SSH port forwarding is a mechanism in SSH for tunneling application ports from the client machine to the server machine, or vice versa. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines. It can also be abused by hackers and malware to open access from the Internet to the internal network.

The basic syntax for a **local port forward** command is straightforward:

```
ssh -L local_port:destination_server_ip:remote_port ssh_server_hostname
```

The basic syntax for a **remote port forward** command is as follows:

```
ssh -R remote_port:localhost:local_port ssh_server_hostname
```

In this example, we have instructed the remote server **ssh.server.com** to forward any connections directed at port **8080** to the local resource listening on port **5534**.

```
ssh –R 8080:localhost:5534 pnap@ssh.server.com
```

Users with access to the SSH server are now able to access resources on your local machine.