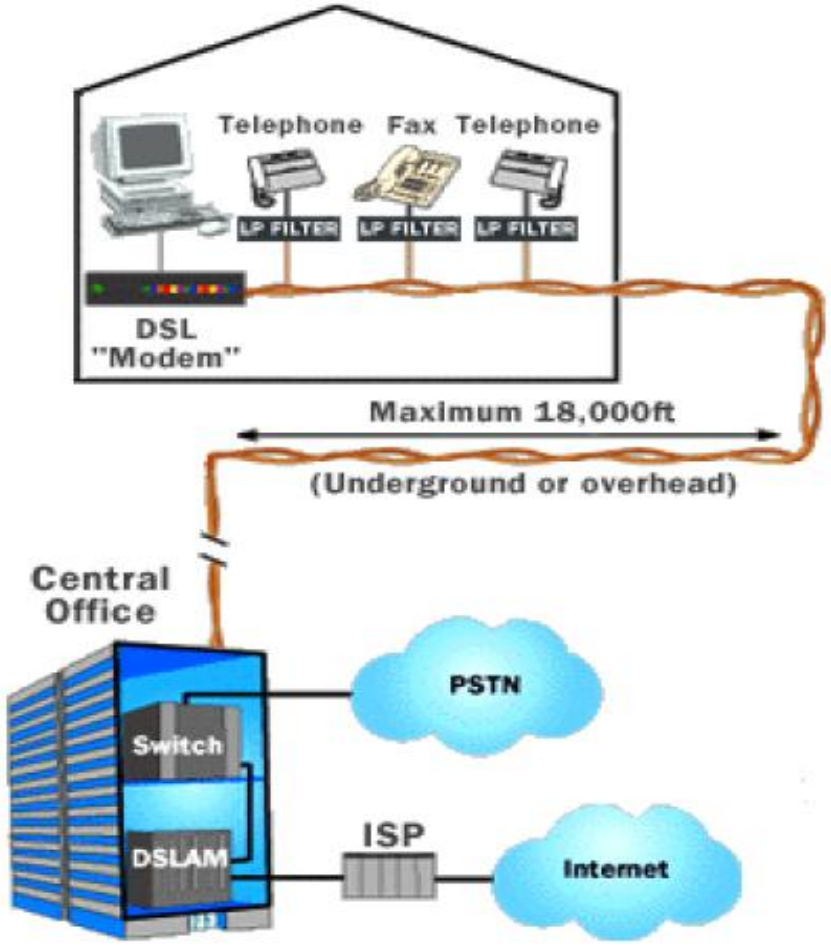
4.1.2.3.2 Komponen Sistem DSL

Digital Subscriber Line (DSL) memiliki 3 komponen penting. Komponen tersebut adalah DSL Transceiver, Filter dan DSLAM (*Digital Subscriber Line Access Multiplexer*).



Sumber : Dokumen Kemendikbud

Gambar 4.21 Blok Diagram Sistem DSL antara 2 central dan 2 user

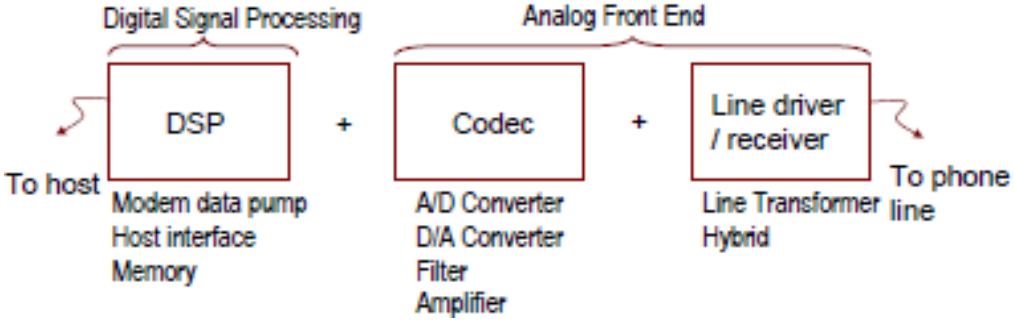


Sumber : How Stuff Works (2001)

Gambar 4.22 Komponen Sistem DSL (dari end-user sampai Central Telepon)

1. DSL Transceiver

DSL Transceiver terdiri dari *High Pass Filter* (HPF) dan *Low Pass Filter* (LPF) yang berfungsi memisahkan band-band suara (voice band) dengan band frekuensi yang lebih tinggi. Band suara ditransmisikan ke jalur telepon pelanggan, sedangkan band frekuensi yang lebih tinggi, digunakan untuk kecepatan data tinggi antar PC.



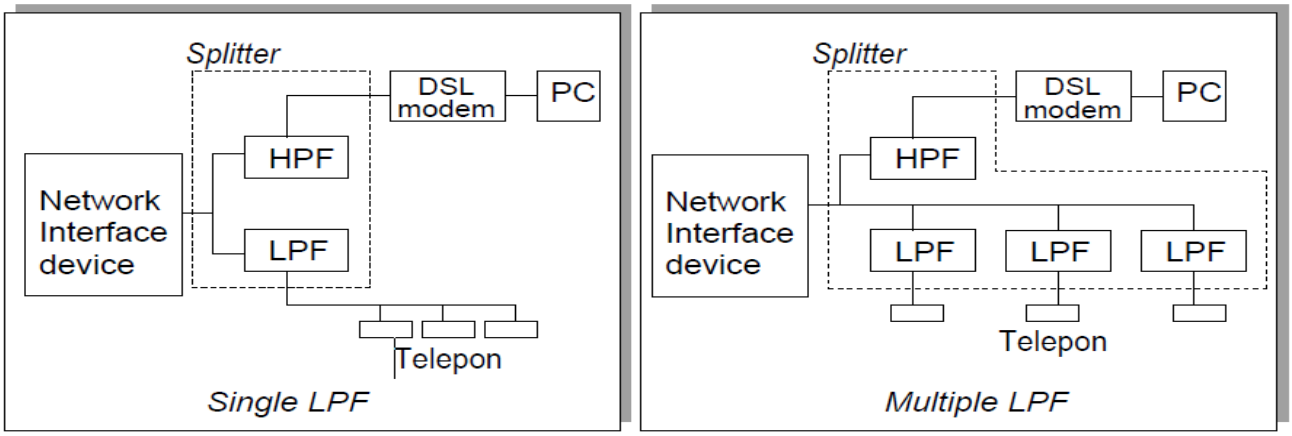
Sumber : Dokumen Kemendikbud

Gambar 4.23 Konsep Subsistem DSP dan AFE dalam Sistem DSL

2. Filter

Filter digunakan untuk memisahkan jalur data dan jalur suara. Biasanya disediakan oleh

ISP satu paket dengan DSL Modem.



Sumber : Dokumen Kemendikbud

Gambar 4.24 Pengaturan Filter di sisi User

3. DSLAM

DSLAM diletakkan di sentral telepon. DSLAM berfungsi menerima sinyal dari banyak pelanggan DSL / Sambungan Telepon, dan meneruskan ke backbone berkecepatan tinggi, menggunakan teknik *multiplexing.* Sesuai dengan spesifikasi produk dari vendor yang membuatnya. DSLAM terhubung dengan line DSL dengan kombinasi *Asynchronous Transfer Mode* (ATM), *Frame Relay* atau *Internet Protocol* (IP).

Sumber : Dokumen Kemendikbud

Gambar 4.25 DSLAM dan Komponennya

Fungsi DSLAM antara lain:

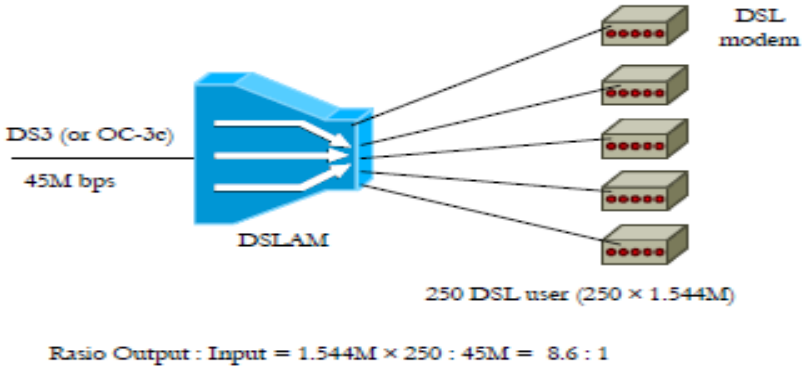
- Sebagai filter *voice* dan data
- Sebagai modulator dan demodulator DSL
- Sebagai *multiplexer*

Cara Kerja DSLAM adalah sebagai berikut:

1) DSLAM memisahkan frekuensi sinyal suara dari trafik kecepatan tinggi, serta mengontrol dan merutekan trafik Digital Subcriber line (xDSL) antara perangkat end-user, seperti router, modem, network interface card, dengan jaringan penyedia layanan.
2) DSLAM menyalurkan data digital memasuki jaringan suara PSTN ketika mencapai di CO (Central office).
3) DSLAM mengalihkan kanal suara (biasanya dengan menggunakan

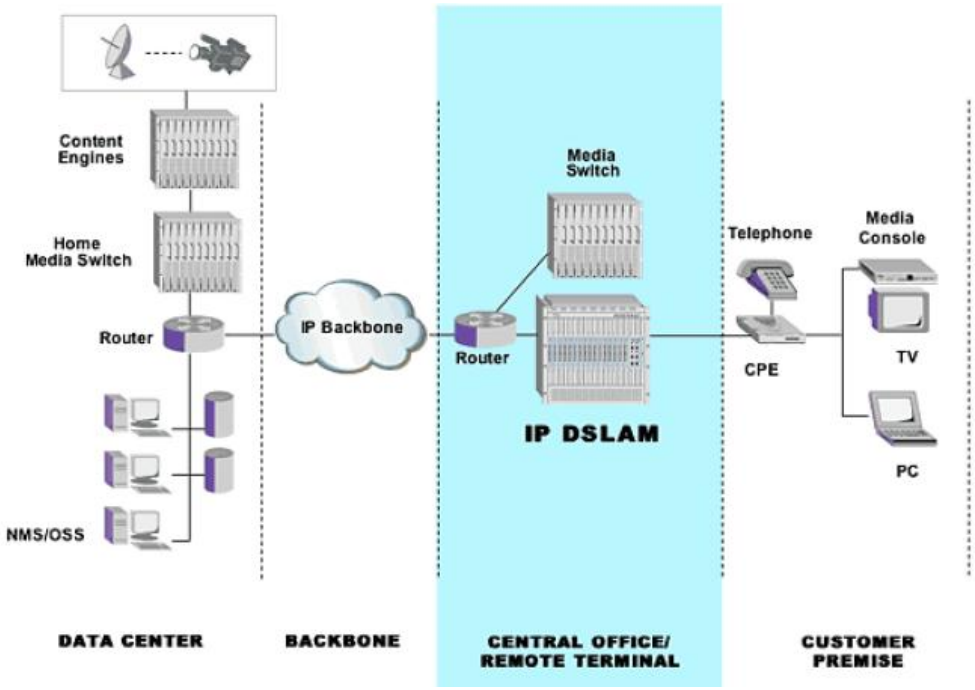
splitter) sehingga sinyal tersebut dapat dikirim melalui PSTN, dan kanal data yang sudah ada kemudian ditransmisikan melalui DSLAM yang sebenarnya adalah kumpulan modem DSL3.

4) Setelah menghilangkan sinyal suara analog, DSLAM mengumpulkan sinyal-sinyal yang berasal dari end-user dan menyatukannya menjadi sinyal tunggal dengan bandwidth yang lebar, melalui proses multiplexing.
5) Sinyal yang sudah disatukan ini disalurkan dengan kecepatan Mbps kedalam kanal oleh peralatan switching backbone melalui Network Service Provider (NSP).
6) Sinyal yang dikirimkan melalui internet atau jaringan lain muncul kembali pada CO yang dituju, dimanan DSLAM yang lain menunggu.
7) DSLAM bersifat fleksibel dan bisa mendukung berbagai macam DSL yang terdapat dalam sebuah CO, dan juga bisa mendukung berbagai protokol dan modulasi, seperti modulasi CAP dan DMT
8) DSLAM juga menyediakan routing maupun penomoran IP secara dinamik untuk pelanggan (end-user)
9) Jika tidak tersedia tempat di dalam MDF atau ternyata jarak antara sentral dan pelanggan terlalu jauh, solusinya adalah dengan menggunakan mini DSLAM. Mini DSLAM ini dapat diletakkan pada RK yang terdapat diantara CO dan pelanggan.



Sumber : Dokumen Kemendikbud

Gambar 4.26 Rasio Kecepatan Data sebelum dan sesudah melalui DSLAM



Sumber : Dokumen Kemendikbud

Gambar 4.27 Posisi DSLAM di Central Office

1.1.1.1.1 Jenis-jenis DSL

Teknologi DSL adalah teknologi akses yang menggunakan perangkat khusus pada central office dan pelanggan yang memungkinkan transmisi. Macam-macam teknologi DSL antara lain :

1. Symmetric Digital Subscriber Line (SDSL)
   SDSL sangat cocok digunakan untuk mengakses internet kecepatan tinggi karena memberikan kecepatan atau lebar pita sampai 2,3 Mbps dan diberikan secara simetris. Teknologi ini menggunakan kecepatan data 784 kbps, baik untuk kirim (uplink) atau terima (downlink). SDSL hanya menawarkan komunikaais data saja. SDSL merupakan solusi yang cocok untuk kalangan bisnis untuk digunakan sebagai komunikasi antar cabang atau hubungan situs web ke internet. SDSL sangat cocok digunakan untuk mengakses internet kecepatan tinggi untuk perumahan karena memberikan kecepatan atau lebar pita sampai 2.3 Mbps dan diberikan secara simetris, dengan jarak maksimum sampai 2.4 Km. Sangat cocok untuk akses LAN jarak jauh (remote LAN), layanan VOD (Video On Demand), residential video converencing dan lain-lain. Adapun contoh koneksi SDSL dapat dilihat pada gambar 4.10 pada bagian Mengamati/Observasi.
2. Asymmetric Digital Subscriber Line (ADSL)
   Teknologi ADSL adalah teknologi akses dengan perangkat khusus pada sentral dan pelangan yang memungkinkan transmisi broadband melalui satu pair kabel. Teknologi ini mempunyai kecepatan data yang berbeda untuk kirim (uplink) dan terima (downlink).Teknologi ADSL cocok digunakan untuk mengakses internet dan menjadi pilihan pengguna.

Untuk uplink bisa mencapai 8 Mbps sementara untuk downlink bisa mencapai 1 Mbps dengan jarak kabel maksimum samapi dengan 5,5 km. Sasaran teknologi ini adalah terutama pelanggan pribadi yang lebih banyak menerima data daripada mengirim data, sebagai contoh adalah untuk mengakses internet. Kelebihan ADSL dibanding yang lain adalah kecepatannya yang tertinggi dengan jarak yang memadai dan bisa mendukung layanan komunikasi suara. Kedua layanan komunikasi data dan suara diberikan melalui dua kanal yang terpisah , tetapi tetap satu kabel yang sama. Sementara teknologi DSL yang lain menggunakan dua kabel yang terpisah untuk bisa memberikan kedua layanan komunikasi tersebut.

Karena berbagai kelebihan yang dimiliki oleh teknologi ADSL ini maka teknologi ini berkembang sangat cepat. Pengiriman data melalui ADSL dilakukan dengan beberapa tahap. Modem memodulasi dan mengkodekan (encode) data digital dari PC dan kemudian digabungkan dengan sinyal telepon untuk dikirimkan ke kantor telepon. Di kantor telepon sinyal telepon dipisahkan dari sinyal digital ADSL untuk kemudian dimodulasikan dan di-encode. Melalui jaringan komunikasi data sinyal ini dikirimkan ke pihak yang dituju, seperti ISP atau kantor lain . jaringan data yang digunakan ini tergantung dari penyelenggara jasa ASDL, bisa frame relay atau ATM (Asynchronous Transfer Mode).

Sementara sinyal digital dari ISP atau jaringan perusahaan lain dimodulasi dan di-encode menjadi sinyal ASDL di kantor telepon. Kemudian modem menggabungkan nya dengan sinyal telepon sebelum dikirimkan ke pelanggan, perangkat pemisah (splitter) memisahkan sinyal telepon dari sinyal digital. Sinyal digital dimodulasi dan di-decode kemudian dikirimkan ke PC. Sinyal telepon yang digabungkan dengan sinyal ASDL dalam satu kabel tetap di beri daya oleh perusahaan telepon. Meskipun jalur ADSL tidak berfungsi atau PC tidak dihidupkan jalur telepon tetap dapat berfungsi seperti biasa. Terdapat dua teknik modulasi berbeda yang diterapkan pada ADSL. Teknik modulasi yang pertama adalah menerapkan teknik modulasi CAP (Carierless Amplitude and Phase). CAP menggabungkan sinyal data upstream dan downstream, kemudian memisahkannya pada modem penerima dengan teknik echo cancellation. Teknik modulasi yang lain adalah DMT (Discrete Multitone), yang memisahkan sinyal upstream dari sinyal downstream dengan pita pembawa (carrier band) yang terpisah. Di masa yang akan datang produk-produk ADSL akan menggunakn teknik modulasi DMT.

3. High Bit Rate Subscriber Line (HDSL)
   HDSL merupakan teknologi aplikasi pada jaringan local tembaga untuk menyalurkan layanan 2 Mbps. HDSL sangat cocok digunakan untuk gedung-gedung perkantoran atau kompleks perkantoran, karena memberikan

kecepatan atau lebar data sampai 10 Mbps dan dapat dibagi-bagi kepada seluruh pengguna akhir. Infrastruktur yang dibutuhkan untuk koneksi HDSL ini dapat menggunakan jalur PBX yang dimiliki gedung, tanpa harus menginvestasi pembangunan jaringan komputer. Jarak maksimum cukup panjang mencapai 1 Km. HDSL memakai dua pasang twisted cable yang akan membawa data dengan kecepatan 1,544Mbps upstream (dari pelanggan ke jaringan) dan downstream (dari jaringan ke pelanggan). Selain itu teknologi HDSL juga juga menggunakan tiga pasang twisted cable dengan kecepatan 2,048Mbps dengan data rate hingga 12 kaki. Contoh konfigurasi HDSL dapat dilihat pada gambar 4.18 dan gambar 4.19 pada bagian mengamati.

4. Very High Bit Rate Digital Subscriber Line (VDSL)

   VDSL adalah perangkat aktif di jaringan akses pelanggan yang digunakan untuk mendukung implementasi layanak multimedia pada jaringan broadband dengan menggunakan satu pair kabel tembaga. Teknologi VDSL bersifat asimetrik. Rentang operasinya terbatas pada 1.000 sampai 4.500 kaki (304 meter-1,37 Km), tetapi ia dapat menangani lebar pita rata-rata 13Mbps sampai 52 Mbps untuk downstream dan 1,5 Mbps sampai 2,3 Mbps untuk upstream-nya melalui sepasang kawat tembaga pilin. Lebar pita yang tersisa memungkinkan perusahaan telekomunikasi memberikan program layanan HDTV(high-definition television) dengan menggunakan teknologi VDSL. Teknologi ini dapat pula mengirimkan data dengan kecepatan 1,6 Mbps dan menerima data dengan kecepatan 25 Mbps dengan jarak maksimum sampai 900 meter. Karena kecepatannya yang tinggi maka teknologi imi memerlukan kabel serat optik yang kemampuannya lebih tinggi daripada memakai kabel tembaga yang ada. Contoh konfigurasi VDSL dapat dilihat pada gambar 4.15 dan gambar 4.16.

4.1.2.4 Mengasosiasi/Menalar

Hasil analisis untuk prinsip kerja subscriber internet telepon dapat diuraikan seperti berikut:

Teknologi yang menyediakan penghantar data digital melewati kabel yang digunakan dalam jarak dekat dari jaringan telepon setempat. Biasanya kecepatan unduh dari DSL berkisar dari 128 kb/d sampai 24.000 kb/d tergantung dari teknologi DSL tersebut. Kecepatan unggah DSL lebih rendah dari unduh versi ADSL dan sama cepat untuk SDSL.

Untuk subscriber internet telepon, ADSL merupakan teknologi DSL yang cocok untuk merepresentasikannya. ADSL menggunakan kabel telpon yang telah ada, jadi bukan fiber optics. ADSL juga dijuluki revolusi di bidang internet atau istilah asingnya “broadband”. ADSL mampu mengirimkan data dengan kecepatan bit yang tinggi, berkisar antara 1.5 Mbps – 8 Mbps untuk arah downstream (sentral – pelanggan), dan antara 16 Kbps –

640 Kbps untuk arah upstream (pelanggan – sentral). Kemampuan transmisi ADSL inilah yang mampu mengirimkan layanan interaktif multimedia melalui jaringan akses tembaga. ADSL sendiri merupakan salah satu anggota dari “DSL Family”. Teknologi x-DSL sendiri mempunyai berbagai macam variasi.

4.1.3 Rangkuman

Dengan mengikuti kegiatan belajar ini, dapat disimpulkan subscriber internet telepon merupakan teknologi modem yang menggunakan jalur telepon yang sudah ada untuk mentransport data dengan bandwidth lebar, seperti multimedia dan video. Seperti contoh DSL (Digital Subscriber Line). Komponen DSL meliputi: DSL Transceiver, Filtering, dan DSLAM.

Kegiatan belajar ini juga memberikan pemahaman mengenai 4 macam DSL, yaitu:

1. Symmetric Digital Subscriber Line (SDSL)
   SDSL sangat cocok digunakan untuk mengakses internet kecepatan tinggi karena memberikan kecepatan atau lebar pita sampai 2,3 Mbps dan diberikan secara simetris. Teknologi ini menggunakan kecepatan data 784 kbps, baik untuk kirim (uplink) atau terima (downlink). SDSL hanya menawarkan komunikaais data saja.
2. Asymmetric Digital Subscriber Line (ADSL)
   Teknologi ADSL adalah teknologi akses dengan perangkat khusus pada sentral dan pelangan yang memungkinkan transmisi broadband melalui satu pair kabel. Teknologi ini mempunyai kecepatan data yang berbeda untuk kirim (uplink) dan terima (downlink).Teknologi ADSL cocok digunakan untuk mengakses internet dan menjadi pilihan pengguna. Untuk uplink bisa mencapai 8 Mbps sementara untuk downlink bisa mencapai 1 Mbps dengan jarak kabel maksimum samapi dengan 5,5 km.
3. High Bit Rate Subscriber Line (HDSL)
   HDSL merupakan teknologi aplikasi pada jaringan local tembaga untuk menyalurkan layanan 2 Mbps. HDSL sangat cocok digunakan untuk gedung-gedung perkantoran atau kompleks perkantoran, karena memberikan kecepatan atau lebar data sampai 10 Mbps dan dapat dibagi-bagi kepada seluruh pengguna akhir.
4. Very High Bit Rate Digital Subscriber Line (VDSL)
   VDSL adalah perangkat aktif di jaringan akses pelanggan yang digunakan untuk mendukung implementasi layanak multimedia pada jaringan broadband dengan menggunakan satu pair kabel tembaga

4.1.4 Tugas

Tugas

Mengamati berbagai jenis modem Digital Subscriber Line (DSL) untuk internet telepon!

Langkah Kerja

1. Buatlah kelompok dengan anggota 3 – 4 orang.
2. Uraikan pengamatan kelompok tentang SDSL!
3. Uraikan pengamatan kelompok tentang ADSL!
4. Uraikan pengamatan kelompok tentang HDSL!
5. Uraikan pengamatan kelompok tentang VDSL!
6. Buat laporan dan diskusikan dengan teman sekelompok.

Bandingkan dan Simpulkan

Presentasikan hasil kerja kelompok anda di depan kelas dan bandingkan hasil kerja kelompok Anda dengan kelompok lain.

Berdasarkan hasil perbandingan tersebut hal penting apa yang harus dirumuskan secara bersama.

4.1.5 Penilaian Diri

Dalam test ini setiap anda harus membaca dengan cermat dan teliti setiap butir soal dibawah ini. Kemudian berdasarkan uraian materi diatas tulislah jawabannya pada lembar kerja penilaian diri yang telah disediakan.

1) Apa yang anda pahami tentang konsep dasar DSL?
2) Tulislah komponen-komponen DSL?
3) Bagaimana cara kerja DSLAM?
4) Jelaskan prinsip kerja ADSL!

Lembar Kerja Penilaian Diri

LJ- 01: Apa yang anda pahami tentang konsep dasar DSL?

……

……

……

……

……

LJ- 02: Tulislah komponen-komponen DSL?

……

……

……

……

……

……

……

……

LJ- 03: Bagaimana cara kerja DSLAM?

……

……

……

……

……

……

……

LJ- 04: Jelaskan prinsip kerja ADSL!

……

……

……

……

……

……

BAB V

5.1 Kegiatan Belajar 5: Konfigurasi pada Subcriber Internet Telepon

5.1.1 Tujuan Pembelajaran

Setelah mempelajari kegiatan belajar 5, diharapkan siswa dapat:

1) Memahami Konfigurasi pada subscriber internet telepon
2) Menyajikan hasil instalasi dan konfigurasi pada subscriber internet telepon

5.1.2 Aktifitas Belajar Siswa

5.1.2.1 Mengamati/Observasi

Amatilah gambar-gambar berikut!

Sumber : Dokumen Kemendikbud

Gambar 5.1 Modem Router ADSL

Sumber : Dokumen Kemendikbud

Gambar 5.2 Personal Computer (PC)

Sumber : Dokumen Kemendikbud

Gambar 5.3 Kabel RJ 11

Sumber : Dokumen Kemendikbud

Gambar 5.4 Kabel RJ 45

Sumber : Dokumen Kemendikbud

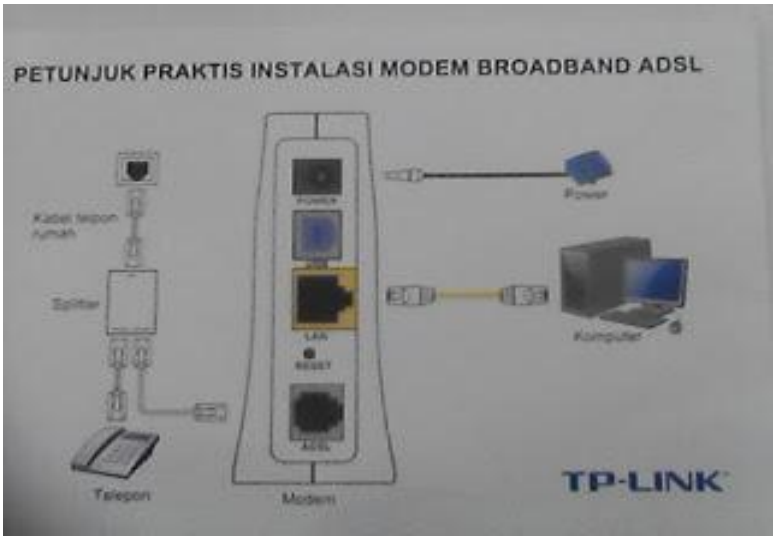
Gambar 5.5 Spitter

Sumber : Dokumen Kemendikbud

Gambar 5.6 Telepon

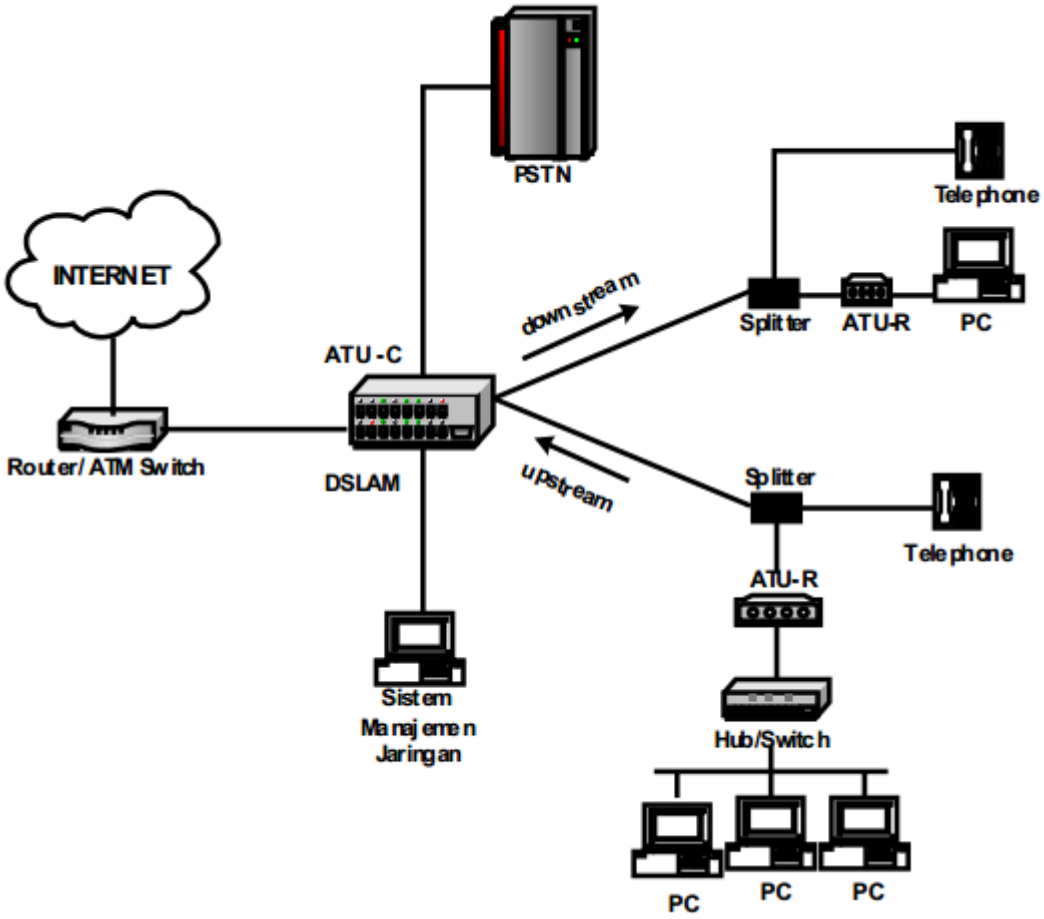
Sumber : Dokumen Kemendikbud

Gambar 5.7 Rowset



Sumber : Dokumen Kemendikbud

Gambar 5.8 Petunjuk Praktis Instalasi Modem Broadband ADSL



Sumber : Dokumen Kemendikbud

Gambar 5.9 Mekanisme Kerja Modem ADSL

5.1.2.2 Menanya

Dengan mengamati gambar yang ada pada bagian observasi, menurut anda:

1) Bagimanakah konfigurasi pada subscriber internet telepon?
2) Dapatkah anda menjelaskan hasil instalasi dan konfigurasi pada subscriber internet telepon?

5.1.2.3 Mencoba/Mengumpulkan Informasi

Teknologi modem voice konvensional (sistem narowband) saat ini yang mempunyai kecepatan 56 kbps tentu saja tidak dapat mengakomodasi perkembangan komunikasi data sekarang ini. Para pengguna menginginkan kapasitas transfer yang lebih besar untuk transfer data yang lebih cepat. Oleh karena itu, teknologi ADSL (Assymetric Digital Subscriber Lines) merupakan salah satu alternatif terbaik yang cocok diterapkan untuk mempercepat akses transfer data di subscriber lines.

Teknologi ADSL (Assymetric Digital Subscriber Lines) mampu menghasilkan kecepatan hingga 384 kbps untuk downstream dan 64 kbps untuk upstream. Teknologi ADSL (Assymetric Digital Subscriber Lines) memungkinkan akses internet dan pembicaraan. Untuk dapat melakukan koneksi layanan access dengan teknologi ADSL (Assymetric Digital

Subscriber Lines) pengguna harus menggunakan modem ADSL.

5.1.2.3.1 ADSL

ADSL (Asymmetric Digital Subscriber Line) adalah salah satu jenis teknologi DSL dimana pembagian bandwidth data untuk transmisi downstream lebih besar daripada upstream. Teknologi ADSL ini memungkinkan pelanggan dapat melakukan akses data dan melakukan panggilan telepon analog biasa secara bersamaan karena teknologi ini memisahkan frekuensi suara dan frekuensi data. ADSL tahap awal mampu mentransmisikan sampai 8 Mbps kepada subscriber (downlink) dan kurang lebih 640 kbps untuk transmisi arah yang berlawanan (uplink). Penambahan kecepatan ini 50 kali dari kapasitas akses lama (akses internet dial- up). Perbedaan kecepatan yang mencolok ini disebabkan perbedaan penggunaan frekuensi untuk mengirim sinyal data. Laju data pada ADSL dipengaruhi oleh beberapa faktor, diantaranya adalah panjang kabel, diameter kabel, level bising pada kabel, adanya bridge tap, dan interferensi cross- couple. Dari faktor-faktor yang telah disebutkan tampak bahwa laju data ADSL sangat bergantung pada media transmisinya, yaitu kabel. Dari sisi kabel sendiri terdapat suatu faktor pelemahan yang sebanding dengan panjang kabel dan frekuensi, tetapi berbanding terbalik terhadap diameter kabel.

5.1.2.3.3 Jenis-Jenis Modem ADSL

Jenis modem ADSL yang banyak digunakan saat ini adalah modem USB dan Router ADSL. Kedua modem tersebut dijelaskan seperti berikut:

1) Modem USB memperoleh catu daya dan tersambung ke komputer melalui USB, seluruh konfigurasi dilakukan melalui komputer. Modem USB lebih murah daripada modem router. Akan tetapi, kalau komputer terkena virus akan bermasalah dan kemungkinan perlu me-reset modem ADSL tersebut. Fungsi proxy dan firewall harus dilakukan oleh komputer.
2) Modem router, sebetulnya merupakan komputer sendiri yang biasanya bersatu dengan beberapa sambungan LAN, mempunyai kemampuan proxy dan firewall sendiri. Modem router lebih memudahkan operator atau pengguna kantor kecil untuk bekerja menggunakan ADSL. Harga modem router sedikit lebih mahal daripada modem USB. Untuk keandalan dan kepraktisan, akan jauh lebih baik menggunakan modem router.

5.1.2.3.2 Perangkat ADSL

Perangkat pada modem router ADSL adalah sebagai berikut:

1) Satu di sisi pelanggan (disebut CPE, Customer Premised Equipment)
   Di sisi pelanggan harus ada penerima DSL (modem ADSL) dan splitter.
2) Satu lagi di sisi TELKOM.
3) Di sisi TELKOM terdapat ADSL multiplexer disebut DSLAM (Digital Subscriber Line Access Multiplexer) untuk menerima sambungan dari pelanggan. Modem ADSL atau ADSL Transceiver Remote (ATU-R) mengubah sinyal digital menjadi sinyal

analog dan sebaliknya. Modem ADSL memberikan jalur tersendiri dari pelanggan hingga ke DSLAM yang berarti pelanggan tidak akan merasakan turunnya unjuk kerja apabila terjadi penambahan pelanggan.

Modem ADSL Modem ADSL atau ADSL Transceiver Remote (ATU-R) mengubah sinyal digital menjadi sinyal analog dan sebaliknya. Modem ADSL memberikan jalur tersendiri dari pelanggan hingga ke DSLAM yang berarti pelanggan tidak akan merasakan turunnya unjuk kerja apabila terjadi penambahan pelanggan. Downstream adalah pentransmisian sinyal berkecepatan tinggi dari sentral menuju pelanggan. Kecepatan data downstream berkisar 1,5 Mbps – 16 Mbps. Sedangkan upstream adalah pentrasmisian sinyal berkecepatan rendah dari pelanggan menuju sentral. Kecepatan data upstream berkisar 512 Kbps – 800 Kbps.

5.1.2.3.5 Cara Kerja Modem ADSL

Mekanisme kerja ADSL sebagai berikut : informasi dari internet dapat diakses setelah melalui router/ATM switch diteruskan ke DSLAM. Di dalam DSLAM sendiri terdapat dua saluran yaitu suara dan data, sehingga perlu adanya sistem manajemen jaringan untuk mengaturnya. Dari DSLAM informasi diteruskan ke sisi pelanggan masuk ke splitter. Di dalam splitter input DSLAM dipisah menjadi dua yaitu berupa voice dan data. Untuk suara langsung menuju saluran telepon sedangkan data menuju modem ADSL/ATU-R sehingga tidak terjadi interferensi antara sinyal suara dan data. Modem ADSL siap digunakan untuk koneksi internet, tetapi jika ingin di- share maka perlu adanya hub/switch untuk membagi koneksi dengan yang lain.

5.1.2.3.4 Implementasi Modem ADSL

Speedy merupakan salah satu implementasi ADSL yang ada di pasaran, khususnya di Indonesia. Dengan layanan ini, jaringan akses telepon pelanggan ditingkatkan kemampuannya menjadi jaringan digital berkecepatan tinggi, sehingga selain mendapatkan fasilitas telepon (voice), pelanggan juga dapat melakukan akses internet (dedicated) dengan kecepatan (downstream) yang tinggi (s/d 800 Kbps). Data dan suara dapat disalurkan secara simultan melalui satu saluran telepon biasa dengan kecepatan yang dijaminkan sesuai dengan paket layanan yang diluncurkan dari modem sampai BRAS (Broadband Remote Access Server).

5.1.2.3.6 Koneksi Telepon dari Telkom

Langkah-langkah instalasi untuk koneksi telepon dari Telkom adalah sebagai berikut:

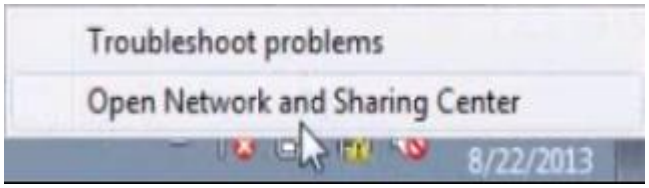
- Masukkan kabel dari sentral ke rowset
- Dari rowset, kemudian hubungkan ke splter menggunakan kabel RJ 11
- Setelah dihubungkan ke splitter, selanjutnya dari splitter hubungkan ke telepon dan modem menggunakan kabel RJ11
- Test koneksi atau tidaknya dari sentral dengan cara angkat

ganggang telepon dan dengarkan, jika terdengar bunyi maka sudah terkoneksi ke sentral.

- Masukkan kabel power ke modemnya dan tekan tombol power yang ada di modemnya.
- Jika modemnya sudah pernah dipakai, maka kita perlu mereset terlebih dahulu modem tersebut, dengan cara menekan lubang kecil yang ada di modem tersebut secara pelan-pelan selama 10 detik menggunakan alat yang ujungnya kecil (misalnya menggunakan ujung bolpoin).
- Pasangkan kabel RJ45 ke modem dan dari modem ke komputer atau laptopnya.

Sedangkan untuk langkah-langkah Konfigurasi koneksi Telepon dari Telkom seperti berikut:

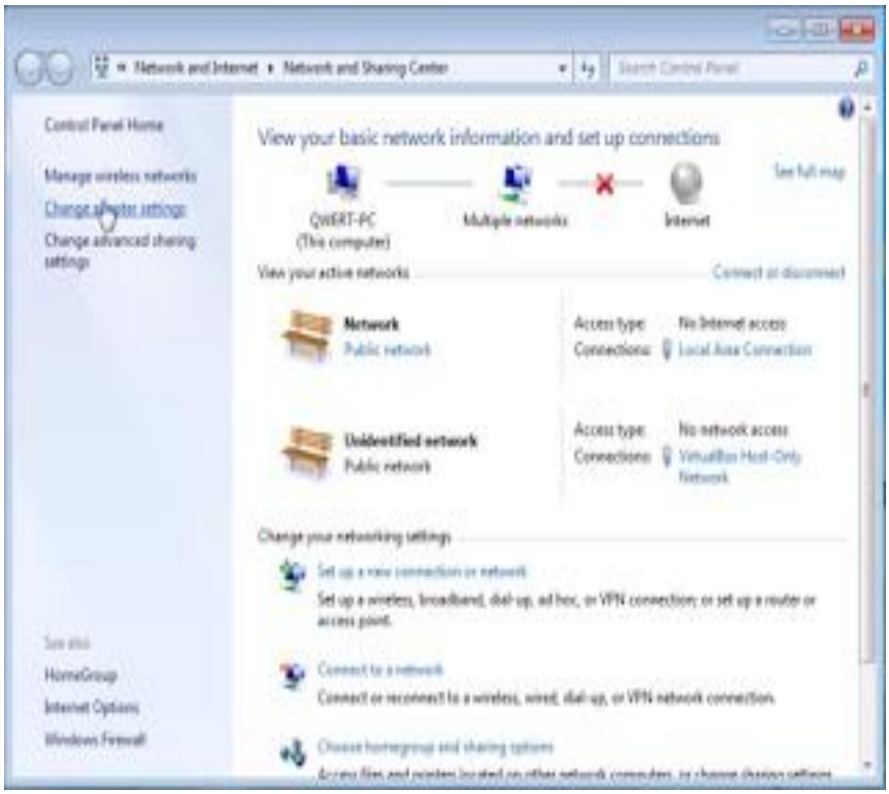
1) Lihat IP dan username serta passwordnya di modem tersebut (bisaanya berada di belakang modem).
2) Jika sudah diketahui IP modemnya, selanjutnya kita setting IP di computer atau laptonya dengan network yang sama dengan modemnya dan gatewaynya isikan dengan IP modem tersebut. Contoh menyetting IP di computer atau laptop adalah sebagai berikut :
   a) Klik kanan pada gambar tv di bawah, kemudian pilih open network and sharing center



Sumber : Dokumen Kemendikbud

Gambar 5.10 Tampilan untuk Akses Open Network and Sharing Center

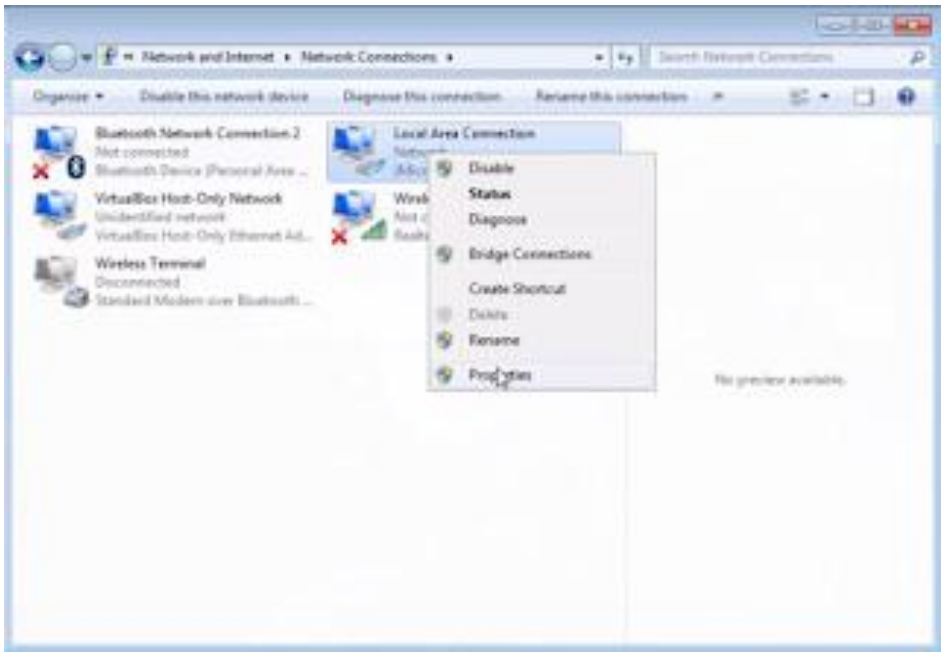
   b) Maka akan muncul tampilan seperti berikut, kemudian pilih change adapter setting



Sumber : Dokumen Kemendikbud

Gambar 5.11 Tampilan Menu Network and Sharing Center

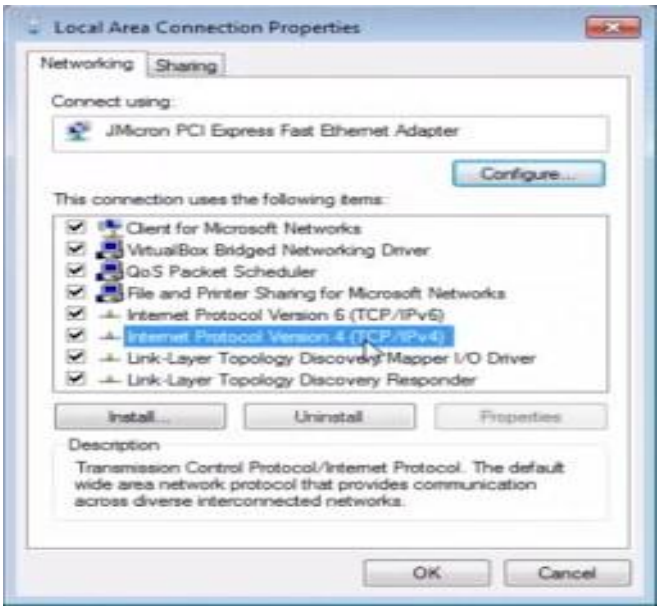
c) Klik kanan pada local area connection dan pilih properties



Sumber : Dokumen Kemendikbud

Gambar 5.12 Network Connection yang tersedia

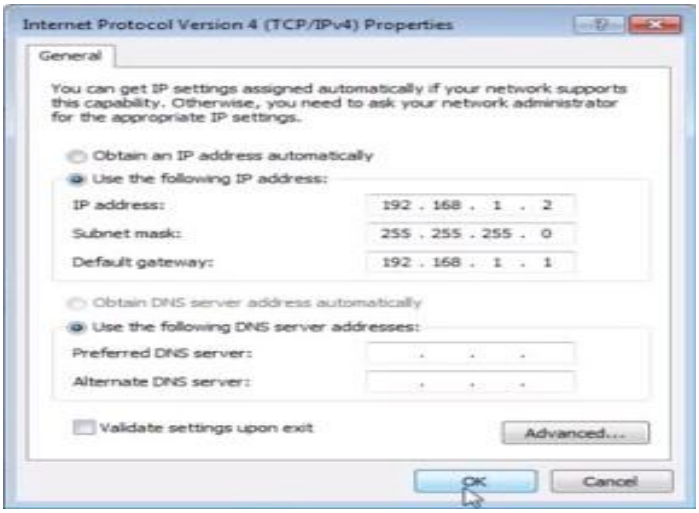
d) Arahkan cursor ke IPv4, kemudian properties



Sumber : Dokumen Kemendikbud

Gambar 5.13 Tampilan Properties LAN

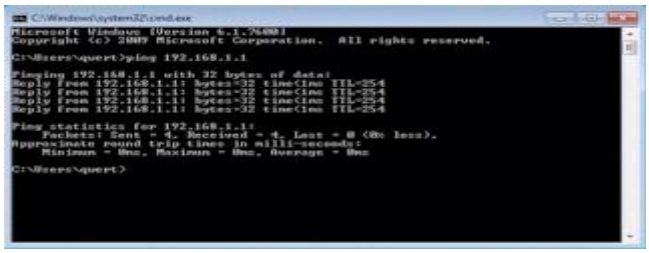
e) Akan tampil seperti di bawah ini, selanjutnya pilih use the following IP address. Maksudnya yaitu untuk mengatur IP secara manual. Di bawah ini saya contohkan IP modemnya 192.168.1.1, maka IP computer atau laptop di isi dengan 192.168.1.2. IP modem dan IP computer atau laptop tidak boleh sama, karena dalam sebuah IP, networknya harus sama dan hostnya berbeda. Kemudian gateway kita isi dengan IP modem tersebut. Jika sudah selesai, maka pilih OK



Sumber : Dokumen Kemendikbud

Gambar 5.14 Tampilan Properties IP

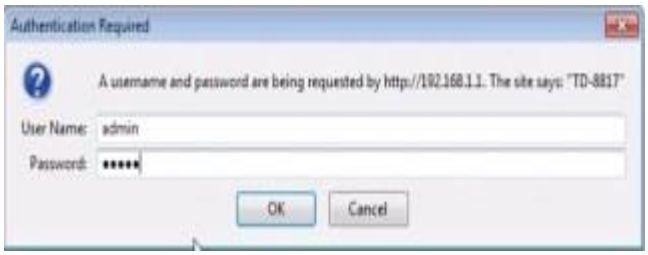
Selanjutnya kita hubungkan komputer atau laptop dengan modemnya, dengan cara ke CMD, kemudian ketikkan ping <IP modemnya>. Contohnya ping 192.168.1.1. Jika muncul TTL, maka proses menghubungkan berhasil.



Sumber : Dokumen Kemendikbud

Gambar 5.15 Tampilan CMD untuk menghubungkan Laptop/PC dengan Modem

Kemudian ke browser, di address bar isikan IP modemnya, tekan enter, selanjutnya di minta user name dan password, maka kita isi dengan user dan password yang ada di modem tersebut. Tekan OK. Disini saya contohkan IP modemnya 192.168.1.1 dan user name dan passwordnya adalah admin.



Sumber : Dokumen Kemendikbud

Gambar 5.16 Tampilan Authentication Required

Akan muncul tampilan berikut:

Sumber : Dokumen Kemendikbud

Gambar 5.17 Tampilan Menu Utama ADSL Telkom

Pilih Run Wizard ke Menu Quick Start maka akan muncul tampilan seperti berikut:

Sumber : Dokumen Kemendikbud

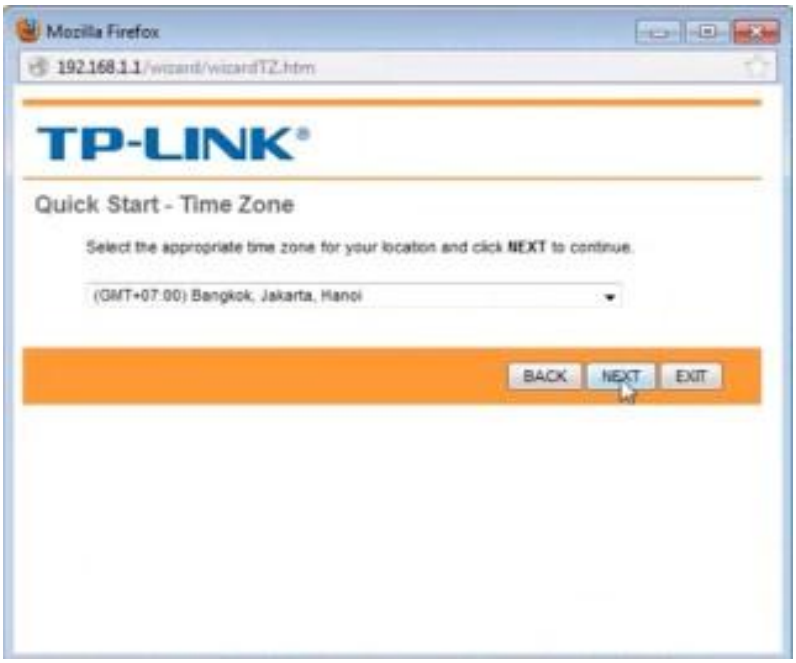
Gambar 5.18 Tampilan Menu Quick Start

Pilih Next seperti tampilan berikut:

Sumber : Dokumen Kemendikbud

Gambar 5.19 Tampilan setelah Memilih Run Wizard

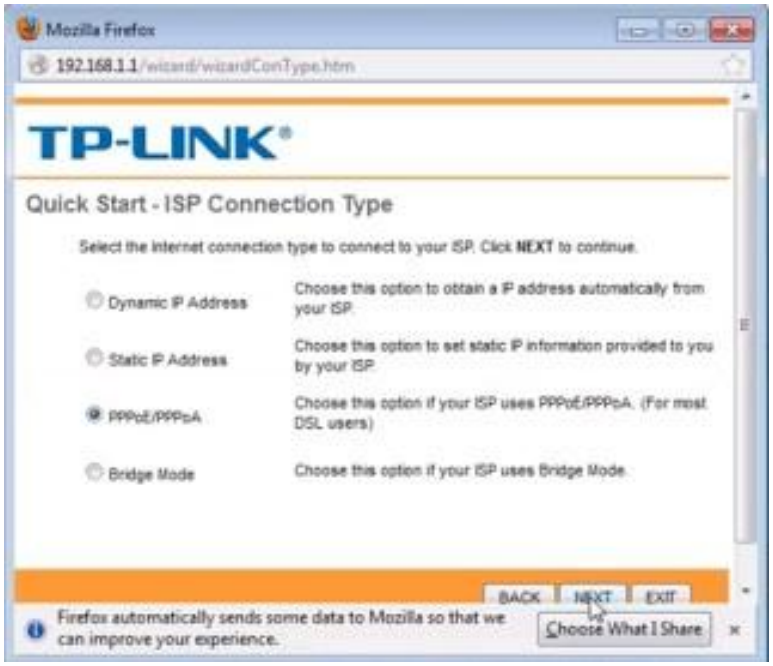
Atur zona waktunya, jika sudah selesai maka pilih next seperti gambar berikut:



Sumber : Dokumen Kemendikbud

Gambar 5.20Tampilan mengatur Zona Waktu

Pilih PPPoE/PPPoA, kemudian next



Sumber : Dokumen Kemendikbud

Gambar 5.21 Tampilan memilih ISP

Selanjutnya, ketikkan username dan passwordnya yang sudah anda daftarkan di BRAS / sentral telepon, kemudian next.

Sumber : Dokumen Kemendikbud

Gambar 5.22 Tampilan untuk memasukkan Username dan Password

Selanjutnya, pilih Next seperti gambar berikut:

Sumber : Dokumen Kemendikbud

Gambar 5.23 Proses Instalasi Selesai

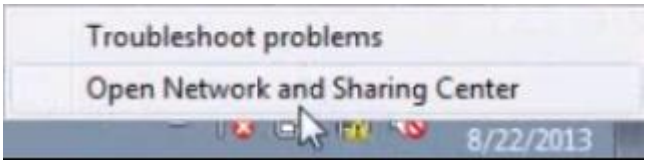
Pilih Close

Sumber : Dokumen Kemendikbud

Gambar 5.24 Tampilan Akhir Konfigurasi pada Browser

Ke menu status, untuk melihat apakah mendapatkan IP atau belum.. Jika sudah mendapatkan IP, selanjutnya ke menu interface setup, kemudian ke LAN. Di menu tersebut DHCP di buat enable. Sehingga setiap komputer mendapatkan IP secara otomatis. Sebelumnya kita terlebih dahulu mengatur IPnya supaya mendapatkan IP secara otomatis, dengan langkah-langkah berikut ini :

a) Klik kanan pada gambar tv di bawah, kemudian pilih open network and sharing center



Sumber : Dokumen Kemendikbud

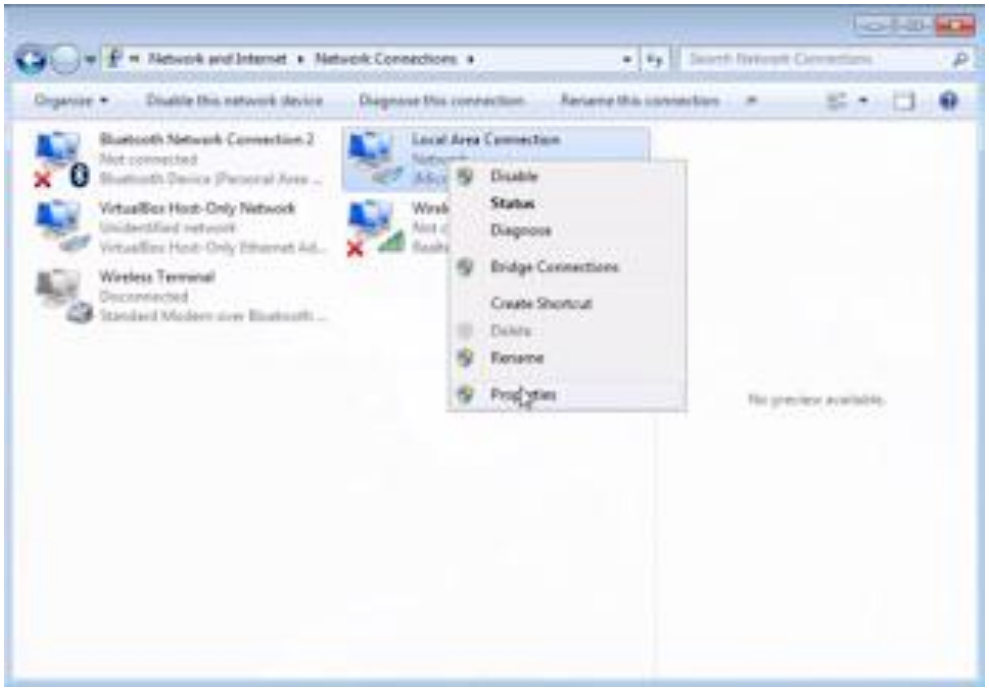
Gambar 5.25 Mengakses Network and Sharing Center

b) Maka akan muncul tampilan, kemudian pilih change adapter setting

Sumber : Dokumen Kemendikbud

Gambar 5.26 Tampilan Network and Sharing Center

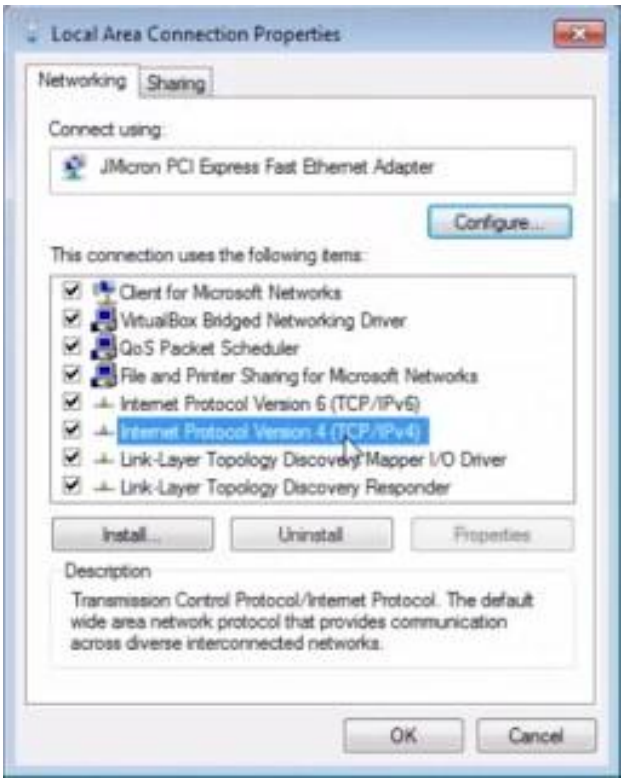
c) Klik kanan pada local area connection dan pilih properties



Sumber : Dokumen Kemendikbud

Gambar 5.27 Local Area Connection yang akan diatur

d) Arahkan cursor ke IPv4, kemudian properties



Sumber : Dokumen Kemendikbud

Gambar 5.28 Tampilan Properties LAN

e) Pilih obtain an IP address automaticly agar mendapatkan IP secara otomatis, kemudian OK

Sumber : Dokumen Kemendikbud

Gambar 5.29 Tampilan Properties IP

f) Selanjutnya di local area connection, klik kanan dan pilih status untuk melihat IP yang di dapatkan pada computer atau laptop tersebut

g) Jika sudah berhasil mendapatkan IPnya, selanjutnya kita test browsing. Untuk pertama kali browsing akan muncul error, dan untuk seterusnya akan berhasil. Contoh setelah selesai instalasi dan konfigurasi.

5.1.2.3.7 Keunggulan dan Kekurangan ADSL

Keunggulan ADSL dibanding dengan modem Dial-Up biasa adalah sebagai berikut:

- Dibandingkan dengan modem 56k, DSL mampu menawarkan kecepatan hingga 125 kali lebih cepat. Kecepatan ini memungkinkan untuk bisa ber-video teleconferrence ataupun menonton film di internet.
- Biaya koneksi DSL biasanya flat dan relatif murah, sehingga bebas menggunakan tanpa perlu takut kelebihan biaya.
- Tidak perlu menunggu call setup yang lama lagi, begitu komputer hidup, koneksi langsung tersambung dan always on (selama modem ADSL hidup)
- Biasanya perusahaan telepon yang paling terjamin, dimana hanya beberapa saat down time dalam setahun .
- Karena koneksi dilakukan dengan kabel sendiri, maka setiap pelanggan mendapatkan masing-masing koneksi point-to-point ke internet. Sehingga kestabilan koneksi dan keamanan lebih terjamin.

Selain keunggulan yang dibandingkan dengan modem Dial-up lainnya, keunggulan ADSL sendiri adalah sebagai berikut:

- ADSL memberikan kemampuan internet dan telepon secara simultan.
- ADSL menggunakan koneksi point to point.
- ADSL murah bagi penyelenggara jaringan.
- ADSL mendukung aplikasi multimedia.
- ADSL menggunakan mode transmisi asimetrik.
- Karena kecepatan download tinggi, maka waktu yang diperlukan untuk proses download semakin cepat sehingga lebih ekonomis

Sedangkan kekurangan dari modem ADSL adalah sebagai berikut:

- Keterbatasan jarak.
- Kabel tembaga tidak tahan lama.
- Redaman kabel tembaga.
- Kecepatan akses internet juga masih dipengaruhi kecepatan ISP.

5.1.2.4. Mengasosiasi/Menalar

Berdasarkan konfigurasi subscriber internet telepon yang dilakukan, dapat dianalisa bahwa:

1) Asymmetric Digital Subscriber Line (ADSL): teknologi ADSL adalah teknologi akses dengan perangkat khusus pada sentral dan pelangan yang memungkinkan transmisi broadband melalui satu pair kabel.
2) ADSL (Asymmetric Digital Subscriber Line) adalah salah satu jenis teknologi

DSL dimana pembagian bandwidth data untuk transmisi downstream lebih besar daripada upstream.

3) Jenis-jenis Modem ADSL yang banyak digunakan yaitu, modem USB dan router ADSL
4) Modem USB memperoleh satu daya dan tersambung ke komputer melalui USB, seluruh konfigurasi dilakukan melalui komputer.
5) Modem router, merupakan komputer sendiri yang biasanya bersatu dengan beberapa sambungan LAN, mempunyai kemampuan proxy dan firewall sendiri
6) Perangkat ADSL yaitu:
    a. Satu di sisi pelanggan (disebut CPE, Customer Premised Equipment)
    b. Satu lagi di sisi TELKOM.
7) Kecepatan data modem ADSL adalah downstream berkisar 1,5 Mbps – 16 Mbps.
8) Sedangkan upstream adalah pentrasmisian sinyal berkecepatan rendah dari pelanggan menuju sentral.
9) Kecepatan data upstream berkisar 512 Kbps – 800 Kbps.
10) Langkah-langkah instalasi Koneksi Telepon dari Telkom:

    a. Masukkan kabel dari sentral ke rowset
    b. Dari rowset, kemudian hubungkan ke spltter menggunakan kabel RJ 11
    c. Setelah dihubungkan ke splitter, selanjutnya dari splitter hubungkan ke telepon dan modem menggunakan kabel RJ11
    d. Test koneksi atau tidaknya dari sentral dengan cara angkat ganggang telepon dan dengarkan, jika terdengar bunyi maka sudah terkoneksi ke sentral.
    e. Masukkan kabel power ke modemnya dan tekan tombol power yang ada di modemnya.
    f. Jika modemnya sudah pernah dipakai, maka kita perlu mereset terlebih dahulu modem tersebut, dengan cara menekan lubang kecil yang ada di modem tersebut secara pelan-pelan selama 10 detik menggunakan alat yang ujungnya kecil (misalnya menggunakan ujung bolpoin).
    g. Pasangkan kabel RJ45 ke modem dan dari modem ke komputer atau laptopnya.

5.1.3 Rangkuman

Setelah membahas semua mengenai subscriber internet telepon, apa yang anda pelajari? Well, dapat disimpulkan bahwa ada berbagai jenis subscriber internet telepon tetapi yang biasa diterapkan di Indonesia adalah ADSL.

Keunggulan yang dimiliki ADSL dibandingkan dengan modem Dial Up biasa yaitu:

- Dibandingkan dengan modem 56k, DSL mampu menawarkan kecepatan hingga 125 kali

lebih cepat. Kecepatan ini memungkinkan untuk bisa ber-video teleconferrence ataupun menonton film di internet.

- Biaya koneksi DSL biasanya flat dan relatif murah, sehingga bebas menggunakan tanpa perlu takut kelebihan biaya.
- Tidak perlu menunggu call setup yang lama lagi, begitu komputer hidup, koneksi langsung tersambung dan always on (selama modem ADSL hidup)
- Biasanya perusahaan telepon yang paling terjamin, dimana hanya beberapa saat down time dalam setahun .
- Karena koneksi dilakukan dengan kabel sendiri, maka setiap pelanggan mendapatkan masing-masing koneksi point-to-point ke internet. Sehingga kestabilan koneksi dan keamanan lebih terjamin.

Keunggulan modem ADSL antara lain

- ADSL memberikan kemampuan internet dan telepon secara simultan.
- ADSL menggunakan koneksi point to point.
- ADSL murah bagi penyelenggara jaringan.
- ADSL mendukung aplikasi multimedia.
- ADSL menggunakan mode transmisi asimetrik.
- Karena kecepatan download tinggi, maka waktu yang diperlukan untuk proses download semakin cepat sehingga lebih ekonomis

Kekurangan modem ADSL antara lain :

- Keterbatasan jarak.
- Kabel tembaga tidak tahan lama.
- Redaman kabel tembaga.
- Kecepatan akses internet juga masih dipengaruhi kecepatan ISP

5.1.4 Tugas

Tugas

Melakukan proses pengamatan langkah-langkah konfigurasi pada Subcriber Internet telepon serta menyajikan hasil konfigurasi Subcriber Internet telepon.

Langkah Kerja

1. Buatlah kelompok dengan anggota 3 – 4 orang.
2. Uraikan pengamatan kelompok tentang instalasi telepon dari Telkom !
3. Uraikan pengamatan kelompok tentang konfigurasi telepon dari Telkom!
4. Uraikan pengamatan kelompok tentang implementasi ADSL!
5. Uraikan pengamatan kelompok tentang cara kerja modem ADSL!
6. Buat laporan dan diskusikan dengan teman sekelompok.

Bandingkan dan Simpulkan

Presentasikan hasil kerja kelompok anda di depan kelas dan bandingkan hasil kerja kelompok Anda dengan kelompok lain.

Berdasarkan hasil perbandingan tersebut hal penting apa yang harus dirumuskan secara bersama.

5.1.5 Penilaian Diri

Dalam test ini setiap anda harus membaca dengan cermat dan teliti setiap butir soal dibawah ini. Kemudian berdasarkan uraian materi diatas tulislah jawabannya pada lembar kerja penilaian diri yang telah disediakan.

1) Apa yang anda pahami tentang Teknologi x-DSL? Jelaskan secara singkat!
2) Jelaskan perbedaan atau kesamaan dari Teknologi ADSL dan Model ADSL!
3) Tuliskan dan jelaskan 2 jenis modem ADSL!
4) Berapakan kecepatan data modem ADSL?
5) Tuliskan langkah mengintalasi koneksi telepon dari Telkom!

6) Tuliskan keunggulan modem ADSL!

Lembar Kerja Penilaian Diri

LJ- 01: Apa yang anda pahami tentang Teknologi x-DSL? Jelaskan secara singkat!

……
……
……
……
……
……

LJ- 02: Jelaskan perbedaan atau kesamaan dari Teknologi ADSL dan Model ADSL!

……
……
……
……
……
……
……
……
……

LJ- 03: Tuliskan dan jelaskan 2 jenis modem ADSL!

……
……
……
……
……
……
……
……

LJ- 04: Berapakan kecepatan data modem ADSL?

……
……
……

……
……
……
……

LJ- 05: Tuliskan langkah mengintalasi koneksi telepon dari Telkom!

……
……
……
……
……
……
……

LJ- 06: Tuliskan keunggulan modem ADSL!

……
……
……
……
……
……
……

BAB VI

6.1.1. Kegiatan Belajar 5: Prosedur Pengamatan Kerja

6.1.1. Tujuan Pembelajaran

Setelah mempelajari kegiatan belajar 6, diharapkan siswa dapat:

1) Memahami prosedur pengamatan kerja pada sistem komunikasi VoIP
2) Menyajikan hasil analisa prosedur pengamatan kerja sistem komunikasi VoIP

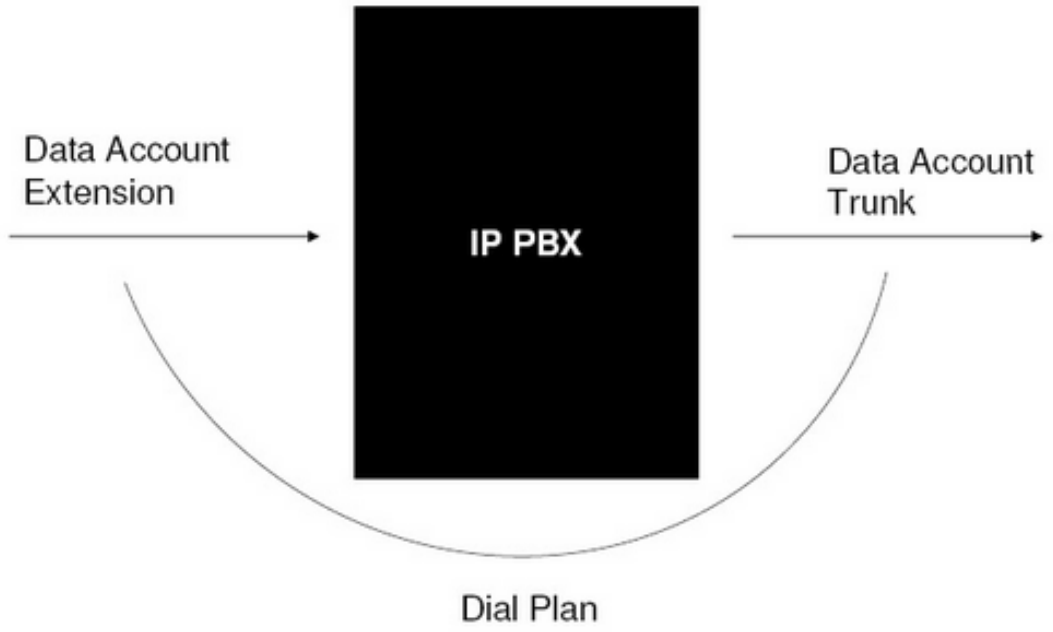
6.1.2 Aktifitas Belajar Siswa

6.1.2.1 Mengamati/Observasi

Amatilah gambar-gambar berikut:

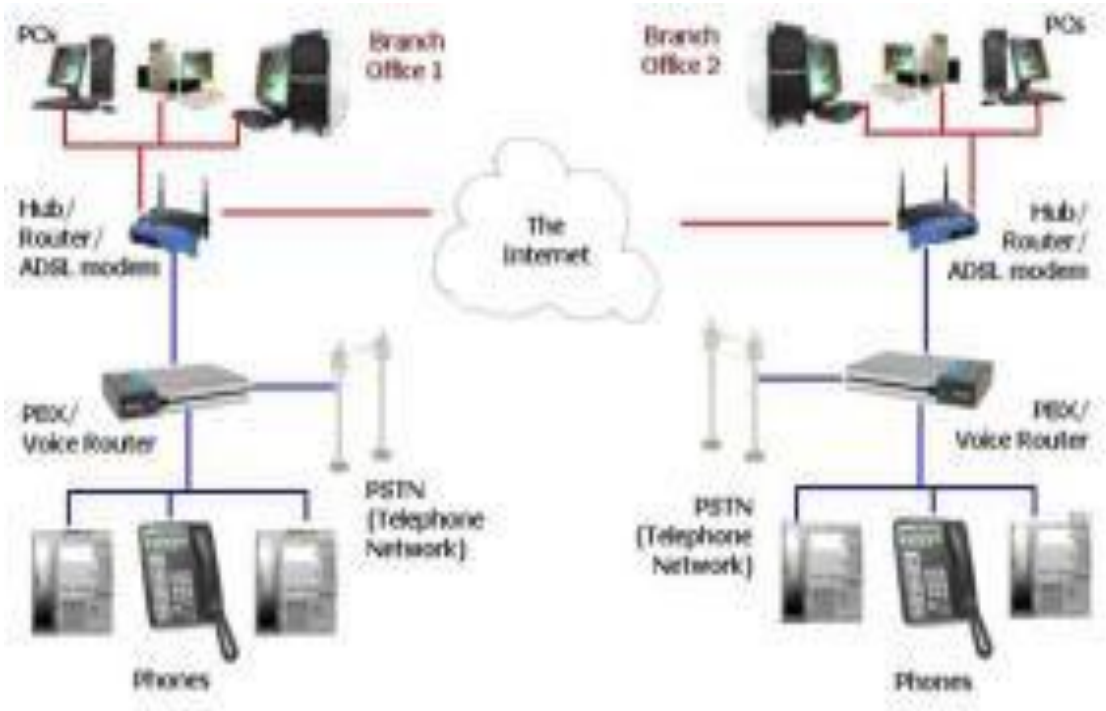
Sumber : http://blogmasjoko.blogspot.com/2011/12/belajar-ip-pbx.html

Gambar 6.1 Komponen Dasar IP-PBX



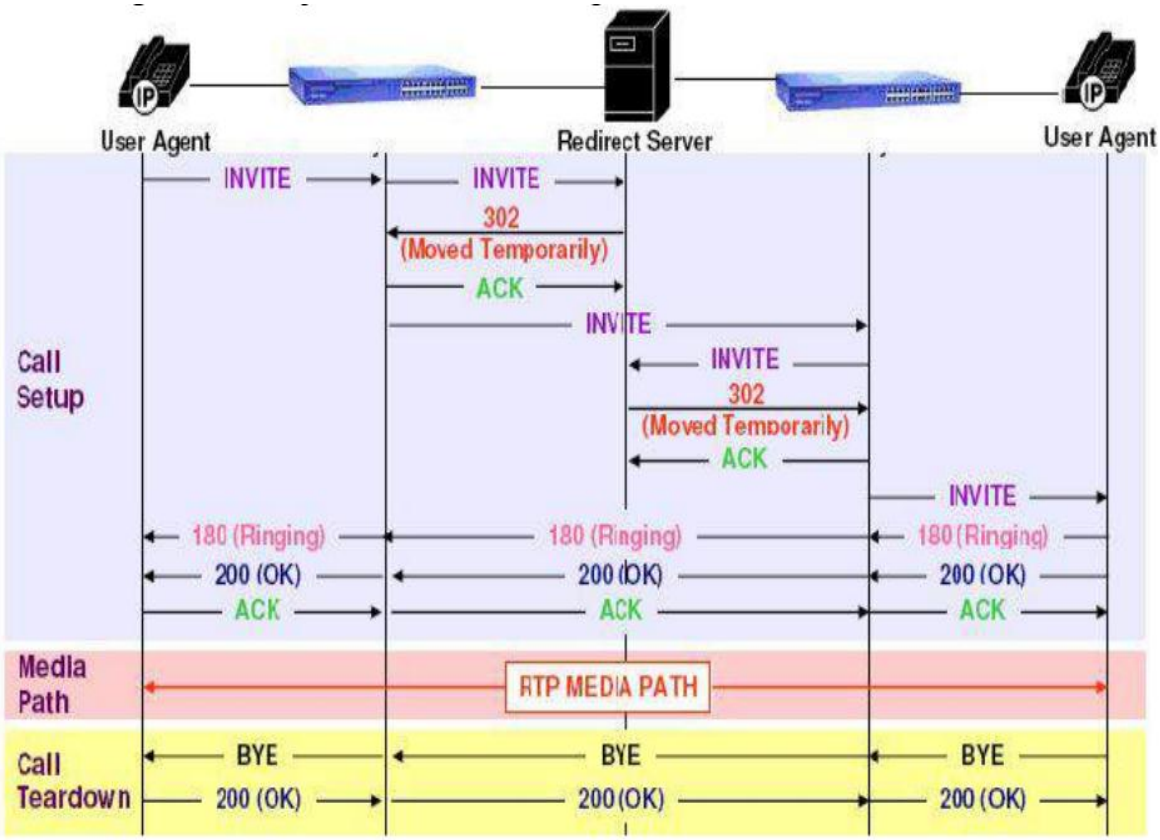
Sumber : http://blogmasjoko.blogspot.com/2011/12/belajar-ip-pbx.html

Gambar 6.2 Data Account



Sumber : Dokumen Kemendikbud

Gambar 6.3 Cara Kerja VoIP



Sumber : Dokumen Kemendikbud

Gambar 6.4 Pengamatan Kerja VoIP

6.1.2.2 Menanya

Dengan mengamati gambar yang ada pada bagian observasi, menurut anda:

1) Bagimanakah prosedur pengamatan kerja pada sistem komunikasi VoIP?
2) Dapatkah anda menjelaskan hasil analisa prosedur pengamatan kerja sistem komunikasi VoIP?

6.1.2.3 Mencoba/Mengumpulkan Informasi

Voice over Internet Protocol (juga disebut VoIP, IP Telephony, Internet telephony atau Digital Phone) adalah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet. Data suara diubah menjadi kode digital dan dialirkan melalui jaringan yang mengirimkan paket-paket data, dan bukan lewat sirkuit analog telepon biasa.

Voice over Internet Protocol (VoIP) adalah teknologi yang mampu melewatkan trafik suara, video dan data yang berbentuk paket melalui jaringan IP. Dalam komunikasi VoIP, pemakai melakukan hubungan telepon melalui terminal yang berupa PC atau telepon.

Kebutuhan perangkat VoIP antara lain:

- Hub
- Router
- ADSL Modem
- VoIP phone Adaptor

6.1.2.3.1 Konsep Kerja Server Softswitch

Softswitch merupakan sebuah sistem telekomunikasi masa depan yang mampu memenuhi kebutuhan pelanggan yaitu mampu memberikan layanan triple play sekaligus dimana layanan ini hanya mungkin dilakukan oleh sistem dengan jaringan yang maju seperti teknologi yang berbasis IP.

Bagian yang paling kompleks dalam suatu sentral lokal adalah bagian software yang mengatur call processing. Salah satu solusi untuk mengatasi masalah ini adalah dengan menciptakan suatu alat yang dapat menyambungkan komunikasi suara (voice) dalam bentuk paket maupun circuit. Industri pertelekomunikasian menyimpulkan cara yang terbaik adalah dengan memisahkan fungsi call processing dari fungsi switching secara fisik dan menghubungkan keduanya melaui suatu protocol standar tersendiri.

6.1.2.3.2 Prinsip Kerja VoIP

Pada Sumber : Dokumen Kemendikbud

menunjukkan pinsip kerja VoIP. Prinsip kerja VoIP adalah mengubah suara analog yang didapatkan dari speaker pada Komputer menjadi paket data digital, kemudian dari PC diteruskan melalui Hub/ Router/ ADSL Modem dikirimkan melalui jaringan internet dan akan diterima oleh tempat tujuan melalui media yang sama. Atau bisa juga melalui melalui media telepon diteruskan ke phone adapter yang disambungkan ke internet dan bisa diterima oleh telepon tujuan.

Untuk Pengiriman sebuah sinyal ke remote destination dapat dilakukan secara digital yaitu sebelum dikirim data yang berupa sinyal analog diubah ke bentuk data digital dengan ADC (Analog to Digital Converter), kemudian ditransmisikan, dan di penerima dipulihkan kembali menjadi data analog dengan DAC (Digital to Analog Converter). Begitu juga dengan VoIP, digitalisasi voice dalam bentuk packets data, dikirimkan dan di pulihkan kembali dalam bentuk voice di penerima. Format digital lebih mudah dikendaikan, dalam hal ini dapat dikompresi, dan dapat diubah ke format yang lebih baik dan data digital lebih tahan terhadap noise daripada analog.

Bentuk paling sederhana dalam sistem VoIP adalah dua buah komputer terhubung dengan internet. Syarat-syarat dasar untuk mengadakan koneksi VoIP adalah komputer yang terhubung ke internet, mempunyai sound card yang dihubungkan dengan speaker dan mikropon. Dengan dukungan software khusus, kedua pemakai komputer bisa saling terhubung dalam koneksi VoIP satu sama lain. Bentuk hubungan tersebut bisa dalam bentuk pertukaran file, suara, gambar. Penekanan utama dalam VoIP adalah hubungan keduanya dalam bentuk suara.

Pada perkembangannya, sistem koneksi VoIP mengalami evolusi. Bentuk peralatan pun berkembang, tidak hanya berbentuk komputer yang saling berhubungan, tetapi peralatan lain seperti pesawat telepon biasa terhubung dengan jaringan VoIP. Jaringan data digital dengan gateway untuk VoIP memungkinkan berhubungan dengan PABX atau jaringan analog telepon biasa. Komunikasi antara komputer dengan pesawat

(extension) di kantor adalah memungkinkan. Bentuk komunikasi bukan Cuma suara saja. Bisa berbentuk tulisan (chating) atau jika jaringannya cukup besar bisa dipakai untuk Video Conference. Dalam bentuk yang lebih lanjut komunikasi ini lebih dikenal dengan IP Telephony yang merupakan komunikasi bentuk multimedia sebagai kelanjutan bentuk komunkasi suara (VoIP). Keluwesan dari VoIP dalam bentuk jaringan, peralatan dan media komunikasinya membuat VoIP menjadi cepat popular di masyarakat umum.

6.1.2.3.3 Proses Kerja PBX Server Softswitch

PBX adalah sebuah sentral privat dengan fitur seperti sentral public yang di gunakan oleh suatu lembaga / perusahaan dalam melayani komunikasai internet perusahaan tersebut.

Sebuah sistem IP PBX terdiri dari satu atau lebih telepon SIP, server IP PBX dan secara opsional VoIP Gateway untuk terhubung ke jalur PSTN yang ada. Fungsi PBX IP server mirip dengan cara kerja proxy server: klien SIP, baik berupa software (softphone) atau perangkat keras berbasis ponsel, mendaftar ke server IP PBX, dan ketika mereka ingin membuat panggilan mereka meminta IP PBX untuk melakukan panggilan. IP PBX memiliki daftar semua ponsel / pengguna dan alamat yang sesuai dengan SIP mereka dan dengan demikian dapat menghubungkan panggilan internal atau rute panggilan eksternal baik melalui gateway VoIP atau penyedia layanan VoIP.

Beberapa fungsi yang mendukung model komunikasi berbasis IP antara lain adalah:

1) Address Discovery:
   - Pengenalan lokasi tujuan
   - Bisa membedakan antara lokasi berupa IP Address, Internet Uniform Resource Identifier (URI), atauphone number
2) Device Interoperability:
   - Peralatan VoIP yang diproduksi oleh vendor yang berbeda harus bisa saling interoperability, dengan jalan mengikuti standarisasi yang sudah ditetapkan, dan bekerja pada jenis protocol yang sama
3) Interoperability dengan telepon PSTN:
   - Arsitektur VoIP yang dibuat harus support fungsional untuk level protocol translation dan transcoding data
   - Dengan memperhatikan fungsionalitas ini, call dari jaringan IP dapat di-forwardkan ke dan dari jaringanPSTN
4) Session-level Control:
   - Meliputi: session-level otorisasi, otentifikasi, user billing, dan lain-lain

Alasan memilih jaringan Internet adalah sebagai berikut:

- Jaringan IP sendiri merupakan jaringan komunikasi data yang berbasis packet-switched
- Jaringan IP adalah jaringan global, tidak berdasarkan zona
- Bisa menekan biaya percakapan

Infrastruktur pendukung jaringan Internet adalah sebagai berikut:

Circuit-Switched

- Sebelum ada call, ada pembentukan jalur end-to-end dan membuat

dedicated link antar user yang hendak berkomunikasi.

- Dengan menggunakan dedicated circuit, delay yang dihasilkan oleh elemen sinyal (yang dibawa voice) relative konstan.
- Komponen yang digunakan selama percakapan, tidak dapat digunakan oleh user lain, sampai percakapan selesai.
- Setiap circuit mempunyai kapasitas tertentu untuk membawa sejumlah informasi, untuk suara, informasi berupa speech yang terkodekan
- Dedicated circuit selalu menyediakan jalur, meskipun terdapat kondisi dimana tidak ada informasi yang dilewatkan

Packet-Switched

- Informasi dipecah-pecah menjadi beberapa paket, kemudian masing-masing paket ditransmisikan secara independen ke tujuan.
- Tidak ada jalur dedicated end-to-end sebelum pentransmisian informasi. Setiap paket berisi informasi tujuan.
- Tiap elemen router dijaringan internet akan me-rutekan masing-masing paket ke elemen router berikutnya hingga sampai tujuan.
- Bisasanya masing-masing paket dengan tujuan yang sama, akan melewati jalur yang berbeda, sehingga sampai di tempat tujuan tidak dalam waktu yang sama.

Terdapat level Media pada kerja VoIP yang memiliki fungsi sebagai berikut:

- Semua komponen dalam sebuah arsitektur VoIP harus bias inter operasi dengan menggunakan protocol standart (H323/SIP).
- Dengan sifat ini bisa dimungkinkan:
  - Pemakaian peralatan multi vendor dalam satu sistim
  - Beberapa provider VoIP bias saling berkoordinasi satu dengan yang lain dalam membawa trafik VoIP
- Layanan voice over data yang dilewatkan protocol media transport, seperti RTP.
- Terdiri dari bermacam-macam pemrosesan level media yang digunakan untuk percampuran call dengan tujuan untuk konferensi multiparty, transcoding yang memungkinkan transportasi melalui beberapa jenis jaringan

6.1.2.3.4 Komponen Fungsional VoIP

Komponen fungsional VoIP adalah sebagai berikut:

1. Voice Calling Device

Peralatan untuk membangkitkan dan menerima call.

-IP Telephone

- Merupakan peralatan berbentuk telepon yang terhubung langsung ke jaringan internet.
- Mempunyai built-in software yang bias berkomunikasi dengan perlatan VoIP lain dijaringan Internet, dan protocol yang bisa mengirim paket data voice

- Terhubung kejaringan menggunakan jack RJ-45 atau wifi VoIP Phone yang terhubung dengan jaringan wireless IEEE 802.11

-Softphone

- Merupakan software yang mengimplementasikan fungsi-fungsi telepon
- Bisa dipasang di PC atau PDA
- Dengan softphone, user VoIP tidak perlu lagi menambahi peralatan telepon dijaringannya.

Telepon Analog Peralatan telepon analog yang terhubung ke PSTN

Analog Telephone Adapter (ATA)

- Peralatan yang digunakan jika sebuah pesawat telepon analog akan dihubungkan langsung ke jaringan internet
- Peralatan ini mentranslasikan bentuk informasi digital dari jaringan internet ke dalam bentuk informasi analog yang diterima pesawat telepon atau sebaliknya

2. Gateway

Sebagai pembatas dari dua jaringan yang berbeda, dan bertugas membantu agar kedua jaringan tersebut dapat saling berkomunikasi. Terdiri dari dua komponen utama:

- Gateway Controller
  - mentranslasikan sebuah informasi ke dalam format yang dapat dimengerti oleh masing-masing jaringan
  - mentranslasikan SIP signaling di jaringan Internet ke SS7 signaling di jaringan PSTN atau sebaliknya
- Media Gateway
  - melakukan transcoding dari packet-based dijaringan IP ke dalam bentuk frame- frame TDM di PSTN atau sebaliknya

3. Media Server
   - Memproses RTP stream dari VoIP untuk mendekodekan nada DTMF, mencampur beberapa media stream ke dalam bentuk sebuah conference, membunyikan pengumuman, memproses script Voice XML, speech recognition, konversi text to speech, perekaman audio dan lain-lain.
   - Media ini bias diintegrasikan bersama gateway
4. Session control server
   - Menyediakan fungsi-fungsi level sesi, seperti otentikasi, otorisasi dan perijinan panggilan.
   - Me-rutekan dan mem-forward panggilan ke jaringan atau service provider yang lain.
   - Meyediakan layanan caller IP, call waiting dan dapat berinteraksi dengan server aplikasi. Merupakan komponen optional pada arsitektur VoIP, bias menjadi salah satu bagian dari gateway controller.
   - Juga bias dianggap sebagai SIP erver atau call agent

6.1.2.3.5 4 Layanan VoIP

Layanan VoIP dapat dibagi menjadi 4 layanan, yaitu sebagai berikut:

- Computer to Computer

Layanan ini merupakan layanan voice call yang menggunakan komputer sebagai alat komunikasi. Dengan menggunakan layanan khusus di internet kita bisa menggunakan komputer kita yang telah terhubung dengan internet untuk melakukan panggilan ke komputer lain yang menggunakan layanan yang sama. Banyak penyedia layanan VoIP di internet. Salah satu layanan yang mendukung panggilan suara melalui internet adalah Yahoo messenger. Dengan menggunakan Yahoo messenger kita bisa melakukan voice call dengan sesama user. Begitu juga penyedia layanan lainnya, seperti MSN messenger ataupun Skype. Layanan VoIP computer to computer dapat dilakukan secara gratis, anda hanya cukup menyediakan koneksi internet pada komputer anda.

- Computer to Phone

Layanan ini merupakan layanan yang memungkinkan kita melakukan panggilan dari komputer ke telepon, baik itu telepon tetap (PSTN) ataupun mobile phone (handphone). Layanan ini juga membutuhkan penyedia layanan di internet. Salah satu penyedia layanan ini adalah Skype. Layanan ini juga tidak gratis seperti layanan computer to computer VoIP, layanan ini membutuhkan biaya yang harus dibeli terlebih dahulu (sistem prabayar). Cara menggunakan layanan ini juga tidak sulit. Pertama, kita harus memiliki account di penyedia layanan terkait, biasanya membuat account tidak di pungut biaya. Lalu kita membeli credit atau bisa juga disebut pulsa, yang nantinya akan digunakan untuk melakukan panggilan ke telepon. Panggilan yang dilakukan tidak hanya ke nomor telepon lokal, namun panggilan dapat dilakukan untuk menghubungi nomor internasional di seluruh dunia. Dan juga, kita dapat melakukan panggilan baik ke telepon tetap ataupun handphone. Tarif yang digunakan mengacu pada penyedia layanan.

- Phone to Computer

Layanan VoIP call ini merupakan layanan yang memungkinkan anda melakukan panggilan dari telepon ke komputer. Lagi-lagi penyedia layanan yang mendukung layanan ini salah satunya adalah Skype. Saat kita mempunyai account skype, kita juga dapat mempunyai apa yang di sebut Online Number. Online number inilah yang nantinya dapat di hubungi dari telepon manapun.

- Phone to Phone

Layanan dilakukan dengan menggunakan pesawat telepon khusus atau telepon konvensional yang di hubungkan dengan VoIP adapter. Untuk menggunakan layanan ini kita harus menggunakan penyedia layanan phone to phone VoIP. Salah satu penyedia layanan ini adalah Phone Power. Dengan layanan ini kita dapat melakukan panggilan kemana pun diseluruh dunia yang menggunakan alat yang mendukung.

6.1.2.3.6 Quality of Service (QoS)

Alasan untuk mengadakan pengecekan QoS pada jaringan yaitu:

- VoIP bias dijalankan pada beberapa jenis jaringan yang punya karakteristik sendiri.
- Selain itu adanya transcoding pada gateway dimasing-masing jaringan menyebabkan VoIP sangat peka terhadap kondisi jaringan yang dilewati.
- Hal ini menyebabkan terjadinya penurunan kualitas informasi (suara, gambar maupun text) yang dibawa.

Beberapa parameter penentu kualitas layanan (QoS) pada VoIP adalah sebagai berikut:

1. Jitter
    - Merupakan variasi delay yang terjadi akibat adanya selisih waktu atau interval antar ke datangan paketd ipenerima.
    - Untuk mengatasi jitter maka paketd ata yang dating dikumpulkan dulu dalam jitter buffer selama waktu yang telah ditentukan sampai paket dapat diterima pada sisi penerima dengan urutan yang benar.
2. Delay
    - Waktu yang dibutuhkan untuk mengirimkan data dari sumber (pengirim) ketujuan (penerima).
    - Delay maksimum yang direkomendasikan oleh ITU untuk aplikasi suara adalah150 ms, dan yang masih bias diterima pengguna adalah 250 ms

Beberapa delay yang dapat mengganggu kualitas suara dalam VoIP:

- Propagation delay -delay yang terjadi akibat transmisi melalui jarak antar pengirim dan penerima
- Serialization delay -delay pada saat proses peletakan bit ke dalam circuit
- Processing delay -delay yang terjadi saat proses coding, compression, decompression dan decoding
- Packet ization delay -delay yang terjadi saat proses paket isasi digital voice sample
- Queuing delay -delay akibat waktu tunggu paket sampai dilayani
- Jitter buffer delay akibat adanya buffer untuk mengatasi jitter

3. Echo
    - Disebabkan perbedaan impedansi dari jaringan yang menggunakan four-wire dengan two-wire.
    - Efek echo adalah suatu efek yang dialami mendengar suara sendiri ketika sedang melakukan percakapan. Jika lebih dari 25 ms dapat

menyebabkan terhentinya pembicaraan.

4. Loss packet

Kehilangan paket ketika terjadi peak load dan congestion (kemacetan transmisi paket akibat padatnya traffic yang harus dilayani) dalam batas waktu tertentu.

6.1.2.4 Mengasosiasi/Menalar

Hasil penalaran pada prosedur pengamatan kerja sistem telekomunikasi adalah sebagai berikut:

1. Proses komunikasi diawali dengan sebuah pesan atau informasi yang harus dikirimkan dari individu/perangkat satu ke perangkat lain.
2. Pesan/informasi tersebut selanjutnya dikonfersi kedalam bentuk biner atau bit yang selanjutnya bit tersebut di encode menjadi sinyal. Proses ini terjadi pada perangkat encoder.
3. Sinyal tersebut kemudian oleh trans mitter dikirimkan/dipancarkan melalui media yang telah dipilih.
4. Dibutuhkan media transmisi (radio, optik, coaxial, tembaga) yang baik agar gangguan selama disaluran dapat dikurangi.
5. Selanjutnya sinyal tersebut diterima oleh stasiun penerima.
6. Sinyal tersebut didecode kedalam f ormat biner atau bit yang selanjutnya diubah kedalam pesan/i nformasi asli agar dapat dibaca/did engar oleh perangkat penerima.

Sedangkan untuk hasil penalaran pada pengamatan kerja sistem telekomunikasi pada VoIP, adalah sebagai berikut:

1. Transmission Control Protocol (TCP) merupakan protokol yang menjaga reliabilitas hubungan komunikasi end-to-end. Konsep dasar cara kerja TCP adalah mengirim dan menerima segmen–segmen informasi dengan panjang data bervariasi pada suatu datagram internet. Dalam hubungan VoIP, TCP digunakan pada saat signaling, TCP digunakan untuk menjamin setup suatu panggilan pada sesi signaling. TCP tidak digunakan dalam pengiriman data suara karena pada komunikasi data VoIP penanganan data yang mengalami keterlambatan lebih penting daripada penanganan paket yang hilang.
2. User Datagram Protocol (UDP) merupakan salah satu protocol utama diatas IP, yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas. UDP digunakan pada VoIP pada pengiriman audio streaming yang berlangsung terus menerus dan lebih mementingkan kecepatan pengiriman data agar tiba di tujuan tanpa memperhatikan adanya paket yang hilang walaupun mencapai 50% dari jumlah paket yang dikirimkan. Karena UDP mampu mengirimkan data streaming dengan cepat. Untuk mengurangi jumlah paket yang hilang saat pengiriman data (karena tidak

terdapat mekanisme pengiriman ulang) maka pada teknologi VoIP pengiriman data banyak dilakukan pada private network.

3. Internet Protocol (IP) Internet Protocol didesain untuk interkoneksi sistem komunikasi komputer pada jaringan paket switched. Pada jaringan TCP/IP, sebuah komputer di identifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan untuk mencegah kesalahan pada transfer data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat transfer data. Untuk komunikasi datanya, Internet Protokol mengimplementasikan dua fungsi dasar yaitu addressing dan fragmentasi. Salah satu hal penting dalam IP dalam pengiriman informasi adalah metode pengalamatan pengirim dan penerima.

6.1.3 Rangkuman

Berdasarkan gambar-gambar dan materi yang sudah dikumpulkan, maka para siswa dapat menyimpulkan beberapa hal:

1) Voice over Internet Protocol (juga disebut VoIP, IP Telephony, Internet telephony atau Digital Phone) adalah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet.
2) Data suara diubah menjadi kode digital dan dialirkan melalui jaringan yang mengirimkan paket-paket data, dan bukan lewat sirkuit analog telepon biasa.
3) Voice over Internet Protocol (VoIP) adalah teknologi yang mampu melewatkan trafik suara, video dan data yang berbentuk paket melalui jaringan IP.
4) Dalam komunikasi VoIP, pemakai melakukan hubungan telepon melalui terminal yang berupa PC atau telepon.
5) Kebutuhan perangkat VoIP: Hub, Router, ADSL Modem dan VoIP phone Adaptor
6) Softswitch merupakan sebuah sistem telekomunikasi masa depan yang mampu memenuhi kebutuhan pelanggan yaitu mampu memberikan layanan triple play sekaligus dimana layanan ini hanya mungkin dilakukan oleh sistem dengan jaringan yang maju seperti teknologi yang berbasis IP.
7) Prinsip kerja VoIP adalah mengubah suara analog yang didapatkan dari speaker pada Komputer menjadi paket data digital, kemudian dari PC diteruskan melalui Hub/ Router/ ADSL Modem dikirimkan melalui jaringan internet dan akan diterima oleh tempat tujuan melalui media yang sama.
8) Syarat-syarat dasar untuk mengadakan koneksi VoIP adalah komputer yang terhubung ke internet, mempunyai sound card yang

dihubungkan dengan speaker dan mikropon.

9) Bentuk hubungan tersebut bisa dalam bentuk pertukaran file, suara, gambar.
10) Penekanan utama dalam VoIP adalah hubungan keduanya dalam bentuk suara.
11) Sebuah sistem IP PBX terdiri dari satu atau lebih telepon SIP, server IP PBX dan secara opsional VOIP Gateway untuk terhubung ke jalur PSTN yang ada.
12) Fungsi PBX IP server mirip dengan cara kerja proxy server klien SIP, baik berupa software (softphone) atau perangkat keras berbasis ponsel, mendaftar ke server IP PBX, dan ketika mereka ingin membuat panggilan mereka meminta IP PBX untuk melakukan panggilan.
13) IP PBX memiliki daftar semua ponsel / pengguna dan alamat yang sesuai dengan SIP mereka dan dengan demikian dapat menghubungkan panggilan internal atau rute panggilan eksternal baik melalui gateway VOIP atau penyedia layanan VOIP.
14) Beberapa fungsi untuk men-support model komunikasi berbasis IP: Address Discovery, Device Interoperability, Interoperability dengan telepon PSTN dan Session-level Control
15) Alasan memilih Jaringan Internet
    - Jaringan IP sendiri merupakan jaringan komunikasi data yang berbasis packet-switched
    - Jaringan IP adalah jaringan global, tidak berdasarkan zona
    - Bisa menekan biaya percakapan
16) Infrastruktur Pendukung yaitu: Circuit-Switched, Packet-Switched
17) Fungsi-fungsi level Media: Interoperability antar Komponen
18) Komponen Fungsional VoIP adalah: Voice Calling Device, Gateway, Media Server dan Session control server.
19) Peralatan untuk membangkitkan dan menerima call.
20) Layanan VoIP dapat dibagi menjadi 4, yaitu :
    - Computer to Computer
        - Layanan ini merupakan layanan voice call yang menggunakan komputer sebagai alat komunikasi.
        - Salah satu layanan yang mendukung panggilan suara melalui internet adalah Yahoo messenger.
        - Layanan VoIP computer to computer dapat dilakukan secara gratis, anda hanya cukup menyediakan koneksi internet pada komputer anda.
    - Computer to Phone
        - Layanan ini merupakan layanan yang memungkinkan kita melakukan panggilan dari komputer ke telepon, baik itu telepon tetap (PSTN)

ataupun mobile phone (handphone).
- Layanan ini juga tidak gratis seperti layanan computer to computer VoIP, layanan ini membutuhkan biaya yang harus dibeli terlebih dahulu (sistem prabayar). Phone to Computer
- Layanan VoIP call ini merupakan layanan yang memungkinkan anda melakukan panggilan dari telepon ke komputer.

➢ Phone to Computer
- Layanan VoIP call ini merupakan layanan yang memungkinkan anda melakukan panggilan dari telepon ke komputer

➢ Phone to Phone
- Layanan dilakukan dengan menggunakan pesawat telepon khusus atau telepon konvensional yang di hubungkan dengan VoIP adapter.
- Untuk menggunakan layanan ini kita harus menggunakan penyedia layanan phone to phone VoIP.
- Salah satu penyedia layanan ini adalah Phone Power.

21) Kelebihan VoIP
- Di antaranya adalah dari segi biaya, jelas lebih murah dari tarif telepon tradisional.
- Selain itu, biaya maintenance dapat ditekan karena voice dan data network terpisah, sehingga IP Phone dapat ditambah, dipindah dan diubah.

22) QoS pada VoIP
- VoIP bisa dijalankan pada beberapa jenis jaringan yang punya karakteristik sendiri.
- Selain itu adanya transcoding pada gateway dimasing-masing jaringan menyebabkan VoIP sangat peka terhadap kondisi jaringan yang dilewati.
- Hal ini menyebabkan terjadinya penurunan kualitas informasi (suara, gambar maupun text) yang dibawa.

23) Beberapa parameter penentu Kualitas Layanan(QoS) dari VoIP adalah:

➢ Jitter
- Merupakan variasi delay yang terjadi akibat adanya selisih waktu atau interval antar ke datangan paketd ipenerima.
- Untuk mengatasi jitter maka paketd ata yang dating dikumpulkan dulu dalam jitter buffer selama waktu yang telah ditentukan sampai paket dapat diterima pada sisi penerima dengan urutan yang benar.

➢ Delay

- Waktu yang dibutuhkan untuk mengirimkan data dari sumber (pengirim) ketujuan (penerima).
- Delay maksimum yang direkomendasikan oleh ITU untuk aplikasi suara adalah150 ms, dan yang masih bias diterima pengguna adalah 250 ms
- Beberapa delay yang dapat mengganggu kualitas suara dalam VoIP:
  - Propagation delay - delay yang terjadi akibat transmisi melalui jarak antar pengirim dan penerima
  - Serialization delay - delay pada saat proses peletakan bit ke dalam circuit
  - Processing delay - delay yang terjadi saat proses coding, compression, decompression dan decoding
  - Packet ization delay - delay yang terjadi saat proses paket isasi digital voice sample
  - Queuing delay -delay akibat waktu tunggu paket sampai dilayani
  - Jitter buffer delay akibat adanya buffer untuk mengatasi jitter

➢ Echo
- Disebabkan perbedaan impedansi dari jaringan yang menggunakan four-wire dengan two-wire.
- Efek echo adalah suatu efek yang dialami mendengar suara sendiri ketika sedang melakukan percakapan. Jika lebih dari 25 ms dapat menyebabkan terhentinya pembicaraan.

➢ Loss packet
- Kehilangan paket ketika terjadi peak load dan congestion (kemacetan transmisi paket akibat padatnya traffic yang harus dilayani) dalam batas waktu tertentu.

24) Pengujian Sisi Server

No	Nama Pengujian	Indikator Pengujian	Status Pengujian
1	Komputer Server Booting dengan normal	Muncul halaman login pada layar monitor	Muncul halaman login
2	Komputer Server dapat dikonfigurasi melalui remote web base	Muncul tampilan pada web browsure halaman Briker user mode	Muncul halaman Briker user mode

25) Pengujian pada Sisi Client

No	Nama Pengujian	Indikator Pengujian	Status Pengujian
1	VoIP client sudah ter- install dengan benar	Akan muncul program VoIP client pada yaitu X-lite Softphone	Softphone bisa dijalankan dan di konfigurasi
2	VoIP client sudah tergister ke server	Pada softphone akan muncul username dan status ready	Softphone bisa melakukan dan menerima panggilan

Berdasarkan pengamatan dan analisa system kerja system VoIP, maka dapat disimpulkan

- VoIP server mempunyai webbase yang bisa dibuka melalui panggilan IP server pada brwoser sehingga memudahkan admin dalam melakukan konfigurasi dan menambah user account.
- VoIP server berperan menangani panggilan SIP dari seluruh client yang teregister ke dalam server.
- Antara VoIP client dapat saling berkomunikasi dua arah ketika sudah teregister ke dalam server VoIP dan juga dapat melakukan panggilan video call.
- Penggunaan VoIP merupakan solusi alternatif komunikasi masa depan, oleh karena itu untuk pengembangan selanjutnya dapat dilakukan analisis performansi VoIP dengan VoIP monitoring dan sistem VoIP ini dapat dikembangkan dengan telepon analog sehingga komunikasi akan lebih murah.

6.1.4 Tugas

Tugas

Melakukan pengamatan pada prosedur kerja pada sistem komunikasi VoIP serta menyajikan hasil analisa prosedur pengamatan kerja sistem komunikasi VoIP.

Langkah Kerja

1. Buatlah kelompok dengan anggota 3 – 4 orang.
2. Uraikan pengamatan kelompok tentang TCP!
3. Uraikan pengamatan kelompok tentang UDP!
4. Uraikan pengamatan kelompok tentang IP!
5. Jika ingin menambahkan 1 client pada sistem VoIP, konfigurasi apa saja yang harus dilakukan?
6. Buat laporan dan diskusikan dengan teman sekelompok.

Bandingkan dan Simpulkan

Presentasikan hasil kerja kelompok anda di depan kelas dan bandingkan hasil kerja kelompok Anda dengan kelompok lain.

Berdasarkan hasil perbandingan tersebut hal penting apa yang harus dirumuskan secara bersama.

6.1.5 Penilaian Diri

Dalam test ini setiap anda harus membaca dengan cermat dan teliti setiap butir soal dibawah ini. Kemudian berdasarkan uraian materi diatas tulislah jawabannya pada lembar kerja penilaian diri yang telah disediakan.

1) Tuliskan kepanjangan VoIP dan jelaskan apa yang anda ketahui tentang VoIP!
2) Jelaskan cara kerja VoIP secara singkat!
3) Tuliskan kebutuhan perangkat VoIP dan syarat dasar untuk mengadakan koneksi VoIP!
4) Apa sajakah yang termasuk pada :
    a. Infrastruktur Pendukung VoIP
    b. Fungsi level Media
    c. Komponen Fungsional VoIP
5) Jelaskan kategori layanan VoIP di bawah ini:

a. Computer to Computer
b. Computer to Phone
c. Phone to Computer
d. Phone to Phone

6) Jelaskan bagaimanakah parameter penentu Kualitas Layanan(QoS) dari VoIP!

Lembar Kerja Penilaian Diri

LJ- 01: Kepanjangan VoIP:

……...
……...
……...
……...

LJ- 02: Cara kerja VoIP:

……...
……...
……...
……...

LJ- 03: Perangkat VoIP dan syarat dasar untuk mengadakan koneksi VoIP:

……...
……...
……...
……...

LJ- 04.a): Infranstruktur pendukung VoIP:

……...
……...
……...
……...

LJ- 04.b): Fungsi level media:

……...
……...
……...
……...

LJ- 04.c): Komponen Fungsional VoIP:

……...
……...
……...
……...

LJ- 05.a): Computer to Computer:

……...

……...

……...

……...

LJ- 05.b): Computer to Phone:

……...

……...

……...

……...

LJ- 05.c): Phone to Computer:

……...

……...

……...

……...

LJ- 05.d): Phone to Phone:

……...

……...

……...

……...

LJ- 06: parameter penentu Kualitas Layanan (QoS) dari VoIP:

……...

……...

……...

……..

DAFTAR PUSTAKA

Banerjee, K. (2005). *SIP Introduction*. Retrieved November 1, 2014, from eMultimedia: http://www.siptutorial.net/SIP/

Covington, G. A. (2006). *Voice over Wireless Data Network.* Washington: Washington University in St. Louise.

Fauzy, R., & Suherman. (2006). *Jaringan Telekomunikasi Masa Depan (Next Generation Network - NGN).* Medan: Departemen Teknik Elektro Universitas Sumatera Utara.

J.Rosenberg, H.Schulzrinn, G.Camarillo, A.Johnston, J.Peterson, R.Sparks, et al. (2002). SIP: Session Initiation Protocol. *RFC 3261* .

Kementerian Pendidikan dan Kebudayaan. (2012). Sistem Keamanan Jaringan (Firewall). In D. P. SMK, *Teknik Komputer dan Jaringan* (pp. 453-476).

Mitchell, B. (2014). *SIP - Session Initial Protocol*. Retrieved November 2, 2014, from CompNetworking: http://compnetworking.about.com/od/voipvoiceoverip/g/bldef_sip.htm

Mulyana, E., & Purbo, O. W. *Firewall: Internet Security.* Bandung: Computer Network Research Group ITB.

Munadi, R. (2009, Desember 28). *Kapasity Softswitch.* Retrieved Oktober 27, 2014, from http://www.rendymunadi.wordpress.com

Munadi, R. (2009, Desember 21). *New Era of Softswitch.* Retrieved Oktober 27, 2014, from http://www.rendymunadi.wordpress.com

Munadi, R. (2009, Desember 28). *Softswitch dan Aplikasi.* Retrieved Oktober 27, 2014, from http://www.rendymunadi.wordpress.com

Munadi, R. (2009, Desember 28). *Softswitch Layanan dan Aplikasi.* Retrieved Oktober 27, 2014, from http://www.rendymunadi.wordpress.com

Navora, S. (2012, Maret 6). *Mengapa Softswitch dibutuhkan? .* Retrieved Oktober 26, 2014, from SMKTelkom Study Zone: http://smktelkomzone.blogspot.com/2012/03/mengapa-softswitch-dibutuhkan.html

Purbo, O. W. (2007). *Instalasi Softswitch SIP.* Jakarta.

Setiawan, D. *kombinasi Firewall di OSI Layer.* Fasilkom UNSRI.

Stallings, W. (2003). *The Session Initial Protocol*. Retrieved November 2, 2014, from Cisco: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/sip.html

Sudiarta, P. K., & Sukadermi, G. (2009). Penerapan Teknologi VoIP untuk mengoptimalkan Penggunaan Jaringan Intranet Kampus Universitas Udayana. *Teknologi Elektro* , 62-70.

Tharom, T. (2002). *Teknis dan Bisnis VoIP.* Jakarta: PT. Alex Media Komputindo.

GLOSARIUM

Application Server adalah elemen jaringan yang menyediakan aplikasi tambahan di luar fitur teleponi yang membutuhkan server tersendiri, misalnya voice mail, prepaid call, fixed-SMS, voice VPN, dll.

Bandwidth adalah suatu ukuran dari banyaknya informasi yang dapat mengalir dari suatu tempat ke tempat lain dalam suatu waktu tertentu. Bandwidth dapat dipakai untuk mengukur baik aliran data analog maupun aliran data digital.

Briker merupakan IPPBX yang berbentuk software atau sistem operasi Linux yang dikhususkan untuk layanan VoIP.

Feature Server adalah elemen jaringan yang berfungsi sebagai penyedia aplikasi fitur teleponi.

Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar.

Internet Protocol (IP) merupakan suatu protokol didesain untuk interkoneksi sistem komunikasi komputer pada jaringan paket switched.

IP MASQUERADE adalah salah satu bentuk translasi alamat jaringan (NAT), yang memungkinkan bagi komputer-komputer yang terhubung dalam jaringan lokal yang menggunakan alamat IP privat untu berkomunikasi ke internet melalui firewall.

Media Gateway adalah elemen jaringan yang berfungsi sebagai elemen transport untuk merutekan trafik dalam jaringan softswitch dan juga mengirim atau menerima trafik dari jaringan lain yang berbeda, seperti PSTN, PLMN, dan jaringan akses pelanggan.

Media Server adalah elemen jaringan berfungsi membantu Softswitch untuk mendukung layanan/aplikasi seperti messaging, audio dan video conferencing, music on hold, announcement, dll.

Operating Support System (OSS) adalah elemen jaringan yang berfungsi untuk mendukung operasi dan pemeliharaan jaringan, seperti manajemen jaringan, provisioning, billing, monitoring, statistik, dll.

PBX adalah sebuah sentral privat dengan fitur seperti sentral public yang di gunakan oleh suatu lembaga / perusahaan dalam melayani komunikasai internet perusahaan tersebut

Proxy adalah suatu server yang menyediakan layanan untuk meneruskan setiap permintaan kita kepada server lain di internet.

RFC (**Request for Comment**) merupakan salah satu dari seri dokumen infomasi dan standar Internet bernomor yang diikuti secara luas oleh perangkat lunakuntuk digunakan dalam jaringan, Internet dan beberapa sistem operasi jaringan, mulai dari Unix, Windows, dan Novell NetWare.

Session Description Protocol (SDP) yaitu konten yang menggambarkan isi dari sesi, termasuk telepon, radio internet, dan aplikasi multimedia.

Signaling Gateway adalah elemen jaringan yang berfungsi sebagai interface pensinyalan dari jaringan sofswitch ke SS7 PSTN atau PLMN.

SIP (Session Initial Protocol) adalah protokol yang digunakan untuk inisiasi, modifikasi dan terminasi sesi komunikasi VoIP.

Subscriber merupakan teknologi yang menyediakan penghantar data digital melewati kabel yang digunakan dalam jarak dekat dari jaringan telepon setempat.

Transmission Control Protocol (TCP) merupakan protokol yang menjaga reliabilitas hubungan komunikasi end- to-end.

Troughput adalah bandwidth yang sebenarnya (aktual) yang diukur dengan satuan waktu tertentu dan pada kondisi jaringan tertentu yang digunakan untuk melakukan transfer file dengan ukuran tertentu.

User Datagram Protocol (UDP) merupakan salah satu protocol utama diatas IP, yang lebih sederhana dibandingkan dengan TCP.

VOIP (Voice Over Internet Protocol) atau biasa disebut digital phone merupakan salah satu bagian dari teknologi transmisi untuk mentransmisikan komunikasi suara melalui IP, seperti internet ataupun packet-switched networks.

INDEKS

KOMUNIKASI DATA

Paket Keahlian Teknik Komputer dan Jaringan

Komunikasi Data merupakan salah satu mata pelajaran paket Teknik Komputer dan Jaringan (TKJ) pada program keahlian Teknik Komputer dan Informatika (TKI) Berdasarkan struktur kurikulum mata pelajaran Komunikasi Data disampaikan di kelas XI semester 1 dan 2 Sekolah Menengah Kejuruan, masing-masing 4 jam pelajaran untuk setiap pertemuan kelas.

Buku ini merupakan panduan untuk para siswa memahami Komunikasi Data pada semester 2 sehingga dapat menerapkannya dalam real work pada sistem Jaringan Komputer. Buku ini menggunakan pendekatan Scientifik yang merupakan cerminan dari kurikulum 2013. Pokok Pahasan yang akan dibahas pada buku ini adalah sebagai berikut:

1) Prosedur Instalasi Server Softswitch berbasis SIP
2) Konfigurasi Ekstensi dan Dial-Plan Server Softwitch
3) Fungsi Firewall pada Jaringan VoIP
4) Prinsip kerja subscriber Internet Telepon
5) Konfigurasi pada subscriber internet telepon, dan
6) Prosedur Pengamatan Kerja

BARCODE

ISBN