Netwerkbeheersysteem: Whitepaper over beste praktijken

Inhoud

Inleiding
Netwerkbeheer
Foutenbeheer
Platforms voor netwerkbeheer
Infrastructuur voor probleemoplossing
Detectie en melding van fouten
Proactieve foutbewaking en -melding
Configuratie-beheer
Configuratienormen
Configuratie-bestandsbeheer
voorraadbeheer
Softwarebeheer
Prestatiebeheer
Overeenkomst op serviceniveau
Prestatiebewaking, meting en rapportage
Prestatieanalyse en -afstemming
Beveiligingsbeheer
Verificatie
Authorization
accounting
SNMP-beveiliging
Boekhoudbeheer
Strategie voor activering en gegevensverzameling van NetFlow
IP-accounting instellen

Inleiding

Het beheermodel van het netwerk van de Internationale Organisatie voor Normalisatie (ISO) definieert vijf functionele gebieden van netwerkbeheer. Dit document bestrijkt alle functionele gebieden. Het algemene doel van dit document is praktische aanbevelingen te doen voor elk functioneel gebied om de algemene doeltreffendheid van de huidige beheersinstrumenten en -praktijken te verbeteren. Het voorziet ook in ontwerprichtsnoeren voor de toekomstige implementatie van netwerkbeheerinstrumenten en -technologieën.

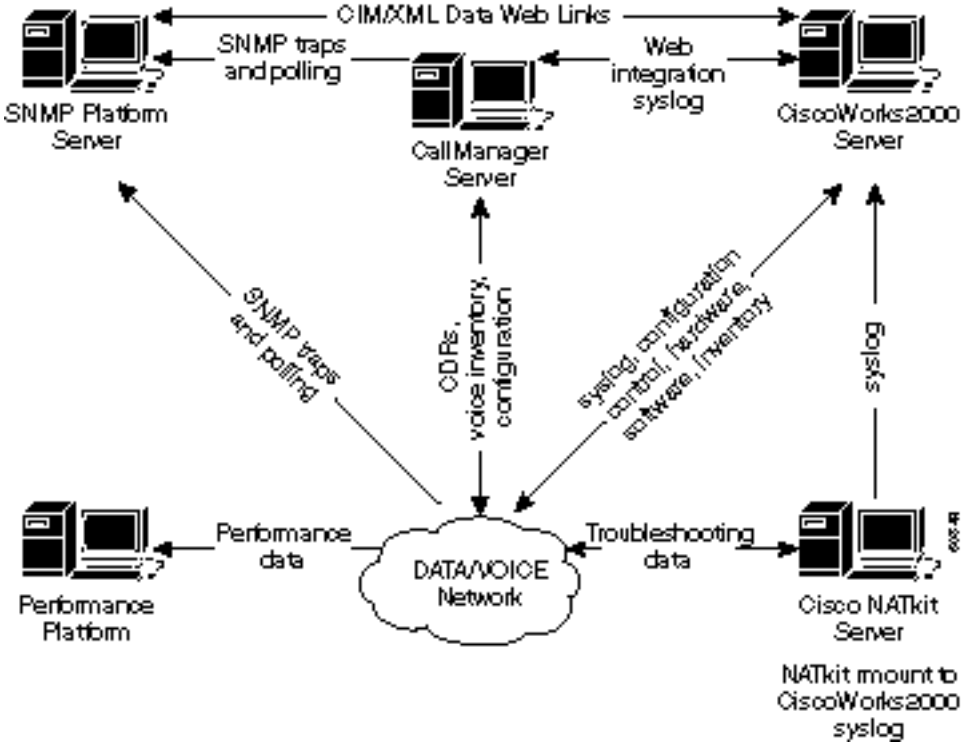
Netwerkbeheer

De vijf functionele gebieden van het ISO-netwerkbeheermodel zijn hieronder vermeld.

- Foutenbeheer-detecteren, isoleren, melden en corrigeren fouten die in het netwerk worden aangetroffen.

- Configuratie-beheer-configuratie van netwerkapparaten zoals configuratie, bestandsbeheer, voorraadbeheer en softwarebeheer.
- Prestatiebeheer-monitoren en meten verschillende aspecten van prestaties zodat de algehele prestaties op een acceptabel niveau kunnen worden gehandhaafd.
- Beveiligingsbeheer - Geef toegang tot netwerkapparaten en bedrijfsmiddelen aan geautoriseerde personen.
- Accountbeheer—Gebruik informatie over netwerkbronnen.

In het volgende diagram wordt een referentiekaart weergegeven die volgens Cisco Systems de minimale oplossing voor het beheer van een gegevensnetwerk moet zijn. Deze architectuur omvat een Cisco CallManager server voor hen die Voice over Internet Protocol (VoIP) willen beheren: Het diagram toont hoe u de server CallManager in de topologie van NMS zou integreren.



De netwerkbeheerarchitectuur omvat het volgende:

- Simple Network Management Protocol (SNMP)-platform voor foutbeheer
- Prestatiebewakingsplatform voor prestatiebeheer op lange termijn en trending
- CiscoWorks2000-server voor configuratiebeheer, systeemverzameling en hardware- en softwarevoorraadbeheer

Sommige SNMP-platforms kunnen direct gegevens met de CiscoWorks2000-server delen met gebruik van de Common Information Model/eXtensible Markup Language (CIM/XML) methoden. CIM is een gemeenschappelijk gegevensmodel van een implementatieneutraal schema voor de beschrijving van algemene beheerinformatie in een netwerk-/ondernemingsomgeving. CIM bestaat uit een specificatie en een schema. De specificatie definieert de details voor integratie met andere beheermodellen zoals SNMP MIBs of Desktopbeheerinformatiebestanden van de Automation Management Task Force (DMTF MIFs), terwijl het schema de eigenlijke modelbeschrijvingen bevat.

XML is een markeertaal die wordt gebruikt voor het weergeven van gestructureerde gegevens in tekstvorm. Een specifiek doel van XML was het grootste deel van de beschrijvende kracht van SGML te behouden terwijl het zoveel mogelijk van de complexiteit werd verwijderd. XML is in concept gelijk aan HTML, maar waar HTML wordt gebruikt om grafische informatie over een

document over te brengen, wordt XML gebruikt om gestructureerde gegevens in een document weer te geven.

De geavanceerde serviceklanten van Cisco zouden ook NATkit-server van Cisco voor extra proactieve controle en het oplossen van problemen omvatten. De NATkit server zou of een externe diskmontage (berg) of FTP-toegang (File Transfer Protocol) tot de gegevens op de CiscoWorks2000-server hebben.

Het hoofdstuk Network Management Basics van het *Overzicht* van de *Internetworking-technologie* biedt een gedetailleerder overzicht van de basisgegevens voor netwerkbeheer.

Foutenbeheer

Het doel van het foutenbeheer is om netwerkproblemen op te sporen, te registreren, gebruikers op de hoogte te stellen van, en (voor zover mogelijk) automatisch op te lossen om het netwerk effectief te houden. Omdat fouten downtime of onacceptabele netwerkdegradatie kunnen veroorzaken, is het foutenbeheer wellicht het meest toegepaste van de ISO-netwerkbeheerelementen.

Platforms voor netwerkbeheer

Een netwerkbeheerplatform dat in de onderneming wordt ingezet beheert een infrastructuur die uit meerdere netwerkelementen bestaat. Het platform ontvangt en verwerkt gebeurtenissen van netwerkelementen in het netwerk. Evenementen van servers en andere kritieke bronnen kunnen ook naar een beheerplatform worden doorgestuurd. De volgende algemeen beschikbare functies zijn opgenomen in een standaard beheerplatform:

- Netwerkontdekking
- Topologie in kaart brengen van netwerkelementen
- Event Manager
- Gegevensverzameling en graaf
- Videobrowser

Netwerkbeheerplatforms kunnen worden gezien als de hoofdconsole voor netwerkbewerkingen bij het detecteren van fouten in de infrastructuur. De mogelijkheid om problemen in elk netwerk snel te detecteren is van cruciaal belang. Het personeel van de netwerkoperaties kan op een grafische netwerkkaart vertrouwen om de operationele staten van kritieke netwerkelementen zoals routers en switches te tonen.

Netwerkbeheerplatforms zoals HP OpenView, Computer Associates Unicenter en SUN Solutions kunnen een ontdekking van netwerkapparaten uitvoeren. Elk netwerkapparaat wordt vertegenwoordigd door een grafisch element op de console van het beheerplatform. Verschillende kleuren op de grafische elementen vertegenwoordigen de huidige operationele status van netwerkapparaten. Netwerkapparaten kunnen worden geconfigureerd om meldingen, SNMP-traps genaamd, naar netwerkbeheerplatforms te verzenden. Na het ontvangen van de kennisgevingen verandert het grafische element dat het netwerkapparaat weergeeft in een andere kleur, afhankelijk van de ernst van het ontvangen bericht. Het bericht, gewoonlijk een gebeurtenis genoemd, wordt in een logbestand geplaatst. Het is vooral belangrijk dat de meeste huidige bestanden van Cisco Management Information Base (MIB) op het SNMP-platform worden geladen om te verzekeren dat de verschillende waarschuwingen van Cisco-apparaten correct worden geïnterpreteerd.

Cisco publiceert de MIB bestanden voor het beheer van verschillende netwerkapparaten. De Cisco MIB-bestanden bevinden zich op de cisco.com website en bevatten de volgende informatie:

- MIB-bestanden gepubliceerd in SNMPv1-indeling
- MIB-bestanden gepubliceerd in SNMPv2-indeling
- Ondersteunde SNMP-trap op Cisco-apparaten
- OID's voor Cisco huidige SNMP MIB-objecten

Een aantal netwerkbeheerplatforms zijn in staat om meerdere geografisch gedistribueerde sites te beheren. Dit wordt bereikt door het uitwisselen van beheergegevens tussen beheerconsoles op afgelegen locaties met een beheerstation op de hoofdlocatie. Het belangrijkste voordeel van een gedistribueerde architectuur is dat het beheerverkeer vermindert, dus, die een effectiever gebruik van bandbreedte voorziet. Een gedistribueerde architectuur stelt personeel ook in staat om hun netwerken lokaal te beheren vanaf afgelegen locaties met systemen.

Een recente verbetering van beheerplatforms is de mogelijkheid om netwerkelementen op afstand te beheren met behulp van een webinterface. Deze verbetering heft de behoefte aan speciale clientsoftware op individuele gebruikersstations op om toegang te krijgen tot een beheerplatform.

Een typische onderneming bestaat uit verschillende netwerkelementen. Elk apparaat vereist echter gewoonlijk een systeem voor het beheer van elementen die specifiek zijn voor de verkoper om de netwerkelementen doeltreffend te kunnen beheren. Daarom kunnen dubbele beheerstations netwerkelementen voor dezelfde informatie opvragen. De gegevens die door verschillende systemen worden verzameld, worden in afzonderlijke databases opgeslagen, waardoor administratieve overheadkosten voor gebruikers worden gecreëerd. Deze beperking heeft netwerkbedrijven en softwareverkopers ertoe aangezet normen aan te nemen zoals Common Object Application Broker Architecture (CORBA) en Computer-Integrated Manufacturing (CIM) om de uitwisseling van beheergegevens tussen beheerplatforms en systemen voor het beheer van elementen te vergemakkelijken. Wanneer verkopers standaarden overnemen in de ontwikkeling van beheersystemen kunnen gebruikers interoperabiliteit en kostenbesparingen verwachten in de implementatie en het beheer van de infrastructuur.

CORBA specificeert een systeem dat interoperabiliteit tussen objecten biedt in een heterogene, gedistribueerde omgeving en op een manier die transparant is voor de programmeur. Zijn ontwerp is gebaseerd op het object Management Group (OMG).

Infrastructuur voor probleemoplossing

Trial File Transfer Protocol (TFTP) en systeemlogservers (syslog) zijn cruciale componenten van een infrastructuur voor het oplossen van problemen in netwerkbewerkingen. De TFTP-server wordt voornamelijk gebruikt voor het opslaan van configuratiebestanden en softwarebeelden voor netwerkapparaten. De routers en switches kunnen de systeemmeldingen naar een systeemserver verzenden. De berichten vergemakkelijken de functie voor het oplossen van problemen wanneer er problemen worden aangetroffen. Af en toe heeft het Cisco ondersteuningspersoneel de syslogberichten nodig om de analyse van de worteloorzaak uit te voeren.

Met de gedistribueerde systeemverzamelingsfunctie CiscoWorks2000 Resource Management Essentials (Essentials) kunt u meerdere UNIX- of NT-verzamelstations op afgelegen locaties inzetten om berichtverzameling en -filtering uit te voeren. De filters kunnen specificeren welke syslogberichten zullen worden verstuurd naar de belangrijkste server van de Hoofdzaak. Een belangrijk voordeel van het implementeren van gedistribueerde collectie is het verminderen van berichten die naar de belangrijkste syslogservers worden doorgestuurd.

Detectie en melding van fouten

Het doel van het foutenbeheer is het detecteren, isoleren, melden en corrigeren van fouten in het netwerk. Netwerkapparaten kunnen beheerstations waarschuwen wanneer er een storing in de systemen optreedt. Een effectief systeem voor het beheer van fouten bestaat uit verschillende subsystemen. De detectie van fouten wordt verwezenlijkt wanneer de apparaten SNMP-trap-berichten, SNMP-opiniepeiling, RMON-drempels (Remote Monitoring) en syslog-berichten verzenden. Een beheersysteem waarschuwt de eindgebruiker wanneer een fout wordt gemeld en er corrigerende maatregelen kunnen worden genomen.

Splitsen moeten consistent op netwerkapparaten zijn ingeschakeld. Aanvullende vallen worden ondersteund met nieuwe Cisco IOS-softwarereleases voor routers en switches. Het is belangrijk om het configuratiebestand te controleren en bij te werken om te zorgen voor een goede decodering van de vallen. Een periodieke beoordeling van geconfigureerde vallen door het Cisco Assurance Network Services (ANS)-team zal zorgen voor een effectieve foutdetectie in het netwerk.

De volgende tabel toont de CISCO-STACK-MIB-vallen die door de switches van Cisco Catalyst Local Area Network (LAN) worden ondersteund en kunnen worden gebruikt om de foutomstandigheden op te sporen.

Trap	Beschrijving
moduleUp	De agent entiteit heeft ontdekt dat het **moduleStatus** object in deze MIB is overgestapt naar de **ok(2)** staat voor een van zijn modules.
moduleDown	De agent entiteit heeft ontdekt dat het *moduleStatus*-object in deze MIB van de **ok(2)** staat voor een van zijn modules is overgestapt.
chassisAlarm	De agent-entiteit heeft gedetecteerd dat het *chassisTempAlarm*, *chassisMinorAlarm*, of *chassisMajorAlarm* voorwerp in deze MIB naar **on(2)** staat is overgeschakeld. Een *chassisMajorAlarm* geeft aan dat één van de volgende voorwaarden bestaat: • Elke spanningsstoring • Gelijktijdige temperatuur en ventilatorstoring • 100% stroomonderbreking (twee op twee of één op één) • ELEKTRICITEIT WISSELBAAR, alleen-lezen geheugen (EEPROM) defect • Niet-vluchtige RAM (NVRAM)-storing • MCP-communicatiestoornis • NMP-status onbekend Een chassisMinorAlarm geeft aan dat één van de volgende voorwaarden bestaat: • Temperatuuralarm • Ventilatorfalen

	• Gedeeltelijke stroomonderbreking (één op twee) • Twee oncompatibele voedingen
chassisUitschakelen	De agent-entiteit heeft gedetecteerd dat het *chassisTempAlarm*, *chassisMinorAlarm*, of *chassisMajorAlarm* voorwerp in deze MIB naar **off(1)** staat is overgeschakeld.

Milieubewaking (MMM) vallen worden gedefinieerd in CISCO-ENVMON-MIB-val. De milieu-val stuurt Cisco ondernemingsspecifieke milieumonitoring-meldingen wanneer een milieudrempel wordt overschreden. Wanneer envmon wordt gebruikt, kan een specifiek type omgevingsval worden toegestaan, of kunnen alle valtypes van het milieubewakingssysteem worden geaccepteerd. Als geen optie is opgegeven, zijn alle milieutypen ingeschakeld. Dit kan een of meer van de volgende waarden hebben:

- voltage-A ciscoEnvMonVoltagenotification wordt verzonden als het voltage dat op een bepaald testpunt wordt gemeten buiten het normale bereik voor het testpunt is (zoals in het waarschuwings-, kritieke of sluitingsstadium).
- shutdown-A ciscoEnvMonShutdownnotification wordt verstuurd als de milieumonitoring opmerkt dat een testpunt een kritieke toestand bereikt en op het punt staat een shutdown te starten.
- voorziening-een ciscoEnvMontRedundantSupplynotification wordt verzonden als de overtollige elektriciteitstoevoer (waar uitgebreid) mislukt.
- ventilator-Een ciscoEnvMonFannotification wordt verstuurd indien één van de fans in de ventilatorserie (indien uitgebreid) mislukt.
- Temperatuur-A ciscoEnvMonTemperatureKennisgeving wordt verzonden als de temperatuur die op een bepaald testpunt wordt gemeten buiten het normale bereik voor het testpunt is (zoals in het fase van waarschuwing, kritisch of afsluiten).

De detectie van fouten en de controle van netwerkelementen kunnen van het apparatenniveau tot het protocol en interfaceniveaus worden uitgebreid. Voor een netwerkomgeving kan foutcontrole Virtual Local Area Network (VLAN), asynchrone overdrachtmodus (ATM), foutindicaties op fysieke interfaces, enzovoort omvatten. De implementatie van het foutenbeheer op het niveau van het protocol is beschikbaar met behulp van een beheersysteem voor elementen zoals de CiscoWorks2000 Campus Manager. De TrafficDirector-toepassing in Campus Manager richt zich op het beheer van switches door gebruik te maken van mini-RMON-ondersteuning op Catalyst-switches.

Met een toenemend aantal netwerkelementen en de complexiteit van netwerkproblemen kan een systeem voor het beheer van gebeurtenissen worden overwogen dat verschillende netwerkgebeurtenissen (syslog, val, logbestanden) kan correleren. Deze architectuur achter een evenementenbeheersysteem is vergelijkbaar met een Manager van Managers (MOM) - systeem. Een goed ontworpen systeem voor het beheer van gebeurtenissen stelt personeel in het netwerk Operations Center (NOC) in staat proactief en effectief te zijn bij het detecteren en diagnosticeren van netwerkproblemen. Met prioritering van gebeurtenissen en onderdrukking kan het personeel van de netwerkexploitatie zich concentreren op kritieke netwerkgebeurtenissen, verschillende systemen voor Event Management onderzoeken, waaronder het Cisco Info Center, en een haalbaarheidsanalyse uitvoeren om de mogelijkheden van dergelijke systemen volledig te verkennen. Ga voor meer informatie naar het Cisco Info Center.

Proactieve foutbewaking en -melding

RMON - alarm en gebeurtenis zijn twee groepen die in de RMON - specificatie worden gedefinieerd. Normaal gesproken voert een beheerscentrum opiniepeilingen uit op netwerkapparaten om de status of waarde van bepaalde variabelen te bepalen. Een beheerstation poilt bijvoorbeeld een router om het gebruik van de centrale verwerkingseenheid (CPU) te ontdekken en om een gebeurtenis te genereren wanneer de waarde een geconfigureerde drempel bereikt. Deze methode verspilt netwerkbandbreedte en kan ook de eigenlijke drempel, afhankelijk van het steminterval, missen.

Met RMON - alarm en gebeurtenissen, wordt een netwerkapparaat gevormd om zichzelf voor stijgende en dalende drempels te controleren. Bij een vooraf vastgesteld tijdsinterval neemt het netwerkapparaat een monster van een variabele en vergelijkt het met de drempels. Een SNMP-val kan naar een beheerstation worden verzonden als de werkelijke waarde de geconfigureerde drempelwaarden overschrijdt of onder de ingestelde waarde daalt. RMON - alarm en eventgroepen verstrekken een pro-actieve methode om kritieke netwerkapparaten te beheren.

Cisco Systems raadt het uitvoeren van RMON - alarm en gebeurtenis op kritieke netwerkapparaten aan. De gecontroleerde variabelen kunnen een CPU-gebruik, bufferfouten, input/output-druppels of enige variabelen van geïntegreerde types omvatten. Om te beginnen met Cisco IOS-softwarerelease 11.1(1)ondersteunen alle routerafbeeldingen RMON - alarm en eventgroepen.

Voor gedetailleerde informatie over RMON - alarm en gebeurtenis implementatie, zie de sectie van de RMON - Alarm en van de Implementatie van de gebeurtenis.

RMON - geheugenbeperkingen

RMON - geheugengebruik is constant bij alle platforms van de switch met betrekking tot statistieken, geschiedenissen, alarmen en gebeurtenissen. RMON gebruikt wat een *emmer* wordt genoemd om historiën en statistieken op de RMON - agent op te slaan (wat in dit geval de switch is). De emmer grootte wordt gedefinieerd op de RMON - sonde (SwitchProbe - apparaat) of RMON - toepassing (TrafficDirector-gereedschap) en vervolgens naar de in te stellen switch verzonden.

Ongeveer 450 K coderuimte is nodig om mini-RMON te ondersteunen (bijvoorbeeld vier RMON-groepen: statistieken, geschiedenis, alarmen en gebeurtenissen). De dynamische geheugeneis voor RMON varieert omdat het van de baanloze configuratie afhangt.

De volgende tabel definieert de RMON - geheugengebruiksinformatie voor elke mini-RMON-groep.

RMON - groepsdefinitie	Gebruikte DRAM-ruimte	Opmerkingen
Statistieken	140 bytes per switched Ethernet/Fast Ethernet-poort	Per poort
Geschiedenis	3,6 K voor 50 emmers *	Elke extra emmer gebruikt 56 bytes
Alarm en gebeurtenis	2,6 K per alarm en de bijbehorende items	Per wekker per poort

*RMON gebruikt wat een *emmer* wordt genoemd om historiën en statistieken op de RMON - agent op te slaan (zoals een switch).

RMON - alarmen en gebeurtenissen

Door RMON als deel van een oplossing van het foutbeheer te integreren kan een gebruiker het netwerk proactief controleren alvorens een potentieel probleem zich voordoet. Als het aantal ontvangen uitzendpakketten bijvoorbeeld aanzienlijk wordt verhoogd, kan dit een toename in CPU-gebruik veroorzaken. Door RMON - alarm en gebeurtenis in te voeren, kan een gebruiker een drempel instellen om het aantal ontvangen uitzending te controleren en het SNMP platform door middel van een SNMP val te waarschuwen als de gevormde drempel wordt bereikt. RMON - alarmen en gebeurtenissen elimineren de buitensporige opiniepeiling die normaal door het SNMP platform wordt uitgevoerd om het zelfde doel te bereiken.

Er zijn twee methoden beschikbaar waarmee u RMON - alarm en gebeurtenis kunt configureren:

- Opdracht-line interface (CLI)
- SNMP SET

De volgende steekproefprocedures tonen hoe om een drempel in te stellen om het aantal uitgezonden pakketten te controleren dat op een interface wordt ontvangen. In deze procedures wordt dezelfde teller gebruikt zoals in het opdrachtvoorbeeld **van de** showinterface aan het eind van deze sectie wordt getoond.

Opdracht-line interfacevoorbeeld

Om RMON - alarm en gebeurtenis toe te passen die de CLI interface gebruikt, voer de volgende stappen uit:

1. Vind de interface index geassocieerd met Ethernet 0 door de ifTable MIB te lopen.
```
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. Verkrijg de OID gekoppeld aan het CLI-veld die gemonitord moet worden. De OID voor 'uitzendingen' is bijvoorbeeld 1.3.6.1.2.1.2.2.1.12. De Cisco OIDs voor specifieke MIB-variabelen zijn beschikbaar op de website van cisco.com.
3. Bepaal de volgende parameters voor het instellen van drempels en gebeurtenissen.stijgende en dalende drempelstype bemonstering (absoluut of delta)bemonsteringsintervalactie wanneer de drempel is bereiktVoor de toepassing van dit voorbeeld wordt een drempel ingesteld om het aantal op Ethernet ontvangen uitzending-pakketten te controleren. Er zal een val worden gegenereerd als het aantal ontvangen uitzending-pakketten groter is dan 500 tussen 60-seconden monsters. De drempel wordt opnieuw geactiveerd wanneer het aantal input-uitzendingen niet tussen de genomen monsters toeneemt.**Opmerking:** Voor gedetailleerdere informatie over deze opdrachtparameters, controleer de documentatie van Cisco Connection Online (CCO) voor RMON - alarm en gebeurtenis opdrachten voor uw specifieke Cisco IOS-versie.
4. Specificeer de verzonden val (RMON - gebeurtenis) wanneer de drempel wordt bereikt met de volgende CLI-opdrachten (de Cisco IOS-opdrachten worden in vet weergegeven):**Prime-event 1 klem poort beschrijving "High Broadcast on Ethernet 0" eigenaar van Ciscormon event 2 blog Description "Normale uitzending die op ethernet 0 wordt ontvangen" eigenaar**

cisco

5. Specificeer de drempels en relevante parameters (RMON - alarm) met de volgende CLI-opdrachten:**alarmsignaal 1 bij binnenkomst 12.1 60 delta stijgende drempel 500 1dalingsdrempel 0 2 eigenaar cisco**
6. Gebruik SNMP om deze tabellen te raadplegen om te controleren of de eventTable items op het apparaat zijn aangemaakt.

```
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. Gebruik SNMP om deze tabellen te inroepen om te controleren of de alarmwaarden voor Tabellen zijn ingesteld.

```
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)
```

SNMP SET-voorbeeld

Voltooi de volgende stappen om RMON - alarm en -gebeurtenis met de SNMP ET-handeling uit te voeren:

1. Specificeer de verzonden val (RMON - gebeurtenis) wanneer de drempel wordt bereikt met de volgende SNMP ET-operaties:
```
# 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. Specificeer de drempels en relevante parameters (RMON - alarm) met behulp van de volgende SNMP-reeks-bewerkingen:
```
# 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. Bekijk deze tabellen om te controleren of de eventTable items op het apparaat zijn gezet.
```
% 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. Bekijk deze tabellen om te controleren of de waarden voor alarmtabel zijn ingesteld.
   ```
   % snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1
   ```

raakvlak tonen

Dit voorbeeld is een resultaat van de **show interface** opdracht.

poort> **toont 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
```

Configuratie-beheer

Het doel van het configuratiebeheer is om de netwerk- en systeemconfiguratie-informatie te controleren zodat de effecten van verschillende versies van hardware- en softwareelementen op de netwerkwerking kunnen worden getraceerd en beheerd.

Configuratienormen

Met een toenemend aantal netwerkapparaten, is het van cruciaal belang om de plaats van een

netwerkapparaat nauwkeurig te kunnen identificeren. Deze locatieinformatie moet een gedetailleerde beschrijving van betekenis geven aan degenen die belast zijn met verzendingsbronnen wanneer een netwerkprobleem zich voordoet. Als u een resolutie wilt bespoedigen als er een netwerkprobleem is, moet u er zeker van zijn dat u over de beschikbare contactinformatie beschikt van de persoon of instantie die verantwoordelijk is voor de apparaten. De contactgegevens moeten het telefoonnummer en de naam van de persoon of dienst bevatten.

Namen conventies voor netwerkapparaten, te beginnen bij de naam van het apparaat in de interface, moeten gepland en geïmplementeerd worden als onderdeel van de configuratiestandaard. Een goed gedefinieerde naamgevingsconventie biedt personeel de mogelijkheid om nauwkeurige informatie te verstrekken wanneer er netwerkproblemen worden opgelost. De naamgevingsconventie voor apparaten kan gebruikmaken van geografische locatie, bouwnaam, vloer enzovoort. Voor de interface naamgeving conventie, kan het het segment omvatten waarmee een poort is verbonden, naam van verbindende hub, enzovoort. Op seriële interfaces moet het het eigenlijke bandbreedte-nummer, het lokale DLCI-nummer (Data Link Connection Identifier) (indien Frame Relay), de bestemming en de circuit-ID of de informatie die door de vervoerder is verstrekt, omvatten.

Configuratie-bestandsbeheer

Wanneer u nieuwe configuratieopdrachten aan bestaande behoeften van netwerkapparaten toevoegt, moet u de opdrachten voor integriteit controleren voordat er daadwerkelijk implementatie plaatsvindt. Een slecht geconfigureerd netwerkapparaat kan een desastreus effect hebben op de connectiviteit en prestaties van het netwerk. De opdrachtparameters van de configuratie moeten worden gecontroleerd om fouten of onverenigbaarheden te voorkomen. Het is raadzaam om regelmatig een grondig onderzoek van de configuraties met Cisco-engineers te plannen.

Een volledig functionele CiscoWorks2000 korrelgrootte maakt het automatisch maken van back-ups van configuratiebestanden op routers en Cisco Catalyst-switches mogelijk. De veiligheidsfunctie van de Hoofdzaak kan worden gebruikt om authenticatie bij configuratieveranderingen uit te voeren. Er is een register van wijzigingen beschikbaar om wijzigingen te volgen en de naam van de gebruiker van personen die wijzigingen aanbrengen. Voor configuratieveranderingen op meerdere apparaten zijn twee opties beschikbaar: de web-gebaseerde NetConfig in de huidige versie van CiscoWorks2000 Essentials of het **cisco-**configuratiescherm. U kunt de configuratiebestanden downloaden en uploaden door gebruik te maken van CiscoWorks2000 Essentials met behulp van de vooraf gedefinieerde of door de gebruiker gedefinieerde sjablonen.

Deze functies kunnen worden verwezenlijkt met de gereedschappen voor configuratiebeheer in CiscoWorks2000 Essentials:

- configuratiebestanden uit het configuratiearchief van de basisproducten naar een apparaat of meerdere apparaten afdrukken
- Trek de configuratie van het apparaat naar het archief van de Hoofdstukken
- Haal de nieuwste configuratie uit het archief en schrijf dit naar een bestand
- Import configuratie uit een bestand en druk de configuratie naar apparaten
- Vergelijk de laatste twee configuraties in het archief van de Hoofdstukken
- Configuratie ouder dan een bepaalde datum of versie uit het archief verwijderen
- Kopieert de opstartconfiguratie naar de actieve configuratie

voorraadbeheer

De zoekfunctie van de meeste netwerkbeheerplatforms is bedoeld om een dynamische lijst van de in het netwerk gevonden apparaten te bieden. Detectiemachines zoals die welke in netwerkbeheerplatforms worden ingezet, moeten worden gebruikt.

Een inventarisdatabase bevat gedetailleerde configuratieinformatie over netwerkapparaten. Gemeenschappelijke informatie omvat modellen van hardware, geïnstalleerde modules, softwarebeelden, microcodespiegels, enz. Al deze informatie is van cruciaal belang voor de voltooiing van taken zoals software en hardware-onderhoud. De bijgewerkte lijst van netwerkapparaten die door het zoekproces worden verzameld, kan worden gebruikt als een hoofdlijst om inventarisinformatie te verzamelen met behulp van SNMP of het scripting. Een apparaatlijst kan van CiscoWorks2000 Campus Manager worden geïmporteerd in de opslagdatabase van CiscoWorks2000 Essentials om een actuele inventaris van Cisco Catalyst switches te verkrijgen.

Softwarebeheer

Een succesvolle upgrade van Cisco IOS beelden op netwerkapparaten vereist een gedetailleerde analyse van de vereisten zoals geheugen, laars-rom, microcoderingsniveau, enz. De vereisten worden normaal gesproken gedocumenteerd en beschikbaar op de website van Cisco in de vorm van opmerkingen en installatiehandleidingen. Het proces om een netwerkapparaat te verbeteren dat Cisco IOS in werking stelt omvat het downloaden van een correct beeld van CCO, het maken van een back-up van de huidige afbeelding, het verzekeren dat aan alle hardwarevereisten wordt voldaan en het laden van de nieuwe afbeelding in het apparaat.

Het upgradevenster om het onderhoud van het apparaat te voltooien is beperkt voor sommige organisaties. In een grote netwerkomgeving met beperkte middelen, kan het nodig zijn om software-upgrades te plannen en te automatiseren na bedrijfsuren. De procedure kan worden voltooid met behulp van de scriptietaal, zoals Verwacht, of met behulp van een applicatie die specifiek is geschreven om een dergelijke taak uit te voeren.

Veranderingen in software in netwerkapparaten zoals Cisco IOS beelden en microcodeversies moeten worden getraceerd om te helpen in de analysecefase wanneer een ander softwareonderhoud vereist is. Indien een rapport over de wijzigingsgeschiedenis beschikbaar is, kan de persoon die de upgrade uitvoert het risico van het laden van onverenigbare beelden of microcode in netwerkapparaten tot een minimum beperken.

Prestatiebeheer

Overeenkomst op serviceniveau

Een overeenkomst inzake serviceniveau (SLA) is een schriftelijke overeenkomst tussen een dienstverlener en zijn klanten over het verwachte prestatieniveau van netwerkdiensten. De SLA bestaat uit parameters waarover de aanbieder en zijn klanten overeenstemming hebben bereikt. De waarden die voor de maatstaf worden ingesteld, moeten realistisch, betekenisvol en meetbaar zijn voor beide partijen.

Verschillende interfacestatistieken kunnen van netwerkapparaten worden verzameld om het prestatieniveau te meten. Deze statistieken kunnen als maatstaf in de SLA worden opgenomen. Statistieken zoals druppels in de rij, druppels in de wachtrij en genegeerde pakketten zijn handig voor het diagnosticeren van prestatiegerelateerde problemen.

Op het niveau van het apparaat kunnen prestatiemetrieken het gebruik van CPU, buffertoewijzing (grote buffer, middelmatige buffer, fouten, hit ratio) en geheugentoewijzing omvatten. De prestaties van bepaalde netwerkprotocollen zijn direct gerelateerd aan de beschikbaarheid van buffer in netwerkapparaten. De prestatiestatistieken op het niveau van de meetapparatuur zijn van cruciaal belang voor het optimaliseren van de prestaties van protocollen op hoger niveau.

Netwerkapparaten zoals routers ondersteunen verschillende laagse protocollen zoals Data Link Switching Workgroup (DLSW), Remote Source Route Bridging (RSRB), AppleTalk, enzovoort. Prestatiestatistieken van WAN-technologieën (Wide Area Network), waaronder Frame Relay, ATM, Integrated Services Digital Network (ISDN), en andere kunnen worden gevolgd en verzameld.

Prestatiebewaking, meting en rapportage

Verschillende prestatiemetrieken op de interface-, apparaat- en protocolniveaus moeten regelmatig met SNMP worden verzameld. De stemmachine in een netwerkbeheersysteem kan worden gebruikt voor gegevensverzameling. De meeste netwerkbeheersystemen zijn in staat om opgevraagde gegevens te verzamelen, op te slaan en te presenteren.

Op de markt zijn diverse oplossingen beschikbaar om tegemoet te komen aan de behoeften van prestatiemanagement voor ondernemingsomgevingen. Deze systemen zijn in staat gegevens te verzamelen, op te slaan en aan te bieden van netwerkapparaten en servers. De web-gebaseerde interface voor de meeste producten maakt de prestatiegegevens toegankelijk vanuit alle hoeken van het bedrijf. Enkele van de algemeen gebruikte oplossingen voor prestatiebeheer omvatten:

- InfoVista-weergave
- SAS IT-servicevisie
- Trinagy TREND

Uit een evaluatie van de bovengenoemde producten zal blijken of zij aan de eisen van de verschillende gebruikers voldoen. Sommige verkopers ondersteunen integratie met netwerkbeheer en systeembeheerplatforms. InfoVista ondersteunt bijvoorbeeld de BMC Patrol Agent om belangrijke prestatiestatistieken van toepassingsservers te leveren. Elk product heeft een ander prijsmodel en mogelijkheden met het basisaanbod. Ondersteuning voor prestatiebeheer voor Cisco's apparaten zoals NetFlow, RMON en Cisco IOS Service Assurance Agent/Response Time Reporter (RTR/SAA CSAA/RTR) is beschikbaar op sommige oplossingen. Concord heeft onlangs extra ondersteuning toegevoegd voor Cisco's WAN-switches, die kunnen worden gebruikt om prestatiegegevens te verzamelen en weer te geven.

De optie CSAA/RTR Service Assurance Agent (SAA)/Response Time Reporter (RTR) in Cisco IOS kan worden gebruikt om de responstijd tussen IP-apparaten te meten. Een bronrouter die met CSAA geconfigureerd is, is in staat om de responsietijd op een bestemming IP-apparaat te meten dat een router of een IP-apparaat kan zijn. De responstijd kan tussen de bron en de bestemming of voor elke hop langs het pad worden gemeten. SNMP-traps kunnen worden ingesteld om beheerconsoles te waarschuwen als de responstijd de vooraf gedefinieerde drempels overschrijdt.

Recente verbeteringen aan Cisco IOS breidt de mogelijkheden van CSAA uit om het volgende te meten:

- HyperText Transfer Protocol (HTTP)-serviceprestatiesDomain Name System (DNS)-raadplegingTCP-verbinding (Transmission Control Protocol)HTTP-transactietijd
- Interpack-vertraging-variantie (Jitter) van Voice-over-IP (VoIP) verkeer

- Response time between end points for a Specific Quality of Service (QoS)IP-type (ToS) bits
- Packet-verlies met CSAA-gegenereerde pakketten

Het configureren van de CSA-functie op routers kan worden voltooid met de Cisco Internetwork Performance Monitor (IPM) toepassing. CSAA/RTR is ingesloten in veel maar niet alle functiesets van de Cisco IOS-software. Een release van de Cisco IOS-softwarerelease die CSAA/RTR ondersteunt, moet worden geïnstalleerd op het apparaat dat IPM gebruikt om prestatiestatistieken te verzamelen. Raadpleeg voor een samenvatting van Cisco IOS-versies die CSAA/RTR/IPM ondersteunen de website van de IPM waar vragen vaak worden gesteld.

Aanvullende informatie over IPM omvat:

- Overzicht van IPM
- Service Assurance Agent

Prestatieanalyse en -afstemming

Het gebruikersverkeer is aanzienlijk toegenomen en heeft een hogere vraag op netwerkbronnen geplaatst. Netwerkmanagers hebben doorgaans een beperkte weergave van de typen verkeer in het netwerk. De gebruiker en de toepassing van het verkeer profileren verstrekt een gedetailleerd overzicht van het verkeer in het netwerk. Twee technologieën, RMON sondes en NetFlow, bieden de mogelijkheid om verkeersprofielen te verzamelen.

RMON

De RMON - normen worden ontworpen om in een gedistribueerde architectuur te worden ingezet waar de agenten (of ingebed of in standalone spelden) met een centraal station (de beheerconsole) via SNMP communiceren. De RFC 1757 RMON - standaard organiseert monitoringfuncties in negen groepen om Ethernet-topologieën te ondersteunen, en voegt een tiende groep in RFC 1513 toe voor Token Ring-unieke parameters. Snelle Ethernet link monitoring wordt geleverd in het kader van de RFC 1757-standaard en Fibre-Distributed Data Interface (FDDI) ring bewaking wordt geboden in het kader van zowel RFC 1757 als RFC 1513.

De opkomende RFC 2021 RMON - specificatie drijft externe controlenormen voorbij de laag van de Toegangscontrole van de Media (MAC) aan het netwerk en de toepassingslagen. Met deze instelling kunnen beheerders netwerktoepassingen zoals webverkeer, NetWare, Notes, e-mail, databases en Network File System (NFS) analyseren en probleemoplossing. RMON - alarmen, statistieken, geschiedenis, en host/conversatiegroepen kunnen nu worden gebruikt om netwerkbeschikbaarheid proactief te controleren en te onderhouden op basis van toepassingslaag verkeer-het meest kritieke verkeer in het netwerk. RMON2 stelt netwerkbeheerders in staat om hun implementatie van op standaarden gebaseerde controleoplossingen te blijven voortzetten om missie-kritieke, op server-gebaseerde toepassingen te ondersteunen.

De volgende tabellen geven een lijst van de functies van de RMON - groepen.

RMON - groep (RFC 1757)	Functie
Statistieken	Tellers voor pakketten, octetten, uitzendingen, fouten, en aanbiedingen op het segment of de haven.

Geschiedenis	Periodiek genomen monsters en slaat statistiekgroeptellers op voor later terugwinning.
Zouden	Hiermee houdt u statistieken bij over elk host-apparaat in het segment of de poort.
Host Top N	Een door de gebruiker gedefinieerd subset rapport van de Hosts Group, gesorteerd door een statistische teller. Door alleen de resultaten terug te geven, wordt het beheerverkeer tot een minimum beperkt.
Verkeersmatrix	Hiermee worden gespreksstatistieken tussen hosts op het netwerk onderhouden.
alarmen	Een drempel die op kritieke RMON - variabelen voor proactief beheer kan worden ingesteld.
Evenementen	genereert SNMP-traps en logingangen wanneer een alarmgroepsdrempel wordt overschreden.
Packet Capture	Beheert buffers voor pakketten die door de groep van het filter worden opgenomen voor het uploaden naar de beheerconsole.
Token Ring	Ring station - gedetailleerde statistieken op individuele stations Ring station orde - een geordende lijst van stations momenteel op de configuratie van Ring station - configuratie en plaatsing/verwijdering per station Bron routing - statistieken van bron routing, zoals hoptellingen en anderen

RMON2	Functie
Protocolmap	Protocollen waarvoor de agent statistieken controleert en onderhoudt.
Protocoldistributie	Statistieken voor elk protocol.
Network Layer Host	Statistieken voor elk adres van de netwerklaag op het segment, de ring of de poort.
Network Layer Matrix	Verkeersstatistieken voor paren van de adressen van de netwerklaag.
Application Layer Host	Statistieken per toepassingslaagprotocol voor elk netwerkadres.
Application Layer Matrix	Verkeersstatistieken door toepassingslaagprotocol voor paren van de adressen van de netwerklaag.
Door gebruiker definieerbare historie	Uitbreidt geschiedenis voorbij RMON1 link-laag statistieken om RMON, RMON2, MIB-I, of MIB-II statistieken te omvatten.
Toewijzing van adres	MAC-to-netwerk laag adresbindingen.
Configuratie	Agent-functies en -configuraties.

groep	

NetFlow

De functie Cisco NetFlow maakt het mogelijk om gedetailleerde statistieken van verkeersstromen te vergaren voor functies voor capaciteitsplanning, facturering en probleemoplossing. NetFlow kan op individuele interfaces worden geconfigureerd, die informatie bieden over verkeer dat door die interfaces passeert. De volgende soorten informatie maken deel uit van de gedetailleerde verkeersstatistieken:

- IP-adressen van bron en bestemming
- I- en uitvoerinterfacenummers
- TCP/UDP-bronpoort en doelpoorten
- Aantal bytes en pakketten in de stroom
- Autonome systeemnummers van bron en bestemming
- IP-type service (ToS)

NetFlow-gegevens die op netwerkapparaten zijn verzameld, worden geëxporteerd naar een verzamelmachine. De verzamelaar voert functies uit zoals het beperken van het gegevensvolume (filtering en aggregatie), hiërarchische gegevensopslag en bestandssysteembeheer. Cisco biedt NetFlow Collector en NetFlow Analyzer toepassingen voor het verzamelen en analyseren van gegevens van routers en Cisco Catalyst switches. Er zijn ook gedeelde gereedschappen zoals flow die Cisco NetFlow-gebruikersdatagram Protocol (UDP)-records kunnen verzamelen.

NetFlow-gegevens worden getransporteerd met behulp van UDP-pakketten in drie verschillende indelingen:

- Versie 1—Het oorspronkelijke formaat dat in de eerste NetFlow-releases wordt ondersteund.
- Versie 5-A latere verbetering die het toegevoegde Protocol van de Grens van het Protocol (BGP) autonome systeeminformatie en de getallen van de stroomsequentie.
- Versie 7-A nog latere verbetering die NetFlow switchondersteuning voor Cisco Catalyst 5000 Series switches met een NetFlow-functiekaart (NFFC) heeft toegevoegd.

Versies 2 tot en met 4 en versie 6 zijn niet vrijgegeven of worden niet ondersteund door FlowCollector. In alle drie versies bestaat het datagram uit een header en een of meer stroomrecords.

Raadpleeg voor meer informatie het witboek van de NetFlow Services-Oplossingen.

De volgende tabel schetst ondersteunde Cisco IOS-versies voor het verzamelen van NetFlow-gegevens van routers en Catalyst-switches.

Cisco IOS-softwarerelease	Ondersteunde Cisco hardwareplatform(s)	Ondersteunde NetFlow-uitgevoerde versie(s)
11.1 CA en 11.1 CC	Cisco 7200, 7500 en RSP7000	V1 en V5
11,2 en 11,2 P	Cisco 7200, 7500 en RSP7000	V1
11,2 P	Cisco Route Switch Module	V1

	(RSM)	
11.3 en 11.3 T	Cisco 7200, 7500 en RSP7000	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000 en RSM	V1 en V5
12,0 T	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8 000 TOEREN/MIN en BPX 8600	V1 en V5
12.0(3)T en later	Cisco 1600*, 1720, 2500***, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR720 0, 7500, RSP7000, RSM, MGX 8800 TOEREN/MGX en BPX 8650	V1, V5 en V8
12.0(6)S	Cisco 12000-software	V1, V5 en V8
—	Cisco Catalyst 5000 met NetFlow-functiekaart (NFFC)**	V7

* Ondersteuning voor NetFlow Export V1, V5 en V8 op Cisco 1600- en 2500-platforms is gericht op Cisco IOS-softwarerelease 12.0(T). NetFlow-ondersteuning voor deze platforms is niet beschikbaar in de Cisco IOS 12.0 hoofdrelease.

** Ondersteuning voor NetFlow V1, V5 en V8 op het AS5300-platform is bedoeld voor Cisco IOS-softwarerelease 12.06(T).

** MLS en NetFlow data export wordt ondersteund in Catalyst 5000 Series supervisor software release 4.1(1) of hoger.

Beveiligingsbeheer

Het beveiligingsbeheer heeft tot doel de toegang tot de netwerkmiddelen te controleren overeenkomstig de plaatselijke richtsnoeren, zodat het netwerk niet kan worden gesaboteerd (opzettelijk of onbedoeld). Een subsysteem voor beveiligingsbeheer kan bijvoorbeeld gebruikers

controleren die zich aan een netwerkbron houden, waardoor ze geen toegang hebben tot degenen die een ongepaste toegangscode invoeren. Beveiligingsbeheer is een zeer breed onderwerp; Daarom heeft dit gebied van het document alleen betrekking op beveiliging met betrekking tot SNMP en basisbeveiliging van de toegang tot apparatuur.

Gedetailleerde informatie over geavanceerde beveiliging omvat:

- Verhoogde veiligheid op IP-netwerken
- OpenSystems

Een goede uitvoering van het veiligheidsbeheer begint met een goed beveiligingsbeleid en goede beveiligingsprocedures. Het is belangrijk om een platform-specifieke minimum configuratienorm te creëren voor alle routers en switches die de beste praktijken van de industrie voor veiligheid en prestaties volgen.

Er zijn verschillende methoden om de toegang op Cisco-routers en Catalyst-switches te controleren. Enkele van deze methoden zijn:

- Toegangscontrolelijsten (ACL's)
- Gebruikersnaam en wachtwoorden lokaal aan het apparaat
- Terminal Access Control System (TACACS)

TACACS is een standaard beveiligingsprotocol dat tussen clientapparaten op een netwerk en tegen een TACACS-server loopt. TACACS is een authenticatiemechanisme dat wordt gebruikt om de identiteit van een apparaat dat toegang op afstand tot een bevoorrechte databank zoekt, te authentiseren. Varianten op TACACS omvatten TACACS+, de AAA-architectuur die verificatie-, autorisatie- en boekhoudkundige functies scheidt.

TACACS+ wordt door Cisco gebruikt om een fijnere controle toe te staan over wie het apparaat van Cisco in niet-geprivilegieerde en geprivilegieerde modus kan benaderen. Meervoudige TACACS+ servers kunnen worden geconfigureerd voor fouttolerantie. Dankzij TACACS+ is de router en de switch voor een naam en wachtwoord gevraagd. Verificatie kan worden ingesteld voor inlogcontrole of voor het authentiseren van afzonderlijke opdrachten.

Verificatie

Verificatie is het proces voor het identificeren van gebruikers, inclusief de dialoog over inloggen en wachtwoorden, uitdaging en antwoord, en berichtenondersteuning. Verificatie is de manier waarop een gebruiker wordt geïdentificeerd voordat toegang tot de router of switch wordt verleend. Er bestaat een fundamenteel verband tussen authenticatie en autorisatie. Hoe meer autorisatie een gebruiker ontvangt, des te sterker de authenticatie dient te zijn.

Authorization

Een vergunning biedt een afstandsbediening, inclusief een eenmalige vergunning en vergunning voor elke service die door de gebruiker wordt gevraagd. Op een router van Cisco, is het bereik van het machtigingsniveau voor gebruikers 0 tot 15 met 0 het laagste niveau en 15 het hoogste.

accounting

Boekhouding maakt het mogelijk om beveiligingsinformatie te verzamelen en te verzenden die gebruikt wordt voor facturering, controle en rapportage, zoals gebruikersidentiteit, start- en stop-tijden en uitgevoerde opdrachten. Met accounting kunnen netwerkmanagers de services

bijhouden die gebruikers gebruiken en ook de hoeveelheid netwerkbronnen die ze gebruiken.

De volgende tabel toont basissteekproefopdrachten voor het gebruik van TACACS+, verificatie, autorisatie en accounting op een Cisco-router en een Catalyst switch. Raadpleeg het document Verificatie, autorisatie en accounting voor meer uitgebreide opdrachten.

Cisco IOS-opdracht	**doel**
router	
nieuw model	Verificatie, autorisatie, accounting (AAA) inschakelen als de primaire methode voor toegangscontrole.
AAA-accounting {*systeem	Netwerk	aansluiting	exce	commandoniveau*} {*start-stop	wachttijd	stop-only*} {*tacacs+	straal*}	Boekhouding met de mondiale configuratieopdrachten inschakelen.
Standaard AAA-authenticatie tacs+	Stel de router in zodat de verbindingen naar een eindlijn die met de standaardinstelling voor inloggen is ingesteld, geauthentiseerd worden met TACACS+ en mislukt als de verificatie om welke reden dan ook faalt.
AAA toestemming EXEC standaardinstellingen tac's+ geen	Stel de router in om te controleren of de gebruiker een EXEC-schaal mag gebruiken door de TACACS+ server te vragen.
IP-adres van de tacacs-server host *tacacs+ server*	Specificeer de TACACS+ server die voor verificatie met de mondiale configuratieopdrachten zal worden gebruikt.
Gedeeld geheim op **tacacs-server**	Specificeer het gedeelde geheim dat door de servers TACACS+ en de router van Cisco met de mondiale configuratieopdracht bekend is.
Catalyst 9300 Switch	
ingestelde loginlogtac ' s voor verificatie maken [*all] mogelijk	console	http	telnet*] [*primair*]	Schakel TACACS+ verificatie in voor normale inlogmodus. Gebruik de console of de Telnet sleutelwoorden om TACACS+ alleen voor de verbindingspogingen van de console of van het telnet toe te staan.
set autorisatie exec laat {*optie} reserve*	autorisatie voor normale inlogmodus inschakelen. Gebruik

optie toe} [*console*	*telnet*	*beide*]	de console of de sleutelwoorden van Telnet om vergunning slechts voor de verbindingspogingen van de console of van het telnet toe te staan.
Toets tacacs-server *gedeeld geheim* instellen	Specificeer het gedeelde geheim dat door de TACACS+ servers en de switch bekend is.
IP-adres van tacacs-server host *tacacs+ server*	Specificeer de TACACS+ server die voor verificatie met de mondiale configuratieopdrachten zal worden gebruikt.
Stel accounting opdrachten in om {*configuratie*}	*all*} {*stop-only*} *tacacs*+	Boekhouding van configuratieopdrachten inschakelen.

Voor meer informatie over de manier waarop u AAA kunt configureren om de toegang tot de opdrachtregel-interface in de Catalyst ondernemings LAN-switches te controleren, raadpleegt u het CONTROLERENDE Toegang tot de Switch door verificatie, autorisatie en accounting-document te gebruiken.

SNMP-beveiliging

Het SNMP-protocol kan worden gebruikt om configuratiewijzigingen in de routers en Catalyst-switches toe te passen die vergelijkbaar zijn met die welke door de CLI zijn gegenereerd. Correcte beveiligingsmaatregelen dienen op netwerkapparaten te worden ingesteld om toegang door onbevoegden en verandering via SNMP te voorkomen. De communautaire sms'en moeten voldoen aan de standaard wachtwoordrichtlijnen voor lengte, tekens en moeite met raden van gebruik. Het is belangrijk om de communautaire koorden te veranderen van hun openbare en particuliere faillieten.

Alle SNMP-beheerhost(s) moeten een statisch IP-adres hebben en expliciet SNMP-communicatierechten met het netwerkapparaat worden toegekend door middel van een vooraf gedefinieerde IP-adres en toegangscontrolelijst (ACL). Cisco IOS en Cisco Catalyst software bieden beveiligingsfuncties die ervoor zorgen dat alleen geautoriseerde beheerstations wijzigingen op netwerkapparaten mogen uitvoeren.

Functies voor routerbeveiliging

SNMP-prioriteitsniveau

Deze optie beperkt de soorten bewerkingen die een beheerstation op een router kan uitvoeren. Er zijn twee soorten bevoorrechtingsniveau op routers: Alleen lezen (RO) en lezen (RW). Het RO-niveau laat alleen een beheerstation toe om de routergegevens te vragen. Het staat niet toe dat configuratieopdrachten zoals het opnieuw opstarten van een router en het sluiten van interfaces worden uitgevoerd. Alleen het RW-bevoorrechtingsniveau kan worden gebruikt voor het uitvoeren van dergelijke bewerkingen.

SNMP-toegangscontrolelijst (ACL)

De functie SNMP ACL kan in combinatie met de functie SNMP-privilege worden gebruikt om specifieke beheerstations te beperken van het vragen van beheerinformatie van routers.

SNMP-weergave

Deze optie beperkt specifieke informatie die vanaf routers door beheerstations kan worden opgeroepen. Het kan met de eigenschappen van het de Voorraad van SNMP en ACL worden gebruikt om de beperkte toegang van gegevens door beheersconsoles af te dwingen. Voor configuratiemonsters van SNMP View, ga naar de SNMP serverweergave.

SNMP versie 3

SNMP versie 3 (SNMPv3) biedt veilige uitwisselingen van beheergegevens tussen netwerkapparaten en beheerstations. De encryptie en de authenticatie eigenschappen in SNMPv3 verzekeren hoge veiligheid in het vervoer van pakketten naar een beheerconsole. SNMPv3 wordt ondersteund in Cisco IOS-softwarerelease 12.0(3)T en hoger. Voor een technisch overzicht van SNMPv3, ga naar SNMPv3 documentatie.

Toegangscontrolelijst (ACL) op interfaces

De functie ACL biedt beveiligingsmaatregelen ter voorkoming van aanvallen zoals IP-spoofing. ACL kan op inkomende of uitgaande interfaces op routers worden toegepast.

Functie voor Catalyst LAN-Switch

IP-toegangslijst

De optie IP-toegangslijst beperkt de toegang tot het inkomende telnet en SNMP tot de switch van onbevoegde bron-IP-adressen. Syslogberichten en SNMP-traps worden ondersteund om een beheersysteem te informeren wanneer er sprake is van een schending of ongeautoriseerde toegang.

Een combinatie van de Cisco IOS veiligheidseigenschappen kan worden gebruikt om routers en Catalyst switches te beheren. Er moet een beveiligingsbeleid worden vastgesteld dat het aantal beheerscentra beperkt dat in staat is om toegang te krijgen tot de switches en routers.

Voor meer informatie over hoe om veiligheid op IP netwerken te verhogen, ga naar het Verhoogde Beveiliging op IP netwerken.

Boekhoudbeheer

Boekhoudbeheer is het proces dat wordt gebruikt om de parameters voor het gebruik van het netwerk te meten, zodat individuele of groepgebruikers op het netwerk op passende wijze kunnen worden gereguleerd met het oog op boekhouding of "chargeback". Net als bij prestatiemanagement is de eerste stap naar een passend boekhoudbeheer het meten van het gebruik van alle belangrijke netwerkbronnen. Het gebruik van netwerkbronnen kan worden gemeten met behulp van de functies voor Cisco NetFlow en Cisco IP-accounting. De analyse van de gegevens die via deze methoden worden verzameld, biedt inzicht in de huidige gebruikspatronen.

Een op gebruik gebaseerd boekhoudings- en facturatiesysteem is een essentieel onderdeel van

elke overeenkomst inzake serviceniveaus (SLA). Het biedt zowel een praktische manier om verplichtingen uit hoofde van een SLA vast te stellen als duidelijke gevolgen voor gedrag buiten de voorwaarden van de SLA.

De gegevens kunnen worden verzameld via sondes of Cisco NetFlow. Cisco biedt NetFlow Collector en NetFlow Analyzer toepassingen voor het verzamelen en analyseren van gegevens van routers en Catalyst switches. Aandeelware toepassingen zoals flow worden ook gebruikt om NetFlow-gegevens te verzamelen. Een continue meting van het gebruik van hulpbronnen kan informatie over de facturering opleveren, evenals een beoordeling van de aanhoudende eerlijke en optimale middelen. Sommige algemeen gebruikte oplossingen voor boekhoudbeheer omvatten:

- Bewijs-software

Strategie voor activering en gegevensverzameling van NetFlow

NetFlow (netwerkstroom) is een technologie voor het opvangen van de gegevens die vereist zijn voor netwerkplanning, controle en accounting. NetFlow dient te worden ingezet op edge/aggregation routerinterfaces voor serviceproviders of WAN access routerinterfaces voor ondernemingen.

Cisco Systems raadt een zorgvuldig geplande NetFlow-toepassing aan met NetFlow-services die op deze strategisch gelegen routers zijn geactiveerd. NetFlow kan geleidelijk worden ingezet (interface per interface) en strategisch (op goed gekozen routers) in plaats van NetFlow op elke router op het netwerk te implementeren. Cisco-personeel werkt met klanten om te bepalen op welke belangrijke routers en belangrijke interfaces NetFlow moeten worden geactiveerd op basis van de verkeersstroompatronen, netwerktopologie en architectuur van de klant.

Belangrijkste inzetoverwegingen zijn:

- NetFlow-services moeten worden gebruikt als een tool voor randmeting en toegangslijsten voor prestatiesversnelling en moeten niet worden geactiveerd op routers of routers die met zeer hoge CPU-gebruiksnelheden worden gebruikt.
- Begrijp de door toepassing aangestuurde gegevensverzamelingsvereisten. Boekhoudkundige toepassingen vereisen alleen van oorsprong en beëindiging van informatie over routerstromen, terwijl monitoringtoepassingen een uitgebreidere (gegevensintensieve) end-to-end weergave kunnen vereisen.
- Begrijp het effect van netwerktopologie en het routingbeleid op de strategie van de stroomverzameling. Vermijd bijvoorbeeld het verzamelen van dubbele stromen door NetFlow te activeren op belangrijke aggregation routers waar verkeer vandaan komt of eindigt en niet op backbone routers of intermediaire routers die dubbele weergave van dezelfde stroominformatie zouden bieden.
- Dienstverrichters in het *transitoriebedrijf* (die geen verkeer vervoeren dat niet van oorsprong is of eindigt op hun netwerk) mogen NetFlow-exportgegevens gebruiken om het gebruik van de netwerkhulpbronnen voor de boekhouding en de facturering te meten.

IP-accounting instellen

Ondersteuning van Cisco IP-accounting biedt basisfuncties voor IP-accounting. Door IP-accounting mogelijk te maken, kunnen gebruikers het aantal bytes en pakketten zien die door de

Cisco IOS-software zijn geschakeld op een bron- en IP-adresbasis. Alleen het IP-transitoverkeer wordt gemeten en alleen op uitgaande basis. Verkeer dat door de software wordt gegenereerd of dat in de software eindigt, wordt niet in de financieel administratieve statistieken opgenomen. Om een nauwkeurige boekhouding te kunnen voeren, onderhoudt de software twee boekhouddatabases: een actieve en een controlepuntendatabank.

Cisco IP-accounting ondersteuning biedt ook informatie die IP-verkeer identificeert dat IP-toegangslijsten niet haalt. Het identificeren van IP bron adressen die IP toegang schenden lijsten van mogelijke pogingen om veiligheid te breken. De gegevens geven ook aan dat de configuratie van de IP-toegangslijsten moet worden geverifieerd. Om deze optie beschikbaar te maken voor gebruikers, schakelt u IP accounting van toegangslijsten schendingen in met de **ip accounting-toegangsrechten-**opdracht. De gebruikers kunnen dan het aantal bytes en pakketten van één bron weergeven die geprobeerd hebben de beveiliging tegen de toegangslijst van het brondoelpaar te doorbreken. Standaard zal IP-accounting het aantal pakketten weergeven dat toegangslijsten heeft doorgegeven en is routeerd.

U kunt IP-accounting als volgt gebruiken voor elke interface in interfacemodi:

Opdracht	doel
ip-accounting	Toegang tot basis-IP-accounting.
schending van ip - boekhoudkundige toegangsrechten	IP-accounting met de mogelijkheid om IP-verkeer te identificeren dat geen IP-toegangslijsten bevat.

Om andere IP-accounting functies te configureren gebruikt u een of meer van de volgende opdrachten in mondiale configuratiemodus:

Opdracht	doel
ip-*drempelwaarde*	Stel het maximale aantal aan te maken boekingsposten in.
ip-accounting-lijst van *ip-adres vervanging*	Boekhoudinformatie voor hosts filteren.
ip-boekhouding-*omzettingen*	Beheer van het aantal transitobestanden dat in de IP-boekhoudingsdatabase zal worden opgeslagen.

Raadpleeg Cisco Technical Tips Convention voor informatie over conventies die in dit document gebruikt worden.