Segunda parte. Propuesta

Capítulo 4. Diseño del Sistema

4. Diseño del Sistema

Para la implementación del sistema de videoconferencia en la plataforma educativa EDUCAFI, se hace uso de Dimdim que es una herramienta de software libre, la cual permite hacer modificaciones al código fuente para adecuarlas a las necesidades que se requieran, a través de Dimdim los docentes podrán interactuar con los alumnos, pero solo los alumnos que estén inscritos en el mismo curso podrán acceder al sala de videoconferencia, hasta que el docente inicie sesión en la sala de videoconferencia los alumnos podrán acceder a ella de lo contrario el acceso no será permitido y una vez que el docente haya terminado la sesión de videoconferencia automáticamente todos los alumnos que se encuentren dentro de ella terminarán su sesión de videoconferencia.

4.1 Modelo de Procesos

El docente se conecta a Internet mediante un navegador Web, para establecer una conexión con la plataforma Moodle mediante el servidor Apache, quien se encarga de establecer la conexión entre el docente y la plataforma. Una vez establecida la conexión el docente tiene que autenticarse en la plataforma Moodle, el lenguaje de programación PHP se va encargar de hacer la verificación de los datos del docente haciendo una conexión con la Base de Datos MySQL, ya autenticado se establecerá la conexión con el servidor Dimdim para el cual también debe autenticarse y comenzar la sesión de videoconferencia.

Para los demás usuarios (alumnos) el procedimiento de autenticación es el mismo, sólo que una vez que estén dentro de la plataforma Moodle no podrán accesar a la sesión de videoconferencia hasta que el docente lo haga.

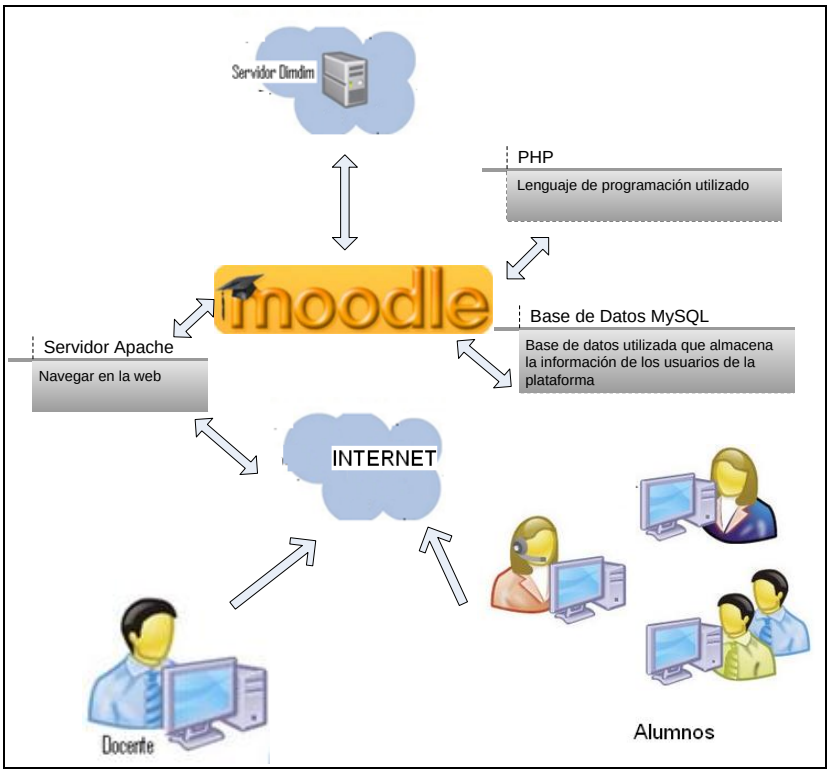

Figura 4.1. Modelo de procesos

4.1.1 Servidor Web

Para conectarse al servidor Moodle es necesario contar con un servidor Web, este es un software para atender y responder a las diferentes peticiones que hacen los usuarios a través de los navegadores, proporcionando los recursos que soliciten usando el protocolo HTTP o el protocolo HTTPS (Web seguro) para Moodle se utilizó la aplicación Apache como se mencionó en el capítulo 3. Un servidor Web básico cuenta con un esquema de funcionamiento muy simple, basado en ejecutar infinitamente el siguiente bucle:

- Espera peticiones en el puerto TCP indicado (el estándar por defecto para HTTP es el 80 y para HTTPS es el 443)
- Recibe una petición
- Busca el recurso
- Envía el recurso utilizando la misma conexión por la que recibió petición
- Vuelve al segundo punto

Protocolo TCP/IP

Los protocolos son reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadoras conectadas en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet.

El protocolo TCP/IP (Transmition Control Protocol/Internet Protocol) hace posible enlazar cualquier tipo de computadoras, sin importar el sistema operativo que usen o el fabricante. Este protocolo fue desarrollado originalmente por el ARPA (Advanced Research Projects Agency) del Departamento de Defensa de los Estados Unidos. Actualmente, es posible tener una red mundial llamada Internet usando este protocolo. Este sistema de IP permite a las redes enviar correo electrónico (e-mail), transferencia de archivos (FTP) y tener una interacción con otras computadoras (TELNET) no importando donde estén localizadas, tan solo que sean accesibles a través de Internet.

Los servicios más importantes de TCP/IP son:

Transferencia de Archivos FTP (File Transfer Protocol). Este protocolo permite a los usuarios obtener o enviar archivos a otras computadoras en una red amplia (Internet), se debe implementar cierta seguridad para restringir el acceso a ciertos usuarios y además a ciertas partes del servidor (computadora).

Acceso Remoto: El acceso remoto (Telnet) en un protocolo que permite el acceso directo de un usuario a otra computadora en la red, para establecer un Telnet, se debe establecer la dirección o nombre de la computadora a la cual se desea conectar; mientras se tenga el enlace, todo lo que se escriba en la pantalla, será ejecutado en la computadora remota, haciendo un tanto invisible a la computadora local. Cuando se accede por este tipo de protocolos, generalmente

la computadora remota pregunta por un nombre de usuario y por una contraseña; cuando se desea terminar con la sesión, basta con terminar este protocolo, para salir generalmente con los comandos: logout, logoff, exit, etc.

Sistemas de archivo en red (NFS): Permite a un sistema acceder archivos en otra computadora de una manera más apropiada que mediante un FTP. El NFS da la impresión de que los discos duros de la computadora remota están directamente conectados a la computadora local. De esta manera, se crea un disco virtual en el sistema local. Esto es bastante usado para diferentes propósitos, tales como poner gran cantidad de información en una cuantas computadoras, pero permitiendo el acceso a esos discos. Esto aparte de los beneficios económicos, permite trabajar a los usuarios en varias computadoras y compartir archivos comunes.

Impresión Remota: Permite acceder impresoras conectadas en la red, para lo cual se crean colas de impresión y el uso de dichas impresoras se puede restringir, mediante alguna contraseña o a ciertos usuarios. Los beneficios son el poder compartir estos recursos.

Ejecución remota: Esto permite correr algún programa en particular en alguna computadora, es útil cuando se tiene un trabajo de gran tamaño que no es posible correr en un sistema pequeño, siendo necesario ejecutarlo en uno grande. Se tiene diferentes tipos de ejecución remota, por ejemplo, se puede dar algún comando o algunos para que sean ejecutados en alguna computadora en específico. Con un sistema más sofisticado, es posible que ese proceso sea cargado a alguna computadora que se encuentre disponible para hacerlo.

Servidores de Nombres: En instalaciones grandes, hay una buena cantidad de colección de nombres que tienen que ser manejados, esto incluye a usuarios junto con sus contraseñas, nombre, direcciones de computadoras en la red y cuentas. Resulta muy tedioso estar manejando esta gran cantidad de información,

por lo que se puede destinar a una computadora que maneje este sistema, en ocasiones es necesario acceder estos servidores de nombres desde otra computadora a través de la red.

Servidores de Terminales: En algunas ocasiones, no se requiere tener conectadas las terminales directamente a las computadoras, entonces, ellos se conectan a un servidor de terminales. Un servidor de terminales es simplemente una pequeña computadora que solo necesita correr el Telnet (o algunos otros protocolos para hacer el acceso remoto). Si se tiene una computadora conectada a uno de estos servidores, simplemente se tiene que teclear el nombre de la computadora a la cual se desea conectar. Generalmente se puede tener varios enlaces simultáneamente, el servidor de terminales permitirá hacer la conmutación de una a otra en un tiempo muy reducido.

Puerto

Es una numeración lógica que se asigna a las conexiones, tanto en el origen como en el destino o denominado también como un canal lógico. No tiene ninguna significación física (Protocolos de Comunicación, 2011).

Puertos de Comunicación

El permitir o denegar acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otra computadora) deben “escuchar” en un puerto conocido de antemano para que un cliente (que inicia la conexión) pueda conectarse, esto quiere decir que cuando el sistema operativo recibe una petición a ese puerto, la pasa a la aplicación que escucha en él, si hay alguna, y a ninguna otra. Los servicios más habituales tienen asignados los llamados puertos bien conocidos, por ejemplo el 80 para Web, el 21 para Ftp, el 23 para Telnet, etc.

Los estados de un puerto son:

- **Abierto:** Acepta conexiones. Hay una aplicación escuchando en este puerto, esto no quiere decir que se tenga acceso a la aplicación, sólo que hay posibilidad de conectarse.
- **Cerrado:** Se rechaza la conexión; probablemente no hay aplicación escuchando en este puerto, o no se permite el acceso por alguna razón. Este es el comportamiento normal del sistema operativo.
- **Bloqueado:** No hay respuesta. Es el estado ideal para un cliente en Internet, de esta forma ni siquiera se sabe si la computadora está conectada. Normalmente este comportamiento se debe a un cortafuegos de algún tipo, o a que el ordenador está apagado.

¿Por qué es peligroso tener un puerto abierto? Al fin y al cabo los puertos son puntos de acceso a aplicaciones corriendo en un ordenador. Aunque en teoría no fuese un problema, estas aplicaciones pueden tener vulnerabilidades que pueden ser aprovechadas por otros usuarios, desde el punto de vista de seguridad, es recomendable permitir el acceso sólo a los servicios que sean imprescindibles, dado que cualquier servicio expuesto a Internet es un punto de acceso potencial para intrusos (Conceptos básicos del servidor web, 2003).

Puerto 80 (HTTP)

Hace referencia a Hypertext Transfer Protocol (HTTP en español Protocolo de Transferencia de Hipertexto) es el protocolo usado en cada transacción de la World Wide Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura Web (clientes, servidores) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Cuando se solicita una página Web desde el navegador, esté realiza una conexión al puerto 80 del servidor Web la URL debe comenzar con "http”.

Puerto 443 (HTTPS)

Este puerto hace referencia a Hypertext Transfer Protocol Secure (HTTPS para web seguro) es una combinación del protocolo HTTP y protocolos criptográficos, se emplea para lograr conexiones más seguras en la WWW, cada vez que se intercambie información sensible (por ejemplo, contraseñas) en internet. De esta manera la información sensible, en el caso de ser interceptada por un ajeno, estará cifrada. El nivel de protección que ofrece depende de la corrección de la implementación del navegador web, del software y de los algoritmos criptográficos soportados.

- **Características del HTTPS**

Para distinguir una comunicación o página Web segura, la URL debe comenzar con "https://" (empleando el puerto 443 por defecto); en tanto la tradicional es "http://" (empleando el puerto 80 por defecto). Originalmente HTTPS sólo utilizaba encriptación SSL, luego reemplazado por TLS, por lo tanto el usuario ya sea docente o alumno tendrá que hacer peticiones al servidor Moodle mediante un navegador Web pero haciendo la petición mediante Web seguro (https), se utilizó Web seguro la razón es que la información que se maneja la plataforma es muy importante, por ejemplo, cuentas de usuario para acceder a la plataforma, archivos, etc. (Protocolos de Comunicación, 2011).

4.1.2 Diseño de base de datos

Para almacenar la información correspondiente a las sesiones de videoconferencia se creó la tabla mdl_dimdim dentro de la base de datos de nuestro servidor Moodle, esta tabla fue creada por la plataforma Moodle al momento de implementar el sistema de videoconferencia. La información que se almacena es la referente a una sesión de videoconferencia, toda sesión tendrá un *id* único para identificar la sesión, el campo “curso” es un índice que hace referencia al curso en el cual se está creando la sesión de videoconferencia, por lo

tanto toda sesión creada tiene asociada un curso que pertenece al docente quien crea la sesión y en donde los alumnos la pueden ver para establecer el contacto. La tabla contiene los siguientes campos:

Campo	Tipo
id	bigint(10)
course	bigint(10)
name	varchar(255)
studentlogs	smallint(4)
emailuser	varchar(255)
displayname	varchar(255)
startnow	varchar(255)
timezone	varchar(255)
lobby	varchar(255)
meetinghours	smallint(4)
meetingminutes	smallint(4)
maxparticipants	smallint(4)
timemodified	bigint(10)
audiovideosettings	smallint(4)
privatechat	varchar(255)
publicchat	varchar(255)
screencast	varchar(255)
whiteboard	varchar(255)
participantlist	varchar(255)
displaydialinfo	varchar(255)
interntoll	text
moderatorpasscode	text
attendeepasscode	text
enterpriseusername	varchar(255)
enterpriseuserpassword	varchar(255)
feedback	varchar(255)
assistantenabled	varchar(255)
handsfreeonload	varchar(255)
assignmikeonjoin	varchar(255)
allowattendeeinvite	varchar(255)
featuredocshare	varchar(255)
featurecobshare	varchar(255)
featurerecording	varchar(255)

Tabla 4.1 Campos de la tabla mdl_dimdim.

Descripción de la tabla mdl_dimdim

Id: Valor único que representa a una sesión de videoconferencia.
course: Hace referencia al curso en el que fue creada la sesión de videoconferencia.
name: Almacena el nombre que se le dio a la sesión de videoconferencia.
studentlogs: Contiene el número de alumnos que ingresan a la sesión.
emailuser: Almacena el correo electrónico del docente quien configuró esa sesión de videoconferencia.
displayname: En este campo se tiene el nombre del docente quien creó la sesión de videoconferencia.
startnow: Contiene la información para iniciar la sesión de videoconferencia contiene un valor por defecto el cual es “on” con esto se podrá iniciar la sesión.
timezone: Almacena la zona horaria en la que fue creada la sesión.
lobby: Almacena la información relacionada con la sala de espera, 0 si esta deshabilitada y 1 cuando este habilitada.
meetinghours: En este campo se tiene el tiempo requerido para la sesión en horas.
meetingminutes: Almacena el tiempo requerido para la sesión en minutos.
maxparticipants: Tiene el número máximo de participantes que ingresaran a la sesión.
timemodified: Guarda la hora de modificación de la sesión, cuando se realizan cambios en la configuración de la misma.
audiovideosettings: Almacena la información referente a las configuraciones de audio y video, con cuatro valores diferentes:

- 0 indica que se configuró con audio y video
- 1 indica que se configuró solo con audio
- indica que se configuró solo con video
- indica que se configuró sin audio y video

privatechat: Se tiene la información referente a si la sesión permitirá chat privado o no lo permitirá, tiene dos valores diferentes:

- 0 está habilitado el chat privado
- 1 está deshabilitado el chat privado

publicchat: Almacena la información referente a si la sesión permitirá chat público o no lo permitirá, tiene dos valores diferentes:

- 0 está habilitado el chat público
- 1 está deshabilitado el chat público

screencast: Guarda la información si se permitirá tener la opción de escritorio remoto o no se tendrá, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

whiteboard: Almacena la información si se permitirá tener la opción de mostrar pizarra o no se tendrá, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

participantlist: Contiene la información para mostrar la lista de participantes en la sesión o no se mostrará, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

displaydialinfo: Almacena los datos para mostrar la información del estado en línea de los participantes, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

interntoll: Contiene un número interno para cada sesión.

moderatorpasscode: Guarda la contraseña del moderador, en el caso que se establezca un moderador de la sesión.

attendeepasscode: Almacena un código de acceso de los asistentes, en el caso que se le quiera poner esta restricción a la sesión.

meetingkey: Contiene una cadena que fungirá como llave de acceso para entrar a la sesión, en el caso que se desee poner esta restricción.

enterpriseusername: Almacena el nombre de usuario del docente quien creó la sesión.

enterpriseuserpassword: Guarda el nombre de usuario del docente quien creó la sesión.

feedback: Almacena los comentarios referentes a la sesión creada.

assistantenabled: Contiene los datos para permitir o no la entrada de los alumnos, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

handsfreeonload: Almacena los datos para permitir el uso de manos libres al iniciar la sesión, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

assignmikeonjoin: Asignar micrófono al unirse a la sesión, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

allowattendeeinvite: Guarda la información que permitirá tener la opción de poder invitar a otros participantes a la sesión, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

featuredocshare: Contiene la información si se permitirá tener la opción de compartir documentos o no se tendrá, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

featurecobshare: Almacena la información que permite compartir documentos dentro de la sesión, tiene dos valores diferentes:

- 0 está habilitado
- 1 está deshabilitado

Featurerecording: Almacena la información que permitirá o no poder grabar la sesión.

Todos estos datos son solicitados cada vez que el docente creé una nueva sesión, el *id* se genera automáticamente y el campo curso se llena dependiendo en donde se creó la sesión, por lo tanto las sesiones solo podrán ser creadas dentro de un curso en la plataforma.

Diagrama Entidad Relación

Se muestra la relación que existe entre la tabla mdl_course y la tabla mdl_dimdim, existe una relación de uno a muchos, un curso puede tener una o más sesiones de videoconferencia pero una sesión de videoconferencia solo puede estar asociada a un curso. En la tabla mdl_dimdim el campo course es el encargado de asociar el curso en que se crea la sesión.

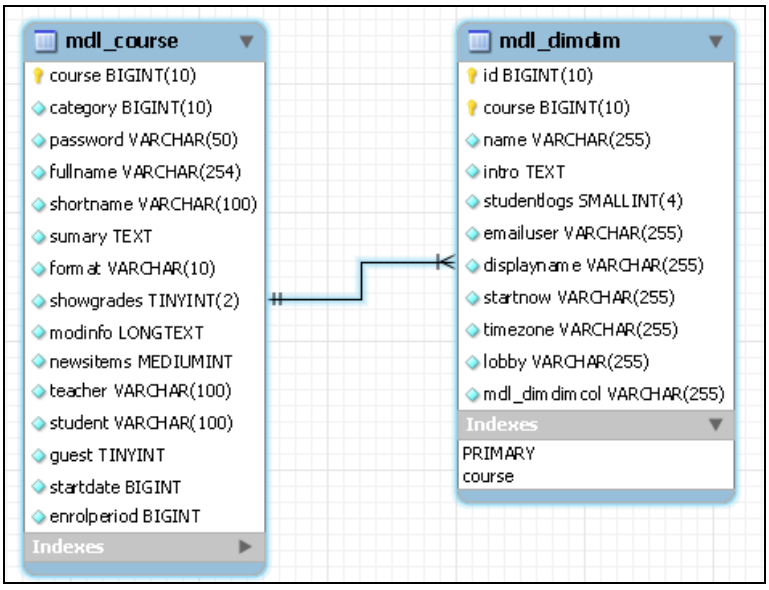

Figura 4.2. Diagrama Entidad Relación.

El campo course de la tabla mdl_course es el único que se relaciona con el campo course de la tabla mdl_dimdim, por lo cual debe existir esta relación para que cada sesión de videoconferencia tenga asociada un curso y solo uno.

4.1.3 Diseño de la aplicación con PHP

Se realizaron modificaciones al archivo dimdim.php esto para ajustar la aplicación a las necesidades requeridas, principalmente fueron modificaciones de lenguaje para ajustarlas al idioma en español, a continuación se mencionan las etiquetas que fueron modificadas.

$string['meetingName'] = 'Nombre de la sesión de videoconferencia';
$string['maxParticipants'] = 'Número máximo de participantes';
$string['startschedule'] = 'Fecha y hora de Inicio';
$string['configserverhost'] ='Host del servidor Dimdim o IP en la cual fue configurado';
$string['configserverport'] = 'Puerto del servidor Dimdim en el cual fue configurado';
$string['currentusers'] = 'Usuarios actuales';
$string['deletesession'] = 'Borrar esta sesión';
$string['deletesessionsure'] = '¿Estás seguro que quieres borrar esta sesión?';
$string['generalconfig'] = 'Configuración general';
$string['messages'] = 'Mensajes';
$string['neverdeletemessages'] = 'Nunca borrar mensajes';
$string['noguests'] = 'La session no está disponible para visitantes';
$string['nomessages'] = 'No hay mensajes todavía';
$string['conferencename'] = 'Nombre de la reunión';
$string['5'] = '5';
$string['10'] = '10';
$string['15'] = '15';
$string['20'] = '20';
$string['enable'] = 'Habilitar';

```
$string['disable'] = 'Deshabilitar';
$string['lobby'] = 'Área de espera';
$string['enterprise_username_label'] = 'Nombre de usuario de tu cuenta Dimdim';
$string['enterprise_password_label'] = 'Contraseña de tu cuenta Dimdim';
$string['meetinghours'] = 'Duración de la reunión en horas';
$string['1hour'] = '1';
$string['2hour'] = '2';
$string['3hour'] = '3';
$string['4hour'] = '4';
$string['5hour'] = '5';
$string['0mike'] = '0';
$string['1mike'] = '1';
$string['2mike'] = '2';
$string['3mike'] = '3';
$string['4mike'] = '4';
$string['5mike'] = '5';
$string['Audio Video'] = 'Audio Video';
$string['audio'] = 'Audio';
$string['audio-video'] = 'Audio-Video';
#$string['Video-Chat'] =  'Video Chat';
$string['NoAudioVideo'] = 'No Audio-Video';
$string['Video-Only'] = 'Solo Video';
$string['Network'] = 'Red';
$string['savemessages'] = 'Guardar sesiones anteriores';
$string['sessions'] = 'Sesiones';
$string['privatechat'] = 'Chat Privado';
$string['publicchat'] = 'Chat Público';
$string['screencast'] = 'Impresión de pantalla';
$string['whiteboard'] = 'Pizarrón';
$string['participantlist'] = 'Lista de participantes';
```

```
$string['interntoll'] = 'Llamada internacional';
$string['moderatorpasscode'] = 'Contraseña del moderador';
$string['attendeepasscode'] = 'Contraseña del asistente';
$string['meetingkey'] = 'Clave de la reunión';
$string['assistantenabled'] = 'Asistente Activado';
$string['handsfreeonload'] = 'Manos libres al iniciar';
$string['featuredocshare'] = 'Compartir documentos';
```