

Redes en la actualidad

1.0 Introducción

Pasos para la instalación del software Packet Tracer que es un programa de software flexible que te dará la oportunidad de usar las representaciones de red y teorías de la construcción de los modelos de red, explorar LAN y WAN. Packet Tracer permite simular redes reales. Función:

- Agregar dispositivos y conectarlos a través de cables o inalámbricos.
- Seleccionar, eliminar, inspeccionar, etiquetar y agrupar componentes dentro de la red.
- Administrar una red existente o de muestra.

1.1 Las redes afectan nuestras vidas

La necesidad de interactuar está después de sustentar la vida. La conexión de esta interacción son las redes. Cisco menciona que los cambiadores del mundo se hacen y no se nacen trabajando hacia la educación y desarrollo de habilidades de la próxima generación de talentos.

El avance de tecnologías de red son los agentes de cambio más significativos donde las limitaciones físicas y geográficas no son más importantes para la actualidad. La red más importante es Internet, la creación de la nube nos permite almacenar documentos, imágenes, accediendo a ellos en cualquier lugar y en cualquier momento.

1.2 Componentes de la red

• **Roles de host** → Hosts son todas las computadoras que están conectadas a una red y participan en la comunicación de la misma. Los hosts pueden llamar a dispositivos finales, también se llaman clientes. **Dispositivos de la red** a los que se le asigna un número para comunicación. Ese número se llama dirección de protocolo de Internet (IP) la cual identifica al host y la red a la que está conectado.

Los **servidores** son computadoras con software que proporciona información como correo electrónico, páginas web a dispositivos finales de la red. Un servicio requiere un software de servidor y una computadora con software de servidor puede proporcionar servicios a clientes diferentes.

Los **clientes** son un tipo de host que disponen de software para solicitar y mostrar información obtenida del servidor. (chrome, navegadores)

cliente



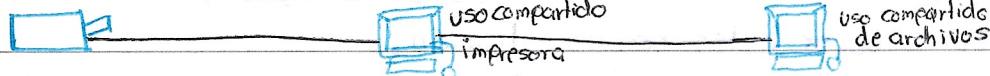
Internet

Servidor

D	M	A

Scribe

- Pares → Una red entre pares es el uso de una computadora para 2 roles al mismo tiempo el rol de cliente con el software de cliente y el rol del Servidor con el software del Servidor en una red.



Ventajas:

Desventajas:

- Fácil configuración
- Menos complejidad
- Menor costo
- Tareas sencillas
- Administración no centralizada
- No es tan segura
- No son escalables
- Lentificar el rendimiento

- Dispositivos finales → Son los dispositivos que se familiarizan con las personas en la actualidad, cada uno tiene una dirección en la red, cuando inicia la comunicación utiliza la dirección del dispositivo final de destino para especificar donde entregar el mensaje. La terminal es el origen o destino de un mensaje transmitido por la red.

- Dispositivos intermedios → Son los dispositivos intermedios que conectan a los dispositivos finales individuales a la red. Puede formar una red interna, proporciona conectividad y garantiza el flujo de datos en la red. Utiliza la dirección del host destino y las interconexiones de la red para la ruta del mensaje.

Ejemplos: Router inalámbrico, switch de multicapa, switch LAN, Dispositivo Firewall, ROUTER, apilados

Ellos pueden regenerar y retransmitir señales de comunicación, conservar información de rutas, Notificar errores, dirigir datos, permitir o denegar datos por seguridad.

- Medios de red → Proporciona el canal por donde viaja el mensaje de inicio a fin.

Tipos de medios que interconectan dispositivos:

- Hilos metálicos dentro de cables → Los datos se codifican en impulsos eléctricos.
- Fibra de vidrio o plástico (Fibra óptica) → Datos codificados como pulsos de luz.
- Transmisión inalámbrica → Datos codificados de modulación de ondas electromagnéticas.

1.3 Topologías y representaciones de red

Los encargados del aspecto de la red, componentes, ubicación, donde se conectan los dispositivos en la red son los arquitectos y administradores.

Dispositivos y conexiones que forman una red:

Medios de red: Inalámbricos, Medios LAN, Medios WAN

Dispositivos finales: computadoras de escritorio, laptop, impresora, teléfono IP, televisor.

Dispositivos intermediarios: Router inalámbrico, switch LAN, Router, switch multicapa, fire wall.

Un diagrama de topología es una representación lógica de los componentes físicos de la red para comprender como se conectan estos dispositivos y el funcionamiento de una red.

Descripción de como se conectan entre sí:

- Tarjeta de interfaz de red (NIC) → conecta físicamente el dispositivo final a la red.
- Puerto Físico → Conector o conexión en un dispositivo de red que se conectan los medios a un terminal o dispositivo de red.
- Interfaz → Puertos especializados en el dispositivo de red para redes individuales.

Un router conecta redes con frecuencia, sus puertos se denominan **interfaces de red**.

- Diagramas de topología → Documentación obligatoria que muestra un mapa visual de como está conectada la red.

Topologías Físicas Ilustran la ubicación física de dispositivos intermedios y la instalación del cable, las habitaciones están etiquetadas en esta topología.

Topologías lógicas Ilustran dispositivos, puertos y esquema de direccionamiento de la red. Dispositivos finales conectados a los intermedios y medios utilizados.

1.4 Tipos comunes de redes

- Redes de muchos tamaños → Existen redes de muchos tamaños desde la conexión de 2 PC's las cuales permiten compartir recursos como impresoras, imágenes, documentos y música, las redes de oficina pequeñas o domésticas se llaman **SOHO**.

Las empresas usan redes para dar consolidación, almacenamiento y acceso a la información en los servidores. **Internet** es la red más extensa que existe el mundo.

Significa "red de redes" y es una colección de redes privadas y públicas interconectadas. La red doméstica conecta dispositivos a internet, la red SOHO permite conexión a una red corporativa o compartir recursos centralizados, la red mediana o grande pueden tener muchas ubicaciones con miles de hosts conectados. Redes mundiales es el internet que conecta millones de computadoras.

- LAN y WAN → La infraestructura de una red varía en lo siguiente:

Tamaño del área que abarca, cantidad de usuarios conectados, cantidad y servicios disponibles, área de responsabilidad.

LAN → Infraestructura que abarca un área pequeña, interconectan terminales en áreas como casa, edificio, oficina o campus, casi siempre la administración

está a cargo de una única organización o persona, proporciona ancho de banda a hosts, intermedios.

WAN → Infraestructura de red que abarca un área extensa, administradas por proveedores de servicios (SP) o Proveedores de Servicios de Internet (ISP), estas interconectan LAN entre estados, ciudades, países o continentes, proporcionan enlaces de velocidad más lento entre LAN's.

- **Internet** → Colección global de redes interconectadas, algunas redes LAN están interconectadas a través de una WAN y las WAN están interconectadas entre sí, este mismo garantiza una comunicación efectiva es una infraestructura heterogénea aplicando estándares y tecnologías uniformes. Algunas organizaciones mantienen la estructura y protocolos de internet como (IETF), (ICANN), (IAB).
- **Intranets y extranets** → Intranet se refiere a la conexión privada de LAN y WAN que hay en una organización, solo se accede entre miembros y empleados de la organización. Extranet proporciona acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la empresa. Un ejemplo serían los proveedores, clientes y colaboradores.

1.5 Conexiones a internet

- **Tecnologías de acceso** → Los usuarios domésticos, oficinas pequeñas requieren conexión ISP para tener internet, se varía mucho entre las conexiones ISP y conexiones por ubicación. Las más utilizadas son banda ancha por cable, por línea de suscriptor digital (DSL), WAN inalámbricas y servicios móviles. Los SPs ofrecen conexiones de nivel empresarial los cuales cuentan con DSL, líneas arrendadas y red Ethernet.
- **Domésticas y oficinas** → **Cable** → señal transmitida en el cable de la TV de pago, gran ancho de banda, alta disponibilidad y conexión activa. **DSL** → Línea de suscriptor digital transportada por la línea de teléfono conectándolo por una línea de suscriptor digital asimétrica (ADSL) mayor velocidad de descarga a la de carga. **Celular** → Su acceso a internet utiliza una red de telefonía celular dependiendo de su cobertura móvil para acceder, esta se ve afectada por la capacidad del celular y la torre que este conectado. **Satelital** → Beneficia a las áreas que de otra manera no tendrían conexión, mediante antenas parabólicas mandan señal y se requiere una línea de vista despejada al satélite. **Telefonía Dial-up** → Bajo costo en su servicio funcionando con teléfono y módem, su conexión es baja y no es suficiente para datos masivos, útil para viajes.

- Conexiones a internet empresariales → Hay diferencias para las conexiones empresariales debido a que necesitan más ancho de banda y servicios administrados. Las conexiones más utilizadas son:

Líneas arrendadas dedicadas → Circuitos reservados en la red del proveedor que conectan oficinas separadas por ubicación por redes privadas de datos o voz alquilados mensual o anualmente. Metro Ethernet → Ethernet WAN o MAN extiende el acceso LAN a la WAN. DSL empresarial → Varios formatos conforman esta red pero la más utilizada es la (SDSL) Suscriptor digital simétrica, similar a DSL pero proporciona misma velocidad de carga y descarga. Satelital → Proporcionada cuando una solución por cable no está disponible.

- Red convergente → Separadores tradicionales → Las conexiones de cable para datos, telefonía y red de video iban separadas y no se comunican entre sí cada red tenía sus estándares y reglas. Multiples servicios en multiples redes. redes convergentes → La red de datos, telefonía y video transmiten datos, voz, video entre dispositivos en la misma infraestructura, mismas regla y estándares. Multiples servicios en una sola red.

1.6 Redes confiables

- Arquitectura de red → Al tener millones de conexiones 24/7 se necesita fiabilidad con ella tenemos 4 aspectos que confirman su fiabilidad, es importante recalcar que una red se debe crear sobre la base de una arquitectura de red estándar para garantizar funcionalidad y crecimiento al entorno. Una arquitectura de red es la tecnología que dan soporte a la infraestructura, servicios, protocolos, reglas programados para trasladar datos en la red.
- Tolerancia a fallas → Aquella que limita la cantidad de dispositivos afectados durante una falla, permite recuperación rápida, dependen de rutas entre el origen y el destino del mensaje, cuando hay varias rutas que conducen a un destino se llama redundancia. Una red packet-switch es una forma de que las redes proporcionen redundancia, Una comunicación de paquetes divide el tráfico en paquetes enrutados en una red compartida, Un archivo se divide en paquetes (bloques de mensajes) contiene dirección de origen y destino y gracias a que los routers estiman la condición de la red los paquetes toman rutas diferentes para llegar al destino. Las conexiones redundantes permiten usar rutas alternativas cuando falla un dispositivo o un enlace.

- Escalabilidad → Una red escalable se expande rápido para admitir nuevos usuarios y apps sin degradar el rendimiento de los servicios de usuarios, los diseñadores siguen estándares y protocolos para su aceptación permitiendo a los proveedores centrarse en mejorar los productos y servicios sin añadir reglas para operar en la red.
- Calidad de servicio → La calidad de servicio(QoS) se convierte en un mecanismo principal para administrar la congestión y garantizar un envío confiable de contenido. Una congestión ocurre cuando se excede el ancho de banda por la demanda que pedimos y agotamos la cantidad disponible. Ancho de banda es la medida bits que se transmiten por segundo, la demanda de ancho de banda puede exceder la disponibilidad congestionando la red. Cuando esto sucede, los dispositivos rebancan los paquetes en cola en la memoria hasta que haya recursos para transmitirlos, la prioridad la tienen los servicios de voz y la última es las páginas web.
- Seguridad de la red → Los administradores deben proporcionar soluciones a los dos problemas de seguridad: seguridad de la infraestructura y seguridad de información. Asegurar la infraestructura incluye asegurar físicamente los dispositivos que proporcionan conectividad y evitar acceso no autorizado. Se puede utilizar hardware y software para evitar el acceso físico a los dispositivos de la red e incluyendo medidas de seguridad para accesos no autorizados. Los requisitos son:
 - Confidencialidad → Solamente los destinatarios deseados puedan acceder a sus datos y leerlos.
 - Integridad → Seguridad de que los datos no se alterarán en la transmisión del origen al destino.
 - Disponibilidad → Tener la seguridad de acceder confiable y oportuna a los servicios de datos para usuarios autorizados.

1.7 Tendencias de red

- Tendencias recientes → Existen varias tendencias de redes que afectan a organizaciones y consumidores como bring your own device(BYOD), colaboración en línea, comunicaciones de video, computación en la nube.
- BYOD → Concepto de traer cualquier dispositivo, cualquier contenido, cualquier manera. Siendo tendencia global con cambios en la forma que usamos los dispositivos, permite a los usuarios finales la libertad de usar herramientas para acceder a información. Significa que se puede usar cualquier dispositivo, de cualquier forma, en cualquier lugar.
- Colaboración en línea → Definida como "El acto de trabajar con otras personas en un proyecto conjunto", las herramientas de colaboración permiten conectar, interactuar y lograr objetivos inmediatamente de sus usuarios.

- Comunicaciones de video → El video se usa para comunicaciones, colaboraciones y entretenimiento. Las video llamadas se realizan de punto a punto con internet. La video conferencia es una herramienta para comunicarse para extenderse a límites geográficos y culturales.
- Computación en la nube → Forma de acceder y almacenar datos, permite almacenar archivos personales, hacer copias de seguridad en servidores a través de internet. Es posible gracias a centros de datos los cuales son instalaciones utilizadas para alojar sistemas informáticos que almacenan estos archivos, se suelen almacenar en centros de datos distribuidos por seguridad, fiabilidad y tolerancia a fallos. Los tipos de nubes son:
Públicas → Apps y servicios basados en la nube ofrecidos en una nube pública disponible para el público en general. Utiliza internet para proporcionar el servicio.
Privadas → Ofrecen una nube privada diseñada para una organización específica, como el gobierno. Se configura la red pero es costoso.
Híbridas → Se compone de 2 o más nubes (privada/pública) cada una es un objeto distinto pero están conectados a la misma arquitectura. Su acceso es basado en derechos de acceso.
Comunitarias → Creada para utilización exclusiva de entidades u organizaciones, se adapta una nube pública con las necesidades personalizadas para la comunidad. Utilizadas por múltiples organizaciones con mismas necesidades y son similares al entorno público pero con los niveles de seguridad, privacidad, reglas de una privada.
- Tendencias tecnológicas en el hogar → Incluida "Tecnología del hogar inteligente". Es integrado en los electrodomésticos de diario para conectarse con otros dispositivos "inteligentes". Esto se volverá más común cuando se expandan las redes domésticas y la velocidad del internet.
- Redes Powerline → Utilizan el cableado eléctrico para conectar dispositivos mediante un adaptador estandar de línea eléctrica, los dispositivos pueden conectarse a la LAN en un enchufe. No hay cables de datos, la red utiliza los cables eléctricos para enviar información por frecuencias. Ideal cuando el punto de acceso inalámbrico no llega a toda la casa.
- Banda Ancha inalámbrica → **WISP** el proveedor de servicios de internet inalámbrico es un ISP que conecta a suscriptores a un punto de acceso con tecnologías inalámbricas similares a las redes WLAN, encontrados en entornos rurales donde DSL no está disponible. Su diferencia principal es que la conexión al proveedor (ISP) es inalámbrica y no por cable físico.
Servicio de banda Ancha → Solución que utiliza la misma tecnología que un teléfono (celular). Se instala una antena fuera del hogar que proporciona conectividad.

1.8 Seguridad de la red

- Amenazas de Seguridad → La seguridad de la red es prioridad de los administradores. Una parte integral de la red informática, independiente del tamaño.

La red debe ser capaz de proteger los datos al mismo tiempo que brinda la calidad que los usuarios esperan. Asegurar una red implica protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y controlar amenazas. Amenazas externas o internas. Externas: **Virus, gusanos, caballos de troya** → Contienen software malicioso que se ejecuta en el dispositivo del usuario. **Spyware y adware** → Tipos de software que se instalan en el dispositivo del usuario, recopila en secreto información del usuario. **Ataques día cero** → o de hora cero, producidos el primer día que se reconoce una vulnerabilidad. **Amenazas de atacantes** → Personas que ataca dispositivos o recursos de red. **Denegación de Servicio** → Ralentizan o bloquean las aplicaciones en un dispositivo de red. **Intercepción y robo de datos** → Ataque que captura información privada de la red de una organización. **Robo de identidad** → Roba credenciales de inicio de sesión para acceder a datos privados.

- Soluciones de seguridad → Sin una solución única la seguridad debe implementarse por capaz dando más de una solución donde si una falla otra puede identificarla. Seguridad en red doméstica:
Antivirus → Protege al dispositivo de software malicioso. **Filtrado Firewall** → Bloquea el acceso no autorizado dentro y fuera de la red. Seguridad redes corporativas: **Sistemas de Firewall dedicados** → Capacidades firewall que filtran grandes cantidades de tráfico con más granularidad. **Listas de control de acceso(ACL)** → Filtran más el acceso y reenvío de tráfico en función de la IP y apps. **Sistema de prevención de intrusiones(IPS)** → Identifican amenazas de rápida propagación, como ataques día cero o hora cero. **Redes privadas Virtuales(VPN)** → Proporciona acceso seguro a una organización para trabajadores remotos.