

BitTorrent™ Application Protocol

Accelerate Performance and Security of Network Equipment Handling BitTorrent and Encrypted BitTorrent Application Traffic

BitTorrent, a peer-to-peer (P2P) file sharing protocol is used globally for distributing large amounts of data across the Internet. According to Digital Music News Research Group, BitTorrent is one of the most common protocols for transferring large files, and may encompass 15% of all peer-to-peer traffic.

The mechanism by which BitTorrent breaks up files for distribution allows a single end-point to download small “pieces” from multiple peers simultaneously.

BitTorrent works in a P2P “seeding” approach, meaning that when the first seed (person) makes a file available for download, each other person who downloads that data also uploads it for other peers, encouraging additional data availability or additional “seeds”. This approach, while being highly efficient, also makes the BitTorrent protocol extremely complex and opens up network equipment to enormous amounts of peer connections. Add to that complexity Encrypted BitTorrent; an important element since it has become a possible liability for service providers with folks trying to avoid QoS policies, not to mention possible issues with file obfuscation, law enforcement avoidance and exploit prevention.

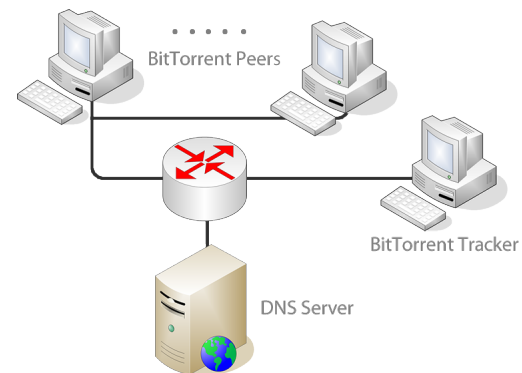
In many instances BitTorrent and Encrypted BitTorrent create a significant reduction in performance of network equipment and ultimately bandwidth connectivity. BreakingPoint enables testing of network equipment with both protocols by emulating the BitTorrent/Encrypted BitTorrent Data Transfer, consisting of two peers, who each make DNS requests to resolve the tracker, access the tracker, receive the peer list, and then establish a full peer-to-peer connection.

Utilizing BreakingPoint’s BitTorrent solution allows users to emulate a BitTorrent transfer across many peers while also sending a mix of blended applications. This functionality is particularly useful for Deep Packet Inspection (DPI) and security devices. Rate-shaping products sometimes want to throttle the bandwidth consumed by P2P applications in order to ensure that their goals for quality of service on other mission critical applications are met. Selecting the encrypted option for BitTorrent will help ensure that those DPI devices are still able to recognize and shape the traffic even if the specific contents are unknown.

BreakingPoint Testing Tools Emulate Encrypted BitTorrent:

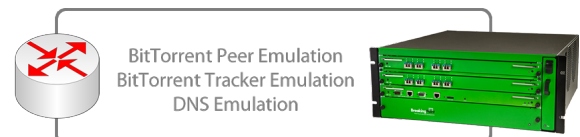
- Emulate all aspects of the BitTorrent protocol including tracking, peering as well as the DNS queries required to locate the respective parties during transfers.
- Utilizing the optional encrypted mode allows users to verify their deep packet inspection devices are behaving properly even when presented with encrypted P2P traffic.
- Blending other applications with BitTorrent provides a mechanism to ensure QoS on mission critical applications even when BitTorrent traffic is present.

Figure 1 - Traditional BitTorrent Connection Diagram



There are several players in a BitTorrent connection. The “tracker” maintains a list of the seeds while the peers actually act as both clients and servers.

Figure 2 - Test Bed Utilizing BreakingPoint



A test bed with BreakingPoint allows you to simulate the tracking, peering and downloading of files while sending other blended applications to ensure their quality of service.