Use of flow data for traffic analysis and network performance characterization.

Authors:

Andrey Bobyshev (Fermilab), Phil DeMar (Fermilab), Vyto Grigaliunas (Fermilab), Maxim Grigoriev (Fermilab)

Abstract:

At Fermilab, there is a long history of utilizing network flow data collected from site routers for various analyses, including network performance characterization, anomalous traffic detection, investigation of computer security incidents, network traffic statistics and others. Fermilab’s flow analysis model is currently built as a distributed system that collects flow data from the site network border routers, as well as from internal core routers & aggregation switches. The flow data is complete, not sampled, with a daily volume of approximately 10GBytes. Despite the high volume of collected information, large scale analysis is conducted in near real-time to satisfy demands of the user community for timely availability of the analyzed data.

In this paper, we present Fermilab's Netflow Collection and Analysis system, as well as tools developed to analyze the flow data. Tools presented will include traffic characterization and network performance estimation for the US-CMS Tier1 Center, verification of path symmetry for network traffic re-routed over alternate path circuits, and profiling of traffic patterns for individual systems to characterize their typical behavior and enable identification of anomalous behavior.