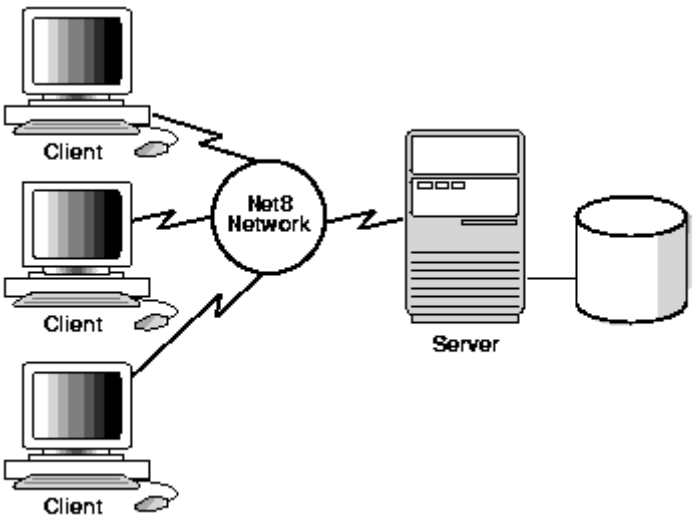
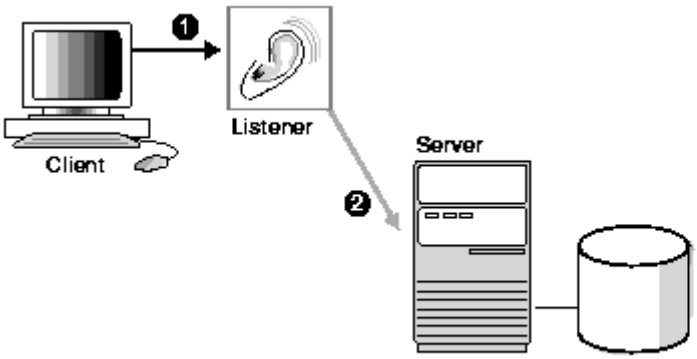
La función principal del protocolo Net 8 es establecer sesiones de red y transferir datos entre una máquina cliente y un servidor o entre dos servidores. Net8 debe estar presente en cada máquina de la red. Una vez que se establece la conexión, Net8 actúa como portador entre el cliente y el servidor.

La siguiente figura representa la conexión entre un cliente y un servidor:



Las sesiones de red se establecen con la ayuda de un LISTENER. Dicho LISTENER es un proceso autónomo que reside en el servidor. El LISTENER recibe peticiones de conexión por parte de los clientes y pasa dichas peticiones al servidor de Base de Datos. Cada vez que un cliente o servidor actuando como cliente, solicita una sesión con un servidor, el LISTENER recibe dicha solicitud.

La siguiente figura representa el papel del LISTENER en una solicitud de sesión:

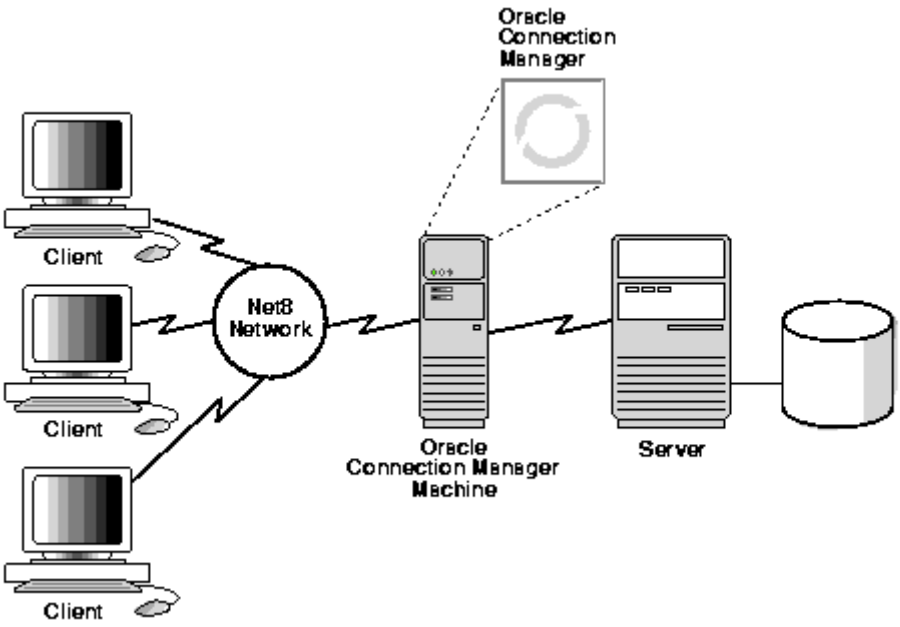


En entornos en los que se espera un gran número de conexiones sobre un mismo servicio, Net 8 ofrece un proceso de enrutamiento de sesiones llamado ORACLE Conexión Manager que normalmente reside en una máquina independiente.

Net 8 ofrece este servicio para entornos con:

- Gran número de usuarios accediendo a un único servicio y con un único protocolo.
- Servidores y clientes con distintos protocolos.
- Necesidad de control de clientes que acceden a servidores determinados en entornos TCP/IP.

La siguiente figura representa como las conexiones de clientes son manejadas por este ORACLE Conexión Manager, que reside en una maquina separada:



Cuando un usuario se conecta a un servicio de base de datos a través de la red, es pasado (a través de la red) un descriptor de conexión conteniendo la información de red necesaria.

Un descriptor de conexión contiene:

- Ruta de Red del servicio, incluyendo la localización del LISTENER a través de una dirección de protocolo.
- Nombre del servicio, normalmente el nombre global de la base de datos (dominio de base de datos y nombre de la misma)

La conexión por medio de un descriptor completo de conexión crea una cadena de conexión bastante larga, como se puede ver en el siguiente ejemplo:

```
CONNECT
scott/tiger@(description=(address=(protocol=tcp)(host=sales-server)(port=1521))
(connect_data=(service_name=sales.us.acme.com)))
```

Para evitar estas extensas cadenas de conexión, un descriptor de conexión puede ser mapeado a un identificador de conexión. Esta información es almacenada en, al menos, un método de nombres. Los clientes, por medio de este método, sólo necesitan indicar el identificador de conexión en la cadena de conexión:

```
CONNECT scott/tiger@sales
```

Durante el proceso de conexión, el cliente contacta con un método de resolución de nombres para resolver el identificador de conexión y obtener un descriptor de conexión. Una vez traducido se reenvía la petición al LISTENER.

El LISTENER, a través del protocolo, acepta la conexión del cliente. Compara la información del cliente con la información recibida desde la Base de Datos. Si la información coincide, la conexión queda establecida.

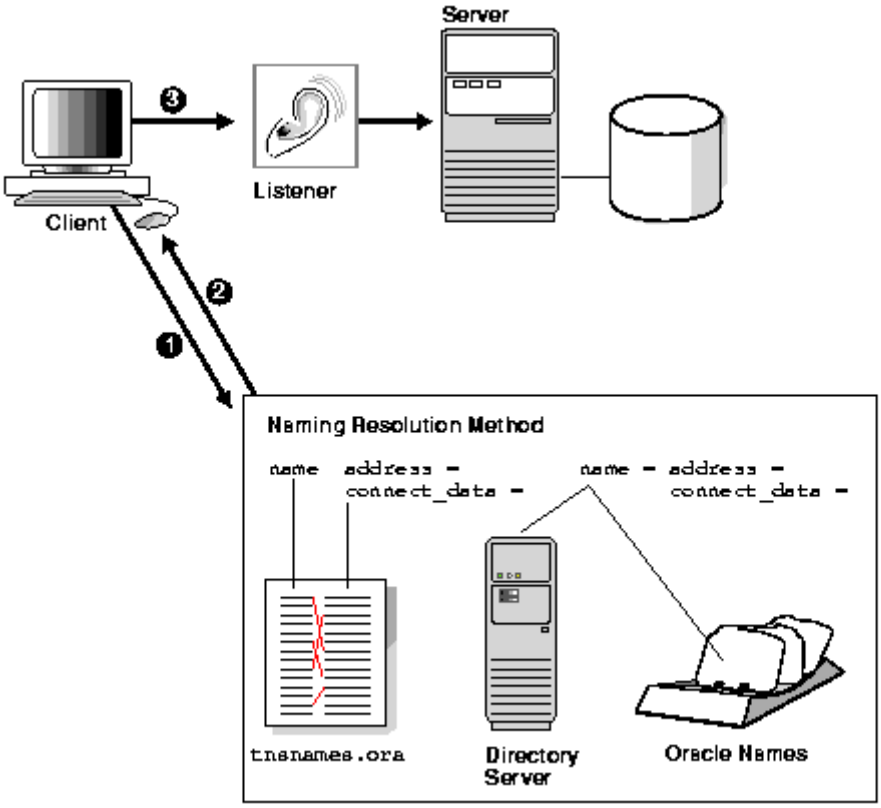
Para configurar la red para conexión de clientes y servidores es necesario:

- Configurar el Método de Nombres
- Configurar el LISTENER en el servidor

La configuración del método de Nombres permite las siguientes variantes:

- `Local Naming:` En ficheros en la máquina local
- `Directory Naming:` Por medio de LDAP
- `Oracle Names:` Servidor ORACLE de traducción de nombres
- `Host Naming:` Utilizando un sistema existente de traducción de direcciones IP
- `External Naming:` Un servicio de traducción de nombres externos

La siguiente figura muestra el funcionamiento del método de nombres:



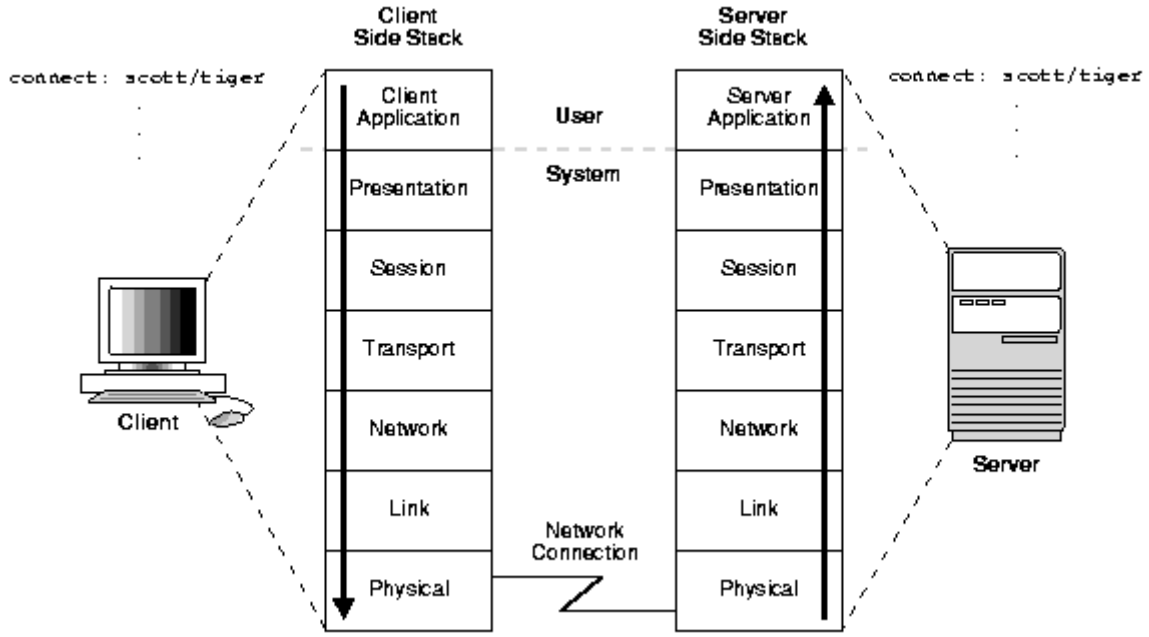
La configuración del LISTENER se realiza por medio de una o más direcciones de escucha y la información acerca del servicio de destino.

Las direcciones de escucha se configuran en el fichero LISTENER.ORA, la información del servicio puede ser configurada en el mismo fichero o no:

- Una base de datos ORACLE 8i registra cierta información con el LISTENER, como su nombre de servicio, nombre de instancia, …. Esta funcionalidad, llamada “SERVICE REGISTRATION” no requiere configuración en el fichero LISTENER.ORA.
- Otros servicios, bases de datos ORACLE 7 u ORACLE 8.0 requieren configuración de servicios en el fichero LISTENER.ORA

Capas cubiertas por Net8:□

En el modelo de comunicaciones OSI, las comunicaciones se establecen en las 7 capas que muestra la siguiente figura:



Net8 proporciona la funcionalidad de las capas de Sesión y Transporte. Es responsable del establecimiento y mantenimiento de la conexión entre el cliente y el servidor así como del intercambio de mensajes entre ellos. Para proporcionar estas funcionalidades, Net8 tiene tres componentes:

Network Interface (NI): Este componente proporciona un interface genérico para clientes y servidores ORACLE así como para procesos externos que tratan de acceder a la funcionalidad de Net8. NI hace uso de NN (Network Naming) para la resolución de identificadores de conexión.

Network Session (NS): Este componente recibe peticiones de NI e implementa las cuestiones genéricas de conexión a nivel de máquina. Concretamente implementa las funciones de open, close, send, receive. NI hace uso de NR (Network Route) para encaminar la sesión hacia el destino y NA (Network Authentication) para negociar detalles de autentificación con el destino.

Oracle Protocols: Son implementaciones de la capa de transporte. Son responsables de la correspondencia de las funcionalidades de NS a protocolos standard del mercado utilizados en la conexión cliente servidor. Cada protocolo es responsable de las correspondencias entre NS y el protocolo especifico. Los protocolos incluidos son:

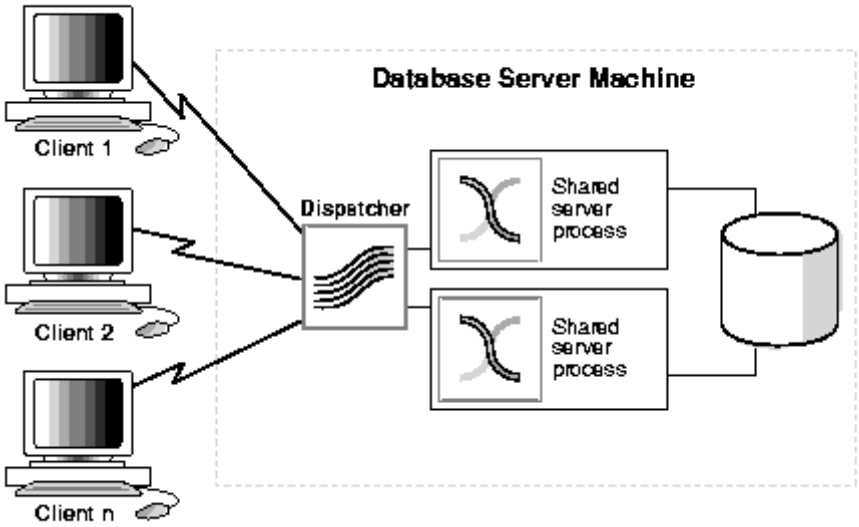
- TCP/IP
- TCP/IP con SSL
- SPX
- Named Pipes
- LU6.2

Modelos de Conexión:

Hay disponibles dos modelos de conexión entre clientes y servidores:

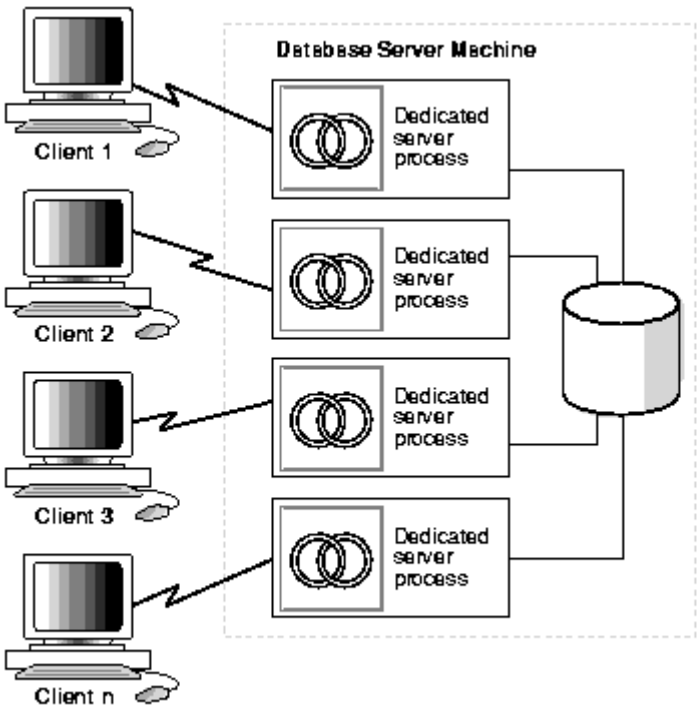
Multithreaded Server Model: En este modelo los procesos cliente son atendidos por un "DISPATCHER". Dicho proceso soporta múltiples conexiones concurrentemente. Este enfoque utilizando DISPATCHER permite dar servicio a un gran número de clientes con una carga aceptable del servidor.

La siguiente figura muestra el modelo expuesto:



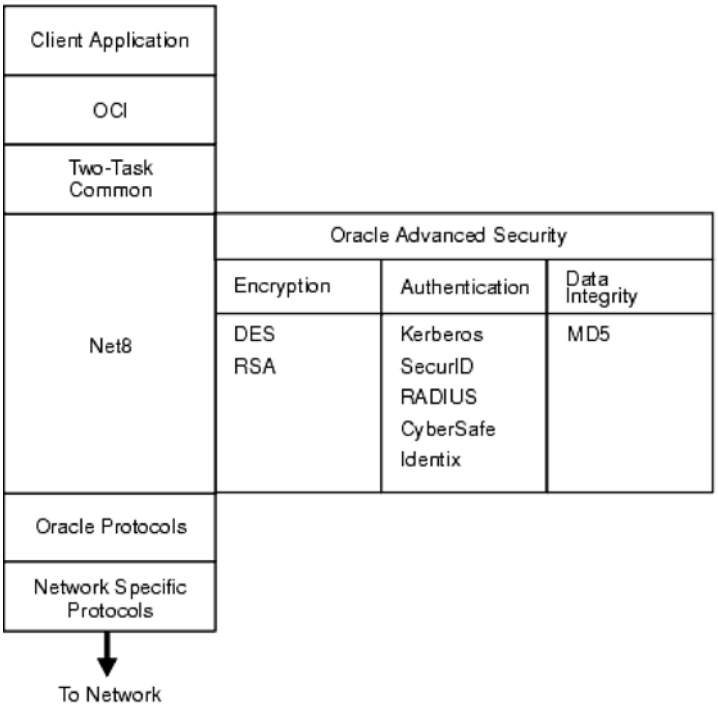
Dedicated Server Model: En este modelo cada proceso cliente es atendido por un proceso servidor. La instancia de Base de Datos y el LISTENER deben residir en la misma máquina. Net8 permite crear procesos dedicados antes de recibir peticiones de conexión.

La siguiente figura muestra el modelo expuesto:



La función principal del protocolo Net8 es establecer sesiones de red y transferir datos entre una máquina cliente y un servidor o dos servidores o entre dos servidores. Net8 debe estar presentes en cada máquina de la red. Una vez que se establece la conexión Net8 actúa como portador entre el cliente y el servidor.

Las características de ORACLE Advanced Security son un añadido al protocolo standard Net8.



Estas características de seguridad adicionales proporcionan:

Privacidad de Datos. Asegura que la información no es divulgada durante la transmisión. Soporta dos tipos de encriptación:

- **RSA Encryption:** Este módulo utiliza el algoritmo, de RSA Data Security, RC4. Todo el tráfico es salvaguardado utilizando una clave por sesión. Cualquiera de los componentes de la sesión (cliente o servidor) pueden solicitar la encriptación. La clave puede ser de 40, 56 o 128 bits. Mínimo coste en cuanto a rendimiento.

- **DES Encryption:** US Data Encryption Standard, requerido por instituciones financieras americanas. Advanced Security proporciona un algoritmo DES con clave de 56 bits. Ofrece asimismo un algoritmo DES de clave 40 bits por compatibilidad con versiones anteriores.

Integridad de Datos. Asegura que la información no es modificada o borrada durante la transmisión, ORACLE Advanced Security opcionalmente genera un mensaje criptográfico por medio del algoritmo MD5 y lo incluye con cada paquete enviado a través de la red.

Adicionalmente, la funcionalidad SSL de ORACLE Advanced Security permite el uso del algoritmo Secure Hash Algorithm (SHA) es algo más lento que el MD5 pero proporciona una clave más larga que lo hace más seguro contra ataques de “fuerza bruta” e inversión.

Autentificación El establecimiento de la identidad del usuario es un tema primordial en entornos distribuidos, de otra forma no se podría garantizar la seguridad a nivel de usuario. Las claves de acceso son el método tradicional de los entornos ORACLE. ORACLE Advanced Security proporciona se integra con servicios de autenticación más robustos, proporciona autenticación centralizada. Esto proporciona un nivel alto de confianza en la identidad del usuario, clientes y servidores en entornos distribuidos. Tener una facilidad de autentificación centralizada que autentifique todos los miembros de la red (clientes a servidores, servidores a servidores, usuarios a clientes

y servidores) es una forma efectiva de evitar la falsificación de identidad.

Autorización

La autorización de usuarios, un standard de Oracle 8i se implementa por medio de roles y privilegios. Esta implementación se ve mejorada por la integración de directorios LDAP versión 3. ORACLE Advanced Security permite el uso de ORACLE Internet Directory.