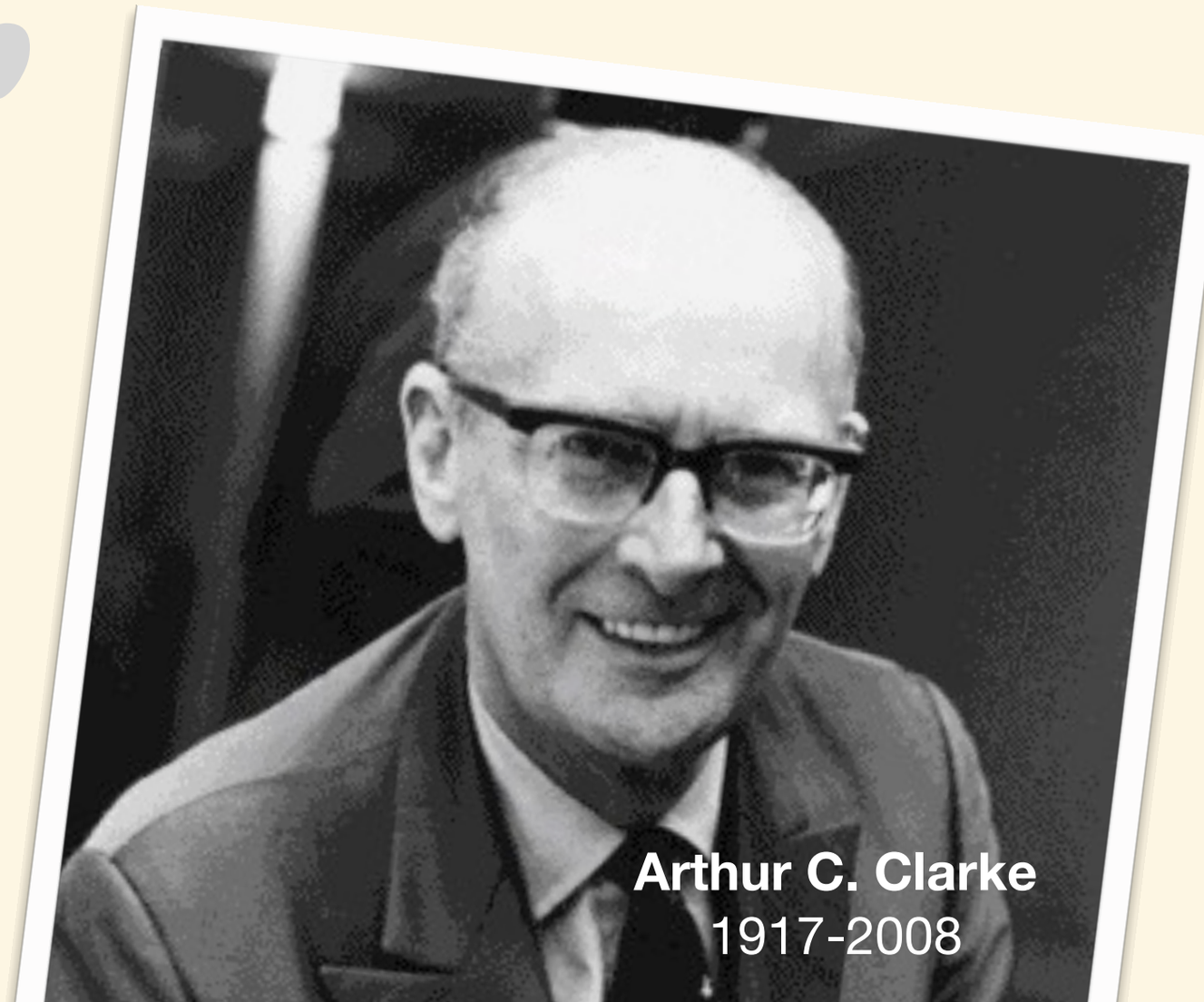
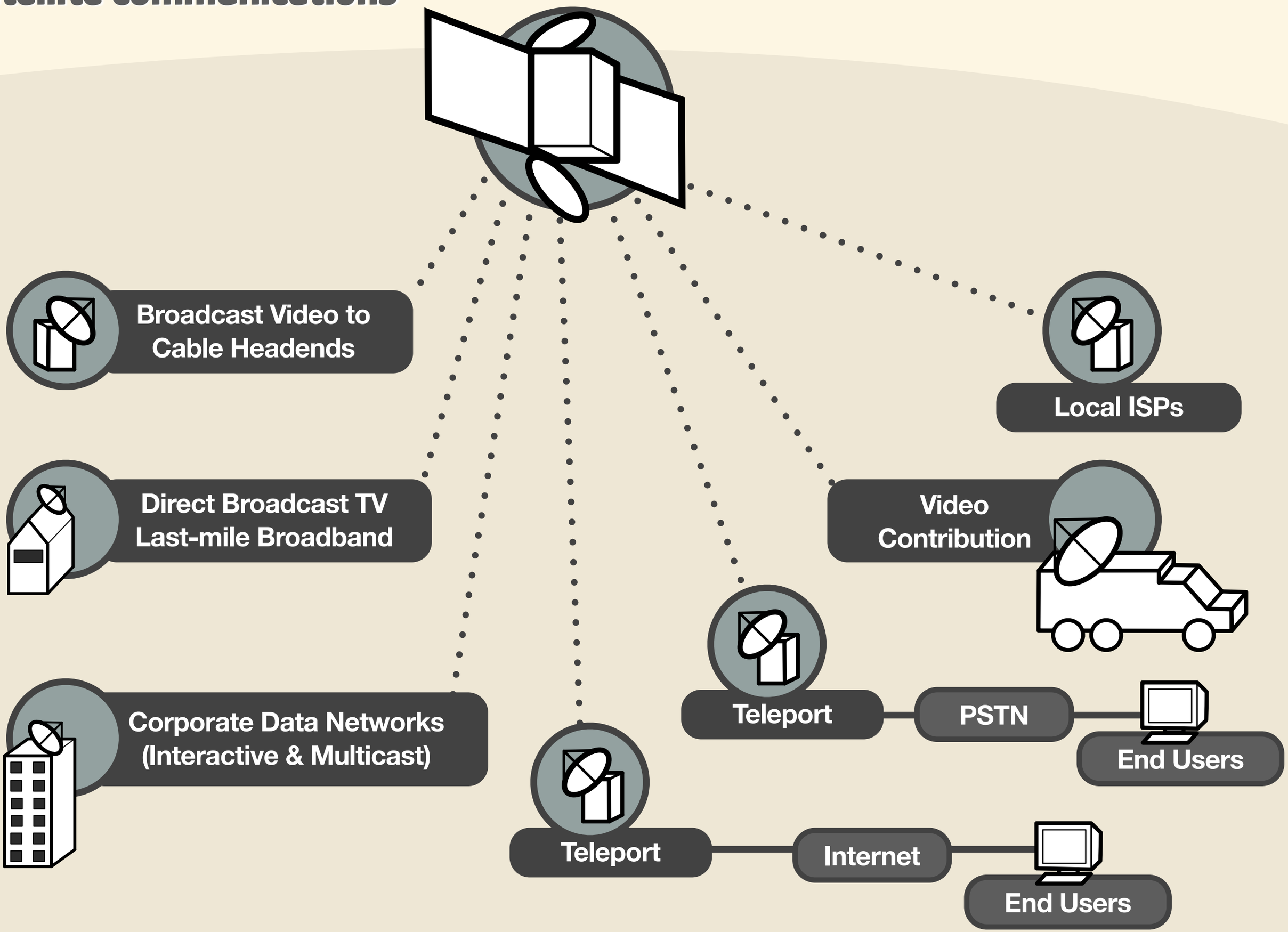
Satellite Telephony Security

DON’T PANIC

“WHEN TERRESTRIAL COMMUNICATION **FAIL**, **WE PREVAIL!**”



Satellite Communications



Dan Veeneman
Low Earth Orbit Satellites

Dan Veeneman
Future & Existing Satellite Systems

Warezzman
DVB Satellite Hacking

Jim Geovedi, Raditya Iryandi,
Hacking a Bird in the Sky: Hijacking VSAT Connection

Jim Geovedi, Raditya Iryandi, Anthony Zboralski
Hacking a Bird in the Sky: Exploiting Satellite Trust Relationship

Adam Laurie
$atellite Hacking for Fun & Pr0fit!

Leonardo Nve Egea, Christian Martorella
Playing in a Satellite Environment 1.2

Jim Geovedi, Raditya Iryandi
Hacking Satellite: A New Universe to Discover

Jim Geovedi, Raditya Iryandi, Raoul Chiesa
Hacking a Bird in the Sky: The Revenge of Angry Birds

Jim Geovedi
Satellite Telephony Security: What Is and What Will Never Be

1996 1998 2004 2006 2008 2009 2011

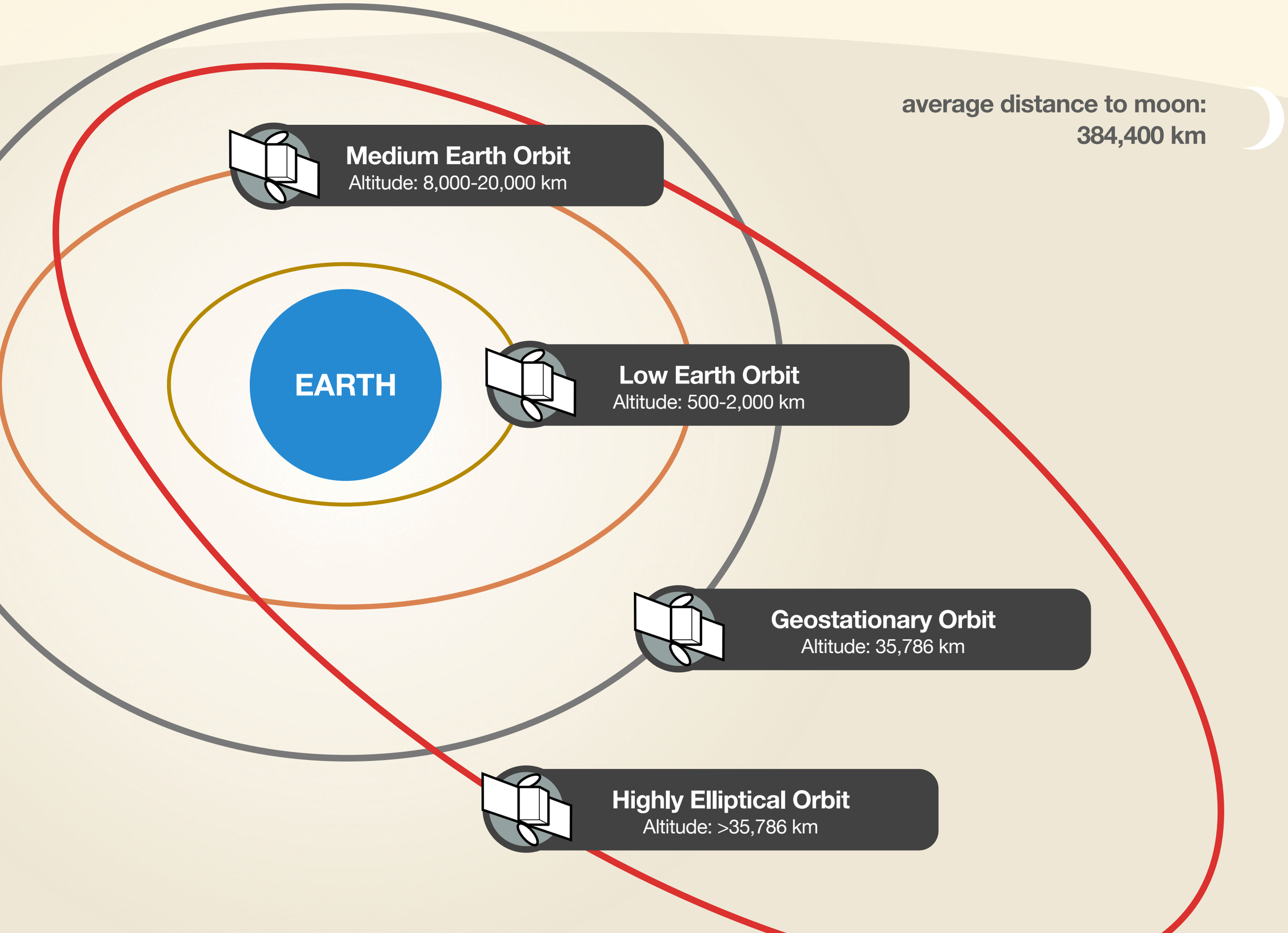
Satellite Phone


PRESS
AP


Globalstar
Home
12:00 PM
Wednesday April 2, 2008
No upcoming appointments
1 Active task
Calendar
Contacts

Satellite Phone Network

Satellite Orbits



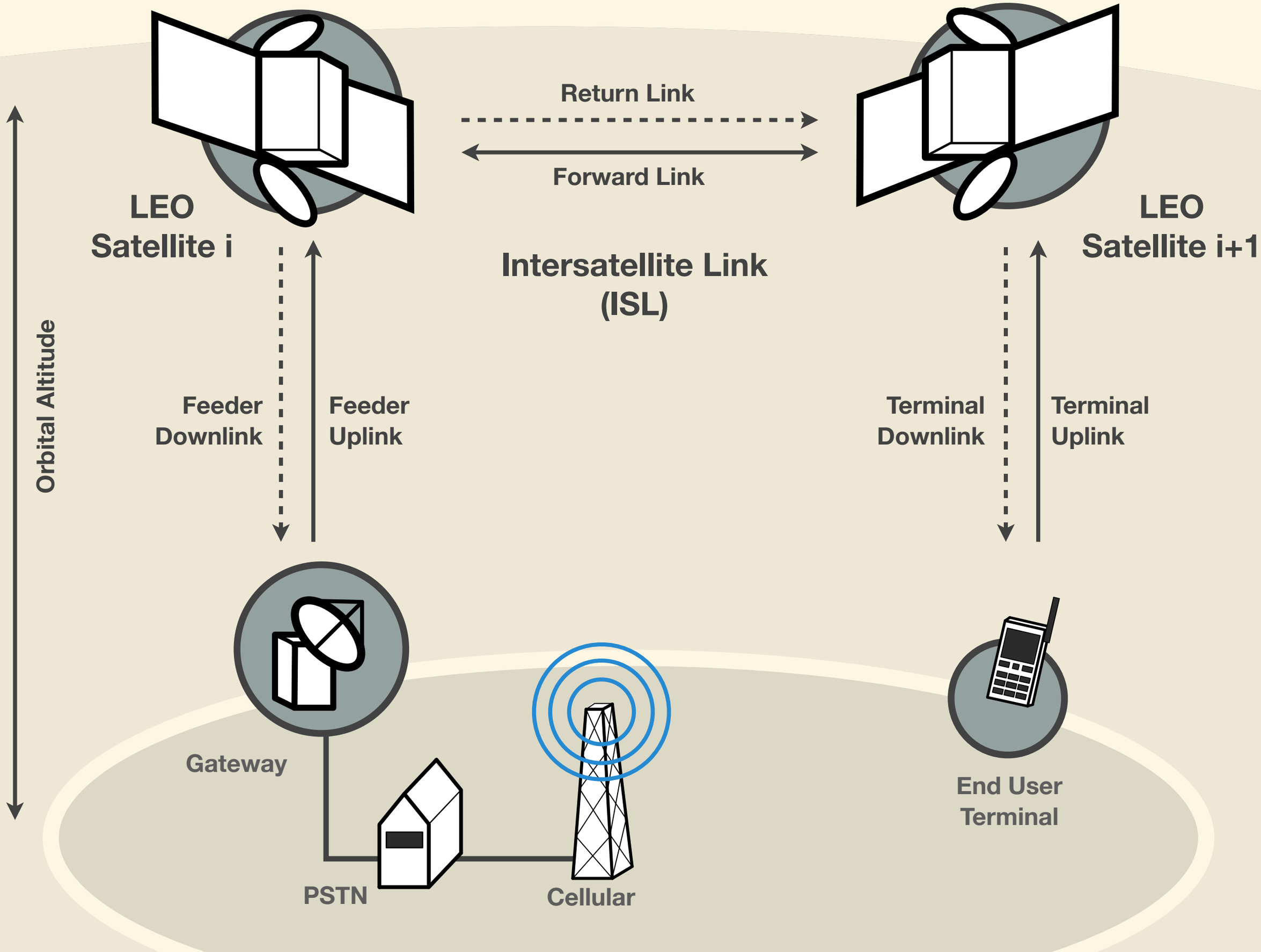
GEO (Geostationary Earth Orbit) Satellite Operators

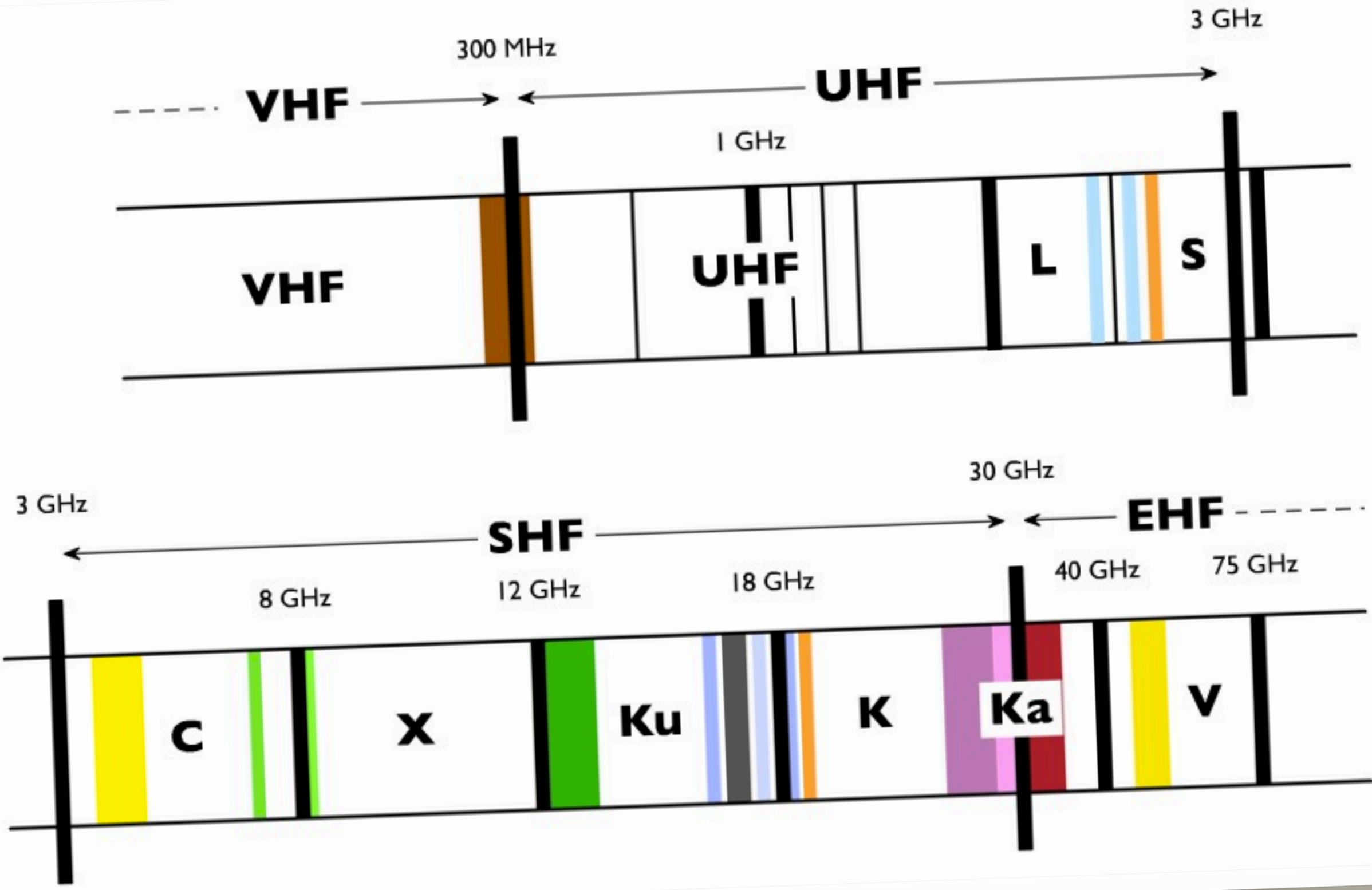
ACeS, ICO, Inmarsat, SkyTerra, TerreStar, Thuraya

LEO (Low Earth Orbit) Satellite Operators

Globalstar, Iridium

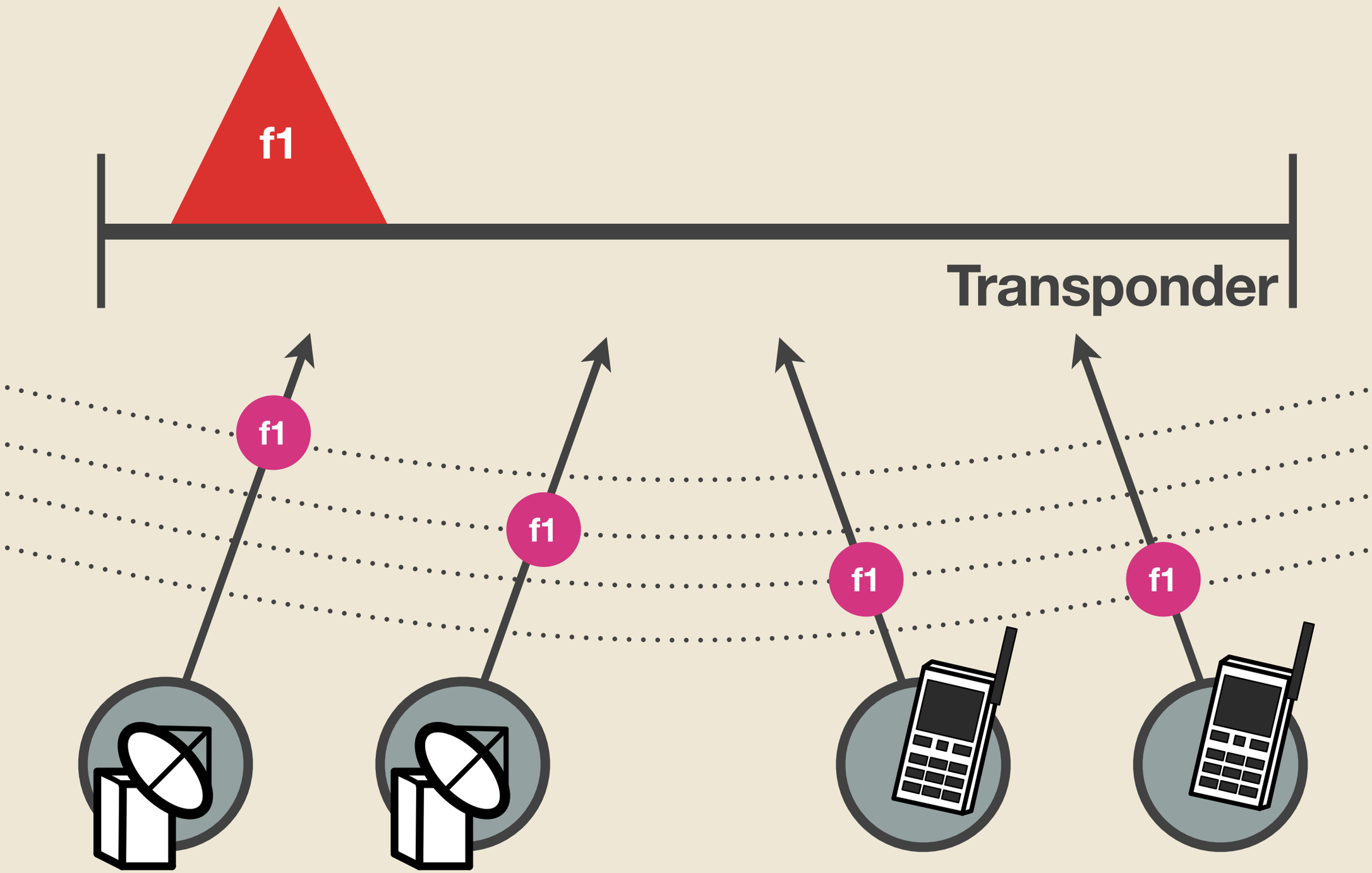
LEO Communication Satellite Constellation System



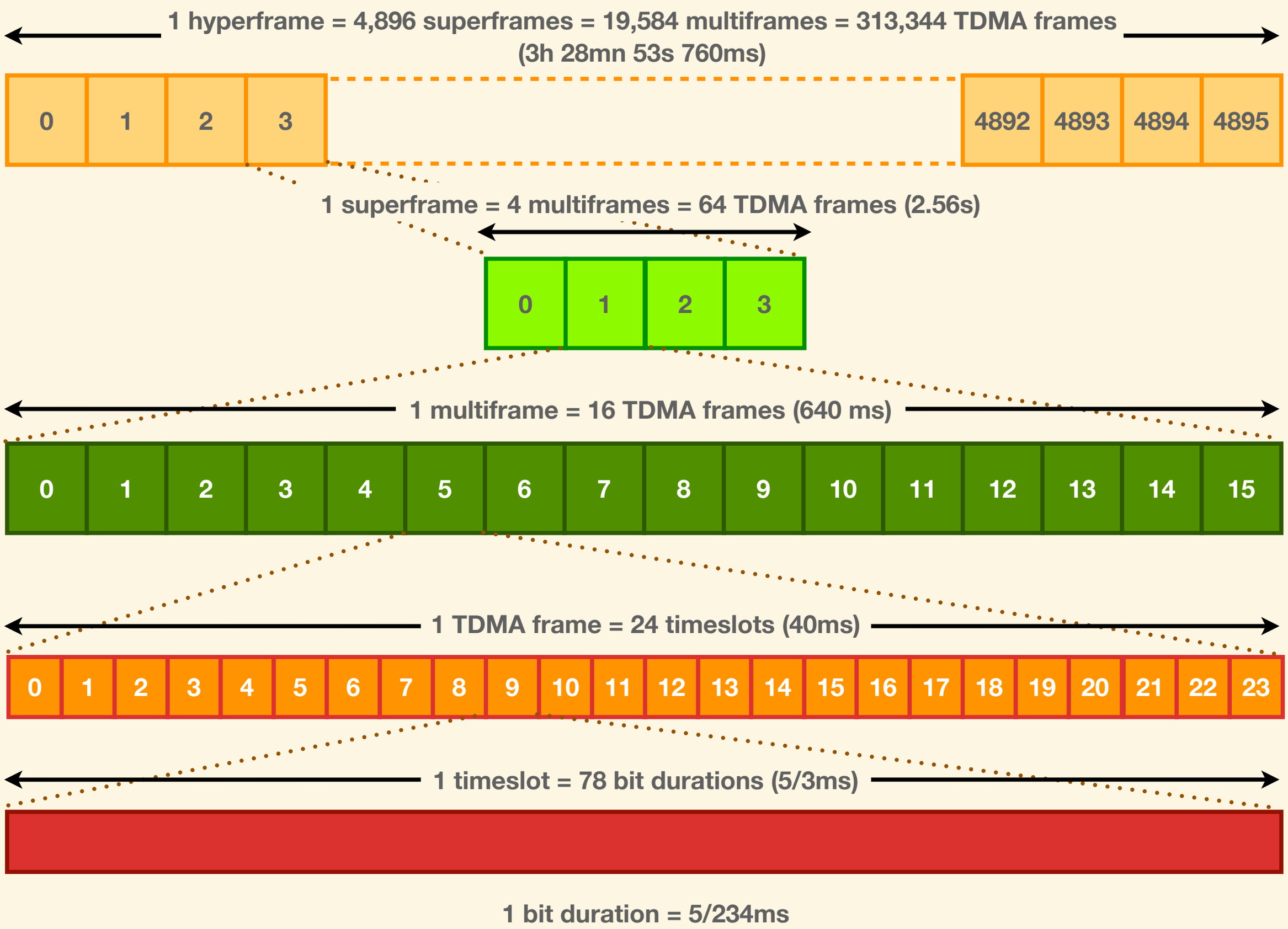


Frequency Band Designations

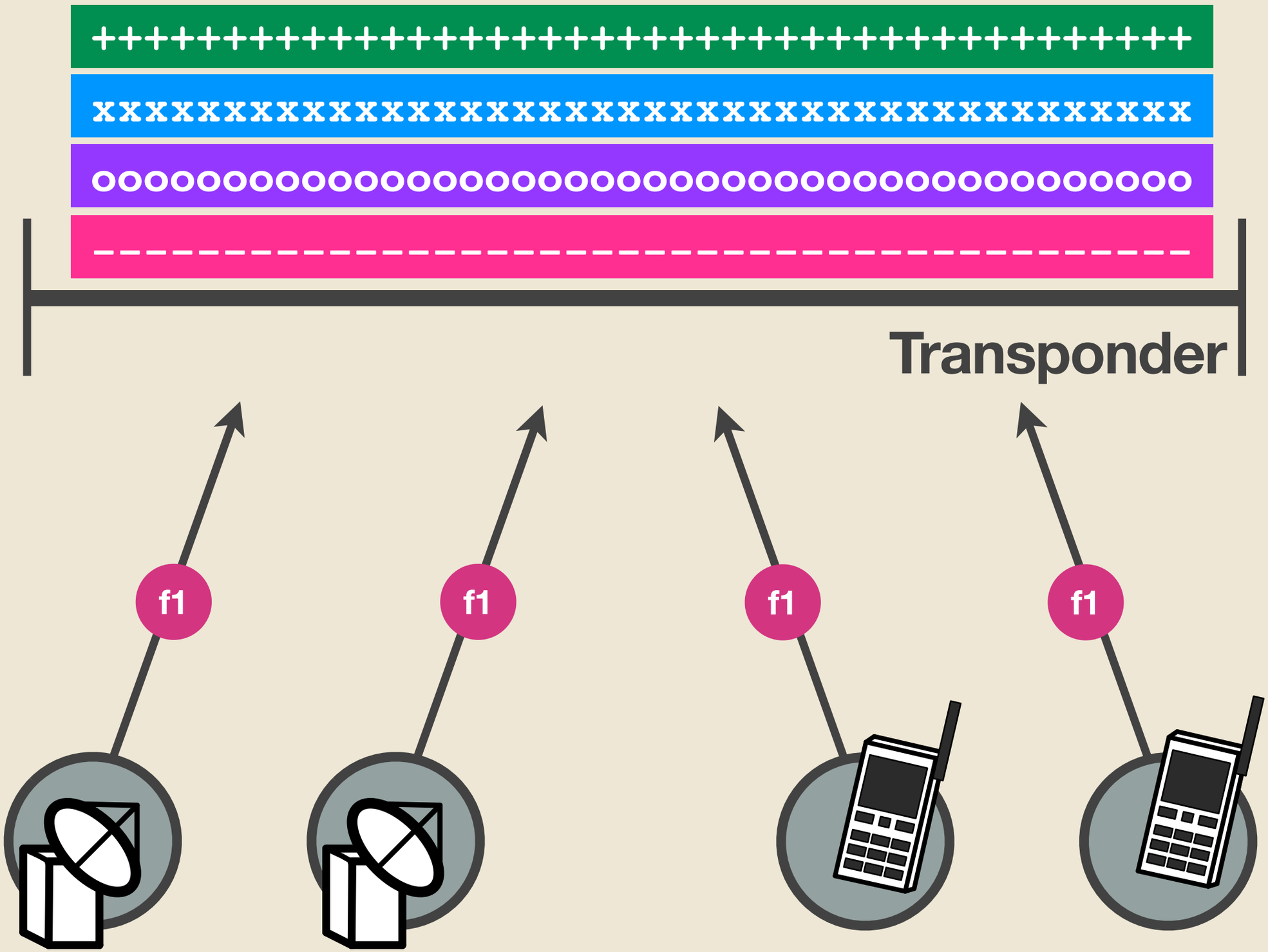
TDMA (Time Division Multiple Access)



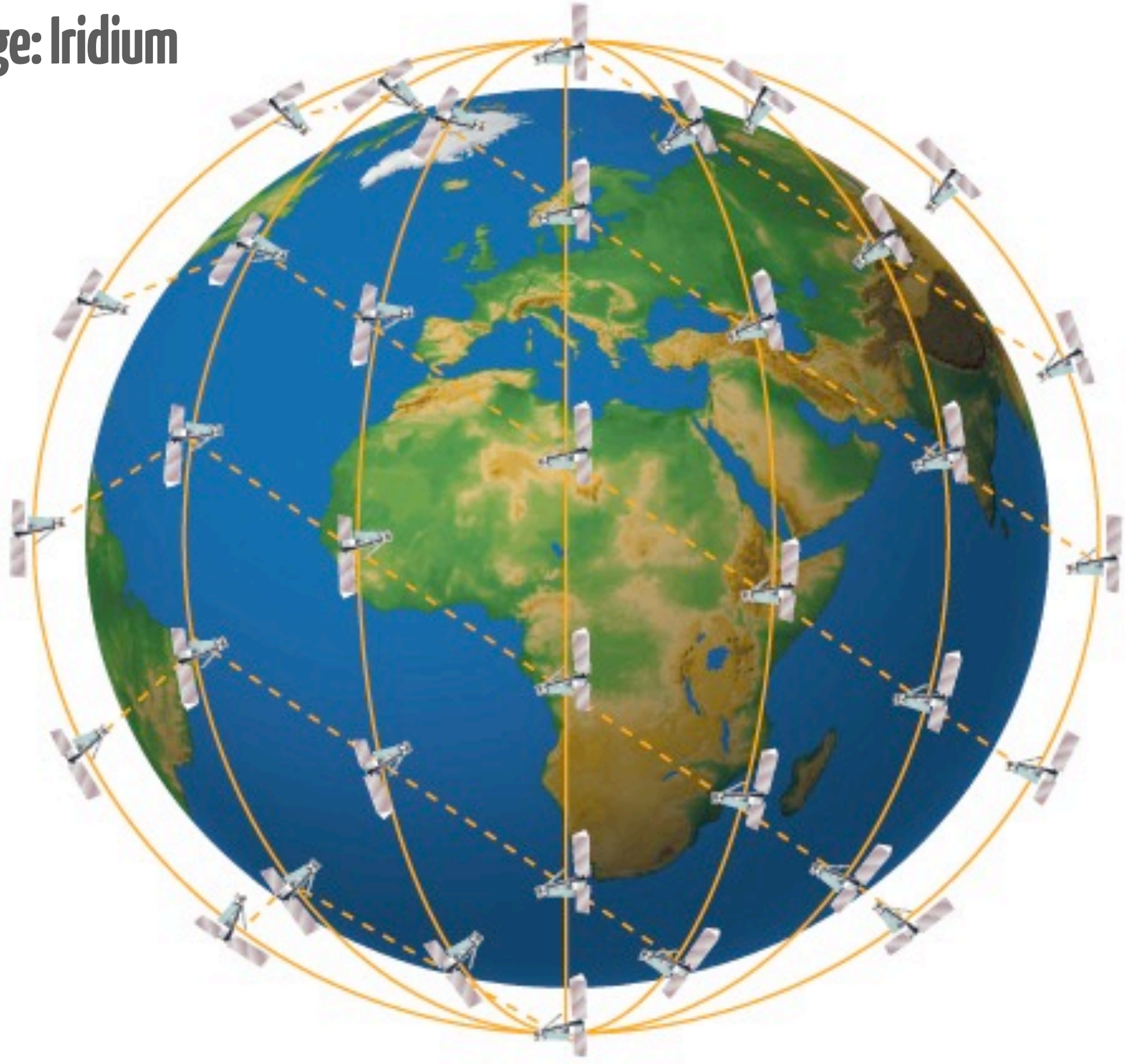
Timeframe Structure and Timeslots



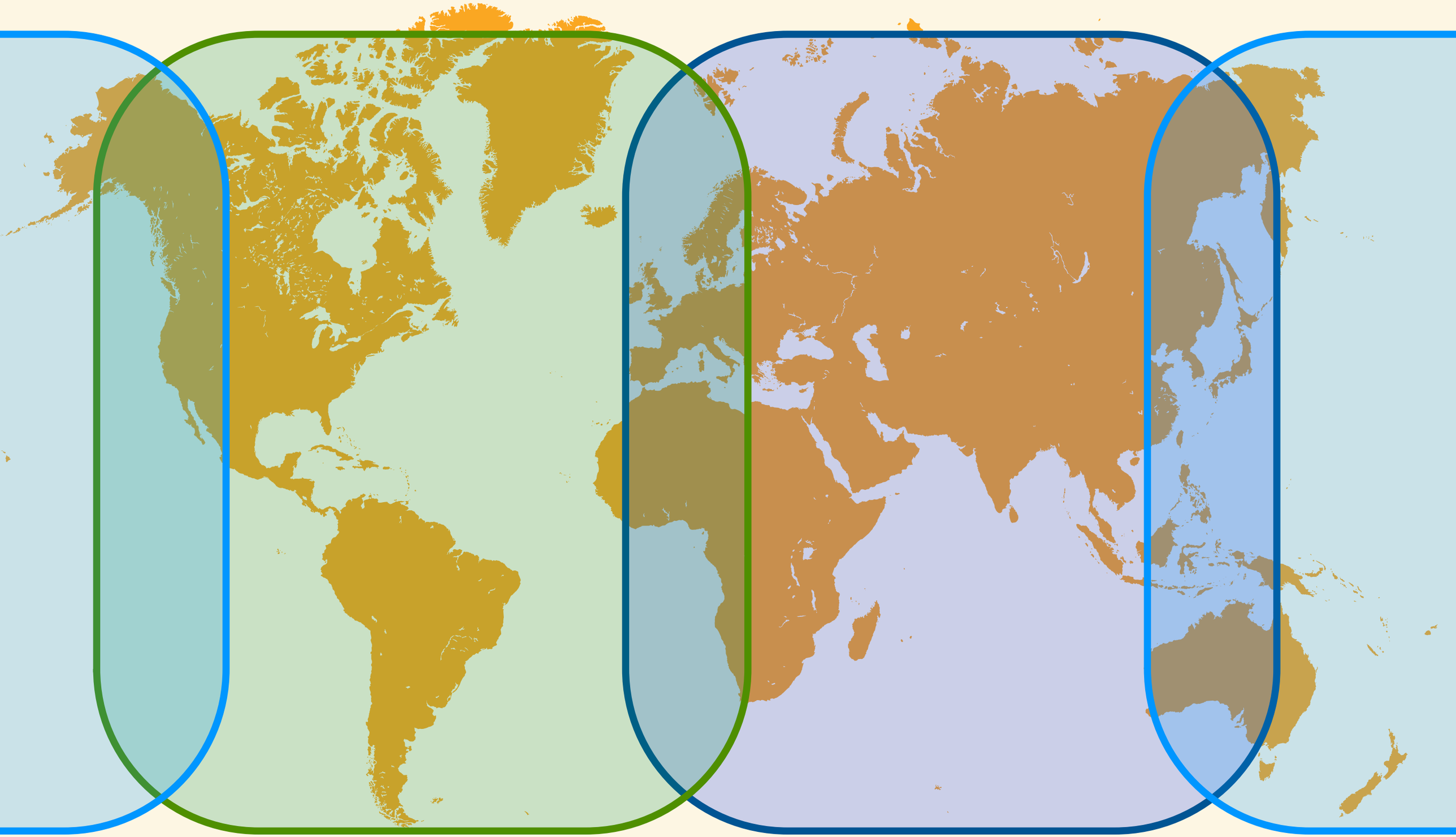
CDMA (Code Division Multiple Access)



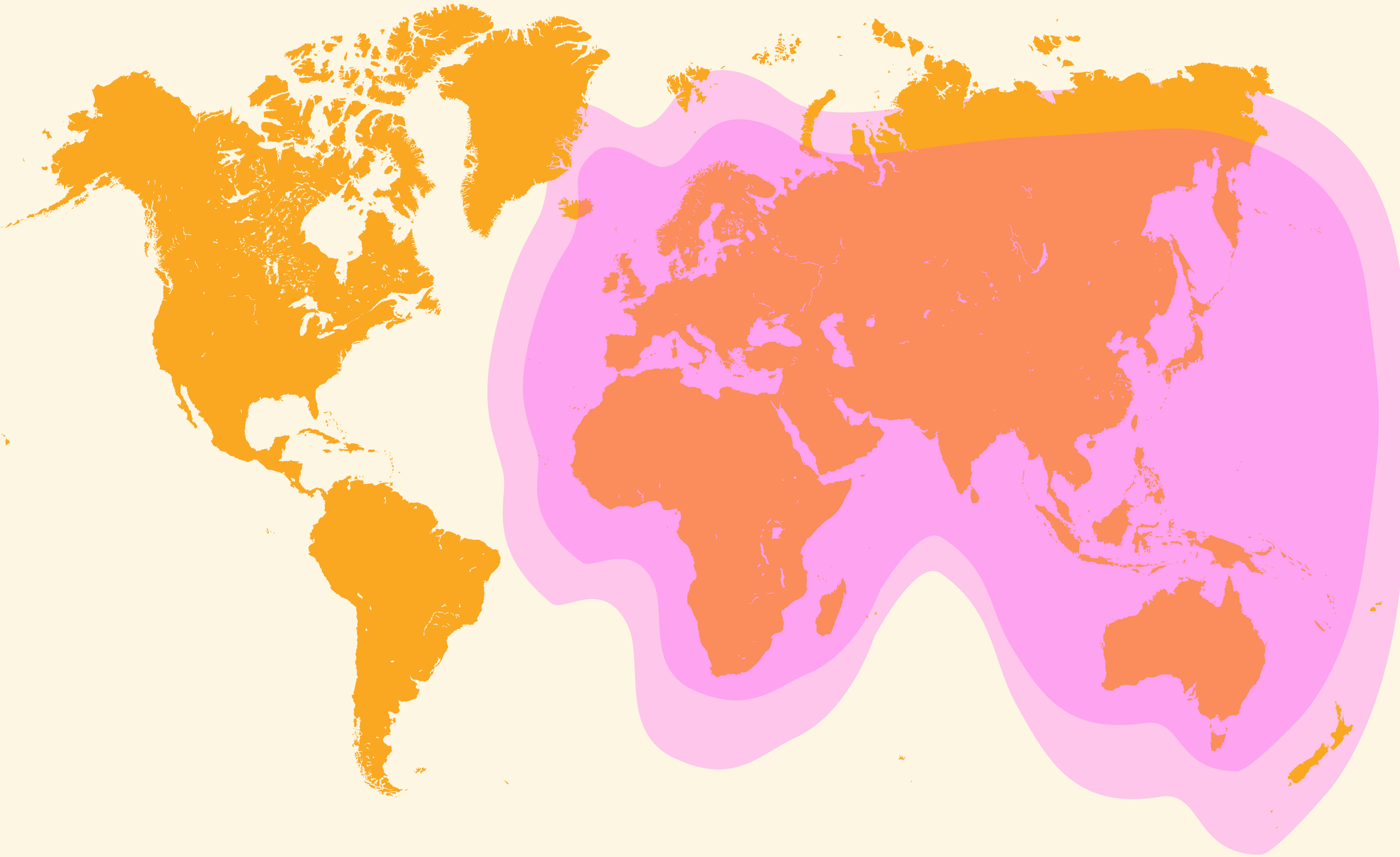
Coverage: Iridium



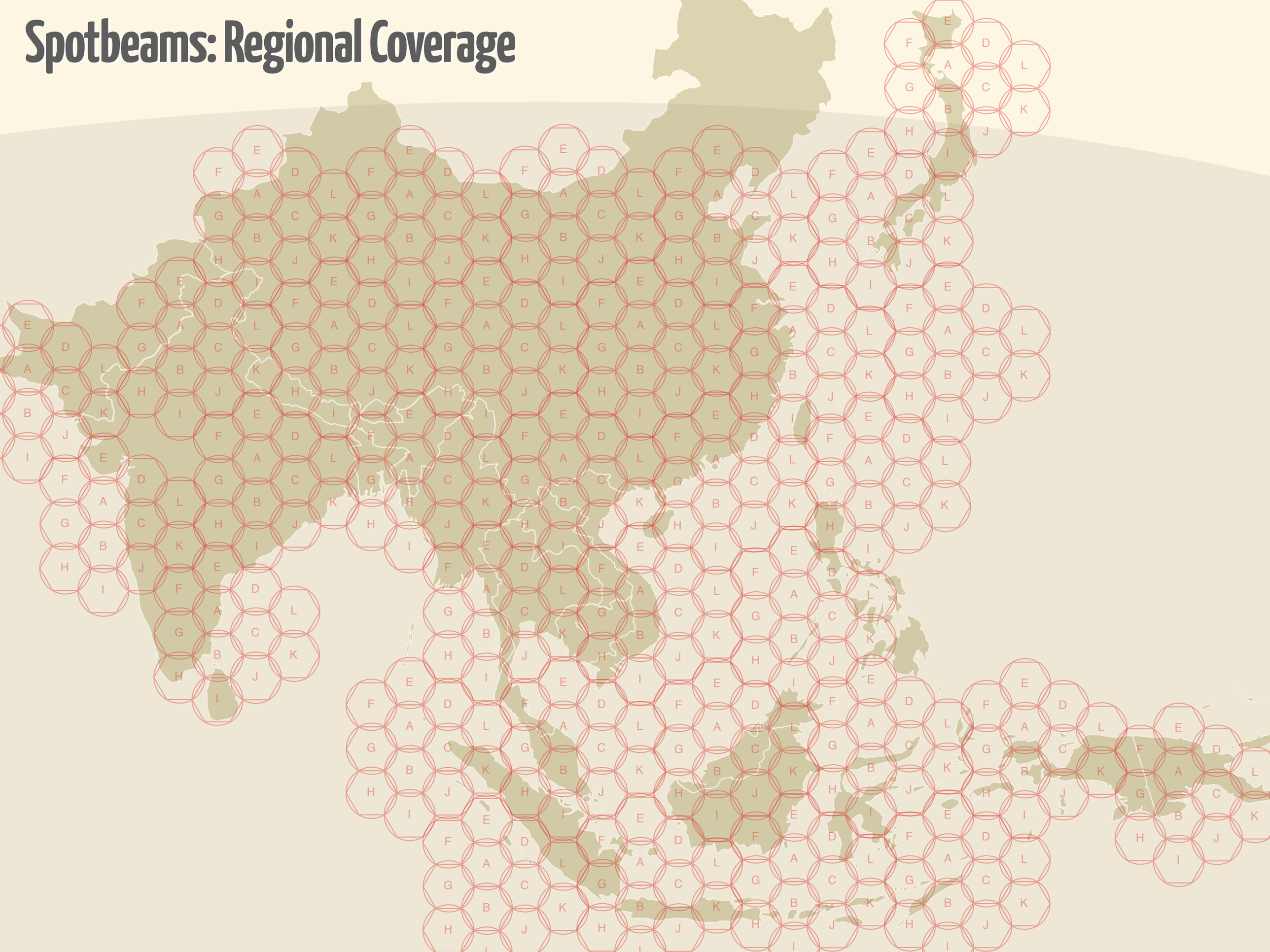
Coverage: Inmarsat



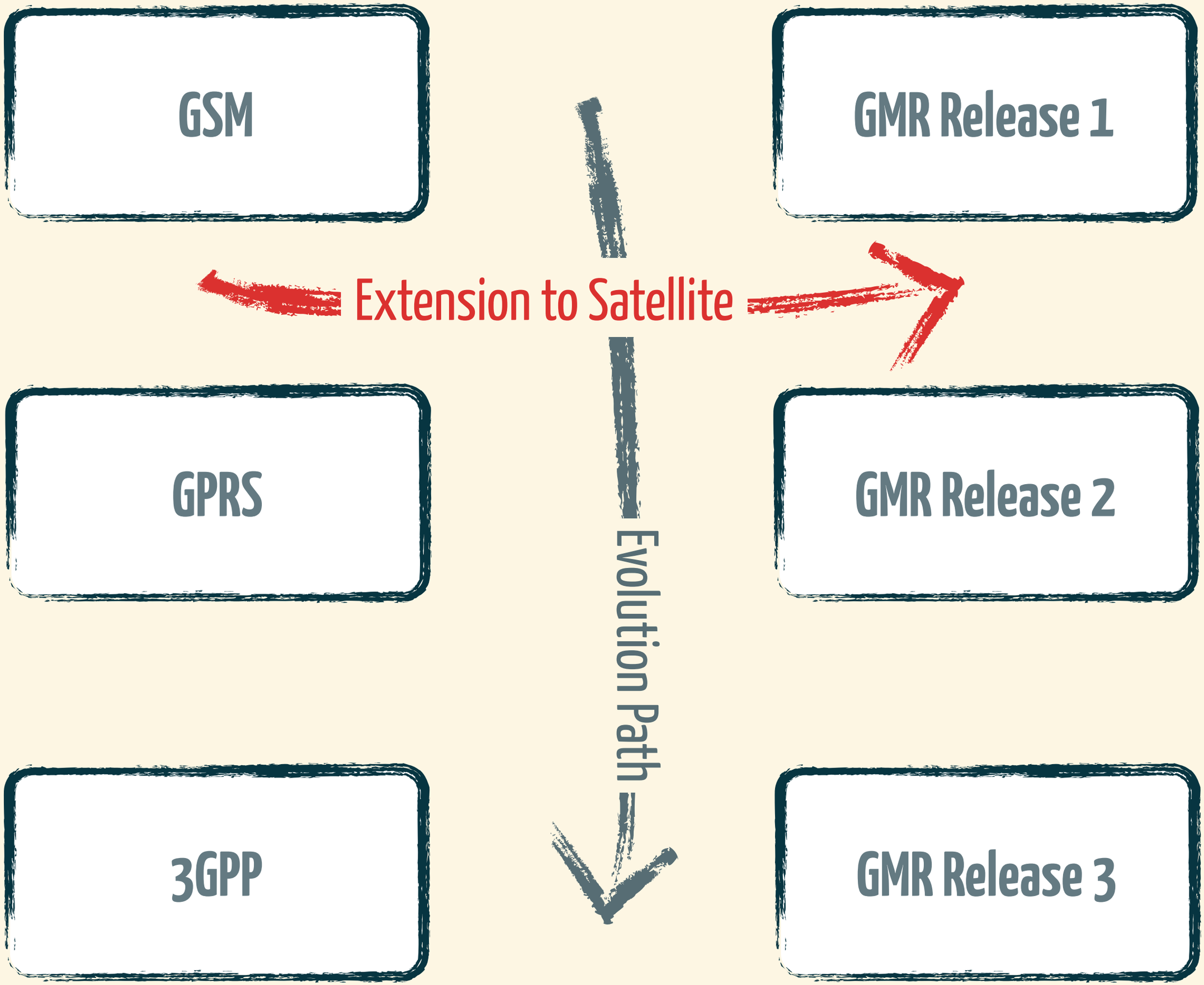
Coverage: Thuraya



Spotbeams: Regional Coverage

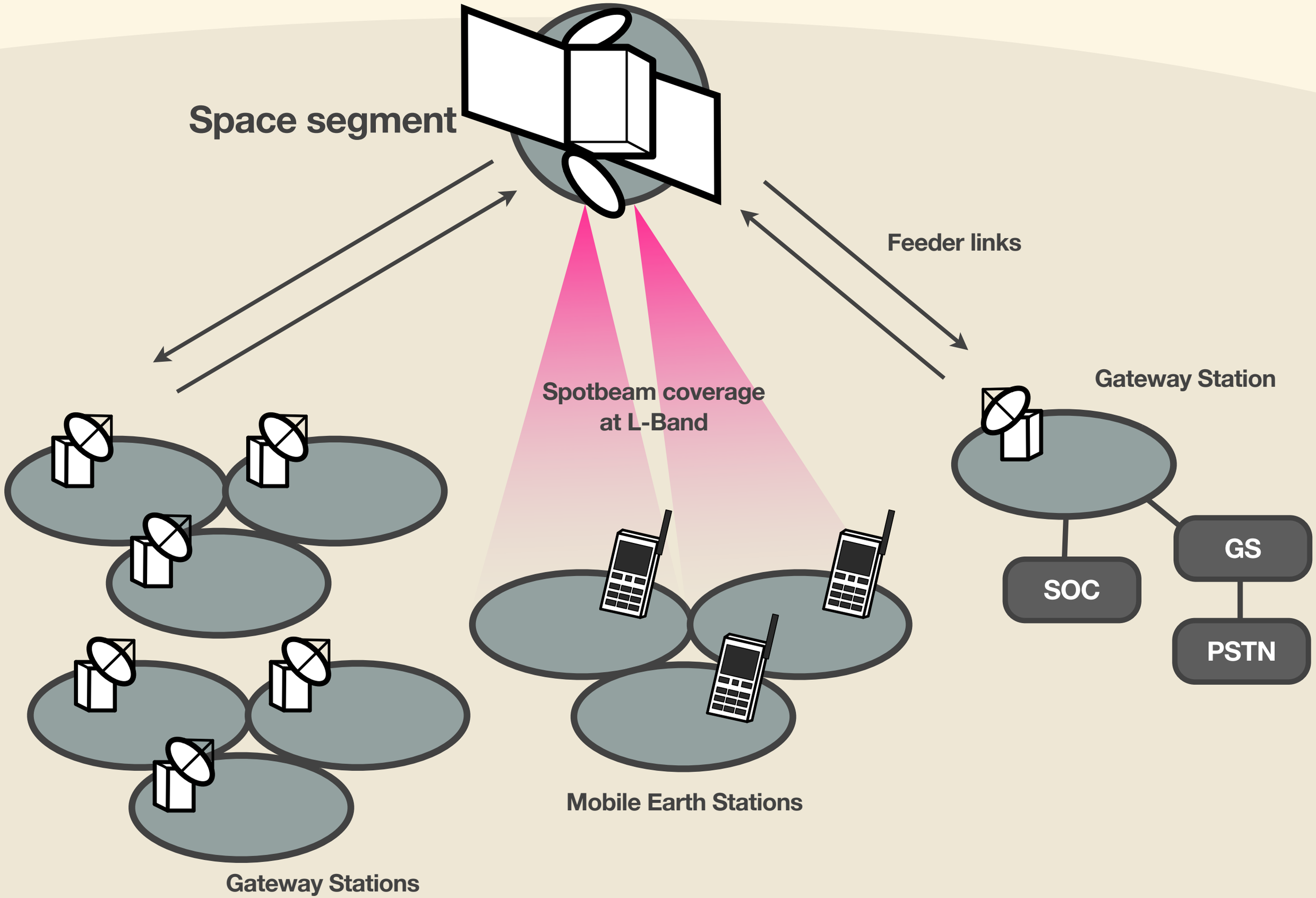


GMR (GEO-Mobile Radio Interface)

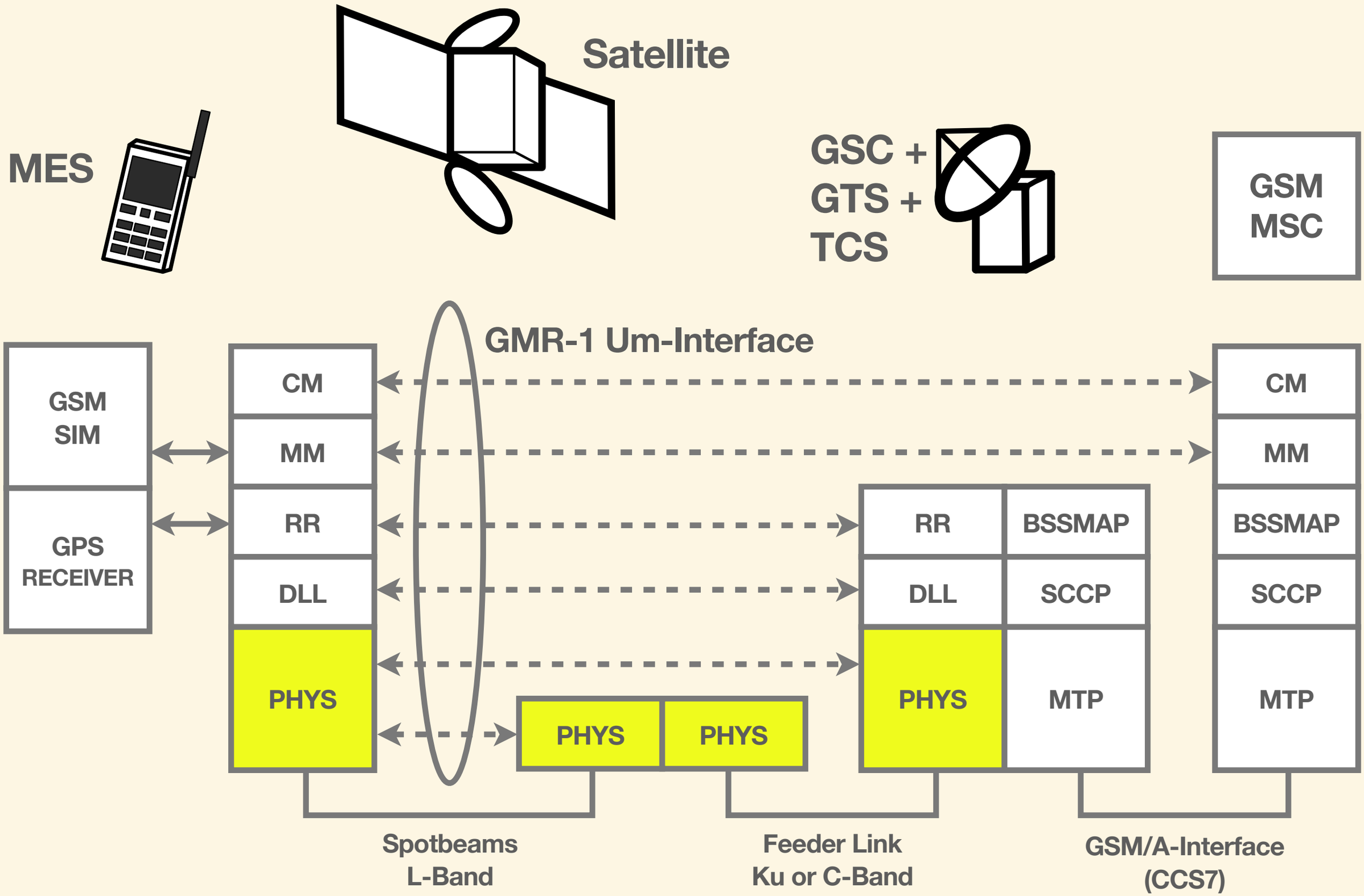

GSM
GMR Release 1
Extension to Satellite
GPRS
GMR Release 2
Evolution Path
3GPP
GMR Release 3

GMR-1

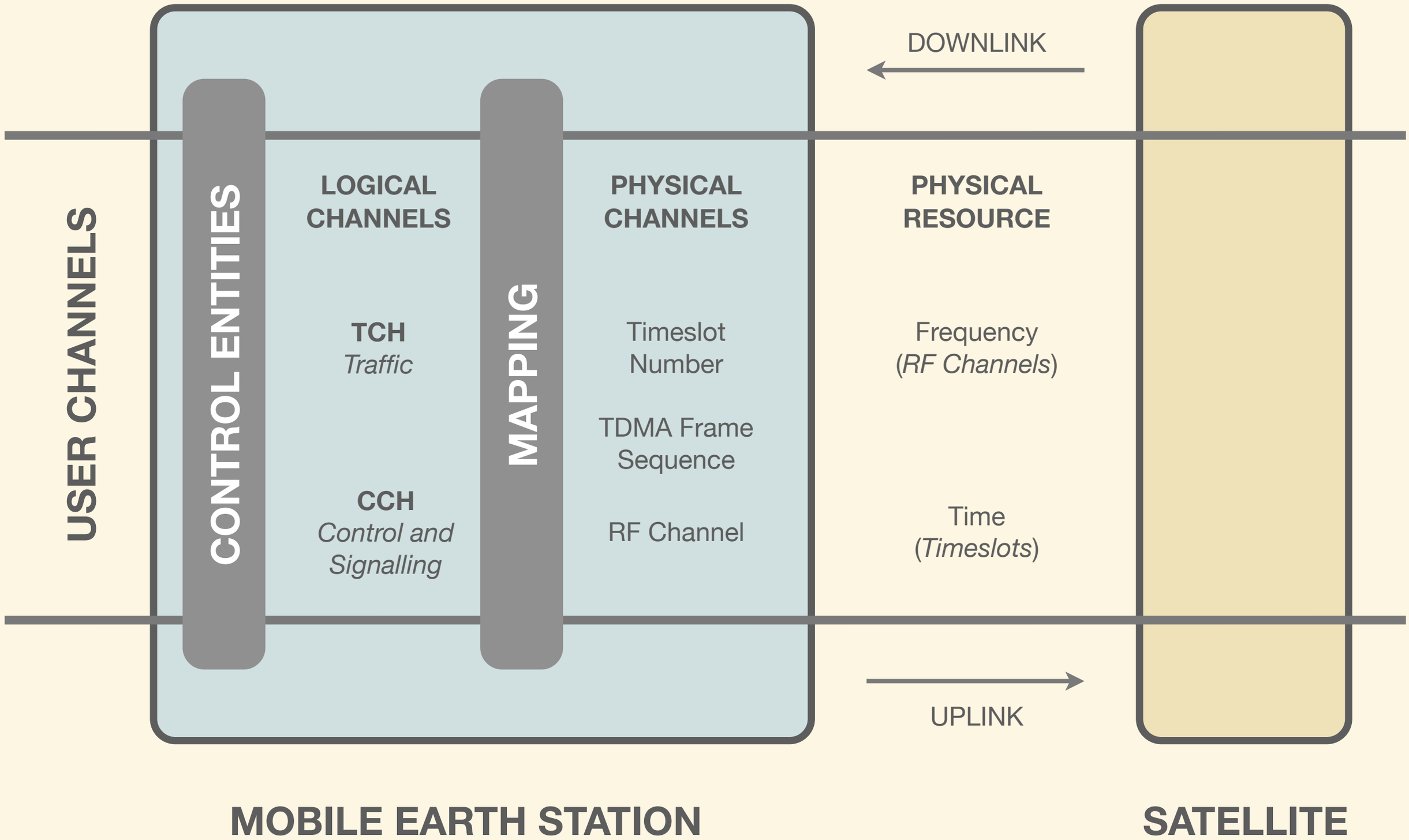
GMR-1 System Elements



GMR-1 Protocol Architecture



GMR-1 Logical Channel Mapping onto Physical Channel



GMR-1 (GSM-based) Services

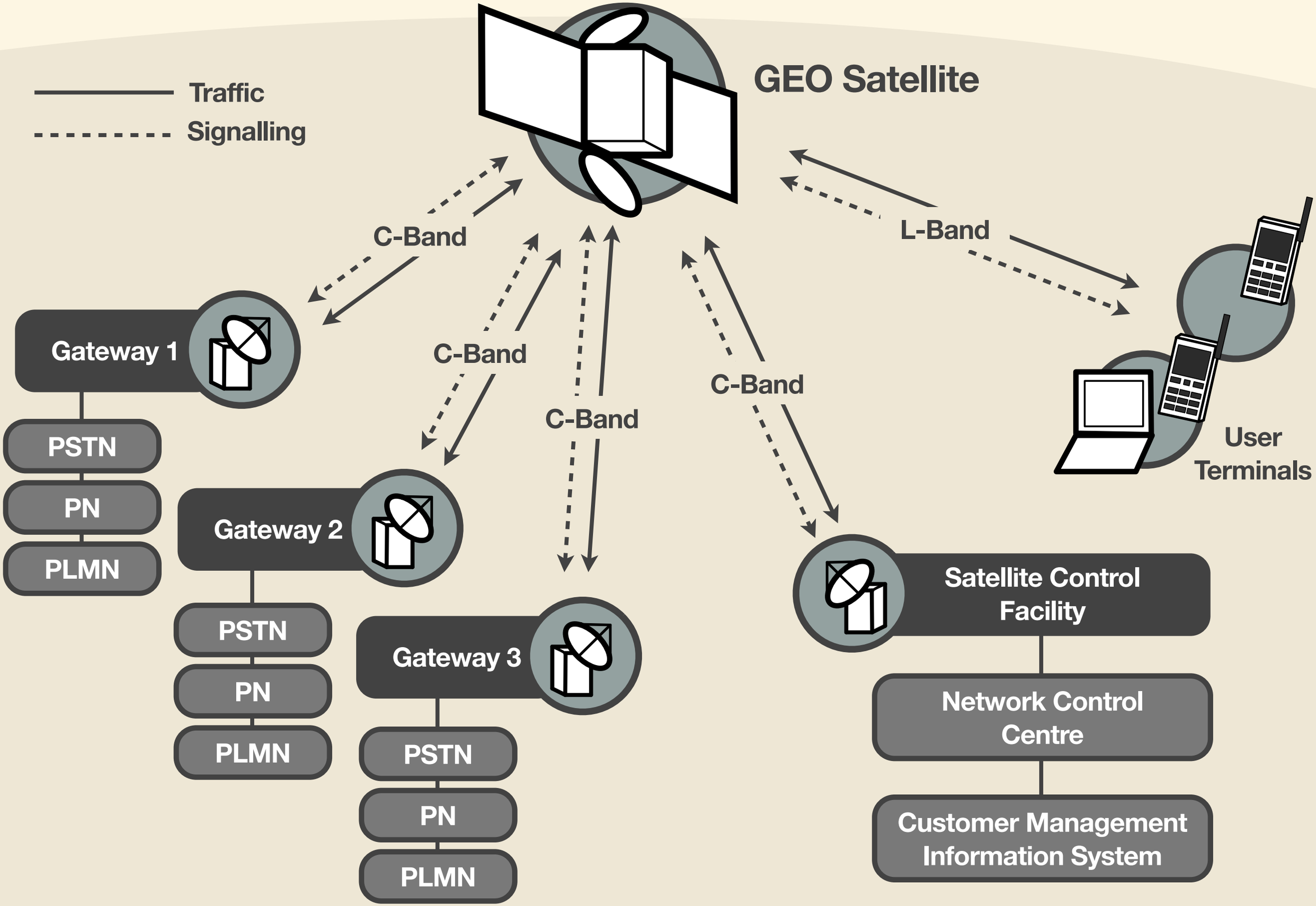
- Standard GSM-based services (Phase 2)
- Roaming
- Single number routing
- Numbers and addressing
- Authentication and privacy

GMR-1 Extended Services

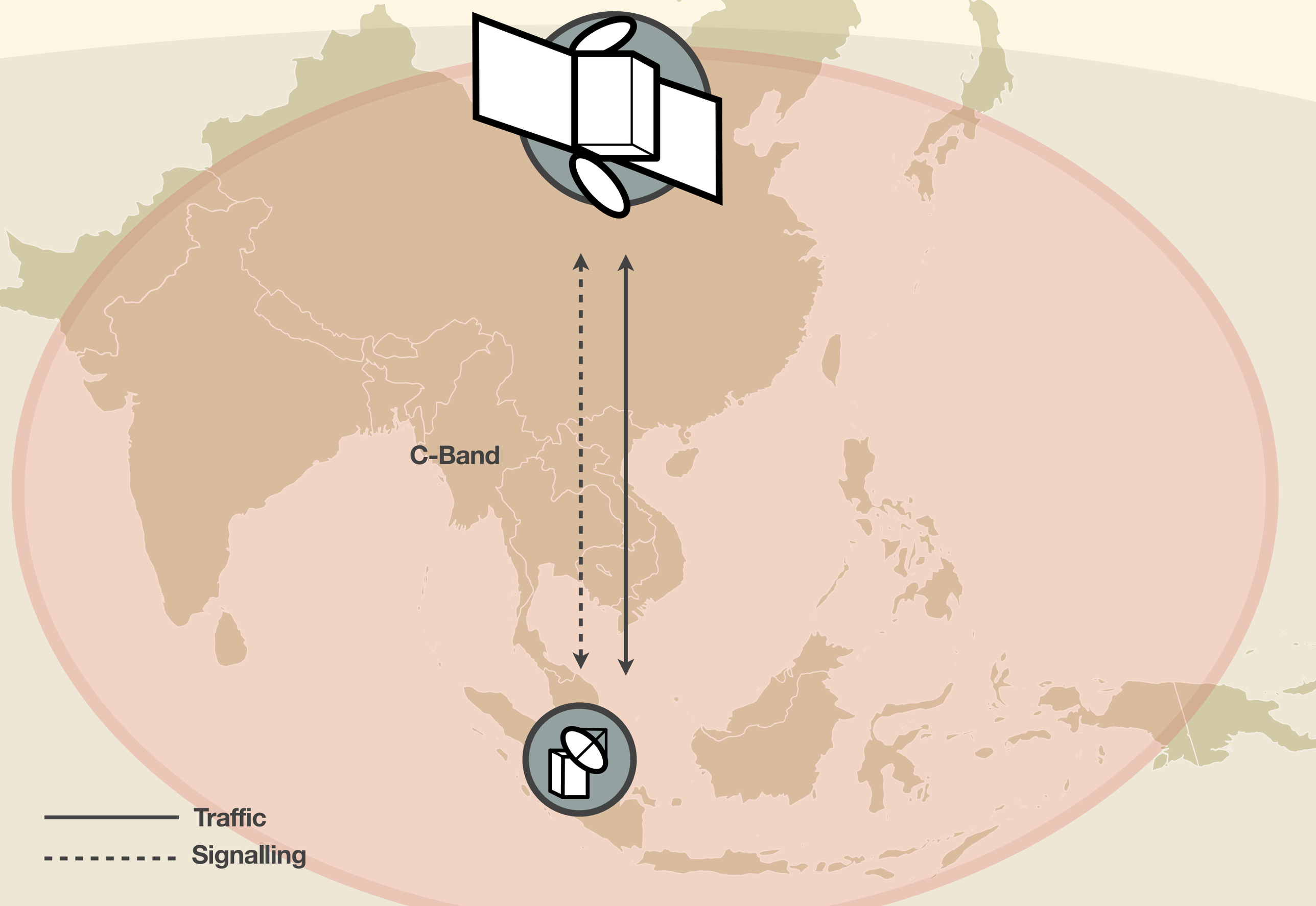
- Single-hopped terminal-to-terminal calls
- Optimal routing
- High penetration alerting
- Position based services

GMR-2

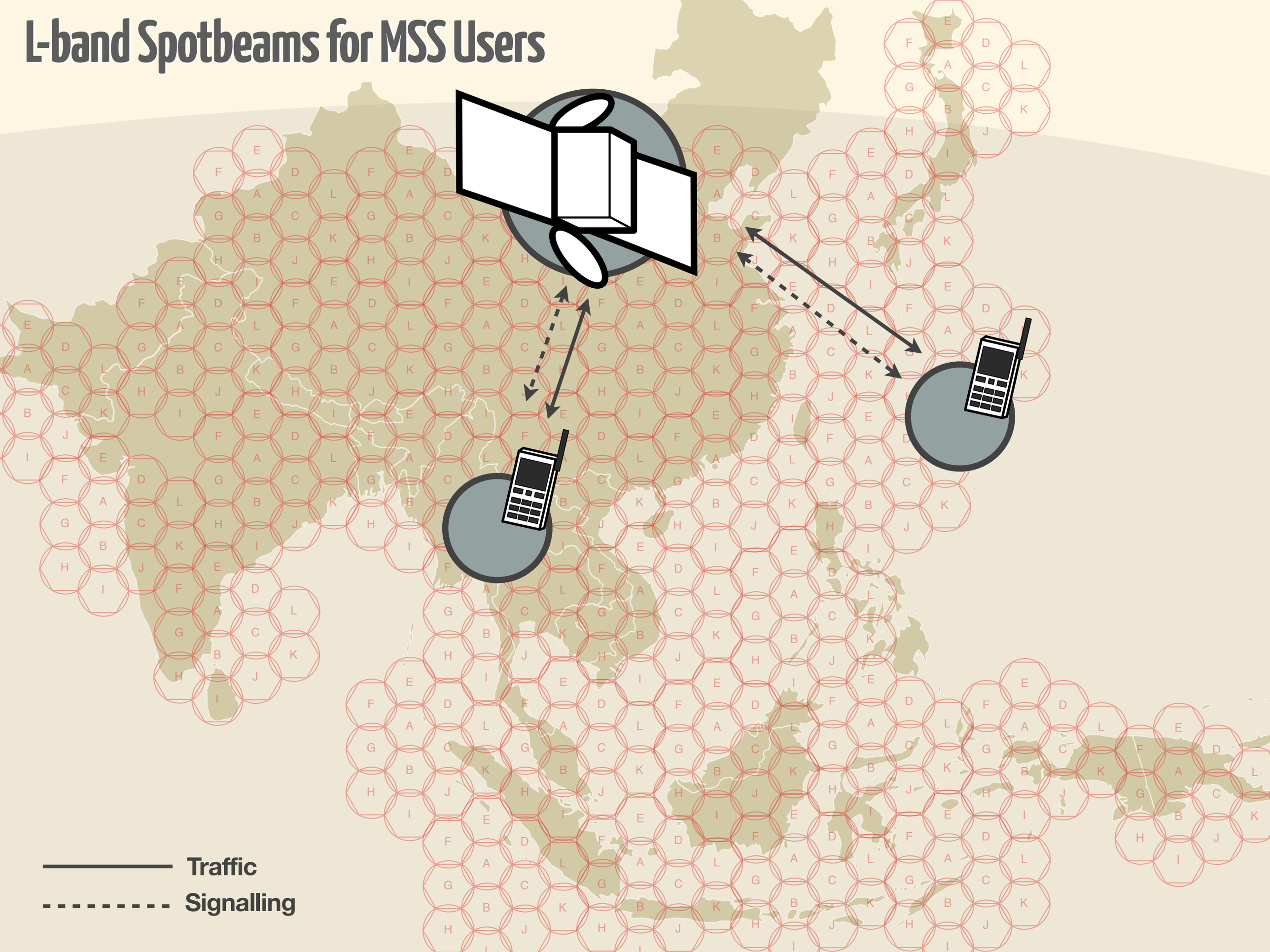
GMR-2 System Elements



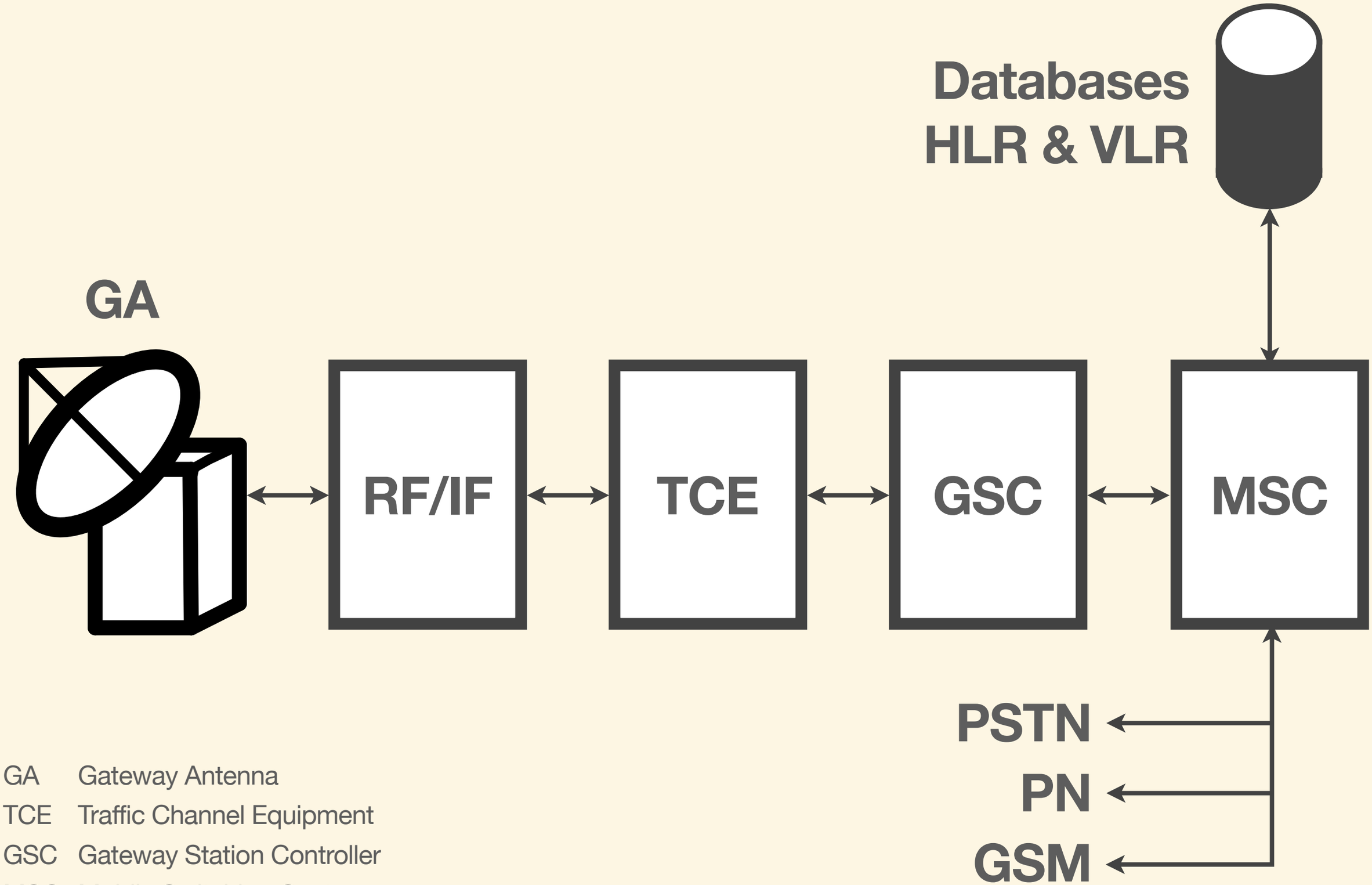
C-band Regional Coverage for Signalling & Communication



L-band Spotbeams for MSS Users



GMR-2 Gateway Internal Structure



GA Gateway Antenna
TCE Traffic Channel Equipment
GSC Gateway Station Controller
MSC Mobile Switching Center

GMR Satellite ~~Monitoring~~ System

Intercepting

Satellite Phone Interception

- Law-enforcements require tapping
- Test equipment
- Limited use of encryption
- Modifiable phone equipment

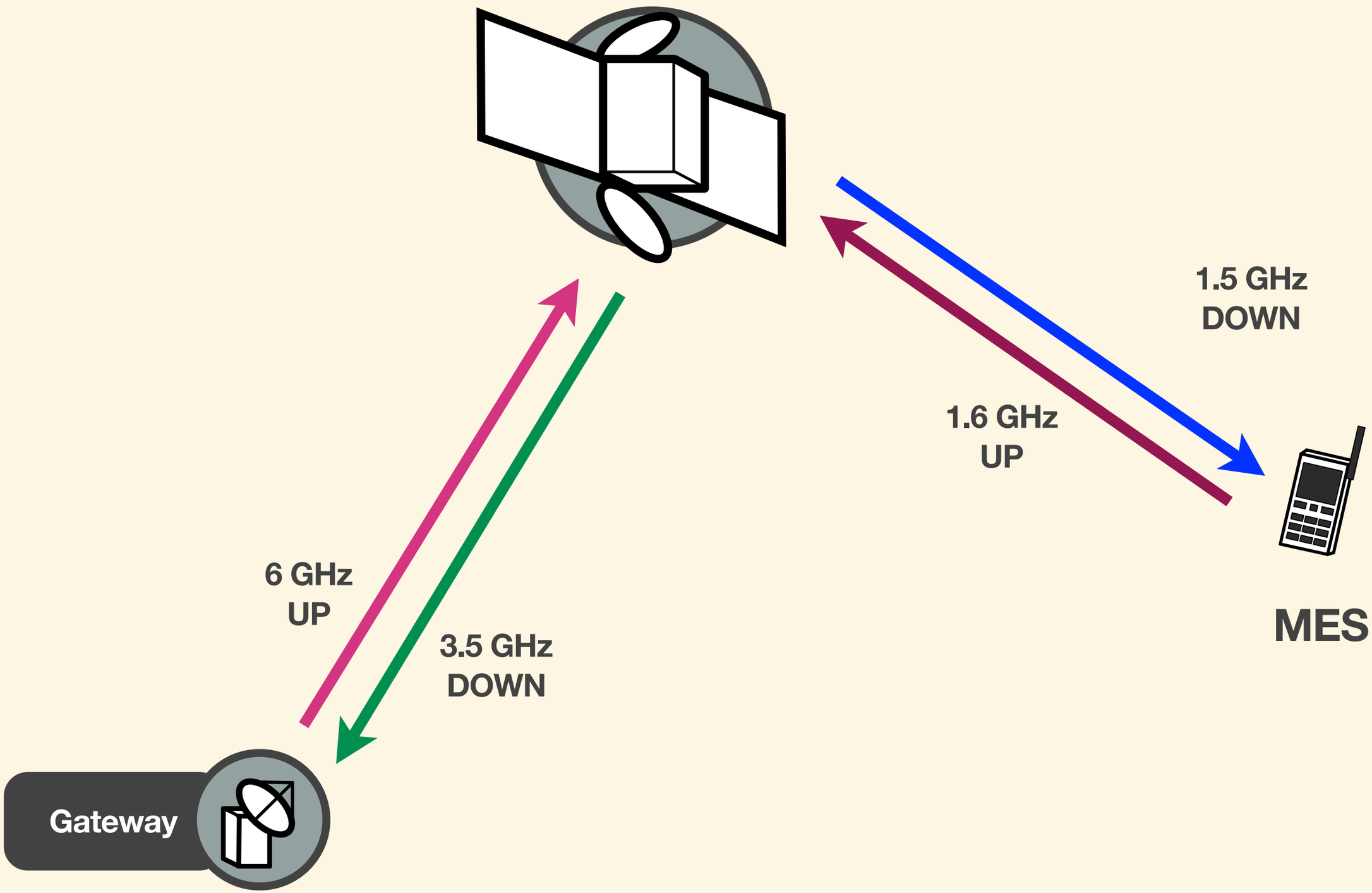
Tactical Interception

Receives L-band from satellite and line-of-sight from handset

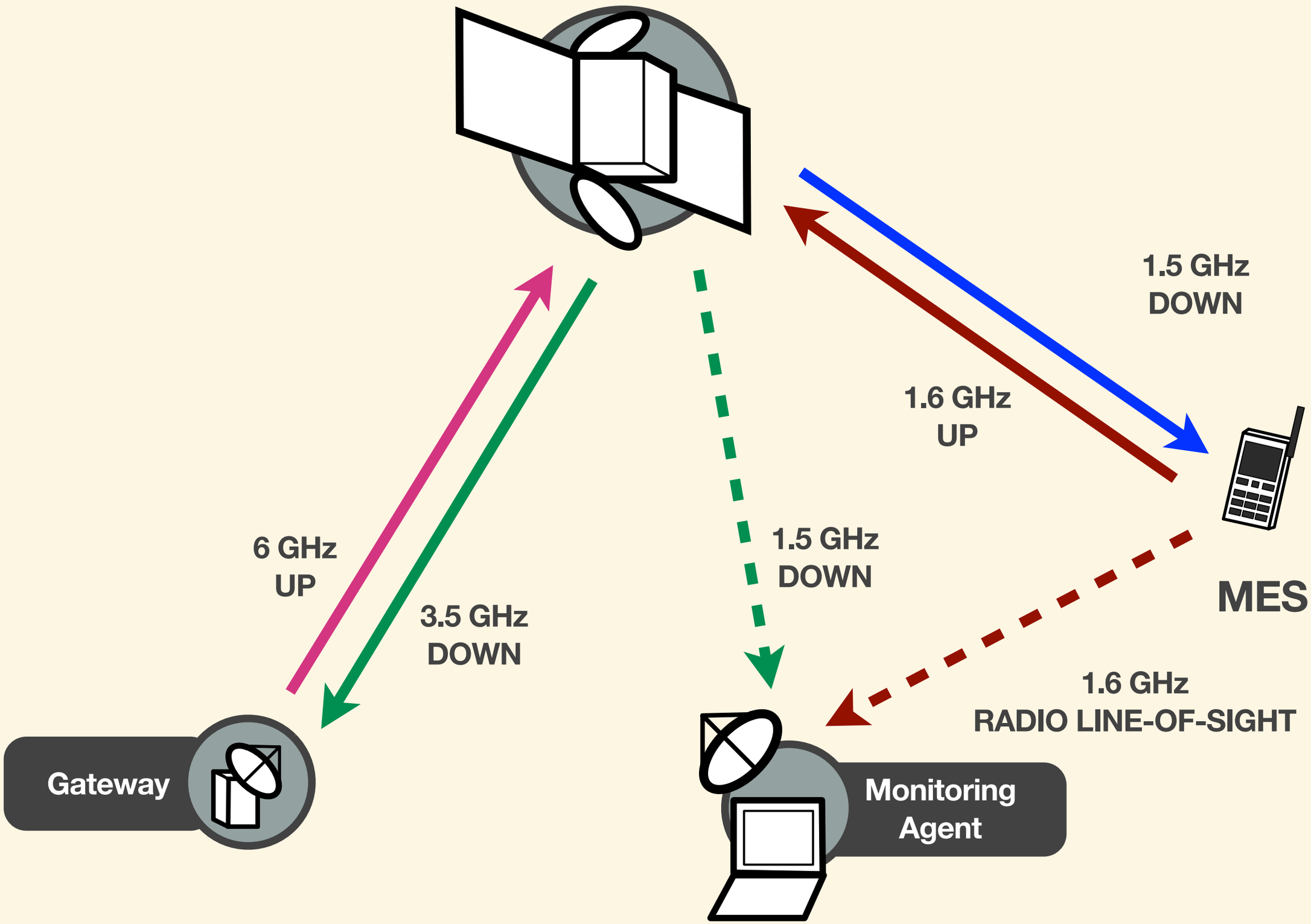
Strategic Interception

Receives L-band from satellite and C-band from satellite

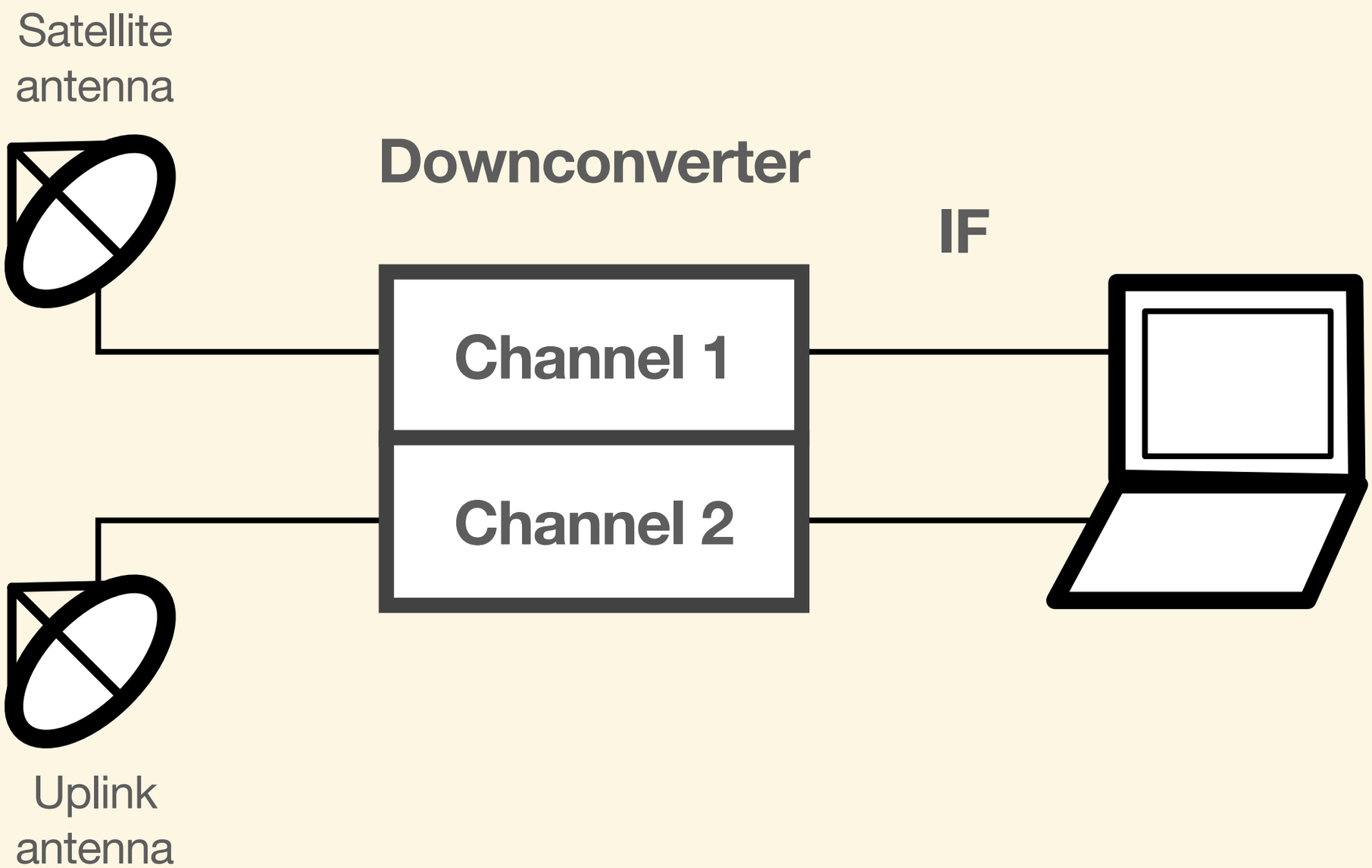
Satellite Interception Operation



Tactical Satellite Interception Operation



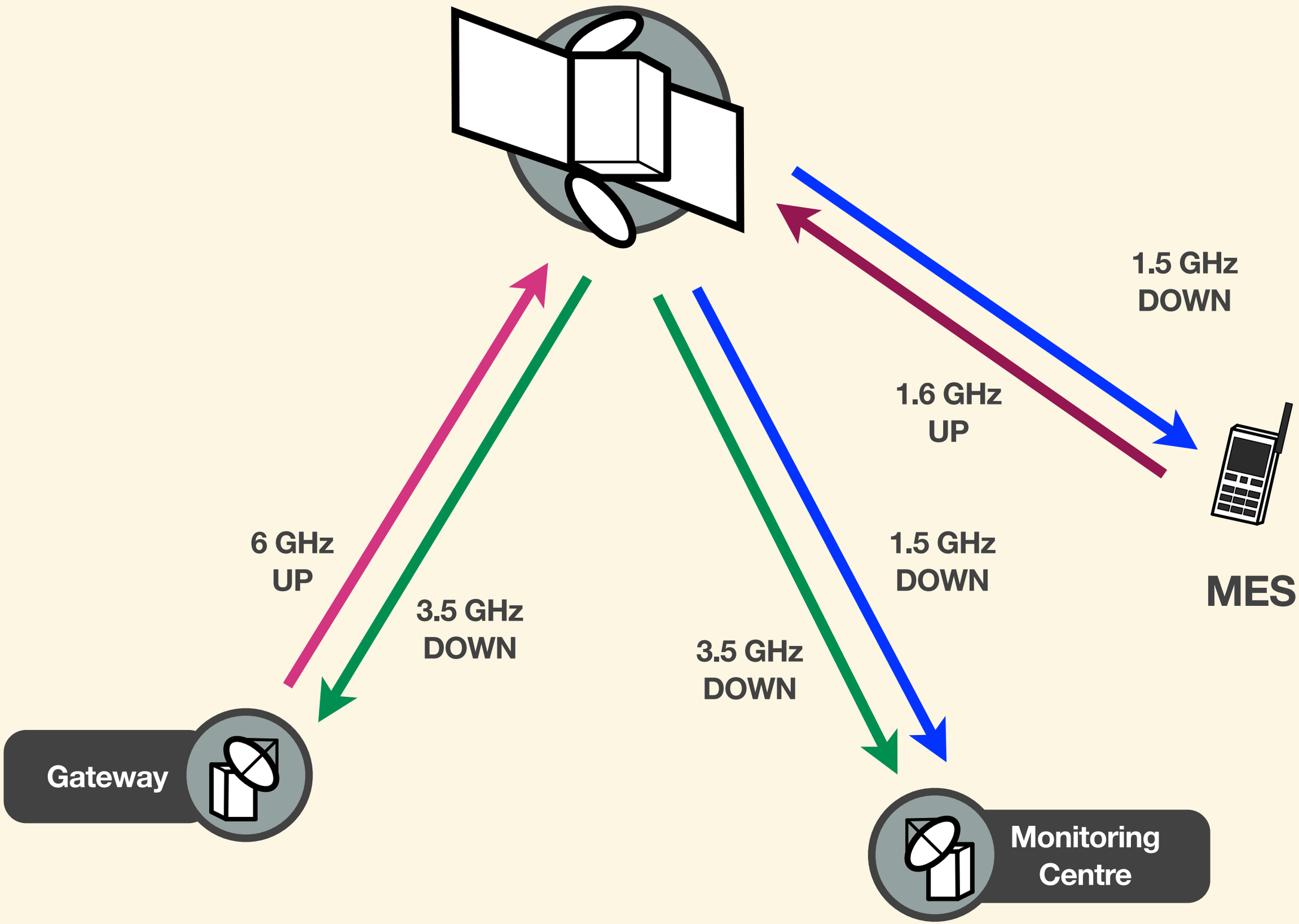
Tactical Satellite Interception Operation



Call Analysis

- Spotbeam IDs, GPS co-ordinates, operating frequency.
- Date, time and duration of call.
- MES IMSI.
- GPS co-ordinates of MES.
- Random Reference Number (CallerID).
- TMSI called by MES.
- Mobile or Fixed Originated Call (Voice, Fax, Data or SMS).
- Terminal type.
- Ciphering key sequence number.
- RAND and SRES.
- Encryption Algorithm

Strategic Satellite Interception Operation



FAQ

What’s next?

OsmocomGMR

GEO Mobile Radio

This is the homepage of the Osmocom sub-project *GEO Mobile Radio*.

It is collecting information and software related to the ETSI GEO Mobile Radio specification and its practical implementations like the Thuraya satellite phone network

GEO Mobile Radio is a set of specifications describing a satellite based mobile phone network.

Radio aspects

It uses the L-band frequencies 1634 to 1656 MHz (earth to space) and 1532.5 to 1554.5 MHz (space to earth) for communication between mobile phones and the respective satellites. The polarization is circular (left) and the modulation is pi/4 QPSK, using a channel spacing of 31.25 kHz

Index

- GMR_Specifications -- An Introduction and Overview into the GMR specifications
- Thuraya_SO2510 -- A popular handset for use in the Thuraya system.
- Thuraya_SG2520 -- A dual-mode GSM/ Thuraya handset running WindowsCE.
- Thuraya_Beams -- Information about the Thuraya beams
  - http://bit.ly/nInTOi -- Google Maps view of the Thuraya beams that we have found so far
- OsmoGMR_Software -- Software that we wrote for GMR analysis
- Receiver_Setup -- How to receive GMR signals coming down from a satellite

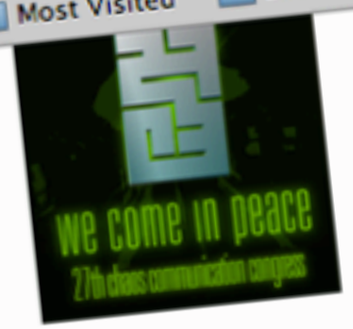
Download in other formats:
Plain Text

27C3: Wideband GSM Sniffin

events.ccc.de/congress/2010/Fahrplan/events/4208.en.html

Most Visited | Socials | Tools

27C3 – Version 1.6.3



Index
Day 1 – 2010-12-27
Day 2 – 2010-12-28
Day 3 – 2010-12-29
Day 4 – 2010-12-30
Speakers
Events
Community
Culture
Hacking
Making
Science
Society

27th Chaos Communication Congress

We come in peace

Wideband GSM Sniffing

GSM is still the most widely used security technology in the world with a user base of 5 billion and a quickly growing number of critical applications. 26C3's rainbow table attack on GSM's A5/1 encryption convinced many users that GSM calls should be considered unprotected. The network operators, however, have not woken up to the threat yet. Perhaps the new capabilities to be unleashed this year – like wide-band sniffing and real-time signal processing – will wake them up.

Now that GSM A5/1 encryption can be cracked in seconds, the complexity of wireless phone snooping moved to signal processing. Since GSM hops over a multitude of channels, a large chunk of radio spectrum needs to be analyzed, for example with USRPs, and decoded before storage or decoding. We demonstrate how this high bandwidth task can be achieved with cheap programmable phones.

Attached files

- GSM Sniffing [Slides] (application/pdf – 755.6 KB)

SPEAKERS	
	Karsten Nohl
	Sylvain Munaut
SCHEDULE	
Day	Day 2 – 2010-12-28
Room	Saal 1
Start time	14:00
Duration	01:00
INFO	
ID	4208
Event type	Lecture
Track	Hacking
Language used for presentation	English

FEEDBACK

Did you attend this event? Give Feedback

<<< >>>

@geovedi

http://www.slideshare.net/geovedi/presentations