

QoS 자주 묻는 질문

목차

[소개](#)

[일반](#)

[분류 및 표시](#)

[대기열 처리 및 정체 관리](#)

[혼잡 회피 가중 랜덤 조기 탐지\(WRED\)](#)

[폴리싱 및 셰이핑](#)

[QoS\(Quality of Service\) 프레임 릴레이](#)

[비동기 전송 모드\(ATM\)를 통한 QoS\(Quality of Service\)](#)

[음성 및 서비스 품질\(QoS\)](#)

[관련 정보](#)

소개

이 문서에서는 QoS(Quality of Service)와 관련된 가장 자주 묻는 질문(FAQ)을 다룹니다.

일반

Q. QoS(Quality of Service)란 무엇입니까?

A. QoS는 프레임 릴레이, ATM(Asynchronous Transfer Mode), 이더넷 및 802.1 네트워크, SONET, IP 라우팅 네트워크 등 다양한 기본 기술을 통해 선택된 네트워크 트래픽에 더 나은 서비스를 제공하는 네트워크의 기능을 의미합니다.

QoS는 애플리케이션이 데이터 처리량 용량(대역폭), 레이턴시 변형(지터), 지연 등의 측면에서 예측 가능한 서비스 레벨을 요청 및 수신할 수 있도록 하는 기술 모음입니다. 특히 QoS 기능은 다음과 같은 방법으로 더 우수하고 예측 가능한 네트워크 서비스를 제공합니다.

- 전용 대역폭 지원
- 손실 특성 개선
- 네트워크 혼잡 방지 및 관리
- 네트워크 트래픽 셰이핑
- 네트워크 전반에 걸쳐 트래픽 우선 순위 설정

IETF(Internet Engineering Task Force)는 QoS에 대해 다음 두 가지 아키텍처를 정의합니다.

- 통합 서비스(IntServ)
- 차별화된 서비스(DiffServ)

IntServ는 RSVP(Resource Reservation Protocol)를 사용하여 네트워크를 통해 엔드 투 엔드 경로에 있는 디바이스를 따라 애플리케이션의 트래픽에 대한 QoS 요구 사항을 명시적으로 알립니다. 경로를 따라 모든 네트워크 디바이스가 필요한 대역폭을 예약할 수 있는 경우 원래 애플리케이션이

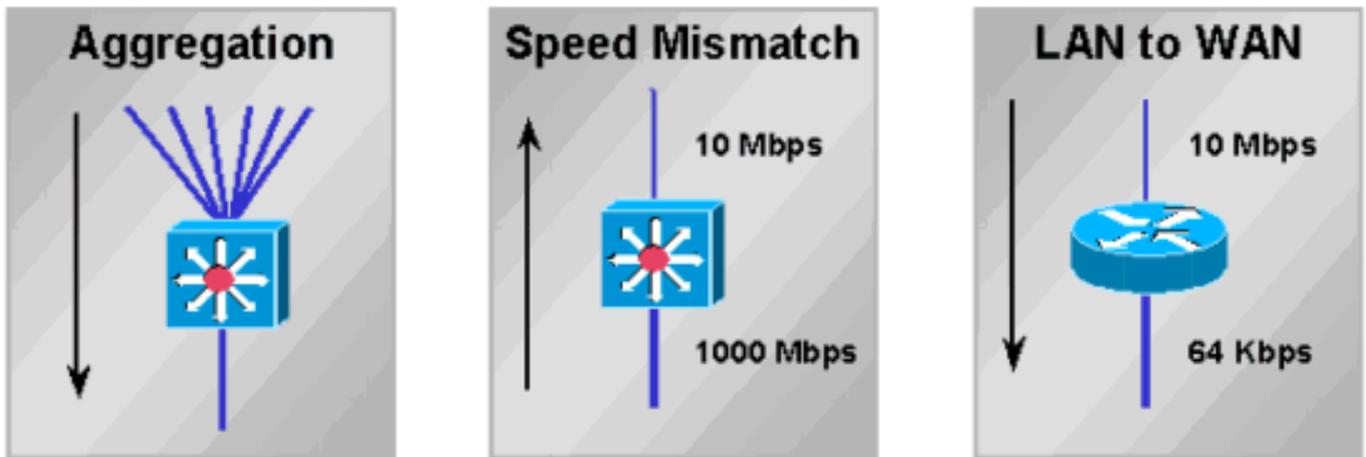
전송을 시작할 수 있습니다.RFC(Request for Comments) 2205는 RSVP를 정의하고 RFC 1633은 IntServ를 정의합니다.

DiffServ는 집계된 QoS 및 프로비저닝된 QoS에 중점을 둡니다.DiffServ는 애플리케이션의 QoS 요구 사항을 알리는 대신 IP 헤더에 DSCP(DiffServ Code Point)를 사용하여 필요한 QoS 레벨을 나타냅니다.Cisco IOS® 소프트웨어 릴리스 12.1(5)T는 Cisco 라우터에 DiffServ 규정 준수를 도입했습니다.자세한 내용은 다음 문서를 참조하십시오.

- [Cisco IOS 12.1의 통합 서비스](#)
- [엔드 투 엔드 QoS\(Quality of Service\)를 위한 DiffServ 구현](#)
- [DSCP를 통한 서비스 품질 정책 구현](#)

Q. 혼잡, 지연 및 지터란 무엇입니까?

A. 인터페이스는 처리할 수 있는 트래픽보다 많은 트래픽이 표시될 때 정체 현상이 발생합니다.네트워크 혼잡 포인트는 QoS(Quality of Service) 메커니즘에 대한 강력한 후보입니다.다음은 일반적인 혼잡 지점의 예입니다.



네트워크 혼잡이 지연됩니다.Understanding [Delay in Packet Voice Networks](#)(패킷 음성 네트워크 지연 이해)에서 설명한 대로 네트워크 및 해당 디바이스에는 여러 가지 지연이 발생합니다.지연 편차는 지터로 알려져 있으며, [Cisco IOS 플랫폼\(Packet Voice Networks\)의 지터 이해에 설명되어 있습니다](#). 실시간 및 인터랙티브 트래픽을 지원하려면 지연과 지터를 모두 제어하고 최소화해야 합니다.

Q. MQC란 무엇입니까?

A. MQC는 모듈형 QoS(Quality of Service) CLI(Command Line Interface)를 의미합니다. Cisco 라우터 및 스위치에서 QoS 구성을 간소화하기 위해 설계되었으며, 공통 명령 구문 및 플랫폼 전반에 걸친 QoS 동작 집합을 정의했습니다.이 모델은 각 QoS 기능과 각 플랫폼에 대해 고유한 구문을 정의하는 이전 모델을 대체합니다.

MQC에는 다음 3단계가 포함되어 있습니다.

1. **class-map** 명령을 실행하여 트래픽 클래스를 정의합니다.
2. **policy-map** 명령을 실행하여 트래픽 클래스를 하나 이상의 QoS 기능과 연결하여 트래픽 정책을 생성합니다.

3. **service-policy** 명령을 실행하여 인터페이스, 하위 인터페이스 또는 VC(Virtual Circuit)에 트래픽 정책을 연결합니다.

참고: MQC 구문을 사용하여 DiffServ의 트래픽 조정 기능(예: 표시 및 셰이핑)을 구현합니다.

자세한 내용은 [Modular Quality of Service Command-Line Interface](#)를 참조하십시오.

Q. DCEF가 활성화된 VIP 의미는 무엇입니까?

A. Cisco 7500 Series의 VIP(Versatile Interface Processor)에서 Cisco IOS 12.1(5)T, 12.1(5)E 및 12.0(14)S를 기준으로 분산 QoS(Quality of Service) 기능만 지원됩니다. 분산 Cisco Express Forwarding(dCEF)을 활성화하면 분산된 QoS가 자동으로 활성화됩니다.

레거시 IP(Interface Processor)로 알려진 비 VIP 인터페이스는 RSP(Route Switch Processor)에서 활성화된 중앙 QoS 기능을 지원합니다. 자세한 내용은 다음 문서를 참조하십시오.

- [분산 클래스 기반 가중 공정 대기열 처리 및 분산 가중 임의 조기 탐지](#)
- [분산형 낮은 레이턴시 대기열 처리](#)
- [분산된 트래픽 셰이핑](#)
- [Versatile Interface Processor-Based Distributed FRF.11 및 FRF.12 for Cisco IOS Release 12.1 T](#)

Q. QoS(Quality of Service) 정책이 지원하는 클래스는 몇 개입니까?

A. Cisco IOS 12.2 이전 버전에서는 최대 256개의 클래스만 정의할 수 있으며, 동일한 클래스가 다른 정책에 재사용되는 경우 각 정책 내에서 최대 256개의 클래스를 정의할 수 있습니다. 두 개의 정책이 있는 경우 두 정책의 총 클래스 수는 256개를 초과할 수 없습니다. 정책에 CBWFQ(Class-Based Weighted Fair Queuing)가 포함된 경우(즉, 클래스 내에 대역폭[또는 priority] 문이 포함되어 있음) 지원되는 총 클래스 수는 64개입니다.

Cisco IOS 버전 12.2(12), 12.2(12)T 및 12.2(12)S에서 256개의 전역 클래스 맵의 이 제한이 변경되었으며, 이제 최대 1024개의 전역 클래스 맵을 구성하고 동일한 정책 맵 내에서 256개의 클래스 맵을 사용할 수 있습니다.

Q. 서비스 정책이 적용될 때 라우팅 업데이트 및 PPP(Point-to-Point Protocol)/HDLC(High-Level Data Link Control) keepalive는 어떻게 처리됩니까?

A. Cisco IOS 라우터는 다음 두 가지 메커니즘을 사용하여 제어 패킷의 우선순위를 지정합니다.

- IP 우선 순위
- pak_priority

두 메커니즘 모두 라우터 및 아웃바운드 인터페이스가 혼잡할 때 대기열 시스템에서 키 제어 패킷이 삭제 또는 삭제되지 않도록 설계되었습니다. 자세한 내용은 QoS [서비스 정책이 포함된 인터페이스에서 라우팅 업데이트 및 제어 패킷이 대기되는 방법 이해](#)를 참조하십시오.

Q. IRB(Integrated Routing and Bridging)로 구성된 인터페이스에서 QoS(Quality of Service)가 지원됩니까?

A. 아니요. 인터페이스가 IRB에 대해 구성된 경우 QoS 기능을 구성할 수 없습니다.

분류 및 표시

Q. QoS(Quality of Service) 사전 분류란 무엇입니까?

A. QoS 사전 분류를 사용하면 터널 캡슐화 및/또는 암호화를 수행하는 패킷의 원래 IP 헤더 내용을 매칭하고 분류할 수 있습니다. 이 기능은 원래 패킷 헤더에서 터널 헤더로 ToS(Type of Service) 바이트의 원래 값을 복사하는 프로세스를 설명하지 않습니다. 자세한 내용은 다음 문서를 참조하십시오.

- [가상 사설 네트워크에 대한 QoS 구성](#)
- [QoS\(Quality of Service for Virtual Private Networks\), 12.2\(2\)T 기능 모듈](#)

Q. 어떤 패킷 헤더 필드를 알 수 있습니까? 어떤 값을 사용할 수 있습니까?

A. 클래스 기반 표시 기능을 사용하면 패킷의 레이어 2, 레이어 3 또는 MPLS(Multiprotocol Label Switching) 헤더를 설정하거나 표시할 수 있습니다. 자세한 내용은 다음 문서를 참조하십시오.

- [클래스 기반 패킷 표시 구성](#)
- [라우터가 ATM 셀에서 CLP 비트를 설정하는 경우는 언제입니까?](#)
- [프레임 릴레이 PVC에서 패킷 표시 구성](#)

Q. URL을 기준으로 트래픽의 우선 순위를 지정할 수 있습니까?

A. 네.NBAR(Network Based Application Recognition)를 사용하면 애플리케이션 레이어의 필드에서 매칭하여 패킷을 분류할 수 있습니다. NBAR가 도입되기 전에 가장 세분화된 분류는 레이어 4 TCP(Transmission Control Protocol) 및 UDP(User Datagram Protocol) 포트 번호였습니다. 자세한 내용은 다음 문서를 참조하십시오.

- [네트워크 기반 애플리케이션 인식 Q&A](#)
- [NBAR 애플리케이션 네트워킹](#)
- [네트워크 기반 애플리케이션 인식 및 액세스 제어 목록을 사용하여 코드 적색 WORM 차단](#)
- [Nimda 바이러스로부터 네트워크를 보호하는 방법](#)

Q. NBAR(Network Based Application Recognition)를 지원하는 플랫폼과 Cisco IOS 소프트웨어 버전은 무엇입니까?

A. NBAR 지원은 다음 버전의 Cisco IOS 소프트웨어에 도입되었습니다.

플랫폼	최소 Cisco IOS 소프트웨어 버전
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

참고: NBAR를 사용하려면 Cisco CEF(Express Forwarding)를 활성화해야 합니다.

DNBAR(Distributed NBAR)는 다음 플랫폼에서 사용할 수 있습니다.

플랫폼	최소 Cisco IOS 소프트웨어 버전
7500	12.2(4)T, 12.1(6)E
FlexWAN	12.1(6)E

참고: NBAR는 Catalyst 6000 MSFC(Multilayer Switch Feature Card) VLAN 인터페이스, Cisco 12000 Series 또는 Catalyst 5000 Series용 RSM(Route Switch Module)에서 지원되지 않습니다.위에 나열된 특정 플랫폼이 표시되지 않으면 Cisco 기술 담당자에게 문의하십시오.

대기열 처리 및 정체 관리

Q. 큐잉의 목적은 무엇입니까?

A. 큐잉(Queueing)은 대역폭을 사용할 수 있을 때까지 초과 패킷을 버퍼에 저장하여 네트워크 디바이스의 인터페이스에서 일시적인 정체를 수용하도록 설계되었습니다. Cisco IOS 라우터는 다양한 애플리케이션의 대역폭, 지터 및 지연 요구 사항을 충족하기 위해 여러 대기열 처리 방법을 지원합니다.

대부분의 인터페이스의 기본 메커니즘은 FIFO(First In First Out)입니다. 일부 트래픽 유형에는 더 까다로운 지연/지터 요구 사항이 있습니다. 따라서 다음 대체 대기열 처리 메커니즘 중 하나를 구성하거나 기본적으로 활성화해야 합니다.

- WFQ(Weighted Fair Queueing)
- 클래스 기반 CBWFQ(Weighted Fair Queueing)
- LLQ(Low Latency Queueing): PQ(Priority Queue)가 있는 CBWFQ입니다(PQCBWFQ라고도 함).
- PQ(Priority Queueing)
- CQ(Custom Queueing)

큐잉은 일반적으로 아웃바운드 인터페이스에서만 발생합니다. 라우터는 인터페이스를 나가는 패킷을 대기열에 넣습니다. 인바운드 트래픽을 폴리싱할 수 있지만, 일반적으로 인바운드(dCEF(Distributed Cisco Express Forwarding))를 사용하여 Cisco 7500 Series 라우터에서 수신 측 버퍼링을 대기시켜 인그레스 인터페이스에서 이그레스 인터페이스로 패킷을 전달하는 경우는 예외입니다. 자세한 내용은 [99%에서 실행되는 VIP CPU 이해 및 Rx-Side 버퍼링](#)을 참조하십시오. Cisco 7500 및 12000 Series와 같은 하이엔드 분산 플랫폼에서 인바운드 인터페이스는 인바운드 인터페이스의 스위칭 결정 이후 혼잡한 아웃바운드 인터페이스로 전환된 초과 트래픽을 저장하기 위해 자체 패킷 버퍼를 사용할 수 있습니다. 드문 경우이지만, 일반적으로 인바운드 인터페이스가 더 느린 아웃바운드 인터페이스를 제공할 경우 인바운드 인터페이스가 패킷 메모리가 부족해지면 무시된 오류가 증가할 수 있습니다. 과도한 혼잡 때문에 출력 대기열이 삭제될 수 있습니다. 입력 대기열 삭제는 대부분의 시간에 다른 근본 원인을 갖습니다. 삭제 문제 해결에 대한 자세한 내용은 다음 문서를 참조하십시오.

- [입력 대기열 삭제 및 출력 대기열 삭제 문제 해결](#)

자세한 내용은 다음 문서를 참조하십시오.

- [ATM 포트 어댑터에서 "무시된" 오류 문제 해결](#)
- [Cisco 12000 Series 인터넷 라우터에서 무시된 오류 및 메모리 손실 문제 해결](#)

Q. WFQ(Weighted Fair Queueing) 및 CBWFQ(Class Based Weighted Fair Queueing)는 어떻게 운영되니까?

A. 공정 대기열 처리에서는 활성 대화 또는 IP 흐름 간에 인터페이스의 대역폭을 균등하게 할당하려고 합니다.IP 헤더의 여러 필드와 패킷 길이를 기반으로 해싱 알고리즘을 사용하여 대화 식별 번호로 식별되는 패킷을 하위 큐로 분류합니다.다음은 가중치를 계산하는 방법입니다.

- $W=K/(\text{우선순위} + 1)$

K= 4096(Cisco IOS 12.0(4)T 및 이전 릴리스) 및 32384(12.0(5)T 이상 릴리스).

가중치가 낮을수록 우선순위가 높으며 대역폭의 점유율이 높습니다.가중치 외에도 패킷의 길이를 고려합니다.

CBWFQ에서는 트래픽 클래스를 정의하고 이를 최소 대역폭 보증으로 할당할 수 있습니다.이 메커니즘 뒤에 있는 알고리즘은 이름을 설명하는 WFQ입니다.CBWFQ를 구성하려면 map-class 문에서 특정 클래스를 정의합니다.그런 다음 정책 맵의 각 클래스에 정책을 할당합니다.그러면 이 정책 맵은 인터페이스에 아웃바운드 연결됩니다.자세한 내용은 다음 문서를 참조하십시오.

- [ATM에서 클래스 기반 가중 공정 대기열 이해](#)
- [ATM에서 가중치 공정 대기열 이해](#)

Q. CBWFQ(Class Based Weighted Fair Queueing)의 클래스가 대역폭을 사용하지 않는 경우 다른 클래스에서 대역폭을 사용할 수 있습니까?

A. 네.bandwidth 및 priority 명령을 실행하여 제공되는 대역폭은 "reserved" 및 "bandwidth to be set"과 같은 단어로 설명되었지만, 두 명령 모두 진정한 예약을 구현합니다.즉, 트래픽 클래스가 구성된 대역폭을 사용하지 않는 경우 사용되지 않는 대역폭은 다른 클래스 간에 공유됩니다.

큐잉 시스템은 우선 순위 클래스를 사용하여 이 규칙에 중요한 예외를 적용합니다.위에서 언급한 대로, 우선 순위 클래스의 제공된 부드는 트래픽 폴리서에서 계량합니다.혼잡 상황에서 우선순위 클래스는 초과 대역폭을 사용할 수 없습니다.자세한 내용은 QoS [서비스 정책의 대역폭 및 우선순위 명령 비교를 참조하십시오](#).

Q. 하위 인터페이스에서 CBWFQ(Class Based Weighted Fair Queuing)가 지원되니까?

A. Cisco IOS 논리적 인터페이스는 기본적으로 혼잡 상태를 지원하지 않으며 대기열 처리 방법을 적용하는 서비스 정책의 직접 적용을 지원하지 않습니다.대신 먼저 GTS(Generic Traffic Shaping) 또는 클래스 기반 셰이핑을 사용하여 하위 인터페이스에 셰이핑을 적용해야 합니다.자세한 내용은 이더넷 하위 인터페이스에 [QoS 기능 적용을 참조하십시오](#).

Q. 정책 맵에서 와 문의 차이는 무엇입니까?

A. priority 및 bandwidth 명령은 기능 및 일반적으로 지원하는 애플리케이션에 모두 다릅니다.다음 표에는 이러한 차이점이 요약되어 있습니다.

합수	bandwidth 명령	priority 명령
최소 대역폭 보증	예	예

최대 대역폭 보증	아니요	예
내장형 폴리서	아니요	예
짧은 지연 시간 제공	아니요	예

자세한 내용은 QoS 서비스 정책의 [대역폭 및 우선순위 명령 비교를 참조하십시오.](#)

Q. FlexWAN 및 VIP(Versatile Interface Processor)에서 큐 제한은 어떻게 계산됩니까?

A. VIP 또는 FlexWAN에 SRAM이 충분하다고 가정할 경우, 대기열 제한은 평균 패킷 크기가 250바이트인 최대 지연 500ms를 기준으로 계산됩니다. 다음은 대역폭이 1Mbps인 클래스의 예입니다.

$$\text{대기열 제한} = 1000000 / (250 \times 8 \times 2) = 250$$

사용 가능한 패킷 메모리의 양이 감소하고 VCS(Virtual Circuit)의 수가 증가함에 따라 대기열 제한이 더 작습니다.

다음 예에서는 PA-A3가 Cisco 7600 Series용 FlexWAN 카드에 설치되고 2MB PVC(Permanent Virtual Circuit)가 있는 여러 하위 인터페이스를 지원합니다. 서비스 정책은 각 VC에 적용됩니다.

```
class-map match-any XETRA-CLASS
  match access-group 104
class-map match-any SNA-CLASS
  match access-group 101
  match access-group 102
  match access-group 103
policy-map POLICY-2048Kbps
  class XETRA-CLASS
    bandwidth 320
  class SNA-CLASS
    bandwidth 512

interface ATM6/0/0
  no ip address
  no atm sonet ilmi-keepalive
  no ATM ilmi-keepalive
!
interface ATM6/0/0.11 point-to-point
  mtu 1578
  bandwidth 2048
  ip address 22.161.104.101 255.255.255.252
  pvc ABCD
    class-vc 2048Kbps-PVC
    service-policy out POLICY-2048Kbps
```

ATM(Asynchronous Transfer Mode) 인터페이스는 전체 인터페이스에 대한 큐 제한을 가져옵니다. 제한은 사용 가능한 총 버퍼, FlexWAN의 물리적 인터페이스 수 및 인터페이스에서 허용되는 최대 대기열 지연의 기능입니다. 각 PVC는 PVC의 SCR(Continued Cell Rate) 또는 MCR(Minimum Cell Rate)에 따라 인터페이스 제한의 일부를 가져오고, 각 클래스는 대역폭 할당을 기반으로 PVC 제한의 일부를 가져옵니다.

다음은 **show policy-map interface** 명령의 샘플 출력입니다. 전역 버퍼가 3687인 FlexWAN에서 파

생됩니다.이 값을 보려면 **show buffer** 명령을 실행합니다.각 2Mbps PVC는 2Mbps의 PVC 대역폭 (2047/149760 x 3687 = 50)에 따라 50개의 패킷이 할당됩니다. 다음 출력에 표시된 대로 각 클래스는 50의 일부를 할당합니다.

```
service-policy output: POLICY-2048Kbps
class-map: XETRA-CLASS (match-any)
  687569 packets, 835743045 bytes
  5 minute offered rate 48000 bps, drop rate 6000 BPS
match: access-group 104
  687569 packets, 835743045 bytes
  5 minute rate 48000 BPS
queue size 0, queue limit 7
packets output 687668, packet drops 22
tail/random drops 22, no buffer drops 0, other drops 0
bandwidth: kbps 320, weight 15

class-map: SNA-CLASS (match-any)
  2719163 packets, 469699994 bytes
  5 minute offered rate 14000 BPS, drop rate 0 BPS
match: access-group 101
  1572388 packets, 229528571 bytes
  5 minute rate 14000 BPS
match: access-group 102
  1146056 packets, 239926212 bytes
  5 minute rate 0 BPS
match: access-group 103
  718 packets, 245211 bytes
  5 minute rate 0 BPS
queue size 0, queue limit 12
packets output 2719227, packet drops 0
tail/random drops 0, no buffer drops 0, other drops 0
bandwidth: kbps 512, weight 25
queue-limit 100

class-map: class-default (match-any)
  6526152 packets, 1302263701 bytes
  5 minute offered rate 44000 BPS, drop rate 0 BPS
match: any
  6526152 packets, 1302263701 bytes
  5 minute rate 44000 BPS
queue size 0, queue limit 29
packets output 6526840, packet drops 259
tail/random drops 259, no buffer drops 0, other drops 0
```

트래픽 스트림에서 큰 패킷 크기를 사용하는 경우 큐 제한에 도달하기 전에 버퍼가 부족해질 수 있으므로 **show policy-map interface** 명령 출력은 no buffer drops 필드에 대한 증가 값을 보고할 수 있습니다.이 경우 우선 순위가 낮은 클래스의 queue-limit를 수동으로 조정하십시오.자세한 내용은 IP에서 [ATM CoS로 전송 큐 제한 이해를 참조하십시오](#).

Q. queue-limit 값을 어떻게 확인합니까?

A. 분산되지 않은 플랫폼에서 대기열 제한은 기본적으로 64패킷입니다.다음 예는 Cisco 3600 Series 라우터에서 출력되었습니다.

```
november# show policy-map interface s0
Serial0

Service-policy output: policy1
```

```

Class-map: class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 BPS, drop rate 0 BPS
  Match: ip precedence 5
  Weighted Fair Queueing
    Output Queue: Conversation 265
    Bandwidth 30 (kbps) Max Threshold 64 (packets)
    !--- Max Threshold is the queue-limit. (pkts matched/bytes matched) 0/0 (depth/total
drops/no-buffer drops) 0/0/0 Class-map: class2 (match-all) 0 packets, 0 bytes 5 minute offered
rate 0 BPS, drop rate 0 BPS Match: ip precedence 2 Match: ip precedence 3 Weighted Fair Queueing
Output Queue: Conversation 266 Bandwidth 24 (kbps) Max Threshold 64 (packets) (pkts
matched/bytes matched) 0/0 (depth/total drops/no-buffer drops) 0/0/0 Class-map: class-default
(match-any) 0 packets, 0 bytes 5 minute offered rate 0 BPS, drop rate 0 BPS Match: any

```

Q. 클래스 내에서 공정한 대기열 처리를 활성화할 수 있습니까?

A. QoS(Distributed Quality of Service)가 포함된 Cisco 7500 Series는 클래스당 공정한 대기열 처리를 지원합니다. Cisco 7200 Series 및 Cisco 2600/3600 Series를 비롯한 기타 플랫폼은 클래스 기본 클래스에서 WFQ(Weighted Fair Queueing)를 지원합니다. 모든 대역폭 클래스는 FIFO(First In First Out)를 사용합니다.

Q. 대기열 처리를 모니터링하는 데 사용할 수 있는 명령은 무엇입니까?

A. 다음 명령을 사용하여 대기열 처리를 모니터링합니다.

- **show queue {interface}{interface number}** - Cisco 7500 Series가 아닌 Cisco IOS 플랫폼에서 이 명령은 활성 대기열 또는 대화를 표시합니다. 인터페이스 또는 VC(Virtual Circuit)가 혼잡하지 않으면 대기열이 나열되지 않습니다. Cisco 7500 Series에서는 **show queue** 명령이 지원되지 않습니다.
- **show queuing interface-number [vc [[vpi/ vci]** - 인터페이스 또는 VC의 대기열 통계를 표시합니다. 정체 현상이 발생하지 않더라도 일부 히트를 볼 수 있습니다. 그 이유는 프로세스 스위칭된 패킷은 존재하는 혼잡을 불문하고 항상 계산되기 때문입니다. Cisco CEF(Express Forwarding) 및 Fast-Switched 패킷은 혼잡이 발생하지 않는 한 계산되지 않습니다. PQ(Priority Queueing), CQ(Custom Queueing), WFQ(Weighted Fair Queueing)와 같은 레거시 대기열 메커니즘은 분류 통계를 제공하지 않습니다. 12.0(5)T 이후 이미지의 모듈형 MQC(Quality of Service Command Line Interface) 기반 기능만 이러한 통계를 제공합니다.
- **show policy interface {interface}{interface number}** - packets 카운터는 클래스 기준과 일치하는 패킷 수를 계산합니다. 이 카운터는 인터페이스가 혼잡한지 여부를 증가시킵니다. 일치하는 카운터는 인터페이스가 혼잡할 때 클래스의 기준과 일치하는 패킷 수를 나타냅니다. 패킷 카운터에 대한 자세한 내용은 다음 문서를 참조하십시오. [show policy-map interface 출력의 패킷 카운터 이해](#)
- Cisco 클래스 기반 QoS 컨피그레이션 및 통계 MIB - SNMP(Simple Network Management Protocol) 모니터링 기능을 제공합니다.

Q. RSVP는 CBWFQ(Class Based Weighted Fair Queueing)와 함께 사용할 수 있습니다. RSVP(Resource Reservation Protocol)와 CBWFQ가 모두 인터페이스에 대해 구성된 경우 RSVP와 CBWFQ가 독립적으로 작동하면서 각각 단독으로 실행되는 것과 동일한 동작을 나타내니까? RSVP는 대역폭 가용성, 평가 및 할당과 관련하여 CBWFQ가 구성되지 않은 것처럼 동작합니다.

A. Cisco IOS Software Release 12.1(5)T 이상에서 RSVP 및 CB-WFQ를 사용할 경우 라우터는 오버서브스크립션 없이 RSVP 플로우 및 CBWFQ 클래스가 인터페이스 또는 PVC에서 사용 가능한

대역폭을 공유하도록 작동할 수 있습니다.

IOS Software Release 12.2(1)T 이상에서는 RSVP가 자체 "ip rsvp 대역폭" 풀을 사용하여 승인 제어를 수행할 수 있는 반면, CBWFQ는 RSVP 패킷의 분류, 폴링 및 예약을 수행합니다. 이는 발신자가 미리 표시한 패킷과 비 RSVP 패킷이 다르게 표시되었다고 가정합니다.

혼잡 회피 가중 랜덤 조기 탐지(WRED)

Q. WRED(Weighted Random Early Detection) 및 LLQ(Low Latency Queuing) 또는 CBWFQ(Class Based Weighted Fair Queuing)를 동시에 활성화할 수 있습니까?

A. 네. 큐잉은 큐에서 나가는 패킷의 순서를 정의합니다. 즉, 패킷 스케줄링 메커니즘을 정의합니다. 또한 공정한 대역폭 할당 및 최소 대역폭 보장을 제공하는 데에도 사용할 수 있습니다. 반면 RFC(Request for Comments) 2475는 "지정된 규칙에 따라 패킷을 삭제하는 프로세스"로 삭제를 정의합니다. 기본 삭제 메커니즘은 tail drop입니다. 이 경우 큐가 가득 찰 때 인터페이스가 패킷을 삭제합니다. 대체 삭제 메커니즘은 RED(Random Early Detection)와 Cisco의 WRED입니다. 이 WRED는 큐가 가득 찰 때까지 패킷을 무작위로 삭제하기 시작하며 일관된 평균 대기열 깊이를 유지하려고 합니다. WRED는 패킷의 IP 우선순위 값을 사용하여 차별화된 삭제 결정을 합니다. 자세한 내용은 [WRED\(Weighted Random Early Detection\)를 참조하십시오.](#)

Q. 어떻게 WRED(Weighted Random Early Detection)를 모니터링하고 실제로 그 효과를 볼 수 있습니까?

A. WRED는 평균 대기열 깊이를 모니터링하고 계산된 값이 최소 임계값 이상으로 이동하면 패킷을 삭제하기 시작합니다. 다음 예와 같이 `show policy-map interface` 명령을 실행하고 평균 대기열 깊이 값을 모니터링합니다.

```
Router# show policy interface s2/1
```

```
Serial2/1
output : p1
Class c1
  Weighted Fair Queueing
    Output Queue: Conversation 265
    Bandwidth 20 (%)
    (pkts matched/bytes matched) 168174/41370804
    (pkts discards/bytes discards/tail drops) 20438/5027748/0
    mean queue depth: 39

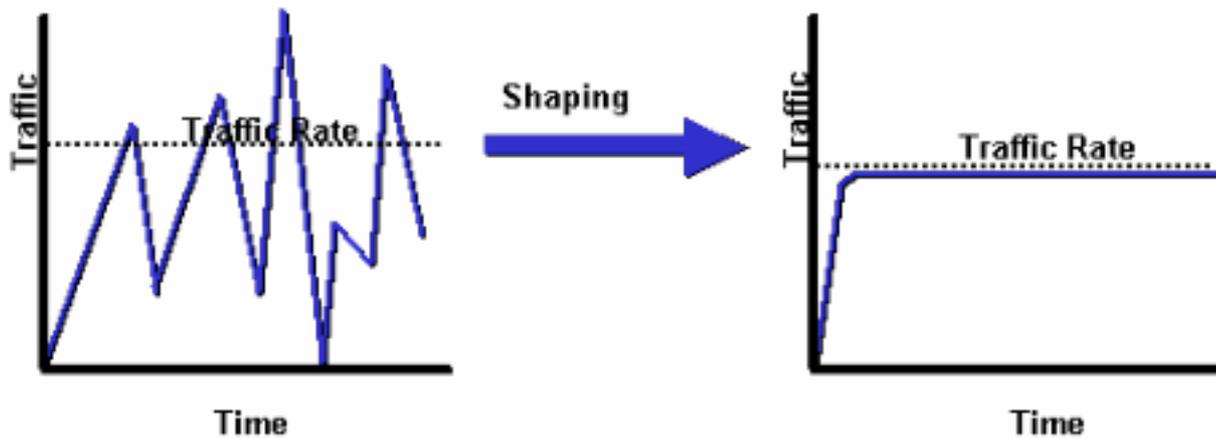
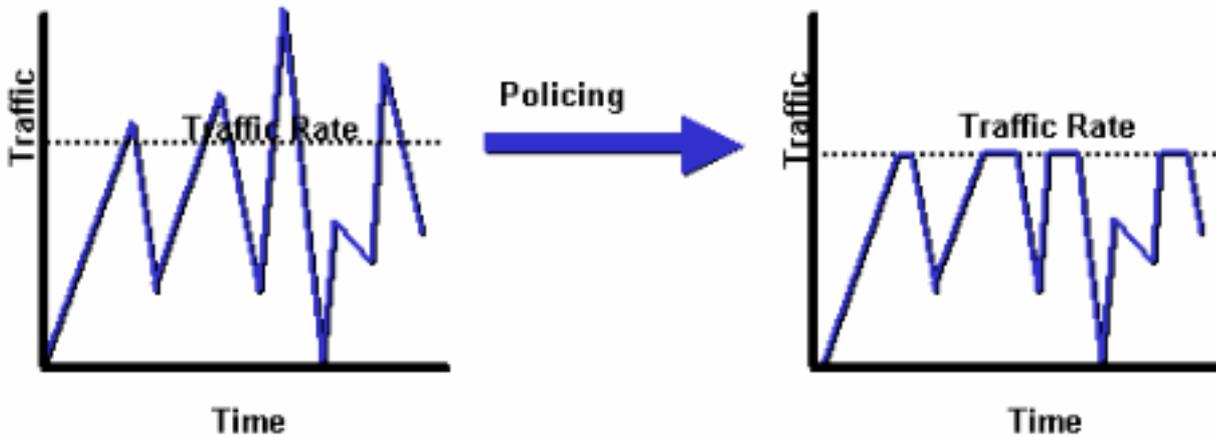
Dscp      Random drop      Tail drop      Minimum  Maximum  Mark
(Prec)    pkts/bytes        pkts/bytes     threshold threshold probability
0(0)     2362/581052      1996/491016    20       40       1/10
1        0/0              0/0            22       40       1/10
2        0/0              0/0            24       40       1/10
[output omitted]
```

폴링 및 셰이핑

Q: 폴링과 셰이핑의 차이는 무엇입니까?

A. 다음 다이어그램은 주요 차이점을 보여줍니다. 트래픽 셰이핑은 큐에서 초과 패킷을 보존한 다음 시간 증분에 따라 나중에 전송하기 위해 초과 시간을 예약합니다. 트래픽 셰이핑의 결과는 매끄러운

패킷 출력 속도입니다. 반면 트래픽 폴리싱은 버스트를 전파합니다. 트래픽 속도가 구성된 최대 속도에 도달하면 초과 트래픽이 삭제(또는 언급됨)됩니다. 그 결과 출력은 크레스트 및 트러스트가 있는 톱니처럼 나타납니다.



자세한 내용은 폴리싱 및 셰이핑 개요를 참조하십시오.

Q. 토큰 버킷이란 무엇이며 알고리즘은 어떻게 작동합니까?

A. 토큰 버킷 자체에는 폐기 또는 우선순위 정책이 없습니다. 다음은 토큰 버킷 은유가 작동하는 방법의 예입니다.

- 토큰은 일정한 속도로 버킷에 입력됩니다.
- 각 토큰은 소스에서 특정 비트 수를 보낼 수 있는 권한입니다.
- 패킷을 전송하려면 트래픽 조절기가 버킷에서 패킷 크기와 동일한 수의 토큰을 제거할 수 있어야 합니다.
- 버킷에 패킷을 전송할 수 있는 토큰이 충분하지 않을 경우, 패킷은 버킷에 충분한 토큰(셰이퍼의 경우)이 있을 때까지 기다리거나 패킷이 폐기되거나 (폴리서의 경우) 아래로 표시됨
- 버킷 자체에는 지정된 용량이 있습니다. 버킷이 용량에 도달하면 새로 도착하는 토큰은 폐기되며 향후 패킷에 사용할 수 없습니다. 따라서 언제든지 소스가 네트워크로 전송할 수 있는 최대 버스트는 버킷 크기와 거의 비례합니다. 토큰 버킷은 버스트티를 허용하지만 그 범위를 제한합니다.

Q. 클래스 기반 폴리싱과 같은 트래픽 폴리싱을 사용하는 경우 BC(Committed Burst) 및 Excess Burst(Be)는 무엇을 의미하며 이러한 값을 어떻게 선택해야 합니까?

A. 트래픽 폴리서는 잉여 패킷을 버퍼링하지 않고 나중에 송수신합니다(예: 웨이퍼). 대신 폴리서는 간단한 전송을 실행하거나 버퍼링 없이 정책을 보내지 않습니다. 혼잡 기간 동안에는 버퍼링할 수 없으므로 확장 버스트를 올바르게 구성하여 패킷을 덜 공격적으로 삭제하는 것이 가장 좋습니다. 따라서 폴리서가 일반 버스트 및 확장 버스트 값을 사용하여 구성된 CIR(Committed Information Rate)에 도달하는지 확인해야 합니다.

버스트 매개변수는 라우터에 대한 일반 버퍼링 규칙에 따라 느슨하게 모델링됩니다. 이 규칙은 혼잡 시 모든 연결의 미해결 TCP(Transmission Control Protocol) 창을 수용하기 위해 왕복 시간 비트 전송률과 동일한 버퍼링을 구성할 것을 권장합니다.

다음 표에서는 일반 및 확장 버스트 값에 대한 목적 및 권장 수식에 대해 설명합니다.

버스트 매개변수	목적	권장 수식
정상 버스트	<ul style="list-style-type: none"> 표준 토큰 버킷을 구현합니다. 토큰 버킷의 최대 크기를 설정합니다(Be가 BC보다 클 경우 토큰을 빌릴 수 있음). 새로 도착하는 토큰이 삭제되고 버킷이 용량에 도달하면 향후 패킷에서 사용할 수 없으므로 토큰 버킷의 크기를 결정합니다. 	$CIR \text{ [BPS]} * (1 \text{ byte}) / (8 \text{ bits}) * 1.5 \text{ seconds}$ <p>참고: 1.5초는 일반적인 왕복 시간입니다.</p>
확장 버스트	<ul style="list-style-type: none"> 확장 버스트 기능이 있는 토큰 버킷을 구현합니다. BC = Be를 설정하여 비활성화되었습니다. BC가 Be인 경우, 트래픽 조절기는 토큰을 빌릴 수 없으며, 토큰이 충분하지 않으면 패킷을 삭제합니다. 	$2 * \text{normal burst}$

모든 플랫폼이 정책에 대해 동일한 범위의 값을 사용하거나 지원하는 것은 아닙니다. 특정 플랫폼에 대해 지원되는 값을 알아보려면 다음 문서를 참조하십시오.

- [폴리싱 및 셰이핑 개요](#)

Q. CAR(Committed Access Rate) 또는 클래스 기반 폴리싱은 패킷이 CIR(Committed Information Rate)을 따르는지 아니면 초과하는지를 어떻게 결정합니까? 라우터가 구성된 CIR보다 비율이 낮더라도 패킷을 삭제하고 초과 속도를 보고합니다.

A. 트래픽 폴리서는 일반 버스트 및 확장 버스트 값을 사용하여 구성된 CIR에 도달하도록 합니다. 충분한 버스트 값을 설정하면 처리량이 향상됩니다. 버스트 값이 너무 낮게 구성된 경우 달성 속도가 구성된 속도보다 훨씬 낮을 수 있습니다. 일시적인 버스트를 처벌하는 것은 TCP(Transmission Control Protocol) 트래픽의 처리량에 심각한 악영향을 미칠 수 있습니다. CAR에서는 **show interface rate-limit** 명령을 실행하여 현재 버스트를 모니터링하고 표시된 값이 제한(BC) 및 확장 제한(Be) 값에 일관되게 근접하는지 여부를 확인합니다.

```
rate-limit 256000 7500 7500 conform-action continue exceed-action drop
rate-limit 512000 7500 7500 conform-action continue exceed-action drop
```

```
router# show interfaces virtual-access 26 rate-limit
Virtual-Access26 Cable Customers
  Input
    matches: all traffic
    params: 256000 BPS, 7500 limit, 7500 extended limit
    conformed 2248 packets, 257557 bytes; action: continue
    exceeded 35 packets, 22392 bytes; action: drop
    last packet: 156ms ago, current burst: 0 bytes
    last cleared 00:02:49 ago, conformed 12000 BPS, exceeded 1000 BPS
  Output
    matches: all traffic
    params: 512000 BPS, 7500 limit, 7500 extended limit
    conformed 3338 packets, 4115194 bytes; action: continue
    exceeded 565 packets, 797648 bytes; action: drop
    last packet: 188ms ago, current burst: 7392 bytes
    last cleared 00:02:49 ago, conformed 194000 BPS, exceeded 37000 BPS
```

자세한 내용은 다음 문서를 참조하십시오.

- [폴리싱 및 셰이핑 개요](#)
- [Catalyst 6000의 QoS 폴리싱](#)
- [Catalyst 4000의 서비스 품질\(FAQ\)](#)
- [Catalyst G-L3 Series Switch 및 WS-X4232-L3 Layer 3 Module QoS FAQ](#)

Q. 버스트 및 대기열 제한은 서로 독립적입니까?

A. 예, 폴리서 버스트 및 대기열 제한은 서로 별개이며 독립적입니다. 정책을 특정 수의 패킷(또는 바이트)을 허용하는 게이트로 볼 수 있으며, 큐는 네트워크에서 전송하기 전에 허용되는 패킷을 보유하는 크기 **대기열 제한**의 버킷으로 볼 수 있습니다. 버킷이 게이트에서 허용되는 **버스트**의 바이트/패킷을 보관할 수 있을 만큼 충분히 커야 합니다(폴리서).

QoS(Quality of Service) 프레임 릴레이

Q. CIR(Committed Information Rate), BC(Committed Burst), Excess Burst(Be) 및 Minimum CIR(MinCIR)에 대해 어떤 값을 선택해야 합니까?

A. Frame Relay Traffic Shaping(프레임 릴레이 트래픽 셰이핑 명령을 실행하여 활성화하는 프레임 릴레이 트래픽 셰이핑)은 여러 구성 가능한 매개변수를 지원합니다. 이러한 매개변수에는 `cir`, 및 `bc` 포함됩니다. 이러한 값을 선택하고 관련 show 명령을 이해하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오.

- [7200 라우터 및 하위 플랫폼에서 프레임 릴레이 트래픽 셰이핑 구성](#)

- [프레임 릴레이 트래픽 셰이핑에 대한 명령 표시](#)
- [QoS\(Quality of Service\)를 통한 VoIP over Frame Relay\(조각화, 트래픽 셰이핑, IP RTP 우선순위\)](#)

Q. Frame Relay 주 인터페이스의 Priority Queuing은 Cisco IOS 12.1에서 작동합니까?

A. 프레임 릴레이 인터페이스는 인터페이스 대기열 메커니즘 및 VC(Per-Virtual Circuit) 대기열 메커니즘을 모두 지원합니다. Cisco IOS 12.0(4)T부터 인터페이스 대기열은 FRTS(Frame Relay Traffic Shaping)를 구성할 때만 FIFO(First In First Out) 또는 PIQ(Per Interface Priority Queuing)를 지원합니다. 따라서 Cisco IOS 12.1로 업그레이드하면 다음 컨피그레이션이 더 이상 작동하지 않습니다.

```
interface Serial0/0
  frame-relay traffic-shaping
  bandwidth 256
  no ip address
  encapsulation frame-relay IETF
  priority-group 1

!
interface Serial0/0.1 point-to-point
  bandwidth 128
  ip address 136.238.91.214 255.255.255.252
  no ip mroute-cache
  traffic-shape rate 128000 7936 7936 1000
  traffic-shape adaptive 32000
  frame-relay interface-dlci 200 IETF
```

FRTS가 활성화되지 않은 경우 CBWFQ(Class Based Weighted Fair Queuing)와 같은 대체 대기열 처리 방법을 기본 인터페이스에 적용할 수 있습니다. 이 방법은 단일 대역폭 파이프처럼 작동합니다. 또한 Cisco IOS 12.1.1(T)부터 프레임 릴레이 주 인터페이스에서 PIQ(Frame Relay Permanent Virtual Circuits)를 활성화할 수 있습니다. 다음 예와 같이 high, medium, normal 또는 low priority PVC를 정의하고 기본 인터페이스에서 **frame-relay interface-queue priority** 명령을 실행할 수 있습니다.

```
interface Serial3/0
  description framerelay main interface
  no ip address
  encapsulation frame-relay
  no ip mroute-cache
  frame-relay traffic-shaping
  frame-relay interface-queue priority

interface Serial3/0.103 point-to-point
  description frame-relay subinterface
  ip address 1.1.1.1 255.255.255.252
  frame-relay interface-dlci 103
  class frameclass

map-class frame-relay frameclass
  frame-relay adaptive-shaping becn
  frame-relay cir 60800
  frame-relay BC 7600
  frame-relay be 22800
  frame-relay mincir 8000
  service-policy output queueingpolicy
```

Q. FRTS(Frame Relay Traffic Shaping)는 dCEF(Distributed Cisco Express Forwarding) 및 dCBWFQ(Distributed Class Based Weighted Fair Queuing)와 연동 됩니까?

A. Cisco IOS 12.1(5)T부터 Cisco 7500 Series의 VIP에서는 분산 버전의 QoS 기능만 지원됩니다. 프레임 릴레이 인터페이스에서 트래픽 셰이핑을 활성화하려면 DTS(Distributed Traffic Shaping)를 사용합니다. 자세한 내용은 다음 문서를 참조하십시오.

- [Versatile Interface Processor-Based Distributed FRF.11 및 FRF.12 for Cisco IOS Release 12.1 T](#)
- [Cisco 7500 Series에서 분산형 QoS로 프레임 릴레이 트래픽 셰이핑](#)

비동기 전송 모드(ATM)를 통한 QoS(Quality of Service)

Q. ATM(Asynchronous Transfer Mode) 인터페이스에서 CBWFQ(Class Based Weighted Fair Queueing) 및 LLQ(Low Latency Queueing)가 포함된 서비스 정책을 어디에서 적용합니까?

A. Cisco IOS 12.2부터 ATM 인터페이스는 3가지 레벨 또는 논리적 인터페이스에서 서비스 정책을 지원합니다. 기본 인터페이스, 하위 인터페이스 및 PVC(Permanent Virtual Circuit) 정책을 적용하는 것은 활성화 중인 QoS(Quality of Service) 기능의 기능입니다. ATM 인터페이스는 VC당 혼잡 수준을 모니터링하고 VC당 초과 패킷에 대한 대기열을 유지 관리하기 때문에 VC(Virtual Circuit)당 대기열 정책을 적용해야 합니다. 자세한 내용은 다음 문서를 참조하십시오.

- [ATM 인터페이스에서 QoS 서비스 정책을 적용하는 방법은?](#)
- [PA-A3 및 NM-1A ATM 인터페이스에서 VC당 전송 대기열 이해](#)

Q. IP에서 ATM(Asynchronous Transfer Mode) COs(Class of Service) 큐잉으로 계산되는 바이트는 무엇입니까?

A. 각각 CBWFQ(Class-Based Weighted Fair Queueing) 및 LLQ(Low Latency Queueing)를 활성화하기 위해 서비스 정책에 구성된 bandwidth 및 priority 명령은 show interface 명령 출력에 의해 계산된 것과 동일한 오버헤드 바이트를 계산하는 Kbps 값을 사용합니다. 특히 레이어 3 대기열 처리 시스템은 LLC/SNAP(Logical Link Control/Subnetwork Access Protocol)를 계산합니다. 다음 항목은 계산되지 않습니다.

- ATM Adaptation Layer 5(AAL5) 트레일러
- 마지막 셀을 48바이트의 짝수로 만들기 위한 패딩
- 5바이트 셀 헤더
- [IP에서 ATM COs 큐잉으로 계산되는 바이트는 무엇입니까?](#)

Q. 서비스 정책을 동시에 지원할 수 있는 VCS(Virtual Circuit)는 몇 개입니까?

A. 다음 문서는 지원할 수 있는 ATM(Asynchronous Transfer Mode) VCS 수에 대한 유용한 지침을 제공합니다. 약 200~300개의 VBR-nrt Permanent Virtual Circuits(PVC)가 안전하게 구축되었습니다.

- [IP-ATM Class of Service 설계 가이드](#)

또한 다음을 고려하십시오.

- 강력한 프로세서를 사용합니다. 예를 들어, VIP4-80은 VIP2-50보다 훨씬 높은 성능을 제공합니다.
- 사용 가능한 패킷 메모리의 양입니다. NPE-400에서는 최대 32MB(256MB의 시스템)가 패킷 버퍼에 대해 별도로 설정됩니다. NPE-200의 경우 128MB의 시스템에서 패킷 버퍼에 대해 최대 16MB가 할당됩니다.
- 최대 200개의 ATM PVC에서 동시에 작동하는 per-VC WRED(Weighted Random Early Detection)의 컨피그레이션이 광범위하게 테스트되었습니다. VIP2-50에서 VC당 대기열에 사용할 수 있는 패킷 메모리의 양은 유한합니다. 예를 들어 8MB SRAM이 포함된 VIP2-50은 WRED가 작동하는 VC당 ATM CO에 대한 IP에 1085개의 패킷 버퍼를 제공합니다. 100개의 ATM PVC가 구성되었고 모든 VCS가 동시에 과도한 혼잡을 겪고 있다면(비 TCP 흐름 제어 소스가 사용되는 테스트 환경에서 시뮬레이션될 수 있음), 평균적으로 각 PVC에는 약 10개의 버퍼링 패킷이 있으며, 이는 WRED가 정상적으로 작동하기에는 너무 짧을 수 있습니다. 따라서 SRAM이 큰 VIP2-50 장치는 VC WRED당 실행되는 ATM PVC가 많고 동시에 혼잡을 일으킬 수 있는 설계에서 적극 권장됩니다.
- 구성된 활성 PVC의 수가 많을수록 SCR(Continued Cell Rate)이 낮아야 하며, 따라서 PVC에서 작동하는 데 WRED에 필요한 대기열이 짧습니다. 따라서 IP에서 COs(ATM Class of Service) Phase 1 기능의 기본 WRED 프로필을 사용하는 경우와 마찬가지로, 매우 많은 수의 저속 혼잡한 ATM PVC에서 per-VC WRED가 활성화된 경우 낮은 WRED 삭제 임계값을 구성하면 VIP에서 버퍼 부족 위험을 최소화할 수 있습니다. VIP에 버퍼 부족이 발생하지 않습니다. VIP에서 버퍼가 부족한 경우 IP to ATM COs Phase 1 기능은 버퍼 부족 기간 동안 FIFO(First In First Out) tail drop(즉, 이 PVC에서 IP to ATM COs 기능이 활성화되지 않은 경우 발생하는 삭제 정책)으로 간단히 다운그레이드됩니다.
- 합리적으로 지원할 수 있는 최대 동시 VCS 수입니다.

Q. 클래스 기반 CBWFQ(Weighted Fair Queueing) 및 LLQ(Low Latency Queueing) 등의 IP-ATM(ATM Class of Service) 기능을 지원하는 ATM(Asynchronous Transfer Mode) 하드웨어는 무엇입니까?

A. IP-ATM COs는 VC(Per-Virtual Circuit)를 기준으로 활성화되는 기능 집합을 의미합니다. 이 정의를 통해 IP-ATM CO는 ATM 인터페이스 프로세서(AIP), PA-A1 또는 4500 ATM 네트워크 프로세서에서 지원되지 않습니다. 이 ATM 하드웨어는 PA-A3 및 대부분의 네트워크 모듈(ATM-25 제외)이 정의하므로 VC당 큐잉을 지원하지 않습니다. 자세한 내용은 다음 문서를 참조하십시오.

- [IP-ATM CO에 대한 ATM 하드웨어 지원 이해](#)
- [RSP 기반 플랫폼의 VC 클래스 기반 가중 공정 대기열](#)
- [Cisco 7200, 3600 및 2600 라우터의 VC 클래스 기반, 가중 공정 대기열\(CBWFQ당\)](#)
- [PA-A3-8T1/E1 IMA ATM 포트 어댑터의 VC 단위 대기열](#)
- [MC3810에서 ATM Per-VC Queueing 구성](#)

음성 및 서비스 품질(QoS)

Q. LFI(Link Fragmentation and Interleaving)는 어떻게 작동합니까?

A. 네트워크에서 FTP(File Transfer Protocol) 전송과 같은 대용량 패킷을 WAN을 통해 처리할 경우

텔넷 및 VoIP 등의 인터랙티브 트래픽이 레이턴시를 증가시키기 쉽습니다. 인터랙티브 트래픽의 패킷 지연은 FTP 패킷이 느린 WAN 링크에서 대기될 때 중요합니다. 더 큰 패킷을 조각화하고 더 큰 패킷(FTP) 패킷의 프래그먼트 간에 더 작은(음성) 패킷을 큐잉하는 방법을 고안했습니다. Cisco IOS 라우터는 여러 레이어 2 프래그먼트화 메커니즘을 지원합니다. 자세한 내용은 다음 문서를 참조하십시오.

- [링크 효율성 메커니즘 개요](#)
- [QoS\(Quality of Service\)를 통한 VoIP over Frame Relay\(조각화, 트래픽 셰이핑, IP RTP 우선순위\)](#)
- [QoS\(Quality of Service\)를 통한 VoIP 링크\(LLQ/IP RTP 우선순위, LFI, cRTP\)](#)

Q. VoIP(Voice over IP) 성능을 모니터링하는 데 사용할 수 있는 툴은 무엇입니까?

A. Cisco는 현재 Cisco의 Voice over IP 솔루션을 사용하여 네트워크에서 QoS(Quality of Service)를 모니터링하는 여러 옵션을 제공합니다. 이러한 솔루션은 PSQM(Perceptual Speech Quality Measurement) 또는 음성 품질 측정을 위한 새로운 제안 알고리즘 중 일부를 사용하여 음성 품질을 측정하지 않습니다. HP(Agent) 및 NetIQ의 툴을 이러한 용도로 사용할 수 있습니다. 그러나 Cisco는 지연, 지터 및 패킷 손실을 측정함으로써 경험하는 음성 품질에 대한 아이디어를 제공하는 툴을 제공합니다. 자세한 내용은 [Cisco Service Assurance Agent](#) 및 [Internetwork Performance Monitor](#)를 사용하여 Voice over IP Networks에서 서비스 품질 관리를 참조하십시오.

Q.%SW_MGR-3-CM_ERROR_FEATURE_CLASS:연결 관리자 기능 오류:클래스 SSS:(QoS) - 설치 오류, 무시.

A. 관찰된 기능 설치 오류는 유효하지 않은 구성이 템플릿에 적용될 때 예상되는 동작입니다. 충돌 때문에 서비스 정책이 적용되지 않았음을 나타냅니다. 일반적으로 계층적 정책 맵에서 하위 정책의 클래스 기본값에 대한 셰이핑을 구성하는 대신 인터페이스의 상위 정책에서 구성해야 합니다. 이 메시지는 추적과 함께 출력됩니다.

세션 기반 정책을 사용하는 경우, class-default의 셰이핑은 하위 인터페이스 또는 PVC 수준에서만 수행해야 합니다. 물리적 인터페이스에서 셰이핑은 지원되지 않습니다. 물리적 인터페이스에서 컨피그레이션이 수행되는 경우 이 오류 메시지가 발생하는 것은 정상적인 동작입니다.

LNS의 경우 세션이 시작될 때 서비스 정책을 radius 서버를 통해 프로비저닝할 수 있기 때문일 수 있습니다. RADIUS 서버 컨피그레이션을 보고 세션이 시작되거나 플랩될 때 radius 서버를 통해 설치된 잘못된 서비스 정책을 보려면 show tech 명령을 실행합니다.

[관련 정보](#)

- [성능 튜닝 기본 사항](#)
- [QoS\(Quality of Service\) 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)