

Module 1 Componentes de la red

1. Roles de host

Dirección IP: Identifica al host y la red en la que está conectado el host.

- Cliente
- Servidor

2. Entre pares

RED en la que múltiples computadoras tienen el mismo rol. Funcionan como clientes y como servidores al mismo tiempo.

Ventajas de las redes entre pares:

- Fácil de configurar
- Menos complejo
- Menor costo porque es posible que no se necesiten dispositivos de red ni servidores dedicados.
- Se pueden utilizar para tareas sencillas como transferir archivos y compartir impresoras.

Las desventajas de las redes entre pares:

- La administración no está centralizada
- No son tan seguras
- No son escalables
- Todos los dispositivos pueden funcionar como clientes y como servidores, lo que puede dificultar el rendimiento

3. Dispositivos finales

Para comunicarse entre sí dentro de la red utilizan direcciones.

4. Dispositivos intermediarios

EJ: Router, Switch LAN, Switch multicapa, Firewall

Funciones:

- Regenerar y retransmitir señales de comunicación.
- Conservar información acerca de las rutas.
- Notificar a dispositivos de errores y fallas de comunicación.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace.
- Clasificar y dirigir mensajes de acuerdo a las prioridades.
- Permitir o denegar el flujo de datos de acuerdo a los parámetros de seguridad.

5. Medios de red

Cobre, Fibra óptica y Tecnología inalámbrica.

1.3 Topologías y representaciones de red

1.3.1 Diagramas de topología

Diagramas de topologías físicas:

Ilustran la ubicación física de los dispositivos intermedios y la instalación de cable.

Diagramas de topologías lógicas:

Los diagramas de topología lógica ilustran los dispositivos, los puertos y el esquema de direccionamiento de la red.

1.4 Redes de muchos tamaños

Redes Domésticas: Permiten conectar unos pocos ordenadores e dispositivos entre sí.

Redes SOHO: Smart Office Home Office. Son redes para pequeñas oficinas y casas. Para conectar una oficina con la central.

Redes medianas:

Redes mundiales:

1.5 LAN y WAN

LAN: Local area network

- Suelen estar mantenidas por una única persona

WAN: Wide area network

- Interconectan LAN
- Administración a cargo de varios proveedores de servicios.

1.6 Internet

Red no centralizada y heterogénea interconectada.

La implementación de estándares es necesaria para su correcto funcionamiento.

Intranets y extranets:

Intranet: Conexión privada de una empresa.

Extranet: Conexión proporcionada a proveedores, clientes y colaboradores.

1.5 Conexiones a internet

1.5.1 Tecnologías de acceso a internet

Se requiere de un **ISP** para acceder a internet.

Cable - Típicamente ofrecido por los proveedores de servicios de televisión por cable, la señal de datos de Internet se transmite en el mismo cable que ofrece la televisión por cable.

- **DSL** - Las líneas de suscriptor digital también proporcionan un gran ancho de banda, alta disponibilidad y una conexión permanente a Internet. DSL se transporta por la línea de teléfono. En general los usuarios de oficinas en el hogar o pequeñas se conectan mediante una línea de suscriptor digital asimétrica (ADSL), esto implica que la velocidad de descarga es mayor que la velocidad de carga.
- **Celular** - El acceso a internet celular utiliza una red de telefonía celular para conectarse. En cualquier lugar donde tenga cobertura de telefonía móvil, puede tener acceso a Internet.
- **Satelital** - áreas aisladas. Las antenas parabólicas requieren una línea de vista despejada al satélite.
- **Telefonía por Dial-up** - Es una opción de bajo costo que funciona con cualquier línea telefónica y un módem.

1.5.3 Conexiones de internet empresariales:

- **Líneas arrendadas dedicadas** -
- **Metro Ethernet** - Esto a veces se conoce como Ethernet WAN. En este módulo, nos referiremos a él como Metro Ethernet. Metro ethernet extienden la tecnología de acceso LAN a la WAN.
- **DSL empresarial** - línea de suscriptor digital simétrica (SDSL), que es similar a la versión de DSL para el consumidor, pero proporciona las mismas velocidades de subida y descarga.
- **Satelital** - El servicio satelital puede proporcionar una conexión cuando una solución por cable no está disponible.

1.5.4 Redes convergentes

Redes separadas tradicionales:

Red de televisor, telefonía y datos separadas. No podían comunicarse entre sí.

Redes convergentes:

Mediante la implementación de un conjunto de reglas, las redes están empezando a poder soportar tipos diferentes de dispositivos en una misma infraestructura.

1.6 Redes confiables

1.6.1 Arquitectura de red

Aspectos importantes

- Tolerancia a fallas
- Escalabilidad
- Calidad de servicio (QoS)

- Seguridad

1.6.1.1 Tolerancia a fallas

Una red tolerante a fallas es aquella que limita la cantidad de dispositivos afectados durante una falla.

1.6.1.2 Escalabilidad

Una red es fácilmente expansible si se utilizan estándares a la hora de diseñarla y configurarla.

1.6.1.3 Calidad de servicio

La red tiene recursos **limitados**.

- Se establecen prioridades para en relación con el QoS.
- Si no hay recursos suficientes en la red para atender las peticiones se ponen procesos en cola.
- Se van ejecutando en función de su nivel de prioridad.

1.6.1.4 Seguridad en la red

Requisitos para alcanzar los objetivos de seguridad en la red.

Confidencialidad: Solamente los destinatarios deseados puedan acceder a los datos.

Integridad: La información contenida en los datos no se va a alterar durante la transmisión.

Disponibilidad: Tener acceso de forma confiable y oportuna a los servicios de datos para usuarios autorizados.

1.7 Tendencias recientes

BYOD: Bring your own device.

Permite la libertad a los usuarios de usar herramientas personales para acceder a la información.

Colaboración en línea

Comunicaciones de video

Computación en la nube

- Permite el almacenado, procesado de datos en un servidor remoto

Tipos de nubes.

- Nubes públicas: pay per use
- Nubes privadas: *bespoke*
- Nubes híbridas: (por ejemplo: parte privada, parte pública)
- Nubes comunitarias: Las nubes comunitarias son utilizadas por múltiples organizaciones que tienen necesidades e inquietudes similares. (Hospitales).

1.7.2 Tendencias tecnológicas en el hogar

Dispositivos inteligentes

Redes powerline: Emplea el cableado eléctrico existente para enviar datos a través de él.

1.7.3 Banda ancha inalámbrica

WISP: Wireless internet service provider.

- Suelen estar en entornos rurales.
- Se instala una antena de transmisión en una estructura elevada preexistente.
- Se instalan antenas de recepción en las casas de los suscriptores. Se proporciona internet cableado dentro de la casa de los suscriptores.

1.8 Seguridad en la red

1.8.1 Amenazas de seguridad

Virus, gusanos y caballos de Troya - Estos contienen software malicioso o código que se ejecuta en un dispositivo de usuario.

•**Spyware y adware** - Estos son tipos de software que se instalan en el dispositivo de un usuario. El software recopila en secreto información sobre el usuario.

•**Ataques de día cero** - También llamados ataques de hora cero, se producen el primer día que se conoce una vulnerabilidad

•**Amenazas de Atacantes** - una persona malintencionada ataca dispositivos de usuario o recursos de red.

•**Ataques por denegación de servicio** - Estos ataques ralentizan o bloquean las aplicaciones y procesos en un dispositivo de red.

•**Intercepción y robo de datos** - Este ataque captura información privada de la red de una organización.

•**Robo de identidad** - Este ataque roba las credenciales de inicio de sesión de un usuario para acceder a datos privados.

1.8.2 Soluciones de seguridad

Antivirus y antispyware -

Filtrado de Firewall - El filtrado de firewall bloquea el acceso no autorizado dentro y fuera de la red.

Dispositivos de seguridad instalados en redes corporativas

Sistemas de firewall dedicados - pueden filtrar grandes cantidades de tráfico con más granularidad.

Listas de control de acceso (ACL) - filtra en función de las direcciones IP y las aplicaciones.

Sistemas de prevención de intrusiones (IPS)- Estos identifican amenazas de rápida propagación, como ataques de día cero o de hora cero.

VPN- Estos proporcionan acceso seguro a una organización para trabajadores remotos.