애플리케이션 **보안 · 가속 · 성능**을 보장하는

파이오링크 슈퍼ADC

PAS-K

User Guide

PIOLINK

등록 상표

PIOLINK는 ㈜파이오링크의 등록상표입니다.

일러두기

- 본 사용 설명서의 저작권은 ㈜파이오링크에 있습니다. 본 사용 설명서는 저작권법에 의하여 법적으로 보호 받고 있으며, 저작권자의 사전 서면 허가 없이는 어떠한 이유에서든 무단으로 전체 혹은 일부분의 내용을 발췌하거나 어떠한 형태로든 복제할 수 없습니다.
- 본 사용 설명서는 제품의 기능 향상과 인쇄상의 오류 수정 등으로 인하여 예고 없이 변경될 수 있습니다.
- 본 사용 설명서 및 그 내용에 의해 직접, 간접으로 발생될 수 있는 피해 및 재산상 손해에 대해 ㈜파이오링크에 법적인 책임이 없음을 밝힙니다.
- 이 제품은 업무용으로 전자파 적합 등록을 한 제품이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

PIOLINK Application Switch-K 1500/2400/2800/4200/4400/4800 사용 설명서 (2013.09)

전화: 1544-9890/ Web page: http://www.piolink.co.kr

시작하기 전에

설명서 소개

이 설명서는 PAS-K1500/2400/2800/4200/4400/4800 사용자를 위한 사용 설명서입니다. 이 설명서에는 CLI(Command Line Interface)를 통한 PAS-K1500/2400/2800/4200/4400/4800의 설정과 관리 방법에 대해 설명합니다. PAS-K1500/2400/2800/4200/4400/4800을 사용하기 전에 반드시 이 사용 설명서를 읽어본 후 유의하여 제품을 조작하도록 합니다. PAS-K1500/2400/2800/4200/4400/4800을 설치하는 방법은 이 설명서와 함께 제공되는 설치 설명서를 참고하도록 합니다.

대상 독자

이 사용 설명서는 이미 L2, L3 장비는 물론 PAS-K1500/2400/2800/4200/4400/4800과 같은 AP-ADC에 대한 지식과 LAN, WAN, STP, SNMP, Ethernet, 라우팅 등에 대해 이해하고 있고, LAN(Local Area Network) 구축 및 운영에 대한 경험을 가지고 있는 네트워크 관리자를 대상으로 작성되었습니다. 그러므로 이 사용 설명서에서는 이러한 내용을 별도로 설명하지 않습니다.

PLOS 버전

PLOS는 PAS-K에 설치되어 있는 파이오링크 운영 체제를 의미합니다. 이 사용 설명서는 PLOS v1.7.0.0.1 이상의 버전이 설치된 PAS-K1500/2400/2800/4200/4400/4800을 기준으로 작성되었습니다. 이전 버전의 PLOS가 설치되어 있는 경우에는 이 사용 설명서에서 설명하는 기능이 지원되지 않을 수 있고, 설명에 맞게 설정한 경우에도 정상적으로 동작하지 않을 수 있습니다. 최신 버전의 PLOS로 업데이트하는 방법은 이 설명서의 **제4장 시스템 관리와 모니터링**에 설명되어 있습니다.

설명서의 표기법

다음은 이 설명서에서 사용하는 제품의 이름과 참고 및 주의 표시에 대한 설명입니다.

제품 명칭 표기

이 설명서에서는 제품을 지칭할 때 다음과 같은 명칭을 사용합니다.

- PIOLINK Application Switch-K
  파이오링크의 AP-ADC(Advanced Platform-Application Delivery Controller) 제품군을 지칭하는 공식적인 제품 명으로, 설명서의 내용 중 제목(Title)에만 사용됩니다.
- PAS-K
  PIOLINK Application Switch-K 의 약칭으로 설명서의 본문(Contents)에서 모든 제품에 공통적으로 해당되는 내용을 설명할 때 사용되는 명칭입니다.
- PAS-K1500, PAS-K2400, PAS-K2800, PAS-K4200, PAS-K4400, PAS-K4800
  각 제품에 해당되는 내용을 설명할 때 사용되는 명칭입니다.

참고 및 주의 표기

이 사용 설명서에서 사용자에게 특별히 전달하고자 하는 내용을 다음과 같은 아이콘과 글꼴을 사용하여 표시합니다.

참고: 설명서의 내용과 관련하여 함께 알아두면 유용한 사항이나 제품을 사용하면서 도움이 될 만한 참고 사항과 관련 자료 등을 소개합니다.

주의: 데이터를 손실하거나 혹은 제품이 잘못 동작할 수 있는 상황을 설명하고, 그 상황에 대한 대처 방법을 알려줍니다.

화면 내용 표기

이 사용 설명서는 터미널 세션에서 출력되는 내용이나 사용자가 직접 입력해야 하는 CLI 명령이나 키워드 등을 구분하기 위해 다음과 같은 표기를 사용합니다.

표기	설 명	예
#	시스템 프롬프트를 나타내는 기호	`(config)#`
bold	명령어나 키워드는 굵게 표시합니다.	`(config)# **hostname**`
<Italics>	값을 지정하는 인자(변수)는 기울임꼴(italic)로 표시합니다.	`(config)# **ping** *<HOST>*`
[ ]	옵션 기능으로 사용할 변수나 명령어를 대괄호 [ ] 안에 표시합니다.	`(config)# **show interface** [*<NAME>* | **mgmt**]`
{**x** | **y** | **z**}	선택 가능한 변수들을 수직선으로 나누어 중괄호 { } 안에 표기하며, 사용할 변수를 선택합니다.	`(config-slb[s2])# **status** {**enable** | **disable**}`

제품 아이콘

아이콘	예
	구성도나 제품 설명 등에 사용되는 제품 아이콘으로, PAS-K1500/2400/2800/4200/4400/4800을 나타냅니다.

관련 문서

이 설명서와 함께 다음과 같은 문서가 제공됩니다.

- PAS-K1500/2400/2800/4200/4400/4800 명령 설명서 (Command Reference)
  PAS-K 에서 제공하는 CLI(Command Line Interface) 명령의 사용 방법을 알려주는 설명서입니다. CLI 명령을 기능에 따라 분류하여 각 장마다 유사한 기능을 제공하는 명령들을 설명하고 있으며, 각 명령을 사용하는 방법과 참고 사항, 사용 예 등을 확인할 수 있습니다.
- PAS-K1500/2400/2800/4200/4400/4800 설치 설명서 (Installation Guide)
  PAS-K 의 앞면, 뒷면, 옆면에 있는 각 부분의 기능을 소개하고, PAS-K 를 랙에 설치한 후 각 포트에 장비를 연결하는 방법을 알려주는 설명서입니다. PAS-K 의 하드웨어 사양과 장비 연결 시 사용하는 케이블에 대한 상세한 사양도 이 설명서에서 확인할 수 있습니다.
- PAS-K1500/2400/2800/4200/4400/4800 케이스 스터디 (Case Study)
  PAS-K 의 설정 사례를 보여주는 설명서입니다. PAS-K 의 주요 기능을 보다 쉽게 설정할 수 있도록 다양한 구성 예와 함께 CLI 명령을 사용한 설정 방법을 설명합니다.
- PAS-K1500/2400/2800/4200/4400/4800 MIB 설명서 (MIB Reference)
  PAS-K 가 제공하는 SNMP MIB 정보에 대해 알려주는 설명서입니다.

서비스 지원

고객 서비스나 기술 지원, 혹은 기술 교육에 관한 자세한 정보가 필요한 경우에는 다음 연락처로 문의하시면 필요한 도움을 받을 수 있습니다.

- 기술지원센터(TAC) 1544-9890
- E-mail support@piolink.com

설명서 구성

이 설명서의 각 장은 다음과 같은 내용으로 구성되어 있습니다.

제1장 PIOLINK Application Switch-K 소개

이 장에서는 PAS-K에서 제공하는 주요한 기능들과 특징에 대해 소개합니다.

제2장 사용하기 전에

이 장에서는 CLI로 접속하는 방법과 기본적인 CLI 사용 방법에 대해 소개합니다.

제3장 기본 네트워크 설정

이 장에서는 PAS-K의 기본적인 구성 작업에 대해 알아봅니다. PAS-K는 출하될 때 이미 기본적인 구성이 되어 있는 상태이기 때문에 이 장에서 설명하는 구성 작업을 하지 않고 제품을 바로 사용할 수 있습니다. 하지만 사용자의 네트워크 환경에 맞게 장비의 설정을 변경해야 하는 경우에는 이 장의 내용을 참고하여 원하는 환경으로 구성하도록 합니다.

제4장 시스템 관리와 모니터링

이 장에서는 PAS-K 시스템을 관리하는데 필수적인 기능들과 시스템의 기본적인 정보와 상태 정보, 로그 등을 모니터링하는 방법에 대해 살펴봅니다.

제5장 SNMP 설정

이 장에서는 SNMP(Simple Network Management Protocol)에 대해 살펴본 후 PAS-K에 SNMP를 설정하는 방법에 대해 소개합니다.

제6장 포트 바운더리 설정

이 장에서는 PAS-K의 포트로 수신되는 패킷을 처리하기 위해 포트 바운더리를 설정하는 방법에 대해 설명합니다.

제7장 부하 분산 설정

이 장에서는 서버와 방화벽, VPN 등의 부하를 적절하게 분산하여 자원의 가용성과 안정성을 높여주는 PAS-K의 L4, L7 부하 분산 기능에 대해 살펴봅니다.

제8장 Failover 설정

이 장에서는 Failover를 위한 VRRP(Virtual Router Redundancy Protocol)와 eVRRP(enhanced VRRP)에 대해 살펴본 후 PAS-K에 Failover를 구성하기 위해 이 기능들을 PAS-K에서 설정하는 방법에 대해 설명합니다.

제9장 보안 설정

이 장에서는 PAS-K에서 기본으로 제공되는 보안 기능인 시스템 접근 제어와 방화벽 기능에 대해 살펴봅니다.

제10장 QoS 설정

이 장에서는 PAS-K에서 제공하는 QoS(Quality of Service) 기능에 대해 소개한 후 PAS-K에서 QoS 기능을 사용할 수 있도록 설정하는 방법에 대해 설명합니다.

목 차

PAS-K 1500/2400/2800/4200/4400/4800 사용 설명서 i

시작하기 전에 3
설명서 소개 3
대상 독자 3
PLOS 버전 3
설명서의 표기법 3
관련 문서 4
서비스 지원 4
설명서 구성 5
목 차 6

제 1 장 PIOLINK Application Switch-K 소개 17

제품 개요 17

제품 개요 18
소개 18
주요 기능 20
주요 특징 21

제 2 장 사용하기 전에 22

유지 보수 라이센스 등록 22

유지 보수 라이센스 등록 23
유지 보수 라이센스 발급 23
CLI에서 설정하기 26
유지 보수 라이센스 등록하기 26

CLI 사용 27
CLI 접속 27
PIOLINK Application Switch-K 부팅하기 27
CLI 로그인하기 28
CLI 로그아웃하기 28
기본적인 CLI 사용 방법 29
명령이나 키워드 출력 29
명령 라인 편집 30
명령 모드 30

제 3 장 기본 네트워크 설정 31

포트 설정 32
CLI에서 설정하기 33
포트 속도와 전송 모드 설정 33
MDI/MDI-X 설정 33
Auto negotiation 설정 34
흐름 제어(flow control) 설정 34
Flood rate 설정 34

Description 설정 34
포트의 동작 상태 설정 35
포트 정보 출력 35

VLAN 설정 36
VLAN 개요 36
CLI에서 설정하기 38
VLAN 생성 및 포트 추가 38
VLAN 설정 정보 보기 38
VLAN 멀티캐스트 브리지 설정 39
VLAN 멀티캐스트 브리지 설정 정보 보기 39

MAC Ageing Time 설정 40
CLI에서 설정하기 40
MAC Ageing Time 설정 40
MAC Ageing Time 설정 정보 보기 40

IP 주소/라우팅 설정 41
IPv4 주소 41
IPv6 주소 41
라우팅 설정 43
CLI에서 설정하기 44
인터페이스의 IP 주소 설정 44
인터페이스의 MTU 설정 44
인터페이스 활성화/비활성화 44
기본 게이트웨이 추가 45
고정 경로 추가 45
IPv6 Neighbor 설정 46
설정 정보 확인 46

Proxy ARP 설정 47
Proxy ARP 개요 47
CLI에서 설정하기 48
Proxy ARP 설정 48
Proxy ARP 설정 정보 보기 48

ARP Locktime 설정 49
ARP Locktime 개요 49
CLI에서 설정하기 50
ARP Locktime 설정 50
ARP Locktime 설정 정보 보기 50

ARP Filter 설정 51
CLI에서 설정하기 51
Input ARP Filter 설정하기 51
Ouput ARP Filter 설정하기 52
ARP Filter 설정 정보 보기 52

저장 MAC 응답 설정 53
CLI에서 설정하기 53
저장 MAC 응답 설정 53
저장 MAC 응답 설정 정보 보기 53

정적(Static) ARP 캐시 설정 54
CLI에서 설정하기 54
정적 ARP 캐시 설정 54

정적 ARP 캐시 설정 정보 보기 54
DNS 설정 55
CLI에서 설정하기 55
DNS 서버 설정 55
DNS 서버 설정 정보 보기 55
링크 싱크(Linksync)설정 56
링크 싱크 개요 56
CLI에서 설정하기 57
링크 싱크 설정 57
링크 싱크 설정 정보 보기 58
포트 미러링 설정 59
포트 미러링 개요 59
CLI에서 설정하기 60
포트 미러링 설정 60
포트 미러링 설정 정보 보기 60
Link Aggregation 설정 61
Link Aggregation 개요 61
포트 트렁킹 61
LACP 61
Link Aggregation 설정 시 주의 사항 62
CLI에서 설정하기 63
포트 트렁킹 설정 63
포트 트렁킹 정보 보기 63
LACP 설정 63
LACP 장비 우선순위 설정 64
LACP 설정 정보 보기 64
포트 Failover설정 65
개요 65
CLI에서 설정하기 65
포트 Failover 설정 65
그룹 포트의 설정 정보 보기 65
STP/RSTP/PVSTP/MSTP 설정 66
STP(Spanning Tree Protocol) 개요 66
BPDU(Bridge Protocol Data Unit) 67
포트의 상태 68
경로 선택하기 69
RSTP(Rapid Spanning Tree Protocol) 개요 70
포트의 상태 70
BPDU 정책 변화 70
네트워크 Convergence 시간 단축 71
PVSTP/MSTP(Per VLAN Spanning Tree Protocol/Multiple Spanning Tree Protocol) 개요 73
CLI에서 설정하기 76
STP/RSTP/PVSTP/MSTP 활성화/비활성화 76
우선순위 설정 76
경로 비용 설정 77
포트 우선순위 설정 77
Hello Time 설정 78
Forward Delay Time 설정 78
Maximum Aging Time 설정 78

Edge 포트 설정 79
MST Region 설정 79
Instance 설정 80
설정 정보 보기 82

NAT64/DNS64 설정 83
CLI에서 설정하기 83
Source NAT 풀 설정 83
NAT64 Prefix 설정 84
DNS64 필터 설정 84
DNS64 네임 서버 설정 85
NAT64 규칙 설정 85
설정 정보 보기 86
NAT64 세션 엔트리 정보 86

네트워크 연결 확인 87
Ping 연결 테스트 87
패킷 경로 추적 88

제 4 장 시스템 관리와 모니터링 89

시스템 정보 90
CLI에서 시스템 정보 출력하기 90
시스템 기본 정보 출력 90
시스템 자원 사용 상태 출력 90
하드웨어 상태 출력 90

기본 시스템 관리 91
시스템 이름 설정 91
시스템 이름 설정 91
로그인 배너 설정 91
관리 접근 서비스 설정 92
관리 접근 서비스 상태 및 포트 설정 92
관리 접근 서비스 설정 정보 보기 92
터미널 설정 93
터미널 연결 제한 시간 설정 93
터미널 길이 설정 93
터미널 설정 정보 보기 93
시스템 시간 설정 94
시스템 시간 직접 설정 94
시스템 시간 직접 설정 정보 보기 94
NTP(Network Time Protocol) 클라이언트 설정 95
NTP(Network Time Protocol) 클라이언트 설정 정보 보기 95

설정 파일 96
설정 파일 개요 96
CLI에서 설정 파일 사용하기 97
설정 파일 저장 97
설정 파일 복사 97
설정 파일 업로드/다운로드 98
초기 설정 복구 99
설정 파일 내용 출력 99

PLOS 101

CLI에서 설정하기 101
PLOS 업데이트 101
PLOS 정보 출력 101
시스템 종료 101
세션 유지 시간 102
개요 102
유지 시간을 설정할 수 있는 세션의 종류 102
세션 유지 시간의 기본 설정값 104
CLI에서 설정하기 105
세션 유지 시간 설정 105
세션 유지 시간 설정 정보 보기 106
기술 지원 도우미 107
CLI에서 설정하기 107
동작 로그 정보 설정 107
사용자 계정 및 인증 108
사용자 관리 108
CLI에서 사용자 관리하기 108
RADIUS 서버 설정 110
CLI에서 설정하기 110
로그 관리 112
로그 개요 112
CLI에서 설정하기 114
이벤트 레벨 설정 114
시스로그 서버 설정 114
이메일 알람 설정 115
로그 설정 정보 보기 116
이메일 알람 설정 정보 보기 116
로그 출력 116
로그 삭제 116
포트 모니터링 117
CLI에서 모니터링하기 117
시스템 감시 118
명령 사용 이력 조회 118
FAN Hot Swap 118

제 5 장 SNMP 설정 119

SNMP 개요 120
SNMP 구성 요소 120
SNMP 매니저와 에이전트의 통신 122
인증 122
통신 명령 122
로드 타임아웃 123
SNMP 버전 123
SNMP 설정 124
설정하기 전에 124
SNMP 설정 항목 124

SNMP 설정 시 주의 사항-SNMP의 동작 상태와 SNMP 설정 값의 적용 124
CLI에서 설정하기 125
SNMP 커뮤니티 설정 125
SNMP 사용자 설정 125
SNMP 로드 타임아웃 설정 126
SNMP 트랩 호스트 설정 126
SNMP Generic 트랩 설정 127
장비 정보(이름, 연락처, 위치) 설정 127
SNMP 활성화 및 설정 적용 127
SNMP 설정 정보 보기 128

제 6 장 포트 바운더리 설정 129

포트 바운더리 개요 129

포트 바운더리 개요 130
포트 바운더리의 적용 범위 제한 131
포트 바운더리의 ID 131
Promisc 모드와 Include MAC 모드 132

포트 바운더리 설정 133
CLI에서 설정하기 134
포트 바운더리 설정 134
포트 바운더리 설정 정보 보기 135

제 7 장 부하 분산 설정 136

L4 부하 분산 137
개요 137
L4 서버 부하 분산 137
기존 네트워크 vs 서버 부하 분산 적용 네트워크 138
가상 서버 기반 부하 분산 139
필터 139
서버 부하 분산의 NAT 모드 139
애플리케이션 종류 143
고급 L4 서버 부하 분산 143
방화벽 부하 분산 144
방화벽 개요 144
방화벽 부하 분산 구성 145
필터 145
지속 연결 145
방화벽 부하 분산의 동작 방식 146
고급 방화벽/VPN 부하 분산 146
VPN 부하 분산 147
VPN 개요 147
VPN 부하 분산 구성 148
지속 연결 149
필터 149
캐시 서버 부하 분산 150
개요 150
캐시 서버 부하 분산 구성 150
필터 151

게이트웨이 부하 분산 152
동작 과정 153
필터와 NAT 규칙 155
글로벌 서버 부하 분산 156
용어 157
글로벌 서버 부하 분산 동작 과정 158
PAS-K의 DNS 동작 160
실제 서버 선택 과정 160
L4 부하 분산 서비스의 고가용성 기능 161
실제 서버 백업 161
서비스 백업 161
Stateful Failover 161
세션 유지 시간 162

L7 부하 분산 163
개요 163
L7 부하 분산 과정 163
버퍼링 164
구문 해석(Parsing) 164
지연 바인딩(Delayed Binding) 164
커넥션 풀링(Connection Pooling) 166
실제 서버 선택 167
TCP Splicing 167
Non-HTTP 트래픽 처리 167
L7 서버 부하 분산 171
고급 L7 서버 부하 분산 171
L7 캐시 서버 부하 분산 172
필터 172
고급 L7 캐시 서버 부하 분산 172
패턴(Pattern) 173
규칙(Rule) 175
액션(Action) 175
URL 변경(URL Manipulation) 177
HTTP Redirection 178
URL Rewrite 178
그룹(Group) 179

실제 서버(Real Server) 180
최대 연결 세션 기능(Max Connection) 180
백업 실제 서버(Backup Real Server) 180
Graceful Shutdown 기능 181
서버의 MTU 181

부하 분산 방식 182

장애 감시(Health Check) 185
개요 185
장애 감시 방법 187
HTTP 장애 감시 187
ICMP 장애 감시 188
NTP 장애 감시 189
TCP 장애 감시 190
TFTP 장애 감시 192
UDP 장애 감시 193

스크립트 장애 감시 194
RADIUS 서버 장애 감시 194
지속 연결(Persistence) 195
지속 연결 기능의 종류 196
IP 지속 연결 196
HTTP 쿠키 지속 연결 197
HTTP 헤더 지속 연결 202
세션 ID 지속 연결 203
애플리케이션 가속(Application Accelerator) 204
개요 204
HTTP 압축(HTTP Compression) 204
캐싱(Caching) 206
SSL 가속(SSL Acceleration) 207
백엔드 기능 208
비밀 키와 인증서(Certificate) 208
프로필(Profile) 208
SSL SNI(Server Name Indication) 209
장애 감시 설정 210
CLI에서 설정하기 210
장애 감시 설정 210
설정 정보 보기 215
실제 서버 설정 216
CLI에서 설정하기 216
실제 서버 설정 216
설정 정보 보기 219
정적 필터 220
CLI에서 설정하기 220
정적 필터 설정 220
HTTP 압축 규칙 설정 221
CLI에서 설정하기 221
설정 정보 보기 221
캐싱 규칙 설정 222
CLI에서 설정하기 222
설정 정보 보기 222
SSL 가속 설정 223
CLI에서 설정하기 223
비밀 키 설정 223
인증 요청서 설정 225
인증서 설정 226
클라이언트 인증서 설정 227
프로필 설정 228
설정 정보 보기 229
L4 서버 부하 분산 설정 230
CLI에서 설정하기 230
L4 서버 부하 분산 서비스 정의 230
필터 설정 232
설정 정보 보기 233

고급 L4 서버 부하 분산 설정 234
CLI에서 설정하기 234
고급 L4 서버 부하 분산 서비스 정의 234
설정 정보 보기 236
방화벽/VPN 부하 분산 설정 237
CLI에서 설정하기 237
방화벽/VPN 부하 분산 서비스 정의 237
필터 설정 240
설정 정보 보기 241
고급 방화벽/VPN 부하 분산 설정 242
CLI에서 설정하기 242
고급 방화벽/VPN 부하 분산 서비스 정의 242
필터 설정 243
설정 정보 보기 244
L4 캐시 서버 부하 분산 설정 245
CLI에서 설정하기 245
캐시 서버 부하 분산 서비스 정의 245
필터 설정 246
설정 정보 보기 247
게이트웨이 부하 분산 설정 248
CLI에서 설정하기 248
게이트웨이 부하 분산 서비스 정의 248
필터 설정 249
설정 정보 보기 250
글로벌 서버 부하 분산 설정 251
설정 시 주의 사항 251
CLI에서 설정하기 251
글로벌 서버 부하 분산 서비스 정의 251
네임 서버 설정 252
그룹 설정 253
규칙 설정 254
설정 정보 보기 255
L7 서버 부하 분산 설정 256
CLI에서 설정하기 256
패턴 정의 256
L7 서버 부하 분산 서비스 정의 258
그룹 설정 260
규칙 설정 263
URL 변경 설정 265
설정 정보 보기 266
고급 L7 서버 부하 분산 설정 267
CLI에서 설정하기 267
고급 L7 서버 부하 분산 서비스 정의 267
그룹 설정 269
URL 변경 설정 271
RTS(Revers To Sender) 실제 서버 설정 272
규칙 설정 273
설정 정보 보기 274

L7 캐시 서버 부하 분산 설정 275
CLI에서 설정하기 275
L7 캐시 서버 부하 분산 서비스 정의 275
그룹 설정 277
규칙 설정 277
URL 변경 설정 277
필터 설정 277
설정 정보 보기 278
고급 L7 캐시 서버 부하 분산 설정 279
CLI에서 설정하기 279
고급 L7 캐시 서버 부하 분산 서비스 정의 279
그룹 설정 281
URL 변경 설정 281
규칙 설정 281
필터 설정 282
설정 정보 보기 283
세션 엔트리 및 통계 정보 출력 284
세션 엔트리 목록 보기 284
통계 정보 보기 287
CLI에서 보기 287
부하 분산 서비스 목록 보기 288

제 8 장 Failover 설정 289

VRRP와 eVRRP 289
VRRP와 eVRRP 290
VRRP 개요 290
eVRRP(Enhanced VRRP) 개요 292
Active-Standby Failover 294
주의 사항 296
Stateful Failover 297
Stateful Failover의 동작 예 297
Stateful Failover 사용 시 주의사항 298
eVRRP 설정하기 299
Active-Standby Failover 설정 299
CLI에서 설정하기 299
Stateful Failover 설정하기 303
CLI에서 설정하기 303
Failover 설정 정보 보기 304
CLI에서 보기 304

제 9 장 보안 설정 305

보안 기능 개요 306
시스템 접근 제어 306
방화벽(Firewall) 308
보안 기능 설정 309

시스템 접근 제어 설정 309
접근 규칙 설정하기 309
기본 접근 정책 설정하기 310
시스템 접근 제어 설정 정보 보기 310
방화벽 설정 311
컨텐트 설정하기 311
컨텐트 그룹 설정하기 312
필터 설정하기 313
필터 그룹 설정하기 315
정책 설정하기 316
방화벽 설정 정보 보기 317

제 10 장 QoS 설정 318

QoS 개요 319
기능 소개 319
구성 요소 319
클래스 319
정책 320
대역폭 제한(Rate Limit) 320
서비스 큐 스케줄링(Service Queue Scheduling) 320

QoS 설정하기 321
설정 과정 321
CLI에서 설정하기 322
클래스 맵(Class map) 설정 322
정책 맵(Policy map) 설정 323
서비스 정책(Service policy) 설정 324
서비스 큐 스케줄링(Service Queue Scheduling) 설정 325
대역폭 제한 설정 326
설정 정보 보기 327

제1장
PIOLINK Application Switch-K 소개

이 장에서는 PAS-K에서 제공하는 주요한 기능들과 특징에 대해 소개합니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- 제품 개요

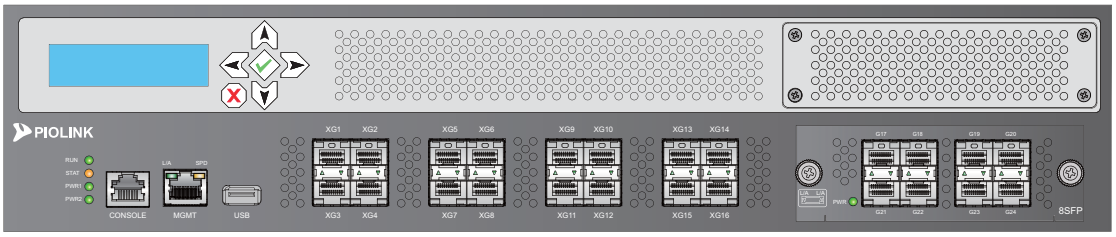
제품 개요

소개

파이오링크 PAS-K1500/2400/2800/4200/4400은 서비스 포트 번호나 패킷의 컨텐트와 같은 4계층 이상의 패킷 정보를 분석하여 인터넷 비즈니스 애플리케이션을 위한 네트워크 트래픽 솔루션과 지능적인 다계층 (Layer4~7) 트래픽 관리 서비스를 제공하는 AP-ADC(Advanced Platform-Application Delivery Controller)입니다.

PAS-K의 트래픽 솔루션과 트래픽 관리 서비스는 기존 네트워크가 해결해야 할 서비스의 품질 문제와 성능 문제 그리고 보안 문제를 효과적으로 개선시켜 줍니다.

PAS-K 모델에 따라 제공되는 하드웨어 구성이 다릅니다. 각 모델별 제품 사양 및 하드웨어 구성은 이 설명서와 함께 제공되는 **PAS-K1500/2400/2800/4200/4400/4800 설치 설명서**를 참고하시기 바랍니다. 다음은 PAS-K 모델 중 상위 모델인 PAS-K4200/4400/4800의 앞면입니다.

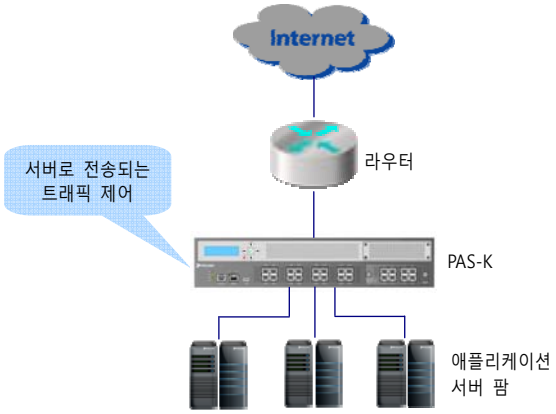


[그림 - PAS-K4200/4400/4800의 앞면]

항목	설 명
10 기가빗 이더넷 Fiber 포트	10Gbps를 지원하는 LC 커넥터 타입의 SFP+ 모듈 슬롯 16개
옵션 모듈 (기가빗 이더넷 Copper 포트, 기가빗 이더넷 Fiber 포트)	10/100/1000BASE-T를 지원하는 RJ-45 커넥터 타입의 이더넷 포트 8개 1000BASE-X를 지원하는 LC 커넥터 타입의 SFP 모듈 슬롯 8개
콘솔 포트	콘솔 터미널 장치를 연결하여 시스템을 관리할 수 있는 RJ-45 커넥터 타입의 포트 1개
관리용 이더넷 포트	시스템 관리에 사용되는 RJ-45 커넥터 타입의 이더넷 포트 1개
시스템 상태 LED	시스템의 동작 상태와 하드웨어 오류, 전원 공급 상태 등을 표시해주는 LED
USB 포트	이미지 부팅, PLOS 업데이트, 설정/로그 백업을 할 수 있는 USB 포트 1개
LCD 패널과 컨트롤 버튼	다음 항목들을 조회 및 설정하는 LCD 패널과 버튼 - 호스트 이름 - CPU와 Memory 사용률 정보 및 Failover 상태 정보 **참고:** 제품에 전원이 들어오면 호스트 이름이 LCD 화면의 상단에 출력되며, 호스트 이름 하단에 CPU/Memory 사용률 정보와 Failover 상태 정보가 5초 간격으로 화면에 출력됩니다. Failover 상태 정보는 Failover 기능이 설정된 상태에서만 화면에 출력됩니다. - 관리용 이더넷 포트의 IP 주소, 서브넷 마스크, 기본 게이트웨이 - 시스템 리부팅

참고: USB 포트를 사용한 이미지 부팅, PLOS 업데이트, 설정/로그 백업 기능은 추후 버전의 PLOS에서 지원될 예정입니다.

PAS-K는 아래 구성도에서와 같이 애플리케이션 서버의 앞 단에 위치하여 클라이언트로부터 전송되는 트래픽을 정책에 맞게 서버로 분배하거나 불필요한 트래픽을 차단시켜줍니다.



[그림 - PAS-K의 일반적인 구성도]

PAS-K는 지능적인 스위칭 기술을 이용하여 웹 사이트, 서버 팜, 캐시 클러스터, 방화벽 시스템 등의 가용성을 높여주며, 기존의 서비스에 영향을 주지 않고 손쉽게 자원을 확장할 수 있게 해줍니다.

주요 기능

PAS-K에서 제공하는 주요 기능은 다음과 같습니다.

L7 부하 분산 서비스 : 서버/캐시 서버 부하 분산

PAS-K는 자신을 통해 전송되는 인터넷 트래픽을 IP 패킷 데이터의 영역까지 검사하여 트래픽을 가장 적절한 서버나 애플리케이션 자원으로 보내고, 서비스를 제공하지 않을 트래픽은 차단시켜줍니다. 이와 같은 PAS-K의 트래픽 관리 서비스는 데이터 센터의 자원을 최적화시킴으로 비용을 절감시키며 동시에 자원의 성능까지 향상시킵니다. 그리고 기업의 고객과 파트너, 직원에게 보다 더 높은 품질의 온라인 서비스를 제공할 수 있게 해줍니다.

L4 부하 분산 서비스 : VPN/방화벽 부하 분산, 서버/캐시 서버 부하 분산, 게이트웨이 부하 분산

네트워크 상에서 다수의 서버가 동일한 애플리케이션을 운용할 때 이들의 앞 단에서 트래픽이 각 서버로 골고루 분배되도록 세션의 흐름을 제어하기 때문에 각 서버 또는 애플리케이션의 성능, 접속, 복원력을 극대화시킵니다. TCP/UDP 포트 정보를 이용하여 트래픽을 분류하고 해당 트래픽을 처리할 수 있는 서버 및 애플리케이션으로 보내거나 차단시킬 수 있으므로, 트래픽 종류에 따라 차별화된 서비스가 가능하며 특정한 애플리케이션 서비스를 위한 서버 팜 구축이 쉬워지고 불필요한 종류의 애플리케이션의 전송 차단이 가능합니다.

고 가용성(High Availability) & 장애 감시(Health Check)

Active-standby failover 기능과 장애 감시 기능을 통해 PAS-K와 연동된 서버, 애플리케이션, 컨텐트 가용성을 계속 모니터링하여 정상 작동 중인 서버들에만 새로운 세션을 연결(정상 상태가 아닌 서버들은 가용성이 확보될 때 다시 연결을 시도)함으로써 무중단, 무장애 서비스를 실현할 수 있도록 지원합니다. 또한 서버/장비의 앞 단에 위치하면서 서비스 중단 없이 이들의 확장이 가능토록 지원합니다.

편리한 관리 환경

PAS-K는 관리를 위해서 명령 기반의 CLI(Command Line Interface)를 제공합니다. PAS-K의 관리 도구는 반드시 로그인을 거친 후에만 사용할 수 있도록 기본적인 보안 장치가 마련되어 있습니다.

주요 특징

PAS-K의 주요한 특징을 정리하면 다음과 같습니다.

다양한 부하 분산 기능 동시 수행

- 다양한 애플리케이션 서버의 부하 분산을 동시에 수행 가능(HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SSL 등)
- 서버 부하 분산과 캐시 서버 부하 분산을 동시에 수행 가능
- 방화벽 부하 분산과 캐시 서버 부하 분산을 동시에 수행 가능
- VPN 부하 분산 시 지점-센터 접속뿐 아니라 센터-지점 접속도 허용

연결 유지 (Persistence) 기능

PAS-K의 부하 분산 서비스는 출발지 IP 주소, SSL ID, Cookie, HTTP 헤더 등을 기반으로 특정 클라이언트가 요청하는 모든 연결을 항상 동일한 실제 서버를 통해 이루어질 수 있게 해주는 지속 연결 기능(persistence 혹은 sticky connection)을 제공합니다.

- 서버 부하 분산의 연결 유지
  같은 클라이언트로부터 오는 연결 요청을 동일한 서버로 연결합니다.
- 방화벽 부하 분산의 연결 유지
  동일한 세션에 속하는 패킷들이 모두 동일한 방화벽을 통해 전송되고, 방화벽 부하 분산이 적용된 외부 PAS-K와 내부 PAS-K에서 송수신되는 패킷의 경로를 기억하여 경로를 지속적으로 유지합니다.
- VPN 부하 분산의 연결 유지
  지사 네트워크를 하나의 VPN 클라이언트 군으로 등록하여 보안 채널의 지속성을 유지시켜줍니다.

네트워크 변경 없이 설치

자체 개발한 브리징 기술을 이용하여 VPN, 방화벽과 같은 복잡한 네트워크도 하나의 서브넷으로 구성 가능합니다.

전원 이중화 지원

PAS-K에 공급되는 전원을 이중으로 구성하여 안전한 전원을 공급할 수 있도록 전원 이중화 기능을 기본으로 제공합니다. 또한, PAS-K2400/2800/4200/4400/4800의 전원 공급기는 Hot Swap 기능을 지원합니다. 하나의 전원 공급기에 장애가 발생한 경우에는 전원을 켠 상태에서 다른 전원 공급기로 교체할 수 있습니다.

제2장
사용하기 전에

이 장에서는 CLI를 사용하여 PAS-K에 접속하는 방법과 기본적인 CLI 사용 방법에 대해 소개합니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- 유지 보수 라이센스 등록
- CLI 사용

유지 보수 라이센스 등록

PAS-K를 사용하기 위해서는 먼저 PAS-K에 유지 보수 라이센스를 등록해야 합니다. 제품 구입 후 당사의 파트너 포탈 홈페이지(http://partner.piolink.com)에서 제품을 등록하시면 해당 제품의 유지 보수 라이센스를 발급 받을 수 있습니다.

이 절에서는 PAS-K를 사용하기 위해 필요한 유지 보수 라이센스를 발급 받는 방법과 CLI 명령을 사용하여 PAS-K에 유지 보수 라이센스를 등록하는 방법에 대해 설명합니다.

주의: 유지 보수 라이센스를 등록하지 않으면 CLI를 사용하여 PAS-K를 설정할 수 있는 <Configuration 모드>로 이동할 수 없습니다. 제품 설치 후 다음 설명을 참고하여 라이센스 발급과 등록 과정을 반드시 수행하도록 합니다.

참고: 유지 보수 라이센스 발급과 관련된 상세한 정보는 제품의 구입처나 당사 기술지원센터(TAC: 1544-9890)로 문의하시기 바랍니다.

유지 보수 라이센스 발급

PAS-K의 유지 보수 라이센스를 발급받는 방법은 다음과 같습니다.

1. 인터넷 익스플로러나 파이어폭스와 같은 웹 브라우저를 실행합니다. 그리고, 웹 브라우저의 주소 입력란에 'http://partner.piolink.com'을 입력한 후 [**Enter**] 키를 누르거나 [**이동**] 버튼을 클릭합니다.

2. 다음과 같은 화면이 나타나면 ID와 PASSWORD를 입력하고 [**LOGIN**] 버튼을 클릭합니다.

참고: ID가 없는 경우 [**회원가입**] 버튼을 클릭하여 회원 가입 신청을 합니다. 가입 신청 후 관리자 승인이 이루어져야 로그인을 할 수 있습니다.

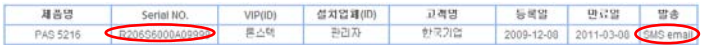
3. 화면 좌측에 있는 **제품등록** 메뉴를 클릭합니다.

4. 제품 라이센스 발급 화면에서 다음 설명을 참고하여 각 항목을 작성한 후 [**라이센스 발급**] 버튼을 클릭합니다.

항 목	설 명
제품설치 대수	등록할 제품의 수를 드롭다운 목록에서 선택합니다. 1 ~ 5대까지 선택이 가능하며, 선택한 제품 수만큼 **제품정보** 부분이 추가됩니다.
제품정보	[**시리얼 검색**] 버튼을 클릭하면 다음과 같은 팝업 창이 나타납니다. 제품 박스 및 뒷면에 붙어있는 시리얼 번호의 뒷자리 5자리를 입력하고 [**검색**] 버튼을 클릭합니다. 
설치업체 정보	제품 설치 담당자의 정보를 입력합니다. 입력한 휴대폰 번호와 이메일 주소로 라이센스 키를 전송하므로 정확한 정보를 입력해야 합니다.
고객 정보	제품을 구입한 고객의 정보를 입력합니다.

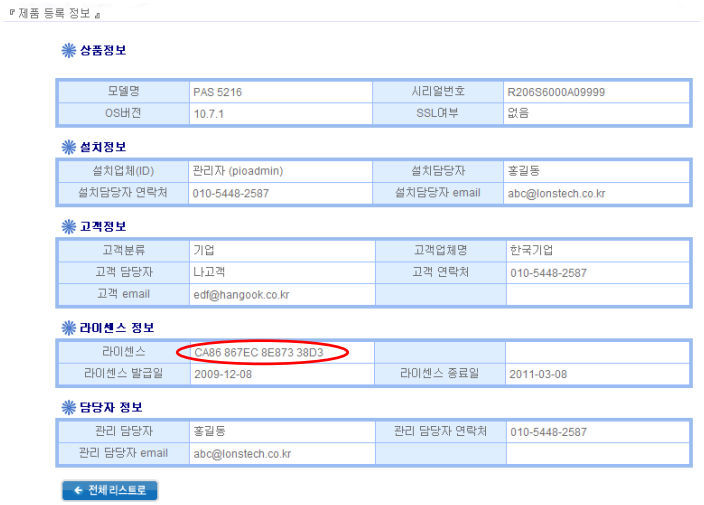
5. 화면 좌측에 있는 **등록완료 리스트** 메뉴를 클릭합니다.

6. 제품 등록 리스트 화면에서 시리얼 번호를 클릭합니다.



참고: SMS email을 클릭하면 제품 등록 시 입력한 휴대폰 번호와 이메일 주소로 라이센스 키가 발송됩니다.

7. **제품 등록 정보** 화면에서 라이센스 키를 확인합니다.


제품 등록 정보

상품정보

모델명	PAS 5216	시리얼번호	R206S6000A09999
OS버전	10.7.1	SSL여부	없음

설치정보

설치업체(ID)	관리자 (pioadmin)	설치담당자	홍길동
설치담당자 연락처	010-5448-2587	설치담당자 email	abc@lonstech.co.kr

고객정보

고객분류	기업	고객업체명	한국기업
고객 담당자	나고객	고객 연락처	010-5448-2587
고객 email	edf@hangook.co.kr		

라이센스 정보

라이센스	CA86 867EC 8E873 38D3		
라이센스 발급일	2009-12-08	라이센스 종료일	2011-03-08

담당자 정보

관리 담당자	홍길동	관리 담당자 연락처	010-5448-2587
관리 담당자 email	abc@lonstech.co.kr		

전체리스트로

CLI에서 설정하기

유지 보수 라이센스를 발급받은 다음에는, PAS-K에 라이센스를 등록해야 합니다. 이 절에서는 CLI 명령을 사용하여 PAS-K에 유지 보수 라이센스를 등록하는 방법에 대해 설명합니다.

유지 보수 라이센스 등록하기

PAS-K를 처음 설치할 때, 유지 보수 라이센스가 등록되어 있지 않은 상태에서 **configure** 명령을 사용하면, 다음과 같은 에러 메시지가 출력되며 <Configuration 모드>로 이동할 수 없습니다.

```
switch# configure
 ======================================================
      Error occurred
 ======================================================
Warranty-license does not exist. Please check again.
 ======================================================
switch#
```

따라서, 장비 설정을 위해 <Configuration 모드>로 이동하려면, PAS-K의 유지 보수 라이센스를 등록해야 합니다. 유지 보수 라이센스를 등록하려면, <Privileged 모드>에서 다음 명령을 사용합니다.

명 령	설 명
warranty-license <*LICENSE*>	발급받은 PAS-K 유지 보수 라이센스를 등록합니다. • <*LICENSE*> 영문자 대문자와 숫자로 이루어진 XXXX-XXXXX-XXXXX-XXXX 형식(4-5-5-4자)의 시리얼 번호를 대쉬(-)를 제외하고 입력

참고: PAS-K는 등록한 유지 보수 라이센스의 유효 기간이 만료되기 한달 전부터 사용자가 <Configuration 모드>로 이동 시, 다음과 같이 라이센스 만료일을 알려주는 메시지를 출력합니다.

```
switch# configure
warranty-license will expire 2012.06.30.
```

그리고, PAS-K 운용 중에 유지 보수 라이센스의 유효 기간이 만료되면, <Configuration 모드>로 이동 시, 다음과 같은 메시지를 출력하여 라이센스 유효 기간이 만료되었음을 알려줍니다.

```
switch# configure
Warranty-license has expired.(date 2012.5.31)
```

참고: 유지 보수 라이센스의 유효 기간이 만료되면, <Configuration 모드>로 이동하여 PAS-K를 설정할 수는 있지만, PLOS를 업데이트할 경우, 다음과 같은 메시지가 출력되며 업데이트를 진행할 수 없습니다.

```
Warranty-license has expired.(date 2012.05.31)
```

참고: PAS-K는 하루에 한 번 새벽 00시 01분에 라이센스의 만료일을 확인하고, 라이센스 만료일에 대한 로그 메시지를 사용자에게 전달합니다. 따라서, 사용자는 장비에 접속하지 않아도 만료일이 어느 정도 남아 있는지, 또는 라이센스가 언제 만료되었는지에 대한 정보를 확인할 수 있습니다.

라이센스의 만료 기한이 1달 이내인 경우에는 다음과 같이 만료일에 대해 기록한 로그 메시지를 전송합니다.

```
[Nov 20 13:52:04] (user.notice) warrantylicense: Warranty-license will expire 2011/11/30.
```

라이센스의 유효 기간이 이미 만료된 경우에는 다음과 같이 라이센스 만료일을 표시한 로그 메시지를 전송합니다.

```
[Nov 20 13:49:34] (user.notice) warrantylicense: Warranty-license has expired.(date 2011/10/31)
```

CLI 사용

이 절에서는 PAS-K의 전원을 켜고 부팅한 후 CLI로 접속하는 방법과 기본적인 CLI 사용 방법에 대해 설명합니다.

CLI 접속

PIOLINK Application Switch-K 부팅하기

사용자가 PAS-K에 전원을 켰을 때, 부팅 과정은 다음 순으로 진행되며, 마지막에 로그인 프롬프트가 나타납니다.

- 소프트웨어 버전 확인
- 하드웨어 초기화 자체 전원 테스트
- PAS-K 로그인 프롬프트

다음은 PAS-K1500/2400/2800/4200/4400/4800의 전원을 켰을 때, 나타나는 메시지입니다.

```
BOOT-K2-V1.0.3 (32bit,SP,BE,MIPS)
Build Date: 2011. 12. 05. (? 20:18:03 KST )
Copyright (C) 2000-2011 PIOLINK, Inc.
S/N  : R211K20000A0315      MAC  : 00-06-C4-80-2-A5

Loading: ........ 41943040 bytes read
33853404 bytes

Setting up loopback
localtime link
QC module loading
Starting syslogd
logfiler started.
Starting snmpd
Switch module Init

User defined switch configuration is loaded
Starting switch IMISH
Starting Cron
Starting keepaeud
Starting Health check
Hardware Monitoring
watchdog enable ENABLE
createdb: database creation failed:
createuser: creation of new role failed:
ALTER ROLE
psql:<stdin>:13:
ALTER TABLE
 * Starting NTP server ntpd
   ...done.
 * Starting Tomcat servlet engine tomcat6
   ...done.

switch login:
```

포트 및 LED에 대한 자세한 설명은 이 설명서와 함께 제공되는 설치 설명서를 참고하도록 합니다.

CLI 로그인하기

PAS-K가 부팅되면 콘솔 창에 다음과 같은 로그인 프롬프트가 표시됩니다. 로그인 프롬프트에 사용자 ID와 패스워드를 입력하면 PAS-K로 로그인할 수 있습니다. 최초로 CLI로 로그인하는 경우에는 root 사용자 계정으로 로그인하도록 합니다. root 사용자 계정의 ID는 root이고 패스워드는 admin입니다.

```
login : root
password :
```

root는 관리자 권한을 가지는 사용자로, 장비의 상태를 모니터링할 수 있을 뿐만 아니라 설정을 변경할 수도 있습니다. admin은 매우 흔히 사용되는 패스워드이므로 PAS-K에 로그인한 후에는 보안을 위해 반드시 사용자의 패스워드를 변경하도록 합니다. PAS-K의 사용자 패스워드를 변경하는 방법은 이 설명서의 제4장 시스템 관리와 모니터링에 설명되어 있습니다.

CLI 로그아웃하기

PAS-K의 CLI에서 로그아웃하려면, 모든 명령 모드에서 다음 명령을 실행합니다.

명 령	설 명
quit	CLI 에서 로그아웃합니다.

기본적인 CLI 사용 방법

CLI는 PAS-K를 설정하거나, 모니터링하고, 유지하는데 사용하는 기본 사용자 인터페이스입니다. 사용자는 콘솔 포트나 터미널 또는 다른 원격 접속 툴을 이용하여 PAS-K에 접속할 수 있으며, 접속한 후에는 CLI를 이용하여 PAS-K를 직접 관리하거나 다양한 설정을 할 수 있습니다.

명령이나 키워드 출력

시스템 프롬프트에서 "**?**" 를 입력하면 해당 명령 모드에서 사용 가능한 명령 리스트와 또한 특정 명령과 함께 사용할 수 있는 키워드나 인자 리스트도 확인할 수 있습니다.

다음과 같이 명령 모드에서 명령 이름, 키워드, 인자 등에 대한 명확한 도움을 얻기 위해 "**?**" 를 이용합니다.

```
(config)# ?
```

참고: 명령 모드에서 help 를 입력하면 "?"를 입력한 것과 같이 명령이름, 키워드, 인자 등에 대한 설명을 출력합니다.
(config)# help

다음과 같이 알파벳 문자와 함께 바로 뒤에 "**?**" 를 입력하면 입력한 알파벳 문자로 시작되는 명령 리스트가 나타납니다. 이 때, 문자와 "**?**" 사이에는 빈칸이 없어야 합니다.

```
(config)# s?
```

특정 명령을 입력한 후, 키워드나 인자를 입력하지 않고 "**?**"를 입력하면 특정 명령에서 사용 가능한 키워드나 인자 리스트가 나타납니다. 이 때, 명령 입력 후 반드시 1칸의 공백이 있어야 합니다.

```
(config)# vlan ?
```

사용자는 단축이 가능한 명령이나 키워드에 한해 다른 명령이나 키워드와 구분할 수 있는 최소한의 문자로 단축하여 사용할 수 있습니다. 예를 들면, "**show**" 명령은 "**sh**" 로 단축하여 사용할 수 있으며, 아래와 같이 "**sh**" 를 입력한 후, Tab키를 누릅니다.

```
(config)# sh<TAB>
```

명령 라인 편집

히스토리 버퍼에는 사용자가 최근에 사용한 100개의 명령 라인이 저장되며, 사용자는 이를 이용해 프롬프트에서 사용한 명령을 수정하거나 재사용할 수 있습니다. 아래 표의 키보드 단축키와 사용 설명을 참조하시기 바랍니다.

[표 - 키보드 단축 키]

단축 키	기 능
Ctrl+A	명령문의 맨 앞으로 커서 이동
Ctrl+B, 왼쪽 화살표(←)	한 글자 왼쪽으로 커서 이동
Ctrl+C	진행 중인 명령 작업을 중단하고, 초기 프롬프트 상태로 전환
Ctrl+D	커서 위치에 있는 글자 삭제
Ctrl+E	명령문의 맨 뒤로 커서 이동
Ctrl+F, 오른쪽 화살표(→)	커서 위치를 한 글자 오른쪽으로 이동
Ctrl+K	커서 위치에서 명령문 끝까지 삭제
Ctrl+N, 아래쪽 화살표(↓)	히스토리 버퍼에 저장된 다음 명령 라인으로 이동
Ctrl+P, 위쪽 화살표(↑)	히스토리 버퍼에 저장된 이전 명령 라인으로 이동
Ctrl+U	명령문의 맨 처음부터 커서 위치 바로 앞까지 삭제
Ctrl+W	커서 바로 앞 단어 삭제

명령 모드

PAS-K의 CLI는 Privileged 모드와 Configuration 모드로 구분됩니다. 각각의 모드는 네트워크 모니터링을 위한 명령과 PAS-K의 설정과 유지를 위해 사용할 수 있는 명령을 가집니다. 사용자 레벨에 따라 명령 모드로의 접근이 제한될 수 있으며, 사용자는 해당 모드에서 "?"를 입력하면 사용 가능한 명령 리스트를 확인할 수 있습니다.

사용자가 ID와 패스워드를 입력하여 CLI로 로그인 하면, 기본적으로 PAS-K의 Privileged 모드로 접속됩니다. 일반 사용자(user)의 경우 장비의 설정을 변경할 수 없으며 모니터링만 가능합니다. 관리자(super user) 권한의 사용자일 경우, Configuration 모드로 접속하여 PAS-K가 제공하는 모든 명령을 사용할 수 있습니다. 관리자(super user)는 Configuration 모드에서 PAS-K의 사용 중인 설정을 변경할 수 있으며, 새로운 계정을 만들 수도 있습니다.

다음 표는 주요 명령 모드와 접속 방법, 해당 명령 모드 프롬프트와 각각의 명령 모드에서 빠져 나가는 법을 설명합니다.

[표 - 주요 명령 모드]

명령 모드	접속 방법	프롬프트	나가기
Privileged	일반 사용자(user) 또는 관리자(super user) 접속	#	exit나 quit 명령
Configuration	관리자(super user) 접속	(config)#	exit나 quit 명령

제3장
기본 네트워크 설정

이 장에서는 PAS-K의 기본적인 구성 작업에 대해 알아봅니다. PAS-K는 출하될 때 이미 기본적인 구성이 되어 있는 상태이기 때문에 이 장에서 설명하는 구성 작업을 하지 않고 제품을 바로 사용할 수 있습니다. 하지만 사용자의 네트워크 환경에 맞게 장비의 설정을 변경해야 하는 경우에는 이 장의 내용을 참고하여 원하는 환경으로 구성하도록 합니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- 포트 설정
- VLAN 설정
- MAC Ageing Time 설정
- IP 주소/라우팅 설정
- Proxy ARP 설정
- ARP Locktime 설정
- 저장 MAC 응답 설정
- 정적(Static) ARP 캐시 설정
- DNS 설정
- 링크 싱크(LinkSync) 설정
- 포트 미러링 설정
- Link Aggregation 설정
- 포트 Failover 설정
- STP/RSTP/PVSTP/MSTP 설정
- NAT64/DNS64 설정
- 네트워크 연결 확인

포트 설정

PAS-K의 포트에 연결되어 있는 상대 장비와 데이터를 정상적으로 송수신하려면 다음과 같은 포트 특성이 바르게 설정되어 있어야 합니다.

- **속도(speed)**
  PAS-K 의 포트에 연결할 케이블의 속도를 설정합니다.

- **전송 모드(duplex mode)**
  데이터 송수신 방식을 설정합니다. 설정 방식에는 무전기와 같이 상대방이 보낸 데이터를 수신중에는 송신을 할 수 없는 반이중 모드(Half duplex mode)와 전화와 같이 양쪽에서 동시에 데이터를 전송해도 통신을 할 수 있는 전이중 모드(Full duplex mode)가 있습니다.

- **MDI/MDI-X**
  MDI(Medium Dependent Interface)와 MDIX(Medium Dependent Interface with Crossover)는 이더넷 포트에 대한 커넥터의 유형입니다. 커넥터 유형이 상대 포트와 동일하게 설정(MDI-MDI, MDIX-MDIX)되어 있으면 교차 케이블을, 서로 다르게 설정되어 있는 경우(MDI-MDIX, MDIX-MDI)에는 직렬 케이블을 사용해야 합니다.

- **흐름 제어(flow control)**
  흐름 제어는 두 장비 간에 패킷을 송수신할 때 각 장비의 포트 수신 한도를 넘는 패킷을 수신하여 패킷 분실이 일어나지 않도록 수신할 패킷의 흐름을 조절하는 기능입니다. PAS-K 는 수신 한도를 넘는 포트에게 패킷을 보내는 장비에게 조절 패킷(pause packet)을 전송하여, 송신측과 수신측의 포트간의 처리 속도차로 발생할 수 있는 패킷 손실(packet loss)를 피합니다.

- **포트의 동작 상태**
  PAS-K 의 각 이더넷 포트의 활성화 여부를 설정합니다. 활성화 상태로 설정한 포트는 동작하게 되고 비활성화 상태로 설정한 포트는 동작하지 않습니다.

- **Flood rate**
  Flood rate 는 다량의 Broadcast 패킷, Multicast 패킷, DLF(Destination Lookup Fail) 패킷이 네트워크 상에 전송되어 네트워크 속도가 느려지거나 다운되는 현상을 방지하는 기능입니다. Flood rate 기능을 설정하면 PAS-K 는 사용자가 설정한 임계값을 넘는 Broadcast 패킷, Multicast 패킷, DLF 패킷을 폐기하여 네트워크의 가용성을 유지합니다.

기본적으로 PAS-K의 모든 포트는 다음과 같이 설정되어 있습니다.

[표 - 포트의 기본 설정]

항 목	기본 설정
속도	Copper 포트: Auto negotiation이 활성화되어 있는 상태로 상대 포트의 속도를 인식하여 자동으로 설정 기가빗 이더넷 Fiber 포트: 1000 (Mbps) 10 기가빗 이더넷 Fiber 포트: 10000 (Mbps)
전송 모드	자동 모드. 자동 모드로 설정된 포트는 상대 포트의 전송 모드를 인식하여, 두 포트의 전송 모드를 동일하게 설정합니다.
MDI/MDI-X	자동 모드(Auto-MDIX mode). 자동 모드로 설정된 포트는 연결된 케이블의 유형을 자동으로 감지하므로 직렬 케이블나 교차 케이블을 모두 사용할 수 있습니다.
Auto negotiation	Copper 포트: 활성화 상태 Fiber 포트: 비활성화 상태
흐름 제어	비활성화 상태
동작 상태	활성화 상태

만약 PAS-K의 포트와 연결된 상대 장비의 포트가 자동 모드를 지원하지 않는 경우에는 이 절에서 설명하는 방법을 통해 포트의 속도와 전송 모드, MDI/MDI-X를 사용자가 수동으로 설정해주어야 정상적으로 통신할 수 있습니다.

CLI에서 설정하기

다음은 CLI 명령을 사용하여 포트를 설정하는 방법입니다.

포트 속도와 전송 모드 설정

포트의 속도는 <Configuration 모드>에서 다음 명령을 사용하여 설정합니다.

명 령	설 명
port <*NAME*> **speed** {**10** | **100** | **1000** | **10000**}	포트의 속도를 설정합니다. • <*NAME*> 두 개 이상의 포트를 지정하는 경우에는 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용 • **10** 10 Mbps • **100** 100 Mbps • **1000** 1000 Mbps • **10000** 10000 Mbps

참고: 포트 종류에 따라 설정할 수 있는 속도와 기본값은 다음과 같습니다.
기가빗 이더넷 Copper 포트: 10, 100, 1000 (기본값: 상대 포트의 속도에 따라 자동으로 설정)
기가빗 이더넷 Fiber 포트: 100, 1000 (기본값: 1000)
10 기가빗 이더넷 Fiber 포트: 100, 1000, 10000 (기본값: 10000)

포트의 전송 모드는 <Configuration 모드>에서 다음 명령을 사용하여 설정합니다.

명 령	설 명
port <*NAME*> **duplex** {**half** | **full**}	포트의 전송 모드를 설정합니다. • **half** 반이중 방식 (기본값) • **full** 전이중 방식

참고: 포트의 전송 모드는 기가빗 이더넷 Copper 포트에만 설정할 수 있습니다.

MDI/MDI-X 설정

포트의 MDI/MDI-X는 <Configuration 모드>에서 다음 명령을 사용하여 설정합니다.

명 령	설 명
port <*NAME*> **mdi-mdix** {**mdi** | **mdix** | **auto**}	포트의 MDI/MDI-X 를 설정합니다. • **mdi** MDI • **mdix** MDI-X • **auto** 상대 포트에 따라 자동으로 설정 (기본값)

참고: 상대 포트가 동일하게 설정되어 있는 경우(MDI-MDI, MDIX-MDIX)에는 교차 케이블을, 서로 다르게 설정되어 있는 경우(MDI-MDIX, MDIX-MDI)에는 직렬 케이블을 사용하도록 합니다. 'auto'로 설정한 경우에는 두 케이블 중 아무거나 사용할 수 있습니다.

참고: MDI/MDIX 설정은 옵션 모듈의 기가빗 이더넷 Copper 포트에만 설정할 수 있습니다.

Auto negotiation 설정

Auto negotiation 기능이 설정된 포트는 상대 포트의 속도를 인식하여, 두 포트가 최적의 공유 속도를 이용할 수 있도록 자동으로 속도를 설정합니다. Auto negotiation 기능은 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
port *<NAME>* **auto-nego** {**enable** | **disable**}	Auto negotiation 기능의 사용 여부를 설정합니다. • **enable** Auto negotiation 기능 활성화 • **disable** Auto negotiation 기능 비활성화 (기본값)

참고: auto-negotiation 기능을 활성화하면 포트 속도(speed)와 전송 모드(duplex)는 설정할 수 없습니다.

흐름 제어(flow control) 설정

포트의 흐름 제어는 <Configuration 모드>에서 다음 명령을 사용하여 설정합니다.

명 령	설 명
port *<NAME>* **flow-ctrl** {**on** | **off**}	포트의 흐름 제어 기능의 사용 여부를 설정합니다. • **on** 흐름제어 기능 활성화 • **off** 흐름제어 기능 비활성화 (기본값)

Flood rate 설정

Flood rate는 <Configuration 모드>에서 다음 명령을 사용하여 설정합니다.

명 령	설 명
port *<NAME>* **flood-rate** {**broadcast** *<BROADCAST>* | **multicast** *<MULTICAST>* | **dlf** *<DLF>*}	Flood rate 기능을 사용하고자 할 경우, 임계값을 설정합니다. • **broadcast** *<BROADCAST>* Broadcast 패킷 임계값. 설정 범위: 0 ~ 1000000 (pps) • **multicast** *<MULTICAST>* Multicast 패킷 임계값. 설정 범위: 0 ~ 1000000 (pps) • **dlf** *<DLF>* DLF 패킷 임계값. 설정 범위: 0 ~ 1000000 (pps)

Description 설정

포트에 대한 설명은 <Configuration 모드>에서 다음 명령을 사용하여 설정합니다.

명 령	설 명
port *<NAME>* **description** *<DESCRIPTION>*	해당 포트에 대한 설명을 입력합니다. • *<DESCRIPTION>* 해당 포트에 대한 부가 설명. 최대 255자의 알파벳 대/소문자, 숫자, 특수 문자로 이루어진 문자열로 지정 가능.

포트의 동작 상태 설정

포트의 동작 상태는 <Configuration 모드>에서 다음 명령을 사용하여 설정합니다.

명 령	설 명
port <*NAME*> **status {enable | disable}**	포트의 동작 상태를 설정합니다. • **enable** 포트 활성화 (기본값) • **disable** 포트 비활성화

주의: 포트를 비 활성화하면 현재 포트를 통해 형성된 모든 연결이 끊어지게 되므로 포트를 비활성화할 때에는 주의가 필요합니다.

포트 정보 출력

상태 정보 출력

PAS-K에 있는 이더넷 포트의 현재 상태를 확인하려면, <Priviliger 모드> 또는 <Configuration 모드>에서 **show port** 명령을 사용합니다. 특정 포트에 대한 설정 정보를 확인하려면, **show port** 명령 뒤에 해당 포트의 이름 (<*NAME*>)을 입력하면 됩니다.

통계 정보 출력

PAS-K에 있는 이더넷 포트의 통계 정보를 확인하려면, <Priviliger 모드> 또는 <Configuration 모드>에서 **show port-statistics** 명령을 사용합니다.

참고: 포트 통계 정보는 누적된 정보가 출력됩니다. 포트 통계 정보를 초기화하려면, <Priviliger 모드> 또는 <Configuration 모드>에서 **no port-statistics** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

VLAN 설정

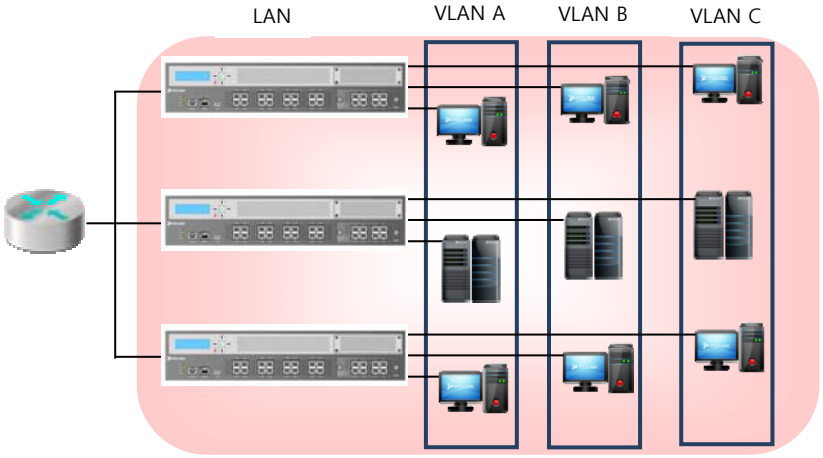
이 절에서는 VLAN(Virtual LAN)의 기본적인 개념과 여러 스위치에서 VLAN을 공유할 수 있는 802.1Q tagged VLAN에 대해 소개하고, CLI에서 VLAN을 설정하는 방법에 대해 설명합니다.

VLAN 개요

VLAN은 호스트들을 물리적인 위치에 관계없이 포트나 MAC 주소, IP 주소 또는 프로토콜 등의 기준으로 분류한 그룹입니다. VLAN은 하나의 브로드캐스트 도메인으로, 물리적인 LAN과 동일한 속성을 가지며, 하나의 LAN을 여러 브로드캐스트 도메인으로 나눌 수 있습니다. 브로드캐스트 도메인이란 같은 네트워크 상에 존재하는 호스트 그룹을 의미합니다.

VLAN에 연결된 모든 노드들은 물리적으로 같은 스위치에 물려있거나 같은 지역에 있을 필요는 없습니다. 같은 VLAN으로 구성된 호스트들은 마치 같은 브리지나 스위치에 연결되어 있는 것처럼 보이지만 실제로는 서로 다른 빌딩에 있는 서로 다른 스위치에 연결되어 있으면서 같은 VLAN으로 구성되는 경우도 있습니다.

아래의 그림은 건물에 위치한 하나의 LAN을 포트별로 나누어 3개의 VLAN으로 구성한 예입니다. 그림에서 스위치의 1번 포트에 연결한 호스트 그룹은 VLAN A, 2번 포트에 연결한 호스트의 그룹은 VLAN B, 3번 포트에 연결한 호스트의 그룹은 VLAN 3으로 구성되어 있습니다.



[그림 - VLAN 구성의 예]

VLAN을 사용하면 브로드캐스트 도메인을 각각의 논리적인 그룹으로 제한하여 전체적인 브로드캐스트 트래픽을 줄이게 되어 가용한 네트워크 대역폭을 증가시킵니다. 뿐만 아니라, VLAN에 속하는 자원(호스트 및 네트워크 장비)들은 물리적으로 같은 장소에 위치할 필요가 없기 때문에 자원의 관리가 용이해집니다.

VLAN ID

PAS-K에는 4096개의 VLAN을 생성할 수 있습니다. PAS-K는 VLAN ID로 0 ~ 4095 사이의 값을 설정할 수 있는데 특정 ID는 이미 시스템에서 사용하는 ID이기 때문에 사용자가 지정할 수 없습니다. 다음 표는 PAS-K에서 사용 가능한 VLAN ID 범위를 설명합니다.

[표 - VLAN 범위]

VLAN ID	설 명
0, 4081 ~ 4095	시스템이 사용하는 ID. 사용자는 이 ID를 사용하여 VLAN를 생성할 수 없습니다.
1	기본 VLAN의 ID. 이 ID를 가진 VLAN은 삭제할 수 없습니다.
2 ~ 4080	일반 VLAN에서 사용 가능한 ID. 사용자는 2~4080 범위의 ID를 가진 VLAN을 생성하거나 수정, 삭제할 수 있습니다.

기본 VLAN (default VLAN)

PAS-K에서는 L2 스위치 기능에 의해 구성 정보가 미 설정 상태여도, 장치 가동 후 곧바로 패킷의 L2 중계를 할 수 있습니다. 모든 포트는 기본 VLAN에 속합니다. 기본 VLAN의 이름은 'default'이고, ID는 '1', 포트는 'untagged port'로 모든 포트를 사용합니다. PAS-K에서 제공하는 VLAN은 중복(overlapped) VLAN이기 때문에 한 포트가 여러 VLAN에 포함될 수 있습니다.

참고: 기본 VLAN에는 라우팅 및 부하 분산 서비스를 적용할 수 없습니다.

IEEE 802.1Q Tagged VLAN

IEEE 802.1Q는 브리지를 통해 전송되는 프레임이 어느 VLAN 그룹인지 식별하기 위해 프레임 헤더에 태그를 사용합니다. 태그는 전송된 프레임이 어떤 VLAN으로부터 전송되었는지를 식별하는데 사용됩니다. 태그는 이더넷 프레임에 삽입되며, 태그된 프레임에는 태그 필드 내에 VLAN ID 식별에 사용되는 12비트(bit)의 VID가 포함됩니다. 태그에 포함된 VID에 따라 PAS-K는 포트 사이에서 프레임을 전송합니다. 같은 VID를 가지는 포트는 서로 통신을 할 수 있습니다.

IEEE 802.1Q tagged VLAN에서 VLAN간의 통신 시 다음과 같은 ingress, Egress 과정을 수행합니다.

Ingress 과정

IEEE 802.1Q 포트는 tagged나 untagged 프레임을 전송할 수 있습니다. Ingress 포트는 수신된 프레임에 태그가 포함되었는지 식별하고, 수신된 프레임을 태그에 포함된 VID에 따라 분류합니다. 포트에 tagged 프레임이 전송된 경우, 태그에 포함된 VID로 어떤 VLAN ID를 식별한 후 tagged 프레임을 egress 포트로 바로 전달합니다. Untagged 프레임이 수신된 경우, 포트는 자신의 PVID를 untagged 프레임에 삽입합니다. PVID는 각각의 물리적인 포트에 할당되는 기본 VID입니다. 이 PVID는 포트에 전송된 untagged 프레임 (VID가 null인 프레임)에 할당됩니다.

Egress 과정

Egress 과정은 외부로 송신하는 프레임을 tagged 프레임으로 송신할지 untagged 프레임으로 송신할 지 여부를 결정합니다. PAS-K와 연결된 네트워크 장비 중에는 tagged 프레임만 수용 가능한 장비 또는 tagged 프레임을 untagged 프레임으로 요청하는 장비도 있을 수 있습니다. 이러한 경우에 VLAN 생성 시 네트워크 장비를 연결할 포트를 네트워크 장비의 요청에 따라 tagged 포트 또는 untagged 포트로 설정 가능(Hybird mode)합니다. Tagged 포트인 경우(Trunk mode) 프레임에 태그를 붙이며, untagged 포트인 경우(Access mode) 프레임에 태그를 붙이지 않습니다.

CLI에서 설정하기

이 절에서는 CLI에서 VLAN을 설정하는 방법에 대해 살펴봅니다.

VLAN 생성 및 포트 추가

VLAN을 생성하고 포트를 VLAN에 추가하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**vlan** *<NAME>* **vid** *<VID>*	VLAN을 생성합니다. • *<NAME>* vlan 이름. 최대 10자의 알파벳, 숫자, '-', '_' 문자로 이루어진 문자열로 지정, 첫 글자는 반드시 알파벳을 사용해야 하며, **eth0**, **inbound**는 지정할 수 없음 • *<VID>* VLAN을 식별할 ID. (설정 범위: 2 ~ 4080)
2	**vlan** *<NAME>* **port** *<NAME>* {**tagged** | **untagged**}	VLAN에 포함시킬 포트를 설정합니다. 포트에 연결된 장비가 IEEE 802.1Q를 지원하는 경우에는 **tagged** 옵션을 추가합니다. • *<NAME>* 포트 이름. 두 개 이상의 포트를 지정하는 경우에는 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용 • **tagged** tagged 옵션 활성화. • **untagged** untagged 옵션 활성화.

참고: VLAN에 추가한 포트를 삭제하려면 <Configuration 모드>에서 **no vlan** *<NAME>* **port** *<NAME>* 명령을 사용합니다.

참고: PAS-K에 정의되어 있는 특정 VLAN을 삭제하려면, <Configuration 모드>에서 **no vlan** *<NAME>* 명령을 사용합니다.

VLAN 설정 정보 보기

VLAN의 설정 정보를 확인하려면, <Priviliger 모드> 또는 <Configuration 모드>에서 **show vlan** 명령을 사용합니다. 특정 VLAN에 대한 설정 정보를 확인하려면, **show vlan** 명령 뒤에 해당 VLAN의 이름(*<NAME>*)을 입력하면 됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

참고: Tagged 프레임에 포함되는 태그 필드에는 VLAN의 ID나 패킷의 우선순위를 결정하는 표준인 802.1p 값이 들어갈 수 있습니다. 태그 필드는 목적지가 속한 VLAN에만 프레임을 브로드캐스트할 수 있게 하여 대역폭의 낭비를 줄이고 보안성을 향상시켜 줍니다. 그리고, 스위치 간에 VLAN을 공유할 수 있게 하여 LAN의 범위를 넓힐 수 있습니다.

주의: 802.1Q를 지원하지 않는 장비나 NIC 등과 연결되어 있는 포트는 반드시 untagged 포트로 지정해야 합니다. 802.1Q를 지원하지 않는 장비로 태그 필드가 포함된 프레임을 전송하면 프레임을 제대로 인식하지 못하거나 혹은 크기 오류(oversize packet)가 발생한 패킷으로 인식하여 폐기하게 됩니다.

VLAN 멀티캐스트 브리지 설정

IEEE 802.1Q 확장 브리징은 VLAN 간의 멀티캐스팅 프레임 전송을 지원합니다. VLAN 간에 멀티캐스트 브리지를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**multicast-bridge**	<멀티캐스트 브리지 설정 모드>로 들어갑니다.
2	**interface** *<INTERFACE>* (필수 설정)	멀티캐스트 브리지 기능을 적용할 VLAN 인터페이스를 설정합니다. • *<INTERFACE>* 추가할 VLAN 인터페이스 이름. 2개의 VLAN 인터페이스를 동시에 설정하기 위해서는 공백 없이 쉼표(,)로 각 인터페이스를 구분하도록 합니다. **참고**: 멀티캐스트 브리지 기능을 사용하기 위해서는 반드시 2개의 VLAN 인터페이스를 설정해야 합니다.
3	**ip** *<IP>* (필수 설정)	VLAN 멀티캐스트 브리지 인터페이스에 적용할 IP 주소를 설정합니다. • *<IP>* IP 주소 입력. 한 개의 IP 주소만 지정 가능.
4	**status** {**enable** | **disable**}	멀티캐스트 브리지 기능의 사용 여부를 설정합니다. • **enable** 멀티캐스트 브리지 기능 활성화 • **disable** 멀티캐스트 브리지 기능 비활성화 (기본값)
5	**current**	멀티캐스트 브리지 설정 정보를 확인합니다.
6	**apply**	멀티캐스트 브리지 설정을 저장하고 시스템에 적용합니다.

참고: 설정한 인터페이스 및 IP 주소를 삭제하려면 <멀티캐스트 브리지 설정 모드>에서 다음의 명령을 사용합니다.

```
(config-multicast-bridge)# no interface <INTERFACE>
(config-multicast-bridge)# no ip
```

참고: 멀티캐스트 브리지 기능은 하드웨어적인 제약 사항으로 인해 PAS-K4200/4400 모델에서만 지원합니다.

VLAN 멀티캐스트 브리지 설정 정보 보기

멀티캐스트 브리지의 설정 정보와 상태를 확인하려면, <Priviliger 모드> 또는 <Configuration 모드>에서 **show multicast-bridge** 명령을 통해 확인할 수 있습니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

MAC Ageing Time 설정

MAC Ageing Time은 PAS-K가 MAC 주소를 학습하여(learning) MAC 테이블에 저장한 후 삭제하기까지의 시간을 말합니다. Ageing Time이 경과된 MAC 주소는 더 이상 유효한 값이 아니라고 판단되어 MAC 테이블에서 삭제됩니다.

CLI에서 설정하기

MAC Ageing Time 설정

사용자가 Ageing Time을 직접 설정하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
mac ageing-time *<AGEING-TIME>*	MAC 주소의 Ageing Time 을 설정합니다. '0'으로 지정하면 학습한 MAC 주소를 삭제하지 않습니다. • *<AGEING-TIME>* MAC Ageing 시간 설정. 설정 범위: 0 ~ 1,000,000(초), 기본값: 300(초)

참고: 설정한 Ageing Time을 기본값으로 변경하려면, <Configuration 모드>에서 **no mac ageing-time** 명령을 사용합니다.

MAC Ageing Time 설정 정보 보기

MAC 테이블에 저장된 모든 MAC 주소와 Ageing Time 정보를 확인하려면, <Priviliger 모드> 또는 <Configuration 모드>에서 **show mac** 명령을 통해 확인할 수 있습니다. 포트별 MAC 테이블 정보를 확인하려면 **show mac [port** [*<NAME>*]] 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다

IP 주소/라우팅 설정

PAS-K가 다른 네트워크 장비와 통신하기 위해서는 IP 주소 및 라우팅 정보가 필요합니다. IP 주소는 IPv4와 IPv6 두 가지로 나뉘며, PAS-K는 IPv4와 IPv6를 모두 지원합니다. 이 절에서는 다른 네트워크 장비와 통신하기 위해 PAS-K에 설정해야 하는 항목들과 설정하는 방법에 대해 살펴봅니다.

IPv4 주소

IPv4(Internet Protocol version 4)는 32 비트로 이루어진 주소 체계로 3 자리 10 진수가 4 마디(옥텟)로 구성되어 있습니다. 특정 IPv4 주소는 특수한 사용을 위해 예약되어 있으며, 이러한 IPv4 주소는 호스트, 서브넷, 또는 네트워크 주소로 사용할 수 없습니다. 다음 표는 클래스 별로 예약되거나 사용 가능한 IPv4 주소의 범위 리스트를 보여줍니다.

[표 - 예약/사용 가능한 IPv4 주소]

클래스	주 소	상 태
A	0.0.0.0 1.0.0.0 ~ 126.0.0.0 127.0.0.0	예약 사용 가능 예약
B	128.0.0.0 ~ 191.254.0.0 191.255.0.0	사용 가능 예약
C	192.0.0.0 192.0.1.0 ~ 223.255.254 223.255.255.0	예약 사용 가능 예약
D	224.0.0.0 ~ 239.255.255.255	멀티캐스트 그룹 주소
E	240.0.0.0 ~ 255.255.255.254 255.255.255.255	예약 브로드캐스트

IPv6 주소

인터넷을 이용하여 다양한 서비스를 누릴 수 있게 되면서 인터넷 사용자 수는 날로 증가하고, 인터넷 통신에서 필요한 IP 주소가 고갈되는 문제가 대두되고 있습니다. IPv6(Internet Protocol version 6)는 이러한 IP 주소 부족 문제를 해결하고, 좀더 안정적이고 향상된 기능을 제공하기 위해 만들어진 차세대 버전 인터넷 프로토콜입니다.

IPv6는 IP를 사용하여 통신하는 모든 기기에 고유한 IP 주소를 제공하는 것을 목적으로 만들어졌습니다. IPv6는 32 비트로 이루어졌던 기존의 IPv4와는 달리 128비트로 이루어지기 때문에 거의 무한대에 가까운 개수의 IP 주소를 사용할 수 있게 됩니다. 따라서, 사용자 기기나 홈 네트워크, 자동차 등 IP를 사용하여 통신하는 모든 기기에 고유한 IP 주소를 충분하게 제공할 수 있습니다.

모든 기기가 자신의 고유 IP 주소를 가지면, NAT(Network Address Translation)등의 사용이 줄어들기 때문에 네트워크 장비들이 패킷을 주고 받을 때 주소 변환에 따른 부하를 줄일 수 있습니다. 또한, 패킷 헤더가 IPv4보다 단순해졌기 때문에 패킷의 처리 속도가 빨라지고 효율적인 라우팅을 수행할 수 있다는 장점이 있습니다.

그러나, IPv4에서 IPv6로 전환되는 과정에서 IPv4와 IPv6가 혼용되는 사용 환경에 대응하기 위해서는 듀얼 스택(IPv4를 IPv6으로 전환하기 위한 방법으로 IPv4와 IPv6를 모두 지원)이 요구되며, IPv4 망과 IPv6망을 전환을 해주는 기능도 필요합니다.

㈜파이오링크의 PAS-K는 IPv4와 IPv6의 통합 및 공존을 위해 필요한 서비스를 제공하고, 향후 IPv6에 대한 시장의 요구 사항이 증가하고 더 많이 채택됨에 따라 IPv6 표준과 호환되는 IPv6 기능을 지속적으로 개선하고 제공할 것을 계획하고 있습니다.

IPv6 주소는 다음과 같은 세 가지 종류가 있습니다.

[표 – IPv6 주소의 종류]

종류	설 명
유니캐스트 주소	단일 호스트 간의 패킷 전송 • 글로벌 유니캐스트 주소(Global unicast address) : 외부의 IPv6 네트워크와 데이터 통신을 하기 위해 사용 • 링크 로컬 유니캐스트 주소(Local unicast address) : - 링크 로컬 주소(Link-local address): 인접한 두 노드 사이에 정보를 교환하기 위한 목적으로 사용 (링크 로컬 주소로는 fe80::/10부터 febf::/10까지 사용 가능) - 사이트 로컬: 동일한 사이트(로컬 네트워크)에서 통신하기 위한 목적으로 사용 (사이트 로컬 주소로는 fec0::/10에서 feff::/10까지 사용 가능)
애니캐스트 주소	단일 호스트에서 가까이 있는 여러 개의 호스트들로 패킷 전송
멀티캐스트 주소	단일 호스트에서 다중 호스트들로 패킷 전송

참고: 링크 로컬 주소는 주변 라우터 또는 인터페이스와 통신하거나 주소 할당을 하기 위해 최소한으로 필요한 IP 주소로, 인터페이스가 활성화 됨에 따라 자동으로 생성됩니다. 링크 로컬 주소는 추가/수정하거나 삭제할 수 없습니다.

IPv6 주소 표기

128비트의 IPv6 주소는 8개의 16비트 단위의 16진수를 콜론(:)으로 구분한 X:X:X:X:X:X:X:X의 형태로 표기됩니다. 다음은 IPv6 주소를 표기한 예입니다.

2001:0320:0000:010a:3afe:0000:3afe:0001

IPv6 주소는 IPv4 주소보다 길기 때문에 표현하기가 어려운 단점이 있지만, 다음과 같은 방법으로 길이를 간단하게 줄일 수가 있습니다.

(1) 선행하는 0의 생략

각 16비트의 블록 내에서 맨 앞에 표기된 0을 생략할 수 있습니다. 그러나, 최소 1개의 숫자는 남겨두어야 합니다.

(2) 연속된 0의 생략

연속된 0을 생략할 수 있습니다. 단, 연속된 0을 생략하는 것은 하나의 주소에서 1회만 가능 합니다.

다음은 IPv6 주소를 생략하여 표기하는 경우의 예입니다.

2001:**0**DB8:**0000**:**0000**:**000**8:0800:200C:417A
→ 선행하는 0의 생략
2001:**DB8:0:0:8:**800:200C:417A
→ 연속된 0의 생략
2001:DB8::8:800:200C:417A

[표 – IPv6 주소의 압축된 표시]

IPv6 주소 종류	압축하기 전 표시	압축한 후 표시
유니캐스트 주소	2001:0:0:0:0DB8:800:200C:417A	2001::0DB8:800:200C:417A
멀티캐스트 주소	FF01:0:0:0:0:0:0:101	FF01::101
루프백 주소	0:0:0:0:0:0:0:1	::1
불특정 주소	0:0:0:0:0:0:0:0	::

IPv6 Prefix 표기

IPv6-Prefix는 주소에서 연속으로 놓인 비트 값을 나타내며 Prefix 길이는 10진수 값으로서 주소에서 Prefix를 포함하는 상위의 연속된 비트의 길이를 나타냅니다. IPv6의 Prefix는 IPv4의 클래스 도메인 간 라우팅(CIDR) 표기와 같은 방법으로 **IPv6-Prefix/Prefix-길이**의 형태로 표기됩니다. 예를 들어, 2001:0DB8:8086:6502::/32는 주소의 처음 32비트인 2001:0DB8 부분이 네트워크 Prefix라는 것을 의미합니다.

라우팅 정보를 설정할 경우에 IPv4에서는 넷 마스크 비트 수를 통해 IP 대역을 할당하였지만, IPv6에서는 넷 마스크 비트 수 대신 Prefix를 사용하여 IP 대역을 할당합니다.

IPv6 라우팅 설정

라우팅 정보를 입력할 경우에도 IP 주소를 설정할 때와 마찬가지로 IP 주소를 간단하게 줄여서 표시할 수 있습니다.

다음은 IPv6 주소 2001:0DB8:0000:0000:0008:0800:200C:417A를 예로 들어, 기본 게이트웨이와 특정 게이트웨이, 그리고 고정 경로를 설정한 경우입니다.

기본 게이트웨이 설정:

```
route6 default-gateway 2001:DB8::8:800:200C:417A
```

-> 선행하는 0과 연속된 0을 생략

고정 경로 설정(특정 게이트웨이):

```
route6 network 2001:DB8::/32 gateway 3ffe:DB8::8:800:200C:417A
```

-> 선행하는 0과 연속된 0을 생략

고정 경로 설정(특정 인터페이스):

```
route6 network 2001:DB8::/32 interface vlan1
```

-> 선행하는 0과 연속된 0을 생략

참고: IPv6 Prefix에 대한 자세한 내용은 RFC 2373을 참조하시기 바랍니다.

라우팅 설정

PAS-K의 기본적인 네트워크 통신을 위해 다음과 같은 기본 게이트웨이를 설정하고, 특정 네트워크로의 라우팅 경로를 지정해야하는 경우, 해당 네트워크로의 게이트웨이 또는 인터페이스를 지정하여 고정 경로를 설정합니다. 또한, 링크 로드 분산을 목적으로하는 ECMP(Equal-Cost Multipath Protocol)를 지원하여 다중 경로로 패킷을 라우팅할 수 있는 기능을 지원합니다.

- **기본 게이트웨이**
  기본 게이트웨이란 동일 네트워크에 존재하지 않는 네트워크 장비에 액세스할 때 통로 역할을 하는 장비를 말합니다. PAS-K 가 라우팅 테이블에 존재하지 않는 네트워크 대역으로 프레임을 전송하기 위해서는 기본 게이트웨이를 설정해야 합니다.
- **고정 경로**
  고정 경로는 사용자가 정의하는 경로로 출발지와 목적지 사이에서 패킷을 이동하는데 경유하는 특정(지정한) 경로입니다. 고정 경로는 PAS-K 를 특정 목적지 호스트 또는 네트워크를 위한 경로로 설정할 때 필요합니다. 고정 경로는 목적지 IP 주소 및 네트워크 주소, 서브넷 마스크, 게이트웨이 IP 주소, 인터페이스로 구성됩니다.

CLI에서 설정하기

인터페이스의 IP 주소 설정

<Configuration 모드>에서 다음 명령을 실행하여 특정 인터페이스에 IP 주소, 서브넷 마스크, 브로드캐스트 주소를 설정합니다.

명 령	설 명
interface *<NAME>* {**ip** *<ADDRESS>* | **ip6** *<ADDRESS>*} [**broadcast** *<BROADCAST>*]	인터페이스에 IP 주소를 설정합니다. • *<NAME>* IP 주소를 설정할 VLAN 인터페이스의 이름. (mgmt: 관리포트 인터페이스) • **ip** *<ADDRESS>* 설정할 IPv4 주소와 넷 마스크 비트 • **ip6** *<ADDRESS>* 설정할 IPv6 주소와 Prefix • *<BROADCAST>* 브로드캐스트 주소

참고: 각 VLAN 인터페이스는 서로 다른 네트워크 대역의 IP 주소를 사용해야 합니다. IP 주소 설정 시 다른 VLAN 인터페이스와 동일한 네트워크 대역의 IP 주소를 입력하면 에러 메시지가 출력됩니다.

참고: 사용자가 네트워크 인터페이스에 IP 주소를 할당할 때, PAS-K는 자동으로 IP 주소에 대한 ARP를 보냅니다. ARP는 모든 네트워크 노드에 ARP 매핑에 대해 통지합니다.

참고: 지정한 인터페이스의 IP 주소를 삭제하려면, <Configuration 모드>에서 다음 명령을 사용합니다.

```
(config)# no interface <NAME> {ip <ADDRESS> | ip6 <ADDRESS>} [broadcast <BROADCAST>]
```

참고: 관리 포트 인터페이스(mgmt)에는 기본적으로 192.168.100.1/24 IPv4 주소가 설정되어 있습니다.

인터페이스의 MTU 설정

<Configuration 모드>에서 다음 명령을 실행하여 특정 인터페이스의 MTU 값을 설정합니다.

명 령	설 명
interface *<NAME>* **mtu** *<MTU>*	인터페이스의 MTU 를 설정합니다. • *<MTU>* 인터페이스의 MTU 값 (설정 범위: 68 ~ 1500, 기본값: 1500)

참고: 지정한 인터페이스의 MTU를 기본값으로 변경하려면, <Configuration 모드>에서 **no interface** *<NAME>* **mtu** 명령을 실행합니다.

인터페이스 활성화/비활성화

VLAN을 정의하면, 해당 VLAN 인터페이스의 상태는 기본적으로 활성화 상태가 됩니다. 인터페이스 상태가 비활성화되면 해당 인터페이스를 통해 통신이 이루어지지 않습니다. 시스템에 기본으로 정의되어 있는 관리 포트 인터페이스(mgmt)의 상태도 활성화하거나 비활성화할 수 있습니다.

<Configuration 모드>에서 다음 명령을 실행하여 인터페이스의 활성화 여부를 설정합니다.

명 령	설 명
interface *<NAME>* **status** {**up** | **down**}	인터페이스의 상태를 설정합니다. • **up** 인터페이스 활성화 (기본값) • **down** 인터페이스 비활성화

기본 게이트웨이 추가

기본 게이트웨이를 추가하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
route default-gateway *<GATEWAY>*	IPv4 기본 게이트웨이를 추가합니다. • *<GATEWAY>* 기본 게이트웨이 IPv4 주소. **참고:** PAS-K는 ECMP 기능을 지원하기 위해 최대 16개의 기본 게이트웨이를 설정할 수 있습니다. 여러 개의 기본 게이트웨이를 추가하려면 공백 없이 쉼표(,)로 각 IP 주소를 구분하도록 합니다.
route6 default-gateway *<GATEWAY>*	IPv6 기본 게이트웨이를 추가합니다. • *<GATEWAY>* 기본 게이트웨이 IPv6 주소.

주의: 기본 게이트웨이의 IP 주소는 반드시 PAS-K에 등록된 VLAN 인터페이스의 IP 주소 중 하나와 동일한 네트워크 대역에 존재해야 합니다.

참고: IP 라우팅 테이블에서 기본 게이트웨이를 삭제하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no {route | route6} default-gateway <GATEWAY>
```

고정 경로 추가

고정 경로를 설정하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
route network *<DEST>* {**gateway** *<GATEWAY>* | **interface** *<INTERFACE>*}	IPv4 고정 경로를 설정합니다. • *<DEST>* 추가할 고정 경로의 목적지 IPv4 주소 • *<GATEWAY>* 목적지에 도달하기 위해 경유할 게이트웨이 주소 • *<INTERFACE>* 목적지에 도달하기 위해 경유할 VLAN 인터페이스 이름 **참고:** PAS-K는 ECMP 기능을 지원하기 위해 하나의 목적지에 대해 최대 16개의 고정 경로를 설정할 수 있습니다. 여러 개의 고정 경로를 추가하려면 공백 없이 쉼표(,)로 각 IP 주소 또는 인터페이스 이름을 구분하도록 합니다.
route6 network *<DEST>* {**gateway** *<GATEWAY>* | **interface** *<INTERFACE>*}	IPv6 고정 경로를 설정합니다. • *<DEST>* 추가할 고정 경로의 목적지 IPv6 주소 • *<GATEWAY>* 목적지에 도달하기 위해 경유할 게이트웨이 주소 • *<INTERFACE>* 목적지에 도달하기 위해 경유할 VLAN 인터페이스 이름

주의: 고정 경로를 추가하려면, 추가하려는 고정 경로와 같은 네트워크 대역의 IP 주소가 PAS-K의 VLAN 인터페이스에 설정되어 있어야 합니다. 그렇지 않으면 고정 경로를 추가할 수 없습니다.

참고: IP 라우팅 테이블에서 고정 경로를 삭제하려면, <Configuration 모드>에서 다음 명령을 사용합니다.

```
(config)# no route network <DEST> gateway <GATEWAY>
(config)# no route network <DEST> interface <INTERFACE>
(config)# no route6 network <DEST>
```

참고: ECMP 기능은 IPv4 환경에서만 동작합니다.

IPv6 Neighbor 설정

IPv6 환경에서는 NDP(Neighbor Discovery Protocol)를 사용하여 얻은 이웃 노드들의 정보(IPv6 주소와 MAC 주소)는 자동적으로 neighbor 테이블에 등록되지만, 네트워크 관리자가 수동으로 등록할 수도 있습니다. 수동으로 neighbor 정보(IPv6 주소와 MAC 주소)를 등록하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
neighbor *<IP> <MAC>*	수동으로 neighbor 정보(IPv6 주소와 MAC 주소)를 등록합니다. • *<IP>* Neighbor의 IPv6 주소 입력 • *<MAC>* Neighbor의 MAC 주소 입력

참고: 등록한 neighbor 정보를 삭제하려면, <Configuration 모드>에서 **no neighbor** *<IP>* 명령을 실행합니다.

설정 정보 확인

VLAN 인터페이스의 IP 설정 정보 출력

PAS-K의 각 VLAN 인터페이스의 IP 주소 설정을 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
show interface [*<NAME>*]	인터페이스 및 관리 포트의 정보를 확인합니다. • *<NAME>* 특정 VLAN 인터페이스의 IP 주소를 확인하려면, VLAN 인터페이스의 이름을 입력하고, 관리 포트의 IP 주소를 확인하려면, **mgmt**를 입력합니다.

경로 설정 정보 출력

PAS-K의 경로 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
show route	IPv4 기본 게이트웨이 및 경로 설정 정보 조회
show route default-gateway	IPv4 기본 게이트웨이 설정 정보 조회
show route network [*<DEST>*]	IPv4 경로 설정 정보 조회 특정 목적지에 대한 경로 설정 정보를 조회하려면, 해당 목적지의 IPv4 주소를 입력
show route6	IPv6 기본 게이트웨이 및 경로 설정 정보 조회
show route6 network [*<DEST>*]	IPv6 경로 설정 정보 조회. 특정 목적지에 대한 경로 설정 정보를 조회하려면, 해당 목적지의 IPv6 주소를 입력

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

IPv6 Neighbor 정보 출력

IPv6 Neighbor 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show neighbor** 명령을 사용합니다. 특정 neighbor에 대한 정보를 확인하려면, **show neighbor** 명령 뒤에 해당 IPv6 주소(*<IP>*)를 입력하면 됩니다.

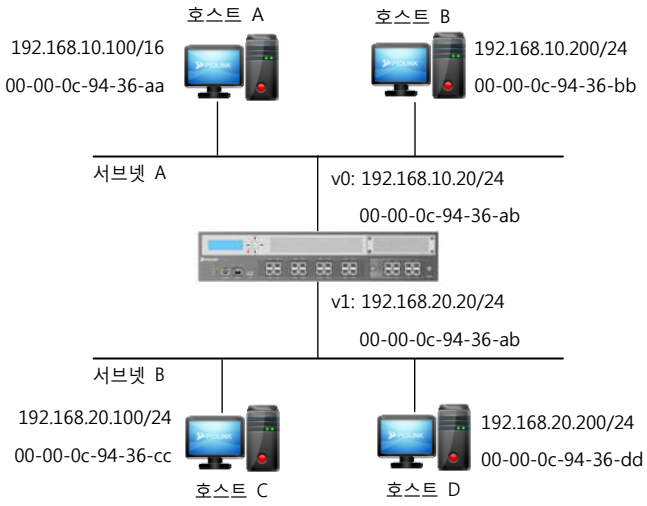
참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

Proxy ARP 설정

Proxy ARP 개요

ARP는 네트워크 상에서 IP 주소와 물리적인 주소(MAC 주소)를 대응시키기 위해 사용되는 프로토콜입니다. Proxy ARP는 라우터의 서로 다른 인터페이스에 연결된 호스트가 같은 네트워크일 때 라우터가 ARP 응답을 대신 해주는 기능입니다. 따라서, ARP를 요청한 호스트는 라우터를 목적지 호스트로 판단하고 데이터를 전송하며, 라우터는 실제 목적지 호스트로 데이터를 전송합니다.

아래 그림은 proxy ARP의 동작을 보여주는 예제입니다.



[그림 - Proxy ARP의 동작]

서브넷 A의 호스트 A(192.168.10.100)는 서브넷 B의 호스트 D(192.168.20.200)에게 패킷을 전송하려 할 때, 호스트 A의 서브넷 마스크가 16비트이기 때문에 호스트 A는 192.168.0.0 대역의 모든 호스트를 같은 네트워크에 속해있다고 판단합니다. 따라서, 호스트 A는 호스트 D와 통신하기 위해 호스트 D 에게 ARP 요청을 서브넷 A에 브로드캐스트합니다. 호스트 A가 브로드캐스트한 ARP 요청은 PAS-K의 v0 인터페이스를 포함한 서브넷 A에 속한 모든 호스트에게 전송되지만, 기본적으로 PAS-K는 ARP 브로드캐스트를 다른 네트워크에 전송할 수 없으므로, 호스트 A의 ARP 브로드캐스트는 호스트 D에 전송될 수 없습니다.

그러나, 만약 PAS-K에 Proxy ARP 기능이 활성화되어 있다면, PAS-K가 호스트 A로부터 호스트 D를 찾는 ARP 요청을 수신했을 때, 라우팅 테이블에 호스트 D가 속한 네트워크의 경로가 존재한다면 호스트 A에게 자신의 MAC 주소(00-00-0c-94-36-ab)를 전송합니다. 따라서 호스트 A는 호스트 D에게 전송하는 패킷을 00-00-0c-94-36-ab MAC 주소로 전송합니다. PAS-K는 호스트 D가 자신이 가지고 있는 경로에 속하므로 호스트 A로부터 수신된 패킷을 호스트 D에게 전송합니다.

또한, 호스트 A의 ARP 캐시에는 서브넷 B에 속한 호스트의 MAC 주소를 모두 PAS-K의 MAC 주소로 저장하기 때문에 호스트 A는 서브넷 B에 속하는 호스트에게 패킷을 전송 시 모두 PAS-K에게 전송하고, PAS-K는 이를 모두 서브넷 B에 속하는 호스트로 전송합니다. 호스트 A에 저장된 ARP 캐시 정보는 다음과 같습니다.

[표 - ARP 캐시 정보]

IP 주소	MAC 주소
192.168.10.200	00-00-0c-94-36-bb
192.168.10.20	00-00-0c-94-36-ab
192.168.20.100	00-00-0c-94-36-ab
192.168.20.200	00-00-0c-94-36-ab

CLI에서 설정하기

이 절에서는 CLI에서 proxy ARP를 설정하는 방법에 대해 살펴봅니다.

Proxy ARP 설정

PAS-K에는 기본적으로 proxy ARP 기능이 비활성화되어 있습니다. Proxy ARP 기능의 상태를 변경하려면 <Configuration 모드>에서 다음과 같은 명령을 실행합니다.

명 령	설 명
arp proxy-arp {enable | disable}	Proxy ARP 기능의 사용 여부를 설정합니다. • **enable** Proxy ARP 기능 활성화 • **disable** Proxy ARP 기능 비활성화 (기본값)

Proxy ARP 설정 정보 보기

Proxy ARP 의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show arp** 명령을 실행합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

ARP Locktime 설정

이 절에서는 ARP Locktime 기능에 대해 상세히 살펴보고, CLI를 통해 ARP Locktime 기능을 설정하는 방법에 대해 알아봅니다.

ARP Locktime 개요

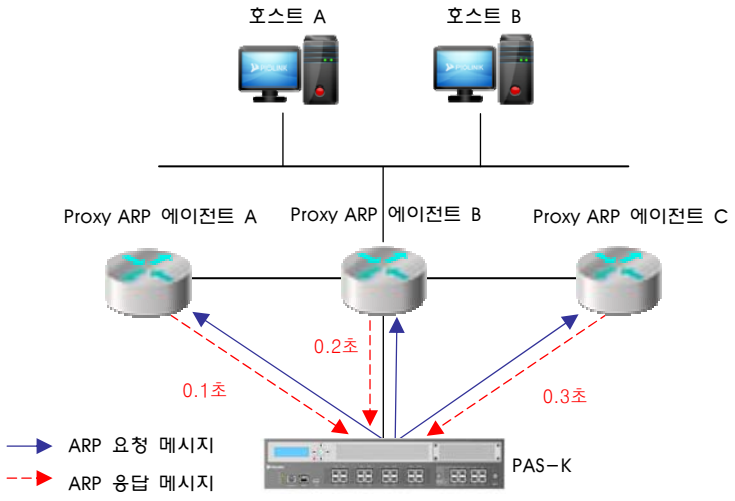
IP 네트워크 상에서 통신을 수행하는 경우, 데이터를 전송하려는 호스트는 목적지 호스트의 IP 주소에 해당하는 MAC 주소를 알아내기 위해 ARP 요청 패킷을 전송합니다. 이를 수신한 목적지 호스트는 자신의 MAC 주소 정보를 담고 있는 ARP 응답 패킷을 전송합니다. ARP 응답 패킷을 수신하게 되면 ARP 응답 패킷을 전송한 호스트의 IP 주소와 MAC 주소를 자신의 ARP 테이블에 등록하여 이후에 데이터를 전송할 때 사용합니다. ARP 테이블에 엔트리 정보를 등록해두면 데이터를 전송할 때, 먼저 목적지 IP 주소에 대응하는 MAC 주소가 있는지 ARP 테이블에서 확인합니다. 만약, 해당 MAC 주소가 ARP 테이블에 등록되어 있으면 ARP 요청 패킷을 전송하는 과정 없이 바로 목적지 호스트에게 IP 패킷을 전송합니다. 이렇게 등록된 엔트리 정보는 일정 시간 동안 ARP 테이블에 저장됩니다. 그리고, IP 주소가 재할당되거나 중복되는 IP 주소가 할당되는 경우, 혹은 새로운 MAC 주소를 가진 호스트가 추가되는 경우에 ARP 테이블을 갱신합니다.

그러나, ARP 테이블을 지속적으로 갱신하는 경우, ARP 테이블을 이용한 ARP Flooding 공격으로 인한 피해를 입게 될 수 있습니다. ARP Flooding 공격은 존재하지 않는 ARP 주소나 잘못된 ARP 주소를 시스템의 ARP 테이블에 등록하여 지속적으로 ARP 요청 패킷이나 ARP 응답 패킷을 전송하는 것을 말합니다. ARP Flooding 공격이 계속되면 과도한 ARP 패킷 처리로 인해 CPU의 과부하를 초래하고, 시스템의 다른 프로세스들이 올바른 서비스를 제공하지 못하도록 합니다.

이러한 문제가 발생하는 것을 방지하기 위해서 PAS-K는 ARP Locktime 기능을 지원합니다. ARP Locktime은 ARP 엔트리의 갱신 주기를 설정하여 사용자가 지정한 시간(locktime) 동안 해당 ARP 엔트리가 갱신되지 않도록 합니다. ARP Locktime 기능을 이용하여 ARP 테이블의 갱신 주기를 지정해두면 ARP Flooding 공격으로 인한 피해를 방지하고 다수의 Proxy ARP 에이전트가 존재하는 네트워크에서 효율적으로 ARP 테이블을 관리할 수 있습니다.

네트워크 상에 다수의 Proxy ARP 에이전트가 존재할 경우 호스트의 ARP 요청에 대해 둘 이상의 Proxy ARP 에이전트가 응답 패킷을 보내면, 불필요하게 계속해서 ARP 테이블을 갱신하게 됩니다.

이 때, ARP Locktime을 설정해 두면, 지정된 시간 내에 ARP 응답 패킷을 보낸 여러 Proxy ARP 에이전트 중에 가장 먼저 ARP 응답 패킷을 보낸 에이전트의 엔트리만을 ARP 테이블에 등록합니다. 다음 그림과 같이 3개의 Proxy ARP 에이전트가 존재하고, PAS-K가 호스트 A의 MAC 주소를 알아내려고 하는 경우를 예로 들어봅니다. PAS-K에는 APR Locktime이 1초로 설정되어 있습니다.



[그림 - 다수의 Proxy ARP 에이전트가 있는 경우 ARP Locktime의 사용 예]

PAS-K가 호스트 A의 MAC 주소를 알아내기 위해 먼저 자신의 IP 주소와 MAC 주소의 정보가 담겨있는 ARP 요청 패킷을 통해 호스트 A의 MAC 주소에 대한 정보를 요청합니다. 그러면, ARP 요청 패킷은 브로드캐스트되어 PAS-K와 연결되어 있는 모든 Proxy ARP 에이전트로 전송됩니다. ARP 요청 패킷을 받은 Proxy ARP 에이전트 A, B, C는 호스트 A를 대신해 자신의 MAC 주소의 정보를 담은 ARP 응답 패킷을 PAS-K에 전송합니다. 이 때, ARP 응답 패킷이 위의 그림과 같이 Proxy ARP 에이전트 A, B, C가 각각 0.1초, 0.2초 0.3초로 전송되면 PAS-K는 가장 먼저 도착한 Proxy ARP 에이전트 A의 엔트리만을 ARP 테이블에 등록하고 그 후에 도착한 Proxy ARP 에이전트 B와 C의 엔트리 정보는 등록하지 않습니다. 그리고, Locktime으로 설정된 1초가 지나면 다시 가장 먼저 도착한 엔트리 정보만을 갱신합니다.

즉, ARP Locktime 기능을 실행하면 가장 먼저 ARP 응답 패킷을 보낸 Proxy ARP 에이전트 A의 MAC 주소를 사용하여 호스트 A에게 데이터를 전송하므로 가장 빠르게 통신할 수 있습니다. PAS-K의 ARP Locktime의 설정값은 0 ~ 10,000,000이고 단위는 1/100초입니다.

CLI에서 설정하기

이 절에서는 CLI 명령을 사용하여 ARP Locktime 기능을 설정하고, 설정을 확인하는 방법에 대해 살펴봅니다.

ARP Locktime 설정

PAS-K에 ARP Locktime 기능을 설정하려면 <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
arp locktime <*LOCKTIME*>	ARP Locktime 기능을 설정합니다. • <*LOCKTIME*> APR 테이블을 갱신한 이후 일정 시간 동안 새로운 갱신을 허용하지 않도록 지정할 시간 (설정 범위: 0 ~ 10,000,000, 단위: 1/100 (초), 기본값: 100(초))

ARP Locktime 설정 정보 보기

ARP Locktime 기능의 설정 정보를 확인하려면, <Configuration 모드>에서 **show arp** 명령을 실행합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

ARP Filter 설정

PAS-K의 가상 브리지 구성은 IP 통신을 위한 ARP를 처리하기 위해 Proxy ARP를 사용합니다. Proxy ARP를 사용하게 되면 불필요한 ARP 응답을 하게 되어 장애가 발생하는 경우가 있습니다. 이러한 문제를 해결하기 위해 PAS-K는 ARP Filter 기능을 제공합니다. ARP Filter는 필터를 적용할 정책, 출발지, 목적지 네트워크를 설정하여 Proxy ARP를 통제합니다. 필터의 종류는 두 가지가 있으며 각 필터는 다음과 같습니다.

- **Input** PAS-K 인터페이스의 MAC 주소를 요청하는 ARP 패킷에 적용할 필터
- **Output** PAS-K 가 다른 호스트의 MAC 주소를 요청하는 ARP 패킷에 적용할 필터

CLI에서 설정하기

이 절에서는 CLI에서 ARP Filter를 설정하는 방법에 대해 살펴봅니다.

Input ARP Filter 설정하기

PAS-K에 Input ARP Filter를 설정하려면 <Configuration 모드>에서 다음과 같은 과정을 수행합니다. Input ARP Filter는 최대 32개의 필터를 등록할 수 있으므로, 여러 개의 Input ARP Filter를 설정하려는 경우에는 다음 과정을 반복합니다.

순서	명 령	설 명
1	**arp-filter**	<ARP Filter 설정 모드>로 들어갑니다.
2	**input** *<ID>*	Input ARP Filter를 정의하고, <Input ARP Filter 설정 모드>로 들어갑니다. • *<ID>* Inpit ARP Filter ID. 설정 범위: 1 ~ 32 **참고:** ID는 우선 순위 역할을 하며, 숫자가 작을수록 우선 순위가 높습니다.
3	**action** {**accept** | **drop**}	Input ARP Filter 의 정책을 지정합니다. • **accept** 조건과 일치하는 패킷을 허용 (기본값) • **drop** 조건과 일치하는 패킷을 폐기 **참고:** Input ARP Filter의 정책을 기본값으로 변경하려면, **no action** 명령을 실행합니다.
4	**sip** *<SIP>*	Input ARP Filter를 적용할 패킷의 출발지 IP 주소 또는 대역을 지정합니다. • *<SIP>* 출발지 IP 주소와 넷마스크 비트. 기본값: 0.0.0.0/0 **참고:** 설정한 출발지 IP 주소를 삭제하려면, **no sip** 명령을 실행합니다.
5	**dip** *<DIP>*	Input ARP Filter를 적용할 패킷의 목적지 IP 주소 또는 대역을 지정합니다. • *<DIP>* 목적지 IP 주소와 넷마스크 비트. 기본값: 0.0.0.0/0 **참고:** 설정한 목적지 IP 주소를 삭제하려면, **no dip** 명령을 실행합니다.
6	**interface** *<INTERFACE>*	Input ARP Filter를 적용할 인터페이스를 지정합니다. • *<INTERFACE>* 인터페이스 이름 **참고:** 설정한 인터페이스를 삭제하려면, **no interface** 명령을 실행합니다.
7	**current**	설정한 Input ARP Filter 정보를 확인합니다.
8	**apply**	설정한 Input ARP Filter를 저장하고 시스템에 적용합니다.

참고: 생성한 Input ARP Filter를 삭제하려면 <ARP Filter 설정 모드>에서 **no input** *<ID>* 명령을 실행합니다.

Ouput ARP Filter 설정하기

PAS-K에 Output ARP Filter를 설정하려면 <Configuration 모드>에서 다음과 같은 과정을 수행합니다. Output ARP Filter는 최대 32개의 필터를 등록할 수 있으므로, 여러 개의 Output ARP Filter를 설정하려는 경우에는 다음 과정을 반복합니다.

순서	명 령	설 명
1	**arp-filter**	<ARP Filter 설정 모드>로 들어갑니다.
2	**output** *<ID>*	Output ARP Filter를 정의하고, <Output ARP Filter 설정 모드>로 들어갑니다. • *<ID>* Outpit ARP Filter ID. 설정 범위: 1 ~ 32. **참고:** ID는 우선 순위 역할을 하며, 숫자가 작을수록 우선 순위가 높습니다.
3	**action {accept | drop}**	Output ARP Filter 의 정책을 지정합니다. • **accept** 조건과 일치하는 패킷을 허용 (기본값) • **drop** 조건과 일치하는 패킷을 폐기 **참고:** Output ARP Filter의 정책을 기본값으로 변경하려면, **no action** 명령을 실행합니다.
4	**sip** *<SIP>*	Output ARP Filter를 적용할 패킷의 출발지 IP 주소 또는 대역을 지정합니다. • *<SIP>* 출발지 IP 주소와 넷마스크 비트. 기본값: 0.0.0.0/0 **참고:** 설정한 출발지 IP 주소를 삭제하려면, **no sip** 명령을 실행합니다.
5	**dip** *<DIP>*	Output ARP Filter를 적용할 패킷의 목적지 IP 주소 또는 대역을 지정합니다. • *<DIP>* 목적지 IP 주소와 넷마스크 비트. 기본값: 0.0.0.0/0 **참고:** 설정한 목적지 IP 주소를 삭제하려면, **no dip** 명령을 실행합니다.
6	**interface** *<INTERFACE>*	Output ARP Filter를 적용할 인터페이스를 지정합니다. • *<INTERFACE>* 인터페이스 이름 **참고:** 설정한 인터페이스를 삭제하려면, **no interface** 명령을 실행합니다.
7	**current**	설정한 Output ARP Filter 정보를 확인합니다.
8	**apply**	설정한 Output ARP Filter를 저장하고 시스템에 적용합니다.

참고: 생성한 Output ARP Filter를 삭제하려면 <ARP Filter 설정 모드>에서 **no output** *<ID>* 명령을 실행합니다.

ARP Filter 설정 정보 보기

ARP Filter의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show arp-filter** 명령을 실행합니다.

참고: 해당 명령 실행시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

저장 MAC 응답 설정

저장 MAC 응답 기능은 클라이언트가 전송한 요청 패킷의 출발지 MAC 주소와 목적지 MAC 주소를 저장해두었다가 응답 패킷을 전송할 때 저장된 MAC 주소를 그대로 사용합니다. 저장 MAC 응답 기능을 사용하지 않으면 응답 패킷을 보낼 때마다 라우팅을 수행합니다.

저장 MAC 응답 기능을 사용하기 위해서는 요청 패킷의 출발지/목적지 MAC 주소가 응답 패킷에 그대로 사용할 수 있는 환경이어야 합니다. 기본적으로 저장 MAC 응답 기능은 비활성화 상태입니다.

CLI에서 설정하기

저장 MAC 응답 설정

저장 MAC 응답 기능을 설정하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
env reply_with_stored_mac {enable | disable}	저장 MAC 응답 기능의 사용 여부를 설정합니다. • **enable** 저장 MAC 응답 기능 활성화 • **disable** 저장 MAC 응답 기능 비활성화 (기본값)

저장 MAC 응답 설정 정보 보기

저장 MAC 응답 기능의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show env** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다

정적(Static) ARP 캐시 설정

ARP(Address Resolution Protocol)는 IP 네트워크 상에서 IP 주소를 MAC 주소로 대응시키기 위해 사용되는 프로토콜입니다. 예를 들어, 장비 A가 장비 B에게 패킷을 전송하려고 할 때, 장비 B의 MAC 주소를 알고 있지 않은 경우에는 ARP 프로토콜을 사용하여 목적지 B의 IP 주소와 MAC 주소 FF:FF:FF:FF:FF:FF를 가지는 ARP 패킷을 전송합니다. 장비 B는 자신의 IP 주소를 가진 ARP 패킷을 받으면 장비 A에게 자신의 MAC 주소를 알려주는 패킷을 보냅니다. 이와 같은 방식으로 수집된 IP 주소와 이에 해당하는 MAC 주소는 장비의 ARP 캐시라고 불리는 메모리에 테이블 형태로 저장됩니다. 저장된 정보는 다음 패킷 전송 시에 사용됩니다.

PAS-K에서는 위에서 설명한 동적 ARP 기능을 지원할 뿐만 아니라 사용자가 직접 IP 주소와 MAC 주소를 매핑시킬 수 있는 정적 ARP 캐시 기능도 지원합니다. 정적 ARP 캐시 기능을 이용하여 IP 주소와 MAC 주소를 매핑한 경우에는 해당 IP 주소에 대해 동적 ARP 기능이 수행되지 않습니다.

CLI에서 설정하기

정적 ARP 캐시 설정

특정 IP 주소에 대한 MAC 주소를 사용자가 직접 입력하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
arp static *<IPADDR> <HWADDR>*	IP 주소에 대한 MAC 주소를 설정합니다. • *<IPADDR> <HWADDR>* Ip 주소 및 MAC 주소 입력.

참고: 정적 ARP 캐시 항목를 삭제하려면 <Configuration 모드>에서 **no arp static** *<IPADDR>* 명령을 사용합니다.

정적 ARP 캐시 설정 정보 보기

정적 ARP 캐시 기능의 정보를 확인하려면, <Configuration 모드>에서 **show arp static** 명령을 사용합니다. **show arp static** *<IPADDR>* 명령을 사용하면 지정한 IP에 대한 MAC 주소와 interface 정보 만을 확인 할 수 있습니다.

참고: <Configuration 모드>에서 **show arp** 명령을 사용하면 ARP 테이블의 내용을 확인할 수 있습니다. 동적 ARP 기능을 통해 추가된 ARP 항목은 Dynamic 부분에 표시되고, 사용자가 직접 추가한 정적 ARP 캐시 항목은 Static 부분에 표시됩니다.

참고: 자동으로 생성된 동적 ARP 캐시 항목를 삭제하려면 <Configuration 모드>에서 **no arp dynamic** [*<IPADDR>*] 명령을 사용합니다. IP 주소를 입력하면 해당 동적 ARP 캐시항목만 삭제됩니다.

DNS 설정

DNS(Domain Name System)는 호스트의 이름이나 도메인 이름을 실제 IP 주소로 변환해주는 시스템입니다. PAS-K에 DNS 서버를 등록하면 사용자는 ping, telnet, traceroute 등의 IP 주소를 이용한 명령을 실행할 때, 복잡한 IP 주소 대신 호스트 이름을 사용하여 보다 편리하게 여러가지 작업을 수행할 수 있습니다. DNS 서비스를 사용하려면 먼저 사용자의 네트워크에서 사용할 DNS 서버를 등록해야 합니다.

PAS-K에는 기본 DNS 서버와 보조 DNS 서버를 등록할 수 있습니다. PAS-K는 먼저 기본 DNS 서버에 DNS 쿼리를 전송하고, 기본 DNS 서버에서 응답이 없을 경우, 보조 DNS 서버에게 쿼리를 전송합니다. PAS-K에는 하나의 기본 DNS 서버와 3개의 보조 DNS 서버를 지정할 수 있습니다. 기본적으로 DNS 서비스는 기본 DNS 서버가 사용되고, 기본 DNS 서버가 정상적으로 동작하지 않을 때에는 추가한 순서대로 보조 DNS 서버가 사용됩니다.

CLI에서 설정하기

DNS 서버 설정

PAS-K에 DNS 서버를 등록하기 위해 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
dns *<ID>* **ip** *<IP>*	DNS 서버를 등록합니다. DNS • *<ID>* 서버의 ID 지정. ID가 '1'번인 DNS 서버가 기본 DNS 서버가 되고, 그 뒤에 추가하는 DNS 서버는 보조 DNS1, 보조 DNS2, 보조 DNS3이 됩니다. (설정 범위: 1 ~ 4) • *<IP>* DNS 서버의 IP 주소

참고: 등록한 DNS 서버를 삭제하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no dns <ID>
```

DNS 서버 설정 정보 보기

등록한 모든 DNS 서버 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show dns** 명령을 실행합니다. 특정 ID의 DNS 주소만 확인하려면, **show dns** 명령어 뒤에 ID를 입력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

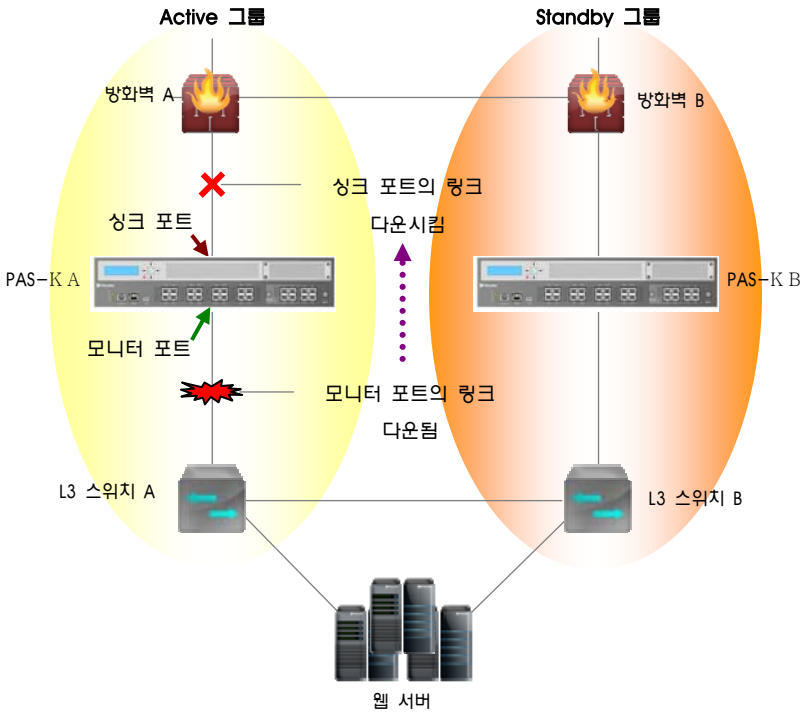
링크 싱크(Linksync)설정

이 절에서는 링크 싱크의 기능에 대해 소개한 후 CLI에서 링크 싱크 기능을 설정하는 방법에 대해 차례로 알아봅니다.

링크 싱크 개요

링크 싱크(Linksync)는 모니터 포트와 싱크 포트의 링크 상태를 주기적으로 감시하여 두 포트 간의 링크 상태를 동기화 시켜주는 기능입니다. 링크 싱크는 두 가지 모드(단방향 싱크, 양방향 싱크)를 제공하여, 다양한 네트워크 구성을 지원합니다.

다음 그림은 Active 그룹과 Standby 그룹이 존재하는 Failover 구성에서 링크 싱크 기능이 사용되는 예입니다.



[그림 - 링크 싱크 구성의 예]

위 구성에서 L3 스위치 A와 PAS-K A 가 연결된 링크가 다운되더라도 방화벽 A는 PAS-K A와의 링크가 살아 있기 때문에 요청 패킷을 전송합니다. 그러나 L3 스위치 A와 PAS-K A 간의 링크가 다운되었기 때문에 요청 패킷은 웹 서버에게 전송될 수 없습니다. 이로 인해 웹 서버는 지속적인 서비스를 제공할 수 없게 됩니다.
한편, 링크 싱크 기능을 사용할 경우, PAS-K 는 지속적으로 모니터 포트의 상태를 감시하여 모니터 포트가 다운되었을 경우, 싱크 포트의 링크도 다운시켜 방화벽A가 방화벽 B로 failover됩니다. 이로써, 웹 서버는 PAS-K B를 통해 지속적인 서비스를 제공할 수 있습니다.

- **단방향 모드**
  모니터 포트의 링크 상태를 감시하여 모니터 포트의 링크가 다운될 경우 싱크 포트도 링크 다운시킵니다. 모니터 포트가 링크 업 되면 싱크 포트도 링크 업 시킵니다.

- **양방향 모드**
  기본적인 동작은 단방향 모드와 같지만 모니터 포트와 싱크 포트 모두 링크 상태를 감시한다는 차이점이 있습니다. 양방향 모드의 모니터 포트와 싱크 포트의 상태는 서로의 링크 상태에 따라 변경됩니다. 즉, 앞의 그림에서 싱크 포트의 링크가 다운되면 모니터 포트의 링크도 다운시킵니다. 그렇게 되면, L3 스위치 A로 수신된 패킷이 PAS-K A로 전송되지 않고 L3 스위치 B로 전송되어 PAS-K B를 통해 지속적으로 서비스를 제공할 수 있습니다.

CLI에서 설정하기

이 절에서는 CLI에서 링크 싱크를 설정하는 방법과 링크 싱크를 활성화하는 방법을 살펴봅니다.

링크 싱크 설정

링크 싱크 기능을 동작시키거나 혹은 동작 중인 링크 싱크 기능의 설정을 변경하려면, <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**linksync** *<ID>*	링크 싱크를 생성하고 <링크 싱크 설정 모드>로 들어갑니다. • *<ID>* 링크 싱크의 ID (설정 범위: 1 ~ 16)
2	**mode {one-way | two-way}**	링크 싱크의 모드를 설정합니다. • **one-way** 단방향 싱크 모드(기본값) • **two-way** 양방향 싱크 모드
3	**monitor-port** *<MONITOR-PORT>* (필수 설정)	링크 상태를 확인할 모니터 포트를 설정합니다. • *<MONITOR-PORT>* 모니터 포트 설정. 여러 개의 모니터 포트를 추가하려면 공백 없이 쉼표(,)로 각 포트를 구분하도록 하고, 연속되는 포트는 대쉬(-)를 사용하여 입력하면 편리합니다. **참고:** 링크 싱크 기능을 사용하기 위해서는 반드시 1개 이상의 모니터 포트를 설정해야 합니다.
4	**sync-port** *<SYNC-PORT>* (필수 설정)	모니터 포트의 상태에 따라 링크 상태를 변경할 싱크 포트를 설정합니다. • *<SYNC-PORT>* 싱크 포트 설정. 여러 개의 싱크 포트를 추가하려면 공백 없이 쉼표(,)로 각 포트를 구분하도록 하고, 연속되는 포트는 대쉬(-)를 사용하여 입력하면 편리합니다. **참고:** 링크 싱크 기능을 사용하기 위해서는 반드시 1개 이상의 싱크 포트를 설정해야 합니다.
5	**sync-delay-time** *<SYNC-DELAY-TIME>*	모니터 포트의 링크 상태가 변경되었을 경우, 싱크 포트의 링크 상태를 변경하기까지의 대기 시간을 설정합니다. • *<SYNC-DELAY-TIME>* 링크 상태 변경 전 대기 시간 (설정 범위: 1~30(초), 기본값: 1(초))
6	**status {enable | disable}**	링크 싱크 기능의 사용 여부를 지정합니다. • **enable** 링크 싱크 기능 활성화 (기본값) • **disable** 링크 싱크 기능 비활성화
7	**current**	설정한 링크 싱크 정보를 확인합니다.
8	**apply**	설정된 링크 싱크 정보를 저장하고 시스템에 적용합니다.

참고: 모니터 포트 및 싱크 포트를 삭제하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no monitor-port
(config)# no sync-port
```

정의한 링크 싱크 기능을 삭제하려면, <Configuration 모드>에서 **no linksync** *<ID>* 명령을 실행합니다.

참고: PAS-K에는 모드에 관계없이 최대 8개의 링크 싱크를 설정할 수 있으며, 하나의 링크 싱크에 설정된 포트는 다른 링크 싱크 설정에 포함될 수 없습니다.

참고: 링크 싱크 기능에 사용되는 포트는 항상 활성화 상태여야 하며, 비 활성화로 설정된 포트에서는 링크 싱크 기능이 동작하지 않습니다.

참고: 하나의 링크 싱크 설정에는 여러 개의 모니터 포트와 싱크 포트를 설정할 수 있습니다. 이 경우, 모든 모니터 포트들이 링크 다운되어야 싱크 포트의 모든 포트들도 링크 다운되고 모든 모니터 포트가 링크 업되어야 싱크 포트의 모든 포트들도 링크 업됩니다.

링크 싱크 설정 정보 보기

링크 싱크 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show linksync** 명령을 사용합니다. 특정 ID의 링크 싱크 정보를 확인하려면, **show linksync** 명령어 뒤에 링크 싱크 ID를 입력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

포트 미러링 설정

이 절에서는 포트 미러링의 개념과 동작 과정을 살펴본 후 CLI에서 포트 미러링을 설정하는 방법에 대해 차례로 알아봅니다.

포트 미러링 개요

포트 미러링은 특정 포트에 송수신되는 모든 패킷들의 복사본을 다른 포트에 전달하는 기능입니다. 포트 미러링의 대상이 되는 포트를 모니터 대상 포트(mirrored 포트)라고 하고, 모니터 대상 포트의 트래픽이 전달되는 포트를 모니터 포트(mirroring 포트)라고 합니다.

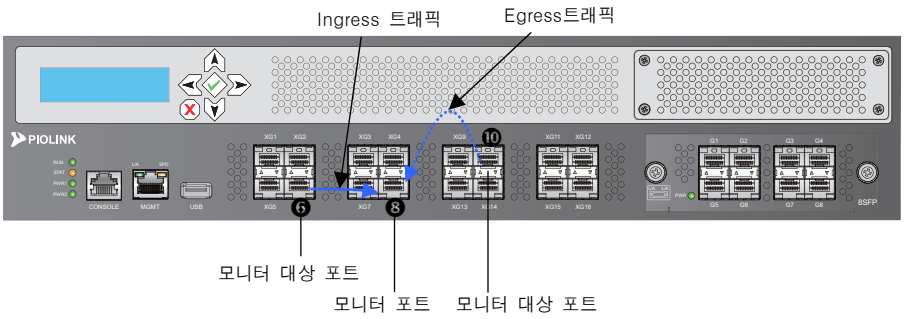
모니터 포트(mirroring 포트)

모니터 포트는 모니터 대상 포트로부터 복사한 모든 데이터를 수신하는 포트입니다. 사용자는 관리용 이더넷 포트를 제외한 PAS-K의 모든 포트를 모니터 포트로 사용할 수 있습니다. 일반적으로는 모니터 포트에는 네트워크 분석기나 RMON 등을 연결하여 네트워크를 모니터링합니다. 모니터 포트는 포트 미러링 기능을 수행하는 동안에는 모니터 대상 포트의 데이터를 수신하는 기능으로만 동작합니다. 포트 미러링 기능이 비활성화되면 다시 정상적인 L2, L3 동작을 수행하게 됩니다.

모니터 대상 포트(mirrored 포트)

모니터 대상 포트는 모니터 포트로부터 모니터링되는 포트입니다. 모니터 대상 포트는 모니터 포트와는 달리 포트 미러링 기능이 동작하는 동안에도 정상적인 L2, L3 동작을 수행합니다. PAS-K에는 동시에 여러 개의 모니터 대상 포트를 지정할 수 있습니다. 다만, 모니터 대상 포트의 전체 대역폭이 반드시 모니터 포트의 대역폭을 초과하지 않아야 합니다. 예를 들어, 여러 개의 기가빗 이더넷 포트를 모니터링하려면, 모니터 포트는 반드시 10 기가빗 이더넷 포트를 지정해야 합니다.

다음 그림은 PAS-K에 포트 미러링 기능을 사용한 예입니다.



[그림 - 포트 미러링]

포트 8은 포트 6의 ingress 트래픽(PAS-K로 수신되는 트래픽)과 포트 10의 egress 트래픽(PAS-K가 송신하는 트래픽)을 모니터링하는 포트입니다. 예를 들어, 포트 8번에 포트 6과 10으로부터 송수신되는 트래픽을 모니터하기 위해 IDS 서버를 모니터 포트에 연결하면 포트 6, 10번의 네트워크를 공격하는 공격자를 탐지할 수 있습니다.

PAS-K의 포트 미러링 기능을 이용하면 사용자는 PAS-K에 연결된 네트워크에서 발생하는 모든 트래픽을 모니터링할 수 있습니다. 이 기능은 주로 네트워크에서 발생한 문제를 해결하기 위한 도구로 사용하거나 보다 나은 네트워크 보안을 제공하기 위해 사용합니다.

단, 포트 미러링 기능 사용 중 많은 양의 트래픽이 발생한 경우에는 CPU 사용률 증가로 인한 시스템 과부하가 발생할 수 있습니다. 그러므로, 포트 미러링 기능을 장기간 사용하는 경우에는 주의가 필요합니다.

CLI에서 설정하기

이 절에서는 CLI에서 모니터 포트와 모니터 대상 포트를 설정하는 방법과 포트 미러링을 활성화하는 방법을 살펴봅니다.

포트 미러링 설정

모니터 포트와 모니터 대상 포트를 설정하고 포트 미러링의 상태를 변경하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**mirroring monitor** *<MONITOR>*	모니터 포트를 설정합니다. • *<MONITOR>* 포트 이름을 입력, 하나의 포트만 지정 가능.
2	**mirroring {mirrored_in** *<MIRRORED_IN>* **| mirrored_out** *<MIRRORED_OUT>*}	모니터 대상 포트와 미러링할 트래픽의 방향을 설정합니다. • *<MIRRORED_IN>* 수신 트래픽을 모니터링할 포트 이름. 두 개 이상의 포트를 지정하는 경우에는 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용 • *<MIRRORED_OUT>* 송신 트래픽을 모니터링할 포트 이름. 두 개 이상의 포트를 지정하는 경우에는 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용
3	**mirroring status {enable | disable}**	포트 미러링 기능의 사용 여부를 지정합니다. • **enable** 포트 미러링 기능 활성화 • **disable** 포트 미러링 기능 비활성화 (기본값)

주의: 모니터 대상 포트의 대역폭 합이 모니터 포트의 대역폭과 같거나 크지 않도록 설정해야 합니다. 모니터 대상 포트의 대역폭 합이 모니터 포트의 대역폭보다 크면, 모니터 포트에서는 그 차이만큼의 트래픽을 손실합니다.

주의: 포트 미러링 설정 시 모니터 포트는 모니터 대상 포트와 같은 VLAN에 속해 있어야 합니다. 그렇지 않으면, 포트 미러링이 올바르게 동작하지 않습니다.

참고: 모니터 대상 포트를 삭제하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no mirroring mirrored_in <MIRRORED_IN>
(config)# no mirroring mirrored_out <MIRRORED_OUT>
```

모니터 포트를 삭제하려면, <Configuration 모드>에서 **no mirroring monitor** 명령을 실행합니다.

포트 미러링 설정 정보 보기

설정한 포트 미러링 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show mirroring** 명령을 실행합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

Link Aggregation 설정

이 절에서는 Link Aggregation의 개념과 PAS-K에 LACP 및 포트 트렁킹을 설정할 때 주의해야 할 사항들에 대해 소개합니다. 또한 CLI에서 LACP와 포트 트렁킹을 설정하는 방법에 대해 차례로 알아봅니다.

Link Aggregation 개요

Link Aggregation은 여러 개의 포트들을 하나의 그룹(트렁크 그룹)으로 설정하여 하나의 논리적인 포트로 사용할 수 있게 하는 기능입니다. Link Aggregation을 이용하면 여러 개의 패스트 이더넷 또는 기가 비트 이더넷 포트들을 하나의 트렁크 그룹으로 설정하고, 이를 대역폭이 큰 하나의 포트로 사용할 수 있습니다. 여러 개의 포트들이 마치 하나의 포트처럼 동작하기 때문에 VLAN이나 STP 등에서도 하나의 포트처럼 관리됩니다.

위와 같이 대역폭을 확장하는 기능 이외에도 Link Aggregation을 사용하면 트렁크 그룹에 속한 여러 포트 중에서 일부 포트에 문제가 발생하여 정상적으로 동작할 수 없는 경우에 나머지 포트에 의해 통신을 계속 할수 있기 때문에 시스템의 안정성을 높일 수 있습니다.

PAS-K가 지원하는 Link Aggregation에는 포트 트렁킹과 LACP 두 가지가 있습니다.

포트 트렁킹

포트 트렁킹은 두 개 이상의 포트를 하나의 논리적인 포트로 통합하여 보다 넓은 대역폭을 사용할 수 있도록 하는 기능입니다. 포트 트렁킹은 논리적인 포트를 사용하여 다른 네트워크의 장비와 연결하는 경우, 장비 간의 설정을 사용자가 수동으로 해야합니다.

PAS-K의 포트 트렁킹 기능은 트래픽을 같은 트렁크 그룹에 속한 포트들에게 분산시켜주는 부하 분산 기능을 제공합니다. 부하 분산 기능을 사용하면 트렁크 그룹 내의 특정 포트가 트래픽을 처리할 수 없는 경우 트래픽은 트렁크 그룹 내의 가용한 다른 포트에게 분산됩니다.

LACP

범용 프로토콜인 LACP(Link Aggregation Control Protocol)는 포트 트렁킹 기능과 같이 두 개 이상의 포트를 하나의 논리적인 포트로 통합하여 보다 더 넓은 대역폭을 사용할 수 있도록 하는 기능입니다. 포트 트렁킹 기능과 LACP가 구별되는 특징은 포트를 통합할 논리적인 통합 포트(Aggregator)와 논리적인 포트로 통합될 대상이 되는 물리적인 멤버 포트만 설정해두면 자동적으로 통합된 대역폭을 형성한다는 점입니다. 따라서 포트 트렁킹에 비해 설정이 간편하고, 환경 변화에 따라 신속하게 대응할 수 있습니다.

LACP 동작 모드

PAS-K가 지원하는 LACP 동작 모드에는 Acitve 모드와 Passive 모드의 두 가지가 있습니다. Active 모드는 상호 Link Aggregation 협상 정보를 교환하여 동작하는 동적 모드로써, 반대편 장비에서 먼저 협상 패킷을 전송할 수 있습니다. Passive 모드는 Link Aggregation 협상 정보를 수신하는 대기 모드로써, 반대편 장비에서 협상 패킷이 송신되어야만 동작합니다. 즉, Passive 모드로 설정된 포트는 Active 모드로 설정된 상대 장비의 포트가 존재해야만 LACP 동작을 수행합니다. Active 모드 포트는 Passive 모드 포트보다 우선순위가 높기 때문에 기준이 됩니다. 따라서 Passive 모드 포트가 Active 모드 포트의 설정을 따라가게 됩니다.

LACP 우선순위 설정

서로 연결된 두 장비의 LACP 동작 모드가 Active 모드로 설정되어 있는 경우에는 어떤 장비를 기준으로 정할 것인지 우선순위를 설정할 필요가 있습니다. PAS-K는 이러한 경우를 위해 장비의 우선순위 지정이 가능합니다. 서로 연결된 두 장비가 각각 Active 모드와 Passive 모드로 설정되면 Active 모드로 설정된 장비가 기준이 되고, 모두 Active 모드로 설정되어 있으면 우선순위 값이 낮은 장비가 기준이 됩니다. 우선순위가 동일한 경우에는 MAC 주소 값이 작은 장비가 높은 우선순위를 갖게 됩니다.

멤버 포트 우선순위 설정

하나의 논리적인 통합 포트(Aggregator)에는 최대 16개의 포트를 멤버 포트로 설정할 수 있으며, 그 중 8개의 멤버 포트만이 활성화됩니다. 만일 멤버 포트가 10개 설정되어 있다면 포트가 가지고 있는 우선순위 값(port ID)이 낮은 순서대로 8개의 포트가 정해지게 됩니다. 그러나, 포트가 가지고 있는 우선순위 값과 상관없이 멤버 포트로 지정하고 싶은 포트가 있다면 사용자가 우선순위(Priority)를 지정할 수 있습니다.

부하 분산 알고리즘 설정

통합 포트로 들어오는 패킷들은 지정된 기준에 따라 각 멤버 포트에 분산되어 처리됩니다. 이 방법은 특정 멤버 포트로의 트래픽 집중을 방지하여 보다 안정적이고 효율적인 통합 포트 운용이 가능하도록 합니다. PAS-K에서 설정 가능한 부하분산 알고리즘은 다음과 같습니다.

부하 분산 알고리즘	의 미
dst-ip	목적지 IP 주소 기반의 해시 방식
dst-mac	목적지 MAC 주소 기반의 해시 방식
src-dst-ip	목적지와 출발지 IP 주소의 XOR 값을 이용한 해시 방식
src-dst-mac	목적지와 출발지 MAC 주소의 XOR 값을 이용한 해시 방식
src-ip	출발지 IP 주소 기반의 해시 방식
src-mac	출발지 MAC 주소 기반의 해시 방식

Link Aggregation 설정 시 주의 사항

PAS-K에 포트 트렁킹 및 LACP를 설정할 때 다음의 사항들에 주의해야 합니다.

- PAS-K 에는 총 7 개의 트렁크 그룹(1~7)을 만들 수 있으며, 각 트렁크 그룹에는 2 ~ 8 개의 포트를 포함시킬 수 있습니다.
- 트렁크 그룹 내의 모든 포트는 반드시 동일한 속도이어야 합니다. 하나의 포트는 동시에 둘 이상의 트렁크 그룹에 속할 수 없습니다.
- 트렁크 그룹에 포함되는 포트들은 모두 같은 VLAN 에 포함되어 있어야 하며, tagged 옵션이 동일해야 합니다.
- 트렁크 그룹은 포트 트렁킹과 LACP 각각 7 개씩을 생성할 수 있는 것이 아니라, 포트 트렁킹과 LACP 를 합한 수가 7 개이어야 합니다.
- 포트 트렁킹 및 LACP 에 멤버 포트로 설정된 포트들은 VLAN 설정을 변경 할 수 없습니다. 멤버 포트를 VLAN 에 포함시키려면, 먼저 VLAN 설정을 한 후 포트 트렁킹 및 LACP 의 멤버 포트로 설정합니다.
- 포트 트렁킹 및 LACP 에 포함된 멤버 포트들의 포트 설정은 변경할 수 없습니다.

CLI에서 설정하기

이 절에서는 CLI에서 포트 트렁킹과 LACP를 설정하는 방법에 대해 살펴봅니다.

포트 트렁킹 설정

포트 트렁킹을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**trunk** *<NUM>* **port** *<PORT>*	트렁크 그룹에 포함될 포트를 설정합니다. • *<NUM>* PAS-K에 미리 정의되어 있는 트렁크 그룹의 번호를 입력(설정 범위: 1 ~ 7) • *<PORT>* 반드시 두 개 이상의 포트를 지정해야 하며, 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용
2	**trunk** *<NUM>* **load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}	트렁크 그룹에 속한 모든 포트에 적용할 부하 분산 알고리즘을 설정합니다. • **load-balance** 부하 분산 알고리즘의 종류 지정 (기본값: src-dst-mac)

참고: 트렁크 그룹을 삭제하려면 <Configuration 모드>에서 **no trunk** *<NUM>* 명령을 실행합니다.

포트 트렁킹 정보 보기

설정한 트렁크 그룹의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show trunk** 명령을 실행합니다. 특정 트렁크 그룹에 대한 설정 정보를 확인하려면, **show trunk** 명령 뒤에 해당 트렁크 그룹의 번호(*<NUM>*)를 입력하면 됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

LACP 설정

LACP를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**lacp** *<NUM>* **port** *<NAME>* **mode** {**active** | **passive**}	LACP 통합 포트를 설정하고 동작 모드를 지정합니다. • *<NUM>* 통합 포트 그룹의 번호 입력(설정 범위: 1~7) **주의:** LACP의 통합 포트 그룹 번호에는 포트 트렁킹의 트렁크 그룹에 설정한 번호를 할당할 수 없습니다. • *<NAME>* 통합 포트에 포함시킬 포트 이름. 반드시 두 개 이상의 포트를 지정해야 하며, 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용 • **active** PAS-K의 설정에 따라 LACP가 동작합니다. 상대 장비도 Active 모드인 경우에는 운선순위가 높은 장비의 설정을 따릅니다. • **passive** 상대 장비의 설정에 따라 LACP가 동작합니다.

2	**lacp** *<NUM>* **port** *<NAME>* **priority** *<PRIORITY>*	멤버 포트의 우선순위를 설정합니다. • *<NUM>* 통합 포트 그룹의 번호 입력(설정 범위: 1~7) • *<NAME>* 통합 포트에 포함시킬 포트 이름. 두 개 이상의 포트를 지정하는 경우에는 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용 • *<PRIORITY>* 멤버 포트 우선순위 (설정범위: 1~65535, 기본값: 32768)
3	**lacp** *<NUM>* **load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}	통합 포트 그룹에 적용할 부하 분산 알고리즘을 설정합니다. • *<NUM>* 통합 포트 그룹의 번호 입력(설정 범위: 1~7) • **dst-ip** 목적지 IP 주소 기반의 해시 방식 • **dst-mac** 목적지 MAC 주소 기반의 해시 방식 • **src-dst-ip** 출발지와 목적지 IP 주소의 XOR값을 이용한 해시 방식 • **src-dst-mac** 출발지와 목적지 MAC 주소의 XOR값을 이용한 해시 방식 • **src-ip** 출발지 IP 주소 기반의 해시 방식 (기본값) • **src-mac** 출발지 MAC 주소 기반의 해시 방식

참고: 설정한 LACP 그룹을 삭제하려면 <Configuration 모드>에서 **no lacp** *<NUM>* 명령을 실행합니다.

참고: 통합 포트 그룹에서 멤버 포트를 삭제하려면 <Configuration 모드>에서 **no lacp** *<NUM>* **port** *<NAME>* 명령을 실행합니다.

참고: 통합 포트 그룹에서 멤버 포트의 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 **no lacp** *<NUM>* **port** *<NAME>* **priority** 명령을 실행합니다.

참고: 설정한 통합 포트 그룹의 부하 부산 알고리즘을 기본값으로 변경하려면 <Configuration 모드>에서 **no lacp** *<NUM>* **load-balance** 명령을 실행합니다.

LACP 장비 우선순위 설정

LACP 장비의 우선순위를 설정하려면 <Configuration 모드>에서 다음의 명령을 수행합니다.

명 령	설 명
lacp-system priority *<PRIORITY>*	장비의 우선순위를 설정합니다. • *<PRIORITY>* 장비 우선순위. (설정 범위: 1~65535, 기본값: 32768)

참고: 설정한 장비의 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 **no lacp system-priority** 명령을 실행합니다.

LACP 설정 정보 보기

설정한 LACP 그룹의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show lacp** 명령을 실행합니다. 특정 LACP 그룹에 대한 설정 정보를 확인하려면, **show lacp** 명령 뒤에 해당 VLAN의 이름(*<NAME>*)을 입력하면 됩니다.

LACP 장비 우선순위를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show lacp-system** 명령을 실행합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

포트 Failover설정

이 절에서는 포트 Failover의 개념과 설정 시 주의 사항들에 대해 소개합니다. 또한 CLI에서 포트 Failover 기능을 설정하는 방법에 대해 차례로 알아봅니다.

개요

포트 Failover는 여러 개의 포트들을 하나의 그룹으로 설정하고, 그룹 내의 액티브 포트에 문제가 발생하여 정상적으로 동작할 수 없는 경우 백업 포트가 이를 대체하여 동작하는 기능입니다.
PAS-K에는 최대 4개의 포트 Failover 그룹을 설정할 수 있으며, 하나의 그룹에는 2~4개의 포트를 지정할 수 있습니다. 각각의 포트에는 가중치를 설정할 수 있고, 가중치가 가장 높은 포트가 액티브 포트가 되며 링크 업 상태로 동작합니다. 액티브 포트에 문제가 발생하여 정상 동작하지 않게되면, 링크다운 상태로 있던 백업 포트 중 우선순위가 높은 포트가 액티브 포트로 대체 동작하게 되어 시스템 안정성을 높일 수 있습니다.

포트 Failover 그룹 내에서 각 포트의 우선순위는 가중치, 대역폭(포트 속도), 포트 번호 순서로 결정됩니다. 기본적으로 포트에 설정된 가중치의 값이 클수록 우선순위가 높으며, 가중치를 설정하지 않은 경우에는 포트 번호가 작을수록 우선순위가 높습니다. ge1~ge2, xg1~xg2 와 같이 포트 번호가 같은 경우에는 대역폭이 클수록 우선순위가 높습니다.

CLI에서 설정하기

이 절에서는 CLI에서 포트 Failover를 설정하는 방법에 대해 살펴봅니다.

포트 Failover 설정

포트 Failover를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

명 령	설 명
trunk-active-backup *<CHANNEL-GROUP>* **port** *<PORT>* **weight** *<WEIGHT>*	포트 Failover의 그룹 번호와 포트의 가중치를 설정합니다. • *<CHANNEL-GROUP>* 포트 Failover 그룹의 번호 입력 (설정 범위: 1 ~ 4) • *<PORT>* 그룹에 포함시킬 포트를 지정. **주의**: 포트 트렁킹 또는 LACP 기능이 설정된 포트는 설정할 수 없습니다. • *<WEIGHT>* 그룹에 속한 각 포트의 가중치를 지정. (설정 범위: 1 ~ 4) **참고**: 각각의 포트에 가중치를 지정하려면, trunk-active-backup 명령을 여러 번 반복해서 실행합니다. 가중치를 설정하지 않는 경우, 가중치가 '0'으로 설정되며 가장 낮은 우선순위를 갖습니다.

참고: 포트 Failover 그룹을 삭제하려면 <Configuration 모드>에서 **no trunk-active-backup** *<CHANNEL-GROUP>* 명령을 실행합니다.

그룹 포트의 설정 정보 보기

설정한 그룹 포트의 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show trunk-active-backup** 명령을 실행합니다.

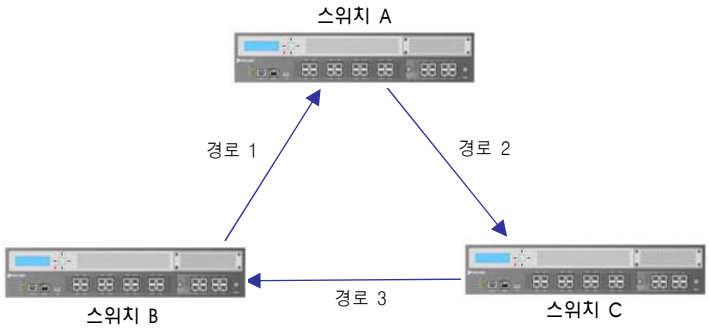
참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

STP/RSTP/PVSTP/MSTP 설정

STP(Spanning Tree Protocol) 개요

스위치로 연결되어 있는 네트워크의 문제는 임의의 두 노드 사이에 원칙적으로는 하나의 경로만 존재해야 한다는 것입니다. 만약 두 노드 간에 두 개 이상의 경로가 존재한다면, 패킷은 이중으로 전달되거나 네트워크 상에서 영원히 순환하는 '루프(Loop)'가 만들어지는 문제가 발생하게 됩니다. 루프는 네트워크 트래픽을 폭주하게 하여 네트워크를 불안정하게 만드는 요인이 됩니다.

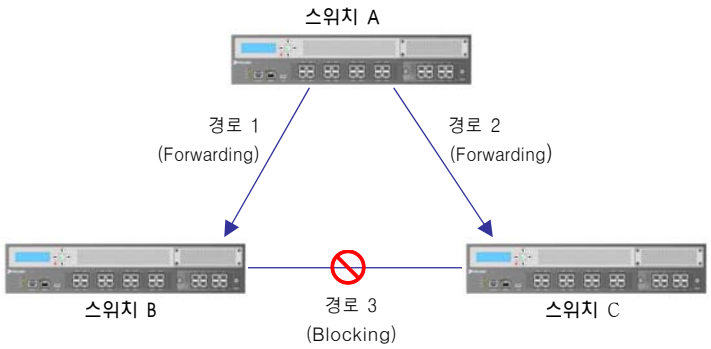
아래와 같은 네트워크는 스위치 A에서 스위치 C까지 도달할 수 있는 2개의 경로가 존재하는데, 직접 연결된 경로 2와 스위치 B를 경유하여 경로 1과 경로 3을 통해 가는 경로입니다. 이와 같이 한 목적지에 대해 2개 이상의 경로가 존재하는 네트워크는 루프가 만들어집니다. 예를 들어, 아래의 그림에서 스위치 A가 패킷을 브로드캐스트하게 되면, 스위치 C는 경로 2를 통해 수신한 패킷을 스위치 B로 브로드캐스트하고, 스위치는 B는 경로 3을 통해 수신한 패킷을 경로 1을 통해 스위치 A로 전송하여 루프가 생성됩니다. 반대로 스위치 A→B-C-A의 루프도 생성됩니다.



[그림 - 루프가 만들어지는 네트워크 구조]

STP(Spanning Tree Protocol)는 목적지에 대한 경로가 2개 이상일 때 발생하는 루핑 현상을 방지하기 위해 사용하는 프로토콜로 IEEE 802.1D 표준 안에 명시되어 있습니다. 스패닝 트리에서는 하나의 노드에 둘 이상의 경로가 존재하는 경우 우선순위 등을 고려하여 최적의 경로를 선택하여 스패닝 트리에 포함시킵니다. 그리고, 그 경로를 제외한 나머지 경로를 blocking 상태(프레임을 전송하지 않는 상태)로 처리하여 스패닝 트리에서 제외합니다. 그리하여 트래픽을 처리할 때에는 blocking 상태가 아닌 최적의 경로를 통해서만 패킷이 전송되도록 합니다.

앞서 살펴본 네트워크에서 경로 3을 blocking 상태로 만들면, 스위치 A에서 스위치 C까지의 경로가 오직 하나(경로 2)만 존재하므로 루핑 현상을 방지할 수 있습니다.

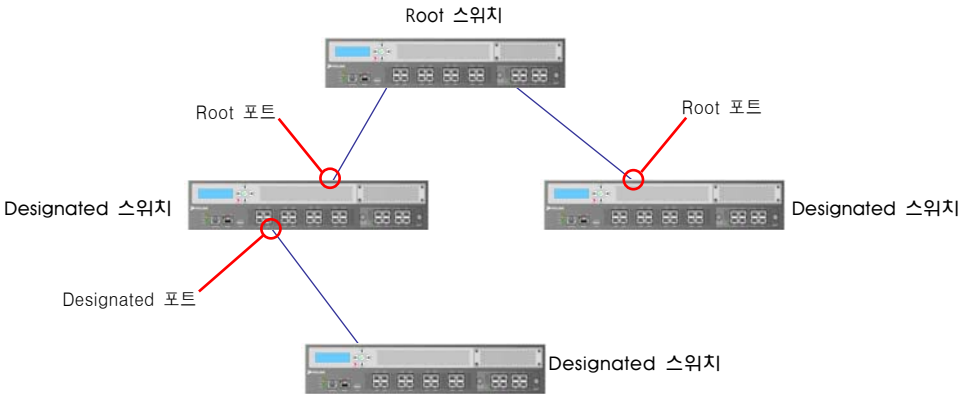


[그림 - 루프를 방지한 네트워크 구조]

단일 경로만 존재하는 STP에서 연결된 경로에 문제가 발생하면, blocking 상태에 있던 경로를 forwarding 상태(트래픽을 전송하는 상태)로 변경하여 네트워크의 가용성을 높이게 됩니다.

BPDU(Bridge Protocol Data Unit)

스패닝 트리는 Root 스위치, designated 스위치, Root 포트, designated 포트 등으로 구성됩니다. Root 스위치는 글자 그대로 스패닝 트리의 루트가 되는 스위치로, Root 스위치를 기준으로 하여 스패닝 트리가 만들어집니다. Designated 스위치는 각 LAN 세그먼트에서 Root 스위치로 패킷을 포워딩할 때 사용되는 스위치입니다. Root 포트는 designated 스위치에서 Root 스위치로 패킷 포워딩 시 사용되는 포트입니다. Designated 포트는 designated 스위치의 포트 중에서 하위의 LAN에 직접 연결되는 포트 입니다.



[그림 - STP 구성 요소]

앞의 그림과 같이 스패닝 트리에 참여하는 스위치와 포트를 결정하기 위해, 각 스위치는 BPDU를 교환합니다. BPDU란 STP/RSTP/MSTP를 설정하고, 유지하기 위해서 LAN에 사용되는 전송 메시지로, 스위치 간 정보교환을 위해 전송되는 프레임 데이터입니다. BPDU에는 다음과 같은 정보가 포함되어 있습니다.

- BPDU를 전송하는 스위치가 루트 스위치로 알고 있는 스위치의 브리지 ID
- 루트 스위치까지의 경로 비용
- BPDU를 전송하는 스위치의 브리지 ID
- BPDU의 aging 시간
- BPDU를 전송하는 인터페이스의 ID
- 스패닝 트리 타이머 값들(hello, forward delay, max-age)

브리지 ID는 스패닝 트리에서 중심이 되는 스위치인 root 스위치를 선출할 때 사용되는 값입니다. 브리지 ID는 스위치의 우선순위(상위 2byte)와 MAC 주소로 구성되어 있는데, 가장 높은 우선순위를 가진 스위치가 root 스위치로 선출됩니다. 우선순위 값이 낮을수록 우선순위는 높습니다. 만약 모든 스위치의 우선순위가 동일한 경우에는 MAC 주소를 비교하여 가장 낮은 MAC 주소를 가진 스위치를 root 스위치로 선택합니다.

경로 비용은 root 포트와 designated 스위치를 선택할 때 사용되는 값입니다. 스위치가 root 스위치로 패킷을 전송할 때 가장 좋은 경로(비용이 가장 적은)를 제공하는 포트, 즉, root 스위치까지의 경로 비용이 가장 적은 포트가 root 포트가 됩니다. 그리고, LAN에서 루트 스위치까지 패킷을 포워딩할 때 경로 비용이 가장 낮은 스위치가 designated 스위치가 됩니다. Designated 스위치의 포트 중에서 LAN에 직접 연결되는 포트가 designated 포트가 됩니다. Root 포트와 Designated 포트를 제외한 통신이 이루어지지 않는 포트는 Blocked 포트라고 합니다. 한편, 경로 비용이 동일한 경우에는 브리지 ID를 사용하여 브리지 ID의 우선순위가 낮은 스위치가 Designated 스위치로 선택됩니다.

BPDU에는 3개의 타이머 값(hello, forward delay, max age)이 포함됩니다. 이 타이머들은 전체 스패닝 트리의 성능에 영향을 미치는 타이머들로 다음과 같은 기능을 수행합니다.

[표 - STP 타이머]

타이머	설명
Hello timer	root 스위치의 BPDU 메시지 전송 주기. root 스위치가 얼마나 자주 BPDU 메시지를 다른 스위치로 브로드캐스트할 지 결정하는 타이머 값입니다. (기본값: 2초)
Forward delay timer	Listening 상태와 learning 상태를 얼마나 오랫동안 유지할 지 결정하는 타이머 값. Listening 상태에서 forward delay 시간이 경과되면 learning 상태로 넘어가고, 다시 learning 상태에서 forward delay 시간이 경과하면 forwarding 상태가 됩니다. 이 타이머는 변경된 토폴로지 정보가 스패닝 트리에 충분히 전파되기 전에 포트가 forwarding 상태로 되어서 루프가 만들어지는 현상을 방지해줍니다. (기본값: 15초)
Max age timer	BPDU의 Aging 시간(유효 시간). 스위치가 수신한 프로토콜 정보(BPDU)를 얼마나 오랫동안 저장할 것인지 결정하는 타이머 값. Max age 타이머의 시간이 지나면 BPDU를 폐기합니다. (기본값: 2초)

BPDU 는 Message Type에 따라 Configuration BPDU와 TCN(Topology Change Notification) BPDU로 구분되며, 다음과 같은 기능을 수행합니다.

[표 – BPDU 타입]

타입	설명
Configuration BPDU	root 스위치가 되지 못한 스위치들이 root 스위치로부터 전달된 BPDU를 기반으로 해서 STP cost 값을 기준으로 BPDU를 재생산하는 일련의 과정을 수행하는 방식
TCN(Topology Change Notification) BPDU	네트워크 토폴로지의 변경을 탐지하여 root 스위치에게 장애가 발생했음을 알리는 일련의 과정을 수행하는 방식

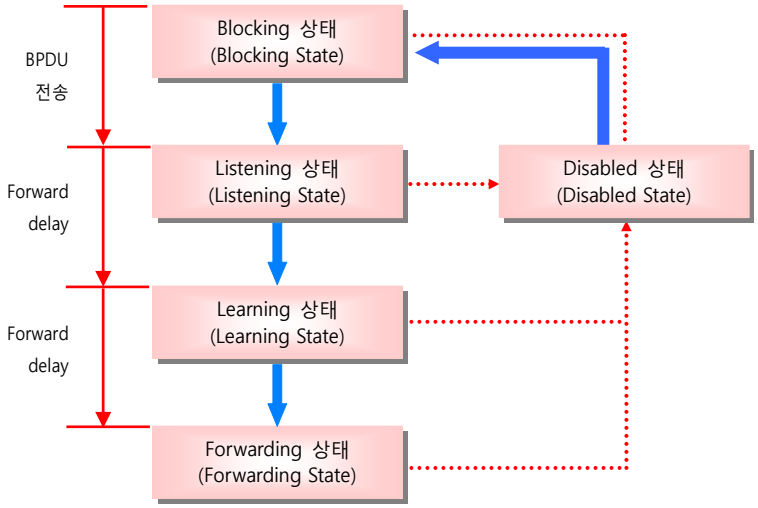
네트워크 토폴로지의 변경으로 학습된 MAC 테이블에 의해 프레임을 전송하지 못할 경우 통신이 단절되는 문제가 발생하면 root 스위치가 TCN BPDU를 전달받아 토폴로지의 변경으로 장애가 발생했음을 인지하게 되면, root 스위치는 BPDU를 재생산해서 다른 스위치들에게 토폴로지 변경을 알려 BPDU 재생산을 요청하는 Configuration BPDU를 전달합니다.

포트의 상태

STP는 네트워크 상의 포트를 다음 5가지 상태로 설정합니다.

- Blocking 상태 - 프레임을 전송하지 않는 상태. STP가 동작하는 포트의 기본 상태.
- Listening 상태 - Blocking 상태에서 forwarding 상태로 가기 전 처음으로 거치는 상태.
- Learning 상태 - 프레임 전송을 준비하는 단계의 상태.
- Forwarding 상태 - 트래픽을 전송하는 상태.
- Disabled 상태 - STP가 비 활성되었거나, 프레임 전송이 불가능한 상태.

포트가 이러한 5가지 포트 상태를 거치는 과정을 그림으로 나타내면 다음과 같습니다.



[그림 - STP가 동작하는 포트의 상태 변화]

STP가 동작하는 포트는 항상 blocking 상태에서 시작하게 됩니다. STP가 동작하도록 설정된 스위치는 초기화될 때 자신이 루트 스위치라고 가정하고 모든 포트를 통해 연결된 장비로 BPDU를 전송합니다. Blocking 상태의 포트는 BPDU를 제외한 모든 프레임을 폐기합니다. BPDU를 수신한 포트는 listening 상태가 됩니다.

Listening 상태의 포트는 다른 장비와 BPDU를 교환하여 루트 스위치를 결정하는 등의 작업을 수행합니다. 그리고 forward delay의 시간이 경과한 후 learning 상태로 전이합니다.

Learning 상태의 포트는 프레임을 전송하기 위해 MAC 주소를 학습합니다. 그리고, forward delay의 시간이 지나면 forwarding 상태가 됩니다. 포트가 forwarding 상태가 되기 전까지 수신된 프레임은 모두 폐기되고, forwarding 상태가 된 이 후부터는 수신된 프레임이 포트를 통해 전송됩니다.

Disabled 상태의 포트는 스패닝 트리에 참여하지 않는 포트로, 포트가 동작하지 않거나 링크가 연결되어 있지 않거나 혹은 STP가 동작하지 않는 포트입니다. 이 상태의 포트는 BPDU를 전송하거나 수신하지도 않고, 프레임을 전송하지도 않습니다.

경로 선택하기

STP는 경로를 선택할 때, 즉, 어떤 스위치를 통해서 패킷을 전송할 지 결정할 때, 스패닝 트리 알고리즘을 사용합니다. 스패닝 트리 알고리즘은 실제 토폴로지 상에서의 포트 역할을 기준으로 하여 네트워크를 통해 루프가 만들어지지 않는 가장 좋은 경로를 계산합니다.

스위치에 2개의 인터페이스가 루프를 형성하게 되는 경우에는 포트의 우선순위와 경로 비용에 따라 어떤 인터페이스를 forwarding 상태로 하고 나머지 인터페이스를 blocking 상태로 할지를 결정하게 됩니다. 포트 우선순위는 주로 네트워크 상에서 인터페이스의 위치를 나타내고 (트래픽 전송에 얼마나 용이한 위치에 있는지), 경로 비용은 인터페이스의 물리적인 속도(media speed)를 나타냅니다.

스패닝 트리는 사용하지 않는 여분의 경로를 대기 상태, 즉 blocking 상태로 설정합니다. 스패닝 트리의 특정 네트워크 세그먼트가 동작하지 않을 때(링크가 끊어지거나) 다른 여분의 경로가 있는 경우, 스패닝 트리 알고리즘은 스패닝 트리 토폴리지를 다시 계산하여 대기 상태인 여분의 경로를 forwarding 상태로 변경합니다.

RSTP(Rapid Spanning Tree Protocol) 개요

STP가 활성화 되어 네트워크에 BPDU가 전송되는 동안, 네트워크의 다른 곳에서는 토폴로지가 계속 변경됩니다. 이렇게 자주 변경되는 토폴로지를 스패닝 트리에 적용(convergence)하는 데까지는 많은 시간이 소요됩니다. IEEE 802.1w 표준안에 정의되어 있는 RSTP(Rapid Spanning-Tree Protocol)는 기존의 STP의 단점을 보완하여 보다 빠른 convergence가 이루어질 수 있게 해주는 프로토콜입니다.

RSTP(802.1w)는 STP(802.1D)에서 사용한 전문적인 용어와 대부분의 설정 파라미터를 그대로 사용하기 때문에 새로운 프로토콜을 쉽고 빠르게 설정할 수 있을 뿐만 아니라, RSTP(802.1w)는 STP(802.1D)를 내부적으로 포함하고 있어 호환이 가능합니다.

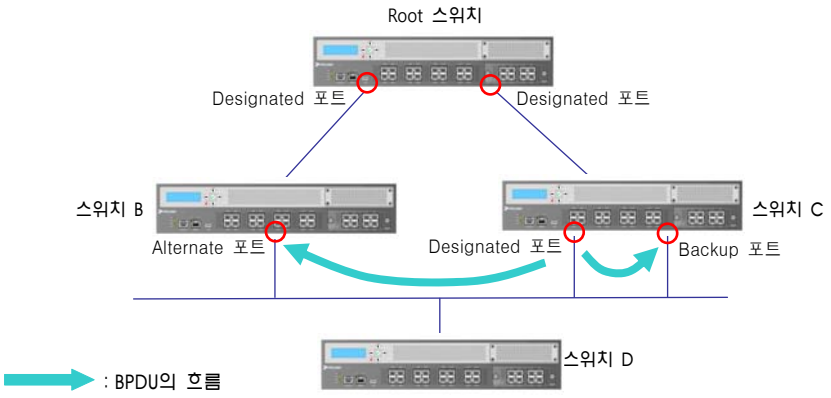
STP와 RSTP의 가장 큰 차이는 포트가 거쳐가는 상태입니다. STP는 Blocking->Listening->Learning을 모두 거친 후 비로소 트래픽을 전송할 수 있는 forwarding 상태가 됩니다. 반면, RSTP는 Blocking 상태에서 바로 forwarding 상태로 변환됩니다. 이와 같은 방법으로 RSTP는 토폴로지의 변경을 즉각 스패닝 트리에 적용시킬 수 있습니다.

포트의 상태

RSTP 802.1w는 포트 상태를 Discarding, Learning, Forwarding의 세 가지로 정의합니다. Learning, Forwarding 상태는 STP와 동일하고, Discarding 상태는 STP의 Disabled, Blocking, Listening 상태를 모두 포함합니다.

RSTP는 Root 포트와 Designated 포트를 forwarding 상태로 설정하고, Alternate 포트와 Backup 포트를 discarding 상태로 설정합니다. Alternate 포트는 다른 장비로부터 우선순위가 높은 BPDU를 받음으로써 Blocked 된 포트를 의미하고, Backup 포트는 같은 장비의 다른 포트로부터 우선순위가 높은 BPDU를 받음으로써 Blocked된 포트를 의미합니다. BPDU 전송은 루트 포트와 Designated 포트에서만 이루어집니다.

아래의 그림은 Alternate 포트와 Backup 포트를 설명한 것입니다.



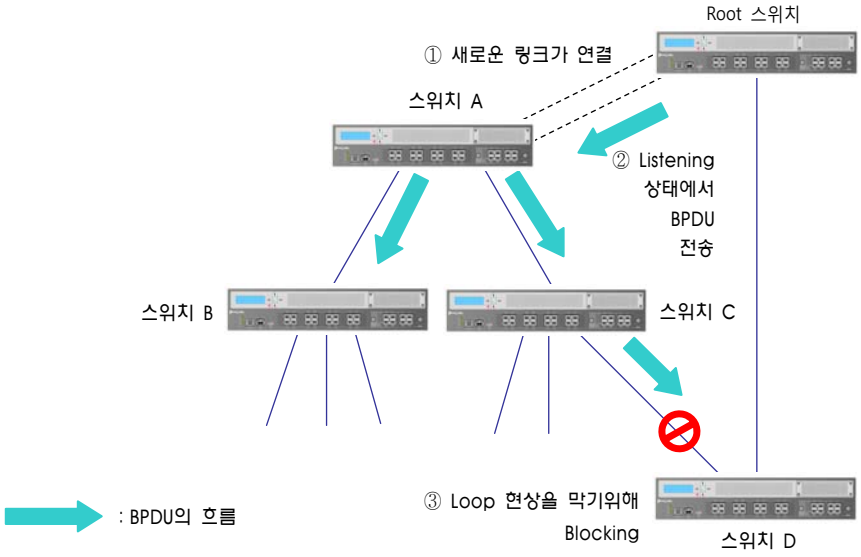
[그림 - Alternate 포트와 Backup 포트]

BPDU 정책 변화

STP는 루트 스위치만 설정된 Hello time에 따라 BPDU를 전송하고, 루트 스위치를 제외한 다른 스위치는 루트 스위치로부터 BPDU를 받았을 때에만 자신의 BPDU를 전송합니다. 그러나 RSTP는 루트 스위치가 아닌 모든 스위치가 Hello time에 따라 BPDU를 전송합니다. BPDU는 실제로 루트 스위치에 의해 주고받는 시간 간격보다 더 자주 변화하는데 RSTP 기능을 사용하면 변화하는 네트워크 환경에 더욱 빨리 대응할 수 있습니다.

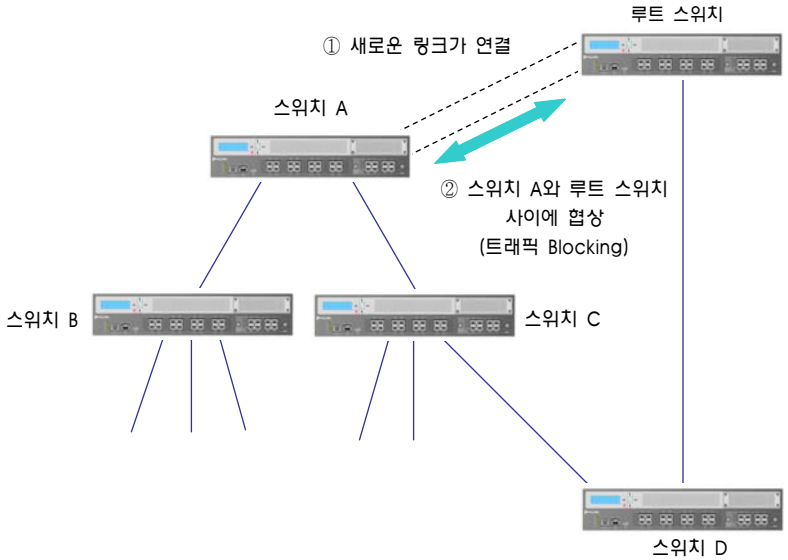
네트워크 Convergence 시간 단축

STP의 경우 링크 토폴로지에 변화가 발생했을 때, 아래와 같은 방법으로 Convergence 가 이루어집니다. 아래의 그림과 같이 스위치 A와 루트 스위치 사이에 새로운 링크가 연결되었다고 가정합니다. 루트 스위치와 스위치 A는 직접 연결되어 있는 것은 아니지만, 스위치 D를 통해 간접적으로 연결되어 있는 상태입니다. 스위치 A와 루트 스위치가 새롭게 연결되면 두 스위치는 일단 Listening 상태가 되기 때문에 포트 간에 패킷은 주고 받을 수 없고, 따라서 루프도 발생하지 않습니다. 이 상태에서 루트 스위치가 스위치 A로 BPDU를 전송하면, 스위치 A는 스위치 B와 스위치 C로 새로운 BPDU를 전송하고, 스위치 C도 스위치 D에 새로운 BPDU를 전송하게 됩니다. 스위치 C로부터 BPDU를 전달받은 스위치 D는 새로운 링크 연결에 따라 루프가 발생하는 것을 막기 위해 스위치 C와 연결된 포트를 Blocking 상태로 만듭니다.



[그림 - STP의 네트워크 Convergence]

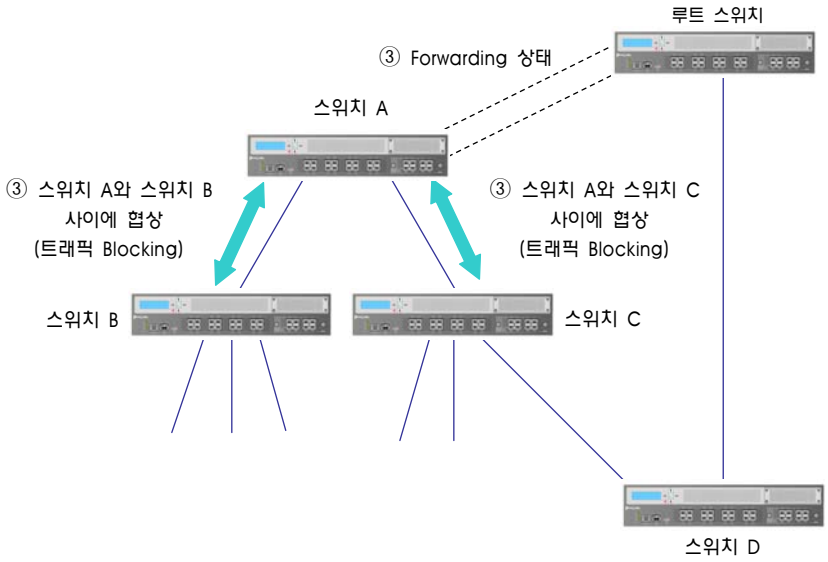
이러한 방법으로 루프 현상을 막는 것은 매우 획기적인 방법이지만, 스위치 D가 스위치 C와 연결된 포트를 막기까지 BPDU의 Forward-delay 시간을 두 번 거치는 동안에 통신이 단절된다는 문제가 있습니다. 그러나, RSTP 기능은 통신이 단절되는 시간을 단축하기 위해 다음과 같은 과정을 거칩니다. 스위치 A와 루트 스위치 사이에 새로운 링크가 연결됩니다. 그러면, 연결되자 마자 스위치 A와 루트 스위치 사이는 패킷을 주고받을 수 없지만, BPDU는 전송할 수 있는 상태가 됩니다.



[그림 - RSTP의 네트워크 Convergence ①]

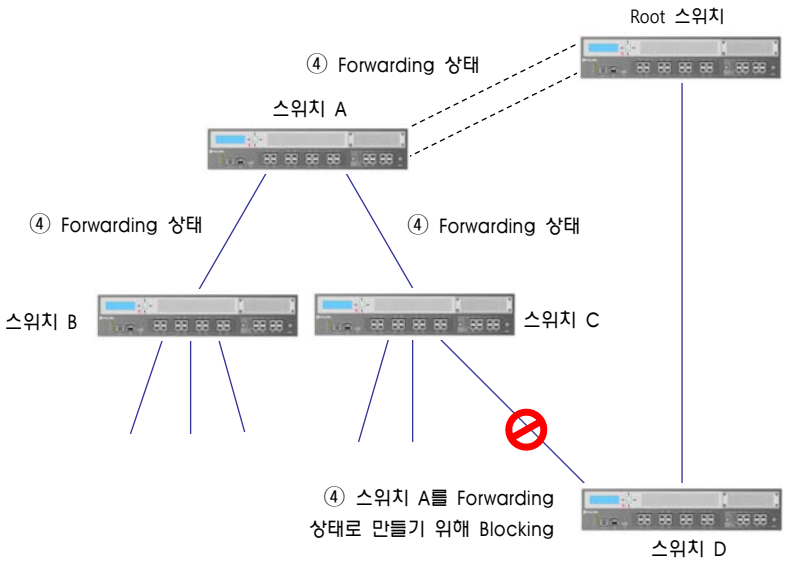
BPDU를 통해 Root와 스위치 A는 협상이 이루어지고 루트 스위치와 스위치 A 사이의 링크를 Forwarding 상태로 만들기 위해 스위치 A의 non-edge designate 포트를 Blocking 상태로 변경합니다. 스위치 A와 루트 스위치가 연결되었지만, 스위치 A와 스위치 B, C의 연결을 막았기 때문에 Loop는 발생하지 않습니다.

이 상태에서 다음 그림과 같이 루트 스위치의 BPDU는 스위치 A를 통해 스위치 B와 스위치 C로 전송됩니다. 스위치 A를 Forwarding 상태로 만들기 위해 다시 스위치 A와 스위치 B, 스위치 A와 스위치 C 간에 협상이 이루어지게 됩니다.



[그림 - RSTP의 네트워크 Convergence ②]

스위치 B는 edge designated 포트만 가지고 있습니다. edge designated 포트는 루프를 발생시키지 않기 때문에 RSTP에서는 Forwarding 상태로 변환할 수 있도록 정의하고 있습니다. 따라서, 스위치 B는 스위치 A를 Forwarding 상태로 만들기 위해 특별히 Blocking 할 포트가 없습니다. 그러나, 스위치 C는 스위치 D와 연결된 포트가 있기 때문에 스위치 A를 Forwarding 상태로 변환시키려면 해당 포트를 Blocking 상태로 만들어야 합니다.



[그림 - RSTP의 네트워크 Convergence ③]

결과적으로 스위치 D와 스위치 C의 연결을 Blocking 하는 것은 STP와 동일합니다. 그러나, RSTP는 특정 포트를 Forwarding 상태로 만들기 위해 장비 간에 이루어지는 협상에 사용자가 설정해 놓은 어떤 시간 기준(Hello Time, Forward Delay Time, Maximun Aging Time)도 사용되지 않을 뿐만 아니라, 포트가 Forwarding 상태로 진행되는 과정에서 Listening과 Learning 과정이 필요하지 않기 때문에 네트워크 Convergence 시간을 획기적으로 단축시킬 수 있습니다.

PVSTP/MSTP(Per VLAN Spanning Tree Protocol/Multiple Spanning Tree Protocol) 개요

PAS-K는 효율적으로 망을 운용하기 위하여 기존의 LAN 도메인을 논리적으로 세분화 한 VLAN 개념을 도입하여 망을 구성하고, VLAN 별 또는 VLAN 그룹 별로 STP를 설정할 수 있는 PVSTP(Per VLAN Spanning Tree Protocol)와 MSTP(Multiple Spanning Tree Protocol)를 지원합니다.

기존의 STP가 하나의 LAN 도메인에서 루프를 방지하기 위해 사용된 프로토콜이라면 PVSTP는 VLAN 환경에 맞는 경로 설정을 위해 VLAN별로 STP를 구성하도록 보완된 프로토콜입니다.

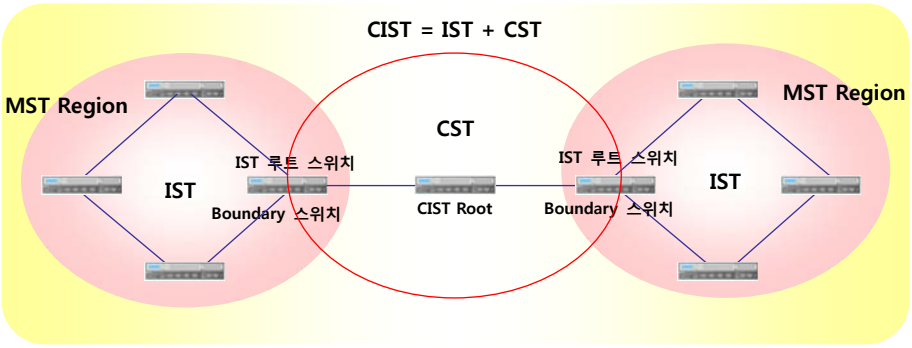
PVSTP에서는 각 instance마다 VLAN을 하나씩만 지정할 수 있고, 각 instance마다 STP가 하나씩 동작합니다. 만약 네트워크에 VLAN ID가 각각 10, 20, 30, 40, 50, 60인 6개의 VLAN이 있다면, VLAN 별로 STP가 하나씩 동작하는 것이기 때문에 총 6개의 STP가 동작합니다.

적은 수의 VLAN이 있는 경우에는 문제가 없지만, 예를 들어 200개의 VLAN이 있는 네트워크에 PVSTP를 적용하면 200개의 STP가 동작하므로 이를 처리하기 위해 장비에 부하가 발생하게 됩니다. 이러한 단점을 보완하기 위한 것이 IEEE 802.1s 표준인 MSTP입니다.

MSTP는 RSTP와 같은 고속 Convergence를 사용합니다. MSTP는 하나의 instance에 여러 개의 VLAN을 할당할 수 있으며, 각 instance별로 하나의 STP가 구동되므로 PVSTP에 비해 STP의 수를 줄일 수 있습니다. MSTP의 instance는 다시 Region으로 통합할 수 있습니다. 하나의 네트워크 환경에서 설정할 수 있는 Region 수는 제한이 없으며, 하나의 Region에는 최대 64개의 instance를 설정할 수 있습니다.

MSTP에서 사용되는 Region은 MST Region이라고 불리며 동일한 Configuration ID를 가진 그룹으로 VLAN을 나눕니다. Configuration ID는 Revision name, Revision, VLAN map으로 구성됩니다. 따라서 Configuration ID가 동일하기 위해서는 이 세 가지가 모두 동일해야 합니다.

각 Region에서 동작하는 스패닝 트리를 IST(Internal Spanning-Tree)라고 하고, 각 Region의 스패닝 트리를 모두 연계했을 때 적용되는 스패닝 트리를 CST(Common Spanning-Tree)라고 합니다. 그리고 이 IST와 CST를 합쳐서 CIST(Common & Internal Spanning-Tree)라고 합니다. 다음은 IST, CST, CIST의 관계를 나타낸 그림입니다.

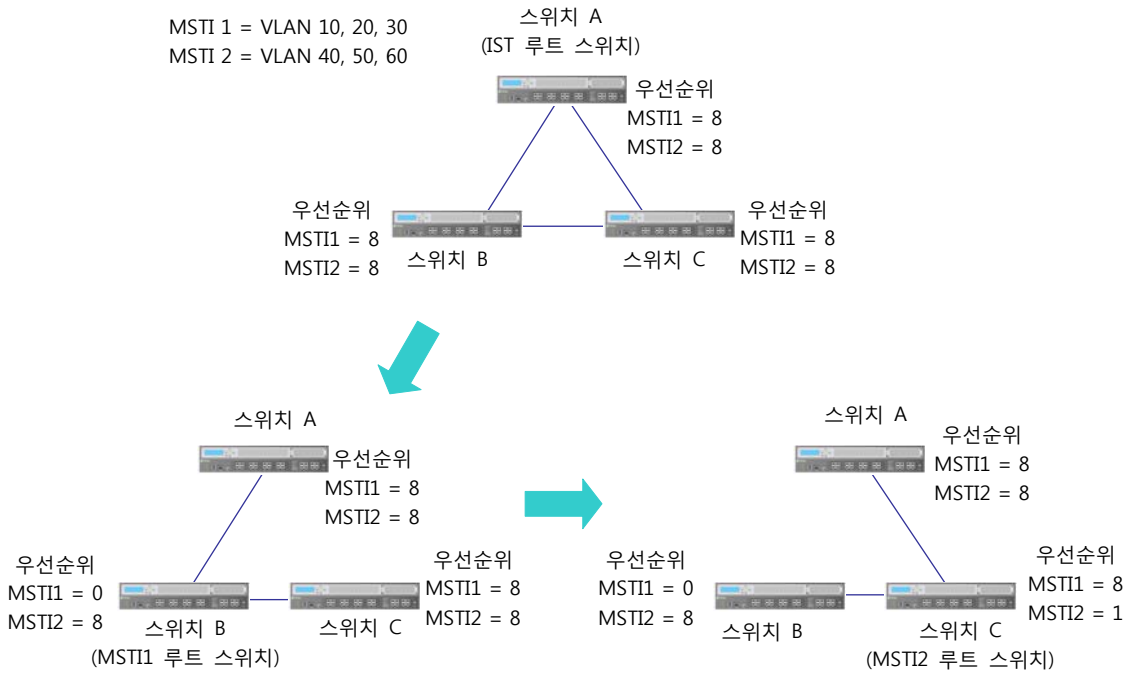


[그림 – IST, CST, ICST의 관계]

MST Region에는 IST instance와 MSTI(Mutiple Spanning Tree Instance)가 동작합니다. IST instance는 MST Region에 기본적으로 할당되어 있는 스패닝 트리 instance이며, ID 값 0번이 할당되어 있어, MSTI0라고도 불립니다. 하나의 MST Region에 추가로 할당된 instance를 MSTI라고 부르며, 이 instance에는 적어도 하나 이상의 VLAN이 포함되어야 합니다.

MST Region 내부의 스패닝 트리는 RSTP와 동일한 방식으로 동작합니다. 다음 그림과 같이 VLAN ID가 각각 10, 20, 30, 40, 50, 60인 6개의 VLAN이 있고, MSTI 1에 VLAN 10, 20, 30이 할당되어 있고, MSTI 2에 VLAN 40, 50, 60이 할당되어 있는 경우, MST Region 내부의 스패닝 트리는 다음과 같이 동작합니다.

먼저 브리지 ID가 가장 낮은 스위치가 IST 루트 스위치로 결정됩니다. MSTI는 우선순위를 조정하지 않으면, 기본적으로 IST 루트 스위치와 동일하게 동작합니다. 하지만 다음 그림과 같이 각각의 스위치에서 MSTI의 우선순위를 조정하면 각 MSTI별로 다르게 동작하도록 조정할 수 있습니다.

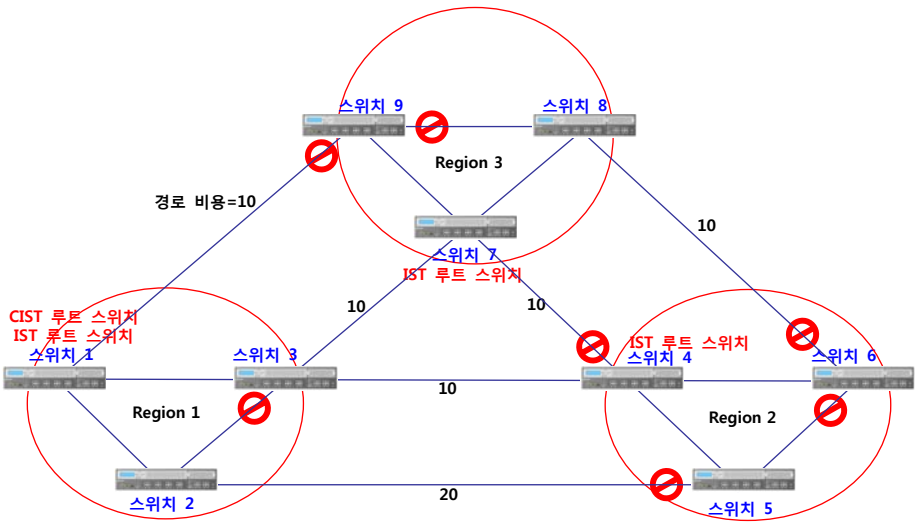


[그림 – MST Region에서의 스패닝 트리 동작]

CIST 영역에는 CIST 루트 스위치가 하나 존재하고, 각 MST Region별로 IST 루트 스위치가 하나 존재합니다. 모든 스위치 중에서 가장 낮은 브리지 ID 값을 갖는 스위치가 CIST 루트 스위치로 선정되며, 각 MST Region에서 CIST 루트 스위치로 가는 경로 비용이 가장 낮은 Boundary 스위치가 IST 루트 스위치로 선정됩니다. Boundary 스위치는 MST Region 외부의 다른 영역으로부터 BPDU를 전송받는 스위치를 말하며, 해당 BPDU를 전송받를 포트는 Boundary 포트라고 합니다.

CIST 루트 스위치를 포함하는 MST Region의 모든 Boundary 포트는 Designated 포트로 선정되며, 모두 Forwarding 상태가 됩니다. CIST 루트 스위치를 포함하는 MST Region의 IST 루트 스위치는 CIST 루트 스위치와 동일합니다.

IST 루트 스위치로 선정된 Boundary 스위치는 Boundary 포트 중 하나를 루트 포트로 선정하고, 나머지 Boundary 포트를 Blocking 상태로 변경합니다. 그리고 IST 루트가 아닌 스위치의 Boundary 포트는 Designated 포트 또는 Alternate 포트로 선정됩니다.



[그림 – CIST 루트 스위치 선정과 포트의 Blocking]

경로 비용이 위 그림과 같고, 스위치 1이 가장 낮은 브리지 ID를 가지고 있고, 2, 3, 4... 순서로 뒤에 붙는 숫자가 작을수록 낮은 브리지 ID를 갖고 있다면, 루트 스위치 선정과 포트의 상태 변화 과정은 다음과 같습니다.

1. 스위치 1이 CIST와 MST Region 1의 루트 스위치로 선정되고, MST Region 1의 모든 Boundary 포트가 Forwarding 상태가 됩니다.
2. 각 MST Region에서 가장 낮은 BID를 갖는 스위치 4와 스위치 7이 각각 MST Region 2와 MST Region 3의 IST 루트 스위치로 선정됩니다. 각 MST Region에서 IST 루트 스위치가 선정되면 MST Region 내부의 포트는 STP의 경우와 동일하게 가장 높은 브리지 ID를 갖는 스위치의 Non-designated 포트가 Blocking 상태가 됩니다.
3. 마지막으로 IST 루트 스위치의 Boundary 포트 중 CIST 루트 스위치와 연결되는 경로 비용이 가장 작은 포트가 루트 포트로 지정되고, 나머지 포트들은 전부 Blocking 상태로 변경됩니다.

CLI에서 설정하기

이 절에서는 CLI에서 STP와 RSTP, PVSTP, MSTP를 설정하는 방법에 대해 살펴봅니다.

참고: STP/RSTP/PVSTP/MSTP 기능을 설정하는 과정에서 포트를 지정하는 경우에는 LinK Aggregation 기능에의해 설정된 트렁크 그룹 또는 통합 포트를 사용할 수 있습니다.

STP/RSTP/PVSTP/MSTP 활성화/비활성화

STP/RSTP/PVSTP/MSTP의 상태를 변경하려면 <Configuration 모드>에서 다음 명령을 실행합니다. 기본적으로 모두 비활성화되어 있습니다.

명 령	설 명
stp status {enable | disable}	STP 기능의 사용 여부를 지정합니다. • **enable** STP 기능 활성화 • **disable** STP 기능 비활성화 (기본값)
rstp status {enable | disable}	RSTP 기능의 사용 여부를 지정합니다. • **enable** RSTP 기능 활성화 • **disable** RSTP 기능 비활성화 (기본값)
pvstp status {enable | disable}	PVSTP 기능의 사용 여부를 지정합니다. • **enable** PVSTP 기능의 활성화 • **disable** PVSTP 기능의 비활성화 (기본값)
mstp status {enable | disable}	MSTP 기능의 사용 여부를 지정합니다. • **enable** MSTP 기능 활성화 • **disable** MSTP 기능 비활성화 (기본값)

주의: 하나의 장비에 STP와 RSTP, PVSTP, MSTP를 동시에 사용할 수 없습니다. 다른 기능을 사용하기 위해서는 동작 중인 기능을 비활성화해야 합니다.

우선순위 설정

STP/RSTP/PVSTP/MSTP 기능을 실행시키기 위해서는 우선, 루트 스위치가 정해져야 합니다. STP/RSTP에서는 루트 스위치가 되고 MSTP에서는 IST 루트 스위치가 됩니다. 브리지 ID는 스패닝 트리의 루트 스위치를 선출할 때 사용되는 우선순위 값입니다. 사용자는 해당 장비의 우선순위를 높여서(우선순위 값을 작은 값으로 설정할수록 우선순위가 높아집니다.) 루트 스위치가 되도록 설정할 수 있습니다. 이러한 활동은 스패닝 트리가 토폴로지를 재계산하도록 하며, 우선순위가 높은 장비를 루트 스위치로 만듭니다. 우선순위를 설정하기 위해 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
stp priority *<PRIORITY>*	루트 스위치 선정을 위한 우선순위를 설정합니다. • *<PRIORITY>* 우선순위. 설정 범위: 0 ~ 15, 기본값: 8
rstp priority *<PRIORITY>*	
pvstp priority *<PRIORITY>*	
mstp priority *<PRIORITY>*	

참고: 설정한 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no stp priority
(config)# no rstp priority
(config)# no pvstp priority
(config)# no mstp priority
```

경로 비용 설정

경로 비용 설정에 의해 사용자는 프레임을 전달하는데 사용하는 루트 브리지로 가는 가장 짧은 거리를 보장합니다. 프레임 전달을 위해 가장 적은 비용을 가지는 경로가 선택됩니다. 일반적으로 높은 대역폭의 포트에는 낮은 비용을 설정하고, 낮은 대역폭의 포트에는 높은 비용을 설정합니다. 설정 가능한 비용 범위는 1 ~ 200000000 사이이며, 포트의 종류에 따라 다음과 같은 기본 비용이 설정되어 있습니다.

[표 - 포트 속도에 따른 기본 경로 비용]

속도	기본 경로 비용
10 Mbps	2000000
100 Mbps	200000
1 Gbps, 10 Gbps	20000

포트에 대한 경로 비용을 설정하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
stp port *<NAME>* **path-cost** *<PATH-COST>*	포트에 대한 경로 비용을 설정합니다. • *<PATH-COST>* 포트의 경로 비용. 설정 범위: 1 ~ 200000000
rstp port *<NAME>* **path-cost** *<PATH-COST>*	
pvstp port *<NAME>* **path-cost** *<PATH-COST>*	
mstp port *<NAME>* **path-cost** *<PATH-COST>*	

참고: 설정한 경로 비용을 기본값으로 변경하려면 <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no stp port <NAME> path-cost
(config)# no rstp port <NAME> path-cost
(config)# no pvstp port <NAME> path-cost
(config)# no mstp port <NAME> path-cost
```

포트 우선순위 설정

가장 낮은 우선순위 값을 가지는 포트는 모든 VLAN에 대해 프레임을 포워딩합니다. 포트의 우선순위를 변경하려면 <Configuration> 모드에서 다음과 같은 명령을 사용합니다.

명 령	설 명
stp port *<NAME>* **priority** *<PRIORITY>*	포트의 우선순위를 설정합니다. • *<PRIORITY>* 포트 우선순위. 설정 범위: 0 ~ 15, 기본값: 8
rstp port *<NAME>* **priority** *<PRIORITY>*	
pvstp port *<NAME>* **priority** *<PRIORITY>*	
mstp port *<NAME>* **priority** *<PRIORITY>*	

참고: 설정한 포트 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no stp port <NAME> priority
(config)# no rstp port <NAME> priority
(config)# no pvstp port <NAME> priority
(config)# no mstp port <NAME> priority
```

Hello Time 설정

사용자는 PAS-K가 다른 PAS-K로 hello 메시지를 얼마나 자주 브로드캐스트할 지 설정할 수 있습니다. PAS-K의 스패닝 트리 hello time(hello 메시지를 보내는 간격)을 변경하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
stp bridge-hello-time *<BRIDGE-HELLO-TIME>* **rstp bridge-hello-time** *<BRIDGE-HELLO-TIME>* **pvstp bridge-hello-time** *<BRIDGE-HELLO-TIME>* **mstp bridge-hello-time** *<BRIDGE-HELLO-TIME>*	Hello time 을 설정합니다. • *<BRIDGE-HELLO-TIME>* hello message 전송 간격. 설정 범위: 1 ~ 10(초), 기본값: 2(초)

참고: 설정한 hello time을 기본값으로 변경하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no stp bridge-hello-time
(config)# no rstp bridge-hello-time
(config)# no pvstp bridge-hello-time
(config)# no mstp bridge-hello-time
```

Forward Delay Time 설정

Forward delay time은 STP가 동작하는 포트의 상태 변화 시간입니다. 예를 들어, forward delay time이 10초 일 경우, 해당 포트는 상태가 변경되는데 10초가 걸립니다. Forward delay time을 변경하라면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
stp bridge-forward-delay *<BRIDGE-FORWARD-DELAY>* **rstp bridge-forward-delay** *<BRIDGE-FORWARD-DELAY>* **pvstp bridge-forward-delay** *<BRIDGE-FORWARD-DELAY>* **mstp bridge-forward-delay** *<BRIDGE-FORWARD-DELAY>*	Forward delay time 을 설정합니다. • *<BRIDGE-FORWARD-DELAY>* Forward delay time. 설정 범위: 4 ~ 30(초), 기본값: 15(초)

참고: 설정한 forward delay time을 기본값으로 변경하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no stp bridge-forward-delay
(config)# no rstp bridge-forward-delay
(config)# no pvstp bridge-bridge-forward-delay
(config)# no mstp bridge-forward-delay
```

Maximum Aging Time 설정

Maximum aging time은 수신한 BPDU 패킷의 age time(유효 시간)입니다. 수신한 BPDU 패킷은 Maximum aging time 값을 초과했을 때 폐기됩니다. Maximum aging time을 변경하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
stp bridge-max-age *<BRIDGE-MAX-AGE>* **rstp bridge-max-age** *<BRIDGE-MAX-AGE>* **pvstp bridge-max-age** *<BRIDGE-MAX-AGE>* **mstp bridge-max-age** *<BRIDGE-MAX-AGE>*	BPDU 패킷의 age time 을 설정합니다. • *<BRIDGE-MAX-AGE>* Max age time. 설정 범위: 6 ~ 40(초), 기본값: 20(초)

참고: Maximum aging time을 설정하려는 경우에는 다음 공식을 만족하는 hello time과 forward delay time 값을 입력해야 합니다.

Maximum aging time≥(Hello Time+1)*2

Maximum aging time≤(Forward Delay Time-1)*2

예를 들어, maximum aging time이 6인 경우에는 hello time은 '1' 또는 '2'만 지정할 수 있고, maximum aging time이10인 경우에는 forward delay time은 '6'이상인 값으로 지정해야 합니다.

참고: 설정한 maximum aging time을 기본값으로 변경하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no stp bridge-max-age
(config)# no rstp bridge-max-age
(config)# no pvstp bridge-max-age
(config)# no mstp bridge-max-age
```

Edge 포트 설정

포트에 연결되어 있는 장비가 네트워크 브리지가 아닌 터미널(일반 호스트)인 경우에는 STP를 동작시킬 필요가 없습니다. 이와 같이 터미널과 연결되어 있는 포트를 edge 포트라고 하는데, 특정 포트를 edge 포트로 설정하면 BPDU를 교환하거나, listening, learning 상태를 거치지 않고 바로 forwarding 상태로 전환됩니다. Edge 포트로 설정되어 있어도 BPDU를 수신하게 되면 더 이상 edge 포트로 동작하지 않습니다. 이런 경우에는 포트를 다시 edge 포트로 설정해주어야 합니다.

지정한 포트를 edge 포트로 설정하려면 <Configuration 모드>에서 다음 명령을 사용합니다. Edge 포트를 잘못 설정하면 루프가 발생할 수 있으므로 주의해야 합니다.

명 령	설 명
stp port *<NAME>* **portfast {enable | disable}** **rstp port** *<NAME>* **portfast {enable | disable}** **pvstp port** *<NAME>* **portfast {enable | disable}** **mstp port** *<NAME>* **portfast {enable | disable}**	Edge 포트 사용 여부를 설정합니다. • *<NAME>* Edge 포트를 설정할 포트의 이름. • **enable** Edge 포트로 설정 • **disable** Edge 포트로 사용하지 않음(기본값)

MST Region 설정

PAS-K에 MSTP를 설정할 경우, MST Configuration ID를 설정하여 장비가 어떤 MST Region에 속하게 될 것인지를 결정합니다. Configuration ID에는 Region name, Revision, VLAN map이 속하게 됩니다. Configuration ID를 설정하려면, <Configuration 모드>에서 다음 과정을 실행합니다.

순서	명 령	설 명
1	**mstp region** *<REGION>*	Region의 이름을 설정합니다 • *<REGION>* Region 이름. 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32자까지 지정. 첫 글자는 반드시 알파벳 사용. **참고**: 설정한 region을 삭제하려면, <Configuration 모드>에서 **no mstp region** 명령을 사용합니다.
2	**mstp revision** *<REVISION>*	Revision 번호를 설정합니다 • *<REVISION>* revision 번호. 같은 MST boundary 안의 스위치들은 모두 같은 Revision 번호로 설정합니다. (설정 범위: 0 ~ 255) **참고**: 설정한 revision을 삭제하려면, <Configuration 모드>에서 **no mstp revision** 명령을 사용합니다.

참고: 설정한 MSTP region을 삭제하려면 <Configuration 모드>에서 **no mstp region** 명령을 사용합니다.

참고: 설정한 MSTP revision을 삭제하려면 <Configuration 모드>에서 **no mstp revision** 명령을 사용합니다.

Instance 설정

PAS-K에 PVSTP/MSTP를 설정하려면 먼저, VLAN을 하나의 instance로 설정해야 합니다.

MSTP instance 설정

MSTP의 instance에 포함시킬 VLAN을 설정해 VLAN Map을 구성하려면, <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
mstp instance *<ID>* **vlan** *<VLAN>*	Instance에 포함시킬 VLAN을 설정하여 VLAN Map을 구성합니다. • *<ID>* Instance ID. 설정 범위: 1 ~ 15 • *<VLAN>* Instance 에 포함시킬 VLAN 이름

참고: 설정한 MSTP instance를 삭제하려면 <Configuration 모드>에서 **no mstp instance** *<ID>* 명령을 사용합니다.

참고: MSTP instance에서 VLAN을 삭제하려면 <Configuration 모드>에서 **no mstp instance** *<ID>* **vlan** *<VLAN>* 명령을 사용합니다.

MSTP의 instance에 포함시킬 VLAN을 지정한 다음에는, 각 VLAN에 속하는 포트도 MSTP instance에 포함시켜야 합니다. 포트를 MSTP instance에 포함시키려면 포트의 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
mstp instance *<ID>* **port** *<NAME>* [**path-cost** *<PATH-COST>* | **priority** *<PRIORITY>*]	Instance에 포함시킬 포트를 설정합니다. • *<ID>* Instance ID . 설정 범위: 1 ~ 15 • *<NAME>* Instance 에 포함할 포트 이름 • *<PATH-COST>* Instance 포트 경로 비용. 설정 범위: 1 ~ 200000000, 기본값: 20000 • *<PRIORITY>* 포트 우선순위. 설정 범위: 0 ~ 15, 기본값: 8

참고: 설정한 MSTP 포트의 경로 비용을 기본값으로 변경하려면 <Configuration 모드>에서 **no mstp instance** *<ID>* **port** *<NAME>* **path-cost** 명령을 사용합니다.

참고: 설정한 MSTP 포트의 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 **no mstp instance** *<ID>* **port** *<NAME>* **priority** 명령을 사용합니다.

포트를 MSTP의 instance에 포함시킨 후, <Configuration 모드>에서 다음 명령을 사용하여 MSTP instance의 우선순위를 설정합니다.

명 령	설 명
mstp instance *<ID>* **msti-priority** *<MSTI-PRIORITY>*	Instance 의 우선순위를 설정합니다. • *<ID>* Instance ID 설정. (설정 범위: 1 ~ 15) • *<MSTI-PRIORITY>* Instance 우선수위 설정. (설정 범위: 0 ~ 15, 기본값: 8)

참고: 설정한 MSTP instance 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 **no mstp instance** *<ID>* **msti-priority** 명령을 사용합니다.

PVSTP instance 설정

PVSTP의 instance를 설정하려면, <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
pvstp vlan *<VLAN_NAME>* **instance** *<INSTANCE>*	Instance에 포함시킬 VLAN을 설정합니다. • *<VLAN_NAME>* Instance 에 포함시킬 VLAN 이름 • *<INSTANCE>* Instance ID. (설정 범위: 2 ~ 16)

참고: PVSTP instance에서 VLAN을 삭제하려면 <Configuration 모드>에서 **no pvstp vlan** *<VLAN_NAME>* 명령을 사용합니다.

PVSTP의 instance에 포함시킬 VLAN을 지정한 다음에는, 각 VLAN에 속하는 포트도 PVSTP instance에 포함시켜야 합니다. 포트를 PVSTP instance에 포함시키려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
pvstp vlan *<VLAN_NAME>* **port** *<NAME>* **path-cost** *<PATH-COST>*	Instance 에 포함시킬 포트를 설정하고, 포트에 대한 경로 비용을 설정합니다. • *<PATH-COST>* Instance 포트 경로 비용. 설정 범위: 1 ~ 200000000, 기본값: 20000
pvstp vlan *<VLAN_NAME>* **port** *<NAME>* **priority** *<PRIORITY>*	Instance 에 포함시킬 포트를 설정하고, 포트의 우선순위를 설정합니다. • *<PRIORITY>* Instance 우선순위. 설정 범위: 0 ~ 15, 기본값: 8

참고: 설정한 PVSTP 포트의 경로 비용을 기본값으로 변경하려면 <Configuration 모드>에서 **no pvstp vlan** *<VLAN_NAME>* **port** *<NAME>* **path-cost** 명령을 사용합니다.

참고: 설정한 PVSTP 포트의 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 **no pvstp vlan** *<VLAN_NAME>* **port** *<NAME>* **priority** 명령을 사용합니다.

PVSTP의 instance에 포함시킬 포트를 지정한 다음에는 <Configuration 모드>에서 다음 명령을 사용하여 instance의 우선순위를 설정합니다.

명 령	설 명
pvstp vlan *<VLAN_NAME>* **priority** *<PRIORITY>*	Instance의 우선순위를 설정합니다. • *<VLAN_NAME>* Instance 에 포함된 VLAN 이름 • *<PRIORITY>* Instance 우선순위. 설정 범위: 0 ~ 15, 기본값: 8

참고: 설정한 PVSTP instance 우선순위를 기본값으로 변경하려면 <Configuration 모드>에서 **no pvstp vlan** *<VLAN_NAME>* **priority** 명령을 사용합니다.

PVSTP는 instance 별로 hello time/forward delay time/maximum aging time을 설정 할 수 있습니다. PVSTP instance 의 hello time/forward delay time/maximum aging time을 변경하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
pvstp vlan *<VLAN_NAME>* **bridge-hello-time** *<BRIDGE-HELLO-TIME>*	Instance 의 hello time 을 설정합니다. • *<BRIDGE-HELLO-TIME>* Instance 의 hello time. 설정 범위: 1 ~ 10(초), 기본값: 2(초)
pvstp vlan *<VLAN_NAME>* **bridge-forward-delay** *<BRIDGE-FORWARD-DELAY>*	Instance 의 forward delay time 을 설정합니다. • *<BRIDGE-FORWARD-DELAY>* Instance 의 forward delay time. 설정 범위: 4 ~ 30(초), 기본값: 15(초)
pvstp vlan *<VLAN_NAME>* **bridge-max-age** *<BRIDGE-MAX-AGE>*	Instance 의 BPDU 패킷의 age time 을 설정합니다. • *<BRIDGE-MAX-AGE>* Instance 의 BPDU age time. 설정 범위: 6 ~ 40(초), 기본값: 20(초)

참고: PVSTP instance의 hello time, forward delay time, age time을 기본값으로 변경하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

```
(config)# no pvstp vlan <VLAN_NAME> bridge-hello-time
(config)# no pvstp vlan <VLAN_NAME> bridge-forward-delay
(config)# no pvstp vlan <VLAN_NAME> bridge-max-age
```

설정 정보 보기

STP/RSTP/PVSTP/MSTP의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
show stp [**port** *<NAME>*]	STP/RSTP/PVSTP/MSTP 의 설정 정보를 출력합니다. port, vlan, instance 옵션을 사용하면 특정 포트 또는 instance 의 정보를 확인할 수 있습니다.
show rstp [**port** *<NAME>*]	
show pvstp [**port** *<NAME>*]	
show mstp [**port** *<NAME>*]	
show pvstp [**vlan** *<VLAN_NAME>* | **port** *<NAME>*]	
show mstp [**instance** *<INSTANCE>*] | **port** *<NAME>*]	

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

NAT64/DNS64 설정

NAT64와 DNS64는 IPv6 주소를 사용하는 호스트와 IPv4 주소를 사용하는 서버간의 통신을 지원하기 위한 기능입니다. NAT64는 Source NAT 풀에 설정한 IPv4 주소를 사용하여 IPv6 호스트의 주소를 IPv4 주소로 변환하여 서버로 전송함으로써, IPv4 주소를 사용하는 서버의 환경 설정 변경 없이 IPv6 주소를 사용하는 호스트와 통신이 이루어지도록 합니다.

DNS64는 NAT64와 연동하여 IPv6 주소를 사용하는 호스트의 DNS 질의에 대해 IPv4 주소를 사용하는 서버의 IP 주소를 IPv6 주소로 변환하여 응답하는 기능입니다. DNS64는 단독으로 사용할 수 없으며 NAT64와 연동해서 사용해야 합니다.

CLI에서 설정하기

Source NAT 풀 설정

Source NAT 풀은 IPv6 주소를 IPv4 주소로 변환 시 사용할 IPv4 주소 대역입니다. Source NAT 풀을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**lsn snat-pool** *<ID>*	<Source NAT 풀 설정 모드>로 들어갑니다. • *<ID>* Source NAT 풀 ID. 설정 범위: 1 ~ 16
2	**pool** *<POOL>*	IPv6 주소를 IPv4 주소로 변환시 사용할 IPv4 주소 대역을 지정합니다. • *<POOL>* IPv4 주소 대역/넷 마스크 비트 형식으로 입력
3	**proxy-arp-interface** *<PROXY-ARP-INTERFACE>*	IPv4 네트워크에 대한 ARP 응답을 대신 수행할 Proxy ARP 인터페이스를 지정합니다. • *<PROXY-ARP-INTERFACE>* IPv4 네트워크와 연결된 VLAN 인터페이스 이름 **참고**: 설정한 Proxy ARP 인터페이스를 삭제하려면 **no proxy-arp-interface** 명령을 사용합니다.
4	**current**	현재 Source NAT 풀 설정을 확인합니다.
5	**apply**	Source NAT 풀 설정을 시스템에 저장합니다.

참고: 설정한 Source NAT 풀을 삭제하려면 <Configuration 모드>에서 **no lsn snat-pool** *<ID>* 명령을 사용합니다.

NAT64 Prefix 설정

NAT64 기능을 사용하기 위해서는 NAT64 기능을 적용할 출발지 IPv6 주소를 NAT64 Prefix로 설정해야 합니다. NAT64 Prefix를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**lsn nat64-prefix** *<ID>*	<NAT64 Prefix 설정 모드>로 들어갑니다. • *<ID>* NAT64 Prefix ID. 설정 범위: 1 ~ 16
2	**network** *<NETWORK>*	IP 주소 변환에 사용할 IPv6 Prefix 를 지정합니다. • *<NETWORK>* IPv6 Prefix/Prefix 길이 형식으로 입력 **참고**: 설정한 IPv6 Prefix를 삭제하려면 **no network** *<NETWORK>* 명령을 사용합니다.
3	**current**	현재 NAT64 Prefix 설정을 확인합니다.
4	**apply**	NAT64 Prefix 설정을 시스템에 저장합니다.

참고: 설정한 NAT64 Prefix를 삭제하려면 <Configuration 모드>에서 **no lsn nat64-prefix** *<ID>* 명령을 사용합니다.

DNS64 필터 설정

DNS64 필터를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 16개의 DNS64 필터를 설정할 수 있습니다.

순서	명 령	설 명
1	**lsn dns64-filter** *<ID>*	<DNS64 필터 설정 모드>로 들어갑니다. • *<ID>* DNS64 필터 ID. 설정 범위: 1 ~ 16
2	**exclude-filter** *<EXCLUDE>*	DNS64 기능을 적용하지 않을 IPv6 네트워크를 지정합니다. • *<EXCLUDE>* DNS64 기능을 적용하지 않을 IPv6 네트워크 **참고**: 설정한 exclude 필터를 삭제하려면 **no exclude-filter** *<EXCLUDE>* 명령을 사용합니다.
3	**include-filter** *<INCLUDE>*	DNS64 기능을 적용할 IPv6 네트워크를 지정합니다. • *<INCLUDE>* DNS64 기능을 적용할 IPv6 네트워크 **참고**: 설정한 include 필터를 삭제하려면 **no include-filter** *<INCLUDE>* 명령을 사용합니다.
4	**current**	현재 DNS64 필터 설정을 확인합니다.
5	**apply**	DNS64 필터 설정을 시스템에 저장합니다.

참고: 설정한 DNS64 필터를 삭제하려면 <Configuration 모드>에서 **no lsn dns64-filter** *<ID>* 명령을 사용합니다.

DNS64 네임 서버 설정

DNS64 기능을 사용하기 위해서는 PAS-K가 수신한 DNS 질의에 응답하기 위한 네임 서버 IP 주소를 설정해야 합니다. DNS64 네임 서버 IP 주소를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**lsn dns64-nsip**	<DNS64 네임 서버 설정 모드>로 들어갑니다.
2	**nsip** *<NSIP>*	네임 서버 주소로 사용할 IPv6 주소를 지정합니다. • *<NSIP>* DNS64 기능에서 사용할 네임 서버 IPv6 주소. **참고**: 설정한 네임 서버 주소를 삭제하려면 **no nsip** *<NSIP>* 명령을 사용합니다.
3	**current**	현재 DNS64 네임 서버 설정을 확인합니다.
4	**apply**	DNS64 네임 서버 설정을 시스템에 저장합니다.

NAT64 규칙 설정

NAT64 기능을 동작 시키기 위한 규칙을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K는 최대 16개의 NAT64 규칙을 설정할 수 있습니다.

순서	명 령	설 명
1	**lsn nat64** *<NAME>*	<NAT64 설정 모드>로 들어갑니다. • *<NAME>* NAT64 규칙 이름.
2	**type** {**stateful** | **stateless**}	NAT64 규칙의 유형을 지정합니다. • stateful 프로토콜의 세션 상태와 포트를 고려하여 NAT64를 수행 • stateless 프로토콜의 세션 상태와 포트에 관계 없이 NAT64를 수행 (기본값)
3	**nat64-prefix** *<NAT64-PREFIX>*	NAT64 규칙에서 사용할 NAT64 Prefix 의 ID 를 지정합니다. • *<NAT64-PREFIX>* NAT64 Prefix ID.
4	**dns64-filter** *<DNS64-FILTER>*	NAT64 규칙에서 사용할 DNS64 필터의 ID 를 지정합니다. • *<DNS64-FILTER>* DNS64 필터 ID. **참고**: 설정한 DNS64 필터를 삭제려면 **no dns64-filter** 명령을 사용합니다.
5	**map** *<IPV6-ADDR>* **to** *<TO>*	고정 NAT64 IP 주소를 설정합니다. 고정 NAT64 IP 주소로 지정된 IP 주소는 대응되는 IP 주소로만 변환됩니다. • *<IPV6-ADDR>* IPv6 주소 • *<TO>* IPv4 주소
6	**snat-pool** *<SNAT-POOL>*	NAT64 규칙에서 사용할 Source NAT 풀의 ID 를 지정합니다. • *<SNAT-POOL>* Source NAT 풀 ID. **참고**: 설정한 Source NAT 풀을 삭제려면 **no dns64-filter** 명령을 사용합니다.
7	**status** {**enable** | **disable**}	설정한 NAT64 규칙의 사용 여부를 설정합니다. • **enable** NAT64 규칙 활성화 (기본값) • **disable** NAT64 규칙 비활성화

8	**current**	현재 NAT64 규칙 설정을 확인합니다.
9	**apply**	NAT64 규칙 설정을 시스템에 저장합니다.

참고: 설정한 NAT64 규칙을 삭제하려면 <Configuration 모드>에서 **no lsn nat64** <*NAME*> 명령을 사용합니다.

설정 정보 보기

NAT64/DNS64의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
show lsn	PAS-K 에 설정된 모든 NAT64/DNS64 관련 정보를 출력합니다.
show lsn snat-pool [<*ID*>]	PAS-K 에 설정된 Source NAT 풀 정보를 출력합니다. ID 를 입력하면 해당 Source NAT 풀의 정보만 출력합니다.
show lsn nat64-prefix [<*ID*>]	PAS-K 에 설정된 NAT64 Prefix 정보를 출력합니다. ID 를 입력하면 해당 NAT64 Prefix 의 정보만 출력합니다.
show lsn dns64-nsip	PAS-K 에 설정된 DNS64 네임 서버 정보를 출력합니다.
show lsn dns64-filter [<*ID*>]	PAS-K 에 설정된 DNS64 필터 정보를 출력합니다. ID 를 입력하면 해당 DNS64 필터의 정보만 출력합니다.
show lsn nat64 [<*NAME*>]	PAS-K 에 설정된 NAT64 규칙 정보를 출력합니다. 이름을 입력하면 해당 NAT64 규칙의 정보만 출력합니다.

NAT64 세션 엔트리 정보

NAT64 기능을 통해 현재 연결되어 있는 모든 세션 엔트리를 확인하려면 <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
show entry-nat64	현재 연결된 모든 세션 엔트리의 목록과 정보를 출력합니다.

NAT64 기능을 통해 연결된 모든 세션 엔트리 목록과 정보를 삭제하려면 <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
no entry-nat64	NAT64 기능을 통해 연결된 모든 세션 엔트리 목록과 정보를 삭제합니다.

네트워크 연결 확인

기본적인 네트워크 설정을 완료한 후, 네트워크 연결을 확인하기 위해서 다음과 같은 작업을 수행할 수 있습니다.

- Ping 연결 테스트
- 패킷 경로 추적

Ping 연결 테스트

사용자는 원격 호스트의 네트워크 연결 확인을 위해 **ping** 명령을 사용할 수 있습니다. **ping** 명령은 지정한 목적지로 ICMP 에코 요청 패킷을 보낸 후, 요청에 대한 응답을 기다립니다. 원격 호스트에서 응답이 오면 사용자는 요청 패킷이 목적지에 도달하는데 걸린 소요 시간을 알 수 있습니다. 사용자는 **ping** 명령의 목적지 주소로 IP 주소나 호스트 이름을 사용할 수 있습니다.

ping 명령에 대한 응답의 유형은 다음과 같습니다.

- Normal response
  호스트의 네트워크 연결이 정상적일 경우
- Destination does not respond
  호스트가 응답하지 않을 경우
- Unknown host
  호스트가 존재하지 않을 경우
- Destination unreachable
  게이트웨이가 지정한 목적지 네트워크로 갈 수 없는 경우
- Network or host unreachable
  라우팅 테이블에 해당 호스트나 네트워크가 존재하지 않을 경우

IPv4 및 IPv6 환경에서 호스트에 대한 네트워크 연결 테스트를 수행하려면, <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
ping *<HOST>*	호스트에 대한 네트워크 연결 테스트를 수행합니다. • *<HOST>* 네트워크 연결 테스트를 수행할 호스트의 IPv4 주소 또는 도메인 네임
ping6 *<HOST>*	호스트에 대한 네트워크 연결 테스트를 수행합니다. • *<HOST>* 네트워크 연결 테스트를 수행할 호스트의 IPv6 주소 또는 도메인 네임 (ex : A:B::C:D)

PAS-K는 ARP 패킷을 이용하여 호스트의 네트워크 연결을 확인하는 ARP Ping 기능을 제공합니다. ARP Ping 기능을 통해 호스트에 대한 네트워크 연결 테스트를 수행하려면, <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
arping *<HOST>*	ARP 패킷을 이용하여 호스트에 대한 네트워크 연결 테스트를 수행합니다. • *<HOST>* 네트워크 연결 테스트를 수행할 호스트의 IP 주소 또는 도메인 네임

참고: ARP Ping 기능은 IPv4 환경에서만 사용할 수 있습니다.

패킷 경로 추적

원격 호스트에게 전송한 패킷의 경로를 추적하기 위해서는 **traceroute** 명령을 사용합니다. **traceroute** 명령은 IP 헤더 내의 TTL(Time To Live) 필드를 사용하여 패킷을 전송하며, 패킷을 전송받은 라우터와 서버가 특정 리턴 메시지를 보내도록 합니다. 패킷 추적은 TTL 필드 값을 1로 설정한 데이터그램을 UDP(User Datagram Protocol) 프로토콜로 목적지 호스트로 전송할 때부터 시작됩니다. 라우터는 전송받은 패킷의 TTL 값이 1이나 0이면 해당 데이터그램을 드롭시키며, 패킷을 전송한 라우터에게 다시 ICMP(Internet Control Message Protocol) 프로토콜로 시간 초과(time-exceeded) 메시지를 전송합니다. 이 때, 시간 초과 메시지를 받은 라우터는 시간 초과 메시지의 송신지 주소 필드를 검사하여 첫 번째 홉의 IP 주소를 확인합니다.

다음 홉의 식별을 위해 라우터는 TTL 값을 2로 해서 다시 UDP 패킷을 전송합니다. 첫 번째 라우터는 TTL 값을 1만큼 감한 뒤 다음 라우터에 데이터를 전송합니다. 두 번째 라우터는 TTL 값이 1인 것을 본 후, 데이터를 버리고, 송신지로 시간 초과 메시지를 보냅니다. 이러한 과정은 데이터그램을 목적지 호스트로 전송하는데 충분한 TTL 값이 될 때까지나 TTL이 최대값에 이를 때까지 계속됩니다.

데이터그램이 목적지 호스트에 도착한 때를 측정하기 위해 **traceroute** 명령은 목적지 호스트가 사용하지 않을 법한 큰 값의 UDP 목적지 포트를 설정합니다. 인식할 수 없는 포트 번호로 데이터그램을 전송받았을 때 호스트는 송신지 호스트에 ICMP 포트로 '도달 불가능(unreachable error)'메시지를 전송합니다. 이 메시지는 경로를 추적하는 라우터에게 도착한 목적지를 표시합니다.

패킷 경로를 추적하려면 <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
traceroute *<HOST>*	호스트에 전송한 패킷의 경로를 추적합니다. • *<HOST>* 패킷의 경로를 추적할 호스트의 IP 주소 또는 도메인 네임

제4장
시스템 관리와 모니터링

이 장에서는 PAS-K 시스템을 관리하는 데 필수적인 기능들과 시스템의 기본적인 정보와 상태 정보, 로그 등을 모니터링하는 방법에 대해 살펴봅니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- 시스템 정보
- 기본 시스템 관리
- 설정 파일
- PLOS
- 시스템 종료
- 세션 유지 시간
- 기술 지원 도우미
- 사용자 계정 및 인증
- 로그 관리
- 포트 모니터링
- 시스템 감시
- 명령 사용 이력 조회
- FAN Hot Swap

시스템 정보

이 절에서는 다음과 같은 시스템 정보를 CLI를 통해 출력하는 방법에 대해 살펴봅니다.

- **시스템 기본 정보**
  장비의 이름, 일련 번호, MAC 주소, 소프트웨어 버전 등의 기본적인 시스템 정보
- **CPU 와 메모리의 사용 상태**
  현재 CPU 의 사용률과 사용 중인 메모리 크기, 사용 가능한 메모리의 용량 등 CPU 와 메모리의 현재 사용 상태 정보
- **하드웨어 상태**
  시스템 온도, 전압, 냉각 팬의 동작 상태, 전원 공급기의 동작 상태 등 시스템 하드웨어의 상태 정보

위의 정보 중에서 시스템 자원의 사용 상황과 하드웨어의 상태는 **자원 모니터링** 기능이 활성화되어 있는 경우에만 출력할 수 있습니다. 자원 모니터링 기능은 CPU나 메모리, 팬, 전원 등과 같은 시스템 자원의 상태를 모니터링하는 기능으로 이 기능이 활성화되어 있어야만 자원과 관련된 실시간 정보가 수집됩니다. 기본적으로 자원 모니터링 기능은 비활성화되어 있으므로, 자원의 상태 정보를 출력하려면 자원 모니터링 기능을 활성화해야 합니다. 자원 모니터링 기능을 활성화하는 방법은 **자원 모니터링 기능 활성화/비활성화** 절에 설명되어 있습니다.

CLI에서 시스템 정보 출력하기

시스템 기본 정보 출력

장비의 이름, 일련 번호, MAC 주소, 소프트웨어 버전 등의 기본적인 시스템 정보를 확인하려면, <Configuration 모드>에서 **`show system`** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

시스템 자원 사용 상태 출력

CPU와 메모리의 현재 사용 상황을 확인하려면, <Configuration 모드>에서 **`show resource`** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

하드웨어 상태 출력

시스템의 현재 온도와 공급되는 전압, 냉각 팬의 동작 상태를 확인하려면, <Configuration 모드>에서 **`show hardwarestatus`** 명령을 사용합니다. **`show hardwarestatus`** 명령으로 출력된 항목들의 값을 통해 다음과 같은 장비의 문제 발생 여부를 판단할 수 있습니다.

- **현재 온도**
  CPU 의 온도가 임계값을 초과한 경우, 냉각 팬이 동작하지 않거나 혹은 제품이 설치된 장소의 온도가 지나치게 높거나 장비 환기구가 막혀 있는 상태임을 의미합니다.
- **냉각 팬 동작 상태**
  냉각 팬의 상태가 'OFF' 인 경우 냉각 팬이 정상적으로 동작하지 않는 상태이므로 장비를 점검해보도록 합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

기본 시스템 관리

이 절에서는 다음과 같은 기본적인 시스템 설정 항목들을 CLI에서 설정하는 방법에 대해 살펴봅니다.

- 시스템 이름
- 로그인 배너
- 관리 접근 서비스
- 터미널 연결 제한 시간
- 시스템 시간

시스템 이름 설정

사용자는 PAS-K 이름을 통해 네트워크 상의 장비를 구분할 수 있습니다. PAS-K의 이름은 CLI 프롬프트의 맨 앞에 표시됩니다. 기본적으로 지정되는 PAS-K의 이름은 'switch'입니다. PAS-K의 이름을 변경하는 방법은 다음과 같습니다.

시스템 이름 설정

PAS-K의 이름을 변경하려면 <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
hostname *<HOSTNAME>*	PAS-K의 이름을 변경합니다. • *<HOSTNAME>* 최대 63자의 알파벳, 숫자, '-', '_' 문자로 이루어진 문자열로 지정, 첫 글자는 반드시 알파벳 또는 숫자를 사용

참고: 설정되어 있는 시스템 이름을 기본값으로 변경하려면, <Configuration 모드>에서 **no hostname** 명령을 사용합니다.

로그인 배너 설정

로그인 배너는 콘솔 또는 SSH, Telnet을 통해 CLI에 접속하는 사용자에게 전달 사항이나 주의 사항을 시스템 로그인 화면에서 볼 수 있도록 하는 기능입니다.

로그인 배너를 설정하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
banner *<TEXT>*	시스템 로그인 전 화면에 출력되는 메시지를 설정합니다. • *<TEXT>* 알파벳, 숫자, 특수문자를 입력할 수 있으며, 문자열의 시작과 끝에는" 를 입력. '\n'을 입력하면 줄바꿈되며, 80자를 초과하는 경우에는 자동으로 줄바꿈이 수행됩니다.

참고: 설정되어 있는 로그인 배너를 삭제하려면, <Configuration 모드>에서 **no banner** 명령을 사용합니다.

참고: 설정되어 있는 로그인 배너를 조회하려면, <Configuration 모드>에서 **show banner** 명령을 사용합니다.

관리 접근 서비스 설정

PAS-K가 부팅되면 관리자가 CLI를 사용하여 장비를 설정할 수 있도록 기본적으로 SSH, Telnet, HTTP, HTTPS 서비스가 실행되는데, 사용자의 편의에 따라 이를 활성화하거나 차단할 수 있습니다. SSH, Telnet, HTTP, HTTPS 서비스를 활성화/비활성화하는 방법은 다음과 같습니다.

관리 접근 서비스 상태 및 포트 설정

관리 접근 서비스의 동작 상태와 포트를 변경하려면 <Configuration 모드>에서 다음 명령을 실행합니다.

순서	명 령	설 명
1	**management-access**	<관리 접근 서비스 설정 모드>로 들어갑니다.
2	**ssh port** *<PORT>*	SSH 서비스의 포트를 지정합니다. • *<PORT>* 설정 범위: 1 ~ 65535, 기본값: 22
3	**ssh status {enable | disable}**	SSH 서비스의 사용 여부를 지정합니다. • **enable** SSH 서비스 활성화 • **disable** SSH 서비스 비활성화 (기본값)
4	**telnet port** *<PORT>*	Telnet 서비스의 포트를 지정합니다. • *<PORT>* 설정 범위: 1 ~ 65535, 기본값: 23
5	**telnet status {enable | disable}**	Telnet 서비스의 사용 여부를 지정합니다. • **enable** Telnet 서비스 활성화 (기본값) • **disable** Telnet 서비스 비활성화
6	**http port** *<PORT>*	HTTP 서비스의 포트를 지정합니다. • *<PORT>* 설정 범위: 1 ~ 65535, 기본값: 8080
7	**http status {enable | disable}**	HTTP 서비스의 사용 여부를 지정합니다. • **enable** HTTP 서비스 활성화 (기본값) • **disable** HTTP 서비스 비활성화
8	**https port** *<PORT>*	HTTPS 서비스의 포트를 지정합니다. • *<PORT>* 설정 범위: 1 ~ 65535, 기본값: 8443
9	**https status {enable | disable}**	HTTPS 서비스의 사용 여부를 지정합니다. • **enable** HTTPS 서비스 활성화 • **disable** HTTPS 서비스 비활성화 (기본값)
10	**current**	관리 접근 서비스의 설정을 확인합니다.
11	**apply**	설정을 저장하고 시스템에 적용합니다.

관리 접근 서비스 설정 정보 보기

관리 접근 서비스의 설정 정보 및 관리 접근 서비스의 동작 상태를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show management-access** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고합니다.

터미널 설정

이 절에서는 CLI의 터미널 연결 제한 시간과 터미널 길이를 변경하는 방법에 대해 살펴봅니다.

터미널 연결 제한 시간 설정

PAS-K에서 터미널 세션 자원을 효율적으로 사용하기 위해 터미널 연결 제한 시간을 설정할 수 있습니다. 설정한 제한 시간 동안 연결된 터미널에서 아무런 동작이 없으면 PAS-K는 이 터미널 연결을 종료합니다. 터미널 연결 제한 시간을 변경하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
terminal timeout *<TIMEOUT>*	터미널 연결 제한 시간을 설정합니다. • *<TIMEOUT>* 터미널 연결 제한 시간 설정. 설정 범위: 1 ~ 65535(분), 기본값: 10(분)

참고: 설정되어 있는 터미널 연결 제한 시간을 기본값으로 변경하려면, <Configuration 모드>에서 **no terminal timeout** 명령을 사용합니다.

터미널 길이 설정

터미널의 길이는 터미널 화면에 나타낼 수 있는 최대 라인 수입니다. 터미널 길이를 설정하려면 <Configuration 모드>에서 다음과 같이 terminal length 명령을 사용합니다.

명 령	설 명
terminal length *<LENGTH>*	터미널 길이(터미널 화면에 나타낼 라인 수)를 설정합니다. • *<LENGTH>* 설정 범위: 0 ~ 100, 기본값: 30

참고: 터미널 길이를 0으로 설정하면 터미널 길이를 무한대로 설정한 것처럼 길이가 긴 출력도 한번에 확인할 수 있습니다.

터미널 설정 정보 보기

터미널 연결 제한 시간, 터미널 길이 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show terminal** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

시스템 시간 설정

PAS-K에서 발생한 각종 이벤트나 장애, 사용자에 의해 실행된 명령 등이 로그로 기록될 때마다 당시의 시스템 시간도 함께 기록됩니다. 이러한 로그들은 시스템에 문제가 발생했을 때 문제를 해결하기 위한 중요한 자료로 사용되므로 시스템의 시간을 정확하게 유지하는 것은 매우 중요합니다.

PAS-K의 시간은 NTP 기능을 사용하여 주기적으로 NTP 서버로부터 정확한 시간을 받아온 후 자동으로 시간을 동기화합니다.

이 절에서는 NTP 기능을 사용하는 방법에 대해 알아보도록 합니다.

시스템 시간 직접 설정

현재 시스템 시간을 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show clock** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

출력된 시스템 시간이 현재 시간과 맞지 않는 경우에는 <Configuration 모드>에서 다음 명령을 사용하여 시스템에 정확한 시간을 설정하도록 합니다.

명 령	설 명
date *<DATE>*	시스템 시간을 설정합니다. • *<DATE>* 시스템 시간을 MM/DD/YYYY hh:mm:ss (월/일/년 시간:분:초) 형식으로 설정.

참고: 시스템 시간을 직접 설정하기 위한 **date** *<DATE>* 명령 사용 시 다음과 같이 반드시 *<DATE>*의 시작과 끝 지점에 큰 따옴표(")를 입력해야 합니다.

```
(config)# date "06/15/2012 15:34:00"
```

시스템 시간 직접 설정 정보 보기

설정한 시간이 시스템에 정상적으로 반영되었는지 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show clock** 명령을 사용합니다.

NTP(Network Time Protocol) 클라이언트 설정

NTP(Network Time Protocol)는 네트워크에 연결된 장비들의 시간을 동기화 시킬 수 있게 해주는 프로토콜입니다. PAS-K는 NTP 프로토콜을 사용하여 시스템의 시간을 설정할 수 있는 NTP 클라이언트 기능을 지원합니다. NTP 클라이언트 기능이 활성화된 장비들은 NTP 서버로 시간 정보를 요청합니다. 그리고, NTP 서버로부터 전달받은 시간 정보와 장비의 현재 시간 정보를 비교한 후 차이가 있을 경우에는 그 차이를 조정하여 장비의 시간을 정확하게 맞춥니다.

PAS-K에 NTP 클라이언트 기능을 설정 하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**ntp**	<NTP 설정 모드>로 들어갑니다.
2	**primary-server** *<PRIMARY-SERVER>*	Primary NTP 서버를 설정합니다 • *<PRIMARY-SERVER>* Primary NTP 서버의 IP 주소 설정.
3	**secondary-server** *<SECONDARY-SERVER>*	Primary NTP 서버에 문제가 발생했을 경우 시간을 동기화할 Secondary NTP 서버를 설정합니다 • *<SECONDARY-SERVER>* Secondary NTP 서버의 IP 주소 설정.
4	**status {enable | disable}** (선택 설정)	NTP 클라이언트 기능의 사용 여부를 지정합니다. • **enable** NTP 클라이언트 기능 활성화 • **disable** NTP 클라이언트 기능 비활성화 (기본값)
5	**current**	NTP 클라이언트 설정을 확인합니다.
6	**apply**	NTP 클라이언트 설정을 저장하고 시스템에 적용합니다.
7	**timezone {+8 | +9}**	PAS-K 가 설치된 지역의 GMT 시간대를 설정합니다. • **+8** 지역이 중국인 경우 • **+9** 지역이 한국 또는 일본인 경우 (기본값)

참고: NTP 서버와 직접 동기화를 수행하려면 <Configuration 모드>에서 다음과 같은 명령을 사용하여 NTP 서버로부터 직접 시간을 동기화할 수 있습니다. *<HOST>* 항목에는 IP 주소 또는 도메인 네임을 입력합니다.

```
(config)# rdate <HOST>
```

참고: 지정한 NTP 서버를 삭제하려면 <NTP 설정 모드>에서 다음과 같은 명령을 사용합니다.

```
(config-ntp)# no primary-server
(config-ntp)# no secondary-server
```

참고: 지정한 GMT 시간대를 기본값으로 변경하려면 <Configuration 모드>에서 **no timezone** 명령을 사용합니다.

NTP(Network Time Protocol) 클라이언트 설정 정보 보기

설정한 NTP 클라이언트의 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show ntp** 명령을 실행합니다. GMT 시간대 설정 정보는 **show timezone** 명령을 통해 확인할 수 있습니다.

설정 파일

이 절에서는 설정 파일과 관련된 다음과 같은 작업을 CLI에서 수행하는 방법을 차례로 살펴봅니다.

- 설정 파일 저장
- 설정 파일 복사
- 설정 파일 업로드
- 설정 파일 다운로드
- 설정 초기화

설정 파일 개요

PAS-K의 설정은 SSD에 저장되며, 6개의 저장 공간(Config-slot 1 ~ 5, Startup-config)으로 분리되어 각각 다른 설정을 저장할 수 있습니다. PAS-K는 부팅 시 Startup-config에 저장된 설정을 사용하여 부팅합니다. Startup-config를 제외한 각 저장 공간 별로 설정 저장, 복사, 업로드, 다운로드, 초기화 기능을 지원합니다.

장비가 부팅되면 SSD에 저장되어 있는 설정 파일을 SDRAM으로 로딩합니다. SDRAM으로 로딩된 설정 파일은 CLI를 통해 사용자가 장비의 구성을 바꿀 때마다 내용이 변경됩니다. 이 설정 파일을 running-config라고 합니다. running-config는 현재 장비의 구성 정보를 가지고 있지만 SDRAM 상에 있기 때문에 장비를 리부팅하면 내용이 모두 지워집니다. 하지만, CLI에서 apply 혹은 write memory 명령을 실행하여 설정 정보를 저장하면 running-config가 startup-config로 SSD에 저장되어 리부팅한 이후에도 계속 사용될 수 있습니다.

각 저장 공간의 설정 파일은 장비의 CLI로 접속한 PC가 실행 중인 PC로 다운로드하거나 외부 서버로 전송하여 보관할 수 있습니다. 그리고, PC에 저장된 설정 파일을 장비로 업로드하여 사용할 수 있습니다. 이러한 기능을 사용하여 설정 파일을 외부 장비에 백업해두면 설정 파일에 문제가 생기거나 혹은 현재 구성 대신 이전 구성으로 되돌려야 하는 경우에 유용하게 사용할 수 있습니다. 이 밖에도, 필요한 경우 현재 설정을 모두 삭제하고 장비가 출하될 때의 기본 설정으로 되돌릴 수도 있습니다.

CLI에서 설정 파일 사용하기

설정 파일 저장

현재 설정을 Startup-config 저장 공간에 저장하는 경우에는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
write-memory	Startup-config 저장 공간에 현재 설정을 저장합니다.

현재 설정을 Config-slot 1 ~ 5 저장 공간에 저장하는 경우에는 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**config-slot** *<ID>*	설정을 저장할 Config-slot을 지정하고 <Config-slot 모드>로 들어갑니다. • *<ID>* 설정을 저장할 Config-slot ID. (설정 범위: 1 ~ 5)
2	**save**	현재 설정을 Config-slot에 저장합니다.

설정 파일 복사

Config-slot 저장 공간에 저장되어 있는 설정 파일을 다른 저장 공간으로 복사하는 경우에는 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**config-slot** *<ID>*	설정이 저장되어 있는 Config-slot을 지정하고 <Config-slot 모드>로 들어갑니다. • *<ID>* Config-slot ID. (설정 범위: 1 ~ 5)
2	**copy-to** {**startup** | *<ID>*}	설정을 복사할 저장 공간을 설정합니다. • **startup** 해당 저장 공간의 설정 파일이 Startup-config에 복사되어 다음 부팅부터 사용 • *<ID>* Config-slot ID. (설정 범위: 1 ~ 5)

참고: Config-slot 저장 공간에 저장되어 있는 파일을 삭제하고 초기화하려면 <config-slot 모드>에서 **reset** 명령을 실행합니다.

설정 파일 업로드/다운로드

Config-slot 설정 파일 업로드/다운로드

Config-slot 저장 공간에 저장되어 있는 설정 파일을 TFTP 서버로 업로드/다운로드하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**config-slot** *<ID>*	설정을 업로드/다운로드할 Config-slot을 지정하고 <Config-slot 모드>로 들어갑니다. • *<ID>* Config-slot ID. (설정 범위: 1 ~ 5)
2	**host** *<HOST>*	설정을 업로드/다운로드할 TFTP 서버의 주소를 설정합니다. • *<HOST>* TFTP 서버의 주소.
3	**path** *<PATH>*	업로드/다운로드할 설정파일의 경로와 이름을 설정합니다. • *<PATH>* 설정 파일의 경로와 이름.
4	**description** *<DESCRIPTION>*	해당 config-slot에 대한 설명을 입력합니다. • *<DESCRIPTION>* Config-slot에 대한 부가 설명.
5	**current**	현재까지 설정한 정보를 확인합니다.
6	**apply**	TFTP 서버의 주소와 설정 파일 이름을 저장합니다.
7	**config-slot** *<ID>*	<Config-slot 모드>로 다시 들어갑니다.
8	{**export** | **import**}	설정 파일을 TFTP 서버로 업로드 또는 다운로드합니다. • **export** 설정 파일을 TFTP 서버로 업로드합니다. • **import** 설정 파일을 TFTP 서버에서 다운로드합니다.

참고: 설정 파일을 TFTP 서버로 업로드하여 백업해두면, 설정 파일에 문제가 생기거나 혹은 현재 구성 대신 이전 구성으로 되돌려야 하는 경우에 유용하게 사용할 수 있습니다.

참고: 네트워크 상의 다른 PAS-K에 기존의 PAS-K와 유사한 설정을 하고자 하는 경우에는, 처음부터 설정할 필요가 없이 다운로드한 설정 파일을 적용한 후 필요한 부분의 설정만 변경하면 됩니다.

부분적 설정 파일 업로드/다운로드

PAS-K는 일부 기능의 설정 파일만 부분적으로 업로드/다운로드할 수 있습니다. 기능을 선택하여 설정 파일을 업로드 다운로드하려면 <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
export-to *<FILE>* **tftp** *<TFTP>*	설정 파일을 TFTP 서버로 업로드합니다. • *<FILE>* 업로드할 설정 파일 종류. 지원 설정 파일: ssl-key, sp-filter, cslb-filter, fwlb-filter, gwlb-filter, tceh-assist, config-slot1, config-slot2, config-slot3, config-slot4, config-slot5, startup-config, ssl-certificate-crt, ssl-certificate-csr, ssl-client-authentication-crl, ssl-client-authentication-crt • *<TFTP>* TFTP 서버의 IP 주소와 설정 파일의 경로 및 이름. 입력 형식: <IP 주소>:/<경로>/<파일 이름>
import-from *<FILE>* **tftp** *<TFTP>*	설정 파일을 TFTP 서버에서 다운로드합니다.

참고: **import-from** 명령을 사용하여 설정 파일을 다운로드한 경우에는 해당 설정이 running-config에 즉시 적용되며, **write-memory** 명령을 실행해야만 startup-config에 저장됩니다.

참고: **export-to, import-from** 명령을 통해 업로드/다운로드할 수 있는 설정 파일은 다음과 같습니다.

- sp-filter 정적 필터 설정
- cslb-filter CSLB 필터 설정
- fwlb-filter FWLB 필터 설정
- gwlb-filter GWLB 필터 설정
- tech-assist 기술지원 도우미 파일(TFTP 서버로 업로드만 가능)
- config-slot1 Config-slot 1에 저장된 설정 파일
- config-slot2 Config-slot 2에 저장된 설정 파일
- config-slot3 Config-slot 3에 저장된 설정 파일
- config-slot4 Config-slot 4에 저장된 설정 파일
- config-slot5 Config-slot 5에 저장된 설정 파일
- startup-config Startup-config에 저장된 설정 파일
- ssl-certificate-crt SSL 인증서 파일
- ssl-certificate-csr SSL 인증 요청서 파일(TFTP 서버로 업로드만 가능)
- ssl-client-authentication-crl 클라이언트 인증서 취소 목록 파일
- ssl-client-authentication-crt 클라이언트 인증서 파일
- ssl-key SSL 비밀 키 파일

초기 설정 복구

장비의 현재 설정을 모두 삭제하고 출하 시 기본 설정(default-config)을 startup-config로 복구하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
reset	Startup-config 저장 공간을 초기화합니다.

주의: 위의 명령을 실행한 후에는 초기화한 설정을 시스템에 적용하기 위해 PAS-K를 다시 시작해야 합니다. PAS-K를 다시 시작하려면 <Configuration 모드>에서 **reboot** 명령을 실행하면 됩니다.

설정 파일 내용 출력

Config-slot 내용 출력

Config-slot의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show config-slot** 명령을 사용합니다. **show config-slot** *<ID>* 명령을 실행하여 특정 config-slot에 대한 설정 정보만을 출력할 수 있습니다.

Running-config 내용 출력

장비의 현재 설정 정보인 running-config 파일의 내용을 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show running-config** 명령을 사용합니다. **show running-config** *<option>* 명령을 실행하여 선택한 특정 인자에 대한 running-config 내용만을 출력할 수 있으며, 인자로 선택 가능한 명령은 **show running-config** 명령 뒤에 '?' 를 입력하여 확인할 수 있습니다.

Startup-config 내용 출력

장비에 저장되어 있는 startup-config의 내용을 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show startup-config** 명령을 사용합니다. **show startup-config** *<option>* 명령을 실행하여 선택한 특정 인자에 대한 startup-config 내용 만을 출력할 수 있으며, 인자로 선택 가능한 명령은 **show startup-config** 명령 뒤에 '?' 를 입력하여 확인할 수 있습니다.

Running-config/Start-config 비교 출력

장비에 저장되어 있는 startup-config와 현재 설정 정보인 running-config의 내용을 비교하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show diff-config** 명령을 사용합니다. **show diff-config** <*option*> 명령을 실행하여 선택한 특정 인자에 대한 비교 내용만을 출력할 수 있으며, 인자로 선택 가능한 명령은 **show diff-config** 명령 뒤에 '?' 를 입력하여 확인할 수 있습니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

PLOS

PLOS는 출하 시 PAS-K에 설치되어 있는 소프트웨어입니다. PAS-K의 PLOS에는 여러 개의 버전이 있으며, 각 버전의 PLOS에서 제공하는 기능이 다를 수 있습니다. 필요한 경우에는, 현재 설치되어 있는 PLOS 버전 보다 높은 버전의 PLOS 또는 낮은 버전의 PLOS로 업데이트할 수 있습니다. 이 절에서는 CLI를 통해 PLOS를 업데이트하는 방법을 살펴봅니다.

CLI에서 설정하기

PLOS 업데이트

CLI 명령을 사용하여 PLOS를 업데이트하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**os-update** *<ARGUMENTS>*	PAS-K에 PLOS를 업데이트합니다. • *<ARGUMENTS>* PLOS가 저장되어 있는 FTP 서버 또는 HTTP 서버의 IP 주소와 파일 이름을 입력합니다. FTP 서버의 경우에는 'ftp://'로, HTTP 서버의 경우에는 'http://'로 시작해야 합니다.
2	**reboot**	다운로드한 PLOS를 시스템에 적용하기 위해 PAS-K를 다시 시작합니다.

참고: FTP 서버를 이용한 PLOS 업데이트 시 ID/Password는 다음과 같은 형식으로 입력할 수 있습니다.

```
(config)# os-update ftp://<ID>:<Password>@<PATH>
```

PLOS 정보 출력

PAS-K에 설치되어 있는 PLOS의 버전과 PLOS 파일 이름을 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show system** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

시스템 종료

운용중인 PAS-K를 종료하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
shutdown	시스템을 종료합니다.

참고: PAS-K 는 제품 앞면의 LCD와 컨트롤 버튼을 사용하여 종료할 수 도 있습니다. LCD와 컨트롤 버튼을 사용하여 종료하는 방법은 이 설명서와 함께 제공되는 설치 설명서를 참고하도록 합니다.

세션 유지 시간

개요

PAS-K는 서버와 클라이언트 사이에 ICMP, TCP, UDP 세션을 생성하거나 생성된 세션을 종료하기 위해 패킷을 주고받을 때 해당 세션의 상태에 대한 엔트리를 생성합니다. PAS-K에 세션 엔트리가 계속 저장되면 적지 않은 메모리 용량을 차지하게 됩니다. 이를 방지하고, 장비의 성능을 향상시키기 위해, PAS-K는 일정한 시간이 경과된 후에도 서버나 클라이언트에서 전송되는 패킷이 없는 세션의 경우, 저장된 세션 엔트리를 삭제합니다. PAS-K는 엔트리를 삭제할 세션을 결정할 때 세션 유지 시간(timeout)을 사용합니다.

유지 시간을 설정할 수 있는 세션의 종류

세션 유지 시간을 사용하여 엔트리를 삭제할 수 있는 세션에는 ICMP 세션과 TCP 세션, UDP 세션이 있습니다. 이 세가지 외에 나머지 종류의 세션을 generic 세션이라하며, (PAS-K에서는)이 generic 세션을 위한 유지 시간도 설정할 수 있습니다.

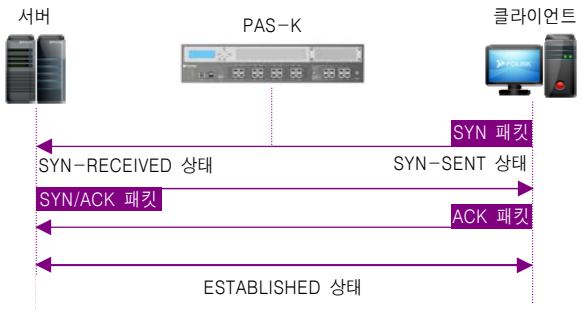
TCP 세션

세션을 맺거나(establish) 종료할 때 클라이언트와 서버 간의 handshaking 과정이 필요한 TCP 세션은 handshaking 과정이 진행되는 단계마다 세션의 상태가 변경됩니다. PAS-K는 TCP 세션의 상태마다 세션 유지 시간을 지정할 수 있습니다. TCP 세션의 상태는 UNASSURED, SYN-SENT, SYN-RECEIVED, ESTABLISHED, CLOSE-WAIT, LAST-ACK, FIN-WAIT, TIME-WAIT, TCP-CLOSE의 9가지가 있습니다.

- **UNASSURED 상태**
  UNASSURED 는 서버와 클라이언트가 handshaking 을 수행하는 과정에서 SYN 패킷을 전송하고, SYN/ACK 패킷을 수신하기까지의 상태입니다. UNASSURED 상태의 세션 유지 시간 값을 설정해두면, SYN/ACK 패킷이 수신되지 않는 비 정상적인 세션을 빨리 종료시킬 수 있습니다. 따라서, SYN Flooding 과 같은 DDoS 공격 발생 시 세션 테이블이 가득 차서 더 이상 세션을 형성하지 못하고 패킷을 폐기하는 현상을 방지할 수 있습니다.
- **SYN-SENT 상태**
  SYN-SENT 상태는 클라이언트가 SYN 패킷을 서버에게 전송하고, SYN 패킷에 대한 응답 메시지인 ACK 패킷을 기다리는 상태입니다.
- **SYN-RECEIVED 상태**
  SYN-RECEIVED 상태는 서버가 SYN 패킷을 전송받은 후, 클라이언트에게 SYN 에 대한 응답 메시지로 보내는 ACK 패킷과 자신의 SYN 패킷을 전송한 상태입니다. 서버가 보낸 SYN 패킷에 대해 클라이언트가 ACK 패킷을 전송하면 ESTABLISHED 상태가 됩니다.
- **ESTABLISHED 상태**
  ESTABLISHED 상태는 서버와 클라이언트가 TCP 세션을 형성한 상태입니다. ESTABLISHED 상태인 TCP 세션에 대한 엔트리의 세션 유지 시간 값이 작으면 이미 형성된 TCP 세션이 사용 중인데도 엔트리가 삭제되는 경우가 발생할 수 있으므로 ESTABLISHED 상태의 기본 세션 유지 시간 값은 3600 초 정도로 크게 설정하도록 합니다.
- **FIN-WAIT 상태**
  클라이언트가 TCP 세션을 종료하기 위해 서버로 FIN 패킷을 보내거나, 서버가 클라이언트로부터 FIN 패킷을 받은 후 FIN/ACK 응답 패킷을 보내면 TCP 세션은 FIN-WAIT 상태가 됩니다.
- **CLOSE-WAIT 상태**
  서버가 TCP 세션을 종료하기 위해 클라이언트로 FIN 패킷을 보내거나, 클라이언트가 서버로부터 FIN 패킷을 받은 후 FIN/ACK 응답 패킷을 보내면 TCP 세션은 CLOSE-WAIT 상태가 됩니다.
- **LAST-ACK 상태**
  서버가 클라이언트로부터 또는 클라이언트가 서버로부터 TCP 세션을 종료하기 위한 요청을 받고 승인한 후, 자신의 FIN 패킷을 전송하고 그에 대한 승인을 기다리는 상태입니다.
- **TIME-WAIT 상태**
  TCP 세션이 정상적으로 종료되면 TCP-WAIT 상태로 됩니다. 아래에 그림과 같이 클라이언트가 서버로 FIN/ACK 응답 패킷을 보낸 후 FIN 패킷을 보내거나, 서버가 이 FIN 패킷을 받은 후 FIN/ACK 응답 패킷을 보내면 TCP 세션은 TIME-WAIT 상태로 됩니다. 또는 서버가 클라이언트로 FIN/ACK 응답 패킷을 보낸 후 FIN 패킷을 보내거나, 클라이언트가 이 FIN 패킷을 받은 후 FIN/ACK 응답 패킷을 보내면 TCP 세션은 TIME-WAIT 상태가 됩니다.

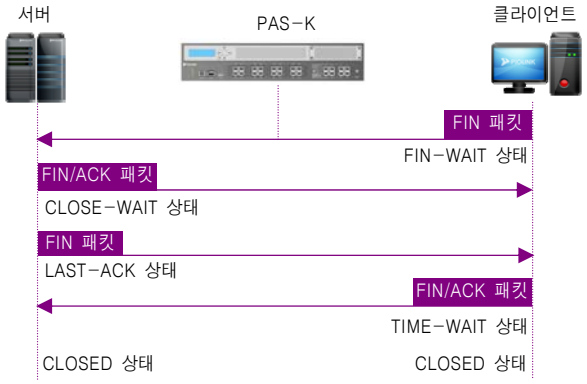
- **TCP-CLOSE 상태**
  TCP-CLOSE 상태는 서버와 클라이언트 사이에 형성된 TCP 세션이 종료된 상태이거나 세션 형성을 위해 SYN 요청 패킷을 보내거나 수신하기 전의 상태입니다. 아래 두 그림의 TIME-WAIT 상태에서 4 분 정도 경과하면 TCP-CLOSE 상태가 됩니다.

다음은 TCP 세션을 생성하기 위해 서버와 클라이언트 간 SYN 패킷 및 ACK 패킷을 전송하여 TCP 연결을 수립하는 과정을 통해 ESTABLISHED 상태가 되어 TCP 세션이 성립되는 과정을 보여주는 그림입니다. (SYN-SENT → SYN-RECEIVED → ESTABLISHED)



[그림 - TCP 세션에 대한 PAS-K 엔트리 상태 (TCP 세션 성립 과정)]

다음은 TCP 세션을 종료하기 위해 서버와 클라이언트 간 FIN 패킷, LAST-ACK 패킷 및 TIME-WAIT 패킷을 전송하여 TCP 연결을 종료하는 과정을 통해 CLOSED 상태가 되어 TCP 세션이 종료되는 과정을 보여주는 그림입니다. (FIN-WAIT → CLOSE-WAIT → LAST-ACK → TIME-WAIT → CLOSED)



[그림 - TCP 세션에 대한 PAS-K 엔트리 상태 (TCP 세션 종료 과정)]

UDP 세션

세션을 맺거나 종료할 때 handshaking 과정이 필요하지 않는 UDP 세션은 다음 2가지 세션 유지 시간을 설정할 수 있습니다.

- **UDP 세션 유지 시간**
  처음으로 UDP 요청 패킷을 받거나 혹은 응답을 보내기 전에 다시 요청 패킷을 받는 경우에 사용되는 UDP 세션에 대한 엔트리의 세션 유지 시간을 설정할 수 있습니다.
- **UDP STREAM 세션 유지 시간**
  PAS-K 는 UDP 요청 패킷을 받은 후 UDP 응답 패킷까지 받으면 UDP 세션을 UDP STREAM 세션으로 간주합니다. UDP STREAM 세션에 대한 세션 유지 시간을 설정할 수 있습니다.

세션 유지 시간의 기본 설정값

PAS-K는 기본적으로 각 세션과 세션의 상태에 대한 엔트리의 세션 유지 시간을 다음과 같은 값으로 설정합니다.

[표 - 세션 유지 시간의 기본 설정 값]

세션/세션 상태 유지 시간	기본값
ICMP	10초
TCP ESTABLISHED	3600초
TCP FIN-WAIT	20초
TCP CLOSE-WAIT	20초
TCP TIME-WAIT	20초
TCP SYN-RECEIVED	20초
TCP SYN-SENT	20초
TCP LAST-ACK	20초
TCP-CLOSE	20초
TCP-UNASSURED	20초
UDP	10초
UDP STREAM	180초
Generic	30초

세션 유지 시간의 값은 사용자가 원하는 값으로 변경할 수 있습니다. 다음 절에서 세션 유지 시간을 설정하는 방법에 대해 설명합니다.

CLI에서 설정하기

세션 유지 시간 설정

CLI에서 각 세션이나 세션 상태에 대한 엔트리의 세션 유지 시간 값을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**session-timeout**	<세션 유지 시간 설정 모드>로 들어갑니다.
2~5번 과정은 <세션 유지 시간 설정 모드>에서 엔트리의 세션 유지 시간을 설정하는 과정입니다. 설정하고자 하는 엔트리의 종류에 따라 해당 과정의 작업을 수행합니다. • ICMP 세션 엔트리 → 2번 • TCP 세션 엔트리 → 3번 • UDP 세션 엔트리 → 4번 • 그 외의 세션 엔트리 → 5번		
2	**icmp** *<ICMP>*	ICMP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<ICMP>* 설정 범위: 0~6000, 기본값: 10 (초)
3	**tcp-unassured** *<TCP-UNASSURED>*	'UNASSURED' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-UNASSURED>* 설정 범위: 0~6000, 기본값: 20 (초)
	tcp-established *<TCP-ESTABLISHED>*	'ESTSABLISHED' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-ESTABLISHED>* 설정 범위: 0~86400, 기본값: 3600 (초)
	tcp-close-wait *<TCP-CLOSE-WAIT>*	'CLOSE-WAIT' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-CLOSE-WAIT>* 설정 범위: 0~6000, 기본값: 20 (초)
	tcp-fin-wait *<TCP-FIN-WAIT>*	'FIN-WAIT' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-FIN-WAIT>* 설정 범위: 0~6000, 기본값: 20 (초)
	tcp-wait *<TCP-WAIT>*	'WAIT' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-WAIT>* 설정 범위: 0~6000, 기본값: 20 (초)
	tcp-last-ack *<TCP-LAST-ACK>*	'LAST-ACK' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-LAST-ACK>* 설정 범위: 0~6000, 기본값: 20 (초)
	tcp-syn-recv *<TCP-SYN-RECV>*	'SYN-RECEIVED' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-SYN-RECV>* 설정 범위: 0~6000, 기본값: 20 (초)
	tcp-syn-sent *<TCP-SYN-SENT>*	'SYN-SENT' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-SYN-SENT>* 설정 범위: 0~6000, 기본값: 20 (초)
	tcp-close *<TCP-CLOSE>*	'TCP-CLOSE' 상태인 TCP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<TCP-CLOSE>* 설정 범위: 0~6000, 기본값: 20 (초)
4	**udp** *<UDP>*	UDP 세션 엔트리의 세션 유지 시간을 변경합니다. • *<UDP>* 설정 범위: 0~6000, 기본값: 10 (초)
	udp-stream *<UDP-STREAM>*	UDP STREAM 세션 엔트리의 세션 유지 시간을 변경합니다. • *<UDP-STREAM>* 설정 범위: 0~6000, 기본값: 180 (초)
5	**generic** *<GENERIC>*	ICMP, TCP, UDP 세션 이외의 다른 세션 엔트리의 세션 유지 시간을 변경합니다. • *<GENERIC>* 설정 범위: 0~6000, 기본값: 30 (초)

6	**current**	설정한 세션이나 세션 상태에 대한 엔트리의 세션 유지 시간 정보를 확인합니다.
7	**apply**	설정된 엔트리의 세션 유지 시간 정보를 저장하고 시스템에 적용합니다.

세션 유지 시간 설정 정보 보기

현재 시스템의 세션 유지 시간 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show session-timeout** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

기술 지원 도우미

장비에 장애가 발생한 경우, 장애 발생 원인을 파악하기 위해서는 여러 차례 관련 정보 (장비 상태 정보 및 로그 정보)를 확인해야 합니다. 이러한 번거로움을 줄이기 위해 PAS-K는 기술 지원 도우미 기능을 지원합니다.

기술 지원 도우미는 PAS-K에 장애 발생 시, 다음과 같은 동작 로그 정보를 통합된 하나의 파일로 제공하는 기능입니다.

- 하드웨어 상태 정보
- CPU 사용량, 메모리 사용량 정보
- 시스템 정보
- 설정 정보(포트, 인터페이스, 라우팅, 부하 분산, Failover, SSL)
- 로그 정보

기술 지원 도우미 기능을 사용하면 장애 발생 시 쉽고 빠르게 정보를 확인하고 원인을 분석함으로써, 신속하게 장애에 대응할 수 있습니다.

이 절에서는 CLI를 통해 기술 지원 도우미 기능을 설정하는 방법에 대해 살펴봅니다.

CLI에서 설정하기

동작 로그 정보 설정

PAS-K의 동작 로그 정보를 TFTP 서버로 업로드 하려면, <Configuration 모드>에서 다음 명령을 사용합니다.

순서	명 령	설 명
1	**tech-assist**	<기술지원 도우미 설정 모드>로 들어갑니다.
2	**save**	동작 로그 정보를 PAS-K의 메모리에 저장합니다.
3	**copy-to** *<COPY-TO>*	PAS-K의 메모리에 저장되어 있는 동작 로그 정보를 TFTP 서버로 업로드합니다. • *<COPY-TO>* TFTP 서버의 IP 주소 및 경로. (경로는 TFTP 서버에 동작 로그 정보를 저장할 파일 또는 폴더의 이름)

참고: 동작 로그 정보가 저장된 날짜 및 시간 정보를 확인하려면, <Configuration 모드>에서 **show tech-assist** 명령을 사용합니다..

참고: 기술 지원 도우미로 생성된 파일을 외부로 보내기 위해서는 다음과 같은 형식으로 입력합니다.

```
(config)# tech-assist copy-to 1.1.1.1:/home/target
```

사용자 계정 및 인증

PAS-K는 HTTP, Telnet, 콘솔, SNMP 등을 통해 PAS-K로 접속하는 사용자를 인증하는 과정을 거칩니다. 이 절에서는 사용자 계정과 인증에 관련된 작업에 대해 살펴보고, CLI에서 설정하는 방법에 대해 설명합니다.

- 사용자 관리
- RADIUS 서버 설정

사용자 관리

CLI를 사용하여 PAS-K를 관리하려면 등록된 사용자 계정을 사용하여 로그인 과정을 거쳐야 합니다. PAS-K에는 기본적으로 ID가 'root'이고 패스워드가 'admin', 그리고 사용자 레벨이 'super user'인 기본 사용자가 등록되어 있습니다.

이 절에서는 CLI에서 새로운 사용자를 등록하는 방법과 등록된 사용자의 정보를 수정 및 삭제하는 방법 등을 살펴봅니다.

CLI에서 사용자 관리하기

사용자 추가

새로운 사용자를 추가하려면 <Configuration 모드>에서 다음 명령을 실행합니다. PAS-K에는 기본적으로 등록되어 있는 'root' 사용자를 포함하여 최대 20명의 사용자를 등록할 수 있습니다.

순서	명 령	설 명
1	**user** *<NAME>*	<사용자 설정 모드>로 들어갑니다. • *<NAME>* 최대 8 자의 알파벳, 숫자, '-', '_' 문자로 이루어진 문자열로 지정. 첫 글자는 반드시 알파벳 사용
2	**password** *<PASSWORD>*	패스워드를 설정합니다 • *<PASSWORD>* 5 ~ 20 문자 사이의 알파벳, 숫자, 특수문자 조합으로 구성
3	**level {superuser | user}**	사용자의 레벨을 설정합니다. • **superuser** <Configuration 모드>로 접속하여 PAS-K 의 설정이 가능한 사용자 • **user** <Configuration 모드>로 접속이 불가능하여 PAS-K 의 설정을 변경할 수 없으며 모니터링만 가능한 사용자 (기본값:)
4	**description** *<DESCRIPTION>*	사용자에 대한g 설명을 입력합니다. • *<DESCRIPTION>* 사용자에 대한 추가적인 설명을 최대 64 자까지 입력 가능.
5	**current**	설정한 사용자 정보를 확인합니다.
6	**apply**	설정한 사용자 정보를 저장하고 시스템에 적용합니다.

참고: 패스워드는 가급적이면 대소문자와 숫자 등을 조합하여 만들기를 권장합니다.

참고: 설정되어 있는 사용자의 패스워드와 레벨, 설명을 변경하는 방법은 사용자 추가 방법과 동일합니다. root 사용자 ID를 사용하여 최초로 로그인한 경우에는 보안을 위해 반드시 패스워드를 변경하도록 합니다.

참고: 지정한 사용자 레벨과 사용자에 대한 설명을 삭제하려면 <사용자 설정 모드>에서 다음과 같은 명령을 사용합니다.

```
(config-user[admin])# no level
(config-user[admin])# no description
```

사용자 삭제

PAS-K에 등록된 사용자를 삭제하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
no user *<NAME>*	사용자를 삭제합니다. • *<NAME>* 삭제할 사용자 이름.

주의: PAS-K에 기본으로 등록되어 있는 사용자 ID 'root'는 삭제할 수 없습니다.

사용자 보기

설정된 사용자의 이름과 레벨 등 사용자에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show user** 명령을 사용합니다. 특정 사용자에 대한 정보만 확인하려면, **show user** 명령 뒤에 사용자 이름(*<NAME>*)을 입력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

RADIUS 서버 설정

PAS-K는 RADIUS(Remote Authentication Dial In User Service) 서버를 이용하여 텔넷, 웹 또는 콘솔 등을 통한 외부 접속에 대해 사용자 인증 기능을 제공합니다. 사용자는 RADIUS 서버와 PAS-K간의 통신 시 사용할 TCP 포트를 지정하고, 인증에 사용되는 인증 키 값을 설정합니다.

만약 외부로부터 PAS-K에 접속 요청이 오면, PAS-K는 RADIUS 서버로 사용자 정보를 보냅니다. 그러면 RADIUS 서버는 설정한 인증 키(secret key) 값과 사용자 정보를 확인하여 접속을 허용할지 여부를 PAS-K에게 알려줍니다. 인증이 완료된 후 사용자는 PAS-K로 접속할 수 있습니다.

CLI에서 설정하기

CLI에서 RADIUS 서버를 설정 하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**radius**	<RADIUS 설정 모드>로 이동합니다.
2	**primary-server** *<PRIMARY-SERVER>*	기본 RADIUS 서버를 설정합니다 • *<PRIMARY-SERVER>* 기본 RADIUS 서버의 IP 주소 **참고**: 설정한 기본 RADIUS 서버를 삭제하려면 **no primary-server** 명령을 사용합니다.
3	**secondary-server** *<SECONDARY-SERVER>*	기본 RADIUS 서버가 정상적으로 동작하지 않는 경우에 사용되는 보조 RADIUS 서버를 설정합니다 • *<SECONDARY-SERVER>* 보조 RADIUS 서버의 IP 주소 **참고**: 설정한 보조 RADIUS 서버를 삭제하려면 **no secondary-server** 명령을 사용합니다.
4	**port** *<PORT>*	RADIUS 서버와 PAS-K간의 통신 시 사용할 TCP 포트를 설정합니다. • *<PORT>* RADIUS 서버와 통신 할 포트 번호 설정 범위: 1500~3000, 기본값: 1812
5	**secret** *<SECRET>*	RADIUS 서버와 PAS-K와의 인증에 사용되는 인증 키 값을 설정합니다. • *<SECRET>* 인증 시 사용할 인증 키 값. 알파벳과 숫자, 특수문자 입력 가능. **참고**: 설정한 인증 키를 삭제하려면 **no secret** 명령을 사용합니다.
6	**timeout** *<TIMEOUT>*	RADIUS 서버 응답 타임아웃을 설정합니다. • *<TIMEOUT>* RADIUS 서버 타임아웃 시간 설정 범위: 1~10, 기본값: 3 (초)
7	**retry** *<RETRY>*	RADIUS 서버의 응답이 없을 때 RADIUS 서버와 접속을 위해 다시 시도할 접속 횟수를 설정합니다. • *<RETRY>* RADIUS 서버 재 접속 시도 횟수 설정 범위: 1~5, 기본값: 3 (회)
8	**ssh** {**enable** | **disable**}	SSH 를 통해 PAS-K 에 접속 시 RADIUS 서버 인증 사용 여부를 지정합니다. • **enable** SSH 접속에 대한 인증 기능 활성화 • **disable** SSH 접속에 대한 인증 기능 비활성화 (기본값)
9	**telnet** {**enable** | **disable**}	텔넷을 통해 PAS-K 접속 시 RADIUS 서버 인증 사용 여부를 지정합니다. • **enable** 텔넷 접속에 대한 인증 기능 활성화 • **disable** 텔넷 접속에 대한 인증 기능 비활성화 (기본값)

10	**console {enable | disable}**	콘솔을 통해 PAS-K 접속 시 RADIUS 서버 인증 사용 여부를 지정합니다. • **enable** 콘솔 접속에 대한 인증 기능 활성화 • **disable** 콘솔 접속에 대한 인증 기능 비활성화 (기본값)
11	**status {enable | disable}** (선택 설정)	RADIUS 기능의 사용 여부를 지정합니다. • **enable** RADIUS 기능 활성화 • **disable** RADIUS 기능 비활성화 (기본값)
12	**current**	설정한 RADIUS 서버 설정 정보를 확인합니다.
13	**apply**	RADIUS 설정을 PAS-K에 적용합니다.

설정 정보 보기

현재 PAS-K에 정의된 RADIUS 서버의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show radius** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

로그 관리

이 절에서는 PAS-K에서 제공하는 로그 관련 기능에 대해 소개한 후 CLI를 통하여 로그 메시지를 조회하거나 로그 메시지의 전송 방식을 설정하는 방법에 대해 설명합니다.

로그 개요

PAS-K는 장비에 문제가 생기거나 설정이 변경되는 등의 이벤트가 발생하면 이벤트에 대한 정보가 담긴 로그 메시지를 생성합니다. 생성된 로그 메시지는 시간과 함께 버퍼에 저장되어 사용자가 필요한 경우에 조회할 수 있습니다.

이벤트의 종류와 레벨

버퍼의 용량이 한정적이기 때문에 이를 효율적으로 사용하기 위해서 사용자는 로그 메시지를 생성하는 이벤트의 종류와 레벨을 지정하여 특정 이벤트에 대한 로그 정보나 지정한 레벨보다 높은 레벨의 로그 정보만 저장할 수 있습니다.

PAS-K에서 로그 메시지를 생성하는 이벤트에는 다음과 같은 13가지 종류가 있습니다.

[표 - 이벤트 종류]

이벤트 종류	설 명
auth	보안 및 인증 관련 이벤트
authpriv	개인적 보안 및 인증 관련 이벤트
cron	클럭(clock), 데몬(cron, at) 관련 이벤트
daemon	일반 시스템 데몬 관련 이벤트
ftp	FTP(file transfer protocol) 관련 이벤트
kern	커널 이벤트
local0-7	로컬 시스템을 위해 예약된 영역 관련 이벤트
lpr	프린트 관련 이벤트
mail	메일 관련 이벤트
news	뉴스 서버 관련 이벤트
syslog	시스로그에 의해 생성되는 내부 이벤트
user	일반적인 사용자 레벨 이벤트
uucp	UNIX-to-UNIX copy 관련 이벤트

이러한 이벤트들 중에서 로그 메시지를 생성할 이벤트를 사용자가 선택할 수 있습니다. 기본적으로는 모든 이벤트들에 대한 로그 메시지가 생성되도록 설정되어 있습니다.

PAS-K는 이벤트는 장비에 영향을 주는 정도에 따라 다음과 같은 8개의 레벨로 나눠집니다.

[표 - 이벤트 레벨]

키워드	레 벨	설 명
emergency	0	시스템에 치명적인 이벤트
alert	1	즉시 조치를 취해야 할 이벤트
critical	2	중요한 이벤트

error	3	에러 메시지
warning	4	경고 메시지
notice	5	중요하지 않은 일반 이벤트
information	6	정보에 해당하는 이벤트
debug	7	디버깅 관련 이벤트

레벨 번호가 가장 낮은 emergency 레벨(레벨 0)이 가장 중요도가 높은 이벤트이며, 레벨 번호가 높아질수록 중요도가 낮아지는 이벤트입니다. 기본적으로 PAS-K는 notice 레벨 이상의 이벤트가 발생한 경우에 로그 메시지를 생성합니다. 로그 메시지를 생성할 이벤트의 레벨은 사용자가 임의로 설정할 수 있습니다.

로그 메시지 전송

로그 메시지는 장비에 발생한 문제를 발견하고 해결하는데 중요한 역할을 합니다. 그런데, 저장 공간이 가득 차면 로그 메시지가 삭제되기 때문에 중요한 정보를 잃을 수 있습니다. 이러한 문제를 방지하기 위해 PAS-K는 주기적으로 로그 메시지를 미리 등록된 이메일 주소와 시스로그 서버로 전송하는 기능을 제공합니다. 네트워크 관리자의 이메일 주소를 등록해두면 네트워크 관리자는 전송 받은 로그 메시지를 통해 빠르고 효과적으로 장비에 발생한 문제를 발견하고 해결할 수 있습니다. 외부의 시스로그 서버로 로그 메시지를 전송하도록 설정해두면 외부에서도 로그 메시지를 확인할 수 있어 편리합니다.

CLI에서 설정하기

이벤트 레벨 설정

로그 메시지를 생성하는 이벤트 종류와 레벨을 지정하려면 <Configuration 모드>에서 다음 명령을 사용합니다.

순서	명 령	설 명
1	**logging**	<로그 설정 모드>로 이동합니다.
2	**facility** {**all** | **auth** | **authpriv** | **cron** | **deamon** | **ftp** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**}	로그 메시지를 생성하는 이벤트 종류를 설정합니다. (기본값: all)
3	**level** {**alert** | **crit** | **debug** | **emerg** | **error** | **info** | **notice** | **warning**}	로그 메시지를 생성하는 이벤트 레벨을 설정합니다. (기본값: notice)

참고: 이벤트 레벨을 지정하면 지정한 레벨보다 높은 레벨의 로그 정보만 저장됩니다. 예를 들어 critical 레벨을 지정하면 critical, alert, emergency 레벨의 로그 정보들이 저장됩니다. Debug 레벨을 지정하면 모든 레벨의 로그 정보들이 저장됩니다.

참고: 설정한 로그 메시지를 생성하는 이벤트 종류 및 레벨을 기본값으로 변경하려면 <로그 설정 모드>에서 다음과 같은 명령을 사용합니다.

```
(config-logging)# no facility
(config-logging)# no level
```

시스로그 서버 설정

시스로그 서버로 로그 메시지를 전송하기 위해서는 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**logging**	<로그 설정 모드>로 이동합니다.
2	**server** *<IPADDR>* [**facility** *<FACILITY>* | **level** *<LEVEL>* | **agent-facility** *<AGENT-FACILITY>*]	시스로그 서버와 전송할 로그 메시지 종류를 설정합니다 • *<IPADDR>* 시스로그 서버의 IP 주소 • *<FACILITY>* 전송할 로그 메시지의 이벤트 종류 • *<LEVEL>* 전송할 로그 메시지의 이벤트 레벨 • *<AGENT-FACILITY>* 전송된 로그 메시지를 저장할 때 지정할 이벤트 종류
3	**server-status** {**enable** | **disable**}	로그 메시지 전송 기능의 사용 여부를 지정합니다. • **enable** 로그 메시지 전송 기능 활성화 • **disable** 로그 메시지 전송 기능 비활성화 (기본값)

참고: PAS-K에는 최대 24개의 시스로그 서버를 등록할 수 있습니다.

참고: 추가한 시스로그 서버를 삭제하려면, <로그 설정 모드>에서 **no server** *<IPADDR>* 명령을 사용합니다. 해당 명령을 사용하면, 동일한 IP 주소를 갖는 시스로그 서버는 모두 삭제됩니다.

이메일 알람 설정

이메일로 로그 메시지를 전송하기 위해서는 <Configuration 모드>에서 다음의 과정을 수행합니다.

순서	명 령	설 명
1	**email-alarm** *<ID>*	<이메일 알람 설정 모드>로 들어갑니다. • *<ID>* 이메일 알람 ID. 설정 범위: 1 ~ 8
2	**from** *<FROM>*	로그 메시지를 보내는 사람의 이메일 주소를 설정합니다. • *<FROM>* 이메일 송신자 주소. 하나의 이메일 주소만 설정 가능 **참고**: 설정한 송신자 이메일 주소를 삭제하려면 **no from** 명령을 사용합니다.
3	**to** *<TO>*	로그 메시지를 받는 사람의 이메일 주소를 설정합니다. • *<TO>* 이메일 수신자 주소. 하나의 이메일 주소만 설정 가능 **참고**: 설정한 수신자 이메일 주소를 삭제하려면 **no to** 명령을 사용합니다.
4	**smtp** *<SMTP>*	SMTP 서버의 IP 주소를 설정합니다. • *<SMTP>* SMTP 서버 IP 주소. 하나의 SMTP 서버만 설정 가능 **참고**: 설정한 SMTP 서버를 삭제하려면 **no smtp** 명령을 사용합니다.
5	**status {enable | disable}**	로그 메시지 이메일 전송 기능의 사용 여부를 지정합니다. • **enable** 로그 메시지 전송 기능 활성화 • **disable** 로그 메시지 전송 기능 비활성화 (기본값)
6	**current**	설정한 이메일 알람 설정 정보를 확인합니다.
7	**apply**	이메일 알람 설정을 시스템에 저장합니다.

참고: 추가한 이메일 알람 설정을 삭제하려면, <Configuration 모드>에서 **no email-alarm** *<ID>* 명령을 사용합니다.

시스로그 정보 이메일 전송 설정

시스로그 정보를 이메일로 전송하기 위해서는 <이메일 알람 설정 모드>에서 다음의 과정을 수행합니다.

순서	명 령	설 명
1	**syslog**	<시스로그 설정 모드>로 들어갑니다.
2	**interval** *<INTERVAL>*	시스로그 정보 전송 주기를 설정합니다. • *<INTERVAL>* 시스로그 정보 전송 주기. 설정 범위: 1 ~ 300, 기본값: 60(초) **참고**: 설정한 전송 주기를 기본값으로 변경하려면 **no interval** 명령을 사용합니다.
3	**log-level {crit | debug | err | info | notice | warning}**	전송할 시스로그 레벨을 설정합니다. 설정한 레벨 이상의 로그만 전송합니다. 기본값: notice **참고**: 설정한 로그 레벨을 기본값으로 변경하려면 **no log-level** 명령을 사용합니다.
4	**status {enable | disable}**	시스로그 정보 이메일 전송 기능의 사용 여부를 지정합니다. • **enable** 시스로그 정보 전송 기능 활성화 • **disable** 시스로그 정보 전송 기능 비활성화 (기본값)
5	**current**	설정한 시스로그 정보 이메일 전송 설정 정보를 확인합니다.
6	**apply**	시스로그 정보 이메일 전송 설정을 시스템에 저장합니다.

로그 설정 정보 보기

현재 시스템의 로그 설정 정보를 보려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show logging** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

이메일 알람 설정 정보 보기

현재 시스템의 이메일 알람 설정 정보를 보려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show email-alarm** [*<ID>*] 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

로그 출력

PAS-K에 저장되어 있는 로그 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
show log [**fix-level** *<LOG_LEVEL>* | **imply-lelvel** *<LOG_LEVEL>* | **keyword** *<STRING>*]	저장되어 있는 로그 메시지 중 다음과 같은 일부의 메시지만 출력합니다. - Failover 발생 정보 - 사용자 로그인/로그아웃 정보 - 장애 감시 결과 변경 정보 - 포트 상태 변화 정보 - CPU/메모리 사용률 정보 - 부팅 동작 정보(부팅완료, 설정복구시작, 리부팅) - SNMP Trap 정보 - 사용자 추가/삭제 정보 - 전원 상태 정보 - 웹 로그인 정보 • **fix-level** 지정한 레벨의 로그만 출력합니다. • *<LOG_LEVEL>* 로그 레벨. (info, debug, error, notice, warning, critical) • **imply-level** 지정한 레벨 이상의 로그만 출력합니다. • **keyword** 지정한 문자열이 포함된 로그만 출력합니다. • *<STRING>* 검색할 문자열
show log-detail [**fix-level** *<LOG_LELVEL>* | **imply-lelvel** *<LOG_LELVEL>* | **keyword** *<STRING>*]	저장되어 있는 모든 로그 메시지를 출력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

로그 삭제

PAS-K에 저장되어 있는 모든 로그를 삭제하려면, <Configuration 모드>에서 **no log** 명령을 사용합니다.

포트 모니터링

PAS-K는 포트의 실시간 트래픽 정보를 조회할 수 있는 포트 모니터링 기능을 제공합니다. 이 절에서는 CLI를 통하여 포트의 실시간 트래픽 정보를 모니터링하는 방법에 대해 설명합니다.

CLI에서 모니터링하기

포트 모니터링 정보를 출력하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show port-monitoring** 명령을 사용합니다. 이 명령을 실행하면 각 포트가 초당 송수신하는 트래픽 정보를 실시간으로 확인할 수 있습니다. 다음은 **show port-monitoring** 명령을 실행했을 때 출력되는 결과를 보여주는 예입니다.

```
(config)# show port-monitoring
================================================================================
PORT-MONITORING
--------------------------------------------------------------------------------
  Port-Monitoring
   Name  RxRate(bps)    RxRate(pps)    TxRate(bps)    TxRate(pps)
   ge1   983987200      120124         983994808      120123
   ge2   983987200      120124         983994808      120124
   ge3   0              0              0              0
   ge4   0              0              0              0
   ge5   0              0              0              0
   ge6   0              0              0              0
   ge7   0              0              0              0
   ge8   0              0              0              0
   xg1   983987200      120123         983994808      120123
   xg2   0              0              0              0
   xg3   983987200      120123         983987200      120123
   xg4   0              0              0              0
   xg5   0              0              0              0
   xg6   0              0              0              0
   xg7   0              0              0              0
   xg8   0              0              0              0
   xg9   0              0              0              0
   xg10  0              0              0              0
   xg11  0              0              0              0
   xg12  0              0              0              0
   xg13  0              0              0              0
   xg14  0              0              0              0
   xg15  0              0              0              0
   xg16  0              0              0              0
================================================================================
```

show port-monitoring 명령을 실행하여 출력된 각 항목은 다음과 같은 정보를 보여줍니다.

[표 - 포트 모니터링 정보]

항 목	설 명
Name	포트 이름
RxRate(bps)	해당 포트가 초당 수신한 비트 수
RxRate(pps)	해당 포트가 초당 수신한 패킷 수
TxRate(bps)	해당 포트가 초당 송신한 비트 수
TxRate(pps)	해당 포트가 초당 송신한 패킷 수

시스템 감시

시스템 감시 기능은 PAS-K의 CPU, 메모리와 같이 주요한 시스템 자원의 사용 상태를 감시하는 기능입니다. 일정 시간마다 시스템 자원(CPU와 메모리의 사용률)의 사용 상태를 확인하고, 각 자원의 사용률이 90%를 초과할 경우, 로그 메시지를 출력하여 시스템 관리자에게 자원의 사용 상태를 알려줍니다. 시스템 감시 기능을 통해 기록되는 로그의 이벤트 레벨은 **Warning**(경고 메시지)입니다. 시스템 감시 기능을 통해 기록된 로그 메시지를 확인하는 방법은 **제4장 시스템 관리와 모니터링** - **로그 관리**를 참고합니다.

참고: 시스템 감시 기능은 PAS-K에서 기본으로 제공하는 기능으로 사용 여부를 설정할 수 없습니다.

명령 사용 이력 조회

명령 사용 이력 조회는 사용자가 콘솔, Telnet, SSH를 통해 PAS-K의 CLI에 로그인한 후 실행한 명령을 조회하는 기능입니다. 명령 사용 이력은 최대 100개까지 출력되며, CLI에서 로그아웃하면 해당 이력이 삭제됩니다.

명령 사용 이력을 조회하려면 다음 명령을 실행합니다. 해당 명령은 전역 명령이므로 어떤 명령 모드에서도 사용 가능합니다.

명 령	설 명
history	사용자가 로그인 후 실행한 명령을 조회합니다.

FAN Hot Swap

PAS-K는 운용 중 팬에 장애가 발생한 경우, 전원을 끄지 않고 FAN을 교체할 수 있는 FAN Hot Swap 기능을 지원합니다. FAN Hot Swap 기능을 통해 FAN을 교체하려면 <Configuration 모드>에서 다음 명령을 사용하여 FAN 동작을 정지 시킨 후 FAN을 교체합니다.

명 령	설 명
fan-hotswap status enable	FAN 동작을 정지합니다.

주의: FAN을 교체한 후에는 반드시 **fan-hotswap status disable** 명령을 사용하여 FAN을 다시 동작시켜야 합니다.

참고: FAN Hot Swap 기능은 PAS-K 2400/2800/4200/4400 제품에서만 지원합니다.

제5장
SNMP 설정

이 장에서는 SNMP (Simple Network Management Protocol)에 대해 살펴본 후 PAS-K에 SNMP를 설정하는 방법에 대해 소개합니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- SNMP 개요
- SNMP 설정

SNMP 개요

SNMP는 네트워크 관리 시스템(NMS)과 네트워크 장비 간의 관리 정보 통신에 사용되는 표준 프로토콜입니다. SNMP는 OSI 모델의 상위 계층인 L7 애플리케이션 층에 속합니다. 네트워크 관리자는 SNMP를 이용하여 다음과 같은 관리를 원격으로 수행할 수 있습니다.

- **네트워크 구성 관리**
  전체 네트워크를 구성하거나 구조를 쉽게 알 수 있습니다.
- **성능 관리**
  각 네트워크 세그먼트 간의 네트워크 사용량, 에러 발생 회수, 처리 속도, 응답 시간 등 성능 분석에 필요한 통계 정보를 얻을 수 있습니다.
- **장비 관리**
  장비의 동작 상태와 포트, 전원, 냉각 팬 등의 각 모듈 상태, CPU, 메모리, 디스크 사용량 등의 시스템 정보를 얻을 수 있습니다. 이러한 정보는 네트워크 상에서 발생한 장비의 문제를 해결하는데 큰 도움을 줍니다.
- **보안 관리**
  SNMP 는 장비의 MIB 정보를 제어하고 보호할 수 있는 보안 기능을 지원합니다. 특히, 최근 버전인 SNMP v3 에서는 보안 기능이 크게 강화되었습니다.

SNMP 구성 요소

SNMP는 크게 다음과 같은 세 가지 요소로 구성됩니다.

- SNMP 매니저(Manager)
- SNMP 에이전트(Agent)
- MIB(Management Information Base)

각 요소에 대해 좀 더 살펴봅니다.

SNMP 매니저

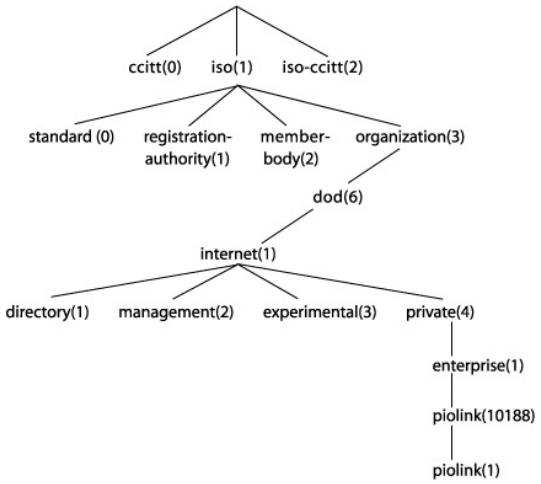
SNMP 매니저는 사용자가 전체 네트워크의 상태를 확인할 수 있는 인터페이스 역할을 합니다. SNMP 매니저는 SNMP 에이전트와의 통신을 통하여 MIB에 있는 장비의 정보를 얻어 네트워크 장비를 모니터링할 수 있고, SNMP 에이전트에게 동작 요청을 보내 장비의 설정을 수정할 수 있습니다.

SNMP 에이전트

SNMP 에이전트는 스위치, 라우터, UNIX 워크스테이션, 프린터 등 네트워크 장비에 내장되어 있는 소프트웨어 모듈입니다. SNMP 에이전트는 SNMP 매니저로부터 정보 요청을 받으면 MIB으로부터 해당 정보를 수집하여 UDP 161 포트를 통해 SNMP 매니저에게 전송합니다. 설정을 변경하는 요청을 받으면 SNMP 에이전트는 해당하는 MIB의 값을 변경합니다. 그리고, SNMP 매니저의 요청을 받지 않은 경우에도, 사용자 인증 오류가 발생하거나, 시스템이 재시작하거나, 이웃 장비 간의 연결이 끊기는 등의 중요한 이벤트가 발생하면, SNMP 에이전트는 트랩(trap)을 발생하여 UDP 162 포트를 통해 SNMP 매니저에게 전달합니다.

SNMP MIB

SNMP MIB은 시스템 정보, 네트워크 사용량, 네트워크 인터페이스 정보 등 네트워크 장비를 관리하기 위한 정보를 포함하고 있는 데이터베이스입니다. MIB에 저장되어 있는 각 정보들을 객체(object)라고 합니다. MIB의 이런 객체들은 관리하기 편하도록 다음의 그림과 같은 계층적 트리 구조로 이루어져 있습니다.



[그림 – MIB 트리 구조]

MIB의 계층 구조에서 맨 윗부분은 네트워크 브로드캐스트 정보를 나타냅니다. 하위에 있는 객체는 상위에 있는 객체보다 더 구체적인 객체입니다. MIB의 각 객체 옆에 있는 숫자는 원하는 데이터를 가져올 때 사용되는 OID 번호입니다. 예를 들면, enterprise의 OID 값은 1.3.6.1.4.1 이 됩니다.

MIB은 계층적 구조를 가지므로 확장이 가능합니다. 표준 MIB에서 제공하지 않는 정보를 모니터링하려는 경우에는 사설 MIB을 추가할 필요가 있습니다. 이런 사설 MIB은 private(4)의 enterprises(1)에 정의하여 사용할 수 있습니다.

MIB의 버전에는 MIB-I과 MIB-II가 있습니다. MIB-II는 MIB-I의 확장판으로 MIB-I의 모든 객체를 포함하여 약 171개의 객체들을 더 포함하고 있습니다.

참고: PAS-K에서 제공하는 MIB은 이 설명서와 함께 제공되는 MIB 설명서를 참고하도록 합니다.

참고: PAS-K에서 제공하는 표준 MIB에는 MIB-II와 UCD-SNMP가 있습니다.

참고: PAS-K가 지원하는 MIB-II에는 시스템 정보, 인터페이스 정보(32비트 타입, 64비트 타입)가 있고, UCD-SNMP에는 CPU 정보와 메모리 정보가 있습니다.

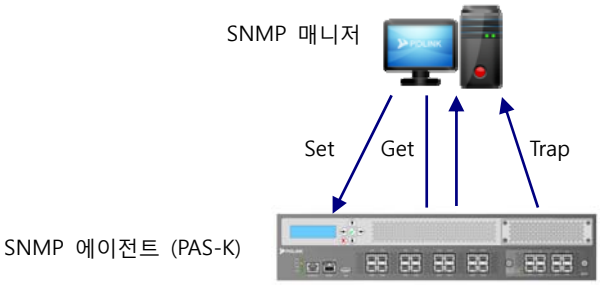
SNMP 매니저와 에이전트의 통신

인증

SNMP 매니저가 SNMP 에이전트에 접속하여 MIB 정보를 받아오거나 MIB 값을 변경하려면 인증 과정을 거쳐야 합니다. 인증 과정을 위해 SNMP v1과 v2에서는 커뮤니티(community)를 사용하고, SNMP v3에서는 사용자 ID와 MD5 암호, DES 암호를 사용합니다. PAS-K에는 기본적으로 읽기, 쓰기 권한을 가진 커뮤니티인 **public**이 설정되어 있고, SNMP v3용 사용자는 정의되어 있지 않습니다.

통신 명령

SNMP 매니저와 에이전트 사이의 통신은 기본적으로 정보를 요청하는 메시지와 이에 대한 응답메시지로 이루어집니다. 다음은 SNMP 매니저와 에이전트 사이의 통신을 나타내는 그림입니다.



[그림 – SNMP 매니저와 에이전트 사이의 통신]

SNMP 매니저와 에이전트 사이의 통신에 사용되는 명령들은 다음과 같습니다.

- **Get**
  Get 명령은 SNMP 매니저가 SNMP 에이전트에게 정보를 요청할 때 사용됩니다. SNMP 에이전트는 SNMP 매니저로부터 요청을 받으면 요청받은 정보를 MIB 으로부터 수집하여 SNMP 매니저에게 전송합니다.
- **Get Next**
  Get Next 명령은 Get 명령처럼 SNMP 에이전트에게 정보를 요청할 때 사용됩니다. 그러나 Get Next 명령을 사용하면 Get 명령과 달리 요청한 특정 정보만 가져오는 것이 아니라 oid 다음 항목의 정보를 가져올 수 있습니다.
- **Set**
  Set 명령은 SNMP 매니저가 SNMP 에이전트에게 MIB 객체의 특정 값을 설정하도록 요청할 때 사용됩니다. SNMP 에이전트는 SNMP 매니저로부터 설정을 변경하는 요청을 받으면 해당하는 MIB 의 값을 변경합니다.
- **트랩**
  트랩은 SNMP 매니저의 요청이 없어도 사용자 인증 오류가 발생하거나, 하드웨어에 이상이 발생하거나, 이웃 장비간의 연결이 끊기는 등의 중요한 이벤트가 발생하면, SNMP 에이전트가 SNMP 매니저에게 전달하는 메시지입니다. 트랩이 활성화 상태인 경우에만 해당하는 이벤트가 발생하면 트랩 메시지를 전달합니다. 특정 트랩 호스트를 지정하면 SNMP 에이전트는 지정한 트랩 호스트에게만 트랩 메시지를 전달합니다.

Generic 트랩

PAS-K는 다음과 같은 이벤트가 발생될 때 트랩 메시지를 전송하는 Generic 트랩을 제공합니다.

- MIB 이 수정되었거나 SNMP 가 활성화될 때
- Link 가 Up/Down 되었을 때

로드 타임아웃

SNMP 에이전트에 요청이 전달되면, SNMP 에이전트는 SNMP 매니저로 응답을 보냅니다. SNMP 매니저가 요청을 보낼 때마다 SNMP 에이전트가 MIB으로부터 새로운 정보를 받아서 응답하면 시스템 자원이 과도하게 사용될 수 있습니다. 이런 현상을 방지하기 위해 SNMP 에이전트가 SNMP 매니저의 요청에 대해 새로운 값을 전송하기까지 대기하는 시간(로드 타임 아웃)을 설정할 수 있습니다. 로드 타임 아웃 값을 설정하면, SNMP 에이전트는 지정한 로드 타임 아웃 시간내에 수신한 같은 항목에 대한 요청이 오면 이전에 전달했던 같은 정보를 전송하게 됩니다.

SNMP 버전

PAS-K에서 지원하는 SNMP 버전은 다음과 같습니다.

- **SNMP v1**
  SNMP 버전 1 은 RFC 1157 에 정의되어 있습니다. SNMP 버전 1 에서는 기본적인 MIB-I 과 MIB-II 를 간략하게 정의하였으며, 시스템, 네트워크, 애플리케이션, 서비스 등에 대한 내용을 포함하고 있습니다. SNMP 버전 1 은 커뮤니티 기반의 보안 기능을 지원하며, SNMP 매니저와 에이전트의 커뮤니티 이름이 매칭되어야만 SNMP 매니저와 에이전트 사이의 통신이 가능하게 합니다. 하지만, 라우팅 테이블처럼 많은 열이 존재하는 오브젝트의 경우, 전체 테이블을 읽고 싶을 때 수많은 요청 및 응답을 반복해야 하며, NMS 관리자 간 통신이 불가능한 문제점이 존재합니다.
- **SNMP v2**
  SNMP 버전 2 는 RFC 1902 에 정의되어 있습니다. SNMP 버전 2 에서는 SNMP 버전 1 의 내용을 포함하고 있을 뿐만 아니라, 데이터 종류, 카운터 크기, 프로토콜 동작 등을 추가하여 보안과 접근 제어(access control) 기능을 강화하였습니다. SNMP 버전 2 는 버전 1 과 같이 커뮤니티 기반의 보안 기능을 지원합니다.
- **SNMP v3**
  SNMP 버전 3 은 가장 최근의 SNMP 버전이며, RFC 2571~ 2575 에 정의되어 있습니다. SNMP 버전 3 에서는 비밀키를 이용하여 사용자 인증을 거친 후 장비에 접근하도록 하고, 데이터를 암호화하여 보안 기능을 크게 강화하였습니다.

참고: SNMP 매니저와 에이전트의 버전이 동일한 경우에만 둘 사이의 통신이 이루어집니다. 그러므로 사용자는 SNMP 에이전트가 지원하는 버전에 따라 SNMP 매니저의 버전을 설정해야 합니다. SNMP 에이전트 역할을 하는 PAS-K는 3개 버전의 SNMP를 동시에 활성화할 수 있습니다. 그러므로 SNMP 매니저가 여러 개인 경우에는, 각 SNMP 매니저에 서로 다른 버전의 SNMP를 설정하여 같은 버전의 SNMP 에이전트와만 통신하도록 할 수 있습니다.

SNMP 설정

설정하기 전에

SNMP 설정 항목

다음은 PAS-K에서 SNMP 기능을 사용하기 위해 설정할 수 있는 항목들입니다.

- SNMP 동작 상태
- SNMP 커뮤니티
- SNMP 사용자
- SNMP 로드 타임아웃
- SNMP 트랩 호스트
- SNMP Generic 트랩
- 장비 정보(이름, 연락처, 위치)

기본 설정

SNMP 항목들의 기본 설정 값은 다음과 같습니다.

[표 - SNMP 기본 설정]

항 목	설 명
SNMP 동작 상태	비활성화
SNMP 커뮤니티	없음
SNMP 사용자	없음
SNMP 로드 타임아웃	60초
SNMP Generic 트랩	비활성화
SNMP 트랩 호스트	없음
장비 정보	없음

SNMP 설정 시 주의 사항–SNMP의 동작 상태와 SNMP 설정 값의 적용

기본적으로 SNMP 항목들은 SNMP의 활성화 여부에 관계 없이 설정을 변경할 수 있습니다. SNMP가 활성화된 상태에서 설정을 변경한 경우에는 변경된 설정이 즉시 SNMP의 동작에 적용되고, SNMP 비활성화된 경우에는 변경 사항이 저장되었다가 SNMP가 활성화될 때 적용됩니다.

CLI에서 설정하기

이 절에서는 CLI 명령을 사용하여 SNMP 기능을 설정하는 방법을 살펴봅니다.

SNMP 커뮤니티 설정

SNMP 커뮤니티는 SNMP 에이전트로 접속할 때, 접속 허용여부, 읽기/쓰기 권한 등을 확인하는데 사용되는 암호 역할을 하는 문자열입니다. 기본으로 설정된 커뮤니티는 없습니다.

SNMP v1과 v2에서 인증 시 사용할 SNMP 커뮤니티를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 8개의 SNMP 커뮤니티를 설정할 수 있습니다. 여러 개의 SNMP 커뮤니티를 설정하려는 경우에는 다음 과정은 반복하면 됩니다.

순서	명 령	설 명
1	**snmp**	<SNMP 설정 모드>로 들어갑니다.
2	**community** *<NAME>*	SNMP 커뮤니티 이름을 지정하고, <Community 설정 모드>로 들어갑니다. • *<NAME>* SNMP 커뮤니티 이름을 1~254자 사이의 알파벳 대/소문자, 숫자, 특수 문자(' ', '\' 제외)로 이루어진 문자열로 지정. 첫 글자는 반드시 알파벳 사용
3	**policy {read-only | read-write}**	SNMP 커뮤니티의 권한을 지정합니다. • **read-only** 읽기만 허용(기본값) • **read-write** 읽기/쓰기 모두 허용
4	**limit-oid** *<LIMIT-OID>* (선택 설정)	SNMP 커뮤니티가 접근할 수 있는 OID 를 지정합니다. OID 를 지정하면 해당 OID 이하의 OID 만 접근할 수 있습니다. • *<LIMIT_OID>* 접근할 수 있는 OID를 알파벳 대/소문자, 숫자, '.', '-'의 조합으로 입력. 여러 개의 OID를 지정하는 경우에는 ','로 구분 **참고**: 설정한 OID를 삭제하려면 **no limit-oid** *<LIMIT_OID>* 명령을 사용합니다.
5	**current**	현재 SNMP 커뮤니티 설정을 확인합니다.
6	**apply**	SNMP 커뮤니티 설정을 시스템에 저장합니다.

참고: 설정한 SNMP 커뮤니티를 삭제하려면 <SNMP 설정 모드>에서 **no community** *<NAME>* 명령을 사용합니다.

SNMP 사용자 설정

SNMP v3에서 인증 시 사용할 SNMP 사용자와 패스워드를 설정하려면, <SNMP 설정 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 8명의 SNMP 사용자를 등록할 수 있습니다.

순서	명 령	설 명
1	**user** *<NAME>* **md5-passwd** *<MD5-PASSWD>*	SNMP v3 에서 인증 시 사용할 사용자와 MD5 패스워드를 설정합니다. • *<NAME>* SNMP 사용자 이름. 2 ~ 32 자 사이의 알파벳 대/소문자, 숫자, '-', '_' 문자로 이루어진 문자열로 지정. 첫 글자는 반드시 알파벳 사용 • *<MD5-PASSWD>* MD5 패스워드. 8 ~ 64 자 사이의 알파벳 대/소문자와 숫자, 특수 문자('/' 제외)의 조합으로 구성

2	**user** *<NAME>* **des-passwd** *<DES-PASSWD>* (선택 설정)	SNMP v3 에서 통신 데이터에 대한 암호화에 사용되는 DES 패스워드를 설정합니다. • *<NAME>* 1 번 과정에서 입력한 사용자 이름 • *<DES-PASSWD>* DES 패스워드. 8 ~ 64 자 사이의 알파벳 대/소문자와 숫자, 특수 문자('\' 제외)의 조합으로 구성

참고: 설정한 SNMP 사용자를 삭제하려면 <SNMP 설정 모드>에서 **no user** *<NAME>* 명령을 사용합니다.

참고: 설정한 DES 패스워드를 삭제하려면 <SNMP 설정 모드>에서 **no user** *<NAME>* **des-passwd** 명령을 사용합니다.

SNMP 로드 타임아웃 설정

SNMP 로드 타임 아웃을 설정하기 위해서는 <Configuration 모드>에서 다음 명령을 실행합니다.

명 령	설 명
load-timeout *<LOAD-TIMEOUT>*	SNMP 로드 타임 아웃을 설정합니다. • *<LOAD-TIMEOUT>* 설정 범위: 0~65535, 기본값: 60 (초)

참고: 설정한 SNMP 로드 타임 아웃을 기본값으로 변경하려면 <SNMP 설정 모드>에서 **no load-timeout** 명령을 사용합니다.

SNMP 트랩 호스트 설정

SNMP 트랩 호스트를 설정하려면 <SNMP 설정 모드>에서 다음 명령을 사용합니다. PAS-K에는 최대 32개의 SNMP 트랩 호스트를 설정할 수 있습니다.

명 령	설 명
trap host *<IP>* [**community** *<COMMUNITY>*]	SNMP 트랩 호스트 및 SNMP 커뮤니티를 설정합니다. SNMP 트랩 호스트 등록 시, 커뮤니티 정보를 입력하지 않을 경우 기본값으로 public 이 설정됩니다. • *<IP>* 트랩 호스트의 IP 주소. • *<COMMUNITY>* SNMP 커뮤니티 이름. 1~254 자 사이의 알파벳 대/소문자, 숫자, 특수 문자(' ', '\' 제외)로 이루어진 문자열로 지정 (기본값: public)

참고: 설정한 SNMP 트랩 호스트를 삭제하려면 <SNMP 설정 모드>에서 **no trap host** *<IP>* 명령을 사용합니다.

참고: SNMP 트랩 호스트를 설정하면 기본적으로 부하 분산 서비스와 실제 서버의 장애 감시 결과에 변동 사항에 대한 트랩 메시지를 전송합니다.

SNMP Generic 트랩 설정

SNMP generic 트랩을 활성화하거나 비활성화하기 위해 <SNMP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
trap cold-start {enable | disable}	MIB 이 수정되었거나 SNMP 가 활성화될 때 트랩 발생 여부를 지정합니다. • **enable** cold start 트랩 기능 활성화 • **disable** cold start 트랩 기능 비활성화 (기본값)
trap link-down {enable | disable}	인터페이스 링크가 다운되었을 때 트랩 발생 여부를 지정합니다. • **enable** 링크 다운 트랩 기능 활성화 • **disable** 링크 다운 트랩 기능 비활성화 (기본값)
trap link-up {enable | disable}	인터페이스 링크가 업되었을 때 트랩 발생 여부를 지정합니다. • **enable** 링크 업 트랩 기능 활성화 • **disable** 링크 업 트랩 기능 비활성화 (기본값)

장비 정보(이름, 연락처, 위치) 설정

PAS-K는 각 장비에 장비의 이름과 장비에 관해 문의할 수 있는 연락처, 장비의 위치에 대한 정보 등을 지정할 수 있습니다. 기본적으로 PAS-K에는 장비의 이름과 위치, 연락처가 설정되어 있지 않습니다.

장비의 이름, 연락처, 위치 정보를 설정하려면 <SNMP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
system name *<NAME>*	장비의 이름을 설정합니다. 장비의 이름은 어떤 장비인지, 어떤 용도로 사용 중인지를 쉽게 알 수 있는 문자열을 사용하도록 합니다. • *<NAME>* 최대 255 자의 알파벳 대/소문자, 숫자, 특수 문자로 이루어진 문자열로 지정 가능.
system contact *<CONTACT>*	장비의 연락처를 설정합니다. 연락처는 주로 관리자의 이메일 주소나 전화 번호를 사용합니다. • *<CONTACT>* 최대 255 자의 알파벳 대/소문자, 숫자, 특수 문자로 이루어진 문자열로 지정 가능
system location *<LOCATION>*	장비의 위치 정보를 설정합니다. 위치 정보는 주로 장비가 설치된 곳의 주소를 지정하는 경우가 많습니다. • *<LOCATION>* 최대 255 자의 알파벳 대/소문자, 숫자, 특수 문자로 이루어진 문자열로 지정 가능

참고: 설정한 SNMP 장비 정보(이름, 연락처, 위치)를 삭제하려면 <SNMP 설정 모드>에서 다음의 명령을 사용합니다.

```
(config-snmp)# no system name
(config-snmp)# no system contact
(config-snmp)# no system location
```

SNMP 활성화 및 설정 적용

기본적으로 SNMP는 비활성화되어 있습니다. SNMP 를 활성화하고, 설정을 적용하려면 <SNMP 설정 모드>에서 다음 명령을 사용합니다.

순서	명 령	설 명
1	**status {enable | disable}**	SNMP 기능의 사용 여부를 지정합니다. • **enable** SNMP 기능 활성화 • **disable** SNMP 기능 비활성화 (기본값)
2	**current**	설정한 SNMP 정보를 확인합니다.
3	**apply**	SNMP 정보를 저장하고 시스템에 적용합니다.

SNMP 설정 정보 보기

현재 SNMP의 설정 정보와 상태를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show snmp** 명령을 실행합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

제6장
포트 바운더리 설정

PAS-K로 수신되는 패킷에 L4-7 스위칭을 수행하기 위해서는 반드시 PAS-K의 포트에 포트 바운더리(port boundary)를 설정해야 합니다. 이 장에서는 포트 바운더리의 개념과 설정 시 주의 사항을 소개하고 CLI에서 포트 바운더리를 설정하는 방법에 대해 살펴보도록 합니다.

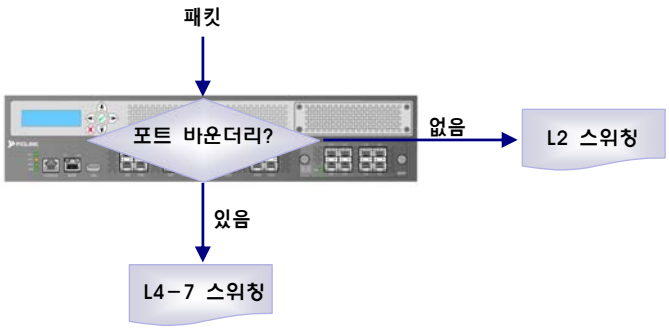
이 장은 다음과 같은 내용으로 구성됩니다.

- 포트 바운더리 개요
- 포트 바운더리 설정

포트 바운더리 개요

PAS-K의 기능 중에서 부하 분산은 L4-7 스위칭을 통해서만 수행되는 기능입니다. PAS-K로 수신되는 패킷에 이러한 기능을 적용하기 위해서는 반드시 PAS-K의 포트에 '포트 바운더리'를 설정해야 합니다. PAS-K는 포트 바운더리가 설정되어 있는 포트로 수신된 패킷은 L4-7 스위칭을 수행하고, 포트 바운더리가 설정되어 있지 않은 패킷은 L2 스위칭으로만 처리하기 때문입니다.

다음 그림은 PAS-K로 패킷이 수신되었을 때 포트 바운더리의 설정 여부에 따라 패킷이 처리되는 과정을 보여줍니다.



[그림 - 포트 바운더리에 따른 패킷 처리 과정]

위 그림에서와 같이 패킷이 수신되면 PAS-K는 먼저 패킷이 수신된 포트에 포트 바운더리가 설정되어 있는지를 확인합니다. 포트 바운더리가 설정되어 있지 않은 포트인 경우에는 L2 스위칭에 의해 처리됩니다. 하지만, 포트 바운더리가 설정되어 있는 경우에는 L4-7 스위칭에 의해 패킷이 처리됩니다.

포트 바운더리의 적용 범위 제한

기본적으로 포트 바운더리는 포트로 송수신되는 모든 패킷에 적용됩니다. 하지만, 필요한 경우에는 출발지(source)나 목적지(destination) IP 대역/포트, 프로토콜 종류, VLAN ID를 사용하여 포트 바운더리를 적용할 패킷을 구체적으로 지정할 수 있습니다.

- **출발지/목적지 IP 대역**
  포트 바운더리에 출발지 IP 대역이나 목적지 IP 대역을 지정하면, 포트를 통해 전송하거나 수신하는 패킷 중에서 출발지 IP 주소나 목적지 IP 주소가 지정한 IP 대역에 속하는 패킷에만 포트 바운더리를 적용합니다.
- **출발지/목적지 포트**
  포트 바운더리에 출발지 포트 번호나 목적지 포트 번호를 지정하면, 지정한 포트를 통해 전송하거나 수신하는 패킷에만 포트 바운더리를 적용합니다.
- **프로토콜**
  포트 바운더리에 TCP나 UDP 프로토콜을 지정하면, 포트를 통해 전송하거나 수신하는 패킷 중에서 지정한 프로토콜 종류의 패킷에만 포트 바운더리를 적용합니다. 그리고, 포트로 송수신되는 패킷에 대해서만 포트 바운더리를 적용할 수 있습니다.
- **VLAN ID**
  포트가 tagged 포트인 경우에는 여러 VLAN으로부터 패킷을 전송하고 수신하게 됩니다. 이런 경우, 포트 바운더리에 VLAN ID를 지정하면 지정한 VLAN의 패킷에만 포트 바운더리를 적용할 수 있습니다.

위 네가지 조건은 하나의 포트 바운더리에서 동시에 사용될 수 있습니다.

포트 바운더리의 ID

하나의 포트에는 여러 포트 바운더리가 적용될 수 있습니다. 그런 경우 PAS-K는 ID가 작은 순으로 포트 바운더리를 적용합니다. 여러 포트 바운더리가 적용된 포트로 패킷이 수신되면 PAS-K는 먼저 ID가 가장 작은 포트 바운더리를 확인합니다. 패킷이 그 포트 바운더리의 조건에 만족하지 않으면 PAS-K는 다음 포트 바운더리를 확인합니다. 만약, 패킷이 모든 포트 바운더리의 조건에 해당하지 않으면 포트 바운더리가 설정되어 있지 않은 포트로 수신된 패킷과 마찬가지로 L2 스위칭이 수행됩니다. 이와 같이 포트 바운더리의 ID는 우선순위와 같은 역할을 합니다.

포트 바운더리의 ID를 지정할 때 유의할 사항은 설정 정보가 구체적인 포트 바운더리일수록 더 낮은(우선순위는 높은) ID로 지정해야 한다는 점입니다.

다음은 서버 부하 분산 + 캐시 서버 부하 분산 구성의 PAS-K에 설정한 포트 바운더리입니다.

포트	포트에 연결된 장비	목적지 IP 대역
3 ~ 4	캐시 서버	192.168.1.100/24
5	라우터	모든 네트워크(0.0.0.0/0)
1 ~ 4	캐시 서버와 서버	모든 네트워크(0.0.0.0/0)

이 포트 바운더리에 ID를 지정하려면, 구체적인 조건을 가진 포트 바운더리일수록 낮은 ID를 설정해야 하므로, 가장 위에 있는 포트 바운더리에 가장 낮은 ID를 설정해야 합니다. 나머지 두 바운더리는 동일한 조건이므로 가장 위에 있는 바운더리보다 높은 ID 값만 지정하면 됩니다.

다음과 같은 3개의 포트 바운더리에 ID를 설정하는 예를 하나 더 살펴보도록 합니다.

❶ 출발지 IP 대역이 100.1.1.0/24인 포트 바운더리
❷ 출발지 IP 대역이 100.1.0.0/16인 포트 바운더리
❸ 출발지 IP 대역이 지정되지 않은 포트 바운더리

위 세 포트 바운더리가 하나의 포트에 동시에 적용되는 경우에는 포트 바운더리의 ID를 반드시 ❶ < ❷ < ❸ 이 되는 값으로 지정해야 합니다.

Promisc 모드와 Include MAC 모드

기본적으로 포트 바운더리가 설정된 포트로 수신되는 모든 패킷은 L4-7 스위칭이 수행됩니다. 이들 패킷 중에는 L4-7 스위칭을 필요로 하지 않는 패킷이 포함되어 있습니다. 이러한 패킷들이 L4-7 스위칭 과정을 거치지 않도록 설정해주면 PAS-K의 부하를 덜어주어 더 나은 성능을 제공합니다.

포트 바운더리의 설정 항목 중에는 포트로 수신된 패킷 중에서 L4-7 스위칭을 반드시 수행할 패킷과 수행할 필요가 없는 패킷을 지정할 때 사용하는 promisc 모드와 Include MAC 모드가 있습니다.

Promisc 모드는 포트로 수신되는 모든 패킷에 L4-7 스위칭을 수행할 것인지 아니면 특정한 패킷만 L4-7 스위칭을 수행하고 나머지 패킷은 포워딩할지를 나타냅니다. Promisc 모드는 on이나 off로 설정할 수 있습니다. Promisc 모드가 on인 포트 바운더리에 속한 포트로 수신되는 모든 패킷은 L4-7 스위칭이 수행됩니다. Promisc 모드가 off인 포트 바운더리에 속한 포트는 수신된 패킷 중에서 패킷의 목적지 MAC 주소가 PAS-K의 MAC 주소와 일치하는 패킷만 L4-7 스위칭이 수행됩니다.

Include MAC 모드는 L4-7 스위칭을 수행할 패킷의 종류(유니캐스트, 멀티캐스트, 브로드캐스트)를 나타냅니다. Include MAC 모드는 none, unicast, multi-broadcast로 설정할 수 있습니다. Include MAC 모드가 none인 이 포트 바운더리에 속한 포트는 promisc 모드의 설정에 따라 패킷의 L4-7 스위칭이 이루어집니다. Include MAC 모드가 unicast인 포트 바운더리에 속한 포트는 목적지 MAC 주소가 PAS-K의 MAC 주소와 일치하는 패킷과 유니캐스트 MAC 주소를 가진 패킷이 L4-7 스위칭이 수행됩니다. Include MAC 모드가 multi-broadcast인 포트 바운더리에 속한 포트는 멀티캐스트나 브로드캐스트 MAC 주소를 가진 패킷만 L4-7 스위칭이 수행됩니다.

다음은 promisc 모드와 Include MAC 모드에 따라 L4-7 스위칭이 수행되는 패킷을 정리한 표입니다.

[표 - Promisc 모드와 Include MAC 모드에 따라 L4-7 스위칭이 수행되는 패킷 종류]

No.	Promisc 모드	Include MAC 모드	L4-7 스위칭이 수행되는 패킷
❶	off	none	목적지 MAC 주소가 PAS-K의 MAC 주소와 일치하는 패킷 (기본 설정)
❷	off	unicast	• 목적지 MAC 주소가 PAS-K의 MAC 주소와 일치하는 패킷 • 유니캐스트 MAC 주소를 가진 패킷
❸	off	multi-broadcast	멀티캐스트 혹은 브로드캐스트 MAC 주소를 가진 패킷
❹	on	none	포트로 수신되는 모든 IP 패킷

Include MAC 모드를 unicast나 multi-broadcast로 지정한 경우에는 반드시 promisc 모드를 off로 설정해야 합니다. Promisc 모드를 off로 설정하고, Include MAC 모드를 multi-broadcast로 설정한 경우는 Include MAC 모드를 unicast로 설정한 경우와 달리, 목적지 MAC 주소가 PAS-K의 MAC 주소와 일치하는 패킷은 L4-7 스위칭이 수행되지 않습니다. 멀티캐스트나 브로드캐스트 MAC 주소를 가진 패킷과 이러한 패킷(목적지 MAC 주소가 PAS-K의 MAC 주소와 일치하는)의 L4-7 스위칭을 모두 수행하도록 설정하려면 다음과 같은 2개의 포트 바운더리를 정의해야 합니다.

- 포트 바운더리 1
  Promisc 모드 'off', Include MAC 모드 'none'
- 포트 바운더리 2
  Promisc 모드 'off', Include MAC 모드 'multi-broadcast'

다음은 앞의 표에서 설명한 4가지 포트 바운더리를 어떤 상황에서 사용해야 하는지를 나타낸 표입니다.

[표 - Promisc 모드와 Include MAC 모드 설정이 사용되는 경우]

No.	설정이 사용되는 경우
❶	• PAS-K가 다음 홉이나 게이트웨이로 설정된 경우 • 서버 부하 분산 서비스의 가상 IP로 접속하는 경우
❷	브리지 모드 네트워크 구성인 경우
❸	서로 다른 VLAN 간에 멀티캐스트 패킷을 송수신하고자 하는 경우
❹	모든 패킷에 L4-7 스위칭을 수행해야 하는 경우

포트 바운더리 설정

PAS-K에 포트 바운더리를 설정하는 과정은 다음과 같습니다.

1. 포트 바운더리 정의 (필수)
2. 포트 지정 (선택)
3. 출발지나 목적지 IP 대역 지정 (선택)
4. 출발지나 목적지 포트 번호 지정 (선택)
5. 패킷의 프로토콜 종류 지정 (선택)
6. 패킷의 VLAN ID 지정 (선택)
7. Promisc 모드와 Include MAC 모드 지정 (선택)
8. 포트 바운더리 활성화/비활성화 (선택)

1번 과정을 제외한 나머지 과정들은 모두 사용자가 수행 여부를 결정할 수 있는 선택 과정입니다. 이 선택 과정을 수행하지 않는 경우에는 포트 바운더리에 다음과 같은 기본값들이 설정됩니다.

[표 - 포트 바운더리 기본 설정]

항목	기본값
포트	모든 포트
출발지 IP 대역	0.0.0.0/0
목적지 IP 대역	0.0.0.0/0
출발지 포트 번호	없음
목적지 포트 번호	없음
프로토콜	전체
VLAN ID	전체
Promisc 모드	off
Include MAC 모드	none
활성화/비활성화	활성화

CLI에서 설정하기

이 절에서는 CLI 명령을 사용하여 포트 바운더리 기능을 설정하는 방법을 살펴봅니다.

포트 바운더리 설정

포트 바운더리를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 16개의 포트 바운더리를 설정할 수 있으므로, 여러 개의 포트 바운더리를 설정하는 경우에는 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**port-boundary** *<ID>*	포트 바운더리를 생성하고 <포트 바운더리 설정 모드>로 들어갑니다. • *<ID>* 포트 바운더리의 ID, 우선순위. 설정 범위: 1 ~ 16
2	**port** *<PORT>*	포트 바운더리에 포함시킬 포트를 설정합니다. • *<PORT>* 두 개 이상의 포트를 지정하는 경우에는 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용 **참고**: 설정한 port를 삭제하려면, **no port** *<PORT>* 명령을 사용합니다. **참고**: 포트를 지정하지 않은 경우에는 설정에서 포트 정보가 보이지 않지만 PAS-K의 모든 포트에 포트 바운더리가 적용됩니다. **주의**: IPv6 포트 바운더리를 설정하려면, 위와 같이 포트 바운더리에 포함시킬 포트를 지정하면 됩니다. 단, 3~10번 과정의 옵션은 설정할 수 없습니다. 옵션을 설정하면 IPv4 패킷에 대해서만 L4-L7 스위칭을 수행합니다. IPv6 포트 바운더리 설정을 위한 옵션 기능은 추후 개발되는 PLOS에서 지원할 예정입니다.
3	**sip** *<SIP>*	포트 바운더리를 적용할 패킷의 출발지 IP 대역을 지정할 수 있습니다. 패킷의 출발지 IP 대역을 설정하면 포트 바운더리에 속한 포트는 설정한 IP 대역에서 전송된 패킷만 포트 바운더리를 적용합니다. • *<SIP>* 출발지 IP 대역. 기본값: 0.0.0.0/0 **참고**: 설정한 sip를 기본값으로 변경하려면, **no sip** 명령을 사용합니다.
4	**sport** *<SPORT>*	포트 바운더리를 적용할 패킷의 출발지 포트 번호를 입력합니다. (프로토콜이 TCP, UDP, all일 경우에만 사용 가능) • *<SPORT>* 출발지 포트 번호. 설정 범위: 1 ~ 65535 **참고**: 설정한 sport를 삭제하려면, **no sport** 명령을 사용합니다.
5	**dip** *<DIP>*	포트 바운더리를 적용할 패킷의 목적지 IP 대역을 지정할 수 있습니다. 패킷의 목적지 IP 대역을 설정하면 포트 바운더리에 속한 포트는 설정한 IP 대역으로 향하는 패킷에만 포트 바운더리를 적용합니다. • *<DIP>* 목적지 IP 대역. 기본값: 0.0.0.0/0 **참고**: 설정한 dip를 기본값으로 변경하려면, **no dip** 명령을 사용합니다.
6	**dport** *<DPORT>*	포트 바운더리를 적용할 패킷의 목적지 포트 번호를 입력합니다. (프로토콜이 TCP, UDP, all일 경우에만 사용 가능) • *<DPORT>* 목적지 포트 번호. 설정 범위: 1 ~ 65535 **참고**: 설정한 dport를 삭제하려면, **no dport** 명령을 사용합니다.
7	**vid** *<VID>*	포트 바운더리에 속한 포트가 tagged 포트인 경우에는 특정한 VLAN의 패킷만 포트 바운더리를 적용하도록 설정할 수 있습니다. • *<VID>* VLAN ID 설정. 설정 범위: 1 ~ 4080 **참고**: 설정한 vid를 삭제하려면, **no vid** 명령을 사용합니다.

8	**protocol {all | icmp | tcp | udp}**	특정 프로토콜의 패킷에만 포트 바운더리를 적용하고자 하는 경우에는 프로토콜의 종류를 설정합니다. (기본값: all) **참고**: 설정한 프로토콜을 기본값으로 변경하려면 **no protocol** 명령을 사용합니다.
9	**promisc {on | off}**	포트 바운더리의 promisc 모드를 설정합니다. • **on** promisc 모드 활성화 • **off** promisc 모드 비활성화 (기본값)
10	**include-mac {none | multi-broadcast | unicast}**	포트 바운더리의 Include MAC 모드를 설정합니다. (기본값: none) **참고**: 설정한 Include MAC 모드를 기본값으로 변경하려면 **no include-mac** 명령을 사용합니다.
11	**status {enale | disable}** (선택 설정)	설정한 포트 바운더리의 사용 여부를 설정합니다. • **enable** 포트 바운더리 기능 활성화 • **disable** 포트 바운더리 기능 비활성화 (기본값)
12	**current**	설정한 포트 바운더리 정보를 확인합니다.
13	**apply**	설정된 포트 바운더리 정보를 저장하고 시스템에 적용합니다.

주의: 출발지/목적지 IP 대역이나 프로토콜 종류, VLAN ID 등을 설정하는 포트 바운더리의 ID는 이 항목들을 설정하지 않는 포트 바운더리의 ID보다 반드시 작아야 합니다.

참고: 설정한 포트 바운더리를 삭제하려면 <Configuration 모드>에서 **no port-boundary** <*ID*> 명령을 실행합니다.

포트 바운더리 설정 정보 보기

포트 바운더리 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show port-boundary** 명령을 통해 확인할 수 있습니다. **show port-boundary** 명령을 포트 바운더리 ID와 함께 실행하면 해당 포트 바운더리 설정에 대한 보다 구체적인 정보를 확인할 수 있습니다.

참고: 해당 명령 실행시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

제7장
부하 분산 설정

이 장에서는 서버와 방화벽, VPN 등의 부하를 적절하게 분산하여 자원의 가용성과 안정성을 높여주는 PAS-K의 L4, L7 부하 분산 기능에 대해 살펴봅니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- L4 부하 분산
- L7 부하 분산
- 실제 서버(Real Server)
- 부하 분산 방식
- 장애 감시(Health Check)
- 지속 연결(Persistence)
- 애플리케이션 가속(Application Accelerator)
- 장애 감시 설정
- 실제 서버 설정
- HTTP 압축 규칙 설정
- 캐싱 규칙 설정
- SSL 가속 설정
- L4 서버 부하 분산 설정
- 방화벽/VPN 부하 분산 설정
- 고급 방화벽/VPN 부하 분산 설정
- L4 캐시 서버 부하 분산 설정
- 게이트웨이 부하 분산 설정
- 글로벌 서버 부하 분산 설정
- L7 서버 부하 분산 설정
- 고급 L7 서버 부하 분산 설정
- L7 캐시 서버 부하 분산 설정
- 고급 L7 캐시 서버 부하 분산 설정
- 세션 엔트리 및 통계 정보 출력

L4 부하 분산

개요

PAS-K는 일반 서버, 캐시 서버, 방화벽, VPN(가상 사설망) 장비의 부하 분산(load balancing) 기능을 제공하여 고가용성(high availability) 구성을 가능하게 해주는 L4 스위치입니다. PAS-K의 부하 분산 기능은 각 장비들의 트래픽을 분산하여 손쉽게 성능을 확장할 수 있도록 하고, 장비의 장애 감시 기능을 통하여 장비에 장애가 발생한 경우에도 다른 장비를 통해 지속적인 서비스가 유지될 수 있도록 합니다. 이와 같이 PAS-K의 부하 분산 기능이 제공하는 고가용성과 안정성을 통하여 대용량의 웹사이트나 중요한 인터넷 업무 장소, 혹은 인터넷 서비스 업체(ISP)에서 손쉽게 장비를 확장하고 유지 관리할 수 있을 뿐 아니라 24시간 중단 없는 서비스를 간단하게 구현할 수 있습니다.

PAS-K에서 제공하는 L4 부하 분산의 특징을 요약하면 다음과 같습니다.

- 네트워크 환경과 트래픽의 특성에 따라 다양하게 적용할 수 있는 여러 종류의 부하 분산 방식을 제공합니다.
- 클라이언트 기반의 지속 연결 기능(persistence)을 제공합니다.
- 기존 네트워크 환경을 변경시키지 않고 부하 분산 기능을 적용할 수 있습니다.
- 브리징(L2) 네트워크 구성과 라우팅(L3) 네트워크 구성에서 모두 사용할 수 있습니다.
- 서버 부하 분산 기능은 Dest-NAT, DSR, LAN-to-LAN과 같은 다양한 NAT 모드를 지원합니다.
- 방화벽 부하 분산 기능은 다양한 종류의 방화벽에 적용될 수 있고 DMZ를 포함한 복잡한 방화벽 구성도 지원합니다.
- 방화벽과 VPN 장비가 동시에 존재하는 네트워크에서도 부하 분산이 가능합니다.
- 서버 부하 분산과 방화벽 부하 분산, 캐시 서버 부하 분산을 동시에 사용할 수 있습니다.
- 다양한 종류의 VPN 터널링 프로토콜과 L2TP 기반의 VPN을 지원하고 본점과 지점 간의 대칭적 VPN 기능이 강화되었습니다.
- 게이트웨이 라인의 상태를 지속적으로 모니터링하고, 내부 네트워크에서 외부 네트워크로 전송되는 트래픽을 정상적으로 연결되어 있는 게이트웨이 라인으로 분산 시켜주는 게이트웨이 부하 분산 기능을 지원합니다.
- 서버 부하 분산 기능을 확장시킨 글로벌 서버 부하 분산 기능을 지원합니다.

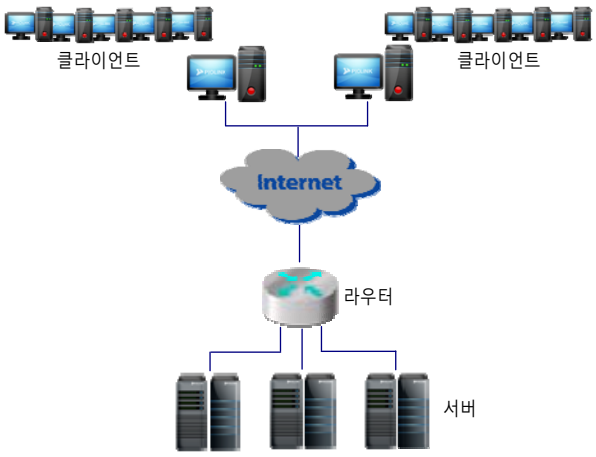
L4 서버 부하 분산

서버 부하 분산(Server Load Balancing-SLB)은 인터넷 트래픽을 동일한 서비스를 제공하는 여러 개의 서버들(서버 풀)에게 효율적으로 배분하여 서버의 부하를 분산시켜주는 기능입니다. 서버 부하 분산 기능을 사용한 네트워크는 다음과 같은 장점을 가질 수 있습니다.

- **서버 이용률과 네트워크 대역폭의 효율이 증가됩니다.**
  사용자의 세션 트래픽이 서버 풀에 있는 현재 가용한 서버들 중에서 부하가 적은 서버를 통해 처리됩니다. 그러므로, 하나의 서버에 트래픽이 집중되는 것을 막아주고 서버의 트래픽 처리 지연으로 인해 발생할 수 있는 대역폭의 낭비도 줄일 수 있습니다.
- **사용자에게 신뢰성 있는 서비스를 제공할 수 있습니다.**
  하나의 서버에 문제가 발생하더라도 나머지 서버들에 의해 애플리케이션과 데이터로 접속할 수 있습니다.
- **서비스의 범용성(scalability)을 높일 수 있습니다.**
  사용자가 늘어나고 서버들의 처리 용량이 부족하게 되는 경우, 기존 서비스에 영향을 주지 않고 새로운 서버를 서버 풀에 추가할 수 있습니다.

기존 네트워크 vs 서버 부하 분산 적용 네트워크

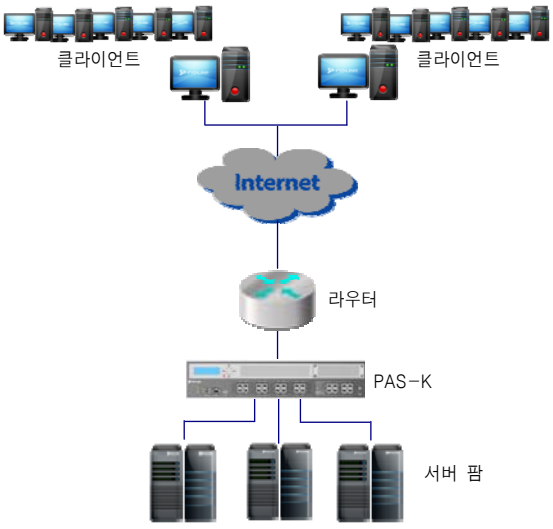
다음은 서버 부하 분산 기능을 사용하지 않고 여러 개의 서버를 사용하는 일반적인 네트워크 구성도입니다.



[그림 - 서버 부하 분산이 적용되지 않은 일반적인 멀티 서버 네트워크 구성도]

위의 그림과 같은 네트워크에서는 일반적으로 각 서버가 하나 내지는 두 개 정도의 고유한 서비스를 제공하도록 한정되어 있습니다. 만약 이런 서버들 중 하나가 많은 사용자들이 자주 사용하는 애플리케이션이나 접속이 빈번한 데이터를 제공하는 경우에는 서버에 과부하가 발생할 수 있습니다. 서버에 과부하가 발생한 상태에서는 서버가 사용자의 서비스 요청을 거부하게 되고 사용자는 다시 서버로 반복해서 서비스를 요청하게 되기 때문에 전체 네트워크 성능이 떨어지게 됩니다. 이러한 상황은 사용자 요청을 처리할 수 있는 가용 서버들이 있는 경우에도 종종 발생합니다.

이와 같이 특정한 서버로만 부하가 집중되는 현상은 다음과 같이 PAS-K를 사용하여 서버 부하 분산 기능을 적용한 네트워크 구성을 통해 해결할 수 있습니다.



[그림 - PAS-K의 서버 부하 분산 기능이 적용된 멀티 서버 네트워크 구성도]

위와 같이 PAS-K와 서버를 연결하고 PAS-K에 서버 부하 분산 기능을 적용하면 PAS-K는 다양한 부하 분산 방식을 사용하여 사용자 트래픽을 서버 팜에 있는 적절한 서버로 배분합니다. 따라서, 앞에서 살펴본 네트워크에서 발생하던 특정 서버의 과부하 발생을 방지할 수 있습니다. 그 밖에도 PAS-K의 서버 부하 분산 기능을 사용하면 네트워크 신뢰성이 향상되고 서버를 추가하고 제거하는 과정이 한결 쉬워지게 됩니다.

참고: PAS-K의 서버 부하 분산 기능은 Linux, Windows Server, FreeBSD, Solaris, HP-UX을 포함한 모든 운영 체제의 서버에 사용될 수 있습니다.

가상 서버 기반 부하 분산

PAS-K는 가상 서버 기반의 부하 분산(virtual server based load balancing)을 지원합니다. 이 방식은 가장 일반적인 서버 부하 분산 방식입니다. 이 방식에서 PAS-K는 가상 서버(virtual server) 역할을 수행하고, 트래픽을 분산 시킬 서버 그룹(서버 팜)에 대한 가상 서버 IP 주소(혹은 주소 범위)를 가집니다. 클라이언트는 서버의 실제 IP 주소 대신 가상 IP 주소를 사용하여 서비스를 요청하게 됩니다. 이 방식은 가상 IP 주소 하나로 HTTP, TELNET, FTP, DNS 등과 같은 서비스를 제공하는 실제 서버를 여러 개 연결하여 서비스 용량을 증가시킴은 물론 서비스의 품질을 향상시키고 일부 서버의 장애도 자동적으로 극복할 수 있도록 해줍니다.

PAS-K에서는 가상 서버를 서버 부하 분산 서비스라고 합니다. 서버 부하 분산 서비스는 가상 IP 주소로 수신된 트래픽을 서비스에 지정된 부하 분산 방식을 사용하여 실제 서버로 전송해줍니다. PAS-K에는 256개의 서버 부하 분산 서비스를 동작 시킬 수 있습니다.

필터

PAS-K는 트래픽 중에서 L4 서버 부하 분산을 적용할 트래픽을 정의하기 위해 필터를 사용합니다. 필터는 프로토콜과 출발지/목적지 IP 주소, 출발지/목적지 포트 번호 등을 다양하게 조합하여 정의할 수 있습니다. 필터의 종류에는 'include' 타입과 'exclude' 타입이 있습니다. Include 타입의 필터에는 L4 서버 부하 분산을 적용할 트래픽의 조건이 포함됩니다. 그리고 exclude 타입의 필터는 L4 서버 부하 분산을 적용하지 않을 트래픽의 조건으로 구성됩니다. 필터를 설정하지 않은 경우에는 설정한 가상 IP 주소를 목적지 IP 주소로하는 include 타입의 필터가 자동으로 생성되며, 가상 IP 주소 삭제시 해당 필터도 자동으로 삭제됩니다.

서버 부하 분산의 NAT 모드

서버 부하 분산 서비스가 적용된 네트워크에서 클라이언트는 가상 IP 주소를 사용하여 서버로 데이터를 요청하게 됩니다. PAS-K는 이러한 클라이언트의 요청을 수신하면 지속 연결과 부하 분산 방식을 사용하여 실제 서버를 선택한 후 요청 패킷의 목적지 주소를 가상 IP 주소 대신 실제 서버의 IP 주소로 변환(NAT)한 후에 실제 서버로 전송합니다. 실제 서버에서 클라이언트로 응답을 전송할 때에도 PAS-K는 응답 패킷의 출발지 주소를 실제 서버의 IP 주소에서 가상 주소로 바꾸어서 클라이언트로 전송합니다.

PAS-K는 서버 부하 분산 서비스에서 클라이언트와 실제 서버 간에 가상 IP 주소와 실제 IP 주소를 변환해주는 다음과 같은 4가지의 NAT 모드를 지원합니다.

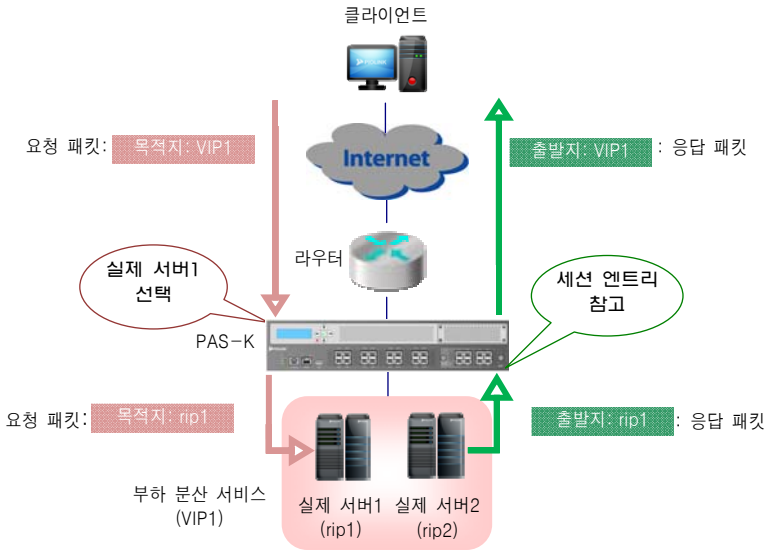
- Dest NAT(Destination NAT) 모드
- Both NAT 모드
- DSR(Direct Server Return) 모드
- LAN-to-LAN 모드

DSR 모드와 LAN-to-LAN 모드는 서버 부하 분산 서비스에서만 사용할 수 있고, Both NAT 모드는 고급 L4 서버 부하 분산 서비스에서만 사용할 수 있습니다.

각 NAT 모드에 대해 살펴봅니다.

Dest NAT(Destination NAT) 모드

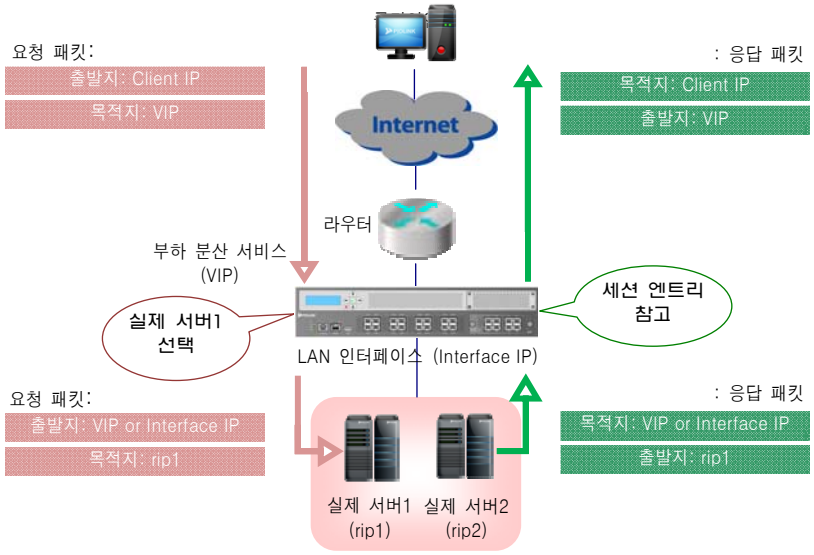
Dest NAT 모드는 가장 일반적으로 서버 부하 분산 서비스에 사용되는 NAT 모드입니다. Dest NAT 모드에서 PAS-K는 앞에서 설명한 서버 부하 분산 서비스의 NAT 기능을 그대로 수행합니다. 즉, 클라이언트가 전송한 패킷의 목적지 주소를 가상 IP 주소에서 실제 서버의 IP 주소로 변환하여 실제 서버로 전송하고, 실제 서버가 전송하는 응답 패킷의 출발지 주소를 실제 서버의 IP 주소에서 가상 IP 주소로 변환한 후 클라이언트로 전송합니다. 다음은 PAS-K에 Dest NAT 모드로 설정된 서버 부하 분산 서비스가 동작 중인 경우, 클라이언트와 실제 서버 간에 송수신되는 패킷의 출발지/목적지 주소가 변환되는 과정을 보여주는 그림입니다.



[그림 – Dest NAT 모드]

Both NAT 모드

Both NAT 모드는 고급 L4 서버 부하 분산 서비스에서만 사용할 수 있는 NAT 모드로, Dest NAT 모드와 유사하게 동작합니다. 그러나, 목적지 주소만 변환하는 Dest NAT 모드와 달리 패킷의 출발지 IP 주소를 실제 서버와 연결된 인터페이스의 IP 주소 또는 고급 L7 서버 부하 분산 서비스의 가상 IP 주소로 변환하여 전송합니다.



[그림 – Both NAT 모드]

DSR(Direct Server Return) 모드

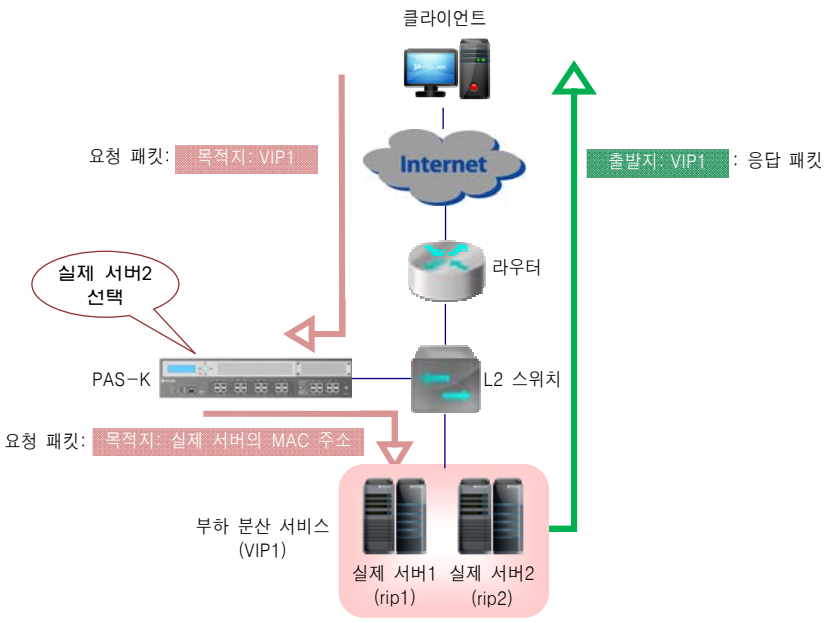
DSR 모드에서는 클라이언트가 PAS-K를 통해 실제 서버로 요청을 전송하고, 실제 서버는 PAS-K를 통하지 않고 바로 클라이언트로 응답을 전송합니다. 클라이언트의 요청을 수신한 PAS-K는 실제 서버를 선택한 후에 요청 패킷의 목적지 MAC 주소를 부하 분산된 실제 서버의 MAC 주소로 변경한 다음 실제 서버로 전송합니다. 따라서, 실제 서버는 MAC 주소가 자신의 MAC 주소와 일치하기 때문에 일단 패킷을 수신하지만 목적지 IP 주소가 자신의 IP 주소가 아니기 때문에 응답을 하지 않습니다. 이러한 문제가 발생하는 것을 방지하기 위해서는 서버에 별도의 구성 작업을 수행해야 합니다.

서버의 OS 종류나 네트워크의 구성 환경에 따라 다양한 방법의 설정이 있으므로 서버의 환경에 알맞은 방법으로 설정합니다. 기본적인 구성 방식은 다음과 같습니다.

- 서버 부하 분산 서비스의 가상 IP 주소를 실제 서버에 추가하여 실제 서버가 클라이언트의 요청에 응답할 수 있도록 설정합니다.
- 위와 같은 구성을 했을 경우, 가상 IP 주소에 대한 ARP 응답을 실제 서버가 직접 하게 되므로 DSR 모드로 설정된 서버 부하 분산 서비스가 정상적으로 동작하지 않는 경우가 발생할 수 있습니다. 이를 방지하기 위하여, 실제 서버에서 ARP 요청 대한 응답을 하지 않도록 설정합니다.

DSR 모드는 FTP(File Transfer Protocol)나 스트리밍(streaming) 서비스와 같이 클라이언트로 전송하는 업로드 트래픽이 많은 애플리케이션을 제공하는 서버에 주로 사용됩니다. DSR 모드는 PAS-K를 거치지 않고 클라이언트로 트래픽을 전송하기 때문에 PAS-K에 부하를 주지 않습니다. 대신, 실제 서버에 별도의 구성 작업을 해야 하는 번거로움이 있습니다.

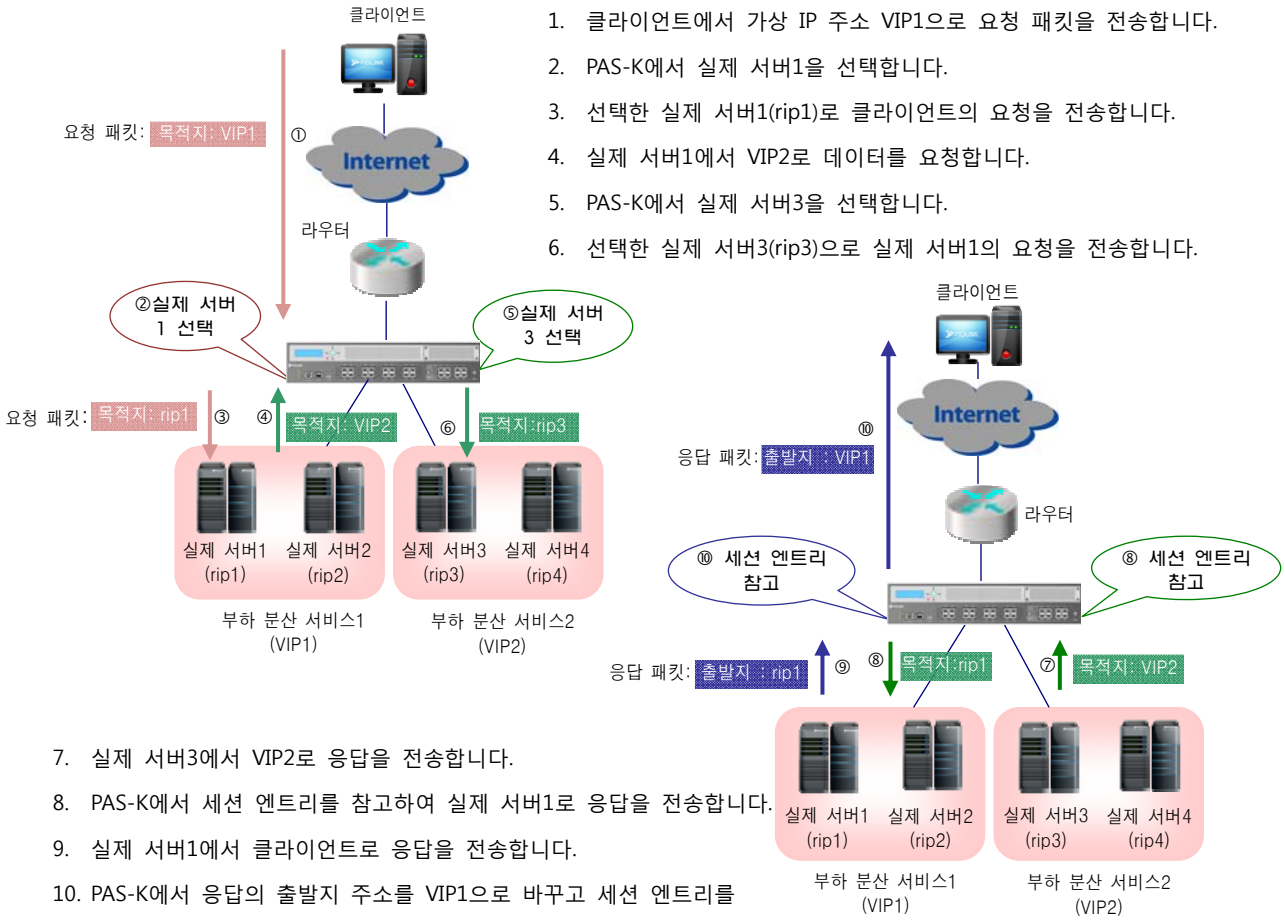
다음 그림은 PAS-K에 DSR 모드로 설정된 서버 부하 분산 서비스가 동작 중인 경우, 클라이언트와 실제 서버 간에 송수신되는 패킷의 출발지/목적지 주소가 변환되는 과정을 보여주는 그림입니다. 그림에서처럼 응답 패킷은 PAS-K를 거치지 않고 실제 서버에서 클라이언트로 바로 전송됩니다.



[그림 - DSR 모드]

LAN to LAN 모드

LAN to LAN 모드는 다른 서버 그룹에서 데이터를 가져와서 클라이언트로 전송해야 하는 서비스에서 사용되는 NAT 모드입니다. 특정 서버 그룹에서 다른 서버 그룹으로 데이터를 요청할 때에는 특정 서버 그룹에 속한 서버가 클라이언트와 같은 역할을 수행하게 됩니다. PAS-K를 LAN to LAN 모드로 설정할 때에는 서버 그룹에서 클라이언트 역할을 수행하는 서버들의 IP 대역을 함께 지정합니다. 다음은 PAS-K에 LAN to LAN 모드로 설정된 서버 부하 분산 서비스가 동작 중인 경우, 클라이언트와 실제 서버 간에 송수신되는 패킷의 출발지/목적지 주소가 변환되는 과정을 보여주는 그림입니다.



1. 클라이언트에서 가상 IP 주소 VIP1으로 요청 패킷을 전송합니다.
2. PAS-K에서 실제 서버1을 선택합니다.
3. 선택한 실제 서버1(rip1)로 클라이언트의 요청을 전송합니다.
4. 실제 서버1에서 VIP2로 데이터를 요청합니다.
5. PAS-K에서 실제 서버3을 선택합니다.
6. 선택한 실제 서버3(rip3)으로 실제 서버1의 요청을 전송합니다.
7. 실제 서버3에서 VIP2로 응답을 전송합니다.
8. PAS-K에서 세션 엔트리를 참고하여 실제 서버1로 응답을 전송합니다.
9. 실제 서버1에서 클라이언트로 응답을 전송합니다.
10. PAS-K에서 응답의 출발지 주소를 VIP1으로 바꾸고 세션 엔트리를 참고하여 클라이언트로 응답을 전송합니다.

[그림 – LAN to LAN 모드]

애플리케이션 종류

PAS-K의 서버 부하 분산 기능을 적용할 수 있는 애플리케이션 서버의 종류는 다음과 같습니다.

- FTP(File Transfer Protocol) 서버
- DNS (Domain Name Service) 서버
- 실시간 스트리밍(Real Time Streaming) 서버
- 무선 애플리케이션(Wireless Application) 서버

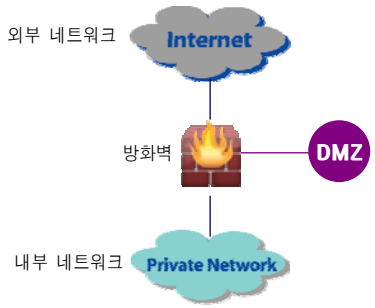
고급 L4 서버 부하 분산

고급 L4 서버 부하 분산은 IPv6를 사용하는 네트워크 환경에서 L4 서버 부하 분산을 지원하는 서비스입니다. 고급 L4 서버 부하 분산에서만 사용할 수 있는 부하 분산 방식으로 First, Consistency 출발지 해시, Consistency 가중치 출발지 해시 방식을 지원합니다.

방화벽 부하 분산

방화벽 개요

방화벽(firewall)은 허가 받지 않은 네트워크 자원의 접근을 차단해주는 기능으로 인터넷 보안을 위해서는 필수적인 기능입니다. 일반적으로 방화벽은 내부 네트워크(LAN)의 게이트웨이로서 동작하기 때문에 방화벽에 장애가 발생하면, single point of failure가 발생하게 됩니다. Single point of failure가 발생하면 내부 네트워크의 모든 호스트들이 외부 네트워크로 접속할 수 없는 심각한 상황을 초래할 수 있습니다. 다음 그림은 방화벽이 적용된 일반적인 네트워크 구성도입니다.



[그림 - 일반적인 방화벽 구성도]

방화벽은 어떤 종류의 트래픽을 허용하고 어떤 종류의 트래픽은 차단할 것인지가 정의되어 있는 규칙의 모음입니다. 위 구성도에서 외부 네트워크와 내부 네트워크, 그리고 DMZ 네트워크를 지나가는 모든 트래픽은 각 패킷을 방화벽의 규칙에 적용하기 위해 반드시 방화벽을 거쳐야 합니다. 그러므로 네트워크에 트래픽의 양이 많아지면 방화벽은 심각한 병목 현상 구간이 될 수 밖에 없습니다. 그리고, 내부 네트워크는 방화벽을 통해서만 외부 네트워크와 연결될 수 있기 때문에 만약 방화벽이 서비스를 수행할 수 없는 상태가 되면 내부 네트워크의 클라이언트들이 더 이상 인터넷을 사용할 수 없는 single point of failure가 발생하게 됩니다.

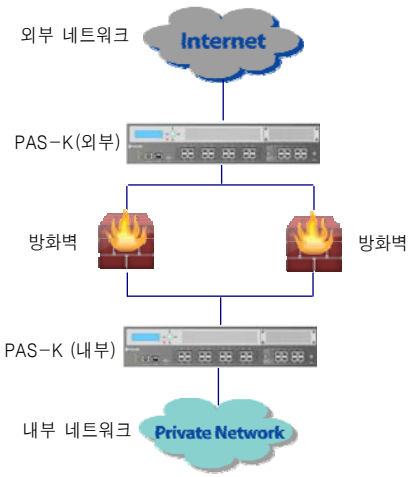
PAS-K의 방화벽 부하 분산 기능은 이와 같이 방화벽으로 인해 발생하는 병목 현상과 single point of failure 문제를 해결하고 방화벽의 성능을 더 향상시켜 줍니다.

참고: 때로는 DMZ가 방화벽 또는 방화벽과 인터넷 사이에 위치하기도 합니다. 일반적으로 DMZ는 자신의 서버를 가지고 있어서 외부 네트워크의 클라이언트가 내부 네트워크 자원을 사용하지 않도록 외부 네트워크의 클라이언트에게 서비스를 제공합니다.

방화벽 부하 분산 구성

PAS-K의 방화벽 부하 분산 기능은 여러 개의 방화벽이 동시에 동작할 수 있게 해줍니다. 여러 개의 방화벽이 동시에 동작하면 방화벽의 생산성을 최대화할 수 있고 방화벽의 성능도 방화벽의 개수만큼 늘어나게 됩니다. 뿐만 아니라 하나의 방화벽만 존재할 때 발생하던 single point of failure도 발생하지 않습니다.

네트워크에 PAS-K의 방화벽 부하 분산 기능을 적용하려면 최소 2개 이상의 PAS-K가 필요합니다. 외부 네트워크와 방화벽 사이에 PAS-K(외부 PAS-K)를 배치하고, 방화벽과 내부 네트워크 사이에 또 하나의 PAS-K(내부 PAS-K)를 배치합니다. 외부 PAS-K는 외부 네트워크에서 내부 네트워크로 들어오는 패킷의 부하 분산을 담당하고, 내부 PAS-K는 반대로 내부 네트워크에서 외부 네트워크로 나가는 패킷의 부하 분산을 담당합니다. 다음 그림은 PAS-K를 사용하여 방화벽의 부하 분산을 적용한 네트워크 구성도입니다.



[그림 - PAS-K의 방화벽 부하 분산 기능이 적용된 서버 네트워크 구성도]

필터

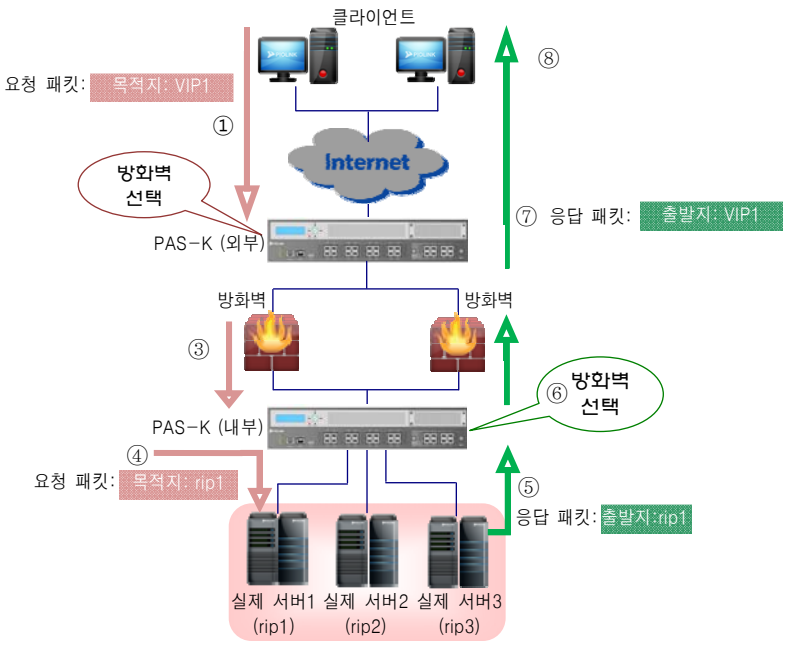
PAS-K는 트래픽 중에서 방화벽 부하 분산을 적용할 트래픽을 정의하기 위해 필터를 사용합니다. 필터는 프로토콜과 출발지/목적지 IP 주소, 출발지/목적지 포트 번호 등을 다양하게 조합하여 정의할 수 있습니다. 필터의 종류에는 'include' 타입과 'exclude' 타입이 있습니다. Include 타입의 필터에는 방화벽 부하 분산을 적용할 트래픽의 조건이 포함됩니다. 그리고 exclude 타입의 필터는 방화벽 부하 분산을 적용하지 않을 트래픽의 조건으로 구성됩니다.

지속 연결

방화벽 부하 분산의 중요한 특징 중 하나는 동일한 세션에 속하는 패킷들이 모두 동일한 방화벽을 통해 전송되어야 한다는 점입니다. 방화벽은 세션의 상태 정보를 사용하여 패킷 필터링을 수행하기 때문에, 현재 상태에 맞지 않은 패킷이 수신되는 경우에는 비 정상적인 패킷으로 간주하여 폐기하게 됩니다. 그러므로, 방화벽의 양쪽에 위치한 PAS-K에 의해 같은 세션의 패킷이 서로 다른 방화벽으로 전송되면 세션이 정상적으로 유지될 수 없습니다. 이를 방지하기 위해 PAS-K는 방화벽 부하 분산이 적용된 외부 PAS-K와 내부 PAS-K에서 송수신되는 패킷의 경로를 기억하여 경로를 지속적으로 유지할 수 있도록 해주는 지속 연결 기능을 지원합니다.

방화벽 부하 분산의 동작 방식

다음은 방화벽 부하 분산과 서버 부하 분산이 동시에 적용된 네트워크에서 클라이언트의 요청이 처리되는 과정을 보여주는 그림입니다.



[그림 - PAS-K의 방화벽 부하 분산 기능이 적용된 서버 네트워크 구성도]

1. 외부 클라이언트가 서비스에 연결하기 위해 PAS-K의 가상 IP 주소를 사용하여 요청을 보냅니다.
2. 외부 PAS-K에서 필터를 사용하여 클라이언트의 요청이 방화벽 부하 분산 기능의 적용 대상인지 확인한 후, 적용 대상인 경우에는 부하 분산 방식과 지속 연결 기능을 통해 적절한 방화벽으로 전송합니다.
3. 선택된 방화벽을 통해 트래픽이 내부 네트워크로 전송됩니다.
4. 서버 부하 분산 기능이 적용된 내부 PAS-K에서 트래픽의 가상 IP 주소와, 부하 분산 방식, 그리고 지속 연결 기능을 통해 적절한 실제 서버를 선택합니다.
5. 실제 서버에서 응답을 보냅니다.
6. 내부 PAS-K는 요청을 수신한 방화벽과 같은 방화벽으로 응답을 보냅니다.
7. 방화벽에서 외부 네트워크로 응답을 전송합니다.
8. 클라이언트에서 응답을 수신합니다.

고급 방화벽/VPN 부하 분산

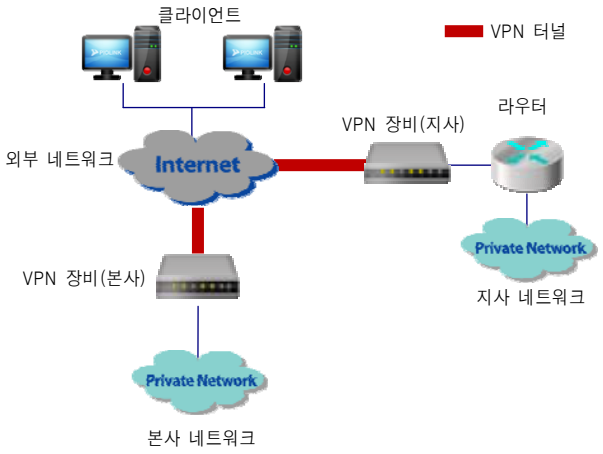
고급 방화벽/VPN 부하 분산은 IPv6를 사용하는 네트워크 환경에서 방화벽 부하 분산과 VPN 부하 분산을 지원하는 서비스입니다. 고급 방화벽/VPN 부하 분산은 부하 분산 방식으로 출발지 IP 주소와 목적지 IP 주소를 동시에 사용하여 해시 키를 계산하는 Both Hashing 방식 만을 지원하며, 내부/외부 구분과 방화벽/VPN 구분 없이 설정할 수 있습니다.

VPN 부하 분산

VPN 개요

VPN은 인터넷과 같은 공유 네트워크를 사용하여 사설 네트워크를 구축할 수 있게 해주는 기술입니다. VPN을 이용하면 전용선을 사용하여 사설 네트워크를 구축할 때보다 비용이 훨씬 저렴하고 네트워크의 운용도 수월해집니다. VPN은 지리적으로 멀리 떨어져 있는 본사와 지사 간에 동일한 데이터를 공유하거나 장소에 상관없이 인터넷을 통해 사내 네트워크로 접속하고자 할 때 주로 사용됩니다.

다음 그림은 VPN 장비를 사용하여 본사와 지사를 연결하는 일반적인 네트워크 구성도입니다.



[그림 - 일반적인 VPN 구성도]

본사와 지사 네트워크에 속한 호스트들이 인터넷을 통해 통신할 때에는 서로 인증 작업을 거쳐야 하고 터널링이라는 기능을 통해 VPN 터널을 생성한 후, 이 터널을 통해 암호화된 데이터를 주고 받습니다. 이러한 인증과 데이터 암호화 작업 등은 VPN 장비에서 이루어집니다.

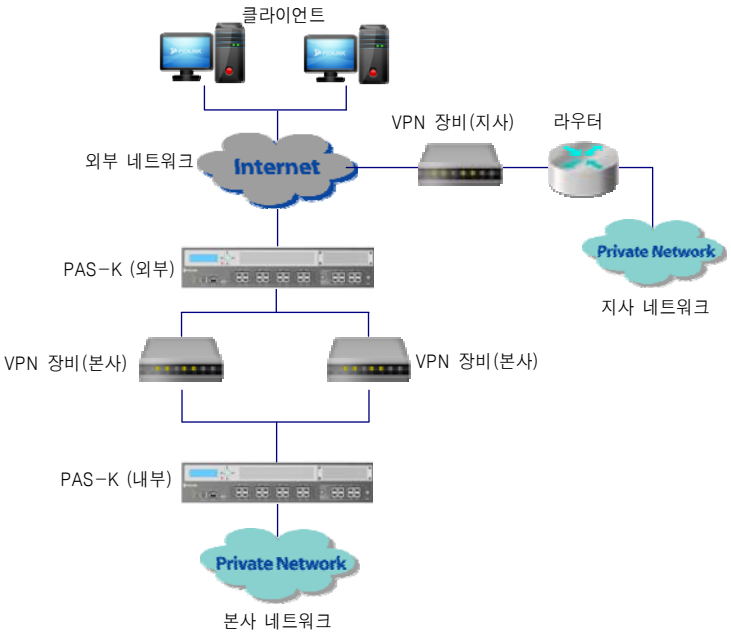
VPN 장비도 방화벽과 마찬가지로 내부 네트워크(앞의 그림에서는 본사 네트워크)의 게이트웨이로서 동작하기 때문에 VPN 장비에 장애가 발생하면 single point of failure가 발생하게 됩니다. 이를 방지하기 위해 본사 네트워크에서는 여분의 VPN 장비를 백업으로 구축하여 이중화기도 합니다. 하지만, 백업 VPN 장비는 평소에는 전혀 사용되지 않고 동작 중인 장비에 문제가 발생한 경우에만 사용되기 때문에 결국 고가의 자원이 낭비되는 상황을 초래하게 될 수 있습니다.

VPN 부하 분산 구성

PAS-K의 VPN 부하 분산 기능은 VPN 장비를 이중화함으로써 VPN의 single point of failure를 방지함과 동시에 VPN 장비들에게 모두 부하를 분산시켜줌으로써 자원이 낭비되는 것을 방지해줍니다. PAS-K는 본사-지사 간 구분 없는 대칭적인 VPN 부하 분산 기능을 지원합니다. 이러한 대칭적 VPN 부하 분산 기능은 지사에서 본사 네트워크로의 접속뿐 만 아니라, 본사에서 지사 네트워크로의 접속까지도 중앙에서 통제 할 수 있게 해줍니다.

PAS-K는 국내 및 국외의 대표적인 VPN 장비에 대한 호환성을 완벽히 지원합니다. 또한, PAS-K 만의 독특한 VPN 부하 분산 구성에 의해 IPSec, AH/ESP, L2TP, DHCP 릴레이 등 모든 VPN 터널링 프로토콜에 대한 부하 분산을 지원합니다.

다음 그림은 PAS-K를 사용하여 VPN 부하 분산을 적용한 네트워크 구성도입니다.



[그림 - VPN 부하 분산 구성도]

PAS-K의 방화벽 부하 분산 기능과 마찬가지로 VPN 부하 분산 기능을 적용하기 위해서도 최소 2개 이상의 PAS-K가 필요합니다. 외부 네트워크와 VPN 장비 사이에 PAS-K(외부 PAS-K)를 배치하고, VPN 장비와 내부 네트워크 사이에 또 하나의 PAS-K(내부 PAS-K)를 배치합니다. 외부 PAS-K는 외부 네트워크에서 내부 네트워크로 들어오는 패킷의 부하 분산을 담당하고 내부 PAS-K는 반대로 내부 네트워크에서 외부 네트워크로 나가는 패킷의 부하 분산을 담당합니다.

PAS-K는 통신의 일관성을 유지해주기 위하여 특정 클라이언트의 패킷은 항상 특정 VPN으로 분산 처리합니다. 그리고, 하나의 VPN 장비에 장애가 발생하면 다른 VPN 장비에 의해 클라이언트의 패킷이 지속적으로 처리될 수 있도록 해줍니다.

지점 간 VPN 연결 기능

PAS-K는 여러 개의 지점 네트워크가 존재하는 VPN 부하 분산 구성에서 지점과 지점 사이의 통신이 본사 네트워크의 VPN을 경유하는 특수한 구성에서는 '지점 간 VPN 연결' 기능을 사용해야 합니다. 지점 간 VPN 연결 기능을 사용하면, 지점 대 지점 사이의 통신이 본사 VPN 장비를 거치는 경우 이를 본사 내부망으로 전송하지 않고 다시 지점으로 전송하여, 지점 간 VPN 연결을 지원하게 됩니다.

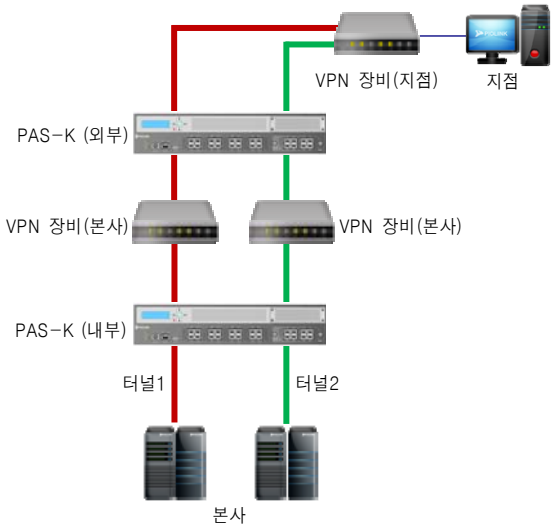
지속 연결

VPN 구성에서 본사의 호스트와 특정 지점의 호스트 사이의 지속 연결이 이루어지면, 이 지속 연결에 해당되는 터널을 통해 패킷이 전송되도록 해야 합니다. 즉, 터널을 형성한 VPN 장비로만 스위칭이 이루어지도록 해야 합니다.

VPN 장비에는 하나의 게이트웨이 IP 주소만 지원하는 단일 터널 VPN 장비와 동시에 여러 개의 게이트웨이 IP 주소를 지원하는 다중 터널 VPN 장비가 있습니다. 단일 터널 VPN 장비의 부하 분산 구성에서는 PAS-K에 별도의 설정 작업을 하지 않아도 지속 연결 기능을 사용할 수 있습니다. 그러나, 다중 터널 VPN 장비의 부하 분산 구성에서 지속 연결 기능을 사용하려면, PAS-K에 다중 터널 지속 연결 기능을 반드시 활성화해야 합니다. 다중 터널 지속 연결 기능에 대해 상세하게 알아봅니다.

다중 터널의 지속 연결

다음은 2대의 PAS-K를 사용하여 구성한 다중 터널 VPN 장비의 부하 분산 구성도입니다.



[그림 - 다중 터널 VPN 장비의 부하 분산 구성도]

단일 터널 VPN 장비를 사용하는 부하 분산 구성의 경우, 동일한 지점 IP 주소를 가진 호스트와 본사 사이에 하나의 터널만 이루어지기 때문에, 내부 PAS-K는 지점의 IP 주소만 이용하여 지속 연결 기능을 지원할 수 있습니다. 그러나, 위의 그림에서와 같이 다중 터널 VPN 장비를 사용하는 부하 분산 구성에서는 지점 IP 주소만으로는 지속 연결 기능을 형성할 수 없습니다.

다중 터널 구성에서는 동일한 지점 IP 주소로 가는 터널이 두 개가 형성될 수 있어, 본사에서 지점으로 패킷을 보낼 때 다른 터널을 사용할 가능성이 있기 때문입니다. 그러므로, 다중 터널 VPN 장비를 사용한 부하 분산 구성인 경우, 내부 PAS-K는 지점의 IP 주소와 본사의 IP 주소를 모두 사용하여 지속 연결을 형성할 터널을 결정해야 합니다. PAS-K에서 다중 터널의 지속 연결 기능을 활성화하면 지점의 IP 주소와 본사의 IP 주소를 모두 사용하여 지속 연결 기능을 수행하게 됩니다.

참고: 다중 터널의 지속 연결 기능은 내부 PAS-K에만 활성화하면 됩니다. 외부 PAS-K는 VPN 장비들의 게이트웨이 IP 주소로 지속 연결을 형성하기 때문에 다중 터널의 지속 연결 기능을 활성화할 필요가 없습니다.

필터

PAS-K의 VPN 부하 분산에서도 방화벽 부하 분산과 마찬가지로 부하 분산을 적용할 트래픽을 필터링하기 위해 필터를 사용합니다. 필터는 프로토콜의 종류와 패킷의 송수신/목적지 IP 주소와 출발지/목적지 포트 번호 등을 다양하게 조합하여 정의할 수 있습니다. 필터의 종류에는 부하 분산 서비스를 적용하려는 트래픽을 필터링하기 위한 'include' 타입과 적용하지 않을 트래픽을 필터링하는 'exclude' 타입이 있습니다.

캐시 서버 부하 분산

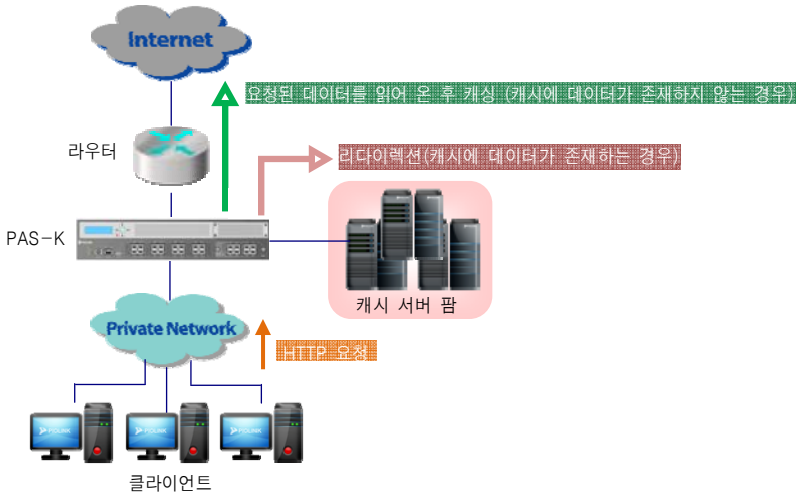
개요

PAS-K의 캐시 서버 부하 분산(Cache Server Load Balancing-CSLB)은 클라이언트의 접속이 많은 웹 트래픽이나 애플리케이션 트래픽을 캐시 서버 팜(cache server farm)으로 리다이렉션(redirection) 해주는 기능입니다.

캐시 서버 부하 분산 기능은 클라이언트에 의해 요청된 정보를 로컬 네트워크에 있는 캐시 서버에 저장해뒀다가 이 후에 클라이언트가 같은 정보를 요청하는 경우 인터넷으로 접속하지 않고 캐시 서버에 저장되어 있는 정보를 보내주는 기능입니다. 인터넷을 통해 다운로드하는 정보 중 대부분이 이전에 다운로드되었던 정보입니다. 이전에 다운로드했던 정보와 중복된 정보들을 인터넷을 통해 계속해서 다운로드하기 위해서는 많은 양의 대역폭이 요구됩니다. 캐시 서버 부하 분산 기능을 사용하면 이와 같이 중복된 정보에 소요되던 대역폭을 절약하여 네트워크의 효율성을 높여줄 수 있습니다. 뿐만 아니라 로컬 네트워크에 연결된 캐시 서버로부터 데이터를 받아오기 때문에 인터넷을 통해 같은 정보를 요청하는 것보다 클라이언트는 훨씬 빨리 정보를 수신할 수 있습니다.

캐시 서버 부하 분산 구성

다음 그림은 PAS-K를 사용하여 구성한 일반적인 캐시 서버 부하 분산 구성도입니다.



[그림 - PAS-K를 이용한 캐시 서버 부하 분산 구성도]

클라이언트에서 외부 네트워크의 데이터를 요청하면 PAS-K는 이 요청이 외부 네트워크로 나가기 전에 가로채어 캐시 서버에 저장된 데이터를 요청하는지 여부를 확인합니다.

캐시 서버 팜의 캐시 서버들은 리다이렉션된 트래픽이 캐시 서버에 저장하고 있는 컨텐트를 요구하는 경우에 해당 컨텐트를 서비스해주고, 그렇지 않은 경우는 그 트래픽이 요구하는 컨텐트를 외부 네트워크를 통해 읽어온 후 캐싱(caching)합니다. 내부 클라이언트의 요구를 캐싱해주는 서버를 normal 캐시라고 하고 외부 클라이언트의 요구를 캐싱하는 서버를 reverse 캐시라고 합니다. PAS-K는 이 두 가지 캐시 서버를 모두 지원합니다.

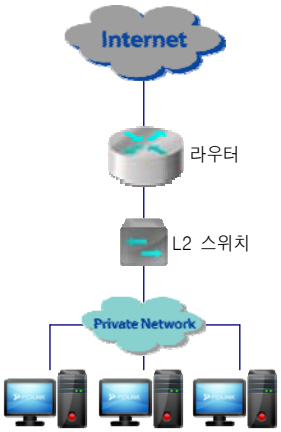
PAS-K는 클라이언트들이 캐시 서버에 대해 별도의 프록시를 설정할 필요가 없는 투명한 캐시 리다이렉션(transparent cache redirection)을 제공합니다. PAS-K는 웹 트래픽 뿐만 아니라 실시간 스트리밍 프로토콜인 RTSP(Real time streaming protocol: TCP/UDP 554)와 NNTP(Net news transfer protocol: TCP 119)와 같은 일반적인 애플리케이션에 대해서도 캐시 리다이렉션을 유연성있게 지원합니다. 또한, 특정한 네트워크 대역에 대해서는 캐시로 리다이렉션하지 않고 직접 실제 서버로 접속할 수 있도록 해주는 바이패스(bypass) 기능도 지원합니다.

필터

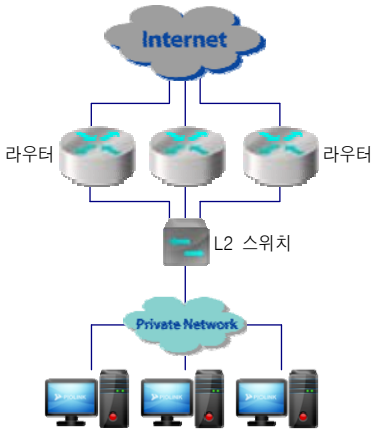
캐시 서버 부하 분산도 방화벽 부하분산 및 VPN 부하 분산과 마찬가지로 캐시 서버 부하 분산을 적용할 트래픽을 위한 필터를 사용합니다. 필터를 통해 캐시 서버 부하 분산 기능을 적용할 트래픽과 적용하지 않을 트래픽을 구분할 수 있습니다. 캐시 서버 부하 분산에서 사용할 수 있는 필터에는 부하 분산을 적용할 트래픽을 위한 조건으로 구성된 'include' 타입과 적용하지 않을 트래픽을 위한 조건으로 구성된 'exclude' 타입이 있습니다.

게이트웨이 부하 분산

하나의 게이트웨이 라인을 통해 외부 네트워크와 연결되어 있는 네트워크의 경우, 네트워크의 규모가 커지거나 네트워크 트래픽이 증가하게 되면, 게이트웨이 라인의 대역폭이 한정되어 있기 때문에 늘어난 트래픽의 양에 비례하여 네트워크 속도가 낮아지게 됩니다. 그리고, 게이트웨이 라인이 하나이기 때문에 라인의 연결 상태가 불안정해지면 전체 네트워크의 안정성에 영향을 미치게 됩니다. 이러한 문제를 방지할 수 있는 방법으로, 추가로 게이트웨이 라인을 더 확보하고, 네트워크를 여러 서브넷으로 분류하여 각 서브넷마다 다른 게이트웨이 라인을 통해 외부 네트워크로 접속하도록 할 수 있습니다.

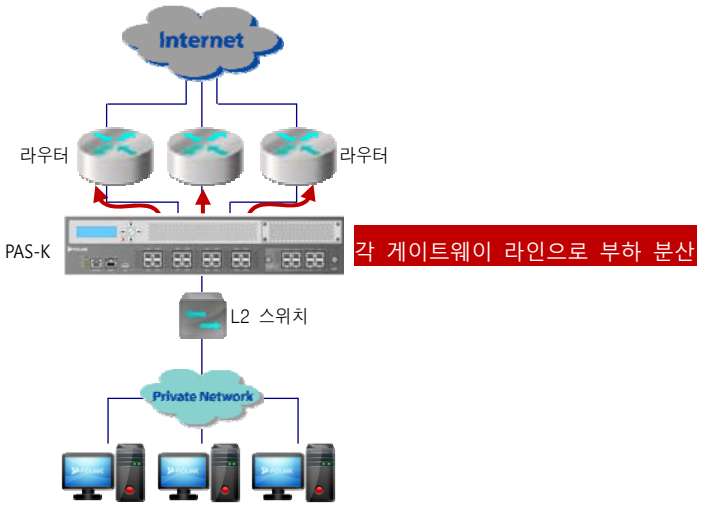


하나의 게이트웨이 라인으로 연결된 네트워크



여러 개의 게이트웨이 라인으로 연결된 네트워크

여러 개의 게이트웨이 라인을 사용하면, 한꺼번에 네트워크 전체가 통신이 되지 않는 문제가 해결되고 네트워크를 서브넷으로 나눔으로 인해 각 게이트웨이 라인의 부하를 줄일 수 있습니다. 하지만, 특정한 서브넷에 트래픽의 양이 급속히 증가할 경우, 해당 서브넷의 속도는 느려질 수 밖에 없습니다. 그리고, 일부 게이트웨이 라인의 연결이 끊어지면, 해당 게이트웨이 라인에 연결된 서브넷은 외부 네트워크와 통신할 수 없게 됩니다. PAS-K는 여러 게이트웨이 라인을 사용하여도 막을 수 없는 이러한 문제들을 해결해주는 게이트웨이 부하 분산 기능(Gateway Load Balancing - GWLB)을 제공합니다.



PAS-K의 게이트웨이 부하 분산 기능은 게이트웨이 라인의 상태를 지속적으로 모니터링하고, 위 그림과 같이 내부 네트워크에서 외부 네트워크로 전송되는 트래픽을 정상적으로 연결되어 있는 게이트웨이 라인으로 분산 시켜줍니다. 그러므로, 일부 게이트웨이 라인의 연결이 끊어져 있는 경우에도 내부 네트워크 모든 사용자들은 외부 네트워크로 접속할 수 있습니다. PAS-K의 게이트웨이 부하 분산 기능은 hash, round robin, least connection, weighted round robin 등의 방식을 사용하여 효율적으로 트래픽을 분산하기 때문에 특정한 게이트웨이 라인에 트래픽이 집중되는 현상도 막을 수 있습니다. 이 밖에도 PAS-K의 게이트웨이 부하 분산 기능을 사용하면, 기존 네트워크 구성이나 설정을 변경할 필요 없이 쉽게 게이트웨이 라인을 추가할 수 있습니다.

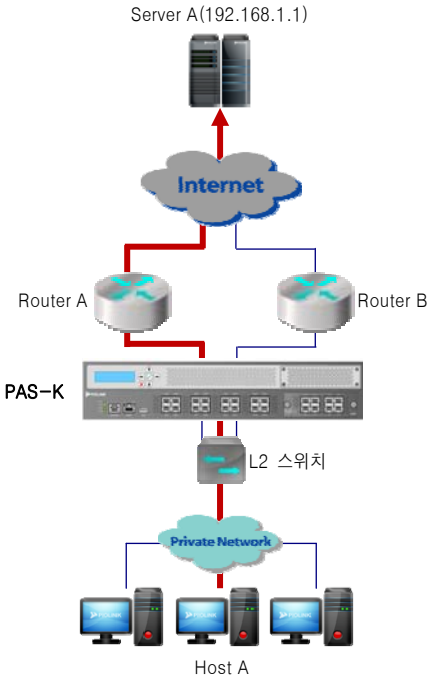
일반적으로, 내부 네트워크에서는 사설 IP 주소를 사용하고, 게이트웨이 라인이 연결된 인터페이스에는 공인 IP 주소가 할당됩니다. 이러한 네트워크에서는 게이트웨이 단에서 사설 IP 주소와 공인 IP 주소를 변환하는 NAT(Network Address Translation) 기능이 필수적으로 지원되어야 합니다. PAS-K의 게이트웨이 부하 분산 기능도 다음과 같은 2가지 유형의 NAT 기능을 제공합니다.

- **Source NAT**
  Source NAT는 내부에서 외부 네트워크로 향하는 트래픽의 출발지 주소(사설 IP 주소)를 공인 IP 주소로 변환해 주는 기능으로, 기존에 제공되던 IP 매스커레이딩(masquerading) 기능을 개선한 기능으로 확인할 수 있습니다. 게이트웨이 라인이 연결된 인터페이스마다 다른 공인 IP 주소가 할당된 경우에는 각 게이트웨이 라인을 통해 전송되는 트래픽의 사설 IP를 해당 공인 IP 주소로 변환합니다. 그러므로, 트래픽이 부하 분산된 경우에도, 트래픽의 출발지 주소는 부하 분산 방식에 의해 선택된 게이트웨이 라인의 공인 IP 주소로 정확하게 변환됩니다.

- **One-to-One NAT**
  One-to-One NAT는 미리 정의된 공인 IP 주소를 사용하여 외부 네트워크에서 PAS-K로 접속했을 때, 트래픽의 목적지 IP 주소를 지정된 특정 사설 IP 주소로 변환해주는 기능입니다. One-to-One NAT 기능을 적용할 공인 IP 주소와 사설 IP 주소는 사용자가 직접 지정할 수 있습니다.

동작 과정

다음은 PAS-K의 내부 네트워크에 있는 Host A가 외부 네트워크에 있는 서버인 Server A(192.168.1.1)로 접속하는 경우, GWLB 기능이 동작하는 과정입니다(Source NAT).

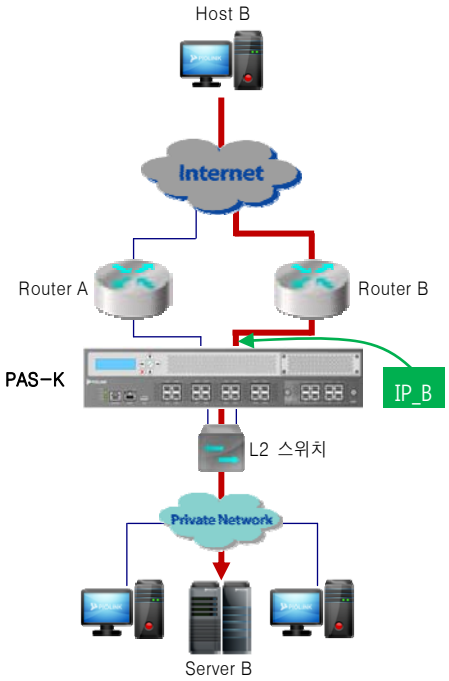


[그림 - PAS-K를 이용한 게이트웨이 부하 분산 동작 과정(Source NAT)]

1. Host A가 외부 서버인 Server A를 목적지로 하는 트래픽을 발생시킵니다.
2. 트래픽이 PAS-K로 수신되면 PAS-K는 트래픽이 게이트웨이 부하 분산 서비스에 정의된 필터에 매칭되는지 확인합니다. 이를 위해, 필터의 조건과 트래픽의 출발지, 목적지 IP 주소, 프로토콜, 포트 등을 비교합니다. 여러 개의 게이트웨이 부하 분산 서비스가 정의되어 있는 경우에는 우선순위가 가장 높은 서비스의 필터부터 비교하고, 트래픽이 필터에 매칭되지 않으면 다음 우선순위를 가진 서비스의 필터와 비교합니다.
3. 트래픽이 필터에 매칭되면, 해당 게이트웨이 부하 분산 서비스의 부하 분산 방식에 의해 두 라우터 중 하나가 선택됩니다. 여기에서는 Router A가 선택된 것으로 가정합니다.

4. Router A에 연결된 게이트웨이 라인(실제 서버, 게이트웨이 부하 분산에서는 라우터와 연결된 게이트웨이 라인이 실제 서버가 됩니다)에 정의된 NAT 규칙 중에서 트래픽의 출발지 IP 주소와 일치하는 것이 있는지 검색합니다.
5. 트래픽의 출발지 IP 주소를 일치한 NAT 규칙의 NAT IP 주소로 변경한 후 트래픽을 외부 네트워크로 전송합니다.
6. 트래픽을 수신한 Server A는 Host A에게 응답하기 위해 NAT IP 주소를 목적지로 하는 트래픽을 전송합니다.
7. 이 트래픽을 수신한 PAS-K는 앞서 트래픽을 외부로 전송할 때 생성된 엔트리를 이용하여 트래픽의 목적지 IP 주소(NAT IP 주소)를 Host A의 IP 주소로 변경한 후 내부 네트워크로 전송합니다.

다음은 외부 네트워크에 있는 Host B가 사설 IP 대역인 PAS-K의 내부 네트워크의 Server B로 접속하고자 할 때, GWLB 기능이 동작하는 과정입니다(One-to-One NAT).



[그림 - PAS-K를 이용한 게이트웨이 부하 분산 동작 과정(One-to-One NAT)]

1. Host B에서 미리 정의된 공인 IP 주소인 IP_B를 목적지로 하는 트래픽을 발생시킵니다.
2. IP_B는 Router B에 해당하는 사업자가 할당한 IP 주소이므로, 트래픽은 Router B를 통해 PAS-K로 전송됩니다.
3. 트래픽을 수신한 PAS-K는 이 트래픽이 게이트웨이 부하 분산 서비스에 정의된 필터에 매칭되는지 확인합니다. 이를 위해, 필터의 조건과 트래픽의 출발지, 목적지 IP 주소, 프로토콜, 포트 등을 비교합니다. 여러 개의 게이트웨이 부하 분산 서비스가 정의되어 있는 경우에는 우선순위가 가장 높은 서비스의 필터부터 비교하고, 트래픽이 필터에 매칭되지 않으면 다음 우선순위를 가진 서비스의 필터와 비교합니다.
4. 트래픽이 필터에 매칭되면, PAS-K는 이 엔트리를 reverse 엔트리로 생성하고, Router B와 연결된 게이트웨이 라인(실제 서버)에 설정된 NAT 규칙 중에서 외부(external) IP 주소가 트래픽의 목적지 IP 주소(IP_B)와 일치하는 것이 있는지 검색합니다.
5. 트래픽의 목적지 IP 주소와 NAT 규칙의 외부 IP 주소가 일치하는 경우, 해당 NAT 규칙의 내부(internal) IP 주소를 트래픽의 목적지 IP 주소로 변경한 후, 내부 네트워크로 전송합니다.
6. 트래픽을 수신한 내부 서버 Server B는 Host B에게 응답하기 위해 Host B의 주소로 트래픽을 전송합니다.
7. 이 트래픽을 수신한 PAS-K는 앞서 트래픽을 외부에서 수신할 때 생성된 엔트리를 이용하여 트래픽의 출발지 IP 주소(외부 IP 주소)를 IP_B로 변경하여 외부 네트워크로 전송합니다.

필터와 NAT 규칙

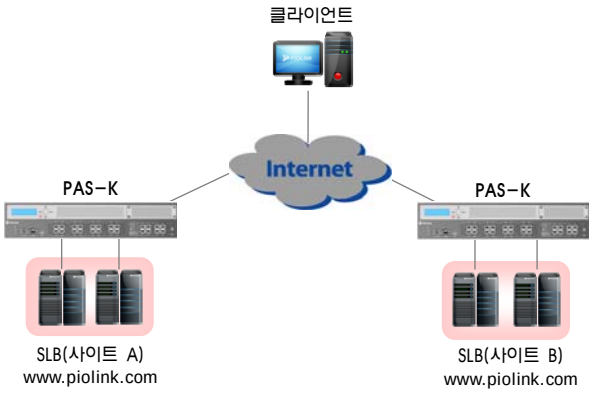
게이트웨이 부하 분산 기능도 방화벽/VPN 부하 분산 기능과 마찬가지로 부하 분산을 적용할 트래픽을 검색하기 위해 필터를 사용합니다. 필터를 통해 게이트웨이 부하 분산 기능을 적용할 트래픽과 적용하지 않을 트래픽을 분류할 수 있습니다. 게이트웨이 부하 분산에서 사용할 수 있는 필터의 유형에는 부하 분산을 '적용'할 트래픽을 구분하기 위한 조건으로 구성된 'include' 유형과 적용하지 '않을' 트래픽을 구분해내기 위한 조건들로 구성된 'exclude' 유형이 있습니다.

트래픽이 필터의 조건에 매칭되면, 게이트웨이 부하 분산 서비스는 설정된 부하 분산 방식에 따라 트래픽이 전송될 게이트웨이 라인(실제 서버)을 선택합니다. 게이트웨이 라인이 선택되면, 그 게이트웨이 라인의 NAT 규칙과 트래픽을 비교한 후, NAT 규칙의 조건에 일치하는 트래픽에만 NAT 규칙이 적용됩니다. NAT 규칙의 유형에는 Source NAT와 One-to-One NAT가 있습니다. Source NAT 유형은 NAT 조건으로 출발지와 목적지 IP 주소를 지정하고, 출발지 IP 주소 변환 시 사용할 NAT IP 주소를 지정합니다. One-to-One NAT 유형은 NAT 조건으로 공인 IP 주소와 비교할 외부 IP 주소(external IP)를 지정하고, 외부 IP 주소 대신 사용할 내부 IP 주소(internal IP)를 지정합니다.

글로벌 서버 부하 분산

글로벌 서버 부하 분산(GSLB - Global Server Load Balancing)은 말 그대로 서버 부하 분산(SLB) 기능을 확장시킨 기능입니다. 서버 부하 분산의 부하 분산 대상은 사이트 내부의 '서버'이지만, 글로벌 서버 부하 분산의 부하 분산 대상은 서버 부하 분산이 적용된 '사이트'입니다. 서버 부하 분산(SLB)은 사이트의 트래픽을 서버들로 적절하게 분산시키고, 글로벌 서버 부하 분산은 트래픽을 사이트로 적절하게 분산 시킵니다. 글로벌 서버 부하 분산에 의해 사이트로 분산된 트래픽은 다시 SLB에 의해 적절한 서버로 분배됩니다. 물론, SLB의 대상이 되는 서버들과 글로벌 서버 부하 분산의 대상이 되는 사이트들은 모두 동일한 서비스(예: 동일한 웹 사이트)를 제공해야 합니다.

다음 그림과 같이 www.piolink.com을 서비스하는 사이트 A와 사이트 B는 물리적으로 떨어져 있지만, PAS-K의 글로벌 서버 부하 분산 기능을 사용하여 www.piolink.com에 대한 클라이언트의 트래픽을 두 사이트가 적절히 나누어 처리하도록 할 수 있습니다.



[그림 - PAS-K를 이용한 글로벌 서버 부하 분산]

이러한 글로벌 서버 부하 분산 기능을 사용하면 한 사이트에 장애가 발생하더라도 나머지 사이트에서 계속 서비스를 제공할 수 있으므로 사이트에서 발생할 수 있는 예상치 못한 장애에 대비할 수 있습니다. 그리고, 가용한 사이트 중에서도 가장 적절한 사이트를 클라이언트에게 알려줌으로써 클라이언트가 사이트에 접속하는 시간을 줄여줄 수 있습니다.

PAS-K의 글로벌 서버 부하 분산 기능은 DNS(Domain Name Server)를 기반으로 이루어집니다. 클라이언트가 글로벌 서버 부하 분산 대상이 되는 사이트에 대한 DNS 질의를 전송하면 이에 대한 응답을 PAS-K가 수행하게 됩니다. PAS-K는 사이트의 상황(장애 감시 결과와 부하 분산 방식의 결과)에 따라 적절한 사이트를 선택하고, 선택한 사이트의 가상 IP 주소를 클라이언트에게 보내줍니다. 이 후 클라이언트는 이 가상 IP 주소를 사용하여 사이트로 접속합니다. 보다 상세한 과정은 [글로벌 서버 부하 분산 동작 과정] 절에서 설명합니다.

용어

다음은 글로벌 서버 부하 분산 기능을 이해하고 PAS-K에서 글로벌 서버 부하 분산을 설정하기 위해 알아두어야 할 용어입니다.

- **영역(zone), 도메인, 호스트**
  www.piolink.com, www1.piolink.com, ftp.piolink.com, mail.piolink.com은 모두 하나의 도메인으로, piolink.com 이라는 영역의 도메인입니다. 그리고, www, www1, ftp, mail은 호스트입니다. 도메인은 영역이 될 수 있습니다. www.piolink.com은 도메인이지만, a.www.piolink.com, b.www.piolink.com 도메인의 영역이 됩니다. DNS 서버에는 각 영역 별로 네임 서버를 지정하고, PAS-K의 글로벌 서버 부하 분산 기능도 '영역'단위로 동작합니다. www.piolink.com과 ftp.piolink.com 도메인에 대한 DNS 질의를 처리하려면 먼저, 영역으로 piolink.com을 정의하고 호스트로 www와 ftp를 지정해야 합니다.

- **실제 서버**
  글로벌 서버 부하 분산에서 실제 서버는 부하 분산 대상이 되는 사이트의 가상 IP 주소입니다. 특정 서버의 IP 주소 또는 PAS-K에 등록된 SLB 서비스의 가상 IP 주소를 실제 서버로 지정해야 합니다. 실제 서버의 IP 주소는 DNS 응답으로 클라이언트에게 전달되고 클라이언트는 이 IP 주소를 사용하여 사이트로 접속합니다.

- **장애 감시**
  글로벌 서버 부하 분산의 장애 감시 기능은 실제 서버로 등록된 IP 주소에 대한 상태를 검사합니다.

- **규칙(rule)**
  글로벌 서버 부하 분산 서비스는 실제 서버를 선택할 때 규칙을 사용합니다. 규칙은 실제 서버를 선택하기 위한 부하 분산 방식과 규칙을 적용할 도메인의 호스트 등으로 구성됩니다.

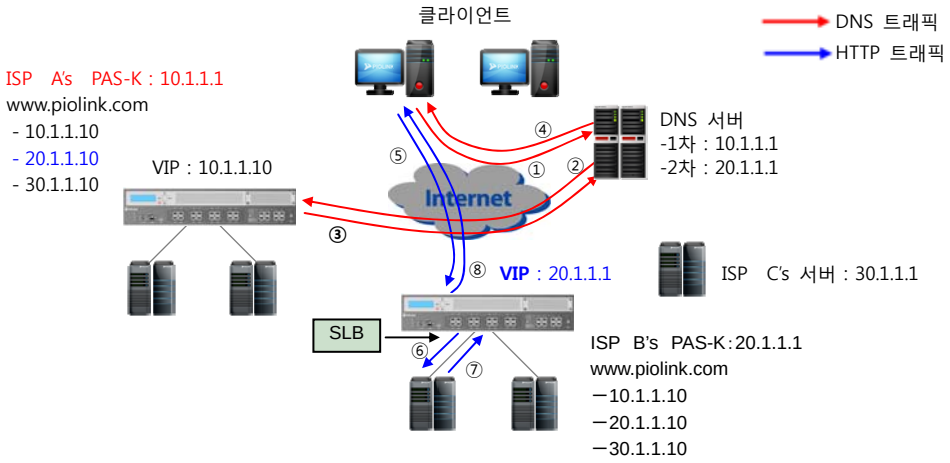
글로벌 서버 부하 분산 동작 과정

글로벌 서버 부하 분산을 위해 PAS-K로 수신된 DNS 질의에 응답하려면 PAS-K가 네임 서버로 동작해야 합니다. 그리고, 외부의 상위 DNS 서버에 PAS-K를 네임 서버로 등록해야 합니다.

그러면, 외부의 상위 DNS 서버는 클라이언트로부터 PAS-K에 등록된 서비스에 대한 DNS 질의를 수신했을 때 서버의 IP 주소를 알아내기 위해 그 질의를 PAS-K로 전송합니다. DNS 질의를 받은 PAS-K는 글로벌 서버 부하 분산 서비스의 부하 분산 방식을 통해 하나의 실제 서버를 선택하고, 선택한 실제 서버의 IP 주소를 응답해줍니다. 외부의 상위 DNS 서버는 PAS-K로부터 수신한 IP 주소를 클라이언트에게 알려주게 되고, 이 후 클라이언트는 이 IP 주소를 사용하여 서버의 도메인으로 접속을 시도합니다.

글로벌 서버 부하 분산 서비스는 등록된 실제 서버에 장애가 발생하면 이 서비스를 응답 대상에서 제외시킵니다. 하지만, 이전에 이 실제 서버의 IP주소를 응답 받은 클라이언트는 이 주소를 로컬 PC의 DNS 캐시 정보에 저장하여 TTL(Time to Live)시간 동안 이용하기 때문에 서비스를 제공할 수 없는 서버로 접속할 수 있습니다. 이를 방지하려면 글로벌 서버 부하 분산을 설정할 때 TTL 값을 일반적인 DNS 서버보다는 작게 설정하여 클라이언트가 DNS 캐시에 저장하는 시간을 단축시키는 것이 좋습니다. 글로벌 서버 부하 분산의 기본 TTL 값은 10초입니다.

다음은 서비스의 안정화를 위해 ISP A, ISP B, ISP C의 3개 지역으로 서버들을 분산시켜 구성하고, ISP A와 ISP B의 서버에는 서버 부하 분산(SLB) 서비스가 설정된 구성입니다. ISP A와 ISP B에 설치된 PAS-K는 글로벌 서버 부하 분산 기능과 SLB 기능이 동시에 동작을 하고 있으며, 클라이언트는 ISP A와 ISP B의 서버에 접속할 때 PAS-K의 가상 IP 주소(SLB에 설정된 가상 IP 주소)를 사용합니다.



[그림 - PAS-K를 이용한 글로벌 서버 부하 분산]

ISP A와 ISP B에 설치된 PAS-K의 글로벌 서버 부하 분산 기능은 실제 서버로 ISP A와 ISP B의 가상 IP 주소(10.1.1.10, 20.1.1.10)와 ISP C의 IP 주소(30.1.1.10)가 설정됩니다. ISP A와 ISP B의 PAS-K는 주기적으로 실제 서버의 상태를 검사(장애 감시)하여 서비스가 가능한 서버를 확인하고 부하 분산을 수행하게 됩니다.

이러한 구성에서 클라이언트가 **www.piolink.com** 웹 서버에 접속하려면 다음과 같은 과정들이 수행됩니다.

1. DNS 질의/응답

① 클라이언트가 www.piolink.com 에 대한 DNS 질의를 DNS 서버로 전송합니다.

② DNS 서버는 등록되어 있는 네임 서버 정보를 조회(상위 DNS 서버와의 통신은 생략)하여 piolink.com 영역에 속한 도메인의 네임 서버가 10.1.1.1와 20.1.1.1인 것을 알아내고 1차 네임서버로 설정된 10.1.1.1에 www.piolink.com 에 대한 DNS 질의를 전송합니다.

③ ISP A에 위치한 10.1.1.1 PAS-K는 글로벌 서버 부하 분산 서비스에 설정된 서비스로 요청된 것을 확인하고 등록된 3개의 실제 서버 IP 주소 중에서 최적의 IP 주소를 선택합니다. 위 구성에서는 20.1.1.10을 응답합니다.

④ PAS-K로부터 www.piolink.com 이 20.1.1.10이라는 응답을 수신한 DNS 서버는 이 주소를 클라이언트에게 보냅니다.

2. HTTP 트래픽 전송

⑤ DNS 서버의 응답을 수신한 클라이언트는 www.piolink.com으로 접속하기 위해 수신한 IP 주소인 20.1.1.10으로 접속을 시도합니다.

⑥ ISP B에 위치한 PAS-K는 클라이언트의 요청을 수신하고(SLB 가상 IP 주소로), 일반적인 SLB 서비스를 통해 최상의 서버를 선택하여 클라이언트의 요청을 전송합니다.

⑦ 클라이언트의 요청을 수신한 서버는 일반적인 웹 서버로서의 응답을 하게 됩니다.

⑧ 웹 서버로부터 응답을 받은 PAS-K는 출발지 IP 주소를 클라이언트가 요청한 가상 IP 주소(20.1.1.10)으로 변경한 후 클라이언트에게 전달합니다.

DNS 서버는 일반적인 DNS 질의와 마찬가지로 먼저 1차 네임 서버로 질의한 후 응답이 없으면 2차 네임 서버로 질의하게 됩니다. 그러므로, 이 구성에서 ISP A의 PAS-K나 모든 서버에 장애가 발생해도 DNS의 동작 원리에 의해 ISP B의 PAS-K로 DNS 질의를 전송하게 됩니다. PAS-K는 정상적으로 동작하지만, 내부의 서버가 동작하지 않는 경우에는 DNS 질의를 받았을 때 다른 사이트의 서비스 IP 주소를 응답합니다.

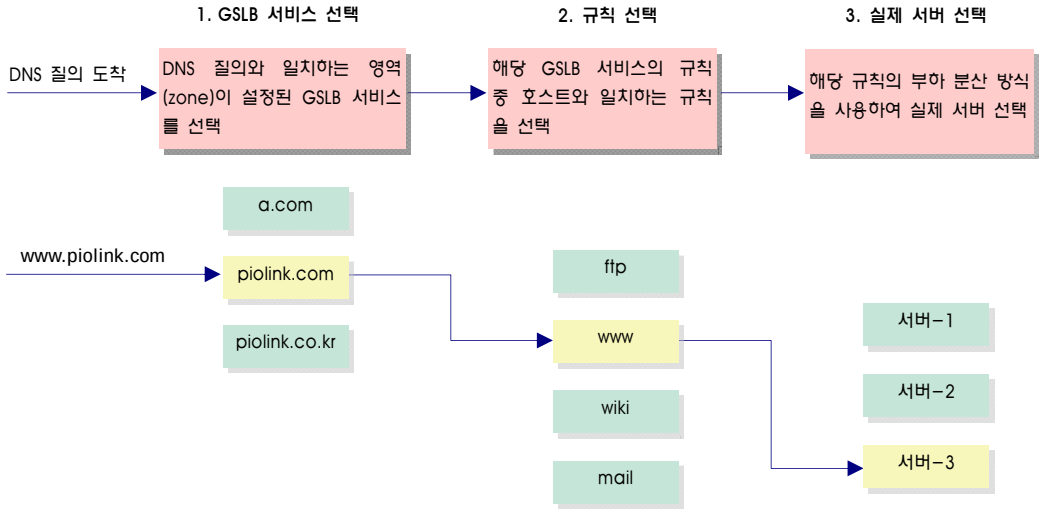
PAS-K의 DNS 동작

글로벌 서버 부하 분산 기능을 사용하기 위해서는 PAS-K가 네임 서버 기능을 수행해야 합니다. PAS-K가 네임 서버로 동작하기 위해서는 클라이언트에게 알려줄 DNS 정보(도메인과 IP 주소)를 가지고 있어야 합니다. 다음은 PAS-K가 DNS 서버로 동작하는 과정입니다.

1. DNS 서버로부터 DNS 질의를 수신한 PAS-K는 설정된 글로벌 서버 부하 분산 서비스를 검색하여 질의된 도메인이 있는지 확인합니다.
2. 도메인이 검색되면, 글로벌 서버 부하 분산서비스의 부하 분산 방식을 사용하여 하나의 서비스 IP 주소를 선택합니다.
3. 2번 과정에서 알아낸 IP 주소를 DNS 서버로 전송합니다. 이 때, PAS-K에 설정되어 있는 네임 서버 정보도 함께 전송합니다.

실제 서버 선택 과정

앞에서는 PAS-K가 글로벌 서버 부하 분산 서비스를 통해 실제 서버를 선택하는 과정을 단순히 부하 분산 서비스에 정의된 부하 분산 방식을 사용하는 것으로 설명하였지만, 실제로는 다음과 같은 3단계를 통해 실제 서버를 선택합니다. 아래 그림은 www.piolink.com 도메인에 대한 쿼리를 수신했을 때 실제 서버를 선택하는 과정을 보여주는 예입니다.



[그림 – 글로벌 부하 분산 서비스의 실제 서버 선택 과정]

1. 우선 PAS-K는 DNS 질의 메시지가 요구하는 영역에 대한 글로벌 서버 부하 분산 서비스가 설정되어 있는지 확인합니다. 그러므로, 세 개의 글로벌 서버 부하 분산 서비스 중 piolink.com이라는 영역이 설정된 서비스를 선택합니다.
2. 그 후에는 선택한 글로벌 서버 부하 분산 서비스의 규칙 중에서 호스트가 일치하는 규칙을 선택합니다. 여기에서는 4개의 규칙 중 호스트가 www 인 규칙이 선택됩니다.
3. 이 단계에서는 2 단계에 선택한 규칙에 설정된 부하 분산 방식을 사용하여 규칙에 등록된 실제 서버를 선택합니다. 실제 서버는 SLB 서비스의 가상 IP 주소나 일반 서버의 IP 주소가 될 수 있습니다. 이 그림에서는 3개의 실제 서버 중에 서버-3을 선택하고 이 실제 서버의 IP 주소를 DNS 응답으로 전송합니다.

L4 부하 분산 서비스의 고가용성 기능

PAS-K는 PAS-K의 상태나 L4 부하 분산 서비스의 동작 상태, 실제 서버의 상태와 관계없이 계속해서 서비스를 처리할 수 있도록 하기 위해 다음과 같은 고 가용성(High availability)기능들을 제공합니다.

- 실제 서버 백업
- 서비스 백업
- Stateful Failover
- 세션 유지 시간

각 기능에 대해 살펴봅니다.

실제 서버 백업

실제 서버 백업은 실제 서버가 더 이상 세션을 처리할 수 없는 상태가 되었을 때, 실제 서버의 역할을 대신 수행할 백업 서버를 지정할 수 있는 기능입니다. 다음과 같은 상황이 되면 PAS-K는 실제 서버가 세션을 처리할 수 없다고 판단하고 백업 서버를 통해 세션을 처리합니다.

- 장애 감시 결과 실제 서버가 동작하지 않는 것으로 판단되는 경우
  이 경우에는 기존에 실제 서버에서 처리되던 세션은 모두 해제되고, 이 후에 수신되는 새로운 세션은 백업 서버로 전송됩니다.
- 실제 서버가 처리 중인 세션의 수가 최대 세션 수(Max connection)에 도달한 경우
  이 경우에는 실제 서버는 현재 세션만 처리하게 되고, 이 후에 수신되는 새로운 세션은 백업 서버로 전송됩니다.

백업 서버는 각 실제 서버마다 하나씩 지정할 수 있고, 하나의 실제 서버는 여러 실제 서버의 백업 서버로 설정될 수 있습니다.

서비스 백업

서비스 백업은 L4 부하 분산 서비스에 속한 모든 실제 서버가 inactive 상태이거나 처리 중인 세션의 개수가 최대 세션 수에 도달하여 더 이상 서비스를 처리할 수 없는 경우에 L4 부하 분산 서비스의 역할을 대신 수행할 백업 서비스를 지정할 수 있는 기능입니다.

Stateful Failover

Stateful failover 기능은 failover(마스터 PAS-K와 백업 PAS-K 간의 절체)가 발생하더라도 기존 마스터 PAS-K의 L4 부하 분산 서비스에서 처리 중이던 서비스가 끊김없이 계속 처리될 수 있도록 해주는 기능입니다. Stateful failover 기능이 활성화되면 마스터 PAS-K와 백업 PAS-K는 일정한 주기마다 서로의 세션 정보를 주고 받아 동기화 작업을 수행합니다. 동기화 작업을 통해 마스터와 백업 PAS-K는 각자 서비스하고 있는 모든 세션들의 정보를 서로 일치시킵니다. 이러한 세션의 동기화 작업을 세션 싱크(session sync)라고 합니다. 세션 싱크는 마스터와 백업 PAS-K 간에 설정된 세션 싱크 VLAN을 통해 이루어집니다. Stateful failover 기능은 각 L4 부하 분산 서비스마다 사용 여부를 지정할 수 있고, 지속 연결(Persistence)을 보장하는 세션만 복구할 것인지 모든 세션을 복구하도록 할 것인지도 설정할 수 있습니다.

참고: 이 장에서는 L4 부하 분산 서비스에 stateful failover 기능을 활성화하는 방법에 대해서만 설명합니다. Stateful failover를 위한 세션 싱크 포트를 설정하는 방법과 failover에 관한 상세한 기능 설명 및 설정 과정은 제9장 Failover에서 소개합니다

주의: Stateful failover 기능을 활성화하면 L4 부하 분산 성능이 저하될 수 있습니다.

세션 유지 시간

PAS-K는 실제 서버와 세션을 생성하거나 생성된 세션을 종료하는 과정에서 생성된 세션 엔트리를삭제하기 위해 L4 서버 부하 분산 서비스별로 세션 유지 시간을 설정할 수 있습니다. L4 서버 부하 분산 서비스에서 세션 유지 시간을 사용하여 엔트리를 삭제할 수 있는 세션에는 TCP 세션과 UDP 세션이 있습니다. 세션 유지 시간에 대한 상세한 설명은 제4장 시스템 관리와 모니터링 – 세션 유지 시간 설정 절을 참고하도록 합니다.

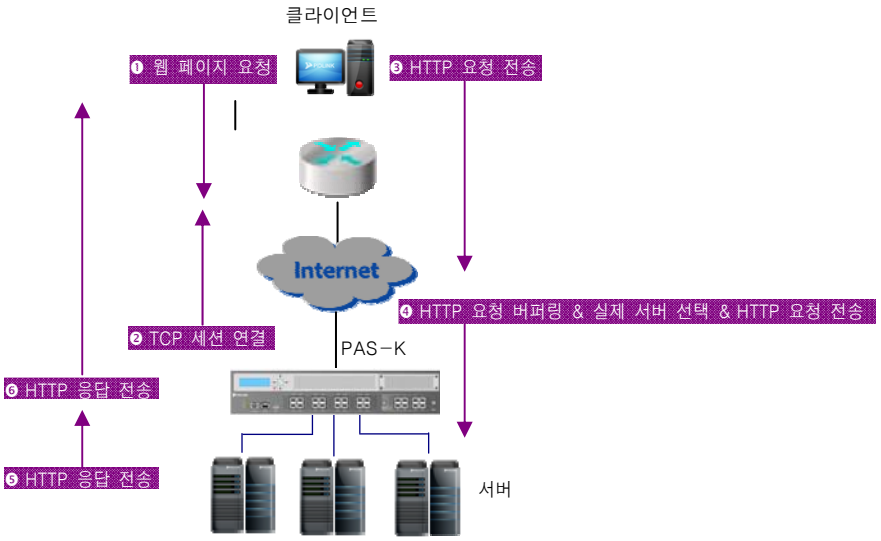
L7 부하 분산

개요

L4 부하 분산은 TCP/IP 헤더에 있는 3, 4계층 정보인 IP 주소와 TCP/UDP 포트 번호를 사용하여 사용자 트래픽을 분산시키는 반해 L7 부하 분산은 7계층 정보인 TCP 페이로드(payload), 애플리케이션 데이터를 사용합니다. PAS-K는 L7 부하 분산을 위해, 수신되는 각 세션에 대해 연결 셋업(connection setup), 트래픽의 구문 해석(parsing), 실제 서버 선택을 위한 부하 분산 방식을 적용, 클라이언트와 PAS-K 간의 TCP 세션과 PAS-K와 서버 간의 TCP 세션을 조정하기 위한 TCP splicing 등 다양한 작업을 수행합니다. PAS-K에서 제공하는 L7 부하 분산의 종류에는 서버 부하 분산과 캐시 서버 부하 분산이 있습니다. PAS-K의 L7 부하 분산 기능은 TCP 프로토콜 상의 HTTP 트래픽에 적용할 수 있습니다. 이 절에서는 PAS-K의 L7 부하 분산 과정과 부하 분산 과정 시 수행하는 작업들, 그리고 L7 서버 부하 분산과 캐시 서버 부하 분산 및 부하 분산 설정 시 사용되는 패턴, 규칙, 그룹 등에 대해 살펴봅니다.

L7 부하 분산 과정

다음은 PAS-K에서 클라이언트의 HTTP 요청에 대한 L7 부하 분산이 수행되는 과정을 보여주는 그림입니다.



[그림 - L7 부하 분산 과정]

수행 과정은 다음과 같은 단계로 이루어집니다.

1. 클라이언트에서 웹 페이지를 요청합니다.
2. 클라이언트의 요청을 수신한 PAS-K는 클라이언트와의 통신에 사용할 TCP 세션을 연결합니다.
3. 클라이언트는 연결된 TCP 세션을 통해 PAS-K로 HTTP 요청을 전송합니다.
4. PAS-K는 HTTP 요청을 버퍼링한 후, 헤더와 URL 정보를 해석하여 이를 기반으로 클라이언트의 HTTP 요청을 처리할 실제 서버를 선택합니다.
5. 선택한 실제 서버로 HTTP 요청을 전송합니다.
6. HTTP 요청을 수신한 실제 서버에서 HTTP 응답을 전송합니다.
7. 실제 서버로부터 수신한 HTTP 응답을 PAS-K가 클라이언트로 전송합니다.

버퍼링

PAS-K는 클라이언트로부터 HTTP 요청을 받으면 전체 컨텐트를 기반으로 실제 서버를 선택해야 하기 때문에 클라이언트의 요청을 버퍼링합니다. 클라이언트의 요청이 하나의 TCP 세그먼트에 들어있을 수도 있지만 때로는 여러 개의 TCP 세그먼트에 나누어져 전송될 수도 있기 때문입니다. PAS-K는 TCP 프로토콜에 따라 최대 8KB까지 TCP 세그먼트들을 버퍼링할 수 있습니다.

구문 해석(Parsing)

클라이언트의 요청이 어떤 정보를 담고 있는지를 알기 위해서는 애플리케이션 레벨의 프로토콜에 따른 데이터의 해석이 필수적입니다. PAS-K는 클라이언트의 요청을 알아내기 위해 HTTP 헤더를 조사합니다. HTTP 요청의 헤더에는 다음과 같이 URI 뿐만 아니라 적절한 HTTP 트랜잭션을 위한 다양한 추가 정보를 담고 있습니다.

```
GET /index.html HTTP/1.1
Accept: "/"
Accept-Language: ko
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.piolink.com
Connection: Keep-Alive
```

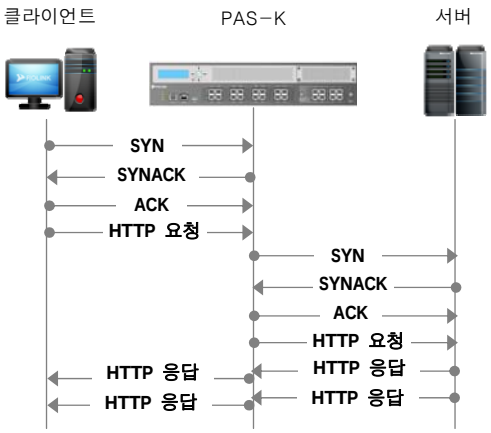
PAS-K는 헤더의 필드 중에서 가장 유용한 필드인 Host와 Cookie, User-Agent, Accept-Language외에도 사용자가 지정한 모든 필드를 구문 해석할 수 있습니다.

지연 바인딩(Delayed Binding)

TCP 프로토콜의 규약에 따라 TCP 페이로드는 TCP 세션이 연결된 후부터 전송되기 시작합니다. 즉, 서버와 클라이언트 간에 TCP 세션이 연결되어야 TCP 페이로드를 수신할 수 있습니다. 하지만, PAS-K는 TCP 페이로드를 기반으로 실제 서버를 선택하기 때문에 TCP 페이로드를 수신하기 전에는 실제 서버를 선택할 수 없습니다.

이를 위해 PAS-K는 실제 서버 대신 클라이언트와의 TCP 접속 과정을 수행하여 TCP 세션을 연결합니다. 이렇게 PAS-K와 클라이언트 사이에 TCP 세션이 연결되면 PAS-K는 클라이언트로부터 받은 HTTP 요청을 분석하고 적절한 실제 서버를 선택합니다. 그리고, 선택된 실제 서버와 TCP 세션을 연결한 후 버퍼링된 클라이언트의 요청을 실제 서버로 전달합니다.

이와 같이 클라이언트와 실제 서버의 TCP 접속이 즉시 이루어지지 않고 HTTP 요청이 모두 수신될 때까지 지연되는 것을 '지연 바인딩(Delayed binding)'이라고 합니다. 다음은 클라이언트와 PAS-K, 그리고 실제 서버 간에 TCP 세션이 맺어지는 지연 바인딩 과정을 보여주는 그림입니다.



[그림 - 지연 바인딩 흐름도]

PAS-K의 L7 캐시 서버 부하 분산의 경우에는 지연 바인딩이 아닌 직접 연결 옵션을 사용하여 클라이언트의 요청을 서버로 전달할 수도 있습니다.

직접 연결(Direct Connect)

직접 연결(Direct Connect)은 클라이언트로부터 TCP SYN 패킷이 수신된 경우, PAS-K가 지연 바인딩을 수행하지 않고 3-way handshake 패킷을 중계하는 방식으로, 클라이언트로부터 HTTP 요청을 수신하는 순간부터 본격적으로 L7 스위칭 처리를 시작합니다.

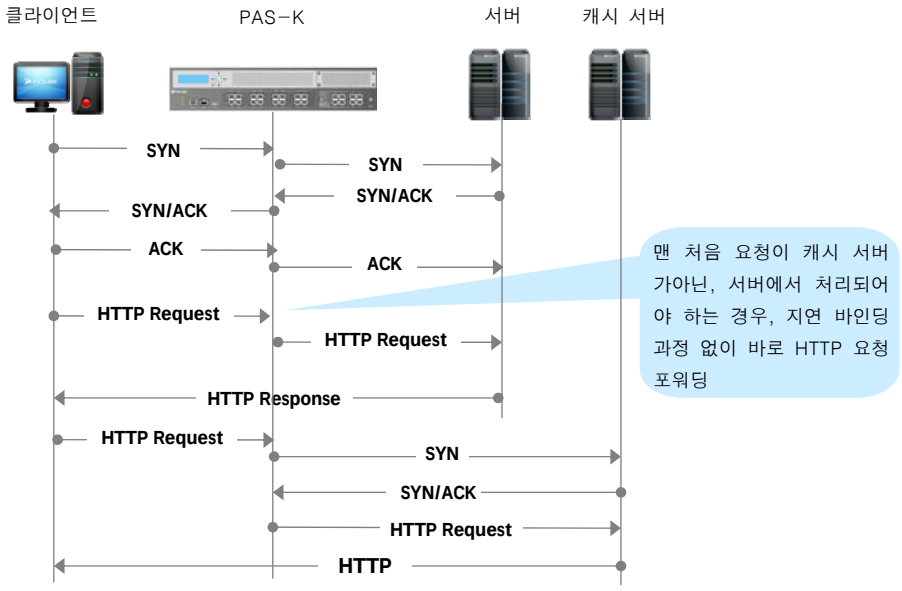
주의: 직접 연결(direct-connect) 옵션은 커넥션 풀링(connection pooling) 기능과 함께 사용할 수 없습니다.

지연 바인딩이 아닌 직접 연결 옵션을 사용하면, 클라이언트는 PAS-K가 아닌 서버와 직접 TCP 연결을 맺게 되고 PAS-K는 중간에서 송수신 되는 패킷을 분석하는 방식으로 트래픽을 처리합니다. 그리고, 클라이언트와 서버가 주고 받는 데이터를 살펴 보다가, 캐시 서버에서 처리 되어야 할 HTTP 요청이 있는 경우 이를 캐시 서버로 부하 분산합니다.

지연 바인딩을 사용하는 경우에는 PAS-K가 TCP 프록시와 같이 중간에 클라이언트의 TCP SYN 패킷을 가로채서 접속을 수락합니다. 그렇기 때문에 악의적인 클라이언트의 공격으로부터 PAS-K가 서버를 일차적으로 보호해주게 됩니다.

그러나 한편, 실제로 서버가 존재하지 않거나 서버에 장애가 발생하여 접속할 수 없는 경우에도 클라이언트는 PAS-K로부터 SYN/ACK 패킷을 전송받기 때문에, TCP 접속이 성공하였다고 판단하게 됩니다. 이렇게 존재하지 않는 서버에 대한 접속 시도가 항상 성공하게 되는 현상은 네트워크의 투명성(네트워크상의 IP주소, 포트 넘버, TCP 혹은 UDP와 같은 프로토콜의 트래픽 주요 특성을 보존하는 것)을 떨어뜨릴 수 있습니다. 따라서, 직접 연결 방식을 사용하면 지연 바인딩 과정 없이 TCP SYN 패킷을 서버로 포워딩 함으로써 이러한 문제를 해결할 수 있습니다.

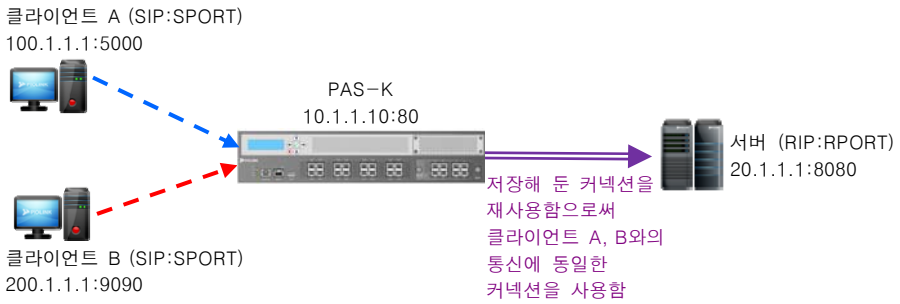
다음 그림은 HTTP 요청에 대해 직접 연결(direct-connect) 옵션이 활성화 되어 있는 경우 L7 캐시 서버 부하 분산이 패킷을 처리하는 과정을 나타낸 그림입니다.



[그림 – 직접 연결 흐름도]

커넥션 풀링(Connection Pooling)

커넥션 풀링(Connection Pooling)은 클라이언트와 PAS-K, 그리고 실제 서버 간에 TCP 커넥션을 연결할 때 매 번 새로운 커넥션을 연결하는 것이 아니라 한번 생성된 커넥션을 풀에 저장해 두었다가 클라이언트로부터 요청이 있을 경우 저장해 두었던 커넥션을 재 사용하는 기능입니다. 다음 그림은 커넥션 풀링의 동작 방법을 보여줍니다.



[그림- 커넥션 풀링의 동작 과정]

100.1.1.1의 가상 IP 주소와 가상 포트 5000을 사용하는 클라이언트 A가 가상 IP 주소와 가상 포트가 각각 10.1.1.10과 80인 PAS-K로 접속해올 경우, 서버 측의 풀에 기존에 사용했던 커넥션이 존재하지 않으면 PAS-K는 지연 바인딩(Delayed Binding)을 하고 가상 IP 주소가 20.1.1.1, 가상 포트가 8080인 서버와의 커넥션을 생성한 후 커넥션에 대한 정보를 풀에 저장합니다.

그 후, 다른 클라이언트 B(IP 주소: 200.1.1.1, 포트: 9090)가 PAS-K로 접속을 시도하면 PAS-K는 새로운 커넥션을 생성하지 않고, 기존에 클라이언트 A와 서버(IP 주소: 20.1.1.1, 포트: 8080)가 사용한 후 저장해 놓은 커넥션을 이용하여 통신합니다.

이러한 커넥션 풀링 기능은 서버 측의 커넥션을 재사용하여 서버가 처리해야 하는 부하를 분산시킴으로써 시스템의 효율을 높여줍니다. 그리고, 서버의 부하 경감에 따라 사용자에게 빠른 속도의 서비스를 제공할 수 있기 때문에 웹 페이지 로딩 시간 단축 및 빠르고 안정적인 서비스를 제공할 수 있습니다.

커넥션 풀링 설정 과정에서는 각 L7 서비스마다 커넥션 풀링 기능의 사용 여부와 커넥션을 재사용할 때 시간을 업데이트할지 여부, 그리고, 'X-Forwarded-For' 헤더의 삽입 여부를 지정할 수 있습니다. 'X-Forwarded-For' 헤더는 장비가 Source NAT를 수행할 경우 서버에서 기존 클라이언트의 IP 주소를 알기 위해 HTTP 요청에 추가하는 헤더입니다.

또한, 각 실제 서버마다 저장할 커넥션의 수(pool-size), 풀에 저장될 커넥션의 유지 시간(pool-age)과 커넥션의 재사용 횟수(pool-reuse) 및 커넥션을 재 사용할 조건(pool-srcmask)을 지정할 수 있습니다. 그리고, 지연 바인딩 시에 특정 IP 주소로 커넥션을 연결하려는 경우에는 Source NAT를 지정할 수 있습니다.

커넥션 재사용 조건

커넥션 풀링 기능을 설정할 경우, 재 사용할 커넥션을 선택하기 위해서는 다음과 같은 조건을 만족해야 합니다. 만약 해당 조건을 모두 만족하는 커넥션이 존재하지 않으면 새로운 커넥션을 생성하게 됩니다.

- 새로운 커넥션과 재사용하려는 커넥션이 적용되는 서비스가 동일해야 합니다.
- 새로운 커넥션과 재사용하려는 커넥션이 부하분산되는 실제 서버가 동일해야 합니다.
- 새로운 커넥션과 재사용하려는 커넥션의 데이터 최대 전송 단위(MSS)가 동일해야 합니다.

실제 서버 선택

PAS-K는 애플리케이션 레벨 프로토콜에 따라 컨텐트를 해석한 후 이를 기반으로 적절한 실제 서버를 선택합니다. 먼저 사용자가 설정한 컨텐트 규칙에 따라 클라이언트의 요청을 어떤 서버 그룹으로 보낼 것인지 결정하고, 그룹이 결정되면 지속 연결 기능과 부하 분산 방식에 의해 그룹에 속한 실제 서버 중에서 하나를 선택합니다.

TCP Splicing

PAS-K는 선택된 서버와 TCP 세션을 연결하면서 '지연 바인딩' 과정을 마치게 됩니다. 지연바인딩이 이루어지면 서로 다른 시점에 맺어진 클라이언트와 PAS-K, 그리고 PAS-K와 서버 간의 두 TCP 세션이 클라이언트와 서버 간의 전체 TCP 세션을 이루게 됩니다. 이 두 TCP 세션이 클라이언트와 서버의 입장에서 완전히 결합된 하나의 TCP 세션처럼 보이게 하기 위해서, PAS-K는 NAT(Network Address Translation) 뿐만 아니라, TCP 일련 번호의 조정 등 다양한 동작을 수행해야 하는데 이러한 일련의 동작을 TCP splicing이라 합니다.

Non-HTTP 트래픽 처리

일반적으로 80번은 HTTP 프로토콜이 사용하는 포트 번호로, 많은 방화벽들은 80번 포트로 수신되는 트래픽을 제외한 모든 트래픽을 차단하는 정책을 가지고 있습니다. 그렇기 때문에 방화벽을 우회하기 위한 수단으로 HTTP 표준을 준수하지 않는 non-HTTP 트래픽이면서 80번 포트를 사용하는 애플리케이션들이 있습니다. 그러나, non-HTTP 트래픽은 80번 포트를 사용한다고 하더라도 주고 받는 데이터가 HTTP 표준을 준수하지 않기 때문에 PAS-K에서 정상적으로 처리할 수 없습니다.

예를 들어, L7 캐시 서버 부하 분산 서비스에서 HTTP 트래픽을 처리하기 위해 다음과 같은 필터가 정의되어 있다고 가정해봅니다.

- 필터의 종류 : include 타입
- 출발지 IP 주소 : 0.0.0.0/0 (any)
- 출발지 포트 번호 : 0 (any)
- 목적지 IP 주소 : 0.0.0.0/0 (any)
- 목적지 포트 번호 : 80

위와 같이 설정되어 있는 경우, PAS-K는 수신된 트래픽이 HTTP 트래픽인지 non-HTTP 트래픽인지 구분하지 않고, 목적지 포트 번호만 확인합니다. 그런 다음 목적지 포트가 80인 패킷에 대하여 L7 캐시 서버 부하 분산 서비스를 수행합니다.

이러한 현상을 해결하기 위해, PAS-K의 L7 캐시 서버 부하 분산 서비스에서는 80번 포트 번호를 사용하면서 HTTP 표준을 준수하지 않는 non-HTTP 트래픽을 정상적으로 처리하도록 하는 non-HTTP 트래픽 처리 기능을 지원합니다. PAS-K는 우선 80포트를 사용하는 트래픽이 수신되면 L7 캐시 서버 부하 분산 서비스에 의해 트래픽을 처리하도록 해보고, TCP 데이터를 분석해 해당 트래픽이 non-HTTP 트래픽으로 판정되면, L7 캐시 서버 부하 분산 서비스는 수행하지 않고 즉시 L4 스위칭처럼 포워딩만 수행합니다.

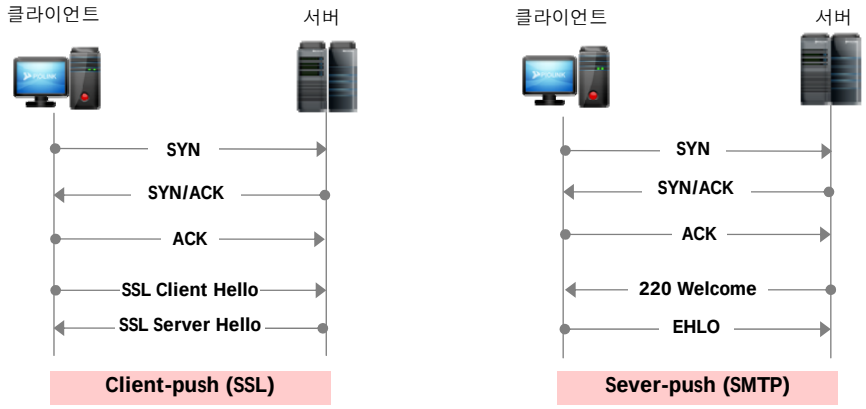
Non-HTTP 트래픽의 처리 방식

이 절에서는 non-HTTP 트래픽의 처리 방식을 이해하기 위해서 먼저, non-HTTP 트래픽의 종류에 대해 살펴본 후, non-HTTP 트래픽 처리 방식에 대해 설명합니다.

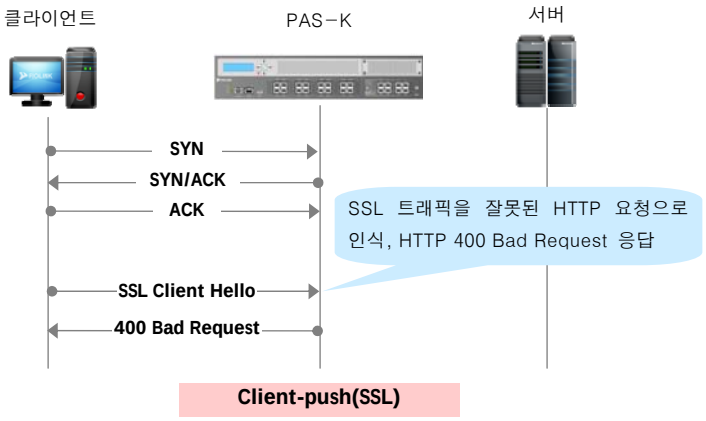
Non-HTTP 트래픽 종류

Non-HTTP 트래픽은 클라이언트와 서버 중 어느 쪽이 데이터를 먼저 전송하는지에 따라 크게 Client-push 프로토콜과 Server-push 프로토콜로 나눌 수 있습니다.

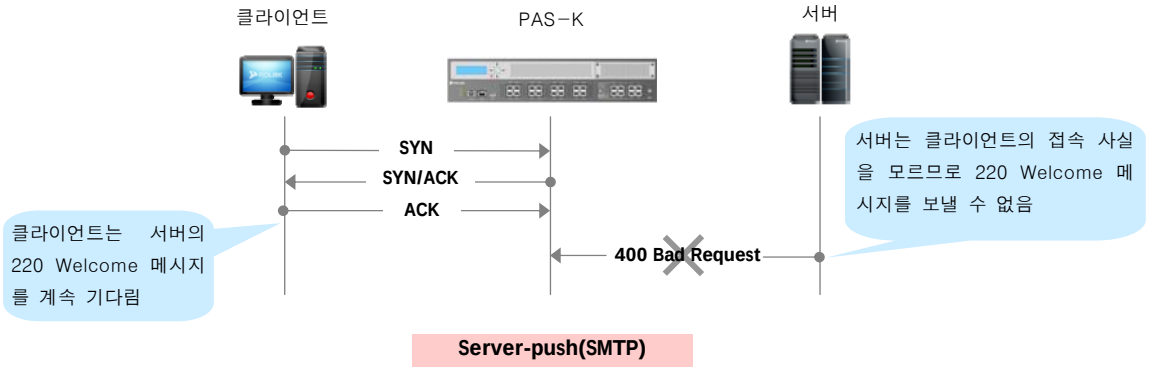
Client-push 프로토콜은 TCP 연결이 수립된 후 클라이언트 쪽에서 데이터를 먼저 전송하는 경우를 말합니다. HTTP도 클라이언트가 먼저 HTTP 요청을 전송하므로 Client-push로 분류할 수 있습니다. Server-push 프로토콜은 클라이언트가 먼저 TCP 연결 요청을 하지만, 일단 3-way handshake 과정이 끝난 후에, 서버가 먼저 데이터를 전송하는 경우를 말합니다. FTP, SMTP, POP3, IMAP 등 대부분의 인터넷 표준 프로토콜들이 이러한 Server-push 형태입니다. 아래의 왼쪽 그림은 클라이언트와 서버 간에 Client-push 프로토콜이 전송되는 과정을 보여주며, 오른쪽 그림은 클라이언트와 서버 간에 Server-push 프로토콜이 전송되는 과정을 보여줍니다.



그러나, Client-push 프로토콜의 경우 다음 그림에서와 같은 이유로 PAS-K가 정상적으로 non-HTTP 트래픽을 처리하지 못합니다.



반면, Server-push 프로토콜의 경우 PAS-K가 중간에 TCP 연결을 가로채는 지연 바인딩(Delayed Binding) 동작을 하게되어 정상적으로 HTTP 트래픽을 처리하지 못합니다.



앞에서 살펴본 것처럼, Client-push 프로토콜과 Server-push 프로토콜의 경우 PAS-K가 정상적으로 non-HTTP 트래픽을 처리하지 못하는 문제가 있습니다. 이러한 문제점을 해결하기 위해 PAS-K는 허용(allow-nonhttp) 옵션을 사용하여 non-HTTP 트래픽을 정상적으로 처리하도록 합니다.

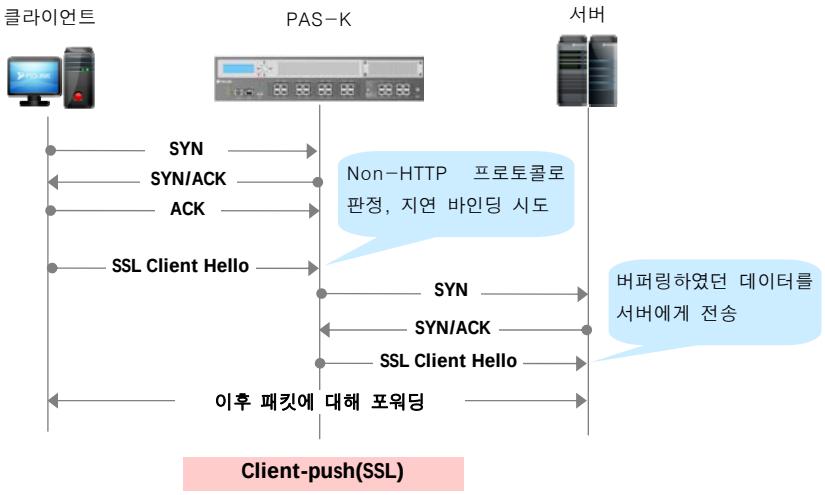
허용(Allow-non http)

PAS-K는 non-HTTP 트래픽을 처리하기 위한 방법으로 허용(Allow-nonhttp) 옵션을 사용할 수 있습니다. 허용(Allow-nonhttp)은 잘못된 HTTP 요청에 대해서는 서버로 바로 포워딩하고, 그 이후에 전송되는 패킷들은 L7 캐시 서버 부하 분산 서비스를 적용하지 않고 단순히 중계하는 방식입니다.

PAS-K는 TCP 연결 수립 후 클라이언트가 전송한 첫 번째 데이터가 잘못된 HTTP 요청으로 판단되면, 이를 non-HTTP 트래픽으로 간주합니다. 그런 다음, 데이터는 일단 임시로 저장을 해두고, 서버로 SYN 패킷을 전송해 서버 쪽 연결을 시도합니다. 서버로부터 SYN/ACK 패킷을 수신하면, 저장해두었던 데이터를 서버로 전송합니다. 이후에는 클라이언트에서 서버로 향하는 패킷이나 서버에서 클라이언트로 향하는 모든 패킷에 대해 TCP 접속이 끝날 때까지 포워딩만을 수행합니다.

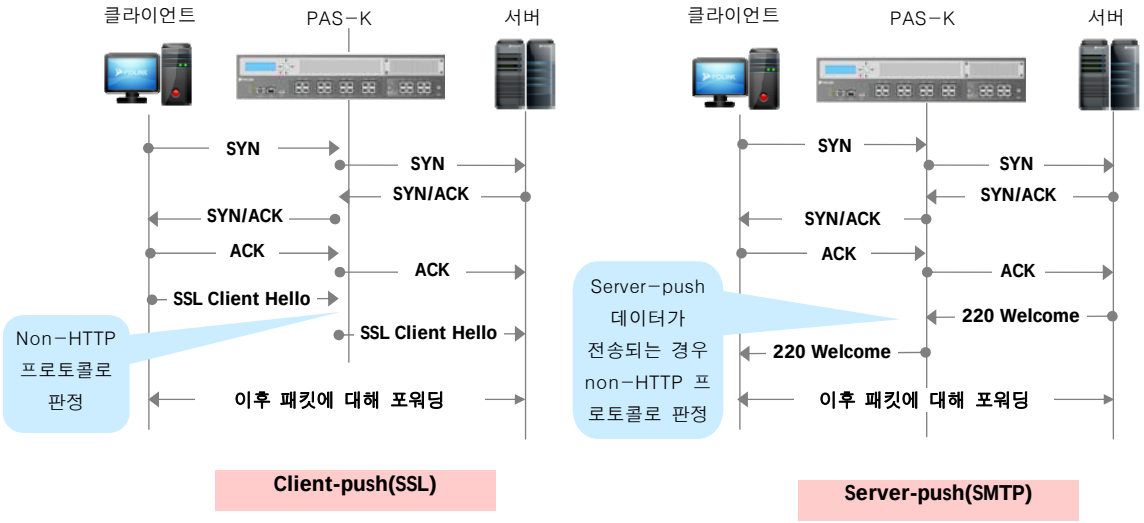
참고: PAS-K는 TCP 연결이 수립된 후 첫 데이터에 대해서만 non-HTTP 트래픽 판정을 합니다. 따라서, 첫 번째 HTTP 요청 및 응답이 정상 처리되는 경우, 두 번째로 클라이언트로부터 전송되는 데이터에 대해서는 non-HTTP 트래픽 판정을 하지 않습니다. 그렇기 때문에, 두번째로 non-HTTP 트래픽이 수신되면 PAS-K는 잘못된 HTTP 요청이라 판단하여 400 Bad Request 응답을 전송합니다.

다음 그림은 Client-push 프로토콜인 SSL에 대해, 허용 옵션이 활성화된 상태에서 PAS-K가 non-HTTP 패킷을 처리하는 과정을 나타낸 그림입니다.



그러나, 허용 옵션만을 사용하는 경우에는 지연 바인딩 동작을 수행하기 때문에 Client-push 프로토콜의 경우만 처리가 가능하고, 서버 쪽에서 먼저 데이터가 전송되는 Server-push 문제에 대해서는 대응이 불가능합니다. 이러한 문제를 해결하기 위해서는 지연바인딩 절에서 설명한 직접 연결(Direct Connect) 옵션을 함께 사용해야 합니다. 허용과 직접 연결의 두가지 옵션을 함께 사용하게되면, PAS-K는 TCP 연결이 수립된 후에 서버 측으로부터 데이터를 먼저 수신할 경우, 이를 non-HTTP 트래픽으로 간주하고 포워딩함으로써, Server-push 프로토콜을 처리합니다.

다음은 직접 연결과 허용의 두가지 옵션을 모두 활성화한 경우에, client-push 와 server-push 프로토콜에 대해 PAS-K가 동작하는 과정을 나타낸 그림입니다.

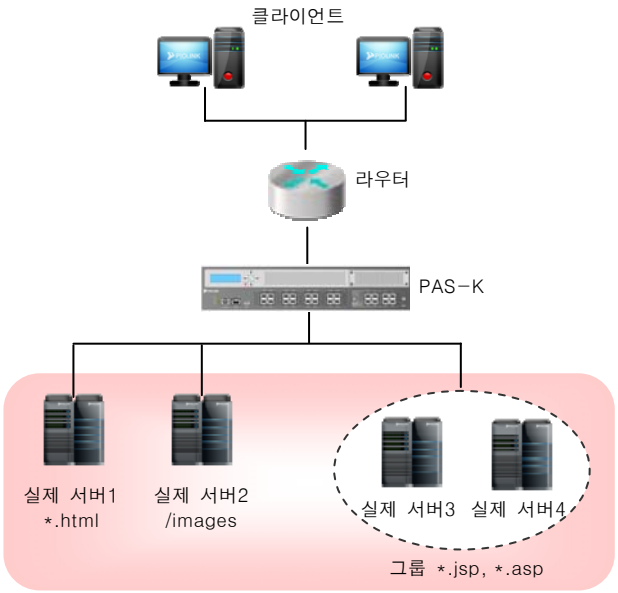


L7 서버 부하 분산

L7 서버 부하 분산 기능은 여러 개의 실제 서버를 묶어서 서버 팜을 구성하고 사용자가 요구하는 컨텐트에 기반하여 실제 서버로 트래픽을 분배하는 서비스입니다. 간단하게는 L4 서버 부하 분산 기능에 컨텐트 개념이 추가된 것으로 생각할 수 있습니다.

각 L7 서버 부하 분산 서비스는 클라이언트에서 사용하는 가상 서버 IP 주소와 포트 번호, 그리고 부하 분산 서비스 간의 우선순위를 나타내는 우선순위 값을 가집니다. 이들 외에 다수의 패턴, 실제 서버, 그룹, 규칙을 유기적으로 사용하여 컨텐트에 기반한 서비스를 설정하게 됩니다.

다음은 사용자가 요구하는 컨텐트의 종류에 따라 실제 서버로 트래픽이 분산될 수 있도록 L7 서버 부하 분산을 적용한 네트워크 구성의 예입니다.



[그림 - L7 부하 분산을 적용한 네트워크 구성도]

고급 L7 서버 부하 분산

고급 L7 서버 부하 분산은 L7 서버 부하 분산 서비스에서 HTTP 압축, 캐싱, SSL 가속과 같은 애플리케이션 가속 기능과 IPv6 환경을 추가적으로 지원하는 서비스입니다. 애플리케이션 가속 기능을 사용하여 실제 서버의 하드웨어 자원 부하를 줄일 수 있고, IPv6 네트워크 환경에서의 L7 서버 부하 분산 서비스를 사용할 수 있습니다.

참고: PAS-K에서 제공하는 애플리케이션 가속은 HTTP 압축, 캐싱, SSL 가속 세가지가 있습니다. 각 애플리케이션 가속 기능에 대한 설명은 이 장의 **애플리케이션 가속(Application Accelerator)**절을 참고하도록 합니다.

RTS(Return To Sender)

RTS는 멀티 네트워크 세그먼트 환경과 같이 여러 라우팅 경로가 존재하는 경우, 응답 패킷에 대해 라우팅을 수행하지 않고, 요청 패킷을 수신한 경로로 응답 패킷을 전송하는 기능입니다. 이 기능은 고급 L7 서버 부하 분산 서비스 설정 시 사용 여부를 지정할 수 있으며, 외부 네트워크로의 상위 경로에 있는 장비(방화벽, 라우터 등)를 RTS 실제 서버로 설정해야 합니다.

L7 캐시 서버 부하 분산

L7 캐시 서버 부하 분산은 L4 캐시 서버 부하 분산 기능과 마찬가지로 사용자가 요구하는 웹 트래픽을 캐시 서버로 리다이렉션하여 네트워크 대역폭을 절약하고 클라이언트의 요청에 대한 응답 시간을 빠르게 해주는 기능입니다.

사용자가 접속하는 웹 사이트에서 제공하는 컨텐트에는 캐싱이 가능한 이미지나 텍스트가 있고, 캐싱이 불가능한 동적 애플리케이션의 산출물 등이 섞여 있습니다. L4 캐시 서버 부하 분산 기능은 사용자가 요구하는 컨텐트의 종류를 구분할 수 없기 때문에 모든 트래픽을 캐시 서버로 리다이렉션합니다. 만약 사용자가 캐싱이 불가능한 컨텐트를 요구한 경우에는 오히려 응답 속도가 지연되어 캐시 서버에 부하를 증가시킬 수 있습니다. 또한, 캐시 서버에 이미 캐싱되어 있는 컨텐트를 요청한 경우에도 사용자의 요청이 해당 캐시 서버로 리다이렉션되지 않고 다른 캐시 서버로 리다이렉션되면 사용자가 요청한 정보를 다시 인터넷을 통해 다운로드해야만 합니다.

L7 캐시 서버 부하 분산은 컨텐트를 구분할 수 있기 때문에 이러한 L4 캐시 서버 부하 분산 기능의 단점을 해결할 수 있습니다. 먼저, 캐싱이 불가능한 컨텐트를 인식하여 사용자가 해당 컨텐트를 요청하는 경우에는 캐시 서버로 리다이렉션하지 않고 바로 서버로 접속하게 하는 바이패스(bypass) 기능을 제공합니다. 그리고, 동일한 컨텐트에 대한 요청은 항상 같은 캐시 서버로 리다이렉션되어 L4 캐시 서버 부하 분산의 두번째 문제점을 해결함과 동시에 캐시의 hit ratio(판별 적중률)를 현저하게 증가시켜줍니다.

각 L7 캐시 서버 부하 분산 서비스는 부하 분산 서비스 간의 우선순위를 나타내는 우선순위 값을 가집니다. L7 캐시 서버 부하 분산 서비스는 패턴을 이용한 규칙, 실제 서버, 그룹, 그리고 캐시 리다이렉션을 적용할 트래픽을 정의하는 필터 등을 유기적으로 사용하여 컨텐트에 기반한 리다이렉션 서비스를 설정합니다. PAS-K에는 L7 캐시 서버 부하 분산 서비스를 포함하여 최대 1024개의 L7 부하 분산 서비스를 정의할 수 있습니다.

필터

PAS-K의 L7 캐시 서버 부하 분산 서비스는 캐시 리다이렉션을 적용할 트래픽을 정의하기 위해 필터를 사용합니다. 필터는 프로토콜과 송수신/목적지 IP 주소, 출발지/목적지 포트 번호 등을 다양하게 조합하여 정의할 수 있습니다. 필터의 종류에는 include 타입과 exclude 타입이 있습니다. Include 타입의 필터에는 캐시 리다이렉션을 적용할 트래픽의 조건이 포함됩니다. 그리고 exclude 타입의 필터는 캐시 리다이렉션을 적용하지 않을 트래픽의 조건으로 구성됩니다.

고급 L7 캐시 서버 부하 분산

고급 L7 캐시 서버 부하 분산은 L7 캐시 서버 부하 분산 서비스에서 HTTP 압축, SSL 가속과 같은 애플리케이션 가속 기능과 IPv6 환경을 추가적으로 지원하는 서비스입니다. 애플리케이션 가속 기능을 사용하여 실제 서버의 하드웨어 자원 부하를 줄일 수 있고, IPv6 네트워크 환경에서의 L7 캐시 서버 부하 분산 서비스를 사용할 수 있습니다.

참고: PAS-K에서 제공하는 애플리케이션 가속은 HTTP 압축, 캐싱, SSL 가속 세가지가 있습니다. 고급 L7 캐시 서버 부하 분산에서는 캐싱을 제외한 HTTP 압축과 SSL 가속 기능을 사용할 수 있습니다. 각 애플리케이션 가속 기능에 대한 설명은 이 장의 **애플리케이션 가속(Application Accelerator)**절을 참고하도록 합니다.

패턴(Pattern)

패턴은 PAS-K가 HTTP 요청을 분류하는 판단 기준입니다. PAS-K는 패턴이 매치되는 결과에 따라 HTTP 요청을 처리하는 방식을 결정하게 됩니다. 패턴은 매치 종류(type)에 따라 동작하는 방식이 다릅니다. HTTP 요청이 수신되면, PAS-K는 HTTP 요청의 헤더에서 패턴에 설정된 매치 종류에 해당되는 항목을 패턴의 문자열과 매치 방법으로 비교합니다. 예를 들어, 매치 종류가 host이고, 문자열이.w3.org, 매치 방법이 suffix인 패턴이 설정되어 있다면, PAS-K는 수신된 HTTP 요청이 *.w3.org의 도메인 이름으로 전송되는 경우 이 패턴이 매치된 것으로 판단합니다. 패턴과 다음 장에서 설명할 규칙을 조합하면 서로 다른 HTTP 트래픽에 대해 L7 부하 분산 서비스의 다양한 정책을 적용할 수 있습니다.

PAS-K에는 최대 512개의 패턴을 설정하고, 적용할 수 있습니다. 패턴은 부하 분산 서비스에 관계없이 하나의 PAS-K 안에서 동일하게 적용됩니다. 패턴을 구성하는 항목들에 대해 상세히 살펴봅니다.

매치 종류

매치 종류는 패턴에서 검사할 HTTP 요청 헤더 또는 IP 헤더의 특정 값 중에서 선택합니다. 매치 종류는 다음 10가지 중에서 선택할 수 있습니다.

- uri HTTP 요청의 URI
- host HTTP 요청의 호스트 필드
- cookie HTTP 요청의 쿠키 필드
- user-agent HTTP 요청의 User-Agent 필드
- accept-language HTTP 요청의 Accept-Language 필드
- user-defined HTTP 요청 헤더 내의 임의의 필드
- HTTP method HTTP 요청의 메소드 (GET, POST 따위)
- HTTP version HTTP 버전 (HTTP/1.0 혹은 HTTP/1.1)
- Client IP network HTTP 요청의 출발지 IP 주소(클라이언트 IP 네트워크 주소)
- Server IP network HTTP 요청의 목적지 IP 주소(서버 IP 네트워크 주소)

참고: 패턴의 매치 기준으로 Client IP network와 Server IP network를 지정한 경우에는 HTTP 트래픽의 출발지/목적지 IP 주소와 넷 마스크 비트 수를 입력합니다. 그리고, HTTP version 항목을 지정한 경우에는 PAS-K가 HTTP/1.0 요청과 HTTP/1.1 요청을 구분하여 처리할 수 있도록 HTTP 버전을 입력해줍니다. 이 세가지를 제외한 나머지 매치 종류들은 HTTP 헤더 내에서의 특정 값들을 검사하도록 하기위해 문자열과 매치 방법을 지정해 주어야 합니다.

문자열

패턴의 문자열은 매치 종류로 지정한 헤더의 특정 값과 비교하는 값입니다. 패턴의 문자열은 128자까지 지정할 수 있고 모든 문자가 포함될 수 있습니다. 패턴의 문자열로 정규식(regular expression)을 사용할 수 있는데, 정규식을 사용하면 첫글자는 알파벳, 두번째 글자는 숫자로된 문자열과 같은 특정한 형태의 문자열을 검사할 수 있습니다.

다음은 정규식에서 사용할 수 있는 특수 문자들입니다.

[표 - 정규식에 사용할 수 있는 특수 문자]

메타 문자	설 명	예
^	라인의 처음이나 문자열의 처음을 표시	^aaa (aaa로 시작하는 문자열)
$	라인의 끝이나 문자열의 끝을 표시	aaa$ (aaa로 끝나는 문자열)
.	임의의 한 문자를 표시	a.c (abc나 aZc와 같이 a와 c 사이에 문자가 포함된 문자열)
[ ]	문자의 집합이나 범위를 표시. 두 문자 사이의 "-"는 범위를 나타냅니다. [] 안에 ^가 있으면 not을 의미합니다	[abc] (a나 b, c) [^a-c] (a와 b, c를 제외한 나머지 문자)

{x}	직전의 선행 문자가 정확히 x번 발생하는 문자열	a{3} (aaa를 포함하는 문자열)
{x,}	직전의 선행 문자가 적어도 x번 발생하는 문자열	a{3,} (aaa나 aaaa 등)
{x,y}	직전의 선행 문자가 적어도 x번 발생하고, y보다 많이 발생하지 않는 문자열	a{2,4} (aa나 aaa, aaaa)
*	직전의 선행 문자가 0번 혹은 여러 번 나타나는 문자열	ab*c (a와 c 사이에 b가 없거나혹은 여러 번 나타나는 문자열: ac, ackkka, abbc, abbbbbc 등)
?	직전의 선행 문자가 0번 혹은 한 번 나타나는 문자열	ab?c (a와 c 사이에 b가 없거나 한번 나타나는 문자열: ac, abc, abcd 등)
+	직전의 선행 문자가 적어도 한 번 이상 나타나는 문자열	ab+c (a와 c 사이에 b가 1번 이상 나타나는 문자열: abc, abbbbc, abbcdef 등)
( )	정규식 내에서 패턴을 그룹으로 묶어 처리할 때 사용	
|	OR 연산자	a|b|c (a나 b, 혹은 c. [abc]나 [a-c]와 동일한 의미)
₩	위의 특수 문자들을 정규식 내에서 일반 문자로 취급하고자 할 때 특수 문자의 앞에 사용하는 문자	file₩.ext (file.ext를 표시)

다음은 일반적으로 사용되는 정규식들입니다.

- ₩.gif$
  gif 로 끝나는 문자열 (a.gif, /images/b.gif 등)
- ^www
  www 로 시작하는 문자열(wwwabc, www.piolink.com 등)
- [A-Za-z0-9]
  모든 알파벳과 숫자
- [^a-z]
  소문자 이외의 문자
- [0-9]{2}
  두자리 숫자
- [A-Za-z]{4}$
  네 개의 알파벳으로 끝나는 문자열
- ([0-9]{1,3}₩.){3}[0-9]{1,3}
  1~3 자리 수의 3 개의 인스턴스를 가지는 IP 주소(192.168.1.10 등)
- [A-Za-z0-9._-]+@[A-Za-z0-9._-]+₩.[A-Za-z0-9._-]{2,4}
  일반 이메일 주소(webmaster@piolink.com 등)

매치 방법

매치 방법은 매치 종류로 선택한 헤더의 특정 값과 패턴의 문자열을 비교하는 방법입니다. 비교 방법에는 다음과 같은 4가지 방법이 있습니다.

- prefix 헤더의 값이 패턴의 문자열로 시작되는지 비교
- suffix 헤더의 값이 패턴의 문자열로 끝나는지 비교
- regex 헤더의 값에 패턴의 정규식이 포함되는지 비교(패턴의 문자열을 정규식으로 지정한 경우)
- any 헤더의 값에 패턴의 문자열이 포함되어 있는지 비교

참고: 매치 방법으로 prefix나 suffix를 사용하면 regex나 any를 선택하는 것보다 PAS-K의 부하를 줄일 수 있습니다.

규칙(Rule)

규칙은 클라이언트가 전송한 HTTP 요청의 종류에 따라 PAS-K가 수행할 동작을 선택하는데 사용됩니다. 규칙은 클라이언트의 HTTP 요청과 비교하는 패턴과 HTTP 요청이 패턴과 일치한 경우에 전송할 서버 그룹, 그리고 규칙에 따라 취할 액션으로 구성됩니다. 규칙을 설정할 때에는, 그룹을 선택하여 해당 그룹 내에서 부하 분산을 수행하게 하거나 규칙에 따라 취할 별도의 액션을 지정할 수 있습니다.

규칙에 패턴을 등록하는 경우에는 'NOT, AND, XOR, OR' 연산자를 사용하여 자유롭게 논리식의 형태로 지정할 수 있고, 논리식의 계산 순서를 명확히 하기 위해서 괄호를 사용할 수도 있습니다. 연산자의 우선순위는 NOT이 제일 높고, AND, XOR, OR 순입니다. 패턴식에는 최대 32개의 패턴을 등록할 수 있습니다. 규칙에 패턴식을 등록하지 않는 경우에는 모든 HTTP 요청이 해당 규칙에 의해 처리됩니다.

하나의 L7 부하 분산 서비스에 여러 개의 규칙이 사용되는 경우에는 규칙의 우선순위에 따라 HTTP 요청에 적용됩니다. 만약 하나의 HTTP 요청이 2개 이상의 규칙에 설정된 패턴식을 만족하는 경우에는 우선순위가 가장 높은 규칙에 의해 처리됩니다.

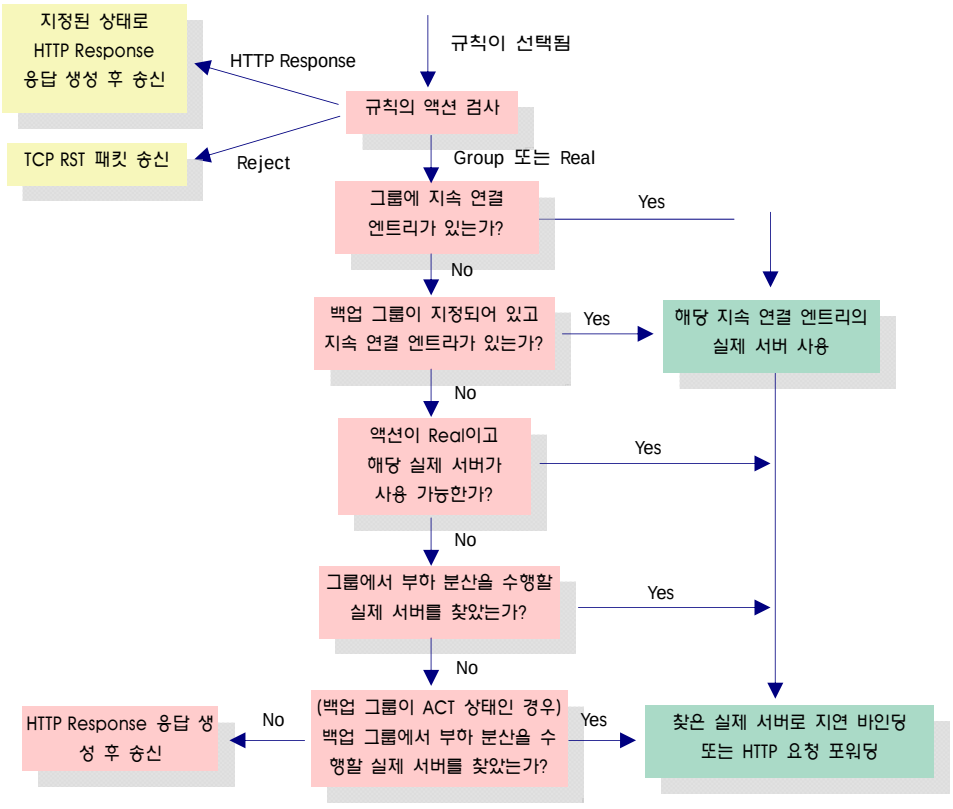
PAS-K에는 L7 부하 분산 서비스 당 최대 256개의 규칙을 설정할 수 있으며, 규칙은 1 ~ 1024 사이의 고유 ID로 구분합니다.

액션(Action)

액션은 규칙을 설정할 때 규칙에 따라 어떻게 동작할 것인지를 설정할 수 있는 기능입니다. 지정할 수 있는 액션의 종류는 다음 4가지 중에서 선택할 수 있습니다.

- Group 해당 그룹 내에서 부하 분산을 수행하도록 지정
- Real 사용자가 해당 그룹 내에서 실제 서버를 직접 선택하도록 지정
- Reject PAS-K 가 TCP RST 패킷을 생성하여 클라이언트에게 전송하도록 지정
- HTTP Response PAS-K 가 직접 HTTP 응답을 생성하여 클라이언트에게 전송하도록 지정

다음은 클라이언트로부터 HTTP 요청을 수신하면 패턴식을 검사하고 우선순위에 따라 규칙을 선택한 다음, 액션을 실행하는 과정을 나타낸 순서도입니다.



Group

선택 가능한 액션 중에서 'Group'을 선택하면 해당 그룹 내에서 부하 분산을 수행하도록 지정할 수 있습니다. 클라이언트의 HTTP 요청이 규칙에 등록된 패턴식에 매치하는 경우, 해당 요청은 그 규칙에 설정된 그룹에서 지정한 부하 분산 방식에 의해 부하 분산하여 실제 서버로 전송됩니다.

Real

선택 가능한 액션 중에서 'Real'을 선택하면 특정 HTTP 요청에 대해 사용자가 직접 클라이언트의 HTTP 요청을 처리할 실제 서버를 지정할 수 있습니다. 실제 서버를 직접 지정하는 경우에는 해당 실제 서버가 여러 그룹에 속해있을 수 있기 때문에 실제 서버가 속한 그룹을 반드시 지정해 주어야 합니다.

또한, 지정한 실제 서버가 사용 불가능한 경우(FULL 또는 INACT 상태인 경우)에도 지정된 그룹 내에서 부하 분산을 수행하여 해당 HTTP 요청을 처리하기 때문에, 해당 실제 서버가 속한 그룹을 지정해야 합니다. 만약, 지정한 그룹에 이미 지속 연결 엔트리가 존재하는 경우에는 지정한 실제 서버를 무시하고 지속 연결 엔트리를 그대로 사용합니다.

Reject

선택 가능한 액션 중에서 'Reject'를 선택하면 클라이언트로부터 HTTP 요청을 받은 경우, PAS-K가 TCP RST 패킷을 생성하여 클라이언트에게 전송하도록 지정할 수 있습니다. TCP RST 패킷을 클라이언트에게 전송하면 클라이언트와 PAS-K 사이의 TCP 접속이 완전히 끊어지기 때문에, 보안 상 위험한 요청들을 완전히 차단할 수 있습니다.

HTTP Response

선택 가능한 액션 중에서 'HTTP Response'를 선택하면 PAS-K가 직접 HTTP 응답을 생성하여 클라이언트에게 전송하도록 지정할 수 있습니다. PAS-K는 L7 부하 분산의 애플리케이션이 HTTP로 지정되어 있는 경우에 클라이언트로부터 HTTP 요청을 받으면, 임의의 상태 코드를 갖는 HTTP 응답을 생성하여 클라이언트에게 전송합니다. HTTP 응답 패킷에는 TCP FIN 플래그가 포함되어 있어 클라이언트와의 TCP 접속을 끊게 됩니다. 상태코드는 서버가 HTTP 요청 메시지를 수신하여 처리한 결과를 알려주는 세 자리의 정수로 된 처리 결과 번호입니다. PAS-K에서 사용할 수 있는 HTTP 상태 코드의 종류와 각각의 코드가 나타내는 의미는 다음과 같습니다.

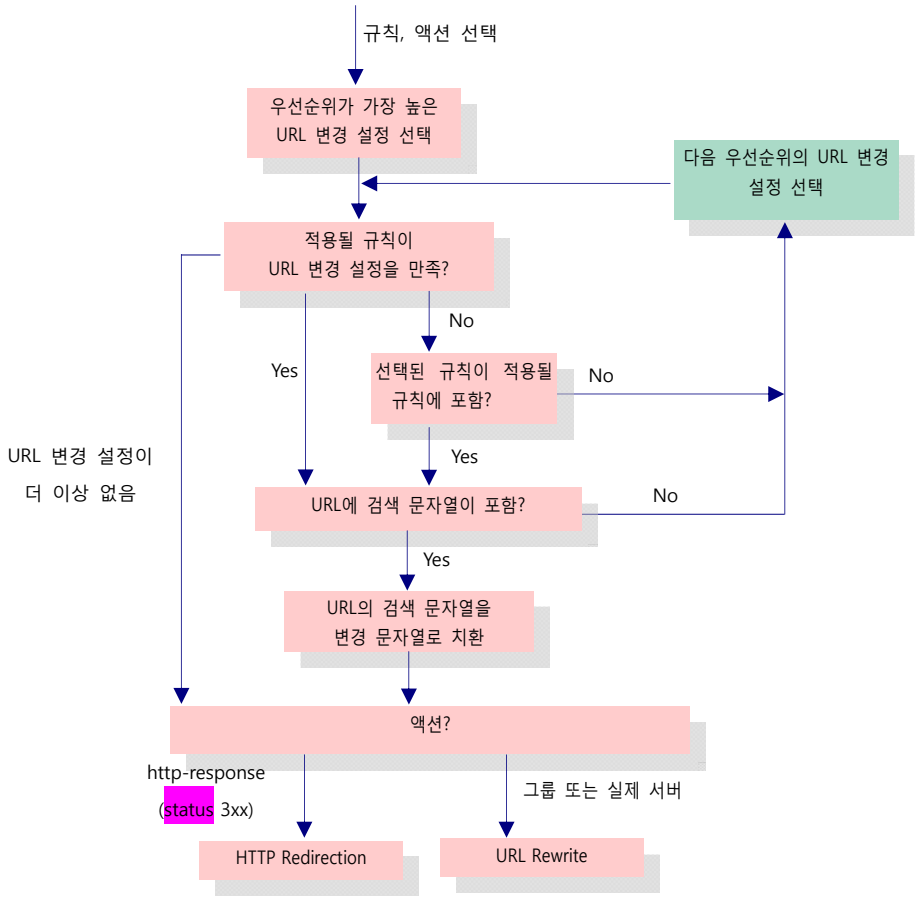
- 3xx Redirection 파일이 이동되었을 때 사용
  - 301 Moved Permanently : 요청된 문서의 위치가 영구적으로 변함
  - 302 Found : 요청된 URI는 변경된 URI에 있음
  - 307 Temporary Redirect : 요청된 URI가 일시적으로 옮겨짐
- 4xx Client Error 클라이언트가 에러를 발생한 것처럼 판단될 경우에 사용
  - 400 Bad Request : 클라이언트의 요청에 문법적인 오류가 있다는 것을 서버가 알아냈다는 것을 의미
  - 403 Forbidden : 클라이언트의 인증정보에 상관없이 페이지에 대한 접근을 거부한다는 것을 의미
  - 404 Not Found : 클라이언트가 요청한 자원이 서버에 없다는 것을 의미
- 5xx Server Error 서버가 에러를 발생시켰으며 요구를 처리할 능력이 없음을 인지한 경우에 사용
  - 503 Service Unavailable : 서비스를 일시적으로 제공할 수 없으나, 앞으로 복구된다는 의미

URL 변경(URL Manipulation)

URL 변경은 클라이언트가 요청한 URL을 PAS-K가 변경하여 실제 서버로 전달해주는 기능입니다. 예를 들어 웹 사이트의 URL 체계가 변경된 경우 클라이언트가 변경 전의 URL로 접속하게 되면 서비스를 이용할 수 없게 됩니다. 이 때, URL 변경 기능을 사용하면 PAS-K가 자동으로 클라이언트와 서버의 사이에서 URL을 변경해주기 때문에, 변경전의 URL로 오는 클라이언트의 HTTP 요청들은 새롭게 바뀐 URL로 접속할 수 있습니다. 따라서, 서비스의 가용성이 향상됩니다.

이러한 설정은 웹 서버에 직접 적용할 수도 있지만, PAS-K의 URL 변경 기능을 사용하면 다수의 웹 서버를 운용하는 경우에도 PAS-K에 한번만 적용할 설정을 입력하면 되므로 관리의 번거로움을 최소화 할 수 있습니다. URL 변경 기능은 사이트 정기 점검이나 장애 복구 등의 페이지로 사용자를 안내하는 용도로도 유용하게 사용할 수 있습니다.

다음은 L7 부하 분산 서비스에서 URL 변경 설정을 적용하는 과정을 나나낸 순서도 입니다.



[그림 - L7 부하 분산 서비스의 URL 변경 설정 적용 과정]

위의 그림에서와 같이 클라이언트로부터 HTTP 요청이 들어오면 PAS-K는 가장 먼저, 선택된 규칙이 URL 변경 설정과 일치하는지 확인합니다. 여러 개의 URL 변경 설정이 정의되어 있는 경우에는 우선순위가 가장 높은 URL 변경 설정부터 비교하고, 규칙이 우선순위가 가장 높은 URL 변경 설정과 일치하지 않으면 다음 우선순위를 가진 URL 변경 설정과 비교합니다. 선택된 규칙이 URL 변경 설정과 일치하면 URL 안에서 검색할 문자열인 '매칭 URL(match)'의 존재 여부를 확인합니다. 만약 매칭 URL이 있는 경우에는 매칭 URL을 변경할 문자열인 '대체 URL(replacement)'로 치환합니다. URL 변경 기능은 매칭 URL이 URL 내에서 여러 번 나오더라도 그 중 맨 처음에 등장하는 매칭 URL만 대체 URL로 치환합니다. 매칭 URL을 대체 URL로 치환하고 나면, 적용되는 규칙의 액션에 따라 URL 변경 기능의 동작 방식을 결정합니다.

URL 변경 기능은 HTTP Redirection과 URL rewrite 의 두가지 방식으로 동작합니다. 규칙의 액션이 HTTP response 3xx인 경우에는 HTTP redirection 기능을 사용해 URL을 변경하고, 액션이 그룹이나 실제 서버인 경우에는 URL rewrite 기능을 사용하여 실제 서버에 HTTP 요청을 포워딩하기 전에 URL을 변경합니다.

매칭 URL의 문자열로는 정규식(regular expression)을 사용하고, 정규식에는 괄호를 사용하여 부분 문자열을 사용할 수도 있습니다. 괄호는 각 부분 문자열에 대응되며 정규식 내에는 최대 9개의 괄호를 사용하여 9개까지의 부분 문자열을 사용할 수 있습니다. 이렇게 대응된 부분 문자열은 대체 URL에서 각각 $0~$9의 형태로 삽입할 수 있습니다.

참고: 매칭 URL의 정규식은 괄호를 사용할 수 있는 것 이외에는 패턴에서 사용되는 정규식과 동일하므로 사용 가능한 특수 문자에 대한 상세한 설명은 이전 절인 [패턴-문자열]을 참고하도록 합니다.

PAS-K에는 L7 부하 분산 서비스 당 최대 256개의 URL 변경 설정을 등록할 수 있습니다.

참고: 적용 가능한 URL 변경 설정이 여러 개인 경우라도 우선순위가 가장 높은 하나의 설정만 처리됩니다. 즉, URL 변경은 하나의 HTTP 요청에 대해 두 번 이상 수행되지 않습니다

참고: URL 변경 기능은 L7 부하 분산의 가장 마지막 단계에서 수행됩니다. 따라서 URL이 변경되더라도 패턴의 매치 등에는 영향을 미치지 않습니다.

HTTP Redirection

HTTP Redirect 기능은 웹 서버의 URL이 변경된 경우, PAS-K가 자동으로 클라이언트가 요청한 URL을 변경된 새로운 URL로 알려주는 기능입니다. 예를 들어, 웹 서버의 컨텐트 위치가 이동한 경우에는, 예전 URL로 접속한 사용자에게 컨텐트가 이동한 새로운 URL을 알려줄 필요가 있습니다. 이 때, HTTP Redirect 기능을 사용하면 자동으로 새로운 URL을 클라이언트에게 알려주며, 클라이언트는 이 새로운 주소로 재 접속됩니다.

URL Rewrite

PAS-K에서 지원하는 URL 변경의 또 다른 방식인 URL rewrite 기능은, 변경된 URL을 클라이언트에게 알리지 않고, 실제 서버에게 전달하는 URL을 PAS-K가 직접 변경하여 클라이언트에게 전송하는 방식입니다. 따라서, HTTP redirection을 사용한 경우처럼 변경된 URL이 웹 브라우저의 주소 표시줄에 보이는 것이 아니고, URL 변경 과정이 PAS-K와 웹 서버 사이에서만 일어나므로 클라이언트는 URL이 변경되었는지의 여부를 알 수 없습니다.

그룹(Group)

실제 서버는 부하 분산된 세션을 실제로 서비스하는 서버를 나타내는 것으로, 그 속성에는 IP 주소, TCP 포트 번호와 가중치가 있습니다. PAS-K는 서비스 당 최대 1024개의 실제 서버를 설정할 수 있으며 이들 서버는 1 ~ 1024 사이의 고유한 ID로 구분됩니다.

그룹은 컨텐트 관점에서 동일한 실제 서버들의 집합으로, 지속 연결 및 부하 분산 방식을 지정하는 단위입니다. 특정 컨텐트에 대한 클라이언트의 요청이 들어오면 먼저 해당 컨텐트를 가진 그룹이 선택됩니다. 선택된 그룹의 지속 연결 설정에 따라 이전에 접속된 실제 서버 정보가 있을 경우는 해당 실제 서버, 그렇지 않은 경우는 부하 분산 방식을 통해서 결정된 실제 서버로 클라이언트의 요청이 전달됩니다.

L7 부하 분산에서는 L4 부하 분산에서 제공하는 rr, wrr, lc, wlc, hash의 다섯 가지 방식 외에 urlhash 부하 분산 방식을 추가로 제공합니다. 이는 나머지 다섯 가지와는 다르게, HTTP 요청의 URI 경로나 특정 부분 문자열을 해싱하여 실제 서버를 선택합니다. 따라서, 동일한 파일에 대한 HTTP 요청이 항상 같은 실제 서버로 전달되는 것을 보장할 수 있고, 이는 L7 캐시 서버 부하 분산에서 cache hit ratio를 증가시키는 데에 유용하게 사용됩니다. 또한, 특정 부분 문자열을 기준으로 해싱을 수행하여 HTTP 요청 내에 접속 유지에 관련된 정보가 포함되어 있는 경우 유용하게 사용할 수 있습니다.

사용자는 PAS-K에 서비스 당 최대 256개의 그룹을 설정할 수 있습니다. 그룹 이름으로는 최대 32문자까지 줄 수 있으며, 이 그룹 이름은 cookie-based persistence의 passive / rewrite / insert 모드에서도 식별을 위해 사용됩니다.

실제 서버(Real Server)

실제 서버는 PAS-K의 부하 분산 서비스의 대상이 되는 장비를 의미합니다. 실제 서버는 웹 서버와 같은 일반적인 서버나 캐시 서버, 방화벽, VPN 장비, 게이트웨이가 될 수 있습니다. 각 부하 분산 서비스마다 서비스의 대상이 되는 실제 서버가 존재하고, PAS-K로 패킷이 수신되면 부하 분산 서비스는 설정된 규칙이나 부하 분산 방식에 따라 패킷을 처리할 실제 서버를 선택합니다. L7 부하 분산 서비스의 경우에는 실제 서버를 그룹으로 묶어서 그룹 별로 규칙이나 부하 분산 방식을 적용합니다.

앞에서 살펴본 각 부하 분산 서비스에서 실제 서버와 관련된 사항들이 설명되어 있습니다. 이 절에서는 앞에서 설명되지 않은 실제 서버와 관련된 다음 기능들에 대해서 알아보도록 합니다.

- 최대 연결 세션 기능(Max Connection)
- 백업 실제 서버 기능(Backup Real Server)
- Graceful Shutdown 기능
- 최소 MTU 설정 기능

최대 연결 세션 기능(Max Connection)

실제 서버에 최대 연결 세션 개수를 설정하면, 실제 서버의 현재 세션 수가 최대 연결 개수에 도달한 경우(FULL 상태) 더 이상의 세션을 실제 서버로 부하 분산하지 않습니다. 만약, 백업 실제 서버가 설정되어 있으면 FULL 상태가 되었을 때 세션이 백업 서버로 부하 분산됩니다. 실제 서버에 지속 연결 세션 엔트리가 존재하는 경우, 실제 서버가 FULL 상태가 되었을 때에는 다음과 같은 2가지 방식으로 동작할 수 있습니다.

- 지속 연결 세션 엔트리와 관련된 세션은 최대 연결 개수의 제한을 받지 않습니다. 즉, 실제 서버가 FULL 상태이더라도 지속 연결 세션 엔트리와 관련된 세션은 실제 서버에서 계속 처리합니다.
- 실제 서버의 지속 연결 세션 엔트리를 삭제하고 지속 연결 기능을 더 이상 지원하지 않습니다.

L4 부하 분산 서비스는 첫번째 방법으로만 동작하고, L7 부하 분산 서비스는 기본적으로 첫번째 방법이 사용되는데 **`persist overmax disable`** 명령을 사용하여 두번째 방법이 사용되도록 할 수 있습니다.

백업 실제 서버(Backup Real Server)

백업 실제 서버는 실제 서버(마스터)가 더 이상 세션을 처리할 수 없는 상태가 되었을 때, 실제 서버의 역할을 대신 수행할 실제 서버(백업) 입니다. 다음과 같은 상황이 되면 PAS-K는 마스터 실제 서버가 세션을 처리할 수 없다고 판단하고 백업 서버를 통해 세션을 처리합니다.

- 장애 감시 결과 마스터 실제 서버가 동작하지 않는 것으로 판단되는 경우
  이 경우에는 마스터 실제 서버에서 처리되던 기존 세션은 모두 해제되고, 이 후에 수신되는 새로운 세션은 백업 서버로 전송됩니다.

- 마스터 실제 서버가 처리 중인 세션의 수가 최대 세션 개수(Max Connection)에 도달한 경우
  이 경우에는 마스터 실제 서버는 현재 세션만 처리하게 되고, 이 후에 수신되는 새로운 세션은 백업 서버로 전송됩니다.

마스터 실제 서버가 다시 동작 가능한 상태가 되면(장애 감시 결과 마스터 실제 서버가 다시 동작하는 것으로 판단되거나 마스터 실제 서버가 처리하는 세션 수가 최대 세션 개수보다 적어진 경우), 백업 실제 서버 대신 마스터 실제 서버로 세션이 부하 분산됩니다. 백업 실제 서버는 L4 부하 분산 서비스에만 설정할 수 있으며 마스터 실제 서버가 다시 동작하면 그동안 백업 실제 서버가 처리하던 세션들을 모두 삭제합니다.

백업 서버를 지정하기 위한 조건은 다음과 같습니다.

- 각 실제 서버마다 하나의 백업 서버를 지정할 수 있습니다.
- 다른 실제 서버에 지정된 백업 서버는 지정할 수 없습니다.
- 백업 서버로 지정된 실제 서버는 부하 분산 서비스에 설정할 수 없습니다.
- 부하 분산 서비스에 설정된 실제 서버는 백업 서버로 지정할 수 없습니다.

Graceful Shutdown 기능

실제 서버에 graceful shutdown 기능을 활성화하면 해당 실제 서버로 새로운 세션 요청이 할당되지 않습니다. 시간이 경과하여 기존의 세션이 모두 종료되면 실제 서버는 부하 분산 서비스에서 제외됩니다. 실제 서버를 부하 분산 서비스에서 제외시킬 수 있는 다른 방법으로 실제 서버를 비활성화하는 방법이 있습니다. Graceful shutdown은 기존의 서비스에 영향을 주지 않으면서 실제 서버를 제거할 수 있는 반면, 실제 서버를 비활성화하면 실제 서버에 연결된 세션이 모두 종료됩니다. Graceful shutdown 기능은 L4와 L7 부하 분산 서비스의 실제 서버에 모두 사용할 수 있고, 기능의 사용 여부는 각 실제 서버마다 설정할 수 있습니다.

서버의 MTU

PAS-K와 클라이언트가 TCP 세션을 연결할 때 전송하는 정보 중에는 MTU(Maximum Transmission Unit)가 있습니다. PAS-K와 클라이언트는 상대방으로부터 수신한 MTU 값을 자신의 MTU와 비교한 후 작은 값에 맞게 패킷을 나누어서 연결된 TCP 세션으로 전송하게 됩니다. L7 부하 분산 서비스는 서버와 통신하기 전에 먼저 PAS-K와 클라이언트 간에 TCP 세션을 연결합니다(지연 바인딩). 따라서, 서버의 MTU 값을 PAS-K가 미리 알고 있어야 클라이언트와 정상적으로 TCP 세션을 연결할 수 있습니다. 기본적으로 PAS-K는 서버의 MTU 값으로 1500을 사용합니다. 이 값은 사용자가 변경 가능 하며, 부하 분산 서비스마다 설정할 수 있으므로 부하 분산 서비스를 적용하는 그룹에 속한 (실제) 서버의 MTU 중에 가장 작은 값을 지정하면 됩니다. L4 부하 분산 서비스는 서버 MTU를 설정할 수 없습니다.

부하 분산 방식

PAS-K의 부하 분산 기능은 부하 분산 방식을 사용하여 트래픽을 분배할 서버나 방화벽, VPN 장비, 캐시 서버 등을 선택합니다. 다음은 PAS-K에서 지원하는 부하 분산 방식입니다.

- 해싱(Hashing)
- 라운드 로빈(Round Robin)
- 가중치 라운드 로빈(Weighted Round Robin)
- 최소 연결(Least Connection)
- 가중치 최소 연결(Weighted Least Connection)
- Slow-Start 최소 연결(Least Connection-Slos-Start)
- Slow-Start 가중치 최소 연결(Weighted Least Connection-Slos-Start)
- Total 최소 연결(Total Least Connection)
- Total 가중치 최소 연결(Weighted Total Least Connection)
- URL 해싱(URL Hashing)
- 최대 가중치(Maximum Weight)
- 정적 근접(Static Proximity)
- 액티브-백업(Active-Backup)
- First 방식(First)

PAS-K는 동적이며 랜덤한 특성을 갖는 해싱 방식과 라운드 로빈, 최소 연결, 가중치 라운드 로빈, 가중치 최소 연결, 최대 가중치 방식 등의 동적 부하 분산 방식을 제공합니다. 동적 방식은 다양한 트래픽 환경에서도 안정적인 서비스 및 속도 향상을 가능하게 해줍니다. 각 방식의 동작 방법에 대해 좀 더 상세히 알아봅니다.

해싱 방식

해싱은 클라이언트의 IP 정보를 사용하여 새로운 연결에 대한 해시 키(hash key)를 계산하고 이 해시 키를 기준으로 실제 서버를 선택하는 방식입니다. 이 방식은 해시 키를 계산할 때 사용하는 클라이언트의 IP 정보에 따라 세가지로 구분되며, 부하 분산의 종류에 따라 설정할 수 있는 방식이 다릅니다.

- **출발지 해싱 방식(Source Hashing)**
  클라이언트의 출발지 IP 주소를 사용하여 해시 키를 계산합니다. 그러므로, 특정 클라이언트에서 요청한 연결은 모두 같은 실제 서버가 선택됩니다. 이 방식은 클라이언트의 정보를 세션 간에 유지해야 하는 애플리케이션에 유용합니다.
  출발지 해싱 방식은 L4 서버 부하 분산, 방화벽/VPN 부하 분산, 게이트웨이 부하 분산, L7 서버 부하 분산, 고급 L7 서버 부하 분산, 고급 L7 캐시 서버 부하 분산에서 사용할 수 있습니다.
- **가중치 출발지 해싱 방식(Weighted Source Hashing)**
  출발지 해싱 방식과 같이 클라이언트의 출발지 IP 주소를 사용하여 해시 키를 계산하며, 실제 서버의 가중치를 반영하여 가중치가 높은 실제 서버가 더 많이 선택되도록하는 방식입니다. 이 부하 분산 방식은 고급 L4 서버 부하 분산 서비스에서만 사용할 수 있습니다.
- **Consistency 출발지 해싱(Source Hashing with Consistency), Consistency 가중치 출발지 해싱(Weighted Source Hashing with Consistency)**
  출발지 해싱 방식과 가중치 출발지 해싱 방식은 실제 서버의 상태가 변경되는 경우, 해시 테이블을 새로 생성하기 때문에 선택되는 실제 서버가 달라질 수 있습니다. Consistency 출발지 해싱과 Consistency 가중치 출발지 해싱 방식은 이러한 상황을 최소화한 방식으로 클라이언트가 처음으로 연결된 실제 서버와 다시 연결될 수 있도록 합니다. 이 부하 분산 방식은 고급 L4 서버 부하 분산 서비스에서만 사용할 수 있습니다.

- **목적지 해싱(Destination Hashing)**
  클라이언트의 목적지 IP 주소를 사용하여 해시 키를 계산합니다. 목적지 해싱 방식은 방화벽/VPN 부하 분산, 게이트웨이 부하 분산에서 사용할 수 있습니다.
- **출발지/목적지 해싱(Both Hashing)**
  클라이언트의 출발지와 목적지 IP 주소를 동시에 사용하여 해시 키를 계산합니다. 출발지/목적지 해싱 방식은 방화벽/VPN 부하 분산, 고급 방화벽/VPN 부하 분산, 게이트웨이 부하 분산, L4 캐시 서버 부하 분산, L7 캐시 서버 부하 분산에서 사용할 수 있습니다.

라운드 로빈 방식

라운드 로빈은 실제 서버를 순차적으로 선택하는 방식입니다. 라운드 로빈 방식에서는 실제 서버의 처리 능력과 무관하게 모든 실제 서버를 동일하게 취급하여 이번에 서버 그룹의 첫번째 실제 서버를 선택하였으면 다음에는 두번째 실제 서버, 그 다음에는 세번째 실제 서버를 선택하는 식입니다. 이 방식은 실제 서버의 처리 능력이 모두 같은 경우에는 효율적일 수 있지만, 그렇지 않은 경우에는 실제 서버마다 다른 가중치를 할당하는 가중치 라운드 로빈 방식이 더 효율적입니다.

가중치 라운드 로빈 방식

가중치 라운드 로빈은 실제 서버 선택 시 실제 서버의 처리 능력을 고려하여 부하 분산을 수행할 수 있게 해주는 방식입니다. 따라서, 각 실제 서버는 처리 능력에 따라 가중치를 할당 받으며, 실제 서버에 할당된 가중치의 비율에 따라 실제 서버를 선택하게 됩니다. 예를 들어, 실제 서버 A, B, C가 4, 3, 2 의 가중치를 할당 받게 되면 가중치 라운드 로빈 방식은 한 주기 동안 ABCABCABA 순으로 실제 서버를 선택합니다. 실제 서버에 기본으로 할당되는 가중치는 1입니다.

최소 연결 방식

최소 연결은 현재 연결된 세션 수가 가장 적은 서버에 새로운 연결을 분배하는 방식입니다. 이 방식은 각 실제 서버의 현재 상태를 실시간으로 확인하여 부하 분산에 반영하기 때문에 다른 방식에 비해 효율적으로 실제 서버의 부하를 분산시킬 수 있습니다.

가중치 최소 연결 방식

가중치 최소 연결은 각 실제 서버에 성능 가중치를 할당한 후 최소 연결 방식을 적용하는 방식입니다. 이 방식은 각 실제 서버에 현재 활성화된 연결 수에 가중치를 나누어 가장 최소의 값을 가지는 실제 서버를 선택합니다. 이 방식을 사용하면 높은 가중치 값을 가진 서버는 낮은 가중치 값을 가지는 서버에 비하여 더 많은 연결을 처리하게 됩니다. 실제 서버에 기본으로 할당되는 가중치는 1입니다.

Slow-Start 최소 연결 방식, Slow-Start 가중치 최소 연결 방식

Slow-Start 최소 연결과 Slow-Start 가중치 최소 연결은 기존의 최소 연결 방식과 가중치 최소 연결 방식에 Slow-Start 옵션을 추가한 방식입니다. 실제 서버를 등록하면 새로운 세션을 연결하기 위해, 추가된 실제 서버로 한꺼번에 트래픽이 전송되는 현상이 발생할 가능성이 있습니다. Slow-Start는 이러한 문제를 방지하기 위한 옵션으로, 추가된 실제 서버로 부하 분산 시킬 세션의 비율(Rate)과 부하 분산할 시간(Timer)을 설정할 수 있습니다. 이 방식을 사용하면, 새로 추가된 실제 서버로 세션이 집중되는 것을 방지하여 실제 서버의 부하를 효율적으로 분산 시킬 수 있습니다.

Total 최소 연결 방식, Total 가중치 최소 연결 방식

Total 최소 연결과 Total 가중치 최소 연결은 최소 연결 방식과 가중치 최소 연결 방식이 해당 부하 분산 서비스를 통해 연결된 세션 수만 확인하는 것과 달리 실제 서버가 등록된 모든 부하 분산 서비스 통해 연결된 세션 수가 가장 적은 서버에 새로운 연결을 분배하는 방식입니다. 하나의 실제 서버를 여러 개의 부하 분산 서비스에 등록한 경우에는 이 방식을 사용하여 효율적으로 실제 서버의 부하를 분산 시킬 수 있습니다.

최대 가중치 방식

최대 가중치는 가중치가 가장 높은 실제 서버에게만 부하를 분산하다가 이 실제 서버에 장애가 발생한 경우 나머지 실제 서버 중에서 가장 높은 가중치의 실제 서버에게 부하를 분산하는 방식입니다. 동일한 가중치를 가진 실제 서버가 여러 개 있는 경우에는 가장 먼저 등록된 실제 서버에게 부하를 분산합니다.

URL 해싱 방식

URL 해싱은 클라이언트의 출발지, 목적지 IP 주소를 사용하는 기존의 해싱 방식과 달리 클라이언트가 요청한 URL을 사용하여 해시 키를 생성합니다. 이러한 URL 해싱 방식을 사용하면 동일한 URL 요청은 같은 실제 서버나 캐시 서버로 연결될 수 있습니다.

정적 근접 방식

정적 근접은 출발지의 IP 주소와 출발지 포트에 따라 실제 서버를 선택하는 방식입니다. 정적 근접 방식은 필터를 사용하여 출발지 IP 주소와 포트 별로 어떤 실제 서버를 할당할지를 지정합니다. 이 방식은 클라이언트에게 가장 적절한 ISP 망의 게이트웨이 라인을 지정해주고자 할 때 사용합니다. 이 부하 분산 방식은 게이트웨이 부하 분산 서비스와 글로벌 서버 부하 분산 서비스에서 사용할 수 있습니다.

액티브-백업 방식

액티브-백업은 'Active' 상태인 실제 서버 하나 만을 선택하는 방식입니다. 'Active' 또는 'Backup' 상태는 실제 서버들의 우선순위에 의해 결정됩니다. 실제 서버들 중 가장 높은 우선순위를 갖는 실제 서버가 'Active' 상태가 되며, 우선순위가 낮은 그 외의 서버들이 'Backup' 상태가 됩니다. 그러나, 'Active' 상태인 실제 서버의 장애 감시가 실패하거나 max-connection이 'FULL'이 되면 'Backup' 상태가 됩니다. 그러면, 그 다음으로 높은 우선순위를 갖는 실제 서버가 'Active' 상태가 됩니다. 액티브-백업 방식은 네트워크 구성 시 하나의 게이트웨이 라인만을 사용하고, 다수의 백업 게이트웨이 라인이 존재할 경우에 사용합니다.

First 방식

First는 ID가 가장 작은 실제 서버로만 부하 분산을 수행하는 방식입니다. 부하 분산 중인 실제 서버에 장애가 발생한 경우에는 다음으로 ID가 작은 실제 서버를 선택하여 부하 분산을 수행합니다. 이 부하 분산 방식은 고급 L4 서버 부하 분산 서비스에서만 사용할 수 있습니다.

장애 감시(Health Check)

개요

장애 감시는 부하 분산 서비스가 적용되고 있는 서버나 방화벽, VPN 장비, 물리적인 라인과 같은 자원의 상태를 주기적으로 검사하여 그 결과를 부하 분산 서비스에 반영하는 기능입니다.

부하 분산 서비스에서 장애 감시는 필수 설정 항목으로, PAS-K는 각 부하 분산 서비스를 시작할 때 실제 서버의 장애 감시를 시작합니다. 감시 결과 실제 서버에 장애가 발생했다고 판단되면, PAS-K는 부하 분산 서비스에서 해당 실제 서버를 선택하지 못하도록 제외시킵니다. 장애가 발생한 실제 서버로 배분했던 클라이언트 요청들은 정상적으로 동작하는 나머지 실제 서버에 의해 처리되도록 조치하여 클라이언트에 대한 서비스가 중단되지 않도록 해줍니다. 장애가 발생했던 실제 서버가 다시 정상화되면, PAS-K는 장애 감시 기능을 통해 실제 서버의 정상 동작을 감지하고 다시 부하 분산의 대상으로 추가하여 클라이언트의 요청을 처리할 수 있게 합니다. 이러한 장애 감시 기능은 특정 자원의 문제로 인해 서비스가 중단되는 상황을 막고 자원을 효율적으로 활용하여 전체적인 성능을 향상시켜줍니다.

PAS-K는 부하 분산 서비스가 시작된 이 후에도 주기적으로 실제 서버의 장애 감시를 수행합니다. 장애 감시는 대부분 특정 패킷을 실제 서버로 전송하고 실제 서버가 그에 대한 응답을 정상적으로 보내는지 여부에 따라 실제 서버의 상태를 판단합니다. 장애 감시를 위해 패킷을 전송하는 주기와 실제 서버의 응답을 기다리는 시간, 응답이 수신되지 않았을 때 다시 패킷을 보내주는 횟수 등을 사용자가 직접 설정할 수 있습니다. PAS-K는 이전에 장애가 발생했던 실제 서버에게도 계속 장애 감시를 위한 패킷을 전송합니다. 장애가 발생했던 실제 서버로부터 응답이 수신되면 실제 서버를 다시 그룹에 추가하게 됩니다. 만약 응답이 한번 수신되는 것으로는 실제 서버가 정상적으로 동작한다고 판단하기 어려운 경우에는 몇 번의 장애 감시를 더 수행하여 응답을 수신한 이후에 실제 서버를 정상으로 판단할 것인지를 설정할 수 있습니다.

PAS-K는 장애 감시의 주기와 응답 대기 시간, 재전송 횟수, 복구 여부를 판단하기 위한 횟수를 기본적으로 다음과 같은 값으로 설정합니다.

[표 - 장애 감시에 사용되는 항목과 기본값]

항 목	기본값	설 명
전송 주기	5(초)	설정된 시간마다 장애 감시를 수행합니다.
응답 대기 시간	3(초)	설정된 시간이 경과되면 실제 서버로부터 응답을 받지 못한 것으로 판단합니다.
재전송 횟수	3(회)	실제 서버로부터 응답을 받지 못한 경우에는 실제 서버가 장애 상태인지를 보다 확실하게 판단하기 위해 설정한 횟수만큼 장애 감시를 추가로 시도합니다.
복구 횟수	0(회)	장애가 발생했던 실제 서버로부터 응답을 수신했을 때 실제 서버의 복구 여부를 보다 확실하게 판단하기 위해 설정한 횟수만큼 추가로 장애 감시를 수행합니다.
포트	0	장애 감시에 사용할 TCP/UDP 목적지 포트 번호.

만약 장애 감시에 사용할 TCP/UDP 목적지 포트를 지정하지 않은 경우(0으로 설정한 경우)에는 실제 서버에 설정된 RPORT가 사용됩니다. 그런데, 실제 서버에도 RPORT가 지정되지 않은(0으로 설정) 경우에는 각 장애 감시 유형마다 다음 표에 나타난 '기본 포트 번호'를 목적지 포트로 사용합니다.

[표 – 장애 감시에 사용되는 애플리케이션 별 포트 번호]

애플리케이션	기본 포트 번호
TCP	0
HTTP	80
TFTP	69(UDP)
NTP	123(UDP)

주의: 장애 감시 유형이 TCP, UDP 중 하나이고 장애 감시 포트 및 실제 서버의 RPORT가 0으로 설정되어 포트 번호가 지정되지 않은 경우에는 장애 감시의 결과가 항상 실패로 간주됩니다.

PAS-K는 기존 서버나 방화벽 등에 장애가 발생했을 때 기능을 대신할 백업 서버를 사용할 수 있습니다. 백업 서버는 평소에는 대기 상태로 있다가 장애 감시 기능을 통해 서버의 장애 감시가 발견되면 기존 서버가 수행하던 작업을 백업 서버가 모두 대신 수행하게 됩니다. 그리고, 서버의 장애가 해결되면 백업 서버는 다시 이전의 대기 상태로 돌아가게 됩니다.

주의: 실제 서버의 장애 감시 결과가 ACT가 아닌 경우에는 정상적으로 부하 분산 서비스가 제공되지 않을 수 있습니다.

실제 서버 설정 필요 사항

장애 감시 기능을 사용하려면 우선 해당 실제 서버에 감시하고자 하는 애플리케이션이 정상적으로 동작하고 있어야 합니다. 그리고, 애플리케이션이 실제로 사용하는 포트와 장애 감시 설정에 입력된 포트도 일치해야 합니다.

장애 감시 방법

PAS-K는 실제 서버의 장애를 감시할 때 다음과 같은 방법을 사용할 수 있습니다.

- HTTP 장애 감시
- ICMP 장애 감시
- NTP 장애 감시
- TCP 장애 감시
- TFTP 장애 감시
- UDP 장애 감시
- 스크립트 장애 감시

각 장애 감시 방법에 대해 상세히 알아봅니다.

HTTP 장애 감시

HTTP는 웹 서버와 웹 브라우저 사이에 데이터를 주고 받기 위한 프로토콜입니다. 웹 브라우저는 웹 서버로 접속해 요청 메시지를 전송하고, 웹 서버는 이를 받아 응답 메시지를 웹 브라우저에게 전달합니다. HTTP 장애 감시는 PAS-K가 이러한 웹 브라우저의 역할을 수행하도록 합니다. HTTP 장애 감시 기능을 사용하면, PAS-K는 실제 서버에 접속해 지정된 URI에 대한 GET 요청을 전송하고, 수신한 응답 메시지를 통해 실제 서버의 정상 동작 여부를 판단합니다.

HTTP 장애 감시 기능에서 사용 가능한 옵션은 다음과 같습니다.

[표 – HTTP 장애 감시에 사용되는 항목]

항 목	설 명
uri (필수 설정)	요청할 파일의 경로
host	HTTP 요청 헤더의 host 필드에 입력할 문자열
user-agent	HTTP 요청 헤더의 user-agent 필드에 입력할 문자열
status-code (필수 설정)	기대하는 HTTP 응답 상태 코드
expect	실제 서버로부터 받기를 기대하는 데이터
unexpect	실제 서버로부터 받아서는 안 되는 데이터 (받게 되는 경우 장애 감시 실패로 간주됨)
content-length	HTTP content-length 헤더에 명시된 컨텐트(파일)의 크기

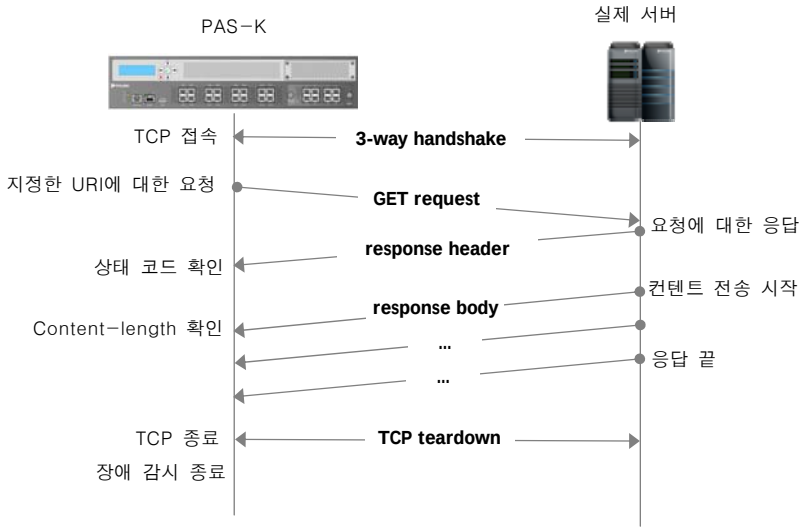
expect, unexpect옵션에는 TCP 장애 감시와 마찬가지로 탈출 문자를 사용하여 바이너리 데이터를 전송할 수 있습니다.

참고: content-length를 0으로 설정하는 것은 HTTP content-length 헤더에 명시된 컨텐트의 크기가 0인지를 검사하겠다는 의미입니다. content-length를 검사하지 않으려면, 0으로 설정하는 것이 아니라, **`no content-length`** 명령을 사용해야 합니다.

참고: content-length는 URI의 응답 크기를 지정하기 때문에, 이 옵션을 사용하여 해당 파일의 변조 여부를 확인할 수 있습니다. 그러나, 만약 해당 URI가 동적인 내용을 가지는 컨텐트라면 매번 크기가 달라지므로 content-length를 지정해서는 안됩니다.

동작 예

다음은 content-length 옵션이 설정되어 있는 경우에 HTTP 장애 감시 기능이 동작하는 과정을 나타낸 그림입니다.



[그림 – HTTP 장애 감시 동작 과정]

ICMP 장애 감시

ICMP 장애 감시는 PAS-K와 실제 서버 간의 물리적인 연결 상태를 검사하는 3계층 장애 감시 기능입니다. 예를 들어, 실제 서버의 전원이 꺼져 있거나 실제 서버와의 통신이 단절되는 경우, 혹은 PAS-K와 실제 서버 간에 케이블이 연결되어 있지 않은 경우로 인해 발생하는 실제 서버의 장애는 ICMP 장애 감시를 통해 확인할 수 있습니다. ICMP 장애 감시는 ICMP 패킷(ping 명령)을 사용하여 실제 서버의 상태를 검사합니다. ICMP 요청 패킷을 실제 서버의 IP 주소로 전송한 후 실제 서버에서 응답이 수신되지 않으면 실제 서버에 장애가 발생했다고 판단하고 부하 분산 서비스에서 해당 실제 서버를 제거합니다.

NTP 장애 감시

NTP(Network Time Protocol)는 NTP 서버로부터 시간 정보를 받아온 후 현재 시스템의 시간 정보를 최신으로 갱신하고 유지하기 위해 사용하는 프로토콜입니다. NTP 장애 감시 기능을 설정하면 PAS-K가 실제 서버에 접속하여 시간 정보를 받아온 후, 실제 서버로부터 받은 시간 정보와 PAS-K의 현재 시간을 비교해 보고 실제 서버의 장애 여부를 판단하게 됩니다. 만약 PAS-K와 실제 서버의 시간 정보에 차이가 있을 경우에는 실제 서버에 장애가 발생하였다고 판단합니다.

NTP 장애 감시 기능에서 사용 가능한 옵션은 다음과 같습니다.

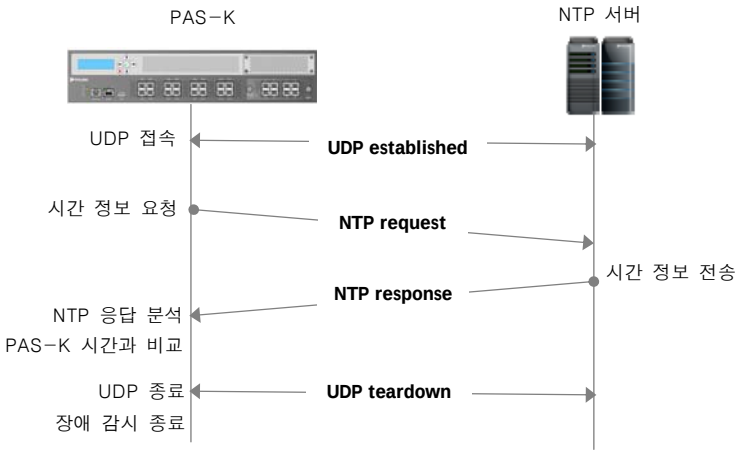
[표 – NTP 장애 감시에 사용되는 항목과 기본값]

항 목	설 명
tolerance	실제 서버와 PAS-K 의 시간 차이 허용 범위. (시간 차이가 Tolerance 값보다 크면 실제 서버에 장애가 발생하였다고 판단함)
update-delay	실제 서버가 시간 정보를 업데이트 하는 주기 (실제 서버가 가장 최근에 시간 정보를 업데이트 한 이후로 경과된 시간이 지정한 주기보다 길면 실제 서버에 장애가 발생하였다고 판단함)

참고: 옵션을 아무것도 지정하지 않는 경우에는, PAS-K와 실제 서버 간의 시간 정보가 일치하는 지의 여부는 판단하지 않고, NTP 프로토콜의 형식에 맞는 응답이 전송되면 장애 감시에 성공한 것으로 판단합니다.

동작 예

다음은 tolerance, update-delay 옵션이 지정되어 있는 경우, NTP 장애 감시 기능이 동작하는 과정을 나타낸 그림입니다.



[그림 – NTP 장애 감시 동작 과정]

TCP 장애 감시

TCP 장애 감시는 HTTP나 FTP, 텔넷 등 TCP에 기반한 애플리케이션을 실제 서버가 서비스할 수 있는지를 검사하는 4계층 장애 감시 기능입니다. TCP 장애 감시는 사용자가 설정한 포트를 사용하여 TCP 세션 연결 요청을 실제 서버로 전송합니다. 실제 서버가 연결 요청에 대한 응답을 전송하여 PAS-K와 실제 서버 간에 TCP 세션이 연결되면 실제 서버가 정상적으로 동작하는 것으로 판단합니다. 이렇게 연결된 TCP 세션은 실제 서버의 동작을 확인한 즉시 PAS-K에서 연결 해지를 요청하여 연결을 종료합니다.

TCP 장애 감시 기능에서 사용 가능한 옵션은 다음과 같습니다.

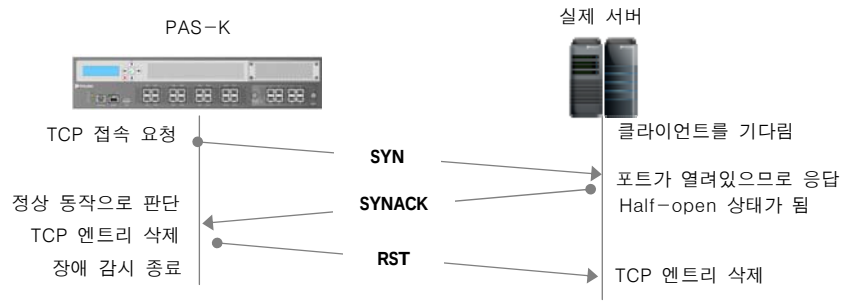
[표 – TCP 장애 감시에 사용되는 항목과 기본값]

항 목	설 명
half-open	TCP handshaking 후 FIN 패킷으로 접속을 끊음
send	TCP 세션이 연결되면 실제 서버로 전송할 데이터
expect	실제 서버로부터 받기를 기대하는 데이터
unexpect	실제 서버로부터 받아서는 안 되는 데이터

TCP Half-open 옵션을 사용하면 PAS-K는 실제 서버로부터 TCP SYN/ACK 패킷을 수신한 경우, ACK 패킷을 전송하는 대신 RST 패킷을 전송하여 바로 접속을 끊게 됩니다. 따라서 주고 받는 패킷의 수가 줄기 때문에 네트워크 자원을 절약할 수 있습니다.

뿐만 아니라 ACK 패킷 대신 RST 패킷을 전송하기 때문에 실제 서버가 PAS-K의 접속 요청을 애플리케이션으로 전달하기 전에 운영 체제가 바로 엔트리를 삭제할 수 있으므로 실제 서버의 부담을 줄일 수 있는 장점이 있습니다.

동작 예



[그림 - TCP Half-open 옵션을 활성화한 TCP 장애 감시의 동작 방식]

PAS-K에 등록된 실제 서버가 많은 경우에 FIN 패킷으로 TCP 접속을 끊게 되면 다수의 세션이 TIME_WAIT 상태로 장시간 남게 되는데, RST으로 TCP 접속을 끊으면 세션 엔트리가 즉시 삭제되므로 PAS의 부담을 줄일 수도 있습니다.

send, expect, unexpect 옵션은 TCP 세션이 연결되었을 때, send 옵션에서 지정한 데이터를 실제 서버로 전송한 후, 기대하는 응답(expect)이 오는지 혹은 받아서는 안 되는 응답(unexpect)이 오는지를 검사합니다. 수신한 데이터에 expect 옵션에서 지정한 문자열이 포함되어 있으면 실제 서버가 정상적으로 동작하는 것으로 판단하고, 만약, unexpect 옵션에서 지정한 문자열이 포함되어 있으면, 장애 감시에 실패한 것으로 판단합니다.

send, expect, unexpect에 지정하는 옵션 값은 기본적으로는 아스키 문자열이지만, 탈출 문자(escape characters)를 사용함으로써 바이너리 데이터를 입력할 수도 있습니다.

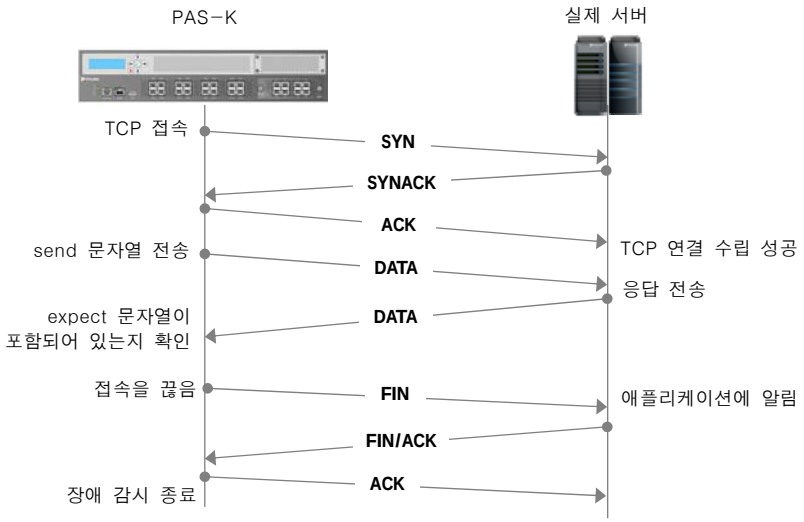
참고: send에 아스키(텍스트) 문자열을 입력하고자 하는 대부분의 경우에는 맨 뒤에 라인의 끝을 나타내는 줄 바꿈 문자인 " \r\n"을 삽입해야 합니다. 그렇지 않으면 서버는 라인의 끝을 입력 받기 전까지 응답 메시지를 주지 않게 되므로, 응답 대기 시간(timeout)을 초과하여 장애 감시에 실패하게 됩니다.

[표 – 탈출 문자에 사용할 수 있는 특수 문자]

탈출 문자	설 명
\\	역 슬래시 (₩)
\r	Carriage Return (CR)
\n	Linefeed (LF)
\t	Horizontal Tab (TAB)
\OOO	임의의 아스키 코드. OOO 위치에 세 자리의 8진수를 입력합니다.
\xHH	임의의 아스키 코드. HH 위치에 두 자리의 16진수를 입력합니다.

동작 예

다음은 send와 expect 옵션이 설정되어 있는 경우, TCP 장애 감시 기능이 동작하는 과정을 나타낸 그림입니다.



[그림 – TCP 장애 감시 동작 과정]

TFTP 장애 감시

TFTP(Trivial File Transfer Protocol)는 특정 서버로부터 파일을 다운로드 받거나 업로드 하기 위해서 사용하는 프로토콜입니다. 로그인 과정이 없기 때문에 보안 상 문제가 되지 않는 간단한 파일들을 다운로드 혹은 업로드 하기 위해 사용됩니다. TFTP 장애 감시 기능을 설정하면 PAS-K가 실제 서버에 접속하여 지정된 이름을 가진 파일을 다운로드 합니다. 그리고, 파일을 다운받는 과정에서 파일 내용을 읽어 expect, unexpect 옵션에서 지정한 특정 항목이 포함되었는지의 여부를 검사합니다. TFTP 장애 감시 기능에서 사용 가능한 옵션은 다음과 같습니다.

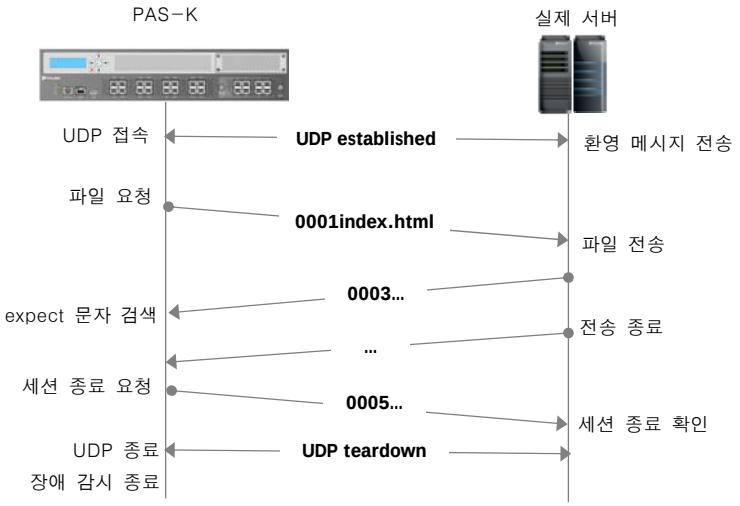
[표 – TFTP 장애 감시에 사용되는 항목과 기본값]

항 목	설 명
filename (필수 설정)	TFTP 서버에 접속하여 다운로드 할 파일의 이름
expect	실제 서버로부터 받기를 기대하는 데이터
unexpect	실제 서버로부터 받아서는 안 되는 데이터

expect, unexpect옵션에는 TCP 장애 감시와 마찬가지로 탈출 문자를 사용하여 바이너리 데이터를 지정할 수 있습니다.

동작 예

다음은 filename과 expect 옵션이 지정되어 있는 경우, TFTP 장애 감시 기능이 동작하는 과정을 나타낸 그림입니다.



[그림 – TFTP 장애 감시 동작 과정]

UDP 장애 감시

UDP 장애 감시는 UDP 프로토콜을 사용하는 애플리케이션의 장애 감시를 수행하는 기능입니다. UDP 장애 감시 기능은 TCP 장애 감시 기능과 마찬가지로 send, expect, unexpect 옵션을 사용하여 실제 서버로부터 원하는 응답이 오는지를 검사할 수 있습니다. UDP 고급 장애 감시 기능을 설정하면 PAS-K는 send 옵션에서 지정한 문자열(데이터)을 내용으로 하는 UDP 패킷을 생성하여 실제 서버에게 전송하고, 실제 서버로부터의 응답 UDP 패킷이 정상적으로 전달되는지 확인합니다.

TCP 기반의 다른 장애 감시들과는 다르게, UDP 장애 감시는 실제 서버로부터의 응답 패킷이 전송될 때 출발지 포트 번호를 검사하지 않습니다. 예를 들어 TFTP 서버의 장애 감시를 위해 PAS-K가 목적지 포트 번호를 69(TFTP)로 하여 UDP 패킷을 전송하면, 응답 패킷의 출발지 포트 번호가 69가 아니더라도 이를 수신합니다(TCP 기반의 장애 감시에서는 이를 장애 감시에 실패한 것으로 인식함). 이것은 UDP 기반 프로토콜은 출발지 포트로 임의의 임시 포트(UDP ephemeral port)를 사용하는 경우가 많기 때문입니다. UDP 장애 감시 기능에서 사용 가능한 옵션은 다음과 같습니다.

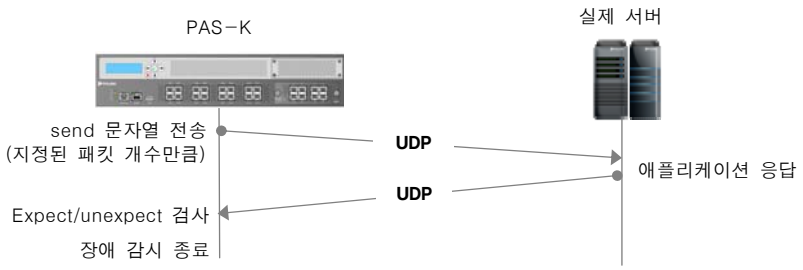
[표 – UDP 장애 감시에 사용되는 항목과 기본값]

항 목	설 명
packets (필수 설정)	반복 전송할 UDP 패킷의 수 (1~ 5 사이로 입력)
send	UDP 패킷에 실어 보낼 데이터
expect	실제 서버로부터 받기를 기대하는 데이터
unexpect	실제 서버로부터 받아서는 안되는 데이터

UDP의 특성 상 패킷이 PAS-K와 실제 서버 사이에서 유실되더라도 자체적으로 재전송할 수 없습니다. 이런 경우에 UDP 장애 감시 기능을 사용하여 packets 옵션을 설정하면, PAS-K가 같은 내용의 패킷을 여러 번 전송합니다. send, expect, unexpect 옵션은 TCP 장애 감시와 마찬가지로 탈출 문자를 사용하여 바이너리 데이터를 전송할 수 있습니다.

동작 예

다음은 send, expect, unexpect 옵션을 모두 설정하였을 경우, UDP 장애 감시 기능이 동작하는 과정을 나타낸 그림입니다.



[그림 – UDP 장애 감시 동작 과정]

스크립트 장애 감시

스크립트 장애 감시는 사용자가 작성한 스크립트를 사용하여 실제 서버의 상태를 검사하는 7계층 장애 감시 기능입니다. 스크립트에는 실제 서버에 전송할 메시지와 서버로부터 수신할 응답 메시지, 그리고 메시지를 주고 받을 때 사용할 포트 번호 및 프로토콜을 지정합니다. 스크립트 장애 감시는 스크립트를 구성하는 다음과 같은 명령에 의해 이루어집니다.

[표 - 스크립트 장애 감시에 사용되는 항목]

항 목	설 명
script *<INDEX>*	<Script 설정 모드>로 진입
command open	실제 서버와 데이터를 송수신할 세션 연결
protocol {tcp | udp}	세션 연결 시 사용할 프로토콜 지정
port *<PORT>*	지정한 포트 번호를 사용하여 실제 서버와 세션 연결
command {send | send-bin}	실제 서버로 아스키(send)나 바이너리(send-bin) 데이터 전송
command {expect | expect-bin}	실제 서버로부터 아스키(expect)나 바이너리(expect-bin) 데이터 수신
data *<DATA>*	지정한 데이터의 종류(아스키/바이너리)에 따라 실제 서버에 전송 하거나 실제 서버로부터 수신할 문자열 입력
command close	세션 해제

스크립트 장애 감시는 실제 서버의 애플리케이션과 컨텐트를 동적으로 검사하는데 사용될 수 있습니다.

참고: 위의 명령들은 <Script 설정 모드>에서 지정할 수 있고 명령의 종류에 따라 새로운 Script 설정 번호를 지정해야 합니다. 자세한 설정 방법은 **장애 감시 설정 – CLI 설정하기 – 스크립트 장애 감시** 절을 참고합니다.

RADIUS 서버 장애 감시

RADIUS 서버 장애 감시는 RADIUS 서버에서 사용하는 인증 정보를 사용하는 서버의 상태를 검사하는 4 계층 장애 감시 기능입니다. 이 기능은 L4 서버 부하 분산 서비스에서 RADIUS 서버의 장애 감시용으로만 사용됩니다.

RADIUS 서버 장애 감시는 RADIUS 서버에 설정된 사용자 ID, 암호, 인증 비밀 키, 과금 비밀 키를 사용하여 RADIUS 서버로 접속한 후 더미(dummy) 요청을 전송합니다. RADIUS 서버가 이 요청에 대한 응답을 전송하는지 여부에 따라 서버의 장애 여부를 판단하게 됩니다.

참고: RADIUS 서버에 더미 요청을 전송하는 것은 보안을 위해서입니다. 더미 요청을 전송해도 RADIUS 서버의 장애감시에는 문제가 없습니다. 하지만, RADIUS 서버에 설정하는 사용자 ID와 암호, 인증/과금 비밀키는 반드시 실제로 RADIUS 서버에서 사용하는 값을 지정해야 합니다.

RADIUS 서버는 사용자 인증(authentication)과 서비스 과금(accounting)을 해주는 서버입니다. 일반적으로 하나의 서버에서 두 기능을 모두 제공하지만 사용하는 포트가 서로 다릅니다. 일반적으로 인증용 포트는 1812, 과금용 포트는 1813을 사용합니다. 때로는 두 기능을 다른 서버에서 제공하기도 합니다. 그래서, PAS-K는 인증용 RADIUS 서버의 장애 감시와 과금용 RADIUS 서버의 장애 감시를 별도로 설정하도록 되어 있습니다.

지속 연결(Persistence)

PAS-K의 부하 분산 서비스는 특정 클라이언트가 요청하는 모든 연결을 항상 동일한 실제 서버를 통해 이루어질 수 있게 해주는 지속 연결 기능(persistence 혹은 sticky connection)을 제공합니다. PAS-K는 지속 연결 유지를 위해 타임아웃(sticky time) 설정 기능을 제공합니다. 타임아웃으로 설정한 시간이 경과되기 전에 동일한 클라이언트로부터의 연결이 시도되면 이전에 연결했던 서버(혹은 방화벽)와 동일한 서버로 연결됩니다. 지속 연결을 위한 타임아웃은 기본으로 60초로 설정되어 있고, 사용자가 변경할 수 있습니다.

서버 부하 분산의 지속 연결

일반적인 서버 부하 분산 환경에서는 클라이언트가 시도하는 여러 개의 인터넷 연결은 서로 독립적으로 동작합니다. 동일한 클라이언트에서 연속적으로 연결을 요청하는 경우에도 이전에 연결된 실제 서버와 관계 없이 부하 분산 방식에 의해 선택된 실제 서버로 연결됩니다. 하지만, 애플리케이션의 종류에 따라 정상적인 기능 동작과 성능을 빠르게 수행하기 위해 같은 클라이언트로부터 오는 여러 연결 요청이 반드시 같은 실제 서버로 연결되어야 할 필요가 있습니다.

인터넷 뱅킹이나 온라인 쇼핑과 같이 복잡한 웹 애플리케이션은 대부분 클라이언트 단위의 정보를 서버마다 저장합니다. 이렇게 저장된 정보들은 클라이언트와 직접 교환되지 않고 서버에서 내부적으로 관리되다가 해당 클라이언트의 요청이 있을 때 액세스됩니다. 예를 들어, 어떤 사용자가 인터넷 서점에서 여러 권의 책을 구입하는 경우 장바구니에 담아둔 책의 목록은 서버에 저장되고, 클라이언트와 서버 간에는 사용자를 식별할 수 있는 간단한 문자열만 전송됩니다.

서버 부하 분산 구성에서 이와 같은 애플리케이션을 원활하게 서비스하기 위해서는 클라이언트가 처음에 연결된 실제 서버로 계속해서 연결되도록 하는 지속 연결 기능이 필수적입니다. 지속 연결 기능을 적용하지 않으면, 하나의 작업 단위(transaction)를 구성하는 여러 TCP 세션 중 하나가 다른 실제 서버에 연결되는 경우, 해당 실제 서버에는 클라이언트에 대한 정보가 없기 때문에 전체 작업을 처음부터 다시 수행해야만 합니다.

방화벽 부하 분산의 지속 연결

방화벽 부하 분산 구성에서는 동일한 세션에 속하는 패킷들이 모두 동일한 방화벽을 통해 전송되어야 합니다. 방화벽은 세션의 상태 정보를 사용하여 패킷 필터링을 수행하기 때문에, 현재 상태에 맞지 않은 패킷이 수신되는 경우에는 비 정상적인 패킷으로 간주하여 폐기하게 됩니다. 그러므로, 방화벽의 양쪽에 위치한 PAS-K에 의해 같은 세션의 패킷이 서로 다른 방화벽으로 전송되면 세션이 정상적으로 유지될 수 없습니다. 이를 방지하기 위해 PAS-K는 방화벽 부하 분산이 적용된 외부 PAS-K와 내부 PAS-K에서 송수신되는 패킷의 경로를 기억하여 경로를 지속적으로 유지할 수 있도록 해주는 지속 연결 기능을 지원합니다.

VPN 부하 분산의 지속 연결

VPN 부하 분산 구성에서는 지사 네트워크의 모든 호스트들은 하나의 게이트웨이를 통하여 터널링(tunneling)을 형성하기 때문에 서브넷 단위로 동일한 보안 채널(secure channel)을 사용해야 합니다. 이를 위해 내부 PAS-K에서 지사 네트워크를 하나의 VPN 클라이언트 군으로 등록하여 보안 채널의 지속성을 유지시켜주는 지속 연결 기능을 지원합니다.

캐시 서버 부하 분산의 지속 연결

캐시 서버 부하 분산 구성에서는 일반적으로 각각의 서버가 컨텐트를 독립적으로 저장하고 있습니다. 캐시 서버는 자신이 갖고 있지 않은 컨텐트를 클라이언트로부터 요청받게 되는 경우, 웹 서버에게 해당 컨텐트를 전송받아 이를 클라이언트에게 다시 전달하는 동작을 수행하게 됩니다. 그러나, 이러한 경우 전체적인 웹 애플리케이션의 성능이 저하될 가능성이 있습니다. 따라서, 지속 연결 기능을 캐시 서버 부하 분산 구성에 적용하면, 실제 서버의 캐시 효율이 높아져 웹 애플리케이션의 성능이 크게 향상됩니다.

지속 연결 기능의 종류

PAS-K는 지속 연결을 위해 사용하는 값의 종류에 따라 다음과 같은 4가지 종류의 지속 연결 기능을 제공합니다.

- IP 지속 연결
- HTTP 쿠키 지속 연결
- HTTP 헤더 지속 연결
- 세션 ID 지속 연결

IP 지속 연결 기능은 모든 부하 분산 서비스에서 모두 사용할 수 있고, HTTP 쿠키 지속 연결 기능과 HTTP 헤더 지속 연결은 부하 분산 대상 애플리케이션이 HTTP인 L7 부하 분산 서비스에서만 사용할 수 있습니다. 또한, 세션 ID 지속 연결 기능은 고급 L7 부하 분산 서비스에서만 사용할 수 있습니다.

각 종류의 지속 연결에 대해 상세히 살펴봅니다.

IP 지속 연결

IP 지속 연결 기능은 L4 부하 분산과 L7 부하 분산에서 사용할 수 있는 지속 연결 기능으로 클라이언트의 IP 주소를 사용하여 실제 서버를 선택하는 방식입니다. 따라서, IP 지속 연결 기능을 사용하면 출발지 IP 주소가 같은 TCP 세션은 항상 동일한 실제 서버로 연결됩니다. PAS-K에서는 설정된 sticky 타임아웃 시간 동안 출발지 IP 주소와 실제 서버 간의 매핑 정보가 유지되기 때문에 이 시간 동안 동일한 출발지 IP 주소를 가지는 요청이 들어오면 이전에 연결된 실제 서버로 보내줍니다.

IP 주소를 통해 클라이언트를 구분하기 어려운 다음과 같은 상황에서 IP 지속 연결 기능을 적용하게 되면 문제가 발생할 수 있습니다.

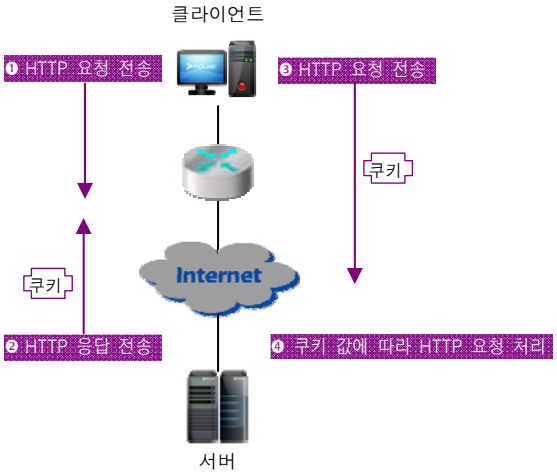
- **여러 클라이언트가 같은 IP 주소를 사용하는 경우**
  주로 방화벽 뒤에 있는 많은 클라이언트들이 같은 프록시 서버를 통해 웹 사이트에 접속하는 경우입니다. 이런 경우, 애플리케이션의 동작에는 문제가 없지만 같은 프록시 서버를 사용하는 클라이언트들이 같은 실제 서버로 연결되므로 부하 분산이 원활하게 이루어지기 어렵습니다.
- **한 클라이언트가 여러 개의 IP 주소를 사용하는 경우**
  NAT 환경이나 무선 인터넷 환경에서 발생되는 경우입니다. 이런 경우, IP 지속 연결 기능을 사용하면 애플리케이션이 제대로 동작할 수 없습니다.

HTTP 쿠키 지속 연결

HTTP 쿠키 지속 연결은 클라이언트와 서버 간에 주고 받는 쿠키 정보를 사용하여 실제 서버를 선택하는 방식입니다. 앞에서 살펴본 IP 지속 연결 기능을 적용하기 힘든 두 가지 상황에 이 방식을 사용하면 문제 없이 지속 연결을 제공할 수 있습니다.

쿠키 개요

쿠키는 HTTP 서버와 클라이언트 간의 상태 정보를 교환하기 위해 사용되는 값으로 일반적으로 서버와 클라이언트 간에 쿠키가 전달되는 과정은 다음과 같습니다.



[그림 - 일반적인 쿠키의 전달 과정]

1. 클라이언트에서 쿠키를 포함하지 않는 HTTP 요청을 전송합니다.
2. 서버가 응답할 때 Set-Cookie 헤더를 사용하여 클라이언트가 저장할 쿠키를 전달합니다.
3. 클라이언트는 서버에서 받은 쿠키를 저장했다가 같은 서버로 접속할 때 HTTP 요청 헤더 Cookie 필드에 넣어서 보냅니다.
4. 서버는 HTTP 요청 헤더에 있는 쿠키 값에 따라 HTTP 요청을 처리합니다.

서버가 클라이언트로 Set-Cookie 필드를 전송할 때 쿠키가 소멸되는 날짜와 시간을 정할 수 있는데, 이 시간이 지나면 클라이언트에 저장된 쿠키는 소멸되어 더 이상 HTTP 요청 헤더에 포함되지 않습니다. 이렇게 소멸 시간이 표시된 쿠키를 영구 쿠키(permanent cookie)라 하고, 소멸 시간이 생략된 쿠키를 임시 쿠키(temporary cookie)라 합니다. 임시 쿠키는 웹 브라우저가 종료될 때 삭제됩니다.

HTTP 쿠키 지속 연결 동작 방식

HTTP 쿠키 지속 연결은 클라이언트와 서버 간에 전송되는 쿠키를 응용하여, 클라이언트가 처음으로 실제 서버에 접속했을 때 실제 서버에 대한 정보를 쿠키에 기록합니다. 이 후, 클라이언트가 전송하는 HTTP 요청에는 실제 서버에 대한 정보가 담긴 쿠키가 포함되어 있기 때문에 쿠키를 통해 해당 클라이언트가 이전에 연결되었던 실제 서버를 알아낼 수 있습니다.

예를 들어, 클라이언트에서 그룹 'CGI'에 속하고 IP 주소가 192.168.1.1인 실제 서버로 HTTP 요청을 전송하면 실제 서버는 HTTP 응답 헤더에 다음과 같은 Set-Cookie 필드를 포함시켜서 전송합니다.

Set-Cookie: PiolinkCGI=c0a80101; path=/

이와 같은 쿠키를 수신한 클라이언트는 이후 HTTP 요청을 전송할 때 헤더의 Cookie 필드에 다음과 같은 값을 삽입합니다.

Cookie: PiolinkCGI=c0a80101

HTTP 쿠키 지속 연결 기능이 활성화되어 있는 부하 분산 서비스에서 이러한 HTTP 요청을 수신하면 부하 분산 방식을 통해 실제 서버를 선택하는 대신 IP 주소가 192.168.1.1인 실제 서버를 바로 선택하게 됩니다.

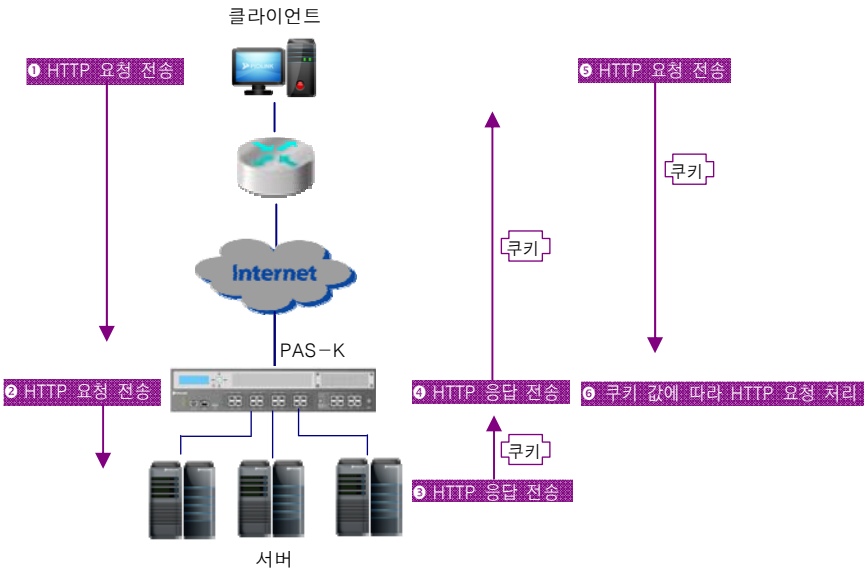
HTTP 쿠키 지속 연결 모드

HTTP 쿠키 지속 연결 기능은 Set-Cookie 값을 기록하는 대상에 따라 Passive, Insert, Rewrite, Hash의 4가지 모드로 나눠집니다. Hash 모드는 나머지 세 모드와 달리 실제 서버가 세션 별로 부여한 쿠키를 지속 연결 기능으로 제공합니다. 이 경우는 서버가 부여한 cookie 값과 이전에 연결된 실제 서버, 즉 그 cookie 값을 부여한 서버를 mapping 하는 정보를 PAS-K에서 설정된 시간 동안 유지하게 됩니다. L7 부하 분산에서는 그룹 별로 지속 연결 방식을 설정할 수 있습니다. 각 모드에 대해 살펴봅니다.

Passive 모드

Passive 모드에서는 영구 쿠키를 실제 서버가 기록합니다. Passive 모드로 설정된 그룹에 속하는 실제 서버는 'Piolink<그룹 이름>'을 이름으로 하고 자신의 IP 주소를 쿠키 값으로 하는 영구 쿠키를 Set-Cookie 필드에 포함시켜 HTTP 응답을 전송합니다. 이 모드에서는 Set-Cookie 필드를 실제 서버가 기록하기 때문에 실제 서버의 설정에 따라 임시 쿠키나 영구 쿠키를 모두 사용할 수 있습니다.

다음은 Passive 모드에서 쿠키가 전달되는 과정을 보여주는 그림입니다.



[그림 - Passive 모드에서 쿠키 전달 과정]

Passive 모드에서 쿠키가 전송되는 과정은 다음과 같습니다.

1. 클라이언트에서 쿠키가 포함되지 않은 HTTP 요청을 전송합니다.
2. L7 부하 분산 서비스에서 부하 분산 방식을 통해 실제 서버를 선택하고 실제 서버로 HTTP 요청을 전달합니다.
3. 실제 서버는 HTTP 응답의 헤더에 영구 쿠키를 삽입하여 전송합니다.
4. PAS-K는 실제 서버가 전송한 HTTP 응답을 클라이언트에게 보냅니다. 이를 수신한 클라이언트는 영구 쿠키를 저장합니다.
5. 클라이언트는 다음 HTTP 요청시 저장해둔 영구 쿠키를 헤더에 포함시켜 보냅니다.
6. L7 부하 분산 서비스는 HTTP 요청에 포함된 영구 쿠키를 기반으로 이전에 연결한 실제 서버를 선택합니다.

Passive 모드는 실제 서버가 쿠키를 기록하게 함으로써 PAS-K의 부하를 덜어주지만, 각 실제 서버에서 HTTP 응답에 Set-Cookie 헤더를 추가하도록 하는 설정을 모두 다르게 설정해주어야 합니다.

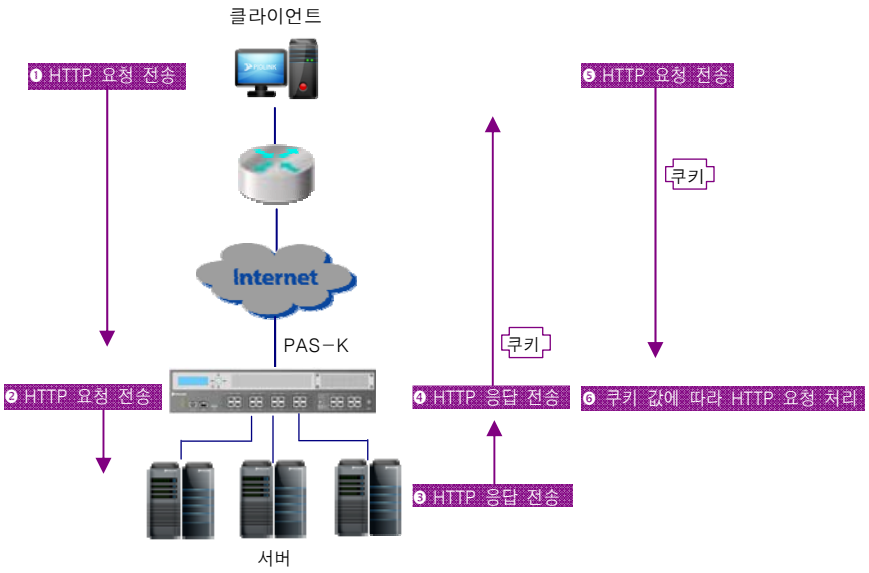
참고: Apache 계열의 웹 서버에서 모든 HTTP 응답에 Set-Cookie 헤더를 추가하도록 하려면 httpd.conf 파일에 다음을 추가해야 합니다.

```
Header add Set-Cookie CookieName=value,…
```

Insert 모드

Insert 모드에서는 PAS-K가 실제 서버의 HTTP 응답 헤더를 조작하여 Set-Cookie 필드를 추가합니다. Insert 모드를 사용하는 경우에는 쿠키의 제한 시간을 설정할 수 있습니다. 제한 시간을 설정하면 현재 시각에 제한 시간만큼을 더한 시각이 쿠키의 소멸 시각이 됩니다. 제한 시간을 설정하지 않으면 Set-Cookie 필드에 소멸 시각이 생략되어 임시 쿠키로 동작합니다.

다음은 Insert 모드에서 쿠키가 전달되는 과정을 보여주는 그림입니다.



[그림 - Insert 모드에서 쿠키 전달 과정]

Insert 모드에서 쿠키가 전송되는 과정은 다음과 같습니다.

1. 클라이언트에서 쿠키가 포함되지 않은 HTTP 요청을 전송합니다.
2. L7 부하 분산 서비스에서 부하 분산 방식을 통해 실제 서버를 선택하고 실제 서버로 HTTP 요청을 전달합니다.
3. 실제 서버는 쿠키에 대한 조작없이 HTTP 응답을 전송합니다.
4. PAS-K에서 HTTP 응답의 헤더에 영구 쿠키를 삽입하여 전송하고, 이를 수신한 클라이언트는 영구 쿠키를 저장합니다.
5. 클라이언트는 다음 HTTP 요청시 저장해둔 영구 쿠키를 헤더에 포함시켜 보냅니다.
6. L7 부하 분산 서비스는 HTTP 요청에 포함된 영구 쿠키를 기반으로 이전에 연결한 실제 서버를 선택합니다.

Insert 모드는 실제 서버에서 Set-Cookie 헤더를 추가하도록 하기 위해 필요한 설정 작업을 하지 않아도 되지만, PAS-K의 부하가 증가됩니다.

Rewrite 모드

Rewrite 모드는 Passive 모드와 Insert 모드의 중간 형태로 실제 서버에서는 영구 쿠키가 들어갈 공간을 만들어두고 실제 쿠키 값은 PAS-K가 삽입하는 방식입니다. 지속 연결 기능이 Rewrite 모드로 설정된 그룹에 속하는 실제 서버들은 'Piolink<그룹 이름>'을 이름으로 하고 55개의 '0'으로 구성된 쿠키 값을 Set-Cookie 필드에 포함시켜야 합니다. 다음은 그룹 이름이 'CGI'인 그룹에 속한 실제 서버가 Rewrite 모드에서 Set-Cookie 필드에 포함 시키는 쿠키 값입니다.

Set-Cookie: PiolinkCGI=0000000000000000000000000000000000000000000000000000

PAS-K는 위와 같은 쿠키 값이 채워진 HTTP 응답을 서버로부터 수신하면 쿠키 값을 변경한 후에 클라이언트로 전송합니다. Rewrite 모드는 Insert 모드와 마찬가지로 쿠키의 제한 시간을 설정할 수 있습니다. 제한 시간을 설정하면 현재 시각에 제한 시간만큼을 더한 시각이 쿠키의 소멸 시각이 됩니다. 제한 시간을 설정하지 않으면 Set-Cookie 필드에 소멸 시각이 생략되어 임시 쿠키로 동작합니다.

Rewrite 모드에서 쿠키가 전달되는 과정은 다음과 같습니다.

1. 클라이언트에서 쿠키가 포함되지 않은 HTTP 요청을 전송합니다.
2. L7 부하 분산 서비스에서 부하 분산 방식을 통해 실제 서버를 선택하고 실제 서버로 HTTP 요청을 전달합니다.
3. 실제 서버는 쿠키 값으로 55개의 '0'을 채운 후에 HTTP 응답을 전송합니다.
4. PAS-K에서 HTTP 응답의 헤더에 영구 쿠키를 삽입하여 전송하고, 이를 수신한 클라이언트는 영구 쿠키를 저장합니다.
5. 클라이언트는 다음 HTTP 요청시 저장해둔 영구 쿠키를 헤더에 포함시켜 보냅니다.
6. L7 부하 분산 서비스는 HTTP 요청에 포함된 영구 쿠키를 기반으로 이전에 연결한 실제 서버를 선택합니다.

Rewrite 모드에서는 같은 그룹의 실제 서버에서 기록하는 쿠키 값이 동일하기 때문에 각 실제 서버에서 HTTP 응답에 Set-Cookie 헤더를 추가하도록 하는 설정을 모두 똑같이 설정할 수 있습니다. 그리고, PAS-K의 부하도 Insert 모드보다는 줄일 수 있습니다

Hash 모드

앞에서 살펴본 Passive, Insert, Rewrite 모드에서는 연결된 실제 서버의 정보를 'Piolink<그룹 이름>'의 이름을 가진 영구 쿠키에 기록하여 HTTP 응답에 포함시켜 전송합니다. Hash 모드에서는 이러한 영구 쿠키 대신 세션 관리를 위해 실제 서버에 임의로 부여되는 '세션 쿠키'가 HTTP 응답에 포함됩니다. 세션 쿠키를 수신한 클라이언트는 이 후 HTTP 요청을 다시 전송할 때 세션 쿠키를 포함시켜서 HTTP 요청을 전송하게 됩니다.

PAS-K는 HTTP 요청에 포함되어 있는 세션 쿠키만 보고는 실제 서버를 알아낼 수 없기 때문에 실제 서버에서 세션 쿠키를 HTTP 응답에 포함시켜 보내면 실제 서버와 세션 쿠키의 매핑 정보를 저장해둡니다. 이 매핑 정보를 사용하여 클라이언트가 전송한 HTTP 요청의 세션 쿠키를 통해 이전에 접속한 실제 서버를 선택할 수 있게 됩니다.

다음은 Hash 모드에서 세션 쿠키가 전달되는 과정과 각 과정에서 클라이언트와 PAS-K, 실제 서버가 수행하는 작업들입니다.

1. 클라이언트는 쿠키가 포함되지 않은 HTTP 요청을 보냅니다.
2. L7 부하 분산 서비스에서 부하 분산 방식을 통해 실제 서버를 선택하고 실제 서버로 HTTP 요청을 전달합니다.
3. 실제 서버는 세션 쿠키를 삽입한 HTTP 응답을 전송합니다.
4. PAS-K는 세션 쿠키와 실제 서버의 매핑 정보를 저장하고, HTTP 응답을 클라이언트로 전송합니다. 이를 수신한 클라이언트는 세션 쿠키를 저장합니다.
6. 클라이언트는 다음 HTTP 요청시 저장해둔 세션 쿠키를 헤더에 포함시켜 보냅니다.
7. L7 부하 분산 서비스는 HTTP 요청에 포함된 세션 쿠키를 기반으로 이전에 연결한 실제 서버를 선택합니다.

PAS-K에서는 매핑 정보를 저장할 때(4번 과정), HTTP 응답에 포함된 세션 쿠키 전체를 저장할 수도 있고 일부만 저장할 수도 있습니다. 쿠키의 일부만 저장하려는 경우에는 저장할 부분에 대한 오프셋(offset)과 길이를 지정하면 됩니다. 그리고, 세션 쿠키와 실제 서버의 매핑 정보를 유지할 제한 시간을 설정하여 제한 시간이 경과되면 해당 매핑 정보가 PAS-K에서 삭제되도록 할 수 있습니다. 이러한 제한 시간과 오프셋, 길이를 적용할 세션 쿠키는 하나만 지정할 수도 있고 세션 쿠키의 이름 뒤에 asterisk(*)를 붙여서 특정 이름으로 시작하는 여러 세션 쿠키에 적용하도록 할 수도 있습니다.

예를 들어, 쿠키 이름을 ASPSESSIONID*으로 지정하고 오프셋을 9, 길이를 8, 제한 시간을 3일로 지정했을 때 다음과 같은 Set-Cookie 필드가 포함된 HTTP 응답이 실제 서버로부터 수신되면 PAS-K는 밑줄 친 부분만 저장하여 이후 클라이언트가 전송한 HTTP 요청의 쿠키 값을 비교할 때 사용됩니다.

Set-Cookie: ASPSESSIONIDQQQQGCBK=GKEIJFEDIOGLELEDCBFOHBDD

HTTP 헤더 지속 연결

클라이언트의 HTTP 요청이 방화벽, 게이트웨이, Proxy, 캐시 서버 등을 거쳐 PAS-K에 접속하는 경우 출발지 IP 주소가 NAT 됩니다. 이러한 경우 PAS-K는 다수(혹은 전부)의 클라이언트가 동일한 출발지 IP를 사용하는 것으로 판단하게 됩니다. 그렇기 때문에, 이 상태에서 IP 지속 연결 기능을 사용하게 되면 그룹 내의 몇몇 실제 서버로 요청이 모두 몰리게 되는 문제가 있습니다. 또한, 클라이언트의 IP 주소가 유동적이거나, 모바일 환경에서 단말기가 원래의 네트워크 커버리지(주파수 도달 범위)를 벗어나는 경우 IP 주소가 바뀌는 경우가 있습니다. 이러한 경우 클라이언트가 웹 서비스 사용 도중에 IP가 바뀌게 되어 서버로의 지속 연결이 수행되지 않는 문제가 발생할 수 있습니다.

HTTP 헤더 지속 연결 기능은 HTTP 요청 헤더에서 특정 필드 값 이나 특정 필드의 부분 문자열을 사용하여 실제 서버를 선택하는 방식입니다. 앞에서 살펴본 경우와 같이 IP 주소가 바뀌게 될 가능성이 있는 상황에서 이 방식을 사용하면 문제 없이 지속 연결을 제공할 수 있습니다.

HTTP 헤더 지속 연결 기능이 동작하는 과정은 다음과 같습니다.

1. 클라이언트는 항상 특정 헤더가 포함된 HTTP 요청을 전송합니다.
2. L7 부하 분산 서비스에서 부하 분산 방식을 통해 실제 서버를 선택하고 지속 연결 엔트리를 생성한 후 실제 서버로 HTTP 요청을 전달합니다.
3. 실제 서버는 HTTP 응답을 전송합니다.
4. 클라이언트는 다음 HTTP 요청시 특정 헤더가 포함된 HTTP 요청을 전송합니다.
5. L7 부하 분산 서비스는 HTTP 요청에 포함된 헤더 필드를 기반으로 지속 연결 엔트리에서 찾아 이전에 선택된 실제 서버로 HTTP 요청을 전달합니다.

Proxy 서버가 출발지 IP를 변경하기 때문에 IP 지속 연결 기능을 사용하기 곤란할 경우에는, HTTP 헤더 필드 지속 연결 기능을 사용하여 다음과 같이 설정하면 클라이언트의 실제 출발지 IP를 기준으로 지속 연결을 수행할 수 있습니다.

```
persist field X-Forwarded-For 20:00
```

위와 같이 설정하면 클라이언트 실제 IP 주소가 적혀있는 X-Forwarded-For 헤더 필드 값을 사용해 지속 연결을 수행하므로, 서로 다른 클라이언트 간에 적절하게 실제 서버가 선택되어 부하를 분산시킬 수 있습니다.

다음은 모바일 환경에서 HTTP User-Agent 헤더 필드에 단말기의 모델과 사양에 대한 정보가 포함되어 있는 경우의 설정 예입니다.

```
User-Agent: DoCoMo/2.0 F2051(c100;TB;serXXX...XXX;iccxxx...xxx)
                                  시리얼 번호
```

이 때, PAS-K는 다음과 같이 단말기의 시리얼 번호를 기준으로 실제 서버에 대한 지속 연결을 수행합니다.

```
persist field User-Agent 30:30 starter ser terminator ;
```

시작문자열 ser과 끝문자 열이 ;사이의 문자(시리얼 넘버)를 기준으로 지속 연결 수행

참고: 만약 클라이언트가 전송한 HTTP 요청 헤더에 지정된 필드가 존재하지 않으면 PAS-K는 지속 연결과 관련된 어떠한 동작도 수행하지 않습니다.

세션 ID 지속 연결

세션 ID 지속 연결은 고급 L7 부하 분산 서비스에서만 사용할 수 있는 지속 연결 기능으로 웹 애플리케이션의 세션 ID를 사용하여 실제 서버를 선택하는 방식입니다. 세션 ID는 웹 애플리케이션이 서버와 클라이언트 간의 세션을 유지하기 위해 응답 패킷의 쿠키 또는 URL에 삽입하는 값으로 클라이언트의 웹 브라우저마다 고유한 값을 부여함으로써 세션을 구분합니다.

PAS-K에서 세션 ID 지속 연결을 사용하기 위해서는 실제 서버의 웹 애플리케이션에서 사용하는 세션 ID 이름을 세션 키로 설정해야 합니다. 웹 애플리케이션에 따라 세션 ID 이름이 다르며, 일반적으로 많이 사용되는 웹 애플리케이션의 세션 ID 이름은 다음과 같습니다. 이외의 웹 애플리케이션을 사용하는 경우에는 세션 ID 이름을 정확히 확인하여 설정해야 합니다.

웹 애플리케이션	세션 ID 이름
PHP	PHPSESSID
JSP	JSESSIONID
ASP	ASPSESSIONID
ASP.NET	ASP.NET_SessionId

세션 ID 지속 연결 기능이 동작하는 과정은 다음과 같습니다.

1. 클라이언트에서 HTTP 요청을 전송합니다.
2. 고급 L7 부하 분산 서비스에서 부하 분산 방식을 통해 실제 서버를 선택하고 지속 연결 엔트리를 생성한 후 실제 서버로 HTTP 요청을 전달합니다.
3. 실제 서버의 웹 애플리케이션은 세션 ID를 삽입한 HTTP 응답을 전송합니다.
4. PAS-K는 HTTP 응답 패킷에 포함된 세션 ID와 실제 서버의 매핑 정보를 저장하고 HTTP 응답 패킷을 클라이언트로 전송합니다.
5. 클라이언트는 세션 ID를 저장하고, 이후 HTTP 요청시 세션 ID가 포함된 HTTP 요청을 전송합니다.
6. 고급 L7 부하 분산 서비스는 PAS-K에 저장해둔 세션 ID와 실제 서버와의 매핑 정보를 이용하여 이전에 선택된 실제 서버로 HTTP 요청을 전달합니다.

PAS-K에 저장된 세션 ID와 실제 서버의 매핑 정보는 설정한 지속 연결 엔트리 지속 시간 동안만 유지하고, 이후에는 삭제됩니다.

애플리케이션 가속(Application Accelerator)

개요

웹을 통해 제공되는 서비스와 컨텐트가 증가함에 따라 네트워크 대역폭 및 서버 성능 증대가 요구되고 있습니다. 그러나, 네트워크 대역폭과 서버 성능 증대에는 많은 비용이 필요하다는 문제가 있습니다. PAS-K는 이를 해결하기 위한 방법으로 애플리케이션 가속 기능을 제공합니다. 애플리케이션 가속은 웹 서버가 웹 응답 이외에 수행하는 부가적인 작업을 대신 수행하여 서버 자원의 부하를 줄임으로써 서버의 성능 및 응답 속도를 향상시킵니다.

PAS-K는 다음과 같은 세가지 방식의 애플리케이션 가속 기능을 제공합니다.

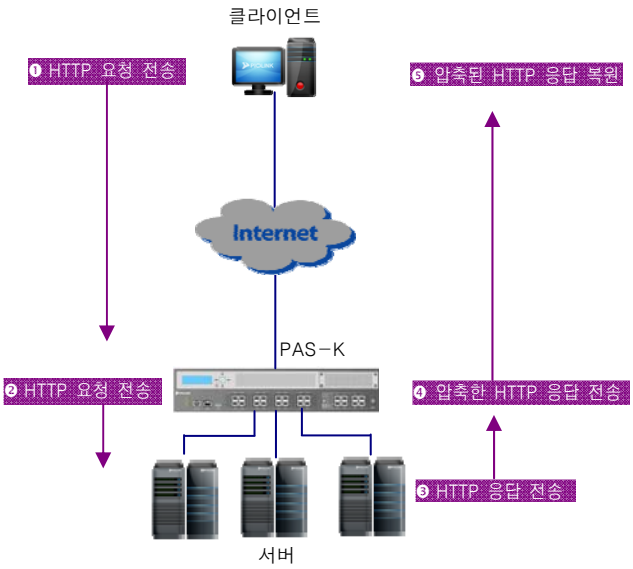
- HTTP 압축
- 캐싱
- SSL 가속

각 가속 기능에 대해 살펴봅니다.

HTTP 압축(HTTP Compression)

HTTP 압축은 HTTP 데이터를 압축하여 전송함으로써 대역폭을 절감하고, 전달 지연을 최소화하는 기능입니다. 웹 서버가 직접 HTTP 압축을 수행하는 경우에는 웹 서버의 CPU와 메모리 등의 하드웨어 자원에 부하가 발생하는 문제가 있습니다. PAS-K는 웹 서버를 대신하여 HTTP 압축을 수행함으로써 서버의 부하를 줄여주는 역할을 합니다. HTTP 압축에 사용되는 압축 알고리즘으로는 Gzip, Deflate가 있으며, PAS-K는 두 가지 알고리즘을 모두 지원합니다.

다음은 HTTP 압축이 수행되는 과정입니다.



[그림 – HTTP 압축 수행 과정]

1. 클라이언트는 웹 브라우저가 지원하는 압축 알고리즘을 Accept-Encoding 헤더에 표시하여 HTTP 요청을 전송합니다.
2. PAS-K는 클라이언트가 전송한 HTTP 요청을 고급 L7 부하 분산 서비스를 통해 서버를 선택하고, 해당 서버로 HTTP 요청을 전송합니다.
3. 웹 서버는 HTTP 요청에 대한 응답을 PAS-K로 전송합니다.
4. PAS-K는 HTTP 응답을 압축하고, 압축 알고리즘을 Content-Encoding 헤더에 표시하여 클라이언트에게 전송합니다.
5. 클라이언트의 웹 브라우저는 수신한 HTTP 응답의 압축을 해제하여 출력합니다.

HTTP 압축을 수행하기 위해서는 다음의 세가지 항목을 지정해야 합니다.

- **압축 컨텐트 유형**
  기본적으로 압축 알고리즘은 모든 컨텐트 유형을 압축할 수 있습니다. 그러나 이미 압축된 파일이거나 압축 알고리즘이 적용된 JPEG 파일 등의 경우에는 압축 효과가 미미하기 때문에 하드웨어 자원의 부하만 증가하는 문제점이 있습니다. PAS-K는 이를 방지하기 위해 기본적으로 'text/html' 컨텐트에 대해서 압축을 수행하며, 추가적으로 압축을 수행할 컨텐트를 MIME Type으로 지정할 수 있습니다.

- **압축 레벨**
  압축 레벨은 압축률을 의미합니다. 레벨이 높을수록 패킷의 크기는 작아지지만 하드웨어의 부하가 증가하고, 압축을 수행하는 시간이 늘어나게 되어 응답 시간이 늦어집니다.

- **압축 최소 길이**
  압축을 수행하면 일정 길이 이상의 압축 결과 파일이 생성됩니다. 이로 인해 압축 전 패킷의 길이가 작은 경우에는 압축 후 길이가 더 커질 수 있습니다. PAS-K는 압축을 수행할 패킷의 최소 길이를 지정하여 불필요한 하드웨어 자원의 사용과 네트워크 대역폭의 낭비를 방지합니다.

캐싱(Caching)

캐싱은 자주 요청되는 컨텐트를 PAS-K가 저장하여 동일한 컨텐트 요청에 대해 대신 응답하는 기능입니다. 캐싱 기능을 사용하면 LAN 구간에서의 트래픽과 서버의 하드웨어 부하를 감소시키고, 클라이언트로의 응답 속도를 향상시킬 수 있습니다.

PAS-K는 특정 컨텐트만 저장하여 운영하는 캐시 서버와는 달리 많이 요청되는 컨텐트 만을 자동적으로 저장하여 클라이언트에게 응답합니다. PAS-K에서 캐싱 기능을 사용하기 위해서는 다음과 같은 항목들을 설정해야 합니다.

- **캐시 크기**
  캐싱 기능에서 사용할 메모리 크기를 지정합니다. 16MB, 64MB, 256MB 중에서 선택할 수 있습니다.

- **캐시 시작 요청 수**
  캐싱을 수행할 기준이 되는 요청 수를 지정합니다. 특정 컨텐트에 대한 요청 횟수가 설정한 캐시 시작 요청 수 이상이 되면 해당 컨텐트를 저장하여 클라이언트에게 응답합니다.

- **캐시 만료 시간**
  캐시된 컨텐트에 대한 유효 시간을 지정합니다. 최대 65535초까지 설정할 수 있으며, 시간이 경과되면 해당 컨텐트는 삭제됩니다. 이 후, 캐시 시작 요청 수에 따라 해당 컨텐트의 캐싱이 다시 수행됩니다.

- **캐시 지원 요청 방식**
  PAS-K는 기본적으로 GET과 HEAD 요청 방식에 대해서만 캐시를 지원합니다. POST 요청 방식에 대해 캐싱 기능을 사용하려는 경우에는 해당 요청 방식을 추가적으로 지정해야 합니다.

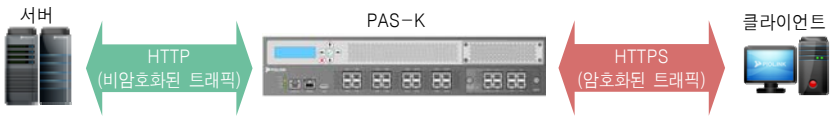
- **캐시 무시 헤더**
  클라이언트는 Expires와 Cache-Control 헤더를 사용하여 컨텐트를 서버에서 직접 응답하도록 할 수 있습니다. 이러한 요청을 수신한 경우, 헤더를 무시하고 캐싱을 수행할지 여부를 설정합니다. 두 가지 헤더를 모두 무시하거나, 특정 헤더만 무시할 수도 있습니다.

SSL 가속(SSL Acceleration)

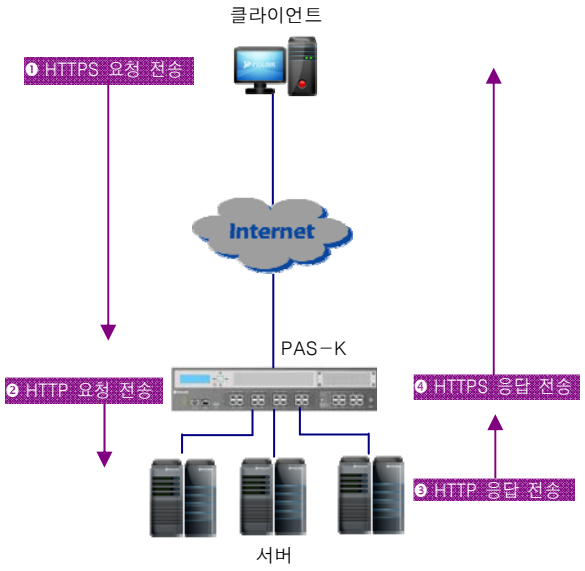
SSL(Secure Sockets Layer)은 서버와 클라이언트가 도청, 피싱, 변조 등의 위협으로부터 안전하게 데이터를 송수신할 수 있게 해주는 보안 프로토콜입니다. SSL 통신을 사용하면 서버와 클라이언트 간의 데이터가 암호화되어 전송되기 때문에 보안성은 높아지지만, 암호화/복호화를 수행하기 위한 서버의 부하가 늘어나게 되고, 클라이언트의 응답 대기시간도 길어집니다. 또한, 서버가 여러 대인 경우에는 SSL 통신을 위한 설정과 인증서와 비밀 키를 모든 서버에 등록하여 관리해야 하는 번거로움도 있습니다.

PAS-K는 이러한 문제점을 해결하기 위해 SSL 가속 기능을 제공합니다. SSL 가속은 PAS-K가 서버를 대신하여 SSL 통신을 제공함으로써 서버가 암호화/복호화를 수행하는데 필요한 하드웨어 자원의 부하를 줄여주는 기능입니다. 또한, SSL 통신을 위한 설정 및 비밀키, 인증서를 PAS-K에만 등록하면 되기 때문에 SSL 서비스를 제공하기 위한 환경을 효율적으로 구성 및 관리할 수 있습니다.

SSL 가속 기능을 사용하면 클라이언트와 PAS-K는 SSL(HTTPS) 통신을 수행하고, 서버와 PAS-K 는 일반 통신(HTTP)을 수행합니다.



다음은 SSL 가속이 수행되는 과정입니다.

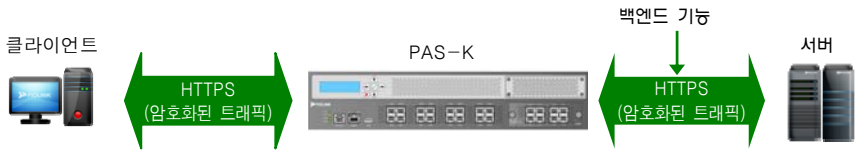


[그림 – SSL 가속 수행 과정]

1. 클라이언트는 웹 브라우저를 통해 HTTPS 요청을 전송합니다.
2. PAS-K는 클라이언트가 전송한 HTTPS 요청을 고급 L7 부하 분산 서비스를 통해 서버를 선택하고, 해당 서버로 HTTP 요청을 전송합니다.
3. 웹 서버는 HTTP 요청에 대한 응답을 PAS-K로 전송합니다.
4. PAS-K는 HTTP 응답을 HTTS로 변환하여 클라이언트에게 전송합니다.

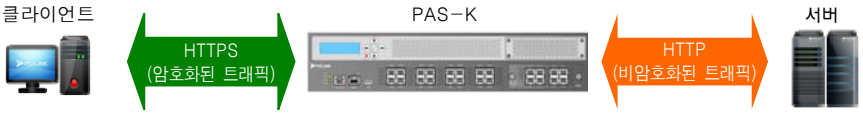
백엔드 기능

백엔드 기능은 다음과 같이 서버와 PAS-K 간에도 암호화된 HTTPS 트래픽을 전송하는 기능입니다.



SSL 기능은 일반적으로 클라이언트와 통신시에만 트래픽을 HTTPS로 암호화하고, 서버와는 HTTP 트래픽을 송수신합니다. 대개의 경우, 클라이언트의 트래픽이 공격의 대상이 되는데다 서버와의 통신에도 HTTPS로 암호화하면 성능이 매우 낮아지기 때문입니다. 하지만, 이미 SSL 기능을 사용 중인 클라이언트-서버 환경에서 PAS-K의 SSL 기능으로 대체하고자 하는 경우에는 백엔드 기능을 활성화하면 서버의 설정을 변경할 필요가 없으므로 설치가 간편해집니다.

백엔드 기능을 사용하지 않는 경우에는 클라이언트와 PAS-K간에는 HTTPS 트래픽이, PAS-K와 서버 간에는 HTTP 트래픽이 송수신됩니다.



참고: 백엔드 기능은 고급 L7 서버 부하 분산 서비스에서만 사용할 수 있습니다.

비밀 키와 인증서(Certificate)

SSL 비밀 키와 인증서는 서버와 클라이언트의 SSL 접속 준비 과정에서 사용하며, 비밀 키는 주고 받는 데이터를 암호화할 때 사용하고, 인증서는 클라이언트가 서버의 신원을 확인할 때 사용합니다.

비밀 키는 기존에 사용 중인 값을 그대로 사용할 수도 있고, PAS-K에서 생성할 수도 있습니다. 인증서는 VeriSign, GeoTrust, Comodo과 같은 인증 기관을 통해 발급 받아야 합니다. 인증 기관으로부터 인증서를 발급 받기 위해서는 CSR(Certificate Signing Request)이라는 인증 요청서를 인증 기관에 접수해야 합니다. 인증 요청서는 PAS-K에서 생성할 수 있습니다.

생성한 비밀 키와 인증 기관으로부터 발급 받은 인증서는 PAS-K에 등록해야 합니다. PAS-K는 등록된 비밀 키와 인증서를 사용하여 클라이언트와의 SSL 세션을 맺게 됩니다.

참고: 인증 기관은 디지털 인증서를 발급하거나 취소, 갱신하는 기관입니다. 널리 알려져 있는 인증 기관으로는 VeriSign, GeoTrust, Comodo 등이 있습니다.

참고: 인증 요청서는 인증 기관에서 발급 받은 공인 인증서 대신 내부에서 사용할 수 있는 자체 서명 인증서(Self-Signed Certificate)로 쓰일 수 있습니다. 자체 서명 인증서는 테스트 용으로만 사용하는 것이 좋습니다.

프로필(Profile)

프로필은 SSL 가속 기능을 사용하기 위해 필요한 인증서에 관한 정보를 담고 있는 설정입니다. 프로필에는 세션 재사용 기능(session resumption)의 사용 여부를 설정할 수 있습니다. 세션 재사용 기능은 클라이언트가 동일한 서버로 재 접속하는 경우, 이전 접속 시 사용했던 정보를 활용하여 접속 준비 과정을 간소화해주는 기능입니다. 세션 재사용 기능을 사용하면 반복적인 SSL 접속 준비 과정(handshaking)을 생략하여 PAS-K의 부하를 줄일 수 있지만, 보안성이 떨어집니다.

SSL SNI(Server Name Indication)

PAS-K는 하나의 IP 주소에서 여러 개의 도메인과 인증서를 사용하는 경우, 클라이언트가 요청한 URL에 따라 부하 분산 서비스를 선택하고, 해당 부하 분산 서비스에 설정된 인증서를 사용하도록 하는 SSL SNI 기능을 지원합니다. 이 기능은 동일한 가상 IP 주소와 포트를 사용하는 고급 L7 서버 부하 분산 서비스가 여러 개인 경우, 자동으로 동작합니다. 클라이언트가 도메인이 아닌 IP 주소로 접속하는 경우에는 우선수위가 높은 고급 L7 서버 부하 분산 서비스를 적용합니다.

장애 감시 설정

부하 분산 서비스를 사용하기 위해서는 먼저 실제 서버의 상태를 감시하기 위한 장애 감시를 설정해야 합니다. 장애 감시는 부하 분산 서비스, 실제 서버와 독립적으로 설정하며, 하나의 장애 감시를 서로 다른 부하 분산 서비스 또는 실제 서버에서 동시에 사용할 수 있습니다. 그러나, 특정 실제 서버의 애플리케이션에 맞게 옵션을 설정한 경우에는 해당 실제 서버에만 사용해야 합니다.

CLI에서 설정하기

이 절에서는 CLI 명령을 사용하여 장애 감시를 설정하는 방법에 대해 살펴봅니다.

장애 감시 설정

다음은 장애 감시를 설정하는 방법입니다. PAS-K에는 최대 128개의 장애 감시를 설정할 수 있으므로, 여러 개의 장애감시를 설정하는 경우에는 다음 과정을 반복하면 됩니다.

참고: 장애 감시의 종류에 따라 추가로 설정해야 하는 항목들이 서로 다르기 때문에 이 절에서는 모든 종류의 장애 감시에서 공통적으로 설정해야 하는 항목들을 설명한 후, 각 장애 감시마다 별도로 설정하는 값들은 다음 절에서 살펴보도록 합니다.

순서	명 령	설 명
1	**health-check** *<ID>*	<Configuration 모드>에서 <Health-Check 설정 모드>로 들어갑니다. • *<ID>* 장애 감시 ID. 설정 범위: 1 ~ 128
2	**type** {**act** | **http** | **icmp** | **inact** | **ntp** | **radius-acct** | **radius-auth** | **script** | **tcp** | **tftp** | **udp**}	장애 감시 종류를 선택합니다. **act**를 선택한 경우에는 항상 장애 감시에 성공한 것으로 판단하고, **inact**를 선택한 경우에는 항상 장애 감시에 실패한 것으로 판단합니다. (기본값: icmp) **참고:** 지정한 장애 감시 종류에 따라 추가로 필요한 설정 작업을 수행합니다.
3	**port** *<PORT>*	장애 감시 패킷(HC 패킷)을 전송할 때 사용할 포트 번호를 설정합니다. • *<PORT>* 포트 번호. 설정 범위: 0 ~ 65535, 기본값: 0
4	**timeout** *<TIMEOUT>*	서버의 장애 여부를 판단하는 타임아웃 값을 설정합니다. 서버로 장애 감시 패킷을 전송한 후 지정된 타임 아웃이 경과할 때까지 서버로부터 응답이 없는 경우에는 서버에 장애가 발생한 것으로 판단합니다. • *<TIMEOUT>* 타임아웃 시간. 설정 범위: 0 ~ 10, 기본값: 3(초)
5	**interval** *<INTERVAL>*	서버의 장애를 판단하기 위해 장애 감시 패킷을 서버로 전송하는 주기를 설정합니다. • *<INTERVAL>* 장애 감시 패킷 전송 주기. 설정 범위: 1 ~ 60, 기본값: 5(초) **참고:** 장애 감시 패킷의 전송 주기가 짧을수록 서버의 장애 여부를 정확하게 파악할 수 있지만, 장애 감시 패킷과 응답 패킷이 네트워크의 부하가 될 수 있으므로 네트워크 상태에 따라 적절한 값으로 설정하도록 합니다.
6	**retry** *<RETRY>*	장애 감시 패킷의 재전송 횟수를 설정합니다. • *<RETRY>* 장애 감시 패킷 재전송 횟수. 설정 범위: 0 ~ 5, 기본값: 3
7	**recover** *<RECOVER>*	서버가 다시 복구되었는지 판단하기 위해 추가로 장애 감시 패킷을 전송할 횟수를 설정합니다. 장애가 발생했던 서버에게 이 명령으로 설정한 횟수만큼 장애 감시 패킷을 보낸 후 응답이 계속 수신되면 해당 서버가 정상적으로 복구되었다고 판단하게 됩니다. • *<RECOVER>* 서버 복구 확인 위한 장애 감시 패킷 전송 횟수. 설정 범위: 0 ~ 5, 기본값: 0
8	**sip** *<SIP>* (선택 설정)	장애 감시 패킷의 출발지 주소로 사용될 IP 주소를 설정합니다. (이 값은 일반적인 부하 분산 서비스에서는 설정할 필요가 없습니다. 장애 감시 패킷의 출발지 주소를 특정한 주소로 사용해야 하는 경우에만 설정하면 됩니다.) • *<SIP>* 장애 감시 패킷의 출발지 IP 주소.

9	**tip** *<TIP>* (선택 설정)	장애 감시 패킷의 목적지 주소로 사용될 IP 주소를 설정합니다. (이 값은 일반적인 부하 분산 서비스에서는 설정할 필요가 없고 특별한 구성에서만 설정합니다. 예를 들어, 가상 IP 주소로 장애 감시 패킷을 전송해야 하는 DSR(Direct Server Return)과 같은 구성에서는 이 명령을 사용하여 전송하는 장애 감시 패킷의 목적지 IP 주소를 가상 IP 주소로 지정해야 합니다.) • *<TIP>* 장애 감시 패킷의 목적지 IP 주소.
10	**status {enable | disable}** (선택 설정)	장애 감시의 사용 여부를 지정합니다. • **enable** 장애 감시 활성화 (기본값) • **disable** 장애 감시 비활성화
11	**current**	장애 감시 설정 정보를 확인합니다.
12	**apply**	장애 감시 설정을 저장하고 시스템에 적용합니다.

참고: 정의한 장애 감시를 삭제하려면 <Configuration 모드>에서 **no health-check** *<ID>* 명령을 실행합니다.

참고: 지정한 장애 감시 종류에 따라 입력한 옵션값을 삭제하거나 기본값으로 변경하려면 <Health-check 설정 모드>에서 다음과 같이 **no <옵션 이름>** 명령을 사용합니다. 다음은 unexpect 옵션의 입력 값을 삭제하는 예입니다.

```
(config-health-check[1])# no unexpect
```

HTTP 장애 감시

장애 감시 방식을 'http'로 설정한 경우에는 <Health-Check 설정 모드>에서 다음과 같은 옵션을 설정할 수 있습니다.

명 령	설 명
uri *<URI>* (필수 설정)	실제 서버가 데이터를 읽어오도록 요청할 URI(파일의 경로)를 설정합니다. • *<URI>* URI 지정. 기본값: /
host *<HOST>*	HTTP 요청 헤더의 Host 필드에 입력할 문자열을 설정합니다. 지정하지 않는 경우 PAS-K는 실제 서버의 IP를 Host 필드에 입력합니다. • *<HOST>* Host 필드 입력 문자열. 일반적으로 서버의 도메인 이름 지정
user-agent *<USER-AGENT>*	HTTP 요청 헤더의 User-Agent 필드에 입력할 문자열을 설정합니다. • *<USER-AGENT>* User-Agent 필드 입력 문자열
status-code *<STATUS-CODE>*	실제 서버로부터 수신하기를 기대하는 HTTP 상태 코드의 종류를 입력합니다. • *<STATUS-CODE>* 설정 가능 상태 코드: 100-101, 200-206, 300-307, 400-417, 500-505 중에서 유효한 세 자리 정수. 복수의 상태 코드 추가 시 공백 없이 쉼표(,)로 구분하며, 연속되는 상태 코드는 대쉬(-)를 사용 (기본값: 200) **참고:** HTTP 상태 코드에 대한 정보는 RFC 2616에 정의되어 있습니다.
expect *<EXPECT>*	실제 서버로부터 수신하기를 기대하는 데이터를 설정합니다. • *<EXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.
unexpect *<UNEXPECT>*	실제 서버로부터 수신하면 안되는 데이터를 설정합니다. • *<UNEXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.
content-length *<CONTENT-LENGTH>*	HTTP content-length 헤더에 명시된 컨텐트(파일)의 크기를 설정합니다. 지정한 값과 일치하지 않는 경우 장애 감시에 실패한 것으로 간주합니다. • *<CONTENT-LENGTH>* 장애 감시를 수행할 컨텐트 파일의 크기 (설정 범위: 0 ~ 4294967295)

ICMP 장애 감시

장애 감시 방식을 'icmp'로 설정한 경우에는 <Health-Check 설정 모드>에서 실제 서버로 ICMP 패킷을 전송 한 후 ICMP 패킷 ID의 증가 여부를 지정할 수 있습니다.

명 령	설 명
increase-icmp-id {enable | disable}	ICMP 장애 감시 기능의 사용 여부를 지정합니다. • **enable** ICMP 패킷 ID를 증가시킴. • **disable** ICMP 패킷 ID를 증가시키지 않음. (기본값)

NTP 장애 감시

장애 감시 방식을 'ntp'로 설정한 경우에는 <Health-Check 설정 모드>에서 다음과 같은 옵션을 설정할 수 있습니다.

명 령	설 명
tolerance *<TOLERANCE>*	실제 서버로부터 받은 시간 정보와 PAS-K 사이의 시간 차이를 허용할 범위를 초단위로 설정합니다. 지정한 값 이상의 시간 차이가 있을 경우에는 실제 서버에 장애가 발생하였다고 판단합니다. • *<TOLERANCE>* 시간 차 허용 범위. 설정 범위: 1 ~ 4294967295(초)
update-delay *<UPDATE-DELAY>*	실제 서버가 시간 정보를 업데이트 하는 주기를 초단위로 입력합니다 실제 서버가 가장 최근에 시간 정보를 업데이트 한 이후로 경과된 시간이 지정한 주기보다 길면 실제 서버에 장애가 발생하였다고 판단합니다. • *<UPDATE-DELAY>* 시간 업데이트 주기. 설정 범위: 1 ~ 4294967295(초)

TCP 장애 감시

장애 감시 방식을 'tcp'로 설정한 경우에는 <Health-Check 설정 모드>에서 다음과 같은 옵션을 설정할 수 있습니다.

명 령	설 명
half-open {enable | disable}	TCP Half-open 옵션을 사용할 지의 여부를 선택합니다. • **enable** TCP Half-open 옵션 사용 • **disable** TCP Half-open 옵션 사용하지 않음 (기본값)
send *<SEND>*	TCP 연결이 생성되면 실제 서버로 전송할 데이터를 입력합니다. • *<SEND>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.
expect *<EXPECT>*	실제 서버로부터 수신하기를 기대하는 데이터를 설정합니다. • *<EXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.
unexpect *<UNEXPECT>*	실제 서버로부터 수신하면 안되는 데이터를 설정합니다. • *<UNEXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.

참고: send, expect, unexpect에 지정하는 옵션 값은 기본적으로는 문자열(아스키)이지만, 탈출문자(escape characters)를 사용함으로써 바이너리 데이터를 입력할 수도 있습니다. 탈출 문자의 사용법은 이 장의 [**장애 감시- 장애 감시 방법 – TCP 장애 감시**] 절을 참고하도록 합니다.

TFTP 장애 감시

장애 감시 방식을 'tftp'로 설정한 경우에는 <Health-Check 설정 모드>에서 다음과 같은 옵션을 설정할 수 있습니다.

명 령	설 명
filename *<FILENAME>* (필수 설정)	TFTP 서버에 접속하여 다운로드 할 파일의 이름을 입력합니다. • *<FILENAME>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다. 파일 이름 뒤에는 해당 파일의 확장자까지 입력해야 합니다.
expect *<EXPECT>*	실제 서버로부터 수신하기를 기대하는 데이터를 설정합니다. • *<EXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.
unexpect *<UNEXPECT>*	실제 서버로부터 수신하면 안되는 데이터를 설정합니다. • *<UNEXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.

참고: send, expect, unexpect에 지정하는 옵션 값은 기본적으로는 문자열(아스키)이지만, 탈출문자(escape characters)를 사용함으로써 바이너리 데이터를 입력할 수도 있습니다. 탈출 문자의 사용법은 이 장의 [**장애 감시- 장애 감시 방법 – TCP 장애 감시**] 절을 참고하도록 합니다.

UDP 장애 감시

장애 감시 방식을 'udp'로 설정한 경우에는 <Health-Check 설정 모드>에서 다음과 같은 옵션을 설정할 수 있습니다.

명 령	설 명
packets *<PACKETS>* (필수 설정)	반복해서 실제 서버로 전송할 UDP 패킷의 수를 설정합니다. • *<PACKETS>* UDP 패킷 수 설정. (설정 범위: 1 ~ 5, 기본값: 1)
send *<SEND>*	UDP 패킷에 담아 실제 서버로 전송할 데이터를 입력합니다. 지정하지 않는 경우 내용이 없는 UDP 패킷을 전송하게 됩니다. • *<SEND>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.
expect *<EXPECT>*	실제 서버로부터 수신하기를 기대하는 데이터를 설정합니다. • *<EXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.
unexpect *<UNEXPECT>*	실제 서버로부터 수신하면 안되는 데이터를 설정합니다. • *<UNEXPECT>* 아스키 문자열을 최대 128 글자까지 지정 가능하며, 문자열에 줄 바꿈을 삽입하려면 '₩r₩n'을 입력합니다.

참고: send, expect, unexpect에 지정하는 옵션 값은 기본적으로는 문자열(아스키)이지만, 탈출문자(escape characters)를 사용함으로써 바이너리 데이터를 입력할 수도 있습니다. 탈출 문자의 사용법은 이 장의 [**장애 감시- 장애 감시 방법 – TCP 장애 감시**] 절을 참고하도록 합니다.

스크립트 장애 감시

장애 감시 방식을 'script'로 설정한 경우에는 <Health-Check 설정 모드>에서 다음과 같은 순서로 스크립트 명령을 설정해야 합니다. 스크립트 명령은 지정한 인덱스에 따라 순서대로 실행되며, 하나의 장애 감시에는 최대 32개의 스크립트 명령을 설정할 수 있습니다.

첫번째로 실제 서버와 세션을 연결하기 위한 스크립트 명령과 프로토콜, 포트 번호를 설정합니다.

순서	명 령	설 명
1	**script** *<INDEX>*	<Health-check 설정 모드>에서 <Script 설정 모드>로 들어갑니다. • *<INDEX>* 스크립트 인덱스 지정. 값이 작을수록 해당 명령이 먼저 실행됩니다. 설정 범위: 1 ~ 32
2	**command open**	서버와 데이터를 송수신할 세션을 연결하도록 설정하고자 할 경우, command open 명령을 스크립트에 추가합니다. **참고:** 첫번 째 스크립트의 command는 반드시 open 이어야 합니다.
3	**protocol {tcp | ucp}**	세션을 연결할 때 사용할 프로토콜을 설정합니다.
4	**port** *<PORT>*	세션을 연결할 때 사용할 포트 번호를 설정합니다. • *<PORT>* 포트 번호. 설정 범위: 0 ~ 65535 **참고:** 다음은 일반적으로 각 프로토콜에서 사용하는 포트입니다. 포트 번호를 지정할 때 참고하도록 합니다. • FTP : 21 • HTTP : 80 • FTP : 21 • IMAP : 143 • SMTP : 25
5	**current**	스크립트 설정 정보를 확인합니다.
6	**apply**	세션 연결을 위한 스크립트 설정을 저장하고 시스템에 적용합니다.

두번째로 실제 서버로 송신하거나 수신할 데이터를 설정합니다. 송수신 데이터를 여러 개 지정하려는 경우에는 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**script** *<INDEX>*	<Health-check 설정 모드>에서 <Script 설정 모드>로 들어갑니다. • *<INDEX>* 스크립트 인덱스 지정. 값이 작을수록 해당 명령이 먼저 실행됩니다. 설정 범위: 1 ~ 32
2	**command {expect | expect-bin | send | send-bin}**	서버와 연결된 세션을 통해 데이터를 전송하려면 **send** 또는 **send-bin** 명령을 스크립트에 추가하고, 수신할 데이터를 지정하고자 하는 경우에는 **expect** 나 **expect-bin** 명령을 스크립트에 추가합니다. • **expect** 아스키 형태의 문자열을 수신 • **expect-bin** 바이너리 형태의 문자열을 수신 • **send** 아스키 문자열 전송 • **send-bin** 바이너리 문자열 전송
3	**data** *<DATA>*	2 번 과정에서 **send** 또는 **expect** 를 지정한 경우에는 송수신할 아스키 문자열을 스크립트에 추가합니다. • *<DATA>* 아스키 문자열을 최대 1024 글자까지 지정. 문자열에 줄 바꿈을 삽입하려면 '\r\n'을 입력. 문자열의 시작과 끝 지점에 큰 따옴표(")를 입력해야 합니다. 2 번 과정에서 **send-bin** 또는 **expect-bin** 을 지정한 경우에는 송수신할 바이너리 문자열을 스크립트에 추가합니다. • *<DATA>* 바이너리 문자열을 16 진수 형태로 최대 2048 글자까지 지정. 문자열의 시작과 끝 지점에 큰 따옴표(")를 입력해야 합니다.
4	**current**	스크립트 설정 정보를 확인합니다.
5	**apply**	스크립트 설정을 저장하고 시스템에 적용합니다.

마지막으로 실제 서버와의 세션을 해제하기 위한 스크립트 명령을 설정합니다

순서	명 령	설 명
1	**script** *<INDEX>*	<Health-check 설정 모드>에서 <Script 설정 모드>로 들어갑니다. • *<INDEX>* 스크립트 인덱스 지정. 값이 작을수록 해당 명령이 먼저 실행됩니다. 설정 범위: 1 ~ 32
2	**command close**	스크립트 장애 감시를 위한 세션을 해제하기 위해 close 명령을 스크립트에 추가합니다.
3	**current**	스크립트 설정 정보를 확인합니다.
4	**apply**	세션 해제를 위한 스크립트 설정을 저장하고 시스템에 적용합니다.

참고: **command close** 명령을 실행하지 않아 세션이 해제되지 않은 상태에서 **command open** 명령을 실행하면, 이전에 연결되었던 세션이 자동 해제되고 새로운 세션을 연결합니다.

참고: 설정한 스크립트를 삭제하려면 <Health-check 설정 모드>에서 **no script** *<INDEX>* 명령을 사용합니다.

RADIUS 서버 장애 감시

실제 서버가 RADIUS 인증 서버나 과금 서버인 경우에는 서버의 장애 감시 방법으로 RADIUS 장애 감시를 사용할 수 있습니다. RADIUS 장애 감시를 위해서는 장애 감시를 할 때 사용할 사용자 이름과 암호, 비밀 키를 PAS-K에 설정해야 합니다. 다음은 <Health-Check 설정 모드> RADIUS 서버 장애 감시를 위해 PAS-K가 RADIUS 서버로 접속하기 위해 필요한 값들을 설정하는 방법입니다.

순서	명 령	설 명
1	**radius-auth-name** *<RADIUS-AUTH-NAME>*	인증용 RADIUS 서버로 접속할 때 사용할 사용자 ID를 지정합니다.
2	**radius-auth-passwd** *<RADIUS-AUTH-PASSWD>*	인증용 RADIUS 서버로 접속할 때 사용할 암호를 지정합니다.
3	**radius-auth-secret** *<RADIUS-AUTH-SECRET>*	인증용 RADIUS 서버로 접속할 때 사용할 비밀 키를 지정합니다.
4	**radius-acct-secret** *<RADIUS-ACCT-SECRET>*	과금용 RADIUS 서버로 접속할 때 사용할 비밀 키를 지정합니다.

설정 정보 보기

장애 감시 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show health-check** 명령을 사용합니다. 특정 장애 감시 설정에 대한 정보를 확인하려면, **show health-check** 명령과 함께 장애 감시 ID를 입력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

참고: <Privileged 모드> 또는 <Configuration 모드>에서 **show map** 명령을 사용하면, 장애 감시를 사용하는 실제 서버와 부하 분산 서비스를 확인할 수 있습니다.

실제 서버 설정

이 절에서는 CLI에서 각 부하 분산 서비스를 통해 트래픽을 분산 시킬 실제 서버를 설정하는 방법에 대해 살펴봅니다. 실제 서버는 부하 분산 서비스와는 독립적으로 설정하며, 하나의 실제 서버를 서로 다른 부하 분산 서비스에 적용할 수 있습니다.

CLI에서 설정하기

실제 서버 설정

PAS-K에는 최대 2048개의 실제 서버를 등록할 수 있습니다. 여러 개의 실제 서버를 설정하는 경우에는 <Configuration 설정 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**real** *<ID>*	실제 서버를 정의합니다. • *<ID>* 실제 서버의 ID. 설정 범위: 1 ~ 2048
2	**name** *<NAME>*	실제 서버의 이름을 설정합니다 • *<NAME>* 알파벳과 숫자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용
3	**rip** *<RIP>* (필수 설정)	실제 서버의 IP 주소를 설정합니다. • *<RIP>* 실제 서버의 IPv4 주소 또는 IPv6 주소 설정
4	**rport** *<RPORT>*	실제 서버에서 사용할 TCP 포트의 번호를 설정합니다 • *<PORT>* TCP 포트 번호. 설정 범위: 1 ~ 65535
5	**mac** *<MAC>*	실제 서버의 MAC 주소를 설정합니다. • *<MAC>* 실제 서버의 MAC 주소 설정 (6 자리의 16 진수 형식으로 입력) **참고**: 방화벽/VLN 부하분산, L4 캐시 서버 부하 분산, 게이트웨이 부하분산 서비스의 경우, 같은 IP의 실제 서버가 존재하거나, 실제 서버가 네트워크에 연결되어 있지 않는 경우에는 반드시 MAC 주소를 설정해야 합니다. MAC 주소를 설정하지 않는 경우 성능이 저하되는 문제가 발생합니다.
6	**interface** *<INTERFACE>*	실제 서버와 연결되어 있는 PAS-K의 VLAN 인터페이스를 설정합니다 • *<INTERFACE>* VLAN 인터페이스 설정.
7	**priority** *<PRIORITY>*	실제 서버의 우선순위를 설정합니다. 실제 서버의 우선순위는 서비스의 부하 분산 방식이 액티브-백업(ab)일 경우, 실제 서버를 선택하는 기준으로 사용됩니다. 우선순위 값이 클수록 우선순위가 높습니다. • *<PRIORITY>* 실제 서버의 우선순위. 설정 범위: 0 ~ 255, 기본값: 0
8	**weight** *<WEIGHT>*	실제 서버에 할당할 가중치를 설정합니다. 실제 서버의 가중치는 서비스의 부하 분산 방식이 wlc(가중치 최소 연결)이나 wrr(가중치 라운드 로빈)일 경우 실제 서버를 선택하는 기준으로 사용됩니다. • *<WEIGHT>* 실제 서버의 가중치. 설정 범위: 1 ~ 100, 기본값: 1
9	**graceful-shutdown {enable | disable}**	실제 서버에 graceful shutdown 기능의 사용 여부를 지정합니다. • **enable** graceful shutdown 기능 활성화 • **disable** graceful shutdown 기능 비활성화 (기본값)
10	**max-connection** *<MAX-CONNECTION>*	실제 서버를 통해 맺어질 수 있는 세션 수를 제한하려면 실제 서버의 최대 세션 개수를 설정합니다. 실제 서버에 맺어진 세션의 수가 최대 세션 개수에 도달하면 서비스는 더 이상 해당 서버로는 부하 분산을 하지 않습니다. '0'을 지정하면 세션 개수를 제한하지 않습니다. • *<CONNECTION>* 실제 서버의 최대 세션 개수. 설정 범위: 0 ~ 10,000,000, 기본값: 0

11	**health-check** *<ID>*	실제 서버의 장애를 감시하는 장애 감시의 ID를 지정합니다. • *<ID>* 실제 서버의 장애 감시 ID. 하나의 실제 서버에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 두 개 이상의 장애 감시 설정을 사용하는 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 가용한 것으로 간주합니다. 그 중 하나의 장애 감시라도 결과가 실패이면 실제 서버는 사용할 수 없는 상태로 판단되어 부하 분산 서비스에서 제외됩니다.
참고: 12 ~ 16번 과정은 L7 부하 분산 서비스에 적용할 실제 서버를 위한 설정입니다. 설정 중인 실제 서버를 L4 부하 분산 서비스에 적용하려는 경우에는 설정하지 않아도 됩니다.		
12	**pool-size** *<POOL-SIZE>*	실제 서버 별로 커넥션을 저장할 최대 개수를 설정합니다. 실제 서버에 저장된 커넥션의 수가 최대 커넥션 개수에 도달하면 더 이상 커넥션을 재사용하지 않습니다. • *<POOL-SIZE>* 커넥션 최대 저장 개수. 설정 범위: 1 ~ 65535, 기본값: 10,000 **참고:** 고급 L7 부하 분산 서비스에서는 해당 설정이 적용되지 않습니다.
13	**pool-age** *<POOL-AGE>*	풀에 저장될 커넥션의 유지 시간을 설정합니다. 설정한 시간이 지나게 되면 커넥션은 삭제됩니다. • *<POOL-AGE>* 커넥션 유지 시간. 설정 범위: 1 ~ 86400(초), 기본값: 3600(초) **참고:** 고급 L7 부하 분산 서비스에서는 해당 설정이 적용되지 않습니다.
14	**pool-reuse** *<POOL-REUSE>*	풀에 저장될 커넥션의 재사용 횟수를 설정합니다. 지정한 횟수만큼 커넥션을 재사용한 후에 삭제합니다. • *<POOL-REUSE>* 커넥션 재 사용 횟수. 설정 범위: 1 ~ 65535. 기본값: 100 **참고:** 고급 L7 부하 분산 서비스에서는 해당 설정이 적용되지 않습니다.
15	**pool-srcmask** *<POOL-SRCMASK>*	커넥션을 재사용하는 조건으로 서브넷 마스크의 비트 수를 비교합니다. IP 주소가 일치하면 커넥션을 재사용 합니다. • *<POOL-SRCMASK>* 커넥션 재사용 조건으로 비교할 서브넷 마스크 설정. 서브넷 마스크가 '32'이면 IP 주소 전체가 같아야 커넥션을 재사용하고, '0'이면 모든 IP 주소에 대해서 재사용. (설정 범위: 0 ~ 32(bit). 기본값: 32(bit)) **참고:** 고급 L7 부하 분산 서비스에서는 해당 설정이 적용되지 않습니다.
16	**src-natip** *<SRC-NATIP>*	지연 바인딩 시 Source NAT 를 적용할 IP 주소를 설정합니다. 지연 바인딩 시 Source NAT하지 않으려면 IP 주소를 0.0.0.0으로 지정하거나 **no src-natip** 명령을 사용합니다. • *<SRC-NATIP>* IP 주소 설정. 최대 64 개의 Source NAT IP 주소를 지정 가능. **주의:** Source NAT를 적용할 IP 주소는 실제 서버와 동일한 IP 대역을 사용할 수 없습니다.
17	**backup** *<BACKUP>*	실제 서버가 더 이상 가용하지 않은 상태(서버가 다운되거나, 실제 서버가 처리 중인 세션의 수가 최대 세션 개수에 도달한 경우, 혹은 실제 서버와의 연결이 끊어진 경우 등) 가 되었을 때, 대신 사용할 백업 서버를 설정합니다. • *<BACKUP>* 백업 서버 ID. (반드시 동일 게이트웨이 부하 분산 서비스 내에 정의되어 있는 실제 서버 ID 입력.) **참고:** 실제 서버가 여러 서비스에서 사용 중일 경우에는 백업 서버를 설정할 수 없습니다.
18	**sp-filter** *<SP-FILTER>*	부하 분산 방식으로 '정적 근접(Static Proximity)'를 사용하는 경우에는 실제 서버에 적용할 정적 근접 필터를 지정합니다. • *<SP-FILTER>* 정적 필터 ID. (반드시 이미 설정되어 있는 정적 근접 필터 ID 를 입력해야 하며, 여러 개의 필터를 지정하는 경우에는 ','로 필터의 ID 를 구분.) **참고:** 정적 근접 필터를 설정하는 방법은 다음 절인 '정적 필터' 절을 참고하도록 합니다. **참고:** 해당 설정은 실제 서버가 글로벌 서버 부하 분산, 게이트웨이 부하 분산 서비스에 적용된 경우에만 유효합니다.

19	**status {enable | disable}** (선택 설정)	실제 서버의 사용 여부를 지정합니다. • **enable** 실제 서버 활성화 • **disable** 실제 서버 비활성화 (기본값)
20	**current**	실제 서버의 설정 정보를 확인합니다.
21	**apply**	실제 서버를 저장하고 시스템에 적용합니다.

참고: 정의한 실제 서버를 삭제하려면 <Configuration 모드>에서 **no real** *<ID>* 명령을 사용합니다.

NAT 규칙 설정

게이트웨이 부하 분산 서비스를 적용할 실제 서버는 사설 IP 주소와 공인 IP 주소를 변환하는 NAT 규칙을 정의해야 합니다. NAT 규칙의 유형에는 Source NAT와 One-to-One NAT가 있습니다. 하나의 실제 서버에는 최대 16개의 NAT 규칙을 정의할 수 있으므로, 여러 개의 NAT 규칙을 설정하는 경우에는 <Real 설정 모드>에서 다음 과정을 반복하면 됩니다.

참고: NAT 규칙은 실제 서버가 게이트웨이 부하 분산 서비스에 설정된 경우에만 동작합니다.

순서	명 령	설 명
1	**nat** *<ID>*	<NAT 설정 모드>로 들어갑니다. • *<ID>* NAT 규칙을 구분할 때 사용할 ID. 설정 범위: 1 ~ 16
2	**type {one-to-one-nat | source-nat}**	NAT 규칙의 종류를 설정합니다. 기본값: source-nat
3	**priority** *<PRIORITY>*	NAT 규칙의 우선순위를 설정합니다. 우선순위는 NAT 규칙을 트래픽에 적용할 순서를 결정할 때 사용됩니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* NAT 규칙 우선순위. 설정 범위: 1 ~ 256, 기본값: 1
4~9번 과정은 2번 과정에서 지정한 NAT 규칙의 종류에 따라 설정 과정이 달라집니다. NAT 규칙 종류에 맞는 과정을 수행한 후 10번 과정부터 수행하면 됩니다. • Source NAT: 4~7번 과정 • One-to-One NAT: 8~9번 과정		
4	**sip** *<SIP>* (Source NAT인 경우에만 설정)	특정한 네트워크에서 전송된 트래픽에만 NAT 규칙을 적용할 경우, 해당 패킷의 출발지 IP 주소와 넷 마스크 비트 수를 입력합니다. 기존에 설정된 출발지 조건을 삭제하려면 0.0.0.0/0을 입력하면 됩니다. 출발지 조건을 삭제하면 NAT 규칙은 트래픽의 출발지에 관계없이 적용됩니다.
5	**dip** *<DIP>* (Source NAT인 경우에만 설정)	특정한 네트워크로 향하는 트래픽에만 NAT 규칙을 적용할 경우, 해당 패킷의 목적지 IP 주소와 넷 마스크 비트 수를 입력합니다. 기존에 설정된 목적지 조건을 삭제하려면 0.0.0.0/0을 입력하면 됩니다. 목적지 조건을 삭제하면 NAT 규칙은 트래픽의 목적지에 관계없이 적용됩니다.
6	**protocol {icmp | tcp | udp | all}** (Source NAT인 경우에만 설정)	특정한 프로토콜의 트래픽에만 NAT 규칙을 적용할 경우, 해당 프로토콜을 설정합니다. ICMP 패킷에만 NAT 규칙을 적용하려는 경우에는 'icmp' 항목을, TCP 패킷이나 UDP 패킷에만 적용하려면 경우에는 각각 'tcp', 'udp' 항목을 지정하면 됩니다. 기존에 설정된 프로토콜 조건을 삭제하려면 'all'을 설정합니다. 프로토콜 조건을 삭제하면 NAT 규칙은 어떤 프로토콜의 트래픽인지 관계없이 적용됩니다. 기본값: all
7	**natip** *<NATIP>* (Source NAT인 경우에만 설정)	4~6번 과정에서 지정한 조건을 만족하는 트래픽의 출발지 주소로 변환할 NAT IP 주소를 설정합니다.
8	**external-ip** *<EXTERNAL-IP>* (One-to-One NAT인 경우에만 설정)	외부에서 수신된 트래픽 중에서 NAT 규칙을 적용할 트래픽의 목적지 IP 주소(공인 IP 주소)를 설정합니다. 이 IP 주소는 NAT 규칙을 정의하는 실제 서버와 연결된 라우터에 할당된 주소이어야 합니다.
9	**internal-ip** *<INTERNAL-IP>* (One-to-One NAT인 경우에만 설정)	8번 과정에서 지정한 공인 IP 주소를 변환할 때 사용할 사설 IP 주소를 설정합니다. 이 IP 주소는 PAS-K에 연결된 내부 네트워크의 IP 대역이어야 합니다.
10	**status {enable | disable}** (선택 설정)	NAT 규칙의 사용 여부를 지정합니다. • **enable** NAT 규칙 활성화 (기본값)

		• **disable** NAT 규칙 비활성화
11	**current**	NAT 규칙의 설정 정보를 확인합니다.
12	**apply**	NAT 규칙을 저장하고 시스템에 적용합니다.

참고: 정의한 NAT 규칙을 삭제하려면 <Real 설정 모드>에서 **no nat** <*ID*> 명령을 사용합니다.

설정 정보 보기

실제 서버 설정 정보를 확인하려면 <Privileged 모드> 또는 <Configuration 모드>에서 **show real** 명령을 사용합니다. 특정 실제 서버에 대한 설정 정보를 확인하려면, **show real** 명령과 함께 실제 서버의 ID를 입력합니다.

NAT 규칙 설정 정보를 확인하려면 <Real 설정 모드>에서 **show nat** 명령을 사용합니다. 특정 NAT 규칙에 대한 설정 정보를 확인하려면, **show nat** 명령과 함께 NAT 규칙의 ID를 입력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

참고: <Privileged 모드> 또는 <Configuration 모드>에서 **show map** 명령을 사용하면, 실제 서버를 사용하는 부하 분산 서비스를 확인할 수 있습니다.

정적 필터

게이트웨이 부하 분산 서비스와 글로벌 서버 부하 분산 서비스에서는 부하 분산 방식으로 '정적 근접(Static Proximity)'을 선택할 수 있습니다. 정적 근접을 선택한 경우에는 이 방식에서 사용할 필터를 정의해야 합니다. 필터는 각 부하 분산 서비스 별로 정의하지 않고, 여러 부하 분산 서비스에서 공용으로 사용할 수 있습니다.

CLI에서 설정하기

이 절에서는 CLI 명령을 사용하여 정적 필터를 설정하는 방법에 대해 살펴봅니다.

정적 필터 설정

다음은 하나의 정적 필터를 설정하는 과정입니다. PAS-K에는 정적 필터를 최대 2048개까지 정의할 수 있으므로, 여러 개의 정적 필터를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**sp-filter** *<ID>*	<SP 설정 모드>로 들어갑니다. • *<ID>* 정적 필터의 ID. (설정 범위: 1 ~ 2048)
2	**sip** *<SIP>*	필터링 조건으로 사용할 출발지 IP 주소와 넷 마스크 비트 수를 입력합니다.
3	**current**	정적 필터의 설정 정보를 확인합니다.
4	**apply**	정적 필터를 저장하고 시스템에 적용합니다.

참고: 설정한 정적 필터를 삭제하려면 <Configuration 모드>에서 **no sp-filter** *<ID>* 명령을 사용하면 됩니다.

참고: 설정한 정적 필터를 확인하려면 <Privileged 모드> 또는 <Configuration 모드>에서 **show filter** [*<id>*] 명령을 사용하면 됩니다.

HTTP 압축 규칙 설정

이 절에서는 CLI에서 고급 L7 부하 분산 서비스에서 사용할 HTTP 압축 규칙을 설정하는 방법에 대해 살펴봅니다.

CLI에서 설정하기

PAS-K에는 최대 256개의 HTTP 압축 규칙을 등록할 수 있습니다. 여러 개의 HTTP 압축 규칙을 설정하는 경우에는 <Configuration 설정 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**layer7 compression** *<ID>*	HTTP 압축 규칙을 정의합니다. • *<ID>* HTTP 압축 규칙의 ID. 설정 범위: 1 ~ 256
2	**level** *<LEVEL>*	압축 레벨을 설정합니다. 레벨이 낮을수록 압축률은 줄어들고, 응답 속도는 빨라집니다. • *<LEVEL>* 압축 레벨. 설정 범위: 1 ~ 9, 기본값: 1 **참고**: 설정한 압축 레벨을 기본값으로 변경하려면, **no level** 명령을 사용합니다.
3	**min-length** *<MIN-LENGTH>*	압축을 수행할 패킷의 최소 길이를 설정합니다 • *<MIN-LENGTH>* 패킷 최소 길이. 설정 범위: 0 ~ 4294967295, 기본값: 0 **참고**: 설정한 패킷 최소 길이를 기본값으로 변경하려면, **no min-length** 명령을 사용합니다.
4	**content-type** *<CONTENT-TYPE>*	압축할 컨텐트 유형을 설정합니다 • *<COTENT-TYPE>* 압축할 컨텐트를 MIME Type 으로 지정. 여러 개의 컨텐트를 지정하는 경우에는 각 컨텐트 유형을 ','로 구분하여 입력. (기본값: text/html) **참고**: 설정한 컨텐트 유형을 삭제하려면, **no content-type** *<CONTENT-TYPE>* 명령을 사용합니다.
5	**status** {**enable** | **disable**}	HTTP 압축 규칙의 사용 여부를 지정합니다. • **enable** HTTP 압축 규칙 활성화 (기본값) • **disable** HTTP 압축 규칙 비활성화
6	**current**	HTTP 압축 규칙의 설정 정보를 확인합니다.
7	**apply**	HTTP 압축 규칙을 저장합니다.

참고: 정의한 HTTP 압축 규칙을 삭제하려면 <Configuration 모드>에서 **no layer7 compression** *<ID>* 명령을 사용합니다.

설정 정보 보기

HTTP 압축 규칙 설정 정보를 확인하려면 <Privileged 모드> 또는 <Configuration 모드>에서 **show layer7 compression** 명령을 사용합니다. 특정 HTTP 압축 규칙에 대한 설정 정보를 확인하려면, **show layer7 compression** 명령과 함께 압축 규칙 ID를 입력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

캐싱 규칙 설정

이 절에서는 CLI에서 고급 L7 서버 부하 분산 서비스에서 사용할 캐싱 규칙을 설정하는 방법에 대해 살펴봅니다.

CLI에서 설정하기

PAS-K에는 최대 256개의 캐싱 규칙을 등록할 수 있습니다. 여러 개의 캐싱 규칙을 설정하는 경우에는 <Configuration 설정 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**layer7 cache** *<ID>*	캐싱 규칙을 정의합니다. • *<ID>* 캐싱 규칙의 ID. 설정 범위: 1 ~ 256
2	**size {16m | 64m | 256m}**	캐시 용량을 설정합니다. (단위: MB) • **16m** 캐시 용량 16 MB 설정. (기본값) • **64m** 캐시 용량 64 MB 설정. • **256m** 캐시 용량 256 MB 설정. **참고**: 설정한 캐시 용량을 기본값으로 변경하려면, **no size** 명령을 사용합니다.
3	**max-age** *<MAX-AGE>*	캐시 유지 시간을 설정합니다 • *<MAX-AGE>* 캐시 유지 시간 설정 (설정 범위: 0 ~ 65535(초)) **참고**: 캐시 유지 시간을 삭제하려면, **no max-age** 명령을 사용합니다.
4	**min-use** *<MIN-USE>*	캐시 시작 요청 수를 설정합니다 • *<MIN-USE>* 캐시 시작 요청 수 설정 (설정 범위: 1 ~ 65535. 기본값: 1) **참고**: 캐시 시작 요청 수를 기본값으로 변경하려면, **no min-use** 명령을 사용합니다.
5	**ignore-heaader {both | cache-control | expires | none}**	캐시 거부 헤더 무시 여부를 설정합니다. • **both** Expires, Cache-Contol 헤더를 모두 무시 • **cache-control** Cache-Contol 헤더만 무시 • **expires** Expires 헤더만 무시 • **none** 해당 요청에 대해 캐싱을 수행하지 않음(기본값)
6	**method {GET | HEAD | POST}** (선택 설정)	캐시를 수행할 요청 방식을 설정합니다. 기본값: GET, HEAD **참고**: 요청 방식을 삭제하려면, **no method {GET | HEAD | POST}** 명령을 사용합니다.
7	**status {enable | disable}**	캐싱 규칙의 사용 여부를 지정합니다. • **enable** 캐싱 규칙 활성화 (기본값) • **disable** 캐싱 규칙 비활성화
8	**current**	캐싱 규칙의 설정 정보를 확인합니다.
9	**apply**	캐싱 규칙을 저장합니다.

참고: 정의한 캐싱 규칙을 삭제하려면 <Configuration 모드>에서 **no layer7 cache** *<ID>* 명령을 사용합니다.

설정 정보 보기

캐싱 규칙 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show layer7 cache** 명령을 사용합니다. 특정 캐싱 규칙에 대한 설정 정보를 확인하려면, **show layer7 cache** 명령과 함께 캐싱 규칙 ID를 입력합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

SSL 가속 설정

이 절에서는 CLI에서 고급 L7 부하 분산 서비스에서 사용할 SSL 가속 기능을 설정하는 방법에 대해 살펴봅니다.

CLI에서 설정하기

CLI 명령을 사용하여 SSL 가속 기능을 설절하는 과정은 다음과 같습니다.

1. 비밀 키 설정
2. 인증 요청서 설정
3. 인증서 설정
4. 클라이언트 인증서 설정
5. 프로필 설정

비밀 키 설정

비밀 키 생성하기

SSL 가속을 위한 비밀 키를 생성하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**ssl key** *<NAME>*	<SSL Key 설정 모드>로 들어갑니다. • *<NAME>* 비밀 키 이름. 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 253 글자까지 지정. 첫 글자는 반드시 알파벳 또는 숫자 사용.
2	**mode generate**	비밀 키 생성 모드를 새로운 비밀 키를 생성하는 generate로 설정합니다.
3	**type rsa**	비밀 키의 종류를 설정합니다. PAS-K는 RSA 방식의 비밀 키를 지원합니다.
4	**length** {**1024** | **2048** | **4096**}	비밀 키의 크기를 설정합니다. 지정할 수 있는 키의 크기는 1024bits, 2048bits, 4096bits가 있습니다. 키의 크기가 클수록 보안성이 뛰어나지만 그만큼 성능이 낮아지게 되므로, 네트워크와 클라이언트, 서버의 특성 등으로 고려하여 적절한 크기로 지정하도록 합니다. (기본값: 1024bits)
5	**encryption** {**aes128** | **aes196** | **aes256** | **des** | **des3** | **no**}	비밀 키를 암호화할 알고리즘을 설정합니다. 암호화하지 않는 경우에는 'no'로 지정하면 됩니다(기본값: no). **주의:** 암호화되지 않은 비밀 키가 유출되면 인증서가 위조될 가능성이 있으므로 암호화 알고리즘을 지정하기를 권장합니다.
6	**passphrase** *<PASSPHRASE>*	암호화 시 사용될 암호를 입력합니다. 타인이 짐작하기 힘들도록 가급적 긴 문장을 사용하는 것이 좋습니다. 암호를 분실하면 알아내거나 수정할 수 없으므로 반드시 따로 기록을 해두어야 합니다. • *<PASSPHRASE>* 암호 입력. 알파벳, 숫자, 특수문자 사용. (설정 범위: 5 ~ 20)
7	**current**	설정한 비밀 키의 설정 정보를 확인합니다.
8	**apply**	비밀 키 파일을 생성합니다.

참고: 비밀 키를 삭제하려면 <Configuration 모드>에서 **no ssl key** *<NAME>* 명령을 사용합니다.

비밀 키 가져오기

인증 기관으로부터 발급받은 비밀 키를 PAS-K에 등록하려면, 비밀 키 파일을 TFTP 서버에 저장한 후 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**ssl key** *<NAME>*	<SSL Key 설정 모드>로 들어갑니다. • *<NAME>* 비밀 키 이름. 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 253 글자까지 지정. 첫 글자는 반드시 알파벳 또는 숫자 사용.
2	**mode import**	비밀 키 생성 모드를 다운로드한 비밀 키를 등록하는 하는 import로 설정합니다.
3	**import-path** *<IMPORT-PATH>*	TFTP 서버에 저장되어 있는 비밀 키를 PAS-K로 다운로드합니다. • *<IMPORT-PATH>* TFTP 서버 IP 주소와 파일 이름을 다음과 같은 형식으로 입력 <SERVER-IP>:<FILE-NAME>
4	**passphrase** *<PASSPHRASE>*	암호화 시 사용될 암호를 입력합니다. • *<PASSPHRASE>* 암호 입력. 알파벳, 숫자, 특수문자 사용. (설정 범위: 5 ~ 20)
5	**current**	다운로드한 비밀 키 파일을 확인합니다.
6	**apply**	다운로드한 비밀 키를 PAS-K에 저장하고 등록합니다.

비밀 키 내보내기

PAS-K에 등록된 비밀 키는 TFTP 서버로 전송할 수 있습니다. 내부에서 사용하는 여러 장비 간 같은 비밀 키를 사용하고자 할 경우에는 비밀 키를 TFTP 서버를 통해 사용자 PC로 다운로드하여 여러 장비에 적용할 수 있습니다. PAS-K에 등록된 비밀 키를 TFTP 서버로 업로드하려면, <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**ssl key** *<NAME>*	<SSL Key 설정 모드>로 들어갑니다. • *<NAME>* 비밀 키 이름. 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 253 글자까지 지정. 첫 글자는 반드시 알파벳 또는 숫자 사용.
2	**export** *<SERVER-IP>* *<FILE-NAME>*	PAS-K에 저장되어 있는 비밀 키를 TFTP 서버로 업로드합니다. • *<SERVER-IP>* TFTP 서버 IP 주소 • *<FILE-NAME>* TFTP 서버 저장 시 사용할 파일 이름

인증 요청서 설정

인증 요청서 생성하기

인증 기관에 공인 인증서를 신청하려는 경우에는 인증 기관에 보낼 인증 요청서인 CSR을 생성해야 합니다. CSR을 생성 하려면, <Certificate 설정 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**ssl certificate** *<NAME>*	<Certificate 설정 모드>로 들어갑니다. • *<NAME>* 인증 요청서 이름. 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 253 글자까지 지정. 첫 글자는 반드시 알파벳 또는 숫자 사용.
2	**mode generate**	인증 요청서 생성 모드를 새로운 인증 요청서를 생성하는 generate로 설정합니다.
3	**cname** *<CNAME>*	인증서에 입력할 이름을 설정합니다 • *<CNAME>* 일반적으로 www.piolink.com나 *.piolink.com과 같은 도메인 이름을 인증서의 이름으로 설정합니다. 접속하려는 도메인 이름이 인증서의 이름과 다르면 웹 브라우저에서 피싱 (Phishing)으로 의심하여 경고 메시지를 출력하므로 정확한 도메인 이름을 입력하도록 합니다. (설정 범위: 0 ~ 64자) **참고:** 와일드 카드(*)가 포함된 도메인에 대한 인증서의 발급 여부는 인증기관마다 다르므로 먼저 인증 기관에 문의하도록 합니다.
4	**country** *<COUNTRY>*	국가 이름을 입력합니다. • *<COUNTRY>* 해당 국가의 두 자리(2-byte) 문자 코드 입력. (기본값: KR)
5	**state** *<STATE>*	지역(시/도)을 설정합니다. • *<STATE>* 지역 이름 입력. (설정 범위: 0 ~ 16자, 기본값: Seoul)
6	**locality** *<LOCALITY>*	도시(구/군) 이름을 입력합니다. • *<LOCALITY>* 도시 이름 입력. (설정 범위: 0 ~ 32자, 기본값: None)
7	**organization** *<ORGANIZATION>*	조직이나 회사 이름을 입력합니다. • *<ORGANIZATION>* 조직 또는 회사 이름 입력. (설정 범위: 0 ~ 32자,기본값: None)
8	**organization-unit** *<ORGANIZATION-UNIT>*	조직이나 회사의 부서 이름을 입력합니다. • *<ORGANIZATION-UNIT>* 조직 또는 회사의 부서 이름 입력. (설정 범위: 0 ~ 32자,기본값: None)
9	**email** *<EMAIL>*	웹 마스터 또는 시스템 관리자의 이메일 주소를 입력합니다. • *<EMAIL>* 이메일 주소 입력. (설정 범위: 0 ~ 64자,기본값: None)
10	**expiration** *<EXPIRATION>*	신청할 인증서의 유효 기간을 입력합니다. • *<EXPIRATION>* 인증서 유효시간 설정. (설정 범위: 1 ~ 10000 (일), 기본값: 365 (일))
11	**key** *<KEY>*	인증 요청서에 포함할 비밀 키를 지정합니다. • *<NAME>* 비밀 키 이름. (설정 범위: 5 ~ 20자)
12	**current**	설정한 인증 요청서의 설정 정보를 확인합니다.
13	**apply**	설정한 인증 요청서를 생성합니다.

참고: 생성한 인증 요청서는 자체 서명 인증서로도 사용할 수 있습니다. 자체 서명 인증서는 인증기관에서 발급된 공인 인증서 대신 회사 내부에서 테스트나 기타 다른 용도로 이용할 수 있습니다. 인증요청서를 자체 서명 인증서로 사용하기 위해 별도의 작업을 수행할 필요는 없습니다.

참고: 인증 요청서를 삭제하려면 <Configuration 모드>에서 **no ssl certificate** *<NAME>* 명령을 사용합니다.

인증 요청서 내보내기

인증 기관에 인증서를 신청하기 위해 생성한 인증 요청서를 TFTP 서버로 업로드하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

순서	명 령	설 명
1	**ssl certificate** *<NAME>*	<Certificate 설정 모드>로 들어갑니다. *<NAME>* 인증 요청서 이름.
2	**export-csr** *<SERVER-IP>* *<FILE-NAME>*	PAS-K에 저장되어 있는 인증 요청서를 TFTP 서버로 업로드합니다. • *<SERVER-IP>* TFTP 서버 IP 주소 • *<FILE-NAME>* TFTP 서버 저장 시 사용할 파일 이름

인증서 설정

인증서 가져오기

인증 기관으로부터 발급받은 인증서를 PAS-K에 등록하려면, 인증서 파일을 TFTP 서버에 저장한 후 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**ssl certificate** *<NAME>*	<Certificate 설정 모드>로 들어갑니다. • *<NAME>* 인증 요청서 이름.
2	**mode import**	인증서 생성 모드를 다운로드한 인증서를 등록하는 import로 설정합니다.
3	**import-path** *<IMPORT-PATH>*	TFTP 서버에 저장되어 있는 인증서를 PAS-K로 다운로드합니다. • *<IMPORT-PATH>* TFTP 서버 IP 주소와 파일 이름을 다음과 같은 형식으로 입력 <SERVER-IP>:<FILE-NAME>
4	**key** *<KEY>*	인증서에 포함할 비밀 키를 지정합니다. • *<KEY>* 비밀 키 이름.
5	**current**	다운로드한 인증서 파일을 확인합니다.
6	**apply**	다운로드한 인증서를 PAS-K에 저장하고 등록합니다.

참고: 인증서를 삭제하려면 <Configuration 모드>에서 **no ssl certificate** *<NAME>* 명령을 사용합니다.

인증서 내보내기

PAS-K에 등록된 인증서를 TFTP 서버로 업로드하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

순서	명 령	설 명
1	**ssl certificate** *<NAME>*	<Certificate 설정 모드>로 들어갑니다. • *<NAME>* 인증서 이름.
2	**export-crt** *<SERVER-IP>* *<FILE-NAME>*	PAS-K에 저장되어 있는 인증서를 TFTP 서버로 업로드합니다. • *<SERVER-IP>* TFTP 서버 IP 주소 • *<FILE-NAME>* TFTP 서버 저장 시 사용할 파일 이름

클라이언트 인증서 설정

클라이언트 인증서 가져오기

클라이언트의 인증서를 검증하기 위해서는 PAS-K에 클라이언트 인증서를 등록해야 합니다. PAS-K에는 최대 256개의 클라이언트의 인증서 등록할 수 있습니다. 여러 개의 클라이언트의 인증서 설정하는 경우에는 <Configuration 설정 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**ssl client-authentication** *<ID>*	<클라이언트 인증서 설정 모드>로 들어갑니다. • *<ID>* 클라이언트 인증서의 ID. 설정 범위: 1 ~ 256
2	**mode {ignore | mandatory}**	SSL 접속 준비 과정에서 클라이언트가 인증서를 전송하지 않은 경우의 대응 방법을 지정합니다. • **ignore** 인증서가 클라이언트의 응답에 포함되지 않은 경우, 세션을 종료합니다. • **mandatory** 인증서가 클라이언트의 응답에 포함되지 않은 경우에도 SSL 접속 준비 과정을 진행합니다.(기본값)
3	**verify-depth** *<VERIFY-DEPTH>*	CA의 인증서 검사 단계를 지정합니다. • *<VERIFY-DEPTH>* 설정 범위: 1 ~ 16, 기본값: 1
4	**import-crl** *<IMPORT>*	TFTP 서버에 저장되어 있는 인증서 취소 목록(Certification Revocation List)을 PAS-K로 다운로드합니다. • *<IMPORT>* TFTP 서버 IP 주소와 파일 이름을 다음과 같은 형식으로 입력 <SERVER-IP>:<FILE-NAME>
5	**import-crt** *<IMPORT>*	TFTP 서버에 저장되어 있는 인증서를 PAS-K로 다운로드합니다. • *<IMPORT>* TFTP 서버 IP 주소와 파일 이름을 다음과 같은 형식으로 입력 <SERVER-IP>:<FILE-NAME>
6	**current**	다운로드한 인증서 파일을 확인합니다.
7	**apply**	다운로드한 인증서를 PAS-K에 저장하고 등록합니다.

참고: 클라이언트 인증서를 삭제하려면 <Configuration 모드>에서 **no ssl client-authentication** *<ID>* 명령을 사용합니다.

클라이언트 인증서 내보내기

클라이언트 인증서를 TFTP 서버로 업로드하려면, <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**ssl client-authentication** *<ID>*	<클라이언트 인증서 설정 모드>로 들어갑니다. • <ID> 클라이언트 인증서의 ID. 설정 범위: 1 ~ 256
2	**export-crl** *<SERVER-IP> <FILE-NAME>*	PAS-K에 저장되어 있는 인증 취소 목록을 TFTP 서버로 업로드합니다. • *<SERVER-IP>* TFTP 서버 IP 주소 • *<FILE-NAME>* TFTP 서버 저장 시 사용할 파일 이름
3	**export-crt** *<SERVER-IP> <FILE-NAME>*	PAS-K에 저장되어 있는 인증서를 TFTP 서버로 업로드합니다. • *<SERVER-IP>* TFTP 서버 IP 주소 • *<FILE-NAME>* TFTP 서버 저장 시 사용할 파일 이름

프로필 설정

SSL 가속 기능을 사용하기 위해서는 프로필을 생성해야 합니다. PAS-K에는 최대 256개의 프로필을 등록할 수 있습니다. 여러 개의 프로필을 설정하는 경우에는 <Configuration 설정 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**ssl profile** *<ID>*	<Profile 설정 모드>로 들어갑니다. • *<ID>* ID. 설정 범위: 1 ~ 256
2	**certificate** *<CERTIFICATE>*	프로필에서 사용할 인증서 파일을 설정합니다. • *<CERTIFICATE>* 인증서 파일 이름.
3	**session-resumption pool-size** *<POOL-SIZE>*	재사용할 SSL 세션 정보를 저장해둘 풀(pool)의 크기(SSL 세션의 개수)를 설정합니다. '0'으로 지정하면 크기가 무한대(메모리가 허용하는 만큼 SSL 세션 정보를 저장)로 설정됩니다. • *<POOL-SIZE>* 풀(pool)의 크기. 설정 범위: 1 ~ 65535, 기본값: 30000
4	**session-resumption timeout** *<TIMEOUT>*	저장해둔 SSL 세션 정보의 유효 시간을 설정합니다. 유효 시간이 경과된 SSL 정보는 풀에서 삭제됩니다. • *<TIMEOUT>* SSL 세션 정보 유효 시간. 설정 범위: 1 ~ 3600 (초), 기본값: 30 (초)
5	**session-resumption status** {**enable** | **disable**}	SSL 세션 재사용 기능의 사용 여부를 지정합니다. • **enable** SSL 세션 재사용 기능 활성화 • **disable** SSL 세션 재사용 기능 비활성화 (기본값)
6	**ciphers** *<CIPHERS>*	SSL 가속 기능에서 지원할 암호 알고리즘을 지정합니다. • <CIPHERS> 암호 알고리즘을 입력. 여러 개의 암호 알고리즘을 입력하는 경우에는 ':'를 사용하여 구분. 지원 알고리즘: AES128-SHA, AES256-SHA, DES-CBC-SHA, DES-CBC3-SHA, EXP-DES-CBC-SHA, RC4-SHA, RC4-MD5, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA, EDH-RSA-DES-CBC-SHA, EDH-RSA-DES-CBC3-SHA, EXP-EDH-RSA-DES-CBC-SHA, EXP-RC2-CBC-MD5, AES128-SHA256, AES256-SHA256, DHE-RSA-AES128-SHA256, DHE-RSA-AES256-SHA256 기본값: ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
7	**prefer-server-cipher** {**enable** | **disable**}	PAS-K 가 선호하는 암호 알고리즘을 우선 사용하도록하는 prefer server cipher 옵션의 활성화 여부를 설정합니다. • **enable** Prefer server cipher 옵션 활성화 • **disable** Prefer server cipher 옵션 비활성화 (기본값)
8	**cipher-protocols** *<CIPHER-PROTOCOLS>*	SSL 가속 기능에서 지원할 암호 프로토콜을 지정합니다. • <CIPHER-PROTOCOLS> 암호 프로토콜을 입력. 여러 개의 암호 프로토콜을 입력하는 경우에는 ','를 사용하여 구분. 지원 프로토콜: SSLv3, TLSv1, TLSv1.1, TLSv1.2 기본값: SSLv3,TLSv1,TLSv1.1
9	**client-authentication** *<CLIENT-AUTHENTICATION>*	클라이언트 인증서 검증에 사용할 클라이언트 인증서를 지정합니다. • <CLIENT-AUTHENTICATION> 클라이언트 인증서 ID
10	**current**	프로필 설정 정보를 확인합니다.
11	**apply**	프로필 설정을 저장합니다.

참고: 정의한 프로필을 삭제하려면 <Configuration 모드>에서 **no ssl profile** *<ID>* 명령을 사용합니다.

설정 정보 보기

SSL 설정 정보 보기

PAS-K에 설정된 비밀 키, 인증 요청서, 인증서, 클라이언트 인증서, 프로필 목록을 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show ssl** 명령을 사용합니다.

비밀 키 정보 보기

비밀 키 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show ssl key** 명령을 사용합니다. 특정 비밀 키에 대한 정보를 확인하려면, **show ssl key** 명령과 함께 비밀 키 이름(<*NAME*>)을 입력합니다.

인증서/인증 요청서 정보 보기

인증서 또는 인증 요청서 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show ssl certificate** 명령을 사용합니다. 특정 인증서/인증 요청서에 대한 정보를 확인하려면, **show ssl certificate** 명령과 함께 인증서/인증 요청서 이름(<*NAME*>)을 입력합니다.

인증서/인증 요청서 상세 정보 보기

인증서 또는 인증 요청서의 상세 정보를 보려면 <Privileged 모드> 또는 <Configuration 모드>에서 **show info ssl certificate** 명령을 사용합니다. 인증서/인증 요청서의 이름(<*NAME*>)을 지정하면 해당 인증서에 대한 정보를 보여줍니다.

프로필 정보 보기

프로필 정보를 보려면 <Privileged 모드> 또는 <Configuration 모드>에서 **show ssl profile** 명령을 사용합니다. 특정 프로필의 정보를 확인하려면, 해당 명령 뒤에 프로필의 아이디(<*ID*>)를 지정하면 해당 프로필에 대한 정보를 화면에 출력합니다.

참고: 해당 명령 실행시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

L4 서버 부하 분산 설정

이 절에서는 CLI에서 PAS-K에 L4 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: L4 서버 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

CLI에서 설정하기

PAS-K에 L4 서버 부하 분산을 설정하는 과정은 다음과 같습니다.

1. L4 서버 부하 분산 서비스 정의
2. 설정 정보 보기

각 단계 별 설정 방법을 차례로 살펴봅니다.

L4 서버 부하 분산 서비스 정의

다음은 L4 서버 부하 분산 서비스를 정의하는 과정입니다. PAS-K에는 L4 서버 부하 분산 서비스를 포함하여 최대 1024개의 L4 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 L4 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**slb** *<NAME>*	<SLB 설정 모드>로 들어가서 L4 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**vip** *<IP>*[,*<IP>*,…] **protocol** *<PROTOCOL>*[,*<PROTOCOL>*,…] **vport** *<VPORT>*[,*<VPORT>*,…] (필수 설정)	부하 분산 서비스의 가상 IP 주소와 프로토콜, 가상 포트를 설정합니다. 여러 개의 가상 IP 주소와 프로토콜, 가상 포트를 지정하고자 하는 경우에는 ','로 구분하여 입력합니다. • *<IP>* 가상 IP 주소 입력. 최대 128 개의 IP 주소 지정 가능. • *<PROTOCOL>* tcp, udp, icmp, all 중에서 가상 포트를 설정할 프로토콜의 종류 입력. • *<VPORT>* 가상 포트 입력. 설정 범위: 1 ~ 65535, 최대 32 개의 포트 지정 **참고:** 설정한 가상 IP 주소와 프로토콜, 가상 포트를 삭제하려면 <SLB 설정 모드>에서 **no vip** *<IP>* **protocol** *<PROTOCOL>* **vport** *<VPORT>* 명령을 실행합니다.
3	**priority** *<PRIORITY>*	L4 서버 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위 입력. 설정 범위: 0 ~ 255, 기본값: 50 **참고**: 설정한 우선순위를 기본값으로 변경하려면, <SLB 설정 모드>에서 **no priority** 명령을 실행합니다.
4	**nat-mode** {**dnat** | **dsr** | **lan-to-lan**}	부하 분산 서비스의 NAT 모드를 설정합니다. (기본값: dnat)
5	**lan-to-lan** *<LAN-TO-LAN>* (NAT 모드가 lan-to-lan인 경우만 설정)	LAN 영역에서 클라이언트 역할을 하는 서버들의 IP 대역을 설정합니다 • *<LAN-TO-LAN>* IP 주소 대역 설정.
6	**lb-method** {**lc** | **lc-ss** | **lc-total** | **rr** | **sh** | **wlc** | **wlc-ss** | **wlc-total** | **wrr**}	부하 분산 서비스에서 사용할 부하 분산 방식을 설정합니다. (기본값: rr)

7	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 서버 부하 분산 서비스에서 삭제하려면 <SLB 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
8	**health-check** *<HEALTH-CHECK>* (선택 설정)	L4 서버 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 입력. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 서버 부하 분산 서비스에서 삭제하려면 <SLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
9	**slow-start rate** *<RATE>* (부하 분산 방식이 lc-ss 또는 wlc-ss인 경우만 설정)	새로 추가된 실제 서버로 부하 분산시킬 세션의 비율을 설정합니다. 설정 값이 클수록 많은 세션이 연결됩니다. • *<RATE>* 세션 비율. 설정 범위: 1 ~ 10, 기본값: 5
10	**slow-start timer** *<TIMER>* (부하 분산 방식이 lc-ss 또는 wlc-ss인 경우만 설정)	Slow-Start 옵션을 사용하여 부하 분산할 시간을 설정합니다. 지정한 시간이 경과한 후에는 최소 연결 방식 또는 가중치 최소 연결 방식으로 동작합니다. '0'으로 설정하면 Slow-Start 기능이 동작하지 않습니다. • *<TIMER>* Slow-Start 옵션 시간. 설정 범위: 0 ~ 600(초), 기본값: 60(초)
11	**sticky time** *<TIME>*	sticky 타임아웃 값을 설정합니다. 지정한 sticky 타임아웃이 경과한 후 연결 엔트리가 소멸되기 전에 동일한 클라이언트로부터의 연결이 시도되면 이전에 연결했던 서버와 동일한 서버로 연결됩니다. '0'으로 설정하면 지속 연결 기능을 사용하지 않습니다. • *<TIME>* sticky 타임아웃 시간. 설정 범위: 0 ~ 65535(초), 기본값: 60(초)
12	**sticky source-subnet** *<SOURCE-SUBNET>*	기본적으로 지속 연결 기능은 출발지 IP 주소 별로 적용됩니다. 지속 연결 기능을 출발지 서브넷별로 적용하려면 지속 연결 기능을 적용할 서브넷 범위를 설정합니다. • *<SOURCE-SUBNET>* 서브넷 마스크 범위. 기본값: 255.255.255.255 **주의:** 서브넷 별로 지속 연결 기능을 적용하려는 경우에는 부하 분산 방식을 'sh'로 설정해야 합니다.
13	**session-sync {enable | disable}**	세션 싱크 기능의 사용 여부를 지정합니다. • **enable** 세션 싱크 기능 활성화 • **disable** 세션 싱크 기능 비활성화 (기본값)
14	**fail-skip {enable | disable}** (선택 설정)	바이패스 기능의 사용 여부를 지정합니다. • **enable** 바이패스 기능 활성화 • **disable** 바이패스 기능 비활성화 (기본값)
15	**backup** *<BACKUP>*	설정 중인 L4 서버 부하 분산 서비스에서 더 이상 서비스 요청을 받을 수 없는 경우, 대신 서비스 요청을 처리할 백업 서비스를 지정합니다. 반드시 이미 생성되어 있는 서비스의 이름을 입력해야 합니다. • *<BACKUP>* 백업 서비스의 이름 **참고:** 설정한 백업 서비스를 L4 서버 부하 분산 서비스에서 삭제하려면 <SLB 설정 모드>에서 **no backup** 명령을 실행합니다.
16	**status {enable | disable}** (선택 설정)	L4 서버 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 기능 활성화 (기본값) • **disable** 부하 분산 서비스 기능 비활성화
17	**current**	L4 서버 부하 분산 서비스의 설정 정보를 확인합니다.

18	**apply**	L4 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 L4 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no slb** *<NAME>* 명령을 사용합니다.

참고: 다음은 각 종류의 부하 분산 서비스에 설정되는 기본 우선순위입니다.

- L4 서버 부하 분산 서비스 : 50
- 고급 L4 서버 부하 분산 서비스 : 100
- L4 캐시 서버 부하 분산 서비스 : 0
- 방화벽/VPN 부하 분산 서비스 : 100
- 고급 방화벽/VPN 부하 분산 서비스 : 100
- 게이트웨이 부하 분산 서비스 : 100
- L7 서버 부하 분산 서비스 : 100
- 고급 L7 서버 부하 분산 서비스 : 100
- L7 캐시 서버 부하 분산 서비스 : 0
- 고급 L7 캐시 서버 부하 분산 서비스 : 100

우선순위 값이 작을수록 먼저 적용되므로, 기본 우선순위를 변경하지 않은 경우에는 L4/L7 캐시 서버 부하 분산 서비스가 가장 먼저 적용되고, 이후에는 L4 서버 부하 분산 서비스가, 그 이후에는 나머지 종류의 부하 분산 서비스가 적용됩니다. 우선순위가 동일한 부하 분산 서비스들은 정의된 시간 순서에 따라서(먼저 정의된 서비스가 우선) 적용됩니다.

필터 설정

L4 서버 부하 분산 서비스를 어떤 트래픽에 적용할 것인지를 구분하기 위해 사용되는 필터를 정의하는 방법은 다음과 같습니다. L4 서버 부하 분산 서비스에는 최대 2048개의 다른 필터를 등록할 수 있으므로, 여러 개의 필터를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

참고: 필터를 설정하지 않은 경우에는 설정한 가상 IP 주소를 목적지 IP 주소로하는 include 타입의 필터가 자동으로 생성되며, 가상 IP 주소 삭제시 해당 필터도 자동으로 삭제됩니다.

순서	명 령	설 명
1	**slb** *<NAME>*	<SLB 설정 모드>로 들어갑니다. • *<NAME>* 필터를 설정할 L4 서버 부하 분산 서비스 이름
2	**filter** *<ID>*	<SLB 설정 모드>에서 <Filter 설정 모드>로 들어갑니다. • *<ID>* 설정 범위: 1~2048. 필터는 L4 서버 부하 분산 서비스 별로 독립적으로 관리되기 때문에 다른 L4 서버 부하 분산 서비스에서 정의한 필터와 같은 ID 를 가질 수 있습니다.
3	**type {include | exclude}**	필터의 종류를 설정합니다. • **include** 필터가 L4 서버 부하 분산 서비스를 '적용'할 트래픽을 필터링하는 경우 (기본값) • **exclude** L4 서버 부하 분산 서비스를 '적용하지 않을' 트래픽을 필터링하는 경우

참고: 이 후의 과정은 필터링에 사용될 조건을 지정하는 과정입니다. 모든 과정을 수행할 필요는 없고 필터링 시 사용할 항목에 해당되는 과정만 수행하면 됩니다. 필터링에 사용할 조건에 따라 이동할 단계는 다음과 같습니다. 하나의 필터에는 여러 개의 조건이 추가될 수 있으므로 하나의 조건을 추가한 후 다른 단계로 이동하여 다른 조건을 계속 추가하면 됩니다.

- **프로토콜** → **4번** 단계
- **출발지 IP 주소** → **5번** 단계
- **출발지 포트 번호** → **6번** 단계
- **목적지 IP 주소** → **7번** 단계
- **목적지 포트 번호** → **8번** 단계

4	**protocol** *<PROTOCOL>*	필터링 조건으로 사용할 프로토콜의 종류를 설정합니다. • *<PROTOCOL>* 지정할 프로토콜이 TCP 나 UDP, ICMP 인 경우에는 각각 tcp, udp, icmp 를 입력하고, 프로토콜을 필터링 조건으로 사용하지 않으려면 all 입력. (기본값: all)

5	**sip** *<SIP>*	필터링 조건으로 사용할 출발지 IP 주소와 넷 마스크 비트 수를 입력합니다. • *<SIP>* 출발지 IP 주소 및 서브넷 마스크 비트 수 설정 (기본값: 0.0.0.0/0)
6	**sport** *<SPORT>*	필터링 조건으로 사용할 출발지 포트 번호를 입력합니다. 프로토콜이 ICMP인 경우에는 필터링 조건으로 사용되지 않습니다. • *<SPORT>* 출발지 포트 번호 설정 (설정 범위: 1 ~ 65535)
7	**dip** *<DIP>*	필터링 조건으로 사용할 목적지 IP 주소와 넷 마스크 비트 수를 입력합니다. • *<DIP>* 목적지 IP 주소 및 서브넷 마스크 비트 수 설정 (기본값: 0.0.0.0/0)
8	**dport** *<DPORT>*	필터링 조건으로 사용할 목적지 포트 번호를 입력합니다. 프로토콜이 ICMP인 경우에는 필터링 조건으로 사용되지 않습니다. • *<DPORT>* 목적지 포트 번호 설정 (설정 범위: 1 ~ 65535)
9	**status** {**enable** | **disable**} (선택 설정)	필터 기능의 사용 여부를 지정합니다. • **enable** 필터 기능 활성화 (기본값) • **disable** 필터 기능 비활성화
10	**current**	필터의 설정 정보를 확인합니다.
11	**apply**	필터의 설정을 저장하고 시스템에 적용합니다.

참고: 정의한 필터를 삭제하려면 <SLB 설정 모드>에서 **no filter** *<ID>* 명령을 사용합니다.

설정 정보 보기

L4 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

L4 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 L4 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show slb** 명령을 사용합니다. **show slb** 명령은 현재 PAS-K에 정의된 L4 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 L4 서버 부하 분산 서비스의 설정 정보 보기

특정 L4 서버 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **show slb** 명령 뒤에 서비스의 이름(*<NAME>*)을 입력합니다.

L4 서버 부하 분산 서비스의 모든 설정 정보(실제 서버, 장애 감시, 세션 설정) 보기

<Privileged 모드> 또는 <Configuration 모드>에서 **show info slb** 명령을 사용하면 각 L4 서버 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 그리고 서비스에 등록된 실제 서버의 설정 정보와 실제 서버를 통해 연결된 세션에 대한 정보를 확인할 수 있습니다.

서비스의 이름을 입력하지 않고 **show info slb** 명령을 실행하면 모든 L4 서버 부하 분산 서비스에 대한 정보가 출력되고, **show info slb** 명령 뒤에 서비스의 이름(*<NAME>*)을 입력하면 해당 서비스에 대한 정보만 확인할 수 있습니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

고급 L4 서버 부하 분산 설정

이 절에서는 CLI에서 PAS-K에 고급 L4 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: 고급 L4 서버 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

CLI에서 설정하기

PAS-K에 고급 L4 서버 부하 분산을 설정하는 과정은 다음과 같습니다.

1. 고급 L4 서버 부하 분산 서비스 정의
2. 설정 정보 보기

각 단계 별 설정 방법을 차례로 살펴봅니다.

고급 L4 서버 부하 분산 서비스 정의

다음은 고급 L4 서버 부하 분산 서비스를 정의하는 과정입니다. PAS-K에는 고급 L4 서버 부하 분산 서비스를 포함하여 최대 1024개의 L4 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 고급 L4 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl4slb** *<NAME>*	<고급 SLB 설정 모드>로 들어가서 고급 L4 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**ip-version {ipv4 | ipv6}**	고급 L4 서버 부하 분산 서비스의 네트워크 종류를 설정합니다. (기본값: ipv4)
3	**vip** *<IP>*[,*<IP>*,…] **protocol** *<PROTOCOL>*[,*<PROTOCOL>*,…] **vport** *<VPORT>*[,*<VPORT>*,…] (필수 설정)	부하 분산 서비스의 가상 IP 주소와 프로토콜, 가상 포트를 설정합니다. 여러 개의 가상 IP 주소와 프로토콜, 가상 포트를 지정하고자 하는 경우에는 ','로 구분하여 입력합니다. • *<IP>* 가상 IP 주소 입력. 최대 128 개의 IP 주소 지정 가능. • *<PROTOCOL>* 가상 포트를 설정할 프로토콜인 'tcp'를 입력. • *<VPORT>* 가상 포트 입력. 설정 범위: 1 ~ 65535, 최대 32 개의 포트 지정 **참고:** 설정한 가상 IP 주소와 프로토콜, 가상 포트를 삭제하려면 <고급 SLB 설정 모드>에서 **no vip** *<IP>* **protocol** *<PROTOCOL>* **vport** *<VPORT>* 명령을 실행합니다.
4	**priority** *<PRIORITY>*	L4 서버 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위 입력. 설정 범위: 1 ~ 256, 기본값: 100 **참고**: 설정한 우선순위를 기본값으로 변경하려면, <고급 SLB 설정 모드>에서 **no priority** 명령을 실행합니다.
5	**nat-mode {bnat | dnat}**	부하 분산 서비스의 NAT 모드를 설정합니다. (기본값: dnat)
6	**lb-method {first | lc | rr | sh | sh-c | wrr | wsh | wsh-c}**	부하 분산 서비스에서 사용할 부하 분산 방식을 설정합니다. (기본값: rr)

7	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 부하 분산 서비스에서 삭제하려면 <고급 SLB 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
8	**health-check** *<HEALTH-CHECK>* (선택 설정)	고급 L4 서버 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 입력. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 부하 분산 서비스에서 삭제하려면 <고급 SLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
9	**sticky type src-ip**	지속 연결 기능 유형을 지정합니다. 고급 L4 서버 부하 분산 서비스는 출발지 IP 주소 별로 지속 연결 기능을 적용하는 'src-ip' 유형만 지원합니다.
10	**sticky time** *<TIME>*	sticky 타임아웃 값을 설정합니다. 지정한 sticky 타임아웃이 경과한 후 연결 엔트리가 소멸되기 전에 동일한 클라이언트로부터의 연결이 시도되면 이전에 연결했던 서버와 동일한 서버로 연결됩니다. '0'으로 설정하면 지속 연결 기능을 사용하지 않습니다. • *<TIME>* sticky 타임아웃 시간. 설정 범위: 0 ~ 65535(초), 기본값: 60(초) **참고**: 설정한 sticky 타임아웃 값을 기본값으로 변경하려면, <고급 SLB 설정 모드>에서 **no sticky time** 명령을 실행합니다.
11	**max-connection** *<MAX-CONNECTION>*	고급 L4 서버 부하 분산 서비스에서 제한할 최대 커넥션 수를 지정합니다. '0'으로 지정한 경우에는 커넥션을 제한하지 않습니다. • *<MAX-CONNECTION>* 최대 커넥션 수. 설정 범위: 0 ~ 320,000, 기본값: 0 **참고**: 설정한 최대 커넥션 수를 기본값으로 변경하려면, <고급 SLB 설정 모드>에서 **no max-connection** 명령을 실행합니다.
12	**backup** *<BACKUP>*	설정 중인 고급 L4 서버 부하 분산 서비스에서 더 이상 서비스 요청을 받을 수 없는 경우, 대신 서비스 요청을 처리할 백업 서비스를 지정합니다. 반드시 이미 생성되어 있는 서비스의 이름을 입력해야 합니다. • *<BACKUP>* 백업 서비스의 이름 **참고:** 설정한 백업 서비스를 고급 L4 서버 부하 분산 서비스에서 삭제하려면 <고급 SLB 설정 모드>에서 **no backup** 명령을 실행합니다.
13	**status {enable | disable}** (선택 설정)	고급 L4 서버 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 기능 활성화 (기본값) • **disable** 부하 분산 서비스 기능 비활성화
14	**current**	고급 L4 서버 부하 분산 서비스의 설정 정보를 확인합니다.
15	**apply**	고급 L4 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 고급 L4 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no advl4slb** *<NAME>* 명령을 사용합니다.

설정 정보 보기

고급 L4 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

고급 L4 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 고급 L4 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **`show advl4slb`** 명령을 사용합니다. **`show advl4slb`** 명령은 현재 PAS-K에 정의된 고급 L4 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 고급 L4 서버 부하 분산 서비스의 설정 정보 보기

특정 고급 L4 서버 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **`show advl4slb`** 명령 뒤에 서비스의 이름(*<NAME>*)을 입력합니다.

고급 L4 서버 부하 분산 서비스의 모든 설정 정보(실제 서버, 장애 감시, 세션 설정) 보기

<Privileged 모드> 또는 <Configuration 모드>에서 **`show info advl4slb`** 명령을 사용하면 각 고급 L4 서버 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 그리고 서비스에 등록된 실제 서버의 설정 정보와 실제 서버를 통해 연결된 세션에 대한 정보를 확인할 수 있습니다.

서비스의 이름을 입력하지 않고 **`show info advl4slb`** 명령을 실행하면 모든 고급 L4 서버 부하 분산 서비스에 대한 정보가 출력되고, **`show info advl4slb`** 명령 뒤에 서비스의 이름(*<NAME>*)을 입력하면 해당 서비스에 대한 정보만 확인할 수 있습니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

방화벽/VPN 부하 분산 설정

이 절에서는 CLI에서 PAS-K에 방화벽/VPN 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: 방화벽/VPN 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

CLI에서 설정하기

PAS-K에 방화벽/VPN 부하 분산을 설정하는 과정은 다음과 같습니다.

1. 방화벽/VPN 부하 분산 서비스 정의
2. 필터 설정
3. 설정 정보 보기

방화벽/VPN 부하 분산 서비스 정의

다음은 방화벽/VPN 부하 분산 서비스를 정의하는 과정입니다. PAS-K에는 방화벽/VPN 부하 분산 서비스를 포함하여 최대 1024개의 L4 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 방화벽/ VPN 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**fwlb** *<NAME>*	<FWLB 설정 모드>로 들어가서 방화벽/VPN 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**priority** *<PRIORITY>*	방화벽/VPN 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위. (설정 범위: 0 ~ 255, 기본값: 100) **참고**: 설정한 우선순위를 기본값으로 변경하려면, <FWLB 설정 모드>에서 **no priority** 명령을 사용합니다.
3	**lb-method** {**bh** | **dh** | **lc** | **lc-total** | **rr** | **sh** | **wlc** | **wlc-total** | **wrr**}	방화벽/VPN 부하 분산 서비스에서 사용할 부하 분산 방식을 설정합니다 (기본값: rr)
4	**vpnlb** {**enable** | **disable**}	현재 설정 중인 부하 분산 서비스를 VPN 부하 분산 서비스로 사용할 지 여부를 설정합니다. • **enable** VPN 부하 분산 서비스로 사용 • **disable** 방화벽 부하 분산 서비스로 사용 (기본값) **참고:** VPN 부하 분산 서비스 사용 여부는 방화벽/VPN 부하 분산 서비스 추가시 설정할 수 있으며, 시스템에 적용된 이후에는 수정할 수 없습니다.
5	**position** {**external** | **internal** | **dmz**}	방화벽/VPN 부하 분산 서비스가 수행될 위치를 설정합니다. • **external** WAN과 방화벽 혹은 VPN 장비 사이에 위치하는 경우 설정 • **internal** LAN과 방화벽 혹은 VPN 장비 사이에 위치하는 경우 설정 (기본값) • **dmz**(방화벽 부하 분산인 경우) DMZ 영역에 위치하는 경우 설정 **참고:** 방화벽/VPN 부하 분산 서비스 수행 위치는 방화벽/VPN 부하 분산 서비스 추가시 설정할 수 있으며, 시스템에 적용된 이후에는 수정할 수 없습니다.

6	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 실제 서버 ID 입력. 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 방화벽/VPN 부하 분산 서비스에서 삭제하려면 <FWLB 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
7	**health-check** *<HEALTH-CHECK>*	방화벽/VPN 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시 ID 입력. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 방화벽/VPN 부하 분산 서비스에서 삭제하려면 <FWLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
8	**sticky time** *<TIME>*	sticky 타임아웃 값을 설정합니다. 지정한 sticky 타임아웃이 경과한 후 연결 엔트리가 소멸되기 전에 동일한 클라이언트로부터의 연결이 시도되면 이전에 연결했던 방화벽(VPN 장비)와 동일한 방화벽(VPN 장비)로 연결됩니다. Sticky 타임아웃을 '0'으로 설정하면 지속 연결 기능을 사용하지 않습니다. • *<TIME>* sticky 타임아웃 값. 설정 범위: 0 ~ 65535(초), 기본값: 60(초)
9	**sticky source-subnet** *<SOURCE-SUBNET>* (지속 연결을 적용할 출발지 서브넷 범위 지정) **sticky destination-subnet** *<DESTINATION-SUBNET>* (지속 연결을 적용할 목적지 서브넷 범위 지정)	기본적으로 지속 연결 기능은 출발지 IP 주소별로 적용됩니다. 지속 연결 기능을 출발지 서브넷별로 적용하려면 **sticky source-subnet** 명령을 사용하고, 목적지 서브넷별로 적용하려면 **sticky destination-subnet** 명령을 사용하여 지속 연결 기능을 적용할 서브넷 범위를 설정합니다. • *<SOURCE-SUBNET>* 서브넷 마스크. 기본값:255.255.255.255 **주의:** 서브넷 별로 지속 연결 기능을 적용하려는 경우에는 부하 분산 방식을 bh, dh, sh 중 하나로 설정해야 합니다. **주의:** 방화벽 부하 분산 서비스(vpnlb가 disable인)의 지속 연결 기능은 출발지와 목적지를 모두 기준으로 사용하지만, VPN 부하 분산 서비스(vpnlb가 enable인)는 출발지나 혹은 목적지만을 기준으로 하는 지속 연결 기능을 지원합니다. VPN 부하 분산 서비스의 수행 위치가 내부(internal)이거나 DMZ이면 목적지만을 기준으로 지속 연결 기능을 수행하고, 수행 위치가 외부(external)이면 출발지 기준으로 지속 연결 기능을 수행합니다. 따라서, 수행 위치가 내부이거나 DMZ인 VPN 부하 분산 서비스에서는 **sticky source-subnet** 명령을 사용할 수 없고, 외부에서 동작하는 VPN 부하 분산 서비스는 **sticky destination-subnet** 명령을 사용할 수 없습니다.
10	**multi-tunnel** {**enable** | **disable**} (VPN 부하 분산 서비스로 사용하는 경우에만 설정)	VPN 부하 분산 서비스에서 다중 터널의 지속 연결 기능 사용 여부를 설정합니다. • **enable** 다중 터널의 지속 연결 기능을 활성화 • **disable** 다중 터널의 지속 연결 기능을 비활성화 (기본값) **참고:** 다중 터널의 지속 연결 기능은 내부 PAS-K 에만 활성화하면 됩니다. 외부 PAS-K는 VPN 장비들의 게이트웨이 IP 주소로 지속 연결을 형성하기 때문에 다중 터널의 지속 연결 기능을 활성화할 필요가 없습니다.
11	**branch-relay** {**enable** | **disable**} (VPN 부하 분산 서비스로 사용하는 경우에만 설정)	VPN 부하 분산 서비스에서 지점간 VPN 연결 기능의 사용 여부를 설정합니다. • **enable** 지점 간 VPN 연결 기능을 활성화 • **disable** 지점 간 VPN 연결 기능을 비활성화 (기본값)
12	**fail-skip** {**enable** | **disable**} (선택 설정)	바이패스 기능의 사용 여부를 지정합니다. • **enable** 바이패스 기능 활성화 • **disable** 바이패스 기능 비활성화 (기본값)
13	**backup** *<BACKUP>*	설정 중인 방화벽/VPN 부하 분산 서비스에서 더 이상 서비스 요청을 받을 수 없는 경우, 대신 서비스 요청을 처리할 백업 서비스를 지정합니다. 반드시 이미 생성되어 있는 서비스의 이름을 입력해야 합니다. • *<BACKUP>* 백업 서비스의 이름 **참고:** 설정한 백업 서비스를 방화벽/VPN 부하 분산 서비스에서 삭제하려면 <FWLB 설정 모드>에서 **no backup** 명령을 실행합니다.

14	**status {enable | disable}** (선택 설정)	방화벽/VPN 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 활성화 (기본값) • **disable** 부하 분산 서비스 비활성화
15	**current**	방화벽/VPN 부하 분산 서비스의 설정 정보를 확인합니다.
16	**apply**	방화벽/VPN 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 방화벽/VPN 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no fwlb** *<NAME>* 명령을 사용합니다.

필터 설정

L4 방화벽/VPN 부하 분산 서비스를 어떤 트래픽에 적용할 것인지를 구분하기 위해 사용되는 필터를 정의하는 방법은 다음과 같습니다. 방화벽/VPN 부하 분산 서비스에는 최대 2048개의 다른 필터를 등록할 수 있으므로, 여러 개의 필터를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**fwlb** *<NAME>*	<FWLB 설정 모드>로 들어갑니다. • *<NAME>* 필터를 설정할 방화벽/VPN 부하 분산 서비스 이름
2	**filter** *<ID>*	<FWLB 설정 모드>에서 <Filter 설정 모드>로 들어갑니다. • *<ID>* 설정 범위: 1~2048. 필터는 방화벽/VPN 부하 분산 서비스 별로 독립적으로 관리되기 때문에 다른 방화벽/VPN 부하 분산 서비스에서 정의한 필터와 같은 ID 를 가질 수 있습니다.
3	**type** {**include** | **exclude**}	필터의 종류를 설정합니다. • **include** 필터가 방화벽/VPN 부하 분산 서비스를 '적용'할 트래픽을 필터링하는 경우 (기본값) • **exclude** 방화벽/VPN 부하 분산 서비스를 '적용하지 않을' 트래픽을 필터링하는 경우 **주의:** 방화벽/VPN 부하 분산 서비스가 정상 동작하려면 최소한 하나 이상의 'include' 타입의 필터를 추가 해야 합니다

참고: 이 후의 과정은 필터링에 사용될 조건을 지정하는 과정입니다. 모든 과정을 수행할 필요는 없고 필터링 시 사용할 항목에 해당되는 과정만 수행하면 됩니다. 필터링에 사용할 조건에 따라 이동할 단계는 다음과 같습니다. 하나의 필터에는 여러 개의 조건이 추가될 수 있으므로 하나의 조건을 추가한 후 다른 단계로 이동하여 다른 조건을 계속 추가하면 됩니다.

- **프로토콜** → **4번** 단계
- **출발지 IP 주소** → **5번** 단계
- **출발지 포트 번호** → **6번** 단계
- **목적지 IP 주소** → **7번** 단계
- **목적지 포트 번호** → **8번** 단계

4	**protocol** *<PROTOCOL>*	필터링 조건으로 사용할 프로토콜의 종류를 설정합니다. • *<PROTOCOL>* 지정할 프로토콜이 TCP 나 UDP, ICMP 인 경우에는 각각 tcp, udp, icmp 를 입력하고, 프로토콜을 필터링 조건으로 사용하지 않으려면 all 입력. (기본값: all)
5	**sip** *<SIP>*	필터링 조건으로 사용할 출발지 IP 주소와 넷 마스크 비트 수를 입력합니다. • *<SIP>* 출발지 IP 주소 및 서브넷 마스크 비트 수 설정 (기본값: 0.0.0.0/0)
6	**sport** *<SPORT>*	필터링 조건으로 사용할 출발지 포트 번호를 입력합니다. 프로토콜이 ICMP인 경우에는 필터링 조건으로 사용되지 않습니다. • *<SPORT>* 출발지 포트 번호 설정 (설정 범위: 1 ~ 65535)
7	**dip** *<DIP>*	필터링 조건으로 사용할 목적지 IP 주소와 넷 마스크 비트 수를 입력합니다. • *<DIP>* 목적지 IP 주소 및 서브넷 마스크 비트 수 설정 (기본값: 0.0.0.0/0)
8	**dport** *<DPORT>*	필터링 조건으로 사용할 목적지 포트 번호를 입력합니다. 프로토콜이 ICMP인 경우에는 필터링 조건으로 사용되지 않습니다. • *<DPORT>* 목적지 포트 번호 설정 (설정 범위: 1 ~ 65535)
9	**status** {**enable** | **disable**} (선택 설정)	필터 기능의 사용 여부를 지정합니다. • **enable** 필터 기능 활성화 (기본값) • **disable** 필터 기능 비활성화
10	**current**	필터의 설정 정보를 확인합니다.
11	**apply**	필터의 설정을 저장하고 시스템에 적용합니다.

참고: 정의한 필터를 삭제하려면 <FWLB 설정 모드>에서 **no filter** *<ID>* 명령을 사용합니다.

설정 정보 보기

방화벽/VPN 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

방화벽/VPN 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 방화벽/VPN 부하 분산 서비스의 설정 정보를 확인하려면 <Privileged 모드> 또는 <Configuration 모드>에서 **show fwlb** 명령을 사용합니다. **show fwlb** 명령은 현재 PAS-K에 정의된 방화벽/VPN 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 방화벽/VPN 부하 분산 서비스의 설정 정보 보기

특정 방화벽/VPN 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **show fwlb** 명령 뒤에 서비스의 이름(<*NAME*>)을 입력합니다.

방화벽/VPN 부하 분산 서비스의 모든 설정 정보(실제 서버, 장애 감시, 필터, 세션) 보기

각 방화벽/VPN 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 필터 정보, 그리고 서비스에 등록된 실제 서버의 설정 정보와 실제 서버를 통해 연결된 세션에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show info fwlb** 명령을 사용합니다.

서비스의 이름을 입력하지 않고 **show info fwlb** 명령을 실행하면 모든 방화벽/VPN 부하 분산 서비스에 대한 정보가 출력되고, **show info fwlb** 명령 뒤에 서비스의 이름(<*NAME*>)을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

고급 방화벽/VPN 부하 분산 설정

이 절에서는 CLI에서 고급 방화벽/VPN 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: 고급 방화벽/VPN 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

CLI에서 설정하기

PAS-K에 고급 방화벽/VPN 부하 분산을 설정하는 과정은 다음과 같습니다.

1. 고급 방화벽/VPN 부하 분산 서비스 정의
2. 필터 설정
3. 설정 정보 보기

고급 방화벽/VPN 부하 분산 서비스 정의

다음은 고급 방화벽/VPN 부하 분산 서비스를 정의하는 과정입니다. PAS-K에는 고급 방화벽/VPN 부하 분산 서비스를 포함하여 최대 1024개의 L4 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 고급 방화벽/VPN 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl4fwlb** *<NAME>*	<고급 FWLB 설정 모드>로 들어가서 방화벽/VPN 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**ip-version {ipv4 | ipv6}**	부하 분산 서비스의 네트워크 종류를 설정합니다. (기본값: ipv4)
3	**priority** *<PRIORITY>*	고급 방화벽/VPN 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 설정 범위: 1 ~ 256, 기본값: 100 **참고**: 설정한 우선순위를 기본값으로 변경하려면, <고급 FWLB 설정 모드>에서 **no priority** 명령을 사용합니다.
4	**lb-method bh**	고급 방화벽/VPN 부하 분산 서비스에서 사용할 부하 분산 방식을 설정합니다
5	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 실제 서버 ID. 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 고급 방화벽/VPN 부하 분산 서비스에서 삭제하려면 <고급 FWLB 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
6	**health-check** *<HEALTH-CHECK>*	고급 방화벽/VPN 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시 ID. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 고급 방화벽/VPN 부하 분산 서비스에서 삭제하려면 <고급 FWLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.

7	**status {enable | disable}** (선택 설정)	고급 방화벽/VPN 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 기능 활성화 (기본값) • **disable** 부하 분산 서비스 기능 비활성화
8	**current**	고급 방화벽/VPN 부하 분산 서비스의 설정 정보를 확인합니다.
9	**apply**	고급 방화벽/VPN 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 고급 방화벽/VPN 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no advl4fwlb** *<NAME>* 명령을 사용합니다.

필터 설정

고급 방화벽/VPN 부하 분산 서비스를 어떤 트래픽에 적용할 것인지를 구분하기 위해 사용되는 필터를 정의하는 방법은 다음과 같습니다. 고급 방화벽/VPN 부하 분산 서비스에는 최대 256개의 다른 필터를 등록할 수 있으므로, 여러 개의 필터를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advfwlb** *<NAME>*	<고급 FWLB 설정 모드>로 들어갑니다. • *<NAME>* 필터를 설정할 고급 방화벽/VPN 부하 분산 서비스 이름
2	**filter** *<ID>*	<고급 FWLB 설정 모드>에서 <Filter 설정 모드>로 들어갑니다. • *<ID>* 필터 ID. 설정 범위: 1 ~ 256. 필터는 고급 방화벽 부하 분산 서비스 별로 독립적으로 관리되기 때문에 다른 고급 방화벽/VPN 부하 분산 서비스에서 정의한 필터와 같은 ID 를 가질 수 있습니다.

참고: 이후의 과정은 필터링에 사용될 조건을 지정하는 과정입니다. 모든 과정을 수행할 필요는 없고 필터링시 사용할 항목에 해당되는 과정만 수행하면 됩니다. 필터링에 사용할 조건에 따라 이동할 단계는 다음과 같습니다. 하나의 필터에는 여러 개의 조건이 추가될 수 있으므로 하나의 조건을 추가한 후 다른 단계로 이동하여 다른 조건을 계속 추가하면 됩니다.

- **프로토콜** → **3번** 단계
- **출발지 IP 주소** → **4번** 단계
- **목적지 IP 주소** → **5번** 단계

3	**protocol** *<PROTOCOL>*	필터링 조건으로 사용할 프로토콜의 종류를 설정합니다. • *<PROTOCOL>* 지정할 프로토콜이 TCP 나 UDP, ICMP 인 경우에는 각각 tcp, udp, icmp 를 입력하고, 프로토콜을 필터링 조건으로 사용하지 않으려면 all 입력. 기본값: all
4	**sip** *<SIP>*	필터링 조건으로 사용할 출발지 IP 주소와 넷 마스크 비트 수를 입력합니다. IPv6인 경우에는 IPv6 주소와 Prefix를 입력합니다. • *<SIP>* 출발지 IP 주소 및 서브넷 마스크 비트 수. 기본값: 0.0.0.0/0
5	**dip** *<DIP>*	필터링 조건으로 사용할 목적지 IP 주소와 넷 마스크 비트 수를 입력합니다. IPv6인 경우에는 IPv6 주소와 Prefix를 입력합니다. • *<DIP>* 목적지 IP 주소 및 서브넷 마스크 비트 수. 기본값: 0.0.0.0/0
6	**status {enable | disable}** (선택 설정)	필터 기능의 사용 여부를 지정합니다. • **enable** 필터 기능 활성화 (기본값) • **disable** 필터 기능 비활성화
7	**current**	필터의 설정 정보를 확인합니다.
8	**apply**	필터의 설정을 저장하고 시스템에 적용합니다.

참고: 정의한 필터를 삭제하려면 <고급 FWLB 설정 모드>에서 **no filter** *<ID>* 명령을 사용합니다.

설정 정보 보기

고급 방화벽/VPN 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

고급 방화벽/VPN 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 고급 방화벽/VPN 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show advl4fwlb** 명령을 사용합니다. **show advl4fwlb** 명령은 현재 PAS-K에 정의된 고급 방화벽/VPN 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 고급 방화벽/VPN 부하 분산 서비스의 설정 정보 보기

특정 고급 방화벽/VPN 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **advl4fwlb** 명령 뒤에 해당 서비스의 이름(<*NAME*>)을 입력하면 됩니다.

고급 방화벽/VPN 부하 분산 서비스의 모든 설정 정보 보기

각 고급 방화벽/VPN 부하 분산 서비스의 설정 정보와 필터 정보, 그리고 서비스에 등록된 실제 서버와 서비스의 장애 감시 결과에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show info advl4fwlb** 명령을 사용합니다.

서비스의 이름을 입력하지 않고 **show info fwlb** 명령을 실행하면 모든 고급 방화벽/VPN 부하 분산 서비스에 대한 정보가 출력되고, **show info fwlb** 명령 뒤에 서비스의 이름(<*NAME*>)을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

L4 캐시 서버 부하 분산 설정

이 절에서는 CLI에서 PAS-K에 L4 캐시 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: L4 캐시 서버 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

CLI에서 설정하기

PAS-K에 L4 캐시 서버 부하 분산을 설정하는 과정은 다음과 같습니다.

1. 캐시 서버 부하 분산 서비스 정의
2. 필터 설정하기
3. 설정 정보 보기

2번 단계의 설정 과정은 [**방화벽/VPN 부하 분산 설정하기**] 절에서 설명한 방화벽 부하 분산 서비스의 필터 설정 방법과 같습니다. 그러므로, 이 절에서는 캐시 서버 부하 분산 서비스를 정의하는 1번 단계의 과정과 설정 정보를 확인하는 3번 과정만 상세하게 살펴보도록 합니다.

캐시 서버 부하 분산 서비스 정의

다음은 L4 캐시 서버 부하 분산 서비스를 정의하는 과정입니다. PAS-K에는 L4 캐시 서버 부하 분산 서비스를 포함하여 최대 1024개의 L4 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 L4 캐시 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**cslb** *<NAME>*	<CSLB 설정 모드>로 들어가서 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**priority** *<PRIORITY>*	L4 캐시 서버 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위 설정. (설정 범위: 0 ~ 255, (기본값: 0)) **참고**: 설정한 우선순위를 기본값으로 변경하려면, <CSLB 설정 모드>에서 **no priority** 명령을 사용합니다.
3	**lb-method {bh | lc | lc-total | rr | wlc | wlc-total | wrr}**	L4 캐시 서버 부하 분산 서비스에서 사용할 부하 분산 방식을 설정합니다. (기본값: rr)
4	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 실제 서버 ID. 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 삭제하려면 <CSLB 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
5	**health-check** *<HEALTH-CHECK>*	L4 캐시 서버 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>*

		장애 감시의 ID. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 삭제하려면 <CSLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
6	**sticky time** *<TIME>*	sticky 타임아웃 값을 설정합니다. 지정한 sticky 타임아웃이 경과한 후 연결 엔트리가 소멸되기 전에 동일한 클라이언트로부터의 연결이 시도되면 이전에 연결했던 캐시 서버와 동일한 캐시 서버로 연결됩니다. Sticky 타임아웃을 '0'으로 설정하면 지속 연결 기능을 사용하지 않습니다. • *<TIME>* sticky 타임아웃 시간. 설정 범위: 0 ~ 65535(초), 기본값: 60(초)
7	**sticky source-subnet** *<SOURCE-SUBNET>* 지속 연결을 적용할 출발지 서브넷 범위 지정 **sticky destination-subnet** *<DESTINATION-SUBNET>* 지속 연결을 적용할 목적지 서브넷 범위 지정	기본적으로 지속 연결 기능은 출발지 IP 주소별로 적용됩니다. 지속 연결 기능을 출발지 서브넷 별로 적용하려면 **sticky source-subnet** 명령을 사용하고, 목적지 서브넷 별로 적용하려면 **sticky destination-subnet** 명령을 사용하여 지속 연결 기능을 적용할 서브넷 범위를 설정합니다. **주의:** 서브넷 별로 지속 연결 기능을 적용하려는 경우에는 부하 분산 방식을 bh로 설정해야 합니다.
8	**fail-skip {enable | disable}** (선택 설정)	바이패스 기능의 사용 여부를 지정합니다. • **enable** 바이패스 기능 활성화 • **disable** 바이패스 기능 비활성화 (기본값)
9	**backup** *<BACKUP>*	설정 중인 L4 캐시 서버 부하 분산 서비스에서 더 이상 서비스 요청을 받을 수 없는 경우, 대신 서비스 요청을 처리할 백업 서비스를 지정합니다. 반드시 이미 생성되어 있는 서비스의 이름을 입력해야 합니다. • *<BACKUP>* 백업 서비스의 이름 **참고:** 설정한 백업 서비스를 L4 캐시 서버 부하 분산 서비스에서 삭제하려면 <CSLB 설정 모드>에서 **no backup** 명령을 실행합니다.
10	**recording-cache {enable | disable}** (선택 설정)	녹취 서버 캐시 기능의 사용 여부를 지정합니다. • **enable** 녹취 서버 캐시 기능 활성화 • **disable** 녹취 서버 캐시 기능 비활성화 (기본값)
11	**transparent-cache {enable | disable}** (선택 설정)	트랜스패런트 캐시 서버 기능의 사용 여부를 지정합니다. • **enable** 트랜스패런트 캐시 서버 기능 활성화 • **disable** 트랜스패런트 캐시 서버 기능 비활성화 (기본값)
12	**status {enable | disable}** (선택 설정)	L4 캐시 서버 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 기능 활성화 • **disable** 부하 분산 서비스 기능 비활성화 (기본값)
13	**current**	L4 캐시 서버 부하 분산 서비스의 설정 정보를 확인합니다.
14	**apply**	L4 캐시 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 L4 캐시 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no cslb** *<NAME>* 명령을 사용합니다.

필터 설정

L4 캐시 서버 부하 분산 서비스를 적용할 트래픽의 필터링할 때 사용할 필터를 설정하는 방법은 방화벽 부하 분산 서비스에서 필터를 설정하는 방법과 동일합니다. 그러므로, 정의한 캐시 서버 부하 분산 서비스의 필터를 설정하는 방법은 **방화벽/VPN 부하 분산 설정** - **CLI에서 설정하기** – **필터 설정** 절의 설명을 참고합니다. L4 캐시 서버 부하 분산 서비스에는 최대 2048개의 다른 필터를 등록할 수 있습니다.

설정 정보 보기

L4 캐시 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

L4 캐시 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 L4 캐시 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show cslb** 명령을 사용합니다. **show cslb** 명령은 현재 PAS-K에 정의된 L4 캐시 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 L4 캐시 서버 부하 분산 서비스의 설정 정보 보기

특정 L4 캐시 서버 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **show cslb** 명령 뒤에 해당 서비스의 이름(<*NAME*>)을 입력하면 됩니다.

L4 캐시 서버 부하 분산 서비스의 모든 설정 정보(실제 서버, 장애 감시, 필터, 세션) 보기

각 L4 캐시 서버 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 필터 설정 정보, 그리고 서비스에 등록된 실제 서버의 설정 정보와 실제 서버를 통해 연결된 세션에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show info cslb** 명령을 사용합니다.

서비스의 이름을 입력하지 않고 **show info cslb** 명령을 실행하면 모든 L4 캐시 서버 부하 분산 서비스에 대한 정보가 출력되고 서비스의 이름을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

게이트웨이 부하 분산 설정

이 절에서는 CLI 에서 PAS-K에 게이트웨이 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: 게이트웨이 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

CLI에서 설정하기

PAS-K에 게이트웨이 부하 분산 기능을 설정하는 과정은 다음과 같습니다.

1. 게이트웨이 부하 분산 서비스 정의
2. 필터 설정하기
3. 설정 정보 보기

2단계의 설정 과정은 [**방화벽/VPN 부하 분산 설정하기**] 절에서 설명한 방화벽 부하 분산 서비스의 필터 설정 방법과 같습니다. 그러므로, 이 절에서는 게이트웨이 부하 분산 서비스를 정의하는 1단계와 설정 정보를 확인하는 3단계의 과정에 대해서 상세하게 설명하도록 합니다.

게이트웨이 부하 분산 서비스 정의

다음은 게이트웨이 부하 분산 서비스를 정의하는 과정입니다. PAS-K에는 게이트웨이 부하 분산 서비스를 포함하여 최대 1024개의 L4 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 게이트웨이 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**gwlb** *<NAME>*	<GWLB 설정 모드>로 들어가서 게이트웨이 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**priority** *<PRIORITY>*	게이트웨이 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위. 설정 범위: 0 ~ 255, (기본값: 100) **참고**: 설정한 우선순위를 기본값으로 변경하려면, <GWLB 설정 모드>에서 **no priority** 명령을 사용합니다.
3	**lb-method** {**ab** | **bh** | **dh** | **lc** | **lc-total**| **rr** | **sh** | **sp** | **wlc** | **wlc-total** | **wrr**}	게이트웨이 부하 분산 서비스에서 사용할 부하 분산 방식을 설정합니다. (기본값: rr)
4	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 실제 서버 ID 설정. 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 게이트웨이 부하 분산 서비스에서 삭제하려면 <GWLB 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
5	**health-check** *<HEALTH-CHECK>*	게이트웨이 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 설정. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시

		ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용.  **참고:** 설정한 장애 감시를 게이트웨이 부하 분산 서비스에서 삭제하려면 <CSLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다.  **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
6	**sticky time** *<TIME>*	sticky 타임아웃 값을 설정합니다. 지정한 sticky 타임아웃이 경과한 후 연결 엔트리가 소멸되기 전에 동일한 클라이언트로부터의 연결이 시도되면 이전에 연결했던 게이트웨이 라인과 동일한 게이트웨이 라인으로 연결됩니다. Sticky 타임아웃을 '0'으로 설정하면 지속 연결 기능을 사용하지 않습니다. • *<TIME>* sticky 타임아웃 값 설정. (설정 범위: 0 ~ 65535(초), 기본값: 60(초))
7	**sticky source-subnet** *<SOURCE-SUBNET>* **sticky destination-subnet** *<DESTINATION-SUBNET>*	기본적으로 지속 연결 기능은 출발지 IP 주소별로 적용됩니다. 지속 연결 기능을 출발지 서브넷 별로 적용하려면 **sticky source-subnet** 명령을 사용하고, 목적지 서브넷 별로 적용하려면 **sticky destination-subnet** 명령을 사용하여 지속 연결 기능을 적용할 서브넷 범위를 설정합니다.  **주의:** 서브넷 별로 지속 연결 기능을 적용하려는 경우에는 부하 분산 방식을 bh, dh, sh 중 하나로 설정해야 합니다.
8	**fail-skip** {**enable** | **disable**} (선택 설정)	바이패스 기능의 사용 여부를 지정합니다. • **enable** 바이패스 기능 활성화 • **disable** 바이패스 기능 비활성화 (기본값)
	backup *<BACKUP>*	설정 중인 게이트웨이 부하 분산 서비스에서 더 이상 서비스 요청을 받을 수 없는 경우, 대신 서비스 요청을 처리할 백업 서비스를 지정합니다. 반드시 이미 생성되어 있는 서비스의 이름을 입력해야 합니다. • *<BACKUP>* 백업 서비스의 이름  **참고:** 설정한 백업 서비스를 게이트웨이 부하 분산 서비스에서 삭제하려면 <GWLB 설정 모드>에서 **no backup** 명령을 실행합니다.
9	**status** {**enable** | **disable**} (선택 설정)	게이트웨이 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 기능 활성화 (기본값) • **disable** 부하 분산 서비스 기능 비활성화
10	**current**	게이트웨이 부하 분산 서비스의 설정 정보를 확인합니다.
11	**apply**	게이트웨이 부하 분산 서비스를 저장하고 시스템에 적용합니다.

 **참고:** 정의한 게이트웨이 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no gwlb** *<NAME>* 명령을 사용합니다.

필터 설정

게이트웨이 부하 분산 서비스를 적용할 트래픽을 필터링할 때 사용할 필터를 설정하는 방법은 방화벽 부하 분산 서비스에서 필터를 설정하는 방법과 동일합니다. 그러므로, 정의한 게이트웨이 부하 분산 서비스의 필터를 설정하는 방법은 **방화벽/VPN 부하 분산 설정** - **CLI에서 설정하기** – **필터 설정** 절의 설명을 참고합니다. 게이트웨이 부하 분산 서비스에는 최대 2048개의 다른 필터를 등록할 수 있습니다.

설정 정보 보기

게이트웨이 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

게이트웨이 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 게이트웨이 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show gwlb** 명령을 사용합니다. **show gwlb** 명령은 현재 PAS-K에 정의된 게이트웨이 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 게이트웨이 부하 분산 서비스의 설정 정보 보기

특정한 게이트웨이 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **show gwlb** 명령 뒤에 해당 서비스의 이름(<*NAME*>)을 입력하면 됩니다.

게이트웨이 부하 분산 서비스의 모든 설정 정보(실제 서버, 장애 감시, 필터, 세션) 보기

각 게이트웨이 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 필터 정보, 그리고 서비스에 등록된 실제 서버의 설정 정보와 실제 서버를 통해 연결된 세션에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show info gwlb** 명령을 사용합니다.

서비스의 이름을 입력하지 않고 **show info gwlb** 명령을 실행하면 모든 게이트웨이 부하 분산 서비스에 대한 정보가 출력되고 서비스의 이름을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

글로벌 서버 부하 분산 설정

이 절에서는 CLI에서 PAS-K에 글로벌 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: 글로벌 서버 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

설정 시 주의 사항

다음은 글로벌 서버 부하 분산 기능 설정 시 주의 사항입니다. 글로벌 서버 부하 분산 기능을 설정하기 전에 반드시 이 사항들을 읽고 숙지하도록 합니다.

- 반드시 PAS-K를 외부의 상위 DNS 서버에 네임 서버로 등록해야 합니다. 네임 서버로 등록할 때 사용하는 네임 서버 IP 주소는 글로벌 서버 부하 분산의 네임 서버 설정에서 지정한 IP 주소여야 하고, PAS-K에도 외부 DNS 서버에 등록한 것과 동일한 네임 서버 정보를 등록해야 합니다.
- 웹 호스팅 서비스를 받는 경우에는 웹 호스팅 업체에 서비스를 원하는 특정 호스트에 대한 DNS 서버 호스팅이 가능한지를 문의하고, 가능할 경우에만 글로벌 서버 부하 분산 서비스를 적용할 수 있습니다.

CLI에서 설정하기

PAS-K에 글로벌 서버 부하 분산 기능을 설정하는 과정은 다음과 같습니다.

1. 글로벌 서버 부하 분산 서비스 정의
2. 네임 서버 설정
3. 그룹 설정
4. 규칙 설정
5. 설정 정보 보기

각 단계별 설정 방법을 차례로 살펴봅니다.

글로벌 서버 부하 분산 서비스 정의

다음은 하나의 글로벌 서버 부하 분산 서비스를 설정하는 과정입니다. 여러 개의 글로벌 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**gslb** *<NAME>*	<GSLB 설정 모드>로 들어가서 글로벌 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**zone** *<ZONE>* (필수 설정)	글로벌 서버 부하 분산 서비스의 영역을 설정합니다. • *<ZONE>* A-Z, a-z, 0-9, -, _, . 사용하여 최대 253 글자까지 지정 가능, 단, 전부 숫자이거나 시작과 끝에 하이픈 사용 불가.
3	**health-check** *<HEALTH-CHECK>*	글로벌 서버 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 설정. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구

		분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 글로벌 서버 부하 분산 서비스에서 삭제하려면 <GSLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
4	**status {enable | disable}** (선택 설정)	글로벌 서버 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 글로벌 서버 부하 분산 서비스 기능 활성화 (기본값) • **disable** 글로벌 서버 부하 분산 서비스 기능 비활성화
5	**current**	글로벌 서버 부하 분산 서비스의 설정 정보를 확인합니다.
6	**apply**	글로벌 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 글로벌 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no gslb** *<NAME>* 명령을 사용합니다.

네임 서버 설정

글로벌 서버 부하 분산 서비스를 설정한 후에는 PAS-K가 수신된 DNS 질의에 응답할 네임 서버로 동작할 수 있도록 네임 서버를 설정합니다. 네임 서버를 정의하고, 네임 서버의 이름과 IP 주소, TTL 값을 설정합니다. 외부의 상위 DNS 서버에서 PAS-K로 DNS 질의를 보내기 위해서는 반드시 정의한 네임 서버의 IP 주소를 외부의 상위 DNS 서버에 등록해야 합니다. 다음은 글로벌 서버 부하 분산 서비스의 네임 서버를 설정하는 방법입니다. 하나의 글로벌 서버 부하 분산서비스에는 최대 16개의 네임 서버를 정의할 수 있으므로, 여러 개의 네임 서버를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**gslb** *<NAME>*	<GSLB 설정 모드>로 들어갑니다. • *<NAME>* 네임 서버를 설정할 글로벌 서버 부하 분산 서비스 이름
2	**name-server** *<ID>*	<Name-Server 설정 모드>로 들어갑니다. • *<ID>* 네임 서버의 ID. 설정 범위: 1 ~ 16
3	**name** *<NAME>*	네임 서버의 이름을 설정합니다. • *<NAME>* 알파벳과 숫자를 사용하여 최대 32 글자까지 지정 가능. 단, 첫 글자는 반드시 알파벳 사용
4	**ip** *<IP>*	네임 서버의 IP 주소를 설정합니다. 네임 서버의 IP 주소는 상위 DNS 서버에 등록할 때 사용됩니다. (혹은 이미 상위 DNS 서버에 등록된 IP 주소를 설정합니다.) 영역에 속한 도메인에 대한 요청을 DNS 서버가 수신하면, DNS 서버는 이 주소로 PAS-K에게 요청을 전송합니다. • *<IP>* 네임 서버의 IP 주소. **주의:** 이 주소는 PAS-K의 게이트웨이 라인의 IP 주소이어야 하고, 반드시 PAS-K의 인터페이스에 설정되지 않은 고정 IP 주소이어야 합니다.
5	**ttl** *<TTL>*	네임 서버의 TTL 값을 설정합니다. 클라이언트는 PAS-K가 전송한 주소 정보를 설정한 TTL 시간 동안 유지할 수 있습니다. • *<TTL>* 네임 서버의 TTL 값 설정. 설정 범위: 1 ~ 65535(초), 기본값: 10(초)
6	**status {enable | disable}** (선택 설정)	네임 서버의 사용 여부를 지정합니다. • **enable** 네임 서버 활성화 (기본값) • **disable** 네임 서버 비활성화
7	**current**	네임 서버의 설정 정보를 확인합니다.
8	**apply**	네임 서버를 저장하고 시스템에 적용합니다.

참고: 설정한 네임 서버를 삭제하려면 <GSLB 설정 모드>에서 **no name-server** *<ID>* 명령을 사용합니다.

그룹 설정

글로벌 서버 부하 분산 서비스를 정의한 후에는 실제 서버의 그룹(Group)을 설정할 수 있습니다. 글로벌 서버 부하 분산 서비스에서는 그룹별로 별도의 부하 분산 방식을 설정합니다. 하나의 글로벌 서버 부하 분산 서비스에는 최대 16 개의 그룹을 설정할 수 있으므로, 여러 개의 그룹을 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**gslb** *<NAME>*	<GSLB 설정 모드>로 들어갑니다. • *<NAME>* 그룹을 설정할 글로벌 서버 부하 분산 서비스 이름
2	**group** *<ID>*	<Group 설정 모드>로 들어갑니다. • *<ID>* 그룹의 ID. (설정 범위: 1 ~ 16)
3	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 실제 서버 ID 설정. 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 그룹에서 삭제하려면 <Group 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
4	**lb-method type** {**ab** | **rr** | **sp**}	그룹에 속한 실제 서버로 부하를 분산시킬 때 사용할 부하 분산 방식을 설정합니다. (기본값: rr)
5	**current**	그룹의 설정 정보를 확인합니다.
6	**apply**	그룹을 저장하고 시스템에 적용합니다.

참고: 설정한 그룹을 삭제하려면 <GSLB 설정 모드>에서 **no group** *<ID>* 명령을 사용합니다.

규칙 설정

그룹을 설정한 후에는 규칙을 설정합니다. 앞에서 정의한 실제 서버 그룹에 글로벌 서버 부하 분산 서비스를 적용하려면, 실제 서버 그룹이 최소한 하나의 규칙에 포함되어 있어야 합니다. 규칙을 설정할 때에는 규칙을 생성하고, 실제 서버의 이름과 IP 주소, MAC 주소, 서비스 IP 주소, 가중치, 인터페이스 등을 설정합니다. 하나의 글로벌 서버 부하 분산 서비스에는 최대 16개의 규칙을 등록할 수 있으므로, 여러 개의 규칙을 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**gslb** *<NAME>*	<GSLB 설정 모드>로 들어갑니다. • *<NAME>* 규칙을 설정할 글로벌 서버 부하 분산 서비스 이름
2	**rule** *<ID>*	글로벌 서버 부하 분산 서비스의 규칙을 정의하고, <Rule 설정 모드>로 들어갑니다. • *<ID>* 규칙의 ID. (설정 범위: 1 ~ 16)
3	**host** *<HOST>*	DNS 요청에 응답할 서비스 도메인(정확히는 호스트)을 설정합니다. 정보를 서비스할 도메인은 이 명령을 사용하여 지정한 domain.<글로벌 서버 부하 분산 부하 분산 서비스의 영역>이 됩니다. • *<HOST>* A-Z, a-z, 0-9, -, _, .을 사용하여 최대 253 글자까지 지정 가능, 단, 전부 숫자이거나 시작과 끝에 하이픈 사용 불가.
4	**group** *<ID>* (필수 설정)	현재 설정 중인 규칙을 적용할 실제 서버 그룹을 설정합니다. • *<ID>* 그룹의 ID 를 콤마로 구분
5	**ttl** *<TTL>*	규칙의 TTL 값을 설정합니다. 클라이언트는 PAS-K가 전송한 주소 정보를 설정한 TTL 시간 동안 유지할 수 있습니다. • *<TTL>* 규칙의 TTL 값 설정. (설정 범위: 1 ~ 65535(초), 기본값: 10(초))
6	**status** {**enable** | **disable**} (선택 설정)	규칙을 글로벌 부하 분산 서비스에 사용 여부를 지정합니다. • **enable** 규칙 활성화 (기본값) • **disable** 규칙 비활성화
7	**current**	규칙의 설정 정보를 확인합니다.
8	**apply**	규칙을 저장하고 시스템에 적용합니다.

참고: 설정한 규칙을 삭제하려면 <GSLB 설정 모드>에서 **no rule** *<ID>* 명령을 사용합니다.

설정 정보 보기

글로벌 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

글로벌 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 글로벌 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show gslb** 명령을 사용합니다. **show gslb** 명령은 현재 PAS-K에 정의된 글로벌 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 글로벌 서버 부하 분산 서비스의 설정 정보 보기

특정한 글로벌 서버 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **show gslb** 명령 뒤에 해당 서비스의 이름(<*NAME*>)을 입력하면 됩니다.

글로벌 서버 부하 분산 서비스의 모든 설정 정보 (실제 서버, 장애 감시, 세션 설정) 보기

각 글로벌 서버 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 그리고 서비스에 등록된 실제 서버에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show info gslb** 명령을 사용합니다.

서비스의 이름을 입력하지 않고 **show info gslb** 명령을 실행하면 모든 글로벌 서버 부하 분산 서비스에 대한 정보가 출력되고 서비스의 이름을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

L7 서버 부하 분산 설정

이 절에서는 CLI에서 PAS-K에 L7 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: L7 서버 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

CLI에서 설정하기

PAS-K에 L7 서버 부하 분산을 설정하는 과정은 다음과 같습니다.

1. 패턴 정의
2. L7 서버 부하 분산 서비스 정의
3. 그룹 설정
4. 규칙 설정
5. URL 변경 설정
6. 설정 정보 보기

각 단계 별 설정 방법을 차례로 살펴봅니다.

패턴 정의

다음은 L7 부하 분산 서비스를 제공할 트래픽(HTTP 요청)을 선택하는데 사용될 패턴을 정의하는과정입니다. PAS-K에는 최대 512개의 패턴을 등록할 수 있으므로, 여러 개의 패턴을 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**layer7 pattern** *<ID>*	패턴을 정의할 수 있는 <Pattern 설정 모드>로 들어갑니다. • *<ID>* 정의할 패턴의 ID. 설정 범위: 1 ~ 512
2	**type {accept-language | cookie | dest-ip | host | method | source-ip | uri | user-agent | user-defined | version}**	패턴의 매치 기준이 되는 HTTP 패킷 헤더의 필드를 설정합니다.(기본값: uri) **참고:** 지정한 매치 종류에 따라 다음과 같은 과정을 수행합니다. · **accept-language**, **cookie**, **host**, **method**, **uri**, **user-agent** : 3~4번 과정 · **user-defined** : 3~5번 과정 · **dest-ip** : 6번 과정 · **source-ip** : 7번 과정 · **version** : 8번 과정
3	**string** *<STRING>*	HTTP 요청 헤더에서 매치 종류에 지정한 값과 비교할 문자열을 설정합니다. • *<STRING>* 패턴의 문자열을 최대 127 자까지 지정. 문자열에는 큰 따옴표(")를 제외한 모든 문자 사용 가능.
4	**match {any | prefix | regex | suffix}**	패턴의 문자열과 HTTP 요청의 헤더 필드를 비교할 방법을 설정합니다 • **prefix** 헤더의 해당 필드가 해당 문자열로 시작하는지 검사합니다. • **suffix** 헤더의 해당 필드가 해당 문자열로 끝나는지 검사합니다. • **regex** 헤더의 해당 필드가 지정된 정규식(regular expression)과 일치하는지 검사합니다. **any** 헤더의 해당 필드에 해당 문자열이 포함되어 있는지 검사합니다. (기본값)

5	**user-defined** *<USER-DEFINED>*	패턴 매치 기준을 user-defined로 설정한 경우에는 헤더 필드의 이름을 설정합니다. 필드의 이름을 입력할 때에는 대소문자를 구분해야 합니다. • *<USER-DEFINED>* 헤더 필드의 이름. 알파벳, 숫자, 특수문자 포함하여 최대 127 자 까지 설정 가능.
6	**dest-ip** *<DEST-IP>*	패턴 매치 기준을 dest-ip 로 설정한 경우에는 HTTP 트래픽의 목적지 IP 주소와 넷 마스크 비트 수를 설정합니다 • *<DEST-IP>* 목적지 IP 주소 및 서브넷 마스크 비트 수
7	**source-ip** *<SOURCE-IP>*	패턴 매치 기준을 source-ip 로 설정한 경우에는 HTTP 트래픽의 출발지 IP 주소와 넷 마스크 비트 수를 입력합니다. • *<SOURCE-IP>* 출발지 IP 주소 및 서브넷 마스크 비트 수
8	**version {http1.0 | http1.1}**	패턴 매치 기준을 version 으로 설정한 경우에는 PAS-K 가 HTTP/1.0 요청과 HTTP/1.1 요청을 구분하여 처리할 수 있도록 HTTP 버전을 설정합니다 (기본값: http1.0)
9	**current**	패턴의 설정 정보를 확인합니다.
10	**apply**	패턴을 저장하고 시스템에 적용합니다.

참고: 정의한 패턴을 삭제하려면 <Configuration 모드>에서 **no layer7 pattern** *<ID>*명령을 사용합니다.

패턴 정보 출력

시스템에 정의되어 있는 패턴의 목록이나 각 패턴에 대한 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show layer7 pattern** 명령을 사용합니다. 특정한 패턴에 대한 설정 정보를 확인하려면, **show layer7 pattern** 명령 뒤에 해당 패턴의 ID를 함께 입력합니다.

L7 서버 부하 분산 서비스 정의

새로운 L7 서버 부하 분산 서비스를 정의하는 방법은 다음과 같습니다. PAS-K에는 L7 서버 부하 분산 서비스를 포함하여 최대 1024개의 L7 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 L7 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**l7slb** *<NAME>*	<L7SLB 설정 모드>로 들어가서 L7 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**vip** *<IP>* **vport** *<VPORT>*	L7 서버 부하 분산 서비스의 가상 IP 주소와 가상 포트를 설정합니다. 여러 개의 가상 포트를 지정하고자 하는 경우에는 ','로 구분하여 입력합니다. • *<IP>* 가상 IP 주소를 입력. 최소 1 개에서 최대 128 개의 IP 주소 지정 • *<VPORT>* 가상 포트 입력. 최대 32 개의 포트 지정. 설정 범위: 1 ~ 65535 **참고:** 최소 1개 이상의 가상 IP 주소와 가상 포트를 설정해야 하며, 설정한 가상 IP 주소와 가상 포트를 삭제하려면 <L7SLB 설정 모드>에서 **no vip** *<IP>* **vport** *<VPORT>* 명령을 실행합니다.
3	**priority** *<PRIORITY>*	L7 서버 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위. 설정 범위: 0 ~ 255, 기본값: 100 **참고**: 설정한 우선순위를 기본값으로 변경하려면, <L7SLB 설정 모드>에서 **no priority** 명령을 실행합니다.
4	**health-check** *<HEALTH-CHECK>*	L7 서버 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 설정. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 L7 서버 부하 분산 서비스에서 삭제하려면 <L7SLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
5	**keep-backup** {**all** | **entry** | **none**}	부하 분산 서비스의 실제 서버에 백업 실제 서버를 설정한 경우, 마스터 실제 서버가 다시 동작 가능한 상태가 되었을 때 백업 실제 서버의 세션을 어떻게 처리할 것인지를 설정합니다. • **none** 백업 실제 서버의 모든 세션 엔트리를 삭제 • **entry** 지속 연결 엔트리만 삭제 • **all** 모든 세션 엔트리를 그대로 유지 (기본값)
6	**server-min-mtu** *<SERVER-MIN-MTU>*	MTU 값을 변경합니다. PAS-K는 클라이언트와 세션을 연결할 때 기본적으로 MTU 값을 1500으로 사용합니다. 실제 서버 중에 MTU 값이 1500보다 작은 서버가 있는 경우에는 값을 변경해주어야 합니다. • *<SERVER-MIN-MTU>* MTU 값. 설정 범위: 60 ~ 1500, 기본값: 1500 **참고:** 부하 분산 서비스의 그룹에 속한 실제 서버들의 MTU 중에서 가장 낮은 MTU 값을 입력합니다.

7	**connection-pooling {enable | disable}**	커넥션 풀링 기능을 사용하여 저장해 두었던 커넥션을 재사용할 지의 여부를 설정합니다. • **enable** 클라이언트와 실제 서버간에 TCP 커넥션을 연결할 때 생성된 커넥션을 풀에 저장해 두었다가 클라이언트로부터 요청이 있을 경우 재사용 (기본값) • **disable** IP 주소와 포트 번호가 같은 경우에만 커넥션을 재사용
8	**age-refresh {enable | disable}**	커넥션 풀링 기능을 설정한 경우, 커넥션을 재사용 할 때 마다 시간을 업데이트 해줄지의 여부를 설정합니다. • **enable** 커넥션을 재사용 할 때 마다 커넥션의 시간을 업데이트함 • **disable** 커넥션을 재사용하여도 시간을 업데이트 하지않음 (기본값)
9	**x-header {enable | disable}**	'X-Forwarded-For' 헤더를 삽입할 지의 여부를 설정합니다. PAS-K가 Source NAT를 수행 할 경우, 서버에서 기존의 클라이언트 IP를 알기 위해서는 HTTP 요청에 'X-Forwarded-For' 헤더를 추가해야 합니다. • **enable** 'X-Forwarded-For' 헤더 삽입 • **disable** 'X-Forwarded-For' 헤더 삽입하지 않음 (기본값)
10	**status {enable | disable}** (선택 설정)	부하 분산 서비스의 사용 여부를 지정합니다. • **enable** L7 서버 부하 분산 서비스 활성화 (기본값) • **disable** L7 서버 부하 분산 서비스 비활성화
11	**current**	L7 서버 부하 분산 서비스의 설정 정보를 확인합니다.
12	**apply**	L7 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 L7 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no l7slb** *<NAME>* 명령을 사용합니다.

그룹 설정

L7 서버 부하 분산 서비스를 정의한 후에는 실제 서버의 그룹(Group)을 설정할 수 있습니다. L4 부하 분산 서비스에서는 서비스마다 부하 분산 방식을 지정하지만, L7 서버 부하 분산 서비스에서는 그룹별로 별도의 부하 분산 방식을 설정합니다. 그리고, 지속 연결 기능의 적용도 그룹 단위로 이루어집니다. 하나의 L7 서버 부하 분산 서비스에는 최대 256 개의 그룹을 설정할 수 있으므로, 여러 개의 그룹을 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**l7slb** *<NAME>*	<L7SLB 설정 모드>로 들어갑니다. • *<NAME>* 그룹을 설정할 L7 서버 부하 분산 서비스 이름
2	**group** *<NAME>*	<Group 설정 모드>로 들어갑니다. • *<NAME>* 알파벳과 숫자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용
3	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. 이 실제 서버의 ID는 반드시 이미 정의되어 있는 것 중 선택해야 합니다. • *<ID>* 실제 서버 ID 설정. 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ‘,’로 구분하고, 연속된 실제 서버 ID 는 ‘-’를 사용. **참고:** 설정한 실제 서버를 그룹에서 삭제하려면 <L7SLB 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
4	**lb-method type** {**lc** | **mw** | **rr** | **sh** | **urlhash** | **wlc** | **wrr**}	그룹에 속한 서버로 부하를 분산시킬 때 사용할 부하 분산 방식을 설정합니다. 기본값: rr
4-1	**lb-method urlhash** {**offset** *<OFFSET>* | **starter** *<STARTER>*} [{**length** *<LENGTH>* | **terminator** <TERMINATOR>}]	4번 과정에서 부하 분산 방식을 urlhash 로 지정한 경우에는 URL에서 사용자가 원하는 특정 부분의 문자열을 추출하여 hash를 수행하고, 부하 분산을 하도록 설정할 수 있습니다. URI에서 부분 문자열을 추출할 위치를 지정할 경우에 사용할 수 있는 옵션에는 offset, starter, length, terminator가 있습니다. offset, starter 옵션을 사용하면 추출할 문자열의 시작 위치를 설정할 수 있습니다. • *<OFFSET>* URI 에서 추출할 문자열의 시작 위치. 첫번째 문자부터 사용하려면 시작 위치의 값을 ‘1’로 지정. 설정범위: 1 ~ 1024 • *<STARTER>* URI 에서 추출하려는 시작 문자열을 입력합니다. 입력한 문자열 자체는 포함되지 않고 그 다음 글자부터 추출됩니다. 알파벳과 숫자, 그리고 작은 따옴표(')를 제외한 특수 문자로 구성된 최대 128 글자의 문자열 입력 가능 추출할 문자열의 끝 위치를 설정하려면 length, terminator 옵션을 사용합니다. • *<LENGTH>* URI 에서 추출할 문자열의 시작 위치부터 끝 위치까지의 길이를 입력합니다. 설정 범위: 1 ~ 1024 • *<TERMINATOR>* URI 에서 추출하려는 끝 문자열을 입력합니다. 입력한 문자열 자체는 포함되지 않고 그 전 글자까지 사용됩니다. 알파벳과 숫자, 그리고 작은 따옴표(')를 제외한 특수 문자로 구성된 최대 128 글자의 문자열 입력 가능
5	**persist type** {**cookie** | **field** | **ip**}	클라이언트가 이전에 연결했던 서버와 계속 연결할 수 있게 해주는 지속 연결 기능을 설정합니다. • **cookie** HTTP 쿠키 지속 연결 기능 사용 • **field** HTTP 헤더 지속 연결 기능을 사용 • **ip** IP 지속 연결 기능을 사용
5-1	**persist cookie type** {**hash** | **insert** | **passive** | **rewrite**}	5번 과정에서 지속 연결 기능을 cookie로 지정한 경우에는 hash, insert, passive, rewrite 옵션 중 하나를 설정합니다.

5-2	**persist cookie hash name** *<NAME>* **persist cookie hash** {**offset** *<OFFSET>* | **length** *<LENGTH>*}	5-1번 과정에서 hash 옵션을 지정한 경우에는 쿠키 이름을 설정합니다. • *<NAME>* 쿠키를 PAS-K 에 저장할 때 사용할 이름. 쿠키의 일부만 저장하려는 경우에는 쿠키의 시작 위치와 길이를 설정합니다. • *<OFFSET>* 저장할 쿠키의 시작 위치를 설정합니다. 설정 범위: 1 ~ 64 • *<LENGTH>* 저장할 쿠키의 길이를 설정합니다. 설정 범위: 1 ~ 64
5-3	**persist field name** *<NAME>* **persist field** [{**offset** *<OFFSET>* | **starter** *<STARTER>*}] | [{**length** *<LENGTH>* | **terminator** *<TERMINATOR>*}]	5번 과정에서 지속 연결 기능을 field로 지정한 경우에는 HTTP 헤더 이름을 설정합니다. • *<NAME>* 지속 연결에 사용할 필드의 이름을 설정합니다. HTTP 헤더에서 사용자가 원하는 특정 부분의 문자열을 추출하여 hash를 수행하고, 부하 분산을 하도록 설정할 수 있습니다. HTTP 헤더에서 부분 문자열을 추출할 위치를 지정할 경우에 사용할 수 있는 옵션에는 offset, starter, length, terminator가 있습니다. • *<OFFSET>* URI 에서 추출할 문자열의 시작 위치를 설정합니다. 설정 범위: 1 ~ 1024 • *<STARTER>* 추출하려는 시작 문자열을 입력합니다. 알파벳과 숫자, 그리고 작은 따옴표(')를 제외한 특수 문자로 구성된 최대 128 글자의 문자열 입력 가능. • *<LENGTH>* 추출할 문자열의 시작 위치부터 끝 위치까지의 길이를 입력합니다. 설정 범위: 1 ~ 1024 • *<TERMINATOR>* 추출하려는 끝 문자열을 입력합니다. 알파벳과 숫자, 그리고 작은 따옴표(')를 제외한 특수 문자로 구성된 최대 128 글자의 문자열 입력 가능 **참고:** 만약 시작 위치가 HTTP 헤더 필드 값의 전체 문자열의 길이를 초과하거나 지정한 시작 문자열이 HTTP 헤더 필드 값에서 발견되지 않는 경우 지속 연결 엔트리를 생성하지 않습니다.
6	**persist timeout** *<TIMEOUT>*	지속 연결 엔트리의 지속 시간을 설정합니다. • *<TIMEOUT>* 지속 시간을 일, 시간, 분, 초([[[dd]:hh]:mm]:ss)의 순서로 입력합니다. 설정 범위: 1 ~ 65535, 기본값: 0(초)
7	**persist overmax** {**enable** | **disable**}	부하 분산 서비스의 실제 서버에 최대 세션 기능을 사용하는 경우(최대 세션 개수를 설정한 경우), 실제 서버가 FULL 상태가 되었을 때 지속 연결 엔트리의 처리 방법을 설정합니다. • **enable** 실제 서버가 FULL 상태가 되어도 지속 연결 엔트리는 최대 연결 개수의 제한을 받지 않도록 하여 지속 연결 기능을 계속 지원함(기본값). • **disable** 실제 서버가 FULL 상태가 되는 경우 더 이상 해당 실제 서버에 지속 연결 기능을 지원하지 않음
8	**current**	그룹의 설정 정보를 확인합니다.
9	**apply**	그룹을 저장하고 시스템에 적용합니다.

참고: offset 또는 starter 옵션을 사용하여 추출할 문자열의 시작 위치를 설정하지 않은 경우에는 URI의 첫글자부터 추출되고, length, terminator 옵션을 사용하여 끝 위치를 설정하지 않은 경우에는 URI의 마지막 글자까지 추출됩니다.

주의: offset, starter, length, terminator 옵션을 사용하여 부분 문자열을 추출할 위치를 지정할 경우에, 다음과 같은 6가지 예외 상황이 있습니다.
- 예외 1: offset이 URI의 길이를 초과하는 경우에는 문자열 맨 처음부터 시작
- 예외 2: starter가 URI에서 발견되지 않으면 문자열 맨 처음부터 시작
- 예외 3: starter가 URI에서 여러 번 발견되는 경우 처음 발견된 부분부터 시작
- 예외 4: 시작 위치부터 length가 URI의 끝을 넘어가는 경우, URI의 끝까지만 사용
- 예외 5: terminator가 발견되지 않으면 URI의 맨 끝까지 사용
- 예외 6: terminator가 여러 번 발견되는 경우 맨 처음 발견된 부분까지 사용

참고: 다음은 offset, starter, length, terminator 옵션을 사용하여 URI가 /abcdabcefghalmv인 경우에 hash가 적용될 부분 문자열을 나타낸 예입니다.

```
(config-l7slb[web]-group[all])# lb-method urlhash
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash offset 3
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash starter bce
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash length 6
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash terminator hal
/abcdabcefghalmv
config-l7slb[web]-group[all])# lb-method urlhash offset 30 (예외 1)
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash starter def (예외 2)
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash starter bc (예외 3)
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash length 50 (예외 4)
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash terminator zzz (예외 5)
/abcdabcefghalmv
(config-l7slb[web]-group[all])# lb-method urlhash terminator bc (예외 6)
/abcdabcefghalmv
```

참고: 지속 연결 기능을 사용하지 않으려면 <Group 설정 모드>에서 **no persist** 명령을 실행하면 됩니다.

주의: HTTP 쿠키 지속 연결 기능을 사용하는 경우에는 PAS-K를 사용하고 있는 국가의 시간대(timezone)를 PAS-K에 설정해야 합니다. 시간대는 Configuration 모드에서 다음과 같은 **timezone** 명령을 사용하여 설정할 수 있습니다.

```
timezone {+8 | +9}
```

PAS-K가 설치된 지역이 중국인 경우에는 '+8'을 지정하고, 한국 또는 일본인 경우에는 '+9'를 설정합니다. 변경한 시간대는 **show clock** 명령을 통해 확인할 수 있습니다. 다음은 PAS-K의 시간대를 GMT 시간보다 8시간 빠른 시간대로 설정한 후 결과를 확인하는 예입니다.

```
(config)# timezone +8
Timezone is applied to system.
(config)# show timezone
================================================================================
  TIMEZONE
 --------------------------------------------------------------------------------
   Timezone           : +8
================================================================================
(config)#
```

PAS-K는 기본적으로 GMT 시간보다 9시간 빠른 시간대(GMT +9)로 설정되어 있습니다.

참고: L7 서버 부하 분산 서비스에서 그룹을 삭제하려면 <L7 SLB 설정 모드>에서 **no group** <*NAME*> 명령을 사용합니다.

규칙 설정

규칙(Rule)은 특정 패턴과 일치하는 HTTP 요청에 대해 어떠한 동작을 수행할 것인지 정의한 것입니다. 예를 들어, URI가 /image라는 문자열로 시작(패턴)하는 HTTP 요청이 Image라는 서버 그룹(그룹)으로 전송되도록 규칙을 정의할 수 있습니다.

L7 서버 부하 분산 서비스에 속하는 그룹에 적용할 규칙을 정의하는 방법은 다음과 같습니다. 하나의 L7 서버 부하 분산 서비스에는 최대 256개의 규칙을 등록할 수 있으므로, 여러 개의 규칙을 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**l7slb** *<NAME>*	<L7SLB 설정 모드>로 들어갑니다. • *<NAME>* 규칙을 설정할 L7 서버 부하 분산 서비스 이름
2	**rule** *<ID>*	<Rule 설정 모드>로 들어갑니다. • *<ID>* 규칙의 ID 설정. (설정 범위: 1 ~ 256)
3	**priority** *<PRIORITY>*	그룹에 적용될 규칙의 우선순위를 설정합니다. 여러 개의 규칙이 그룹에 정의된 경우에는 우선순위가 높은 규칙부터 차례로 적용됩니다. 값이 작을수록 우선순위는 더 높습니다. • *<PRIORITY>* 우선순위 설정. (설정 범위: 0 ~ 255, 기본값: 0) **참고**: 설정한 우선순위를 기본값으로 변경하려면, <Rule 설정 모드>에서 **no priority** 명령을 사용합니다.
4	**pattern** *<PATTERN>*	규칙에서 사용할 패턴을 설정합니다. 하나의 규칙에는 논리식을 사용하여 최대 32개의 패턴을 등록할 수 있습니다. • *<PATTERN>* 규칙에서 사용할 패턴의 ID 나 논리식 입력. 논리식을 사용하는 경우에는 'not, and, xor, or' 연산자를 사용하거나 계산 순서를 명확히 하기 위해서 괄호를 사용할 수도 있습니다. 2 개 이상의 패턴을 등록하는 경우에는 논리 연산자를 사용해야 합니다. 연산자의 우선순위는 not 이 제일 높고, and, xor, or 순으로 낮아집니다. 논리식의 시작과 끝은 큰따옴표(")를 사용하여 표시해야 합니다. 예) "1 or (not 2)" **참고:** 설정한 패턴을 규칙에서 삭제하려면 <Rule 설정 모드>에서 **no pattern** 명령을 사용합니다.
5	**action {group | http-response | real | reject}**	규칙에 따라 취할 액션을 설정합니다. • **group** 해당 그룹 내에서 부하 분산을 수행하도록 지정 (기본값) • **real** 사용자가 해당 그룹 내에서 실제 서버를 직접 선택하도록 지정 • **reject** PAS-K 가 TCP RST 패킷을 생성하여 클라이언트에게 전송하도록 지정 • **http-response** PAS-K 가 직접 HTTP 응답을 생성하여 클라이언트에게 전송하도록 지정 **참고:** L7 캐시 서버 부하 분산 서비스에 사용할 규칙에는 **bypass** 액션을 사용하여 요청이 캐시 서버를 경유하지 않고, 바로 실제 목적지로 전송되도록 설정할 수 있습니다.
6	**http-status** *<STATUS>*	액션이 HTTP Response인 경우, HTTP 상태 코드를 설정합니다. • *<STATUS>* HTTP 상태 코드의 종류를 입력. (사용 가능 상태 코드: 301, 302, 307, 400, 403, 404, 503) **참고:** 상태 코드에 대한 상세한 설명은 이 장의 [**L7 부하 분산 – 규칙(Rule) – 액션(Action) – HTTP Response**] 절을 참고하시기 바랍니다.
7	**group** *<GROUP>*	액션이 group이나 real인 경우, 요청을 처리할 그룹을 설정합니다. 반드시 이미 정의되어 있는 그룹의 이름을 입력해야 합니다. • *<GROUP>* 그룹의 이름.

8	**real** *<REAL>*	액션이 real인 경우, 요청을 처리할 실제 서버를 직접 설정합니다. 반드시 이미 정의되어 있는 실제 서버의 ID를 입력해야 하며, 해당 실제 서버는 7번 과정에서 지정한 그룹 내에 포함되어 있어야 합니다. • *<REAL>* 실제 서버 ID. 설정 범위: 1 ~ 2048
9	**backup-group** *<BACKUP-GROUP>*	7번 과정에서 지정한 그룹에 속한 실제 서버가 모두 INACTIVE이거나 FULL 상태일 경우, 대신 서비스를 제공할 그룹(백업 그룹)을 설정합니다. 반드시 이미 정의되어 있는 그룹의 이름을 입력해야 합니다. • *<BACKUP-GROUP>* 백업으로 설정할 그룹의 이름 설정.
10	**status** {**enable** | **disable**} (선택 설정)	규칙의 사용 여부를 지정합니다. • **enable** 규칙 활성화 (기본값) • **disable** 규칙 비활성화
11	**current**	규칙의 설정 정보를 확인합니다.
12	**apply**	규칙을 저장하고 시스템에 적용합니다.

참고: 설정한 규칙을 삭제하려면 <L7SLB 설정 모드>에서 **no rule** *<ID>* 명령을 사용합니다.

URL 변경 설정

URL 변경 기능을 설정하면 PAS-K가 자동으로 클라이언트와 서버의 사이에서 URL을 변경해줍니다. L7 서버 부하 분산 서비스에서 URL 변경 설정을 정의하는 방법은 다음과 같습니다. PAS-K에는 최대 256개의 URL 변경 설정을 등록할 수 있으므로, 여러 개의 URL 변경 설정을 등록하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**l7slb** *<NAME>*	<L7SLB 설정 모드>로 들어갑니다. • *<NAME>* URL 변경을 설정할 L7 서버 부하 분산 서비스 이름
2	**urlmanip** *<ID>*	<URL 변경 설정 모드>로 들어갑니다. • *<ID>* URL 변경 ID. 설정 범위: 1 ~ 256
3	**priority** *<PRIORITY>*	URL 변경 설정의 우선순위를 설정합니다. 여러 개의 URL 변경 설정이 정의된 경우에는 우선순위가 높은 규칙부터 차례로 적용됩니다. 값이 작을수록 우선순위는 더 높습니다. • *<PRIORITY>* 우선순위. 설정 범위: 0~255, 기본값: 0 **참고**: 설정한 우선순위를 기본값으로 변경하려면, <URL 변경 설정 모드>에서 **no priority** 명령을 사용합니다.
4	**match** *<MATCH>*	URL에서 검색할 문자열인 매칭 URL을 설정합니다. • *<MATCH>* 매칭 URL 을 정규식의 형태로 입력. 정규식에는 '(작은 따옴표)를 제외한 모든 문자를 사용하여 최대 256 byte 입력 가능 **참고: match** 명령을 통해 지정한 매칭 URL을 삭제하려면 **no match** 명령을 사용합니다. 매칭 URL을 지정하지 않으면 PAS-K는 모든 URL이 매칭된 것으로 간주합니다.
5	**replace** *<REPLACE>*	URL에서 검색 문자열과 치환할 변경 문자열인 대체 URL을 입력합니다. • *<REPLACE>* 매칭 URL 을 정규식의 형태로 입력. 정규식에는 '(작은 따옴표)를 제외한 모든 문자를 사용하여 최대 256 byte 입력 가능 **참고: replace** 명령을 통해 지정한 대체 URL을 삭제하려면 **no replace** 명령을 사용합니다. 대체 URL을 지정하지 않으면 URL 변경이 수행되지 않습니다.
6	**https-for-redirect** {**enable** | **disable**}	URL 변경 방식으로 HTTP redirection을 사용하는 경우, 클라이언트가 HTTP로 접속하게 할지 HTTPS로 접속하게 할 지의 여부를 설정합니다. • **enable** HTTPS 로 접속 **disable** HTTP 로 접속(기본값)
7	**rule** *<RULE>*	URL 변경 설정을 적용할 규칙 ID를 설정합니다. • *<RULE>* 규칙의 ID 설정. 두 개 이상의 ID 를 지정하는 경우에는 각 ID 를 ','로 구분하고, 연속된 ID 들을 지정할 때는 '-'를 사용합니다.
8	**status** {**enable** | **disable**} (선택 설정)	URL 변경의 사용 여부를 지정합니다. • **enable** URL 변경 활성화 (기본값) **disable** URL 변경 비활성화
9	**current**	URL 변경 설정 정보를 확인합니다.
10	**apply**	URL 변경 설정을 저장하고 시스템에 적용합니다.

참고: 정의한 URL 변경 기능을 삭제하려면 <L7SLB 설정 모드>에서 **no urlmanip** *<ID>* 명령을 사용합니다.

참고: 설정한 URL 변경 설정을 확인하려면 <L7SLB 설정 모드>에서 **show urlmanip** *<ID>* 명령을 사용합니다.

설정 정보 보기

L7 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

L7 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 L7 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **`show l7slb`** 명령을 사용합니다. **`show l7slb`** 명령은 현재 PAS-K에 정의된 L7 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 L7 서버 부하 분산 서비스의 설정 정보 보기

특정 L7 서버 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **`show l7slb`** 명령 뒤에 해당 서비스의 이름(*<NAME>*)을 입력하면 됩니다.

L7 서버 부하 분산 서비스의 모든 설정 정보(실제 서버, 장애 감시, 필터, 세션) 보기

각 L7 서버 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 그리고 서비스에 등록된 실제 서버의 설정 정보와 실제 서버를 통해 연결된 세션에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **`show info l7slb`** 명령을 사용합니다.

서비스의 이름을 입력하지 않고 **`show info l7slb`** 명령을 실행하면 모든 L7 서버 부하 분산 서비스에 대한 정보가 출력되고 서비스의 이름을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

고급 L7 서버 부하 분산 설정

이 절에서는 CLI에서 고급 L7 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: 고급 L7 서버 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

참고: 고급 L7 서버 부하 분산은 HTTP 압축, 캐싱, SSL 가속과 같은 애플리케이션 가속 기능을 지원하며, 각 가속 기능을 사용하기 위해서는 HTTP 압축 규칙, 캐싱 규칙, SSL 가속이 미리 설정되어 있어야 합니다. 각 기능의 설정 방법은 다음 부분을 참고하도록 합니다.

- HTTP 압축 규칙: [**제7장 부하 분산 설정 – HTTP 압축 규칙 설정**]
- 캐싱 규칙: [**제7장 부하 분산 설정 – 캐싱 규칙 설정**]
- SSL 가속: [**제7장 부하 분산 설정 – SSL 가속 설정**]

CLI에서 설정하기

PAS-K에 고급 L7 서버 부하 분산을 설정하는 과정은 다음과 같습니다.

1. 패턴 정의
2. 고급 L7 서버 부하 분산 서비스 정의
3. 그룹 설정
4. URL 변경 설정
5. 규칙 설정
6. RTS 실제 서버 설정 (선택 설정)
7. 설정 정보 보기

1단계의 설정 과정은 L7 서버 부하 분산 설정 절에서 설명한 패턴 정의 설정 방법과 동일합니다. 그러므로, 이 절에서는 고급 L7 서버 부하 분산 서비스를 정의하는 2단계부터 살펴봅니다.

고급 L7 서버 부하 분산 서비스 정의

고급 L7 서버 부하 분산 서비스를 정의하는 방법은 다음과 같습니다. 여러 개의 고급 L7 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl7slb** *<NAME>*	<고급 L7SLB 설정 모드>에서 고급 L7 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 16 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**ip-version {ipv4 | ipv6}**	부하 분산 서비스의 네트워크 종류를 설정합니다. 기본값: ipv4
3	**vip** *<IP>* **vport** *<port>* (필수 설정)	부하 분산 서비스의 가상 IP 주소와 가상 포트를 설정합니다. 2번 과정에서 지정한 네트워크 종류에 따라 IPv4 또는 IPv6 주소를 설정해야 합니다. • *<IP>* 가상 IP 주소. • *<VPORT>* 가상 포트. 설정 범위: 1 ~ 65535 **참고:** 설정한 가상 IP 주소와 가상 포트를 삭제하려면 <L7SLB 설정 모드>에서 **no vip** *<IP>* **vport** *<VPORT>* 명령을 실행합니다. **참고:** 최소 1개 이상 삭제하려면 <SLB 설

4	**priority** *<PRIORITY>*	고급 L7 서버 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위. 설정 범위: 0 ~ 255, 기본값: 100 **참고**: 설정한 우선순위를 기본값으로 변경하려면, <고급 L7SLB 설정 모드>에서 **no priority** 명령을 사용합니다.
5	**health-check** *<HEALTH-CHECK>*	고급 L7 서버 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 설정. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 삭제하려면 <고급 L7SLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
6	**host** *<HOST>* (선택 설정)	고급 L7 서버 부하 분산 서비스를 적용할 도메인을 설정합니다. 동일한 가상 IP 주소와 가상 포트를 사용하는 부하 분산 서비스가 동작 중인 경우에는 설정된 도메인이 일치하는 부하 분산 서비스를 적용합니다. • *<HOST>* www.piolink.com, mail.piolink.com 과 같은 도메인을 입력 **참고:** 두 개 이상의 고급 L7 서버 부하 분산 서비스가 동일한 가상 IP 주소와 가상 포트를 사용하는 경우에는 다음과 같은 순서로 트래픽에 적용할 부하 분산 서비스를 선택합니다. 1. 도메인이 일치하는 고급 L7 서버 부하 분산 서비스 2. 도메인이 설정되지 않은 고급 L7 서버 부하 분산 서비스 3. 우선순위가 높은 고급 L7 서버 부하 분산 서비스
7	**preserve-src-addr {enable | disable}**	클라이언트가 송신한 요청 패킷의 출발지 IP 주소 유지 여부를 설정합니다. • **enable** 출발지 IP 주소를 유지하여 실제 서버로 전달합니다. (기본값) • **disable** 출발지 IP 주소를 가상 IP 주소로 변경하여 실제 서버로 전달합니다. **참고:** IPv4 네트워크와 IPv6 네트워크는 주소 체계에 따른 호환성 문제로 인해 직접적인 통신을 할 수 없습니다. 그러므로, PAS-K가 IPv4 네트워크와 IPv6 네트워크의 경계에 위치한 경우에는 이 옵션을 비활성화하여 출발지 IP 주소를 가상 IP 주소로 변경함으로써 실제 서버의 IP 주소 버전과 일치시켜야 합니다.
8	**return-to-sender {enable | disable}**	RTS 기능의 사용 여부를 설정합니다. • **enable** 요청 패킷을 수신한 경로로 응답 패킷을 전송합니다. • **disable** 라우팅 테이블 설정에 따라 응답 패킷을 전송합니다. (기본값)
9	**x-forwarded-for {enable | disable}**	'X-Forwarded-For' 헤더를 삽입할 지의 여부를 설정합니다. PAS-K가 Source NAT를 수행 할 경우, 서버에서 기존의 클라이언트 IP를 알기 위해서는 HTTP 요청에 'X-Forwarded-For' 헤더를 추가해야 합니다. • **enable** 'X-Forwarded-For' 헤더 삽입 • **disable** 'X-Forwarded-For' 헤더 삽입하지 않음 (기본값)
10	**ssl** *<SSL>* (선택 설정)	SSL 가속 기능을 사용할 경우에는 해당 서비스에서 사용할 SSL 프로필을 설정합니다. • *<SSL>* SSL 프로필 ID. 설정 범위: 1 ~ 256
11	**status {enable | disable}** (선택 설정)	고급 L7 서버 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 활성화 (기본값) • **disable** 부하 분산 서비스 비활성화
12	**current**	고급 L7 서버 부하 분산 서비스의 설정 정보를 확인합니다.
13	**apply**	고급 L7 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 고급 L7 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no advl7slb** *<NAME>* 명령을 사용합니다.

그룹 설정

고급 L7 서버 부하 분산 서비스를 정의한 후에는 실제 서버의 그룹(Group)을 설정할 수 있습니다. 고급 L7 서버 부하 분산 서비스에서는 그룹별로 별도의 부하 분산 방식을 설정합니다. 그리고, 지속 연결 기능의 적용도 그룹 단위로 이루어집니다. 하나의 고급 L7 서버 부하 분산 서비스에는 최대 256 개의 그룹을 설정할 수 있으므로, 여러 개의 그룹을 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl7slb** *<NAME>*	<고급 L7SLB 설정 모드>로 들어갑니다. • *<NAME>* 그룹을 설정할 L7 서버 부하 분산 서비스 이름
2	**group** *<NAME>*	<Group 설정 모드>로 들어갑니다. • *<NAME>* 알파벳과 숫자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용
3	**real** *<ID>*	서비스를 통해 트래픽을 분산 시킬 실제 서버의 ID를 설정합니다. • *<ID>* 실제 서버 ID. 여러 개의 실제 서버를 지정하는 경우에는 각 실제 서버의 ID 를 ','로 구분하고, 연속된 실제 서버 ID 는 '-'를 사용. **참고:** 설정한 실제 서버를 그룹에서 삭제하려면 <Group 설정 모드>에서 **no real** *<ID>*명령을 실행합니다.
4	**lb-method type {lc | rr | sh | wrr}**	그룹에 속한 서버로 부하를 분산시킬 때 사용할 부하 분산 방식을 설정합니다. (기본값: rr)
5	**persist type {cookie | ip | none | session | ssl}**	클라이언트가 이전에 연결했던 서버와 계속 연결할 수 있게 해주는 지속 연결 기능을 설정합니다. • **cookie** HTTP 쿠키 지속 연결 기능 사용 • **ip** IP 지속 연결 기능을 사용 • **none** 지속 연결 기능을 사용하지 않음 (기본값) • **session** 세션 ID 지속 연결 기능을 사용 • **ssl** SSL 세션 ID 지속 연결 기능을 사용
5-1	**persist cookie-type {insert | passive | rewrite}**	5번 과정에서 지속 연결 기능을 cookie로 지정한 경우에는 HTTP 쿠키 지속 연결 모드를 설정합니다. • **insert** PAS-K 가 Set-Cookie 필드를 추가하고 값을 입력함 • **passive** 실제 서버가 Set-Cookie 필드를 추가하고 갑을 입력함 • **rewrite** 실제 서버가 Set-Cookie 필드를 추가하고, PAS-K 가 값을 입력함
5-2	**persist session-key** *<SESSION-KEY>*	5번 과정에서 지속 연결 기능을 session으로 지정한 경우에는 웹 애플리케이션에서 사용하는 세션 ID 이름을 세션 키로 설정합니다. • *<SESSION-KEY>* 웹 애플리케이션의 세션 ID 이름을 입력. **참고:** 세션 키는 웹 애플리케이션에서 사용하는 세션 ID 이름을 입력합니다. 많이 사용되는 웹 애플리케이션의 세션 ID 이름은 다음과 같습니다. **PHP** PHPSESSID **JSP** JSESSIONID **ASP** ASPSESSIONID **ASP.NET** ASP.NET_SessionId **주의:** 세션 키 설정시 대소문자를 정확히 구분해서 입력해야 합니다.
6	**persist timeout** *<TIMEOUT>*	지속 연결 엔트리의 지속 시간을 설정합니다. • *<TIMEOUT>* 지속 시간을 일, 시간, 분, 초([[[dd]:hh]:mm]:ss)의 순서로 입력합니다. (기본값: 0)
7	**connection-pooling {enable | disable}**	커넥션 풀링 기능을 사용하여 저장해 두었던 커넥션을 재사용할 지의 여부를 설정합니다.

		• **enable** 클라이언트와 실제 서버간에 TCP 커넥션을 연결할 때 생성된 커넥션을 풀에 저장해 두었다가 클라이언트로부터 요청이 있을 경우 재사용 (기본값) • **disable** IP 주소와 포트 번호가 같은 경우에만 커넥션을 재사용
8	**pool-size** *<POOL-SIZE>*	그룹이 저장할 커넥션의 최대 개수를 설정합니다. 그룹에 저장된 커넥션의 수가 최대 커넥션 개수에 도달하면 더 이상 커넥션을 재사용하지 않습니다. • *<POOL-SIZE>* 커넥션 최대 저장 개수. 설정 범위: 1 ~ 30000, 기본값: 2048 **참고:** 설정한 커넥션 최대 저장 개수를 기본값으로 변경하려면 <Group 설정 모드>에서 **no pool-size** 명령을 실행합니다.
9	**backend-ssl** {**enable** | **disable**}	PAS-K와 실제 서버간에 SSL(HTTP) 통신을 사용하는 백엔드 SSL 기능의 사용 여부를 설정합니다. • **enable** 백엔드 SSL 기능 활성화. • **disable** 백엔드 SSL 기능 비활성화. (기본값)
10	**current**	그룹의 설정 정보를 확인합니다.
11	**apply**	그룹을 저장하고 시스템에 적용합니다.

주의: HTTP 쿠키 지속 연결 기능을 사용하는 경우에는 PAS-K를 사용하고 있는 국가의 시간대(timezone)를 PAS-K에 설정해야 합니다. 시간대는 Configuration 모드에서 다음과 같은 **timezone** 명령을 사용하여 설정할 수 있습니다.

```
timezone {+8 | +9}
```

PAS-K가 설치된 지역이 중국인 경우에는 '+8'을 지정하고, 한국 또는 일본인 경우에는 '+9'를 설정합니다. 변경한 시간대는 **show timezone** 명령을 통해 확인할 수 있습니다. 다음은 PAS-K의 시간대를 GMT 시간보다 8시간 빠른 시간대로 설정한 후 결과를 확인하는 예입니다.

```
(config)# timezone +8
Timezone is applied to system.
(config)# show timezone
================================================================================
  TIMEZONE
 --------------------------------------------------------------------------------
    Timezone           : +8
================================================================================
(config)#
```

PAS-K는 기본적으로 GMT 시간보다 9시간 빠른 시간대(GMT +9)로 설정되어 있습니다.

참고: 고급 L7 서버 부하 분산 서비스에서 그룹을 삭제하려면 <고급 L7 SLB 설정 모드>에서 **no group** *<NAME>* 명령을 사용합니다.

URL 변경 설정

URL 변경 기능을 설정하면 PAS-K가 자동으로 클라이언트와 서버의 사이에서 URL을 변경해줍니다. 고급 L7 서버 부하 분산 서비스에서 URL 변경 설정을 정의 방법은 다음과 같습니다. PAS-K에는 최대 256개의 URL 변경 설정을 등록할 수 있으므로, 여러 개의 URL 변경 설정을 등록하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl7slb** *<NAME>*	<고급 L7SLB 설정 모드>로 들어갑니다. • *<NAME>* URL 변경을 설정할 고급 L7 서버 부하 분산 서비스 이름
2	**urlmanip** *<ID>*	<URL 변경 설정 모드>로 들어갑니다. • *<ID>* URL 변경 설정 ID. (설정 범위: 1 ~ 256)
3	**priority** *<PRIORITY>*	URL 변경 설정의 우선순위를 설정합니다. 여러 개의 URL 변경 설정이 정의된 경우에는 우선순위가 높은 규칙부터 차례로 적용됩니다. 값이 작을수록 우선순위는 더 높습니다. • *<PRIORITY>* 우선순위 설정. (설정 범위: 0 ~ 255, 기본값: 0) **참고**: 설정한 우선순위를 기본값으로 변경하려면, <URL 변경 설정 모드>에서 **no priority** 명령을 사용합니다.
4	**match** *<MATCH>*	URL에서 검색할 문자열인 매칭 URL을 설정합니다. • *<MATCH>* 매칭 URL 을 정규식의 형태로 입력. 정규식에는 '(작은 따옴표)를 제외한 모든 문자를 사용하여 최대 256 byte 입력 가능 **참고:** 지정한 매칭 URL을 삭제하려면 **no match** 명령을 사용합니다. 매칭 URL을 지정하지 않으면 PAS-K는 모든 URL이 매칭된 것으로 간주합니다.
5	**replace** *<REPLACE>*	URL에서 검색 문자열과 치환할 변경 문자열인 대체 URL을 입력합니다. • *<REPLACE>* 매칭 URL 을 정규식의 형태로 입력. 정규식에는 '(작은 따옴표)를 제외한 모든 문자를 사용하여 최대 256 byte 입력 가능 **참고:** 지정한 대체 URL을 삭제하려면 **no replace** 명령을 사용합니다. 대체 URL을 지정하지 않으면 URL 변경이 수행되지 않습니다.
6	**status** {**enable** | **disable**} (선택 설정)	URL 변경의 사용 여부를 지정합니다. • **enable** URL 변경 활성화 (기본값) • **disable** URL 변경 비활성화
7	**current**	URL 변경 설정 정보를 확인합니다.
8	**apply**	URL 변경 설정을 저장하고 시스템에 적용합니다.

참고: 정의한 URL 변경 기능을 삭제하려면 <고급 L7SLB 설정 모드>에서 **no urlmanip** *<ID>* 명령을 사용합니다.

참고: 설정한 URL 변경 설정을 확인하려면 <고급 L7SLB 설정 모드>에서 **show urlmanip** *<ID>* 명령을 사용합니다.

RTS(Revers To Sender) 실제 서버 설정

고급 L7 부하 분산 서비스 정의에서 RTS 기능을 활성화 한 경우에는 RTS 실제 서버를 설정합니다. 외부 네트워크와 연결된 경로의 상위 장비(라우터, 방화벽 등)를 RTS 실제 서버로 지정해야 하며, 설정하는 방법은 다음과 같습니다. PAS-K에는 최대 128개의 RTS 실제 서버를 등록할 수 있으므로, 여러 개의 RTS 실제 서버를 등록하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl7slb** *<NAME>*	<고급 L7SLB 설정 모드>로 들어갑니다. • *<NAME>* RTS 실제 서버를 설정할 고급 L7 서버 부하 분산 서비스 이름
2	**rts-real** *<ID>*	<RTS 실제 서버 설정 모드>로 들어갑니다. • *<ID>* RTS 실제 서버 설정 ID. 설정 범위: 1 ~ 128
3	**ip** *<IP>*	RTS 실제 서버의 IP 주소를 설정합니다. • *<IP>* RTS 실제 서버 IP 주소
4	**mac** *<MAC>*	RTS 실제 서버의 MAC 주소를 설정합니다. • *<MAC>* RTS 실제 서버의 MAC 주소를 XX:XX:XX:XX:XX:XX 형식으로 입력
5	**current**	URL 변경 설정의 설정 정보를 확인합니다.
6	**apply**	URL 변경 설정을 저장하고 시스템에 적용합니다.

참고: 정의한 RTS 실제 서버를 삭제하려면 <고급 L7SLB 설정 모드>에서 **no rts-real** *<ID>* 명령을 사용합니다.

규칙 설정

규칙(Rule)은 특정 패턴과 일치하는 HTTP 요청에 대해 어떠한 동작을 수행할 것인지 정의한 것입니다. 예를 들어, URI가 /image라는 문자열로 시작(패턴)하는 HTTP 요청이 Image라는 서버 그룹(그룹)으로 전송되도록 규칙을 정의할 수 있습니다.

고급 L7 서버 부하 분산 서비스에 속하는 그룹에 적용할 규칙을 정의하는 방법은 다음과 같습니다. 하나의 고급 L7 서버 부하 분산 서비스에는 최대 256개의 규칙을 등록할 수 있으므로, 여러 개의 규칙을 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl7slb** *<NAME>*	<고급 L7SLB 설정 모드>로 들어갑니다. • *<NAME>* 규칙을 설정할 고급 L7 서버 부하 분산 서비스 이름
2	**rule** *<ID>*	<Rule 설정 모드>로 들어갑니다. • *<ID>* 규칙의 ID. 설정 범위: 1 ~ 256
3	**priority** *<PRIORITY>*	그룹에 적용될 규칙의 우선순위를 설정합니다. 여러 개의 규칙이 그룹에 정의된 경우에는 우선순위가 높은 규칙부터 차례로 적용됩니다. 값이 작을수록 우선순위는 더 높습니다. • *<PRIORITY>* 우선순위. 설정 범위: 0 ~ 255, 기본값: 0 **참고**: 설정한 우선순위를 기본값으로 변경하려면, <Rule 설정 모드>에서 **no priority** 명령을 사용합니다.
4	**pattern** *<PATTERN>*	규칙에서 사용할 패턴을 설정합니다. 하나의 규칙에는 한개의 패턴만 등록할 수 있습니다. • *<PATTERN>* 규칙에서 사용할 패턴의 ID. 설정 범위: 1 ~ 512 **참고:** 지정한 패턴을 규칙에서 삭제하려면 **no pattern** 명령을 사용합니다.
5	**action** {**group** | **http-response** | **real**}	규칙에 따라 취할 액션을 설정합니다. (기본값: group) • **group** 해당 그룹 내에서 부하 분산을 수행하도록 지정 • **real** 사용자가 해당 그룹 내에서 실제 서버를 직접 선택하도록 지정 • **http-response** PAS-K 가 직접 HTTP 응답을 생성하여 클라이언트에게 전송하도록 지정 **참고:** 설정한 액션을 기본값으로 변경하려면, <Rule 설정 모드>에서 **no action** 명령을 사용합니다.
6	**http-status** *<STATUS>*	액션이 http-response인 경우, HTTP 상태 코드를 설정합니다. • *<STATUS>* HTTP 상태 코드의 종류를 입력. 사용 가능 상태 코드: 301, 302, 307, 400, 403, 404, 503 **참고:** 설정한 HTTP 상태 코드를 규칙에서 삭제하려면 **no http-status** 명령을 사용합니다. **참고:** HTTP 상태 코드에 대한 상세한 설명은 이 장의 [**L7 부하 분산 – 규칙(Rule) – 액션(Action) – HTTP Response**] 절을 참고하도록 합니다.
7	**group** *<GROUP>*	액션이 group이나 real인 경우, 현재 설정 중인 규칙을 사용할 그룹을 설정합니다. 반드시 이미 정의되어 있는 그룹의 이름을 입력해야 합니다. • *<GROUP>* 그룹의 이름.
8	**real** *<REAL>*	액션이 real인 경우, HTTP 요청을 처리할 실제 서버를 설정합니다. 반드시 이미 정의되어 있는 실제 서버의 ID를 입력해야 하며, 해당 실제 서버는 7번 과정에서 지정한 그룹 내에 포함되어 있어야 합니다. • *<REAL>* 실제 서버 ID. 설정 범위: 1 ~ 2048

9	**backup-group** *<BACKUP-GROUP>*	7번 과정에서 지정한 그룹에 속한 실제 서버가 모두 INACTIVE이거나 FULL 상태일 경우, 대신 서비스를 제공할 그룹(백업 그룹)을 설정합니다. 반드시 이미 정의되어 있는 그룹의 이름을 입력해야 합니다. • *<BACKUP-GROUP>* 백업으로 설정할 그룹의 이름 설정. **참고:** 설정한 백업 그룹을 규칙에서 삭제하려면, <Rule 설정 모드>에서 **no backup-group** 명령을 사용합니다.
10	**urlmanip** *<URLMANIP>*	규칙을 적용할 URL 변경 설정의 ID를 설정합니다. 반드시 이미 정의되어 있는 URL 변경 설정의 ID를 입력해야 합니다. • *<URLMANIP>* URL 변경 설정 ID. 설정 범위: 1 ~ 256 **참고:** 설정한 URL 변경을 규칙에서 삭제하려면, <Rule 설정 모드>에서 **no urlmanip** *<URLMANIP>*명령을 사용합니다.
11	**compression** *<COMPRESSION>*	HTTP 압축 기능을 사용할 경우에는 해당 규칙에서 사용할 HTTP 압축 규칙의 ID를 설정합니다. • *<COMPRESSION>* HTTP 압축 규칙 ID. 설정 범위: 1 ~ 256 **참고:** 설정한 HTTP 압축 규칙을 규칙에서 삭제하려면, <Rule 설정 모드>에서 **no compression** 명령을 사용합니다.
12	**cache** *<CACHE>*	캐싱 기능을 사용할 경우에는 해당 규칙에서 사용할 캐싱 규칙의 ID를 설정합니다. • *<CACHE>* 캐싱 규칙 ID (설정 범위: 1 ~ 256) **참고:** 설정한 캐싱 규칙을 규칙에서 삭제하려면, <Rule 설정 모드>에서 **no cache** 명령을 사용합니다.
13	**status {enable | disable}**	규칙의 사용 여부를 지정합니다. • **enable** 규칙 활성화 (기본값) • **disable** 규칙 비활성화
14	**current**	규칙의 설정 정보를 확인합니다.
15	**apply**	규칙을 저장하고 시스템에 적용합니다.

참고: 설정한 규칙을 삭제하려면 <고급 L7SLB 설정 모드>에서 **no rule** *<ID>* 명령을 사용합니다.

설정 정보 보기

고급 L7 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

고급 L7 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 고급 L7 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show advl7slb** 명령을 사용합니다. **show advl7slb** 명령은 현재 PAS-K에 정의된 고급 L7 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다. 특정한 고급 L7 서버 부하 분산 서비스에 대한 상세한 설정 정보를 보려면 해당 서비스의 이름을 입력하면 됩니다.

고급 L7 서버 부하 분산 서비스의 모든 설정 정보 보기

각 고급 L7 서버 부하 분산 서비스의 설정 정보와 해당 서비스에 대한 통계 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show info advl7slb** *<NAME>* 명령을 사용합니다.

서비스의 이름을 입력하지 않고 명령을 실행하면 모든 고급 L7 서버 부하 분산 서비스에 대한 정보가 출력되고 서비스의 이름을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

L7 캐시 서버 부하 분산 설정

이 절에서는 CLI에서 PAS-K에 L7 캐시 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

CLI에서 설정하기

PAS-K에 L7 캐시 서버 부하 분산을 구성하는 과정은 다음과 같습니다.

1. 패턴 정의하기
2. L7 캐시 서버 부하 분산 서비스 정의하기
3. 그룹 설정하기
4. 규칙 설정하기
5. URL 변경 설정
6. 필터 설정하기
7. 설정 정보 보기

1단계와 3~5 단계의 설정 과정은 L7 서버 부하 분산 설정 절에서 설명한 L7 서버 부하 분산 서비스의 설정 방법과 동일합니다. 그러므로, 이 절에서는 L7 캐시 서버 부하 분산 서비스를 정의하는 2단계와 필터를 정의하는 6단계의 설정 과정에 대해서만 상세히 살펴봅니다.

L7 캐시 서버 부하 분산 서비스 정의

새로운 L7 캐시 서버 부하 분산 서비스를 정의하는 방법은 다음과 같습니다. PAS-K에는 L7 캐시 서버 부하 분산 서비스를 포함하여 최대 1024개의 L7 부하 분산 서비스를 추가할 수 있으므로, 여러 개의 L7 캐시 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**l7cslb** *<NAME>*	<L7CSLB 설정 모드>에서 L7 캐시 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 32 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**priority** *<PRIORITY>*	L7 캐시 서버 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위 설정. (설정 범위: 0 ~ 255, 기본값: 0) **참고**: 설정한 우선순위를 기본값으로 변경하려면, <L7CSLB 설정 모드>에서 **no priority** 명령을 사용합니다.
3	**health-check** *<HEALTH-CHECK>*	L7 캐시 서버 부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 설정. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 L7 캐시 서버 부하 분산 서비스에서 삭제하려면 <L7CSLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.

4	**keep-backup {all | entry | none}**	부하 분산 서비스의 실제 서버에 백업 실제 서버를 설정한 경우, 마스터 실제 서버가 다시 동작 가능한 상태가 되었을 때 백업 실제 서버의 세션을 어떻게 처리할 것인지를 설정합니다. • **none** 백업 실제 서버의 모든 세션 엔트리를 삭제 • **entry** 지속 연결 엔트리만 삭제 • **all** 모든 세션 엔트리를 그대로 유지 (기본값)
5	**direct-connect {enable | disable}**	클라이언트가 서버와 직접 TCP 접속을 하도록 하고, PAS-K가 중간에 데이터를 가로채어 필요한 경우 실제 서버로 트래픽을 부하분산 하도록 하는 직접 연결 방식을 사용할 지의 여부를 설정합니다. • **enable** PAS-K가 직접 연결 방식을 수행 • **disable** 지연 바인딩 동작을 수행 (기본값)
6	**allow-nonhttp {enable | disable}**	non-HTTP 트래픽을 포워딩할 지의 여부를 설정합니다. • **enable** non-HTTP 트래픽을 서버로 바로 포워딩하고 그 이후에 전송되는 패킷들은 L7 캐시 서버 부하 분산 서비스를 적용하지 않고 단순히 중계함 • **disable** non-HTTP 트래픽에 대해서도 L7 캐시 서버 부하 분산 서비스를 적용(기본값)
7	**server-min-mtu** *<SERVER-MIN-MTU>*	MTU 값을 변경합니다. PAS-K는 클라이언트와 세션을 연결할 때 기본적으로 MTU 값을 1500으로 사용합니다. 실제 서버 중에 MTU 값이 1500보다 작은 실제 서버가 있는 경우에는 이 값을 변경해주어야 합니다. • *<SERVER-MIN-MTU>* MTU 값 설정 (설정 범위: 60 ~ 1500 기본값: 1500) **참고:** 부하 분산 서비스 그룹에 속한 실제 서버들의 MTU 중에서 가장 낮은 MTU 값을 입력합니다.
8	**connection-pooling {enable | disable}**	커넥션 풀링 기능을 사용하여 저장해 두었던 커넥션을 재사용할 지의 여부를 설정합니다. • **enable** 클라이언트와 실제 서버간에 TCP 커넥션을 연결할 때 생성된 커넥션을 풀에 저장해 두었다가 클라이언트로부터 요청이 있을 경우 재사용 (기본값) • **disable** IP 주소와 포트 번호가 같은 경우에만 커넥션을 재사용
9	**age-refresh {enable | disable}**	커넥션 풀링 기능을 설정한 경우, 커넥션을 재사용 할 때 마다 시간을 업데이트 해줄지의 여부를 설정합니다. • **enable** 커넥션을 재사용 할 때 마다 커넥션의 시간을 업데이트함 • **disable** 커넥션을 재사용하여도 시간을 업데이트 하지않음 (기본값)
10	**x-header {enable | disable}**	'X-Forwarded-For' 헤더 삽입 여부를 설정합니다. PAS-K가 Source NAT를 수행 할 경우, 서버에서 기존의 클라이언트 IP를 알기 위해서는 HTTP 요청에 'X-Forwarded-For' 헤더를 추가해야 합니다. • **enable** 'X-Forwarded-For' 헤더 삽입 • **disable** 'X-Forwarded-For' 헤더 삽입하지 않음 (기본값)
11	**status {enable | disable}** (선택 설정)	L7 캐시 서버 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** L7 캐시 서버 부하 분산 서비스 활성화 (기본값) • **disable** L7 캐시 서버 부하 분산 서비스 비활성화
12	**current**	L7 캐시 서버 부하 분산 서비스의 설정 정보를 확인합니다.
13	**apply**	L7 캐시 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 L7 캐시 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no l7cslb** *<NAME>* 명령을 사용합니다.

그룹 설정

L7 캐시 서버 부하 분산 서비스에 실제 서버의 그룹을 설정하는 방법은 그룹을 적용할 지속연결 기능의 종류 중 HTTP 쿠키 지속 연결 모드가 없는 것을 제외하고는 서버 부하 분산 서비스에 실제 서버의 그룹을 설정하는 방법과 동일합니다. 그러므로, 캐시 서버 부하 분산 서비스에서 사용할 실제 서버의 그룹을 설정하는 방법은 **L7 서버 부하 분산 설정 – CLI에서 설정하기 – 그룹 설정** 절의 설명을 참고합니다.

규칙 설정

L7 캐시 서버 부하 분산 서비스에 규칙을 추가하는 방법은 서버 부하 분산 서비스에 규칙을 추가하는 방법과 동일합니다. 그러므로, 캐시 서버 부하 분산 서비스에서 사용할 규칙을 추가하는 방법은 **L7 서버 부하 분산 설정 – CLI에서 설정하기 – 규칙 설정** 절의 설명을 참고합니다.

URL 변경 설정

L7 캐시 서버 부하 분산 서비스에 URL 변경 기능을 설정하는 방법은 서버 부하 분산 서비스에 URL 변경 기능을 설정하는 방법과 동일합니다. 그러므로, 캐시 서버 부하 분산 서비스에서 사용할 URL 변경 기능을 설정하는 방법은 **L7 서버 부하 분산 설정 – CLI에서 설정하기 – URL 변경 설정** 절의 설명을 참고합니다.

필터 설정

L7 캐시 서버 부하 분산 서비스를 어떤 트래픽에 적용할 것인지를 구분하기 위해 사용되는 필터를 정의하는 방법은 다음과 같습니다. 하나의 L7 캐시 서버 부하 분산 서비스에는 최대 2048개의 필터를 등록할 수 있으므로, 여러 개의 필터를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**l7cslb** *<NAME>*	<L7CSLB 설정 모드>로 들어갑니다. • *<NAME>* 필터를 설정할 L7 캐시 서버 부하 분산 서비스 이름
2	**filter** *<ID>*	L7 캐시 서버 부하 분산 서비스의 트래픽을 구분하기 위해 사용할 필터를 정의합니다. • *<ID>* 필터의 ID. 설정 범위: 1 ~ 2048
3	**type {include | exclude}**	필터의 종류를 설정합니다. • **include** 필터가 캐시 서버 부하 분산 서비스를 적용할 트래픽을 필터링 (기본값) • **exclude** 캐시 서버 부하 분산 서비스를 적용하지 않을 트래픽을 필터링
	참고: 이후의 과정은 필터링에 사용될 조건을 지정하는 과정입니다. 모든 과정을 수행할 필요는 없고 필터링시 사용할 항목에 해당되는 과정만 수행하면 됩니다. 필터링에 사용할 조건에 따라 이동할 단계는 다음과 같습니다. 하나의 필터에는 여러 개의 조건이 추가될 수 있으므로 하나의 조건을 추가한 후 다른 과정으로 이동하여 다른 조건을 계속 추가하면 됩니다. **출발지 IP 주소 → 4 번 과정** **출발지 포트 번호 → 5 번 과정** **목적지 IP 주소 → 6 번 과정** **목적지 포트 번호 → 7 번 과정**	
4	**sip** *<SIP>*	필터링 조건으로 사용할 출발지 IP 주소와 넷 마스크 비트 수를 설정합니다. • *<SIP>* 출발지 IP 주소 및 서브넷 마스크 비트 수
5	**sport** *<SPORT>*	필터링 조건으로 사용할 출발지 포트 번호를 설정합니다. • *<SPORT>* 출발지 포트 번호. 설정 범위: 1 ~ 65535
6	**dip** *<DIP>*	필터링 조건으로 사용할 목적지 IP 주소와 넷 마스크 비트 수를 설정합니다. • *<DIP>* 목적지 IP 주소 및 서브넷 마스크 비트 수

7	**dport** *<DPORT>*	필터링 조건으로 사용할 목적지 포트 번호를 설정합니다. • *<DPORT>* 목적지 포트 번호. 설정 범위: 1 ~ 65535
8	**status** {**enable** | **disable**} (선택 설정)	필터의 사용 여부를 지정합니다. • **enable** 필터 활성화 (기본값) • **disable** 필터 비활성화
9	**current**	필터의 설정 정보를 확인합니다.
10	**apply**	필터를 저장하고 시스템에 적용합니다.

참고: 정의한 필터를 삭제하려면 <L7CSLB 설정 모드>에서 **no filter** *<ID>* 명령을 사용합니다.

설정 정보 보기

L7 캐시 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

L7 캐시 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 L7 캐시 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show l7cslb** 명령을 사용합니다. **show l7cslb** 명령은 현재 PAS-K에 정의된 L7 캐시 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다.

특정 L7 캐시 서버 부하 분산 서비스의 설정 정보 보기

특정한 L7 캐시 서버 부하 분산 서비스에 대한 상세한 설정 정보를 확인하려면, **show l7cslb** 명령 뒤에 '해당 서비스의 이름'을 입력하면 됩니다.

L7 캐시 서버 부하 분산 서비스의 모든 설정 정보(실제 서버, 장애 감시, 필터, 세션) 보기

각 L7 캐시 서버 부하 분산 서비스의 설정 정보와 해당 서비스의 장애 감시 설정 정보, 그리고 서비스에 등록된 실제 서버의 설정 정보와 실제 서버를 통해 연결된 세션에 대한 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show info l7cslb** 명령을 사용합니다.

서비스의 이름을 입력하지 않고 **show info l7cslb** 명령을 실행하면 모든 L7 캐시 서버 부하 분산 서비스에 대한 정보가 출력되고 서비스의 이름을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

고급 L7 캐시 서버 부하 분산 설정

이 절에서는 CLI에서 고급 L7 캐시 서버 부하 분산 기능을 사용할 수 있도록 설정하는 방법을 살펴봅니다.

참고: 고급 L7 캐시 서버 부하 분산 기능을 구성하기 위해서는 VLAN과 IP 주소, 포트 바운더리, 장애 감시, 실제 서버가 미리 설정되어 있어야 합니다. 각 설정 방법은 다음 부분을 참고하도록 합니다.

- VLAN 설정과 IP 주소: [**제3장 기본 네트워크 설정 – VLAN 설정, IP 주소/라우팅 설정**]
- 포트 바운더리: [**제6장 포트 바운더리 설정**]
- 장애 감시: [**제7장 부하 분산 설정 – 장애 감시 설정**]
- 실제 서버: [**제7장 부하 분산 설정 – 실제 서버 설정**]

참고: 고급 L7 캐시 서버 부하 분산은 HTTP 압축, SSL 가속과 같은 애플리케이션 가속 기능을 지원하며, 각 가속 기능을 사용하기 위해서는 HTTP 압축 규칙, SSL 가속이 미리 설정되어 있어야 합니다. 각 기능의 설정 방법은 다음 부분을 참고하도록 합니다.

- HTTP 압축 규칙: [**제7장 부하 분산 설정 – HTTP 압축 규칙 설정**]
- SSL 가속: [**제7장 부하 분산 설정 – SSL 가속 설정**]

CLI에서 설정하기

PAS-K에 고급 L7 캐시 서버 부하 분산을 설정하는 과정은 다음과 같습니다.

1. 패턴 정의
2. 고급 L7 서버 부하 분산 서비스 정의
3. 그룹 설정
4. URL 변경 설정
5. 규칙 설정
6. 필터 설정
7. 설정 정보 보기

1단계의 설정 과정은 L7 서버 부하 분산 설정 절에서 설명한 패턴 정의 설정 방법과 동일하고, 3~5단계의 설정 과정은 고급 L7 서버 부하 분산 서비스의 설정 방법과 동일합니다. 그러므로, 이 절에서는 고급 L7 서버 부하 분산 서비스를 정의하는 2단계와 필터를 정의하는 6단계, 설정 정보를 조회하는 7단계의 설정 과정에 대해서만 상세히 살펴봅니다.

고급 L7 캐시 서버 부하 분산 서비스 정의

고급 L7 캐시 서버 부하 분산 서비스를 정의하는 방법은 다음과 같습니다. 여러 개의 고급 L7 서버 부하 분산 서비스를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl7cslb** *<NAME>*	<고급 L7CSLB 설정 모드>에서 고급 L7 캐시 서버 부하 분산 서비스를 정의합니다. • *<NAME>* 알파벳과 숫자, '-', '_' 문자를 사용하여 최대 16 글자까지 지정. 첫 글자는 반드시 알파벳 사용.
2	**ip-version {ipv4 | ipv6}**	부하 분산 서비스의 네트워크 종류를 설정합니다. (기본값: ipv4)
3	**priority** *<PRIORITY>*	고급 L7 캐시 서버 부하 분산 서비스의 우선순위를 설정합니다. 우선순위 값이 작을수록 우선순위가 높습니다. • *<PRIORITY>* 우선순위 설정. (설정 범위: 0 ~ 255, 기본값: 100) **참고**: 설정한 우선순위를 기본값으로 변경하려면, <고급 L7CSLB 설정 모드>에서 **no priority** 명령을 사용합니다.

4	**health-check** *<HEALTH-CHECK>*	부하 분산 서비스를 적용하는 실제 서버의 상태를 확인하기 위한 장애 감시의 ID를 설정합니다. 부하 분산 서비스에 장애 감시를 설정하면 해당 부하 분산 서비스를 적용하는 모든 실제 서버에 장애 감시가 적용됩니다. • *<HEALTH-CHECK>* 장애 감시의 ID 설정. 하나의 부하 분산 서비스에는 최대 32 개의 장애 감시 ID 설정 가능. 여러 개의 장애 감시를 지정하는 경우에는 각 장애 감시의 ID 를 ','로 구분하고, 연속된 장애 감시 ID 는 '-'를 사용. **참고:** 설정한 장애 감시를 고급 L7 캐시 서버 부하 분산 서비스에서 삭제하려면 <고급 L7CSLB 설정 모드>에서 **no health-check** *<HEALTH-CHECK>*명령을 실행합니다. **참고:** 여러 개의 장애 감시를 지정하거나 실제 서버 설정 시 장애 감시를 지정한 경우에는 각각의 감시 결과가 모두 정상인 경우에만 실제 서버가 정상 동작 중인 것으로 간주합니다.
5	**preserve-src-addr {enable | disable}**	클라이언트가 송신한 요청 패킷의 출발지 IP 주소 유지 여부를 설정합니다. • **enable** 출발지 IP 주소를 유지하여 실제 서버로 전달. (기본값) • **disable** 출발지 IP 주소를 실제 서버와 연결된 인터페이스의 IP 주소로 변경하여 실제 서버로 전달. **참고:** IPv4 네트워크와 IPv6 네트워크는 주소 체계에 따른 호환성 문제로 인해 직접적인 통신을 할 수 없습니다. 그러므로, PAS-K가 IPv4 네트워크와 IPv6 네트워크의 경계에 위치한 경우에는 이 옵션을 비활성화하여 출발지 IP 주소를 변경함으로써 실제 서버의 IP 주소 버전과 일치시켜야 합니다.
6	**x-forwarded-for {enable | disable}**	'X-Forwarded-For' 헤더를 삽입할 지의 여부를 설정합니다. PAS-K가 Source NAT를 수행 할 경우, 서버에서 기존의 클라이언트 IP를 알기 위해서는 HTTP 요청에 'X-Forwarded-For' 헤더를 추가해야 합니다. • **enable** 'X-Forwarded-For' 헤더 삽입 • **disable** 'X-Forwarded-For' 헤더 삽입하지 않음 (기본값)
7	**ssl** *<SSL>* (선택 설정)	SSL 가속 기능을 사용할 경우에는 해당 서비스에서 사용할 SSL 프로필을 설정합니다. • *<SSL>* SSL 프로필 ID. 설정 범위: 1 ~ 256 **참고:** SSL 가속 기능을 설정하기 위해서는 SSL 프로필이 설정되어 있어야 합니다. SSL 프로필에 대한 상세한 설명은 이 장의 [**SSL 가속 설정 – CLI에서 설정하기 – 프로필 설정**] 절을 참고하시기 바랍니다.
8	**status {enable | disable}** (선택 설정)	고급 L7 캐시 서버 부하 분산 서비스의 사용 여부를 지정합니다. • **enable** 부하 분산 서비스 활성화 (기본값) • **disable** 부하 분산 서비스 비활성화
9	**current**	고급 L7 캐시 서버 부하 분산 서비스의 설정 정보를 확인합니다.
10	**apply**	고급 L7 캐시 서버 부하 분산 서비스를 저장하고 시스템에 적용합니다.

참고: 정의한 고급 L7 캐시 서버 부하 분산 서비스를 삭제하려면 <Configuration 모드>에서 **no advl7cslb** *<NAME>* 명령을 사용합니다.

그룹 설정

고급 L7 캐시 서버 부하 분산 서비스에 실제 서버의 그룹을 설정하는 방법은 고급 L7 서버 부하 분산 서비스에 실제 서버의 그룹을 설정하는 방법과 동일합니다. 그러므로, 고급 L7 캐시 서버 부하 분산 서비스에서 사용할 실제 서버의 그룹을 설정하는 방법은 **고급 L7 서버 부하 분산 설정** – **CLI에서 설정하기** – **그룹 설정** 절의 설명을 참고합니다.

URL 변경 설정

고급 L7 캐시 서버 부하 분산 서비스에 URL 변경 기능을 설정하는 방법은 고급 L7 서버 부하 분산 서비스에 URL 변경 기능을 설정하는 방법과 동일합니다. 그러므로, 고급 L7 캐시 서버 부하 분산 서비스에서 사용할 URL 변경 기능을 설정하는 방법은 **고급 L7 서버 부하 분산 설정** – **CLI에서 설정하기** – **URL 변경 설정** 절의 설명을 참고합니다.

규칙 설정

고급 L7 캐시 서버 부하 분산 서비스에 규칙을 설정하는 방법은 캐싱 기능을 설정할 수 없는 것을 제외하고는 고급 L7 서버 부하 분산 서비스에 규칙을 설정하는 방법과 동일합니다. 그러므로, 고급 L7 캐시 서버 부하 분산 서비스에서 사용할 규칙을 설정하는 방법은 **고급 L7 서버 부하 분산 설정** – **CLI에서 설정하기** – **규칙 설정** 절의 설명을 참고합니다.

필터 설정

고급 L7 캐시 서버 부하 분산 서비스를 어떤 트래픽에 적용할 것인지를 구분하기 위해 사용되는 필터를 정의하는 방법은 다음과 같습니다. 하나의 고급 L7 캐시 서버 부하 분산 서비스에는 최대 2048개의 필터를 등록할 수 있으므로, 여러 개의 필터를 설정하는 경우에는 <Configuration 모드>에서 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**advl7cslb** *<NAME>*	<고급 L7CSLB 설정 모드>로 들어갑니다. • *<NAME>* 필터를 설정할 L7 캐시 서버 부하 분산 서비스 이름
2	**filter** *<ID>*	L7 캐시 서버 부하 분산 서비스의 트래픽을 구분하기 위해 사용할 필터를 정의합니다. • *<ID>* 필터의 ID. 설정 범위: 1 ~ 256

참고: 이후의 과정은 필터링에 사용될 조건을 지정하는 과정입니다. 모든 과정을 수행할 필요는 없고 필터링시 사용할 항목에 해당되는 과정만 수행하면 됩니다. 필터링에 사용할 조건에 따라 이동할 단계는 다음과 같습니다. 하나의 필터에는 여러 개의 조건이 추가될 수 있으므로 하나의 조건을 추가한 후 다른 과정으로 이동하여 다른 조건을 계속 추가하면 됩니다.

출발지 IP 주소 → 3 번 과정
출발지 포트 번호 → 4 번 과정
목적지 IP 주소 → 5 번 과정
목적지 포트 번호 → 6 번 과정

3	**sip** *<SIP>*	필터링 조건으로 사용할 출발지 IP 주소와 넷 마스크 비트 수를 입력합니다. IPv6인 경우에는 IPv6 주소와 Prefix를 설정합니다. • *<SIP>* 출발지 IP 주소 및 서브넷 마스크 비트 수
4	**sport** *<SPORT>*	필터링 조건으로 사용할 출발지 포트 번호를 입력합니다. • *<SPORT>* 출발지 포트 번호. 설정 범위: 1 ~ 65535
5	**dip** *<DIP>*	필터링 조건으로 사용할 목적지 IP 주소와 넷 마스크 비트 수를 입력합니다. IPv6인 경우에는 IPv6 주소와 Prefix를 입력합니다. • *<DIP>* 목적지 IP 주소 및 서브넷 마스크 비트 수
6	**dport** *<DPORT>*	필터링 조건으로 사용할 목적지 포트 번호를 입력합니다. • *<DPORT>* 목적지지 포트 번호. 설정 범위: 1 ~ 65535
7	**status** {**enable** | **disable**} (선택 설정)	필터의 사용 여부를 지정합니다. • **enable** 필터 활성화 (기본값) • **disable** 필터 비활성화
8	**current**	필터의 설정 정보를 확인합니다.
9	**apply**	필터를 저장하고 시스템에 적용합니다.

참고: 정의한 필터를 삭제하려면 <고급 L7CSLB 설정 모드>에서 **no filter** *<ID>* 명령을 사용합니다.

설정 정보 보기

고급 L7 캐시 서버 부하 분산 서비스의 설정 작업이 끝나면 다음과 같은 방법으로 설정 정보를 확인할 수 있습니다.

고급 L7 캐시 서버 부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 고급 L7 캐시 서버 부하 분산 서비스의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **`show advl7slb`** 명령을 사용합니다. **`show advl7slb`** 명령은 현재 PAS-K에 정의된 고급 L7 캐시 서버 부하 분산 서비스의 목록과 기본적인 설정 정보를 보여줍니다. 특정한 고급 L7 캐시 서버 부하 분산 서비스에 대한 상세한 설정 정보를 보려면 해당 서비스의 이름을 입력하면 됩니다.

고급 L7 캐시 서버 부하 분산 서비스의 모든 설정 정보 보기

각 고급 L7 캐시 서버 부하 분산 서비스의 설정 정보와 해당 서비스에 대한 통계 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **`show info advl7slb`** *<NAME>* 명령을 사용합니다.

서비스의 이름을 입력하지 않고 명령을 실행하면 모든 고급 L7 캐시 서버 부하 분산 서비스에 대한 정보가 출력되고 서비스의 이름을 입력하면 해당 서비스에 대한 정보만 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

세션 엔트리 및 통계 정보 출력

이 절에서는 CLI 명령을 사용하여 부하 분산 서비스의 실제 서버를 통해 연결된 세션 엔트리 목록과 지속 연결 엔트리를 출력하고, 특정한 세션 엔트리와 지속 연결 엔트리를 삭제하는 방법을 살펴봅니다. 그리고, 각 부하 분산 서비스와 실제 서버의 세션 통계 정보를 출력하는 방법을 알아봅니다.

세션 엔트리 목록 보기

세션 엔트리 목록 보기

PAS-K에 정의된 부하 분산 서비스의 실제 서버를 통해 현재 연결되어 있는 모든 세션 엔트리를 확인하려면<Privileged 모드> 또는 <Configuration 모드>에서 다음 명령을 사용합니다.

명 령	설 명
show entry	현재 연결된 모든 세션 엔트리의 목록 중 일부의 정보만 출력합니다.
show entry-detail	현재 연결된 모든 세션 엔트리의 목록과 정보를 출력합니다.
show entry-adv	고급 부하 분산 서비스의 모든 세션 엔트리의 목록과 정보를 출력합니다.

참고: show entry 명령은 **show entry-detail** 명령에 비해 사용자가 식별하기 쉬운 출력 화면을 제공하는 반면, 프로토콜 번호 정보는 제공하지 않습니다. 프로토콜 번호 정보를 확인하려면, **show entry-detail** 명령을 사용합니다.

참고: show entry-adv 명령은 고급 방화벽/VPN 부하 분산, 고급 L7 서버 부하 분산, 고급 L7 캐시 서버 부하 분산 서비스의 세션 엔트리 목록과 정보 만을 제공합니다.

특정 세션 엔트리 목록 보기

특정 옵션 별 세션 엔트리 출력

사용자가 지정한 옵션의 종류에 따라 세션 엔트리 정보를 확인하려면 <Privileged 모드> 또는 <Configuration 모드>에서 다음과 같은 명령을 제공합니다.

- 특정 출발지/목적지 IP 주소 출력 — **show {entry | entry-detail | entry-adv} ip** *<IP>*
- 특정 출발지 IP 주소 출력 — **show {entry | entry-detail | entry-adv} sip** *<SIP>*
- 특정 목적지 IP 주소 출력 — **show {entry | entry-detail | entry-adv} dip** *<DIP>*
- 특정 포트 출력 — **show {entry | entry-detail | entry-adv} port** *<PORT>*
- 특정 출발지 포트 출력 — **show {entry | entry-detail | entry-adv} sport** *<SPORT>*
- 특정 목적지 포트 출력 — **show {entry | entry-detail | entry-adv} dport** *<DPORT>*
- 특정 프로토콜 출력 — **show {entry | entry-detail | entry-adv} protocol** *<PROTOCOL>*
- 특정 실제 서버 출력 — **show {entry | entry-detail} real** *<REAL>*
- 특정 부하 분산 서비스의 출력 — **show {entry | entry-detail} service** *<SERVICE>*
- 특정 IP 버전(IPv4, IPv6) 출력 — **show entry-adv ip-version** *<VERSION>*

참고: protocol 종류 또는 service 종류를 확인하거나, port 설정 범위를 확인하려면 각각의 명령어 뒤에 '?' 를 입력합니다.

특정 부하 분산 서비스의 지속 연결 세션 엔트리 출력

특정 부하 분산 서비스의 지속 연결 세션 엔트리 정보만 출력하고자 할 경우, <Privileged 모드> 또는 <Configuration 모드>에서 **show persist** *<SERVICE>* 명령을 실행합니다.

지속 연결 세션 엔트리 목록 보기

지속 연결 세션 엔트리의 정보를 확인하려면 <Privileged 모드> 또는 <Configuration 모드>에서 **show persist** 명령을 사용합니다.

세션 엔트리 삭제하기

모든 세션 엔트리와 지속 연결 세션 엔트리를 삭제하려면 <Privileged 모드> 또는 <Configuration 모드>에서 다음의 명령을 사용합니다.

명 령	설 명
no entry **no entry-detail**	현재 연결된 모든 세션 엔트리 목록과 정보를 삭제합니다.
no entry-adv	고급 부하 분산 서비스의 모든 세션 엔트리 목록과 정보를 삭제합니다.
no entry-advl4slb	고급 L4 서버 부하 분산 서비스의 모든 세션 엔트리 목록과 정보를 삭제합니다.
no persist	지속 연결 세션 엔트리 목록과 정보를 삭제합니다.
no persist-advl4slb	고급 L4 서버 부하 분산 서비스의 지속 연결 세션 엔트리 목록과 정보를 삭제합니다.

L4 지속 연결 세션 엔트리는 다른 세션 엔트리에서 사용하고 있지 않은 경우에만 삭제할 수 있습니다. 다른 세션 엔트리에서 사용 중인지는 **show persist** 명령의 출력 값 중에서 'refcnt' 항목을 통해 확인할 수 있습니다. 'refcnt ' 항목은 지속 연결 세션 엔트리를 사용하고 있는 세션 엔트리의 개수를 보여주는 값으로, 이 항목이 '0'인 지속 연결 세션 엔트리만 삭제할 수 있습니다.

refcnt는 **no persist** 명령을 실행해도 삭제되지 않습니다. 지속 연결 세션 엔트리를 반드시 삭제해야 하는 경우에는 먼저 **no entry** 명령을 사용하여 지속 연결 엔트리를 사용하고 있는 세션 엔트리를 삭제하고 **show persist** 명령으로 'refcnt' 값이 0인지 확인한 후에 **no persist** 명령으로 삭제합니다.

특정 세션 엔트리와 지속 연결 세션 엔트리를 삭제하려면 <Privileged 모드> 또는 <Configuration 모드>에서 다음의 명령을 사용합니다.

명 령	설 명
no entry dip *<DIP>*	특정 목적지 IP 주소에 대한 세션 엔트리 목록과 정보를 삭제합니다. • *<DIP>* 목적지 IP 주소
no entry dport *<DPORT>*	특정 목적지 포트에 대한 세션 엔트리 목록과 정보를 삭제합니다. • *<DPORT>* 목적지 포트 번호. 설정 범위: 1 ~ 65535
no entry ip *<IP>*	특정 IP 주소에 대한 세션 엔트리 목록과 정보를 삭제합니다. • *<IP>* IP 주소
no entry port *<PORT>*	특정 포트에 대한 세션 엔트리 목록과 정보를 삭제합니다. • *<PORT>* 목적지 포트 번호. 설정 범위: 1 ~ 65535
no entry protocol *<PROTOCOL>*	특정 프로토콜에 대한 세션 엔트리 목록과 정보를 삭제합니다. • *<PROTOCOL>* 프로토콜. (gre/tcp/udp/dccp/icmp/sctp/udplite)
no entry real *<REAL>*	특정 실제 서버에 대한 세션 엔트리 목록과 정보를 삭제합니다. • *<REAL>* 실제 서버 ID
no entry service *<SERVICE>* [**name** *<NAME>*]	특정 부하 부산 서비스에 대한 세션 엔트리 목록과 정보를 삭제합니다. • *<SERVICE>* 부하 분산 서비스 종류. • *<NAME>* 부하 분산 서비스 이름

no entry sip <*SIP*>	특정 출발지 IP 주소에 대한 세션 엔트리 목록과 정보를 삭제합니다. • <*SIP*> 출발지 IP 주소
no entry sport <*SPORT*>	특정 출발지 포트에 대한 세션 엔트리 목록과 정보를 삭제합니다. • <*SPORT*> 출발지 포트 번호. 설정 범위: 1 ~ 65535
no persist dip <*DIP*>	특정 목적지 IP 주소에 대한 지속 연결 세션 엔트리 목록과 정보를 삭제합니다. • <*DIP*> 목적지 IP 주소
no persist ip <*IP*>	특정 IP 주소에 대한 지속 연결 세션 엔트리 목록과 정보를 삭제합니다. • <*IP*> IP 주소
no persist service <*SERVICE*> [**name** <*NAME*>]	특정 부하 부산 서비스에 대한 지속 연결 세션 엔트리 목록과 정보를 삭제합니다. • <*SERVICE*> 부하 분산 서비스 종류. • <*NAME*> 부하 분산 서비스 이름
no persist sip <*SIP*>	특정 출발지 IP 주소에 대한 지속 연결 세션 엔트리 목록과 정보를 삭제합니다. • <*SIP*> 출발지 IP 주소

통계 정보 보기

이 절에서는 CLI에서 부하 분산 서비스와 관련된 통계 정보를 조회하는 방법에 대해 설명합니다.

CLI에서 보기

지정한 종류의 부하 분산 서비스의 통계 정보 출력

PAS-K는 부하 분산 서비스의 종류 별로 세션 통계 정보를 출력할 수 있도록 다음과 같은 명령을 제공합니다.

- L4 서버 부하 분산 서비스 **show statistics slb**
- L4 캐시 서버 부하 분산 서비스 **show statistics cslb**
- 방화벽/VPN 부하 분산 서비스 **show statistics fwlb**
- 게이트웨이 부하 분산 서비스 **show statistics gwlb**
- 글로벌 서버 부하 분산 서비스 **show statistics gslb**
- L7 서버 부하 분산 서비스 **show statistics l7slb**
- 고급 L7 서버 부하 분산 서비스 **show statistics advl7slb**
- L7 캐시 서버 부하 분산 서비스 **show statistics l7cslb**
- 고급 L7 캐시 서버 부하 분산 서비스 **show statistics advl7cslb**

특정 부하 분산 서비스의 통계 정보 출력

앞에서 살펴본 **show statistics** 명령에 서비스의 이름을 지정하면, 지정한 서비스에 대한 상세한 통계 정보를 확인할 수 있습니다.

show statistics {**slb** | **cslb** | **fwlb** | **gwlb** | **l7slb** | **l7cslb** | **advl7cslb** | **advl7slb** | **gslb**} *<NAME>*

L7 부하 분산 서비스에 대한 통계 정보를 조회하는 경우, **group** 명령어를 옵션으로 지정하여 특정 그룹에 대한 세션 통계 정보만을 출력할 수도 있습니다.

show statistics {**l7slb** | **l7cslb** | **advl7cslb** | **advl7slb**} *<NAME>* **group** *<GROUP>*

실제 서버의 통계 정보 출력

PAS-K는 실제 서버의 세션 통계 정보를 출력할 수 있도록 다음과 같은 명령을 제공하며, 실제 서버의 ID를 지정하면, 지정한 실제 서버에 대한 통계 정보만 확인할 수 있습니다.

show statistics real *<ID>*

부하 분산 서비스 목록 보기

현재 PAS-K에 정의된 모든 부하 분산 서비스 목록을 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **`show lb`** 명령을 사용합니다. **`show lb`** 명령은 현재 PAS-K에 정의된 부하 분산 서비스의 이름과 유형, 우선순위, 활성화 상태, 서비스를 적용하는 실제 서버 개수 정보를 보여줍니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

제8장
Failover 설정

이 장에서는 failover를 위한 VRRP(Virtual Router Redundancy Protocol)와 eVRRP(Enhanced VRRP)에 대해 살펴본 후 PAS-K에 failover를 구성하기 위해 이 기능들을 PAS-K에서 설정하는 방법에 대해 설명합니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- VRRP와 eVRRP
- eVRRP 설정하기
- Failover 설정 정보 보기

VRRP와 eVRRP

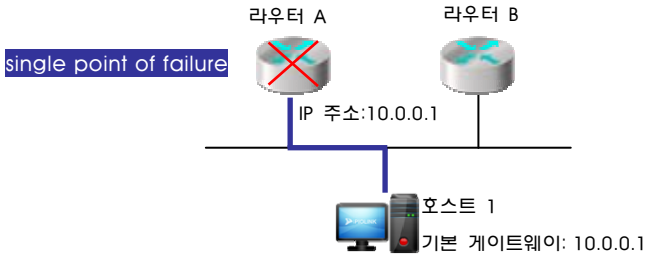
VRRP 개요

호스트에서 특정 목적지로 데이터를 전송하기 위한 경로를 검색하는 방법에는 동적 라우팅(dynamic routing)과 정적 라우팅(static routing)이 있습니다. 동적 라우팅은 RIP나 OSPF와 같은 라우팅 프로토콜을 사용하여 자동으로 네트워크 간의 최적의 경로를 결정하여 라우팅 테이블을 유지하고, 장비의 다운 등으로 인해 라우팅 테이블에 있는 경로가 유효하지 않을 경우에는 자동으로 다른 경로를 검색해줍니다. 이러한 동적 라우팅은 사용자가 별도의 경로 설정 작업을 하지 않아도 되기 때문에 편리하지만, 경로 검색 시 소요되는 시간과 송수신되는 트래픽의 양이 많아 네트워크에 부하가 많이 발생할 수 있습니다.

정적 라우팅은 사용자가 직접 목적지마다 고정 경로를 지정하여 라우팅 테이블을 구성합니다. 정적 라우팅은 경로를 검색할 필요가 없기 때문에 경로 검색으로 인한 부하는 적지만, 라우팅 테이블의 경로가 유효하지 않게 되었을 때 이를 대체할 경로가 자동으로 설정되지 않기 때문에 통신에 장애가 발생할 수 있습니다. 최악의 경우, 기본 게이트웨이로 지정된 장비가 다운되면 외부 네트워크와의 통신이 불가능하게 됩니다. 정적 라우팅에서 기본 게이트웨이와 같이 오직 하나만 존재하여 해당 경로가 다운되었을 때 통신이 끊어지는 경로를 'single point of failure'라고 합니다.

VRRP는 정적 라우팅에 마스터 라우터와 하나 이상의 백업 라우터를 이용하여 마스터 라우터가 다운되었을 때 자동으로 백업 라우터가 마스터의 역할을 수행하도록 하는 이중화(redundancy) 기능을 추가로 지원하는 프로토콜입니다. 이러한 마스터/백업 라우터 이중화 기능은 마스터 라우터가 다운된 경우에도 중단 없이 서비스를 제공할 수 있게 해줍니다. VRRP를 사용하면 동적 라우팅으로 인해 발생하는 경로 검색의 부하를 줄이는 것과 동시에 정적 라우팅의 가장 큰 문제점인 single point of failure가 발생하는 것을 막아줍니다.

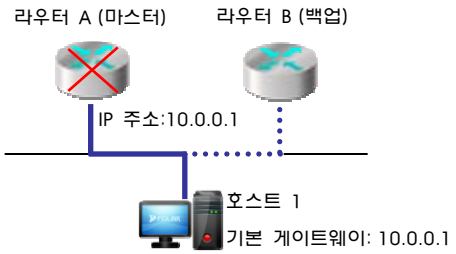
다음 그림은 VRRP를 사용하지 않은 네트워크에서 발생할 수 있는 single point of failure를 보여줍니다.



[그림 - VRRP를 사용하지 않은 네트워크에서 발생하는 Single Point of Failure]

앞의 그림에서 호스트 1은 IP 주소가 10.0.0.1인 라우터 A를 기본 게이트웨이로 사용합니다. 만약, 라우터 A가 다운되면 호스트 1에서 다른 네트워크와의 통신이 불가능해집니다. 이 경우, 호스트 1의 통신 장애의 원인이 된 라우터 A를 single point of failure라고 할 수 있습니다.

이번에는 동일한 네트워크를 VRRP로 구성하여 라우터 A를 마스터로, 라우터 B를 백업으로 설정한 경우를 살펴봅니다.

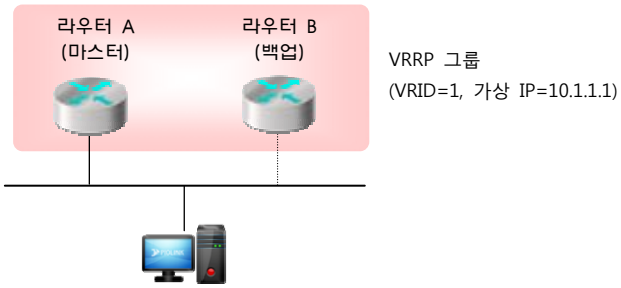


[그림 - VRRP를 사용한 네트워크]

위와 같은 VRRP 구성에서는 호스트 1의 기본 게이트웨이인 라우터 A가 다운된 경우에도 백업으로 설정된 라우터 B에 의해(점선으로 된 경로를 사용하여) 외부와 통신할 수 있습니다. 따라서 single point of failure에 의한 통신 장애가 발생하지 않게 됩니다.

VRRP 그룹

VRRP에서 하나의 마스터 라우터와 여러 개의 백업 라우터로 구성되는 라우터의 그룹을 VRRP 그룹이라고 합니다. VRRP 그룹은 여러 개의 라우터가 하나의 라우터인 것처럼 동작하기 때문에 가상 라우터(virtual router)라고도 합니다. 다음 그림은 라우터 A와 라우터 B로 구성된 VRRP 그룹을 보여줍니다.



[그림 - VRRP의 VRRP 그룹]

VRRP 그룹은 고유한 VRID 값과 하나의 가상 IP 주소, 그리고 가상 MAC 주소를 가지고 있습니다. VRRP 그룹에 속한 라우터들은 'VRRP 라우터'라고 합니다.

마스터 라우터(Master Router)

마스터 라우터는 VRRP 그룹에 속한 VRRP 라우터 중에서 자신의 인터페이스 주소가 VRRP 그룹의 가상 IP 주소로 사용되는 라우터입니다. 가상 IP 주소를 통해 VRRP 그룹으로 전송된 데이터는 실제로는 인터페이스 주소를 사용하는 마스터 라우터로 전송되고 마스터 라우터에서 이 데이터를 목적지로 전송합니다. 그리고, 가상 IP 주소에 대한 ARP 요청도 마스터 라우터에서 응답하게 됩니다.

마스터 라우터는 주기적으로 자신의 상태와 우선순위를 포함한 정보를 VRRP 그룹 내의 다른 VRRP 라우터에게 전송합니다. 마스터 라우터에 의해 전송되는 이 정보를 advertisement라고 하며, 백업 라우터는 수신된 advertisement를 통해 마스터 라우터의 상태와 우선순위를 파악하고 새로운 마스터 라우터의 선출 여부를 판단하게 됩니다.

백업 라우터(backup router)

백업 라우터는 VRRP 그룹에서 하나의 마스터 라우터를 제외한 나머지 VRRP 라우터들을 의미합니다. 마스터 라우터가 정상적으로 동작하는 동안에는 advertisement를 수신하는 것 외에 백업 라우터가 수행하는 작업은 없습니다. 지정된 시간 내에 마스터 라우터로부터 advertisement가 수신되지 않으면 백업 라우터는 마스터 라우터가 정상적으로 동작하지 않는 것으로 판단하고, 우선순위가 가장 높은 백업 라우터가 새로운 마스터 라우터로 선출됩니다. 이 경우, 새로운 마스터 라우터로 선출된 백업 라우터가 마스터 라우터의 역할을 이어 받습니다.

가상 IP 주소(virtual IP address)와 가상 MAC 주소(virtual MAC address)

가상 IP 주소는 마스터 라우터가 자신의 인터페이스 주소로 사용하는 VRRP 그룹의 IP 주소입니다. 마스터 라우터는 가상 IP 주소에 대한 ARP 요청에 대해 응답합니다. 가상 MAC 주소는 VRRP 그룹의 ID 값에 따라 자동으로 할당됩니다.

VRRP 라우터 우선순위

VRRP 라우터의 우선순위는 VRRP 그룹의 백업 라우터들 중에서 마스터 라우터를 선출할 때 기준이 되는 값입니다. VRRP 라우터 우선순위는 1 ~ 254 범위의 값으로 사용자가 직접 지정할 수 있고, 값이 클수록 우선순위는 높습니다. 마스터 라우터에 장애가 발생했을 때, 백업 라우터 중 우선순위가 가장 높은 라우터가 마스터 라우터로 선출됩니다.

eVRRP(Enhanced VRRP) 개요

PAS-K는 L4, L7 부하 분산 서비스의 failover를 지원하기 위해 기존 VRRP를 개선한 eVRRP를 지원합니다. 이 절에서는 eVRRP에 추가된 개념들과 eVRRP의 방식에 대해 소개합니다.

참고: eVRRP와 VRRP의 공통적인 특징은 이 절의 바로 앞에 있는 VRRP 개요 절의 내용을 참고합니다. eVRRP에서는 라우터라는 용어 대신 스위치를 사용합니다. 스위치의 의미는 VRRP에서의 라우터와 동일합니다.

가상 스위치(virtual switch)

eVRRP의 가상 스위치는 여러 인터페이스의 모음(group)으로 failover의 단위입니다. 일반적으로 가상 스위치는 외부 네트워크와 연결되는 아웃바운드 인터페이스(outbound interface)와 내부 네트워크에 연결되는 인바운드 인터페이스(inbound interface)로 구성됩니다. PAS-K는 VLAN 인터페이스만 지원하므로 가상 스위치에는 2개 이상의 VLAN 인터페이스가 속하게 됩니다. 가상 스위치는 하나 이상의 VRRP 그룹에 포함될 수 있습니다. 뿐만 아니라, 설정에 따라 가상 스위치는 IP가 동일한 그룹일 수 있습니다. 이는 같은 IP 주소를 사용하지만 서비스에 따라 다른 포트를 사용하는 경우입니다.

VRRP 그룹

eVRRP에서 VRRP 그룹은 가상 스위치의 모음으로 하나의 마스터 가상 스위치와 여러 개의 백업 가상 스위치들로 구성됩니다. VRRP 그룹의 마스터 가상 스위치에 속한 인터페이스만 사용되고 백업 가상 스위치에 속한 인터페이스들은 대기 상태가 됩니다. VRRP 그룹은 고유한 ID를 가지고 있으며, 이 값은 VRRP 그룹을 구분하고 VRRP 그룹의 가상 MAC 주소를 할당 받는데 사용됩니다. 하나의 PAS-K에는 여러 개의 VRRP 그룹을 설정할 수 있습니다. 여러 VRRP 그룹을 설정한 경우, 일부는 마스터로 나머지는 백업으로 설정하는 것이 가능합니다.

가상 서비스 IP 주소 (SVIP– Service Virtual IP Address)

eVRRP의 가상 서비스 IP 주소는 가상 스위치에 속한 인터페이스에 정의되어 있는 부하 분산 서비스 중에서 eVRRP를 적용할 부하 분산 서비스의 IP 주소입니다. 외부 네트워크의 클라이언트는 가상 서비스 IP 주소를 실제 서버들의 IP 주소로 인식하고, 가상 서비스 IP 주소를 목적지 IP 주소로 하여 실제 서버의 서비스를 요청합니다. 가상 서비스 IP 주소로 수신된 데이터는 부하 분산 서비스에 의해 실제 서버로 전송됩니다. 하나의 VRRP 그룹에는 최대 10개의 가상 서비스 IP 주소를 설정할 수 있습니다. 즉, 최대 10개의 가상 서비스 IP 주소를 하나의 VRRP 그룹으로 설정할 수 있습니다.

참고: 만일 하나의 가상 서비스 IP 주소에 여러 포트를 사용할 경우, 하나의 VRRP 그룹에 10개 이상의 서비스를 등록할 수 있습니다.

주의: 가상 서비스 IP 주소는 단일 VRRP 구성인 경우에는 설정하지 않습니다. 설정 시에는 PAS-K가 오동작할 가능성이 있습니다.

마스터 가상 스위치

마스터 가상 스위치는 VRRP의 마스터 라우터와 마찬가지로 VRRP 그룹에 속한 가상 스위치 중에서 자신의 인터페이스 주소 혹은 서비스 주소로 VRRP 그룹의 주소(가상 IP 주소)를 사용하는 스위치입니다. 가상 서비스 IP 주소나 가상 IP 주소를 목적지로 하여 전송된 데이터는 그 주소를 인터페이스 주소 혹은 서비스 주소로 사용하는 마스터 라우터로 전송되고 마스터 라우터에서 이 데이터를 목적지(실제 서버)로 전송합니다. 그리고, 가상 서비스 IP 주소나 가상 IP 주소에 대한 ARP 요청도 마스터 라우터에서 응답하게 됩니다.

마스터 가상 스위치는 주기적으로 자신의 상태와 우선순위를 포함한 advertisement를 VRRP 그룹 내의 백업 가상 스위치로 전송합니다. 백업 가상 스위치는 수신된 advertisement를 통해 마스터 가상 스위치의 상태와 우선순위를 파악하고 새로운 마스터 가상 스위치를 선출해야 하는지를 판단하게 됩니다.

백업 가상 스위치

백업 가상 스위치는 VRRP 그룹에서 하나의 마스터 가상 스위치를 제외한 나머지 가상 스위치들입니다. 백업 가상 스위치는 마스터 가상 스위치로부터 주기적으로 advertisement를 수신합니다. 백업 가상 스위치가 마스터 가상 스위치가 다운된 것으로 판단하기 전까지 advertisement를 기다리는 시간을 'Dead 간격'이라고 합니다. Dead 간격이 경과할 때까지 마스터 가상 스위치로부터 advertisement가 수신되지 않으면 백업 가상 스위치는 마스터 가상 스위치가 정상적으로 동작하지 않는 것으로 판단하고, 우선순위가 가장 높은 백업 가상 스위치를 새로운 마스터 가상 스위치로 선출합니다. PAS-K에서는 dead 간격을 다음과 같은 공식을 사용하여 계산합니다.

Dead 간격 = advertisement 전송 주기 x 재시도 횟수 + 0.5 x ARP 체크 횟수

공식에서 알 수 있듯이 백업 가상 스위치는 설정된 재시도 횟수만큼 advertisement 전송 주기가 지날 때까지 advertisement를 기다린 후 설정된 ARP 체크 횟수만큼 ARP 요청을 마스터 가상 스위치에게 전송합니다.

PAS-K에서 백업 가상 스위치가 마스터 스위치가 되기 위해서는 백업 가상 스위치 중에서 우선순위가 가장 높아야 하고 선점(preemption) 기능이 활성화되어 있어야 합니다. 선점 기능이 비활성화되어 있는 백업 스위치는 우선순위가 가장 높은 경우에도 마스터 가상 스위치로 선출되지 않습니다.

트랙 포트(track port)와 가상 스위치의 우선순위

VRRP에서는 VRRP 그룹의 마스터 라우터를 선택할 때 각 VRRP 라우터에 설정되어 있는 우선순위를 사용합니다. 이 값은 사용자가 직접 지정하고 failover 동작 중에 변경되지 않습니다.

eVRRP(Enhanced VRRP)에서는 마스터 가상 스위치를 선택할 때 가상 스위치의 기본 우선순위와 트랙 포트의 우선순위를 합한 값을 사용합니다. 가상 스위치의 기본 우선순위는 VRRP 라우터의 우선순위와 마찬가지로 사용자가 직접 설정합니다. 트랙 포트는 특정 포트마다 우선순위를 할당한 후 포트가 정상적으로 연결되어 있는 경우에는 포트의 우선순위가 가상 스위치의 기본 우선순위에 더해지고, 정상적이지 않은 경우에는 더해지지 않습니다. 트랙 포트는 동적인 포트의 동작 상태를 마스터 가상 스위치 선택 시 반영할 수 있게 해줍니다.

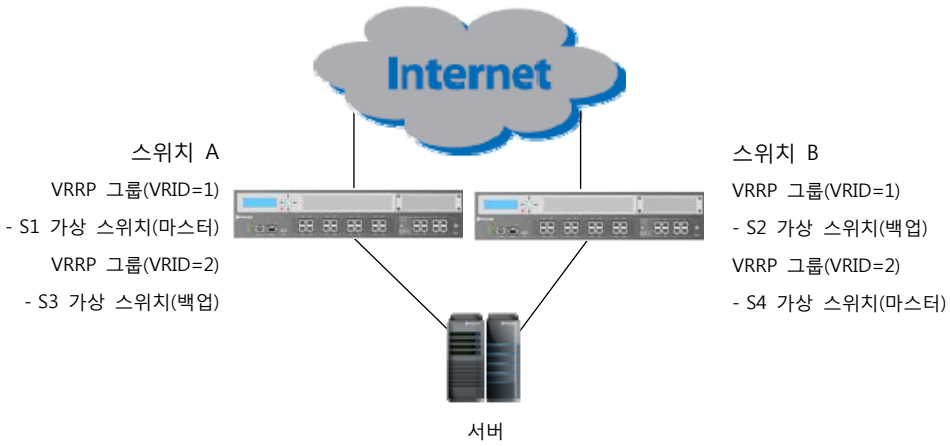
트랙 포트의 우선순위를 가상 스위치의 우선순위에 적용하는 방식에는 다음과 같은 '멤버 우선순위'와 '개별 우선순위'가 있습니다.

- **멤버 우선순위**
  멤버 우선순위는 두 개 이상의 트랙 포트를 하나의 그룹으로 설정하고, 트랙 포트 그룹에 우선순위를 부여합니다. 그룹에 속한 모든 포트가 연결되어 있지 않은 경우에만 가상 스위치에 우선순위를 더하지 않습니다. 트랙 포트 그룹의 포트 중 하나라도 정상적으로 연결되어 있으면 가상 스위치의 기본 우선순위에 트랙 포트 그룹의 우선순위가 더해집니다. 예를 들어, 가상 스위치의 기본 우선순위가 100 이고, 포트 1, 2, 3 을 하나의 트랙 포트 그룹으로 구성하고 우선순위 30 을 설정한 경우, 포트 1, 2, 3 의 연결 상태가 모두 다운되지 않는 이상, 가상 스위치의 우선순위는 130 으로 유지됩니다.
- **개별 우선순위**
  개별 우선순위는 각 포트마다 우선순위를 부여하고, 포트의 연결 상태에 따라 가상 스위치의 기본 우선순위에 포트의 우선순위를 더하거나 혹은 더하지 않는 방식입니다. 예를 들어, 가상 스위치의 기본 우선순위가 100 이고, 포트 1, 2, 3 을 우선순위가 10 인 트랙 포트로 설정한 경우, 가상 스위치의 우선순위는 130 이 됩니다. 만약, 하나의 포트가 연결이 끊어지면 가상 스위치의 우선순위는 10 만큼 감소하여 120 이 됩니다.

Active-Standby Failover

Active-Standby 방식은 VRRP 그룹에서 하나의 마스터 가상 스위치만 동작(active)하고 나머지 백업 가상 스위치는 대기 상태(backup)로 존재하는 failover 방식입니다. 마스터 가상 스위치에 문제가 발생한 경우 백업 가상 스위치가 마스터의 역할을 수행하게 됩니다. 하나의 PAS-K에는 마스터와 백업 가상 스위치가 모두 존재할 수 있습니다.

다음은 각 PAS-K에 2개의 VRRP 그룹을 등록하여 Active-Standby failover를 구성한 예입니다.



[그림 - Active-Standby Failover 구성 예]

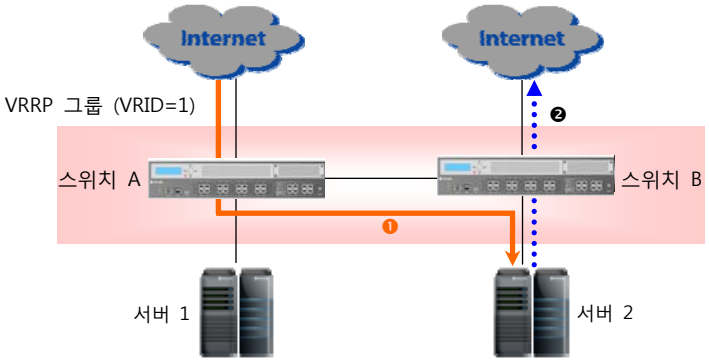
앞의 그림에서 스위치 A와 스위치 B에 VRRP 그룹의 마스터 가상 스위치(S1, S4)가 존재하기 때문에 두 스위치 모두 해당 마스터 가상 스위치에 속한 인터페이스를 통해 데이터를 처리합니다. 동시에 두 스위치에는 상대 스위치에 있는 마스터 가상 스위치에 대한 백업 가상 스위치(S2, S3)도 존재하기 때문에, 만약 마스터 가상 스위치에 문제가 발생하면 다른 스위치가 그 역할을 이어 받아 하나의 스위치만 동작하게 됩니다. 예를 들어, S1 가상 스위치에 문제가 발생하면 백업 가상 스위치인 S2가 마스터가 되기 때문에 스위치 B만 동작하게 됩니다.

Active-Standby failover방식은 두 스위치에 각각 두 개 이상의 부하 분산 서비스를 적절히 나누면, 두 스위치가 동시에 데이터를 처리하여 네트워크의 안정성을 보장함과 동시에 장비와 네트워크 자원을 낭비하지 않고 효율적으로 사용할 수 있습니다. 하지만, Active-Standby failover방식은 설정하는 과정이 복잡하고, 외부 라우팅 정보를 수정해야 하는 번거로움이 있습니다. 그리고 failover가 발생했을 때 마스터와 백업 간의 변환 과정도 기존의 VRRP에 비해 느립니다. 만약, 두 스위치가 하나의 부하 분산 서비스만 사용하여 각각 마스터와 백업으로 동작하거나 여러 개의 부하 분산 서비스를 사용하더라도 하나의 부하 분산 서비스를 사용할 때처럼 각 스위치가 마스터와 백업으로 동작하는 경우에는 설정 과정이 간단합니다. 그리고, 외부 라우팅 정보를 수정할 필요도 없고 필요하지 않고, failover 변환도 빠릅니다. 하지만, 이런 경우에는 하나의 스위치가 대기 상태로만 존재하기 때문에 기존 VRRP처럼 장비의 가용성이 떨어지게 됩니다.

BDR (Backup Direct Return)

BDR은 실제 서버로부터 수신된 패킷에 대한 세션을 가지고 있지 않은 스위치에서 새로운 세션을 생성하여 클라이언트로 직접 응답을 전송하는 기능입니다.

마스터 가상 스위치와 백업 가상 스위치가 서로 다른 네트워크와 서로 다른 서버에 연결되어 있는 다음과 같은 네트워크에 BDR 기능을 적용하는 경우를 예를 들어 살펴봅니다.



[그림 – BDR 기능 동작]

앞의 그림에서 서버 1과 서버 2는 동일한 웹 서비스를 제공하는 웹 서버입니다. 만약 네트워크 1에 연결된 클라이언트에서 스위치 A로 웹 서비스를 요청할 경우, 스위치 A는 부하 분산 서비스에 의해 이 요청을 부하 분산하여 서버 1이나 서버 2로 전송합니다. 부하 분산 결과, 서버 2가 선택되었다면, 스위치 A는 서비스 요청을 스위치 B를 통해 서버 2로 전송합니다(❶). 이 때, 서비스 요청에 대한 세션은 스위치 A에 있습니다. 서버 2는 서비스를 처리한 후, 요청에 대한 응답을 스위치 B로 전송해야 하고, 스위치 B는 서버 2에서 수신한 응답을 서비스를 요청한 클라이언트에게 전송해야 합니다. 하지만, 해당 클라이언트와의 세션은 스위치 A에 있으므로, 스위치 B에서 BDR 기능을 통해 스위치에서 새로운 세션을 생성하여 클라이언트로 직접 응답을 전송합니다(❷).

주의: 서버 부하 분산에서 BDR을 사용할 경우, 외부 네트워크의 클라이언트는 실제 서버로 접속할 수 없습니다.

주의 사항

Active- Standby 방식 사용 시 주의사항

Active-Standby 방식의 failover 기능을 사용할 때에는 다음과 같은 사항을 주의해야 합니다.

- Active-Standby 방식은 하나의 VRRP 그룹에 속한 부하 분산 서비스는 하나의 PAS-K에서만 처리할 수 있습니다. 따라서, 하나의 부하 분산 서비스를 여러 PAS-K에서 동시에 처리할 수 없습니다.
- 방화벽 부하 분산 구성에서 단일 Active-Standby failover를 적용할 경우, 모든 방식의 부하 분산 알고리즘이 사용 가능합니다. 그러나, 다중 Active-Standby failover를 적용할 경우에는 지속 연결 유지 시에 반드시 부하 분산 알고리즘을 해시(Hash)로 설정해야 합니다.

다중 VRRP 그룹 사용 시 주의사항

ARP 응답과 관련된 주의사항

- 기준이 되는 VRRP 그룹을 선정하여 가상 서비스 IP 주소를 설정해야 합니다.
  여러 VRRP 그룹이 있는 경우, PAS-K는 GWLB나 SLB 부하 분산 서비스에 설정된 가상 IP 주소(VIP)에 대한 ARP 응답을 하지 않습니다. 왜냐하면, 여러 개의 VRRP 그룹이 동시에 동작하고 있으므로 어떤 VRRP가 마스터가 될지 알 수 없기 때문입니다.
- 각 VRRP 그룹의 가상 IP 주소가 서로 겹치지 않도록 설정해야 합니다.
  VRRP 그룹의 가상 IP 주소가 겹쳐지면 failover 상태의 변환 과정에 따라 PAS-K가 가상 IP 주소에 대해 의도하지 않은 잘못된 ARP 응답을 보낼 수도 있습니다.

기타 주의사항

- 여러 VRRP 그룹이 설정되어 있는 경우, 항상 IP 포워딩 기능이 동작됩니다(자동으로 활성화 상태로 설정됩니다).
- 여러 VRRP 그룹이 설정되어 있는 경우, ARP 루프(loop) 방지를 위해 proxy ARP 기능이 동작하지 않고, 멀티캐스트 패킷의 루프 현상을 막기 위해 멀티캐스트 브리지 기능이 동작하지 않습니다(자동으로 비활성화 상태로 설정됩니다).
- OSPF나 BGP와 같은 동적 라우팅 프로토콜은 여러 VRRP 그룹이 설정되어 있는 경우에는 사용할 수 없습니다.

Stateful Failover

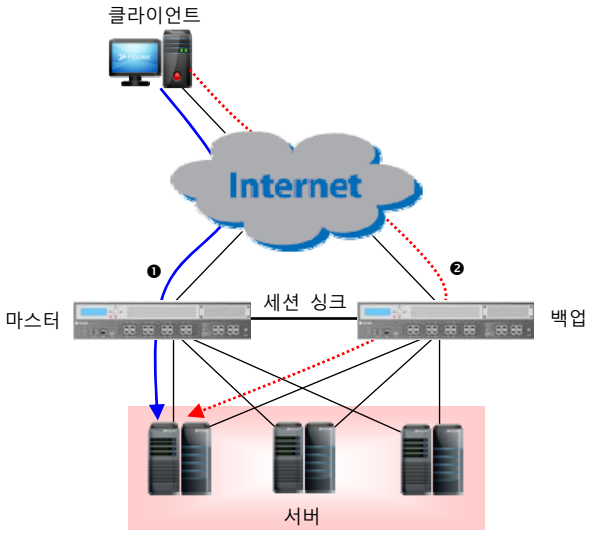
VRRP 기능이 적용된 네트워크에서는 마스터 가상 스위치가 다운되거나 우선순위가 감소되면 마스터 가상 스위치의 역할을 백업 가상 스위치가 이어 받게 됩니다. 따라서 사용자는 스위치 그룹 중 하나의 스위치에 문제가 발생하더라도 다른 스위치를 이용하여 클라이언트에게 중단없는 서비스를 제공할 수 있습니다. 하지만 클라이언트와 서버 간에 연결된 세션까지는 복구가 되지 않아서 기존에 진행 중이던 서비스의 연결은 끊어지고, 클라이언트는 서비스를 다시 요청해야 하는 불편함이 있습니다. PAS-K는 VRRP 기능과 함께 stateful failover 기능을 제공하여 이러한 문제를 해결합니다.

Stateful failover 기능은 failover가 발생하더라도 동일한 서버로 다시 연결되거나 기존에 연결된 세션을 통해 제공되던 서비스가 끊김없이 지속적으로 제공될 수 있도록 합니다. Stateful failover 기능을 활성화하면 마스터와 백업 가상 스위치는 일정한 주기마다 혹은 세션 수가 임계값에 도달했을 때 서로의 세션 정보를 주고 받아 동기화 작업을 수행합니다. 동기화 작업을 통해 마스터와 백업 가상 스위치는 각자 서비스하고 있는 모든 세션들의 정보를 서로 일치시킵니다. 이러한 세션의 동기화 작업을 세션 싱크(session sync)라고 합니다. 세션 싱크는 마스터와 백업 가상 스위치 간에 설정된 세션 싱크 VLAN을 통해 이루어집니다.

Stateful failover는 L4 서버 부하 분산 서비스마다 사용 여부를 설정할 수 있습니다.

Stateful Failover의 동작 예

다음은 failover를 위해 VRRP가 적용되어 있고 stateful failover가 활성화되어 있는 네트워크 환경 구성의 예입니다.



[그림 - Stateful Failover]

앞의 그림에서 클라이언트는 마스터 스위치를 통해 서버에서 제공하는 서비스를 사용하고, 마스터와 백업 스위치는 stateful failover가 활성화되어 서로의 세션 정보를 공유합니다. 클라이언트가 마스터 스위치를 통해 서비스(❶)를 이용하는 도중에 마스터 스위치의 문제로 인해 failover가 발생하면 백업 스위치가 마스터 스위치로 동작하게 됩니다. 새로 마스터가 된 스위치는 세션 정보를 이용하여 클라이언트와 서버 간에 설정된 세션을 그대로 복구하여 클라이언트에게 서비스(❷)를 지속적으로 제공합니다. 만약 stateful failover가 비 활성화되어 있으면 클라이언트는 마스터 스위치를 통해 새로운 세션으로 재 접속합니다.

Stateful Failover 사용 시 주의사항

ICMP 세션 동기화

Stateful failover가 활성화되어도 ICMP 세션은 동기화되지 않습니다. ICMP 세션은 타임아웃이 5초이기 때문에 일반적으로 failover에 소요되는 시간(5 ~10초)보다 짧습니다. 그리고 ICMP echo 요청에 대한 응답이 즉시 연이어 발생하고, 이전 요청/응답이 다음 요청/응답과 무관하기 때문에 이전의 세션을 복구하여 사용할 필요가 없습니다. 이와 같이 ICMP 세션은 세션 정보를 동기화할 필요나 의미가 없기 때문에 PAS-K의 stateful failover 기능은 ICMP 세션을 동기화하지 않습니다.

부하 분산 서비스

Stateful failover는 L4 서버 부하 분산 서비스만 지원합니다. Stateful failover 기능을 활성화하면 마스터와 백업 간에 전송되는 세션 정보의 양과 전송 횟수에 따라 L4 서버 부하 분산 성능이 저하될 수 있습니다.

eVRRP 설정하기

이 절에서는 PAS-K에 지금까지 살펴본 다음과 같은 failover 방식을 적용하는 방법에 대해 알아봅니다.

- Active-Standby Failover
- Stateful Failover

Stateful failover는 단독으로 사용될 수 없고 Active-Standby와 함께 사용해야 하는 failover 기능입니다. 그러므로, 먼저 Active-Standby를 설정한 후에 stateful failover 기능을 설정하도록 합니다.

참고: PAS-K에 eVRRP를 설정하기 전에 eVRRP를 적용할 VLAN 인터페이스와 L4, L7 부하 분산 서비스가 미리 설정되어 있어야 합니다.

Active-Standby Failover 설정

PAS-K에 Active-Standby failover를 구성하려면 먼저 VRRP 그룹을 생성해야 하고 VRRP 그룹에서 다음과 같은 항목들을 설정해야 합니다.

- Failover 모드
- 가상 스위치에 속하는 인터페이스 (필수)
- 인터페이스의 가상 IP 주소(필수)
- 가상 서비스 IP 주소
- 기본 우선순위
- 트랙 포트 우선순위/사용자 정의 우선순위 (필수)
- 선점 여부
- Advertisement 주기
- Dead 주기
- 가상 MAC 의 사용 여부
- 백업 상태 시 비활성화할 포트 바운더리

먼저 VRRP 그룹에서 필수적으로 설정해야 하는 failover 모드와 인터페이스 추가, 가상 IP 주소 설정, 트랙 포트 우선순위나 사용자 정의 우선순위의 설정 방법을 먼저 알아본 후 나머지 항목들의 설정 방법을 알아봅니다.

CLI에서 설정하기

필수 설정 과정

Active-Standby failover를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**failover**	<Failover 설정 모드>로 들어갑니다.
2	**vrrp** *<ID>*	VRRP 그룹을 생성하고 <VRRP 설정 모드>로 들어갑니다. • *<ID>* VRRP의 ID 설정 (설정 범위: 1 ~ 254)
3	**mode active-standby**	VRRP 그룹의 failover 모드를 **active-standby**로 설정합니다.

4	**interface** *<NAME>* **vip** *<VIP>*	VRRP 그룹의 가상 스위치에 포함시킬 인터페이스와 인터페이스의 가상 IP 주소를 설정합니다. • *<NAME>* 가상 스위치에 속할 VLAN 인터페이스의 이름 • *<VIP>* 부하 분산 서비스 대상이 아닌 데이터를 인터페이스와 연결된 실제 서버로 직접 전송할 때 사용할 가상 IP 주소 하나의 인터페이스에 최대 8개의 가상 IP 주소 지정 가능. 여러 개의 가상 IP 주소를 입력하는 경우에는 ','로 IP 주소를 구분하여 지정 **참고**: 설정한 인터페이스를 삭제하려면, **no interface** *<NAME>* 명령을 사용합니다.
5	**track-port** *<PRIORITY>* {**member-port** *<MEMBER-PORT>* | **port** *<PORT>*}	트랙 포트와 우선순위를 설정합니다. • *<PRIORITY>* 트랙 포트, 트랙 포트 멤버의 우선순위 (설정 범위: 1~255) • *<MEMBER-PORT>* 멤버에 포함될 여러 개의 트랙 포트를 지정. 각 포트를 ','로 구분하고, 연속된 포트는'-'를 사용 • *<PORT>* 개별 우선순위를 지정할 포트. 두 개 이상의 포트를 지정하는 경우에는 각 포트를 ','로 구분하고, 연속된 포트들을 지정할 때는 '-'를 사용 **참고**: 설정한 트랙 포트를 삭제하려면, **no track-port** *<PRIORITY>* {**member-port** *<MEMBER-PORT>* | **port** *<PORT>*} 명령을 사용합니다.
6	다음 절인 [**선택 설정 과정**]에 설명되어 있는 항목들 중에서 필요한 항목들을 설정합니다.	
7	**status** {**enable** | **disable**} (선택 설정)	VRRP 그룹의 사용 여부를 지정합니다. • **enable** VRRP 그룹 활성화 (기본값) • **disable** VRRP 그룹 비활성화
8	**current**	설정한 VRRP 그룹의 설정 정보를 확인합니다.
9	**apply**	VRRP 그룹의 설정을 시스템에 적용한 후 <Failover 설정 모드>로 빠져 나갑니다.

선택 설정 과정

VRRP 그룹의 가상 서비스 IP 주소를 지정하려면 <VRRP 설정 모드>에서 다음 명령을 실행합니다. 2개 이상의 VRRP 그룹을 설정하는 경우(다중 VRRP 설정) 가상 서비스 IP 주소를 반드시 지정해 주어야 합니다.

- **가상 서비스 IP 주소**

VRRP 그룹의 가상 서비스 IP 주소를 설정하려면, <VRRP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
svip *<SVIP>*[,*<SVIP>*,•••]	가상 서비스 IP 주소를 설정합니다. VRRP 그룹에 가상 서비스 IP 주소를 지정하지 않으면 PAS-K 에 정의되어 있는 모든 부하 분산 서비스가 하나의 VRRP 그룹으로 설정됩니다. • *<SVIP>* VRRP 그룹의 가상 서비스 IP 주소. 여러 개의 가상 서비스 IP 주소를 입력하는 경우에는 ','로 IP 주소를 구분하여 설정 가능.

참고: 다중 VRRP 그룹을 설정한 경우, 특정 VRRP 그룹에서 사용하고 싶지 않은 서비스의 가상 서비스 IP 주소를 '0.0.0.0'으로 설정합니다.

```
(config-failover-vrrp[1])# svip 0.0.0.0
```

참고: VRRP 그룹의 가상 서비스 IP 주소를 삭제하려면 다음 명령을 사용합니다.

```
(config-failover-vrrp[1])# no svip <SVIP>,<SVIP>,…
```

<SVIP> 항목에는 삭제할 가상 서비스 IP 주소를 입력합니다.

다음 항목들은 반드시 설정하지 않아도 기본값으로 충분히 failover가 이루어질 수 있는 항목들입니다. 하지만, 사용자 환경이나 정책에 따라 적절한 값을 설정하면 failover 기능을 보다 효율적으로 이용할 수 있습니다.

- **가상 스위치의 기본 우선순위**

가상 스위치의 기본 우선순위를 설정하려면, <VRRP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
priority *<PRIORITY>*	가상 스위치의 기본 우선순위를 설정합니다. • *<PRIORITY>* 기본 우선순위 설정 (설정 범위: 0 ~ 254, 기본값: 100) **참고**: 설정한 우선순위를 기본값으로 변경하려면, **no priority** 명령을 사용합니다.

- **선점 기능**

선점 설정은 VRRP 그룹의 백업 가상 스위치의 우선순위가 마스터 가상 스위치의 우선순위보다 높을 때, 백업 가상 스위치가 마스터 가상 스위치로 선출되도록 하는 기능입니다. 선점 기능이 비활성화되어 있는 백업 스위치는 우선순위가 마스터 가상 스위치보다 높은 경우에도 마스터 가상 스위치로 선출되지 않고, 마스터 가상 스위치가 다운 되었을 때만 마스터 가상 스위치로 선출됩니다.

가상 스위치의 선점(preemption) 기능 활성화 여부를 설정하려면, <VRRP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
preemption {enable | disable}	스위치의 선점 기능의 사용 여부를 지정합니다. • **enable** 스위치의 선점 기능 활성화 (기본값) • **disable** 스위치의 선점 기능 비활성화

- **가상 MAC의 사용 여부**

VRRP 그룹의 가상 IP 주소와 가상 서비스 IP 주소에 대한 MAC 주소로 가상 MAC 주소를 사용할 것인지 인터페이스의 실제 MAC 주소를 사용할 것인지 설정하려면, <VRRP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
vmac {enable | disable}	가상 MAC 주소 기능의 사용 여부를 지정합니다. • **enable** 가상 MAC 주소 기능 활성화 (기본값) • **disable** 가상 MAC 주소 기능 비활성화

- **Advertisement 전송 주기**

VRRP 그룹의 마스터 가상 스위치의 advertisement 전송 주기를 설정하려면, <VRRP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
advertise-interval *<ADVERTISE-INTERVAL>*	VRRP 그룹의 마스터 가상 스위치의 advertisement 전송 주기를 설정합니다. • *<ADVERTISE-INTERVAL>* advertisement 전송 주기 설정 (설정 범위: 1 ~ 255, 기본값: 1 (초)) **참고**: 설정한 advertisement 전송 주기를 기본값으로 변경하려면, **no advertise-interval** 명령을 사용합니다.

- **Dead 간격**

Dead 간격을 계산할 때 사용하는 advertisement 재전송 횟수와 ARP 체크 횟수를 설정하려면, <VRRP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
retry *<RETRY>*	advertisement 재전송 횟수를 설정합니다. • *<RETRY>* advertisement 재전송 횟수 설정 (설정 범위: 1 ~ 255, 기본값: 3 (회)) **참고**: 설정한 advertisement 재전송 횟수를 기본값으로 변경하려면, **no retry** 명령을 사용합니다.
arp-count *<ARP-COUNT>*	ARP 체크 횟수를 설정합니다. • *<ARP-COUNT>* ARP 체크 횟수 설정 (설정 범위: 0 ~ 255, 기본값: 0 (회)) **참고**: 설정한 ARP 체크 횟수를 기본값으로 변경하려면, **no arp-count** 명령을 사용합니다.

<RETRY> 항목에는 재시도 횟수를 입력하고 *<ARP-COUNT>* 항목에는 ARP 체크 횟수를 입력합니다. 이 두 항목은 다음과 같은 공식으로 dead 간격을 계산할 때 사용하는 값입니다.

Dead 간격(초) = advertisement 전송 주기 x 재시도 횟수 + 0.5 x ARP 체크 횟수

Dead 간격은 백업 가상 스위치가 마스터 가상 스위치의 다운 상태를 판단하기 전까지 마스터 가상 스위치로부터 advertisement의 수신을 기다리는 시간입니다. Dead 간격은 초 단위이고, 기본으로 설정된 dead 간격은 3초입니다.

- **포트 바운더리 비활성화**

VRRP 그룹의 백업 가상 스위치에 설정된 포트 바운더리가 promisc 모드인 경우, 백업 상태이지만 트래픽을 처리하게 됩니다. 이러한 상황을 방지하기 위해 백업 상태에서는 promisc 모드인 포트 바운더리를 비활성화 하도록 설정해야 합니다. 백업 상태에서 포트 바운더리를 비활성화 하도록 설정하려면, <VRRP 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
port-boundary *<PORT-BOUNDARY>*	백업 상태에서 비활성화할 포트 바운더리를 지정합니다. • *<ADVERTISE-INTERVAL>* 포트 바운더리 ID **참고**: 설정한 비활성화 포트 바운더리를 삭제하려면, **no port-boundary** *<PORT_BOUNDARY>* 명령을 사용합니다.

BDR 기능 설정

BDR 기능은 가상 스위치에서 클라이언트로 응답을 전송할 때 가상 스위치에서 클라이언트와의 세션을 가지고 있지 않으면 새로운 세션을 생성하여 전송하도록 하는 기능입니다. BDR 기능을 활성화하려면 <Failover 설정 모드>에서 다음 명령을 사용합니다.

명 령	설 명
bdr {**enable** | **disable**}	BDR 기능의 사용 여부를 지정합니다. • **enable** BDR 기능 활성화 • **disable** BDR 기능 비활성화 (기본값)

Stateful Failover 설정하기

Stateful failover 기능을 설정하려면 먼저 Active-Standby를 위한 설정 작업이 이미 완료되어 있어야 합니다. Active-Standby 설정 작업을 완료한 후 stateful failover를 설정하는 과정은 다음과 같습니다.

1. L4 서버 부하 분산 서비스의 세션 싱크 활성화
2. 세션 싱크 VLAN 생성
3. Stateful Failover 활성화

CLI에서 설정하기

L4 서버 부하 분산 서비스의 세션 싱크 활성화

L4 서버 부하 분산 서비스의 세션 싱크를 활성화하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**slb** *<NAME>*	<SLB 설정 모드>로 들어갑니다. • *<NAME>* Stateful failover를 설정할 L4 서버 부하 분산 서비스의 이름
2	**session-sync** {**enable** | **disable**}	세션 싱크 기능의 사용 여부를 지정합니다. • **enable** 세션 싱크 기능 활성화 • **disable** 세션 싱크 기능 비활성화 (기본값)
3	**apply**	세션 싱크 설정을 시스템에 적용합니다.

세션 싱크 VLAN 생성

세션 싱크를 위한 VLAN을 생성하고, 마스터 스위치와 백업 스위치간 연결된 포트를 해당 VLAN에 포함합니다. VLAN을 생성하는 방법은 **제3장 기본 네트워크 설정 – VLAN 설정 – CLI에서 설정하기 – VLAN 생성 및 포트 추가** 절을 참고하도록 합니다.

Stateful failover 활성화

Stateful failover 기능을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**failover**	<Failover 설정 모드>로 이동합니다.
2	**session-sync vlan** *<VLAN>*	세션 싱크 VLAN을 지정합니다. • *<VLAN>* 세션 싱크에 사용할 VLAN 이름
3	**session-sync interval** *<INTERVAL>*	마스터와 백업 가상 스위치간에 세션을 동기화하는 주기를 설정합니다. • *<INTERVAL>* 세션 정보의 교환 주기. (설정 범위: 1 ~ 10 기본값: 1(초))
4	**session-sync status** {**enable** | **disable**}	Stateful failover 기능의 사용 여부를 지정합니다. • **enable** Stateful failover 기능 활성화 • **disable** Stateful failover 기능 비활성화 (기본값) **주의:** Stateful failover 기능을 활성화하면 L4 부하 분산 서비스의 성능이 낮아질 수 있으므로 반드시 필요한 경우에만 stateful failover 기능을 사용하기를 권장합니다.
5	**current**	설정한 failover의 설정 정보를 확인합니다.
6	**apply**	failover 설정을 시스템에 적용합니다.

Failover 설정 정보 보기

이 절에서는 CLI에서 Failover의 설정 정보를 출력하는 방법에 대해 살펴봅니다.

CLI에서 보기

Failover 설정은 <Privileged 모드>, <Configuration 모드>에서 **show failover** 명령을 사용하여 조회할 수 있고, VRRP 그룹 설정과 동작 상태는 <Failover 설정 모드>에서 **show vrrp** 명령을 사용하여 조회할 수 있습니다. VRRP의 ID를 입력하면 해당 VRRP 그룹의 상세 설정 정보가 출력됩니다.

<Privileged 모드>, <Configuration 모드>에서 **show info failover** 명령을 사용하면 Failover 설정과 VRRP 그룹 설정, 동작 상태 정보가 모두 출력됩니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

제9장
보안 설정

이 장에서는 PAS-K가 제공하는 보안 기능에 대해 살펴봅니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- 보안 기능 개요
- 보안 기능 설정

보안 기능 개요

보안 기능은 네트워크를 통한 공격이나 위협으로부터 PAS-K를 보호하기 위해 PAS-K에서 기본적으로 제공하는 보안 기능입니다. 보안 기능에는 PAS-K를 보호하는 시스템 보안과 PAS-K와 연결된 네트워크를 보호하는 네트워크 보안 기능으로 나뉘어집니다.

PAS-K의 보안 기능에는 다음과 같은 기능들이 있습니다.

시스템 보안

- **시스템 접근 제어**
  PAS-K 로 접근할 수 있는 호스트를 제한하여 허용되지 않은 호스트의 접근을 차단하는 기능입니다.

네트워크 보안

- **방화벽**
  다양한 조건의 필터를 사용하여 불필요한 트래픽의 송수신을 차단함으로써 네트워크의 자원을 보호하는 기능입니다.

각 기능에 대해 좀 더 상세하게 알아봅니다.

시스템 접근 제어

시스템 접근 제어(system access control) 기능은 시스템을 보호하기 위해 특정한 패킷만 텔넷이나 SSH, HTTP, HTTPS 등을 통해 PAS-K로 수신되도록 제한하는 기능입니다. 시스템 접근 제어 기능을 사용하면 허용되지 않은 사용자가 PAS-K로 접근하여 임의로 PAS-K의 설정을 변경하거나 정보를 조회하는 것을 막을 수 있습니다.

시스템 접근 제어 기능은 사용자 인증 과정의 취약성을 보완하는 용도로 활용할 수 있습니다. 텔넷, SSH, HTTP, SNMP를 통해 PAS-K로 접속하여 시스템을 모니터링하거나 관리하기 위해서는 로그인 ID와 패스워드를 확인하는 사용자 인증 과정을 필수적으로 거쳐야 합니다. 하지만, 인증 시 사용되는 로그인 ID나 패스워드가 노출되면 인증을 통해 호스트의 접근을 통제할 수 없게 됩니다. 이런 경우, 접근 규칙을 이용하여 접근을 허용할 호스트의 조건을 지정해두면 인증 과정을 거치기 전에 먼저 호스트를 필터링하기 때문에 인증 정보가 노출된 경우에도 허가 받지 않은 호스트로부터 시스템을 안전하게 보호할 수 있습니다.

시스템 접근 제어 기능은 접근 규칙(access rule)을 사용하여 허용할 패킷과 차단할 패킷을 지정합니다. 접근 규칙은 패킷에 대한 조건과 조건을 만족하는 패킷의 처리 방법(허용 혹은 차단)으로 구성됩니다. 패킷의 조건은 패킷의 출발지/목적지 IP 주소, 패킷이 수신된 인터페이스, 프로토콜, 포트 번호 등을 조합하여 지정할 수 있습니다.

모든 접근 규칙의 조건에 만족되지 않는 패킷은 기본 접근 정책(default policy)에 의해 처리 방법이 결정됩니다. 기본 접근 정책이 허용(accept)으로 설정되어 있으면 모든 접근 규칙에 만족되지 않는 패킷은 허용되고, 기본 접근 정책이 차단(deny)으로 설정되어 있으면 폐기됩니다.

접근 규칙의 ID

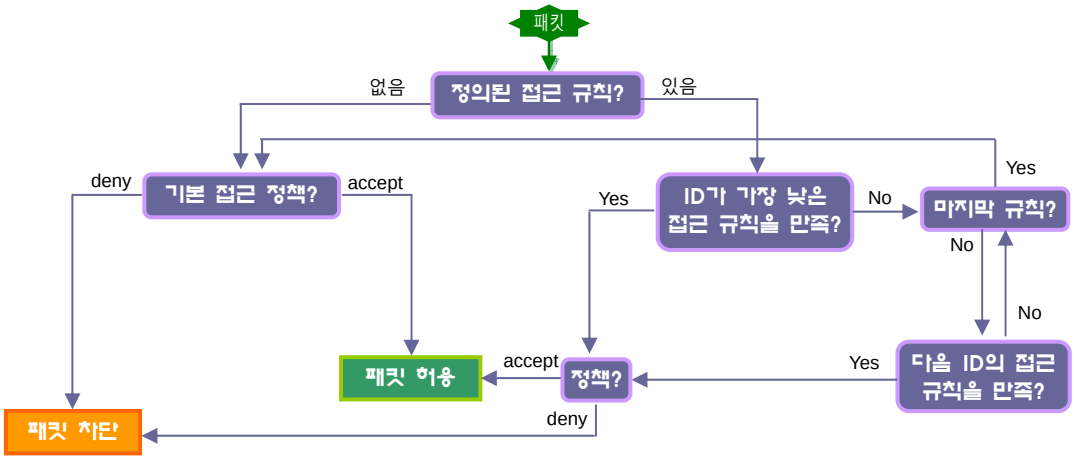
여러 개의 접근 규칙이 정의되어 있으면 PAS-K는 ID가 가장 낮은 접근 규칙부터 패킷에 적용합니다. ID가 가장 낮은 접근 규칙의 조건과 패킷이 일치하지 않은 경우에는 그 다음으로 높은 ID를 가진 접근 규칙의 조건과 패킷을 비교합니다. 이러한 순서대로 접근 규칙과 패킷을 비교하다가 패킷이 접근 규칙의 조건을 만족하면 해당 접근 규칙의 정책(policy)에 따라 패킷이 처리됩니다.

하나의 패킷이 여러 접근 규칙의 조건을 동시에 만족시킬 수 있습니다. 이런 경우, 어떤 접근 규칙을 먼저 적용하느냐에 따라 패킷의 처리가 달라질 수 있습니다. 그러므로, 접근 규칙을 정의할 때에는 사용자가 의도한 대로 패킷이 처리될 수 있도록 접근 규칙의 ID를 설정해야 합니다.

일반적으로 어떤 접근 규칙의 조건이 다른 접근 규칙의 조건에 포함되어 패킷이 여러 접근 규칙에 동시에 만족되는 경우에는 더 구체적인 조건을 가진 접근 규칙의 ID를 더 낮게 설정합니다. 예를 들어, 출발지가 192.168.10.0/24인 조건을 가진 접근 규칙(규칙 1)과 출발지가 192.168.10.0/28이고 프로토콜이 TCP인 조건을 가진 접근 규칙(규칙 2)을 정의해야 한다면, 조건이 더 구체적인 규칙 2의 ID를 더 낮게 설정합니다.

시스템 접근 제어 기능 동작 과정

다음은 시스템 접근 제어 기능에 의해 패킷이 차단되고 허용되는 과정을 나타낸 그림입니다.



[그림 - PAS-K의 접근 제어 과정]

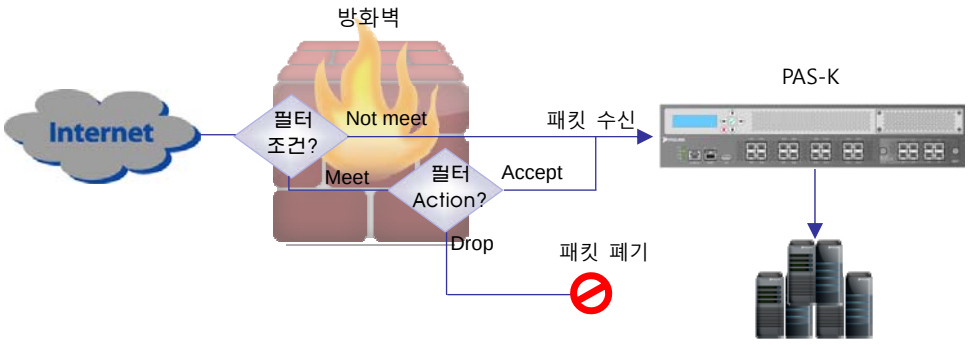
특정 호스트가 PAS-K로 접속하기 위해 패킷을 전송하면 PAS-K는 패킷이 만족하는 접근 규칙이 있는지 확인하기 위해 ID가 가장 낮은 접근 규칙부터 차례대로 패킷과 비교합니다. 패킷이 만족하는 접근 규칙이 존재하면 접근 규칙의 정책에 따라 패킷을 허용하거나 차단합니다. 패킷이 만족하는 접근 규칙이 없거나 접근 규칙이 아예 정의되어 있지 않으면 기본 접근 규칙의 설정에 따라 패킷이 허용되거나 차단됩니다.

방화벽(Firewall)

방화벽은 내부 네트워크를 보호하기 위해 허가된 네트워크 또는 사용자만 내부 네트워크로 접근할 수 있고 허가되지 않은 외부 네트워크의 접근은 차단하는 기능입니다. 네트워크 관리자는 다양한 보안 정책을 설정하여 지속적으로 발견되고 보고되는 보안 상 취약한 부분들을 수정함으로써 네트워크의 보안 수준을 높이는 것이 필요합니다. 방화벽은 네트워크의 보안 수준을 높이는데 꼭 필요한 도구 중에 하나입니다.

PAS-K는 방화벽의 한 종류인 패킷 필터링 방화벽 기능을 제공합니다. 패킷 필터링 방화벽은 내부 네트워크와 외부 네트워크 간에 송수신되는 패킷들을 모니터링하여 설정된 필터의 조건에 따라 패킷을 필터링합니다. 각 필터는 '조건'과 '동작'으로 구성됩니다. 조건은 패킷을 구분할 때 사용되고 동작은 조건을 통해 구분된(조건을 만족하는) 패킷을 허용(accept)할 것인지 폐기(drop)할 것인지 등을 지정합니다. 이러한 패킷 필터링 방화벽을 사용하면 외부 네트워크에 노출시킬 내부 네트워크를 제한할 수 있고(특정 포트 차단 등을 통해) 내부 네트워크에서 외부로 불필요하게 전송되는 트래픽이나 허용하지 않는 사이트로의 접속을 차단할 수 있습니다.

다음 그림은 외부 네트워크로부터 패킷이 수신되었을 PAS-K의 방화벽에 의해 패킷이 필터링되는 과정을 보여주는 그림입니다.



[그림 - PAS-K의 방화벽 동작 과정]

PAS-K는 방화벽의 필터링 조건으로 다음과 같은 값을 사용할 수 있습니다.

- 패킷의 프로토콜 종류
- 패킷의 출발지/목적지 IP 주소
- 패킷의 출발지/목적지 포트 번호
- 패킷의 내용(content)
- TCP 플래그(flag)
- 패킷의 길이
- ICMP 유형

PAS-K는 대부분의 방화벽이 제공하는 필터링 조건인 프로토콜 종류나 IP 주소, 포트 번호뿐 만 아니라 패킷의 길이와 패킷의 내용, TCP 플래그 등의 다양한 필터링 조건을 제공함으로써, 보다 다양하고 높은 수준의 보안 정책을 설정할 수 있습니다.

보안 기능 설정

이 절에서는 지금까지 살펴본 PAS-K의 보안 기능을 PAS-K에 적용할 수 있도록 CLI에서 설정하는 방법에 대해 알아봅니다.

시스템 접근 제어 설정

이 절에서는 시스템 접근 제어 기능을 설정하는 방법에 대해 설명합니다.

접근 규칙 설정하기

시스템 접근 제어 기능을 사용하기 위한 접근 규칙을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 1024개의 접근 규칙을 설정할 수 있습니다. 여러 개의 접근 규칙을 설정하는 경우에는 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**security**	<Security 설정 모드>로 이동합니다.
2	**access**	<System Access 설정 모드>로 이동합니다.
3	**rule** *<ID>*	접근 규칙을 생성합니다. • *<ID>* 접근 규칙의 ID 설정. 설정 범위: 1 ~ 1024
다음 4 ~ 8번 과정은 접근 규칙에 패킷을 비교하는 조건을 추가하는 과정으로, 선택적으로 수행할 수 있습니다. 즉, 접근 규칙에 포함시키고자 하는 조건만 선택하여 추가합니다. 필요한 조건을 추가한 후에는 9번 과정부터 수행합니다.		
4	**source-ip** *<SOURCE-IP>*	패킷의 출발지 IP 주소를 비교 조건으로 추가합니다. • *<SOURCE-IP>* 출발지 IP 주소 설정. 기본값: 0.0.0.0/0 **참고**: 설정한 출발지 IP 주소를 기본값으로 변경하려면, **no source-ip** 명령을 사용합니다.
5	**destination-ip** *<DESTINATION-IP>*	패킷의 목적지 IP 주소를 비교 조건으로 추가합니다. • *<DESTINATION-IP>* 목적지 IP 주소 설정. 기본값: 0.0.0.0/0 **참고**: 설정한 목적지 IP 주소를 기본값으로 변경하려면, **no destination-ip** 명령을 사용합니다.
6	**protocol** {**tcp** | **udp** | **icmp** | **all**}	패킷 비교 조건으로 사용할 프로토콜의 종류를 설정합니다. • **all** 프로토콜을 패킷 비교 조건으로 사용하지 않음 (기본값) • **tcp** TCP를 패킷 비교 조건으로 사용 • **udp** UDP를 패킷 비교 조건으로 사용 • **icmp** ICMP를 패킷 비교 조건으로 사용
프로토콜을 TCP나 UDP로 지정한 경우에는 출발지 포트 번호와 목적지 포트 번호를 비교 조건으로 지정할 수 있습니다. 필요한 경우, 7번과 8번 과정을 참고하여 출발지 포트 번호와 목적지 포트 번호를 비교 조건으로 설정합니다.		
7	**source-port** *<SOURCE-PORT>*	패킷 비교 조건으로 사용할 출발지 포트 번호를 설정합니다. • *<SOURCE-PORT>* 비교할 출발지 포트 번호. 여러 개의 출발지 포트를 추가하려면 공백 없이 쉼표(,)로 각 포트를 구분하도록 하고, 연속되는 포트는 대쉬(-)를 사용하여 입력합니다. 설정 범위: 0 ~ 65535 **참고**: 설정한 출발지 포트 번호를 삭제하려면, **no source-port** *<SOURCE-PORT>* 명령을 사용합니다.
8	**destination-port** *<DESIINATION-PORT>*	패킷 비교 조건으로 사용할 목적지 포트 번호를 설정합니다. • *<DESTINATION-PORT>* 비교할 목적지 포트 번호. 여러 개의 목적지 포트를 추가하려면 공백 없이 쉼표(,)로 각 포트를 구분하도록 하고, 연속되는 포트는 대쉬(-)를 사용하여 입력합니다. 설정 범위: 0 ~ 65535 **참고**: 설정한 목적지 포트 번호를 삭제하려면, **no destination-port** *<DESTINATION-PORT>* 명령을 사용합니다.

9	**policy {accept | deny}**	규칙에 추가된 조건과 일치하는 패킷의 처리 방법을 지정합니다. • **accept** 조건과 일치한 패킷 허용 (기본값) • **deny** 조건과 일치한 패킷 차단
10	**interface {any | mgmt | vlan}**	접근 규칙을 적용할 인터페이스를 설정합니다. • **any** 모든 인터페이스에 접근 규칙 적용 (기본값) • **mgmt** 관리용 이더넷 포트를 인터페이스로 지정 • **vlan** 특정 VLAN에 지정
11	**vlan-name** *<VLAN-NAME>*	10번 과정에서 **vlan** 을 선택한 경우, 접근 규칙을 적용할 VLAN을 설정합니다. • *<VLAN-NAME>* 접근 규칙을 적용할 VLAN의 이름.
12	**status {enable | disable}** (선택 설정)	접근 규칙의 사용 여부를 지정합니다. • **enable** 접근 규칙 활성화 (기본값) • **disable** 접근 규칙 비활성화
13	**current**	설정한 접근 규칙의 설정 정보를 확인합니다.
14	**apply**	설정한 접근 규칙을 PAS-K에 저장하고 적용합니다.

참고: 생성한 접근 규칙을 삭제하려면 <System Access 설정 모드>에서 **no rule** *<ID>* 명령을 사용합니다. *<ID>* 항목에는 삭제할 접근 규칙의 ID를 입력합니다.

기본 접근 정책 설정하기

시스템 접근 제어 기능의 기본 접근 정책을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다.

순서	명 령	설 명
1	**security**	<Security 설정 모드>로 이동합니다.
2	**access**	<System Access 설정 모드>로 이동합니다.
3	**default-policy {accept | deny}**	모든 접근 규칙에 만족되지 않는 패킷의 처리 방법을 지정하기 위해 기본 접근 정책을 설정합니다. • **accept** 모든 접근 규칙에 만족되지 않는 패킷 허용 (기본값) • **deny** 모든 접근 규칙에 만족되지 않는 패킷 차단

주의: 텔넷(Telnet)을 통해 PAS-K에 접속한 경우, 접근 정책이 설정되어 있지 않거나 사용자의 PC를 허용하는 접근 정책이 설정되어 있지 않은 상태에서 기본 접근 정책을 'deny'로 지정하면 PAS-K와의 접속이 끊어지게 됩니다.

시스템 접근 제어 설정 정보 보기

현재 정의된 접근 규칙을 확인하려면, <System Access 설정 모드>에서 **show rule** 명령을 사용합니다. **show rule** 명령에 접근 규칙의 ID를 함께 입력하면 해당 접근 규칙에 대한 정보만 확인할 수 있습니다.

현재 설정된 기본 접근 정책을 확인하려면, <Security 설정 모드>에서 **show access** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

방화벽 설정

이 절에서는 CLI에서 PAS-K에 방화벽 기능을 설정하는 방법에 대해 설명합니다.

PAS-K에 방화벽 기능을 설정하는 과정은 다음과 같습니다.

1. 컨텐트 설정하기(선택 설정)
2. 컨텐트 그룹 설정하기(선택 설정)
3. 필터 설정하기
4. 필터 그룹 설정하기(선택 설정)
5. 정책 설정하기
6. 설정 정보 보기

각 단계별 설정 방법을 차례로 살펴봅니다.

컨텐트 설정하기

컨텐트를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 256개의 컨텐트를 정의할 수 있으므로, 여러 개의 컨텐트를 설정하려는 경우에는 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**security**	<Security 설정 모드>로 이동합니다.
2	**firewall**	<Firewall 설정 모드>로 이동합니다.
3	**content** *<NAME>*	컨텐트를 생성하고 <Content 설정 모드>로 들어갑니다. • *<NAME>* 컨텐트의 이름. 최대 32자의 알파벳, 숫자, '-', '_' 문자로 이루어진 문자열, 첫 글자는 반드시 알파벳 사용
4	**string** *<STRING>*	패킷의 페이로드에서 검색할 문자열을 설정합니다. • *<STRING>* 패킷의 페이로드에서 검색할 문자열. 최대 100자의 알파벳, 특수문자, 숫자 지정 가능
5	**offset** {*<OFFSET>* | **any**}	4번 과정에서 설정한 문자열을 패킷의 페이로드에서 검색할 때 검색을 시작할 패킷 페이로드의 상대적 위치(오프셋)를 설정합니다. • *<OFFSET>* 패킷의 페이로드에서 문자열 검색을 시작할 지점 설정 설정 범위: 0 ~ 2000, 단위: byte • **any** 패킷의 페이로드 처음부터 문자열 검색 (기본값)
6	**depth** {*<DEPTH>* | **any**}	문자열 검색의 끝 지점을 설정합니다. • *<DEPTH>* 패킷의 페이로드에서 문자열 검색을 종료할 지점 설정 설정 범위: 0 ~ 2000, 단위: byte • **any** 패킷의 페이로드 끝까지 문자열 검색 (기본값) **주의**: 문자열 검색을 시작할 오프셋(offset)의 값은 문자열 검색을 종료할 지점인 depth보다 작아야 합니다.
7	**case-sensitive** {**enable** | **disable**}	문자열을 검색할 때 대소문자를 구분하는 case-sensitive 기능의 사용 여부를 설정합니다. • **enable** 대소문자를 구분함 (기본값) • **disable** 대소문자를 구분하지 않음
8	**current**	설정한 컨텐트 정보를 확인합니다.
9	**apply**	설정한 컨텐트를 PAS-K에 저장하고 적용합니다.

참고: 정의한 컨텐트를 삭제하려면 <Firewall 설정 모드>에서 **no content** *<NAME>* 명령을 사용합니다.

컨텐트 그룹 설정하기

컨텐트 그룹은 여러 개의 컨텐트를 묶어 하나의 컨텐트 처럼 사용할 수 있도록 합니다. 컨텐트 그룹을 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. 컨텐트 그룹은 최대 256개까지 정의할 수 있으므로, 여러 개의 컨텐트 그룹을 설정하려는 경우에는 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**security**	<Security 설정 모드>로 이동합니다.
2	**firewall**	<Firewall 설정 모드>로 이동합니다.
3	**content-group** *<NAME>*	컨텐트 그룹을 생성하고 <Content Group 설정 모드>로 들어갑니다. • *<NAME>* 컨텐트의 이름, 최대 32자의 알파벳, 숫자, '-', '_' 문자로 구성된 문자열, 첫 글자는 반드시 알파벳 사용
4	**content** *<CONTENT>*	컨텐트 그룹에 포함시킬 컨텐트를 지정합니다. • *<CONTENT>* ','를 사용하여 동시에 여러 개의 컨텐트 설정 가능. (하나의 컨텐트 그룹에는 최대 256개의 컨텐트 추가 가능) **참고:** 설정한 컨텐트를 컨텐트 그룹에서 삭제하려면 **no content** *<CONTENT>* 명령을 사용합니다. **주의:** 컨텐트 그룹에는 반드시 한 개 이상의 컨텐트를 설정해야 합니다.
5	**current**	설정한 컨텐트 그룹의 정보를 확인합니다.
6	**apply**	설정한 컨텐트 그룹을 PAS-K에 저장하고 적용합니다.

참고: 컨텐트 그룹을 삭제하려면 <Firewall 설정 모드>에서 **no content-group** *<NAME>* 명령을 사용합니다.

참고: 컨텐트 그룹에 추가된 컨텐트는 추가된 순서에 따라 비교 우선순위가 결정됩니다. 그러므로, 컨텐트 그룹에 처음 추가된 컨텐트가 가장 먼저 비교됩니다.

필터 설정하기

필터를 설정하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 256개의 필터를 정의할 수 있으므로, 여러 개의 필터를 설정하려는 경우에는 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**security**	<Security 설정 모드>로 이동합니다.
2	**firewall**	<Firewall 설정 모드>로 이동합니다.
3	**filter** *<NAME>*	필터를 생성하고 <Firewall Filter 설정 모드>로 들어갑니다. • *<NAME>* 최대 32자의 알파벳, 숫자, '-', '_' 문자로 구성된 문자열, 첫 글자는 반드시 알파벳 사용
다음 4 ~ 13번 과정은 필터에 패킷을 비교하는 조건을 추가하는 과정으로, 선택적으로 수행할 수 있습니다. 즉, 필터에 포함시키고자 하는 조건만 선택하여 추가하면 됩니다. 필요한 조건을 추가한 후에는 14번 과정부터 수행하면 됩니다.		
4	**protocol** {**tcp** | **udp** | **icmp** | **all**}	패킷 필터링 조건으로 사용할 프로토콜의 종류를 설정합니다. (기본값: all) 지정한 프로토콜에 따라 다음 과정에서 구체적인 필터링 조건을 추가할 수 있습니다. • TCP : TCP 플래그 → 5번 • ICMP : ICMP 유형 → 7번
5	**tcp-flag** {**urg** | **ack** | **psh** | **syn** | **fin** | **rst** | **none**}	TCP 플래그를 필터링 조건으로 추가합니다. 4번 과정에서 프로토콜의 종류를 tcp로 설정한 경우에는 패킷에 있는 TCP 플래그를 사용하여 보다 다양한 필터링 조건을 생성할 수 있습니다. 한 개 이상의 플래그를 지정하려면 각 플래그를 ','로 구분하여 입력하면 됩니다. 기본적으로는 TCP 플래그를 패킷 필터링 조건으로 사용하지 않도록 설정됩니다.
6	**tcp-flag-option** {**match** | **include**}	TCP 플래그를 필터링 조건으로 추가한 경우에는 TCP 플래그를 비교할 방법을 선택할 수 있습니다. • **match** tcp-flag 명령으로 지정한 모든 TCP 플래그가 '1'로 설정되어 있는지 비교 • **include** 지정한 TCP 플래그 중 하나라도 '1'로 설정되어 있는지 비교
7	**icmp-type** {**destination-unreachable** | **echo-reply** | **echo-request** | **fragmentation-needed** | **host-redirect**|**host-unreachable** | **network-redirect** | **network-unreachable** | **port-unreachable** | **redirect** | **source-quench** | **time-exceeded** | **ttl-zero-during-reassembly** | **ttl-zero-during-transit**}	ICMP의 유형을 필터링 조건으로 추가합니다. 4번 과정에서 프로토콜의 종류를 'icmp'로 설정한 경우에는 ICMP의 유형을 필터링 조건으로 사용하여 보다 다양한 필터링 조건을 생성할 수 있습니다.
8	**source-ip** *<SOURCE-IP>*	패킷의 출발지 IP 주소를 비교 조건으로 추가합니다. • *<SOURCE-IP>* 출발지 IP주소 및 서브넷 마스크 설정. (기본값: 0.0.0.0/0) **참고**: 설정한 출발지 IP 주소를 기본값으로 변경하려면, **no source-ip** 명령을 사용합니다.
9	**dest-ip** *<DEST-IP>*	패킷의 목적지 IP 주소를 비교 조건으로 추가합니다. • *<SOURCE-IP>* 목적지 IP주소 및 서브넷 마스크 설정. (기본값: 0.0.0.0/0) **참고**: 설정한 목적지 IP 주소를 기본값으로 변경하려면, **no dest-ip** 명령을 사용합니다.
10	**source-port** {**eq** | **gt** | **lt** | **any** | **range**} **port-num** *<PORT-NUM>*	출발지 포트 번호를 비교 조건으로 추가합니다. 비교하는 방법에는 5가지 방법이 있습니다. • **eq** 출발지 포트가 설정한 포트와 일치하는지 비교 • **gt** 출발지 포트가 설정한 포트보다 큰 지 비교 • **lt** 출발지 포트가 설정한 포트보다 작은 지 비교 • **range** 출발지 포트가 설정한 범위에 포함되는지 비교 • **any** 출발지 포트를 필터링 조건으로 사용하지 않음(기본값)

		• *<PORT-NUM>* 비교할 포트 번호. (설정 범위: 1 ~ 5000) **참고**: 설정한 출발지 포트 번호를 삭제하려면, **no source-port {eq | gt | lt | any | range} port-num** *<PORT-NUM>* 명령을 사용합니다.
11	**dest-port {eq | gt | lt | any | range} port-num** *<PORT-NUM>*	목적지 포트 번호를 비교 조건으로 추가합니다. (10번 과정 설명 참고) **참고**: 설정한 목적지 포트 번호를 삭제하려면, **no dest-port {eq | gt | lt | any | range} port-num** *<PORT-NUM>* 명령을 사용합니다.
12	**content** *<CONTENT>*	컨텐트나 컨텐트 그룹을 필터링 조건으로 추가합니다. 지정하는 컨텐트나 컨텐트 그룹은 미리 정의되어 있어야 합니다. • *<CONTECNT>* 컨텐트 또는 컨텐트 그룹으로 추가할 컨텐트 지정. **참고**: 설정한 컨텐트나 컨텐트 그룹을 필터에서 삭제하려면, **no content** *<CONTENT>* 명령을 사용합니다.
13	**length** *<LENGTH>*	패킷의 길이를 필터링 조건으로 추가합니다. PAS-K는 지정한 패킷의 길이보다 큰 패킷을 필터링하게 됩니다. • *<LENGTH>* 패킷 길이 입력 (설정 범위: 1 ~ 2000, 단위: byte) **참고**: 설정한 패킷 길이 삭제하려면, **no length** 명령을 사용합니다.
14	**action {accept | drop | reject | rate rate-limit-value** *<RATE-LIMIT-VALUE>*}	필터에 추가된 조건과 일치하는 패킷의 처리 방법을 설정합니다. • **accept** 조건과 일치하는 패킷을 허용 • **drop** 조건과 일치하는 패킷을 폐기 • **reject** 조건과 일치하는 패킷의 출발지 IP 주소로 리셋 패킷을 전송. 프로토콜의 종류가 tcp나 icmp로 설정되어 있는 경우에만 이 방법을 지정할 수 있습니다. 프로토콜의 종류가 udp나 any로 설정된 상태에서 이 방법을 지정한 후 **apply** 명령을 실행하면 오류 메시지가 출력됩니다. • **rate** 지정한 대역폭으로 패킷을 허용 • *<RATE-LIMIT-VALUE>* 패킷 처리 방법을 rate으로 선택한 경우, 패킷을 수신할 패킷 rate 입력. 설정범위: 1~65535, 단위: PPS
15	**log {enable | disable}**	설정한 필터에 의해 패킷이 필터링된 정보를 로그로 기록할지 여부를 설정합니다. • **enable** 로그를 기록 (기본값) • **disable** 로그를 기록하지 않음
16	**current**	설정한 필터 정보를 확인합니다.
17	**apply**	설정한 필터를 PAS-K에 저장합니다.

참고: 필터를 삭제하려면 <Firewall 설정 모드>에서 **no filter** *<NAME>* 명령을 사용합니다.

필터 그룹 설정하기

필터 그룹은 여러 개의 필터를 묶어 하나의 필터처럼 사용할 수 있도록 합니다. 필터 그룹을 생성하려면 <Configuration 모드>에서 다음 과정을 수행합니다. PAS-K에는 최대 256개의 필터 그룹을 설정할 수 있으므로, 여러 개의 필터 그룹을 설정하려는 경우 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**security**	<Security 설정 모드>로 이동합니다.
2	**firewall**	<Firewall 설정 모드>로 이동합니다.
3	**filter-group** *<NAME>*	필터 그룹을 생성합니다. 필터 그룹을 생성하면 <Filter Group 설정 모드>로 들어갑니다. • *<NAME>* 필터의 이름, 최대 32자의 알파벳, 숫자, '-', '_' 문자로 구성된 문자열, 첫 글자는 반드시 알파벳 사용
4	**filter** *<FILTER>*	필터 그룹에 포함시킬 필터를 지정합니다. • *<FILTER>* ','를 사용하여 동시에 여러 개의 필터를 설정 가능하며, 하나의 필터 그룹에는 최대 256개의 서로 다른 필터를 추가할 수 있습니다. **참고:** 설정한 필터를 필터 그룹에서 삭제하려면 **no filter** *<FILTER>* 명령을 사용합니다. **주의:** 필터 그룹에는 반드시 한 개 이상의 필터를 설정해야 합니다.
5	**current**	설정한 필터 그룹의 정보를 확인합니다.
6	**apply**	설정한 필터 그룹을 PAS-K에 저장하고 적용합니다.

참고: 필터 그룹을 삭제하려면 <Firewall 설정 모드>에서 **no filter-group** *<NAME>* 명령을 사용합니다.

참고: 필터 그룹에 추가된 필터는 추가된 순서에 따라 비교 우선순위가 결정됩니다. 그러므로, 필터 그룹에 처음 추가된 필터가 가장 먼저 비교됩니다.

정책 설정하기

필터나 필터 그룹을 정의한 후에는 실제로 PAS-K에 적용할 방화벽 정책을 정의해야 합니다. 방화벽 정책을 정의하려면 <Configuration 모드>에서 다음 과정을 수행합니다. 여러 개의 방화벽 정책을 설정하려는 경우, 다음 과정을 반복하면 됩니다.

순서	명 령	설 명
1	**security**	<Security 설정 모드>로 이동합니다.
2	**firewall**	<Firewall 설정 모드>로 이동합니다.
3	**policy** *<NAME>*	방화벽 정책을 생성하고 <Firewall Policy 설정 모드>로 이동합니다. • *<NAME>* 방화벽 정책 이름을 최대 32자의 알파벳, 숫자, '-', '_' 문자로 구성된 문자열로 지정. 첫 글자는 반드시 알파벳 사용
4	**filter** *<FILTER>* **filter-group** *<FILTER-GROUP>*	방화벽 정책에 사용할 필터나 필터 그룹을 등록합니다. • *<FILTER>* 정책에서 사용할 필터의 이름 • *<FILTER-GROUP>* 정책에서 사용할 필터 그룹의 이름
5	**interface** *<INTERFACE>*	방화벽 정책을 적용할 인터페이스를 설정합니다. • *<INTERFACE>* 방화벽 정책을 적용할 인터페이스 이름
6	**status** {**enable** | **disable**}	방화벽 정책의 사용 여부를 지정합니다. • **enable** 방화벽 정책 활성화 (기본값) **disable** 방화벽 정책 비활성화
7	**current**	설정한 방화벽 정책의 정보를 확인합니다.
8	**apply**	설정한 방화벽 정책을 PAS-K에 저장하고 적용합니다.

참고: 정책에서 필터와 필터 그룹을 삭제하려면 <Firewall Policy 설정 모드>에서 다음과 같은 명령을 사용합니다.

```
(config-security-firewall-policy[p1])# no filter <FILTER>
(config-security-firewall-policy[p1])# no filter-group <FILTER-GROUP>
```

참고: 정책을 삭제하려면 <Firewall 설정 모드>에서 **no policy** *<NAME>* 명령을 사용합니다.

방화벽 설정 정보 보기

컨텐트 설정 정보 보기

설정한 방화벽 컨텐트의 목록을 확인하려면, <Firewall 설정 모드>에서 **show content** 명령을 사용합니다. 특정 방화벽 컨텐트의 상세 설정 정보를 확인하려면, <Firewall 설정 모드>에서 **show content** 명령과 함께 방화벽 컨텐트의 이름을 입력합니다.

컨텐트 그룹 설정 정보 보기

설정한 방화벽 컨텐트 그룹 목록을 확인하려면, <Firewall 설정 모드>에서 **show content-group** 명령을 사용합니다. 특정 방화벽 컨텐트 그룹의 상세 설정 정보를 확인하려면, <Firewall 설정 모드>에서 **show content-group** 명령과 함께 방화벽 컨텐트 그룹의 이름을 입력합니다.

필터 설정 정보 보기

설정한 방화벽 필터 목록을 확인하려면, <Firewall 설정 모드>에서 **show filter** 명령을 사용합니다. 특정 방화벽 필터의 상세 설정 정보를 확인하려면, <Firewall 설정 모드>에서 **show filter** 명령과 함께 방화벽 필터의 이름을 입력합니다.

필터 그룹 설정 정보 보기

설정한 방화벽 필터 목록을 확인하려면, <Firewall 설정 모드>에서 **show filter-group** 명령을 사용합니다. 특정 방화벽 필터의 상세 설정 정보를 확인하려면, <Firewall 설정 모드>에서 **show filter-group** 명령과 함께 방화벽 필터 그룹의 이름을 입력합니다.

정책 설정 정보 보기

설정한 방화벽 정책 목록을 확인하려면, <Firewall 설정 모드>에서 **show policy** 명령을 사용합니다. 특정 방화벽 정책의 상세 설정 정보를 확인하려면, <Firewall 설정 모드>에서 **show policy** 명령과 함께 방화벽 정책의 이름을 입력합니다.

보안 기능 설정 정보 보기

현재 PAS-K에 설정된 시스템 접근제어 기능과 방화벽 기능의 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show security** 명령을 사용합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.

제10장
QoS 설정

이 장에서는 PAS-K에서 제공하는 QoS(Quality of Service) 기능에 대해 상세히 살펴본 후, QoS 설정 시 주의해야 할 사항과 QoS 설정 전에 선행되어야 하는 작업을 소개합니다. 그리고, CLI 명령을 사용하여 PAS-K에 QoS 기능을 설정하는 방법에 대해 알아봅니다.

이 장은 다음과 같은 내용으로 구성됩니다.

- QoS 개요
- QoS 설정하기

QoS 개요

기능 소개

PAS-K는 트래픽에 따라 대역폭을 다르게 할당할 수 있는 QoS(Quality of Service) 기능을 지원합니다. PAS-K의 QoS 기능을 사용하면, '특정' 트래픽에게 일정한 대역폭을 항상 '보장'해주거나, 지정한 양 이하의 대역폭만 사용하도록 대역폭을 '제한'할 수 있습니다.

QoS를 사용하지 않을 때에는 PAS-K는 수신되는 순서에 따라 트래픽을 전송합니다. 즉, 가장 먼저 도착한 트래픽을 가장 먼저 전송합니다. 대역폭이 부족하면, 나중에 도착한 트래픽은 대역폭의 여유가 생길 때까지 대기하고 있다가 사용 가능한 대역폭이 생기면 오래 대기한 패킷부터 전송됩니다. 이와 같이 트래픽을 수신 순서에 따라 전송하면 다음과 같은 문제가 발생할 수 있습니다.

- 트래픽의 특성이 고려되지 않기 때문에, 주요 트래픽이 나중에 전송되거나 전송되지 않을 수 있습니다.
- 특정 트래픽의 대역폭을 제한할 수 없기 때문에, 특정 트래픽에 의해 대역폭이 모두 점유되면 다른 트래픽은 전혀 전송될 수 없습니다.

이러한 문제는 QoS 기능을 사용하여 해결할 수 있습니다. 특정 트래픽에 의한 대역폭 점유를 방지하려면 해당 트래픽을 출발지/목적지 IP 주소, 출발지/목적지 MAC 주소, 출발지/목적지 포트 번호, DSCP(Differentiated Service Code Point), Ethernet type, 프로토콜, 인터페이스를 조건으로 하여 클래스를 분류하고 이 클래스에 최대 대역폭(Peak rate)을 지정하여 문제를 해결 할 수 있습니다.

구성 요소

클래스

클래스는 패킷이 특정한 조건을 만족하는지 검사하기 위해 사용됩니다. 따라서, 클래스는 패킷과 비교할 각종 조건들로 구성됩니다. 클래스에서 사용할 수 있는 조건은 아래의 표와 같이 모두 11가지가 있으며, 조건들 중에서 필요한 항목만 선택하여 사용합니다.

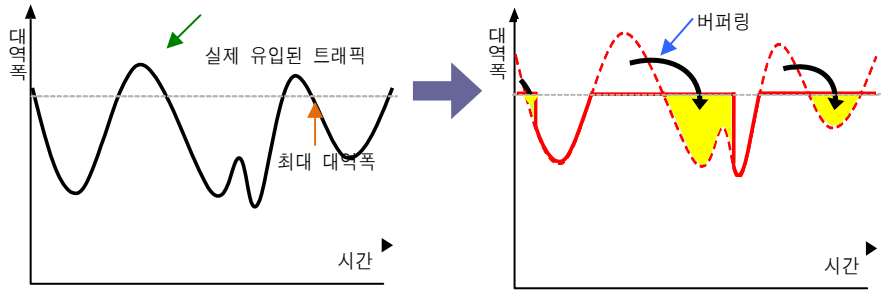
[표 - QoS 클래스의 구성 요소]

항 목	설 명
출발지 IP 주소	출발지 IP 주소 또는 IP 대역을 조건으로 패킷을 분류합니다.
출발지 MAC 주소	출발지 MAC 주소를 조건으로 패킷을 분류합니다.
출발지 포트 번호	출발지 포트 번호를 조건으로 패킷을 분류합니다.
목적지 IP 주소	목적지 IP 주소 또는 IP 대역을 조건으로 패킷을 분류합니다.
목적지 MAC 주소	목적지 MAC 주소를 조건으로 패킷을 분류합니다.
목적지 포트 번호	목적지 포트 번호를 조건으로 패킷을 분류합니다.
DSCP	IP 헤더에 포함된 DSCP(Differentiated Services Code Point) 값을 조건으로 패킷을 분류합니다.
Ethernet type	Ethernet type을 조건으로 패킷을 분류합니다.
프로토콜	IP 프로토콜을 조건으로 패킷을 분류합니다.
수신 인터페이스(포트)	패킷을 수신한 인터페이스(포트)를 조건으로 패킷을 분류합니다.
VLAN	패킷이 속한 VLAN을 조건으로 패킷을 분류합니다.

정책

정책은 특정 클래스에 적용할 대역폭 정책을 정의하기 위해 사용됩니다. 정책은 클래스와 그 클래스의 트래픽에 할당할 최대 대역폭, 그리고 우선순위로 구성됩니다.

[표 - QoS 정책의 구성 요소]

항 목	설 명
클래스	정책을 적용할 트래픽 조건입니다. 하나의 정책에는 여러 개의 클래스를 설정할 수 있으며, 각 클래스마다 서로 다른 정책을 적용할 수 있습니다.
우선순위(priority)	클래스의 우선순위입니다. 이 우선순위는 하나의 정책에 여러 개의 클래스가 정의되어 있는 경우, 각 클래스에 최소 대역폭을 할당하고 남은 대역폭을 할당하는 우선순위로 사용됩니다.
최대 대역폭 (peak rate)	클래스의 트래픽이 사용할 수 있는 최대 대역폭입니다. 최대 대역폭은 트래픽이 지정한 대역폭 이상으로 전송될 수 없도록 대역폭을 제한하기 위해 사용됩니다. 전송되는 트래픽이 적어서 대역폭이 남는 경우에도 해당 클래스의 트래픽은 최대 대역폭만큼만 사용할 수 있습니다. 만약 전송되는 트래픽이 클래스에 할당된 최대 대역폭을 넘는 경우에는 버퍼링을 통해 트래픽이 최대 대역폭을 넘지 않도록 쉐이핑(shaping)하게 됩니다. 트래픽 쉐이핑은 아래 그림과 같이 지정된 대역폭(최대 대역폭)을 넘어서는 트래픽을 버퍼에 저장했다가 이 후 대역폭에 여유가 생겼을 때 전송하는 트래픽 전송 방식입니다. 

대역폭 제한(Rate Limit)

PAS-K는 특정한 트래픽 플로우에서 사용할 수 있는 대역폭을 제한할 수 있습니다. 정책 맵을 사용하여 특정 클래스에 속하는 트래픽의 대역폭만 제한할 수도 있고, 포트 전체의 대역폭을 제한할 수도 있습니다.

서비스 큐 스케줄링(Service Queue Scheduling)

출력 포트에는 큐에 저장되어 있는 패킷이 전송할 수 있는 대역폭 보다 많은 경우 어떤 패킷을 우선적으로 처리할 것인지 방법이 정해져 있습니다. 이러한 방법을 서비스 큐 스케줄링이라고 합니다. PAS-K에는 서비스 큐 스케줄링으로 다음과 같은 방법을 사용할 수 있습니다.

- **SPQ(Strict Priority Queueing)**
  각 큐에 우선순위를 지정하고, 우선순위가 높은 큐에 있는 패킷을 모두 처리한 후, 다음 번 우선순위를 가진 큐의 패킷을 처리하는 방식입니다.

- **RR(Round Robin)**
  큐를 순차적으로 선택하는 방식입니다.

- **WRR(Weight Round Robin)**
  가중치(Weight)를 사용해 처리해 줄 패킷 크기를 큐마다 다르게 설정한 다음, 지정한 가중치에 따라 차례대로 패킷을 처리하는 방식입니다.

- **DRR(Deficit Round Robin)**
  각 큐에 Quantum(처리될 수 있는 최대 패킷의 크기)과 Dificit counter를 정의한 다음, Deficit counter의 크기만큼 큐의 패킷을 처리하는 방식입니다. Dificit counter는 기본적으로 '0'으로 설정되고, 큐의 데이터가 서비스되는 시점에 Quantum값과 합해집니다. 패킷이 처리된 후, Deficit counter는 처리된 패킷의 크기만큼 값이 줄어듭니다.

QoS 설정하기

설정 과정

PAS-K는 패킷 분류를 위한 클래스 맵(Classifier)과 분류된 패킷에 적용할 정책 맵(QoS Action)을 이용하여 QoS 를 설정할 수 있습니다. PAS-K에서 QoS를 설정하는 과정은 다음과 같습니다.

1. 클래스 맵(Class map) 설정
   PAS-K로 수신된 패킷을 특정 클래스로 분류합니다. 패킷을 클래스로 분류할 때에는 각 클래스에 정의되어 있는 기준을 사용합니다. 패킷에 담긴 정보와 클래스에 정의된 기준을 비교하여 서로 일치하면 해당 클래스의 패킷으로 분류합니다.

2. 정책 맵(Policy map) 설정
   클래스 맵을 통해 특정 트래픽 클래스로 분류된 패킷에 적용할 QoS Action을 정의합니다.

3. 서비스 정책(Service policy) 설정
   정의한 정책 맵 중에서 실제로 적용할 정책 맵을 지정합니다.

4. QoS 정책을 적용하여 트래픽 전송
   각 클래스의 패킷을 클래스에 설정된 정책(대역폭 할당 방법)에 따라 전송합니다.

수신된 트래픽을 분류할 때에는 클래스를 사용하고, 트래픽을 전송할 때에는 정책(Policy)을 사용합니다. 따라서, QoS 클래스는 QoS 정책에 추가되어, 해당 정책을 적용받습니다. 그리고, QoS 정책은 해당 인터페이스를 통해 송수신되는 트래픽에 정책을 적용합니다.

CLI에서 설정하기

클래스 맵(Class map) 설정

클래스 맵은 특정 트래픽을 다른 트래픽과 구분하기 위한 기준을 정의한 것입니다. 클래스 맵을 생성하면 PAS-K는 클래스 맵에 정의된 분류 기준에 따라 인바운드 인터페이스 패킷들이 해당 클래스에 속하는지 여부를 확인하게 됩니다. 패킷들이 클래스로 분류되면, 클래스가 속한 정책 맵에 정의된 QoS Action이 패킷에 적용됩니다.

PAS-K에서 클래스 맵을 생성하고 트래픽 분류를 위한 기준을 정의하려면, <Configuration 모드>에서 다음 명령을 실행합니다.

순서	명 령	설 명
1	**qos**	<QoS 설정 모드>로 들어갑니다.
2	**class-map** *<NAME>*	클래스 맵을 정의하고 <Class-map 설정 모드>로 들어갑니다. • *<NAME>* 최대 64개의 클래스 맵 등록이 가능하며, 1 ~ 32자 사이의 알파벳 대/소문자, 숫자, '-', '_' 문자로 구성된 문자열. 첫 글자는 반드시 알파벳 사용. **주의:** 'pbnd' 또는 'vmac'으로 시작하는 이름은 클래스 맵 이름으로 사용할 수 없습니다.
다음 3 ~ 13번 과정은 트래픽의 분류 기준을 설정하는 과정으로, 추가하고자 하는 기준만 선택적으로 설정합니다.		
3	**match source-ip** *<SOURCE-IP>*	출발지 IP 주소 또는 IP 대역을 기준으로 패킷을 분류합니다. • *<SOURCE-IP>* 출발지 IP 주소 또는 IP 대역. 입력 형식: A.B.C.D/M
4	**match dest-ip** *<DEST-IP>*	목적지 IP 주소 또는 IP 대역을 기준으로 패킷을 분류합니다. • *<DEST-IP>* 목적지 IP 주소 또는 IP 대역. 입력 형식: A.B.C.D/M
5	**match source-mac** *<SOURCE-MAC>*	출발지 MAC 주소 기준으로 패킷을 분류합니다. • *<SOURCE-MAC>* 출발지 MAC 주소. 입력 형식: FF:FF:FF:FF:FF:FF
6	**match dest-mac** *<DEST-*MAC>	목적지 MAC 주소 기준으로 패킷을 분류합니다. • *<DEST-*MAC> 목적지 MAC 주소. 입력 형식: FF:FF:FF:FF:FF:FF
7	**match source-port** *<SOURCE-PORT>*	출발지 포트 번호를 기준으로 패킷을 분류합니다. • *<SOURCE-PORT>* 출발지 포트 번호. 설정 범위: 1 ~ 65535
8	**match dest-port** *<DEST-*PORT>	목적지 포트 번호를 기준으로 패킷을 분류합니다. • *<DEST-*PORT> 목적지 포트 번호. 설정 범위: 1 ~ 65535
9	**match protocol** *<PROTOCOL>*	프로토콜을 기준으로 패킷을 분류합니다. • *<PROTOCOL>* 프로토콜 번호. 설정 범위: 0 ~ 255
10	**match dscp** *<DSCP>*	DSCP 필드값을 기준으로 패킷을 분류합니다. • *<DSCP>* DSCP 필드값. 설정 범위: 0 ~ 63
11	**match ether-type** *<ETHER-TYPE>*	Ethernet type 필드값을 기준으로 패킷을 분류합니다. • *<ETHER-TYPE>* Ethernet type 필드값. 설정 범위: 0000~FFFF
12	**match port** *<PORT>*	입력 인터페이스를 기준으로 패킷을 분류합니다. • *<PORT>* 인터페이스 이름. 여러 개의 포트를 추가하려면 공백 없이 쉼표(,)로 각 포트를 구분.
13	**match vlan** *<VLAN>*	패킷이 속한 VLAN을 기준으로 패킷을 분류합니다. • *<VLAN>* VLAN ID. 설정 범위: 1 ~ 4080
14	**match any-traffic {enable | disable}**	분류 기준과 트래픽 분류 기준 사용 여부를 설정합니다. • **enable** 분류 기준과 관계 없이 모든 트래픽에 정책 적용 • **disable** 분류 기준을 사용하여 정책 적용(기본값)
15	**current**	설정한 클래스 맵의 정보를 확인합니다.

16	**apply**	클래스 맵 설정 정보를 저장합니다.

참고: 정의한 클래스 맵을 삭제하려면, <QoS 설정 모드>에서 **no class-map** *<NAME>* 명령을 사용합니다.

참고: 정의한 클래스의 분류 기준을 삭제하려면, <Class-map 설정 모드>에서 **no match** 명령과 함께 삭제하고자 하는 분류 기준을 입력합니다.

정책 맵(Policy map) 설정

정책 맵은 클래스 맵을 통해 분류된 트래픽에 적용할 정책(QoS Action)을 정의한 것입니다. 정책 맵에는 특정 트래픽 클래스로 분류된 패킷에 적용할 QoS Action이 정의됩니다. 하나의 정책 맵에는 서로 다른 분류 기준을 갖는 여러 개의 클래스와 해당 클래스에 적용할 QoS Action을 포함할 수 있습니다. 그리고, 하나의 클래스에 여러 QoS Action이 적용될 수 있도록 여러 개의 QoS Action을 정책 맵에 동시에 추가할 수 있습니다.

정책 맵을 정의하고, 정책을 적용할 클래스 맵을 지정한 다음 해당 클래스를 위해 QoS Action을 설정하려면, <QoS 설정 모드>에서 다음 명령을 실행합니다.

순서	명 령	설 명
1	**policy-map** *<NAME>*	정책 맵을 정의하고 <Policy-map 설정 모드>로 들어갑니다. • *<NAME>* 최대 64개의 클래스 맵 등록이 가능하며, 1 ~ 32자 사이의 알파벳 대/소문자와 숫자, '-', '_' 문자로 구성된 문자열. 첫 글자는 반드시 알파벳 사용. **주의:** 정책 맵 이름으로 'system'은 사용할 수 없습니다.
2	**apply**	정의한 정책 맵을 저장합니다. **참고:** 정책 맵을 저장하기 전에는 클래스 맵을 추가할 수 없습니다.
3	**class-map** *<NAME>*	이미 정의되어 있는 클래스 맵 중에서 정책을 적용할 클래스 맵을 지정하고, <Policy-map-class 설정 모드>로 들어갑니다. • *<NAME>* 정책을 적용할 클래스 맵 이름
4	**precedence** *<PRECEDENCE>*	지정한 클래스 맵의 우선순위를 설정합니다. 하나의 정책 맵에 여러 개의 클래스 맵을 지정한 경우에는 우선순위가 높은(숫자가 작은) 클래스 맵의 정책이 먼저 적용됩니다. • *<PRECEDENCE>* 클래스 맵 우선순위. 설정 범위: 2 ~ 12, 기본값: 6
다음 5 ~ 11번 과정은 정의한 정책 맵에 적용할 QoS Action을 설정하는 과정으로, 추가하고자 하는 QoS Action만 선택적으로 설정합니다.		
5	**drop-precedence {enable | disable}**	분류된 패킷을 우선적으로 차단할지 여부를 지정합니다. • **enable** 패킷을 우선적으로 차단 • **disable** 패킷을 우선적으로 차단하지 않음. (기본값)
6	**dscp** *<DSCP>*	분류된 패킷에 DSCP 필드값을 삽입합니다. • *<DSCP>* DSCP 설정 값. 설정 범위: 0 ~ 63
7	**priority** *<PRIORITY>*	분류된 패킷에 우선순위를 설정합니다. • *<PRIORITY>* 패킷 우선순위 값. 설정 범위: 0 ~ 7
8	**tos-to-priority {enable | disable}**	분류된 패킷의 ToS 값을 우선순위로 사용할지 여부를 지정합니다. • **enable** 분류된 패킷의 ToS 값을 우선순위로 사용 • **disable** 분류된 패킷의 ToS 값을 우선순위로 사용하지 않음 (기본값) **주의:** DSCP 값 또는 우선 순위를 설정한 경우에는 해당 QoS Action을 활성화 할 수 없습니다.
9	**priority-to-tos {enable | disable}**	패킷의 우선순위를 ToS 값으로 설정할지 여부를 지정합니다. • **enable** 패킷의 우선순위를 ToS 값으로 설정 • **disable** 패킷의 우선순위를 ToS 값으로 설정하지 않음 (기본값)

10	**action {deny | permit}**	분류된 패킷의 허용 여부를 설정합니다. • **deny** 분류된 패킷을 차단 • **permit** 분류된 패킷을 허용
11	**rate-limit** *<RATE>* **burst** *<BURST>*	해당 클래스에 속하는 트래픽의 대역폭을 제한합니다. • *<RATE>* 클래스의 트래픽에 보장해 줄 최대 대역폭. 설정 범위: 1 ~ 1000000, 단위: kbps *<BURST>* 클래스의 트래픽이 사용할 수 있는 최대 버스트. 설정 범위: 1 ~ 128000, 단위: kbps
12	**current**	설정한 정책 맵의 정보를 확인합니다.
13	**apply**	정책 맵 설정 정보를 저장합니다.

참고: 정의한 정책 맵을 삭제하려면, <QoS 설정 모드>에서 **no policy-map** *<NAME>* 명령을 사용합니다.

참고: 설정한 QoS Action을 삭제하려면, <Policy-map-class 설정 모드>에서 **no** 명령과 함께 삭제할 수 있는 QoS Action을 입력합니다. 삭제 가능한 QoS Action 항목은 DSCP, Priority, Action 이며, drop-precedence, priority-to-tos, tos-to-priority 항목은 no 명령을 사용할 경우, 기본값으로 변경됩니다.

참고: 대역폭 제한 설정을 삭제하려면, <Policy-map-class 설정 모드>에서 **no rate-limit** *<RATE>* 명령을 사용합니다.

서비스 정책(Service policy) 설정

서비스 정책은 정의한 정책 맵 중에서 실제로 어떤 정책 맵을 적용할 것인지를 지정하는 것입니다. 클래스 맵과 정책 맵을 정의하는 것이 QoS를 위한 규칙을 만드는 과정이라면, 서비스 정책을 정의하는 것은 만들어진 규칙 중에서 어떤 것을 어떤 포트에 사용할 것인지를 선택하는 과정이라고 할 수 있습니다. PAS-K에서 서비스 정책을 설정하려면, <QoS 설정 모드>에서 다음 명령을 실행합니다.

명 령	설 명
service-policy-map *<NAME>*	PAS-K에 적용할 서비스 정책을 정의합니다. • *<NAME>* 설정할 정책 맵(policy-map) 이름

참고: PAS-K에는 1개의 정책 맵만 서비스 정책으로 적용할 수 있습니다.

참고: 정의한 서비스 정책을 삭제하려면, <QoS 설정 모드>에서 **no service-policy** *<NAME>* 명령을 사용합니다. 서비스 정책을 삭제하지 않은 경우에는 다른 정책 맵을 서비스 정책으로 설정할 수 없습니다.

서비스 큐 스케줄링(Service Queue Scheduling) 설정

서비스 큐 스케줄링 기능은 큐에 저장되어 있는 패킷이 전송할 수 있는 대역폭보다 큰 경우 어떤 패킷을 우선적으로 처리할 것인지를 지정합니다. PAS-K의 각 포트에는 8개의 전송 큐가 존재하며, 큐 처리 시 사용할 스케줄링 방식을 설정하려면, <QoS 설정 모드>에서 다음 명령을 실행합니다.

순서	명 령	설 명
1	**service-queue** *<PORT>*	<Service-queue 설정 모드>로 들어갑니다. • *<PORT>* 서비스 큐를 설정할 포트 이름.
2	**output-schedule-mode** {**drr** | **rr** | **spq** | **wrr**}	포트에 적용할 큐 스케줄링 방식을 선택합니다. • **drr** 패킷의 길이를 고려하여 처리하는 방식 • **rr** 큐를 순차적으로 선택하여 처리하는 방식 • **spq** 우선순위가 높은 큐의 패킷을 먼저 처리하는 방식(기본값) • **wrr** 가중치에 따라 패킷을 차례대로 처리하는 방식 **참고:** 큐 스케줄링 방식을 기본값으로 변경하려면 <Service queue 설정 모드>에서 **no output-schedule-mode** 명령을 사용합니다.
3	**output-queue** *<INDEX>* **weight** *<WEIGHT>*	스케줄링 방식을 'drr' 또는 'wrr'로 설정한 경우, 각 큐에 적용할 가중치를 설정합니다. • *<INDEX>* 큐 번호. 설정 범위: 0 ~ 7 • *<WEIGHT>* 해당 큐에 할당할 가중치. 설정 범위: 0 ~ 15 **참고:** 큐에 설정한 가중치를 삭제하려면, <Service queue 설정 모드>에서 **no output-queue** *<INDEX>* **weight** 명령을 사용합니다.

CoS 필드의 우선순위에 따라 전송 큐를 처리하도록 설정하려면, <Service-queue 설정 모드>에서 다음 명령을 실행합니다.

명 령	설 명
input-cos-map *<PRIORITY>* **index** *<INDEX>*	CoS 필드의 우선순위에 따라 전송 큐를 처리하도록 설정합니다. • *<PRIORITY>* CoS 필드 우선순위. 설정 범위: 0 ~ 7 • *<INDEX>* 큐 번호. 설정 범위: 0 ~ 7 우선순위와 큐번호를 설정하지 않을 경우, CoS 필드의 우선순위에 따라 기본적으로 할당되는 큐 번호는 다음과 같습니다.

우선순위	큐 번호
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

참고: CoS 필드 우선 순위 설정을 삭제하려면, <Service queue 설정 모드>에서 **no input-cos-map** *<PRIORITY>* 명령을 사용합니다.

참고: PAS-K4200/4400 모델의 경우, 하드웨어 제약 사항으로 인해 서비스 큐 기능을 지원하지 않습니다.

대역폭 제한 설정

특정 포트를 통해 송수신되는 트래픽의 대역폭을 제한하려면, <Service-queue 설정 모드>에서 다음 명령을 실행합니다.

명 령	설 명
output-rate-limit <*RATE*> **burst** <*BURST*>	지정한 포트를 통해 송수신되는 트래픽의 대역폭을 설정합니다. • <*RATE*> 포트에 보장해줄 최대 대역폭 설정 범위: 1 ~ 1000000, 단위: kbps • <*BURST*> 포트에 허용할 최대 버스트 설정 범위: 1 ~ 128000, 단위: kbps

참고: 포트에 설정한 대역폭 제한을 삭제하려면, 해당 포트의 <Service-queue 설정 모드>에서 **no output-rate-limit** <*RATE*> 명령을 사용합니다.

정의한 큐에 대역폭 제한 설정을 하려면, <Service-queue 설정 모드>에서 다음 명령을 실행합니다.

명 령	설 명
output-queue <*INDEX*> {**max-rate** <*MAX-RATE*> | **min-rate** <*MIN-RATE*>}	정의한 큐에 대역폭 제한 설정을 합니다. • <*INDEX*> 큐 번호. 설정 범위: 0 ~ 7 • <*MAX-RATE*> 최대 대역폭. 설정 범위: 1 ~ 1000000, 단위: kbps • <*MIN-RATE*> 최소 대역폭. 설정 범위: 1 ~ 1000000, 단위: kbps

참고: 큐에 설정한 대역폭 제한을 삭제하려면, <Service-queue 설정 모드>에서 **no output-queue** <*INDEX*> {**max-rate** | **min-rate**} 명령을 사용합니다.

참고: PAS-K4200/4400 모델의 경우, 하드웨어 제약으로 대역폭 제한 기능을 지원하지 않습니다.

설정 정보 보기

QoS 관련 설정 정보 보기

현재 PAS-K에 정의된 서비스 정책이나 큐 스케쥴링 설정 정보를 확인하려면, <Privileged 모드> 또는 <Configuration 모드>에서 **show qos** 명령을 실행합니다.

클래스 맵 설정 정보 보기

현재 정의된 클래스 맵은 <QoS 설정 모드>에서 **show class-map** 명령을 통해 확인할 수 있습니다. 특정한 클래스 맵에 대한 상세한 설정 정보를 확인하려면, **show class-map** <*NAME*> 명령을 실행합니다.

정책 맵 설정 정보 보기

현재 정의된 정책 맵은 <QoS 설정 모드>에서 **show policy-map** 명령을 통해 확인할 수 있습니다. 특정한 클래스 맵에 대한 상세한 설정 정보를 확인하려면, **show policy-map** <*NAME*> 명령을 실행합니다.

서비스 큐 스케줄링 및 대역폭 제한 설정 정보 보기

현재 정의된 서비스 큐 스케줄링 및 대역폭 제한 설정 정보를 확인하려면, <QoS 설정 모드>에서 **show service-queue** 명령을 통해 확인할 수 있습니다. 특정한 포트에 대한 상세한 서비스 큐 스케줄링 및 대역폭 제한 설정 정보를 확인하려면, <QoS 설정 모드>에서 **show service-queue** <*PORT*> 명령을 실행합니다.

참고: 해당 명령 실행 시 출력되는 화면과 설정 정보에 관한 상세한 내용은 이 설명서와 함께 제공되는 명령 설명서를 참고하도록 합니다.