PFr 포워딩 루프를 탐지하고 지우는 데 사용되는 EEM 애플릿

목차

소개

이 문서에서는 PfR(Performance Routing)이 여러 BR(Border Relays)을 통해 트래픽을 최적화하는 네트워크에서 사용되는 EEM(Embedded Event Manager) 애플릿에 대해 설명합니다. 일부 포워딩 루프도 관찰됩니다.루프가 관찰될 때 데이터를 수집하고 전달 루프의 영향을 줄이기 위해 애플릿을 사용합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 EEM 버전 4.0을 지원하는 Cisco IOS® 소프트웨어를 기반으로 합니다.

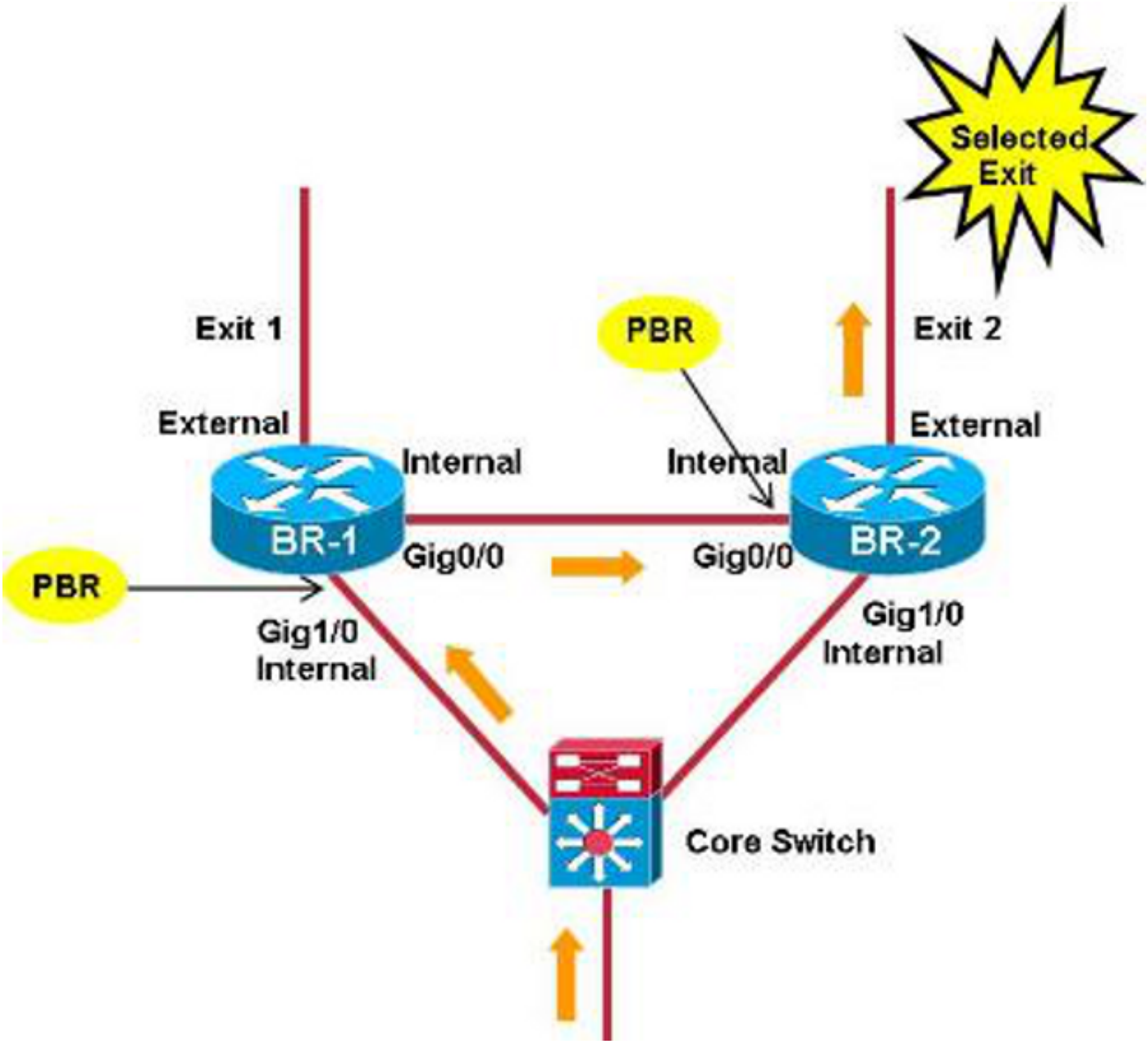
Cisco IOS 릴리스에서 지원하는 EEM 버전을 확인하려면 다음 명령을 사용합니다.

```
Router#sh event manager version | i Embedded
Embedded Event Manager Version 4.00
Router#
```

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

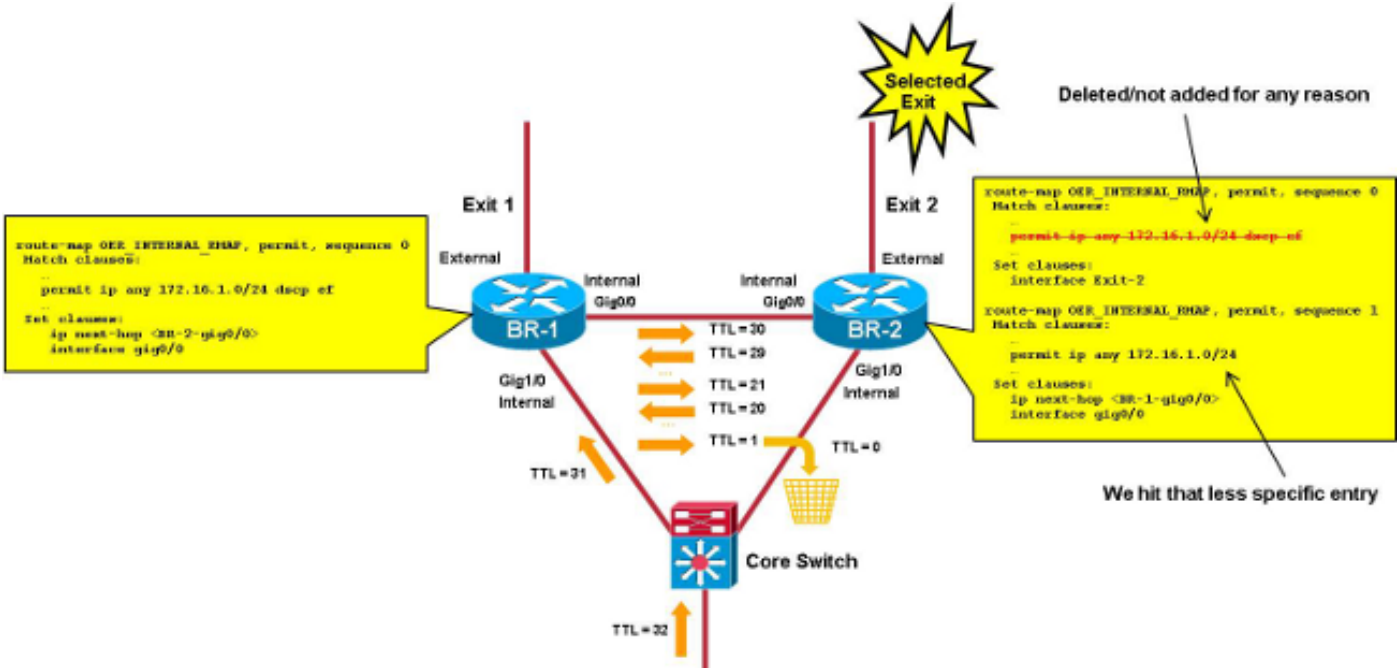
배경 정보

PfR이 TC(Traffic Class)를 제어할 때 BR에 동적 경로 맵/ACL(Access Control List)을 생성합니다.선택한 종료가 있는 BR의 경로 맵은 선택한 종료를 가리키고, 다른 BR의 경로 맵은 내부 인터페이스를 가리킵니다(next-hop = selected BR).



동적 ACL이 서로 다른 BR 간에 제대로 동기화되지 않은 경우(예: 버그) 문제가 발생합니다.

이 그림에서 DSCP EF를 사용하여 172.16.1.0/24으로 향하는 모든 IP 패킷을 확인하는 데 초점을 맞추고 있습니다.이 시나리오에서는 관련 ACL 항목이 선택한 BR(BR-2)에서 제거되지만 BR-1에서는 제거되지 않습니다. 해당 TC의 패킷이 172.16.1.0/24으로 향하는 모든 IP 패킷과 일치하는 접두사 엔트리와 함께 BR-2에 도달했습니다. 접두사 엔트리에 대해 선택한 종료는 **Exit-1이므로 BR**-2의 관련 route-map/ACL은 BR-1을 가리킵니다.



이제 TTL(Time To Live)이 0에 도달할 때까지 해당 TC의 패킷이 BR 간에 반복됩니다.

이 문서에서는 다음 작업을 수행하는 데 필요한 EEM 애플릿을 제공합니다.

- BR 간 포워딩 루프 탐지
- 관련 정보 수집 및 PfR 지우기

MC(Master Controller)/BR 콤보(BR 중 하나에서 MC가 실행되는 경우)의 경우 사용되는 애플릿이 훨씬 더 쉽습니다. 전용 MC가 있는 시나리오도 다릅니다.

EEM 애플릿 세부사항

이 섹션에서는 이 프로세스에 사용되는 액세스 목록과 애플릿 로그 파일에 대해 설명합니다.

사용된 액세스 목록

전달 루프를 탐지하기 위해 애플릿은 ACL을 사용하여 낮은 TTL의 패킷을 확인합니다.

> **참고:**TTL에 대한 ACL 매칭은 ASR(Aggregation Service Router) 1000 Series Version 3.7s(15.2(4)S) 이상에서 지원됩니다.

BR 간에 루프되는 각 패킷에 대해 1개의(및 1개의) 히트를 얻으려면 2x 연속 비교적 낮은 TTL 값(20 및 21)에서 ACE 일치를 사용하는 것이 좋습니다.traceroute 패킷에서 자주 적중하지 않도록 사용되는 TTL 값이 너무 낮으면 안 됩니다.

```
interface gig0/0 (internal interface)
 ip access-group LOOP in
!
ip access-list extended LOOP
 permit ip 10.116.48.0 0.0.31.255 any ttl range 20 21
 permit ip any any
```

ACL은 show pfr **master border topology** 명령 출력에 보고된 내부 인터페이스에 배치해야 합니다.

소스 IP 범위(여기 10.116.48.0/20)은 내부 네트워크(내부 인터페이스를 통해 연결 가능한 접두사)와 일치해야 합니다.

> **참고:**하나의 ACE(Access-list Entry)에서 내부 네트워크를 요약할 수 없는 경우 여러 ACE를 사용할 수 있습니다.그러나 여러 행의 적중 횟수를 확인하려면 스크립트를 약간 수정해야 합니다.

> **참고:**자동 터널 기능을 해제해야 합니다(마스터 PfR 모드**에서 모드 자동 터널** 없음). BR이 직접 연결되지 않은 경우 수동 GRE(Generic Routing Encapsulation) 터널을 생성하고 터널 인터페이스에 ACL을 배치해야 합니다.

루프의 영향을 받는 원격 사이트/TC를 식별하려면 각 원격 사이트/TC에 대해 더 구체적인 ACE를 사용하여 인터페이스에 두 번째 ACL 아웃바운드(아웃바운드)를 추가할 수 있습니다.

```
interface gig0/0 (internal interface)
 ip access-group LOOP-DETAIL out

!
ip access-list extended LOOP-DETAIL

permit ip 10.116.48.0 0.0.31.255 10.116.132.0 0.0.0.255 ttl range 20 21
permit ip 10.116.48.0 0.0.31.255 10.116.128.0 0.0.0.255 ttl range 20 21
 .... (add here one line per remote site)
permit ip any an
```

대상 IP는 다른 원격 사이트의 서브넷과 일치합니다.

```
10.116.132.0/24 -> site-1
10.116.128.0/24 -> site-2
```

루프의 영향을 받는 정확한 TC를 식별해야 하는 경우 원격 사이트당 여러 라인을 추가할 수도 있습니다.

애플릿 임무

애플릿은 ACL 루프의 TTL에서 매칭하는 ACE의 히셋을 30초마다 확인합니다.이러한 검사의 결과에 따라 애플릿에서 다음 작업을 수행할 수 있습니다.

- 히트카운트가 구성된 임계값(THRESHOLD_1)을 초과할 경우, 애플릿은 ACL 카운트를 지우고 15초 만에 히타이트를 다시 확인합니다.
- 15초 후 히트카운트가 두 번째 임계값보다 큰 경우($_2$) 루프가 있을 수 있습니다.루프 문제를 해결하려면 출력 집합을 수집하고 PfR을 지워야 합니다.
- 두 번째 임계값은 전역 변수로 정의되므로 애플릿을 다시 시작하지 않고도 쉽게 조정됩니다.
- 이러한 임계값의 최적 값은 주로 TC당 평균 패킷 속도에 따라 달라집니다.

애플릿 로그 파일

애플릿은 적중 횟수(카운트가 0보다 큰 경우) 및 임시 루프(THRESHOLD_1이 초과되었지만 THRESHOLD_2가 아닌 경우) 또는 실제 루프(THRESHOLD_1과 THRESHOLD_2가 모두 초과된

경우)를 추적하는 로그 파일을 유지 관리합니다.

MC/BR Combo 및 기타 BR 시나리오용 애플릿

이 문서에서 설명하는 가장 간단한 시나리오입니다.루프 탐지 및 PfR 지우기는 동일한 디바이스에서 수행되므로 디바이스 EEM 애플릿 통신을 입력할 필요가 없습니다.별도의 애플릿은 MC/BR 콤보 및 기타 BR에서 실행됩니다.

MC/BR Combo의 애플릿

이 출력은 MC/BR 콤보 상자에 사용되는 애플릿에 대한 중요 정보를 표시합니다.다음은 이 특정 출력에 대한 몇 가지 중요한 참고 사항입니다.

- THRESHOLD_1에 표시된 값은 1000이고 THRESHOLD_2에 표시된 값은 500입니다. 이는 루프의 영향을 받는 TC의 비율이 100/30(33pps)보다 높은 경우 애플릿이 시작됨을 의미합니다.
- DISK 변수는 로그 및 출력 파일이 푸시되는 위치를 식별합니다(bootflash에 표시됨).
- 로그 파일에 있는 항목의 타임스탬프는 **show clock** 명령 출력에서 파생됩니다.중간에 있는 문자("est"로 표시됨)는 시간대를 기반으로 하며 조정되어야 합니다(**action 240** 참조).
- 루프가 발생할 경우 수집해야 하는 출력이 bootflash의 **script-output-xxxxxxx** 파일에 푸시됩니다. 여기서 "xxxxxx"는 1970년 이후의 시간(각 루프 어커런스에 대해 고유한 파일 이름을 만드는 데 사용됨)입니다.
- 수집된 명령은 작업 **330, 340, 350 및 360에** 나열됩니다. 일부 추가/다른 명령을 추가할 수 있습니다.

```
event manager environment THRESHOLD_1 1000
event manager environment THRESHOLD_2 500
event manager environment DISK bootflash
!
event manager applet LOOP-MON authorization bypass
 event timer watchdog name LOOP time 30
 action 100 cli command "enable"
 action 110 cli command "show ip access-list LOOP"
 action 120 set regexp_substr 0
 action 130 regexp "range 20 21 \(([0-9]+) matches\)"
 $_cli_result _regexp_result regexp_substr
 action 140 cli command "clear ip access-list counters LOOP"
 action 150 if $regexp_substr gt 0
 action 200 set MATCHES $regexp_substr
 action 210 file open LOGS $DISK:script-logs.txt a
 action 220 cli command "enable"
 action 230 cli command "show clock"
 action 240 regexp "[0-9]+:[0-9]+:[0-9]+.[0-9]+ est [A-Za-z]+
  [A-Za-z]+ [0-9]+ 201[0-9]" $_cli_result _regexp_result
 action 250 set TIME $_regexp_result
 action 260 if $MATCHES gt $THRESHOLD_1
 action 270 wait 15
 action 280 cli command "show ip access-list LOOP"
 action 290 set regexp_substr 0
 action 300 regexp "range 20 21 \(([0-9]+) matches\)"
  $_cli_result _regexp_result regexp_substr
 action 310 if $regexp_substr gt $THRESHOLD_2
 action 320 cli command "enable"
 action 330 cli command "show ip access-list LOOP-DETAIL
```

```
  | tee /append $DISK:script-output-$_event_pub_sec.txt"
 action 340 cli command "show pfr master traffic-class perf det
  | tee /append $DISK:script-output-$_event_pub_sec.txt"
 action 350 cli command "show route-map dynamic detail
  | tee /append $DISK:script-output-$_event_pub_sec.txt"
 action 360 cli command "show ip route
  | tee /append $DISK:script-output-$_event_pub_sec.txt"
 action 370 cli command "clear pfr master *"
 action 380 cli command "clear ip access-list counters LOOP-DETAIL"
 action 390 file puts LOGS "$TIME - LOOP DETECTED - PfR CLEARED -
  matches $MATCHES > $THRESHOLD_1 and $regexp_substr
> $THRESHOLD_2 - see $DISK:script-output-$_event_pub_sec.txt"
 action 400 syslog priority emergencies msg "LOOP DETECTED -
  PfR CLEARED - see $DISK:script-output-$_event_pub_sec.txt !"
 action 410 else
 action 420 file puts LOGS "$TIME - TEMPORARY LOOP : matches
  $MATCHES > $THRESHOLD_1 and $regexp_substr < or = $THRESHOLD_2"
 action 430 cli command "clear ip access-list counters LOOP-DETAIL"
 action 440 end
 action 450 else
 action 460 cli command "en"
 action 470 cli command "clear ip access-list counters LOOP-DETAIL"
 action 480 file puts LOGS "$TIME - number of matches =
  $MATCHES < $THRESHOLD_1"
 action 490 end
 action 500 else
 action 510 cli command "clear ip access-list counters LOOP-DETAIL"
 action 520 end
```

다른 BR용 애플릿

이 섹션에서는 다른 BR에 사용되는 애플릿에 대해 설명합니다.다음은 이 특정 출력에 대한 몇 가지 중요한 참고 사항입니다.

- MC/BR 콤보 상자의 스크립트가 30초마다 실행되는 동안 애플릿은 20초마다 실행됩니다.이렇게 하면 MC/BR에서 실행되는 애플릿을 통해 PfR이 지워지기 전에 BR에서 애플릿이 실행됩니다.
- 고유한 임계값이 사용되므로 오류 양수를 피할 필요가 없습니다.
- THRESHOLD에 표시된 값은 700이며 MC/BR 애플릿의 **THRESHOLD_1** 값에 따라 설정해야 합니다.
- 애플릿 로그 파일은 **flash0**의 **script-logs.txt** 파일에 푸시됩니다. 이 파일은 **action 170** 및 **DISK** 변수**에서** 변경할 수 있습니다.
- 로그 파일에 있는 항목의 타임스탬프는 **show clock** 명령 출력에서 파생됩니다.중간에 있는 문자(여기에 "est"로 표시됨)는 시간대를 기준으로 하며 조정되어야 합니다(**action 190** 참조).
- 루프의 경우 수집해야 하는 출력이 script**-output-xxxxxxx** 파일에 푸시됩니다. 여기서 "xxxxxx"는 1970년 이후의 시간(초 단위)입니다(각 루프의 고유한 파일 이름을 만드는 데 사용됨).
- 수집된 명령은 **작업 230** 및 **작업 240에** 나열됩니다. 일부 추가/다른 명령을 추가할 수 있습니다.

```
event manager environment THRESHOLD 700
event manager environment DISK flash 0
!
event manager applet LOOP-BR authorization bypass
  event timer watchdog name LOOP time 20
 action 100 cli command "enable"
```

```
action 110 cli command "show ip access-list LOOP"
action 120 set regexp_substr 0
action 130 regexp "range 20 21 \(([0-9]+) matches\)"
 $_cli_result _regexp_result regexp_substr
action 140 cli command "clear ip access-list counters LOOP"
action 150 if $regexp_substr gt 0
action 160  set MATCHES $regexp_substr
action 170  file open LOGS $DISK:script-logs.txt a
action 180  cli command "show clock"
action 190  regexp "[0-9]+:[0-9]+:[0-9]+.[0-9]+
 est [A-Za-z]+ [A-Za-z]+ [0-9]+ 201[0-9]" $_cli_result _regexp_result
action 200  set TIME $_regexp_result
action 210  if $MATCHES gt $THRESHOLD
action 220   cli command "enable"
action 230   cli command "show route-map dynamic detail | tee /append
 $DISK:script-output-$_event_pub_sec.txt"
action 240   cli command "show ip route | tee /append
 $DISK:script-output-$_event_pub_sec.txt"
action 250   file puts LOGS "$TIME : matches = $MATCHES >
 $THRESHOLD - see $DISK:script-output-$_event_pub_sec.txt"
action 260   syslog priority emergencies msg "LOOP DETECTED -
 Outputs captured - see $DISK:script-output-$_event_pub_sec.txt !"
action 270  else
action 280   file puts LOGS "$TIME : matches = $MATCHES < or = $THRESHOLD"
action 290  end
action 300 end
```

전용 MC 시나리오에 대한 애플릿

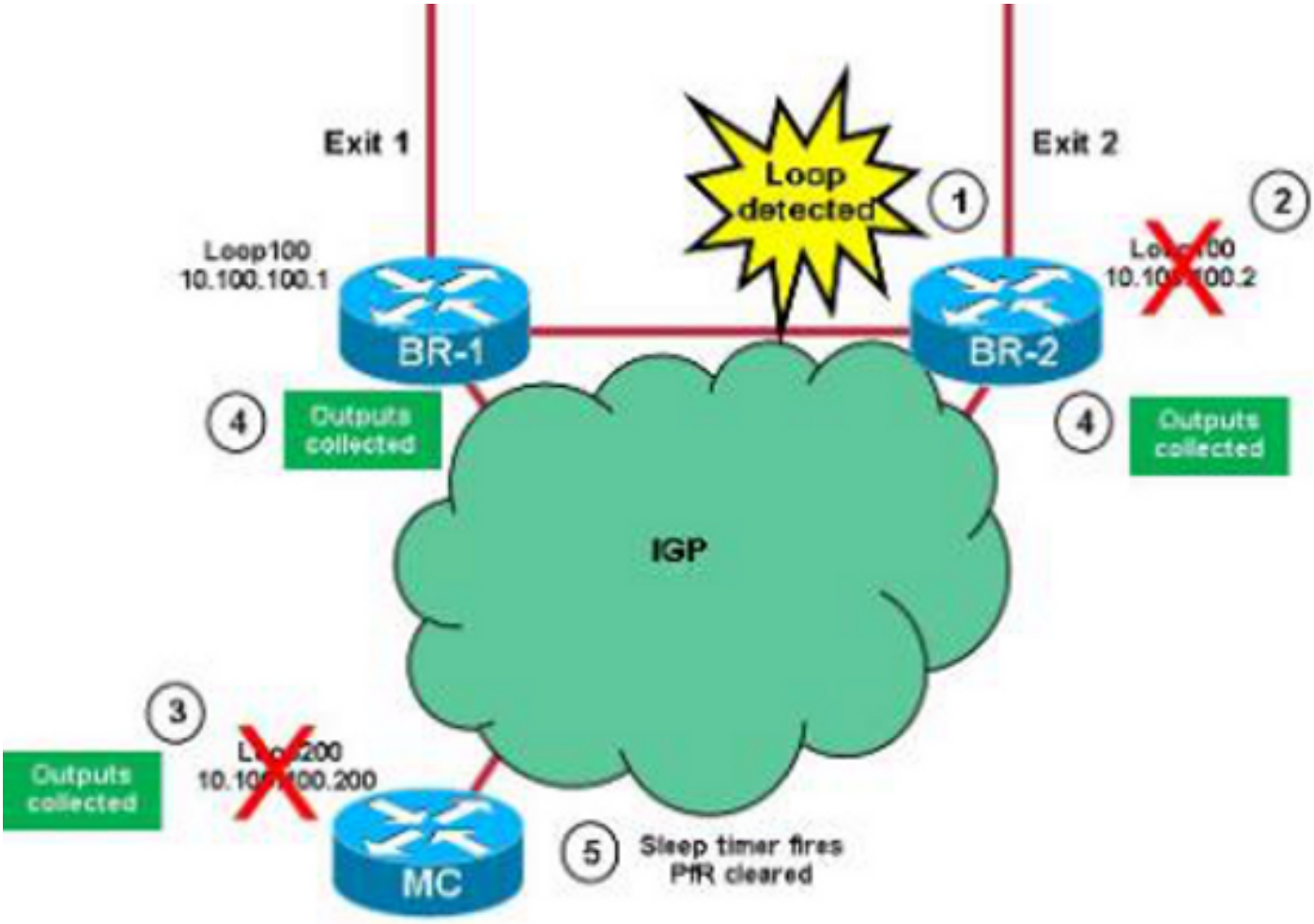
루프 탐지 및 PfR 지우기/통계 수집은 디바이스 간 EEM 애플릿 통신이 필요한 여러 디바이스에서 완료됩니다.디바이스 간의 통신은 서로 다른 방식으로 이루어집니다.이 문서에서는 IGP에서 광고되는 전용 루프백의 연결 가능성을 확인하기 위해 추적되는 객체를 통한 디바이스 통신에 대해 설명합니다.이벤트가 탐지되면 루프백이 종료되므로 추적되는 객체가 오프라인 상태가 될 때 원격 디바이스의 애플릿이 시작할 수 있습니다.서로 다른 정보를 교환해야 하는 경우 다른 루프백을 사용할 수 있습니다.

애플릿 통신

다음 애플릿 및 통신 방법이 사용됩니다.

애플릿 이름	어디서?	뭐?	트리거 ?	통신?
루프-BR	BR	루프를 탐지하려면 ACL 히타이트를 확인합니다.	주기적	종료 루프100
루프-MC	MC	- PfR 정보 수집 - PfR 지우기	추적 연결성 루프100	shut 루프200
COLLECT-BR	BR	정보 수집	추적 연결성 루프200	none

다음 그림을 참조하십시오.



애플릿에서 사용하는 프로세스입니다.

1. 루프는 BR의 LOOP-**BR** 애플릿에서 탐지됩니다.루프가 먼저 BR-2에서 탐지된 것으로 가정합니다.
2. 애플릿은 **BR**-2에서 Loop100을 종료하며, 정보는 IGP(Interior Gateway Protocol)에 광고됩니다.
3. BR-2**의 Loop100에** 대한 추적 객체가 MC에서 오프라인 상태가 되고 LOOP-**MC** 애플릿이 시작됩니다.PfR 마스터 출력이 수집되고 MC의 루프백 **200**이 종료됩니다.이 정보는 IGP에 광고됩니다.10초 절전 타이머가 시작됩니다.
4. MC에서 Loop**200**에 대한 추적 객체가 두 BR에서 모두 오프라인 상태가 됩니다.이렇게 하면 BR 특정 정보**를** 수집하는 COLLECT-BR 애플릿이 트리거됩니다.
5. 절전 타이머(3단계)가 시작되고 MC에서 PfR을 지웁니다.

참고: PfR이 지워지기 전에 BR-1이 루프를 탐지하면 MC에서 오프라인으로 이동하는 추적된 객체가 무시됩니다(LOOP-**MC** 애플릿이 1분에 한 번 실행).

추적 객체 및 루프백 생성

이 섹션에서는 루프백을 생성하고(IP가 IGP에 광고되었는지 확인) 객체를 추적하는 방법에 대해 설명합니다.

개체 추적

다음은 추적 객체를 생성할 때 유의해야 할 몇 가지 중요한 사항입니다.

- BR에는 단일 트랙 객체가 필요합니다. 이 객체는 MC에서 **루프백200**(데이터 수집 트리거)을 추적하기 위해 사용됩니다.
- MC에는 다음과 같은 몇 개의 트랙 객체가 필요합니다. 트랙 1과 2는 각각 BR-1 및 BR-2**에서 루프백100**을 추적하기 위해 사용됩니다.트랙 11과 12는 각각 BR-1과 BR-2 간의 연결을 추적하는 데 사용됩니다(BR 간에 연결 문제가 있을 경우 PfR 지우기 방지).트랙 20은 트랙 11과 12 사이의 논리적 AND를 추적합니다. 이는 MC가 모든 BR에 연결할 수 있는지 확인하기 위해 사용됩니다.
- 연결 **가능성** 문제 탐지 속도를 높이기 위해 트랙 타이머 ip 경로 값이 1초로 설정됩니다(기본값은 15초).

BR-1

```
interface Loopback100
  ip address 10.100.100.1 255.255.255.255
!
track timer ip route 1
track 1 ip route 10.100.100.200 255.255.255.255 reachability
```

BR-2

```
interface Loopback100
ip address 10.100.100.2 255.255.255.255
!
track timer ip route 1
track 1 ip route 10.100.100.200 255.255.255.255 reachability
```

MC

```
interface Loopback200
ip address 10.100.100.200 255.255.255.255
!
track timer ip route 1

track 1 ip route 10.100.100.1 255.255.255.255 reachability
track 2 ip route 10.100.100.2 255.255.255.255 reachability
track 11 ip route 10.116.100.1 255.255.255.255 reachability
track 12 ip route 10.116.100.2 255.255.255.255 reachability
track 20 list boolean and
 object 11
 object 12
```

BR 및 MC 루프백

루프-BR

이 섹션에서는 BR에서 루프를 생성하는 방법에 대해 설명합니다.기억해야 할 몇 가지 중요한 사항이 있습니다.

- THRESHOLD_1 값은 1000이고 **THRESHOLD_2** 값은 500입니다. 이는 루프의 영향을 받는 TC의 비율이 1000/30(33p/s)보다 높은 경우 애플릿이 시작됨을 의미합니다.
- 애플릿 로그 파일은 bootflash의 **script-detect-logs.txt** 파일에 푸시됩니다.이는 **작업 210에서** 그리고 **DISK** 변수로 변경됩니다.

- 로그 파일에 있는 항목의 타임스탬프는 **sh 시계** 출력에서 파생됩니다.'est'로 표시된 가운데 문자는 시간대를 기준으로 하며 조정이 필요합니다(**action 240**).
- MC에 **알리기** 위해 Loopback100을 닫은 후 5초 동안(IGP에서 정보를 전파할 시간이 있는지 확인하기 위해) 기다렸다가 다시 엽니다(**작업 370**).

```
event manager environment THRESHOLD_1 100event manager environment
  THRESHOLD_2 500event manager environment DISK bootflash
!event manager applet LOOP-BR authorization bypass

 event timer watchdog name LOOP time 30 maxrun 27
 action 100 cli command "enable"
 action 110 cli command "show ip access-list LOOP"
 action 120 set regexp_substr 0
 action 130 regexp "range 20 21 \(([0-9]+) matches\)"
  $_cli_result _regexp_result regexp_substr
 action 140 cli command "clear ip access-list counters LOOP"
 action 150 if $regexp_substr gt 0
 action 200  set MATCHES $regexp_substr
 action 210  file open LOGS $DISK:script-detect-logs.txt a
 action 220  cli command "enable"
 action 230  cli command "show clock"
 action 240  regexp "[0-9]+:[0-9]+:[0-9]+.[0-9]+
  est [A-Za-z]+ [A-Za-z]+ [0-9]+ 201[0-9]"
  $_cli_result _regexp_result
 action 250  set TIME $_regexp_result
 action 260  if $MATCHES gt $THRESHOLD_1
 action 270  wait 15
 action 280  cli command "show ip access-list LOOP"
 action 290  set regexp_substr 0
 action 300  regexp "range 20 21 \(([0-9]+) matches\)"
  $_cli_result _regexp_result regexp_substr
 action 310  if $regexp_substr gt $THRESHOLD_2
 action 320  cli command "enable"
 action 330  cli command "conf t"
 action 340  cli command "interface loop100"
 action 350  cli command "shut"
 action 360  file puts LOGS "$TIME - LOOP DETECTED - Message sent to MC -
  matches $MATCHES > $THRESHOLD_1 and $regexp_substr > $THRESHOLD_2"
 action 370  wait 5
 action 375  cli command "enable"
 action 380  cli command "conf t"
 action 390  cli command "interface loop100"
 action 400  cli command "no shut"
 action 410  else
 action 420  file puts LOGS "$TIME - TEMPORARY LOOP : matches $MATCHES >
$THRESHOLD_1 and $regexp_substr < or = $THRESHOLD_2"
 action 430  cli command "clear ip access-list counters LOOP-DETAIL"
 action 440  end
 action 450  else
 action 460  cli command "en"
 action 470  cli command "clear ip access-list counters LOOP-DETAIL"
 action 480  file puts LOGS "$TIME - number of matches =
  $MATCHES < $THRESHOLD_1"
 action 490  end
 action 500 else
 action 510  cli command "clear ip access-list counters LOOP-DETAIL"
 action 520 end
```

루프-MC

이 섹션에서는 MC에서 루프를 생성하는 방법에 대해 설명합니다.기억해야 할 몇 가지 중요한 사항

이 있습니다.

- ratelimit 값은 애플릿이 ratelimit 값 60으로 실행되는 빈도에 따라 달라집니다(스크립트가 분당 1회 최대 1회 실행됨). 이 옵션은 두 BR에서 동일한 루프가 탐지될 때 PfR이 두 번 지워지지 않도록 하기 위해 사용됩니다.
- 작업 130에서 모든 BR에 대한 연결성을 확인하기 전에 2초 동안 기다립니다.이는 MC와 BR 간의 연결 문제로 인해 오탐이 발생하지 않도록 하기 위한 것입니다.
- 작업 240에서 Loopback200을 종료한 후 PfR을 지우기 전에 10초 동안 기다립니다.이는 BR에서 데이터를 수집할 시간이 있는지 확인하기 위한 것입니다.

```
event manage environment DISK bootflash
event manager applet LOOP-MC authorization bypass

event syslog pattern "10.100.100.[0-9]/32 reachability Up->Dow" ratelimit 60
action 100 file open LOGS $DISK:script-logs.txt a
 action 110 regexp "10.100.100.[0-9]" "$_syslog_msg" _regexp_result
 action 120 set BR $_regexp_result
 action 130 wait 2
 action 140 track read 20
 action 150 if $_track_state eq "up"
 action 160  cli command "enable"
 action 170  cli command "show clock"
 action 180  regexp "[0-9]+:[0-9]+:[0-9]+.[0-9]+
  est [A-Za-z]+ [A-Za-z]+ [0-9]+ 201[0-9]"
  "$_cli_result" _regexp_result
 action 190  set TIME "$_regexp_result"
 action 200  cli command "show pfr master traffic-class perf det
  | tee /append $DISK:script-output-$_event_pub_sec.txt"
 action 210  cli command "conf t"
 action 220  cli command "interface loop200"
 action 230  cli command "shut"
 action 240  wait 10
 action 250  cli command "conf t"
 action 260  cli command "interface loop200"
 action 270  cli command "no shut"
 action 280  cli command "end"
 action 290  cli command "clear pfr master *"
 action 300  file puts LOGS "$TIME - LOOP DETECTED by $BR -
  PfR CLEARED - see $DISK:script-output-$_event_pub_sec.txt"
action 310  syslog priority emergencies msg "LOOP DETECTED by $BR -
  PfR CLEARED - see $DISK:script-output-$_event_pub_sec.txt !"
 action 320 else
 action 330  file puts LOGS "$TIME - REACHABILITY LOST with
$BR - REACHABILITY TO ALL BRs NOT OK - NO ACTION"
 action 340 end
```

COLLECT-BR

이 섹션에서는 BR을 수집하는 방법에 대해 설명합니다.BR에서 MC에서 Loopback200(10.100.100.200)에 대한 연결이 끊길 때에서 애플릿이 실행됩니다.수집하기 위해 사용되는 명령은 작업 120, 130 및 140에 나열됩니다.

```
event manager environment DISK bootflash
event manager applet COLLECT-BR authorization bypass

event syslog pattern "10.100.100.200/32 reachability Up->Dow" ratelimit 45
 action 100 file open LOGS $DISK:script-collect-logs.txt a
 action 110 cli command "enable"
```

```
 action 120 cli command "sh ip access-list LOOP-DETAIL |
tee /append $DISK:script-output-$_event_pub_sec.txt"
 action 130 cli command "show route-map dynamic detail
  | tee /append $DISK:script-output-$_event_pub_sec.txt"
 action 140 cli command "show ip route | tee /append
  $DISK:script-output-$_event_pub_sec.txt"
 action 150 cli command "show clock"
 action 160 regexp "[0-9]+:[0-9]+:[0-9]+.[0-9]+ CET [A-Za-z]+ [A-Za-z]+
  [0-9]+ 201[0-9]" "$_cli_result" _regexp_result
 action 170 set TIME "$_regexp_result"
 action 180 file puts LOGS "$TIME - OUTPUTs COLLECTED -
  see $DISK:script-output-$_event_pub_sec.txt"
```

SYSLOG-MC

루프가 탐지될 때 MC의 syslog는 다음과 같습니다.

```
MC#
*Mar  8 08:52:12.529: %TRACKING-5-STATE: 1 ip route 10.100.100.1/32
 reachability Up->Down
MC#
*Mar  8 08:52:16.683: %LINEPROTO-5-UPDOWN:
 Line protocol on Interface Loopback200, changed state to down
*Mar  8 08:52:16.683: %LINK-5-CHANGED: Interface Loopback200,
 changed state to administratively down
MC#
*Mar  8 08:52:19.531: %TRACKING-5-STATE: 1
 ip route 10.100.100.1/32 reachability Down->Up
MC#
*Mar  8 08:52:24.727: %SYS-5-CONFIG_I: Configured from console by
 on vty0 (EEM:LOOP-MC)
*Mar  8 08:52:24.744: %PFR_MC-1-ALERT: MC is inactive due to PfR
 minimum requirements not met;
 Less than two external interfaces are operational
MC#
*Mar  8 08:52:24.757: %HA_EM-0-LOG: LOOP-MC:
 LOOP DETECTED by 10.100.100.1 - PfR CLEARED
 - see unix:script-output-1362732732.txt !
MC#
*Mar  8 08:52:26.723: %LINEPROTO-5-UPDOWN:
 Line protocol on Interface Loopback200, changed state to up
MC#
*Mar  8 08:52:26.723: %LINK-3-UPDOWN: Interface Loopback200,
 changed state to up
MC#
*Mar  8 08:52:29.840: %PFR_MC-5-MC_STATUS_CHANGE: MC is UP
*Mar  8 08:52:30.549: %TRACKING-5-STATE: 2
 ip route 10.100.100.2/32 reachability Up->Down
MC#
*Mar  8 08:52:37.549: %TRACKING-5-STATE: 2
 ip route 10.100.100.2/32 reachability Down->Up
MC#
```

참고:이러한 애플릿은 일부 튜닝과 함께 3개 이상의 BR에서 사용할 수 있습니다.