Policy Framework Working Group
INTERNET-DRAFT
Category: Informational

A. Westerinen
J. Schnizlein
J. Strassner
Cisco Systems
Mark Scherling
Bank One
Bob Quinn
Celox Networks
Jay Perry
CPlane
Shai Herzog
IP Highway
An-Ni Huynh
Lucent Technologies
Mark Carlson
Sun Microsystems
July 2000

Policy Terminology

<draft-ietf-policy-terminology-00.txt>
Friday, July 14, 2000, 12:10 AM

Status of this Memo

Copyright Notice

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 RFC2828 [R2828], 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

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 [R2026]. Benefits across the ISDs are well-stated in the Introduction to RFC2828 [R2828]:

- "Clear, Concise, and Easily Understood Documentation" - Requires that the set of terms and definitions be consistent, self-supporting and uniform across all ISDs.
- Technical Excellence - Where all ISDs use terminology accurately, precisely, and unambiguously.
- 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.
- "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 in this draft. These terms are directly related and specific to network policy. This is a "living" document that is expected to grow over the next several months, as the current terms are reviewed and additional words suggested for inclusion.

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

- Expired Internet-Drafts are not referenced, nor are their terminology and definitions used in this document.
- Multiple definitions may exist across the ISDs. Each definition will be listed, with its source.

Where definitions are contradictory, the recommendations of the draft editors are presented. The draft editors will work with other ISD authors to remove contradictions.

2. Explanation of Paragraph Markings

Section 3 marks terms and definitions as follows:

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

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

  - "P" identifies basic policy-related terms.

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

  - "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 efforts in the IETF have focused on the most widely deployed use of authentication: Remote Authentication Dial In User Service (RADIUS). Referencing the RADIUS RFC (R2138), a network access server sends dial-user credentials to a 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 for that user. 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. The AAA Working Group is also completing its requirements for a general-purpose AAA protocol expanding beyond

RADIUS. The only protocol proposed thus far is Diameter ("radius" pun - not an acronym) [DIAMETER]. And, the Authentication Authorization Accounting ARCHitecture Research Group (AAAARCH) was formed as a new area of research within the IRTF, with the goal of coordination "with the Policy Framework WG and others."

$ CIM
See "Common Information Model."

$ Common Information Model (CIM)
(M) 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 language definition to represent the Model. CIM includes a set of files, written in the language specified in the Specification. These are known as the Core and Common Models, and define an information model for the "enterprise" - addressing systems, devices, users, software distribution, the physical environment, networks and policy. (See also "information model.")

$ Common Open Policy System (COPS)
(M) 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). [RFC 2748] (See also "Policy Decision Point" and "Policy Enforcement Point.")

$ condition
See "policy condition."

$ configuration
(P) 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.

$ COPS
See "Common Open Policy System."

$ data model
(M) 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)
(M) 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. [R2474, DSTERMS]
(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). (See also "Quality of Service.")

$ diffserv
See "Differentiated Services."

$ Directory Enabled Networks (DEN)
(M) 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
See "policy domain."

$ DS
See "Differentiated Services."

$ filter
(M) A set of terms and/or criteria used for the purpose of separating or categorizing. "Filters" are often manipulated and used in network policy.
- Packet filters are defined in [PIB]. They specify the criteria for matching a pattern (for example, IP or 802 traffic criteria) to appear in packets belonging to flows,

e.g. microflows or behavior aggregates. Associated with each filter is a permit/deny flag.

$ goal
See "policy goal."

$ information model
(M) 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, application, protocol, or platform.

$ Internet Protocol Security Policy (IPSP)
(A) An IETF Working Group chartered to define a standard data model, specification language and exchange protocol for supporting IP Security Policies that are compatible with the existing IPsec architecture [RFC 2401] and IKE [RFC 2409], complementing the standards work achieved by the IPsec Working Group.

$ IPSP
See "Internet Protocol Security Policy."

$ MPLS
See "Multiprotocol Label Switching."

$ Multiprotocol Label Switching (MPLS)
(M) Integrates a label swapping framework with network layer routing [R2702]. 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. [R2205, R2748] "Outsourced policy" is contrasted with "provisioned policy", but they are not mutually exclusive and operational systems may combine the two.

$ 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. [PCIM]

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. (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 [PCIM], a rule's actions may be ordered.

$ policy condition
(P) An expression used to determine whether a policy rule's actions should be performed. When the set of conditions associated with a policy rule evaluates to TRUE, then the rule should be enforced. A condition may be defined as the occurrence of an event, or a computed expression typically consisting of three elements: a variable, an operator and another variable or constant. [QoSModel] Some of these elements may be implicit in an implementation or protocol.
- In [PCIM], 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 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. [R2753] (See also "policy decision.")

$ policy domain
(P) A contiguous portion of an Internet over which a consistent set of [..] policies are administered in a coordinated fashion. [R2474] 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. The definition given in RFC 2474 for Differentiated Services is very close to that of a security domain, defined in [SPSL]. In [SPSL], it is stated: "A security domain is defined as a connected set of network entities that are protected by policy enforcement points (PEP) placed on every communication path going through the perimeter of the domain. Every policy enforcement point of the domain works to enforce the common set of security policies associated with the domain."

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

$ Policy Enforcement Point (PEP)
(P) A logical entity that enforces policy decisions. [R2753] (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 conditions/states intended to be maintained by a policy system. At the highest level of abstraction of policy, "goals" are most directly related to business rather than technical terms. For example, a "goal" might be that a particular application receives network

behavior equivalent to having its own dedicated network, despite using a shared infrastructure. (See also "policy abstraction.")

$ Policy Information Base (PIB)
(M) Collections of related policy rule classes (PRCs), defined as a module. [PIB]

$ 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. The need for "policy negotiation" is described in the IPsec Policy Working Group charter [IPSP]: "4) adopt or develop a policy exchange and negotiation protocol. The protocol must be capable of: i) discovering policy servers, ii) distributing and negotiating security policies, and; iii) resolving policy conflicts in both intra/inter domain environments."

$ 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 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. [QoSModel]
- In [PCIM], a more restrictive definition than the prior one exists. PolicyRepository is a model abstraction representing an administratively defined, logical container for reusable policy conditions and policy actions.

$ policy request
(P) Sent by a PEP to a PDP, it is more accurately qualified as a "policy decision request." [R2753] (See also "policy decision.")

$ Policy Retrieval Point (PRP)
(P) A client of a policy repository. [AAA]
- Outside of [AAA], this term is not used, since policy retrieval is a necessary function of a policy-based system. For example, a PDP includes both policy retrieval and decision making functionality.

$ 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. [PCIM]

$ Policy Rule Class (PRC)

(M) An ordered set of scalar attributes, defined in a PIB. "Policy Rule Classes" are arranged in a hierarchical structure similar to tables in SNMP's SMIv2. [R2578, PIB]

$ policy server
(P) A marketing term whose definition is imprecise. Originally, [R2753] 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. This is also known as "policy conversion."

$ PolicyGroup
(M) An abstraction in the Policy Core Information Model [PCIM]. 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.

$ PolicyRepository
(M) An abstraction in the Policy Core Information Model [PCIM]. It is a class representing an administratively defined, logical container for reusable policy conditions and policy actions. (See also "policy repository.")

$ PRC
See "Policy Rule Class."

$ 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 [R2475]. Based on events received, devices use downloaded (pre-provisioned) mechanisms to implement policy. "Provisioned policy" is contrasted with "outsourced policy."

$ PRP
See "Policy Retrieval Point."

$ 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 [R1633], and Differentiated Service [R2475]. 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. Policy controls the set of configuration parameters 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)
(M) A setup protocol designed for an Integrated Services Internet, to reserve network resources for a path. [R2205] And, a signaling mechanism for managing application traffic's QoS in a Differentiated Service network. [DCLASS]

$ role
(P) "Role" is defined from four 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 [PCIM] uses UML to depict its class hierarchy. Relationships/associations are significant in the model.
- An abstract characteristic assigned to a network element that expresses a notion, such as a political, financial, legal, geographical, or architectural attribute, typically not directly derivable from information stored on the system

[SNMPCONF]

- A string characterizing a particular function of a network element or interface, that can be used to identify particular behavior associated with that element. It is a selector for

policy rules, to determine the applicability of the rule to a particular network element. "Roles" abstract the capabilities and/or use of network devices and resources. [PCIM, PIB]

Only the latter two definitions are directly related to network policy. The last is the preferred and recommended definition. The use of the term in [SNMPCONF] contradicts the established usage in references [PCIM] and [PIB].

$ role combination

(P) An unordered set of roles. Two interpretations of "role combination" currently exist:

- The set of roles in a "role combination" must be identical to the set of the roles of the network element or interface [PIB]
- The selection process for a "role-combination" chooses policies associated with the combination itself, policies associated with each of its sub-combinations, and policies associated with each of the individual roles in the combination [PCIM]

These two interpretations are contradictory and require alignment to prevent confusion across the ISDs.

$ RSVP

See "Resource reSerVation Protocol."

$ rule

See "policy rule."

$ schema

(M) 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 ISDs. (See also "data model.")

$ Security Policy Specification Language (SPSL)

(M) A language designed to express security policies, security domains, and the entities that manage those policies and domains. It supports policies for packet filtering, IP Security (IPsec), and IKE exchanges, but may be extended to express other types of policies. [SPSL]

$ service

(P) The behavior or functionality of a network element or host [DMTF, R2216]. Quoting from RFC 2216 [R2216], in order to completely specify a "service", one must define the "functions to be performed à, the information required à 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" on a network element or 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. (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, 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 defines DiffServ 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 combination of an SLA (a negotiated agreement) and its SLOs (the individual metrics and operational data to enforce). [DSTERMS] (See also "Service Level Agreement" and "Service Level Objective.")

$ SLA
See "Service Level Agreement."

$ SLO
See "Service Level Objective."

$ SLS
See "Service Level Specification."

$ SMIv2
See "Structure of Management Information."

$ SPPI
See "Structure of Policy Provisioning Information."

$ SPSL
See "Security Policy Specification Language."

$ Structure of Policy Provisioning Information (SPPI)
(M) An adapted subset of SNMP's Structure of Management Information (SMIv2) that is used to encode collections of

related Policy Rule Classes as a PIB. [R2578, SPPI]

$ Structure of Management Information, version 2 (SMIv2)
(M) 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. [R2578]

$ 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

5. Acknowledgements

This document builds on the work of previous terminology drafts. The authors of these drafts 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.

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

[AAA] AAA Authorization Framework. Internet Draft, draft-ietf-aaa-authz-arch-00.txt, J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, and D. Spence. October 1999.

[DCLASS] Format of the RSVP DCLASS Object. Internet Draft, draft-ietf-issll-dclass-01.txt, Y. Bernet. October 1999.

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

[DIAMETER] DIAMETER Framework Document. Internet Draft, draft-calhoun-diameter-framework-08.txt, P. Calhoun, G. Zorn, P. Pan, and H. Akhtar. June 2000.

[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 2.4. Distributed Management Task Force, Inc. July, 2000. The components of the CIM v2.4 schema are available via links on the following DMTF web page: http://www.dmtf.org/spec/cim_schema_v24.html.

[DSTERMS] New Terminology for Diffserv. Internet Draft, draft-ietf-diffserv-new-terms-02.txt>, D. Grossman. November 1999.

[IPSP] IP Security Policy (ipsp) Working Group Charter. February 2000. http://www.ietf.org/html.charters/ipsp-charter.html.

[PCIM] Policy Core Information Model - Version 1 Specification. Internet Draft, draft-ietf-policy-core-info-model-07.txt, B. Moore, E. Ellison, J. Strassner, and A. Westerinen. July 2000.

[PIB] Quality of Service Policy Information Base. Internet Draft, draft-mfine-cops-pib-02.txt, M. Fine, K. McCloughrie, J. Seligson, K. Chan, S. Hahn, and A. Smith. October 1999.

[QoSModel] Policy Framework QoS Information Model. Internet Draft,

draft-ietf-policy-qos-info-model-01.txt, Y. Snir, Y. Ramberg, J. Strassner, and R. Cohen. April 2000.

[R1633] Integrated Services in the Internet Architecture: An Overview. R. Braden, D. Clark, and S. Shenker. June 1994.

[R2026] The Internet Standards Process -- Revision 3. S. Bradner. October 1996.

[R2138] Remote Authentication Dial In User Service (RADIUS). C. Rigney, A. Rubens, W. Simpson, and S. Willens. April 1997.

[R2205] Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification. R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin. September 1997.

[R2401] Security Architecture for the Internet Protocol. S. Kent, and R. Atkinson. November 1998.

[R2409] The Internet Key Exchange (IKE). D. Harkins, and D. Carrel. November 1998.

[R2474] Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. K. Nichols, S. Blake, F. Baker, and D. Black. December 1998.

[R2475] An Architecture for Differentiated Service. S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. December 1998.

[R2578] Structure of Management Information Version 2 (SMIv2). K. McGloughrie, D. Perkins, J. Schoenwaelder, J. Case, M. Rose, and S. Waldbusser. April 1999.

[R2702] Requirements for Traffic Engineering Over MPLS. D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus. September 1999.

[R2748] The COPS (Common Open Policy Service) Protocol. D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry. January 2000.

[R2753] A Framework for Policy-based Admission Control. R. Yavatkar, D. Pendarakis, and R. Guerin. January 2000.

[R2828] Internet Security Glossary. R. Shirey. May 2000.

[SNMPCONF] Policy Based Management MIB. Internet Draft, draft-ietf-snmpconf-pm-01.txt, S. Waldbusser, J. Saperia and T. Hongal. May 2000.

[SPPI] Structure of Policy Provisioning Information (SPPI).

Fine, J. Seligson, K. Chan, S. Chan, A. Smith, and F. Reichmeyer. March 2000.

[SPSL] Security Policy Specification Language. Internet Draft, draft-ietf-ipsp-spsl-00.txt, M. Condell, C. Lynn, and J. Zao. March 2000.

[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 15
170 West Tasman Drive
San Jose, CA 95134
E-mail: andreaw@cisco.com

John Schnizlein
Cisco Systems
9123 Loughran Road
Fort Washington, MD 20744
E-mail: john.schnizlein@cisco.com

John Strassner
Cisco Systems, Bldg 15
170 West Tasman Drive
San Jose, CA 95134
E-mail: johns@cisco.com

Mark Scherling
Bank One International
62 Beaufort Drive
Kanata, Ontario, Canada
K2L 2G3
E-mail: marks@m3p.ca

Bob Quinn
Celox Networks
One Cabot Road
Hudson, MA 01749
E-mail: bquinn@celoxnetworks.com

Jay Perry
CPlane, Inc.
5150 El Camino Real - B-31

Los Altos, CA 94022
E-mail: jay@cplane.com

Shai Herzog
IPHighway
55 New York Avenue
Framingham, MA 01701
E-mail: herzog@iphighway.com

An-Ni Huynh
Lucent Technologies
2139 Route 35
Holmdel, NJ 07733
E-mail: ahuynh@lucent.com

Mark Carlson
Sun Microsystems
2990 Center Green Court South
Boulder, CO 80301
Email: mark.carlson@sun.com

9. Full Copyright Statement