

Internet & Networking

By Devi Sri Charan

[Public and Private Networks 2](#_Toc508659253)

[Private Network Access 3](#_Toc2083009808)

[Local Web Server Connection 4](#_Toc243514990)

[1. Obtain Necessary Information 4](#_Toc2099057370)

[2. Network Access 5](#_Toc1528249195)

[3. Configure Your Device 5](#_Toc976353162)

[4. Accessing the Web Server 5](#_Toc647227501)

[Firewall Configuration 5](#_Toc1308239092)

[1. Basic Firewall Configuration 6](#_Toc1295368504)

[2. Define Firewall Rules 6](#_Toc160321151)

[3. Create Specific Rules 6](#_Toc455941205)

[4. Implement the Rules 7](#_Toc973300103)

[SSH Connection 7](#_Toc1837986529)

[Using Password Authentication 7](#_Toc687739679)

[Using Passwordless Authentication (SSH Keys) 8](#_Toc1696487679)

[NAT and Port Forwarding 8](#_Toc121887253)

[Network Address Translation (NAT) 9](#_Toc512244260)

[Port Forwarding 9](#_Toc1304442631)

[NAT and Port Forwarding in Action 10](#_Toc711027280)

[Port Forwarding Utilization 11](#_Toc732568134)

[Scenario Setup 12](#_Toc499614908)

[Steps to Configure Port Forwarding 12](#_Toc1026370854)

[Accessing the Website from the External Laptop 12](#_Toc1128404876)

# Public and Private Networks

## **Private Network Access**

To gain access to a private network in a legitimate and ethical manner, we need to follow these steps:

**Prerequisites**

1. **Authorization:** Ensure we have permission to access the private network.
2. **Network Details:** Obtain the necessary network details such as SSID (for wireless), IP address, subnet mask, gateway, and any required authentication credentials.

**Steps**

1. **Install Required Tools:**

Ensure we have the necessary networking tools installed on our Linux machine. Common tools include net-tools, iproute2, and wireless-tools.  
  
sudo apt-get update  
sudo apt-get install net-tools iproute2 wireless-tools

1. **Connect to a Wired Network:**

If we are connecting to a wired network, plug in our Ethernet cable and use the following commands:   
  
sudo dhclient eth0

Replace eth0 with your actual Ethernet interface name, which can be found using:  
  
ip link show

1. **Connect to a Wireless Network:**

If you are connecting to a wireless network, use the following steps:

1. **Identify your wireless interface:**  
   iwconfig
2. **Scan for available networks:**  
   sudo iwlist wlan0 scan  
     
   Replace wlan0 with your actual wireless interface name.
3. **Connect to the network using wpa\_supplicant:**  
   Create a configuration file for wpa\_supplicant:  
     
   sudo nano /etc/wpa\_supplicant/wpa\_supplicant.conf  
     
   Add the following content, replacing SSID and PSK with network's SSID and passphrase:

network={  
 ssid="SSID"  
 psk="PSK"  
}

Save and exit the file, then connect to the network:

sudo wpa\_supplicant -B -i wlan0 -c /etc/wpa\_supplicant/wpa\_supplicant.conf  
sudo dhclient wlan0

1. **Manual IP Configuration:**  
   If the network does not use DHCP, we need to configure the IP address manually:  
     
   sudo ifconfig eth0 192.168.1.10 netmask 255.255.255.0  
   sudo route add default gw 192.168.1.1  
     
   Replace eth0, 192.168.1.10, 255.255.255.0, and 192.168.1.1 with network interface and appropriate network details.
2. **Verify the Connection:**  
   Check your IP address and network connection:  
   ifconfig  
   ping 8.8.8.8

## **Local Web Server Connection**

Connecting to a web server hosted within a company environment typically involves the following steps. Ensure we have proper authorization and follow our company's IT policies.

#### 1. Obtain Necessary Information

* **Server IP Address or Hostname**: Obtain the internal IP address or hostname of the web server.
* **Credentials**: Get the necessary credentials if authentication is required (username, password, or other authentication mechanisms).
* **Port Number**: Determine the port number the web server is listening on (commonly port 80 for HTTP or 443 for HTTPS).

#### 2. Network Access

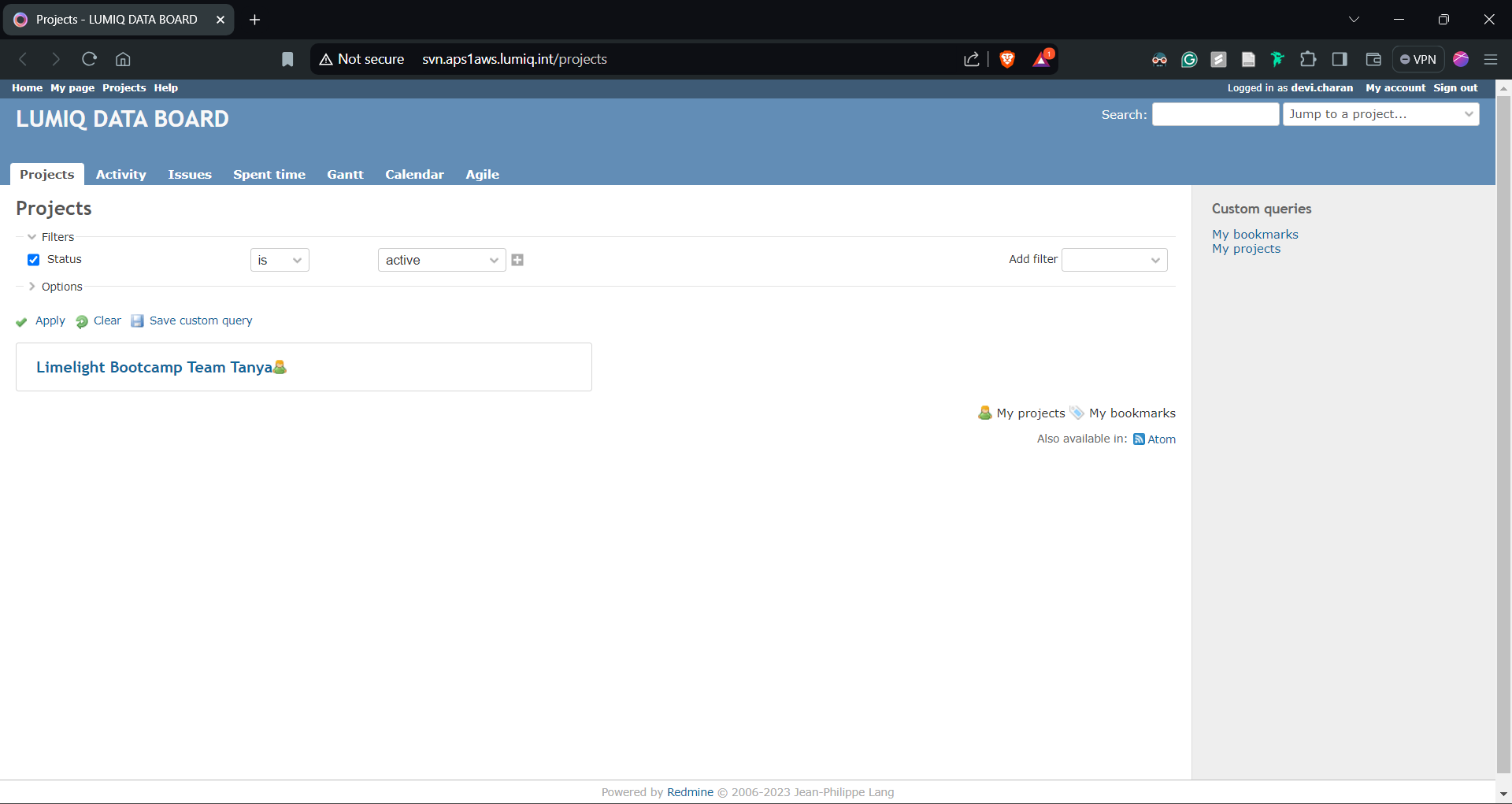
* **Network Connectivity**: Ensure we are connected to the company's network. This can be through:
  + **Wired/Wireless Connection**: Direct connection to the company's internal network.
  + **VPN (Virtual Private Network)**: If we are working remotely, connect to the company's network using a VPN.

#### 3. Configure Your Device

* **Network Configuration**: Set up your device according to the company's network requirements. This might include:
  + Static IP addresses
  + DNS settings
  + Proxy configurations

#### 4. Accessing the Web Server

* **Web Browser**: Open a web browser and enter the server's IP address or hostname in the address bar. For example:
  + <http://svn.aps1aws.lumiq.int>



## **Firewall Configuration**

#### 1. Basic Firewall Configuration

Configure the firewall to define zones or interfaces representing different networks. This could involve:

* **Internal (LAN)**
* **External (WAN/Internet)**
* **DMZ (Demilitarized Zone)**
* **VPN (Virtual Private Network)**

#### 2. Define Firewall Rules

Firewall rules typically include the following components:

* **Source IP/Network**: The origin of the traffic.
* **Destination IP/Network**: The target of the traffic.
* **Source Port**: The port number of the traffic's origin (commonly used for specifying applications).
* **Destination Port**: The port number of the traffic's destination.
* **Protocol**: The protocol used (TCP, UDP, ICMP, etc.).
* **Action**: Permit (allow) or Deny (block) the traffic.

#### 3. Create Specific Rules

Firewall rules:

**Allow Web Traffic (HTTP/HTTPS) from LAN to Internet**

Source IP: Internal Network (e.g., 192.168.1.0/24)  
Destination IP: Any (0.0.0.0/0)  
Source Port: Any  
Destination Port: 80, 443  
Protocol: TCP  
Action: Permit

**Allow SSH Traffic from Specific IP to a Server in DMZ**

Source IP: Specific IP (e.g., 203.0.113.10)  
Destination IP: Server in DMZ (e.g., 192.168.2.10)  
Source Port: Any  
Destination Port: 22  
Protocol: TCP  
Action: Permit

**Deny All Other Traffic**

Source IP: Any  
Destination IP: Any  
Source Port: Any  
Destination Port: Any  
Protocol: Any  
Action: Deny

#### 4. Implement the Rules

# Allow HTTP/HTTPS from LAN to Internet  
iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT  
iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 443 -j ACCEPT  
  
# Allow SSH from specific IP to DMZ server  
iptables -A INPUT -s 203.0.113.10 -d 192.168.2.10 -p tcp --dport 22 -j ACCEPT  
  
# Deny all other traffic  
iptables -P FORWARD DROP

## **SSH Connection**

To establish an SSH connection from our laptop to a peer laptop, you can use either password authentication or a passwordless mechanism using SSH keys. Here's how you can set up both methods:

#### Using Password Authentication

1. **Ensure SSH is installed and running:**
   * On the target (peer) laptop, make sure the SSH server (usually sshd) is installed and running.
   * On the client (our laptop), ensure the SSH client is installed.  
     # On the target laptop (peer):  
     sudo apt-get install openssh-server  
     sudo systemctl start ssh  
     sudo systemctl enable ssh  
       
     # On our laptop (client):  
     sudo apt-get install openssh-client
2. **Find the IP address of the peer laptop:**
   * You can find this using the ifconfig or ip addr command on the peer laptop.  
     # On the peer laptop:  
     ifconfig  
     # or  
     ip addr
3. **Connect using SSH:**
   * From your laptop, use the SSH command followed by the username and IP address of the peer laptop.  
     ssh username@peer\_ip\_address
   * You will be prompted to enter the password of the user on the peer laptop.

#### Using Passwordless Authentication (SSH Keys)

1. **Generate SSH Key Pair on Your Laptop:**
   * If you don’t already have an SSH key pair, generate one using the following command:  
     ssh-keygen -t rsa -b 4096 -C "[your\_email@example.com](mailto:your_email@example.com)"
   * By default, this will generate the keys in ~/.ssh/id\_rsa (private key) and ~/.ssh/id\_rsa.pub (public key). You can press Enter to accept the default file location and optionally set a passphrase for added security.
2. **Copy the Public Key to the Peer Laptop:**
   * Use the ssh-copy-id command to copy your public key to the peer laptop. This command will also handle permissions on the target machine.  
     ssh-copy-id username@peer\_ip\_address
   * You will be prompted to enter the password of the user on the peer laptop.
3. **Connect Using SSH Key:**
   * Once the key is copied, you can connect to the peer laptop without entering a password.  
     ssh username@peer\_ip\_address

## **NAT and Port Forwarding**

#### Network Address Translation (NAT)

NAT is a method used by routers to translate private (local) IP addresses to a single public IP address before packets are sent out to the internet. This is essential because private IP addresses (such as those in the ranges 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) are not routable on the internet.

**Types of NAT**

1. **Static NAT:** Maps a single private IP address to a single public IP address. This is a one-to-one mapping.
2. **Dynamic NAT:** Maps a private IP address to a pool of public IP addresses. This is also one-to-one mapping, but the public IP address is chosen from a pool
3. **PAT (Port Address Translation) / NAT Overload:** Maps multiple private IP addresses to a single public IP address by using different ports. This is a many-to-one mapping.

**Example of NAT**

Consider a private network where devices have the following IP addresses:

* PC1: 192.168.1.2
* PC2: 192.168.1.3

The router has:

* Internal IP: 192.168.1.1
* Public IP: 203.0.113.5

When PC1 wants to communicate with an internet server (e.g., at IP 198.51.100.1), the following steps occur:

1. PC1 sends a packet to 198.51.100.1.
2. The router translates the source IP address from 192.168.1.2 to 203.0.113.5 using NAT.
3. The packet is sent to the internet server with the source IP address of 203.0.113.5.
4. The server responds to 203.0.113.5.
5. The router receives the packet and translates the destination IP address from 203.0.113.5 back to 192.168.1.2.
6. PC1 receives the response.

#### Port Forwarding

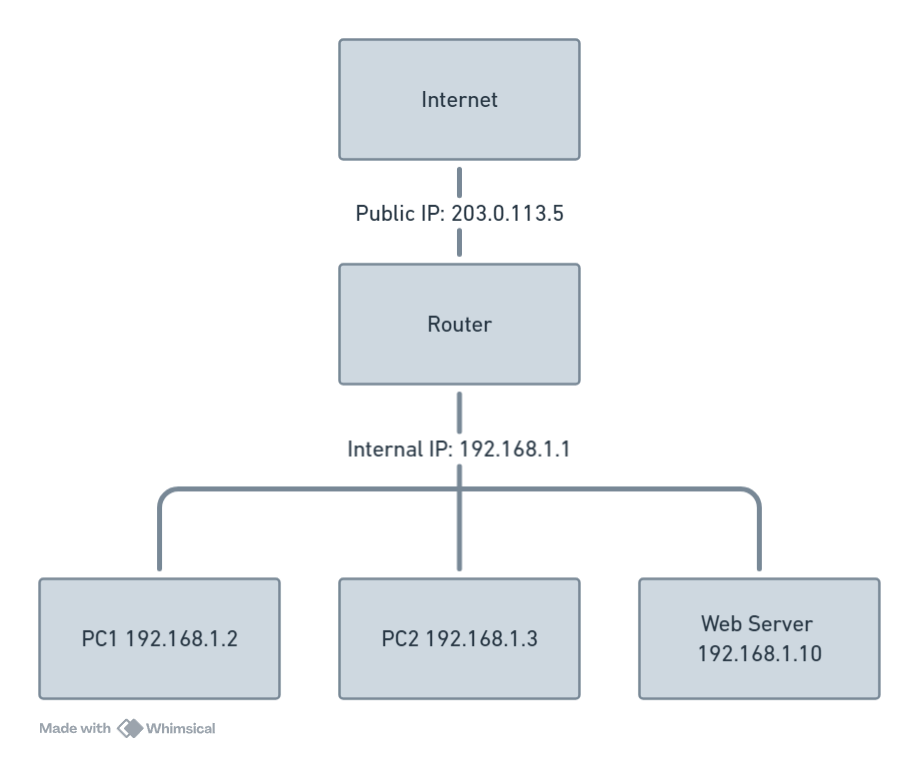
Port forwarding (also known as port mapping) is a technique used to direct external network traffic to a specific device and port on a private network. This is useful for services like web servers, FTP servers, and gaming consoles that need to be accessible from the internet.

**Example of Port Forwarding**

Imagine you have a web server running on a private IP address (192.168.1.10) and you want it to be accessible from the internet on port 80.

1. You configure the router to forward incoming traffic on port 80 of its public IP (203.0.113.5) to port 80 of the private IP (192.168.1.10).
2. An external user accesses the web server by going to http://203.0.113.5.
3. The router receives the request on port 80 and forwards it to 192.168.1.10:80.
4. The web server responds, and the router sends the response back to the external user.

#### NAT and Port Forwarding in Action



1. **NAT Example:**
   * PC1 (192.168.1.2) wants to visit a website at 198.51.100.1.
   * The router translates 192.168.1.2 to 203.0.113.5 and sends the packet to 198.51.100.1.
   * The response comes back to 203.0.113.5, and the router translates it back to 192.168.1.2.
2. **Port Forwarding Example:**
   * An external user accesses http://203.0.113.5:80.
   * The router forwards the request to 192.168.1.10:80.
   * The web server at 192.168.1.10 responds, and the router sends the response back to the external user.

## **Port Forwarding Utilization**

#### Scenario Setup

* **Web Server**: A computer within the private network running a web server (e.g., Apache or Nginx) on IP address 192.168.1.10, port 80.
* **Router**: Connects the private network to the internet with a public IP address (e.g., 203.0.113.5).
* **Laptop**: An external device (outside the private network) that will access the web server.

#### Steps to Configure Port Forwarding

1. **Access the Router’s Admin Interface:**
   * Open a web browser on a computer connected to the private network.
   * Enter the router's internal IP address (commonly 192.168.0.1 or 192.168.1.1) to access the admin interface.
   * Log in using the admin credentials.
2. **Configure Port Forwarding:**
   * Navigate to the port forwarding section, which might be under sections like "Advanced", "NAT", "Virtual Server", or "Applications".
   * Create a new port forwarding rule with the following details:
     + **Service Name**: A descriptive name (e.g., "WebServer").
     + **External Port**: 80 (HTTP) or 443 (HTTPS) depending on your web server configuration.
     + **Internal IP Address**: 192.168.1.10 (IP address of the web server).
     + **Internal Port**: 80 (or 443 if using HTTPS).
     + **Protocol**: TCP.
   * Save the settings.
3. **Ensure Web Server is Running:**
   * Make sure the web server on 192.168.1.10 is running and accessible from within the private network.
4. **Find Your Public IP Address:**
   * From within the private network, open a browser and search for "What is my IP address" to find the router's public IP address (e.g., 203.0.113.5).

#### Accessing the Website from the External Laptop

1. **Open a Web Browser:**
   * On the external laptop, open a web browser.
2. **Enter the Public IP Address:**
   * In the address bar, type the router’s public IP address followed by the port number if necessary (e.g., http://203.0.113.5 for HTTP or https://203.0.113.5 for HTTPS).
   * If you used a non-standard port, you would enter http://203.0.113.5:8080 (if, for example, you forwarded external port 8080 to internal port 80).
3. **Access the Website:**
   * The request should be forwarded by the router to the web server on the private network, and the website should load in the browser.