INSTITUTO SUPERIOR TECNOLÓGICO QUITO

Formamos tu PROPÓSITO DE VIDA

Guía general de redes y comunicación DE DATOS

ISBN: 978-9942-7328-8-0

INSTITUTO SUPERIOR TECNOLÓGICO QUITO - DESDE 1984 - SABER HACER Bien

INSTITUTO SUPERIOR TECNOLÓGICO QUITO
Excelencia en Educación Superior

GUÍA GENERAL DE REDES Y COMUNICACIÓN DE DATOS

AUTOR:

XIMENA MARCILLO

PRIMERA EDICIÓN

AÑO: 2024

TRABAJO EN EDICIÓN:

DOXA EDITION

DIRECCIÓN EDITORIAL: DIEGO JAVIER BASTIDAS LOGROÑO

EDITOR EXTERNO: DAVID FABIAN CEVALLOS SALAS

ISBN:978-9942-7328-8-0

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

SOBRE EL AUTOR

Ximena Marcillo es una ingeniera de sistemas graduada con distinción de la Universidad Politécnica Salesiana en el año 2017. Su carrera ha estado marcada por una destacada trayectoria en proyectos relevantes en el campo de la ingeniería de sistemas. Su experiencia y habilidades técnicas le han permitido destacarse en el ámbito de la informática y la tecnología.

Como profesional comprometida con el desarrollo académico, Ximena Marcillo ha dejado una huella significativa en el campo de la educación. Publicó un libro sobre análisis de sistemas de información, consolidando así su experiencia y conocimiento en un recurso valioso para estudiantes y profesionales en este campo.

Su contribución al ámbito educativo no se limita a la publicación. Desde el año 2018 hasta el 2022, se desempeñó como docente en el Instituto Tecnológico Quito, específicamente en la carrera de Desarrollo de Software. Durante este tiempo, compartió su experiencia práctica y conocimientos teóricos con sus estudiantes, contribuyendo al desarrollo de futuros profesionales en el campo de la tecnología.

En reconocimiento a su dedicación y habilidades de liderazgo, en el año 2023, Ximena Marcillo fue asignada como la coordinadora de la carrera de Desarrollo de Software en el mismo instituto. Además, asumió el rol de directora de la Escuela de Tics (Tecnologías de la Información y Comunicación), demostrando así su capacidad para liderar a nivel institucional y para influir positivamente en el crecimiento y la dirección de programas académicos.

Con una combinación de experiencia en el sector privado, contribuciones significativas a la educación y roles de liderazgo en el ámbito académico, Ximena Marcillo se ha establecido como una figura integral en el campo de la ingeniería de sistemas y el desarrollo de software. Su perfil diversificado, que abarca tanto la práctica como la enseñanza, refleja un compromiso continuo con la excelencia en su campo y un deseo de influir positivamente en las futuras generaciones de profesionales en tecnología.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

ÍNDICE

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

ÍNDICE DE FIGURAS

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

GUÍA GENERAL DE REDES Y COMUNICACIÓN DE DATOS

1. DESCRIPCIÓN DE LA ASIGNATURA

La asignatura de Redes y Comunicación de Datos ofrece una visión completa de los principios esenciales, protocolos y tecnologías involucradas en las redes informáticas y la transferencia de información en entornos digitales. A lo largo del curso, los estudiantes explorarán una variedad de temas cruciales:

1. **Fundamentos de Redes:** Se proporcionará una introducción detallada a los conceptos básicos de las redes informáticas, incluyendo la estructura de la red, modelos de referencia como el modelo OSI, y los componentes de hardware y software esenciales para su funcionamiento.

2. **Protocolos de Comunicación:** Se examinarán en profundidad los protocolos de comunicación más relevantes, como TCP/IP, UDP, HTTP y otros. Los estudiantes comprenderán cómo estos protocolos facilitan el intercambio de datos entre dispositivos conectados en una red.

3. **Enrutamiento y Conmutación:** Se explorarán los principios subyacentes al enrutamiento y la conmutación de datos, cubriendo tanto enrutamiento estático como dinámico, así como los diferentes métodos de conmutación de paquetes y circuitos.

4. **Tecnologías Emergentes:** Se presentarán y discutirán las últimas tendencias y tecnologías emergentes en el ámbito de las redes informáticas, como la computación en la nube, el Internet de las cosas (IoT) y las redes definidas por software (SDN).

A lo largo del curso, se enfatizará la aplicación práctica de los conceptos teóricos a través de estudios de caso, laboratorios prácticos y proyectos de implementación. Los estudiantes desarrollarán habilidades prácticas en la configuración y gestión de redes, así como en la resolución de problemas de conectividad y seguridad. Al concluir la asignatura, estarán

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

preparados para diseñar, implementar y administrar redes informáticas efectivas y seguras en diversos entornos digitales.

2. BIBLIOGRAFÍA

2.1. Básica

- Tanenbaum, A. S., & Wetherall, D. J. (2011). Redes de computadoras. Pearson Educación.

Este texto es un recurso fundamental para comprender los conceptos básicos de las redes de computadoras. Proporciona una visión completa de los principios, protocolos y tecnologías esenciales en el campo de las redes. La claridad en la presentación y la profundidad de los temas abordados hacen de este libro una herramienta imprescindible para el desarrollo de la asignatura.

- Forouzan, B. A. (2016). Comunicaciones y redes de computadores. McGraw-Hill Interamericana.

Este libro ofrece una cobertura exhaustiva de las comunicaciones y redes de computadoras. Su enfoque didáctico y práctico facilita la comprensión de conceptos complejos, mientras que los ejemplos y ejercicios proporcionan una sólida base para el aprendizaje. Es una referencia esencial para los estudiantes que desean adquirir conocimientos profundos en el área de redes y comunicaciones.

2.2. Complementaria

- Kurose, J. F., & Ross, K. W. (2017). Redes de computadoras: Un enfoque descendente. Pearson Educación.

Este libro ofrece una perspectiva única al abordar las redes de computadoras desde un enfoque descendente. Proporciona una comprensión profunda de los principios fundamentales y las aplicaciones prácticas de las redes, lo que lo convierte en una valiosa adición a la bibliografía de la asignatura.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- Peterson, L. L., & Davie, B. S. (2017). Redes de computadoras: una perspectiva de sistemas. Elsevier.

Este texto presenta una visión de las redes de computadoras desde una perspectiva de sistemas, lo que permite a los estudiantes comprender cómo las redes se integran en sistemas más grandes. Su enfoque holístico y su cobertura amplia lo convierten en una referencia valiosa para aquellos que desean comprender las redes en un contexto más amplio.

- Stallings, W. (2019). Comunicaciones y redes de computadoras. Pearson Educación.

Este libro proporciona una visión detallada de las comunicaciones y redes de computadoras, cubriendo una amplia gama de temas, desde los fundamentos hasta las tecnologías emergentes. Su enfoque práctico y su atención a las últimas tendencias lo hacen especialmente útil como recurso complementario para los estudiantes interesados en explorar temas avanzados en el campo.

3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS

Propone sistemas de redes de datos, valorando los procesos de la empresa, que permitan optimizar el flujo de información, tendientes a incrementar la productividad y competitividad.

4. OBJETIVO GENERAL

Desarrollar en los estudiantes un conocimiento integral sobre los principios, protocolos y tecnologías fundamentales en el ámbito de las redes y comunicación de datos, mediante la exploración teórica y práctica de conceptos relacionados con la configuración, administración y seguridad de redes, así como el análisis de casos de estudio y la realización de actividades prácticas, con el propósito de capacitarlos para diseñar, implementar y gestionar redes informáticas efectivas y seguras, así como para resolver problemas de conectividad y seguridad en entornos tecnológicos diversos, al mismo tiempo que se fomenta el desarrollo de habilidades cognitivas, procedimentales y actitudinales que les permitan enfrentar los desafíos actuales y futuros en el campo de las tecnologías de la información y la comunicación.

5. FORMACIÓN CIUDADANA, VALORES Y HABILIDADES BLANDAS

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

6. NORMAS DE CLASE

En relación a las normas de clase, es importante destacar que la evaluación de los componentes de gestión académica se compone de tres notas sumativas, cada una con una puntuación máxima de 6.60/6.60, así como un proyecto práctico, como evaluación formativa que se valora con 3.40/3.40, lo que da un total de 10/10 para la calificación del módulo. Los parciales se califican en una escala de hasta 6.60 puntos, representando cada uno el 2.22 de la calificación total de 6.6 puntos. Para presentarse al proyecto final, el estudiante debe haber obtenido al menos 4.50 puntos sumando las tres primeras notas. En caso de no alcanzar este mínimo en el proyecto, se otorga una oportunidad de recuperación dentro de las 48 horas laborables siguientes, según el calendario académico oficial. La nota mínima acumulada requerida para aprobar la asignatura es 7/10, y es esencial mantener al menos un 70% de asistencia a las clases. Los docentes deben informar a los estudiantes sobre sus notas individuales antes de registrarlas en el sistema, y se espera que los alumnos confirmen su aceptación y conformidad con estas calificaciones. Además, los docentes deben entregar un reporte de notas y asistencia a través del SGA y notificado a la coordinación de carrera y registrar las calificaciones en el sistema en un plazo máximo de 5 días posteriores a la recepción del proyecto final

7. SISTEMA DE EVALUACIÓN

- PRIMER PARCIAL 22%
- SEGUNDO PARCIAL 22%
- TERCER PARCIAL 22%
- PROYECTO FINAL 34%

8. UNIDADES

1. Fundamentos de redes y comunicación de datos
2. Diseño y configuración de redes de datos
3. Gestión de redes y administración de recursos

UNIDAD 1: FUNDAMENTOS DE REDES Y COMUNICACIÓN DE DATOS

Temas y Subtemas

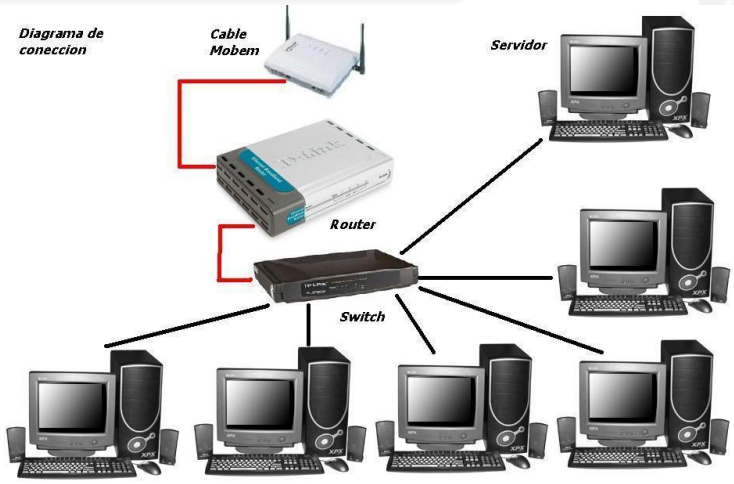
(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

1. Introducción A Las Redes De Computadoras

1.1. Definición De Redes De Computadoras

Una red informática, una red de comunicaciones de datos o una red de computadoras es la interconexión de distinto número de sistemas informáticos a través de una serie de dispositivos de telecomunicaciones y un medio físico (alámbrico o inalámbrico). (Etece, 2023)

Ilustración 1:
Redes de computadoras



Nota: en la ilustración se puede observar el diagrama de conexión de una red de computadoras con sus diferentes componentes.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

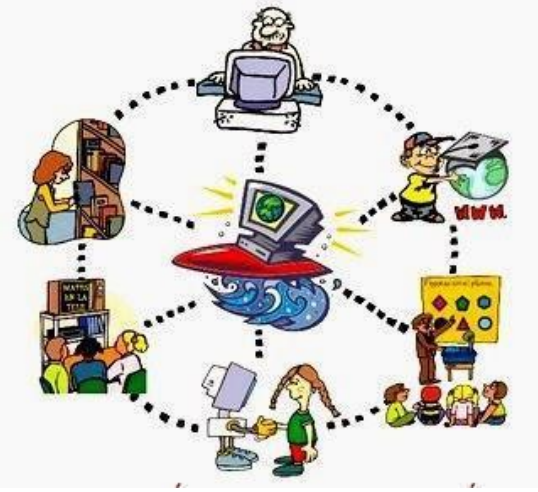
Las redes informáticas hacen referencia a la conexión entre equipos de computación con el objetivo de intercambiar recursos y simplificar la comunicación entre estos. En su forma más elemental, una red de computadoras se compone de dos o más dispositivos interconectados, tales como ordenadores, servidores, impresoras, dispositivos de almacenaje, entre otros, capaces de intercambiar información y servicios. Estas redes pueden fluctuar en su tamaño y complejidad, desde conexiones locales en una vivienda u oficina hasta redes mundiales que cubren amplias áreas geográficas.

1.2. Importancia De Las Redes De Datos En El Mundo Real

Las tecnologías emergentes se han incorporado en nuestro entorno como un recurso que, sin lugar a duda, nos proporciona grandes comodidades y simplificaciones para mejorar nuestra labor, en todas las áreas donde el ser humano se desarrolla, especialmente en los contextos estudiantiles, laborales institucionales y empresas.

El ordenador es un componente esencial de la humanidad, se podría afirmar literalmente que es el mejor amigo del ser humano debido a su uso diario y a su uso personal.

Ilustración 2:
Importancia de las redes de datos



Nota: en la ilustración se puede observar porque motivo es importante las redes de computadoras y el uso en las que se aplica.

Los computadores han tenido mucha importancia para el hombre desde el momento en que se crearon y se ha venido mejorando su funcionamiento; todo esto ha sido uno de los grandes inventos que ha forjado al hombre en su afán por mejorar las condiciones de vida y ejecutar con más facilidad y simpleza los diferentes problemas o dificultades en su vida diaria.

Las computadoras funcionan y hacen su oficio como tal; entrada y salida de información, pero dentro de este funcionamiento homogéneo hay una necesidad de comunicarse o transmitir

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

esa información hacia otro dispositivo para que se pueda llamar informática, lo anteriormente mencionado se puede hacer por memorias portátiles, CDs, DVDs etc., pero no es lo suficientemente eficaz para la rapidez con la que se necesita difundirse esa información.

En la actualidad se conocen muchas formas de que un PC se comunique con otro, por ejemplo: Bluetooth, Redes LAN, Internet, Etc.

Bluetooth es el más lento de todos ya que solo permite interactuar solamente archivo por archivo. El Internet es la red más importante de todas porque nos permite conectar miles de ordenadores a nivel mundial, donde la información corre a millas por segundo dentro de un cubo que cubre todo el planeta, y la información vuela.
Miraremos la total importancia de las redes de computadores dese distintos puntos de vista en este ensayo:

1.2.1. Para Ordenadores

Los ordenadores requieren enviar y recibir información, que será útil para actualizar sus datos.

Para actualizar sus programas y optimizar su desempeño, algo que no puede realizar mientras se encuentra "solamente" cuando no tiene comunicación con alguien.

1.2.2. Para las personas

Enviar información a otros lugares donde no puede acceder personalmente.

Recibir información de personas o lugares que no puede ver directamente.

Acortar distancias, familiares lejos que no pueden estar cerca de nosotros, las redes de computadoras nos dan la oportunidad de verlos y hablar con ellos. (Julio, 2015)

1.3. Tipos De Redes De Datos

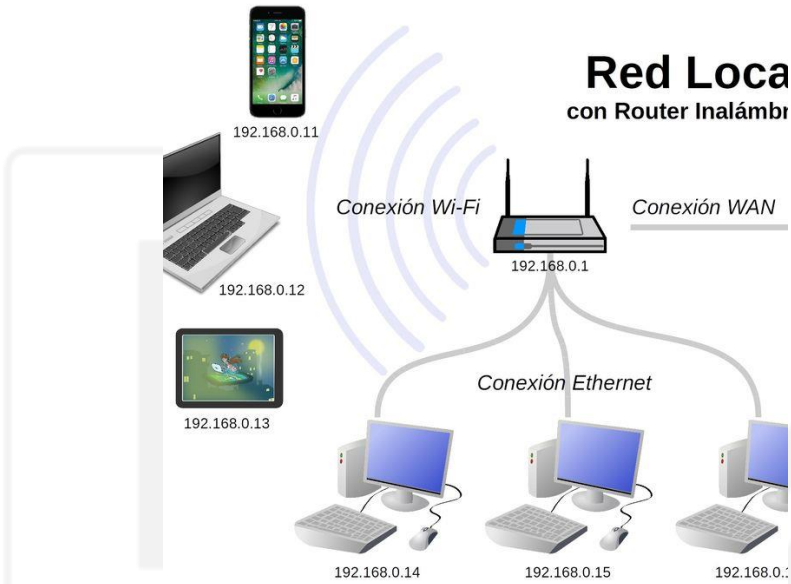
Las redes de datos se categorizan en diversas clases de acuerdo a su amplitud geográfica y su estructura de enlace. Estas clases de redes ofrecen una infraestructura de comunicación que facilita el intercambio eficaz de datos entre aparatos interconectados. Algunas de las redes de datos más habituales incluyen:

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

1.3.1. Red De Área Local (LAN)

Una LAN es una red de datos que se extiende sobre un área geográfica limitada, como un edificio, una oficina o un campus universitario. Estas redes suelen ser propiedad de una sola organización y están diseñadas para proporcionar comunicación rápida y eficiente entre dispositivos dentro de la misma ubicación física.

Ilustración 3:
Red de área local



Nota: en la ilustración se puede observar una conexión alámbrica e inalámbrica de una red LAN

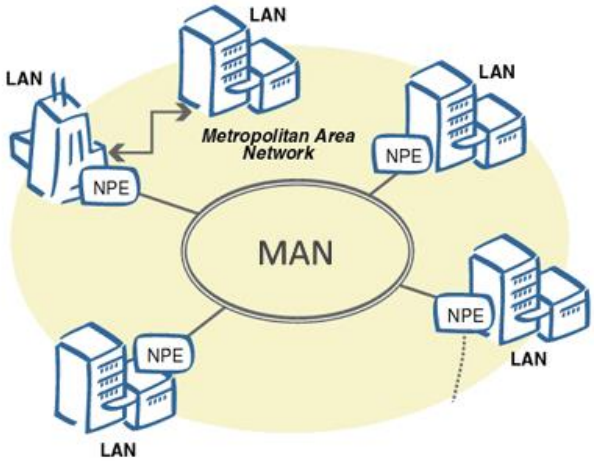
Las redes LAN casi siempre utilizan Ethernet, WiFi o ambas para conectar los dispositivos de la red. Ethernet es un protocolo de conexión física a la red que requiere el uso de cables Ethernet. WiFi es un protocolo para conectarse a una red mediante ondas de radio.

Una variedad de dispositivos puede conectarse a las LAN, incluyendo servidores, ordenadores de escritorio, portátiles, impresoras, dispositivos IoT e incluso videoconsolas. En las oficinas, las LAN suelen utilizarse para proporcionar acceso compartido a los empleados internos a las impresoras o servidores conectados. (CLOUDFLARE, 2024)

1.3.2. Red De Área Metropolitana (MAN)

Una MAN es una red de datos que abarca un área geográfica más grande que una LAN, como una ciudad o una región metropolitana. Estas redes suelen ser propiedad de múltiples organizaciones y pueden ser utilizadas para interconectar múltiples sitios dentro de una misma área geográfica.

Ilustración 4:
Red de área metropolitana



Nota: en la ilustración se puede observar como varias redes de área local (LAN) forma una red de área metropolitana (MAN).

Las redes MAN se caracterizan por los siguientes aspectos clave:

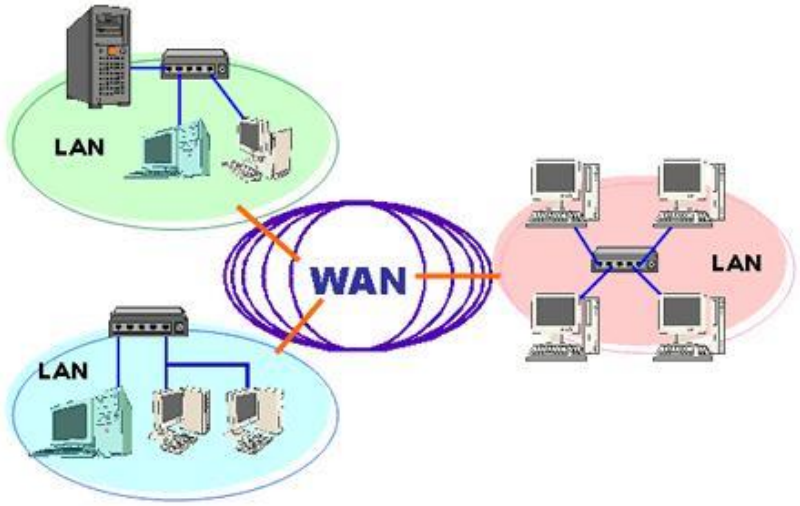
- **Área geográfica:** Las redes MAN abarcan un área geográfica extensa, generalmente dentro de una ciudad o una región metropolitana.
- **Velocidad y ancho de banda:** Las redes MAN ofrecen velocidades de transmisión de datos más altas y un mayor ancho de banda en comparación con las redes LAN.
- **Conexiones cableadas e inalámbricas:** Las redes MAN pueden utilizar tanto conexiones de cableado, como fibra óptica o cables de par trenzado, como tecnologías inalámbricas, como Wi-Fi o redes celulares.
- **Conexiones públicas y privadas:** Las redes MAN pueden utilizar conexiones públicas, como Internet, o conexiones privadas, como líneas alquiladas o circuitos dedicados (Sistemas en redes informáticas, 2024)

1.3.3. Red Área Amplia (WAN)

Una WAN es una red de información que cubre una amplia zona geográfica, tal como un país o incluso múltiples áreas geográficas. Estas redes generalmente pertenecen a los proveedores de servicios de telecomunicaciones y se emplean para vincular dispositivos situados en distintos lugares geográficos.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Ilustración 5:
Red área amplia (WAN)



Nota: en la ilustración se puede observar el funcionamiento y como se conforma una red de área amplia (WAN)

Las empresas disponen de recursos que se ejecutan en diferentes centros de datos locales, sucursales y nubes virtuales privadas (VPC). Para establecer la conexión entre estos recursos, las empresas utilizan múltiples conexiones de red y servicios de Internet. Dado que las empresas no pueden construir su propia infraestructura de red a través de múltiples fronteras geográficas, suelen alquilarla a un proveedor de servicios externo.

Estos son algunos de los tipos de conexiones más comunes:

Líneas alquiladas: Una línea alquilada es una conexión de red directa que se puede alquilar a un proveedor de red grande, como un proveedor de servicios de Internet (ISP). Puede conectar dos puntos de conexión LAN entre sí. Las líneas alquiladas no son necesariamente líneas físicas. Es posible que sean conexiones virtuales que los proveedores de servicios implementan sobre otra infraestructura de red.

Túnel: El túnel es una forma de cifrar los paquetes de datos a medida que se desplazan por la Internet pública. Con la técnica del túnel, se utiliza una conexión a Internet para acceder a los servidores de la empresa en otro país. Pero se envían como paquetes encapsulados, con lo que se forma una red privada virtual (VPN) propia.

Conmutación de etiquetas multiprotocolo: La conmutación de etiquetas multiprotocolo (MPLS) es una técnica que dirige el tráfico de datos en función de etiquetas predeterminadas. Intenta dirigir el tráfico de datos críticos a través de rutas de red más cortas o más rápidas, lo que mejora el rendimiento de la red. Funciona entre las capas 2 y 3 de la

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

interconexión de sistemas abiertos (OSI). Se puede utilizar para crear una red unificada en la infraestructura existente, como IPv6, retransmisión de tramas, ATM o ethernet. Se pueden utilizar líneas alquiladas de MPLS o MPLS con VPN para crear redes eficaces y seguras.

WAN definida por software: La red de área amplia definida por software (SD-WAN) es la evolución posterior de la tecnología MPLS. Abstrae las funciones del MPLS a una capa de software. Dado que la WAN definida por software funciona a través de conexiones de Internet de banda ancha de uso común, normalmente puede reducir los costos de la red y proporcionar una mayor flexibilidad que una conexión fija.

MPLS frente a la WAN definida por software: MPLS puede ralentizar la integración de la nube porque dirige el tráfico a través de las sedes corporativas, que actúan como puntos de estrangulamiento centrales. Por otra parte, la WAN definida por software es compatible con la nube y se integra mucho mejor con la infraestructura moderna en la nube. La WAN definida por software también es rentable. Puede funcionar a través de MPLS de modo que sea posible utilizar el ancho de banda de forma más eficiente en las costosas líneas de alquiler de MPLS. (aws, 2024)

1.3.4. Red De Área Personal (PAN)

Una PAN es una red de datos de tamaño reducido que se utiliza para conectar dispositivos personales, como teléfonos inteligentes, tabletas, computadoras portátiles y dispositivos domésticos inteligentes. Estas redes suelen ser inalámbricas y están diseñadas para proporcionar comunicación entre dispositivos cercanos.

Ilustración 6:
Red de área personal

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Nota: en la ilustración se puede observar todos los dispositivos personales conectados entre sí, de esta forma se realiza una red de área personal.

Las redes de área personal (PAN) son redes inalámbricas, se basan en tecnologías como Bluetooth, Wi-Fi Direct o Near Field Communication (NFC). En una red PAN, los dispositivos se comunican entre sí utilizando una señal de radio de corto alcance. Además:

- La comunicación puede ser bidireccional, lo que significa que los dispositivos pueden enviar y recibir datos entre sí.
- La conexión se establece mediante un proceso de emparejamiento, que implica la autenticación y la autorización de los dispositivos. Una vez emparejados, pueden compartir datos entre sí.
- Las redes PAN pueden utilizarse para una amplia variedad de aplicaciones, como la sincronización de dispositivos, la transferencia de archivos, la transmisión de audio y video, la impresión y el control de dispositivos domésticos inteligentes, etc.

1.4. Componentes Básicos De Una Red De Datos

1.4.1. Nodos

Los nodos son los dispositivos individuales que forman parte de una red de computadoras. Estos pueden incluir computadoras personales, servidores, impresoras, enrutadores, switches, puntos de acceso inalámbrico y otros dispositivos conectados a la red.

Ilustración 7:
Nodos de red

Nota: en la ilustración se puede observar un nodo de red o un punto de red.

Un nodo de red es un aparato que vincula distintas redes entre ellas, o que une dos o más computadoras dentro de una misma infraestructura. Se desempeña como un enlace entre diversas redes y facilita el intercambio de datos e información.

Se emplean para diferentes propósitos, tales como encaminar paquetes de datos de una computadora a otra, compartir recursos entre distintos lugares, facilitar el acceso a la red, entre otros.

Los nodos de red funcionan creando una conexión entre dos o más redes. Esto puede hacerse mediante diversos métodos, como cables, señales inalámbricas y fibras ópticas. Una vez

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

conectados, los nodos intercambian datos entre sí para facilitar la comunicación entre distintos ordenadores o redes. (DONGEE, 23)

1.4.2. Enlaces

Los enlaces son los medios físicos o lógicos que conectan los nodos de una red entre sí para permitir la comunicación. Estos enlaces pueden ser cables de cobre, cables de fibra óptica, conexiones inalámbricas, o incluso conexiones satelitales en el caso de redes de área amplia (WAN).

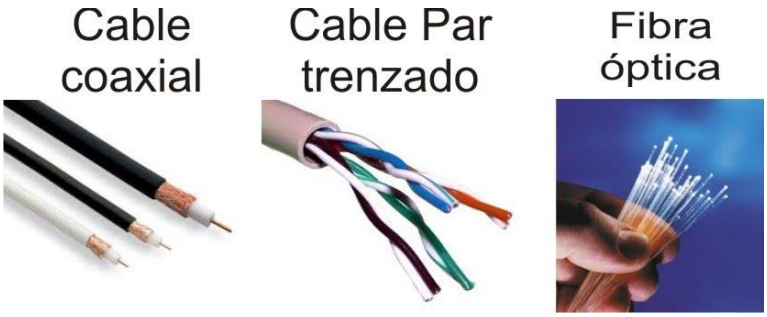
Ilustración 8:
Enlace de datos

Nota: en la ilustración se puede observar los enlaces de datos de un switch

1.4.3. Medios De Transmisión

Los canales de transmisión son las vías físicas mediante las cuales se envían los datos entre los nodos de la red. Estos pueden abarcar cables de cobre (tales como los de Ethernet), cables de fibra óptica, o el espectro electromagnético empleado en conexiones sin cables.

Ilustración 9:
Medios de transmisión



Nota: en la ilustración se puede observar los tipos de medios de transmisión guiados.

Tipos:

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

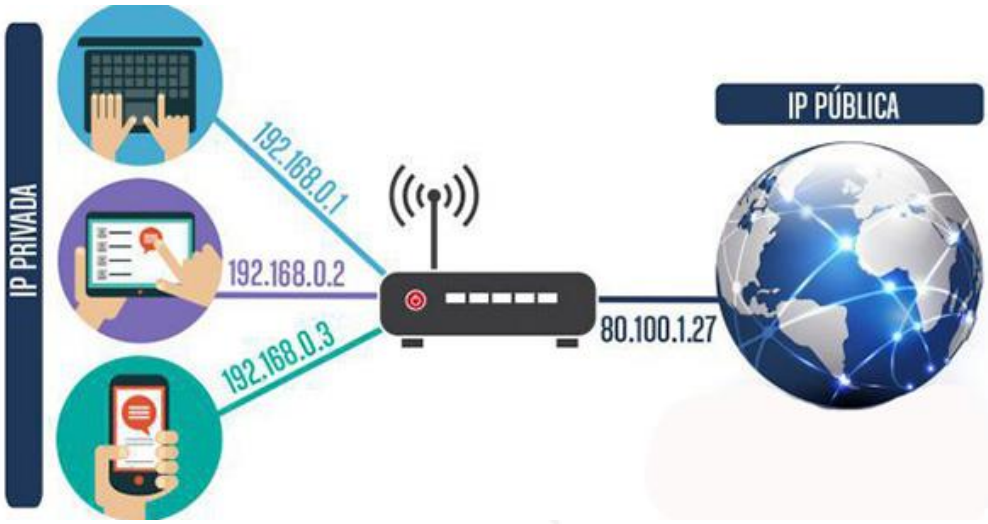
- **Pares trenzados:** Este consiste en dos alambres de cobre aislados, en general de 1mm de espesor. Los alambres se entrelazan en forma helicoidal, como en una molécula de DNA. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor. Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre; en muchos casos pueden obtenerse transmisiones de varios megabits, en distancias de pocos kilómetros. Debido a su adecuado comportamiento y bajo costo, los pares trenzados se utilizan ampliamente y es probable que se presencia permanezca por muchos años.
- **Cable coaxial:** El cable coaxial consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante. Este material aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector. (Colegio Ártica, 2024)
- **Fibra Óptica:** La fibra óptica es un cable conformado por un núcleo de vidrio cubierto por material refractivo y una protección exterior, esta fibra transporta datos entre sus extremos por medio de pulsaciones de luz, es rápida y segura para transmisión de datos con baja atenuación, permite un gran ancho de banda y cubre largas distancias. (Todo para los informáticos, 2024)

1.4.4. Direcciones IP

Las direcciones IP son identificadores numéricos asignados a cada dispositivo conectado a una red. Estas direcciones permiten que los nodos de la red se comuniquen entre sí identificándose mutuamente de manera única en la red.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Ilustración 10:
Direcciones de IP



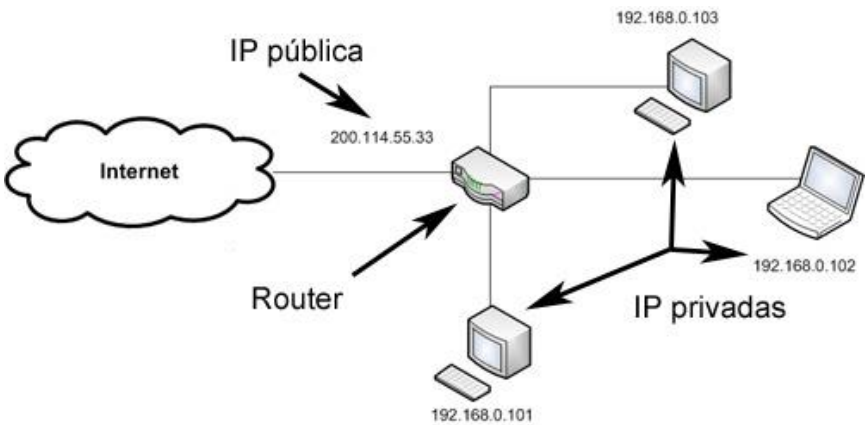
Nota: en la ilustración se puede observar las diferencias en la IP pública y la IP privada

IP Pública

Es imprescindible que nuestro ordenador, tablet o teléfono móvil se identifique de alguna forma para que podamos obtener la información requerida de manera adecuada. Por lo tanto, cada computadora que se conecta a Internet lo identifica con un número singular e irrepetible. Esa cantidad es lo que llamamos dirección IP.

Una dirección IP pública se denomina de tal modo cuando es visible en todo Internet. Cuando accedemos a Internet desde nuestro ordenador obtenemos una dirección IP público suministrada por nuestro proveedor de conexión a Internet. Esa dirección IP es nuestra dirección IP de salida a Internet en ese momento. (HOSTINET, 2024)

Ilustración 11:
IP Pública

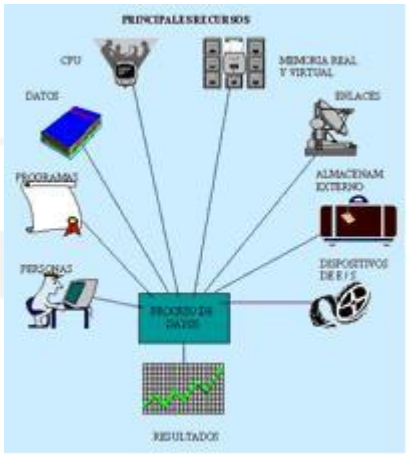


Nota: en la ilustración se puede observar como la IP pública ingresa a una red privada.

1.4.5. Software De Red

Además del hardware tangible, el software de red también desempeña un rol crucial en el funcionamiento de una red de ordenadores. Esto puede abarcar sistemas operativos de red, aplicaciones para la administración de redes, programas de servidor, y otros programas que simplifican la gestión y utilización de la red.

Ilustración 12:
Software de Red



Nota: en la ilustración se puede observar las distintas herramientas de software para realizar configuraciones de redes de datos.

1.5. Historia Y Evolución De Las Redes

Las redes de computadoras tienen sus raíces en la década de 1960, cuando se comenzaron a explorar conceptos de comunicación de datos entre múltiples sistemas informáticos. Uno de los primeros desarrollos significativos fue ARPANET, una red experimental creada por la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos (ARPA) en 1969. ARPANET sentó las bases para la creación de Internet, siendo el primer ejemplo de una red de área amplia (WAN) basada en el protocolo TCP/IP.

En la década de 1970, ARPANET creció y se expandió a otras instituciones académicas y de investigación, convirtiéndose en una red interconectada de computadoras. Durante este período, se desarrollaron los primeros estándares de comunicación, como el modelo de referencia OSI (Open Systems Interconnection) y TCP/IP, que establecieron reglas comunes para la interconexión de sistemas informáticos.

En los años siguientes, la popularidad y la importancia de las redes de computadoras continuaron creciendo con la aparición de redes locales (LAN) y redes de área metropolitana

(MAN). La adopción generalizada de computadoras personales en la década de 1980 impulsó aún más el desarrollo de redes, con la aparición de tecnologías como Ethernet y el acceso a Internet para usuarios finales.

A lo largo de las décadas siguientes, las redes de computadoras han seguido evolucionando con el desarrollo de nuevas tecnologías, como la computación en la nube, la virtualización, las redes inalámbricas y el Internet de las cosas (IoT). Hoy en día, las redes de computadoras son fundamentales en todos los aspectos de la vida moderna, desde la comunicación y el comercio hasta la educación y el entretenimiento.

Ilustración 13:
Evolución de las redes de datos

Nota: en la ilustración se puede observar la evolución de las redes de datos a través de los años.

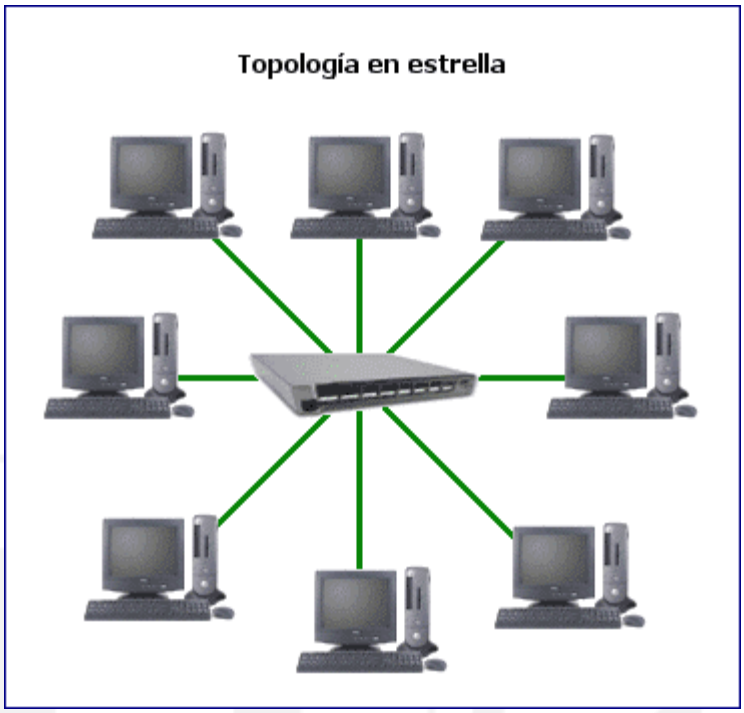
2. Tipos De Topologías De Red

Las estructuras de red de datos hacen referencia a la organización física o lógica de los equipos y conexiones en una red de ordenadores. Existen diversas topologías habituales que se emplean en contextos de redes, cada una con sus particularidades y usos particulares. Estos son algunos de los tipos de topologías de red más habituales:

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

2.1. Topología Estrella

Ilustración 14:
Topología de estrella



Nota: en la ilustración se puede observar el esquema de una topología de estrella

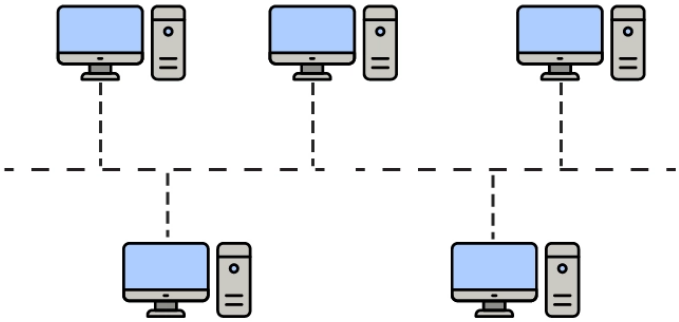
Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

La topología estrella es una de las topologías más populares de un LAN (Local Área Network). Es implementada conectando cada computadora a un Hub central. El Hub puede ser Activo, Pasivo o Inteligente. Un hub activo es solo un punto de conexión y no requiere energía eléctrica. Un Hub activo (el más común) es actualmente un repetidor con múltiples puertos; impulsa la señal antes de pasarla a la siguiente computadora. Un Hub Inteligente es un hub activo, pero con capacidad de diagnóstico, puede detectar errores y corregirlos. (Redes Inalambricas y cableadas , 2024)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Topología De Bus

Ilustración 15:
Topología de bus

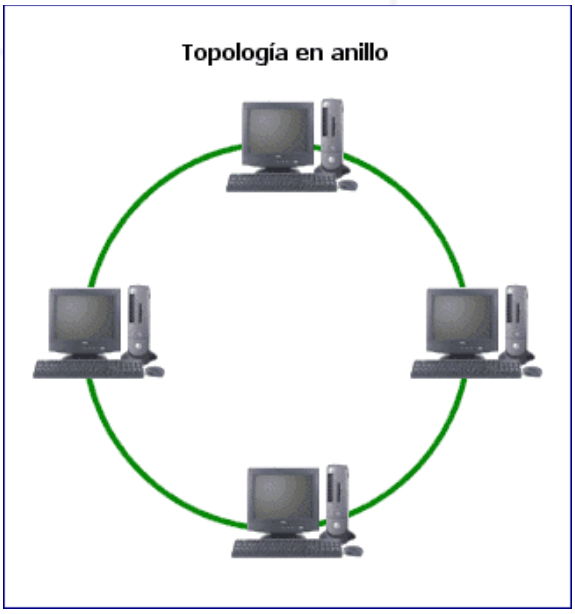


Nota: en la ilustración se puede observar el esquema de una red de topología de bus

La topología en bus tiene una particularidad y es que es este tipo de red los dispositivos están enlazados a un canal o nodo principal. Que entrelaza a todos los dispositivos que harán uso de la red informática. Esta misma particularidad de la red hace que sea una red utilizada en donde los dispositivos a conectar sean pocos, comúnmente se ven en empresas pequeñas y en el uso doméstico. (Topologías de red, 2024)

2.2. Topología De Anillo

Ilustración 16:
Topología anillo



Nota: en la ilustración se puede observar el esquema de una red de datos en forma de anillo.

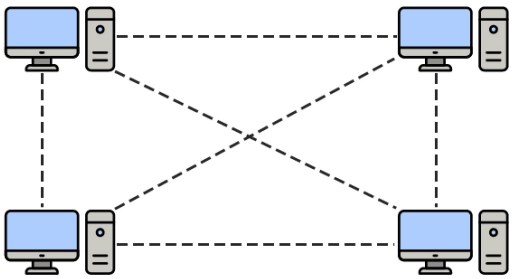
(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

En esta estructura, las computadoras se encargan de potenciar la señal, transmitiéndola a la siguiente computadora para prevenir que dicha señal sea debilitada. La avería de un ordenador puede causar un impacto significativo en el funcionamiento de la red.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. (Topologías físicas de red, 2024)

2.3. Topología De Malla

Ilustración 17:
Topología de malla



Nota: en la ilustración se puede observar el esquema de una red de datos utilizando la topología malla

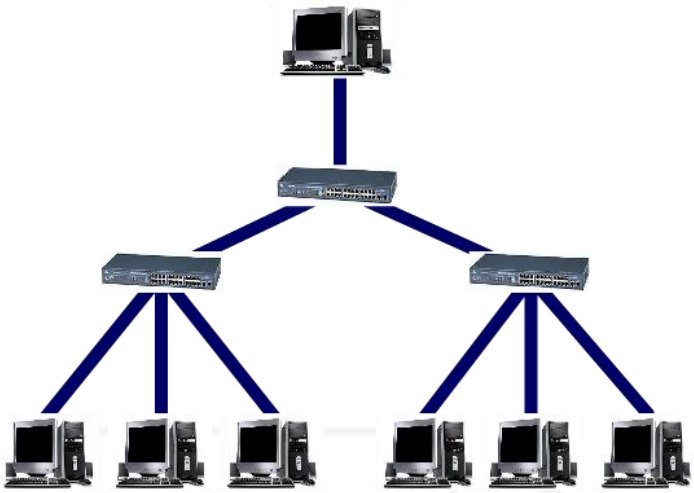
En una topología de malla, cada dispositivo está conectado a otro dispositivo a través de un canal particular. En Topología Mesh, los protocolos utilizados son AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

- Supongamos que el número N de dispositivos está conectado entre sí en una topología de malla, el número total de puertos que requiere cada dispositivo es N-1. En la Figura 1, hay 5 dispositivos conectados entre sí, por lo que el número total de puertos requeridos por cada dispositivo es 4. El número total de puertos requeridos=N*(N-1).
- Supongamos que una cantidad N de dispositivos están conectados entre sí en una topología de malla, entonces la cantidad total de enlaces dedicados necesarios para conectarlos es N C 2, es decir, N (N-1) /2. En la Figura 1, hay 5 dispositivos conectados entre sí, por lo que el número total de enlaces necesarios es 5*4/2 = 10. (AXXES, 2022)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Topología Árbol

Ilustración 18:
Topología de árbol

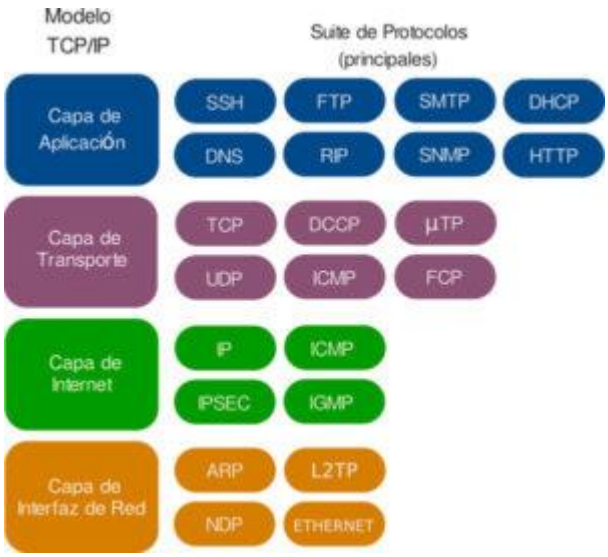


Nota: en la ilustración se puede observar la estructura de una red de datos usada con la topología de árbol

La topología de árbol combina elementos de la topología de estrella y la topología de bus. En esta topología, los dispositivos están organizados en una estructura jerárquica de niveles, con un dispositivo central (como un switch) en la parte superior del árbol. Cada nivel se conecta al nivel superior, creando una estructura de árbol invertida. Esto proporciona una mayor escalabilidad que la topología de estrella, pero puede ser vulnerable a fallos en el dispositivo central. (WIKIDOT, 2024)

3. Protocolos De Red De Datos

Ilustración 19:
Protocolos de red de datos



(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

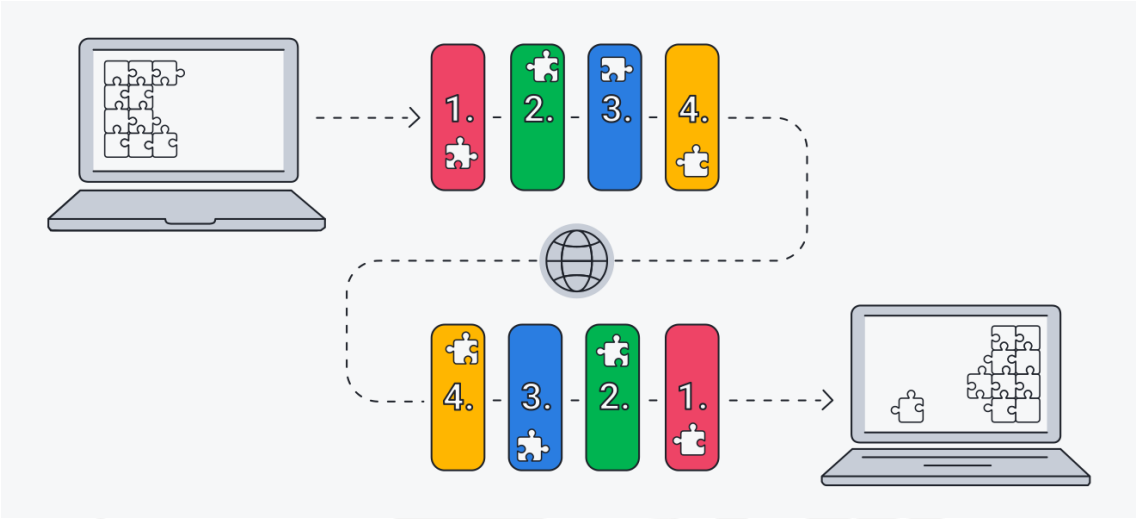
Nota: en la ilustración se puede observar los diferentes protocolos de red, principalmente del modelo TCP/IP.

4. Protocolos De Comunicación

Los protocolos de comunicación son conjuntos de reglas y estándares que permiten que los dispositivos de una red se comuniquen entre sí de manera eficiente y confiable. Aquí tienes una lista de algunos protocolos de comunicación comunes:

Protocolo TCP/IP

Ilustración 20:
Protocolo TCP/IP



Nota: en la ilustración se puede observar la utilización del protocolo TCP/I´P para la comunicación entre computadoras.

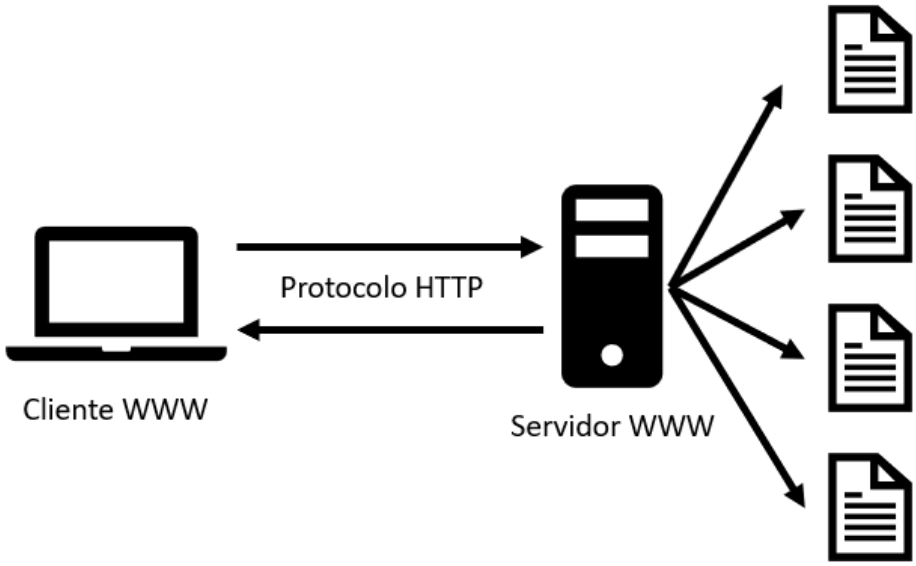
TCP/IP es un protocolo de enlace de datos que se usa en Internet para que los ordenadores y otros dispositivos envíen y reciban datos. TCP/IP son las siglas en inglés de Transmission Control Protocol/Internet Protocol (protocolo de control de transmisión/protocolo de Internet). Posibilita que los dispositivos conectados a Internet se comuniquen entre sí en varias redes.

TCP/IP determina cómo los ordenadores transfieren datos de un dispositivo a otro. Estos datos deben ser exactos para que el receptor obtenga la misma información enviada por el emisor. (AVG, 2024)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Protocolo HTTP

***Ilustración 21**:*
Protocolo HTTP



Nota: en la ilustración se observa el funcionamiento del protocolo HTTP en el modelo cliente – servidor

HTTP es el protocolo utilizado para la transferencia de información en la World Wide Web. Se utiliza para solicitar y enviar páginas web y otros recursos a través de Internet.

Este protocolo es conocido como cliente-servidor. Los mensajes enviados por el cliente a través de un navegador se denominan solicitudes o peticiones y los mensajes de solución enviados por el servidor se llaman respuestas.

HTTP utiliza diversos verbos en mayúscula, al principio de cada solicitud, para enviar y recibir información del navegador. Además, señalan al servidor lo que deben hacer con los datos que ha identificado en la URL. Los siguientes verbos, también denominados métodos HTTP, son los más habituales:

- **GET:** Es el verbo o método más habitual para solicitar datos, aunque no para modificarlos.
- **POST:** Envía datos a un servidor para su actualización.
- **PUT:** Remite datos al servidor para crear un recurso y también para actualizarlo.
- **HEAD:** Es igual que GET, pero no incluye el cuerpo de respuesta, y sirve para describir las acciones para las que se solicita su realización.
- **DELETE:** Borra los recursos que identifica la URL de la petición. Por lo tanto, elimina la información entregada. (Compara Hosting , 2024)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

4.1. Protocolo IPv4

El protocolo entre redes en su versión 4. Es un mecanismo de transmisión de paquetes no orientado a conexión y por tanto no fiable. No permite la corrección de errores debido a que no realiza seguimiento ni comprobación de paquetes. (López)

Ilustración 22:
PDU de IPv4

Nota: en la ilustración se puede observar la unidad de datos de protocolo de IPv4

- *Versión:* IPv4 la versión de este protocolo es la 4 es decir 0100 en binario.
- *Longitud de Cabecera:* Múltiplos de 4 bytes
- *Tipo de servicio:* Este campo se establecen la prioridad, las prestaciones, la fiabilidad y el retardo del envío del paquete.
- *Long Total:* La longitud total del paquete varía entre bytes y 65535 bytes.
- *ID:* Este campo se utiliza para identificar el número de fragmento del paquete dentro de una transmisión de datos.
- *Tiempo de vida:* TTL representa un contador que se va decrementado conforme el paquete va trasegando por los Routers. Son estos son los encargados de decrementar el mismo, si este valor llega a cero el paquete se descarta.
- *Protocolo:* identifica el protocolo de nivel superior que ha sido encapsulado en el paquete: TCP, UDP, ICMP.
- *Dirección Origen:* Tiene una longitud de 4 bytes e identifica el equipo que realiza la transmisión de datos.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- *Dirección de Destino:* Tienen una longitud de 4 bytes e identifica el equipo que recibe la transmisión de datos.

Autoevaluación 1

Instrucciones: Responde las siguientes preguntas seleccionando la opción correcta.

1. ¿Cuál de las siguientes opciones describe mejor una red de computadoras?
    a) Un solo ordenador conectado a Internet.
    b) Varios ordenadores conectados entre sí para compartir recursos.
    c) Un dispositivo de almacenamiento en la nube.
2. ¿Cuál es la función principal de la capa de red en el modelo OSI?
    a) Proporcionar la interfaz entre la red y el usuario.
    b) Controlar la transmisión de datos entre dispositivos.
    c) Determinar la mejor ruta para el envío de datos.
3. ¿Cuál de las siguientes topologías de red permite la comunicación directa entre cualquier par de dispositivos?
    a. Bus.
    b. Estrella.
    c. Malla.
4. ¿Cuál de los siguientes dispositivos de red opera en la capa de enlace de datos y utiliza direcciones MAC para la conmutación?
    a) Router.
    b) Switch.
    c) Hub.
5. ¿Cuál de los siguientes protocolos se utiliza para la transferencia de archivos en una red?
    a) HTTP.
    b) FTP.
    c) TCP.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

6. ¿Qué tipo de medio de transmisión es más inmune a las interferencias electromagnéticas?

    a) Cable de par trenzado.

    b) Cable coaxial.

    c) Fibra óptica.

7. ¿Cuál es la principal diferencia entre TCP y UDP?

    a) TCP garantiza la entrega de los paquetes, mientras que UDP no.

    b) TCP es más rápido que UDP.

    c) TCP se utiliza para la transmisión de voz y vídeo, mientras que UDP se utiliza para transferir archivos.

8. ¿Qué tipo de topología de red es más susceptible a fallos en un solo punto?

    a) Estrella.

    b) Anillo.

    c) Bus.

9. ¿Qué función desempeña un router en una red de computadoras?

    a) Conectar diferentes redes entre sí.

    b) Conectar varios dispositivos en una red local.

    c) Amplificar la señal de red para mejorar la conectividad.

10. ¿Cuál es la función del protocolo ARP (Address Resolution Protocol)?

    a. Convertir direcciones IP en direcciones MAC.

    b. Convertir nombres de dominio en direcciones IP.

    c. Convertir direcciones MAC en direcciones IP.

11. ¿Cuál es la función principal de los protocolos de comunicación en una red de computadoras?

    a) Gestionar el hardware de red.

    b) Establecer reglas para la comunicación entre dispositivos.

    c) Realizar copias de seguridad de los datos.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

12. ¿Cuál es la diferencia clave entre el modelo OSI y el modelo TCP/IP?

    a) El modelo OSI tiene más capas que el modelo TCP/IP.

    b) El modelo TCP/IP es más utilizado en la práctica.

    c) El modelo OSI fue desarrollado antes que el modelo TCP/IP.

13. ¿Cuál de las siguientes capas del modelo OSI se encarga de determinar la mejor ruta para la transmisión de datos?

    a) Capa de aplicación.

    b) Capa de red.

    c) Capa de transporte.

14. ¿Qué protocolo de aplicación se utiliza para transferir páginas web en la World Wide Web?

    a) FTP.

    b) SMTP.

    c) HTTP.

15. ¿Cuál es la función principal del protocolo TCP?

    a) Garantizar la entrega de los paquetes de datos.

    b) Proporcionar un método para la transferencia de archivos.

    c) Gestionar la resolución de direcciones IP a direcciones MAC.

16. ¿Cuál de los siguientes protocolos es responsable de asignar direcciones IP de forma dinámica a los dispositivos en una red?

    a) DHCP.

    b) DNS.

    c) SNMP.

17. ¿Qué protocolo se utiliza para diagnosticar problemas en la conectividad de red, como la falta de respuesta de un host?

    a) ICMP.

    b) TCP.

    c) ARP.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

18. ¿Cuál es la función principal del protocolo ARP?

    a) Convertir direcciones IP en direcciones MAC.

    b) Convertir nombres de dominio en direcciones IP.

    c) Determinar la mejor ruta para la transmisión de datos.

19. ¿Qué tipo de protocolo es el UDP?

    a) Protocolo de transporte.

    b) Protocolo de aplicación.

    c) Protocolo de Internet.

20. ¿Qué estándar define las reglas para la transmisión de datos en una red Ethernet?

    a) IEEE 802.11.

    b) IEEE 802.3.

    c) IEEE 802.1.

Respuestas:

1. B - Varios ordenadores conectados entre sí para compartir recursos.
2. C - Determinar la mejor ruta para el envío de datos.
3. C - Malla.
4. B - Switch.
5. B - FTP.
6. C - Fibra óptica.
7. A - TCP garantiza la entrega de los paquetes, mientras que UDP no.
8. A - Estrella.
9. A - Conectar diferentes redes entre sí.
10. A - Convertir direcciones IP en direcciones MAC.
11. Respuesta: b) Establecer reglas para la comunicación entre dispositivos.
12. Respuesta: c) El modelo OSI fue desarrollado antes que el modelo TCP/IP.
13. Respuesta: b) Capa de red.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

14. Respuesta: c) HTTP.
15. Respuesta: a) Garantizar la entrega de los paquetes de datos.
16. Respuesta: a) DHCP.
17. Respuesta: a) ICMP.
18. Respuesta: a) Convertir direcciones IP en direcciones MAC.
19. Respuesta: a) Protocolo de transporte.
20. Respuesta: b) IEEE 802.3.

Resumen de la Unidad 1

La unidad "Fundamentos de Redes" ofrece un análisis detallado del universo de las redes informáticas. Se examinan los principios esenciales, procedimientos y tecnologías esenciales que respaldan el funcionamiento de las redes de computación. En esta unidad, los alumnos desarrollan una sólida comprensión de variados asuntos, tales como tipos de redes, modelos de referencia (tales como el modelo OSI y TCP/IP), estructuras de red, dispositivos de red, medios de transmisión y protocolos de comunicación. Además, se analizan las funciones y características de los principales dispositivos de red, como switches y routers, así como la importancia de la seguridad en las redes. Al concluir la unidad, los alumnos estarán listos para entender y enfrentar asuntos más sofisticados en el campo de las redes y la comunicación de datos.

UNIDAD 2: DISEÑO Y CONFIGURACIÓN DE REDES

Temas y Subtemas

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Protocolos de comunicación**
- **Modelo OSI**
- **Modelo TCP/IP**
- Subnetting

5. Protocolos de comunicación

Un protocolo de comunicación es un conjunto de reglas y normas que permiten la transferencia de datos entre dispositivos en una red de manera eficiente y fiable. Estos protocolos definen cómo se deben estructurar los datos, cómo se deben enviar y recibir, y cómo se deben manejar los errores y la pérdida de información. Sin los protocolos de comunicación, la interoperabilidad entre diferentes dispositivos y sistemas sería prácticamente imposible.

5.1. Importancia de los Protocolos de Comunicación

- *Interoperabilidad:* Los protocolos permiten que dispositivos de diferentes fabricantes y con diferentes sistemas operativos puedan comunicarse entre sí sin problemas.
- *Eficiencia:* Definen métodos eficientes para la transmisión de datos, optimizando el uso del ancho de banda y reduciendo la latencia.
- *Fiabilidad:* Implementan mecanismos para la detección y corrección de errores, asegurando que los datos se transmitan con precisión.
- *Seguridad:* Muchos protocolos incluyen medidas de seguridad, como el cifrado, para proteger los datos durante la transmisión.

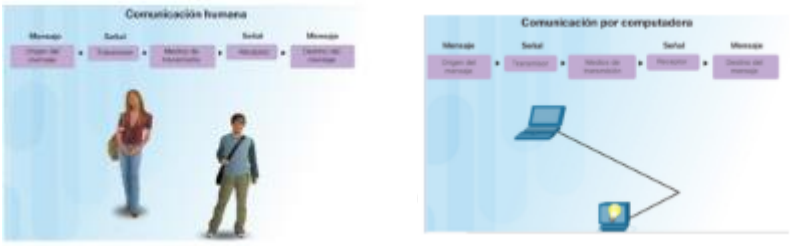
(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

5.2. Aspectos básicos de la comunicación

todos los métodos de comunicación tienen tres elementos en común:

- Origen o emisor
- Destino o receptor
- Canal o medio

Los protocolos o las reglas rigen los métodos de comunicación (CCNA, 2024)



5.3. Formato y encapsulamiento del mensaje

- Existe un formato acordado para las letras y las letras de direccionamiento que es necesario para la correcta entrega.
- Colocar la carta en el sobre dirigido se llama encapsulamiento.
- Cada mensaje de computadora se encapsula en un formato específico, llamado trama, antes de enviarse a través de la red.
- Un marco actúa como sobre ya que proporciona la dirección de origen y de destino

Opciones de entrega del mensaje

Mensaje de unidifusión

Ilustración 23:
Mensaje de unidifusión

Nota: en la ilustración se puede observar cómo funciona el mensaje de unidifusión que se caracteriza por la entrega de uno a uno.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Mensaje de multidifusión

Ilustración 24:
Mensaje multidifusión

Nota: en la ilustración se puede observar el mensaje de multidifusión que se caracteriza por la entrega de uno a muchos

Mensaje de difusión

Ilustración 25:
Mensaje de difusión

Nota: en la ilustración se puede observar el funcionamiento del mensaje de difusión que se caracteriza por la entrega de uno a todos

5.4. Función De Un Protocolo De Comunicación

La función principal de un protocolo de red es establecer la semántica y la coordinación del intercambio de información.

¿Esto qué significa? Que las computadoras en red deben actuar según los parámetros y los criterios contemplados en el protocolo para que puedan comunicarse entre ellas y para recuperar datos que, por alguna razón, no hayan llegado a destino. (adaptive, 2024)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

6. Modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos) es un marco conceptual que estandariza las funciones de una red de telecomunicaciones o un sistema de computación sin importar su estructura subyacente y tecnología. Fue desarrollado por la Organización Internacional de Normalización (ISO) en 1984 y proporciona una guía para diseñar y entender las relaciones entre diferentes protocolos y cómo interactúan. El modelo OSI consta de siete capas, cada una de las cuales realiza una función específica y se comunica con las capas adyacentes.

Al ser un modelo normativo, el Modelo OSI es realmente un constructo teórico, sin correlato directo en el mundo de lo tangible. No es más que un intento de normar las diversas y variadas voces tecnológicas del mundo, dado que existen numerosos fabricantes, compañías y tecnologías en el mundo de las telecomunicaciones.

Este modelo se ha refinado con el tiempo y hoy ofrece siete capas distintas con las que definir las distintas fases que atraviesa la información en su viaje de un dispositivo electrónico a otro conectado en la red. No importa la ubicación geográfica del usuario ni el tipo de tecnología que utilice, todos los medios de interconexión global, como Internet, emplean este tipo de protocolos unificados.

6.1. Funcionamiento Del Modelo OSI

El funcionamiento del Modelo OSI depende directamente de sus siete capas, en las que descompone el complicado proceso de la comunicación digital. Al compartimentarlo, asigna a cada capa funciones muy específicas, dentro de una estructura jerárquica fija.

Así, cada protocolo de comunicación emplea estas capas en su totalidad o sólo algunas de ellas, pero al obedecer este conjunto de reglas, garantiza que la comunicación entre las redes sea eficaz y sobre todo que se de en los mismos términos. (Concepto, 2024)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

***Ilustración 26**:*
Modelo OSI

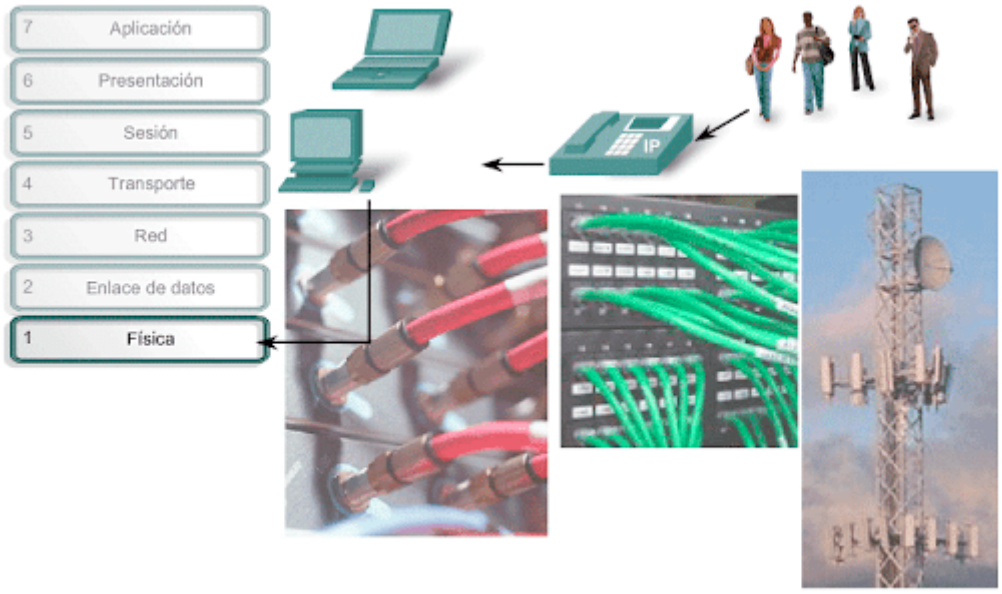
nota: en la ilustración se puede observar las siete capas del modelo OSI, con el funcionamiento de cada una de ellas.

6.2. CAPA 1: FÍSICA

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física. Si desea recordar la Capa 1 en la menor cantidad de palabras posible, piense en señales y medios.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Ilustración 27:
Capa Física

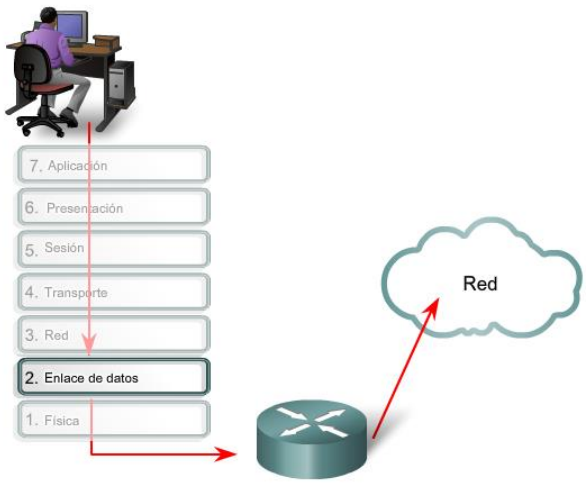


La capa Física interconecta nuestras redes de datos.

6.3. Capa 2: Enlace De Datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio.

Ilustración 28:
Capa De Enlace De Datos



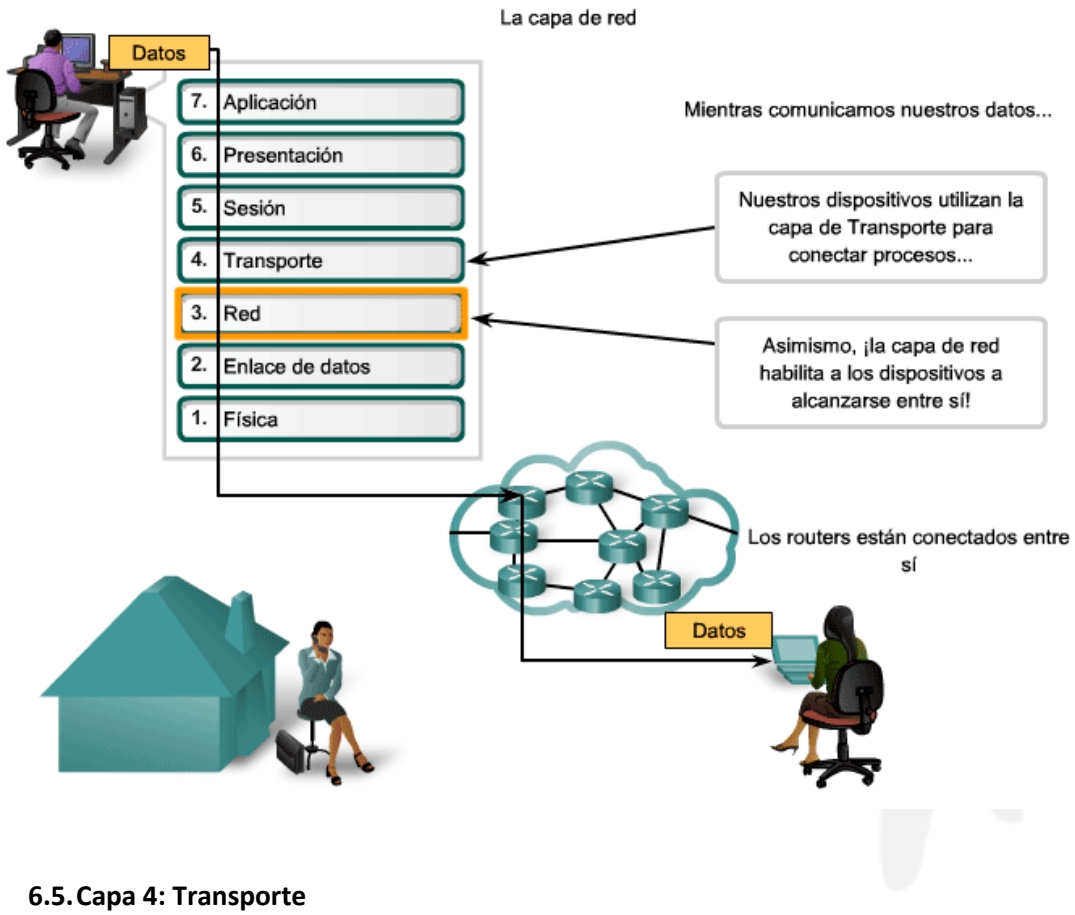
La capa de enlace de datos prepara datos de red para la red física.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

6.4. Capa 3: Red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Si desea recordar la Capa 3 en la menor cantidad de palabras posible, piense en selección de ruta, direccionamiento y enrutamiento.

Ilustración 29:
Capa De Red

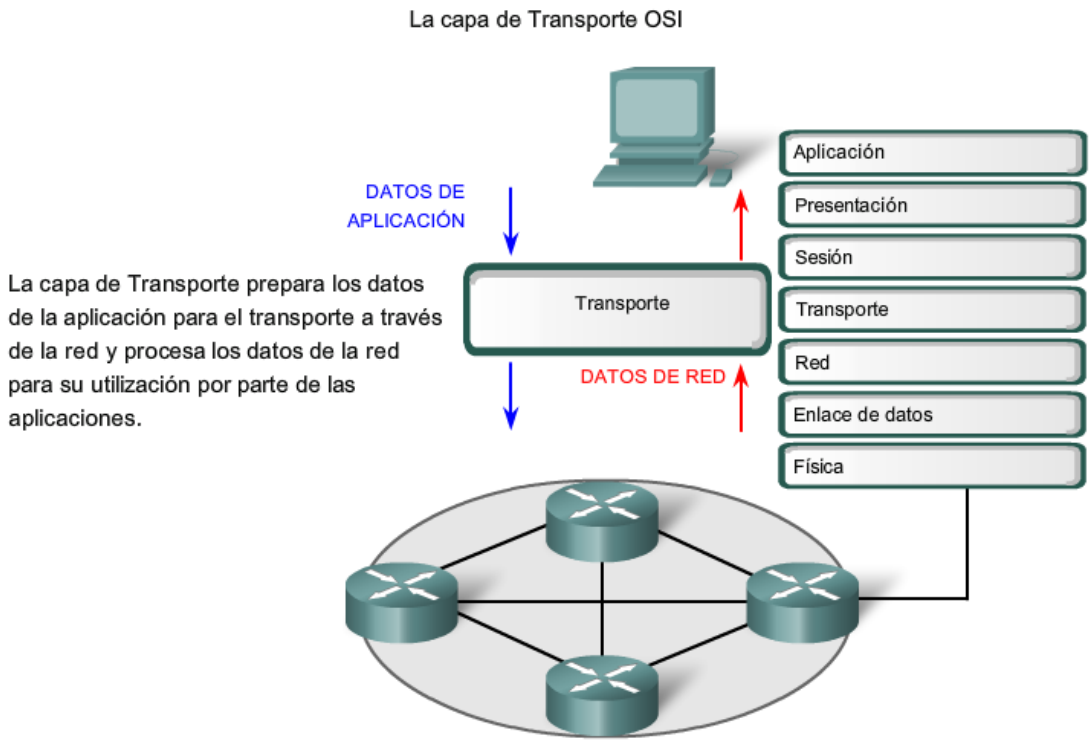


6.5. Capa 4: Transporte

La capa de transporte divide los datos provenientes del emisor y los reestructura en una corriente de datos dentro del sistema del emisor. Se puede concebir la frontera entre la capa de transporte y la capa de sesión como la frontera entre los protocolos de aplicación y los protocolos de transmisión de datos. Aunque las capas de aplicación, presentación y sesión están vinculadas a temas de aplicaciones, las cuatro capas subsiguientes se ocupan del traslado de datos.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Ilustración 30:
Capa De Transporte



La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte. Si desea recordar a la Capa 4 en la menor cantidad de palabras posible, piense en calidad de servicio y confiabilidad.

6.6. Capa 5: Sesión

Como indica su nombre, la capa de sesión configura, gestiona y concluye las sesiones entre dos hosts que están en comunicación. El nivel de sesión suministra sus servicios al nivel de presentación. Además, coordina el diálogo entre las dos capas de presentación de los dos proveedores y gestiona su intercambio de información. Además de controlar la sesión, la capa de sesión proporciona reglas para una transferencia de datos eficaz, clase de servicio y un registro de excepciones respecto a los inconvenientes de la capa de sesión, presentación y aplicación. Si busca retener la Capa 5 en el menor número de palabras posible, considere diálogos y conversaciones.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

6.7. Capa 6: Presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común. Si desea recordar la Capa 6 en la menor cantidad de palabras posible, piense en un formato de datos común.

6.8. Capa 7: Aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. (Blogger, 2024)

Ilustración 31:
Capa Aplicación

La capa de Aplicación ofrece la interfaz a la red.

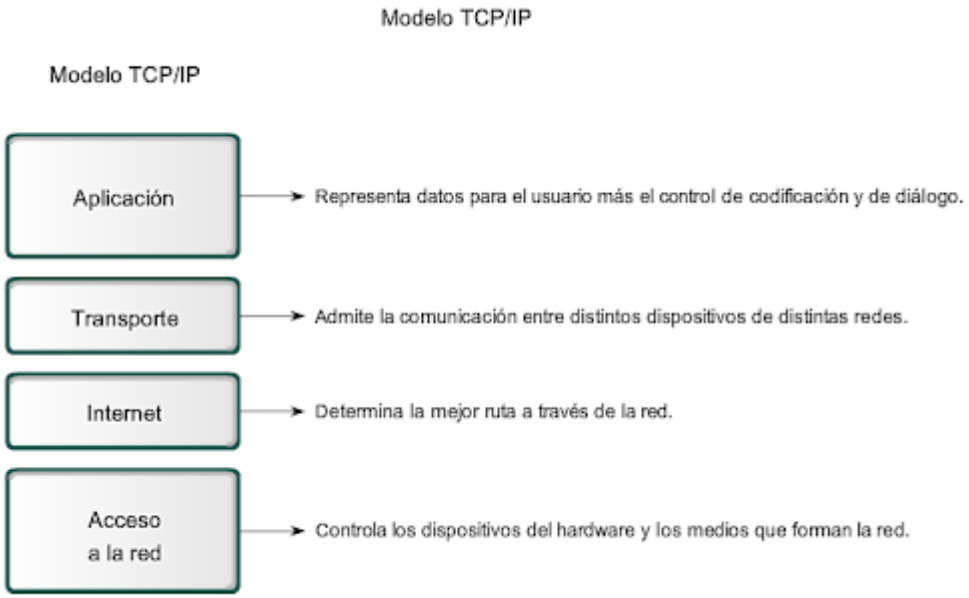
7. Modelo TCP/IP

El modelo TCP/IP, también conocido como el modelo de Internet, es un marco conceptual utilizado para entender y diseñar la estructura y los protocolos de las redes de Internet. Desarrollado en los años 70 y 80 por el Departamento de Defensa de los Estados Unidos, TCP/IP se ha convertido en el estándar para la comunicación en redes de computadoras.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

A diferencia del modelo OSI, el modelo TCP/IP consta de cuatro capas, cada una de las cuales tiene funciones específicas que facilitan la transmisión de datos en redes de computadoras.

Ilustración 32:
Modelo TCP/IP



Nota: *en la ilustración se puede observar las capas del modelo TCP/IP, las cuales son cuatro: aplicación, transporte, Internet y acceso a la red*

Actualmente la mayoría de los ordenadores están conectados a alguna red (internet, intranet, etc.) y casi todos lo hacen utilizando el modelo TCP/IP. Este modelo es un protocolo para comunicación en redes que permite que un equipo pueda comunicarse dentro de una red. Está basado en el modelo teórico OSI de capas con la que comparte 4 de ellas; sin embargo, ofrece muchas más opciones y es un modelo práctico.

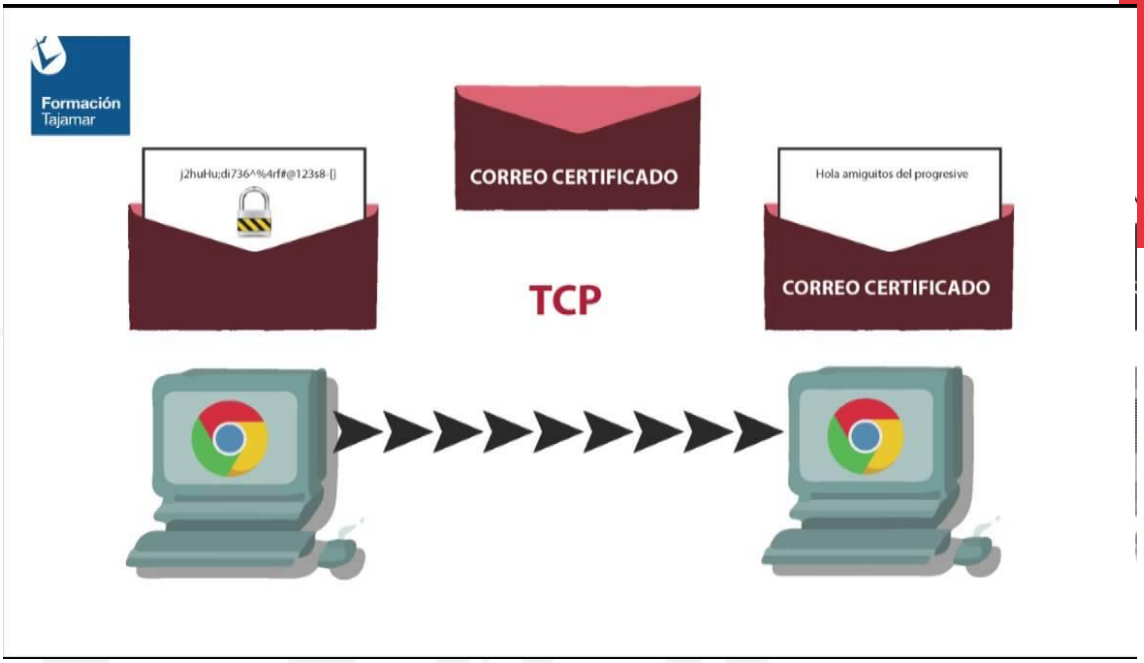
La comprensión de las características principales de la pila de protocolos de Internet TCP/IP posibilita la configuración de redes básicas, por lo que conocer TCP/IP es fundamental en cualquier formación centrada en trabajar con redes e internet (se llama pila de protocolos a una colección ordenada de protocolos organizados por capas).

El protocolo TCP/IP surgió de un proyecto de defensa llamado DARPA en 1969. En 1983 el nuevo conjunto de protocolos TCP/IP fue adoptado como estándar y finalmente se convirtió en el más usado en redes y el protocolo estándar de internet. (Robledano, 2019)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **TCP:** es el Protocolo de Control de Transmisión que permite establecer una conexión y el intercambio de datos entre dos anfitriones. Este protocolo proporciona un transporte fiable de datos.

Ilustración 33:
TCP



Nota: *en la ilustración se puede observar el funcionamiento del protocolo TCP*

- **IP:** protocolo de internet, utiliza direcciones series de cuatro octetos con formato de punto decimal (como por ejemplo 75.4.160.25). Este protocolo lleva los datos a otras máquinas de la red.

El modelo TCP/IP describe la funcionalidad de los protocolos que forman la suite de protocolos TCP/IP. Estos protocolos, que se implementan en los hosts emisores y receptores, interactúan para brindar una entrega extremo a extremo de las aplicaciones a través de la red.

1. Un proceso de comunicación completo incluye estos pasos:
2. Creación de datos en la capa de aplicación del dispositivo final de origen
3. Segmentación y encapsulación de datos a medida que pasan por el stack de protocolos en el dispositivo final de origen
4. Generación de datos en los medios en la capa de acceso a la red del stack
5. Transportación de los datos a través de internetwork, la cual está compuesta por medios y por cualquier dispositivo intermediario

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

6. Recepción de los datos en la capa de acceso a la red del dispositivo final de destino
7. Desencapsulación y reensamblaje de los datos a medida que pasan por el stack en el dispositivo de destino
8. Transmisión de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino (CIDECAME, 2024)

7.1. Capas Del Modelo TCP/IP

- **Capa De Enlace De Datos**

  La capa de enlace de datos (también denominada capa de enlace, capa de interfaz de red o capa física) es la que maneja las partes físicas del envío y recepción de datos mediante el cable Ethernet, la red inalámbrica, la tarjeta de interfaz de red, el controlador del dispositivo en el equipo, etcétera.

- **Capa De Internet**

  La capa de Internet (también denominada capa de red) controla el movimiento de los paquetes alrededor de la red.

- **Capa De Transporte**

  La capa de transporte es la que proporciona una conexión de datos fiable entre dos dispositivos. Divide los datos en paquetes, hace acuse de recibo de los paquetes que recibe del otro dispositivo y se asegura de que el otro dispositivo haga acuse de recibo de los paquetes que recibe a su vez.

- **Capa De Aplicaciones**

  La capa de aplicaciones es el grupo de aplicaciones que requiere comunicación de red. Es con lo que el usuario suele interactuar, como el correo electrónico y la mensajería. Como la capa inferior gestiona los detalles de la comunicación, las aplicaciones no tienen que preocuparse por ello.

7.2. Protocolos de aplicación

Los protocolos de aplicación son normas y reglas que permiten la comunicación y transferencia de datos entre aplicaciones a través de una red. Funcionan en la capa de aplicación del modelo OSI y TCP/IP, y son fundamentales para el funcionamiento de la mayoría de los servicios de Internet y las redes modernas. Estos protocolos definen cómo se deben estructurar

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

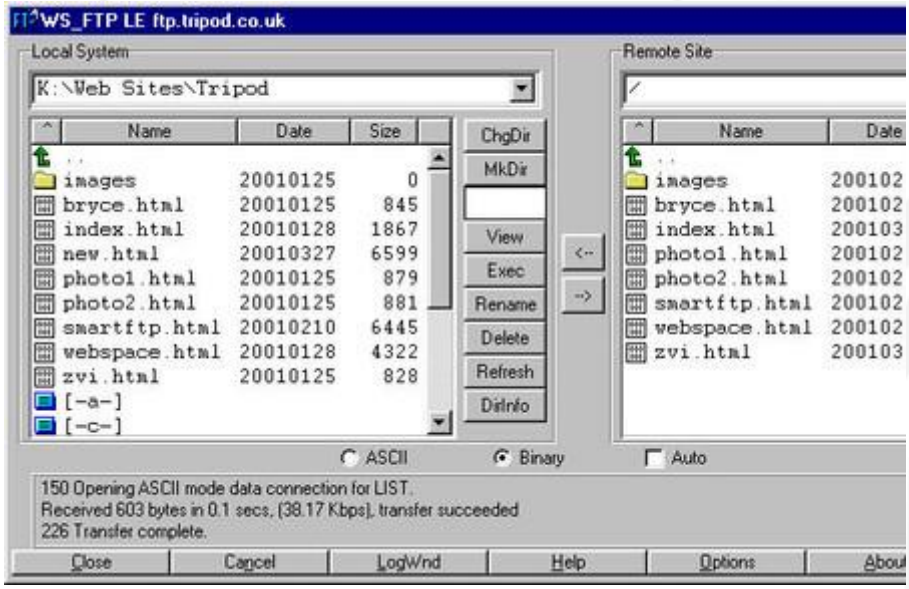
los mensajes, cómo se deben manejar las conexiones y cómo deben responder las aplicaciones a las solicitudes de los usuarios.

7.2.1. HTTP

El protocolo de transferencia de hipertexto (HTTP) constituye los cimientos de la red mundial, y se utiliza para cargar páginas web mediante enlaces de hipertexto. HTTP es un protocolo de capa de aplicación diseñado para transferir información entre los dispositivos conectados de la red, y se ejecuta sobre otras capas del conjunto de protocolos de la red. Un flujo típico sobre HTTP implica una máquina cliente que realiza una solicitud a un servidor, que a continuación envía un mensaje de respuesta. (Cloudflare, 2024)

7.2.2. FTP

Ilustración 34:
FTP



El protocolo FTP comenzó a implementarse en abril de 1971 y culminó en establecer su estructura en 73, aunque durante las décadas de los 70 y 80 del siglo pasado, continuó su perfeccionamiento. Para que comprendas, este protocolo surgió antes de la aparición de Internet o el correo electrónico, dado que constituyó uno de los elementos fundamentales de ARPANET, que fue esa red inicial que posteriormente originó Internet.

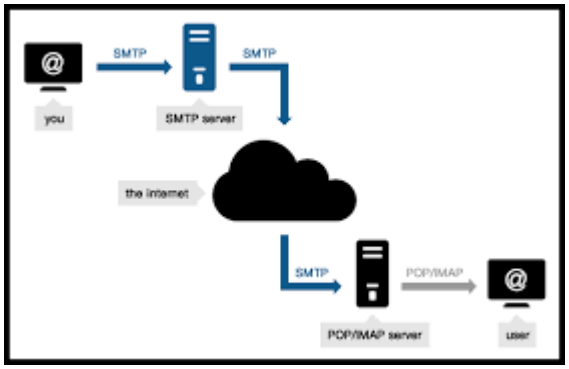
Este protocolo funciona entre ordenadores que estén conectados a una red TCP, que significa *Transmission Control Protocol* o Protocolo de control de transmisión. Este protocolo TCP da soporte a muchas tecnologías, entre ellas a Internet. Para que te hagas a la idea, la familia de protocolos que forman Internet se llama TCP/IP. (Fernández, 2024)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

7.2.3. SMTP

SMTP significa Simple Mail Transfer Protocol, que puede traducirse como “protocolo de transferencia simple de correo”. Se trata de un protocolo de conexión de Internet y, como tal, se encuentra en la séptima capa del modelo OSI, la capa de aplicación. Al igual que cualquier otro protocolo de red, contiene reglas para la comunicación correcta entre los ordenadores de una red. SMTP es responsable de procesar y reenviar correos electrónicos de un remitente a un destinatario.

Ilustración 35:
SMTP



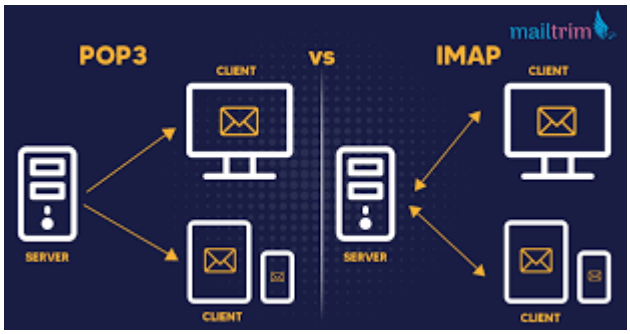
Desde su lanzamiento en 1982 como sucesor del “Mail Box Protocol” en Arpanet, SMTP se ha convertido en el protocolo estándar para el envío de correos electrónicos. Para el usuario medio, el procedimiento que sigue el protocolo SMTP sigue siendo en gran medida invisible, ya que se lleva a cabo en segundo plano mediante el programa de correo electrónico en cuestión. Solo tendremos que configurar el protocolo SMTP si el software, el gestor de correo que tengamos instalado en nuestro ordenador o la aplicación de correo de nuestro móvil no lo determina de forma automática.

7.2.4. POP3

El protocolo POP3 (Post Office Protocol) o también conocido como «Protocolo de Oficina de correo», es uno de los protocolos fundamentales para la gestión del correo electrónico o email. Este protocolo se utiliza por los clientes locales de email para obtener los mensajes de email de un servidor remoto de correo electrónico, este servidor se le llama comúnmente servidor de correo o servidor POP3. Este protocolo pertenece al nivel de aplicación del modelo TCP/IP, actualmente se utiliza la última versión que es la POP3, el resto de las versiones no se utilizan por estar anticuadas, cuando hacemos referencia al protocolo POP siempre nos referiremos al protocolo POP3.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Ilustración 36: POP3

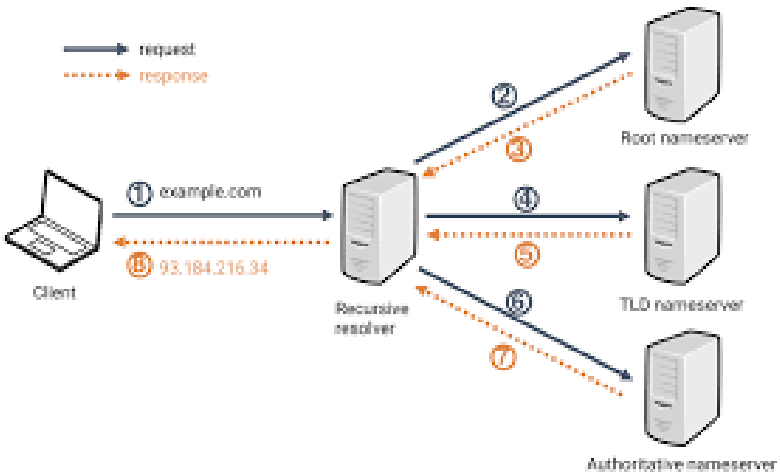


Nota: *en la ilustración se puede observar cómo funciona los protocolos POP3 y IMAP, utilizados para el correo*

El protocolo POP3 utiliza el protocolo de la capa de transporte TCP, hace uso de los puertos TCP 110 para el POP3 sin cifrado de datos, y el puerto TCP 995 para POP3 con cifrado de datos. Actualmente es muy extraño que un proveedor de servicios de correo electrónico no disponga de soporte para SSL/TLS en POP3, por tanto, casi siempre utilizaremos el puerto 995 de TCP porque nos proporciona confidencialidad, si usamos el puerto 110 TCP significa que el tráfico de datos entre el servidor de correo y el cliente de email local no está cifrado, por tanto, podríamos tener problemas de privacidad.

7.2.5. DNS

Ilustración 37:
DNS



Nota: en la ilustración se puede observar el funcionamiento de servidor DNS que se dedica a la transformación de una IP a un nombre de dominio

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

El proceso de solución de DNS supone convertir un nombre de servidor (como www.example.com) en una dirección IP compatible con el ordenador (como 192.168.1.1). Se da una dirección IP a cada dispositivo en Internet, y esa dirección será necesaria para encontrar el dispositivo apropiado de Internet, al igual que se usa la dirección de una calle para encontrar una casa concreta. Cuando un usuario quiere cargar una página, se debe traducir lo que el usuario escribe en su navegador web (example.com) a una dirección que el ordenador pueda entender para poder localizar la página web de example.com.

Para entender el proceso de la resolución de DNS, es importante conocer los diferentes componentes de hardware por los que debe pasar una consulta de DNS. Para el navegador web, la búsqueda de DNS se produce "en segundo plano" y no requiere ninguna interacción del ordenador del usuario, aparte de la solicitud inicial.

7.3. Protocolos de transporte

Los protocolos de transporte son fundamentales en la arquitectura de redes porque gestionan la transferencia de datos entre sistemas finales, asegurando que los datos lleguen de manera fiable, ordenada y sin errores. Funcionan en la capa de transporte tanto del modelo OSI como del modelo TCP/IP, proporcionando servicios esenciales para la comunicación efectiva en redes de computadoras.

7.4. Principales Protocolos De Transporte

7.4.1. UDP

UDP es un protocolo de transporte sin conexión que proporciona una comunicación rápida pero no garantiza la fiabilidad, el orden de los datos ni la corrección de errores.

7.5. Protocolos de Internet

El Protocolo de Internet (IP) es el pilar fundamental sobre el cual se construyen las redes modernas, incluyendo Internet. IP es un protocolo de la capa de red en el modelo OSI y el modelo TCP/IP, y su función principal es proporcionar un esquema de direccionamiento único y una ruta de entrega para los datos enviados entre dispositivos en una red.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

7.6. Funciones Principales del Protocolo de Internet

7.6.1. Direccionamiento

Direcciones IP: IP asigna una dirección única a cada dispositivo en la red. Estas direcciones pueden ser IPv4 (32 bits) o IPv6 (128 bits).

Subredes: Permite dividir grandes redes en subredes más pequeñas para una mejor organización y gestión del tráfico.

7.6.2. Encaminamiento

Encapsulación de Paquetes: Los datos se encapsulan en paquetes IP que contienen la dirección IP de origen y destino.

Enrutamiento: IP determina la mejor ruta para enviar los paquetes desde el origen hasta el destino a través de una serie de dispositivos de red como routers.

7.6.3. Fragmentación y Reensamblaje

Fragmentación: Divide paquetes grandes en fragmentos más pequeños si el medio de transmisión no puede manejar el tamaño del paquete.

Reensamblaje: En el destino, los fragmentos se reensamblan para reconstruir el paquete original.

7.6.4. Versiones del Protocolo de Internet

IPv4 (Internet Protocol version 4)

Descripción: Es la versión más utilizada de IP, definida en el RFC 791.

Características:

Dirección de 32 bits: Permite aproximadamente 4.3 mil millones de direcciones únicas.

Notación Decimal Punteada: Las direcciones se escriben como cuatro números decimales separados por puntos (ej. 192.168.1.1).

Fragmentación: Soporta la fragmentación de paquetes para adaptarse a diferentes tamaños de MTU (Maximum Transmission Unit).

Limitaciones: La creciente demanda de direcciones IP ha llevado a la escasez de direcciones IPv4 disponibles.

IPv6 (Internet Protocol version 6)

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Descripción: Diseñado para reemplazar a IPv4, definido en el RFC 8200.

Características:

Dirección de 128 bits: Permite una cantidad prácticamente ilimitada de direcciones únicas (3.4 x 10^38 direcciones).

Notación Hexadecimal: Las direcciones se escriben como ocho grupos de cuatro dígitos hexadecimales separados por dos puntos (ej. 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Sin Fragmentación: IPv6 no permite la fragmentación en routers, lo que simplifica el procesamiento de paquetes.

Autoconfiguración: IPv6 soporta la autoconfiguración de direcciones (SLAAC) y mejora la funcionalidad de red.

Ventajas: Mejora la seguridad integrada con IPsec obligatorio y proporciona mayor eficiencia en el enrutamiento.

7.6.5. Importancia del Protocolo de Internet

- **Interconexión de Redes Heterogéneas:** IP permite que diferentes tipos de redes se conecten y comuniquen, creando una red global unificada.
- **Escalabilidad:** Con la introducción de IPv6, IP puede soportar un número casi ilimitado de dispositivos, lo cual es crucial para el crecimiento continuo de Internet.
- **Fiabilidad en la Entrega de Datos:** IP proporciona mecanismos para asegurar que los datos se entreguen de manera eficiente y precisa, incluso a través de múltiples redes.
- **Fundamento de la Red:** Todos los servicios y aplicaciones de Internet dependen de IP para la entrega de datos, desde la navegación web hasta la transmisión de video y los servicios de correo electrónico.

7.7. Protocolos de enlace de datos

Los protocolos de enlace de datos son fundamentales en la comunicación de redes, ya que aseguran la transferencia fiable de datos a través de un enlace físico entre dos dispositivos. Operan en la capa de enlace de datos del modelo OSI y son esenciales para la comunicación directa entre dispositivos en una red local (LAN).

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

7.7.1. Funciones Principales del Protocolo de Enlace de Datos

- Control de Acceso al Medio (MAC)
- Descripción: Determina cómo los dispositivos en la misma red física comparten el medio de transmisión.
- Métodos: Incluyen acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD) en Ethernet, y acceso múltiple con detección de portadora y evitación de colisiones (CSMA/CA) en redes inalámbricas.
- Encapsulación de Datos
- Tramas: Los datos se encapsulan en tramas que incluyen una cabecera y una cola para proporcionar información de control y verificar la integridad de los datos.
- Dirección Física: Las tramas contienen direcciones MAC (Media Access Control) para identificar de manera única los dispositivos en la red.
- Detección y Corrección de Errores
- CRC (Cyclic Redundancy Check): Un código de redundancia cíclica se añade a la trama para detectar errores durante la transmisión.
- Retransmisión: Si se detecta un error, la trama puede ser retransmitida para asegurar que los datos lleguen correctamente.
- Control de Flujo
- Mecanismos de Control de Flujo: Evitan que un dispositivo rápido sature a uno más lento enviando datos a una velocidad que este último no pueda manejar.

7.7.2. Principales Protocolos de Enlace de Datos

Ethernet (IEEE 802.3)

Descripción: Es el estándar más común para redes de área local (LAN).

Características:

CSMA/CD: Utiliza acceso múltiple con detección de portadora y detección de colisiones para gestionar el acceso al medio.

Velocidades: Admite múltiples velocidades de transmisión como 10 Mbps, 100 Mbps, 1 Gbps, y superiores.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Tramas Ethernet: Contienen campos para la dirección MAC de origen y destino, tipo de protocolo, datos y CRC.

Ventajas: Amplia compatibilidad, facilidad de implementación, alta velocidad y coste relativamente bajo.

Wi-Fi (IEEE 802.11)

Descripción: Estándar para redes inalámbricas que permite la comunicación sin cables.

Características:

CSMA/CA: Utiliza acceso múltiple con detección de portadora y evitación de colisiones para minimizar las colisiones en un entorno inalámbrico.

Modos de Operación: Incluye modos de infraestructura (con un punto de acceso) y ad hoc (sin punto de acceso).

Seguridad: Soporta varios protocolos de seguridad como WPA2 y WPA3 para proteger la comunicación inalámbrica.

Ventajas: Movilidad, facilidad de instalación, y flexibilidad en la ubicación de los dispositivos.

PPP (Point-to-Point Protocol)

Descripción: Protocolo utilizado para la comunicación directa entre dos nodos de red.

Características:

Encapsulación: Encapsula datos de la capa de red para su transmisión a través de un enlace punto a punto.

Autenticación: Soporta varios métodos de autenticación como PAP y CHAP.

Detección de Errores: Incluye mecanismos para detectar y corregir errores en la transmisión.

Usos Comunes: Conexiones dial-up, enlaces seriales y túneles VPN.

Frame Relay

Descripción: Protocolo de conmutación de paquetes de alta eficiencia para redes de área extensa (WAN).

Características:

Tramas: Encapsula datos en tramas con un tamaño variable para mejorar la eficiencia.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Circuitos Virtuales: Establece circuitos virtuales permanentes (PVC) para la comunicación continua entre puntos específicos.

Control de Flujo: Utiliza el control de flujo para gestionar la transmisión de datos entre puntos finales.

Usos Comunes: Conexiones WAN para empresas y proveedores de servicios de telecomunicaciones.

7.7.3. Importancia de los Protocolos de Enlace de Datos

- **Confiabilidad:** Aseguran que los datos se transfieran de manera precisa y fiable a través del enlace físico.
- **Gestión de Acceso:** Controlan cómo los dispositivos acceden y utilizan el medio de transmisión, evitando colisiones y mejorando la eficiencia.
- **Integridad de los Datos:** Implementan mecanismos para detectar y corregir errores, garantizando la integridad de los datos transmitidos.
- **Interoperabilidad:** Permiten que dispositivos de diferentes fabricantes y tipos se comuniquen eficazmente en una red.

8. Subnetting

Subnetting, una contracción de subnetwork partitioning, es el proceso de dividir una red IP única en subredes más pequeñas y manejables. En lugar de tener una única red grande, el subnetting permite organizar y distribuir direcciones IP de manera más eficiente. Esta técnica se ha vuelto fundamental a medida que las redes crecen en tamaño y complejidad.

8.1. Uso Del Subnetting

Optimización del uso de direcciones IP: El subnetting permite el uso más eficiente de las direcciones IP al dividir una red en bloques más pequeños. Esto es particularmente valioso en un entorno donde las direcciones IP son un recurso limitado.

- *Mejora de la seguridad:* Al crear subredes, se establecen límites más definidos entre los diferentes segmentos de una red. Esto dificulta a los posibles atacantes moverse libremente una vez que han comprometido una parte de la red, mejorando así la seguridad general.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- *Reducción del tráfico de broadcast:* En redes más grandes, el tráfico de broadcast puede convertirse en un problema. El subnetting divide la red en segmentos más pequeños, lo que reduce la cantidad de dispositivos que reciben y procesan los paquetes de broadcast. Esto mejora la eficiencia general de la red.
- *Facilita la administración:* La administración de una red se vuelve más sencilla con subredes bien definidas. Permite asignar responsabilidades específicas para la administración de cada subred, lo que facilita la resolución de problemas y el mantenimiento general.

8.2. Funcionamiento Del Subnetting

El proceso de subnetting implica dividir una red en bloques más pequeños, asignando rangos específicos de direcciones IP a cada subred. Aquí hay pasos clave en el proceso de subnetting:

- *Determinar el número de subredes necesarias:* Este es el primer paso crítico. Evalúa el tamaño y la estructura de tu red para determinar cuántas subredes necesitas. Ten en cuenta el crecimiento futuro para evitar restricciones.
- *Elegir una máscara de subred apropiada:* La máscara de subred define el tamaño de cada subred. Decide cuántos bits asignarás para la dirección de red y cuántos para los hosts en cada subred.
- *Asignar direcciones IP a subredes:* Divide el rango de direcciones IP disponible en tu red en subredes más pequeñas. Asegúrate de dejar espacio para direcciones de red y broadcast en cada subred.
- *Documentar y organizar:* Lleva un registro detallado de las asignaciones de direcciones IP para cada subred. Esto es esencial para la administración continua y la resolución de problemas. (Mallón, 2024)

8.3. Tipos De Subnetting

8.3.1. Subneteo

Es un procedimiento que permite dividir a una red primaria IPv4 en una serie de subredes, de tal forma que cada una de ellas funcione a nivel de envío y recepción de paquetes, como una red individual, aunque todas pertenezcan a la misma red principal y, por lo tanto, al mismo dominio de difusión original.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Cuando trabajamos con una red pequeña no encontramos muchos problemas para configurar el rango de direcciones IPv4 para conseguir un rendimiento óptimo. Pero a medida que se van agregando Host a la red, el desempeño empieza a verse afectado. Esto puede ser corregido, en parte, segmentando la red con switches, reduciendo los Dominios de colisión (host que comparten el mismo medio) enviando las tramas solo al segmento correcto. Pero, aunque se reducen las colisiones con tomar estas medidas, si se continúa aumentando el número de host, aumentan también los envíos de broadcast (Envió de paquetes a todos los dispositivos de la red). Lo que afecta considerablemente el desempeño de la red. Esto se debe a que los Switches solo segmentan a nivel de MAC Address y los envíos de broadcast son a nivel de red 255.255.255.255

Formulas

- **Cantidad de subredes**

$$\mathbf{2^n} \geq numero\ de\ subredes\ solicitadas$$

Donde: N, es el numero de bits "robados" a la porción de host.

- **Cantidad de Host Por Subredes**

$$2^M - 2$$

Donde: M, es el numero de bits disponibles en la porción de host

- **Rango de la subred(salto)**

$$256 - variación\ en\ mascara$$

Ejemplo

Red: 192.168.1.0

Cantidad de subredes: 5

1. **Determinar el valor de N**

$$\mathbf{2^N \geq 5}$$

$$\mathbf{2^3 \geq 5}$$

N=3

2. **Descubrir la nueva mascara:** N, será el numero de bits que se deberá encender en la mascara por clase. Los bits se deben encender de izquierda a derecha

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Mascara por defecto de la IP otorgada: 255.255.255.0

- La mascara por defecto se debe transformar de decimal a binarios

  11111111.11111111.11111111.00000000

- Encender el numero bits según el valor de N

  11111111.11111111.11111111.11100000

- Transformar la mascara de bits a decimal

  255.255.255.224

3. **Descubrir el numero de host por cada subred**

$$2^M - 2$$

Donde M, es el número de ceros sobrante en la nueva mascara

$$2^5 - 2$$

Numero de host por cada subred = 30

4. **Descubrir el rango de subred a subred (salto)**

$$256 - variación\ en\ mascara$$

$$256 - 224$$

Rango = 32

5. **Tabla de direccionamiento**

Una tabla de direccionamiento es esencial para planificar y organizar cómo se asignarán las direcciones IP dentro de una red, incluyendo subredes y direcciones específicas para dispositivos y equipos. A continuación, se presenta un ejemplo de una tabla de direccionamiento que podría ser utilizada en una red de tamaño moderado.

Subred	IP inicial	IP final	Host	Mascara	Broadcast
1	192.168.1.0	192.168.1.30	30	255.255.255.224	192.168.1.31
2	192.168.1.32	192.168.1.62	30	255.255.255.224	192.168.1.63

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

3	192.168.1.64	192.168.1.94	30	255.255.255.224	192.168.1.95
4	192.168.1.96	192.168.1.126	30	255.255.255.224	192.168.1.127
5	192.168.1.128	192.168.1.158	30	255.255.255.224	192.168.1.159

Autoevaluación 2

1. **¿Cuántas capas tiene el modelo OSI?**

   - a) 5
   - b) 6
   - c) 7
   - d) 8

2. **¿Cuál de las siguientes capas del modelo OSI es responsable de la encriptación y compresión de datos?**

   - a) Capa de Aplicación
   - b) Capa de Presentación
   - c) Capa de Sesión
   - d) Capa de Transporte

3. **En el modelo TCP/IP, ¿cuál capa es equivalente a las capas de Aplicación, Presentación y Sesión del modelo OSI?**

   - a) Capa de Transporte
   - b) Capa de Red
   - c) Capa de Enlace de Datos
   - d) Capa de Aplicación

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

4. **¿Cuál de los siguientes protocolos se encuentra en la capa de transporte del modelo TCP/IP?**

   - a) IP
   - b) UDP
   - c) HTTP
   - d) ICMP

5. **¿Qué protocolo se utiliza principalmente para la navegación web?**

   - a) FTP
   - b) HTTP
   - c) SMTP
   - d) DNS

6. **¿Cuál es la longitud de una dirección IPv6?**

   - a) 32 bits
   - b) 48 bits
   - c) 64 bits
   - d) 128 bits

7. **¿Cuál de las siguientes afirmaciones es verdadera sobre el subnetting?**

   - a) Permite dividir una red grande en redes más pequeñas.
   - b) Incrementa el número total de direcciones IP disponibles.
   - c) Es una técnica exclusiva para IPv6.
   - d) No afecta el rendimiento de la red.

8. **En el contexto de subnetting, ¿qué significa CIDR?**

   - a) Classless Inter-Domain Routing
   - b) Common Internet Data Routing
   - c) Classful Internet Domain Routing

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- d) Common Inter-Domain Resource

9. **¿Cuál de los siguientes protocolos de la capa de red proporciona comunicación sin conexión y no garantiza la entrega de paquetes?**

   - a) TCP
   - b) IP
   - c) SMTP
   - d) FTP

10. **¿Qué máscara de subred se utiliza comúnmente para una red de clase C?**

    - a) 255.0.0.0
    - b) 255.255.0.0
    - c) 255.255.255.0
    - d) 255.255.255.255

Respuestas

1. **c) 7** - El modelo OSI tiene 7 capas.
2. **b) Capa de Presentación** - La capa de presentación se encarga de la encriptación y compresión de datos.
3. **d) Capa de Aplicación** - En el modelo TCP/IP, la capa de Aplicación es equivalente a las capas de Aplicación, Presentación y Sesión del modelo OSI.
4. **b) UDP** - UDP es un protocolo de la capa de transporte del modelo TCP/IP.
5. **b) HTTP** - HTTP es el protocolo utilizado principalmente para la navegación web.
6. **d) 128 bits** - Una dirección IPv6 tiene una longitud de 128 bits.
7. **a) Permite dividir una red grande en redes más pequeñas.** - Subnetting permite dividir una red grande en redes más pequeñas.
8. **a) Classless Inter-Domain Routing** - CIDR significa Classless Inter-Domain Routing.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

9. **b) IP** - IP proporciona comunicación sin conexión y no garantiza la entrega de paquetes.
10. **c) 255.255.255.0** - La máscara de subred común para una red de clase C es 255.255.255.0.

Resumen de la Unidad 2

En esta unidad se aborda el modelo OSI, un marco conceptual de siete capas (física, enlace de datos, red, transporte, sesión, presentación y aplicación) que facilita la comprensión y diseño de la comunicación entre sistemas informáticos, y el modelo TCP/IP, base de la comunicación en Internet con cuatro capas (enlace, internet, transporte y aplicación) que gestionan desde la transmisión de bits hasta los servicios de red. Se analizan los principales protocolos de red, incluyendo HTTP/HTTPS para la transferencia de páginas web, FTP para la transferencia de archivos, SMTP para el envío de correos electrónicos, DNS para la traducción de nombres de dominio a direcciones IP, TCP para la transmisión fiable de datos, UDP para la transmisión rápida y no fiable, e IP para el direccionamiento y enrutamiento de paquetes. Además, se estudia el subnetting, técnica que permite dividir una red IP en subredes más pequeñas, mejorando la organización, utilización de direcciones IP, seguridad y rendimiento de la red, a través de conceptos como máscaras de subred y CIDR (Classless Inter-Domain Routing), aplicables tanto en IPv4 como en IPv6. Esta unidad es esencial para el diseño, implementación y mantenimiento de redes de computadoras eficientes y seguras.

UNIDAD 3: ENRUTAMIENTO Y COMUNICACIÓN

Temas y Subtemas

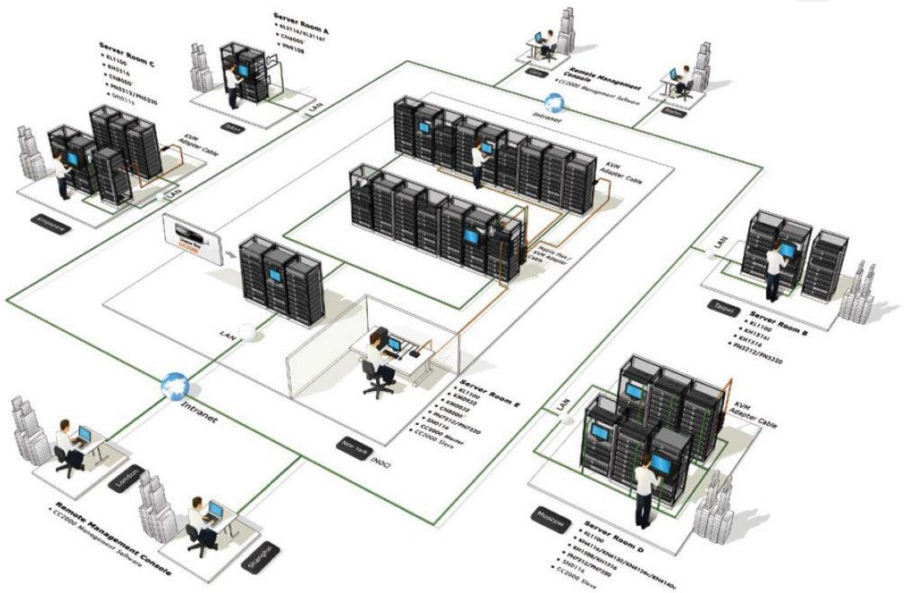
(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Diseño de redes de datos**
- **Enrutamientos y comunicación**
- **Configuración y mantenimiento de enrutadores**
- **Herramientas de monietoreo y gestión de redes**

9. Diseño De Redes De Datos

La capacidad para diseñar redes de datos es esencial para cualquier experto en el área de la tecnología de la información. Esta unidad se enfoca en los fundamentos y procedimientos requeridos para crear redes eficaces y seguras que satisfagan las demandas de una entidad. Se tratarán temas como la organización de la red, la elección de equipos y programas, y las tácticas de diseño para mejorar el desempeño y la protección de la red. Esta unidad capacita a los alumnos en la construcción de infraestructuras de red sólidas y escalables.

Ilustración 38:
Diseño de redes de datos



(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Nota: *en la ilustración se puede observar el diseño de una red de datos para una empresa, en la cual se puede visualizar diferentes gabinetes con servidores, routers, switches y cableado. El cual brinda servicios a la empresa.*

Dependiendo el tamaño del negocio (no en el aspecto físico solamente, sino en el volumen de las operaciones o transacciones), se requerirá algún tipo de interconexión entre las computadoras y otros dispositivos existentes en la empresa para poder optimizar los procesos que se lleven a cabo: compartir impresoras, enviar comunicaciones, almacenar información compartida, generar documentos que dependen de otros datos dentro de la empresa, etc.

Para este caso, analizaremos los pasos previos a la instalación y configuración de una red LAN y los requisitos necesarios para que la misma quede operativa y funcional en la empresa. (InGenio Learning , 2024)

El diseño de red, a veces conocido como topología de red, es la práctica mediante la cual un profesional de telecomunicaciones organiza la infraestructura física, virtual y lógica en una red de TI antes de su instalación.

Esto se hace por medio de la elaboración de planos y diagramas de red. Un diagrama de red suele ser la base del proceso de diseño. Este proporciona una representación visual de su red e integra información como conexiones físicas; cantidad, tipo y ubicación de todos los dispositivos y terminales; direccionamiento IP; y procesos y arquitectura de seguridad.

9.1. Requerimientos de diseño de redes de datos

El diseño de redes de datos debe considerar una variedad de requerimientos para asegurar que la red sea eficiente, segura, escalable y capaz de soportar las necesidades presentes y futuras de la organización. Estos requerimientos se pueden clasificar en varias categorías:

1. Requerimientos de Rendimiento

- **Ancho de Banda:** Es la capacidad máxima de transmisión de datos de la red. Debe ser suficiente para manejar el tráfico esperado sin congestionarse.
- **Latencia:** Es el tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino. Redes de baja latencia son críticas para aplicaciones en tiempo real como videoconferencias y juegos en línea.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Jitter:** Variabilidad en la latencia de los paquetes de datos, que puede afectar la calidad de aplicaciones sensibles al tiempo.
- **Throughput:** Es la cantidad real de datos que pueden ser transmitidos a través de la red en un tiempo determinado. Se debe evaluar en función de la demanda esperada.

2. Requerimientos de Escalabilidad

- **Expansión:** La red debe poder expandirse fácilmente para incluir más dispositivos y usuarios sin una reestructuración significativa.
- **Modularidad:** La red debe diseñarse en módulos que puedan ser añadidos o eliminados según sea necesario.

3. Requerimientos de Seguridad

- **Confidencialidad:** Protección de la información contra acceso no autorizado.
- **Integridad:** Asegurar que los datos no sean alterados durante la transmisión.
- **Disponibilidad:** Asegurar que los recursos de red estén disponibles para los usuarios autorizados cuando se necesiten.
- **Autenticación:** Verificar la identidad de los usuarios y dispositivos que acceden a la red.
- **Control de Acceso:** Políticas y mecanismos para controlar quién puede acceder a qué recursos de la red.

4. Requerimientos de Gestión y Mantenimiento

- **Monitorización y Diagnóstico:** Herramientas y técnicas para monitorizar el rendimiento de la red y diagnosticar problemas.
- **Configuración y Gestión Remota:** Capacidad de gestionar y configurar la red de manera remota.
- **Registro y Auditoría:** Mantener registros detallados de la actividad de la red para auditoría y resolución de problemas.

5. Requerimientos de Fiabilidad y Disponibilidad

- **Redundancia:** Implementar caminos y dispositivos redundantes para evitar puntos únicos de fallo.
- **Resiliencia:** Capacidad de la red para recuperarse rápidamente de fallos o interrupciones.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Mantenimiento Programado:** Planificación de mantenimiento sin interrupciones significativas del servicio.

6. Requerimientos de Compatibilidad e Interoperabilidad

- **Compatibilidad de Dispositivos:** Asegurar que todos los dispositivos y componentes de la red sean compatibles entre sí.
- **Interoperabilidad con Sistemas Existentes:** La nueva red debe ser capaz de integrarse con sistemas y redes existentes sin problemas.

7. Requerimientos de Costo

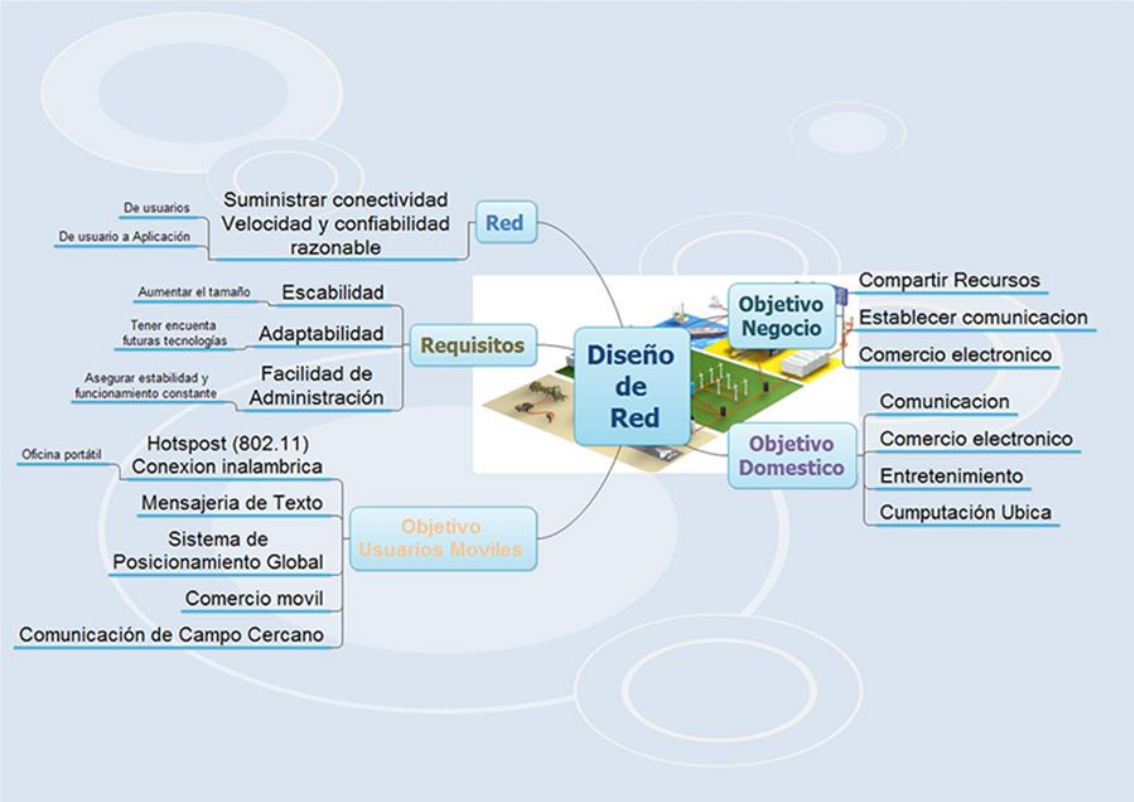
- **Presupuesto Inicial:** Costo de instalación y adquisición de hardware y software.
- **Costo Operativo:** Gastos recurrentes para el mantenimiento y operación de la red.
- **Relación Costo-Beneficio:** Evaluar el retorno de inversión y los beneficios a largo plazo de la red diseñada.

8. Requerimientos de Conformidad y Normativas

- **Normativas y Estándares:** Cumplimiento con normativas locales, nacionales e internacionales.
- **Regulaciones de Datos:** Cumplir con regulaciones específicas de la industria sobre manejo y protección de datos (como GDPR, HIPAA, etc.).

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

***Ilustración 39**:*
Requerimientos de diseño de red de datos



***Nota:** en la ilustración se puede observar las características para el diseño de una red de datos como: requisitos, objetivo de negocio, objetivo doméstico, objetivo de usuarios móviles.*

9.2. Análisis de trafico de red de datos

El tráfico de red se refiere a la cantidad de datos que se mueven a través de una red informática en cualquier momento dado. El tráfico de red, también llamado tráfico de datos se divide en paquetes de datos y se envía a través de una red antes de ser reensamblados por el dispositivo receptor o la computadora.

El tráfico de red tiene dos flujos direccionales, norte-sur y este-oeste. El tráfico afecta la calidad de la red porque una cantidad inusualmente alta de tráfico puede significar velocidades de descarga lentas o conexiones inestables de protocolo de voz sobre Internet (Voice over Internet Protocol, VoIP). El tráfico también está relacionado con la seguridad porque una cantidad inusualmente alta de tráfico podría ser señal de un ataque. (Fortinet, 2024)

9.2.1. Tipos de tráficos de redes

Para administrar mejor el ancho de banda, los administradores de red deciden cómo ciertos tipos de tráfico deben ser tratados por dispositivos de red como enrutadores y

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

conmutadores. Existen dos categorías generales de tráfico de red: en tiempo real y en tiempo no real.

Trafico en tiempo real

El tráfico que se considere importante o crítico para las operaciones comerciales debe entregarse a tiempo y con la más alta calidad posible. Algunos ejemplos de tráfico de red en tiempo real incluyen VoIP, videoconferencias y navegación web.

trafico en tiempo no real

El tráfico en tiempo no real, también conocido como tráfico de mejor esfuerzo, es el tráfico que los administradores de red consideran menos importante en comparación con el tráfico en tiempo real. Algunos ejemplos incluyen el Protocolo de transferencia de archivos (File Transfer Protocol, FTP) para aplicaciones de correo electrónico y publicaciones web. (Fortinet, 2024)

9.3. Planificación de la red de datos

La planificación de la red de datos es una etapa crítica en el diseño y la implementación de una infraestructura de red eficiente y segura. Esta fase implica una serie de pasos que aseguran que la red cumpla con los requisitos técnicos y de negocio. A continuación, se detalla el proceso de planificación de una red de datos:

1. Análisis de Requerimientos

- **Identificación de Necesidades:** Determinar las necesidades de la organización, como el número de usuarios, tipo de aplicaciones, volumen de tráfico y requerimientos de seguridad.
- **Entrevistas y Cuestionarios:** Realizar entrevistas con los stakeholders y utilizar cuestionarios para recopilar información sobre las expectativas y necesidades de los usuarios.

2. Diseño Lógico de la Red

- **Topologías de Red:** Seleccionar la topología de red adecuada (estrella, malla, anillo, bus) basada en los requerimientos de rendimiento y escalabilidad.
- **Segmentación de Red:** Decidir cómo segmentar la red en subredes para mejorar el rendimiento y la seguridad.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Asignación de Direcciones IP:** Planificar la asignación de direcciones IP, incluyendo el uso de direcciones privadas y públicas, y la implementación de DHCP.

3. Diseño Físico de la Red

- **Mapa Físico de la Red:** Crear un diagrama que muestre la disposición física de los dispositivos de red y el cableado.
- **Selección de Hardware:** Elegir routers, switches, firewalls, puntos de acceso, y otros dispositivos de red basados en los requisitos de rendimiento y compatibilidad.
- **Planificación del Cableado:** Planificar el cableado estructurado, incluyendo la ubicación de racks, paneles de parcheo y puntos de acceso.

4. Selección de Tecnología y Proveedores

- **Evaluación de Productos:** Evaluar las opciones de hardware y software disponibles, considerando factores como el costo, la compatibilidad, y el soporte técnico.
- **Proveedores de Servicios:** Seleccionar proveedores de servicios de Internet (ISP) y otros proveedores externos necesarios para el funcionamiento de la red.

5. Implementación de Seguridad

- **Políticas de Seguridad:** Definir políticas de seguridad claras para proteger la red y los datos.
- **Configuración de Firewalls y IDS/IPS:** Implementar y configurar firewalls, sistemas de detección y prevención de intrusos (IDS/IPS), y otras medidas de seguridad.
- **Acceso Seguro:** Configurar VPNs y otros mecanismos para asegurar el acceso remoto seguro.

6. Pruebas y Validación

- **Pruebas de Conectividad:** Realizar pruebas para asegurar que todos los dispositivos están correctamente conectados y comunicándose.
- **Pruebas de Rendimiento:** Evaluar el rendimiento de la red bajo condiciones normales y de carga máxima para identificar posibles cuellos de botella.
- **Pruebas de Seguridad:** Realizar pruebas de penetración y auditorías de seguridad para identificar y mitigar vulnerabilidades.

7. Documentación y Capacitación

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Documentación de la Red:** Crear documentación detallada que describa la configuración de la red, incluyendo diagramas, configuraciones de dispositivos y políticas de seguridad.
- **Capacitación de Personal:** Proporcionar capacitación al personal de TI sobre la gestión y el mantenimiento de la red.

8. Implementación y Monitoreo

- **Despliegue de la Red:** Implementar la red siguiendo el diseño planificado y la documentación.
- **Monitoreo Continuo:** Implementar herramientas de monitoreo para supervisar el rendimiento y la seguridad de la red en tiempo real.
- **Mantenimiento y Actualizaciones:** Establecer un plan de mantenimiento regular y actualizaciones para asegurar la continuidad y la mejora del servicio.

9.4. Selección de Hardware y Software para el diseño de red de datos

La selección adecuada de hardware y software es crucial para el diseño de una red de datos eficiente, segura y escalable. A continuación, se presentan los componentes clave y las consideraciones necesarias para elegir el hardware y software apropiados.

9.4.1. Hardware de Red

1. **Routers**
    - **Función:** Dirigen el tráfico entre diferentes redes, esencial para la comunicación entre la red local (LAN) y la red amplia (WAN).
    - **Consideraciones:**
    - **Capacidad de procesamiento:** Debe manejar el volumen de tráfico esperado.
    - **Puertos y Interfaces:** Suficientes puertos LAN/WAN y soporte para interfaces como Ethernet, fibra óptica, etc.
    - **Características Adicionales:** Soporte para protocolos de enrutamiento avanzados (BGP, OSPF), seguridad integrada (firewall, VPN), y capacidades de gestión remota.
2. **Switches**

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Función:** Conectan múltiples dispositivos dentro de la red local, facilitando la comunicación interna.
- **Consideraciones:**
    - **Capacidad de Puertos:** Número de puertos necesarios, con opción de expansión.
    - **Velocidad de Puertos:** Soporte para velocidades de 1Gbps, 10Gbps, según las necesidades.
    - **Administración:** Switches gestionados para control avanzado de tráfico, VLANs, QoS.
    - **PoE (Power over Ethernet):** Útil para alimentar dispositivos como puntos de acceso y cámaras IP.

3. **Firewalls**
    - **Función:** Proteger la red contra accesos no autorizados y amenazas externas.
    - **Consideraciones:**
    - **Capacidad de Procesamiento:** Para manejar el tráfico sin degradar el rendimiento.
    - **Características de Seguridad:** Filtrado de paquetes, inspección profunda de paquetes (DPI), prevención de intrusiones (IPS).
    - **Gestión y Monitoreo:** Capacidades de gestión centralizada y registro detallado de eventos.
4. **Puntos de Acceso (AP)**
    - **Función:** Proveer conectividad inalámbrica dentro de la red.
    - **Consideraciones:**
        - **Capacidad de Usuarios:** Capacidad de manejar múltiples conexiones simultáneas.
        - **Estándares Wi-Fi:** Compatibilidad con los últimos estándares (Wi-Fi 6).
        - **Cobertura y Escalabilidad:** Capacidad de expandir la cobertura con más puntos de acceso.
5. **Servidores**
    - **Función:** Alojar aplicaciones, servicios y archivos.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Consideraciones:**
    - **Capacidad de Procesamiento y Almacenamiento:** Suficiente CPU, RAM y almacenamiento para las aplicaciones y datos.
    - **Redundancia:** RAID, fuentes de alimentación redundantes, etc.
    - **Sistema Operativo:** Compatibilidad con el software de red y aplicaciones.

6. **Cables y Conectores**
    - **Función:** Conectar físicamente los dispositivos de la red.
    - **Consideraciones:**
        - **Tipos de Cables:** Cat5e, Cat6, fibra óptica, según las necesidades de velocidad y distancia.
        - **Calidad y Longitud:** Cables de calidad para evitar pérdidas de señal y adecuadas longitudes según el diseño físico.

9.4.2. Software de Red

1. **Sistemas Operativos de Red**
    - **Función:** Gestionar la infraestructura de red y los dispositivos conectados.
    - **Ejemplos:** Windows Server, Linux (Ubuntu Server, CentOS), etc.
2. **Software de Gestión de Red**
    - **Función:** Monitorear y administrar el rendimiento y la seguridad de la red.
    - **Consideraciones:**
        - **Capacidades de Monitoreo:** Análisis de tráfico, detección de fallos, alertas.
        - **Gestión Centralizada:** Interfaz para administrar múltiples dispositivos y configuraciones.
        - **Compatibilidad:** Compatible con el hardware y otros sistemas de la red.
3. **Software de Seguridad**
    - **Función:** Proteger la red contra amenazas y ataques.
    - **Ejemplos:** Antivirus, anti-malware, sistemas de detección y prevención de intrusiones (IDS/IPS).
4. **Software de Virtualización**

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

- **Función:** Permitir la creación y gestión de máquinas virtuales.
- **Ejemplos:** VMware, Microsoft Hyper-V, Proxmox.

5. **Aplicaciones de Red**
   - **Función:** Proveer servicios específicos como servidores web, servidores de correo, etc.
   - **Ejemplos:** Apache, Nginx, Microsoft Exchange.
6. **Herramientas de Subneteo y Planificación de IP**
   - **Función:** Ayudar en la planificación y gestión de direcciones IP y subredes.
   - **Ejemplos:** SolarWinds IP Address Manager, Gestores de IPAM.

10. Enrutamientos y comunicación

El enrutamiento y la comunicación son componentes esenciales en la estructura y funcionalidad de las redes de datos. El enrutamiento se refiere al proceso de seleccionar las mejores rutas en una red para enviar datos desde el origen hasta el destino. La comunicación abarca los métodos y protocolos que permiten el intercambio de información entre dispositivos en una red. A continuación, se detallan los aspectos clave del enrutamiento y la comunicación en redes de datos.

10.1. Enrutamiento

Cuando hablamos sobre enrutamiento en redes informáticas estamos haciendo referencia al proceso de selección de un camino para la transferencia de la información. Los principios de un enrutamiento son aplicables más allá del ámbito informático y sirven para hablar sobre redes telefónicas e incluso de redes de transporte.

En lo que se refiere a las redes informáticas, el enrutamiento se encarga de seleccionar las rutas por las que discurren los paquetes de información. Por ejemplo, en el caso de Internet, los paquetes del protocolo IP. Estas decisiones sobre el camino a seguir por la información son tomadas por distintas piezas de hardware conocidas como routers o enrutadores. (Tokio School, 2024)

10.2. Tipos de Enrutamientos

Existen dos tipos fundamentales de establecer el enrutamiento en las redes informáticas:

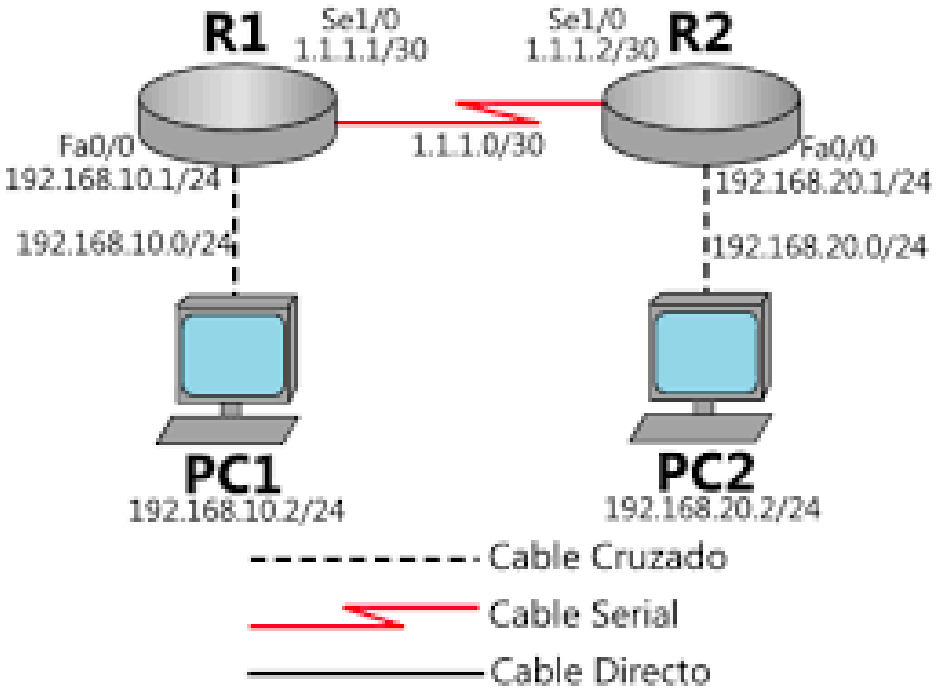
(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

10.2.1. Enrutamiento Estático

El enrutamiento estático es aquel en el que el administrador de la red debe encargarse de configurar manualmente cada uno de los routers que forman la misma. Cuando se lleva a cabo este tipo de enrutamiento hay que acceder a cada router, configurarlo individualmente y enseñarle cada una de las rutas existentes.

Este tipo de enrutamiento hace más fácil el mantenimiento de las tablas de enrutamiento en redes muy pequeñas, en las que se sabe previamente que no va a haber un aumento significativo de la misma. Normalmente, utiliza una única ruta por defecto o predeterminada que es la que dirige el tráfico hacia cualquier red que no tenga coincidencia con otra ruta de la tabla de routing.

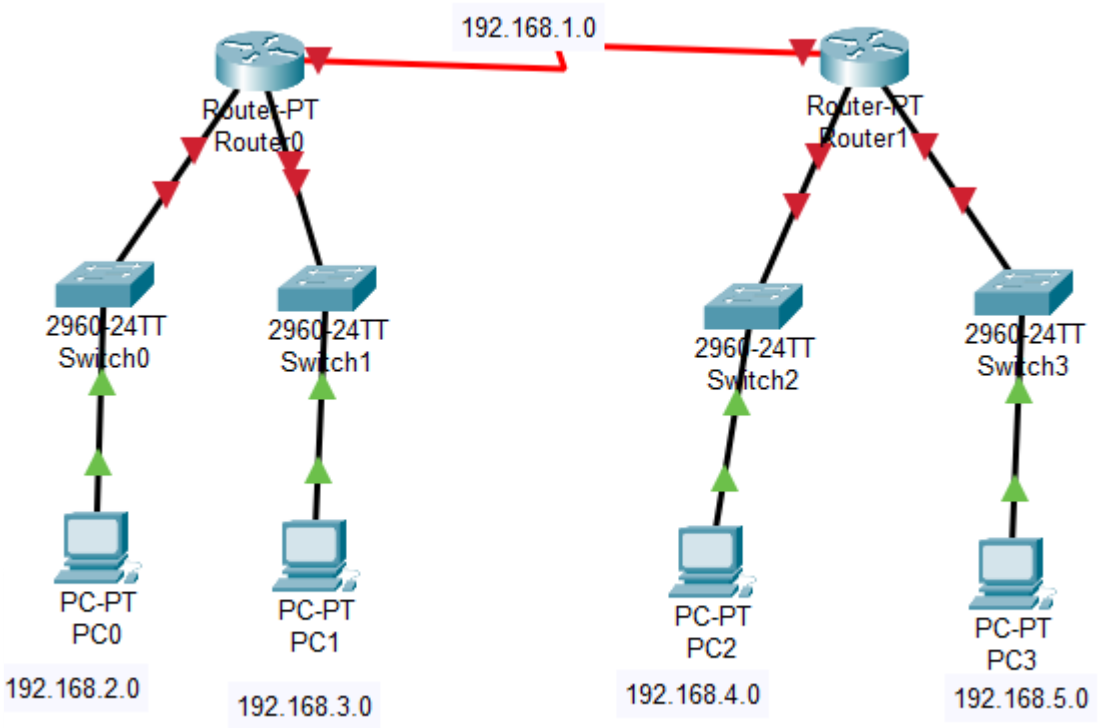
Por lo indicado anteriormente, el enrutamiento estático se utiliza principalmente en redes con una cantidad pequeña de routers, las cuales tienen un solo gateway. Cuando se lleva a cabo este tipo de configuración, hay que especificar en cada router la IP de destino, la IP del router por la que se envían los paquetes, la distancia y la máscara de red. (Limones, 2021)



Ejemplo:

Diseñar y configurar la siguiente red en cisco Packet tracert, para la comunicación entre redes utilizar enrutamiento dinámico.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC



Configuración de IPs

Router A

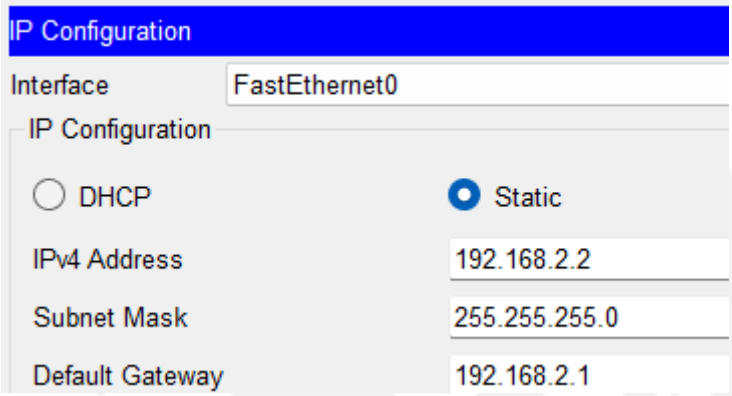
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config)#interface f1/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown

Router(config)#interface s2/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down
```

Router B

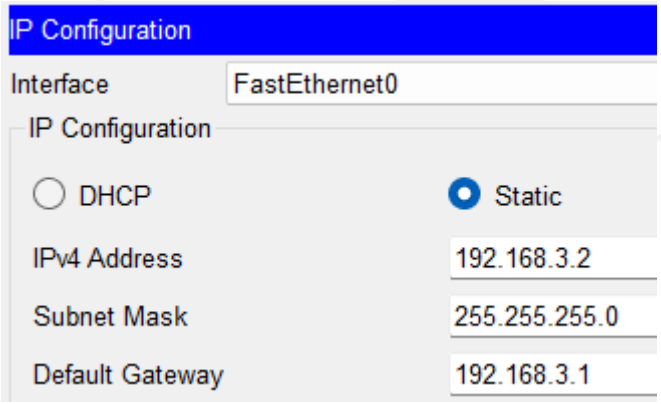
(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shutdown

Router(config)#interface f1/0
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#no shutdown

Router(config)#interface s2/0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown
```

PC0

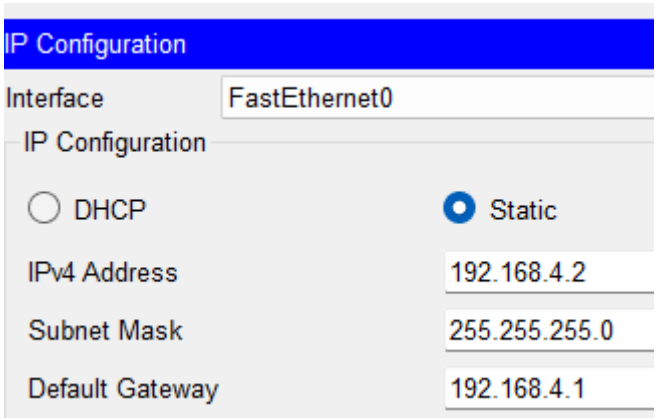


PC1

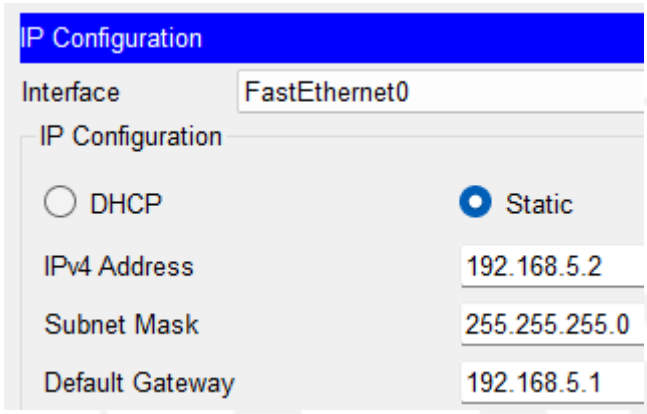


PC2

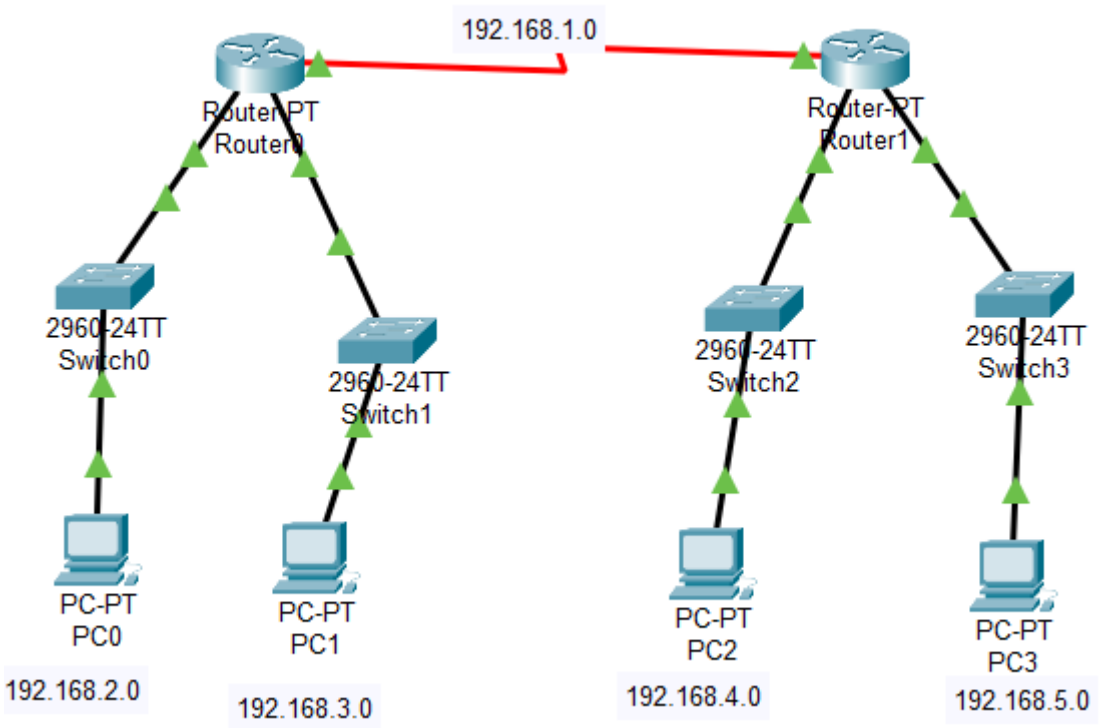
(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC



PC3



Resultado después de las configuraciones de IPs



(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Configuración del enrutamiento estático

Router A

```
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.1.0
Router(config)#ip route 192.168.5.0 255.255.255.0 192.168.1.0
```

Router B

```
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.0
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.1.0
```

Comprobación

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	
	Successful	PC3	PC1	ICMP		0.000	N	1	(edit)	

Enrutamientos dinámicos

El enrutamiento dinámico se basa en la utilización o empleo de protocolos de enrutamiento con el fin de automatizar el intercambio y la actualización de las tablas de enrutamiento de cada uno de los routers. Estos protocolos comparten las tablas de enrutamiento de forma automática con los routers cercanos, lo que hace que su utilización sea recomendada para redes grandes.

Si tenemos una red en la que utilizamos este tipo de enrutamiento, no importará la cantidad de routers que contenga, ya que podremos ir agregando en ella nuevos equipos y automáticamente todos los routers los conocerán sin necesidad de configurar cada uno de ellos de forma individualizada. Todo es automático, por ejemplo, si elimino una red WAN o LAN todos los equipos sabrán que no existe y no enviarán paquetes a la misma. O si, por el contrario, la agrego, todos la conocerán y podrán comunicarse con ella.

Es fundamental comprender que, en este caso, los routers se comunican unos a otros las redes a las que están conectados, lo que lo hace mucho más rápido y eficiente. (Limones, 2021)

RIP

El Routing Information Protocol (RIP) es uno de los protocolos de enrutamiento más antiguos y sencillos que se utilizan para determinar las rutas en redes IP. Originalmente desarrollado en la década de 1980, RIP ha sido ampliamente adoptado en redes pequeñas y

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

medianas debido a su simplicidad y facilidad de implementación. A continuación, se presenta una descripción detallada de RIP, sus características, funcionamiento y consideraciones para su uso.

RIP utiliza un algoritmo de vector distancia para decidir en qué ruta colocar un paquete para llegar a su destino. Cada router RIP mantiene una tabla de routing, que es una lista de todos los destinos que el router sabe cómo llegar. Cada router transmite su tabla de routing completa a sus vecinos/neighbors más cercanos cada 30 segundos. En este contexto, los vecinos son los otros routers a los que un router está conectado directamente, es decir, los otros routers en los mismos segmentos de red que el router seleccionado. Los vecinos, a su vez, pasan la información a sus vecinos más cercanos, y así sucesivamente, hasta que todos los hosts RIP dentro de la red tengan el mismo conocimiento de las rutas de routing . Este conocimiento compartido se conoce como convergencia.

Si un router recibe una actualización en una ruta y la nueva ruta es más corta, actualizará la entrada de la tabla con la longitud y la dirección del siguiente salto de la ruta más corta. Si la nueva ruta es más larga, esperará un período de "*retención*" para ver si las actualizaciones posteriores también reflejan el valor más alto. Solo actualizará la entrada de la tabla si se ha determinado que la nueva ruta más larga es estable.

Si un router falla o se corta una conexión de red, la red descubre esto porque ese router deja de enviar actualizaciones a sus vecinos o deja de enviar y recibir actualizaciones a lo largo de la conexión cortada. Si una ruta determinada en la tabla de routing no se actualiza en seis ciclos de actualización sucesivos (es decir, durante 180 segundos), un router RIP descartará esa ruta y permitirá que el resto de la red conozca el problema a través de sus propias actualizaciones periódicas. (CCNA, 2024)

Versiones de RIP

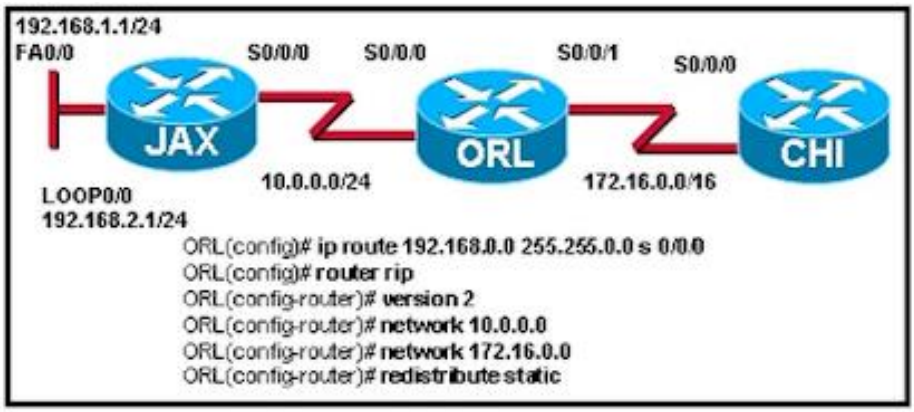
Existen tres versiones del Protocolo de información de enrutamiento: RIPv1, RIPv2 y RIPng.

RIPv1, estandarizado en 1988, también se denomina Protocolo de enrutamiento con clase porque no envía información de máscara de subred en sus actualizaciones de routing. Por otro lado, RIPv2, estandarizado en 1998, se llama Protocolo de enrutamiento sin clase porque envía información de máscara de subred en sus actualizaciones de routing. RIPng es una extensión de RIPv2 que se creó para admitir IPv6.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

En RIPv1, las rutas se deciden en función del destino de IP y el conteo de saltos. RIPv2 avanzó este método y comenzó a incluir máscaras de subred y puertas de enlace. Además, la tabla de routing en RIPv1 se transmite a todas las estaciones de la red conectada, mientras que RIPv2 envía la tabla de routing a una dirección de multidifusión en un esfuerzo por reducir el tráfico de red. Además, RIPv2 usa autenticación para seguridad, una característica que falta en RIPv1.

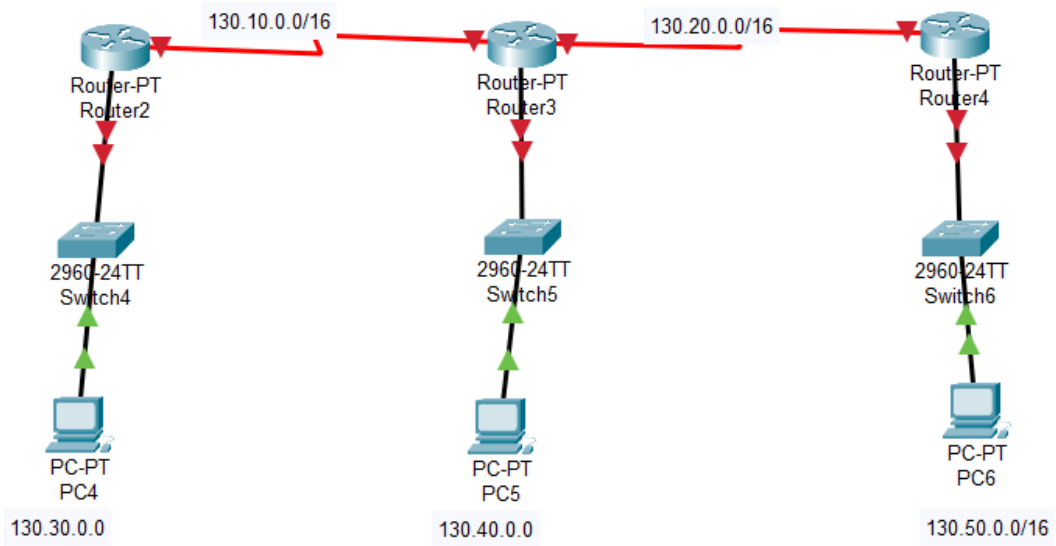
Ilustración 40:
Enrutamiento dinámico



Nota: *en la ilustración se puede observar la configuración de un router con el enrutamiento RIPv2*

Ejemplo:

Configurar la siguiente red de datos y utilizar en enrutamiento RIP para la comunicación entre redes



(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Router A

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#ip address 130.10.0.1 255.255.0.0
Router(config-if)#ip address 130.10.0.1 255.255.0.0
Router(config-if)#no shutdown

Router(config-if)#ip address 130.30.0.1 255.255.0.0
Router(config-if)#no shutdown
```

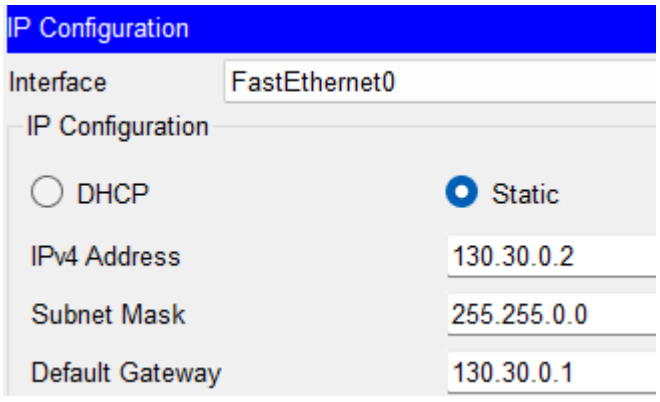
Router B

```
Router(config)#interface Serial2/0
Router(config-if)#ip address 130.10.0.2 255.255.0.0
Router(config-if)#ip address 130.10.0.2 255.255.0.0
Router(config-if)#no shutdown

Router(config-if)#ip address 130.40.0.1 255.255.0.0
Router(config-if)#no shutdown

Router(config-if)#ip address 130.20.0.1 255.255.0.0
Router(config-if)#no shutdown
```

Router C

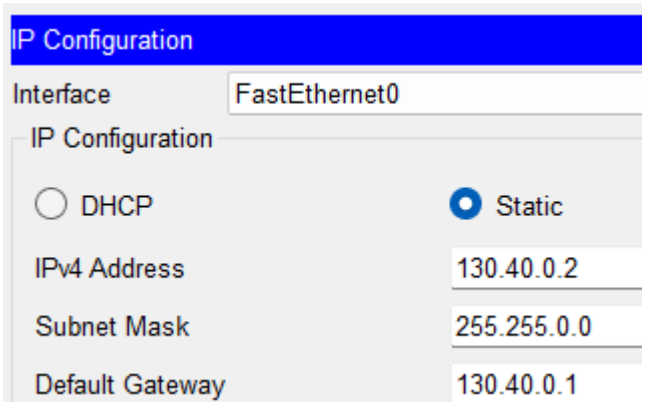
```
Router(config)#interface Serial2/0
Router(config-if)#ip address 130.20.0.2 255.255.0.0
Router(config-if)#ip address 130.20.0.2 255.255.0.0
Router(config-if)#no shutdown
```

PC4

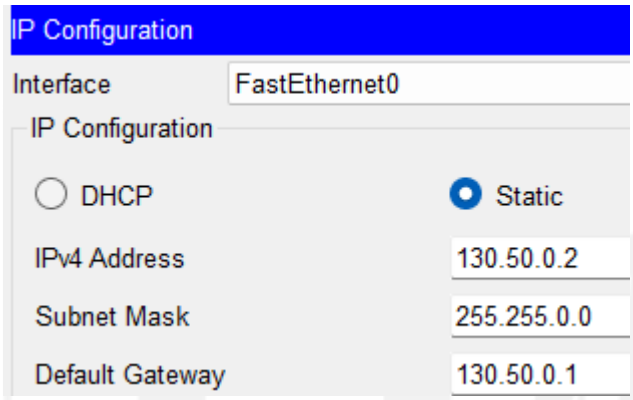


PC5

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC



PC6



Configuración del enrutamiento RIP

Router A

```
Router(config)#router rip
Router(config-router)#network 130.10.0.0
Router(config-router)#network 130.30.0.0
```

Router B

```
Router(config)#router rip
Router(config-router)#network 130.10.0.0
Router(config-router)#network 130.20.0.0
Router(config-router)#network 130.40.0.0
```

Router C

```
Router(config)#router rip
Router(config-router)#network 130.20.0.0
Router(config-router)#network 130.50.0.0
```

Prueba de comunicación

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

```
C:\>ping 130.50.0.2

Pinging 130.50.0.2 with 32 bytes of data:

Reply from 130.50.0.2: bytes=32 time=11ms TTL=125
Reply from 130.50.0.2: bytes=32 time=12ms TTL=125
Reply from 130.50.0.2: bytes=32 time=10ms TTL=125
Reply from 130.50.0.2: bytes=32 time=10ms TTL=125

Ping statistics for 130.50.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 10ms
```

Autoevaluación 3

Instrucciones: Responde las siguientes preguntas seleccionando la opción correcta.

1. ¿Qué función desempeñan los protocolos de enrutamiento en una red de computadoras?
    a) Establecer conexiones físicas entre dispositivos.
    b) Determinar la mejor ruta para el envío de datos.
    c) Gestionar la seguridad de la red.
2. ¿Cuál es la principal diferencia entre el enrutamiento estático y el enrutamiento dinámico?
    a) El enrutamiento estático es más seguro que el enrutamiento dinámico.
    b) El enrutamiento estático requiere una configuración manual, mientras que el enrutamiento dinámico ajusta automáticamente las rutas.
    c) El enrutamiento estático solo se utiliza en redes pequeñas.
3. ¿Qué protocolo de enrutamiento es conocido por su uso en redes de tamaño pequeño y medio, pero no es adecuado para redes grandes debido a su convergencia lenta?
    a) RIP (Routing Information Protocol).
    b) OSPF (Open Shortest Path First).
    c) EIGRP (Enhanced Interior Gateway Routing Protocol).

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

4. ¿Cuál es uno de los beneficios del enrutamiento dinámico sobre el enrutamiento estático?

    a) Mayor control sobre la ruta de los paquetes.

    b) Mayor facilidad de configuración en redes grandes y complejas.

    c) Mejor rendimiento en redes pequeñas.

5. ¿Qué aspecto del diseño de redes se refiere a la disposición física y lógica de los dispositivos de red y los cables que los conectan?

    a) Topología de red.

    b) Seguridad de red.

    c) Capa de aplicación.

6. ¿Cuál de las siguientes herramientas se utiliza comúnmente para monitorear y gestionar dispositivos de red de forma remota?

    a) SNMP (Simple Network Management Protocol).

    b) FTP (File Transfer Protocol).

    c) HTTP (Hypertext Transfer Protocol).

7. ¿Cuál es uno de los principales objetivos de implementar redes redundantes en el diseño de una red de comunicaciones?

    a) Reducir la velocidad de la red.

    b) Mejorar la escalabilidad de la red.

    c) Aumentar la fiabilidad y la disponibilidad de la red.

8. ¿Qué método de autenticación se utiliza comúnmente para garantizar que solo los usuarios autorizados tengan acceso a la red?

    a) WEP (Wired Equivalent Privacy).

    b) WPA (Wi-Fi Protected Access).

    c) WPS (Wi-Fi Protected Setup).

9. ¿Cuál es una de las amenazas comunes a la seguridad de la red que puede resultar en la interceptación de datos confidenciales?

    a) Ataque de denegación de servicio (DoS).

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

b) Ingeniería social.

c) Ataque de sniffing.

10. ¿Qué protocolo se utiliza para asignar direcciones IP de forma dinámica a los dispositivos en una red?

a) DNS (Domain Name System).

b) DHCP (Dynamic Host Configuration Protocol).

c) ARP (Address Resolution Protocol).

Respuestas:

1. Respuesta: b) Determinar la mejor ruta para el envío de datos.
2. Respuesta: b) El enrutamiento estático requiere una configuración manual, mientras que el enrutamiento dinámico ajusta automáticamente las rutas.
3. Respuesta: a) RIP (Routing Information Protocol).
4. Respuesta: b) Mayor facilidad de configuración en redes grandes y complejas.
5. Respuesta: a) Topología de red.
6. Respuesta: a) SNMP (Simple Network Management Protocol).
7. Respuesta: c) Aumentar la fiabilidad y la disponibilidad de la red.
8. Respuesta: b) WPA (Wi-Fi Protected Access).
9. Respuesta: c) Ataque de sniffing.
10. Respuesta: b) DHCP (Dynamic Host Configuration Protocol).

Resumen de la Unidad 3

La unidad "Enrutamiento y Comunicación" proporciona una visión integral sobre los principios fundamentales del enrutamiento y la comunicación en redes de computadoras. En esta unidad, los estudiantes exploran los conceptos básicos del enrutamiento, incluyendo la diferencia entre enrutamiento estático y dinámico, así como los protocolos de enrutamiento más comunes como RIP, OSPF y EIGRP. Además, se abordan temas relacionados con el diseño eficiente de redes para facilitar la comunicación entre dispositivos, la implementación de redes redundantes para mejorar la fiabilidad y disponibilidad de la red, y las herramientas de monitoreo y gestión utilizadas para administrar dispositivos de red de forma remota. Asimismo,

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

se examinan aspectos de seguridad en la comunicación y el enrutamiento, como la autenticación de usuarios y la prevención de amenazas a la seguridad de la red. Al finalizar la unidad, los estudiantes habrán adquirido un conocimiento sólido sobre cómo configurar, administrar y asegurar eficazmente las redes de comunicaciones en entornos diversos.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Bibliografía

adaptive. (4 de junio de 2024). *vitc*. Obtenido de https://vestertraining.com/blog/protocolos-red/

AVG. (21 de febrero de 2024). Obtenido de https://www.avg.com/es/signal/what-is-tcp-ip

aws. (21 de febrero de 2024). Obtenido de https://aws.amazon.com/es/what-is/wan/

AXXES. (30 de noviembre de 2022). Obtenido de https://axessnet.com/topologias-de-red/

Blogger. (4 de junio de 2024). Obtenido de https://grd1503687jjfdog.blogspot.com/p/modelo-osi.html

CCNA. (4 de junio de 2024). Obtenido de https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp3.pdf

CCNA. (19 de junio de 2024). Obtenido de https://ccnadesdecero.es/routing-information-protocol-rip/

CIDECAME. (13 de junio de 2024). Obtenido de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro35/144_capas_con_modelos_tcpip_y_osi.html

Cloudflare. (14 de junio de 2024). Obtenido de https://www.cloudflare.com/es-es/learning/ddos/glossary/hypertext-transfer-protocol-http/

CLOUDFLARE. (21 de Febrerro de 2024). Obtenido de https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-lan/

Colegio Ártica. (24 de febrero de 2024). Obtenido de https://pacsobreredesinformaticas.wordpress.com/medios-de-transmision/

Compara Hosting . (21 de febrero de 2024). Obtenido de https://www.comparahosting.com/diferencia-http-https/

Concepto. (4 de junio de 2024). Obtenido de https://concepto.de/modelo-osi/

DONGEE. (2023 de abril de 23). Obtenido de https://www.dongee.com/tutoriales/nodos-de-red/#:~:text=Un%20nodo%20de%20red%20es,permite%20intercambiar%20datos%20e%20informaci%C3%B3n.

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Etece. (19 de noviembre de 2023). *Concepto*. Obtenido de https://concepto.de/red-de-computadoras/

Fernández, Y. (18 de abril de 2024). *Xataka*. Obtenido de https://www.xataka.com/basics/ftp-que-como-funciona

Fortinet. (19 de junio de 2024). Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/network-traffic#:~:text=El%20an%C3%A1lisis%20de%20tr%C3%A1fico%20de,e%20identificar%20la%20actividad%20inusual.

HOSTINET. (21 de febrero de 2024). Obtenido de https://www.hostinet.com/formacion/hosting-alojamiento/que-es-una-direccion-ip-publica/

InGenio Learning . (14 de junio de 2024). Obtenido de https://ingenio.edu.pe/blog/como-disenar-una-red-conceptos-basicos-herramientas/

Julio, I. (15 de Septiembre de 2015). Obtenido de https://grupo4herramientasinformatica.blogspot.com/2012/08/cipa-4-bloc-para-herramientas-de.html

Limones, E. (24 de septiembre de 2021). *OpenWebinars*. Obtenido de https://openwebinars.net/blog/enrutamiento-estatico-vs-dinamico/

López, Á. H. (s.f.). *concepto básico de redes de datos: Redes LAN volumen I.* Editorial CORHUILA.

Mallón, X. (23 de abril de 2024). *Keeocoding*. Obtenido de https://keepcoding.io/blog/que-es-subnetting/

Redes Inalambricas y cableadas . (21 de febrero de 2024). Obtenido de https://redesinalambricasycableadas.wordpress.com/redes-cableadas/diferentes-topologias-de-red/topologia-de-estrella/

Robledano, A. (19 de junio de 2019). *OpenWebinars*. Obtenido de https://openwebinars.net/blog/que-es-tcpip/

Sistemas en redes informáticas. (21 de febrero de 2024). Obtenido de https://sistemasenredes.com/

Todo para los informáticos. (24 de febrero de 2024). Obtenido de https://todoparainformaticos.blogspot.com/p/medios-de-transmision-de-datos.html

Tokio School. (19 de junio de 2024). Obtenido de https://www.tokioschool.com/enrutamiento/

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC

Topologías de red. (21 de febrero de 2024). Obtenido de https://topologiasdered.com/red-en-bus/

Topologías físicas de red. (21 de febrero de 2024). Obtenido de http://new-prestige.weebly.com/topologigravea-de-anillo.html

WIKIDOT. (21 de Febrero de 2024). Obtenido de http://orgullosamentenormalista.wikidot.com/principales-topologias-de-red

(+593) 96 356 1961 admisiones@itq.edu.ec Antonio de Ulloa N28-30 y Diego de Atienza (Esq). WWW.ITQ.EDU.EC