UMTS CORE NETWORK ARCHITECTURE

The UMTS network architecture can be divided into three main elements:

1. **User Equipment (UE):** The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. The new name was chosen because the considerably greater functionality that the UE could have. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.
2. **Radio Network Subsystem (RNS):** The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface for the overall network.
3. **Core Network:** The core network provides all the central processing and management for the system. It is the equivalent of the GSM Network Switching Subsystem or NSS.

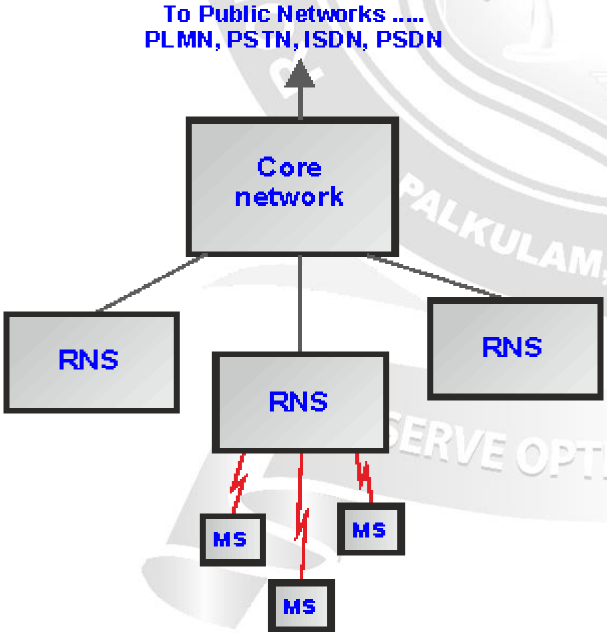


Fig.3.5 UMTS Network Architecture Overview

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

User Equipment, UE

The USER Equipment or UE is a major element of the overall 3G UMTS network architecture. It forms the final interface with the user. In view of the far greater number of applications and facilities that it can perform, the decision was made to call it user equipment rather than a mobile. However it is essentially the handset (inthe broadest terminology), although having access to much higher speed data communications, it can be much more versatile, containing many more applications. It consists of a variety of different elements including RF circuitry, processing, antenna, battery, etc.

There are a number of elements within the UE that can be described separately:

- UE RF circuitry: The RF areas handle all elements of the signal, both forthe receiver and for the transmitter. One of the major challenges for the RF power amplifier was to reduce the power consumption. The form of modulation used for W-CDMA requires the use of a linear amplifier. These inherently take more current than nonlinear amplifiers which can be used for the form of modulation used on GSM. Accordingly to maintain battery life, measures were introduced into many of the designs to ensure the optimum efficiency.
- Baseband processing: The base-band signal processing consists mainly of digital circuitry. This is considerably more complicated than that used in phones for previous generations. Again this has been optimized to reduce the current consumption as far as possible.
- Battery: While current consumption has been minimized as far as possible within the circuitry of the phone, there has been an increase in current drain on the battery. With users expecting the same lifetime between charging batteries as experienced on the previous generation phones, this has necessitated the use of new and improved battery technology. Now Lithium Ion (Li-ion) batteries are used. These phones to remain small and relatively light while still retaining or even improving the overall life between charges.

- Universal Subscriber Identity Module, USIM: The UE also contains a SIM card, although in the case of UMTS it is termed a USIM (Universal Subscriber Identity Module). This is a more advanced version of the SIM card used in GSM and other systems, but embodies the same types of information. It contains the International Mobile Subscriber Identity number (IMSI) as well as the Mobile Station International ISDN Number (MSISDN). Other information that the USIM holds includes the preferred language to enable the correct language information tobe displayed, especially when roaming, and a list of preferred and prohibited Public Land Mobile Networks (PLMN).

3G UMTS Radio Network Subsystem

This is the section of the 3G UMTS / WCDMA network that interfaces to both the UE and the core network. The overall radio access network, i.e. collectively all the Radio Network Subsystem is known as the UTRAN UMTS Radio Access Network.

The radio network subsystem is also known as the UMTS Radio Access Network or UTRAN.

3G UMTS Core Network

The 3G UMTS core network architecture is a migration of that used for GSM with further elements overlaid to enable the additional functionality demanded by UMTS.

In view of the different ways in which data may be carried, the UMTS core network may be split into two different areas:

- **Circuit switched elements:** These elements are primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.
  - It is used to provide voice and CS data services.
  - It contains Mobile Switching Center (MSC) and Gateway MSC(GMSC) as functional entities.
- **Packet switched elements:** These network entities are designed to carry packet

data. This enables much higher network usage as the capacity can be shared and data is carried as packets which are routed according to their destination.

- It is used to provide packet based services.

It contains Serving GPRS support node (SGSN),
Gateway GPRS support node (GGSN),
Domain Name Server (DNS),
Dynamic Host Configuration Protocol (DHCP) server,
packet charging gateway,
and firewalls.

The core network can be split into the following different functional areas:

Functional entities needed to support PS services (e.g.3G-SGSN, 3G- GGSN)

Functional entities needed to support CS services (e.g. 3G-MSC/VLR)

Functional entities common to both types of services (e.g. 3G-HLR)

Other areas that can be considered part of the core network include:

Network management systems (billing and provisioning, service management, element management, etc.)

IN system (service control point (SCP), service signaling point (SSP), etc.)

ATM/SDH/IP switch/transport infrastructure.

Some network elements, particularly those that are associated withregistration are shared by both domains and operate in the same way that they did with GSM.

The below figure shows all the entities that connect to the core network — UTRAN, PSTN, the Internet and the logical connections between terminal equipment (MS,UE), and the PSTN/Internet.

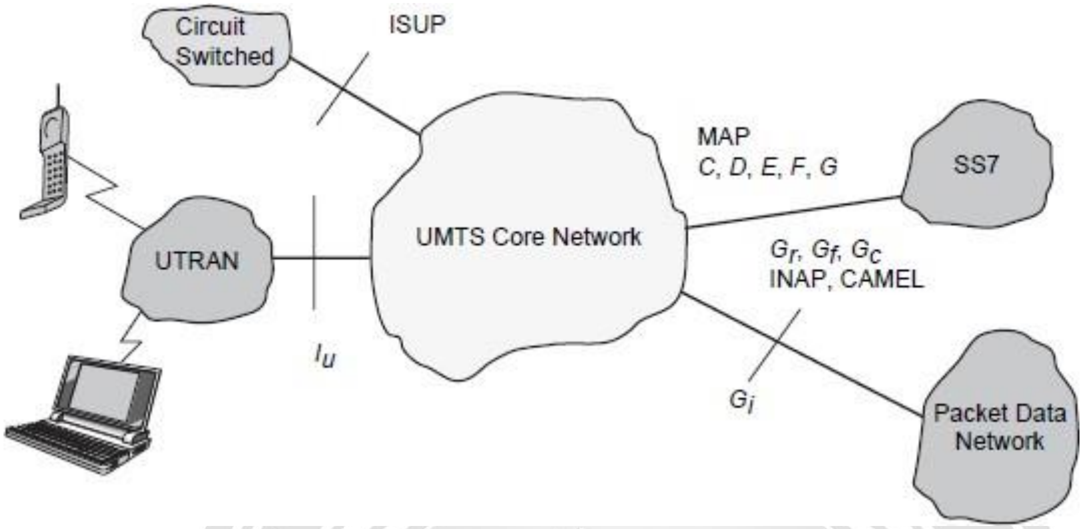


Fig.3.6 UMTS Core network architecture

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Circuit switched elements

The circuit switched elements of the UMTS core network architecture includethe following network entities:

Mobile switching Centre (MSC): This is essentially the same as that within GSM, and it manages the circuit switched calls under way.

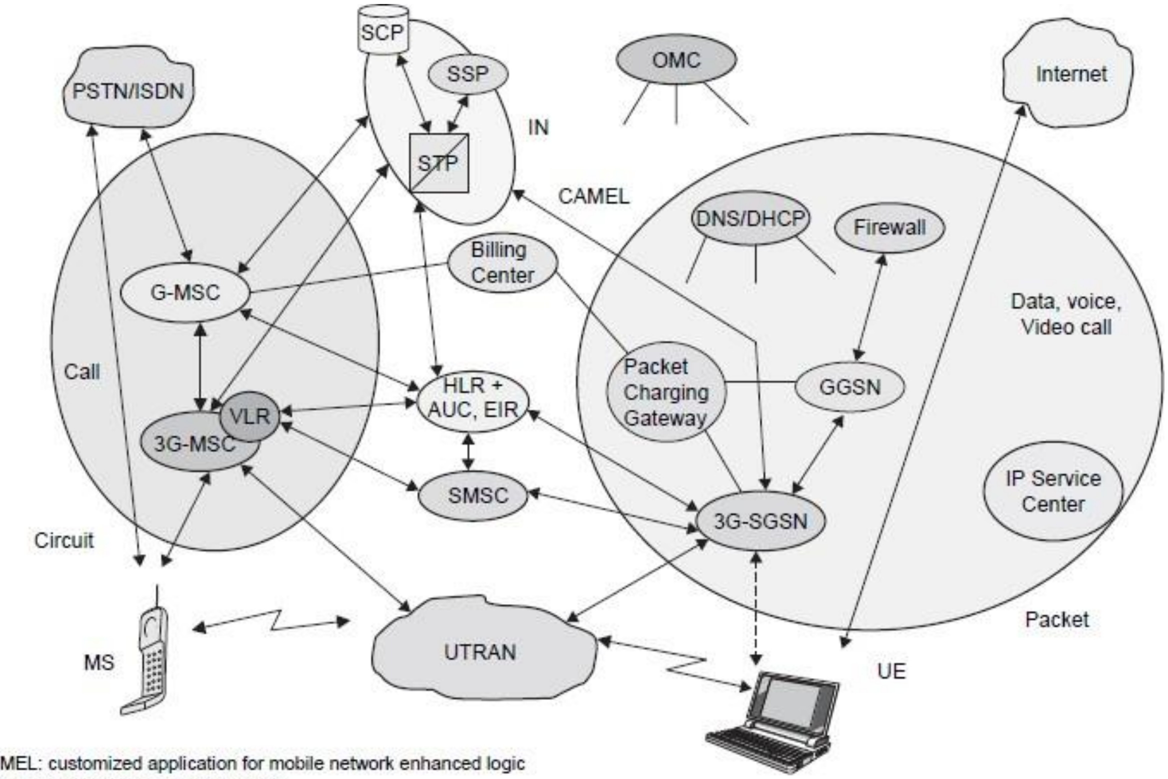
Gateway MSC (GMSC): This is effectively the interface to the external networks.

Packet switched elements

The packet switched elements of the 3G UMTS core network architecture include the following network entities:

Serving GPRS Support Node (SGSN):

Gateway GPRS Support Node (GGSN):



CAMEL: customized application for mobile network enhanced logic
SMSC: short message service center
DNS: domain name server
DHCP: dynamic host configuration protocol

Fig.3.7 Logical architecture of the UMTS core network.

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

3G-MSC

The MSC is the control Centre for the cellular system, coordinating the actions of the BSCs, providing overall control, and acting as the switch and connection into the public telephone network. As such it has a variety of communication links into it which will include fiber optic links as well as some microwave links and some copper wire cables. These enable it to communicate with the BSCs, routing calls tothem and controlling them as required. It also contains the Home and Visitor Location Registers, the databases detailing the last known locations of the mobiles.It also contains the facilities for the Authentication Centre, allowing mobiles onto the network. In addition to this it will also contain the facilities to generate the billing information for the individual accounts.

In view of the importance of the MSC, it contains many backup and duplicate circuits to ensure that it does not fail. Obviously backup power systems are an essential element of this to guard against the possibility of a major power failure, because if the MSC became inoperative then the whole network would collapse.

While the cellular network is not seen by the outside world and its operation is a mystery to many, the cellular network is at the very center of the overall cellular system and the success of the whole end to end system is dependent largely on its performance.

This is essentially the same as that within GSM, and it manages the circuit switched calls under way.

It is the main CN element.It provides CS services.

It provides the necessary control and corresponding signaling interfaces includingSS7, MAP, ISUP (ISDN user part), etc.

It is used to provide the interconnection to external networks like PSTN and ISDN.

The following functionality is provided by the 3G-MSC.

Mobility management:

Handles attach, authentication, updates to the HLR,SRNS relocation, andinter systems handover.

Call management:

Handles call set-up messages from/to the UE.

Supplementary services:

Handles call-related supplementary services suchas call waiting, etc.

CS data services:

The IWF provides rate adaptation and message translationfor circuit modedata services, such as fax.

Vocoding

SS7, MAP and RANAP interfaces:

The 3G-MSC is able to complete originating or terminating calls in thenetwork in interaction with other entities of a mobile network, e.g., HLR, AUC (Authentication center). It also controls/communicates with RNC using RANAP which may use the services of SS7.

ATM/AAL2

Connection to UTRAN for transportation of user plane traffic across the Iu interface. Higher rate CS data rates may be supported using a different adaptation layer.

Short message services (SMS):

This functionality allows the user to send and receive SMS data to and from the SMS-GMSC/SMS-IWMSC (Interworking MSC).

VLR functionality:

The VLR is a database that may be located within the3G-MSC and can serveas intermediate storage for subscriber data in order to support subscriber mobility.

IN and CAMEL.

OAM

(operation, administration, and maintenance) agent functionality.

3G-SGSN-Serving GPRS Support Node

The 3G-SGSN is the main CN element for PS services. The 3G-SGSN provides the necessary control functionality both toward the UE and the 3G-GGSN. It also provides the appropriate signaling and data interfaces including connection to an IP-based network toward the 3G-GGSN, SS7 toward the HLR/EIR/AUC and TCP/IP or SS7 toward the UTRAN.

The 3G-SGSN provides the following functions:

Session management:

Handles session set-up messages from/to the UE andthe GGSN and operates Admission Control and QoS mechanisms.

I_u and G_n MAP interface:

The 3G-SGSN is able to complete originating or terminating sessions in the network by interaction with other entities of a mobile network, e.g., GGSN, HLR, AUC. It also controls/communicates with UTRAN using RANAP.

ATM/AAL5

Physical connection to the UTRAN for transportation of user data plane traffic across the I_u interface using GPRS tunneling protocol(GTP).

Connection across the G_n interface toward the GGSN for transportation of user plane traffic using GTP. Note that no physical transport layer is defined for this interface.

SMS:

This functionality allows the user to send and receive SMS data to and from the SMS-GMSC /SMS-IWMSC.

Mobility management:

Handles attach, authentication, updates to the HLR and SRNS relocation, and intersystem handover.

Subscriber database functionality:

This database (similar to the VLR) is located within the 3G-SGSN andserves as intermediate storage for subscriber data to support subscriber mobility.

Charging:

The SGSN collects charging information related to radio network usage bythe user.

3G-GGSN

The GGSN provides interworking with the external PS network. It is connected with SGSN via an IP-based network. The GGSN may optionally support an SS7interface with the HLR to handle mobile terminated packet sessions.

The 3G-GGSN provides the following functions:

It Maintain information locations at SGSN level (macro-mobility) Gateway between UMTS packet network and external data networks(e.g. IP, X.25)

Gateway-specific access methods to intranet (e.g. PPP termination)Initiate mobile terminate Route Mobile Terminated packets User data screening/security can include subscription based, user controlled, or network controlled screening.

User level address allocation: The GGSN may have to allocate (depending on subscription) a dynamic address to the UE upon PDP context activation.

This functionality may be carried out by use of the DHCP function. Charging: The GGSN collects charging information related to external data network usage by the user.

SMS-GMSC/SMS-IWMSC

The overall requirement for these two nodes is to handle the SMS from pointto point. The functionality required can be split into two parts.

The SMS-GMSC is an MSC capable of receiving a terminated short messagefrom a service center, interrogating an HLR for routing information and SMSinformation, and delivering the short message to the SGSN of the recipient UE.

The SMS-GMSC provides the following functions: Reception of short message packet data unit (PDU)Interrogation of HLR for routing information Forwarding of the short message PDU to the MSC or SGSN using the routing information The SMS-IWMSC is an MSC capable of receiving an originatingshort message from within the PLMN and submitting it to the recipient service center.

The SMS-IWMSC provides the following functions:

Reception of the short message PDU from either the 3G-SGSN or3G-MSC

Establishing a link with the addressed service center

Transferring the short message PDU to the service center

Note: The service center is a function that is responsible for relaying, storing, and forwarding a short message. The service center is not part of UCN, although the MSC and the service center may be integrated.

Firewall

A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.
This entity is used to protect the service providers' backbone data networks from attack from external packet data networks. The security of the backbone data network can be ensured by applying packet filtering mechanisms based on access control lists or any other methods deemed suitable.

Introduction

Firewalls are computer security systems that protect your office/home PCsor your network from intruders, hackers & malicious code. Firewalls protect you from offensive software that may come to reside on your systems or from prying hackers. In a day and age when online security concerns are the top priority of the computer users, Firewalls provide you with the necessary safety and protection.

Firewalls are software programs or hardware devices that filter the traffic that flows into you PC or your network through a internet connection. They sift through the data flow & block that which they deem (based on how & for what youhave tuned the firewall) harmful to your network or computer system.

When connected to the internet, even a standalone PC or a network of interconnected computers make easy targets for malicious software & unscrupulous hackers. A firewall can offer the security that makes you less vulnerable and also protect your data from being compromised or your computers being taken hostage.

Firewalls are setup at every connection to the Internet, therefore subjecting all data flow to careful monitoring. Firewalls can also be tuned to follow "rules". These Rules are simply security rules that can be set up by the network administrators to allow traffic to their web servers, FTP servers, Telnet servers, thereby giving the computer owners/administrators immense control over the traffic that flows in & out of their systems or networks.

Rules will decide who can connect to the internet, what kind of connections can be made, which or what kind of files can be transmitted in out. Basically all traffic in & out can be watched and controlled thus giving the firewall installer a high level of security & protection.

Firewall logic

Firewalls use 3 types of filtering mechanisms:

Packet filtering or packet purity

Data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets.

Proxy

Firewall in this case assumes the role of a recipient & in turn sends it to the node that has requested the information & vice versa. **Inspection**

In this case Firewalls instead of sifting through all of the information in the packets, mark key features in all outgoing requests & check for the same matching characteristics in the inflow to decide if it relevant information that is coming through.

Firewall Rules

Firewalls rules can be customized as per our needs, requirements & securitythreat levels.

We can create or disable firewall filter rules based on such conditions as:

IP Addresses

Blocking off a certain IP address or a range of IP addresses, which you think are predatory.

Domain names

Only certain specific domain names are allowed to access our systems/servers or allow access to only some specified types of domain names or domain name extension like .edu or.mil.

Protocols

A firewall can decide which of the systems can allow or have access to common protocols like IP, SMTP, FTP, UDP, ICMP, Telnet or SNMP.

Ports

Blocking or disabling ports of servers that are connected to the internet will help maintain the kind of data flow you want to see it used for & also close down possible entry points for hackers or malignant software.

Keywords

Firewalls also can sift through the data flow for a match of the keywords or phrases to block out offensive or unwanted data from flowing in. **Types of Firewall**

Software firewalls

New generation Operating systems come with built in firewalls or you can buy a firewall software for the computer that accesses the internet or acts as the gateway to your home network.

Hardware firewalls

Hardware firewalls are usually routers with a built in Ethernet card and hub. Your computer or computers on your network connect to this router & access the web.

Packet firewalls

The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port number are checked against the firewall's rule set. Any packets thataren't specifically allowed onto the network are dropped (i.e., not forwarded totheir destination). For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for TCP port number 23.

Packet-filter firewalls work mainly on the first three layers of the OSI reference model (physical, data-link and network), although the transport layer is used to obtain the source and destination port numbers. While generally fast and efficient, they have no ability to tell whether a packet is part of an existing stream of traffic. Because they treat each packet in isolation, this makes them vulnerable to spoofing attacks and also limits their ability to make more complex decisions based on what stage communications between hosts are at.

Stateful firewalls

In order to recognize a packet's connection state, a firewall needs to record all connections passing through it to ensure it has enough information to assess whether a packet is the tart of a new connection, a part of an existing connection,or not part of any connection. This is what's called "stateful packet inspection." Stateful inspection was first introduced in 1994 by Check Point Software in its FireWall-1 software firewall, and by the late 1990s, it was a common firewall product feature.

This additional information can be used to grant or reject access based on the packet's history in the state table, and to speed up packet processing; that way, packets that are part of an existing connection based on the firewall's state table can be allowed through without further analysis. If a packet does not match an existing connection, it's evaluated according to the rule set for new connections.

Application-layer firewalls

As attacks against Web servers became more common, so too did the need for a firewall that could protect servers and the applications running on them, not merelythe network resources behind them. Application-layer firewall technology first emerged in 1999, enabling firewalls to inspect and filter packets on any OSI layer up to the application layer.

The key benefit of application-layer filtering is the ability to block specific content, such as known malware or certain websites, and recognize when certain applications and protocols -- such as HTTP, FTP and DNS -- are being misused.

Firewall technology is now incorporated into a variety of devices; many routers that pass data between networks contain firewall components and most home computer operating systems include software-based firewalls. Many hardware- based firewalls also provide additional functionality like basic routing to the internal network they protect.

Proxy firewalls

Firewall proxy servers also operate at the firewall's application layer, acting as an intermediary for requests from one network to another for a specific network application. A proxy firewall prevents direct connections between either sides of the firewall; both sides are forced to conduct the session through the proxy, which can block or allow traffic based on its rule set.

Firewalls in the perimeter less age

The role of a firewall is to prevent malicious traffic reaching the resources that it is protecting. Some security experts feel this is an outdated approach to keeping information and the resources it resides on safe. Some of the firewall products that you may want to check out are:

McAfee Internet Security

Microsoft Windows Firewall

Norton Personal Firewall

Trend Micro PC-cillin

ZoneAlarm Security