Guidelines for IPv4 Addressing, AS Numbering for GPRS Network and Mobile Terminals

Version 8.0

12 January 2015

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association’s antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

The GRX Network was first established in 2000 for the purpose of GPRS roaming and only GSM operators were allowed to connect to it. Since then other services have been added such as UMTS roaming and MMS interworking.

With the development of IMS and SIP-related services, the GSMA has recognised the need to involve organisations outside the GSM/UMTS community and has facilitated the GRX network evolving into the IPX concept. Organisations outside the GSMA membership will be allowed to connect for the purpose of IMS/SIP interworking and other similar services. This document has been updated to reflect the fact that non-GSM organisations may connect to the IPX. Terminology has also been changed:

- An organisation connecting to the IPX network is known as a “Service Provider”.
- The term “User Equipment” is now used in place of “Mobile Terminal” and "User Terminal" where appropriate.

All organisations connected to the IPX network, irrespective of whether they are GSM operators or not, will need to adhere to a common set of IP addressing rules and related guidelines that are described in this document.

The GSMA worked closely with the all the RIR communities (RIPE NCC, ARIN and APNIC) to develop and produce the early versions of this document. This was essential to ensure that the proposed guidelines to the Service Providers associated with requesting and implementing Public addresses are aligned with the existing policies and procedures of the RIR community.

Annex A provides an overview on the Internet Registry System and its hierarchical architecture, ranging from the overall co-ordinating body (ICANN) to the end user.
Annex B identifies some useful web links for each RIR associated with their services and Public IP address request policies and procedures.

This document is produced and maintained by the GSMA. However, unlike other documents produced by this organisation, its intended readership extends beyond its members to also include the RIR community. Hence, the style and language used in this document has attempted to accommodate this wider audience wherever possible.

The respective party can submit any changes/comments to this document as follows:-

- GSMA members: mailto:iregpacket@infocentre.gsm.org (using existing change request procedures)
- RIRs: via the authors of this document or directly to the GSMA via the GSM World web site mailto:info@gsmworld.com.

It should be noted that this document been assigned a ”Non Confidential” classification so that it can be distributed within the Public Domain. This document will be made available on the Public GSM World web site http://www.gsmworld.com/about/index.html.

1.2 Scope

This document provides addressing-related guidelines to organisations wishing to inter-connect to each other using a private IP Backbone network including the GRX network and its successor, the IPX. It covers the following areas related to addressing:

1. IP addressing for Service Provider and GRX/IPX Provider network infrastructure
2. Autonomous System (AS) Numbering of the IP network associated with a Service Provider's network infrastructure
3. IP addressing for User Equipment (UEs)

The above is described in a service-agnostic way, but references to other relevant GSMA PRDs where necessary.

This document also describes how Service Providers can request IP addresses and Autonomous System Numbers (ASNs) for use with their networks using procedures that are aligned with the Internet Registry System and the GSM Association (GSMA).

In association with item 3 above, some guidelines are also provided for consideration by the Regional Internet Registry (RIR) communities to assist with their existing procedures for processing Public IPv4 address space requests received from Service Providers.

Administration and Governance procedures for the IPX network are being established. Currently, these new procedures are out of scope and this document refers throughout to the GSMA.

1.3 Definition of Acronyms and Abbreviations

Acronym / Abbreviation	Description
AfriNIC	African Network Information Centre
APN	Access Point Name
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
AS	Autonomous System
ASN	Autonomous System Number
ASO	Address Supporting Organisation
ASP	Application Service Provider
BGP	Border Gateway Protocol
DNS	Domain Name System
DR	Delegated Registry
FNO	Fixed Network Operator
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
HPLMN	Home PLMN
IANA	Internet Assigned Number Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IR	Internet Registry
ISP	Internet Service Provider
LACNIC	Latin American Continent Network Information Centre
LAN	Local Area Network

Acronym / Abbreviation	Description
LIR	Local Internet Registry
MoU	Memorandum of Understanding
MT	Mobile Terminal
NAT	Network Address Translation
NIR	National Internet Registry
PC	Personal Computer
PDN	Packet Data Network
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PRD	Permanent Reference Document
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RFC	Request for Comments
RIR	Regional Internet Registry
SGSN	Serving GPRS Support Node
SSL	Secure Socket Layer (protocol)
UT	User Terminal
VLSM	Variable Length Subnet Mask
VPLMN	Visited PLMN
WAP	Wireless Access Protocol
WTLS	Wireless Transport Layer Security

1.4 Definition of Terms

Term	Description
Public Address	Registered IPv4 address [12].
Private Address	Unregistered IPv4 address [5].
Service Provider	A business entity entering into a contractual relationship with one or more IPX provider(s). Thus, "Service Provider" includes MNOs, FNOs (for example, fixed broadband operators and NGNs), ISPs, ASPs and so on.
PLMN Operator	A mobile network operator offering GPRS / UMTS services. This term is used where the document applies specifically to this type of operator and not to the more general "Service Provider".
IPX Provider	A business entity (such as an IP Carrier) offering IP interconnect capability for one or many IPX Services compliant with the IPX requirements.

1.5 Document Cross-References

Ref	Document Number	Title
1	N/A	Ripe-185: European Internet Registry Policies and Procedures; RIPE Local Internet Registry Working Group http://www.ripe.net/docs/ripe-185.html
2	IETF RFC 1930	"Guidelines for creation, selection and registration of an Autonomous System"
3	GSMA PRD IR.21	"GSMA roaming database, structure and updating procedures"
4	GSMA PRD IR.34	"Inter-Service Provider IP Backbone Guidelines"
5	IETF RFC 1918	Address allocation for Private Internets
6	3GPP TS 23.060	General Packet Radio Service (GPRS); Service description; Stage 2
7	N/A	OMA WAP related specifications: Wireless Application Protocol Push Architectural Overview Wireless Application Protocol Push Proxy Gateway Service

Ref	Document Number	Title
		Specification http://www.openmobilealliance.org/Technical/wapindex.aspx http://www.openmobilealliance.org/tech/affiliates/LicenseAgreement.asp?DocName=/wap/wap-250-pusharchoverview-20010703-a.pdf http://www.openmobilealliance.org/tech/affiliates/LicenseAgreement.asp?DocName=/wap/wap-249-ppgservice-20010713-a.pdf
8	GSMA PRD IR.33	GPRS Roaming Guidelines
9	IETF RFC 3027	Protocol complications with the IP Network Address Translator
10	IETF RFC 2993	Architectural implications of NAT
11	3GPP TS 29.061	Interworking between PLMN supporting GPRS PDN
12	IETF RFC 791	Internet Protocol
13	GSMA PRD IR.88	LTE Roaming Guidelines

2 General Guidelines

The guidelines presented in this document are based upon the following two fundamental requirements:

1. Existing request policies and procedures operated by the RIRs must be adhered to when Service Providers request Public IP address space and Public ASN.
    a. Each service provider must individually submit a request for Public IP address space and Public ASN in accordance with these policies and procedures.
    b. Private addresses must be used wherever possible for UT addressing where IPv4 addressing is needed.
    c. Public addresses are only used for UT addressing for services where it can be demonstrated that the use of Private addresses is not feasible or practical.
    d. Public addresses will not be issued for purposes that this document has shown can be supported using Private addresses, unless the requestor can demonstrate otherwise.
2. Public address space (particularly that of IPv4) must be conservatively and efficiently used.
    a. Private addressing must be used wherever possible for IPv4. Public addressing in IPv4 must only be considered where it is not possible or practical to support Private IPv4 addressing.
    b. Dynamic IP addressing should be deployed wherever possible to conserve both the Public (and Private IPv4) address space available.
    c. Wherever possible, utilise any previously assigned spare Public address space before requesting new Public addresses.

The following has been agreed between the GSMA and the RIR communities in relation to the guidelines presented in this document above:

1. IP addressing guidelines for network infrastructure and User Equipment:
    a. Public addresses are requested from RIRs for this purpose using the existing RIR request policies and procedures.
2. ASN guidelines:

a. Public (registered) ASNs are requested for use in the network infrastructure using their existing request policies and procedures.

b. Private (unregistered) AS Numbers can be requested from the GSMA via the following email address: "as_number@gsm.org".

3 IP Addressing Policy Guidelines for GRX/IPX Network Infrastructure

3.1 General requirements

This section of the document provides guidelines to Service Providers to request and use Public IPv4 and IPv6 addresses for their network infrastructure. Guidelines covering the issue and use of IPv6 addressing is considered work in progress in this version of the present document.

It is essential that all Service Providers adopt these guidelines and adhere to the procedures and processes of the Internet Registry System in order for interworking on the IPX network to operate successfully.

These guidelines do not guarantee that a Service Provider will be assigned public IP address space. Address space assignment will be assessed on an individual request basis as per the existing request policies and procedures of the Internet Registry System.

Service Providers will have one or more IP networks to host their services offered on the IPX network, whether GPRS/UMTS roaming, IMS/SIP, MMS etc.

GSMA PRD IR.34 [4] provides further technical details on the IPX network.

Each IP-addressable network element involved in the above services on the IPX network must be uniquely addressed.

When the GRX network was first proposed, investigations conducted by the GSMA with the Internet community identified that Public addresses would provide the most practical solution to meet its addressing requirements. This addressing solution has been carried forward as the GRX has evolved into the IPX.

3.2 Policy guideline details

3.2.1 Addressing for IPX/GRX network infrastructure

Public IP address space must be used on all network elements involved in the GRX/IPX network by Service Providers and IPX Providers.

Any Public IP addresses used on the IPX network must not duplicate Public IP addresses used on the public Internet.

Private IPv4 address space (as defined in IETF RFC 1918 [5]), rather than Public IPv4 address space, can and should be used wherever possible within Service Providers' internal network and IPX Providers' internal network. This is recommended in order to reduce the amount of Public IPv4 address space required from RIRs. Use of IPv6 address space within the Service Provider's internal network is for further study.

3.2.2 Utilising existing assigned public address space

Service Providers may already have Public address space which has previously been assigned to them. To help conserve the Public address space, wherever possible, service providers should utilise any such existing address space for addressing their network infrastructure before requesting new Public addresses for this purpose.

Note that if the assignment of Public address space is changed for another purpose than it was originally requested for, the details of this change of address usage should be notified by the Service Provider to the organisation, which made the original address allocation. This could be the LIR, NIR, DR, RIR, or an ISP. In case of any doubt, the RIR should be informed.

3.2.3 Requesting new Public address space

New Public address space assignment must be requested by Service Providers and IPX Providers from the appropriate LIR/NIR/DR using existing procedures supported by its respective serving RIR.

This document can be used as part of the request submitted by the Service Provider as a source of reference to help explain the requirement for Public address space.

The LIR/NIR/DR selected should be one that is served by one of the three RIRs that is responsible for serving the country of the requesting Service Provider.

The IP address space request policies and procedures can be obtained from the respective RIR's home web sites as defined in Annex A.

3.2.4 Notification of infrastructure address assignment to GSMA

It is the Service Provider's responsibility to notify their interconnect/roaming partner Service Provider(s) of the Public IP address range(s) assigned to their network infrastructure for all the IP based services they operate on the GRX/IPX network. This must be done so that the other Service Provider can configure the appropriate security mechanisms at the edge of their network.

For Service Providers who are members of the GSMA, GSMA PRD IR.21 [3] should be used for notifying the GSMA and other Service Providers of the Public address range(s) being used by that Service Provider. It is the responsibility the Service Providers to maintain and keep this information up to date. Other mechanisms may be used, but these are outside the scope of the present document.

3.2.5 Notification of infrastructure address assignment to GRX/IPX Provider(s)

It is the Service Provider's responsibility to notify their GRX/IPX Provider(s) of the Public IP address range(s) assigned to their network infrastructure for all the IP based services they operate on the GRX/IPX network. This must be done so that the GRX/IPX Provider can configure the appropriate security mechanisms within their network.

Note that a Service Provider must not include any IP address ranges used for User Terminals in the range of infrastructure IP addresses notified to the IPX Provider(s). This point is explained further in section **Error! Reference source not found.**.

GRX/IPX Providers must ensure that they do not include routing information for User Terminal IP address ranges on their networks. This provides an extra layer of security against attacks initiated from User Terminals.

3.3 Guidance notes

3.3.1 LIR registration

GRX/IPX network connectivity is normally provided by international data carriers. These organisations are usually already established as LIRs. Hence, they will already have the necessary administration in place to process requests for Public IP addresses from the Service Providers.

A Service Provider may belong to an organisation that already has an ISP as part of its constituent, and this ISP is likely to be registered as an LIR (or member) of the respective RIR. In this case, the ISP may be in a position to provide the necessary administration to process requests for Public IP addresses from its associated network operator. This may be the preferred option for larger Service Providers. Smaller Service Providers may elect to request their address space requirements from their GRX/IPX Provider, or from the ISP associated with another Service Provider that is registered as an LIR.

3.3.2 Requesting Public IP address space

Annex B provides some useful information on requesting Public IP address space for the different RIRs.

4 Autonomous System Number Guidelines for Network Infrastructure

4.1 General requirements

This section of the document provides guidelines to Service Providers to request and assign an Autonomous System Number (ASN) to their network infrastructure.

The total IP network of a Service Provider connected to the GRX/IPX Network is considered as an Autonomous System (AS).

Each AS may have an associated AS Number (ASN) to uniquely identify it. This identifier is used in the routing process to interconnect the IP networks of other service providers across the IPX network.

A service provider should use a publicly assigned AS number. As a last resort, if a service provider is unable to obtain a public AS number, a private AS number can be obtained from the GSMA. Private AS Numbers can only be assigned to GSMA Members.

Although the use of publicly assigned AS number is encouraged, if a service provider already has been assigned a private AS number then the service provider does not necessarily need to obtain new publicly assigned AS numbers.

More information on AS numbers, mainly oriented towards their use on the Internet is available in IETF RFC 1930 [2].

4.2 ASN range

The ASN is defined as a 16-bit integer, hence limited to 65535 unique values.

The Internet Registry System has divided the ASN space for Public and Private uses as follows:

- Public ASN range: 0 through to 64511
- Private AS number range: 64512 through to 65535 (i.e. 1024 values)

4.3 Policy guideline details

The following sections describe the policy guidelines and provide guidance notes for Service Providers to request and implement a Public or Private ASN for their network infrastructure.

1. The need for use of an ASN depends on a Service Provider's connectivity to the GRX/IPX network.
   - If a Service Provider exchanges routing information with one or more GRX/IPX Providers, for example using BGP, use of an ASN is mandatory.
   - Otherwise, use of an ASN is optional although there is minimal benefit from using an ASN in this case.
2. A Service Provider should use a public ASN (as defined in section 4.2) for their network. The following must be noted:

If a private ASN is used, private ASNs must not be advertised on the global Internet.
A Service Provider can decide to change their assigned Private ASN to a Public ASN at a later stage

There is no obligation for a Service Provider to use a Public ASN if a Public IP addressing scheme has been deployed in its network i.e. a Private ASN can be assigned to a Service Provider's network even though its network elements have been assigned Public addresses. If the Service Provider already uses an ASN on the public Internet, their ASN used on the GRX/IPX network will normally be the same. If the Service Provider has multiple ASNs on the public Internet, they should re-use one of these on the GRX/IPX network.Any ASN used by a Service Provider must be unique within the IPX network.

3. The GSMA will administer the assignment of Private ASNs to its members.
4. As explained in section 4.1, if a service provider is unable to obtain a public ASN it can request a Private ASN from the GSMA via the following email address: as_number@gsma.com
5. The Service Provider must only use a private ASN when they are a GSMA member. Ex Members should cease to use the assigned AS Number.and notify the GSMA that the ASN is no longer in use
6. It is the Service Provider's responsibility to notify the GSMA via as_number@gsma.com when the private ASN is no longer in use
7. A Service Provider can request a Public ASN from their respective RIR. Details of the ASN request process can be obtained from the home web site of the RIR, as listed in Annex A.
8. The present document can be used as part of the request submitted by the Service Provider as a source of reference to help explain the requirement for a Public ASN.
9. It is the Service Provider's responsibility to notify their interconnect/roaming partner Service Provider(s) of the ASN assigned to their network. For Service Providers who are members of the GSMA, GSMA PRD IR.21 [3] should be used for this purpose. It is the responsibility the Service Providers to maintain and keep this information up to date. Other mechanisms may be used, but these are outside the scope of the present document.

10. It is the Service Provider's responsibility to notify their GRX/IPX Provider(s) of the ASN assigned to their network.
11. It is recognised that with the introduction of the IPX concept and an increased number of Service Providers wishing to connect, the available stock of 16 bits private and public ASNs is relatively small. Therefore, IPX providers are strongly encouraged to insure that their network equipment is ready for 32 bits ASN support.

5 IP Addressing Policy Guidelines for User Equipment

5.1 General

5.1.1 Version of IP addresses

There are two versions of the Internet Protocol that are currently available:

i) IPv4

- Uses a 32-bit address structure
- Theoretically provide up to $2^{32} = 4.3\text{x}10^9$ addresses

ii) IPv6

- Uses a 128-bit address structure
- Theoretically provide up to $2^{128} = 3.4\text{x}10^{38}$ addresses

Although networks can be created using one or both technologies, IPv4 is the version that is currently predominantly used in most private networks and the Internet. However, the remaining available IPv4 address space will eventually become exhausted, and so the introduction of IPv6 is highly recommended. IPv6 address space has already been allocated to the RIRs, and the RIRs have been allocating address space to the ISPs.

Existing deployments of GPRS and UMTS networks generally use IPv4. However, IPv6 deployment is starting to appear.

5.1.2 IPv4 Public and Private addressing

The IP address space is controlled and managed by the RIRs, which has segregated the IPv4 address space into the Public and Private address ranges as described below.

- IPv4 Public address space
  - Used on the Internet
  - Requested via the respective RIR serving the PLMN operator's area (see Annex B)
  - Note that there is insufficient address space to assign a fixed Public IPv4 address to each UE.
- IPv4 Private address space
  - Private address ranges defined in IETF RFC 1918 [5]
  - Must not be used on the Internet
  - Do not have to be requested from any RIR
  - Can be used in Private networks for any purpose

Some of the key benefits associated with Private addressing are as follows:

1. Protection of Public address space

- Use of Private addressing helps to protect the depletion of the Public address space. This effectively enables more Public address space to be made available to those services where it is required.

2. Rapid deployment

- There is no requirement to follow a request process for Private addresses from the RIRs, as is the case for Public addresses.

3. Security factors

- NAT will be typically implemented with additional security measures, e.g. Firewall. In this way, Internet users cannot access users on the Private NAT side, and hence these users are provided some security from unwanted traffic and 'malicious' Internet users. However, it should also be noted that NAT can also limit deployment of some security solutions (e.g. IPsec). IETF RFC 2993 [10] and IETF RFC 3027 [9] provide further information associated with NAT deployment and security considerations.
- Protection from unwanted traffic to the UE user will be required. This becomes increasingly important, particularly when considering billing will be typically based upon the data exchanged by the UE user, who does not want to be charged for receiving unsolicited data traffic.

Some of the caveats associated with Private addressing are as follows:

1. NAT must be used

- The limitations associated with NAT are described in the following section.

2. Limitations on Private address range

- The 10.0.0.0/8 Private address range can offer approximately 16.8 million host addresses for assignment to the UE.

5.1.3 Network Address Translation (NAT)

5.1.3.1 Overview

The NAT function allows one addresses from one scheme to an address of another. It is commonly used to translate Private IPv4 addresses to Public IPv4 address in order to interconnect to a global IP network (e.g. Internet).

The NAT function is normally incorporated on a device that is situated on a border-device (e.g. BG, firewall) of the private network.

5.1.3.2 NAT limitations

There are a number of limitations associated with the use of NAT. IETF RFC 3027 [9] also defines some of the main protocol complications associated with NAT.

Some of the general limitations associated with NAT are listed below, but it is beyond the scope of this paper to elaborate further on them.

1. NAT can be used where connections are initiated by a user on the private network side of the NAT. However, NAT cannot resolve a Private address if the request has been initiated from the Public network side of the NAT, e.g. for 'push-based' services where remote servers may send un-requested messages to users. A typical example for this in PLMN-based services is when mail arrives at the mail server and a 'mail waiting' notification needs to be sent to the recipient that is located on the private network side of the network. However, there are alternative solutions to overcome this type of limitation (for example, 'WAP push services'), allowing Private addresses to still support this type of push-based service.

2. Scalability and the management of large numbers of these devices and active sessions.

3. NAT does provide some benefits to security, as it will make it difficult for unwanted users to directly access devices located on the private network side. However, NAT also has the potential to interrupt the end-to-end nature of Internet applications. This could interfere with some aspects of end-to-end security and other end-to-end functions, such as the following examples:

- Certain types of the security protocol IPsec cannot be used in conjunction with NAT.
- End-to-end applications associated with connection control, lawful intercept, quality of service and duration-based-billing could be interrupted.

4. NAT imposes topology restrictions and other constraints on the protocols and applications that run across NATs.

5.2 Service Provider assignment to User Equipment

5.2.1 General

Service Providers require IP addresses for assignment to their subscriber's UEs. One or more IP addresses may be required per UE. The number and type of addresses assigned to the UE will depend upon the capability of the UE and the services supported by the Service Provider. The following types of IP address can be used for this purpose:

- IPv4 Public address space
- IPv4 Private address space
- IPv6 address space

It is recognised that it will not be possible to assign every UE with a Public IPv4 address as this would exhaust the available supply. Service Providers must share the responsibility for applying the guidelines presented in this document to ensure that the available Public address space is used conservatively and efficiently in accordance with the policies laid out by the RIRs. It is therefore recommended that Service Providers adopt the following general policy:

- IPv6 prefixes and Private IPv4 addresses are used wherever possible for UE addressing.
- Public IPv4 addresses are only used for UE addressing for services where it can be demonstrated that the use of IPv6 prefixes and Private IPv4 addresses is not feasible or practical.

Service Providers will be responsible for submitting their own request(s) for IPv6 and Public IPv4 address space to the appropriate RIR. These requests should be in accordance with the existing policies and procedures of the relevant RIR.

5.2.2 Conformance to RIR policies

Any use of Public address space for UEs must conform to the existing IP address space request policies and procedures defined by the RIRs.

Public addresses can be requested from the RIR serving the area of the requesting user. The relevant procedures for this process are provided in Annex B of this document. The requestor must be able to meet the criteria for the issue of these addresses before any address space is allocated and assigned to them. This criteria is predominately associated with the requestor being able to demonstrate conservation and effective utilisation of the Public address space requested.

5.2.3 UE Public Address Space request and approval guideline details

The following guidelines have been agreed for use by the network operators and the Internet Registries in conjunction with Public IPv4 address space associated with the Mobile Terminals.

5.2.3.1 Network Operator guidelines

Note 1: There is insufficient available address space for all network operators to assign every MT a Public IP address as the default.

Note 2: Each network operator will be responsible for submitting their own request(s) for Public IP address space requirements to the appropriate Internet Registry in accordance with the existing request policies and procedures supported by the relevant RIR.

Note 3: Each network operator will be responsible for designing and implementing services, and for IP address deployment in their own network. However, all operators have a shared responsibility to adhere to the principles of conserving Public IP address space and its efficient usage.

- Annex A describes the Internet Registry System.
- Annex B provides a summary of the main web links associated with the IP address request procedures for each RIR.
- Annex D provides some examples and guidelines on how various types of services could be designed and implemented by network operators. Note that implementation of these designs are not mandatory - see Note 3 above.

The following guidance is provided for note and consideration by the network operator when requesting Public address space from the appropriate Internet Registry: -

- The request must demonstrate and justify the requirement for Public addresses
- Identify any efforts the network operator is making to contribute towards the conservation of Public address space, e.g.: -
  - Identify the quantity of Private addresses being used for existing or planned services in relation to the quantity of Public addresses now being requested.
  - Identify any use of dynamic addressing to demonstrate efficient usage of addresses, e.g. the volume of users expected to share the requested Public address space.
- Requests for Public addresses for use with GPRS services identified in these guidelines that have been shown can be supported using Private addressing may be rejected unless the network operator can otherwise justify.
  - E.g. Public addresses cannot be justified for WAP-only services. Note that for this particular case, requests will be rejected by the Internet Registry unless there are exceptional circumstances that can be satisfactorily explained
- This PRD IR.40 document can be used as part of the request submitted by the network operator as a source of reference to help explain the requirement for Public address space.

5.2.3.2 Internet Registry guidelines

The Internet Registry receiving a request for Public address space from a network operator will process it according it is existing procedures to determine if the request will be approved or rejected. To assist the Internet Registries with this activity, the GSMA also proposes the following additional guidelines for their consideration:

1. Main GPRS services requiring Public address
   - “Open Internet Access”
   - “Internet” Service APN (for roamers)

In both the above cases, the numbers of customers expected to take up these services is expected to be relatively small compared to NAT-compatible WAP and web services.

2. Other services that require Public addresses
   - Internet Registry to apply their normal rules for assessment

6 Annex A: Internet Registry System

6.1 Overview

The Internet Registry system has been established to primarily administer and manage the available public Internet address space on a worldwide basis. It is comprised of various hierarchically organised bodies, including an overall co-ordinating body (ICANN), the Address Supporting Organisation (ASO) and the Regional Internet Registries (RIR). RIRs are classified according to their primary function and territorial scope within the hierarchical structure and can be organised as Regional IRs (RIR), National IRs (NIR), Delegated Registries (DR) and Local IRs (LIR), followed by Internet Service Providers (ISPs) and End Users (EUs), as depicted in Figure 1.

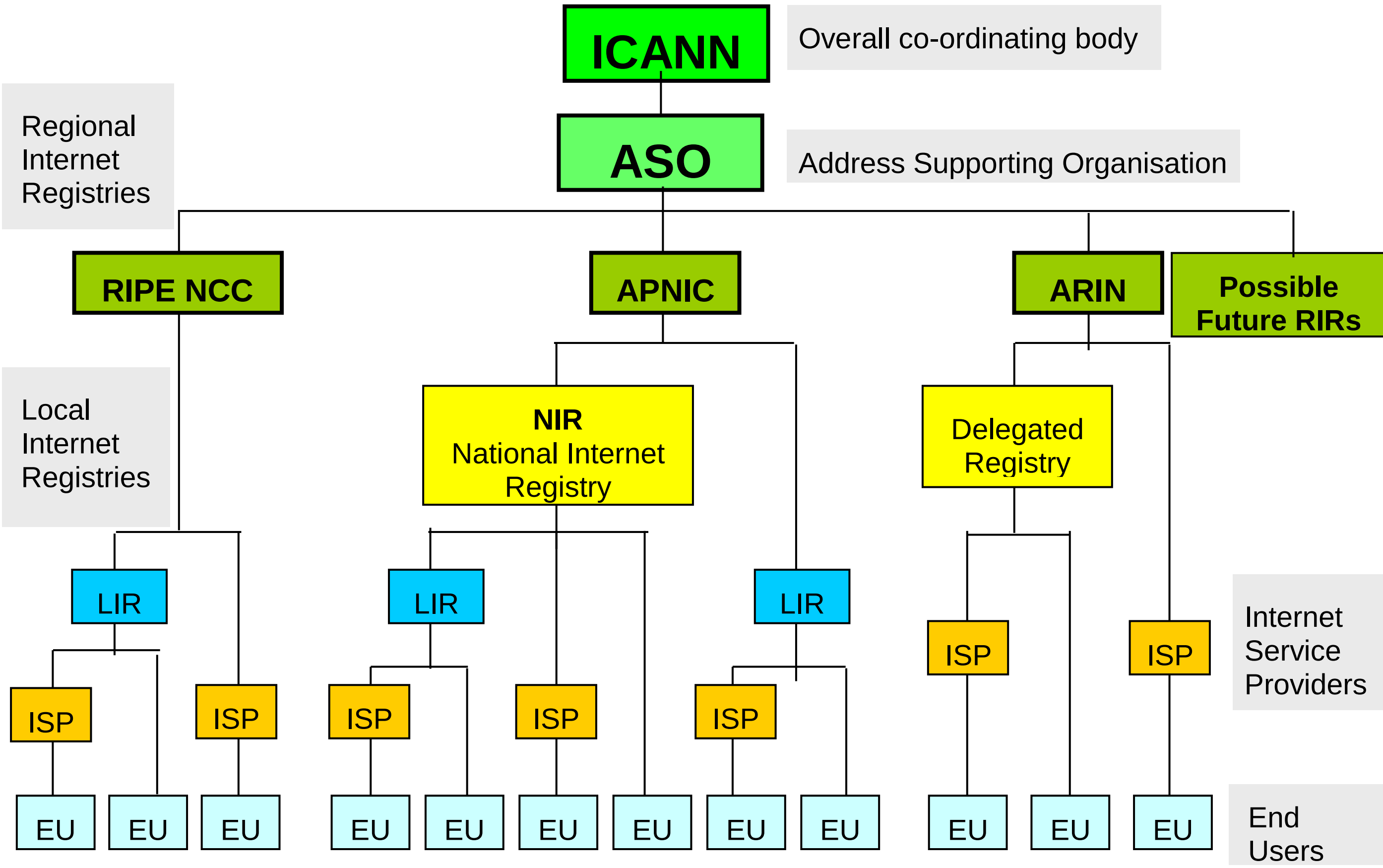
ICANN
Overall co-ordinating body
Regional Internet Registries
ASO
Address Supporting Organisation
RIPE NCC
APNIC
ARIN
Possible Future RIRs
Local Internet Registries
NIR National Internet Registry
Delegated Registry
LIR
LIR
LIR
ISP
ISP
ISP
ISP
ISP
ISP
ISP
Internet Service Providers
EU
EU
EU
EU
EU
EU
EU
EU
EU
EU
EU
EU
End Users

Figure 1: Internet Registry system structure

6.2 ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) (http://www.icann.org) is a technical co-ordination body for the Internet and has authority over all number and domain name spaces used in the Internet. ICANN was created in October 1998 by a broad coalition of the Internet's business, technical, academic and user communities. It assumed responsibility for a set of technical functions that were previously performed under US government contract by IANA and other groups.

ICANN co-ordinates the assignment of the three identifiers listed below that must be globally unique for the Internet to function.

- Internet domain names
- IP Address numbers - ICANN allocates public Internet address space to RIRs
- Protocol parameters and port numbers

In addition, ICANN co-ordinates the stable operation of the Internet's root server system.

6.3 Address Supporting Organisation (ASO)

The ASO is run by the Address Council of nine members, with three members from each of the three Regional Internet Registries (RIRs). The work is governed by a Memorandum of Understanding (MoU) which defines the functions as:

- Definition of global policies for the distribution and registration of Internet address space (currently IPv4 and IPv6);
- Definition of global policies for the distribution and registration of identifiers used in Internet inter-domain routing (currently BGP autonomous system numbers)
- Definition of global policies concerning the part of the DNS name space which is derived from the Internet address space and the inter-domain routing identifiers (currently in-addr.arpa and ip6.int).

6.4 Regional Internet Registry (RIR)

The Regional Internet Registries have operated for some years under the authority of IANA, but are now recognised within the ICANN framework.

There are currently five RIRs: RIPE NCC, ARIN, APNIC, AfriNIC and LACNIC. Each RIR serves and represents its members for specific geographic areas as identified in the table below.

Each RIR may have different local structures organised to serve the Internet community. For example, APNIC supports NIRs in addition to LIRs, and similarly ARIN supports DRs.

The RIR will be responsible for the allocation of IP address space to all the LIRs/NIRs it serves, and registering those allocations and subsequent assignments in a publicly-available "who-is" database.

RIR	Areas Served	Reference
RIPE NCC (Réseaux IP Européens Network Coordination Centre)	Europe The Middle East Central Asia African countries located north of the Equator	http://www.ripe.net
ARIN (American Registry for Internet Numbers)	North America South America Caribbean African countries located south of the Equator	http://www.arin.net
APNIC (Asia Pacific Network Information Centre)	Entire Asia Pacific region, including 62 economies/countries/regions in South and Central Asia, South-East Asia, Indochina and Oceania	http://www.apnic.net
AfriNIC	To serve the African region	http://www.afrinic.org

RIR	Areas Served	Reference
(African Network Information Centre)	Start-up operations day not yet known	
LACNIC (Latin American Continent Network Information Centre)	To serve the Latin American region Start-up operations day not yet known	http://www.lacnic.org

Table 1: RIRs and their served areas

6.5 National Internet Registries

NIRs are only operated and supported in the APNIC organisational structure.

NIRs provide registration and allocation services for members (generally ISPs) organised on a national basis. NIRs operate in Japan (JPNIC), Korea (KRNIC), China (CNNIC), Taiwan (TWNIC) and in Indonesia (APJII). All of these NIRs operate within the APNIC policy framework and receive their resources directly from APNIC.

6.6 Delegated Registries

Delegated Registries are only operated and supported in the ARIN organisational structure, and are equivalent in functionality to the NIRs for APNIC.

There are two Delegated Registries in the ARIN region, which are as follows: -

- RNP - Brazilian Registry
- NIC-Mexico - Mexican Registry

6.7 Local Internet Registries

LIRs are established under the authority of an RIR.

The LIR holds allocations of address space for assignment to end-users. LIRs are typically operated by Internet Service Providers (ISP) and serve the customers of those ISPs as well as the customers of smaller ISPs who are connected to the rest of Internet through the larger ISP. Other organisations such as large international Enterprises can also operate as an LIR.

In the ARIN region, the term ISP is used in place of the term "LIR".

6.8 End Users

End users are part of the IR system to the extent that they need to conform to the policies and processes associated with this system.

Addressing and deployment plans must be documented and submitted by the end user to their applicable LIR/NIR/DR in accordance with the respective address request policy/process of that LIR/NIR. Additional information may be required from the end user in order for the IR to make any necessary address assignment decisions.

An appropriate LIR or NIR/DR should be selected by the end user to permit aggregation of routing information to be optimised and most efficiently deployed.

End users will be expected to plan their networks to use a minimum amount of address space.

Note 1: LIRs are typically operated by ISPs, with each ISP allocated a specific range of addresses for assignment to its end users. Hence, changing ISPs will require the end user to renumber their networks into the address space of the new ISP.

Note 2: Address assignments are made for specific purposes and should not be sub-allocated or sub-assigned other than as documented with IR by the end user. Any change to the registered deployment plans must be notified by the end user to their assigning IR.

Note 3: End users should adopt techniques such as Variable Length Subnet Masking (VLSM) and use appropriate technologies that ensure their assigned address space is used efficiently.

7 Annex B: RIR Public IP address request web links

Reference	Notes
http://www.ripe.net/ripencc/new-mem	Contains useful information on how to become a member of the RIPE NCC and how to request address space
http://www.ripe.net/ripencc/mem-services/registration/index.html	RIPE registration services/templates (e.g. ripe-141) associated with submitting address space requirements to a LIR.
http://ripe.net/ripe/docs/ripe-141.html	Note: LIRs do not have to use ripe-141 for their internal operations, but if a significant amount of addresses is required, then the LIR will have to submit the request to the NCC for a second opinion. In this case the request needs to be in a specific format that is described in document ripe-141.
http://ripe.net/ripe/docs/ripe-185.html	European IP Address Space Request Form. Identifies the information that will be required by the LIR when address space is requested by the end user. Further details on these requirements can be found in [1]

Table 2: RIPE NCC IP address space request web links

Reference	Notes
http://www.arin.net/regserv.html	Registration Services
http://www.arin.net/regserv/initial-isp.html	ISP Guidelines for Requesting Initial IP Address Space
http://www.arin.net/regserv/ip-assignment.html	Internet Protocol (IP) Assignment Guidelines for End Users

Table 3: ARIN IP address space request web links

Reference	Notes
http://www.apnic.net/registration.html	APNIC Registration Services
http://www.apnic.net/apnic-bin/isp-address-request.pl http://ftp.apnic.net/apnic/docs/isp-address-request	To request address space allocation as an APNIC member Text version of above, i.e. APNIC-065 - APNIC Internet Service Provider Internet Address Request Form
http://www.apnic.net/membersteps.html	Step by step guide to the membership application procedure
http://www.apnic.net/docs/add-manage-policy.html	APNIC-076: Policies for address space management in the Asia Pacific region
http://www.apnic.net/apnic-bin/second-opinion-request.pl	Second opinion request form for customer assignments.
http://www.apnic.net/faq/awfaq.html	Assignment Window Q&A

Table 4: APNIC IP address space request web links

Information on AfriNIC and APNIC will be added in a future version of the document.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
Draft A	21st June 2000	First Draft	IREG	Kim Fullbrook / Telefonica-O2
Issue 1.0	11th July 2000	Incorporated various comments from RIPE NCC and feedback received at GPRSWP #10	IREG	Kim Fullbrook / Telefonica-O2
Issue 1.1	21st July 2000	• Amendment to title • New references [9] - [5] • Document scope incorporated within a new 'Introduction' section • Section 5.1: New Note 1 • Section 5.2: Amendment to Note 2	IREG	Kim Fullbrook / Telefonica-O2
Issue 1.2	15 August 2000	Various comments from APNIC, ARIN and RIPE NCC: • Section 1: Note to [3] and [4]; new [12] - [18] • Section 3: Various amendments to entire section • Section 4: New Figure 1, various amendments to entire section; New Sections 4.4 and 4.5 • Section 5: Various amendments to most of this section • Section 6: Minor amendments to section 6.3	IREG	Kim Fullbrook / Telefonica-O2
Issue 1.3	31st August 2000	New meeting document number GPRS 54/00 instead of GPRS 46/00	IREG	Kim Fullbrook / Telefonica-O2
Rev 0	5th September 2000	Conversion of GPRS Doc 54/00 to IREG 062/00	IREG	Kim Fullbrook / Telefonica-O2
Rev 1	6th September 2000	Changes to: • Title • Section 3.1: Note 2 deleted as no longer relevant • Section 6.3: Changes to Item 4; Note 5 deleted,	IREG	Kim Fullbrook / Telefonica-O2
Rev 0 PRD IR.40 vsn 3.0.1	9th Oct 2000	The following changes were made: • New meeting document number GPRS Doc 060/00; assigned as PRD IR.40 (proposed vsn 3.0.1) • Corrections to dates in 'Document History' • Section 3.1, new Note 3: Contact details for RIRs to notify GSMA of proposed changes to this document.	IREG	Kim Fullbrook / Telefonica-O2

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
PRD IR.40 vsn 3.0.2	21 May 2001	Document structure completely re-organised, with new section added for IP addressing for Mobile Terminals • Internet Registry System overview moved to new Annex A • RIR address request web links moved to new Annex B • Addition of new IP addressing guidelines for mobile terminals • New Annex C: IP addressing factors for consideration when designing guidelines for GPRS/UMTS-based services using IPv4 addressing	IREG	Kim Fullbrook / Telefonica-O2
PRD IR.40 vsn 3.0.3	7 Aug 2001	Document updated to reflect comments received from RIRs for sections related to "IP addressing for mobile terminals". General changes to most of document to help clarify and rationalise the guidelines. Examples of network designs for GPRS services moved from document body to a New Annex D	IREG	Kim Fullbrook / Telefonica-O2
PRD IR.40 vsn 3.0.4	10 Aug 2001	Minor updates to document as result of comments received on v3.0.3 at Packet#3 meeting on 8 Aug 2001.	IREG	Kim Fullbrook / Telefonica-O2
v3.0.5	16 Aug 2001	Following sections updated with review comments received from PacketWP: • Changed text to provide further clarification • 5.5.3, Item 2.2 change to service title • 5.6 Changed text to provide further clarification • New reference documents: [10], [11], [12] & [31] • 10.1 Correction to state 3.4x10^{38} addresses • 10.2.2 Changes to item 3 • 10.2.3 Item 1 details on NAT limitations moved out to a later section specifically on NAT; Item 2 - Changed text for further clarification • 10.4 deleted " only one PDP context per MT is typically supported" • 10.6 Changed text to provide further clarification	IREG	Kim Fullbrook / Telefonica-O2
Proposed v3.1.0	17 Aug 2001	Document submitted to IREG for approval as proposed version 3.1.0 with following minor text changes from v3.0.5: • Section 1.4 - Note 3, typo correction for info@gsmworld.com • Section 2.3 - Correction to date of RIPE meeting • Section 8.3 - clarification to text describing ASO members.	IREG	Kim Fullbrook / Telefonica-O2

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
v3.1.0	21 Sept 2001	Document approved at IREG #41 with a document classification of "Unrestricted - Public"	IREG	Kim Fullbrook / Telefonica-O2
v4.0.0	30 March 2007	Major round of updates to support needs of IPX network: • Include non-mobile networks and terminals • Made clear that addresses cannot duplicate any on Internet • Clarify when ASNs are required • Include rules for notifying IPX Networks about IP address ranges used • Update terminology to be consistent with other IPX documents • Made clear that addresses cannot duplicate any on Internet	IREG	Kim Fullbrook / Telefonica-O2
5.0	22 October 2010	New template applied, IPv6 information updated and other numerous minor fixes.	Packet #46	Massimo Chiavacci / Telecom Italia Sparkle
6.0	16 March 2011	Submitted to DAG and EMC for approval	Packet #48 IREG #60 DAG #79	Massimo Chiavacci / Telecom Italia Sparkle
7.0	16 April 2012	Submitted to DAG and EMC for approval	DAG #92	Massimo Chiavacci / Telecom Italia Sparkle
8.0	12 Jan 2015	Incorporation of CR1001 approved in PSMC#118 meeting (12 Nov 2013)	PSMC	Massimo Chiavacci / Telecom Italia Sparkle

Other Information

Type	Description
Document Owner	IREG Packet
Editor / Company	Massimo Chiavacci

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.