Command-line protocol NetFlow

router(config-if)#ip route-cache flow-sampled

Il comando consente di abilitare il netflow su una specifica interfaccia nella modalità "compionato". Il netflow abilitato nella modalità "campionato" permette di diminuire, come illustrato nel paragrafo stima del traffico netflow, la quantità di traffico esportato.

router(config)#ip flow-sampling-mode packet-interval <value>

Il comando consente di configurare l'intervallo di campionamento. Il valore di default un campione ogni 4 miliardi. L'intervallo di campionamento configurabile è compreso 10 e 16382.

router(config)#ip flow-export version 5

Il comando consente di esportare, verso il collettore NFC, i flussi contenuti nella cache nel formato versione 5

router(config)# ip flow-export source <interface>

Il comando consente di configurare l'indirizzo sorgente dei dati esportati verso il collettore NFC.

router(config)#ip flow-cache timeout inactive <seconds>

Il comando consente di configurare l'intervallo di tempo oltre il quale un flusso inattivo memorizzato nella cache è espulso. Il valore di default è 15 secondi. Il valore configurabile è compreso nell'intervallo fra 10 e 600 secondi.

router(config)#ip flow-cache timeout active <minutes>

Il comando consente di configurare l'intervallo di tempo oltre il quale un flusso attivo memorizzato nella cache è espulso. Il valore di default è 30 minuti. Il valore configurabile è compreso nell'intervallo fra 1 e 60 minuti.

router(config)#ip flow-export destination <ip-address> <udp port>

Il comando abilita l'export delle informazioni contenute nella netflow cache verso un collettore NFC.

E' consigliato utilizzare i seguenti valori per le politiche di gestione dei flussi:

router(config)# ip flow-cache timeout inactive 15 (*valore di default)*

r**outer(config)# ip flow-cache timeout active 1**

Per quanto riguarda la scelta dell'intervallo di campionamento è consigliato utilizzare il valore 10.

La stima del traffico netflow esportato, illustrata nel prossimo paragrafo, mostra come il valore 10 è un buon compromesso tra quantità di traffico generato ed l'accuratezza della ricostruzione delle caratteristiche proprie di ciascun flusso.

Numero di flussi per secondo è pari a:

Numero di pacchetti ricevuti / Numero di pacchetti medio per flusso

- Il numero di pacchetti medio per flusso è circa 15

Il traffico esportato (bytes/sec) relativo è pari a:

(Numero di flussi per secondo) / (Numero di flussi esportati per trama UDP * fattore di campionamento) * **Lunghezza trama UDP**

- Nella versione netflow 5 è possibile esportare fino a 30 flussi in una singola trama UDP di lunghezza pari approssimativamente a 1500 bytes

Nell'ipotesi di attivare il netflow sampled (fattore di campionamento pari a 10) su un interfaccia 1 GBE la stima del traffico esportato è la seguente:

Numero di pacchetti ricevuti sull'interfaccia 1 GBE del router:

143032 pacchetti/sec

Numero di flussi per secondo è pari a:

Numero di pacchetti ricevuti / Numero di pacchetti medio per flusso

143032 / 15 = 9535 flussi/sec

Il traffico esportato (bit/sec) relativo è pari a:

(Numero di flussi per secondo) * **Lunghezza trama UDP * 8/ (Numero di flussi esportati per trama UDP * fattore di campionamento)**

9535 * 1500 * 8 / (15 * 10) = ~ 762 Kbit/sec

Nell'ipotesi di attivare il netflow sampled (fattore di campionamento pari a 10) su una interfaccia OC-48 la stima del traffico esportato è la seguente:

Numero di pacchetti ricevuti sull'interfaccia OC-48 del router:

137484* pacchetti/sec

Numero di flussi per secondo è pari a:

Numero di pacchetti ricevuti / Numero di pacchetti medio per flusso

137484 / 15 = 9165 flussi/sec

Il traffico esportato (bit/sec) relativo è pari a:

(Numero di flussi per secondo) * **Lunghezza trama UDP * 8/ (Numero di flussi esportati per trama UDP * fattore di campionamento)**

9165 * 1500 * 8 / (15 * 10) = ~ 733 Kbit/sec

Nell'ipotesi di attivare il netflow sampled (fattore di campionamento pari a 100) su un interfaccia 1 GBE la stima del traffico esportato è la seguente:

~ 76 Kbit/sec

Nell'ipotesi di attivare il netflow sampled (fattore di campionamento pari a 100) su una interfaccia OC-48 la stima del traffico esportato è la seguente:

~ 73 Kbit/sec

- In generale l'attivazione del netflow provoca un aumento del grado di utilizzazione della CPU*.
- In particolare maggiore è il numero di flussi che popola la "netflow cache" più alto diventa l'utilizzo percentuale CPU*.
- A parità di condizioni l'attivazione della versione campionata del netflow determina un generale e consistente miglioramento del grado di utilizzazione della CPU*. All'aumentare del fattore di campionamento migliorano le prestazioni della CPU* tuttavia risulta meno accurata la ricostruzione dei dati.
- L'attivazione della funzionalità "netflow cache aggregation" con la versione 8 riduce da la quantità di traffico esportato verso il collettore e migliora la scalabilità della soluzione senza peraltro determinare un significativo peggioramento del grado di utilizzazione della CPU*.

** Line Card CPU*

Per esaminare il contenuto e le caratteristiche della netflow cache

router#show ip cache flow

Per verificare i parametri di campionamento

router#show ip flow sampling

Per verificare i dati relativi alla quantità di traffico esportato

Router#show ip flow export

Per verificare se il netflow è abilitato a livello di interfaccia

Router#show ip interface

- Per verificare la percentuale di utilizzazione della CPU della line card legata all'attivazione del netflow

Router#execute-on slot [*slot* #] show proc cpu