Network Working Group
Request for Comments: 3822
Category: Standards Track

D. Peterson
Computer Network Technology (CNT)

July 2004

Finding Fibre Channel over TCP/IP (FCIP) Entities Using Service Location Protocol version 2 (SLPv2)

Status of this Memo

Copyright Notice

Abstract

This document defines the use of Service Location Protocol version 2 (SLPv2) by Fibre Channel over TCP/IP (FCIP) Entities.

1. Introduction

This document describes the use of the Service Location Protocol version 2 in performing dynamic discovery of participating Fibre Channel over TCP/IP (FCIP) Entities. Implementation guidelines, service type templates, and security considerations are specified.

2. Notation Conventions

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].

3. Terminology

Here are some definitions that may aid readers that are unfamiliar with either SLP or FCIP. Some of these definitions have been reproduced from [RFC2608] and [RFC3105].

User Agent (UA)	A process working on the client's behalf to establish contact with some service. The UA retrieves service information from the Service Agents or Directory Agents.
Service Agent (SA)	A process working on behalf of one or more services to advertise the services and their capabilities.
Directory Agent (DA)	A process which collects service advertisements. There can only be one DA present per given host.
Scope	A named set of services, typically making up a logical administrative group.
Service Advertisement	A URL, attributes, and a lifetime (indicating how long the advertisement is valid), providing service access information and capabilities description for a particular service.
FCIP Entity	The principle FCIP interface point to the IP network.
FCIP Entity Name	The world wide name of the switch if the FCIP Entity resides in a switch or the world wide node name of the associated Nx_Port.
FCIP Discovery Domain	The FCIP Discovery Domain specifies which FCIP Entities are allowed to discover each other within the bounds of the scope.

4. Using SLPv2 for FCIP Service Discovery

At least two FCIP Entities must be involved in the entity discovery process. The end result is that an FCIP Entity will discover one or more peer FCIP Entities.

4.1. Discovering FCIP Entities using SLPv2

Figure 1 shows the relationship between FCIP Entities and their associated SLPv2 agents.

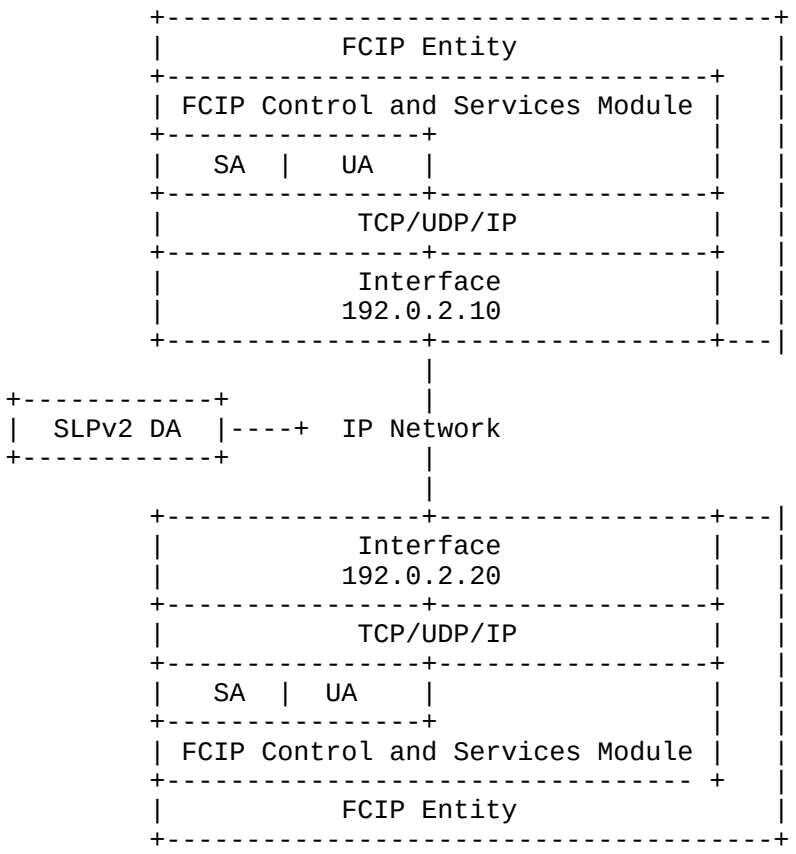

Figure 1: FCIP Entity and SLPv2 Agent Relationship.

As indicated in Figure 1, each FCIP Entity contains an FCIP Control and Services Module that interfaces to an SLPv2 SA and UA.

The SA constructs a service advertisement of the type "service:fcip:entity" for each of the service URLs it wishes to register. The service advertisement contains a lifetime, along with other attributes defined in the service template.

The remainder of the discovery process is identical to that used by any client/server pair implementing SLPv2:

1. If an SLPv2 DA is found [RFC2608], the SA contacts the DA and registers the service advertisement. Whether or not one or more SLPv2 DAs are discovered, the SA maintains the service advertisement itself and answers multicast UA queries directly.

2. When the FCIP Entity requires contact information for a peer FCIP Entity, the UA either contacts the DA using unicast or the SA using multicast using an SLPv2 service request. The UA service request includes a query, based on the attributes, to indicate the characteristics of the peer FCIP Entities it requires.

3. Once the UA has the IP address and port number of a peer FCIP Entity, it may begin the normal connection procedure, as described in [RFC3821], to a peer FCIP Entity.

The use of a DA is RECOMMENDED for SLPv2 operations in an FCIP environment.

4.1.1. FCIP Discovery Domains

The concept of a discovery domain provides further granularity of control of allowed discovery between FCIP Entities within a specific SLPv2 scope.

Figure 2 shows an example relationship between FCIP Entities and their associated discovery domains within a specified SLPv2 scope.

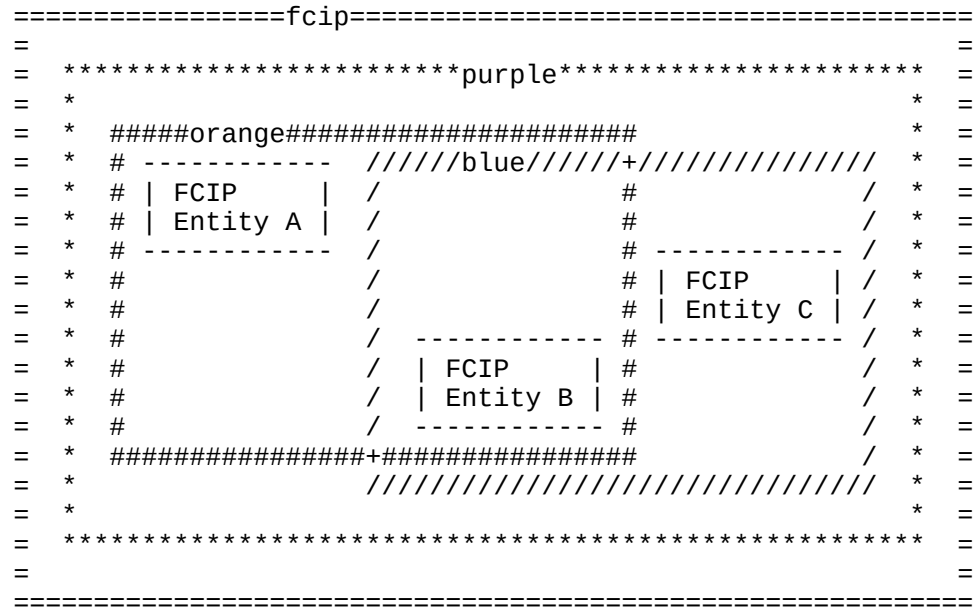

Figure 2: FCIP Entity and Discovery Domain Example.

Within the specified scope "fcip", the administrator has defined a discovery domain "purple", allowing FCIP Entities A, B, and C to discover each other. This discovery domain is illustrated using the "*" character.

Within the specified scope "fcip", the administrator has defined a discovery domain "orange", allowing FCIP Entity A to discover FCIP Entity B, but not FCIP Entity C. This discovery domain is illustrated using the "#" character.

Within the specified scope "fcip", the administrator has defined a discovery domain "blue", allowing FCIP Entity C to discover FCIP Entity B, but not FCIP Entity A. This discovery domain is illustrated using the "/" character.

For the example relationship shown in Figure 2, the value of the fcip-discovery-domain attribute for each FCIP Entity is as follows:

FCIP Entity A = orange,purple

FCIP Entity B = orange,blue,purple

FCIP Entity C = blue,purple

5. FCIP SLPv2 Templates

Two templates are provided: an FCIP Entity template, and an abstract template to provide a means of adding other FCIP related templates in the future.

5.1. The FCIP Abstract Service Type Template

This template defines the abstract service "service:fcip". It is used as a top-level service to encapsulate all other FCIP related services.

Name of submitter: David Peterson
Language of service template: en
Security Considerations: see section 6.

Template Text:

```
--------------------------template begins here-----------------------
template-type=fcip

template-version=0.1

template-description=
   This is an abstract service type.  The purpose of the fcip service
```

type is to encompass all of the services used to support the FCIP protocol.

template-url-syntax =

url-path= ; Depends on the concrete service type.

----------template ends here----------

5.2. The FCIP Entity Concrete Service Type Template

This template defines the service "service:fcip:entity". A device containing FCIP Entities that wishes to have them discovered via SLPv2 would register each of them with each of their addresses, as this service type.

FCIP Entities wishing to discover other FCIP Entities in this manner will generally use one of the following example query strings:

1. Find a specific FCIP Entity, given its FCIP Entity Name:

   Service: service:fcip:entity
   Scope: fcip-entity-scope-list
   Query: (fcip-entity-name=\ff\10\00\00\60\69\20\34\0C)

2. Find all of the FCIP Entities within a specified FCIP Discovery Domain:

   Service: service:fcip:entity
   Scope: fcip-entity-scope-list
   Query: (fcip-discovery-domain=fcip-discovery-domain-name)

3. In addition, a management application may wish to discover all FCIP Entities:

   Service: service:fcip:entity
   Scope: management-service-scope-list
   Query: none

Name of submitter: David Peterson
Language of service template: en
Security Considerations: see section 6.

Template Text:
----------template begins here----------
template-type=fcip:entity

template-version=0.1

```
   template-description=
     This is a concrete service type.  The fcip:entity service type is
     used to register individual FCIP Entity addresses to be discovered
     by others.  UAs will generally search for these by including one of
     the following:
     - the FCIP Entity Name for which an address is needed
     - the FCIP Discovery Domain Name for which addresses are requested
     - the service URL

   template-url-syntax =
     url-path = hostport
     hostport = host [ ":" port ]
     host = hostname / hostnumber
     hostname = *( domainlabel "." ) toplabel
     alphanum = ALPHA / DIGIT
     domainlabel = alphanum / alphanum * [alphanum / "-"] alphanum
     toplabel = ALPHA / ALPHA * [ alphanum / "-" ] alphanum
     hostnumber = ipv4-number
     ipv4-number = 1*3DIGIT 3("." 1*3DIGIT)
     port = 1*DIGIT

     ;
     ; A DNS host name should be used along with the well-known
     ; IANA FCIP port number for operation with NAT/NAPT devices.
     ;
     ; Examples:
     ; service:fcip:entity://host.example.com
     ; service:fcip:entity://192.0.2.0:4000
     ;

   fcip-entity-name = opaque L
   # If the FCIP Entity is a VE_Port/B_Access implementation [FC-BB-2]
   # residing in a switch, the fcip-entity-name is the Fibre Channel
   # Switch Name [FC-SW-3].  Otherwise, the fcip-entity-name is the
   # Fibre Channel Node Name [FC-FS] of the port (e.g., an Nx_Port)
   # associated with the FCIP Entity.
   # An entity representing multiple endpoints must register each of
   # the endpoints using SLPv2.

   transports = string M L
   tcp
   # This is a list of transport protocols that the registered entity
   # supports.  FCIP is currently supported over TCP only.
   tcp
```

```
mgmt-entity = string M O L
# The URL's of the management interface(s) are appropriate for SNMP,
# web-based, or telnet management of the FCIP Entity.
# Examples:
#  http://fcipentity.example.com:1080/
#  telnet://fcipentity.example.com

fcip-discovery-domain = string M L
fcip
# The fcip-discovery-domain string contains the name(s) of the FCIP
# discovery domain(s) to which this FCIP Entity belongs.

-------------------------template ends here-----------------------
```

6. Security Considerations

The SLPv2 security model as specified in [RFC2608] does not provide confidentiality, but does provide an authentication mechanism for UAs to assure that service advertisements only come from trusted SAs with the exception that it does not provide a mechanism for authenticating "zero-result responses". See [RFC3723] for a discussion of the SLPv2 [RFC2608] security model.

Once an FCIP Entity is discovered, authentication and authorization are handled by the FCIP protocol. It is the responsibility of the providers of these services to ensure that an inappropriately advertised or discovered service does not compromise their security.

When no security is used for SLPv2, there is a risk of distribution of false discovery information. The primary countermeasure for this risk is authentication. When this risk is a significant concern, IPsec SAs SHOULD be used for FCIP traffic subject to this risk to ensure that FCIP traffic only flows between endpoints that have participated in IKE authentication. For example, if an attacker distributes discovery information falsely claiming that it is an FCIP endpoint, it will lack the secret information necessary to successfully complete IKE authentication, and hence will be prevented from falsely sending or receiving FCIP traffic.

There remains a risk of a denial of service attack based on repeated use of false discovery information that will cause the initiation of IKE negotiation. The countermeasures for this are administrative configuration of each FCIP Entity to limit the peers that it is willing to communicate with (i.e., by IP address range and/or DNS domain), and maintenance of a negative authentication cache to avoid repeatedly contacting an FCIP Entity that fails to authenticate. These three measures (i.e., IP address range limits, DNS domain limits, negative authentication cache) MUST be implemented.

6.1. Security Implementation

Security for SLPv2 in an IP storage environment is specified in [RFC3723]. IPsec is mandatory-to-implement for IPS clients and servers. Thus, all IP storage clients, including those invoking SLP, can be assumed to support IPsec. SLP servers, however, cannot be assumed to implement IPsec, since there is no such requirement in standard SLP. In particular, SLP Directory Agents (DA) may be running on machines other than those running the IPS protocols.

IPsec SHOULD be implemented for SLPv2 as specified in [RFC3723]; this includes ESP with a non-null transform to provide both authentication and confidentiality.

Because the IP storage services have their own authentication capabilities when located, SLPv2 authentication is OPTIONAL to implement and use (as discussed in more detail in [RFC3723]).

7. IANA Considerations

This document describes two SLP Templates in Section 5. They should be registered in the IANA "SVRLOC Templates" registry. This process is described in the IANA Considerations section of [RFC2609].

8. Internationalization Considerations

SLP allows internationalized strings to be registered and retrieved. Attributes in the template that are not marked with an 'L' (literal) will be registered in a localized manner. An "en" (English) localization MUST be registered, and others MAY be registered.

9. Summary

This document describes how SLPv2 can be used by FCIP Entities to find other FCIP Entities. Service type templates for FCIP Entities are presented.

10. Acknowledgements

This document was produced by the FCIP discovery team, including Todd Sperry (Adaptec), Larry Lamars (SanValley), Robert Snively (Brocade), Ravi Natarajan (Lightsand), Anil Rijhsinghani (McData), and Venkat Rangan (Rhapsody Networks). Thanks also to Mark Bakke (Cisco) for initial help and consultation, and David Black, Erik Guttman, and James Kempf for assistance during expert review.

11. References

11.1. Normative References

[RFC2608] Guttman, E., Perkins, C., Veizades, J. and M. Day, "Service Location Protocol, Version 2", RFC 2608, June 1999.

[RFC2609] Guttman, E., Perkins, C. and J. Kempf, "Service Templates and Service: Schemes", RFC 2609, June 1999.

[RFC2119] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3821] Rajagopal, M., Bhagwat, R. and R. Weber, "Fibre Channel Over TCP/IP (FCIP)", RFC 3821, July 2004.

[FC-SW-3] Fibre Channel Switch Fabric - 3, ANSI INCITS 384-2004.

[FC-BB-2] Fibre Channel Backbone - 2, ANSI INCITS 372-2003.

[FC-FS] Fibre Channel Framing and Signaling, T11 Project 1331-D, Rev 1.90, April 9, 2003.

[RFC3723] Aboba, B., Tseng, J., Walker, J., Rangan, V. and F. Travostino, "Securing Block Storage Protocols over IP", RFC 3723, April 2004.

11.2. Informative References

[RFC3105] Kempf, J. and G. Montenegro, "Finding an RSIP Server with SLP", RFC 3105, October 2001.

12. Author's Address

David Peterson
Computer Network Technology (CNT)
6000 Nathan Lane North
Minneapolis, MN 55442

Phone: 763-268-6139
EMail: dap@cnt.com

13. Full Copyright Statement

Intellectual Property

Acknowledgement

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