3GPP TR 23.851 V6.1.0 (2004-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network sharing; Architecture and Functional Description (Release 6)

Keywords
UMTS, network, architecture

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

In the current mobile telephony marketplace, functionality that enables various forms of network sharing is becoming more and more important. These aspects have not really been addressed in either 2G or 3G systems, although there is functionality that supports a very basic type of network sharing in the current specifications within 3GPP. In [1], 3GPP has studied service requirements and functionality necessary for supporting a standardized network sharing.

The present document discusses issues and describes functionalities required for Network Sharing as outlined in [1]. The intention is to present one (or more) architectural alternatives for achieving the required functionality within a 3GPP network. An important part of the work is to adapt the network functionality so that supporting mobile telephones that do not have any of the possibly new functionality being introduced for network sharing support can be handled in a more efficient way than in pre-Rel-6 networks.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 22.951: “Service Aspects and Requirements for Network Sharing”

[2] 3GPP TS 23.060: “General Packet Radio Service (GPRS); Service description; Stage 2”

[3] 3GPP TS 23.122: “NAS Functions related to Mobile Station (MS) in idle mode”

[4] 3GPP TS 25.331: “RRC Protocol Specification”

[5] 3GPP TR 22.101: “Service Principles”

[6] 3GPP TS 22.115: "Charging and Billing"

[7] 3GPP TS 25.401: " UTRAN overall description ", Release 5

[8] 3GPP TS 23.236: "Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes"

3 Definitions, symbols and abbreviations

3.1 Definitions

3.2 Symbols

For the purposes of the present document, the following symbols apply:

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BCCH	Broadcast Control Channel
BSC	Base Station Controller
CDR	Charging Data Record
CN	Core Network
CS	Circuit Switched
GMM	GPRS Mobility Management
GWCN	Gateway Core Network
HLR	Home Location Register
HPLMN	Home PLMN
IMSI	International Mobile Subscriber Identity
LA	Location Area
LAI	Location Area Identity
MCC	Mobile Country Code
MIB	Master Information Block
MM	Mobility Management
MNC	Mobile Network Code
MOCN	Multi-Operator Core Network
MSC	Mobile Switching Centre
NAS	Non-Access Stratum
NMO	Network Mode of Operation
NRI	Network Resource Identifier
PS	Packet Switched
RAI	Routing Area Identity
SNA	Shared Network Area
PLMN	Public Land Mobile Network
RAN	Radio Access Network
RA	Routing Area
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
SGSN	Serving GPRS Support Node
SIB	System Information Block
SND	Shared Network Domain
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VLR	Visitor Location Register
VPLMN	Visited PLMN

4 General Description

Shared networks is a way for operators to share the heavy deployment costs for mobile networks, especially in the roll-out phase. It also gives operators that do not have licenses of their own the possibility of supplying their subscribers with mobile telephony services. Already R99 contains limited basic functionality, *e.g.* equivalent PLMNs, that makes

the deployment of shared networks at least technically feasible within this release. The support for shared networks are then somewhat enhanced with the introduction of the shared network area (SNA) handover functionality in Rel-5. The different scenarios and requirements described in 3GPP TR 22.951 [1] provide an overview of the service and user requirements that are to be fulfilled for efficient network sharing within 3GPP. In this Section we describe the scenarios in TS 22.951 from an architectural point of view that will aid in the development of a shared network architecture to support the service requirements.

A network sharing architecture should allow the different core network operators to connect to a shared radio access network. The operators do not only share the radio network elements, but may also share the radio resources themselves, *e.g.* the operators' licensed 3G spectra. In addition to this shared radio access network the operators may or may not have additional dedicated radio access networks, like for example, 2G radio access networks. Since operators deploying shared networks using pre-Rel-6 network functionality will also have to share core network nodes (MSCs and SGSNs), such a scenario must be within the scope of the network sharing stage 2 work and be supported by any proposed architectural solution for network sharing. Examples of network sharing scenarios that should (at least) be considered in this technical report are shown in the figures below.

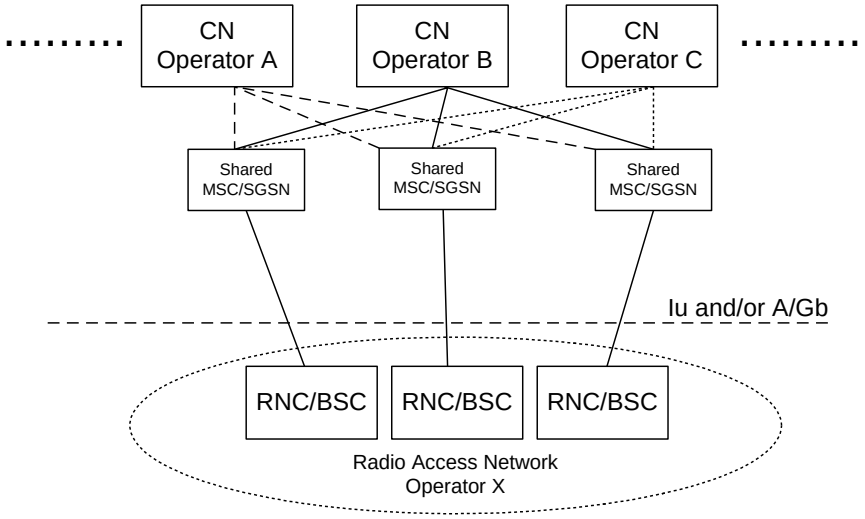


Figure 1: A shared-network architecture constrained by pre-Rel-6 network functionality, which will be referred to as the Gateway Core Network (GWCN), where MSCs and SGSNs are also shared besides the radio access network . It should be possible to use any enhanced Rel-6 network sharing functionality in this architecture since it is important for legacy shared networks. The RAN operator may or may not be one of the CN operators.

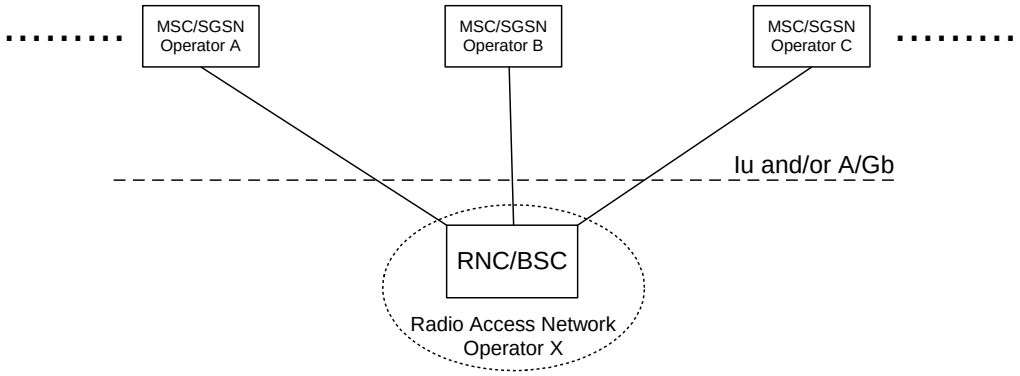


Figure 2: The Multi-Operator Core Network (MOCN) in which multiple CN nodes are connected to the same RNC and the CN nodes are operated by different operators. The RAN operator may or may not be one of the CN operators.

The scenario in Figure 1, the GWCN, is important for legacy shared networks, since this is how they need to be deployed with pre-Rel-6 network functionality. Figure 2 depicts a shared network, the MOCN, that is more cleanly divided in relation to the core network and the radio access network and may be preferrable from a technical and operational point of view. Since it is expected that standardized support for shared networks will introduce functionality that greatly enhances and simplifies the operation of shared networks, both of the scenarios in Figure 1 and Figure 2 (and combinations thereof) need to be taken into account and supported so that the use of these new functionalities are not just associated with the deployment of shared networks according to Figure 2. The introduction of the MOCN connections to RANs enables a few different use cases. For the geographical sharing scenario (described Scenario 2 in [1]) the MOCN solution could be an alternative to national roaming. The sharing partners could connect their core networks directly to the other operators RAN and they would not hence need to roam into the networks of the other operators.

4.1 CN operator and Network Selection

4.1.1 Core network operator identity

Network sharing is an agreement between operators and should be transparent to the user. This implies that a UE and/or user needs to be able to discriminate between core network operators available in a shared radio access network and that these operators can be handled in the same way as operators in non-shared networks.

A core network operator should be identified by a PLMN-id (MCC+MNC). This has the least impact on already stable procedures and functionalities in networks and UEs relating to network selection and handling of network identities.

4.1.2 System broadcast information for network sharing

The following system broadcast information is the same in all cells of a Location Area (LA) belonging to a shared RAN:

- Available CN operators,
- NMO, of each CN, if different,
- T3212 timeout value and Attach/detach, which are common for all the available CN operators.

It is noted that each CN might configure different NMOs for non-supporting UEs and for supporting UEs. It is FFS whether the value of T3212 may be transmitted to UEs by way of mobility management signalling on a per-UE basis. This would allow CN operators to use different values of T3212 without affecting the broadcast system information.

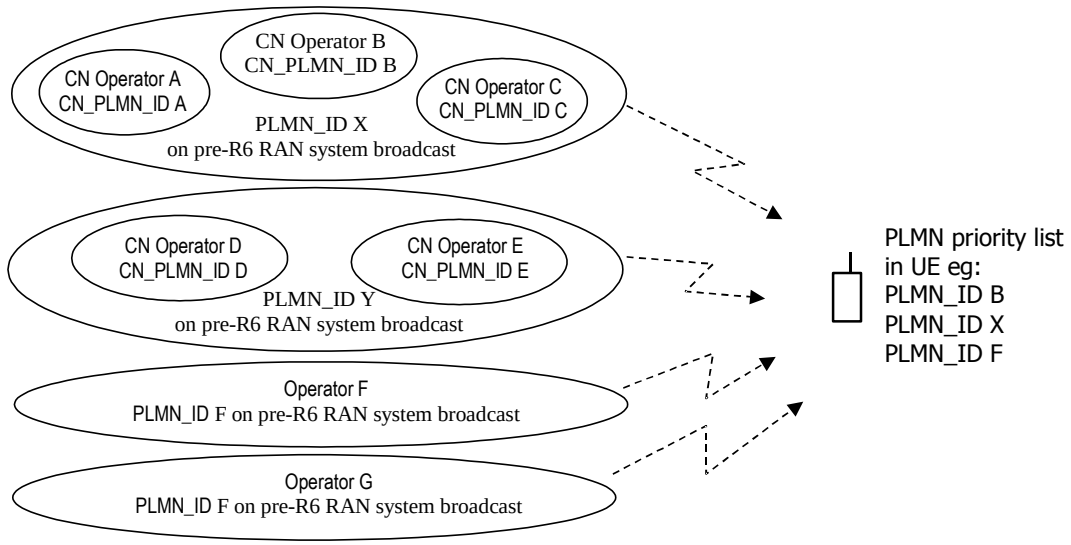
When UE detects that the LA has changed, it should check the identities of available CN operators and their associated network configuration information from the network before any potential re-registration to another network as specified in following chapters.

4.1.3 Network selection solution alternatives

Three different solutions that extend the network selection procedures as defined in TS 23.122 for the selection of a CN operator in Rel-6 shared networks have been identified:

- UE Based solution
- Broadcast channel based solution
- Connected mode based solution

The figure below describes an example case where a RAN with RAN PLMN ID X on pre-Rel-6 system broadcast offers services to three core networks from operators with CN PLMN IDs A, B and C. The RAN with RAN PLMN ID Y on pre-Rel-6 system broadcast offers services to core networks from operators with CN PLMN IDs D and E. Two conventional networks indicate their PLMN IDs F and G on legacy pre-Rel-6 system broadcast.



TS 23.122 in R5, Ref [3], clause 4.4.3.1 defines the PLMN priority order when the mobile is switched on as follows:

1. Registered PLMN
2. Home PLMN
3. PLMN selector lists (user controlled and operator controlled) in the USIM.

According to TR22.951, Ref [1], the UE shall enable the user to register with a core network operator that the user either has a subscription with, or with which the user's home operator has a roaming agreement. The network selection can either be done manually by the UE user or performed automatically by the UE. In the manual selection mode the UE should display all PLMNs it can receive, arranged according to the priority list. In the automatic selection mode the UE should select the PLMN according to the priority lists.

This chapter outlines the different solution alternatives how to indicate the available core network operators and other parameters to the UE user and how to select a core network operator in Rel-6 shared networks.

4.1.3.1 UE based solution

In the UE based solution, the operator configures the operator identities for all LAs of all the roaming partners in the USIM. When UE camps on a particular PLMN, it decodes the LAI from the BCCH and retrieves the list of operator identities associated with the PLMN identity and this particular LA from the USIM. Subsequently it registers to the network and indicates the selected operator.

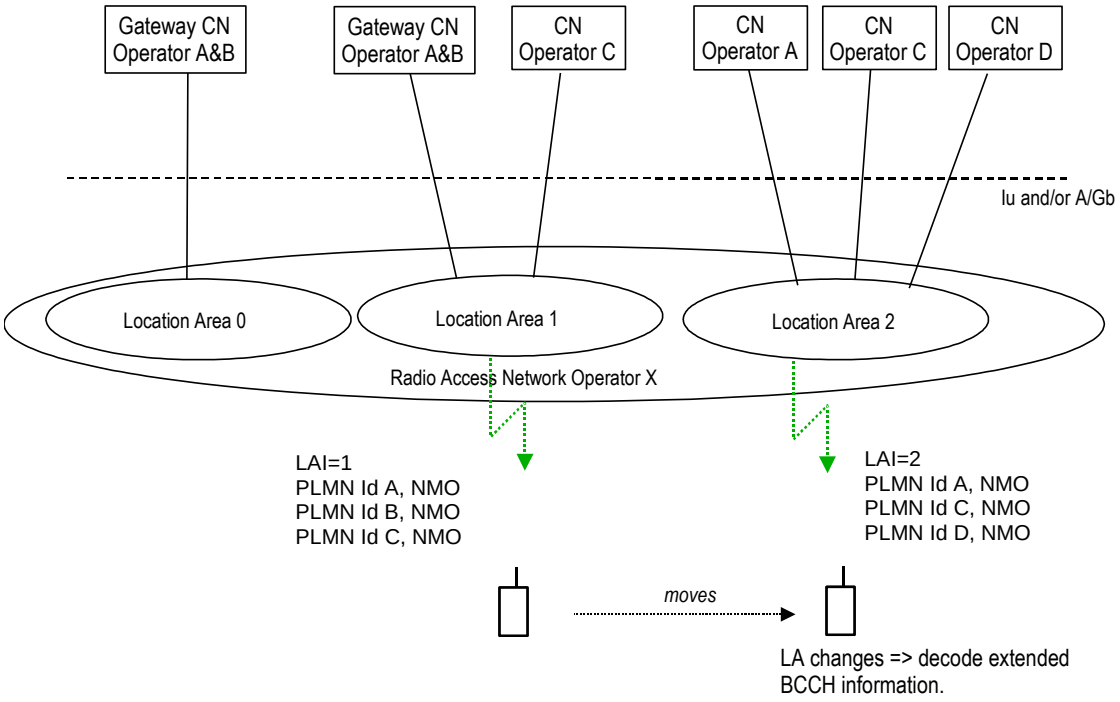
- not all USIM cards (even if the UE is a supporting UE) support this
- information in the USIM card becomes outdated when
  - a new sharing partner joins shared network, or
  - an existing partner quits shared network, or
- keeping the information up to date in all the USIM cards is major burden

This alternative does not seem to be a feasible solution due to its difficulties to cope with changes in the shared networks.

4.1.3.2 Broadcast channel based solution

Each cell in Rel-6 shared RAN broadcasts the operator identities and other relevant information, like NMO, about the CN operators providing service via the shared RAN. A supporting UE decodes this information and uses it in the PLMN selection process. When UE performs registration procedure with a shared network it indicates the selected operator to the network.

The figure below illustrates the solution.



When UE identifies that the LA changes in the broadcast channel, it decodes also the extended BCCH information containing the operator identities and other relevant network configuration information. The broadcast information could be optimised to avoid broadcasting the network configuration information for all the operators sharing a particular gateway core network, because essentially this information is same for all these operators [see sub clause 4.1.4].

Automatic network selection

The UEs takes each CN, indicated on RAN system broadcast, as an individual network. All these CNs together with other available conventional networks are compared with UE lists of preferred networks. The UE selects a network from these available networks according to the priority order described in TS 23.122.

Manual network selection

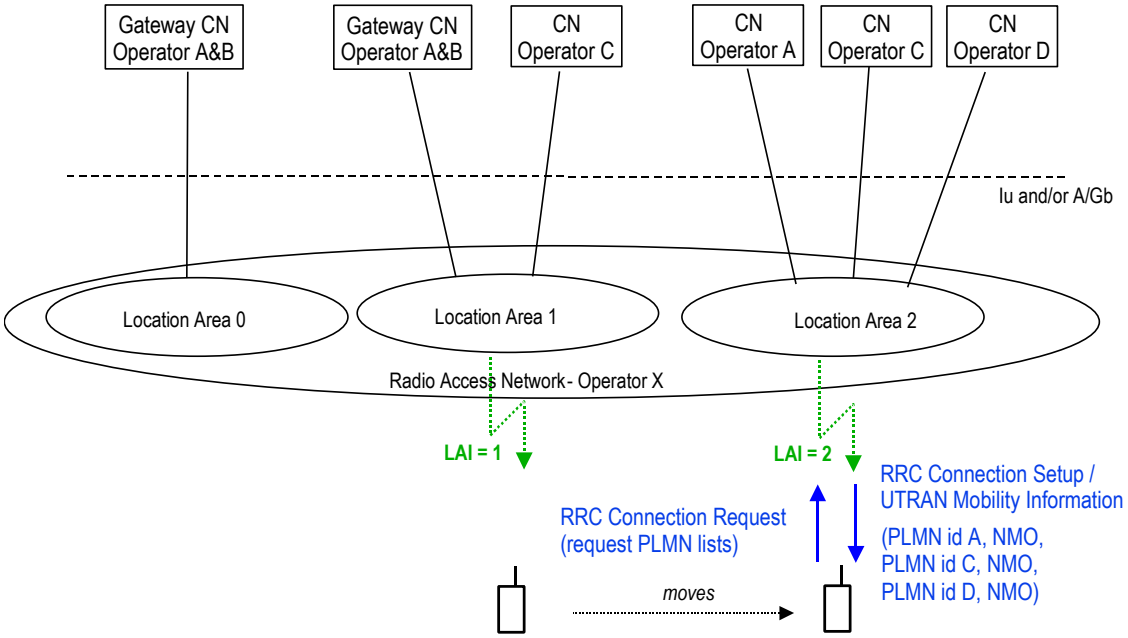
All available CNs, that are indicated on the system broadcast of the shared RAN, are presented to the user like conventional networks together with available conventional networks in accordance with the priority order described in TS 23.122. The user selects a network from the presented list of networks.

It has been determined that the addition of core network operator information to the system information in UTRAN, for example in the MIB or in a SIB, is feasible and can be done in such a way that the information would be ignored by non-supporing UEs but respected by supporting UEs.

4.1.3.3 Connected mode based solution

In connected mode based solution the UE asks network to provide information about available CN operators and other relevant information, like their associated NMO settings.

The following figure illustrates the connected mode based solution.



When UE identifies that the LA has changed it initiates the LA updating procedure. During RRC connection establishment a supporting UE indicates to the network that the list of CN operator identities with associated other NAS information should be provided. RNC returns the relevant information to UE during or immediately after the RRC connection establishment. This information could be provided e.g. either in RRC Connection Setup or UTRAN Mobility Information depending on whether the information can fit into the former message.

Automatic network selection

The UE collects the information about available networks, i.e. PLMN IDs from conventional networks and available CN operators from all shared networks by using dedicated connections towards the shared network(s) according to one the mechanisms described above. The UE selects a network from these available networks according to the priority order described in TS 23.122.

Manual network selection

For manual network selection the UE has to present to the user allthe available networks including the CNs that are behind a shared RAN. The UE derives from each shared networkRAN the list of available CNs and presents these like conventional networks together with available conventional networks to the user, arranged in the priority order described in TS 23.122. The UE performs attach and indicates the user selected CN to the network.

Alternatively, the CN may send the list of CN operator identities to supporting UEs in NAS messages. The supporting UE selects one of the listed CN operators. The list of CN operator identities is configured in the CN nodes and may change per Location Area. Especially for national roamers with supporting UEs the automatic network selection procedure could be optimised and the network assigns a CN operator without sending the list of CN operator identities to the UE when only one of the sharing CN operators accepts to serve the UE.

4.1.3.4 Behaviour of non-supporting UEs

Non-supporting UEs perform network selection according to TS 23.122 (pre-Rel-6). These UEs evaluate only the PLMN ID from pre-Rel-6 RAN system broadcast and will not be aware of the multiple CN operators available in the shared network. Therefore the network selects a CN operator from the available CN operators to serve these UEs as described in clause 4.3.

4.1.4 Optimisation by Shared Network Domain areas

4.1.4.1 Description

A Shared Network Domain (SND) corresponds to the area for which the broadcasted system information by the shared RAN is the same i.e. the same CN operators are available behind the shared RAN with the same configuration i.e. Network Mode of Operation (NMO). A SND is set of one to several location areas. The SND optimisation compared to the existing LA based mechanism described in the sections above is working as follows:

Each cell in the Rel-6 shared UTRAN broadcasts the identity of the Shared Network Domain. It is FFS whether these identities are unique within the shared RAN or whether these identities are of a "color-code" fashion (i.e. not unique within the shared RAN). When UE detects that SND has changed, it should check the identities of available CN operators and their associated network configuration information from the network before registering to the network as specified in above chapters.

The procedure could be optimised such that the UE temporarily stores the information for later use, i.e. when the UE next time enters the same SND area it would identify the shared network domain identity and retrieve the associated information from either USIM or terminal equipment. This approach is not applicable to the "color-code" solution.

4.1.4.2 Advantages

The main advantage of the SND optimisation resides in the case when the UE does not have to check the identities of available CN operators when LA or RA changes, because the current SND the UE is moving under has not changed.

In specific network sharing scenarios for which the number of sharing partners (long list of PLMN-ids) is high and the SND very big e.g. big part of a country, the UEs will have check the full list of PLMN-ids at each LA/RA change, although this information is likely to be always the same. However it remains FFS whether even in those specific cases this optimisation brings significant gains worth the complexity added.

4.1.4.3 Drawbacks

One main drawback of the SND concept is that it complicates network planning and management because of adding another area concept to existing RA, LA, and pool areas. The same functionality may be obtained based on Location Areas without introducing new area concepts. Furthermore, with SND the UE needs to store the SND identity and compare it at each LA change. For this purpose it needs to read and compare always the new SND identity at LA change.

4.1.5 Attach/detach handling

A supporting UE may indicate the selected CN operator at network selection and re-selection. This is obviously an optional information element in attach or location/routing area updating request messages. When a UE should attach to the same CN from which it detached certain information needs to be stored on the SIM. Three different mechanisms are discussed:

a) the serving CN operator encoded in the RA/LA identity

b) the NRI as part of the (P)TMSI identifies the CN operator

c) the CN operator is stored as a new information element on the SIM

Variant a) derives the CN from which the UE detached from the RA/LA stored on the SIM. The UE attaches to this CN when it is available. To enable such a mechanism the shared network configures multiple identities for each RA/LA for use in mobility management signaling. For GWCN an SGSN or MSC needs to configure for each RA/LA a separate identity for each sharing CN operator and potentially an additional identity for the non-supporting UEs. For MOCN an SGSN or MSC needs to configure for each RA/LA one identity for the sharing CN operator and potentially an additional identity for the non-supporting UEs. Also the resolution of RAI/LAI to SGSN or MSC/VLR addresses to find the old serving node has to configure all these identities accordingly. As the serving CN operator is encoded in the RAI/LAI a new MSC/VLR or SGSN can derive the old MSC/VLR or SGSN from old RAI/LAI also in MOCN configurations when multiple CN nodes (operators) serve the same physical RA/LA.

Variant b) uses the NRI to route attach signaling to the same CN from which the UE detached. The NRI is stored on the SIM as part of the (P)TMSI. The UE attaches to the shared RAN as identified by the RAI/LAI stored on the SIM. This

allows to use the same unique identity for each RA/LA for all sharing operators. This mechanism works also for non-supporting UEs. A new MSC/VLR or SGSN can derive the old MSC/VLR or SGSN from old RAI/LAI and NRI also in MOCN configurations when multiple CN nodes (operators) serve the same physical RA/LA.

Variant b) cannot re-attach to the same "PLMN" when a UE detaches from a CN operator on a shared network and attaches in another area where the same CN operator has a legacy network with the same ID. In this case an international roamer may attach to another CN operator when the same shared network is still available as the UE is searching for the RAN-PLMN-ID derived from LAI/RAI. When detach/attach are performed the same location the CN node is not changed. The change of the network in case of very specific network configurations should not harm as this can never generate a load compared to detach/attach at the same location.

Variant c) stores the serving CN operator as a new information element on the SIM. A UE performs attach to this CN when it is available. The UE could also search for a legacy PLMN with the ID of the stored serving CN operator.

4.1.5.1 Comparison

All variants allow supporting UEs to attach to the same serving CN operator from which the UE detached. Variant a) introduces considerable implementation, planning and configuration effort as the number of RA/LA identities multiplies. Variant a) and c) enables a supporting UE to attach to a legacy PLMN with ID of the old CN operator when detach was from a shared network. This is therefore only applicably when one operator shares the network in parts of a country and only for international roamers as national roamers are typically not accepted by the shared network when the CN operator has a non-shared PLMN in the same location.

Variant c) requires the SIM storage of new information element for shared networks.

From the comparison variant b) is preferred as it provides the intended attach/detach behavior without a need for new functionality. The marginal advantage of variant a) and c) for a specific geographical network configuration and only a subset of the terminals does not justify the additional effort.

4.2 Relationship with Iu Flex

"Intra Domain Connection of RAN Nodes to Multiple CN Nodes" [8] specifies a NAS Node Selection Function for the RAN nodes that differentiates between CN nodes. For network sharing these CN nodes belong to different CN operators. In case of MOCN, the Network Resource Identifier (NRI) value range, i.e. the TMSI value range is split between the CN operators. The NAS Node Selection Function in the RAN nodes is configured to select the CN node of the serving CN operator according to the NRI and to route initial NAS signalling to the selected CN node.

A UE entering an area where a MOCN is configured may have an NRI (TMSI) that is not conforming to the NRI split between CN operators of the MOCN. In this case and also when no NRI can be derived by the RAN the initial NAS signalling may be routed to a node of a CN operator that is not serving this UE. These UEs need to be transferred to a CN node of the CN operator that serves this UE.

It should be noted that "Intra Domain Connection of RAN Nodes to Multiple CN Nodes" [8] can be configured in parallel to network sharing by MOCN or GWCN to use the original features, like load sharing or increase of CN node services areas.

More sophisticated mechanisms for supporting UEs are FFS.

4.3 Assignment of CN operator and CN node

4.3.1 Description

In case of MOCN the redirection to another CN operator requires a change of the CN node until a CN node is found that serves the UE. Possible mechanisms to do this are:

1. The CN node may indicate to RNC that the initial NAS message should be forwarded to a node of another CN operator. Other information, like current value of N(SD), subscriber's identity (IMSI), and cause code may be forwarded too. The following mechanisms for handling of the redirection in the RNC have been identified (in subclause 4.x below is an information flow also given):

a. The RNC keeps track of what CN operators have been tried during the assignment procedure. It is done through information kept in the RNC during the assignment procedure.

b. Redirecting in RNC based on a random or weighted random selection to one of the remaining CN operators may be done. This ensures a statistical distribution between the available CN operators.

c. As an optimization, redirecting in RNC based on the IMSI passed from the CN node may be done. Only IMSI ranges of the CN operators of the MOCN are configured into the RNC. The gain from using this optimization in relation to complexity in the network is FFS.

d. Preventing the UE from timing out during the assignment procedure is handled by measuring the time duration of the assignment procedure. If there is not sufficient time to do a new attach attempt, the RNC simply drops the whole registration message. The UE is then expected to resend the registration request.

e. The setting of an appropriate cause code in the NAS registration reject message if all CN operators has rejected should be handled by RNC. The RNC does a cause code ranking and returns the corresponding NAS reject message to the UE. Information stored in a cache is used.

f. As an optimization, the connection-less interrogation described below may be considered. The gain from using this optimization in relation to complexity in the network is FFS.

2. The CN node may ask a node of another CN operator to serve the UE. The CN node, which will be able to serve the UE, allocates a Network Resource Identity to the UE. At the next NAS establishment, after this TMSI and Network Resource Identity allocation by the second CN, the signalling goes directly between UE and second CN node. There are two options envisaged for this:

   a. The first CN node asks other CN nodes of other operator(s) whether they want to serve the UE. It selects one CN node which has accepted to serve the UE and allocates to the UE an NRI received from the selected CN node. The selected CN node may also provide the first CN node with information to authenticate the UE. Information flows are described below in subclause 4.3.2.

   b. The first CN node forwards the initial NAS message to a second CN of another operator that might serve the UE, and then relays the L3 signalling between UE and second CN node.

3. The first CN node allocates a Network Resource Identity from a CN node of another operator to the UE and a 'wrong' LA/RA. This causes the UE to re-attach to another operator's CN node, which might serve the UE. For that purpose a range of NRIs from other CN nodes is configured on the first CN node.

All methods could present an issue with the MM timers in the UE if the redirect takes too long time. Method 1 requires some Iu, A and Gb enhancements. The method transfers the parts of or the complete (G)MM protocol machine possibly including link layer status from one CN node to another. It is ffs what information needs to be transferred. The handling for method 1 may involve several or all of the alternatives a) to f) above.

Method 2 requires some inter SGSN and inter MSC signaling enhancements. Method 2 works in A/Gb mode as well as in Iu mode.

Method 3 requires each CN node to derive authentication vectors from HLRs of networks that are not served by the CN node as the TMSI that contains the Network Resource Identity is allocated encrypted only. When multiple CN operators share the network this may require multiple attach/update procedures. The UE may receive services first when an update/attach is accepted by a serving CN node.

When a UE performs an initial access to a shared network one of available CN operators is selected to serve the UE. If due to Iu-Flexibility [8] multiple CN nodes of the selected CN operator serve the UE's location then one from these CN nodes is selected to serve the UE. After this initial access to the shared network the UE does not change to another available CN operator as long as the selected CN operator is available to serve the UE's location. Only the network selection procedures specified in 23.122 may cause a reselection of another available CN operator. Furthermore the UE does not change to another CN node as long as the selected CN node is available to serve the UE's location. The mechanisms specified for Iu-Flexibility [8] manage that CN operator and CN node are not changed as long as CN operator and CN node can serve the UE's location.

The RAN routes the UE's initial access to a shared network to one of the available CN nodes. For non-supporting UEs the shared network selects an operator from the available CN operators. Supporting UEs may select an operator from the available CN operators. When MOCN or when Iu-Flexibility [8] are configured it may be necessary to transfer the UE's initial access from one CN node to another, e.g. as the accessed CN node does not belong to the selected operator or because of load balancing between CN nodes belonging to the selected operator.

When MOCN or when Iu-Flexibility [8] are configured and the UE's initial access to the shared network is confirmed by the CN node of the selected CN operator the UE gets assigned a Network Resource Identifier as defined for Iu-Flexibility [8] and all subsequent accesses to the shared network the RAN routes to the serving CN node of the serving CN operator.

4.3.2 Information flow for CN centric redirection

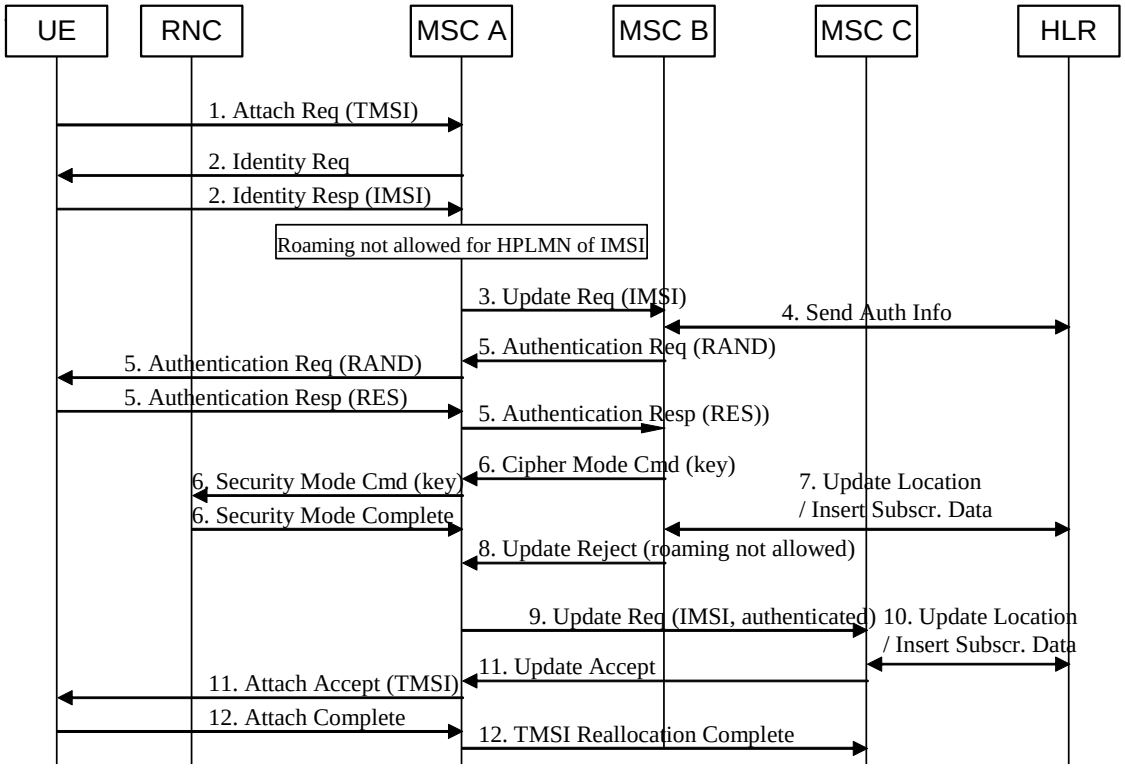


Figure 6: Information flow for CN centric redirection with connection-oriented signalling.

1) The UE selected the shared RAN and sends an Attach Request with TMSI. The RAN routes the signalling based on the NRI to MSC A. Or, if there is no CN node configured in RAN for the indicated NRI the RAN selects a CN node by load balancing or other rules.

2) When MSC A can not resolve the TMSI, MSC A performs the Identity Request procedure to get the IMSI from the UE. There is no need to contact MSCs of other operators as the NRI value space is coordinated between sharing CN operators and the first message is already routed to the CN operator that uses the UE's NRI. This assumes that also non-shared networks like GERAN networks which sharing CN operators use in parallel to the shared network use the same NRI split. Otherwise, first all other CNs need to try to resolve the TMSI.

3) MSC A determines from the IMSI that roaming is not allowed for the subscriber. MSC A selects the next MSC to which attachment should be tried and sends an Update Request to this MSC (MSC B). This message is sent on a signalling connection that the RNC provides between the two MSCs in which RNC routing does not require to store any MM UE information during the assignment procedure.

4) MSC B supports in general roaming for the HPLMN of the IMSI and requests Authentication Vectors from the HLR.

5) MSC B asks MSC A to authenticate the subscriber.

6) MSC B compares the authentication result and asks MSC A to start RAN ciphering.

7) MSC B updates the HLR and receives subscriber data from HLR.

8) The subscription data do not allow (e.g. regional or 3G) roaming. MSC B sends a reject message to MSC A. The signalling connection between the MSCs is released.

9) MSC A selects another MSC to which attachment should be tried, sends another Update Request to this MSC (MSC C) and indicates that the UE is already authenticated and that ciphering started. This message is sent on a signalling connection that the RNC provides between the two MSCs.

10) MSC C updates the HLR and receives subscriber data from HLR.

11) Subscriber data allow for roaming and MSC C ask MSC A to accept the attach request and to allocate the new TMSI to the UE.

12) The UE confirms the new TMSI with Attach Complete, which MSC A indicates to MSC C.

13) As the attach is performed via another MSC a potential follow on proceed request is ignored and the signalling connection with the UE is released.

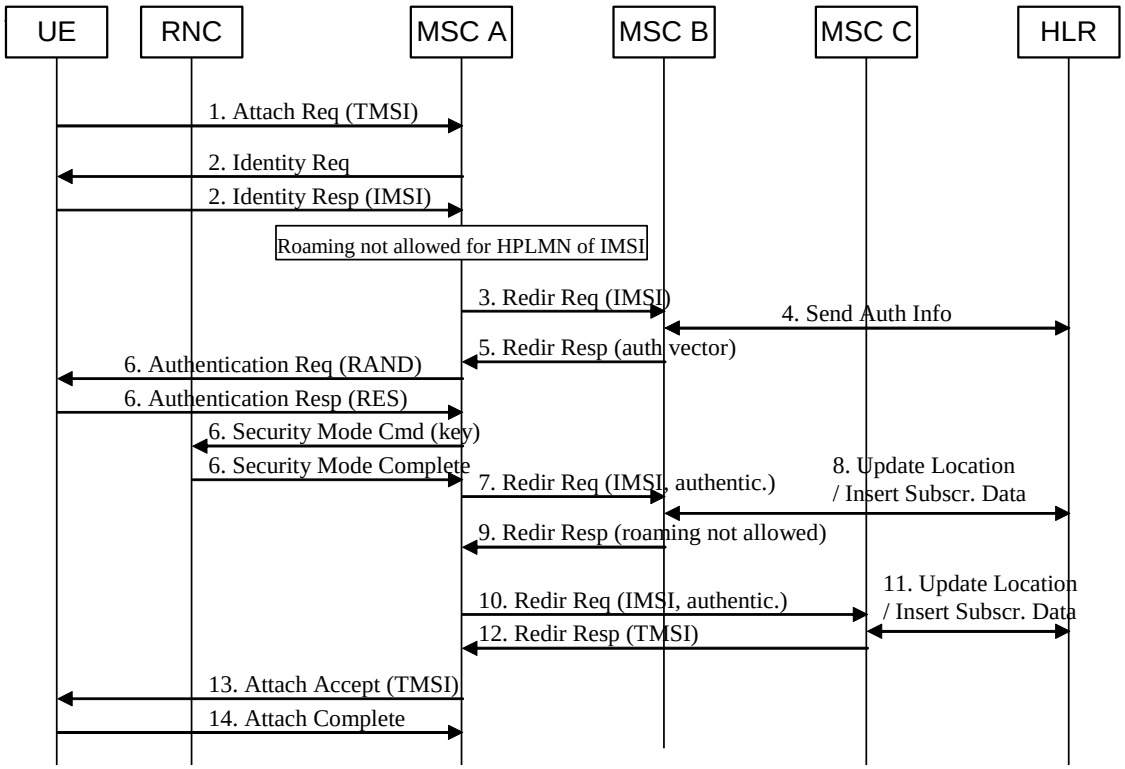


Figure 7: Information flow for connection-less CN centric redirection.

1) The UE selected the shared RAN and sends an Attach Request with TMSI. The RAN routes the signalling based on the NRI to MSC A. Or, if there is no CN node configured in RAN for the indicated NRI the RAN selects a CN node by load balancing or other rules.

2) When MSC A can not resolve the TMSI it may perform redirection requests with the TMSI instead with the IMSI. Otherwise, MSC A performs the Identity Request procedure to get the IMSI from the UE. When the NRI value space is coordinated between sharing CN operators then MSCs don't need to contact MSCs of other operators as the first message is already routed to the CN operator that uses the UE's NRI. This assumes that also non-shared networks like GERAN networks which sharing CN operators use in parallel to the shared network use the same NRI split. Otherwise, first all other CNs need to try to resolve the TMSI.

3) MSC A determines from the IMSI that roaming is not allowed for the subscriber. MSC A sends an Redirection Request to the RNC. Together with the Redirection Request it is indicated that redirection is required and a bitmap information element is added to keep track on redirections. The RNC determines a redirection target (MSC B in this case), marks CN B in the bitmap and forwards the Redirection Request together with the bitmap to MSC B. This message is sent connection-less on signalling resources that the RNC provides between the two MSCs The RNC does not store any UE specific information during the redirection.

4) MSC B supports in general roaming for the HPLMN of the IMSI and requests Authentication Vectors from the HLR.

5) MSC B provides an authentication vector to MSC A and returns also the bitmap.

6) MSC A authenticates the UE and starts RAN ciphering.

7) MSC A sends another Redirection Request to the RNC together with the bitmap. The RNC forwards the message to MSC B. The message indicates that the IMSI is authenticated.

8) MSC B updates the HLR and receives subscriber data from HLR.

9) The subscription data do not allow roaming (e.g. regional or 3G restrictions). MSC B sends a Redirection Response message to MSC A indicating a reject cause "roaming not allowed".

10) MSC A sends again Redirect Request together with the bitmap and the indication that redirection is required to trhe RNC. The RNC determines a redirection target (MSC C in this case), marks CN C in the bitmap and forwards the Redirection Request together with the bitmap to MSC C. The message indicates that the IMSI is authenticated.

11) MSC C updates the HLR and receives subscriber data from HLR.

12) Subscriber data allow for roaming and MSC C allocates a TMSI for the UE and sends it in the Redirection Response message to MSC A.

13) MSC A accepts the Attach and sends the new TMSI to the UE.

14) The UE confirms the new TMSI with Attach Complete.

After attach the signalling connection between UE and MSC A is released. Any subsequent mobile originated or mobile terminated transaction is routed to MSC C because of the allocated NRI. At the first signalling connection between UE and MSC C the UE may be re-authenticated and the TMSI may be reallocated.

MSC A repeats the redirection procedure until another MSC delivers a TMSI, or until the RNC rejects the redirection request, which indicates that no more CNs are available for redirection. This RNC reject indicates whether all CNs are tried, which causes a reject to the UE with "PLMN not allowed", or whether additional CNs are available in other parts of the shared RAN, which causes a reject to the UE with "no suitable cell in LA".

Alternatively this mechanism may use connection-oriented signalling.

4.3.3 Connection-less interrogation in RAN Centric redirection

To optimise the response time for attach of non-supporting UEs without valid NRI in larger shared networks, a connection-less interrogation of CN nodes may be used. In smaller shared networks, a longer response time may result from performing a connection-less interrogation. The gain from the connection-less interrogation in relation to complexity in the network is FFS.

The connection-less interrogation is an optimisation in the RAN centric redirect procedure and is described in the information flow diagram below. The connection-less interrogation provides a preliminary answer to the question if the CN operator can accept an attach from the UE. If the IMSI is known in the RNC, the IMSI is provided to the core network in the connection-less interrogation message. The answer is based on the IMSI of the UE and the roaming agreements the CN operator has. If IMSI is not provided in the connection-less interrogation, the MSC/SGSN tries to retrieve the IMSI from the old MSC / old SGSN. The connection-less interrogation does not involve any UE or HLR communication. If the IMSI of the UE is not known in the core network, this is indicated in the interrogation response so that a connection-oriented procedure can be performed to retrieve the IMSI. If the IMSI is available in the core network(s) it is provided to the RNC in the interrogation response.

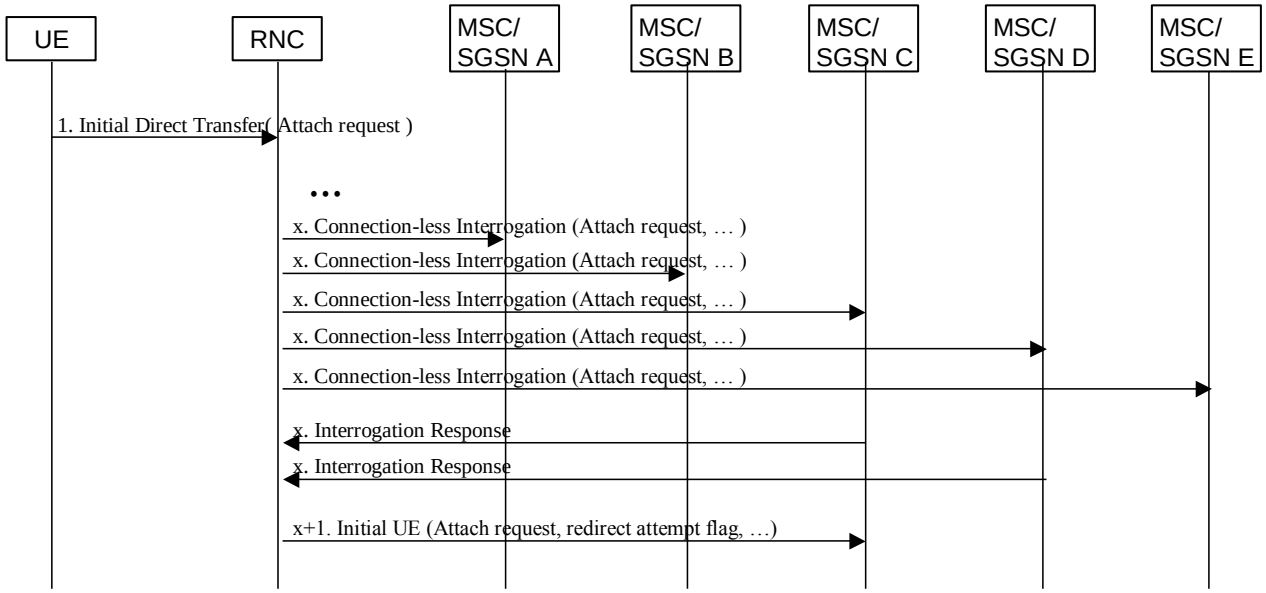


Figure 8, Connetion-less interrogation optimisation

4.4 Network name display

[Editor's note: TR 22.951 specifies certain requirements to network name display. Those requirements are identified and principles for the solutions are described here.]

The requirement on network name display in TR 22.951 states that the terminal shall always show the name of the core network operator the user has registered with.

Since core network operators are identified by ordinary PLMN-ids (MCC+MNC), no fundamentally new mechanisms or functionalities are needed for treating core network operators in shared networks in relation to network name display. If registration with a core network operator in a shared network is successful, the UE should follow exactly the same procedures for determining what should be shown on the display as if the chosen core network operator was not part of a shared network (see TS 22.101 [5]).

4.5 void

4.6 Usage of Gs interface

[Editor's note: It seems that multi-operator CN has certain impacts to the usage of Gs interface. Currently only one network mode of operation can be broadcast over the radio interface whereas in multi-operator CN operators may have different network configurations. The problem and the principle of the associated solution is described here.]

In networks without network sharing a UE is always served by the same CN operator for PS and CS domains. This behaviour should continue in networks that are shared.

The Gs interface may be configured to guarantee that the same CN operator serves the subscriber in CS and PS domains for non-supporting UEs. For GW CN the Gs messages indicate the CN operator that serves already the PS domain to the CS domain. For MOCN it is sufficient to configure the Gs interface as for this scenario the Gs is configured only between nodes belonging to the same CN operator.

Supporting UEs should select the same CN operator for CS and PS domains. The Gs interface may be used to reduce the time until a UE is attached to CS and PS domains.

4.7 Pre-Rel-6 Functionality

4.7.1 Shared Networks Access Control

The Shared Networks Access Control functionality available from Rel-5 onwards and defined in [7] allows the CN to request the UTRAN to apply UE specific access control to LAs of the UTRAN and LAs of neighbouring networks. The Shared Networks Access Control function is based on either whole PLMNs or Shared Network Areas (SNAs). An SNA is an area corresponding to one ore more LAs within a single PLMN to which UE access can be controlled. In order to apply Shared Networks Access Control for the UTRAN or for a neighbouring system, the UTRAN should be aware of whether the concerned LA belongs to one (or several) SNA(s) or not. If access for a specific UE needs to be restricted, the CN should provide SNA Access Information for that UE. The SNA Access Information indicates which PLMNs and/or which SNAs the UE is allowed to access. Based on whether the LA belongs to the PLMNs or SNAs the UE is allowed to access, the UTRAN determines if access to a certain LA for a certain UE should be allowed. If access is not allowed, the UTRAN should prevent the UE to obtain new resources in the concerned LA.

4.8 HPLMN support

In a GWCN multiple operators share MSC/VLR or SGSN. From transparency required for the user follows that a shared VLR/SGSN has to be treated by the HLRs belonging to the sharing scenario like a VLR/SGSN in the HPLMN to prevent roaming restrictions, for example. As the HLR derives from VLR/SGSN number whether the subscriber roams in H- or V-PLMN two different approaches exist:

1) The HLR configures all VLR/SGSN numbers of shared networks and handles these like own numbers, or

2) A VLR or SGSN of the GWCN gets one specific number from each supported HPLMN, i.e. a VLR or SGSN has multiple numbers.

For 1) the HLR decision whether the VLR/SGSN in H- or VPLMN has to be modified. Without GWCN it is sufficient to check Country Code (CC) and Network Destination Code (NDC) of the VLR/SGSN number to derive whether the user roams in the HPLMN or not. The HLR has to implement a configurable list of CC+NDC for GWCN network sharing scenarios. This list is compared with the CC+NDC of the VLR/SGSN number.

For 2) a number from every HPLMN belonging to the sharing scenario is assigned to each VLR or SGSN. The VLR/SGSN indicates towards the HLR always the number of the corresponding HPLMN. The HLR can continue to check CC+NDC to derive whether the user roams in V- or HPLMN. The HPLMN has to perform global title translation for some of the internal numbers that are assigned to VLRs/SGSNs in other networks. Without GWCN this is configuration dependent and typically not needed. The global title translation may be performed in a gateway node. When regional subscriptions are used the allocated zone codes have to be co-ordinated between operators.

One option requires HLR modifications and the other modifies VLR/SGSN. MSC/VLR and SGSN need already modifications for Network Sharing, e.g. configuration which PLMN IDs are part of the sharing scenario, HPLMN dependent routing of mobile originated services and others. For this reason approach 2) is preferred as it adds functionality to the anyhow impacted MSC/VLR and SGSN and avoids HLR modifications.

4.9 Information flow for RAN centric redirection

An example of an information flow for the RAN centric redirection is shown below. In this example an attach request from a non-supporting UE is directed to three different CN operators. The first rejects since it has no roaming agreement with the subscribers Home PLMN. The second rejects because of a roaming restriction found in HLR. The third CN operator accepts and completes the attach request. The different “MSC/SGSNs” in the example below shall be seen as different CN operators. One specific CN operator may of course also have several pooled MSCs/SGSNs connected to the RNC if Iu-flex is used. This is discussed further in subclause 4.10.

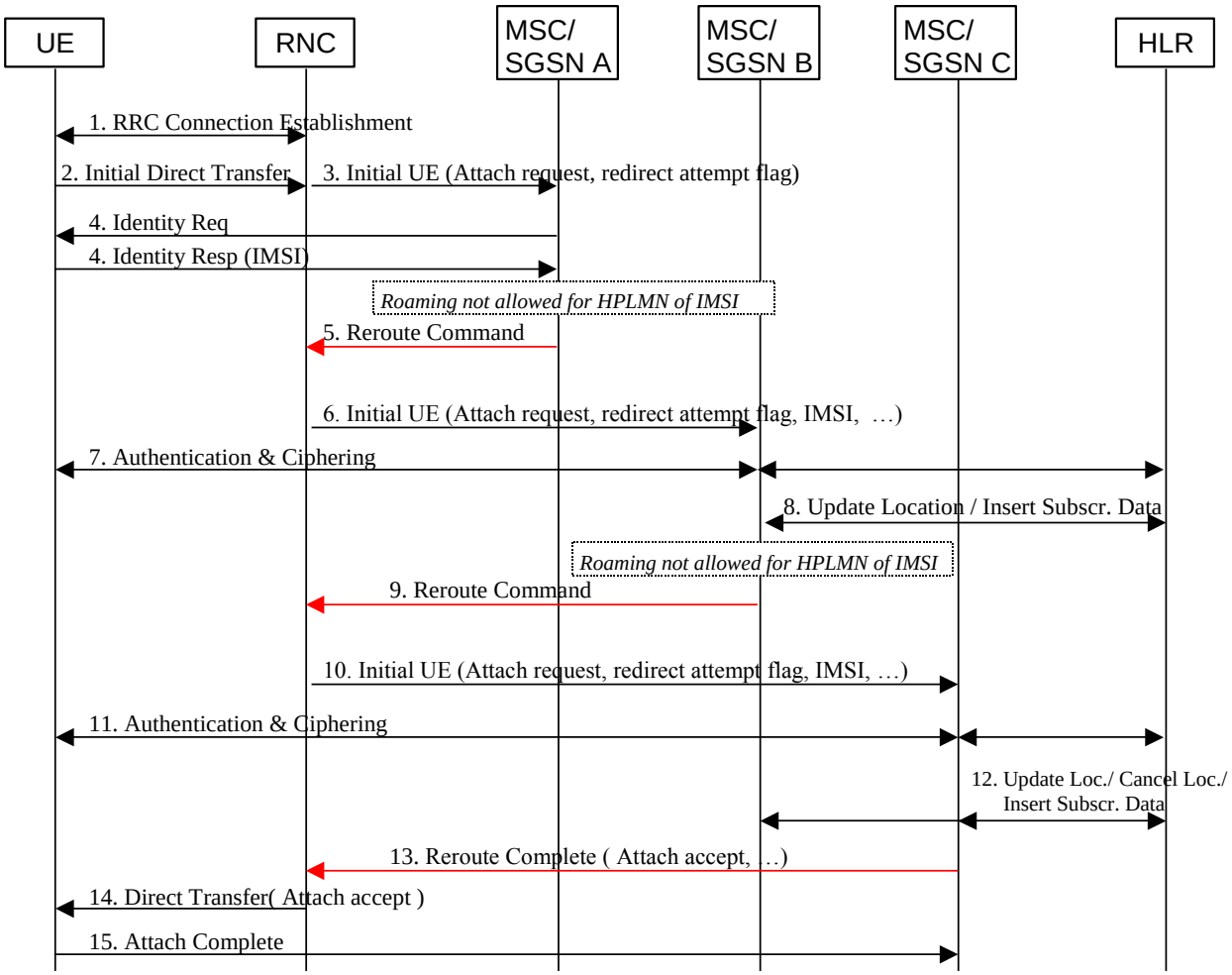


Figure 9, Information flow for RAN centric redirection

1) The RRC connection is established.

2) RNC receives an Initial Direct Transfer from an UE. The RNC is configured to work in a Shared RAN MOCN, and therefore it forwards the NAS message in an Initial UE with an additional *redirect attempt flag* set. The flag indicates that the MSC/SGSN shall respond to the attach request with a *Reroute Command* or *Reroute Complete* message. Selection of CN node is based on NRI (valid or invalid) if present in IDNNS or by random selection. A *redirect attempt flag* could also simply be the fact that the Initial UE message does not include any selected PLMN-ID (later RAN3 decision), which a supporting UE would include. Redirect is never done for supporting UEs.

3) The MSC/SGSN receives the Initial UE with the *redirect attempt flag* set. It then knows it shall answer with a *Reroute Command* or *Reroute Complete* message. Those new messages might also be extensions to the Direct Transfer message (later RAN3 decision).

4) The MSC/SGSN needs the IMSI of the UE. It is retrieved either from old MSC / old SGSN or from the UE as in this example. By comparing the IMSI with the roaming agreements of the CN operator, the MSC/SGSN discovers that roaming is not allowed. Attach procedure is aborted.

5) A message is sent back to the RNC with two NAS messages, the attach reject message and the original attach request message received from the UE (alternatively the original NAS message may be stored in the RNC). The IMSI is also included in the message, plus a reject cause code to the RNC. The message should be a new RANAP message, *Reroute Command*. It might also be an extended Direct Transfer message (later RAN3 decision).
The signalling connection between RNC and MSC/SGSN A is released. The RNC selects a MSC/SGSN in the next step. The already tried MSC/SGSNs is stored in the RNC during the redirect procedure so that the same node is not selected twice.

6) The RNC sends a new Initial UE to the next selected MSC/SGSN with the original NAS attach request message. Redirect attempt flag is set and IMSI may also be included to avoid a second IMSI retrieval from UE or old MSC/SGSN. The MSC/SGSN receiving the message starts its attach procedure.

7) MSC/SGSN B does in general support roaming for the HPLMN of the IMSI and hence authentication is done and RAN ciphering is established.

8) MSC/SGSN B updates the HLR and receives subscriber data from HLR.

9) The subscription data do not allow roaming (e.g. regional or 3G). MSC/SGSN B sends a Reroute Command message including the attach reject message, a reject cause code, the original attach request message (alternatively stored in the RNC), and the N(SD) (for MSC only). IMSI is included in Reroute Command message only if it was not included in the Initial UE received by the MSC/SGSN.
The signalling connection between the RNC and the MSC/SGSN B is released. The RNC then selects a new MSC/SGSN as in step 5.

10) The MSC/SGSN **C** receives an Initial UE (with the original NAS attach request message) with the redirect attempt flag is set, an IMSI, and N(SD) (if MSC). The MSC/SGSN C starts the attach procedure and uses provided information (IMSI and N(SD)).

11) MSC/SGSN C does in general support roaming for the HPLMN of the IMSI and hence authentication is done and RAN ciphering is established.

12) MSC/SGSN C updates the HLR and receives subscriber data from HLR. Subscriber data allows roaming, and the MSC/SGSN C completes the attach procedure. This includes the assignment of a new TMSI/P-TMSI with an NRI that can be used by RNC to route subsequent signalling between UE and correct MSC/SGSN (Iu-flex functionality). The Update Location sent to HLR also triggers a Cancel Location sent to the MSC/SGSN B.

13) A *Reroute Complete* message with the NAS Attach accept message is sent to RNC. By usage of a specific Reroute Complete message, the RNC knows that the redirect is finished and can both forward the NAS message to the UE and clean up any stored redirect data (it is a later RAN3 decision if an extension to the Direct Transfer message shall be used instead of a new message).

14) The Attach Accept is forwarded to the UE. The UE stores the TMSI/P-TMSI with the Iu-flex NRI to be used for future signalling, even after power off. This is existing functionality.

15) UE responds with an Attach Complete message.

If the RNC finds no more MSC/SGSN to redirect to after receiving a Reroute Command message, e.g. step 5 or step 9, it compares the cause code with cause codes from other Reroute Command messages it has earlier received for this UE. A cause code ranking is done and the “softest” cause code is chosen and the corresponding saved NAS attach reject message is returned to the UE.

Each CN node that receives an Initial UE, shall run its own authentication procedure. This may in some rare situations cause the UE to be authenticated more than once, however the trust-model used is that one CN operator shall not trust an authentication done by another CN operator. This will of course not be an optimal usage of radio resources, but given the rare occurrence of this, the increased signalling should not be of any significance.

During the redirect procedure the RNC keeps a timer, which corresponds to the UE timer of releasing the RR connection (20 seconds). If the RNC when receiving a Reroute Command message finds that there is not sufficient time for another redirect, further redirect attempts are stopped (for this attach request message). The UE will repeat its attach request four times (each time waiting 15 seconds before it re-establishes the RR connection for another try). The risk that a random selection after four retries would still have missed one MSC/SGSN that would have accepted the UE can be calculated to a very small probability.

4.10 RAN Centric redirection architectural description aspects

- The used IMSI ranges of all the CN operators in the shared network may be configured in each RNC in shared RAN. This ensures that never more than one redirection is needed for home subscribers of the CN operators of the shared network.

- Specification and design of the redirect function must consider that a CN operator shall be able to use pooled CN resources, i.e. Iu-flex. Moreover, the redirect selection function (using stored info in RNC e.g. earlier tried nodes, info received in Reroute Command and randomising function) is highly related to the Iu-flex selection

function in the RNC, see figure below. This needs to be considered when specifying the redirect function to minimize impact in standards and products.

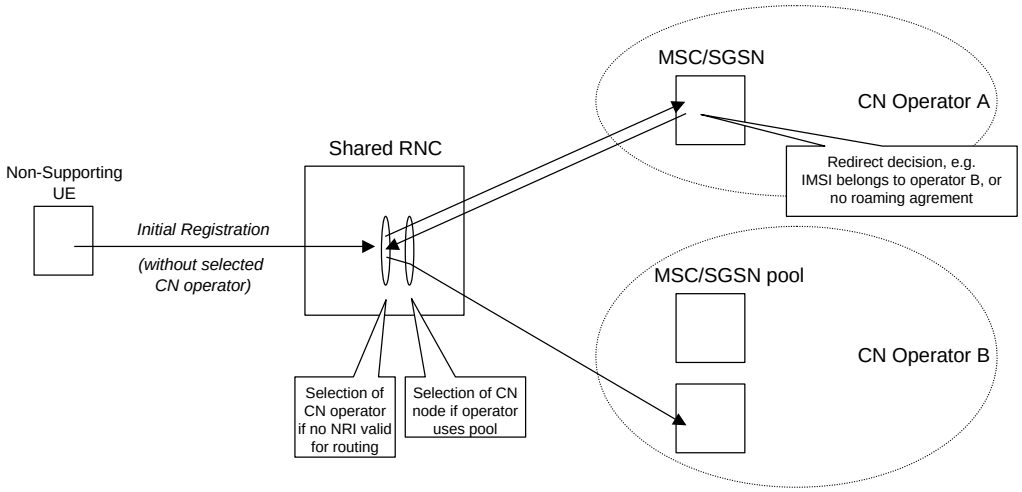


Figure 10, Pool aspects for MOCN redirect function

- There may be need for special consideration to be taken when the coverage of the shared RAN is non-coinciding for all the CN operators.

5 Functional Description

5.1 MS Functions

A mon-supporting UE should behave according to the NMO of the selected core network. Non-supporting UE behaves according to the default NMO of MOCN.

In Iu mode the UE selects the core network as described in [3] and provides the identity of the selected core network to the RNC in RRC signalling as described in [4].

5.2 RNC Functions

The RNC routes the initial NAS signalling messages from a supporting UE according to the selected core network.

For MOCN the RNC provides functionality defined for "Intra Domain Connection of RAN Nodes to Multiple CN Nodes" [8].

In the case the selected core network operator shares also part of its CN i.e. MSC/SGSN, the RNC forwards the selected core network operator identity to CN.

Functions to direct signalling between different CN operators, if any, are FFS.

RNC broadcasts supporting UEs a dedicated set of NAS information (see 3GPP TS 24.008) for each core network in the MOCN, which is FFS.

5.3 BSC Functions

[Editor's note: This chapter describes BSC functions.]

5.4 MSC Functions

When a UE accesses the MSC the first time, i.e. when there is no VLR entry for this UE, the MSC verifies whether the UE belongs to one of the operators sharing the MSC or their roaming partners. For that purposes the MSC derives the IMSI from another MSC/VLR or from the UE. In case of GWCN the MSC determines a serving CN operator unless the old MSC/VLR or the UE have indicated a CN operator. For GWCN the MSC/VLR stores the serving CN operator, for the sole purpose of separating charging information for different CN operators (see subclause 6.2). In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the MSC may need to transfer the UE to another MSC, for example, when the MSC does not belong to the selected operator or for load balancing between MSCs serving the same shared network area by means of Iu-Flexibility. In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the MSC/VLR that finally serves the UE assigns to the UE a Network Resource Identifier, which is part of the TMSI. All subsequent UE accesses the RAN routes to the serving MSC/VLR.

5.4.1 Transferring UEs to another MSC/VLR

If the first MSC is not able to provide service to the UE, the MSC needs to be able to transfer the UE to another CN. Mechanisms for this and related MSC functions are described in "Assignment of CN operator and CN node".

5.5 SGSN Functions

When a UE accesses the SGSN the first time, i.e. when the UE is not yet known by the SGSN, the SGSN verifies whether the UE belongs to one of the operators sharing the SGSN or their roaming partners. For that purposes the SGSN derives the IMSI from another SGSN or from the UE. In case of GWCN the SGSN determines a serving CN operator unless the old SGSN or the UE have indicated a CN operator. For GWCN the SGSN stores the serving CN operator, for the sole purpose of separating charging information for different CN operators (see subclause 6.2). In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the SGSN may need to transfer the UE to another SGSN, for example, when the SGSN does not belong to the selected operator or for load balancing between SGSNs serving the same shared network area by means of Iu-Flexibility. In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the SGSN that finally serves the UE assigns to the UE a Network Resource Identifier, which is part of the TMSI. All subsequent UE accesses the RAN routes to the serving SGSN.

5.5.1 Transferring UEs to another SGSN

If the first SGSN is not able to provide service to the UE, the SGSN needs to be able to transfer the UE to another CN. Mechanisms for this and related SGSN functions are described in "Assignment of CN operator and CN node".

6 Charging and Accounting Aspects

In [6] it is stated that charging solutions shall support the shared network architecture so that both end users and network sharing partners can be correctly charged for their usage of the shared network.

6.1 Inter-operator charging and accounting

CN operators will presumably consume different amount of resources of the shared RAN. The RAN operator may therefore want to charge CN operators accordingly. Generally, volume/time based charging and accounting will not be sufficient because resource consumption is also dependent on quality parameters (e.g. Eb/No - power consumption) of the delivered resources. It is FFS whether the shared RNS therefore should be capable of generating the following charging and accounting information:

- Identity of CN Operator (probably PLMN-id), whose end user has consumed the resource of the RAN.
- Resource, e.g. radio bearer
- Start time – indicating the set up time of radio resource.
- op time – indicating the time the radio resource was released.
- ference to geographical area where the radio resource was used, e.g. cell reference.

- SI of the end user, who has consumed radio resource.

It is noted that the information generated in the RNS is not intended for end-user charging. The format of the charging information ("RAN-CDR") should be standardized.

[Editor's note: It might be possible to provide this charging information by monitoring the Iu interface signalling. This needs further study, but solutions that minimise the impact on the RNC are desirable.]

6.2 End customer charging

End users should be correctly charged in a shared network. The charging system of the shared network should be able to separate the charging information generated by shared MSC/SGSN and send it to the correct CN operator, i.e. the CN operator that served the end user, based on available information in the CDRs generated by the shared MSC/SGSN.

Note: This section is only relevant in the GWCN, where MSC/SGSNs are shared.

7 Security Aspects

8 Conclusions

The following main conclusions regarding the architecture for network sharing have been made and can be used for further work on network sharing in SA2 and in other groups.

- Core network operator should be identified by a PLMN-id (MCC+MNC).
- A network sharing information, i.e. available core network operators in the shared network, should be transmitted in broadcast system information.
- Network sharing supporting UE should be able to indicate to the network which core network operator he wants to receive services from.
- For supporting UEs, redirection should be avoided.
- The UE behaviour for GWCN and MOCN should be the same. It should not be necessary to broadcast to the UE whether the shared network is a GWCN or a MOCN.
- The open issues are related to redirection and to Gs interface use in the MOCN architecture.

9 Open Issues

Following open issues have been identified which need further studies:

- Optimisation of authentication vector usage in MOCN; In case of rerouting, the first attempted CN node may have retrieved authentication vectors from old CN node and authenticated the user before rerouting is initiated. This leads to a situation in which the next CN node authenticates the user with old authentication vectors and the authentication will fail. This could be avoided if the first attempted CN node forwards the unused authentication vectors to the next CN node during rerouting.
- Involvement of the HLR when transferring UEs between CN operators and how multiple MSCs/SGSNs can access subscription data in the HLR for the same UE
- The need for cause code coordination in MOCN needs to be evaluated. There is a trade off between impact of existing standards and benefit of the function.
- The network selection mechanisms in MOCN need to be defined when the LS response from RAN2 and GERAN2 is available.

Annex A (informative): Signaling flows for manual and automatic network selection

In this Annex we present signalling flows for manual and automatic network selection in a GWCN and a MOCN architecture for successful and unsuccesfull registration attempts. The examples are based on that information concerning available core network operators are broadcasted in system information.

The examples refer to ATTACH REQUEST and REJECT messages. Depending on whether messaging goes to the CS or PS domain, these messages represent the relevant NAS messages for these purposes.

Network selection in a GWCN

Non-supporting UEs cannot understand the Rel-6 multiple PLMN information in the broadcast system information and therefore are only able to identify the common PLMN of the shared network. The signaling flow is thus just as if the UE was attaching to a pre-Rel-6 network, see the figure below.

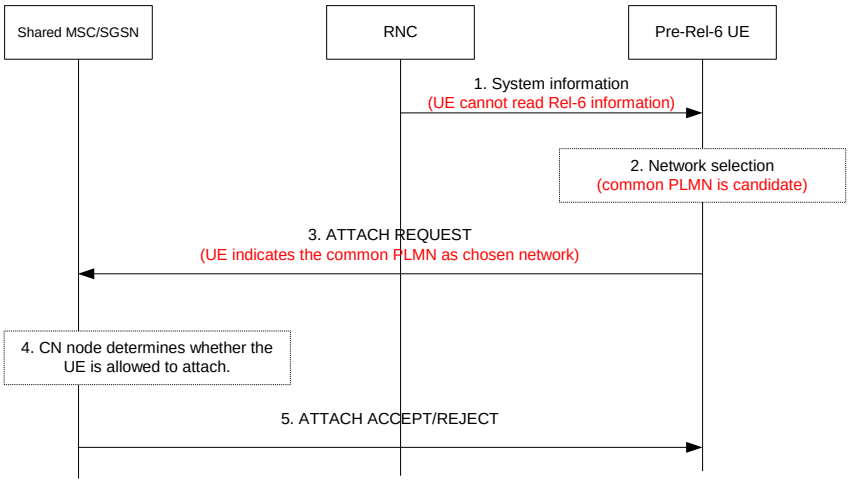


Figure A1. Successful registration by a non-supporting UE in a GWCN.

1. The UE reads the broadcast system information in the shared RAN. The non-supporting UE ignores the Rel-6 shared network information since it cannot handle this information. It therefore treats the common PLMN as the candidate for network selection.
2. The UE performs network selection as specified in pre-Rel-6 versions of TS23.122.
3. The UE sends an ATTACH REQUEST message to the network.
4. The core network determines whether the UE is allowed to attach to the network according to already established procedures.
5. The shared core network node sends the appropriate ACCEPT/REJECT message back to the UE.

Signalling regarding, for example, authentication have been left out for simplicity. This is the case for all the flows presented in this Annex.

Supporting UEs can make use of the additional information in the broadcast system information. The signaling flow is shown in the figure below.

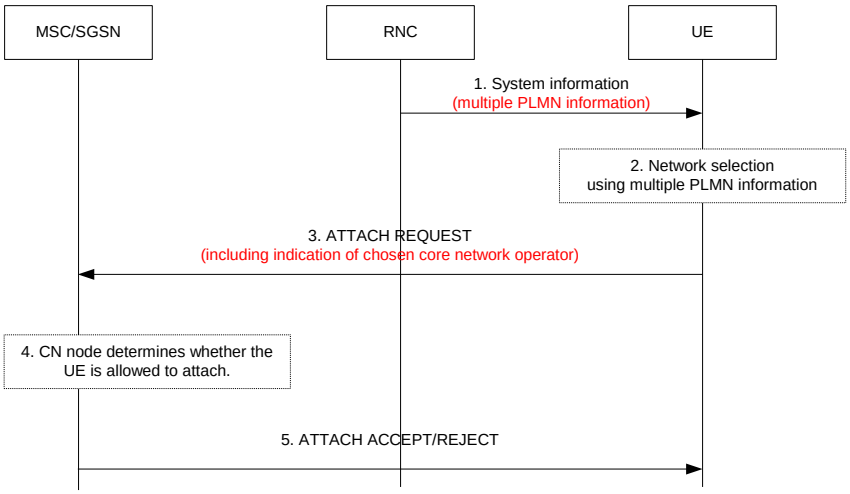


Figure A2. Network selection by a supporting UE in a GWCN.

1. The UE reads the broadcast system information in the shared RAN and detects that this is a shared network. It reads the additional shared network PLMN information and supplies the shared network PLMNs as inputs to the network selection procedure in the UE. The common PLMN is not given as a candidate for network selection.
2. The UE performs network selection as defined in the Rel-6 version of TS23.122 (to be defined by stage 3 work).
3. The UE sends an ATTACH REQUEST message to the network, indicating the chosen core network operator.
4. The core network determines whether the UE is allowed to attach.
5. The shared core network node sends the appropriate ACCEPT/REJECT message back to the UE.

Network selection in a MOCN

[Editor's note: Non-supporting UE network selection makes use of redirection functionality not decided upon yet.]

Supporting UEs can make use of the additional information in the broadcast system information. The signaling flow is shown in the figure below.

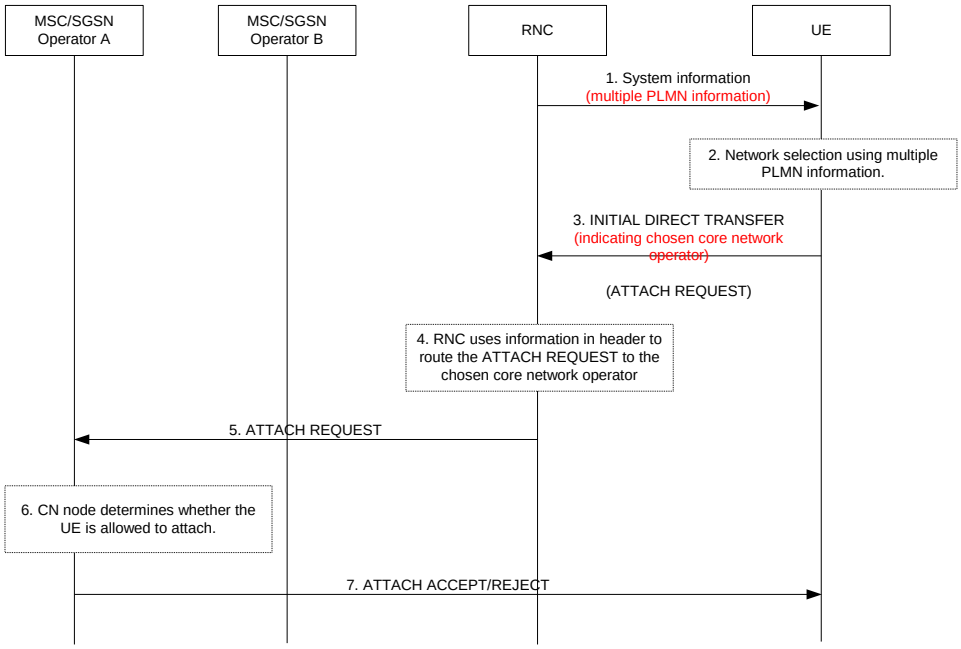


Figure A3. Network selection by a supporting UE in a MOCN.

1. The UE reads the broadcast system information in the shared RAN and detects that this is a shared network. It reads the additional shared network PLMN information and supplies the shared network PLMNs as inputs to the network selection procedure in the UE. The common PLMN (as broadcasted in the MIB) is not given as a candidate for network selection.

2. The UE performs network selection as defined in the Rel-6 version of TS23.122 (to be defined by stage 3 work).

3. The UE sends an ATTACH REQUEST message encapsulated in a INITIAL DIRECT TRANSFER message (RRC). It adds information concerning the chosen core network operator for routing purposes in the RNC.

4. The RNC uses the routing information to determine which core network operator the message should be sent to. This optimises the attach procedure since no rerouting is necessary.

5. The ATTACH REQUEST message is sent to the core network operator chosen by the UE.

6. The core network determines whether the UE is allowed to attach to the network.

7. The shared core network node sends the appropriate ACCEPT/REJECT message back to the UE. In case of an ATTACH ACCEPT message, the core network assigns the UE an appropriate TMSI/P-TMSI so that this identity can be used for any further rerouting of messages by the RNC.

Annex B:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2003-01					First draft of TR – creation of version 0.0.0 at TSG SA2#29 (S2-030190)	---	0.0.0
2003-01					Raised to version 0.1.0 at TSG SA2#29	0.0.0	0.1.0
2003-05					Revised as per approved documents at TSG SA2#31: - S2-031599 (Gs interface) - S2-031382 (Rerouting of registration signalling) - S2-031407 (Text in Sec 1 and Sec 2) - S2-031542 (Text in Sec 4) Between TSG SA2#31 and TSG SA2#32 the TR was assigned number 23.851. This change is included in version 0.2.0. The document containing the above changes and additions changes that was approved at TSG SA2#32 is S2-031973.	0.1.0	0.2.0
2003-05					Revised as per approved document S2-031973	0.2.0	0.2.1
2003-05					Revised as per approved documents at TSG SA2#32: - S2-032045 (network name display; removal of sentence, see meeting minutes) - S2-032132 (shared network domain introduction) - S2-032133 (network selection alternatives) - S2-032134 (core network operator identity)	0.2.1	0.3.0
2003-08					Revised as per approved documents at TSG SA2#33: - S2-032702 (charging) - S2-032703 (Introduction of GWCN) - S2-032704 (Signalling of selected operator identity from UE to CN)	0.3.0	0.4.0
2003-08					Editorial updates	0.4.0	0.4.1
2003-08					Revised as per approved documents at TSG SA2#34: - S2-033094 (Network Sharing with HPLMN Support) - S2-033199 (Shared Network Access) - S2-033250 (TR clarification and clean-up to SND definition and network selection solution alternatives)	0.4.1	0.5.0
2003-09	SA#21				First presentation for Information at TSG SA#21.	0.5.0	1.0.0
2003-11					Revised as per approved documents at TSG SA2#35: - S2-033745 (Re-routeing mechanisms) - S2-033746 (Initial Assignment of UEs to CN Operators) - S2-033747 (Relationship with Iu Flex)	1.0.0	1.1.0
2004-01					Revised as per approved documents at TSG SA2#36: -S2-034119 (Gs interface usage) -S2-034120 (Redirecting UEs between CN nodes) -S2-034121 (PLMN and Core Network operator selections) -S2-034122 (Connected Mode CN Selection)	1.1.0	1.2.0
2004-02					Revised as per approved documents at TSG SA2#38 -S2-040714 (Assignment of CN operator and CN node) -S2-040857 (Attach/Detach handling in Shared Networks) -S2-040716 (Signaling flows for network selection) -S2-041038 (Proposed conclusions)	1.2.0	1.3.0
2004-03	SA #23	SP-040051			Presentation to SA #21 plenary for approval	1.3.0	2.0.0
2004-03	SA #23	SP-040051			Raised to v.6.0.0 after approval at SA#23 (same content as	2.0.0	6.0.0

					previous version)		
2004-06	SA#24	SP-040324	001	1	Clarification of Gs usage	6.0.0	6.1.0
2004-06	SA#24	SP-040324	005	1	Clarification of CN operator identity usage in MSC and SGSN	6.0.0	6.1.0
2004-06	SA#24	SP-040324	006	4	Information flow of the CN centric redirection	6.0.0	6.1.0
2004-06	SA#24	SP-040324	011	3	Detailing RAN Centric redirection	6.0.0	6.1.0
2004-06	SA#24	SP-040324	012	3	Connection-less interrogation as optimisation	6.0.0	6.1.0