

netconf Working Group  
INTERNET-DRAFT  
Document: [draft-boucadair-netconf-req-00.txt](#)  
Category: Informational  
Expires January 2005

M. Boucadair  
C. Jacquenet  
M. Achemlal  
Y. Adam  
France Telecom  
July 2004

## Requirements for Efficient and Automated Configuration Management <[draft-boucadair-netconf-req-00.txt](#)>

### Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at

<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at

<http://www.ietf.org/shadow.html>.

### Abstract

Given the ever-increasing importance of configuration tasks for the provisioning of a wide range of IP resources, networks, and services in today's Internet, this draft aims at listing the basic requirements that should drive the specification of a protocol to convey configuration information towards network devices. This memo doesn't aim at listing candidate protocols to convey such information, nor at choosing one of these. This draft basically describes a whole set of issues a service provider has to deal with, hence a list of requirements to better address such issues.

### Table of Contents

|                    |                   |                   |
|--------------------|-------------------|-------------------|
| <a href="#">1.</a> | Introduction..... | <a href="#">3</a> |
|--------------------|-------------------|-------------------|

|                    |  |                   |
|--------------------|--|-------------------|
| <a href="#">2.</a> | Conventions used in this document..... | <a href="#">3</a> |
| <a href="#">3.</a> | Terminology.....                       | <a href="#">3</a> |
| <a href="#">4.</a> | Motivations and Goals.....             | <a href="#">5</a> |

|                            |  |                    |
|----------------------------|--|--------------------|
| <a href="#">5.</a>         | Positioning this Draft within the NETCONF Working Group.....       | <a href="#">5</a>  |
| <a href="#">6.</a>         | Current Issues with Configuration Procedures.....                  | <a href="#">6</a>  |
| <a href="#">6.1.</a>       | Protocol Diversity.....  | <a href="#">6</a>  |
| <a href="#">6.2.</a>       | Topology Discovery.....  | <a href="#">6</a>  |
| <a href="#">6.3.</a>       | Device capabilities discovery.....                                 | <a href="#">6</a>  |
| <a href="#">6.4.</a>       | Impact on the performance.....                                     | <a href="#">7</a>  |
| <a href="#">6.5.</a>       | Scalability.....   | <a href="#">7</a>  |
| <a href="#">6.6.</a>       | Automation.....  | <a href="#">7</a>  |
| <a href="#">6.7.</a>       | Security issues.....   | <a href="#">8</a>  |
| <a href="#">7.</a>         | Towards a Service-Oriented Configuration Policy.....               | <a href="#">8</a>  |
| <a href="#">8.</a>         | Requirements.....  | <a href="#">9</a>  |
| <a href="#">8.1.</a>       | Protocol Requirements.....   | <a href="#">9</a>  |
| <a href="#">8.1.1.</a>     | Functional Requirements.....                                       | <a href="#">9</a>  |
| <a href="#">8.1.2.</a>     | Performance requirements.....                                      | <a href="#">10</a> |
| <a href="#">8.1.3.</a>     | Backward Compatibility.....  | <a href="#">10</a> |
| <a href="#">8.2.</a>       | Information requirements.....                                      | <a href="#">10</a> |
| <a href="#">8.2.1.</a>     | Network services.....  | <a href="#">11</a> |
| <a href="#">8.2.1.1.</a>   | Identification of Interfaces.....                                  | <a href="#">11</a> |
| <a href="#">8.2.1.2.</a>   | Quality of Service (QoS).....                                      | <a href="#">12</a> |
| <a href="#">8.2.1.3.</a>   | Security.....  | <a href="#">12</a> |
| <a href="#">8.2.1.4.</a>   | Applications.....  | <a href="#">12</a> |
| <a href="#">8.2.2.</a>     | Forwarding services.....   | <a href="#">13</a> |
| <a href="#">8.2.2.1.</a>   | Routing and Forwarding Configuration Information.....              | <a href="#">13</a> |
| <a href="#">8.2.2.2.</a>   | Traffic Engineering Configuration Information.....                 | <a href="#">13</a> |
| <a href="#">8.2.2.3.</a>   | Configuration Information for Tunnel Design and<br>Activation..... | <a href="#">13</a> |
| <a href="#">8.2.2.4.</a>   | Tunnel Identification Information.....                             | <a href="#">14</a> |
| <a href="#">8.2.2.5.</a>   | Tunneling Protocol Configuration Information.....                  | <a href="#">14</a> |
| <a href="#">8.2.3.</a>     | Management services.....   | <a href="#">14</a> |
| <a href="#">8.2.3.1.</a>   | Fault Management.....  | <a href="#">14</a> |
| <a href="#">8.2.3.2.</a>   | Configuration Management.....                                      | <a href="#">14</a> |
| <a href="#">8.2.3.3.</a>   | Performance Management.....  | <a href="#">15</a> |
| <a href="#">8.2.3.4.</a>   | Security Management.....   | <a href="#">15</a> |
| <a href="#">8.2.3.4.1.</a> | Device Authentication.....   | <a href="#">15</a> |
| <a href="#">8.2.3.4.2.</a> | Integrity of configuration information.....                        | <a href="#">15</a> |
| <a href="#">8.2.3.4.3.</a> | Confidentiality of exchanged data.....                             | <a href="#">15</a> |
| <a href="#">8.2.3.4.4.</a> | Key management.....  | <a href="#">16</a> |
| <a href="#">8.2.3.4.5.</a> | Log of connections.....  | <a href="#">16</a> |
| <a href="#">8.2.3.4.6.</a> | Profiles.....  | <a href="#">16</a> |
| <a href="#">9.</a>         | Security Considerations.....                                       | <a href="#">16</a> |

|                     |                         |                    |
|---------------------|-------------------------|--------------------|
| <a href="#">10.</a> | References.....         | <a href="#">16</a> |
| <a href="#">11.</a> | Acknowledgments.....    | <a href="#">17</a> |
| <a href="#">12.</a> | Authors' Addresses..... | <a href="#">17</a> |

## [1.](#) Introduction

In today's Internet, configuration procedures are achieved by technical personnel who's required an ever-growing level of expertise because of the various technologies and features that need to be used, configured and activated to deploy a wide range of IP service offerings. This level of expertise has become mandatory as each equipment manufacturer has developed its own interfaces and configuration schemes. In addition, as IP services may rely upon the activation of a set of sophisticated yet complex features, the time to adequately provision such services is also increasing.

As a consequence, the specification and the use of standardized protocol (for conveying configuration information) and interfaces SHOULD dramatically help in facilitating if not automating the configuration process and the operational production of a wide range of IP services.

This draft aims at describing basic requirements for configuration task purposes, from a service provider perspective.

This document is structured as follows:

- [Section 3](#) introduces some terminology that is used by this document
- [Section 4](#) presents the goals and motivations of this draft
- Sections [5](#) position this draft within the current netconf working group initiative.
- [Section 6](#) summarizes important issues that are related to configuration tasks in today's IP networks.
- [Section 7](#) discusses the importance of introducing a service-

- oriented configuration scheme.
- [Section 8](#) lists configuration information and protocol requirements.

## [2.](#) Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [2].

## [3.](#) Terminology

This section aims at providing a set of basic definitions for the terms that will be used by this document.

- . Decision point: is an entity that is responsible for generating decisions related to configuration tasks that yield the production of configuration data which needs to be conveyed

towards (and processed by) a participating device.

- . Endpoint: one of the extremities of a tunnel.
- . Participating device: any networking equipment that will participate in the establishment, the activation and the maintenance of a given network service. Such devices may include routers and hosts, whatever the configuration procedures and underlying technologies to be used for the deployment of such service.
- . Subscriber: A subscriber (or a customer) is a legal representative who has the (legal) ability to subscribe to a service offering.
- . Tunnel activation: the configuration tasks that position a tunnel facility into an activated state, so that it can be used to convey traffic. Obviously, a tunnel must not (and, hopefully, cannot) be activated before it has been established.
- . Tunnel establishment: all the configuration tasks that lead to the configuration of a tunnel facility. Once the tunnel is established, it needs to be activated in order to be able to convey traffic.

- . Tunnel maintenance: the period of time during which a tunnel facility remains activated.
- . Tunnel: a tunnel is a transport facility that is designed to convey' (IP) data traffic between one endpoint and another (point-to-point tunnels), or between one endpoint and several others (point-to-multipoint tunnels). Tunnels can be used for different purposes, e.g.:
  - Access IP multicast networks over IP clouds that do not support multicast forwarding capabilities,
  - Access IPv6 networks over IPv4 clouds,
  - Deploy IP Virtual Private Networks,
  - Deploy Mobile IP architectures.
- . User: A user is an entity (a human being or a process, from a general perspective) who has been identified (and possibly authenticated) by a service provider, and who will access this service offering according to his associated rights and duties.
- . VPN: Virtual Private Network. A collection of switching resources (e.g. routers) and transmission resources that will be used over an IP backbone thanks to the establishment and the activation of tunnels. These tunnels will convey the IP traffic that characterizes the data oriented-communication service of a customer (VPNs that are designed to support intranet-based

applications) or a set of customers (VPNs that are designed to support extranet-based applications). Thus, IP VPN networks are an applicability example of tunnel configuration and management activities.

#### 4. Motivations and Goals

Operators and protocol developers have gained experience to implement, deploy and manipulate a large set of protocols and associated information. Some data models have also been defined for network management purposes. Thus, several protocols have been standardized, such as SNMP (Simple Network Management Protocol, [RFC 3410](#)([3])), COPS (Common Open Policy Service, [RFC 2748](#)([4])), (COPS-PR, [RFC 3084](#)([5])). Multiple data models have been defined and used by operators like: CIM (Core information model, [6]), DEN (Directory enabled Network), SMI (Structure of Management Information, [7]),

SPPI (Structure of Policy Provisioning Information, [8]), MIB (Management Information Base), PIB (Policy Information Management)à

Despite this standardization effort, some operators and standardization bodies address a negative report ([RFC3535](#)) about the capacity of existing tools to deal with operator's requirements about network management and configuration operations.

The purpose of this document is to clarify what are such requirements from a configuration task perspective. This initiative also aims at gathering any feedback from other service providers or vendors in order to agree on a common yet consolidated set of requirements, which SHOULD dramatically help in facilitating if not automating the configuration process and the operational production of a wide range of IP services.

## [5.](#) Positioning this Draft within the NETCONF Working Group

In mid-2003, the IETF netconf (Network Configuration) working group has been set up. The main objective of netconf is to produce a protocol suitable for network configuration. A proposal to use XML (Extensible Markup Language) for configuration purposes has been adopted. The choice of this technology hasn't been motivated nor discussed by some formal document yet.

For instance, neither an analysis of existing configuration-based protocols nor a requirement draft have been published. Therefore, there is no explicit consensus about this technical choice (possibly an implicit consensus between some netconf WG members). Because of the lack of guidance documents (framework and requirement documents) and also of a clear view on the actual requirements, the netconf working group may experience some difficulties to make the Internet community widely adopt its ongoing protocol specification effort.

## [6.](#) Current Issues with Configuration Procedures

This section aims at listing issues that SHOULD be carefully studied when dealing with configuration tasks. The items below SHOULD be taken into account when designing a protocol for configuration purposes.

### [6.1.](#) Protocol Diversity

The production of a whole set of IP yet complex services relies upon the activation of a set of capabilities in the participating devices. Especially, a large set of protocols need to be configured, such as routing protocols, management protocols, security protocols, not to mention capabilities that relate to addressing scheme management, QoS policy enforcement, etc.

Such a diversity of features and protocols MAY increase the risk of inconsistencies. Therefore, the configuration information which is forwarded to the whole set of participating devices for producing a given service or a set of services SHOULD be consistent, whatever the number of features/services to be activated/deployed in the network.

### [6.2.](#) Topology Discovery

Network operators SHOULD have means to dynamically discover the topology of their network. This topology information should be as elaborate as possible, including details like: the links that connect network devices, including information about their capacity, such as the total bandwidth, the available bandwidth, the bandwidth that can be reserved, etc.

### [6.3.](#) Device capabilities discovery

As stated above a large number of participating devices are involved in deploying and offering IP-based services. These devices could vary depending on the following:

- The manufacturer in charge of designing these devices
- The version of operating system of the devices
- The supported protocols
- Configuration tools
- Others

As a result, it isn't evident to have homogenous capabilities and means to activate similar functionalities in two participating devices. Therefore, operators SHOULD have means to (1) detect the capabilities, (2) have an exhaustive description and (3) list activated process and functions of a given of participating devices.

This COULD be done automatically or in demand.

#### 6.4. Impact on the performance

Configuring network devices and IP services is a human task, and occurrences of erroneous configurations are therefore plausible. Such occurrences MAY seriously affect the overall quality of a service, like the access to a service or its global availability. From this perspective, some performance indicators SHOULD be defined and measured to qualify:

- The impact of any modification of an operational configuration, in terms of performances,
- The time needed to deliver and achieve any elementary configuration task.

Simulation tools can also be useful to qualify any possible impact of an elementary configuration task before such task is performed.

#### 6.5. Scalability

As far as scalability is concerned, adequate indicators SHOULD be specified in order to qualify the ability of a given technical means to support a large number of configuration processes. The maintenance of these processes SHOULD not impact the performance of a given system (a system is a set of elements that compose the key fundamentals of an architecture that aims at delivering configuration data).

Therefore, configuration operations SHOULD be qualified with performance indicators in order to check whether the architecture designed for configuration management is scalable in terms of:

- Volume of configuration data to be processed per unit of time and according to the number of capabilities and devices that need to be configured,
- Volume of information generated by any reporting mechanism that may be associated to a configuration process,
- Number of processes that are created in order to achieve specific configuration operations,

#### 6.6. Automation

The efficiency of a configuration process SHOULD be enhanced by the introduction of the highest level of automation when performing configuration tasks.

Automation is defined as follows:



- Automatic provisioning of configuration information to the participating devices,
- Dynamic enforcement of configuration policies,
- Dynamic reporting mechanisms to notify about the actual processing of configuration information by a participating device.

#### [6.7.](#) Security issues

Configuring a network or a service raises several security issues that need to be addressed, such as:

- The integrity of the configuration information, possibly yielding the preservation of the confidentiality of such information when being conveyed over a public IP infrastructure,
- The need for authorizing and authenticating devices/entities that have the ability of manipulating configuration information (define, instantiate, forward and process).
- Mutual authentication between a decision point and a device that will receive configuration data

In addition, additional configuration data SHOULD NOT yield additional security lacks.

### [7.](#) Towards a Service-Oriented Configuration Policy

Current configuration practice basically focuses on elementary functions, i.e. configuration management for a given service offering is decomposed in a set of elementary tasks. Thus, the consistency of configuration operations for producing IP services MUST be checked by any means appropriate, while current. Configuration methods can, at best, only check if provisioning decisions are correctly enforced by a single device.

A network device SHOULD be seen as a means to deploy a service and not just as a component of such service. Thus, service configuration and production techniques SHOULD NOT focus on a set of devices taken one-by-one, but on the service itself, which will rely upon a set of

features that need to be configured and activated in various regions of the network that supports such service.

Service providers could dedicate centralized entities that will be responsible for the provisioning and the management of participating devices. The main function of these centralized entities is to make appropriate decisions and generate convenient configuration data that will be delivered to the participating devices. In addition, these

centralized entities will make sure of the consistency of the decisions that have been taken to produce the service, as per a dynamic configuration policy enforcement scheme.

Service-oriented configuration SHOULD rely upon the following requirements:

- The data models MUST be service-oriented;
- The configuration protocol(s) SHOULD at large extent possible reuse existing data and information models;
- The configuration protocol(s) SHOULD be open for further enhancement and adding new functionalities that could reveal in the future as a must;
- The configuration protocol(s) SHOULD provide means to validate the consistence and the validation of service configuration

## [8. Requirements](#)

### [8.1. Protocol Requirements](#)

Configuration information SHOULD be provided to the participating devices by means of a communication protocol that would be used between the aforementioned participating devices and a presumably centralized entity that would aim at storing, maintaining and updating this configuration information as appropriate, as well as making adequate decisions at the right time and under various conditions.

#### [8.1.1. Functional Requirements](#)

The vendor-independent communication protocol for conveying configuration information SHOULD have the following characteristics:

1. The protocol SHOULD use a reliable transport mode, and independent

from the network layer (i.e. IPv4/IPv6),

2. The protocol architecture SHOULD provide a means for dynamically provision the configuration information to the participating devices, so that it may introduce a high level of automation in the actual negotiation and invocation of a whole range of IP service offerings.
3. The protocol SHOULD provide the relevant means (encoding capabilities, operations and command primitives, extension capabilities that SHOULD allow additional operations, etc.) to be able to reliably convey any kind of configuration information,
4. The protocol SHOULD be a privileged vector for the dynamic provisioning of any kind of configuration data, as well as the dynamic enforcement of any kind of policy such as a routing

policy, a QoS policy and/or a security policy. This requirement MAY yield the definition and the support of vendor-independent instantiation procedures that will aim at uniquely identifying the configuration data model and/or the policy enforcement scheme that refer to a given IP service offering.

5. The protocol SHOULD support a reporting mechanism that may be used for statistical information retrieval,
6. The protocol SHOULD support the appropriate security mechanisms to provide guarantees as far as the preservation of the confidentiality of the configuration information is concerned.
7. The protocol SHOULD support a notification mechanism that may be used to initiate configuration-related tasks (i.e. inform that a link drop down)

#### [8.1.2](#). Performance requirements

The protocol architecture for conveying configuration information within a network SHOULD be designed so that:

1. The activation of the protocol by the participating devices SHOULD not affect the overall switching performances of such devices, whatever the volume of configuration data these devices will have to process on a given period of time,

2. The activation of the protocol SHOULD NOT dramatically affect the global resources of the network infrastructure that will convey the protocol-specific traffic, whatever the volume of such traffic and whatever the scope (set of IP service offerings the configuration data refer to, set of policies to dynamically enforced, etc.) covered by such traffic.

#### 8.1.3. Backward Compatibility

The introduction and the activation of a protocol for conveying configuration data SHOULD allow for smooth migration procedures, so that vendor-specific and vendor-independent configuration procedures and management MAY gracefully co-exist on a (hopefully) limited period of time.

Also, in case of any kind of protocol failure, it MUST be possible to rely upon any vendor-specific configuration procedure to keep on performing configuration tasks without any risk of disruption that may affect the availability of a (set of) service offerings, and/or the access to network resources.

#### 8.2. Information requirements

The increase of network service offerings, of the protocol amount to be implemented by equipment as well as the diversity of vendors made the configuration tasks being critical. These tasks are commonly achieved with vendor-specific solutions that deal with device-related information. Moreover the configuration information may be spread across different repositories through the network. It then becomes more and more difficult for the service provider to get a unified (and obviously confident) view of its network in term on offered services rather than a network device jigsaw.

Configuration information SHOULD therefore be provided to the participating devices as unified service parameters being independent from the aforementioned devices vendors. These parameters MUST relate to a standardized service model rather than device-specific as it used to be. Examples of the so-called service model may be tunneling service, internal routing service, VPN service. Their definition is outside the scope of this draft.

Current service providers' concerns focus on the unification of

accesses to heterogeneous devices (those that are part of a multi-vendor environment) and introduce a high level of automation when achieving configuration of this infrastructure. This unification depends on two major issues, the definition of a protocol (the container) and the definition of data models (the content). Standardizing these two points bring new opportunities:

- Equipment are seen as functional blocks providing a set of standardized capabilities;
- These functional blocks are described as vendor-independent capabilities;
- These functional blocks are all managed homogeneously, whatever the underlying technology;

As a result, it would be possible to add semantic rules to automate detection and correction of false configurations, either at the scale of a single device or at the scale of a whole network. Furthermore, an equipment from vendor X could be replaced by another device from vendor Y with no impact on the configuration management.

To do so, the data models SHOULD satisfy the requirements described below.

#### [8.2.1.](#) Network services

##### [8.2.1.1.](#) Identification of Interfaces

Configuration information that relates to identification deals with the namespace of the interfaces of a network equipment. This naming scheme describes the properties of an interface, and must take into

account all the parameters that are required to correctly configure an interface. The following information MUST be provided:

A name, with a generic syntax not related to a specific vendor. The name can define the media type of the interface;  
Depending on the media type, further information MAY be added (link mode, MTU, speed...);

- Optionally, a logical descriptor. Depending on the media type it can be relevant to have a logical descriptor (for VLANs declared on Ethernet interfaces, for instance). In this case

the encapsulation type must be provided;

- Optionally, a description field giving general information about the interface (i.e. 00C192 link from LA to SFö)

#### [8.2.1.2. Quality of Service \(QoS\)](#)

IP services are provided with a level of quality that MAY be guaranteed (either qualitatively or quantitatively) by any means appropriate. QoS policies SHOULD be dynamically enforced according to a data model that will accurately reflect all the elementary QoS capabilities that MAY be configured and activated to enforce such policies.

For instance, in the case of the activation of the DiffServ QoS model within a network infrastructure, the participating routers should be provided with the appropriate parameters.

#### [8.2.1.3. Security](#)

The protocol architecture MUST provide security functions that provide source authentication, integrity and confidentiality of configuration information. The security functions MUST be activated, whatever the contents of the payload.

In order to protect device accesses, the configuration architecture MUST provide a filtering / fire-walling access scheme that would allow to control remote and in-band accesses (i.e. console security rules, access lists)

#### [8.2.1.4. Applications](#)

Network devices usually run network functions that allow activation of specific services, like HTTP, BOOTP, DHCP, SYSLOG ... Such devices must therefore be provided with the relevant information related to these services:

- the ability to enable or disable the service;
- the mandatory parameters for each of the service.

#### [8.2.2. Forwarding services](#)

#### [8.2.2.1](#). Routing and Forwarding Configuration Information

Routing and forwarding configuration information deals with the decision criteria that should be taken by a participating device to forward an incoming IP datagram, according to a given routing policy. From this perspective, the participating devices should be provided with the following information:

- In the case of the activation of dynamic routing protocols for the computation and the selection of routes that will be considered for forwarding traffic, the participating routers SHOULD be provided with the relevant metric information so that the routers (dynamically) assign the metric values accordingly,
- In the case where the traffic is to be conveyed across domains, the participating devices should be provided with the relevant BGP-4 (Border Gateway Protocol, version 4)-based reachability information, including the BGP-4 attribute-related information that will be taken into account by the route selection process of the router to decide where to forward the corresponding traffic,
- Also, the participating routers should be provided with the configuration information related to any static route that may identify specific next hops to reach a given destination prefix.

#### [8.2.2.2](#). Traffic Engineering Configuration Information

Traffic engineering is an important task of configuration management: within this context, the participating devices should be provided with the configuration information that will help them to choose the appropriate routes that lead to a set of destinations, according to specific constraints.

These constraints may be expressed in terms of time duration (e.g. the use of a traffic-engineered route on a weekly basis), traffic characterization (e.g. all the IP multicast traffic should be conveyed by a specific route), security concerns (e.g. use IPsec [\[9\]](#) tunnels whenever possible), and/or QoS considerations (e.g. EF (Expedited Forwarding, [\[10\]](#))-marked traffic should always use a subset of activated and well-identified routes).

The enforcement of an IP traffic engineering policy would therefore yield the use of specific routes that will be dynamically computed and selected according to the aforementioned type of configuration information.

#### [8.2.2.3](#). Configuration Information for Tunnel Design and Activation

#### [8.2.2.4](#). Tunnel Identification Information

The identification of a tunnel should be globally unique, especially if the tunnel is to be established and activated across autonomous systems. The tunnel identification schemes (e.g. endpoint numbering) should be left to service providers, given that the corresponding formalism may be commonly understood, whatever the number of autonomous systems the tunnel may cross.

The tunnel identification information should at least be composed of the tunnel endpoint identification information. The tunnel identification information may also be composed of an informal description of the tunnel, e.g. the purpose of its establishment, the customer(s) who may use this tunnel, etc.

There may be cases where this additional information is irrelevant, e.g. in the case where the tunnel has been designed to convey public Internet traffic, where a user wishes to access IP multicast-based services through non-multicast capable clouds.

#### [8.2.2.5](#). Tunneling Protocol Configuration Information

Any participating device MUST be provided with the configuration information related to the tunneling technique to be used for the establishment and the activation of the tunnel. Such techniques include Generic Routing Encapsulation (GRE, [\[11\]](#)), IP Secure in tunnel mode (IPSec), Layer 2 Tunneling Protocol (L2TP, [\[12\]](#)), etc.

### [8.2.3](#). Management services

#### [8.2.3.1](#). Fault Management

Fault management is one of the critical points when managing a given service. Indeed, an operator MAY deploy means to detect fault occurring in its network and has pre-configured policies that SHOULD be enforced by participating devices to limit the impact on the quality of service.

Mechanisms to monitor and report the incidents that occurred to the service management SHOULD be independent of the configuration protocol.

#### [8.2.3.2](#). Configuration Management

Configuration management is responsible for the provisioning of configuration information to produce a service. Errors during a configuration procedure could impact the availability of a given service offering, while consistency checks are mandatory so as to



correctly enforce a configuration policy.

The following requirements have been identified:

- Data provisioning SHOULD be as automated as possible
- An operator SHOULD have means to detect and diagnose configuration errors
- An operator SHOULD deploy means to check the consistency of the configuration information forwarded to the participating devices, especially when a whole range of IP services can be delivered upon subscription requests.
- An operator MAY simulate the impact of the enforcement of a given configuration policy on its services before delivering such information to the participating devices.

#### [8.2.3.3](#). Performance Management

Performance management is mainly deals with the monitoring of the network and the status of the services.

The performance of a configuration policy/architecture will be studied in the next version of this draft.

#### [8.2.3.4](#). Security Management

##### [8.2.3.4.1](#). Device Authentication

It MUST be possible to activate mutual authentication between a participating device and a centralized entity that is responsible for instantiating and forwarding configuration data to these participating devices. The authentication MUST be checked before exchanging any configuration data to prevent DoS (Denial of Service) attacks.

##### [8.2.3.4.2](#). Integrity of configuration information

Two types of integrity MUST be provided. The first one MAY be done at the network layer, e.g. by using the IPsec protocol suite. It will protect each IP datagram, exchanged between a participating device and the configuration management platform(s), from malicious

modification. The second one SHOULD protect the configuration data at the application layer (e.g. the entire file configuration is integrity protected).

#### [8.2.3.4.3](#). Confidentiality of exchanged data

The participating device SHOULD provide security functions that provide confidentiality. The encryption algorithms MUST be selectable manually and/or automatically. The encryption algorithms MUST be the standard ones.

#### [8.2.3.4.4](#). Key management

The configuration system MUST provide a scalable key management scheme. The number of keys to be managed must be at most linearly proportional to the number of the devices.

#### [8.2.3.4.5](#). Log of connections

The participating device MUST log all configuration connections. At least the following information must be provided:

- Identity of the device which provided the configuration information,
- Date of the connection,
- Identity of the user that has launched the configuration process,
- Version of the configuration data has been enforced.

#### [8.2.3.4.6](#). Profiles

The configuration system MUST allow the definition and the activation of several privilege levels. Each level could be associated to a set of administrative functions. And each configuration administrator could be assigned a specific privileged access level to perform a (possibly limited) set of configuration tasks.

### [9](#). Security Considerations

This draft reflects a set of requirements as far as the design and

the enforcement of configuration policies are concerned for (automated) service subscription, delivery and exploitation. As such, the document addresses some security concerns that have been depicted in [section 9.2.3.5](#), and that SHOULD be taken into account when considering the specification of a protocol that will convey configuration information, as well as configuration information itself.

## [10](#). References

- [1] Bradner, S., "The Internet Standards Process -- Revision 3", [BCP 9](#), [RFC 2026](#), October 1996.
- [2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997

- [3] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", [RFC 3410](#), December 2002.
- [4] Boyle, J., Cohen, R., Durham, D., Herzog, S., Raja, R. and A. Sastry, "The COPS (Common Open Policy Service) Protocol", [RFC 2748](#), January 2000.
- [5] Chan, K., Durham, D., Gai, S., Herzog, S., McCloghrie, K., Reichmeyer, F., Seligson, J., Smith, A. and R. Yavatkar, "COPS Usage for Policy Provisioning (COPS-PR)", [RFC 3084](#), March 2001.
- [6] Distributed Management Task Force, "Common Information Model (CIM) Specification Version 2.2", DSP 0004, June 1999.
- [7] McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)", STD 58, [RFC 2578](#), April 1999.
- [8] McCloghrie, K., Fine, M., Seligson, J., Chan, K., Hahn, S., Sahita, R., Smith, A. and F. Reichmeyer, "Structure of Policy Provisioning Information (SPPI)", [RFC 3159](#), August 2001.

- [9] Atkinson R., "Security Architecture for the Internet Protocol", [RFC 2401](#), August 1998.
- [10] Davie, B., Charny, A., Bennett, J.C.R., Benson, K., Le Boudec, J.Y., Courtney, W., Davari, S., Firoiu, V. and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", [RFC 3246](#), March 2002.
- [11] Farinacci, D., et al., "Generic Routing Encapsulation (GRE)", [RFC 2784](#), March 2000.
- [12] Townsley, W., et al., "Layer Two Tunneling Protocol "L2TP"", [RFC 2661](#), August 1999.

## [11](#). Acknowledgments

## [12](#). Authors' Addresses

Mohamed Boucadair  
France Telecom R & D  
42, rue des Coutures  
14000 Caen,  
France  
Phone: 33 2 31 75 92 31  
Email: mohamed.boucadair@francetelecom.com

Boucadair et al. Informational - Expires January 2005

[Page 17]

---

Internet Draft      Network Configuration requirements

July 2004

Christian Jacquenet  
France Telecom Long Distance  
3 Avenue François Château  
35901 Rennes Cedex,  
France  
Phone: 33 2 99 87 63 31  
Email: christian.jacquenet@francetelecom.com

Mohammed Achemlal  
France Telecom R & D  
42, rue des Coutures  
14000 Caen, France  
Phone: 33 2 31 75 92 28  
Email: mohammed.achemlal@francetelecom.com

Yan Adam  
France Telecom R&D LANNION  
2 Avenue Pierre Marzin  
22307 Lannion Cedex  
France  
Phone: 33 2 96 05 29 19  
Email: yan.adam@francetelecom.com

## Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

