3GPP TSG CN Plenary Meeting #17 **NP-020388**
4th - 6th September 2002. Biarritz, France.

Source:	**SA2 / CN3 Chair**
Title:	**LS (not direct to CN Plenary) on Proposed solutions for the identification of source IP address information over the Go interface**
Agenda item:	**6.3.2**
Document for:	**INFORMATION**

3GPP TSG-SA WG2 meeting #26 **Tdoc S2-022621**
Toronto, Canada, 19th – 23rd August 2002

Title:	Response on "Proposed solutions for the identification of source IP address information over the Go interface"
Source:	SA2
To:	CN3, CN1
Cc:	
Answer to	S2-022232 (=N3-020738)

Contact Person:
Name: Teuvo Järvelä
E-mail Address: teuvo.jarvela@northstream.se

Attachments: **S2-022620**

---

1. Overall Description:

SA2 would like to thank CN3 for their liaison statement on "Proposed solutions for the identification of source IP address information over the Go interface". SA2 has considered the proposed CR to 23.207 CR 40 rev 2 including changes CN3 made and found it acceptable. SA2 has modified it to reflect the latest version of 23.207 (version 5.4.0). This modification is purely CR control administrative and do not have any impact on the text proposed in this CR by SA2 and CN3. The SA2 approved CR to 23.207 CR 40 rev 4 is attached into this LS.

2. Actions:

To CN3

SA2 has now introduced this feature (CR to 23.207 CR 40 rev 4) in its stage2 documentation and asks CN3 to introduce stage 3 CR 29.207 CR 22rev 1 (N3-020731) concerning this issue in its documentation.

SA2 kindly asks CN3 to include this functionality for Release 5 and submit the related stage 3 CR 29.207 CR 22rev 1 (N3-020731) to the next CN plenary in September for TSG-CN approval.

To CN1

None

3. Date of Next SA2 Meetings:

SA2#27	14th- 18th October 2002	Beijing, China
SA2#28	11th – 15th November 2002	Bangkok, Thailand

3GPP TSG-SA2
Toronto, Canada 19-23 August 2002

Tdoc S2-022620

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **40** ⌘ **rev** **4** ⌘ Current version: **5.4.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Source IP address filtering for Service Based Local Policy
Source:	⌘	AWS
Work item code:	⌘	E2E QoS
Date:	⌘	01/08/2002
Category:	⌘	**F**
Release:	⌘	REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	An issue has been identified in the lack of source address information available to the nodes enforcing service based local policy
Summary of change:	⌘	Introduces restriction that a user's source IP address uses the same 64 bit prefix for the address they receive their data on and provides the operator a mechanism for identifying this information in its packet filters in service based local policy over the Go interface .
Consequences if not approved:	⌘	Lack of source information would allow for misuse of service and negative service experience for the user

Clauses affected:	⌘	5.2.2 and 5.2.3			
Other specs Affected:	⌘	**Y** / **N**	Other core specifications	⌘	29.207 CR 22 rev1
		N	Test specifications		
		N	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

****

5.2 Capabilities of Functional Elements

This section provides functional descriptions of capabilities in GGSN, UE, and P-CSCF(PCF).

5.2.1 GGSN

This clause provides functional descriptions of capabilities in GGSN. The capabilities are part of IP BS Manager (see 5.1.1.1) or corresponding user plane functions. Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

The **DiffServ Edge Function** shall be compliant to the IETF specifications for Differentiated Services. The IETF Differentiated Services architecture will be used to provide QoS for the external bearer service.

RSVP/IntServ Function

[Editor's note: Detailed functional description of RSVP/IntServ Function is FFS]

The **Service-based Local Policy Enforcement Point** controls the quality of service that is provided to a set of IP packets (or IP "flows") defined by a packet classifier. The policy enforcement function includes policy-based admission control that is applied to the IP bearers associated with the flows, and configuration of the packet handling and policy based "gating" functionality in the user plane. Service-based local policy decisions are either "pushed" to or requested by the GGSN via the Go interface.

Policy-based admission control ensures that the resources that can be used by a particular IP flow are within the "authorized resources" specified via the Go interface. The authorized resources provide an upper bound on the resources that can be reserved or allocated for an IP flow. The authorized resources may be expressed as an Intserv-style Flowspec. This information is mapped by the **Translation/mapping function** in the GGSN to give the authorized resources for UMTS bearer admission control.

In the user plane, policy enforcement is defined in terms of a "gate" implemented in the GGSN. A gate is a policy enforcement function that interacts through Go interface with PCF as the Policy Decision Point for QoS resource authorisation at the IP BS level for a unidirectional flow of packets. Gate operations as defined in TS23.228 are to define the control and to manage media flows based on policy, and are under the control of PCF. A gate operates on a unidirectional flow of packets, i.e., in either the upstream or downstream direction. A gate consists of a packet classifier, a traffic metering function, and user plane actions to be taken for the set of packets matching the classifier. When a gate is enabled, the packets in a flow are subject to the Diffserv edge treatment (policing or marking) as determined by traffic metering and user plane actions. When a gate is disabled, all of the packets in the flow are dropped.

The packet classifier associated with a gate is a micro-flow classifier including the standard 5-tuple: (source IP address, destination IP address, source port, destination port, protocol), identifying a set of packets associated with a unidirectional flow.

Elements of the 5-tuple may be wild-carded. This is FFS in Stage 3 work. It is possible for a set of packets to match more than one classifier. When this happens, the sequence of actions associated with the gates are executed in sequence. Packets that are marked by a gate may not be (re)marked by a subsequent gate to a Diffserv Code Point corresponding to a better service class.

The **Binding Mechanism Handling** associates the PDP context bearer with one or more IP flows in order to support service-based local policy enforcement and QoS inter-working. Binding information is included in PDP Context Activation or Modification messages to associate the PDP context bearer with QoS and policy decision information provided by the PCF and associated with IP flows. In order to allow QoS and policy information to be "pulled" from the PCF, the binding information shall allow the GGSN to determine the address of the PCF to be used.

5.2.2 UE

This clause provides functional descriptions of capabilities in UE. The capabilities are part of IP BS Manager (see 5.1.1.1) or corresponding user plane functions. Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

DiffServ Edge Function acts as a DiffServ (DS) boundary for the traffic from applications running on the UE. As specified in RFC2475, DS boundary node must be able to apply the appropriate PHB to packets based on the DS code point. In addition, DS boundary nodes may be required to perform traffic conditioning functions. When GGSN DiffServ marking is used, the DiffServ edge function in the UE is not needed.

RSVP/Intserv Function provides the capability for the UE to request end-to-end QoS using RSVP messages as defined in IETF standards. RSVP messages may also be used by the network to inform the DSCP to be used by the UE. RSVP messages shall include the authorization token and flow identifier(s) in a policy data object if the authorization token is available in the UE. RSVP may be used to trigger PDP context activation/modification. The inter-working between MT and TE is FFS.

Binding Mechanism associates the PDP context bearer to the IP flow to support IP policy enforcement and QoS inter-working in the GGSN. The authorization token and flow identifiers are used to provide the binding mechanism and is included by the UE in the PDP Context Activation or Modification messages. The authorization token may also be used to bind a RSVP session with a SIP session by including the authorization token and flow identifier(s) in RSVP messages. For IMS services, the authorization token is provided to the UE by the P-CSCF during SIP session establishment.

The manner in which QoS preconditions for a SIP session shall be met are as stated in TS 23.228. The functionality shall be compliant to the IETF specification on Integration of Resource Management and SIP.

For each bi-directional media flow, the UE shall ensure that the 64 bit IPv6 address prefix of the source address of outgoing packets is the same as the prefix of the destination address supplied for incoming packets.

5.2.3 P-CSCF(PCF)

This clause provides functional descriptions of capabilities in P-CSCF(PCF). Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

Service-based Local Policy Decision Point

- Authorize QoS resources (bandwidth, etc.) for the session. The P-CSCF (PCF) shall use the SDP contained in the SIP signaling message to calculate the proper authorization. The authorization shall be expressed in terms of the IP resources to be authorized. The authorization shall include limits on IP packet flows and restrictions on IP destination address and port. For bi-directional media flows, the P-CSCF(PCF), according to operator policy, may assume that the 64-bit IPv6 address prefix of the source address for downstream packets is the same as the prefix of the destination address for upstream packets of the same media flow. The implementation of this P-CSCF(PCF) assumption would be determined by operator policy in order to reduce the possibilites of bearer misuse In the filters supplied by the PCF for bi-directional flows, the source address prefix for downstream packets may be identified as the same as the destination address prefix for the upstream. Similarly, the source address prefix for the upstream packets may be identified as the same as the destination address prefix for the downstream.

- The P-CSCF (PCF) shall be able to enforce the behaviour of the UE in respect to the assignment of IMS media components to the same PDP Context or to separate PDP Contexts. This behaviour of the UE is controlled by the IMS network using the indications described in Sections 4.2.5.1 of [4]. In case the UE violates this indication, and attempts to carry multiple IMS media components in a single PDP context despite of an indication that mandated separate PDP contexts, the P-CSCF/PCF shall take care that such a PDP context would be rejected by the GGSN. To do so, the P-CSCF/PCF uses the Go interface.

- The P-CSCF (PCF) shall be able to decide if new QoS authorization (bandwidth, etc.) is needed due to the mid-call media or codec change. A new authorization shall be required when the resources requested by the

UE for a flow exceeds previous authorization, or a new flow is added, or when elements of the packet classifier(s) for authorized flows change.

- The PCF functions as a Policy Decision Point for the service-based local policy control.
- The PCF shall exchange the authorization information with the GGSN via the Go interface.
- PCF provides final policy decisions controlling the allocated QoS resources for the authorized media stream. The decision shall be transferred from the PCF to the GGSN.
- At IP multimedia session release, the PCF shall revoke the QoS resource authorization for the session.

Binding Mechanism Handling

- The PCF generates an authorization token for each SIP session and the P-CSCF sends the authorization token to the UE in SIP signalling. The authorization token may contain information that identifies its generator. The authorization token shall be unique across all PDP contexts associated with an APN. The authorization token conforms to the IETF specification on SIP Extensions for Media Authorization.