

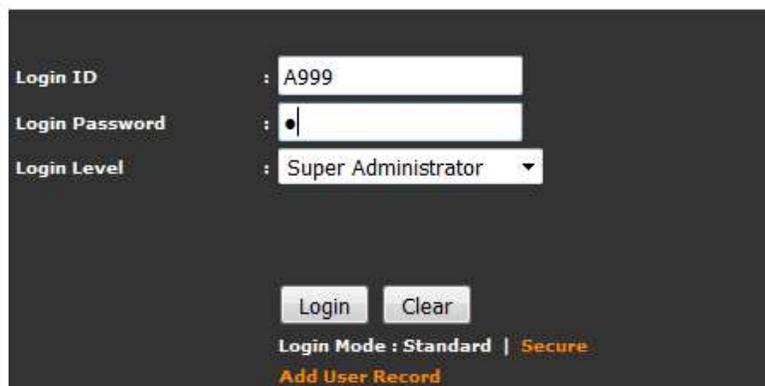
Steps to connect ACTAtek terminal device remotely from public network using web browser or Android phones/Tabs.

- Step 1
 - Assigning Port Address to the terminal i.e. 80, 8080 ,1024 or range (80, 1024 - 65535)
- Step 2
 - Open Port on windows firewall to be accessible from public network
- Step 3
 - Enable port forwarding to allows access Private terminal IP from public network.
- Step 4.
 - Access terminal from public network using browser or Android mobiles.
- Step 5.
 - Troubleshooting

Steps for assigning Port Address to the terminal i.e. 80, 8080 ,1024 or range (80, 1024 - 65535)

Login to the terminal from internet browser using IP address Example 192.168.1.100(Default Login ID : A999; Password : 1)

ACTAtek



Login ID : A999

Login Password :

Login Level : Super Administrator

Login Clear

Login Mode : Standard | Secure

[Add User Record](#)

Go to Terminal Setup under terminal setting as shown below:

Change the Web port as shown below or else use Default :80.

Terminal	MTU(100-1500) <input type="text" value="1500"/>
<ul style="list-style-type: none">• Log Off• Terminal Status• Add Record	Fingerprint Related Setting
User Administration	Security Level (for Automatch) <input type="text" value="Normal"/>
<ul style="list-style-type: none">• Attendance Report• Daily Report• View Event Log• Add Event Log• View User List• Add New User• Departments• User Messages• Admin Setting	Detection Method <input checked="" type="radio"/> Fast <input type="radio"/> Normal <input type="radio"/> Slow
Access Control	Smart Card Related Setting
<ul style="list-style-type: none">• Access Groups• Triggers• Holidays Setting	Parity Error detection <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Terminal Settings	Console Display Timeout Settings
<ul style="list-style-type: none">• Terminal Setup• Authentication/Log Setup• Terminal List• Door Open Schedule• Bell Schedule• Connection Profile• Terminal Clock• External Devices• DDNS	Welcome Message Timeout <input type="text" value="1 sec"/>
Terminal	Console Display Timeout <input type="text" value="30 sec"/>
<ul style="list-style-type: none">• Cloud Storage Service• SMS Service• Alert Log• Syslog• Backup System Data• Restore System Data• Firmware Upgrade• Download Report• Capture Fingerprint• Remote Door Open• Reboot	Console Clock Format <input type="radio"/> 12 hours <input checked="" type="radio"/> 24 hours
Support	Wiegand Configuration
<ul style="list-style-type: none">• Register	Wiegand Type <input type="text" value="Disable"/>
	Access Method <input type="text" value="Finger Print, Password"/>
	Wiegand Output Format <input type="text" value="User ID + Facility Code"/> HIT Terminal Setup
	User Facility Code (FC) <input type="text" value="1"/> (1 - 255)
	Miscellaneous
	Terminal Mode <input checked="" type="radio"/> Stand Alone <input type="radio"/> Access Manager
	Job Code <input checked="" type="radio"/> Disable <input type="radio"/> Enable
	Door SW Mode <input checked="" type="radio"/> Door Switch <input type="radio"/> Door Sense
	Door Strike 1 Option <input type="radio"/> Disable <input checked="" type="radio"/> Access Granted <input type="radio"/> Emergency Mode
	Relay Delay <input type="text" value="8"/> sec (1-90)
	Door Strike 2 Option <input type="radio"/> Disable <input type="radio"/> Door Strike 1 Clone <input type="radio"/> Access Denied <input checked="" type="radio"/> Bell Schedule <input type="radio"/> Active Alarm (Door Strike 2) When Door Opening Time Is Exceeded 30sec
	Relay Delay <input type="text" value="8"/> sec (1-90)
	Note: Setting should not be changed while in operation
	Network Camera IP Address: <input type="text"/> Port: <input type="text" value="80"/>
	Manufacturer: <input type="text" value="Axis"/> Model: <input type="text" value="Axis 2100"/>
	Language <input type="text" value="English"/>
	Webserver Port <input type="text" value="8080"/> (80, 1024 - 65535) change the port : default will be 80
	Allowed IP <input checked="" type="radio"/> Disable <input type="radio"/> Enable * <input type="text"/> (e.g. 192.168.1.*)

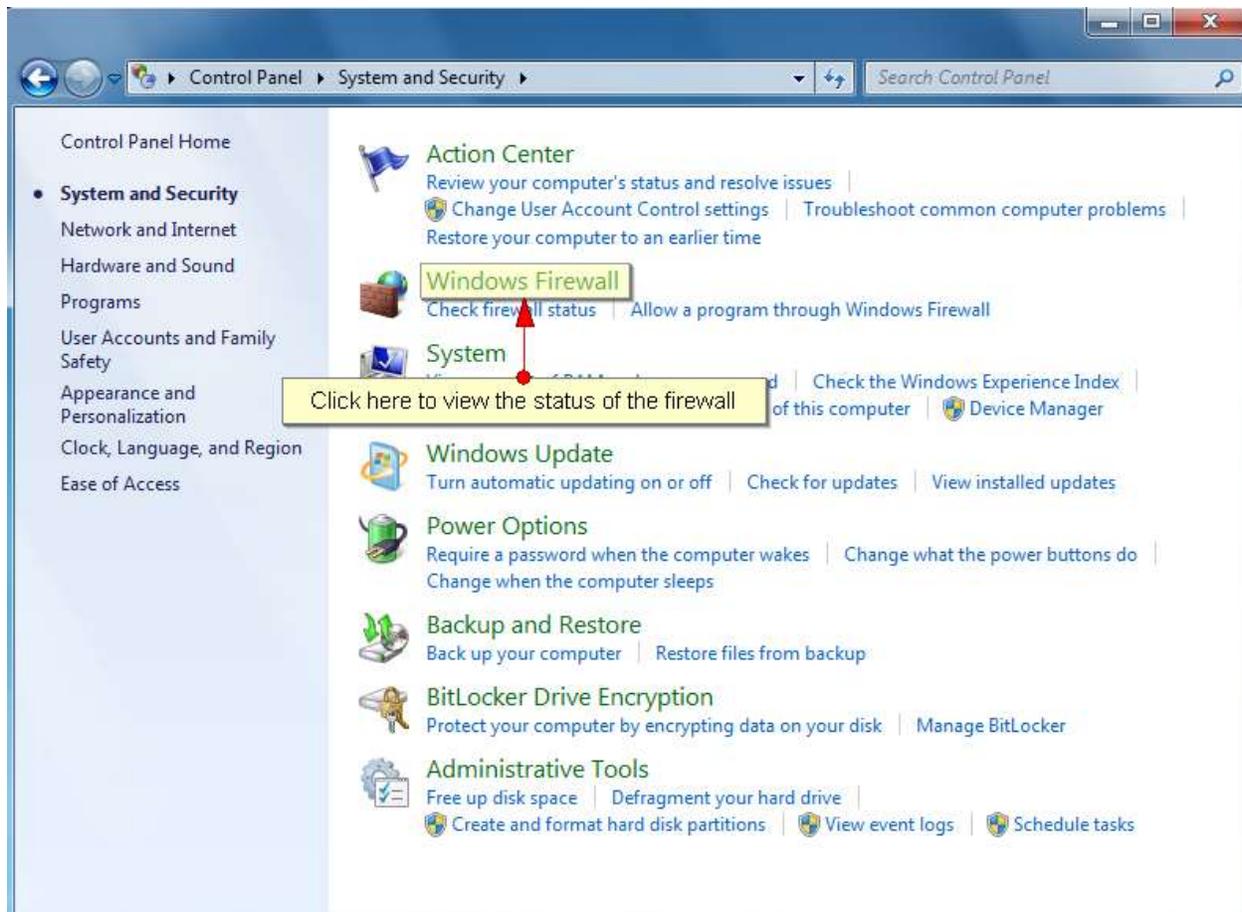
Steps to open Port on firewall to be accessible from public network

1. Open the Control Panel. Windows Firewall is a software firewall that acts in conjunction with your router's hardware firewall. Windows Firewall is especially important if you have multiple devices on the same network, as it helps prevent the spread of viruses between computers on a local network.



- In Windows Vista/7, click the Start menu and select Control Panel.
- In Windows 8, press **Win+X** and select Control Panel.

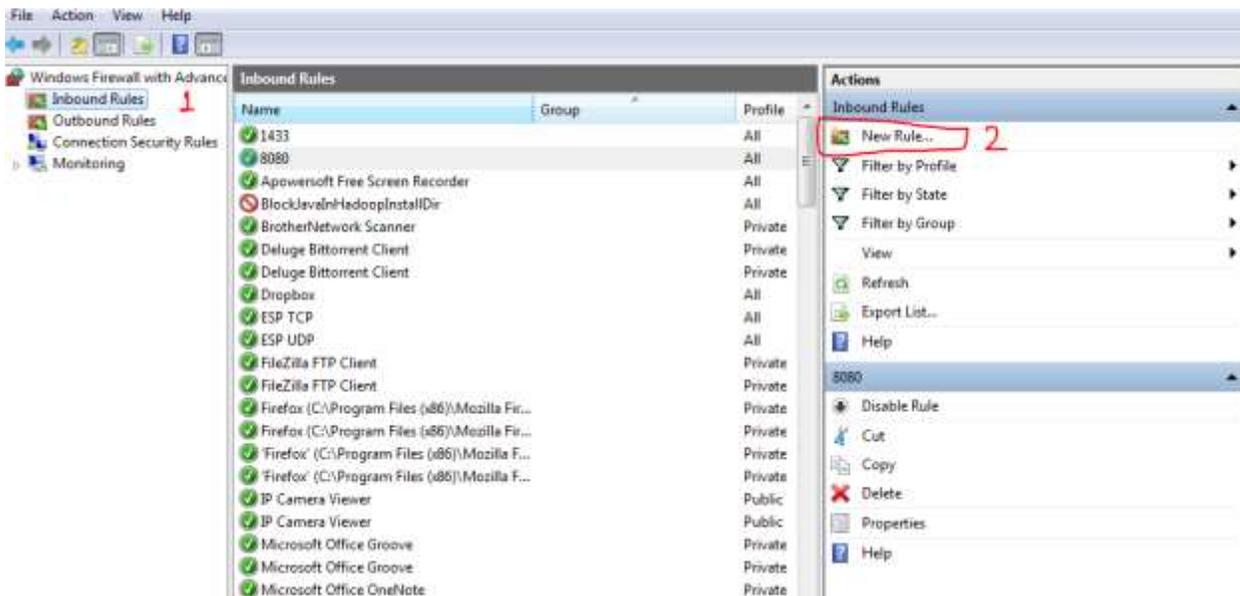
2. **Open Windows Firewall.** This can be found towards the end of the list of Control Panel options. If you are in Category View, select System and Security and then click Windows Firewall.



3. Click on **Advanced settings** from the left menu

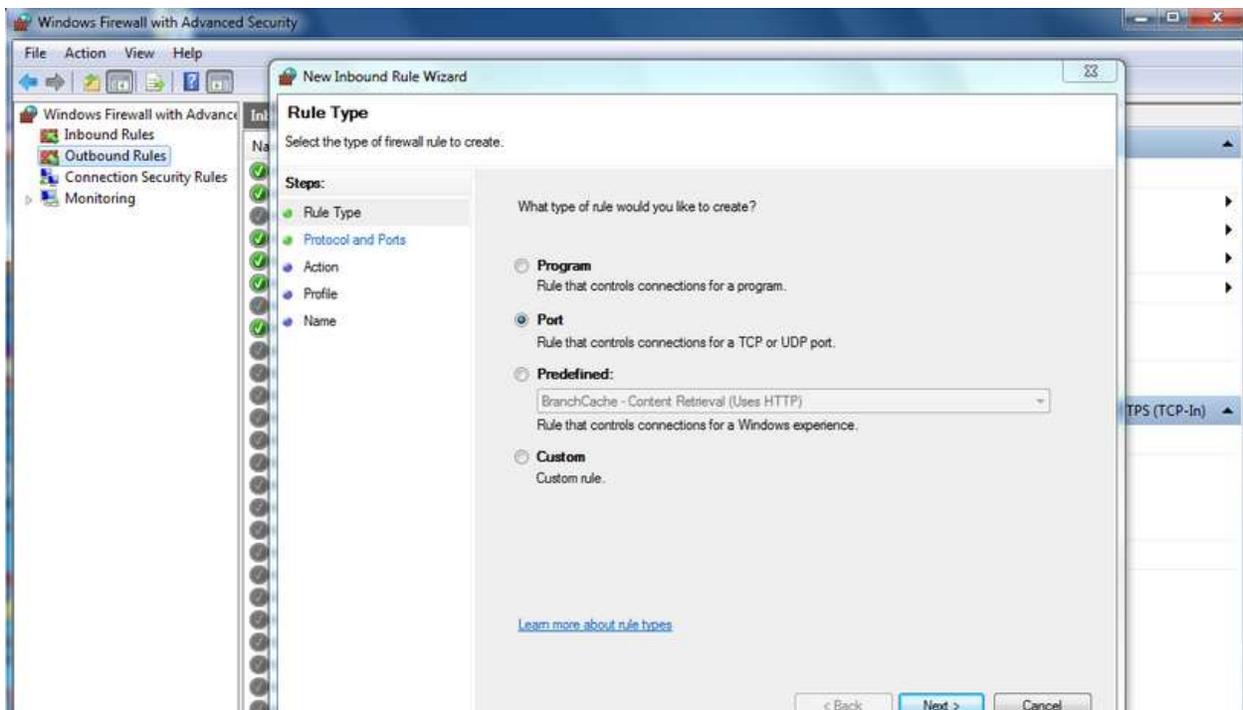


4. On **Advanced settings** window you will need to click on **Inbound Rules** to list the inbound connections. After that click on **New Rule...** in order to add the custom rule:



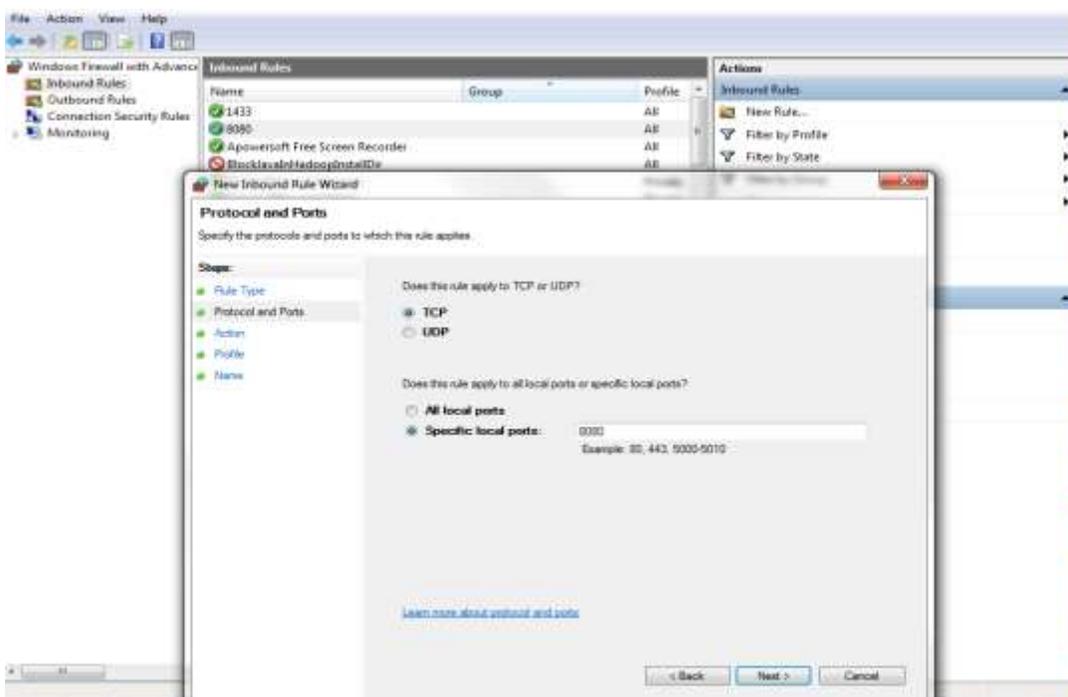
- Click here to open Inbound Rules page
- Click here to add a new rule

5. Check **Port** radio button to add a **TCP** port rule:



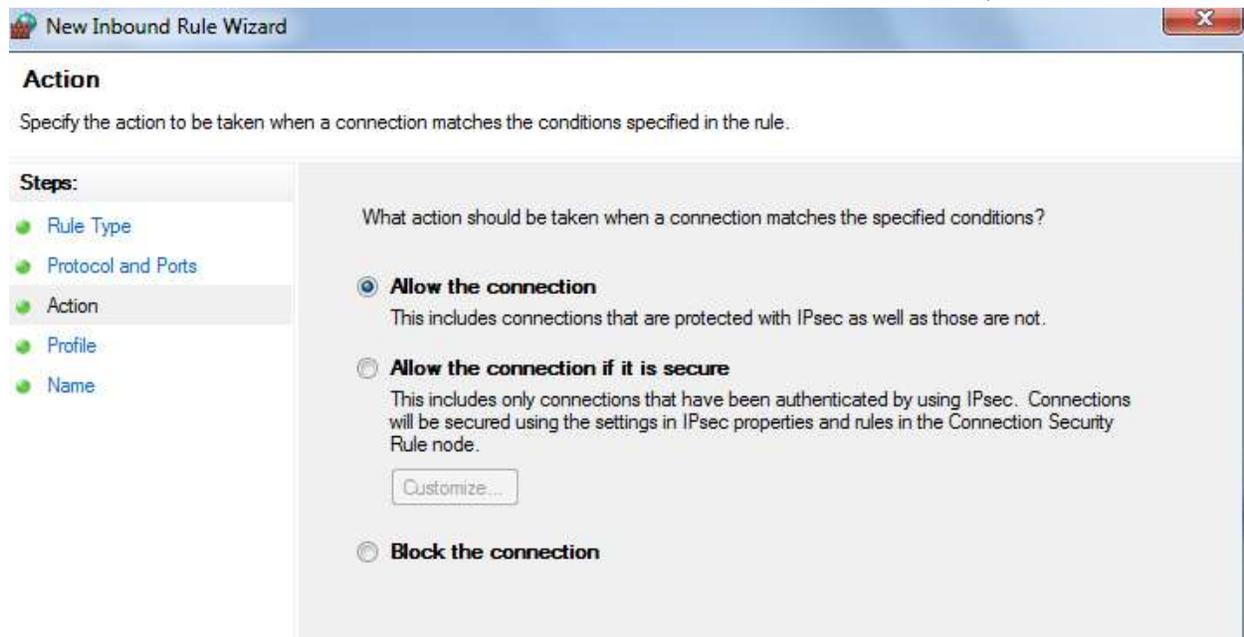
Click on **Next** button to go to the next step

6. Check the **TCP** rule and the **Specific local ports** radio button to add the port: Default is 80 but using 8080 to accessible this device from public network.



Click on **Next** button to go to the next step

7. Check the **Allow the connection** action to allow the broadcaster to use the 8080 port:



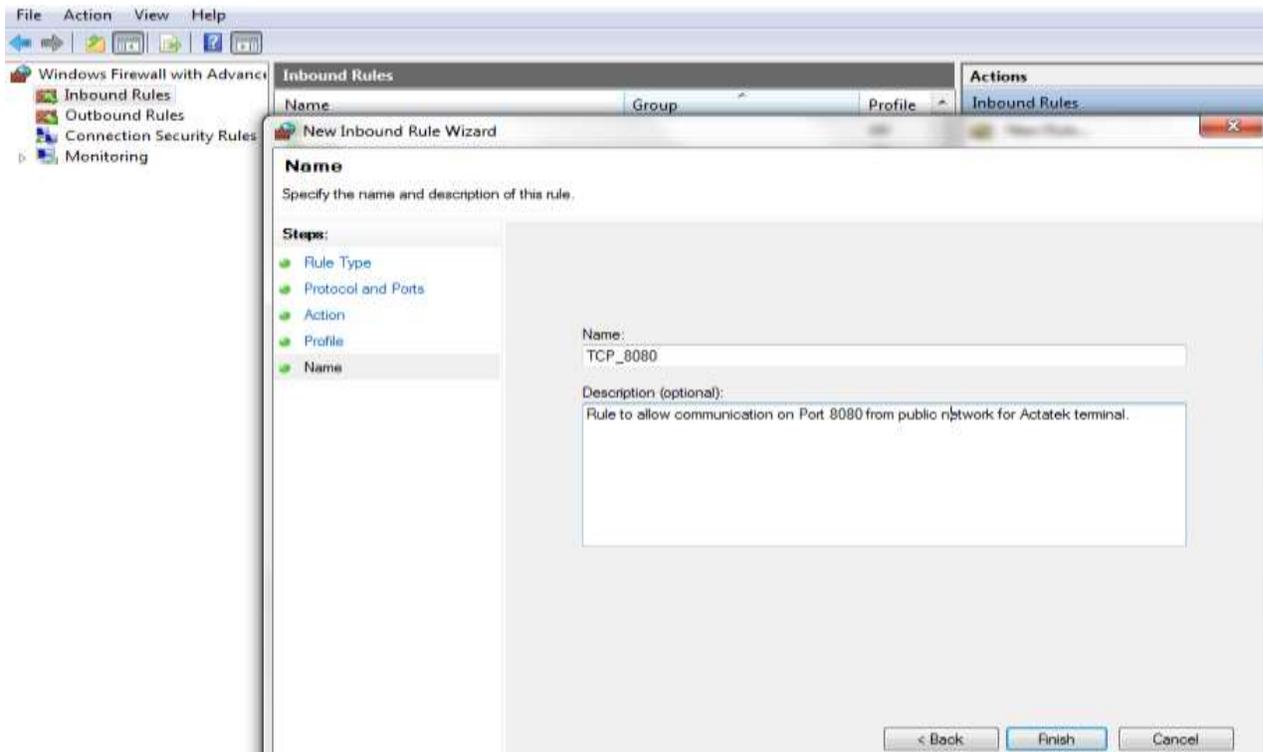
Click on **Next** button to go to the next step

8. Check the profiles to which the rule applies:



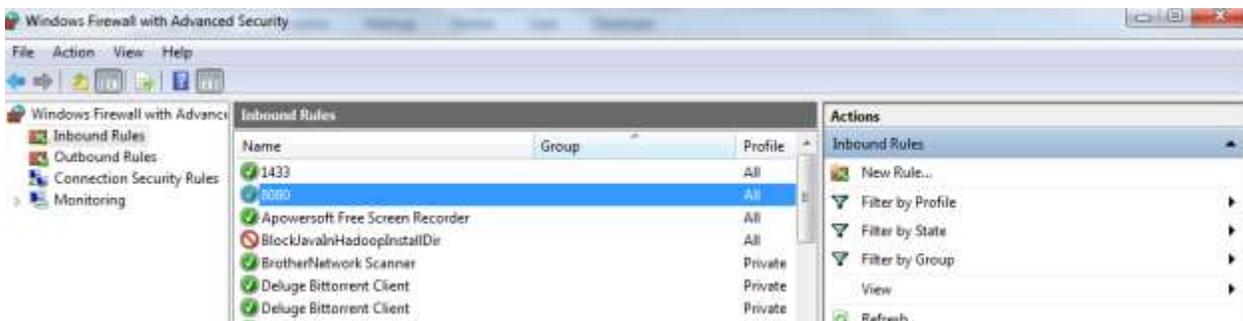
Click on **Next** button to go to the next step

9. Enter a name and a description for this rule:



Click on **Next** button to go to the next step

10. The Port 8080 was successfully added to the firewall exceptions.



*****Note: Repeat steps 4 through 10 for each port that you want to open.**

Steps to enable port forwarding to allows access Private terminal IP from public network.

Login to your router using default user id and Password. Check Router manual how to connect from network using IP address from internet browser.



The screenshot shows the TELUS router's web interface. At the top, there is a navigation bar with icons for Home, Status, Wireless Setup, Firewall, and Advanced Setup. Below this, the 'Summary' section displays: Internet Service Provider: Connected; Wireless: Enabled; 4 Client Connected; System Up Time: 42d, 5h, 15m; DSL Link Up Time: 41d, 22h, 46m; Current Time: May 12 2016 03:52 RM. The 'Product Info' section shows: Model#: T1200H; Serial#: N/A; MAC Address: 4C:8B:30:55:42:A1; Firmware Version: T1200H.31.128L.03; Language: Auto-detect. A login form is present with fields for Username and Password, and a 'Login' button. The 'WAN Connection Status' section lists: WAN Type: DSL; Dynamic/Static: Dynamic; Modem IP Address: 154.5.231.234; Subnet Mask: 255.255.252.0; Default Gateway: 154.5.228.1; Lease Time Remaining: 13H 14M 0S; DNS Address #1: 75.153.176.9; DNS Address #2: 75.153.176.1. The 'Wireless' section shows: SSID: TELUS0215; Security: Enabled; Security Type: WPA2-AES. The 'Home Network' section lists connected devices: Unknown (192.168.1.90), Jakin-ID-Laptop (192.168.1.70), DELL-I52-PC (192.168.1.67), Mays-iPad (192.168.1.65), android-5298884... (192.168.1.66), and android- (Connected). The 'Firewall' section shows: UPnP Setting: Enabled; Firewall: NAT Only; Blocking/Filtering: Disabled. A 'Diagnostics - Login Required' section lists: Ping, Traceroute, Wireless Reset, Device Reboot, Factory Reset, DHCP Release/Renew, HPNA Diagnostic, and User's Manual.

After login go to Firewall main menu and HIT Port forwarding as shown below:

The screenshot shows the 'Firewall' configuration page in the TELUS router's web interface. The navigation bar at the top is the same as in the previous screenshot. The 'Firewall' section is active, showing a sidebar with options: Firewall, IPv6 Firewall, Port Forwarding, Applications, DMZ Hosting, IPv6 DMZ Hosting, and UPnP. The main content area is titled 'Firewall' and contains the following text: 'The default firewall security level is set to NAT Only. Activating the firewall is optional. When the firewall is activated, security is enhanced, but some network functionality will be lost.' Below this, there are four numbered steps: 1. Select the WAN PING block mode. When enabled, the modem will not respond to all pings from WAN side. The 'WAN PING block mode' is set to 'Enable'. 2. Select IP addressing type. The 'Apply rule to' dropdown is set to 'All Dynamic IP Addresses'. 3. Set the Firewall Security Level. The security level is set to 'NAT Only'. 4. Click Apply to save changes. An 'Apply' button is visible at the bottom.

Add port forwarding details like IP address: Terminal IP address assigned to the terminal (Ex: 192.168.1.100) Port 8080 as shown below and Protocol : TCP

Port Forwarding

Enter ports or port ranges required to forward Internet applications to a LAN device below.

1. Set the LAN/WAN port and IP information.

Select LAN Device: Manually enter the IP address

LAN IP Address: 192.168.1.68

External (WAN) Start Port: 8080

External (WAN) End Port: 8080

Internal (LAN) Start Port: 8080

Internal (LAN) End Port: 8080

Protocol: TCP

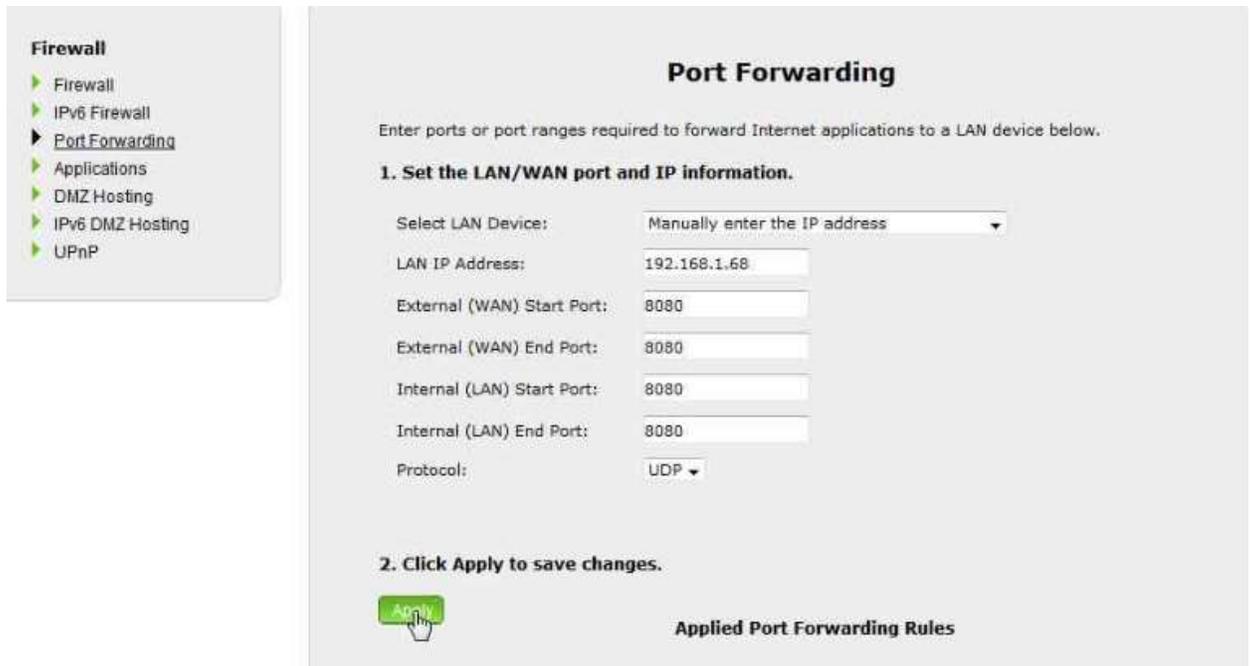
2. Click Apply to save changes.

[Apply](#)

Applied Port Forwarding Rules

Click on **APPLY** button to go to the next step

Add port forwarding details like IP address: Terminal IP address assigned to the terminal (Ex: 192.168.1.100) Port 8080 as shown below and Protocol : UDP



Click on **APPLY** button to go to the next step

Two entries will be there under Applied Port forwarding rules.

LAN START/ END PORT	PROTOCOL	LAN IP ADDRESS	WAN START/END PORT	MODIFY	REMOVE
8080/8080	TCP	192.168.1.68	8080/8080	Modify	Remove
8080/8080	UDP	192.168.1.68	8080/8080	Modify	Remove

Congratulation: you have successfully applied port forwarding rules.

- **Access terminal from public network using browser or Android mobiles.**

It is important to know **public IP address** of the network in which terminal device is connected . Visit :<http://www.whatismypublicip.com/> to know Public IP address.

*****NOTE: Please Must visit this website from the network in which terminal device is connected.**



Once you know the Public IP address: connect the device from any public network by Android phone, tab or computer using below URL:
i.e. [http://public IP address: Port NO](http://154.5.231.234:8080) Example : <http://154.5.231.234:8080> as shown below:



Trouble-shootings:

Question: We have followed all the above steps but still not able to connect from public network.

Answer: Confirm the web port assigned to the terminal device from terminal devices using below steps:

Go to terminal settings>Terminal Setup>webserver port as shown in Pic 3.

Step2: Check Webserver port is open on public network:

Visit " <http://www.canyouseeme.org/> website from the network in terminal device is connected and see whether particular port is opened or not.

If port is closed: **Error:** I could **not** see your service on **154.5.231.234** on port **(80)**:

for solution, Repeat steps STEPS 2 as mentioned above i.e. **Steps to open Port on firewall to be accessible from public network.**

Please NOTE: If port is opened : **Success:** I can see your service on **154.5.231.234** on port **(8080)**.**You are good to connect your device from public Network.**

Question: How do I get my public IP address?

Answer: To know public IP address of the network in which terminal device is connected . Visit :<http://www.whatismypublicip.com/> to know Public IP address or else contact your IT team for more support.

*****NOTE: Please Must visit this website from the network in which terminal device is connected.**