ÁREA 2. DESARROLLO DE SOFTWARE DE BASE

SUBÁREA 2.3 REDES DE COMPUTADORAS

TEMAS IMPORTANTE:

**Sistemas de Capas TCP/IP y OSI:**

El modelo TCP/IP es un modelo de referencia utilizado en redes de computadoras para la comunicación de datos. Este modelo fue desarrollado por el Departamento de Defensa de los Estados Unidos y se convirtió en el modelo de red utilizado en Internet.

1. **Entender la diferencia entre estos dos modelos y para qué sirven cada una de las capas**

El modelo de capas TCP/IP es un modelo de referencia utilizado en redes de computadoras para la comunicación de datos. El modelo consta de cuatro capas:

1. Capa de enlace de datos: Esta capa define cómo se transmiten los datos a través del medio físico, como los cables y las señales de radio. También se encarga de la detección y corrección de errores en los datos.

2. Capa de red: Esta capa se encarga de la transmisión de datos entre redes diferentes. La capa de red utiliza direcciones IP para enrutar los datos a través de la red.

3. Capa de transporte: Esta capa se encarga de la transferencia de datos entre los extremos de una conexión. Los protocolos más comunes en esta capa son TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario).

4. Capa de aplicación: Esta capa define los protocolos y servicios que los programas utilizan para comunicarse a través de la red. Algunos ejemplos de protocolos de la capa de aplicación son HTTP (Protocolo de Transferencia de Hipertexto), SMTP (Protocolo Simple de Transferencia de Correo) y FTP (Protocolo de Transferencia de Archivos).

Modelo OSI:

El modelo OSI (Interconexión de Sistemas Abiertos) es un modelo de referencia utilizado en redes de computadoras para la comunicación de datos. Fue desarrollado por la Organización Internacional de Normalización (ISO) para estandarizar la comunicación entre sistemas informáticos.

El modelo OSI consta de siete capas:

* Capa física: Esta capa se encarga de la transmisión de bits a través del medio físico, como los cables y las señales de radio.
* Capa de enlace de datos: Esta capa define cómo se transmiten los datos a través del medio físico y cómo se detectan y corrigen los errores en los datos.
* Capa de red: Esta capa se encarga de la transmisión de datos entre redes diferentes. La capa de red utiliza direcciones IP para enrutar los datos a través de la red
* Capa de transporte: Esta capa se encarga de la transferencia de datos entre los extremos de una conexión. Los protocolos más comunes en esta capa son TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario).
* Capa de sesión: Esta capa se encarga de establecer, mantener y terminar sesiones entre aplicaciones en diferentes sistemas
* Capa de presentación: Esta capa se encarga de la representación de los datos para que puedan ser entendidos por diferentes sistemas. Se encarga de la compresión, encriptación y codificación de los datos.
* Capa de aplicación: Esta capa define los protocolos y servicios que los programas utilizan para comunicarse a través de la red. Algunos ejemplos de protocolos de la capa de aplicación son HTTP (Protocolo de Transferencia de Hipertexto), SMTP (Protocolo Simple de Transferencia de Correo) y FTP (Protocolo de Transferencia de Archivos).

La principal diferencia entre el modelo TCP/IP y el modelo OSI es que el modelo TCP/IP consta de cuatro capas, mientras que el modelo OSI consta de siete capas.

Otra diferencia importante es que el modelo TCP/IP fue desarrollado como un modelo práctico para la implementación de redes, mientras que el modelo OSI fue desarrollado como un modelo teórico para estandarizar la comunicación entre sistemas informáticos.

El modelo TCP/IP es el modelo de red utilizado en Internet y se considera el modelo de referencia para la mayoría de las redes modernas. Cada capa del modelo TCP/IP es responsable de una función específica en la comunicación de datos y, al trabajar juntas, permiten la comunicación confiable y eficiente en las redes.

Por otro lado, el modelo OSI es menos utilizado en la práctica, pero se considera importante para entender cómo funciona la comunicación en redes de computadoras y cómo se pueden estandarizar las diferentes funciones en las redes.

En resumen, la principal diferencia entre el modelo TCP/IP y el modelo OSI es que el modelo TCP/IP es más práctico y se enfoca en la implementación de redes, mientras que el modelo OSI es más teórico y se enfoca en estandarizar la comunicación entre sistemas informáticos.

1. **Entender la relación entre la capa de aplicación del modelo TCP/IP y las capas inferiores, especialmente la de transporte:**

La capa de aplicación del modelo TCP/IP es la capa más alta del modelo y se encarga de definir los protocolos y servicios que los programas utilizan para comunicarse a través de la red. Algunos ejemplos de protocolos de la capa de aplicación son HTTP, SMTP y FTP.

La capa de transporte, que se encuentra por debajo de la capa de aplicación, se encarga de la transferencia de datos entre los extremos de una conexión. Los protocolos más comunes en esta capa son TCP y UDP.

La capa de aplicación utiliza los servicios proporcionados por la capa de transporte para enviar y recibir datos. Por ejemplo, si un programa utiliza el protocolo HTTP para solicitar una página web, la capa de aplicación utilizará la capa de transporte para establecer una conexión y transferir los datos.

TCP es un protocolo de la capa de transporte que proporciona una conexión confiable y orientada a conexión entre dos extremos. TCP se encarga de dividir los datos en paquetes y reensamblarlos en el extremo receptor. Además, TCP incluye mecanismos de control de flujo y control de congestión para garantizar que los paquetes se entreguen de manera confiable y eficiente.

UDP es otro protocolo de la capa de transporte que proporciona una conexión no confiable y no orientada a conexión entre dos extremos. UDP es más rápido que TCP pero no incluye mecanismos de control de flujo y control de congestión.

En resumen, la capa de aplicación del modelo TCP/IP utiliza la capa de transporte para transferir datos entre dos extremos. La elección del protocolo de la capa de transporte depende de los requisitos específicos de la aplicación, como la confiabilidad y la velocidad de transferencia de datos.

1. **Entender el funcionamiento y servicios que ofrecen las capas de transporte y de red, además de las diferencias entre IPv4 e IPv6**

La capa de transporte y la capa de red son dos capas importantes del modelo TCP/IP. Cada una tiene funciones y servicios específicos que ofrecen a la red.

La capa de transporte se encarga de la transferencia de datos confiable y eficiente entre dos extremos. Esta capa se divide en dos protocolos: TCP y UDP.

TCP (Protocolo de Control de Transmisión) es un protocolo de conexión orientada que ofrece un flujo de datos confiable, garantizando que los datos lleguen a su destino en orden y sin errores. TCP divide los datos en segmentos y se encarga de la entrega de cada segmento a través de la red. TCP también utiliza mecanismos de control de congestión para evitar la congestión de la red y garantizar una transferencia de datos eficiente.

UDP (Protocolo de Datagrama de Usuario) es un protocolo sin conexión que se utiliza cuando se necesita una transferencia de datos rápida, pero no confiable. UDP no garantiza la entrega de los datos y no incluye mecanismos de control de congestión. UDP se utiliza comúnmente en aplicaciones como la transmisión de video y audio en tiempo real, donde la velocidad es más importante que la confiabilidad.

La capa de red es responsable de la transferencia de datos a través de la red desde el origen hasta el destino. La capa de red utiliza protocolos como el Protocolo de Internet (IP) para enrutar los datos a través de la red y encontrar el camino más eficiente desde el origen hasta el destino.

El protocolo IP divide los datos en paquetes y agrega información de encabezado que incluye la dirección IP del origen y el destino. Esta información se utiliza para enrutar el paquete a través de la red y garantizar que llegue al destino correcto. La capa de red también utiliza otros protocolos, como el Protocolo de Control de Internet (ICMP), que se utiliza para informar al origen sobre errores en la transferencia de datos y para supervisar la disponibilidad de la red.

En resumen, la capa de transporte se encarga de la transferencia confiable y eficiente de datos entre dos extremos, mientras que la capa de red se encarga de la transferencia de datos a través de la red desde el origen hasta el destino. Ambas capas son fundamentales para la comunicación en red y trabajan juntas para garantizar una transferencia de datos confiable y eficiente.

Diferencias entre IPv4 e IPv6:

IPv4 e IPv6 son dos versiones del Protocolo de Internet que se utilizan para direccionar y enrutar los paquetes de datos en una red de computadoras. A continuación, se presentan algunas diferencias importantes entre IPv4 e IPv6:

* Longitud de dirección: IPv4 utiliza direcciones de 32 bits, mientras que IPv6 utiliza direcciones de 128 bits. Esto significa que IPv6 puede soportar muchas más direcciones únicas que IPv4, lo que lo hace ideal para el creciente número de dispositivos conectados a internet.
* Formato de dirección: En IPv4, las direcciones se representan en formato decimal y están separadas por puntos, por ejemplo, 192.168.0.1. En IPv6, las direcciones se representan en formato hexadecimal y están separadas por dos puntos, por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
* Funcionamiento de direcciones privadas: En IPv4, las direcciones privadas se utilizan dentro de una red privada y no se enrutan en internet público. En IPv6, también existen direcciones privadas, pero se utilizan junto con direcciones globales únicas para permitir que los dispositivos se comuniquen de forma segura dentro de una red privada y con internet público.
* Autenticación y privacidad: IPv6 tiene características de autenticación y privacidad integradas, lo que lo hace más seguro que IPv4. Por ejemplo, IPv6 admite la autenticación de extremo a extremo para garantizar la integridad y autenticidad de los datos transmitidos.
* Uso de extensiones de cabecera: En IPv6, las extensiones de cabecera se utilizan para proporcionar información adicional sobre el paquete, como la calidad de servicio y la seguridad. En IPv4, esta información se incluye en la cabecera del paquete, lo que lo hace menos flexible y más propenso a errores.

En resumen, IPv6 es una versión más reciente del Protocolo de Internet que tiene varias ventajas sobre IPv4, incluyendo mayor cantidad de direcciones disponibles, características de seguridad integradas y mayor flexibilidad en la gestión de paquetes de datos. A medida que la cantidad de dispositivos conectados a internet sigue creciendo, IPv6 se está convirtiendo en una opción cada vez más popular para las redes modernas.

1. **Entender el funcionamiento de la capa de enlace y su interacción con la capa física**

La capa de enlace es la segunda capa del modelo OSI y del modelo TCP/IP. Es responsable de enviar y recibir datos en la red local o LAN (Local Area Network). La capa de enlace de datos se comunica directamente con la capa física de la red para enviar y recibir datos en la forma de tramas (frames).

La capa de enlace de datos agrega una cabecera de enlace de datos a los datos del nivel superior (la capa de red). Esta cabecera incluye información como la dirección física de origen y destino (MAC), el tamaño de la trama, información de control de errores y otras opciones.

La capa de enlace también es responsable de la detección de errores en la trama mediante técnicas como la comprobación de redundancia cíclica (CRC) y el reenvío de tramas en caso de errores.

La capa de enlace interactúa con la capa física de la red para enviar y recibir las tramas en la red. La capa física es responsable de la transmisión y recepción de bits a través del medio de transmisión físico, como cables de cobre, fibra óptica o señales inalámbricas.

La capa de enlace utiliza la capa física para enviar y recibir tramas. La capa física convierte las tramas en señales eléctricas, ópticas o inalámbricas que pueden viajar a través del medio de transmisión físico. La capa física también es responsable de la detección de errores en la transmisión de bits, como el ruido y la interferencia, y puede utilizar técnicas de corrección de errores para garantizar una transmisión precisa y confiable de los datos.

En resumen, la capa de enlace es responsable de la transmisión y recepción de tramas en la red local, mientras que la capa física es responsable de la transmisión y recepción de bits a través del medio de transmisión físico. La interacción entre la capa de enlace y la capa física es fundamental para garantizar una transmisión precisa y confiable de los datos en la red.

1. **Entender las características de las diferentes topologías de red, sus ventajas y desventajas. Algunas de las topologías a considerar: bus, estrella, malla y anillo**

Las topologías de red se refieren a la forma en que los dispositivos están conectados en una red. A continuación se describen las características de las topologías de red más comunes:

* Topología de red en bus: En una topología en bus, todos los dispositivos de la red están conectados a un solo cable de comunicación centralizado. Cada dispositivo se conecta directamente al cable de la red. La ventaja de esta topología es que es fácil de configurar y es económica. Sin embargo, si falla el cable principal, toda la red puede quedar inoperable.

Ventajas:

* + Es fácil de implementar y económica, ya que se necesita menos cableado.
  + Es adecuada para redes pequeñas con pocos dispositivos.
  + Es fácil de detectar fallos en los dispositivos.

Desventajas:

* + Si el cable principal falla, toda la red puede verse afectada.
  + El rendimiento de la red se reduce cuando hay muchos dispositivos conectados a ella.
  + No es adecuada para redes grandes y complejas.
* Topología de red en anillo: En una topología en anillo, los dispositivos se conectan en un círculo cerrado, donde cada dispositivo se conecta directamente al dispositivo adyacente. Los datos se transmiten en una sola dirección alrededor del anillo. La ventaja de esta topología es que proporciona un alto nivel de estabilidad y rendimiento. Sin embargo, si un dispositivo falla, toda la red puede verse afectada.

Ventajas:

* + Proporciona un alto rendimiento y estabilidad, ya que los datos se transmiten en una sola dirección alrededor del anillo.
  + Es adecuada para redes grandes con muchos dispositivos.
  + Es fácil de detectar fallos en los dispositivos.

Desventajas:

* + Si un dispositivo falla, toda la red puede verse afectada.
  + Es costosa de implementar y mantener.
  + No es adecuada para redes que requieren una gran cantidad de tráfico de datos en ambas direcciones.
* Topología de red en estrella: En una topología en estrella, todos los dispositivos de la red se conectan a un concentrador centralizado. Cada dispositivo se conecta directamente al concentrador. La ventaja de esta topología es que es fácil de configurar y permite la detección de fallos de manera rápida. Sin embargo, si falla el concentrador, toda la red puede quedar inoperable.

Ventajas:

* + Es fácil de configurar y permite la detección de fallos de manera rápida.
  + Es adecuada para redes grandes con muchos dispositivos.
  + Permite un alto rendimiento de la red.

Desventajas:

* Si el concentrador central falla, toda la red puede verse afectada.
* Es costosa de implementar y mantener.
* No es adecuada para redes que requieren una gran cantidad de tráfico de datos en ambas direcciones.
* Topología de red en malla: En una topología en malla, cada dispositivo de la red está conectado a varios otros dispositivos de la red. La ventaja de esta topología es que es muy resistente y tolerante a fallos, ya que si un dispositivo falla, otros dispositivos pueden tomar su lugar. Sin embargo, es una topología muy costosa y compleja.

Ventajas:

* Es muy resistente y tolerante a fallos, ya que si un dispositivo falla, otros dispositivos pueden tomar su lugar.
* Permite un alto rendimiento de la red.
* Es adecuada para redes grandes y complejas.

Desventajas:

* Es costosa y compleja de implementar.
* Requiere una gran cantidad de cableado.
* Puede generar congestión en la red debido a la gran cantidad de datos que se transmiten.
* Topología de red híbrida: Una topología híbrida combina dos o más topologías diferentes. Por ejemplo, una red en estrella que tenga varias redes en anillo conectadas a través del concentrador central. Esta topología ofrece una alta capacidad de redundancia y escalabilidad.

Ventajas:

* Ofrece una alta capacidad de redundancia y escalabilidad.
* Es adecuada para redes grandes y complejas.
* Permite un alto rendimiento de la red.

Desventajas:

* Es costosa y compleja de implementar.
* Requiere una gran cantidad de cableado.
* Puede generar congestión en la red debido a la gran cantidad de datos que se transmiten.

**Estándares de Redes:**

1. **Revisar los protocolos de ruteo más usados: RIP, OSPF, BGP, etc**

Los protocolos de ruteo son utilizados en redes de computadoras para permitir que los routers o encaminadores, intercambien información acerca de las redes que conocen y los caminos disponibles para llegar a ellas. Algunos de los protocolos de ruteo más usados son:

* Protocolo de Información de Enrutamiento de Puerta de Enlace Interior (Interior Gateway Routing Protocol - IGRP): es un protocolo de ruteo de distancia vectorial propietario de Cisco. Utiliza una métrica compuesta de ancho de banda, retraso, confiabilidad y carga para calcular la mejor ruta.
* Protocolo de Información de Enrutamiento de Estado de Enlace (Open Shortest Path First - OSPF): es un protocolo de ruteo de estado de enlace que calcula las rutas más cortas y confiables utilizando una métrica basada en el costo de los enlaces. Es ampliamente utilizado en redes grandes y complejas.
* Protocolo de Enrutamiento de Gateway de Borde (Border Gateway Protocol - BGP): es un protocolo de ruteo de vector de distancia utilizado para interconectar redes grandes y autónomas de Internet. BGP utiliza una política basada en rutas para seleccionar la mejor ruta y permite la propagación de información de ruteo entre diferentes dominios de enrutamiento.
* Protocolo de Enrutamiento de Información de Vector de Distancia (Routing Information Protocol - RIP): es un protocolo de ruteo de vector de distancia simple que utiliza el número de saltos para determinar la mejor ruta. Es utilizado en redes pequeñas y de baja complejidad.
* Protocolo de Enrutamiento de Estado de Enlace Mejorado (Enhanced Interior Gateway Routing Protocol - EIGRP): es un protocolo de ruteo propietario de Cisco que combina las características de los protocolos de vector de distancia y estado de enlace. EIGRP utiliza una métrica basada en el ancho de banda, la carga, la demora y la fiabilidad de los enlaces para calcular las mejores rutas.

Cabe destacar que existen muchos otros protocolos de ruteo, pero estos son algunos de los más utilizados en la actualidad.

1. **Revisar protocolos para transmisión de video y audio (videollamadas, video de alta definición y otros)**

Existen varios protocolos utilizados para la transmisión de video y audio en tiempo real, entre ellos se encuentran:

* Real-Time Transport Protocol (RTP): Es un protocolo utilizado para la transmisión de datos en tiempo real, incluyendo audio y video. Se encarga de dividir los datos en paquetes y enviarlos de manera eficiente a través de la red.
* Real-Time Control Protocol (RTCP): Es un protocolo complementario al RTP que se utiliza para la retroalimentación y el control de calidad de la transmisión. Proporciona información sobre la calidad de la transmisión y estadísticas de rendimiento.
* Streaming Protocolos: Son protocolos utilizados para la transmisión de video y audio a través de Internet. Algunos de los protocolos de streaming más comunes son Real-Time Messaging Protocol (RTMP), HTTP Live Streaming (HLS), Dynamic Adaptive Streaming over HTTP (DASH), y Smooth Streaming.
* H.264/MPEG-4 AVC: Es un estándar de codificación de video ampliamente utilizado para la compresión de video en tiempo real. Es utilizado en aplicaciones como videoconferencia, transmisión de televisión en vivo y streaming de video.
* Advanced Audio Coding (AAC): Es un formato de codificación de audio utilizado en la mayoría de los servicios de transmisión de música y video en línea. Ofrece una alta calidad de sonido con una tasa de bits más baja que otros formatos de audio.

Es importante mencionar que la elección del protocolo adecuado dependerá del tipo de aplicación, el ancho de banda disponible, la calidad deseada y otros factores específicos de cada caso.

1. **Entender el funcionamiento de WiFi (IEEE 802.11)**

El WiFi (Wireless Fidelity) es una tecnología de comunicación inalámbrica basada en el estándar IEEE 802.11, que permite la conexión a Internet y a redes de computadoras sin necesidad de cables.

El funcionamiento de WiFi se basa en la transmisión y recepción de ondas de radio de alta frecuencia entre dispositivos. Para ello, se utiliza un router inalámbrico que actúa como punto de acceso para conectar dispositivos inalámbricos a la red. El router emite una señal de radio que es detectada por los dispositivos inalámbricos dentro de su alcance.

La comunicación inalámbrica a través de WiFi utiliza el protocolo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) para evitar colisiones en la transmisión de datos. Este protocolo se encarga de detectar si el canal de comunicación está libre antes de transmitir los datos, y en caso de detectar que está ocupado, espera un tiempo aleatorio antes de volver a intentarlo para evitar colisiones.

El estándar IEEE 802.11 define varias variantes de WiFi, como 802.11a, 802.11b, 802.11g, 802.11n y 802.11ac, cada una con características específicas en cuanto a velocidad de transferencia de datos, alcance y frecuencia de operación.

En resumen, el funcionamiento de WiFi se basa en la transmisión y recepción de ondas de radio de alta frecuencia entre dispositivos inalámbricos y un punto de acceso, utilizando el protocolo CSMA/CA para evitar colisiones en la transmisión de datos

1. **Revisar protocolos que ofrecen calidad de servicio (QoS), por ejemplo: MPLS, DiffServ, CoS, DSCP, etc**

Existen varios protocolos que ofrecen calidad de servicio (QoS) en las redes de computadoras, algunos de los más importantes son:

* Differentiated Services (DiffServ): Es un protocolo utilizado para asignar diferentes niveles de prioridad a los paquetes de datos en función de su tipo de tráfico, con el fin de mejorar la calidad de servicio. DiffServ utiliza un campo en el encabezado de los paquetes para indicar su nivel de prioridad.
* Integrated Services (IntServ): Es un protocolo utilizado para garantizar la calidad de servicio de los flujos de datos específicos en la red. IntServ utiliza el protocolo RSVP (Resource Reservation Protocol) para solicitar recursos de red específicos, como ancho de banda y latencia, para flujos de datos específicos.
* Multi-Protocol Label Switching (MPLS): Es un protocolo utilizado para mejorar la calidad de servicio al crear caminos de red dedicados para flujos de datos específicos. MPLS utiliza etiquetas para identificar flujos de datos específicos y enrutarlos a través de la red.
* Quality of Service Protocol (QoS Protocol): Es un protocolo utilizado para garantizar la calidad de servicio en redes de voz y video en tiempo real. QoS Protocol utiliza diferentes mecanismos para controlar la tasa de transmisión, el retraso y la pérdida de paquetes.
* Class of Service (CoS) es un mecanismo utilizado para proporcionar calidad de servicio (QoS) en las redes de computadoras. CoS se utiliza comúnmente en redes Ethernet, y permite priorizar el tráfico de red para diferentes aplicaciones y servicios en función de su nivel de importancia. El protocolo CoS se basa en la asignación de etiquetas de prioridad a los paquetes de datos en el nivel de enlace de datos de la red. Estas etiquetas indican la importancia del tráfico de red y permiten que los dispositivos de red, como switches y routers, asignen la prioridad adecuada a los paquetes
* Differentiated Services Code Point (DSCP) es un mecanismo utilizado para proporcionar calidad de servicio (QoS) en las redes de computadoras. DSCP se utiliza para priorizar el tráfico de red y mejorar la calidad de servicio en redes de voz, video y otras aplicaciones sensibles al retraso o la pérdida de paquetes.

1. **Revisar protocolos desarrollados para ofrecer seguridad en la transmisión de los datos, como IPSec, SSL y otros**

Existen varios protocolos desarrollados para ofrecer seguridad en la transmisión de datos en redes de computadoras, entre ellos se encuentran:

* SSL/TLS: Secure Sockets Layer (SSL) y Transport Layer Security (TLS) son protocolos de cifrado y autenticación utilizados para garantizar la seguridad de las comunicaciones en la web. Estos protocolos utilizan certificados digitales para autenticar a los servidores y cifrado simétrico para garantizar la privacidad de la información.
* IPSec: Internet Protocol Security (IPSec) es un protocolo de seguridad utilizado para garantizar la seguridad de las comunicaciones en redes IP. IPSec proporciona autenticación, confidencialidad y protección contra ataques de denegación de servicio (DoS).
* SSH: Secure Shell (SSH) es un protocolo de red seguro utilizado para la gestión remota de dispositivos de red y servidores. SSH proporciona autenticación y cifrado para garantizar la seguridad de las comunicaciones.
* Kerberos: Kerberos es un protocolo de autenticación de red utilizado para proporcionar seguridad en la autenticación de usuarios y servicios. Kerberos utiliza cifrado de clave simétrica para garantizar la privacidad de las comunicaciones.
* VPN: Virtual Private Network (VPN) es una tecnología utilizada para crear una red privada virtual a través de una red pública como Internet. Las VPN utilizan cifrado para garantizar la privacidad de las comunicaciones y autenticación para garantizar la seguridad de las conexiones.
* WPA/WPA2: Wi-Fi Protected Access (WPA) y Wi-Fi Protected Access II (WPA2) son protocolos de seguridad utilizados en redes inalámbricas. Estos protocolos utilizan cifrado y autenticación para garantizar la seguridad de las comunicaciones inalámbricas.

En resumen, existen varios protocolos desarrollados para ofrecer seguridad en la transmisión de datos en redes de computadoras. Los protocolos mencionados anteriormente, como SSL/TLS, IPSec, SSH, Kerberos, VPN y WPA/WPA2, son algunos de los protocolos más utilizados y populares.