Bloque III

Tema 12: Diseño, planificación y despliegue de redes

Objetivos

- Conocer el ciclo de vida de una red
- Conocer las fases y las herramientas asociadas

Bibliografía principal

- Priscilla Oppenheimer, **“Top-Down Network Design”**, Cisco Press, 2010.

Índice

Índice

1.1. Introducción (I)

- Es importante tomar una aproximación estructurada para planificar e implementar una red, y documentar cada paso.
- Existen varios modelos para llevar a cabo estas tareas.
- Cada modelo incluye:
  - Identificación de requisitos
  - Creación de un plan de implementación
  - Implementación de los cambios
  - Verificación del trabajo
  - Documentación

1.1. Introducción (II)

- Existen varios modelos para llevar a cabo estas tareas:
  - *Servicios de ciclo de vida de Cisco* **(Cisco Lifecycle Services)**. Utiliza el modelo PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar, Optimizar).
  - *Biblioteca de infraestructura IT* **(ITIL, IT Infrastructure Library).**
  - *Fallo, configuración, contabilidad, rendimiento y seguridad* **(FCAPS, Fault, Configuration, Accounting, Performance, and Security)**.
  - *Red de gestión de telecomunicaciones* **(TMN, Telecommunications Management Network)**. Se basa en FCAPS.

1.2. Modelo PPDIOO de Cisco (I)

- Define el ciclo de vida continuo del servicio de una red.
- El modelo PPDIO* tienen 6 fases:
  - **Preparar**: se identifican los requisitos de la red, y se sugiere una arquitectura conceptual de la red.
  - **Planificar**: Se identifican los requisitos de la red, áreas donde se instalará la red e identificación de los usuarios de los servicios.
  - **Diseñar**: basado en los requisitos anteriores, se realiza la mayor parte del diseño lógico y físico de la red.
  - **Implementar**: se construye la red según el diseño especificado. Se puede verificar la validez del diseño en este paso.
  - **Operar**: la efectividad del diseño se evalúa finalmente en esta fase. La monitorización de la red permitirá optimizar su diseño.
  - **Optimizar**: se identifican y resuelven problemas en la red antes de que ocurran. Puede requerir volver a diseñar la red.

**PPDIO: Prepare, Plan, Design, Implement, Operate and Optimize*

1.2. Modelo PPDIOO de Cisco (II)

- PPDIOO define un **marco de trabajo**, no es tiene por qué seguirse estrictamente.
- Aunque no aparezca, es igualmente importante añadir una **fase de "retirada"** de la red o de una parte, una vez que quede obsoleta.
- El **ciclo** se repite cada vez que la red evoluciona.

1.2.1 fase: Preparar

- En esta fase:
  - se identifican los **requisitos** de la organización
  - Se propone una estrategia de red
  - Se propone una **arquitectura de alto nivel** identificando tecnologías que puedan dar el mejor soporte a la red.
  - Puede incluir una **justificación financiera** de la propuesta.

1.2.2. fase: Planificar

- En esta fase:
  - Se identifican las necesidades de la red según los objetivos del usuario, infraestructura disponible, etc.
  - Se caracteriza las localizaciones y las redes existentes.
  - Se analiza si la infraestructura existente y entorno de operación es suficiente para soportar el sistema propuesto.
  - El plan de proyecto que se genere permite gestionar las tareas, responsabilidades, hitos y recursos necesarios para cambiar la red.
  - Por supuesto, el plan debe acatar los requisitos de negocio y parámetros establecidos en los requisitos de negocio.

1.2.3. fase: Diseñar

- En esta fase:
  - Los requisitos identificados en la fase de planificación dirigen el **diseño de la red** en esta fase.
  - La especificación del diseño de la red debe:
    - Ser **completo** y **detallado**.
    - Satisfacer los **requisitos de negocio y técnicos**.
    - Especifica el soporte para alta **disponibilidad, fiabilidad, seguridad, escalabilidad y rendimiento**.
  - Es posible que existan elementos de diseño en **otras fases**.

1.2.4. fase: Implementar

- En esta fase:
  - Se **implementa** la red **o se añaden** componentes a la red existente, de acuerdo al diseño.
  - Los dispositivos nuevos **no deben interrumpir** el funcionamiento de la red antigua, ni crear vulnerabilidades.

1.2.5. fase: Operar

- En esta fase:
  - Se **comprueba que el diseño** ha sido correcto.
  - Se realizan operaciones de **mantenimiento diarios** para el correcto funcionamiento de la red.
  - La **detección de errores**, su **corrección** y la **monitorización** del rendimiento son la entrada para la fase de optimización.

1.2.6. fase: Optimizar

- En esta fase:
  - Se gestiona proactivamente la red, para **identificar y resolver problemas antes** de que afecten a la organización.
  - La **respuesta ante fallos** debe complementar la anterior tarea.
  - Será necesario **rediseñar la red** si aparecen demasiados errores, si se identifican nuevos requisitos técnicos o de negocio, aparecen nuevas aplicaciones, o si el rendimiento no cumple las expectativas.

1.2.7. Beneficios de PPDIOO

Beneficios de aplicar el ciclo de vida al diseño de un Campus:

- **Reducción del coste** total de propiedad de la red (*TCO, Total Cost Ownership*).
- Incremento de la **disponibilidad** de la red.
- Mejora de la **capacidad de adaptación** del negocio.
- **Acceso más rápido** a aplicaciones y servicios.

1.2.7.1. Reducción del TCO

- La reducción del coste total de propiedad de la red es fundamental para la empresa.
- Un ciclo de vida de red adecuado consigue esta reducción de la siguiente manera:
  - Identificando y validando los requisitos tecnológicos.
  - Planificando para soportar cambios en la infraestructura y requisitos de los recursos.
  - Estableciendo un diseño bien fundamentado y acorde con los requisitos técnicos y los objetivos de negocio.
  - Acelerando la implementación exitosa.
  - Mejorando la eficiencia de la red, y del personal encargado de ella.
  - Reduciendo los costes de mantenimiento gracias al uso de herramientas y procedimientos de operación eficientes.

1.2.7.2. Aumento de la disponibilidad

- La disponibilidad de la red es una prioridad para la empresa, ya que puede acarrear importantes pérdidas económicas.
- Un buen ciclo de vida de red aumenta la disponibilidad mediante:
  - La evaluación del estado de seguridad de la red
  - La evaluación la capacidad de la red para soportar el diseño propuesto.
  - La selección del software y hardware correcto, y su mantenimiento/ actualización.
  - La producción de un diseño robusto de operación y validación de operaciones de red.
  - La comprobación del sistema antes de ponerlo en producción.
  - La mejora de las capacidades del personal.
  - La monitorización proactiva del sistema, identificando tendencias y alertas.
  - La identificación proactiva de brechas de seguridad.
  - La propuesta de planes de contingencia ante brechas.

1.2.7.3. Capacidad de adaptación

- Las empresas deben reaccionar rápidamente a los cambios económicos para tener ventaja competitiva.
- El ciclo de vida de red mejora la capacidad de adaptación mediante:
  - Establecimiento de requisitos de negocio y estrategias tecnológicas.
  - La preparación de las localizaciones de la empresa para soportar lo que se quiere implementar.
  - La integración en el diseño detallado de los requisitos técnicos y objetivos de negocio.
  - La instalación, configuración e integración de los componentes del sistema mediante expertos.
  - La mejora constante del rendimiento.

1.2.7.4. Acceso rápido a servicios

- Para un entorno productivo es vital acceder rápidamente a servicios y aplicaciones.
- Un buen ciclo de vida de red aumenta la velocidad de acceso mediante:
  - La evaluación y mejora de la preparación de la red para soportar los servicios y tecnologías de red actuales y previstos.
  - La mejora de la eficiencia de la provisión del servicio al incrementar la disponibilidad, capacidad en recursos y rendimiento de la red.
  - La mejora de la disponiblidad, fiabilidad y estabilidad de la red y las aplicaciones en red.
  - La gestión y resolución de problemas de red y la actualización del software de aplicación.

Índice

2. Análisis de requisitos y modelado de una red.

- El análisis de los requisitos del cliente permite identificar los objetivos del diseñador.
- Por lo general, el diseño de la red no se hace desde el principio, sino que ha de adaptarse a una infraestructura existente. Por ello es necesario caracterizarla.

2.1. Análisis de requisitos (I)

- Para analizar convenientemente los requisitos del cliente, es necesario seguir los siguientes pasos:
  - **Identificar** las **aplicaciones y servicios** de red esperadas para la red.
  - Definir los **objetivos** de la organización.
  - Definir y **comprobar las restricciones** de la organización.
  - Definir los **objetivos técnicos**.
  - Definir y comprobar todas las **restricciones técnicas.**

2.1. Análisis de requisitos (II)

- Los requisitos de la red son de dos tipos:
  - **Objetivos de negocio**
    - Requiere comprender entre otros:
      - los **objetivos de la empresa** (permite seleccionar productos que mejor se ajusten)
      - **su estructura** (organización, sedes remotas, etc. para identificar las comunidades de usuarios y su estructura lógica y de gestión)
      - **cómo medirá el cliente el éxito** del despliegue de la red (para identificar cómo afectará el rendimiento de la red a la empresa, y cuáles son factores de rendimiento prioritarios).
  - **Objetivos técnicos**
    - Capacidad, seguridad, rendimiento...

2.1.1. Análisis de requisitos de negocio (I)

- Aunque para un ingeniero es más interesante analizar los requisitos técnicos, es fundamental analizar los objetivos de negocio.
- Es necesario estudiar previamente el **entorno** del negocio del cliente: mercado, servicios, productos, ventaja competitiva, etc.
- Este conocimiento **permite identificar servicios** y productos que fortalezcan la posición del cliente.

2.1.1. Análisis de requisitos de negocio (II)

- Es necesario conocer la estructura de la organización de la empresa, ya que:
  - **la red** que se diseñe **reflejará** la estructura corporativa.
  - Este conocimiento permite identificar **comunidades de usuarios y el tráfico** que generan.
  - Permite identificar si habrá usuarios en sedes remotas, o centralizadas en oficinas, etc.

2.1.1. Análisis de requisitos de negocio (III)

- En la **entrevista** con el cliente es necesario:
  - Que indique **cuál es el objetivo general** del proyecto de diseño de la red, desde el punto de vista del negocio.
  - Que indique **qué significa** que el proyecto sea **"exitoso"**, y si depende de los cambios de objetivos fiscales de la empresa.
  - Que indique qué **alcance tendría un fracaso**.

2.1.1. Análisis de requisitos de negocio (IV)

Ejemplo de requisitos de negocio:

- Aumentar beneficios
- Aumentar la cuota de mercado
- Expandirse a nuevos mercados
- Aumentar la ventaja competitiva
- Reducir costes
- Incrementar la productividad de los empleados.
- Reducir los ciclos de desarrollo de productos
- Ofrecer nuevos servicios a los clientes
- Ofrecer mejor soporte a los clientes
- Dar acceso a otros participantes en la red
- Evitar parada del negocio debido a problemas de seguridad de red.
- Evitar parada del negocio debido a desastres naturales.
- Modernizar tecnologías desfasadas.
- Reducir costes de red y de telecomunicaciones.
- Hacer centros de datos más eficientes.

2.1.1. Análisis de requisitos de negocio (V)

Consideraciones sobre redes corporativas:

- Las redes deben estar orientados al negocio
- Las redes ofrecen un servicio*.
- Pueden requerir proporcionar la movilidad de usuarios.
- Es importante proporcionar seguridad y robustez.

2.1.2. Análisis de las restricciones de negocio (I)

•**Políticas y asuntos internos.** Es necesario escuchar si hay implicaciones, problemas con grupos, grupos que deseen que falle el proyecto, etc. ¿Cuál es la idea de la empresa ante el riesgo? ¿Se comprueban los sistemas correctamente? ¿Hay tecnologías o fabricantes "prohibidos"? ¿Hay que cumplir algún estándar?…

•**Presupuesto.** Incluye comprar los equipos, licencias, comprobación, acuerdos de mantenimiento, cursos y personal. Será necesario buscar soluciones de compromiso entre rendimiento y coste.

•**Calendario del proyecto.** Es necesario identificar los hitos intermedios, para controlar las fechas de entrega. Hay que considerar si la red existente es suficiente, o de si hay que llevar a cabo actualizaciones que afecten a la planificación temporal.

2.1.3. Análisis de requisitos técnicos

- Los requisitos técnicos de la red permiten elegir en el **diseño las tecnologías** que mejor se ajusten a las necesidades de la empresa.
- Debido a las restricciones de presupuesto del cliente, **es necesario priorizar** y llegar a una solución de compromiso.
- Requisitos típicos:
  - Escalabilidad
  - Disponibilidad
  - Rendimiento
  - Seguridad
  - Que sea gestionable
  - Usabilidad
  - Que sea asequible

2.1.3.1. Escalabilidad

- **Escalabilidad**: el diseño debe permitir crecer a la red.
  - Planificar para crecer. ¿Cuánto crecerá la red en 2-5 años? ¿cuántas localizaciones /usuarios /servidores?
  - **Extender el acceso a los datos**. Es posible que requiera el acceso de otras compañías o de trabajadores a parte de los datos.
  - **Restricciones de escalabilidad.** Hay restricciones técnicas inherentes a la tecnología utilizada.

2.1.3.2. Disponibilidad

- **Disponibilidad**: ¿cuánto tiempo está funcionando?
  - **Recuperación ante desastres**. Incluye procedimientos para realizar copias en varias localizaciones, y acciones para conmutar a a tecnologías de respaldo.
  - **Especificación de los requisitos de disponibilidad**. Debe estar especificado de forma precisa, incluyendo cuándo puede no estar disponible. Ej. 99'99%, pudiendo fallar de 4:00am a 7:00am. Disponibilidad del 99'999% en casos críticos. Esto afecta al mantenimiento.
    - Tiempo medio entre fallos: (*MTBF, mean time between failure*). Ej. 4000h
    - Tiempo medio de reparación: (MTTR, *mean time to repair*). Ej.: 1h
    - Porcentaje de disponibilidad: MTBF/(MTBF+MTTR). Ej.: 4000/4001=99.98%
  - Hay que averiguar cuál es el precio de no estar disponible.
  - Hay que distinguir los requisitos para partes de la red.

2.1.3.3. Rendimiento (I)

- **Rendimiento de red:** Un usuario no suele saber qué parámetros hacen que la red satisfaga las necesidades de sus aplicaciones.
- Parámetros de rendimiento:
  - **Capacidad (*ancho de banda**):** datos/s (bps)
  - **Utilización:** porcentaje de la capacidad usada.
  - **Utilización óptima:** utilización media previa a la saturación.
  - **Tasa de transferencia (*throughput*):** datos correctamente entregados por unidad de tiempo.
  - **Carga ofrecida:** cantidad de datos que están preparados para enviar a la red desde todos los nodos en un instante de tiempo.
  - **Precisión (*accuracy*)**: Cantidad de tráfico útil correctamente enviado, relativo al tráfico total.
  - **Eficiencia:** esfuerzo para obtener una tasa de transferencia dada.
  - **Latencia:** tiempo entre que un dato está disponible para enviar, y llega a su destino.
  - **Variación de la latencia (jitter):** variación con respecto a la media de los retardos.
  - **Tiempo de respuesta:** tiempo medio entre la solicitud de un servicio y su respuesta.

2.1.3.3. Rendimiento (II)

Algunas consideraciones adicionales:

- La utilización de red óptima permite absorber picos de tráfico sin degradar significativamente la red. Por eso debe estar por debajo de 100%. Se estima que para una red WAN su valor es el 70%, y 37% para una Ethernet LAN
- Tasa de transferencia. Se puede especificar para sesiones, conexiones o para la red completa. La tasa óptima debería coincidir con la capacidad. Sin embargo, depende de protocolos de capas inferiores.
- Tasa de transferencia de dispositivos de red. Se especifican en paquetes por segundo (pps) que puede reenviar el dispositivo antes de empezar a descartar paquetes. Algunos pueden enviar a la velocidad del cable (velocidad máxima teórica)¥.
- La tasa de transferencia de la aplicación (*goodput*) difiere de la de la red (overheads, envío de mensajes de confirmación, etc). En muchos casos puede deberse al equipo que genera el tráfico.
- La precisión se puede medir en tasa de bits erróneos (BER, *bit error rate*) o (PER, *packet error rate*).
- La latencia de respuesta admitida depende de la aplicación. Ej.: 100ms para aplicaciones interactivas.

2.1.3.4. Seguridad (I)

- **Seguridad de red:** toda empresa tiene datos, transacción y equipos que proteger. El primer paso para el diseño de seguridad del sistema es la planificación:
- Puede requerirse que el sistema tenga suficiente seguridad para **reducir un posible riesgo** a un nivel deseado.
- Un objetivo práctico es asegurar que **el coste de implementar la seguridad no sea mayor que el de recuperarse** de un incidente.

2.1.3.4. Seguridad (II)

Para los requisitos de seguridad hay que:

- **Identificar los activos de red.** ¿Cuáles son los elementos de la red que pueden ser atacados? ¿Cuánto cuesta recuperarlos? ¿Cuál es su valor?
  - Cortafuegos e IDS suelen ser objetivos principales.
- **Analizar riesgos de seguridad.** Es necesario identificar continuamente qué elementos son sensibles, y cómo puede afectar a la empresa. El cliente debe indicar qué impacto tiene no emplear ningún elemento de seguridad.
- Evaluar ataques de reconocimiento. Es el paso previo a un ataque.
- Uno de los ataques más complejos del que protegerse es el ataque de denegación de servicio.

2.1.3.4. Seguridad (III)

Ejemplo de requisitos básicos:

- **Confidencialidad de datos**, para que sólo los usuarios autorizados puedan acceder a ellos.
- **Integridad de los datos**, para que sólo lo usuarios autorizados puedan modificarlos
- **Acceso ininterrumpido** a recursos de computación importantes.

2.1.3.5. Gestión

No todos los clientes lo tienen en cuenta.

Las funciones de gestión se resumen en (FCAPS):

- **Gestión de fallos (Fault management):** Detectar, aislar u corregir problemas, informarlos a usuarios y gestores, y considerar tendencias para problemas relacionados.
- **Gestión de la configuración (Configuration management):** controlar, operar identificar y recopilar datos de los dispositivos gestionados.
- **Gestión de la contabilidad (Accounting management):** monitorizar el uso de la red para identificar costes de usuarios de red y requisitos de capacidad.
- **Gestión del rendimiento (Performance management):** analizar el tráfico y el comportamiento de las aplicaciones para optimizar la red y satisfacer los SLAs, y planificar la expansión.
- **Gestión de la seguridad (Security management):** monitorizar y comprobar las políticas de protección, mantener y distribuir las contraseñas e información de identificación, gestionar claves, etc.

2.1.3.6. Usabilidad

- Los usuarios deben poder usar la red fácilmente.
- Es recomendable usar protocolos de configuración, nomenclatura, etc. amigables para los usuarios. P.e.: DHCP.
- La movilidad es uno de los aspectos que pueden mejorar la usabilidad de la red.

2.1.3.7. Adaptabilidad

- Los objetivos de negocio, marco legal, nuevos protocolos, etc. pueden cambiar.
- Es necesario realizar un diseño flexible para satisfacer los requisitos cambiantes. Por ejemplo, los requisitos de QoS.
- Se recomienda no depender de tecnologías obsoletas.

2.1.3.8. Red asequible

La red debe transportar la mayor cantidad de tráfico dado un coste económico (equipamiento y costes de operación).

Dependiendo de la empresa, ésta puede ser el requisito principal.

Por ejemplo, para **reducir costes de operación** se puede considerar en el diseño:

- Elegir dispositivos fáciles de configurar y mantener.
- Elegir un diseño de red fácil de entender y abordar.
- Desarrollar una buena documentación.
- Seleccionar protocolos y aplicaciones de red fáciles para que el usuario pueda resolver problemas de forma autónoma.

2.2. Modelado de la red existente

- Suele existir una infraestructura de red previa, por lo que no se puede diseñar desde cero, sino que se introducen mejoras en la red.
- La caracterización de la red existente permite identificar las expectativas de rendimiento del cliente, y las estructuras lógicas y físicas de la red.
- Para describir la red actual es necesario realizar distintas caracterizaciones:
  - Caracterización del **mapa de la red**.
  - Caracterización de los esquemas de **nombrado** y asignación de direcciones.
  - Caracterización del **cableado.**
  - Caracterización del **rendimiento** de la red actual.

2.2.1. Caracterización del mapa de la red

- Los mapas de red permiten deducir la arquitectura lógica (topología, etc.) de la red.
- En el caso de redes muy extensas se pueden realizar varios mapas, o en su caso, seguir un orden top-down (información geográfica, conexiones WAN entre sitios remotos, conexiones WAN y LAN entre campus y edificios).
- Se puede desarrollar un **mapa de los servicios**: aplicación (FTP, HTTP, etc), red (DHCP, etc.).
- Por cada **campus** se puede precisar los edificios/plantas/habitaciones, la localización de los servidores/ encaminadores/ conmutadores/ estaciones de monitorización/ LAN virtuales/ estaciones de trabajo.

2.2.2. Caracterización del esquema de nombrado

- Permite analizar la escalabilidad del esquema de direccionamiento, y su facilidad de mantenimiento.
- Suele ser necesario documentar su localización.

2.2.3. Caracterización del cableado

- Permite identificar los niveles de escalabilidad y disponibilidad de la red.

2.2.4. Caracterización del rendimiento de la red

- Estudio del rendimiento base de la red: es necesario para poder establecer el rendimiento actual y justificar las mejoras que se introducen.
- Análisis de la disponibilidad de la red, obteniendo del histórico de su funcionamiento los tiempos medios entre fallos (*Mean Time Between Failure, MTBF*) y el tiempo medio de reparación (*Mean Time To Repair, MTTR*).
- Análisis de la utilización de la red, a lo largo de un extenso periodo
- Análisis del porcentaje de error de la red.
- Análisis de la eficiencia de la red, comprobando la sobrecarga por protocolo.
- Análisis del tiempo de respuesta y retardo (p.e. mediante el *Round Trip Time*).

2.2.5. Caracterización del tráfico de red

- Parte del diseño requiere conocer qué aplicaciones de red se usan o se prevé usar, y así conocer el tráfico que tendrá que servir la red.
- En la caracterización del tráfico destaca:
  - **Caracterización de flujos de tráfico**. Un flujo de tráfico de red individual puede definirse como información de aplicación y de protocolos transmitidas entre dos entidades en una sola sesión.
  - **Caracterización de la carga de tráfico**. Necesario para dimensionar correctamente la red. Su objetivo principal es evitar generar cuellos de botella.
  - Caracterización de la **eficiencia de la red.**

2.2.5.1. Caracterización de flujos de tráfico

- Requiere:
  - Identificar el origen y destino del flujo, la dirección (bidireccional o no) y simetría (tasa de transmisión en cada sentido) del mismo.
  - Identificar las fuentes de tráfico (aplicaciones) más importantes, y la comunidad de usuarios (departamento o perfil de usuario) que lo utiliza.
  - Localizar los almacenes de datos (p.e. servidores) de la red.

2.2.5.1.1. Identificación de aplicaciones de red

- Hay que hacer un registro de las aplicaciones. Debe incluir las aplicaciones actuales y previstas.
- Además, debe incluir las aplicaciones del sistema.

Nombre de la aplicación (tal como se conoce en la empresa)	Tipo de aplicación	¿Nueva?(S/N)	¿Es crítica? 1.- Muy crítica 2.- algo crítica 3.- No es crítica	Comentarios ¿se seguirá utilizando? ¿uso según calendario? Etc.

Plantilla de tabla de registro de aplicaciones

2.2.5.1.1. Identificación de aplicaciones de red

Ejemplos de tipo de aplicaciones de usuario:

- Correo electrónico
- Compartición y transferencia de ficheros
- Acceso y actualización de base de datos.
- Navegación web
- Juego en red
- Terminal remoto
- Calendario
- Imágenes médicas
- Videoconferencia
- Vídeo bajo demanda
- Video multidifusión planificado
- Cámara de vigilancia
- Voz sobre IP
- FAX
- Pizarra electrónica
- Directorio en línea
- Enseñanza a distancia
- Punto de venta
- Comercio electrónico

2.2.5.1.2. Características de las aplicaciones

- Normalmente existen cientos de aplicaciones en la empresa, pero hay que centrarse en el top-N de las aplicaciones clave para la empresa.
- Es necesario comprender las características de la aplicación. Si es necesario, hay que entrevistar a los que soportan dichas aplicaciones.
- Hay que identificar las siguientes características por cada aplicación:

Nombre de la aplicación	Fabricante	Versión, parches, etc.	Lugares donde se utiliza	Protocolos y puertos que usa	Requisitos de capacidad de red y rendimiento	Número de conexiones concurrentes	¿Está habilitada la compresión?	¿Está habilitado el cifrado?

2.2.5.2. Caracterización de la carga de tráfico

- A partir de los requisitos de tasa de transmisión de las aplicaciones, de las fuentes de tráfico y la localización de los almacenes de datos y comunidad de usuarios se puede estimar la carga de tráfico.

Índice de contenidos

3. Planificación y despliegue de una red.

- Tras definir los requisitos del proyecto, según la metodología PPDIOO, se lleva a cabo el diseño de la topología y las soluciones de red.
- Tras el diseño, se llevará a cabo la implementación, atendiendo al diseño detallado elaborado en el paso anterior.

3.1. Metodología Top-down para el diseño de una red

- En la fase del diseño de la red se detallan las decisiones de diseño de:
  - La infraestructura de red
  - Servicios de la infraestructura
  - Las aplicaciones
- Se puede desarrollar un prototipo para identificar fallos en el diseño antes de desplegarlo en toda la red.
- Se detalla cada aspecto del diseño para guiar la implementación.

3.1. Metodología Top-down para el diseño de una red

- El diseño de red top-down es una metodología para el diseño de redes que comienza desde las capas altas del modelo OSI y continúa hacia las más bajas.
- Se analizan los requisitos de aplicaciones y la estructura lógica antes de elegir los dispositivos físicos.
- El diseño de red top-down es iterativo.
- El diseño se compone de un diseño **lógico** y un diseño **físico** de la red.

3.1.0. Documento de diseño

- El cliente suele enviar un **RFP (*Request for Proposal*)**, indicando las necesidades del proyecto, con los siguientes puntos:
  - Objetivos de negocio del proyecto
  - Alcance del proyecto.
  - Información de las redes y aplicaciones existentes.
  - Información sobre las nuevas aplicaciones.
  - Requisitos técnicos (escalabilidad, disponibilidad, etc).
  - Requisitos de garantía de los productos.
  - Restricciones del entorno que pueden afectar a la implementación.
  - Requisitos de formación y soporte.
  - Calendario preliminar con entregables e hitos.
  - Condiciones y términos legales.

3.1.0. Documento de diseño

- La respuesta al RFP debe contener:
  - Una topología para el nuevo diseño.
  - Información sobre los protocolos, tecnologías y productos usados en el diseño.
  - Un plan de implementación.
  - Un plan de formación.
  - Información de servicio y soporte.
  - Precios y opciones de pago.
  - Cualificación de los fabricantes y proveedores.
  - Recomendaciones de otros clientes.
  - Condiciones y términos contractuales legales.

3.1.0. Documento de diseño

- Es importante que quede claro cómo se satisfacen los requisitos del cliente en la propuesta, diferenciándose de los competidores.
- Hay que seguir el formato de respuesta indicado en el RFP. Al menos hay que incluir:
  - Resumen ejecutivo.
  - Objetivos del proyecto.
  - Alcance del proyecto.
  - Requisitos de diseño.
  - Estado actual de la red.
  - Diseño lógico.
  - Diseño físico
  - Resultados del testeado del diseño.
  - Plan de implementación.
  - Presupuesto del proyecto.
  - Apéndice con el documento de diseño.

3.1.0.1. Resumen ejecutivo

- Debe ocupar no más de una página.
- Debe resaltar los puntos más importantes del documento.
- Debe dirigirse a los gestores y participantes con capacidad de decisión en el proyecto.
- Aunque incluya información técnica, no debe incluir detalles.

3.1.0.2. Objetivo del proyecto

- Debe ocupar no más de un párrafo.
- Debe destacar el **objetivo de negocio** principal, el que hará más exitoso la actividad principal de la organización.
- Debe ser claro, para que el lector compruebe que se ha entendido el objetivo de la empresa.

3.1.0.3. Alcance del proyecto

- Se indica si es una segmento de red LAN, la red completa de la empresa, etc.
- Se indica qué departamentos se ven afectados.
- Se indica si es una modificación de una red existente, o el diseño de una nueva.
- Se puede indicar qué no se abordará (e.j.: aplicaciones concretas), para que se clarifique en el resultado que no ha sido un fallo de diseño.

3.1.0.4. Requisitos de diseño

- Se indican los requisitos de negocio y técnicos más importantes.
- Deben aparecer priorizados, marcando los críticos.
  - Objetivos de negocio. Es crítico identificarlos correctamente.
  - Objetivos técnicos. Puede indicarse la relación de compromiso que el cliente admite (e.j.: latencia vs precio)
  - Comunidades de usuarios (*Comunidad, usuarios, ubicación, aplicaciones que usa*) y almacenes de datos (*Almacén, ubicación, aplicación, comunidad que lo usa*).
  - Aplicaciones de red (*nombre de aplicación, tipo, aplicación nueva, ¿es crítica?, coste de fallo, MTBF aceptable*) y características (*aplicación, tipo de flujo, protocolos de la aplicación, comunidades que lo usan, almacenes de datos, tasa de transmisión requerida, requisitos de QoS*).

3.1.0.5. Estado de la red

- Se describe la estructura y rendimiento de la red actual.
- Se usa un mapa de alto nivel con ubicaciones de dispositivos de red y almacenes de datos, y segmentos de red.
- Se incluyen en los mapas los elementos lógicos y físicos (e.j.: firewall y clústeres) y la topología de la red.
- Se indica la estrategia de nombrado de dispositivos y de asignación de direcciones.
- Se presenta el análisis de rendimiento de la red.

3.1.0.6. Diseño lógico

- Debe contener:
  - La topología de la red, con figuras ilustrativas
  - Un esquema para asignar direcciones a subredes y dispositivos.
  - Un esquema para nombrar dispositivos.
  - Lista de protocolos de conmutación y encaminamiento, y recomendaciones de implementación.
  - Productos y mecanismos de seguridad, y procedimientos y políticas de seguridad.
  - Arquitecturas, procedimientos y productos de gestión recomendados.
  - Justificación de las decisiones tomadas, relacionándolas con los objetivos de negocio.

3.1.0.7. Diseño físico

- Describe las características y usos recomendados para las tecnologías y dispositivos elegidos para la implementación.
- Puede incluir información sobre los proveedores.
- Si es pertinente, se puede incluir el precio de los dispositivos y su mantenimiento.
- Debe contener información de la disponibilidad de los productos (e.j.: obsoleto, se espera que esté disponible en tal fecha, etc.)

3.1.0.8. Resultados del testeado del diseño de red

- Se describen los resultados de los tests de la red diseñada.
- Es muy importante, pues permite mostrar al cliente la consecución de los objetivos técnicos.
- Se ha de describir el entorno de los tests.
- Debe incluir:
  - Objetivos de los tests.
  - Criterios de aceptación del test.
  - Herramientas de testeo.
  - Scripts de tests.
  - Resultados y observaciones. Incluir las optimizaciones que se recomienden para el diseño.

3.1.0.9. Plan de implementación

- Se incluyen los consejos de implementación del diseño realizado.
- El nivel de detalle depende del proyecto y del rol del proponente (¿es del departamento de IT? → muy detallado. ¿Es un vendedor de dispositivos? → descripción somera).
- Debe contener las secciones relativas al despliegue de la red diseñada.

3.1.0.9. Plan de implementación

- Contenido:
  - Calendario del proyecto.
  - Plan de instalación de enlaces, dispositivos y servicios de los proveedores.
  - Plan o recomendación de subcontratación de despliegue o mantenimiento de la red.
  - Plan de comunicación del diseño a usuarios, gestores y administradores de la red.
  - Plan de formación a usuarios y administradores.
  - Plan de comprobación del rendimiento del despliegue.
  - Lista de riesgos conocidos que puedan retrasar el proyecto.
  - Un plan de respaldo en caso de fallo en la implementación.
  - Un plan de extensión de la red ante nuevos requisitos.
  -

3.1.0.10. Presupuesto

- Debe incluir:
  - la compra, el soporte y mantenimiento del equipamiento.
  - licencias de software
  - contratos de servicios y formación
  - Si hay subcontratación, hay que incluirlo.
- Puede incluir un análisis de **retorno de inversión** (*Return of Investment, ROI*), que explique cómo rápidamente se recuperará el dinero desembolsado.

3.1.0.11. Apéndice del documento de diseño

- Puede incluir las descripciones detalladas de mapas de red, configuración, esquemas de direccionamiento, etc.
- Puede incluir listados de información de contacto de la organización, o del diseñador.
- Puede incluir los métodos de pago.
- Puede incluir la condiciones y términos del contrato.
- Puede incluir información del diseñador, para demostrar al cliente su cualificación.

3.1.1. Diseño lógico de la red

- **La topología de red** es un mapa de una interconexión de redes que especifica segmentos de red, puntos de interconexión y comunidades de usuarios. El propósito de este mapa es mostrar la geometría de la red.
- Destacan tres **modelos** de topología de red:
  - **Modelo Jerárquico.** La red se divide en capas con distintas funciones. Se implementan políticas que permiten que las capas más bajas del modelo filtren el tráfico desde abajo.
  - **Modelo tolerante a fallos.** Su objetivo principal es poder gestionar los fallos en la red. La red sigue funcionando incluso cuando ocurre un fallo. Se suele aplicar cuando predominan aplicaciones críticas.
  - **Modelo seguro.** Para entornos en los que la seguridad es la principal preocupación, como en organizaciones que ofrecen servicios en una extranet, pero que requieren no comprometer la seguridad de la red interna.

3.1.2. Modelo seguro

- Durante el diseño en el modelo seguro es necesario:
  - Implementar mecanismos de seguridad que sean fáciles de gestionar
  - Aislar los servicios de seguridad del resto del sistema
  - Restringir el acceso a zonas sensibles de la red
  - Desplegar mecanismos de detección de intrusos
  - Publicitar entre los usuarios los mecanismos de seguridad implementados

3.1.2. Modelo seguro

- Los mecanismos para proporcionar seguridad en topologías de este modelo son:
  - Características de **seguridad integradas en los dispositivos de red**, como encaminadores (p.e. Con VPN), conmutadores (p.e. Listas de control de acceso) y dispositivos inalámbricos (p.e. cifrado con WEP y WPA).
  - **Cortafuegos** entre red interna y externa, y definición de zona desmilitarizada (DMZ).
  - **Consolidación de la red**. Se trata de actualizar periódicamente los mecanismos de protección, actualizando los parches, cerrando los puertos sin usar, desactivando los servicios no usados, y definiendo las listas de control de acceso.
  - **Sistema de detección de intrusiones** (IDS).

3.1.3. Modelo tolerante a fallos

- La funcionalidad en un modelo tolerante a fallos se divide en:
  - **Detección de errores**, identificando la zona donde se ha producido el error.
  - Conmutación al **sistema de respaldo**, asegurando que el sistema sigue dando resultados aceptables.
  - **Creación de informes** de para el sistema operativo.

3.1.3. Modelo tolerante a fallos

- Para asegurar la continuidad del sistema aún en caso de fallos, se introducen en el diseño elementos redundantes de distintos tipos:
  - Redundancia de **equipo a encaminador pasarela**: se ofrecen distintos métodos para acceder al encaminador por el que se conecta a las redes.
  - Redundancia de **servidor**: se duplican o respaldan los distintos tipos de servidores.
  - Redundancia de **rutas**: se proporcionan distintas rutas, pro si alguna deja de estar disponible.
  - Redundancia de **enlaces**: se disponen enlaces de respaldo, que se activan si se cae algún enlace primario.

3.1.4. Modelo jerárquico

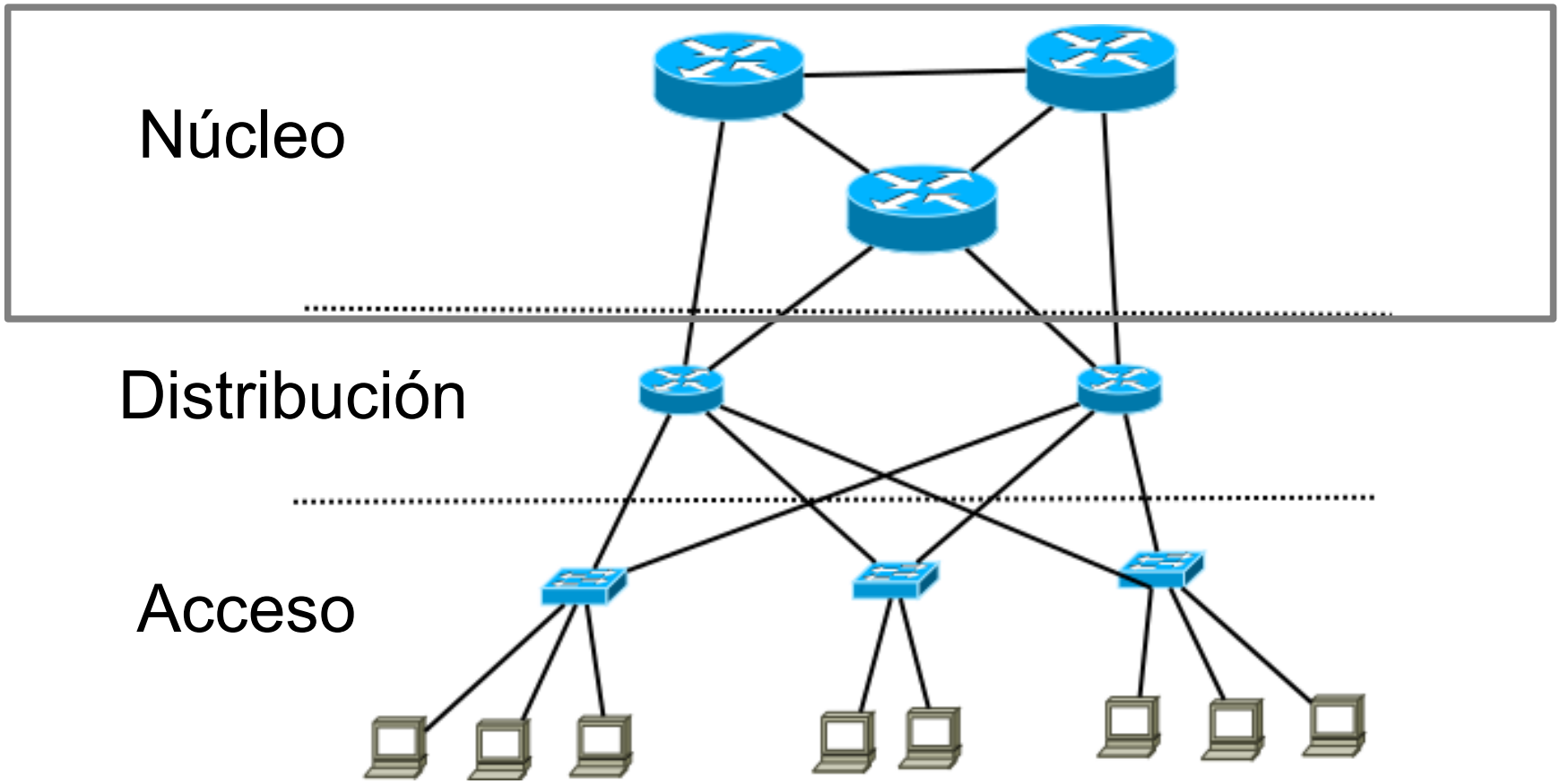
- Cisco propone el modelo jerárquico de tres capas:
  - **Núcleo:** es el centro topológico de la red, provisto de conmutación de alta velocidad, alta disponibilidad, y alta capacidad.
  - **Distribución:** es la capa responsable del filtrado de tráfico y su encaminamiento.
  - **Acceso:** es la capa más externa, la que proporciona la conectividad a los usuarios de la red.

- Esas tres capas son lógicas, no físicas, por lo que pueden solaparse en la implementación. Este diseño permite la **gestión** de tráfico **eficientemente**, **reduciendo la carga** de la red, e incrementando la **disponibilidad** de la red.

3.1.4. Modelo jerárquico

- Ventajas del modelo jerárquico:
  - **Gestión** efectiva: su diseño permite identificar y gestionar dispositivos y enlaces de forma eficiente. Si hay que reparar un dispositivo, en principio no se interfiere con las otras capas.
  - Mejor **rendimiento**: el uso de direccionamiento con subredes y la "summarization" en los routers permite que sea más rápida la convergencia en redes amplias.
  - Menor **coste**: el diseño es tan simple que permite ahorra y rentabilizar recursos. El hecho de usar sólo una conexión hacia otras redes, redunda en un mayor ahorro de ancho de banda.
  - Mayor **escalabilidad**: es fácil ampliar la red con nuevos campus.
  - Mayor **velocidad**: el acceso a los servicios **locales** se hace de forma rápida, y sólo para los servicios corporativos es necesario acceder a la capa del núcleo.

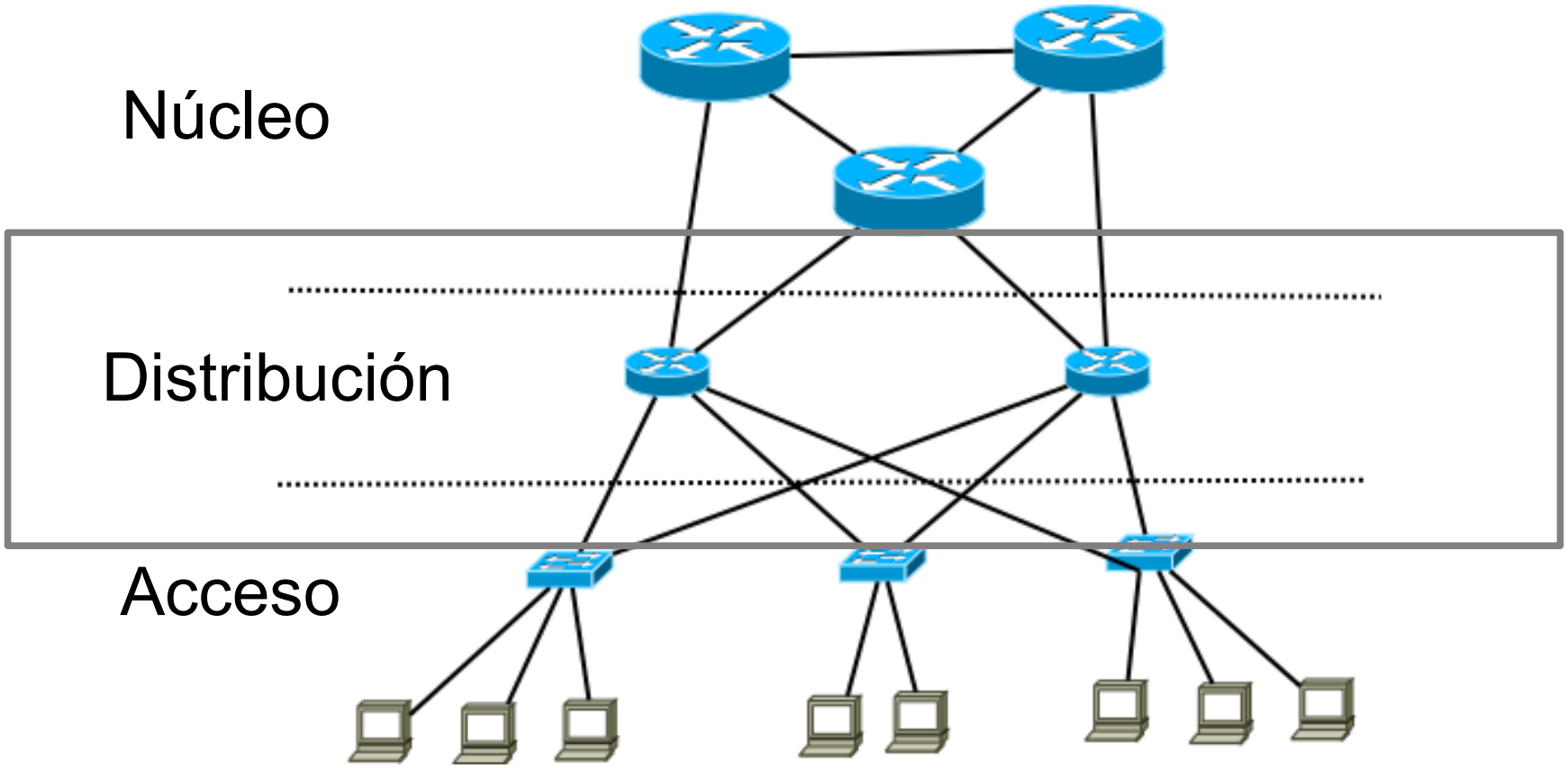
3.1.4. Modelo jerárquico



3.1.4.1. Capa del núcleo del modelo jerárquico

- Las funciones típicas del núcleo son:
  - Conmutación de alta velocidad para gran volumen de tráfico
  - Redundancia y tolerancia a fallos.
  - Compartición de carga.
  - Convergencia rápida de los protocolos de encaminamiento.
  - Baja latencia.
  - Alto ancho de banda.

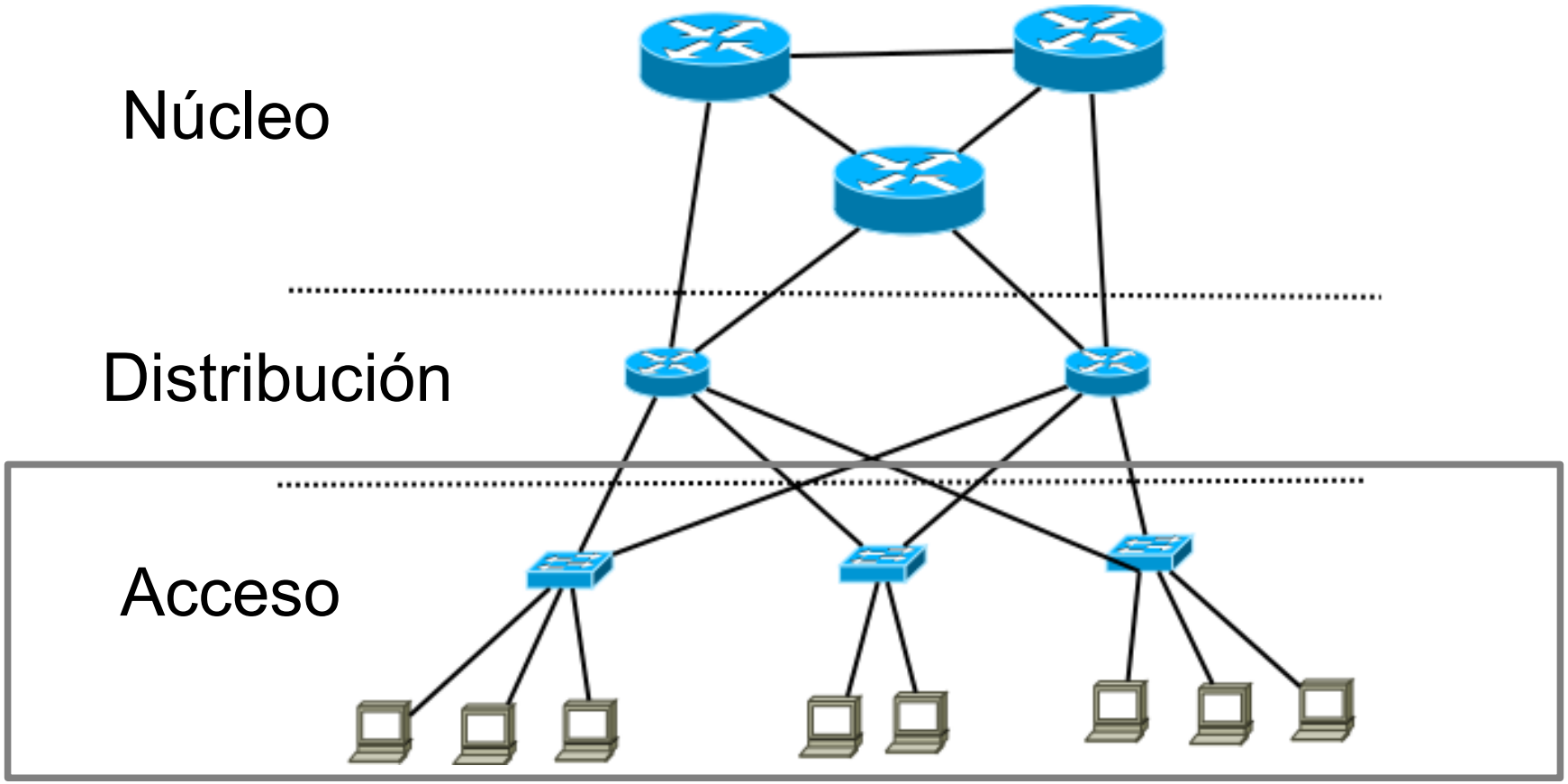
3.1.4. Modelo jerárquico



3.1.4.2. Capa de distribución del modelo jerárquico

- Las funciones típicas de la **capa de distribución** son:
  - Listas de acceso y aplicación de políticas de QoS (calidad de servicio)
  - Filtrado y encolado de paquetes
  - Redistribución de protocolos de encaminamiento
  - Encaminamiento entre VLAN,
  - Definición de dominios de difusión y multidifusión.
  - Agregación de direcciones o áreas.
  - Balanceo de carga.
  - Agregación de rutas
  - Políticas de seguridad y de red
  - Cortafuegos y NAT
  - Acceso controlado a los recursos del núcleo.

3.1.4. Modelo jerárquico



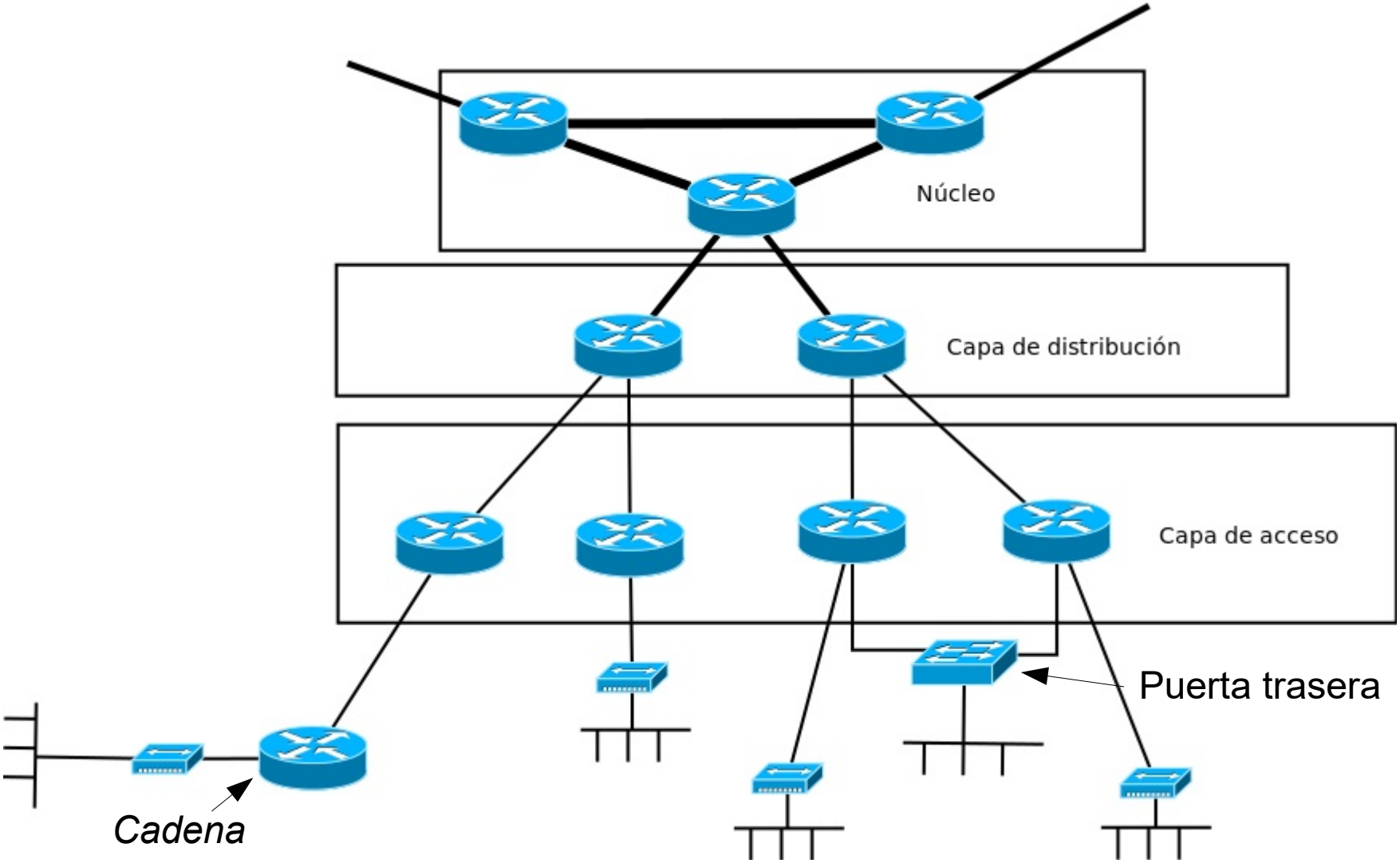
3.1.4.3. Capa de acceso del modelo jerárquico

- Las funciones típicas de la **capa de acceso** son:
  - Listas de control de acceso
  - Filtrado de tráfico
  - Segmentado
  - Creación de distintos dominios de colisión
  - Encaminamiento estático
  - Filtrado del nivel MAC
  - Conmutación y compartición de carga

3.1.4.5. Buenas prácticas en el modelo jerárquico

- Mantener constante el diámetro de la red corporativa. El ***diámetro de la red*** es el número de saltos desde un router de acceso a otro. Facilita la resolución de problemas, y permite controlar el retardo medio, predecir las rutas y los requisitos de capacidad.
- La red debe diseñarse desde el nivel de acceso. De esta manera se tiene más información acerca de los requisitos de capacidad, etc.
- En la capa de acceso hay que evitar dos errores frecuentes, consistentes en añadir redes a las interconexiones de forma no controlada:
  - Añadir cadenas: consiste en interconectar dos ramas, evitando seguir las rutas dispuestas en las restantes capas, y añadiendo una cuarta capa.
  - Añadir puertas traseras. Se trata de una interconexión entre dispositivos de la misma capa. Puede tratarse de conmutadores, puentes o encaminadores, que pueden causar problemas en el encaminamiento.

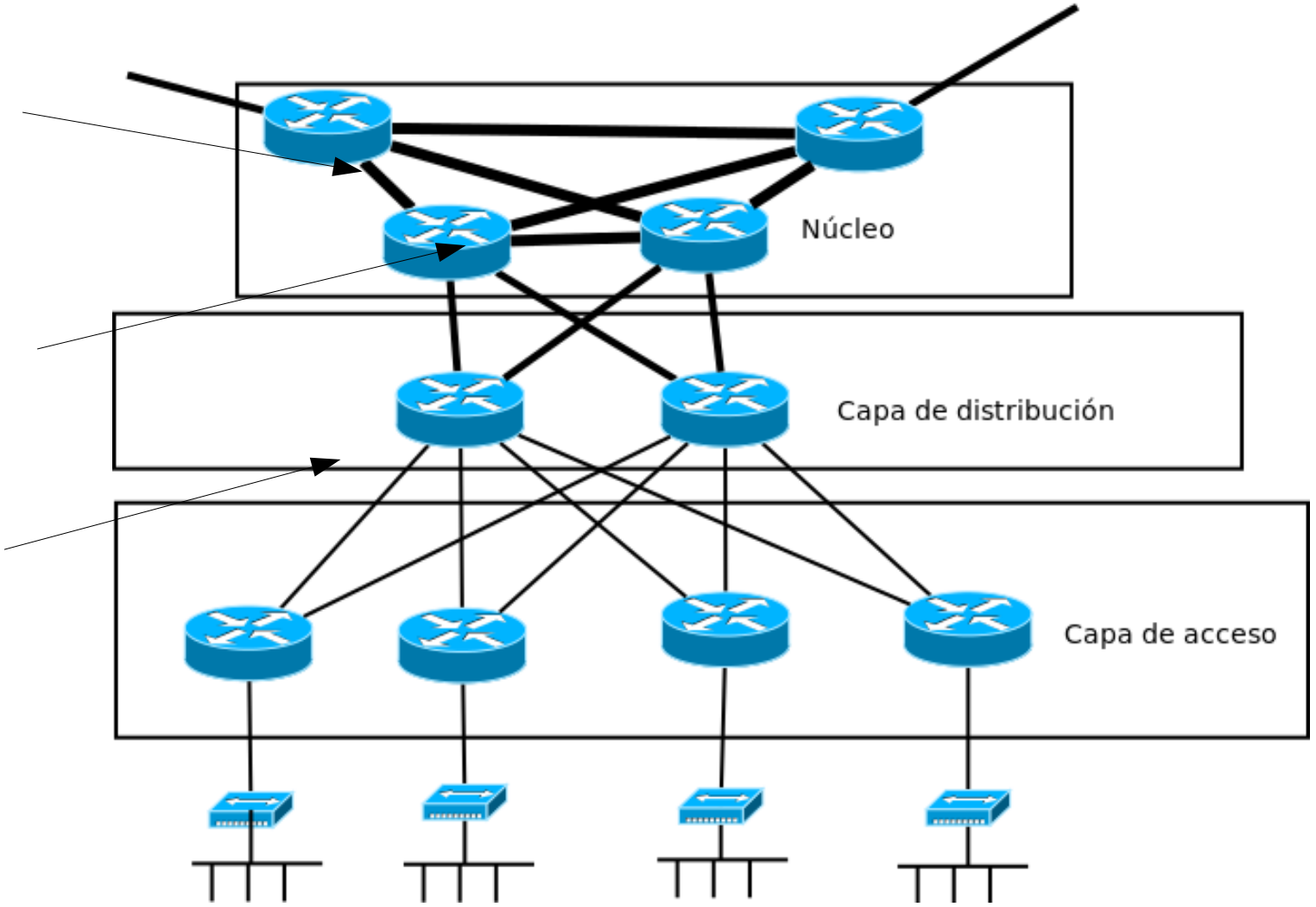
3.1.4.5. Buenas prácticas en el modelo jerárquico



3.1.4.6. Topologías redundantes

- Entre capas o incluso dentro de un Campus se pueden duplicar recursos para conseguir un mayor nivel de disponibilidad de la red.
- La redundancia implica mayores costes de despliegue y mantenimiento, por lo que hay que elegir correctamente qué elementos replicar.
- Hay dos tipos básicos de topologías redundantes aplicables al modelo jerárquico:
  - **Rutas de respaldo**
    - Rutas alternativas, aunque no tengan prestaciones iguales.
  - **Compartición de carga**
    - Se ofrecen rutas paralelas para compartir la carga de tráfico.

3.1.4.6. Topologías redundantes



3.1.5. Diseño lógico de la red

Direccionamiento y nombres

- La asignación de direcciones IP no planificada puede dar lugar a asignaciones duplicadas, direcciones no permitidas para acceder a Internet, incapacidad para introducir más elementos en la red, o desperdicio de direcciones que no puedan asignarse.
- Un modelo estructurado (utilizando el prefijo de red y asignando subredes) de asignación de direcciones facilita la gestión y solución de problemas en la red corporativa.
- La asignación de direcciones debería planificarse de forma global para toda la red corporativa.
- La asignación dinámica de direcciones (mediante DHCP, p.e.) se recomienda si existen más de 30 equipos diferentes, procurando la disponibilidad de estos servidores, vitales para el funcionamiento de la red.

3.1.5. Diseño lógico de la red

- **Direccionamiento jerárquico**: es un modelo para asignar direcciones estructuradas, y permite el uso de encaminamiento jerárquico, que es un modelo para distribuir la información de la topología entre los encaminadores de una red. Facilita que los encaminadores no tengan que conocer la topología completa de la red.
- El direccionamiento jerárquico aprovecha el encaminamiento entre dominios sin clases (CIDR), que permite:
  - la **agregación** o **resumen** (*summarization*) de las direcciones de red, reduciendo la cantidad de datos enviados entre encaminadores, y almacenados en las tablas de encaminamiento. Para poder aplicarlo, es necesario:
  - que las direcciones a agregar compartan varios bits de la izquierda.
  - Los encaminadores deben poder tomar las decisiones de encaminamiento basados en la longitud de los prefijos de red.
  - Los protocolos de encaminamiento elegidos deben poder transmitir la longitud del prefijo de red.
  - el uso de ***máscaras de subred de longitud variable*** (VLSM), que permite a su vez dividir una red en subredes de distinto tamaño, optimizando el espacio de direcciones disponibles.

3.1.5. Diseño lógico de la red

Modelo de asignación de nombres:

- Un buen modelo de asignación de nombres puede aumentar la productividad y reducir la complejidad de la administración de la red.
- Consejos para asignar nombres:
  - Los nombres deben no ser ambiguos, deben ser distintos, pero cortos y significativos.
  - deberían incluir una indicación del tipo de dispositivo (encaminador “rt”, conmutador “sw”...).
  - pueden incluir un código de lugar.
  - evitar caracteres extraños, como “-”, “!”, “_”, “*”, etc, pues pueden ser la fuente de confusiones tanto humanas como de las herramientas de administración.
  - evitar espacios dentro del nombre.
  - se recomienda usar siempre mayúsculas o minúsculas, para que sea fácil de recordar.
  - procurar usar alrededor de 8 caracteres, para evitar problemas con algunos SO.
  - si un dispositivo tiene más de una interfaz (o más de una dirección IP), asignarle a todas el mismo nombre.

3.2. Plan de implementación

- Tras la fase de diseño, el diseño de la implementación se lleva a cabo, siguiendo estos pasos:

1. **Planificación de la implementación** (durante la fase de diseño de PPDIOO). Se planifica la implementación para que sea ágil su puesta en marcha. Se efectúa la estimación de costes.
2. **Implementación y verificación del diseño** (durante la fase de implementación de PPDIOO). Se implementa y verifica la red.
3. **Monitorización y posible rediseño** (fases de operación y optimización de PPDIOO). Se pone en funcionamiento la red, y se monitoriza constantemente. En caso de fallos frecuentes, es necesario rediseñar la red.

3.2. Plan de implementación

- Durante la fase de creación e implementación de un plan de implementación se llevan a cabo las siguientes tareas:
  - Planificar la implementación.
  - Seleccionar las herramientas y recursos.
  - Coordinar el trabajo entre los especialistas.
  - Verificar la implementación.
  - Interpretar los resultados de rendimiento.
  - Documentar los resultados iniciales, el rendimiento y las recomendaciones.

3.2. Plan de implementación

- Antes de desarrollar el plan de implementación, es necesario identificar:
  - Información de la red (Topología actual, equipamiento, plan de direccionamiento, requisitos de escalabilidad, utilización de enlaces, herramientas y comandos que serán necesarios, etc).
  - Dependencias en el plan de implementación que pongan en riesgo otros servicios de la red, incluyendo la identificación de riesgos y cómo gestionarlos.
  - Los recursos recomendados asociados con las tareas, incluyendo el calendario y responsabilidades de los recursos.

3.2. Plan de implementación

- Un plan de implementación suele incluir:
  - La identificación de dispositivos y aplicaciones a implementar.
  - Una lista de tareas a hacer.
  - Recursos y herramientas necesarias.
  - El calendario del trabajo, coordinado con todos los recursos necesarios.
  - La configuración de los dispositivos y requisitos software.
  - Tests y procedimientos de verificación.

3.1. Metodologías

- Existen varias metodologías estructuradas para llevar a cabo la planificación y gestión de proyectos, que incluyen el plan de implementación:
  - FCAPS (ISO): Este estándar tiene como objetivo la gestión de redes y sistemas. El plan de implementación se considera en la gestión de cambios.
  - ITIL (Gran Bretaña): Especifica un conjunto de buenas prácticas para la gestión de sistemas adoptadas en la industria de las IT.
  - TMN (ITU-T): define prácticas para la gestión de sistemas.
  - Cisco LifeCycle Services (Cisco): define las actividades necesarias para desplegar tecnologías de Cisco y optimizar su rendimiento a lo largo del ciclo de vida de la red.
  - PPDIOO (CiscO): acrónimo que los pasos definidos en los *servicios de ciclo de vida* de Cisco.

3.2. Documentación del plan de implementación

- La documentación de implementación debe estar actualizada, ser precisa y estar accesible. Esta información se utilizará durante la implementación y la verificación.
- Debe contener toda la información posible sobre la configuración y el equipamiento, así como problemas conocidos y procedimientos de verificación.
- Se recomienda mantener una plantilla de documento de implementación.
- Concretamente, debe incluir al menos:
  - Información de la red: ej.: equipamiento y su ubicación, así como información de acceso.
  - Herramientas requeridas: ej.: software, tipos de cables, etc.
  - Recursos requeridos: p.e., información de contacto de personas involucradas, y tareas asignadas.
  - Tareas del plan de implementación: p.e.: descripción paso a paso del procedimiento de configuración del algoritmo de encaminamiento de los *routers*.
  - Tareas de verificación: p.e. Descripción paso a paso de cómo comprobar la conectividad de un interfaz.
  - Medidas y resultados de rendimiento
  - Capturas de pantalla, fotografías, figuras, etc.

3.3. Coordinación

- La instalación de una red es más sencilla si se hace de forma coordinada. Es necesario planificar:
  - Comunicación con los administradores de red. Ellos pueden dar información y soporte para acceder a ciertos equipos de la red.
  - Comunicación con los administradores de las instalaciones. Para el acceso a ciertas partes de la red se necesitará su colaboración, y acordar con antelación las visitas.
  - Comunicación con los empleados. Es necesario anunciarles cuándo se producirán las instalaciones, durante cuánto tiempo, indicando qué partes de la red o aplicaciones no estarán disponibles, para que puedan reorganizar sus calendarios.
  - Mantener una reunión preinstalación con todo aquel involucrado en la instalación. Así se revisarán los procedimientos, y se aclarará con quién se debe poner en contacto cada uno en caso de de problemas. Recordar las buenas prácticas sobre seguridad laboral.
  - Proporcionar informas periódicos al dueño de las instaciones., indicando el progreso de la implementación, riesgos identificados, plan de resolución de esos riesgos, etc.

3.4. Planificación de recuperación ante desastres

- La paralización de un sistema puede causar pérdidas millonarias a la empresa.
- La recuperación de desastres consiste en la planificación e implementación de sistemas y prácticas para asegurar que cuando un desastre ocurra, el núcleo del negocio siga funcionando.
- Se puede llamar: “plan de continuidad del negocio”.

3.4. Planificación de recuperación ante desastres

- Las causas de un desastre pueden ser:
  - Naturales (terremotos, inundaciones, huracanes, tormentas de hielo, fuego forestal, pandemias...).
  - Causado por humanos:
    - No intencionado (retroexcavadoras/obras, incendios, enfermedad, apagones, etc.).
    - Intencionado (actos de guerra, terrorismo, hacking, huelgas, etc.).

3.4. Planificación de recuperación ante desastres

- Un plan de recuperación ante desastres tiene las siguientes fases:
  - Evaluación
  - Planificación
  - Testeo
  - Implementación o recuperación

3.4.1. Evaluación de riesgos

- Hay que evaluar el impacto del fallo de cada aplicación de la red, y establecer un plan de recuperación para los sistemas críticos, considerando:
  - Pérdidas económicas
  - Parada del funcionamiento
  - Satisfacción y retención de los clientes
  - Pérdida de productividad
  - Debilitamiento de la marca de la empresa
  - Implicaciones legales
  - Precio en bolsa

3.4.2. Planificación ante un desastre

- El plan de continuidad de los sistemas críticos suele tener dos elementos:
  - Diseño de la red para una alta disponibilidad
  - Respaldo de los sistemas críticos en ubicaciones geográficas separadas.
- Hay que tener en cuenta en el plan que los desastres no sólo afectarán a la red, sino que puede que transportes, comunicaciones, etc., también dejen de funcionar.

3.4.2. Planificación ante un desastre

Tras identificar posibles amenazas, el equipo de recuperación de desastres:

1. Forma un grupo de planificación.
2. Realiza una auditoría y estimación de riesgos.
3. Establece prioridades para aplicaciones, servicios y sistemas (críticas, importantes, y el resto).
4. Desarrolla estrategias de recuperación para el personal de aplicaciones, administradores del sistema, de las bases de datos y de la red.
5. Preparar un inventario actualizado y documentación del plan.
6. Desarrolla criterios y procedimientos de verificación.
7. Implementa el plan.
8. Lleva a cabo pruebas periódicas para comprobar que el equipo de trabajo está preparado.

3.4.3. Testeado

- Para asegurar una recuperación fluida ante desastres, es recomendable entrenar al personal, y realizar simulacros.
- Estas simulaciones se llevan a cabo en otros ámbitos críticos, y son igualmente útiles para el mantenimiento de las redes.

3.4.4. Recuperación

- Se recomienda establecer una checklist clara para seguirla cuando llegue el momento. Básicamente:
  - Asegurarse de que el personal está a salvo. ¿Están todos localizados? Enviar a casa al personal no crítico.
  - Comprobar que los sistemas de respaldo están encendidos.
  - Evaluar la probabilidad de que se produzcan desastres secundarios.
  - Monitorizar la red para comprobar que todo está funcionando.
- Hay que tener en cuenta que la restauración de los sistemas principales pueden causar interrupciones en el negocio.

Índice de contenidos

1. Ciclo de vida de una red.
2. Análisis de requisitos y modelado de una red.
3. Planificación y despliegue de una red.
4. **Operaciones de gestión y mantenimiento de una red.**

4. Operaciones de gestión y mantenimiento de una red.

- La gestión de la red es el proceso de documentar, monitorizar, diagnosticar y resolver problemas y configurar dispositivos de red.
- Los administradores de la red son los responsables de cuidar la salud de la red de la empresa, por lo que deben identificar, aislar y solucionar los fallos que se produzcan.
- Las tareas de gestión de red pueden categorizarse en:
  - Tareas estructuradas: se llevan a cabo según un plan predefinido.
  - Tareas ejecutadas tras una interrupción: para resolver problemas cuando aparecen.
- Son destacables dos modelos de gestión: FCAPS e ITIL.

4. Operaciones de gestión y mantenimiento de una red.

FCAPS define los siguientes aspectos:

- Fallo (Fault): identificar y corregir errores en la red.
- Configuración (Configuration): monitorizar y controlar los dispositivos de red y su configuración.
- Contabilidad (Accounting): asegurar que los dispositivos pueden contabilizar su uso como recurso.
- Rendimiento (Performance): evaluar la tasa de transferencia, e identificar cuellos de botella.
- Seguridad (Security): proteger la red de ataques intencionados, u operaciones no intencionadas.

4. Operaciones de gestión y mantenimiento de una red.

ITIL define los siguientes aspectos:

- Estrategia de servicio: identifica los recursos IT que pueden desarrollarse como valores estratégicos para usuarios.
- Diseño de servicio: desarrolla un diseño para implementar una estrategia de servicio, incluyendo disponibilidad, capacidad, continuidad y seguridad.
- Transición del servicio: implementa el servicio en producción, definiendo la gestión del cambio, del lanzamiento, de la configuración y de del conocimiento del servicio.
- Operación del servicio: mantiene el servicio en unos niveles definidos, incluyendo la gestión de incidentes.
- Mejora continua del servicio: mejora la calidad del nivel de servicio que el departamento de IT proporciona.

4.1. Arquitectura de un sistema de gestión de red

- La arquitectura de un sistema de gestión de red (*NMS, Network Management System*) se compone de:
  - **Sistema de gestión de red** (NMS): sistem aque ejecuta las aplicaciones y monitoriza los dispositivos gestionados.
  - **Protocolo de gestión de red**: protocolos que permiten intercambian información entre los NMS y los dispositivos gestionados.
  - **Dispositivos gestionados**.
  - **Agentes de gestión**: software en los dispositivos gestionados, que recopilan la información de gestión.
  - **Información de gestión**: información útil del dispositivo que se almacena generalmente en los MIB (*Management Information Base*).

4.2. Planificación de la gestión de red

- Incluye los siguientes aspectos:
  - Calendario de mantenimiento
  - Formalización de procedimiento de control de cambios
  - Establecimiento de procedimientos de documentación de red.
  - Establecimiento de comunicación efectiva
  - Definición de plantillas y convenciones.
  - Planificación para la recuperación ante desastres.

4.2. Planificación de la gestión de red

- La documentación de un plan de gestión suele incluir:
  - Plantillas y estándares de configuración. Ej.: lista de acceso 100 para …
  - Historial de configuración.
  - Inventario de equipamiento (con número de serie e información de contrato de soporte).
  - Inventario de circuito.
  - Asignación de direcciones IP.
  - Esquemas de red.
  - Plan de comunicación.
  - Detalles de comunicación fuera de banda.
  - Patrones de tráfico esperados (*baseline*).

4.3. Protocolos de gestión de red

- Algunos de los protocolos y estándares más usados son:
  - SNMP(Simple Network Management Protocol): es el protocolo más sencillo.
  - MIB (Management Information Base): define tipos de información específica que un servidor de SNMP puede obtener de un dispositivo.
  - RMON (Monitorización remota): extiende la información de la MIB, almacenando información en el dispositivo, que luego se puede recuperar.