

TNS Connections

What Could Possibly Go Wrong?

 Axel vom Stein – BSS Bohnenberg GmbH

 Martin Klier – Performing Databases

Speaker

- Martin Klier, Oracle ACE Director
- Performing Databases since 2014

- Solution Architect and Database Expert
- My focus:
 - Performance & Tuning
 - Highly Available Systems
 - Cluster and Replication

- Linux since 1997
- Oracle Database since 2003



Oracle ACE
Director

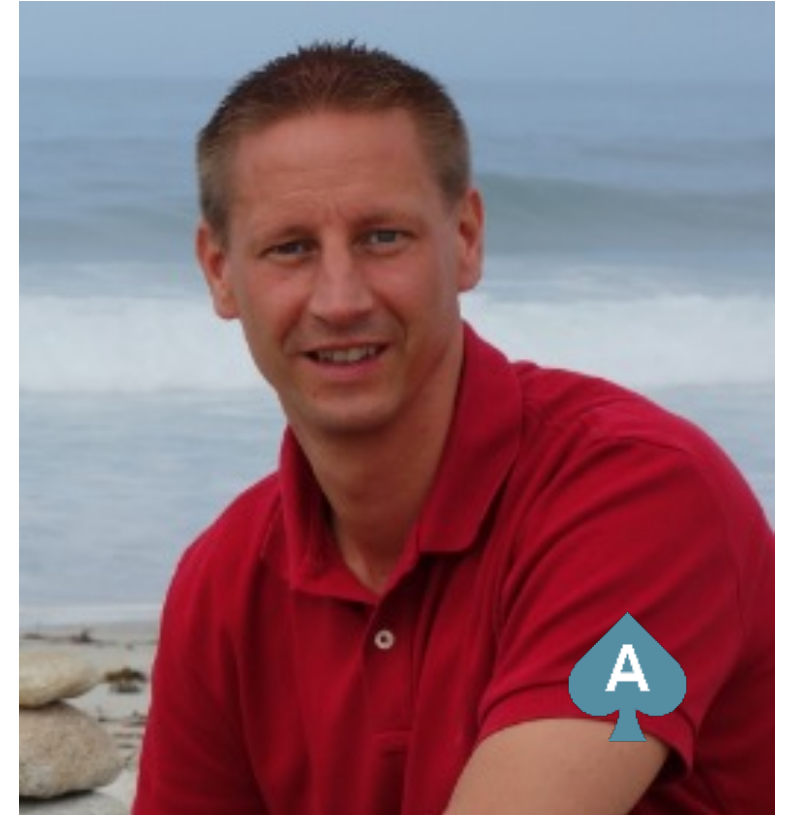
SYMPOSIUM ^{L2}
Proud Member of symposium42

Speaker

- Axel vom Stein, Oracle ACE Pro
- Technical Project Manager, Head of IT
- Working for BSS since 2001

- Oracle:
 - since 2001
 - started out as a developer (PL/SQL, C, C#)
 - interest moved more towards DBA topics

- My focus:
 - teaching trainees and young professionals
 - HA - concepts
 - standardization & automation



Oracle ACE
Pro

SYMPOSIUM ^{L2}
Proud Member of symposium42



The Oracle ACE Program

500+ technical experts helping peers globally



- The Oracle ACE Program recognizes and rewards community members for their technical and community contributions to the Oracle community
- 3 membership levels: Director, Pro, and Associate
- Nominate yourself or a colleague at ace.oracle.com/nominate
- Learn more at ace.oracle.com



ora2know

The German Oracle Database Community



ora2know

The German Oracle Database Community

<https://www.ora2know.de>

Logistics / Warehousing

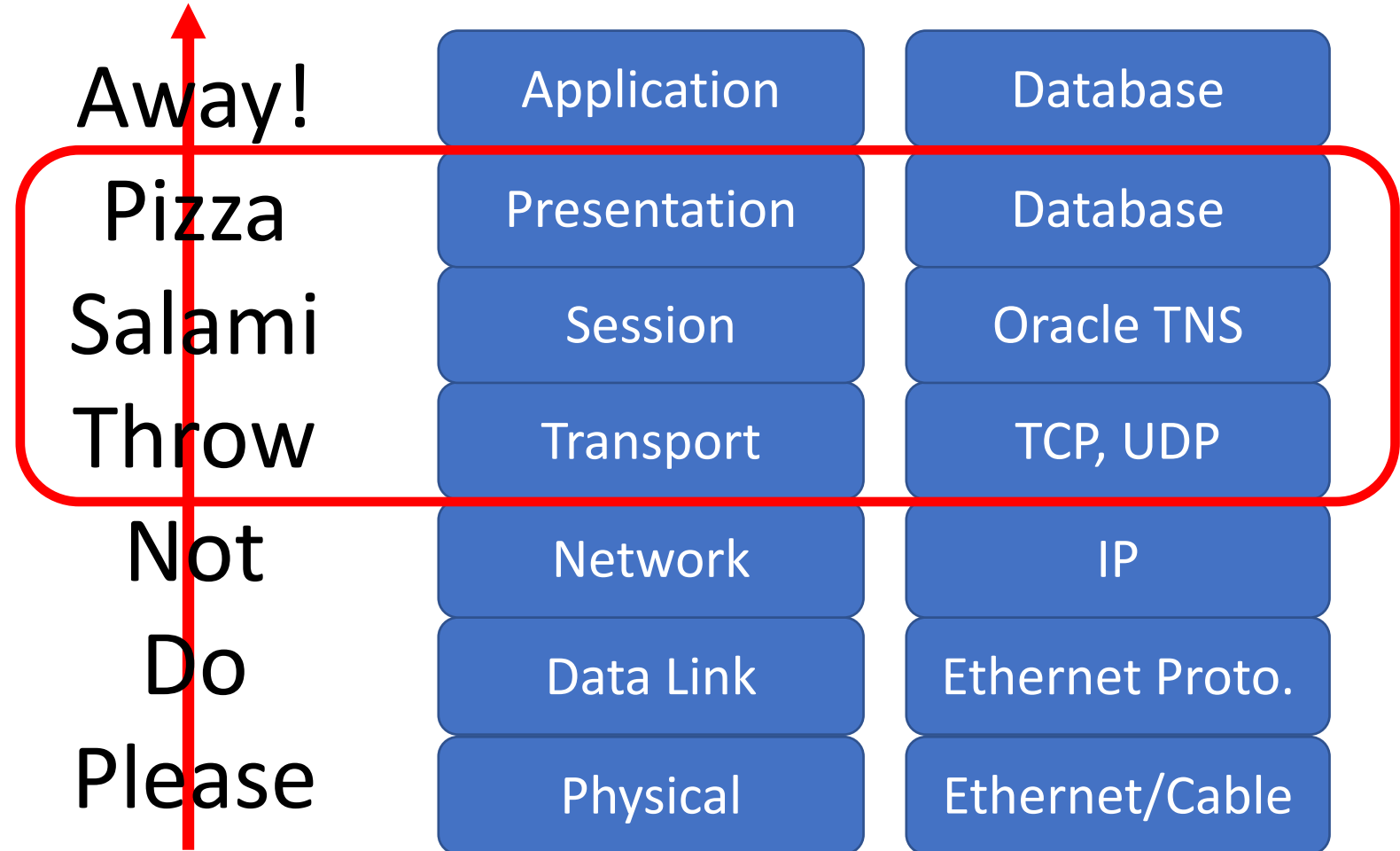
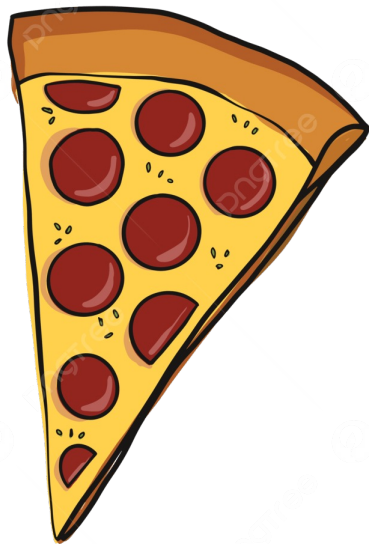


Logistics Warehousing



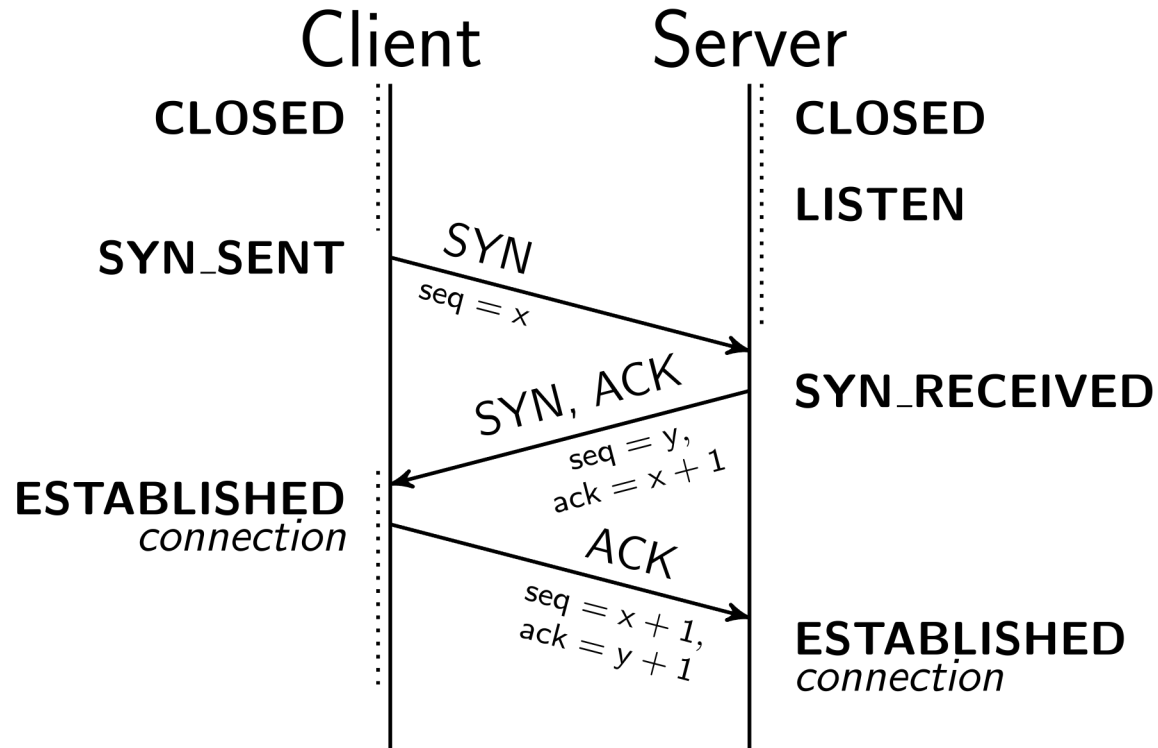
Networking Basics

ISO/OSI 7-Layer Model

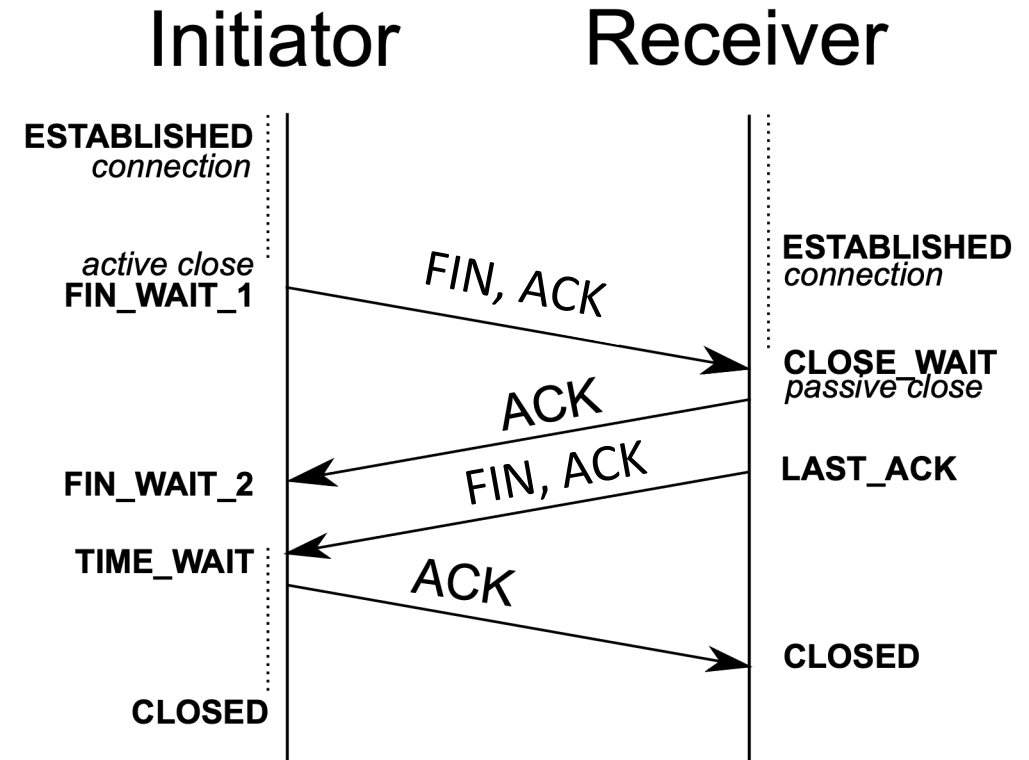


Transport - TCP Basics: Connections

3-Way Handshake



Connection Teardown



Transport – TCP Basics: netcat Example

“Server” with open netcat port

```
nc -lvk 1522
```

(= listen, verbose, keep open port 1522)

netcat “client” from random port

```
nc lab26ai.lab01.pdb.lan 1522
```

(= connect to host lab26ai at port 1522)

192.168.0.100



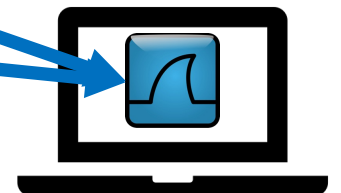
```
tcpdump -i ens33 -w <filename>
```



192.168.0.200



```
tcpdump -i ens17 -w <filename>
```



Mac w/ Wireshark

```
netstat -tulpen
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	Benutzer	Inode	PID/Program name
tcp	0	0	0.0.0.0:1522	0.0.0.0:*	LISTEN	0	8544762	1113753/nc

Transport - TCP Basics: netcat Example

```

[usn — root@lab26ai-1:~ — ssh -o StrictHostKeyChecking=no root@lab26ai-1.lab01.pdb.lan — 153x46]
[root@lab26ai-1 ~]#
[root@lab26ai-1 ~]#
[root@lab26ai-1 ~]# nc -lvk 1522
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1522
Ncat: Listening on 0.0.0.0:1522
Ncat: Connection from 10.22.11.45.
Ncat: Connection from 10.22.11.45:60962.
Hallo Axel!

[usn — -bash — 137x35]
[odysseus:~ usn$ echo 'Hallo Axel!' | nc lab26ai-1.lab01.pdb.lan 1522
odysseus:~ usn$
  
```

Opening Socket 10.22.21.50:1522

Connection from 10.22.11.45:60449 (random high port)

(ip.src==10.22.21.50 or ip.dst==10.22.21.50) and tcp.port==1522

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1128	12:05:15.638731	10.22.11.45	60449	10.22.21.50	1522	TCP	68	60449 → 1522 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1240 WS=64 TSval=3110016318 TSecr=0 SACK_PERM
1129	12:05:15.660566	10.22.21.50	1522	10.22.11.45	60449	TCP	64	1522 → 60449 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1992944886 TSecr=3110016318 WS=128
1130	12:05:15.660728	10.22.11.45	60449	10.22.21.50	1522	TCP	56	60449 → 1522 [ACK] Seq=1 Ack=1 Win=131456 Len=0 TSval=3110016341 TSecr=1992944886
1131	12:05:15.661257	10.22.11.45	60449	10.22.21.50	1522	TCP	68	60449 → 1522 [PSH, ACK] Seq=1 Ack=1 Win=131456 Len=12 TSval=3110016341 TSecr=1992944886
1132	12:05:15.661384	10.22.11.45	60449	10.22.21.50	1522	TCP	56	60449 → 1522 [FIN, ACK] Seq=13 Ack=1 Win=131456 Len=0 TSval=3110016341 TSecr=1992944886
1134	12:05:15.683092	10.22.21.50	1522	10.22.11.45	60449	TCP	56	1522 → 60449 [ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=1992944908 TSecr=3110016341
1135	12:05:15.683102	10.22.21.50	1522	10.22.11.45	60449	TCP	56	1522 → 60449 [FIN, ACK] Seq=1 Ack=14 Win=65152 Len=0 TSval=1992944908 TSecr=3110016341
1138	12:05:15.683461	10.22.11.45	60449	10.22.21.50	1522	TCP	56	60449 → 1522 [ACK] Seq=14 Ack=2 Win=131456 Len=0 TSval=3110016363 TSecr=1992944908

```

> Frame 1131: Packet, 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface ppp0, id 0
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 10.22.11.45, Dst: 10.22.21.50
> Transmission Control Protocol, Src Port: 60449, Dst Port: 1522, Seq: 1, Ack: 1, Len: 12
  Source Port: 60449
  Destination Port: 1522
  [Stream index: 32]
  [Stream Packet Number: 4]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 12]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 560682208
  [Next Sequence Number: 13 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1347369990
  
```

```

0000 ff 03 00 21 45 02 00 40 00 00 40 00 40 06 06 2c ...!E..@ ..@..@..
0010 0a 16 0b 2d 0a 16 15 32 ec 21 05 f2 21 6b 54 e0 ......2 !...!kT.
0020 50 4f 3c 06 80 18 08 06 27 12 00 00 01 01 08 0a PO<.....'.....
0030 b9 5f 15 55 76 c9 ec f6 48 61 6c 6c 6f 20 41 78 ...Uv... Hallo Ax
0040 65 6c 21 0a ..!..
  
```

Transport - TCP Basics: netcat Example

Establish

Dest Port	Protocol	Length	Info
1522	TCP	68	60449 → 1522 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS
60449	TCP	64	1522 → 60449 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len
1522	TCP	56	60449 → 1522 [ACK] Seq=1 Ack=1 Win=131456 Len=0 TSval=
1522	TCP	Data 68	60449 → 1522 [PSH, ACK] Seq=1 Ack=1 Win=131456 Len=12
1522	TCP	56	60449 → 1522 [FIN, ACK] Seq=13 Ack=1 Win=131456 Len=0
60449	TCP	56	1522 → 60449 [ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=
60449	TCP	56	1522 → 60449 [FIN, ACK] Seq=1 Ack=14 Win=65152 Len=0 T
1522	TCP	56	60449 → 1522 [ACK] Seq=14 Ack=2 Win=131456 Len=0 TSval

Teardown

```
[PSH, ACK] Seq=1 Ack=1 Win=131456 Len=12 TSval=3110016341 TSecr=1992944886
[FIN, ACK] Seq=13 Ack=1 Win=131456 Len=0 TSval=3110016341 TSecr=1992944886
[ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=1992944908 TSecr=3110016341
[FIN, ACK] Seq=1 Ack=14 Win=65152 Len=0 TSval=1992944908 TSecr=3110016341
[ACK] Seq=14 Ack=2 Win=131456 Len=0 TSval=3110016363 TSecr=1992944908
```

```
000 ff 03 00 21 45 02 00 40 00 00 40 00 40 06 06 2c  ...!E..@ ..@..@.,
010 0a 16 0b 2d 0a 16 15 32 ec 21 05 f2 21 6b 54 e0  ...-...2 !...!kT.
020 50 4f 3c 06 80 18 08 06 27 12 00 00 01 01 08 0a  P0<.....'.....
030 b9 5f 15 55 76 c9 ec f6 48 61 6c 6c 6f 20 41 78  .Uv... Hallo Ax
040 65 6c 21 0a                                     e!..
```

Transparent Network Substrate “TNS”, “Oracle Net”, “Net8”

TNS Connection Protocol Options

- **PROTOCOL=TCP**
sqlplus scott/tiger@dbhost1.example.com:1521/orclpdb1
- **PROTOCOL=TCPS**
sqlplus scott/tiger@'tcps://dbhost1.example.com:2484/orclpdb1?ssl_server_dn_match=yes'
- **PROTOCOL=IPC** (“Inter-Process Communication”)
Example: EXTPROC
- **PROTOCOL=BEQ** (“Bequeath”)
Example: sqlplus / as sysdba

What can go wrong... sqlnet.ora



```
NAMES.DIRECTORY_PATH = (TNSNAMES, EZCONNECT, HOSTNAME)
```

listener.ora:
=> DEFAULT_SERVICE_LISTENER

```
SQLNET.OUTBOUND_CONNECT_TIMEOUT = 10
```

Overridden by tnsnames.ora CONNECT_TIMEOUT

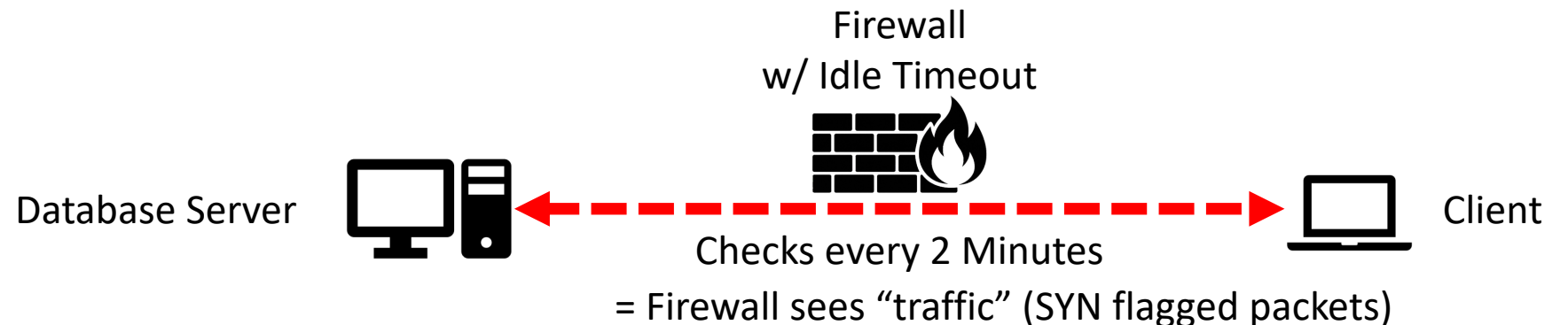
```
SQLNET.RECV_TIMEOUT = 30
```

```
SQLNET.SEND_TIMEOUT = 30
```

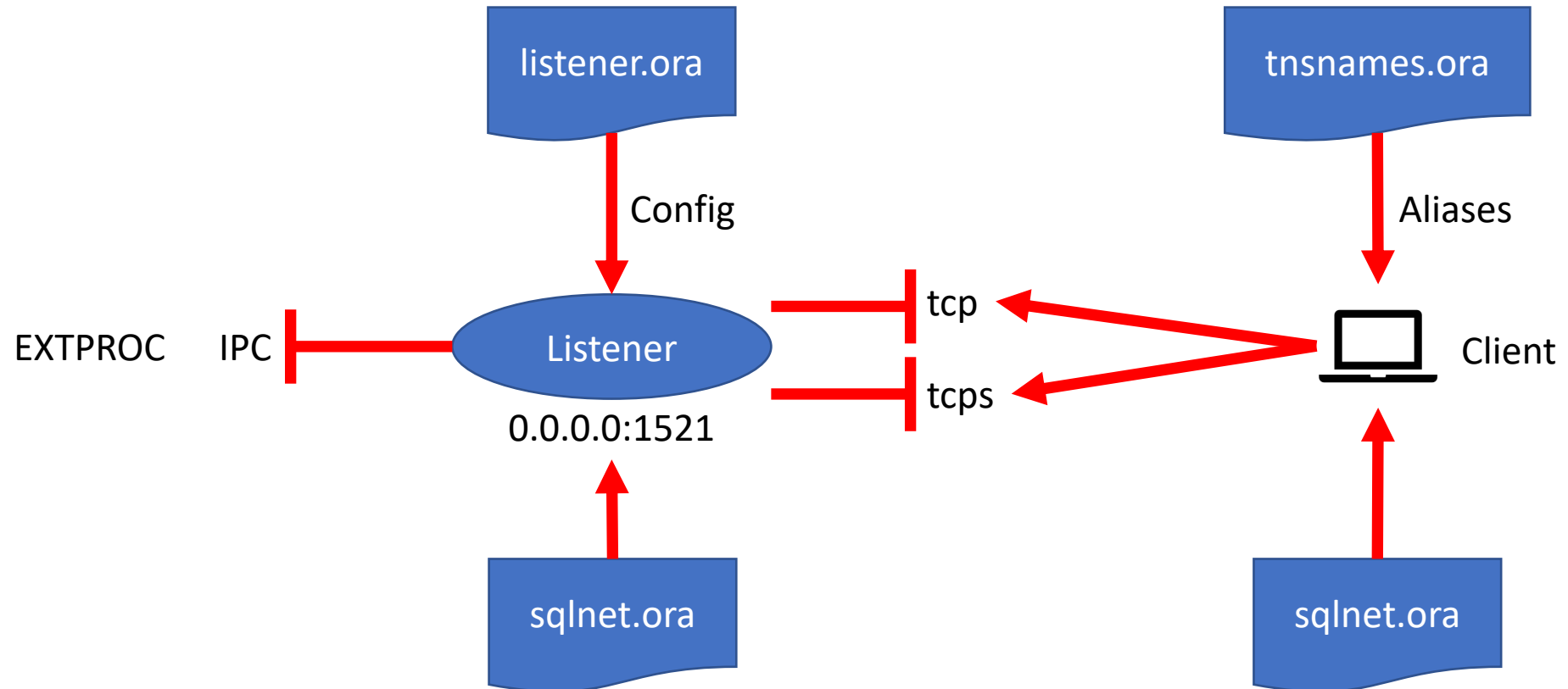
Limiting Connection Idle Time (SQL >30s will die!)

```
SQLNET.EXPIRE_TIME = 2
```

Firewall is my friend ...



Listener Endpoints



The Listener

```

Listener Parameter File  $ORACLE_HOME/network/admin/listener.ora
Listener Log File       $ORACLE_BASE/diag/tnslsnr/myhostname/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=LISTENER)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=192.168.0.100)(PORT=1521)))
Services Summary...
Service "45c1127082e7edbee4199af2a00a0fed" has 1 instance(s)
  Instance "MYSID1", status READY, has 1 handler(s) for this service...
Service "MYSERVICE1" has 1 instance(s)
  Instance "MYSID1", status READY has 1 handler(s) for this service...
Service "MYSERVICE2" has 1 instance(s)
  Instance "MYSID1", status READY has 1 handler(s) for this service...
Service "MYSID1_DGMGRL" has 2 instance(s)
  Instance "MYSID1", status UNKNOWN has 1 handler(s) for this service...

```

Config + Log

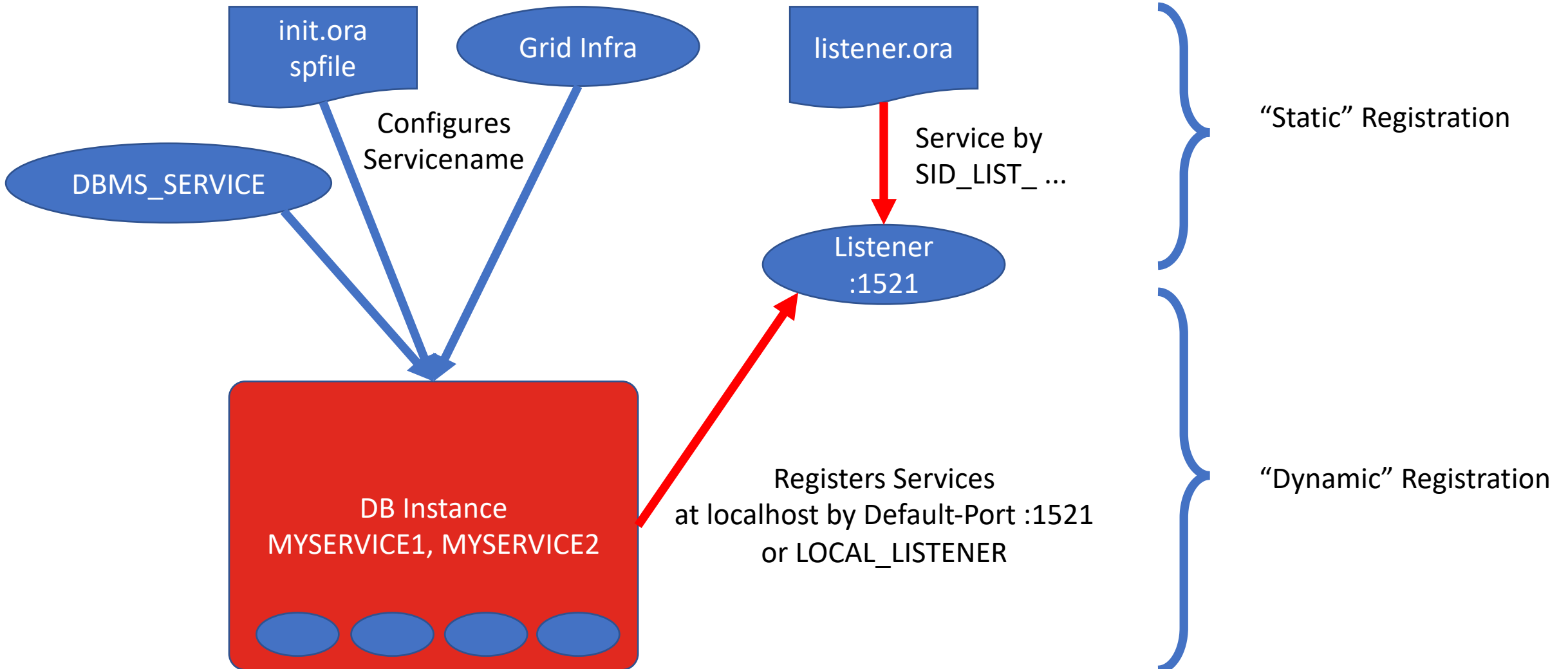
Endpoints

PDB GUID Service

Dynamic Services

Static Service

Instance Registration@Listener



What can go wrong... listener.ora

HUGO ?

```

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = dbserver01.example.local) (PORT = 1521))
    )
  )
  
```

1523 ?
LOCAL_LISTENER !

HUGO !

```

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = TEST)
      (ORACLE_HOME = /u01/app/oracle/product/19.0.0/dbhome_1)
      (SID_NAME = TEST)
    )
  )
  
```

HUGO !

```

USE_SID_AS_SERVICE_LISTENER = ON
  
```

HUGO !

```

DEFAULT_SERVICE_LISTENER = MYDEFAULTSERVICE
  
```

tnslsnr ... just sayin' ...

TNS Connection via Listener (Linux/Unix)

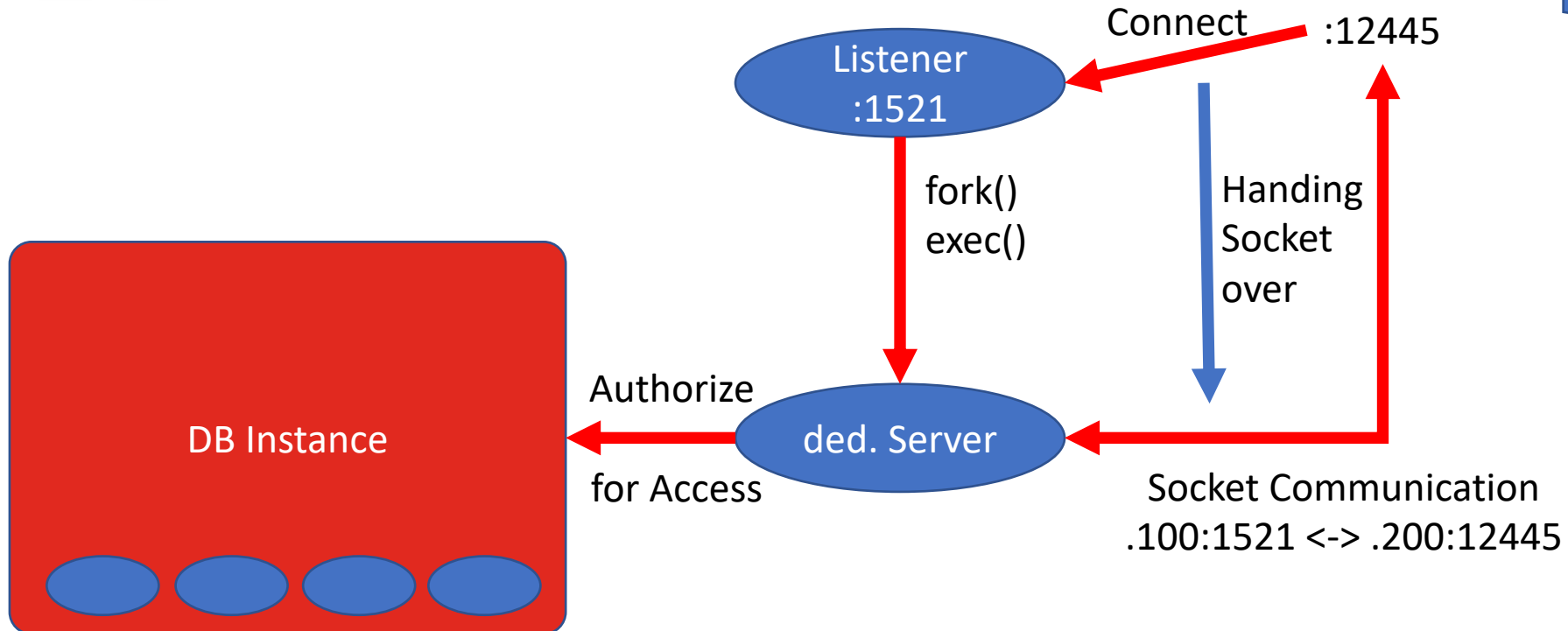
Database Server
192.168.0.100



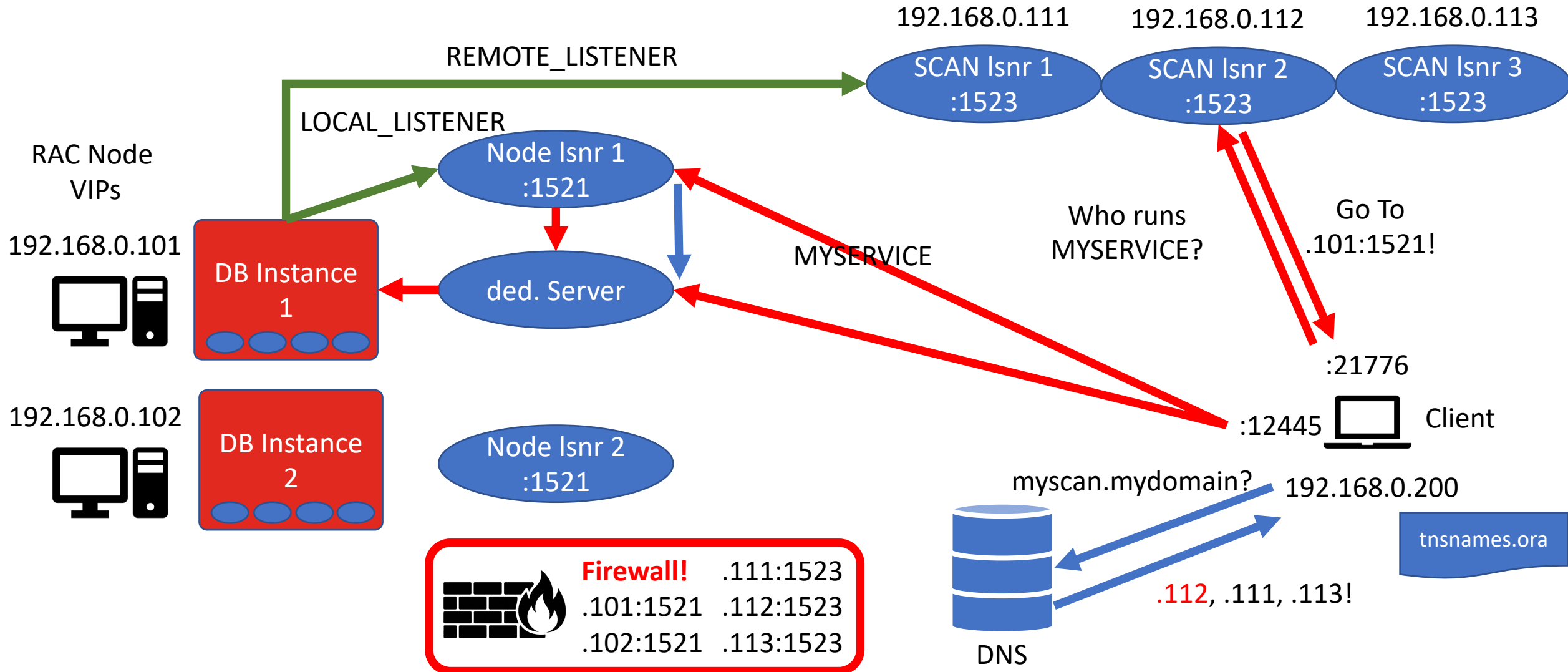
Client
192.168.0.200



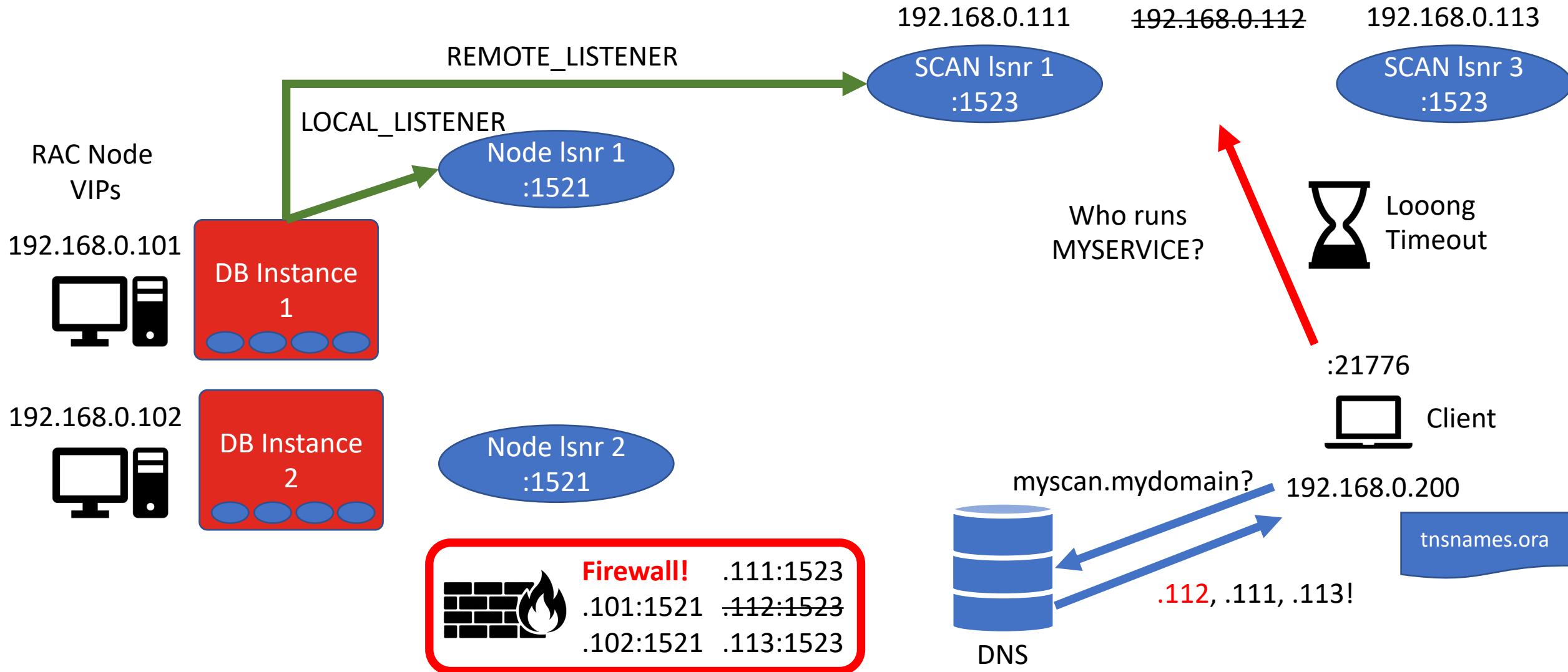
tnsnames.ora



TNS Connection via SCAN Listener



TNS **No!** Connection via SCAN Listener



TNS Connection Timeouts

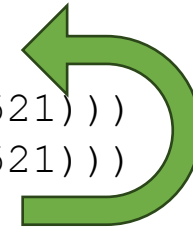
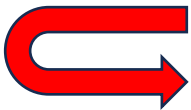
Timeout after 3s

Retry again 3x

Wait 1s

Classic ADDRESS LIST w/o SCAN Listener (Link: Data Guard!)

```
(DESCRIPTION= (CONNECT_TIMEOUT=3) (RETRY_COUNT=3) (RETRY_DELAY=1)
  (ADDRESS_LIST= (LOAD_BALANCE=OFF) (FAILOVER=ON)
    (ADDRESS= (PROTOCOL=TCP) (HOST=dataguard-A) (PORT=1521))
    (ADDRESS= (PROTOCOL=TCP) (HOST=dataguard-B) (PORT=1521))
  )
  (CONNECT_DATA= (SERVER=DEDICATED) (SERVICE_NAME=MYSERVICE)
)
)
```



11gR2+ ADDRESS Syntax for SCAN Listener

Timeout after 3s

```
(DESCRIPTION=
  (RETRY_COUNT=3) (RETRY_DELAY=1)
  (ADDRESS= (PROTOCOL=TCP) (HOST=myscan.mydomain) (PORT=1521))
  (CONNECT_DATA= (SERVER=DEDICATED) (SERVICE_NAME=MYSERVICE)
)
)
```

.112
.111
.113



What can go wrong... tnsnames.ora

- Duplicate TNS names
(Last always wins)
- IFILE=/path/to/myfile.ora
Have it nested, have fun! (max. 3 levels)
- Duplicate TNS names in IFILE vs. tnsnames.ora
Position of IFILE matters!
- IFILE also possible for listener.ora, sqlnet.ora ...

What can go wrong... Duplicates in IFILE

Overwritten by
IFILE content

```
MYDBOX =  
  (DESCRIPTION =  
    (ADDRESS_LIST =  
      (ADDRESS = (PROTOCOL = TCP) (HOST = 192.168.0.100) (PORT = 1521))  
    )  
    (CONNECT_DATA = (SERVICE_NAME = MYSERVICE))  
  )
```

```
IFILE=/home/oracle/tnsnames_ifile.ora
```

Overwrites
IFILE content

```
YOURDBOX =  
  (DESCRIPTION =  
    (ADDRESS_LIST =  
      (ADDRESS = (PROTOCOL = TCP) (HOST = 192.168.0.100) (PORT = 1521))  
    )  
    (CONNECT_DATA = (SERVICE_NAME = YOURSERVICE))  
  )
```

What can go wrong... \$TWO_TASK

- "Two Task" = classic naming of Oracle for Client-Server-Communication
Opposite: Bequeath Connect
- Can contain
 - TNS alias
 - TNS connect string
 - EZconnect string
- Is used INSTEAD OF bequeath connect
(adds "@\$TWO_TASK" to your "sqlplus user/pw")
- In Windows: %LOCAL%

What can go wrong... Connection Errors

```
SQL> connect sys/oracle@192.168.0.100:1521/freepdb1 as sysdba
```

ERROR:

```
ORA-12650: No common encryption or data integrity algorithm
```

ONNE: Encryption and Hash Cipher

Network Encryption (protects from curious people, but not from data manipulation)

SQLNET.ENCRYPTION_{CLIENT|SERVER} → REJECTED, **ACCEPTED**, REQUESTED, REQUIRED

SQLNET.ENCRYPTION_TYPES_{CLIENT|SERVER} → AES128, AE192, AES256

Network Data Integrity (protects from altering data, but not from curious people)

SQLNET.CRYPTO_CHECKSUM_{CLIENT|SERVER} → REJECTED, **ACCEPTED**, REQUESTED, REQUIRED

SQLNET.CRYPTO_CHECKSUM_TYPES_{CLIENT|SERVER} → SHA256, SHA384, SHA512

Security →

Min ←

Max ↓

		SERVER SETTING			
		REJECTED	ACCEPTED	REQUESTED	REQUIRED
CLIENT SETTING	REJECTED	OFF	OFF	OFF	FAIL
	ACCEPTED	OFF	OFF	ON	ON
	REQUESTED	OFF	ON	ON	ON
	REQUIRED	FAIL	ON	ON	ON

Analysis with SQL

```

WITH y AS (
  SELECT c.CON_ID, c.SID, c.Client_Version, c.Client_Charset, c.Authentication_Type,
         c.Client_OCI_Library, c.Client_Connection_String,
         /* Protokoll (TCP or TCPS) */
         CASE WHEN MAX(CASE WHEN c.Network_Service_Banner LIKE '%TCPS%' THEN 1 END) = 1 THEN 'TCPS' ELSE 'TCP' END AS Protocol,
         /* Encrpytion Algorithm or NONE - (26ai supported: AES128,192,256) */
         NVL(MAX(REGEXP_SUBSTR(c.Network_Service_Banner, '(AES128|AES192|AES256|3DES|DES|RC4)',1,1,'i')), 'NONE') AS Encryption,
         /* Checksum Algorithmus or NONE - (26ai supported: SHA256,384,512) */
         NVL(MAX(REGEXP_SUBSTR(c.Network_Service_Banner, '(SHA256|SHA384|SHA512|MD5|SHA1)',1,1,'i')), 'NONE') AS Checksum
  FROM gv$session_connect_info c
  GROUP BY c.Con_ID, c.SID, c.Client_Version, c.Client_Charset, c.Authentication_Type,
           c.Client_OCI_Library, c.Client_Connection_String
)
SELECT * FROM (
  SELECT y.Protocol, s.Server, s.Service_Name, s.Port,
         y.Encryption, y.Checksum,
         y.Con_ID, y.SID, s.Serial#,
         y.Client_Version, y.Client_Charset, y.Authentication_Type, y.Client_OCI_Library,
         s.Username as DbUser , s.OsUser, s.Machine, s.Logon_Time, s.Status,
         s.Program,
         s.Module, s.Action, s.Client_Info, /* <== DBMS_APPLICATION_INFO */
         y.Client_Connection_String
  FROM gv$Session s, y
  WHERE y.SID = s.SID
        AND s.Type != 'BACKGROUND')

```

gv\$session_connect_info

gv\$session

Analysis with SQL

PROTO	SERVER	SERVICE	PORT	ENCRYPTION	CHECKSUM	CID	SID	CLIENT_VER	CLIENT_CHARSET	AUTH_TYPE	OCI_LIBRARY	SERIAL#
TCP	DEDICATED	SYS\$USERS	0	NONE	NONE	3	211	23.26.0.00.00	Unknown	DATABASE	Unknown	17301
TCP	DEDICATED	freepdb1	50770	AES128	SHA384	3	178	19.23.0.0.0	US7ASCII	INTERNAL	Full Instant Client	60970
TCP	SHARED	freeXDB	50764	NONE	NONE	1	210	19.23.0.0.0	WE8MSWIN1252	INTERNAL	Full Instant Client	43111
TCP	DEDICATED	SYS\$USERS	0	NONE	NONE	1	212	23.26.0.00.00	Unknown	DATABASE	Unknown	42757
TCP	DEDICATED	freepdb1	13432	AES192	SHA1	3	52	23.26.0.00.00	US7ASCII	INTERNAL	Home-based	48044
TCP	DEDICATED	freepdb1	55638	AES192	SHA1	3	206	18.5.0.0.0	AL32UTF8	INTERNAL	Full Instant Client	46659
TCP	DEDICATED	freepdb1	51163	NONE	NONE	3	16	19.23.0.0.0	US7ASCII	INTERNAL	Full Instant Client	43910
TCP	SHARED	freeXDB	50765	NONE	NONE	1	43	19.23.0.0.0	WE8MSWIN1252	INTERNAL	Full Instant Client	4386
TCP	DEDICATED	freepdb1	49793	AES192	SHA256	3	204	19.23.0.0.0	US7ASCII	INTERNAL	Full Instant Client	12824
TCP	DEDICATED	freepdb1	51166	NONE	NONE	3	215	19.23.0.0.0	US7ASCII	INTERNAL	Full Instant Client	22026

DBUSER	OSUSER	MACHINE	LOGON_TIME	STATUS	PROGRAM	MODULE	ACTION	CLIENT_INFO	CLIENT_CON_STRING
SYS	oracle	new-host-41	04.04.2026 18:49:17	ACTIVE	oracle@new-host-41 (J001)	DBMS_SCHED	ORACLE_APE		
SYS	myuser	mymachine	04.04.2026 18:11:49	INACTIVE	plsqldev.exe	PL/SQL Dev	SQL Window		(DESCRIPTION=(ADDI
SYS	myuser	mymachine	04.04.2026 18:11:10	INACTIVE	plsqldev.exe	PL/SQL Dev	Primary Se		(DESCRIPTION=(ADDI
	oracle	new-host-41	04.04.2026 18:51:25	ACTIVE	oracle@new-host-41 (J002)				
SYS	oracle	new-host-41	04.04.2026 12:00:17	INACTIVE	sqlplus@new-host-41 (TNS	sqlplus@ne			(DESCRIPTION=(CONI
SYS	myuser	mymachine	04.04.2026 18:02:40	INACTIVE	sqlplus.exe	sqlplus.ex			(DESCRIPTION=(CONI
SYS	myuser	mymachine	03.04.2026 18:12:57	INACTIVE	plsqldev.exe	PL/SQL Dev	Primary Se		(DESCRIPTION=(ADDI
SYS	myuser	mymachine	04.04.2026 18:11:16	ACTIVE	plsqldev.exe	PL/SQL Dev	SELECT * F		(DESCRIPTION=(ADDI
SYS	myuser	mymachine	04.04.2026 10:52:54	INACTIVE	plsqldev.exe	PL/SQL Dev	SQL Window	Example	(DESCRIPTION=(ADDI
SYS	myuser	mymachine	03.04.2026 18:13:09	INACTIVE	plsqldev.exe	PL/SQL Dev	SQL Window		(DESCRIPTION=(ADDI

What can go wrong... Connection Errors

```
SQL> connect sys/oracle@192.168.0.100:1521/freepdb1 as sysdba  
ERROR:  
ORA-28041: authentication protocol internal error
```

```
SQL> connect sys/oracle@192.168.0.100:1521/freepdb1 as sysdba  
ERROR:  
ORA-12699: Native service internal error occurred.
```

ORA-28041

authentication protocol internal error

Cause Authentication protocol failed with an internal error.

Action Contact Oracle Support Services.

ORA-12699

Native service internal error occurred.

Cause An internal error occurred in the native services component.

Action Enable tracing to determine the exact error. Contact Oracle Support.

Client Version 23.5.0.24.07 => Fixed with 23.26.xx

War Story: Stealth Mode



Ping? No Pong.

SYN = Attack

A-Queue dead.

THANK YOU VERY MUCH!

martin.klier@performing-db.com

axel.vomstein@bss.gmbh

Further reading

<https://docs.oracle.com/en/database/oracle/oracle-database/21/netrf/database-net-services-reference.pdf>