Listening In
Passive Capture and Analysis of Oracle Network Traffic

Jonah H. Harris
myYearbook.com
About Me

- Sr. DBA at myYearbook.com
- Oracle DBA and developer since Oracle7
- Research Oracle Internals
- Speaker at IOUG, VOUG, NYOUG
- Technical Reviewer for IOUG SELECT
- Blog about Oracle technology
You’re asking… what’s in it for me?

- Learn how to detect network-related issues.
- Diagnose and solve network-related issues.
- Gain a better understanding of the Oracle Network Protocol.
Disclaimer

- This is my hobby
- I’ve never been an Oracle insider
- The material in this presentation has been based on years of researching Oracle internals as well as analyzing network traffic and trace files.
- In addition to similar research from Ian Redfern, the majority of this paper is based primarily on my own personal research and discussions with Tanel Põder
- Do your own research!
- Use at your own risk!
A Common User Question

Question

- Why is the database sooooo slow?

The sarcastic response you’re considering…

- The edition of Oracle we’re using lacks the ALTER SYSTEM SPEEDUP DATABASE option.

Answer

- I don’t know…
- It’s not the database, it’s the application…
- I’ll look into it…
- How do you know it’s a database issue?
Troubleshooting the Issue

- Check Session Waits
- Check for a Long Running Query
- Check Session Performance Counters
- Check X, Y, Z…
Check Session Wait Events

- V$SESSION
- V$SESSION_WAIT
- V$SESSION_EVENT
- V$SESS_TIME_MODEL

Nope, nothing there…
Check Long Running Queries…

- V$SQL
- V$SESSION_LONGOPS

Hmm, looks like short queries…
Check Session Counters

- V$SESSTAT

Counters aren’t increasing, …
Troubleshooting the Issue

- Check Session Waits; zero.
- Check for a Long Running Query; zip.
- Check Session Performance Counters; zilch.
- Check X, Y, Z; nada.

All looks good from within Oracle… what next?
Check the Operating System

- Check Process CPU Usage and State
  - Determine whether it’s doing anything...
- Dump Call Stack
  - Get a list of all the function calls made by Oracle as well as the call we’re currently in…
Check the OS—CPU

- UNIX/Linux
  - nmon, top, glance, …
- Windows
  - More difficult due to threads-based model…
Examine the Process State

- Output from top
Check the OS—Call Stack

- UNIX/Linux
  - pstack, procstack, gdb, dbx, …
- Windows
  - More difficult…
Examine the Call Stack

- Represents the program’s function calls
- Stack data structure
- Top entry is the current function
Top of the Stack—read(), write()

- Operating System calls (syscalls)
- Used to read/write data from a file descriptor (socket).
Trace Client/Server?

- SQLNET.ORA
  - CLIENT_TRACE_LEVEL
  - SERVER_TRACE_LEVEL
- LISTENER.ORA
  - TRACE_FILE_LISTENER
Trace Client/Server? Uh, no.

- **Pros**
  - It works [for some things]

- **Cons**
  - Is not passive; Tracing/Logging has overhead
  - Difficult to find valuable information
  - Difficult to use for more than one connection
Oracle Network Architecture

- Layered
- Based on the Open Systems Interconnect (OSI) model
Oracle Net Components

- Oracle Protocol Support
- Oracle Net Foundation Layer
- Two Task Common Layer
- Application & RDBMS Layer
Oracle Protocol Support

- Maps TNS to underlying network transport
Oracle Net Foundation Layer

- Handles connections and messaging
- Transparent Network Substrate (TNS)
Two Task Common Layer

- Performs client/server character set conversion.
Application & RDBMS Layer

- Application (Client) Interface
  - UPI
  - OCI
  - JDBC
  - .NET

- RDBMS (Server) Interface
  - OPI (Oracle Programmatic Interface)
TNS Packets

- Transparent Network Substrate (TNS)
- Note: 1007807.6, SQL*NET PACKET
- STRUCTURE: NS PACKET HEADER

Every TNS packet has a header

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NSPHDLEN</th>
<th>NSPHDPSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NSPHDTYPE</th>
<th>reserved</th>
<th>NSPHDHSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
TNS Packet Types

- Connect
- Accept
- Acknowledge
- Refuse
- Redirect
- Data
- Null
- Abort
- Resend
- Marker
- Attention
- Control Information
Translating TNS Packets to Code

- Packet Header

```c
struct nsphd {
    ub2  nsphdlen;          /* Packet Length (in bytes) */
    ub2  nsphdpsm;          /* Packet Checksum */
    ub1  nsphdtyp;          /* Packet Type */
    ub1  nsphdrsv;          /* Reserved for Future Use? */
    ub2  nsphdhsm;          /* Packet Header Checksum */
};
```
TNS Connect Packet

Performs a connection to an Oracle server.

```c
struct nspcn {
    ub2   nspcnvsn;          /* Packet Version */
    ub2   nspcnlov;          /* Lowest Compatible Version */
    ub2   nspcnopt;          /* Supports Global Service Options */
    ub2   nspcnnsdu;         /* Session Data Unit Size (in bytes) */
    ub2   nspcnntdu;         /* Transport Data Unit Size (in bytes) */
    ub2   nspcntdu;          /* NT Protocol Characteristics */
    ub2   nspcntna;          /* Line Turnaround Value */
    ub2   nspcnnone;         /* The number 1 in Host Byte Order */
    ub2   nspcnlen;          /* Length of Connect Data (in bytes) */
    ub2   nspcnoff;          /* Byte Offset to Connect Data */
    ub4   nspcnmxc;          /* Maximum Connect Data */
    ub1   nspcnf10;          /* Connect Flags 0 */
    ub1   nspcnf11;          /* Connect Flags 1 */
    ub4   nspcnncf1;         /* cross facility item 1 */
    ub4   nspcnncf2;         /* cross facility item 2 */
    text  nspcnucid[8];     /* unique connection id */
    text  nspcnxic[8];      /* unique connection id */
    text  *nspcndat;        /* Connect Data */
};
```
TNS Accept Packet

Server’s response to a connection request.

```c
struct nspac
{
    ub2   nspacvsn;          /* Version that this connection is to run at */
    ub2   nspacopt;          /* Global service options */
    ub2   nspacsdu;          /* Session Data Unit Size (in bytes) */
    ub2   nspactdu;          /* Transport Data Unit Size (in bytes) */
    ub2   nspacone;          /* The value '1' in host byte order */
    ub2   nspaclen;          /* Length of connect data */
    ub2   nspacoff;          /* Offset to start of connect data */
    ub1   nspacfl0;          /* Connect Flags 0 */
    ub1   nspacfl1;          /* Connect Flags 1 */
    text  *nspacdat;         /* Connect Data */
};
```
TNS Refuse Packet

A denied connection request by the server.

```c
struct nsprf {
    ub1 nsprfurs;               /* User (application) reason for refusal */
    ub1 nsprfsrs;                      /* System (NS) reason for refusal */
    ub2 nsprflen;                               /* Length of refuse data */
    text *nsprfdat;                               /* Start of connect data */
};
```
TNS Redirect Packet

- Server asks client to performs connection redirection.

```c
struct nsprd {
    ub2 nsprdlen; /* Length of redirect data */
    text *nsprddat; /* Start of connect data */
};
```
TNS Resend Packet

- Server requests the client to resend the packet.
- Packet is the standard TNS header with packet type NSPTRS.
TNS Null Packet

- Generally used for keep-alive.
- Packet is the standard TNS header with packet type NSPTNL.
TNS Data Packet

- The most commonly used packet.
- Encapsulates TTI/TTC Subpackets

```c
struct nspda
{
    ub2    nspdaflg; /* Data Flags */
    text   *nspdadat; /* start of data */
};
```
Issue #1: Slow Connections

- Connecting to server is slow
Establishing a Connection

- Connect to Server
- Negotiate Additional Network Options
- Negotiate Protocol Version
- Negotiate Data Types
- Authenticate

Code (Upon Request)
- oconnect.c
Making the Connection

- Client requests a connection to TNS entry ORCL.
- Network Naming attempts each directory_path method in order.
- Network Naming parses TNSNAMES.ORA looking for the ORCL entry.
- Client builds and sends a TNS Connect Packet (NSPTCN) to the appropriate listener.
- The Listener responds with a TNS Resend (NSPTRS) or Redirect [to another port] (NSPTRD) packet.
- Client responds accordingly.
- Server responds with an Accept (NSPTAC) or Refuse (NSPTRF) packet.
Negotiating Additional Options

- Additional Services
  - Authentication
  - Encryption
  - Data Integrity
  - Supervisor
Negotiating Protocol Versions

- TTI Protocol Packet
  - What versions are acceptable?
    - 4, 5, 6
  - Server replies with info
Negotiating Data Types

- TTI Data Type Packet
  - Client character conversions
- Server replies with its own representations
Authentication

- Client sends server basic information
  - User Name
  - Terminal Name
  - Machine Name
  - Program Name
  - …
- Server responds with challenge/response…
Why can it be slow?

- Parsing large TNSNAMES.ORA files
- Network Connectivity (Firewall/VPN)
- Overloaded Server
Large TNSNAMES.ORA

Reason
- Increases parse time

How to detect
- Oracle Net Tracing
  - Time between loading TNSNAMES.ORA and finding the appropriate entry.

How to fix
- Use different TNSNAMES.ORA files
- Use EZCONNECT or a different directory method
Network Connectivity

- Reason
  - Network latency slows down packet transfer.

- How to detect
  - Inside Oracle
    - SQL*Net message to client with high wait times
  - Wire-level Monitoring
    - Look for delays in TCP ACK
  - Client/Server Oracle Net Tracing (least-preferred)
    - Look at time between send/recv from NS and NT

- How to fix
  - Fix the network.
Overloaded Server

- **Reason**
  - Server is CPU-bound and has a high load

- **How to detect**
  - Wire-level Monitoring (Server-side)
    - Calculate time between receiving a TNS packet and sending a response.
  - Server-side Listener Tracing (least-preferred)

- **How to fix**
  - Find cause of load
    - Buy new hardware
    - Tune queries
Issue #2: Slow Queries

- Simple queries take a long time to return…
Querying the Database

- Open a cursor
- Parse the query
- Execute the query
- Fetch the data
- Cancel the cursor
- Close the cursor

Code (Upon Request)
- oquery.c
Open a Cursor

- TTC Open (OOPEN)
  - Opens a statement

- Protocol
  - Client requests OOPEN
  - Server replies with cursor #
Parse/Execute the Query

- TTC (OALL7/8)
  - Supports several options
    - Parse
    - Bind
    - Execute
    - Fetch
    - Cancel
    - Commit
    - Exact Fetch
    - Send Vector
    - No PL/SQL

- Protocol
  - Client sends OALL packet with cursor #, SQL statement, and flags (Parse, No PL/SQL, Execute), then requesting column/data type info.
  - Server replies with Success/Fail
Fetch Data

- OALL7/8 Packet
  - Options
    - No PL/SQL
    - Fetch

- Protocol
  - Client sends OALL packet with No PL/SQL and Fetch options
  - Server replies with data.
Why can it be slow?

- Network Connectivity (Firewall/VPN)
- Overloaded Server
- Underlying Network Protocol Settings
- Fetching method used by an application
Underlying Network Protocol

- Reason
  - Oracle NT/NS relies on fast UNP

- How to detect
  - Wire-level Monitoring (UNP Fragmentation)
  - Inside Oracle (SDU/UNP Issues)
    - SQL*Net message to client/more data to client

- How to fix
  - Tune OS-level protocols using best practices
  - Make sure Oracle Net matches UNP (SDU==MTU) in listener.ora and tnsnames.ora
Fetch Method

- Reason
  - One-at-a-time fetching means one-roundtrip-per-fetch.

- How to detect
  - Wire-level Monitoring (lots of fetch packets)
  - Inside Oracle
    - Look for a lack of SQL*Net more data to client

- How to fix
  - Use Array-based Fetching
    - OCI (prefetching)
  - Tune Explicit Fetch Sizes
Wire-level Monitoring Tools for Oracle

- Oracle Itself
- Wireshark
- WireCache SQL Query Analyzer
- SCAPE for Oracle (SCAPE4O)
Oracle Network Monitoring

- **Pros**
  - The simplest method
- **Cons**
  - Not manageable for large-scale systems
Wireshark

Pros
- Free
- Dissects TNS packets
- Records Conversations
- Can be used with stored packet captures

Cons
- Does not decode TTI/TTC packets (yet)
WireCache SQL Query Analyzer

Pros
- Dissects TNS packets
- Dissects TTI/TTC Packets
- Records Conversations
- Can be used with stored packet captures

Cons
- Commercial Product
<table>
<thead>
<tr>
<th>%TIME</th>
<th>TIME</th>
<th>COUNT</th>
<th>STMT</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.0</td>
<td>18826.34</td>
<td>123.25</td>
<td>&lt;= TOTAL</td>
</tr>
<tr>
<td>84.8</td>
<td>15983.94</td>
<td>80.36</td>
<td>-- SELECT</td>
</tr>
<tr>
<td>11.5</td>
<td>459.78</td>
<td>0.00</td>
<td>-- INSERT</td>
</tr>
<tr>
<td>2.7</td>
<td>459.78</td>
<td>0.00</td>
<td>-- COMMIT/ROLLBACK</td>
</tr>
<tr>
<td>0.6</td>
<td>459.78</td>
<td>0.00</td>
<td>-- ALTER/CREATE</td>
</tr>
<tr>
<td>0.5</td>
<td>2171.89</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>0.1</td>
<td>2171.89</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>0.0</td>
<td>2171.89</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>28.4</td>
<td>5385.38</td>
<td>0.00</td>
<td>SELECT CC_FIRST_CASE_DT FROM PS_RF_INST</td>
</tr>
<tr>
<td>10.4</td>
<td>15983.94</td>
<td>0.00</td>
<td>UPDATE PS_RF_INST_PROD SET CC_FIRST_CASE</td>
</tr>
<tr>
<td>8.2</td>
<td>1427.12</td>
<td>0.00</td>
<td>SELECT DISTINCT SC.CC_CAUSE_ID, C.DESCRI</td>
</tr>
<tr>
<td>7.5</td>
<td>749.77</td>
<td>0.00</td>
<td>SELECT INST.PRODUCT_ID,INST.CC_RECALL_F</td>
</tr>
<tr>
<td>4.0</td>
<td>673.29</td>
<td>0.00</td>
<td>SELECT INST.CC_POP_FLG, PROD.CC_POP_GRA</td>
</tr>
<tr>
<td>3.5</td>
<td>416.79</td>
<td>0.00</td>
<td>SELECT PRODUCT_ID FROM PS_RF_INST_PROD</td>
</tr>
<tr>
<td>2.7</td>
<td>416.79</td>
<td>0.00</td>
<td>SELECT TO_CHAR(BO_ID) FROM PS_BO WHERE</td>
</tr>
<tr>
<td>1.9</td>
<td>368.44</td>
<td>0.00</td>
<td>SELECT CM_ID, COUNTRY_CODE, PHONE, EXTE</td>
</tr>
</tbody>
</table>
SCAPE for Oracle (SCAPE4O)

- SQL Capture and Analysis by Passive Evaluation
- Pros
  - Free
  - Dissects TNS packets
  - Dissects TTI/TTC Packets
  - Records Conversations
  - Can be used with stored packet captures
- Cons
  - Alpha-quality
SCAPE for Oracle (SCAPE4O)
Items Learned in this Session

- How to detect network-related issues.
- How to diagnose and solve network-related issues.
- Gained a better understanding of the Oracle Network Protocol
Questions?
Thank You

- Fill out evaluation
  - Jonah H. Harris
  - Listening In: Passive Capture and Analysis of Oracle Network Traffic
  - Session 381

- Further Information
  - jonah.harris@gmail.com
  - http://www.oracle-internals.com/