UF1348: Monitorización y resolución de incidencias en la interconexión de redes privadas con redes públicas

Elaborado por: Pedro Mora Pérez

Edición: 5.1

EDITORIAL ELEARNING S.L.

ISBN: 978-84-16360-82-6

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa

Bienvenidos a la Unidad Formativa UF1348: Monitorización y resolución de incidencias en la interconexión de redes privadas con redes públicas. Esta unidad formativa pertenece al Módulo Formativo MF0956_2: Interconexión de redes privadas y redes públicas, que forma parte del certificado de profesionalidad IFCM0110: Operación en sistemas de comunicaciones de voz y datos, de la familia profesional de Informática y comunicaciones.

Presentación de los contenidos

La finalidad de esta unidad formativa es enseñar al alumno a mantener los dispositivos de interconexión de red para asegurar la continuidad del servicio, y atender y gestionar incidencias y alertas en los elementos de conectividad de la red privada, para mantener la conexión con la red pública según especificaciones de la organización.

Para ello, en primer lugar se analizarán los procedimientos de monitorización y procedimientos de diagnóstico de averías en dispositivos de interconexión de redes.

Objetivos del módulo o unidad formativa

Al finalizar este módulo formativo aprenderás a:

– Monitorizar y verificar el funcionamiento de los equipos de interconexión con redes externas mediante herramientas software específicas.

– Resolver las incidencias detectadas en los dispositivos de interconexión de redes privadas y públicas, siguiendo unas instrucciones dadas.

Índice

UD1

Procedimientos de monitorización en dispositivos de interconexión de redes

1.1. Herramientas de monitorización en dispositivos de interconexión de redes
   1.1.1. Descripción
   1.1.2. Uso
   1.1.3. Funciones principales
   1.1.4. Herramientas y aplicaciones utilizadas. Características

1.2. Pruebas de monitorización
   1.2.1. Tipos de prueba
   1.2.2. Selección, conexión y configuración de la herramienta

1.3. Procedimientos sistemáticos de monitorización de equipos de interconexión de redes
   1.3.1. Elementos a monitorizar
   1.3.2. Herramientas a utilizar
   1.3.3. Pasos a seguir
   1.3.4. Resultados del proceso
   1.3.5. Listas de comprobación

1.1. Herramientas de monitorización en dispositivos de interconexión de redes

Introducción

Dos de las herramientas principales para detectar alarmas usadas son MDM Multiservice Data Manager) NMS (Network Management System) de Nortel para detectar problemas en Red a nivel de líneas sobre equipos Passport / DPN y (Network Node Manager) de HPOV HP Open view que nos avisa de cambios de estado en equipos mediante SNMP (Simple Network Management Protocol).

Netcool de Omnibus es una herramienta que se está implantando desde hace algún tiempo y nos sirve también para monitorizar tanto la Red como los routers mediante la combinación de ambos tipos de alarma, las alarmas tanto de NMS como de los equipos llegan a una colectora que compara los datos que le llegan con una Base de Datos y el resultado final filtrado es mostrado por Netcool en el terminal del centro a quien pertenezca la gestión de esa línea.

Netcool incorpora también algunas herramientas de diagnóstico y pruebas desde la propia consola de alarmas.

El Sistema de gestión es una plataforma multivendedor, donde se integran diversas herramientas comerciales.

Entre ellas podemos destacar: Openview, Netcool, Oracle, MDM.

Desde el punto de vista de los elementos gestionados, puede decirse que el sistema integra 2 entornos diferentes:

– Ámbito Multiservicio, dentro de este entorno se supervisan las alarmas procedentes de los equipos en domicilio de cliente -pertenecientes a servicios MS-, bien a través de los traps que envían los propios equipos bien a través de las alarmas de los puertos de acceso (Passport, DPN) donde se conectan los routers.

– Ámbito IP, dentro de este entorno se supervisan las alarmas procedentes tanto de los routers de servicios IP, como de los equipos de acceso o de los equipos de core de la red IP. Dentro de este entorno están configurados monitores (ISM) que permiten realizar un seguimiento de la calidad de la Red.

La supervisión de alarmas de ambos entornos ha sido consolidada en un punto de entrada única (Consola Única), con objeto de facilitar las tareas de operación a los administradores de routers, evitando el tener 2 consolas abiertas para aquellos operadores que tenga servicios mixtos (MS e IP)

1.1.1. Descripción

Las herramientas de monitorización de red, son imprescindibles para cualquier entorno de comunicaciones, ya que su principal función es la búsqueda de componentes defectuosos o lentos, para avisar a los administradores de red, de dichos eventos mediante la generación de alarmas por las herramientas de monitorización.

Prácticamente la totalidad de las herramientas disponibles, poseen un amplio catálogo de eventos generadores de alarmas.

A diferencia de otros sistemas de monitoreo, como por ejemplo de intrusos, los sistemas de monitoreo en equipos de interconexión de red, buscan problemas en los diferentes dispositivos, para ir en busca de problemas causados por fallas o sobrecargas en servidores, o en la infraestructura de red.

La aparición de las diferentes herramientas de monitoreo, se ha hecho posible gracias a diversos procesos que se han generado en los diferentes ejecutivos del mundo de las TI, y su evolución gracias a la llegada de protocolos más avanzados de visualización de tráfico, como por ejemplo, netflow, jflow, Cflow, Sflow, IPFIX o Netstream.

Todo este desempeño, ha originado el propósito de estas herramientas de monitorización, para tener una perspectiva del todo, para poder clasificar los diferentes eventos que afectan a la operativa de una infraestructura de comunicaciones o servicio de negocio.

Estas herramientas de monitoreo, en su primera generación, mostraban elementos a través de una serie de colores.

Estas aplicaciones propietarias eran aptas para monitorear dispositivos activos e inactivos.

El código de colores era:

– En verde: todo está funcionando bien.

– En amarillo: se detectó que hay algún problema temporal que no afecta la disponibilidad, sin embargo, se deben realizar ajustes para no perder la comunicación.

– En naranja: el problema se ha hecho persistente y requiere pronta atención para evitar afectaciones a la disponibilidad.

– En rojo: el dispositivo se encuentra fuera de servicio en este momento y requiere acciones inmediatas para su restablecimiento.

En una 2ª generación de estas herramientas de monitoreo, realizaban un análisis exhaustivo muy profundo con el objetivo de poder evaluar independientemente, todos los componentes internos de cada dispositivo a gestionar por la herramienta de monitoreo.

Para analizar tal cantidad de elementos, estas herramientas de 2ª generación, se apoyaban en utilidades como por ejemplo analizadores de tráfico o sniffers, cuyas funciones son recolectar información de tráfico de la red y generar informes conforme a los parámetros recopilados.

Todas estas funciones, se gestionan desde una consola central.

Por último en una 3ª generación, estas herramientas analizaban todos los componentes de forma exhaustiva y de un extremo a otro, orientado al servicio.

En esta generación de herramientas de monitorización, son capaces de proporcionar información sobre problemas en las comunicaciones de la red, como por ejemplo cuellos de botella o problemas de latencia, que puedan existir a lo largo de todos los componentes del servicio.

En esta generación, cada dispositivo sabe cuándo informar a cada dispositivo sin que afecte a la operativa que está realizando, ya que de otra manera, estaría afectando al rendimiento, generando una sobrecarga de información y así, poder gestionar todos los dispositivos de una forma más eficiente.

El potencial de estas nuevas herramientas de la 3ª generación son:

– Predicciones de desempeño.

– Modelado de escenarios (simulación y emulación).

– Análisis y planeación de capacidad.

– Funcionalidades de ajustes a las configuraciones.

– Mediciones de impacto al negocio (calidad, salud y riesgos en los servicios prestados).

– Experiencia del usuario.

En definitiva, una buena herramienta de monitorización, sus principales funcionalidades deben de cubrir aspectos tales como:

– La administración remota de la herramienta, a través de navegadores, aplicaciones de Windows, etc.

– Notificaciones de las alarmas o eventos que se produzcan, a través de la visualización de la consola, por correo electrónico, por sms, o por medio de cualquier dispositivo que sea útil y de gran uso para recibir la información de la herramienta.

– Poseer una amplia gama de sensores, que posean capacidades para dar cobertura a un amplio abanico de elementos a gestionar.

– Poseer la posibilidad de poder administrar múltiples ubicaciones, desde tan solo una Tener localizado única instalación.

– Ofrecer soporte para todos los protocolos de obtención de datos, que mejore los métodos comunes de operación de estas herramientas.

1.1.2. Uso

Los usos de las herramientas de monitorización, tienen su esencia en las redes multiservicios y red IP, donde las herramientas de gestión de fallos o de monitorización (por ejemplo Netcool), junto con la plataforma de hardware que lo sustenta, hacen la operativa de estas herramientas, en los diferentes servicios de la red.

Para afrontar las nuevas demandas en los usos de las herramientas de monitorización, es posible hacer unas nuevas implementaciones o modificaciones en estas herramientas, para mejorar y optimizar el funcionamiento de las mismas.

Podemos tener un ejemplo claro con el sistema Netcool.

– Unificación el criterio de tratamiento de las alarmas.

– Inclusión de nuevos campos en las alarmas de NetCool que enriquecen la información proporcionada.

– Supresión de campos no empleados en las alarmas de NetCool.

– Redistribución de las funciones de los servidores de gestión y de la redundancia de los mismos.

Los usos más comunes para la obtención de una correcta información del ancho de banda y del consumo de los equipos de red, es imprescindible para gestionar con eficiencia las redes, podrían ser:

– Evitan cuellos de botella con respecto al ancho de banda y en relación a los servidores.

– Localización de los dispositivos que están consumiendo ancho de banda.

– Proporcionar una mejor calidad en el servicio, gracias al servicio de proactividad que proporciona las herramientas de monitorización.

– Optimización de la carga en el ancho de banda y en el procesamiento de hardware, que se ajuste a un escenario real.

– Tener localizados todos aquellos puntos o dispositivos, que usan el ancho de banda, dónde se usan y cómo se están utilizando.

– Evitar estrangulamientos de ancho de banda y de rendimiento de servidor

– Proporcionar una mejor calidad de servicio a sus usuarios de manera proactiva

– Reducir costos comprando el ancho de banda y el equipo necesario basándose en cargas efectivas

– Incrementar ganancias evitando pérdidas causadas por fallos de sistemas no descubiertos

– Ganar tranquilidad: mientras PRTG no se comunique mediante correo electrónico, SMS, radio localizador, etc. se puede estar seguro que todo esta funcionando correctamente y de esta manera se puede dedicar a otros negocios importantes.

Estos usos de las herramientas de monitorización y gestión de fallos, facilita enormemente la resolución de problemas de manera proactiva, antes de que dichas amenazas se conviertan en un verdadero problema real para la infraestructura subyacente de comunicaciones y para el negocio que se sustenta bajo dicha infraestructura.

1.1.3. Funciones principales

A continuación, se va a proceder a realizar una descripción de la funcionalidad, los criterios de utilización y una ejemplificación de la herramienta de monitorización de red, para tener una ida profunda de este tipo de herramientas.

En este punto también haremos un estudio de nivel medio-alto sobre este tipo de herramientas, ya que son de vital importancia conocerlas a fondo para la resolución de incidencias en redes telemáticas.

- Gestión. Es la planificación, organización, supervisión y control de los elementos de comunicación para garantizar un nivel de servicio aceptable.

- Objetivos. Que la utilización de los recursos se aproxime al 100%, mejorando la disponibilidad y los recursos.

- Métodos de Gestión. Conjunto de herramientas, aplicaciones y metodologías que permiten gestionar una red.

Existen dos métodos básicos para la gestión:

- Monitorización de la red. Consiste en obtener información de los elementos que componen la red.

- Control de la red. Actúa sobre dichos elementos.

Métodos de Monitorización:

- Sondeo (Polling). Consiste en acceder de forma periódica a la información de los elementos gestionados. Es sencillo pero supone mucho tráfico.

- Notificaciones (Event Reporting). Son los elementos quienes envían notificaciones ante determinados eventos. Los elementos son más complejos.

- Mixtos. Sondean un grupo de elementos, y notifican al gestor cuando ocurre algún evento.

- Gestión integrada. Por lo general se va a disponer de un único sistema de gestión para todos los elementos gestionados, que nos va a facilitar los datos mediante una interfaz sencilla y única.

Para ello todos los elementos de la red, independientemente del fabricante, modelo, etc., deben facilitarnos los datos y responder a nuestras consultas de igual forma.

El protocolo empleado para gestionar equipos en Internet es SNMP (Simple Network Management Protocol)

1. Gestión en internet: SNMP

1.1. Modelo de Información

Para referenciar los distintos recursos de un sistema remoto para gestionarlo, utilizaremos el protocolo SNMP.

Protocolo que funciona sobre IP, con lo que podremos utilizar cualquier red IP (pública o privada) para gestionar dichos equipos.

Una de las preguntas importantes en este sentido sería por ejemplo la siguiente:

¿Cómo obtendremos los distintos recursos del sistema remoto? Para ello utilizaremos un método común a todos los sistemas para nombrar los objetos: Object Identifier (OID).

Se creará un Árbol de OIDs, que sigue una arquitectura jerárquica y está definido por una serie de números enteros, no negativos, separados por puntos (dependiendo del orden dentro de dicho árbol).

1.2. Modelo de Gestión SNMP

1.2.1. Protocolo SNMP

El protocolo SNMP o “Simple Network Management Protocol” es, como su nombre indica, un protocolo sencillo para la gestión de redes, es decir, que nos permitirá gestionar los distintos equipos de red (configurar y consultar parámetros) de una forma sencilla.

Para ello se sirve del protocolo UDP, ya que básicamente haremos consultas, y el elemento consultado nos enviará la respuesta.

Existe otro método de funcionamiento; mediante Traps, es decir, cuando el elemento gestionado sufra algún cambio, nos enviará una notificación, indicando qué es lo que ha ocurrido, sin necesidad de que nosotros le hayamos preguntado.

Las consultas se harán a través del puerto 161, y cuando el equipo gestionado nos quiera enviar un trap, lo hará al puerto 162 del sistema gestor (o equipo de gestión).

Los mensajes SNMP seguirán siempre el siguiente formato:

– Versión SNMP. La versión SNMP que estamos utilizando.

– Community. La Comunidad SNMP (o clave SNMP) con la que vamos a hacer la consulta.

– PDU SNMP. En ella se indica si el mensaje es de petición, de respuesta, o de trap, así como los datos de la consulta/respuesta/trap.

1.2.2. Operaciones SNMP

Para poder consultar/configurar los distintos parámetros, se emplearán distintos tipos de PDUs:

– GetRequest. El gestor realiza una petición de valores específicos de la MIB del agente.

– GetNextRequest. Solicitamos el valor siguiente al que enviamos.

– GetResponse. El agente devuelve los valores solicitados en la consulta del gestor.

– SetRequest. El gestor asigna un valor a una variable del agente.

– Traps. El agente nos notifica que ha ocurrido algún evento.

1.2.3. Control de Acceso

Este control de acceso se utiliza para limitar quién puede acceder o modificar parámetros por SNMP un determinado agente.

Existen una política de autenticación y una política de autorización:

– Autenticación. Para ello se utiliza la community snmp, que sería algo así como una clave.

– Autorización. Dependiendo de la "clave" (o community) que utilicemos, podremos tener acceso a toda o a una parte del árbol de MIBs, y si este acceso es de escritura o de sólo lectura.

A esto se le llama vista.

Este control de acceso también se puede limitar por IPs, es decir, podremos filtrar desde que IPs se nos pueden hacer consultas desde un sistema gestor, así como la community que deben emplear.

1.1.4. Herramientas y aplicaciones utilizadas. Características.

MRTG: Multi Router Traffic Grapher

MRTG o Multi Router Traffic Grapher es una herramienta para monitorizar la carga de tráfico en los enlaces de una red.

MRTG genera páginas HTML que contienen gráficos PNG, que nos muestran el estado del tráfico de forma activa.

Básicamente MRTG es un script escrito en Perl, que se encarga de leer vía SNMP variables de los distintos elementos de la red a monitorizar.

Posteriormente, mediante una rutina escrita en lenguaje C representa dichas medidas en gráficos, que se insertan en páginas Web, para ser visualizados con cualquier explorador de Internet.

Esta Web incluirá cuatro gráficas para cada medida; una diaria, una semanal, una mensual y una anual, pudiéndose así observar las evoluciones con distinta precisión.

MRTG está diseñado para mostrar el tráfico, tanto de entrada como de salida, de los distintos interfaces de los equipos.

Aun así podremos editar el fichero de configuración y añadir gráficas para cualquier variable de los equipos, tales como uso de CPU, memoria libre/ocupada, número de conexiones establecidas, etc.

Al igual que otras herramientas de monitorización de tráfico de red, este protocolo utiliza el protocolo de administración de redes SNMP, para gestionar y recolectar información proveniente de los dispositivos (habitualmente routers), los cuales están vinculados a colectoras que gestionan dichos dispositivos.

Debido a la ingesta información que se genera, hay que distinguir la información de entrada y salida que se generan en dichos dispositivos, para poder clasificar esta información y tratarla posteriormente para la generación de informes, como resultado.

También, se pueden utilizar aplicaciones en lugar de consultar un dispositivo que utilice SNMP, utilizando 2 valores que se corresponderían con la entrada y salida del dispositivo. Para ello se utiliza normalmente Scripts que monitorean la máquina local.

Funcionamiento

MRTG, utiliza un "demonio", el cual es "invocado" por las tareas pertinentes para la recolecta de información, ejecutando los scripts incluidos en la configuración.

Esta recolecta de información, esta aplicación la realiza cada 5 minutos.

Las últimas versiones, a diferencia de las primeras versiones, almacenan la información en una base de datos, gestionada por RRDtool, a partir de la cual se generan los informes y gráficas, de forma separada las una de las otras.

Netcool

Dos de las herramientas principales para detectar alarmas usadas en los centros de gestión Personalizados son MDM (Multi service Data Manager) NMS (Network Management System) de Nortel para detectar problemas en Red a nivel de líneas sobre equipos Passport / DPN y (Network Node Manager) de HPOV HP Open view que nos avisa de cambios de estado en equipos mediante SNMP (Simple Network Management Protocol).

Las principales características que presenta Netcool Network Management son:

– Un conjunto de herramientas de monitorización de red, que proporcionan descubrimiento de red, gestión de incidencias, supervisión y configuración.

– Permite la generación de informes de red, complejos y diversos de topologías heterogéneas y homogéneas, cuyos informes y visualización, están centralizados.

– Mecanismos de supervisión y descubrimiento de la red.

– Gestión de incidencias y errores en los dispositivos SNMP gestionados.

– Proporciona la funcionalidad idónea que dan un soporte eficaz a la gestión de despliegue y cambios en la configuración de red.

Netcool incorpora también algunas herramientas de diagnóstico y pruebas desde la propia consola de alarmas.

– La capa Netcool es la capa superior del Sistema de Gestión. Es ésta la que proporciona el interfaz de cara al usuario. En ella se realizan diversas tareas:

  · Consolidación de alarmas.

  · Recolección.

  · Duplicación.

  · Correlación.

  · Enriquecimiento.

– Como se ha comentado anteriormente el sistema, y como consecuencia de su desarrollo, integra dos subsistemas independientes (MS, IP) en uno solo. Por esta razón, se puede dividir en dos niveles:

  · Nivel de Recolección.

  · Nivel de Presentación.

– El objeto de la capa de presentación es doble; por un lado consolida las alarmas de los entornos IP y MS.

De este modo el operador al conectarse a este nivel -que se ha denominado Consola Única- puede tener en una misma lista de eventos, alarmas de ambos entornos.

Por otro lado esta capa de presentación atiende las peticiones de todos los operadores que se conectan al sistema.

Herramientas de la Consola Netcool

En el menú Tools de la consola de Netcool, aparecen diferentes herramientas algunas de ellas útiles para el tratamiento de las incidencias, y otras para actualizar o corregir posibles errores en la Base de Datos que tiene el Sistema de Gestión de Interlan con los datos de todos los routers que actualmente están en gestión.

Las primeras herramientas que aparecen en el menú son el ping y el telnet, en ambas te pide como valor la IP de gestión, o el nemónico.

Históricos

Te pide como valor el nemónico del router (Name of the host), y dibuja una gráfica que representa el valor que se seleccione de la lista Tipo de histórico:

– *CpuUsage*: Representa el uso de CPU.

– *MemoryUsage*: Representa el uso de memoria.

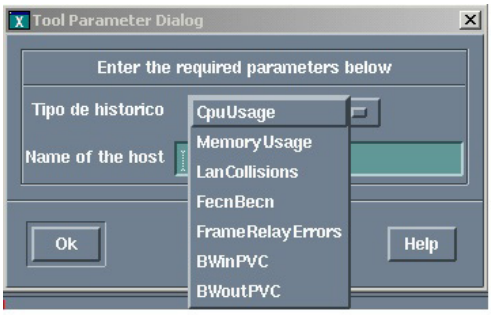
– *LanCollisions*: Representa las colisiones LAN

– *FencBenc*: Representa el Fenc y el Benc

– *FrameRelayErrors*: Representa los errores en la FR

– *BWinPVC*: Tráfico de entrada por PVC

– BWoutPVC: Tráfico de salida por PVC



Net Config

Te pide como valor el nemónico del router (Name of the host), y según la opción seleccionada en la lista VpoInterlanNetConfig te indica lo siguiente:

– *Addresses*: Muestra la colectora en la que está dado de alta el equipo, así como los interfaces que tiene el equipo y las direcciones IP, máscara de red y dirección de red, de cada uno.

– *Routing Table*: Muestra la tabla de rutas del equipo (Destination, Gateway, Type, Mask, Interface).

– *ArpCache*: Muestra la tabla de arp del router.

– *SystemInfo*: NO ESTÁ OPERATIVA.