1.0 Introduction

What is SSL?

SSL is the security protocol used in almost 100% of secure Internet transactions. Essentially, SSL transforms a typical reliable transport protocol (such as TCP) into a secure communications channel suitable for conducting sensitive transactions' The SSL protocol defines the methods by which a secure communications channel can be established—it does not indicate which cryptographic algorithms need to be used. SSL supports many different algorithms, and serves as a framework whereby cryptography can be

Secure Sockets Layer

SSL (**Secure Sockets Layer**) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

What is SSL in computer network?

The **Secure Sockets Layer** (**SSL**) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal **network**.

used in a convenient and distributed manner.

Uses for SSL

The uses for SSL are endless. Any application that needs to transmit data over an unsecured network such as the Internet or a company intranet is a potential candidate for SSL. SSL provides security, and more importantly, peace of mind. When using SSL, you can be fairly sure that your data are safe from eavesdroppers and tampering.

SSL is relatively new to the embedded world because it has been too complex for traditional embeddedsystems microprocessors to handle. However, starting with Rev. A of the Rabbit 3000 microprocessor, hardware assistance has been added to speed up some of the more complex SSL cryptography operations, making SSL a viable solution in a market where standard (usually complex) security protocols have not traditionally been supported. The applications for embedded applications are as numerous as those for the PC world. The following are just a few potential applications for embedded SSL.

- The Internet-enabled vending machine can now become a reality—SSL makes tampering with communications almost impossible.
- Home automation systems can be Internet-enabled—forgot to turn off the oven? Just log into your house from your computer at work and turn it off. SSL provides a secure means of protecting your home from hackers.
- Readings from medical devices can be sent over a standard network—SSL protects your privacy.
- Make a telephone switch Web-configurable—SSL encrypts all data, so no one monitoring the network can read your information. Since Web-based access means that your data will likely be travelling over a competitor's network, SSL makes a lot of sense.
- Remote-entry configuration—change the passcode on all the doors of a building simultaneously. SSL protects the passcode, allowing the doors to be connected to a standard corporate network, no need for expensive proprietary hardware!

i. At the time of this writing, HTTP file upload over an SSL-secured channel is not supported.

- Television cable box monitoring/billing—connect a cable box to the Internet to monitor use and provide
online billing.
- Utilities monitoring/billing (gas, electric, water)—connect gas and electric meters to the Internet without
the worry of users tampering with the information sent.

SSL is designed to run over TCP/IP. Figure 1 shows how the SSL protocol fits into the overall TCP/IP reference model.

Figure 1. How SSL Fits Into the 5-Layer TCP/IP Reference Model

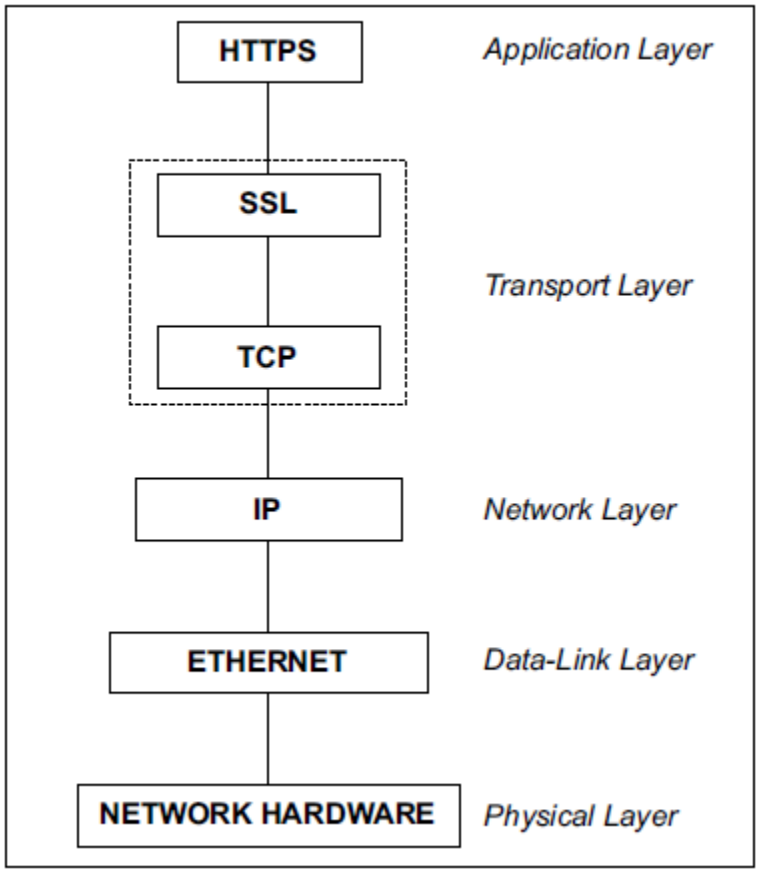


Figure 1. How SSL Fits Into the 5-Layer TCP/IP Reference Model

What can SSL do for my application?

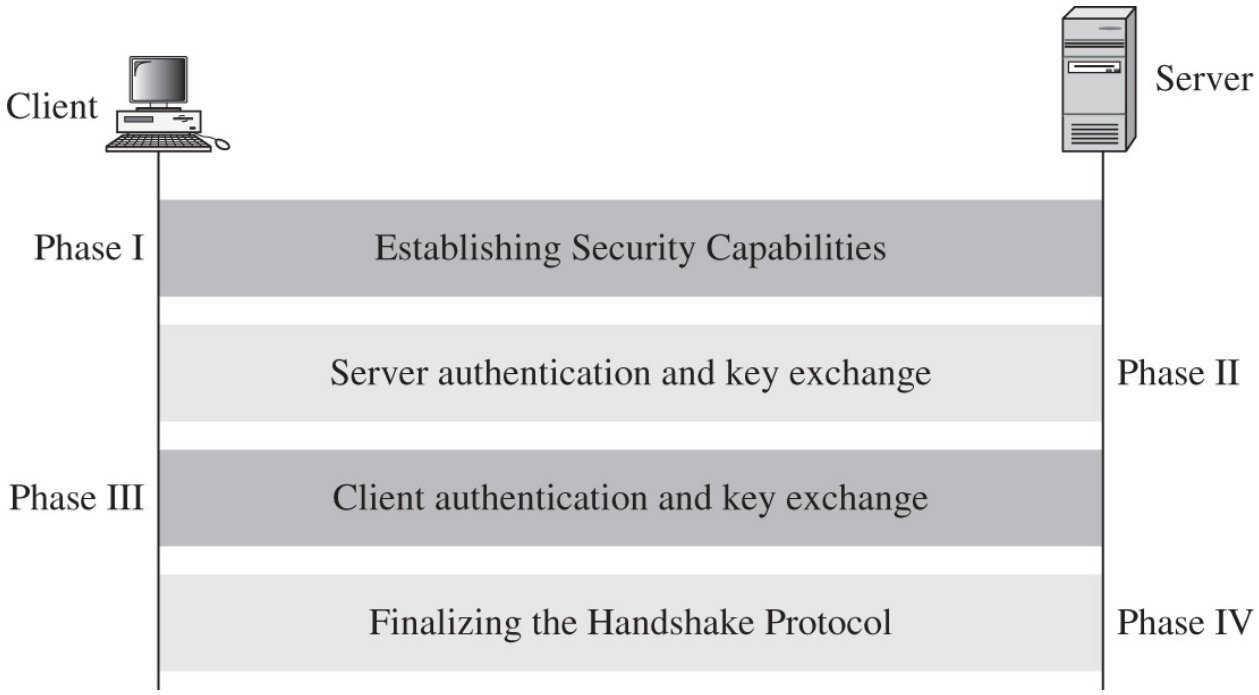
SSL protects the communications channel. It also provides authentication (on the client side, optionally on
the server side) of communicating parties. SSL can secure any connection between two points, and no one monitoring the connection can do anything destructive or gain unauthorized access to any sensitive information.

SSL provides a secure channel without the need for either end to meet to exchange keys. SSL is to secure communications as TCP is to normal communications—it provides a standard communications infrastructure that compliant applications can use easily and nearly invisibly.

SSL provides a vitally important component of any secure system. Basic authentication mechanisms such as the Telnet password and basic HTTP authentication become very powerful security options when executed
using SSL instead of plain TCP—passwords are no longer sent plain-text, making these methods

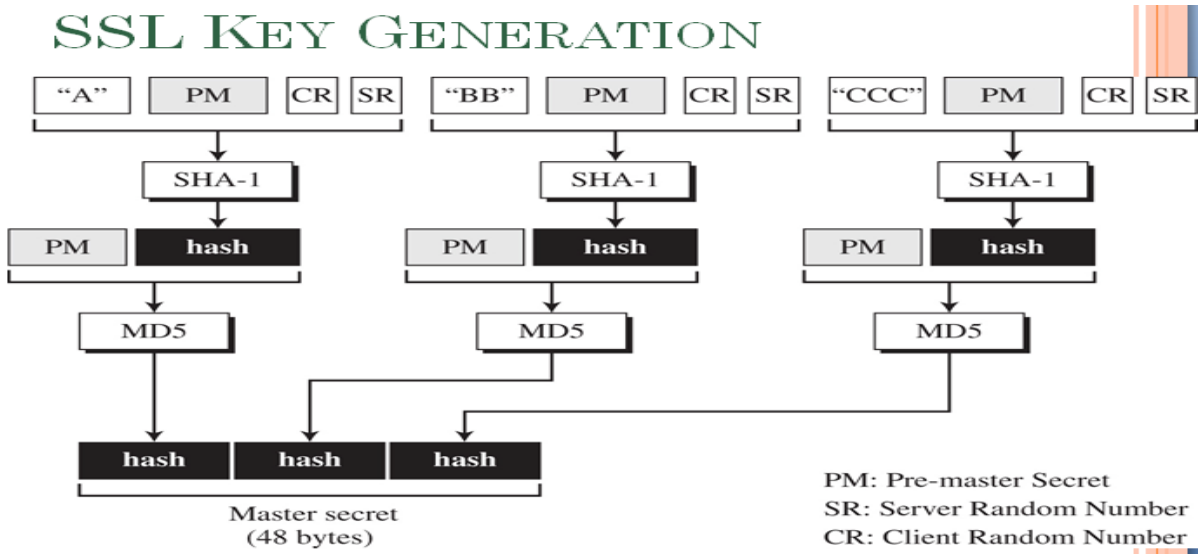
much more useful. SSL encrypts the *connection*, not the data at either end, and does not contain any mechanism
for user authentication or password protection (only the connection is authenticated—the security
fails if the machine at either end is compromised).

Secure Socket Layer Protocol



Finalization handshakes protocol (Sender signs/encrypts "finished" message Receiver decrypts/verifies message to confirm keys)

The SSL handshake is a complicated process that involves significant cryptographic key exchanges. However, the handshake can be completed by calling SSL_accept() on the SSL server and SSL_connect() on the SSL client.



Pre-Master Secret: Key Exchange. The client and server exchange random numbers and a special number called the **Pre-Master Secret**. These numbers are combined with additional data permitting client and server to create their shared **secret**, called the **Master Secret**.

Client and server use to generate master key used to create cipher keys

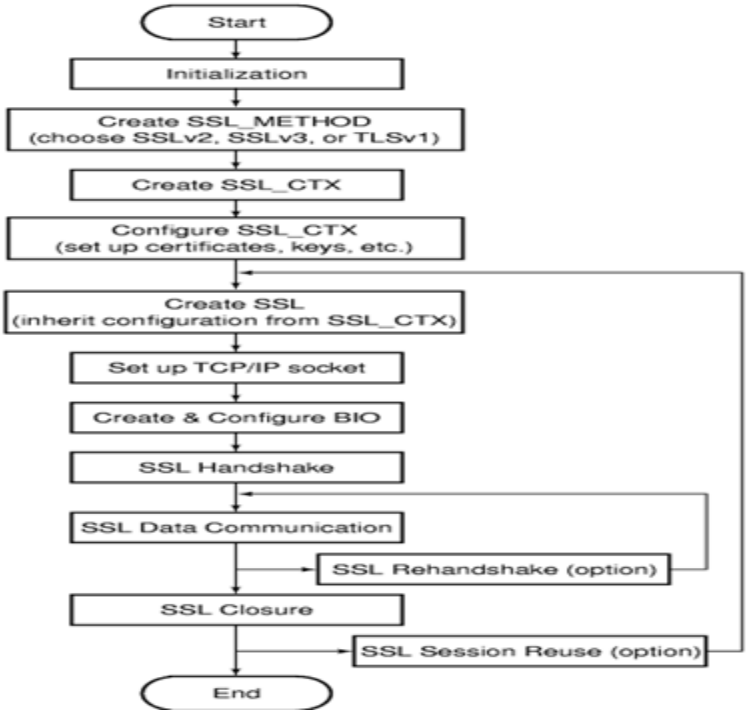
In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest.

ALGORITHM USED:

- **DES.** Data Encryption Standard, an encryption algorithm used by the U.S. Government.
- **DSA.** Digital Signature Algorithm, part of the digital authentication standard used by the U.S. Government.
- **KEA.** Key Exchange Algorithm, an algorithm used for key exchange by the U.S. Government.
- **MD5.** Message Digest algorithm developed by Rivest.
- **RC2 and RC4**. Rivest encryption ciphers developed for RSA Data Security.
- **RSA.** A public-key algorithm for both encryption and authentication. Developed by Rivest, Shamir, and Adleman.
- **RSA key exchange.** A key-exchange algorithm for SSL based on the RSA algorithm.
- **SHA-1.** Secure Hash Algorithm, a hash function used by the U.S. Government.
- **SKIPJACK.** A classified symmetric-key algorithm implemented in FORTEZZA-compliant hardware used by the U.S. Government. (For more information, see FORTEZZA Cipher Suites.)

Triple-DES. DES applied three times

Overview of SSL Application with OpenSSL APIs



Secure Sockets Layer

SSL (**Secure Sockets Layer**) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

What is SSL in computer network?

The **Secure Sockets Layer** (**SSL**) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal **network**.

How do you get an SSL certificate?

- Step 1: Host with a dedicated IP address. In order to provide the best security, SSL certificates require your website to have its own dedicated IP address. ...
- Step 2: Buy a Certificate. ...
- Step 3: Activate the certificate. ...
- Step 4: Install the certificate. ...
- Step 5: Update your site to use HTTPS.

To Install an SSL Certificate in Microsoft IIS 7

1. Click **Start**, mouse-over **Administrative Tools**, and then click **Internet Services Manager**.
2. In the **Internet Information Services (IIS) Manager** window, select your server.
3. Scroll to the bottom, and then double-click **Server Certificates**.
4. From the **Actions** panel on the right, click **Complete Certificate Request...**.
5. To locate your certificate file, click **...**.
6. In the **Open** window, select ***.*** as your file name extension, select your certificate (it might be saved as a .txt, .cer, or .crt), and then click **Open**.
7. In the **Complete Certificate Request** window, enter a **Friendly name** for the certificate file, and then click **OK**.

   For Wildcard SSL certificates make sure your **Friendly Name** to matches your Common Name (i.e. *.coolexample.com).

8. In the **Internet Information Services (IIS) Manager** window, select the name of the server where you installed the certificate.
9. Click + beside **Sites**, select the site to secure with the SSL certificate.
10. In the **Actions** panel on the right, click **Bindings...**.
11. Click **Add...**.
12. In the **Add Site Binding** window:
    - For **Type**, select **https**.
    - For **IP address**, select **All Unassigned**, or the IP address of the site.
    - For **Port**, type **443**.

- For **SSL Certificate**, select the SSL certificate you just installed, and then click **OK**.

13. Close the **Site Bindings** window.
14. Close the **Internet Information Services (IIS) Manager** window. Your SSL certificate installation is complete.

Visit your website at ***https://***www.coolexample.com (replacing *coolexample.com* with your domain name) to verify the installation. If you have problems, see Test your SSL's configuration to help diagnose issues.

As a courtesy, we provide information about how to use certain third-party products, but we do not endorse or directly support third-party products and we are not responsible for the functions or reliability of such products.

What is the IIS?
IIS (**Internet Information Server**) is a group of Internet servers (including a Web or Hypertext Transfer Protocol server and a File Transfer Protocol server) with additional capabilities for Microsoft's Windows NT and Windows 2000 Server operating systems.

What is the IIS Manager?
The **IIS Manager** is the graphical user interface of **IIS**, Microsoft's web server. You can start it from the command prompt or Start menu. On your desktop, click Start > Programs or All Programs > Administrative Tools > Internet Information Services (**IIS**) **Manager**.

How much does it cost to get a SSL certificate?

- Thawte. Thawte offers five SSL certificate options; Thawte SSL (**$149**/yr), Web Server SSL ($249/yr), Web Server EV SSL ($599/yr)and SGC SuperCerts ($699) and Wildcard SSL (**$639**/yr). All the certificates have 128/256 bit encryption and come with warranty ranging from 100,000 US to 500,000 USD.

What is a security certificate on a website?
An organisation that wants to have a **secure** website that uses encryption has to obtain a site, or host, **certificate**. If a site uses encryption you may see a closed padlock in the status bar at the bottom of your browser window. You may also see "https:" rather than "http:" in the URL.

What are the SSL and TLS used for?

The **Transport Layer Security** (**TLS**) and **Secure Sockets Layer** (**SSL**) authentication protocol. This protocol provides authentication over an encrypted channel instead of a less-secure clear channel.

What is meant by SSL connection?

SSL is an acronym for Secure Sockets Layer, an encryption technology that was created by Netscape. **SSL** creates an encrypted **connection** between your web server and your visitors' web browser allowing for private information to be transmitted without the problems of eavesdropping, data tampering, or message forgery.

What is a security certificate?

An organisation that wants to have a **secure** website that uses encryption has to obtain a site, or host, **certificate**. If a site uses encryption you may see a closed padlock in the status bar at the bottom of your browser window. You may also see "https:" rather than "http:" in the URL.

Do you need a SSL certificate?

Not Every E-Commerce Site Needs **SSL**. If you use Paypal or another third party payment gateway and all the sensitive data is being processed at the gateway's website then you likely **do** not **need an SSL Certificate**. For example, a customer clicks to buy items in their shopping cart on your website.

Is https is secure?

Hyper Text Transfer Protocol Secure (**HTTPS**) is the **secure** version of **HTTP**, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of **HTTPS** stands for '**Secure**'. It means all communications between your browser and the website are encrypted.

What is Transport Layer Security?

Transport Layer Security (**TLS**) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, **TLS** ensures that no third party may eavesdrop or tamper with any message. **TLS** is the successor to the **Secure** Sockets **Layer** (SSL).

What browsers support TLS?

Have you heard talk about SSL 3.0, **TLS** 1.0, **TLS 1.1**, and **TLS** 1.2 but never really knew the differences between the different versions? Secure Socket Layer (SSL) and Transport Security Layer (**TLS**) are both cryptographic protocols which provide secure communication over networks.

What is SSLv3?

SSLv3 is an old version of the security system that underlies secure Web transactions and is known as the “Secure Sockets Layer” (SSL) or “Transport Layer Security” (TLS).

What is the certificate?

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

What is a secure socket layer?

SSL (**Secure Sockets Layer**) is the standard security technology for establishing an **encrypted** link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

How do I fix my security certificate?
To do this, follow these steps:

- In Windows Internet Explorer, click Continue to this website (not recommended). ...
- Click the Certificate Error button to open the information window.
- Click View Certificates, and then click Install Certificate.
- On the warning message that appears, click Yes to install the certificate.

How do I remove security certificate errors?

- Open Internet Explorer and click on "Tools," or the gear icon. Click "Internet Options" and click on the "Advanced" tab. Navigate to the "Security" subheading and **remove** the check marks on both the "Check for publisher's **certificate** revocation" and "check for server **certificate** revocation" options.

How do you know if a site is secure?
Before you type your card details into a **website**, ensure that the site is **secure**. Look out for a small padlock symbol in the address bar (or elsewhere in your browser window) and a **web** address beginning with https:// (the s stands for '**secure**'). You also need to check that the **website** is trustworthy.

What is the https port?
When you have another protocol like **HTTPS**, it specifies its own default **port** (443) so that means when you use **HTTPS** to connect to a website your browser is again always going to have to just assume its going to be there on **port** 443. This also explains why you can't run more than one web server on **port** 80 and 443.

What is the Wtls?
Wireless Transport Layer Security (**WTLS**) is a security protocol, part of the Wireless Application Protocol (WAP) stack. It sits between the WTP and WDP layers in the WAP communications stack.

What is the meaning of security protocol?
A **security protocol** (cryptographic **protocol** or encryption **protocol**) is an abstract or concrete **protocol** that performs a **security**-related function and applies cryptographic methods, often as sequences of cryptographic primitives. A **protocol** describes how the algorithms should be used.

What is a DTLS client?
In information technology, the **Datagram Transport Layer Security** (**DTLS**) communications **protocol** provides communications security for datagram **protocols**. **DTLS** allows datagram-

based applications to communicate in a way that is designed [by whom?] to prevent eavesdropping, tampering, or message forgery.

What is SSL encryption and how does it work?
After the secure connection is made, the session key is used to encrypt all transmitted data. Browser connects to a web server (website) secured with SSL (**https**). Browser requests that the server identify itself. Server sends a copy of its **SSL Certificate**, including the server's public key.

What is a digital certificate?
Digital Certificates are a means by which consumers and businesses can utilise the security applications of Public Key Infrastructure (PKI). PKI comprises of the technology to enables secure e-commerce and Internet based communication.

How do I fix an expired certificate?
Just double-click on the time in the lower right corner on the Taskbar, select “Change date and time settings” > “Change date and time…“, then set the time correctly. Be sure to check the time, month, date and the year. As soon as it is corrected, this will usually **fix** this issue.

How do you fix security certificate errors?
If the error continues after trying the above steps:**Launch Internet Explorer on a desktop computer.**Click Tools | Internet Options. ... **Click the Advanced tab.**Under "Security", uncheck the boxes "Check for publisher's revocation" and "Check for server certificate revocation."**Click Apply.**Click Ok.

How do I unblock a site with certificate errors?
Open the desktop, and then tap or click the Internet Explorer icon on the taskbar. Tap or click the Tools button (Image), and then tap or click Compatibility View settings. To remove a website: Click the website(s) where you would like to turn off Compatibility View, clicking Remove after each one.

What is a certificate error for a website?
Occasionally you'll get an **error** message telling you there's a problem with a website's security **certificate**. A site's **certificate** enables Internet Explorer to establish a secure connection with the site. **Certificate errors** occur when there's a problem with a **certificate** or a web server's use of the **certificate**.

What does a green lock on the URL mean?
A **green** padlock plus the name of the company or organization, also in **green**, **means** this website is using an Extended Validation (EV) certificate. An EV certificate is a special type of

site certificate that requires a significantly more rigorous identity verification process than other types of certificates.

An **Extended Validation Certificate** (**EV**) is a **certificate** used for HTTPS websites and software that proves the legal entity controlling the web site or software package. Obtaining an **EV certificate** requires verification of the requesting entity's identity by a **certificate** authority (CA).

How do you buy online?
A faster, safer way to buy online.

- Faster. Enter your details – your credit card, debit card and bank account numbers, your shipping address and contact number – just once. ...
- Safer. We don't share your financial details with sellers. ...
- Flexible. Add all your credit cards, debit cards and bank account details. ...
- Anywhere.

What port is ssh on?

- In this How-To we're going to walk you though changing the default **SSH port** on a Linux system. The Secure Shell (**SSH**) Protocol by default uses **port** 22.

What is wireless datagram protocol?

- **Wireless Datagram Protocol** (WDP)defines the movement of information from receiver to the sender and resembles the User **Datagram Protocol** in the Internet **protocol** suite. The **Wireless Datagram Protocol** (WDP), a **protocol** in WAP architecture, covers the Transport Layer **Protocols** in the Internet model.

What is wireless transaction protocol?
Wireless transaction protocol (WTP) is a standard used in mobile telephony. It is a layer of the **Wireless** Application **Protocol** (WAP) that is intended to bring Internet access to mobile phones.

What is HTTP traffic?
This is determined by the number of visitors and the number of pages they visit. Sites monitor the incoming and outgoing **traffic** to see which parts or pages of their site are popular and if there are any apparent trends, such as one specific page being viewed mostly by people in a particular country.

How do you remove a security certificate?

- Click Start, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
- In IIS Manager, expand the local computer, and then expand Web Sites.
- Right-click Administration, and then click Properties.

- Click the Directory Security tab, and then Server Certificate.

Who owns VeriSign?

- **Symantec** now owns the Secure Sockets Layer (SSL) and code signing certificate services, the managed public key infrastructure (MPKI) services, the VeriSign trust seal, the VeriSign identity protection (VIP) authentication service and the VIP fraud detection service (FDS).

What is the difference between domain name extensions?

- GB.NET **is** an alternate domain for Great Britain. The .net portion of the extension represents the word network and **is** most commonly **used** by businesses that are directly involved in providing Internet services. HU.**COM is** an alternate domain for Hungary.