3GPP TSG_CN **Tdoc NP-000518**
Plenary Meeting #9, Oahu, Hawaii
20th – 22nd September 2000.

Source: **TSG CN WG2**

Title: **All LSs from TSG_CN WG 5 since TSG_CN#8**

Agenda item: **6.5.1**

Document for: **Information**

TDoc #	To	Title	Source
N5-000182	S1 (OSA ad hoc)	Liaison Statement to S1 on Connectivity Management	BT
N5-000183	S1 (OSA ad hoc)	Liaison Statement to S1 on the concept of Enterprise Operator	BT

3GPP TSG_CN WG5#5 **Tdoc N5-000182**
Bristol, UK
5th-7th of September 2000.

Source:	**TSG CN WG5**
To:	**TSG SA WG1 (OSA ADHOC GROUP)**
Title:	**Liaison Statement to S1 on Connectivity Management**
Contact:	**Richard Stretch (richard.stretch@bt.com)**

1.0 Introduction

During the last CN5 meeting in Bristol, the group reviewed their documentation in regards to the Release 2000 specifications. The Release '99 specification is based mainly upon Parlay 2.1 with some specific additions made by CN5. One part not included in the Release 99 specification but seen as valuable addition for Release 2000, is the area of Connectivity management.

Connectivity management was included in the ETSI SPAN 6 SPAR Requirements Technical Report. These Requirements were used by ETSI SPAN3 as a basis for their API specification. CN5 see this functionality of great value for the ongoing enhancement of the API for Release 2000.

CN5 would like S1 to review and consider the following text for inclusion in the S1 Requirements for OSA Release 2000 (21.121)

2.0 Connectivity Management

2.1 Overview and summary of Business Drivers

Existing IP Service Provider networks offer IP connectivity with a limited range of service levels and attributes. The rapid development of IP network technology is enabling an explosion in the range of connectivity services and connectivity attributes supported by a common network infrastructure. From a commercial perspective, this is being driven by fierce competition between Internet Service Providers (ISPs) and between Network Service Provider (NSPs). Such service and connectivity attributes include Quality of Service (QoS), bandwidth management, data security, tailored routing and reachability, Virtual Private Network (VPN) membership and connectivity, access control, address translation and management, roaming and mobility, and resilience.

This explosion in the types and attributes of IP connectivity is leading to a major problem for service providers, namely the control and management of such diverse modes of connectivity. Even with existing service provider networks, this is a problem which has been present, given the scale and diversity of IP access (fixed, dial, dial roaming, shared broadband, tunneled, etc.), and the richness of Internet peering. Indeed, the problem of the management of connectivity attributes is unparalleled in data networks; it is comparable to the equivalent problem in existing voice networks but goes beyond these in the complexity and diversity of network access and peering. The ability to manage IP connectivity services in a scalable way, allowing diversity, customization and appropriate dynamics will be critical to the success of the service provider.

The benefits that connectivity management seeks to achieve are as follows:

1. Facilitating the rapid introduction of services: Through the use of a common policy framework, new services can be defined, created and deployed by manipulating the policy database (adding or changing attributes to well defined objects). These policies are then realized in the network by simple commands passed through well-defined APIs. The Connectivity Manager does not replace the service management function but provides the infrastructure necessary to introduce services quickly.
2. Enhanced application connectivity: By providing an API to the applications, they can modify policies and configuration rules by entering the data through a web interface. These policies are internally validated and the Connectivity Manager will make the necessary network changes. In a PSTN advanced 800 example, the application can make changes to their routing tables due to overloads on the any of their call centers dynamically by changing the routing thresholds.
3. Improved operations: The policy management framework will automate dynamic service-specific configuration, both static and dynamic, through the integrated database and APIs to the network elements. The offloading of application specific changes (as in 2) will result in operations productivity improvements, automated downloading of configurations to network elements, and reduction of errors by making consistency checks of rules before implementing them in the network. In the case of a VPN, the inter-domain policy and configuration are automated.

Connectivity Management provides the control and management of the following connectivity attributes:

- Network Quality of Service, including support of Service Level Agreements (SLAs) e.g. packet loss, delay, rate control, and throughput.
- Network Security Policy: e.g. IPsec and IKE policy, firewall policy.
- Access control (packet filtering, etc.) and network admission control (e.g. for VoIP)
- Network Address Translation (NAT) Policy
- Multicast routing and session policy

However, for Phase 2 only Network Quality of Service will be addressed. The remainder will be deferred to Phase 3 or beyond.

2.1.1 Definition of connectivity management

Connectivity Management is:

- A set of functions which provide configuration and control of both the attributes of IP connectivity and policies governing IP connectivity, within and between IP domains. Such attributes include QoS, security and routing policy.
- The interfaces made available to management applications used to configure, monitor and control the network.
- The interfaces used to enable cross-domain services. These functions can be invoked through a number of open interfaces, including APIs used by management applications, control protocol interfaces to the IP network, and control interfaces to peer functions in other domains.
- The mechanisms and interfaces needed to provide interoperability and to control equipment from multiple vendors.

For Phase 2, the definition for Connectivity Management is restricted to the interface made available for configuring and controlling Provisioned Quality of Service policies.

2.1.2 Clients of Connectivity Management

There are numerous possible clients of connectivity management. These clients are the requestors of network connectivity or connectivity attributes, and may be end users, applications, or other platform components. In many cases, users of IP network services may not directly call the connectivity management but would rely on other entities, such as a network administrator.
Possible clients of Connectivity Management include, but are not limited to:

- Configuration Applications: Customer or Third Party applications
- Connectivity Management functions in customer networks

2.1.3 Control of Provider IP QoS

This functional area allows applications to control QoS attributes of IP connectivity across a provider domain. This includes a number of functional areas, including the control, configuration and customization of provider QoS services (for example, IP Virtual Leased Line Services)
As such, these APIs are intended to be complementary to existing QoS APIs such as end-station RSVP and DiffServ APIs. The functional area envisaged here enables network administrators, network management applications and QoS agents to interact with provider IP QoS capabilities. One of the main purposes of opening this interface to users and applications in customer or peer domains is to allow the capability of dynamic creation of IP QoS connectivity or QoS policies at the network layer.

3.0 Service Interface: Connectivity Management

This section details the requirements for the interface to the Connectivity Management service. In particular, Phase 2 requirements are focused on provisioned Quality of Service (QoS). The provisioned QoS functions are typically invoked by an enterprise network operator to manage an enterprise network. The enterprise network may include multiple networks; for example local site networks interconnected via a core network (such as WAN, ATM).

The Connectivity Management service for Phase 2 supports functions to permit the enterprise network operator to provision specific Quality of Service (QoS) parameters, as specified in service level agreements with the underlying local/core network providers. As QoS parameters may differ depending on the underlying network technology, e.g. PSTN, IP, or ATM, network operators should be able to define QoS parameter as appropriate for each technology.

The requirements are given in a numbered format, and all connectivity management requirements are denoted as *CM.*

Each requirement has a *name*, a *description*, and identifies *information* (information elements) associated with that requirement. The requirements are defined in terms of requests and indications - indications usually being the result of a previous request. The entity supplying the request or indication is identified as the *invoker.*

Connectivity Management Requirements

CM – 1.1. Identifying End Point(s)

Invoker: Client Application (Enterprise Network Operator)

Description: End point is a component that can be used to identify a specific flow through the network. The network is provisioned by the Enterprise Network Operator to support a specific QoS level for that flow. End point can be a source or destination end point. Source and destination end points of a flow can be used to identify the specific flow.

Source or destination end points are defined by a network address. Source or destination end points may be comprised of single network address, a range of network addresses, or ANY network address. Disjoint network addresses comprising various flows can be grouped together to create one flow to receive the same service level. The network address component that identifies an end point should be specified in such a way that enables accommodating different address structures, such as IPv4, IPv6, or ATM, that could be used by different networks.

End points can be assigned names (string of characters) by the enterprise operator. This is to enable defining flows using descriptive end point components (pertaining to physical or virtual structures) that are meaningful to network operator, such as domains, organization units, sites, hosts, or users. These descriptive components can be used by the enterprise operator to identify flows, instead of using network addresses. In addition, if there are elements in a specific communication protocol that can identify attributes of a flow, they should be included in the definition of the component. The information stored for each such component may include information used by the

network operators but not necessarily required to provision the network, such as telephone number for a user component, or city name and zip code for a site component.

Information: Type of network

Network addresses

Descriptive components associated with network addresses

Attributes of the descriptive components

CM - 1.2. Identifying Communications Protocol(s)

Invoker: Client Application (Enterprise Network Operator)

Description: Communication protocol is a type of component that can be used to identify a specific flow through the network. The network is provisioned by the Enterprise Network Operator to support a specific QoS level for that flow. Protocol ID is used to identify a specific communication protocol. The network operator should be able to use protocol IDs from various networks (e.g., IP networks), each of which may have a different list of supported protocols and associated IDs.

Specific protocols can be assigned names (string of characters) by the enterprise operator. This is required to enable defining flows using descriptive protocol names that are meaningful to the network operator, such as World Wide Web protocol. These descriptive names, instead of protocol IDs, can be used by the network operator to identify flows. It should be possible to group a set of protocols under one descriptive name, that can be used again as a component to identify a specific flow that receives a certain level of service.

Information: Network type

Protocol and group of protocols

Protocol ID

CM - 1.3. Identifying Application(s)

Invoker: Client Application (Enterprise Network Operator)

Description: An application on the generating or receiving side of a traffic flow, is a type of component that can be used to identify a specific flow through the network. The network is provisioned by the Enterprise Network Operator to support a specific QoS level for that flow. Application ID is used to identify a specific application as its packets flow through the network. The network operator should be able to use Application IDs from various networks (e.g., port numbers in IP networks), each of which may have a different list of supported applications and associated IDs.

Specific applications can be assigned names (string of characters) by the enterprise operator. This is required to enable defining flows using descriptive application names that are meaningful to network operator, such as NetShow Video or RealVideo. These descriptive names,

instead of Application IDs, can be used to identify flows. It should be possible to group applications and name the group with a descriptive name as well (e.g., "Video" that includes NetShow and RealVideo application streams).

Information: Network type

Application or group of applications

Application ID

CM - 1.4. Identifying Flow(s)

Invoker: Client Application (Enterprise Network Operator)

Description: Required Service levels are applied to pre-specified flows traveling through the network. A flow is identified by the following flow components: end point component(s), protocol component(s), and application component(s). A flow is an aggregate of any number of these components.

Specific flow(s) can be assigned names (string of characters) by the enterprise operator, to enable identifying flows using descriptive names that are meaningful to the network operator, such as "CEO video conferencing". It should be possible to group flows and name the group with a descriptive name as well (e.g., "research department flow").

Information: Flow or group of flows

Components comprising a flow

CM - 1.5. Setting Policy Rule Conditions

Invoker: Client Application (Enterprise Network Operator)

Description: Policy condition is a component of policy rules (see setting policy rules). Policy condition contains flow components. The policy conditions are included in logical expressions, which must evaluate to "TRUE" in order for an associated action to be triggered. [For example, it should support a structure where the following can be articulated: "If (*condition A* AND *condition B*) OR (*condition C* AND *condition D*) then. action *E*"; in this case satisfying conditions A and B (subset of conditions A, B, C, and D) is sufficient to trigger action E.]

Specific conditions can be assigned names (string of characters) by the enterprise operator, to enable identifying conditions using descriptive names that are meaningful to network operator, such as "Issuing IPO". These descriptive names can be used to set up conditions. It should be possible to group conditions and name the group with a descriptive name as well.

Information: Condition or group of conditions

Flow(s)

CM - 1.6. Setting Time of Day Triggers

Invoker: Client Application (Enterprise Network Operator)

Description: Time of day trigger is a component of policy rules (see setting policy rules). When conditions of the policy rule are met and the time of day specified in a policy rule is current, the action specified for the policy rule is activated. It is required to specify the time of day trigger to accommodate any time of the day, any day of the week, any year (four digits), with facilities to set up recurring events.

Specific time of day events can be assigned names (string of characters) by the enterprise operator, to enable identifying conditions using descriptive names that are meaningful to network operator, such as "Every Monday 1:00PM". These descriptive names can be used to set up time of day triggers. It should be possible to group such events and name the group with a descriptive name as well.

Information: Time of day triggers(s)

CM - 1.7. Setting Policy Rules

Invoker: Client Application (Enterprise Network Operator)

Description: Policy rules are composed of conditions, time of day triggers, and actions. If conditions and time of day requirements are met, then the action is applied to network elements that provide the required service level for the specific flow(s).

Specific policy rules events can be assigned names (string of characters) by the enterprise operator, to enable identifying conditions using descriptive names that are meaningful to the network operator, such as "Gold Service". It should be possible to group policy rules and name the group with a descriptive name as well.

Information: Conditions or group of conditions

Time and day triggers

Action(s)

CM - 1.8. Setting Policy Rule Actions

Invoker: Client Application (Enterprise Network Operator)

Description: Action is a component of a policy rule (see preceding requirement). Policy rule action operates on network elements to provide certain service levels to certain flows. The actions supported should include marking packets (that belong to a pre-specified flow) with specific codes in the Type-Of-Service (TOS) field so that DiffServ enabled network elements can provide the required service levels. Codes that are associated with these marks can also be associated with a Traffic Class. The actions should support traffic conditioning as specified by a traffic descriptor, including pre-specified burst rate, peak rate, packet loss, packet delay, treatment to flow when it exceeds traffic description, bandwidth sharing, assigning priorities to certain flows. Traffic class

can be associated with a traffic descriptor. In addition, actions should include denying / accepting inbound traffic and transmitting, dropping, or remarking outbound traffic.

Specific actions can be assigned names (string of characters) by the enterprise operator, to enable creating policy rules that are meaningful to the network operator, such as “deny Web traffic”. It should be possible to group policy rules and name the group with a descriptive name as well. When actions are grouped together in a group, either all the actions in that group are performed (when conditions are met) or none (i.e., logic AND grouping).

Information: Conditions or group of conditions

Time and day triggers

Action(s)

CM - 1.9. Grouping Policy Rules Components

Invoker: Client Application (Enterprise Network Operator)

Description: As specified for each of the components of policy rules, some components can be grouped together in a group. Such a group can be named using a descriptive name as chosen by the network operator. Operations to add, remove, modify, and list the group members should be supported.

Information: New member

Current member

CM - 1.10. Enable Disable Policy Rule Components

Invoker: Client Application (Enterprise Network Operator)

Description: Any single or a group of policy rule components can be set to an enabled or disabled state. This feature enables the enterprise network operator to remove and add “active” conditions and “active” actions from a policy rule without physically removing or adding the rules in the policy database. This is used as a designing tool that can be used by the network operator to stage rules without yet committing them for action, or putting portions of rules in the rule database, and only when complete activate the rules.

Information: Enable

Disable

3GPP TSG_CN WG5#5 **Tdoc N5-000183**
Bristol, UK
5th-7th of September 2000.

Source:	**TSG CN WG5**
To:	**TSG SA WG1 (OSA ADHOC GROUP)**
Title:	**Liaison Statement to S1 on the concept of Enterprise Operator**
Contact:	**Richard Stretch (richard.stretch@bt.com)**

1.0 Introduction

During the last CN5 meeting in Bristol, the group reviewed their documentation in regards to the Release 2000 specifications. The group would like S1 to review and consider as additions to their Requirements for Release 2000 the Concept of Enterprise Operator (effectively being an enterprise that acts as a negotiator between a number of Service Providers and Network Operators).
CN5 have attached the following relevant text from the Parlay 2.1 Framework specification on the Enterprise Operator.

Description of the Enterprise Operator

Attachment

In the model, the enterprise operators act in the role of *subscriber/customer* of services and the client applications act in the role of *users or consumers* of *services*. The framework itself acts in the role of *retailer* of services. The following example illustrates these roles:

Service (to be subscribed): Call Center Service, Mobility Service, etc.

Framework Operators

Enterprise Operator: A Financial institution such as a Bank or Insurance Company (Such an enterprise has a conformant Subscription Application in its domain which "talks" to its peer in the Framework).

User/Consumer: Client Applications (or their associated users) in the enterprise domain that use the Call Center Service or the Mobility Service.

The Service Subscription interface is used by an enterprise operator to subscribe to new services and is done before a client application of the enterprise can use the new service. In general, the service subscription is performed after an off-line negotiation of a set of services and the associated price between the framework operator and the enterprise operator. The service subscription is performed online by the enterprise operator in the frame of an existing off-line negotiated contract between the framework operator and the enterprise. The on-line service subscription function is used for subscriber, client application, and service contract management. The following section describes a service subscription model.

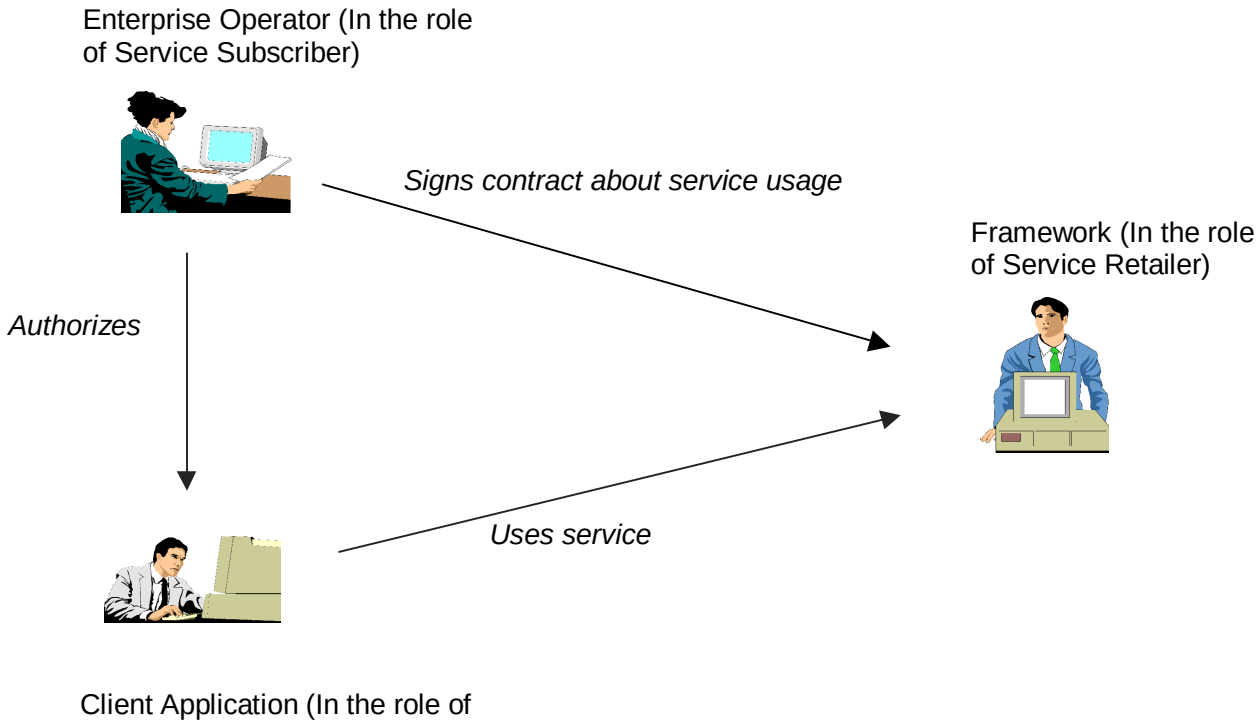

Figure 1 – Enterprise Operator

The enterprise operator provides to the Framework the data about the client applications in its domain and the type of services each of them should be allowed access to using the subscription interfaces offered by the Framework. The Framework provides (to the enterprise operator) the subscription interfaces for subscriber, client application and service contract management. This gives the enterprise operators the capability to dynamically create, modify and delete, in the framework domain, the client applications and service contracts belonging to its domain.