Applet EEM utilizzate per rilevare e cancellare i loop di inoltro PfR

Sommario

Introduzione

In questo documento vengono descritte le applet Embedded Event Manager (EEM) utilizzate nelle reti in cui Performance Routing (PfR) ottimizza il traffico attraverso più Border Relay (BR). Vengono inoltre osservati alcuni loop di inoltro. Le applet vengono utilizzate per raccogliere dati quando viene osservato un loop e per ridurre l'impatto di un loop di inoltro.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato un software Cisco IOS® che supporta EEM versione 4.0.

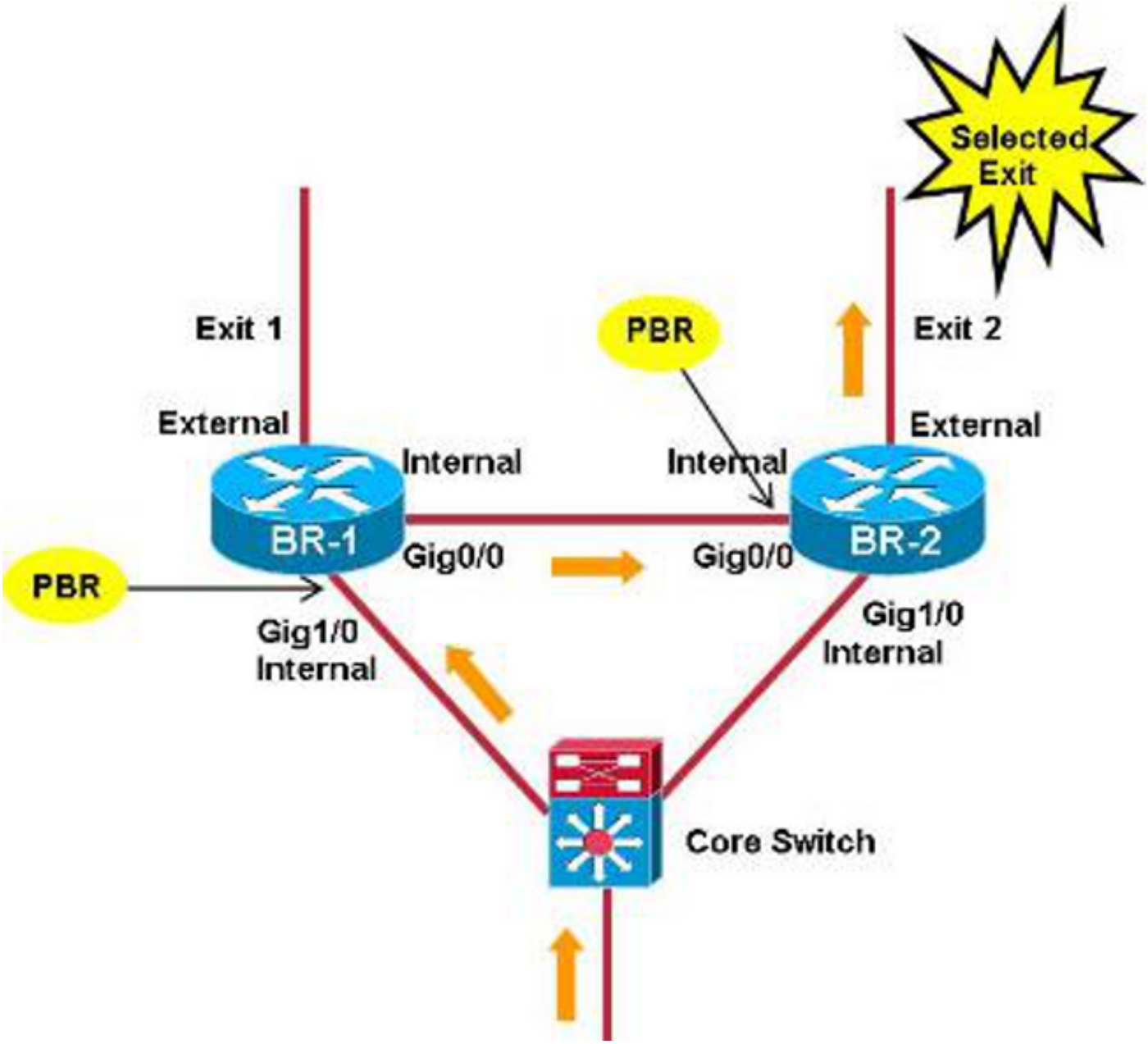
Per controllare la versione EEM supportata dalla versione Cisco IOS in uso, utilizzare questo comando:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

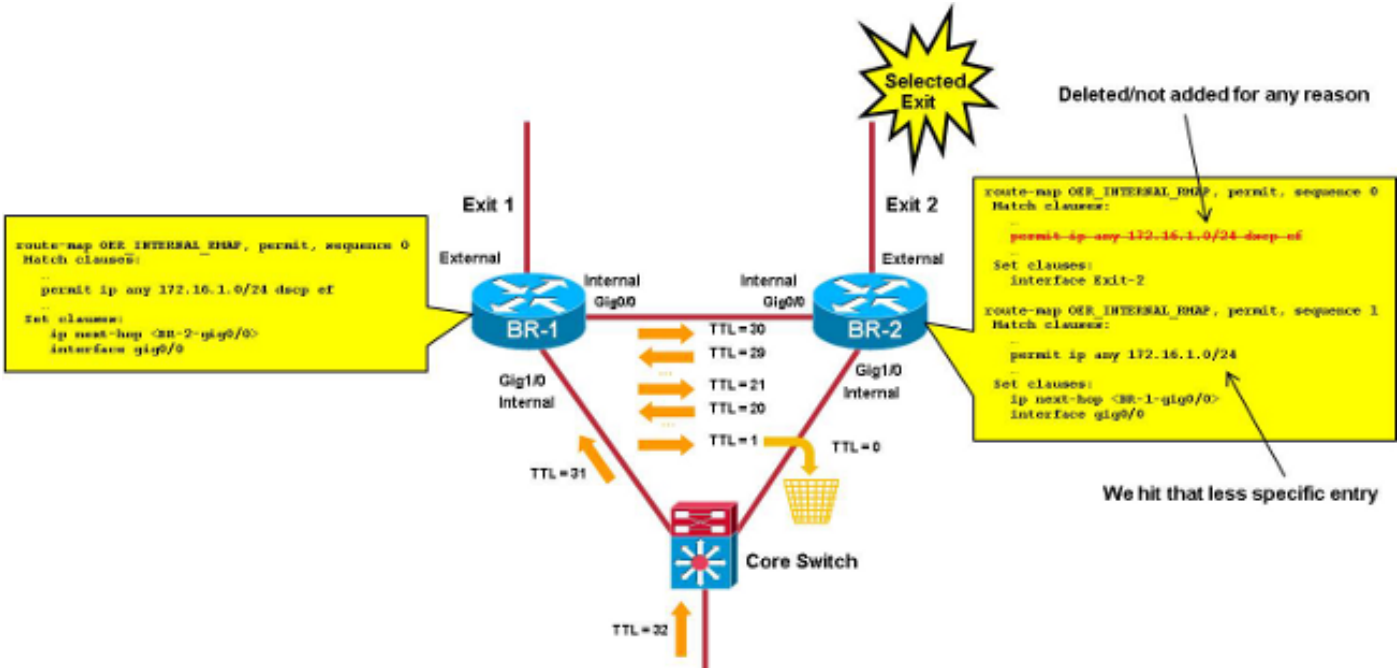
Premesse

Quando PfR controlla una classe di traffico (TC), crea una mappa di percorso dinamica/un elenco di controllo di accesso (ACL, Access Control List) sui BR. La mappa del percorso su una BR con un punto di uscita selezionato a un'uscita selezionata, mentre una mappa del percorso su altre BR punta a un'interfaccia interna (hop successivo = BR selezionato).



Il problema si verifica quando gli ACL dinamici non sono sincronizzati correttamente tra i diversi BR (ad esempio a causa di bug).

In questa immagine, l'attenzione è focalizzata sulla corrispondenza tra TC e qualsiasi pacchetto IP destinato a 172.16.1.0/24 con DSCP EF. In questo scenario, la voce ACL correlata viene rimossa dal BR selezionato (BR-2), ma non dal BR-1. Pacchetti di tale risposta TC al BR-2 con la voce di prefisso che corrisponde a tutti i pacchetti IP destinati a 172.16.1.0/24. L'uscita selezionata per la voce di prefisso è **Exit-1**, quindi il percorso-map/ACL correlato su BR-2 punta a BR-1.



I pacchetti di quel TC passano ora in loop tra i BR fino a quando il valore TTL (Time To Live) non raggiunge 0.

Questo documento fornisce le applet EEM necessarie per:

- Rileva un loop di inoltro tra barre
- Raccogliere le informazioni pertinenti e cancellare il

Le applet utilizzate nel caso di un controller master (MC)/BR combinato sono molto più semplici (quando MC viene eseguito su uno dei BR). Viene inoltre trattato lo scenario con MC dedicati.

Dettagli applet EEM

In questa sezione vengono descritti gli elenchi degli accessi utilizzati per questo processo, nonché i file di log delle applet.

Elenchi di accesso utilizzati

Per rilevare i loop di inoltro, l'applet si basa su un ACL per far corrispondere i pacchetti con un valore TTL basso.

> **Nota:** La corrispondenza ACL su TTL è supportata su Aggregation Service Router (ASR) serie 1000 versione 3.7 (15.2(4)S) e successive.

Si consiglia di utilizzare la corrispondenza ACE su due valori TTL consecutivi, relativamente bassi (20 e 21) per ottenere una (e una sola) corrispondenza per ciascun pacchetto che esegue il loop tra i BR. Il valore TTL utilizzato non deve essere troppo basso per evitare riscontri frequenti da pacchetti traceroute.

```
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
```

L'ACL deve essere posizionato sull'interfaccia interna specificata nell'output del comando **show pfr master border topology**.

L'intervallo IP di origine (qui 10.116.48.0/20) deve corrispondere alla rete o alle reti interne (prefissi raggiungibili tramite interfacce interne).

> **Nota:** Se non è possibile riepilogare le reti interne in una voce dell'elenco degli accessi (ACE, Access-list Entry), è possibile utilizzare più ACE; tuttavia, lo script deve essere leggermente modificato per controllare il numero di passaggi su più righe.

> **Nota:** La funzione **auto-**tunnel deve essere disattivata (**nessun tunnel automatico in modalità** master PfR). Se i BR non sono collegati direttamente, è necessario creare manualmente i tunnel GRE (Generic Routing Encapsulation) e posizionare l'ACL sull'interfaccia del tunnel.

Per identificare il sito remoto/centro di traduzione interessato dal loop, è possibile aggiungere un secondo ACL in uscita sull'interfaccia, con ACE più specifici per ciascun sito remoto/centro di traduzione.

```
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
```

L'indirizzo IP di destinazione corrisponde alla subnet nei diversi siti remoti:

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

Èinoltre possibile aggiungere più linee per sito remoto se è necessario identificare il TC esatto interessato dal loop.

Compiti applet

L'applet controlla gli hitcount della corrispondenza ACE sul valore TTL nel ciclo ACL ogni trenta secondi. In base all'esito di questi controlli, l'applet potrebbe eseguire le attività seguenti:

- Se gli hitcount superano una soglia configurata (THRESHOLD_1), l'applet cancella il conteggio ACL e lo ricontrolla in quindici secondi.
- Dopo i quindici secondi, se gli hitcount superano una seconda soglia (`SOGLIA_2`), potrebbe esserci un loop. Per risolvere il problema del loop, dovete raccogliere un set di output e cancellare il PfR.

- Le seconde soglie sono definite come variabili globali, in modo che siano facilmente sintonizzate senza dover riavviare l'applet.
- Il valore ottimale per queste soglie dipende principalmente dalla velocità media dei pacchetti per TC.

File di log applet

L'applet mantiene un file di log che tiene traccia del numero di hitcount (quando il conteggio è maggiore di 0) e di eventuali rilevamenti di loop temporanei (quando SOGLIA_1 è superato ma non SOGLIA_2) o di un loop reale (quando vengono superati sia SOGLIA_1 che SOGLIA_2).

Applet per MC/BR Combo e altri scenari BR

Questi sono gli scenari più semplici descritti nel presente documento. Il rilevamento loop e la cancellazione PfR vengono eseguiti sullo stesso dispositivo, quindi non è necessario accedere alla comunicazione EEM applet del dispositivo. Un'applet separata viene eseguita su una casella combinata MC/BR e su altre barre.

Applet su unità combo MC/BR

Questo output visualizza informazioni importanti per l'applet utilizzata nella combinazione MC/BR. Di seguito sono riportate alcune note importanti per questo output specifico:

- Il valore visualizzato per **THRESHOLD_1** è 1000 e i valori visualizzati per **THRESHOLD_2** sono 500. Ciò implica che l'applet viene avviata se la frequenza del TC interessato dal ciclo è superiore a 1000/30 (33 punti per pollice).
- La variabile **DISK** identifica la posizione in cui vengono inseriti i file di log e di output (mostrata qui in bootflash).
- L'indicatore orario delle voci nel file di log deriva dall'output del comando **show clock**. I caratteri al centro (qui "set") dipendono dal fuso orario e devono essere regolati (vedere **azione 240**).
- Gli output che devono essere raccolti in caso di loop vengono inseriti nel file **script-output-xxxxxx** in bootflash, dove "xxxxxx" è il numero di secondi dal 1970 (utilizzato per creare nomi di file univoci per ogni occorrenza di loop).
- I comandi raccolti sono elencati nelle **azioni 330, 340, 350 e 360**. È possibile aggiungere altri/diversi comandi.

```
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 per altri BR

In questa sezione viene descritta l'applet utilizzata per altri BR. Di seguito sono riportate alcune note importanti per questo output specifico:

- L'applet viene eseguita ogni venti secondi mentre lo script di una combinazione MC/BR viene eseguito ogni trenta secondi. In questo modo, l'applet sulla BR viene avviata prima che il PfR venga cancellato tramite l'applet in esecuzione sulla MC/BR.
- Poiché viene utilizzata una soglia univoca, non è necessario evitare errori positivi.
- Il valore visualizzato per **THRESHOLD** è 700 e deve essere impostato in base al valore **THRESHOLD_1** nell'applet MC/BR.
- Il file di log dell'applet viene inserito nel file **script-logs.txt** in **flash0**. È possibile modificare questa impostazione nell'**azione 170** e nella variabile **DISK**.
- L'indicatore orario delle voci nel file di log deriva dall'output del comando **show clock**. I

caratteri al centro (qui "set") dipendono dal fuso orario e devono essere regolati (vedere **azione 190**).
- Gli output che devono essere raccolti in caso di loop vengono inseriti nel file **script-output-xxxxxxx**, dove "xxxxxx" è il numero di secondi dal 1970 (utilizzato per creare nomi di file univoci per ogni occorrenza di loop).
- I comandi raccolti sono elencati nelle **azioni 230** e **240**. È possibile aggiungere altri/diversi comandi.

```
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
```

Applet per uno scenario MC dedicato

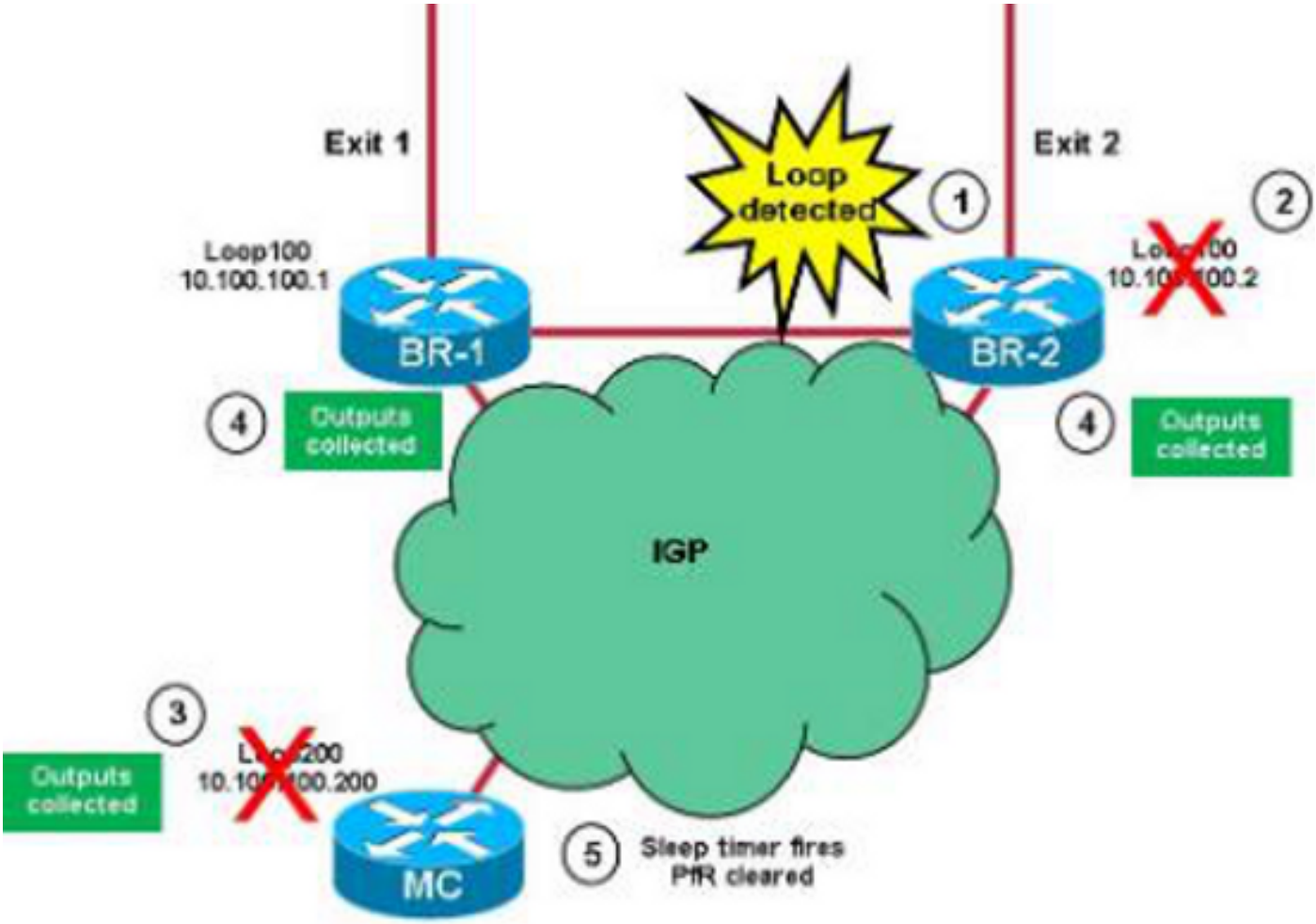
Il rilevamento loop e la raccolta di dati PfR di cancellazione/stato vengono completati su dispositivi diversi che devono disporre di una comunicazione EEM applet tra dispositivi. La comunicazione tra i dispositivi avviene in modi diversi. Questo documento descrive la comunicazione del dispositivo tramite oggetti tracciati per verificare la raggiungibilità dei loopback dedicati pubblicizzati in IGP. Quando viene rilevato un evento, il loopback viene arrestato, consentendo l'avvio delle applet su dispositivi remoti quando l'oggetto rilevato passa alla modalità offline. È possibile utilizzare loopback diversi se è necessario scambiare informazioni diverse.

Comunicazione applet

Vengono utilizzati i seguenti applet e metodi di comunicazione:

Nome applet	Dove?	Cosa?	Fattore scatenante?	Comunicazione?
LOOP-BR	BR	Per rilevare i loop, controllare gli hitcount ACL	Periodico	chiusura di Loop100
LOOP-MC	MC	- Raccolta dei dati PfR - Cancella PfR	Traccia raggiungibilità Loop100	chiusura di Loop200
COLLECT-BR	BR	Raccogli informazioni	Track reachability Loop200	nessuna

Di seguito è riportata un'immagine che illustra quanto segue:



Questo è il processo utilizzato dagli applet:

1. Viene rilevato un loop dall'applet **LOOP-BR** sui BR. Si presume che il loop venga rilevato prima su BR-2.
2. L'applet chiude **Loop100** su BR-2 e le informazioni vengono pubblicizzate sul protocollo IGP (Interior Gateway Protocol).
3. L'oggetto tracciato per **Loop100** di BR-2 viene disconnesso nell'MC e viene avviata l'applet **LOOP-MC**. Gli output master PfR vengono raccolti e il **loopback 200** sull'MC viene arrestato. Le informazioni vengono pubblicizzate su IGP. Inizia un timer di sospensione di dieci secondi.

4. L'oggetto tracciato per **Loop200** sull'MC viene disconnesso su entrambi i BR. In questo modo viene attivata l'applet **COLLECT-BR** che raccoglie informazioni specifiche di BR.
5. Il timer per lo spegnimento ritardato (punto 3) si avvia e MC cancella il PfR.

Nota: Se BR-1 rileva il loop prima che il PfR venga cancellato, l'oggetto tracciato disconnesso viene ignorato in MC (l'applet **LOOP-MC** viene eseguita una volta al minuto).

Creazione di oggetti traccia e loopback

Questa sezione descrive come creare loopback (assicurarsi che gli IP siano annunciati sull'IGP) e tenere traccia degli oggetti.

Traccia oggetti

Di seguito sono riportati alcuni punti importanti da tenere presenti quando create gli oggetti traccia:

- Sui BR è necessario un singolo oggetto traccia, che viene utilizzato per tenere traccia di **loopback200** su MC (attiva la raccolta dei dati).
- Su MC sono necessari diversi oggetti traccia: I brani 1 e 2 vengono utilizzati per tenere traccia di **loopback100** su BR-1 e BR-2, rispettivamente.I brani 11 e 12 vengono utilizzati per tenere traccia della connettività tra BR-1 e BR-2, rispettivamente (evita la cancellazione del PfR in caso di problemi di connettività tra BR).Il brano 20 tiene traccia dell'AND logico tra i brani 11 e 12. Viene utilizzato per verificare che MC sia raggiungibile da tutte le BR.
- Il valore **track timer ip route** è impostato su un secondo per accelerare il rilevamento dei problemi di raggiungibilità (il valore predefinito è 15 secondi).

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
```

Loopback BR e MC

LOOP-BR

In questa sezione viene descritto come creare loopback nelle schede di rete. Ecco alcune note importanti da tenere a mente:

- Il valore di **THRESHOLD_1** è 1000 e il valore di **THRESHOLD_2** è 500. Ciò implica che l'applet viene avviata se la frequenza dei TC interessati dal loop è superiore a 1000/30 (33 p/s).
- Il file di log dell'applet viene inserito nel file **script-detect-logs.txt** in bootflash. Questa condizione viene modificata nell'**azione 210** e con la variabile **DISK**.
- L'indicatore orario delle voci nel file di log deriva dall'output **dell'orologio**. I caratteri al centro (visualizzati come 'set') dipendono dal fuso orario e richiedono una regolazione (**azione 240**).
- Dopo aver chiuso il **loopback100** per inviare una notifica a MC, attendere cinque secondi (per assicurarsi che IGP abbia il tempo di propagare le informazioni) e riaprirlo (**azione 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

Questa sezione descrive come creare loopback sull'MC. Ecco alcune note importanti da tenere a mente:

- Il valore di ratelimit dipende dalla frequenza con cui l'applet viene eseguita con un valore di ratelimit pari a 60 (lo script viene eseguito una volta al minuto al massimo). Questa opzione viene utilizzata per evitare che il PfR venga cancellato due volte quando lo stesso loop viene rilevato da entrambi i BR.
- Nell'**azione 130**, attendere due secondi prima di verificare la raggiungibilità di tutti i BR. Ciò al fine di evitare un falso positivo causato da problemi di connettività tra la console centrale e le schede di rete.
- Nell'**azione 240**, attendere dieci secondi dopo aver chiuso **Loopback200**, prima di cancellare il PfR. Ciò al fine di garantire che i BR abbiano il tempo di raccogliere i dati.

```
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

In questa sezione viene descritto come raccogliere la BR. L'applet viene avviata quando un BR perde la raggiungibilità a **Loopback200** (10.100.100.200) su MC. I comandi utilizzati per la raccolta sono elencati nelle **azioni 120**, **130** e **140**.

```
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

Di seguito è riportato il syslog su MC quando viene rilevato un loop:

```
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#
```

Nota: Queste applet possono essere utilizzate con tre o più BR con una certa regolazione.