
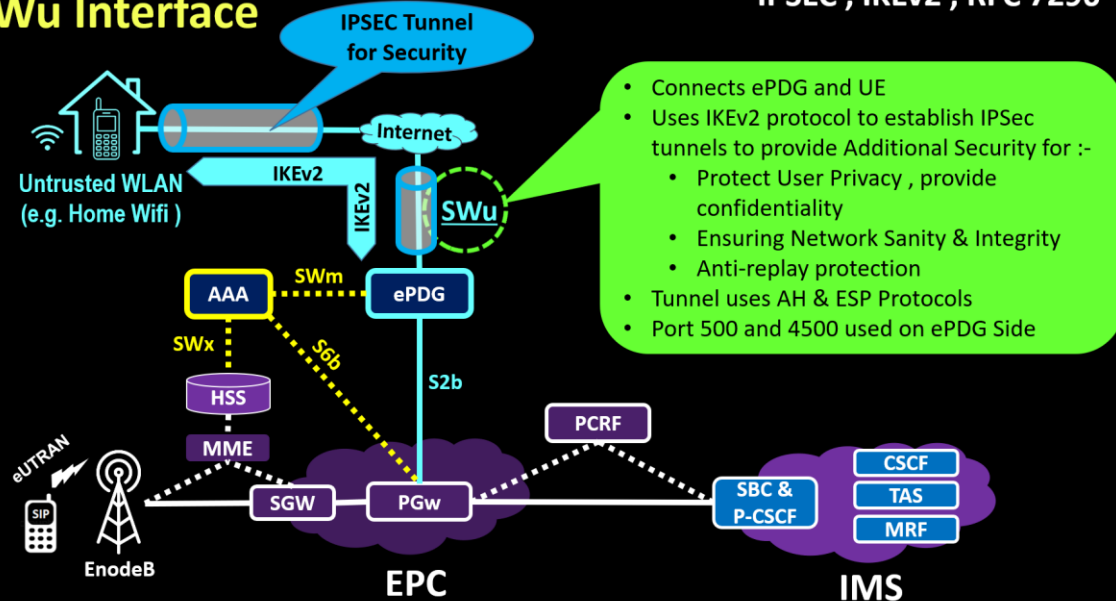




SWu Interface

SWu Interface

IPSEC , IKEv2 , RFC 7296 



Let's start with SWu Interface

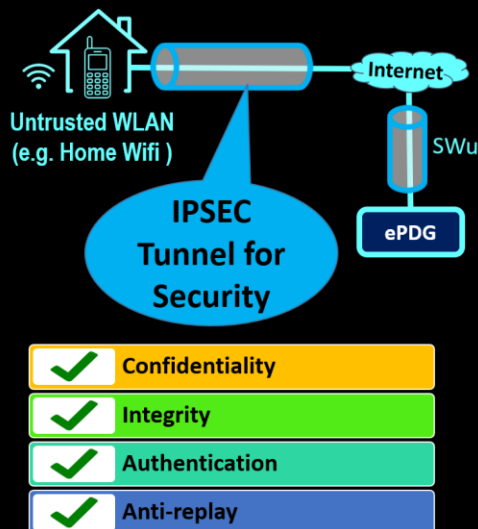
1. This Interface is used between ePDG and UE
2. SWu interface is running on IKEv2 – i.e. Internet Key Exchange
3. It uses IKEv2 protocol to establish IPsec tunnel between ePDG and UE
4. IKEv2 is used to perform IPSEC authentication, session development and negotiation of IPSEC Tunnels
5. It is a secure Interface from Core Networks towards users in non-3GPP access network
6. Since Users or UE is residing in non-3GPP access networks , Additional Security via IPSEC Tunnel & IKEv2 protocol is implemented via Encryption of traffic & Use of cryptographic techniques for :-
 - Protect User Privacy , provide confidentiality
 - Ensuring Network Sanity & Integrity
 - Error Free authentication
 - Anti-replay protection
7. These IPSEC tunnels are supported on both IPv4 & IPv6 IP Addresses . These uses AH & ESP Protocols . Typically VoWifi uses UE to connect to ePDG Public IP on Port 500 and 4500 for Setup and IPsec encrypted packets transfer . Which Means these Ports has to be allowed on both UE Side CPE & ePDG Side firewalls
8. As far as specs are concerned , You can refer to **RFC 5996 / 7296** for more details on IKEv2 and IPsec ESP encryption used here



What is IP Sec ?

8

What is IP Sec ?



Authentication Header (AH)

- Data integrity
- Data origin authentication
- Replay protection

Encapsulating Security Payload (ESP)

- Encryption only
- Authentication only (Integrity , Origin authentication , Replay protection)
- Both Encryption and authentication

www.TelecomTutorial.info

IPSEC Stands for Internet Protocol Security (IPsec) , Well it allows us to secure the network layer IP traffic . Since VoWifi traffic transit via Internet , It becomes important for us to protect it otherwise Man in Middle can decode you traffic can listen all your calls and read your SMS during transit Below features are offered by IPSEC :-

- **Confidentiality** : IPSEC ensures that No one but the sender and receiver will be able to read our data by encrypting our data
- **Integrity** : IPSEC ensures that No body changes the data in our packets while its travelling from Internet . The sender and receiver will be able to verify whether Data have been modified during the transit using a hash value
- **Authentication** : IPSEC helps UE and ePDG to ensure that they are speaking to right entity & Not some one spoofed in Internet , Here both UE and ePDG authenticate each other
- **Anti-replay** : At worst , Even if a packet is encrypted and authenticated , the Middle man may attempt to catch and re-send those packets to make fool of receiver . IPsec protects this well

To do these things, IPsec uses two protocols which are defined by the IETF :-

1. **Authentication Header (AH)** :- Here , AH provides a method for authentication , Here AH authenticates IP headers and their payloads . AH does below tasks :-
 - a) **Data integrity** : a message digest that is generated by an algorithm such as HMAC-MD5 or HMAC-SHA



- b) **Data origin authentication** : using a shared secret key to create the message digest
- c) **Replay protection** : Replay protection is provided by using a sequence number field with the AH header

2. Encapsulating Security Payload (ESP) : ESP protocol handles Encryption & Authentication . ESP can be used in various modes such as :-

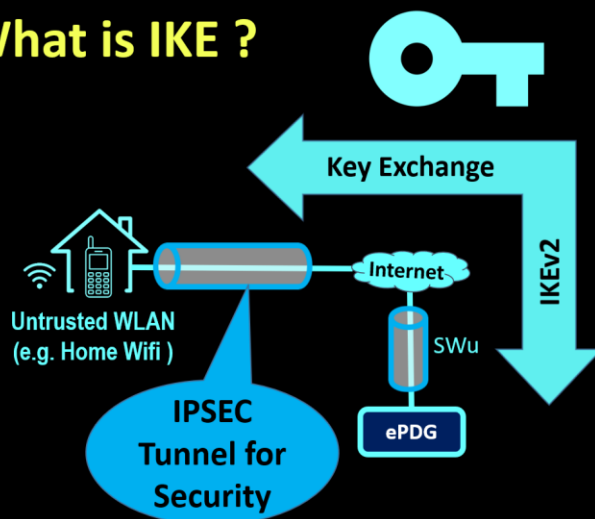
- Encryption only
- Authentication only
- Both Encryption and authentication

ESP in fact provides more advanced Security by offering Both Encryption and authentication

What is IKE?

8

What is IKE ?



- Use of **Internet Key Exchange (IKE)** is
 - To generate the same symmetrical key independently for both Party
 - Key is used for encrypts and decrypts packets passing in tunnels
 - A Security Association (SA) is the outcome of an IKE negotiation
- IKE establish SA (security association) for either ESP or AH (IPSec)

www.TelecomTutorial.info

What is IKE?

First thing First , Why do we need IKE ? The aim of the Internet Key Exchange (IKE) is to generate the same symmetrical key independently for both parties. This key then encrypts and decrypts the standard IP packets passing thru tunnels . A Security Association (SA) is the outcome of an IKE negotiation.

Well , IKE and IPSEC work in conjunction with each other. IKE helps in establishing SA (security association) for either ESP (Encapsulated security protocol) or AH (Authentication header) which are part of IPSec protocols . IKE is a network security protocol designed to dynamically exchange encryption keys and create Security Association (SA) between UE & ePDG . These Security Associations or SAs can be established dynamically and removed at a negotiated time period



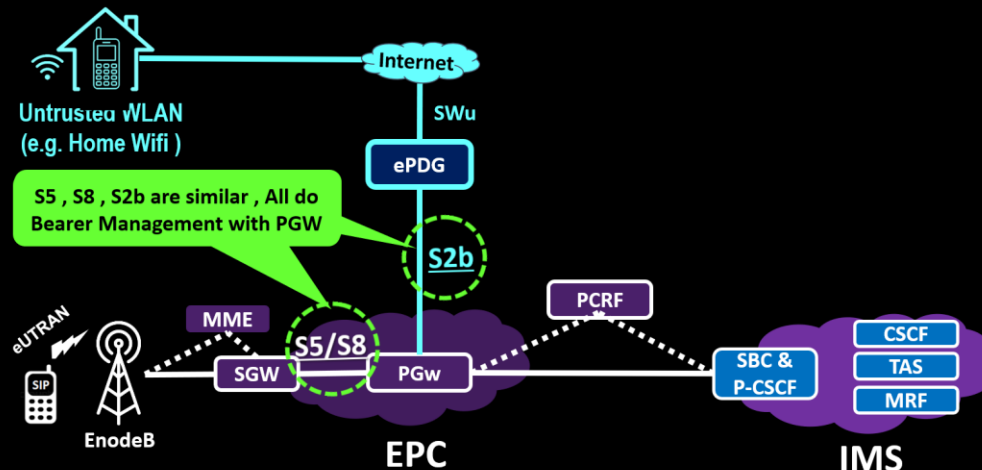
S2b Interface



S2b Interface

GTP PMIP

3GPP TS 29.274



www.TelecomTutorial.info

S2b Interface

Now, We are going to discuss very interesting concept of Bearer management . Here we will see similarity between s5/s8 & s2b

What is s5/s8 interface

- Basically , s5/s8 is Interface between the S-GW and P-GW (i.e. used in EPC LTE Network – 4G Network)
- The both are technically same , we call it s5 if it's local & we call it s8 if its used for roaming scenario

What is s2b interface

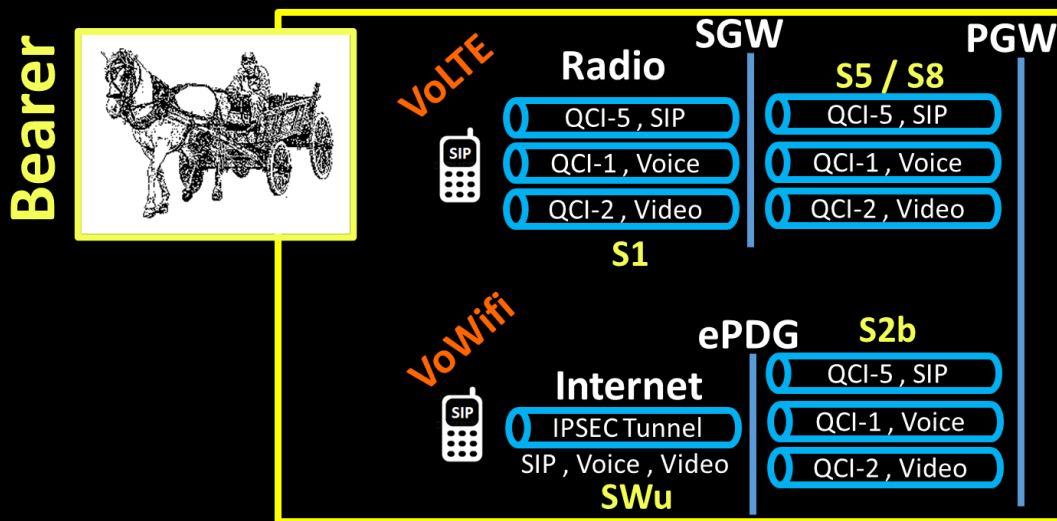
- S2b Connect ePDG to the P-GW & it's used for VoWifi Access

Now , Let's see similarities between these s5/s8 & s2b

- Both are used to Provide connectivity to PGW for Session Creation
- Both works on similar Protocol and uses same messages for Bearer creation & Deletion



Bearer Formation for VoWifi



Now , Let's understand the Bearer formation for VoWifi . 'Bearer' in the dictionary means "Carrier" or "Porter" which carries something from a point to another point. Under the context of communication technology, I would define the 'Bearer' as a 'pipe line' connecting two or more points in the communication system in which data traffic follow through.

QCIs are correlated with bearer in EPC network. There is separate bearer and QCI for all type of traffic such as IMS SIP Signaling , IMS Voice Call & IMS Video Call . There are 2 types of bearers – Default & Dedicated . Refer to this diagram where we are going to discuss very interesting concept of Wifi Calling . While VoLTE have End to End Bearers for SIP , Voice & Video Call , i.e. These separate 3 bearers exists between UE to Radio , Radio to SGW , SGW to PGW . The same thing doesn't happen with VoWifi . In VoWifi , These bearers are created between ePDG to PGW only . All type of traffic viz , SIP Signaling , Voice & Video comes via IPSEC tunnel and terminated on ePDG . Further ePDG map this traffic to various bearers created with PGW . In other words , There are no bearers between ePDG & UE in VoWifi , These separate bearers exists between ePDG & PGW only

Let's see what is role of these Bearers

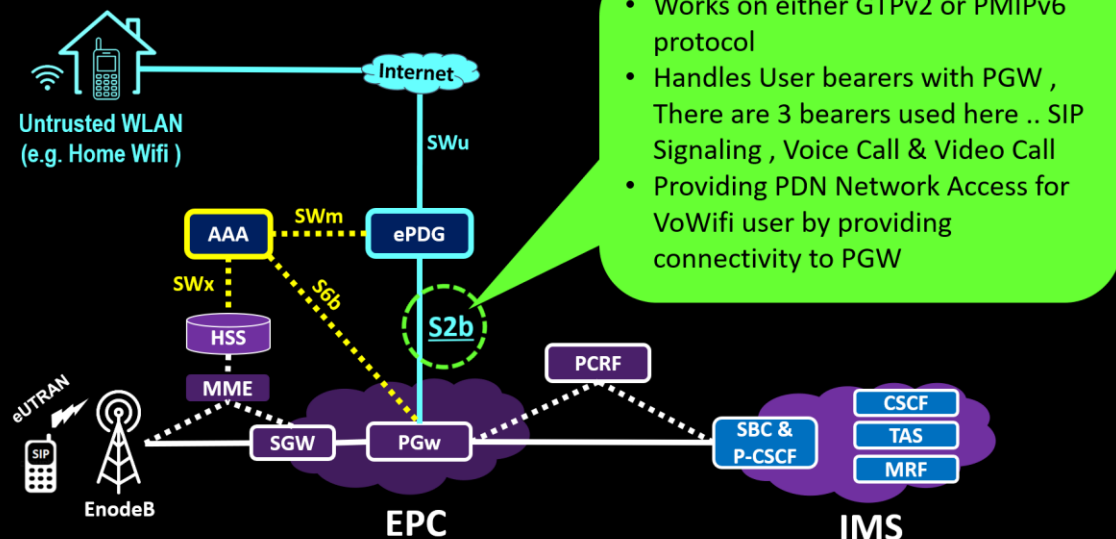
- QCI=5 is used for VoLTE IMS Signaling , This is Default EPS Bearer which is established during VoWifi Attach & Registration . This is used for Allocating IP address to UE . This is always connected type bearer
- QCI=1 is used for VoWifi IMS Voice Call , While QCI=2 is used for VoWifi IMS Video Call . These are Dedicated bearers which are created during call & is released once call is over . These offer specific QoS which is guaranteed



S2b Interface

S2b Interface

GTP , 3GPP TS 29.274 



www.TelecomTutor.info

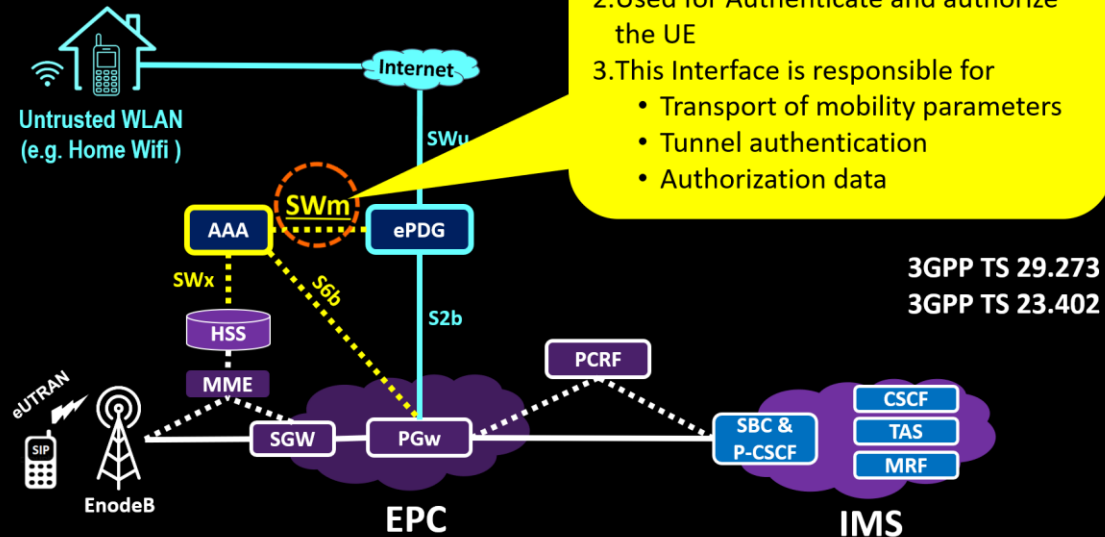
Other details about S2b Interface

1. S2b connects ePDG to P-GW, Its derived from 3GPP TS 29.274 Specs
2. It Works on either GTPv2 or PMIPv6 protocol
3. The role of S2b is to maintain User bearers with PGW, There are 3 bearers used here .. SIP Signaling, Voice Call & Video Call
4. Just like VoLTE, The bearer creation/deletion/modification happens between ePDG and PGW. The Bearer in VoWifi are not End to End, They exist only in core network between ePDG to PGW
5. QCI-5 based SIP Signaling Bearers is created during VoWifi Attach / Registration, It is released during Detach or Disconnection
6. Similarly, The Voice or Video Call bearer is created only during call. It's terminated after call release
7. S2b is critical link which is used for providing PDN Network Access for VoWifi user by providing connectivity to PGW



SWm Interface

SWm Interface Diameter




SWm Interface

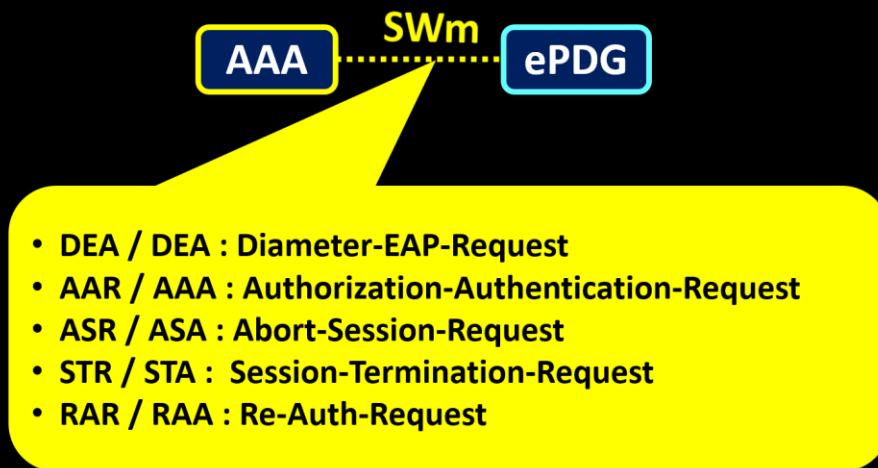
1. It connects ePDG to AAA (Full form of AAA is Authentication, Authorization and Accounting server)
2. It is used for Authenticate and authorize the UE . It uses EAP-AKA method
3. This Interface is responsible for Transport of mobility parameters between ePDG to AAA , Carrying Tunnel authentication Data & Authorization Users
4. It is used for Passing Information from HSS to ePDG , For Ex :- HSS may pass static IP Address to user which is passed from HSS to AAA & further AAA to ePDG for Action
5. You should refer to 3GPP Specs 29.273 & 23.402 for further studies and details on this Interface



SWm Interface - Messages

SWm Interface Diameter

3GPP TS 29.273 
3GPP TS 23.402



www.TelecomTutorial.info

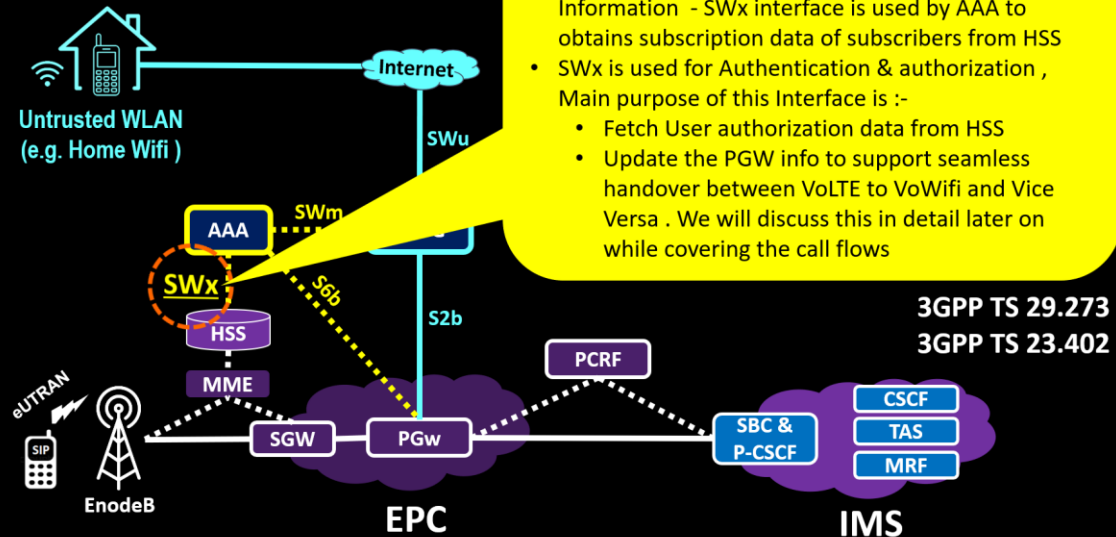
Let's understand few messages which are exchanged to make it bit more clear :-

- **Diameter-EAP-Request (DER) / Diameter-EAP-Answer (DEA)** :- ePDG Send DER with user details , AAA Authenticates & reverts back with User details such as APN Details , QOS , PGW , AMBR & EAP-Payload details
- **Authorization-Authentication-Request (AAR) / Authorization-Authentication-Answer (AAA)** : ePDG trigger this to AAA for getting most recent service authorization information
- **Abort-Session-Request (ASR) / Abort-Session-Answer (ASA)** : Used during Detach of User to Abort the session
- **Session-Termination-Request (STR) / Session-Termination-Answer (STA)** : ePDG Inform AAA that resources are released and user session is terminated
- **Re-Auth-Request (RAR) / Re-Auth-Answer (RAA)** : It is triggered by HSS whenever subscription data is changed or updated for connected user



SWx Interface

SWx Interface Diameter



SWx Interface

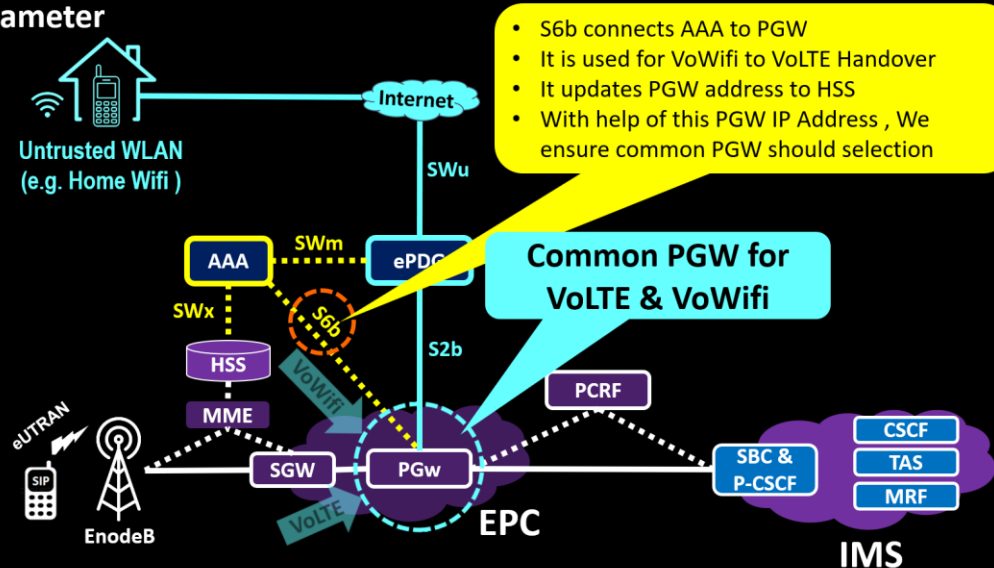
1. SWx interface is used to connect AAA to HSS
2. HSS stands for Home Subscriber Server
3. HSS is repository and Database for all user Information , It includes Authentication & Subscription information for user
4. In easy words , All Services are defined in HSS , In case customer is not allowed for VoWIFI Service in HSS Profile , The user will not be allowed to use VoWifi service
5. SWx interface is used by AAA to obtains subscription data of subscribers from HSS
6. Just like SWm , The SWx is used for Authentication & authorization , Main purpose of this Interface is :-
 - Registration & De-Registration of User in Network & corresponding update on AAA & HSS
 - Transport UEs mobility parameters
 - Fetch User authorization data from HSS
 - Update the PGW info to support seamless handover between VoLTE to VoWifi and Vice Versa . We will discuss this in detail later on while covering the call flows



S6b Interface

S6b Interface Diameter

3GPP TS 29.273
3GPP TS 23.402



www.TelecomTutorial.info

S6b Interface

- It Connects AAA & PGW
- In Operator Network , There are multiple PGWs who serve users

Common PGW

- In case VoWifi PDN is established on One PGW & VoLTE PDN is established on another PGW , Handover will not happen between VoWifi to VoLTE
- Here s6b solves real problem .. When ever UE is attached on non-3GPP access , This interface is used to update PGW address to HSS
- With help of this PGW IP Address , We ensure common PGW should selected to serve both VoLTE & VoWifi Service



Future Reading & References

Future Reading & References



- **RFC 7296**
 - Internet Key Exchange Protocol Version 2 (IKEv2)
 - Basics of SWu Interface
- **3GPP TS 29.274**
 - S2b interface by the ePDG to the PGW
- **3GPP TS 29.273**
 - 3GPP EPS AAA interfaces
 - AAA Links , Descriptions , Format & Usage

www.TelecomTutorial.info

Well now we are at the end of this Module , You can refer to these documents for Future Reading & References

You need to simply type them in google & download PDF copy

- **RFC 7296**
 - Internet Key Exchange Protocol Version 2 (IKEv2)
 - Basics of SWu Interface
- **3GPP TS 29.274**
 - S2b interface by the ePDG to the PGW
- **3GPP TS 29.273**
 - 3GPP EPS AAA interfaces
 - AAA Links , Descriptions , Format & Usage