

Progetto Gestione di reti

Marco Pierotti

Questo progetto è incentrato sull'analisi del traffico riguardo i protocolli presenti su una rete.

Lo scopo finale è quello di creare un grafico , ovvero una pagina html, che rappresenti la quantità di dati scambiati in base all'ora considerata.

Per raggiungere lo scopo è stato necessario monitorare per 10 ore il traffico della rete domestica, ciò è stato possibile con ntopng, grazie al quale è possibile vedere dettagliatamente l'evoluzione del traffico in base ai protocolli presenti, i flows, i pacchetti/bit scambiati.

In particolare questo tool permette di scaricare le informazioni in formato .json grazie ad una particolare funzionalità che registra su file i dati ogni tot secondi/MB/pacchetti scambiati.

Per cui alla fine delle 10 ore di monitoraggio erano stati creati 10 file .json (traffico[9-18].json) con i dati necessari per la creazione del grafico. Queste informazioni però erano sparse in più file ed era necessario concentrarle per permettere alla pagina html di estrapolare per poterle utilizzare per la modellazione del diagramma.

Ho quindi creato uno script bash che permette di dividere le informazioni presenti in ogni file di input (i 10 file .json) e di ricomporle in un unico file di output (traffico_tot.json).

In particolare ho conservato il numero dei pacchetti scambiati da ogni protocollo e il nome del protocollo creando un campo nel file json finale per ogni ora monitorata.

Per informazioni aggiuntive sullo script bash si rimanda al file sorgente in cui è stato fatto ampio uso di commenti per chiarire passo passo ogni passaggio.

Per generare il file .json finale basta eseguire da terminale il comando `./json_tot traffico*.json` al termine del quale sarà presente il file necessario alla creazione del grafico.

Traffico_dati.html è la pagina in cui è mostrato il risultato.

Come si può vedere i cerchi in corrispondenza dell'ora e del protocollo stanno ad indicare la quantità di pacchetti scambiati in quell'ora, il raggio del cerchio corrispondente è stato modellato in base alla percentuale di traffico del protocollo nelle 10 ore per cui sarà più grande in presenza di picchi di scambio pacchetti e sarà più piccolo altrove.

Passando sopra il nome del protocollo i cerchi corrispondenti spariscono lasciando il posto al numero esatto di pacchetti scambiati, permettendo all'utente di monitorare con esattezza la quantità di traffico.