Service Location Working Group   Mikael Pahmp
INTERNET DRAFT   Axis Communications
23 **June 1999**   Erik Guttman
                                                  Sun Microsystems, Inc
                                                         Kent Lidstrom
                                                  Axis Communications

The Networked Removable Storage Media Abstract Service Type
draft-ietf-svrloc-nrsm-scheme-00.txt

Status of This Memo

Abstract

   This document describes the Abstract Service Type for removable
   networked storage media. These include CD-ROMs, DVDs, DAT tapes,
   optical disks and other media types. Through the use of this
   template and the Service Location Procotocol [1] networked
   removable storage devices can advertise the currently available
   media and client systems can discover them.

1. Introduction

It is increasingly common to find networked storage devices which
are available using a range of access protocols. One common class
of storage devices allow removable storage (such as CD-ROMs, tapes
and optical disks) to be made available to the network simply by
inserting the media to the networked storage device.

This presents a problem: How are clients to discover which media
is currently available, or becomes avaiLable over time? By using
SLP [1] and advertising the attributes of the removable storage
media, the data on the storage media becomes accessible without
any prior client configuration.

Abstract Service templates are defined in [2].

2. Definitions

This document defines the Networked Removable Storage Media abstract
service type and two concrete types for the CIFS and NCP file sharing
protocols.

2.1. CIFS

The Common Internet File System (CIFS) protocol [3] is based on the
standard Server Message Block (SMB) protocol widely in use by
personal computers and workstations running a wide variety of
operating systems.

2.2. NCP

The NetWare Core Protocol (NCP) is one of the core protocols of the
NetWare (TM) operating system. No known public specification of this
protocol exists. Clients with access to a NCP client implementation
may still use the information available in a Networked Removable
Storage Media service: URL of the NCP concrete type to access the
media.

2.3. UNC

Networked Removable Storage Media service: URLs of the CIFS or NCP
concrete type uses a Uniform Naming Convention (UNC) [3] path string
as part of the url-path to describe the network path to the media.

Client implementations of the CIFS and NCP protocols usually accepts
UNC path strings for accessing shared network storage resources.

[3](#). **Networked Removable Storage Media Service Template**

  Name of submitters: Mikael Pahmp <Mikael.Pahmp@axis.com>
                      Erik Guttman <Erik.Guttman@sun.com>
                      Kent Lidstrom <Kent.Lidstrom@axis.com>

  Language of service template: en

  Security Considerations:
    The attributes included in the template, especially those concerning
    access control, are to be used to provide clients with configuration
    information regarding server features, not security per se.
    Authentication of and access control must be performed by the data
    access protocols themselves.

  Template Text:
  ------------------------template begins here-----------------------
  template-type = nrsm

  template-version = 0.0

  template-description =
    This is an abstract service type defining Networked Removable
    Storage Media.

  template-url-syntax =
    url-path =   ; Depends on the concrete service type.
                         ; See these templates.

  media-name = STRING
  ; This is the human readable name for this media. The name may be
  ; given by the media itself or user defined.

  capacity = INTEGER 0
  ; This is the memory capacity of the storage media, in units of
  ; kilobyte.

  writeable = BOOLEAN
  ; If this is TRUE, then the media is read/write. If it is FALSE

```
; the media is read-only.  Note that stating that media is read/
; write does not indicate that *anyone* may write to it.  Access
; control may be in place preventing unauthorized writing to the
; media.
```

```
  media-type = STRING L
  ; This is the media type of the removable media.  This can take
  ; one of the following values:
  ;
  ;   CDROM       The removable media is a CD with data content.
  ;   DVD         The media is a DVD.
  ;   JAZ         The media is a JAZ diskette.
  ;   DAT         The media is a DAT tape.
  ;   OPTICAL     The media is an optical disk.
  ;   TAPE        The media is a tape.
  CDROM,DVD,JAZ,DAT,OPTICAL,TAPE

  volume-description = STRING
  ; This string describes the contents of the removable storage
  ; media.  This string will be supplied to users in user interfaces
  ; to provide them with information to determine whether this
  ; particular storage media is of interest.

  access-control = BOOLEAN O
  ; This indicates that access control is being used to limit the
  ; availability of the storage media.  No attempt is made to define
  ; *what* access control is in place if the value of this attribute
  ; is TRUE.

  used-space=INTEGER O
  ; The amount of used space of the storage media,
  ; in units of kilobytes.

  file-system = STRING O
  ; The file system present on the networked storage media.  For
  ; example "ISO 9660 with Rock Ridge Extensions"

  worm = BOOLEAN O
  ; If this is TRUE, the media supports Write Once Read Many:  Thus
```

```
      ; data can be appended but not deleted or altered on the media.

      contact-person = STRING O
      ; The name of a contact person who is the operator of the removable
      ; storage media device.  This is the person to contact to
      ; unload or load particular media if the storage device if is in a
      ; remote location.  It is suggested that this string include
      ; information that would enable other humans to reach the contact
      ; person, such as a phone number or an email address.

      location = STRING O
      ; The physical location of the removable storage media device.
      ; This should be a descriptive human readable text.

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

[3.1](). Concrete 'nrsm' Service Template for CIFS

```
   Name of submitters: Mikael Pahmp <Mikael.Pahmp@axis.com>
                       Erik Guttman <Erik.Guttman@sun.com>
                       Kent Lidstrom <Kent.Lidstrom@axis.com>

   Language of service template: en

   Security Considerations:
     See the security considerations of the nrsm template.

   Template Text:
   ------------------------template begins here----------------------
   template-type = nrsm:cifs

   template-version = 0.0

   template-description =
     This is the concrete service template for CIFS access to Networked
     Removable Storage Media.

   template-url-syntax =
     url-path = "/" unc-path
     ; "unc-path" is a UNC path string as defined in [3] and escaped
     ; according to the rules in [2].

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

3.2. Concrete 'nrsm' Service Template for NCP

   Name of submitters: Mikael Pahmp <Mikael.Pahmp@axis.com>
                       Erik Guttman <Erik.Guttman@sun.com>
                       Kent Lidstrom <Kent.Lidstrom@axis.com>

   Language of service template: en

   Security Considerations:
     See the security considerations of the nrsm template.

   Template Text:
   ------------------------template begins here-----------------------
   template-type = nrsm:ncp

   template-version = 0.0

   template-description =
     This is the concrete service template for NCP access to Networked
     Removable Storage Media.

   template-url-syntax =
     url-path = "/" unc-path
     ; "unc-path" is a UNC path string as defined in [3] escaped
     ; according to the rules in [2].

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

4. Security Considerations

   The attributes included in the nrsm service template, especially those
   concerning access control, are to be used to provide clients with
   configuration information regarding server features, not security per
   se. Authentication of and access control must be performed by the
   data access protocols themselves.

   SLP [1] provides authentication features which allow clients to verify
   the authenticity of URLs and service attributes. If the attributes
   present in this service template are obtained in a different manner
   (than SLP) they may be supplied by a malicious source attempting to
   misdirect clients or hide available resources.

5. References

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

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

   [3] Leach, P. and D. Naik, "A Common Internet File System (CIFS/1.0)
       Protocol", draft-leach-cifs-v1-spec-01.txt,
       December 1997 (work in progress)

6. Authors' Addresses

   Mikael Pahmp   Erik Guttman
   Axis Communications   Sun Microsystems
   Scheelev. 16   Bahnstr. 2
   S-223 70 Lund, Sweden   74915 Waibstadt Germany
   Mikael.Pahmp@axis.com   Erik.Guttman@sun.com
   +46 46 270 1881   +49 7263 911 701

   Kent Lidstrom
   Axis Communications
   Scheelev. 16
   S-223 70 Lund, Sweden
   Kent.Lidstrom@axis.com
   +46 46 270 1941