Sistema de gerenciamento de rede: White Paper de práticas recomendadas

Contents

Introduction

O modelo de gerenciamento de rede tipo International Organization for Standardization (ISO) define cinco áreas funcionais de gerenciamento de rede. Este documento abrange todas as áreas funcionais. O propósito geral deste documento é fornecer recomendações práticas sobre cada área funcional para aumentar a eficácia geral das ferramentas e das práticas de gerenciamento atuais. Ele também contém diretrizes de design para a futura implementação de tecnologias e ferramentas de gerenciamento de rede.

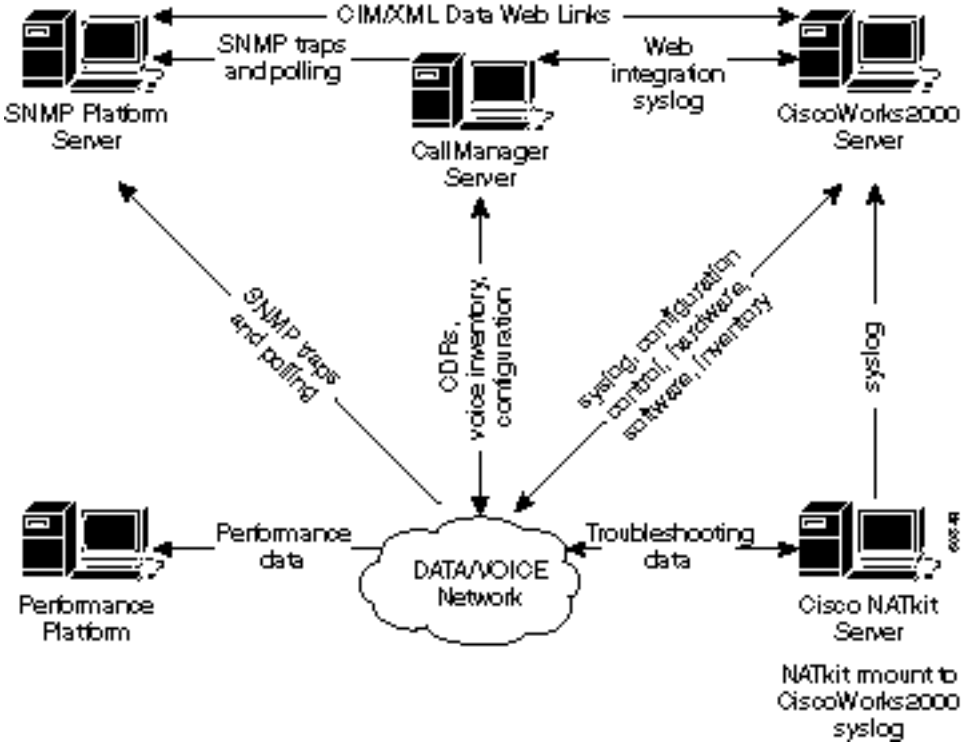
Gerenciamento de Rede

As cinco áreas funcionais do modelo de gerenciamento de rede ISO estão listadas abaixo.

- Gerenciamento de falhas — Detectar, isolar, notificar e corrigir falhas encontradas na rede.
- Gerenciamento de configuração — Aspectos de configuração dos dispositivos de rede, como

gerenciamento de arquivos de configuração, gerenciamento de inventário e gerenciamento de software.
- Gerenciamento de desempenho — Monitorar e medir vários aspectos do desempenho para que o desempenho geral possa ser mantido em um nível aceitável.
- Gestão de segurança — Fornecer acesso a dispositivos de rede e recursos corporativos para indivíduos autorizados.
- Gestão contábil — Informações de utilização dos recursos de rede.

O diagrama seguinte mostra uma arquitetura de referência que os Sistemas Cisco acreditam que deverá ser a solução mínima para gerenciamento de uma rede de dados. Esta arquitetura inclui um servidor Cisco CallManager para aqueles que planejam gerenciar VoIP (Voz sobre IP): O diagrama mostra como integrar o servidor CallManager na topologia do NMS.



A arquitetura de gerenciamento da rede inclui o seguinte:

- Plataforma do SNMP (Protocolo simples de gerenciamento de rede) para gerenciamento de falhas
- Plataforma de monitoramento de desempenho para gerenciamento de desempenho a longo prazo e tendências
- Servidor CiscoWorks2000 para gerenciamento de configurações, coleta de syslog e gerenciamento de inventário de hardware e software

Algumas plataformas SNMP podem compartilhar dados diretamente com o servidor CiscoWorks2000, usando métodos de CIM/XML (Common Information Model/eXtensible Markup Language). CIM é um modelo de dados comum de um esquema de implementação neutra para descrever informações gerais de gerenciamento em um ambiente empresarial/de rede. O CIM é composto de uma especificação e um esquema. A especificação define os detalhes da integração com outros modelos de gerenciamento, como SNMP MIBs ou DMTF MIFs (Desktop Management Task Force Management Information Files), enquanto o esquema fornece as descrições reais do modelo.

XML é uma linguagem de marcação, utilizada para representar dados estruturados em forma textual. Um objetivo específico do XML era manter a maior parte do poder descritivo do SGML,

retirando ao máximo sua complexidade. XML é semelhante em conceito ao HTML, mas enquanto o HTML é usado para conduzir informações gráficas sobre um documento, o XML é usado para representar dados estruturados em um documento.

Os clientes de serviços avançados da Cisco também incluiriam o servidor NATkit da Cisco para monitoramento proativo adicional e Troubleshooting. O servidor NATkit terá uma rmount (montagem de disco remota) ou um FTP (protocolo de transferência de arquivos) para acesso aos dados localizados no servidor CiscoWorks2000.

O capítulo Fundamentos de gerenciamento de rede da Visão geral sobre a tecnologia de comunicação inter-redes oferece uma visão geral mais detalhada sobre os fundamentos de gerenciamento de rede.

Gerenciamento de falhas

O objetivo do gerenciamento de falhas é detectar, registrar, notificar usuários e (na medida do possível) corrigir automaticamente os problemas de rede para manter a rede funcionando de forma eficaz. Como as falhas podem causar tempo inativo ou degradação de rede inaceitável, o gerenciamento de falhas talvez seja o elemento de gerenciamento de rede ISO mais largamente implementado.

Plataformas de gerenciamento de rede

Uma plataforma de gerenciamento de rede implantada na empresa gerencia uma infraestrutura que consiste em elementos de rede de vários fornecedores. A plataforma recebe e processa eventos de elementos de rede na rede. Eventos dos servidores e outros recursos críticos podem também ser encaminhados para uma plataforma de gerenciamento. As seguintes funções geralmente disponíveis estão incluídas em uma plataforma de gerenciamento padrão:

- Descoberta de rede
- Mapeamento de topologia dos elementos da rede
- Manipulador de eventos
- Coletor e executor de gráfico de dados de desempenho
- Navegador de dados de gerenciamento

Épossível considerar as plataformas de gerenciamento de rede como o console principal para as operações de rede de detecção de defeitos na infra-estrutura. A capacidade de detectar problemas rapidamente em qualquer rede é fundamental. A equipe de operações de rede pode contar com um mapa gráfico de rede para exibir os estados operacionais dos elementos importantes da rede, como roteadores e switches.

As plataformas de gerenciamento de rede, como HP OpenView, Computer Associates Unicenter e SUN Solstice, podem executar uma descoberta dos dispositivos da rede. Cada dispositivo de rede é representado por um elemento gráfico no console da plataforma de gerenciamento. Cores diferentes nos elementos gráficos representam o status operacional atual dos dispositivos de rede. Os dispositivos de rede podem ser configurados para enviar notificações, denominadas interceptações SNMP, para as plataformas de gerenciamento de rede. Após receber as notificações, o elemento gráfico representante do dispositivo de rede muda para uma cor diferente, dependendo da severidade da notificação recebida. A notificação, geralmente chamada de evento, é colocada em um arquivo de registro. É especialmente importante que os arquivos mais recentes da Base de Informações de Gerenciamento Cisco (MIB) sejam carregados na plataforma SNMP para garantir que os vários alertas dos dispositivos Cisco sejam interpretados

corretamente.

A Cisco publica arquivos de MIB para o gerenciamento de vários dispositivos da rede. Os arquivos MIB da Cisco estão localizados no site cisco.com e incluem as seguintes informações:

- Arquivos MIB publicados no formato SNMPv1
- Arquivos MIB publicados em formato SNMPv2
- Armadilhas de SNMP suportadas nos dispositivos da Cisco
- OIDs para objetos MIB SNMP atuais Cisco

Uma série de plataformas de gerenciamento de rede são capazes de gerenciar vários locais distribuídos geograficamente. Isto é obtido por meio da troca de dados de gerenciamento entre os consoles de gerenciamento em sites remotos e uma estação de gerenciamento no site principal. A principal vantagem de uma arquitetura distribuída é a redução do tráfego de gerenciamento, o que proporciona uma utilização mais eficaz da largura de banda. Uma arquitetura distribuída também permite que a equipe gerencie localmente suas redes a partir de locais remotos com sistemas.

Um aprimoramento recente das plataformas de gerenciamento inclui a capacidade de gerenciamento remoto dos elementos de rede, usando uma interface da Web. Essa melhoria elimina a necessidade de software de cliente especial em estações de usuário individual para acessar uma plataforma de gerenciamento.

Uma empresa típica é formada por diferentes elementos de rede. No entanto, cada dispositivo normalmente exige sistemas de gerenciamento de elemento específico do fornecedor para gerenciar efetivamente os elementos da rede. Por isso, as estações de gerenciamento duplicadas podem estar elegendo elementos de rede para as mesmas informações. Os dados coletados por diferentes sistemas são armazenados em bancos de dados separados, criando carga adicional de administração para os usuários. Essa limitação fez com que os fornecedores de redes de comunicação e de software adotassem padrões como o CORBA e o CIM para facilita o intercâmbio de dados de gerenciamento entre plataformas de gerenciamento e sistemas de gerenciamento de elementos. Com fornecedores adotando padrões em desenvolvimento de sistema de gerenciamento, os usuários poderão contar com interoperabilidade e economia na distribuição e gerenciamento da infra-estrutura.

O CORBA especifica um sistema que proporciona interoperabilidade entre objetos em um ambiente heterogêneo e distribuído e de uma forma transparente para o programador. O design é baseado no modelo de objeto do OMG (Object Management Group).

Troubleshooting de Infra-estrutura

Os servidores TFTP (Trivial File Transfer Protocol) e syslog (log de sistema) são componentes essenciais de uma infraestrutura de solução de problemas nas operações de rede. O servidor TFTP é usado principalmente para armazenar os arquivos de configuração e as imagens de software para os dispositivos de rede. Os roteadores e switches são capazes de enviar mensagens do registro de sistema para um servidor syslog. As mensagens facilitam a função de Troubleshooting quando são encontrados problemas. Ocasionalmente, a equipe de suporte da Cisco precisa das mensagens de syslog para realizar análises da causa do problema.

A função de coleta de syslog distribuída do CiscoWorks2000 Resource Management Essentials (Essentials) permite a implantação de diversas estações de coleta UNIX ou NT em localizações remotas para executar coleta e filtragem de mensagens. Os filtros podem especificar quais mensagens de syslog serão encaminhadas para o servidor principal Essentials. Um dos principais

benefícios da implementação de coleta distribuída é a redução das mensagens encaminhadas para os principais servidores syslog.

Falha na detecção e notificação

A finalidade do gerenciamento de falhas é detectar, isolar, notificar e corrigir defeitos identificados na rede. Os dispositivos de rede podem alertar as estações de gerenciamento quando ocorre uma falha nos sistemas. Um sistema eficaz de gerenciamento de falhas consiste em vários subsistemas. A detecção de falhas é realizada quando os dispositivos enviam mensagens de interceptação SNMP, pesquisa SNMP, limites de monitoração remota (RMON) e mensagens syslog. Um sistema de gerenciamento alerta o usuário final quando uma falha é relatada e ações corretivas podem ser tomadas.

As interceptações devem ser ativadas constantemente nos dispositivos de rede. Interceptações adicionais são compatíveis com os novos lançamentos do software Cisco IOS para roteadores e switches. É importante verificar e atualizar o arquivo de configuração para garantir a decodificação adequada das interceptações. Um exame periódico dos desvios configurados com a equipe da Cisco Assured Network Services (ANS) assegurará a detecção eficaz de falha na rede.

A tabela a seguir lista as interceptações CISCO-STACK-MIB que são compatíveis e podem ser usadas para monitorar as condições de falha nos switches da rede de área local (LAN) do Cisco Catalyst.

Armadilha	**Descrição**
moduleUp	A entidade agente detectou que o **objeto moduleStatus neste MIB fez a transição para o estado ok(2) de um de seus módulos.**
moduleDown	A entidade de agente detectou que o objeto moduleStatus nesse MIB fez a transição para fora do estado ok(2) para um de seus módulos.
chassisAlarmOn	A entidade do agente detectou que o objeto chassisTempAlarm, chassisMinorAlarm ou chassisMajorAlarm nesse MIB mudou para o estado ligado(2). Um *chassisMajorAlarm indica que existe uma das seguintes condições:* • Qualquer falha de tensão • Temperatura simultânea e falha no ventilador • Cem por cento de falha de fonte de alimentação (duas em duas ou uma em uma). • Falha da EEPROM (Memória programável de somente leitura apagável) • Falha de RAM não-volátil (NVRAM) • Falha de comunicação do MCP • Status NMP desconhecido Um chassisMinorAlarm indica que existe uma das seguintes condições:

	• Alarme de temperatura • Falha na ventoinha • Falha parcial da fonte de alimentação (uma de duas) • Duas fontes de alimentação de tipo incompatível
chassisAlarmOff	A entidade agente detectou que o objeto *chassisTempAlarm*, **chassisMinorAlarm** ou *chassisMajorAlarm neste MIB fez a transição para o estado* **off(1).**

As armadilhas de monitor ambiental (envmon) são definidas na armadilha CISCO-ENVMON-MIB. O desvio envmon envia notificações do monitor ambiental específicas do empreendimento quando um limiar ambiental for excedido. Quando envmon é usado, um tipo de armadilha ambiental específica pode ser habilitada ou todos os tipos de armadilha do sistema de monitoramento ambiental podem ser aceitos. Se não forem especificadas opções, todos os tipos de ambiente serão habilitados. Pode ser um ou mais dos valores a seguir:

- tensão — Um ciscoEnvMonVoltageNotification será enviado se a tensão medida em determinado ponto de teste estiver fora do intervalo normal do ponto de teste (como ocorre no estágio de aviso, grave ou de desligamento).
- desligamento — Um ciscoEnvMonShutdownNotification será enviado se o monitor ambiental detectar que um ponto de teste está atingindo um estado grave e está prestes a iniciar um desligamento.
- alimentação — Um ciscoEnvMonRedundantSupplyNotification será enviado se ocorrer uma falha na fonte de alimentação redundante (quando existente).
- ventoinha — Um ciscoEnvMonFanNotification será enviado se ocorrer uma falha em qualquer uma das ventoinhas na matriz de ventoinhas (quando existente).
- temperatura — Um ciscoEnvMonTemperatureNotification será enviado se a temperatura medida em determinado ponto de teste estiver fora do intervalo normal do ponto de teste (como ocorre no estágio de aviso, grave ou de desligamento).

Detecção e monitoramento de falha dos elementos de rede podem ser ampliados do nível do dispositivo aos níveis de protocolo e interface, Para um ambiente de rede, o monitoramento de falhas pode incluir VLAN (Virtual Local Area Network), modo de transferência assíncrona (ATM), indicações de falha em interfaces físicas, etc. A implementação do gerenciamento de falha de nível de protocolo está disponível ao se utilizar um sistema de gerenciamento de elemento, tal como o gerenciador de campus CiscoWorks2000. O aplicativo TrafficDirector no Campus Manager concentra-se no gerenciamento de switches e utiliza o suporte de mini-RMON nos switches Catalyst.

Com o crescente número de elementos de rede e a complexidade dos problemas de rede, um sistema para gerenciamento de eventos capaz de correlacionar diferentes eventos de rede (syslog, desvios, arquivos de registro) poderá ser considerado. Essa arquitetura por trás de um sistema de gerenciamento de eventos é comparável a um sistema MOM. Um sistema de gerenciamento de eventos bem desenvolvido permite que a equipe do centro de operações de rede (NOC) seja proativa e eficaz na detecção e no diagnóstico de problemas de rede. A priorização e a supressão de eventos permitem que a equipe de operações de rede se concentre nos eventos importantes da rede, investigue vários sistemas de gerenciamento de eventos, incluindo o Cisco Info Center, e realize uma análise de viabilidade para explorar completamente as capacidades desses sistemas. Para obter mais informações, acesse o Cisco Info Center.

Monitoração e notificação de falha proativa

Evento e alarme de RMON são dois grupos definidos na especificação de RMON. Em geral, uma estação de gerenciamento executa poll em dispositivos de rede para determinar o status ou o valor de certas variáveis. Por exemplo, uma estação de gerenciamento faz uma chamada seletiva de um roteador para saber a utilização da CPU e gerar um evento quando as ocorrências de valor atingem um limiar configurado. Este método desperdiça largura de banda de rede e pode também perder o limiar atual dependendo do intervalo de chamada seletiva.

Com os eventos e o alarme do RMON, um dispositivo de rede é configurado para monitorar a si mesmo em limiares de elevação e queda. Em um intervalo de tempo predefinido, o dispositivo de rede coleta uma amostra de uma variável e compara com os limites. Uma interceptação SNMP pode ser enviada para uma estação de gerenciamento, se o valor real estiver acima ou abaixo dos limites configurados. Os grupos de alarmes e eventos RMON fornecem um método proativo de gerenciamento de dispositivos importantes da rede.

A Cisco Systems recomenda a implementação de grupos de alarmes e eventos RMON em dispositivos importantes da rede. Variáveis monitoradas podem incluir utilização da CPU, falhas de buffer, desconexões de entrada/saída ou qualquer variável de tipos inteiros. Começando com o Software Cisco IOS versão 11.1 (1), todas as imagens do roteador são compatíveis com os grupos de alarmes e eventos RMON.

Para obter informações detalhadas sobre a implementação de evento e alarme RMON, consulte a seção Implementação de evento e alarme RMON.

Restrições de memória RMON

O uso da memória RMON é constante em todas as plataformas de switching em relação a estatística, históricos, alarmes e eventos. O RMON usa o que é chamado de *bucket para armazenar históricos e estatísticas no agente RMON (que, nesse caso, é o switch).* O tamanho do bucket é definido na prova de RMON (dispositivo SwitchProbe) ou aplicativo de RMON (ferramenta TrafficDirector) e, em seguida, é enviado ao switch para ser configurado.

Aproximadamente 450 K de espaço de código são necessários para oferecer suporte ao mini-RMON (por exemplo, quatro grupos de RMON: estatísticas, históricos, alarmes e eventos). O requisito de memória dinâmica para RMON varia porque depende da configuração do tempo de execução.

A tabela a seguir define as informações de utilização de memória RMON de tempo de execução para cada minigrupo de RMON.

Definição de grupo RMON	Espaço DRAM usado	Notas
Estatísticas	140 bytes por porta Ethernet/Fast Ethernet comutada	Por porta
Histórico	3,6 K para 50 buckets *	Cada bucket adicional utiliza 56 bytes.
Alarme e	2,6 K por alarme e suas	Por alarme por

Evento	entradas de evento correspondentes	porta

*O RMON usa o que é chamado de *bucket para armazenar históricos e estatísticas no agente RMON (como um switch).*

Implementação de evento e alarme de RMON

Com a incorporação do RMON como parte de uma solução de gerenciamento de falhas, um usuário pode monitorar a rede, de forma pró-ativa, antes que ocorra um problema em potencial. Por exemplo, se o número de pacotes de broadcast recebidos aumentar significativamente, isso pode causar um aumento na utilização do CPU. Através da implementação do alarme e evento RMON, um usuário pode configurar um limiar para monitorar o número de pacotes de difusão recebidos e alertar a plataforma SNMP por meio de um desvio SNMP se o limiar configurado for atingido. Os alarmes e eventos de RMON eliminam o poll em excesso normalmente executado pela plataforma SNMP para atingir o mesmo objetivo.

Dois métodos estão disponíveis para configurar o alarme e o evento de RMON:

- Interface de linha de comando (CLI)
- SNMP SET

Os procedimentos de amostra a seguir mostram como definir um limite para monitorar o número de pacotes de transmissão recebidos em uma interface. O mesmo contador é utilizado nesses procedimentos, como mostrado no exemplo do comando show interface no final desta seção.

Exemplo de interface de linha de comando

Para implementar o alarme de RMON e o evento usando a interface CLI, efetue os seguintes passos:

1. Encontre o índice de interface associado à Ethernet 0 percorrendo o ifTable MIB.
```
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. Obtenha o OID associado ao campo CLI a ser monitorado. Neste exemplo, o OID de 'difusão é 1.3.6.1.2.1.2.2.1.12. Os OIDs da Cisco para variáveis de MIB específicas estão disponíveis no site da web cisco.com.
3. Determine os seguintes parâmetros para configurar limites e eventos.limiares de elevação e de quedatipo de amostragem (absoluta ou delta)intervalo de amostragemação a ser realizada quando o limiar é alcançadoPara os fins deste exemplo, um limite está sendo configurado para monitorar o número de pacotes de transmissão recebidos na Ethernet 0. Uma interceptação será gerada se o número de pacotes de transmissão recebidos for maior que 500 entre as amostras de 60 segundos. O limiar será reativado quando o número de difusões de entrada não aumentar entre amostras tiradas.**Observação:** para obter detalhes sobre esses parâmetros de comando, consulte a documentação do Cisco Connection Online (CCO) para obter os comandos de alarme e evento RMON para sua versão específica do Cisco IOS.
4. Especifique trap sent (evento RMON) quando o limiar for atingido usando os seguintes comandos de CLI (os comandos do Cisco IOS são exibidos em negrito):**rmon event 1 trap**

gateway description "High Broadcast on Ethernet 0" owner ciscormon event 2 log description "normal broadcast received on ethernet 0" owner cisco

5. Especifique os limiares e parâmetros relevantes (alarme RMON) usando os seguintes comandos de CLI:**rmon alarm 1 ifEntry.12.1 60 delta rising-threshold 500 1falling-threshold 0 2 owner cisco**
6. Use o SNMP para pesquisar essas tabelas a fim de verificar se as entradas do eventTable foram realizadas no 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. Use o SNMP para pesquisar essas tabelas a fim de verificar se as entradas do alarmTable foram definidas.

```
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)
```

Exemplo de SET de SNMP

Para implementar o alarme e o evento de RMON com a operação SNMP SET, siga estas etapas:

1. Especifique a interceptação enviada (evento de RMON) quando o limite for atingido, usando as seguintes operações de SNMP SET:
```
# 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 os limites e parâmetros relevantes (alarme de RMON), usando as seguintes operações de SNMP SET:
```
# 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. Pesquise essas tabelas a fim de verificar se as entradas do eventTable foram realizadas no 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. Pesquise essas tabelas a fim de verificar se as entradas do alarmTable foram definidas.

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

show interface

Este exemplo é um resultado do comando **show interface.**

gateway> **show interface ethernet 0**

```
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
```

Gerenciamento de configuração

O objetivo do gerenciamento de configuração é monitorar as informações de rede e de configuração do sistema, de modo que os efeitos da operação de rede de várias versões de elementos de hardware e software possam ser rastreados e gerenciados.

Padrões de configuração

Com um número crescente de dispositivos de rede implantados, é fundamental identificar com precisão o local de um dispositivo de rede. Essas informações de localização devem fornecer uma descrição detalhada significativa àqueles que estiverem encarregados das tarefas de envio de recursos, quando ocorrer um problema de rede. Para acelerar uma resolução se ocorrer um problema de rede, verifique se as informações de contato da pessoa ou do departamento responsável pelos dispositivos estão disponíveis. As informações de contato devem incluir número de telefone e nome da pessoa ou do departamento.

As convenções de nomenclatura de rede, iniciando no nome de dispositivo de cada interface, deve ser planejada e implementada como parte do padrão de configuração. Uma convenção de nomenclatura bem definida dá à equipe a capacidade de fornecer informações precisas ao resolver problemas de rede. A convenção de nomenclatura dos dispositivos pode usar localização geográfica, nome de edifícios, andar e assim por diante. Para a convenção de nomenclatura da interface, é possível incluir o segmento ao qual uma porta está conectada, o nome do hub de conexão e assim por diante. Em interfaces seriais, ela deve incluir a largura de banda real, o número do Identificador da conexão do enlace de dados (DLCI) local (se Frame Relay), o destino e o ID do circuito ou informações fornecidas pela portadora.

Gerenciamento de arquivos de configuração

Ao adicionar novos comandos de configuração nas necessidades dos dispositivos de rede atuais, verifique os comandos quanto à integridade antes da implementação real. Um dispositivo de rede configurado incorretamente pode ter um efeito desastroso na conectividade e no desempenho da rede. Os parâmetros do comando de configuração devem ser verificados para evitar problemas de falta de correspondência ou incompatibilidade. É aconselhável agendar regularmente uma revisão completa das configurações com os engenheiros Cisco.

Um CiscoWorks2000 Essentials totalmente funcional permite o backup automático dos arquivos de configuração nos roteadores e switches Cisco Catalyst. O recurso de segurança do Essentials pode ser utilizado para executar a autenticação em alterações de configuração. Um registro de exame de alterações está disponível para rastrear alterações e o nome de usuário das pessoas que fazem as alterações. Para alterações de configuração em vários dispositivos, há duas opções disponíveis: a NetConfig baseada na Web na versão atual do CiscoWorks2000 Essentials ou no script **cwconfig.** Você pode fazer o download e o upload dos arquivos de configuração no CiscoWorks2000 Essentials, utilizando os moldes predefinidos ou definidos pelo usuário.

Essas funções podem ser realizadas com as ferramentas de gerenciamento de configuração no CiscoWorks2000 Essentials:

- Retire os arquivos de configuração do arquivo de configuração Essentials (Fundamentos) para um dispositivo ou dispositivos múltiplos
- Extraia a configuração do dispositivo para o arquivo do Essentials
- Extraia a configuração mais recente do arquivo e grave em um arquivo
- Importar a configuração de um arquivo e enviá-la aos dispositivos
- Compare as duas últimas configurações no arquivo Essentials
- Exclua as configurações anteriores a uma data ou versão especificada do arquivo
- Copiar a configuração de inicialização para a configuração de execução

Inventory Management

A função de descoberta da maioria das plataformas de gerenciamento é planejada para fornecer

uma listagem dinâmica de dispositivos encontrados na rede. Deve-se utilizar mecanismos de descoberta como os implementados nas plataformas de gerenciamento de rede.

Um banco de dados de inventário fornece informações de configuração detalhadas nos dispositivos de rede. As informações comuns incluem modelos de hardware, módulos instalados, imagens de software, níveis de microcódigo etc. Todas essas informações são fundamentais para concluir tarefas, como manutenção de software e hardware. A listagem atualizada de dispositivos de rede coletadas pelo processo de descoberta pode ser usada como lista principal para coletar informações de estoque usando SNMP ou scripts. Uma lista de dispositivos pode ser importada do CiscoWorks2000 Campus Manager para o banco de dados de inventário do CiscoWorks2000 Essentials, para obter um inventário atualizado dos switches Cisco Catalyst.

Gerenciamento do software

Uma atualização bem-sucedida de imagens do Cisco IOS em dispositivos de rede exige uma análise detalhada dos requisitos como memória, ROM de inicialização, nível de microcódigo e outros. Normalmente, os requisitos são documentados e disponibilizados no site da Cisco na forma de notas de versão e guias de instalação. O processo de atualização de um dispositivo de rede que esteja executando o Cisco IOS inclui fazer o download de uma imagem correta do CCO, fazer o backup da imagem atual, verificar se todos os requisitos de hardware foram atendidos e carregar a nova imagem no dispositivo.

A janela de atualização para concluir a manutenção do dispositivo é bastante limitada para algumas empresas. Em um ambiente de rede com recursos limitados, pode ser necessário programar e automatizar as atualizações de software para fora do horário comercial. O procedimento pode ser concluído com o uso da linguagem de scripts, como Expect, ou de um aplicativo gravado especificamente para realizar essa tarefa.

As alterações de software nos dispositivos de rede, como imagens do Cisco IOS e versões de microcódigo, devem ser rastreadas para ajudar na fase de análise quando outra manutenção de software for necessária. Com um relatório de histórico de modificação prontamente disponível, o responsável executando a atualização pode minimizar o risco de carregar imagens incompatíveis ou microcódigo nos dispositivos de rede.

Gerenciamento de desempenho

Contrato de nível de serviço

Um Contrato de Nível de Serviço (SLA) é um contrato por escrito entre um fornecedor de serviço e seus clientes sobre o nível de desempenho esperado dos serviços de rede. O SLA consiste em métricas acordadas entre o provedor e seus clientes. Os valores definidos para as métricas dever ser realistas, significativos e mensuráveis para ambas as partes.

Várias estatísticas de interface podem ser coletadas dos dispositivos de rede para medir o nível de desempenho. Essas estatísticas podem ser incluídas como métricas no SLA. Estatísticas como descartes da fila de entrada, descartes da fila de saída e pacotes ignorados são úteis para o diagnóstico de problemas relacionados ao desempenho.

No nível de dispositivo, a métrica de desempenho pode incluir utilização de CPU, alocação de buffer (grande, médio, perdas, taxa de acerto) e alocação de memória. O desempenho de certos protocolos de rede está diretamente relacionado à disponibilidade de buffer nos dispositivos de

rede. Medir as estatísticas de desempenho de nível do dispositivo é decisivo na otimização do desempenho de protocolos de um nível mais alto.

Dispositivos de rede, como roteadores, oferecem suporte a vários protocolos de camada superior, como Data Link Switching Workgroup (DLSW), Remote Source Route Bridging (RSRB), AppleTalk e assim por diante. Estatísticas de desempenho de tecnologias de WAN (rede de área ampla), incluindo Frame Relay, ATM, ISDN (Rede Digital de Serviços Integrados) e outros, podem ser monitoradas e coletadas.

Monitoramento, medição e relatório de desempenho

Diferentes métricas de desempenho em níveis de interface, dispositivo e protocolo devem ser coletadas regularmente com o uso do SNMP. O mecanismo de apuração em um sistema de gerenciamento de rede pode ser usado para propósitos de coleta de dados. A maioria dos sistemas de gerenciamento de rede é capaz de coletar, armazenar e apresentar dados em poll.

Várias soluções estão disponíveis no mercado para atender às necessidades de gerenciamento de desempenho em ambientes corporativos. Esses sistemas são capazes de coletar, armazenar e apresentar dados a partir de dispositivos e servidores de rede. Para a maioria dos produtos, a interface baseada na Web torna os dados de desempenho acessíveis em qualquer lugar da empresa. Algumas das soluções de gerenciamento de desempenho implantadas normalmente incluem:

- InfoVista VistaView
- SAS IT Service Vision
- Trinagy TREND

Uma avaliação dos produtos acima determinará se eles satisfazem às exigências dos diferentes usuários. Alguns fornecedores dão suporte à integração com plataformas de gerenciamento de rede e de sistema. Por exemplo, o InfoVista oferece suporte ao BMC Patrol Agent para fornecer estatísticas importantes de desempenho pelos servidores de aplicativos. Cada produto tem um modelo de preço diferente e recursos diferentes com a oferta base. O suporte para recursos de gerenciamento de desempenho para dispositivos da Cisco, como NetFlow, RMON e Agente de garantia de serviço Cisco IOS/Relator de tempo de resposta (RTR/SAA CSAA/RTR), está disponível em algumas soluções. Recentemente, a Concord agregou o suporte para switches de WAN da Cisco que podem ser usados para coletar e visualizar dados de desempenho.

O recurso CSAA/RTR Service Assurance Agent (SAA)/Response Time Reporter (RTR)(Agente de Garantia de Serviço (SAA)/Reporter de Tempo de Resposta (RTR)) do Cisco IOS pode ser utilizado para medir o tempo de resposta entre dispositivos IP. Um roteador de origem com CSAA configurado é capaz de medir o tempo de resposta para um dispositivo IP de destino, que pode ser um roteador ou um dispositivo IP. O tempo de resposta pode ser medido entre a origem e o destino ou para cada salto ao longo do caminho. Os desvios SNMP podem ser configurados para alertar consoles de gerenciamento de alertas quando o tempo de resposta excede aos limiares predefinidos.

As recentes melhorias no Cisco IOS ampliam os recursos do CSAA para medir o seguinte:

- Desempenho do serviço HTTP (HyperText Transfer Protocol)Consulta de DNS (sistema de nome de domínio)Conexão do protocolo TCPTempo de transação HTTP
- Variação (jitter) de retardo entre pacotes de tráfego de VoIP (Voz sobre IP)
- Tempo de resposta entre os endpoints para uma qualidade de serviço (QoS) específicaBits

do tipo de serviço (ToS) IP
- Perda de pacotes usando pacotes gerados por CSAA

A configuração do recurso CSAA em roteadores pode ser realizada usando o aplicativo Cisco Internetwork Performance Monitor (IPM). O CSSA/RTR está incluído em vários, mas não em todos os conjuntos de recursos do software Cisco IOS. Uma versão do software Cisco IOS compatível com CSAA/RTR deve ser instalada no dispositivo que o IPM usa para coletar as estatísticas de desempenho. Para obter um resumo das versões do Cisco IOS que oferecem suporte a CSAA/RTR/IPM, consulte o site na Web Perguntas mais freqüentes sobre IPM.

As informações adicionais sobre o IPM incluem:

- Visão geral do IPM
- Agente de garantia de serviço

Análise e ajuste de desempenho

O tráfego do usuário aumentou de forma significativa e intensificou a demanda de recursos da rede. Normalmente, os gerentes de rede têm uma visão limitada sobre os tipos de tráfego em execução na rede. A caracterização de perfil de tráfego de aplicativo e usuário fornece uma visão detalhada do tráfego na rede. Duas tecnologias, RMON probes e NetFlow, fornecem a capacidade de coletar os perfis de tráfego.

RMON

Os padrões RMON são criados para serem implantados em uma arquitetura distribuída onde agentes (integrados ou em probes independentes) se comunicam com uma estação central (o console de gerenciamento) por meio de SNMP. O padrão RFC 1757 RMON organiza as funções de monitoração em nove grupos para oferecer suporte às topologias de Ethernet e adicione um décimo grupo na RFC 1513 para parâmetros exclusivos de Token Ring. O monitoramento de link Fast Ethernet é fornecido na estrutura do padrão RFC 1757 e o monitoramento de anel FDDI (Fiber-Distributed Data Interface) é fornecido na estrutura do RFC 1757 e RFC 1513.

A especificação RFC 2021 RMON emergente leva os padrões de monitoramento remoto além da camada MAC (Media Access Control) para as camadas da rede e de aplicativos. Essa configuração permite que administradores analisem e solucionem problemas de aplicações em rede, como tráfego da Web, NetWare, Notes, e-mail, acesso a banco de dados, NFS e outros. Alarmes, estatísticas, histórico e host/grupos de conversação RMON podem ser usados para monitorar proativamente e manter a disponibilidade da rede com base no tráfego de camada do aplicativo, o tráfego mais crítico na rede. O RMON2 permite que os administradores de rede continuem a implantação das soluções de monitoramento baseadas em padrões para oferecer suporte a aplicativos essenciais baseados em servidores.

As tabelas a seguir listam as funções dos grupos RMON.

Grupo RMON (RFC 1757)	Função

Estatísticas	Contadores de pacotes, octetos, transmissões, erros e ofertas no segmento ou na porta.
Histórico	Faz amostragens e salva os contadores de grupo de estatística para a recuperação posterior periodicamente.
Hosts	Mantém as estatísticas sobre cada dispositivo host no segmento ou na porta.
Host Top N	Um relatório de subconjunto definido pelo usuário do grupo Hosts, classificado por um contador estatístico. Ao retornar apenas os resultados, o tráfego de gerenciamento é minimizado.
Matriz de Tráfego	Mantém as estatísticas de conversa entre hosts na rede.
Alarmes	Um limite que pode ser definido em variáveis RMON essenciais no gerenciamento proativo.
Events	Gera armadilhas de SNMP e entradas de registro quando é ultrapassado um limiar de grupo de alarmes.
Captura do pacote	Gerencia os buffers dos pacotes capturados pelo grupo de filtro para fazer upload para o console de gerenciamento.
Token Ring	Estação do anel — estatísticas detalhadas sobre a Solicitação da estação de anel das estações individuais — uma lista de estações solicitada atualmente na Configuração da estação de anel — configuração e inserção/remoção de acordo com o roteamento de origem da estação — estatísticas sobre o roteamento de origem, como contagens de salto, entre outros

RMON2	Função
Diretório do Protocolo	Protocolos para os quais o agente monitora e mantém estatísticas.
Distribuição de protocolo	Estatísticas para cada protocolo.
Host da camada da rede	Estatísticas para cada endereço de camada de rede no segmento, anel ou porta.
Matriz da camada da rede	As estatísticas de tráfego para pares de endereços de camada de rede.
Host de Camada	Estatísticas por protocolo de camada de aplicação de cada endereço da rede.

de Aplicativos	
Matriz da Camada de Aplicativo	Estatísticas de tráfego por protocolo da camada de aplicativos para os pares de endereços da camada de rede.
Histórico definido pelo usuário	Estende o histórico além das estatísticas da camada de link RMON1 para incluir as estatísticas RMON, RMON2, MIB-I ou MIB-II.
Mapeamento de endereços	Ligações de endereço de camada MAC à rede.
Grupo de configuração	Capacidades e configurações de agente.

Netflow

O recurso Cisco NetFlow permite que estatísticas detalhadas de fluxos de tráfego sejam coletadas para as funções de planejamento de capacidade, faturamento e Troubleshooting. O NetFlow pode ser configurado em interfaces individuais, fornecendo informações sobre o tráfego que passa por essas interfaces. Os seguintes tipos de informações fazem parte das estatísticas de tráfego detalhadas:

- Endereços IP de origem e de destino
- Números de interface de entrada e saída
- Porta de origem TCP/UDP e portas de destino
- Número de bytes e pacotes no fluxo
- Números de sistemas autônomos de origem e de destino
- ToS (Tipo de serviço) de IP

Os dados do NetFlow coletados nos dispositivos de rede são exportados para uma máquina coletora. O coletor realiza funções como redução do volume de dados (filtragem e agregação), armazenamento de dados hierárquicos e gerenciamento do sistema de arquivos. A Cisco fornece os aplicativos NetFlow Collector e NetFlow Analyzer para coletar e analisar os dados dos roteadores e switches Cisco Catalyst. Existem também ferramentas shareware, como cflowd, que podem coletar os registros de UDP (protocolo de datagrama do usuário) Cisco NetFlow.

Os dados do NetFlow são transportados usando pacotes UDP em três formatos diferentes:

- Versão 1 — O formato original compatível nas versões iniciais do NetFlow.
- Versão 5 — Um aprimoramento posterior que adicionou informações do sistema autônomo do Protocolo BGP e números de sequência de fluxo.
- Versão 7 — Um aprimoramento ainda mais recente que adicionou o suporte de switching do NetFlow para switches Cisco Catalyst 5000 Series equipados com uma placa NFFC.

As versões de 2 a 4 e a versão 6 não foram lançadas ou não são suportadas pelo FlowCollector. Em todas as três versões, o datagrama consiste em um cabeçalho e um ou mais registros de fluxo.

Para obter mais informações, consulte o white paper Guia de soluções dos serviços NetFlow.

A tabela a seguir descreve as versões compatíveis do Cisco IOS para coletar dados do NetFlow em roteadores e switches Catalyst.

Versão do Cisco IOS Software	Plataformas de Hardware da Cisco Suportadas	Versões Exportadas de NetFlow Suportado
11.1 CA e 11.1 CC	Cisco 7200, 7500 e RSP7000	V1 e V5
11.2 e 11.2P	Cisco 7200, 7500 e RSP7000	V1
11,2 P	Cisco Route Switch Module (RSM)	V1
11.3 e 11.3 T	Cisco 7200, 7500 e RSP7000	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000 e RSM	V1 e V5
12,0 T	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM e BPX 8600	V1 e V5
12.0(3)T e posterior	Cisco 1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM e BPX 8650	V1, V5 e V8
12.0(6)S	Cisco 12000	V1, V5 e V8
—	Cisco Catalyst 5000 com placa NFFC***	V7

* O suporte para NetFlow Export V1, V5 e V8 nas plataformas Cisco 1600 e 2500 é direcionado para o software Cisco IOS versão 12.0 (T). O suporte do NetFlow para essas plataformas não está disponível na versão principal do Cisco IOS 12.0.

** O suporte para NetFlow V1, V5 e V8 na plataforma AS5300 é direcionado para o software Cisco IOS versão 12.6 (T).

*** O MLS e a exportação de dados NetFlow são suportados no Catalyst 5000 Series Supervisor Engine Software Release 4.1(1) ou mais recente.

Gerenciamento de segurança

O objetivo da gestão de segurança é controlar o acesso aos recursos da rede de acordo com as diretrizes locais de modo que não seja possível sabotar a rede (intencional ou involuntariamente). Um subsistema de gerenciamento da segurança, por exemplo, pode monitorar o registro de usuários em um recurso de rede, recusando acesso àqueles que inserirem códigos inadequados de acesso. A gestão da segurança é um assunto muito amplo; portanto, essa área do documento aborda somente a segurança relacionada ao SNMP e a segurança básica de acesso ao dispositivo.

As informações detalhadas sobre segurança avançada incluem:

- Aumentando a segurança em redes IP
- OpenSystems

Uma boa implementação da gestão de segurança começa com a aplicação de políticas e procedimentos de segurança adequados. É importante criar um padrão de configuração mínima específico da plataforma para todos os roteadores e switches que seguem as melhores práticas do setor para segurança e desempenho.

Existem vários métodos de controle de acesso nos roteadores Cisco e switches Catalyst. Alguns desses métodos incluem:

- Listas de controle de acesso (ACL)
- IDs de usuário e senhas locais para o dispositivo
- Terminal Access Controller Access Control System (TACACS)

O TACACS é um protocolo de segurança padrão da Internet Engineering Task Force (RFC 1492) que é executado entre dispositivos clientes em uma rede e em um servidor TACACS. TACACS é um mecanismo de autenticação usado para autenticar a identidade de um dispositivo que busca acesso remoto a um banco de dados com privilégios. As variações do TACACS incluem o TACACS+, a arquitetura AAA que separa as funções de autenticação, autorização e auditoria.

O TACACS+ é usado pelo Cisco para permitir um controle maior sobre quem acessa o dispositivo Cisco no modo privilegiado e não-privilegiado. Vários servidores TACACS+ podem ser configurados para tolerância a falhas. Com o TACACS+ ativado, o roteador e o switch solicitam ao usuário um nome de usuário e uma senha. A autenticação pode ser configurada para controle de logon ou para autenticar comandos individuais.

Autenticação

A autenticação é o processo de identificação de usuários, incluindo o login e senha, desafio e resposta, e suporte para mensagens. A autenticação é a forma como um usuário é identificado antes de ter acesso ao roteador ou switch. Existe uma relação fundamental entre autenticação e autorização. Quanto mais privilégios de autorização um usuário recebe, mais segura deverá ser a autenticação.

Autorização

A autorização fornece controle de acesso remoto, incluindo autorização de uma vez e autorização para cada serviço que for solicitado pelo usuário. Em um Cisco Router, o intervalo de nível de autorização para usuários é de 0 a 15 com 0 sendo o nível mais baixo e 15 o mais alto.

Relatório

A auditoria permite a coleta e o envio das informações de segurança usadas para faturamento, auditoria e relatório, como identidades de usuário, horários de início e término e comandos executados. O relatório permite aos gerentes de rede rastrear os serviços que os usuários estão acessando, bem como a quantidade de recursos de rede que estão consumindo.

A tabela a seguir lista os comandos básicos de amostra para o uso de TACACS+, autenticação, autorização e auditoria em um roteador Cisco e um switch Catalyst. Consulte o documento Comandos de autenticação, autorização e auditoria para obter mais detalhes sobre os comandos.

Comando do Cisco IOS	Propósito
Router	
aaa new-model	Ative a autenticação, a autorização e a auditoria (AAA) como o método primário para o controle de acesso.
Auditoria AAA {*system* | *rede* | *ligação* | *EXEC* | *nível de comando*} {*start-stop* | *wait-start* | *stop only*} {*tacacs+* | *radius*}	Habilite o relatório com os comandos de configuração global.
AAA authentication login default tacacs+	Configure o roteador de modo que as conexões com as linhas terminais configuradas com o padrão de login sejam autenticadas com TACACS+ e não funcionem caso ocorra uma falha na autenticação por qualquer motivo.
AAA authorization exec default tacacs+ none	Configure o roteador para verificar se o usuário tem permissão para executar um shell EXEC perguntando ao servidor TACACS+.
tacacs-server host *tacacs+ server ip address*	Especifique o servidor TACACS+ que será usado para autenticação com comandos de configuração global.
tacacs-server key shared-secret	Especifique o segredo compartilhado conhecido pelos servidores TACACS+ e o roteador Cisco com o comando de configuração global.
Catalyst Switch	
set authentication login tacacs enable [*all* | *console* | *http* | *telnet*] [*primary*]	Ative a autenticação do TACACS+ para modo de login normal. Use o console ou as palavras-chave de Telnet para ativar o TACACS+ apenas para tentativas de conexão da porta de console ou Telnet.

set authorization exec enable {option} fallback option} [*console* | *telnet* | *ambos*]	Habilite autorização para o modo de logon normal. Use o console ou palavras-chave de Telnet para habilitar a autorização somente para a porta de console ou as tentativas de conexão Telnet.
Set tacacs-server key *shared-secret*	Especifique o segredo compartilhado que é conhecido pelos servidores TACACS+ e pelo switch.
Set tacacs-server host tacacs+ server ip address	Especifique o servidor TACACS+ que será usado para autenticação com comandos de configuração global.
Set accounting commands enable {*config* | *all*} {*stop-only*} *tacacs+*	Ative a contabilização dos comandos de configuração.

Para obter mais informações sobre como configurar o AAA para monitorar e controlar o acesso à interface de linha de comando nos switches de LAN corporativa CATALYST, consulte o documento Controle de acesso ao switch usando autenticação, autorização e auditoria.

Segurança de SNMP

O protocolo SNMP pode ser usado para fazer alterações de configuração nos roteadores e switches Catalyst semelhantes aos emitidos na CLI. Configure medidas de segurança apropriadas nos dispositivos de rede para impedir acesso não autorizado e alterações via SNMP. As strings de comunidade devem seguir as diretrizes padrão de senha para tamanho, caracteres e dificuldade de adivinhação. É importante alterar as strings de comunidade dos padrões público e privado.

Todos os hosts de gerenciamento de SNMP devem ter um endereço IP estático e receber explicitamente direitos de comunicação de SNMP com o dispositivo de rede por aquele endereço IP predefinido e Lista de Controle de Acesso (ACL). Os softwares Cisco IOS e Cisco Catalyst fornecem recursos de segurança que garantem que apenas as estações de gerenciamento autorizadas tenham permissão para fazer alterações em dispositivos de rede.

Recursos de segurança do roteador

Nível de privilégio SNMP

Esse recurso limita os tipos de operações que uma estação de gerenciamento pode ter em um roteador. Existem dois tipos de nível de privilégio nos roteadores: Somente leitura (RO) e Leitura-gravação (RW). O nível de RO só permite que uma estação de gerenciamento consulte os dados do roteador. Ele não permite a execução de comandos de configuração, como a reinicialização de um roteador e o fechamento de interfaces. Apenas o nível de privilégio RW pode ser usado para realizar essas operações.

Lista ACL de SNMP

Épossível usar o recurso SNMP ACL com o recurso de privilégio SNMP para limitar as

requisições de informações das estações de gerenciamento específico feitas aos roteadores.

Visualização de SNMP

Esse recurso limita as informações específicas que as estações de gerenciamento podem recuperar dos roteadores. Pode ser utilizado com recursos de nível de privilégio de SNMP e de ACL para aplicar acesso restrito de dados por consoles de gerenciamento. Para amostras de configuração da visualização do SNMP, acesse snmp-server view.

SNMP Versão 3

O SNMP versão 3 (SNMPv3) fornece trocas seguras de dados de gerenciamento entre dispositivos de rede e estações de gerenciamento. Os recursos de criptografia e autenticação do SNMPv3 garantem elevado grau de segurança no transporte de pacotes para um console de gerenciamento. O SNMPv3 é compatível como o software Cisco IOS versão 12.0(3)T e posterior. Para obter um resumo técnico de SNMPv3, acesse a documentação de SNMPv3.

Lista de Controle de Acesso (ACL) em interfaces

O recurso de ACL fornece medidas de segurança que evitam ataques, como falsificação de IP. O ACL pode ser aplicado em interfaces de entrada ou de saída nos roteadores.

Recurso de segurança do switch de LAN Catalyst

Lista de permissão IP

O recurso de Lista de permissão IP restringe o acesso de entrada Telnet e SNMP ao switch a partir de endereços IP de origem não autorizada. As mensagens do syslog e as armadilhas do SNMP são suportadas para notificar um sistema de gerenciamento quando ocorre uma violação ou acesso não autorizado.

Uma combinação dos recursos de segurança do Cisco IOS pode ser usada para gerenciar roteadores e switches Catalyst. É necessário estabelecer uma política de segurança que limite o número de estações de gerenciamento que podem acessar os switches e roteadores.

Para obter mais informações sobre como aumentar a segurança nas redes IP, acesse Aumento de segurança nas redes IP.

Gerenciamento de relatórios

Gerenciamento de contabilidade é o processo utilizado para medir os parâmetros de utilização da rede, de modo que cada usuário ou grupos de usuários na rede possam ser adequadamente regulados para finalidades contábeis ou de cobrança retroativa. Similar ao gerenciamento de desempenho, o primeiro passo em direção a um gerenciamento correto de relatório é medir a utilização de todos os recursos de rede importantes. A utilização do recurso de rede pode ser medida, utilizando os recursos Cisco NetFlow e Cisco IP Accounting. Uma análise dos dados coletados por esses métodos fornece uma percepção nos padrões atuais de utilização.

Um sistema de contabilidade e cobrança com base no uso é uma parte essencial de qualquer contrato de nível de serviço (SLA). Fornece uma maneira prática de definir obrigações em um SAL e as conseqüências para comportamentos que não estejam de acordo com os termos do

SLA.

Os dados podem ser coletados através de testes ou do Cisco NetFlow. A Cisco fornece os aplicativos NetFlow Collector e NetFlow Analyzer para coletar e analisar os dados dos roteadores e switches Catalyst. Aplicativos shareware, como cflowd, também são usados para a coleta de dados do NetFlow. Uma medição contínua do uso dos recursos pode conceder informações de faturamento, bem como as avaliações de informações contínuas consideráveis e recursos ideais. Algumas soluções de gerenciamento de relatório implantadas normalmente incluem:

- Software evidente

Estratégia de ativação de NetFlow e de coleta de dados

NetFlow (fluxo de rede) é uma tecnologia de medida lateral de entrada que permite a captura dos dados necessários para o planejamento de rede, monitoramento e aplicativos de relatório. O NetFlow deve ser distribuído em interfaces de roteador de ponta/agregação para provedores de serviço ou interfaces de roteador de acesso de WAN para clientes de empreendimento.

A Cisco Systems recomenda uma distribuição de NetFlow cuidadosamente planejada com os serviços NetFlow ativados nesses roteadores estrategicamente localizados. O NetFlow pode ser implementado incrementalmente (interface por interface) e estrategicamente (em roteadores selecionados meticulosamente), ao invés de ser implementado em cada roteador da rede. A equipe da Cisco trabalhará com os clientes para determinar em quais roteadores-chave e interfaces-chave o NetFlow deve ser ativado com base nos padrões de fluxo de tráfego, na topologia de rede e na arquitetura do cliente.

As principais considerações de distribuição incluem:

- Os serviços de NetFlow devem ser utilizados como medidores de margem e ferramenta de aceleração de desempenho da lista de acesso e não devem ser ativados em roteadores hot core/backbone ou roteadores que estejam sendo executados em taxas de utilização de CPU muito altas.
- Compreendendo os requisitos de levantamento de dados direcionados ao aplicativo. Aplicativos de contabilidade só podem requerer informações de fluxo do roteador de origem e terminação, enquanto aplicativos de monitoramento podem requerer uma visão mais abrangente de ponta-a-ponta (com muitos dados).
- Entenda o impacto da topologia de rede e da política de roteamento na estratégia de coleta de fluxo. Por exemplo, evite coletar fluxos duplicados ao ativar o NetFlow em roteadores de agregação-chave em que o tráfego se origina ou termina, e não em roteadores de backbone ou intermediários, o que forneceria visões duplicadas das informações do mesmo fluxo.
- Os provedores de serviços no mercado das *transportadoras (que não transportam tráfego de origem nem de término na rede) podem utilizar os dados do NetFlow Export para medir o uso de tráfego em trânsito dos recursos de rede para fins de contabilidade e cobrança.*

Configurar a contabilidade IP

O suporte de relatório de IP Cisco fornece funções básicas de relatório de IP. Ao habilitar a contabilização de IP, os usuários podem visualizar o número de bytes e pacotes comutados pelo Cisco IOS Software com IP Addresses de base de origem e de destino. Apenas o tráfego IP de trânsito é medido e apelas em base de saída. O tráfego gerado pelo software ou terminando no

software não foi incluído nas estatísticas de contabilidade. Para manter a precisão dos totais de contabilidade, o software mantém dois bancos de dados de contabilidade: um banco de dados ativo e um de ponto de controle.

O suporte de contabilidade IP da Cisco também fornece informações que identificam o tráfego IP com falha nas listas de acesso IP. Identificar a fonte de endereço IP que viola as listas de acesso de IP, sinaliza as possíveis tentativas de romper a segurança. Os dados também indicam que as configurações da lista de acesso IP devem ser verificadas. Para tornar esse recurso disponível para os usuários, habilite a contabilidade IP de violações da lista de acesso, usando o comando ip accounting access-violations. Os usuários podem exibir o número de bytes e pacotes de uma única origem que tentou violar a segurança de acordo com a lista de acesso para o par de destino de origem. Como padrão, o relatório de IP exibe o número de pacotes que passaram por listas de acesso e foram roteados.

Para ativar a contabilidade IP, use um dos seguintes comandos para cada interface no modo de configuração de interface:

Comando	Propósito
ip accounting	Ative contabilidade básica IP.
ip accounting access violations	Habilite a contabilidade IP com a capacidade de identificar tráfego IP que falhe nas listas de acessos IP.

Para configurar outras funções de relatório de IP, use um ou mais dos seguintes comandos no modo de configuração global:

Comando	Propósito
ip accounting-threshold threshold	Defina o número máximo de entradas contábeis a serem criadas.
ip accounting-list ip-address wildcard	Filtre informações de contabilização para hosts.
ip accounting-transits count	Controle o número de registros de transmissão que serão armazenados no banco de dados de contabilidade de IP.

Consulte as Convenções de dicas técnicas da Cisco para obter informações sobre as convenções usadas neste documento.