Sistema de administración de red: Informe oficial de Mejores Prácticas

Contenido

Introducción

El modelo de administración de red del International Organization for Standardization (ISO) define cinco zonas funcionales de administración de red. Este documentos abarca todas las áreas funcionales. El propósito total de este documento es proporcionar a las recomendaciones prácticas en cada área funcional de aumentar las herramientas de administración y las prácticas de la eficacia general de las actuales. También proporciona a la instrucción de diseño para la instrumentación de la herramienta de administración de red y las Tecnologías futuras.

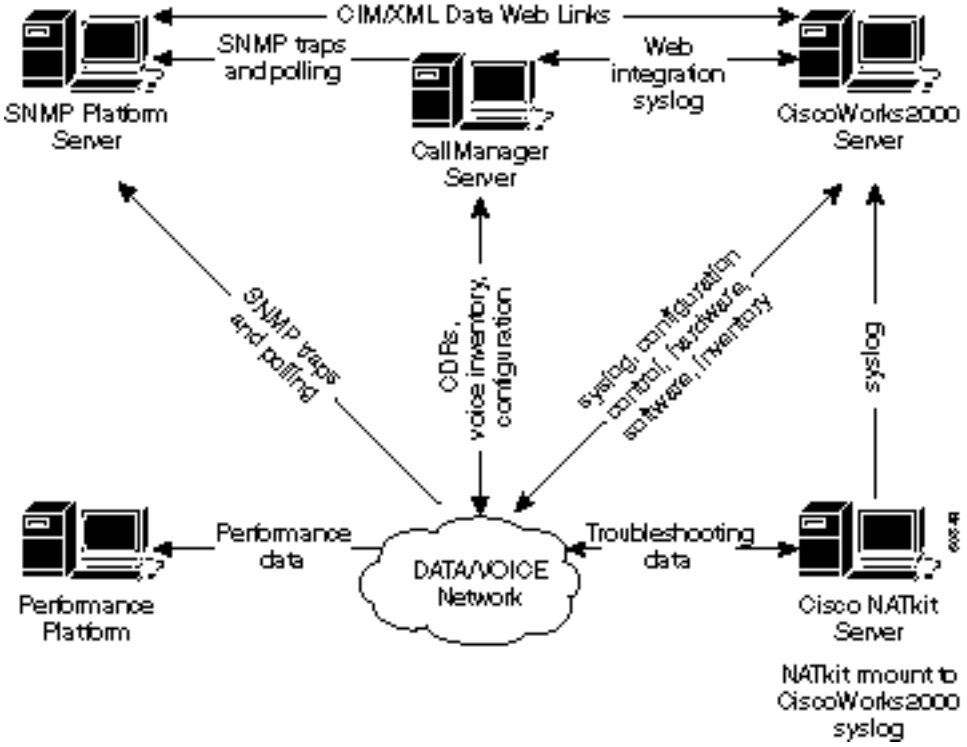
Administración de la red

Las cinco áreas funcionales del modelo de administración de red ISO son mencionadas abajo.

- Administración de incidente — Detecte, aísle, notifique, y corrija los incidentes encontrados en la red.

- Administración de la configuración — Configuraciones de aspecto de los dispositivos de red tales como administración de archivos de configuración, Administración de inventario, y administración del software.
- Administración del rendimiento — Monitor y aspectos del rendimiento de la medida diversos para poder mantener el rendimiento general en un nivel aceptable.
- Administración de seguridad — Proporcione al acceso a los dispositivos de red y a los recursos corporativos a los individuos autorizados.
- Administración de contabilidad — Información de uso de un recurso de la red.

El diagrama siguiente muestra que una arquitectura de referencia que Cisco Systems cree debe ser la solución mínima para manejar una red de datos. Esta arquitectura incluye a un servidor del CallManager de Cisco para los que planeen manejar el protocolo voice over internet (VoIP): El diagrama muestra cómo debe integrar el servidor del CallManager a la topología de NMS.



La arquitectura de administración de red incluye el siguiente:

- Plataforma del Simple Network Management Protocol (SNMP) para la Administración de incidente
- Plataforma de supervisión de rendimiento para la administración del rendimiento a largo plazo y tender
- Servidor CiscoWorks2000 para la administración de la configuración, la colección de syslog, y la administración de inventario de hardware y de software

Algunas plataformas SNMP pueden compartir directamente los datos con el servidor CiscoWorks2000 usando los métodos del Modelo de información común/Lenguaje de marcado extensible (CIM/XML). El CIM es un modelo de datos común de un esquema de instrumentación neutral para describir la información para administración total en un entorno de la red/de la empresa. El CIM se comprende de una especificación y de un esquema. La especificación define los detalles para la integración con otros modelos de administración tales como MIB o ficheros de información para administración de escritorio del grupo de trabajo de la Administración (DMTF MIFs) SNMP, mientras que el esquema proporciona a las descripciones del modelo real.

El XML es un lenguaje de marcado usado para representar los datos estructurados en la forma

textual. Una meta específica del XML era guardar la mayor parte de poder descriptivo del SGML mientras la eliminación tanto de la complejidad como sea posible. El XML es similar en el concepto al HTML, pero mientras que el HTML se utiliza para transportar la información gráfica sobre un documento, el XML se utiliza para representar los datos estructurados en un documento.

Los clientes del Advanced Services de Cisco también incluirían al servidor NATkit de Cisco para el control proactivo y el troubleshooting adicionales. El servidor NATkit cualquiera tendría un soporte remoto del disco (rmount) o acceso por Protocolo de transferencia de archivos (FTP) a los datos que residen en el servidor CiscoWorks2000.

El capítulo de las nociones básicas sobre administración de redes de la *descripción de tecnología de conexión entre redes* proporciona a una descripción más detallada con respecto a las nociones básicas sobre administración de redes.

Administración de incidente

El objetivo de la administración de fallas es detectar, registrar, notifica a los usuarios de, y (en la medida de lo posible) fije automáticamente los problemas de red para guardar la red el ejecutarse con eficacia. Porque los incidentes pueden causar el tiempo muerto o la degradación de red inaceptable, la Administración de incidente es quizás ejecutada lo más extensamente posible de los elementos de administración de red ISO.

Plataformas de administración de redes

Una plataforma de administración de redes desplegada en la empresa maneja una infraestructura que consista en los elementos de red de vendedores múltiples. La plataforma recibe y los eventos de procesos de los elementos de red en la red. Los eventos de los servidores y de otros recursos críticos se pueden también remitir a una plataforma de administración. Las funciones comúnmente disponibles siguientes se incluyen en una plataforma de administración estándar:

- Detección de red
- Mapeos de topología de elemento de red
- Administrador de evento
- Recolector de datos de rendimiento y grapher
- Buscador de datos de administración

Las plataformas de administración de redes se pueden ver como la consola principal para las operaciones de la red en la detección de los incidentes en la infraestructura. La capacidad de detectar los problemas en cualquier red es rápidamente crítica. Los personales de operaciones de la red pueden confiar en un mapa de la red gráfico para visualizar al estado operacional de elemento crítico de red tal como Routers y Switches.

Las plataformas de administración de redes tal HP OpenView, Computer Associates Unicenter, y SUN Solstice pueden realizar un descubrimiento de los dispositivos de red. Cada dispositivo de red es representado por un elemento gráfico en la consola de la plataforma de administración. Diversos colores en los elementos gráficos representan el estado de funcionamiento del dispositivo de red actual. Los dispositivos de red se pueden configurar para enviar las notificaciones, llamadas SNMP traps, a las plataformas de administración de redes. Sobre la recepción de las notificaciones, el elemento gráfico que representa el dispositivo de red cambia a un diverso color dependiendo de la gravedad de la notificación recibida. La notificación, generalmente llamada un evento, se pone en un archivo del registro. Es determinado importante que los ficheros más actuales del Management Information Base de Cisco (MIB) estén cargados

en la plataforma SNMP para asegurarse de que las diversas alertas de los dispositivos de Cisco están interpretadas correctamente.

Cisco publica los archivos MIB para manejar los diversos dispositivos de red. Los archivos MIB de Cisco están situados en el sitio web de cisco.com, e incluyen la siguiente información:

- Archivos MIB publicados en el formato SNMPv1
- Archivos MIB publicados en el formato SNMPv2
- SNMP traps utilizado en los dispositivos de Cisco
- OID para los objetos MIB de las actuales de Cisco SNMP

Varias plataformas de administración de redes son capaces de manejar los sitios distribuidos del múltiplo geográficamente. Esto es lograda intercambiando los datos de administración entre las consolas de administración en los sitios remotos por una estación de administración en el sitio principal. La ventaja principal de una arquitectura distribuida es que reduce el tráfico de administración, así, proporcionando a un más uso eficaz de ancho de banda. Una arquitectura distribuida también permite que los personales localmente manejen sus redes de los sitios remotos con los sistemas.

Una mejora reciente a las plataformas de administración es la capacidad remotamente a los elementos de red de administración usando una interfaz Web. Esta mejora elimina la necesidad del software cliente especial en las estaciones de usuario individual de tener acceso a una plataforma de administración.

Una empresa típica se comprende de diversos elementos de red. Sin embargo, cada dispositivo requiere normalmente los sistemas de administración de elemento específico del proveedor para manejar eficazmente los elementos de red. Por lo tanto, las estaciones de administración duplicados pueden sondear los elementos de red para la misma información. Los datos recogidos por diversos sistemas se salvan en las bases de datos diferentes, creando la tarea de administración para los usuarios. Esta limitación ha incitado el establecimiento de una red y los proveedores de software para adoptar los estándares tales como pedido de objeto común Broker la arquitectura (CORBA) y la Fabricación integrada por computadora (CIM) para facilitar el intercambio de los datos de administración entre las plataformas de administración y los sistemas de administración del elemento. Con los vendedores adoptando los estándares en el desarrollo del sistema de administración, los usuarios pueden contar con la Interoperabilidad y los Ahorros de costos en desplegar y el manejo de la infraestructura.

CORBA especifica un sistema que proporcione a la Interoperabilidad entre los objetos en un entorno heterogéneo, distribuido y de una forma que sea transparente al programador. Su diseño se basa en el modelo de objeto del grupo de administración de objetos (OMG).

Infraestructura de solución de problemas

El Trivial File Transfer Protocol (TFTP) y los servidores del registro del sistema (Syslog) son componentes fundamentales de una infraestructura del troubleshooting en las operaciones de la red. El servidor TFTP se utiliza sobre todo para salvar los archivos de configuración y las imágenes del software para los dispositivos de red. El Routers y el Switches son capaces de enviar los mensajes del registro del sistema a un servidor de Syslog. Los mensajes facilitan la función de Troubleshooting cuando se encuentran los problemas. De vez en cuando, el personal de servicio técnico de Cisco necesita los mensajes de Syslog realizar la Análisis de la causa de raíz.

La función distribuida de la colección de syslog del esencial de la administración de recursos

CiscoWorks2000 (esencial) permite el despliegue las estaciones de la colección de vario UNIX o de NT en los sitios remotos realizar la obtención de mensajes y la filtración. Los filtros pueden especificar qué mensajes de Syslog serán remitidos al servidor principal de Essentials. Un beneficio mayor de ejecutar de la recolección distribuida es la reducción de mensajes remitida a los servidores de Syslog principales.

Detección y notificación de incidente

El propósito de la administración de fallas es detectar, aislar, notificar, y corregir los incidentes encontrados en la red. Los dispositivos de red son capaces de alertar las estaciones de administración cuando un incidente ocurre en los sistemas. Un sistema de administración del error eficaz consiste en varios subsistemas. La detección de incidente es realizada cuando los dispositivos envían los mensajes del SNMP trap, la Consulta SNMP, los umbrales del Monitoreo remoto (RMON), y los mensajes de Syslog. Un sistema de administración alerta al usuario final cuando un incidente está señalado y las acciones correctivas pueden ser tomadas.

Los desvíos se deben activar constantemente en los dispositivos de red. Los desvíos adicionales se utilizan con las versiones de software del nuevo Cisco IOS para el Routers y el Switches. Es importante controlar y poner al día el archivo de configuración para asegurar la decodificación adecuada de trampa. Una revisión periódica de trampas configuradas con el equipo confiado Cisco de los servicios de red (American National Standard) asegurará la detección de error eficaz en la red.

La tabla siguiente enumera los desvíos CISCO-STACK-MIB por los cuales son utilizados, y se puede utilizar para vigilar las condiciones de incidente encendido, Switches del red de área local (LAN) del Cisco Catalyst.

Trampa	Descripción
moduleUp	La entidad del agente ha detectado que el **objeto moduleStatus** en este MIB transitioned **ok(2) al** estado para uno de sus módulos.
moduleDown	La entidad del agente ha detectado que el *objeto moduleStatus* en este MIB transitioned fuera **ok(2) del** estado para uno de sus módulos.
chassisAlarmOn	La entidad del agente ha detectado que el *chassisTempAlarm*, *chassisMinorAlarm*, o *objeto chassisMajorAlarm* en este MIB transitioned **on(2) al** estado. *Un chassisMajorAlarm* indica que existe una de las condiciones siguientes: • Cualquier falla de voltaje • Temperatura simultánea y error de la fan • El ciento por ciento de falla de la fuente de alimentación (dos fuera de dos, o una fuera de uno) • Error eléctricamente borrable de memoria programable de sólo lectura (EEPROM) • Error de memoria RAM no volátil (NVRAM) • Error de comunicación MCP

	• Estado de NMP desconocido Un chassisMinorAlarm indica que existe una de las condiciones siguientes: • Alarma de temperatura • Error de la fan • Falla parcial de la fuente de alimentación (una fuera de dos) • Dos fuentes de alimentación de tipo incompatible
chassisAlarmOff	La entidad del agente ha detectado que el *chassisTempAlarm*, *chassisMinorAlarm*, o *objeto chassisMajorAlarm* en este MIB transitioned **off(1) al** estado.

Los desvíos ambientales del monitor (envmon) se definen en el desvío CISCO-ENVMON-MIB. El desvío del envmon envía Cisco las notificaciones ambientales empresa-específicas del monitor cuando se excede un umbral ambiental. Cuando se utiliza el envmon, un tipo de trampa ambiental específico puede ser activado, o todos los tipos de trampa del sistema de monitor de entorno pueden ser validados. Si no se especifica ninguna opción, se activan todos los tipos ambientales. Puede ser uno o más de los valores siguientes:

- voltaje — Se envía un ciscoEnvMonVoltageNotification si el voltaje medido en un punto de prueba dado está fuera del iIntervalo normal para el punto de prueba (por ejemplo está en el amonestador, crítico, o la etapa de cierre).
- parada normal — Se envía un ciscoEnvMonShutdownNotification si el monitor ambiental detecta que un punto de prueba está alcanzando a un estado crítico y es alrededor iniciar una parada normal.
- fuente — Se envía un ciscoEnvMonRedundantSupplyNotification si la fuente de alimentación redundante (cuando sea extant) falla.
- fan — Se envía un ciscoEnvMonFanNotification si de las fans en el arsenal de la fan (cuando sea extant) falla.
- temperatura — Se envía un ciscoEnvMonTemperatureNotification si la temperatura medida en un punto de prueba dado está fuera del iIntervalo normal para el punto de prueba (por ejemplo está en el amonestador, crítico, o la etapa de cierre).

Los elementos de la detección y del monitoreo de la red de incidente se pueden ampliar del dispositivo llano al protocolo y a los niveles de la interfaz. Para un entorno de red, el control defectuoso puede incluir la red de área local virtual (VLA N), Asynchronous Transfer Mode (ATM), las indicaciones del incidente en las interfaces físicas, y así sucesivamente. La implementación de la administración de fallas en el nivel de protocolo está disponible con un sistema de administración del elemento tal como el encargado del campus CiscoWorks2000. La aplicación TrafficDirector en el encargado del campus se centra en el administrador de switches que utiliza la mini-RMON ayuda en el Switches del catalizador.

Con un número creciente de elementos de red y la complejidad de los problemas de red, un sistema de administración del evento que es capaz de correlacionar diversos eventos de red (Syslog, desvío, archivos del registro) puede ser considerado. Esta arquitectura detrás de un sistema de administración del evento es comparable a un sistema del administrador de administradores (MAMÁ). Un sistema de administración de eventos bien diseñado permite que los personales en el Network Operations Center (NOC) sean dinámicos y eficaces en la detección y el diagnóstico de los problemas de red. La priorización y la supresión del evento permiten que el

personal de operación de la red se centre en los eventos de la red crítica, que investigue varios sistemas de administración del evento incluyendo el Cisco Info Center, y que conduzca una análisis de factibilidad para explorar completamente las capacidades de tales sistemas. Para obtener más información, vaya al Cisco Info Center.

Supervisión y notificación de incidentes proactivos

La alarma RMON y el evento son dos grupos definidos en la especificación de RMON. Normalmente, una estación de administración realiza la interrogación en los dispositivos de red para determinar el estatus o el valor de ciertas variables. Por ejemplo, una estación de administración sondea a un router para descubrir la utilización de la Unidad de procesamiento central (CPU) y para generar un evento cuando el valor golpea los alcances un umbral configurado. Este método pierde el ancho de banda de la red y puede también faltar el umbral real dependiendo del intervalo de sondeo.

Con la alarma RMON y los eventos, un dispositivo de red se configura para vigilarse para los umbrales de levantamiento y que caen. En un intervalo de tiempo predefinido, la voluntad del dispositivo de red recoge una muestra de una variable y la compara contra los umbrales. Un SNMP trap se puede enviar a una estación de administración si el valor real se excede o baja debajo de los umbrales configurados. Los grupos de la alarma RMON y del evento proporcionan a un método proactivo de manejar los dispositivos de red críticos.

Cisco Systems recomienda el ejecutar de la alarma RMON y del evento en los dispositivos de red críticos. Las variables vigiladas pueden incluir la utilización CPU, los errores del almacenador intermediario, los descensos de la entrada-salida, o cualquier variable de los tipos del número entero. Comenzando con el Cisco IOS Software Release 11.1(1), todas las imágenes del router utilizan los grupos de la alarma RMON y del evento.

Para información detallada sobre la implementación de eventos y alarma de RMON, refiera a la sección de implementación de eventos y alarma de RMON.

Restricciones de memoria RMON

El USO de memoria RMON es constante a través de todas las plataformas del switch seleccionar referente las estadísticas, los historiales, las alarmas, y a los eventos. RMON utiliza qué se llama un *compartimiento* para salvar los historiales y las estadísticas en el agente RMON (que es el conmutador en este caso). El tamaño del compartimiento se define en la punta de prueba RMON (dispositivo de SwitchProbe) o la aplicación RMON (herramienta TrafficDirector), después se envía al conmutador que se fijará.

Aproximadamente 450 K de espacio de códigos es necesarios utilizar mini-RMON (por ejemplo, cuatro grupos RMON: estadísticas, historial, alarmas, y eventos). El requisito de memoria dinámica para RMON varía porque depende de la configuración de tiempo de ejecución.

La tabla siguiente define el información sobre el USO de la memoria RMON de tiempo de ejecución para cada mini-RMON grupo.

Definición del grupo RMON	Espacio en DRAM usado	Notas
Estadístic	140 bytes por	Por el puerto

as	Ethernet/Fast Ethernet el puerto cambiado	
Historial	3.6 K para 50 compartimientos *	Cada compartimiento adicional utiliza 56 bytes
Alarma y evento	2.6 K por la alarma y sus entradas de evento correspondiente	Por la alarma por el puerto

El *RMON utiliza qué se llama un *compartimiento* para salvar los historiales y las estadísticas en el agente RMON (tal como un conmutador).

Alarma RMON e implementación de eventos

Incorporando RMON como parte de una solución de administración del incidente, un usuario puede dinámico vigila la red antes de que ocurra un problema potencial. Por ejemplo, si el número de paquetes de broadcast recibidos aumenta perceptiblemente, puede causar un aumento en la utilización CPU. Ejecutando la alarma RMON y el evento, un usuario puede poner un umbral para vigilar el número de paquetes de broadcast recibidos y para alertar la plataforma SNMP mediante un SNMP trap si se alcanza el umbral configurado. Las alarmas RMON y los eventos eliminan el sondeo excesivo realizados normalmente por la plataforma SNMP para lograr la misma meta.

Dos métodos están disponibles de cuál configurar la alarma RMON y el evento:

- Comando line interface(cli)
- CONJUNTO SNMP

La demostración siguiente de los procedimientos de la muestra cómo fijar un umbral para vigilar el número de paquetes de broadcast recibidos en un interfaz. El mismo contador se utiliza en estos procedimientos como se muestra en el ejemplo del comando show interface en el extremo de esta sección.

Ejemplo de la interfaz de línea de comandos

Para ejecutar la alarma RMON y el evento usando el CLI interconecte, realice los pasos siguientes:

1. Encuentre el índice del interfaz asociado a los Ethernetes 0 recorriendo el MIB ifTable.
```
interfaces.ifTable.ifEntry.ifDescr.1 = "Ethernet0"
interfaces.ifTable.ifEntry.ifDescr.2 = "Ethernet1"
interfaces.ifTable.ifEntry.ifDescr.3 = "FastEthernet0"
interfaces.ifTable.ifEntry.ifDescr.4 = "Fddi0"
```
2. Obtenga el OID asociado al campo CLI que se vigilará. Por este ejemplo, el OID para las “difusiones” es 1.3.6.1.2.1.2.2.1.12. Cisco OID para las variables MIB específicas está disponible del sitio web de cisco.com.
3. Determine los parámetros siguientes para poner los umbrales y los eventos.umbrales de levantamiento y que caenmuestreando el tipo (absoluto o delta)intervalo de muestreoacción cuando se alcanza el umbralCon el fin de este ejemplo, un umbral se está poniendo para vigilar el número de paquetes de broadcast recibidos en los Ethernetes 0. Un desvío será generado si el número de paquetes de broadcast recibidos es mayor de 500 entre las 60-

segundas muestras. El umbral será reactivado cuando el número de difusiones de la entrada no aumenta entre las muestras recogidas.**Nota:** Para detallado sobre estos parámetros de comando, controle la documentación en línea de la conexión de Cisco (CCO) para saber si hay alarma RMON y comandos event para su versión determinada del Cisco IOS.

4. Especifique el desvío enviado (evento RMON) cuando el umbral se alcanza usando los comandos CLI siguientes (visualizan a los comandos cisco ios en intrépido):**broadcast de alta calidad de la descripción del gateway de trampa del evento 1 del rmon “en el owner cisco de los Ethernetes el 0"la difusión normal de la descripción del registro del evento 2 del rmon “recibió en el owner cisco de los Ethernetes el 0"**
5. Especifique los umbrales y los parámetros pertinentes (alarma RMON) usando los comandos CLI siguientes:**subir-umbral 500 1 del delta ifEntry.12.1 60 de la alarma RMON 1owner cisco 2 del caer-umbral 0**
6. Utilice el SNMP para sondear estas tablas para verificar que las entradas de la tabla de eventos fueron hechas en el dispositivo.

```
rmon.event.eventTable.eventEntry.eventIndex.1 = 1

rmon.event.eventTable.eventEntry.eventIndex.2 = 2

rmon.event.eventTable.eventEntry.eventDescription.1 =
"High Broadcast on Ethernet 0"

rmon.event.eventTable.eventEntry.eventDescription.2 =
"normal broadcast received on ethernet 0"

rmon.event.eventTable.eventEntry.eventType.1 = snmp-trap(3)

rmon.event.eventTable.eventEntry.eventType.2 = log(2)

rmon.event.eventTable.eventEntry.eventCommunity.1 = "gateway"

rmon.event.eventTable.eventEntry.eventCommunity.2 = ""

rmon.event.eventTable.eventEntry.eventLastTimeSent.1 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventLastTimeSent.2 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventOwner.1 = "cisco"

rmon.event.eventTable.eventEntry.eventOwner.2 = "cisco"

rmon.event.eventTable.eventEntry.eventStatus.1 = valid(1)

rmon.event.eventTable.eventEntry.eventStatus.2 = valid(1)
```

7. Utilice el SNMP para sondear estas tablas para verificar que las entradas alarmtables fueron fijadas.

```
rmon.alarm.alarmTable.alarmEntry.alarmIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmInterval.1 = 60

rmon.alarm.alarmTable.alarmEntry.alarmVariable.1 = OID:
interfaces.ifTable.ifEntry.ifInNUcastPkts.2

rmon.alarm.alarmTable.alarmEntry.alarmSampleType.1 = absoluteValue(1)

rmon.alarm.alarmTable.alarmEntry.alarmValue.1 = 170183
```

```
rmon.alarm.alarmTable.alarmEntry.alarmStartupAlarm.1 =
risingOrFallingAlarm(3)

rmon.alarm.alarmTable.alarmEntry.alarmRisingThreshold.1 = 500

rmon.alarm.alarmTable.alarmEntry.alarmFallingThreshold.1 = 0

rmon.alarm.alarmTable.alarmEntry.alarmRisingEventIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmFallingEventIndex.1 = 2

rmon.alarm.alarmTable.alarmEntry.alarmOwner.1 = "cisco"

rmon.alarm.alarmTable.alarmEntry.alarmStatus.1 = valid(1)
```

Ejemplo de la operación SNMP SET

Para ejecutar la alarma RMON y el evento con la operación DETERMINADA SNMP, complete estos pasos:

1. Especifique el desvío enviado (evento RMON) cuando el umbral se alcanza usando las operaciones DETERMINADAS siguientes SNMP:
```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.1
  octetstring "High Broadcast on Ethernet 0"
  eventDescription.1 : DISPLAY STRING- (ascii): High Broadcast on Ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.1
  integer 3 eventType.1 : INTEGER: SNMP-trap

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.4.1 octetstring "gateway"
  eventCommunity.1 : OCTET STRING- (ASCII): gateway

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.1
  octetstring "cisco" eventOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.1 integer 1
  eventStatus.1 : INTEGER: valid
```
2. Especifique los umbrales y los parámetros pertinentes (alarma RMON) usando las operaciones DETERMINADAS siguientes SNMP:
```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.2
  octetstring "normal broadcast received on ethernet 0"
  eventDescription.2 : DISPLAY STRING- (ASCII): normal broadcast
  received on ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.2 integer 2
  eventType.2 : INTEGER: log

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.2 octetstring "cisco"
  eventOwner.2 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.2 integer 1
  eventStatus.2 : INTEGER: valid
```
3. Sondee estas tablas para verificar que las entradas de la tabla de eventos fueron hechas en el dispositivo.
```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.9.1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.2.1 integer 60
  alarmInterval.1 : INTEGER: 60

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.3.1
```

```
 objectidentifier .1.3.6.1.2.1.2.2.1.12.2
  alarmVariable.1 : OBJECT IDENTIFIER:
.iso.org.dod.internet.mgmt.mib2.interfaces.ifTable
  ifEntry.ifInNUcastPkts.2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.4.1 integer 2

alarmSampleType.1 : INTEGER: deltaValue

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.7.1 integer 500
  alarmRisingThreshold.1 : INTEGER: 500

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.8.1 integer 0
  alarmFallingThreshold.1 : INTEGER: 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.9.1 integer 1
  alarmRisingEventIndex.1 : INTEGER: 1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.10.1 integer 2
  alarmFallingEventIndex.1 : INTEGER: 2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.11.1 octetstring
"cisco"
  alarmOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.12.1 integer 1
  alarmStatus.1 : INTEGER: valid
```

4. Sondee estas tablas para verificar que las entradas alarmtables fueron fijadas.

```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1
```

show interface

Este ejemplo es un resultado del **comando show interface**.

interfaces Ethernet *0 de la* demostración del gateway**>**

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0000.0c38.1669 (bia 0000.0c38.1669)
Description: NMS workstation LAN
Internet address is 172.16.97.132/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 27 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
21337627 packets input, 3263376846 bytes, 0 no buffer

Received 7731303 broadcasts , 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
17328035 packets output, 2824522759 bytes, 0 underruns
174 output errors, 44368 collisions, 4 interface resets
0 babbles, 0 late collision, 104772 deferred
174 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Administración de la configuración

El objetivo de la administración de configuración es vigilar la red y la Información de la configuración del sistema para poder ser seguido y manejar los efectos sobre la operación de la red de las diversas versiones de los elementos del hardware y software.

Estándares de la configuración

Con un número creciente de dispositivos de red desplegados, es crítico poder identificar exactamente la ubicación de un dispositivo de red. Esta información sobre la ubicación debe proveer de una descripción detallada significativa a ésas encargadas el envío de los recursos cuando ocurre un problema de red. Para apresurar una resolución si ocurre un problema de red, asegúrese tener información de contacto disponible de la persona o del departamento responsable de los dispositivos. La información de contacto debe incluir el número de teléfono y el nombre de la persona o del departamento.

Las convenciones para nombres para los dispositivos de red, a partir del Nombre del dispositivo a la interfaz individual, deben ser planeadas y ser ejecutadas como parte del estándar de la configuración. Una convención para nombres bien definida provee de los personales la capacidad de proporcionar a la información precisa al resolver problemas los problemas de red. La convención para nombres para los dispositivos puede utilizar la ubicación geográfica, nombre constructivo, suelo, y así sucesivamente. Para la convención para nombres del interfaz, puede incluir el segmento con el cual un puerto está conectado, nombre del concentrador de conexión, y así sucesivamente. En las interfaces en serie, debe incluir el ancho de banda real, número del Identificador de conexión del link de datos local (DLCI) (si Frame Relay), destino, y la identificación del circuito o la información proporcionada por el portador.

Administración de archivos de configuración

Cuando usted agrega los nuevos comandos configuration en las necesidades existentes de los dispositivos de red, usted debe verificar los comandos para la integridad antes de que ocurra la implementación actual. Incorrectamente un dispositivo de la red configurada puede tener un efecto desastroso sobre la conectividad de red y el funcionamiento. Los parámetros de comando Configuration se deben controlar para evitar las discordancías o los problemas de incompatibilidad. Es recomendable programar un estudio completo de las configuraciones con los ingenieros de Cisco en una base normal.

A completamente - el esencial funcional CiscoWorks2000 permite los archivos de configuración de respaldo en el Routers y el Switches del Cisco Catalyst automáticamente. La función de seguridad del esencial se puede utilizar para realizar la autenticación en los cambios de configuración. Un registro de la auditoría de cambio está disponible seguir los cambios y el Nombre de usuario de los individuos que publican los cambios. Para los cambios de configuración en los dispositivos múltiples, dos opciones están disponibles: el NetConfig basada en la Web en la versión actual del esencial CiscoWorks2000 o del script del **cwconfig**. Los archivos de configuración se pueden descargar y cargar por teletratamiento usando el esencial CiscoWorks2000 que utiliza haber predefinido o las plantillas definidas por el usuario.

Estas funciones se pueden lograr con las herramientas de administración de la configuración en el esencial CiscoWorks2000:

- Empuje los archivos de configuración del archivo de configuración del esencial a un

dispositivo o a los dispositivos múltiples
- Tire de la configuración del dispositivo al archivo del esencial
- Extraiga configuración más posterior del archivo y escríbala a un fichero
- Importe la configuración de un fichero y empuje la configuración a los dispositivos
- Compare las dos configuraciones pasadas en el archivo del esencial
- Suprima las configuraciones más viejas que una fecha especificada o una versión del archivo
- Copie la configuración de inicio a la configuración corriente

Inventory Management

La función del descubrimiento de la mayoría de las plataformas de administración de redes se piensa para proporcionar a una lista dinámica de dispositivos encontrados en la red. Los motores de detección tales como ésos ejecutados en las plataformas de administración de redes deben ser utilizados.

Una base de datos del inventario proporciona a la información de la configuración detallada en los dispositivos de red. La información común incluye los modelos de la dotación física, los módulos instalados, las imágenes del software, los niveles del microcódigo, y así sucesivamente. Todas estas informaciones son cruciales en completar las tareas tales como mantenimiento de software y de hardware. El anuncio actualizado de los dispositivos de red recogidos por el proceso de descubrimiento se puede utilizar como lista maestra para recoger la información del inventario usando el SNMP o scripting. Una lista de dispositivos se puede importar del encargado del campus CiscoWorks2000 en la base de datos del inventario del esencial CiscoWorks2000 para obtener un Inventario actualizable de Switches del Cisco Catalyst.

Administración de software

Una actualización satisfactoria de las imágenes del Cisco IOS en los dispositivos de red requiere una análisis detallado de los requisitos tales como memoria, ROM del cargador del programa inicial, nivel del microcódigo, y así sucesivamente. Los requisitos están documentados normalmente y disponibles en el sitio web de Cisco bajo la forma de Release Note y guías de instalación. El proceso de actualizar el Cisco IOS corriente de un dispositivo de red incluye descargar una imagen correcta de CCO, sosteniendo la imagen actual, asegurarse de todos los requisitos de hardware se resuelven, y después cargar la nueva imagen en el dispositivo.

La ventana de la mejora para completar el mantenimiento del dispositivo es bastante limitada para algunas organizaciones. En un entorno de red grande con los recursos limitados, puede ser que sea necesario programar y automatizar las actualizaciones de software después de las horas de oficina. El procedimiento se puede completar con el lenguaje de la secuenciación de comandos por ejemplo espera o una aplicación escrita específicamente para realizar tal tarea.

Los cambios al software en los dispositivos de red tales como imágenes y versiones de microcódigo del Cisco IOS se deben seguir para ayudar a la fase de análisis en que se requiere otro mantenimiento de programas. Con un historial de modificaciones fácilmente disponible, la persona que realiza la mejora puede minimizar el riesgo de cargar las imágenes o el microcódigo incompatibles en los dispositivos de red.

Administración de rendimiento

Contrato de nivel de servicio

Un Acuerdo de nivel de servicio (SLA) es un acuerdo escrito entre un proveedor de servicio y sus clientes en el nivel de rendimiento esperado de servicios de red. SLA consiste en la métrica convenida en entre el proveedor y sus clientes. Los valores fijados para la métrica deben ser realistas, significativos, y mensurables para ambas partes.

Las diversas estadísticas del interfaz se pueden recoger de los dispositivos de red para medir el nivel de rendimiento. Estas estadísticas se pueden incluir como métrica en SLA. Las estadísticas tales como caídas de entradas en la cola, pérdidas de la cola de salida, y paquetes ignorados son útiles para diagnosticar los problemas relacionados con el rendimiento.

En el nivel del dispositivo, las mediciones de rendimiento pueden incluir la utilización CPU, la Asignación de memoria intermedia (almacenador intermediario, memoria intermedia mediana, faltas, proporción de aciertos grandes), y la asignación de memoria. El funcionamiento de ciertos protocolos de red se relaciona directamente con la disponibilidad del búfer en los dispositivos de red. Las estadísticas de medición del funcionamiento del dispositivo-nivel son críticas en la optimización del funcionamiento de los protocolos de mayor nivel.

Los dispositivos de red tales como Routers utilizan los diversos protocolos de capa más altas tales como grupo de trabajo de la transferencia del link de datos (DLSW), ruta del origen remoto que puentea (RSRB), APPLETALK, y así sucesivamente. Las estadísticas del funcionamiento de las Tecnologías de Red de área ancha (WAN) incluyendo el Frame Relay, la atmósfera, el Integrated Services Digital Network (ISDN), y otros pueden ser vigiladas y ser recogidas.

Supervisión del rendimiento, medición e informes

Diversas mediciones de rendimiento en el interfaz, el dispositivo, y los niveles del protocolo se deben recoger en una base normal usando el SNMP. El motor del sondeo en un sistema de administración de red se puede utilizar para los propósitos de la recopilación de datos. La mayoría de los sistemas de administración de red son capaces de recoger, de salvar, y de presentar los datos interrogados.

Las diversas soluciones están disponibles en el mercado dirigir las necesidades de la Administración del rendimiento de los entornos de la empresa. Estos sistemas son capaces de recoger, de salvar, y de presentar los datos de los dispositivos de red y de los servidores. El interfaz basada en la Web en la mayoría de los Productos hace los Datos del rendimiento accesibles dondequiera adentro de la empresa. Algunas de las soluciones de administración de rendimiento comúnmente implementadas son:

- InfoVista VistaView
- Servicio Vision SAS las TIC
- TENDENCIA Trinagy

Una evaluación de los Productos antedichos determinará si cumplen los requisitos de diversos usuarios. Algunos vendedores admiten la integración con las Plataformas de la Administración de redes y de la administración del sistema. Por ejemplo, InfoVista utiliza el agente de la patrulla BMC para proporcionar a las estadísticas del rendimiento clave de los servidores de aplicaciones. Cada producto tiene un diverso modelo de precio y capacidades con el ofrecimiento bajo. La ayuda para las características de la Administración del rendimiento para los dispositivos de Cisco tales como Netflow, RMON, y Service Assurance Agent del Cisco IOS/reportero del tiempo de respuesta (RTR/SAA CSAA/RTR) está disponible en algunas soluciones. La concordia tiene recientemente apoyo añadido para el Switches PÁLIDO de Cisco que se puede utilizar para recoger y para ver los Datos del rendimiento.

La característica de la informante de la hora del Service Assurance Agent (SAA) /Response CSAA/RTR (RTR) en el Cisco IOS se puede utilizar para medir el tiempo de respuesta entre los dispositivos IP. Un router de la fuente configurado con CSAA configurado es capaz de medir el tiempo de respuesta a un dispositivo IP del destino que pueda ser un router o un dispositivo IP. El tiempo de respuesta se puede medir entre la fuente y el destino o para cada salto a lo largo de la trayectoria. El SNMP traps se puede configurar para alertar las consolas de administración si el tiempo de respuesta excede los umbrales predefinidos.

Las mejoras recientes al Cisco IOS amplían las capacidades de CSAA para medir el siguiente:

- Rendimiento del servicio de Protocolo de transporte de hipertexto (HTTP)Búsqueda del Sistema de nombres de dominio (DNS)Conexión del Protocolo de control de transmisión (tcp)Tiempo de transacción HTTP
- Variante del retraso entre paquetes (oscilación) de voz sobre el tráfico IP (VoIP)
- Tiempo de respuesta entre las puntas del extremo para un Calidad de Servicio (QoS) específicoBits del Tipo de servicio (ToS) IP
- Pérdida del paquete usando los paquetes generados mediantes CSAA

Configurar la característica CSAA en el Routers puede ser realizado usando la aplicación Internetwork Performance Monitor (IPM) de Cisco. El CSAA/RTR se integra en muchos pero no todos los conjuntos de la característica del software del Cisco IOS. Una versión de la versión de software del Cisco IOS que utiliza el CSAA/RTR se debe instalar en el dispositivo que el IPM utiliza para recoger las estadísticas del funcionamiento. Para un resumen de las versiones del Cisco IOS que utilizan el CSAA/RTR/IPM, refiera al sitio web con frecuencia pedido de las preguntas IPM.

La información adicional con respecto al IPM incluye:

- Descripción del IPM
- Agente de garantía del servicio

Análisis y ajuste del rendimiento

El tráfico de usuarios ha aumentado perceptiblemente y ha colocado un más de mucha demanda en los recursos de red. Los administradores de la red tienen típicamente una opinión limitada sobre los tipos de tráfico que se ejecutan en la red. El User and application traffic profiling proporciona a una vista detallada del tráfico en la red. Dos Tecnologías, las puntas de prueba RMON y el Netflow, proporcionan a la capacidad de recoger los perfiles del tráfico.

RMON

Los estándares de RMON se diseñan para ser desplegados en una arquitectura distribuida donde los agentes (o integrado o en los sondeos autónomos) comunican con una estación central (la consola de administración) vía el SNMP. El estándar de RMON del RFC 1757 ordena las funciones de supervisión en nueve grupos para utilizar las topologías de Ethernet, y agrega a un décimo grupo en el RFC 1513 para los parámetros Anillo-únicos simbólicos. La supervisión rápida del link de los Ethernetes se proporciona en el marco del estándar del RFC 1757, y la supervisión del anillo de Fiber Distributed Data Interface (FDDI) se proporciona en el marco del RFC 1757 y del RFC 1513.

La especificación de RMON emergente del RFC 2021 conduce la supervisión remota estándares mas allá el capa de control de acceso de medios (MAC) a la red y a las capas de la aplicación.

Esta disposición permite a los administradores analizar y resolver problemas las aplicaciones conectadas en red tales como tráfico de la Web, NetWare, notas, email, acceso a bases de datos, Network File System (NFS), y otros. Las alarmas RMON, las estadísticas, el historial, y el host/los grupos de conversación se pueden ahora utilizar dinámico vigilan y mantienen la disponibilidad de la red basada en el tráfico- de la capa de la aplicación la mayoría del tráfico crítico en la red. El RMON2 permite a los administradores de la red continuar su despliegue de las soluciones que vigilan estándar-basadas para utilizar misión-crítico, las aplicaciones basadas en servidor.

Las tablas siguientes enumeran las funciones de los grupos RMON.

Grupo RMON (RFC 1757)	Función
Estadísticas	Contadores para los paquetes, los octetos, las difusiones, los errores, y las ofertas en el segmento o el puerto.
Historial	Muestrea y guarda periódicamente a los contadores del grupo de estadísticas para la extracción posterior.
Host	Mantiene las estadísticas sobre cada dispositivo host en el segmento o el puerto.
Host N superior	Un informe de subconjunto definido por el usuario de los host agrupa, clasificado por un contador estadístico. Volviendo solamente los resultados, se minimiza el tráfico de administración.
Matriz del tráfico	Mantiene las estadísticas de conversación entre los host en la red.
Alarmas	Un umbral que se puede fijar en las variables críticas RMON para la administración proactiva.
Eventos	Genera el SNMP traps y las entradas de registro cuando se excede un Umbral de grupo de alarmas.
Captura de paquetes	Maneja los almacenadores intermediarios para los paquetes capturados por el Grupo de filtro para cargar por teletratamiento a la consola de administración.
Token Ring	Ring Station — estadísticas detalladas en la orden individual de las estaciones Ring Station — una lista ordenada de estación actualmente en la configuración del anillo Ring Station — configuración e inserción/retiro por la encaminamiento de la fuente de la estación — estadísticas sobre la encaminamiento de la fuente, tal como conteos saltos, y otras

RMON2	Función

Directorio de protocolos	Protocolos para los cuales el agente vigila y mantiene las estadísticas.
Distribución del protocolo	Estadísticas para cada protocolo.
Host de capa de red	Estadísticas para cada dirección de capa de red en el segmento, el anillo, o el puerto.
Matriz de capa de red	Estadísticas del tráfico para los pares de direcciones de capa de red.
Host de la capa de la aplicación	Estadísticas por el protocolo de la capa de la aplicación para cada dirección de red.
Matriz de capa de la aplicación	Trafique las estadísticas por el protocolo de la capa de la aplicación para los pares de direcciones de capa de red.
Historial definido por el usuario	Amplía el historial más allá estadísticas de la capa del link RMON1 para incluir cualquier estadística RMON, RMON2, MIB-I, o MIB-II.
Reproducción de direcciones	Vinculaciones de direcciones MAC a capa de red.
Grupo de configuración	Capacidades del agente y configuraciones.

Netflow

NetFlow de Cisco la característica permite que las estadísticas detalladas de los flujos de tráfico sean recogidas para la planificación de capacidad, la factura, y las funciones de Troubleshooting. El Netflow se puede configurar en las interfaces individuales, proporcionando a la información en el tráfico que pasa a través de esos interfaces. Los siguientes tipos de información son parte de las estadísticas detalladas del tráfico:

- Direcciones IP de origen y de destino
- Números de las interfaces de entrada y salida
- Puertos del puerto de origen y de destino TCP/UDP
- Número de bytes y paquete en el flujo
- Números del sistema autónomo de origen y destino
- Tipo de servicio (ToS) IP

Los datos de NetFlow recopilados en los dispositivos de red se exportan a una máquina del colector. El colector realiza las funciones tales como reducción del volumen de datos (filtración y

agregación), del almacenamiento de datos jerárquico, y de la Administración de sistema de archivos. Cisco proporciona al colector NetFlow y a las aplicaciones de NetFlow Analyzer para recopilar y analizar los datos del Routers y del Switches del Cisco Catalyst. Hay también herramientas del shareware tales como cflowd que pueda recoger NetFlow de Cisco los expedientes del User Datagram Protocol (UDP).

Los datos de NetFlow se transportan usando los paquetes UDP en tres diversos formatos:

- Versión 1 — El formato original utilizado en las versiones de NetFlow inicial.
- Versión 5 — Una mejora posterior que agregó los números de serie de la información del sistema autónomo del Protocolo de gateway marginal (BGP) y del flujo.
- Versión 7 — Una mejora todavía posterior que agregó la ayuda del Switching de Netflow para los Cisco Catalyst 5000 Series Switch equipó de una placa de función del Netflow (NFFC).

Las versiones 2 a 4 y versión 6 no release/versión ni son utilizadas por FlowCollector. En las tres versiones, el datagrama consiste en una encabezado y uno o más expedientes del flujo.

Para más información, refiera al Libro Blanco de la guía de las soluciones de los servicios de NetFlow.

La tabla siguiente resume las versiones utilizadas del Cisco IOS para recopilar los datos de NetFlow del Routers y del Switches del catalizador.

Versión de software del IOS de Cisco	Plataforma del hardware de Cisco utilizada	Versiones exportadas Netflow utilizadas
11.1 CA y 11.1 CC	7200, 7500 y RSP7000 de Cisco	V1 y V5
11.2 y 11.2 P	7200, 7500 y RSP7000 de Cisco	V1
11.2 P	Módulo del switch de la ruta de Cisco (RSM)	V1
11.3 y 11.3 T	7200, 7500 y RSP7000 de Cisco	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, y RSM	V1 y V5
12.0T	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM, y BPX 8600	V1 y V5
12.0(3)T y más adelante	Cisco 1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800,	V1, V5 y V8

	7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM, y BPX 8650	
12.0(6)S	Cisco 12000	V1, V5 y V8
	Cisco Catalyst 5000 con la placa de función del Netflow *** (NFFC)	V7

* La ayuda para la exportación de NetFlow V1, V5, y V8 en las Plataformas de Cisco 1600 y 2500 se apunta para el Cisco IOS Software Release 12.0(T). La ayuda del Netflow para estas Plataformas no está disponible en la versión de la línea principal del Cisco IOS 12.0.

** La ayuda para el Netflow V1, V5, y V8 en la plataforma AS5300 se apunta para el Cisco IOS Software Release 12.06(T).

El *** MLS y la exportación de datos de NetFlow se utiliza en la versión de software Supervisor Engine de las Catalyst 5000 Series 4.1(1) o más adelante.

Administración de seguridad:

El objetivo de la administración de seguridad es controlar el acceso a los recursos de red según las directivas locales para no poder sabotear la red (intencionalmente o involuntariamente). Un subsistema de administración de seguridad, por ejemplo, puede vigilar a los usuarios que abren una sesión a un recurso de red, rechazando el acceso a los que ingresen los códigos del acceso inapropiado. La Administración de seguridad es un tema muy amplio; por lo tanto esta área del documento cubre solamente la Seguridad con respecto al SNMP y a la Seguridad básica del acceso del dispositivo.

La información detallada sobre la Seguridad avanzada incluye:

- Seguridad creciente en las redes IP
- OpenSystems

Comienzo buen de una instrumentación de la administración de seguridad con las políticas de seguridad de sonido y los procedimientos en el lugar. Es importante crear un estándar de configuración mínima específica de la plataforma para todo el Routers y Switches que sigan las mejores prácticas de la industria para la Seguridad y el funcionamiento.

Hay diversos métodos de controlar el acceso en el Routers de Cisco y el Switches del catalizador. Algunos de estos métodos incluyen:

- Listas de control de acceso (ACL)
- Identificaciones del usuario y contraseñas locales al dispositivo
- Sistema de control de acceso del Terminal Access Controller (TACACS)

TACACS es un protocolo de seguridad estándar del Internet Engineering Task Force (RFC 1492) que se ejecuta entre los dispositivos cliente en una red y contra un servidor TACACS. TACACS es un mecanismo de autenticación que se utiliza para autenticar la identidad de un Acceso Remoto que busca del dispositivo a una base de datos privilegiada. Las variaciones de TACACS incluyen TACACS+, la arquitectura AAA que separa la autenticación, la autorización, y las

funciones de contabilidad.

TACACS+ es utilizado por Cisco para permitir un control más fino sobre quién puede tener acceso al dispositivo de Cisco en sin privilegios y el modo privilegiado. Los servidores múltiples TACACS+ se pueden configurar para la tolerancia de incidente. Con TACACS+ activado, el router y el conmutador incita al usuario para un Nombre de usuario y una contraseña. La autenticación puede ser configurada para el control de inicio de sesión o autenticar los comandos individuales.

Autenticación

La autenticación es el proceso de identificar a los usuarios, incluyendo el diálogo de la clave y de la contraseña, el desafío y la respuesta, y la ayuda de la Mensajería. La autenticación es la manera que identifican a un usuario antes de no ser prohibida el acceso al router o al conmutador. Hay una relación fundamental entre la autenticación y la autorización. Cuanto más privilegios de autorización que un usuario recibe, más fuerte la autenticación debe ser.

Autorización

La autorización proporciona al control de acceso remoto, incluyendo la autorización única y la autorización para cada servicio que sea pedido por el usuario. En un router de Cisco, el alcance del nivel de autorización para usuarios es 0 a 15 con 0 que es el más bajo y 15 el más alto.

Contabilidad

Las estadísticas permiten la recogida y el envío de la información sobre seguridad usado para cargar en cuenta, auditoría, y señalar, tal como Identificaciones del usuario, las horas de inicio y de detención, y los comandos ejecutados. El considerar permite a los administradores de la red seguir los servicios a que los usuarios están teniendo acceso así como al periodo de los recursos de red que están consumiendo.

La tabla siguiente enumera los ejemplos de comando básicos para usar TACACS+, la autenticación, la autorización, y considerar en un router de Cisco y un conmutador del catalizador. Refiera al documento de la autenticación, de la autorización, y de los comandos de contabilidad para comandos más profundizados.

Comando del IOS de Cisco	Propósito
Router	
aaa de modelo nuevo	Active la autenticación, autorización, considerando (AAA) como el método principal el control de acceso.
Estadísticas AAA {*sistema* | *red* | *conexión* | *ejecutivo* | *nivel del comando*} {*por marcha-parada* | *espera-principio* | *parada-solamente*} {*tacacs+* | *radio*}	Estadísticas del permiso con los comandos global configuration.

Valor predeterminado inicio de sesión tacacs+ de la autenticación AAA	Ponga al router de modo que las conexiones a cualquier línea de la terminal configurado con el valor predeterminado inicio de sesión sean autenticadas con TACACS+, y fallará si la autenticación falla por cualquier motivo.
TACACS+ predeterminado del exec de autorización AAA ningunos	Ponga al router para controlar si se permite al usuario funcionar con un EXEC shell pidiendo el servidor TACACS+.
IP address del servidor del ***host*** *tacacs+ del tacacs-****servidor***	Especificar el servidor TACACS+ que será utilizado para autenticación con los comandos de configuración global.
secreto compartido ***dominante del tacacs-servidor***	Especifique el secreto compartido que es sabido por los servidores TACACS+ y el router de Cisco con el comando global configuration.
Catalyst Switch	
fije el permiso del inicio de sesión en TACACS de la autenticación [*todo* **|** ***consola*	*HTTP* |** **[primary]** ***telnet*****]**	Permiso autenticación de TACACS+ para el modo de inicio de sesión normal. Utilice las palabras claves de consola o de Telnet para activar TACACS+ solamente para el puerto de la consola o los intentos de conexión de Telnet.
fije la ***opción*****} del** ***retraso del*** **permiso del exec de autorización {***opción}* **[***consola	telnet	ambos***]**	Modo de inicio de sesión de la autorización para normal del permiso. Utilice las palabras claves de consola o de Telnet para activar la autorización solamente para el puerto de la consola o los intentos de conexión de Telnet.
Fije el ***secreto compartido*** **dominante del tacacs-servidor**	Especifique el secreto compartido que es sabido por los servidores y el conmutador TACACS+.
Fije el ***IP address del servidor del*** **host** ***tacacs+ del tacacs-*** **servidor**	Especificar el servidor TACACS+ que será utilizado para autenticación con los comandos de configuración global.
Permiso de los comandos set accounting {*config	todos***} {***tacacs de la parada-solamente***} +**	Estadísticas del permiso de los comandos configuration.

Para más información sobre cómo configurar el AAA para vigilar y para controlar el acceso a la interfaz de línea de comandos en el Switches LAN de la empresa del catalizador, refiera al acceso que controla al conmutador usando el documento de la autenticación, de la autorización, y de estadísticas.

Seguridad SNMP

El protocolo SNMP se puede utilizar para realizar los cambios de configuración en el Routers y el Switches del catalizador similares a ésos publicados del CLI. Las medidas de seguridad apropiada se deben configurar en los dispositivos de red para prevenir el acceso no autorizado y para cambiar vía el SNMP. Las cadenas de comunidad deben seguir las pautas estándar para contraseñas para la longitud, los caracteres, y la dificultad de conjeturar. Es importante cambiar las cadenas de comunidad de sus valores públicos y privados predeterminados.

Todos los host de la administración de SNMP se deben tener una dirección IP estática y conceder explícitamente las derechas de la comunicación SNMP con el dispositivo de red por ésa predefinido por la dirección IP y la lista de control de acceso (ACL). El software del Cisco IOS y del Cisco Catalyst proporciona a las funciones de seguridad que se aseguran de que solamente las estaciones de administración autorizada estén permitidas realizar los cambios en los dispositivos de red.

Funciones de Router Security

Nivel de privilegio SNMP

Esta característica limita los tipos de operaciones que una estación de administración pueda tener en un router. Hay dos tipos de nivel de privilegio en el Routers: Inalterable (RO) y Leer-escribir (RW). El nivel RO permite solamente que una estación de administración pregunte los datos del router. No permite los comandos configuration tales como reiniciar a un router y cierre de los interfaces que se realizarán. Solamente el nivel de privilegio RW se puede utilizar para realizar tales operaciones.

Lista de control de acceso (ACL) SNMP

La característica SNMP ACL se puede utilizar conjuntamente con la función de privilegio SNMP para limitar las estaciones de administración específicas de pedir la información para administración del Routers.

Opinión SNMP

Esta característica limita la información específica que se puede extraer del Routers por las estaciones de administración. Puede ser utilizada con el nivel de privilegio SNMP y las características ACL para aplicar el acceso de datos restringido por las consolas de administración. Para las muestras de la configuración de opinión SNMP, vaya a la opinión del SNMP-servidor.

Versión 3 de SNMP

El SNMP versión 3 (SNMPv3) proporciona a los intercambios seguros de los datos de administración entre los dispositivos de red y las estaciones de administración. Las características del cifrado y de la autenticación en SNMPv3 aseguran la gran seguridad en el transporte de los paquetes a una consola de administración. SNMPv3 se utiliza en el Cisco IOS Software Release

12.0(3)T y Posterior. Para una descripción técnica general de SNMPv3, vaya a la documentación SNMPv3.

Lista de control de acceso (ACL) en los interfaces

La característica ACL proporciona medidas de seguridad ya que previene ataques como la simulación del IP. La ACL puede aplicarse en interfaces entrantes o salientes en routers.

LAN de Catalyst cambie la función de seguridad

El IP permite la lista

La característica de la lista del permiso IP restringe la Telnet entrante y el acceso SNMP al conmutador de los IP Addresses de la fuente no autorizada. Se admiten mensajes de Syslog y notificaciones de trampa SNMP para notificar a un sistema de administración cuando ocurre una violación o acceso no autorizado.

Una combinación de las características de Seguridad de Cisco IOS se puede utilizar para manejar el Routers y el Switches del catalizador. Una política de seguridad necesita ser establecida que limita el número de estaciones de administración capaces de tener acceso el Switches y al Routers.

Para más información sobre cómo aumentar la Seguridad en las redes IP, vaya a la seguridad creciente en las redes IP.

Administración de contabilidad

La administración de contabilidad es el proceso usado para medir los parámetros de utilización de la red para poder regular los usuarios individuales o del grupo en la red apropiadamente con el propósito de considerar o del chargeback. Similar a la Administración del rendimiento, el primer paso hacia la administración de contabilidad apropiada es medir la utilización de los recursos de red importantísimos. La utilización de los recursos de red se puede medir usando las características de contabilidad IP NetFlow de Cisco y de Cisco. El análisis de los datos recopilados con estos métodos proporciona a la penetración en los modelos del uso actual.

Un sistema de contabilidad y facturación basado en el uso es una parte esencial de cualquier Acuerdo de nivel de servicio (SLA). Proporciona a una manera práctica de definir las obligaciones bajo SLA y las consecuencias claras para el comportamiento fuera de los términos de SLA.

Los datos se pueden recoger vía las puntas de prueba o NetFlow de Cisco. Cisco proporciona al colector NetFlow y a las aplicaciones de NetFlow Analyzer para recopilar y analizar los datos del Routers y del Switches del catalizador. Las aplicaciones de shareware tales como cflowd también se utilizan para recopilar los datos de NetFlow. Un uso de las mediciones de recurso en curso puede rendir la información de factura, así como la información evalúa la feria y a los recursos óptimos continuos. Algunas de las soluciones de administración de contabilidad comúnmente implementadas son:

- Software evidente

Activación de Netflow y estrategia de obtención de datos

NetFlow (flujo de red) es una tecnología de medición de lado de entrada que permite capturar los datos requeridos para aplicaciones de planificación, supervisión y contabilidad de redes. El Netflow se debe desplegar en los interfaces del borde/del router de la agregación para los proveedores de servicio o los interfaces del router de acceso a WAN para los clientes de la empresa.

Cisco Systems recomienda cuidadosamente un despliegue de NetFlow planificado con los servicios de NetFlow activado en éstos Routers estratégico localizado. El Netflow se puede desplegar ampliado (interfaz por el interfaz) y estratégico (en el Routers bien elegido), bastante que el Netflow que despliega en cada router en la red. El personal de Cisco trabajará con los clientes para determinar en qué Routers y Netflow dominantes de los interfaces de la clave se debe activar sobre la base de los patrones del flujo de tráfico, de la topología de red, y de la arquitectura del cliente.

Las consideraciones de despliegue fundamental incluyen:

- Los servicios de NetFlow deben ser utilizados como herramienta de la aceleración del funcionamiento del medidor de borde y de la lista de acceso y no deben ser activados en el Routers *caliente de la* base/de la estructura básica o el Routers que se ejecuta muy CPU elevada a las velocidades de utilización.
- Entienda los requisitos para la obtención de datos aplicación-conducidos. Las aplicaciones de contabilidad pueden requerir solamente originar y terminar la información de flujo del router mientras que vigilan las aplicaciones pueden requerir (intensiva de datos) una visión de punta a punta más completa.
- Entienda el impacto de la topología de red y de la directiva de la encaminamiento en la estrategia de la colección del flujo. Por ejemplo, evite recoger los flujos duplicados por el Netflow que activa en los routeres de agrupamiento clave donde el tráfico origina o termina y no en el Routers o los routeres intermedios de la estructura básica que proporcionarían a las vistas duplicadas de la misma información de flujo.
- Los proveedores de servicio en el negocio de *portadora de tránsito* (tráfico de transporte ni que origina ni que termina en su red) pueden utilizar los datos de exportación de NetFlow para los usos de recursos de la red de tráfico en tránsito de medición para los propósitos de contabilidad y facturación.

Configure las estadísticas IP

La ayuda de las estadísticas IP de Cisco proporciona a las funciones de contabilidad básicas IP. Activando las estadísticas IP, los usuarios pueden ver el número de bytes y paquete cambiado a través del software del Cisco IOS sobre una base de la fuente y de la dirección IP del destino. Solamente el tráfico IP de tránsito se mide y solamente en una considerando el saliente. El tráfico generado el software o terminando en el software no se incluye en las estadísticas de contabilidad. Para mantener los totales de la contabilidad precisa, el software mantiene dos bases de datos de contabilidad: un active y una base de datos control-acentuada.

La ayuda de las estadísticas IP de Cisco también proporciona a la información que identifica el tráfico IP que falla las Listas de acceso IP. La identificación de los direccionamientos de IP de origen que violan las Listas de acceso IP señala las tentativas posibles de violar la seguridad. Los datos también indican que las configuraciones de la lista de acceso IP deben ser verificadas. Para poner esta característica a disposición los usuarios, estadísticas IP del permiso de las violaciones de lista de acceso usando el **comando ip accounting access-violations**. Los usuarios pueden entonces visualizar el número de bytes y paquete de una fuente única que intentó violar la

seguridad contra la lista de acceso para el par de destino fuente. Por abandono, las estadísticas IP visualizan el número de paquetes que han pasado las Listas de acceso y fueron encaminadas.

Para activar las estadísticas IP, utilice uno de los comandos siguientes para cada interfaz en el modo de configuración de la interfaz:

Comando	Propósito
estadísticas IP	Estadísticas básicas IP del permiso.
violaciones de acceso de las estadísticas IP	Estadísticas IP del permiso con la capacidad de identificar el tráfico IP que falla las Listas de acceso IP.

Para configurar otras funciones de contabilidad IP, utilice uno o más de los comandos siguientes en el modo de configuración global:

Comando	Propósito
*umbral del estadística-**umbral IP***	Fije la cantidad máxima de entrada de contabilidad que se creará.
*comodín del IP address de la estadística-**lista IP***	Información de la cuenta del filtro para los host.
*cuenta de los estadística-**tránsitos IP***	Controle el número de expedientes del tránsito que sean salvados en la base de datos de contabilidad IP.

Consulte Convenciones de sugerencias técnicas de Cisco para obtener información sobre las convenciones utilizadas en este documento.