네트워크 관리 시스템:모범 사례 백서

목차

소개

ISO(International Organization for Standardization) 네트워크 관리 모델은 네트워크 관리의 5가지 기능 영역을 정의합니다.이 문서는 모든 기능 영역을 다룹니다.이 문서의 전반적인 목적은 현재의 관리 툴과 관행의 전반적인 효과를 높이기 위해 각 기능 영역에 대한 실용적인 권장 사항을 제공하는 것입니다.또한 향후 네트워크 관리 툴 및 기술을 구현하기 위한 설계 지침을 제공합니다.

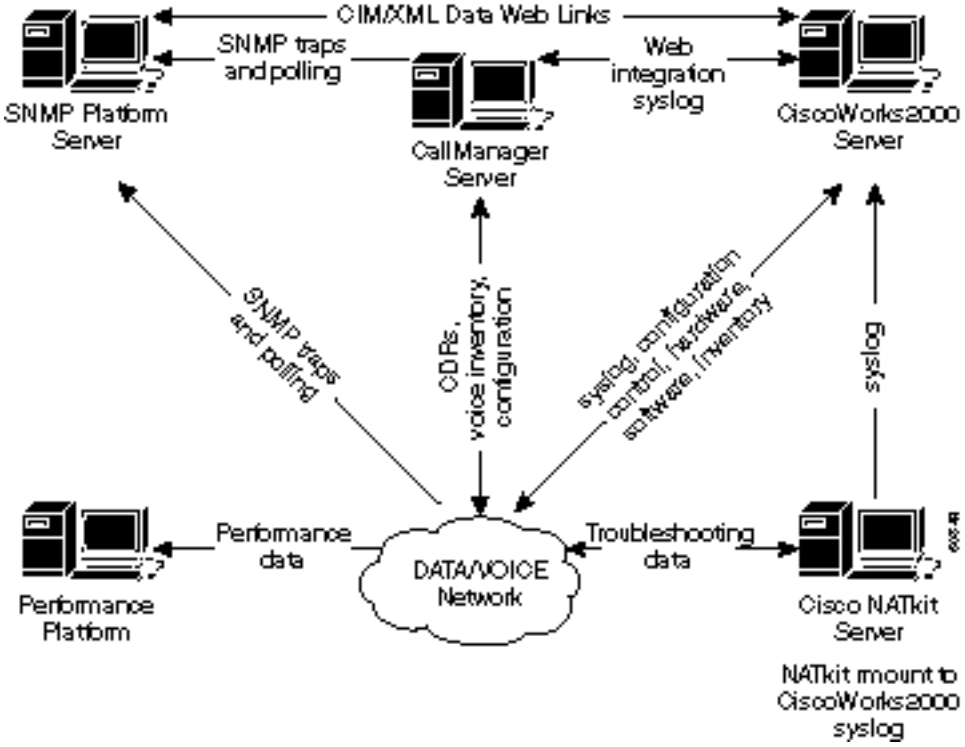
네트워크 관리

ISO 네트워크 관리 모델의 5가지 기능 영역이 아래에 나열되어 있습니다.

- Fault Management(결함 관리) - 네트워크에서 발생한 결함을 탐지, 격리, 통지 및 수정합니다.
- Configuration Management(컨피그레이션 관리) - 컨피그레이션 파일 관리, 인벤토리 관리, 소프트웨어 관리와 같은 네트워크 디바이스의 컨피그레이션 부분입니다.
- 성능 관리 - 전체 성능을 적정한 수준으로 유지할 수 있도록 다양한 성능 측면을 모니터링하고 측정합니다.

- 보안 관리 - 권한이 있는 개인에게 네트워크 디바이스 및 기업 리소스에 대한 액세스를 제공합니다.
- Accounting Management - 네트워크 리소스의 사용 정보입니다.

다음 다이어그램은 Cisco Systems가 데이터 네트워크 관리를 위한 최소 솔루션이라고 생각하는 참조 아키텍처를 보여줍니다.이 아키텍처에는 VoIP(Voice over Internet Protocol)를 관리하려는 사용자를 위한 Cisco CallManager 서버가 포함되어 있습니다.다이어그램은 CallManager 서버를 NMS 토폴로지에 통합하는 방법을 보여줍니다.



네트워크 관리 아키텍처는 다음과 같습니다.

- 장애 관리를 위한 SNMP(Simple Network Management Protocol) 플랫폼
- 장기적인 성능 관리 및 추세 분석을 위한 성능 모니터링 플랫폼
- 구성 관리, syslog 수집, 하드웨어 및 소프트웨어 인벤토리 관리를 위한 CiscoWorks2000 서버

일부 SNMP 플랫폼은 CIM/XML(Common Information Model/eXtensible Markup Language) 메서드를 사용하여 CiscoWorks2000 서버와 직접 데이터를 공유할 수 있습니다.CIM은 네트워크/엔터프라이즈 환경에서 전체 관리 정보를 설명하기 위한 구현 중립적 스키마의 공통 데이터 모델입니다.CIM은 사양과 스키마로 구성됩니다.세부 항목은 SNMP MIB 또는 Desktop Management DMTF MIF(Task Force Management Information Files)와 같은 다른 관리 모델과의 통합에 대한 세부 정보를 정의하는 반면, 스키마는 실제 모델 설명을 제공합니다.

XML은 구조화된 데이터를 텍스트 형식으로 표현하는 데 사용되는 마크업 언어입니다.XML의 구체적인 목표는 SGML의 설명적 기능을 최대한 유지하면서 복잡성을 최대한 제거하는 것입니다.XML은 HTML과 개념적으로 유사하지만 HTML은 문서에 대한 그래픽 정보를 전달하는 데 사용되지만 XML은 문서에서 구조화된 데이터를 나타내는 데 사용됩니다.

Cisco의 고급 서비스 고객은 사전 대응적 모니터링 및 문제 해결을 위한 Cisco의 NATkit 서버도 포함할 것입니다.NATkit 서버는 CiscoWorks2000 서버에 있는 데이터에 대한 원격 디스크 마운트(rmount) 또는 FTP(파일 전송 프로토콜) 액세스를 가질 수 있습니다.

Internetworking Technology Overview(인터네트워킹 기술 개요)의 Network Management Basics(*네트워크 관리 기본 사항*) 장은 네트워크 관리 기본 사항에 대한 자세한 개요를 제공합니다.

결함 관리

장애 관리의 목표는 네트워크를 효과적으로 실행하기 위해 네트워크 문제를 탐지, 로깅, 사용자에게 알리고(가능한 한) 자동으로 해결하는 것입니다.결함은 다운타임이나 허용되지 않는 네트워크 저하를 일으킬 수 있으므로, 결함 관리는 아마도 ISO 네트워크 관리 요소 중 가장 널리 구현된 것일 것입니다.

네트워크 관리 플랫폼

기업에 구축된 네트워크 관리 플랫폼은 멀티벤더 네트워크 요소로 구성된 인프라를 관리합니다.이 플랫폼은 네트워크의 네트워크 요소에서 이벤트를 수신하고 처리합니다.서버 및 기타 중요 리소스의 이벤트를 관리 플랫폼으로 전달할 수도 있습니다.다음과 같이 일반적으로 사용 가능한 기능이 표준 관리 플랫폼에 포함되어 있습니다.

- 네트워크 검색
- 네트워크 요소의 토폴로지 매핑
- 이벤트 처리기
- 성능 데이터 수집기 및 작성자
- 관리 데이터 브라우저

네트워크 관리 플랫폼은 인프라에서 결함을 탐지하는 네트워크 운영을 위한 기본 콘솔로 볼 수 있습니다.모든 네트워크에서 문제를 신속하게 탐지하는 기능은 매우 중요합니다.네트워크 운영 담당자는 그래픽 네트워크 맵에 의존하여 라우터 및 스위치와 같은 중요한 네트워크 요소의 운영 상태를 표시할 수 있습니다.

HP OpenView, Computer Associates Unicenter 및 SUN Solstice와 같은 네트워크 관리 플랫폼은 네트워크 장치를 검색할 수 있습니다.각 네트워크 디바이스는 관리 플랫폼 콘솔의 그래픽 요소로 표시됩니다.그래픽 요소의 다양한 색상은 네트워크 장치의 현재 작동 상태를 나타냅니다.네트워크 디바이스는 SNMP 트랩이라는 알림을 네트워크 관리 플랫폼으로 전송하도록 구성할 수 있습니다.알림을 받으면 네트워크 디바이스를 나타내는 그래픽 요소가 수신한 알림의 심각도에 따라 다른 색상으로 변경됩니다.일반적으로 이벤트라고 하는 알림이 로그 파일에 저장됩니다.특히 Cisco 디바이스의 다양한 알림이 올바르게 해석되도록 SNMP 플랫폼에 최신 Cisco MIB(Management Information Base) 파일을 로드해야 합니다.

Cisco는 다양한 네트워크 디바이스를 관리하기 위한 MIB 파일을 게시합니다.Cisco MIB 파일은 cisco.com 웹 사이트에 있으며 다음 정보를 포함합니다.

- SNMPv1 형식으로 게시된 MIB 파일
- SNMPv2 형식으로 게시된 MIB 파일
- Cisco 디바이스에서 지원되는 SNMP 트랩
- Cisco 현재 SNMP MIB 개체에 대한 OID

여러 네트워크 관리 플랫폼이 지리적으로 분산된 여러 사이트를 관리할 수 있습니다.이는 원격 사이트의 관리 콘솔과 기본 사이트의 관리 스테이션 간에 관리 데이터를 교환함으로써 이루어집니다.분산 아키텍처의 주요 장점은 관리 트래픽을 줄여 더 효과적인 대역폭 사용을 제공한다는 것입니다.또한 분산 아키텍처를 통해 직원은 시스템을 사용하여 원격 사이트에서 네트워크를 로컬로 관리할 수 있습니다.

관리 플랫폼의 최신 개선 사항은 웹 인터페이스를 사용하여 네트워크 요소를 원격으로 관리할 수 있다는 것입니다.이러한 개선을 통해 개별 사용자 스테이션에서 관리 플랫폼에 액세스하기 위한 특별한 클라이언트 소프트웨어가 필요하지 않습니다.

일반적인 기업은 서로 다른 네트워크 요소로 구성됩니다.그러나 네트워크 요소를 효과적으로 관리하기 위해 일반적으로 각 디바이스에는 공급업체별 요소 관리 시스템이 필요합니다.따라서 중복된 관리 스테이션은 동일한 정보에 대해 네트워크 요소를 폴링할 수 있습니다.여러 시스템에서 수집한 데이터는 별도의 데이터베이스에 저장되므로 사용자의 관리 오버헤드가 발생합니다.이러한 제한 때문에 네트워킹 및 소프트웨어 공급업체는 관리 플랫폼과 요소 관리 시스템 간에 관리 데이터를 쉽게 교환할 수 있도록 CORBA(Common Object Request Broker Architecture) 및 CIM(Computer-Integrated Manufacturing)과 같은 표준을 채택해야 했습니다.벤더가 관리 시스템 개발 표준을 채택함에 따라 사용자는 인프라 구축 및 관리에 있어서 상호운용성과 비용 절감을 기대할 수 있습니다.

CORBA는 이기종 분산 환경에서 그리고 프로그래머에게 투명한 방식으로 객체 간의 상호 운용성을 제공하는 시스템을 지정합니다.이 설계는 OMG(Object Management Group) 객체 모델을 기반으로 합니다.

인프라 문제 해결

TFTP(Trivial File Transfer Protocol) 및 시스템 로그(syslog) 서버는 네트워크 운영 시 문제 해결 인프라의 중요한 구성 요소입니다.TFTP 서버는 주로 네트워크 디바이스에 대한 컨피그레이션 파일 및 소프트웨어 이미지를 저장하는 데 사용됩니다.라우터와 스위치는 시스템 로그 메시지를 syslog 서버로 전송할 수 있습니다.이 메시지는 문제 발생 시 문제 해결 기능을 용이하게 합니다.Cisco 지원 담당자는 근본 원인 분석을 수행하기 위해 syslog 메시지가 필요한 경우가 있습니다.

CiscoWorks2000 Resource Management Essentials(Essentials) 분산 syslog 수집 기능을 사용하면 원격 사이트에서 여러 UNIX 또는 NT 수집 스테이션을 구축하여 메시지 수집 및 필터링을 수행할 수 있습니다.필터는 어떤 syslog 메시지가 주 Essentials 서버로 전달될지 지정할 수 있습니다.분산형 수집을 구현할 경우 주 syslog 서버로 전달되는 메시지의 수가 감소합니다.

결함 감지 및 알림

결함 관리의 목적은 네트워크에서 발생한 결함을 탐지, 격리, 통지 및 수정하는 것입니다.네트워크 디바이스는 시스템에서 결함이 발생할 경우 관리 스테이션에 알림을 보낼 수 있습니다.효과적인 결함 관리 시스템은 여러 하위 시스템으로 구성됩니다.디바이스에서 SNMP 트랩 메시지, SNMP 폴링, RMON(원격 모니터링) 임계값 및 syslog 메시지를 전송할 때 장애 탐지가 수행됩니다.관리 시스템은 결함이 보고되고 시정 조치가 수행될 때 최종 사용자에게 알립니다.

네트워크 디바이스에서 트랩을 일관되게 활성화해야 합니다.라우터 및 스위치용 새로운 Cisco IOS 소프트웨어 릴리스에서 추가 트랩이 지원됩니다.트랩의 적절한 디코딩을 위해 컨피그레이션 파일을 확인하고 업데이트하는 것이 중요합니다.Cisco ANS(Assured Network Services) 팀을 통해 구성된 트랩을 정기적으로 검토하여 네트워크에서 효과적인 장애 탐지를 보장합니다.

다음 표에는 Cisco Catalyst LAN(Local Area Network) 스위치에서 지원되고, Cisco Catalyst LAN(Local Area Network) 스위치의 결함 상태를 모니터링하는 데 사용할 수 있는 CISCO-STACK-MIB 트랩이 나열되어 있습니다.

트랩	설명
모듈 위로	에이전트 엔터티에서 이 MIB의 **moduleStatus** 개체가 해당 모듈 중 하나에 대해 **ok(2)** 상태로 전환되었음을 감지했습니다.
모듈 다운	에이전트 엔터티에서 이 MIB의 *moduleStatus* 개체가 해당 모듈 중 하나에 대해 **ok(2)** 상태에서 벗어났음을 감지했습니다.
섀시	에이전트 엔티티에서 이 MIB의

alarm On	chassisTempAlarm, chassisMinorAlarm 또는 *chassisMajorAlarm* 개체가 **on(2) 상태로 전환되었음을** 감지했습니다.chassisMajorAlarm은 다음 조건 중 하나가 있음을 나타냅니다. • 모든 전압 장애 • 동시 온도 및 팬 고장 • 100% 전원 공급 장치 장애(2/2 또는 1/1) • EEPROM(전기적으로 삭제 가능한 프로그래밍 가능 읽기 전용 메모리) 실패 • 비휘발성 RAM(NVRAM) 오류 • MCP 통신 실패 • 알 수 없는 NMP 상태 chassisMinorAlarm은 다음 조건 중 하나가 있음을 나타냅니다. • 온도 경보 • 팬 장애 • 부분 전원 공급 장치 장애(2개 중 1개) • 호환되지 않는 유형의 전원 공급 장치 2개
섀시 alarm Off	에이전트 엔티티에서 이 MIB의 *chassisTempAlarm*, chassisMinorAlarm 또는 chassisMajorAlarm 개체가 **off(1) 상태로 전환되었음을** 감지했습니다.

환경 모니터(환경 모니터링) 트랩은 CISCO-ENVMON-MIB 트랩에 정의됩니다.환경 임계값이 초과되면 환경 트랩은 Cisco 기업별 환경 모니터 알림을 전송합니다.envmon을 사용하면 특정 환경 트랩 유형을 활성화하거나 환경 모니터 시스템의 모든 트랩 유형을 허용할 수 있습니다.옵션을 지정하지 않으면 모든 환경 유형이 활성화됩니다.다음 값 중 하나 이상이 될 수 있습니다.

- 전압 - 지정된 테스트 지점에서 측정한 전압이 테스트 지점의 정상 범위(예: 경고, 한계 또는 종료 단계)를 벗어나는 경우 ciscoEnvMonVoltageNotification이 전송됩니다.
- shutdown - 환경 모니터가 테스트 지점이 위험 상태에 도달하고 종료를 시작하려는 경우 ciscoEnvMonShutdownNotification이 전송됩니다.
- supply - 예비 전원 공급 장치(extenant인 경우)에 장애가 발생하면 ciscoEnvMonRedundantSupplyNotification이 전송됩니다.
- fan - 팬 어레이(extenant)의 팬 중 하나에 장애가 발생하면 ciscoEnvMonFanNotification이 전송됩니다.
- 온도 - 지정된 테스트 지점에서 측정한 온도가 테스트 지점의 정상 범위(예: 경고, 한계 또는 종료 단계)를 벗어나면 ciscoEnvMonTemperatureNotification이 전송됩니다.

네트워크 요소의 장애 감지 및 모니터링은 디바이스 레벨에서 프로토콜 및 인터페이스 레벨로 확장할 수 있습니다.네트워크 환경의 경우 장애 모니터링에는 VLAN(Virtual Local Area Network), ATM(Asynchronous Transfer Mode), 물리적 인터페이스의 결함 표시 등이 포함될 수 있습니다.프로토콜 레벨 결함 관리 구현은 CiscoWorks2000 Campus Manager와 같은 요소 관리 시스템을 사용하여 사용할 수 있습니다.Campus Manager의 TrafficDirector 애플리케이션은 Catalyst 스위치에서 mini-RMON 지원을 활용하는 스위치 관리에 중점을 둡니다.

네트워크 요소의 수와 네트워크 문제의 복잡성이 증가함에 따라 서로 다른 네트워크 이벤트(syslog, trap, log 파일)와 상관관계를 분석할 수 있는 이벤트 관리 시스템을 고려할 수 있습니다.이벤트 관리 시스템의 이 아키텍처는 MOM(Manager of Managers) 시스템과 유사합니다.잘 설계된 이벤트 관리 시스템을 통해 NOC(Network Operations Center) 담당자는 사전 대응적이고 효과적으로 네트워크 문제를 탐지하고 진단할 수 있습니다.이벤트 우선 순위 지정 및 억제 기능을 통해 네트워크 운영 담

당자는 중요한 네트워크 이벤트에 집중하고, Cisco Info Center를 비롯한 여러 이벤트 관리 시스템을 조사하고, 실행 가능성 분석을 수행하여 해당 시스템의 기능을 완전히 살펴볼 수 있습니다.자세한 내용은 Cisco Info Center를 참조하십시오.

사전 예방적 장애 모니터링 및 알림

RMON 경보 및 이벤트는 RMON 사양에 정의된 두 개의 그룹입니다.일반적으로 관리 스테이션은 특정 변수의 상태 또는 값을 확인하기 위해 네트워크 디바이스에서 폴링을 수행합니다.예를 들어, 관리 스테이션은 라우터를 폴링하여 CPU(Central Processing Unit) 사용률을 확인하고 값이 구성된 임계값에 도달하면 이벤트를 생성합니다.이 방법은 네트워크 대역폭을 낭비하고 폴링 간격에 따라 실제 임계값을 초과할 수도 있습니다.

RMON 경보 및 이벤트를 통해 네트워크 디바이스가 임계값 증가 및 감소를 위해 자체 모니터링하도록 구성됩니다.미리 정의된 시간 간격으로 네트워크 디바이스는 변수의 샘플을 가져와 임계값과 비교합니다.실제 값이 구성된 임계값을 초과하거나 미달할 경우 SNMP 트랩을 관리 스테이션으로 전송할 수 있습니다.RMON 경보 및 이벤트 그룹은 중요한 네트워크 장치를 사전 대응적으로 관리하는 방법을 제공합니다.

Cisco Systems는 중요한 네트워크 장치에 RMON 경보 및 이벤트를 구현할 것을 권장합니다.모니터링되는 변수에는 CPU 사용률, 버퍼 오류, 입력/출력 삭제 또는 정수 유형의 변수가 포함될 수 있습니다.Cisco IOS Software Release 11.1(1)부터 모든 라우터 이미지는 RMON 경보 및 이벤트 그룹을 지원합니다.

RMON 경보 및 이벤트 구현에 대한 자세한 내용은 RMON Alarm and Event Implementation 섹션을 참조하십시오.

RMON 메모리 제약 조건

RMON 메모리 사용량은 통계, 기록, 경보 및 이벤트와 관련된 모든 스위치 플랫폼에서 일정합니다.RMON은 RMON 에이전트(이 경우 스위치)에 내역과 통계를 저장하기 위해 버킷이라고 하는 것을 사용합니다. 버킷 크기는 RMON 프로브(SwitchProbe 디바이스) 또는 RMON 애플리케이션(TrafficDirector 툴)에 정의된 다음 설정할 스위치로 전송됩니다.

mini-RMON을 지원하려면 약 450K의 코드 공간이 필요합니다(예: RMON 그룹 4개).통계, 기록, 경보 및 이벤트) RMON에 대한 동적 메모리 요구 사항은 런타임 컨피그레이션에 따라 달라지기 때문입니다.

다음 표에서는 각 mini-RMON 그룹에 대한 런타임 RMON 메모리 사용량 정보를 정의합니다.

RMON 그룹 정의	사용된 DRAM 공간	참고
통계	스위치드 이더넷/고속 이더넷 포트당 140바이트	포트당
기록	50버킷의 경우 3.6K *	각 추가 버킷은 56바이트를 사용합니다.
경보 및 이벤트	경보당 2.6K 및 해당 이벤트 항목	포트당 경보 수

*RMON은 RMON 에이전트(예: 스위치)에 내역과 통계를 저장하기 위해 버킷이라고 하는 것을 사용합니다.

RMON 경보 및 이벤트 구현

사용자는 장애 관리 솔루션의 일부로 RMON을 통합함으로써 잠재적인 문제가 발생하기 전에 미리 네트워크를 모니터링할 수 있습니다.예를 들어 수신된 브로드캐스트 패킷 수가 크게 증가하면 CPU 사용률이 증가할 수 있습니다.사용자는 RMON 경보 및 이벤트를 구현하여 임계값을 설정하여 수신된 브로드캐스트 패킷 수를 모니터링하고 구성된 임계값에 도달하면 SNMP 트랩을 통해 SNMP 플랫폼에 알림을 보낼 수 있습니다.RMON 경보 및 이벤트는 동일한 목표를 달성하기 위해 SNMP 플랫폼에서 일반적으로 수행하는 과도한 폴링을 제거합니다.

RMON 경보 및 이벤트를 구성하는 두 가지 방법을 사용할 수 있습니다.

- 명령줄 인터페이스(CLI)
- SNMP 세트

다음 샘플 절차에서는 인터페이스에서 수신된 브로드캐스트 패킷 수를 모니터링하기 위해 임계값을 설정하는 방법을 보여줍니다.이 섹션 끝에 있는 show interface 명령 예에 표시된 것과 동일한 카운터가 이러한 절차에 사용됩니다.

명령줄 인터페이스 예

CLI 인터페이스를 사용하여 RMON 경보 및 이벤트를 구현하려면 다음 단계를 수행합니다.

1. ifTable MIB를 확인하여 이더넷 0과 연결된 인터페이스 인덱스를 찾습니다.
   ```
   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. 모니터링할 CLI 필드와 연결된 OID를 가져옵니다.이 예에서 '브로드캐스트'의 OID는 1.3.6.1.2.1.2.2.1.12입니다. 특정 MIB 변수에 대한 Cisco OID는 cisco.com 웹 사이트에서 사용할 수 있습니다.
3. 임계값 및 이벤트 설정을 위한 다음 매개변수를 결정합니다.상승 및 낙하 임계값샘플링 유형(절대 또는 델타)샘플링 간격임계값에 도달했을 때의 작업이 예에서는 이더넷 0에서 수신된 브로드캐스트 패킷 수를 모니터링하기 위해 임계값을 설정하고 있습니다. 수신된 브로드캐스트 패킷 수가 60초 샘플 사이의 500보다 크면 트랩이 생성됩니다.가져온 샘플 간에 입력 브로드캐스트 수가 증가하지 않으면 임계값이 다시 활성화됩니다.**참고:** 이러한 명령 매개변수에 대한 자세한 내용은 특정 Cisco IOS 버전에 대한 RMON 경보 및 이벤트 명령에 대한 Cisco Connection Online(CCO) 설명서를 참조하십시오.
4. 다음 CLI 명령을 사용하여 임계값에 도달할 때 전송된 트랩(RMON 이벤트)을 지정합니다(Cisco IOS 명령은 굵은 글꼴로 표시됨).**rmon 이벤트 1 트랩 게이트웨이 설명 "High Broadcast on Ethernet 0" 소유자 ciscormon 이벤트 2 로그 설명 "일반 브로드캐스트 received on ethernet 0" 소유자 cisco**
5. 다음 CLI 명령을 사용하여 임계값 및 관련 매개변수(RMON alarm)를 지정합니다.**rmon 경보 1 ifEntry.12.1 60 델타 rising-threshold 500 1하락 임계값 0 2 소유자 cisco**
6. SNMP를 사용하여 이러한 테이블을 폴링하여 디바이스에서 eventTable 항목이 생성되었는지 확인합니다.
   ```
   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. SNMP를 사용하여 이러한 테이블을 폴링하여 alarmTable 항목이 설정되었는지 확인합니다.

```
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 예

SNMP SET 작업과 함께 RMON 경보 및 이벤트를 구현하려면 다음 단계를 완료하십시오.

1. 다음 SNMP SET 작업을 사용하여 임계값에 도달할 때 전송된 트랩(RMON 이벤트)을 지정합니다.

```
# 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. 다음 SNMP SET 작업을 사용하여 임계값 및 관련 매개변수(RMON 경보)를 지정합니다.

```
# 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. 이 테이블을 폴링하여 디바이스에서 eventTable 항목이 만들어졌는지 확인합니다.

```
% 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. 이러한 테이블을 폴링하여 alarmTable 항목이 설정되었는지 확인합니다.

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

[show interface]

이 예는 **show interface** 명령의 결과입니다.

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
```

컨피그레이션 관리

컨피그레이션 관리의 목표는 다양한 버전의 하드웨어 및 소프트웨어 요소의 네트워크 운영에 미치는 영향을 추적하고 관리할 수 있도록 네트워크 및 시스템 컨피그레이션 정보를 모니터링하는 것입니다.

구성 표준

네트워크 디바이스가 점점 더 많이 구축됨에 따라 네트워크 디바이스의 위치를 정확하게 파악하는 것이 중요합니다.이 위치 정보는 네트워크 문제가 발생할 때 리소스를 디스패치하는 담당자에게 의미 있는 자세한 설명을 제공해야 합니다.네트워크 문제가 발생할 경우 신속하게 해결하려면 해당 장치를 담당하는 담당자 또는 부서의 연락처 정보를 확인해야 합니다.연락처 정보에는 전화 번호와 담당자 또는 부서의 이름이 포함되어야 합니다.

디바이스 이름에서 개별 인터페이스에 이르기까지 네트워크 디바이스에 대한 명명 규칙을 계획하고 컨피그레이션 표준의 일부로 구현해야 합니다.잘 정의된 명명 규칙을 통해 담당자는 네트워크 문제를 해결할 때 정확한 정보를 제공할 수 있습니다.디바이스에 대한 명명 규칙은 지리적 위치, 건물 이름, 층 등을 사용할 수 있습니다.인터페이스 명명 규칙의 경우 포트가 연결된 세그먼트, 연결 허브 이름 등을 포함할 수 있습니다.직렬 인터페이스에서는 실제 대역폭, DLCI(Local Data Link Connection Identifier) 번호(Frame Relay인 경우), 대상, 통신 사업자가 제공하는 회선 ID 또는 정보를 포함해야 합니다.

구성 파일 관리

기존 네트워크 디바이스 요구 사항에 대해 새 컨피그레이션 명령을 추가할 경우, 실제 구현이 이루어지기 전에 무결성 명령을 확인해야 합니다.잘못 구성된 네트워크 디바이스는 네트워크 연결 및 성능에 심각한 영향을 미칠 수 있습니다.불일치 또는 비호환성 문제를 방지하려면 컨피그레이션 명

령 매개변수를 선택해야 합니다.Cisco 엔지니어와 정기적으로 구성을 철저하게 검토하는 것이 좋습니다.

완벽한 기능을 갖춘 CiscoWorks2000 Essentials를 사용하면 라우터와 Cisco Catalyst 스위치의 구성 파일을 자동으로 백업할 수 있습니다.Essentials의 보안 기능을 사용하여 컨피그레이션 변경 시 인증을 수행할 수 있습니다.변경 감사 로그를 사용하여 변경 사항 및 변경 사항을 발급하는 개인의 사용자 이름을 추적할 수 있습니다.여러 디바이스의 컨피그레이션 변경 시 다음 두 가지 옵션을 사용할 수 있습니다.현재 버전의 CiscoWorks2000 Essentials 또는 cwconfig 스크립트에서 웹 기반 NetConfig를 제공합니다.사전 정의 또는 사용자 정의 템플릿을 사용하여 CiscoWorks2000 Essentials를 사용하여 구성 파일을 다운로드하고 업로드할 수 있습니다.

이러한 기능은 CiscoWorks2000 Essentials의 구성 관리 도구를 사용하여 수행할 수 있습니다.

- Essentials 컨피그레이션 아카이브에서 디바이스 또는 여러 디바이스로 컨피그레이션 파일 푸시
- 디바이스에서 Essentials 아카이브로 컨피그레이션 가져오기
- 아카이브에서 최신 컨피그레이션을 추출하여 파일에 기록
- 파일에서 컨피그레이션을 가져오고 디바이스에 컨피그레이션을 푸시합니다.
- Essentials 아카이브의 마지막 두 구성 비교
- 아카이브에서 지정된 날짜 또는 버전보다 오래된 구성 삭제
- 시작 컨피그레이션을 실행 중인 컨피그레이션에 복사

인벤토리 관리

대부분의 네트워크 관리 플랫폼의 검색 기능은 네트워크에 있는 디바이스의 동적 목록을 제공하기 위한 것입니다.네트워크 관리 플랫폼에 구현된 검색 엔진을 사용해야 합니다.

인벤토리 데이터베이스는 네트워크 디바이스에 대한 자세한 컨피그레이션 정보를 제공합니다.일반적인 정보에는 하드웨어, 설치된 모듈, 소프트웨어 이미지, 마이크로코드 수준 등의 모델이 포함됩니다.이러한 모든 정보는 소프트웨어 및 하드웨어 유지 보수 등의 작업을 완료하는 데 매우 중요합니다.검색 프로세스에서 수집하는 네트워크 디바이스의 최신 목록을 마스터 목록으로 사용하여 SNMP 또는 스크립팅을 사용하여 인벤토리 정보를 수집할 수 있습니다.CiscoWorks2000 Campus Manager에서 CiscoWorks2000 Essentials의 인벤토리 데이터베이스로 디바이스 목록을 가져와서 Cisco Catalyst 스위치의 최신 인벤토리를 얻을 수 있습니다.

소프트웨어 관리

네트워크 디바이스에서 Cisco IOS 이미지를 성공적으로 업그레이드하려면 메모리, 부트 ROM, 마이크로코드 레벨 등의 요구 사항을 세부적으로 분석해야 합니다.이러한 요구 사항은 일반적으로 Cisco 웹 사이트에서 릴리스 정보 및 설치 가이드 형태로 문서화되어 제공됩니다.Cisco IOS를 실행하는 네트워크 디바이스를 업그레이드하는 프로세스에는 CCO에서 올바른 이미지를 다운로드하고, 현재 이미지를 백업하고, 모든 하드웨어 요구 사항을 충족하는지 확인한 다음, 새 이미지를 디바이스에 로드하는 작업이 포함됩니다.

일부 조직에서는 디바이스 유지 관리를 완료하는 업그레이드 기간이 상당히 제한됩니다.리소스가 제한된 대규모 네트워크 환경에서는 업무 시간 이후에 소프트웨어 업그레이드를 예약하고 자동화해야 할 수도 있습니다.이 절차는 Expect와 같은 스크립팅 언어 또는 이러한 작업을 수행하기 위해 특별히 작성된 애플리케이션을 사용하여 완료할 수 있습니다.

또 다른 소프트웨어 유지 보수가 필요할 경우 분석 단계에서 Cisco IOS 이미지 및 마이크로코드 버전 같은 네트워크 디바이스의 소프트웨어에 대한 변경 사항을 추적해야 합니다.수정 이력 보고서를

즉시 사용할 수 있으므로 업그레이드를 수행하는 사람은 호환되지 않는 이미지나 마이크로코드를 네트워크 디바이스로 로드할 위험을 최소화할 수 있습니다.

성능 관리

서비스 수준 계약

SLA(Service Level Agreement)는 네트워크 서비스의 예상 성능 수준에 대한 서비스 제공자와 고객 간의 서면 계약입니다.SLA는 공급자와 고객 간에 합의된 메트릭으로 구성됩니다.메트릭스에 대해 설정된 값은 현실적이고 의미 있고 양쪽에 측정 가능해야 합니다.

성능 수준을 측정하기 위해 네트워크 디바이스에서 다양한 인터페이스 통계를 수집할 수 있습니다 .이러한 통계는 SLA에 메트릭으로 포함될 수 있습니다.입력 대기열 삭제, 출력 대기열 삭제 및 무시된 패킷과 같은 통계는 성능 관련 문제를 진단하는 데 유용합니다.

디바이스 레벨에서 성능 메트릭에는 CPU 사용률, 버퍼 할당(빅 버퍼, 중간 버퍼, 실패, 적중률) 및 메모리 할당이 포함될 수 있습니다.특정 네트워크 프로토콜의 성능은 네트워크 디바이스의 버퍼 가용성과 직접 관련이 있습니다.디바이스 레벨 성능 통계 측정은 상위 레벨 프로토콜의 성능을 최적화하는 데 매우 중요합니다.

라우터와 같은 네트워크 장치는 DLSW(Data Link Switching Workgroup), RSRB(Remote Source Route Bridging), AppleTalk 등과 같은 다양한 상위 계층 프로토콜을 지원합니다.프레임 릴레이, ATM, ISDN(Integrated Services Digital Network) 등을 포함한 WAN(Wide-Area Network) 기술의 성능 통계를 모니터링하고 수집할 수 있습니다.

성능 모니터링, 측정 및 보고

SNMP를 사용하여 인터페이스, 디바이스 및 프로토콜 레벨에서 서로 다른 성능 메트릭을 정기적으로 수집해야 합니다.네트워크 관리 시스템의 폴링 엔진을 데이터 수집 용도로 사용할 수 있습니다 .대부분의 네트워크 관리 시스템은 폴링된 데이터를 수집, 저장 및 제공할 수 있습니다.

엔터프라이즈 환경을 위한 성능 관리 요구 사항을 해결하기 위해 다양한 솔루션이 시장에 제공되고 있습니다.이러한 시스템은 네트워크 디바이스 및 서버에서 데이터를 수집, 저장 및 제공할 수 있습니다.대부분의 제품에 대한 웹 기반 인터페이스를 통해 기업 내 어디서든 성능 데이터에 액세스할 수 있습니다.일반적으로 구축된 성능 관리 솔루션 중 일부는 다음과 같습니다.

- InfoVista VistaView
- SAS IT 서비스 비전
- 트리너지 트렌드

위의 제품을 평가하면 각기 다른 사용자의 요구 사항을 충족하는지 여부가 결정됩니다.일부 공급업체는 네트워크 관리 및 시스템 관리 플랫폼과의 통합을 지원합니다.예를 들어 InfoVista는 BMC Patrol Agent를 지원하여 애플리케이션 서버의 주요 성능 통계를 제공합니다.각 제품에는 기본 제품과 다른 가격 모델과 기능이 있습니다.일부 솔루션에서 NetFlow, RMON, Cisco IOS ASR(Service Assurance Agent/Response Time Reporter) 등의 Cisco 디바이스에 대한 성능 관리 기능을 지원할 수 있습니다.최근 Concord는 성능 데이터를 수집하고 보는 데 사용할 수 있는 Cisco WAN 스위치에 대한 지원을 추가했습니다.

Cisco IOS의 CSAA/RTR(Service Assurance Agent)/RTR(Response Time Reporter) 기능을 사용하여 IP 디바이스 간의 응답 시간을 측정할 수 있습니다.CSAA가 구성된 소스 라우터는 라우터 또는 IP 디바이스일 수 있는 대상 IP 디바이스에 대한 응답 시간을 측정할 수 있습니다.응답 시간은 소스와 대상 사이 또는 경로를 따라 각 홉에 대해 측정할 수 있습니다.응답 시간이 미리 정의된 임계값을

초과할 경우 관리 콘솔에 알림을 보내도록 SNMP 트랩을 구성할 수 있습니다.

Cisco IOS의 최근 개선 사항은 CSAA의 기능을 확장하여 다음을 측정합니다.

- HTTP(HyperText Transfer Protocol) 서비스 성능DNS(Domain Name System) 조회 TCP(Transmission Control Protocol) 연결HTTP 트랜잭션 시간
- VoIP(Voice over IP) 트래픽의 패킷 간 지연 변화(지터)
- 특정 QoS(Quality of Service)에 대한 엔드포인트 간 응답 시간IP Type of Service(ToS) 비트
- CSAA에서 생성한 패킷을 사용한 패킷 손실

Cisco IPM(Internetwork Performance Monitor) 애플리케이션을 사용하여 라우터에서 CSAA 기능을 구성할 수 있습니다.CSAA/RTR은 Cisco IOS 소프트웨어의 모든 기능 집합에는 포함되어 있지 않습니다.IPM에서 성능 통계를 수집하는 데 사용하는 디바이스에 CSAA/RTR을 지원하는 Cisco IOS 소프트웨어 릴리스의 릴리스가 설치되어 있어야 합니다.CSAA/RTR/IPM을 지원하는 Cisco IOS 버전에 대한 요약은 IPM FAQ 웹 사이트를 참조하십시오.

IPM에 대한 추가 정보에는 다음이 포함됩니다.

- IPM 개요
- 서비스 보증 에이전트

성능 분석 및 튜닝

사용자 트래픽이 크게 증가하여 네트워크 리소스에 대한 수요가 증가했습니다.네트워크 관리자는 일반적으로 네트워크에서 실행 중인 트래픽 유형에 대해 제한된 보기를 갖습니다.사용자 및 애플리케이션 트래픽 프로파일링은 네트워크의 트래픽에 대한 자세한 보기를 제공합니다.RMON 프로브와 NetFlow라는 두 가지 기술을 통해 트래픽 프로필을 수집할 수 있습니다.

RMON

RMON 표준은 에이전트가 SNMP를 통해 중앙 스테이션(관리 콘솔)과 통신하는 분산 아키텍처에 구축되도록 설계되었습니다.RFC 1757 RMON 표준은 모니터링 기능을 이더넷 토폴로지를 지원하기 위해 9개의 그룹으로 구성하고 토큰 링 고유 매개 변수를 위해 RFC 1513에 10번째 그룹을 추가합니다.고속 이더넷 링크 모니터링은 RFC 1757 표준의 프레임워크에서 제공되며 FDDI(Fiber-Distributed Data Interface) 링 모니터링은 RFC 1757 및 RFC 1513 프레임워크에서 제공됩니다.

새로운 RFC 2021 RMON 사양은 MAC(Media Access Control) 레이어를 넘어 네트워크 및 애플리케이션 레이어에 대한 원격 모니터링 표준을 지원합니다.이 설정을 통해 관리자는 웹 트래픽, NetWare, Notes, e-메일, 데이터베이스 액세스, NFS(Network File System) 등 네트워크 애플리케이션을 분석하고 문제를 해결할 수 있습니다.이제 RMON 경보, 통계, 이력 및 호스트/대화 그룹을 사용하여 네트워크에서 가장 중요한 트래픽인 애플리케이션 레이어 트래픽을 기반으로 네트워크 가용성을 사전 대응적으로 모니터링하고 유지할 수 있습니다.네트워크 관리자는 RMON2를 통해 표준 기반 모니터링 솔루션을 계속 구축하여 미션 크리티컬 서버 기반 애플리케이션을 지원할 수 있습니다.

다음 표에는 RMON 그룹의 기능이 나열되어 있습니다.

RMON 그룹(RFC	함수

1757)	
통계	세그먼트 또는 포트의 패킷, 패킷, 패킷, 브로드캐스트, 오류 및 제안에 대한 카운터입니다.
기록	나중에 검색할 수 있도록 통계 그룹 카운터를 주기적으로 샘플링하고 저장합니다.
호스트	세그먼트 또는 포트의 각 호스트 디바이스에 대한 통계를 유지 관리합니다.
호스트 상위 N	통계 카운터를 기준으로 정렬된 Hosts 그룹의 사용자 정의 하위 집합 보고서.결과만 반환하면 관리 트래픽이 최소화됩니다.
트래픽 매트릭스	네트워크의 호스트 간 대화 통계를 유지합니다.
경보	사전 관리를 위해 중요한 RMON 변수에 설정할 수 있는 임계값입니다.
이벤트	경보 그룹 임계값을 초과할 경우 SNMP 트랩 및 로그 항목을 생성합니다.
패킷 캡처	관리 콘솔로 업로드하기 위해 필터 그룹에서 캡처한 패킷의 버퍼를 관리합니다.
토큰 링	벨소리 스테이션 - 개별 스테이션 벨소리 스테이션 순서에 대한 자세한 통계—벨소리 스테이션 구성에 현재 있는 순서가 지정된 스테이션 목록(스테이션당 컨피그레이션 및 삽입/제거 소스 라우팅) - 소스 라우팅에 대한 통계(예: 홉수 등)

RMON2	함수
프로토콜 디렉토리	에이전트가 통계를 모니터링하고 유지 관리하는 프로토콜입니다.
프로토콜 배포	각 프로토콜에 대한 통계입니다.
네트워크 레이어 호스트	세그먼트, 링 또는 포트의 각 네트워크 레이어 주소에 대한 통계입니다.
네트워크 레이어 매트릭스	네트워크 레이어 주소 쌍에 대한 트래픽 통계입니다.
애플리케이션 레이어 호스트	각 네트워크 주소에 대한 애플리케이션 레이어 프로토콜별 통계
애플리케이션 레이어 매트릭스	네트워크 레이어 주소 쌍에 대한 애플리케이션 레이어 프로토콜별 트래픽 통계입니다.
사용자 정의 가능 기록	RMON1 링크 레이어 통계를 넘어 RMON, RMON2, MIB-I 또는 MIB-II 통계를 포함하도록 기록을 확장합니다.
주소 매핑	MAC-네트워크 레이어 주소 바인딩입니다.
구성 그룹	상담원 기능 및 구성

NetFlow

Cisco NetFlow 기능을 사용하면 용량 계획, 청구 및 문제 해결 기능을 위해 트래픽 흐름에 대한 자세한 통계를 수집할 수 있습니다.개별 인터페이스에서 NetFlow를 구성하여 해당 인터페이스를 통과하는 트래픽에 대한 정보를 제공할 수 있습니다.다음 정보 유형은 자세한 트래픽 통계의 일부입니다.

- 소스 및 대상 IP 주소
- 입력 및 출력 인터페이스 번호
- TCP/UDP 소스 포트 및 대상 포트
- 흐름의 바이트 및 패킷 수
- 소스 및 대상 자동 시스템 번호
- IP 서비스 유형(ToS)

네트워크 디바이스에 수집된 NetFlow 데이터는 컬렉터 시스템으로 내보내집니다.컬렉터는 데이터 볼륨(필터링 및 어그리게이션), 계층적 데이터 스토리지, 파일 시스템 관리 등의 기능을 수행합니다.Cisco는 라우터 및 Cisco Catalyst 스위치에서 데이터를 수집 및 분석할 수 있도록 NetFlow Collector 및 NetFlow Analyzer 애플리케이션을 제공합니다.Cisco NetFlow UDP(user datagram protocol) 레코드를 수집할 수 있는 cflowd와 같은 공유 웨어 툴도 있습니다.

NetFlow 데이터는 UDP 패킷을 사용하여 다음과 같은 세 가지 형식으로 전송됩니다.

- 버전 1 - 초기 NetFlow 릴리스에서 지원되는 원래 형식입니다.
- 버전 5 - BGP(Border Gateway Protocol) 자동 시스템 정보 및 흐름 시퀀스 번호를 추가한 이후 개선 기능입니다.
- 버전 7 - NFFC(NetFlow Feature Card)가 장착된 Cisco Catalyst 5000 Series 스위치에 대한 NetFlow 스위칭 지원이 추가된 최신 개선 기능입니다.

버전 2~4 및 버전 6이 릴리스되지 않았거나 FlowCollector에서 지원되지 않습니다.세 가지 버전 모두에서 데이터그램은 헤더와 하나 이상의 플로우 레코드로 구성됩니다.

자세한 내용은 NetFlow Services Solutions Guide 백서를 참조하십시오.

다음 표에는 라우터와 Catalyst 스위치에서 NetFlow 데이터를 수집하기 위해 지원되는 Cisco IOS 버전이 설명되어 있습니다.

Cisco IOS 소프트웨어 릴리스	지원되는 Cisco 하드웨어 플랫폼	지원되는 NetFlow 내보내기 버전
11.1CA 및 11.1CC	Cisco 7200, 7500 및 RSP7000	V1 및 V5
11.2 및 11.2P	Cisco 7200, 7500 및 RSP7000	V1
오후 11.2시	Cisco RSM(Route Switch Module)	V1
11.3 및 11.3T	Cisco 7200, 7500 및 RSP7000	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000 및 RSM	V1 및 V5

12.0피트	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 880 RPM 및 BPX 00	V1 및 V5
12.0(3)T 이상	Cisco 1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR720, 7500, RSP 00, RSM, MGX8800 RPM 및 BPX 8650	V1, V5 및 V8
12.0(6)S	Cisco 12000	V1, V5 및 V8
—	Cisco Catalyst 5000 with NetFlow Feature Card(NFFC)***	V7

* Cisco 1600 및 2500 플랫폼에서 NetFlow Export V1, V5 및 V8에 대한 지원은 Cisco IOS Software 릴리스 12.0(T)을 대상으로 합니다. 이러한 플랫폼에 대한 NetFlow 지원은 Cisco IOS 12.0 메인라인 릴리스에서 제공되지 않습니다.

** AS5300 플랫폼에서 NetFlow V1, V5 및 V8에 대한 지원은 Cisco IOS Software 릴리스 12.06(T)을 대상으로 합니다.

*** MLS 및 NetFlow 데이터 내보내기는 Catalyst 5000 시리즈 수퍼바이저 엔진 소프트웨어 릴리스 4.1(1) 이상에서 지원됩니다.

보안 관리

보안 관리의 목적은 네트워크 리소스에 대한 액세스를 로컬 지침에 따라 제어하여 네트워크를 고의적으로 또는 의도하지 않게 왜곡할 수 없도록 하는 것입니다.예를 들어 보안 관리 하위 시스템은 네트워크 리소스에 로그온하는 사용자를 모니터링하여 부적절한 액세스 코드를 입력하는 사용자에 대한 액세스를 거부할 수 있습니다.보안 관리는 매우 광범위한 주제입니다.따라서 문서의 이 영역은 SNMP 및 기본 디바이스 액세스 보안과 관련된 보안만 다룹니다.

고급 보안에 대한 자세한 내용은 다음과 같습니다.

- IP 네트워크의 보안 강화
- 오픈 시스템

올바른 보안 관리 구현은 안전한 보안 정책 및 절차를 통해 시작됩니다.보안 및 성능에 대한 업계 모범 사례를 따르는 모든 라우터 및 스위치에 대해 플랫폼별 최소 구성 표준을 만드는 것이 중요합니다.

Cisco 라우터 및 Catalyst 스위치에서 액세스를 제어하는 다양한 방법이 있습니다.이러한 방법 중 일부는 다음과 같습니다.

- 액세스 제어 목록(ACL)
- 디바이스에 로컬로 존재하는 사용자 ID 및 비밀번호
- TACACS(Terminal Access Controller Access Control System)

TACACS는 네트워크의 클라이언트 디바이스 및 TACACS 서버에 대해 실행되는 RFC 1492(Internet Engineering Task Force) 표준 보안 프로토콜입니다.TACACS는 권한 있는 데이터베이스에 대한 원격 액세스를 원하는 디바이스의 ID를 인증하는 데 사용되는 인증 메커니즘입니다 .TACACS의 변형에는 인증, 권한 부여 및 계정 관리 기능을 분리하는 AAA 아키텍처인 TACACS+가 포함됩니다.

Cisco는 TACACS+를 사용하여 권한 없는 모드에서 Cisco 디바이스에 액세스할 수 있는 사용자를 보다 세부적으로 제어할 수 있습니다.내결함성을 위해 여러 TACACS+ 서버를 구성할 수 있습니다 .TACACS+가 활성화된 경우 라우터와 스위치에서 사용자에게 사용자 이름과 비밀번호를 묻는 메시지를 표시합니다.로그인 제어를 위해 또는 개별 명령을 인증하도록 인증을 구성할 수 있습니다.

인증

인증은 로그인 및 비밀번호 대화, 시도 및 응답, 메시징 지원을 포함한 사용자를 식별하는 프로세스입니다.인증은 라우터 또는 스위치에 대한 액세스가 허용되기 전에 사용자를 식별하는 방법입니다 .인증과 권한 부여 사이에는 근본적인 관계가 있습니다.사용자가 더 많은 권한 부여 권한을 받을 수록 더 강력한 인증이 필요합니다.

Ahthorization(권한 부여)

권한 부여는 사용자가 요청하는 각 서비스에 대한 1회 권한 부여 및 권한 부여를 포함하여 원격 액세스 제어를 제공합니다.Cisco 라우터에서 사용자에 대한 권한 부여 수준 범위는 0~15이며, 0은 가장 낮은 레벨이고 15는 가장 높은 레벨입니다.

회계

계정 관리를 사용하면 사용자 ID, 시작 및 중지 시간, 실행된 명령 등 청구, 감사 및 보고에 사용되는 보안 정보를 수집하고 전송할 수 있습니다.네트워크 관리자는 어카운팅을 통해 사용자가 액세스하는 서비스 및 사용하는 네트워크 리소스의 양을 추적할 수 있습니다.

다음 표에는 Cisco 라우터 및 Catalyst 스위치에서 TACACS+ 사용, 인증, 권한 부여 및 계정 관리를 위한 기본 샘플 명령이 나열되어 있습니다.자세한 명령은 Authentication, Authorization 및 Accounting Commands 문서를 참조하십시오.

Cisco IOS 명령	목적
라우터	
aaa 새 모델	액세스 제어를 위한 기본 방법으로 AAA(Authentication, Authorization, Accounting)를 활성화합니다.
AAA 계정 관리 {*시스템	네트워크	연결	exec	명령 수준*} {*start-stop	대기 시작	중지 전용*} {*tacacs+	반경*}	글로벌 컨피그레이션 명령으로 어카운팅을 활성화합니다.
AAA 인증 로그인 기본	로그인 기본값으로 구성된 모든

tacacs+	터미널 회선에 대한 연결이 TACACS+로 인증되도록 라우터를 설정하고 어떤 이유로 인증이 실패할 경우 실패합니다.
AAA 권한 부여 exec 기본 tacacs+ 없음	TACACS+ 서버에 요청하여 사용자가 EXEC 셸을 실행할 수 있는지 확인하려면 라우터를 설정합니다.
tacacs-server host tacacs+ *서버 ip 주소*	전역 컨피그레이션 명령으로 인증에 사용할 TACACS+ 서버를 지정합니다.
tacacs-server key *shared-secret*	TACACS+ 서버 및 Cisco 라우터에 의해 알려진 공유 암호를 전역 컨피그레이션 명령으로 지정합니다.
Catalyst 스위치	
authentication login tacacs enable 설정 [*all	콘솔	http	telnet*] [*기본*]	일반 로그인 모드에 대해 TACACS+ 인증을 활성화합니다.콘솔 포트 또는 텔넷 연결 시도에 대해서만 TACACS+를 활성화하려면 콘솔 또는 텔넷 키워드를 사용합니다.
set authorization exec enable {*option*} *fallback option*} [*console	텔넷	모두*]	일반 로그인 모드에 대한 권한 부여를 활성화합니다.콘솔 포트 또는 텔넷 연결 시도에 대해서만 권한 부여를 활성화하려면 콘솔 또는 텔넷 키워드를 사용합니다.
tacacs-server key *shared-secret 설정*	TACACS+ 서버 및 스위치에 의해 알려진 공유 암호를 지정합니다.
tacacs-server host tacacs+ *서버 IP 주소 설정*	전역 컨피그레이션 명령으로 인증에 사용할 TACACS+ 서버를 지정합니다.
Set accounting 명령 {config 사용 *설정	all*} {*stop-only*} *tacacs+*	컨피그레이션 명령의 어카운팅을 활성화합니다.

Catalyst 엔터프라이즈 LAN 스위치에서 명령줄 인터페이스에 대한 액세스를 모니터링하고 제어하도록 AAA를 구성하는 방법에 대한 자세한 내용은 Controling Access to the Switch Using Authentication, Authorization, and Accounting 문서를 참조하십시오.

SNMP 보안

SNMP 프로토콜을 사용하여 라우터와 Catalyst 스위치의 컨피그레이션을 CLI에서 발급한 것과 비슷하게 변경할 수 있습니다.SNMP를 통한 무단 액세스 및 변경을 방지하려면 네트워크 디바이스에 적절한 보안 조치를 구성해야 합니다.커뮤니티 문자열은 길이, 문자 및 추측 난이도 표준 암호 지침을 따라야 합니다.커뮤니티 문자열을 공용 및 개인 기본값에서 변경하는 것이 중요합니다.

모든 SNMP 관리 호스트는 고정 IP 주소를 가져야 하며 IP 주소 및 ACL(Access Control List)에 의해 미리 정의된 네트워크 디바이스와의 SNMP 통신 권한을 명시적으로 부여받아야 합니다. Cisco IOS 및 Cisco Catalyst 소프트웨어는 인증된 관리 스테이션만 네트워크 장치에서 변경을 수행할 수 있도

록 하는 보안 기능을 제공합니다.

라우터 보안 기능

SNMP 권한 레벨

이 기능은 관리 스테이션이 라우터에서 수행할 수 있는 작업 유형을 제한합니다.라우터에는 두 가지 유형의 권한 수준이 있습니다.읽기 전용(RO) 및 읽기-쓰기(RW). RO 레벨에서는 관리 스테이션에서 라우터 데이터를 쿼리할 수만 있습니다.라우터 재부팅 및 인터페이스 종료와 같은 컨피그레이션 명령을 수행할 수 없습니다.RW 권한 레벨만 이러한 작업을 수행하는 데 사용할 수 있습니다.

SNMP ACL(Access Control List)

SNMP ACL 기능을 SNMP 권한 기능과 함께 사용하여 특정 관리 스테이션이 라우터에서 관리 정보를 요청하지 못하도록 제한할 수 있습니다.

SNMP 보기

이 기능은 관리 스테이션별로 라우터에서 검색할 수 있는 특정 정보를 제한합니다.SNMP 권한 레벨 및 ACL 기능과 함께 사용하여 관리 콘솔별로 제한된 데이터 액세스를 적용할 수 있습니다.SNMP View의 컨피그레이션 샘플을 보려면 snmp-server 보기로 이동하십시오.

SNMP 버전 3

SNMP 버전 3(SNMPv3)은 네트워크 장치와 관리 스테이션 간에 관리 데이터를 안전하게 교환합니다.SNMPv3의 암호화 및 인증 기능은 관리 콘솔로 패킷을 전송할 때 높은 보안을 보장합니다.SNMPv3은 Cisco IOS Software 릴리스 12.0(3)T 이상에서 지원됩니다.SNMPv3에 대한 기술 개요는 SNMPv3 문서를 참조하십시오.

인터페이스의 ACL(Access Control List)

ACL 기능은 IP 스푸핑과 같은 공격을 방지하는 보안 조치를 제공합니다.ACL은 라우터의 수신 또는 발신 인터페이스에 적용할 수 있습니다.

Catalyst LAN 스위치 보안 기능

IP 허용 목록

IP Permit List 기능은 무단 소스 IP 주소에서 스위치에 대한 인바운드 텔넷 및 SNMP 액세스를 제한합니다.Syslog 메시지 및 SNMP 트랩은 위반 또는 무단 액세스가 발생할 경우 관리 시스템에 알리기 위해 지원됩니다.

Cisco IOS 보안 기능의 조합을 사용하여 라우터와 Catalyst 스위치를 관리할 수 있습니다.스위치와 라우터에 액세스할 수 있는 관리 스테이션 수를 제한하는 보안 정책을 설정해야 합니다.

IP 네트워크의 보안을 강화하는 방법에 대한 자세한 내용은 IP 네트워크의 보안 강화를 참조하십시오.

회계 관리

어카운팅 관리는 네트워크의 개별 또는 그룹 사용자를 어카운팅 또는 과금 용도로 적절하게 규제할

수 있도록 네트워크 사용률 매개변수를 측정하는 데 사용되는 프로세스입니다.성과 관리와 마찬가지로, 적절한 회계 관리를 위한 첫 번째 단계는 모든 중요한 네트워크 리소스의 활용률을 측정하는 것입니다.네트워크 리소스 사용률은 Cisco NetFlow 및 Cisco IP Accounting 기능을 사용하여 측정할 수 있습니다.이러한 방법을 통해 수집된 데이터를 분석하면 현재 사용 패턴을 파악할 수 있습니다.

사용량 기반 회계 및 청구 시스템은 모든 SLA(Service Level Agreement)의 필수 요소입니다. SLA에 따라 의무를 정의하는 실질적인 방법과 SLA 조건 외 동작에 대한 명확한 결과를 제공합니다.

데이터는 프로브 또는 Cisco NetFlow를 통해 수집할 수 있습니다.Cisco는 라우터 및 Catalyst 스위치에서 데이터를 수집 및 분석할 수 있도록 NetFlow Collector 및 NetFlow Analyzer 애플리케이션을 제공합니다.cflowd와 같은 Shareware 애플리케이션도 NetFlow 데이터를 수집하는 데 사용됩니다.리소스 사용을 지속적으로 측정하면 청구 정보가 산출될 수 있을 뿐만 아니라, 정보가 지속적으로 공정하고 최적화된 리소스를 평가합니다.일반적으로 구축되는 회계 관리 솔루션은 다음과 같습니다.

- 명백한 소프트웨어

NetFlow 활성화 및 데이터 수집 전략

NetFlow(네트워크 흐름)는 네트워크 계획, 모니터링 및 어카운팅 애플리케이션에 필요한 데이터를 캡처할 수 있는 입력 측면 측정 기술입니다.NetFlow는 서비스 제공자를 위한 에지/어그리게이션 라우터 인터페이스 또는 엔터프라이즈 고객을 위한 WAN 액세스 라우터 인터페이스에 구축되어야 합니다.

Cisco Systems는 전략적으로 배치된 라우터에서 NetFlow 서비스를 활성화하여 신중하게 계획된 NetFlow 구축을 권장합니다.NetFlow는 네트워크의 모든 라우터에 NetFlow를 구축하는 대신 점진적으로(인터페이스별 인터페이스) 구축하고 전략적으로(선택한 라우터에서) 구축할 수 있습니다.Cisco 직원은 고객과 협력하여 고객의 트래픽 흐름 패턴, 네트워크 토폴로지, 아키텍처를 기반으로 NetFlow를 활성화해야 할 주요 라우터와 주요 인터페이스를 결정합니다.

주요 구축 고려 사항은 다음과 같습니다.

- NetFlow 서비스는 에지 측정 및 액세스 목록 성능 가속화 툴로 활용되어야 하며, 매우 높은 CPU 활용률로 실행되는 *핫* 코어/백본 라우터 또는 라우터에서 활성화해서는 안 됩니다.
- 애플리케이션 중심의 데이터 수집 요구 사항 이해어카운팅 애플리케이션은 라우터 플로우 정보를 시작하거나 종료하기만 하면 되지만, 모니터링 애플리케이션을 모니터링하려면 더욱 포괄적인(데이터 집약적) 엔드 투 엔드 보기가 필요할 수 있습니다.
- 네트워크 토폴로지 및 라우팅 정책이 플로우 수집 전략에 미치는 영향을 이해합니다.예를 들어, 동일한 플로우 정보의 중복 보기를 제공하는 백본 라우터 또는 중간 라우터가 아닌 트래픽이 시작되거나 종료되는 키 어그리게이션 라우터에서 NetFlow를 활성화하여 중복 흐름을 수집하지 마십시오.
- *트랜짓 캐리어* 비즈니스의 통신 사업자(네트워크에서 발신 또는 종료되지 않는 트래픽 전송)는 NetFlow Export 데이터를 활용하여 회계 및 청구 용도로 네트워크 리소스의 트랜짓 트래픽 사용량을 측정할 수 있습니다.

IP 어카운팅 구성

Cisco IP 어카운팅 지원은 기본적인 IP 어카운팅 기능을 제공합니다.IP 어카운팅을 활성화하면 소

스 및 대상 IP 주소를 기준으로 Cisco IOS 소프트웨어를 통해 전환된 바이트 및 패킷 수를 확인할 수 있습니다.트랜짓 IP 트래픽만 측정되며 아웃바운드에서만 측정됩니다.소프트웨어에서 생성되거나 소프트웨어에서 종료되는 트래픽은 회계 통계에 포함되지 않습니다.정확한 어카운팅 합계를 유지하기 위해 소프트웨어는 두 가지 어카운팅 데이터베이스를 유지 관리합니다.활성 및 체크포인트 데이터베이스.

Cisco IP 어카운팅 지원에서는 IP 액세스 목록에 실패한 IP 트래픽을 식별하는 정보도 제공합니다.IP 액세스 목록을 위반하는 IP 소스 주소를 식별하면 보안 침해가 발생할 수 있는 시도를 알리는 신호입니다.또한 이 데이터는 IP 액세스 목록 컨피그레이션을 확인해야 함을 나타냅니다.사용자가 이 기능을 사용할 수 있게 하려면 **ip accounting access-violations** 명령을 사용하여 액세스 목록 위반에 대한 IP 어카운팅을 활성화합니다.그런 다음 사용자는 소스 대상 쌍의 액세스 목록에 대해 보안을 위반하려고 시도한 단일 소스의 바이트 및 패킷 수를 표시할 수 있습니다.기본적으로 IP 어카운팅은 액세스 목록을 통과하고 라우팅된 패킷 수를 표시합니다.

IP 어카운팅을 활성화하려면 인터페이스 컨피그레이션 모드에서 각 인터페이스에 다음 명령 중 하나를 사용합니다.

명령	목적
ip 계정 관리	기본 IP 어카운팅을 활성화합니다.
ip 계정 액세스 위반	IP 액세스 목록에 실패한 IP 트래픽을 식별하는 기능을 사용하여 IP 어카운팅을 활성화합니다.

다른 IP 어카운팅 기능을 구성하려면 글로벌 컨피그레이션 모드에서 다음 명령 중 하나 이상을 사용합니다.

명령	목적
ip accounting-threshold *임계값*	생성할 최대 계정 항목 수를 설정합니다.
ip accounting-list *ip-address 와일드카드*	호스트에 대한 계정 정보를 필터링합니다.
ip accounting-transits *수*	IP 어카운팅 데이터베이스에 저장될 전송 레코드 수를 제어합니다.

이 문서에 사용된 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.