INTERNET-DRAFT
<draft-ietf-aft-socks-ext-00>
Expires in six months

M. VanHeyningen
Aventail Corporation

22 July 1997

Feature Discovery: A Generic Extension Mechanism for SOCKS Version 5

Status of this Memo

Abstract

This document specifies a command extension to the SOCKS Version 5 protocol which enables compliant clients to discover features supported by the server. After discovering the support of such features, the client may use them in subsequent connections to that server. This mechanism does not provide for negotiation; it is a way of instructing the client what features the server supports, not establishing which features the client supports or wishes to use.

LIST-FEATURES Command

LIST-FEATURES is a new SOCKS V5 command, with an identifier of X'10' (16 decimal.) This command is formatted as a standard command, per section 4 of [SOCKS5]. Servers which do not support the LIST-FEATURES command should respond with the "Command not supported" error.

The client may set DST.ADDR and DST.PORT to the destination host and port of interest, or may send an IPv4 address of 0.0.0.0 to indicate the query is not for any specific host. The server may use this information, along with the address of the client, to customize the reply.

The client may request that the server hold the connection after the LIST-FEATURES command is completed to perform another SOCKS5 command by sending a FLAG field of X'01'.

The reply to the command is also formatted as a standard reply [SOCKS5, sec 6.] If the client has requested a persistent connection and the server chooses to grant that request, it returns a FLAG of X'01'. The address returned should be an IPv4 address of 0.0.0.0.

After the reply to the command is sent, the server sends a structure called the Feature Description List described below. After sending the FDL, the server holds the connection open for another command if it has granted a persistent connection; otherwise it closes it.

The Feature Description List

The structure passed by the server which advertises its full set of features is called the Feature Description List (FDL).

Terminology and syntax

The FDL is a tag-length-value (TLV) structure. Tags consist of a main tag and a subtag. These are written as separated by a hyphen, with the value following parentheses. For example:

```
TAG-SUBTAG("Hello.")
```

When encoded into the structure, the tag and subtag each map to one byte in the tag table. The length of the value is a single byte, followed by the value itself.

For example, if TAG is X'07' and SUBTAG is X'13, the above example would be encoded in hexidecimal as follows:

```
07 13 06 48 65 6c 6c 6f 2e
```

An FDL consists of zero or more of these associations concatenated together, and is terminated by a TVL with a TAG of END (X'FF').

FDL Meta-information

The tag FDL (X'00') is used to describe information about the FDL itself, rather than about the server.

At this time only one subtag, SCOPE (X'10') is defined. It defines the scope of the FDL, and advises whether a client which made a different FDL request would have been advertised the same feature set. Servers may provide this information, and clients may use it to

determine when the FDL must be re-fetched.

The following bytes may be included in the value field, and indicate the following restrictions on scope:

Value	Scope restriction
X'01'	Client address
X'02'	Authentication method used
X'03'	Destination host specified in request

SOCKS version support

The tag SOCKS (X'01') is used to advertise versions of the SOCKS protocol this server will support. The subtags are versions, as defined by the VER field. No semantics are currently defined for the value field.

Address type support

The tag ADDR (X'02') is used to advertise address types supported by this client. The subtags are ATYP values as defined in [SOCKS5]. No semantics are currently defined for the value field.

Authentication method support

The tag AUTH (X'03') is used to advertise authentication methods the server will support. The subtags are individual authentication METHOD identifiers. The semantics associated with the value are authentication-method specific; none are defined at this time.

Command support

The tag COMMAND (X'04') is used to advertise commands the server will support. The subtags are the CMD identifiers.

The semantics associated with the value are command-specific. For the LIST-FEATURES command, a value containing X'01' indicates the server supports persistent connections with this command.

Server information

The tag SERVER (X'10') is used to advertise information about the server. Several subtags are defined:

Subtag	Byte	Contents

```
      HOSTNAME X'01' Preferred hostname of the server
      URL      X'02' URL with info on this server (policy, config...)
      OPAQUE   X'03' Opaque identifier for this server
      LOAD     X'04' Current server load (in ASCII floating point)
```

Security Considerations

Since LIST-FEATURES is a SOCKS5 command, it may be performed only after authentication has taken place. Servers may wish to restrict access to this command to users who have already authenticated successfully, although that would also serve to limit its use in automating configuration for users who may not yet be able to authenticate successfully.

Servers may prefer not to advertise all the features they support, particualrly with regard to authentication methods supported.

References

[RFC 1928] Leech, M. et al, "SOCKS Protocol V5," April 1996

[SOCKS5] Leech, M. et al, "SOCKS Protocl V5," Internet Draft draft-ietf-aft-socks-pro-v5-00, March 1997, work in progress.

Author's Address

Marc VanHeyningen
Aventail Corporation
117 South Main Street; Suite 400
Seattle, WA 98104 USA

Phone: +1 (206) 777-5600
Email: marcvh@aventail.com