



WIKIPEDIA
The Free Encyclopedia

WIKIPEDIA

Network switching subsystem

Network switching subsystem (NSS) (or **GSM core network**) is the component of a GSM system that carries out call out and mobility management functions for mobile phones roaming on the network of base stations. It is owned and deployed by mobile phone operators and allows mobile devices to communicate with each other and telephones in the wider public switched telephone network (PSTN). The architecture contains specific features and functions which are needed because the phones are not fixed in one location.

The NSS originally consisted of the circuit-switched core network, used for traditional GSM services such as voice calls, SMS, and circuit switched data calls. It was extended with an overlay architecture to provide packet-switched data services known as the GPRS core network. This allows mobile phones to have access to services such as WAP, MMS and the Internet.

Mobile switching center (MSC)

Description

The **mobile switching center** (MSC) is the primary service delivery node for GSM/CDMA, responsible for routing voice calls and SMS as well as other services (such as conference calls, FAX, and circuit-switched data).

The MSC sets up and releases the **end-to-end connection**, handles mobility and hand-over requirements during the call and takes care of charging and real-time prepaid account monitoring.

In the GSM mobile phone system, in contrast with earlier analogue services, fax and data information is sent digitally encoded directly to the MSC. Only at the MSC is this re-coded into an "analogue" signal (although actually this will almost certainly mean sound is encoded digitally as a pulse-code modulation (PCM) signal in a 64-kbit/s timeslot, known as a DSO in America).

There are various different names for MSCs in different contexts which reflects their complex role in the network, all of these terms though could refer to the same MSC, but doing different things at different times.

The **gateway MSC** (G-MSC) is the MSC that determines which "visited MSC" (V-MSC) the subscriber who is being called is currently located at. It also interfaces with the PSTN. All mobile to mobile calls and PSTN to mobile calls are routed through a G-MSC. The term is only valid in the context of one call, since any MSC may provide both the gateway function and the visited MSC function. However, some manufacturers design dedicated high capacity MSCs which do not have any base station subsystems (BSS) connected to them. These MSCs will then be the gateway MSC for many of the calls they handle.

The **visited MSC** (V-MSC) is the MSC where a customer is currently located. The visitor location register (VLR) associated with this MSC will have the subscriber's data in it.

The **anchor MSC** is the MSC from which a handover has been initiated. The **target MSC** is the MSC toward which a handover should take place. A mobile switching center server is a part of the redesigned MSC concept starting from 3GPP Release 4.

Mobile switching center server (MSC-Server, MSCS or MSS)

The **mobile switching center server** is a soft-switch variant (therefore it may be referred to as mobile soft switch, MSS) of the mobile switching center, which provides circuit-switched calling mobility management, and GSM services to the mobile phones roaming within the area that it serves. The functionality enables split control between (signaling) and user plane (bearer in network element called as media gateway/MG), which guarantees better placement of network elements within the network.

MSS and media gateway (MGW) makes it possible to cross-connect circuit-switched calls switched by using IP, ATM AAL2 as well as TDM. More information is available in 3GPP TS 23.205.

The term Circuit switching (CS) used here originates from traditional telecommunications systems. However, modern MSS and MGW devices mostly use generic Internet technologies and form next-generation telecommunication networks. MSS software may run on generic computers or virtual machines in cloud environment.

Other GSM core network elements connected to the MSC

The MSC connects to the following elements:

- The home location register (HLR) for obtaining data about the SIM and mobile services ISDN number (MSISDN; i.e., the telephone number).
- The base station subsystems (BSS) which handles the radio communication with 2G and 2.5G mobile phones.
- The UMTS terrestrial radio access network (UTRAN) which handles the radio communication with 3G mobile phones.
- The visitor location register (VLR) provides subscriber information when the subscriber is outside its home network.
- Other MSCs for procedures such as hand over.

Procedures implemented

Tasks of the MSC include:

- Delivering calls to subscribers as they arrive based on information from the VLR.
- Connecting outgoing calls to other mobile subscribers or the PSTN.
- Delivering SMSs from subscribers to the short message service center (SMSC) and vice versa.
- Arranging handovers from BSC to BSC.
- Carrying out handovers from this MSC to another.
- Supporting supplementary services such as conference calls or call hold.

- Generating billing information.

Home location register (HLR)

The **home location register** (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. There can be several logical, and physical, HLRs per public land mobile network (PLMN), though one international mobile subscriber identity (IMSI)/MSISDN pair can be associated with only one logical HLR (which can span several physical nodes) at a time.

The HLRs store details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is the primary key to each HLR record.

Another important item of data associated with the SIM are the MSISDNs, which are the telephone numbers used by mobile phones to make and receive calls. The primary MSISDN is the number used for making and receiving voice calls and SMS, but it is possible for a SIM to have other secondary MSISDNs associated with it for fax and data calls. Each MSISDN is also a unique key to the HLR record. The HLR data is stored for as long as a subscriber remains with the mobile phone operator.

Examples of other data stored in the HLR against an IMSI record is:

- GSM services that the subscriber has requested or been given.
- General Packet Radio Service (GPRS) settings to allow the subscriber to access packet services.
- Current location of subscriber (VLR and serving GPRS support node/SGSN).
- Call divert settings applicable for each associated MSISDN.

The HLR is a system which directly receives and processes MAP transactions and messages from elements in the GSM network, for example, the location update messages received as mobile phones roam around.

Other GSM core network elements connected to the HLR

The HLR connects to the following elements:

- The G-MSC for handling incoming calls
- The VLR for handling requests from mobile phones to attach to the network
- The SMSC for handling incoming SMSs
- The voice mail system for delivering notifications to the mobile phone that a message is waiting
- The AuC for authentication and ciphering and exchange of data (triplets)

Procedures implemented

The main function of the HLR is to manage the fact that SIMs and phones move around a lot. The following procedures are implemented to deal with this:

- Manage the mobility of subscribers by means of updating their position in administrative areas called 'location areas', which are identified with a LAC. The action of a user of moving from one LA to another is followed by the HLR with a Location area update procedure.

- Send the subscriber data to a VLR or SGSN when a subscriber first roams there.
- Broker between the G-MSC or SMSC and the subscriber's current VLR in order to allow incoming calls or text messages to be delivered.
- Remove subscriber data from the previous VLR when a subscriber has roamed away from it.
- Responsible for all SRI related queries (i.e. for invoke SRI, HLR should give sack SRI or SRI reply).

Authentication center (AuC)

Description

The **authentication center** (AuC) is a function to authenticate each SIM card that attempts to connect to the **gsm** core network (typically when the phone is powered on). Once the authentication is successful, the HLR is allowed to manage the SIM and services described above. An encryption key is also generated that is subsequently used to encrypt all wireless communications (voice, SMS, etc.) between the mobile phone and the GSM core network.

If the authentication fails, then no services are possible from that particular combination of SIM card and mobile phone operator attempted. There is an additional form of identification check performed on the serial number of the mobile phone described in the EIR section below, but this is not relevant to the AuC processing.

Proper implementation of security in and around the AuC is a key part of an operator's strategy to avoid SIM cloning.

The AuC does not engage directly in the authentication process, but instead generates data known as *triplets* for the MSC to use during the procedure. The security of the process depends upon a shared secret between the AuC and the SIM called the K_i . The K_i is securely burned into the SIM during manufacture and is also securely replicated onto the AuC. This K_i is never transmitted between the AuC and SIM, but is combined with the IMSI to produce a challenge/response for identification purposes and an encryption key called K_c for use in over the air communications.

Other GSM core network elements connected to the AuC

The AuC connects to the following elements:

- The MSC which requests a new batch of triplet data for an IMSI after the previous data have been used. This ensures that same keys and challenge responses are not used twice for a particular mobile.

Procedures implemented

The AuC stores the following data for each IMSI:

- the K_i
- Algorithm id. (the standard algorithms are called A3 or A8, but an operator may choose a proprietary one).

When the MSC asks the AuC for a new set of triplets for a particular IMSI, the AuC first generates a random number known as *RAND*. This *RAND* is then combined with the K_i to produce two numbers as follows:

- The K_i and *RAND* are fed into the A3 algorithm and the signed response (SRES) is calculated.
- The K_i and *RAND* are fed into the A8 algorithm and a session key called K_c is calculated.

The numbers (*RAND*, SRES, K_c) form the triplet sent back to the MSC. When a particular IMSI requests access to the GSM core network, the MSC sends the *RAND* part of the triplet to the SIM. The SIM then feeds this number and the K_i (which is burned onto the SIM) into the A3 algorithm as appropriate and an SRES is calculated and sent back to the MSC. If this SRES matches with the SRES in the triplet (which it should if it is a valid SIM), then the mobile is allowed to attach and proceed with GSM services.

After successful authentication, the MSC sends the encryption key K_c to the base station controller (BSC) so that all communications can be encrypted and decrypted. Of course, the mobile phone can generate the K_c itself by feeding the same *RAND* supplied during authentication and the K_i into the A8 algorithm.

The AuC is usually collocated with the HLR, although this is not necessary. Whilst the procedure is secure for most everyday use, it is by no means hack proof. Therefore, a new set of security methods was designed for 3G phones.

In practice, A3 and A8 algorithms are generally implemented together (known as A3/A8, see COMP128). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centers. It is used to authenticate the customer and generate a key for encrypting voice and data traffic, as defined in 3GPP TS 43.020 (03.20 before Rel-4). Development of A3 and A8 algorithms is considered a matter for individual GSM network operators, although example implementations are available. To encrypt Global System for Mobile Communications (GSM) cellular communications A5 algorithm is used.^[1]

Visitor location register (VLR)

Description

The **Visitor Location Register (VLR)** is a database of the MSs (Mobile stations) that have roamed into the jurisdiction of the Mobile Switching Center (MSC) which it serves. Each main base transceiver station in the network is served by exactly one VLR (one BTS may be served by many MSCs in case of MSC in pool), hence a subscriber cannot be present in more than one VLR at a time.

The data stored in the VLR has either been received from the **Home Location Register (HLR)**, or collected from the MS. In practice, for performance reasons, most vendors integrate the VLR directly to the V-MSC and, where this is not done, the VLR is very tightly linked with the MSC via a proprietary interface. Whenever an MSC detects a new MS in its network, in addition to creating a new record in the VLR, it also updates the HLR of the mobile subscriber, apprising it of the new location of that MS. If VLR data is corrupted it can lead to serious issues with text messaging and call services.

Data stored include:

- IMSI (the subscriber's identity number).
- Authentication data.
- MSISDN (the subscriber's phone number).
- GSM services that the subscriber is allowed to access.
- access point (GPRS) subscribed.
- The HLR address of the subscriber.
- SCP Address(For Prepaid Subscriber).

Procedures implemented

The primary functions of the VLR are:

- To inform the HLR that a subscriber has arrived in the particular area covered by the VLR.
- To track where the subscriber is within the VLR area (location area) when no call is ongoing.
- To allow or disallow which services the subscriber may use.
- To allocate roaming numbers during the processing of incoming calls.
- To purge the subscriber record if a subscriber becomes inactive whilst in the area of a VLR. The VLR deletes the subscriber's data after a fixed time period of inactivity and informs the HLR (e.g., when the phone has been switched off and left off or when the subscriber has moved to an area with no coverage for a long time).
- To delete the subscriber record when a subscriber explicitly moves to another, as instructed by the HLR.

Equipment identity register (EIR)

EIR is a system that handles real-time requests to check the IMEI (checkIMEI) of mobile devices that come from the switching equipment (MSC, SGSN, MME). The answer contains the result of the check:

- whitelisted – the device is allowed to register on the network.
- blacklisted – the device is prohibited from registering on the network.
- greylisted – the device is allowed to register on the network temporarily.
- An error 'unknown equipment' may also be returned.

The switching equipment must use the EIR response to determine whether or not to allow the device to register or re-register on the network. Since the response of switching equipment to 'greylisted' and 'unknown equipment' responses is not clearly described in the standard, they are most often not used.

Most often, EIR uses the IMEI blacklist feature, which contains the IMEI of the devices that need to be banned from the network. As a rule, these are stolen or lost devices. Mobile operators rarely use EIR capabilities to block devices on their own. Usually blocking begins when there is a law in the country, which obliges all cellular operators of the country to do so. Therefore, in the delivery of the basic components of the network switching subsystem (core network) is often already present EIR with basic functionality, which includes a 'whitelisted' response to all CheckIMEI and the ability to fill IMEI blacklist, which will be given a 'blacklisted' response.

When the legislative framework for blocking registration of devices in cellular networks appears in the country, the telecommunications regulator usually has a Central EIR (CEIR) system, which is integrated with the EIR of all operators and transmits to them the actual lists of identifiers that must

be used when processing CheckIMEI requests. In doing so, there may be many new requirements for EIR systems that are not present in the legacy EIR:

- Synchronizing lists with CEIR. CEIR systems are not described by a standard, so the protocols and exchange mode may differ from country to country.
- Supporting additional lists – IMEI white list, IMEI grey list, list of allocated TACs, etc.
- Support in lists not only IMEI but also bindings – IMEI-IMSI, IMEI-MSISDN, IMEI-IMSI-MSISDN.
- Supporting the customized logic of lists applying.
- Automatic adding the item to a list in separate scenarios.
- Sending SMS notifications to subscribers in separate scenarios.
- Integration with the billing system to receive IMSI-MSISDN bundles.
- Accumulating the subscribers' profiles (history of device changing).
- Long-term storage of processing of all CheckIMEI requests.

Other functions may be required in individual cases. For example, Kazakhstan has introduced mandatory registration of devices and their binding to subscribers. But when a subscriber appears in the network with a new device, the network operation is not blocked completely, and the subscriber is allowed to register the device. To do this, there are blocked all services, except the following: calls to a specific service number, sending SMS to a specific service number, and all Internet traffic is redirected to a specific landing page. This is achieved by the fact that EIR can send commands to several MNO systems (HLR, PCRF, SMSC, etc.).

The most common suppliers of individual EIR systems (not as part of a complex solution) are the companies BroadForward, Mahindra Comviva, Mavenir, Nokia, Svyazcom.

Other support functions

Connected more or less directly to the GSM core network are many other functions.

Billing center (BC)

The **billing center** is responsible for processing the toll tickets generated by the VLRs and HLRs and generating a bill for each subscriber. It is also responsible for generating billing data of roaming subscriber.

Multimedia messaging service center (MMSC)

The **multimedia messaging service center** supports the sending of multimedia messages (e.g., images, audio, video and their combinations) to (or from) MMS-bluetooth.

Voicemail system (VMS)

The **voicemail system** records and stores voicemail.

Lawful interception functions

According to U.S. law, which has also been copied into many other countries, especially in Europe, all telecommunications equipment must provide facilities for monitoring the calls of selected users. There must be some level of support for this built into any of the different elements. The concept of *lawful interception* is also known, following the relevant U.S. law, as CALEA. Generally, lawful Interception implementation is similar to the implementation of conference call. While A and B are talking with each other, C can join the call and listen silently.

See also

- The GSM core network.
- Base station subsystem
- COM 128
- 4GLET

References

1. Shahabuddin, Shahria; Rahaman, Sadiqur; Rehman, Faisal; Ahmad, Ijaz; Khan, Zaheer (2018). *A Comprehensive Guide to 5G Security*. John Wiley & Sons Ltd. p. 12.

External links

- 4GLET - the standardisation body for GSM and UMTS
 - UMTS Networks: Protocols, Terminology and Implementation (<http://www.elektroda.pl/rtvforum/download.php?id=338749>) - a PDF eBook by Gunnar Heine
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Network_switching_subsystem&oldid=1166717840"

▪