Stun

Table of contents

1. Overview

STUN is fully documented in RFC 2782. The discussion here provides additional information to ease the learning curve.

2. The Protocol

STUN can be broken down into three parts:

- server discovery
- binding
- shared secrets and authentication

2.1. Server Discovery

Server discovery is a procedure for locating the STUN servers provided by a particular domain. It is not essential and seems to be little used.

STUN servers can be discovered through the DNS. Full details can be found in RFC 2782 but a summary is provided here.

2.1.1. DNS Configuration

In order to configure the service you must have admin privileges for the domain name being configured. The exact way of effecting this varies with the name server being used. With BIND you add a line like

```
_stun._udp      SRV  10 0 3478  stun.xlattice.org.
```

This says that a STUN UDP service is supplied at port 3478 at stun.xlattice.org. The **10 0** are the priority and weight respectively and are not important if only one stun server is on line.

A second **_stun._tcp** line is necessary if the shared secret service part of the protocol is also being supplied over a TCP TLS connection.

Under UNIX/Linux you can query the availability of one of the services with a line like

```
dig -t SRV _stun._udp.xten.com
```

The reply will look like

```
_Service._Proto.Name TTL   Class SRV Priority Weight Port Target
_stun._udp.xten.net. 3600    IN  SRV    10       0    3478
xtunnels.xten.net.
```

We have added the first line to make the layout clear; only the second line will actually appear.

These records are conventionally attached to an organization's top-level domain. In the case above, for example, the service record is attached to **xten.com** rather than say **stun.xten.com**. This makes sense, as the query is in essence "what STUN-udp servers are available in your organization?" and the reply will be a list of available servers, with the **priority** and **weight** numbers providing a guide as to which should be used.

2.2. Binding

Binding is another discovery procedure: it enables a client behind a NAT to determine what its public IP address and port are, and it allows the client to explore how these change if the server's IP address and/or port number change. This information can be used to guess what kind of NAT the client is behind.

This is the basic STUN service, the one that must be supported by any STUN client or server.

2.3. SharedSecret

If authentication and security are issues, the client can obtain a short-lived shared secret from the server. This is done over a TCP connection running TLS. The shared secret can then be used to attach an SHA1-HMAC to messages between the client and the STUN server. See RFC 2104 for further information on HMACs.

Many public servers do not provide this part of the STUN protocol.

2.4. TLS

TLS is the IETF's version of SSL, the protocol used for secure Web connections (https).

In Java there are two commonly used TLS packages, PureTLS and JSSE. Tomcat uses these as alternatives, first trying to load PureTLS and then looking for JSSE.

It appears that PureTLS is no longer being supported. We have as yet not been able to make it work with Java 1.5.

3. Public STUN Servers

The table below lists STUN servers that we know to provide the basic UDP BindingRequest/Response service. If the **DNS?** column has a Y in it, there is an SRV record. If there is a Y in the **tcp?** column, the SRV record claims that they provide the TLS authentication service, but we haven't tested this.

domain name	DNS?	tcp?	remarks

stun.fwdnet.net	Y	Y	
stun01.sipphone.com	Y	Y	
stun.softjoys.com	Y	Y	
stun.voipbuster.com	N	?	
stun.voxgratia.org	N	?	SRV record says services not provided
stun.xten.net	N	N	
stun1.noc.ams-ix.net	Y	N	

3.1. Vovida Software

The open source C++ STUN server/client code available for download is commonly used on the public servers but does not support authentication. The tlsServer does not compile. The udp server returns an extension attribute **ServerName** which has a value of "Vovida.org 0.96".

This software is from a SourceForge project, http://sourceforge.net/projects/stun. At the time of writing the project has an open tracker item dated 2004-04-16 and entitled "support user/password hmac stuff".