Comp 8005 – Final Project

Port Forwarder

Shan Bains & Jivanjot Brar

3/24/2014

Table of Contents

Objective

To design and implement a minimum-functionality Port Forwarder using any language of our choice using advanced TCP/IP programming techniques.

Description

Port forwarding is a mechanism that facilitates the forwarding of network traffic (connections) from one machine to another. The most common use of this technique is to allow an access to an externally available service (such as a web server), which is running on a server in a private LAN. In this way, remote client systems are able to connect to servers offering specific services within a private LAN, depending on the port that is used to connect to the service.

We have designed and implemented a port forwarding server that will forward incoming connection requests to specific ports/services from any IP address, to any user-specified IP address and port. For example, an inbound connection from 192.168.1.5 to port 80 may be forwarded to 192.168.1.25, port 80, or to 192.168.1.25, port 8005. Our server application was written using C programming while utilizing e-poll services.

Constraints

Your port forwarder must provide the following minimum functionality:

- Forward any IP: port pair to any other user-specified IP: port pair.
- The application must support multiple inbound connection requests, as well as simultaneous two-way traffic.
- Only TCP connections will be forwarded by the basic implementation.
- You are required to provide a detailed test case that will document the complete functionality of the port forwarding application. For example, beyond the basic functionality tests you may want to test and see how well your application performs under a heavy load, i.e., heavy throughput from multiple clients.
- Your application will read the IP: port combinations to forward to from a separate configuration file.

Design

The port forwarding server is designed to listen on various incoming ports and then transfer incoming connection from those ports to the file destination. The image below displays the connection and data flow between the client and the port forwarding machine and between port forwarding machine and the final destination machine. The image describes two client machines accessing the final server through the port forwarding machine. One client access the final server content using a web browser and tries to access data on port 80 of the server, where else the second client tries to access the final server using Ssh on port 22. Both clients connected to the port forwarding machine of port 8000 and 2200. These are the port that port forwarding server is listening on for new connections. The port forwarding server then connects with the final server and transfers the data from the client to the server and after receiving data from the server, the port forwarding server sends appropriate data back to the appropriate clients.

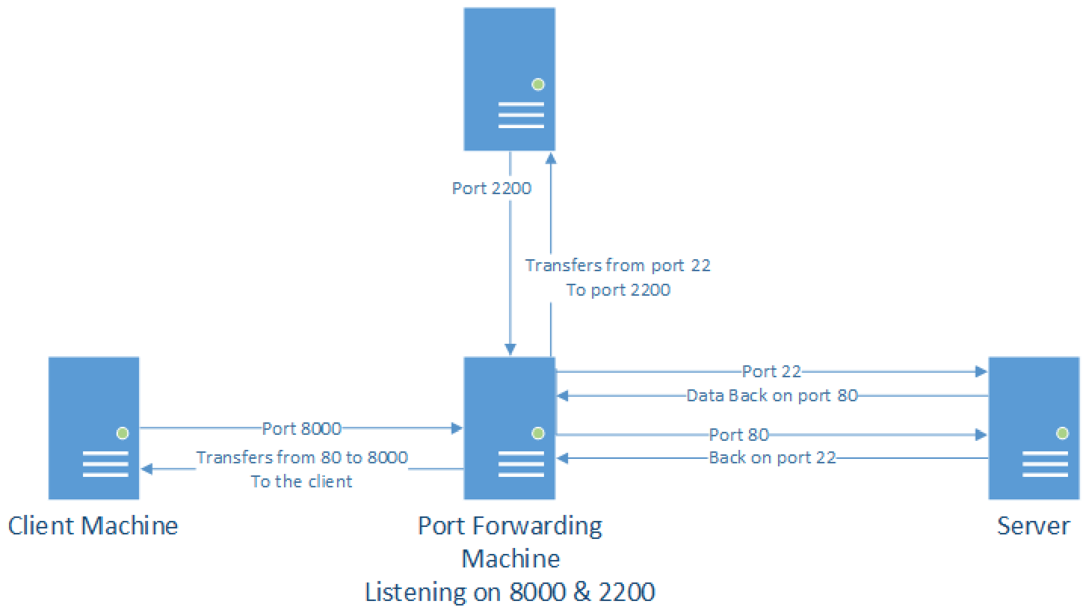


Figure 1: Basic Data flow diagram

The figure 2 below describes the same functionality described above in figure 1 in a greater detail. The figure describes three separate states of the port forwarding server.

State 1 includes accepting connections from the client and establishing connection with final destination machine described in the configuration file and then storing the two connections in a table in order to route the incoming data to the appropriate destination machine.

State 2 includes receiving data from the client and forwarding it to the appropriate final destination. For example in the figure 1, port forwarding machine receives data on port 8000 and then forwards the data to the final destination on port 80.

State 3 includes receiving data from the server machine and forwarding it to the appropriate client machine. For example in the figure 1, port forwarding machine receives data from the server on port 80 and port 22, it then looking at the connection table sends the data coming port 22 to port 2200 and data from port 80 to port 8000.

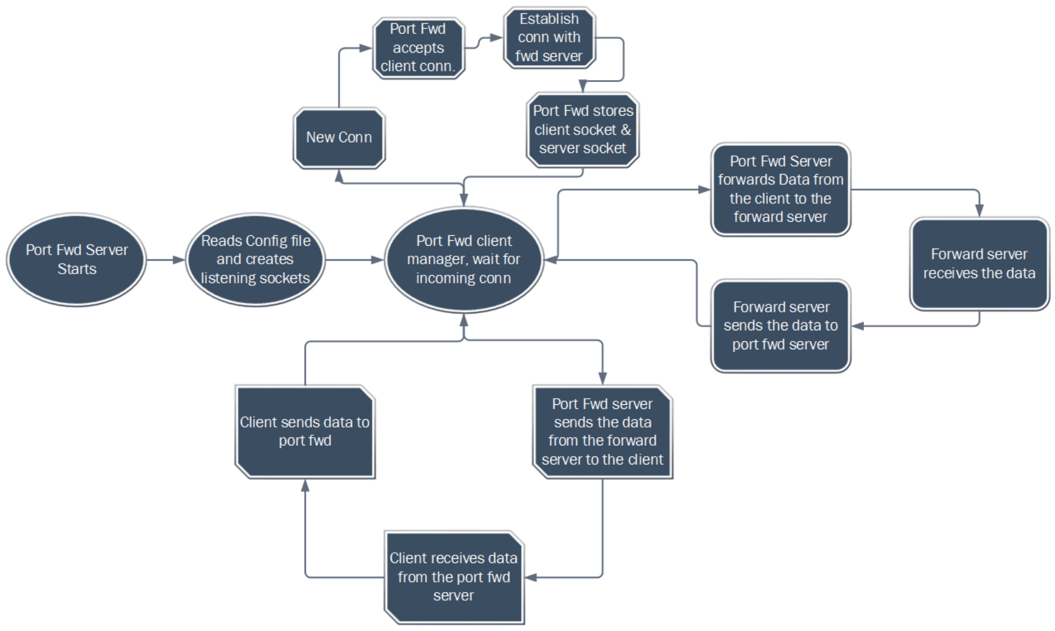

Port Fwd accepts client conn.
Establish conn with fwd server
New Conn
Port Fwd stores client socket & server socket
Port Fwd Server forwards Data from the client to the forward server
Port Fwd Server Starts
Reads Config file and creates listening sockets
Port Fwd client manager, wait for incoming conn
Forward server receives the data
Forward server sends the data to port fwd server
Client sends data to port fwd
Port Fwd server sends the data from the forward server to the client
Client receives data from the port fwd server

Figure 2: Detailed Data Flow Diagram

Port Forwarder Design Pseudo code

```
Main {
Read file "config"
Create sockets to listen the ports define in config file
Bind listening ports
    While (TRUE) {
        Block and listen for events
        Receive connection request from client
```

```
                Accept connection request from client
                Create connection with final server (Machine 3)
                Read & Forward request from the client to the server
                Read & Forward data response from the server to the client
                Keep connection running until the user ends it
        }
}
```

How to Use & Run the Application

Machine 1 (client) →Machine 2 (Port Forwarder) →Machine 3 (Server/Service)

1) Copy the whole Port_Forwarder folder to /root/Documents on Machine 2
2) Navigate to /Port_Forwarder/src/ folder
3) Edit the config file to the right ip address and ports for the service
    a. E.g. 8000 192.168.0.23 80 for http service (11 is the IP of Machine 3)
    b. E.g. 2200 192.168.0.23 22 for ssh service
    c. E.g. 2300 192.168.0.23 22 for Telnet service
4) Compile the Port Forwarder application by navigating to /Port_Forwarder/src/ folder in the Terminal and typing "make" command, the output will be "port_fd" executable file.
5) Make sure the services on the server (machine 3) are installed and running
    a. # yum install httpd*
    b. # yum install sshd*
    c. # yum install telnet-server
    d. # service httpd start
    e. # service sshd start
    f. # systemctl start xinetd.service
    g. # chkconfig telnet on
6) Make sure the services are installed and running on the client (machine 1)
    a. # yum install sshd*
    b. # yum install telnet
    c. # service sshd start
7) Run the program by navigating into /Port_Forwarder/src/ folder and typing "./port_fd command on Machine 2
8) Test http service

   a. Open a web-browser on Machine 1 and enter “192.168.0.x:8000” (x is the IP of Machine 2)
   b. If seeing the Fedora Test Page, it is working.

9) Test ssh service
   a. Open a terminal and enter “# 192.168.0.x –p 2200” where x is the IP of Machine 2 and 2200 is ssh service with port 22 in the config file
   b. If prompting for password, it is forwarded successfully

10) Test telnet service
   a. Open a terminal and enter “# 192.168.0.x –p 2300” where x is the IP of Machine 2 and 2300 is telnet service with port 23 in the config file
   b. If prompting for password, it is forwarded successfully

Testing

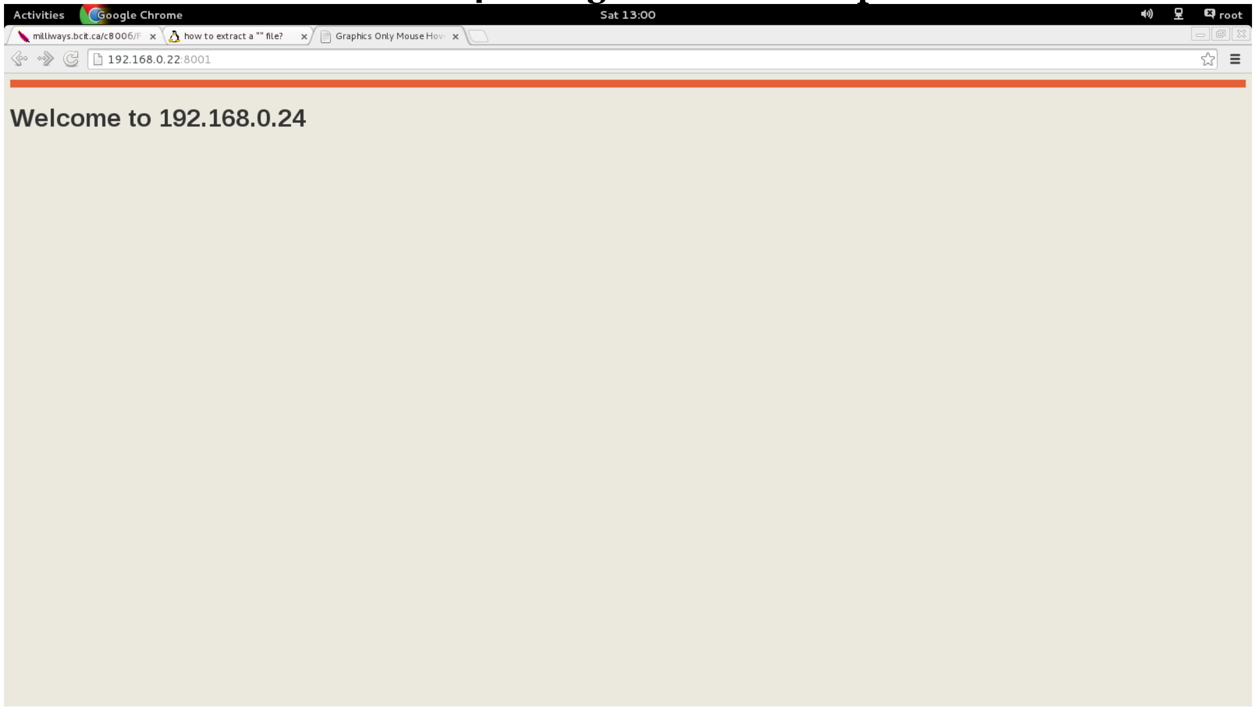
Port Forwarding from port 8001 to 80

Station 23 – running port forwarding application

```
root@DataComm Port_Forwarding]# ./port_fd
> Creating TCP socket
>> Waiting for Connections
```

Station 24 - running the web server with index.html page

Station 22 – access station 24 through station 22 on port 8001

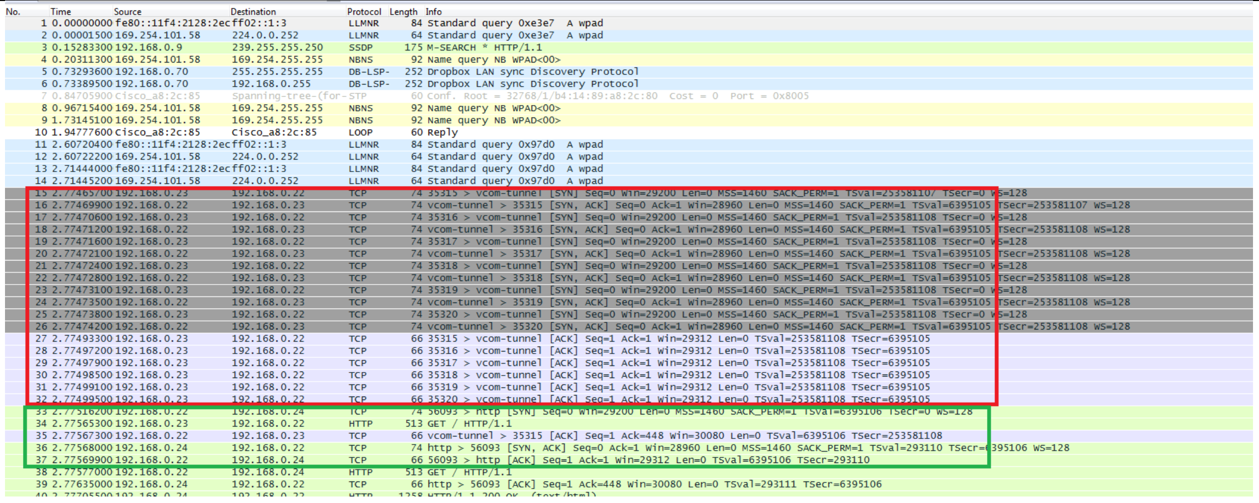


Welcome to 192.168.0.24

Station 23 – Final command line output

```
>>> PORT FWD: Accepted Connection from Machine 1 [192.168.0.23:35315]
 >>>> Connecting to Machine 3 - [192.168.0.24:80].
first_time: 6 >>> PORT FWD: Established Connection with Machine 3
[192.168.0.24:80]
```

WireShark Output – 3 Way handshake

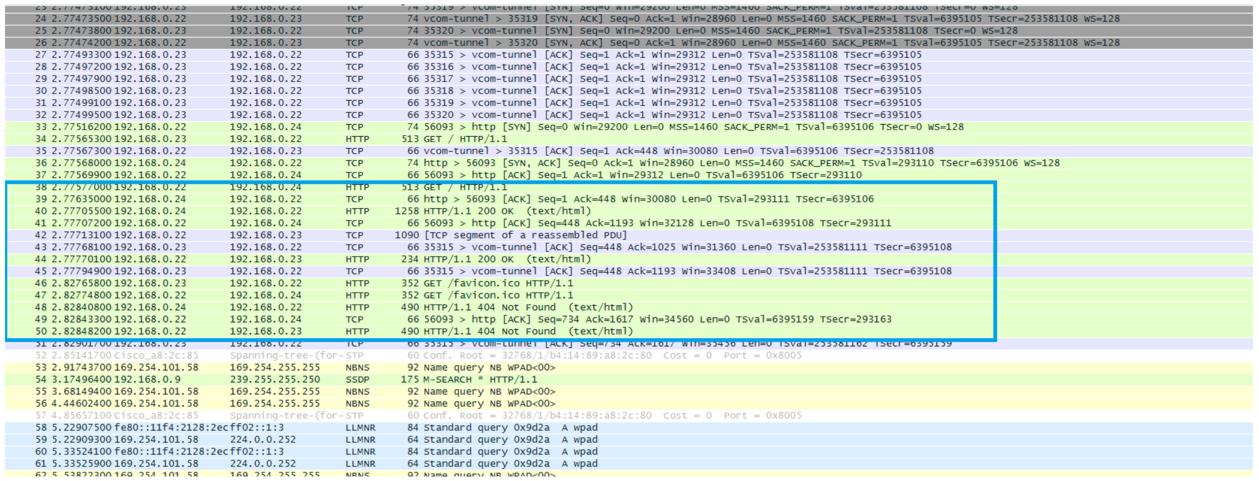


```
No.  Time       Source                   Destination            Protocol Length Info
   1 0.00000000 fe80::11f4:2128:2ec ff02::1:3              LLMNR      84 Standard query 0xe3e7  A wpad
   2 0.00001500 169.254.101.58           224.0.0.252            LLMNR      64 Standard query 0xe3e7  A wpad
   3 0.15283300 192.168.0.9              239.255.255.250        SSDP      175 M-SEARCH * HTTP/1.1
   4 0.20311300 169.254.101.58           169.254.255.255        NBNS       92 Name query NB WPAD<00>
   5 0.73293600 192.168.0.70             255.255.255.255        DB-LSP-   252 Dropbox LAN sync Discovery Protocol
   6 0.73389500 192.168.0.70             192.168.0.255          DB-LSP-   252 Dropbox LAN sync Discovery Protocol
   7 0.84705900 Cisco_a8:2c:85           Spanning-tree-(for-    STP        60 Conf. Root = 32768/1/b4:14:89:a8:2c:80  Cost = 0  Port = 0x8005
   8 0.96715400 169.254.101.58           169.254.255.255        NBNS       92 Name query NB WPAD<00>
   9 1.73145100 169.254.101.58           169.254.255.255        NBNS       92 Name query NB WPAD<00>
  10 1.94777600 Cisco_a8:2c:85           Cisco_a8:2c:85         LOOP       60 Reply
  11 2.60720400 fe80::11f4:2128:2ec ff02::1:3              LLMNR      84 Standard query 0x97d0  A wpad
  12 2.60722200 169.254.101.58           224.0.0.252            LLMNR      64 Standard query 0x97d0  A wpad
  13 2.71444000 fe80::11f4:2128:2ec ff02::1:3              LLMNR      84 Standard query 0x97d0  A wpad
  14 2.71445200 169.254.101.58           224.0.0.252            LLMNR      64 Standard query 0x97d0  A wpad
  15 2.77465700 192.168.0.23             192.168.0.22           TCP        74 35315 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581107 TSecr=0 WS=128
  16 2.77469900 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35315 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581107 WS=128
  17 2.77470600 192.168.0.23             192.168.0.22           TCP        74 35316 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581108 TSecr=0 WS=128
  18 2.77471200 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35316 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581108 WS=128
  19 2.77471600 192.168.0.23             192.168.0.22           TCP        74 35317 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581108 TSecr=0 WS=128
  20 2.77472100 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35317 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581108 WS=128
  21 2.77472400 192.168.0.23             192.168.0.22           TCP        74 35318 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581108 TSecr=0 WS=128
  22 2.77472800 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35318 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581108 WS=128
  23 2.77473100 192.168.0.23             192.168.0.22           TCP        74 35319 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581108 TSecr=0 WS=128
  24 2.77473500 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35319 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581108 WS=128
  25 2.77473800 192.168.0.23             192.168.0.22           TCP        74 35320 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581108 TSecr=0 WS=128
  26 2.77474200 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35320 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581108 WS=128
  27 2.77493300 192.168.0.23             192.168.0.22           TCP        66 35315 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  28 2.77497200 192.168.0.23             192.168.0.22           TCP        66 35316 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  29 2.77497900 192.168.0.23             192.168.0.22           TCP        66 35317 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  30 2.77498500 192.168.0.23             192.168.0.22           TCP        66 35318 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  31 2.77499100 192.168.0.23             192.168.0.22           TCP        66 35319 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  32 2.77499500 192.168.0.23             192.168.0.22           TCP        66 35320 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  33 2.77516200 192.168.0.22             192.168.0.24           TCP        74 56093 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=6395106 TSecr=0 WS=128
  34 2.77565300 192.168.0.23             192.168.0.22           HTTP      513 GET / HTTP/1.1
  35 2.77567300 192.168.0.22             192.168.0.23           TCP        66 vcom-tunnel > 35315 [ACK] Seq=1 Ack=448 Win=30080 Len=0 TSval=6395106 TSecr=253581108
  36 2.77568000 192.168.0.24             192.168.0.22           TCP        74 http > 56093 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=293110 TSecr=6395106 WS=128
  37 2.77569900 192.168.0.22             192.168.0.24           TCP        66 56093 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=6395106 TSecr=293110
  38 2.77577000 192.168.0.22             192.168.0.24           HTTP      513 GET / HTTP/1.1
  39 2.77635000 192.168.0.24             192.168.0.22           TCP        66 http > 56093 [ACK] Seq=1 Ack=448 Win=30080 Len=0 TSval=293111 TSecr=6395106
  40 2.77705500 192.168.0.24             192.168.0.22           HTTP     1258 HTTP/1.1 200 OK  (text/html)
```

The section in red shows the 3 way handshake that took place between the port forward machine (Station 23) and the client machine (Station 22)

The section in the green shows the 3 way handshake that took place between the client (Station 22) and the web server (Station 24).

WireShark Output



```
  23 2.77473100 192.168.0.23             192.168.0.22           TCP        74 35319 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581108 TSecr=0 WS=128
  24 2.77473500 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35319 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581108 WS=128
  25 2.77473800 192.168.0.23             192.168.0.22           TCP        74 35320 > vcom-tunnel [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=253581108 TSecr=0 WS=128
  26 2.77474200 192.168.0.22             192.168.0.23           TCP        74 vcom-tunnel > 35320 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=6395105 TSecr=253581108 WS=128
  27 2.77493300 192.168.0.23             192.168.0.22           TCP        66 35315 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  28 2.77497200 192.168.0.23             192.168.0.22           TCP        66 35316 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  29 2.77497900 192.168.0.23             192.168.0.22           TCP        66 35317 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  30 2.77498500 192.168.0.23             192.168.0.22           TCP        66 35318 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  31 2.77499100 192.168.0.23             192.168.0.22           TCP        66 35319 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  32 2.77499500 192.168.0.23             192.168.0.22           TCP        66 35320 > vcom-tunnel [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=253581108 TSecr=6395105
  33 2.77516200 192.168.0.22             192.168.0.24           TCP        74 56093 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=6395106 TSecr=0 WS=128
  34 2.77565300 192.168.0.23             192.168.0.22           HTTP      513 GET / HTTP/1.1
  35 2.77567300 192.168.0.22             192.168.0.23           TCP        66 vcom-tunnel > 35315 [ACK] Seq=1 Ack=448 Win=30080 Len=0 TSval=6395106 TSecr=253581108
  36 2.77568000 192.168.0.24             192.168.0.22           TCP        74 http > 56093 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=293110 TSecr=6395106 WS=128
  37 2.77569900 192.168.0.22             192.168.0.24           TCP        66 56093 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=6395106 TSecr=293110
  38 2.77577000 192.168.0.22             192.168.0.24           HTTP      513 GET / HTTP/1.1
  39 2.77635000 192.168.0.24             192.168.0.22           TCP        66 http > 56093 [ACK] Seq=1 Ack=448 Win=30080 Len=0 TSval=293111 TSecr=6395106
  40 2.77705500 192.168.0.24             192.168.0.22           HTTP     1258 HTTP/1.1 200 OK  (text/html)
  41 2.77707200 192.168.0.22             192.168.0.24           TCP        66 56093 > http [ACK] Seq=448 Ack=1193 Win=32128 Len=0 TSval=6395108 TSecr=293111
  42 2.77713100 192.168.0.22             192.168.0.23           TCP      1090 [TCP segment of a reassembled PDU]
  43 2.77768100 192.168.0.23             192.168.0.22           TCP        66 35315 > vcom-tunnel [ACK] Seq=448 Ack=1025 Win=31360 Len=0 TSval=253581111 TSecr=6395108
  44 2.77770100 192.168.0.22             192.168.0.23           HTTP      234 HTTP/1.1 200 OK  (text/html)
  45 2.77794900 192.168.0.23             192.168.0.22           TCP        66 35315 > vcom-tunnel [ACK] Seq=448 Ack=1193 Win=33408 Len=0 TSval=253581111 TSecr=6395108
  46 2.82765800 192.168.0.23             192.168.0.22           HTTP      352 GET /favicon.ico HTTP/1.1
  47 2.82774800 192.168.0.22             192.168.0.24           HTTP      352 GET /favicon.ico HTTP/1.1
  48 2.82840800 192.168.0.24             192.168.0.22           HTTP      490 HTTP/1.1 404 Not Found  (text/html)
  49 2.82843300 192.168.0.22             192.168.0.24           TCP        66 56093 > http [ACK] Seq=734 Ack=1617 Win=34560 Len=0 TSval=6395159 TSecr=293163
  50 2.82848200 192.168.0.22             192.168.0.23           HTTP      490 HTTP/1.1 404 Not Found  (text/html)
  51 2.82901700 192.168.0.23             192.168.0.22           TCP        66 35315 > vcom-tunnel [ACK] Seq=734 Ack=1617 Win=33456 Len=0 TSval=253581162 TSecr=6395159
  52 2.85141700 Cisco_a8:2c:85           Spanning-tree-(for-    STP        60 Conf. Root = 32768/1/b4:14:89:a8:2c:80  Cost = 0  Port = 0x8005
  53 2.91743700 169.254.101.58           169.254.255.255        NBNS       92 Name query NB WPAD<00>
  54 3.17496400 192.168.0.9              239.255.255.250        SSDP      175 M-SEARCH * HTTP/1.1
  55 3.68149400 169.254.101.58           169.254.255.255        NBNS       92 Name query NB WPAD<00>
  56 4.44602400 169.254.101.58           169.254.255.255        NBNS       92 Name query NB WPAD<00>
  57 4.85657100 Cisco_a8:2c:85           Spanning-tree-(for-    STP        60 Conf. Root = 32768/1/b4:14:89:a8:2c:80  Cost = 0  Port = 0x8005
  58 5.22907500 fe80::11f4:2128:2ec ff02::1:3              LLMNR      84 Standard query 0x9d2a  A wpad
  59 5.22909300 169.254.101.58           224.0.0.252            LLMNR      64 Standard query 0x9d2a  A wpad
  60 5.33524100 fe80::11f4:2128:2ec ff02::1:3              LLMNR      84 Standard query 0x9d2a  A wpad
  61 5.33525900 169.254.101.58           224.0.0.252            LLMNR      64 Standard query 0x9d2a  A wpad
  62 5.53822300 169.254.101.58           169.254.255.255        NBNS       92 Name query NB WPAD<00>
```

The section in blue shows the data transfer that took place between the port forwarder, the webserver and the client machine.

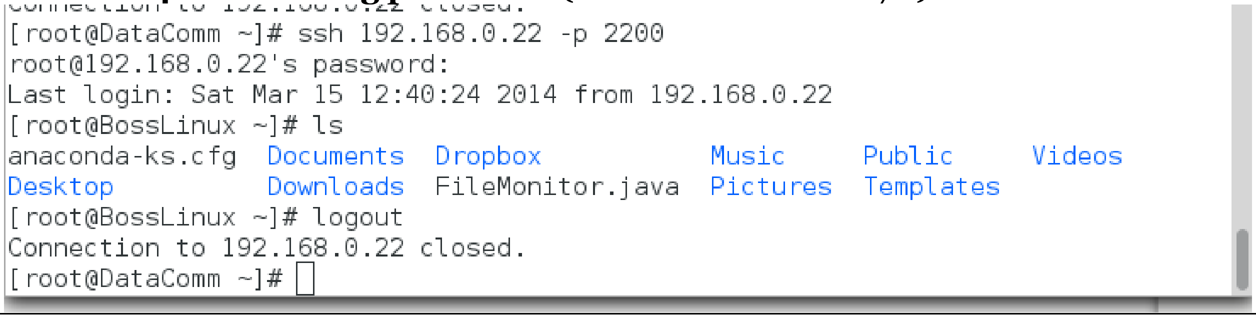
Port Forwarding SSH from port 2200 to 22

Port Forwarding application running on station 23

Command line output:

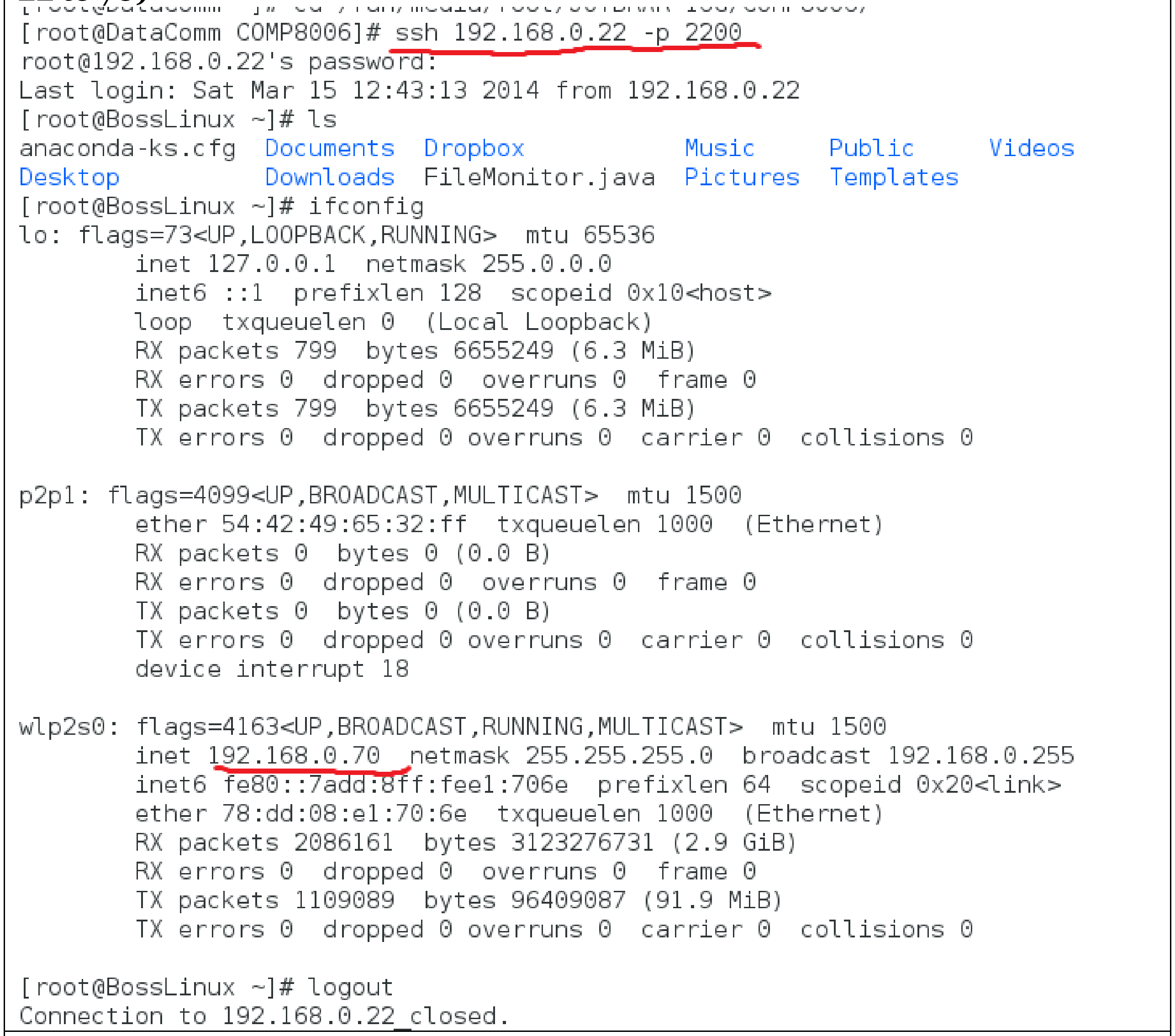
```
[root@DataComm Port_Forwarding]# ./port_fd
> Creating TCP socket
>> Waiting for Connections
```

Station 24 – SSH using port 2200 (from station 22 to 70)



```
[root@DataComm ~]# ssh 192.168.0.22 -p 2200
root@192.168.0.22's password:
Last login: Sat Mar 15 12:40:24 2014 from 192.168.0.22
[root@BossLinux ~]# ls
anaconda-ks.cfg  Documents  Dropbox          Music     Public     Videos
Desktop          Downloads  FileMonitor.java  Pictures  Templates
[root@BossLinux ~]# logout
Connection to 192.168.0.22 closed.
[root@DataComm ~]# 
```

Station 22 – IFCONFIG settings after SSH has been completed (from station 22 to 70)

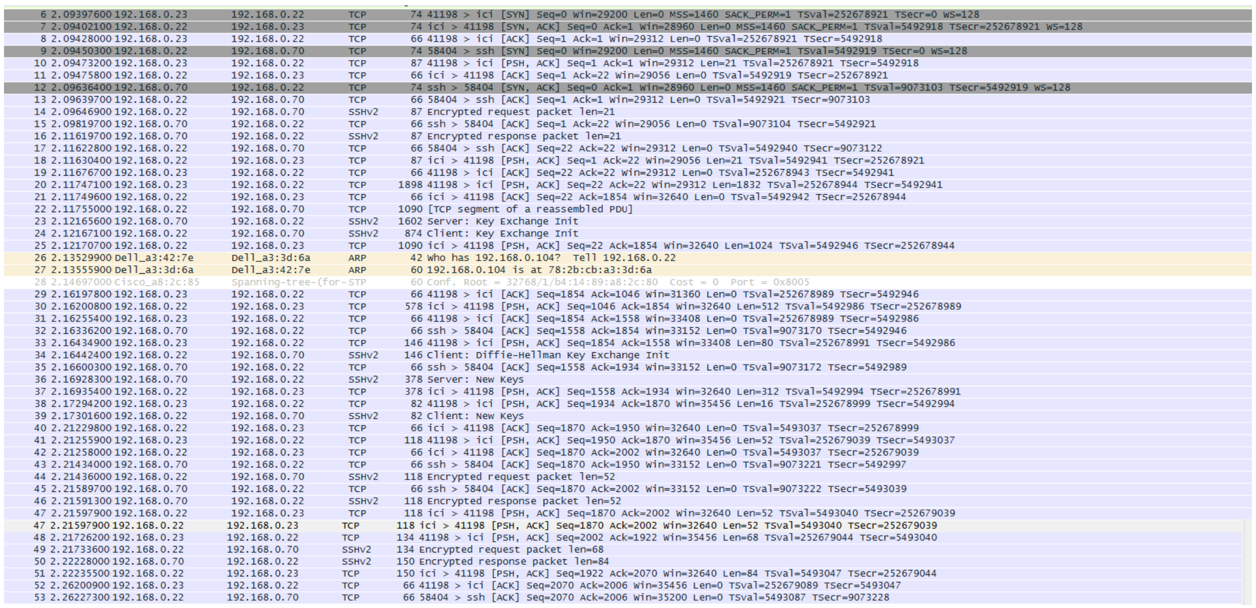


```
[root@DataComm COMP8006]# ssh 192.168.0.22 -p 2200
root@192.168.0.22's password:
Last login: Sat Mar 15 12:43:13 2014 from 192.168.0.22
[root@BossLinux ~]# ls
anaconda-ks.cfg  Documents  Dropbox          Music     Public     Videos
Desktop          Downloads  FileMonitor.java  Pictures  Templates
[root@BossLinux ~]# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 799  bytes 6655249 (6.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 799  bytes 6655249 (6.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

p2p1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 54:42:49:65:32:ff  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.70  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::7add:8ff:fee1:706e  prefixlen 64  scopeid 0x20<link>
        ether 78:dd:08:e1:70:6e  txqueuelen 1000  (Ethernet)
        RX packets 2086161  bytes 3123276731 (2.9 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1109089  bytes 96409087 (91.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@BossLinux ~]# logout
Connection to 192.168.0.22 closed.
```

Station 23 – Final command line output

```
>>> PORT FWD: Accepted Connection from Machine 1 [192.168.0.23:41198]
 >>>> Connecting to Machine 3 - [192.168.0.70:22].
first_time: 9 >>> PORT FWD: Established Connection with Machine 3
[192.168.0.70:22]
```

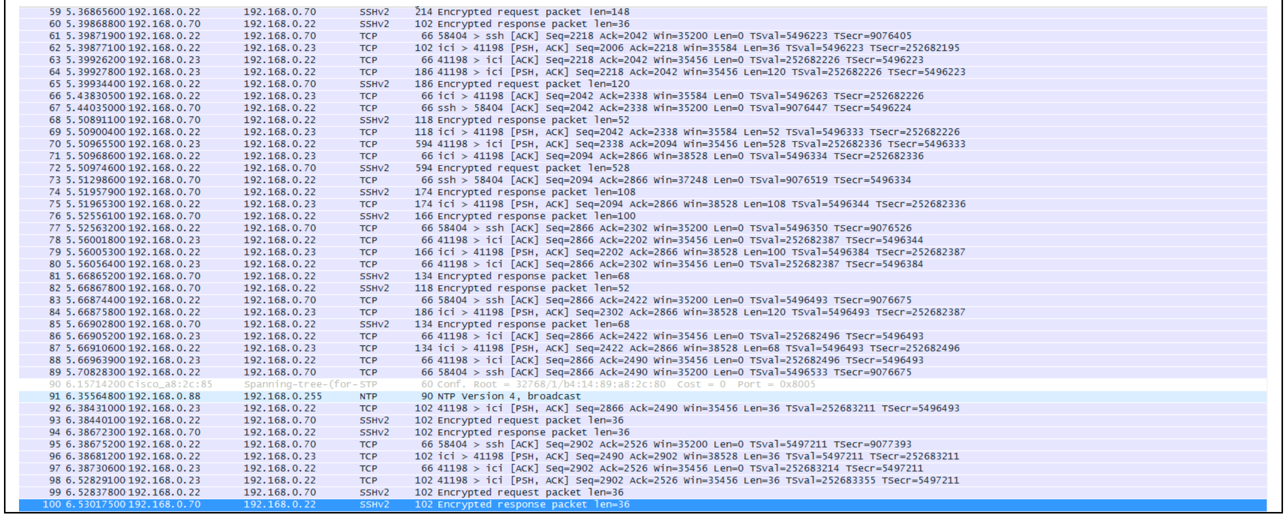
WireShark Output – 3 Way Handshake



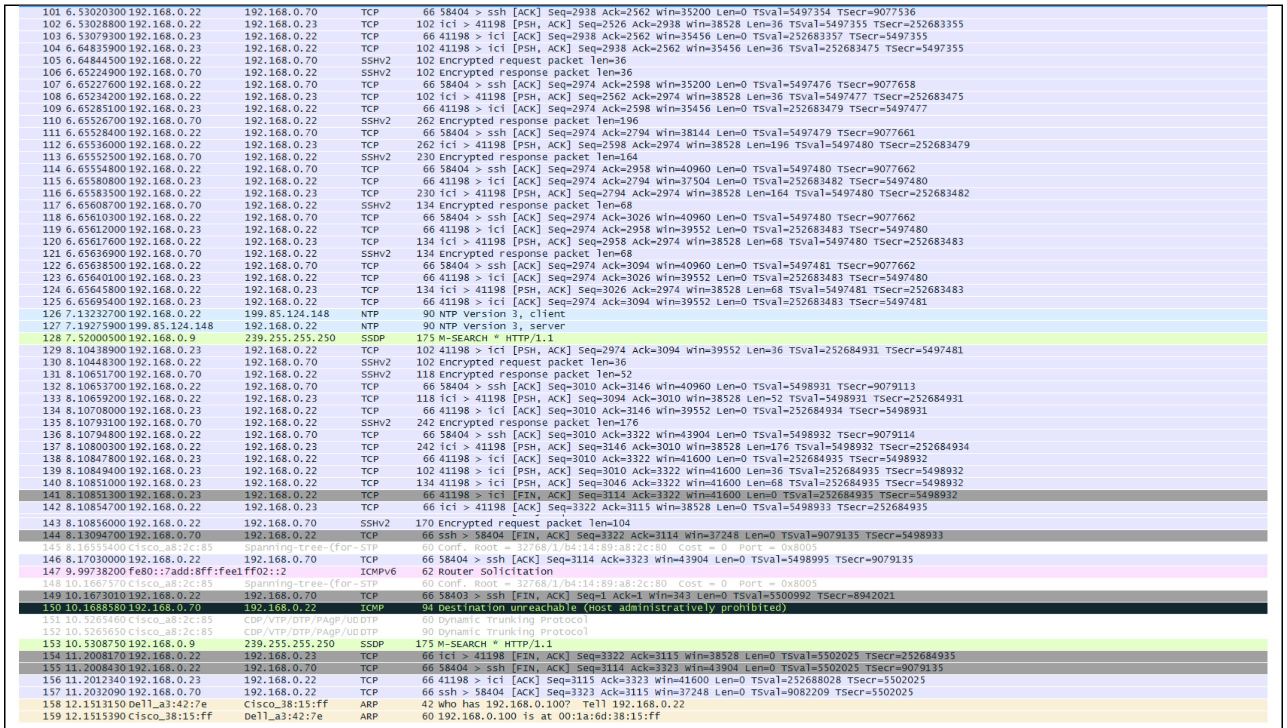
```
  6 2.09397600 192.168.0.23   192.168.0.22   TCP     74 41198 > ici [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=252678921 TSecr=0 WS=128
  7 2.09402100 192.168.0.22   192.168.0.23   TCP     74 ici > 41198 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=5492918 TSecr=252678921 WS=128
  8 2.09428000 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=252678921 TSecr=5492918
  9 2.09450300 192.168.0.22   192.168.0.70   TCP     74 58404 > ssh [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=5492919 TSecr=0 WS=128
 10 2.09473200 192.168.0.23   192.168.0.22   TCP     87 41198 > ici [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=21 TSval=252678921 TSecr=5492918
 11 2.09475800 192.168.0.22   192.168.0.23   TCP     66 ici > 41198 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSval=5492919 TSecr=252678921
 12 2.09636400 192.168.0.70   192.168.0.22   TCP     74 ssh > 58404 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=9073103 TSecr=5492919 WS=128
 13 2.09639700 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=5492921 TSecr=9073103
 14 2.09646900 192.168.0.22   192.168.0.70   SSHv2   87 Encrypted request packet len=21
 15 2.09819700 192.168.0.70   192.168.0.22   TCP     66 ssh > 58404 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSval=9073104 TSecr=5492921
 16 2.11619700 192.168.0.70   192.168.0.22   SSHv2   87 Encrypted response packet len=21
 17 2.11622800 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=22 Ack=22 Win=29312 Len=0 TSval=5492940 TSecr=9073122
 18 2.11630400 192.168.0.22   192.168.0.23   TCP     87 ici > 41198 [PSH, ACK] Seq=1 Ack=22 Win=29056 Len=21 TSval=5492941 TSecr=252678921
 19 2.11676700 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=22 Ack=22 Win=29312 Len=0 TSval=252678943 TSecr=5492941
 20 2.11747100 192.168.0.23   192.168.0.22   TCP   1898 41198 > ici [PSH, ACK] Seq=22 Ack=22 Win=29312 Len=1832 TSval=252678944 TSecr=5492941
 21 2.11749600 192.168.0.22   192.168.0.23   TCP     66 ici > 41198 [ACK] Seq=22 Ack=1854 Win=32640 Len=0 TSval=5492942 TSecr=252678944
 22 2.11755000 192.168.0.22   192.168.0.70   TCP   1090 [TCP segment of a reassembled PDU]
 23 2.12165600 192.168.0.70   192.168.0.22   SSHv2 1602 Server: Key Exchange Init
 24 2.12167100 192.168.0.22   192.168.0.70   SSHv2  874 Client: Key Exchange Init
 25 2.12170700 192.168.0.22   192.168.0.23   TCP   1090 ici > 41198 [PSH, ACK] Seq=22 Ack=1854 Win=32640 Len=1024 TSval=5492946 TSecr=252678944
 26 2.13529900 Dell_a3:42:7e  Dell_a3:3d:6a  ARP     42 Who has 192.168.0.104?  Tell 192.168.0.22
 27 2.13555900 Dell_a3:3d:6a  Dell_a3:42:7e  ARP     60 192.168.0.104 is at 78:2b:cb:a3:3d:6a
 28 2.14697000 Cisco_a8:2c:85 Spanning-tree-(for-STP 60 Conf. Root = 32768/1/b4:14:89:a8:2c:80  Cost = 0  Port = 0x8005
 29 2.16197800 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=1854 Ack=1046 Win=31360 Len=0 TSval=252678989 TSecr=5492946
 30 2.16200800 192.168.0.22   192.168.0.23   TCP    578 ici > 41198 [PSH, ACK] Seq=1046 Ack=1854 Win=32640 Len=512 TSval=5492986 TSecr=252678989
 31 2.16255400 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=1854 Ack=1558 Win=33408 Len=0 TSval=252678989 TSecr=5492986
 32 2.16336200 192.168.0.70   192.168.0.22   TCP     66 ssh > 58404 [ACK] Seq=1558 Ack=1854 Win=33152 Len=0 TSval=9073170 TSecr=5492946
 33 2.16434900 192.168.0.23   192.168.0.22   TCP    146 41198 > ici [PSH, ACK] Seq=1854 Ack=1558 Win=33408 Len=80 TSval=252678991 TSecr=5492986
 34 2.16442400 192.168.0.22   192.168.0.70   SSHv2  146 Client: Diffie-Hellman Key Exchange Init
 35 2.16600300 192.168.0.70   192.168.0.22   TCP     66 ssh > 58404 [ACK] Seq=1558 Ack=1934 Win=33152 Len=0 TSval=9073172 TSecr=5492989
 36 2.16928300 192.168.0.70   192.168.0.22   SSHv2  378 Server: New Keys
 37 2.16935400 192.168.0.22   192.168.0.23   TCP    378 ici > 41198 [PSH, ACK] Seq=1558 Ack=1934 Win=32640 Len=312 TSval=5492994 TSecr=252678991
 38 2.17294200 192.168.0.23   192.168.0.22   TCP     82 41198 > ici [PSH, ACK] Seq=1934 Ack=1870 Win=35456 Len=16 TSval=252678999 TSecr=5492994
 39 2.17301600 192.168.0.22   192.168.0.70   SSHv2   82 Client: New Keys
 40 2.21229800 192.168.0.22   192.168.0.23   TCP     66 ici > 41198 [ACK] Seq=1870 Ack=1950 Win=32640 Len=0 TSval=5493037 TSecr=252678999
 41 2.21255900 192.168.0.23   192.168.0.22   TCP    118 41198 > ici [PSH, ACK] Seq=1950 Ack=1870 Win=35456 Len=52 TSval=252679039 TSecr=5493037
 42 2.21258000 192.168.0.22   192.168.0.23   TCP     66 ici > 41198 [ACK] Seq=1870 Ack=2002 Win=32640 Len=0 TSval=5493037 TSecr=252679039
 43 2.21434000 192.168.0.70   192.168.0.22   TCP     66 ssh > 58404 [ACK] Seq=1870 Ack=1950 Win=33152 Len=0 TSval=9073221 TSecr=5492997
 44 2.21436000 192.168.0.22   192.168.0.70   SSHv2  118 Encrypted request packet len=52
 45 2.21589700 192.168.0.70   192.168.0.22   TCP     66 ssh > 58404 [ACK] Seq=1870 Ack=2002 Win=33152 Len=0 TSval=9073222 TSecr=5493039
 46 2.21591300 192.168.0.70   192.168.0.22   SSHv2  118 Encrypted response packet len=52
 47 2.21597900 192.168.0.22   192.168.0.23   TCP    118 ici > 41198 [PSH, ACK] Seq=1870 Ack=2002 Win=32640 Len=52 TSval=5493040 TSecr=252679039
 47 2.21597900 192.168.0.22   192.168.0.23   TCP    118 ici > 41198 [PSH, ACK] Seq=1870 Ack=2002 Win=32640 Len=52 TSval=5493040 TSecr=252679039
 48 2.21726200 192.168.0.23   192.168.0.22   TCP    134 41198 > ici [PSH, ACK] Seq=2002 Ack=1922 Win=35456 Len=68 TSval=252679044 TSecr=5493040
 49 2.21733600 192.168.0.22   192.168.0.70   SSHv2  134 Encrypted request packet len=68
 50 2.22228000 192.168.0.70   192.168.0.22   SSHv2  150 Encrypted response packet len=84
 51 2.22235500 192.168.0.22   192.168.0.23   TCP    150 ici > 41198 [PSH, ACK] Seq=1922 Ack=2070 Win=32640 Len=84 TSval=5493047 TSecr=252679044
 52 2.26200900 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=2070 Ack=2006 Win=35456 Len=0 TSval=252679089 TSecr=5493047
 53 2.26227300 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=2070 Ack=2006 Win=35200 Len=0 TSval=5493087 TSecr=9073228
```

The image above shows the 3 way handshake that takes place between the port forwarding server, host and client machine.

WireShark Output – SSH activity



```
 59 5.36865600 192.168.0.22   192.168.0.70   SSHv2  214 Encrypted request packet len=148
 60 5.39868800 192.168.0.70   192.168.0.22   SSHv2  102 Encrypted response packet len=36
 61 5.39871900 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=2218 Ack=2042 Win=35200 Len=0 TSval=5496223 TSecr=9076405
 62 5.39877100 192.168.0.22   192.168.0.23   TCP    102 ici > 41198 [PSH, ACK] Seq=2006 Ack=2218 Win=35584 Len=36 TSval=5496223 TSecr=252682195
 63 5.39926200 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=2218 Ack=2042 Win=35456 Len=0 TSval=252682226 TSecr=5496223
 64 5.39927800 192.168.0.23   192.168.0.22   TCP    186 41198 > ici [PSH, ACK] Seq=2218 Ack=2042 Win=35456 Len=120 TSval=252682226 TSecr=5496223
 65 5.39934400 192.168.0.22   192.168.0.70   SSHv2  186 Encrypted request packet len=120
 66 5.43830500 192.168.0.22   192.168.0.23   TCP     66 ici > 41198 [ACK] Seq=2042 Ack=2338 Win=35584 Len=0 TSval=5496263 TSecr=252682226
 67 5.44035000 192.168.0.70   192.168.0.22   TCP     66 ssh > 58404 [ACK] Seq=2042 Ack=2338 Win=35200 Len=0 TSval=9076447 TSecr=5496224
 68 5.50891100 192.168.0.70   192.168.0.22   SSHv2  118 Encrypted response packet len=52
 69 5.50900400 192.168.0.22   192.168.0.23   TCP    118 ici > 41198 [PSH, ACK] Seq=2042 Ack=2338 Win=35584 Len=52 TSval=5496333 TSecr=252682226
 70 5.50965500 192.168.0.23   192.168.0.22   TCP    594 41198 > ici [PSH, ACK] Seq=2338 Ack=2094 Win=35456 Len=528 TSval=252682336 TSecr=5496333
 71 5.50968600 192.168.0.22   192.168.0.23   TCP     66 ici > 41198 [ACK] Seq=2094 Ack=2866 Win=38528 Len=0 TSval=5496334 TSecr=252682336
 72 5.50974600 192.168.0.22   192.168.0.70   SSHv2  594 Encrypted request packet len=528
 73 5.51298600 192.168.0.70   192.168.0.22   TCP     66 ssh > 58404 [ACK] Seq=2094 Ack=2866 Win=37248 Len=0 TSval=9076519 TSecr=5496334
 74 5.51957900 192.168.0.70   192.168.0.22   SSHv2  174 Encrypted response packet len=108
 75 5.51965300 192.168.0.22   192.168.0.23   TCP    174 ici > 41198 [PSH, ACK] Seq=2094 Ack=2866 Win=38528 Len=108 TSval=5496344 TSecr=252682336
 76 5.52556100 192.168.0.70   192.168.0.22   SSHv2  166 Encrypted response packet len=100
 77 5.52563200 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=2866 Ack=2302 Win=35200 Len=0 TSval=5496350 TSecr=9076526
 78 5.56001800 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=2866 Ack=2202 Win=35456 Len=0 TSval=252682387 TSecr=5496344
 79 5.56005300 192.168.0.22   192.168.0.23   TCP    166 ici > 41198 [PSH, ACK] Seq=2202 Ack=2866 Win=38528 Len=100 TSval=5496384 TSecr=252682387
 80 5.56056400 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=2866 Ack=2302 Win=35456 Len=0 TSval=252682387 TSecr=5496384
 81 5.66865200 192.168.0.70   192.168.0.22   SSHv2  134 Encrypted response packet len=68
 82 5.66867800 192.168.0.70   192.168.0.22   SSHv2  118 Encrypted response packet len=52
 83 5.66874400 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=2866 Ack=2422 Win=35200 Len=0 TSval=5496493 TSecr=9076675
 84 5.66875800 192.168.0.22   192.168.0.23   TCP    186 ici > 41198 [PSH, ACK] Seq=2302 Ack=2866 Win=38528 Len=120 TSval=5496493 TSecr=252682387
 85 5.66902800 192.168.0.70   192.168.0.22   SSHv2  134 Encrypted response packet len=68
 86 5.66905200 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=2866 Ack=2422 Win=35456 Len=0 TSval=252682496 TSecr=5496493
 87 5.66910600 192.168.0.22   192.168.0.23   TCP    134 ici > 41198 [PSH, ACK] Seq=2422 Ack=2866 Win=38528 Len=68 TSval=5496493 TSecr=252682496
 88 5.66963900 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=2866 Ack=2490 Win=35456 Len=0 TSval=252682496 TSecr=5496493
 89 5.70828300 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=2866 Ack=2490 Win=35200 Len=0 TSval=5496533 TSecr=9076675
 90 6.15714200 Cisco_a8:2c:85 Spanning-tree-(for-STP 60 Conf. Root = 32768/1/b4:14:89:a8:2c:80  Cost = 0  Port = 0x8005
 91 6.35564800 192.168.0.88   192.168.0.255  NTP     90 NTP Version 4, broadcast
 92 6.38431000 192.168.0.23   192.168.0.22   TCP    102 41198 > ici [PSH, ACK] Seq=2866 Ack=2490 Win=35456 Len=36 TSval=252683211 TSecr=5496493
 93 6.38440100 192.168.0.22   192.168.0.70   SSHv2  102 Encrypted request packet len=36
 94 6.38672300 192.168.0.70   192.168.0.22   SSHv2  102 Encrypted response packet len=36
 95 6.38675200 192.168.0.22   192.168.0.70   TCP     66 58404 > ssh [ACK] Seq=2902 Ack=2526 Win=35200 Len=0 TSval=5497211 TSecr=9077393
 96 6.38681200 192.168.0.22   192.168.0.23   TCP    102 ici > 41198 [PSH, ACK] Seq=2490 Ack=2902 Win=38528 Len=36 TSval=5497211 TSecr=252683211
 97 6.38730600 192.168.0.23   192.168.0.22   TCP     66 41198 > ici [ACK] Seq=2902 Ack=2526 Win=35456 Len=0 TSval=252683214 TSecr=5497211
 98 6.52829100 192.168.0.23   192.168.0.22   TCP    102 41198 > ici [PSH, ACK] Seq=2902 Ack=2526 Win=35456 Len=36 TSval=252683355 TSecr=5497211
 99 6.52837800 192.168.0.22   192.168.0.70   SSHv2  102 Encrypted request packet len=36
100 6.53017500 192.168.0.70   192.168.0.22   SSHv2  102 Encrypted response packet len=36
```



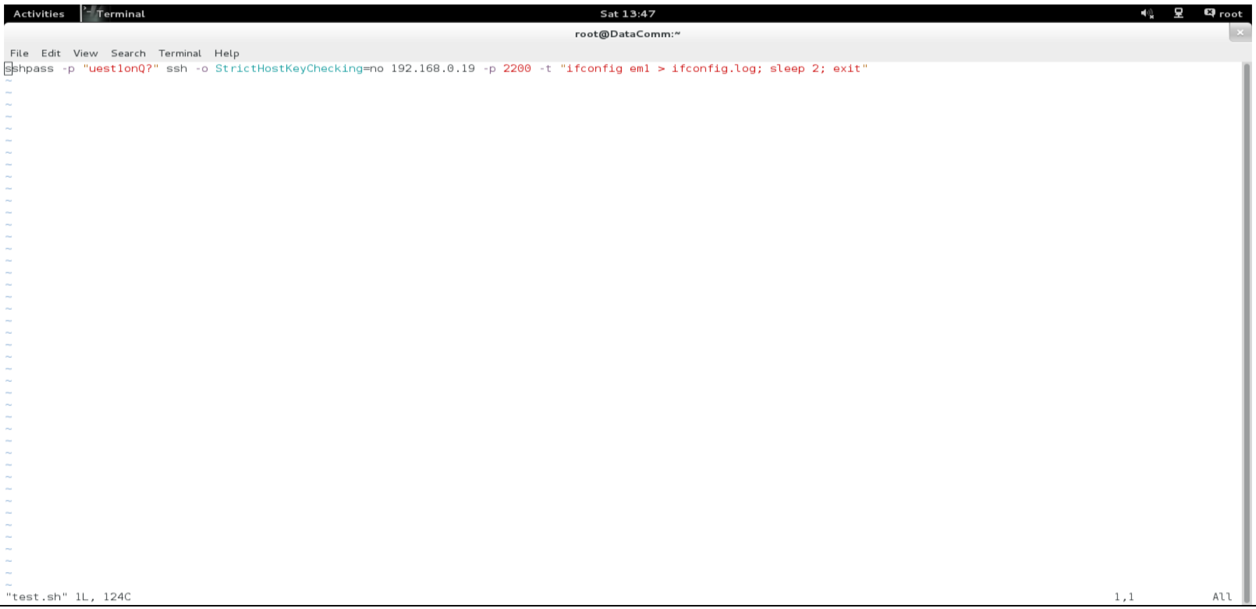
```
101 6.53020300 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=2938 Ack=2562 Win=35200 Len=0 TSval=5497354 TSecr=9077536
102 6.53028800 192.168.0.22     192.168.0.23      TCP     102 ici > 41198 [PSH, ACK] Seq=2526 Ack=2938 Win=38528 Len=36 TSval=5497355 TSecr=252683355
103 6.53079300 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=2938 Ack=2562 Win=35456 Len=0 TSval=252683357 TSecr=5497355
104 6.64835900 192.168.0.23     192.168.0.22      TCP     102 41198 > ici [PSH, ACK] Seq=2938 Ack=2562 Win=35456 Len=36 TSval=252683475 TSecr=5497355
105 6.64844500 192.168.0.22     192.168.0.70      SSHv2   102 Encrypted request packet len=36
106 6.65224900 192.168.0.70     192.168.0.22      SSHv2   102 Encrypted response packet len=36
107 6.65227600 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=2974 Ack=2598 Win=35200 Len=0 TSval=5497476 TSecr=9077658
108 6.65234200 192.168.0.22     192.168.0.23      TCP     102 ici > 41198 [PSH, ACK] Seq=2562 Ack=2974 Win=38528 Len=36 TSval=5497477 TSecr=252683475
109 6.65285100 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=2974 Ack=2598 Win=35456 Len=0 TSval=252683479 TSecr=5497477
110 6.65526700 192.168.0.70     192.168.0.22      SSHv2   262 Encrypted response packet len=196
111 6.65528400 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=2974 Ack=2794 Win=38144 Len=0 TSval=5497479 TSecr=9077661
112 6.65536000 192.168.0.22     192.168.0.23      TCP     262 ici > 41198 [PSH, ACK] Seq=2598 Ack=2974 Win=38528 Len=196 TSval=5497480 TSecr=252683479
113 6.65552500 192.168.0.70     192.168.0.22      SSHv2   230 Encrypted response packet len=164
114 6.65554800 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=2974 Ack=2958 Win=40960 Len=0 TSval=5497480 TSecr=9077662
115 6.65580800 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=2974 Ack=2794 Win=37504 Len=0 TSval=252683482 TSecr=5497480
116 6.65583500 192.168.0.22     192.168.0.23      TCP     230 ici > 41198 [PSH, ACK] Seq=2794 Ack=2974 Win=38528 Len=164 TSval=5497480 TSecr=252683482
117 6.65608700 192.168.0.70     192.168.0.22      SSHv2   134 Encrypted response packet len=68
118 6.65610300 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=2974 Ack=3026 Win=40960 Len=0 TSval=5497480 TSecr=9077662
119 6.65612000 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=2974 Ack=2958 Win=39552 Len=0 TSval=252683483 TSecr=5497480
120 6.65617600 192.168.0.22     192.168.0.23      TCP     134 ici > 41198 [PSH, ACK] Seq=2958 Ack=2974 Win=38528 Len=68 TSval=5497480 TSecr=252683483
121 6.65636900 192.168.0.70     192.168.0.22      SSHv2   134 Encrypted response packet len=68
122 6.65638500 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=2974 Ack=3094 Win=40960 Len=0 TSval=5497481 TSecr=9077662
123 6.65640100 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=2974 Ack=3026 Win=39552 Len=0 TSval=252683483 TSecr=5497480
124 6.65645800 192.168.0.22     192.168.0.23      TCP     134 ici > 41198 [PSH, ACK] Seq=3026 Ack=2974 Win=38528 Len=68 TSval=5497481 TSecr=252683483
125 6.65695400 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=2974 Ack=3094 Win=39552 Len=0 TSval=252683483 TSecr=5497481
126 7.13232700 192.168.0.22     199.85.124.148    NTP      90 NTP Version 3, client
127 7.19275900 199.85.124.148   192.168.0.22      NTP      90 NTP Version 3, server
128 7.52000500 192.168.0.9      239.255.255.250   SSDP    175 M-SEARCH * HTTP/1.1
129 8.10438900 192.168.0.23     192.168.0.22      TCP     102 41198 > ici [PSH, ACK] Seq=2974 Ack=3094 Win=39552 Len=36 TSval=252684931 TSecr=5497481
130 8.10448300 192.168.0.22     192.168.0.70      SSHv2   102 Encrypted request packet len=36
131 8.10651700 192.168.0.70     192.168.0.22      SSHv2   118 Encrypted response packet len=52
132 8.10653700 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=3010 Ack=3146 Win=40960 Len=0 TSval=5498931 TSecr=9079113
133 8.10659200 192.168.0.22     192.168.0.23      TCP     118 ici > 41198 [PSH, ACK] Seq=3094 Ack=3010 Win=38528 Len=52 TSval=5498931 TSecr=252684931
134 8.10708000 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=3010 Ack=3146 Win=39552 Len=0 TSval=252684934 TSecr=5498931
135 8.10793100 192.168.0.70     192.168.0.22      SSHv2   242 Encrypted response packet len=176
136 8.10794800 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=3010 Ack=3322 Win=43904 Len=0 TSval=5498932 TSecr=9079114
137 8.10800300 192.168.0.22     192.168.0.23      TCP     242 ici > 41198 [PSH, ACK] Seq=3146 Ack=3010 Win=38528 Len=176 TSval=5498932 TSecr=252684934
138 8.10847800 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=3010 Ack=3322 Win=41600 Len=0 TSval=252684935 TSecr=5498932
139 8.10849400 192.168.0.23     192.168.0.22      TCP     102 41198 > ici [PSH, ACK] Seq=3010 Ack=3322 Win=41600 Len=36 TSval=252684935 TSecr=5498932
140 8.10851000 192.168.0.23     192.168.0.22      TCP     134 41198 > ici [PSH, ACK] Seq=3046 Ack=3322 Win=41600 Len=68 TSval=252684935 TSecr=5498932
141 8.10851300 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [FIN, ACK] Seq=3114 Ack=3322 Win=41600 Len=0 TSval=252684935 TSecr=5498932
142 8.10854700 192.168.0.22     192.168.0.23      TCP      66 ici > 41198 [ACK] Seq=3322 Ack=3115 Win=38528 Len=0 TSval=5498933 TSecr=252684935
143 8.10856000 192.168.0.22     192.168.0.70      SSHv2   170 Encrypted request packet len=104
144 8.13094700 192.168.0.70     192.168.0.22      TCP      66 ssh > 58404 [FIN, ACK] Seq=3322 Ack=3114 Win=37248 Len=0 TSval=9079135 TSecr=5498933
145 8.16555400 Cisco_a8:2c:85   Spanning-tree-(for-STP     60 Conf. Root = 32768/1/b4:14:89:a8:2c:80  Cost = 0  Port = 0x8005
146 8.17030000 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [ACK] Seq=3114 Ack=3323 Win=43904 Len=0 TSval=5498995 TSecr=9079135
147 9.99738200 fe80::7add:8ff:fee1ff02::2         ICMPv6   62 Router Solicitation
148 10.1667570 Cisco_a8:2c:85   Spanning-tree-(for-STP     60 Conf. Root = 32768/1/b4:14:89:a8:2c:80  Cost = 0  Port = 0x8005
149 10.1673010 192.168.0.22     192.168.0.70      TCP      66 58403 > ssh [FIN, ACK] Seq=1 Ack=1 Win=343 Len=0 TSval=5500992 TSecr=8942021
150 10.1688580 192.168.0.70     192.168.0.22      ICMP     94 Destination unreachable (Host administratively prohibited)
151 10.5265460 Cisco_a8:2c:85   CDP/VTP/DTP/PAgP/UDDTP     60 Dynamic Trunking Protocol
152 10.5265650 Cisco_a8:2c:85   CDP/VTP/DTP/PAgP/UDDTP     90 Dynamic Trunking Protocol
153 10.5308750 192.168.0.9      239.255.255.250   SSDP    175 M-SEARCH * HTTP/1.1
154 11.2008170 192.168.0.22     192.168.0.23      TCP      66 ici > 41198 [FIN, ACK] Seq=3322 Ack=3115 Win=38528 Len=0 TSval=5502025 TSecr=252684935
155 11.2008430 192.168.0.22     192.168.0.70      TCP      66 58404 > ssh [FIN, ACK] Seq=3114 Ack=3323 Win=43904 Len=0 TSval=5502025 TSecr=9079135
156 11.2012340 192.168.0.23     192.168.0.22      TCP      66 41198 > ici [ACK] Seq=3115 Ack=3323 Win=41600 Len=0 TSval=252688028 TSecr=5502025
157 11.2032090 192.168.0.70     192.168.0.22      TCP      66 ssh > 58404 [ACK] Seq=3323 Ack=3115 Win=37248 Len=0 TSval=9082209 TSecr=5502025
158 12.1513150 Dell_a3:42:7e    Cisco_38:15:ff    ARP      42 Who has 192.168.0.100?  Tell 192.168.0.22
159 12.1515390 Cisco_38:15:ff   Dell_a3:42:7e     ARP      60 192.168.0.100 is at 00:1a:6d:38:15:ff
```

The section above shows the SSH activity that took place between the port forwarder server, host and client machines.

Testing SSH port forwarding under a heavy load with multiple connections.

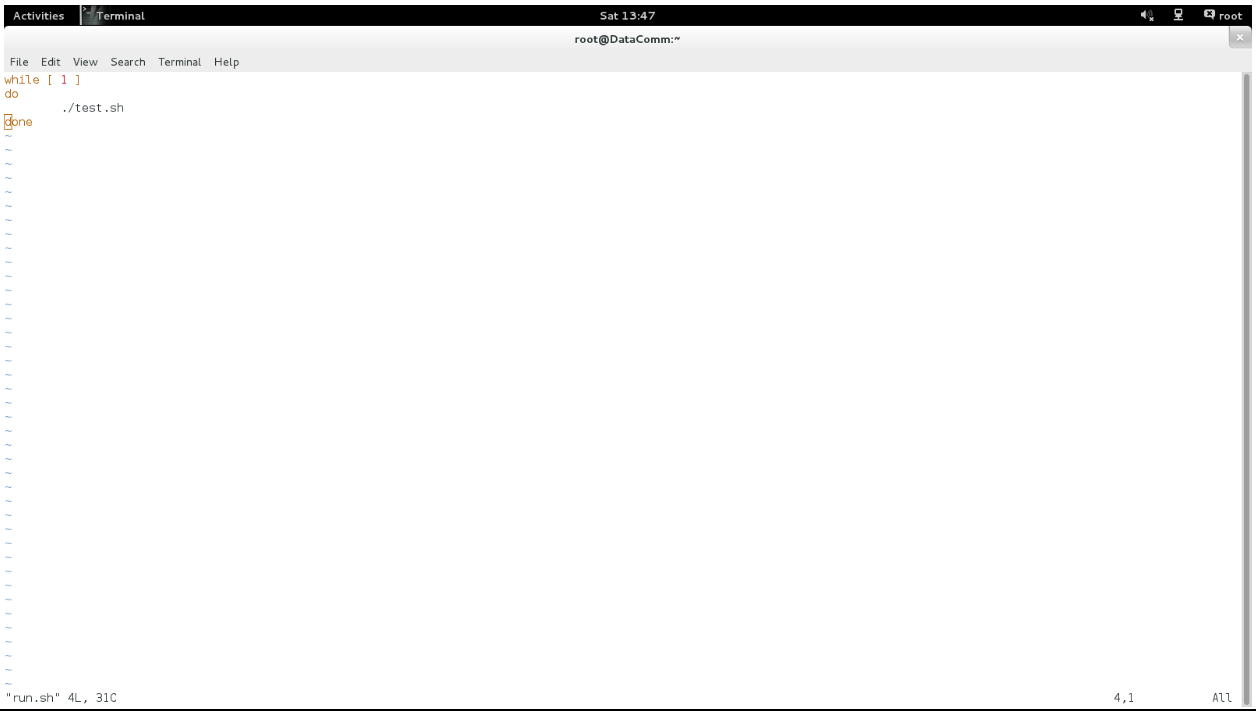
Script used to login/SSH into station 22 multiple times

Test.sh



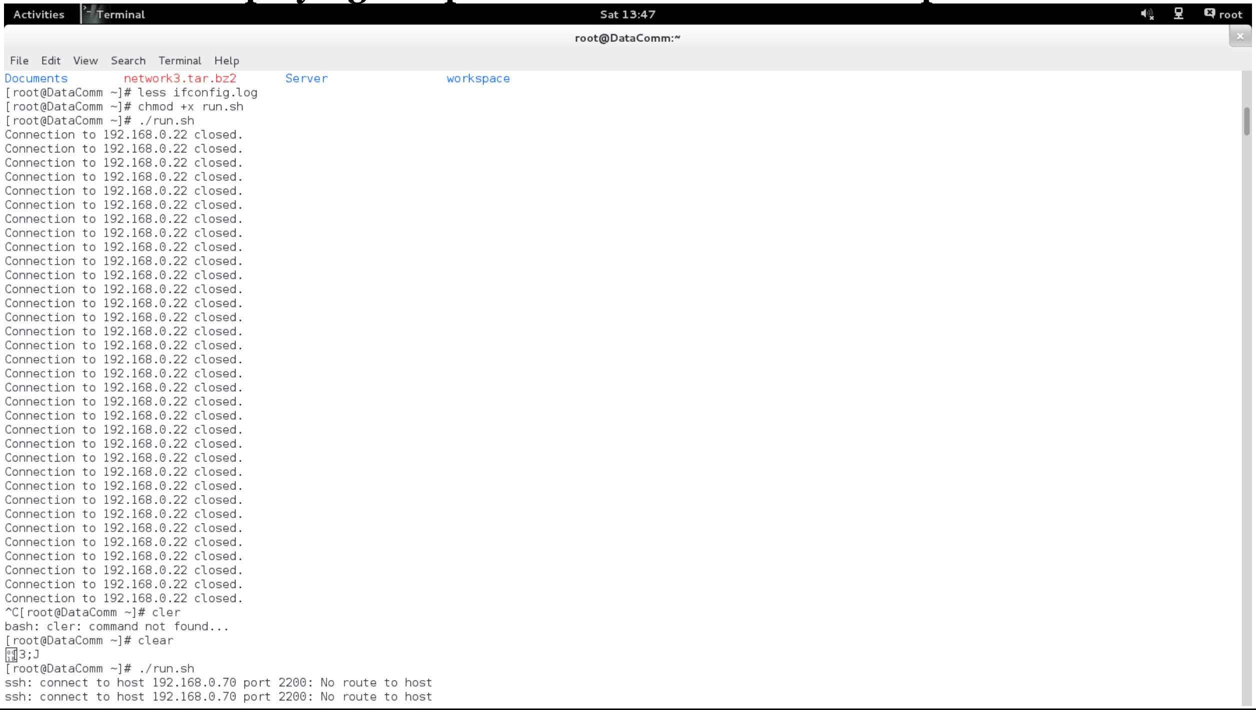
```
sshpass -p "uest1onQ?" ssh -o StrictHostKeyChecking=no 192.168.0.19 -p 2200 -t "ifconfig em1 > ifconfig.log; sleep 2; exit"
~
~
~
"test.sh" 1L, 124C                                                                    1,1           All
```

Bash script to run test.sh in an infinite loop



```
while [ 1 ]
do
        ./test.sh
done
~
"run.sh" 4L, 31C                                                    4,1           All
```

Screenshot displaying completed SSH connection attempts on station 22



```
Documents        network3.tar.bz2      Server                workspace
[root@DataComm ~]# less ifconfig.log
[root@DataComm ~]# chmod +x run.sh
[root@DataComm ~]# ./run.sh
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
Connection to 192.168.0.22 closed.
^C[root@DataComm ~]# cler
bash: cler: command not found...
[root@DataComm ~]# clear
3;J
[root@DataComm ~]# ./run.sh
ssh: connect to host 192.168.0.70 port 2200: No route to host
ssh: connect to host 192.168.0.70 port 2200: No route to host
```