DTMF SSH Reverse Tunnel

Why:
I needed to be able to access a remote node that was on a DHCP from the ISP and behind two routers. First option was to use a vpn. Then I thought of a GSM router. Both cost money. But a reverse ssh tunnel started using DTMF would be easy and cheap.

Node ---------WWW---------Server

Let's start off with the ssh reverse tunnel. First you need to make the ssh keys. This allows you to login without a password. Stop here if you think/feel that network security is important for your network. I'll be referencing Dave McKay article.
https://www.howtogeek.com/428413/what-is-reverse-ssh-tunneling-and-how-to-use-it/

Log in to your node as the repeater user (ASL). You should be in your home directory.

```
repater@asl2064:~ $
```

The tilde symbol (~) lets you know you're in your home directory. You can also type in pwd.

```
repeater@asl2064:~ $ pwd
/home/repeater
```

Type in ssh-keygen

```
repeater@asl2064:~ $ ssh-keygen
```

Default answers are ok.

Next we need to send the new key to the server.

```
repeater@asl2064:~ $ ssh-copy-id user@server.com
```

replace user with your login and change server.com to your domain or IP address.
You will be asked for your password. The key will be copied over to the server.
Note: use the -p flag if you use a different ssh port.
i.e.: ssh-copy-id -p xxxx user@server.com

Let's test it.

```
repeater@asl2064:~ $ ssh user@server.com
```

You should have connected without using a password.

The Reverse tunnel uses the -R flag.
Let's test it out.

```
repeater@asl2064:~ $ ssh -R 43022:localhost:22 user@server.com
```

Note: -p flag before the user@

Should be logged in to your server.
Login to your server and see if you can connect to your node.

```
repeater@server:~ $ ssh localhost -p 43022
```

Ok, let’s jump back on the node. Exit out of all the ssh connections.
We will use the sudo command next.

Change directory to /etc

```
repeater@asl2064:/etc $ sudo nano tunnel.sh
```

Next type/copy and edit the next two lines.

```
#!/bin/bash
/bin/su -s /bin/bash -c 'ssh -f -N -T -R 43022:localhost:22 user@server.com' user
```

Crtl X to exit and Y to save.

Let’s make the tunnel.sh executable.

```
repeater@asl2064:/etc $ chmod +x tunnel.sh
```

Let’s test it. .

```
repeater@asl2064:~ $ sudo /etc/tunnel.sh
```

You should now be able to login to your node from your server.

```
repeater@server:~ $ ssh localhost -p 43022
```

Now to get ASL to run the command.

Change directory to /etc/asterisk/

```
repeater@asl2064:~ $ cd /etc/asterisk
```

Edit rpt.conf

```
repeater@asl2064:/etc/astersk $ nano rpt.conf
```

Under ; Control operator (cop) functions. Change these to something other than these codes listed below!
add 980 = cmd,/etc/tunnel.sh

Ctrl X to exit Y to save.
restart Asterisk.

You should be able to key up your radio and send *980 to your node. Now on your server you can login to your node.

```
repeater@server:~ $ ssh localhost -p 43022
```

To kill the reverse tunnel. Do a ps aux | grep ssh.

```
repeater@asl2064:~ $ ps aux | grep ssh
root       516  0.0  0.4  10200  4704 ?        Ss   17:29   0:00 /usr/sbin/sshd -D
repeater  1324  0.0  0.3   8892  3104 ?        Ss   17:31   0:00 ssh -f -N -T -R
43022:localhost:22 -p 8022 repeater@144.202.120.35
```

You are looking for the line that has ssh -f -N -T -R

The numbers after repeater 1324 is the pid. Use kill -9 1324.

```
repeater@asl2064:~ $ kill -9 1324Connection to localhost closed by remote host.
Connection to localhost closed.
```