IP Sockets Overview

To connect embedded systems together using the internet requires the use of data sockets to send information from one location to another. This process has been around for a long time and as such there are a number of methods available to communicate with servers and devices using sockets to establish a bi-directional communication link between two endpoints.

In general you usually have a listening device and a dialing device. Servers are generally setup as listening devices and remote modems are generally setup as dialing devices, however, this is not always the case and there are many examples which differ from this generalization.

There are certain requirements with both the listening devices and dialing devices which must be taken into consideration when setting up a communication link between two endpoints. This application note will discuss these points in more detail.

Listening Device Requirements

In general the listening device must be accessible on the network and be able to accept incoming data socket requests from remote devices. This usually means having a firewall with a few specific open ports to allow incoming requests to be accepted through the accessible ports. Devices on the internet which have open ports are immediately susceptible to attack from hackers, spammers, viruses and bots which exploit specific vulnerabilities in the listening device's operating system. As a result many security measures have been developed to prevent unauthorized access but care must be taken to ensure that these measures are effectively managed.

For a device which is listening on the internet it would usually have a fixed IP address which does not change over time. This IP address can then be used by any remote device to communicate with the listening device in a similar way to a phone number is used on a telephone.

This fixed IP address would be publicly available and any device legitimate or otherwise would be able to communicate with it. On a HTTP webserver, the server would have a fixed IP address and would be listening for incoming data traffic on port 80. Mapped to this IP address would be a domain name such as 'www.example.com'. When the user types in 'www.example.com' to their web browser, the web browser looks up the IP address using DNS and it returns the IP address of the server. The web browser then contacts the server's IP address directly on port 80 and the https webserver responds with the web page.

The exact same process can be applied to data socket connections using mobile devices.

- The mobile device uses a fixed IP address SIM card
- The mobile device is setup to listen on a specific port i.e. 1024
- The mobile device opens its firewall to specific devices
- The mobile device waits for an incoming data socket connection
- The dialing device attempts to open a socket on the IP address of the fixed IP address SIM card on the listening port i.e. 1024

Dialing Device Requirements

In general the dialing device can use any standard SIM card and does not require a specific setup or fixed IP address SIM card. As the dialing device is dialing out to the server it is not listening for incoming data connections and therefore does not need to be as concerned about security as the listening device.

GPRS Connection

```
//Set extended error messages
AT+CMEE=2

//Set GPRS APN Name
AT+CGDCONT=1,”IP”,”APN Name”
```

Outgoing Connection

//Set packet size and timeouts on context 1-6
AT#SCFG=1,1,300,90,600,50

//Open GPRS context 1-6 with GPRS Username and GPRS Password. (This will return your ISP assigned IP address)
AT#SGACT=1,1,”username”,”password”

//Open Socket on Port Number at IP Address
AT#SD=1,0,Port Number,”IP Address”,255,0

// Close GPRS context 1-6
AT#SGACT=1,0

Incoming Connection

//Open GPRS context 1-6 with GPRS Username and GPRS Password
AT#SGACT=1,1,”username”,”password”

//Setup Firewall
AT#FRWL=1,”IP Address”,”Subnet Mask”
//Allow all: AT#FRWL=1,”0.0.0.0”,”0.0.0.0”

//Socket listen 1-6
AT#SL=1,1,”Port Number”

Socket Status

//Check status of each socket from 1-6
AT#SS

Application Example

Modem A (Local): IP Address – 80.80.80.80, Port Number – 1024
Modem B (Remote): IP Address – 80.80.80.81, Port Number – 1024

Modem A Config

AT+CMEE=2

AT+CGDCONT=1,”IP”,”APN Name”

AT#SGACT=1,1,”username”,”password”

AT#SD=1,0,1024,”080.080.080.081”,255,0

Modem B Config

AT+CMEE=2

AT+CGDCONT=1,”IP”,”APN Name”

AT#SGACT=1,1,”username”,”password”

AT#FRWL=1,”80.80.80.80”,”255.255.255.255”

AT#SL=1,1,1024,255

Siretta Ltd
Basingstoke Road
Spencers Wood
Reading
Berkshire RG7 1PW
sales
email
web
+44(0)118 976 9000
sales@siretta.com
www.siretta.com

Successful Connection

Upon success modem A (80.80.80.80) will show: CONNECT
Upon success modem B (80.80.80.81) will show: SRING:1 Showing a connection is requested on connection context 1.

Type AT#SA=1 to allow the connection and you will get the response below: CONNECT

Either modem can close the connection using the closure command +++

Up to 6 active socket connections can be stored at any time, however only 1 active connection can be maintained on a single channel (COM Port).