

Playing in a Satellite environment 1.2

Christian Martorella
Leonardo Nve
cmartorella@s21sec.com



Why 1.2?

1. because I'm sure that some people will publish more attacks.
- .2 because there are previously presentations about satellites.

Who commented this before?

- Warezzman – (in 2004 at Undercon VIII first Spanish hacker CON)
- Jim Geovedi & Raditya Iryandi (HITBSecConf2006)
- Andre Adelbach (Hack.lu 2006)
- Adam Laurie (Blackhat 2009 at DC)
- Leonardo Nve at S21Sec Blog (February 2009)

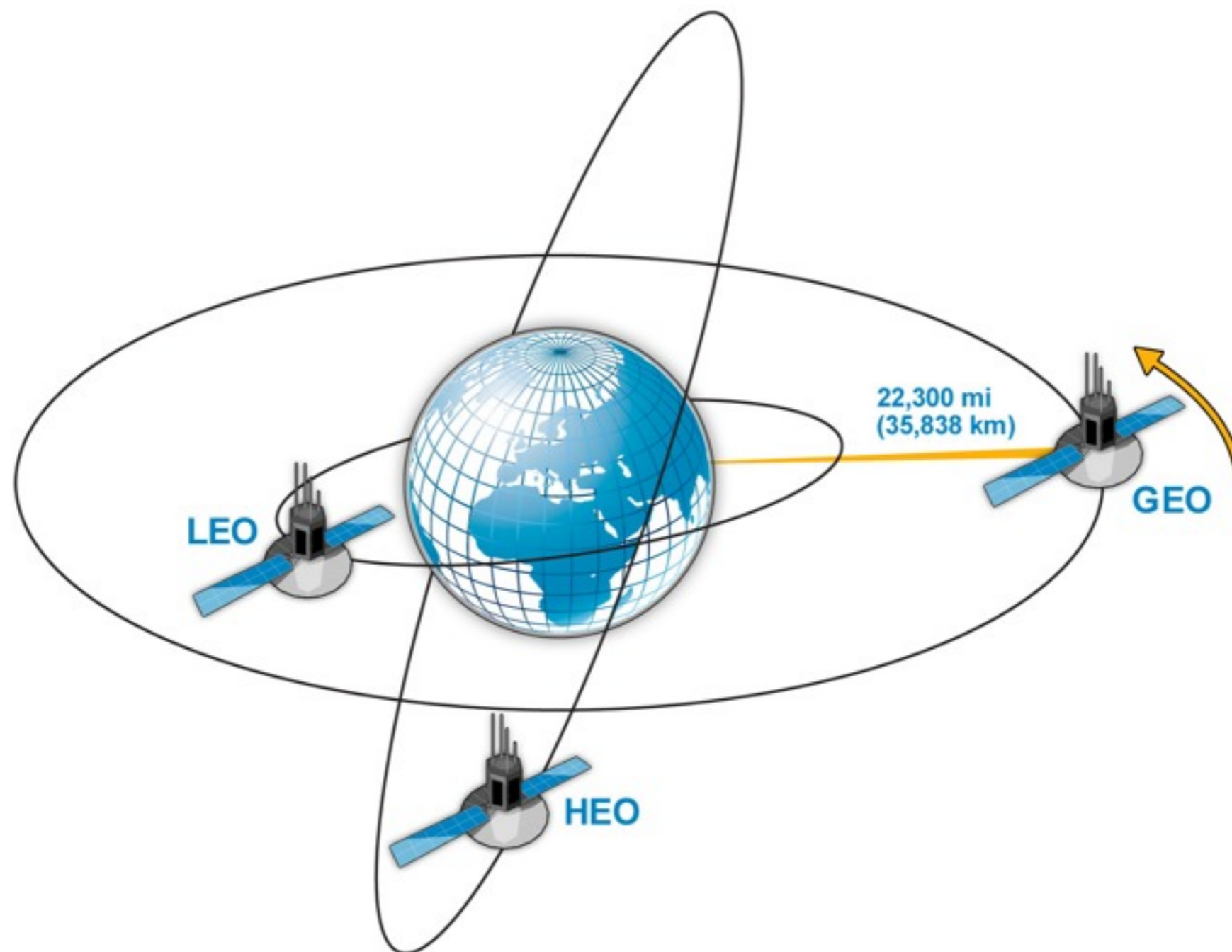
Intro to SAT

- A satellite is a radio-frequency repeater - that is launched by a rocket and placed in orbit around the earth.

Intro to SAT

- Orbit based satellites
 - Low Earth orbiting (LEO)
 - Geostationary orbit (GEO)
 - Other: Molniya, High (HEO), etc.
- Function based satellites
 - Communications
 - Earth observation
 - Other: Scientifics, ISS, GPS, etc.

Intro to SAT



Intro to SAT

- Satellite LEO
 - Meteorological
 - HAM (Amateur Radio Operator)
 - GPS
- Satellite GEO
 - UFO (UHF Follow ON) Military
 - Inmarsat
 - Meteorological (Meteosat)
 - SCPC / Telephony link FDMA



The signal from the sky you have been waiting

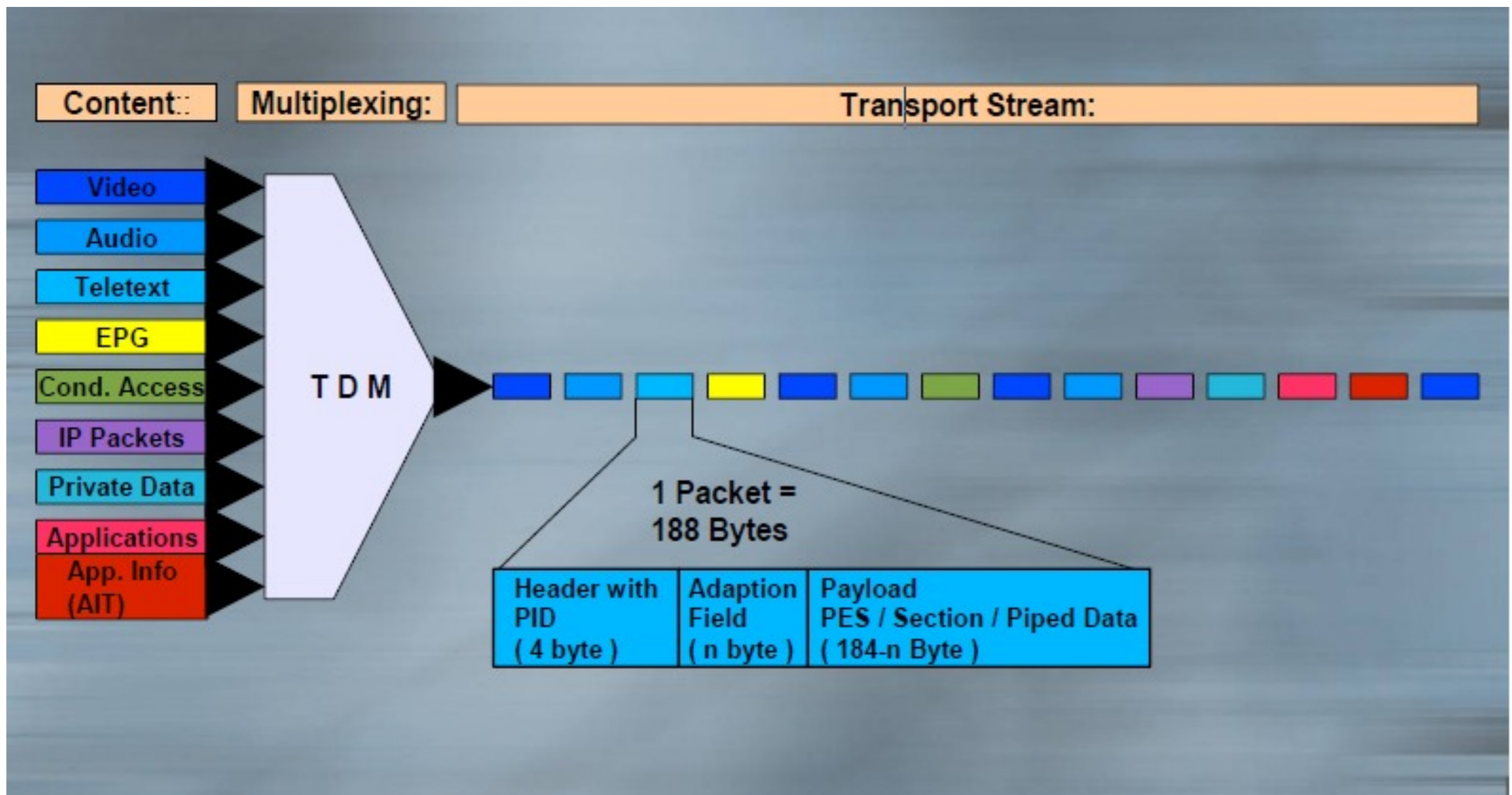
DVB

- Defines audio and video transmission, and data connections.
- Standard of “European Telecommunications Standards Institute” (ETSI).
- DVB-S & DVB-S2 is the specification for Satellite communications.

DVB-S

- Transponder: Like channels (in Satellite comms)
 - Frequency (C band or Ku). Ex: 12.092Ghz
 - Polarization. (horizontal/vertical)
 - Symbol Rate. Ex: 27500Kbps
 - FEC.
- Every satellite has many transponders onboard which are operating on different frequencies

DVB-S TS (Transport Stream)



DVB-S TS (Transport Stream)

Header



Program ID (PID): It permits different programs at same transponder with different components [Example BBC1 PIDs: 600 (video), 601 (English audio), 603 (subtitles), 4167 (teletext)]

Special PIDs: NIT (Network Information Table), SDT (Service Description Table), PMT (Program Map Tables), PAT (Program Association Table).

DVB Feeds

- Temporal video links.
 - Live emissions, sports, news.
 - FTA – In open video. (unencrypted)

DVB Feeds



Hispasat Pre news
feed (live news)



ATLAS Agency to TV
feeds

DVB Feeds

BBC NEWS WORLD EDITION

NEWS SPORT WEATHER WORLD SERVICE A-Z INDEX SEARCH

You are in: Programmes: Newsnight

Newsnight

Thursday, 13 June, 2002, 00:28 GMT 01:28 UK

Enthusiast watches Nato spy pictures

By Mark Urban
Newsnight's Diplomatic Editor



Nato surveillance flights in the Balkans are beaming their pictures over an insecure satellite link - and anyone can tune in and watch their operations live.

The discovery was made last November by John Locker, a satellite enthusiast in north west England.



John Locker tried to alert the US military

He told Newsnight that he spent months e-mailing and faxing US and other Allied military officers to warn them of the dangers before finally deciding to go public.

Our investigation produced responses from Nato and American spokesmen that the pictures were unclassified. They said they would reveal nothing of value to a potential enemy.

One officer even told me that the broadcasts contained no information about the position or types of aircraft conducting the surveillance missions.

WATCH/LISTEN REAL MEDIA

ON THIS STORY

- The BBC's Mark Urban "A serious threat to Nato continues"

Newsnight

- Home
- Newsnight Review
- Latest programme
- Recent highlights
- About Newsnight
- Contact us

newsnight FORUM

NATO security risk?

See also:

- 09 Mar 00 | Europe Nato spy 'leaked bombing secrets'
- 09 Mar 00 | Politics Nato spy revelations 'staggering'
- 23 Oct 01 | Americas Hacktivists take sides in war

Internet links:

- The Center for Public Integrity

The BBC is not responsible for the content of external internet sites

News Front Page



- Africa
- Americas
- Asia-Pacific
- Europe
- Middle East
- South Asia
- UK
- Business
- Entertainment
- Science/Nature
- Technology
- Health

Talking Point

Country Profiles In Depth

Programmes

SPORT

WEATHER

SERVICES

- Daily E-mail
- News Ticker
- Mobile/PDAs

Text Only

Feedback

Help

EDITIONS

Change to UK

DVB Feeds

BBC NEWS WORLD EDITION

You are in: Programmes: Newsnight

Newsnight

Thursday, 13 June, 2002, 00:28 GMT 01:28 UK

Enthusiast watches Nato spy pictures

By Mark Urban
Newsnight's Diplomatic Editor

Nato surveillance flights in the Balkans are beaming their pictures over an insecure satellite link - and anyone can tune in and watch their operations live.

The discovery was made last November by John Locker, a satellite enthusiast in north west England.

He told Newsnight that he spent months e-mailing and faxing US and other Allied military officers to warn them of the dangers before finally deciding to go public.

Our investigation produced responses from Nato and American spokesmen that the pictures were unclassified. They said they would reveal nothing of value to a potential enemy.

One officer even told me that the broadcasts contained no information about the position or types of aircraft conducting the surveillance missions.

John Locker tried to alert the US military

WATCH/LISTEN ON THIS STORY

The BBC's Mark Urban "A serious threat to Nato continues"

Newsnight

Home

Newsnight Review

Latest programme

Recent highlights

About Newsnight

Contact us

newsnight FORUM

NATO security risk?

See also:

- 09 Mar 00 | Europe Nato spy 'leaked bombing secrets'
- 09 Mar 00 | Politics Nato spy revelations 'staggering'
- 23 Oct 01 | Americas Hacktivists take sides in war

Internet links:

- The Center for Public Integrity

The BBC is not responsible for the content of external internet sites



DVB Feeds

- Find feeds:

- Lists of channels in www

Dr HANS: <http://drhans.jinak.cz/news/index.php>

Zackyfiles: <http://www.zackyfiles.com> (in spanish)

Satplaza: <http://www.satplaza.com>

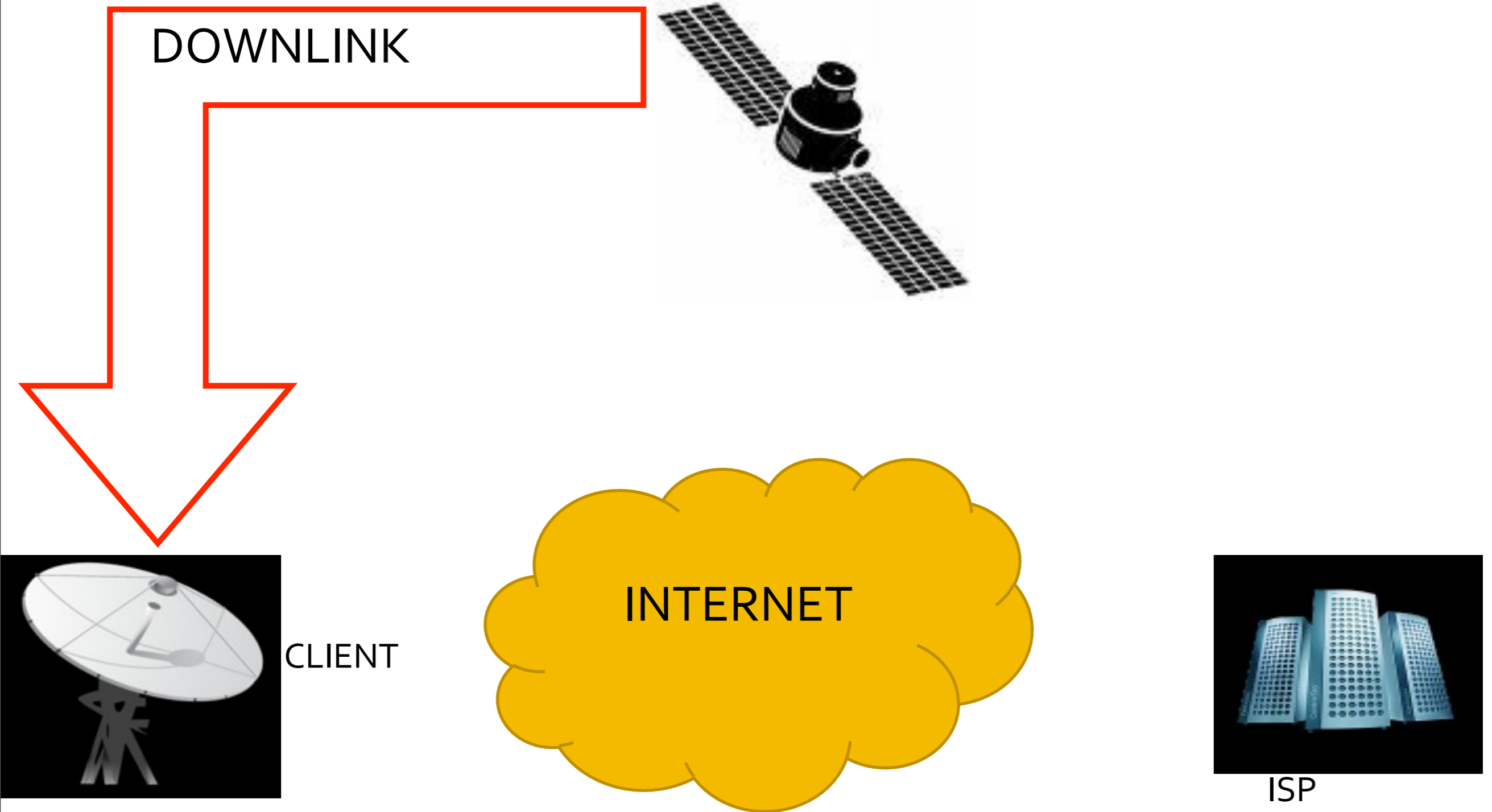
- Blind Scan

- Visual representations of the signal

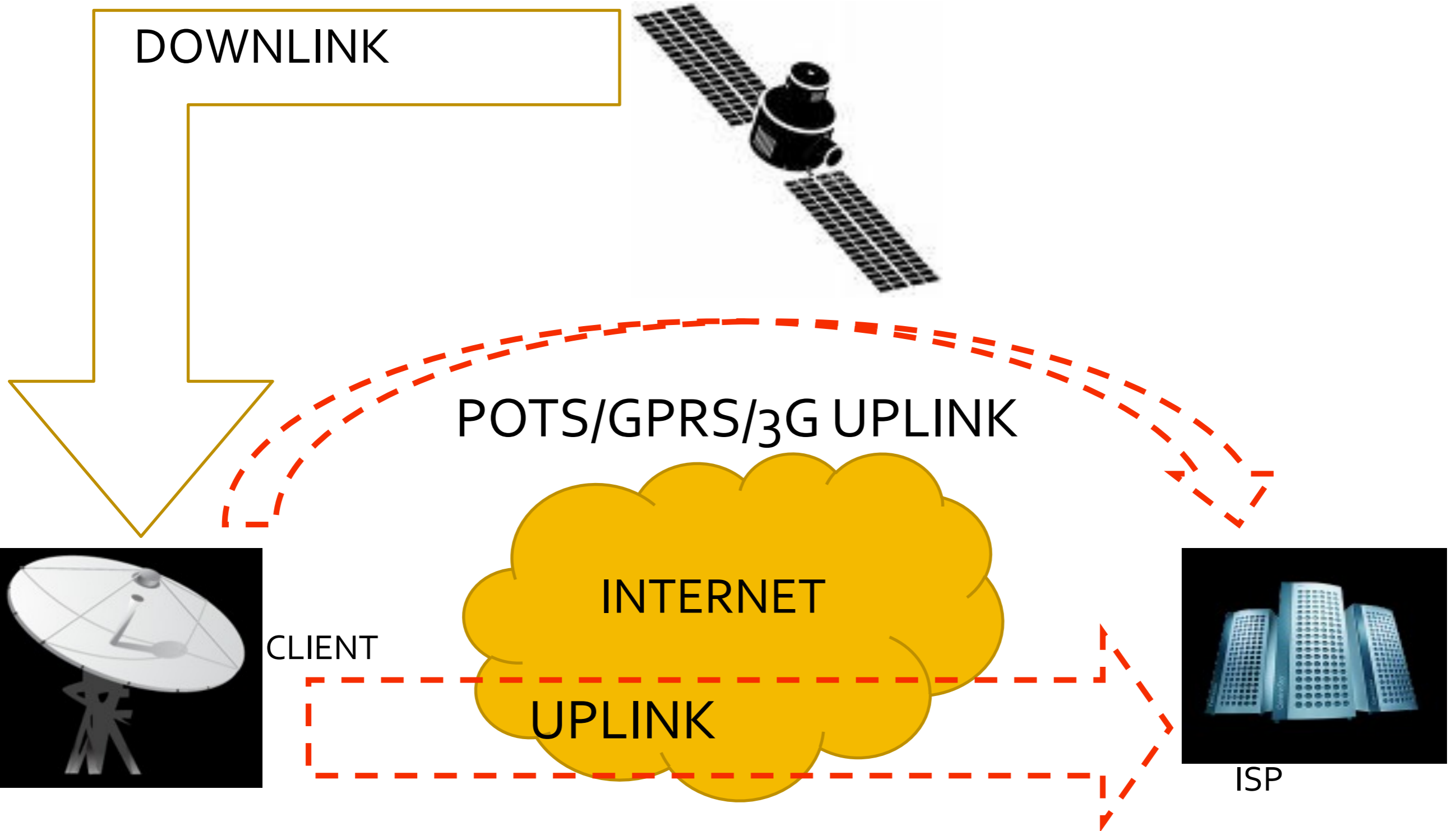
DVB Data

- Two scenarios
 - Satmodem
 - Satellite Interactive Terminal (SIT) or Astromodem

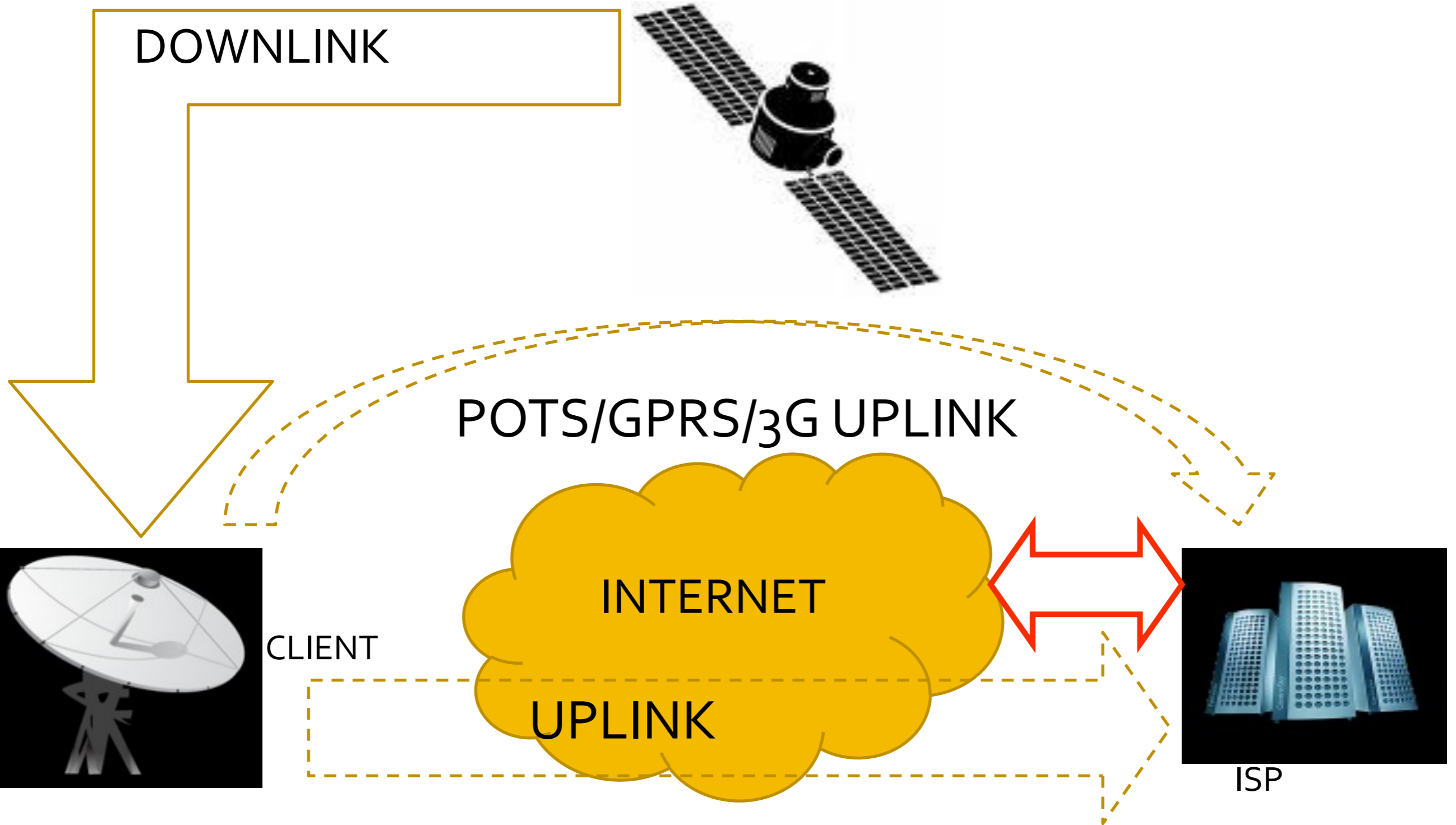
DVB Data - Satmodem



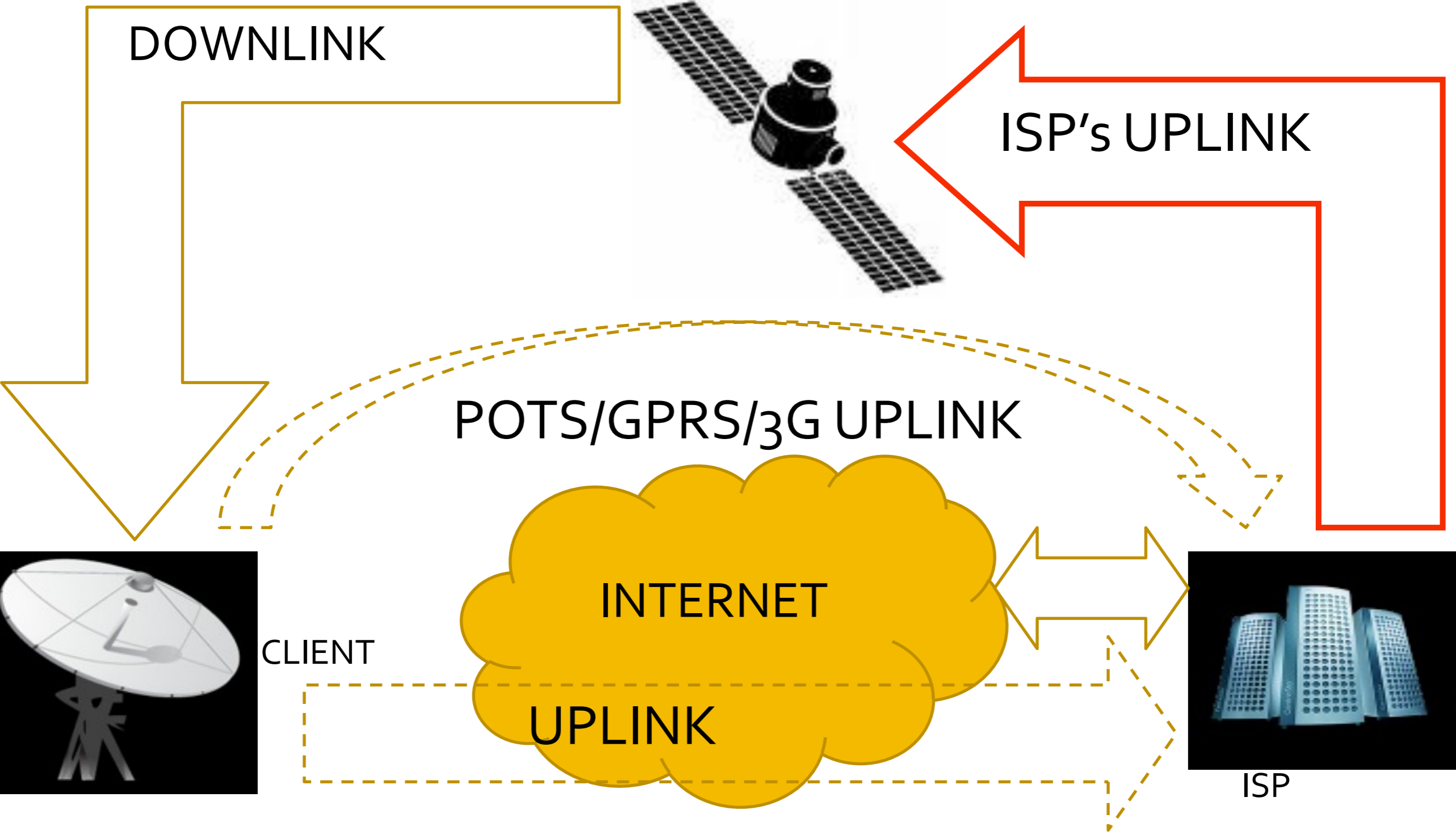
DVB Data - Satmodem



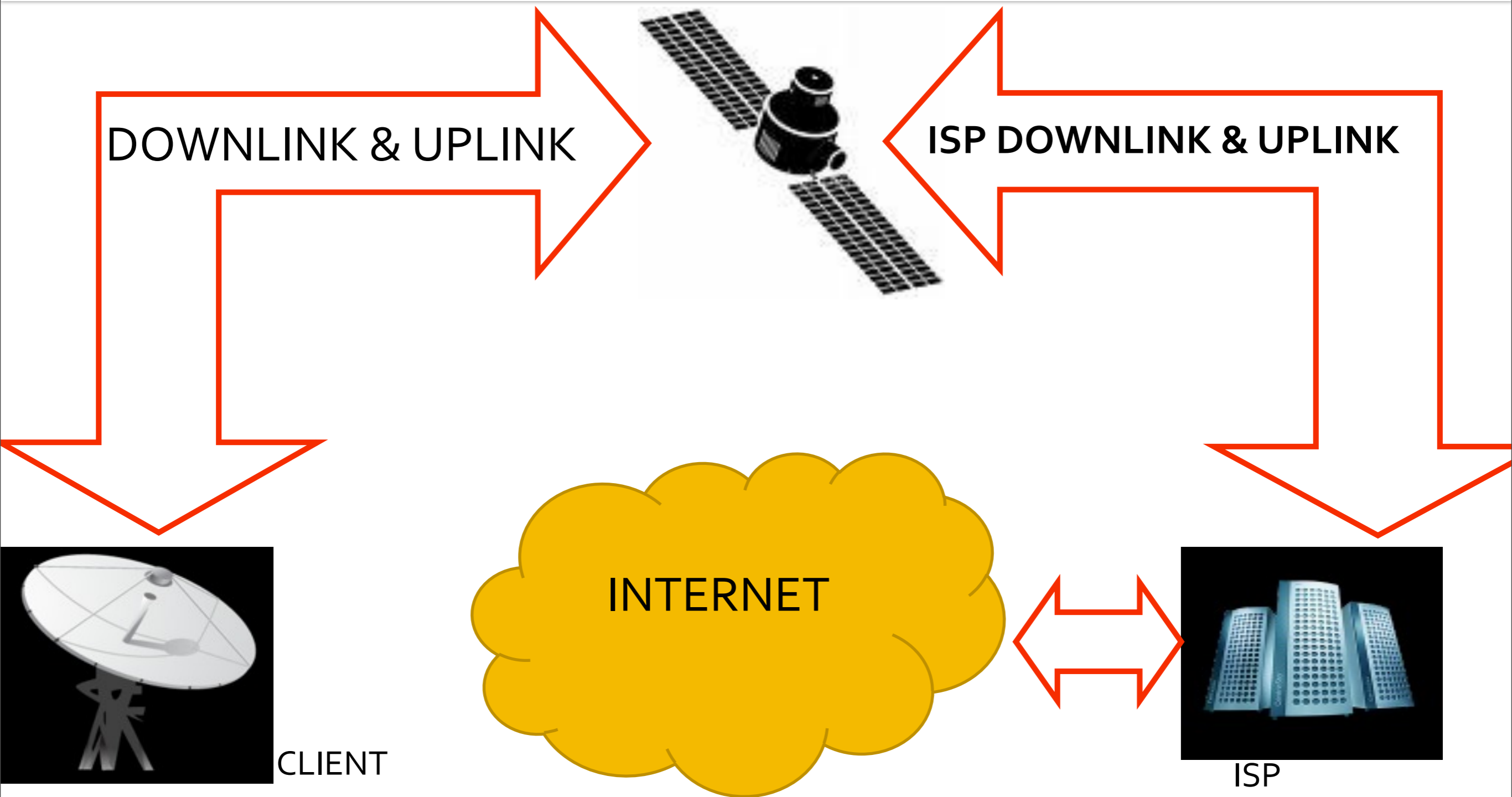
DVB Data - Satmodem



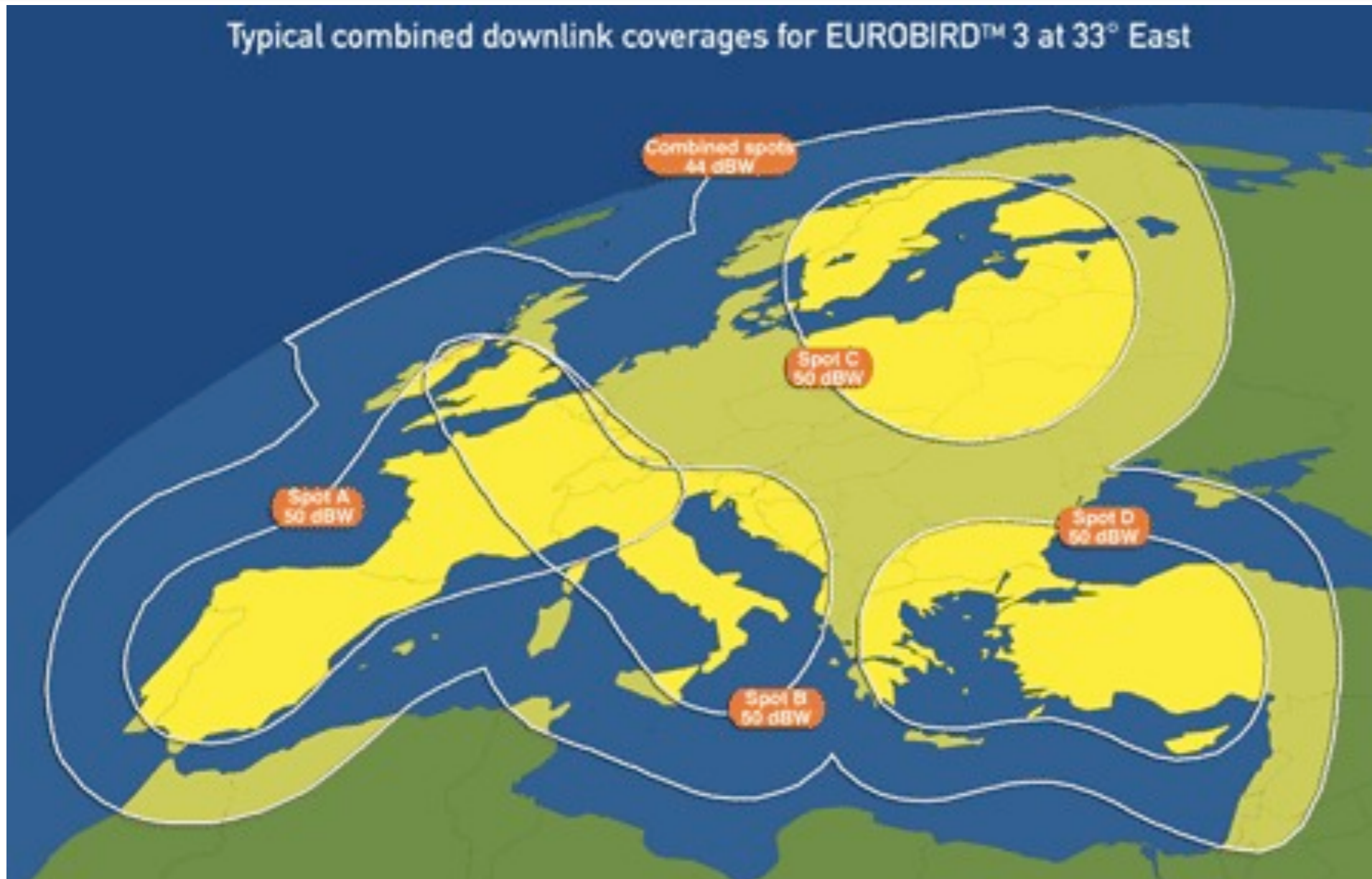
DVB Data - Satmodem



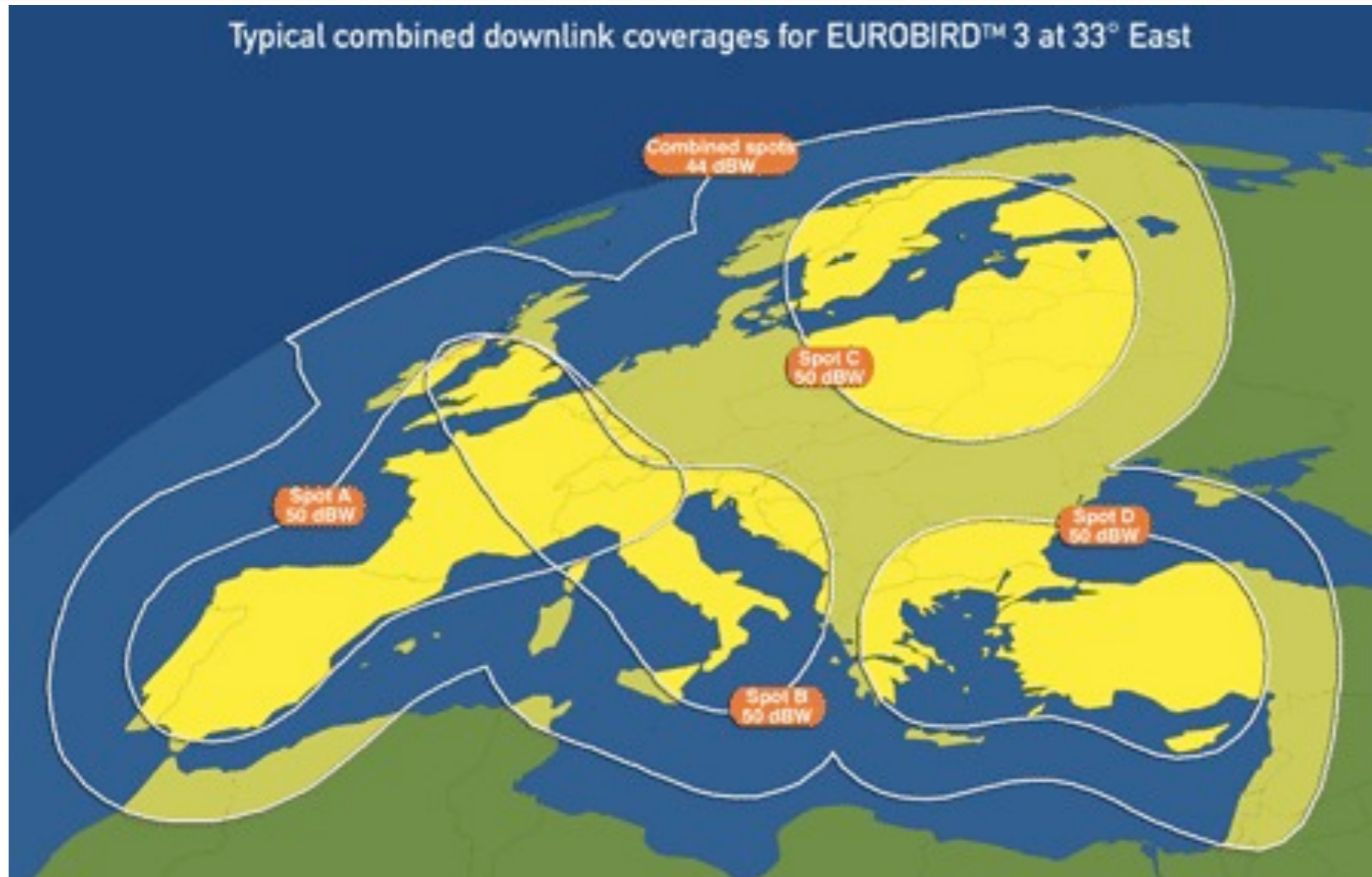
DVB Data - Astromodem



Satellite Coverage



Satellite Coverage



Anyone with coverage can SNIFF the DVB Data, and usually it is unencrypted.

DVB Data

- What do you need:
 - **Skystar 2 DVB Card**
 - linuxtv-dvb-apps
 - Wireshark
 - The antenna
 - Data to point it.

DVB Data

We bought it for 50€!!! from an
PayTV ex-"hacker" :P
(Including a set-top box that we
will not use)

DVB Data

Personalize Gift and Greeting Cards

Use your own photos and we'll deliver to their door

Buy Gift Cards

Home > Buy > Search results for "skystar 2" [Opt out of the new search experience](#)

Find in Search [\[Advanced Search \]](#)

Include title and description

Related Searches: [skystar](#), [skystar hd](#), [skystar usb](#), [dreambox](#), [skystar hd2](#)

Refine search

Categories

- Computers & Networking (2)
- PC Components (2)

In Computer Video & TV Cards

Price

\$ to \$



Brand

Installed Memory

All items Auctions only Buy It Now only

2 results found for **skystar 2** [\[Save this search \]](#)

View as [\[Customize view \]](#) Sort by

		Price	Time Left
	SkyStar 2 TV PCI Revision 2.6D for Satellite Internet P <i>Buy It Now</i>	\$41.00	6d 1h 4m
	SkyStar 2 TV PCI Revision 2.6D for Satellite Internet P 2 Bids	\$24.00	2d 0h 45m

2 items found in eBay Stores

Nuevo
 Usado
 Sin especificar
[Elegir más...](#)

Vendedor
[Especifica vendedores...](#)

Mis preferencias

ANTENA PARABOLICA SATYCON 80CM (KIT COMPLETO) Ubicación: España *¡Cómpralo ya!* 29,16 EUR +9,00 EUR 6d 2h 56m

LOCALIZADOR DE SATELITE PARA ANTENA PARABOLICA Ubicación: España *¡Cómpralo ya!* 12,00 EUR +8,00 EUR 68d 23h 19m

¿NO ENCUENTRAS LO QUE ESTÁS BUSCANDO?

DVB Data

Linux has the modules for this card by default,
we only need the tools to manage it:

linuxtv-dvb-apps

Sniffing Data

Once the antenna and the card is installed and linuxtv-dvb-apps compiled and installed, the process is:

- 1- Tune the DVB Card
- 2- Find a PID with data
- 3- Create an Ethernet interface associated to that PID

We can repeat 2 to 3 any times we want.

Sniffing Data

1- **Tune the DVB Card**

2- Find a PID with data

3- Create an Ethernet interface associated to that PID

Sniffing Data

Tune DVB Card

The tool we must use is *szap* and we need the transponder's parameters in a configuration file.

For example, for "Sirius-4 Nordic Beam":

```
# echo "sirius4N:12322:v:0:27500:0:0:0" >> channels.conf
```

<http://www.fastsatfinder.com/transponders.html>

Sniffing Data

We run szap with the channel configuration file and the transponder we want use (the configuration file can have more than one).

```
# szap -c channels.conf sirius4N
```

We must keep it running.

Sniffing Data

```
root@sathunter:~  
[root@sathunter ~]# szap -c channels.conf data1  
reading channels from file 'channels.conf'  
zapping to 1 'data1':  
sat 0, frequency = 12591 MHz V, symbolrate 30000000, vpid = 0x0000, apid = 0x000  
0  
using '/dev/dvb/adapter0/frontend0' and '/dev/dvb/adapter0/demux0'  
status 03 | signal 6aea | snr 6c99 | ber 00008856 | unc 00000000 |  
status 1f | signal b146 | snr d7ca | ber 00000af3 | unc 00000000 | FE_HAS_LOCK  
status 1f | signal b1b5 | snr d803 | ber 00000000 | unc 00000000 | FE_HAS_LOCK  
status 1f | signal b072 | snr d746 | ber 00000000 | unc 00000000 | FE_HAS_LOCK  
status 1f | signal b1ad | snr d782 | ber 00000000 | unc 00000000 | FE_HAS_LOCK  
status 1f | signal b12b | snr d7c7 | ber 00000000 | unc 00000000 | FE_HAS_LOCK  
status 1f | signal b181 | snr d776 | ber 00000000 | unc 00000000 | FE_HAS_LOCK  
status 1f | signal b164 | snr d7bb | ber 00000000 | unc 00000000 | FE_HAS_LOCK  
█
```

Sniffing Data

1- Tune the DVB Card

2- **Find a PID with data**

3- Create an Ethernet interface associated to that PID

Sniffing Data

- Find a PID

```
#dvbsnoop -s pidscan
```

Search for *data section* on results.

Sniffing Data

```
root@sathunter:~  
[root@sathunter ~]# dvbsnoop -s pidscan  
dvbsnoop V1.4.50 -- http://dvbsnoop.sourceforge.net/  
-----  
Transponder PID-Scan...  
-----  
PID found:    0 (0x0000) [SECTION: Program Association Table (PAT)]  
PID found:   16 (0x0010) [SECTION: Network Information Table (NIT) - actual network]  
PID found:   17 (0x0011) [SECTION: Service Description Table (SDT) - actual transport stream]  
PID found:   20 (0x0014) [SECTION: Time Date Table (TDT)]  
PID found: 1000 (0x03e8) [SECTION: Program Map Table (PMT)]  
PID found: 1001 (0x03e9) [SECTION: Program Map Table (PMT)]  
PID found: 1010 (0x03f2) [SECTION: User private]  
PID found: 1011 (0x03f3) [SECTION: User private]  
PID found: 1012 (0x03f4) [SECTION: User private]  
PID found: 1013 (0x03f5) [SECTION: User private]  
PID found: 1014 (0x03f6) [SECTION: Network Information Table (NIT) - other network]  
PID found: 1020 (0x03fc) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1021 (0x03fd) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1022 (0x03fe) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1023 (0x03ff) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1025 (0x0401) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1026 (0x0402) [SECTION: DSM-CC - private data section // DVB datagram]
```

Sniffing Data

1- Tune the DVB Card

2- Find a PID with data

3- **Create an Ethernet interface associated to that PID**

Sniffing Data

- Create an interface associated to a PID

```
#dvbnet -a <adapter number> -p <PID>
```

- Activate it

```
#ifconfig dvbo_<iface number> up
```

Sniffing Data

```
root@sathunter:~  
[root@sathunter ~]# dvbnet -a 0 -p 1022  
  
DVB Network Interface Manager  
Version 1.1.0-TVF (Build vie mar 06 12:54:43 2009)  
Copyright (C) 2003, TV Files S.p.A  
  
Device: /dev/dvb/adapter0/net0  
Status: device dvb0_0 for pid 1022 created successfully.  
[root@sathunter ~]# ifconfig dvb0_0 up  
[root@sathunter ~]# ifconfig dvb0_0  
dvb0_0      Link encap:Ethernet  HWaddr 00:D0:D7:0C:67:8D  
            inet6 addr: fe80::2d0:d7ff:fe0c:678d/64 Scope:Link  
            UP BROADCAST RUNNING NOARP MULTICAST  MTU:4096  Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)  
            Base address:0x3fe  
  
[root@sathunter ~]# █
```


Sniffing Data

Back to de pidscan results

```
root@sathunter:~  
[root@sathunter ~]# dvbsnoop -s pidscan  
dvbsnoop V1.4.50 -- http://dvbsnoop.sourceforge.net/  
  
-----  
Transponder PID-Scan...  
-----  
PID found:    0 (0x0000) [SECTION: Program Association Table (PAT)]  
PID found:   16 (0x0010) [SECTION: Network Information Table (NIT) - actual network]  
PID found:   17 (0x0011) [SECTION: Service Description Table (SDT) - actual transport stream]  
PID found:   20 (0x0014) [SECTION: Time Date Table (TDT)]  
PID found: 1000 (0x03e8) [SECTION: Program Map Table (PMT)]  
PID found: 1001 (0x03e9) [SECTION: Program Map Table (PMT)]  
PID found: 1010 (0x03f2) [SECTION: User private]  
PID found: 1011 (0x03f3) [SECTION: User private]  
PID found: 1012 (0x03f4) [SECTION: User private]  
PID found: 1013 (0x03f5) [SECTION: User private]  
PID found: 1014 (0x03f6) [SECTION: Network Information Table (NIT) - other network]  
PID found: 1020 (0x03fc) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1021 (0x03fd) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1022 (0x03fe) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1023 (0x03ff) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1025 (0x0401) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 1026 (0x0402) [SECTION: DSM-CC - private data section // DVB datagram]
```

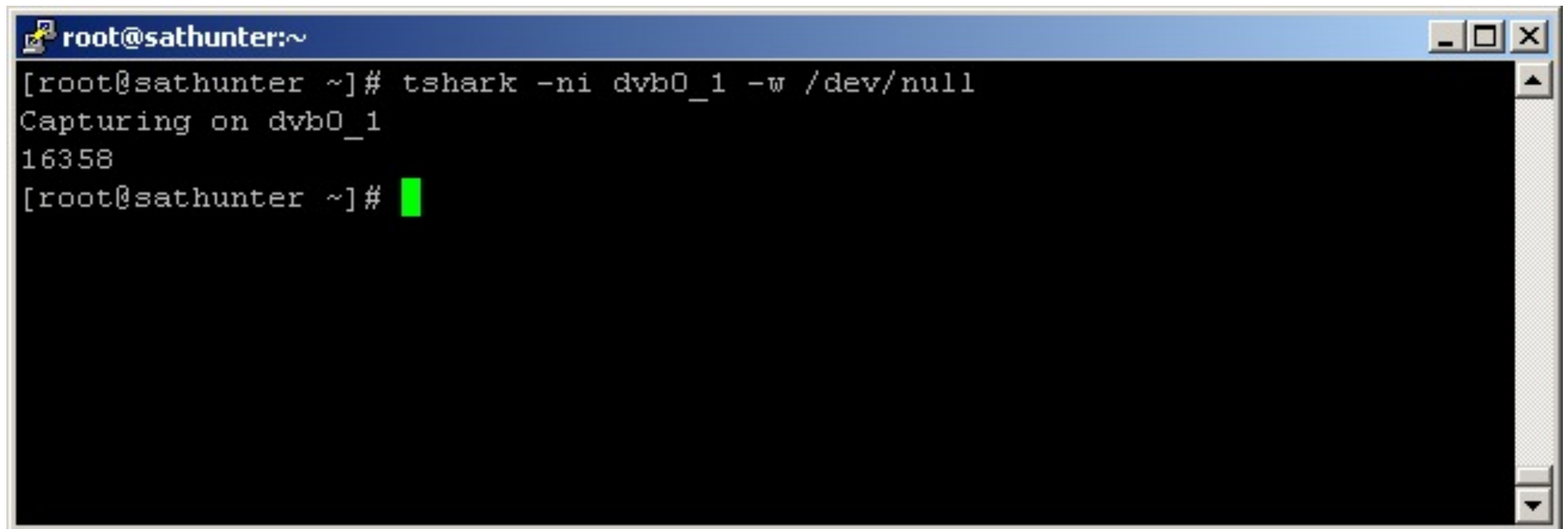
Sniffing Data

Create another interface

```
root@sathunter:~  
[root@sathunter ~]# dvbnet -a 0 -p 1021  
  
DVB Network Interface Manager  
Version 1.1.0-TVF (Build vie mar 06 12:54:43 2009)  
Copyright (C) 2003, TV Files S.p.A  
  
Device: /dev/dvb/adapter0/net0  
Status: device dvb0_1 for pid 1021 created successfully.  
[root@sathunter ~]# ifconfig dvb0_1 up  
[root@sathunter ~]# ifconfig dvb0_1  
dvb0_1      Link encap:Ethernet  HWaddr 00:D0:D7:0C:67:8D  
            inet6 addr: fe80::2d0:d7ff:fe0c:678d/64 Scope:Link  
            UP BROADCAST RUNNING NOARP MULTICAST  MTU:4096  Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)  
            Base address:0x3fd
```

Sniffing Data

Wireshark is our friend

A terminal window titled 'root@sathunter:~' with standard window controls. The terminal shows the execution of the command 'tshark -ni dvb0_1 -w /dev/null'. The output indicates that capturing has started on the 'dvb0_1' interface and that 16358 packets have been captured. The prompt is currently blocked by a green cursor.

```
root@sathunter:~  
[root@sathunter ~]# tshark -ni dvb0_1 -w /dev/null  
Capturing on dvb0_1  
16358  
[root@sathunter ~]#
```

16358 packets in 10 seconds

Sniffing data

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	17122	11988350	7,650	0	0	0,000
Ethernet	100,00%	17122	11988350	7,650	0	0	0,000
Internet Protocol	100,00%	17122	11988350	7,650	0	0	0,000
Generic Routing Encapsulation	13,41%	2296	1100945	0,703	7	294	0,000
User Datagram Protocol	7,67%	1313	489998	0,313	0	0	0,000
Domain Name Service	0,71%	121	23855	0,015	120	23750	0,015
Data	3,84%	658	286093	0,183	658	286093	0,183
UDP Encapsulation of IPsec Packets	2,98%	510	177409	0,113	1	43	0,000
eDonkey Protocol	0,02%	4	305	0,000	4	305	0,000
Simple Network Management Protocol	0,04%	7	700	0,000	7	700	0,000
Internet Security Association and Key Management Protocol	0,05%	9	1271	0,001	9	1271	0,001
Hypertext Transfer Protocol	0,01%	1	95	0,000	1	95	0,000
Network Time Protocol	0,02%	3	270	0,000	3	270	0,000
Transmission Control Protocol	64,99%	11128	8923504	5,694	4796	1517444	0,968
Hypertext Transfer Protocol	25,23%	4320	6194417	3,953	4165	6093498	3,888
Data	7,31%	1251	970027	0,619	1251	970027	0,619
Simple Mail Transfer Protocol	1,27%	218	28045	0,018	218	28045	0,018
MSN Messenger Service	0,19%	32	6636	0,004	32	6636	0,004
Secure Socket Layer	1,43%	244	132109	0,084	243	131519	0,084
TPKT - ISO on TCP - RFC1006	0,22%	37	2451	0,002	37	2451	0,002
SSH Protocol	0,22%	38	6256	0,004	38	6256	0,004
Financial Information eXchange Protocol	0,05%	8	1157	0,001	6	558	0,000
Post Office Protocol	0,66%	113	59548	0,038	113	59548	0,038
Modbus/TCP	0,18%	30	1980	0,001	30	1980	0,001
Virtual Network Computing	0,15%	26	1616	0,001	0	0	0,000
MySQL Protocol	0,01%	2	224	0,000	2	224	0,000
Firebird SQL Database Remote Protocol	0,07%	12	1520	0,001	12	1520	0,001
Point-to-Point Tunneling Protocol	0,01%	1	74	0,000	1	74	0,000
Data	0,19%	33	1914	0,001	33	1914	0,001
Encapsulating Security Payload	13,33%	2283	1466738	0,936	2283	1466738	0,936
Internet Control Message Protocol	0,40%	69	5251	0,003	69	5251	0,003

Sniffing Data

- Malicious users can:
 - Catch passwords.
 - Catch cookies and get into authenticated HTTP sessions.
 - Read emails
 - Catch sensitive files
 - Do traffic analysis
 - Etc

We can have more than one PID assigned to an interface, this will be very useful.

Sniffing Data

Reminder:

In satellite communications we have two scenarios:

A- Satmodem, Only Downlink via Satellite

B- Astromodem, Both uplink and downlink via Satellite.

Sniffing Data

In Satmodem scenario we can only sniff the downloaded data. We can only sniff one direction in a connection.

Sniffing data

In an astromodem scenario and depending the infraestructure configuration. We can find a PID used to send the uploaded packets to the main ISP to be routed to Internet so we can sniff all the traffic, uploaded and downloaded data.

(???)

Wardriving? no way...



Wardriving? no way...



SatDriving

Active Attacks

For this chapter, we will suppose all the time that we are in a Satmodem scenario so we can't sniff uploaded data of the client with the Satlink.

Some “old” Stuff in Sat hacking

- DNS Spoofing
- TCP hijacking
- Attacking GRE

DNS Spoofing

DNS Spoofing is the art of making a DNS entry to point to an another IP than it would be supposed to point to. (SecureSphere)

DNS Spoofing

- Data we need to perform this attack
 - DNS Request ID
 - Source Port
 - Source IP
 - Destination IP
 - Name/IP asking for

DNS Spoofing

- It's trivial to see that if we sniff a DNS request we have all that information and we can spoof the answer.
- Many tools around do this job, the only thing we also need is to be faster than the real DNS server (jizz).

DNS Spoofing

- Why is this attack important?
 - Phishing attacks
 - With this attack, uplink sniff can be possible
 - Rogue WPAD service
 - Sslstrip can be use to avoid SSL connections.

Some “old” Stuff in Sat hacking

- DNS Spoofing
- TCP hijacking
- Attacking GRE

TCP hijacking

TCP session hijacking is when an attacker takes over a **TCP** session between two machines.
(ISS)

TCP hijacking

A

1 Seq=S₁ ACK=A₁ Datalen=L₁



2 Seq=A₁ ACK=S₁+L₁ Datalen=L₂

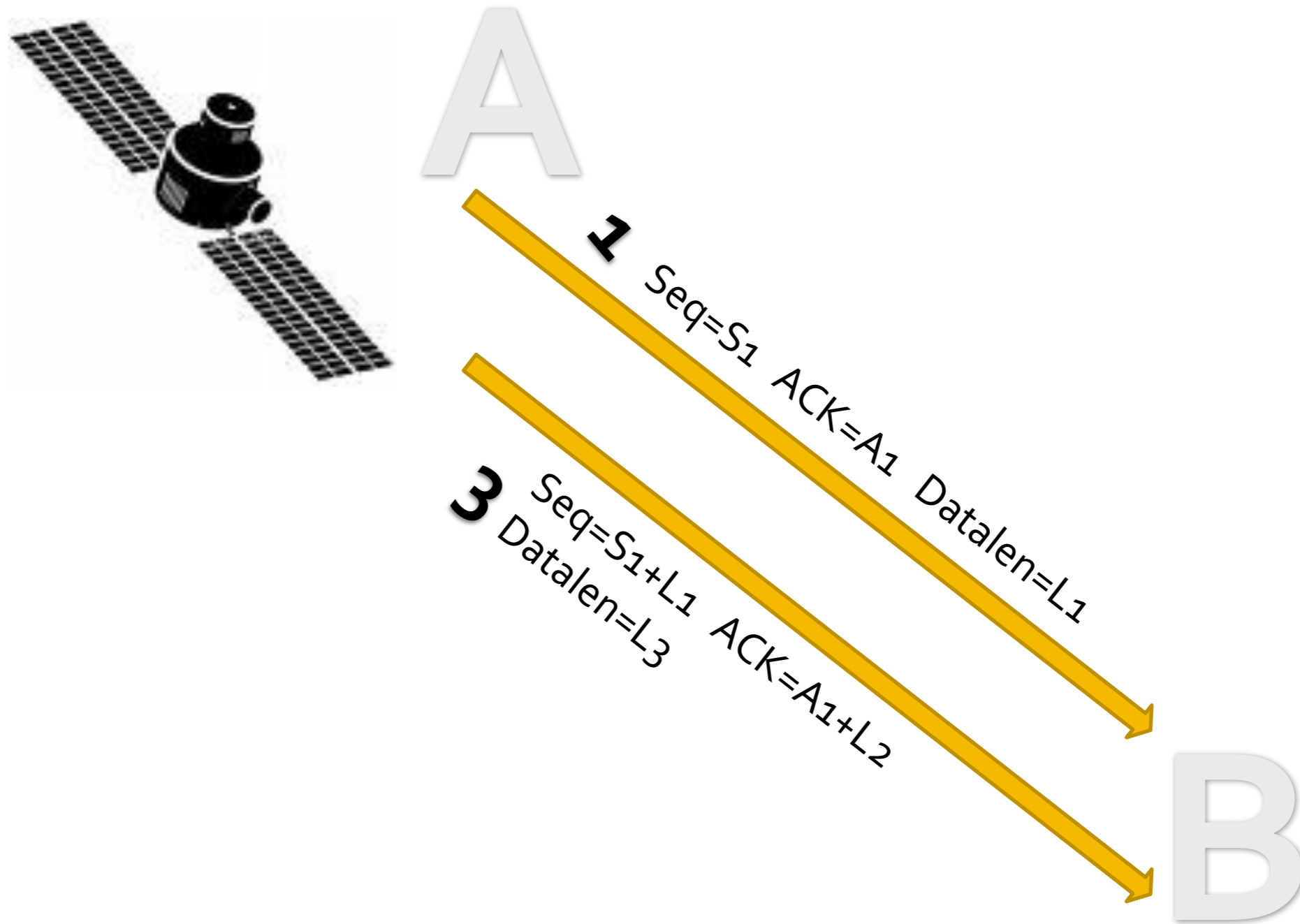


3 Seq=S₁+L₁ ACK=A₁+L₂ Datalen=L₃

B

If we sniff **1** we can predict Seq and Ack of **2** and we can send the payload we want in **2**

TCP Hijacking



TCP Hijacking

- Initially we can only have a false connection with A.
- In certain circumstances, we can make this attack with B, when L2 is predictable.
- Some tools for doing this:
 - Hunt
 - Shijack
 - Scapy

Some “old” Stuff in Sat hacking

- DNS Spoofing
- TCP hijacking
- **Attacking GRE**

Attacking GRE

- Generic Routing Encapsulation
- Point to point tunneling protocol
- 13% of Satellite's data traffic in our transponder is GRE

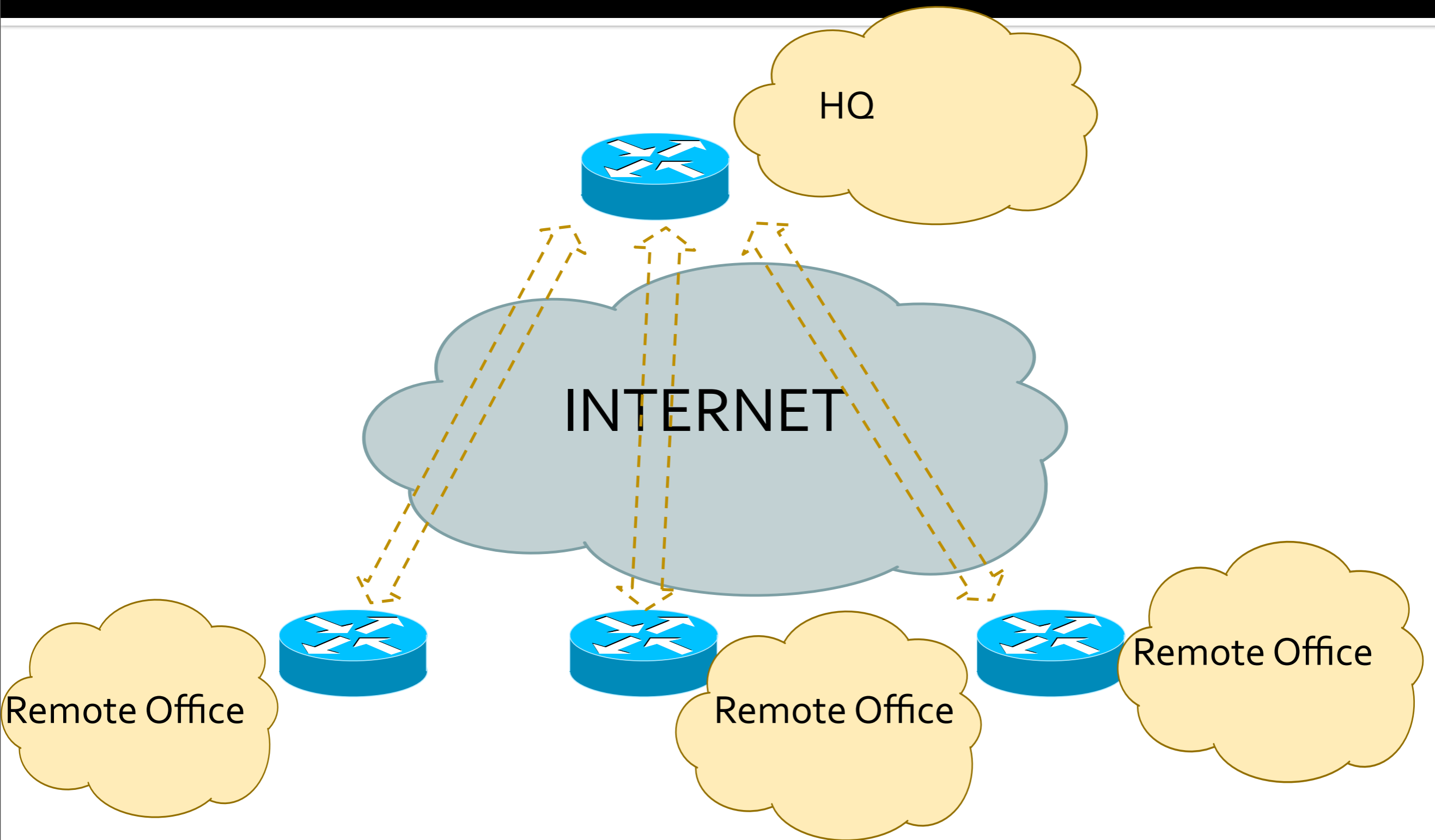
Attacking GRE

This chapter is based in Phenoelit's discussion paper written by FX applied to satellite scenario.

Original paper:

<http://www.phenoelit-us.org/irpas/gre.html>

Attacking GRE



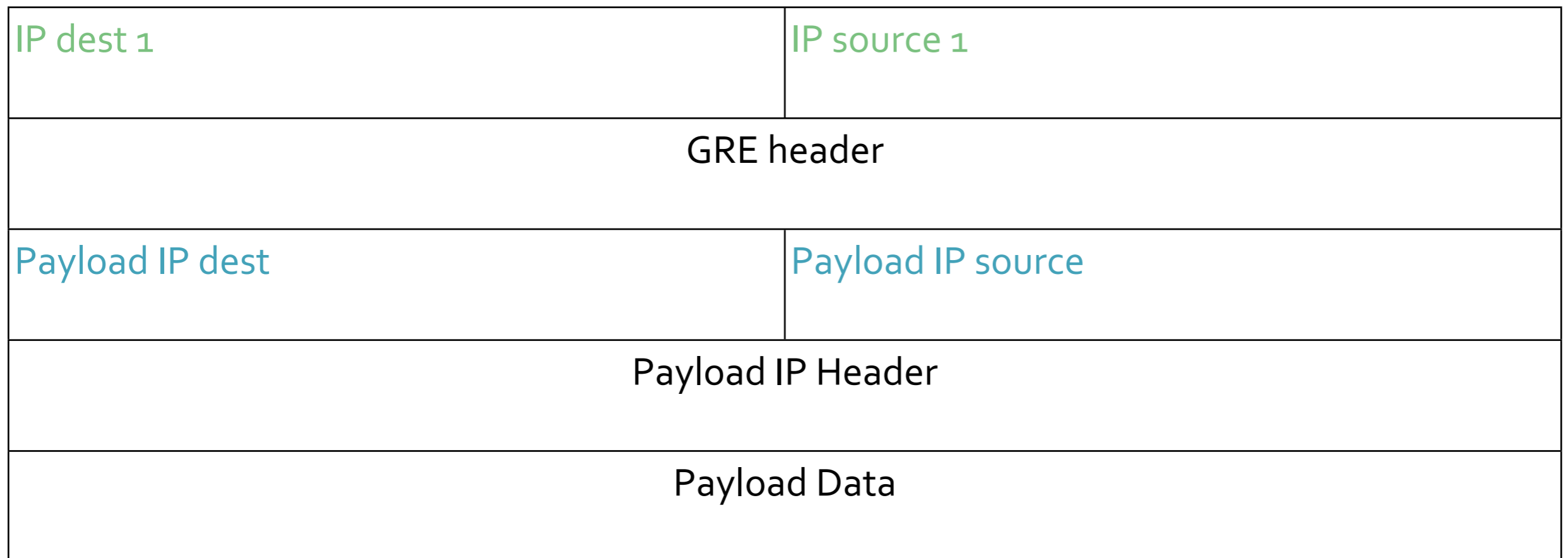
Attacking GRE

Find a target:

```
#tshark -ni dvbo_0 -R gre -w capture.cap
```

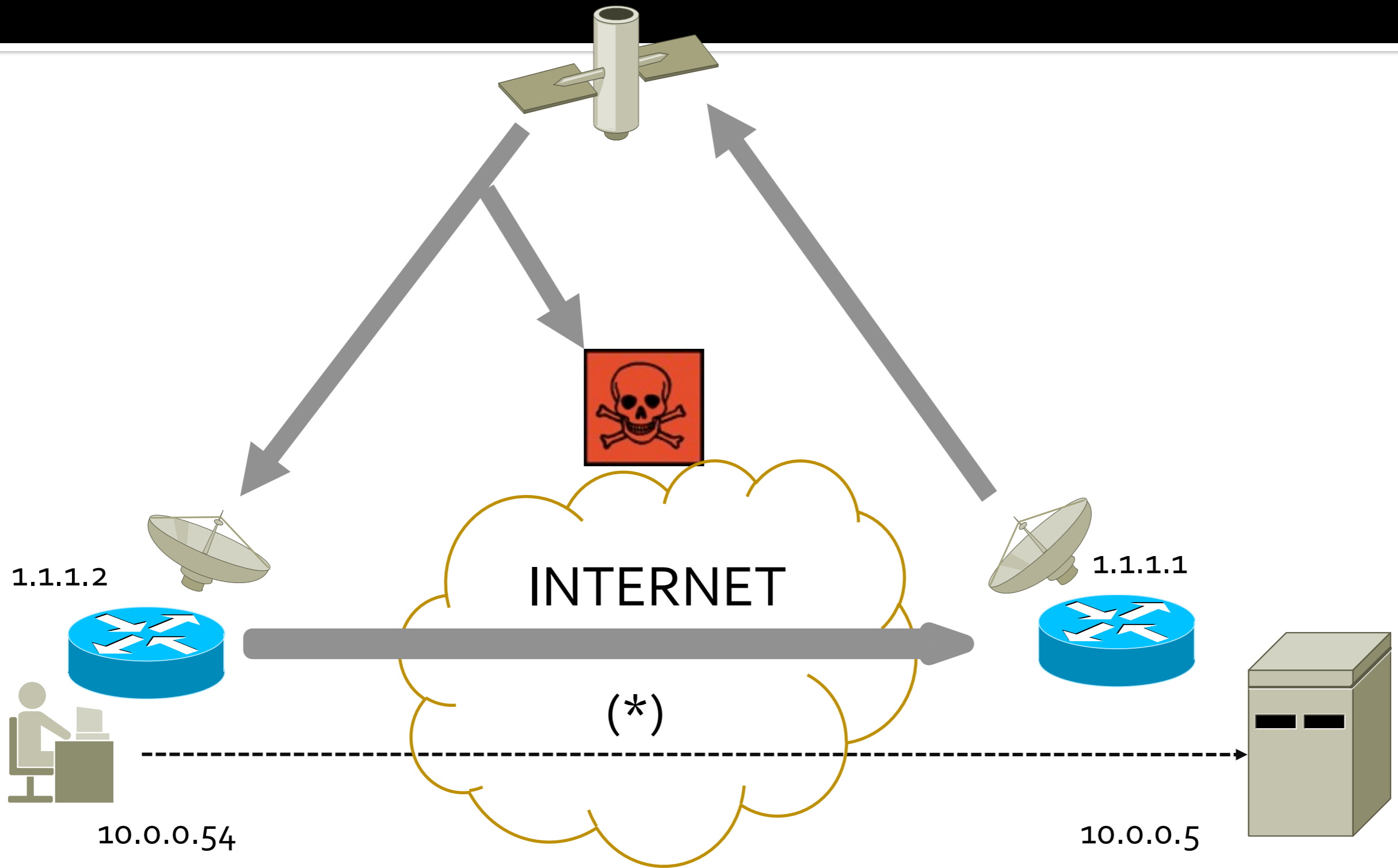
Attacking GRE

GRE Packet



- IP **source 1** must be Internet reachable **IP dest 1** and
- The **payload's IPs** usually are internal.

Attacking GRE

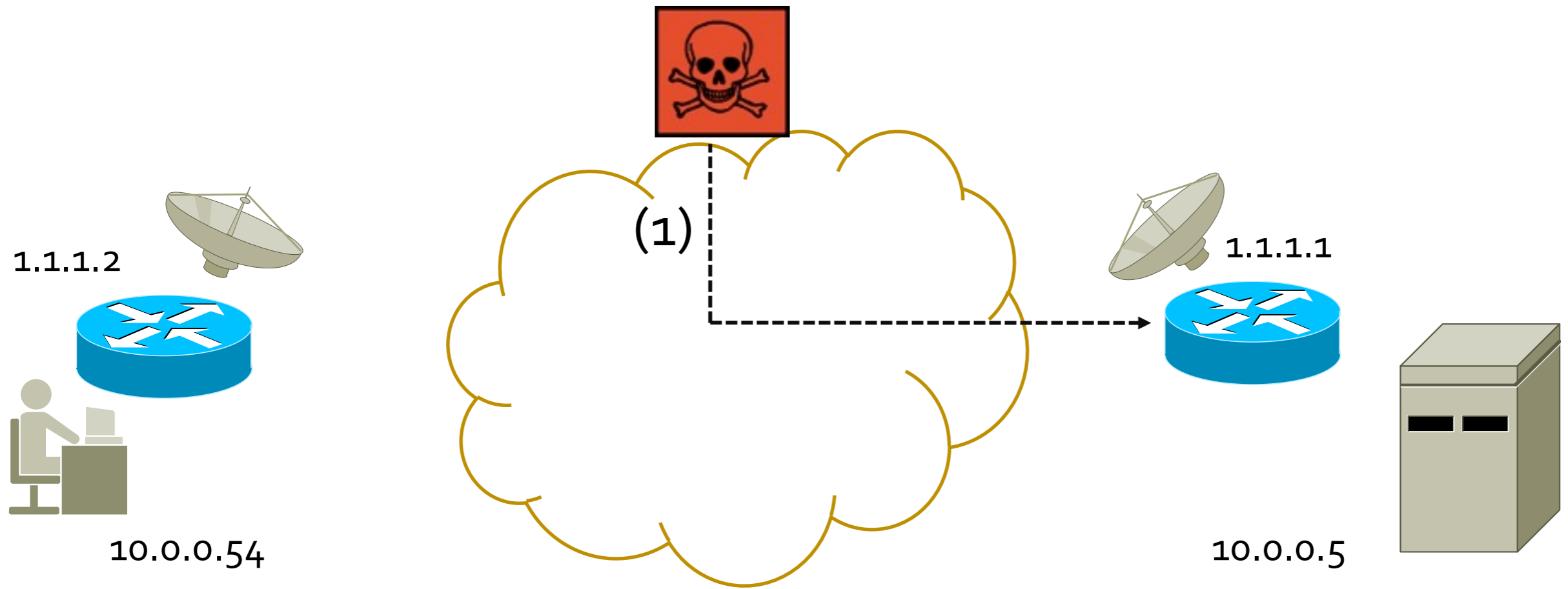
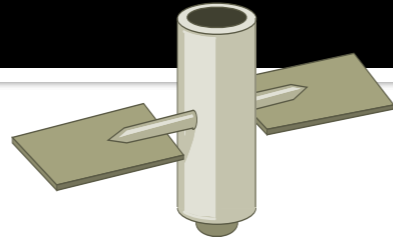


Attacking GRE

(*) GRE Packet

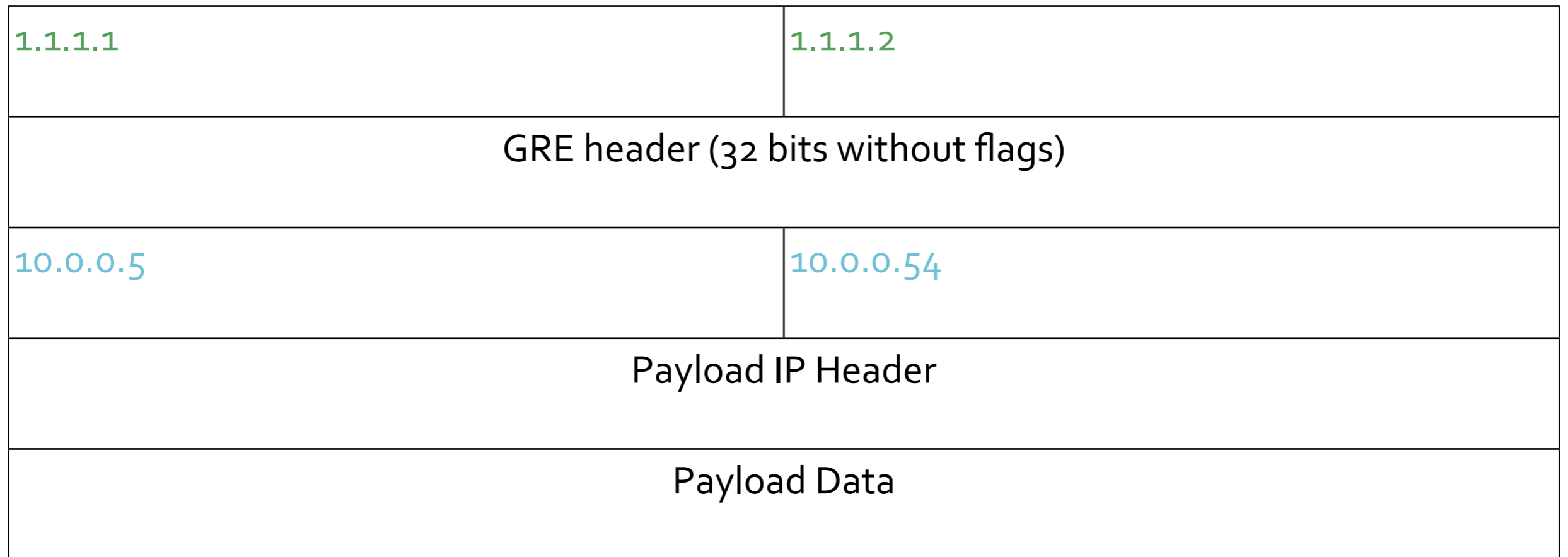
1.1.1.1	1.1.1.2
GRE header (32 bits without flags)	
10.0.0.5	10.0.0.54
Payload IP Header	
Payload Data	

Attacking GRE

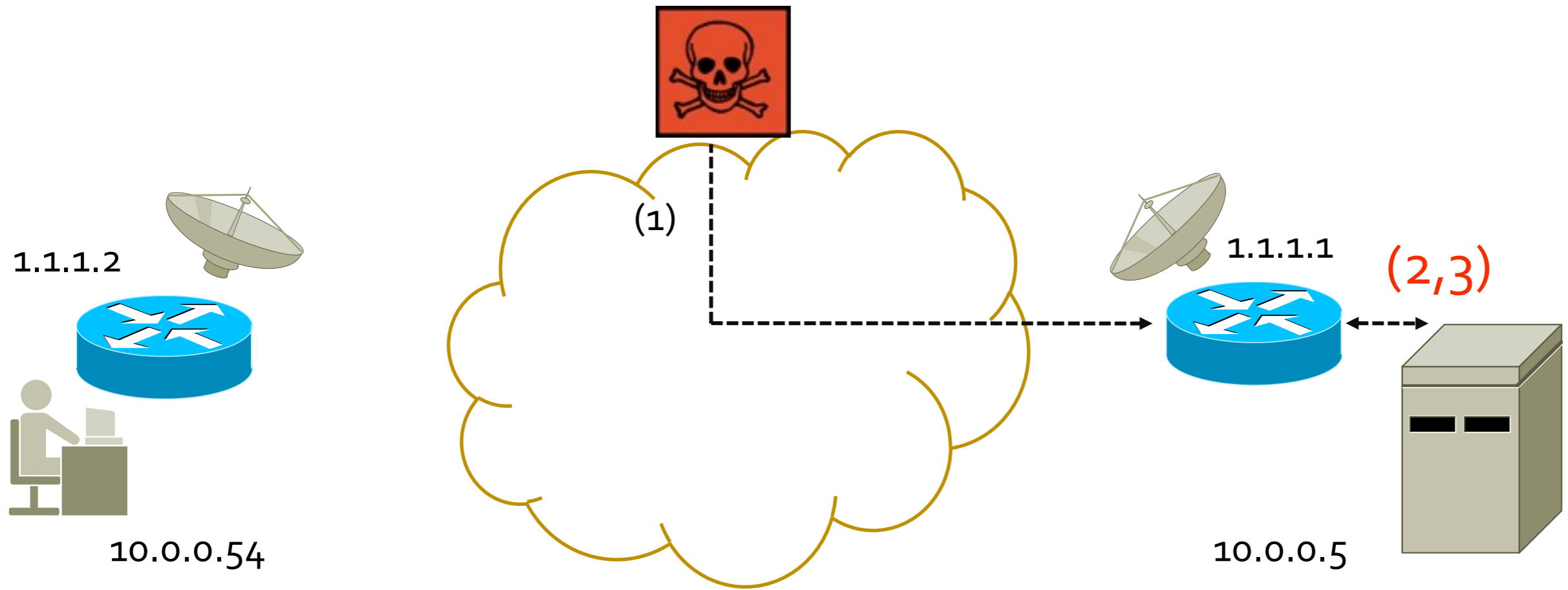
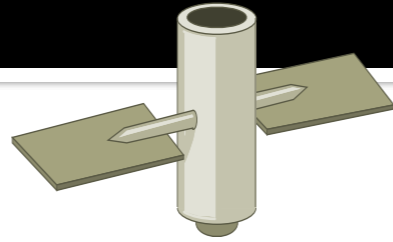


Attacking GRE

(1) GRE Packet

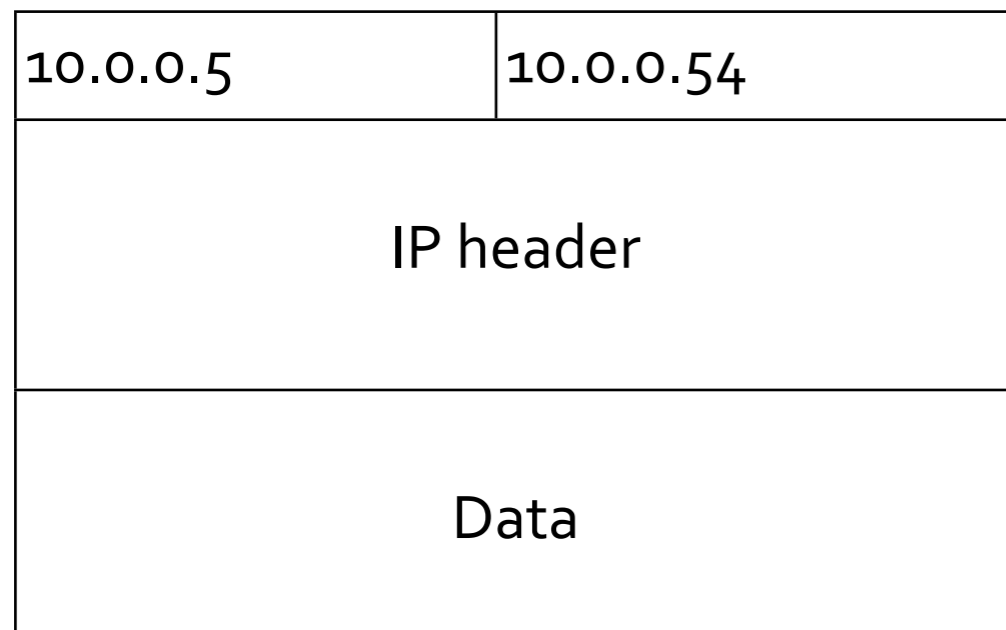


Attacking GRE

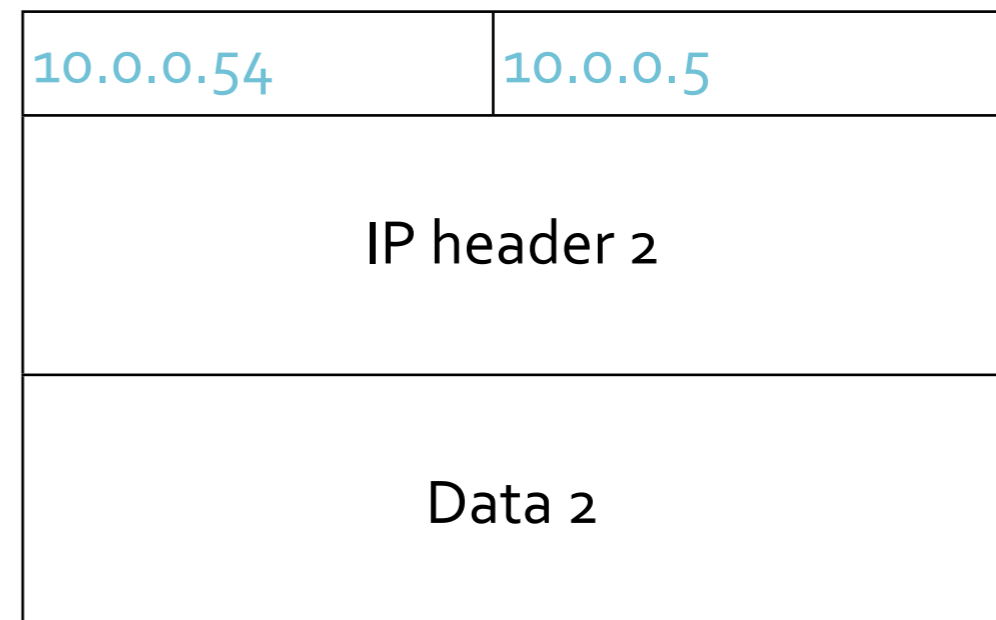


Attacking GRE

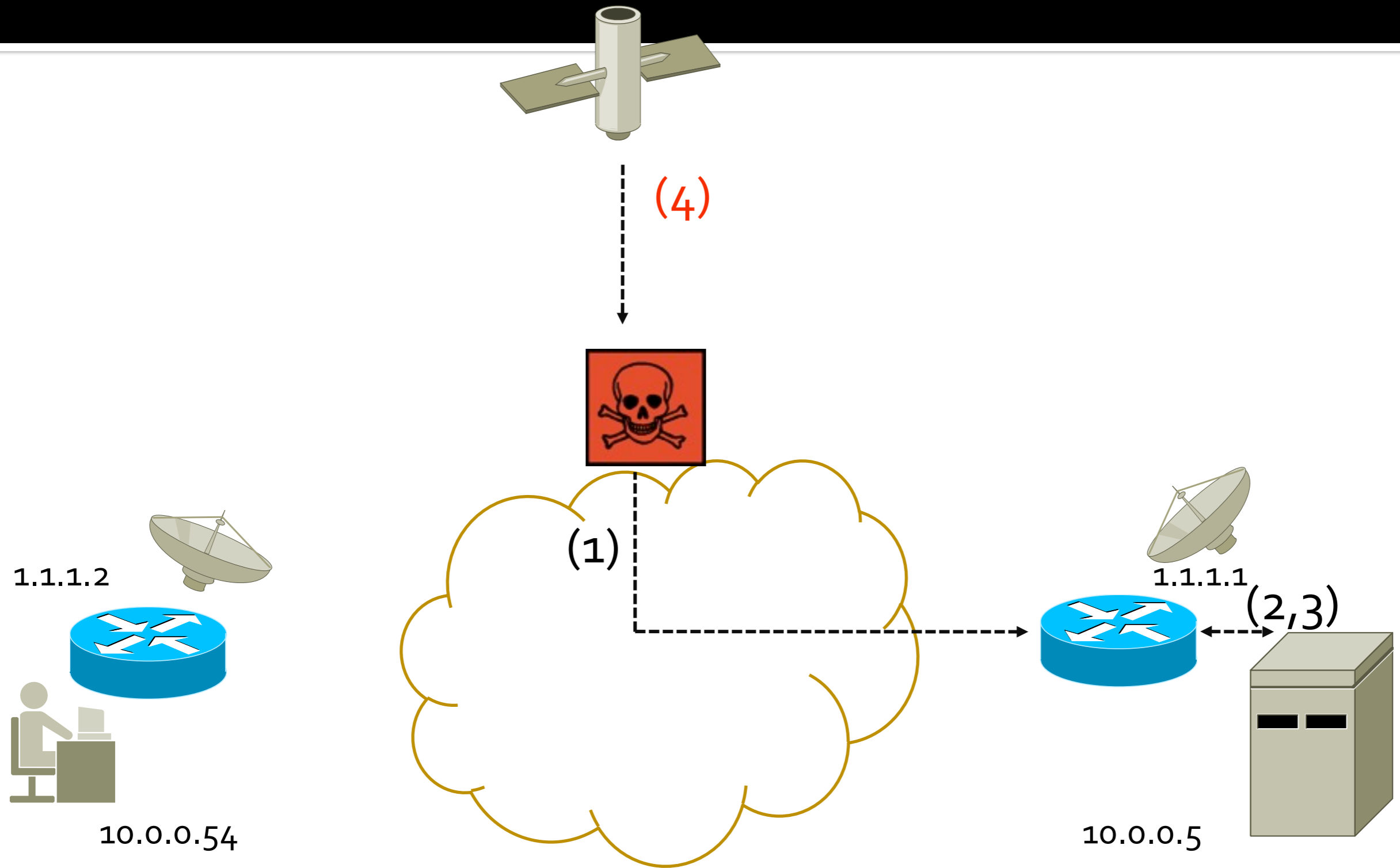
(2) IP Packet



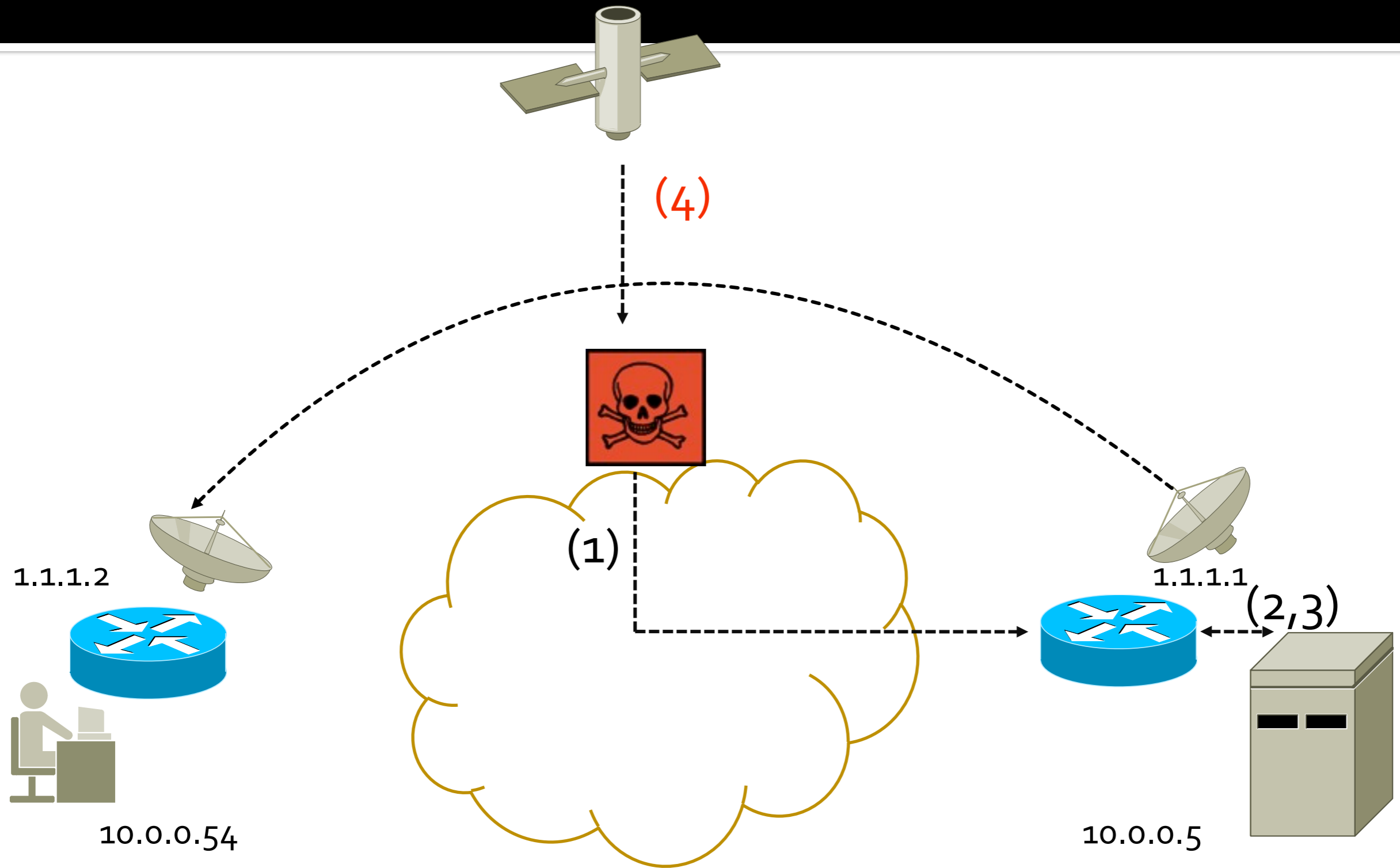
(3) IP Packet



Attacking GRE

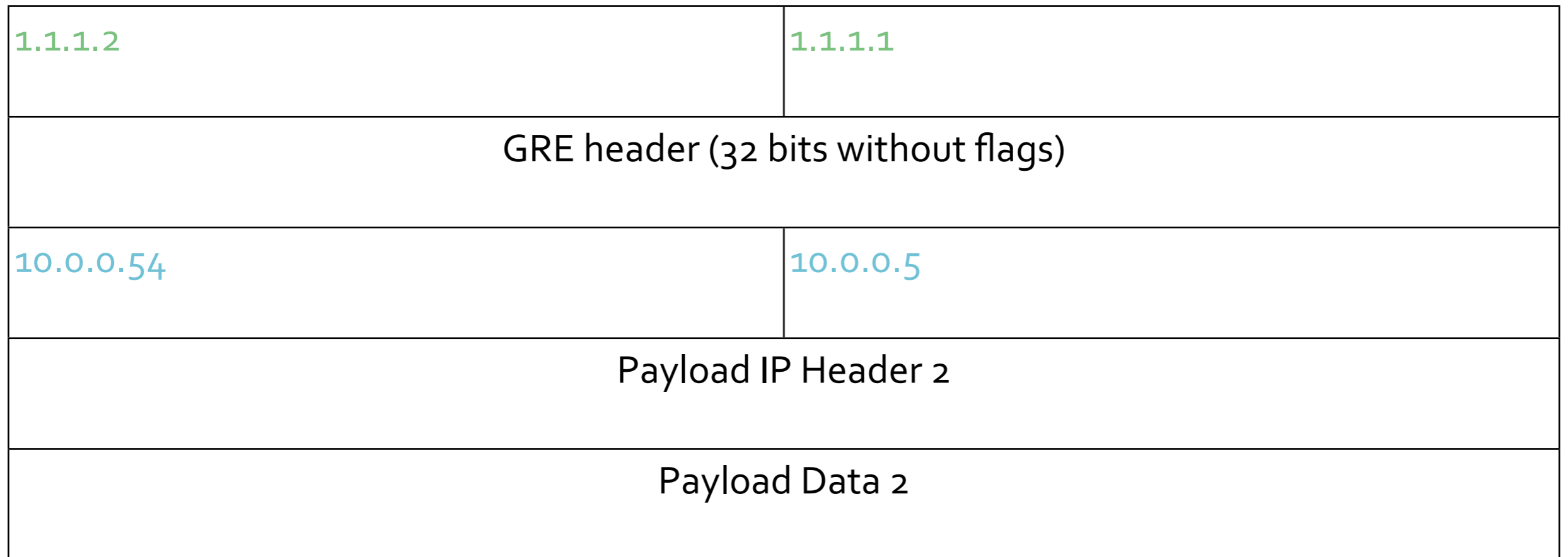


Attacking GRE



Attacking GRE

(4) GRE Packet



Attacking GRE

In Phenoelit's attack payload's IP source is our public IP. This attack lacks when that IP isn't reachable from the internal LAN and you can be logged.

I use internal IP because we can sniff the responses.

To better improve the attack, find a internal IP not used.

HTSNACBT Attack

How
To
Scan
NSA
And
Cannot
Be
Traced

HTSNACBT Attack

We can spoof (putting a satellite's routable source IP) a *SYN packet* with any destination IP and *TCP* port, and we can sniff the responses.

We can analyze the responses.

HTSNACBT Attack

OR... We can configure our linux box like a satellite connected host.

VERY EASY!!!

HTSNACBT Attack

- What we need:
 - An internet connection (Let's use it as **uplink**) with any technology which let you spoof your source address.
 - A receiver, a card.....

HTSNACBT Attack

- Let's rock!
 - Find a satellite IP not used, I ping IPs next to another sniffable satellite IP to find a non responding IP. We must sniff our ping with the DVB Card (you must save the packets).
 - This will be our IP!

HTSNACBT Attack

- Configure Linux to use it.

```
root@sathunter:~  
[root@sathunter ~]# arp -n  
Address          HWtype  HWaddress      Flags Mask    Iface  
192.168.1.50     ether   00:13:02:49:23:73  C           eth0  
[REDACTED] 2     ether   [REDACTED] 3           eth2  
[REDACTED]     ether   [REDACTED]           eth2  
8[REDACTED].1    ether   00:05:[REDACTED]:01  C           eth2  
[root@sathunter ~]#
```

We need our router's MAC

HTSNACBT Attack

Configure our dvb interface to receive this IP (I suppose that you have configured the PID...)

The IP is the one we have selected and in the ICMP scan, we must get the destination MAC sniffed.

HTSNACBT Attack

```
root@sathunter:~  
[root@sathunter ~]# tshark -Vnr sat_captured.cap | less  
Frame 1 (54 bytes on wire, 54 bytes captured)  
  Arrival Time: Mar 25, 2009 01:58:47.220140000  
  [Time delta from previous captured frame: 0.000000000 seconds]  
  [Time delta from previous displayed frame: 0.000000000 seconds]  
  [Time since reference or first frame: 0.000000000 seconds]  
  Frame Number: 1  
  Frame Length: 54 bytes  
  Capture Length: 54 bytes  
  [Frame is marked: False]  
  [Protocols in frame: eth:ip:tcp]  
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:6[REDACTED] (00:6[REDACTED]b)  
  Destination: 00:6[REDACTED] (00:6[REDACTED]b)  
  Address: 00:6[REDACTED] (00:6[REDACTED]b)  
  ....0. .... = IG bit: Individual address (unicast)  
  ....0. .... = LG bit: Globally unique address (factory default)  
  Source: 00:00:00:00:00:00 (00:00:00:00:00:00)  
  Address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
  ....0. .... = IG bit: Individual address (unicast)  
  ....0. .... = LG bit: Globally unique address (factory default)  
  Type: IP (0x0800)  
Internet Protocol, Src: 8[REDACTED]4 (8[REDACTED]4), Dst: [REDACTED]73 ([REDACTED]73)  
  Version: 4  
  Header length: 20 bytes  
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    ....0. = ECN-Capable Transport (ECT): 0  
    ....0. = ECN-CE: 0  
  Total Length: 40  
  Identification: 0x9cb4 (40116)  
  Flags: 0x00  
    0... = Reserved bit: Not set
```

Here we get the MAC address we must configure in our DVB interface

HTSNACBT Attack

```
root@sathunter:~  
[root@sathunter ~]# ifconfig dvb0_0 [REDACTED]73 netmask 255.255.255.255 hw ether 00:6[REDACTED]b  
[root@sathunter ~]# █
```

I use netmask /32 to avoid routing problems

HTSNACBT Attack

Now we can configure our Internet interface with the same IP and configure a default route with a false router setting this one with a static MAC (our real router's MAC).

HTSNACBT Attack

```
root@sathunter:~  
[root@sathunter ~]# ifconfig eth2 [REDACTED]73 netmask 255.255.255.252  
[root@sathunter ~]# route add default gw [REDACTED]74 dev eth2  
[root@sathunter ~]# arp -s [REDACTED]74 00:05:[REDACTED]01  
[root@sathunter ~]# █
```

HTSNACBT Attack

IT WORKS!

```
root@sathunter:~  
[root@sathunter ~]# ping www.nsa.gov  
PING www.nsa.gov (12.110.110.204) 56(84) bytes of data.  
  
--- www.nsa.gov ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 2999ms  
  
[root@sathunter ~]# ping www.google.es  
PING www.l.google.com (209.85.229.99) 56(84) bytes of data.  
64 bytes from ww-in-f99.google.com (209.85.229.99): icmp_seq=1 ttl=237 time=69.0 ms  
64 bytes from ww-in-f99.google.com (209.85.229.99): icmp_seq=2 ttl=237 time=59.6 ms  
  
--- www.l.google.com ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/mdev = 59.685/64.360/69.036/4.682 ms  
[root@sathunter ~]# █
```

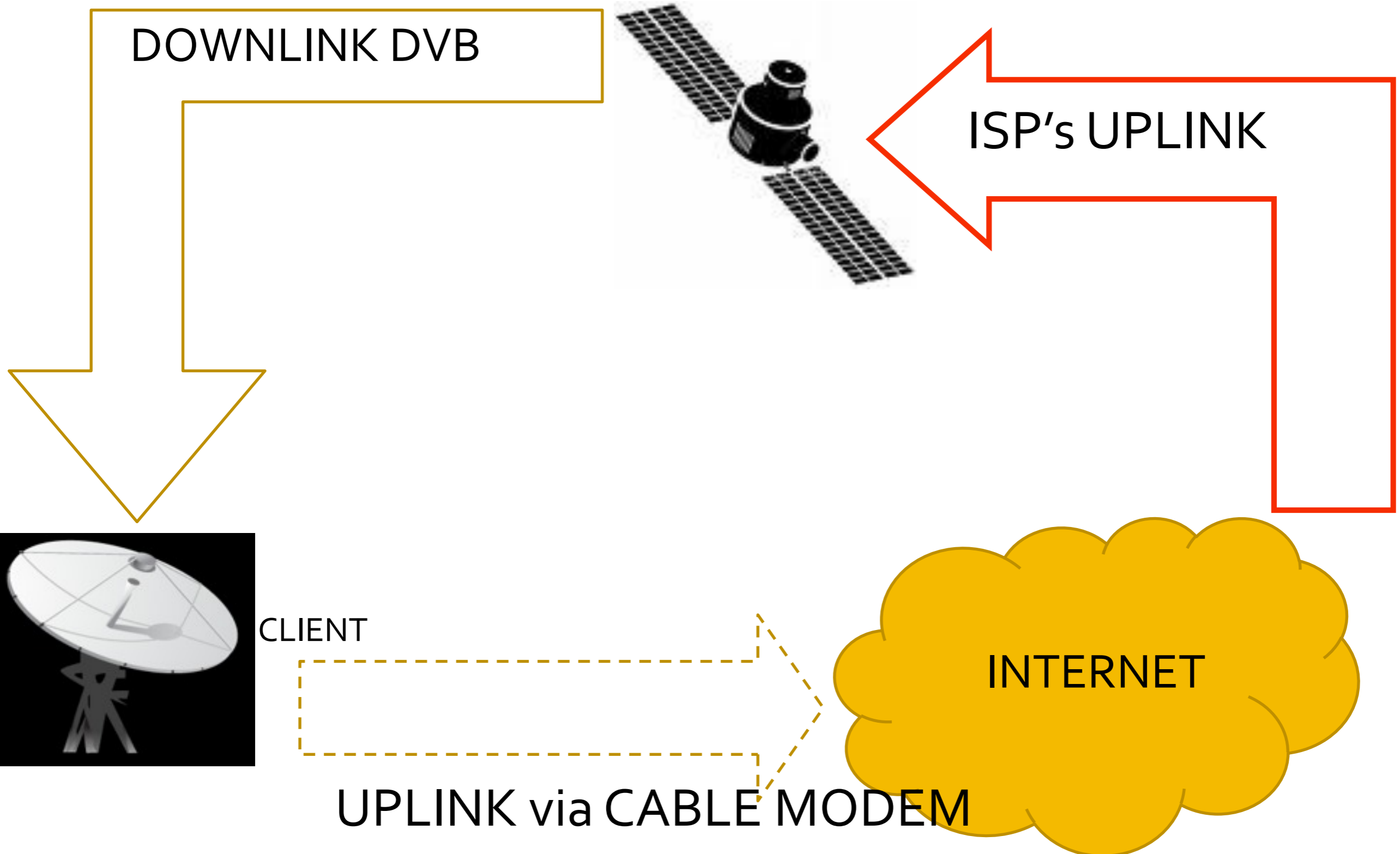
HTSNACBT Attack

IT WORKS!

```
root@sathunter:~  
[root@sathunter ~]# ping www.nsa.gov  
PING www.nsa.gov (12.110.110.204) 56(84) bytes of data.  
  
--- www.nsa.gov ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 2999ms  
  
[root@sathunter ~]# ping www.google.es  
PING www.l.google.com (209.85.229.99) 56(84) bytes of data.  
64 bytes from ww-in-f99.google.com (209.85.229.99): icmp_seq=1 ttl=237 time=69.0 ms  
64 bytes from ww-in-f99.google.com (209.85.229.99): icmp_seq=2 ttl=237 time=59.6 ms  
  
--- www.l.google.com ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/mdev = 59.685/64.360/69.036/4.682 ms  
[root@sathunter ~]# █
```

That's all !!!

HTSNACBT Attack - Connection



HTSNACBT Attack

Some things you must remember:

- The DNS server you use must allow request from any IP or you must use the satellite ISP DNS server.
- If you have any firewall (iptables) disable it.
- All the things you make can be sniffed by others users.

HTSNACBT Attack

Now attacking GRE is very easy, you only need to configure your Linux with IP of one of the routers (the one with the satellite connection) and configure the tunneling.

[http://www.google.es/search?
rlz=1C1GPEA_en_ES312&sourceid=chrome&ie=UTF-8&q=configuring
+GRE+linux](http://www.google.es/search?rlz=1C1GPEA_en_ES312&sourceid=chrome&ie=UTF-8&q=configuring+GRE+linux)

The other scenario

What happened with the scenario where the client use an astromodem?

We can capture the downlink and the uplink so all these attacks are easier to do.

We can capture all queries for the DNS Spoofing attack.

We can capture all traffic in a TCP connection, we can hijack easily in any direction.

What TODO now?

- Leonardo is studying the different methods to trace illegal users. (He only have a few ideas).
- In the future we would like to study the possibilities of sending DVB (or other protocol) data to a satellite via Astromodem.

Conclusions

- Satellite communications are insecure.
- They can be sniffed.
- A lot of attacks can be made, we just talked about only few layer 4 and layer 3 attacks.

Conclusions

- With these technologies in our sky, an anonymous connection is possible.
- Many kinds of Denial of Service are also possible.

THANKYOU!!!!

Questions time

