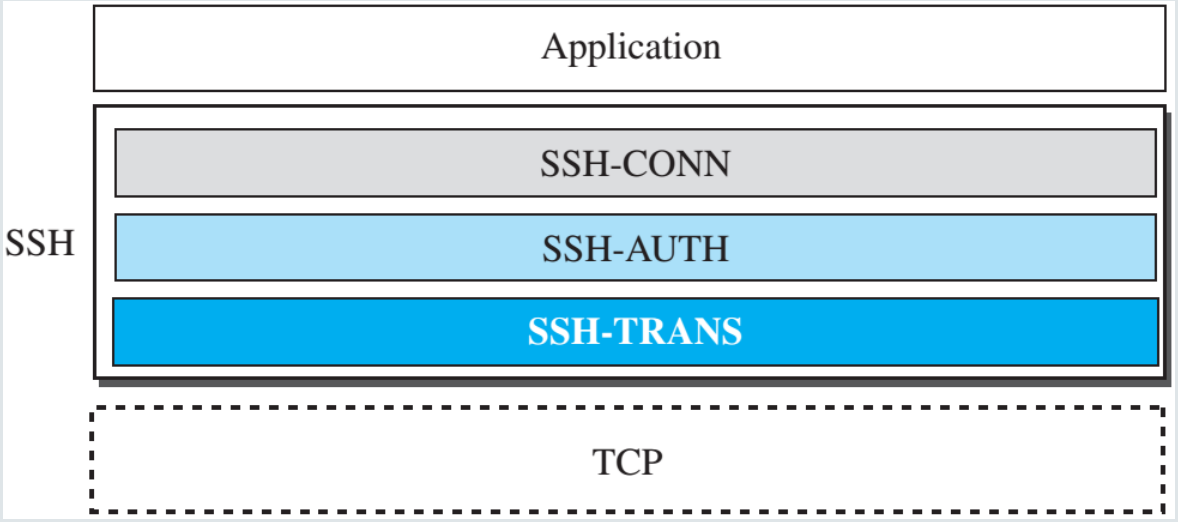
SSH

Secure Shell

SSH: Secure SHell

- Diseñado para reemplazar a TELNET
- Comprende tres componentes:
  - SSH – TRANS: protocolo SSH de capa de transporte
  - SSH – AUTH: Protocolo de autenticación SSH
  - SSH – CONN: Protocolo de conexión SSH



SSH - TRANS

- Ofrece un canal seguro sobre TCP
- Inicialmente se establece una conexión TCP insegura y luego el cliente y el servidor negocian un canal seguro
- Los servicios ofrecidos por este protocolo son:
  - Privacidad o confidencialidad del mensaje intercambiado
  - Integridad de datos (los datos no serán alterados por un intruso)
  - Autenticación de servidor (así el cliente tiene la seguridad que interactúa con el servidor correcto)
  - Compresión de mensajes.

SSH - AUTH

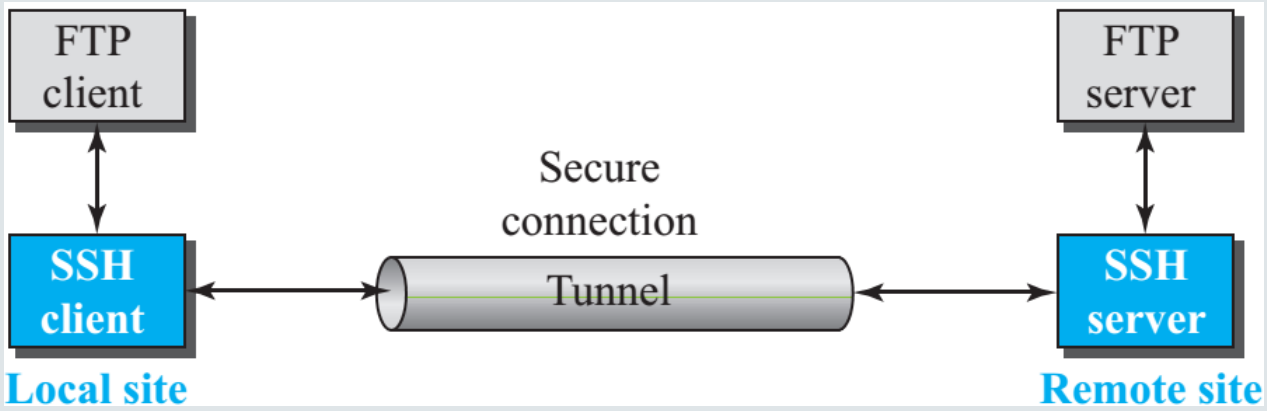
- Autentica al cliente frente al servidor.
- Se utiliza después de establecer un canal seguro y haber autenticado al servidor.
  - El cliente envía una petición al servidor, incluyendo el nombre de usuario, nombre de servidor, el método de autenticación y los datos requeridos
  - El servidor responde con un mensaje de éxito que confirma que el cliente esta autenticado o un mensaje de fracaso lo que significa que el proceso debe repetirse con un nuevo mensaje de petición.

SSH - CONN

- Después de establecer un canal seguro y autenticar al cliente y al servidor SSH invoca al protocolo SSH – CONN
- SSH – CONN ofrece servicios de multiplexado.
- Pueden crearse múltiples canales lógicos entre el cliente y el servidor
- Cada canal puede utilizarse para diferentes propósitos como acceso remoto, transferencia de archivos y otros.

USOS DE SSH

- Acceso remoto
- Transferencia de archivos
  - sftp – transferencia de archivos segura
  - scp – copia de archivos segura
- Reenvío de puerto: permite establecer un canal seguro entre aplicaciones que no proveen servicios de seguridad



FORMATO DE PAQUETE SSH

- Lenght: Longitud de paquete sin incluir el padding
- Padding: Se agrega para mejorar el nivel seguridad del paquete
- Type: Tipo de paquete enviado
- CRC : Se usa para control de errores