

TSVWG
Internet-Draft
Intended status: Standards Track (PS)
Expires: Jan 2nd, 2008
Updates: RFC [3181](#)

James Polk
Subha Dhesikan
Cisco Systems
July 2nd, 2007

Signaled Domain and Sub-domain Identification Element
[draft-polk-tsvwg-signaled-domain-id-00](#)

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on Jan 2nd, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document defines a domain and a sub-domain identification element for use by signaled policy based admission protocols such as Resource ReSerVation Protocol (RSVP) and Common Open Policy Service (COPS). This element identifies the domain and sub-domain to which the reservation belongs and is used, along with the PREEMPTION_PRI element, to make capacity-based admission control (CAC) decisions.

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 [[RFC2119](#)].

Table of Contents

1.	Introduction	2
2.	Motivation	3
3.	Functional Summary	4
4.	DOMAIN_SUBDOMAIN Element	5
5.	Rules of use of the DOMAIN_SUBDOMAIN Element	6
6.	DOMAIN_SUBDOMAIN Element Errors	7
7.	Security Considerations	7
8.	IANA Considerations	7
9.	Acknowledgements	8
10.	References	8
	10.1. Normative References	8
	10.2. Informational References	8
	Authors' Addresses	9
	Intellectual Property and Copyright Statements	9

[1.](#) Introduction

This document defines a domain/sub-domain identification element for use by signaled policy based admission protocols such as RSVP [[RFC2205](#)] and COPS [[RFC2748](#)]. This element identifies the domain and sub-domain to which the reservation belongs and is used along with the PREEMPTION_PRI element [[RFC3181](#)] to make capacity-based admission control (CAC) decisions. This is independent of whether the reservation is individual, a tunnel or an aggregate.

[RFC 3181](#) allows a reservation from one domain to preempt a reservation from another domain. This may not be a desirable action as priorities are relative within a domain and the preempted reservation may be just as important as the reservation that has been newly admitted. There is also a risk of some domains arbitrarily using high priority values to gain a better chance at network resources than reservations from other domains. Hence, the need for the domain and sub-domain identification information within a reservation request to limit reservations considered for preemption to be within the same domain/sub-domain.

To meet this requirement, two identifiers are necessary, one is a unique domain identifier, and the other is a sub-domain identifier.

[RFC 3181](#) [[RFC3181](#)] provides a reservation preemption priority policy element (PREEMPTION_PRI), which defines the relative priority one

reservation has when compared to another when deciding to admit a flow, and another relative priority value for defending against

preemption from a future flow.

Attempting to replace [RFC 3181](#) with a rewritten document that carves out a domain value and a subdomain value within the existing 16 bit preemption priority field, while maintaining the existing admitting priority value appears to be less than optimal, given the number of domains that can be registered as unique. The same limitation holds for the 16 bit defending priority field.

Therefore, a new element needs to be created to satisfy the domain/sub-domain identifier requirements stated above - and preserve the preemption priority policy element defined within [RFC 3181](#).

This element creates the ability to preserve the original domain/subdomain-values, while allowing transit network domains to have their own identifiers while the their portion of the network, relative to the end-to-end flow.

This document updates [RFC 3181](#).

2. Motivation

The requirement of differing sub-domain treatments of flows allows a single domain to administer how a group of endpoints can communicate relative to the rest of the endpoints within the network. To give a concrete example, lets look at a country's military organizations communicating with each other, within their own branches of the service. A policy can be established within this government communications such that each branch of the military has the per flow ability to preempt higher priority flows only within the same branch of service, and not preempt flows existing at a saturated network interface identified as from any other branch of the military. This is regardless of the priority value indicated in the flow establishment or flow retention.

To accomplish this scenario, three pieces of information are required: the priority of the flow, the sub-domain of the branch of service the user of the flow is in, and the overall domain of this government's network. RSVP affords the additional ability to distinguish the difference between the call establishment and call retention to allow a flow to be established at a higher priority than that same flow is defending against being preempted by future flows.

Once a router interface becomes saturated, and cannot allow any additional calls through that interface, the router has to make preemption decisions if it decides to allow future flows, provided

none of the existing flows terminate somewhere else. As described in [[ID-RPH-DISA](#)] for how the Session Initiation Protocol (SIP)

addresses this issue, this DOMAIN_SUBDOMAIN element will provide the final two pieces of information necessary to meet the desired functionality.

3. Functional Summary

This DOMAIN-SUBDOMAIN element is an encapsulation of the Policy Data object which is defined in [\[RFC2750\]](#). This element may be present in RSVP PATH and RESV message. If the element is present in the PATH message, it is used in policy control. In the RESV message, the element is used for not only policy control but also for resource control.

If the DOMAIN_SUBDOMAIN element is present in any RSVP message, the PREEMPTION_PRI element needs to be present as well. The reverse is not true.

The DOMAIN-SUBDOMAIN element may be created along with the PREEMPTION-PRI element at the RSVP host where the PATH or RESV message originates. It is then carried to the RSVP-enabled routers along the path in the RSVP message. Alternatively, the element may be inserted by the intermediate RSVP routers. This is done when this element, along with the PREEMPTION-PRI element, is created by the Policy Decision Points (PDP) or the Local decisions Points (LDP) along the path. The PDP/LDP creates this element and provides it to the PEP for insertion into the RSVP message before the message is forwarded.

PDP, LDP and/or PEP use the contents of this element to make decisions on the treatment of the PATH and RESV message. When a RSVP-enabled router receives the PREEMPTION-PRI element and the DOMAIN_SUBDOMAIN element, it may hand these elements to the LDP/PDP if configured to do so. The PDP/LDP uses these elements in making policy control decisions. The decision is then conveyed to the PEP for enforcement. The RSVP messages containing these elements are then forwarded to the next hop. The PDP/LDP may ask for the elements to be removed before forwarding as well.

If an error occurs during the processing of the DOMAIN-SUBDOMAIN element, the PathErr or ResvErr is returned as appropriate. The error information is then added to the PREEMPTION_PRI object and included in the error message as stated in [RFC 3181](#).

When a RSVP message containing this element enters a different domain during transit, the PDP/LDP in the new domain may add a Transit-Domain-value and a Transit-Sub-Domain-value for use within the transit domain. This is done as the original domain and sub-domain id may not be relevant within the new domain. In such a

case, the edge LDP/PDP may translate the original domain and sub-domain id to a transit domain and sub-domain id based on SLAs or other criteria and add it to the RSVP message. The original ids are

left unchanged. The transit ids are removed when exiting the transit domain.

4. DOMAIN_SUBDOMAIN Element

The format of DOMAIN_SUBDOMAIN identification element is as follows:

+-----+-----+-----+-----+	
	Length (16)
+-----+-----+-----+-----+	
	TBD
+-----+-----+-----+-----+	
	Transit Domain-Value
+-----+-----+-----+-----+	
	Transit Sub-Domain-Value
+-----+-----+-----+-----+	

Length: 16 bits

Always 16. The overall length of the policy element, in bytes.

P-Type: 16 bits

DOMAIN_SUBDOMAIN = XXXX (to be assigned by IANA)

TBD field: (currently) 16 bits

(this may be one or two fields)

(to be fleshed out in next rev of doc)

Reserved: 16 bits

Always 0. (for future extensibility)

Transit domain-value: 16 bits (IANA assigned)

An IANA registered domain identifier of the network the packet is in now

Original domain-value: 16 bits (IANA assigned)

An IANA registered domain identifier of the original network which started this flow.

If the DOMAIN_SUBDOMAIN element is in a packet within the original domain (or on either end of a domain1->domain2->domain1 scenario), these two domain-values are the same.

Transit sub-domain-value: 16 bits (unassigned)

Transit domain's sub-domain identifier

Original sub-domain-value: 16 bits (unassigned)

Locally controlled sub-domain identifier of a subgroup of nodes within the original domain

If the DOMAIN_SUBDOMAIN element is in a packet within the original domain (or on either end of a domain1->domain2->domain1

scenario), these two sub-domain-values are the same.

[Editor's note: we might build a table to show the above point]

The domain and subdomain values MAY be paired with SIP Resource-Priority header (RPH) namespace [[RFC4412](#)] with the delimiter defined in [[ID-RPH-DISA](#)] as how an RPH namespace is divided into two parts.

Editor's note: Should merging be considered within this document (along the lines of how it is in [RFC 3181](#))?

5. Rules of use of the DOMAIN_SUBDOMAIN Element

The following rules are to be followed when utilizing the DOMAIN_SUBDOMAIN element:

- the DOMAIN_SUBDOMAIN element is optional (i.e., RSVP/COPS will function if this element is not in a message)
- If a Domain-value is required within a network, there MAY or MAY NOT be a Sub-domain-value within that network (i.e., this element can be used merely to identify a domain in which there are no sub-domains).
- Domain-values are IANA registered to be unique per network (i.e., Cisco would have one domain identifier throughout the company's network).
- There is no difference between a Transit and Original domain from IANA's point of view. IANA controls the one registration list.
- Sub-Domain-values are not to be registered, and are to be administered locally, if present in the element.
- Domain-values not understood SHOULD be ignored, thereby treating the reservation request as if this element weren't present in the PATH or RESV message (in the case of RSVP).
- Sub-Domain-values not understood should be considered as if there was no sub-domain-value in the element (i.e., a default of 0, which MUST be valid in any network having sub-domains).
- Network or domain border entities SHOULD NOT change Domain-value field when exiting or entering a network boundary. This can cause problems when sending packets in the reverse direction. An exception to this rule is in such cases the value(s) can be successfully changed back in the reverse direction.

- The Transit-Domain-value is to be changed when existing a domain.
The burden of entering a new value is on the ingress node of the

new domain in during the e2e flow.

- The Original-Domain-value MUST NOT be changed at reservation establishment or while the reservation remains operational.
- The Original-Sub-Domain-value MUST NOT be changed at reservation establishment or while the reservation remains operational.
- This DOMAIN_SUBDOMAIN element MUST be accompanied by the PREEMPTION_PRI element defined in [[RFC3181](#)].
- Since the DOMAIN_SUBDOMAIN element MUST be accompanied by the PREEMPTION_PRI element, implementers ought have to look for an error in only one place. Therefore, DOMAIN_SUBDOMAIN error codes will be added to the PREEMPTION_PRI element error field, of which there are presently only 3 IANA registered.
- The PREEMPTION_PRI element defined in [[RFC3181](#)] MAY be in a PATH or RESV message (in RSVP) without this DOMAIN_SUBDOMAIN element but the reverse is not true.

6. DOMAIN_SUBDOMAIN Element Errors

There is no error field in this element, but there are errors associated with this element. This element's errors will be in the PREEMPTION_PRI error field defined in [[RFC3181](#)], that currently only has 3 errors IANA registered.

New DOMAIN_SUBDOMAIN errors are TBD at this time.

7. Security Considerations

The integrity of DOMAIN_SUBDOMAIN element is guaranteed, as any other policy element is, by the encapsulation into a Policy Data object [[RFC2750](#)].

As such, this document introduces no additional security considerations above that found in [[RFC3181](#)].

8. IANA Considerations

The following is to be IANA assigned within the RSVP parameters registration area. Extensions to this document requesting new IANA registrations MUST be done through a standards track RFC to ensure community review.

8.1 DOMAIN_SUBDOMAIN P-Type Registration

IANA shall register DOMAIN_SUBDOMAIN as a new P-Type, similar to how

PREEMPTION_PRI was registered from [RFC 3181](#). Please refer to [section 4](#) of this document for the element's format.

[8.2](#) Domain-value Registration

IANA shall register each network requesting a domain number be assigned to it. Subdomain-values are not registered.

[an example of this registration table will be built in a future rev of this doc].

[9.](#) Acknowledgements

None at this time.

[10.](#) References

[10.1.](#) Normative References

- [RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997
- [RFC2205] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", [RFC 2205](#), September 1997
- [RFC2748] Boyle, J., Cohen, R., Durham, D., Herzog, S., Raja, R. and A. Sastry, "The COPS (Common Open Policy Service) Protocol", [RFC 2748](#), January 2000.
- [RFC3181] S. Herzog, "Signaled Preemption Priority Policy Element", [RFC 3181](#), October 2001
- [RFC2750] S. Herzog, "RSVP Extensions for Policy Control", [RFC 2750](#), January 2000
- [RFC4412] Schulzrinne, H., Polk, J., "Communications Resource Priority for the Session Initiation Protocol (SIP)", [RFC 4411](#), Feb 2006

[10.2.](#) Informational References

- [ID-RPH-DISA] J. Polk "New Session Initiation Protocol Resource-Priority Header Namespaces for the Defense Information Services Agency", [draft-polk-sip-rph-new-namespaces-00](#), "work in progress", Feb 2007

Authors' Addresses

James Polk
Cisco Systems
3913 Treemont Circle
Colleyville, Texas
USA

Email: jmpolk@cisco.com

Subha Dhesikan
Cisco Systems
170 W Tasman St
San Jose
CA-95135

sdhesika@cisco.com

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

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.

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, THE IETF TRUST 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.

Intellectual Property

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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

