

Hacking a Bird in the Sky

Hijacking Very Small Aperture Terminal (VSAT) Connections

Jim Geovedi and Raditya Iryandi

BELLUA ASIA PACIFIC

Disclaimer

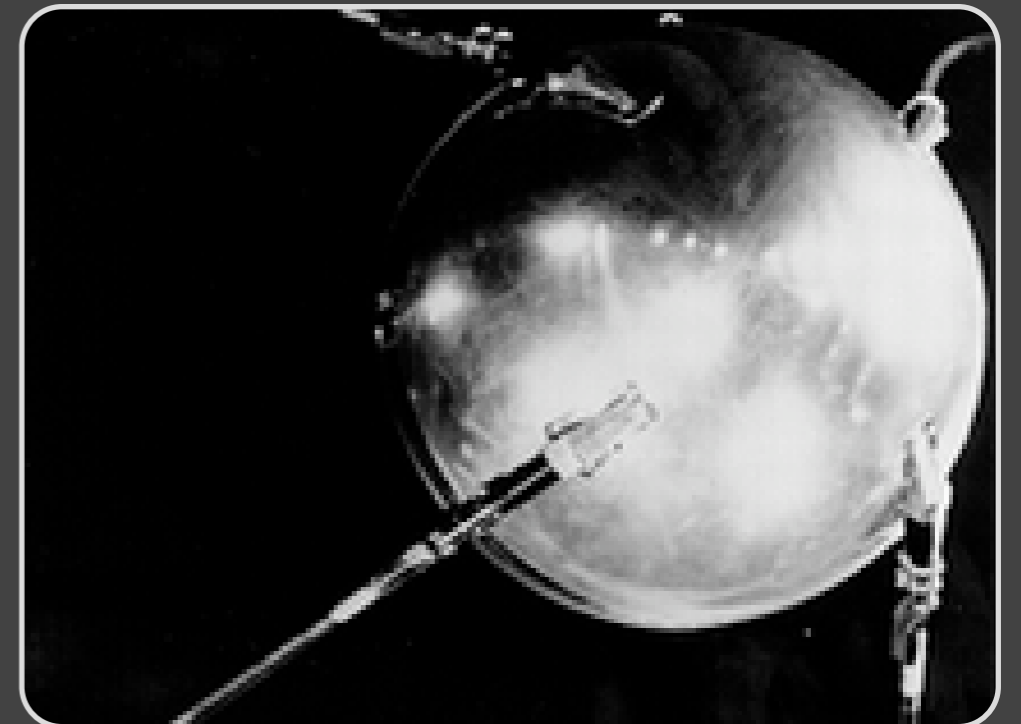
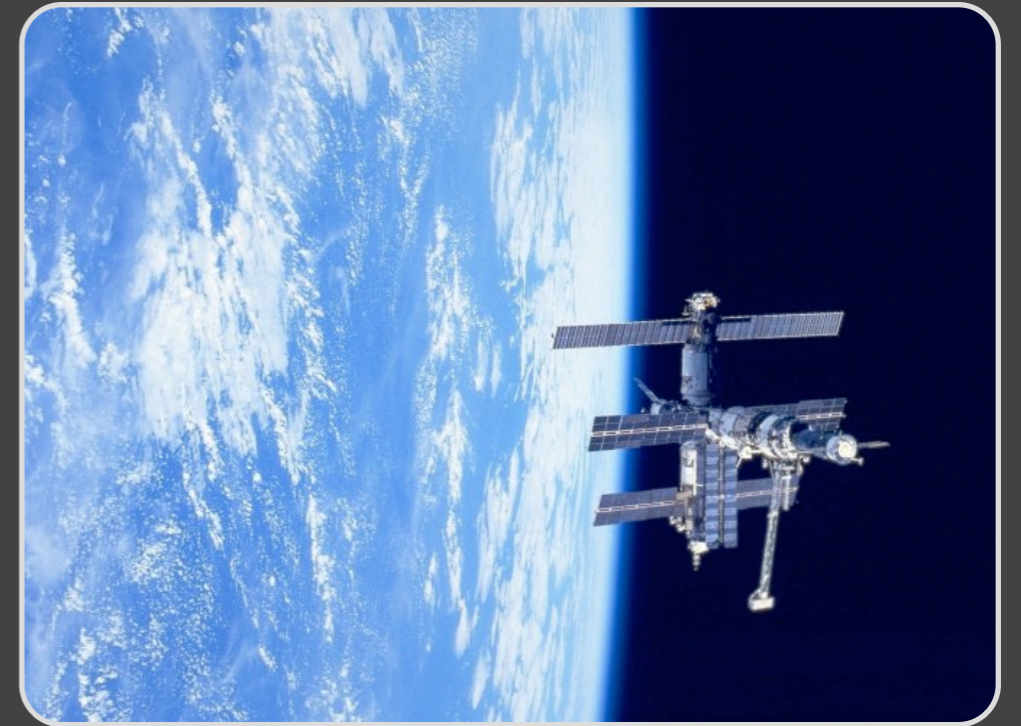
This presentation is intended to demonstrate the inherent security, design and configuration flaws in publicly accessible satellite communication networks and promote the use of safer satellite communication systems. Viewers and readers are responsible for their own actions and strongly encourage to behave themselves.

Satellite

- A satellite is **any object that orbits another object** (which known as its primary).

Artificial Satellites

- It was the English sci-fi writer **Arthur C. Clarke** who conceived the possibility of artificial communication satellites in 1945. Clarke examined the logistics of satellite launch, possible orbits and other aspects.
- The first artificial satellite was **Sputnik 1** launched by Soviet Union on 4 October 1957



Types of Artificial Satellites

- Astronomical satellites
- Reconnaissance satellites
- Navigation satellites
- Killer satellites/anti-satellite weapons
- Solar power satellites
- Space stations
- Weather satellites
- Miniaturised satellites
- Biosatellites

How is a Satellite Launched into an Orbit?



Satellite Internet Services

- Used in locations where terrestrial Internet access is not available and in locations which move frequently, e.g. vessels at sea and war zone.
- Can be used where the most basic utilities are lacking, require a generator or battery power supply that can produce enough electricity.

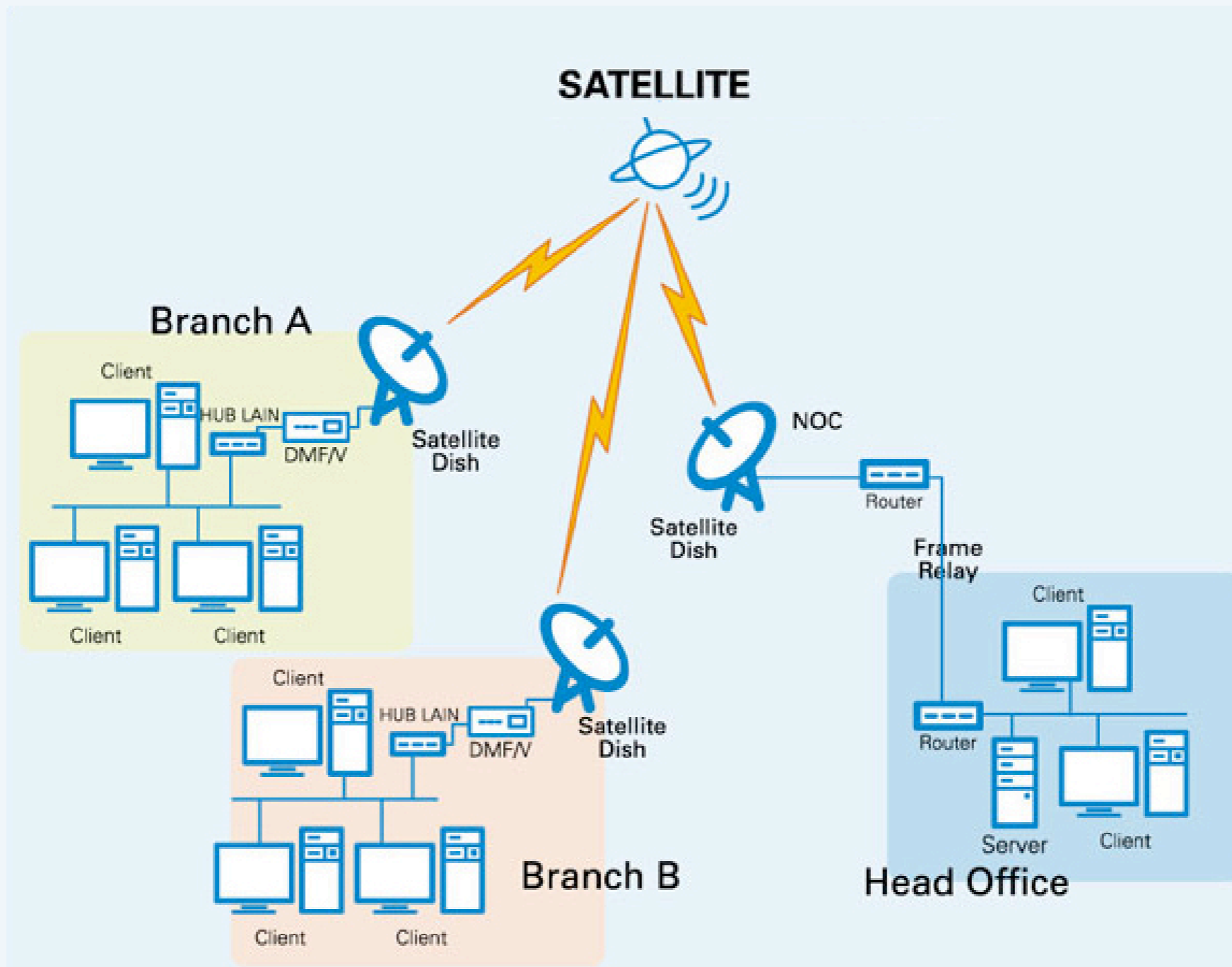
Three Types of Satellite Internet Services

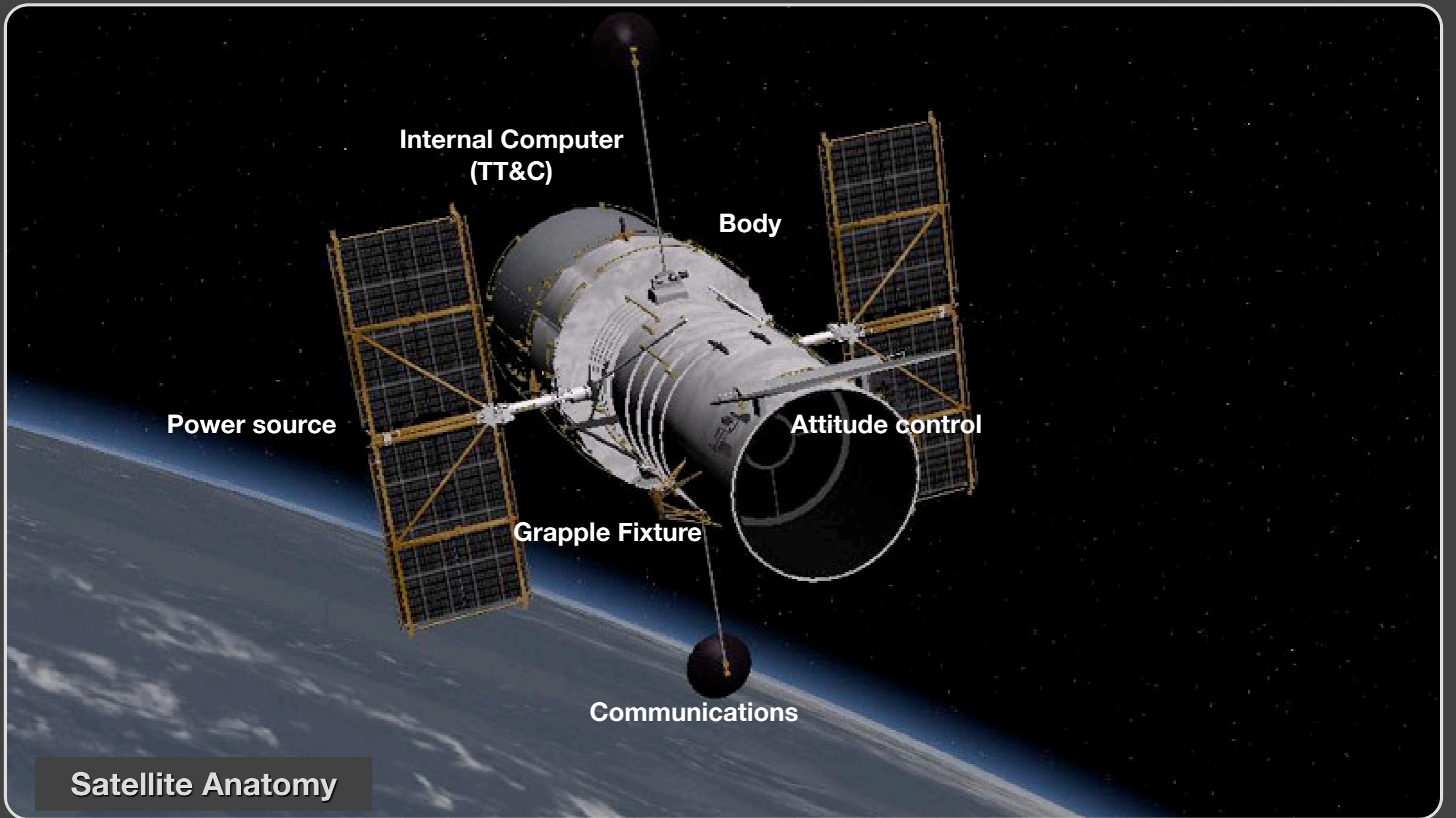
- **One-way multicast:** used for IP multicast-based data, audio and video distribution. Most Internet protocols will not work correctly over one-way access, since they require a return channel.
- **One-way with terrestrial return:** used with traditional dial-up access to the Internet, with outbound data travelling through a telephone modem, but downloads are sent via satellite at a speed near that of broadband Internet access.
- **Two-way satellite access:** allows upload and download data communications.

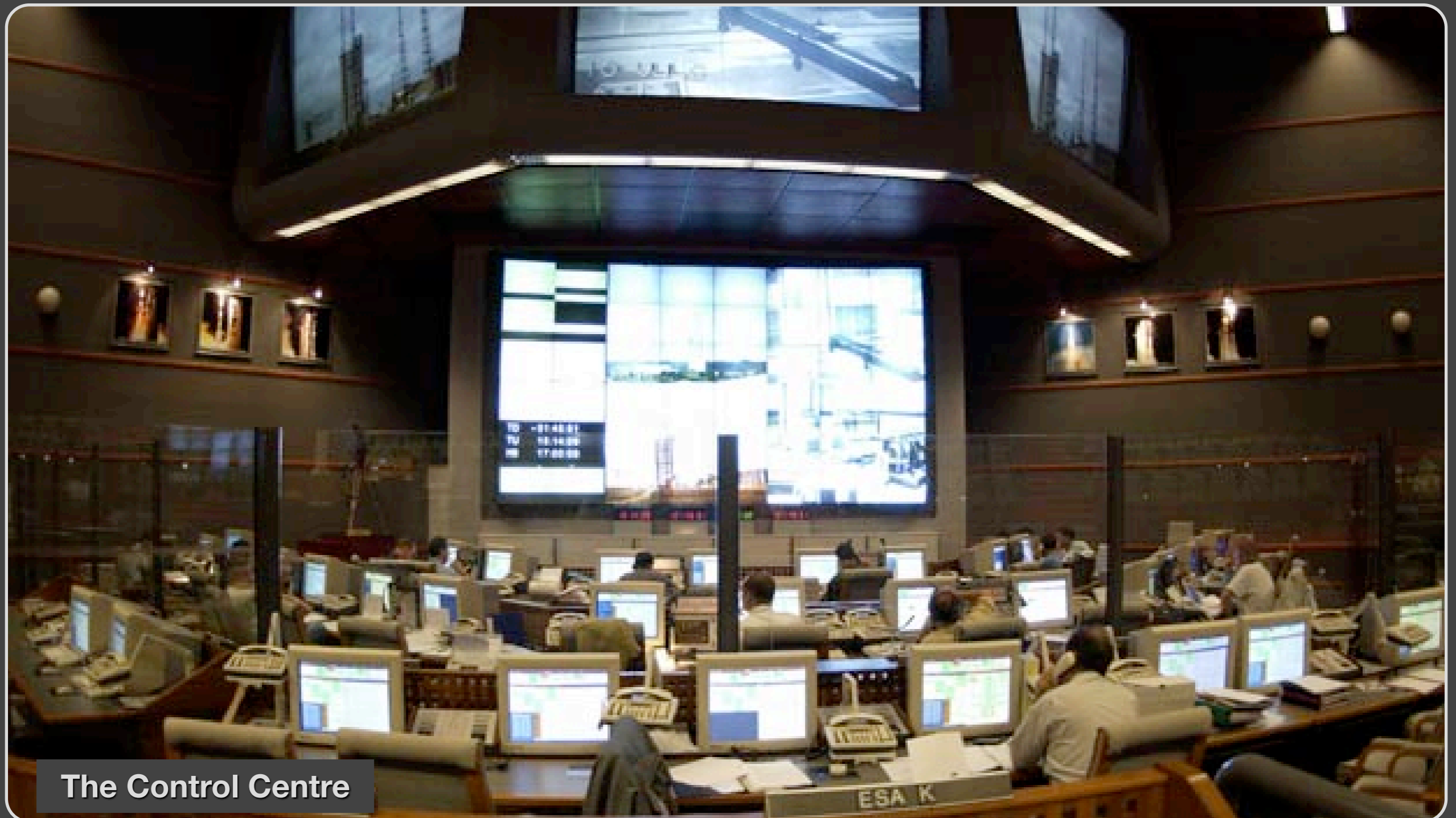
Very Small Aperture Terminal (VSAT)

- Two-way satellite ground station with a dish antenna that is smaller than 3 metres.
- Nearly all VSAT systems are now based on IP, with a very broad spectrum of applications.
- Most commonly used interactive and transactional application (online communication between head office and branches, flight ticket and hotel reservation, ATM (Automated Teller Machine) and small data traffic) and terminal application with centralised database (data entry, inventory control and payment point)









The Control Centre



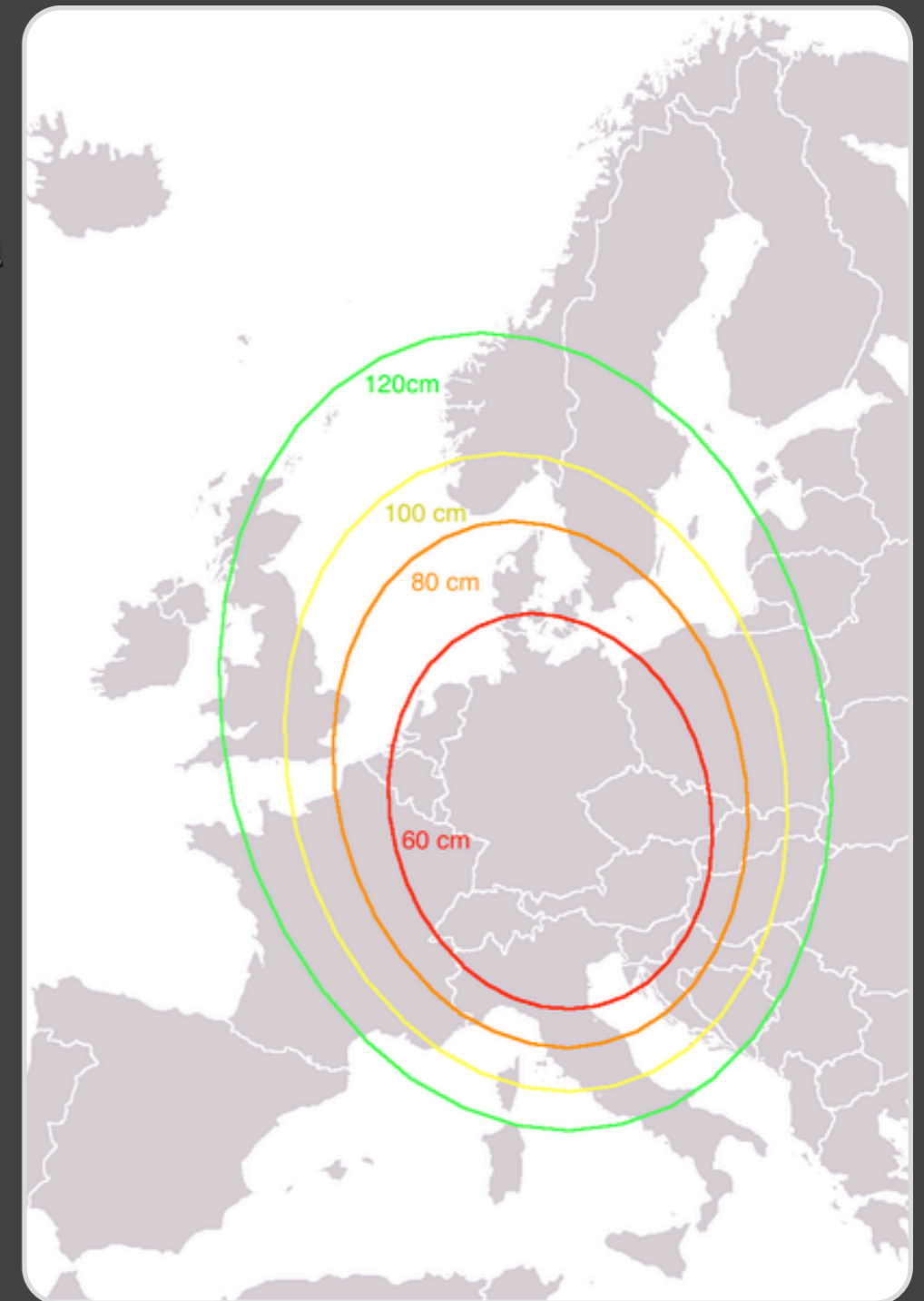
Tracking, Telemetry and Command Station

Topologies of VSAT

- A **star topology**, using a central uplink site, such as a network operations centre (NOC), to transport data back and forth to each VSAT terminal via satellite,
- A **mesh topology**, where each VSAT terminal relays data via satellite to another terminal by acting as a hub, minimising the need for a centralised uplink site,
- and a **combination of both** star and mesh topologies.

Satellite Footprint

- The footprint of a satellite is the ground area that its transponders cover, and determines the satellite dish diameter required to receive each transponder's signal.
- There is usually a different map for each transponder (or group of transponders) as each may be aimed to cover different areas of the ground.
- Footprint maps usually show either the estimated minimal satellite dish diameter required, or the signal strength in each area measured in dBW.

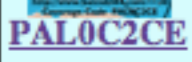




100° E - 145.9° E

(SE Asia, Australia, China, Japan, Korea)

Satellite Name	Position	HD TV	TV Digital	TV Analog	Radio Digital	Radio Analog	Data
ASIASAT 2	100.5° East	0	97	0	51	0	4
EXPRESS A2	103.0° East	0	13	0	12	0	2
ASIASAT 3S	105.5° East	0	258	0	56	0	22
CAKRAWARTA 1	107.7° East	0	70	0	19	0	5
TELKOM 1	108.0° East	0	57	0	0	0	4
AAP 1	108.2° East	0	57	0	0	0	17
BSAT 1A, 2A	110.0° East	10	3	4	14	0	0
JCSAT 110	110.0° East	0	63	0	20	0	0
SINOSAT 1	110.5° East	0	59	0	36	0	4
PALAPA C2	113.0° East	0	31	2	4	0	8
KOREASAT 2	113.0° East	0	48	0	0	0	3
KOREASAT 3	116.0° East	0	125	0	1	0	12
TELKOM 2	118.0° East	0	1	0	0	0	0
THAICOM 1A	120.0° East	0	6	0	1	0	0
ASIASAT 4	122.0° East	0	79	0	1	0	17
JCSAT 4A	124.0° East	0	93	0	0	0	7
JCSAT 3	128.0° East	0	142	0	103	0	21
JCSAT 5A	132.0° East	0	2	0	0	0	0
APSTAR 6	134.0° East	0	46	2	55	0	3
APSTAR V / TELSTAR 18	138.0° East	0	151	0	0	0	2
EXPRESS AM3	140.0° East	0	14	0	8	0	1
SUPERBIRD C	144.0° East	0	57	0	4	0	0

source: <http://www.satcodx4.com/eng/> accessed on 28 August 2006

		R-DIG	RADIO DANGDUT TPI	MPEG-2 1002	6700 3/4 1213	1213 2 1 1	BID	TPI	2005-09-22, 13:25 SatcoDX Indonesia 2006-08-27, 11:09 Indonesia 2
1K 10.970 V		TV-DIG-CRYPT	ABC Asia Pacific	MPEG-2 VICS	28850 3/4 770 771	769 3 1 4369	ENG	SCOPUS PROVIDER	2004-12-26, 11:32 2006-08-28, 14:16 AutoScan China 1
		TV-DIG-CRYPT	DW	MPEG-2 VICS	28850 3/4 1026 1027	1025 4 1 4369	DEU	SCOPUS PROVIDER	2004-12-26, 11:32 2006-08-28, 14:16 AutoScan China 1
		TV-DIG-CRYPT	NASA TV	MPEG-2 VICS	28850 3/4 1282 1283	1281 5 1 4369	ENG	SCOPUS PROVIDER	2004-12-26, 11:32 2006-08-28, 14:16 AutoScan China 1
		DATA	Data Service		28850 3/4	1 1 4369			2004-11-11, 13:20 SatcoDX China 2006-08-28, 14:16 AutoScan China 1
		DATA	Data Service		28850 3/4	2 1 4369			2004-11-11, 13:20 SatcoDX China 2006-08-28, 14:16 AutoScan China 1
3K 11.472 H		TV-DIG	Global TV	MPEG-2 32	28125 3/4 33 34	33 1 1 4369	BID	SCOPUS PROVIDER	2005-11-02, 00:49 Planko 2005-12-10, 09:21 AutoScan Indonesia 1
		TV-DIG	Metro TV	MPEG-2 1056	28125 3/4 1057 1058	1057 2 1 4369	BID	SCOPUS PROVIDER	2005-11-02, 00:49 Planko 2005-12-10, 09:21 AutoScan Indonesia 1
		TV-DIG	MQTV	MPEG-2 2084 2080	28125 3/4 2081 2082	2081 3 1 4369	BID	SCOPUS PROVIDER	2005-11-02, 00:49 Planko 2005-12-10, 09:21 AutoScan Indonesia 1
		TV-DIG	TPI TV	MPEG-2 1001	28125 3/4 1110 1211	1110 1 1 1		TPI	2006-06-10, 11:54 AutoScan Indonesia 1 2006-06-10, 11:54 AutoScan Indonesia 1
		R-DIG	RADIO DANGDUT TPI	MPEG-2	28125 3/4	1213 2 1		TPI	2006-06-10, 11:54 AutoScan Indonesia 1 2006-06-10, 11:54

MEASAT

- 01 COMPANY PROFILE
- 02 SATELLITE FLEET
- 03 SERVICES
- 04 SUPPORT
- 05 MEDIA RELATIONS
- 06 CLIENTELE

home contact us location map sitemap



24-Hour Technical Support

Providing round-the-clock advice and assistant.

Our 24-Hour Hotline is **+60 (3) 8213 2288**

Live Chat Support

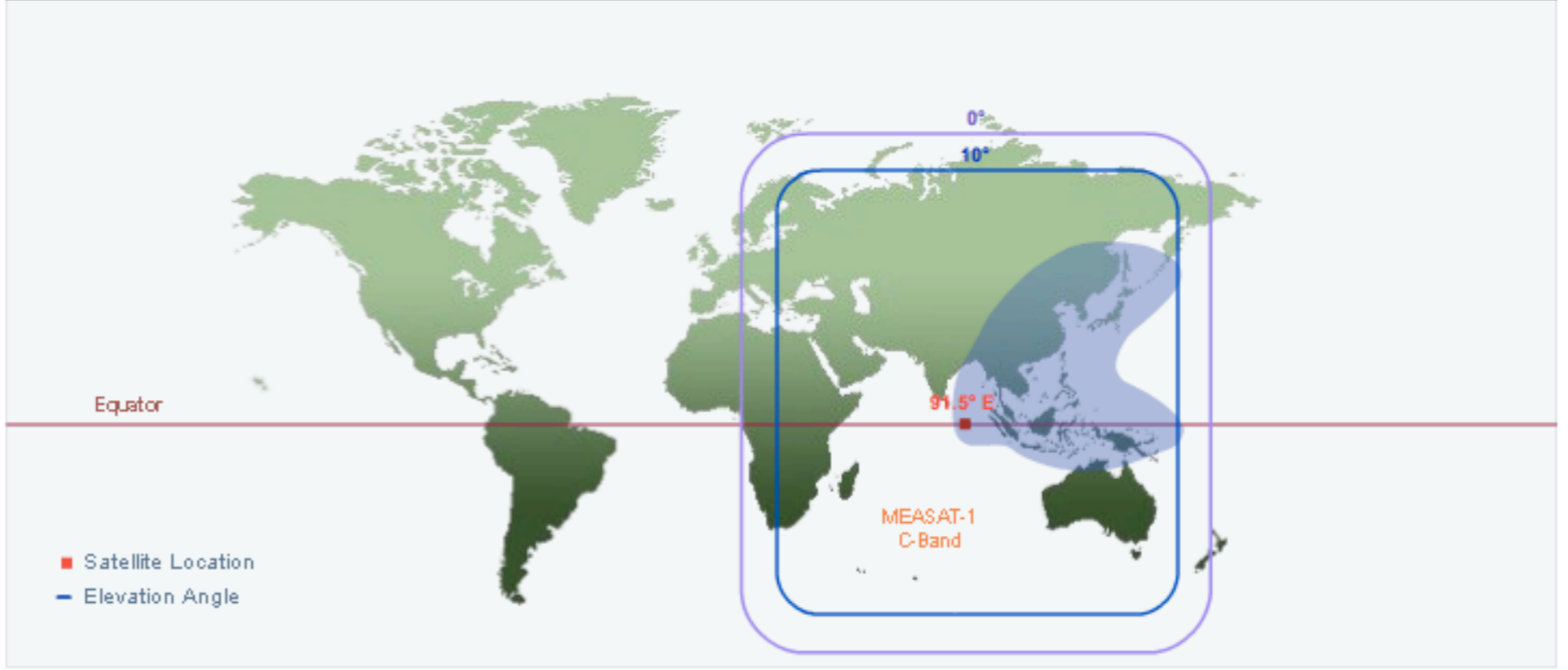


Search

Satellite Fleet



- Satellite Fleet
- MEASAT-1
- MEASAT-2
- MEASAT-3
- MEASAT-1R
- MEASAT-5



MEASAT



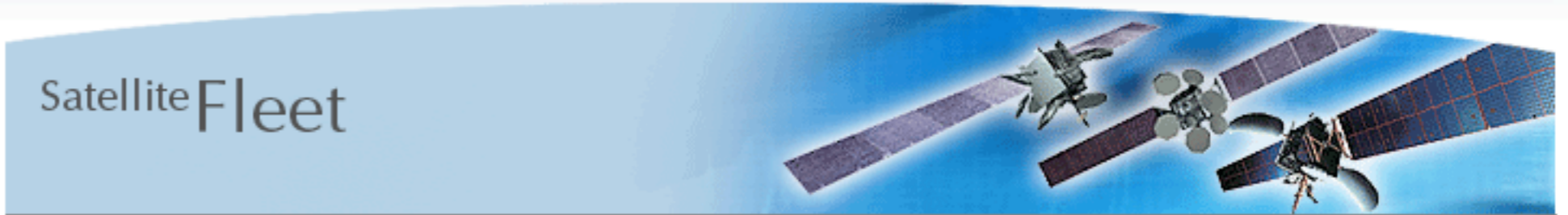
24-Hour Technical Support

Providing round-the-clock advice and assistant.

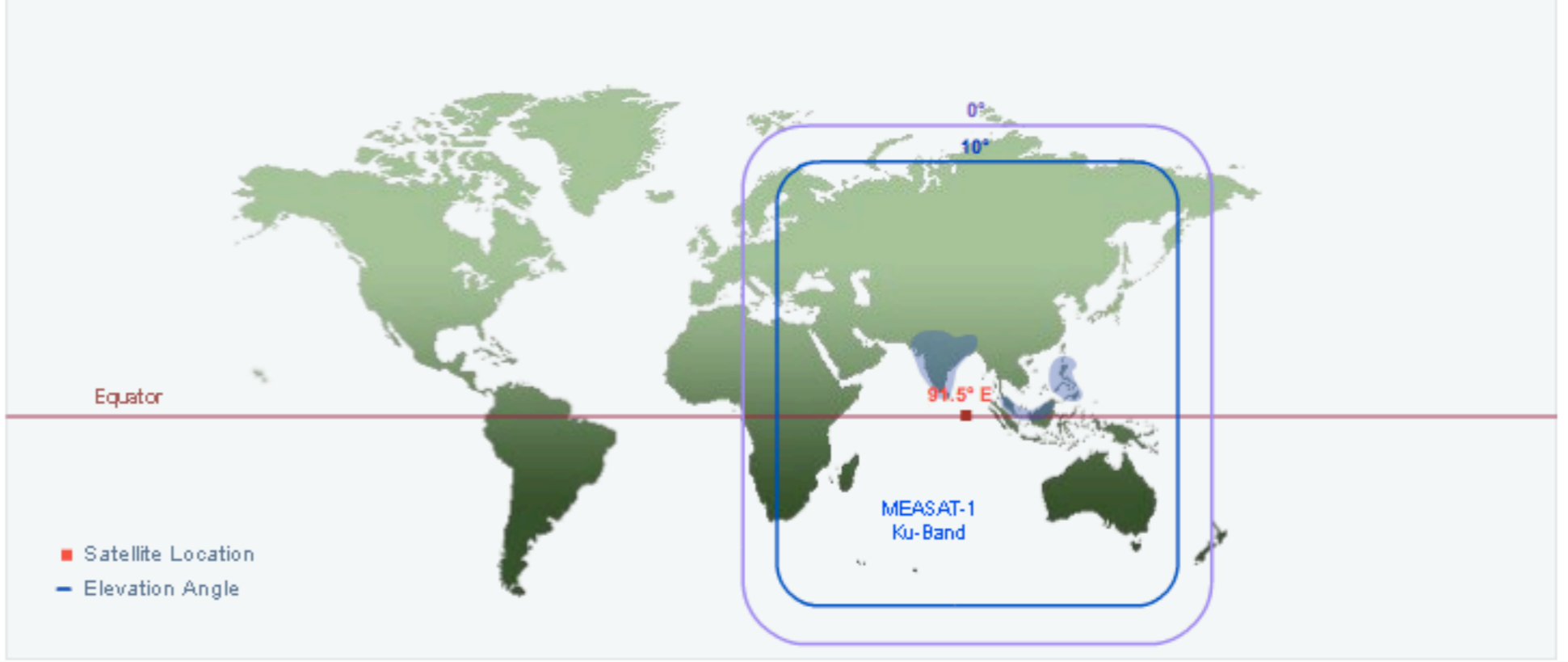
Our 24-Hour Hotline Is **+60 (3) 8213 2288**

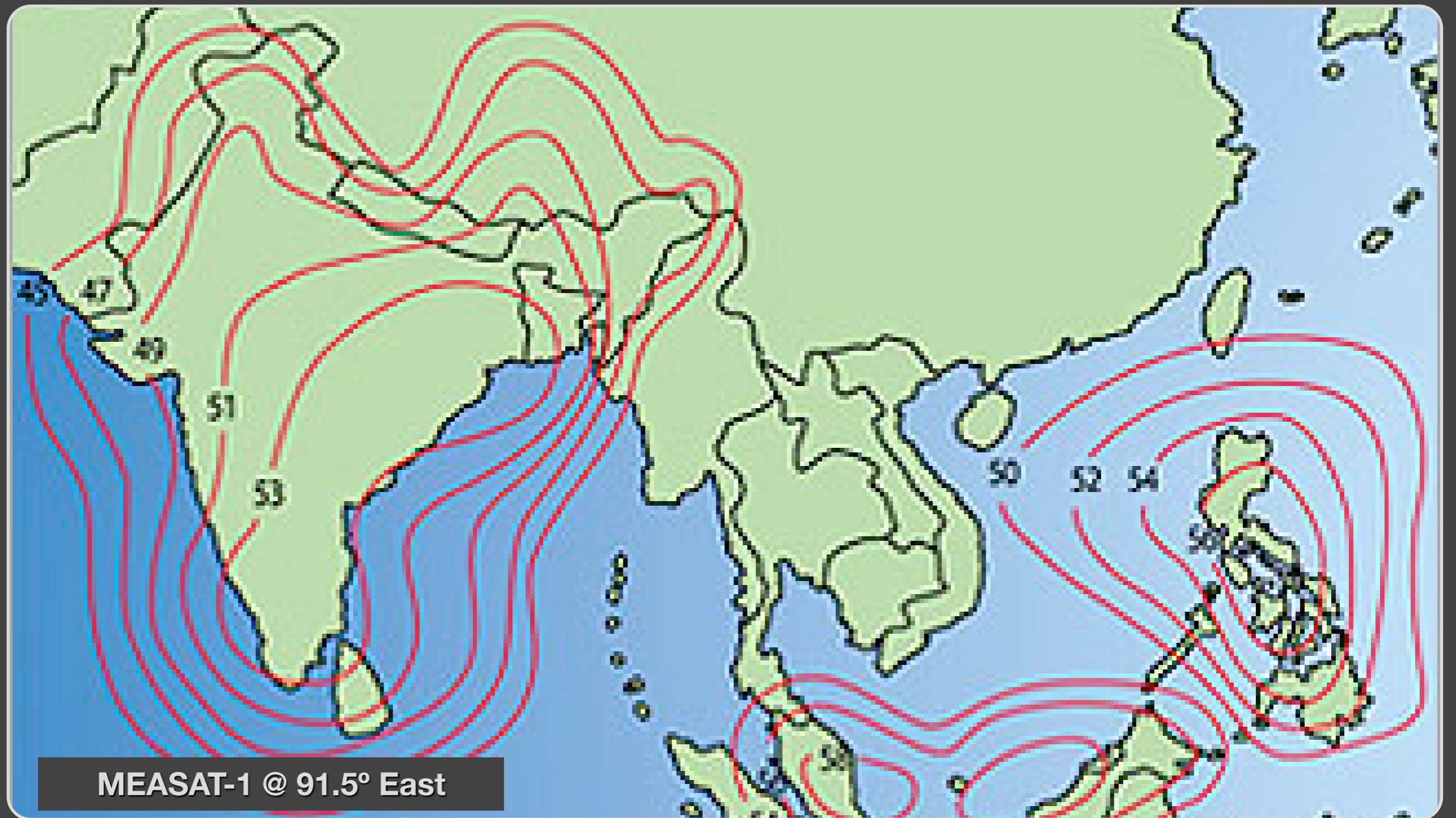
Live Chat Support

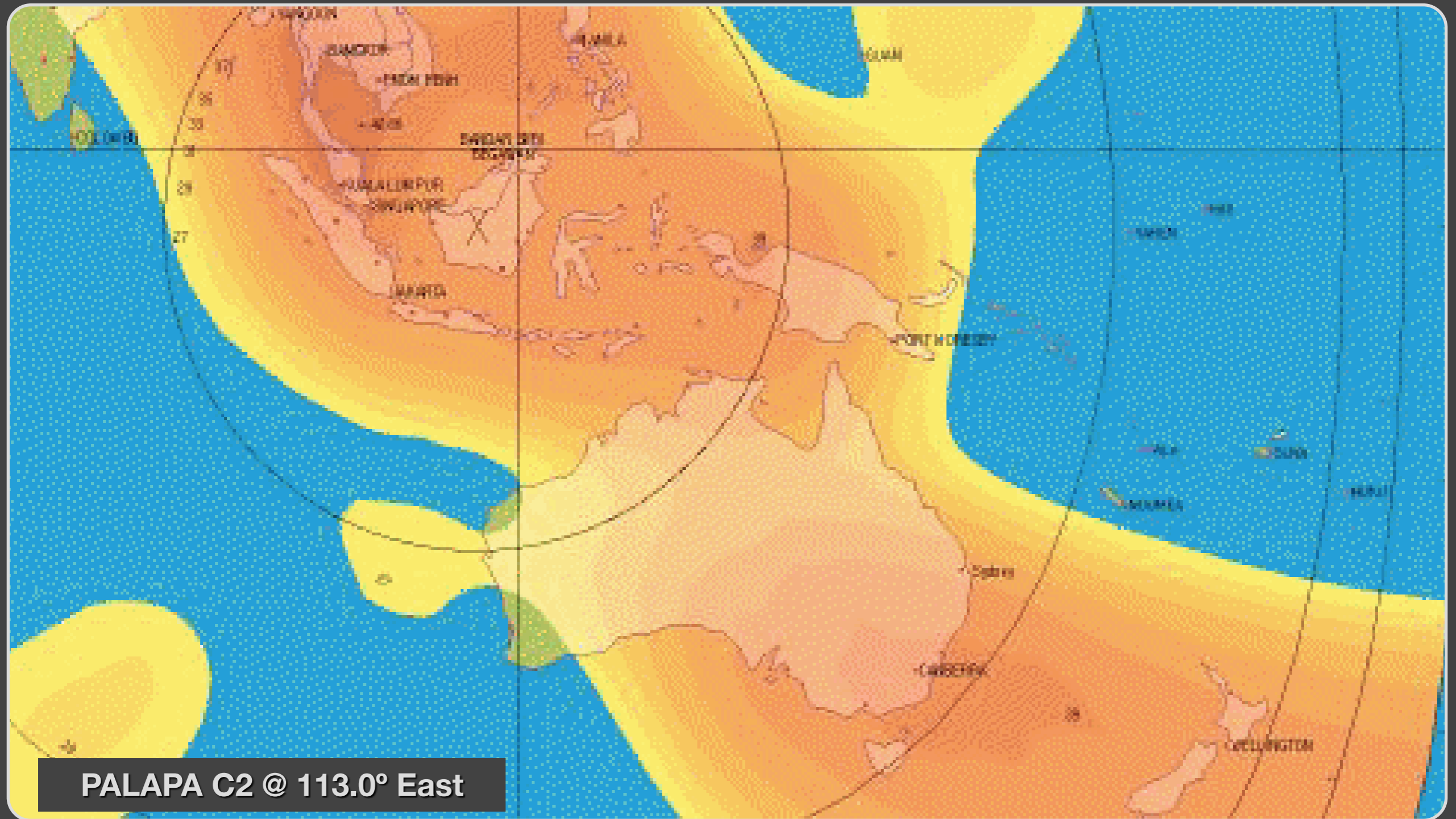
Search



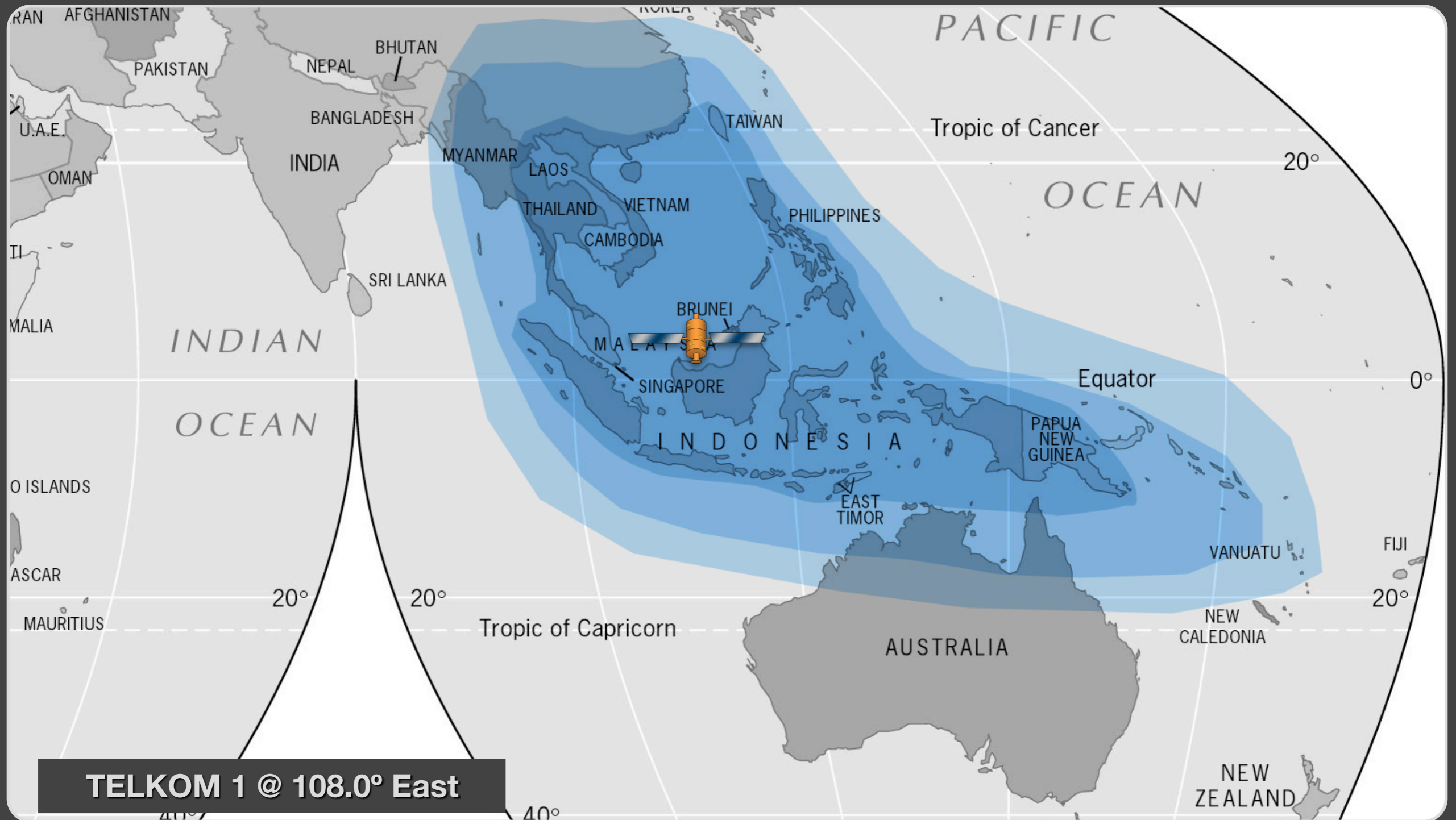
- [Satellite Fleet](#)
- [MEASAT-1](#)
- [MEASAT-2](#)
- [MEASAT-3](#)
- [MEASAT-1R](#)
- [MEASAT-5](#)

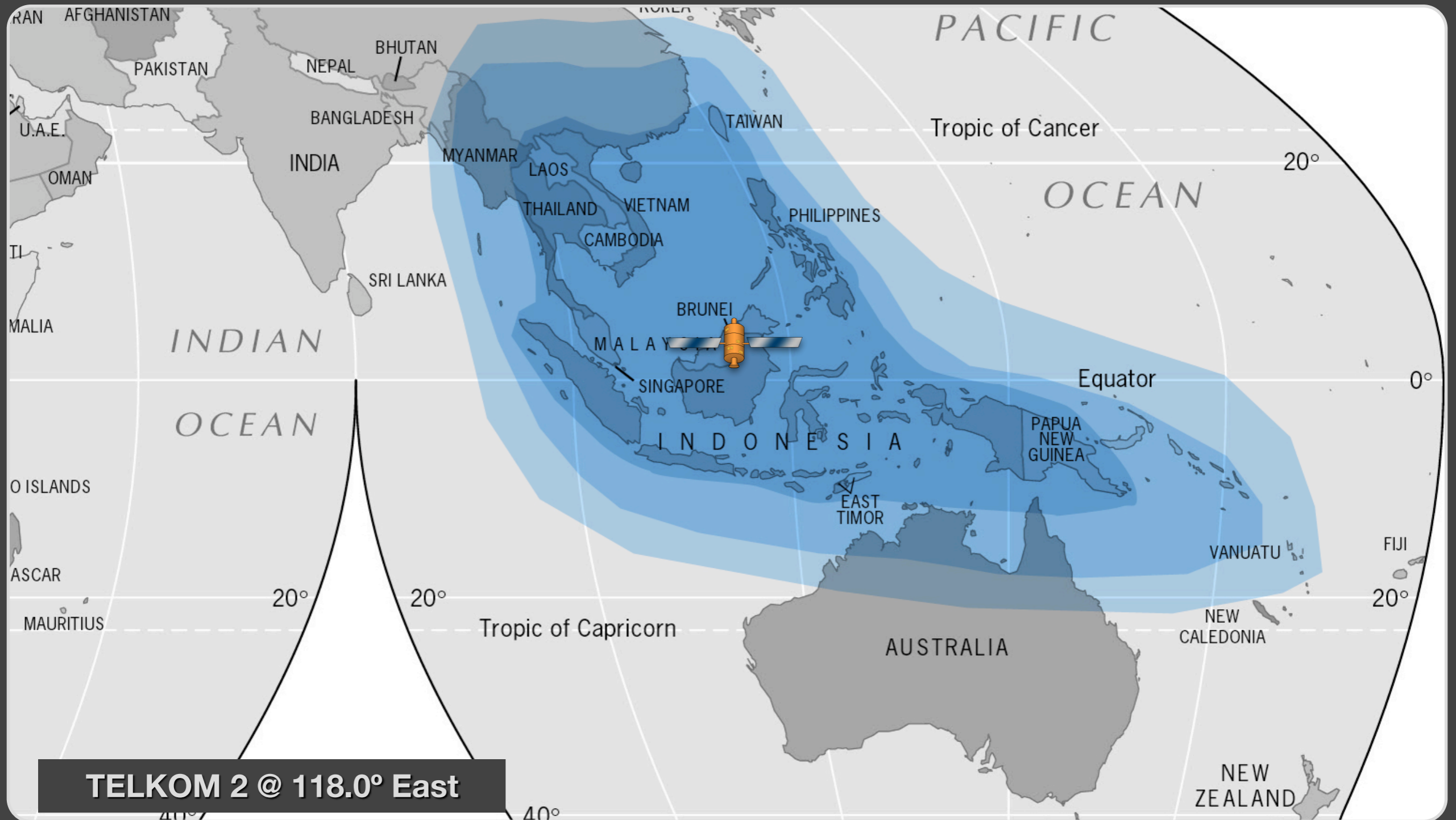






PALAPA C2 @ 113.0° East





Attacks against Satellite Systems

It's politically sensitive, but it's going to happen. Some people don't want to hear this, and it sure isn't in vogue ... but—absolutely—we're going to fight in space. We're going to fight from space and we're going to fight into space...

General Joseph W. Ashy
Former Commander in Chief U.S. Space Command

source: http://www.au.af.mil/au/awc/awcgate/saas/spacy_wl.pdf accessed on 21 September 2006

Hypothetical Attacks against Satellite Systems

Denial of Service Attacks

- **Jam uplink and downlink**
 - White noise at frequency.
 - Requires directed antenna.
 - Requires very low power.
 - Difficult to detect, especially if occurring at irregular intervals.



source: <http://www.decodesystems.com/attacks.html> accessed on 28 August 2006

Denial of Service Attacks

- Overpower uplink
 - Can be done with transportable satellite ground terminals
 - In tri-band (C-band, X-band, and Ku-band).
 - Power limited.
 - Uplink equipment now contains ID coding.



source: <http://www.decodesystems.com/attacks.html> accessed on 28 August 2006

Orbital Positioning Attacks

- **Ranging transponder spoofing**
 - Multiple ground stations triangulate satellite position using a series of tones sent to a transponder.
 - Ground stations observe phase differentials.
 - Ground or airborne spoofer could transmit false response, resulting in incorrect orbit determination.



source: <http://www.decodesystems.com/attacks.html> accessed on 28 August 2006

Orbital Positioning Attacks

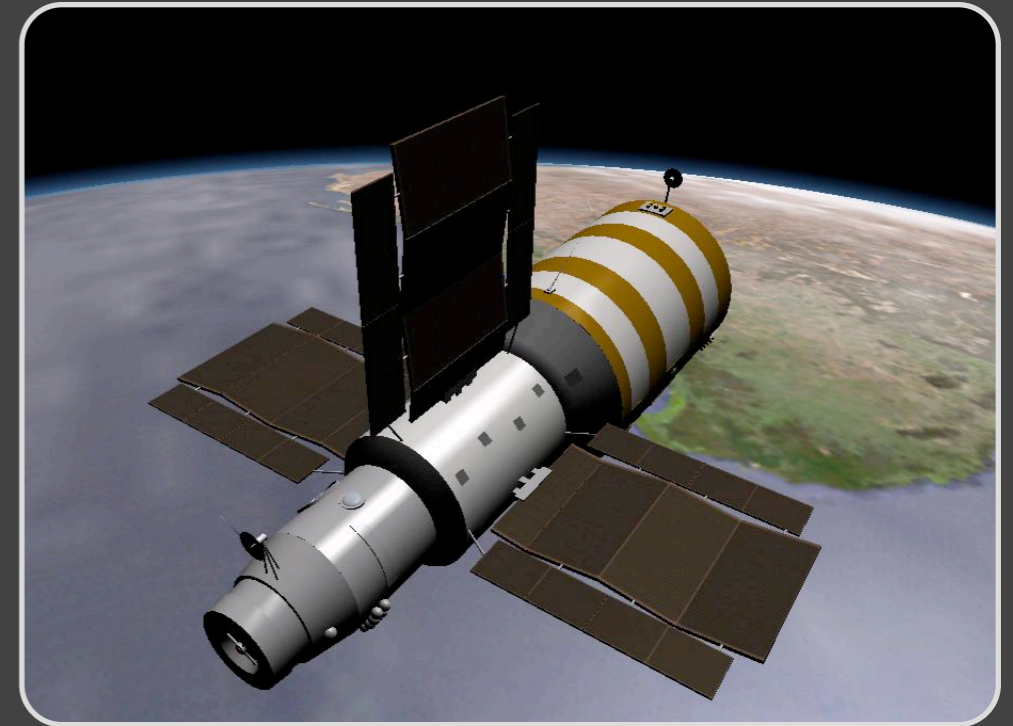
- **Direct commanding**
 - Preparation and delivery of telecommand queue.
- **Command replay**
 - Record outbound telecommand queue from TT&C facility. Replay later to initiate duplicate action.



source: <http://www.decodesystems.com/attacks.html> accessed on 28 August 2006

Orbital Positioning Attacks

- **Insertion after confirmation but prior to execution**
 - SCC formulates telecommand queue and sends to TT&C.
 - TT&C uplinks and receives readback, which it returns to SCC.
 - If readback is correct, SCC waits for proper time to execute.
 - Channel is vulnerable to update during this period — new telecommand queue may be uploaded prior to authenticated execute.



source: <http://www.decodesystems.com/attacks.html> accessed on 28 August 2006

Practical Attacks against Satellite Systems















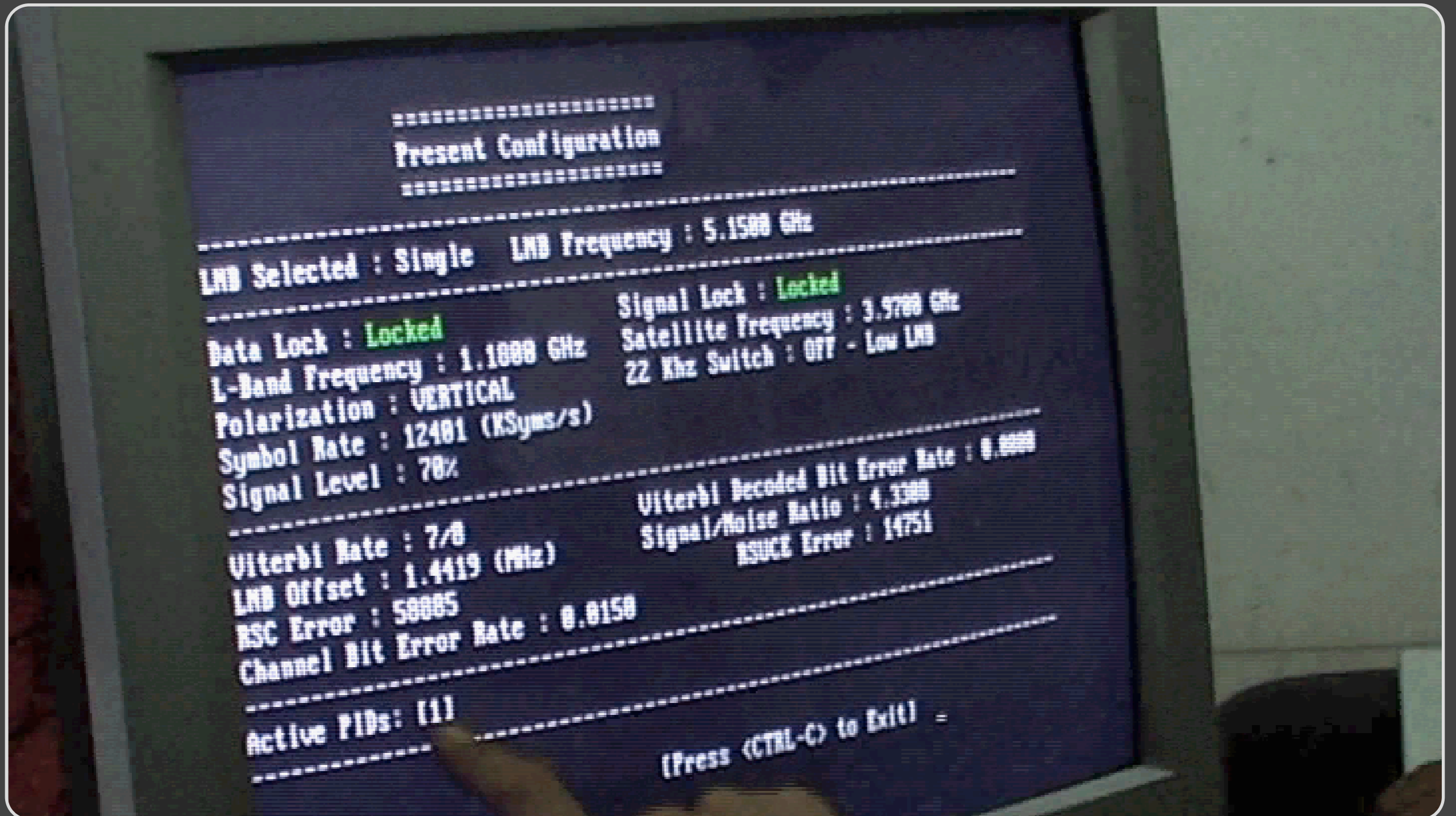


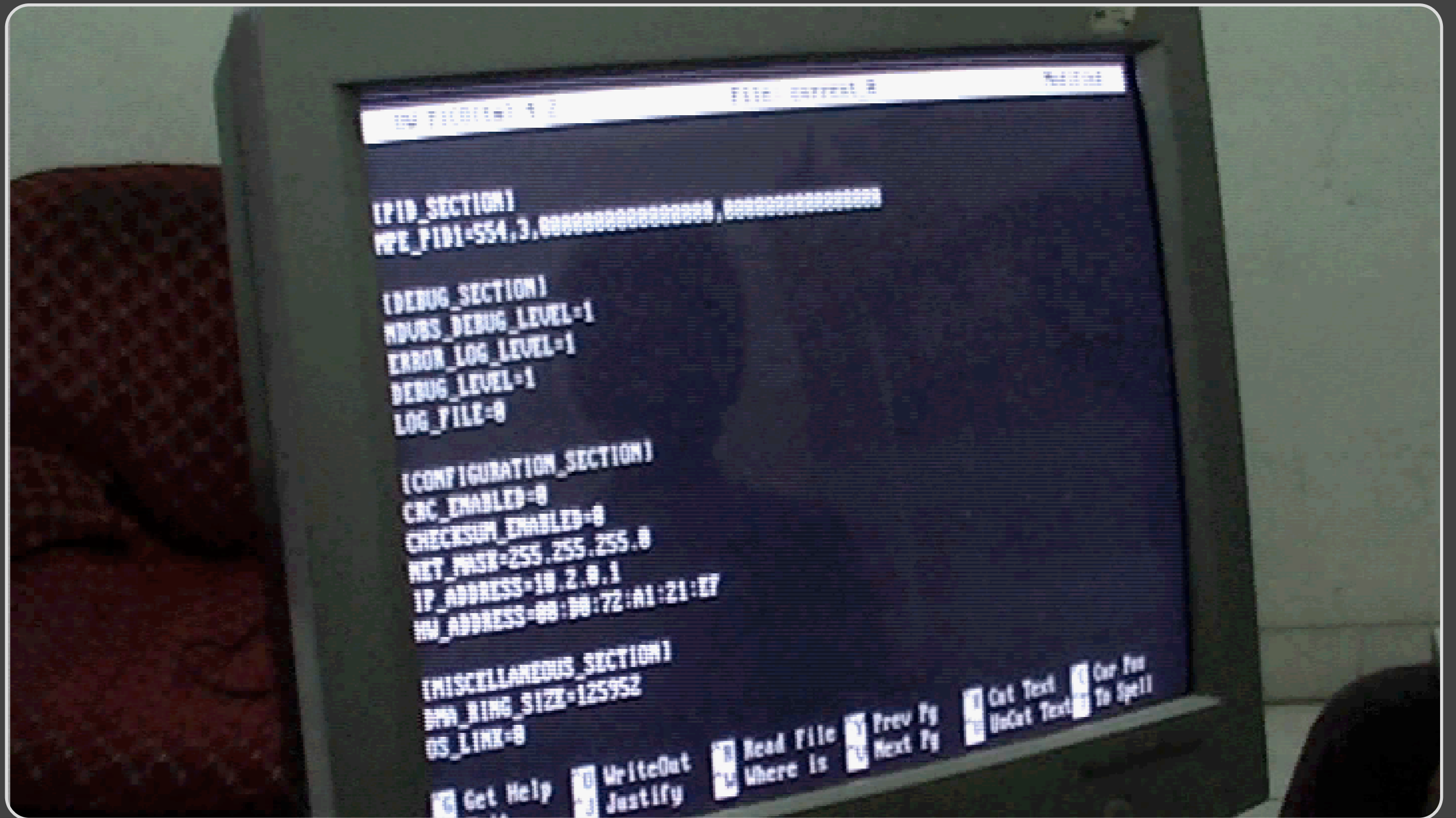













```

[root@dvbhack ~]# scan_pid sniff_mac
[root@dvbhack bellua_dvb_tools]# ./sniff_mac
what PID?
554
Sniff MAC for PID:554
-----
MAC found! 00000000.00:d0:72:a1:21:ef.0455

[root@dvbhack bellua_dvb_tools]# cd /
[root@dvbhack /]# ifconfig aba_0 inet 200.110.17.89 netmask 255.255.255.240
netmask: No address associated with name
ifconfig: '--help' gives usage information.
[root@dvbhack /]# ifconfig aba_0 inet 200.110.17.89 netmask 255.255.255.240
[root@dvbhack /]# ping
Usage: ping [-L] [-d] [-f] [-q] [-s packetsize] [-t ttl] [-i interval] [-w deadline]
[-p pattern] [-M mtu discovery hint] [-S sndbuf]
[-T timestamp option] [-Q tos] [hop1 ...] destination
[root@dvbhack /]# ping -i 200.110.17.89 www.yahoo.com
PING www.yahoo-ht2.akadns.net (209.131.36.158) from 200.110.17.89 : 56(84) bytes
of data.
64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_seq=1 ttl=53 time:

```

Discussion

- Other attacks against satellite?
- Law issues?