# Chapter 6: Establishing (Secure) Communication using TCP/IP Sockets

## Objective

You need to know:

* What a socket is
* Everything on the internet runs on sockets
* Many are just text based protocols
* How to make, read and write sockets in WICED
* Symmetric and asymmetric keys
* X509 certificate
* TLS

## Remind them that only 2 ¼ Hours

## Sockets – Fundamentals of TCP Communication

Almost everything on the internet runs using TCP sockets

Think of it as a hose where you put stuff in and it comes out on the other side in order

Identified with two pairs of ip/port numbers

IANA – Internet Assigned Name Authority… [www.iana.org](http://www.iana.org) … all the numbers are here

You guys know some standard ports (80,25,53 etc)

Often people just do text based protocols (in fact HTTP is just plain text)

Tell them that they are going to make a TCP client which is going to attach to a TCP server.

They are going to open the socket

Then send text strings through socket

The server is going to respond with text

… explain WWEP

## WICED-SDK TCP Server & Client using Sockets

Go through the setup flow … follow the diagram #s/letters

## Transmitting and Receiving Data using Streams

Explain the stream and the firmware flow

## WICED Socket Documentation

Quick mention of where the documentation is.. .show the TCP Sockets, streams and TLS

### Security: Symmetric and Asymmetric Encryption: A Foundation

Explain Symmetric key

Explain asymmetric key… and the magic of the public/private key pair

Explain the TLS connection setup picture

### X.509 Certificates

Explain a cryptographic hash – like md5 or sha-256 is just a very weird checksum … take something big and make it unique and small

Explain how the CA signs a certificate. You send your public key… the add their public key… then hash it… then encrypt it with their private key. To verify the cert you take create the same hash… then you unencrpyt the signature with their public key… then you compare them.

Show the certificates in the browser

### TCP/IP Sockets with TLS

Explain that it is a simple modification to add TLS to a TCP socket

Explain wiced\_TLS\_init\_Identity is for you to send your certificate (optional)

Explain root\_ca\_certificates (is for you to check the server certificate) If you open a TLS socket and you don’t check then you are subject to MIM… this is very common