



POSITIVE TECHNOLOGIES

# How to Intercept a Conversation Held on the Other Side of the Planet



# Who we are

Sergey Puzankov

Dmitry Kurbatov

Information Security Specialists

Positive Technologies

# Topics

Denial of Service on Mobile Switching Center  
Fraud in SS7 network

**Hot for Mobile network operators**

Short Message Interception  
USSD Money Transfer  
Subscriber's Location  
Voice Call Interception

**Hot for everyone**

# All of us are subscribers

Service Availability  
Quality of Service  
Security



# Mobile Services Dynamics

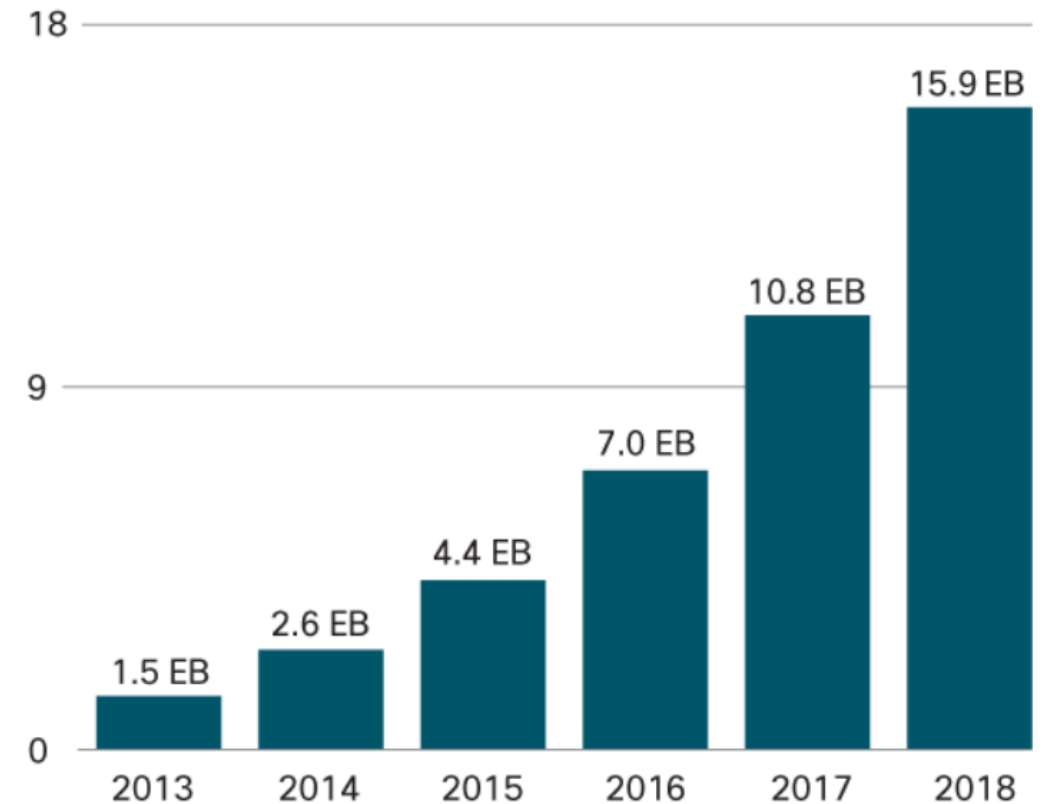
Voice

Mobile Data Traffic



Exabytes per Month

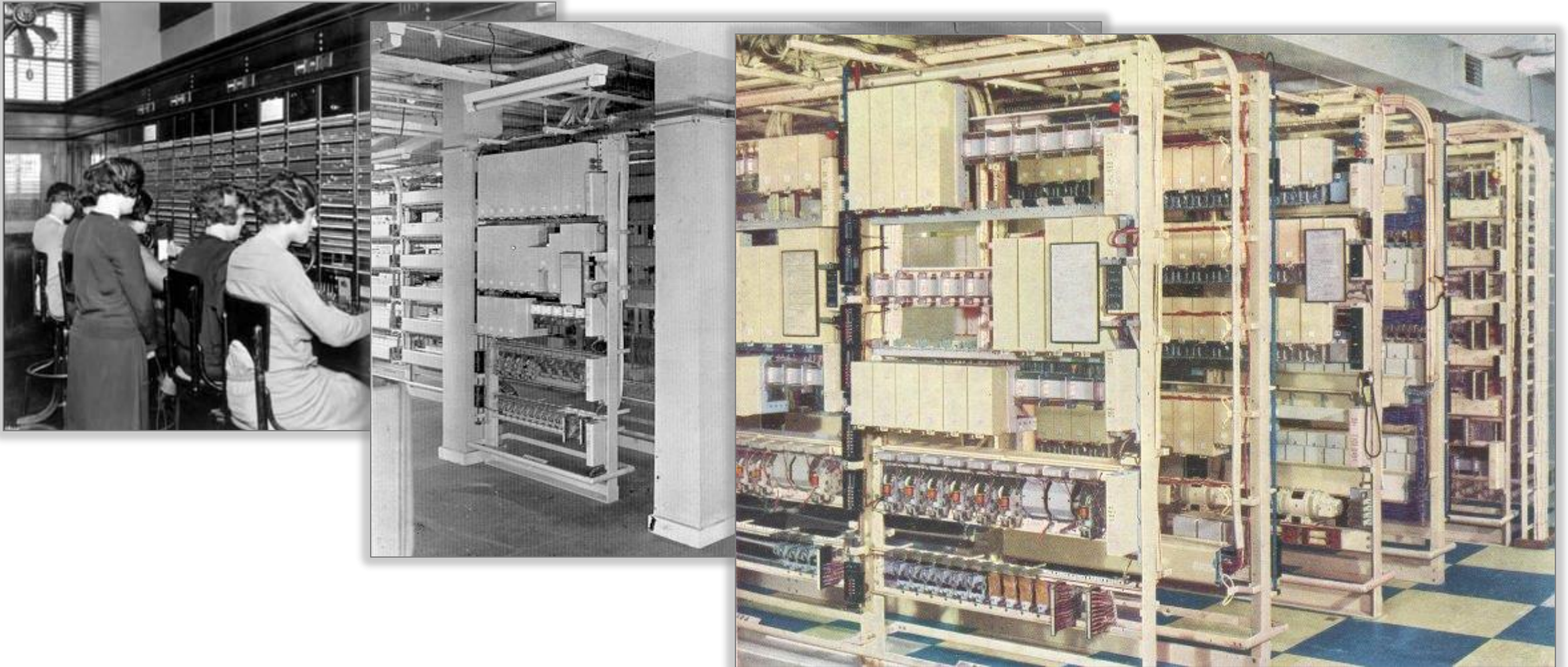
61% CAGR 2013-2018



Source: Cisco VNI Mobile, 2014



# Yesterday: Closed Ecosystems

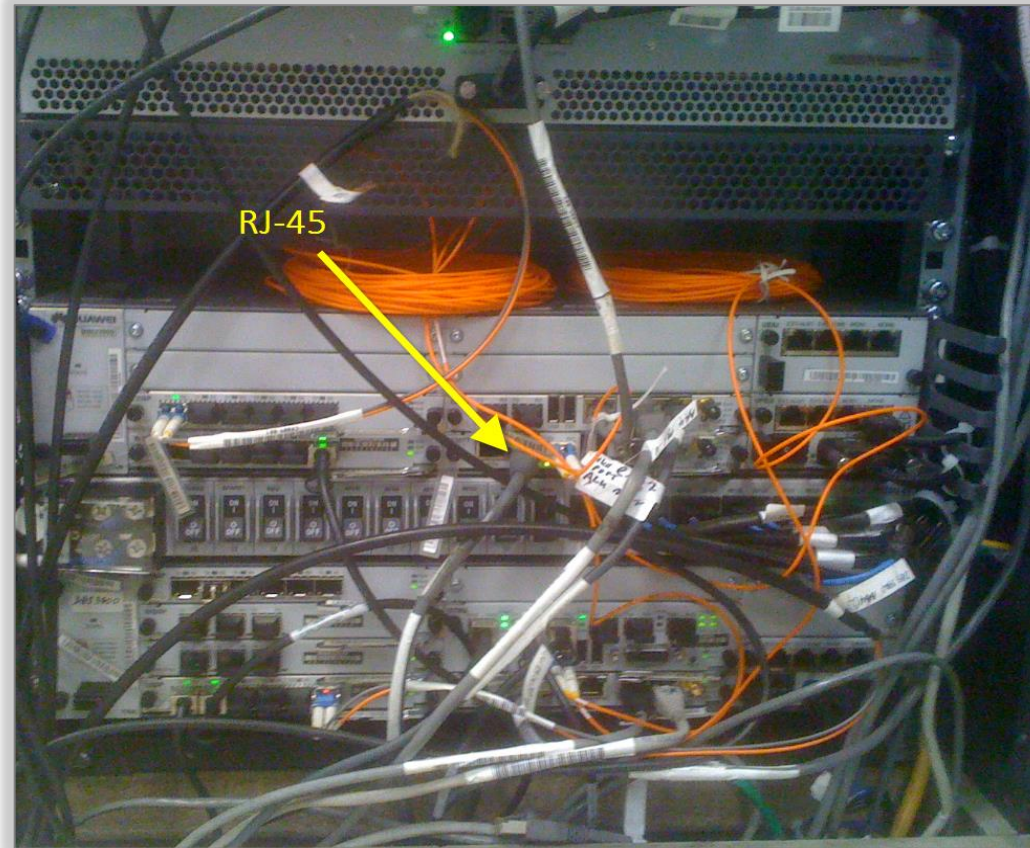


# Today: Unified Technologies





# Today: Common Interfaces



# Today: IP Connectivity

The screenshot shows the Shodan search engine interface. The browser address bar displays 'www.shodanhq.com/search?q=GGSN'. The Shodan logo and search bar are at the top, with the search term 'GGSN' entered. The search results are displayed in a table format, showing the first 10 results out of approximately 33. The results are categorized by Services and Top Countries. The Services section lists SNMP (14), Telnet (9), FTP (3), HTTPS Alternate (2), and SMB (2). The Top Countries section lists China (12), Italy (7), Israel (3), United States (2), and Russian Federation (2). The main results table shows the following entries:

IP address removed	Company name removed	Added on 13.05.2014	ZXR10 xGH-16, ZTE ZXR10 Software Version: ZXUN xGH(GGSN)V4.10.10(1.0.0)
IP address removed	Company name removed	Added on 12.05.2014	Sharename Type Comment
			print\$ Disk Printer Drivers
			nas Disk
			IPC\$ IPC IPC Service (GGSN server (Samba, Ubuntu))
			Server Comment
			GGSN GGSN server (Samba, Ubuntu)
			Workgroup Master
			WORKGROUP GGSN
IP address removed	Company name removed	Added on 10.05.2014	220 GGSN-RMS_re0 FTP server (Version 6.00LS) ready.
			530 User anonymous unknown

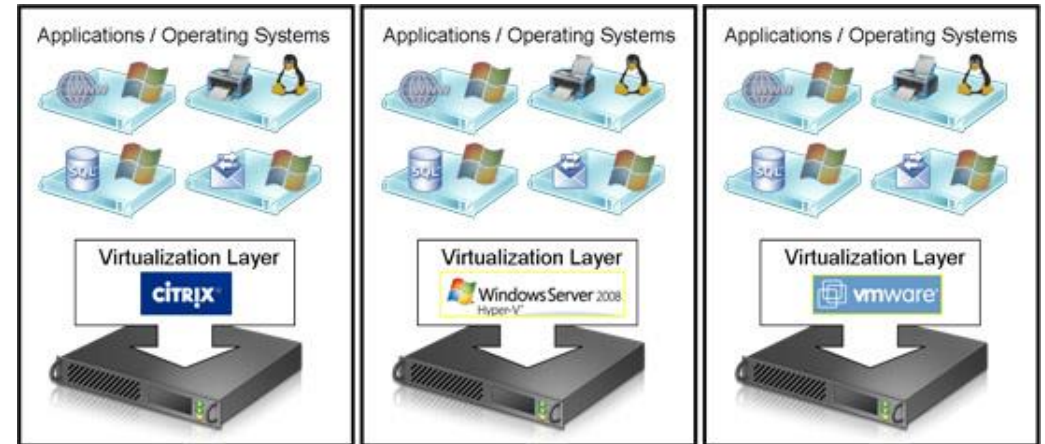
# Today: Widen Borders

Get your own femtocell

- Hack it
- Upload modified firmware
- Make a call/SMS interception
- Get into IPsec
- Get into Core network



# Tomorrow: virtualization



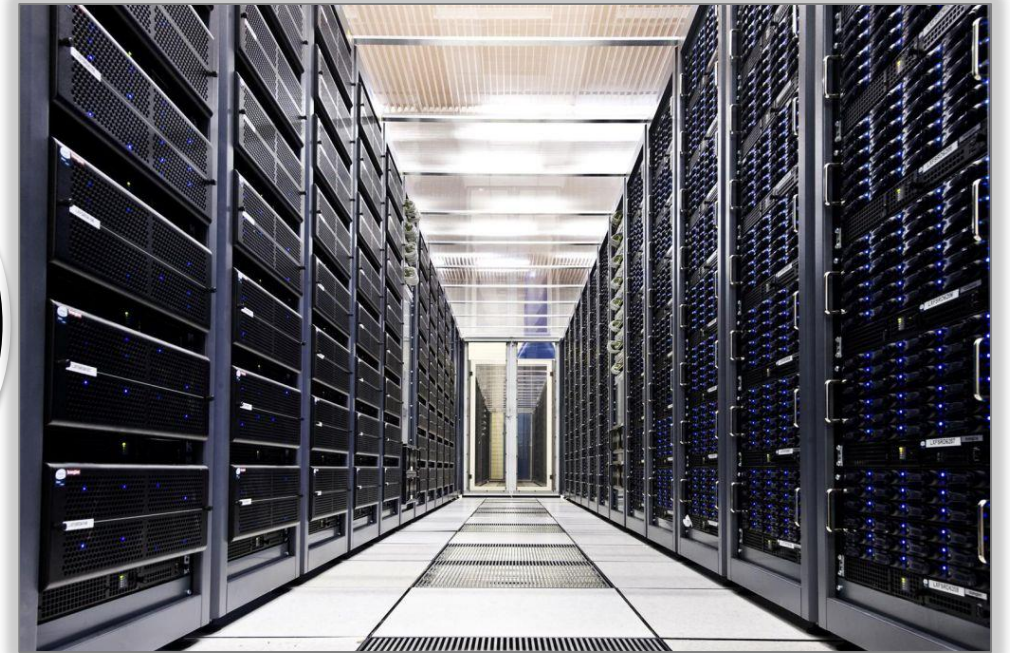


# Time Machine

Through SIGTRAN back to 1970's

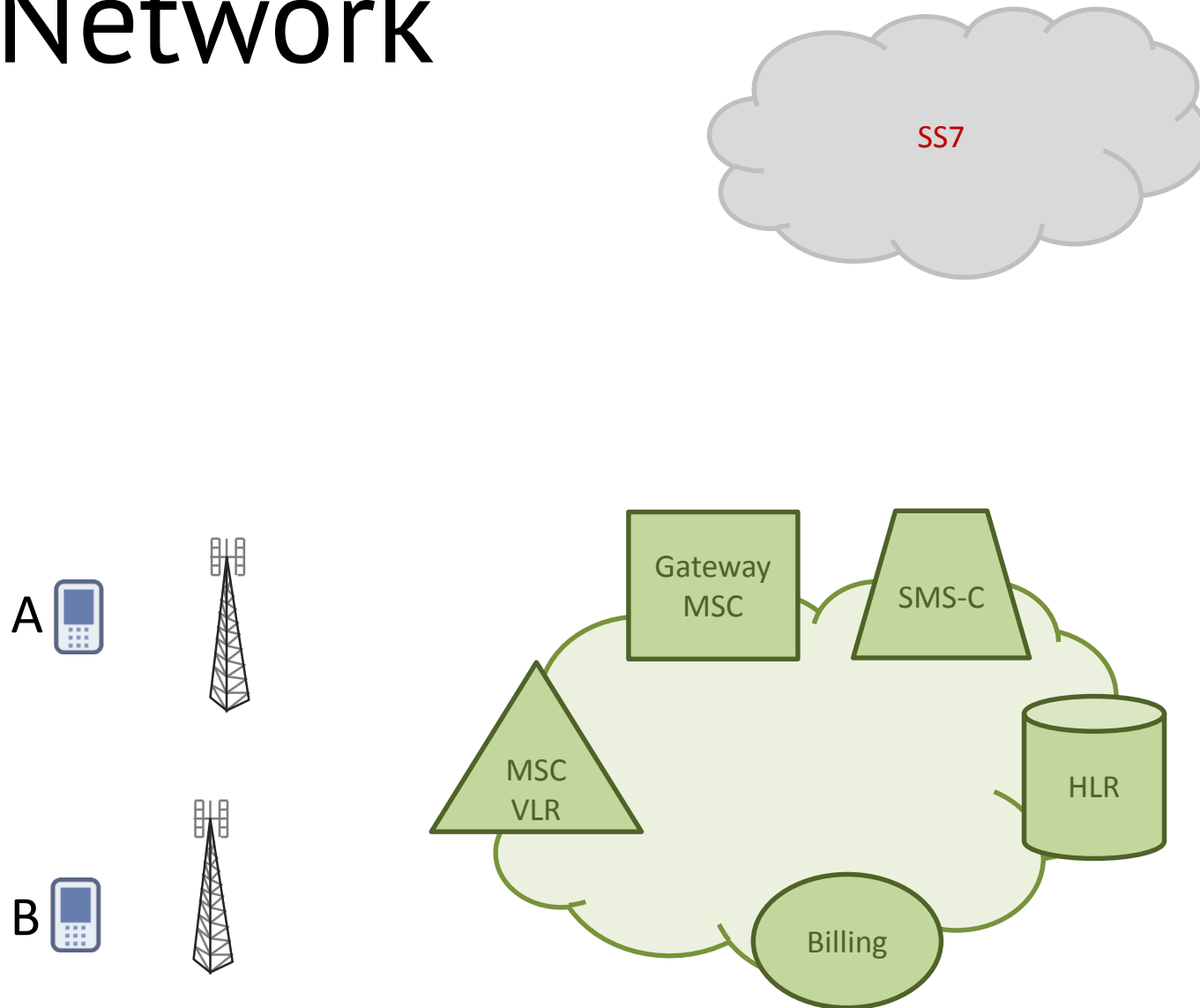


SIGTRAN





# SS7 Network

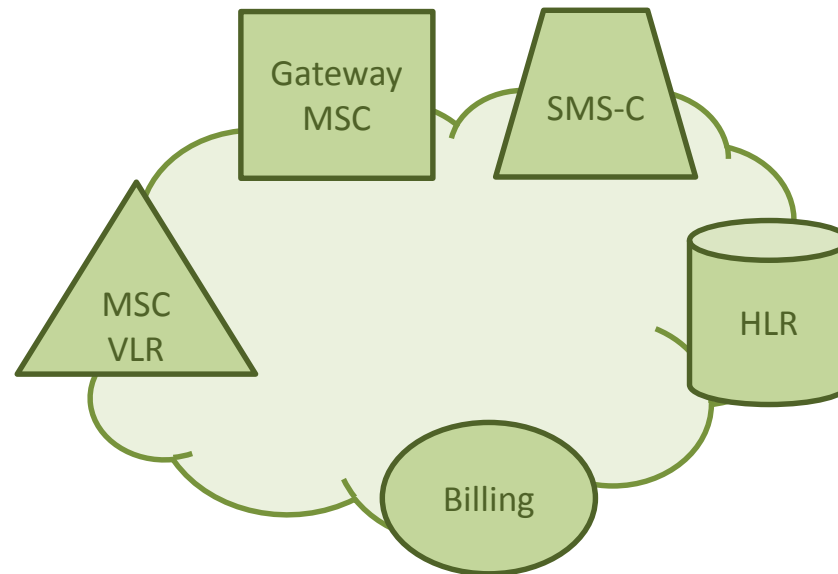
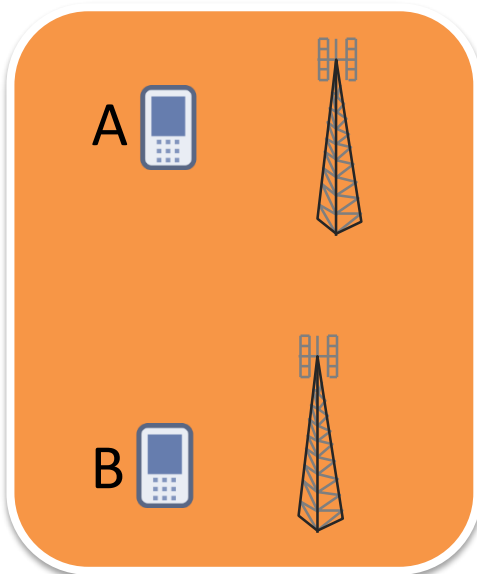


# Radio Part

Cell Phone

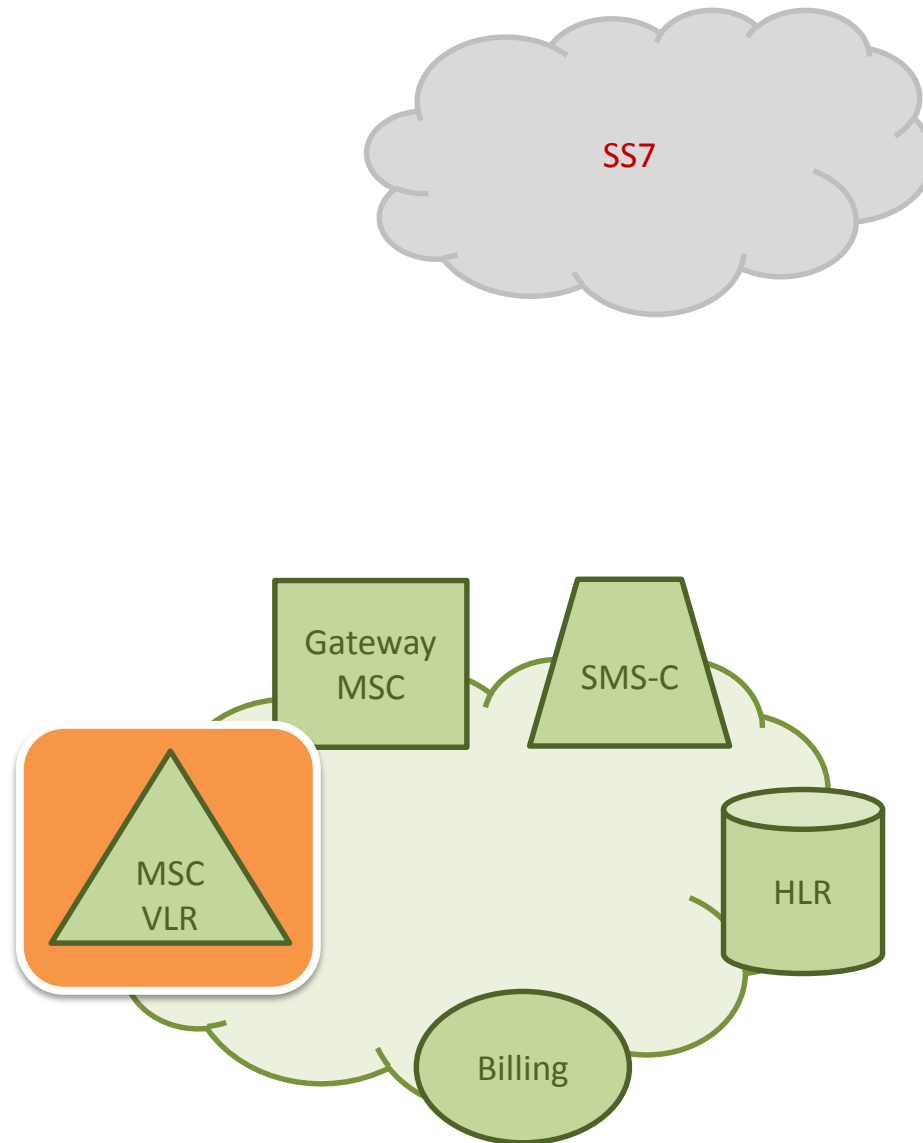
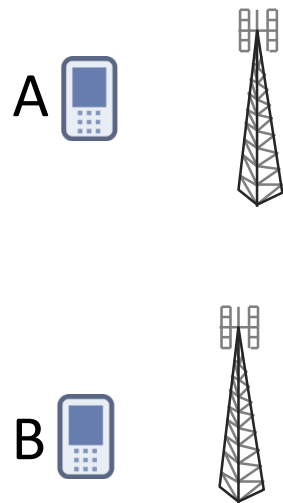
Base Transceiver Station

Base Station Controller



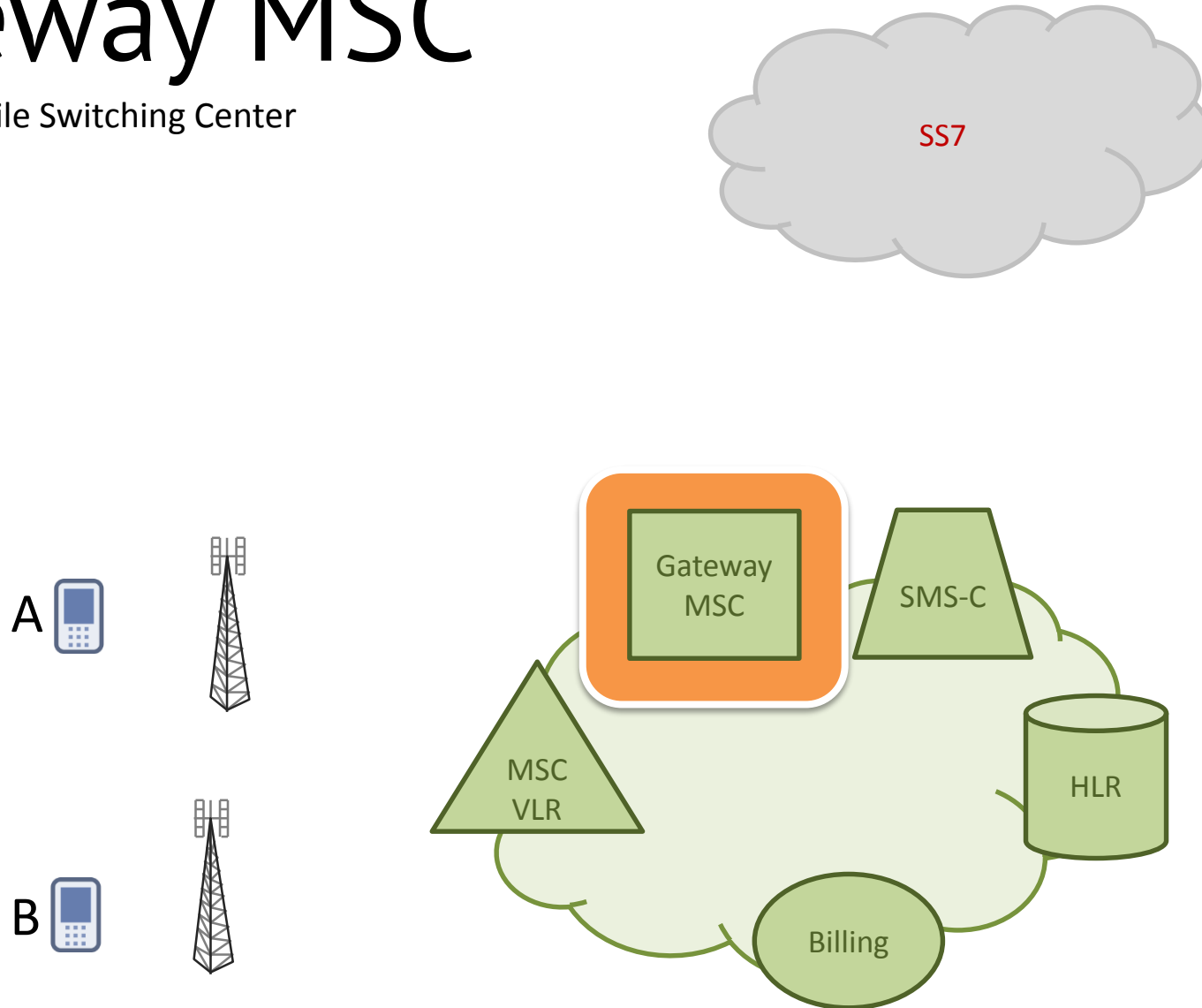
# MSC/VLR

Mobile Switching Center  
Visitor Location Register



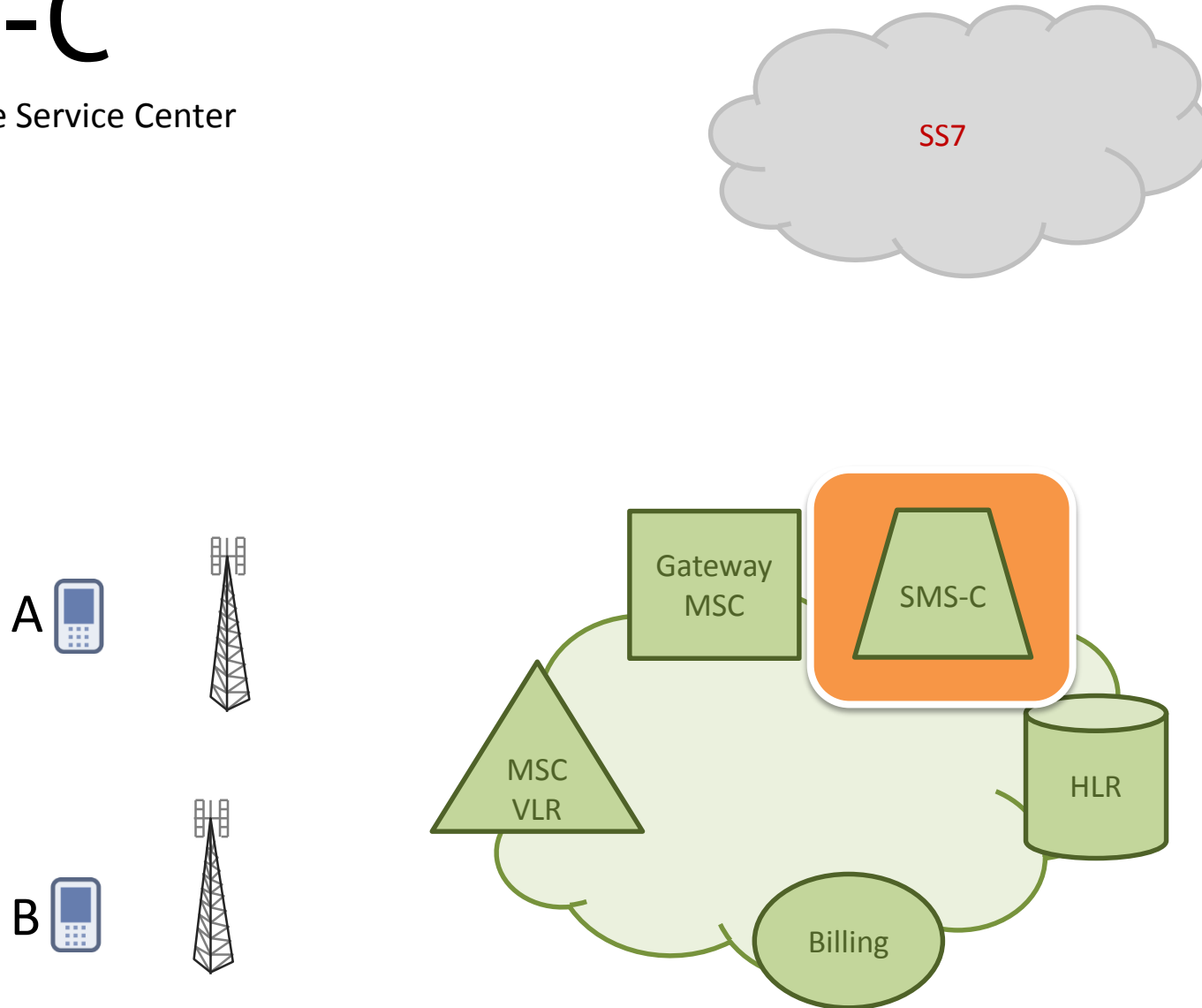
# Gateway MSC

Gateway Mobile Switching Center



# SMS-C

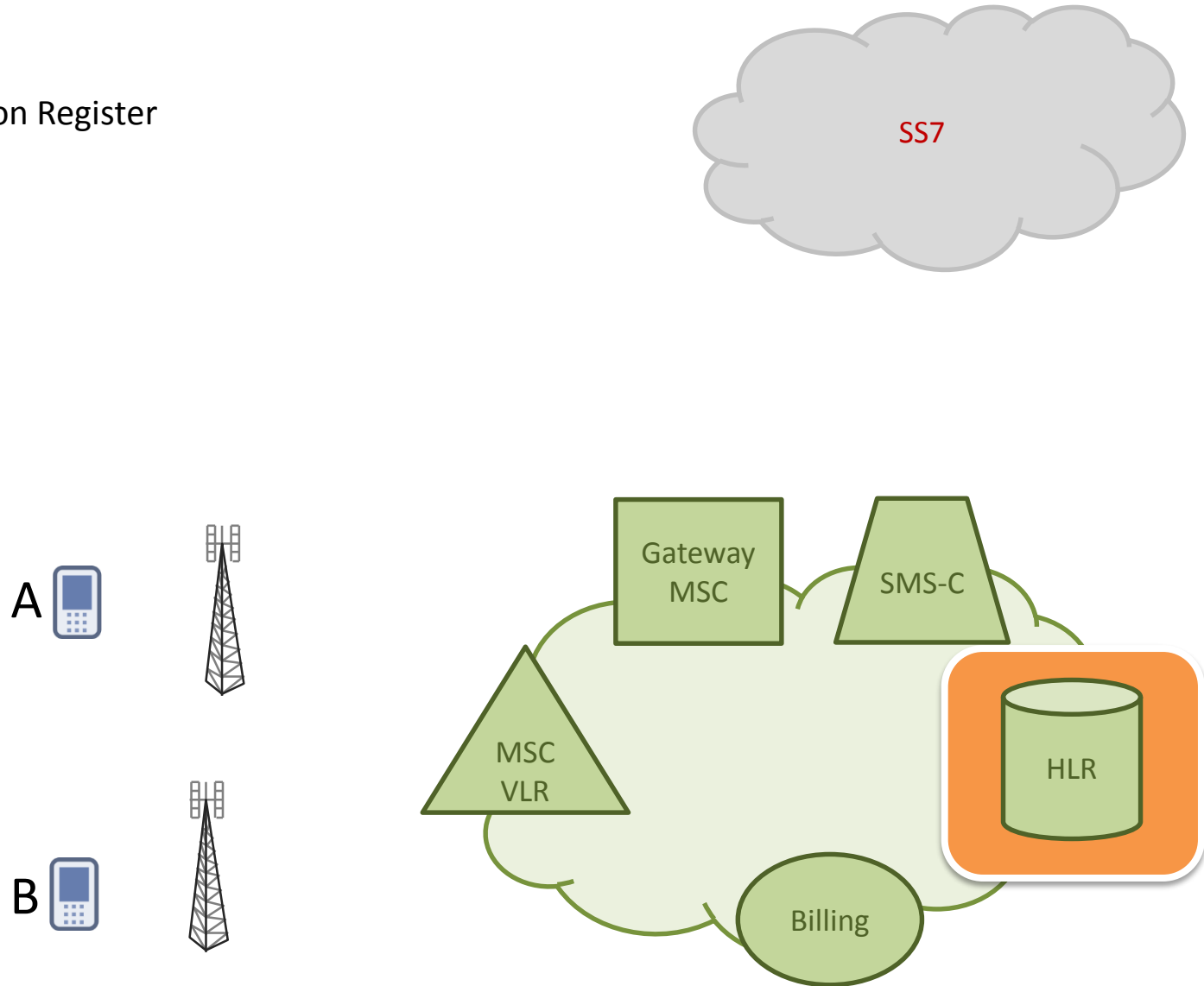
Short Message Service Center



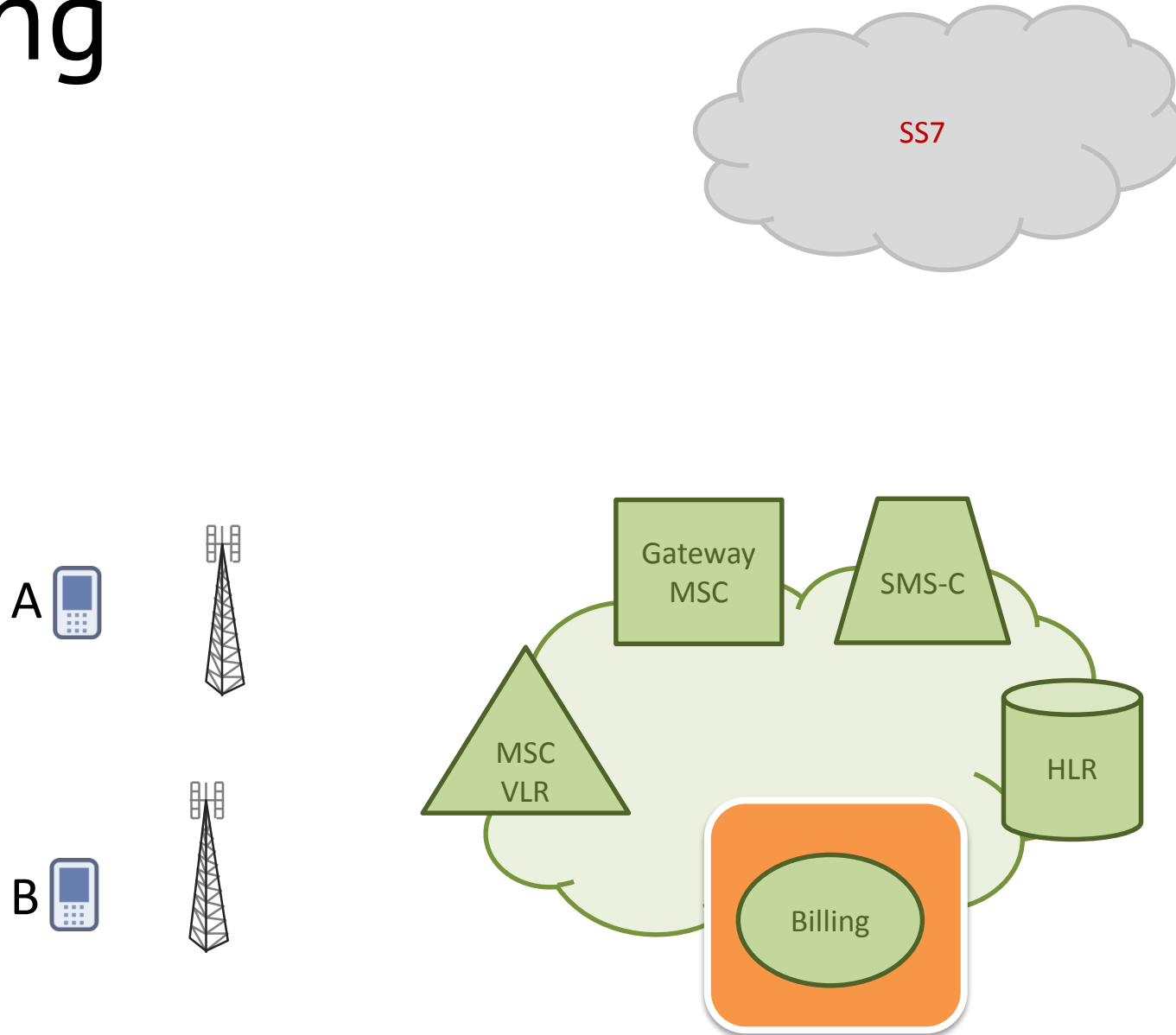


# HLR

Homey Location Register

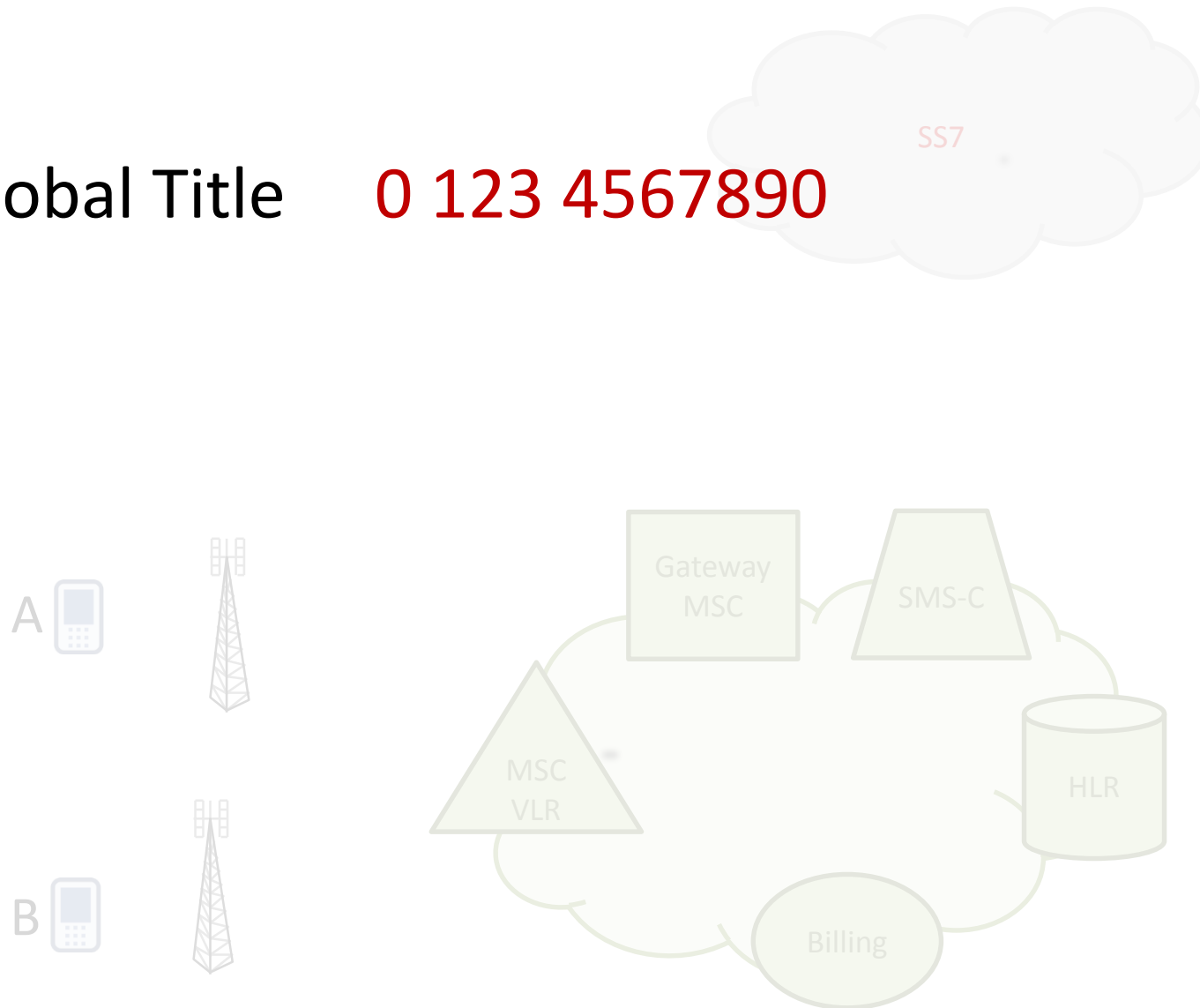


# Billing



# IDs

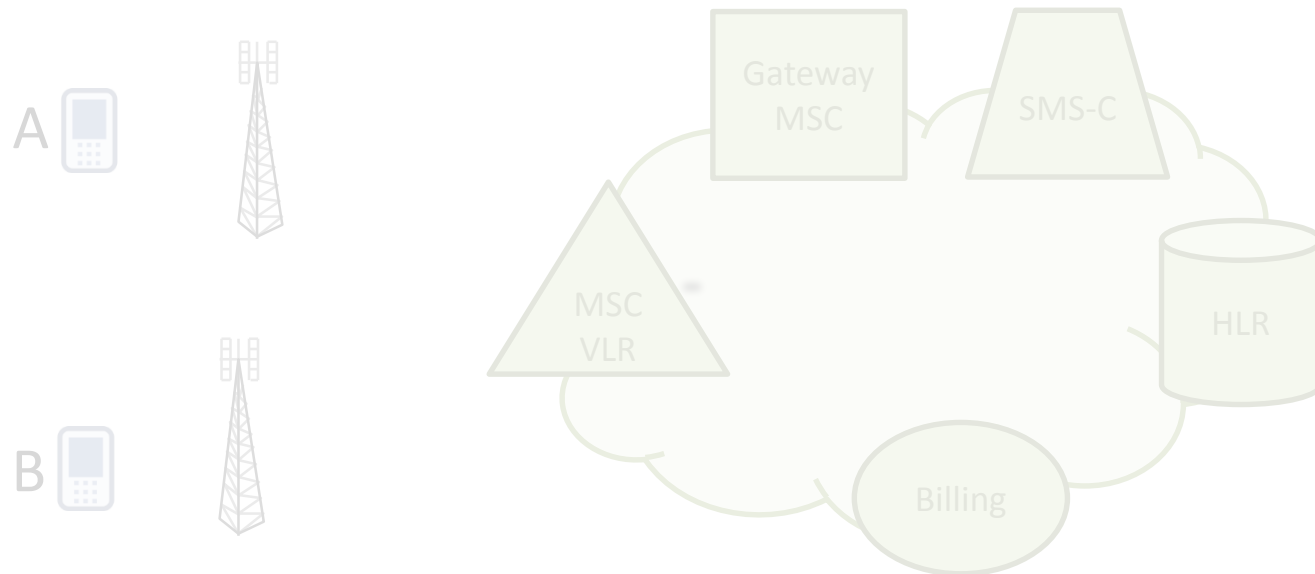
GT – Global Title    0 123 4567890



# IDs

**GT** – Global Title     0 123 4567890

**MSISDN** – A or B mobile numbers     0 123 4567890

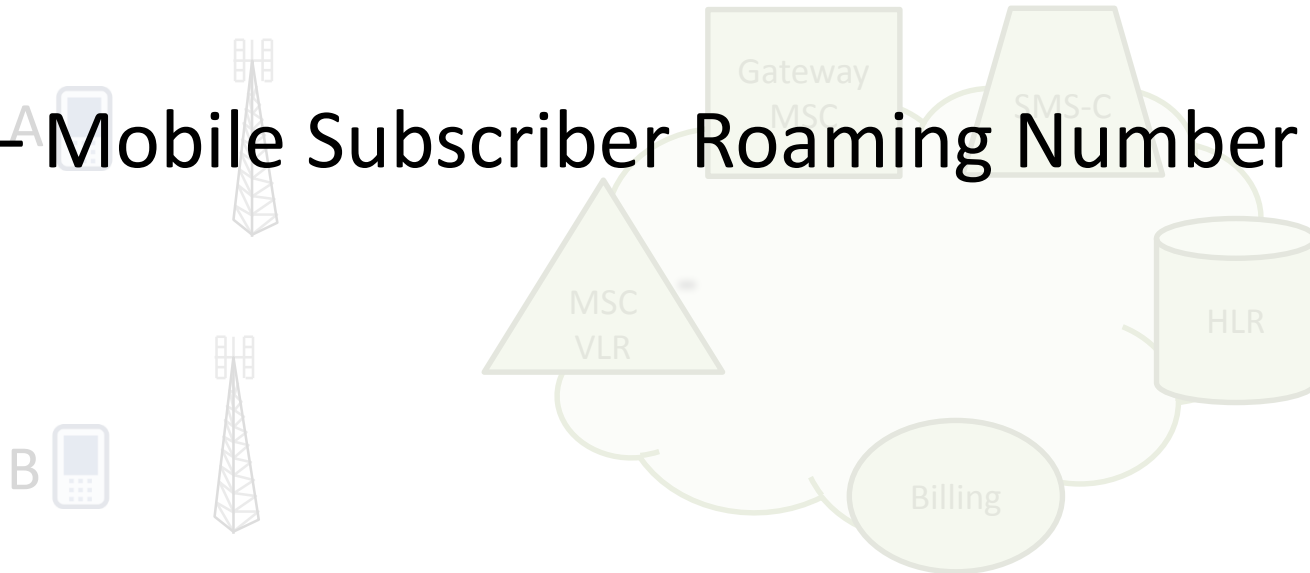


# IDs

**GT** – Global Title    0 123 4567890

**MSISDN** – A or B mobile numbers    0 123 4567890

**MSRN** – Mobile Subscriber Roaming Number    0 123 4567890





# IDs

**GT** – Global Title    0 123 4567890

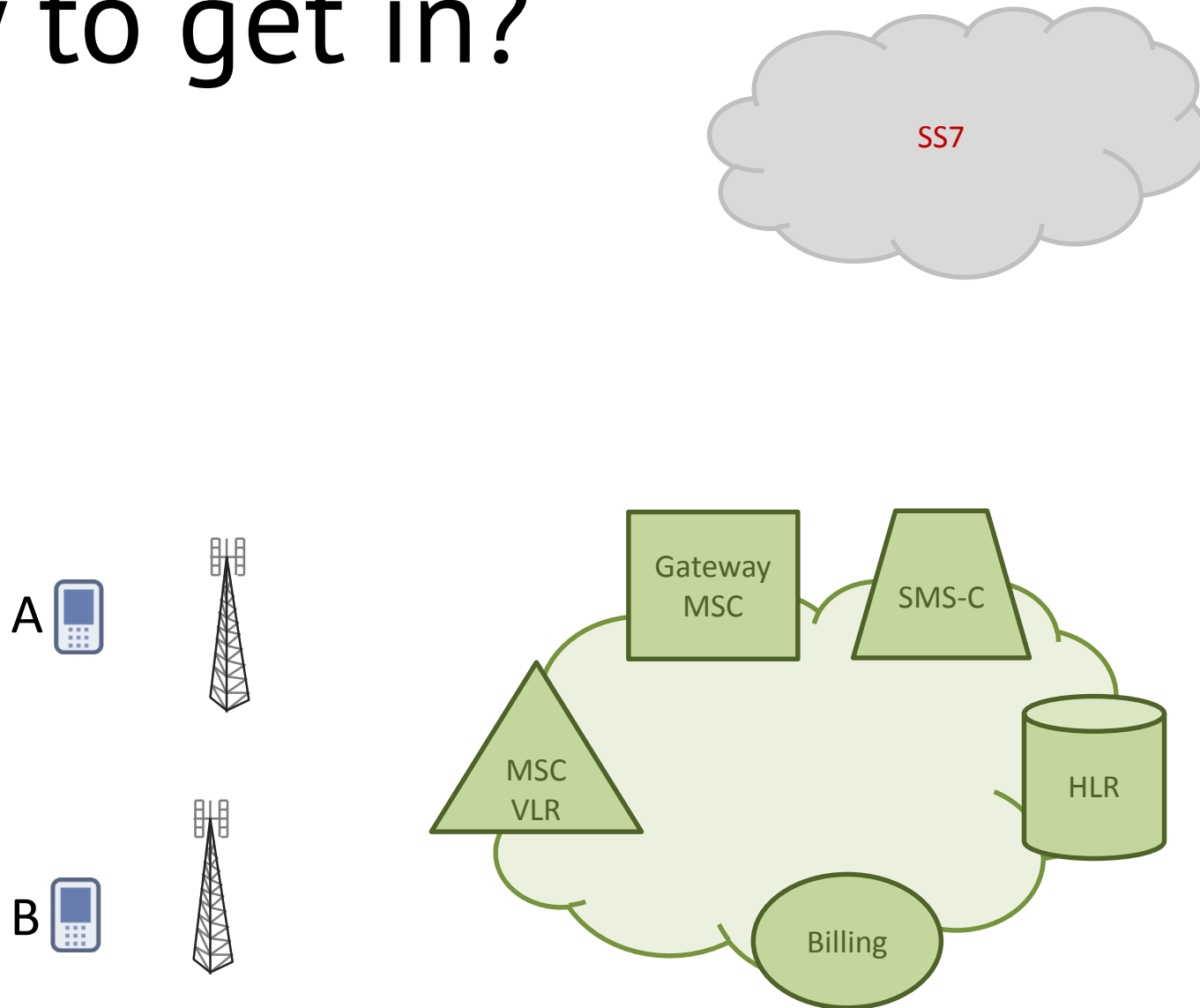
**MSISDN** – A or B mobile numbers    0 123 4567890

**MSRN** – Mobile Subscriber Roaming Number    0 123 4567890

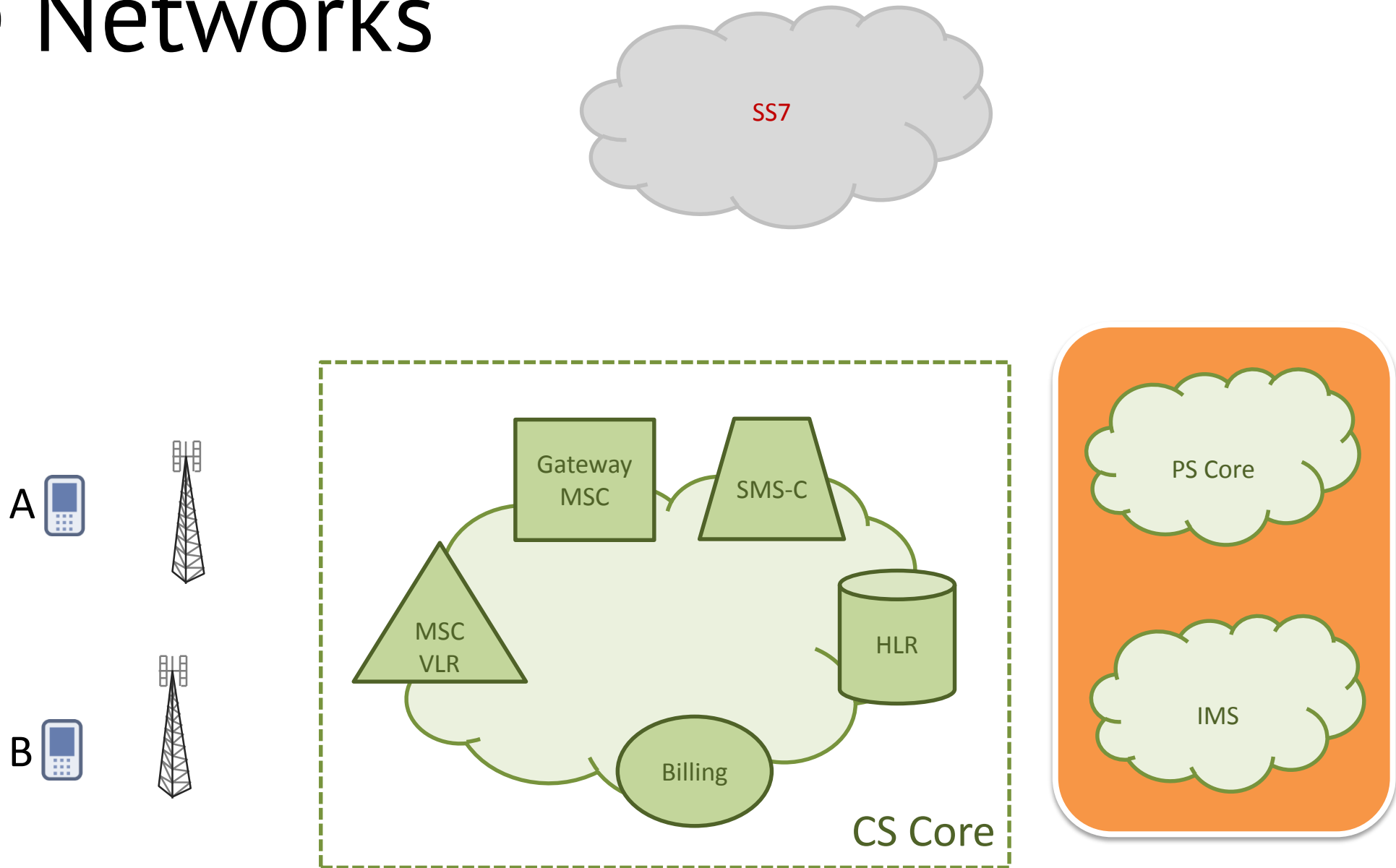
**IMSI** – International Mobile Subscriber Identity    15 digits



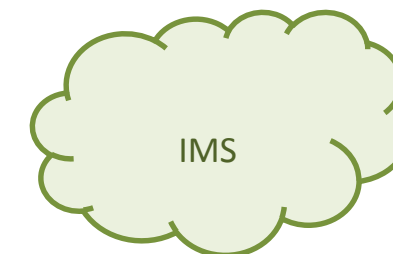
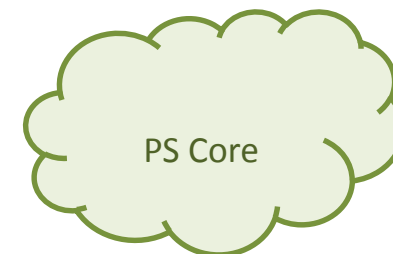
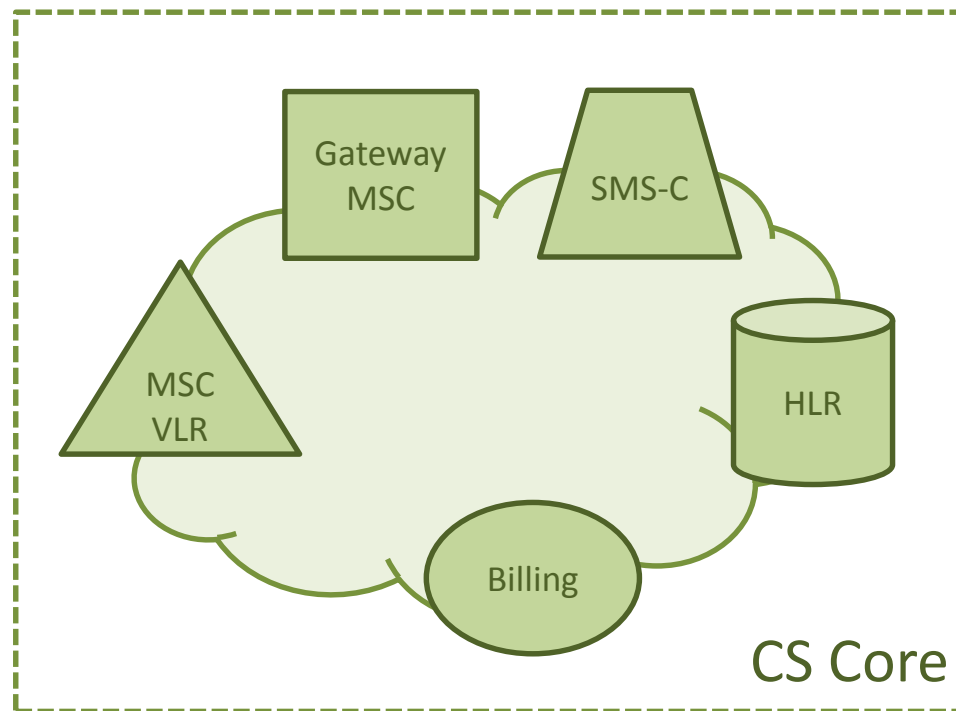
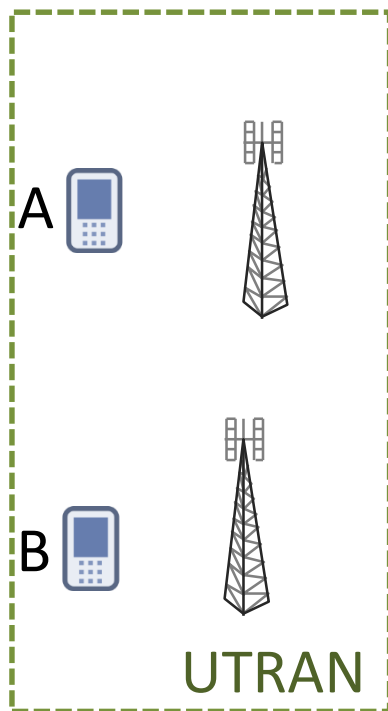
# How to get in?



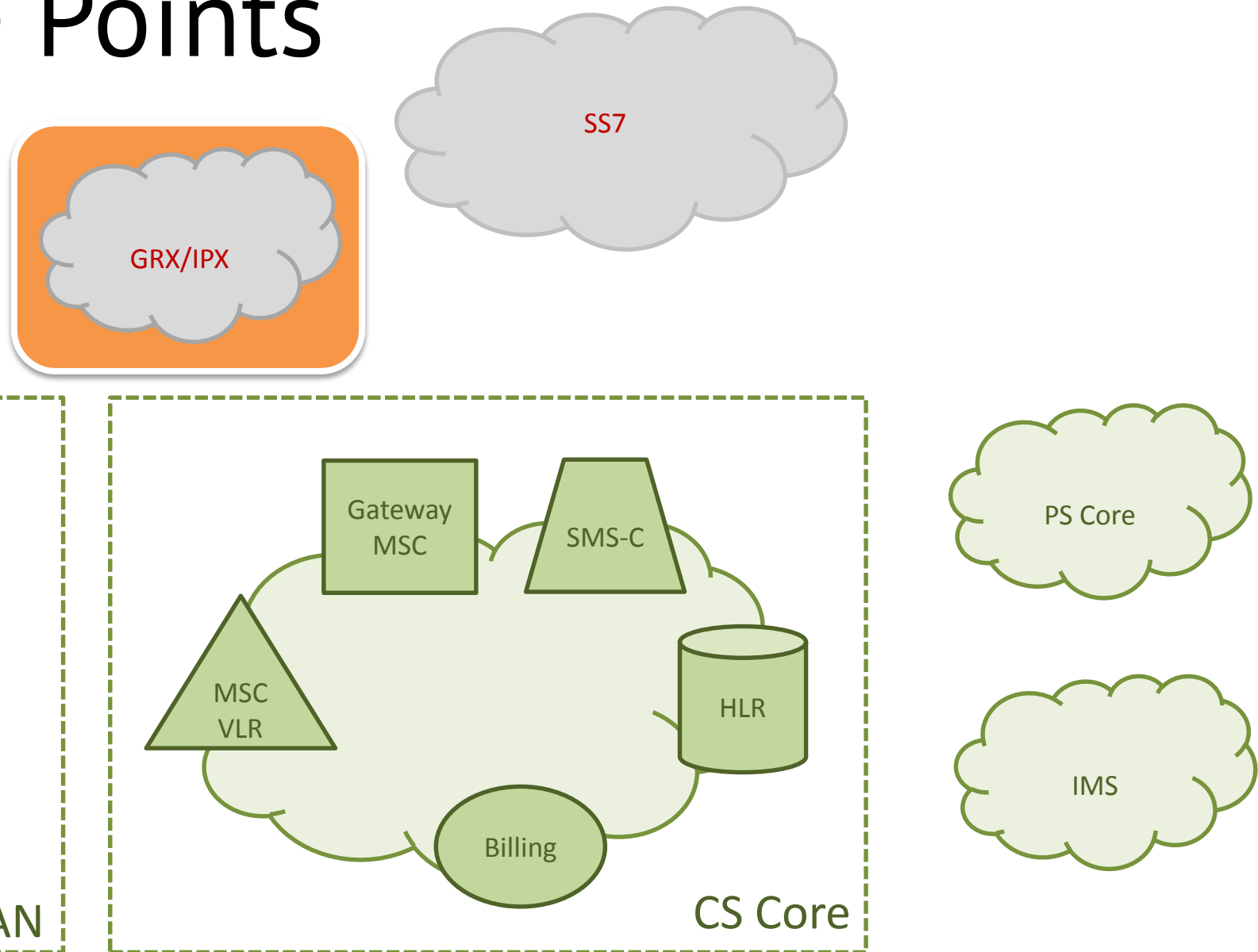
# Core Networks



# Access Networks

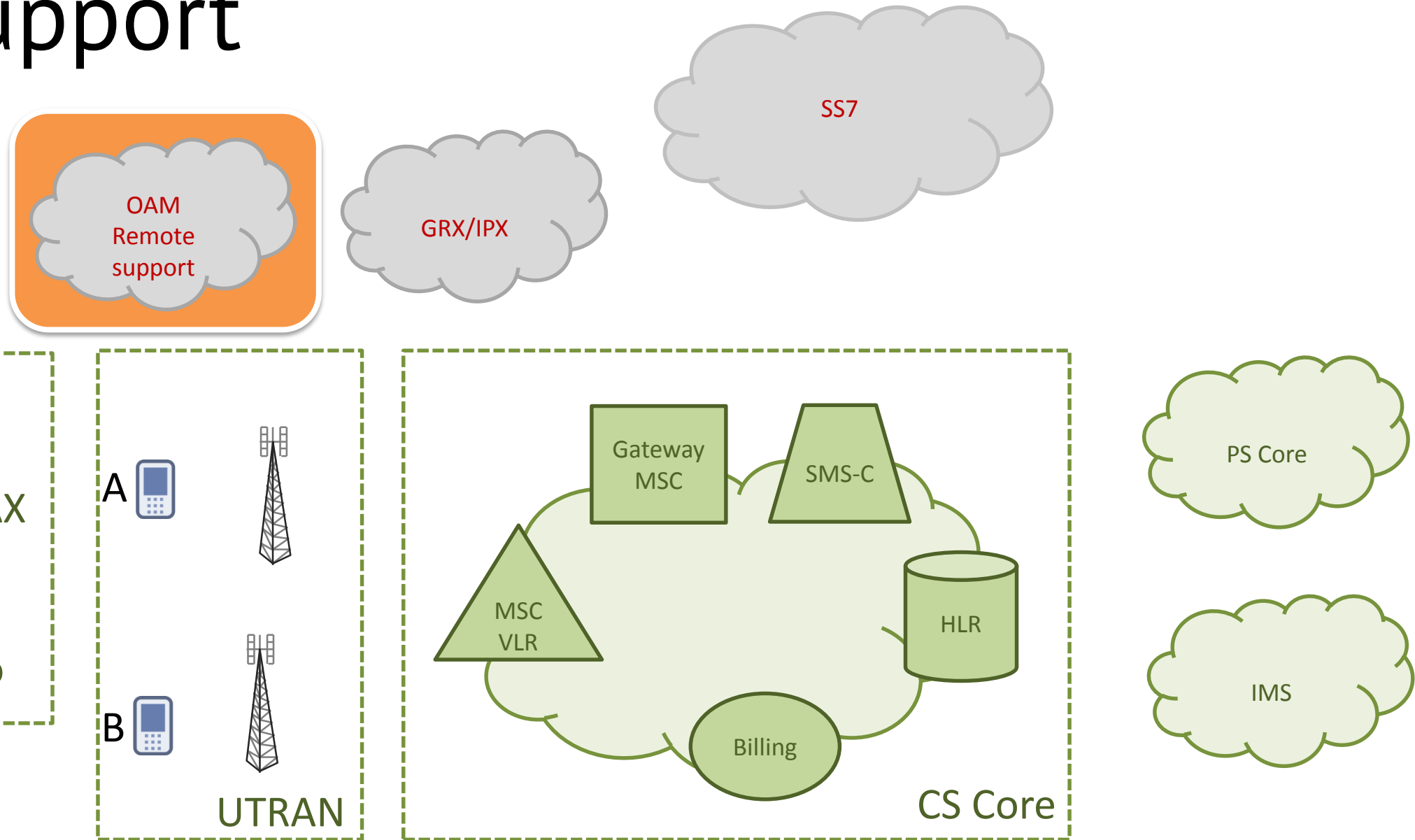


# Exchange Points

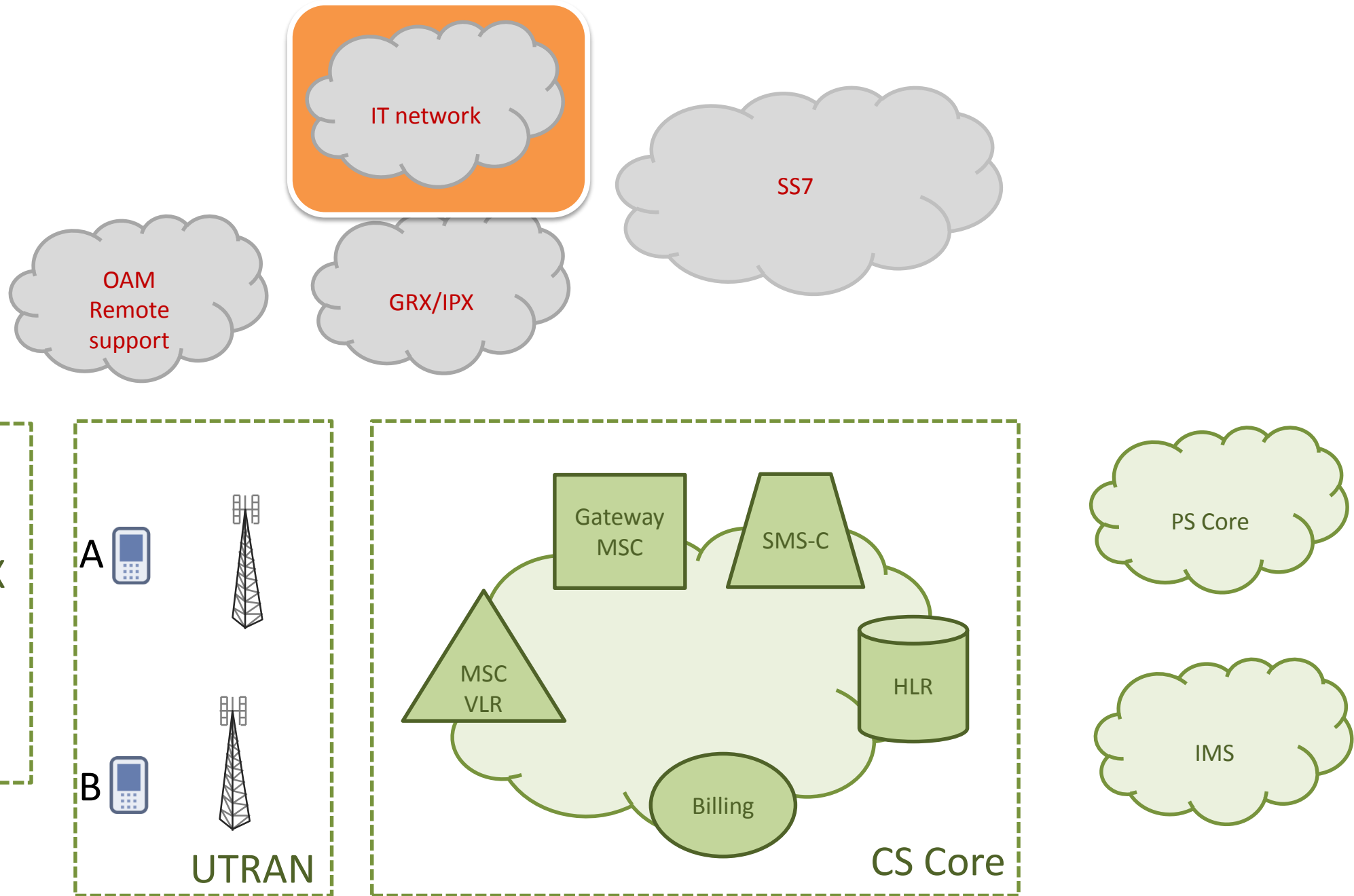




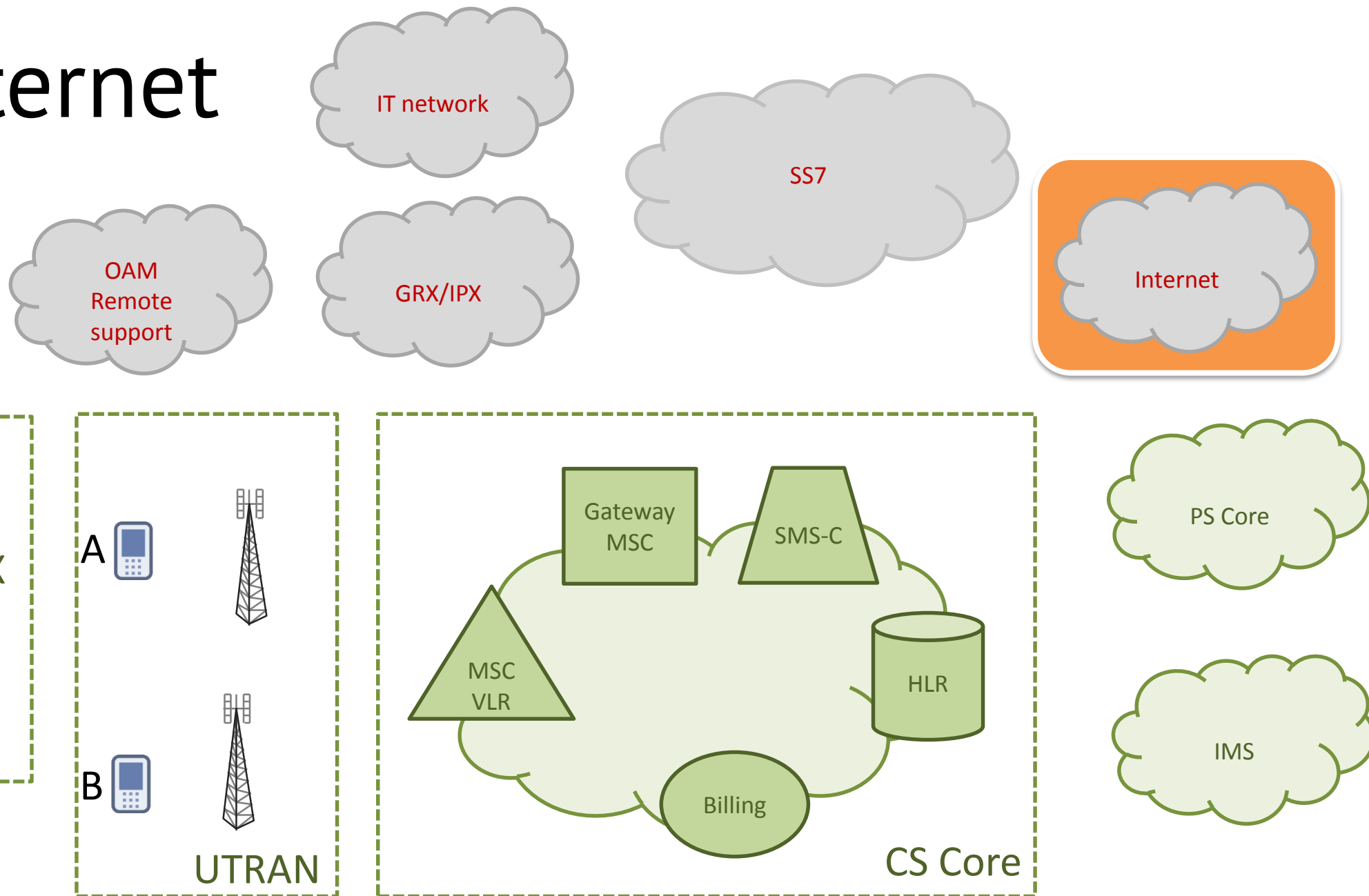
# Support



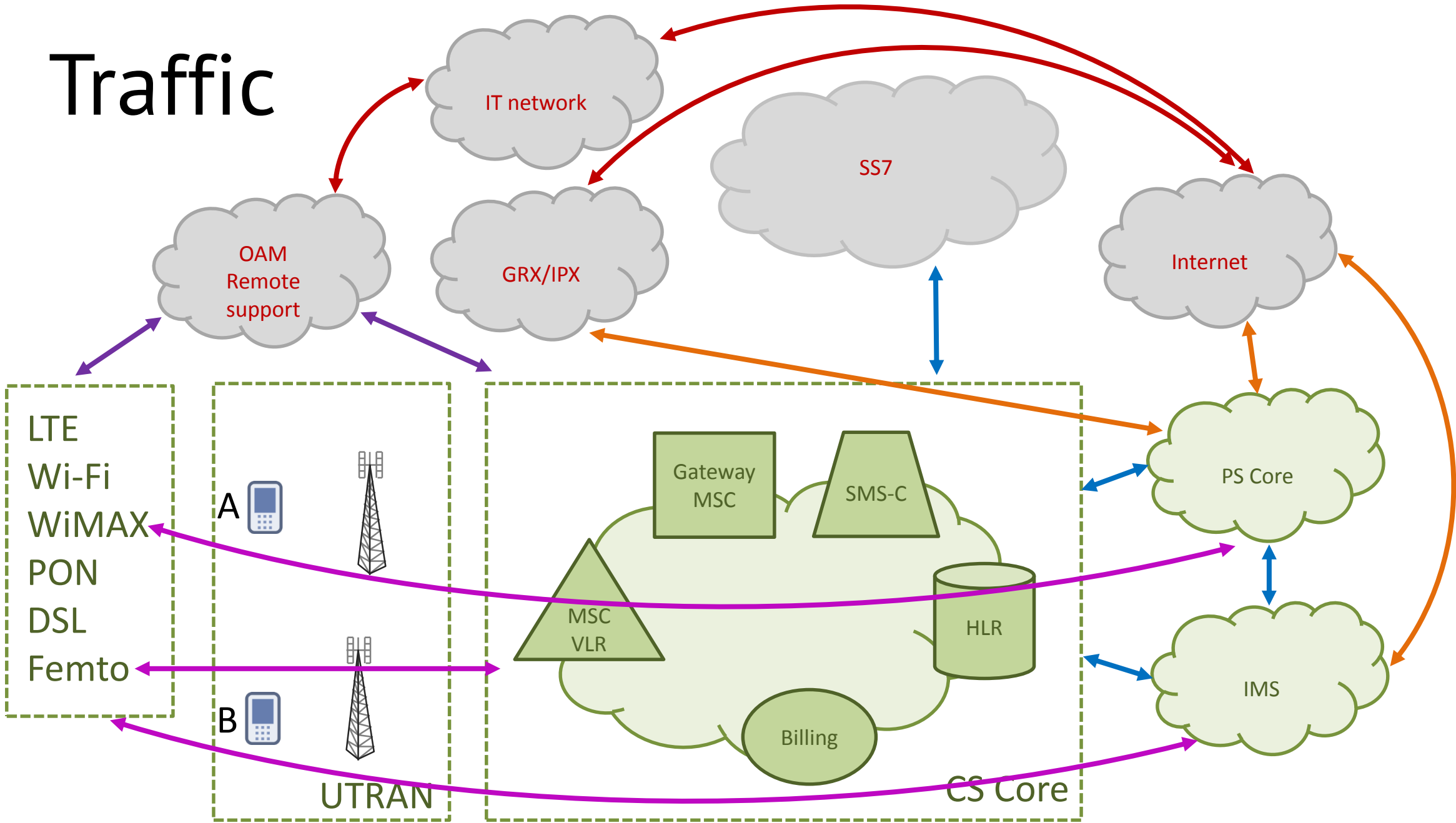
# IT



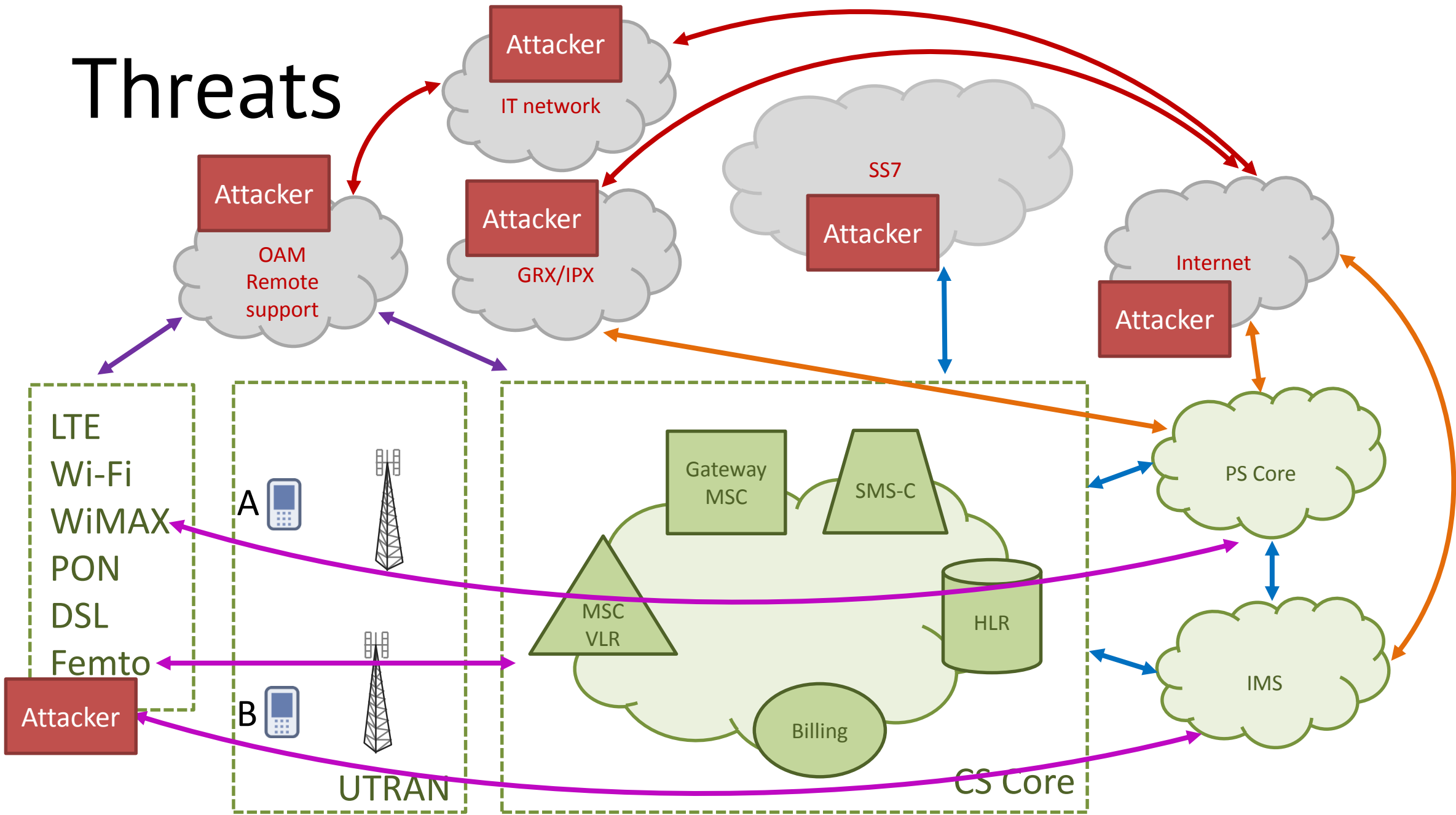
# Internet



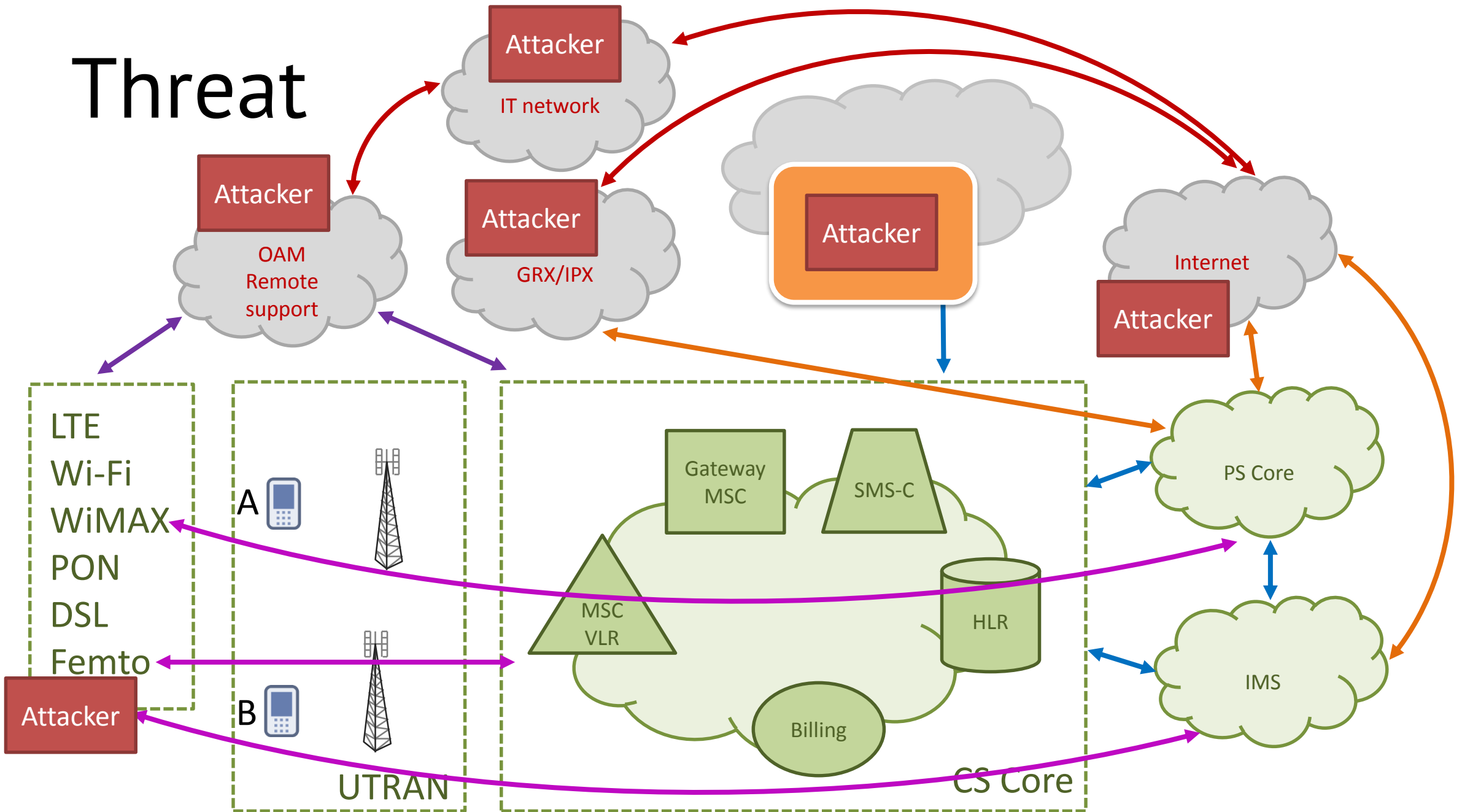
# Traffic



# Threats



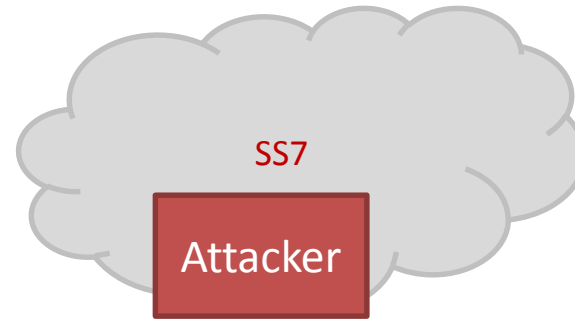
# Threat



# Mobile Switching Center DoS

Just like DHCP Starvation

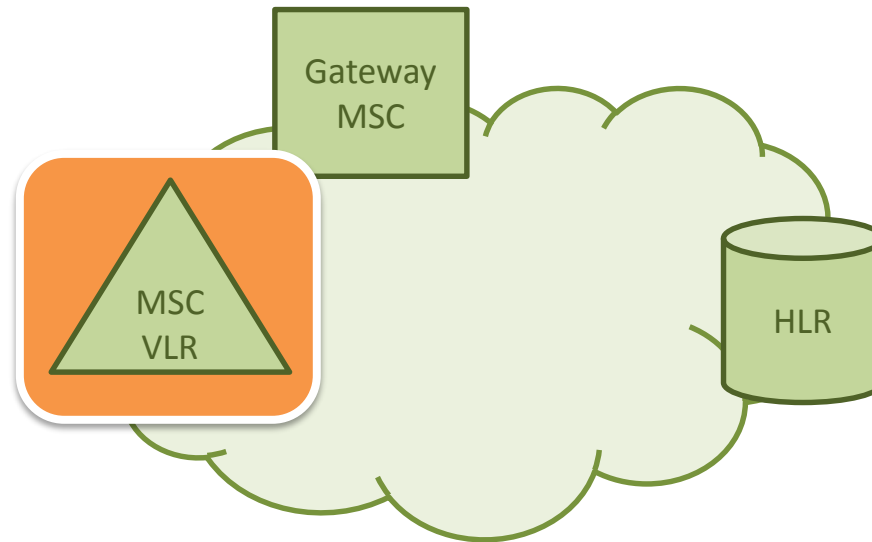
# Collect info



We know

**B-Number** 0 123 45678**02**

B

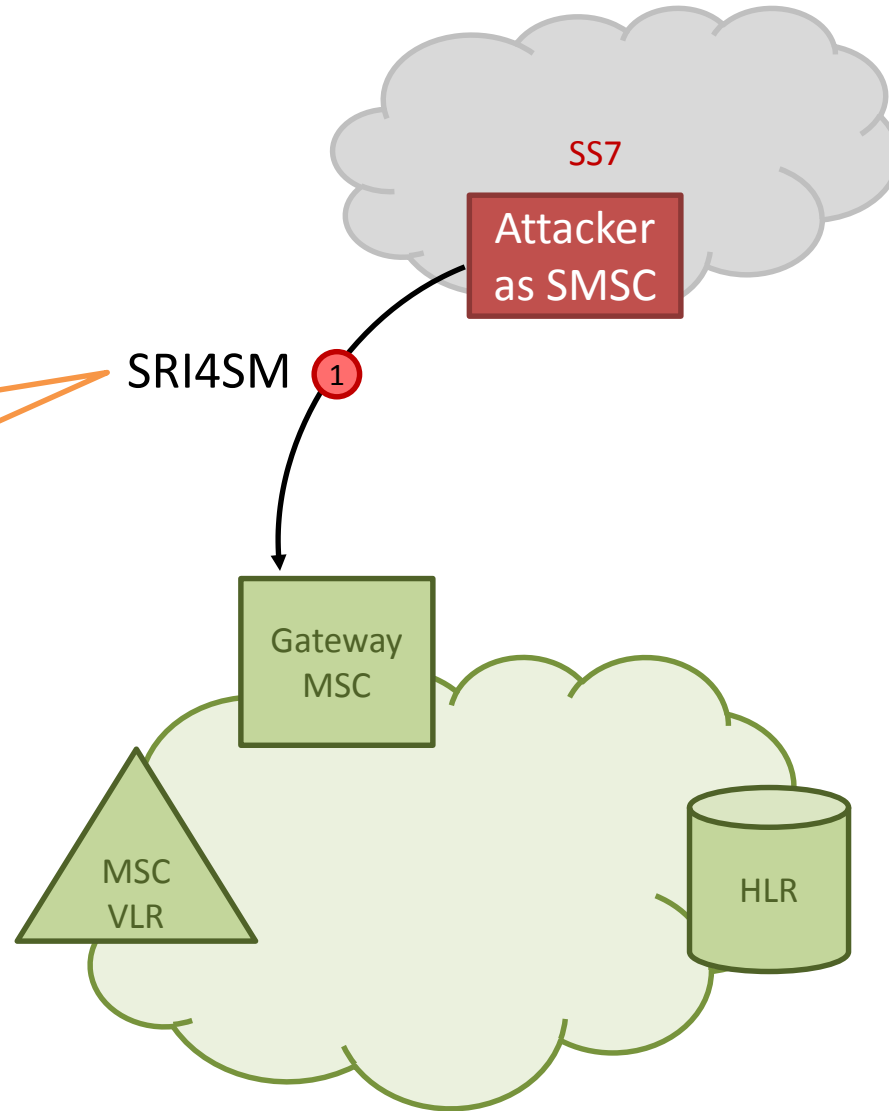




# Collect info

**sendRoutingInfoForSM**  
I am **SMSC**.  
**My GT** 1 321 4567801.  
Where is  
**Subscriber-B MSISDN** 0 123 4567802?

B 

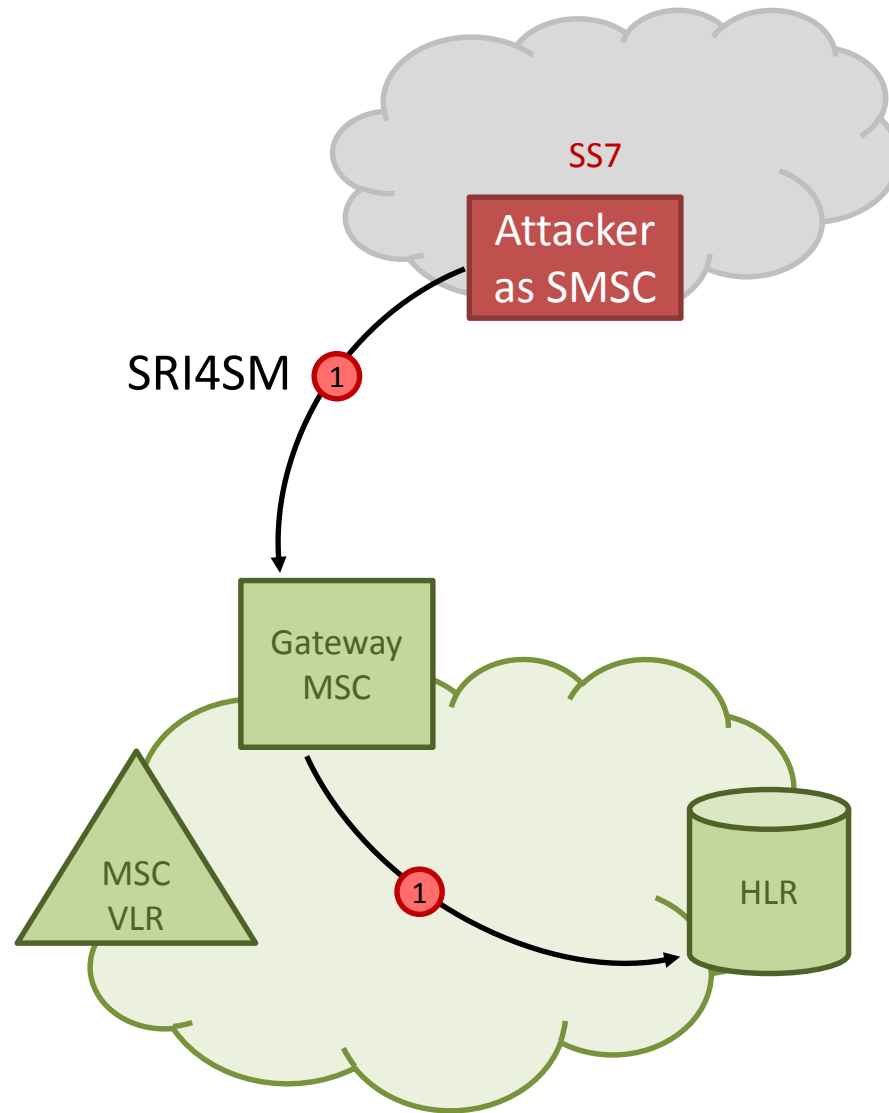


We know

**B-Number** 0 123 4567802

# Collect info

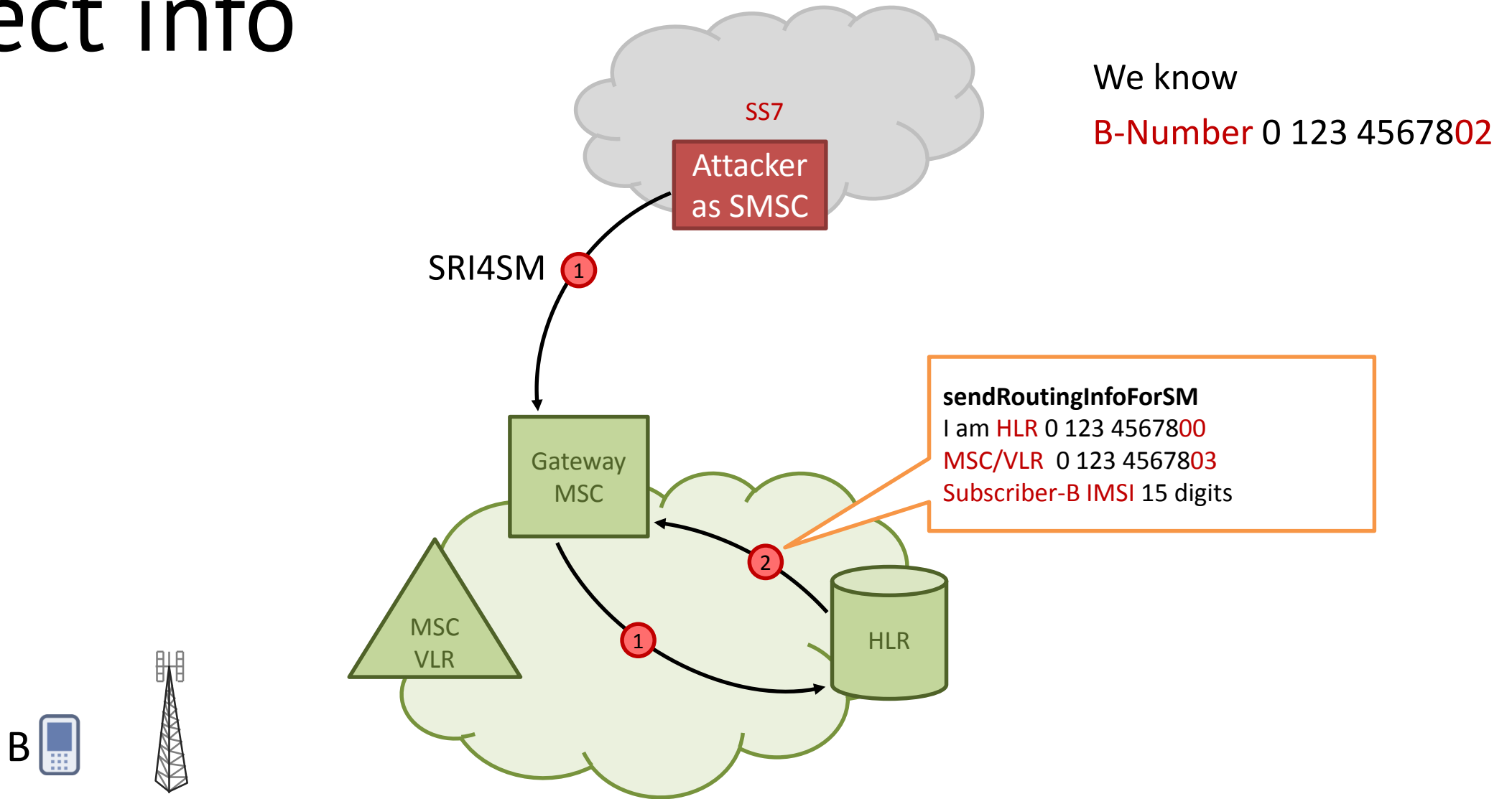
B



We know

**B-Number** 0 123 45678**02**

# Collect info



# Collect info

We know

**B-Number** 0 123 4567802

Protocol Length Info

GSM MAP 194 invoke sendRoutingInfoForSM

GSM MAP 206 returnResultLast sendRoutingInfoForSM

Called Party address (11 bytes)

Calling Party address (11 bytes)

Address Indicator

SubSystem Number: HLR (Home Location Register) (6)

[Linked to TCAP]

Global Title 0x4 (9 bytes)

Translation Type: 0x00

0001 .... = Numbering Plan: ISDN/telephony (0x01)

.... 0001 = Encoding Scheme: BCD, odd number of digits (0x01)

...000 0100 = Nature of Address Indicator: International number (0x04)

Calling Party Digits: HLR 0 123 4567800

Transaction Capabilities Application Part

GSM Mobile Application

Component: returnResultLast (2)

returnResultLast

invokeID: 1

resultretres

opCode: localValue (0)

imsi: Subscriber-B IMSI 15 digits

TBCD digits:

locationInfoWithLMSI

networkNode-Number: MSC/VLR 0 123 4567803

1... .... = Extension: No Extension

.001 .... = Nature of number: International Number (0x01)

0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)

Address digits:

## sendRoutingInfoForSM

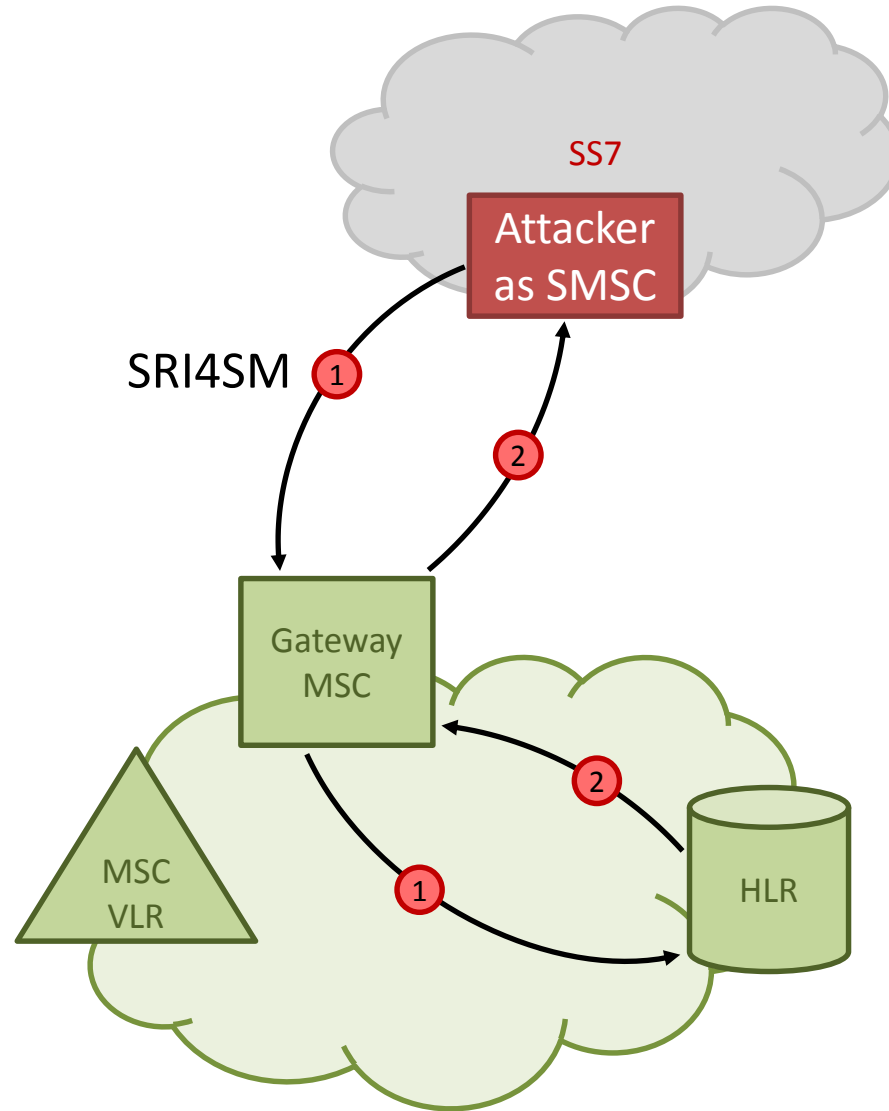
I am HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

# Collect info

B



We know

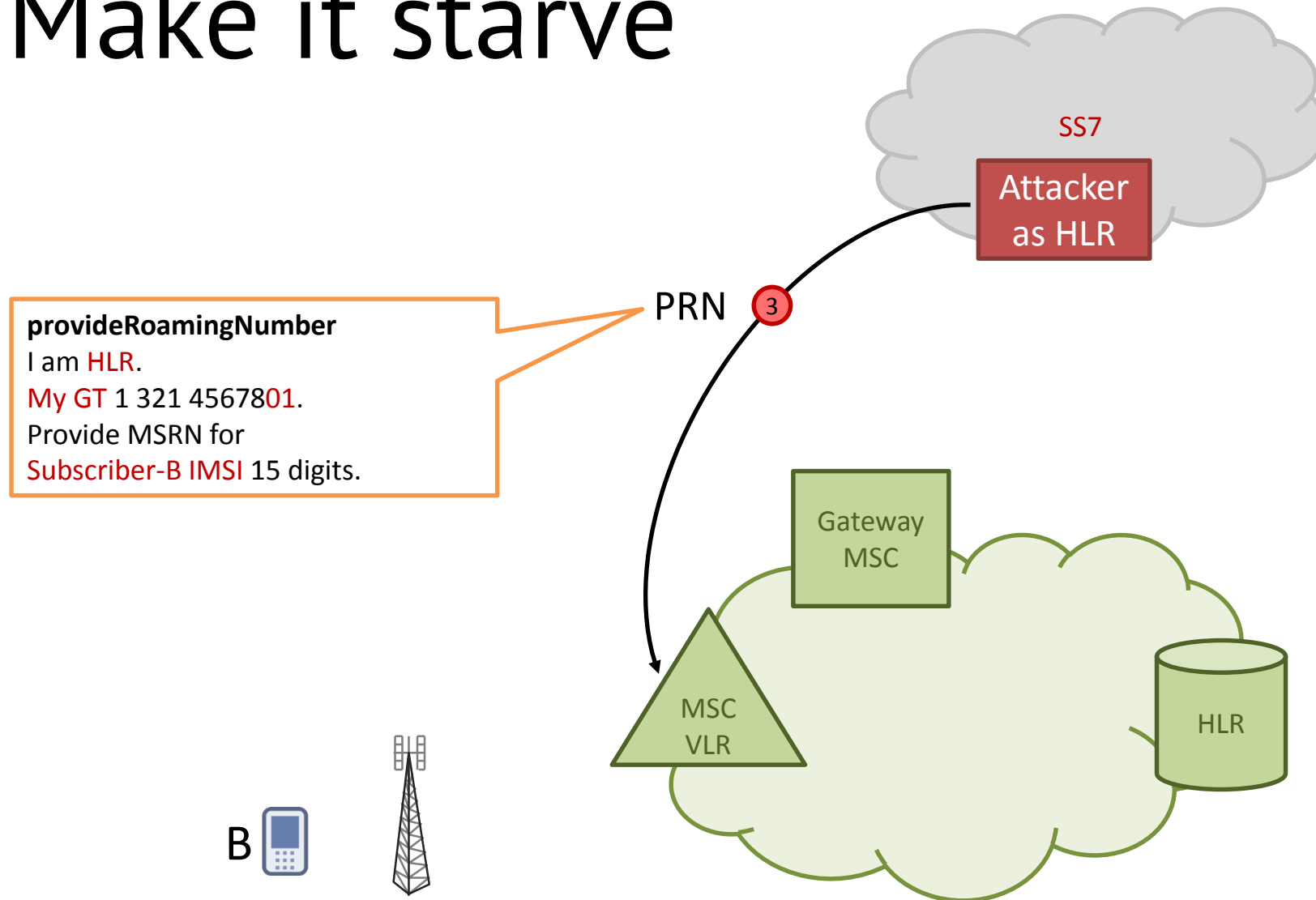
B-Number 0 123 4567802

HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

# Make it starve

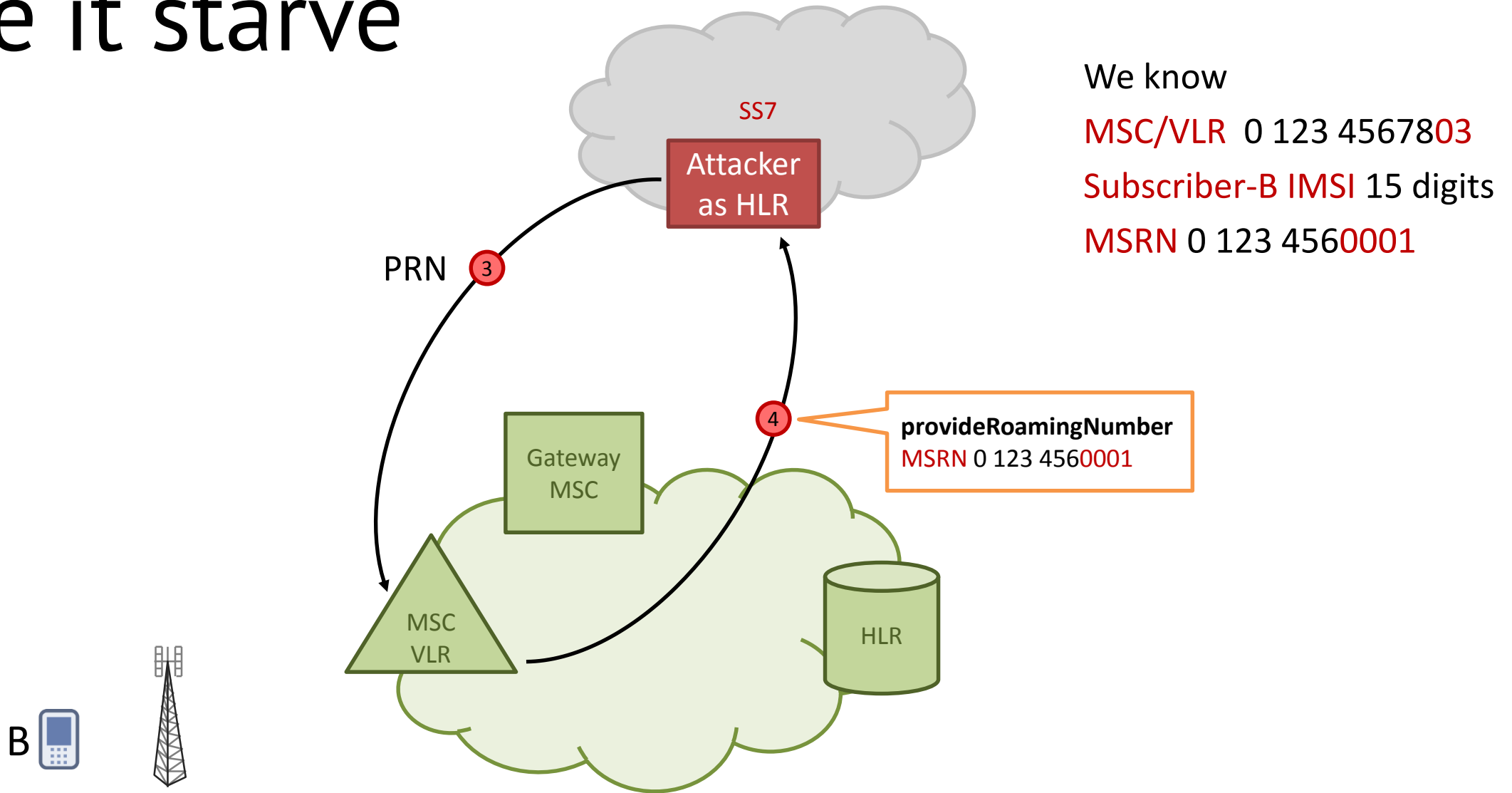


We know

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

# Make it starve

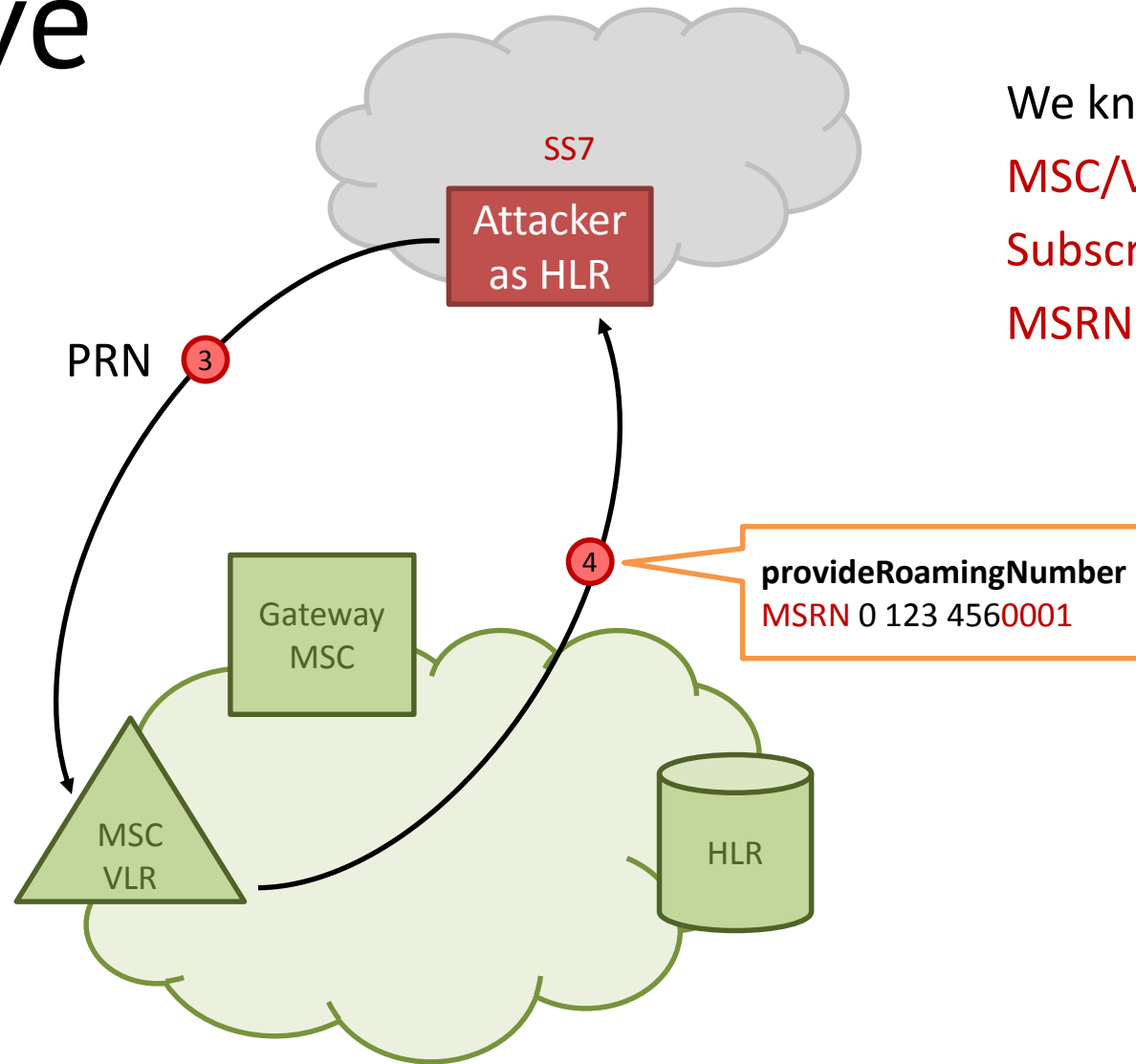


# Make it starve

Default timeouts for MSRN:

- Ericsson – 30 sec
- Huawei – 45 sec

B 



We know

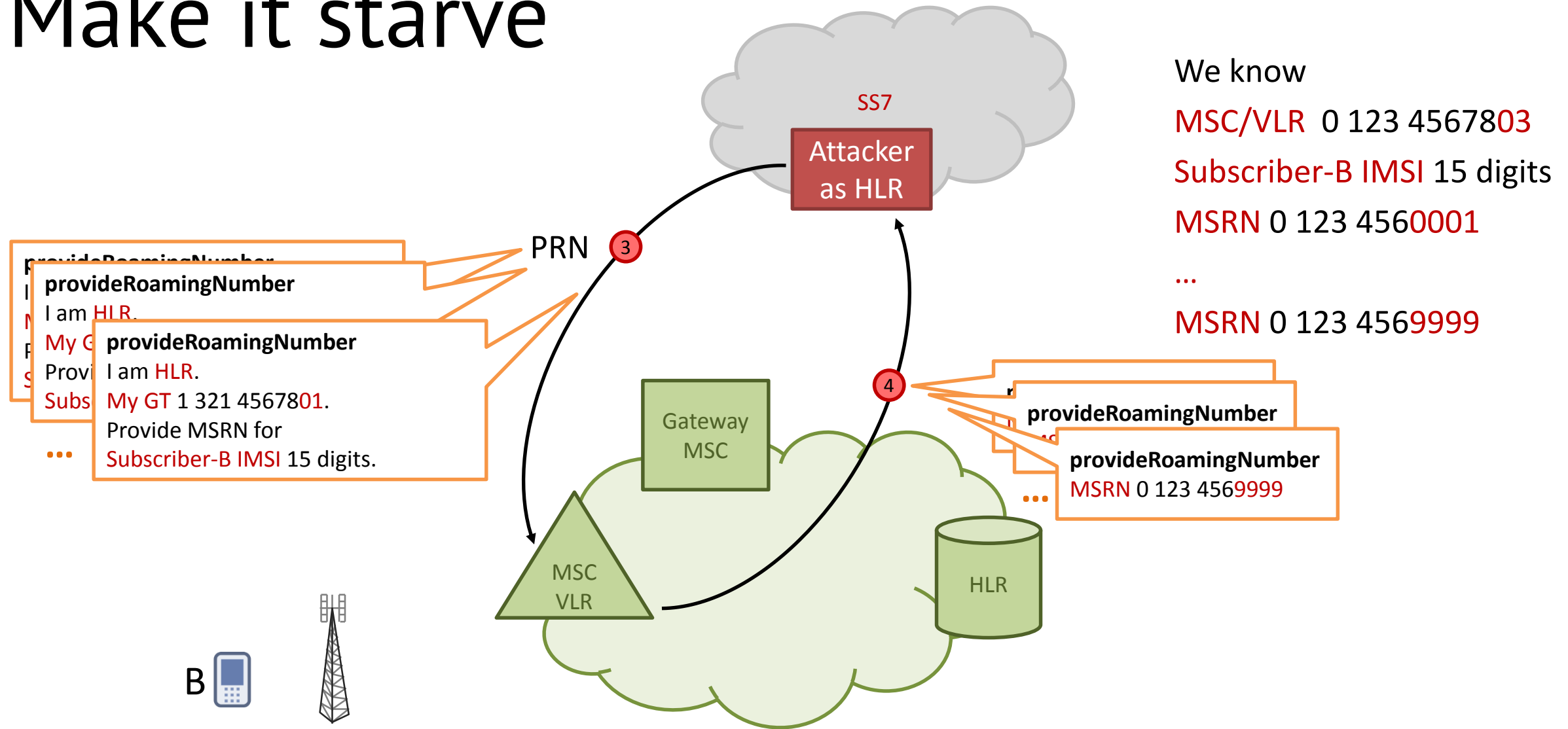
MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

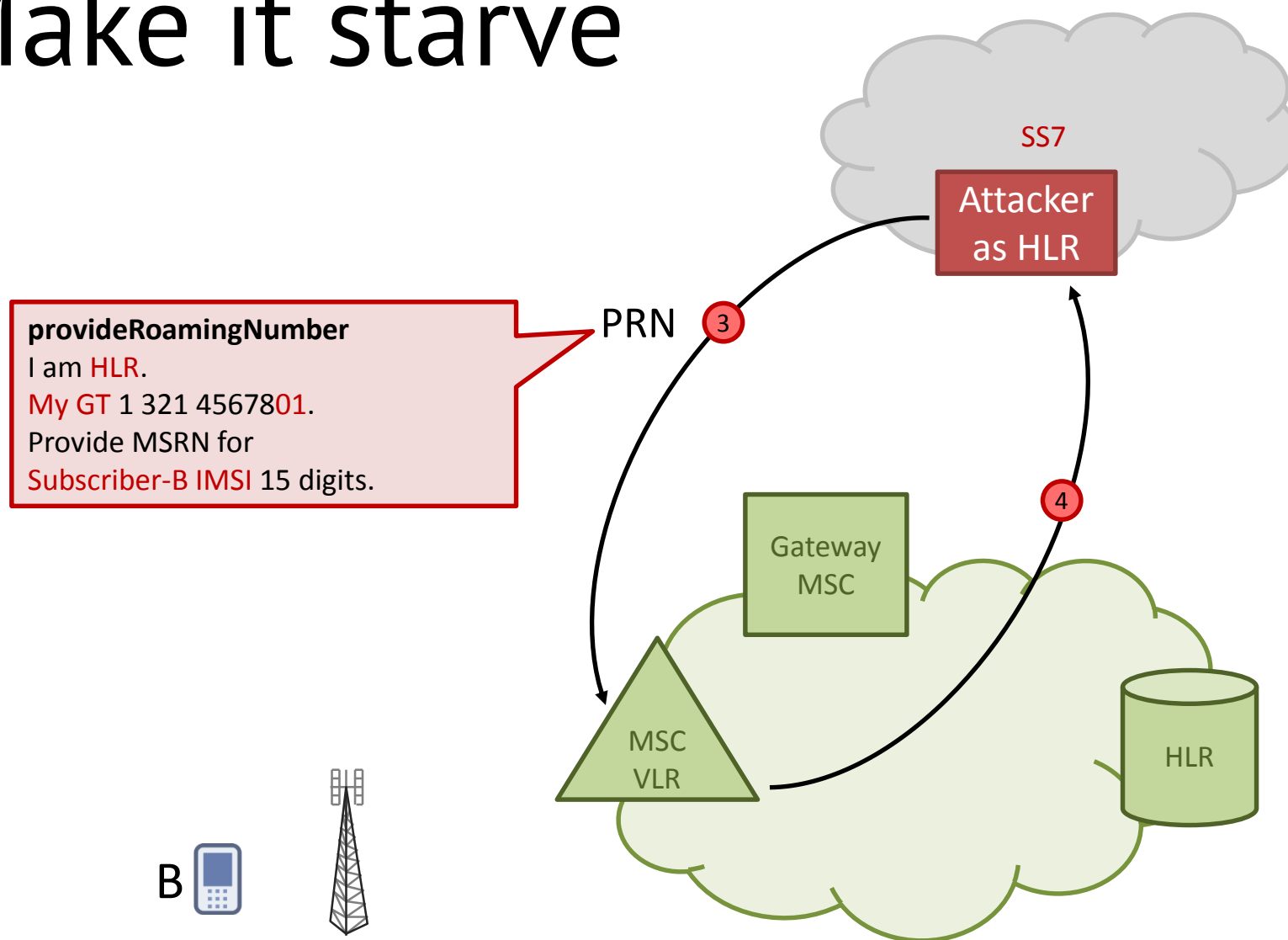
MSRN 0 123 4560001



# Make it starve



# Make it starve



We know

**MSC/VLR 0 123 4567803**

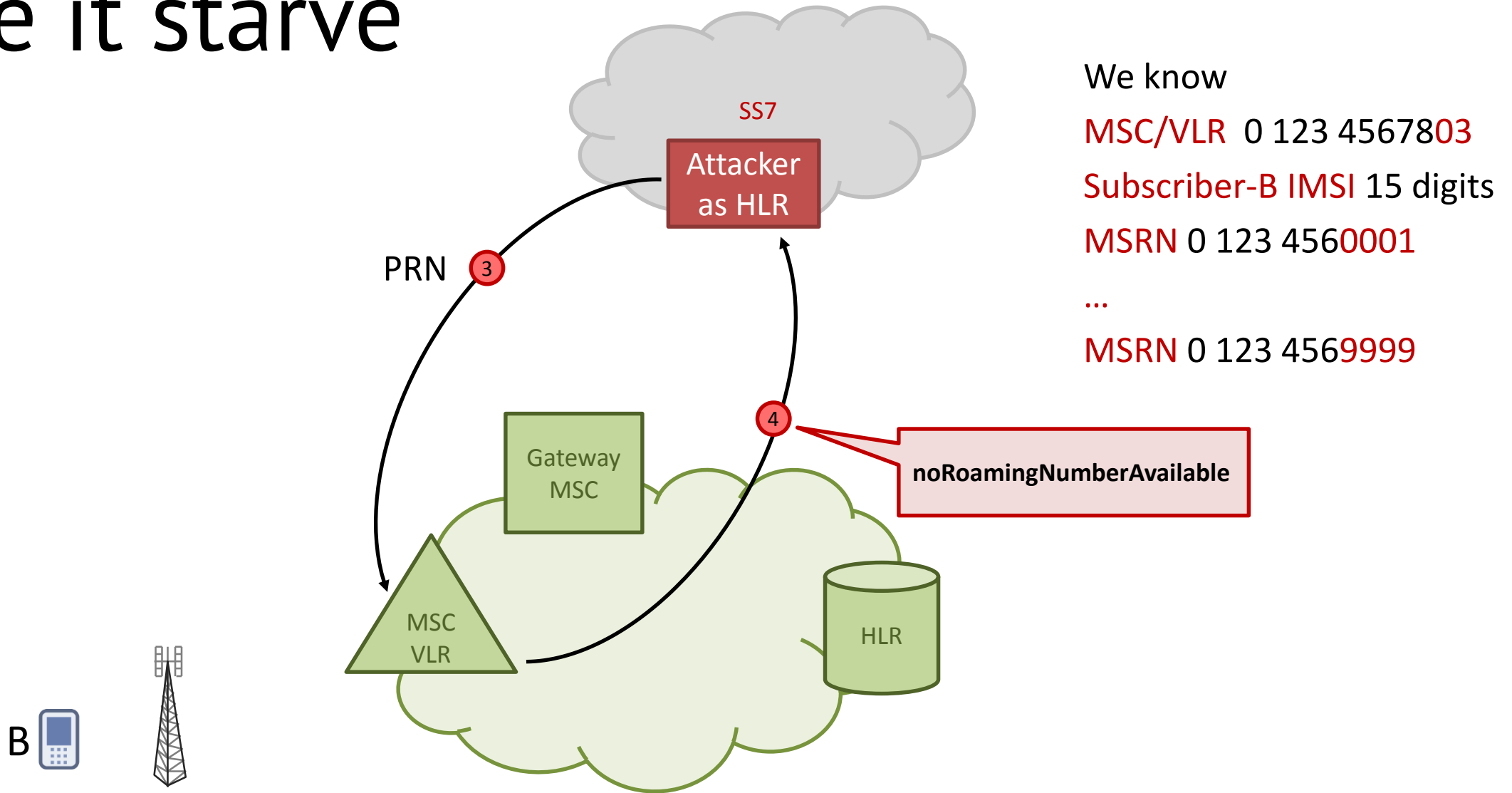
**Subscriber-B IMSI 15 digits**

**MSRN 0 123 4560001**

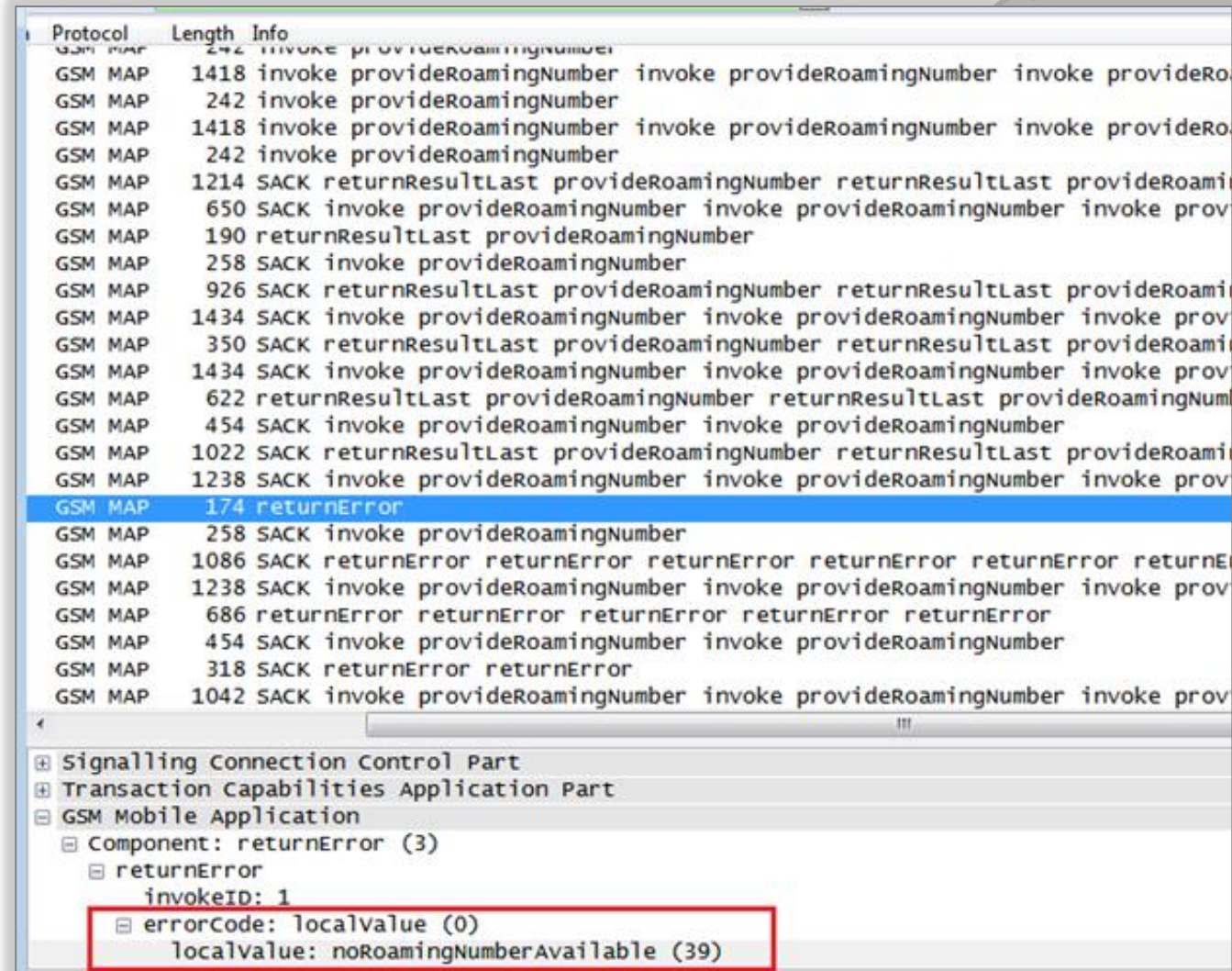
...

**MSRN 0 123 4569999**

# Make it starve



# Make it starve



Protocol	Length	Info
GSM MAP	242	invoke provideRoamingNumber
GSM MAP	1418	invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	242	invoke provideRoamingNumber
GSM MAP	1418	invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	242	invoke provideRoamingNumber
GSM MAP	1214	SACK returnResultLast provideRoamingNumber returnResultLast provideRoamingNumber
GSM MAP	650	SACK invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	190	returnResultLast provideRoamingNumber
GSM MAP	258	SACK invoke provideRoamingNumber
GSM MAP	926	SACK returnResultLast provideRoamingNumber returnResultLast provideRoamingNumber
GSM MAP	1434	SACK invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	350	SACK returnResultLast provideRoamingNumber returnResultLast provideRoamingNumber
GSM MAP	1434	SACK invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	622	returnResultLast provideRoamingNumber returnResultLast provideRoamingNumber
GSM MAP	454	SACK invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	1022	SACK returnResultLast provideRoamingNumber returnResultLast provideRoamingNumber
GSM MAP	1238	SACK invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	174	returnError
GSM MAP	258	SACK invoke provideRoamingNumber
GSM MAP	1086	SACK returnError returnError returnError returnError returnError returnError
GSM MAP	1238	SACK invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	686	returnError returnError returnError returnError returnError
GSM MAP	454	SACK invoke provideRoamingNumber invoke provideRoamingNumber
GSM MAP	318	SACK returnError returnError
GSM MAP	1042	SACK invoke provideRoamingNumber invoke provideRoamingNumber invoke provideRoamingNumber

Signalling Connection Control Part

Transaction Capabilities Application Part

GSM Mobile Application

- Component: returnError (3)
  - returnError
    - invokeID: 1
      - errorCode: localValue (0)
        - localValue: noRoamingNumberAvailable (39)

We know

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

MSRN 0 123 4560001

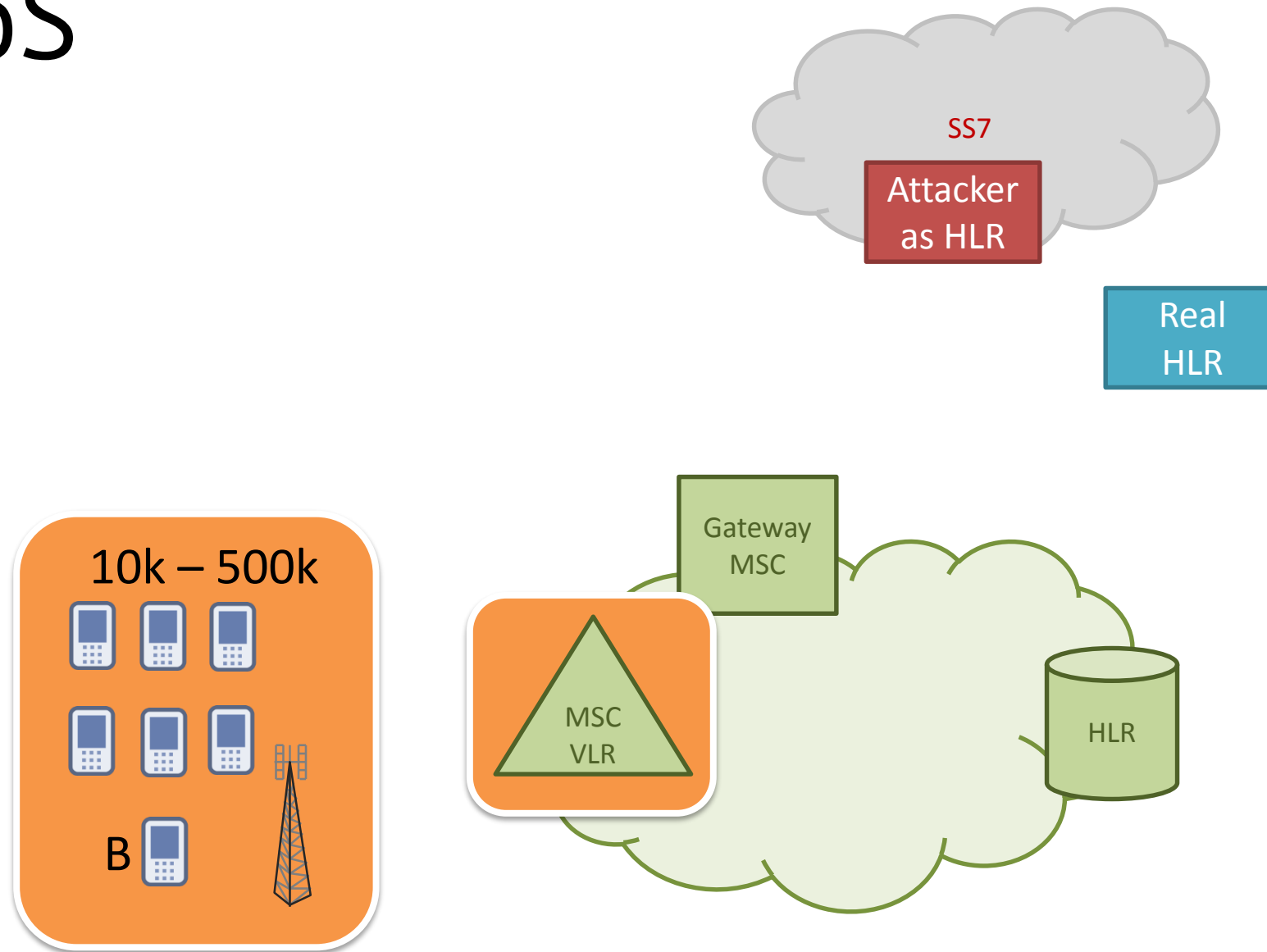
...

MSRN 0 123 4569999

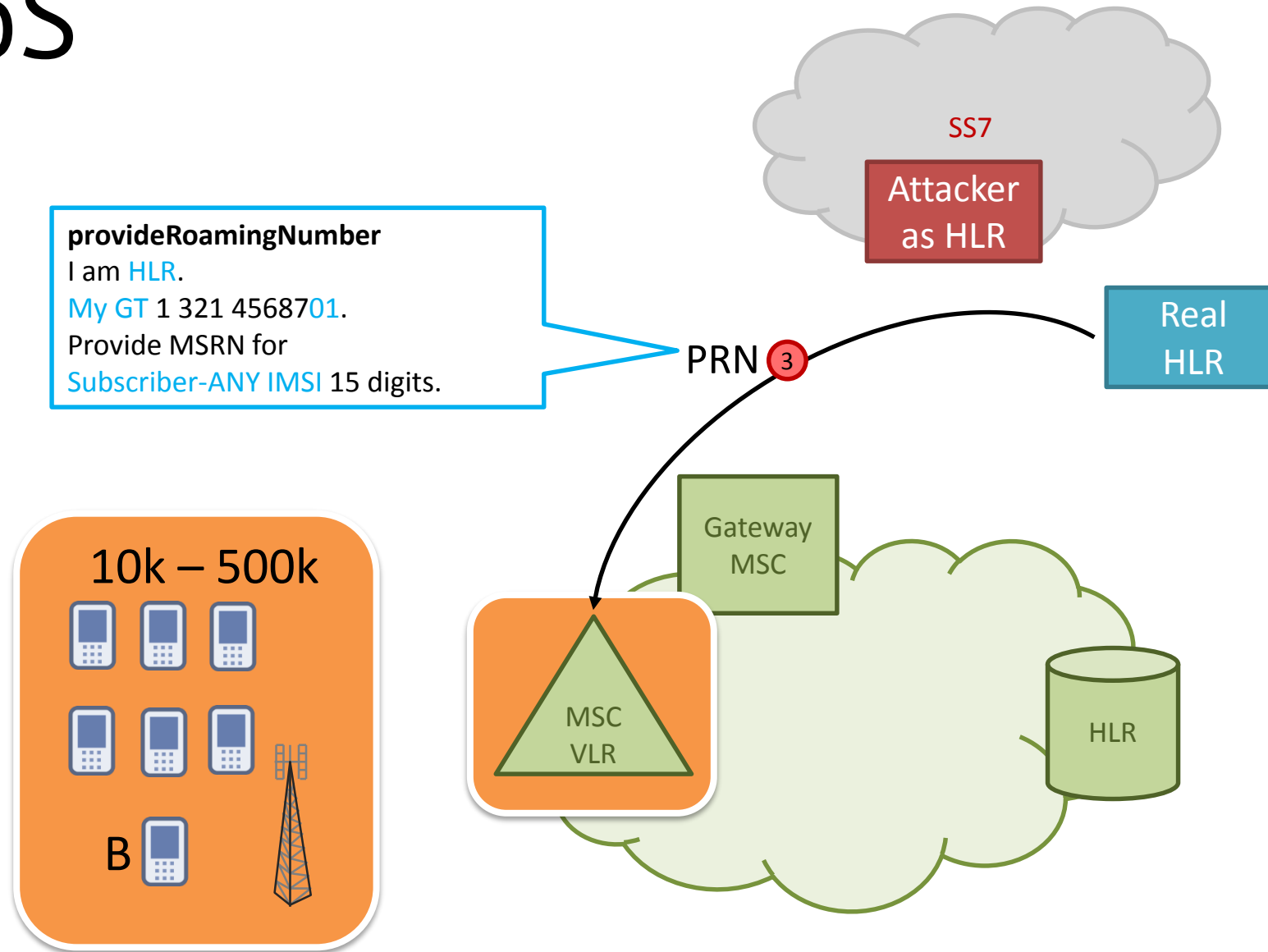
noRoamingNumberAvailable

HLR

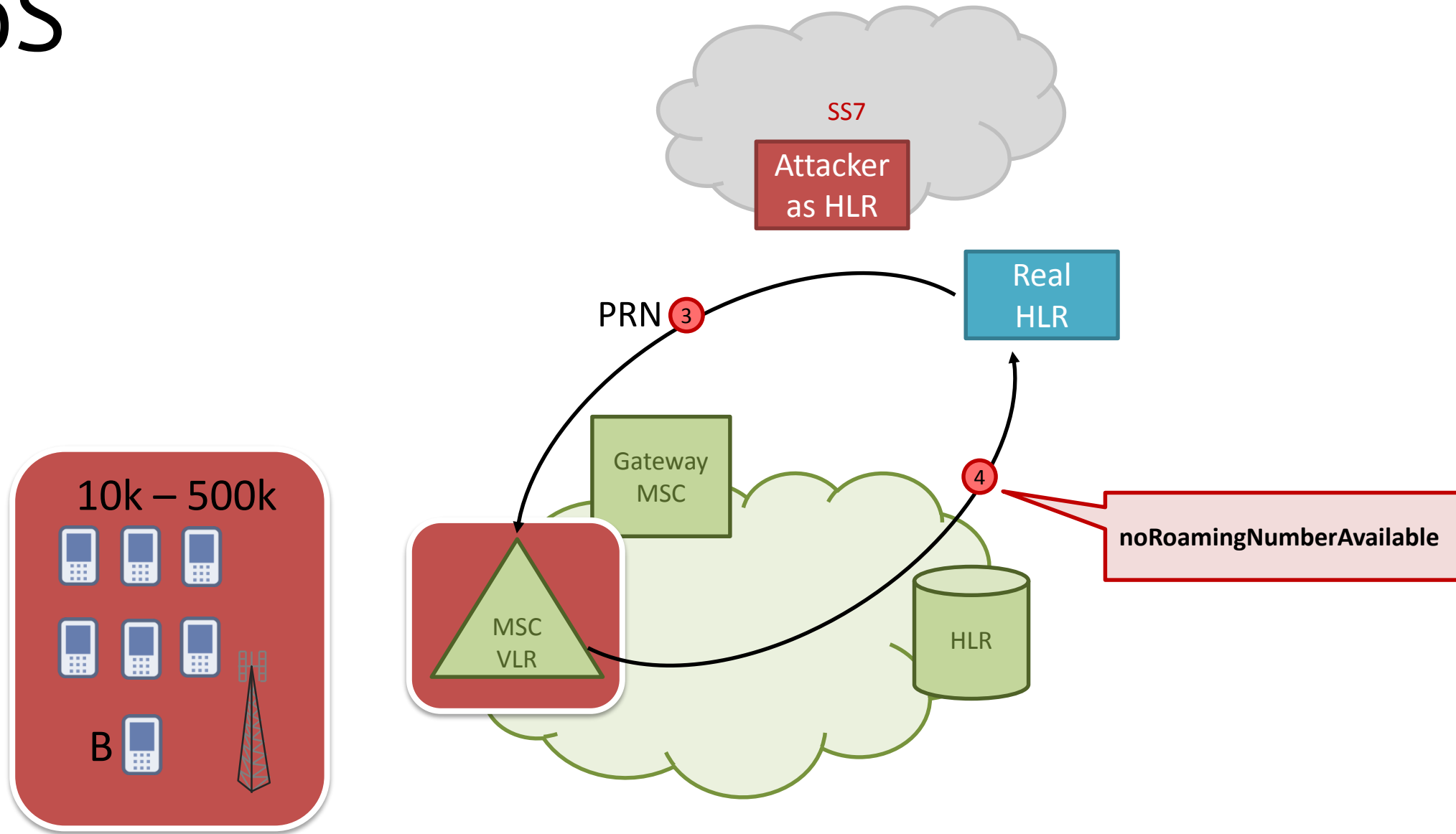
# DoS



# DoS



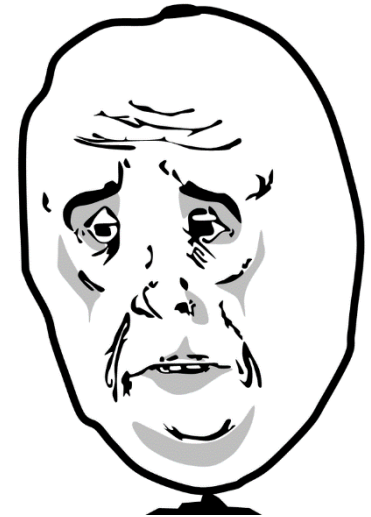
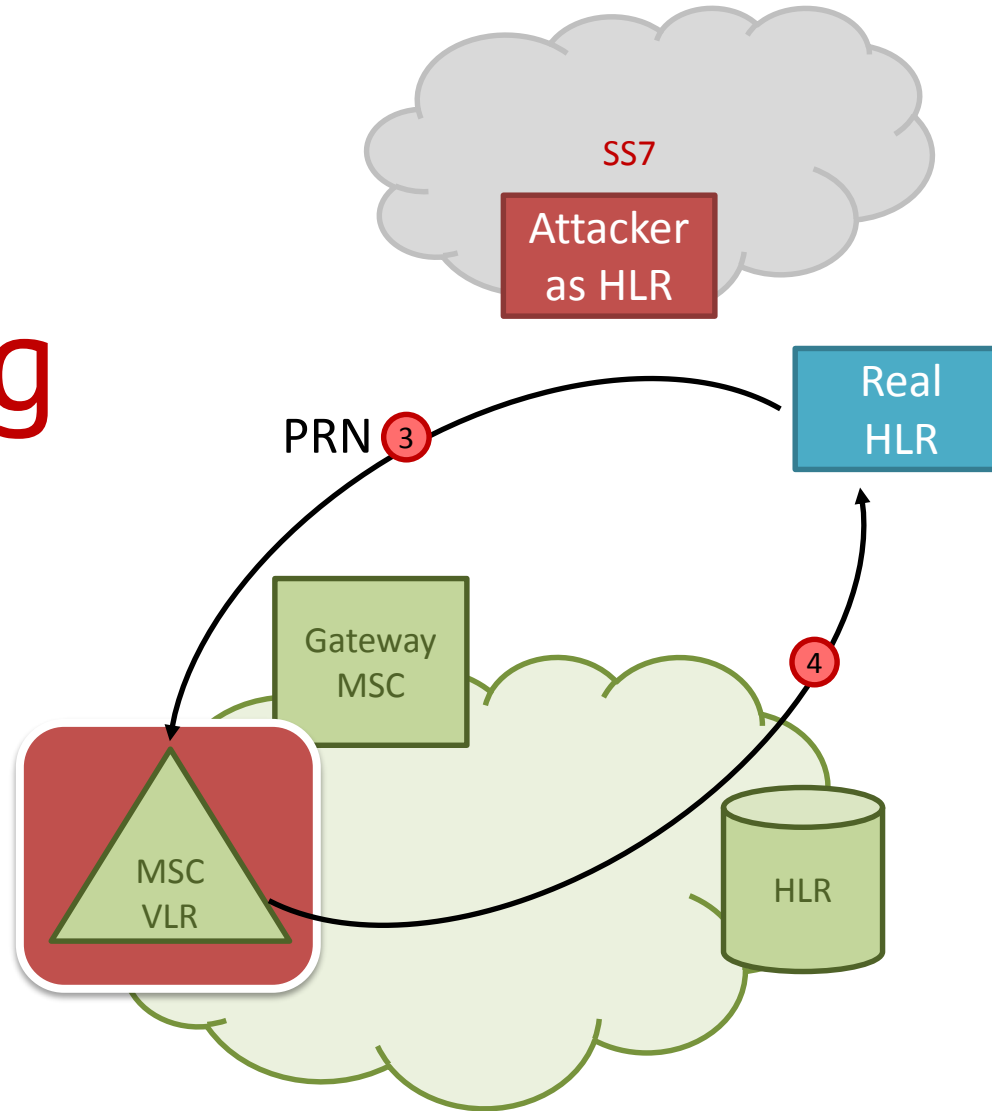
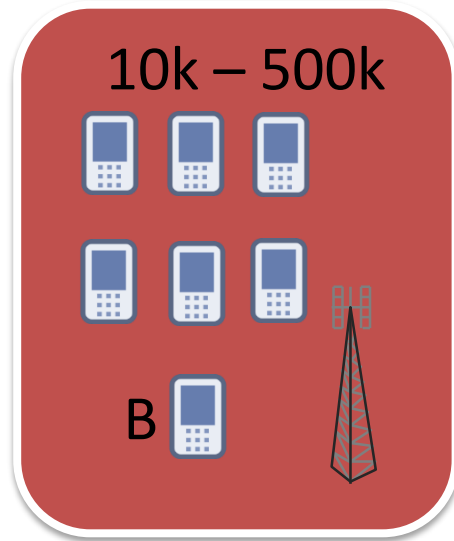
# DoS





# DoS

## No incoming calls

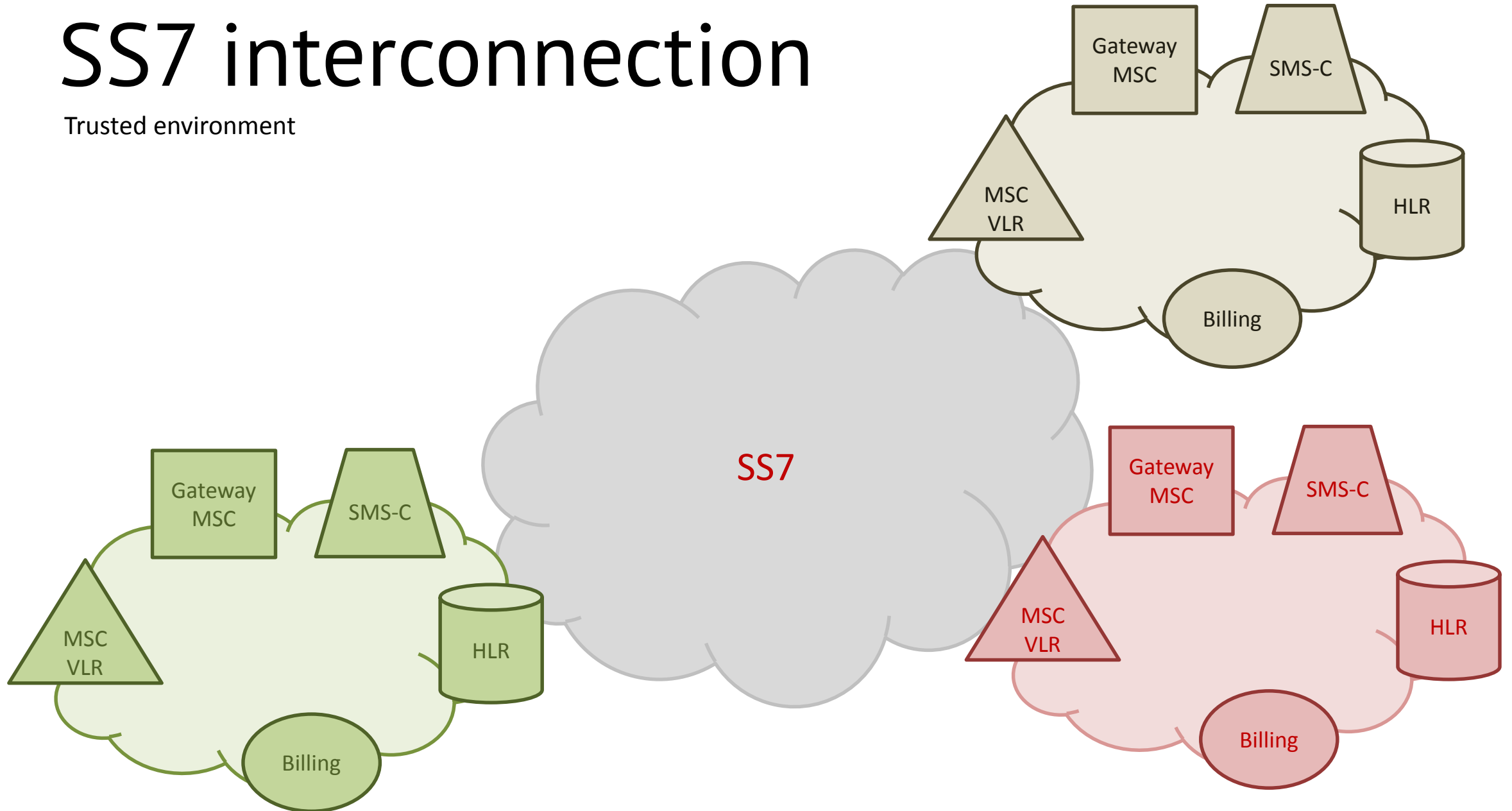


Sad calling party

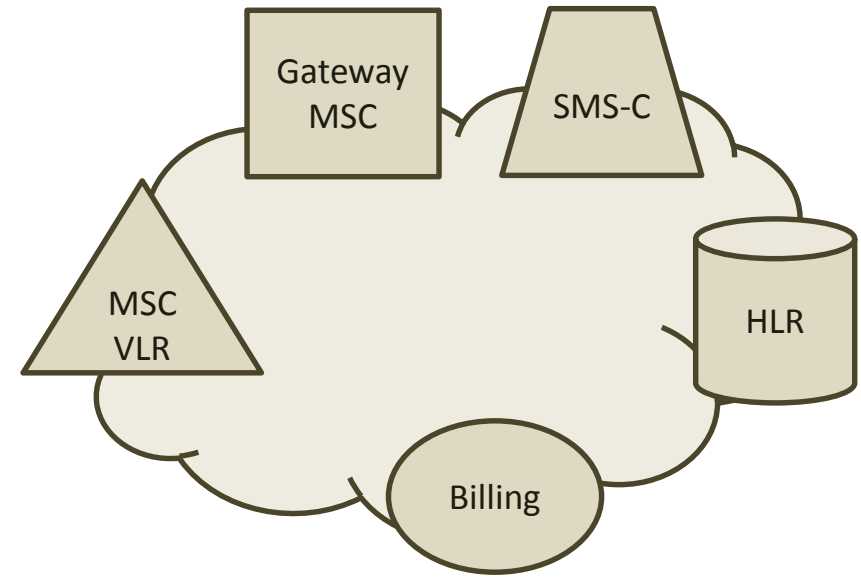
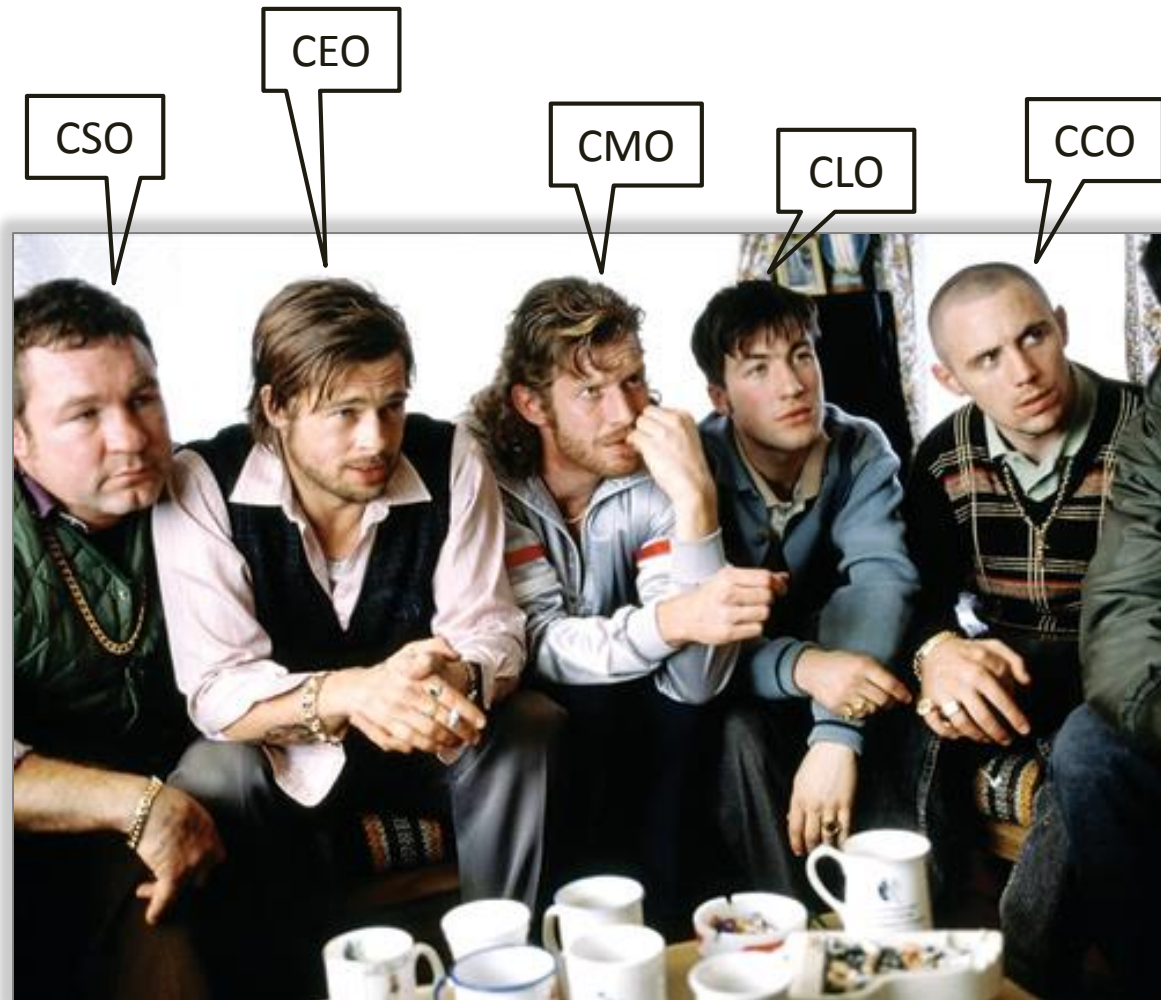
# Fraud in SS7

# SS7 interconnection

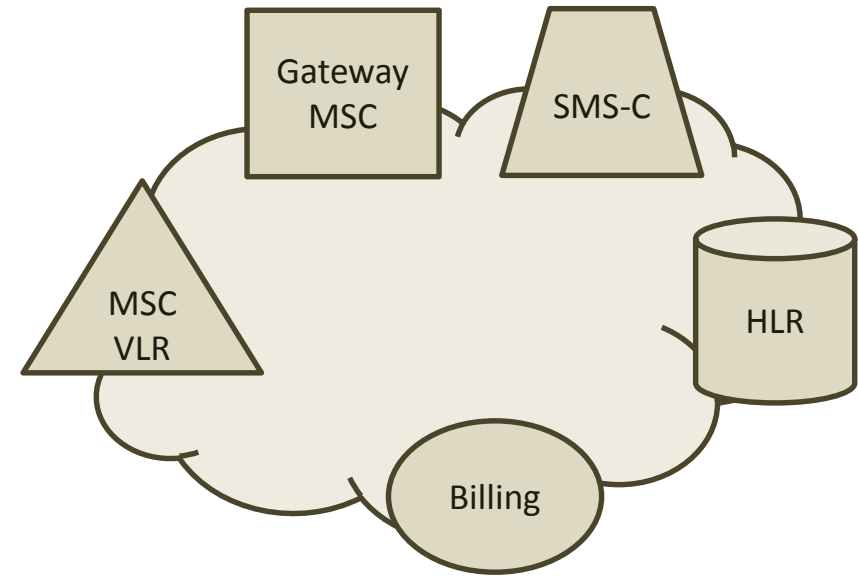
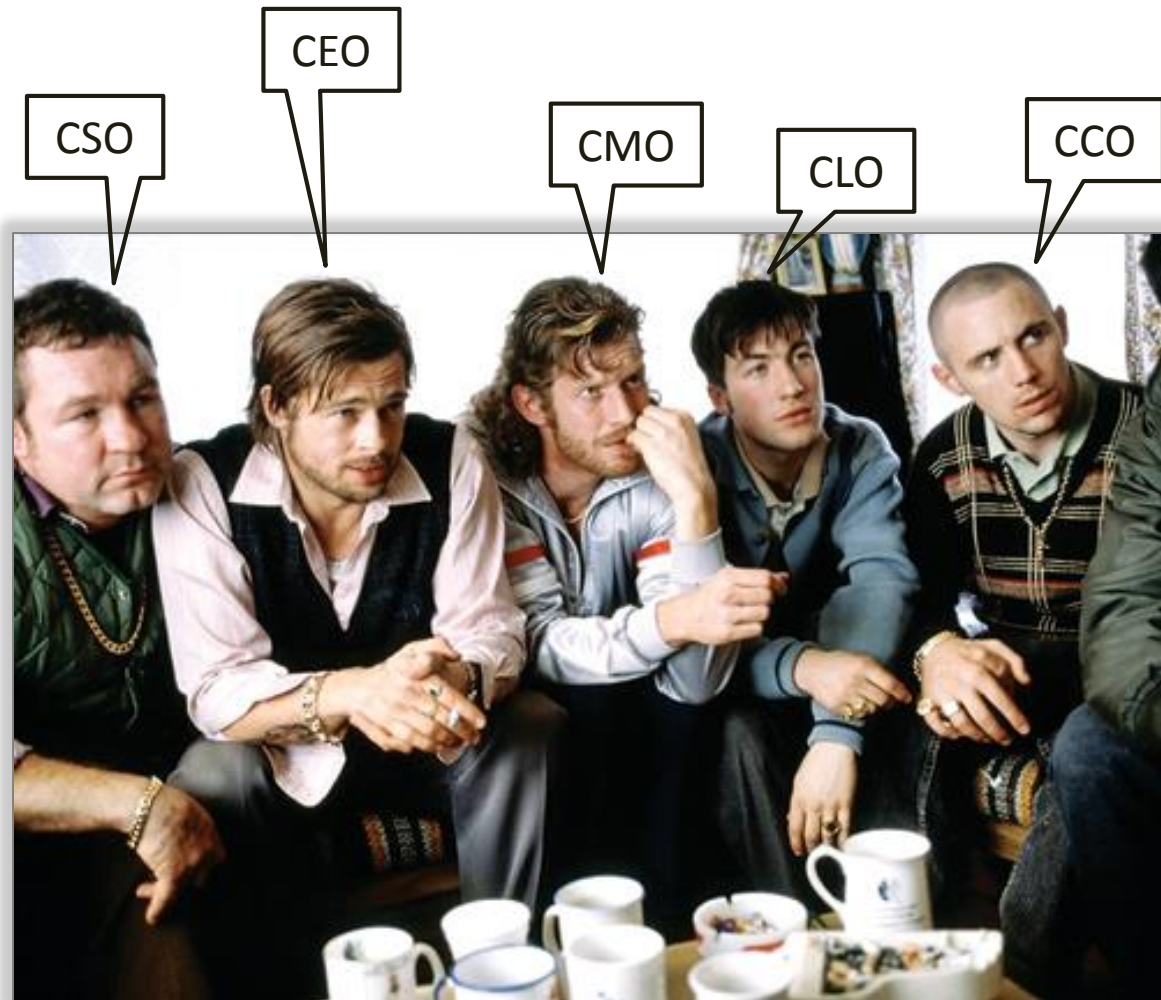
Trusted environment



# Leadership team



# Leadership team

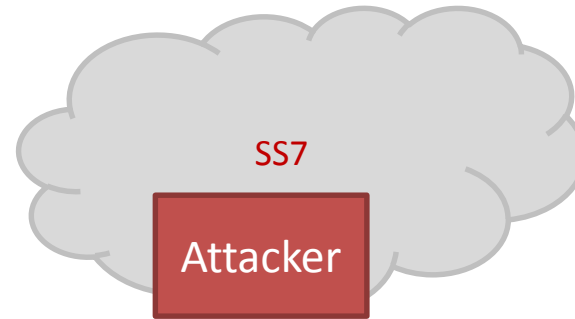


Really?!  
Trust them?

# Uncharged calls

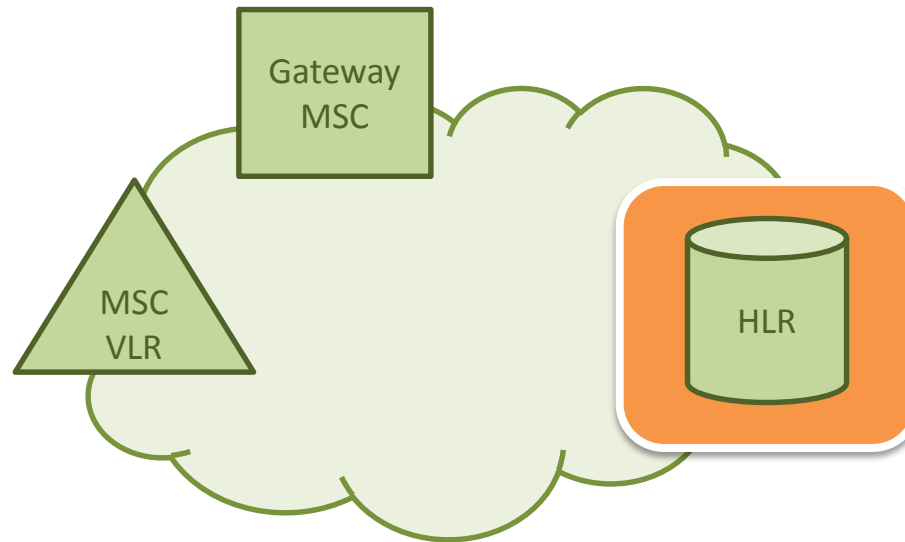
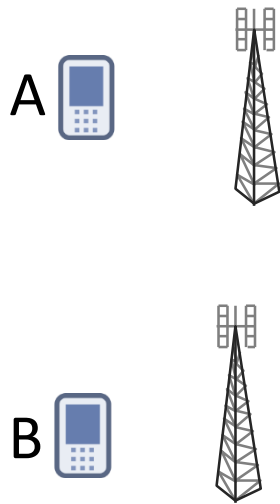
- 1) Spoof MSC
- 2) Initiate «home network» call
- 3) Forward call anywhere

# Collect info



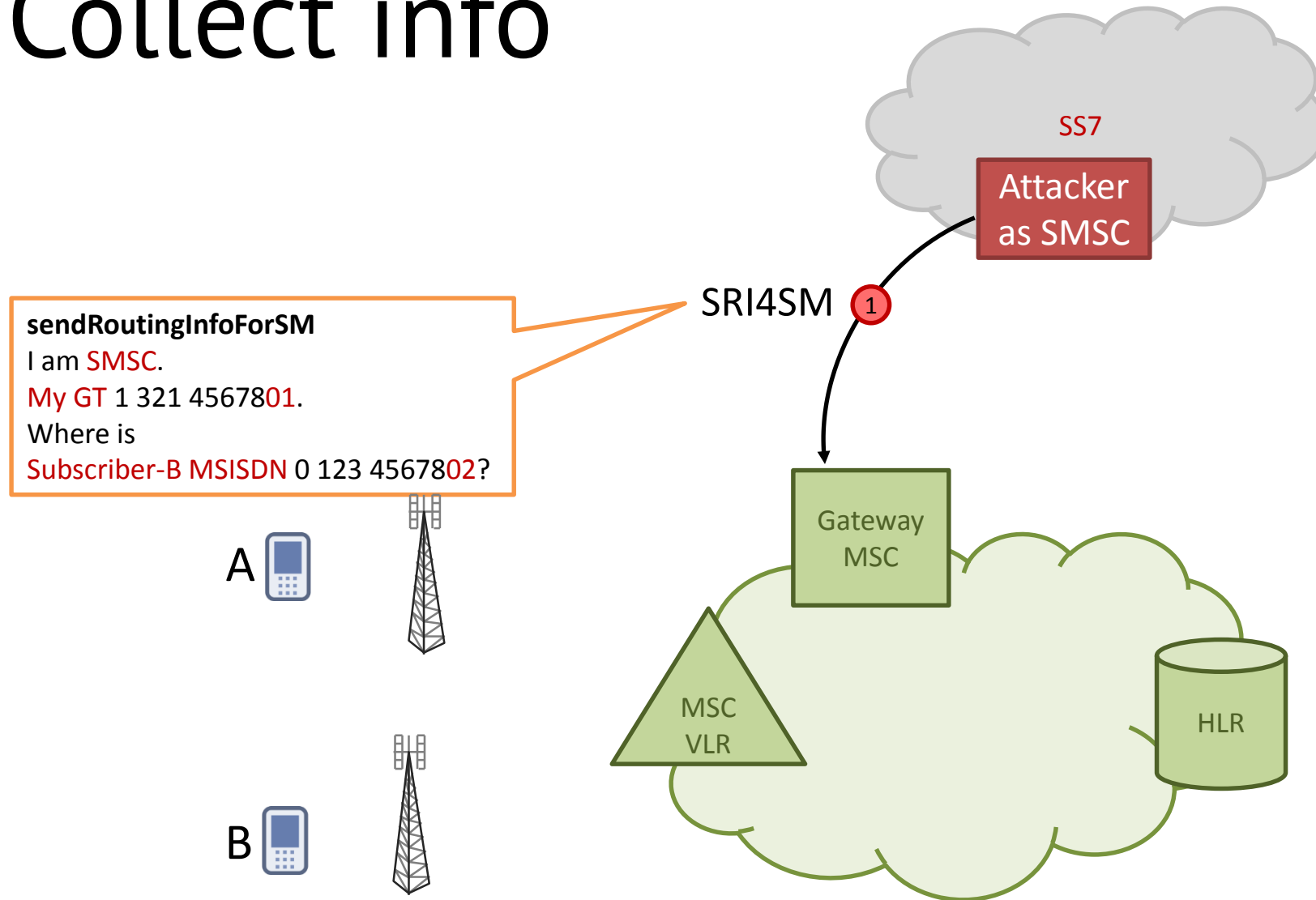
We know

**B-Number** 0 123 45678**02**





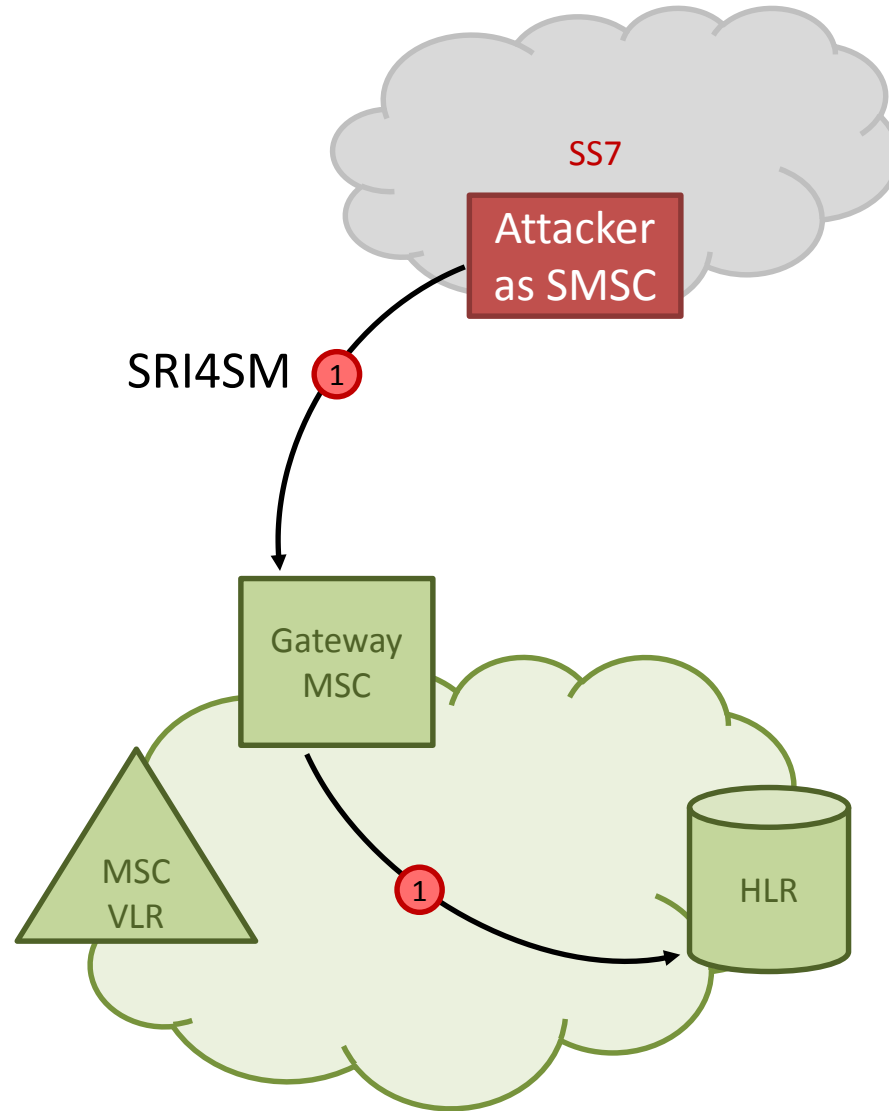
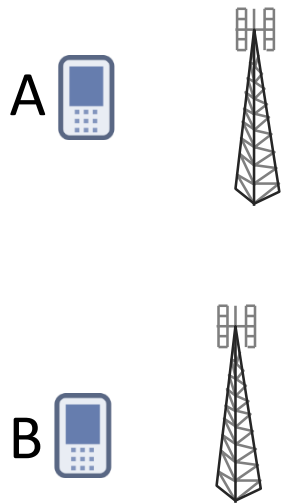
# Collect info



We know

**B-Number** 0 123 4567802

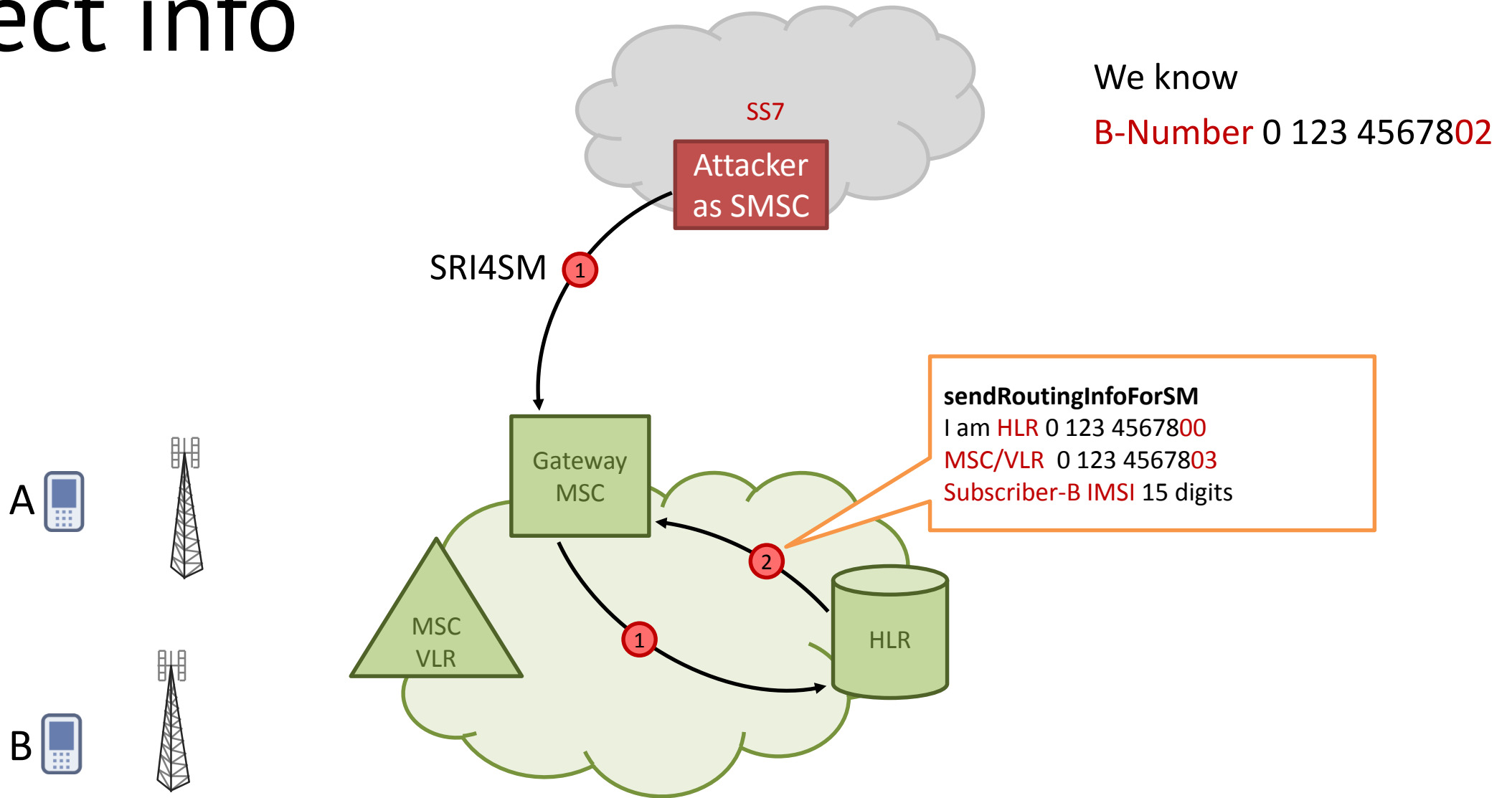
# Collect info



We know

**B-Number** 0 123 45678**02**

# Collect info



# Collect info

We know

**B-Number** 0 123 4567802

Protocol Length Info

GSM MAP 194 invoke sendRoutingInfoForSM

GSM MAP 206 returnResultLast sendRoutingInfoForSM

Called Party address (11 bytes)

Calling Party address (11 bytes)

Address Indicator

SubSystem Number: HLR (Home Location Register) (6)

[Linked to TCAP]

Global Title 0x4 (9 bytes)

Translation Type: 0x00

0001 .... = Numbering Plan: ISDN/telephony (0x01)

.... 0001 = Encoding Scheme: BCD, odd number of digits (0x01)

...000 0100 = Nature of Address Indicator: International number (0x04)

Calling Party Digits: HLR 0 123 4567800

Transaction Capabilities Application Part

GSM Mobile Application

Component: returnResultLast (2)

returnResultLast

invokeID: 1

resultretres

opCode: localValue (0)

imsi: Subscriber-B IMSI 15 digits

TBCD digits:

locationInfoWithLMSI

networkNode-Number: MSC/VLR 0 123 4567803

1... .... = Extension: No Extension

.001 .... = Nature of number: International Number (0x01)

0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)

Address digits:

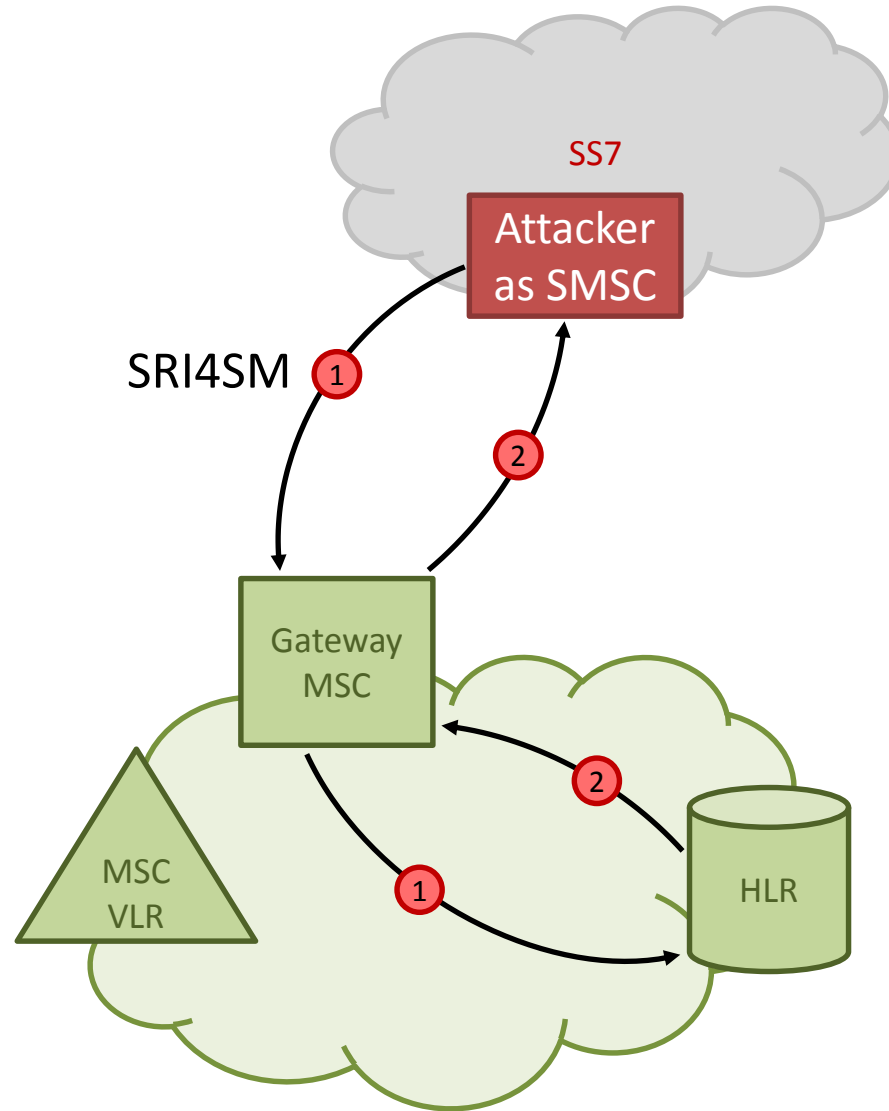
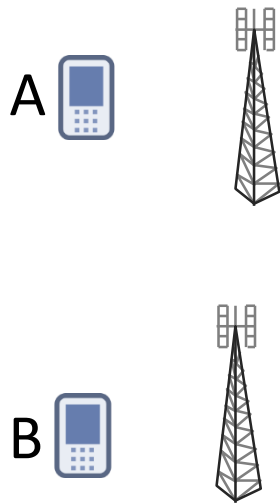
## sendRoutingInfoForSM

I am HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

# Collect info



We know

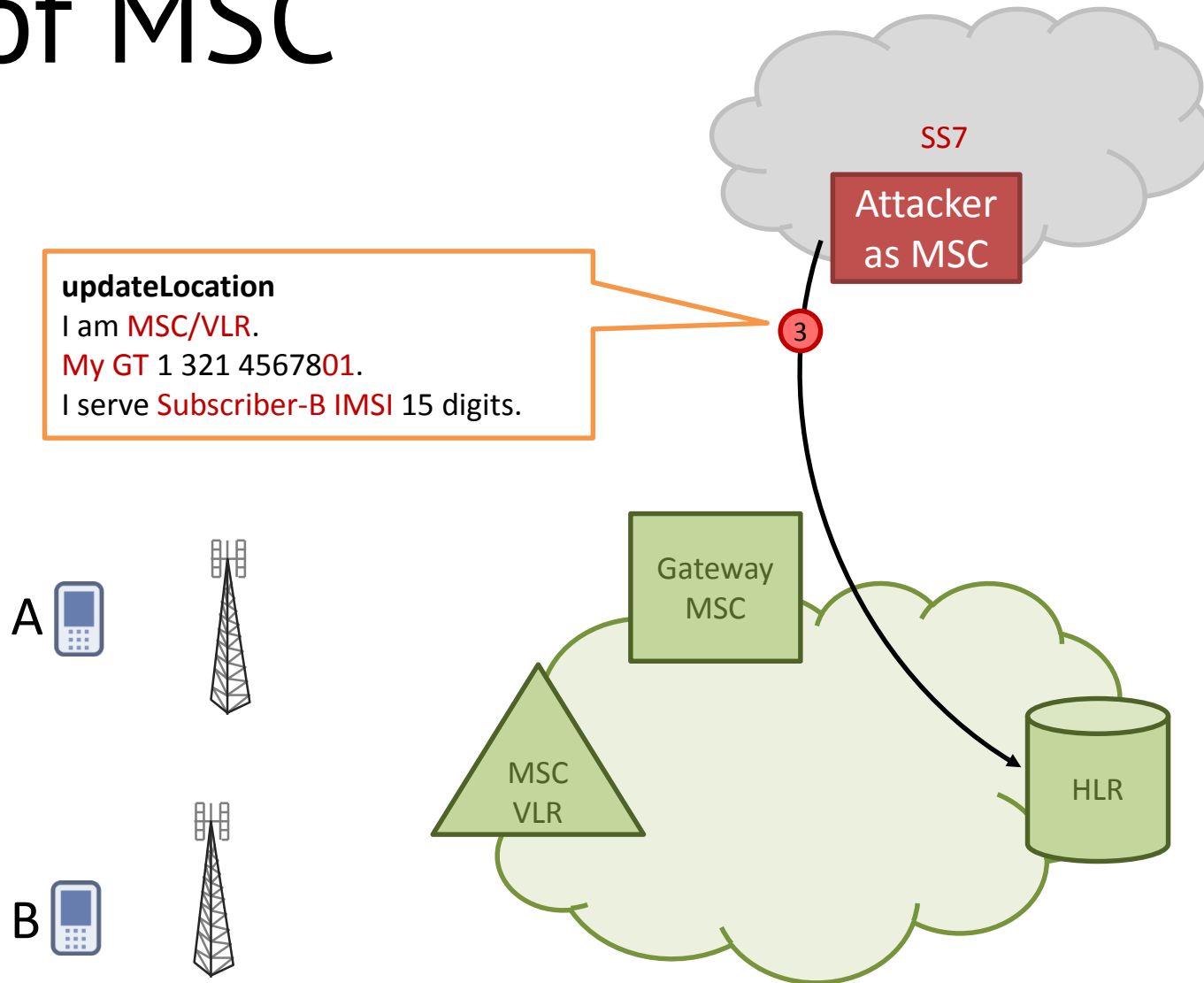
B-Number 0 123 4567802

HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

# Spoof MSC

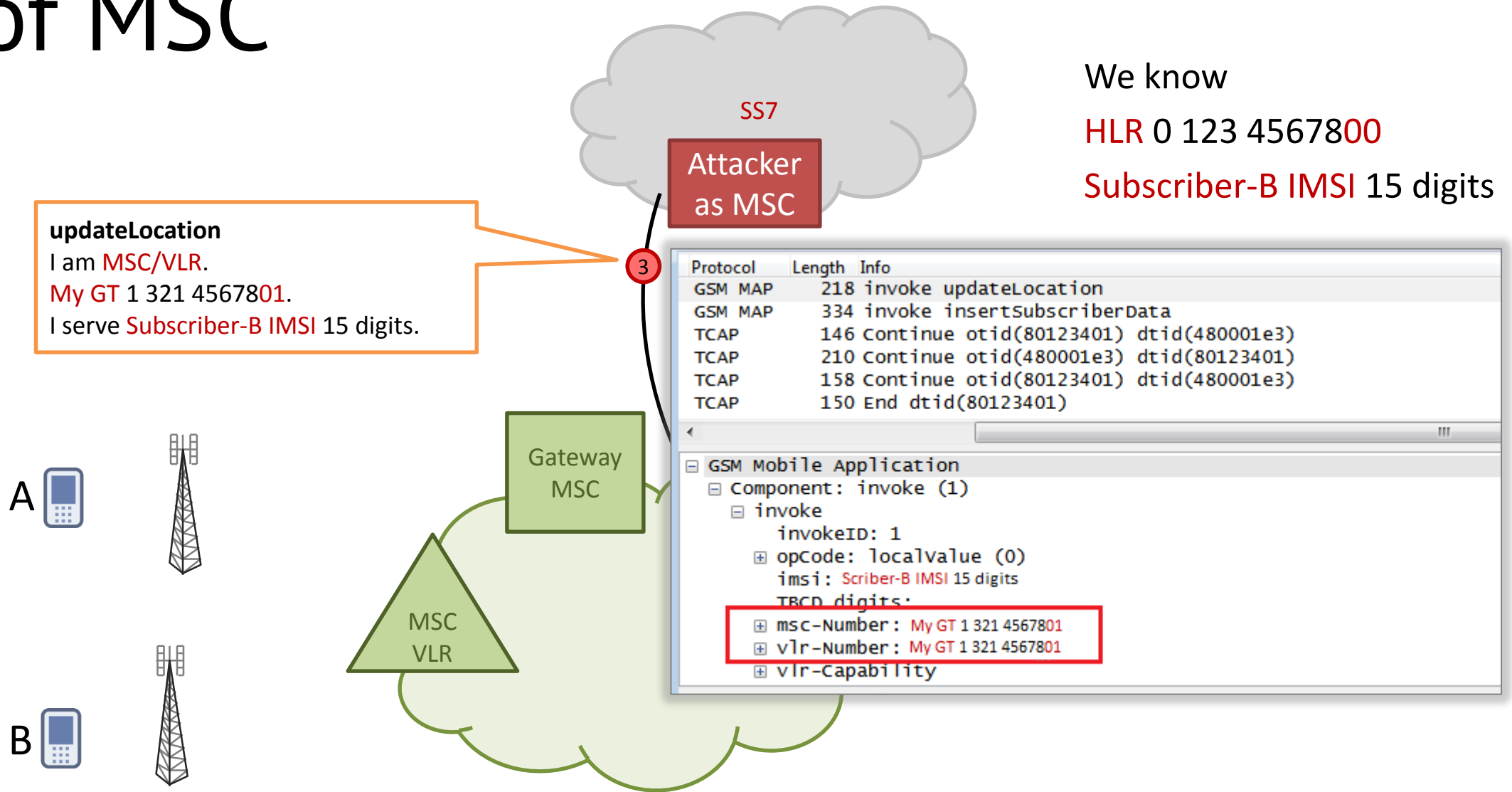


We know

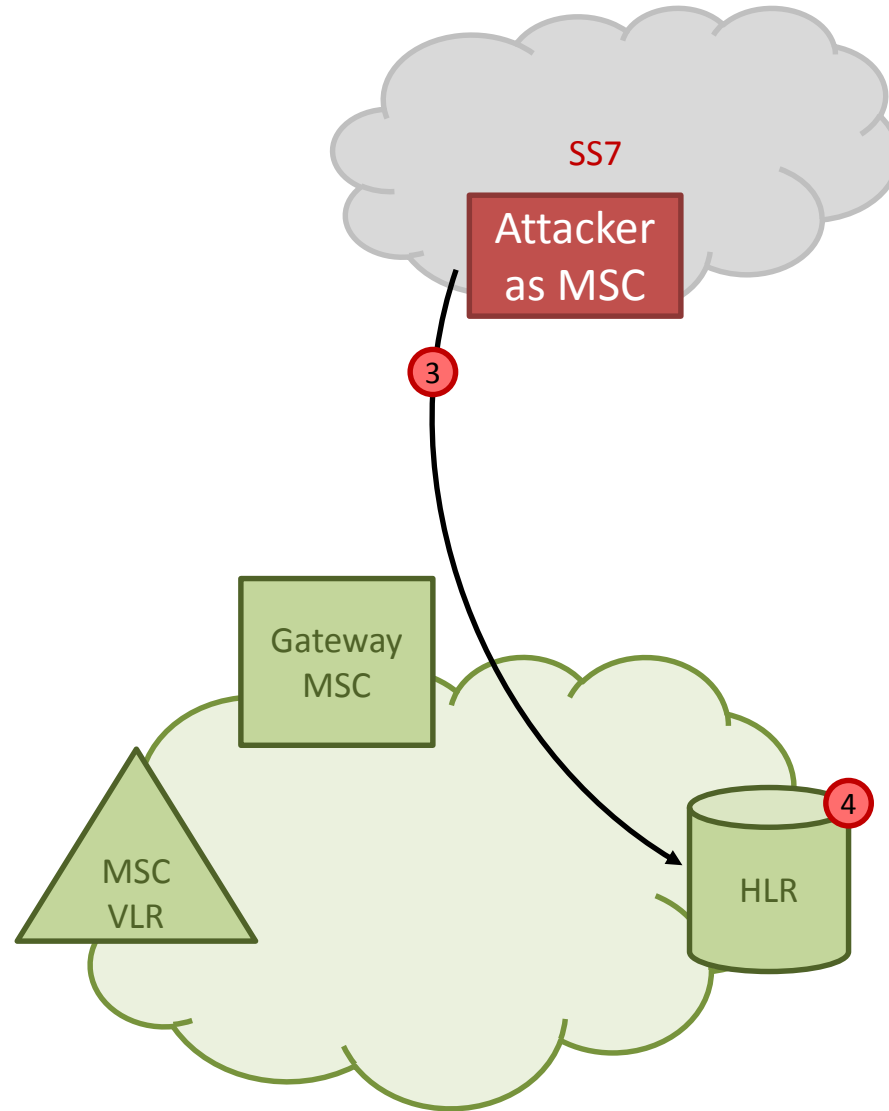
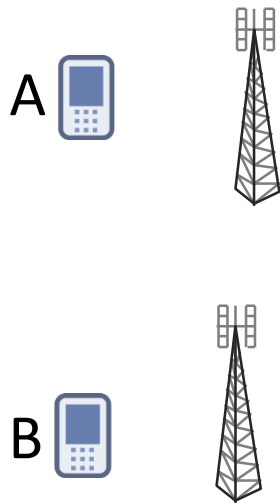
**HLR 0 123 4567800**

**Subscriber-B IMSI 15 digits**

# Spoof MSC



# Spoof MSC



We know

HLR 0 123 4567800

Subscriber-B IMSI 15 digits

HLR stores

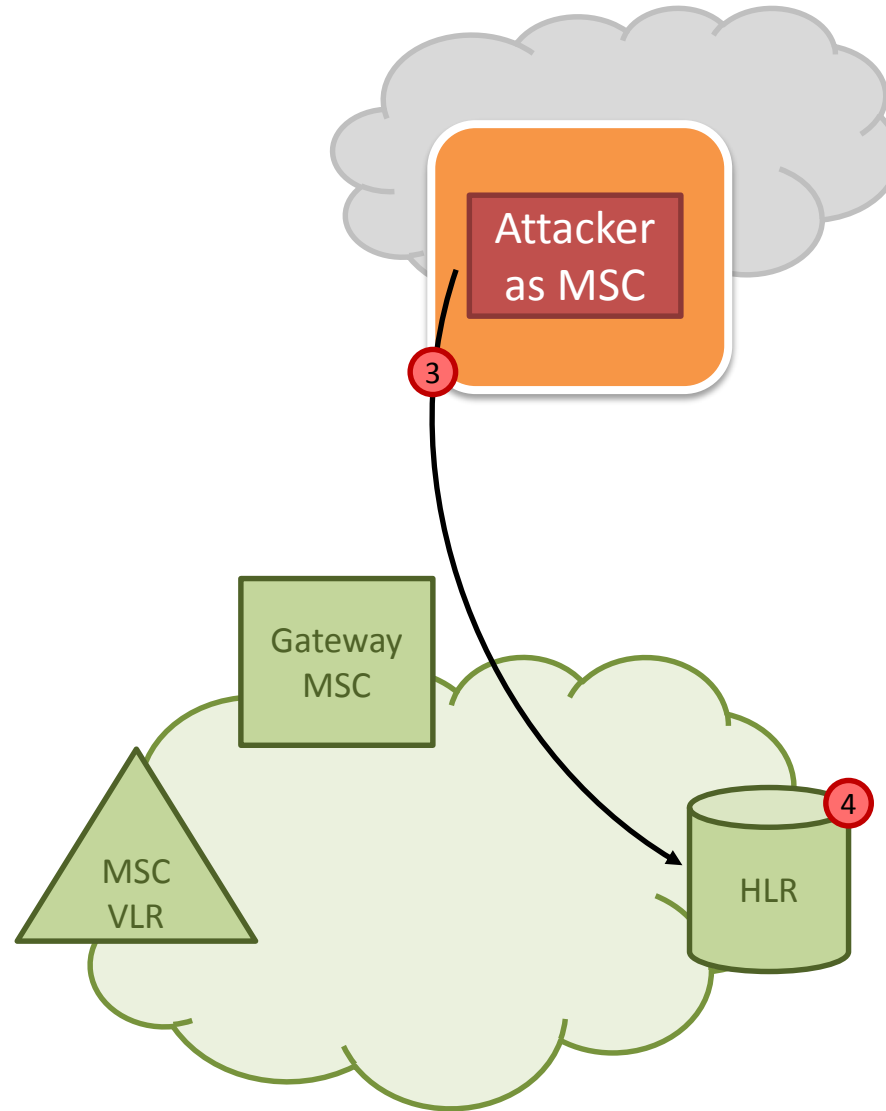
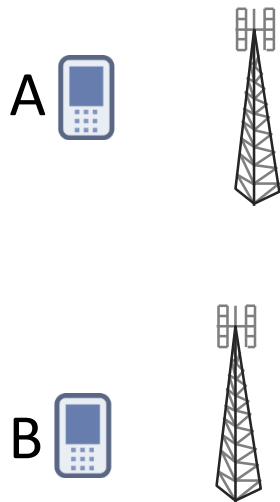
Subscriber-B IMSI 15 digits

MSC/VLR 1 321 4567801



# Spoof MSC

We serve  
Subscriber-B



We know

HLR 0 123 4567800

Subscriber-B IMSI 15 digits

HLR stores

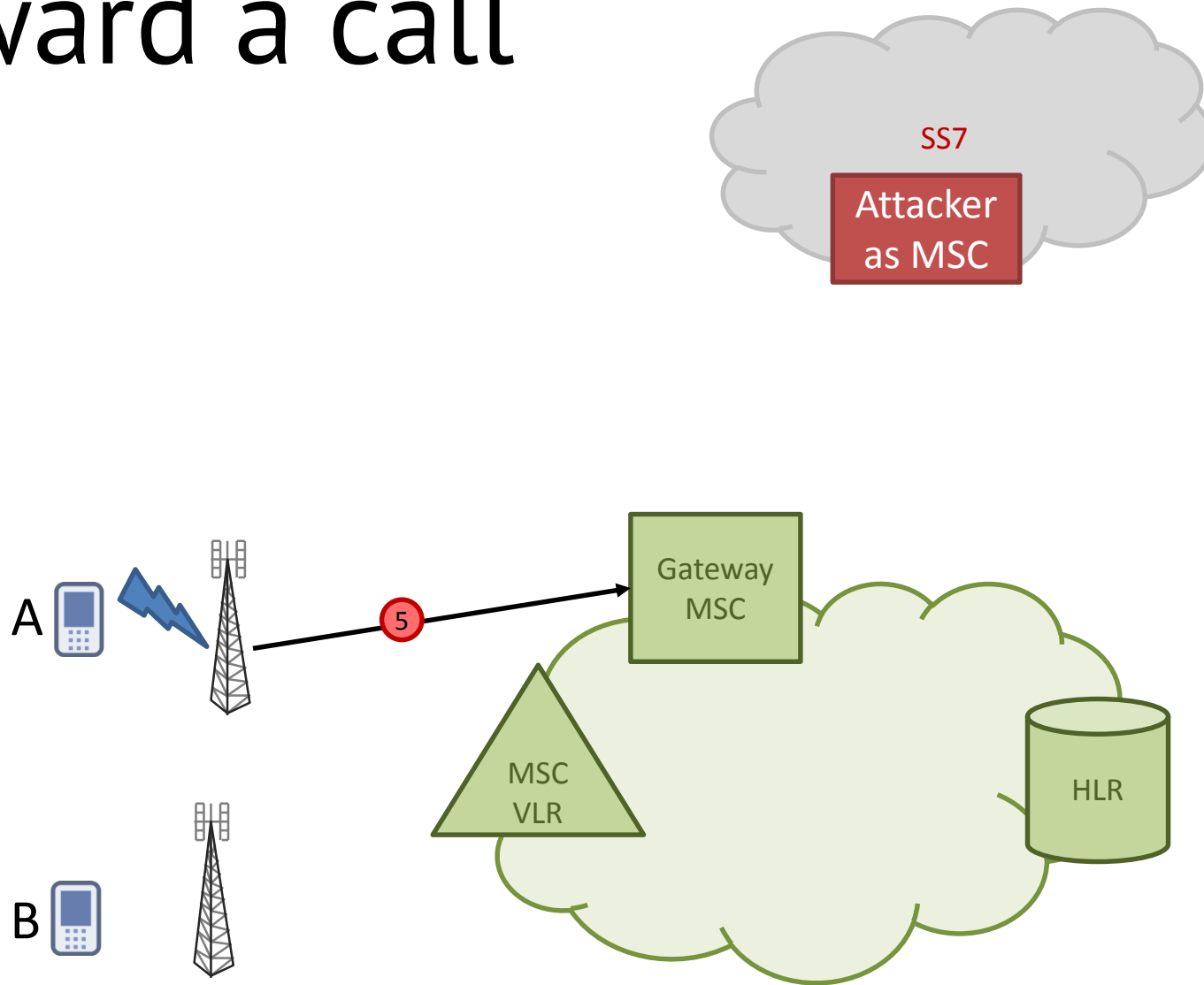
Subscriber-B IMSI 15 digits

MSC/VLR 1 321 4567801



**NOT BAD**

# Forward a call



HLR stores

Subscriber-B

MSISDN 0 123 4567802

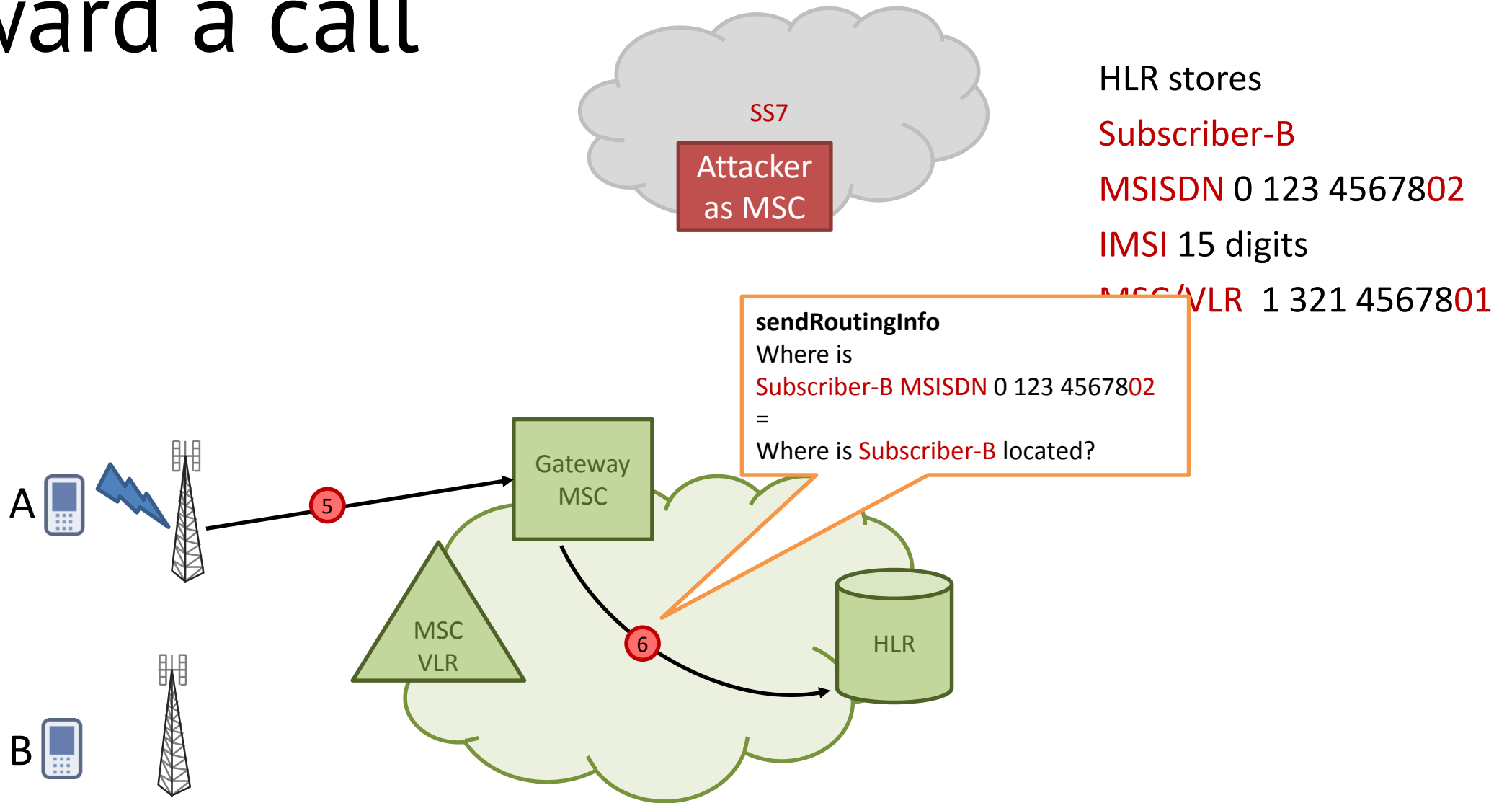
IMSI 15 digits

MSC/VLR 1 321 4567801

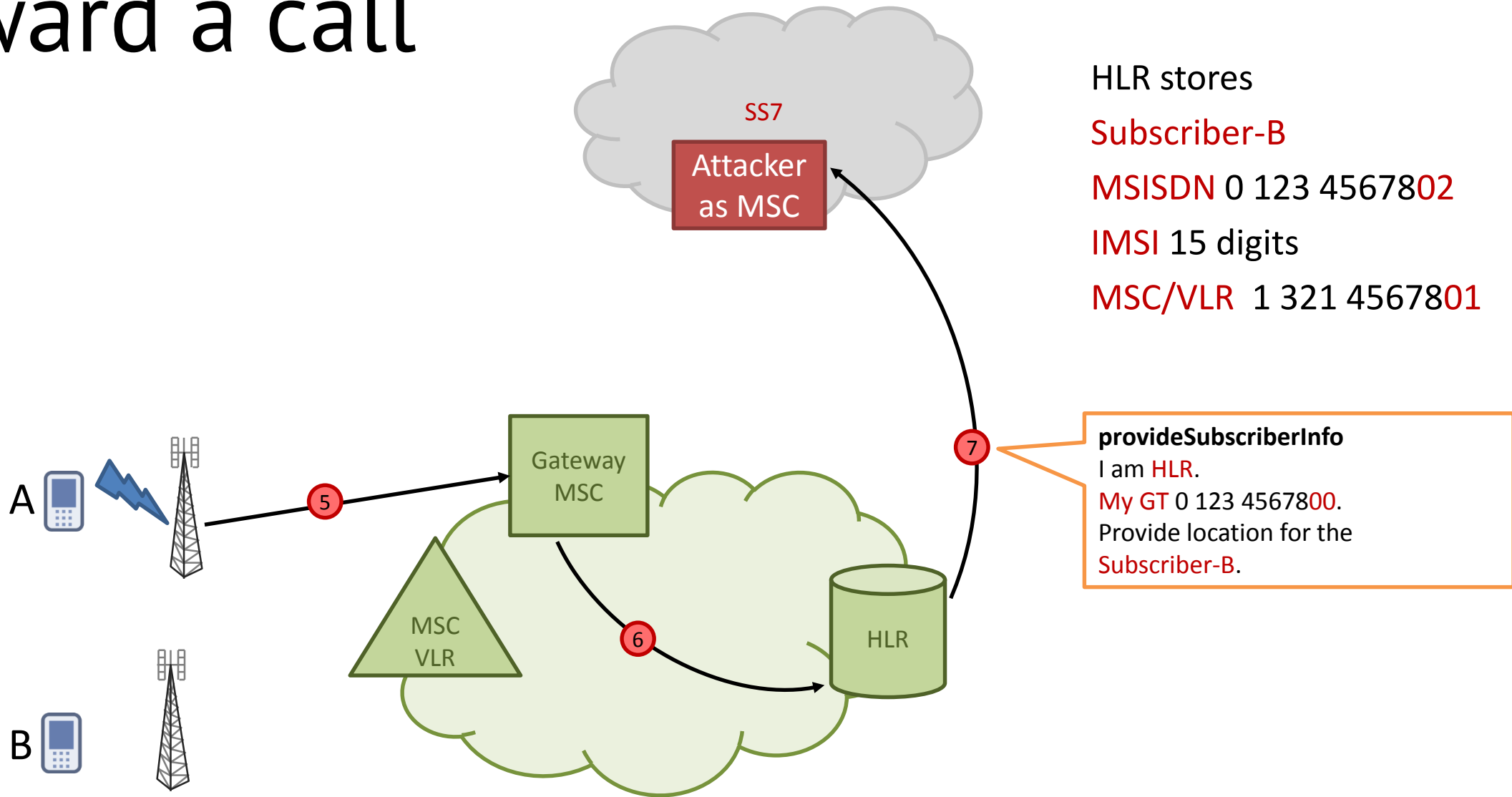
GatewayMSC knows

nothing

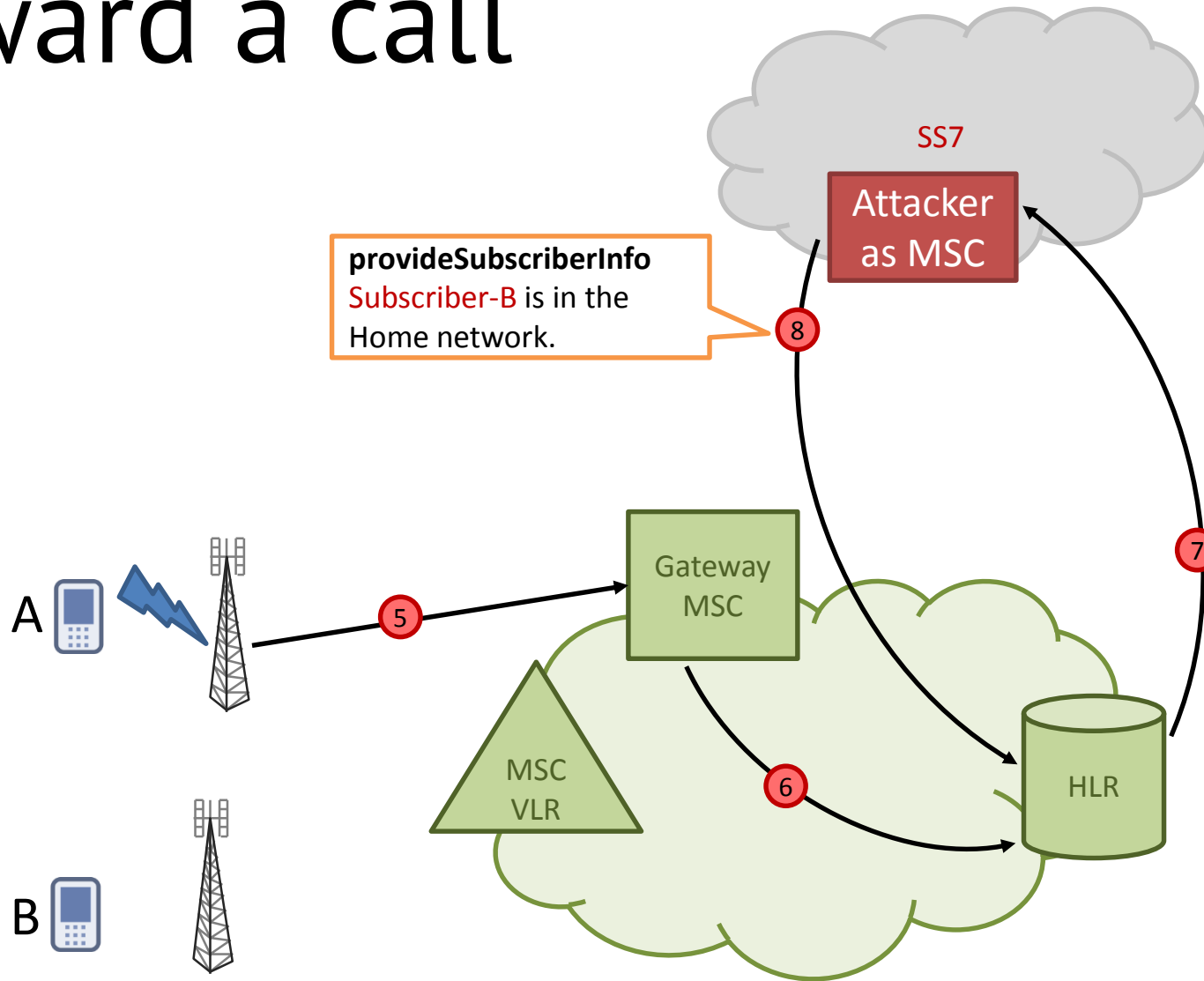
# Forward a call



# Forward a call



# Forward a call



HLR stores

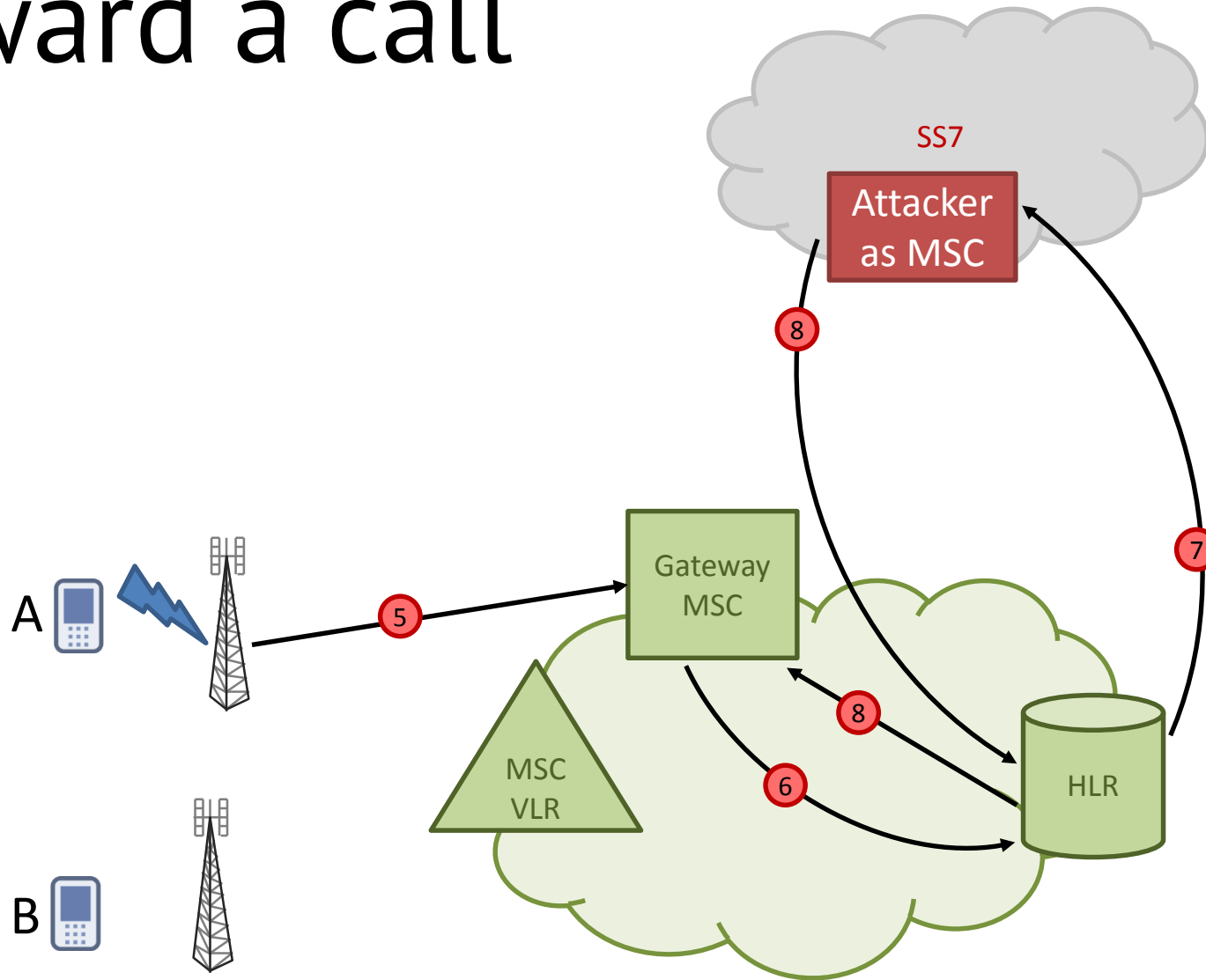
Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

MSC/VLR 1 321 4567801

# Forward a call



HLR stores

Subscriber-B

MSISDN 0 123 4567802

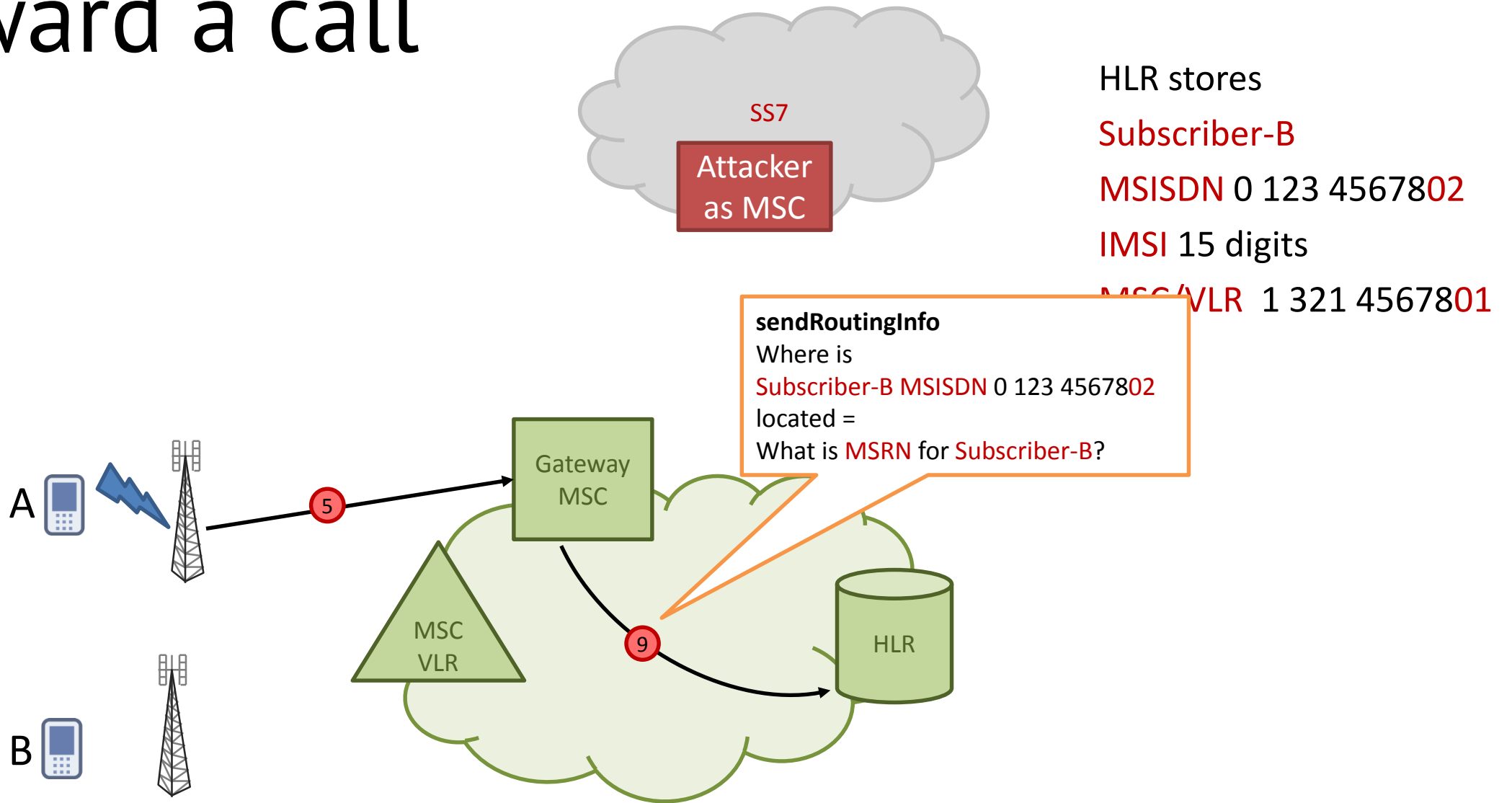
IMSI 15 digits

MSC/VLR 1 321 4567801

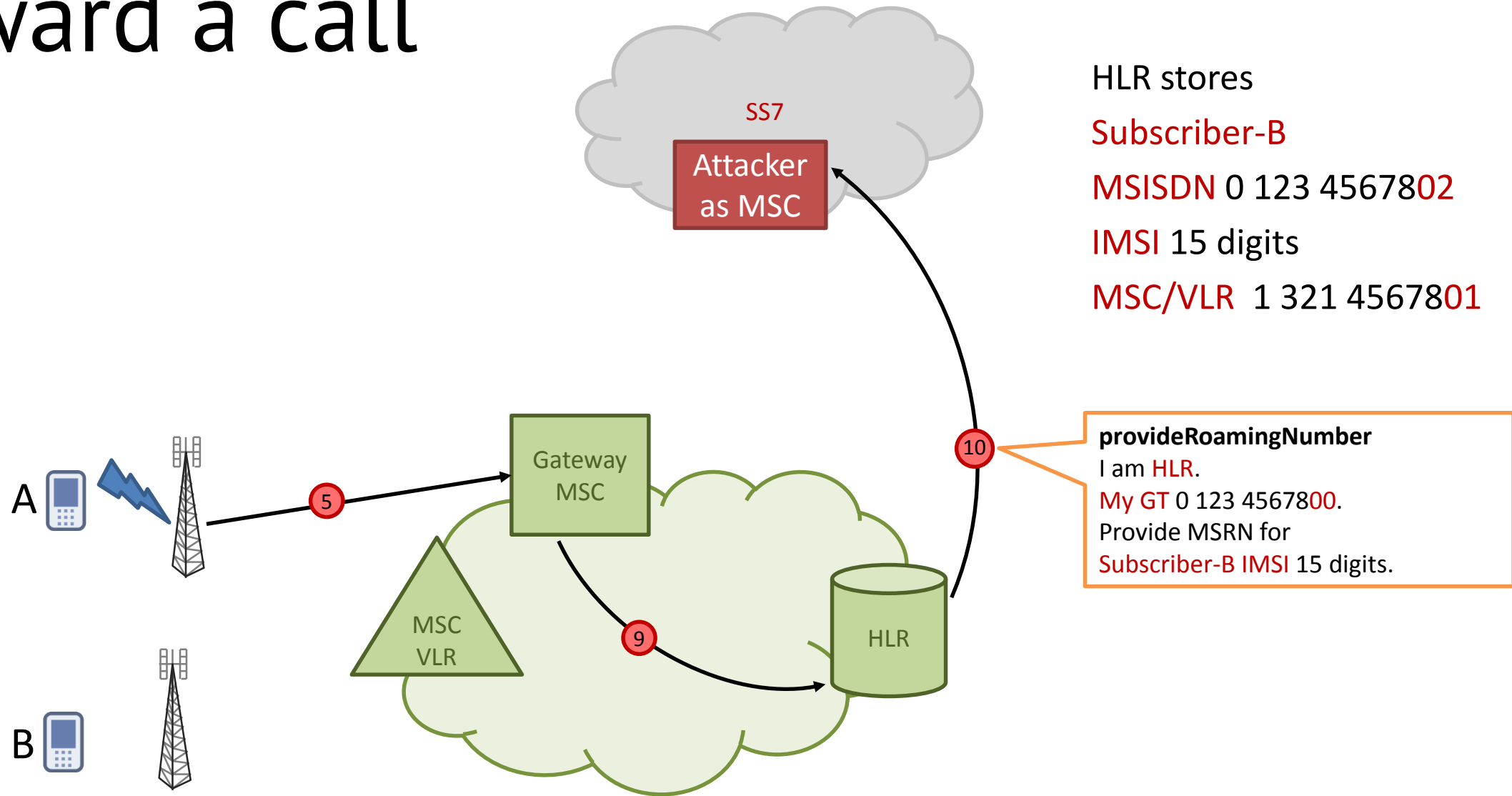
GatewayMSC knows that  
Subscriber-B is at home.

This information will be  
sent to a billing platform.

# Forward a call

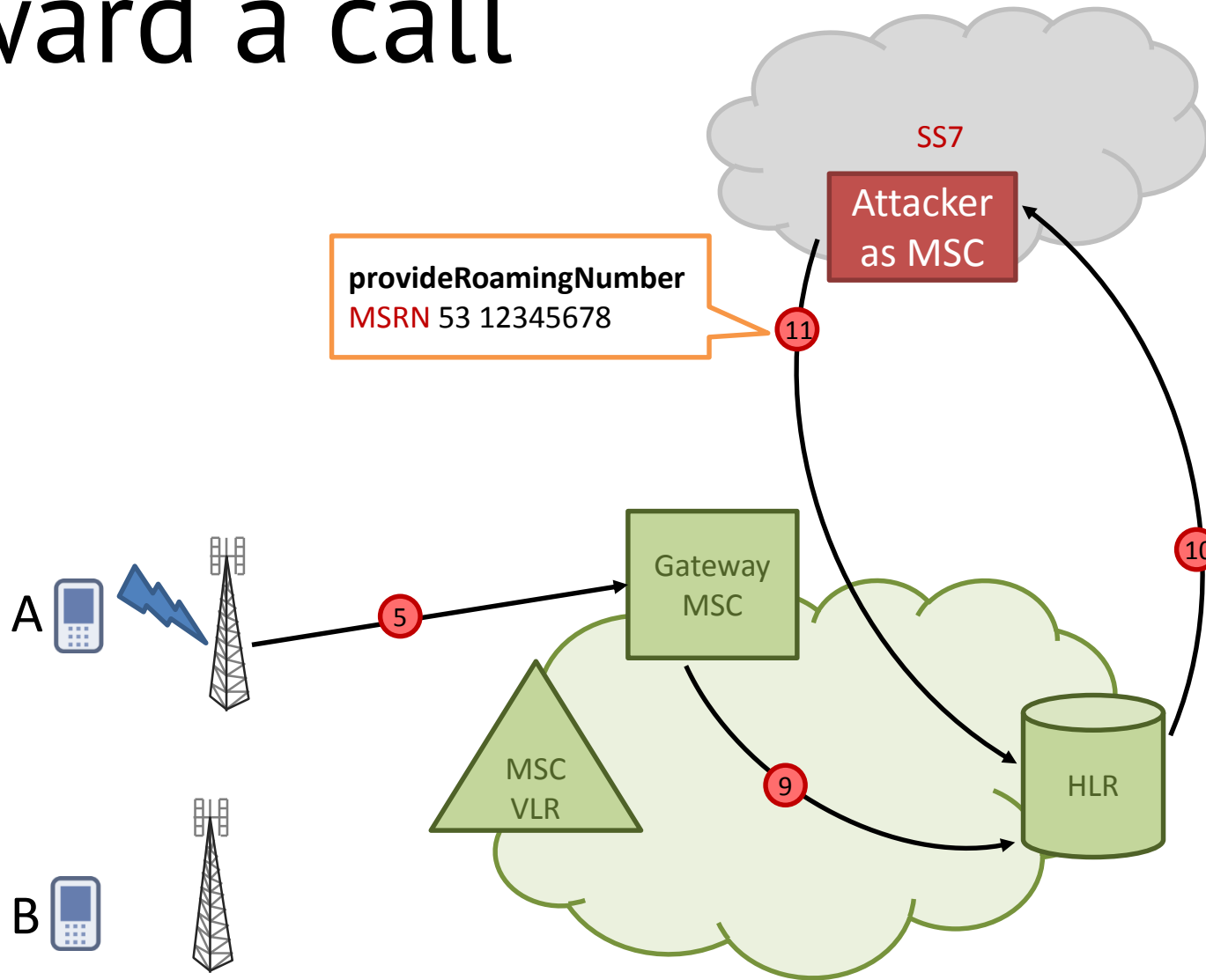


# Forward a call





# Forward a call



HLR stores

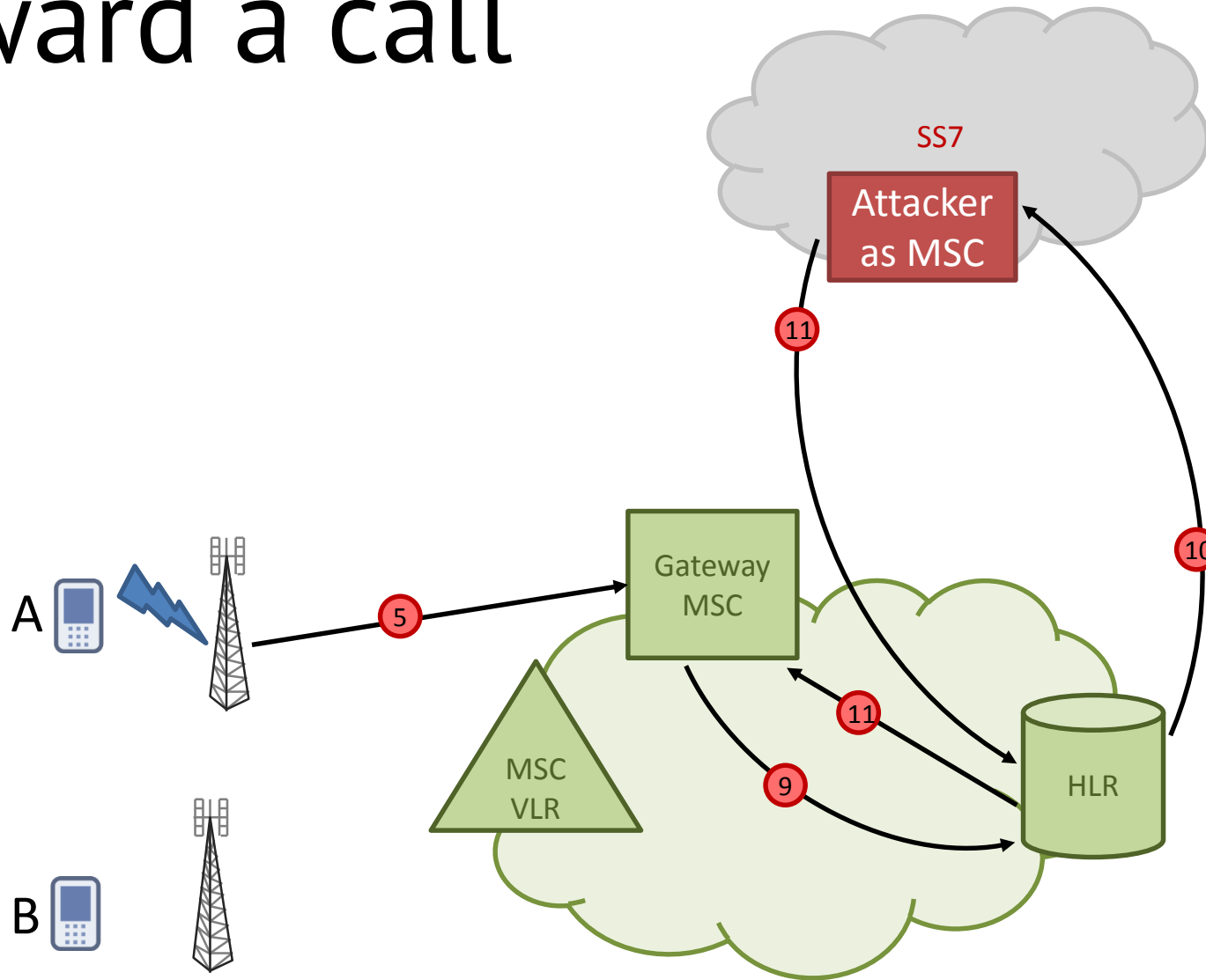
Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

MSC/VLR 1 321 4567801

# Forward a call



HLR stores

Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

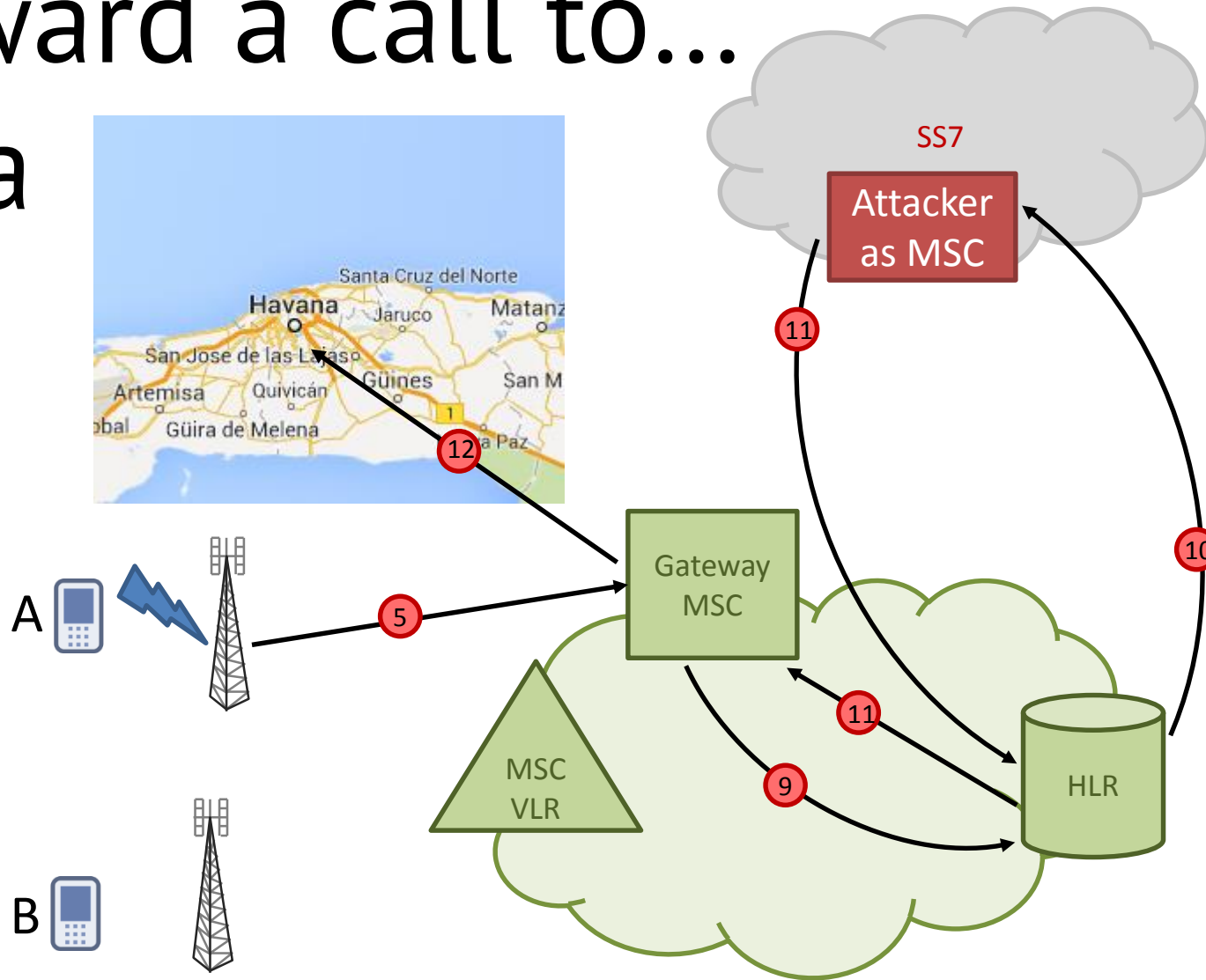
MSC/VLR 1 321 4567801

GatewayMSC knows

Subscriber-B

MSRN 53 12345678

# Forward a call to... Cuba



HLR stores

Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

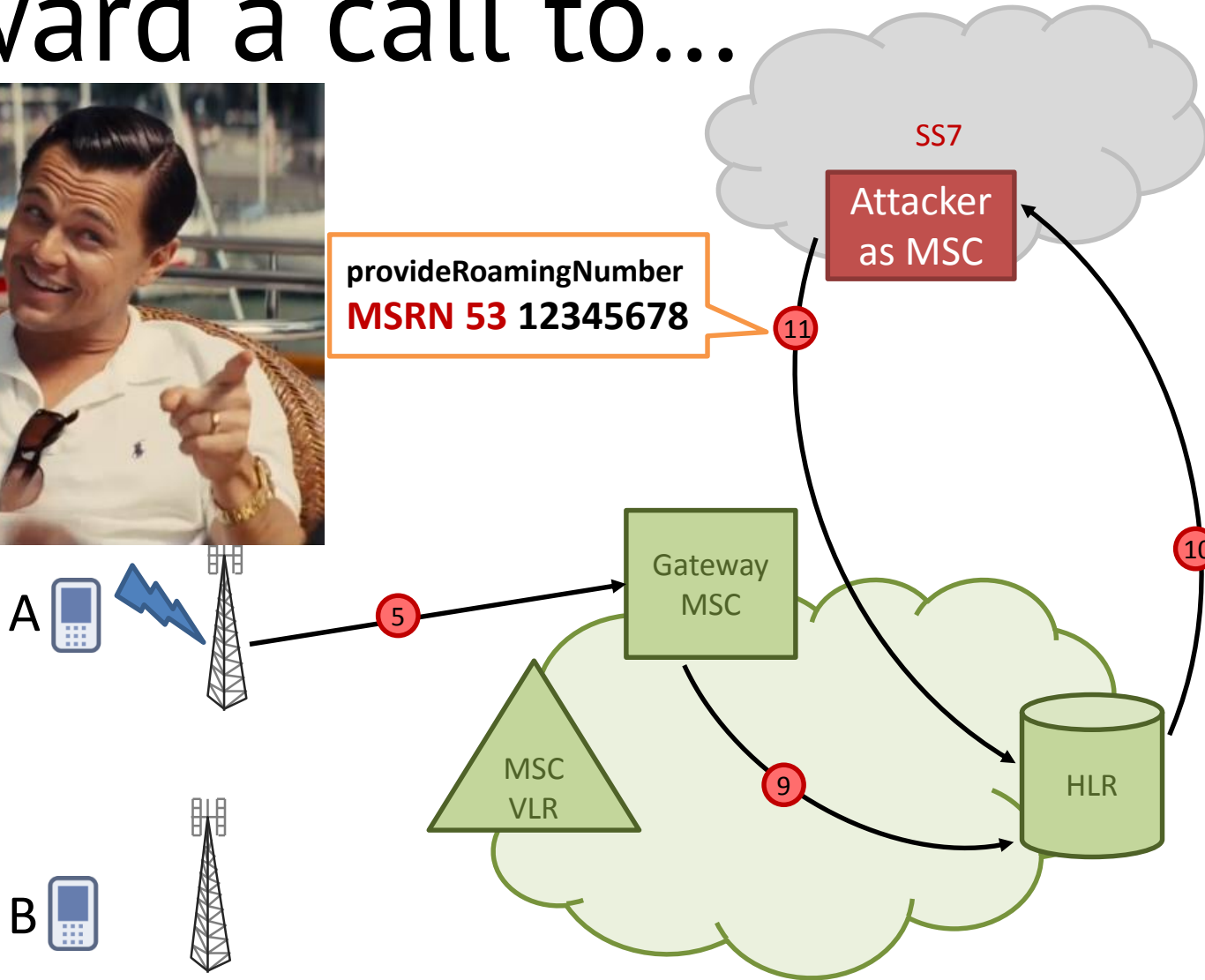
MSC/VLR 1 321 4567801

GatewayMSC knows

Subscriber-B

MSRN 53 12345678

# Forward a call to...



HLR stores

Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

MSC/VLR 1 321 4567801

GatewayMSC knows

Subscriber-B

MSRN 53 12345678

# Who pays?

Call from  to  while at “home” = \$ 0.05

Call from  to  = \$ 1.00

# Who pays?

Call from  to  while at “home” = \$ 0.05

Call from  to  = \$ 1.00



\$ 1.00 - \$ 0.05 = **\$ 0.95** – Attacker profit

# Who pays?

Call from  A to  B while at “home” = \$ 0.05

Call from  A to  Cuba = \$ 1.00

\$ 1.00 - \$ 0.05 = **\$ 0.95** – Attacker profit

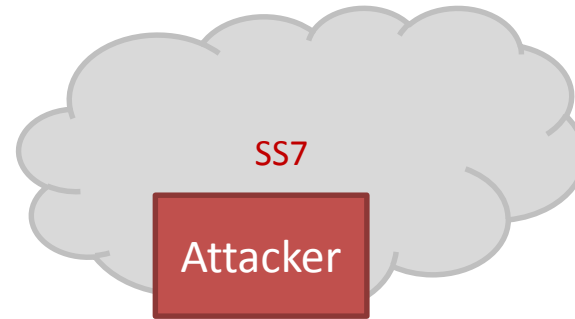
How much Mobile operator loses? Call from  MNO to  Cuba = **\$ 0.30**

# SMS Interception

- 1) Collect info
- 2) Spoof MSC
- 3) Receive incoming SMSs

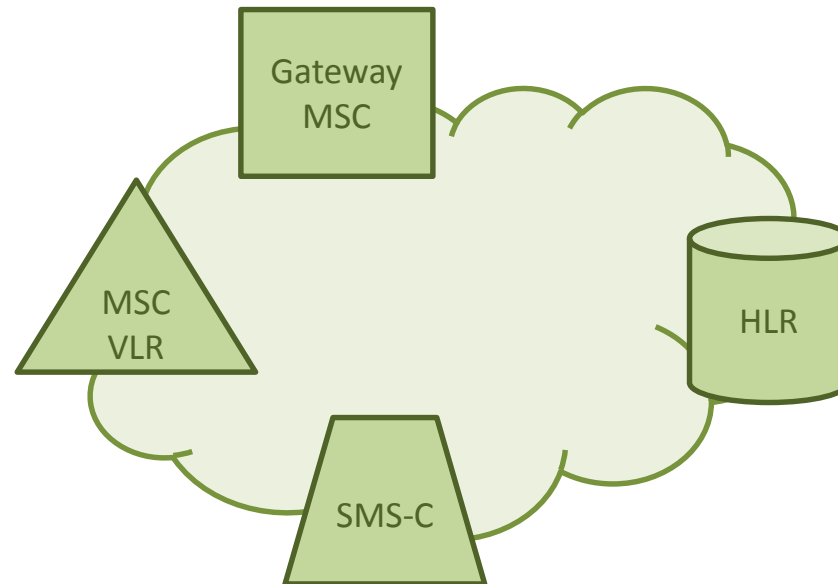
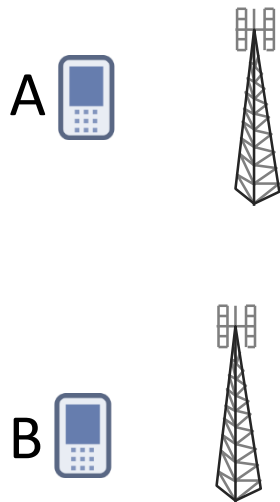


# Collect info



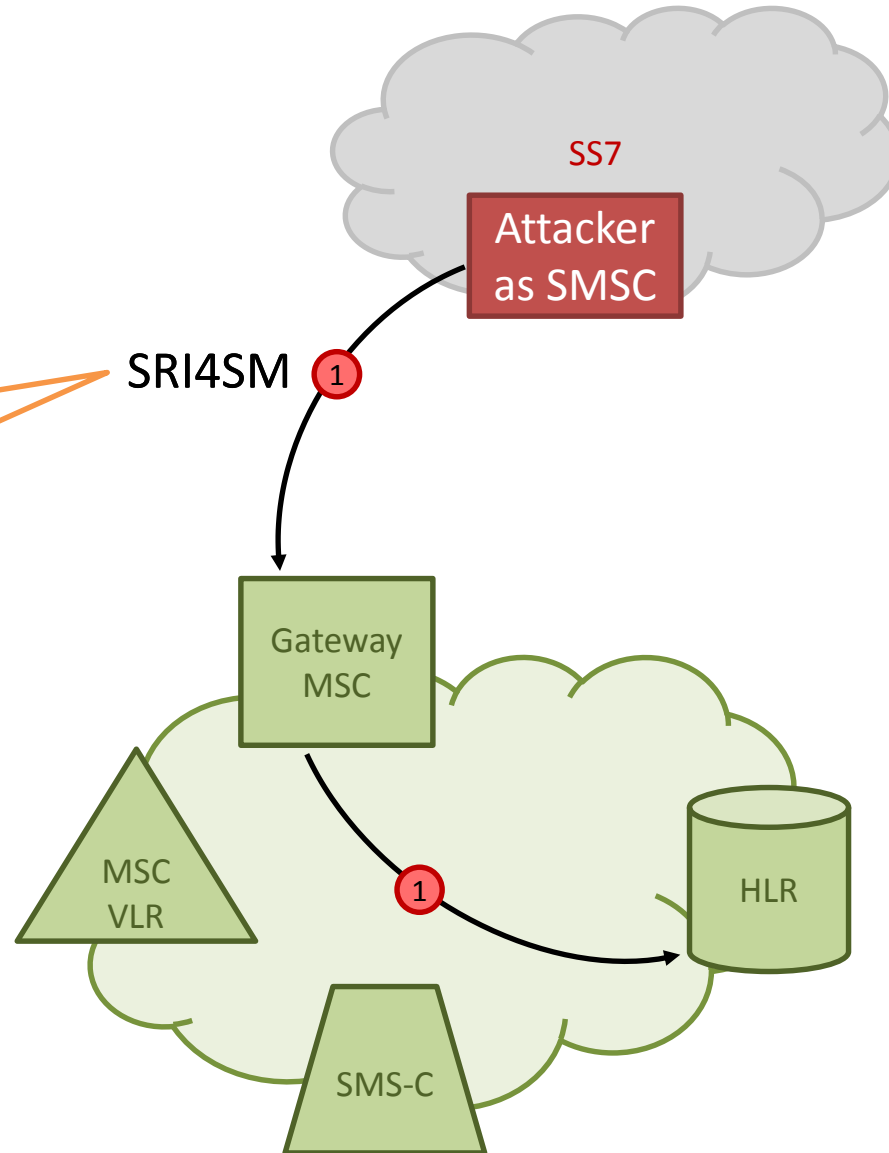
We know

**B-Number** 0 123 45678**02**



# Collect info

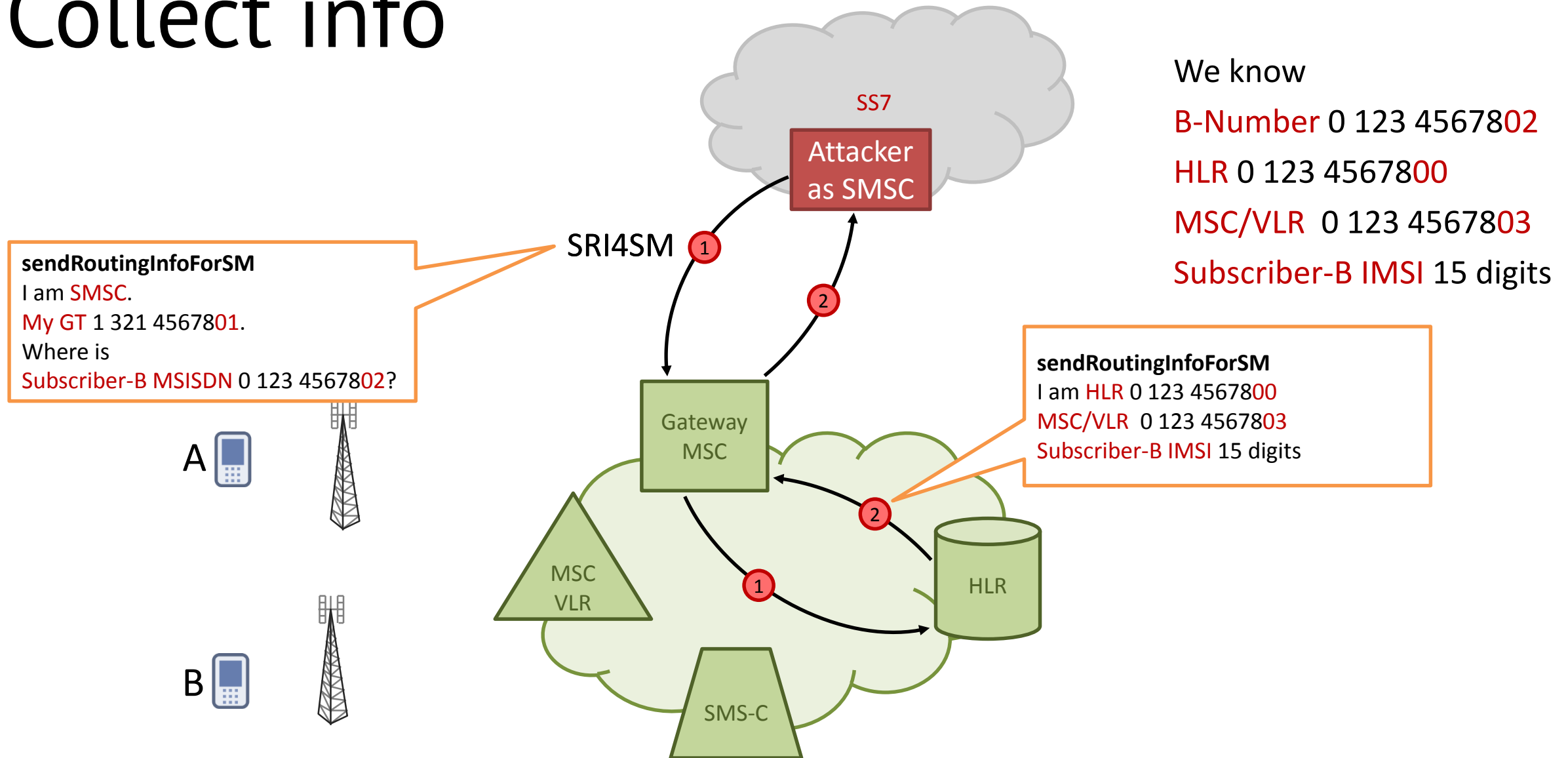
**sendRoutingInfoForSM**  
I am **SMSC**.  
**My GT** 1 321 4567801.  
Where is  
**Subscriber-B MSISDN** 0 123 4567802?



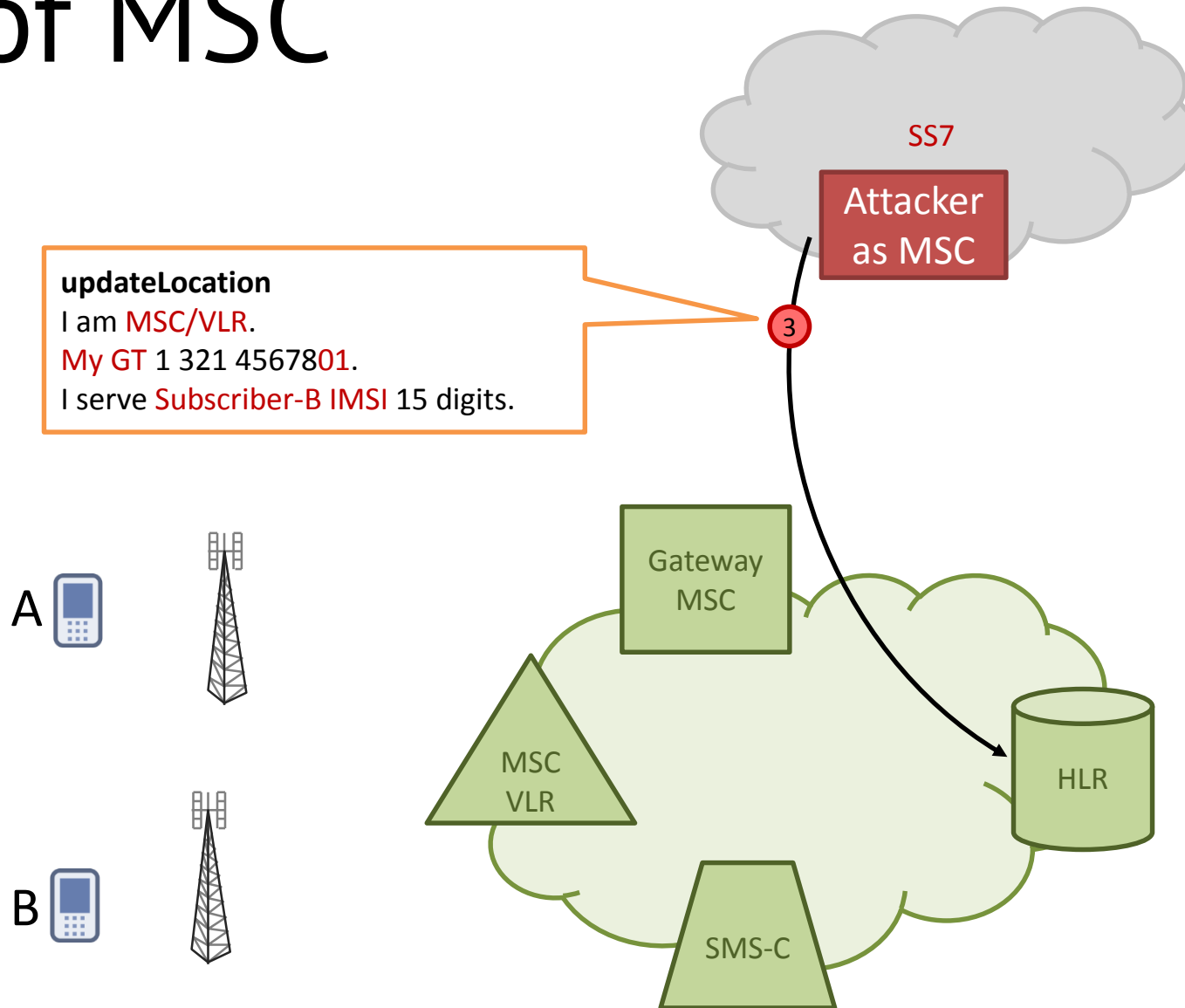
We know

**B-Number** 0 123 4567802

# Collect info



# Spoof MSC



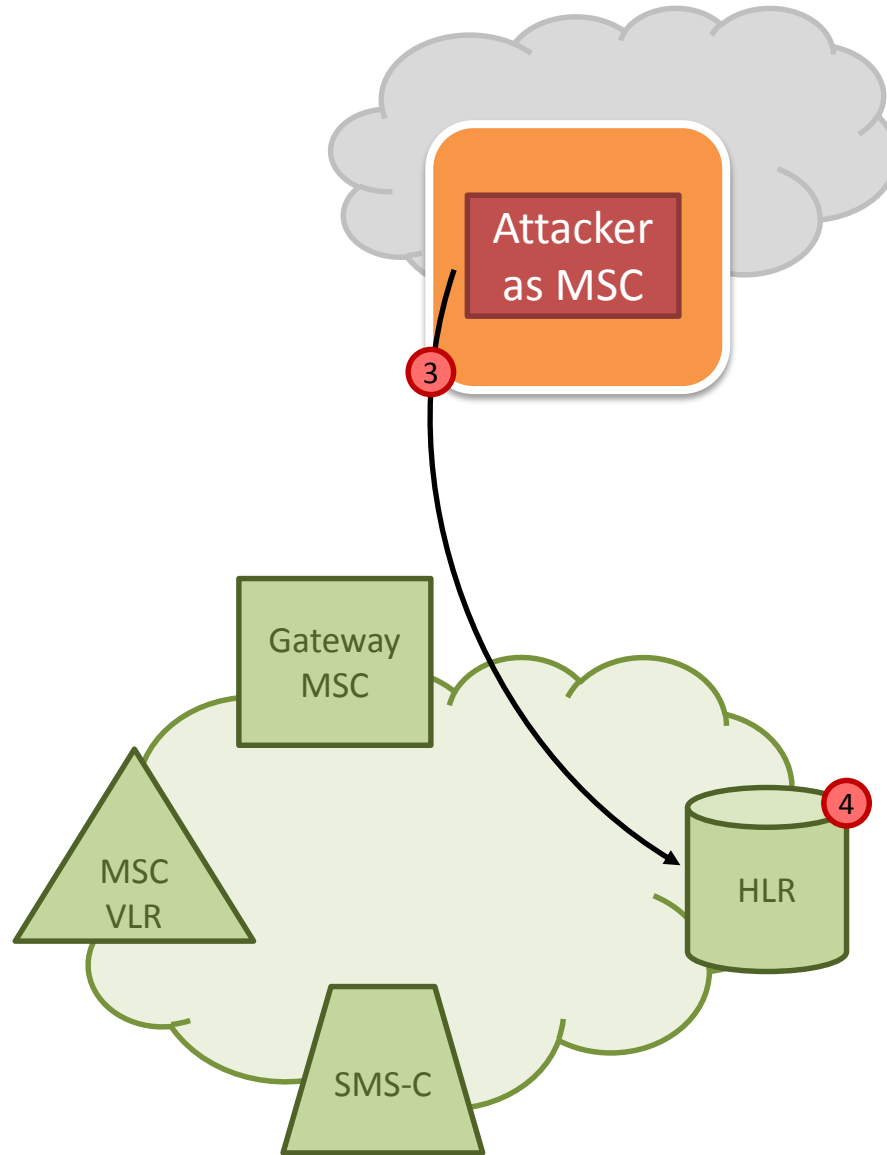
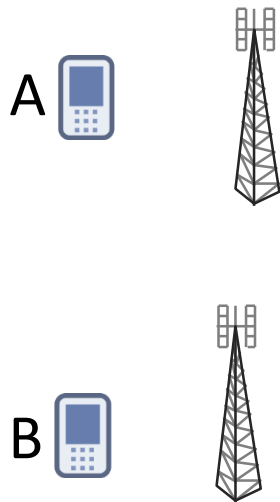
We know

HLR 0 123 4567800

Subscriber-B IMSI 15 digits

# Spoof MSC

We serve  
Subscriber-B



We know

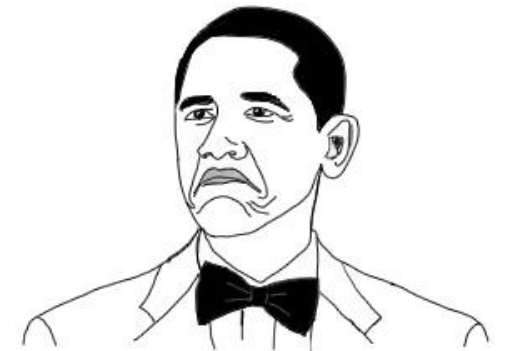
HLR 0 123 4567800

Subscriber-B IMSI 15 digits

HLR stores

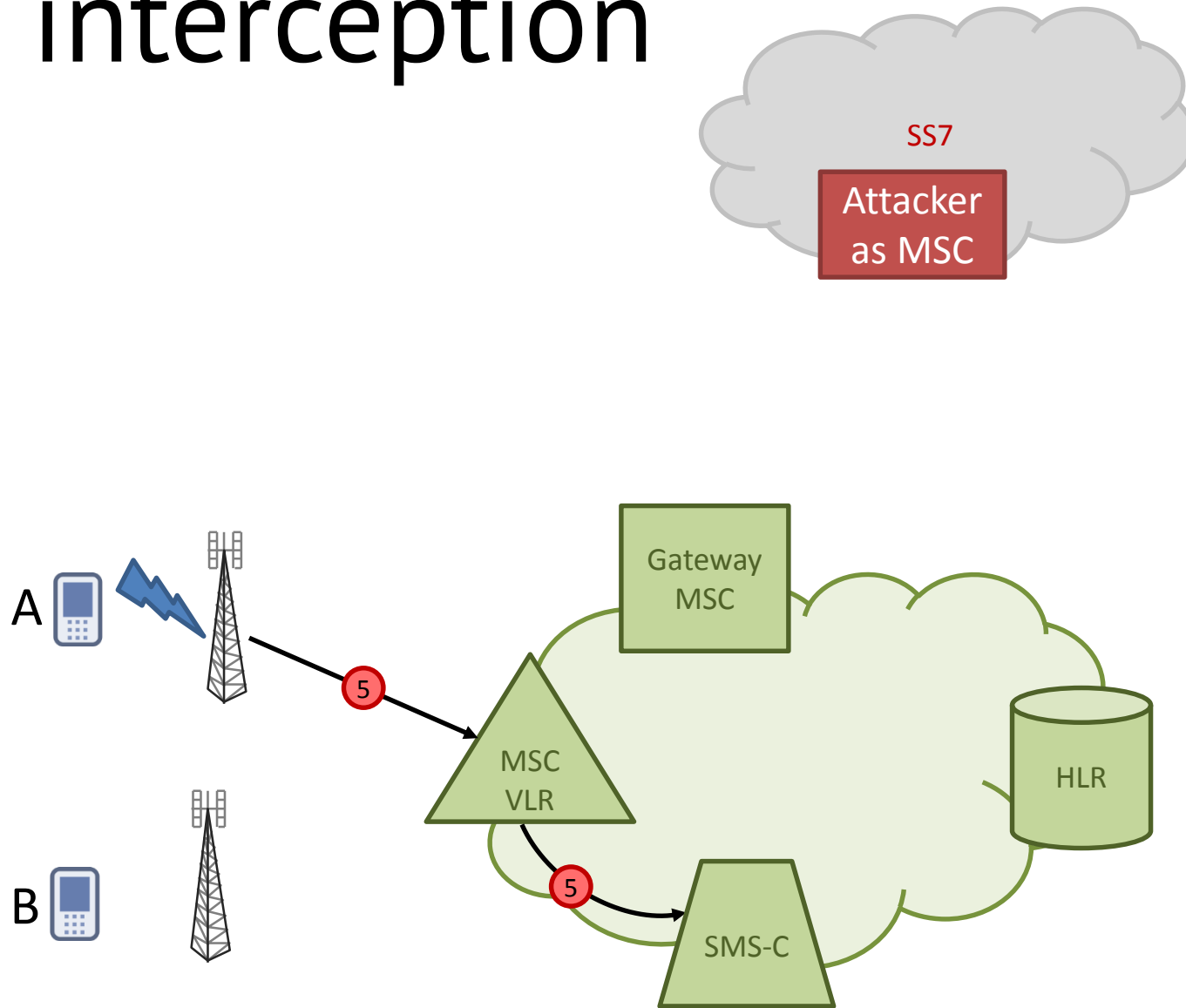
Subscriber-B IMSI 15 digits

MSC/VLR 1 321 4567801



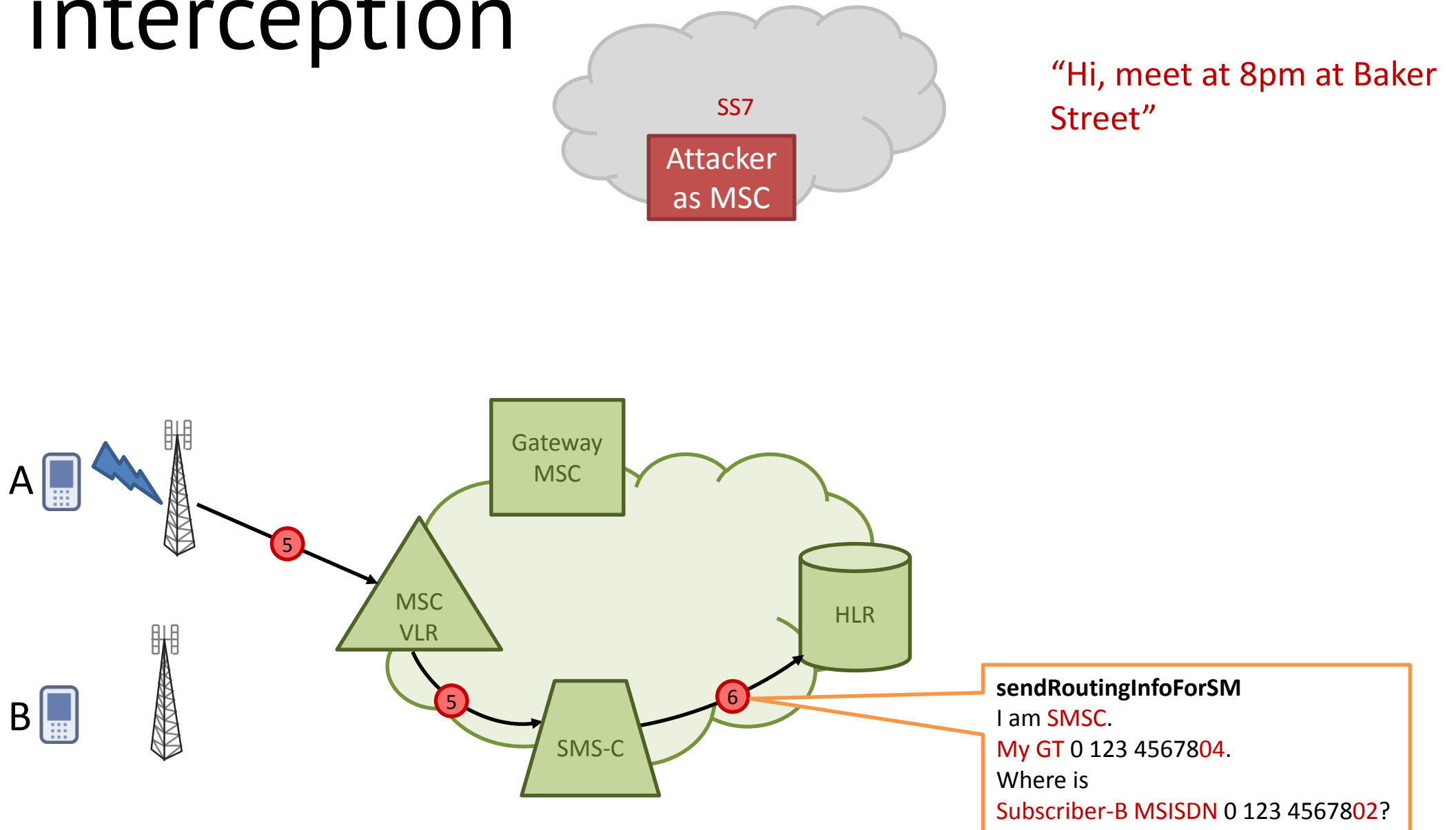
**NOT BAD**

# SMS interception

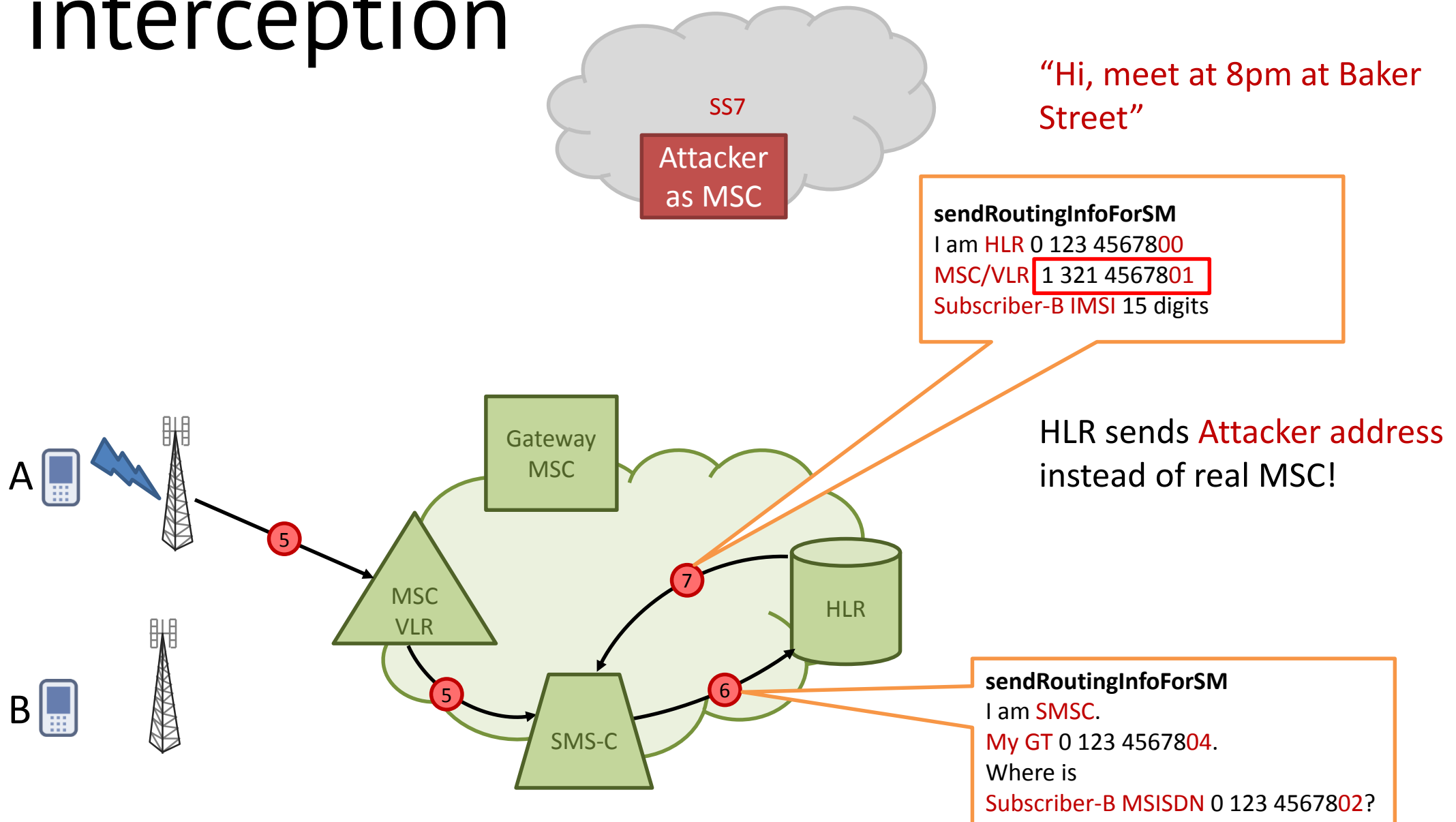


“Hi, meet at 8pm at Baker Street”

# SMS interception

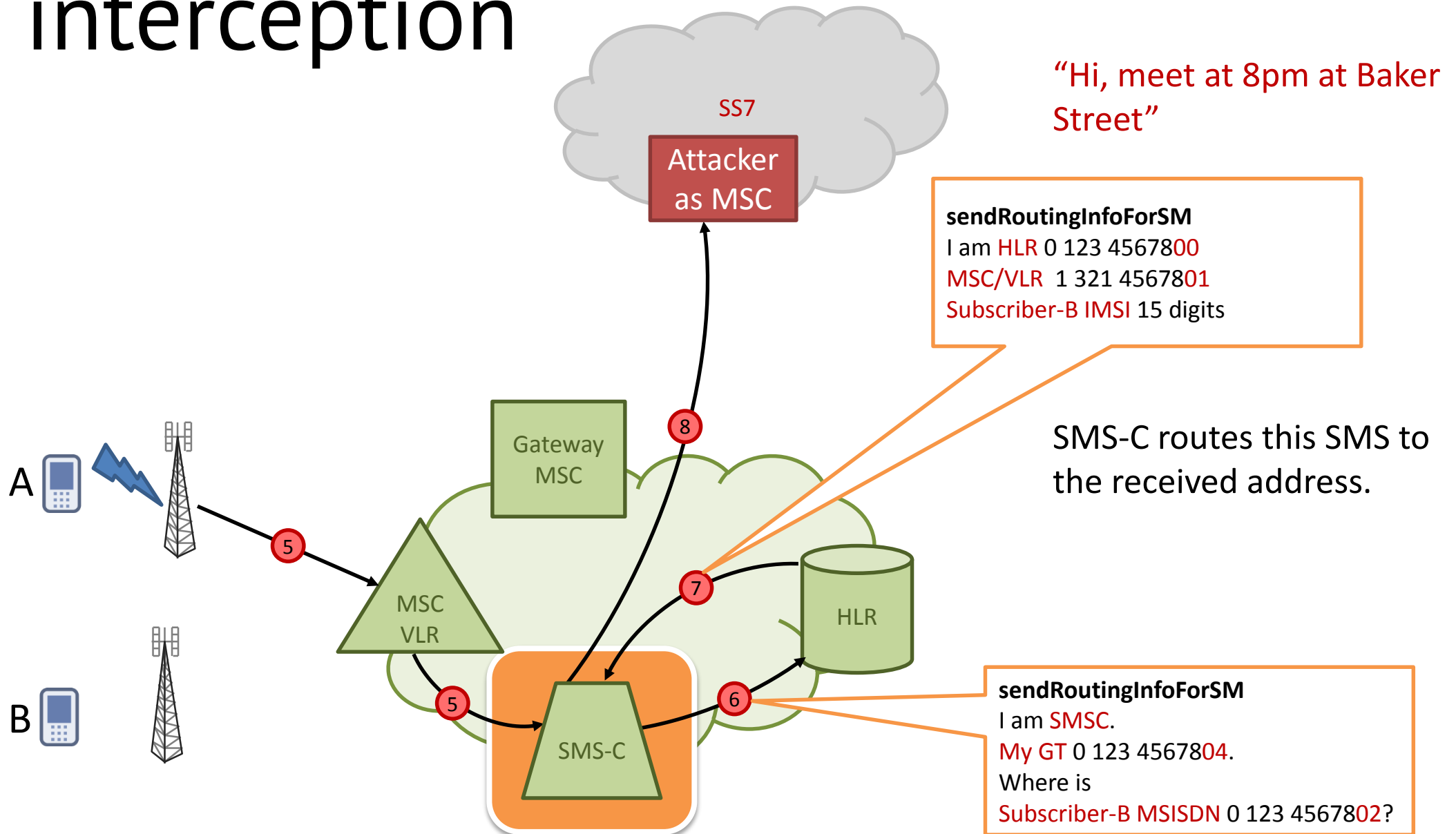


# SMS interception

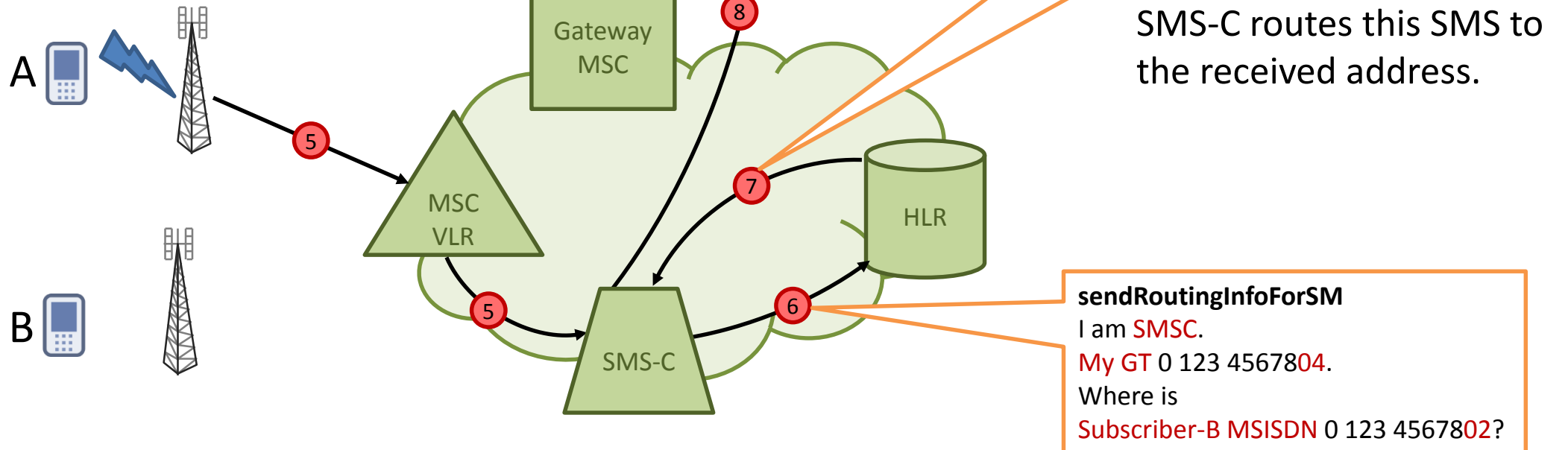




# SMS interception



# SMS interception



# SMS interception



1. SMS chats
2. One time passwords
3. Confirmation codes
4. Password recovery

# Money Transfer

## Using USSD

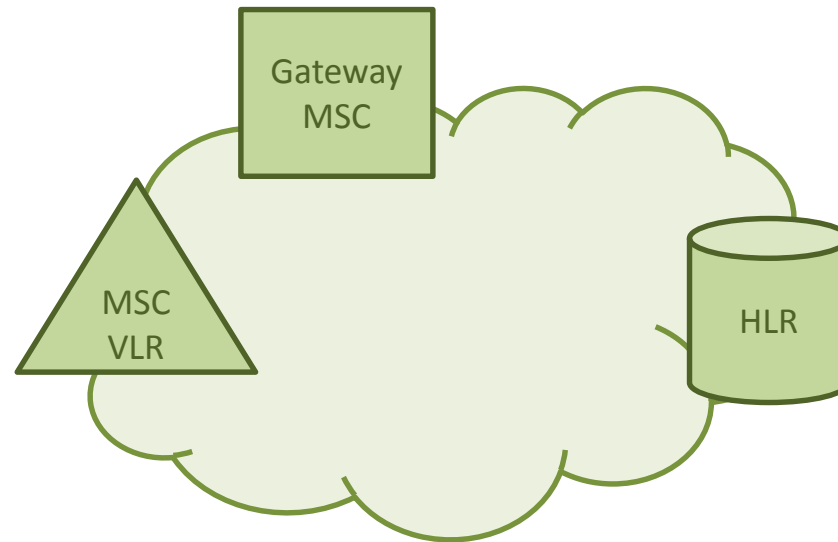
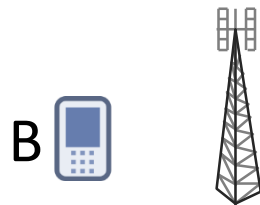
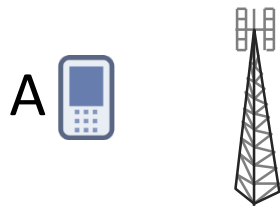
- 1) Collect info
- 2) Request account status
- 3) Transfer money

# Collect info



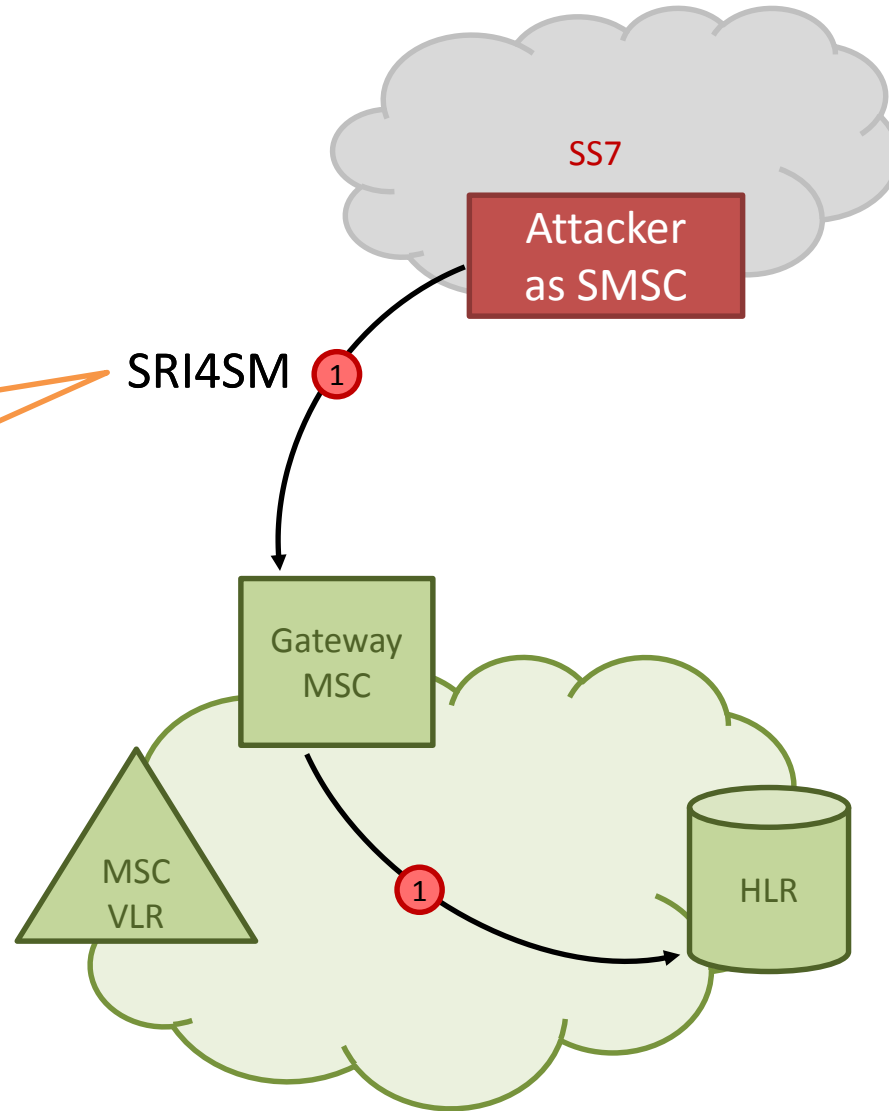
We know

**B-Number** 0 123 45678**02**



# Collect info

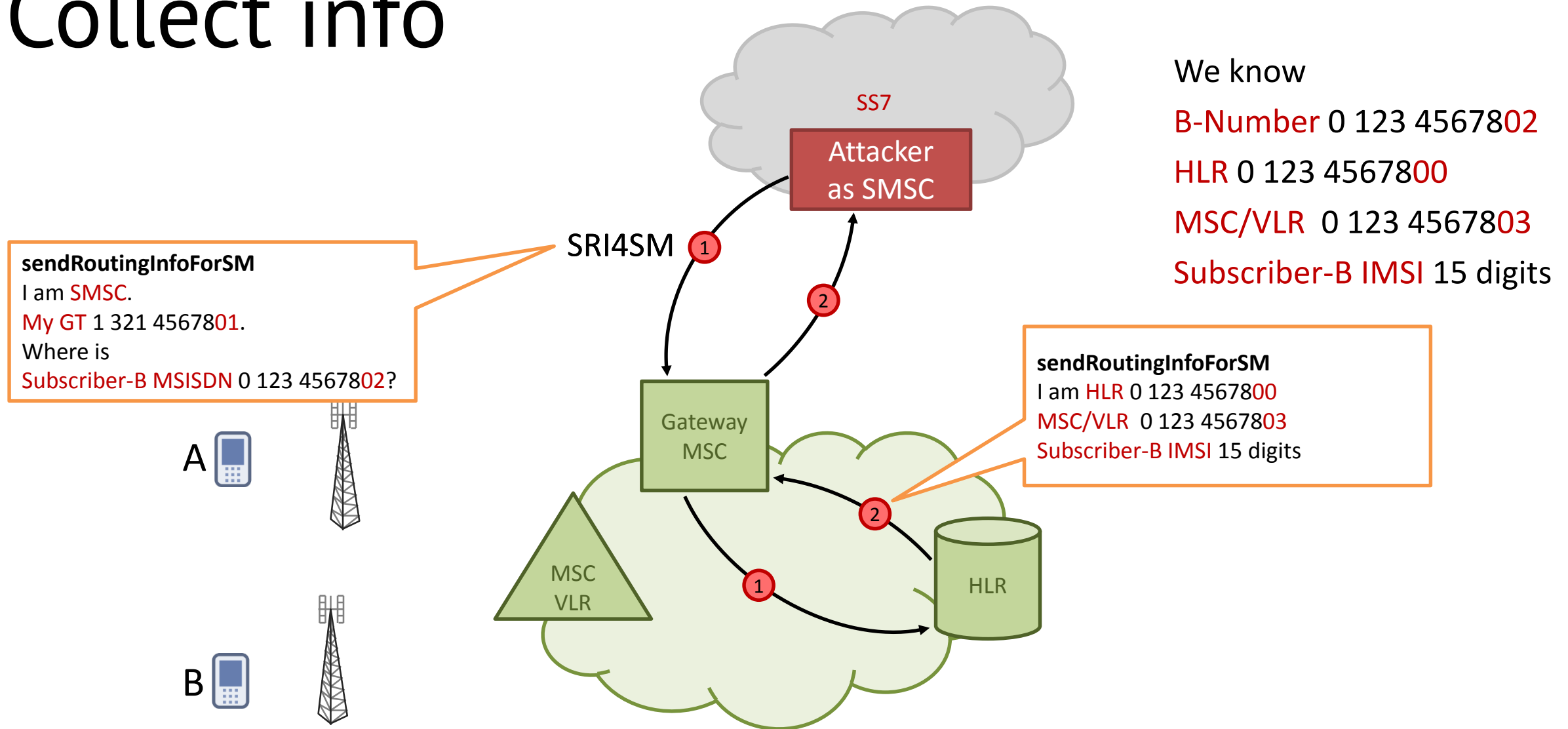
**sendRoutingInfoForSM**  
I am **SMSC**.  
**My GT** 1 321 4567801.  
Where is  
**Subscriber-B MSISDN** 0 123 4567802?



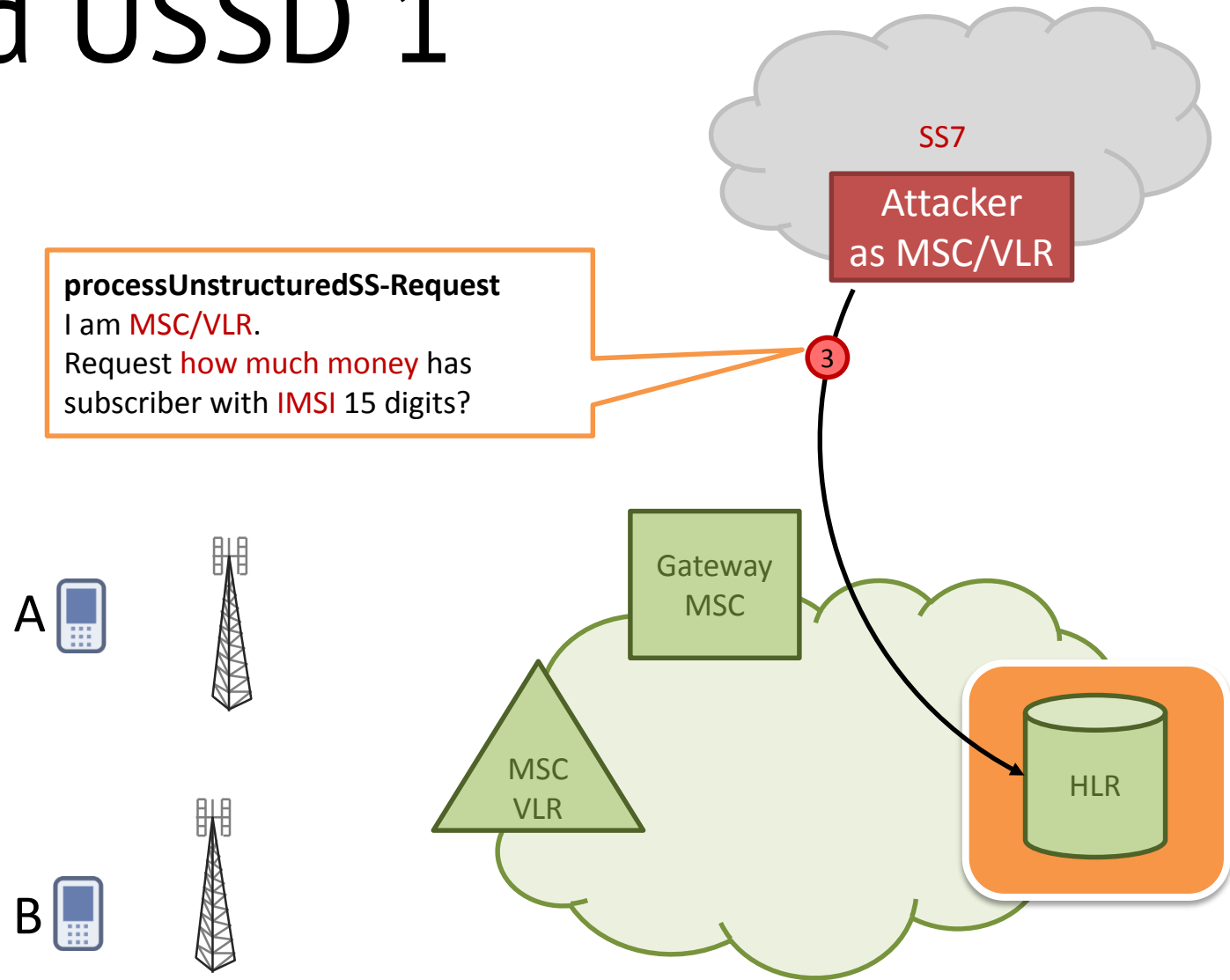
We know

**B-Number** 0 123 4567802

# Collect info



# Send USSD 1



We know

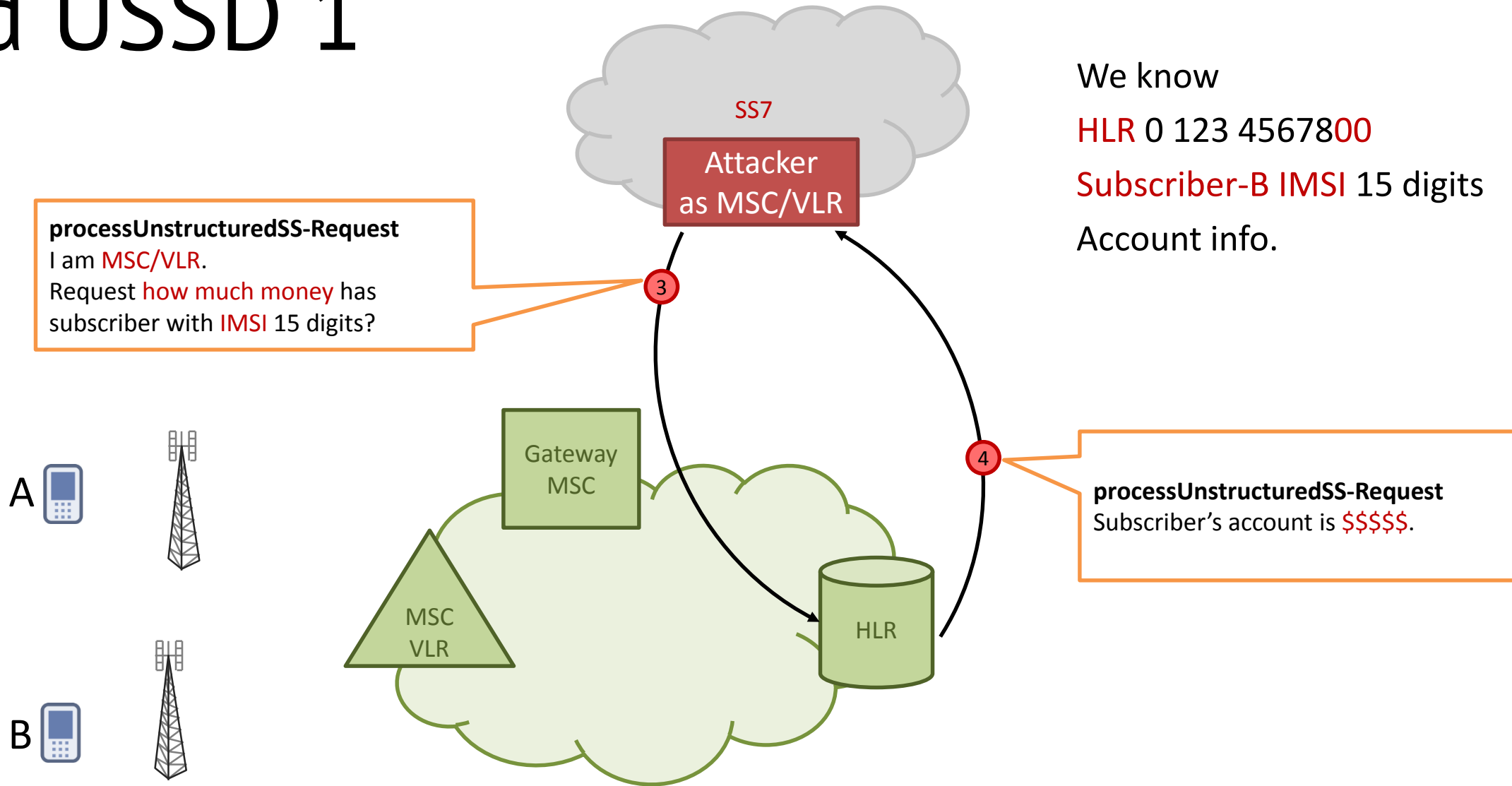
**HLR 0 123 4567800**

**Subscriber-B IMSI 15** digits

**\*100#**



# Send USSD 1



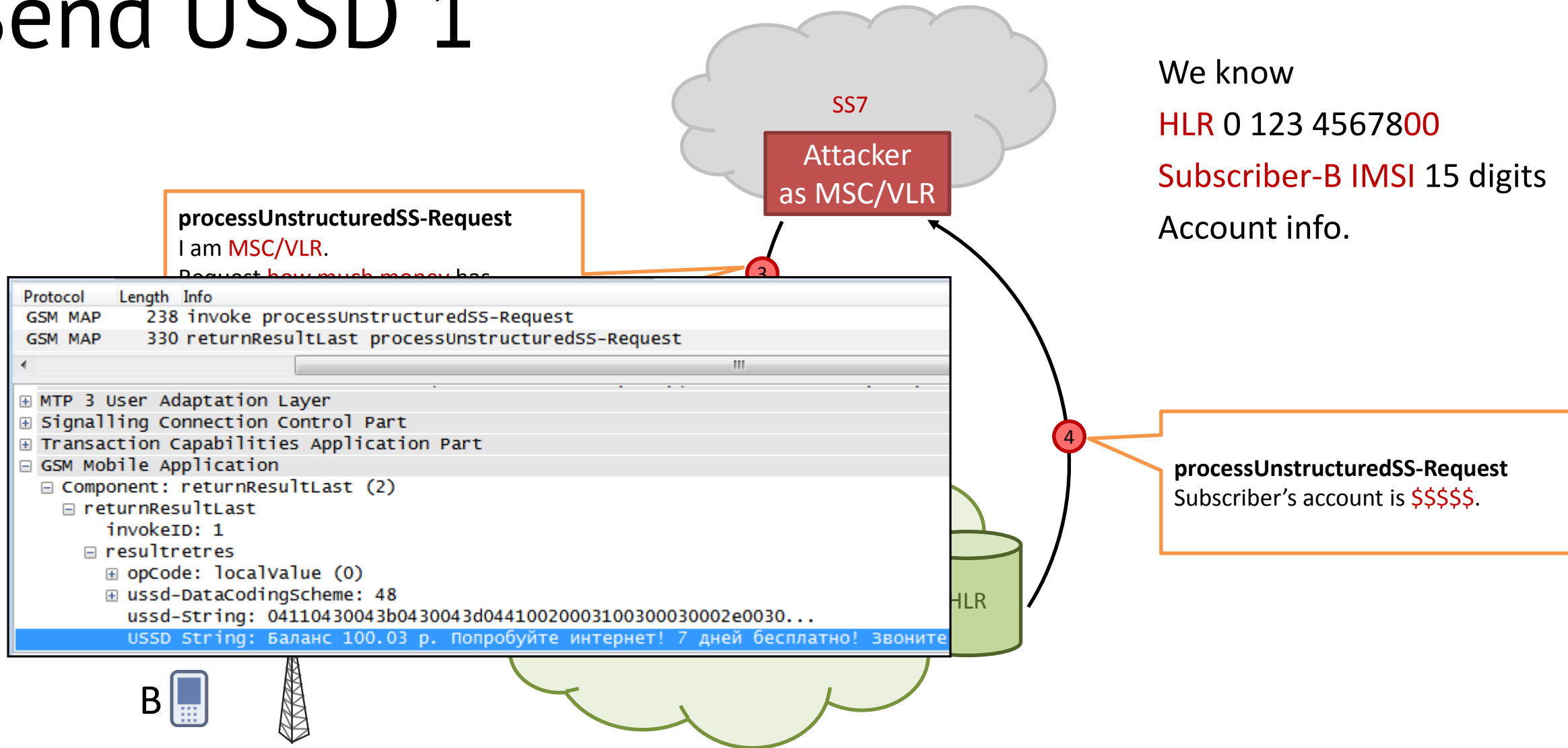
# Send USSD 1

We know

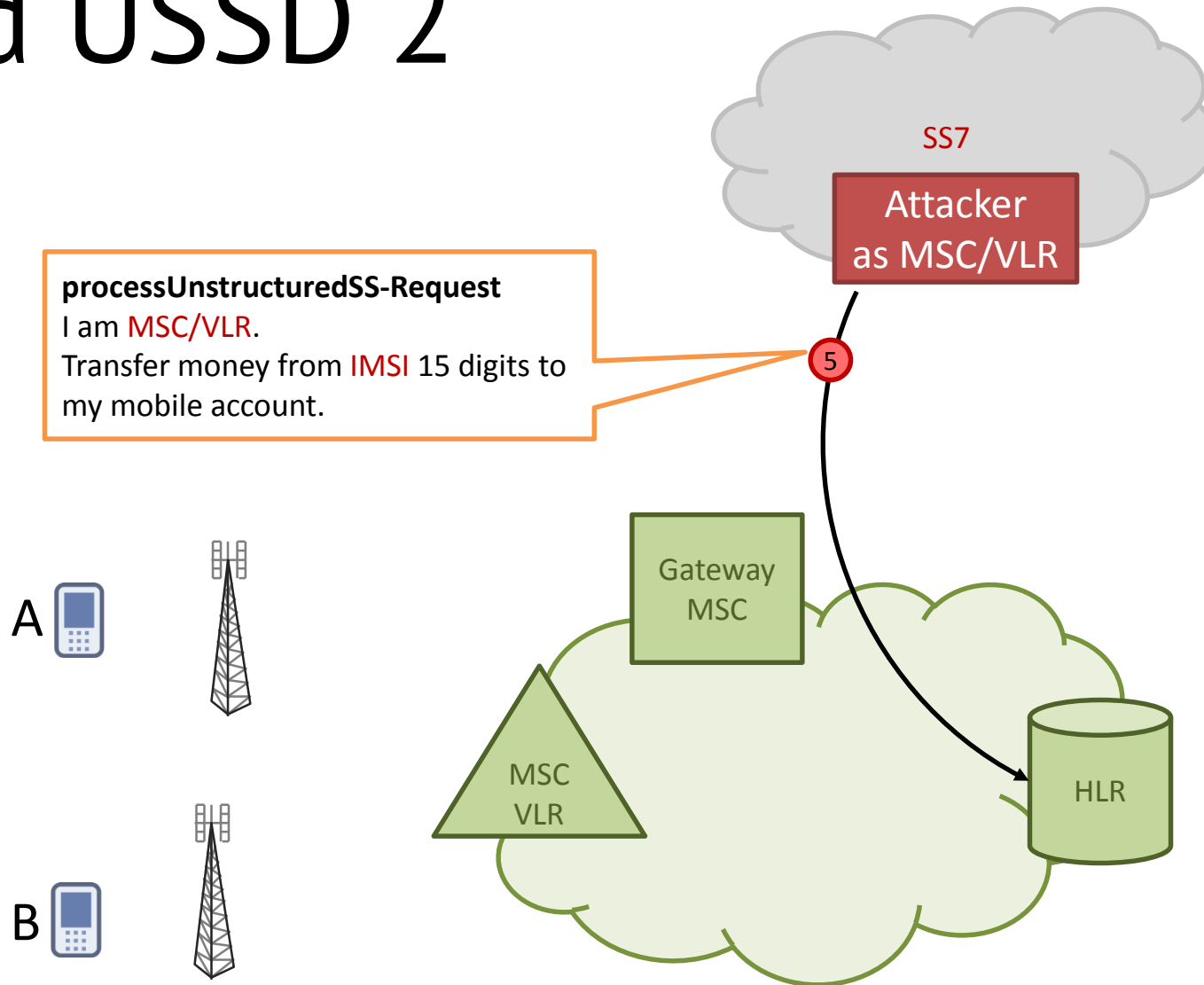
HLR 0 123 4567800

Subscriber-B IMSI 15 digits

Account info.



# Send USSD 2



We know

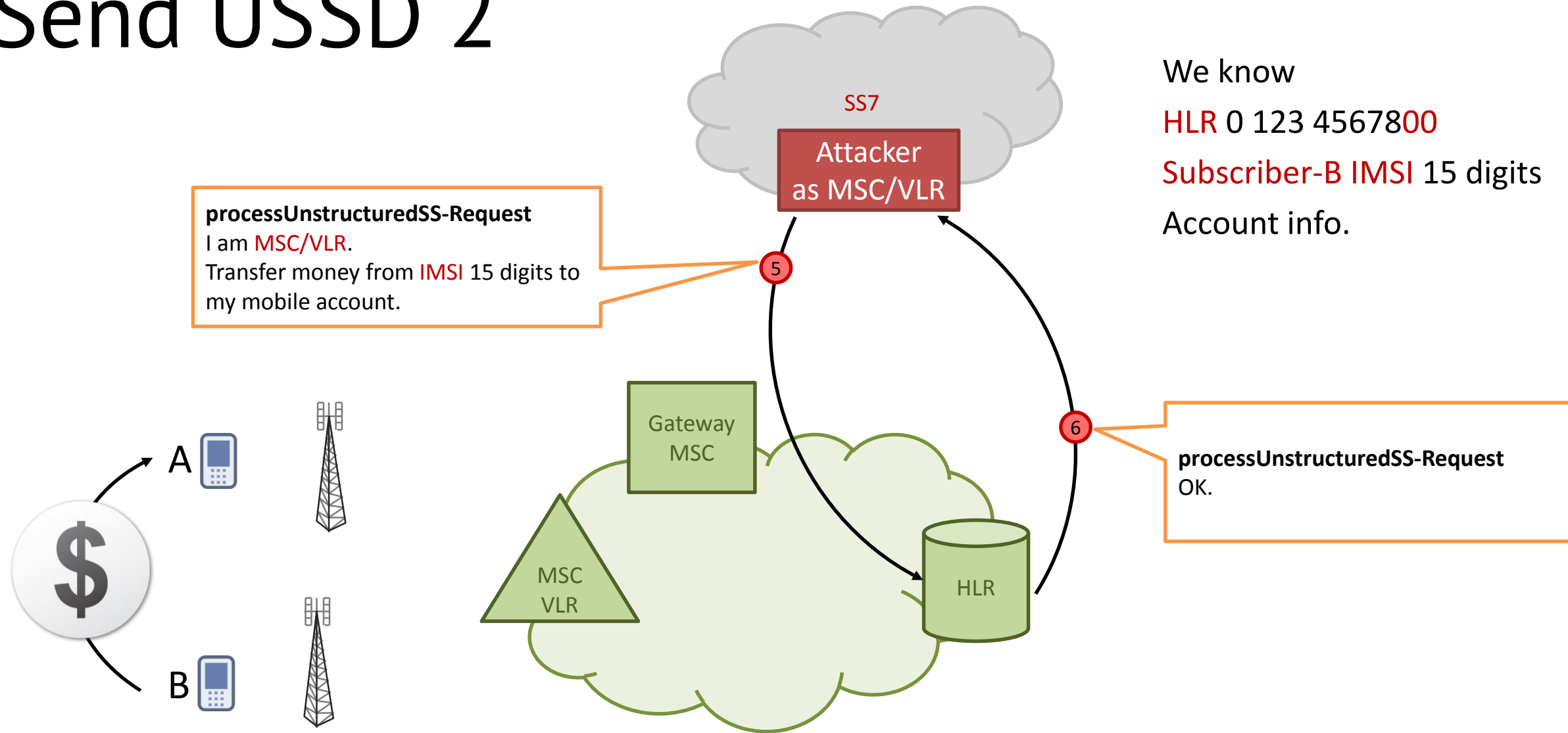
**HLR** 0 123 45678**00**

**Subscriber-B IMSI** 15 digits

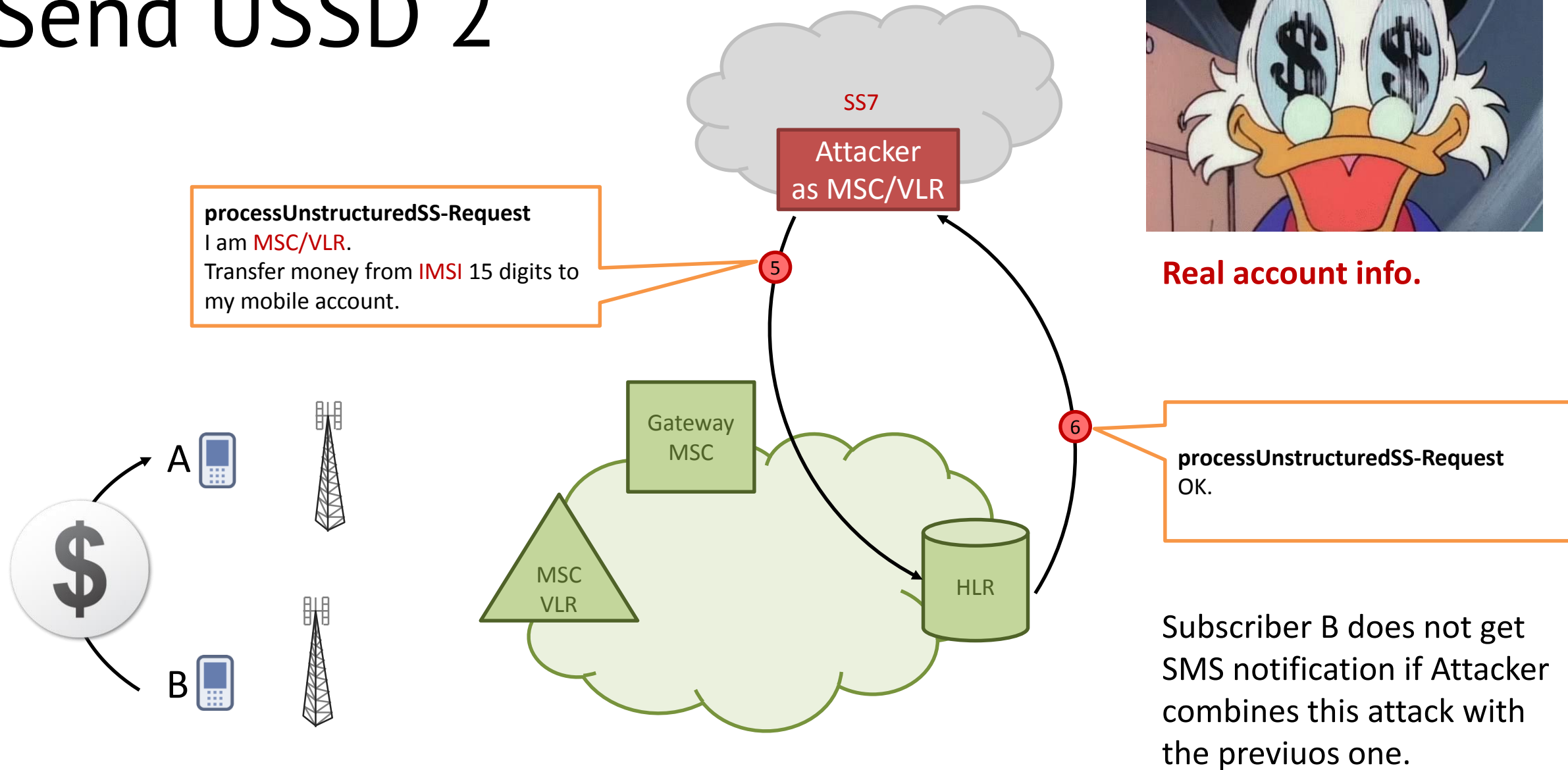
Account info.

**\*123\*01238765400\*100#**

# Send USSD 2



# Send USSD 2



Real account info.

Subscriber B does not get SMS notification if Attacker combines this attack with the previuos one.

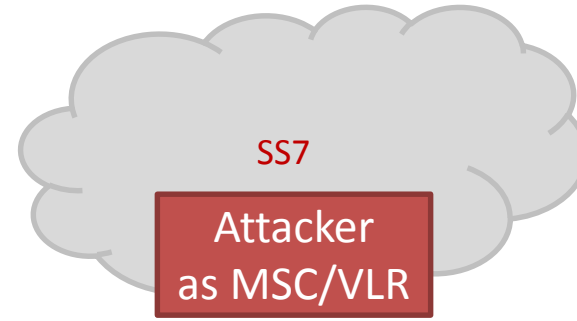
# Send USSD 2



**processUnstructuredSS-Request**

I am **MSC/VLR**.

Transfer money from **IMSI** 15 digits to my mobile account.



5

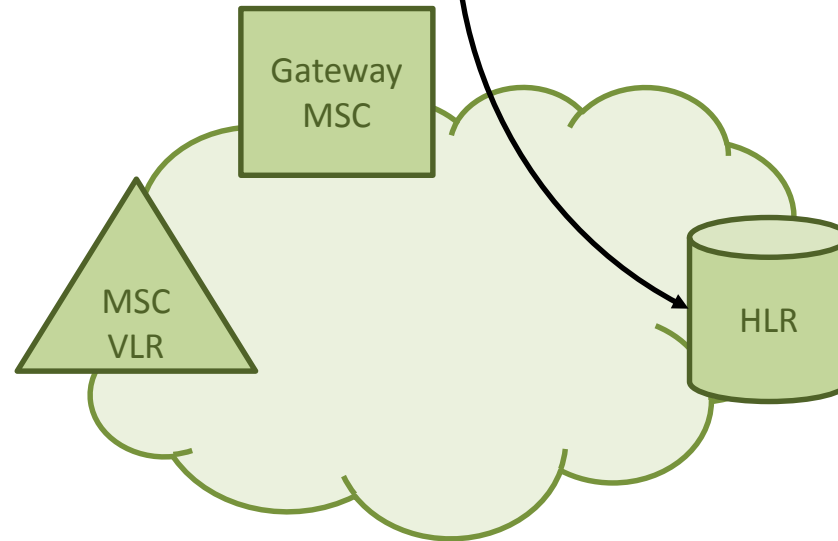
6



**Real account info.**

**processUnstructuredSS-Request**  
OK.

Subscriber B does not get SMS notification if Attacker combines this attack with the previous one.



# Subscriber Location Discovery

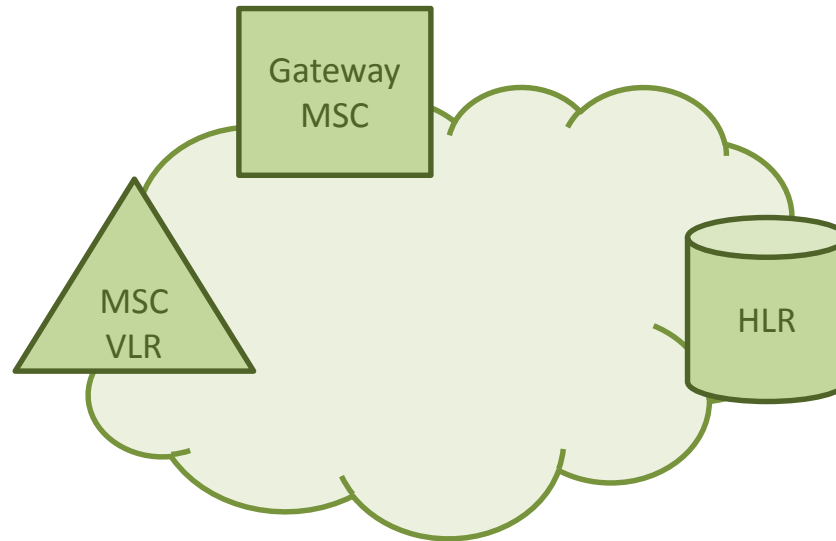
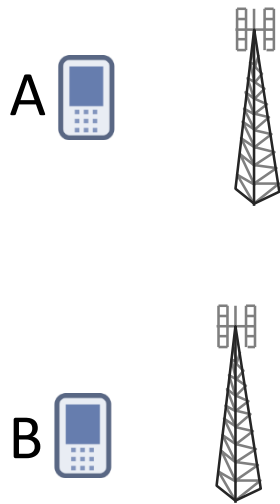
- 1) Collect info
- 2) Receive Cell ID
- 3) Get point on the map

# Collect info



We know

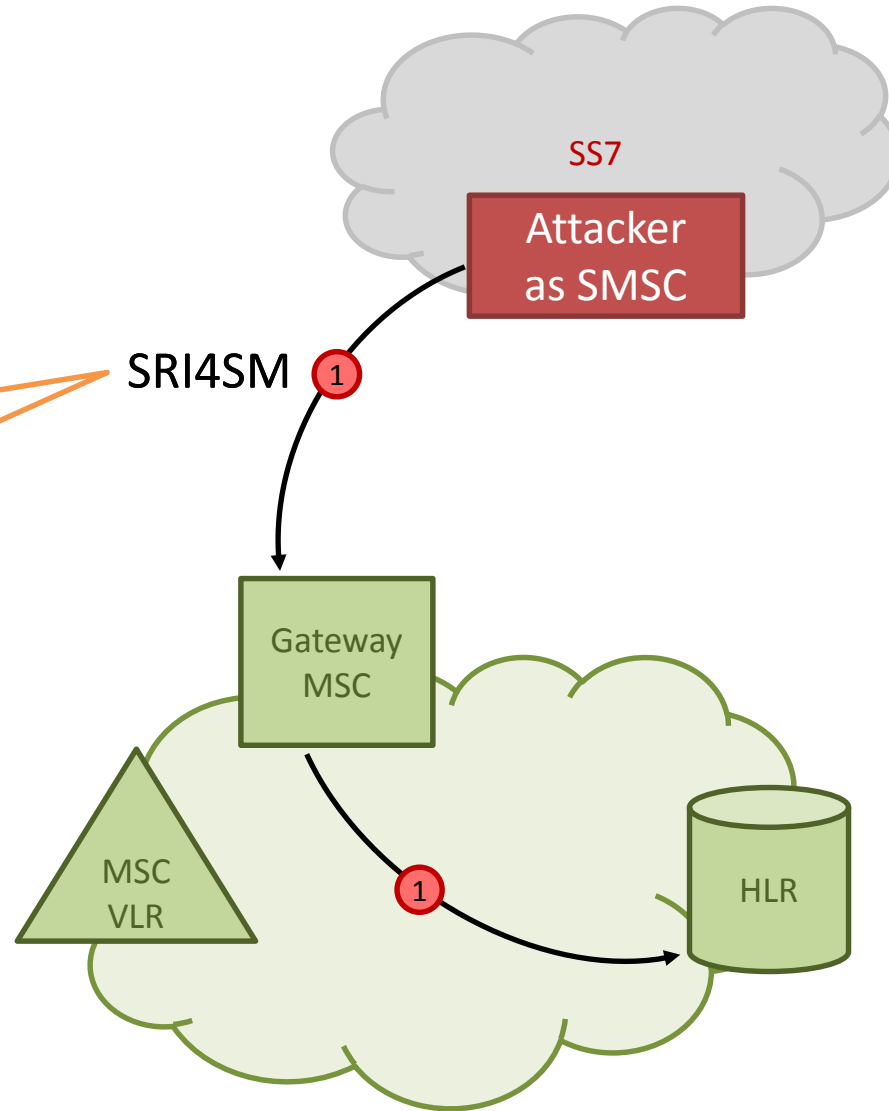
**B-Number** 0 123 45678**02**





# Collect info

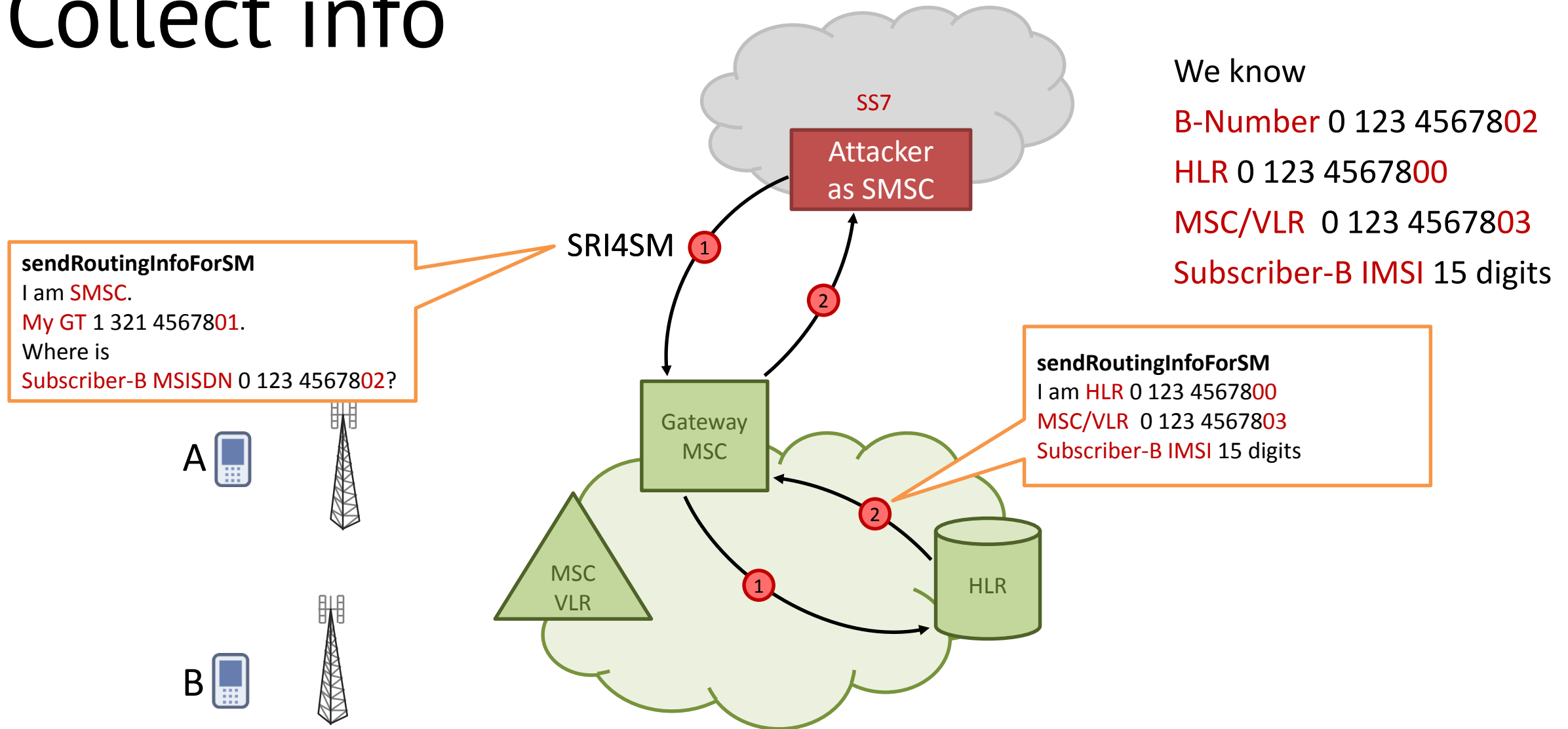
**sendRoutingInfoForSM**  
I am **SMSC**.  
My GT 1 321 4567801.  
Where is  
Subscriber-B MSISDN 0 123 4567802?



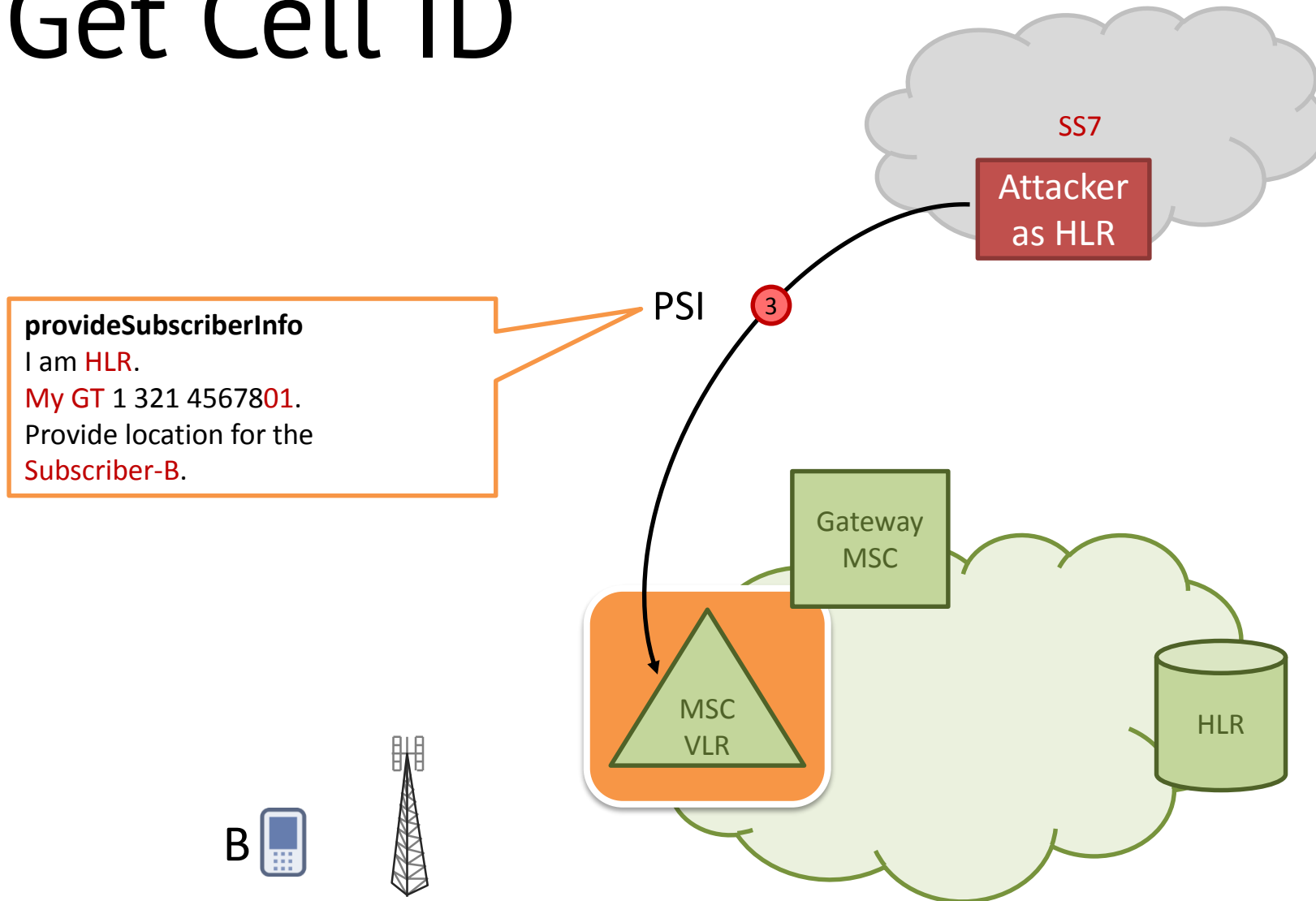
We know

**B-Number** 0 123 4567802

# Collect info



# Get Cell ID



We know

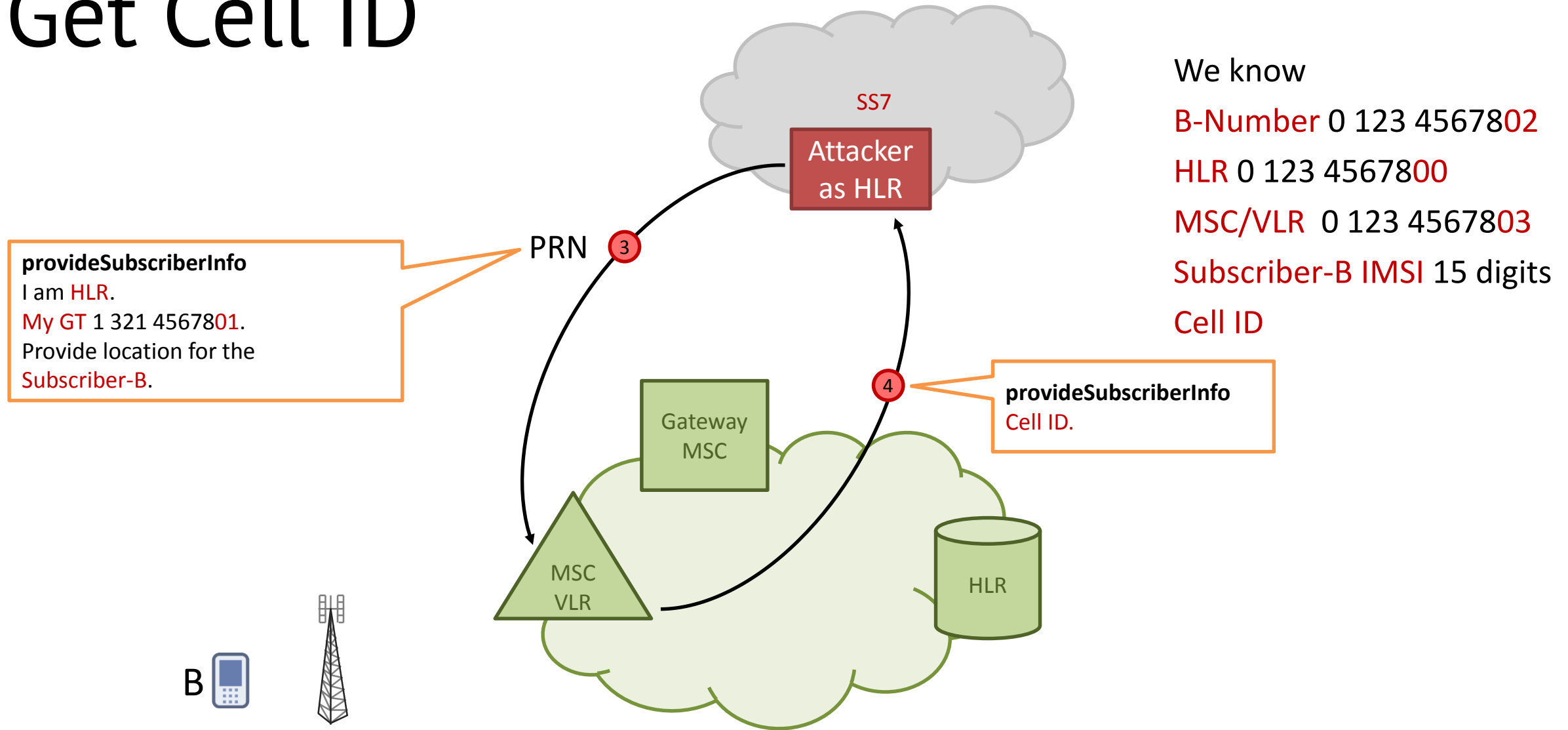
**B-Number** 0 123 4567802

**HLR** 0 123 4567800

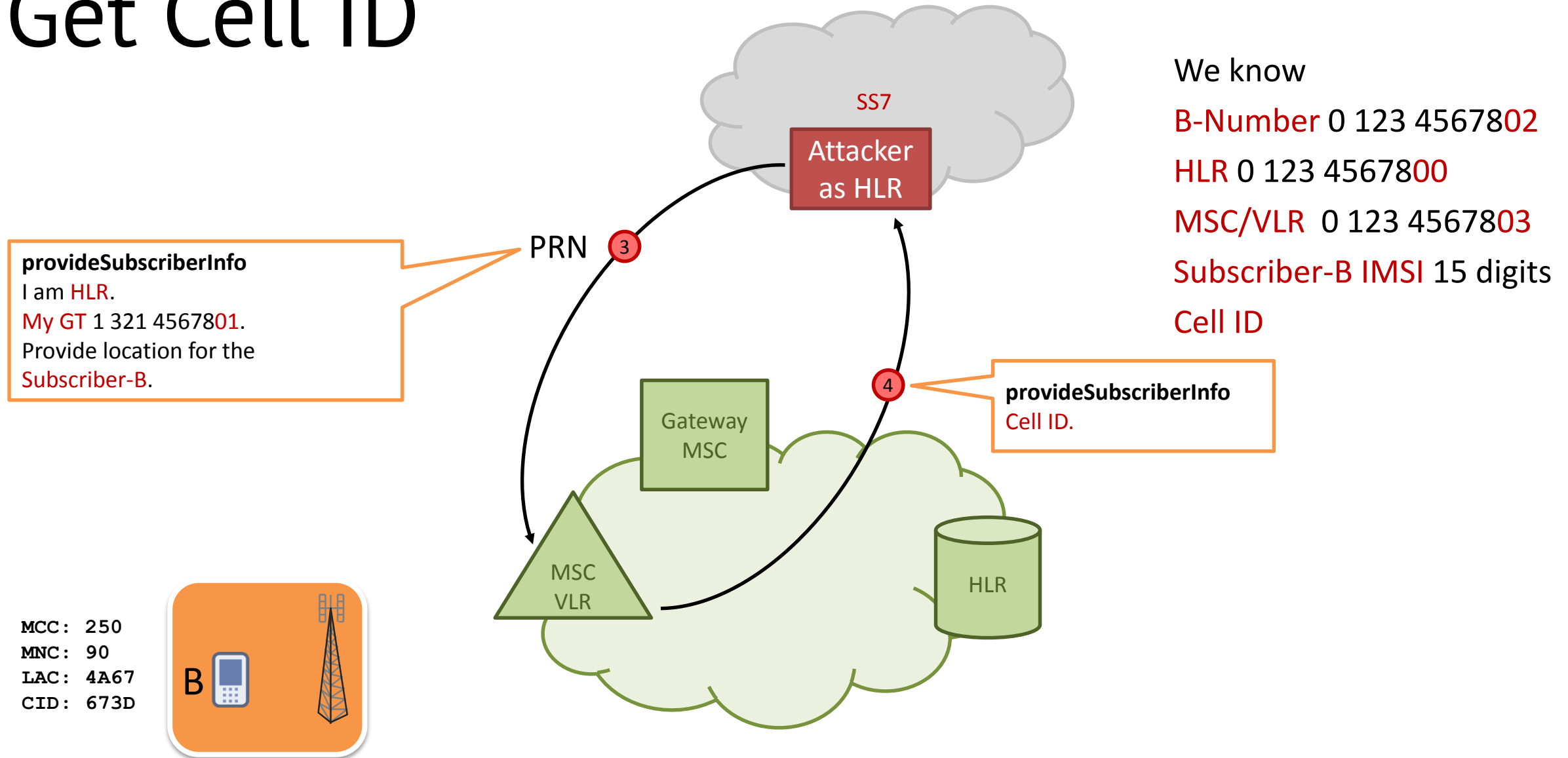
**MSC/VLR** 0 123 4567803

**Subscriber-B IMSI** 15 digits

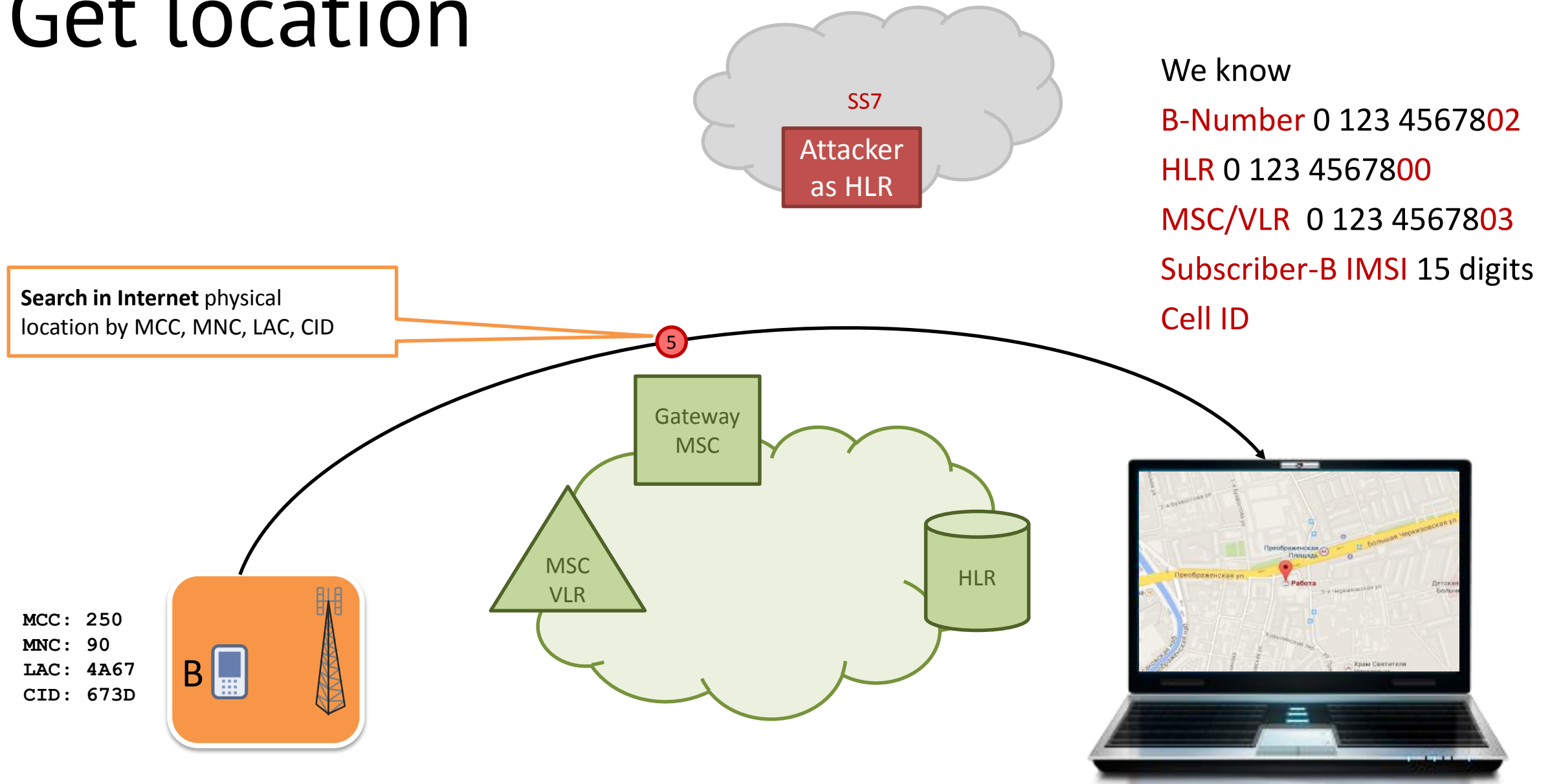
# Get Cell ID



# Get Cell ID




# Get location



# Get location

<https://www.freelancer.com/projects/geolocation/looking-get-lac-cell-from.html>

 Нужно выполнить работу?

[Опубликовать проект](#)

## Looking to get LAC/CELL ID from a VLR lookup

[f](#)[t](#)[M](#)[v](#)[p](#)[+](#) 0

Ставки	Ср. ставка (USD)	Бюджет проекта (USD)
4	\$389	\$100 - \$150

**Описание проекта:**  
Looking for a LBS provider who can immediately offer us a advanced VLR lookup service that will return the LAC code and the CID of a MSISDN using a HTTP API.  
(You have to do perform a SS7 MAP Anytime interrogation query to get the LAC and CID from the VLR.)

Price per query up to \$150. More than 50 queries per month required (\$50x150=\$7,500 monthly)

In case you are able to immediately provide a demo lookup you are welcome to bid.

Please do not bid if you are not capable of providing advanced location based services.


Skills required: Gsm Geolocation, SS7 signaling, Tier1

**Требуемые навыки:**  
Геолокация

**Показать больше** lac cid lookup, cid lac lookup, lac lookup, vlr geolocation, vlr lookup, cell lac lookup, vlr lac, lac cell, geolocation lookup lac, msisdn, geolocation api, lac cid gsm, lac cid, cell lookup google mcc lac, cell lac mnc, cell lac database, cell lac, google map api cell lac, cell lac google, cell lac info, cell lac latitude longitude java, google map cell lac, excel vba lookup cut cell, lbs, lookup


# Get location

https://www.freelancer.com/projects/geolocation/looking-get-lac-cell-from.html

 Нужно выполнить работу? Выберите категорию

[Опубликовать проект](#)

## Looking to get LAC/CELL ID from a VLR lookup

 0

Ставки	Ср. ставка (USD)	Бюджет проекта (USD)
4	\$389	\$100 - \$150

**Описание проекта:**  
Looking for a LBS provider who can immediately offer us a advanced VLR lookup service that will return the LAC code and the CID of a MSISDN using a HTTP API.  
(You have to do perform a SS7 MAP Anytime interrogation query to get the LAC and CID from the VLR.)

Price per query up to \$150. More than 50 queries per month required (\$50x150=\$7,500 monthly)

In case you are able to immediately provide a demo lookup you are welcome to bid.

Please do not bid if you are not capable of providing advanced location based services.

Skills required:Gsm Geolocation,SS7 signaling,Tier1

**Требуемые навыки:**  
Геолокация

**Показать больше** lac cid lookup, cid lac lookup, lac lookup, vlr geolocation, vlr lookup, cell lac lookup, vlr lac, lac cell, geolocation lookup lac, msisdn, geolocation api, lac cid gsm, lac cid, cell lookup google mcc lac, cell lac mnc, cell lac database, cell lac, google map api cell lac, cell lac google, cell lac info, cell lac latitude longitude java, google map cell lac, excel vba lookup cut cell, lbs, lookup





# Voice Call Interception

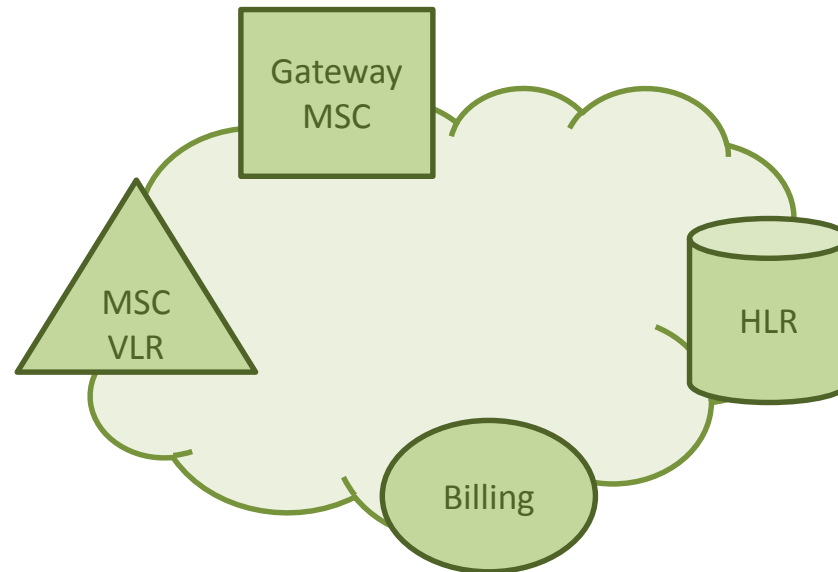
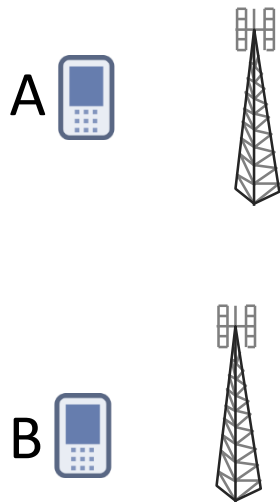
- 1) Collect info
- 2) Change subscriber profile
- 3) Add third party into mobile call

# Collect info



We know

A-Number 0 123 4567802



# Collect info

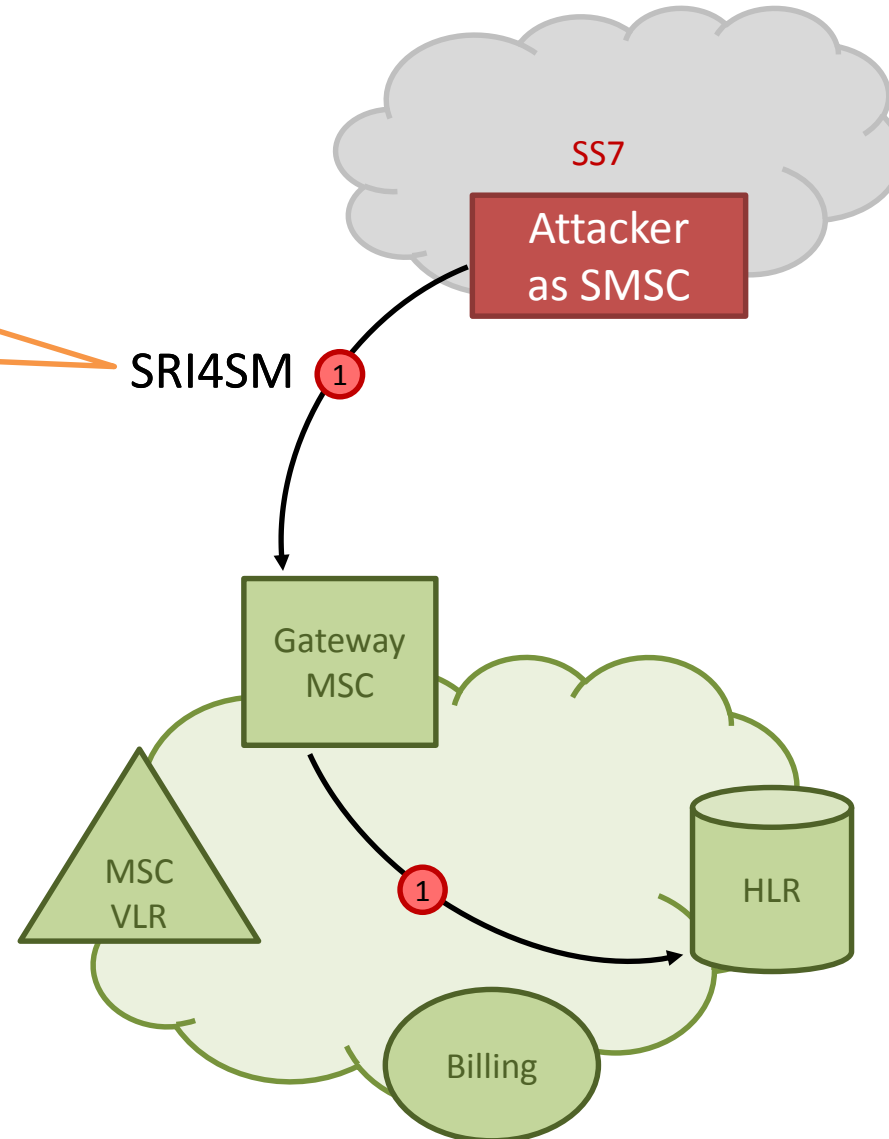
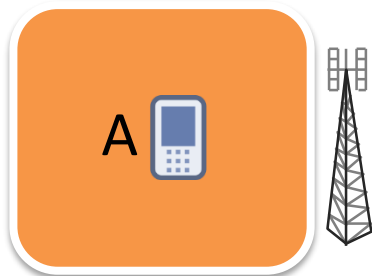
**sendRoutingInfoForSM**

I am **SMSC**.

My **GT** 1 321 456780**1**.

Where is

**Subscriber-A MSISDN** 0 123 456780**2**?



We know

**A-Number** 0 123 456780**2**

# Collect info

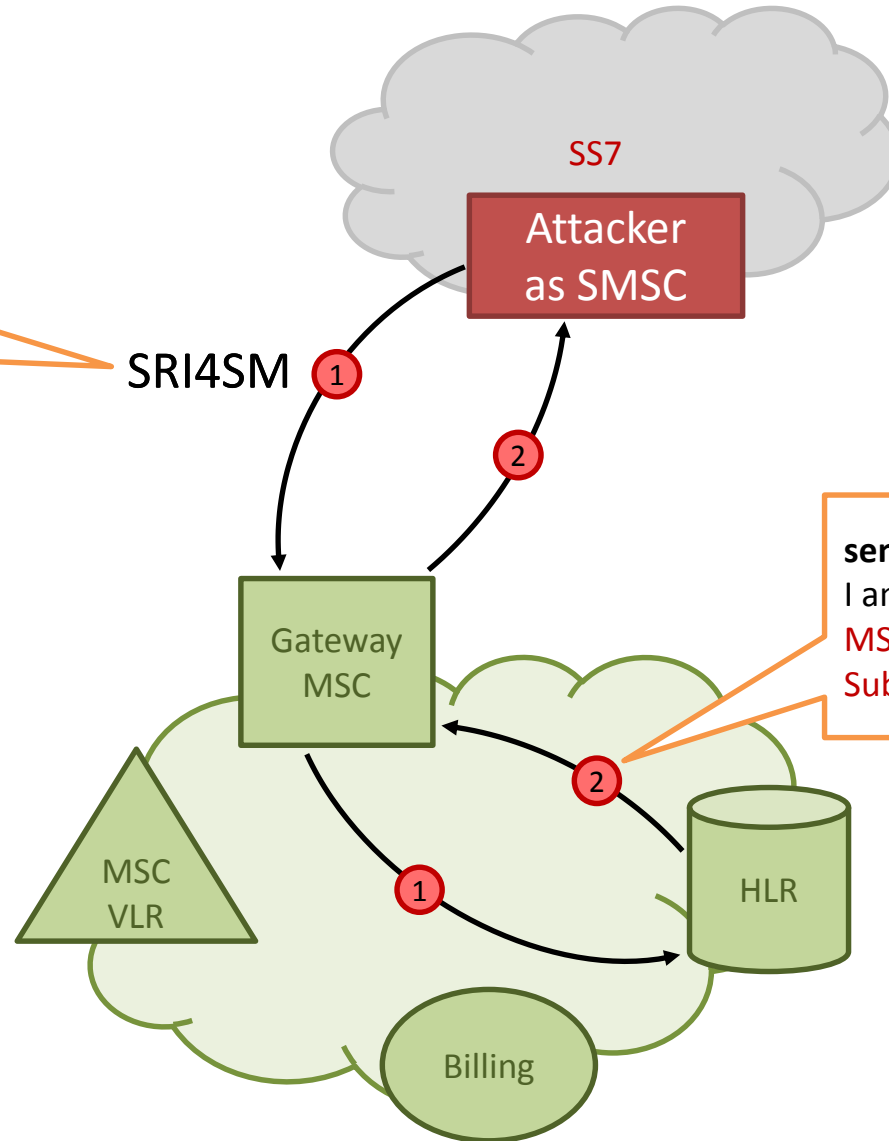
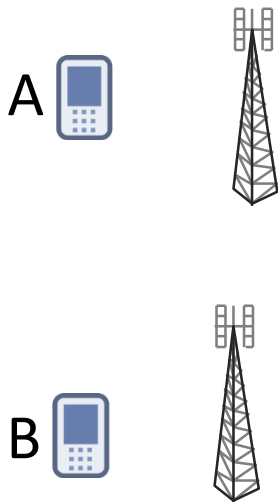
**sendRoutingInfoForSM**

I am **SMSC**.

**My GT** 1 321 456780**1**.

Where is

**Subscriber-A MSISDN** 0 123 456780**2**?



We know

**A-Number** 0 123 456780**2**

**HLR** 0 123 456780**0**

**MSC/VLR** 0 123 456780**3**

**Subscriber-A IMSI** 15 digits

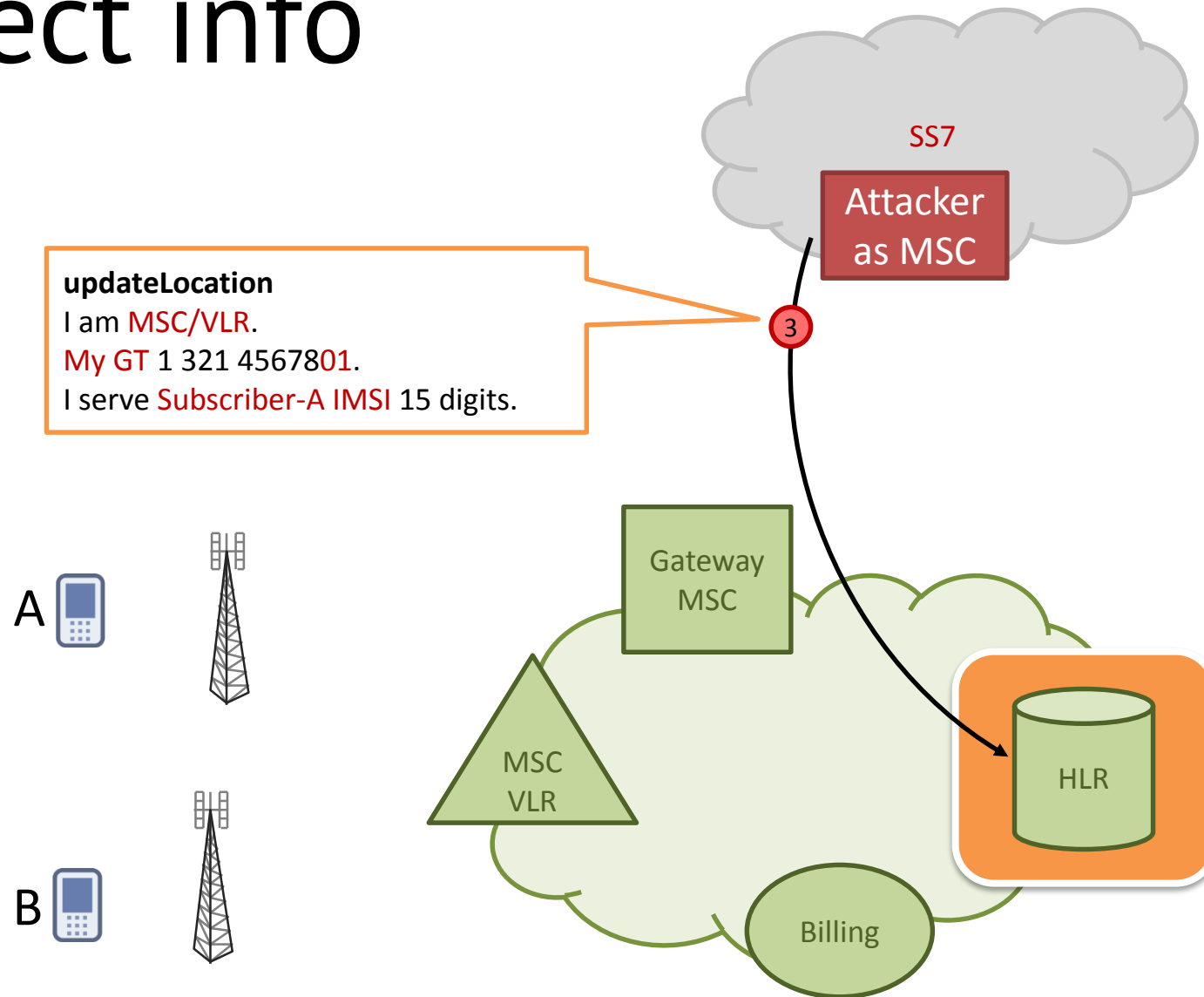
**sendRoutingInfoForSM**

I am **HLR** 0 123 456780**0**

**MSC/VLR** 0 123 456780**3**

**Subscriber-A IMSI** 15 digits

# Collect info



We know

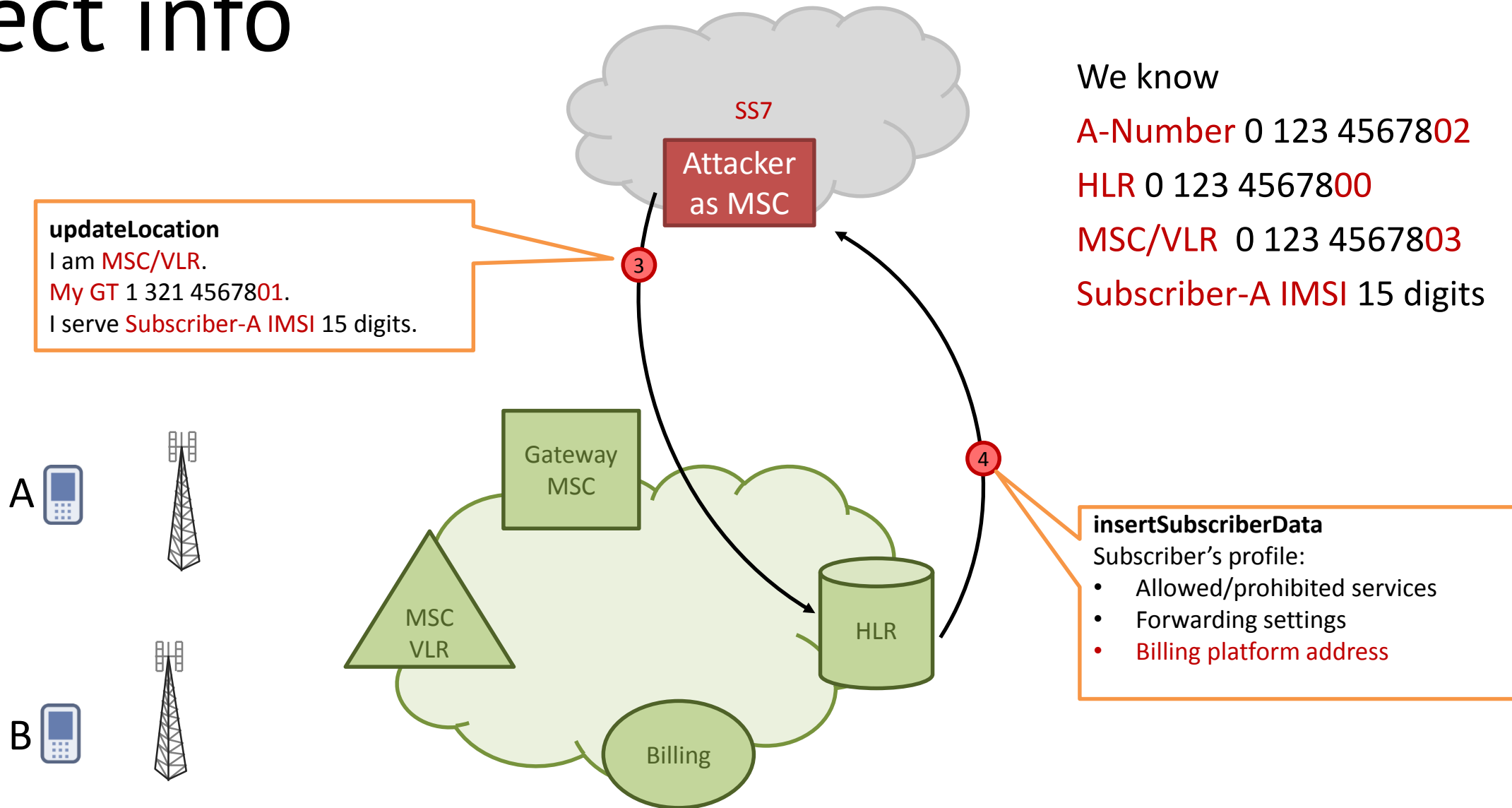
**A-Number** 0 123 45678**02**

**HLR** 0 123 45678**00**

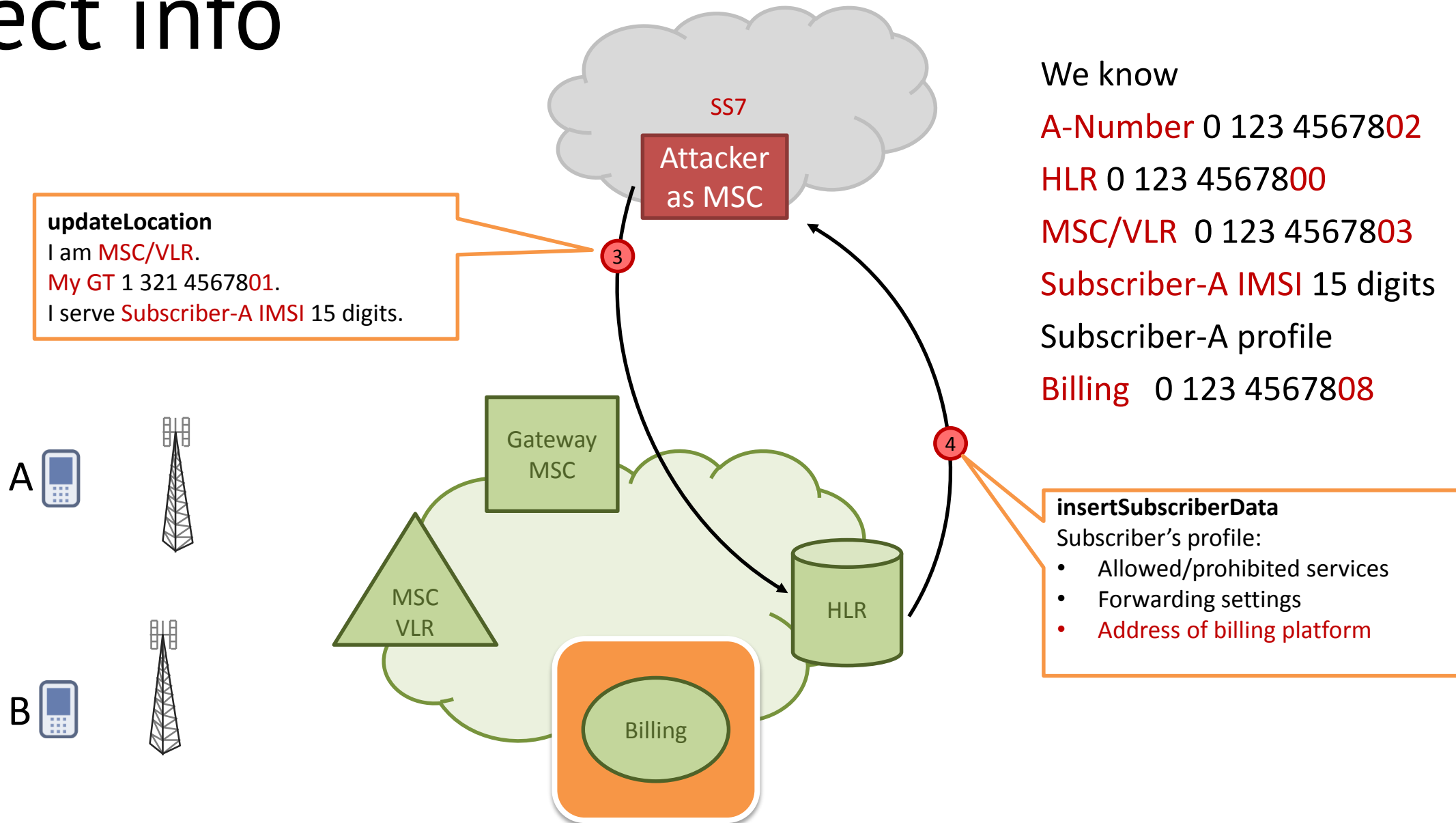
**MSC/VLR** 0 123 45678**03**

**Subscriber-A IMSI** 15 digits

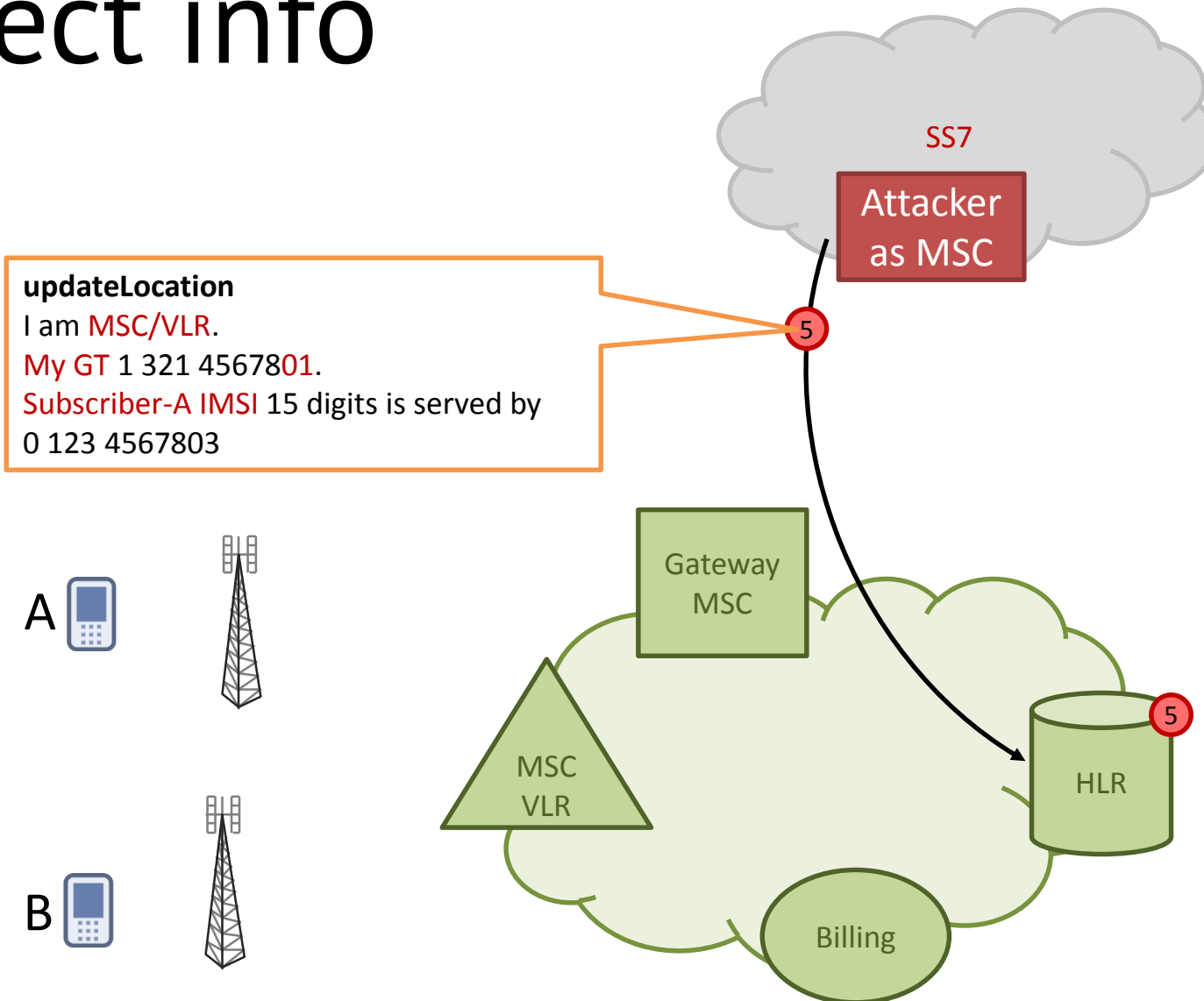
# Collect info



# Collect info



# Collect info



We know

**A-Number** 0 123 45678**02**

**HLR** 0 123 45678**00**

**MSC/VLR** 0 123 45678**03**

**Subscriber-A IMSI** 15 digits

**Subscriber-A profile**

**Billing** 0 123 45678**08**



# Collect info

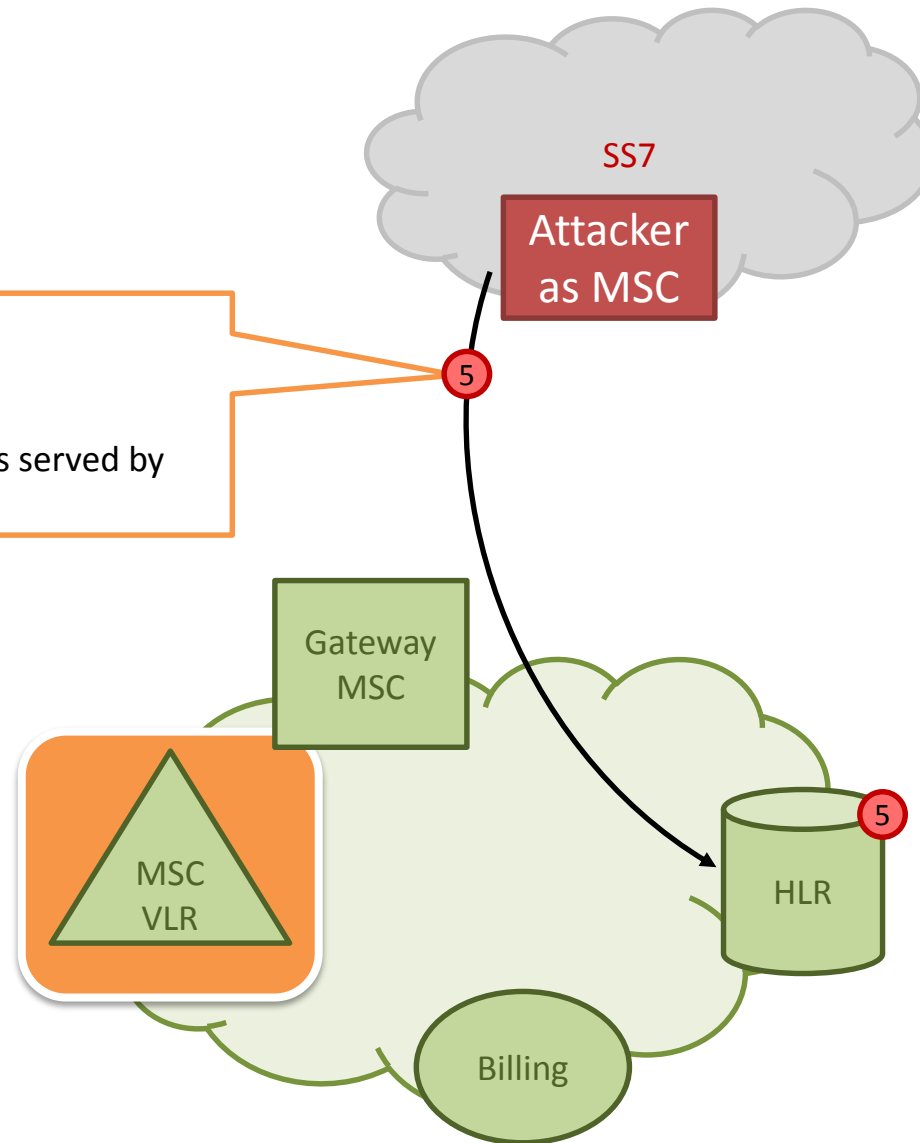
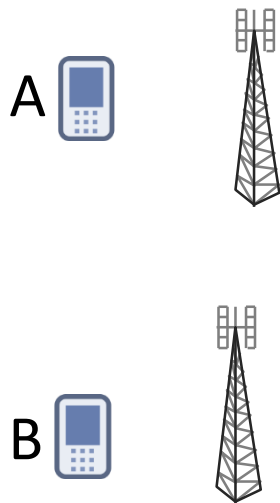
## updateLocation

I am MSC/VLR.

My GT 1 321 4567801.

Subscriber-A IMSI 15 digits is served by

0 123 4567803



We know

A-Number 0 123 4567802

HLR 0 123 4567800

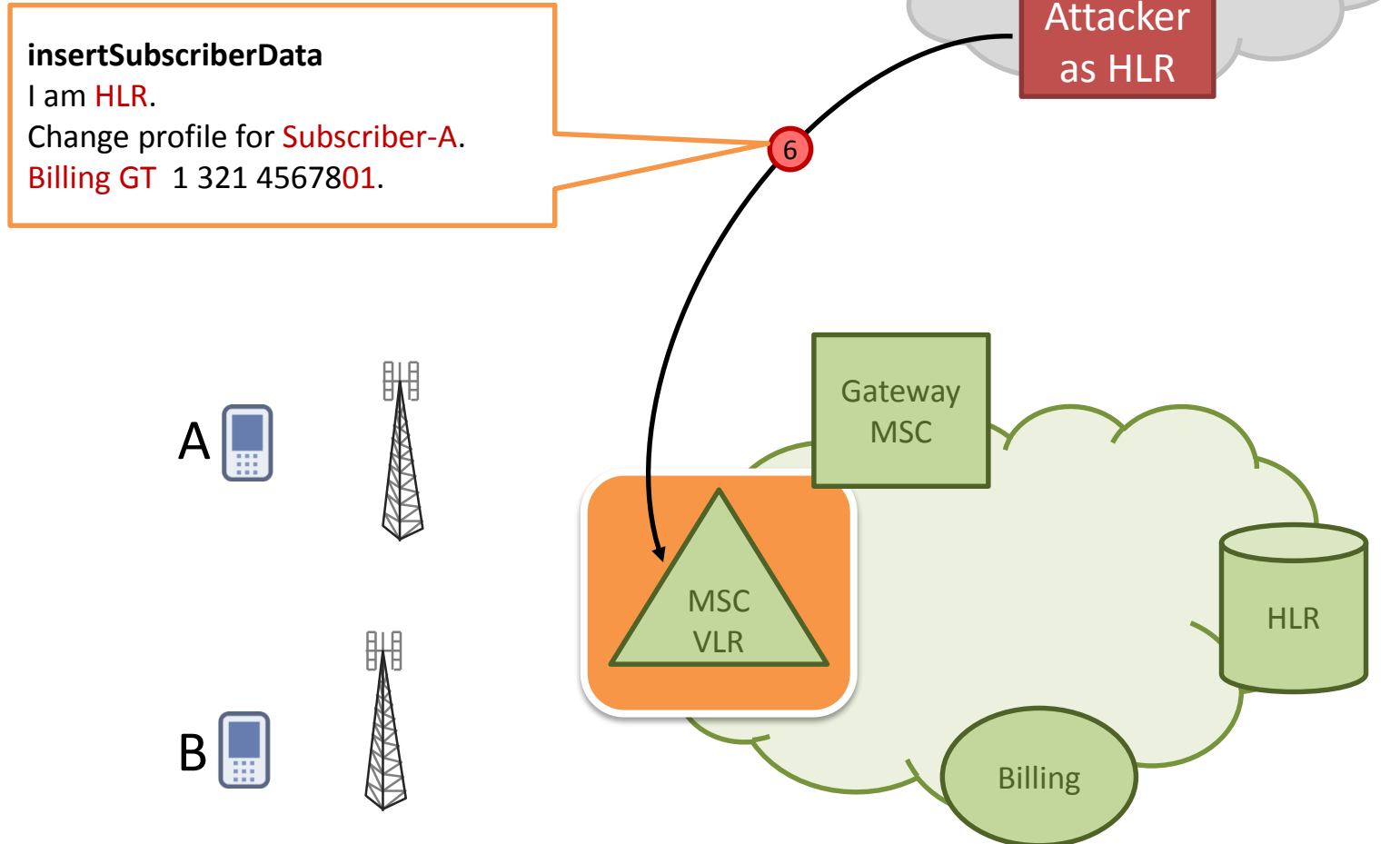
MSC/VLR 0 123 4567803

Subscriber-A IMSI 15 digits

Subscriber-A profile

Billing 0 123 4567808

# Change profile



We know

**A-Number** 0 123 456780**2**

**HLR** 0 123 456780**0**

**MSC/VLR** 0 123 456780**3**

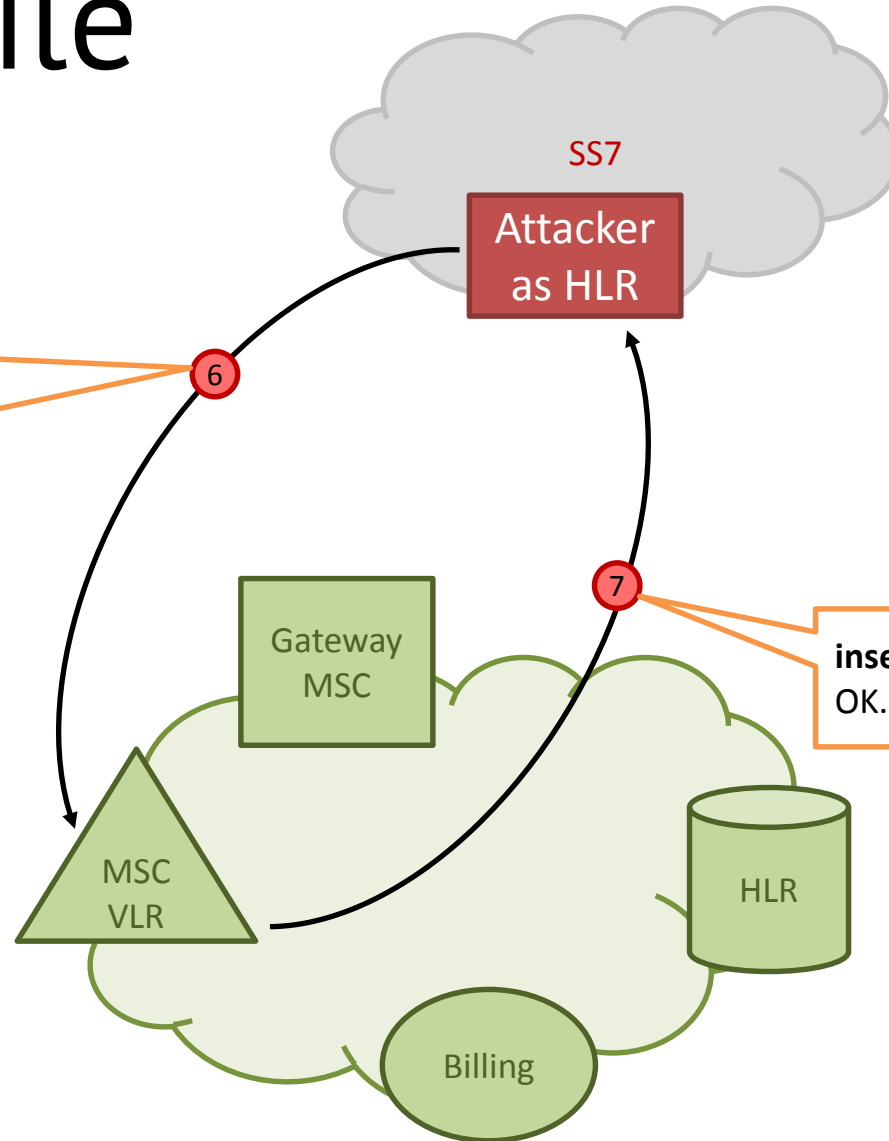
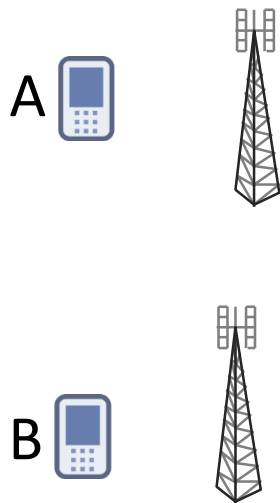
**Subscriber-A IMSI** 15 digits

**Subscriber-A profile**

**Billing** 0 123 456780**8**

# Change profile

**insertSubscriberData**  
I am **HLR**.  
Change profile for **Subscriber-A**.  
**Billing GT** 1 321 4567801.



We know

**A-Number** 0 123 456780**2**

**HLR** 0 123 456780**0**

**MSC/VLR** 0 123 456780**3**

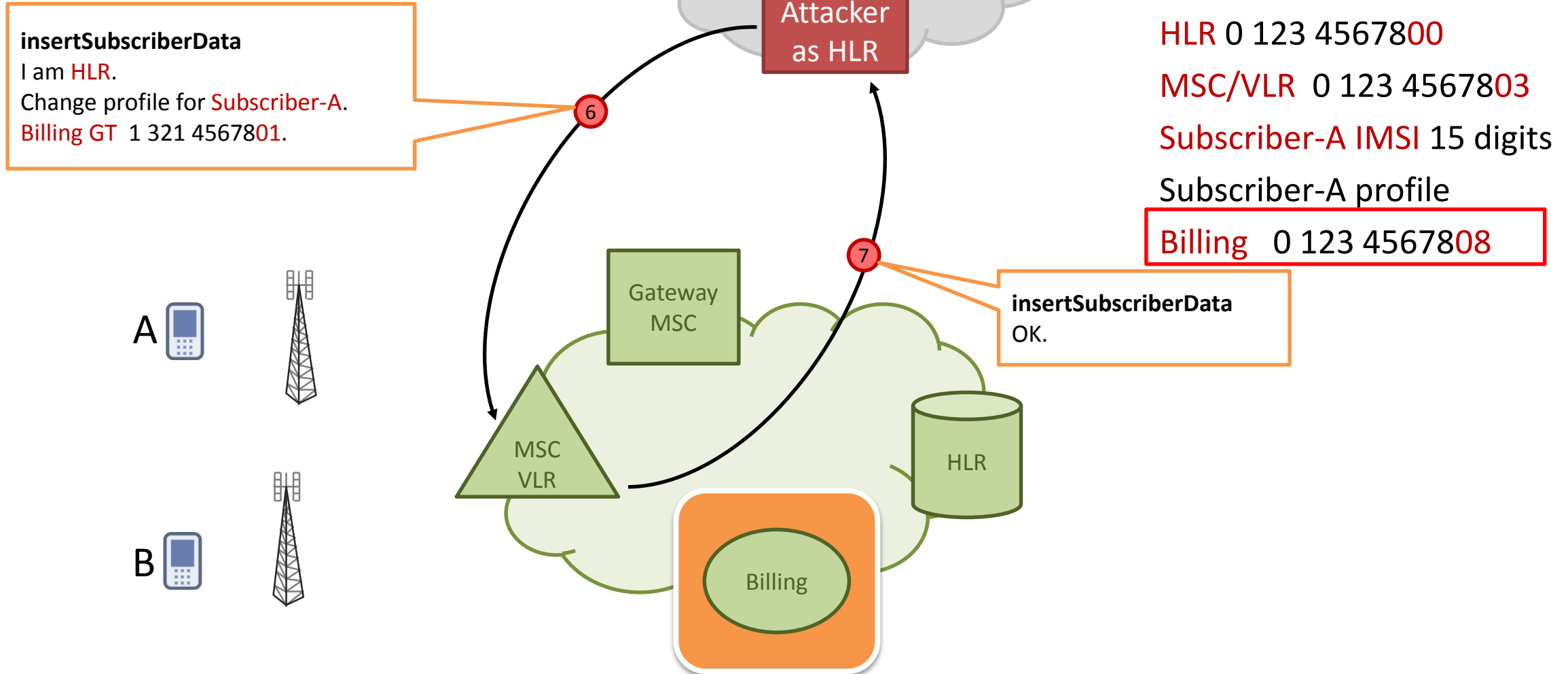
**Subscriber-A IMSI** 15 digits

**Subscriber-A profile**

**Billing** 0 123 456780**8**

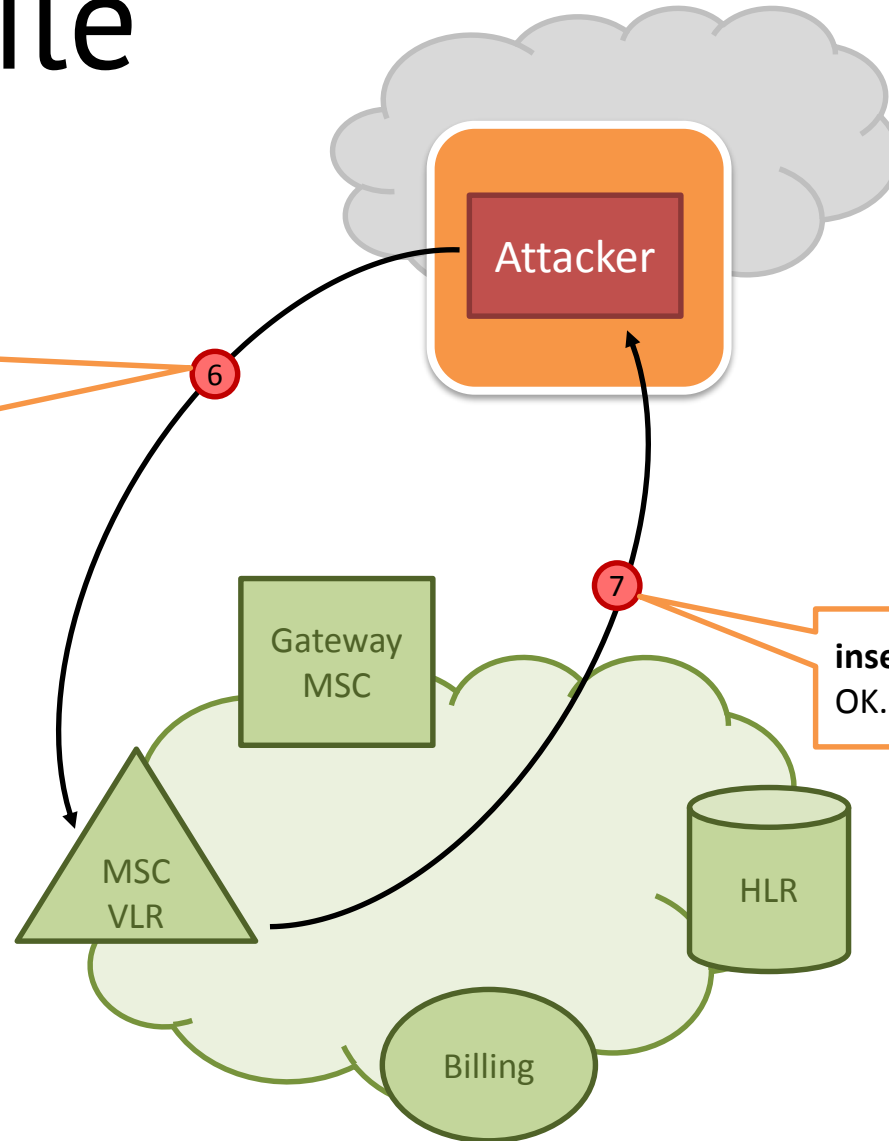
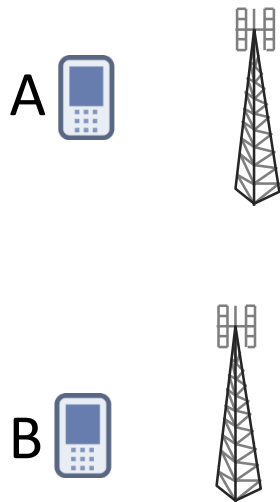
**insertSubscriberData**  
OK.

# Change profile



# Change profile

**insertSubscriberData**  
I am HLR.  
Change profile for Subscriber-A.  
Billing GT **1 321 4567801.**



We know

A-Number 0 123 4567802

HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-A IMSI 15 digits

Subscriber-A profile

Billing 0 123 4567808

**insertSubscriberData**  
OK.

# Call interception



We know

A-Number 0 123 4567802

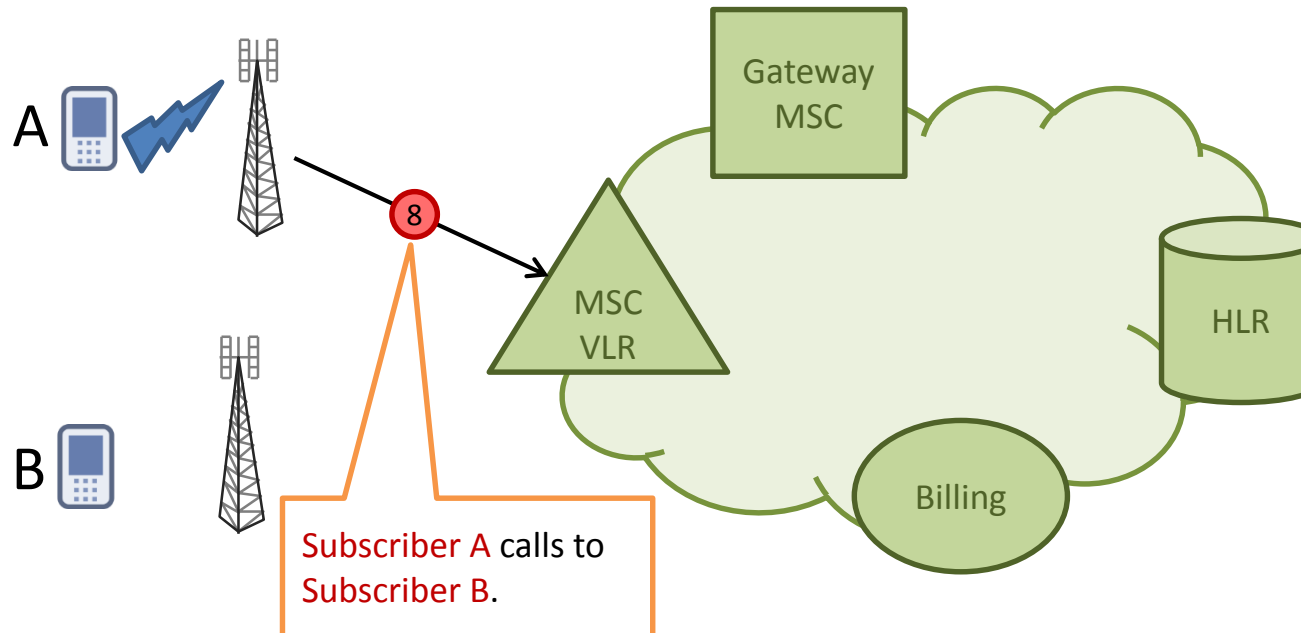
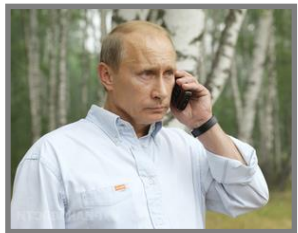
HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-A IMSI 15 digits

Subscriber-A profile

Billing 0 123 4567808



# Call interception



We know

A-Number 0 123 4567802

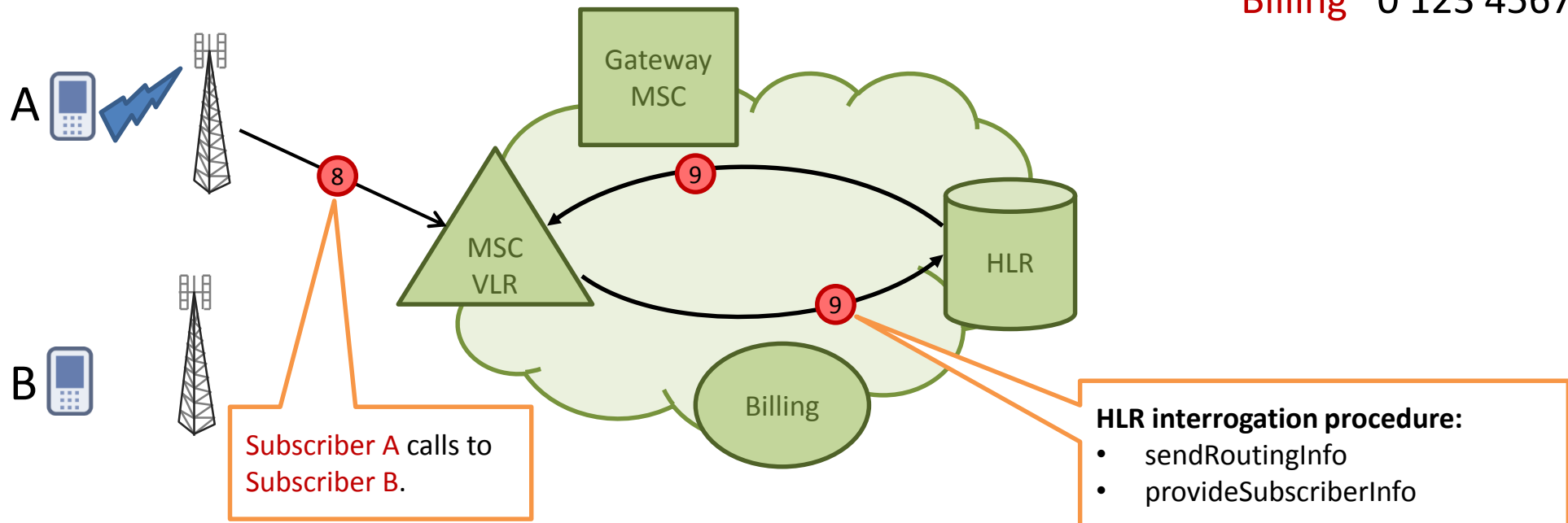
HLR 0 123 4567800

MSC/VLR 0 123 4567803

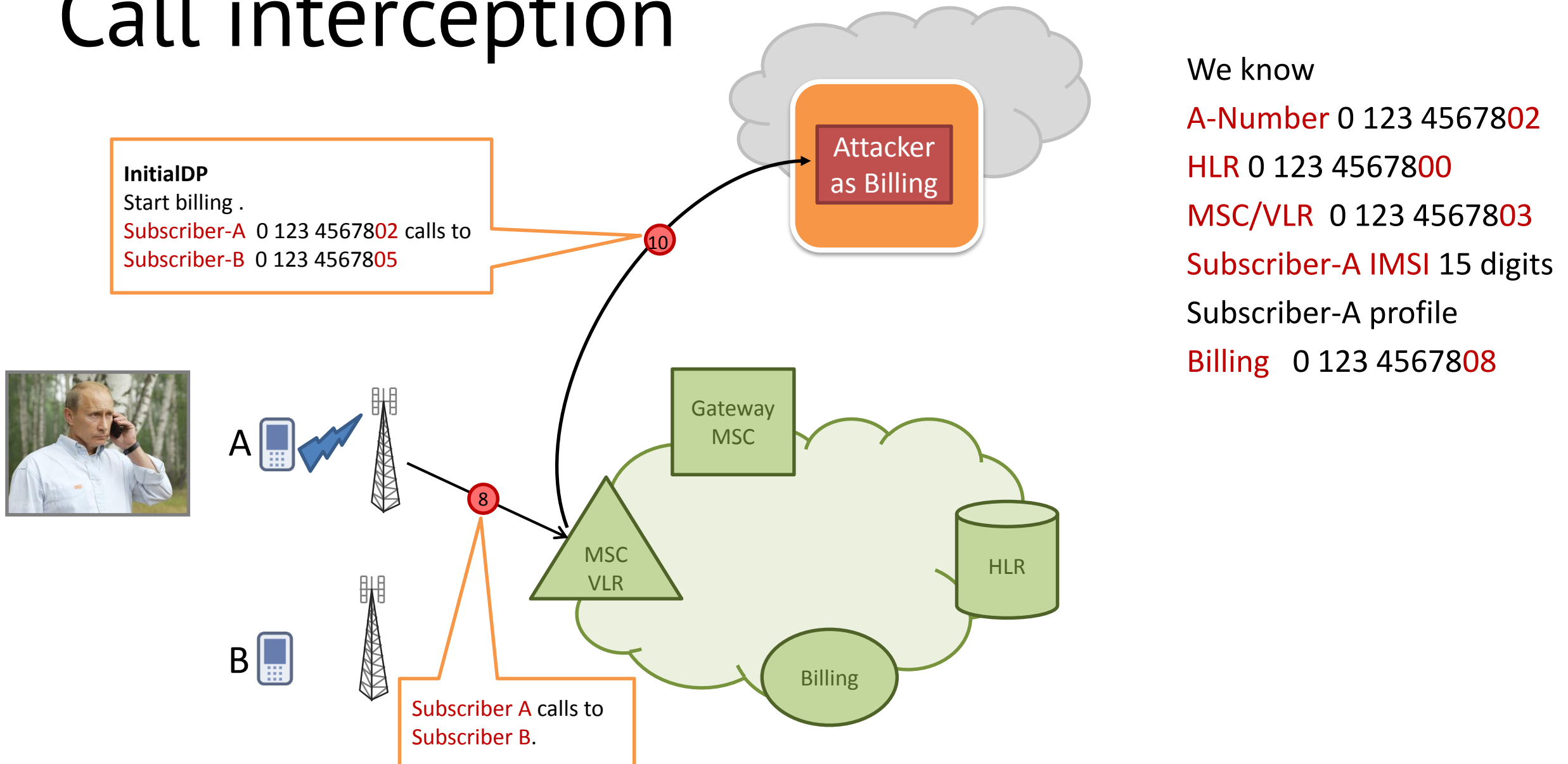
Subscriber-A IMSI 15 digits

Subscriber-A profile

Billing 0 123 4567808

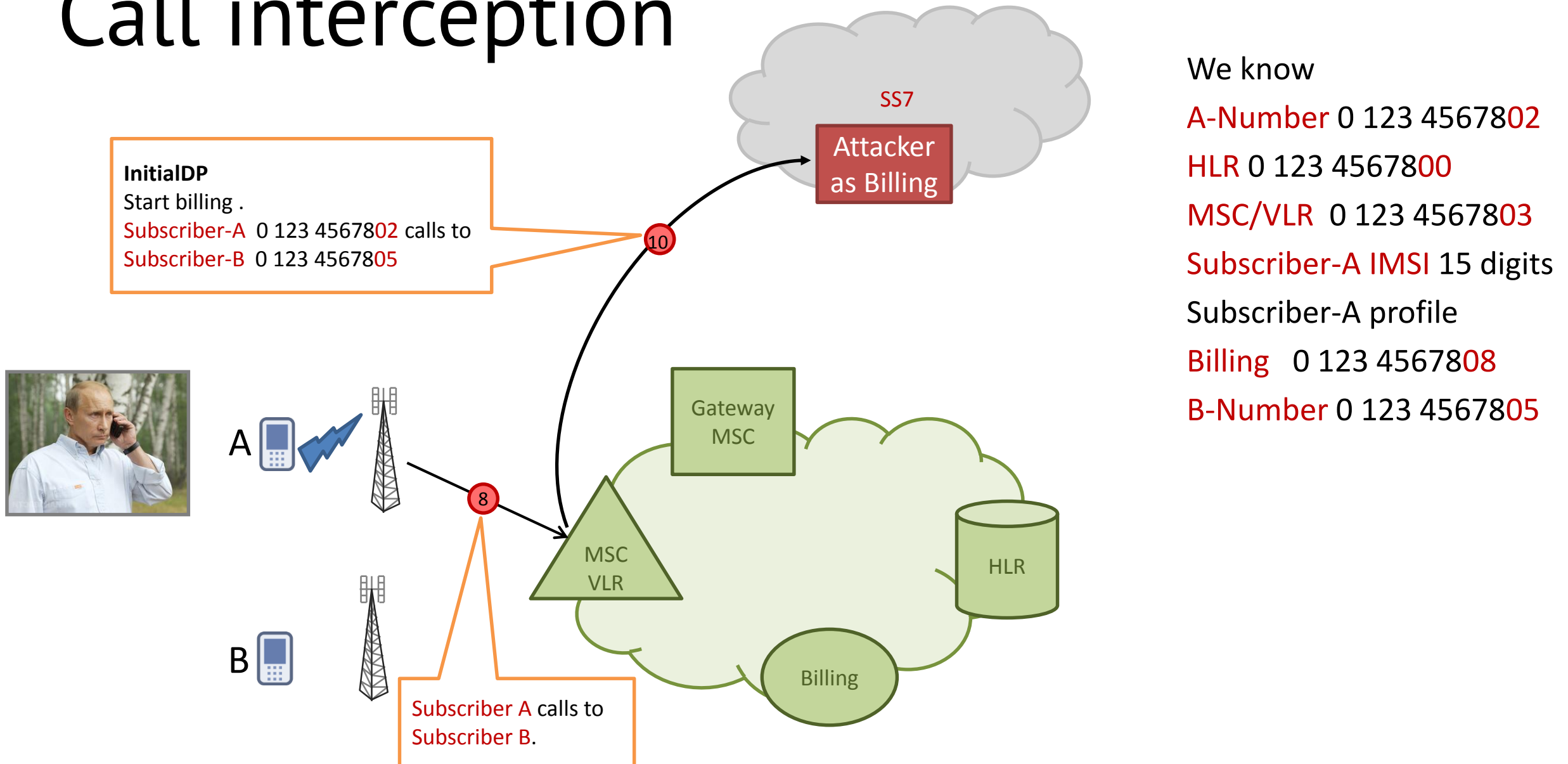


# Call interception

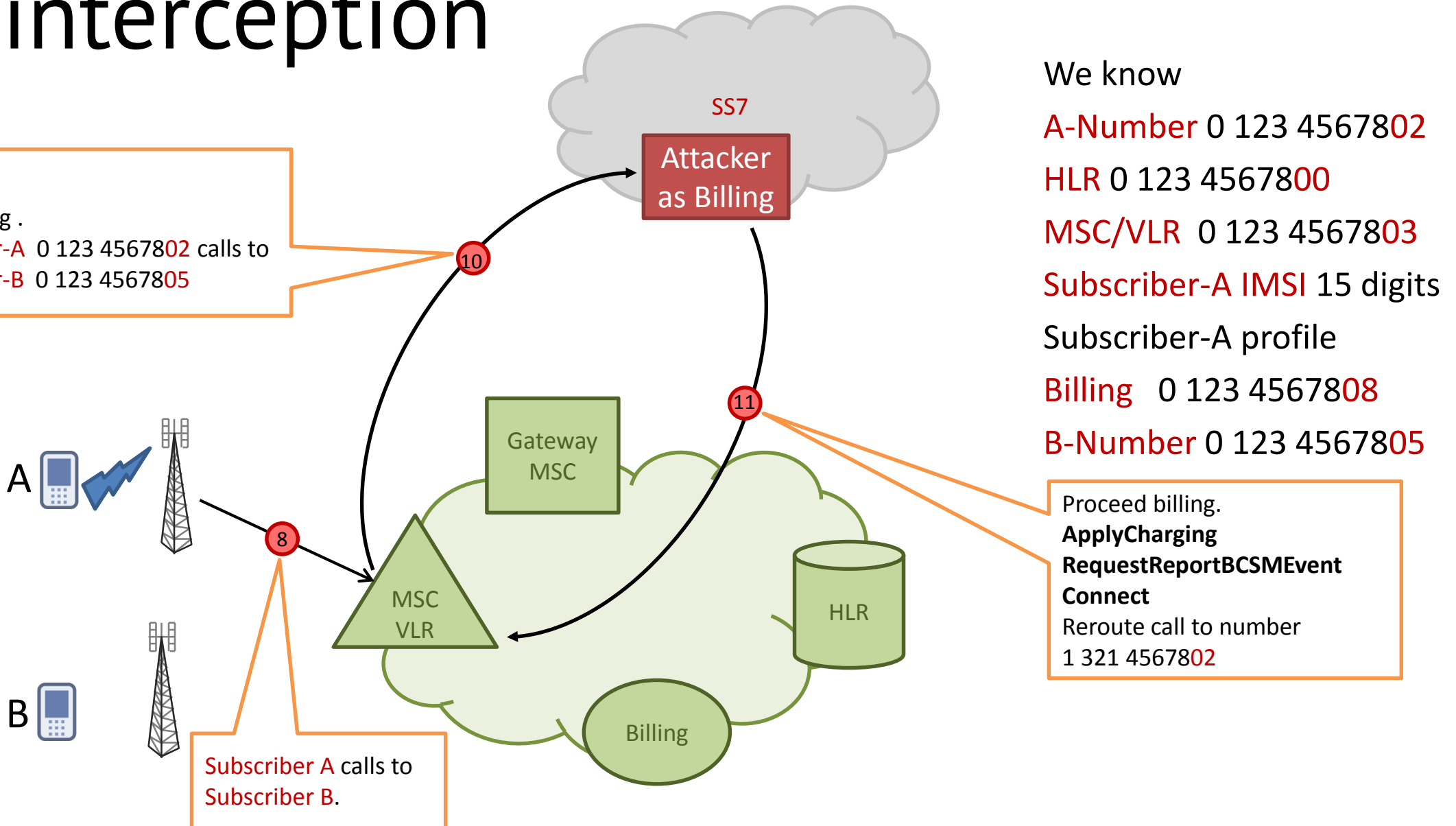




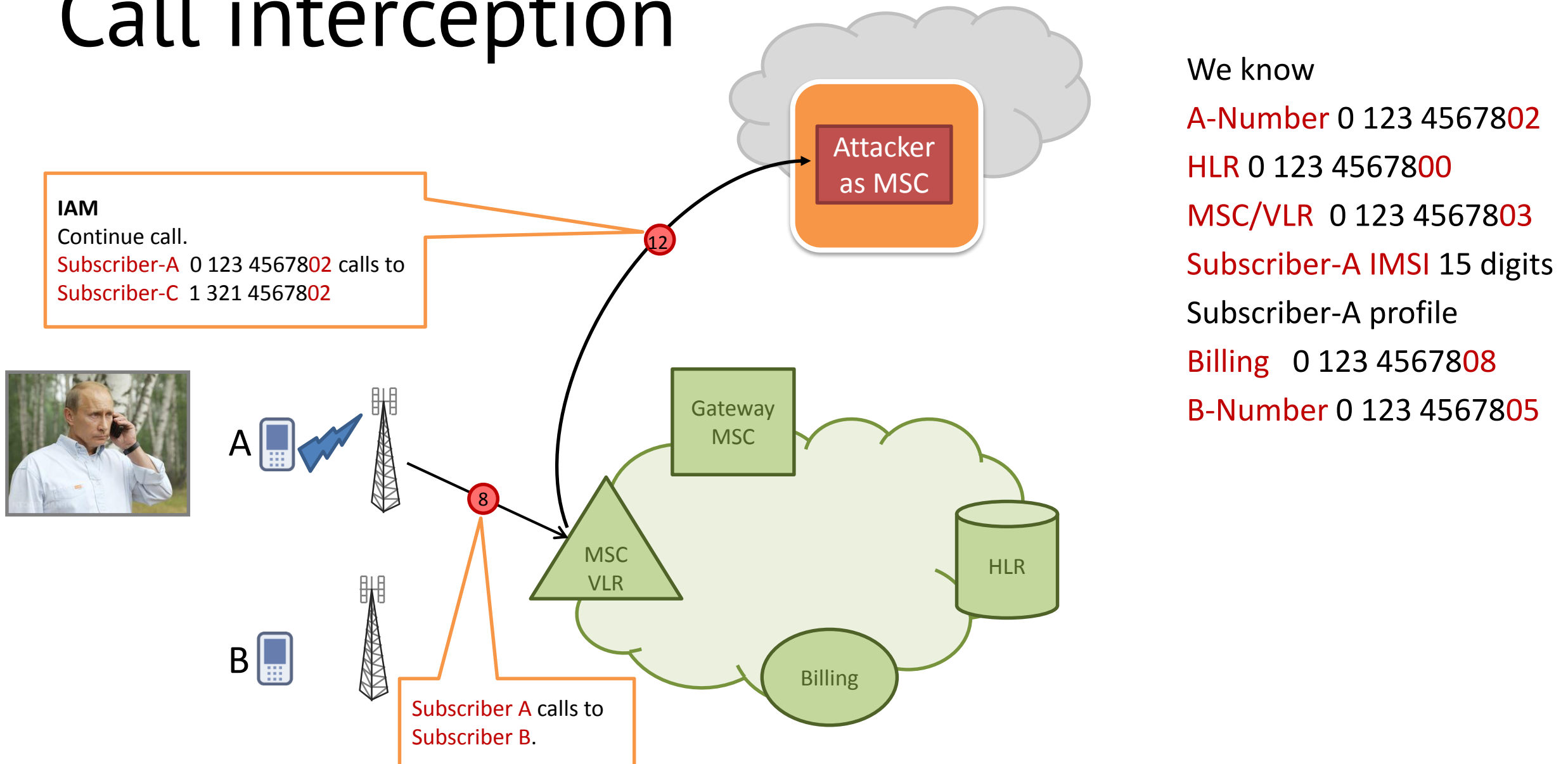
# Call interception



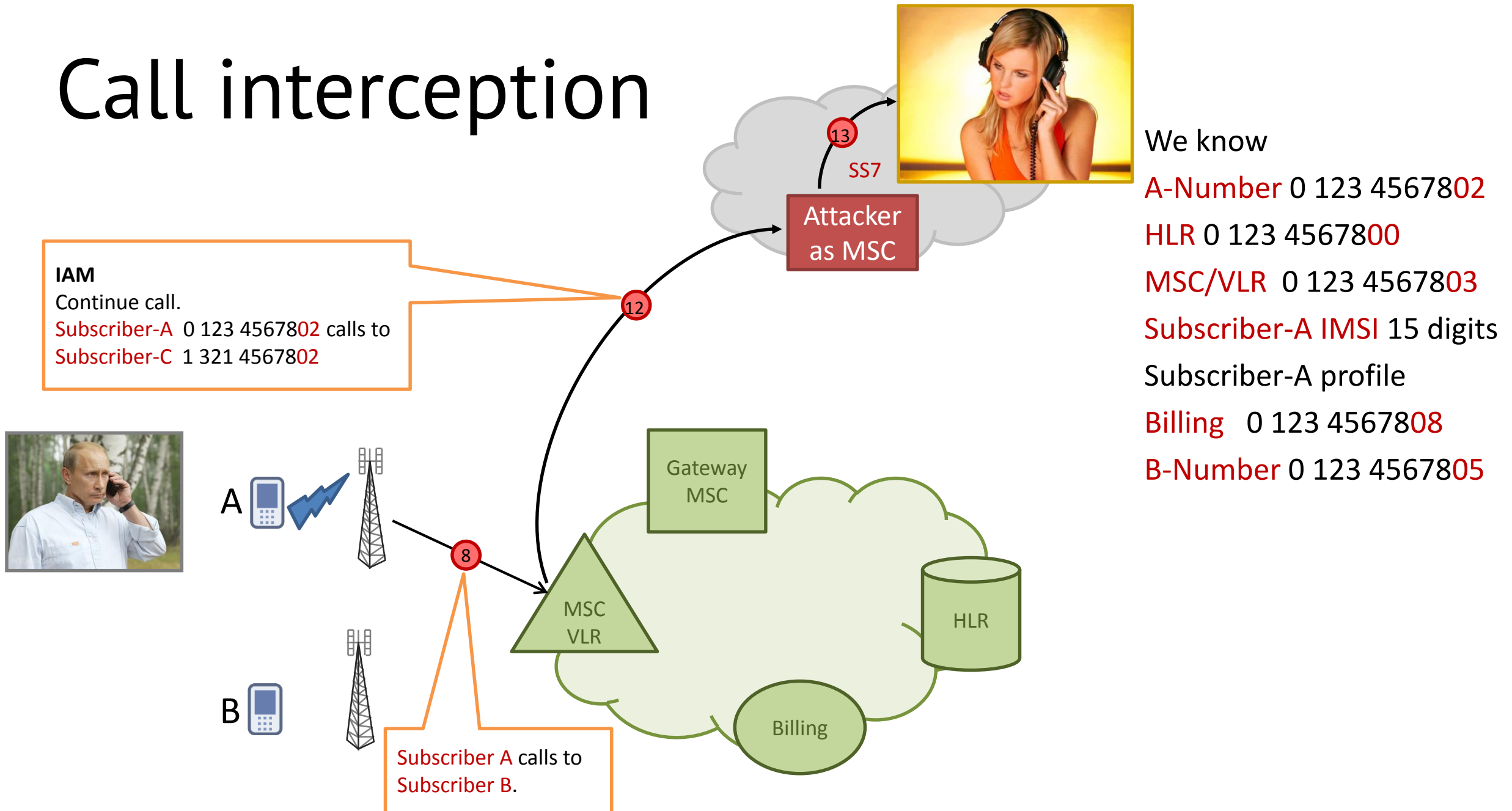
# Call interception



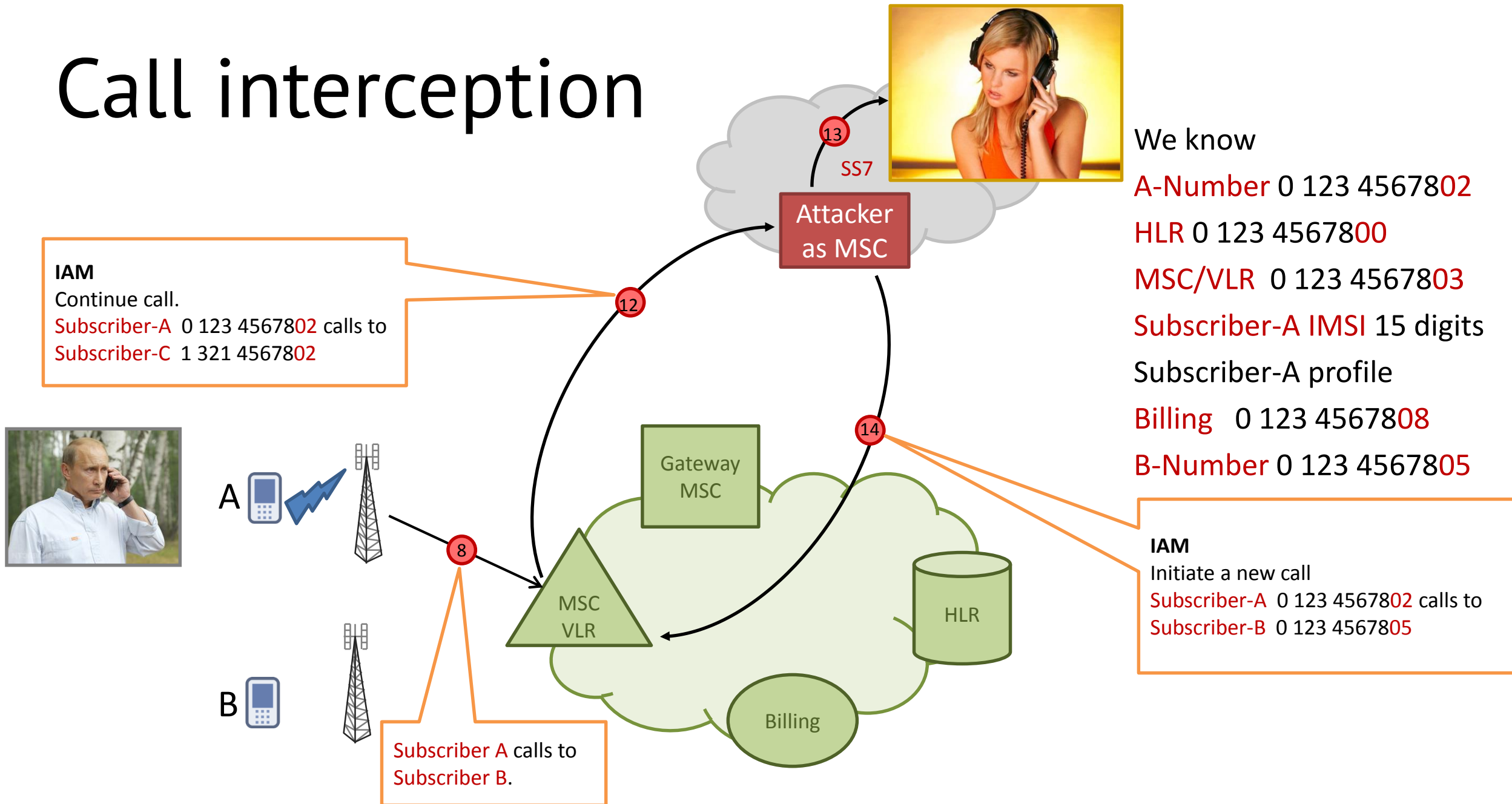
# Call interception



# Call interception



# Call interception



# Call interception



We know

A-Number 0 123 4567802

HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-A IMSI 15 digits

Subscriber-A profile

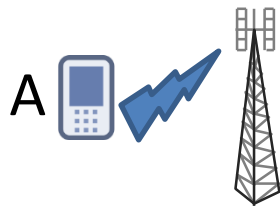
Billing 0 123 4567808

B-Number 0 123 4567805

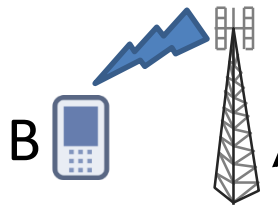
## IAM

Continue call.

Subscriber-A 0 123 4567802 calls to  
Subscriber-C 1 321 4567802

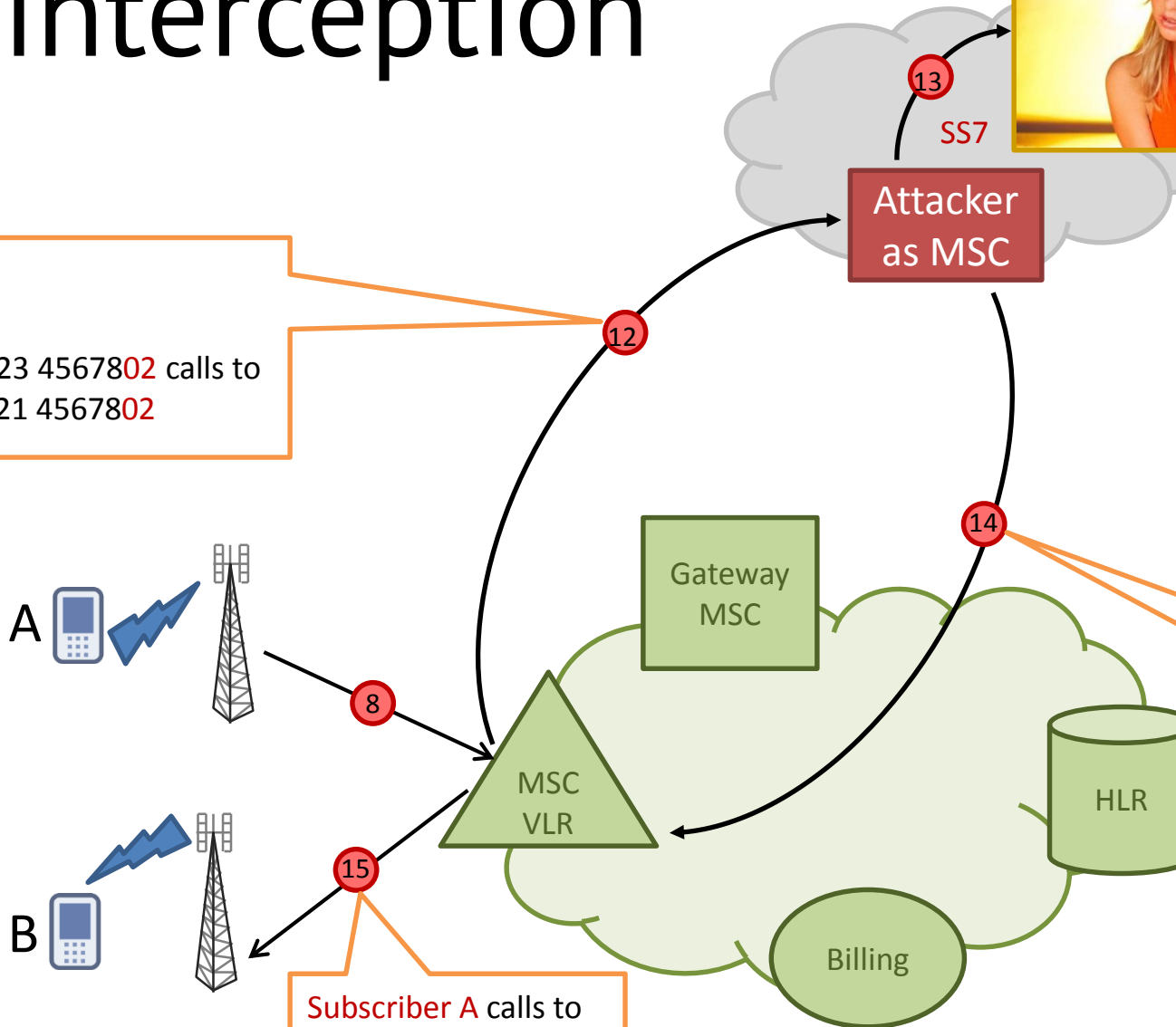


A



B

Subscriber A calls to  
Subscriber B.



## IAM

Initiate a new call

Subscriber-A 0 123 4567802 calls to  
Subscriber-B 0 123 4567805





*That's all Folks!*

# Conclusion

SS7 rules

Just the tip of the iceberg





# The End.

# Questions?

Sergey Puzankov

Dmitry Kurbatov

[spuzankov@ptsecurity.com](mailto:spuzankov@ptsecurity.com)

[dkurbatov@ptsecurity.com](mailto:dkurbatov@ptsecurity.com)



POSITIVE TECHNOLOGIES