Edward Nova
Tutor Virtual
Curso: Auxiliar de
CIBERSEGURIDAD

INFOTEP

Módulo 1 C 2: Introducción a las redes (CCNA) | Actividad. 3 | Valor 10 puntos
Nombre del Participante: Vladimir Cornelio Domínguez

Asignación

Después de leer el material didáctico del módulo, responda cada pregunta según lo aprendido.

1. ¿Cuáles son los factores por considerar al seleccionar dispositivos para una red pequeña?

- **Rendimiento y velocidad:** Determinado por la **velocidad del puerto** (p. ej., 100 Mbps, 1 Gbps) y la capacidad de procesamiento para manejar el tráfico.
- **Número de puertos:** Suficientes para conectar todos los dispositivos actuales y futuros.
- **Tipo de dispositivos: Routers** (para conectividad a internet), **switches** (para conectividad local) y **puntos de acceso inalámbrico** (para Wi-Fi).
- **Características requeridas:** ¿Necesitas **PoE** (Power over Ethernet) para alimentar teléfonos IP o cámaras? ¿Necesitas funciones de **seguridad** o **VLANs**?
- **Costo:** Debe ajustarse al presupuesto.
- **Escalabilidad:** La capacidad de añadir más dispositivos o puertos en el futuro.

2. ¿Por qué es importante la redundancia en una red pequeña?

La redundancia es crucial para la **continuidad del negocio** y la **alta disponibilidad**.

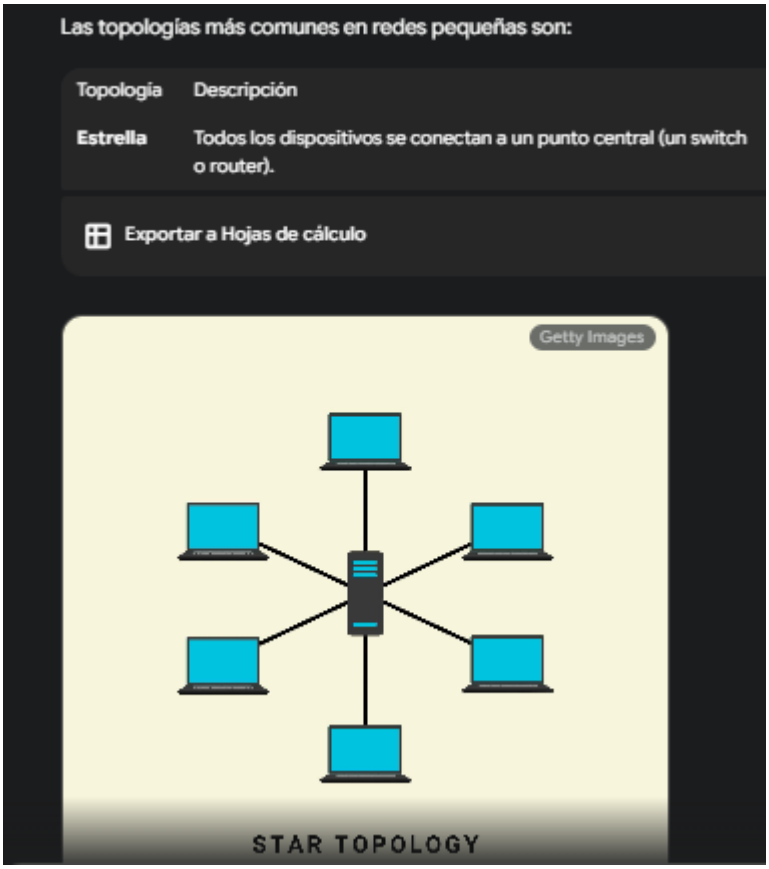
- **Evita puntos únicos de falla:** Si un dispositivo (como un router o switch principal) falla, un dispositivo de respaldo toma el control, minimizando el tiempo de inactividad.
- **Garantiza el acceso:** Asegura que los empleados puedan seguir trabajando y que los servicios críticos permanezcan accesibles.

Ejemplo: Tener dos conexiones a internet de diferentes proveedores o dos switches configurados para redundancia.

3. ¿Cómo se asignan las direcciones IP en una red pequeña?

En redes pequeñas, las direcciones IP se asignan principalmente de dos maneras:

- **Asignación Dinámica (DHCP - Protocolo de Configuración Dinámica de Host):**
  - **Ventaja:** Facilita la administración. Un **servidor DHCP** (a menudo integrado en el router) asigna automáticamente direcciones IP a los dispositivos al conectarse.
  - **Uso:** Ideal para la mayoría de las estaciones de trabajo, teléfonos móviles e impresoras.
- **Asignación Estática:**
  - **Ventaja:** La dirección IP de un dispositivo nunca cambia, lo que es útil para la accesibilidad predecible.



- **Uso:** Servidores, impresoras de red y dispositivos de infraestructura (routers, switches) que necesitan una dirección fija para ser fácilmente localizables.

4. ¿Cuáles son las topologías de redes comunes para redes pequeñas y cuáles son sus ventajas y desventajas?

| **Fácil de instalar y gestionar.** El fallo de un cable no afecta a toda la red. **Fácil detección de fallos.** | Requiere más cable. El **fallo del dispositivo central detiene toda la red.** | | **Malla (Parcial)** | Algunos dispositivos clave tienen múltiples conexiones a otros dispositivos clave. | **Alta redundancia y tolerancia a fallos.** Si una ruta falla, hay otra disponible. | **Más compleja y costosa** de instalar y mantener (más puertos y cableado). |

La **topología en estrella** es la más utilizada en entornos de oficina pequeños.

5. ¿Cómo se administra el tráfico en una red pequeña para garantizar un rendimiento óptimo?

Se logra principalmente mediante:

- **Calidad de Servicio (QoS - Quality of Service):**
  - **Prioriza el tráfico crítico** (como voz y video) sobre el tráfico menos sensible al tiempo (como la navegación web o la transferencia de archivos).
  - Asegura que las aplicaciones en tiempo real tengan el ancho de banda y la baja latencia que necesitan.
- **Monitoreo de red:** Uso de herramientas para identificar cuellos de botella y dispositivos con alto uso.
- **Segmentación (VLANs):** Separar el tráfico en dominios lógicos (p. ej., datos de empleados, invitados, voz) para reducir la congestión en un solo segmento

6. ¿Cuáles son los protocolos y aplicaciones de red comunes utilizados en redes pequeñas?

Categoría	Protocolos Comunes	Aplicaciones de Red Comunes
Direccionamiento/Núcleo	**TCP/IP** (base de internet), **DHCP** (asignación de IP), **DNS** (resolución de nombres).	Acceso a internet, Correo electrónico.
Acceso a Recursos	**HTTP/HTTPS** (navegación web), **SMB/CIFS** (compartir archivos en Windows), **NFS** (compartir archivos en Linux/Unix).	Servidores de archivos, Intranets.
Voz y Video	**RTP** (Protocolo de Transporte en Tiempo Real), **SIP** (Voz sobre IP - VoIP).	Videoconferencias, Telefonía IP.
Administración	**ICMP** (Ping), **SNMP** (Monitoreo de red).	Herramientas de diagnóstico (Ping, Traceroute), Software de monitoreo.

7. ¿Cuáles son las consideraciones específicas a tener en cuenta al implementar aplicaciones de voz y video en una red pequeña?

implementar aplicaciones de voz (VoIP) y video requiere enfocarse en:

- **Latencia y Jitter bajos:** El retraso (latencia) y la variación en el retraso (jitter) deben ser mínimos para que las llamadas y transmisiones sean claras y fluidas.
- **QoS (Quality of Service):** Es **esencial**. Debe configurarse en los switches y routers para dar a este tráfico la máxima prioridad.
- **Ancho de banda suficiente:** Estas aplicaciones consumen mucho ancho de banda, especialmente el video de alta definición.
- **PoE (Power over Ethernet):** A menudo se requiere en los switches para alimentar directamente los teléfonos IP y las cámaras de vigilancia.

8. ¿Cómo se puede escalar una red pequeña para que pueda manejar una mayor cantidad de dispositivos y tráfico?

Para crecer, la red puede escalar mediante:

- **Actualización de Dispositivos:** Reemplazar routers y switches por modelos con **más puertos** y **mayor rendimiento** (p. ej., pasar de 100 Mbps a 1 Gbps).
- **Modularidad:** Implementar **switches apilables** que se pueden agregar y administrar como una sola unidad.
- **Segmentación de Red (VLANs):** Dividir la red en múltiples segmentos lógicos para **reducir los dominios de colisión y difusión**, mejorando el rendimiento general.
- **Expansión Wi-Fi:** Agregar más **puntos de acceso** para aumentar la cobertura y la capacidad (número de dispositivos conectados).

9. ¿Cuál es la importancia de documentar y hacer un inventario de dispositivos en una red pequeña?

Esto es fundamental para la **administración eficiente** y la **recuperación ante desastres**.

- **Documentación de la red:** Incluye diagramas de topología, esquemas de direccionamiento IP y configuraciones de dispositivos. Esto **acelera la resolución de problemas** y facilita las actualizaciones.
- **Inventario de dispositivos:** Una lista detallada de todo el hardware (routers, switches, servidores, PC, etc.), incluyendo:
    - Marca y modelo.
    - Número de serie.
    - Ubicación física.
    - Fecha de compra y estado de la garantía.

Beneficio: Permite conocer qué activos tienes, cuándo deben ser reemplazados y dónde se encuentran, lo que es vital para el presupuesto y la seguridad.

10. ¿Cómo se pueden prevenir y manejar las amenazas a la seguridad en una red pequeña, especialmente cuando se utiliza por parte de los empleados?

Dado que los empleados son usuarios de la red, las medidas deben centrarse en la **formación** y la **tecnología**:

- **Firewall y Antivirus/Antimalware:**
    - Un **firewall** de borde (en el router) para filtrar el tráfico malicioso que entra y sale de internet.
    - Software **antivirus/antimalware** en todos los dispositivos.
- **Autenticación Sólida:**
    - Políticas de **contraseñas fuertes** y cambios regulares.
    - Uso de **autenticación multifactor (MFA)** siempre que sea posible.

- **Actualizaciones y Parches:**
  - Mantener el **firmware** de los dispositivos de red y el software del sistema operativo **actualizado** para corregir vulnerabilidades.
- **Segmentación (VLANs):** Aislar el tráfico de invitados o dispositivos no confiables del tráfico de la red principal de la empresa.
- **Formación a Empleados:**
  - Capacitación regular sobre **concienciación en ciberseguridad**, como identificar correos electrónicos de **phishing** y la importancia de no descargar software no autorizado.