1. O protocolo HTTP e a Web

O protocolo HTTP e a WWW

O servizo web é o máis utilizado polos usuarios de Internet. Facemos uso do servizo cada vez que abrimos unha páxina web co noso navegador web (Internet Explorer, Mozilla Firefox, Google Chrome, etc.). O navegador web non é máis que un cliente web que realiza a petición dunha páxina web a un servidor web especificando na petición o nome DNS do equipo que ten instalado o servidor web e a ruta e nome da páxina web solicitada. O servidor le no sitio web o arquivo correspondente á páxina web solicitada e envíallo ao cliente.

Temos que distinguir dous conceptos básicos:

- Páxina web: Arquivo escrito nunha linguaxe de marcas que, ademais de texto, contén como elementos principais hipervínculos ou hiperenlaces que enlaza a páxina con outras partes desta ou con outras páxinas que estean no mesmo equipo ou noutros equipos da rede.
- Sitio web: Conxunto de páxinas web e arquivos complementarios que se distribúen en Internet e/ou nun Intranet baixo un mesmo nome DNS. Por exemplo, o sitio www.mec.es está formado polo conxunto de páxinas web e arquivos complementarios dos que se accede a través do nome www.mec.es.

Un equipo *servidor web* ten que ter unhas características apropiadas para dar servizo aos clientes. En función do tipo de contidos que ofreza, do número de clientes que poidan acceder simultáneamente ao servizo, do número de sitios web que sirva, etc., deberase facer unha estimación da memoria que deberá ter o equipo, as unidades de disco, o procesador ou os procesadores, o ancho de banda da conexión a rede e outras características hardware e software.

Hai unha gran variedade de software *servidor web* tanto libre coma propietario (Microsoft IIS, Apache Web Server, Nginx, etc.). As características que se deben valorar deste software son, entre outras:

- Se é software libre ou propietario.
- Recursos que consume.
- Posibilidade de administrar varios sitios.
- Control de acceso a usuarios.
- Seguridade nas transmisións.
- Integración de módulos de servidor (PHP, ASP, Perl, etc.).

Sumario

1. Estrutura da World Wide Web

Habitualmente, os usuarios utilizamos expresións como "*buscar na web*" ou "*navegar na web*". Pero, A que nos referimos con "a web"?.

Web é o termo que usamos frecuentemente para referirnos a "World Wide Web" ou WWW. "World Wide Web" significa Rede Global Mundial.

En 1989, Tim Berners Lee e Robert Caillou, investigadores do CERN propuxeron a creación da World Wide Wide. Despois colaboraron no seu desenvolvemento mediante a súa participación na elaboración de diversos estándares ou especificacións.

A World Wide Web é un sistema global de documentos ou páxinas web enlazados entre si mediante hipervínculos ou hiperenlaces. Ilustración que mostra unha bóla do mundo cunha fita que a rodea co texto "World Wide Web". Hai unha conexión de cable coa bóla do mundo. Arredor da bóla hai varios textos relativos a www como "hipertext", "design", "universality", "oportunity" e "social networks".

O funcionamento da WWW baséase en:

- Unha rede de documentos enlazados a través de hipervínculos, hiperenlaces ou hiperligazóns. Cada documento é un nodo da rede.
- Unha rede de servidores encargados de aloxar e distribuír os documentos.
- Programas clientes chamados navegadores que mostran os documentos cos hiperenlaces de forma que se se pulsa co rato sobre eles se abren as páxinas web coas que están enlazados.

Os documentos web deben estar escritos nunha linguaxe de marcas que os describe. A linguaxe de marcas máis utilizada é HTML. Nos inicios, os hiperenlaces enlazaban con outros documentos web polo que a estes documentos se lles chamou hipertextos. Aos documentos web fóronselles engadindo novos elementos como imaxes, sons, animacións e outros. A estes documentos web que integran outros elementos chámaselles hipermedios.

Actualmente os hiperenlaces non só enlazan con outros documentos web senón que poden enlazar con calquera outro tipo de arquivo ou con recursos doutros servizos como direccións|enderezos de correo electrónico.

2. URL

Supoñemos que xa sabes o que é unha URL. Polo menos, é seguro que utilizas URLs habitualmente cando estás a usar Internet. Neste apartado vas coñecer o contido completo dunha URL e para que serve cada unha das súas partes ou dos seus elementos.

No RFC 1738 defínese a URL (Uniform Resources Locator, Localizador Uniforme de Recursos).

Unha URL é unha secuencia de caracteres cun formato determinado que permite localizar un recurso en Internet ou noutra rede calquera. Fotografía dun teléfono movil que mostra na súa pantalla o texto "Go to URL: http://semapedia.org? ".

Por exemplo, a URL correspondente á páxina web principal do Ministerio de Educación e Ciencia é:

```
http://www.mec.es/index.html
```

Unha URL ten o seguinte formato:

```
Protocolo://usuario:contrasinal@máquina:puerto/ruta_recurso
```

Na seguinte táboa describe cada elemento dunha URL cando o protocolo é http: Elementos dunha URL.

Elementos dunha URL

Elemento URL	Descrición
Protocolo	Especifica o protocolo mediante o que se accede ao recurso. Para páxinas web o protocolo é http. Poden especificarse outros protocolos como ftp.
usuario:contrasinal	É un elemento que se pode excluír nunha URL. Deberíase usar cando no servidor se controla o acceso ao recurso mediante un nome de usuario e un contrasinal indicados na URL. Case nunca se utilizan e desaconséllase a súa utilización por seguridade. Hai outras formas de controlar o acceso e máis seguras.
máquina	É o nome DNS ou o enderezo IP da máquina onde se atopa o servizo que proporciona o recurso que se trata de localizar. Unha URL para unha páxina web consta como mínimo do protocolo e da máquina, como por exemplo http://www.mec.es.
porto	Especifica o porto do servidor co que hai que conectar. Non é obrigatorio, se non se especifica asúmese un por defecto para o protocolo usado. Por exemplo, para http asúmese por defecto o porto 80. Se houbese que usar outro, habería que especificalo.

ruta	Especifica a ruta onde ten que localizar o recurso o servidor e o nome do recurso. Se non se especifica, o servidor asume un nome de recurso por defecto (é habitual que sexa index.html).
outros	Especifícanse despois da ruta e serven para enviar datos ao servidor para que os procese. Por exemplo, úsanse cando solicitamos unha busca en Google.

Non confundir URL con URI. Este último é o acrónimo de Universal Resource Identifier (Identificador Universal de Recurso), que é un concepto máis xeral. Unha URL é un caso particular de URI para referirse a un recurso localizado nun servidor web.

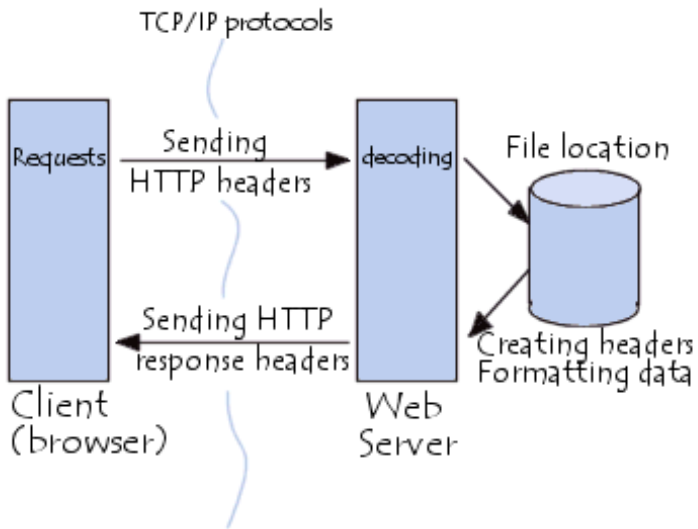
3. O protocolo HTTP

O protocolo HTTP (HyperText Transfer Protocol) é un protocolo de transferencia de hipertexto que segue o modelo cliente/servidor e establece as normas para o intercambio da información contida nas páxinas web.

O protocolo HTTP foi desenvolvido dende 1990 por W3C e IETF. Desenvolvéronse as versións 0.9, 1.0 e 1.1. A versión 1.1 é a que se emprega a día de hoxe e foi publicada no RFC 2616.

As características máis relevantes do funcionamento de HTTP son as seguintes:

- Un servidor HTTP utiliza por defecto o porto 80, aínda que pode usar outros portos.
- Para establecer unha comunicación HTTP entre cliente e servidor necesítase crear previamente unha conexión TCP.
- A comunicación entre clientes e servidores realízase mediante mensaxes de petición e de resposta codificadas en ASCII.
- Cada elemento dunha páxina web (documento, imaxes, vídeos, etc.), transfírese independentemente coa súa mensaxe de petición e a súa mensaxe de resposta.



O contido dunha páxina web que se transfire entre un servidor e un cliente está codificado nunha linguaxe de marcas que describe como se ha de visualizar a páxina web. Das linguaxes de marcas para descrición de páxinas web, sen dúbida é HTML o máis utilizado. Os navegadores web son clientes HTTP que interpretan o contido dunha páxina web escrita en HTML ou noutra linguaxe para crear unha representación da páxina para ser visualizada polo usuario.

Cando nun navegador web escribimos a URL dunha páxina web:

- Solicítase ao servidor DNS que resolva o nome de equipo servidor web ou HTTP usado na URL.
- Obtida a IP do servidor HTTP, establécese unha conexión TCP entre cliente e servidor HTTP.
- Establecida a conexión TCP, faise a petición do documento web ao servidor e este devolve o seu contido nunha mensaxe de resposta.
- Se o documento web inclúe elementos adicionais como imaxes, hai un proceso de envío petición/resposta por cada imaxe.

Un navegador web é un exemplo de axente de usuario (AU). Outros tipos de axentes de usuario inclúen o software de indexación usado por provedores de consulta (web crawler), navegadores vocais, aplicacións móbiles e outros software que acceden, consumen ou exhiben contido web.

Mensaxes HTTP.

Dende que un cliente HTTP (navegador web) establece unha conexión cun servidor HTTP, para descargar unha páxina web ata que a descarga de forma completa, desenvólvese unha sesión HTTP. Normalmente, nunha sesión HTTP prodúcense varias transaccións de mensaxes de petición e resposta entre cliente e servidor.

Por cada recurso adicional (imaxe, audio, vídeo, etc.) que contén unha páxina web envíase unha mensaxe de petición do recurso dende o cliente cara ao servidor e unha mensaxe de resposta dende o servidor ao cliente co recurso solicitado ou cunha indicación de que o recurso non se puido obter.

A seguinte imaxe mostra unha captura de pantalla da páxina web do Ministerio de Educación http://www.educacion.gob.es/portada.html. Sobre a captura destácanse os recursos adicionais e represéntanse as mensaxes de petición e resposta que enviaría e recibiría un cliente HTTP que consultase esa páxina web.

As mensaxes son textos codificados en ASCII e constan de catro campos:

- Liña de petición ou de resposta (segundo sexa o caso): contén a información principal sobre a petición ou a resposta.
- Encabezados: conteñen información adicional sobre opcións relativas á mensaxe, (unha liña de encabezado por cada opción que se especifique).
- Unha liña baleira: xerouse cun ENTER. Considerámola como un campo aínda que non é máis que un separador entre as liñas de encabezados e o corpo da mensaxe.
- Un corpo de mensaxe: este campo é opcional. Nas mensaxes de resposta úsase para enviar o contido do recurso solicitado.

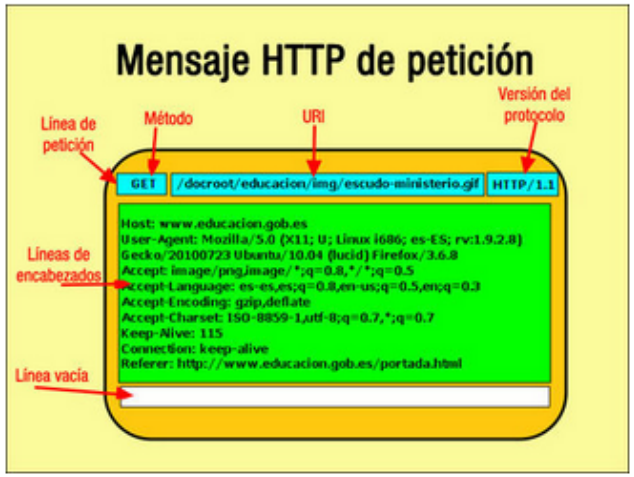
Mensaxes de petición.

Acabamos de ver o formato das mensaxes HTTP. Agora imos afondar un pouco máis no estudo das mensaxes de petición. Como xa sabes unha mensaxe de petición é enviada ao servidor HTTP dende o cliente.

Nunha mensaxe de petición, a liña de petición contén tres datos separados por un espazo:

- Método da petición.
- Enderezo URI do recurso.
- Versión de HTTP.

A seguinte imaxe mostra un exemplo dunha mensaxe de petición para solicitar mediante o método GET o recurso escudo-ministerio.gif.



- O método da petición indica a acción que se pretende realizar sobre o recurso indicado na petición. Os métodos máis utilizados son GET e POST.
- O enderezo URI do recurso especifica a ruta do recurso dentro do directorio raíz do sitio web do que se solicita o recurso. Por exemplo, a URI /imag/escudo.gif indica que o recurso solicitado é escudo.gif e encóntrase no directorio imag baixo o directorio raíz do sitio.
- As liñas de encabezados indican varias opcións relativas á petición. Cada encabezado represéntase cunha liña de texto co nome da opción ou do encabezado, o carácter ": " e o valor asignado á opción.
- O corpo da petición está baleiro se a petición usa o método GET e contén información que se envía o servidor se usa o método POST.

Podes instalar unha extensión para o teu navegador que che permita ver o contido das mensaxes de petición e resposta HTTP das conexións que establezas. Para Mozilla Firefox a extensión chámase "Live Http Headers". Para Internet Explorer, unha posible extensión é "IEWatch".

Métodos e encabezados das mensaxes de petición

O método dunha petición HTTP indica a acción que se quere realizar sobre o recurso obxecto da petición.

Na versión 1.0 de HTTP só se admitían tres métodos.

- *GET*: o cliente solicita que o servidor lle envíe unha representación do recurso indicado na petición. Con representación referímonos ao contido do arquivo correspondente ao recurso. Sempre que pulsamos co rato nun enlace dunha páxina web a calquera recurso ou escribimos unha URL na barra de direccións|enderezos do navegador, este envía polo menos unha mensaxe de petición co método GET.
- *POST*: mediante este método, o cliente envía información ao recurso indicado do servidor para que sexa procesada por unha aplicación. Normalmente úsase este método cando enchemos un formulario dunha páxina web e pulsamos un botón como "Enviar", "Confirmar" ou calquera similar. No corpo da mensaxe envíase a información a procesar.
- *HEAD*: solicítase ao servidor que envíe soamente os encabezados correspondentes á petición do recurso que se indique. Para un mesmo recurso, o servidor respondería coa mesma liña de resposta e os mesmos encabezados que para unha petición GET pero non enviaría o contido do recurso. Úsano os navegadores por exemplo para saber se unha páxina web que teñen almacenada en caché foi actualizada no servidor.

A versión 1.1 de HTTP engade os seguintes métodos:

- *PUT*: Serve para que se solicite almacenar a información enviada no recurso indicado na URI. Para que o servidor acepte unha petición PUT ten que telo autorizado na súa configuración.
- *DELETE*: Serve para solicitar ao servidor que elimine o recurso indicado na URI. Para que o servidor acepte unha petición DELETE ten que telo autorizado na súa configuración.
- *OPTIONS*: Solicita ao servidor que o informe sobre as características da comunicación que permite establecer. Serve para que o cliente estableza opcións axeitadas nas seguintes peticións cara ao servidor.
- *TRACE*: Serve para saber se a petición chega correctamente ao servidor. Solicítase ao servidor que responda coa petición que se lle enviou.
- *CONNECT*: Éste método utilízase para solicitar ao servidor unha canle de comunicación segura usando https.

Os encabezados dunha petición permiten indicar opcións relativas á petición. Algúns dos encabezados para as mensaxes de petición son:

Encabezados de peticións HTTP

Encabezado	Significado
Host	Equipo ao que se envía a petición.
User-Agent	Nome e versión do cliente (navegador) e do sistema operativo.
Accept	Tipo de contido que acepta o navegador.
Accept-Language	Idiomas que espera o navegador nas páxinas recibidas.
Accept-Encoding	Sistema de codificación que espera o navegador para o recurso a recibir.

Accept-Charset	Xogo ou conxunto de carácteres que espera recibir o navegador.
Referer	URL dende onde se orixinou a petición (URL da páxina que contiña o enlace).
Cookie	Contido da cookie almacenada no equipo cliente e relativa ao sitio web ao que se fai a petición.

Mensaxes de resposta

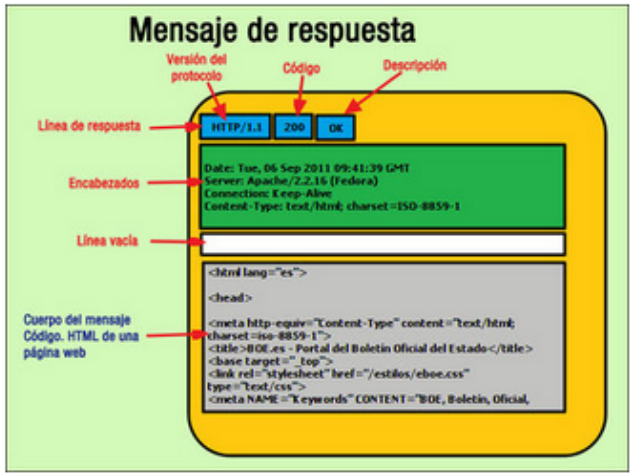
As mensaxes HTTP de resposta son enviadas polo servidor HTTP a clientes HTTP en resposta a unha petición. Nunha mensaxe de resposta hai unha liña de petición, varias liñas de encabezados, unha liña baleira e un corpo da mensaxe. No corpo da mensaxe, o servidor envía o contido do recurso que se lle solicitou (cando se solicita o seu envío). Por exemplo, pode conter o código HTML dunha páxina web.

Nunha mensaxe de resposta, a liña de resposta (tamén chamada liña de estado) contén tres datos:

- Versión do protocolo.
- Código de resposta ou código de estado.
- Descrición de resposta ou descrición de estado.

O código de resposta é un valor numérico que representa como foi recibida e procesada a petición á que se está a responder. A descrición é unha frase curta que describe o que se está a indicar co código de resposta (a cada código corresponde unha descrición).

A seguinte imaxe mostra cada un dos elementos que forman parte dunha mensaxe de resposta HTTP.



Os encabezados dunha resposta indican opcións relativas á resposta. Algúns deses encabezados son:

Encabezados de respostas HTTP

Encabezado	Significado
Date	Data e hora en que comezou o envío do recurso solicitado.
Server	Nome do software servidor.
Content-Language	Código do idioma en que está escrito o recurso que se envía no corpo da mensaxe.
Content-Encoding	Sistema de codificación que se utiliza na representación do recurso dentro do corpo da mensaxe.
Connection	Serve para indicar se o servidor mantén a conexión TCP para as seguintes transaccións HTTP dende o cliente. Se ten o valor keep-alive mantén a conexión e se ten o valor close péchaa, en cuxo caso, se o cliente ten que enviar unha nova petición HTTP terá que solicitar previamente unha nova conexión TCP.

Códigos de resposta

Un código de resposta ou código de estado é un número de tres cifras que se inclúe na liña de resposta dunha mensaxe de resposta HTTP, e que serve para indicar se unha petición se recibiu e se atendeu correctamente, ou se se produciu calquera problema ou circunstancia que alterase unha normal recepción e atención da petición.

O primeiro díxito do código representa un grupo de respostas. Identifica de forma xeral o tipo de resposta. Os dous díxitos seguintes permiten especificar a resposta concreta dentro do grupo. Por exemplo, o código de resposta 200 para unha petición GET indica que se está a responder cunha resposta que inclúe o recurso que se solicitou e o código 201 indica que se creou no servidor o recurso que se solicitou.

Na seguinte táboa represéntanse os posibles grupos de códigos de resposta e unha descrición do que se indica nas respostas pertencentes a cada grupo.

Códigos de resposta

Código	Descrición
1xx	Resposta Informativa: Indícalle ao cliente que se recibiu a petición e se está a continuar. Trátase dunha resposta provisional e hai que realizar unha nova transacción HTTP para que se poida obter a reposta definitiva. Non se aconsella que os servidores envíen estas respostas.
2xx	Petición correcta: Indica que a petición recibida anteriormente foi recibida, aceptada e procesada correctamente no servidor.
3xx	Reenderezo: Indícaselle ao cliente HTTP que ten que realizar algunha acción adicional para que se poida resolver completamente a petición que se realizou.

4xx Erros do cliente: Recibiuse unha petición cunha sintaxe errónea ou non se puido procesar a petición.
5xx Erro de servidor: Produciuse un erro no servidor que lle impediu atender e procesar a petición.

4. Tipos MIME

O protocolo HTTP transmite a información en código ASCII. Entón, Como pode transmitir arquivos non ASCII como os de imaxe, de vídeo e outros moitos? A resposta é: usando MIME. MIME ou Multipurpose Internet Mail Extensions (Extensións Multipropósito de Correo de Internet), establece un conxunto de especificacións para que se poidan enviar varios tipos de arquivo mediante correo electrónico. En principio MIME estaba orientado a usarse no correo electrónico. MIME úsase tamén no protocolo HTTP para dar maior funcionalidade a este permitindo que poida transmitir multitude de tipos de arquivos sempre que navegador e servidor soporten MIME.

Un tipo MIME é a especificación dun tipo de arquivo que pode transmitirse usando as extensións MIME para HTTP ou para correo electrónico. MIME foi desenvolvido por IETF e publicado nos RFCs 2045, 2046, 2047, 2077, 4288 e 4289.

MIME establece unha serie de encabezados que se poden engadir aos xa existentes para HTTP, e que se poden usar nas liñas de encabezados das mensaxes HTTP. Dous destes encabezados son:

- *Mime-version*: versión de MIME (a actual é 1.0).
- *Content-type*: especifica o tipo MIME para un arquivo enviado. Por exemplo. para un arquivo de imaxe "JPG", o tipo MIME é "*image/jpeg*".

Se un servidor HTTP envía un arquivo sen especificar o tipo MIME asociado ou especificándoo de forma incorrecta, pode acontecer que o navegador web non abra o arquivo correctamente porque descoñeza a aplicación que ten que abrilo.

Podes consultar a lista de tipos mime na seguinte ligazón

5. Servidores Web

Á hora de decidirnos por un servidor web ou HTTP, podemos optar entre varios servidores dispoñibles. Na seguinte táboa lístanse e describen os servidores web máis utilizados.

Servidores web

Servidor	Descrición
Apache	É o máis usado en Internet. Desenvolvido por Apache Software Foundation. É software libre, gratuíto e multiplataforma (Unix, Linux, Windows. Netware).
Microsoft IIS	É software propietario e só se pode instalar en sistemas Windows.
Oracle iPlanet Web Server	Está desenvolvido en Java por Oracle. Soporta o uso de aplicacións JSP, Servlets, PHP,Actualmente é multiplataforma. Este producto é continuación do Sun Java System Web Server, desde o momento que Oracle adquiriu Sun

Tomcat	Ao igual que Apache está desenvolvido por Apache Software Foundation. É software libre, gratuíto e multiplataforma. Usa unha tecnoloxía distinta á de Apache. Permite traballar con algunhas páxinas dinámicas coas que non pode traballar Apache. Pode traballar como un servidor de aplicacións.
Ngnix	É un servidor que consume moi poucos recursos. Pódese instalar en sistemas Unix/Linux e Windows. É software libre e gratuíto.
Lighhttp	É tamén un servidor que consume moi poucos recursos e moi doado de configurar coa súa ferramenta gráfica de configuración. É software libre, gratuíto e multiplataforma.

Poden consultarse as estatísticas de uso dos servidores web no sitio web de Netcraft

Tamén como curiosidade, se queremos crear un servidor web, que sirva unicamente un so arquivo, podemos usar o comando *nc*

```
while true; do { echo -e 'HTTP/1.1 200 OK\r\n'; cat index.html; } | nc -l 8080; done
```

Servidores Web virtuais

Os servidores virtuais permiten que un mesmo servidor web poida traballar como servidor para varios sitios web. Así, usando servidores virtuais poderemos facer que un servidor web Apache administre os sitios `www.motoclubpblancas.com` e `www.centroelacebo.com` As empresas de hosting usan os servidores virtuais para poder aloxar varios sitios web.

Pódense crear tres tipos de servidores virtuais:

- Baseados en enderezos IP: por cada dirección|enderezo IP do equipo servidor web terase un servidor web virtual. Para ter esta configuración necesitaríase ter no equipo varios adaptadores de rede ou, o que sería mellor, crear varias interfaces virtuais de rede sobre un mesmo adaptador de rede e dar unha IP a cada unha das interfaces virtuais.
- Baseados en portos: o servidor web usará un porto de escoita por cada servidor virtual. Isto realízase por exemplo cando un servidor ten dous servidores virtuais e un escoita no porto 80 e o outro escoita no porto 443 debido a que ten que usar o protocolo https.
- Baseados en nomes: o servidor web pode aloxar varios sitios web pertencentes a distintos dominios usando para todos eles o mesmo enderezo e o mesmo porto de escoita.

6. Navegadores Web

Un navegador web é un cliente http ou cliente do servizo web pero non todo cliente do servizo web é un navegador.

Un navegador web é un programa cliente web que interpreta os documentos recibidos (xeralmente en código HTML), como páxinas web e que os presenta en pantalla amosando enlaces que permiten que o usuario interactúe con eles para acceder a outros documentos web. Tamén a partir do código HTML, un navegador representa en pantalla marcos, viñetas, cores de fondo, imaxes e outros moitos elementos.

Existe un amplo abano de navegadores web. A seguinte táboa mostra algúns deles. Hai moitos máis pero os que aparecen na táboa son dos máis destacados.

Navegadores Web

Navegador	Comentario
Internet Explorer	É moi utilizado por estar integrado nos sistemas Windows. Facilita e acelera a interacción con outros servizos.
Mozilla Firefox	Dispón dunha gran cantidade de complementos e extensións que se poden instalar para realizar diversas tarefas adicionais.
Google Chrome	Desarrollado por Google é de máis recente aparición que o resto de navegadores. É moi funcional e doado de usar.
Apple Safari	Desarrollado por Apple inclúese nos seus sistemas operativos. Ten unha aparencia cunha estética moi coidada.
Konqueror	Interfaz moi simple pero a navegación é moi rápida.
Ephipany	Adaptado para o escritorio GNOME.

7. HTTPS

O protocolo HTTPS (HTTP Secure) utiliza o protocolo HTTP combinado co protocolo SSL, (Secure Sockets Layer, Protocolo de Capa de Conexión Seguro), ou co protocolo TSL (Transport Layer Security, Seguridade na Capa de Transporte), para transmitir as mensaxes HTTP cifradas e para garantir a identidade do servidor ante os clientes.

Un servidor HTTPS usa por defecto o porto 443 como porto de escoita. Un cliente web, para conectarse cun servidor HTTPS ten que escribir na URL o protocolo https:// en lugar de http://.

Nunha conexión https, ao usar os protocolos SSL ou TSL, garántese:

- A **confidencialidade**: as mensaxes transmitidas están cifradas.
- A **integridade**: se unha mensaxe se modifica accidentalmente ou intencionadamente, o receptor detecta que se produciu esa modificación.
- A **autenticación**: pódese asegurar a identidade do servidor e/ou do cliente mediante o uso de certificados dixitais.

Certificados

Un servidor web HTTPS debe dispoñer dun certificado para poder establecer conexións seguras cos clientes.

Un certificado dixital ou electrónico é un documento dixital emitido por unha entidade Autoridad de Certificación (AC) que serve para garantir a identidade dun usuario nunha conexión.

Para establecer conexións seguras HTTPS, o servidor web ten que ter instalado un certificado que terá obtido dunha Autoridade de Certificación. Ao dispoñer dun certificado, o servidor envía as mensaxes asinadas cunha clave privada. A primeira vez que un cliente se conecta cun servidor HTTPS recibe unha clave pública, que lle servirá para descifrar as mensaxes enviadas polo servidor e verificar a súa

identidade. O cliente cifrará as mensaxes coa clave pública, e o servidor descifraraos coa clave privada.

Cando un navegador web se conecta por primeira vez cun sitio HTTPS, recibe a clave pública dende o servidor, dános información sobre o certificado correspondente e pídenos confirmación sobre se consideramos válido o certificado e, polo tanto, desexamos usar a clave pública para conectarnos co servidor. As seguintes conexións do cliente co servidor verificarán de forma automática a identidade do servidor e non nos pedirán autorización.

Os navegadores web normalmente dispoñen dunha lista de Autoridades de Certificación, que lles permite establecer conexións automaticamente (sen ter que confirmar) con servidores HTTPS, que dispoñen dun certificado emitido por algunha desas Autoridades de Certificación.

Autoridades de Certificación

Unha Autoridade de Certificación é unha entidade considerada de confianza que se encarga de emitir certificados para usuarios que sirvan para garantir a identidade destes ante outros usuarios.

Para que un servidor web poida traballar con HTTPS, debe obter un certificado dunha Autoridade de Certificación. Desta forma, os clientes web poderán confiar na identidade do servidor web ao estar certificado por unha entidade considerada de confianza.

Como veremos despois, é posible xerar un certificado autoasinado nun ordenador cun determinado software, sen que o emitise unha Autoridade de Certificación. Pero os usuarios dificilmente confiarían en sitios con certificados autofirrnados. Nós usaremos esta técnica para realizar probas con certificados. Normalmente, hai que pagar para obter un certificado dunha AC ademais de ter que cumprir uns requisitos.

Hai varias Autoridades de Certificación ás que podemos solicitar un certificado, entre elas:

- VeriSign.
- GlobalSign.
- CyberTrust.
- RSA Security.

A *Fábrica Nacional de Moeda e Timbre* (FNMT) é unha entidade dependente do Goberno de España e encárgase de emitir certificados para que os cidadáns se identifiquen ante as Administracións Públicas, Empresas Públicas, Universidades, etc.

No seguinte vídeo podes ver un resumo sobre os certificados dixitais:

https://www.youtube.com/watch?v=EU6vgU077xU

Última modificación: viernes, 30 de septiembre de 2022, 21:58