EEM-Applets zum Erkennen und Löschen von PfR-Weiterleitungsschleifen

Inhalt

Einführung

In diesem Dokument werden EEM-Applets (Embedded Event Manager) beschrieben, die in Netzwerken verwendet werden, in denen Performance Routing (PfR) den Datenverkehr über mehrere Border Relays (BRs) optimiert. Einige Weiterleitungsschleifen werden ebenfalls beobachtet. Die Applets werden zum Sammeln von Daten verwendet, wenn eine Schleife beobachtet wird, um die Auswirkungen einer Weiterleitungsschleife zu mindern.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IOS® Software, die EEM Version 4.0 unterstützt.

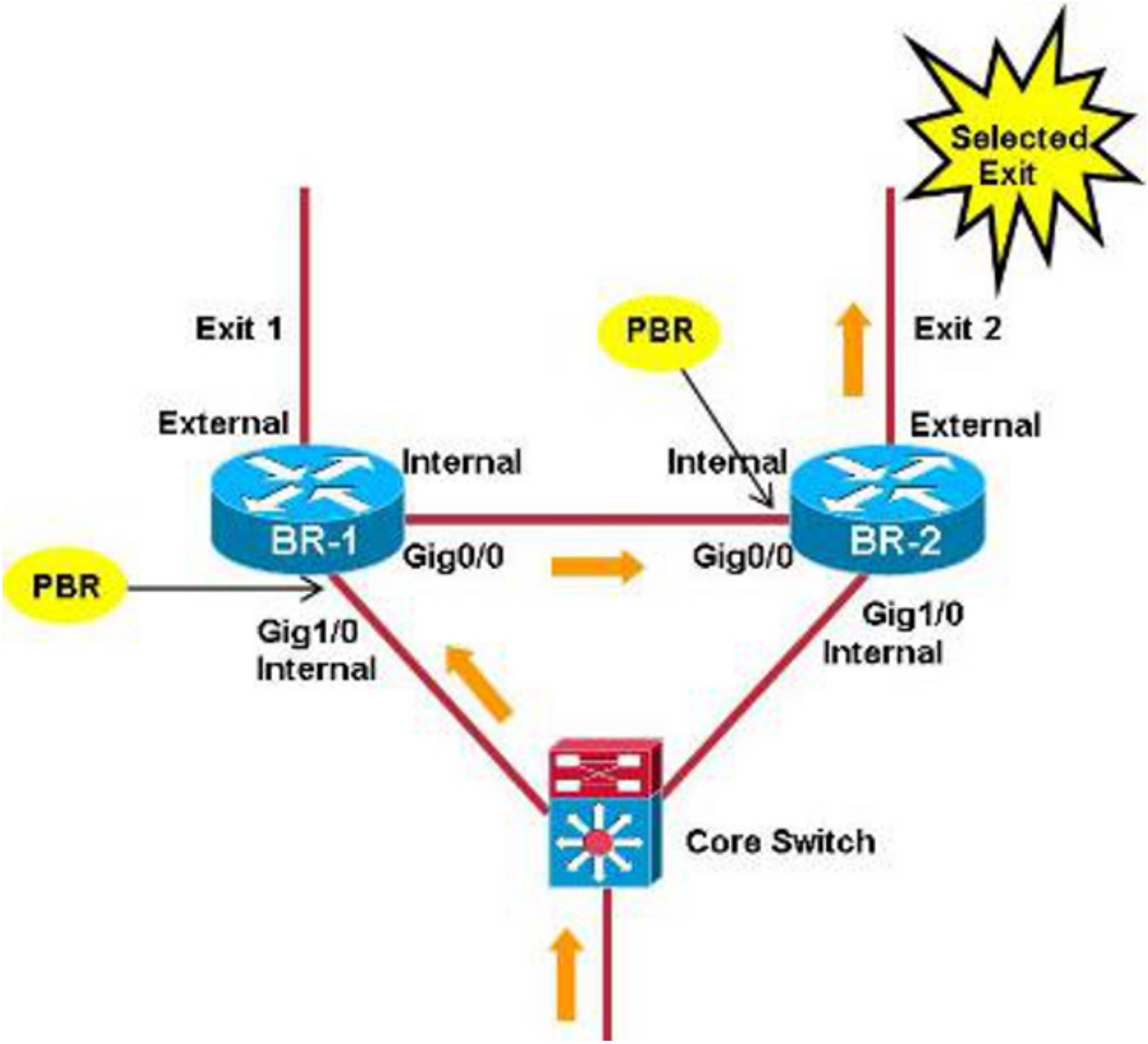
Verwenden Sie den folgenden Befehl, um die von Ihrer Cisco IOS-Version unterstützte EEM-Version zu überprüfen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

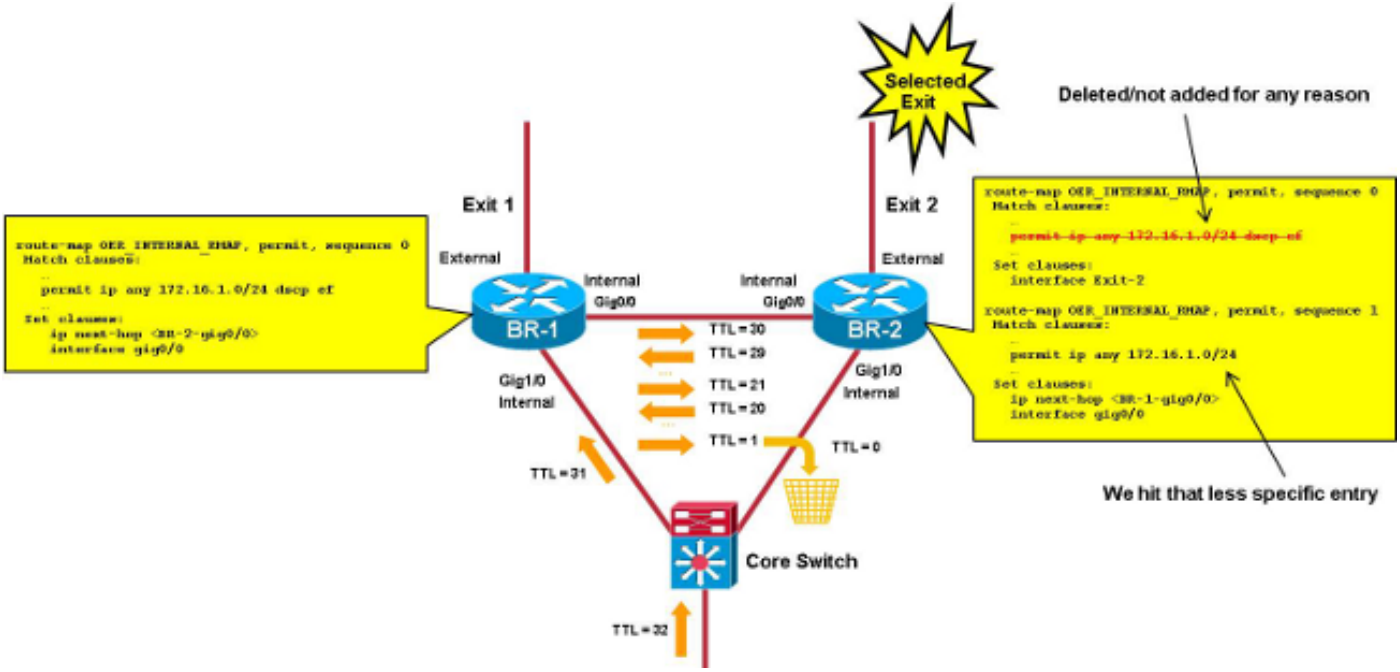
Hintergrundinformationen

Wenn der PfR eine Traffic Class (TC) steuert, erstellt er eine dynamische Route Map/Access Control List (ACL) für die BRs. Die Routenübersicht auf einem BR mit einem ausgewählten Exit verweist auf einen ausgewählten Exit, während eine Routenübersicht auf anderen BRs auf eine interne Schnittstelle zeigt (Next-Hop = ausgewählter BR).



Ein Problem tritt auf, wenn die dynamischen ACLs nicht richtig zwischen den verschiedenen BRs synchronisiert werden (z. B. aufgrund von Fehlern).

In diesem Bild liegt der Schwerpunkt auf der TC-Zuordnung aller IP-Pakete, die für 172.16.1.0/24 bestimmt sind, mit DSCP EF. In diesem Szenario wird der zugehörige ACL-Eintrag aus dem ausgewählten BR (BR-2) entfernt, jedoch nicht aus BR-1. Pakete dieses TC werden auf BR-2 mit dem Präfixeintrag aufgerufen, der allen IP-Paketen entspricht, die für 172.16.1.0/24 bestimmt sind. Der ausgewählte Ausgang für den Präfixeintrag ist **Exit-1**, sodass die zugehörige Route-Map/ACL auf BR-2 auf BR-1 verweist.



Die Pakete dieses TC-Loops laufen nun zwischen den BRs, bis die TTL (Time To Live) 0 erreicht.

Dieses Dokument enthält die EEM-Applets, die für Folgendes verwendet werden:

- Erkennung einer Weiterleitungsschleife zwischen BRs
- Sammeln relevanter Informationen und Löschen des PfR

Die Applets, die bei einer Kombination aus Master Controller (MC)/BR verwendet werden, sind wesentlich einfacher (wenn MC auf einem der BRs ausgeführt wird). Das Szenario mit dedizierten MCs wird ebenfalls behandelt.

EEM-Applet-Details

In diesem Abschnitt werden die für diesen Prozess verwendeten Zugriffslisten sowie Applet-Protokolldateien beschrieben.

Verwendete Zugriffslisten

Um Weiterleitungsschleifen zu erkennen, verwendet das Applet eine ACL, um Pakete mit niedriger TTL zuzuordnen.

> **Hinweis**: Die ACL-Zuordnung auf TTL wird auf Aggregation Service Routern (ASR) der Serie 1000 ab Version 3.7s (15.2(4)S unterstützt.

Es wird empfohlen, ACE-Abgleich bei zwei aufeinander folgenden, relativ niedrigen TTL-Werten (20 und 21) durchzuführen, um für jedes Paket, das zwischen BRs hin- und herschaltet, einen (und nur einen) Treffer zu erhalten. Der verwendete TTL-Wert sollte nicht zu niedrig sein, um häufige Treffer durch Traceroute-Pakete zu vermeiden.

```
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
```

Die ACL sollte auf der internen Schnittstelle platziert werden, die in der Befehlsausgabe für die **show pfr-Master-Topologie** gemeldet wird.

Der Quell-IP-Bereich (hier 10.116.48.0/20) sollte mit dem bzw. den internen Netzwerken übereinstimmen (Präfixe, die über interne Schnittstellen erreichbar sind).

> **Hinweis**: Wenn Sie interne Netzwerke in einem Access-List Entry (ACE) nicht zusammenfassen können, können Sie mehrere ACEs verwenden. Das Skript muss jedoch leicht geändert werden, um die Trefferanzahl für mehrere Zeilen zu überprüfen.

> **Hinweis**: Die **Auto-**Tunnel**-**Funktion muss deaktiviert werden (**keine automatischen Tunnel** im Master-PfR-Modus). Wenn die BRs nicht direkt verbunden sind, müssen manuelle GRE-Tunnel (Generic Routing Encapsulation) erstellt und die ACL auf der Tunnelschnittstelle platziert werden.

Um festzustellen, welcher Remote-Standort/TC von der Schleife betroffen ist, können Sie eine zweite ausgehende ACL an der Schnittstelle mit spezifischeren ACEs für jeden Remote-Standort/TC hinzufügen.

```
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
```

Die Ziel-IP-Adresse stimmt mit dem Subnetz der verschiedenen Remote-Standorte überein:

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

Sie können auch mehrere Zeilen pro Remote-Standort hinzufügen, wenn Sie den genauen TC identifizieren müssen, der von der Schleife betroffen ist.

Applet-Funktionen

Das Applet überprüft alle dreißig Sekunden die Anzahl der ACE-Übereinstimmungen auf der TTL in der ACL-Schleife. Je nach Ergebnis dieser Prüfungen kann das Applet folgende Aufgaben ausführen:

- Wenn die Anzahl der Treffer einen konfigurierten Grenzwert überschreitet (THRESHOLD_1), löscht das Applet die ACL-Anzahl und überprüft die Anzahl der Treffer in fünfzehn Sekunden.
- Wenn die Anzahl der Treffer nach den fünfzehn Sekunden einen zweiten Grenzwert

überschreitet (SCHWELLENWERT_2), es kann eine Schleife geben. Sie müssen eine Reihe von Ausgaben sammeln und den PfR löschen, um das Schleifenproblem zu beheben.
- Die zweiten Schwellenwerte werden als globale Variablen definiert, sodass sie ohne Neustart des Applets einfach angepasst werden können.
- Der optimale Wert für diese Schwellenwerte hängt hauptsächlich von der durchschnittlichen Paketrate pro TC ab.

Applet-Protokolldateien

Das Applet verwaltet eine Protokolldatei, die die Anzahl der Treffer (wenn die Anzahl größer als 0 ist) und alle Begegnungen mit temporären Schleifen (wenn THRESHOLD_1 überschritten wird, aber nicht THRESHOLD_2) oder einer realen Schleife (wenn sowohl THRESHOLD_1 als auch THRESHOLD_2 überschritten werden) erfasst.

Applets für MC/BR-Kombi und andere BR-Szenarien

Dies sind die einfachsten Szenarien, die in diesem Dokument beschrieben werden. Die Loop-Erkennung und PfR-Aufhebung erfolgen auf demselben Gerät, sodass keine EEM-Applet-Kommunikation für das Gerät eingegeben werden muss. Ein separates Applet wird auf einer MC/BR-Kombination und anderen BRs ausgeführt.

Applet auf MC/BR-Kombi

Diese Ausgabe zeigt wichtige Informationen für das Applet an, das auf der MC/BR-Kombi verwendet wird. Hier einige wichtige Hinweise für diese spezifische Ausgabe:

- Der für **THRESHOLD_1** angezeigte Wert ist 1000, und die für **THRESHOLD_2** angezeigten Werte sind 500. Dies impliziert, dass das Applet gestartet wird, wenn die Rate des von der Schleife betroffenen TC über 1000/30 (33 pps) liegt.
- Die **DISK**-Variable gibt an, wo die Protokoll- und Ausgabedateien gepeilt werden (hier im Bootflash angezeigt).
- Der Zeitstempel der Einträge in der Protokolldatei leitet sich von der Ausgabe des Befehls **show clock** ab. Die Zeichen in der Mitte (hier als "est" angezeigt) hängen von der Zeitzone ab und müssen angepasst werden (siehe **Aktion 240**).
- Die Ausgaben, die im Falle einer Schleife erfasst werden müssen, werden in der **script-output-xxxxxx-**Datei in bootflash gepeilt, wobei "xxxxxx" die Anzahl der Sekunden seit 1970 ist (um eindeutige Dateinamen für jedes Schleifenereignis zu erstellen).
- Die gesammelten Befehle werden in den **Aktionen 330, 340, 350 und 360** aufgelistet. Einige weitere/verschiedene Befehle können hinzugefügt werden.

```
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
```

Applet für andere BRs

In diesem Abschnitt wird das Applet beschrieben, das für andere BRs verwendet wird. Hier einige wichtige Hinweise für diese spezifische Ausgabe:

- Das Applet wird alle zwanzig Sekunden ausgeführt, während das Skript auf einer MC/BR-Kombination alle dreißig Sekunden ausgeführt wird. Dadurch wird sichergestellt, dass das Applet auf dem BR gestartet wird, bevor der PfR über das Applet gelöscht wird, das auf dem MC/BR ausgeführt wird.
- Es wird ein eindeutiger Grenzwert verwendet, sodass keine Fehlerpositiv zu vermeiden ist.
- Der für den **THRESHOLD** angezeigte Wert beträgt 700 und sollte entsprechend dem Wert

THRESHOLD_1 im MC/BR-Applet festgelegt werden.
- Die Applet-Protokolldatei wird in die Datei script-logs.txt in flash0 übertragen. Dies kann in Aktion 170 und der DISK-Variable geändert werden.
- Der Zeitstempel der Einträge in der Protokolldatei leitet sich von der Ausgabe des Befehls show clock ab. Die Zeichen in der Mitte (hier als "est" angezeigt) hängen von der Zeitzone ab und müssen angepasst werden (siehe Aktion 190).
- Die Ausgaben, die im Falle einer Schleife erfasst werden müssen, werden in die Datei script-output-xxxxxxx getippt, wobei "xxxxxx" für die Anzahl der Sekunden seit 1970 steht (für die Erstellung eindeutiger Dateinamen für jedes Schleifenereignis).
- Die gesammelten Befehle werden in Aktion 230 und Aktion 240 aufgelistet. Einige weitere/verschiedene Befehle können hinzugefügt werden.

```
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
```

Applets für dediziertes MC-Szenario

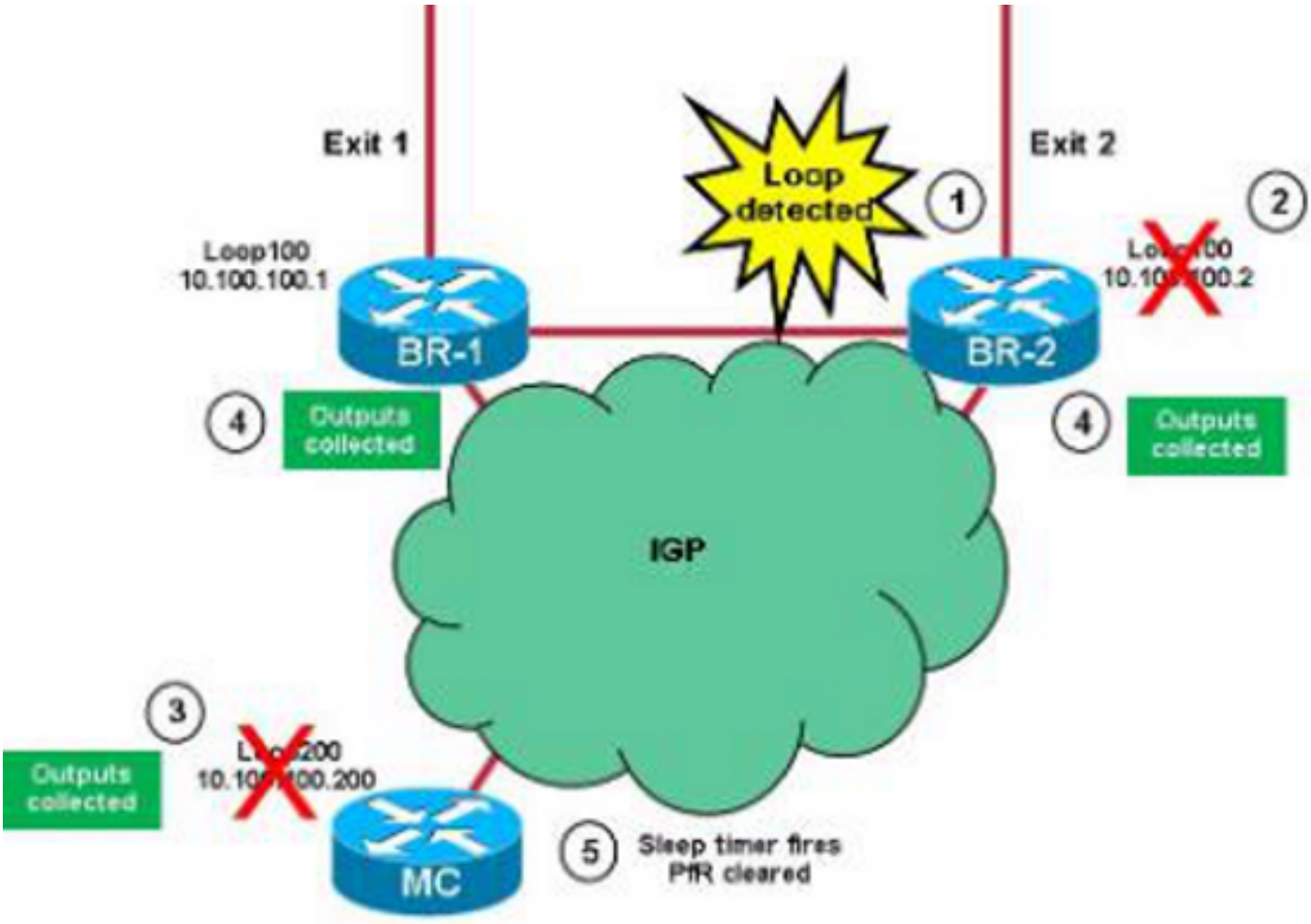
Die Loop-Erkennung und PfR-Clearing-/Statistikauflistung wird auf verschiedenen Geräten ausgeführt, die über EEM-Applet-Kommunikation zwischen Geräten verfügen müssen. Die Kommunikation zwischen den Geräten erfolgt auf unterschiedliche Weise. Dieses Dokument beschreibt die Gerätekommunikation über verfolgte Objekte, um die Erreichbarkeit von dedizierten Loopbacks zu überprüfen, die im IGP angekündigt werden. Wenn ein Ereignis erkannt wird, wird das Loopback geschlossen, wodurch Applets auf Remote-Geräten gestartet werden können, wenn das verfolgte Objekt offline geht. Sie können verschiedene Loopbacks verwenden, wenn andere Informationen ausgetauscht werden müssen.

Applet-Kommunikation

Diese Applets und Kommunikationsmethoden werden verwendet:

Applet-Name	Wo ?	Was?	Trigger ?	Kommunikation ?
LOOP-BR	BRs	Überprüfen Sie die ACL-Zugriffszahlen, um Schleifen zu erkennen.	Regelmäßig	shut Loop100
LOOP-MC	MC	- PfR-Informationen sammeln - Löscht PfR	Track Reachability Loop100	shut Loop200
SAMMLUNG BR	BRs	Sammeln von Informationen	Track Reachability Loop200	Keine

Das folgende Bild veranschaulicht dies:



Dies ist der Prozess, der von den Applets verwendet wird:

1. Eine Schleife wird vom **LOOP-BR-**Applet auf den BRs erkannt. Es wird davon ausgegangen, dass die Schleife zuerst auf BR-2 erkannt wird.

2. Das Applet schließt **Loop100** auf BR-2, und die Informationen werden im Interior Gateway Protocol (IGP) angekündigt.
3. Das verfolgte Objekt für **Loop100** von BR-2 wird auf dem MC offline geschaltet, und das **LOOP-MC-**Applet wird gestartet. PfR-Master-Ausgaben werden erfasst, und **Loopback 200** auf dem MC wird heruntergefahren. Die Informationen werden über IGP bekannt gegeben. Ein Zehn-Sekunden-Ruhemodus wird gestartet.
4. Das verfolgte Objekt für **Loop200** auf dem MC wird auf beiden BRs offline geschaltet. Dies löst das **COLLECT-BR-**Applet aus, das BR-spezifische Informationen sammelt.
5. Der Schlaf-Timer (Schritt 3) wird gestartet, und der MC löscht den PfR.

Hinweis: Wenn BR-1 die Schleife erkennt, bevor der PfR gelöscht wird, wird das verfolgte Objekt, das offline geht, auf MC ignoriert (das **LOOP-MC-**Applet wird einmal pro Minute ausgeführt).

Erstellen von Track-Objekten und Loopbacks

In diesem Abschnitt wird beschrieben, wie Sie Loopbacks erstellen (sicherstellen, dass die IPs auf dem IGP angekündigt werden) und Objekte verfolgen.

Track-Objekte

Beim Erstellen von Verfolgungsobjekten sollten Sie folgende wichtige Punkte berücksichtigen:

- Auf BRs wird ein einzelnes Spur-Objekt benötigt, das zum Nachverfolgen von **Loopback200** auf MC verwendet wird (dies löst die Datenerfassung aus).
- Auf dem MC werden mehrere Verfolgungsobjekte benötigt: Die Tracks 1 und 2 werden zum Nachverfolgen von **Loopback100** auf BR-1 bzw. BR-2 verwendet.Die Spuren 11 und 12 werden verwendet, um die Verbindungen zwischen BR-1 und BR-2 zu verfolgen (vermeidet die PfR-Entfernung, wenn Verbindungsprobleme zwischen BRs auftreten).Track 20 verfolgt den logischen UND zwischen den Spuren 11 und 12. Diese Funktion wird verwendet, um zu überprüfen, ob MC für alle BRs erreichbar ist.
- Der **IP-Route-**Wert für **den Track-Timer** wird auf eine Sekunde festgelegt, um die Erkennung von Erreichbarkeitsproblemen zu beschleunigen (der Standardwert ist 15 Sekunden).

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- und MC-Loopbacks

LOOP-BR

In diesem Abschnitt wird beschrieben, wie Sie Loopbacks auf den BRs erstellen. Hier einige wichtige Punkte:

- Der Wert **THRESHOLD_1** ist 1000 und der Wert **THRESHOLD_2** 500. Dies impliziert, dass das Applet gestartet wird, wenn die Rate der von der Schleife betroffenen TCs über 1000/30 (33 p/s) liegt.
- Die Applet-Protokolldatei wird in die Datei **script-detect-logs.txt** in bootflash übertragen. Dies wird in **Aktion 210** und mit der **DISK-**Variable geändert.
- Der Timestamp der Einträge in der Protokolldatei wird von der **sh clock-**Ausgabe abgeleitet. Die Zeichen in der Mitte (als 'est' angezeigt) hängen von der Zeitzone ab und müssen angepasst werden (**Aktion 240**).
- Nachdem Sie den **Loopback100** geschlossen haben, um das MC zu benachrichtigen, warten Sie fünf Sekunden (um sicherzustellen, dass das IGP die Zeit zur Weitergabe der Informationen hat), und öffnen Sie die Informationen erneut (**Aktion 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
```

LOOP-MC

In diesem Abschnitt wird beschrieben, wie Loopbacks auf dem MC erstellt werden. Hier einige wichtige Punkte:

- Der Ratenlimitierungswert hängt davon ab, wie oft das Applet mit einem Ratenlimit von 60 ausgeführt wird (Skript wird einmal pro Minute max. ausgeführt). Dies wird verwendet, um die doppelte PfR-Clearance zu vermeiden, wenn die gleiche Schleife von beiden BRs erkannt wird.
- In Action 130 warten Sie zwei Sekunden, bevor Sie die Erreichbarkeit aller BRs überprüfen. Dies dient der Vermeidung von Fehlalarmen, die durch Verbindungsprobleme zwischen dem MC und den BRs verursacht werden.
- In Action 240 warten Sie zehn Sekunden, nachdem Sie Loopback200 heruntergefahren haben, bevor Sie den PfR löschen. Damit soll sichergestellt werden, dass die BR Zeit haben, die Daten zu erfassen.

```
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
```

SAMMLUNG BR

In diesem Abschnitt wird beschrieben, wie der BR erfasst wird. Das Applet wird gestartet, wenn ein BR die Erreichbarkeit von **Loopback200** (10.100.100.200) auf MC verliert. Die Befehle, die zum Erfassen verwendet werden, werden in den **Aktionen 120**, **130** und **140** aufgelistet.

```
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

Hier ist das Syslog auf dem MC, wenn eine Schleife erkannt wird:

```
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#
```

Hinweis: Diese Applets können mit drei oder mehr BRs mit einigen Einstellungen verwendet werden.