ETSI TR 129 941 V17.1.0 (2022-05)

5G;
Guidelines on Port Allocation for New 3GPP Interfaces
(3GPP TR 29.941 version 17.1.0 Release 17)

Reference
DTR/TSGC-0429941vh10

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

3GPP TR 29.835 [2] studies Port Number Allocation Alternatives for New 3GPP Interfaces. This specification documents the outcome of the study by providing the guidelines for addressing the problem.

1 Scope

IETF has indicated to 3GPP that future IANA port number assignment requests for protocol only used inside 3GPP networks will be likely rejected except if there is a strong justification for it. The present document provides guidelines for resolving the problem with allocating port numbers for new 3GPP interfaces, as an alternative to IANA assigned port numbers.

Starting from 3GPP Rel-17, any 3GPP working group can rely on these guidelines when defining new interfaces, which require new default port number allocation.

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 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 29.835: "Study on Port Number Allocation Alternatives for New 3GPP Interfaces".

[3] IETF RFC 793: "Transmission Control Protocol".

[4] IETF RFC 1078: "TCP Port Service Multiplexer (TCPMUX)"

[5] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

[6] IETF RFC 4960: "Stream Control Transmission Protocol".

[7] IETF RFC 5226: "Guidelines for Writing an IANA Considerations clause in RFCs".

[8] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[9] IETF RFC 6083: "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[10] IETF RFC 6335: "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry".

[11] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[12] IETF RFC 6762: "Multicast DNS".

[13] IETF RFC 6763: "DNS-Based Service Discovery".

[14] IETF RFC 7301: "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension".

[15] IETF RFC 7605: "Recommendations on Using Assigned Transport Port Numbers".

[16] IETF RFC 7805: "Moving Outdated TCP Extensions and TCP-Related Documents to Historic or Informational Status".

[17] IETF RFC 8126: "Guidelines for Writing an IANA Considerations Clause in RFCs".

[18] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[19] IETF RFC 1035: "Domain Names – Implementation and specification".

[20] 3GPP TS 29.641: "3GPP registry for Service Names and Port Numbers".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Symbols

Void.3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

4 Selected Solutions

4.1 General

Since 2015, IANA had gradually warned 3GPP that a solution should be found to avoid port assignments for protocols only used in 3GPP networks (and not on the public Internet). The last requests were exceptionally granted by the Internet Engineering Steering Group (IESG) only at the conditions that it was the last one(s). Now, it is clear that application for a new port will not be granted without a strong justification and only if:

- The recommendations given in IETF RFC 7605 [3] have been carefully followed (see Annex C.4);
- It is proved that there is no other solution than port assignment for service port discovery.

The IETF RFC 7605 [3] provides recommendations to designers of application and service protocols on how to use the transport protocol port number space and when to request a port assignment from IANA. In this document, it is reminded that:

> IANA assigns port numbers so that Internet endpoints do not need pairwise, explicit coordination of the meaning of their port numbers. This is the primary reason for requesting port number assignment by IANA: to have a common agreement between all endpoints on the Internet as to the default meaning of a port number, which provides the endpoints with a default port number for a particular protocol or service.

It is also clarified that:

> Port numbers can also be used for other purposes. Assigned port numbers can simplify end-system configuration, so that individual installations do not need to coordinate their use of arbitrary port numbers. Such assignments may also have the effect of simplifying firewall management, so that a single, fixed firewall configuration can either permit or deny a service that uses the assigned ports.

In typical roaming scenarios, three or more administrative domains can be crossed: visited and home PLMN, one or more IPX providers connecting together via an IPX peering point for traffic exchange between PLMNs. Operators and service providers may even decide to rely on the global connectivity provided by the public Internet for interconnection.

As roaming implies the need for a global configuration of the port to use for a particular protocol, it is strongly recommended for 3GPP to apply to IANA for assigned service name and port number for any protocol potentially supported by roaming interfaces when no other service port discovery (e.g. DNS-based solutions) is applicable.

In non-roaming scenarios, a given interface can still cross multiple domains. For instance, RAN can be supported by an IP-based network distinct from the one supporting the core network even if both are under the same PLMN Another example is the RAN sharing case (i.e. same RAN is used by multiple PLMN's CN) in which the interface between RAN and CN also crosses multiple administrative domains. In such a case, it is also strongly recommended for 3GPP to apply to IANA for assigned service name and port number for any protocol potentially supported by inter-domain interfaces when no other service port discovery (e.g. DNS-based solutions) is applicable.

For 3GPP interfaces that would be used only in intra-domain scenarios, alternative solutions to IANA assigned port numbers are required.

Table 4.1-1 provides brief summary of the identified alternative solutions.

Table 4.1-1: Solution summary

Solution	Port allocation method	Applicable transport layer protocol	Suitable (NOTE)		Comments
			Inter-domain	Intra-domain	
#1	Un-assigned	UDP, TCP, SCTP	Part	Yes	**DNS infrastructure based solution (DNS-SD)** The port number is selected dynamically by the interface application locally. DNS server is kept up-to-date with the records like hostnames, IP addresses, locally assigned port numbers, service names supported, etc. for application clients to discover using DNS PTR query. This solution is suitable for inter-domain scenario with certain limitations. Inter-PLMN service discovery can be provided using operator DNS servers connected to the IPX, the private, inter-operator IP backbone network. But if the traffic related to the discovered application/interface needs to be controlled, this will not work as the destination port is unknown to security gateway/firewall.
#2	Un-assigned	UDP, TCP, SCTP	Part	Yes	**DNS infrastructure based solution (DNS SRV)** This is an alternative to solution#1 in which there is only one logical instance of service <Service> and all clients are expected to use that one logical instance. Application clients can discover the server end point details using DNS SRV query. Requires DNS infrastructure application clients that support DNS queries. This solution is suitable for inter-domain scenario with certain limitations. Inter-PLMN service discovery can be provided using operator DNS servers connected to the IPX, the private, inter-operator IP backbone network operator DNS servers connected to the IPX, the private, inter-operator IP backbone network. But if the traffic related to the discovered application/interface needs to be controlled, this will not work as the destination port is unknown to security gateway/firewall.
#3	Un-assigned	UDP, TCP, SCTP	No	Yes	**Multicast DNS based solution (mDNS)** Instead of sending the DNS query to a unicast DNS server, the query is sent to a link-local multicast address. The nodes are implemented with mDNS resolver and responder. The node supporting the service responds to the mDNS query. This solution is not suitable for Inter-domain scenario, because multicast is restricted to local link.
#4	Un-assigned	UDP, TCP, SCTP	Part	Yes	**Unicast DNS based solution (uDNS)** Similar to Solution#3 with only difference that the mDNS query is sent to a pre-configured IP address instead of the link-local multicast address. This solution is suitable for inter-domain scenario with certain limitations. If the IP address can be dynamically resolved, e.g. using an FQDN to retrieve an IP from the DNS and inter-domain interface is secured it can be used for Inter-domain scenario. But if DNS has to be used, then this solution has less value than the Solution#1 and the Solution#2.
#5	Fixed	SCTP	Yes	Yes	**SCTP MUX based solution using standardized PPID (SCTP MUX)** All new interfaces/applications use a common standardized port number and unique standardized SCTP Payload Protocol Identifier (PPID). The server side implements an SCTP multiplexer that distributes the traffic to intended applications based on PPID value. This solution is suitable for Inter-domain scenario.

#6	Fixed	UDP, TCP, SCTP	Part	Yes	**3GPP allocated port number solution (3GPP)** IANA does not assign any port number from the Dynamic/Private range [49152 - 65535]. If 3GPP standardizes a subrange [65400 - 65500] from this range for 3GPP interfaces and starts allocating port numbers, this may cause port number clash during the actual deployments. This solution is suitable for inter-domain scenario with certain limitations. The limitation may be mitigated if firewall implementations will start supporting 3GPP allocated port number range.
#7	Fixed	UDP, TCP, SCTP	No	Yes	**OAM allocated port number solution (OAM)** Operator becomes responsible for allocating port numbers via OAM from either the User range [1024-49151] or from the Dynamic/Private range [49152 - 65535]. Operator is also responsible for avoiding port number clashes. This solution is not suitable for Inter-domain scenario.
#8	Un-assigned	UDP, TCP, SCTP	Yes	Yes	**Port Registration and Retrieval via NRF based solution (NRF)** NRF is enhanced to support the registration of port number information and the retrieval of the port number by an application client. An application client can use the NF Discovery service to retrieve the port number of a specific protocol, by indicating the protocol type. On client side, this solution requires support of SBI interface to NRF. On server side, NRF will need to support port number registration and discovery for non-SBI interfaces/applications. If the traffic related to the discovered application/interface needs to be controlled, this will not work as the destination port is unknown for security gateway/firewall. This solution is suitable for inter-domain scenario.
NOTE:	'Part' indicates the solution is partially suitable for the inter-domain scenario and certain limitations need to be considered. For instance, with inter-domain scenario, it is not possible to prevent firewalls/security gateways located between two domains from restricting outgoing/incoming network traffic for a specific port not assigned by IANA. It is therefore strongly recommended for 3GPP to apply to IANA for assigned service name and port number.				

Annex A on this specification summarizes IANA port allocation policy.

Annexes B.1 and B.2 provide essential background information and also how IANA classifies different port number ranges. Annex B.3 explains relations between the services and port numbers.

Annex C explains IANA procedures for Service Name and Port Number registry management.

3GPP procedures for Service Name and Port Number registry management are specified in 3GPP TS 29.641 [20].

4.2 DNS based solutions#1-4

4.2.1 General

DNS procedures can be used to discover a service or a service instance in a given domain using PTR (see IETF RFC 1035 [19]) and/or SRV resource record lookups.

The PTR and SRV lookup are performed on the name:

<Service>.<Domain>

The <Service> portion consists of a pair of DNS labels separated by a dot, following the convention already established for SRV records (IETF RFC 2782 [8]).

The first label of the pair is an underscore character followed by an IANA registered Service Name (IETF RFC 6335 [10]).

NOTE 1: Service names are assigned on a "first come, first served" basis, as described in clause 8.1 of IETF RFC 6335 [10]. There is no substantive review of the request, other than to ensure that it is well-formed and doesn't duplicate an existing assignment.

For new service names registered by 3GPP, the Service Name should start with "3gpp-", followed by a name identifying the application protocol defined by 3GPP. This name should be the acronym used to identify the protocol in 3GPP specifications.

The second label is either "_tcp" (for application protocols that run over TCP) or "_udp" (for application protocols that run over any transport protocol other than TCP, e.g. SCTP).

EXAMPLE: IANA-assigned Service Name for the SCTP application W1AP supporting the service provided by the W1 interface defined by 3GPP:

"_3gpp-w1ap._udp"

The <Domain> portion specifies the DNS subdomain within which those names are registered. It may be:

- "local." in the absence of any conventional Unicast DNS server, meaning "link-local Multicast DNS" (see IETF RFC 6762 [12]);
- A subdomain of any conventional Unicast DNS domain name operated by the operator, e.g. "example.com";
- A subdomain of "mnc<MNC>.mcc<MCC>.3gppnetwork.org" for service discovery across PLMNs (e.g. in roaming cases).

When relying on a DNS infrastructure, the operators are responsible for:

- The selection of the subdomain name in which the Service Instance Names are registered, and
- The provisioning of the authoritative DNS server of this subdomain with the corresponding PTR, SRV, TXT and A/AAAA records used to discover and contact the target nodes.

4.2.2 Solution#1: DNS-SD based solution

4.2.2.1 General

The DNS-based Service Discovery (DNS-SD) (see IETF RFC 6763 [13]) allows clients to discover one or multiple nodes in the network supporting a specific service, the application protocol and the transport protocol used for accessing the service, using standard DNS queries sent to a conventional unicast DNS server available in the network.

In 3GPP networks, any IP-based interface can been considered as a specific service provided by a node on a given IP address and an IP port number. By identifying an interface with a unique service name, the DNS-based Service Discovery (DNS-SD) can be used by clients to discover the IP port number used by a remote node for a given interface.

In this proposed solution, it is assumed that a conventional unicast DNS server is available in the network. When a node is activated in the network, the service application is assigned with any available port from either the User Port number range [1024-49151] or the Dynamic/Private Port range [49152 - 65535]. The DNS server of the domain needs to be updated with the node's DNS records (configured hostnames, IP addresses, locally assigned port numbers, service names supported, etc.). This update can be done manually by the network administrator or done automatically by the node with mechanisms such as Dynamic DNS (DDNS).

The name of the service supported by a given 3GPP interface is registered to IANA. It consists of a pair of DNS labels separated by a dot, following the convention already established for SRV records (IETF RFC 2782 [5]).

- The first label of the pair is an underscore character followed by an IANA registered Service Name (IETF RFC 6335 [10]).
- The second label is either "_tcp" (for application protocols that run over TCP) or "_udp" (for application protocols that run over any transport protocol other than TCP).

Service names are assigned by IANA on a "first come, first served" basis, as described in Clause 8.1 of IETF RFC 6335 [10]. There is no substantive review of the request, other than to ensure that it is well-formed and doesn't duplicate an existing assignment. The assignment of a standard service name is therefore straightforward.

4.2.2.2 Detailed description

The proposed solution is based on the following assumptions:

- A listening port is locally assigned to a service application hosted in a node;
- The DNS server of the domain is updated with the resource records of the service application (configured hostnames, node's IP addresses, locally assigned port numbers, service names supported, etc.);
- The service application client implements a DNS resolver.

To set-up a transport connection with the application server, the following steps apply:

1 The client is configured with an IANA registered service name <Service> identifying a specific service and the application protocol used to support the service.

2 To discover the list of available service instances supporting the service <Service> in the domain <Domain>, the client performs a DNS-SD PTR lookup (see IETF RFC 6763 [13]) for the name:

<Service>.<Domain>

NOTE 1: the domain name in which the service instances have to be discovered is either configured in the client or derived from service-specific information e.g. IMSI/SUPI, PLMN-Id, etc.3 The DNS query is sent to the conventional unicast DNS server.

4 The result of the DNS-SD's PTR lookup is a set of zero or more PTR records giving the list of available instances in the form of Service Instance Names:

Service Instance Name = <Instance>.<Service>.<Domain>

In which the <Instance> portion is a user-friendly name, consisting of arbitrary Net-Unicode text, as defined in IETF RFC 6763 [13].

When at least one PTR record is present in the DNS response, the following additional records are included in the DNS response:

- The SRV record(s) for each Service Instance Name listed in the PTR record(s), providing the port number and target host name of the Service Instance Name.
- All address records (type "A" and "AAAA") for the target host name listed in the SRV record(s).
- The TXT record(s) containing a single zero octet (i.e., a single empty string.) for each Service Instance Name named in the PTR record(s).

NOTE 2: DNS clients are able of functioning correctly with DNS servers (and Multicast DNS Responders) that fail to generate these additional records automatically, by issuing subsequent queries for any further record(s) they require.

NOTE 3: As described in IETF RFC 6763 [13], TXT record(s) containing a single zero octet indicate that there is no additional data for the given Service Instance

5 In the event that more than one SRV is returned, the client shall correctly interpret the priority and weight fields to select the target node i.e.:

- Lower-numbered priority instances should be used in preference to higher-numbered priority instances, and
- Instances with equal priority should be selected randomly in proportion to their relative weights.

NOTE 4: It is recommended to give the same weight to all the instances with the same priority.

6 The client can set up connection(s) with the remote node(s) using the IP address(es) and port number(s) retrieved from the DNS server and then application data can be exchanged between the client and the server.

4.2.2.3 Pros and cons

Pros:

- Port numbers are locally assigned in the node supporting the interface applications.
- Limit the need for manual configuration.
- Leveraging on a proven DNS infrastructure and mature technology.
- The "_tcp" and "_udp" subdomains can be delegated to a dedicated DNS server.

Cons:

- Rely on the availability of a DNS infrastructure.
- 3GPP nodes need to implement a DNS resolver in order to discover interfaces supported by other nodes.
- The discovery mechanism implies additional signalling before setting up the connection between nodes.

4.2.3 Solution#2: Service discovery using DNS SRV records

4.2.3.1 General

This is an alternative to solution#1 in which there is only one logical instance of service <Service> and all clients are expected to use that one logical instance. Of course, the logical instance can be load-shared across multiple nodes, but all the nodes provide an equivalent service.

In this proposed solution, to discover the list of available service instances, the client performs a simple SRV lookup (see IETF RFC 2782 [5]) instead of a PTR lookup in solution#1:

The result of the SRV lookup is SRV record(s) providing the port number and target host name of the nodes supporting the service. All address records (type "A" and "AAAA") for the target host name listed in the SRV record are also provided.

4.2.3.2 Detailed description

The proposed solution is based on the following assumptions:

- A listening port is locally assigned to a service application hosted in a node;
- The DNS server of the domain is updated with the resource records of the service application (configured hostnames, node's IP addresses, locally assigned port numbers, service names supported, etc.);
- The service application client implements a DNS resolver.

To set-up a transport connection with the application server, the following steps apply:

1 The client is configured with an IANA registered service name <Service> identifying a specific service and the application protocol used to support the service.

2 To discover the list of available service instances supporting the service <Service> in the domain <Domain>, the client performs a DNS SRV lookup (see IETF RFC 6763 [13]) for the name:

<Service>.<Domain>

NOTE 1: the domain name in which the service instances have to be discovered is either configured in the client or derived from service-specific information e.g. IMSI/SUPI, PLMN-Id, etc. See 3GPP TS 23.003.

3 The DNS query is sent to the conventional unicast DNS server.

4 The result of the DNS SRV lookup is a set of zero or more SRV records providing the port number and host name of the target nodes supporting the service. All address records (type "A" and "AAAA") for the target host name listed in the SRV record are also provided:

NOTE 2: DNS clients are able of functioning correctly with DNS servers that fail to generate these additional A/AAAA records automatically, by issuing subsequent queries for any further record(s) they require.

5 In the event that more than one SRV is returned, the client shall correctly interpret the priority and weight fields to select the target node i.e.:

- Lower-numbered priority instances should be used in preference to higher-numbered priority instances, and
- Instances with equal priority should be selected randomly in proportion to their relative weights.

NOTE 3: It is recommended to give the same weight to all the instances with the same priority.

6 The client can set up connection(s) with the remote node(s) using the IP address(es) and port number(s) retrieved from the DNS server and then application data can be exchanged between the client and the server.

4.2.3.3 Pros and cons

Pros:

- Port numbers are locally assigned in the node supporting the interface applications.
- Limit the need for manual configuration.
- Leveraging on a proven DNS infrastructure and mature technology.
- The "_tcp" and "_udp" subdomains can be delegated to a dedicated DNS server.

Cons:

- Rely on the availability of a DNS infrastructure.
- 3GPP nodes need to implement a DNS resolver in order to discover interfaces supported by other nodes.
- The discovery mechanism implies additional signalling before setting up the connection between nodes.
- It is not possible to discriminate multiple service instances. All clients are expected to use that the same logical instance.

4.2.4 Solution#3: Use of multicast address on local link (mDNS)

4.2.4.1 General

This is an alternative to solution#1 and solution#2 in the absence of DNS server in the domain.

Multicast DNS (mDNS) (see IETF RFC 6762 [12]) provides the ability to perform DNS-like operations on the local link in the absence of any conventional Unicast DNS server. DNS queries are multicasted on a local link and any node receiving the query responds with a unicast packet directed back to the querier if it supports the service requested by the querier. The response can also be multicasted on local link, all the nodes on this local link being updated at the same time.

Multicast DNS can provide zero-configuration operation -- just connect a DNS-SD/mDNS device, and its services are advertised on the local link with no further user interaction.

4.2.4.2 Detailed description

The proposed solution is based on the following assumptions:

- A listening port is locally assigned to a service application hosted in a node;
- The application server implements a Multicast DNS responder listening for DNS queries on the UDP port 5353
- the application client implements either a full Multicast DNS resolver sending DNS queries from the UDP source port 5353 or a minimal Multicast DNS resolver (light enhancement of a legacy DNS resolver) sending DNS queries from high-numbered ephemeral UDP source port.

To set-up a transport connection with the SCTP application server, the following steps apply:

1 The client is configured with an IANA registered service name <Service> identifying a specific service and the application protocol used to support the service.

2 To discover the list of available service instances supporting the service <Service> on the local link, the client performs a DNS PRT lookup (solution#1, see clause 4.2.2.2) or SRV lookup (solution#2, see clause 4.2.3.2) for the name:

<Service>.local.

3 DNS queries are sent to the mDNS IPv4 link-local multicast address 224.0.0.251 or mDNS IPv6 link-local multicast address FF02::FB, to UDP destination port 5353 and using as UDP source port either:

- port 5353 if the client supports a fully compliant mDNS resolver; or
- a high-numbered ephemeral UDP source port other than port 5353, if the client supports minimal Multicast DNS resolver

NOTE 1: It is recommended to use the mDNS IPv4 link-local multicast address only if IPv6 is not not avalaible.

4 A node receiving the mDNS request and supporting the desired service shall provide in the response its own DNS records as described in clauses 4.2.2.2 (solution#1) and 4.2.3.2 (solution#2).

5 The DNS response is either unicast to the source IP address of the DNS querier, or the response is multicast on the local link.

NOTE 2: DNS querier can asked for unicast response by setting the unicast-response bit, the top bit in the class field of a DNS question.

6 The client can set up connection(s) with the remote node(s) using the IP address(es) and port number(s) retrieved from the DNS server and then application data can be exchanged between the client and the server.

4.2.4.3 Pros and cons

Pros:

- Port numbers are locally assigned in the node supporting the interface applications.
- Little or no administration or configuration to set the nodes up
- Work when no DNS infrastructure is present
- Can be used also during DNS infrastructure failures

Cons:

- All the nodes have to be on the same logical local network.
- (Minimal) Multicast DNS resolvers and Multicast DNS responders have to be implemented in the nodes.
- Additional traffic with multicast queries and responses.
- The discovery mechanism implies additional signalling before setting up the connection between nodes.

4.2.5 Solution#4: Direct unicast DNS queries to the target node (uDNS)

4.2.5.1 General

This is an alternative to solution#3 when there is no DNS server and the target node can be outside the local link.

In this proposed solution, instead of relying on Multicast DNS queries sent on the local link, the client sends its DNS query via unicast directly to the node, using the destination port 5353. The IP address of the target node is discovered by configuration.

The node receiving the unicast DNS query and supporting the desired service answers via with a unicast packet directed back to the client, using the source IP address and port of the received DNS query.

4.2.5.2 Detailed description

The proposed solution is based on the following assumptions:

- A listening port is locally assigned to a service application hosted in a node;
- The application server implements a Multicast DNS responder listening for DNS queries on the UDP port 5353
- the application client implements either a full Multicast DNS resolver sending DNS queries from the UDP source port 5353 or a minimal Multicast DNS resolver (light enhancement of a legacy DNS resolver) sending DNS queries from high-numbered ephemeral UDP source port.

To set-up a transport connection with the application server, the following steps apply:

1 The client is configured with:
   - An IANA registered service name <Service> identifying a specific service and the application protocol used to support the service;
   - The IP address of the target node.

2 To discover the list of available service instances supporting the service <Service> on the local link, the client performs a DNS PRT lookup (solution#1, see clause 4.2.2.2) or SRV lookup (solution#2, see clause 4.2.3.2) for the name:

   <Service>.local.

3 DNS queries are sent to the unicast IP address of the target node configured in the client, to UDP destination port 5353 and using as UDP source port either:
   - Port 5353 if the client supports a fully compliant mDNS resolver; or
   - High-numbered ephemeral UDP source port other than port 5353, if the client supports minimal Multicast DNS resolver

NOTE: It is recommended to use the mDNS IPv4 link-local multicast address only if IPv6 is not not avalaible.

4 A node receiving the mDNS request and supporting the desired service will provide in the response its own DNS records as described in clause 4.2.2.2 (solution#1) and 4.2.3.2 (solution#2).

5 The DNS response is unicast to the source IP address of the DNS querier.

6 The client can set up connection(s) with the remote node(s) using the IP address(es) and port number(s) retrieved from the DNS server and then application data can be exchanged between the client and the server.

4.2.5.3 Pros and cons

Pros:

- Port numbers are locally assigned in the node supporting the interface applications.
- Minimal administration or configuration to set the nodes up
- Work when no DNS infrastructure is present
- Can be used also during DNS infrastructure failures

Cons:

- (Minimal) Multicast DNS resolvers and Multicast DNS responders have to be implemented in the nodes.
- The discovery mechanism implies additional signalling before setting up the connection between nodes.
- The signalling between the client and the target node outside the local link shall be protected with confidentiality, integrity and replay protection, using for instance IPsec.

4.2.6 Guidelines for DNS based solutions#1-4

It is beneficial to use solution#1 (DNS-SD) and solution#2 (DNS SRV), if DNS infrastructure is readily available and if the clients support DNS-based discovery mechanisms.

When relying on a DNS infrastructure, the <Domain> portion of the Service Instance Name in which the Service Instance Names are registered depends on the nature of the interface on which the transport protocol is used:

- If the interface is only used in an intra-domain scenario, the operators are free to use any suitable subdomain of the domain for which the operator is responsible, e.g. "example.com";
- If the interface may be used in an inter-domain scenario, the <Domain> portion must be a subdomain of the domain "mnc<MNC>.mcc<MCC>.3gppnetwork.org", e.g.:
  - "epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" when the DNS server is located in the 3GPP core network;
  - "ran.mnc<MNC>.mcc<MCC>.3gppnetwork.org" when the DNS server is located in the 3GPP radio access network.

Operators are responsible for the provisioning of the authoritative DNS server of this subdomain with the corresponding resource records (PTR, SRV, TXT and A/AAAA) used to discover and contact the service instances.

It is beneficial to use solution#3 (mDNS), if DNS infrastructure is not available and the clients support mDNS queries. Solution#3 however is not suitable for the inter-domain scenario, because multicast is restricted to the local link.

It is beneficial to use solution#4 (uDNS), if there is no DNS server, the target node can be outside the local link and the clients support unicast DNS queries. Solution#4 can also be used for the inter-domain scenario, but that requires DNS infrastructure. If DNS has to be used, then solution#4 has less value than solution#1 and solution#2.

NOTE: For inter-domain scenario, it is not possible to prevent firewalls/security gateways located between two domains from restricting outgoing/incoming network traffic for a specific port not assigned by IANA. It is therefore strongly recommended for 3GPP to apply to IANA for assigned service name and port number.

4.3 SCTP based solution#5 – SCTP Multiplexer (Port)

4.3.1 General

The TCP Port Service Multiplexer (TCPMUX) is defined in IETF RFC 1078 [4]. The specification describes a multiplexing service that may be accessed with a network protocol to contact any one of a number of available TCP services of a host on a single, well-known port number.

The same principle is applied to SCTP applications.

An SCTP (IETF RFC 4960 [6]) packet is composed of a common header and chunks.

The SCTP common header contains:

- The SCTP Source Port Number that can be used by the receiver in combination with the source IP address, the SCTP destination port, and possibly the destination IP address to identify the association to which this packet belongs.
- The SCTP Destination Port Number that can be used by the receiving host to de-multiplex the SCTP packet to the correct receiving endpoint/application.

A SCTP chunk represents a protocol message, which can be used by the protocol itself or can contain user data. User data are contained in DATA chunks that include a Payload Protocol Identifier. The Payload Protocol Identifier is used to identify the application which uses the services of SCTP.

As it is contained in each DATA chunk, the Payload Protocol Identifier identifies the protocol being carried over SCTP independently of the port numbers being used. The Payload Protocol Identifier can be used therefore to de-multiplex the SCTP packet to the correct receiving endpoint/application above SCTP instead of the SCTP Destination Port Number.

The proposed solution based on the Payload Protocol Identifier parsing would then allow to contact multiple applications on a single well-known STCP port using the SCTP Payload Protocol Identifier instead of requesting IANA for allocation of a new well-known SCTP port number each time a new application is defined.

The SCTP multiplexer is implemented as a stand-alone process above the SCTP layer, listening at the well-known SCTP port and used to initiate and manage associations with remote SCTP endpoints and distribute received SCTP messages to upper-layer applications based on the Payload Protocol Identifier. The SCTP multiplexer is seen as a regular SCTP user. There is no impact on the SCTP stack.

The well-known port can be:

- The port already allocated for TCPMUX (port 1);
- A port already allocated for another SCTP application defined by 3GPP;
- A new port dedicated to SCTP multiplexing allocated in a port range locally administrated by 3GPP.
- A new port dedicated to SCTP multiplexing allocated by IANA.

In the figure below, a single SCTP host is supporting 4 new applications in addition of an existing W1 application (identified by the IANA-assigned port 38472). The port number used to identify the multiplexer is 47002 (given only as possible unassigned User Port that can be assigned by IANA for the SCTP multiplexer application).

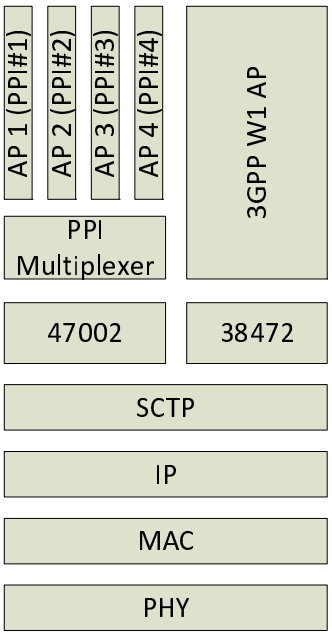


Figure 4.3.1-1: SCTP server-side illustration for SCTP Multiplexer (port)

When DTLS over SCTP, as described in IETF RFC 6083 [9], is used to provide mutual authentication, integrity protection, replay protection and confidentiality protection, only SCTP user data are integrity protected and encrypted by DTLS. The Payload Data (DATA) header, in which the SCTP Payload Protocol Identifier is indicated, is therefore sent as clear text. The SCTP Multiplexer can still use the SCTP Payload Protocol Identifier to distribute SCTP messages to upper-layer applications. Moreover, the SCTP associations being managed by the SCTP Multiplexer and the DTLS connections being handled by the applications (identified by the SCTP Payload Protocol Identifier) above the SCTP Multiplexer, it is possible to have multiple DTLS connections over a the same SCTP association, one DTLS connection per application (or per SCTP Payload Protocol Identifier).

In the figure below, a single SCTP host is supporting 4 new applications in addition of an existing W1 application (identified by the IANA-assigned port 38472). The port number used to identify the multiplexer is 47002 (given only as possible unassigned User Port that can be used). DTLS over SCTP is used to provide communications privacy for applications above the SCTP Multiplexer.

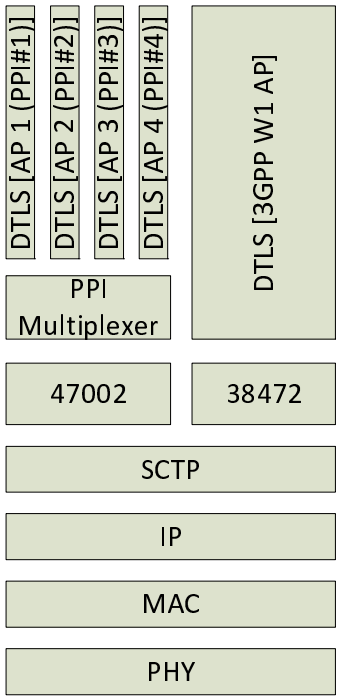


Figure 4.3.1-2: SCTP server-side illustration for SCTP Multiplexer (port) with used of DTLS over SCTP

4.3.2 Detailed description

The proposed solution is based on the following assumptions:

- The server implements an SCTP multiplexer that can serve multiple applications on a single well-known STCP port.
- Each SCTP application hosted in the server is configured with an internal IP address and a listening port. The SCTP multiplexer is configured with forwarding rules that associate an SCTP Payload Protocol Identifier with a target internal IP address/port. The forwarding rules are used by the SCTP multiplexer to forward incoming SCTP application traffic received on the well-known STCP port to the internal application processes.
- The client is configured with the IP address of the server to contact and use the well-known STCP port associated to the SCTP multiplexer or the IP address is discovered using basic DNS procedures.

To set-up a transport connection with the SCTP application server, the following steps apply:

1 The client sends an INIT signal to the SCTP multiplexer on the dedicated port to initiate an association.

2 On receipt of the INIT signal, the SCTP multiplexer sends an INIT-ACK response to the client. This INIT-ACK signal contains a state cookie.

3 On receipt of this INIT-ACK signal, the client sends a COOKIE-ECHO response, which just echoes the state cookie.

4 After verifying the authenticity of the state cookie, the SCTP multiplexer then allocates the resources for the association, sends a COOKIE-ACK response acknowledging the COOKIE-ECHO signal, and the association is said ESTABLISHED.

5 The client can send to the SCTP multiplexer user data encapsulated within SCTP DATA chunks, each DATA chunk including a Payload Protocol Identifier identifying the requested application.

6 The SCTP multiplexer checks the Payload Protocol Identifier included in each received DATA chunk.

a If the Payload Protocol Identifier is supported i.e., there is an internal process that supports the requested application, the SCTP multiplexer delivers the user data to the correct receiving application. The reception of the DATA chunk is then acknowledged by a SACK chunks and protocol data exchange between the client and the application behind the SCTP multiplexer can continue.

b If the Payload Identifier is not supported i.e., there is no internal process that supports the requested application, the SCTP multiplexer will abort the created SCTP association, sending an ABORT chunk to the client that contains a User-Initiated Abort cause code (12). A specific Upper Layer Abort Reason (e.g. "Unsupported Payload Protocol Identifier") can also be included and be delivered to the upper-layer protocol at the peer.

4.3.3 Pros and cons

Pros:

- Multiple SCTP applications can be run on the same port.
- Minimal administration or configuration to set the nodes up.
- Does not rely on DNS infrastructure.

Cons:

- An SCTP multiplexer process needs to be implemented in servers.
- Only applicable to protocols carried over SCTP.
- Need for IANA port number allocation if the one assigned to TCPMUX is not reused.
- Need for a 3GPP-managed port allocation if the port used for SCTP multiplexer is neither the one for TCPMUX nor one allocated by IANA.
- Not possible to use the port number to distinguish SCTP applications.

4.3.4 Guidelines for SCTP based solution#5

Solution#5 (SCTP MUX) is beneficial for clients that utilize SCTP.

It is strongly recommended to apply to IANA for assigned service name and SCTP port number for the first application of this solution in 3GPP networks. For additional SCTP applications, only the service name will have to be assigned by IANA as all the new SCTP application will be multiplexed over the same assigned STCP port using the SCTP Payload Protocol Identifier.

With IANA assigned service name and port numbers, solution#5 is beneficial for inter-domain scenario.

4.4 3GPP allocated port number solution#6

4.4.1 General

In scenarios, when IANA allocated default port numbers cannot be used, while a new 3GPP interface application may require a pre-defined specific server port number, 3GPP becomes responsible for allocating a server port number. Such port numbers should be assigned from a sub-range of the Dynamic/Private Port range [49152 - 65535].

NOTE: Clause 4 in IETF RFC 6335 [2] specifies that the term "assignment" is used to refer to the procedure by which IANA provides service names and/or port numbers to requesting parties and that other RFCs refer to this as "allocation" or "registration". IANA does not assign port numbers from Dynamic/Private Port range [49152 - 65535] and therefore any application designer is free to use any of these ports at will.

When a new 3GPP Rel-17 and onwards application requires pre-defined server port number, during the application initialization the operating system will tell the new application if the port is already in use or not. If the port is in use by another, legacy application, the new application or operating system shall ensure that the legacy application stops using the port. It is up to the implementation to decide if the legacy application will be forced to stop using the port immediately, or if the legacy application will be granted some period of time for graciously removing the port from usage.

Any sub-range from [49152 - 65535] range would be good for this purpose. 3GPP decided to set aside a sub-range of 101 ports from 65400 to 65500. 3GPP allocated port numbers are documented in 3GPP TS 29.641 [20].

4.4.2 Detailed description

The proposed solution is based on the following assumptions:

1. Dynamic/Private Port number range [49152 - 65535] is not restricted by IANA and may be used by 3GPP or non-3GPP applications without any restrictions.

2. Many existing interface applications are dynamically selecting port numbers from range [49152 - 65535] when populating source port field in UDP/TCP/SCTP header, e.g. for load balancing. In a request-response type of communication, the remote peer typically sends the response message to the port number, which is populating the source port field of the received request message.

3. Let's assume, 3GPP specifies in Rel-17 or onwards that the port number of some new application 'X' is e.g. 50000.

4. When sending a request message, the new application X will populate the port numbers as follows:

   - Destination port: e.g. 50000

   - Source port: e.g. 60000

5. When the application peer sends a response, the new remote application X will populate the port numbers in a reverse order:

   - Destination port: 60000

   - Source port: 50000

6. Now, in the network there will be other, legacy interface applications that were taken into use before application X is specified. Let's look into how the traffic for these applications would be handled.

7. Application X sends a request to the destination port 50000.

   a. If the application X peer receives such legit message, it will correctly handle the message.

   b. If a legacy application receives such message at port 50000, then the following scenarios should be checked. Note, that legacy application may expect only a response message at port 50000. If the application does not listen to port 50000, the message will be discarded. Even if the application listens to port 50000, it obviously cannot correctly parse the X application request and therefore an application/protocol specific error handling will be triggered. The legacy application will discard the message also in this case and may either log an error or may resend the request. For resending the request, the sequence numbers in the outstanding request and in the received erroneous message shall match. The latter case is highly hypothetical, because it is unlikely the legacy application can correctly extract a sequence number from the erroneous message, in the first place. Even less likely would be finding the match.

8. Legacy application sends a response to the destination port 50000, because it received a request from this port.

   a. If the legacy application peer receives such legit message, it will correctly handle the message.

   b. If an application X receives such message at port 50000, then the following scenarios should be checked. Note, that application X may expect only a request message at port 50000. The application X obviously cannot correctly parse the legacy application request and therefore an application/protocol specific error handling will be triggered. In order to optimize the error handling, the application X should be able to detect the legacy application type. In such case, the message shall be silently discarded. There will be only a handful of legacy applications running on the given NF, i.e. the NF will be connected only to a handful of 3GPP interfaces. Therefore, such additional, but trivial feature will not cause any considerable extra efforts.

The following use case needs to be considered:

- A legacy application client already runs on a network entity and a new 3GPP Rel-17 app is initializing;

- Both apps share the same IP address;

- The new 3GPP Rel-17 app shall listen to e.g. port 50000 for incoming requests;

- There is a small, but non-zero probability that the legacy app has sent a request to another server and is expecting a response to port 50000;
- The system will not allow new 3GPP Rel-17 app to run, because port 50000 is already in use;
- Implementation needs to find a way to somehow remove port 50000 from the legacy app usage, which will enable new 3GPP Rel-17 app to start;
- Once the new 3GPP Rel-17 app is up and running, the system will ensure the legacy app will always select another port from the dynamic range. No more clashes will happen on this network entity.

4.4.3 Pros and cons

Pros:

- The solution will have no impact on legacy applications.

Cons:

- If a legacy application client already runs on a network entity and a new 3GPP Rel-17 app is initializing on the same entity while both applications share the same IP address and port, then the system will not permit the new app to start. Implementation will need to find a way to free up the port in usage by the legacy application client, which will enable new 3GPP Rel-17 application to start.

4.4.4 Guidelines for 3GPP allocated port number solution#6

It is beneficial to use solution#6 (3GPP), if obtaining new default port number from IANA is deemed unsuitable, but when it is preferable for applications to use a fixed port number.

For inter-domain scenario, currently it is not possible to prevent firewalls/security gateways located between two domains from restricting outgoing/incoming network traffic for a specific port not assigned by IANA. This limitation may be mitigated if firewall implementations will start supporting 3GPP allocated port number range. This will be similar to the GTP-aware firewall implementations, which are already commonplace in operator networks. It is strongly recommended that 3GPP applies for IANA-assigned service name and port numbers.

4.5 OAM allocated port number solution#7

4.5.1 General

Each operator becomes responsible for allocating a port number to each new 3GPP application from either the User Port number range [1024-49151] or from the Dynamic/Private Port range [49152 - 65535].

4.5.2 Detailed description

The proposed solution is based on the following assumptions:

1. An operator determines which port numbers are not used as default ones in their network (either from the User Port number range [1024-49151] or from the Dynamic/Private Port range [49152 - 65535]).
2. The operator selects certain unused port number as a default one for the new 3GPP interface application and configures all relevant network entities with OAM.
3. Many existing interface applications are dynamically selecting port numbers from range [49152 - 65535] when populating source port field in UDP/TCP/SCTP header, e.g. for load balancing. In a request-response type of communication, the remote peer typically sends the response message to the source port number of the received request message. If the new port number is selected from the Dynamic/Private Port range [49152 - 65535], then the solution will be similar to the one, which is described in clause 4.4 for Solution#6.
4. If the new port number is selected from the User Port number range [1024-49151], then the drawbacks described in the above bullet point 3 will be eliminated.

The following use case needs to be considered, if Dynamic/Private Port range [49152 - 65535] is used:

- A legacy application client already runs on a network entity and a new 3GPP Rel-17 app is initializing;
- Both apps share the same IP address;
- The new 3GPP Rel-17 app shall listen to e.g. port 50000 for incoming requests;
- There is a small, but non-zero probability that the legacy app has sent a request to another server and is expecting a response to port 50000;
- The system will not allow new 3GPP Rel-17 app to run, because port 50000 is already in use;
- OAM needs to find a way to somehow remove port 50000 from the legacy app usage, which will enable new 3GPP Rel-17 app to start;
- Once the new 3GPP Rel-17 app is up and running, the system will ensure the legacy app will always select another port from the dynamic range. No more clashes will happen on this network entity.

4.5.3 Pros and cons

Pros:

- Gives full control and flexibility to operators when selecting default port numbers for new 3GPP interfaces.

Cons:

- The new application cannot have hard-coded default port number. That is, it will learn the default port number after successful configuration action.
- Makes the default port setting logic more complex in a new application.
- If a legacy application client already runs on a network entity and a new 3GPP Rel-17 app is initializing on the same entity while both applications share the same IP address and port, then the system will not permit the new app to start. OAM will need to find a way to free up the port in usage by the legacy application client, which will enable new 3GPP Rel-17 application to start.

4.5.4 Guidelines for OAM allocated port number solution7

It is beneficial to use solution#7 (OAM), if obtaining new default port number from IANA or from 3GPP is deemed unsuitable, but when it is preferable for applications to use a fixed port number. Solution#7 is not suitable for the inter-domain scenario.

4.6 Port Registration and Retrieval via NRF solution#8

4.6.1 General

This is an alternative solution which allows port information registration to the NRF and port information retrieval from the NRF. This solution is applicable for those NFs have entry in the NRF and provide specific protocols for non-SBI interfaces.

This solution is mostly used to register port numbers for 3GPP interface applications whose port numbers are not allocated by IANA. It is recommended that the port number for 3GPP interface applications should be allocated from User Port number range [1024-49151] or from Dynamic/Private Port range [49152 - 65535].

To avoid potential port clash, an operator shall investigate the port numbers used by existing interfaces/applications hosted by an NF before deploying that NF, and thus determine one port number to be used and registered. Other mechanisms to detect and remove the port clash (e.g. described in clause 4.4 and 4.5 for solution#6 and solution#7, respectively) may also be used if necessary.

4.6.2 Detailed description

Normally, same port number is allocated to a group of NFs hosting the same protocol. However, different port numbers may be allocated for same protocol per NF Types, NF Sets, or even per NF instance.

To configure port numbers in the NRF, a data type of PortInfo is defined to carry a list of port record, and each port record indicates the port number and related protocol type. A PortInfo is included in the NF Profile to register the protocol and associated port numbers used by the NF. One PortInfo instance can be shared by multiple NFs which have the same NF type or belong to same NF Set. If one NF needs to be configured with different port number than other NFs using the same protocol, the NF can be configured with its own PortInfo.

A requesting NF thus can use the NF Discovery service to retrieve the port number of a specific protocol, by indicating the protocol type. Other parameters such as NF type, NF Set ID, or NF Instance ID may also be provided as discovery parameter.

4.6.3 Pros and cons

Pros:

- Reuse NRF mechanism for port configuration and retrieval.
- Port number for a protocol can be configured at granularity of NF type, NF Set, or individual NF instance.

Cons:

- This solution relies on NRF mechanism, and is more applicable to non-SBI interfaces hosted by core network NFs.
- If this solution is used for RAN interfaces, the RAN node may need to support SBI interface to a localized NRF.
- The use cases for the NRF based solution will be reduced to non-roaming core network interfaces.

4.6.4 Guidelines for Port Registration and Retrieval via NRF solution#8

It is beneficial to use solution#8 (NRF), if the network element can support service-based interface and access an NRF.

5 Summary

5.1 General

As indicated in the clause 4.1, it is strongly recommended for 3GPP to apply to IANA for assigned service name and port number for any protocol potentially supported by roaming and inter-domain interfaces when no other service port discovery (e.g. DNS-based solutions) is applicable.

When the IANA assignment request cannot be justified, one of the alternative solutions described in clause 4 should be adopted.

5.2 3GPP allocated Service Name and Port Number registry

3GPP CT4 maintains 3GPP TS 29.641 [20] as a repository of the 3GPP assigned Service Name and Port Numbers, which are necessary for the solution#6, which is specified in clause 4.4.

Annex A:
IANA port allocation policy

IANA maintains the list of service names and port numbers used to distinguish between different services that run over transport protocols such as TCP, UDP, DCCP and SCTP. The IANA registration procedures for service names and port numbers are described in IEFT RFC 6335 [2].

- Service names are assigned on a first-come, first-served process. Assignments are made to anyone on a "first come, first served" basis. There is no substantive review of the request, other than to ensure that it is well-formed and doesn't duplicate an existing assignment.

- Port numbers are assigned in various ways, based on three ranges: System Ports [0-1023], User Ports [1024-49151], and the Dynamic and/or Private Ports [49152 - 65535].

According to Clause 8.1.2 of IEFT RFC 6335 [2], IANA follows one the following procedures for port number value allocation defined in IEFT RFC 8126 [9]:

- IETF Review:

  - New values are assigned only through IETF RFCs in the IETF Stream, i.e., documents that has been approved by the IESG as having IETF consensus.

- IESG Approval:

  - New value assignment is directly approved by the IESG without the need for approved IETF RFCs.

- Expert Review:

  - New values are assigned after review and approval by a designated expert. An approved IETF RFC is not required but information needs to be provided with the request for the designated expert to evaluate.

System Ports are assigned by IANA using the "IETF Review" or "IESG Approval" procedures.

User Ports are assigned by IANA using the "IETF Review" process or the "IESG Approval" process or the "Expert Review" process.

Dynamic Ports are not assigned. The Dynamic Ports range has been specifically set aside for local and dynamic use. Application software may simply use any dynamic port that is available on the local host, without any sort of assignment, assuming that the port used by applications are discovered by clients dynamically at run-time.

System and User ports should not be used without or prior to IANA registration. The registration procedures for service names and port numbers are described in IEFT RFC 6335 [2].

Recently, however, IANA became more restrictive to reserving new port numbers to private networks. IANA experts are now following the recommendations given in Clause 6 of IETF RFC 7605 [3]. Each port number assignment request must be now strongly justified by the applicants as independently useful service. This was done on purpose, as the range of port number that can be allocated by IANA is fixed and IANA does not want to run out of available port numbers in future, due to uncontrolled requests as it was done in the past (e.g. range of port numbers allocated to a single company etc.).

Annex B:
Port number use

B.1 General

In IP networking, the destination or origination IP address of a message is completed by a port number. If the IP address identifies the device e.g. computer, the port number is used to identify an application or service running on the device.

The current use of ports was clearly established in the Transmission Control Protocol [13]

Multiplexing:

- To allow for many processes within a single Host to use TCP communication facilities simultaneously, the TCP provides a set of addresses or ports within each host. Concatenated with the network and host addresses from the internet communication layer, this forms a socket. A pair of sockets uniquely identifies each connection.
- That is, a socket may be simultaneously used in multiple connections.
- The binding of ports to processes is handled independently by each Host. However, it proves useful to attach frequently used processes (e.g., a "logger" or timesharing service) to fixed sockets which are made known to the public. These services can then be accessed through the known addresses. Establishing and learning the port addresses of other processes may involve more dynamic mechanisms.

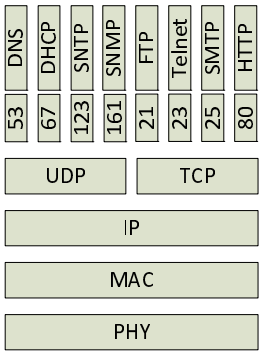
The port number is a 16-bit unsigned number, ranging then from 0 to 65535.

As indicated in the IETF RFC 6335 [2], this range [0-65535] is subdivided as follows:

- 0-1023: the System Ports, also known as the Well Known Ports, assigned by IANA
- 1024-49151: the User Ports, also known as the Registered Ports, assigned by IANA
- 49152-65535: the Dynamic Ports, also known as the Private or Ephemeral Ports, not assigned, controlled, nor registered.

B.2 Port number ranges

System ports [0-1023] are assigned by IANA and were initially reserved to services that required privileged/root access to the operating system. They have been reserved for common applications, typically server applications. The port numbers assigned to these server applications have to be known by the client's transport layer and are used by the client as destination port number in message requests sent to the server applications. Clients know that servers will be listening for their requests at these reserved port numbers.

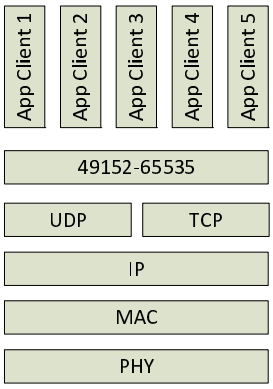


B.2-1: Example of Well-Known port numbers used by servers.

User ports [1024-49151] are assigned by IANA and also used to identify server applications as for System port except that they were reserved for services that did not require privileged access.

NOTE: Today, the distinction between System and User ports is not any more obvious. Operating systems may allow access to System port numbers to non-privileged services and well-known services are usually replicated on User ports (e.g. HTTP on port 8080).

Dynamic ports [49152-65535] are not assigned/allocated by IANA. They are automatically allocated by the IP stack software to be used as source port of an outgoing IP message. These port numbers are used by clients to identify the internal process sending the message and the receiver can simply reply to the client by using the received source port number as destination port number in the reply sent to the client. The port allocations are temporary and only valid for the duration of the communication session. After completion (or timeout) of the communication session, the ports become available for reuse, although most IP stacks will usually not reuse that port number until the entire pool of ephemeral ports have been used. So, if the client program reconnects, it will be assigned a different ephemeral port number for its side of the new connection.



B2-2: Dynamic port numbers used by clients.

Even if not recommended, Dynamic Port numbers may also be used to temporary identify a server application in a node. This implies that:

- The client has a mean to discover the port allocated to the server at run-time.
- The dynamic port assigned to the service cannot be reused by a client program in the same node as long as the port needs to be used as listening port by the service.

B.3 Service identified by port number not assigned by IANA

Not all the services need assigned port numbers. Any service can use:

- Any unassigned port in the System and User port ranges
- Any port number from the Dynamic port range.
- Port numbers assigned to another protocol if this protocol is not used e.g. ports assigned to the Service Location Protocol (SLP) can be reused by any service if this service is not deployed in a private network and there is then no risk of conflict.

Services assigned with System/User ports by IANA may also use unassigned ports to reduce the impact of potential attacks on the well-known ports and then be more securely operated. For instance, a node that provides an HTTP interface for internal management will likely use another port that the port 80.

For port numbers picked in the Dynamic port range to identify a service application, there is a need to ensure that this port will not be re-allocated to another client program in the same node to avoid conflict. Mechanisms to achieve such a "long-lived" port assignment of dynamic port include:

- Configure the range of dynamic ports that can be dynamically assigned by the IP stack: the range defined by IANA is [49152-65535] but IP stacks can usually be tuned to use another range, e.g. [32768-60999]. This implies that port numbers outside this range can be used as listening ports by servers, including ports normally considered as "dynamic ports" by IANA.
- When booting the node, start all services before any other process start and begin establishing connections. Therefore, all the servers can be assigned with any available port from the unassigned ports in System/User port

range or any port from the Dynamic port range. Then a client program will only be able to use remaining port numbers in the dynamic port range and no conflict will happen.

When the port used to identify a service is not assigned by IANA, the clients have to discover the destination port to use when sending a request. As indicated in the IETF RFC 6335 [2], possible discovery mechanisms include:

- Explicit configuration of both endpoints;
- Internal mechanisms within the same host (e.g. a configuration file, indicated within a URI or using interprocess communication);
- Information provided by another service e.g. FTP, SIP, etc.;
- Relying on specific service names and use of existing port discovery services defined by IETF: mDNS as defined in IETF RFC 6762 [8], DNS-based Service Discovery defined in IETF RFC 6763 [6], etc. Service names can be simply registered by IANA on a "first-come, first-served" basis in a namespace much larger than the port number range.

Annex C: IANA procedures for Service Name and Port Number registry management

C.1 General principles

IANA is responsible for the management and maintenance of service name and port number registry. Because assigned port numbers are a limited resource that is globally shared by the entire Internet community, the conservation of the port space is the key priority of IANA when addressing port number assignment request. IANA strives to limit assigned port number consumption and promotes the use of alternate solutions for service identification, such as explicit configuration of both endpoints, the use of service names and dynamic ports along with service discovery mechanism, in-band port negotiation and/or application layer service multiplexing.

Another priority is to allocate port primarily to applications used on the Internet.

IANA assigns port numbers so that **Internet** endpoints do not need pairwise, explicit coordination of the meaning of their port numbers. This is the primary reason for requesting port number assignment by IANA -- to have a common agreement between all endpoints on the **Internet** as to the default meaning of a port number, which provides the endpoints with a default port number for a particular protocol or service.

C.2 Assignment Procedure

As described in the IETFC RFC 6335 [2], a service name or port number assignment request sent to IANA contains the following information:

Table C.2-1: Service Name/port number assignment request form

Field	Required/ optional	Description
Service Name	Required	Unique service name for the service associated with the assignment request. The name MUST be compliant with the syntax defined in clause 5.1 of IETF RFC 6335 [2] (NOTE)
Transport Protocol(s)	Required	TCP, UDP, SCTP, and/or DCCP. It is required even if the request is only for service name assignment
Assignee	Required	Name and email address of the organization, company or individual person responsible for the initial assignment.
Contact	Required	Name and email address of the Contact person for the assignment
Description	Required	Short description of the service associated with the assignment request
Reference	Required	A description of (or a reference to a document describing) the protocol or application using this port.
Port Number	Optional	Suggested port number or port range (user or system)
Service Code	Optional	Required only for DCCP
Known Unauthorized Uses	Optional	Known/reported unauthorized uses by applications or organizations who are not the Assignee
Assignment Notes	Optional	Indications of owner/name change, or any other assignment process issue
NOTE: For 3GPP defined service names, the name shall be prefixed by "3gpp-"		

When receiving the assignment request, IANA will follow the one of the procedures described in the following clause.

C.3 IANA Policies for Port Number assignment

When IANA receives an assignment request that is only requesting service name, IANA will usually assign the service name under a simple "First Come First Served" policy defined in IETF RFC 5226 [14]

When IANA receives an assignment request that is requesting a port number, IANA will initiate an "IETF Review" or "IESG Approval" procedures or an "Expert Review" procedure defined in IETF RFC 5226 [14], depending on the requested port range:

- Ports in the Dynamic Ports range (49152-65535) cannot be assigned through IANA. **A port number in that range MUST NOT be used as a service identifier**.

- Ports in the User Ports range (1024-49151) will be assigned under the "IETF Review" or "IESG Approval" procedures defined in IETF RFC 5226 [14] for IETF protocol. In other cases, the requester must input the documentation to the "Expert Review" procedure defined in IETF RFC 5226 [14], by which IANA will have a technical expert review the request to determine whether to grant the assignment. The submitted documentation **MUST explain why using a port number in the Dynamic Ports range is unsuitable** for the given application.

- Ports in the System Ports range (0-1023) will only be assigned under the "IETF Review" or "IESG Approval" procedures defined in IETF RFC 5226 [14]. A request for a System Port number **MUST document *both* why using a port number from the Dynamic Ports range is unsuitable *and* why using a port number from the User Ports range is unsuitable** for that application.

C.4 Recommendations to designers of application and service protocols

Used as companion document of the IETF RFC 6335 [2], the IETF RFC 7605 [3] provides recommendations to designers of application and service protocols on how to use the transport protocol port number space and when to request a port assignment from IANA.

First, a set of questions is given to help designers to check whether a port number assignment is deemed required for a given service application. These questions are listed hereafter:

- Is this really a new service or could an existing service suffice?

- Is this an experimental service [RFC3692]? If so, consider using the current experimental ports [RFC2780].

- Is this service independently useful? Some systems are composed from collections of different service capabilities, but not all component functions are useful as independent services. Port numbers are typically shared among the smallest independently useful set of functions. Different service uses or properties can be supported in separate pairwise endpoint associations after an initial negotiation, e.g., to support software decomposition.

- Can this service use a Dynamic port number that is coordinated out-of-band? For example:

  - By explicit configuration of both endpoints.

  - By internal mechanisms within the same host (e.g., a configuration file, indicated within a URI or using interprocess communication).

  - Using information exchanged on a related service: FTP [RFC959], SIP [RFC3261], etc.

  - Using an existing port discovery service: portmapper [RFC1833], mDNS [RFC6762] [RFC6763], etc.

Moreover, a set of recommendations and requirements for registration and use of port is provided to help designers to determine whether a port number assignment is required. These recommendations and requirements are provided for information hereafter:

- Each assigned port requested MUST be justified by the applicant as an independently useful service.

- Developers SHOULD NOT apply for System port number assignments because the increased privilege they are intended to provide is not always enforced.

- System implementers SHOULD enforce the need for privilege for processes to listen on System port numbers.

- New services SHOULD support security capabilities, either directly or via a content protection such as TLS [RFC5246] or Datagram TLS (DTLS) [RFC6347], or transport protection such as the TCP-AO [RFC5925]. Insecure versions of new or existing secure services SHOULD be avoided because of the new vulnerability they create.

- When requesting both secure and insecure port assignments for the same service, justification is expected for the utility and safety of each port as an independent service (clause 6). Precedent (e.g., citing other protocols that use a separate insecure port) is inadequate justification by itself.
- Security SHOULD NOT rely on assigned port number distinctions alone; every service, whether secure or not, is likely to be attacked.
- Version support SHOULD be included in new services rather than relying on different port number assignments for different versions.
- Version numbers SHOULD NOT be included in either the service name or service description, to avoid the need to make additional port number assignments for future variants of a service.
- Service names and descriptions for multiple transport port number assignments SHOULD match only when they describe the same service, excepting only enhancements for each supported transport.
- Names of discovery services SHOULD use an identifiable suffix; the suggestion is "-disc".
- UDP over IPv4 multi-host services SHOULD use multicast rather than broadcast.
- Services that use multipoint communication SHOULD be scalable and SHOULD NOT rely solely on the efficiency of multicast transmission for scalability.
- Services SHOULD NOT use UDP as a performance enhancement over TCP, e.g., to circumnavigate TCP's congestion control.
- Users MUST NOT deploy implementations that use assigned port numbers prior their assignment by IANA.
- Users MUST NOT deploy implementations that default to using the experimental System port numbers (1021 and 1022 [RFC4727]) outside a controlled environment where they can be updated with a subsequent assigned port [RFC3692].
- Users writing specifications SHOULD use symbolic names for port numbers and service names until an IANA assignment has been completed. Implementations SHOULD use experimental port numbers during this time, but those numbers MUST NOT be cited in documentation except as interim.

C.5 3GPP port assignment applications since 2009

IETF RFC 6335 [2] was published in 2011 to update IANA's procedures by obsoleting the previous UDP and TCP port assignment procedures. Before that, the principles for service name and port number management were based on a set of informal guidelines developed based on the review experience from previous assignment request and never publicly documented. Port numbers were managed informally, and sometimes inconsistently and arbitrarily e.g., some services were assigned ranges of many port numbers even where not strictly necessary.

Published in 2015, IETF RFC 7605 [3] provides additional information to designers on how to use assigned port numbers that complements the IANA process described in IETF RFC 6335 [2].

Whereas the conditions of port assignment have been further clarified and reinforced based on the conservation principle, it seems that 3GPP did not really appraise the policy change and did not modify accordingly their use of port numbers in 3GPP systems. The port number assignment was recently still considered as a by default solution for service identification even if other solutions were applicable.

Table C.5-1 hereafter lists the port numbers assigned to 3GPP since 2009. In this table, it can be noticed that most of the applications were for SCTP and protocols only inside 3GPP networks, without inter-domain interfaces.

Table C.5-1: Service Name/port number assigned to 3GPP since 2009

Service Name	Port Number	Transport Protocol	Description	Registration Date	Intra/Inter
sgsap	29118	sctp	SGsAP	11/06/2009	Intra (MME/MSC)
sbcap	29168	sctp	SBcAP	11/06/2009	Intra (MME/CBC)
s102	23272	udp	S102 application	26/08/2009	Intra (1xCS IWS/MME)
s1-control	36412	sctp	S1-Control Plane	01/09/2009	Intra (MME/eNB)
x2-control	36422	sctp	X2-Control Plane	01/09/2009	Intra (eNB/eNB)
iuhsctpassoc	29169	sctp	HNBAP and RUA Common Association	08/09/2009	Inter (HNB/HNB-GW)
3gpp-cbsp	48049	tcp	Cell Broadcast Service Protocol	07/12/2009	Intra (BSC/CBC)
lcs-ap	9082	sctp	LCS Application Protocol	04/06/2010	Intra (MME/E-SMLC)
wlcp	36411	udp	Wireless LAN Control plane Protocol (WLCP)	14/11/2014	Intra (UE/TWAG)
slmap	36423	sctp	SLm Interface Application Protocol	18/06/2015	Intra (E-SMLC/LMU)
nq-ap	36424	sctp	Nq/Nq' Application Protocol	18/06/2015	Intra (the RCAF/MME or SGSN)
xw-control	36462	sctp	Xw-Control Plane	13/11/2015	Intra (eNB/WT)
pfcp	8805	udp	Destination Port number for PFCP	08/05/2017	Intra (CU/UP)
ng-control	38412	sctp	NG Control Plane	18/05/2017	Intra (gNB/ng-eNB-AMF)
xn-control	38422	sctp	Xn Control Plane	18/05/2017	Intra (gNB-gNB/ng-eNB)
f1-control	38472	sctp	F1 Control Plane	23/06/2017	Intra (gNBCU/gNBDU)
e1-interface	38462	sctp	E1 signalling transport	06/11/2018	Intra (gNB-CU-CP/gNB-CU-UP)
3gpp-monp	8809	udp	MCPTT Off-Network Protocol (MONP)	15/04/2019	Intra (MCPTT client/MCPTT client)
3gpp-w1ap	37472	sctp	W1 signalling transport	16/07/2020	Intra (ng-eNB-DU/ng-eNB-CU

Since 2015, IANA had gradually warned 3GPP that a solution should be found to avoid port assignments for protocols only used in 3GPP. Exceptions were made at the beginning and the last requests were granted by IESG only at the conditions that it was the last one(s). Now, it is clear that application for a new port will not be granted without a strong justification for it, only if the recommendations given in IETF RFC 7605 [3] have been carefully followed and it is proved that there is no other solution than port assignment for service port discovery.

Annex D:
Change history

Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2020-09	CT4#101e	C4-205007				Skeleton	0.0.0
2020-11	CT4#101e	C4-205774				C4-205481 was incorporated.	0.1.0
2021-04	CT4#103e	C4-212403				C4-212403 was implemented, which updates the skeleton	0.1.1
2021-04	CT4#103e	C4-212591				The following pCRs were implemented: C4-212402, C4-212404, C4-212405, C4-212406.	0.2.0
2021-05	CT4#104e	C4-213521				The following pCRs were implemented: C4-213024, C4-213025, C4-213026, C4-213027, C4-213039, C4-2133365.	0.3.0
2021-06	CT#92e	CP-211086				TR presented for information	1.0.0
2021+06	CT'92e	CP-211339				Presentation sheet updated	1.0.1
2021-08	CT4#105e	C4-314748				The following pCRs were implemented: C4-214038, C4-214053, C4-214054, C4-214055, C4-214056, C4-214542, C4-214579 and C4-214745.	1.1.0
2021-10	CT4#106e	C4-315511				The following pCRs were implemented: C4-215343, C4-215499.	1.2.0
2021-11	CT4#107e	C4-316464				The following pCR was implemented: C4-216017.	1.3.0
2021-12	CT#94e	CP-213151				V2.0.0 presented for approval	2.0.0
2021-12	CT#94e					V17.0.0 published after CT#94	17.0.0
2022-03	CT#95e		0001	1	F	Moving Annex D into new TS	17.1.0

History

Document history		
V17.1.0	May 2022	Publication