

UF1880: Gestión de redes telemáticas

Elaborado por: Silvia Clara Menéndez Arantes

Edición: 5.1

EDITORIAL ELEARNING S.L.

ISBN: 978-84-16492-08-4

No está permitida la reproducción total o parcial de esta obra bajo cualquiera de sus formas gráficas o audiovisuales sin la autorización previa y por escrito de los titulares del depósito legal.

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa

Bienvenido a la Unidad Formativa **UF1880: Gestión de redes telemáticas**. Esta Unidad formativa pertenece al **Módulo Formativo MF0230_3: Administración de redes telemáticas**, que forma parte del Certificado de Profesionalidad **IFCT0410: Administración y Diseño de redes departamentales**, de la familia de **Informática y Comunicaciones**.

Presentación de los contenidos

La finalidad de esta Unidad Formativa es enseñar al alumno a definir e implantar los procedimientos de monitorización de los elementos de la infraestructura de red de datos para la fase de explotación, así como supervisar el mantenimiento de la red de datos adaptando los planes preventivos establecidos a las particularidades de la instalación.

Para ello, en primer lugar se analizará el ciclo de vida de las redes, la administración de redes y los protocolos de gestión de red. También se estudiará el análisis del protocolo simple de administración de red y el análisis de la especificación de monitorización remota de red. Por último, se profundizará en la monitorización de redes, el análisis del rendimiento de redes y el mantenimiento preventivo.

Objetivos de la Unidad Formativa

Al finalizar esta Unidad Formativa aprenderás a:

- Implantar procedimientos de monitorización y alarmas para el mantenimiento y mejora del rendimiento de la red.
- Aplicar procedimientos de mantenimiento preventivo definidos en la documentación técnica.

Índice

UD1. Ciclo de vida de las redes	13
1.1. Explicación del ciclo de vida de una red usando el modelo PPDIOO como referencia	15
1.2. Descripción de las tareas y objetivos de las distintas fases	23
1.2.1. Planificar	28
1.2.2. Diseñar	31
1.2.3. Implementar	32
1.2.4. Operar	33
1.2.5. Optimizar	35
UD2. Administración de redes	43
2.1. Explicación del concepto de administración de redes como el conjunto de las fases operar y optimizar del modelo PPDIOO.....	47
2.2. Recomendaciones básicas de buenas prácticas.....	53
2.2.1. Mantener una organización (NOC) responsabilizada con la administración de red.....	56
2.2.2. Monitorizar la red para garantizar niveles de servicio en el presente y el futuro	60
2.2.3. Controlar, analizar, probar y registrar cambios en la red..	68

2.2.4.	Mantener y velar por la seguridad en la red	73
2.2.5.	Mantener un registro de incidentes y solicitudes.....	83
2.3.	Visión general y procesos comprendidos.....	89
2.3.1.	Gestión de la configuración	98
2.3.2.	Gestión de la disponibilidad.....	106
2.3.3.	Gestión de la capacidad	109
2.3.4.	Gestión de la seguridad	110
2.3.5.	Gestión de incidencias.....	120
2.4.	El centro de operaciones de red.....	124
2.4.1.	Explicación de sus funciones	127
2.5.	Gestión de la configuración	129
2.5.1.	Explicación de los objetivos.....	131
2.5.2.	Enumeración de las actividades	132
2.5.3.	Identificación y comparación de herramientas comerciales y de código abierto	135
2.6.	Gestión de la disponibilidad.....	142
2.6.1.	Explicación de los objetivos.....	143
2.6.2.	Enumeración de las actividades	144
2.7.	Gestión de la capacidad	145
2.7.1.	Explicación de los objetivos.....	146
2.7.2.	Enumeración de las actividades	148
2.8.	Gestión de la seguridad	149
2.8.1.	Caracterización de la seguridad de la información como garantía de su disponibilidad, integridad y confidencialidad.....	150
2.8.2.	Explicación de los objetivos de la gestión de la seguridad	151
2.8.3.	Referencia y explicación de los objetivos de control incluidos en el control 10.6 de la norma ISO 27002...	152
2.8.4.	Enumeración de las actividades	159

Índice

2.8.5. Recomendaciones básicas de buenas prácticas....	162
2.8.6. Sistemas de detección de intrusiones NIDS (Nessus, Snort)	166
2.8.7. Identificación y comparación de herramientas comerciales y de código abierto	206
2.9. Gestión de incidencias.....	208
2.9.1. Explicación de los objetivos.....	210
2.9.2. Enumeración de las actividades	211
 UD3. Protocolos de gestión de red	221
3.1. Explicación del marco conceptual.....	223
3.1.1. Entidades que participan en la gestión.....	230
3.1.2. Estructuras de datos utilizadas	233
3.1.3. Protocolos de comunicación	236
3.2. Componentes de la infraestructura y arquitectura	239
3.2.1. Entidad gestora	241
3.2.2. Dispositivos gestionados.....	242
3.2.3. Protocolos de gestión	247
3.3. Grupos de estándares	252
3.3.1. CMISE/CMIP de OSI.....	254
3.3.2. SNMP de TCP/IP.....	254
 UD4. Análisis del protocolo simple de administración de red (SNMP)	263
4.1. Objetivos y características de SNMP	265
4.2. Descripción de la arquitectura	267
4.2.1. Dispositivos administrados	268
4.2.2. Agentes.....	270
4.2.3. Sistema de administración	271

4.3.	Comandos básicos.....	277
4.3.1.	Lectura.....	278
4.3.2.	Escritura.....	279
4.3.3.	Notificación.....	279
4.3.4.	Operaciones transversales	279
4.4.	Base de información de administración (MIB)	280
4.4.1.	Explicación del concepto	282
4.4.2.	Organización jerárquica.....	284
4.5.	Explicación del concepto TRAP	288
4.6.	Comparación de versiones.....	292
4.7.	Ejemplificación de usos	297
UD5.	Análisis de la especificación de monitorización remota de red (RMON).....	307
5.1.	Explicación de las limitaciones de SNMP y de la necesidad de monitorización remota en redes	309
5.2.	Caracterización de RMON.....	310
5.3.	Explicación de las ventajas aportadas	325
5.4.	Descripción de la arquitectura cliente servidor en la que opera ..	326
5.5.	Comparación de las versiones indicando las capas del modelo TCP/IP en las que opera.....	327
5.6.	Ejemplificación de usos	328
UD6.	Monitorización de redes.....	339
6.1.	Clasificación y ejemplificación de los tipos de herramientas de monitorización.....	341
6.1.1.	Diagnóstico	350
6.1.2.	Monitorización activa de la disponibilidad:SNMP	371

Índice

6.1.3. Monitorización pasiva de la disponibilidad: NetFlow y Nagios.....	384
6.1.4. Monitorización del rendimiento: Cricket, MRTG, Cacti .	401
6.2. Criterios de identificación de los servicios a monitorizar.....	407
6.3. Criterios de planificar los procedimientos de monitorización para que tengan la menor incidencia en el funcionamiento de la red .	411
6.4. Protocolos de administración de red	414
6.5. Ejemplificación y comparación de herramientas comerciales y de código abierto	415
UD7. Análisis del rendimiento de redes	423
7.1. Planificación del análisis del rendimiento	425
7.1.1. Propósito.....	429
7.1.2. Destinatarios de la información	434
7.2. Indicadores y métricas	438
7.2.1. Explicación de los conceptos	440
7.3. Identificación de indicadores de rendimiento de la red	445
7.3.1. Capacidad nominal y efectiva del canal	446
7.3.2. Utilización del canal.....	449
7.3.3. Retardo de extremo a extremo	450
7.3.4. Dispersión del retardo (jitter)	455
7.3.5. Pérdida de paquetes y errores.....	456
7.4. Identificación de indicadores de rendimiento de sistemas	458
7.4.1. Disponibilidad	459
7.4.2. Memoria, utilización y carga de CPU.....	465
7.4.3. Utilización de dispositivos de entrada y salida.....	476

7.5.	Identificación de indicadores de rendimiento de servicios	478
7.5.1.	Disponibilidad	479
7.5.2.	Tiempo de respuesta	480
7.5.3.	Carga.....	482
7.6.	Ejemplos de mediciones	488
7.7.	Ánálisis de tendencias y medidas correctivas	495
7.8.	Desarrollo de un supuesto práctico donde se muestren	497
7.8.1.	El empleo de los perfiles de tráfico y utilización de la red para determinar cómo va a evolucionar su uso	497
7.8.2.	El análisis de los resultados obtenidos por la monitorización con el fin de proponer modificaciones....	514
UD8.	Mantenimiento preventivo	529
8.1.	Definición y objetivos de mantenimiento preventivo.....	531
8.2.	Gestión de paradas de mantenimiento.....	534
8.2.1.	Periodicidad	536
8.2.2.	Análisis de la necesidad	538
8.2.3.	Planificación y acuerdo de ventanas de mantenimiento	540
8.2.4.	Informes de realización.....	543
8.3.	Explicación de la relación entre el mantenimiento preventivo y los planes de calidad.....	548
8.4.	Ejemplificación de operaciones de mantenimiento indicadas en las especificaciones del fabricante de distintos tipos de dispositivos de comunicaciones	551
8.5.	El Firmware de los dispositivos de comunicaciones	552
8.5.1.	Definición del concepto de Firmware	553
8.5.2.	Explicación de la necesidad de actualización	554
8.5.3.	Identificación y descripción de las fases del proceso de actualización del firmware	556
8.5.4.	Recomendaciones básicas de buenas prácticas....	557

Índice

8.6. Desarrollo de supuestos prácticos de resolución de incidencias donde se ponga de manifiesto	558
8.6.1. La aplicación de los criterios de selección de equipos que pueden actualizar su Firmware	560
8.6.2. La localización de las versiones actualizadas del firmware	562
8.6.3. La actualización del Firmware	568
8.6.4. La comprobación del correcto funcionamiento del equipo actualizado.....	576
Glosario	585
Soluciones	587
Anexo	589

Área: informática y comunicaciones

UD1

Ciclo de vida de
las redes

- 1.1. Explicación del ciclo de vida de una red usando el modelo PPDIOO como referencia
- 1.2. Descripción de las tareas y objetivos de las distintas fases
 - 1.2.1. Planificar
 - 1.2.2. Diseñar
 - 1.2.3. Implementar
 - 1.2.4. Operar
 - 1.2.5. Optimizar

1.1. Explicación del ciclo de vida de una red usando el modelo PPDIOO como referencia

Las redes son uno de los activos más valiosos y estratégicos en el mundo de las comunicaciones por lo que se hace necesario disponer de mayor disponibilidad, seguridad y confiabilidad.

Además actualmente las redes tienden a ser convergentes y complejas por lo que se hace necesario tener un gran conocimiento y habilidades especializadas en las tecnologías de red que cada vez son más avanzadas e incluyen muchos aspectos, tales como seguridad, redes inalámbricas, voz, datos, y redes de almacenamiento.

El hecho de que una empresa sea capaz de cumplir con estas necesidades se ve comprometido cuando no se usa un método probado y consistente así como si no se dispone de personal altamente especializado.

El planteamiento o método que aquí se presenta trata de alinear los requerimientos de negocio y técnicos ajustándolos a través de las seis fases del ciclo de vida de una red PPDIOO.

Cisco define una metodología exclusiva del ciclo de vida de una red, esto es, las actividades que vamos a necesitar en cada fase del ciclo de vida de una red, con ello, nos vamos a asegurar la excelencia de los servicios.

El modelo PPDIOO consta de una serie de fases que son:

- Preparar
- Planear
- Diseñar
- Implementar
- Operar
- Optimizar

Es tan importante disponer de un método que esté probado y sea consistente como saber aplicarlo en los diferentes escenarios que se nos pueden plantear, es decir, los diferentes tipos y tamaños de empresas, localizaciones, alcances geográficos así como los diferentes requerimientos tecnológicos.

De esta idea podemos extraer que es muy importante seleccionar un proveedor de sistemas de red que sea confiable, sólido y que tenga un gran alcance, en el sentido de poder dar soporte a las diferentes necesidades empresariales y dominar la red.

El hecho de usar un método para hacer las cosas, es debido a que en general, los profesionales del Networking (redes), suelen crear redes muy complejas, caóticas y desordenadas, que cuando después surgen problemas, estos no se pueden resolver usando el mismo criterio con el que se creó la red.

Esto es fruto de un trabajo mal hecho.



Imagina que haces un cable de red siguiendo tu propio código de colores, y mañana se estropea y es otra persona la que lo tiene que arreglar... Si todos usamos el mismo código de colores para la creación del cable será mucho más fácil.



Convergencia de redes

Una red creada con esta complejidad y de forma caótica normalmente no ofrece los rendimientos esperados, o no es escalable cuando la empresa crece y la red también necesita hacerlo, además de que muchas veces no se tienen en cuenta cosas como la seguridad, y por tanto, esta red no va a satisfacer los requerimientos totales del cliente a medio o largo plazo.

La solución a este problema es el uso de un método sistemático y racionalizado en el que se diseña la red y su escalabilidad. Estos métodos provienen de la búsqueda de soluciones a través de la experiencia acumulada a la hora de diseñar productos.

La ventaja de usar el método PPDIOO se basa en varios beneficios:

- Se baja el coste total de propiedad por validación de requerimientos y planeamiento para cambios de infraestructura y requerimientos de recursos.
- Hay una mayor disponibilidad de la red ya que previamente se ha realizado un diseño en condiciones de la misma y se han validado las operaciones.
- Mejora la agilidad de los negocios, ya que se establecen requerimientos y estrategias tecnológicas.
- Se mejora la velocidad de acceso a los recursos, aplicaciones y servicios en red, esto se consigue mejorando la disponibilidad, seguridad, escalabilidad, fiabilidad, etc.

Vamos a recordar lo que es el modelo OSI para una mejor comprensión del texto, ya que hablaremos de él en más ocasiones.

Modelo OSI

El modelo OSI es un modelo de interconexión de sistemas abiertos compuesto de 7 capas, que permite dividir los problemas de red en partes más pequeñas y manejables. La capa de comienzo es la capa física, siendo esta la capa más baja de la jerarquía, iremos ascendiendo por las diferentes capas hasta llegar a la última que es la capa de aplicación, la más cercana al usuario.

Las capas se nombran en el siguiente orden:

7. Capa de aplicación
6. Capa de presentación
5. Capa de sesión
4. Capa de transporte

3. Capa de red
2. Capa de enlace de datos
1. Capa física

Comenzamos a explicar algunos aspectos de estas capas comenzando desde la capa física.

– **Capa física**

Esta capa, la de más bajo nivel permite la transmisión y recepción de los datos sin procesar a través del medio físico, esto es por ejemplo el cableado (eléctrico, óptico). Es la capa que lleva las señales eléctricas y la mecánica, la que lleva los voltios y los estados binarios de una señal.

– **Capa de enlace de datos**

Esta capa permite la transferencia de datos sin errores de las tramas de un nodo a otro, y permite que las capas superiores obtengan una transmisión sin errores.

Nos permite:

- Establecer y finalizar los vínculos entre dos nodos
- Controla el tráfico de tramas
- Transmite/recibe tramas secuencialmente
- Detecta errores de la capa física y confirma las tramas

Los protocolos que operan en esta capa adjuntaran un Chequeo de Redundancia Cíclica (Cyclical Redundancy Check a CRC) al final de cada trama.

- Delimita perfectamente las tramas
- Comprueba errores de la trama
- Administra el acceso/uso al medio

La capa de enlace de datos se divide en dos subcapas, el Control Lógico del Enlace (Logical Link Control o LLC) y el Control de Acceso al Medio (Media Access Control MAC).

- **Capa de red**

Es la encargada de controlar el funcionamiento de la subred, estipula que ruta deben tomar los datos en función de cómo es la red, las prioridades de los servicios y otros aspectos. Es en esta capa donde se encuentran ubicados dispositivos como el router.

Por tanto esta capa nos permite:

- Enrutamiento de paquetes entre las diferentes redes, es decir encontrar la mejor ruta
- Controlar el tráfico de la subred
- Fragmenta las tramas
- Asigna direcciones lógicas y físicas. Aquí encontramos la dirección IP
- Contabiliza y hace un seguimiento de las tramas
- Da soporte a las capas superiores

- **Capa de transporte de red**

Esta capa ofrece la garantía de que los paquetes se entregan a su destino sin errores, pérdidas o duplicaciones. Verdaderamente esta capa y las siguientes son capas “origen a destino” a las que no les interesan los detalles de la comunicación subyacentes. Nos proporciona:

- Segmentación de los mensajes
- Confirmación del mensaje, entregas confiables extremo a extremo, ACKs
- Controla el tráfico
- Multiplexación de sesión
- Divide los mensajes en subunidades más pequeñas para su correcta transmisión, tramas, a las que pone un encabezamiento que incluye información de control y marcadores de tamaño

La Capa 3 para determinar la ruta que deben seguir los paquetes de datos.

– **Capa de sesión**

Establece sesiones entre los diferentes procesos que se están ejecutando en las diferentes estaciones de red. No permite:

- Establecer, mantener y finalizar sesiones de red
- Da soporte a la sesión permitiendo que los equipos se comuniquen en red, implementando seguridad, reconociendo nombres, etc.

Los protocolos que operan en la capa de sesión pueden proporcionar dos tipos distintos de enfoques para que los datos vayan del emisor al receptor: la comunicación orientada a la conexión (TCP) y la comunicación sin conexión (UDP).

– **Capa de presentación**

Aporta formato a los datos que se presentan en la siguiente capa, es decir a la capa de aplicación, traduce formatos y nos permite:

- Convertir códigos de caracteres
- Convertir datos
- Compresión de los datos, reduciendo el nº de bits
- Cifrar los datos

Por ejemplo, cuando ejecutamos el navegador para acceder a una página web, o el gestor de correo electrónico estamos operando en la capa de aplicación.

– **Capa de aplicación**

Es la más cercana al usuario, procesos y aplicaciones mediante las cuales se tiene acceso a la red.

Sus funciones son:

- Uso compartido de recursos y redirección de dispositivos
- Acceso a archivos remotos
- Acceso a la impresora remota
- Administración de la red