



TOWERS OF POWER

GSM Infrastructure and
Development

IMSI & IMEI

IMSI

IMSI - International Mobile Subscriber Identifier

Unique number of the mobile subscriber.

MCC-MNC-MSIN

MCC= Mobile Country Code (e.g. 310 for USA) -

MNC = Mobile Network Code (e.g. 410 for AT&T),

MSIN = Sequential Serial Number

IMSI is stored on SIM CARD

IMEI

International Mobile Station Equipment Identity

is a unique number, used to identify mobile phones.

Can be found printed inside the battery compartment of the phone.

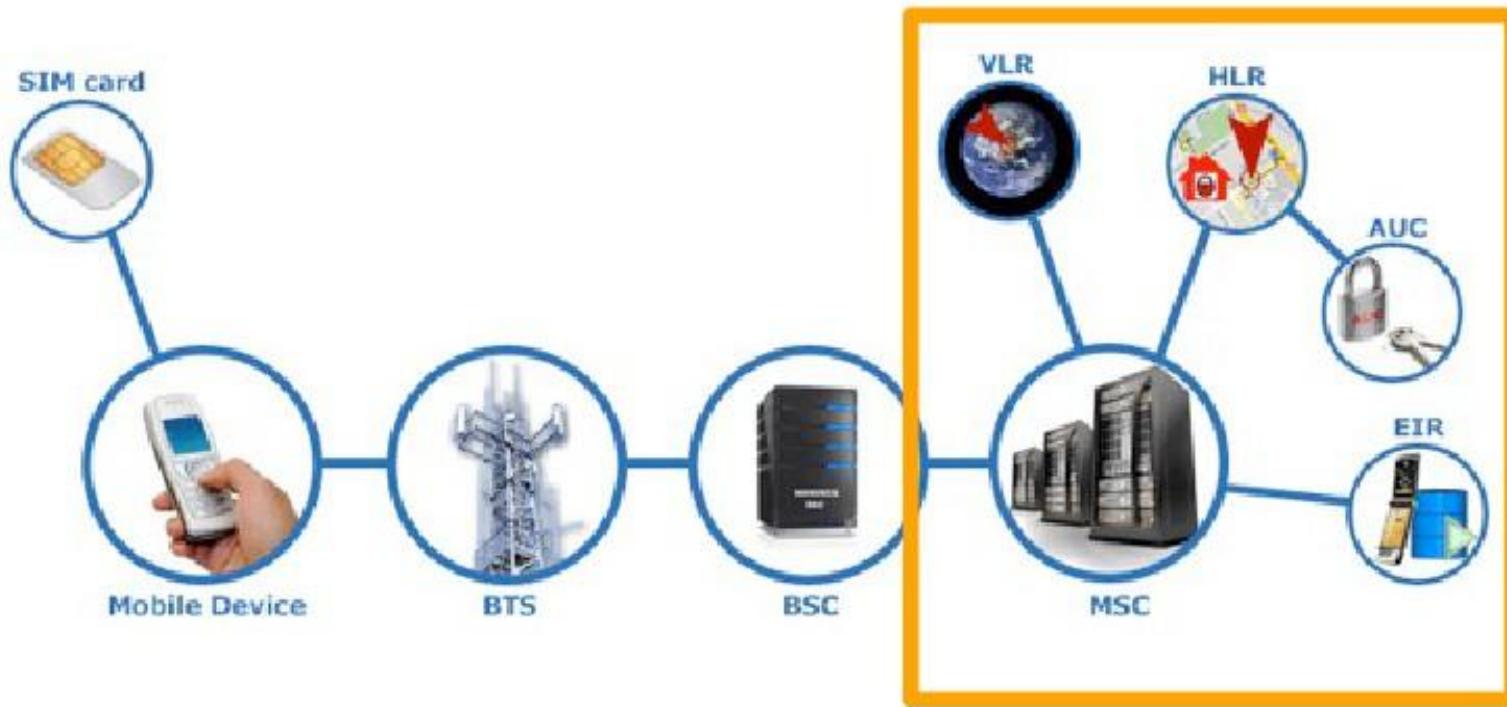
Can also be displayed on-screen on most phones by entering

***#06#**



GSM SYSTEM ARCHITECTURE

NETWORK SUBSYSTEM



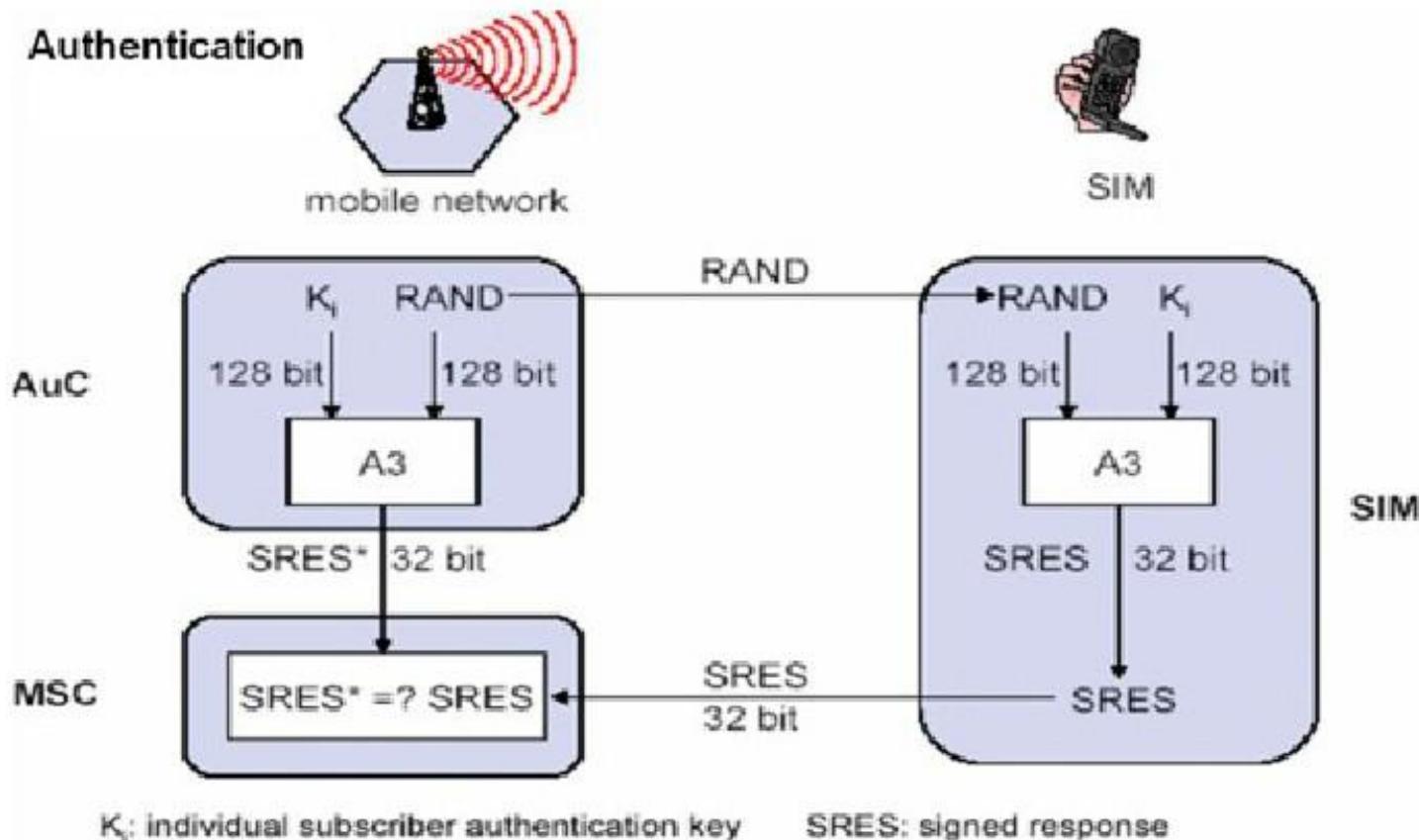
MOBILE SWITCHING CENTER



HOME LOOKUP REGISTRY



AUTHENTICATION CENTER (AUC)



VLR + EIR

Visitor Location Register:

- responsible for mobility management and handles local caller traffic
- each MSC has its own VLR

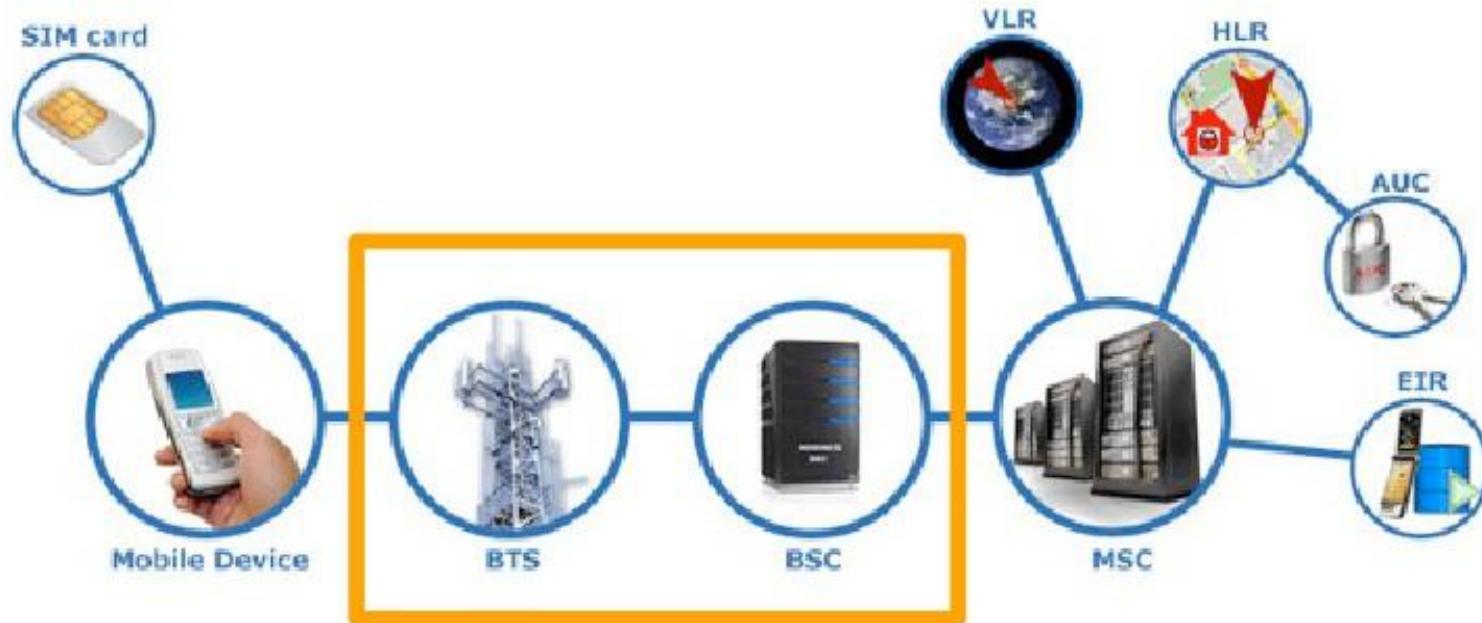


Equipment Identification Register:

- a database that contains the information about the identity of the mobile equipment (IMEI)
- Keeps track black listed phones



BASE STATION SUBSYSTEM



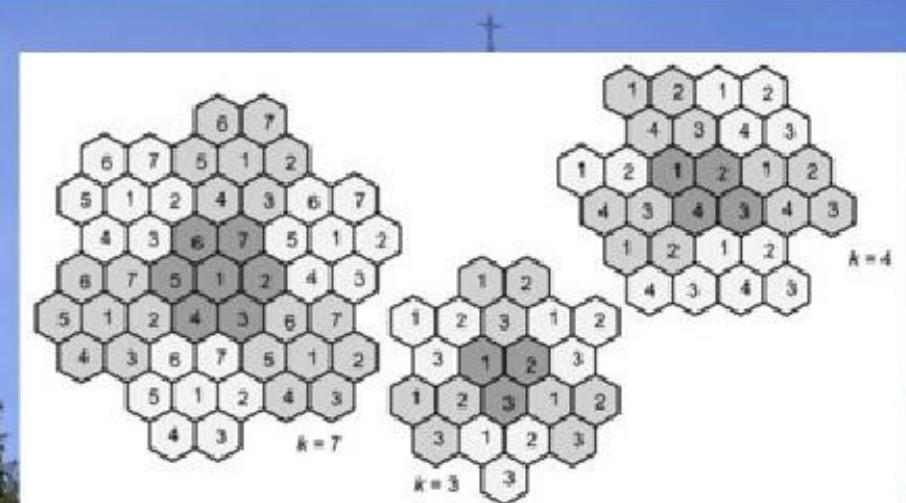
BASE STATION CONTROLLER

The **intelligence** of the BTS



BASE TRANSCEIVER STATION

The Tower of Power



Designed as cells in order for efficient **frequency reuse**

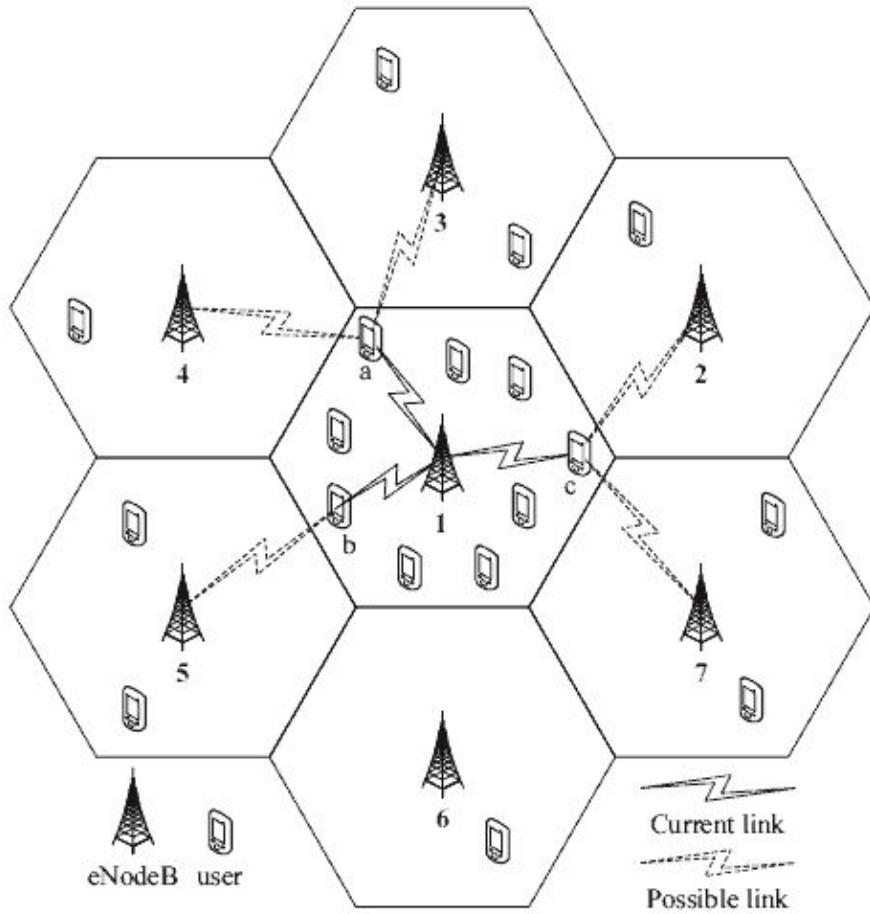


Figure 1: Network model.

ARFCN	Frequency (MHz)	
	Downlink	Uplink
128	869.2	824.2
129	869.4	824.4
130	869.6	824.6
131	869.8	824.8
132	870	825
133	870.2	825.2
134	870.4	825.4
135	870.6	825.6
136	870.8	825.8
137	871	826
138	871.2	826.2
139	871.4	826.4
140	871.6	826.6
141	871.8	826.8
142	872	827
143	872.2	827.2
144	872.4	827.4
145	872.6	827.6
146	872.8	827.8
147	873	828
148	873.2	828.2

ARFCN

http://niviuk.free.fr/gsm_arfcn.php

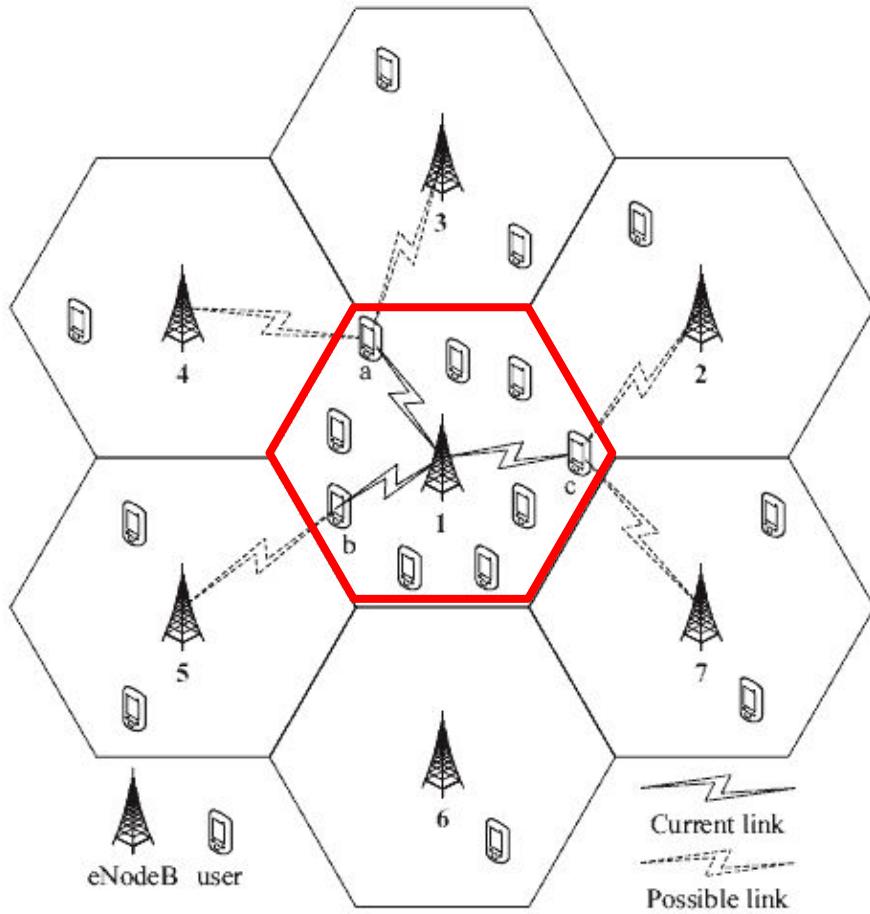


Figure 1: Network model.

ARFCN	Frequency (MHz)	
	Downlink	Uplink
128	869.2	824.2
129	869.4	824.4
130	869.6	824.6
131	869.8	824.8
132	870	825
133	870.2	825.2
134	870.4	825.4
135	870.6	825.6
136	870.8	825.8
137	871	826
138	871.2	826.2
139	871.4	826.4
140	871.6	826.6
141	871.8	826.8
142	872	827
143	872.2	827.2
144	872.4	827.4
145	872.6	827.6
146	872.8	827.8
147	873	828
148	873.2	828.2

ARFCN

http://niviuk.free.fr/gsm_arfcn.php

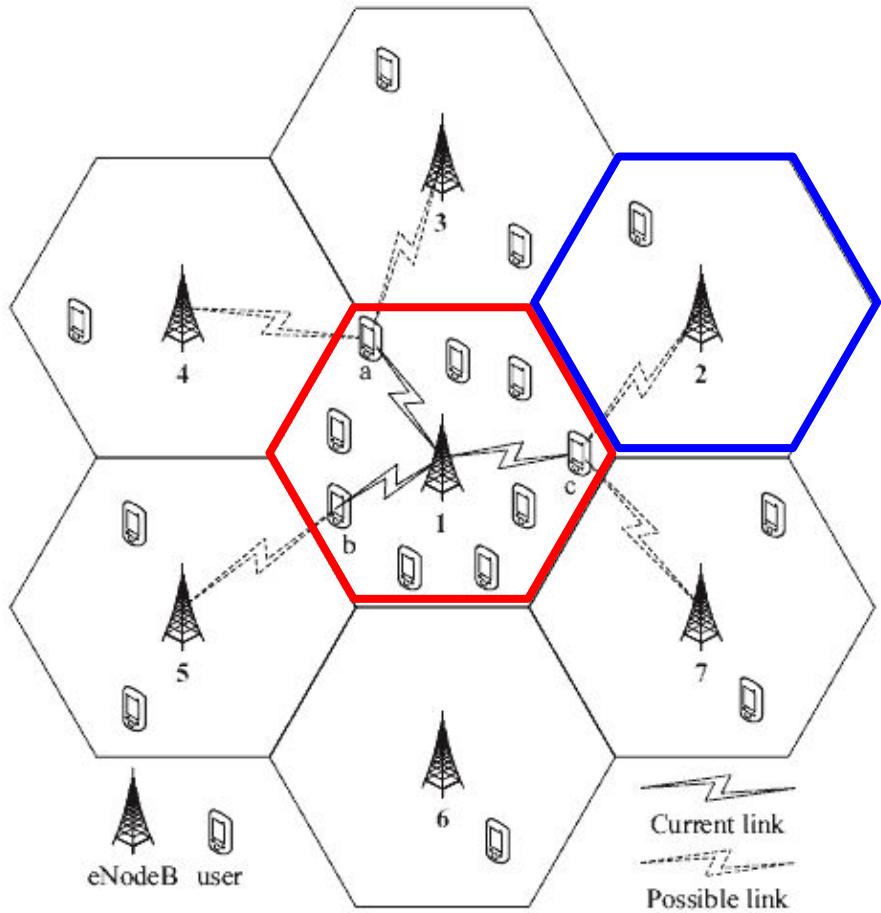


Figure 1: Network model.

ARFCN	Frequency (MHz)	
	Downlink	Uplink
128	869.2	824.2
129	869.4	824.4
130	869.6	824.6
131	869.8	824.8
132	870	825
133	870.2	825.2
134	870.4	825.4
135	870.6	825.6
136	870.8	825.8
137	871	826
138	871.2	826.2
139	871.4	826.4
140	871.6	826.6
141	871.8	826.8
142	872	827
143	872.2	827.2
144	872.4	827.4
145	872.6	827.6
146	872.8	827.8
147	873	828
148	873.2	828.2

ARFCN

http://niviuk.free.fr/gsm_arfcn.php

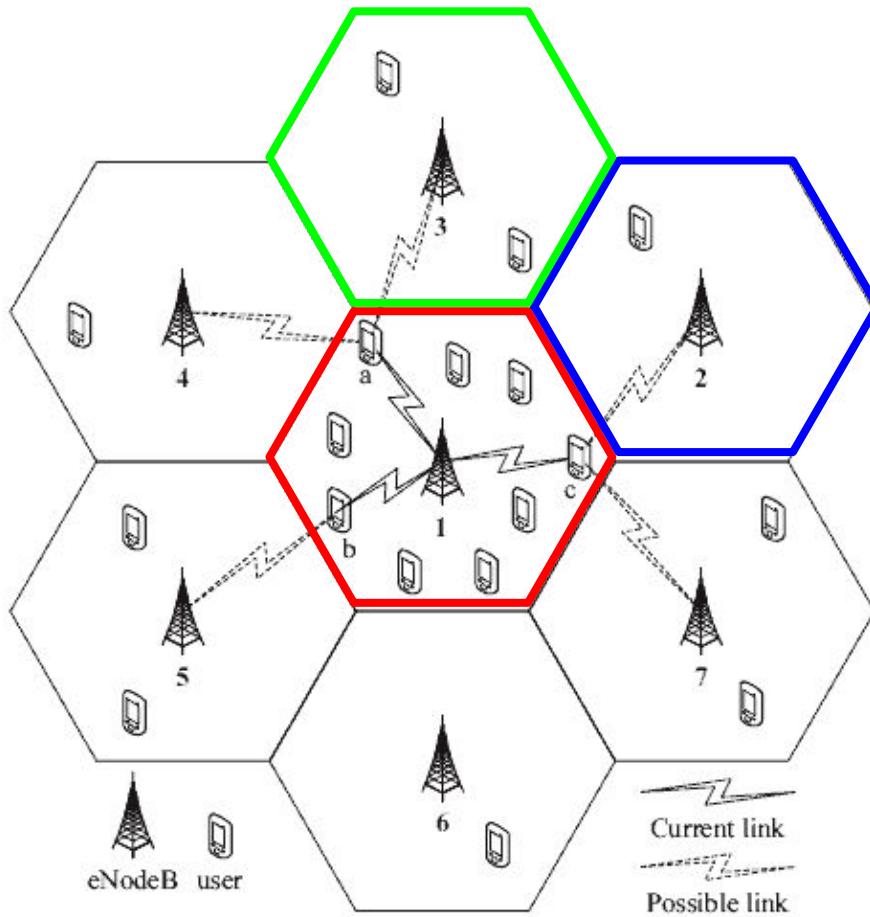


Figure 1: Network model.

ARFCN	Frequency (MHz)	
	Downlink	Uplink
128	869.2	824.2
129	869.4	824.4
130	869.6	824.6
131	869.8	824.8
132	870	825
133	870.2	825.2
134	870.4	825.4
135	870.6	825.6
136	870.8	825.8
137	871	826
138	871.2	826.2
139	871.4	826.4
140	871.6	826.6
141	871.8	826.8
142	872	827
143	872.2	827.2
144	872.4	827.4
145	872.6	827.6
146	872.8	827.8
147	873	828
148	873.2	828.2

ARFCN

http://niviuk.free.fr/gsm_arfcn.php

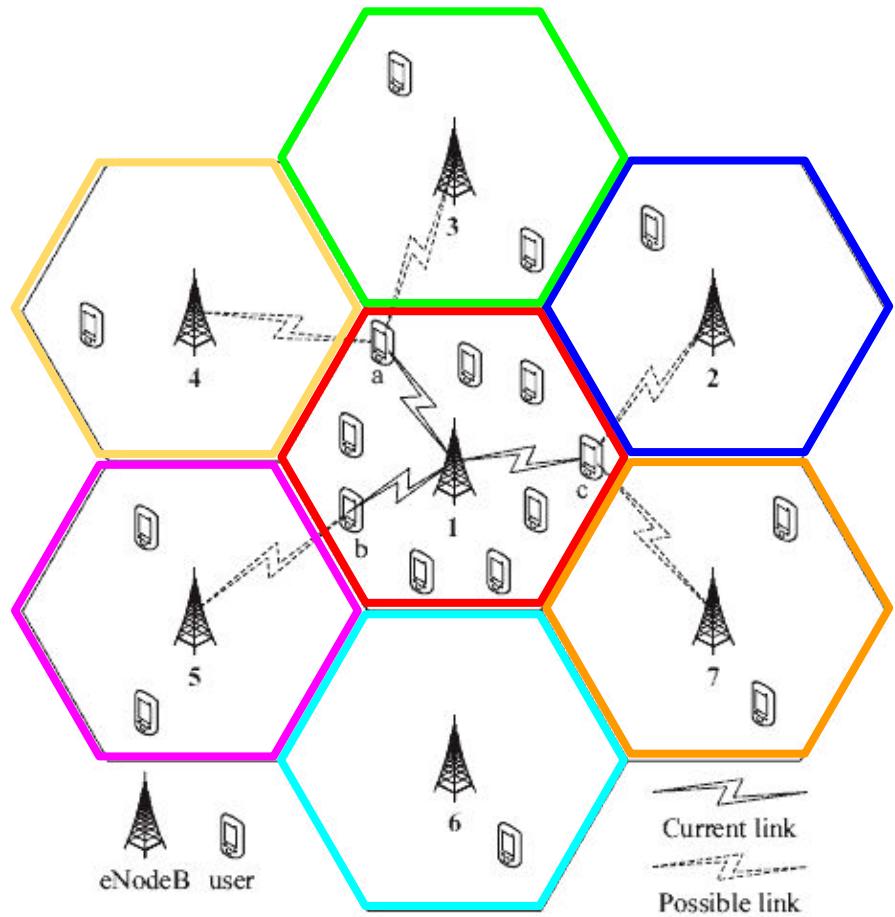


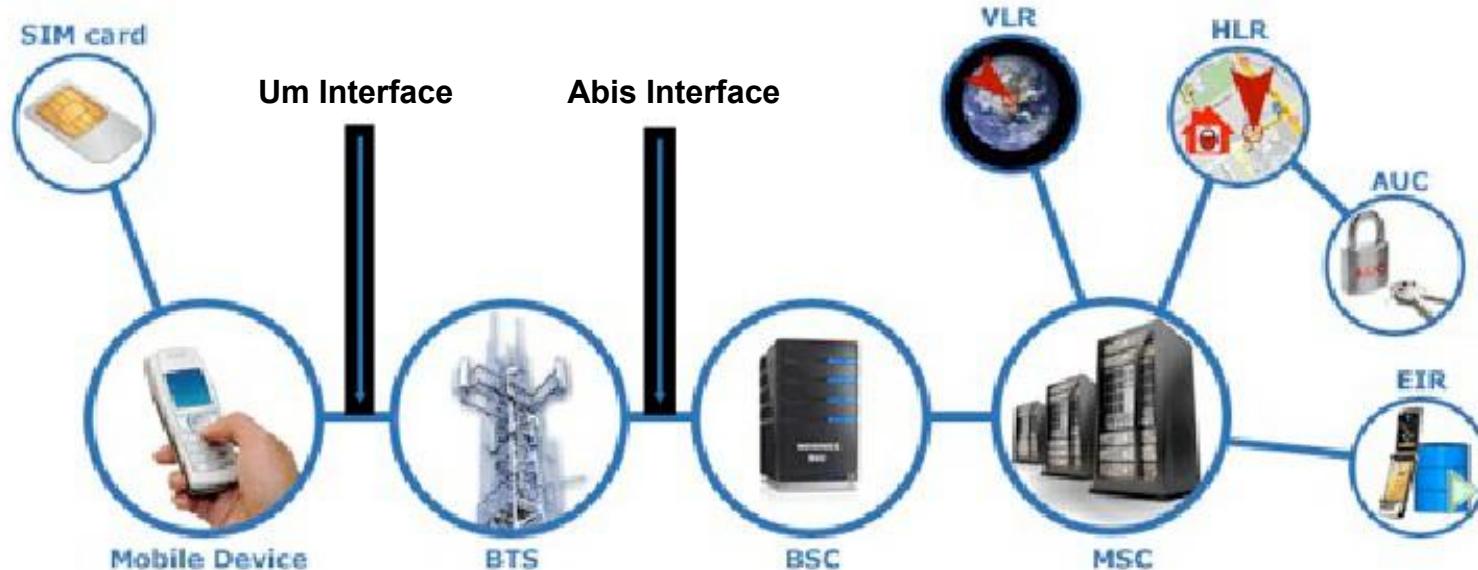
Figure 1: Network model.

ARFCN	Frequency (MHz)	
	Downlink	Uplink
128	869.2	824.2
129	869.4	824.4
130	869.6	824.6
131	869.8	824.8
132	870	825
133	870.2	825.2
134	870.4	825.4
135	870.6	825.6
136	870.8	825.8
137	871	826
138	871.2	826.2
139	871.4	826.4
140	871.6	826.6
141	871.8	826.8
142	872	827
143	872.2	827.2
144	872.4	827.4
145	872.6	827.6
146	872.8	827.8
147	873	828
148	873.2	828.2

ARFCN

http://niviuk.free.fr/gsm_arfcn.php

INTERFACING



Um Logical Channels

Traffic Channels

Full rate traffic channel

Half rate traffic channel

TCH/F

TCH/H

Dedicated control Channels

Standalone Dedicated Control Channel

Fast Associated Control Channel

Slow Associated Control Channel

SDCCH

FACCH

SACCH

Common control Channels

Broadcast Control Channel

Synchronization Channel

Frequency Correction Channel

Paging Channel

Access Grant Channel

Random Access Channel

BCCH

SCH

FCCH

PCH

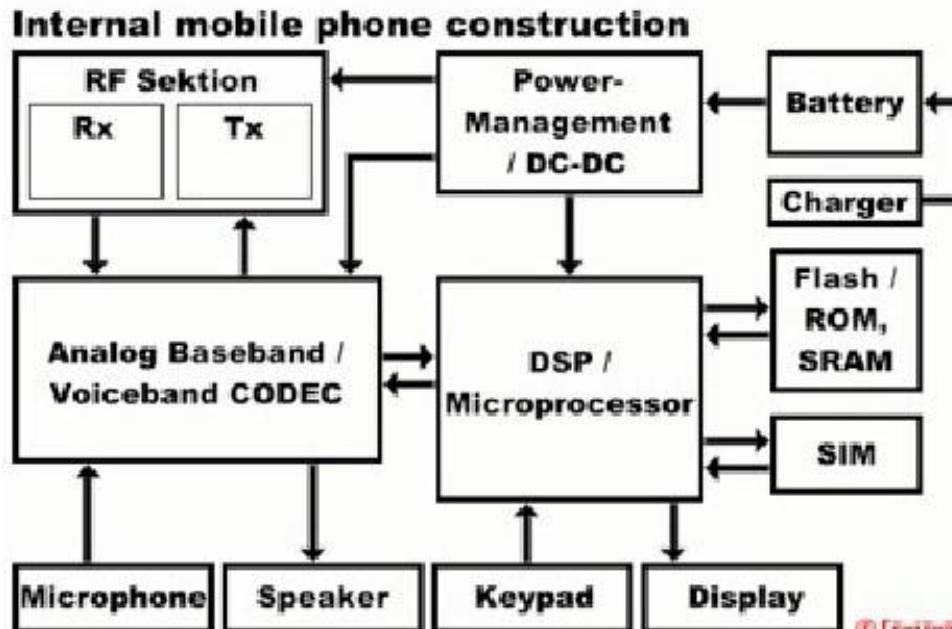
AGCH

RACH

MOBILE STATION SYSTEM



MOBILE DEVICE



SUBSCRIBER IDENTITY MODULE

International Mobile Subscriber

Identifier (**IMSI**)

Unique number of the mobile subscriber.

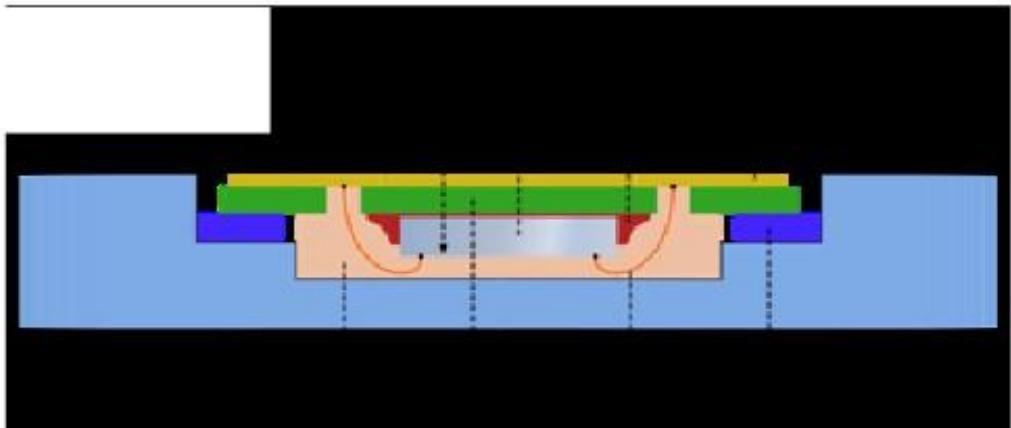
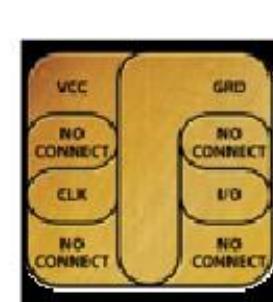
MCC + MNC + MSIN

Mobile Country Code + Mobile Network Code

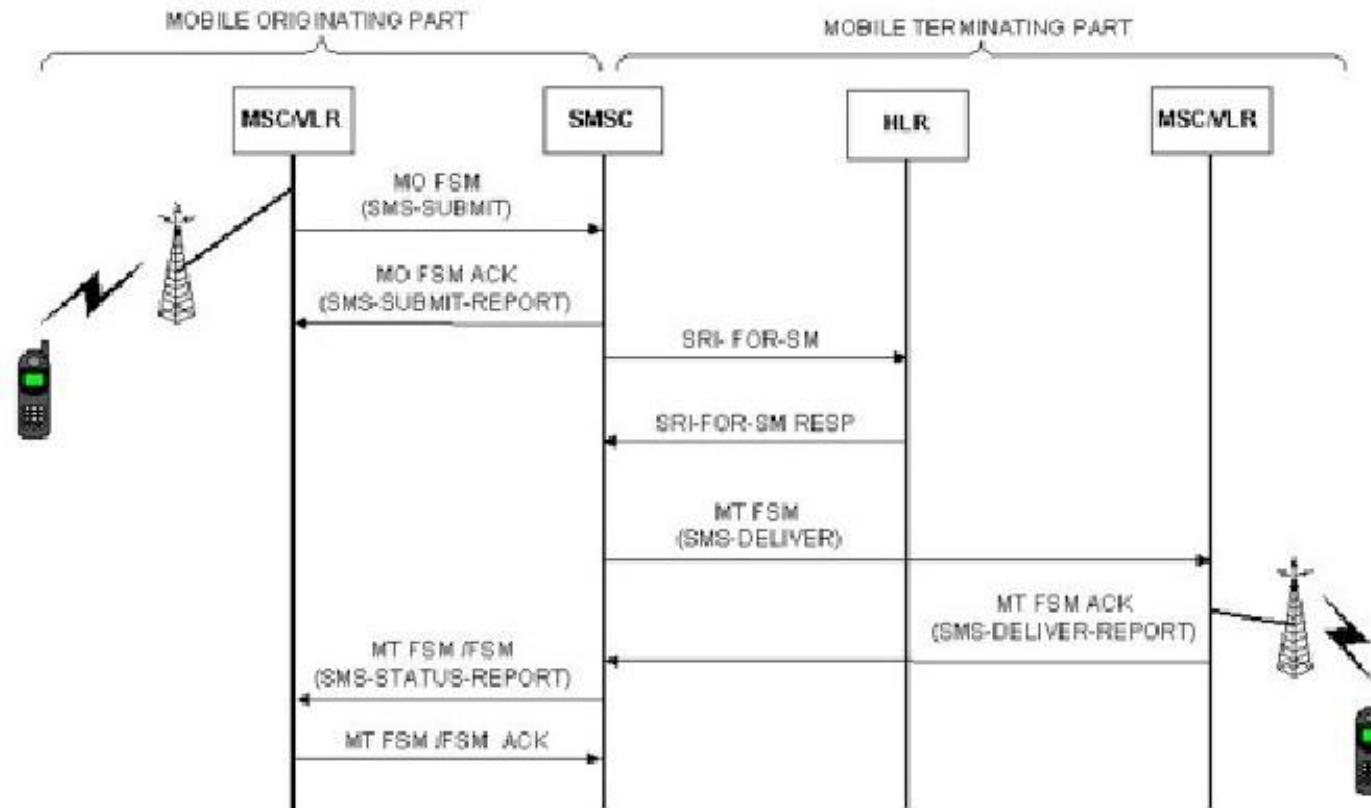
+ Mobile Subscriber Id Number

International Mobile Equipment

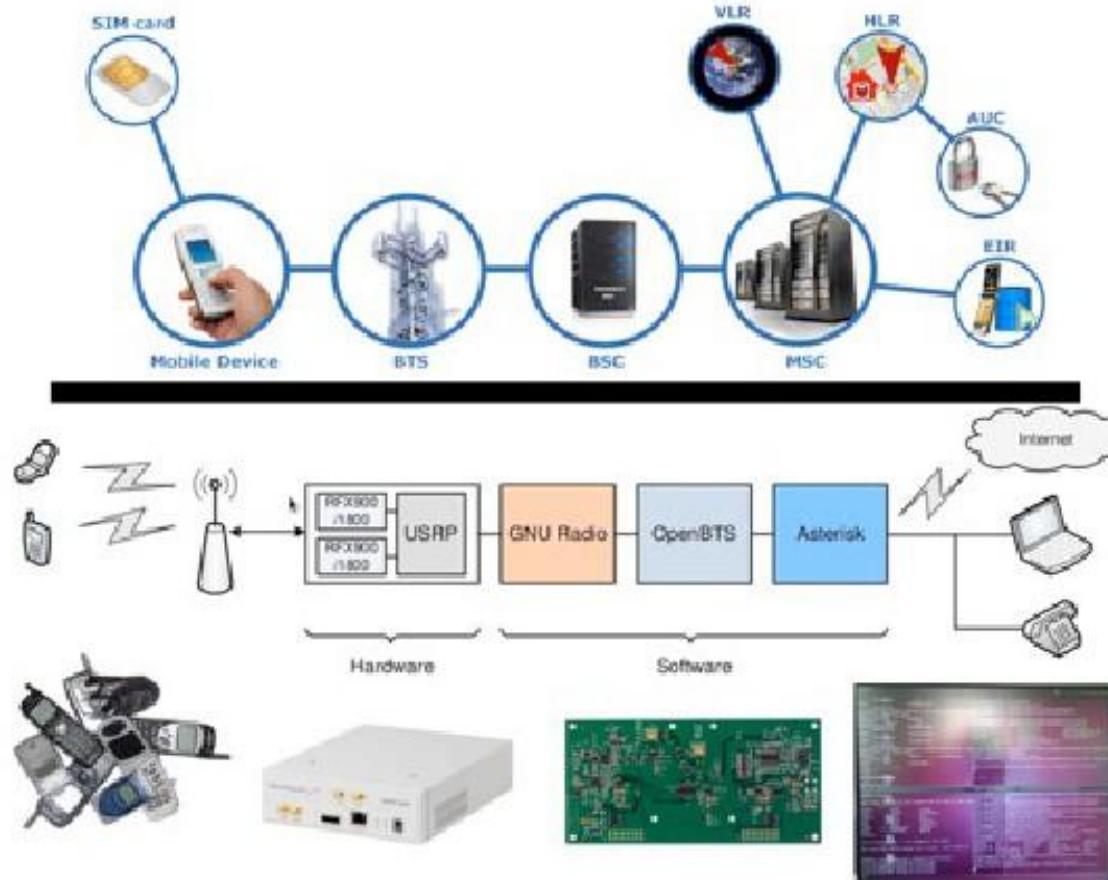
Identifier (**IMEI**) - a number stored on the hardware devices describing it - unique to each phone - like a serial number



OTHER NETWORK COMPONENTS



OPEN SOURCE BTSs



Software Defined Radios

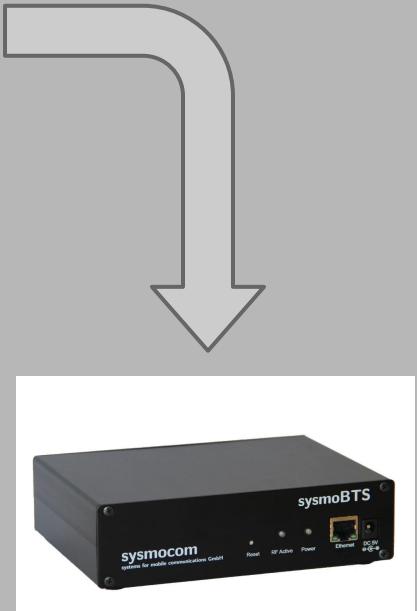
Software-defined radio (SDR)



Software-defined radio (SDR) is a radio communication system where components that have been typically implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, etc.) are instead implemented by means of software on a personal computer or embedded system.

Some examples are: Ettus USRP, Blade RF, LimeSDR, RTL-SDR

GSM in Software



Software based **BTS** (Base Transceiver station) forward call traffic through to an operator's [mobile switching center](#).

This software delivers calls via [SIP](#) to a VOIP soft switch (such as [FreeSWITCH](#) or [yate](#)) or [PBX](#) (such as [Asterisk](#)) forming a self-contained cellular network in a single computer system.

Software based Cellular uses a [software-defined radio transceiver](#) with no specialized GSM hardware.

Open Source Cellular Options



Original
Open Source
GSM



sysmocom
systems for mobile communications GmbH



3G Support
Rhizomatica



BladeRF
4G Support

OpenCellular

ENDAGA

facebook



\$1000 ?

TELECOM INFRA PROJECT

Open Source Cellular Software



R H I Z O M A T I C A

wiki.rhizomatica.org

Hardware



BSC
Base Station
Controller



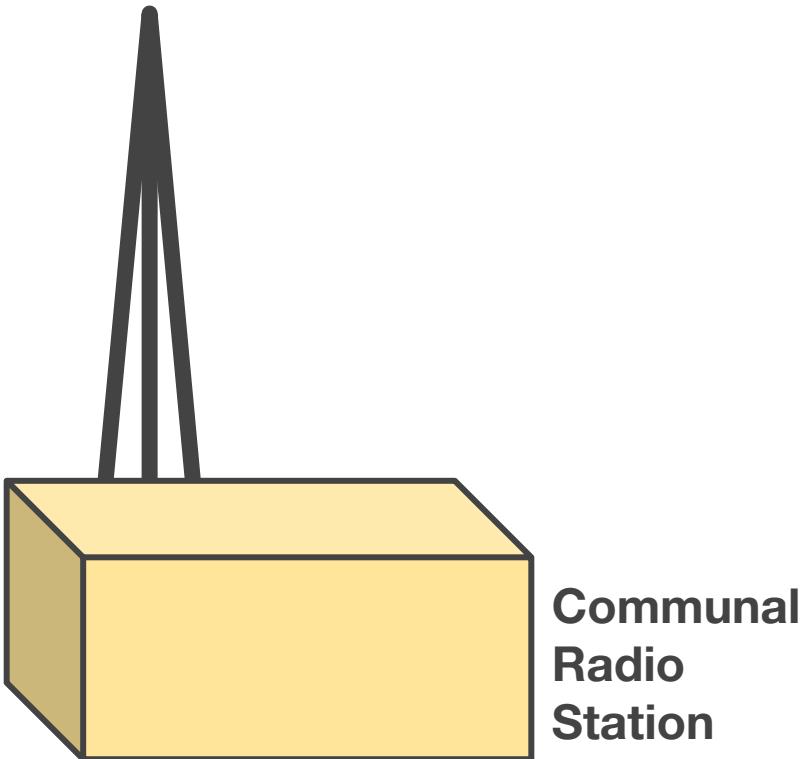
BTS
Base Transceiver
Station



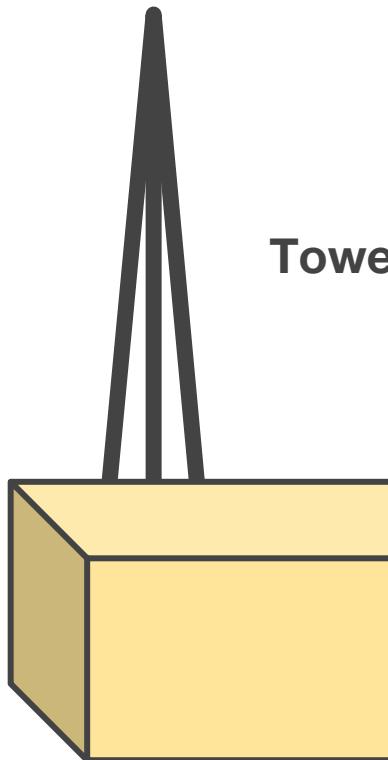
Antennas
Omni-Directional



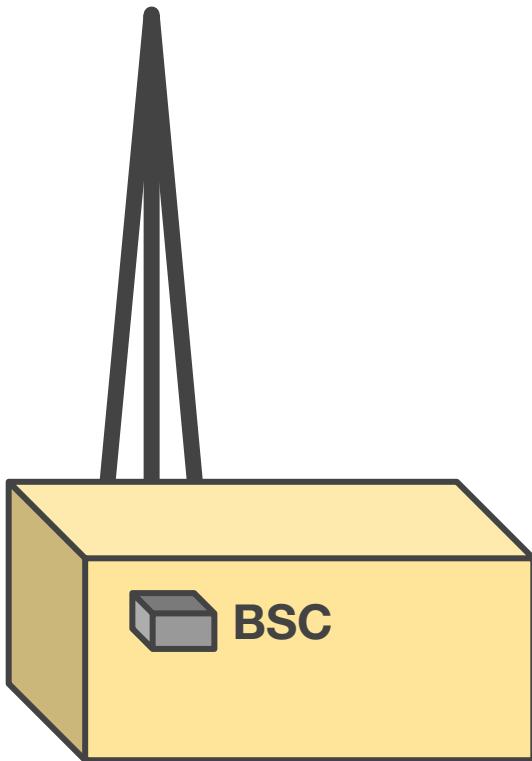
Community Cellular



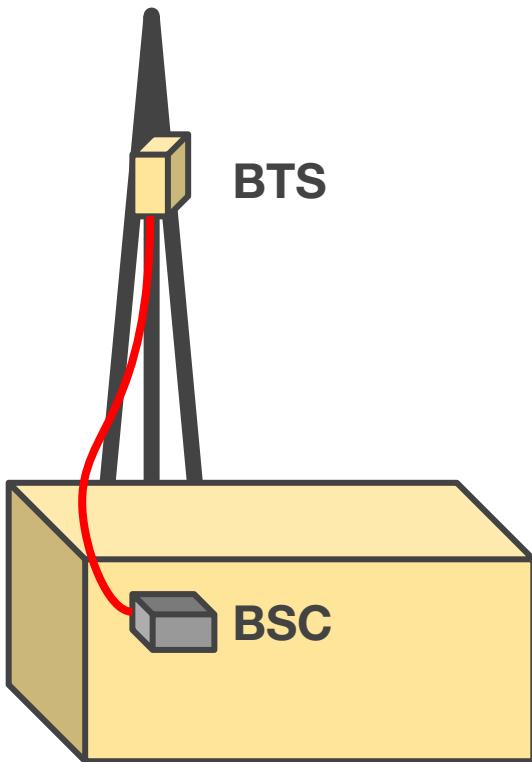
Community Cellular



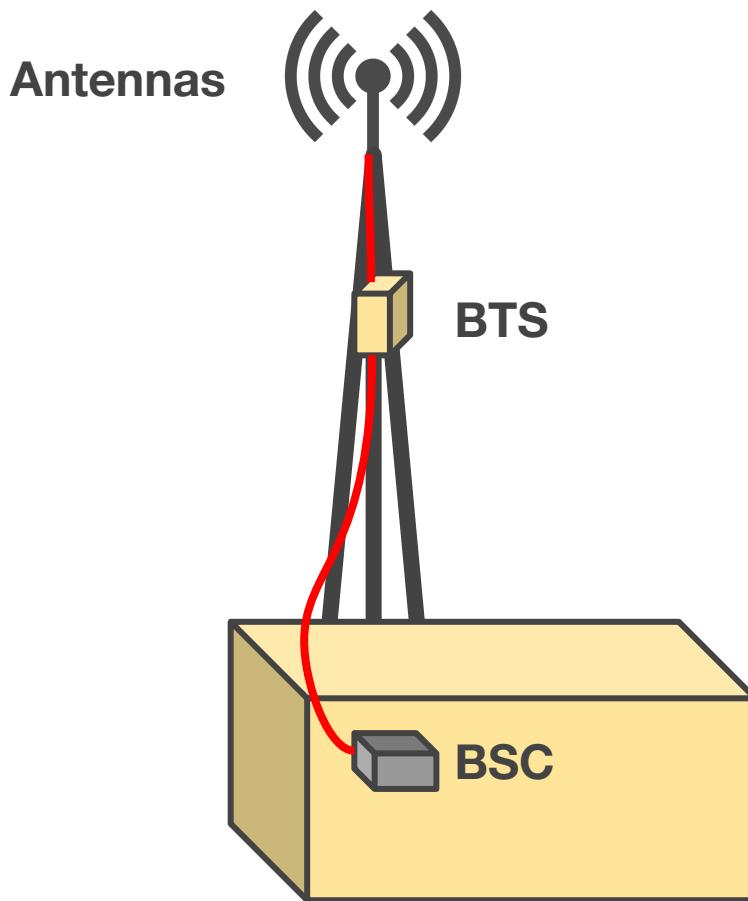
Community Cellular



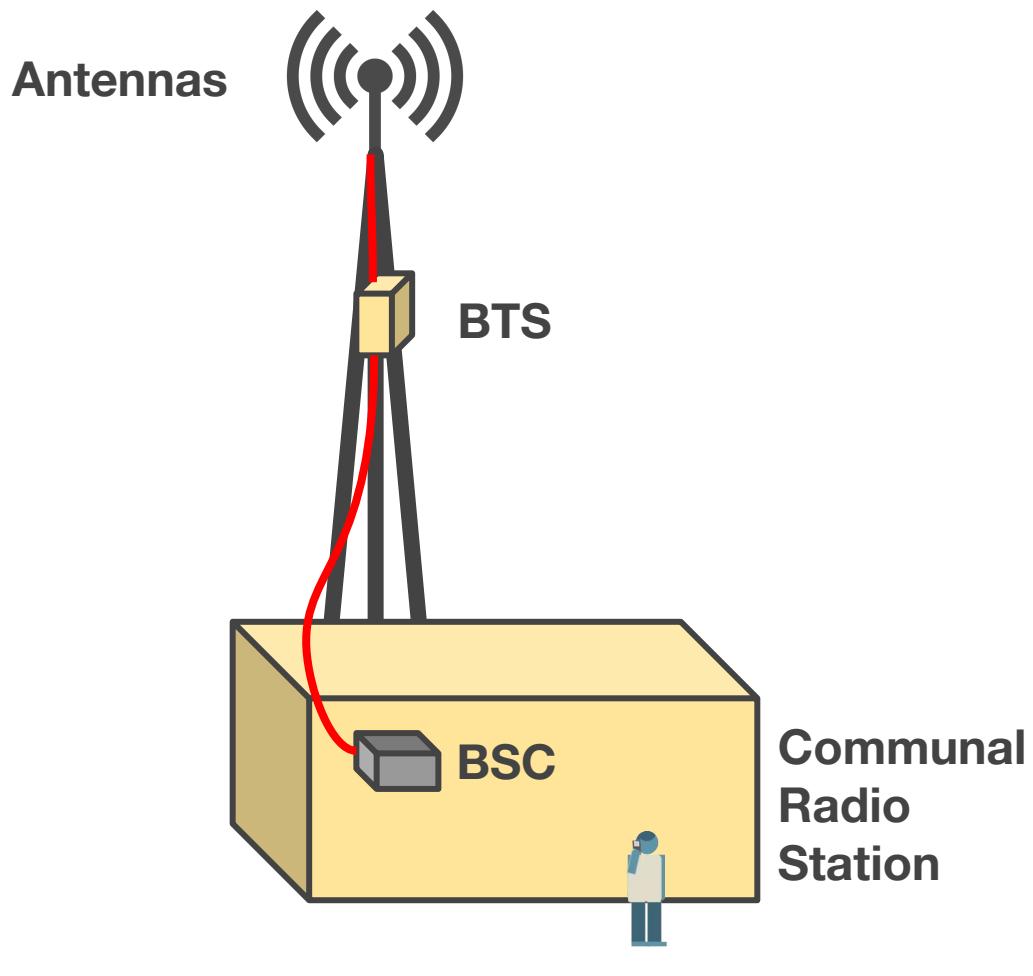
Community Cellular



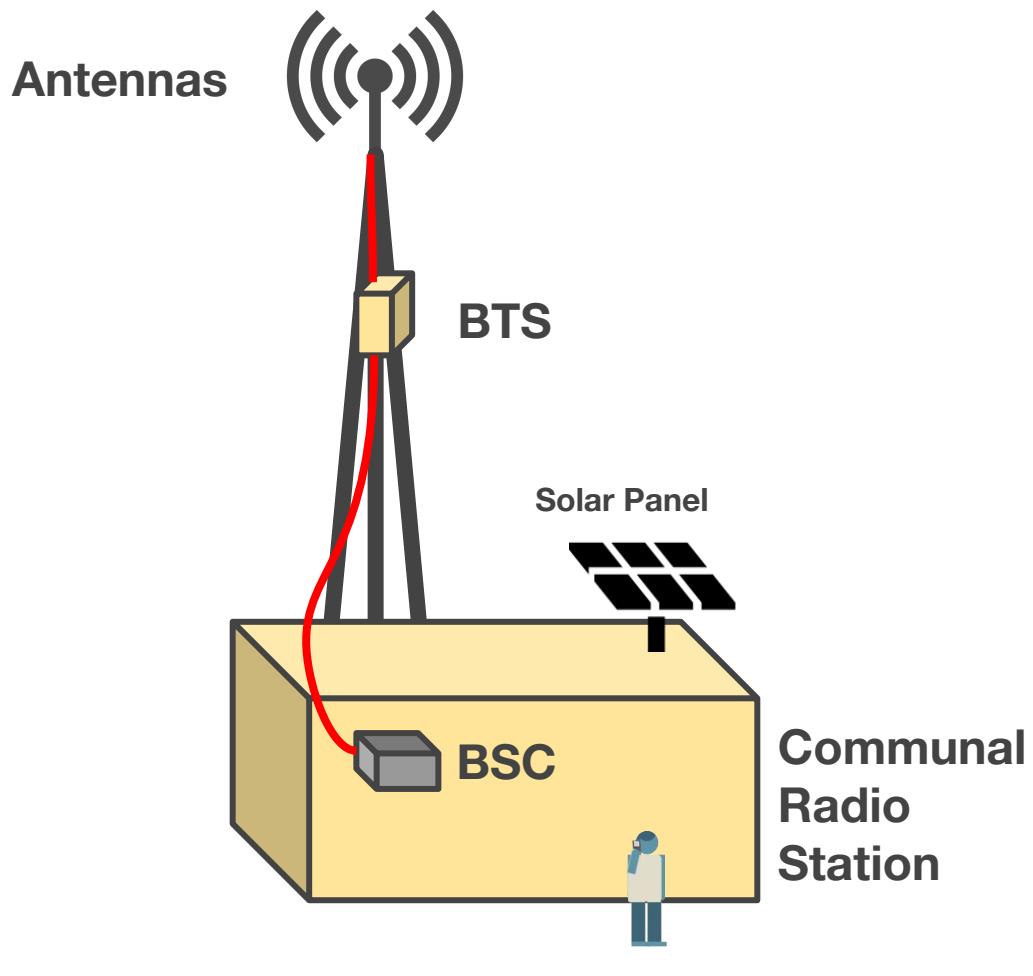
Community Cellular



Community Cellular



Community Cellular

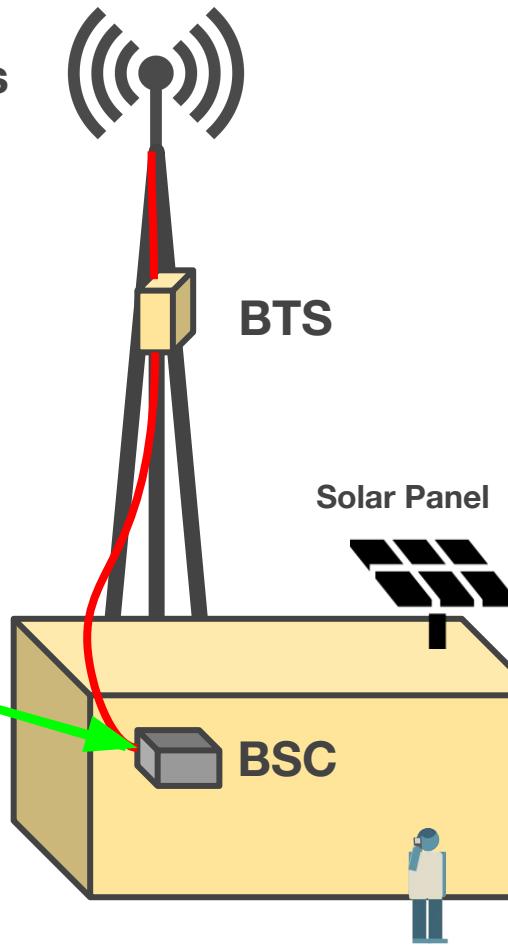


Community Cellular

Internet
VPN

Remote
Management

Long Distance Calls





Nuran LiteCell 1.0 BTS

\$4800

- **2 TRX**
- **Power consumption: 52 Watts**
- **Rating: IP67**
- **Up to 30 concurrent calls (half rate)**



Band	Reception	Transmission
850	824–850 MHz	869–895 MHz
900	880–915 MHz	925–960 MHz
1800	1710–1785 MHz	1805–1880 MHz
1900	1850–1910 MHz	1930–1990 MHz

Nuran LiteCell 1.5

BTS



Nuran LiteCell 1.5

BTS

Ethernet
To BSC



Nuran LiteCell 1.5

BTS



**Antenna
N-Type**

Nuran LiteCell 1.5

BTS

**Power
24V**



Nuran LiteCell 1.5

BTS

**GPS
(Timing)**

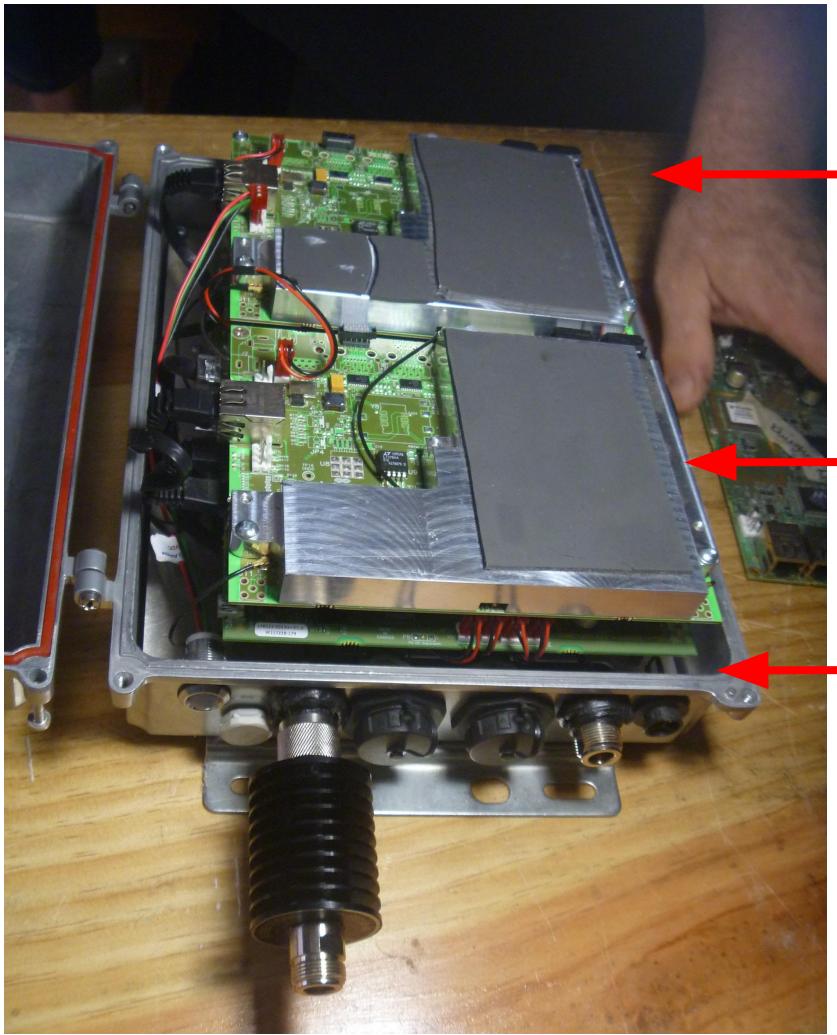




UmSITE-TM3

\$4000





TRX 1

TRX 2

**Controller
- Linux**



TRX 1
8 Channels

TRX 2
8 Channels



TRX 1
8 Channels
- 1 control

TRX 2
8 Channels

Um Logical Channels

Traffic Channels

Full rate traffic channel

Half rate traffic channel

TCH/F

TCH/H

Dedicated control Channels

Standalone Dedicated Control Channel

Fast Associated Control Channel

Slow Associated Control Channel

SDCCH

FACCH

SACCH

Common control Channels

Broadcast Control Channel

Synchronization Channel

Frequency Correction Channel

Paging Channel

Access Grant Channel

Random Access Channel

BCCH

SCH

FCCH

PCH

AGCH

RACH



TRX 1

8 Channels

- 1 control
- 7 Full Rate “Call” TCH/F

TRX 2

8 Channels

- 8 Full Rate “Call” TCH/F



TRX 1

8 Channels

- 1 control
- 7 Full Rate “Call” TCH/F

TRX 2

8 Channels

- 8 Full Rate “Call” TCH/F

15 Full Rate Calls



TRX 1

8 Channels

- 1 control
- 14 Half Rate “Call” TCH/H

TRX 2

8 Channels

- 16 Half Rate “Call” TCH/H

30 Half Rate Calls

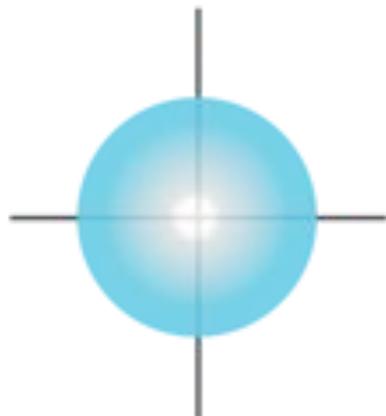


Omni Directional
Antennas
1 BTS



Sector/Patch Antennas
3 BTS

Omni-directional dipole

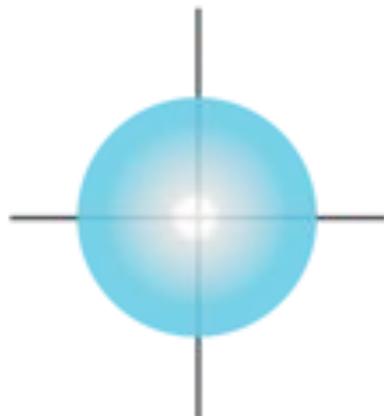


2.2dBi gain

Example: Light Bulb



Omni-directional dipole

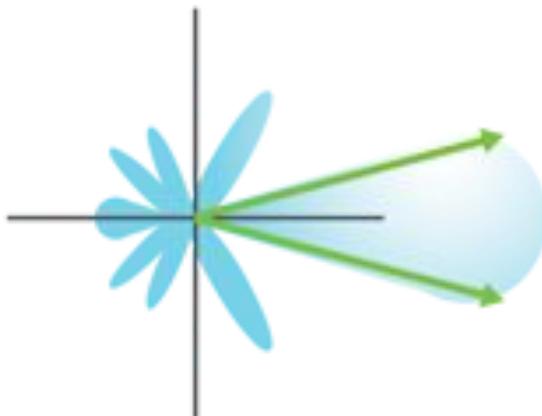


2.2dBi gain

Example: Light Bulb



High gain directional

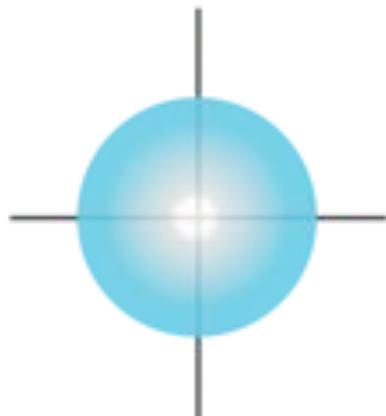


6dBi gain

Example: Flashlight



Omni-directional dipole

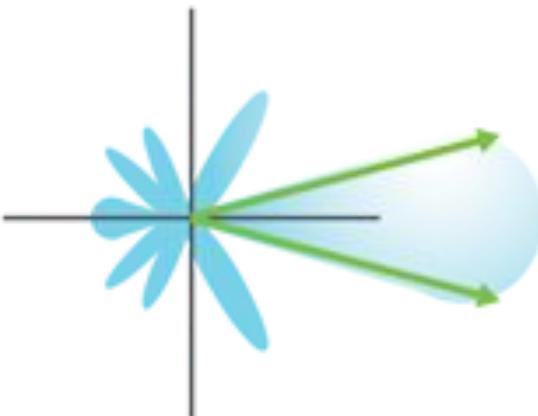


2.2dBi gain

Example: Light Bulb



High gain directional



6dBi gain

Example: Flashlight



Multi-sector array with high gain directional



6dBi gain per sector

Example: Multiple Flashlights





Products >Antennas & Filter Products

Antennas & Filter Products

Everything you need for indoor and outdoor RF applications, including antennas, filter products, and mobile amplifiers.

[Filter Products](#)[In-Building Antennas](#)[Microwave Antennas](#)[Mobile Amplifiers](#)[Mobile Antennas, Mounts & Accessories](#)[Outdoor Base Station Antennas](#)



Ventev / TerraWave - 824-960 MHz 6 dBi Omni Stick Antenna with N Jack

TESSCO SKU : 392017 Mfg Part #: T09060010006 Qty/UOM : 1 EACH UPC: 888063920172

Ventev's TerraWave 824-960 MHz 6 dBi omni-directional stick antenna with N Jack is designed for applications in the 900 MHz frequency, including, radio frequency identification (RFID) applications, cellular systems, global system for mobile (GSM) communications, code-division multiple access systems (CDMA) applications, multipoint applications and wireless video links. The antenna's fiberglass radome withstands the harshest environmental conditions. Includes a heavy-duty L-bracket for mast or vertical surface mounting. Every TerraWave antenna is RoHS compliant, and is covered by Ventev's two-year TerraNet warranty program. For more information, contact a regional sales executive at 210-375-8482, 800-851-4965 or sales@terrawave.com, or visit www.terrawave.com.

List: \$75.60

Your Price: \$68.00

Qty:

Add

[View Worksheet](#)



Ventev / TerraWave - 800-2500 MHz 7/10dBi Patch Antenna

TESSCO SKU : 322000 Mfg Part #: M4070100P11206 Qty/UOM : 1 EACH UPC: 888063220005

TerraWave M4070100P11206 is a patch antenna operating in the 800 - 2500 MHz frequency range. The dual band patch antenna features 7 dBi gain in 800 - 960 MHz or 10 dBi in frequency range 1710 - 2500 MHz. Maximum power input 50 watts. The antenna is terminated with an N Plug (female) connector. A 12 inch jumper is included along with antenna mounting hardware.

List: \$67.38

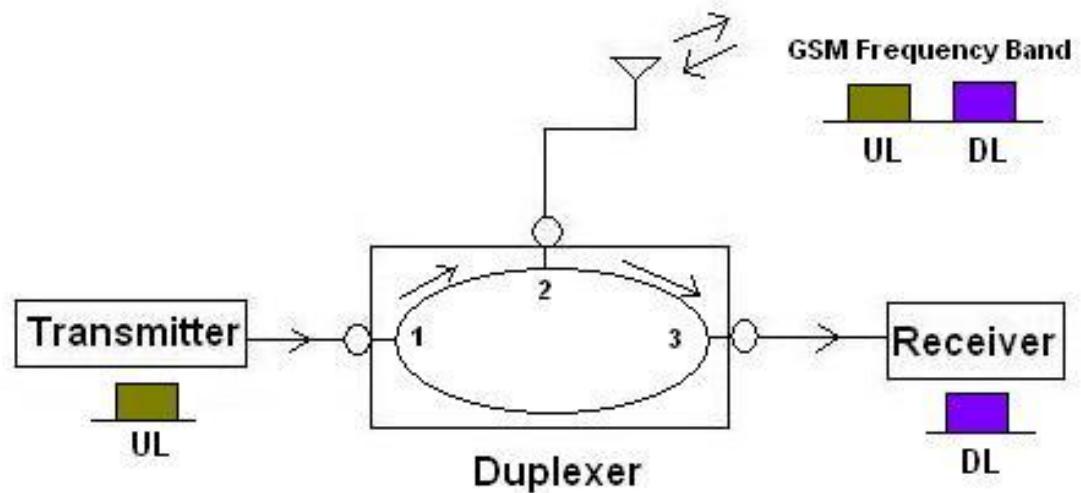
Your Price: \$58.20

Qty:

Add

[View Worksheet](#)

DUPLEXER



Open Source Cellular Software



R H I Z O M A T I C A

OsmoTRX

OpenBSC

OsmoNITB

RAI - Rhizomatica Administration Interface

RCCN - Rhizomatica Community Cellular Network

Freeswitch (Call Routing)

Kannel (Text Messages)



Harald Welte



Comparing TCP/IP with OSI

OSI Model	TCP/IP Hierarchy	Protocols				
7 th Application Layer						
6 th Presentation Layer	Application Layer	HTTP	SMTP	POP3	FTP	...
5 th Session Layer						
4 th Transport Layer	Transport Layer	TCP		UDP		
3 rd Network Layer	Network Layer	IP			ICMP	
2 nd Link Layer	Link Layer	ARP	RARP	Ethernet	PPP	...
1 st Physical Layer						

Link Layer : includes device driver and network interface card

Network Layer : handles the movement of packets, i.e. Routing

Transport Layer : provides a reliable flow of data between two hosts

Application Layer : handles the details of the particular application



OsmoTRX

<https://osmocom.org/projects/osmotrx/wiki/OsmoTRX>



OsmoTRX

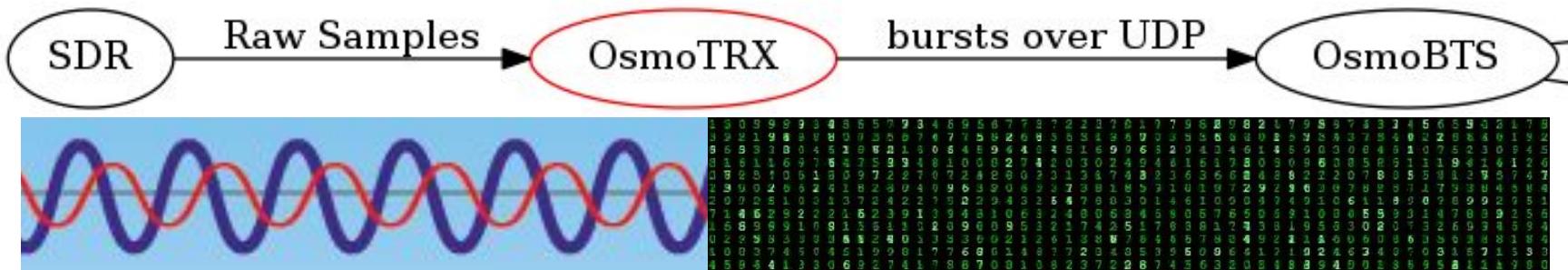
OsmoTRX is a software-defined radio transceiver that implements the Layer 1 physical layer of a BTS comprising the following 3GPP specifications:

- **TS 05.01 "Physical layer on the radio path"**
- **TS 05.02 "Multiplexing and Multiple Access on the Radio Path"**
- **TS 05.04 "Modulation"**
- **TS 05.10 "Radio subsystem synchronization"**



<https://osmocom.org/projects/osmotrx/wiki/OsmoTRX>

OsmoTRX





OpenBSC

<https://osmocom.org/projects/openbsc/wiki/OpenBSC>

OpenBSC

BSC (Base Station Controller) software that connects A-bis protocol,
and implemented according to GSM technical Specification

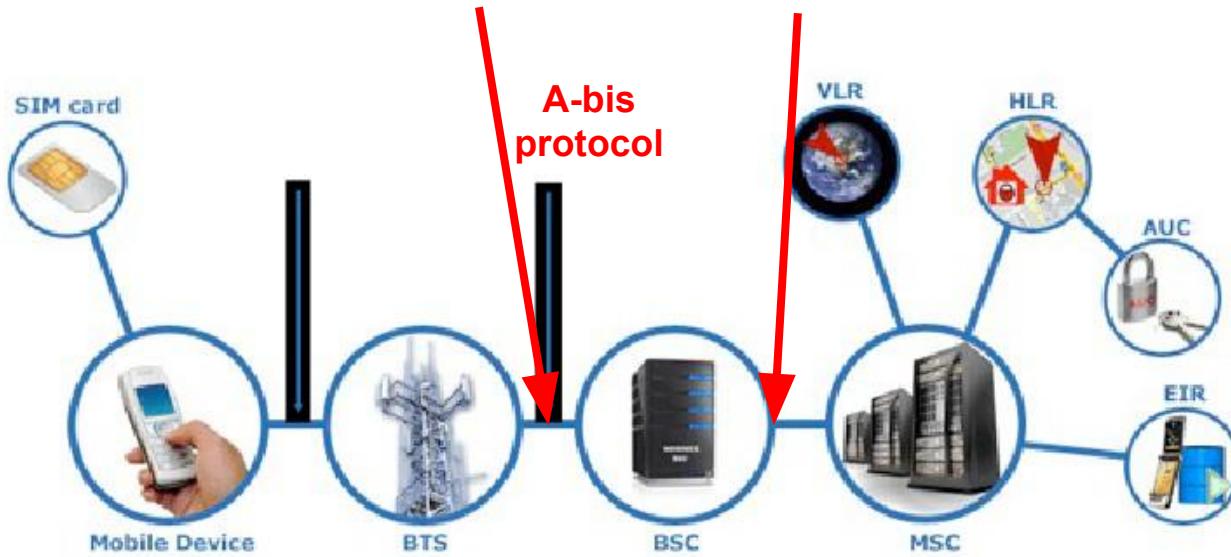
OpenBSC

BSC (Base Station Controller) software that connects A-bis protocol,
and implemented according to GSM technical Specification

OsmoBSC
Mode

OpenBSC

OsmoBSC Mode



OpenBSC

BSC (Base Station Controller) software that connects A-bis protocol,
and implemented according to GSM technical Specification

OsmoNITB
Mode

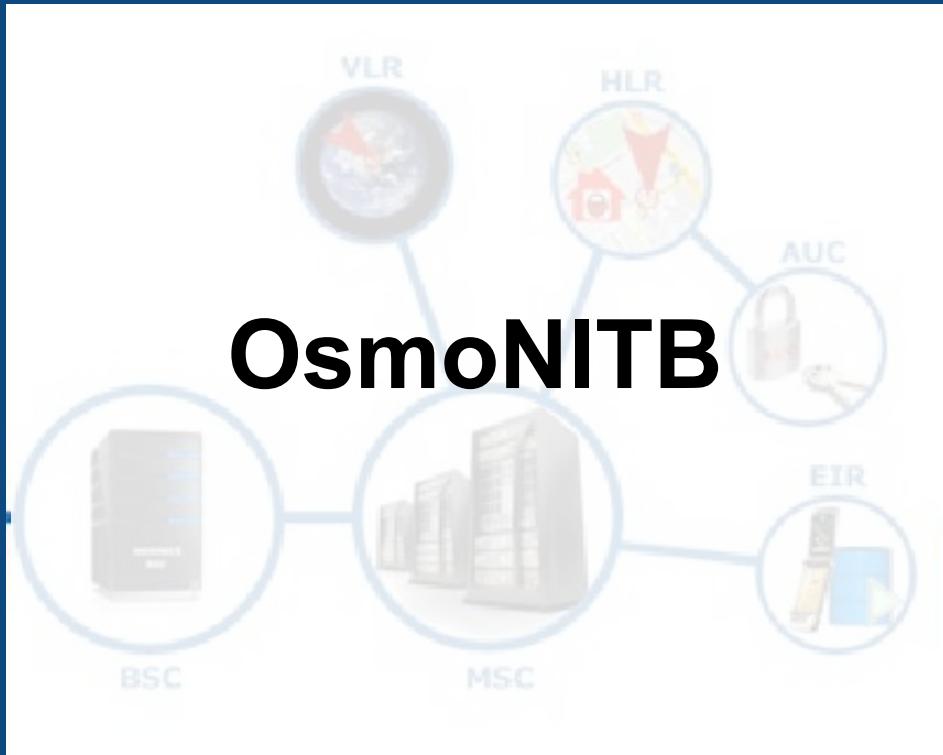


BSC
Base Station
Controller



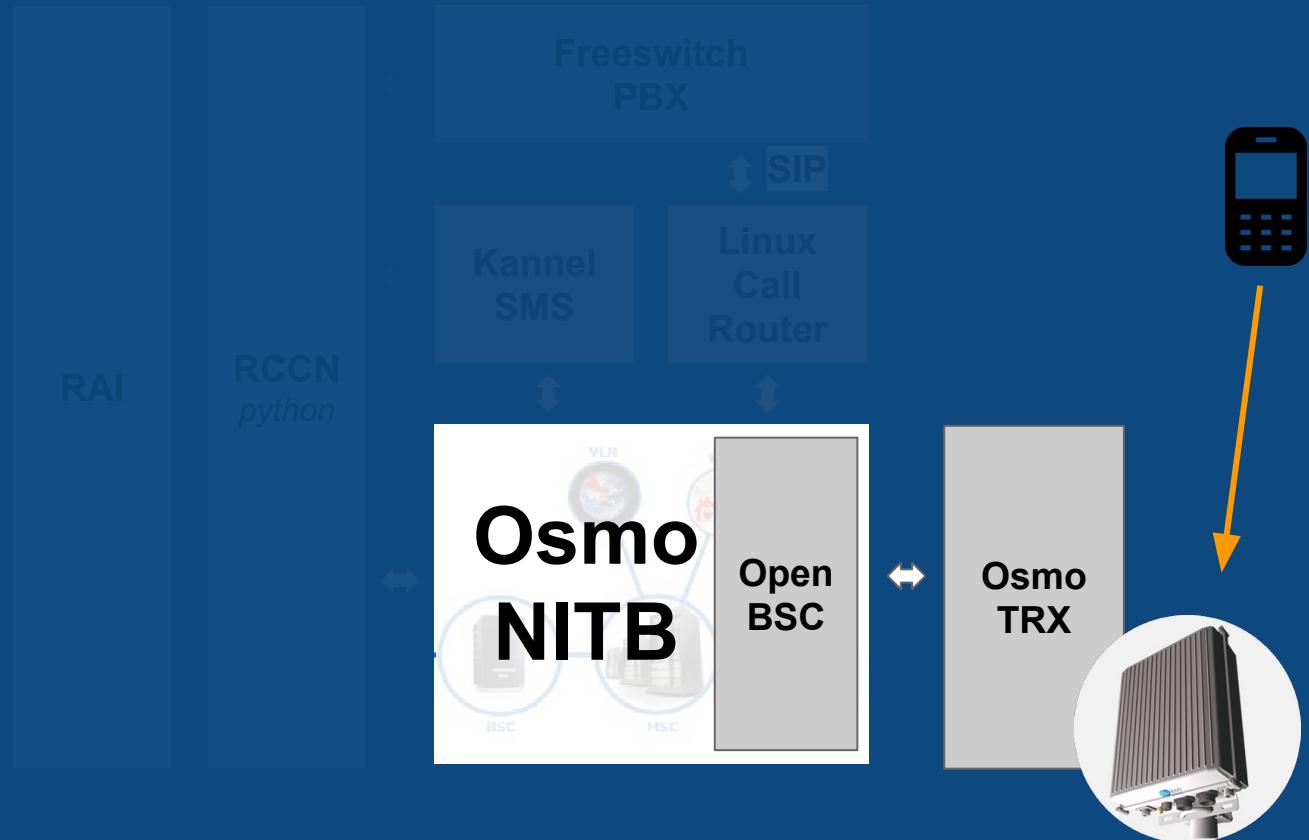


BSC
Base Station
Controller





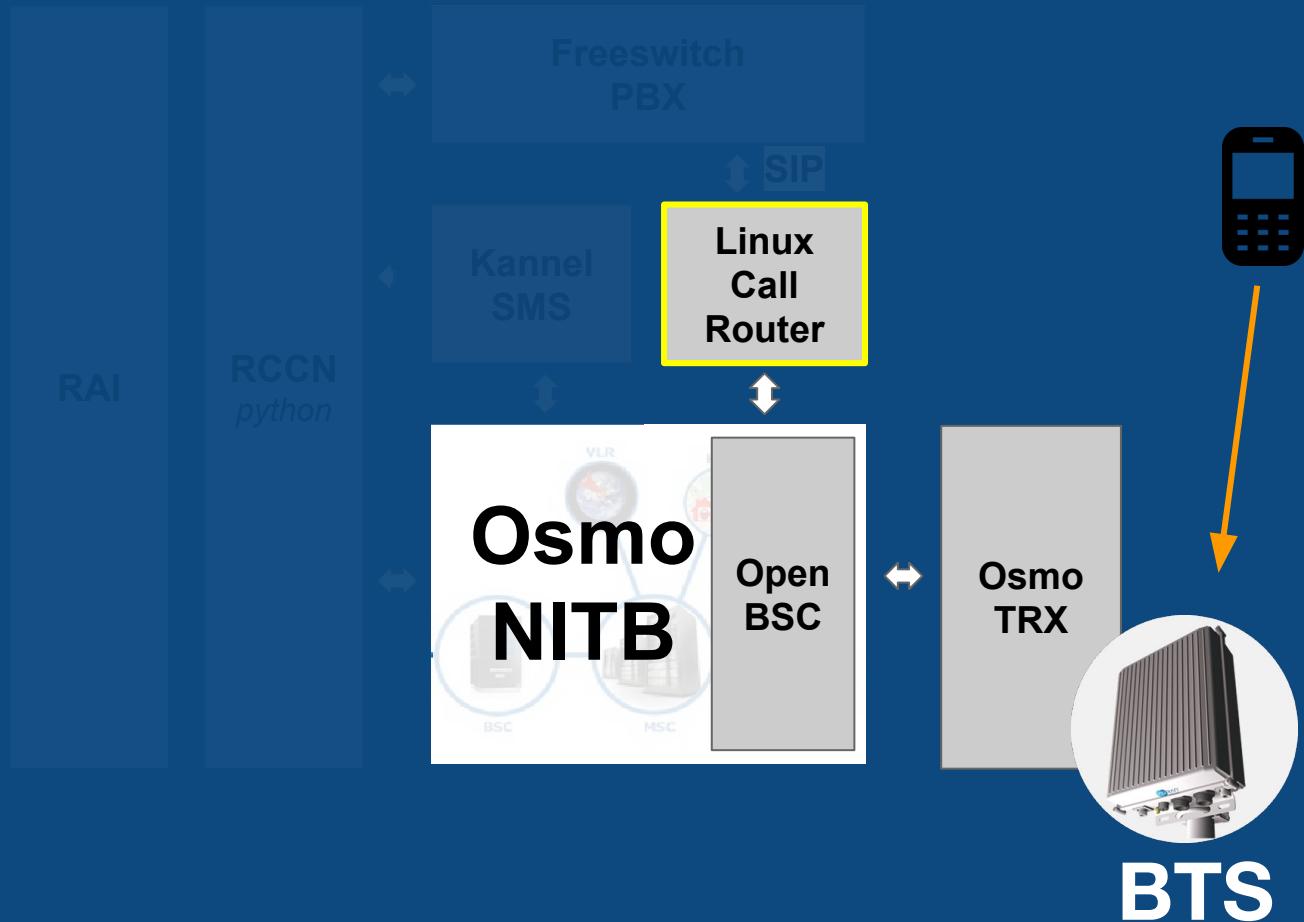
BSC
Base Station
Controller



BTS



BSC
Base Station
Controller

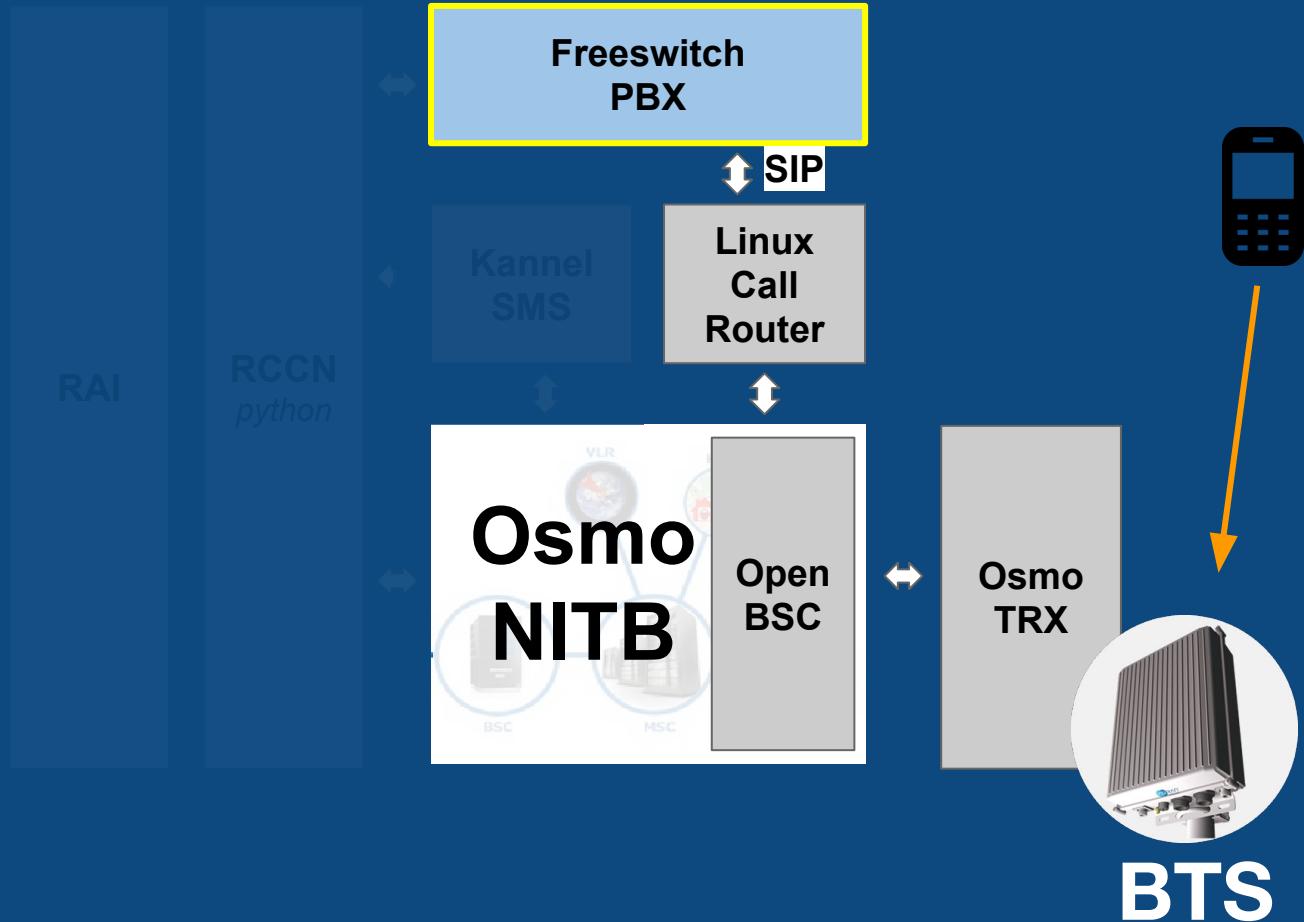




Linux Call Router
makes it possible to
connect telephones
to a Linux box.



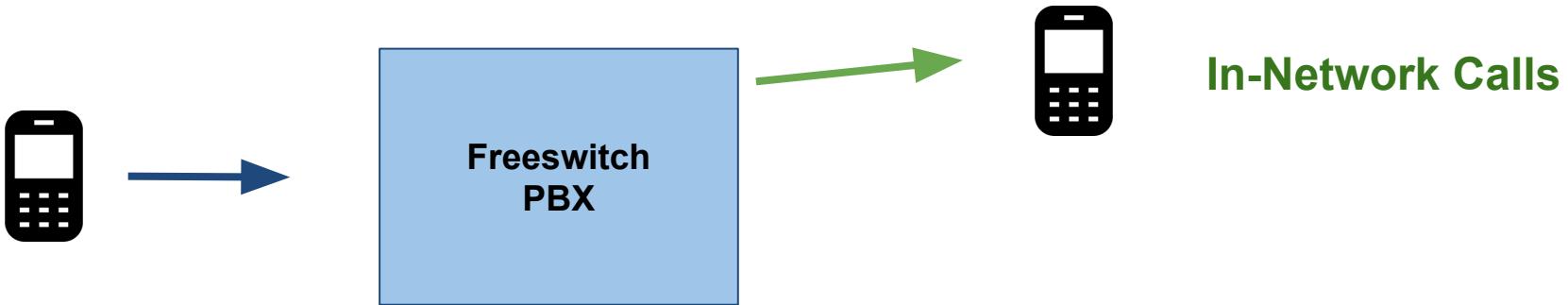
BSC
Base Station
Controller



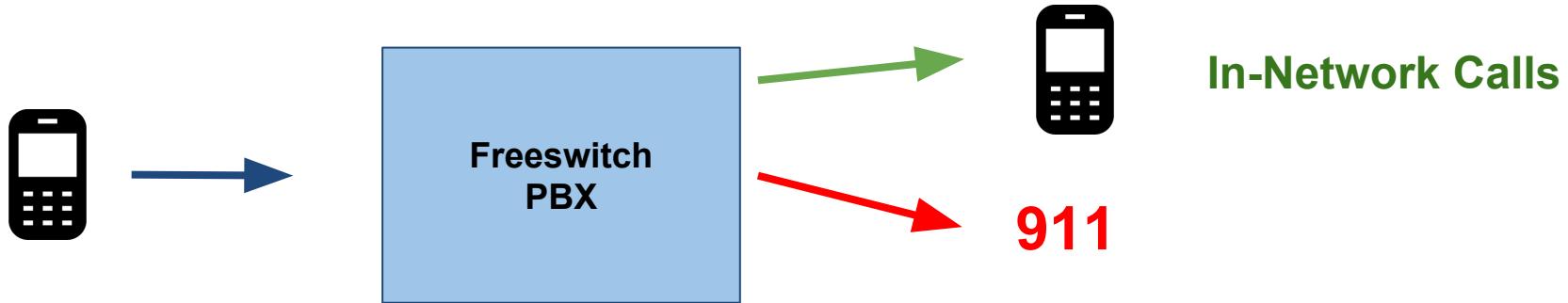


FreeSWITCH is a scalable open source cross-platform telephony platform designed to route and interconnect communication protocols.

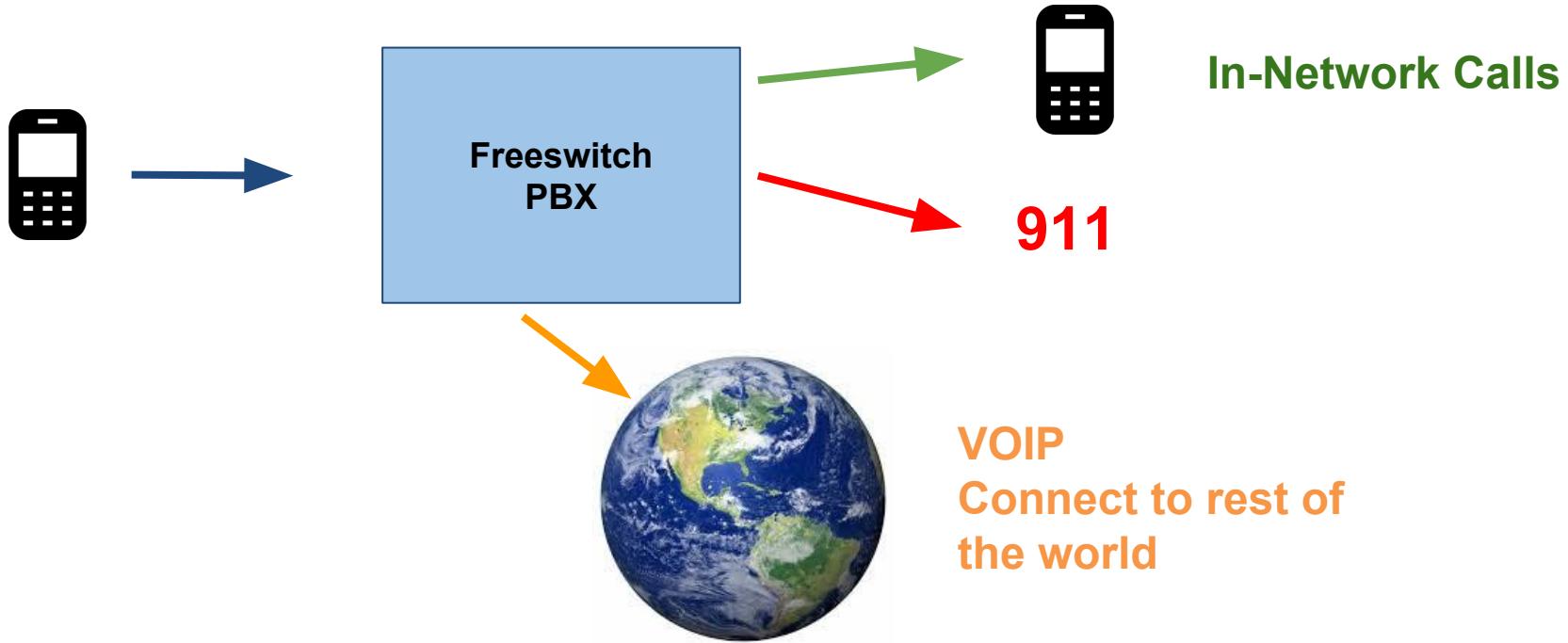
FreeSWITCH



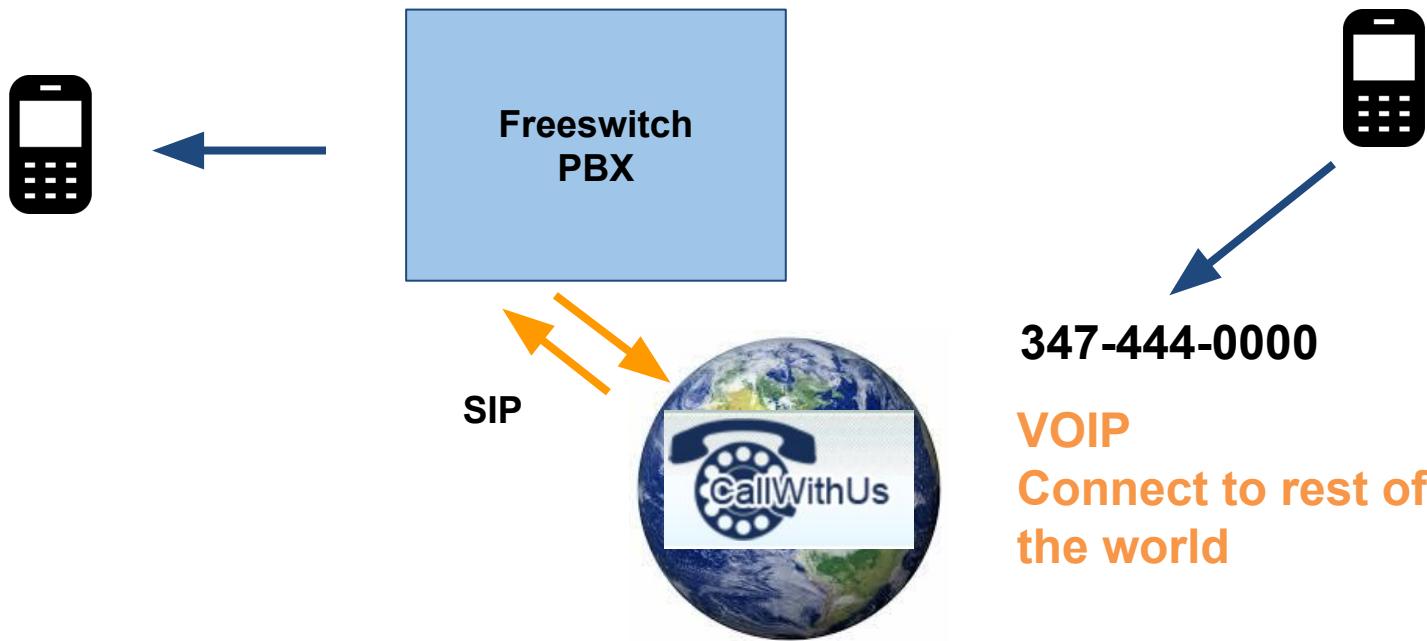
FreeSWITCH



FreeSWITCH

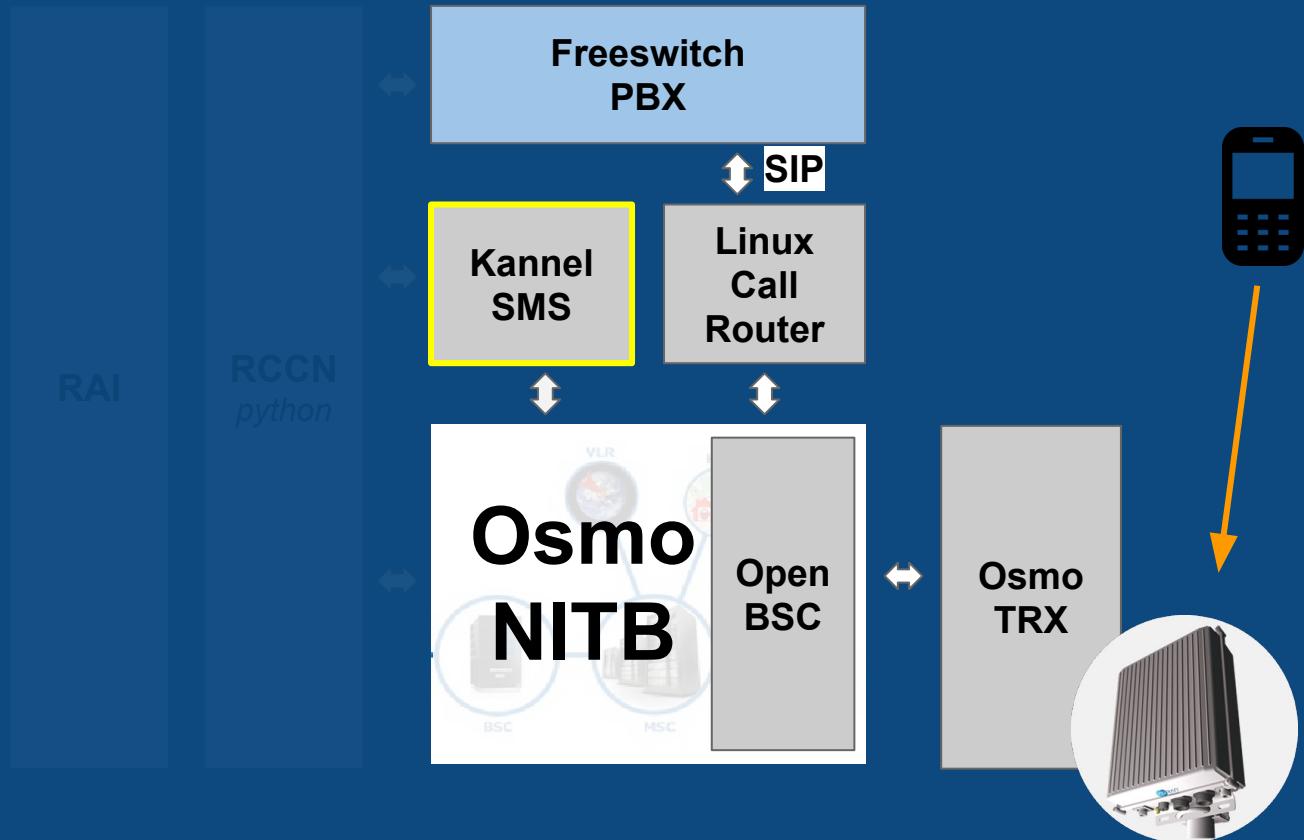


FreeSWITCH





BSC
Base Station
Controller

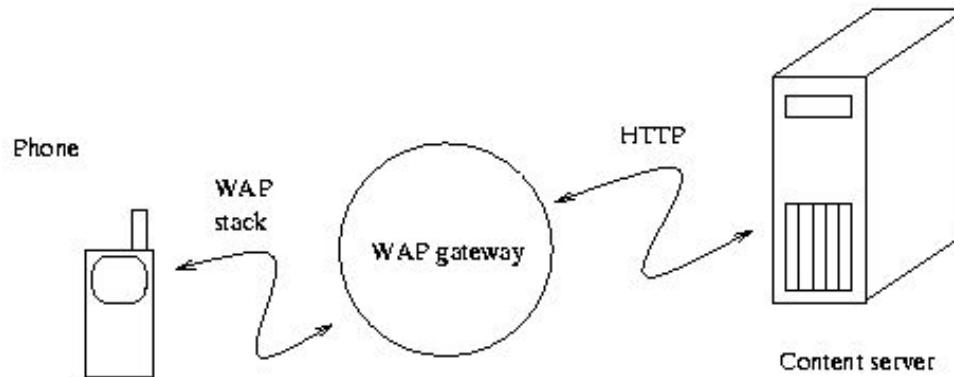


BTS

Kannel

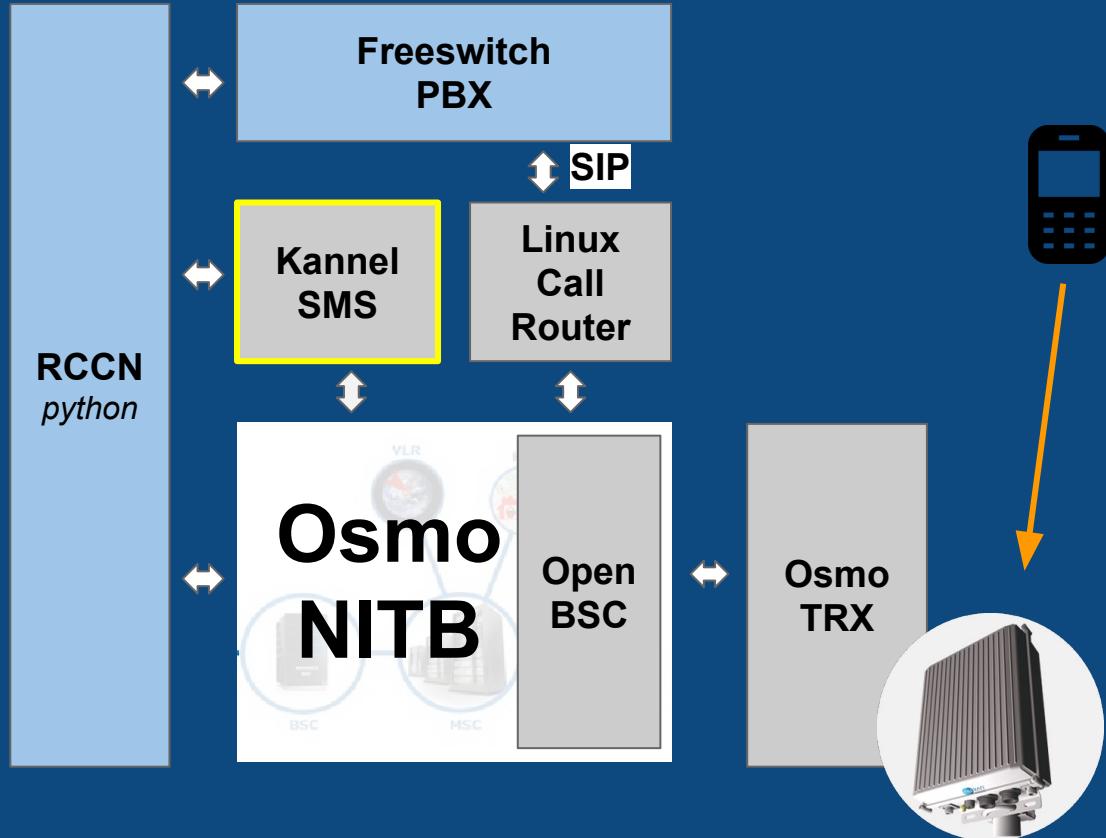
Kannel is a WAP and SMS gateway.

WAP (Wireless Application Protocol) gateway talks to the phone using the WAP protocol stack, and translates the requests it receives to normal HTTP.





BSC
Base Station
Controller



BTS



R H I Z O M A T I C A

RCCN

is a **python package** with the glue code that makes all the software components work together. It exposes a REST api, the RAPI.

[Code](#)[Issues 0](#)[Pull requests 0](#)[Projects 0](#)[Wiki](#)[Pulse](#)[Graphs](#)

Branch: master ▾

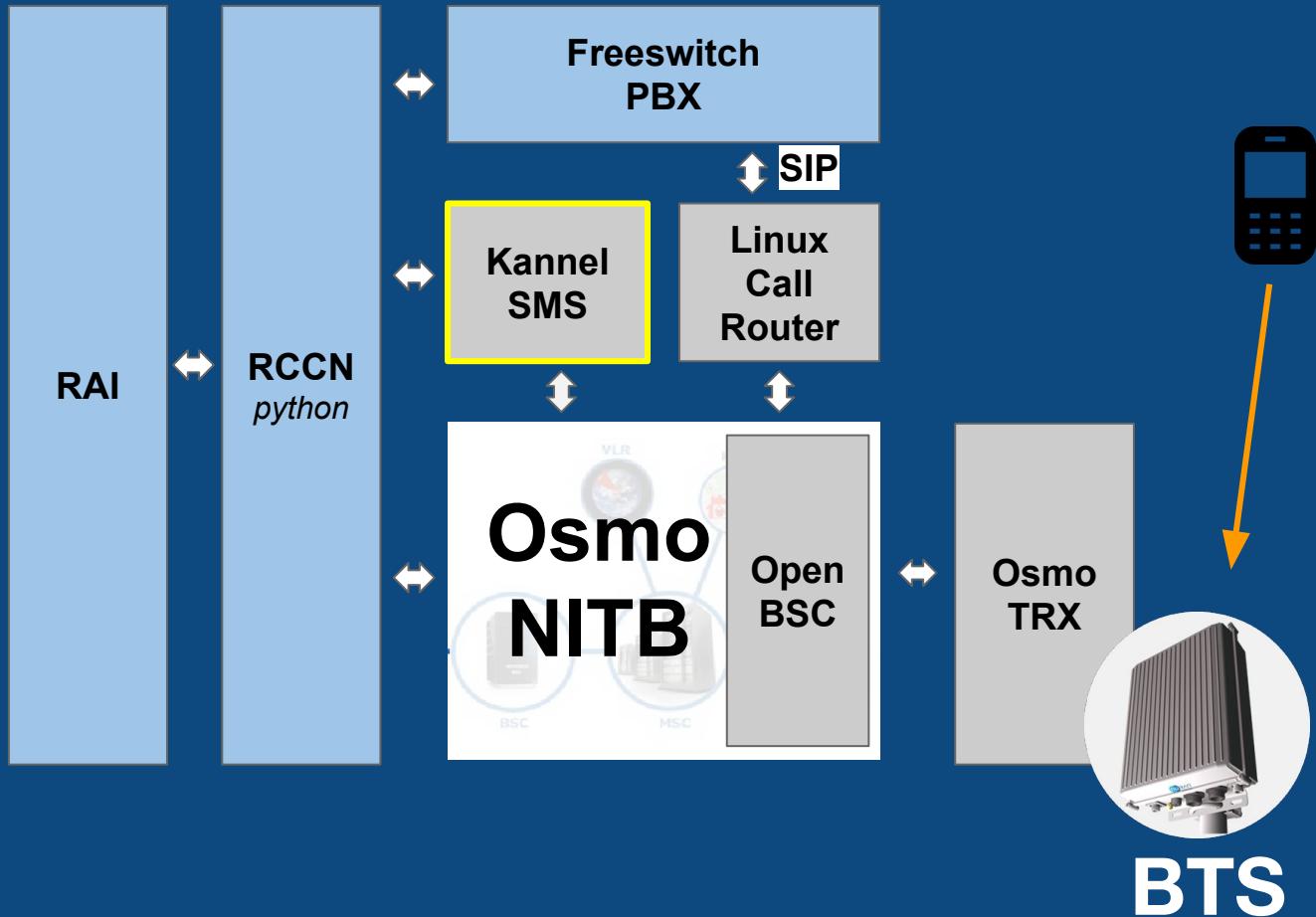
rccn / rccn /

[Create new file](#)[Upload files](#)[Find file](#)[History](#)

 Keith Make	in inbound loop work and add some more audio feedback	Latest commit 9154c98 17 days ago
..		
 extensions	Moved/deleted stuff, now it's only the content of /var/rhizomatica	3 years ago
 log	Renamed git_placeholder to .gitignore (to keep the empty directory)	3 years ago
 modules	Add a filter to drop some autogenerated SMS	17 days ago
 __init__.py	Moved/deleted stuff, now it's only the content of /var/rhizomatica	3 years ago
 config.py	Riak IP Address is configurable	6 months ago
 config_values.py.example	Added sms notification for when credit is added to a user.	2 years ago
 context.py	Make in inbound loop work and add some more audio feedback	17 days ago
 dialplan.py	Stop Unauthorised MS from calling DID number to get on system	17 days ago
 install.py	Fix decimal() into to_decimal() in install.py	2 years ago
 populate_distributed_db.py	Add riak_ip_address to populate_dist db	a month ago
 push.py	More info on d_hlr anomalies	5 months ago
 rapi.py	Add IMEI stuff to rapi	6 months ago
 rccn.py	Stop Unauthorised MS from calling DID number to get on system	17 days ago
 rhs.py	debugging rhs	2 years ago
 rip.py	Fix RIP cron job, exclude msisdn==10000	2 years ago
 rrc.py	more roaming stuff	7 months ago
 rsc.py	Some help to track down monthly deactivation problems	10 months ago
 wi.py	Add some scripts for D_HLR management	5 months ago



BSC
Base Station
Controller





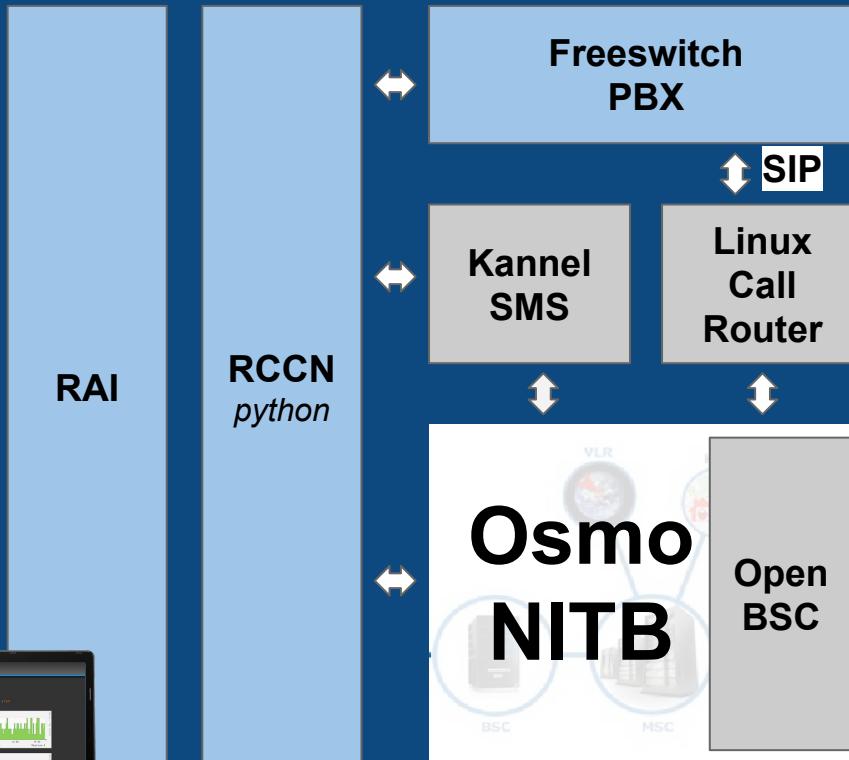
R H I Z O M A T I C A

RAI

is a php package that uses the REST api and exposes an http administrative interface, allowing admins to register users, manage payments, broadcast text messages and access the live system statistics.



BSC
Base Station
Controller

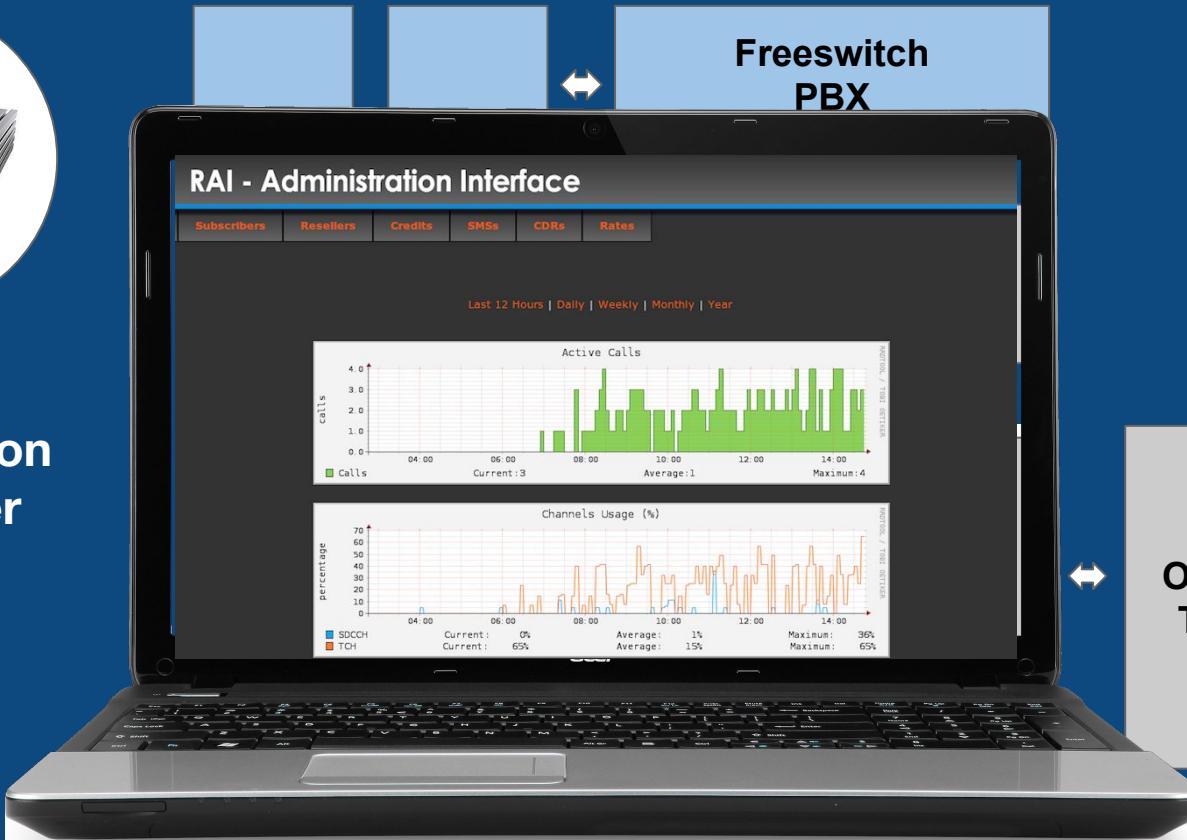


SIP





BSC
Base Station
Controller



Freeswitch
PBX

Osmo
TRX

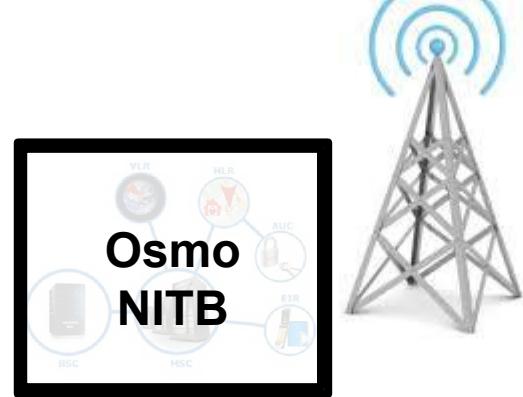
ROAMING



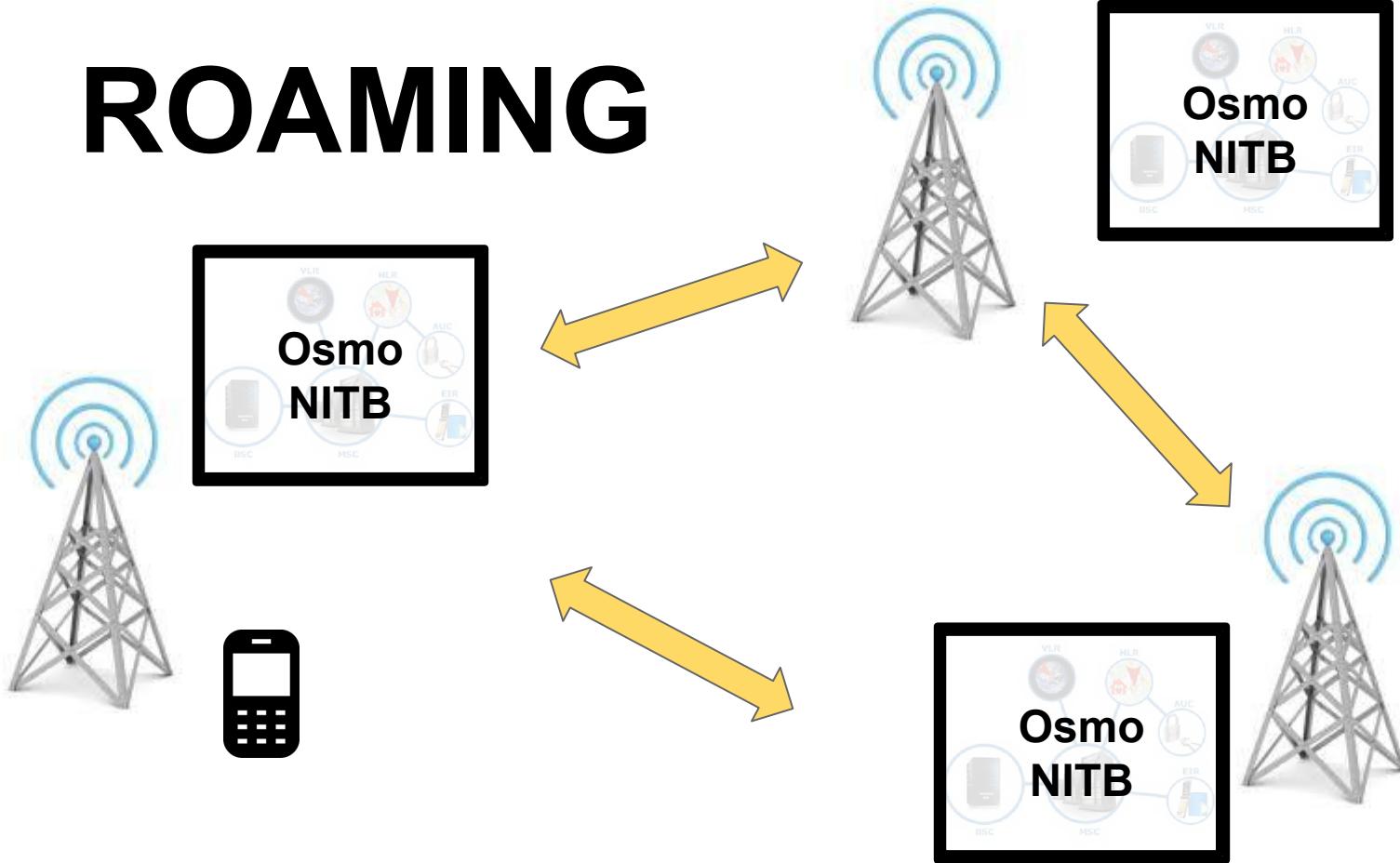
ROAMING



ROAMING

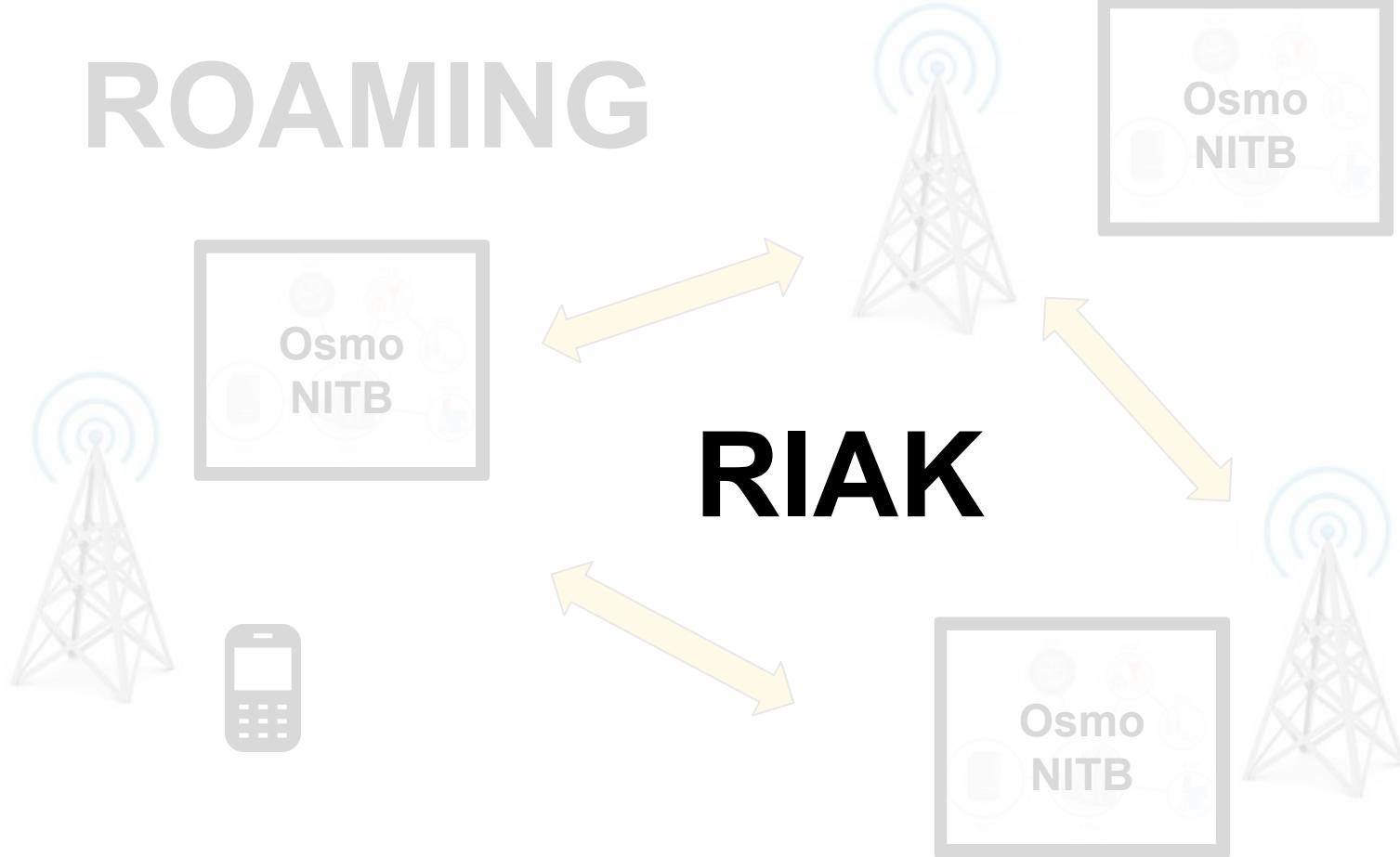


ROAMING



ROAMING

RIAK



RIAK

ROAMING

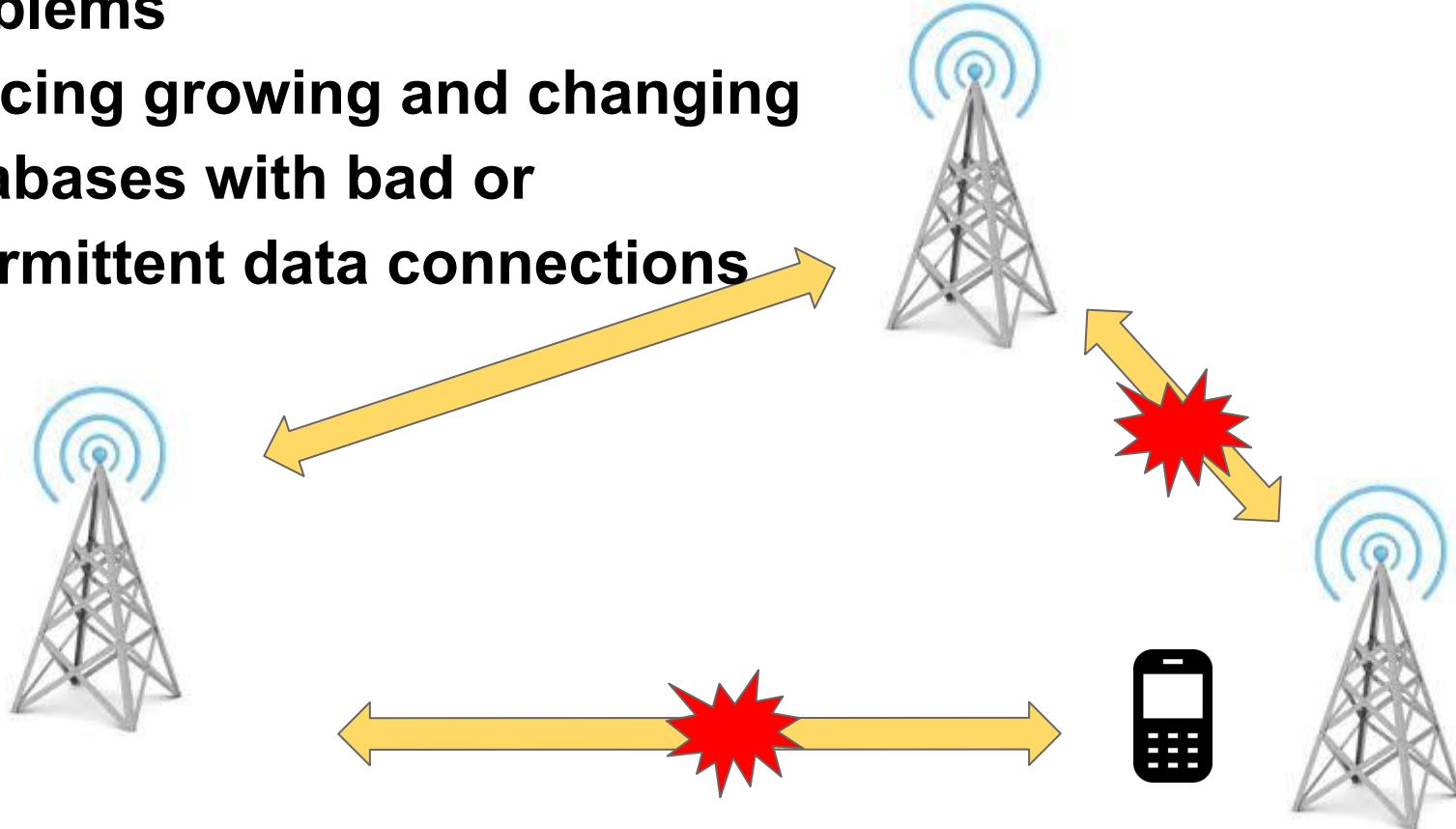


Distributed NoSQL Database

Riak KV is a distributed NoSQL database that is highly available, scalable and easy to operate. It automatically distributes data across the cluster to ensure fast performance and fault-tolerance.

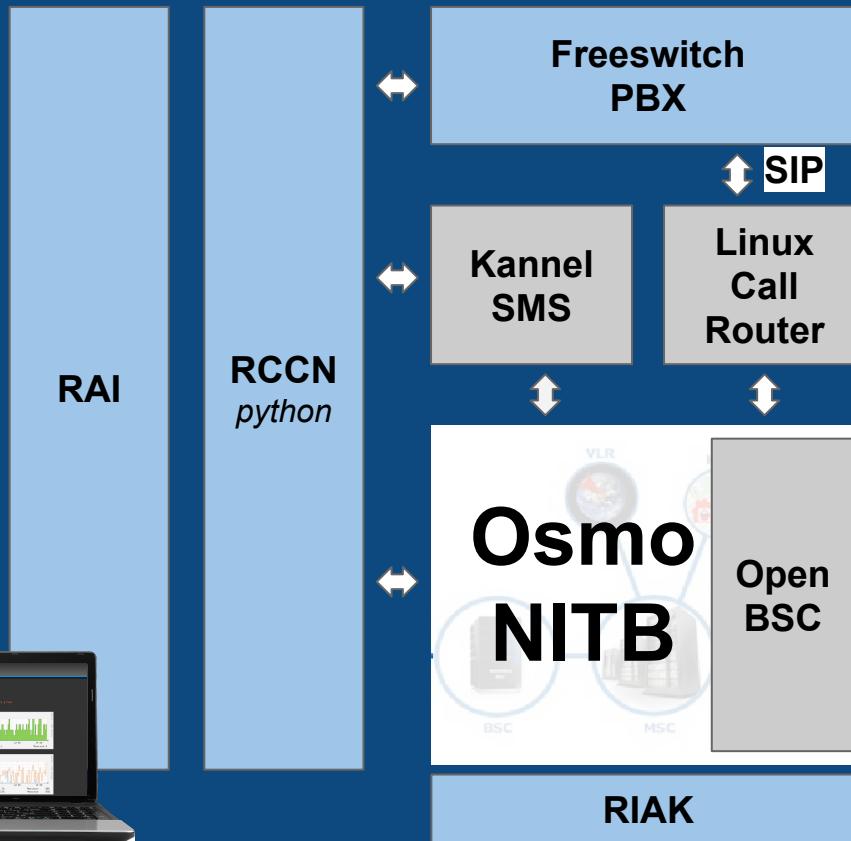
Problems

**Syncing growing and changing
databases with bad or
intermittent data connections**





BSC
Base Station
Controller



Installation



BSC
Base Station
Controller

Installing Ubuntu

1. Download Ubuntu 12.04.5 Server 64bit
2. Make Bootable Flash Drive with Ubuntu 12.04.5 - Startup disk creator.
3. Copy this [rhizomatica.seed](https://github.com/Rhizomatica/puppet) to the preseed directory folder inside the bootable flash drive. - <https://github.com/Rhizomatica/puppet>
4. Replace the ubuntu-server.seed file with the rhizomatica.seed. AKA delete the ubuntu-server.seed and rename the rhizomatica.seed file to ubuntu-server.seed
5. Attach the Bootable Flash to the BSC with a monitor mouse and keyboard. Follow the installation instructions.



(Virtual Private Network)

Public IP
186.245.124.111



Cloud Server

Public IP
186.245.124.111



Cloud Server

VPN Server
10.99.0.1

Public IP
186.245.124.111



Cloud Server

VPN Server
10.99.0.1



BSC1

Public IP
186.245.124.111



Cloud Server

VPN Server
10.99.0.1



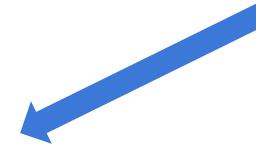
BSC1
VPN Client
10.99.0.2

Public IP
186.245.124.111



Cloud Server

VPN Server
10.99.0.1



BSC1
VPN Client
10.99.0.2



Public IP
186.245.104.000



Cloud Server

VPN Server
10.89.0.1

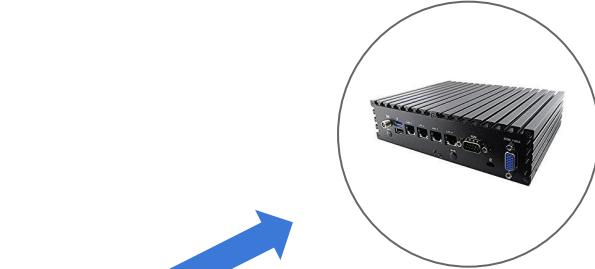




Public IP
186.245.124.111



Cloud Server
VPN Server
10.99.0.1



BSC1
VPN Client
10.99.0.2



puppet

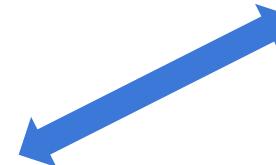
Puppet provides way of delivering operating software, updates and configurations to several remote servers

Puppet



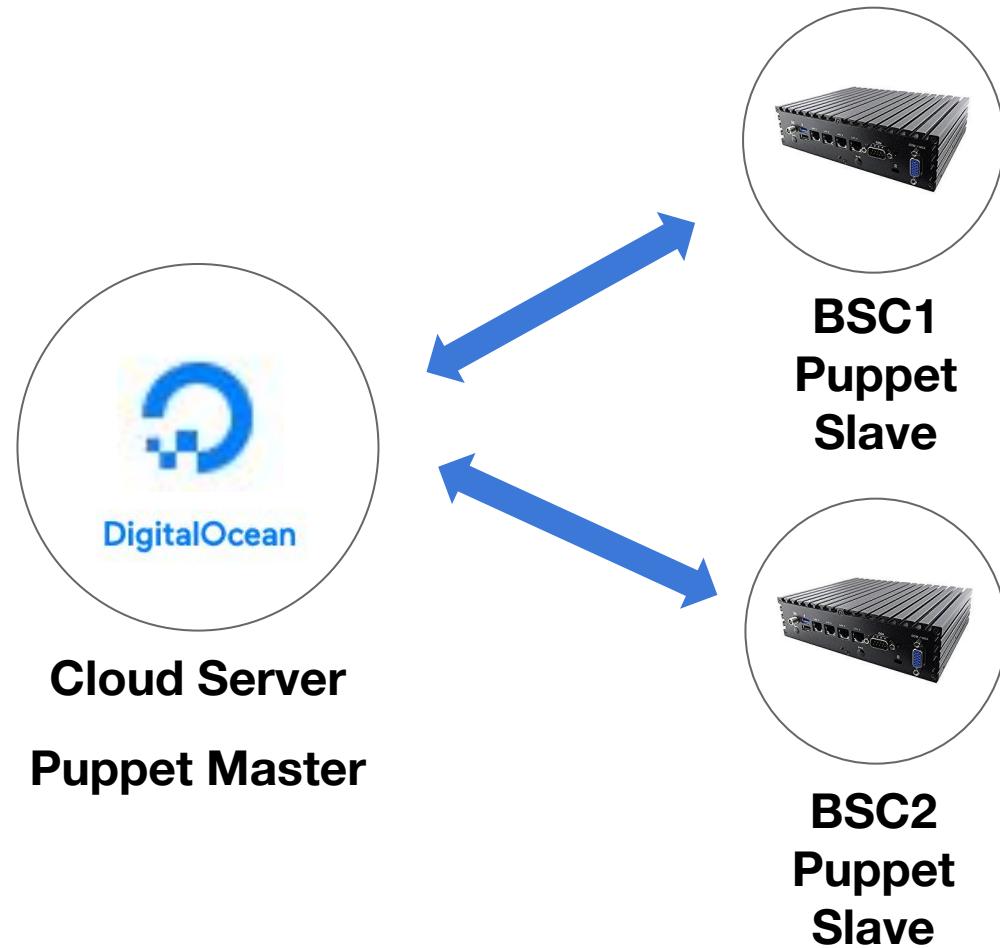
Cloud Server

Puppet Master

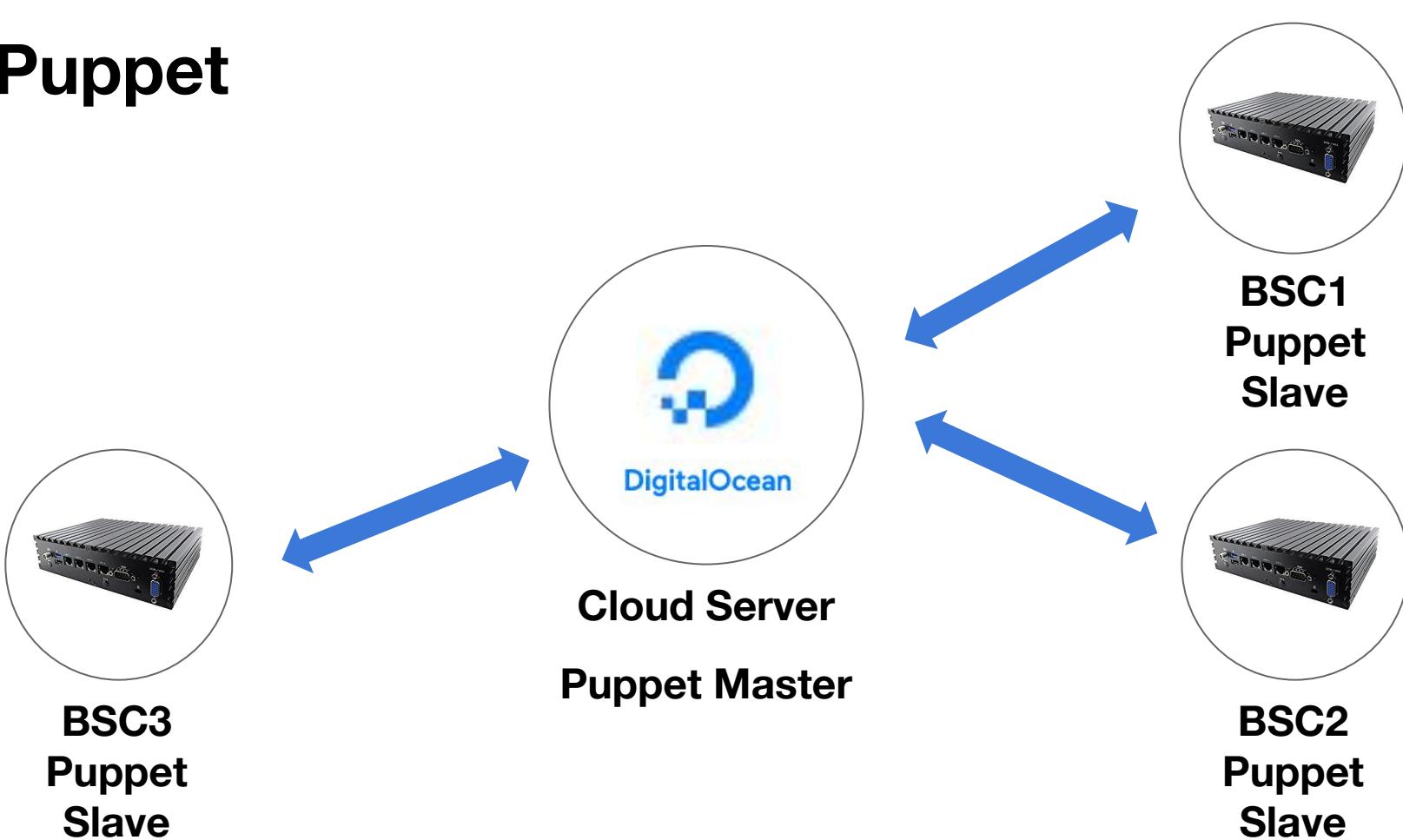


**BSC1
Puppet
Slave**

Puppet



Puppet



Puppet

**Use Rhizomatica Puppet Recipe
To install GSM System**

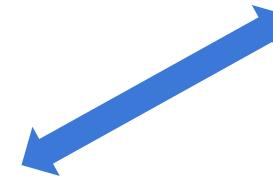
Full instructions:

<https://github.com/Rhizomatica/puppet>



Cloud Server

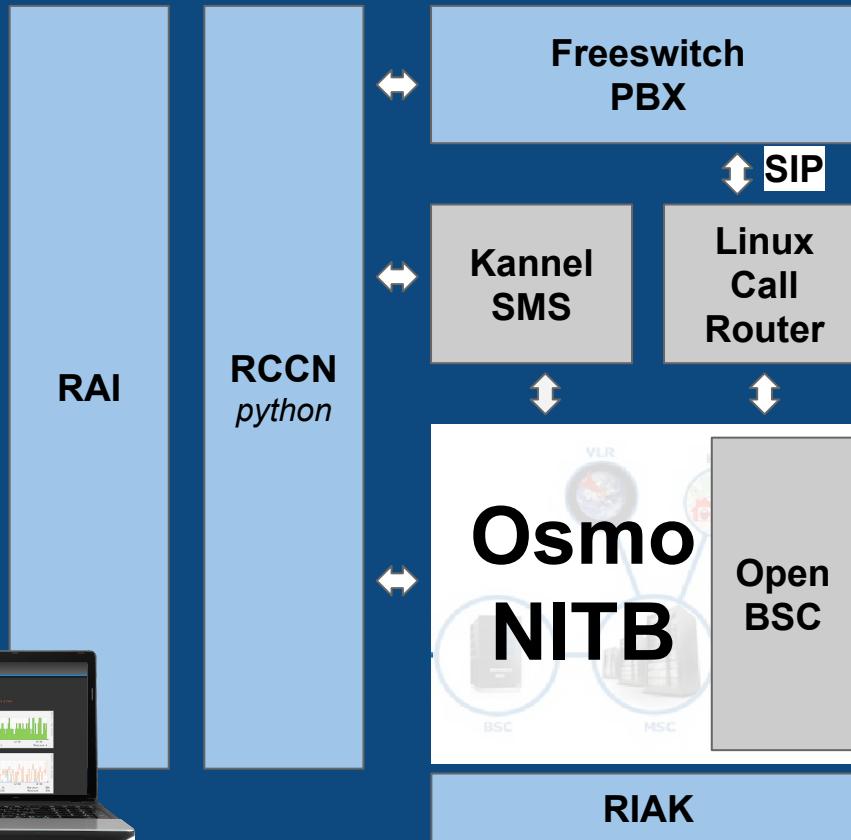
Puppet Master



**BSC1
Puppet
Slave**



BSC
Base Station
Controller



After running puppet several times you should have a working system, although there will be several fixes that need to be completed.

SETUP BTS SCRIPT

Use Fabric to install:
`setup-bts.py`

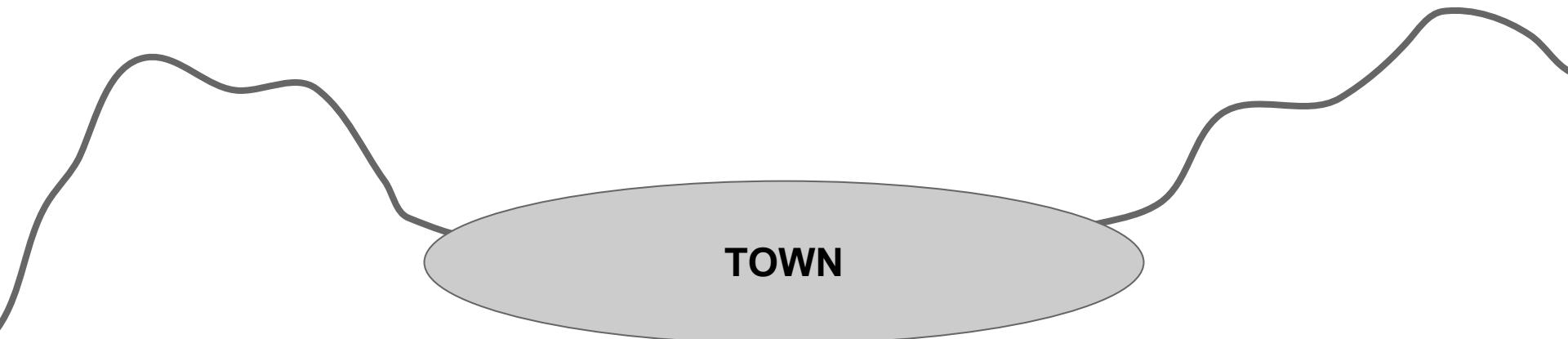


BTS
**Base Transceiver
Station**

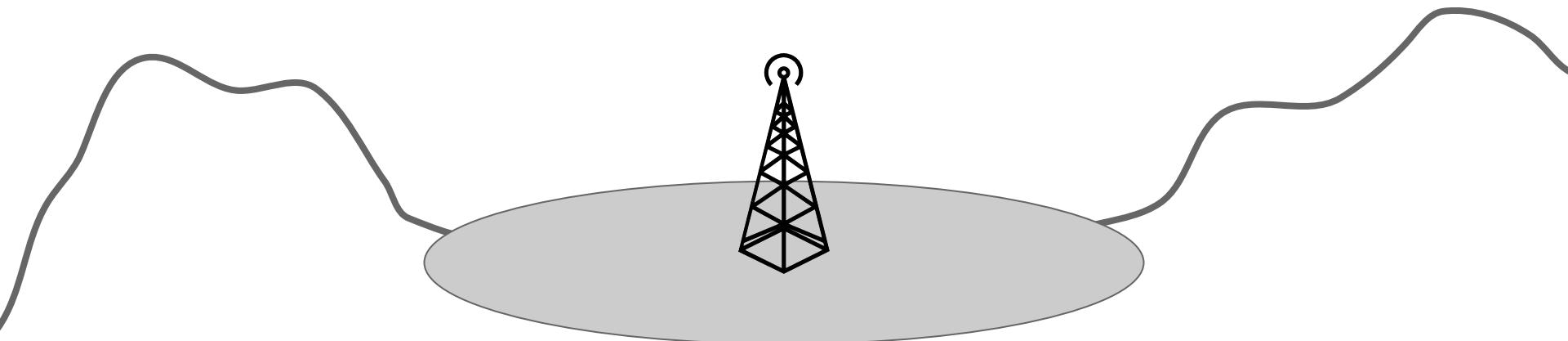
Site Location

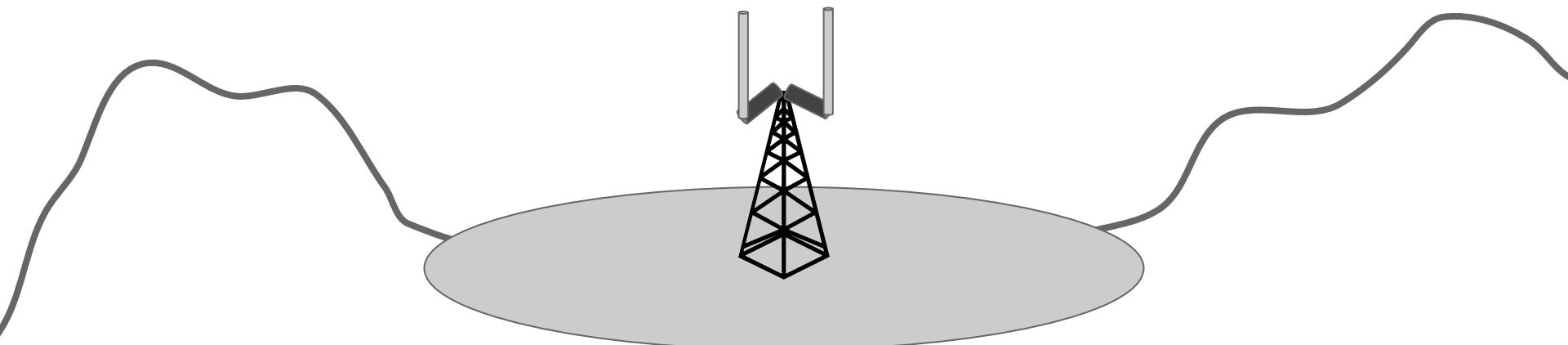


Site Location



Site Location





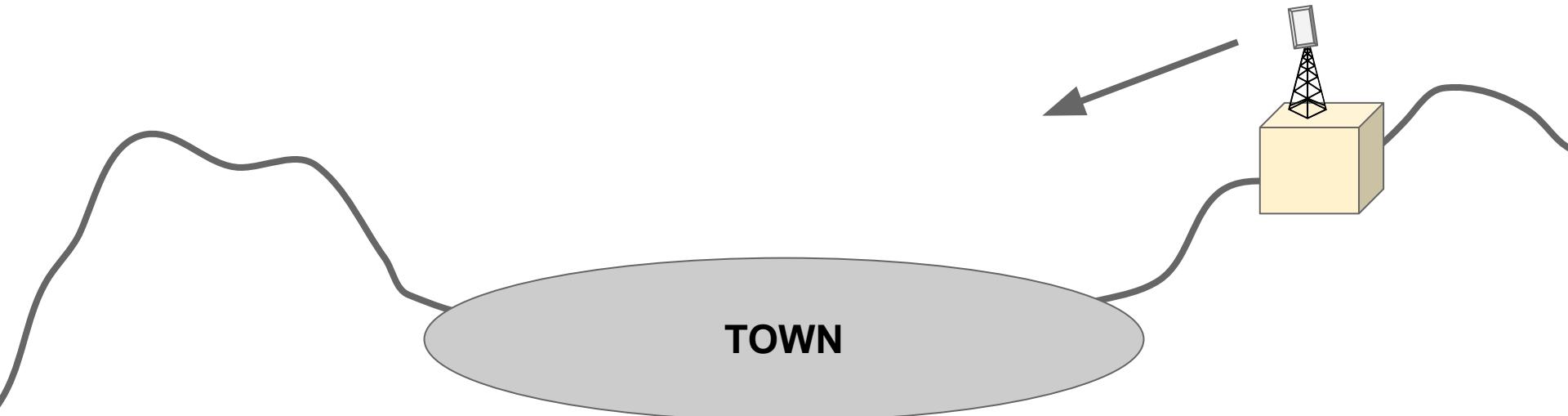
Site Location

Omni Directional Antenna
(antennas at least 6 feet apart)



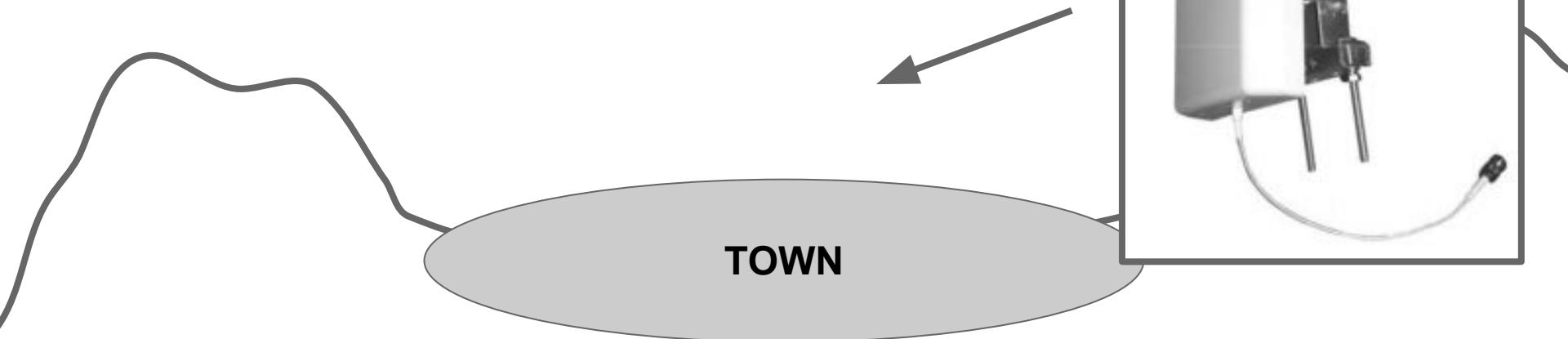
Site Location

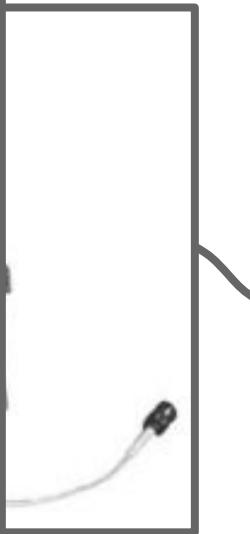
Patch Antennas



Site Location

Patch Antennas

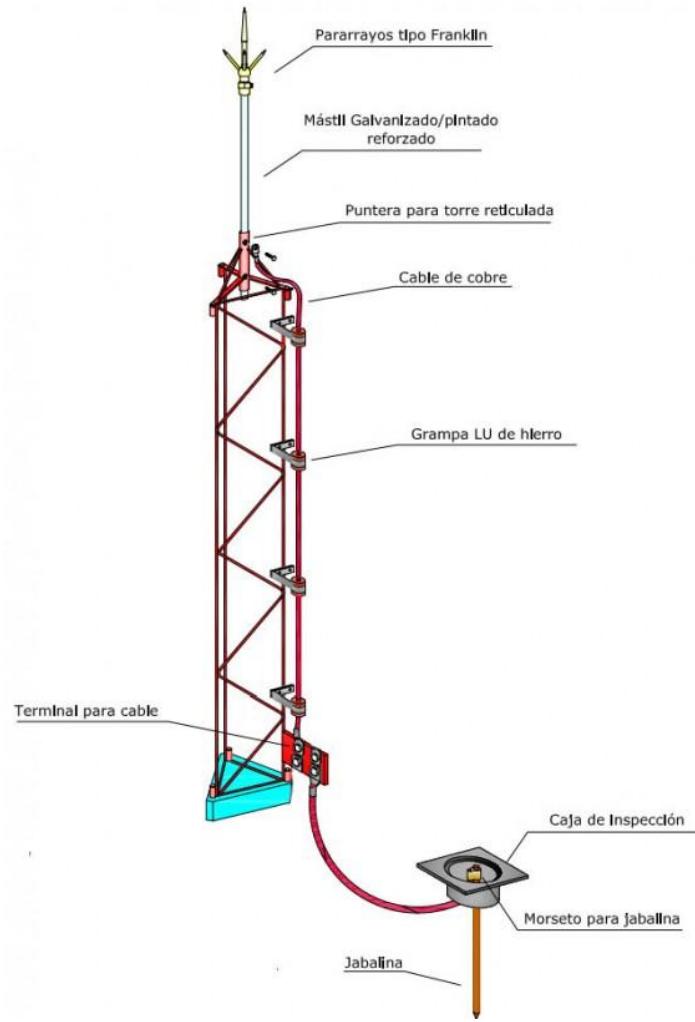




Tower Lighting Protection

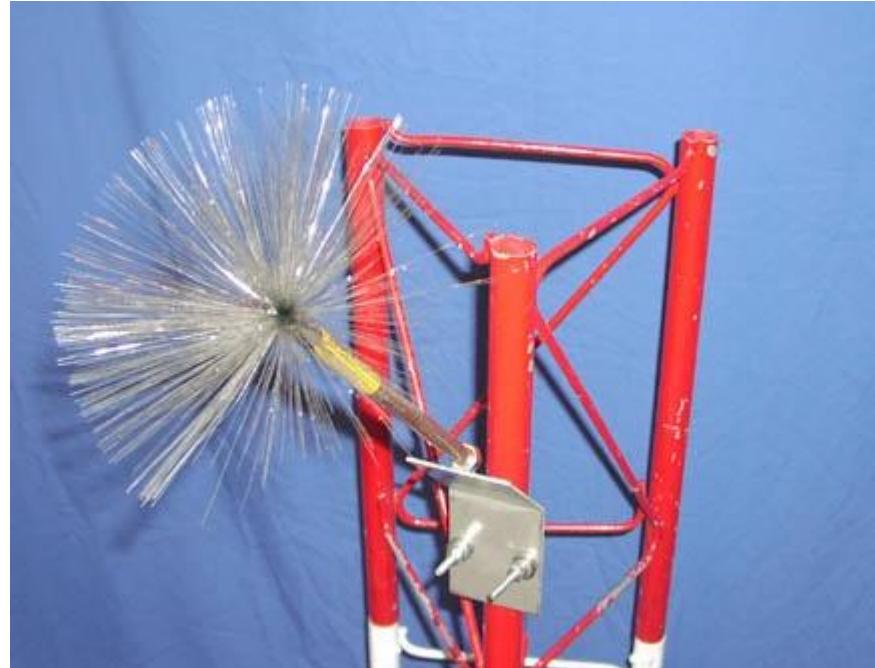
Lightning Protection

- Grounding



Lightning Protection

- Lightning
Dissipator



Climbing Gear





Waterproof Connections

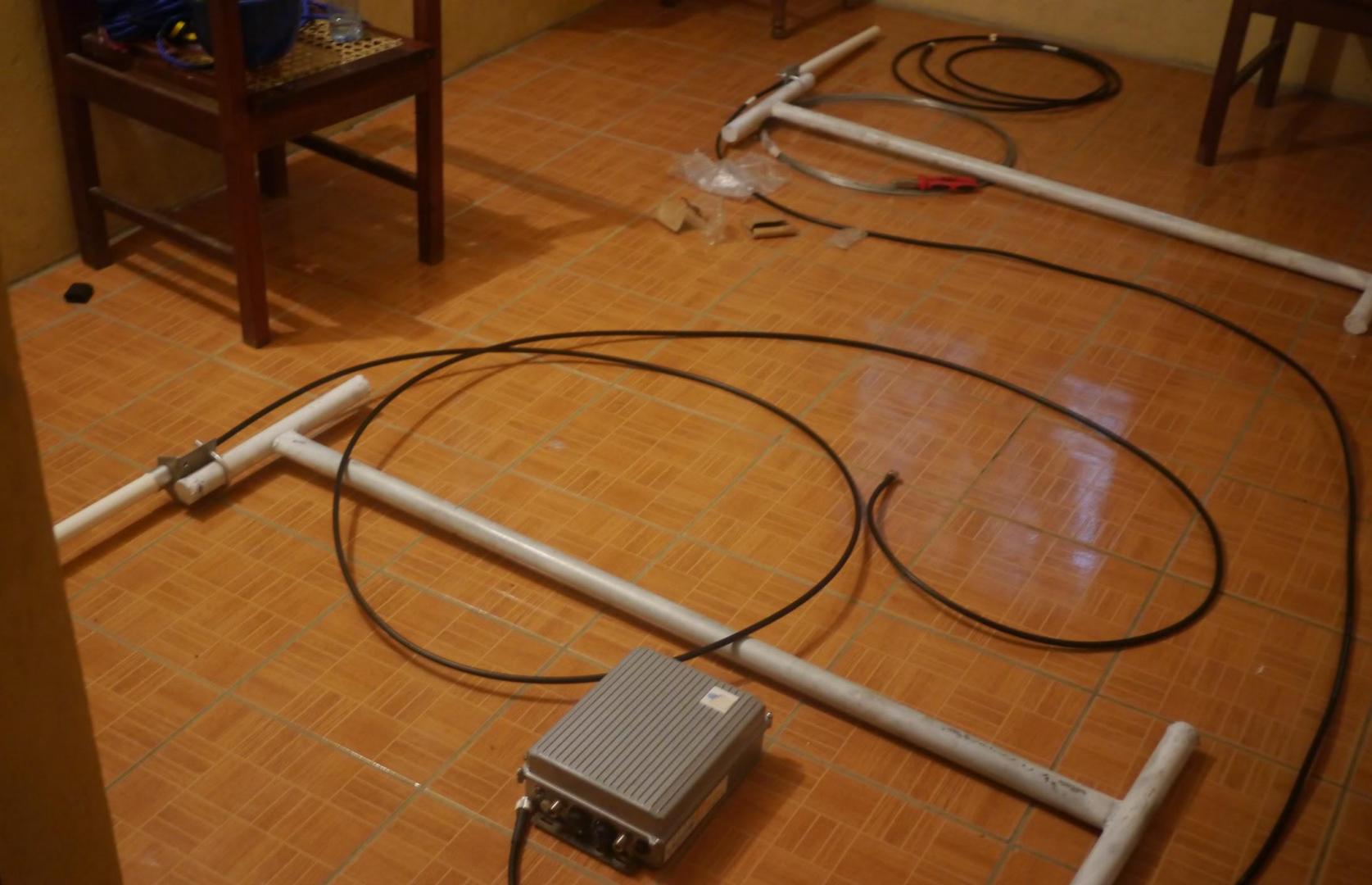


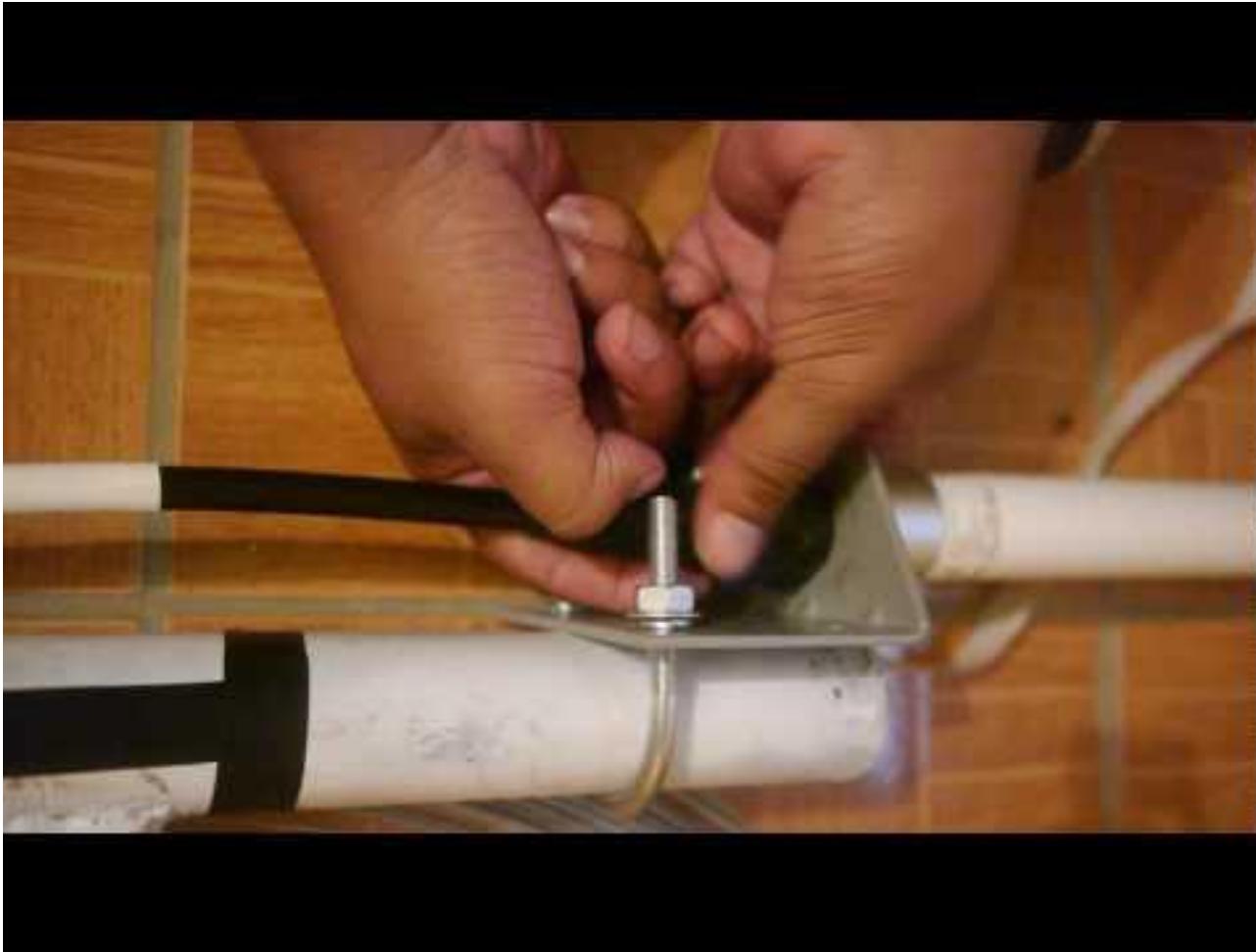
**Tape > Coax Seal >
Tape**



Tower Installation Prep









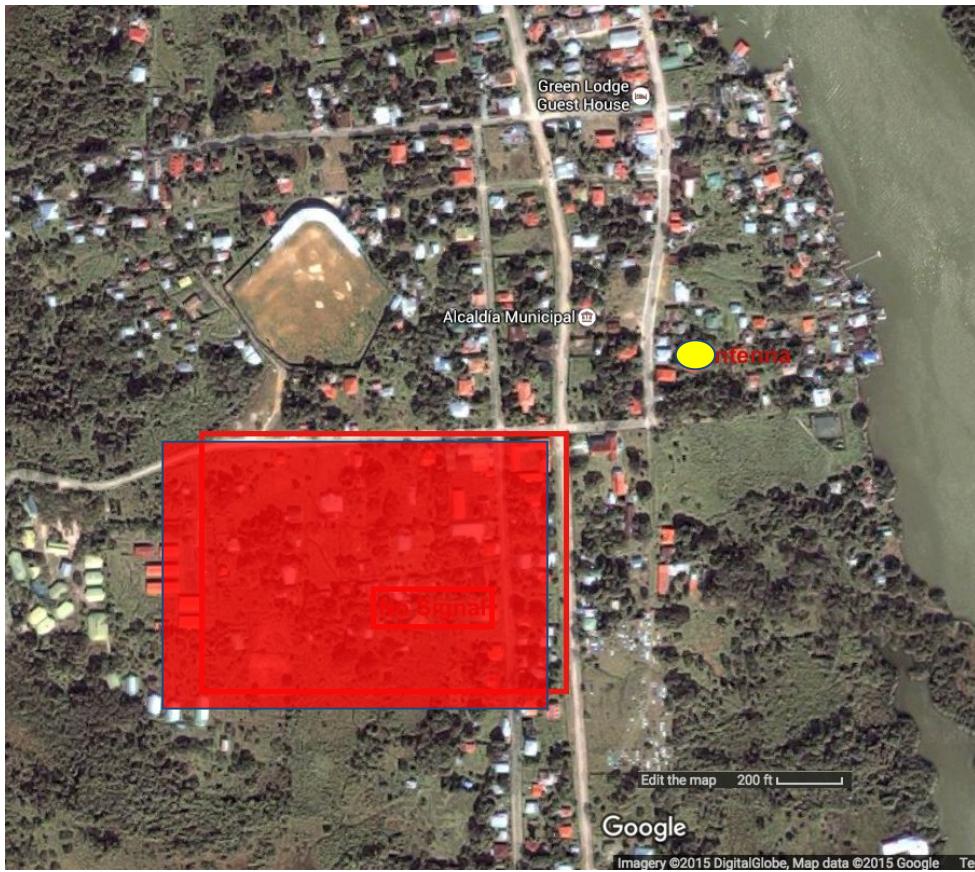








RF Troubleshooting













BSC
**Base Station
Controller**





BSC
**Base Station
Controller**





BSC
Base Station
Controller

Installing Ubuntu

1. Download Ubuntu 12.04.5 Server 64bit
2. Make Bootable Flash Drive with Ubuntu 12.04.5 - Startup disk creator.
3. Copy this [rhizomatica.seed](https://github.com/Rhizomatica/puppet) to the preseed directory folder inside the bootable flash drive. - <https://github.com/Rhizomatica/puppet>
4. Replace the ubuntu-server.seed file with the rhizomatica.seed. AKA delete the ubuntu-server.seed and rename the rhizomatica.seed file to ubuntu-server.seed
5. Attach the Bootable Flash to the BSC with a monitor mouse and keyboard. Follow the installation instructions.



BSC
Base Station
Controller



BTS
Base Transceiver
Station