This study examines how a private WAN, used by Google to link its data servers throughout the world, was implemented and valued. The B4 features specifications that include high bandwidth needs, scalability, and total network management. In this work, the authors demonstrate their deployment of Google's WAN B4 utilizing SDN and OpenFlow. In reality, they used two WANs to complete the task rather than just one, the user-facing network for internet traffic exchange and B4 for maintaining communication between data centers. They choose SDN over conventional WAN principles because they sought fault tolerance, cost-effectiveness, and control. Large buffers and routing tables are typically required for WAN, which raises the cost. Instead, they discovered that the majority of switch faults are caused by software, not hardware, and that software fault tolerance may be improved simply by removing software functions from the switch. When they sought to grow beyond what they could handle, they even created their chips. A routing application policy (RAP) was built to integrate openflow with the current router. Each RIB will be converted into two tables by the RAP. On B4 hardware ports, BGP and ISIS operate. To ensure that every router receives an equal amount of bandwidth, traffic engineering is used. In cases when the application is linked to a bandwidth function, relative priority is also used. Depending on the relative importance of the flow, the function will determine the required bandwidth for each application. The tunnel group generation, which employs the bandwidth function to distribute bandwidth to FG, and the prioritization of bottleneck edges make up the two primary parts of the TE optimization method. Tunnel group quantization modifies each TG's division ratio to match the desired particle size. NS. Table swapping via hardware is supported. Three different modes of operation for B4 switches include encapsulating, transiting, and decapsulating. Depending on whether their IP matches, switches will map packets into FG. Each incoming packet is hashed before being forwarded to a tunnel. An address rather than a tunnel identifies the target IP. Configuring switches at several locations is necessary for tunnel installation. A single link failure results in traffic loss for milliseconds until the network converges, according to performance measurements. When a transit router fails, it takes around 3.3 seconds for the network to converge because nearby switches need to update a number of multitable pathways for a number of tunnels. An encap switch takes a little bit longer and loss is a little bit greater. As we increase the number of pathways accessible to the algorithm, the overall throughput rises. More hardware resources will be used as a result. By distinguishing between various traffic classes, a high utilization may be accepted. The fact that TE can manage classes with mixed priorities is a significant advantage. The load balancing algorithm's results are excellent since they demonstrate that the max-min ratio in utilization is 1.05 d 2.0 with failures on and around 75% of site to site edges. Overall, the B4 system was excellent and well beyond most expectations, however it did experience a significant outage during the repair window. Based on priority and dynamically shifting communication patterns, the centralized solution distributes an equal amount of bandwidth to all the nodes. More traffic has been handled by the software defined WAN, which is also expanding. SDN is not the answer since bottlenecks in bridging protocol packets have been seen to persist. An efficient way to integrate SDN architecture into the pre-existing network is through a hybrid approach that supports both new traffic engineering techniques and current protocols.