BAB II
TINJAUAN PUSTAKA

2.1. Global System for Mobile Communication (GSM)

Global System for Mobile Communication atau GSM merupakan generasi kedua (2G) dari standar sistem seluler yang dikembangkan oleh sekelompok pengembang di Eropa, yang menetapkan protokol standar telekomunikasi transmisi suara dan data antara telepon genggam dan perangkat bergerak lainnya. Tidak seperti generasi pertama yang masih bersifat analog, transmisi GSM sudah bersifat digital dan berbasis pada teknik modulasi TDMA.

Gambar 2.1. Simbol GSM
(Sumber: wikipedia.org)

Jaringan GSM beroperasi di beberapa *band* frekuensi, termasuk di antaranya pada frekuensi 900 MHz dan 1.8 GHz di Eropa dan 850 MHz dan 1.9 GHz di Amerika Serikat dan Kanada. Teknologi TDMA GSM berdasar pada sistem *circuit-switched* yang membagi setiap *channel* 200 kHz ke dalam delapan *time slot.* GSM memiliki kemampuan untuk mentransmisikan informasi hingga kecepatan dari 64 kbps hingga 120 Mbps.

Dibanding dengan jaringan *mobile* generasi pertama yang masih bersifat analog, jaringan GSM sebagai generasi kedua memiliki keuntungan-keuntungan seperti berikut:

- Percakapan via suara yang sudah terenkripsi;

- Penggunaan spektrum frekuensi radio yang lebih efisien, sehingga membuat setiap *band* frekuensi dapat digunakan oleh banyak pengguna;
- Telah menyediakan layanan data, seperti SMS, dan tidak hanya menyediakan layanan suara saja.

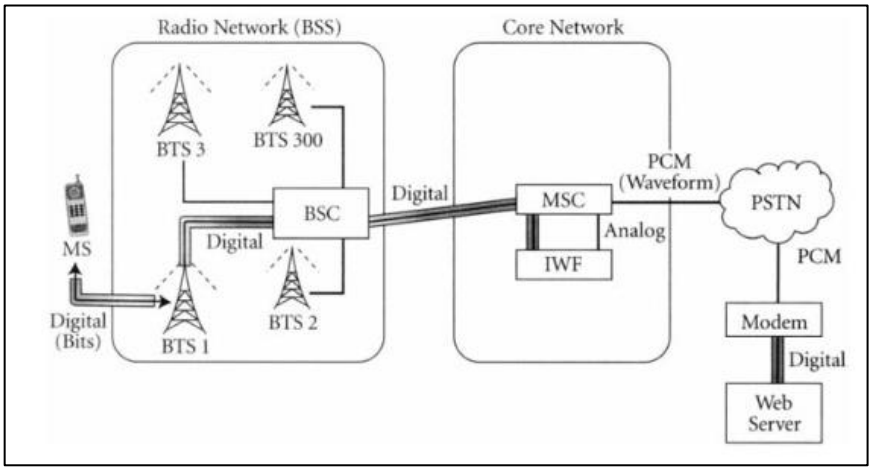
Teknologi 2G membuat penyedia jaringan mampu memberikan layanan yang beragam, seperti pesan teks, pesan gambar, dan MMS (*multimedia message service*). Semua pesan yang dikirim melalui sistem 2G telah dienkripsi secara digital, membuat transmisi data hanya bisa diterima dan dilihat oleh penerima yang seharusnya.

Sistem GSM memanfaatkan SIM atau *Subscriber Identity Module*. Sistem SIM membuat beragam layanan dapat dipersonalisasikan sesuai keinginan pengguna hanya dengan satu buah perangkat bergerak. Kartu SIM menyimpan informasi mengenai pelanggan, seperti identitas dan kontak telepon. Kartu SIM ini bisa digunakan di berbagai perangkat yang sesuai, sehingga pengguna bisa menggunakan layanan yang sama pada perangkat yang berbeda. Terlebih lagi, kartu SIM sudah diprogram dengan parameter-parameter keamanan, sehingga komunikasi antar infrastruktur dapat dilakukan secara aman. Kartu SIM juga menimpan informasi mengenai jaringan seluler (lokasi area) yang digunakan oleh pengguna yang bergerak di dalam wilayah layanan.

2.1.1. Arsitektur Jaringan GSM

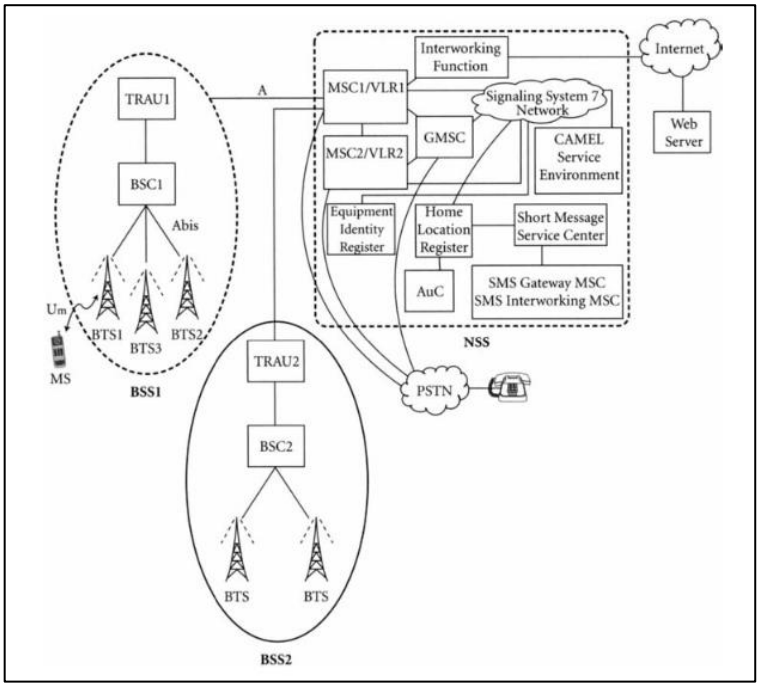
Sistem jaringan berbasis GSM terdiri dari jaringan akses radio yang disebut BSS (Base Station System) dan jaringan inti yang disebut dengan NSS (Network Switching System). Perbedaan utama antara peralatan bergerak/*mobile equipment* (ME) dan stasiun bergerak/*mobile station* (MS) adalah MS adalah istilah untuk menyebut ME (peralatannya) dan kartu SIM yang ada di dalamnya.

Gambar di bawah ini mengilustrasikan arsitektur level tinggi dari sebuah PLMN (Public Land Mobile Network) GSM.



Gambar 2.2. Arsitektur Sistem GSM

(Sumber: GSM and Personal Communication Handbook, 1998)



Gambar 2.3. Arsitektur PLMN GSM

(Sumber: GSM and Personal Communication Handbook, 1998)

Sebuah BSS terdiri dari sebuah Base Station Controller (BSC), TRAU (Transcorder Rate Adaptation Unit), dan sejumlah Base Transceiver Stations (BTS). MS berkomunikasi dengan BTS menggunakan teknik TDMA berbasis *air interface* yang disebut *Um Interface.* Secara umum, sebuah BTS mengendalikan

satu buah sell, yang mana bisa jadi berupa sel omnidirectional atau sebuah sektor 120°. Dalam praktiknya, satu buah BTS dapat mengatur sejumlah sel sekaligus (contoh: tiga buah sel dengan sektrorisasi 120°). BTS menerima sinyal dari MS melalui sejumlah transceiver yang mendukung saluran radio dengan frekuensi 200 kHz dan *frame* delapan slot waktu.

Satu buah BSC dapat mengontrol ratusan BTS, tergantung pada kapasitas BSC. *Interface* antara BTS dan BSC disebut sebagai Abis interface. Walaupun pada dasarnya dapat menggunakan medium perambatan apa saja, dalam Abis Interface tautan T1/E1 lebih umum digunakan. Tarkadang frekuensi *microwave* juga digunakan sebagai medium untuk mengimplementasikan Abis Interface nirkabel. Sebuah BSC terhubung ke TRAU, yang melaksanakan konversi *data rate* antara BSC dan NSS. Keberadaan NSS sangat berpengaruh dalam fungsi-fungsi seperti otentifikasi, *routing* panggilan, *billing*, dan juga layanan SMS. Beberapa *core network* menggunakan Signaling System 7 (SS7) untuk melakukan pertukaran sinyal pesan.

Sedangkan di dalam jaringan inti, sebuah NSS (yang terdiri dari berbagai macam peralatan dengan fungsinya masing-masing) dapat mendukung nyaris semua macam layanan data.

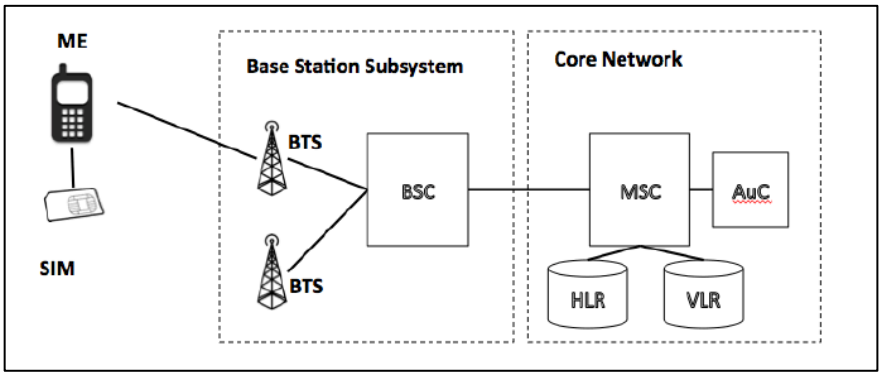
Home Location Register (HLR) merupakan *database* pusat yang menyimpan informasi mengenai setiap pelanggan. Sebuah operator layanan yang bekerja secara nasional bisa saja memiliki satu buah HLR utama dengan sejumlah HLR cabang yang tersebar secara merata di setiap daerah. HLR-HLR ini menyimpan informasi yang sama dan terus saling memperbaharui dalam jaringan berkecepatan tinggi. Jumlah HLR yang dimiliki oleh penyedia layanan tergantung atas beberapa faktor, di antaranya yaitu jumlah pelanggan, kapasitas peralatan, dan sasaran *delay*. Informmasi yang disimpan di dalam HLR yaitu termasuk informasi pengguna, batasan layanan, layanan tambahan, lokasi pengguna, nommor IMSI (Internasional Mobile Subscriber Identitiy), dan nomor ISDN MS.

VLR (Visitor Location Register) melacak keberadaan sebuah MS di dalam wilayah geografis yang dapat dijangkau oleh VLR tersebut, dan mengirimkan pembaharuan lokasi MS sebelum melakukan panggilan untuk memastikan BTS mana yang digunakan.

Authentication Center (AuC) menyimpan datra pengguna, dan berfungsi dalam otentifikasi dan enkripsi jalur radio antara MS dan BSC. AuC biasanya terintegrasi di dalam HLR.

a. Base Transceiver Station (BTS)

Di dalam arsitektur jaringan GSM, terdapat sebuah infrastruktur telekomunikasi yang disebut dengan *Base Transceiver Station* (BTS). BTS ini memiliki fungsi untuk menerima dan mengirimkan sinyal radio antara perangkat pelanggan *(mobile station)* dan penyedia layanan atau operator.

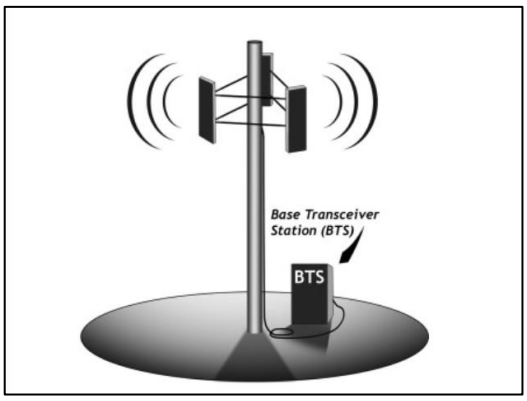


Gambar 2.4. Posisi BTS dalam Arsitektur Jaringan GSM
(Sumber: Security Issues and Attack on the GSM Standard, 2013)

Dalam jaringan GSM, BTS bertugas untuk meng-*cover* suatu wilayah cakupan yang disebut sebagai *cell.* BTS mengatur lalu lintas komunikasi radio antar telepon selular dan komunikasi antara telepon selular tanpa kabel dengan telepon rumah yang berbasis *fixed line.*

Sebuah BTS terhubung ke jaringan telepon rumah melalui sebuah RNC *(Rado Network Controller).* RNC ini mengatur sejumlah BTS secara sekaligus. RNC juga terhubung ke MSC (*Mobile Switching Center)* yang bertugas mengatur

BTS-BTS dan *cell-cell* yang berada dalam satu wilayah pemasaran. Pada dasarnya, istilah BTS mencakup *tower,* antena pemancarnya, dan stasiun transceiver.



Gambar 2.5. Bagian-bagian BTS
(Sumber: sciencedirect.com)

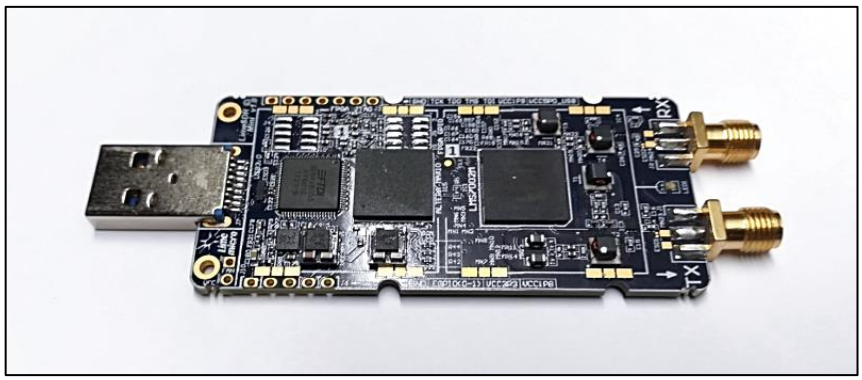
2.2. Software Defined Radio (SDR)

Teknologi radio adalah teknologi yang mengizinkan dua buah perangkat untuk mengirim dan menerima informasi secara nirkabel menggunakan radiasi elektromagnetik. Dulu, radio dibuat dengan menggunakan berbagai rangkaian komponen dan perangkat keras. Di era sekarang, fungsi komponen dan perangkat keras tersebut dapat digantikan oleh perangkat lunak yang ada di dalam sebuah perangkat komputer.

SDR Forum bersama IEEE mendefinisikan *Software Defined Radio* sebagai sebuah radio dimana sebagian besar semua fungsi fisiknya telah digantikan atau disimulasikan menggunakan *software.*

Radio adalah segala jenis perangkat yang mampu mentransmisikan dan menerima sinyal frekuensi radio (RF) pada gelombang elektromagnetik untuk memfasilitasi pertukaran informasi, seperti ponsel, komputer, atau televisi. Perangkat radio generasi terdahulu memiliki keterbatasan berupa ketergantungan terhadap *hardware,* sehingga menimbulkan biaya produksi yang tinggi serta fleksibilitas yang rendah. SDR adalah teknologi yang dikembangkan untuk

mengatasi masalah ini, dengan memberikan teknologi radio yang relatif lebih terjangkau, efisien, dan lebih fleksibel karena mengizinkan *upgrade* atau pengembangan via perangkat lunak saja tanpa perlu memodifikasi *hardware*-nya.



Gambar 2.6. LimeSDR, contoh *software defined radio*
(Sumber: hackaday.com)

Secara umum, SDR terdiri dari rangkaian *hardware* dan *software* dimana fungsi dan kemampuan operasi radionya dapat dikembangkan dan diimplementasikan melalui *software* dan *firmware* yang dapat dimodifikasi dengan mudah. Perangkat SDR umumnya mencakup FPGA (*Field Programmable Gate Arrays),* DSP *(Digital Signal Processors),* GGP *(General Purpose Processor),* dan SoC (*System on Chip)* yang *programmable.* Penggunaan teknologi-teknologi terseut bertujuan agar pengembangan fungsi radio dapat dilakukan tanpa memerlukan penambahan *hardware* baru.

Beberapa keuntungan yang dapat diberikan oleh SDR untuk manufaktur perangkat dan penyedia layanan radio, di antaranya:

- Dapat diimplementasikan dengan cepat untuk menghasilkan produk baru;
- Menyediakan beragam *software* yang sudah jadi/tersedia, sehingga mampu mengurangi biaya pengembangan;
- Dapat diprogram secara *remote,* sehingga bisa mengurangi biaya dan tenaga *maintenance* untuk perbaikan;
- Dapat dikembangkan tanpa memerlukan penambahan fisik infrastruktur.

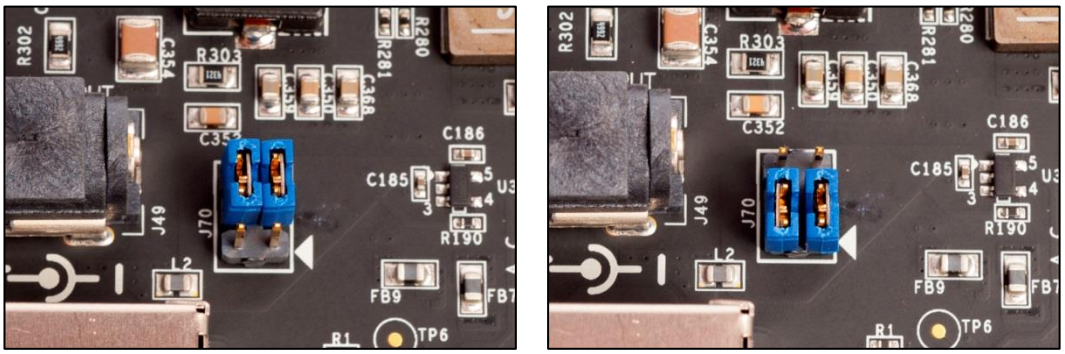
2.2.1. Nuand BladeRF x40

BladeRF x40 merupakan *software-defined radio* berbasis USB 3.0 yang dibuat oleh Nuand. Perangkat ini dapat mengakses frekuensi dari 300 MHz hingga 3.8 GHz tanpa memerlukan perangkat tambahan lainnya. Menggunakan perangkat lunak *open source* seperti GNURadio, BladeRF dapat langsung digunakan.

Dengan perangkat keras dan lunak yang fleksibel, BladeRF dapat dikonfigurasikan untuk berfungsi sebagai modem RF, *picocell* GSM dan LTE, penerima sinyal GPS, transmitter ATSC, atau bahkan perpaduan penerima sinyal Bluetooth/wifi tanpa memerlukan *expansion card. Software* dan *firmware* BladeRF pun semuanya tersedia secara *open source.*

Gambar 2.7. Perangkat SDR Nuand BladeRF x40
(Sumber: nuand.com)

Nuand BladeRF x40 ditenagai oleh tegangan 5V. Tegangan ini bisa kita dapatkan dengan menghubungkan BladeRF x40 dengan *adaptor* 5V yang memiliki kemampuan arus 1.5 hingga 3A melalui *port* DC *barrel jack* yang ada di badan BladeRF. Perangkat ini juga dapat ditenagai oleh tegangan USB, namun untuk melakukannya, kita harus mengganti posisi *jumper* J70. Untuk menggunakan tegangan dari USB, *jumper* J70 menghubungkan pin 2 dan 3 dan pin 4 dan 5. Untuk menggunakan tegangan dari *adaptor* eksternal, *jumper* tersebut dipindahkan untuk menghubungkan pin 1 dan 2 serta pin 5 dan 6.

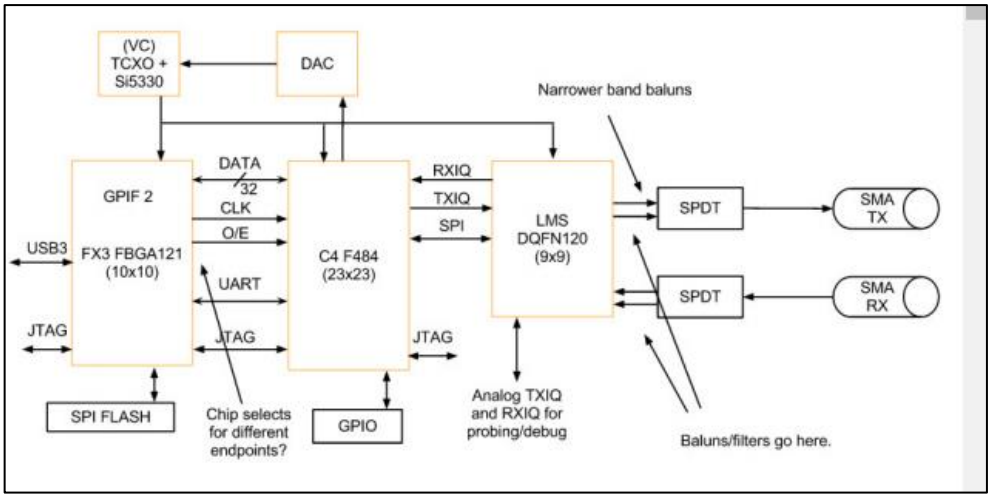


(a) (b)

Gambar 2.8. Konfigurasi pin untuk: (a). Sumber tegangan dari USB. (b). Sumber tegangan dari DC *supply*.

Beberapa *hardware* yang merupakan bagian dari *board* SDR Nuand BladeRF di antaranya adalah:

- Si5338 *clock generator* untuk menghasilkan *sample rate* sesuai kebutuhan;
- Lime *microsystems* LMS6002D;
- Altera Cyclone IV E (40kLE or 115kLE) FPGA untuk pemrosesan dan kontrol sinyal;
- Cypress FX3 USB3 Superspeed Microcontroller.



Gambar 2.9. Diagram blok perangkat Nuand BladeRF

(Sumber: nuand.com)

Dengan *hardware* seperti speifikasi di atas, BladeRF x40 mampu menyediakan beragam fitur sesuai kebutuhan. Fitur-fitur yang disediakan di antaranya adalah sebagai berikut:

- *Frequency range* dari 300 MHz hingga 3.8 GHz;
- Jalur sinyal RX dan TX yang independen, mendukung operasi *half* dan *full duplex,* akses langsung ke pin analog ADC/DAC, serta *pre-module setting* untuk pengaturan frekuensi, *sample rate, bandwidth,* dan *gain*;
- Mendukung USB 3.0, *backward compatible* dengan USB 2.0;
- Didukung oleh beragam *software third-party* populer seperti GNU Radio gr-osmosdr, Prothos SoapySDR, SDRangel, SDR Console, SDR# via sdrsharp-bladeRF, dan Mathwork MATLAB dan Simulink via libbladeRF *bindings*;
- *Bandwidth* instan hingga 28 MHz;
- *Arbitary sample rate* hingga 40 MSPS;
- *Factory-calibrated* 1 PPM VCTCXO;
- FPGA Altera Cyclone IV;
- Dapat dikustomisasikan dengan 32 I/O *pin,* konektor JTAG, konektor SMB untuk konfigurasi MIMO, dan *triggered muti-device sampling synchronization;*
- Dapat digunakan untuk beragam aplikasi, dari *modem* kustom, pengembangan *waveform, wireless video,* simulasi GPS, *whitespace exploration,* dan simulasi ADSB.

Parameter	Min	Typ	Max	Unit
RF Specifications				
ADC/DAC Sample Rate	0.160		40	MHz
ADC/DAC Resolution		12		bits
VCTCXO Accuracy		1		ppm
RF Tuning Range	300		3800	MHz
RF Bandwidth Filter	1.5		28	MHz
CW Output Power		+6		dBm
FPGA Specifications				
Logic Elements	39,600		114,480	LE
Embedded 18x18 Multipliers	116		266	
BRAM	1,134		3,888	kbits
Physical Specifications				
Dimensions		8.7 x 13.1 x 1.8		cm
Weight		80		g
Operating Temp: x40/x115	0		70	°C
Operating Temp: x115 Thermal	-40		85	°C

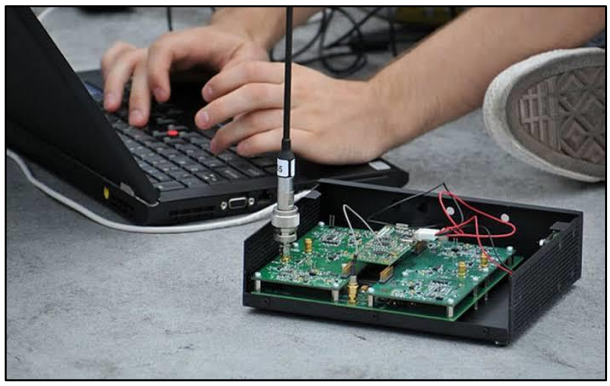
Add-on Options	
XB-100 GPIO Board	GPIO breakout with LEDs and DIP switches
XB-200 Transverter	600 kHz to 300 MHz transverter with VHF filterbank, custom filter path, and bypass mode
Case	Clear polycarbonate case for the bladeRF x40 or bladeRF x115

Gambar 2.10. Spesifikasi BladeRF

2.3. OpenBTS

OpenBTS memiliki fungsi yang sama dengan BTS GSM umumnya, namun berbasis pada *software open-source.* OpenBTS memungkinkan telepon genggam GSM untuk dapat menggunakan layanan telepon tanpa melalui jaringan operator selular komersial.

OpenBTS mensimulasikan infrastruktur operator GSM dari BTS ke belakang. Trafik telekomunikasi yang umumnya diteruskan dari *user* ke BTS kemudian ke *Mobile Switching Center* (MSC) pada OpenBTS trafik justru diterminasikan pada perangkat yang sama dengan cara mem-*forward* data ke Asterisk PBX melalui VoIP.



Gambar 2.11. Contoh Perangkat OpenBTS

(Sumber: telset.id)

OpenBTS merupakan sebuah aplikasi *open source* yang berjalan pada *platform* Linux yang bekerja sebagai sebuah perangkat *downsizing* dari BTS pada umumnya, dan bekerja menggunakan bantuan perangkat keras yang disebut USRP (*Universal Software Radio Peripheral)* untuk memancarkan dan menerima sinyal jaringan GSM. OpenBTS memanfaatkan program Asterisk sebagai pengganti MSC pada sistem GSM pada umumnya untuk mentransmisikan suara, dan menggunakan aplikasi Jabber untuk memfasilitasi fitur SMS.

2.3.1. YateBTS

YateBTS merupakan implementasi perangkat lunak dari jaringan akses radio GSM/GPRS yang berbasis pada Yate (Yet Another Telephony Engine), sebuah perangkat lunak *open source* yang berfungsi untuk melakukan komunikasi baik via suara, video, atau pun pesan singkat. YateBTS berfungsi untuk menerima sinyal GSM yang datang dari perangkat *mobile* pengguna, dan mengirimkannya melalui koneksi VoIP.

Gambar 2.12. Logo YateBTS

(Sumber: yatebts.com)

Saat menggunakan jaringan YateBTS, sinyal GSM yang diterima oleh antena yang terhubung dengan YateBTS akan diproses oleh aplikasi Yate. Yate kemudian memproses koneksi yang datang tersebut melalui protokol yang diperlukan untuk berkomunikasi dengan pihak yang ingin kita tuju.

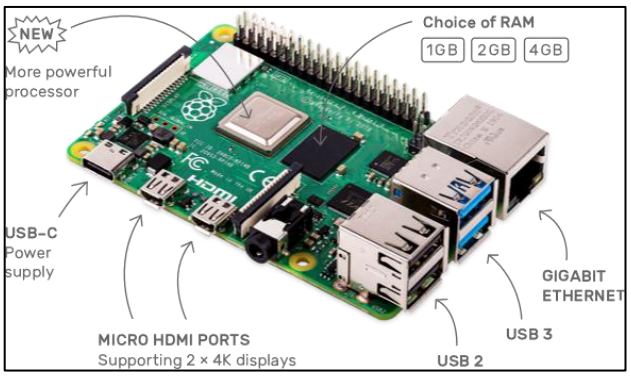
YateBTS dapat dikonfigurasikan untuk bekerja pada dua mode. Kedua mode tersebut adalah sebagai berikut:

- Mode Jaringan PC (*Network in a PC (NiPC) Mode)*, di mana YateBTS bekerja sebagai jaringan GSM/GPRS tersendiri dan terhubung ke luar menggunakan VoIP.
- *Radio Access Network (*RAN*)* Mode, dimana YateBTS bekerja sebagai sebuah bagian dari jaringan GSM/GPRS yang lebih besar, seperti YateUCN atau jaringan NiPC lain.

2.4. Raspberry Pi

Raspberry Pi, sering juga disebut *RPi* atau *Raspi*, merupakan perangkat komputer mini yang berbasis pada satu buah *board* tunggal yang dikembangkan oleh sekelompok pengembang yang tergabung dalam Raspberry Pi Foundation di Inggris dengan tujuan awal membantu pelajar untuk mempelajari dasar-dasar ilmu komputer.

Raspberry Pi pertama kali diluncurkan pada tahun 2012, dan telah mengalami perubahan pesat melalui beragam versi produk. Raspberry Pi yang dirilis pertama kali memiliki CPU *single-core* 700 MHz dan RAM yang hanya sebesar 256 MB. Raspberry Pi merupakan komputer mini yang bekerja pada *platform* Linux, namun juga menyediakan beberapa *set* GPIO (*General Purpose Input/Output)* yang dapat digunakan untuk mengontrol komponen elektronik seperti untuk implementasi *Internet of Things* (IoT).

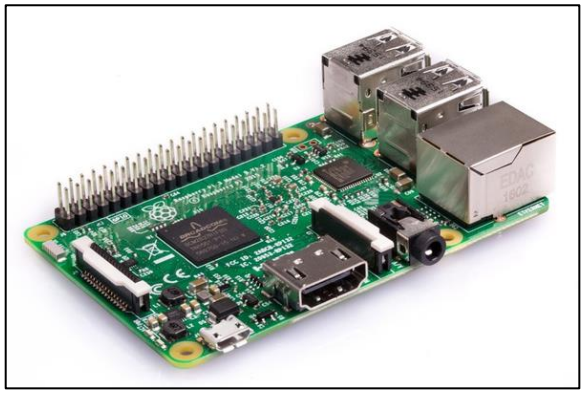


Gambar 2.13. Raspberry Pi 4 Model B

(Sumber: raspberrypi.org)

Pada saat laporan akhir ini dibuat, versi paling mutakhir dari Raspberry Pi adalah Raspberry Pi 4 Model B yang dirilis pada bulan Juni 2019. Perangkat ini memiliki *processor* ARM Cortex-A72 yang memiliki *quad core* 64-bit berfrekuensi 1.5 GHz, memiliki perangkat wifi 802.11ac dan Bluetooth 5 yang sudah *in-built*, masing-masing dua buah *port* USB 2.0 dan 3.0, *port* Ethernet gigabit, kapasitas RAM hingga 4GB, dan dapat mendukung dua buah *output* monitor hingga resolusi 4K. Model terbaru ini juga dapat ditenagai melalui konektor USB-C.

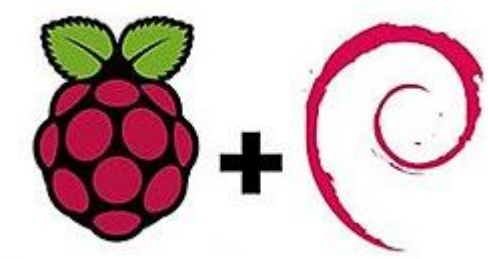
Dalam pembuatan tugas akhir sendiri, penulis menggunakan Raspberry Pi 3B, yang memiliki CPU Quad Core 1.2 GHz Broadcom BCM2837 64-bit, 1 GB RAM, *wireless* LAN dan Bluetooth, 4 *port* USB 2.0, dan kabel HDMI biasa.



Gambar 2.14. Raspberry Pi 3
(Sumber: raspberrypi.org)

2.4.1. Raspberry Pi OS

Raspberry Pi OS (dulunya disebut sebagai Raspbian), adalah sebuah sistem operasi (*operating system)* untuk perangkat Raspberry Pi yang berbasis pada distribusi Debian GNU/Linux, dan merupakan OS yang dikembangkan untuk memanfaatkan ARM CPU *low perfomance* dari Raspberry Pi. Sejak Raspberry Pi pertama kali dirilis pada tahun 2013, sudah ada beberapa versi Raspbian yang telah dirilis. Sejak tahun 2015, Raspberry Pi Foundation memberikan Raspbian beserta pembaharuan-pembaharuan terbarunya secara gratis sebagai OS utama dari serial komputer papan tunggal Raspberry Pi.



Gambar 2.15. Simbol Raspberry Pi OS
(Sumber: raspberrypi.org)

Raspbian dibuat oleh Mike Thompson dan Peter Green sebagai proyek independen, dan pertama kali dirilis pada bulan Juni 2012. Raspberry Pi OS terus dikembangkan dan diperbaharui hingga saat ini. Raspberry Pi OS dirilis bersama LXDE yang sudah dimodifikasi sebagai tampilan *desktop environment*-nya dan Openbox sebagai *window manager*. Semua versi Raspberry Pi OS didistribusikan dengan aplikasi bawaan berupa program aljabar Wolfram Mathematica, versi ringan dari *video game* Minecraft, serta versi ringan dari *web browser* Chromium pada versi terbarunya.

Dalam pembuatan laporan akhir, penulis menggunakan Raspbian Jessie. Pemilihan Raspberry Pi 3B dan OS Raspbian Jessie yang lebih lemah daripada Raspberry Pi 4 dan Raspberry Pi OS ini diambil karena kebutuhan *software* yang pada saat ini hanya mampu bekerja secara efektif di *environment* tersebut.