Network Working Group
Request for Comments: 3198
Category: Informational

A. Westerinen
J. Schnizlein
Cisco Systems
J. Strassner
Intelliden Corporation
M. Scherling
xCert
B. Quinn
Celox Networks
S. Herzog
PolicyConsulting
A. Huynh
Lucent Technologies
M. Carlson
Sun Microsystems
J. Perry
Network Appliance
S. Waldbusser
November 2001

Terminology for Policy-Based Management

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

This document is a glossary of policy-related terms. It provides abbreviations, explanations, and recommendations for use of these terms. The document takes the approach and format of RFC 2828, which defines an Internet Security Glossary. The intent is to improve the comprehensibility and consistency of writing that deals with network policy, particularly Internet Standards documents (ISDs).

Table of Contents

1. Introduction..... 2
2. Explanation of Paragraph Markings..... 3
3. Terms..... 3
4. Intellectual Property..... 16
5. Acknowledgements..... 17
6. Security Considerations..... 17
7. References..... 17
8. Authors' Addresses..... 19
9. Full Copyright Statement..... 21

1. Introduction

This document provides abbreviations, definitions, and explanations of terms related to network policy. All definitions are provided in Section 3, with the terms listed in alphabetical order.

The intent is to improve the comprehensibility and consistency of Internet Standards documents (ISDs) -- i.e., RFCs, Internet-Drafts, and other material produced as part of the Internet Standards Process [RFC2026]. Benefits across the ISDs are well-stated in the Introduction to RFC 2828 [RFC2828]:

- o "Clear, Concise, and Easily Understood Documentation" - Requires that the set of terms and definitions be consistent, self-supporting and uniform across all ISDs.

- o Technical Excellence - Where all ISDs use terminology accurately, precisely, and unambiguously.

- o Prior Implementation and Testing - Requires that terms are used in their plainest form, that private and "made-up" terms are avoided in ISDs, and that new definitions are not created that conflict with established ones.

- o "Openness, Fairness, and Timeliness" - Where ISDs avoid terms that are proprietary or otherwise favor a particular vendor, or that create a bias toward a particular technology or mechanism.

Common and/or controversial policy terms are defined. These terms are directly related and specific to network policy.

Wherever possible, this document takes definitions from existing ISDs. It should be noted that:

- o Expired Internet-Drafts are not referenced, nor are their terminology and definitions used in this document.

- o Multiple definitions may exist across the ISDs. Each definition is listed, with its source.

2. Explanation of Paragraph Markings

Section 3 marks terms and definitions as follows:

- o Capitalization: Only terms that are proper nouns are capitalized.

- o Paragraph Marking: Definitions and explanations are stated in paragraphs that are marked as follows:

- "P" identifies basic policy-related terms.

- "T" identifies various techniques to create or convey policy-related information in a network. For example, COPS and an "Information Model" are two techniques for communicating and describing policy-related data. SNMP and MIBs are another.

- "A" identifies specific Work Groups and general "areas of use" of policy. For example, AAA and QoS are two "areas of use" where policy concepts are extremely important to their function and operation.

3. Terms

Note: In providing policy definitions, other "technology specific" terms (for example, related to Differentiated Services) may be used and referenced. These non-policy terms will not be defined in this document, and the reader is requested to go to the referenced ISD for additional detail.

$ AAA
See "Authentication, Authorization, Accounting".

$ abstraction levels
See "policy abstraction".

$ action
See "policy action".

$ Authentication, Authorization, Accounting (AAA)
(A) AAA deals with control, authentication, authorization and accounting of systems and environments based on policies set by the administrators and users of the systems. The use of policy may be implicit - as defined by RADIUS [RFC2138]. In RADIUS, a network access server sends dial-user credentials to an AAA server, and receives authentication that the user is

who he/she claims, along with a set of attribute-value pairs authorizing various service features. Policy is implied in both the authentication, which can be restricted by time of day, number of sessions, calling number, etc., and the attribute-values authorized.

$ CIM
See "Common Information Model".

$ Common Information Model (CIM)
(T) An object-oriented information model published by the DMTF (Distributed Management Task Force) [DMTF]. It consists of a Specification detailing the abstract modeling constructs and principles of the Information Model, and a textual language definition to represent the Model. CIM's schemas are defined as a set of files, written in the language of the Specification, with graphical renderings using UML [UML]. Sets of classes and associations represent CIM's Core and Common Models, defining an information model for the "enterprise" - addressing general concepts (in Core), and

systems, devices, users, software distribution, the physical environment, networks and policy (in the Common Models). (See also "information model".)

$ Common Open Policy Service (COPS)
(T) A simple query and response TCP-based protocol that can be used to exchange policy information between a Policy Decision Point (PDP) and its clients (Policy Enforcement Points, PEPs) [RFC2748]. The COPS protocol is used to provide for the outsourcing of policy decisions for RSVP [RFC2749]. Another usage is for the provisioning of policy [RFC3084]. (See also "Policy Decision Point" and "Policy Enforcement Point".)

$ condition
See "policy condition".

$ configuration
(P) "Configuration" can be defined from two perspectives:
- The set of parameters in network elements and other systems that determine their function and operation. Some parameters are static, such as packet queue assignment and can be predefined and downloaded to a network element. Others are more dynamic, such as the actions taken by a network device upon the occurrence of some event. The distinction between static (predefined) "configuration" and the dynamic state of network elements blurs as setting parameters becomes more responsive, and signaling controls greater degrees of a network device's behavior.

- A static setup of a network element, done before shipment to a customer and which cannot be modified by the customer.

The first is the accepted usage in the Internet community.

$ COPS
See "Common Open Policy Service".

$ data model
(T) A mapping of the contents of an information model into a form that is specific to a particular type of data store or repository. A "data model" is basically the rendering of an information model according to a specific set of mechanisms for representing, organizing, storing and handling data. It has three parts [DecSupp]:
- A collection of data structures such as lists, tables, relations, etc.
- A collection of operations that can be applied to the structures such as retrieval, update, summation, etc.
- A collection of integrity rules that define the legal states (set of values) or changes of state (operations on values).

(See also "information model".)

$ DEN
See "Directory Enabled Networks".

$ Differentiated Services (DS)
(T) The IP header field, called the DS-field. In IPv4, it defines the layout of the ToS (Type of Service) octet; in IPv6, it is

the Traffic Class octet [RFC2474].
(A) "Differentiated Services" is also an "area of use" for QoS policies. It requires policy to define the correspondence between codepoints in the packet's DS-field and individual per-hop behaviors (to achieve a specified per-domain behavior). In addition, policy can be used to specify the routing of packets based on various classification criteria. (See also "Quality of Service" and "filter".)

$ diffserv
See "Differentiated Services".

$ Directory Enabled Networks (DEN)
(T) A data model that is the LDAP mapping of CIM (the Common Information Model). Its goals are to enable the deployment and use of policy by starting with common service and user concepts (defined in the information model), specifying their

mapping/storage in an LDAP-based repository, and using these concepts in vendor/device-independent policy rules [DMTF]. (See also "Common Information Model" and "data model".)

$ domain
(P) A collection of elements and services, administered in a coordinated fashion. (See also "policy domain".)

$ DS
See "Differentiated Services".

$ filter
(T) A set of terms and/or criteria used for the purpose of separating or categorizing. This is accomplished via single- or multi-field matching of traffic header and/or payload data. "Filters" are often manipulated and used in network operation and policy. For example, packet filters specify the criteria for matching a pattern (for example, IP or 802 criteria) to distinguish separable classes of traffic.

$ goal
See "policy goal".

$ information model
(T) An abstraction and representation of the entities in a managed environment, their properties, attributes and operations, and the way that they relate to each other. It is independent of any specific repository, software usage, protocol, or platform.

$ Management Information Base (MIB)
(T) A collection of information that can be accessed via the Simple Network Management Protocol. Management information is defined in MIB modules using the rules contained in SNMP's Structure of Management Information (SMI) specifications [RFC2570]. Management information is an abstract concept, and definitions can be created for high level policy specifications, low level policy, as well as technology and

vendor specific configurations, status and statistics. (See also "Simple Network Management Protocol" and "Structure of Management Information".)

$ MIB
See "Management Information Base".

$ MPLS
See "Multiprotocol Label Switching". (Also, MPLS may refer to Multi-Protocol Lambda Switching in optical networks. But, this is unrelated to policy and not discussed further in this document.)

$ Multiprotocol Label Switching (MPLS)
(T) Integrates a label swapping and switching framework with network layer routing [RFC2702]. The basic idea involves assigning short fixed length labels to packets at the ingress to an MPLS cloud. Throughout the interior of the MPLS domain, the labels attached to packets are used to make forwarding decisions (usually without recourse to the original packet headers).

$ outsourced policy
(P) An execution model where a policy enforcement device issues a query to delegate a decision for a specific policy event to another component, external to it. For example, in RSVP, the arrival of a new RSVP message to a PEP requires a fast policy decision (not to delay the end-to-end setup). The PEP may use COPS-RSVP to send a query to the PDP, asking for a policy decision [RFC2205, RFC2748]. "Outsourced policy" is contrasted with "provisioned policy", but they are not mutually exclusive and operational systems may combine the two.

$ PCIM
See "Policy Core Information Model".

$ PDP
See "Policy Decision Point".

$ PEP
See "Policy Enforcement Point".

$ PIB
See "Policy Information Base".

$ policy
(P) "Policy" can be defined from two perspectives:
- A definite goal, course or method of action to guide and determine present and future decisions. "Policies" are implemented or executed within a particular context (such as policies defined within a business unit).
- Policies as a set of rules to administer, manage, and control access to network resources [RFC3060].

Note that these two views are not contradictory since individual rules may be defined in support of business goals. (See also "policy goal", "policy abstraction" and "policy rule".)

$ policy abstraction
(P) Policy can be represented at different levels, ranging from business goals to device-specific configuration parameters. Translation between different levels of "abstraction" may require information other than policy, such as network and host parameter configuration and capabilities. Various documents and implementations may specify explicit levels of abstraction. However, these do not necessarily correspond to distinct processing entities or the complete set of levels in all environments. (See also "configuration" and "policy translation".)

$ policy action
(P) Definition of what is to be done to enforce a policy rule, when the conditions of the rule are met. Policy actions may result in the execution of one or more operations to affect and/or configure network traffic and network resources.
- In [RFC3060], a rule's actions may be ordered.

$ policy condition
(P) A representation of the necessary state and/or prerequisites that define whether a policy rule's actions should be performed. This representation need not be completely specified, but may be implicitly provided in an implementation or protocol. When the policy condition(s) associated with a policy rule evaluate to TRUE, then (subject to other considerations such as rule priorities and decision strategies) the rule should be enforced.
(T) In [RFC3060], a rule's conditions can be expressed as either an ORed set of ANDed sets of statements (disjunctive normal form), or an ANDed set of ORed sets of statements (conjunctive normal form). Individual condition statements can also be negated.

$ policy conflict
(P) Occurs when the actions of two rules (that are both satisfied simultaneously) contradict each other. The entity implementing the policy would not be able to determine which action to perform. The implementers of policy systems must provide conflict detection and avoidance or resolution mechanisms to prevent this situation. "Policy conflict" is contrasted with "policy error".

```
$ policy conversion
   See "policy translation".

$ Policy Core Information Model (PCIM) [RFC3060]
   (T) An information model describing the basic concepts of policy
       groups, rules, conditions, actions, repositories and their
       relationships.  This model is described as a "core" model
       since it cannot be applied without domain-specific extensions
       (for example, extensions for QoS or IPsec).  PCIM is "core"
       with respect to the area of policy.  However, it is a "Common
       Model," with respect to CIM - in that it extends the basic CIM
       concepts for policy.  (See also "Common Information Model".)

$ policy decision
   (P) Two perspectives of "policy decision" exist:
       -  A "process" perspective that deals with the evaluation of a
          policy rule's conditions
       -  A "result" perspective that deals with the actions for
          enforcement, when the conditions of a policy rule are TRUE

$ Policy Decision Point (PDP)
   (P) A logical entity that makes policy decisions for itself or for
       other network elements that request such decisions [RFC2753].
       (See also "policy decision".)

$ policy domain
   (P) A collection of elements and services, and/or a portion of an
       Internet over which a common and consistent set of policies
       are administered in a coordinated fashion [RFC2474]. This
       definition of a policy domain does not preclude multiple
       sources of policy creation within an organization, but does
       require that the resultant policies be coordinated.
       -  Policies defined in the context of one domain may need to
          be communicated or negotiated outside of that domain. (See
          also "policy negotiation".)

$ policy enforcement
   (P) The execution of a policy decision.

$ Policy Enforcement Point (PEP)
   (P) A logical entity that enforces policy decisions [RFC2753].
       (See also "policy enforcement".)

$ policy error
   (P) "Policy errors" occur when attempts to enforce policy actions
       fail, whether due to temporary state or permanent mismatch
       between the policy actions and the device enforcement
       capabilities.  This is contrasted with "policy conflict".
```



```
$ policy goal
   (P) Goals are the business objectives or desired state intended to
       be maintained by a policy system.  As the highest level of
       abstraction of policy, these goals are most directly described
       in business rather than technical terms.  For example, a goal
       might state that a particular application operate on a network
       as though it had its own dedicated network, despite using a
       shared infrastructure. 'Policy goals' can include the
       objectives of a service level agreement, as well as the
```

assignment of resources to applications or individuals. A policy system may be created that automatically strives to achieve a goal through feedback regarding whether the goal (such as a service level) is being met.

$ Policy Information Base (PIB)
(T) Collections of related PRovisioning Classes (PRCs), defined as a module. (See also "PRovisioning Class".)

$ policy mapping
See "policy translation".

$ policy negotiation
(P) Exposing the desired or appropriate part of a policy to another domain. This is necessary to support partial interconnection between domains, which are operating with different sets of policies.

$ policy repository
(P) "Policy repository" can be defined from three perspectives:
- A specific data store that holds policy rules, their conditions and actions, and related policy data. A database or directory would be an example of such a store.
- A logical container representing the administrative scope and naming of policy rules, their conditions and actions, and related policy data. A "QoS policy" domain would be an example of such a container.
- In [RFC3060], a more restrictive definition than the prior one exists. A PolicyRepository is a model abstraction representing an administratively defined, logical container for reusable policy elements.

$ policy request
(P) A message requesting a policy-related service. This may refer to a request to retrieve a specific set of policy rules, to determine the actions to enforce, or other policy requests. When sent by a PEP to a PDP, it is more accurately qualified as a "policy decision request" [RFC2753]. (See also "policy decision".)

$ policy rule
(P) A basic building block of a policy-based system. It is the binding of a set of actions to a set of conditions - where the conditions are evaluated to determine whether the actions are performed [RFC3060].

$ policy server
(P) A marketing term whose definition is imprecise. Originally, [RFC2753] referenced a "policy server". As the RFC evolved, this term became more precise and known as the Policy Decision Point (PDP). Today, the term is used in marketing and other literature to refer specifically to a PDP, or for any entity that uses/services policy.

$ policy translation
(P) The transformation of a policy from a representation and/or level of abstraction, to another representation or level of abstraction. For example, it may be necessary to convert PIB

data to a command line format. In this "conversion," the translation to the new representation is likely to require a change in the level of abstraction (becoming more or less specific). Although these are logically distinct tasks, they are (in most cases) blurred in the act of translating/converting/mapping. Therefore, this is also known as "policy conversion" or "policy mapping".

$ PolicyGroup
(T) An abstraction in the Policy Core Information Model [RFC3060]. It is a class representing a container, aggregating either policy rules or other policy groups. It allows the grouping of rules into a Policy, and the refinement of high-level Policies to lower-level or different (i.e., converted or translated) peer groups.

$ PRC
See "PRovisioning Class".

$ PRI
See "PRovisioning Instance".

$ provisioned policy
(P) An execution model where network elements are pre-configured, based on policy, prior to processing events. Configuration is pushed to the network device, e.g., based on time of day or at initial booting of the device. The focus of this model is on the distribution of configuration information, and is exemplified by Differentiated Services [RFC2475]. Based on events received, devices use downloaded (pre-provisioned)

mechanisms to implement policy. "Provisioned policy" is contrasted with "outsourced policy".

$ PRovisioning Class (PRC)
(T) An ordered set of attributes representing a type of policy data. PRCs are defined in PIB modules (encoded using SPPI) and registered in the Object Identifier tree. Instances of each PRC are organized in tables, similar to conceptual tables in SMIv2. (See also "Structure of Policy Provisioning Information" and "Policy Information Base".)
The acronym, PRC, has evolved from "policy rule class" to "provisioning class". The reason for the change is that a discrepancy existed between the use of the words, "policy rule" in the PRC context versus other uses in PCIM and the industry. In the latter, rules are If/Then statements - a binding of conditions to actions. PRCs are not "rules" by this definition, but the encoding of (network-wide) configuration information for a device.

$ PRovisioning Instance (PRI)
(T) An instantiation of a PRovisioning Class. (See also "PRovisioning Class".)

$ QoS
See "Quality of Service".

$ Quality of Service (QoS)

(A) At a high level of abstraction, "Quality of Service" refers to the ability to deliver network services according to the parameters specified in a Service Level Agreement. "Quality" is characterized by service availability, delay, jitter, throughput and packet loss ratio. At a network resource level, "Quality of Service" refers to a set of capabilities that allow a service provider to prioritize traffic, control bandwidth, and network latency. There are two different approaches to "Quality of Service" on IP networks: Integrated Services [RFC1633], and Differentiated Service [RFC2475]. Integrated Services require policy control over the creation of signaled reservations, which provide specific quantitative end-to-end behavior for a (set of) flow(s). In contrast, Differentiated Services require policy to define the correspondence between codepoints in the packet's DS-field and individual per-hop behaviors (to achieve a specified per-domain behavior). A maximum of 64 per-hop behaviors limit the number of classes of service traffic that can be marked at any point in a domain. These classes of service signal the treatment of the packets with respect to various QoS aspects, such as flow priority and packet drop precedence. In

addition, policy can be used to specify the routing of packets based on various classification criteria. Policy controls the set of configuration parameters and routing for each class in Differentiated Service, and the admission conditions for reservations in Integrated Services. (See also "policy abstraction" and "Service Level Agreement".)

$ Resource reSerVation Protocol (RSVP)

(T) A setup protocol designed for an Integrated Services Internet, to reserve network resources for a path [RFC2205]. And, a signaling mechanism for managing application traffic's QoS in a Differentiated Service network.

$ role

(P) "Role" is defined from three perspectives:

- A business position or function, to which people and logical entities are assigned [X.500]
- The labeled endpoints of a UML (Unified Modeling Language) association. Quoting from [UML], "When a class participates in an association, it has a specific role that it plays in that relationship; a role is just the face the class at the near end of the association presents to the class at the other end of the association". The Policy Core Information Model [RFC3060] uses UML to depict its class hierarchy. Relationships/associations are significant in the model.
- An administratively specified characteristic of a managed element (for example, an interface). It is a selector for policy rules and PRovisioning Classes (PRCs), to determine the applicability of the rule/PRC to a particular managed element [RFC3060].

Only the third definition (roles as selectors of policy) is directly related to the management of network policy. However, the first definition (roles as business positions and functions) may be referenced in policy conditions and actions.

```
    $ role combination
       (P) A lexicographically ordered set of roles that characterize
           managed elements and indicate the applicability of policy
           rules and PRovisioning Classes (PRCs).  A policy system uses
           the set of roles reported by the managed element to determine
           the correct rules/PRCs to be sent for enforcement.  That
           determination may examine all applicable policy rules
           identified by the role combination, its sub-combinations and
           the individual roles in the combination [RFC3060].  In the
           case of PRCs, a PRC must explicitly match the role combination
           of the managed element in order to be applicable and/or
           enforced.  (The comparison is typically case-sensitive.)  The
```



```
           final set of rules/PRCs for enforcement are defined by the
           policy system, as appropriate for the specified role
           combination of the managed element.

    $ RSVP
       See "Resource reSerVation Protocol".

    $ rule
       See "policy rule".

    $ rule based engine
       (T) A rule based engine is able to evaluate policy condition(s)
           and trigger appropriate policy actions.  A particular rule
           based engine may only be capable of acting upon policy rules
           that are formatted in a specified way or adhere to a specific
           language.

    $ schema
       (T) Two different perspectives of schema are defined:
           -  A set of rules that determines what data can be stored in a
              database or directory service [DirServs]
           -  A collection of data models that are each bound to the same
              type of repository.
           The latter is the preferred and recommended one for Internet
           Standards documents.  (See also "data model".)

    $ service
       (P) The behavior or functionality provided by a network, network
           element or host [DMTF, RFC2216].  Quoting from RFC 2216
           [RFC2216], in order to completely specify a "service", one
           must define the "functions to be performed ..., the
           information required ... to perform these functions, and the
           information made available by the element to other elements of
           the system".  Policy can be used to configure a "service" in a
           network or on a network element/host, invoke its
           functionality, and/or coordinate services in an interdomain or
           end-to-end environment.

    $ Service Level Agreement (SLA)
       (P) The documented result of a negotiation between a
           customer/consumer and a provider of a service, that specifies
           the levels of availability, serviceability, performance,
           operation or other attributes of the service [RFC2475]. (See
           also "Service Level Objective".)
```

```
   $ Service Level Objective (SLO)
      (P) Partitions an SLA into individual metrics and operational
          information to enforce and/or monitor the SLA.  "Service Level
          Objectives" may be defined as part of an SLA, an SLS, or in a
          separate document.  It is a set of parameters and their
          values.  The actions of enforcing and reporting monitored
          compliance can be implemented as one or more policies.  (See
          also "Service Level Agreement".)

   $ Service Level Specification (SLS)
      (P) Specifies handling of customer's traffic by a network
          provider.  It is negotiated between a customer and the
          provider, and (for example) in a DiffServ environment, defines
          parameters such as specific Code Points and the Per-Hop-
          Behavior, profile characteristics and treatment of the traffic
          for those Code Points.  An SLS is a specific SLA (a negotiated
          agreement) and its SLOs (the individual metrics and
          operational data to enforce) to guarantee quality of service
          for network traffic.  (See also "Service Level Agreement" and
          "Service Level Objective".)

   $ Simple Network Management Protocol (SNMP)
      (T) SNMP is a framework (including a protocol) for managing
          systems in a network environment [RFC2570].  It can be used
          for policy-based configuration and control using a specific
          MIB Module designed to execute policies on managed elements
          via scripts.  The elements (instances) in a network device are
          evaluated using a policy filter, to determine where policy
          will be applied.

   $ SLA
      See "Service Level Agreement".

   $ SLO
      See "Service Level Objective".

   $ SLS
      See "Service Level Specification".

   $ SMIv2
      See "Structure of Management Information".

   $ SNMP
      See "Simple Network Management Protocol".

   $ SPPI
      See "Structure of Policy Provisioning Information".
```

```
$ Structure of Policy Provisioning Information (SPPI)
   (T) An adapted subset of SNMP's Structure of Management
       Information (SMIv2) that is used to encode collections of
       related PRovisioning Classes as a PIB [RFC3159]. (See also
       "Policy Information Base" and "PRovisioning Class".)

$ Structure of Management Information, version 2 (SMIv2)
   (T) An adapted subset of OSI's Abstract Syntax Notation One, ASN.1
       (1988) used to encode collections of related objects as SNMP
       Management Information Base (MIB) modules [RFC2578].

$ subject
   (P) An entity, or collection of entities, which originates a
       request, and is verified as authorized/not authorized to
       perform that request.

$ target
   (P) An entity, or collection of entities, which is affected by a
       policy.  For example, the "targets" of a policy to reconfigure
       a network device are the individual services that are updated
       and configured.
```

4. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11.

Copies of claims of rights made available for publication 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 Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

5. Acknowledgements

This document builds on the work of previous terminology drafts. The authors of these documents were Fran Reichmeyer, Dan Grossman, John Strassner, Ed Ellesson and Matthew Condell. Also, definitions for the general concepts of policy and policy rule include input from Predrag Spasic. Very helpful comments and suggestions were received

from Juergen Schoenwaelder, Joe Salowey, Jon Saperia, Ravi Sahita, Bob Moore, Guus Sliepen, T.H. Jonatan and Dave Perkins.

6. Security Considerations

This document only defines policy-related terms. It does not describe in detail the vulnerabilities of, threats to, or mechanisms that protect specific policy implementations or policy-related Internet protocols.

7. References

[DecSupp] Building Effective Decision Support Systems. R. Sprague, and E. Carleson. Prentice Hall, 1982.

[DirServs] Understanding and Deploying LDAP Directory Services. T. Howes, M. Smith, and G. Good. MacMillan Technical Publications, 1999.

[DMTF] Common Information Model (CIM) Schema, version 2.x. Distributed Management Task Force, Inc. The components of the CIM v2.x schema are available via links on the following DMTF web page: http://www.dmtf.org/standards/standard_cim.php.

[RFC1633] Braden, R., Clark, D. and S. Shenker, "Integrated Services in the Internet Architecture: An Overview", RFC 1633, June 1994.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2138] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[RFC2205] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC2216] Shenker, S. and J. Wroclawski, "Network Element Service Specification Template", September 1997.

[RFC2474] Nichols, K., Blake, S., Baker, F. and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z. and W. Weiss, "An Architecture for Differentiated Service", RFC 2475, December 1998.

[RFC2570] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", RFC 2570, April 1999.

[RFC2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S.Waldbusser, "Structure of Management Information Version 2 (SMIv2)", RFC 2578, April 1999.

[RFC2702] Awduche, D., Malcolm, J., Agogbua, J., O'Dell, M. and J. McManus, "Requirements for Traffic Engineering Over MPLS", RFC 2702, September 1999.

[RFC2748] Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R. and A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[RFC2749] Herzog, S., Boyle, J., Cohen, R., Durham, D., Rajan, R. and A. Sastry, "COPS Usage for RSVP", RFC 2749, January 2000.

[RFC2753] Yavatkar, R., Pendarakis, D. and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, January 2000.

[RFC2828] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, May 2000.

[RFC3060] Moore, B., Ellesson, E., Strassner, J. and A. Westerinen, "Policy Core Information Model -- Version 1 Specification", RFC 3060, February 2001.

[RFC3084] Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R. and A. Smith, "COPS Usage for Policy Provisioning (COPS-PR)", RFC 3084, February 2001.

[RFC3159] McCloghrie, K., Fine, M., Seligson, J., Chan, K., Hahn, S., Sahita, R., Smith, A. and F. Reichmeyer, "Structure of Policy Provisioning Information," RFC 3159, August 2001.

[UML] The Unified Modeling Language User Guide. G. Booch, J. Rumbaugh, and I. Jacobson. Addison-Wesley, 1999.

[X.500] Data Communications Networks Directory, Recommendations X.500-X.521, Volume VIII - Fascicle VIII.8. CCITT, IXth Plenary Assembly, Melbourne. November 1988.

8. Authors' Addresses

Andrea Westerinen
Cisco Systems, Bldg 20
725 Alder Drive
Milpitas, CA 95035

EMail: andreaw@cisco.com

John Schnizlein
Cisco Systems
9123 Loughran Road

Fort Washington, MD 20744

EMail: john.schnizlein@cisco.com

John Strassner
Intelliden Corporation
90 South Cascade Avenue
Colorado Springs, CO 80903
Phone: +1-719-785-0648

EMail: john.strassner@intelliden.com

Mark Scherling
Xcert International Inc.
Suite 300
505 Burrard Street
Vancouver, BC
V7X 1M3

EMail: mscherling@xcert.com

Bob Quinn
Celox Networks
2 Park Central Drive
Southborough, MA 01772

EMail: bquinn@celoxnetworks.com

Jay Perry
Network Appliance
495 East Java Drive
Sunnyvale, CA 94089

EMail: jay.perry@netapp.com

Shai Herzog
PolicyConsulting.com
200 Clove Rd.
New Rochelle, NY 10801

EMail: herzog@PolicyConsulting.com

An-Ni Huynh
Lucent Technologies
2139 Route 35
Holmdel, NJ 07733

Mark Carlson
Sun Microsystems, Inc.
500 Eldorado Boulevard
Broomfield, CO 80021

EMail: mark.carlson@sun.com

Steve Waldbusser

Phone: +1-650-948-6500
Fax: +1-650-745-0671
EMail: waldbusser@nextbeacon.com

9. Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.