Sistema di gestione di rete: White paper sulle procedure ottimali

Sommario

Introduzione

Il modello ISO (International Organization for Standardization) definisce cinque aree funzionali della gestione della rete. Questo documento copre tutte le aree funzionali. L'obiettivo generale di questo documento è quello di fornire raccomandazioni pratiche su ciascuna area funzionale per aumentare l'efficacia complessiva degli attuali strumenti e pratiche di gestione. Fornisce inoltre linee guida di progettazione per la futura implementazione di tecnologie e strumenti di gestione della rete.

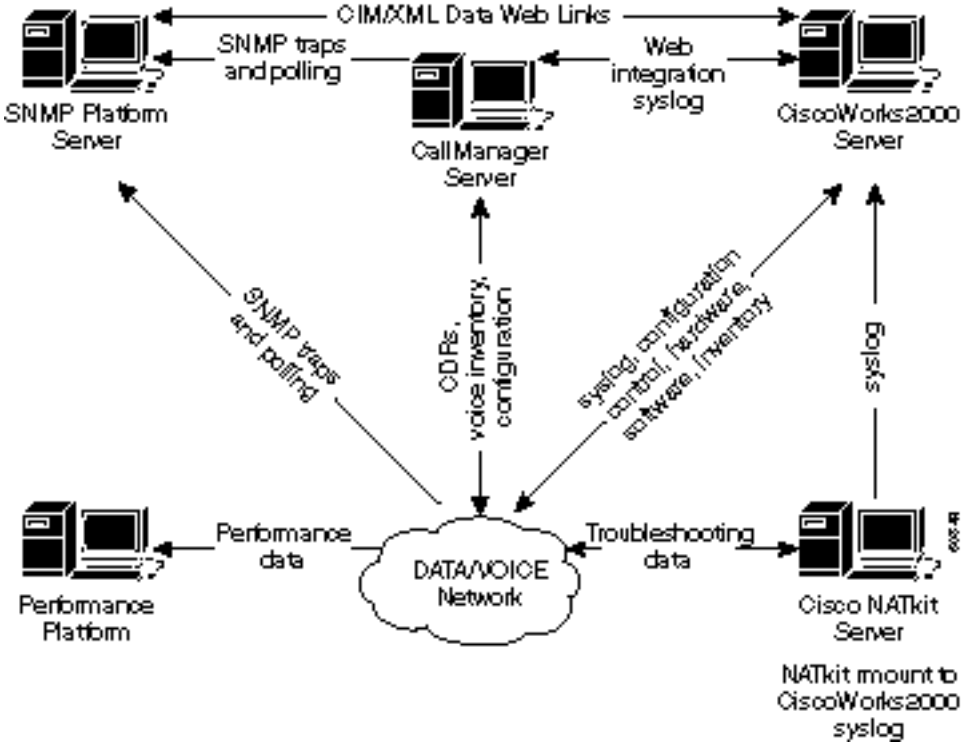
Gestione della rete

Di seguito sono elencate le cinque aree funzionali del modello di gestione di rete ISO.

- Gestione degli errori (Fault Management) - Consente di rilevare, isolare, notificare e correggere gli errori rilevati nella rete.

- Gestione della configurazione: aspetti della configurazione dei dispositivi di rete, ad esempio la gestione dei file di configurazione, dell'inventario e del software.
- Gestione delle prestazioni: monitoraggio e misurazione dei vari aspetti delle prestazioni in modo da mantenere le prestazioni globali a un livello accettabile.
- Gestione della sicurezza: accesso ai dispositivi di rete e alle risorse aziendali da parte di utenti autorizzati.
- Accounting Management: informazioni sull'uso delle risorse di rete.

Il diagramma seguente mostra un'architettura di riferimento che Cisco Systems ritiene debba essere la soluzione minima per la gestione di una rete di dati. Questa architettura include un server Cisco CallManager per coloro che intendono gestire il protocollo VoIP (Voice over Internet Protocol): Il diagramma mostra come integrare il server CallManager nella topologia NMS.



L'architettura di gestione della rete include quanto segue:

- Piattaforma SNMP (Simple Network Management Protocol) per la gestione degli errori
- Piattaforma di monitoraggio delle prestazioni per la gestione e l'analisi delle tendenze a lungo termine
- Server CiscoWorks2000 per la gestione della configurazione, la raccolta di syslog e la gestione dell'inventario hardware e software

Alcune piattaforme SNMP possono condividere direttamente i dati con il server CiscoWorks2000 utilizzando i metodi CIM/XML (Common Information Model/eXtensible Markup Language). CIM è un modello di dati comune di uno schema neutro dal punto di vista dell'implementazione per la descrizione delle informazioni di gestione complessive in un ambiente di rete/aziendale. CIM è costituito da una specifica e da uno schema. La specifica definisce i dettagli per l'integrazione con altri modelli di gestione, quali MIB SNMP o file MIF DMTF (Desktop Management Task Force Management Information Files), mentre lo schema fornisce le descrizioni effettive del modello.

XML è un linguaggio di markup utilizzato per rappresentare dati strutturati in formato testo. Uno degli obiettivi specifici del linguaggio XML era quello di mantenere la maggior parte della potenza descrittiva del linguaggio SGML eliminando al contempo la maggior parte della complessità possibile. Il formato XML è simile al formato HTML, ma mentre il formato HTML viene utilizzato

per fornire informazioni grafiche su un documento, il formato XML viene utilizzato per rappresentare i dati strutturati in un documento.

I clienti dei servizi avanzati di Cisco includono anche il server Cisco NATkit per attività aggiuntive di monitoraggio proattivo e risoluzione dei problemi. Il server NATkit disporrà di un accesso remoto tramite montaggio su disco (rmount) o protocollo di trasferimento file (FTP) ai dati che risiedono sul server CiscoWorks2000.

Il capitolo Network Management Basics di *Internetworking Technology Overview* fornisce una panoramica più dettagliata sulle nozioni di base della gestione della rete.

Gestione degli errori

L'obiettivo della gestione degli errori è quello di rilevare, registrare, notificare agli utenti e (per quanto possibile) risolvere automaticamente i problemi della rete per garantirne l'efficienza. Poiché gli errori possono causare downtime o un degrado inaccettabile della rete, la gestione degli errori è forse la più implementata tra gli elementi di gestione di rete ISO.

Piattaforme di gestione della rete

Una piattaforma di gestione di rete implementata nell'azienda gestisce un'infrastruttura costituita da elementi di rete multifornitore. La piattaforma riceve ed elabora gli eventi dagli elementi di rete nella rete. Gli eventi provenienti dai server e da altre risorse critiche possono inoltre essere inoltrati a una piattaforma di gestione. In una piattaforma di gestione standard sono incluse le seguenti funzioni comunemente disponibili:

- Individuazione rete
- Mappatura topologica di elementi di rete
- Gestore eventi
- Agente di raccolta e grafico dati prestazioni
- Browser dati di gestione

Le piattaforme di gestione della rete possono essere visualizzate come la console principale per le operazioni di rete nel rilevamento degli errori nell'infrastruttura. La capacità di rilevare rapidamente i problemi in qualsiasi rete è fondamentale. Il personale addetto alle operazioni di rete può utilizzare una mappa grafica della rete per visualizzare gli stati operativi degli elementi critici della rete, quali router e switch.

Le piattaforme di gestione della rete quali HP OpenView, Computer Associates Unicenter e SUN Solstice possono eseguire il rilevamento dei dispositivi di rete. Ogni dispositivo di rete è rappresentato da un elemento grafico sulla console della piattaforma di gestione. I diversi colori degli elementi grafici rappresentano lo stato operativo corrente dei dispositivi di rete. I dispositivi di rete possono essere configurati per l'invio di notifiche, chiamate trap SNMP, alle piattaforme di gestione di rete. Alla ricezione delle notifiche, l'elemento grafico che rappresenta il dispositivo di rete cambia di colore a seconda della gravità della notifica ricevuta. La notifica, generalmente denominata evento, viene inserita in un file di registro. È particolarmente importante che i file MIB (Cisco Management Information Base) più recenti vengano caricati sulla piattaforma SNMP per garantire che i vari avvisi provenienti dai dispositivi Cisco vengano interpretati correttamente.

Cisco pubblica i file MIB per la gestione di vari dispositivi di rete. I file MIB Cisco si trovano sul sito Web cisco.com e includono le seguenti informazioni:

- File MIB pubblicati in formato SNMPv1
- File MIB pubblicati in formato SNMPv2
- Trap SNMP supportate su dispositivi Cisco
- OID per gli oggetti MIB SNMP correnti Cisco

Diverse piattaforme di gestione della rete sono in grado di gestire più siti geograficamente distribuiti. A tale scopo, è necessario scambiare i dati di gestione tra le console di gestione di siti remoti con una stazione di gestione sul sito principale. Il vantaggio principale di un'architettura distribuita è la riduzione del traffico di gestione, che consente un utilizzo più efficiente della larghezza di banda. Un'architettura distribuita consente inoltre al personale di gestire localmente le reti da siti remoti con sistemi.

Un recente miglioramento alle piattaforme di gestione è la capacità di gestire in remoto gli elementi di rete utilizzando un'interfaccia Web. Questo miglioramento elimina la necessità di installare software client speciali sulle singole stazioni utente per accedere a una piattaforma di gestione.

Un'azienda tipica è composta da diversi elementi di rete. Tuttavia, per gestire in modo efficace gli elementi della rete, ogni dispositivo in genere richiede sistemi di gestione degli elementi specifici del fornitore. È pertanto possibile che stazioni di gestione duplicate eseguano il polling degli elementi di rete per le stesse informazioni. I dati raccolti da diversi sistemi vengono memorizzati in database separati, creando un sovraccarico amministrativo per gli utenti. Questa limitazione ha spinto i fornitori di reti e software ad adottare standard quali CORBA (Common Object Request Broker Architecture) e CIM (Computer-Integrated Manufacturing) per facilitare lo scambio di dati di gestione tra piattaforme di gestione e sistemi di gestione degli elementi. Con l'adozione di standard da parte dei fornitori per lo sviluppo dei sistemi di gestione, gli utenti possono aspettarsi l'interoperabilità e un risparmio sui costi nell'installazione e nella gestione dell'infrastruttura.

CORBA specifica un sistema che fornisce interoperabilità tra gli oggetti in un ambiente eterogeneo distribuito e in modo trasparente per il programmatore. Il progetto si basa sul modello a oggetti OMG (Object Management Group).

Infrastruttura di risoluzione dei problemi

I server TFTP (Trivial File Transfer Protocol) e syslog (System Log) sono componenti fondamentali di un'infrastruttura per la risoluzione dei problemi nelle operazioni di rete. Il server TFTP viene utilizzato principalmente per l'archiviazione dei file di configurazione e delle immagini software dei dispositivi di rete. I router e gli switch possono inviare messaggi di registro del sistema a un server syslog. I messaggi facilitano la funzione di risoluzione dei problemi in caso di problemi. A volte, il personale di supporto Cisco ha bisogno dei messaggi syslog per eseguire l'analisi della causa principale.

La funzione di raccolta syslog distribuito di CiscoWorks 2000 Resource Management Essentials (Essentials) consente la distribuzione di diverse stazioni di raccolta UNIX o NT nei siti remoti per la raccolta e il filtraggio dei messaggi. I filtri possono specificare quali messaggi syslog verranno inoltrati al server Essentials principale. Uno dei principali vantaggi dell'implementazione della raccolta distribuita è la riduzione dei messaggi inoltrati ai principali server syslog.

Rilevamento e notifica degli errori

Lo scopo della gestione degli errori è quello di rilevare, isolare, notificare e correggere gli errori rilevati nella rete. I dispositivi di rete sono in grado di avvisare le stazioni di gestione quando si

verifica un errore sui sistemi. Un sistema efficace di gestione dei guasti è costituito da diversi sottosistemi. Il rilevamento degli errori viene eseguito quando i dispositivi inviano messaggi trap SNMP, polling SNMP, soglie RMON (monitoraggio remoto) e messaggi syslog. Un sistema di gestione avvisa l'utente finale quando viene segnalato un guasto ed è possibile intraprendere azioni correttive.

Ènecessario attivare le registrazioni in modo coerente sui dispositivi di rete. Le nuove versioni del software Cisco IOS per router e switch supportano trap aggiuntive. È importante controllare e aggiornare il file di configurazione per garantire la corretta decodifica delle trap. L'analisi periodica delle trap configurate con il team Cisco Assured Network Services (ANS) assicura un rilevamento efficace dei guasti nella rete.

Nella tabella seguente vengono elencati i trap CISCO-STACK-MIB supportati dagli switch LAN (Local Area Network) Cisco Catalyst e che possono essere utilizzati per monitorare le condizioni di errore.

Trap	Descrizione
moduloSu	L'entità agente ha rilevato che l'oggetto **moduleStatus** in questo MIB è passato allo stato **ok(2)** per uno dei relativi moduli.
moduloGiù	L'entità agente ha rilevato che l'oggetto *moduleStatus* in questo MIB è passato dallo stato **ok(2)** per uno dei relativi moduli.
chassisAllarmeAttivato	L'entità agente ha rilevato che l'oggetto *chassisTempAlarm*, *chassisMinorAlarm* o *chassisMajorAlarm* in questo MIB è passato allo stato **on(2)**. Un *chassisMajorAlarm* indica che si è verificata una delle seguenti condizioni: • Qualsiasi guasto di tensione • Guasto simultaneo della temperatura e della ventola • Guasto al 100% dell'alimentatore (due su due o uno su uno) • Errore della memoria di sola lettura programmabile cancellabile elettricamente (EEPROM) • Errore della NVRAM (Nonvolatile RAM) • Errore di comunicazione MCP • Stato NMP sconosciuto Un oggetto chassisMinorAlarm indica che si verifica una delle seguenti condizioni: • Allarme temperatura • Guasto della ventola • Guasto parziale dell'alimentazione (uno su due) • Due alimentatori di tipo incompatibile
chassisAllarmeDisattivat	L'entità agente ha rilevato che l'oggetto *chassisTempAlarm*, *chassisMinorAlarm* o

o	*chassisMajorAlarm* in questo MIB è passato allo stato **off(1)**.

Le trap envmon (monitoraggio ambientale) sono definite in trappole CISCO-ENVMON-MIB. La trap envmon invia notifiche per il monitoraggio ambientale specifico dell'azienda Cisco quando viene superata una soglia ambientale. Quando si utilizza envmon, è possibile abilitare un tipo di trap ambientale specifico oppure accettare tutti i tipi di trap del sistema di monitoraggio ambientale. Se non viene specificata alcuna opzione, vengono attivati tutti i tipi di ambiente. Può corrispondere a uno o più dei valori seguenti:

- Voltaggio - Viene inviata una notifica ciscoEnvMonVoltageNotification se la tensione misurata in un determinato punto di test non rientra nel normale intervallo per il punto di test (come in fase di avviso, critico o di arresto).
- shutdown - Viene inviata una notifica ciscoEnvMonShutdownNotification se il monitoraggio ambientale rileva che un punto di test sta raggiungendo uno stato critico e sta per avviare un arresto.
- supply—In caso di guasto dell'alimentatore ridondante (se esistente), viene inviata una notifica di fornitura ciscoEnvMonRedundantSupplyNotification.
- fan—Viene inviata una notifica ciscoEnvMonFanNotification se una delle ventole nell'array di ventole (se presente) si guasta.
- temperatura—Viene inviata una notifica ciscoEnvMonTemperatureNotification se la temperatura misurata in un determinato punto di test non rientra nell'intervallo normale per il punto di test (ad esempio, in fase di avvertenza, critica o di arresto).

La rilevazione e il monitoraggio degli errori degli elementi di rete possono essere estesi dal livello del dispositivo a quello del protocollo e dell'interfaccia. In un ambiente di rete, il monitoraggio degli errori può includere VLAN (Virtual Local Area Network), ATM (asynchronous transfer mode), indicazioni di errore sulle interfacce fisiche e così via. L'implementazione della gestione degli errori a livello di protocollo è disponibile utilizzando un sistema di gestione degli elementi come CiscoWorks 2000 Campus Manager. L'applicazione TrafficDirector in Campus Manager è incentrata sulla gestione dello switch tramite il supporto mini-RMON sugli switch Catalyst.

Con un numero crescente di elementi di rete e la complessità dei problemi di rete, è possibile prendere in considerazione un sistema di gestione degli eventi in grado di correlare diversi eventi di rete (syslog, trap, file di registro). Questa architettura alla base di un sistema di gestione degli eventi è paragonabile a un sistema di gestione dei manager (MOM). Un sistema di gestione degli eventi ben progettato consente al personale del centro operativo di rete di essere proattivo ed efficace nel rilevare e diagnosticare i problemi di rete. La definizione delle priorità e la soppressione degli eventi consentono al personale addetto alle operazioni di rete di concentrarsi su eventi di rete critici, di esaminare diversi sistemi di gestione degli eventi, tra cui Cisco Info Center, e di condurre un'analisi di fattibilità per esplorare appieno le funzionalità di tali sistemi. Per ulteriori informazioni, visitare il Cisco Info Center.

Monitoraggio proattivo degli errori e notifica

Gli allarmi e gli eventi RMON sono due gruppi definiti nella specifica RMON. In genere, una stazione di gestione esegue il polling sui dispositivi di rete per determinare lo stato o il valore di determinate variabili. Ad esempio, una stazione di gestione esegue il polling di un router per individuare l'utilizzo della CPU e generare un evento quando il valore raggiunge una soglia configurata. Questo metodo spreca larghezza di banda della rete e può anche non raggiungere la soglia effettiva a seconda dell'intervallo di polling.

Con gli eventi e gli allarmi RMON, un dispositivo di rete è configurato in modo da monitorare se stesso alla ricerca di soglie in aumento e in diminuzione. A un intervallo di tempo predefinito, il dispositivo di rete preleva un campione di una variabile e lo confronta con le soglie. Una trap SNMP può essere inviata a una stazione di gestione se il valore effettivo supera o scende al di sotto delle soglie configurate. I gruppi di allarme e di eventi RMON forniscono un metodo proattivo di gestione dei dispositivi di rete critici.

Cisco Systems consiglia di implementare gli eventi e gli allarmi RMON sui dispositivi di rete critici. Le variabili monitorate possono includere l'utilizzo della CPU, errori del buffer, interruzioni di input/output o qualsiasi variabile di tipo Integer. A partire dal software Cisco IOS versione 11.1(1), tutte le immagini del router supportano i gruppi di eventi e di allarmi RMON.

Per informazioni dettagliate sull'implementazione di eventi e allarmi RMON, consultare la sezione Implementazione di eventi e allarmi RMON.

Vincoli di memoria RMON

L'utilizzo della memoria RMON è costante su tutte le piattaforme di switch in relazione a statistiche, storie, allarmi ed eventi. RMON utilizza un *bucket* per archiviare cronologie e statistiche sull'agente RMON (che in questo caso è lo switch). Le dimensioni del bucket vengono definite sulla sonda RMON (dispositivo SwitchProbe) o sull'applicazione RMON (strumento TrafficDirector), quindi inviate allo switch da impostare.

Per supportare i comandi mini-RMON, sono necessari circa 450 K di spazio di codice (ad esempio, quattro gruppi RMON: statistiche, cronologia, allarmi ed eventi). I requisiti di memoria dinamica per RMON variano perché dipendono dalla configurazione del runtime.

Nella tabella seguente vengono definite le informazioni sull'utilizzo della memoria RMON di runtime per ogni gruppo di minidischi RMON.

Definizione gruppo RMON	Spazio DRAM utilizzato	Note
Statistiche	140 byte per porta Ethernet/Fast Ethernet commutata	Per porta
Cronologia	3,6 K per 50 bucket *	Ogni bucket aggiuntivo utilizza 56 byte
Allarmi ed eventi	2,6 K per allarme e corrispondenti voci di evento	Per allarme per porta

*RMON utilizza un *bucket* per memorizzare cronologie e statistiche sull'agente RMON (come un interruttore).

Implementazione di eventi e allarmi RMON

Incorporando RMON come parte di una soluzione di fault management, un utente può monitorare proattivamente la rete prima che si verifichi un potenziale problema. Ad esempio, se il numero di pacchetti di broadcast ricevuti aumenta in modo significativo, l'utilizzo della CPU potrebbe

aumentare. Implementando un evento e un allarme RMON, un utente può impostare una soglia per monitorare il numero di pacchetti broadcast ricevuti e avvisare la piattaforma SNMP tramite una trap SNMP se viene raggiunta la soglia configurata. Gli allarmi e gli eventi RMON eliminano il polling eccessivo normalmente eseguito dalla piattaforma SNMP per raggiungere lo stesso obiettivo.

Sono disponibili due metodi per configurare gli eventi e gli allarmi RMON:

- Interfaccia della riga di comando (CLI)
- SET SNMP

Le procedure di esempio seguenti mostrano come impostare una soglia per monitorare il numero di pacchetti broadcast ricevuti su un'interfaccia. In queste procedure viene utilizzato lo stesso contatore mostrato nell'esempio del comando **show interface** alla fine di questa sezione.

Esempio di interfaccia della riga di comando

Per implementare gli eventi e gli allarmi RMON utilizzando l'interfaccia CLI, attenersi alla seguente procedura:

1. Trovare l'indice di interfaccia associato a Ethernet 0 percorrendo il 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. Ottenere l'OID associato al campo CLI da monitorare. Per questo esempio, l'OID per 'broadcasts' è 1.3.6.1.2.1.2.2.1.12. Gli OID Cisco per specifiche variabili MIB sono disponibili sul sito Web cisco.com.
3. Determinare i seguenti parametri per l'impostazione di soglie ed eventi.soglie crescenti e decrescentitipo di campionamento (assoluto o delta)intervallo di campionamentoazione al raggiungimento della sogliaPer questo esempio, è in corso l'impostazione di una soglia per monitorare il numero di pacchetti broadcast ricevuti su Ethernet 0. Se il numero di pacchetti broadcast ricevuti è maggiore di 500 tra campioni di 60 secondi, verrà generata una trap. La soglia viene riattivata quando il numero di trasmissioni in entrata non aumenta tra i campioni acquisiti.**Nota:** Per informazioni dettagliate su questi parametri dei comandi, consultare la documentazione di Cisco Connection Online (CCO) per i comandi di allarme e di evento RMON per la specifica versione di Cisco IOS.
4. Specificare la trap inviata (evento RMON) quando si raggiunge la soglia utilizzando i seguenti comandi CLI (i comandi Cisco IOS sono visualizzati in grassetto):**rmon evento 1 trap gateway descrizione "High Broadcast on Ethernet 0" proprietario ciscormon event 2 descrizione registro "normal broadcast received on ethernet 0" proprietario di cisco**
5. Specificare le soglie e i parametri rilevanti (allarme RMON) utilizzando i seguenti comandi CLI:**rmon alarm 1 ifEntry.12.1 60 delta 500 1soglia di caduta 0 2 proprietario cisco**
6. Utilizzare SNMP per eseguire il polling di queste tabelle per verificare che le voci eventTable siano state create sul 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. Usare SNMP per eseguire il polling di queste tabelle per verificare che le voci alarmTable siano state impostate.

```
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)
```

Esempio di set di SNMP

Per implementare gli eventi e gli allarmi RMON con l'operazione SNMP SET, attenersi alla seguente procedura:

1. Specificare la trap inviata (evento RMON) quando viene raggiunta la soglia utilizzando le seguenti operazioni SET di 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. Specificare le soglie e i parametri pertinenti (allarme RMON) utilizzando le seguenti operazioni 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. Eseguire il polling di queste tabelle per verificare che le voci eventTable siano state create nel 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. Eseguire il polling di queste tabelle per verificare che le voci alarmTable siano state impostate.
```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1
```

show interface

L'esempio è il risultato del 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
```

Gestione della configurazione

L'obiettivo della gestione della configurazione è monitorare le informazioni sulla configurazione della rete e del sistema in modo da poter tenere traccia e gestire gli effetti sul funzionamento della rete di diverse versioni di elementi hardware e software.

Standard di configurazione

Con un numero crescente di dispositivi di rete installati, è fondamentale essere in grado di identificare con precisione la posizione di un dispositivo di rete. Queste informazioni sulla posizione devono fornire una descrizione dettagliata significativa per coloro che devono inviare risorse quando si verifica un problema di rete. Per accelerare la risoluzione di un problema di rete, assicurarsi di avere a disposizione le informazioni di contatto della persona o dell'ufficio responsabili dei dispositivi. Le informazioni di contatto devono includere il numero di telefono e il nome della persona o dell'ufficio.

Le convenzioni di denominazione per i dispositivi di rete, a partire dal nome del dispositivo fino alla singola interfaccia, devono essere pianificate e implementate come parte dello standard di configurazione. Una convenzione di denominazione ben definita consente al personale di fornire informazioni accurate durante la risoluzione dei problemi di rete. La convenzione di denominazione per i dispositivi può utilizzare la posizione geografica, il nome dell'edificio, il piano

e così via. Per la convenzione di denominazione dell'interfaccia, può includere il segmento a cui è connessa una porta, il nome dell'hub di connessione e così via. Sulle interfacce seriali, deve includere la larghezza di banda effettiva, il numero DLCI (Local Data Link Identifier) (se Frame Relay), la destinazione e l'ID del circuito o le informazioni fornite dal vettore.

Gestione dei file di configurazione

Quando si aggiungono nuovi comandi di configurazione alle esigenze dei dispositivi di rete esistenti, è necessario verificare l'integrità dei comandi prima di eseguire l'implementazione effettiva. Un dispositivo di rete configurato in modo errato può avere un effetto disastroso sulla connettività e sulle prestazioni della rete. I parametri del comando di configurazione devono essere controllati per evitare incompatibilità o mancata corrispondenza. Si consiglia di pianificare un esame approfondito delle configurazioni con i tecnici Cisco su base regolare.

Il software CiscoWorks 2000 Essentials è completamente funzionale e consente di eseguire automaticamente il backup dei file di configurazione sui router e sugli switch Cisco Catalyst. La funzionalità di protezione di Essentials può essere utilizzata per eseguire l'autenticazione sulle modifiche alla configurazione. È disponibile un registro di controllo delle modifiche per tenere traccia delle modifiche e del nome utente degli utenti che eseguono le modifiche. Per le modifiche alla configurazione su più dispositivi, sono disponibili due opzioni: NetConfig basato sul Web nella versione corrente di CiscoWorks 2000 Essentials o nello script **cwconfig**. I file di configurazione possono essere scaricati e caricati utilizzando CiscoWorks 2000 Essentials con i modelli predefiniti o definiti dall'utente.

Per eseguire queste funzioni è possibile utilizzare gli strumenti di gestione della configurazione di CiscoWorks 2000 Essentials:

- Eseguire il push dei file di configurazione dall'archivio di configurazione Essentials a uno o più dispositivi
- Pull della configurazione dal dispositivo all'archivio Essentials
- Estrarre la configurazione più recente dall'archivio e scriverla in un file
- Importa la configurazione da un file ed esegue il push della configurazione nei dispositivi
- Confronta le ultime due configurazioni nell'archivio Essentials
- Elimina dall'archivio le configurazioni precedenti a una data o a una versione specificata
- Copiare la configurazione di avvio nella configurazione in esecuzione

Gestione inventario

La funzione di rilevamento della maggior parte delle piattaforme di gestione della rete ha lo scopo di fornire un elenco dinamico dei dispositivi presenti nella rete. È consigliabile utilizzare motori di individuazione, come quelli implementati nelle piattaforme di gestione di rete.

Un database di inventario fornisce informazioni dettagliate sulla configurazione dei dispositivi di rete. Le informazioni comuni includono modelli di hardware, moduli installati, immagini software, livelli di microcodice e così via. Tutte queste informazioni sono fondamentali per il completamento di attività quali la manutenzione di software e hardware. L'elenco aggiornato dei dispositivi di rete raccolti dal processo di rilevamento può essere utilizzato come elenco principale per raccogliere informazioni di inventario utilizzando SNMP o script. È possibile importare un elenco di dispositivi da CiscoWorks 2000 Campus Manager nel database di inventario di CiscoWorks 2000 Essentials per ottenere un inventario aggiornato degli switch Cisco Catalyst.

Gestione software

Per un aggiornamento corretto delle immagini Cisco IOS sui dispositivi di rete, è necessaria un'analisi dettagliata di requisiti quali memoria, ROM di avvio, livello di microcodice e così via. I requisiti sono normalmente documentati e disponibili sul sito Web di Cisco sotto forma di note sulla versione e guide all'installazione. Il processo di aggiornamento di un dispositivo di rete con Cisco IOS include il download di un'immagine corretta da CCO, il backup dell'immagine corrente, la verifica che tutti i requisiti hardware siano soddisfatti e quindi il caricamento della nuova immagine nel dispositivo.

La finestra di aggiornamento per completare la manutenzione del dispositivo è abbastanza limitata per alcune organizzazioni. In un ambiente di rete di grandi dimensioni con risorse limitate, potrebbe essere necessario pianificare e automatizzare gli aggiornamenti del software dopo l'orario di lavoro. La procedura può essere completata utilizzando un linguaggio di script quale Expect o un'applicazione scritta appositamente per eseguire tale operazione.

Le modifiche al software nei dispositivi di rete, come le immagini Cisco IOS e le versioni del microcodice, devono essere registrate per essere utili nella fase di analisi quando è necessaria un'altra manutenzione del software. Grazie a un rapporto sulla cronologia delle modifiche facilmente disponibile, l'utente che esegue l'aggiornamento può ridurre al minimo il rischio di caricare immagini o microcodici incompatibili nei dispositivi di rete.

Gestione delle prestazioni

Contratto di servizio

Un accordo sui livelli di servizio (SLA, Service Level Agreement) è un accordo scritto tra un provider di servizi e i loro clienti sul livello di prestazioni previsto dei servizi di rete. Lo SLA è costituito da metriche concordate tra il fornitore e i clienti. I valori impostati per le metriche devono essere realistici, significativi e misurabili per entrambe le parti.

Èpossibile raccogliere diverse statistiche di interfaccia dai dispositivi di rete per misurare il livello delle prestazioni. Queste statistiche possono essere incluse come metriche nello SLA. Statistiche quali i rilasci delle code di input, i rilasci delle code di output e i pacchetti ignorati sono utili per la diagnosi di problemi relativi alle prestazioni.

A livello di dispositivo, le metriche delle prestazioni possono includere l'utilizzo della CPU, l'allocazione del buffer (buffer grande, buffer medio, accessi non riusciti, rapporto di accesso) e l'allocazione della memoria. Le prestazioni di alcuni protocolli di rete sono direttamente correlate alla disponibilità di buffer nei dispositivi di rete. La misurazione delle statistiche delle prestazioni a livello di dispositivo è fondamentale per ottimizzare le prestazioni dei protocolli di livello superiore.

I dispositivi di rete, ad esempio i router, supportano vari protocolli di livello superiore, ad esempio DLSW (Data Link Switching Workgroup), RSRB (Remote Source Route Bridging), AppleTalk e così via. È possibile monitorare e raccogliere statistiche sulle prestazioni delle tecnologie WAN (Wide-Area Network), tra cui Frame Relay, ATM, ISDN (Integrated Services Digital Network) e altre.

Monitoraggio, misurazione e reporting delle prestazioni

Utilizzando il protocollo SNMP è necessario raccogliere regolarmente metriche delle prestazioni

diverse a livello di interfaccia, dispositivo e protocollo. Il motore di polling in un sistema di gestione di rete può essere utilizzato per la raccolta dei dati. La maggior parte dei sistemi di gestione della rete è in grado di raccogliere, archiviare e presentare dati sottoposti a polling.

Sul mercato sono disponibili diverse soluzioni per soddisfare le esigenze di gestione delle prestazioni per gli ambienti aziendali. Questi sistemi sono in grado di raccogliere, archiviare e presentare dati da dispositivi di rete e server. L'interfaccia basata sul Web della maggior parte dei prodotti rende accessibili i dati sulle prestazioni da qualsiasi punto dell'azienda. Alcune delle soluzioni di gestione delle prestazioni più diffuse includono:

- Vista di InfoVista
- Visione del servizio IT SAS
- Trinagy TREND

Una valutazione dei prodotti di cui sopra determinerà se soddisfano le esigenze dei diversi utenti. Alcuni fornitori supportano l'integrazione con le piattaforme di gestione di rete e di sistema. Ad esempio, InfoVista supporta l'agente di pattuglia BMC per fornire statistiche chiave sulle prestazioni dai server applicazioni. Ogni prodotto ha un modello di prezzo e funzionalità differenti con l'offerta di base. Il supporto per le funzionalità di gestione delle prestazioni per i dispositivi Cisco come NetFlow, RMON e Cisco IOS Service Assurance Agent/Response Time Reporter (RTR/SAA CSAA/RTR) è disponibile su alcune soluzioni. Concord ha recentemente aggiunto il supporto per gli switch WAN di Cisco che può essere utilizzato per raccogliere e visualizzare i dati sulle prestazioni.

La funzionalità CSA/RTR Service Assurance Agent (SAA)/Response Time Reporter (RTR) di Cisco IOS può essere utilizzata per misurare il tempo di risposta tra i dispositivi IP. Un router di origine configurato con CSA configurato è in grado di misurare il tempo di risposta a un dispositivo IP di destinazione che può essere un router o un dispositivo IP. Il tempo di risposta può essere misurato tra l'origine e la destinazione o per ciascun hop sul percorso. Le trap SNMP possono essere configurate per avvisare le console di gestione se il tempo di risposta supera le soglie predefinite.

I recenti miglioramenti apportati a Cisco IOS estendono le funzionalità di CSA per misurare quanto segue:

- Prestazioni del servizio HTTP (HyperText Transfer Protocol)Ricerca DNS (Domain Name System)Connessione TCP (Transmission Control Protocol)Ora transazione HTTP
- Variazione del ritardo tra pacchetti (jitter) del traffico Voice over IP (VoIP)
- Tempo di risposta tra gli endpoint per una qualità del servizio (QoS) specificaBit IP type of service (ToS)
- Perdita di pacchetti usando pacchetti generati da CSA

Per configurare la funzione CSA sui router, è possibile usare l'applicazione Cisco Internetwork Performance Monitor (IPM). Il CSAA/RTR è incorporato in molte ma non in tutte le funzionalità del software Cisco IOS. Sul dispositivo utilizzato da IPM per raccogliere le statistiche sulle prestazioni deve essere installata una versione del software Cisco IOS che supporti CSAA/RTR. Per un riepilogo delle versioni di Cisco IOS che supportano CSA/RTR/IPM, visitare il sito Web delle domande frequenti su IPM.

Ulteriori informazioni su IPM includono:

- Panoramica di IPM
- Service Assurance Agent

Analisi e tuning delle prestazioni

Il traffico degli utenti è aumentato in modo significativo e ha aumentato la domanda di risorse di rete. I gestori di rete in genere dispongono di una visualizzazione limitata dei tipi di traffico in esecuzione nella rete. La profilatura del traffico di utenti e applicazioni fornisce una visualizzazione dettagliata del traffico nella rete. Due tecnologie, le sonde RMON e NetFlow, offrono la possibilità di raccogliere profili di traffico.

RMON

Gli standard RMON sono progettati per essere implementati in un'architettura distribuita in cui gli agenti (sia incorporati che in sonde standalone) comunicano con una stazione centrale (la console di gestione) tramite SNMP. Lo standard RFC 1757 RMON organizza le funzioni di monitoraggio in nove gruppi per supportare le topologie Ethernet e aggiunge un decimo gruppo nella RFC 1513 per i parametri univoci di Token Ring. Il monitoraggio del collegamento Fast Ethernet è fornito nell'ambito dello standard RFC 1757 e il monitoraggio degli anelli FDDI (Fiber-Distributed Data Interface) è fornito nell'ambito della RFC 1757 e della RFC 1513.

La nuova specifica RFC 2021 RMON guida gli standard di monitoraggio remoto oltre il livello MAC (Media Access Control) a livello di rete e di applicazione. Questa configurazione consente agli amministratori di analizzare e risolvere i problemi relativi alle applicazioni di rete, ad esempio traffico Web, NetWare, Notes, e-mail, accesso al database, NFS (Network File System) e altri. Gli allarmi, le statistiche, la cronologia e i gruppi host/conversazione RMON possono ora essere utilizzati per monitorare e mantenere proattivamente la disponibilità della rete in base al traffico a livello di applicazione, ovvero il traffico più critico della rete. RMON2 consente agli amministratori di rete di continuare a implementare soluzioni di monitoraggio basate su standard per supportare applicazioni mission critical basate su server.

Nelle tabelle seguenti sono elencate le funzioni dei gruppi RMON.

RMON Group (RFC 1757)	Funzione
Statistiche	Contatori per pacchetti, ottetti, trasmissioni, errori e offerte sul segmento o sulla porta.
Cronologia	Esegue periodicamente il campionamento e il salvataggio dei contatori dei gruppi di statistiche per il successivo recupero.
Host	Gestisce le statistiche su ciascun dispositivo host sul segmento o sulla porta.
Host Top N	Un subset definito dall'utente del gruppo Hosts, ordinato in base a un contatore statistico. Restituendo solo i risultati, il traffico di gestione viene ridotto al minimo.
Matrice traffico	Gestisce le statistiche di conversazione tra gli host della rete.

Allarmi	Una soglia che può essere impostata su variabili RMON critiche per la gestione proattiva.
Eventi	Genera trap SNMP e voci di log quando viene superata la soglia di un gruppo di allarmi.
Acquisizione pacchetti	Gestisce i buffer per i pacchetti acquisiti dal gruppo Filter per il caricamento nella console di gestione.
Token Ring	Stazione ad anello—statistiche dettagliate sulle singole stazioni Ordine delle stazioni ad anello—un elenco ordinato delle stazioni attualmente nella configurazione della stazione ad anello—configurazione e inserimento/rimozione per stazione Instradamento sorgente—statistiche sull'instradamento sorgente, come il numero di hop, e altre

RMON2	Funzione
Directory di protocollo	Protocolli per i quali l'agente controlla e gestisce le statistiche.
Distribuzione protocollo	Statistiche per ogni protocollo.
Host livello rete	Statistiche per ogni indirizzo di livello rete sul segmento, anello o porta.
Network Layer Matrix	Statistiche del traffico per coppie di indirizzi del livello di rete.
Host livello applicazione	Statistiche per protocollo del livello applicazione per ogni indirizzo di rete.
Matrice livello applicazione	Statistiche sul traffico per protocollo del livello applicazione per coppie di indirizzi del livello rete.
Cronologia definibile dall'utente	Estende la cronologia oltre le statistiche dei livelli di collegamento RMON1 per includere qualsiasi statistica RMON, RMON2, MIB-I o MIB-II.
Mapping indirizzi	Associazioni di indirizzi da MAC a livello di rete.
Gruppo di configura	Capacità e configurazioni degli agenti.

zione	

NetFlow

La funzione Cisco NetFlow consente di raccogliere statistiche dettagliate sui flussi di traffico per la pianificazione della capacità, la fatturazione e la risoluzione dei problemi. NetFlow può essere configurato su singole interfacce, fornendo informazioni sul traffico che passa attraverso queste interfacce. Le statistiche dettagliate sul traffico comprendono i seguenti tipi di informazioni:

- Indirizzi IP di origine e di destinazione
- Numeri di interfaccia di input e output
- Porta di origine e di destinazione TCP/UDP
- Numero di byte e pacchetti nel flusso
- Numeri di sistema autonomi di origine e destinazione
- ToS (IP type of service)

I dati NetFlow raccolti sui dispositivi di rete vengono esportati in un dispositivo di raccolta. L'agente di raccolta esegue funzioni quali la riduzione del volume dei dati (filtraggio e aggregazione), la memorizzazione gerarchica dei dati e la gestione dei file system. Cisco fornisce NetFlow Collector e le applicazioni NetFlow Analyzer per la raccolta e l'analisi dei dati dai router e dagli switch Cisco Catalyst. Sono inoltre disponibili strumenti shareware, ad esempio cflowd, in grado di raccogliere i record UDP (User Datagram Protocol) di Cisco NetFlow.

I dati NetFlow vengono trasportati utilizzando pacchetti UDP in tre formati diversi:

- Versione 1 - Il formato originale supportato nelle release iniziali di NetFlow.
- Versione 5—Una versione successiva che ha aggiunto le informazioni di sistema autonome Border Gateway Protocol (BGP) e i numeri di sequenza del flusso.
- Versione 7—Un miglioramento ancora più recente che ha aggiunto il supporto della commutazione NetFlow per gli switch Cisco Catalyst serie 5000 dotati di una NetFlow Feature Card (NFC).

Le versioni da 2 a 4 e la versione 6 non sono state rilasciate o non sono supportate da FlowCollector. In tutte e tre le versioni, il datagramma è costituito da un'intestazione e da uno o più record di flusso.

Per ulteriori informazioni, consultare il white paper NetFlow Services Solutions Guide.

La tabella seguente illustra le versioni supportate di Cisco IOS per la raccolta dei dati NetFlow dai router e dagli switch Catalyst.

Per preparare questo documento, è stato utilizzato Cisco IOS Software Release	Piattaforme hardware Cisco supportate	Versioni esportate NetFlow supportate
11.1 CA e 11.1 CC	Cisco 7200, 7500 e RSP7000	V1 e V5
11.2 e 11.2 P	Cisco 7200,	V1

	7500 e RSP7000	
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 versioni successive	Cisco 1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR7200, 7500, RSP7000,	V1, V5 e V8

	RSM, MGX8800 RPM e BPX 8650	
12.0(6)S	Cisco 12000	V1, V5 e V8
—	Cisco Catalyst 5000 con NetFlow Feature Card (NFC)***	V7

* Il supporto per NetFlow Export V1, V5 e V8 sulle piattaforme Cisco 1600 e 2500 è destinato al software Cisco IOS versione 12.0(T). Il supporto NetFlow per queste piattaforme non è disponibile nella versione principale di Cisco IOS 12.0.

** Il supporto per NetFlow V1, V5 e V8 sulla piattaforma AS5300 è destinato al software Cisco IOS versione 12.06(T).

*** L'esportazione dei dati MLS e NetFlow è supportata nel software Catalyst serie 5000 supervisor engine versione 4.1(1) o successive.

Gestione della sicurezza

L'obiettivo della gestione della sicurezza è controllare l'accesso alle risorse di rete in base alle linee guida locali, in modo che la rete non possa essere sabotata (intenzionalmente o meno). Un sottosistema di gestione della sicurezza, ad esempio, può monitorare gli utenti che accedono a una risorsa di rete, rifiutando l'accesso a coloro che immettono codici di accesso non appropriati. La gestione della sicurezza è un tema molto ampio; pertanto, quest'area del documento copre solo la sicurezza relativa a SNMP e alla sicurezza di accesso di base ai dispositivi.

Informazioni dettagliate sulla sicurezza avanzata includono:

- Aumento della sicurezza sulle reti IP
- OpenSystem

Una buona implementazione della gestione della sicurezza inizia con l'implementazione di politiche e procedure di sicurezza valide. È importante creare uno standard minimo di configurazione specifico per la piattaforma per tutti i router e gli switch che seguono le best practice del settore per la sicurezza e le prestazioni.

Esistono diversi metodi per controllare l'accesso sui router e sugli switch Catalyst Cisco. Alcuni di questi metodi includono:

- Access Control Lists (ACL)
- ID utente e password locali per il dispositivo
- TACACS (Terminal Access Controller Access Control System)

TACACS è un protocollo di sicurezza standard della Internet Engineering Task Force (RFC 1492) eseguito tra dispositivi client su una rete e su un server TACACS. TACACS è un meccanismo di

autenticazione utilizzato per autenticare l'identità di un dispositivo che richiede l'accesso remoto a un database con privilegi. Le variazioni di TACACS includono TACACS+, l'architettura AAA che separa le funzioni di autenticazione, autorizzazione e contabilità.

TACACS+ viene utilizzato da Cisco per consentire un controllo più preciso sugli utenti che possono accedere al dispositivo Cisco in modalità non privilegiata e privilegiata. È possibile configurare più server TACACS+ per la tolleranza di errore. Con TACACS+ abilitato, il router e lo switch richiedono un nome utente e una password. L'autenticazione può essere configurata per il controllo dell'accesso o per autenticare singoli comandi.

Autenticazione

L'autenticazione è il processo di identificazione degli utenti, che include la finestra di dialogo di accesso e password, la richiesta di verifica e risposta e il supporto della messaggistica. L'autenticazione è il modo in cui un utente viene identificato prima di poter accedere al router o allo switch. Esiste una relazione fondamentale tra autenticazione e autorizzazione. Maggiore è il numero di privilegi di autorizzazione che un utente riceve, maggiore è il livello di autenticazione.

Authorization

L'autorizzazione fornisce il controllo dell'accesso remoto, incluse l'autorizzazione unica e l'autorizzazione per ogni servizio richiesto dall'utente. Su un router Cisco, l'intervallo del livello di autorizzazione per gli utenti è compreso tra 0 e 15, dove 0 corrisponde al livello più basso e 15 al livello più alto.

Contabilità

L'accounting consente di raccogliere e inviare le informazioni di protezione utilizzate per la fatturazione, la verifica e la creazione di report, ad esempio le identità degli utenti, gli orari di inizio e fine e i comandi eseguiti. L'accounting consente ai manager di rete di tenere traccia dei servizi a cui gli utenti accedono nonché della quantità di risorse di rete utilizzate.

Nella tabella seguente vengono elencati alcuni comandi di esempio di base per l'utilizzo di TACACS+, autenticazione, autorizzazione e accounting su un router Cisco e uno switch Catalyst. Per ulteriori informazioni sui comandi, consultare il documento Comandi di autenticazione, autorizzazione e accounting.

Comando Cisco IOS	Scopo
Router	
aaa new-model	Abilitare Autenticazione, Autorizzazione, Contabilità (AAA) come metodo principale per il controllo degli accessi.
{*system*} di accounting AAA / *rete | connessione | exec | livello comando*} {*start-stop | avvio in attesa | stop-only*}	Abilitare l'accounting con i comandi di configurazione globale.

{*tacacs+	raggio*}	
TACACS+ predefinito per l'accesso con autenticazione AAA	Configurare il router in modo che le connessioni a qualsiasi linea terminale configurata con l'impostazione predefinita di accesso vengano autenticate con TACACS+ e non possano essere eseguite se l'autenticazione non riesce per qualsiasi motivo.
AAA authorization exec default tacacs+ none	Configurare il router per verificare se all'utente è consentito eseguire una shell in modalità di esecuzione chiedendo conferma al server TACACS+.
indirizzo ip *server tacacs+* host *tacacs*	Specificare il server TACACS+ che verrà utilizzato per l'autenticazione con i comandi di configurazione globale.
chiave tacacs-server *shared-secret*	Specificare il segreto condiviso noto dai server TACACS+ e dal router Cisco con il comando di configurazione globale.
Catalyst Switch	
set authentication login tacacs enable [*all] console		http	telnet*] [*primario*]	Abilitare l'autenticazione TACACS+ per la modalità di accesso normale. Usare le parole chiave console o Telnet per abilitare TACACS+ solo per i tentativi di connessione alla porta console o Telnet.
set authorization exec enable {*opzione} opzione di fallback*} [*console	telnet	entrambi*]	Abilitare l'autorizzazione per la modalità di accesso normale. Utilizzare le parole chiave console o Telnet per abilitare l'autorizzazione solo per i tentativi di connessione tramite porta console o Telnet.
Imposta chiave tacacs-server *shared-secret*	Specificare il segreto condiviso noto ai server e allo switch TACACS+.
Impostare l'*indirizzo IP del server TACACS+* host *TACACS+*	Specificare il server TACACS+ che verrà utilizzato per l'autenticazione con i comandi di configurazione globale.
Imposta i comandi di accounting per abilitare {*config	all*} {*stop-only*} *tacacs+*	Abilita l'accounting dei comandi di configurazione.

Per ulteriori informazioni su come configurare il server AAA per monitorare e controllare l'accesso all'interfaccia della riga di comando sugli switch LAN aziendali Catalyst, consultare il documento

sul controllo dell'accesso allo switch tramite autenticazione, autorizzazione e accounting.

SNMP Security

Il protocollo SNMP può essere usato per apportare modifiche alla configurazione sui router e sugli switch Catalyst simili a quelle emesse dalla CLI. È necessario configurare misure di sicurezza appropriate sui dispositivi di rete per impedire l'accesso non autorizzato e la modifica tramite SNMP. Le stringhe della community devono seguire le linee guida standard per le password in termini di lunghezza, caratteri e difficoltà di indovinazione. è importante modificare le stringhe della community dai default pubblici e privati.

Tutti gli host di gestione SNMP devono disporre di un indirizzo IP statico e disporre esplicitamente dei diritti di comunicazione SNMP con il dispositivo di rete in base all'indirizzo IP e all'elenco di controllo di accesso (ACL) predefiniti. I software Cisco IOS e Cisco Catalyst offrono funzionalità di sicurezza che garantiscono che solo le stazioni di gestione autorizzate siano autorizzate a eseguire modifiche sui dispositivi di rete.

Funzioni di sicurezza dei router

Livello di privilegio SNMP

Questa funzione limita i tipi di operazioni che una stazione di gestione può eseguire su un router. Esistono due tipi di livello di privilegio sui router: Read-Only (RO) e Read-Write (RW). Il livello RO consente solo a una stazione di gestione di eseguire query sui dati del router. Non consente l'esecuzione di comandi di configurazione come il riavvio di un router e lo spegnimento delle interfacce. Per eseguire queste operazioni è possibile utilizzare solo il livello di privilegio RW.

SNMP Access Control List (ACL)

La funzione ACL SNMP può essere utilizzata insieme alla funzione di privilegio SNMP per impedire a specifiche stazioni di gestione di richiedere informazioni di gestione ai router.

SNMP View

Questa funzione limita le informazioni specifiche che possono essere recuperate dai router dalle stazioni di gestione. Può essere utilizzato con il livello di privilegio SNMP e le funzionalità ACL per imporre l'accesso limitato ai dati da parte delle console di gestione. Per gli esempi di configurazione della visualizzazione SNMP, passare alla visualizzazione snmp-server.

SNMP versione 3

L'SNMP versione 3 (SNMPv3) garantisce scambi sicuri di dati di gestione tra dispositivi di rete e stazioni di gestione. Le funzionalità di crittografia e autenticazione di SNMPv3 garantiscono un'elevata sicurezza nel trasporto dei pacchetti a una console di gestione. Il protocollo SNMPv3 è supportato nel software Cisco IOS versione 12.0(3)T e successive. Per una panoramica tecnica di SNMPv3, consultare la documentazione di SNMPv3.

Access Control List (ACL) sulle interfacce

La funzionalità ACL fornisce misure di sicurezza per prevenire attacchi come lo spoofing IP. L'ACL può essere applicato alle interfacce in entrata o in uscita sui router.

Funzione di sicurezza Catalyst LAN Switch

Elenco autorizzazioni IP

La funzionalità Elenco autorizzazioni IP limita l'accesso Telnet e SNMP in entrata allo switch da indirizzi IP di origine non autorizzati. I messaggi Syslog e le trap SNMP sono supportati per notificare a un sistema di gestione quando si verifica una violazione o un accesso non autorizzato.

Èpossibile usare una combinazione delle funzionalità di sicurezza di Cisco IOS per gestire i router e gli switch Catalyst. È necessario stabilire una policy di sicurezza che limiti il numero di stazioni di gestione in grado di accedere agli switch e ai router.

Per ulteriori informazioni su come aumentare la sicurezza sulle reti IP, vedere Aumento della sicurezza sulle reti IP.

Gestione contabile

La gestione contabile è il processo utilizzato per misurare i parametri di utilizzo della rete in modo che gli utenti singoli o di gruppo sulla rete possano essere regolati in modo appropriato ai fini della contabilità o del chargeback. Analogamente alla gestione delle prestazioni, il primo passo verso una gestione contabile appropriata consiste nel misurare l'utilizzo di tutte le risorse di rete importanti. L'utilizzo delle risorse di rete può essere misurato utilizzando le funzionalità di Cisco NetFlow e Cisco IP Accounting. L'analisi dei dati raccolti tramite questi metodi fornisce informazioni dettagliate sui modelli di utilizzo correnti.

Un sistema di contabilità e fatturazione basato sull'uso è una parte essenziale di qualsiasi accordo sui livelli di servizio (SLA). Esso fornisce sia un modo pratico per definire gli obblighi derivanti da uno SLA sia chiare conseguenze per un comportamento non conforme ai termini dello SLA.

I dati possono essere raccolti tramite richieste o Cisco NetFlow. Cisco fornisce le applicazioni NetFlow Collector e NetFlow Analyzer per la raccolta e l'analisi dei dati dai router e dagli switch Catalyst. Le applicazioni shareware come cflowd vengono utilizzate anche per raccogliere dati NetFlow. Una valutazione continua dell'utilizzo delle risorse può fornire informazioni sulla fatturazione, nonché informazioni per valutare la correttezza e l'ottimizzazione delle risorse. Alcune soluzioni di gestione della contabilità comunemente implementate includono:

- Software Evident

Strategia di attivazione e raccolta dati di NetFlow

NetFlow (flusso di rete) è una tecnologia di misurazione del lato dell'input che consente di acquisire i dati necessari per le applicazioni di pianificazione, monitoraggio e contabilità della rete. NetFlow deve essere implementato su interfacce di router edge/di aggregazione per i provider di servizi o su interfacce di router di accesso WAN per i clienti aziendali.

Cisco Systems consiglia un'installazione NetFlow attentamente pianificata con i servizi NetFlow attivati su questi router situati strategicamente. NetFlow può essere implementato in modo incrementale (interfaccia per interfaccia) e strategico (su router scelti bene), anziché su ogni router della rete. Il personale Cisco collaborerà con i clienti per determinare quali router e interfacce chiave attivare NetFlow in base ai modelli di flusso del traffico, alla topologia di rete e all'architettura del cliente.

Le considerazioni principali sull'implementazione includono:

- I servizi NetFlow devono essere utilizzati come strumento di accelerazione delle prestazioni di edge metering e access list e non devono essere attivati su router o router *hot* core/backbone in esecuzione a tassi di utilizzo della CPU molto elevati.
- Comprendere i requisiti di raccolta dei dati basati sulle applicazioni. Le applicazioni contabili possono richiedere solo l'origine e la chiusura delle informazioni sul flusso del router, mentre le applicazioni di monitoraggio possono richiedere una vista completa (ad uso intensivo di dati).
- Comprendere l'impatto della topologia di rete e dei criteri di routing sulla strategia di raccolta del flusso. Ad esempio, evitare di raccogliere flussi duplicati attivando NetFlow sui router di aggregazione chiave in cui il traffico ha origine o termina e non sui router backbone o sui router intermedi che forniscono viste duplicate delle stesse informazioni di flusso.
- I fornitori di servizi nel settore dei *vettori di transito* (che trasportano traffico che non ha origine né termina sulla loro rete) possono utilizzare i dati di esportazione NetFlow per misurare l'utilizzo del traffico di transito delle risorse di rete a fini di contabilità e fatturazione.

Configura accounting IP

Il supporto per l'accounting IP di Cisco offre funzioni di base per l'accounting IP. Abilitando l'accounting IP, gli utenti possono visualizzare il numero di byte e di pacchetti scambiati tramite il software Cisco IOS in base all'indirizzo IP di origine e di destinazione. Viene misurato solo il traffico IP di transito e solo su base in uscita. Il traffico generato dal software o che termina nel software non è incluso nelle statistiche di contabilità. Per mantenere accurati i totali contabili, il software gestisce due database di contabilità: un database attivo e un database a punti di controllo.

Il supporto dell'accounting IP di Cisco fornisce anche informazioni che identificano il traffico IP che non supera gli elenchi di accesso IP. L'identificazione degli indirizzi IP di origine che violano gli accessi IP elenca i possibili tentativi di violare la sicurezza. I dati indicano anche che è necessario verificare le configurazioni dell'elenco degli accessi IP. Per rendere disponibile questa funzione agli utenti, abilitare l'accounting IP delle violazioni dell'elenco di accesso utilizzando il comando **ip accounting access-violence**. Gli utenti possono quindi visualizzare il numero di byte e di pacchetti provenienti da una singola origine che hanno tentato di violare la sicurezza rispetto all'elenco degli accessi per la coppia di destinazione di origine. Per impostazione predefinita, l'accounting IP visualizza il numero di pacchetti che hanno superato gli elenchi di accesso e sono stati instradati.

Per abilitare l'accounting IP, utilizzare uno dei comandi seguenti per ogni interfaccia in modalità di configurazione interfaccia:

Comando	Scopo
ip accounting	Abilitare l'accounting IP di base.
violazioni accesso accounting ip	Abilitare l'accounting IP e consentire di identificare il traffico IP che non supera gli elenchi di accesso IP.

Per configurare altre funzioni di accounting IP, utilizzare uno o più dei comandi seguenti in modalità di configurazione globale:

Comando	Scopo
ip accounting-threshold *threshold*	Impostare il numero massimo di voci contabili da creare.
ip accounting-list *indirizzo-ip*	Filtrare le informazioni di accounting per gli host.
conteggio ***transizioni accounting ip***	Controllare il numero di record di transito che verranno memorizzati nel database di accounting IP.

Per informazioni sulle convenzioni usate in questo documento, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.