

Administración de la Configuración OSPF con SNMP

Contenido

[Introducción](#)

[Segundo plano de OSPF](#)

[Definiciones de procesos](#)

[Propietario del proceso](#)

[Metas de procesos](#)

[Indicadores de rendimiento de procesos'1](#)

[Entradas del proceso](#)

[Resultado del proceso](#)

[Definiciones de tareas](#)

[Tareas de inicialización](#)

[Tareas iterativas](#)

[Identificación de datos](#)

[Características de datos generales](#)

[Identificación de datos SNMP](#)

[Identificación de datos RMON](#)

[Identificación de datos Syslog](#)

[Identificación de datos IOS CLI de Cisco](#)

[Recolección de datos](#)

[Colección de datos SNMP](#)

[Recopilación de datos de RMON](#)

[Recolección de datos de Syslog](#)

[Recolección de datos CLI de Cisco IOS](#)

[Presentación de datos](#)

[Informe de área OSPF](#)

[Informe de interfaz OSPF](#)

[Informe de vecinos OSPF](#)

[Herramientas comerciales y públicas para el monitoreo de Internet](#)

[Datos de sondeo de SNMP](#)

[Algoritmos de obtención de datos de ejemplo](#)

[Información Relacionada](#)

Introducción

El protocolo de ruteo Open Shortest Path First (OSPF) está definido por RFC 2328 OSPF versión 2. El objetivo de este documento es proporcionar un esquema de procedimientos que permita a las organizaciones implementar procedimientos de administración de la configuración para

verificar implementaciones OSPF frente a planes de diseño OSPF y auditar periódicamente la implementación OSPF para garantizar la coherencia a largo plazo con el diseño deseado.

Este artículo se centra en las funciones de administración de la configuración del modelo FCAPS definido por ITU-T (falla, configuración, contabilidad/inventario, rendimiento, seguridad). El ITU-T M.3400 define la administración de la configuración para proveer funciones que ejerciten el control, identificación, recolección de datos y provisión de datos a los NE (Elementos de red).

La información proporcionada en este documento se presenta en varias secciones principales que se describen a continuación.

La sección [Fondo OSPF](#) proporciona una descripción general tecnológica de OSPF que incluye información básica sobre aspectos importantes de una implementación OSPF.

La sección [Definiciones de Proceso](#) proporciona una descripción general de las definiciones de proceso utilizadas para lograr la administración de la configuración OSPF. Los detalles del proceso se describen en términos de objetivos, indicadores de rendimiento, entradas, salidas y tareas individuales.

La sección Definiciones de tareas proporciona definiciones detalladas de las tareas del proceso. Cada tarea se describe en términos de objetivos, insumos de tareas, resultados de tareas, recursos necesarios para realizar la tarea y habilidades laborales necesarias para un ejecutor de tareas.

La sección de Identificación de Datos describe la identificación de los datos para OSPF. La identificación de datos considera el origen o la ubicación de la información. Por ejemplo, el sistema contiene la información en la base de información de administración (MIB) del protocolo de administración simple de red (SNMP), archivos de registro generados por el Syslog o estructuras internas de datos a los que sólo se puede tener acceso por medio de la interfaz de línea de comandos (CLI).

La sección de Recolección de datos de este documento describe la recolección de datos OSPF. La recolección de los datos está estrechamente relacionada con la ubicación de los datos. Por ejemplo, los datos MIB SNMP son reunidos por varios mecanismos tales como notificaciones de trampa, eventos y alarmas de supervisión remota (RMON) o consultas. Los datos de las estructuras internas de datos son recabados por secuencias automáticas de comandos o por un usuario en forma manual, conectándose al sistema para enviar el comando CLI, y luego registrar la salida.

La sección Presentación de datos proporciona ejemplos de la forma en que se presentan los datos en formatos de informe. Después de identificar y recopilar los datos, se analizan. Este documento brinda ejemplos de informes que pueden ser utilizados para registrar y comparar datos de configuración OSPF.

Las secciones Herramientas comerciales y públicas para el monitoreo de Internet, Datos de sondeo SNMP y Algoritmos de obtención de datos de ejemplo proporcionan información sobre el desarrollo de herramientas para implementar el procedimiento de administración de configuración OSPF.

[Segundo plano de OSPF](#)

OSPF es un protocolo de gateway interno diseñado para su utilización en un sistema autónomo

único. El OSPF usa tecnología basada en el Trayecto más corto primero (SPF) o en el estado del link, distinta de la tecnología Bellman-Ford o de vector de distancia encontrada en los protocolos de ruteo como, por ejemplo, el Protocolo de información de ruteo (RIP). Los anuncios de estado de link (LAS) individuales describen partes del dominio de ruteo OSPF; por ejemplo, el sistema autónomo completo. Estas LSA están saturadas a través del dominio de ruteo y forman una base de datos de estados de link. Cada router en un dominio posee una base de datos de estados de link idéntica. La sincronización de las bases de datos de estado de link se mantiene con un algoritmo de inundación confiable. De la base de datos de estado de link, cada router construye una tabla de ruteo calculando el árbol de trayecto más corto, y la raíz del árbol es el mismo cálculo del router. Este cálculo comúnmente se denomina algoritmo Dijkstra.

Los LSA son pequeños y cada LSA describe una pequeña parte del dominio de ruteo de OSPF, especialmente, la vecindad de un router único, la vecindad de una red de tránsito única, una ruta entre áreas única o una ruta externa única.

Esta tabla define las características clave de OSPF:

Función	Descripción
Adyacencia	Cuando los pares de routers OSPF se vuelven adyacentes, los dos routers sincronizan sus bases de datos de estado de link intercambiando resúmenes de base de datos en forma de paquetes de intercambio de base de datos OSPF. Los routers adyacentes mantienen la sincronización de sus bases de datos de estado de link mediante el algoritmo de inundación confiable. Los routers conectados por líneas seriales siempre se vuelven adyacentes. En las redes multiacceso (Ethernet), todos los routers conectados a la red se vuelven adyacentes tanto al router designado (DR) como al router designado de reserva (BDR).
Router designado	Cuando se elige un DR en todas las redes de acceso múltiple, se crea la red LSA que describe el entorno local de la red. También desempeña un papel especial en el algoritmo de inundación, ya que todos los routers en la red están sincronizando sus bases de datos de estado de link enviando y recibiendo LSA hacia y desde el DR durante el proceso de inundación.
Respalde del router designado	Cuando el DR actual desaparece, se elige un BDR en redes de acceso múltiple para acelerar la transición de DR. Cuando el BDR toma el control, no necesita pasar por el proceso de adyacencia en la red de área local (LAN). El BDR también habilita el algoritmo de inundación confiable para que proceda en ausencia del DR antes de que se note la desaparición del DR.
Soport	OSPF trata a las redes, tales como las redes de

e para red de acceso múltiple de no difusión	datos públicos (PDN) de Frame Relay, como si fueran LAN. Sin embargo, se necesita información de configuración adicional para que los routers conectados a estas redes se encuentren inicialmente entre sí.
áreas de administración de configuración OSPF	OSPF permite que los sistemas autónomos se dividan en áreas. Esto proporciona un nivel adicional de protección de ruteo para que el ruteo dentro de un área esté protegido de toda la información externa al área. Además, al dividir un sistema autónomo en áreas, el costo del procedimiento Dijkstra, en cuanto a los ciclos de la CPU, se reducen.
Links virtuales	Al permitir la configuración de los links virtuales, el OSPF elimina las restricciones topológicas en los diseños de área en un sistema autónomo.
Autenticación de intercambios de protocolo de ruteo	Cada vez que un router OSPF recibe un paquete de protocolo de ruteo, opcionalmente puede autenticar el paquete antes de procesarlo más.
Métrica de ruteo flexible	En OSPF, las métricas están asignadas a las interfaces de routers de salida. El costo de un trayecto es la suma de las interfaces de componente del trayecto. La métrica de ruteo se deriva, de forma predeterminada, del ancho de banda del link. Puede ser asignada por el administrador del sistema con el objeto de indicar cualquier combinación de características de red, tales como retraso, ancho de banda y costo.
Trayecto múltiple de costo equivalente	Cuando existen varias rutas de mejor costo a un destino, OSPF las encuentra y las utiliza para cargar el tráfico compartido al destino.
Soporte de subred de longitud variable	Admite máscaras de subred de longitud variable al llevar una máscara de red con cada destino anunciado.

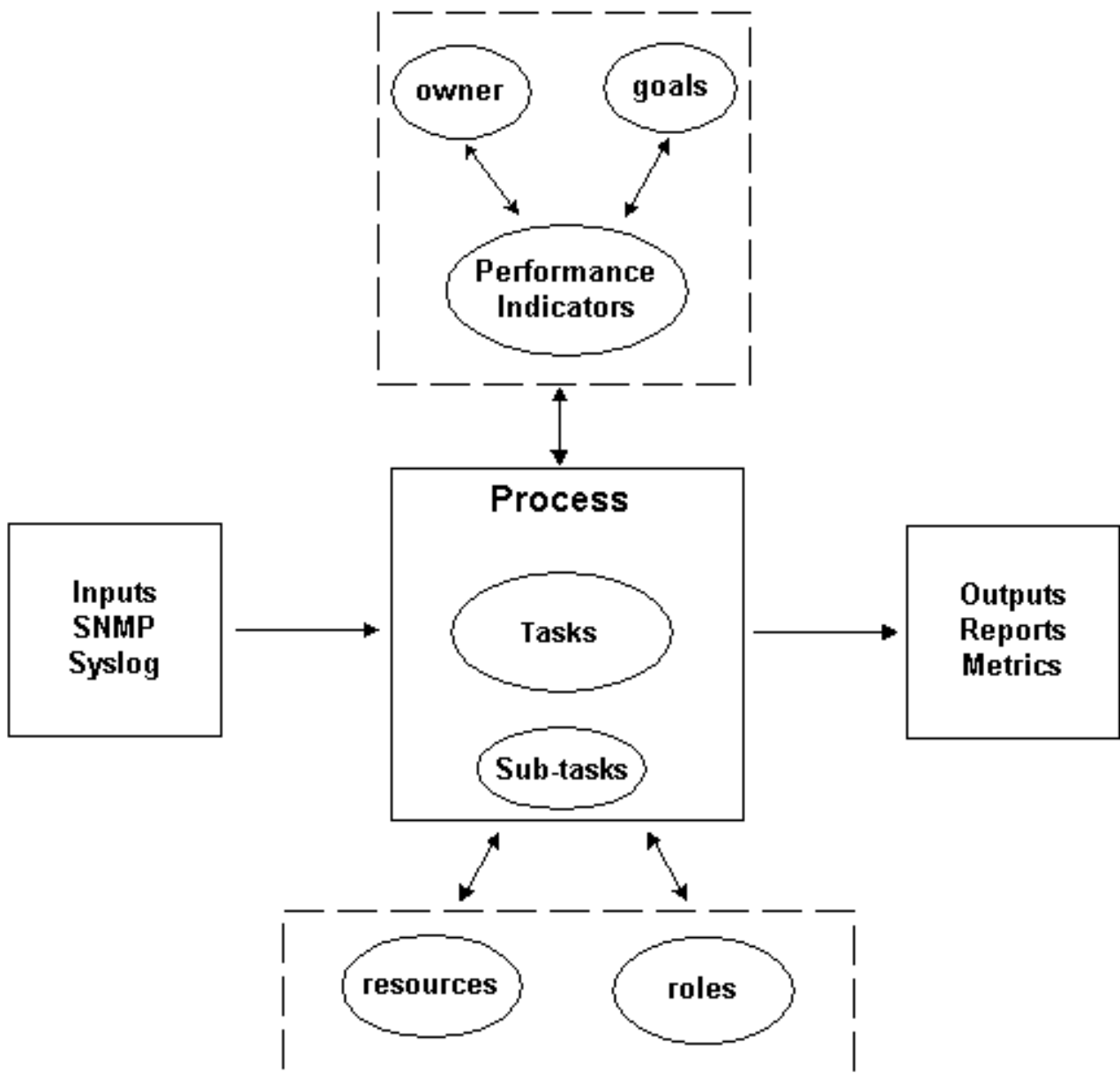
e.	
Soporte de área stub	Para que admitan routers con memoria insuficiente, las áreas pueden configurarse como stubs. Las LSA externas no se desbordan dentro y en todas las zonas fragmentadas. El ruteo a destinos externos en áreas stub se basa solamente en el valor predeterminado.

Definiciones de procesos

Una definición de proceso es una serie conectada de acciones, actividades y cambios realizados por agentes con el objeto de cumplir un propósito o alcanzar una meta.

El control de proceso es el proceso de planeamiento y regulación, con el objetivo de ejecutar un proceso de manera efectiva y eficiente.

Esto se muestra gráficamente en la siguiente figura.



El resultado del proceso debe cumplir con las normas operativas definidas por una organización y basadas en los objetivos de la empresa. Si el proceso cumple con el conjunto de normas, se considera eficaz ya que se puede repetir, medir, administrar y además, contribuye con los objetivos comerciales. Si las actividades se realizan con un mínimo esfuerzo, el proceso también se considera eficaz.

Propietario del proceso

Los procesos abarcan varios límites organizativos. Por consiguiente, es importante tener un único propietario del proceso que sea responsable de la definición del proceso. El propietario es el elemento fundamental para determinar e informar si el proceso es eficaz y eficiente. Si el proceso no es eficaz o eficiente, el titular del proceso será quien haga las modificaciones al proceso. La modificación del proceso está regida por los procesos de control y revisión de cambios.

Metas de procesos

Los objetivos del proceso son establecidos para especificar la dirección y el alcance para la

definición del proceso. Las metas también se utilizan para definir mediciones que se utilizan para medir la eficacia de un proceso.

El objetivo de este proceso es proporcionar un marco para verificar la configuración implementada de una implementación OSPF en un diseño previsto y proporcionar un mecanismo para auditar periódicamente la implementación OSPF para asegurar la consistencia a lo largo del tiempo con respecto al diseño esperado.

[Indicadores de rendimiento de procesos'1](#)

Los indicadores de funcionamiento del proceso se utilizan para medir la efectividad de la definición del proceso. Los indicadores de rendimiento deben ser mensurables y cuantificables. Los indicadores de rendimiento que se presentan a continuación son numéricos o se miden por tiempo. Los indicadores de rendimiento para el proceso de administración de configuración OSPF se definen de la siguiente manera:

- La cantidad de tiempo requerida para ejecutar todo el proceso.
- La frecuencia de ejecución requerida para detectar de manera proactiva los problemas OSPF antes de que impacten a los usuarios.
- La carga de la red asociada a la ejecución del proceso.
- Cantidad de medidas correctivas recomendadas por el proceso.
- El número de acciones correctivas implementadas como resultado del proceso.
- La cantidad de tiempo solicitado para instrumentar las acciones correctivas.
- La cantidad de tiempo solicitado para instrumentar las acciones correctivas.
- La acumulación de acciones correctivas.
- El tiempo de inactividad atribuido a problemas relacionados con OSPF.
- El número de elementos agregados, eliminados o modificados en el archivo simiente. Ésta es una indicación de precisión y estabilidad.

[Entradas del proceso](#)

Las entradas del proceso se utilizan para definir los criterios y los requisitos previos de un proceso. Muchas veces, la identificación de los procesos de entradas proporciona información sobre dependencias externas. A continuación, encontrará una lista de las entradas relacionadas con la administración de la configuración de OSPF.

- documentación de diseño OSPF
- Obtención de datos de MIB de OSPF por el sondeo de SNMP
- Información de syslog

[Resultado del proceso](#)

Las salidas de proceso se definen de la siguiente manera:

- Informes de configuración OSPF definidos en la sección [Presentación de datos](#) de este documento
- Recomendaciones de configuración OSPF para llevar a cabo acciones correctivas

[Definiciones de tareas](#)

Las siguientes secciones definen la inicialización y las tareas iterativas asociadas con la administración de la configuración de OSPF.

Tareas de inicialización

Las tareas de inicialización son ejecutadas una vez durante la implementación del proceso y no deben ser ejecutadas con cada iteración del proceso.

Verifique las tareas de requisitos previos

Al verificar las tareas previas necesarias, si se determina que cualquiera de ellas no está implementada o no proporciona información suficiente como para satisfacer las necesidades de este procedimiento, este hecho debe quedar documentado por parte del propietario del proceso y presentado a la administración. La tabla a continuación describe las tareas previas de inicialización necesarias.

Tarea previa necesaria	Descripción
Entradas y objetivos de la tarea	<ol style="list-style-type: none"> 1. Verifique la existencia de los documentos de diseño de OSPF y que la siguiente información esté disponible en los documentos de diseño de red: Definiciones de área: nombres, rangos de direcciones y tipo de área identificaciones de Router de borde de área/Router de borde del sistema autónomo (ABR/ASBR) Identificación DR/BDR Interfaces y nodos del Registro de Internet (IR) asignados a áreas 2. Utilice una plantilla de configuración estándar SNMP para verificar que SNMP esté configurado en la red. Nota: Esto se utiliza más adelante como entrada para crear el archivo simiente. 3. Use una plantilla de configuración de Syslog estándar para verificar que Syslog esté implementándose en la red.
Resultado de la tarea	La salida de la tarea es un informe de estado sobre la condición de las tareas previas necesarias. Si cualquiera de las tareas de respaldo se considera ineficaz, el propietario del proceso debe enviar una solicitud para que se actualicen los procesos de respaldo. Si los procesos de soporte no se pueden actualizar, realice una evaluación del impacto de este proceso.
Func	Conjunto de habilidades de ingeniero de red

ión de la tare a	
---------------------------	--

Crear un archivo simiente

El proceso de administración de configuración OSPF requiere del uso de un archivo simiente para eliminar la necesidad de contar con una función de detección de red. El archivo proveedor registra un conjunto de routers que están controlados por el proceso OSPF y también se usa como punto focal para coordinarse con los procesos de administración de cambios en una organización. Por ejemplo, si se ingresan nodos nuevos en la red, éstos deben ser agregados al archivo simiente OSPF. Si se realizan cambios en los nombres de comunidad SNMP debido a los requisitos de seguridad, esas modificaciones deberán reflejarse en el archivo simiente. La siguiente tabla describe los procesos para crear un archivo simiente.

Proces o	Descripción
Obj etiv os de la Tar ea	Cree un archivo simiente que se utilizará para inicializar el software de administración de configuración OSPF. El formateo del archivo simiente depende de los recursos utilizados para implementar el proceso de administración de configuración OSPF. Si se desarrollan scripts personalizados, el diseño del software define el formato del archivo simiente. Si se usa un sistema de administración de red (NMS), el formato del archivo simiente es definido por la documentación de NMS.
Entr ada s de tare as	<ol style="list-style-type: none"> 1. Formatee el archivo simiente. 2. Utilice la documentación de diseño de OSPF para identificar los siguientes datos: Direcciones IP de todos los nodos Identificaciones de comunidad SNMP Cuentas y contraseñas de inicio de sesión de Telnet y CLI. 3. Programe y/o nombres de contacto para el proceso de administración de cambios en la red.
Sali da de la tare a	Un archivo simiente para el proceso de administración de la configuración OSPF.
Rec urso s de la	<ul style="list-style-type: none"> • Sistema comercial NMS • Sistema de software desarrollado de forma personalizada • Proceso manual: inicie sesión en cada

tarea	elemento de red y ejecute líneas de comandos y registre el resultado.
Función de la tarea	<ul style="list-style-type: none"> • NMS: ingeniero de red, administrador de NMS y conjuntos de habilidades de secuencias de comandos de NMS. • Guiones personalizados: conjunto de habilidades de ingeniero de red y script NMS. • Procesos manuales: ingeniero de red.

Tareas iterativas

Las tareas iterativas se ejecutan con cada iteración del proceso y su frecuencia se determina y modifica para mejorar los indicadores de rendimiento.

Mantener el archivo simiente

El archivo simiente es crítico para la implementación efectiva del proceso de administración de la configuración OSPF. Por consiguiente, el estado actual del archivo simiente debe ser administrado en forma activa. El propietario del proceso de administración de configuración OSPF debe realizar un seguimiento de los cambios en la red que afectan al contenido del archivo simiente.

Proceso	Descripción
Objetivos de la Tarea	<ol style="list-style-type: none"> 1. Mantenga la moneda del archivo simiente mediante el seguimiento y las interacciones con las funciones organizativas que controlan los movimientos, las adiciones, los cambios y las modificaciones de la configuración de red. 2. Mantener el control de la versión y de la copia de respaldo para el archivo simiente.
Entradas de tareas	<ol style="list-style-type: none"> 1. La información sobre la administración de cambios, como movimientos, adiciones, o cambios que afectan el contenido del archivo simiente. 2. Información de ingeniería/diseño que afecta el contenido del archivo simiente.
Salida de la tarea	<ol style="list-style-type: none"> 1. Informe semanal sobre el estado del valor del archivo simiente. 2. Definición y documentación que describe la ubicación y los procedimientos de restauración de copias de seguridad de archivos simientes.
Recursos de la	<ul style="list-style-type: none"> • Sistema comercial NMS • Sistema de software desarrollado de forma personalizada • Proceso manual: inicie sesión en cada

tarea	elemento de red y ejecute líneas de comandos y registre el resultado.
Función de la tarea	<ul style="list-style-type: none"> • NMS: ingeniero de red, administrador de NMS y conjuntos de habilidades de secuencias de comandos de NMS. • Guiones personalizados: conjunto de habilidades de ingeniero de red y script NMS. • Procesos manuales: ingeniero de red.

[Ejecute el escaneo de OSPF.](#)

Los dos pasos utilizados para ejecutar el escaneo OSPF son:

1. Recolección de los datos.
2. Analizando los datos.

La frecuencia de estos dos pasos variará según cómo se utilice el proceso. Por ejemplo, este proceso se puede utilizar para verificar las modificaciones de la instalación. En este caso, la recolección de datos se ejecuta antes y después del cambio y el análisis de datos se lleva a cabo luego del cambio a fin de determinar el éxito del cambio.

Si este proceso se utiliza para verificar los registros de diseños de administración de configuración OSPF, la recolección de datos y la frecuencia de análisis dependerán de la velocidad de cambio en la red. Por ejemplo, si existe una cantidad significativa de cambios en la red, las verificaciones de diseño se llevan a cabo una vez a la semana. Si hay muy pocos cambios en la red, las verificaciones de diseño no se realizan más de una vez al mes.

[Revisión de los informes OSPF](#)

El formato de los informes de la administración de la configuración de OSPF depende de los recursos usados para implementar el proceso de administración de configuración de OSPF. La siguiente tabla brinda formatos sugeridos de informe desarrollados de forma personalizada.

Informe	Formato
Entradas de tareas	Para los informes de administración de configuración OSPF, vea la sección Presentación de datos dentro de este documento.
Salida de la tarea	Si se encuentran problemas entre los informes de exploración y los registros de diseño lógico, se debe tomar una decisión con respecto a cuál ítem es correcto y cuál es incorrecto. El ítem incorrecto debe ser corregido. Esto puede implicar la modificación de los registros de diseño o un cambio en el orden de la red.
Recursos de	<ul style="list-style-type: none"> • Sistema comercial NMS • Sistema de software desarrollado de forma personalizada

la tarea	<ul style="list-style-type: none"> Manual: inicie sesión en cada elemento de red y ejecute líneas de comandos y registre el resultado
Función de la tarea	<ul style="list-style-type: none"> NMS: ingeniero de red, administrador de NMS y conjuntos de habilidades de secuencias de comandos de NMS. Guiones personalizados: conjunto de habilidades de ingeniero de red y script NMS. Procesos manuales: ingeniero de red.

Identificación de datos

Características de datos generales

La siguiente tabla describe los datos que pueden aplicarse a la gestión de configuración OSPF.

Datos	Descripción
Áreas OSPF	<p>La información que describe las áreas adjuntas del router, incluyen:</p> <ul style="list-style-type: none"> ID de área Autenticación de área Ejecuciones de SPF Cantidad de ABR en un área. Número de ASBR en un área Recuento de LSA de área: coherencia entre routers en un área Suma de comprobación de LSA de área: coherencia entre los routers del área Frecuencia de descartes de paquetes debido a errores de direccionamiento por área Frecuencia de descartes de paquetes de protocolo por el proceso de ruteo por área Frecuencia de rechazos de paquetes enrutados debido a la condición de ruta no encontrada por área.
Interfaces OSPF	<p>Describe una interfaz desde el punto de vista de OSPF tal como:</p> <ul style="list-style-type: none"> Dirección IP ID de área Estado administrativo Métricas OSPF asignadas a la interfaz Temporizadores OSPF asignados a la interfaz Estado OSPF
estado	Describe un vecino OSPF.

de vecino OSPF	<ul style="list-style-type: none"> • ID del router vecino • Estado vecino • Eventos de vecino: el número de veces que la relación de vecino ha cambiado de estado o se ha producido un error. • Cola de retransmisión de vecino: la longitud actual de la cola de retransmisión.
----------------	--

Identificación de datos SNMP

Actualmente, Cisco soporta el [MIB OSPF Versión 2 RFC 1253](#) . RFC 1253 no contiene definiciones de trampa SNMP para OSPF. La última versión de OSPF MIB es [RFC 1850 OSPF versión 2](#) . Las trampas SNMP se definen para OSPF en RFC 1850. RFC 1850 no se soporta en la implementación de Cisco de la MIB OSPF.

Para más detalles, consulte la sección de Datos de sondeo SNMP de este documento.

Consulte la página [Cisco Network Management Software](#) para obtener una lista definitiva de qué MIB se soportan en qué plataforma y versión de código.

Identificación de datos RMON

No se requieren datos específicos de RMON para este procedimiento.

Identificación de datos Syslog

En general, Syslog genera mensajes específicos para el servicio para diferentes tecnologías. Aunque la información de syslog es más adecuada para la administración de fallas y de rendimiento, la información suministrada aquí es una referencia. Para un ejemplo de información de Syslog OSPF generada por dispositivos de Cisco, consulte Mensajes de Error de OSPF.

Para obtener una lista completa de los mensajes del sistema por función, consulte [Mensajes y Procedimientos de Recuperación](#).

Identificación de datos IOS CLI de Cisco

En esta versión del procedimiento de administración de configuración OSPF, no se requieren datos de CLI.

Recolección de datos

Colección de datos SNMP

La siguiente tabla define los diferentes componentes de la recopilación de datos SNMP.

Compo nente de	Definición

datos SNMP	
Configuración general de SNMP	Consulte Configuración de SNMP para obtener información general sobre las mejores prácticas de configuración SNMP.
Configuración SNMP específica del servicio	No hay configuraciones específicas de servicio SNMP requeridas para este procedimiento.
requerimientos para SNMP MIB	Consulte la sección Identificación de datos que figura más arriba.
Grupo de consultas MIB de SNMP	Los datos sondeados SNMP son recolectados por un sistema comercial como hp OpenView o por scripts personalizados. Para obtener más información sobre los algoritmos de recopilación, vea la sección Ejemplo de Algoritmos de Recopilación de Datos de este documento.
recolección de trampas MIB SNMP	La versión actual de MIB de OSPF admitida en dispositivos Cisco no admite trampas SNMP. No se requieren trampas de SNMP para este procedimiento.

[Recopilación de datos de RMON](#)

No se requieren configuraciones RMON ni datos en esta versión del procedimiento.

[Recolección de datos de Syslog](#)

Las pautas generales de configuración de syslog están fuera del alcance de este documento. Para más información, consulte la [configuración y resolución de problemas del firewall Secure PIX de Cisco con una red interna única](#).

Los requerimientos específicos del OSPF (abrir la ruta más corta en primer lugar) son dirigidos por la configuración del router OSPF para registrar los cambios del vecino con un mensaje de syslog utilizando el siguiente comando:

```
OSPF_ROUTER(config)# ospf log-adj-changes
```

[Recolección de datos CLI de Cisco IOS](#)

En general, la CLI de Cisco IOS proporciona el acceso más directo a la información no procesada

incluida en el NE. No obstante, el acceso CLI está mejor preparado para los procedimientos de resolución de problemas y las actividades de administración de cambios que para la administración global de la configuración, según lo define este procedimiento. El acceso a través de CLI no pesará para la administración de una red grande. En estos casos, se requiere acceso a información automatizada.

En esta versión del procedimiento de administración de la configuración OSPF, no se requieren configuraciones CLI ni datos.

Presentación de datos

Informe de área OSPF

El siguiente es un formato de ejemplo para el informe de área OSPF. El formato del informe está determinado por las capacidades de un sistema comercial NMS, si se utiliza uno, o la salida diseñada de las secuencias de comandos personalizadas.

Área	Campos de datos	Última ejecución	Esta ejecución
ID de área nº 1	Autenticación		
	Ejecuciones de SPF		
	Recuento de ABR		
	Cuenta ASBR		
	Conteo de LSA		
	Suma de comprobación LSA		
	Errores de dirección		
	Ruteo de Descartes		
	No se ha encontrado ruta		
ID de área nº n	Autenticación		
	Ejecuciones de SPF		
	Recuento de ABR		
	Cuenta ASBR		
	Conteo de LSA		
	Suma de comprobación LSA		
	Errores de dirección		
	Ruteo de Descartes		
	No se ha encontrado ruta		

ID de nodo nro	az de #n	ID de área		
		Estado de la administración		
		Estado OSPF		
		Metrics/Costs/Timers		
	Interfaz ID #1	IP Address		
		ID de área		
		Estado de la administración		
		Estado OSPF		
		Metrics/Costs/Timers		
	Interfaz de #n	IP Address		
		ID de área		
		Estado de la administración		
		Estado OSPF		
		Metrics/Costs/Timers		

Informe de vecinos OSPF

El siguiente es un formato de ejemplo para el informe de vecino OSPF. En la práctica, el formato del informe se determina por las capacidades de un NMS (Sistema de administración de la red) comercial, si se utiliza uno, o por el resultado designado de la secuencia de comandos personalizada

Área	Dispositivo	Vecinos	Campos de datos	Última ejecución	Esta ejecución
ID de área nº 1	ID de nodo # 1	ID del vecino #1	ID del router		
			Dirección IP del router		
			Estado		
			Events		
			Cola de retransmisión		
		ID del vecino #n	ID del router		
			Dirección IP del router		
			Estado		
			Events		

	ID de nodo nro	ID del vecino #1	Cola de retransmisión		
			ID del router		
			Dirección IP del router		
			Estado		
			Events		
		Cola de retransmisión			
		ID del vecino #n	ID del router		
			Dirección IP del router		
			Estado		
			Events		
Cola de retransmisión					
ID de área nº n	ID de nodo # 1	ID del vecino #1	ID del router		
			Dirección IP del router		
			Estado		
			Events		
			Cola de retransmisión		
	ID del vecino #n	ID del router			
		Dirección IP del router			
		Estado			
		Events			
		Cola de retransmisión			
ID de nodo nro	ID del vecino #1	ID del router			
		Dirección IP del router			
		Estado			
		Events			
		Cola de retransmisión			

			n		
		ID del vecino #n	ID del router		
			Dirección IP del router		
			Estado		
			Events		
			Cola de retransmisión		

Herramientas comerciales y públicas para el monitoreo de Internet

Las herramientas comerciales existen para ayudar en la recopilación y el procesamiento de la información de registro del sistema (Syslog) y para la recopilación de sondeos de las variables MIB de SNMP generales.

No se conocen herramientas de monitoreo de Internet públicas o comerciales que soporten la administración de configuración OSPF como se define en este procedimiento. Por lo tanto, se requieren los procedimientos y las secuencias de comandos personalizados locales.

Datos de sondeo de SNMP

RFC 1213 de tabla de rutas

Nombre del Objeto	Descripción del Objeto
ipRoute Dest	La dirección IP de destino de la ruta. Una entrada con un valor de 0.0.0.0 se considera una ruta predeterminada. En la tabla pueden aparecer varias rutas a un único destino, pero el acceso a tales entradas múltiples depende de los mecanismos de acceso a tabla definidos por el protocolo de administración de red en uso. ::= { ipRouteEntry 1 } identificador de objeto = 1.3.6.1.2.1.4.21.1.1
ipRoute Mask	Indica que la máscara debe ser lógica con la dirección de destino antes de compararla con el valor del campo ipRouteDest. Para aquellos sistemas que no admiten las máscaras de subred arbitrarias, un agente crea el valor de ipRouteMask al determinar si el valor del campo ipRouteDest correspondiente pertenece a una red de clase A, B o C, mediante una de las siguientes redes de máscara: <ul style="list-style-type: none"> • Clase A = 255.0.0.0 • Clase B = 255.255.0.0

	<ul style="list-style-type: none"> • Clase C = 255.255.255.0 <p>Si el valor de ipRouteDest es 0.0.0.0, la ruta predeterminada, el valor de la máscara también es 0.0.0.0.</p> <p>Nota: Todos los subsistemas de IP Routing utilizan implícitamente este mecanismo.</p> <p>::= { ipRouteEntry 11 } identificador de objeto = 1.3.6.1.2.1.4.21.1.11</p>
ipRouteNextHop	<p>La dirección IP del siguiente salto de esta ruta. En el caso de un límite de ruta a una interfaz que se obtiene con medios de difusión, el valor de este campo es la dirección de IP del agente en la interfaz. ::= { ipRouteEntry 7 } identificador de objeto = 1.3.6.1.2.1.4.21.1.7</p>
ipRouteIfIndex	<p>El valor de índice que identifica de forma única la interfaz local a través de la cual se alcanza el salto siguiente de la ruta. Esta interfaz es la misma interfaz identificada por el valor IfIndex. ::= { ipRouteEntry 2 } identificador de objeto = 1.3.6.1.2.1.4.21.1.2</p>

Objetos misceláneos de RFC 1213

Nombre del Objeto	Descripción del Objeto
ipAdEntIfIndex	<p>Valor del índice que identifica de manera exclusiva la interfaz aplicable a la entrada. Esta interfaz es la misma interfaz identificada por el valor IfIndex. ::= { ipAddrEntry 2 } identificador de objeto = 1.3.6.1.2.1.4.20.1.2</p>
ipInAddrErrors	<p>Cantidad de datagramas de entrada descartados debido a que la dirección IP en sus encabezados IP era un campo de destino no válido para la entidad. Este recuento incluye direcciones no válidas (0.0.0.0) y direcciones de clase no admitidas (clase E). Para entidades que no son puertas de enlace IP y que no reenvían datagramas, el contador incluye datagramas descartados porque la dirección de destino no era una dirección local. { ip 5 } object identificador = 1.3.6.1.2.1.4.5</p>
ipRoutingDiscards	<p>El número de entradas de ruteo válidas descartadas. Una razón posible para descartar tal entrada es liberar espacio del búfer para otras entradas de ruteo. { ip 23 } identificador de objeto = 1.3.6.1.2.1.4.23</p>
ipOutNoRoutes	<p>El número de datagramas IP descartados debido a que no se pudo encontrar una ruta para transmitirlos a su destino. { ip 12 } identificador de objeto = 1.3.6.1.2.1.4.12</p>

Nombre del Objeto	Descripción del Objeto
ospfAreaID	Un entero de 32 bits identifica de forma única un área. El ID de área 0.0.0.0 se utiliza para la estructura básica OSPF. ::= { ospfAreaEntry 1 } identificador de objeto = 1.3.6.1.2.1.14.2.1.1
Tipo ospfAuth	El tipo de autenticación especificado para este área. Es posible asignar tipos de autenticación adicionales localmente por área. El valor predeterminado es 0. ::= { ospfAreaEntry 2 } identificador de objeto = 1.3.6.1.2.1.14.2.1.2
OspfSpfRuns	La cantidad de veces que la tabla de ruta dentro del área se ha calculado usando la base de datos de estado de link de esta área. identificador de objeto = 1.3.6.1.2.1.14.2.1.4
ospfAreaBdrRtrCount	La cantidad total de ABR que puede alcanzarse dentro de esta área. Esto es 0 inicialmente, el valor predeterminado, y es calculado en cada pase SPF. ::= { ospfAreaEntry 5 } identificador de objeto = 1.3.6.1.2.1.14.2.1.5
ospfASBdrRtrCount	El número total de ABSR alcanzable dentro de esta área. Esto es inicialmente 0 (el valor predeterminado) y se calcula en cada paso SPF. ::= { ospfAreaEntry 6 } identificador de objeto = 1.3.6.1.2.1.14.2.1.6
ospfAreaLSACount	Número total de LSA en la base de datos de estado de link de un área, excluidas las LSA externas. El valor predeterminado es 0. ::= { ospfAreaEntry 7 } identificador de objeto = 1.3.6.1.2.1.14.2.1.7
ospfAreaLSACksumSum	La suma de 32 bits sin asignar de las sumas de comprobación LS de LSA contenidas en la base de datos de estado de link de área. Esta suma excluye los LSA externos (LS tipo 5). La suma puede ser utilizada para determinar si ha habido un cambio en la base de datos de estados del link y para comparar las bases de datos de estados del link de los dos routers. El valor predeterminado es 0. ::= { ospfAreaEntry 8 } identificador de objeto = 1.3.6.1.2.1.14.2.1.8

Tabla de interfaz OSPF RFC 1253

Nombre del	Descripción del Objeto

Objeto	
OspfIfIpAddress	La dirección IP de la interfaz OSPF. Identificador de objeto = 1.3.6.1.2.1.14.7.1.1
OspfIfEvents	La cantidad de veces que la interfaz OSPF ha cambiado su estado o se ha producido un error. Identificador de objeto = 1.3.6.1.2.1.14.7.1.15
OspfIfState	El estado de la interfaz OSPF. identificador de objetos = 1.3.6.1.2.1.14.7.1.12

Tabla de vecino OSPF RFC 1253

Nombre del Objeto	Descripción del Objeto
OspfNbrIpAddress	La dirección IP de este vecino. ::= { ospfNbrEntry 1 } identificador de objeto = 1.3.6.1.2.1.14.10.1.1
ospfNbrAddressesLessIndex	El valor correspondiente a IfIndex en la MIB estándar de Internet sobre un índice que no tiene una dirección IP. Al crear filas, esto se puede derivar de la instancia. ::= { ospfNbrEntry 2 } identificador de objeto = 1.3.6.1.2.1.14.10.1.2
ospfNbrRtrId	Un entero de 32 bits, representado como una dirección IP, que identifica de forma única al router vecino en el sistema autónomo. El valor predeterminado es 0.0.0.0. ::= { ospfNbrEntry 3 } identificador de objeto = 1.3.6.1.2.1.14.10.1.3
ospfNbrState	El estado de la relación con el vecino. Los estados son: <ul style="list-style-type: none"> • down (1) • intento (2) • init (3) • twoWay (4) • exchangeStart (5) • intercambio (6) • carga (7) • completo (8). ::= { ospfNbrEntry 6 } identificador de objeto = 1.3.6.1.2.1.14.10.1.6
ospfNbrEvents	La cantidad de veces que se ha modificado el estado de la relación de vecino o que se ha producido un error. El valor predeterminado es 0. ::= { ospfNbrEntry 7 } identificador de objeto = 1.3.6.1.2.1.14.10.1.7
ospfNbrLSRRetransQLen	La longitud actual de la cola de retransmisión. El valor predeterminado es 0. ::= { ospfNbrEntry 8 } identificador de objeto = 1.3.6.1.2.1.14.10.1.8

Algoritmos de obtención de datos de ejemplo

Durante la investigación de este trabajo se desarrolló un programa prototipo "C". El programa, denominado oscan, se creó utilizando Microsoft Developer Studio 97 con Visual C++ versión 5.0. Hay dos librerías específicas que proveen la Interfaz de programación de aplicaciones (API) de la función SNMP. Estas bibliotecas son snmpapi.lib y mgmtapi.lib

Las funciones proporcionadas por la API de Microsoft se agrupan en tres categorías principales y se enumeran en la tabla siguiente.

Funciones del agente	Funciones del administrador	Funciones de utilidad
SnmpExtensionInit	SnmpMgrClose	SnmpUtilUtilMemUnloc
SnmpExtensionInitEx	SnmpMgrGetTrap	SnmpUtilUtilMemFree
SnmpExtensionQuery	SnmpMgrOidToString	SnmpUtilOidAppend
SnmpExtensionTrap	SnmpMgrOpen	SnmpUtilOidCmp
	SnmpMgrRequest	SnmpUtilOidCpy
	SnmpMgrStringToOid	SnmpUtilOidFree
	SnmpMgrTrapListen	SnmpUtilOidFree
		SnmpUtilPrintAsnSnmp
		Cualquier
		SnmpUtilVarBindCpy
		SnmpUtilVarBindListCpy
		SnmpUtilVarBindFree
		SnmpUtilVarBindListFree

El código del prototipo oscan encapsuló la API de Microsoft con un conjunto de funciones adicionales enumeradas a continuación.

- snmpWalkStrOid
- snmpWalkAsnOid
- snmpWalkVarBind
- snmpWalkVarBindList

Estas funciones proporcionan un API genérico que permita acceder a las diversas tablas SNMP MIB utilizadas para mantener los datos de configuración de OSPF. El identificador de objeto (OID) de la tabla a la que se accederá se pasa a la API oscan, junto con una función de devolución de llamada específica de la tabla. La función de devolución de llamadas tiene la inteligencia de actuar según los datos devueltos desde las tablas.

Rutina principal

La primera tarea es crear una lista de nodos que serán el destino del programa oscan. Para evitar el problema de "detección de dispositivos", se requiere un archivo simiente para identificar los nodos que se van a escanear. El archivo simiente brinda información como la dirección IP y las cadenas de comunidad SNMP de sólo lectura.

El programa oscan necesita mantener varias estructuras de datos internas para almacenar la información SNMP que se recopila desde los routers. En general, hay una estructura interna de datos para cada tabla de MIB de SNMP que se recopila.

```

Main
load node array based on information in the seed file.
while more entries in the node array
start SNMP session for this node
collect IP route table for this node
collect OSPF area table for this node
collect OSPF Neighbor table for this node
collect sysName for this node
collect OSPF Interface table for this node
end SNMP session for this node
end while

```

Tabla de ruta IP

Se debe tener cuidado al acceder a la tabla de rutas IP con SNMP, ya que es sencillo sobrecargar la CPU de un router durante esta operación. En consecuencia, el programa oscan utiliza un parámetro de retardo configurable por el usuario. El parámetro proporciona un retraso entre cada petición de SNMP. Para entornos grandes, esto significa que el tiempo total para recopilar la información puede ser muy significativo.

La tabla de rutas incluye cuatro secciones de información que le interesan a oscan:

- ipRouteDest
- ipRouteMask
- ipRouteNextHop
- ipRouteIfIndex

La tabla de ruta es indexada por ipRouteDest. Por lo tanto, cada objeto que se devuelve de la **solicitud get-request** SNMP tiene el ipRouteDest agregado al OID.

El objeto ipRouteIfIndex es un entero que se utiliza en la tabla de direcciones IP para indexar (ipAddrTable). La ipAddrTable se indexa por medio del objeto ipAdEntAddr (la dirección IP de la interfaz). Para obtener la dirección IP de la interfaz, es necesario pasar por un proceso que consta de cuatro etapas:

1. Recoja el ipRouteIfIndex desde la tabla de ruteo.
2. Acceda a ipAddrTable usando ipRouteIfIndex para coincidencia de patrones.
3. Al encontrar un patrón, convierta el OID en una cadena y recolecte los cuatro últimos campos con punto decimal que serán la dirección IP de la interfaz.
4. Vuelva a guardar la dirección IP de la interfaz en la tabla de ruta IP.

El algoritmo general para acceder a la tabla de ruteo IP se muestra a continuación. En este punto, sólo se almacena el valor integer de ipRouteIfIndex. Más adelante en el proceso, cuando se recopile la información de la interfaz, se accede a la ipAddrTable (Tabla de direcciones IP) y la información restante se recopila y se ubica dentro de la tabla de ruteo de IP interna.

```

OID List =
ipRouteDestOID,
ipRouteMaskOID,
ipRouteNextHopOID,
ipRouteIfIndexOID;

```

```

For each object returned by SNMP route table walk
Sleep // user configurable polling delay.

```



```

check varbind oid against OID list
if OID is ipRouteDestOID
add new entry in the internal route table array
if OID is one of the others
search internal route array for matching index value
store information in array

```

La información obtenida se representa en una tabla similar al resultado familiar del router CLI a continuación.

```

ROUTE TABLE
*****
Destination      Mask                GW                  Interface
10.10.10.4        255.255.255.252    10.10.10.5         10.10.10.5
10.10.10.16       255.255.255.252    10.10.10.6         10.10.10.5
10.10.10.24       255.255.255.252    10.10.10.25        10.10.10.25
10.10.10.28       255.255.255.252    10.10.11.2         10.10.11.1
10.10.10.36       255.255.255.252    10.10.10.6         10.10.10.5
10.10.11.0        255.255.255.0      10.10.11.1         10.10.11.1
10.10.13.0        255.255.255.0      10.10.11.2         10.10.11.1

```

Tabla de Área OSPF

La recopilación de información de una tabla de área OSPF se realiza por medio del escaneo de la tabla de área OSPF (ospfAreaTable) y el procesamiento de los datos a medida que retornan. El índice para ospfAreaTable es ospfAreald. El ospfAreald se almacena en formato decimal punteado el cual es idéntico a una dirección IP. Por lo tanto, las mismas subrutinas que se utilizaron para procesar y buscar ipRouteTable e ipRouteIndex se pueden volver a utilizar aquí.

Hay varios elementos de datos que no están realmente en la tabla de área OSPF que se incluyen en esta sección. Por ejemplo, los objetos ipInAddrErrors, IpRoutingDiscards e ipOutNoRoute se encuentran en la definición MIB-2, pero no están asociados con un área OSPF. Estos objetos están asociados a un router. Por lo tanto, estos contadores son usados como área métrica agregando los valores para cada nodo en un área a un contador de área. Por ejemplo, en el informe de área OSPF, la cantidad de paquetes rechazados debido a que no se encontró ruta es, en realidad, la suma de los paquetes rechazados por todos los routers de esa área. Esta es una métrica de nivel elevado que provee una descripción general de la integridad del ruteo del área.

```

OID List =
ipInAddrErrorsOID,
ipRoutingDiscardsOID,
ipOutNoRouteOID,
areaIdOID,
authTypeOID,
spfRunsOID,
abrCountOID,
asbrCountOID,
lsaCountOID,
lsaChecksumSumOID;

```

```

For object returned from the SNMP walk of the Area Table
Sleep // user configurable polling delay.
check varbind oid against OID list.
if OID is ospfAreaId
add new entry in the internal route table array
if OID one of the others
search internal array for matching index value

```

```

store information in array
end of for loop
get ipInAddrErrors, ipRoutingDiscards, ipOutNoRoute
add values to overall Area counters

```

La información recopilada está representada en la tabla ASCII que se encuentra a continuación.

```

AREAS
*****
AREA = 0.0.0.0AREA = 0.0.0.2
authType = 0authType = 0
spfRuns = 38spfRuns = 18
abrCount = 2abrCount = 1
asbrCount = 0asbrCount = 0
lsaCount = 11lsaCount = 7
lsaCksumSum = 340985lsaCksumSum = 319204
ipInAddrErrors = 0 ipInAddrErrors = 0
ipRoutingDiscards = 0ipRoutingDiscards = 0
ipOutNoRoutes = 0ipOutNoRoutes = 0

```

Tabla de Vecinos OSPF

El índice de la tabla vecina es de dos valores:

- ospfNbrIpAddr: la dirección IP del vecino es ospfNbrIpAddr.
- ospfNbrAddresslessIndex: ospfNbrAddresslessIndex puede ser uno de dos valores: Para una interfaz con una dirección IP asignada, es cero. Para una interfaz que no tiene una dirección IP asignada, el valor se interpreta como el IfIndex de la MIB estándar de Internet.

Al haber dos valores para el índice, es necesario que ajuste los algoritmos que se usaron anteriormente para obtener la información adicional que se adjunta a los OID devueltos. Después de realizar este ajuste, las mismas subrutinas que se utilizaron para procesar y buscar ipRouteTable e ipRouteIfIndex se pueden volver a utilizar aquí.

```

OID List =
ospfNbrIpAddrOID,
ospfNbrAddressLessIndexOID,
ospfNbrRtrIdOID,
ospfNbrStateOID,
ospfNbrEventsOID,
ospfNbrLSRetransQLenOID,

```

```

For object returned from the SNMP walk of the Neighbor Table
Sleep // user configurable polling delay.
check varbind OID against OID list.
if OID matches ospfNbrIpAddr
add new entry in the internal neighbor table array
if OID matches one of the others
search array for matching index value
store information in array

```

La información recopilada está representada en la tabla ASCII que se encuentra a continuación.

```

NEIGHBORS
*****
NEIGHBOR #0NEIGHBOR #1

```

Nbr Ip Addr = 10.10.10.6Nbr Ip Addr = 10.10.11.2
Nbr Rtr Id = 10.10.10.17Nbr Rtr Id = 10.10.10.29
Nbr State = 8Nbr State = 8
Nbr Events = 6Nbr Events = 30
Nbr Retrans = 0Nbr Retrans = 0

[Información Relacionada](#)

- [Guía de configuración de OSPF](#)
- [Experiencia de RFC 1246 con el protocolo OSPF](#)
- [Análisis del protocolo OSPF de RFC 1245](#)
- [RFC 1224 Técnicas para administrar alertas generadas asincrónicamente](#)
- [Página de Soporte OSPF](#)
- [Página de Soporte de IP Routing](#)
- [Soporte Técnico - Cisco Systems](#)