

# Oracle® Application Protocol

*Ensuring High-Performance of Network Equipment Using Stateful Oracle Transparent Network Substrate (TNS) Protocol Traffic*

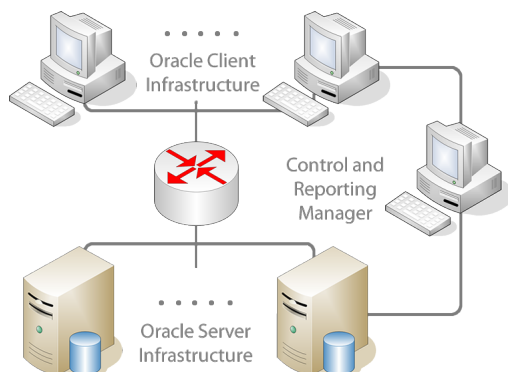
Transparent Network Substrate (TNS) is Oracle's networking architecture, which provides a uniform application interface to enable network applications to access the underlying network protocols transparently. The TNS protocol is used for both database authentication and database query requests and responses, which typically running on TCP port 1512. The Oracle TNS protocol helps network devices communicate with Oracle business services, including critical databases.

The BreakingPoint simulation of the Oracle TNS protocol has two main functions:

1. **Login:** Database username, database password, server name, database name, server OS, server banner, client username, client machine name, client program path, client program name
2. **Query:** Select: Column list, table name, WHERE comparison expression, ORDER BY expression

Traditional large-scale network infrastructure testing with Oracle would require a massive datacenter with many TNS servers as well as possibly hundreds of high-end servers acting as Oracle clients. In addition to the sheer amount of hardware required to generate the necessary scale of TNS traffic, the expense of purchasing a

**Figure 1 - Traditional Large-Scale Oracle Test Bed**



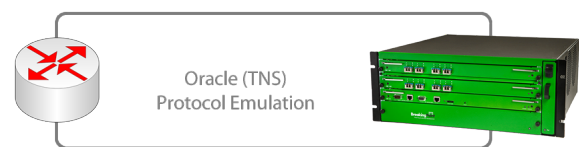
*Typical TNS test beds require tens and possibly hundreds of servers to generate high volume Oracle traffic. This can be expensive for both time and money.*

## BreakingPoint Testing Tools Emulate Oracle TNS:

- Eliminate the need for expansive datacenters which decreases power consumption and the expense of maintaining an Oracle infrastructure.
- Properly test network equipment with stateful Oracle TNS traffic.
- Help ensure proper performance and security levels when used in conjunction with blended applications at extremely high performance levels.
- Incorporate Oracle TNS security vulnerabilities such as TNS Listener DDoS to determine susceptible equipment.

third-party control and monitoring solution can be cost prohibitive. BreakingPoint's emulation of TNS eliminates the need for a datacenter as well as the control solution during testing, saving money in hardware, power, licensing and most importantly time.

**Figure 2 - Typical BreakingPoint Test Bed**



*Utilizing BreakingPoint, users are able to replace an expensive data center infrastructure with a single BreakingPoint Elite capable of generating tens of gigabits per second of TNS traffic with hundreds of thousands of queries per second.*