



“ENSAYO MODELOS Y DISPOSITIVOS DE COMUNICACIÓN UNIDAD 5”

**ENSAYO DE FUNDAMENTOS DE
TELECOMUNICACIONES**

INGENIERIA EN SISTEMAS COMPUTACIONALES

PRESENTA:

EDGAR CORTÉS RESÉNDIZ

RICARDO MURGUIA RIVAS

JIQUILPAN, MICHOACÁN, DICIEMBRE DE 2024

INTRODUCCION

La comunicación en redes es un proceso esencial que permite la interconexión de dispositivos y el intercambio de información de manera eficiente y segura. Este tema abarca conceptos fundamentales como el modelo OSI, que desglosa la comunicación en siete capas funcionales para estandarizar procesos y garantizar interoperabilidad entre sistemas. Además, se estudian los protocolos y estándares de comunicación que rigen el funcionamiento de las redes, la clasificación de dispositivos de red según su rol (activos, pasivos y de seguridad), y sus características funcionales específicas. También se consideran los estándares de interfaces físicas y lógicas, fundamentales para la conexión y configuración de redes, así como los mecanismos de detección y corrección de errores que aseguran la integridad de los datos transmitidos. Este enfoque integral proporciona una base sólida para comprender y optimizar las redes de comunicación modernas.

ENSAYO

La comunicación entre los distintos dispositivos se realiza mediante modelos de comunicación y responde a la semántica y sintaxis del mensaje que incorpora al propio mensaje información preestablecida. Dado que esta información destinada a su procesamiento se denomina metainformación. Los mensajes de cada transmisión deben tener una estructura o sintaxis con el fin de que tanto el emisor como el receptor los interpreten correctamente. El modelo de comunicación ha de incluir la información necesaria para el control de los errores de transmisión, para lo que han de incluirse controles de errores y retransmisiones. En torno a, se introdujo un modelo de red, en el que el concepto de red se dividía en siete capas, generalmente conocidas como capas. El modelo no es un protocolo específico, sino un conjunto de reglas para el diseño de protocolos. Tales capas siguen recogiendo una parte de la funcionalidad de diversas capas de protocolo original. Existe un protocolo estándar para cada capa del modelo, y también tiene dos protocolos superiores, autenticación y enrutamiento, aparte de los siete. El modelo de referencia define siete capas, cada una de las cuales representa un agrupamiento de características o funciones específicas, que proporciona un punto de articulación entre los niveles superior e inferior y está relacionada con las dos capas adyacentes del modelo.

Control de Tráfico y Tecnología de Apoyo: La regulación de tráfico es la encargada de gestionar todos los dispositivos que están dentro de la capa física: regulación de colisiones, topologías de redes, topologías de broadcast y maestro/esclavo, ubicación de equipos en la red, etc. El estándar que predomina, el Ethernet, está regulado por el estudio del IEEE 802.3, exceptuando el estándar de redes Wi-Fi regulado por el IEEE 802.11. Para el modelado de redes en el mundo, son dos las organizaciones interesadas: ISO y ITU-T. Le toca a ITU-T, gobernando el que usemos la capa de protocolos más usada en Internet (y en esencia el mundo): TCP/IP. Como ya se mencionó anteriormente, en mesh routers no se basa todo en

su capa física; la inmensa mayoría basa su conectividad directa con otros AP con el estándar RSTP.

En cuanto a las regulaciones frecuentes en las formas alámbricas de las redes del modelo OSI, se hace uso del AU que tiene que ver con la identificación de dos vértices directamente conectados, que son EE. UU., Canadá y un pequeño país en Colombia en la región de los Andes, a un bloque del viejo continente, España. En cuanto a las radiocomunicaciones, es similar a nivel mundial compartir la utilización bajo los estándares de la IEEE particular, con relación a modelos como el 802.11u, que hace referencia a redes que no están manejadas internamente con la función de DHCP; por ello, en lugares cerrados, la reglamentación es particular por país. Para los dispositivos de comunicación, cuando existe la posibilidad de realizar un envío de información a un elemento externo, enlaces de comunicación, direccionamiento o dependencia de la longitud de los mensajes, se hace uso de los protocolos de comunicación.

En las comunicaciones de redes, todos los dispositivos de red pueden enviar datos de forma similar, pero se necesita amortizar correctamente en qué momento y con qué dispositivo de atención, esta puede ser de diferente modo. Se deben amortizar nuevas capacidades en los diferentes equipos o dispositivos de conmutación existentes: Repasando las diferentes formas de clasificar los dispositivos de red, la definición más extendida es basar esta clasificación en la compatibilidad de cada uno de ellos con las diferentes capas del modelo. De este modo encontramos dos tipos de dispositivos: los de dos capas o switches, que pueden conmutar paquetes a nivel de enlace, y los de tres capas o routers que pueden hacer lo mismo a nivel de red. Existen otros dispositivos polivalentes que pueden ser conmutadores de nivel de enlace o ruteadores de nivel de red indistintamente o al mismo tiempo. Entre estos dispositivos encontramos los módem-router y los PC-servidores con más de una tarjeta de red. Entre las funciones más destacadas de networking destacamos el encaminamiento. La conectividad, la distribución, el switching y un largo etcétera que se nos antoja imprescindible en un mundo de datos. ¿Qué sería de la comunicación de datos sin un router, un switch, un hub, un módem o un caché?

El mecanismo de detección y corrección de errores se emplea para garantizar que los datos transmitidos entre dispositivos no se encuentren corruptos. Este proceso implica el cálculo de una suma de verificación a partir de los bytes que componen los datos. Los bytes se suman de manera que, si dos bytes ya procesados resultan en un valor idéntico al de otro par de bytes, se logra una comunicación sin pérdida de información. Al enviar los datos, los dispositivos incluyen una suma de verificación, que actúa como un método rápido y efectivo para verificar la integridad de los datos transmitidos. Un mecanismo ampliamente utilizado para la detección de errores es el protocolo de suma de verificación en Internet, que utiliza códigos de redundancia cíclicos (CRC) calculados mediante un polinomio de XOR, dividiendo los datos en secciones junto a una cantidad específica de bits. Los datos se fragmentan utilizando un generador polinómico fijo, acompañados de una serie de bits de verificación que permiten detectar y corregir posibles errores.

CONCLUSION

En conclusión, la detección y corrección de errores son aspectos fundamentales en la transmisión de datos a través de dispositivos como smartphones y otros smart devices, especialmente en el contexto del modelo OSI. Este modelo, que establece capas para la comunicación de datos, es esencial para entender cómo estos dispositivos manejan la información y cómo los errores pueden ser identificados y corregidos a lo largo del proceso de transmisión.

Además, la detección y corrección de errores son elementos clave en la transmisión de datos, especialmente en el marco del modelo OSI, que descompone la comunicación en capas que facilitan la identificación y rectificación de fallos. Esta capacidad de detectar errores, desde el nivel físico hasta el de aplicación, es esencial para asegurar la integridad de la información intercambiada entre dispositivos de transmisión como smartphones y otros dispositivos inteligentes. Además, los cortafuegos desempeñan un papel vital en este panorama, protegiendo los datos de accesos no autorizados y, al mismo tiempo, contribuyendo a la detección de actividades sospechosas que podrían indicar errores o brechas de seguridad. La evolución de la tecnología ha ampliado el acceso a la información, lo que incrementa la posibilidad de errores en la transmisión, haciendo que la implementación de sistemas de corrección sea más crítica que nunca. Por lo tanto, es crucial que los usuarios mantengan la conciencia sobre la importancia de estas medidas y el papel que juegan tanto en su seguridad personal como en la integridad de la información que manejan. En definitiva, mientras que los avances tecnológicos han transformado nuestra manera de comunicarnos y acceder a información, es nuestra responsabilidad asegurarnos de que esta evolución no comprometa la confiabilidad y seguridad de los datos que fluye a través de estos dispositivos.