Using Oracle Data Guard ® with Cisco Wide Area Application Services for Data Center Replication

Oracle Data Guard is one of the most effective and comprehensive data protection and disaster recovery solutions available for enterprise data. The solution offers protection for Oracle Databases, providing customers the ability to protect business data.

Challenges encountered with latency, packet loss, and constrained bandwidths when deploying Oracle Data Guard over a WAN can still limit performance. This is usually unacceptable for data center to data center replication, which often involves large volumes of business application data and time-sensitive service level agreements (SLAs) such as RPO and RTO.

Cisco Wide Area Application Services (WAAS) optimizes the performance of many different applications by transparently mitigating certain network constraints. The Cisco WAAS supports optimizing data center to data center replication. With Cisco WAAS, Oracle Data Guard can transport redo logs much faster and more efficiently to meet SLAs without costly network upgrades.

The following sections are discussed:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Purpose

This document illustrates how Cisco WAAS optimizes Oracle Data Guard redo transport services by providing configuration examples and test results derived from experiments conducted with Data Guard and Cisco hardware and software. Only wide area latency and packet loss rates are simulated. Product information and additional technical details outside the scope of this paper are covered in the references listed at the end.

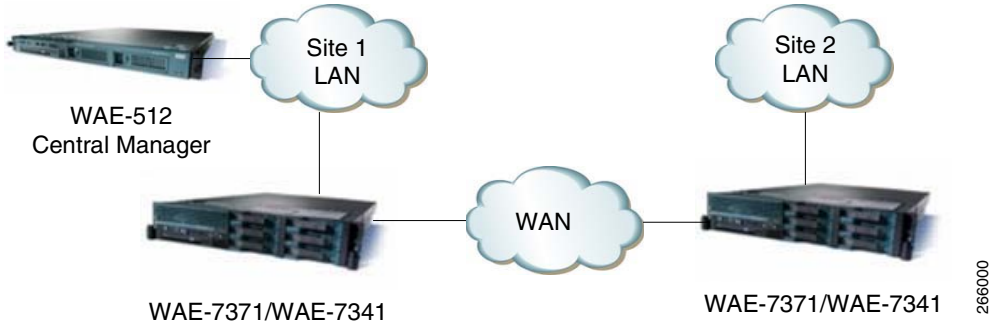
Intended Audience

This document contains technical information of interest primarily to Oracle Database Administrators and Network Administrators whose companies use Oracle Data Guard to replicate data between geographically dispersed data centers. This paper assumes a basic familiarity with Oracle Data Guard and no familiarity with Cisco WAAS on the reader's part.

What is Cisco WAAS?

The Cisco WAAS solution typically consists of at least three Wide Area Application Engines (WAEs) running Cisco WAAS software. Figure 1 depicts the solution at a high level and shows the High-Level WAAS Network Topology.

Figure 1 High-Level WAAS Network Topology



One WAE has to be configured as Central Manager (CM) device mode, which provides a management GUI, among other services. At least two additional WAEs, one in each site, examine traffic flowing through them and use built-in replication policies to determine whether to optimize the traffic or allow it to pass through the network natively.

The three basic optimizations include the following:

- Data Redundancy Elimination (DRE)
- Lempel-Ziv (LZ) compression
- Transport Flow Optimizations (TFO)

DRE is an advanced form of network compression that reduces the amount of data to be transmitted. DRE maintains an application-independent history of previously-seen data from TCP byte streams. This enables transmission of a unique block of data only once; after that, only a reference to that block is transmitted.

LZ compression applies the well-known Lempel-Ziv lossless compression algorithm to the DRE-optimized data to shrink it even further. In particular, LZ compression effectively shrinks the data that DRE was not able to compress due to seeing it for the first time.

Finally, TFO sends the twice-compressed data using a robust TCP proxy with advanced TCP window sizing and scaling, congestion management, and packet loss recovery techniques.

The net effect of DRE, LZ, and TFO is a decrease in the amount of bandwidth used along with better utilization of that bandwidth with only a small increase in latency due to processing in the WAE.

Effect of Cisco WAAS on Network Traffic

Network traffic flow depends on whether WAEs are deployed inline or with various interception and redirection methods. With the inline deployment, the WAE interface connects directly to a LAN-facing network device on one side so that traffic can flow through the WAE. A "fail to wire" mechanism allows traffic to keep flowing natively if a WAE stops operating for some reason. The inline deployment option is not available for the WAE network module.

An alternative to inline deployment is an interception method like Web Cache Communication Protocol version 2 (WCCPv2) or policy-based routing (PBR), which can identify and redirect traffic through the WAE. WCCPv2 uses Generic Route Encapsulation (GRE) tunnels for redirection by default in case the intercepting network device and the WAE are not in the same Layer 2 domain. If they are on the same domain, WCCPv2 can redirect traffic by rewriting frame header address fields in a process called Layer 2 redirection (L2-redirect). WCCPv2 redirection provides automatic load-balancing, fail-over, and fail-through operation when redundant WAEs are deployed.

Once the WAEs are in the data path, Cisco WAAS is transparent, meaning it does not use tunnels or require host or application configuration changes. When an end node in one site establishes a connection with an end node in the other site using the TCP three-way handshake, the WAE devices in each site automatically discover each other. The WAEs do this by marking the handshake packets with TCP option 0x21 to signal the peer WAE to establish an optimization session. Subsequent packets do not have this option added. The end nodes see the option on the SYN packets but ignore it. They do not see the option on the SYN-ACK packets, since the origin WAE remove its before forwarding packets to the source node.

To handle cases where a peer WAE fails for some reason, after auto-discovery is complete, each WAE increments the sequence number by 2,147,483,648 (0x8000000) on packets going to the peer WAE and decrements it by the same amount on packets going to the end node for each TCP flow. If a WAE fails, an end node sees a jump in the sequence number which causes it to reset the connection. In this case, the application has to reestablish a TCP connection, which then passes through the remaining WAE unoptimized. Optimization resumes for TCP connections established after the WAE is restored to service.

Table 1 shows an actual network trace between a source host, with an IP address of 101.1.33.17, and a destination host, with an IP address of 201.1.33.17, which illustrates the concepts above. The shaded rows are from a trace taken in the network between the two WAEs. The unshaded rows are from a trace on the source host. The asterisk represents packets where the TCP option 0X21 is present.

Table 1 Oracle Data Guard and Cisco WAAS Network Trace

No.	Source	Destination	Src Port	Dest Port	TCP Flags	Seq.	Ack.
1	101.1.33.17	201.1.33.17	33938	1521	SYN	0	N/A
*1	101.1.33.17	201.1.33.17	33938	1521	SYN	0	N/A
2	201.1.33.17	101.1.33.17	1521	33938	SYN, ACK	0	1
*2	201.1.33.17	101.1.33.17	1521	33938	SYN, ACK	0	1
3	101.1.33.17	201.1.33.17	33938	1521	ACK	1	1
*3	101.1.33.17	201.1.33.17	33938	1521	ACK	2147483649	2147483649
*4	101.1.33.17	201.1.33.17	33938	1521	PSH, ACK	2147483649	2147483649
4	101.1.33.17	201.1.33.17	33938	1521	PSH, ACK	1	1
5	101.1.33.17	201.1.33.17	33938	1521	PSH, ACK	2147483659	2147483649
5	201.1.33.17	101.1.33.17	1521	33938	ACK	1	57
6	201.1.33.17	101.1.33.17	1521	33938	ACK	2147483649	2147483659
6	201.1.33.17	101.1.33.17	1521	33938	PSH, ACK	1	57
7	201.1.33.17	101.1.33.17	1521	33938	PSH, ACK	2147483649	2147483659
7	101.1.33.17	201.1.33.17	33938	1521	PSH, ACK	57	57
8	101.1.33.17	201.1.33.17	33938	1521	ACK	2147483725	2147483659
8	201.1.33.17	101.1.33.17	1521	33938	ACK	57	89
9	201.1.33.17	101.1.33.17	1521	33938	PSH, ACK	2147483659	2147483725
9	201.1.33.17	101.1.33.17	1521	33938	PSH, ACK	57	89
10	101.1.33.17	201.1.33.17	33938	1521	ACK	2147483725	2147483747
10	101.1.33.17	201.1.33.17	33938	1521	PSH, ACK	89	93
11	101.1.33.17	201.1.33.17	33938	1521	PSH, ACK	2147483725	2147483747
11	201.1.33.17	101.1.33.17	1521	33938	ACK	93	129
12	201.1.33.17	101.1.33.17	1521	33938	ACK	2147483747	2147483775
12	101.1.33.17	201.1.33.17	33938	1521	ACK	129	93

Notice the sequence number jump in the third WAN packet which the controller never sees. The fourth WAN packet is not a retransmission; it contains ten bytes of control information that the peer WAE does not pass along to the destination controller.

How Does Cisco WAAS Optimize Oracle Data Guard?

Prior to Cisco WAAS software version 4.0.19, only two device modes, Central Manager (CM) and Application Accelerator (AA), were available. AA mode is designed to accelerate user applications with a large number of short lived TCP connections between the data center and branch locations. In contrast, replication applications like EMC SRDF and NetApp SnapMirror typically use a relatively small number of block-mode replication connections over the higher bandwidths and relatively lower WAN latencies usually found between data centers. To accommodate such replication applications, Cisco introduced the

Replication Accelerator (RA) device mode with version 4.0.19. While the function of Data Guard is replication, AA mode rather than RA mode is used. This is because the Data Guard replication transmits archive log files to replicate between sites and does not send block level replication data.

The WAEs look for packets destined for SQL traffic on port 1521, where Database redo log files traffic is configured, and apply all possible optimizations to the traffic. The customer can customize this default port configuration.

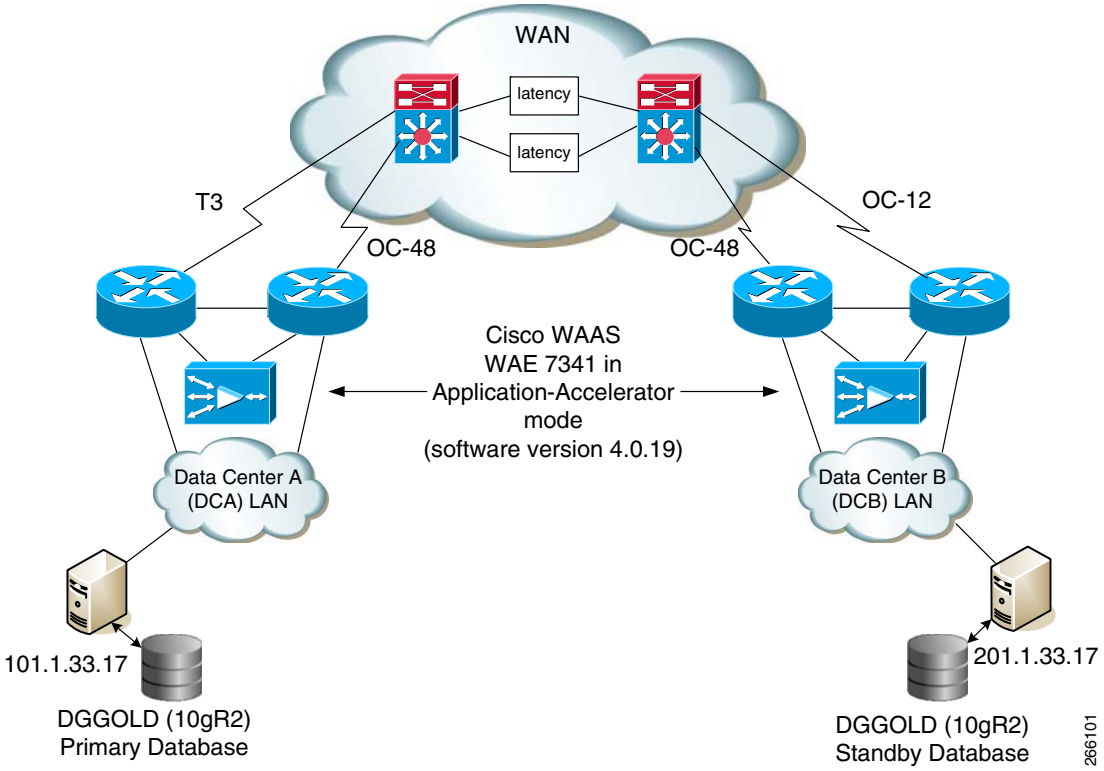
For optimization to occur, the WAEs must see the SYN packets at the start of each TCP session. This is not a problem for Data Guard, which, by default, starts a new session for each new log file that is replicated, regardless of whether the previous session is still transferring data or not. Each of these new sessions is a new TCP connection.

Oracle Data Guard and Cisco WAAS Test Topology

To illustrate how Cisco WAAS optimizes Oracle Data Guard traffic, Cisco had set up a test environment to emulate a production data center environment as closely as possible. The environment models two data centers connected by a wide area network (WAN). Each data center has the following equipment:

- Cisco WAE-7341 appliance running Cisco WAAS software version 4.0.19.
- Data center local area network (LAN) consisting of Cisco Catalyst 6500 switches.
- Data center storage area network (SAN) consisting of Cisco MDS 9500 switches.
- Inter-data center WAN consisting of Cisco Catalyst 6500s with T3, OC-12 and OC-48 links.
- WAN interfaces as well as latency and packet loss generators using Linux Netem.

Figure 2 Oracle Data Guard and Cisco WAAS Network Topology



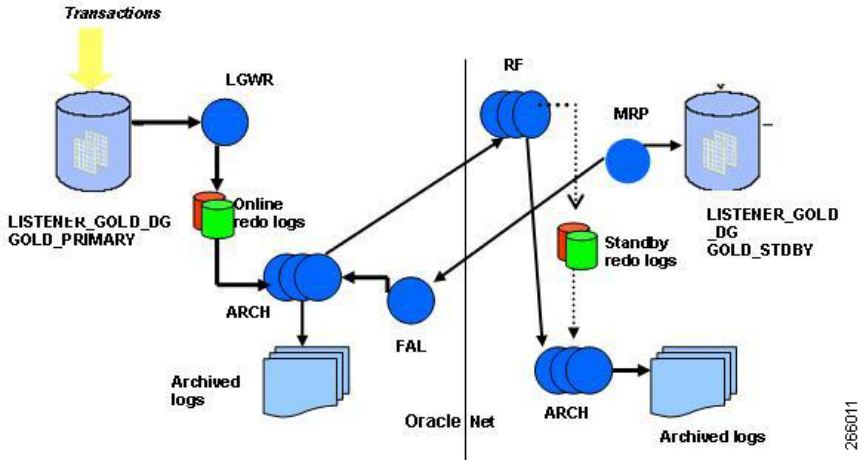
Oracle Data Guard Architecture and Configuration

Table 2 lists the hardware and software components used in the test topology

Table 2 Topology Hardware and Software Components

Component	Version
Oracle Database	10.2.0.3 64-bit
Operating System	RedHat ES 4 Update 4
Primary Host	Location : Datacenter A (101.1.33.17)
Standby Host	Location: Datacenter B (201.1.33.17)

Figure 3 Data guard Architecture



As the primary database processes transactions, the ARCH process on the primary database is configured to transmit the redo data to the standby in Async mode. On the standby, one or more RFS processes are used to receive redo data and the MRP process applies the redo data to the standby. The primary database also has the *Fetch Archive Log (FAL)* process to provide a client-server mechanism for transmitting archived logs to the standby following a communication loss between the primary and standby for automatic gap resolution and resynchronization.

The following section highlights the Initialization Parameters specific to the Oracle Data Guard configuration on the primary database.

Primary Database init.ora

```
instance_name = DGGOLD
DB_UNIQUE_NAME = 'DGGOLD_primary'
_LOG_ARCHIVE_CALLOUT='LOCAL_FIRST=TRUE'
##COMMON TO BOTH PRIMARY AND STANDBY ROLES
log_archive_config ='DG_CONFIG=(DGGOLD_primary,DG GOLD_stdby)'
log_archive_dest_1='LOCATION=/oracle/archive/DGGOLD/DGGOLD.arch VALID_FOR=(ALL_LOGFILES,
ALL_ROLES) DB_UNIQUE_NAME=DGGOLD_primary'
log_archive_dest_2='SERVICE=DGGOLD_stdby ARCH VALID_FOR=(ONLINE_LOGFILES, PRIMARY_ROLE)
DB_UNIQUE_NAME=DGGOLD_stdby max_connections=4 delay=05'
log_archive_dest_state_1=enable
log_archive_dest_state_2=enable
log_archive_max_processes=20
log_archive_format='%t_%s_%r.dbf'
remote_login_passwordfile=EXCLUSIVE
#SPECIFIC TO STANDBY ROLE
FAL_CLIENT=DGGOLD_primary
FAL_SERVER=DGGOLD_stdby
standby_archive_dest=/oracle/archive/DGGOLD/DGGOLD.arch
standby_file_management=auto
```

Note Values for **log_archive_max_processes, max_connections** and **delay** are just recommended values to handle redo generation of 28MB/sec and can be changed as applicable to the customer environment based on the amount of generated redo.

The following section highlights the Initialization Parameters specific to Oracle Data Guard configuration on the standby database.

Standby init.ora

```
instance_name =DGGOLD
DB_UNIQUE_NAME  = 'DGGOLD_stdby'
log_archive_config ='DG_CONFIG=(DGGOLD_primary, DGGOLD_stdby)'
log_archive_dest_1='LOCATION=/oracle/archive/DGGOLD/DGGOLD.arch VALID_FOR=(ALL_LOGFILES,
ALL_ROLES) DB_UNIQUE_NAME=DGGOLD_stdby'
log_archive_dest_2='SERVICE=DGGOLD_primary VALID_FOR=(ONLINE_LOGFILES, PRIMARY_ROLE)
DB_UNIQUE_NAME=DGGOLD_primary max_connections=4 delay=05'
log_archive_dest_state_1=enable
log_archive_dest_state_2=enable
log_archive_max_processes=20
log_archive_format='%t_%s_%r.dbf'
remote_login_passwordfile=EXCLUSIVE
```

Network Services Configuration

The TCP send/receive size is set to 4665000 (for improved efficiency in log shipping).

```
cat /proc/sys/net/core/wmem_max
cat /proc/sys/net/core/rmem_max
```

SDU = 32768 was added in tnsnames.ora in both the Primary and the DR. A separate listener for Data guard was configured.

On Primary: /etc/listener.ora

```
LISTENER_DGGOLD_DG =
 (DESCRIPTION_LIST =
  (DESCRIPTION =
   (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST =dcap-dca-oradb01)(PORT = 1521))
   )
  )
 )
SID_LIST_LISTENER_DGGOLD_DG =
 (SID_LIST =
  (SID_DESC =
   (SDU=32768)
   (SID_NAME = DGGOLD)
   (ORACLE_HOME = /oracle/product/10.2.0.2-64)
  )
 )
```

/etc/tnsnames.ora

```
DGGOLD_stdby,DGGOLD_stdby.cisco.com =
 (DESCRIPTION =
 (SDU = 32768)
  (ADDRESS_LIST =
    (ADDRESS =
     (PROTOCOL = TCP)
     (HOST =dcap-dcb-oradb01)
     (PORT = 1521)
    )
  )
  (CONNECT_DATA =
   (SERVICE_NAME = DGGOLD)
  )
)
```

On standby host: /etc/listener.ora

```
LISTENER_DGGOLD_DG =
 (DESCRIPTION_LIST =
  (DESCRIPTION =
   (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST =dcap-dcb-oradb01)(PORT = 1521))
   )
  )
 )
SID_LIST_LISTENER_DGGOLD_DG =
 (SID_LIST =
  (SID_DESC =
   (SDU=32768)
   (SID_NAME =DGGOLD)
   (ORACLE_HOME = /oracle/product/10.2.0.2-64)
  )
 )
DGGOLD_primary,DGGOLD_primary.cisco.com =
 (DESCRIPTION =
 (SDU = 32768)
  (ADDRESS_LIST =
    (ADDRESS =
     (COMMUNITY = cisco.com)
     (PROTOCOL = TCP)
     (HOST =dcap-dca-oradb01)
     (PORT = 1521)
    )
  )
  (CONNECT_DATA =
   (SERVICE_NAME = DGGOLD)
  )
)
```

Cisco WAAS Configuration

The test topology also features WAE-7341 devices in each data center. WCCPv2 with L2-redirect and GRE return perform traffic interception and redirection.

To support WCCPv2 interception and redirection, the network devices to which the WAEs are connected must be set up for WCCPv2. In the test topology, each WAN edge router has a configuration similar to the following:

WAN Edge Router Configuration for WCCPv2

```
!
ip wccp 61
ip wccp 62
!
interface POS2/2/0
 description WAN INTERFACE
 ip wccp 62 redirect in
end
!
interface TenGigabitEthernet1/1
 description LAN INTERFACE
 ip wccp 61 redirect in
end
!
interface Vlan81
 ip address 10.0.81.3 255.255.255.0
```

```
 standby timers 1 3
 standby 1 ip 10.0.81.1
 standby 1 priority 170
 standby 1 preempt delay minimum 1
!
```

The WAEs must be in AA mode to support Oracle Data Guard traffic. To verify the current mode, the following CLI command is used:

```
dca-wae-7341-1#show device-mode current
Current device mode: application-accelerator
```

The above output shows the WAE is in AA mode. Following are the relevant portions of the WAE configuration

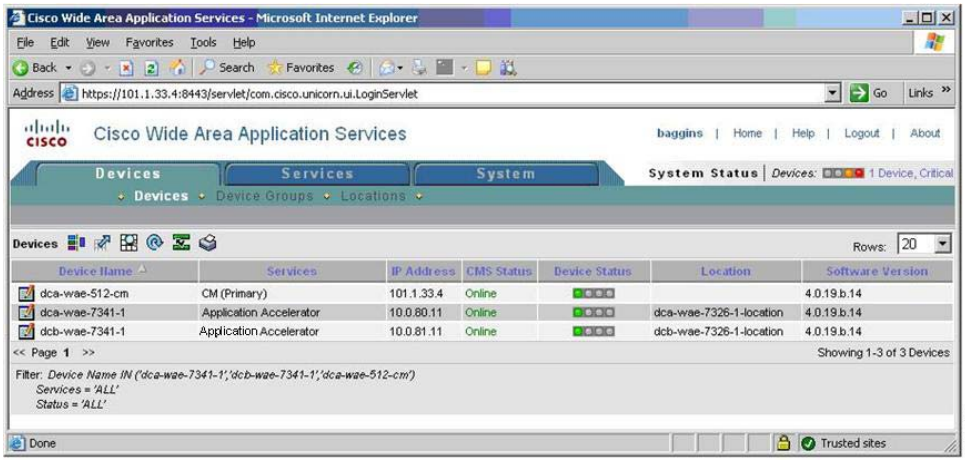
WAE Configuration

```
device mode application-accelerator
!
ip default-gateway 10.0.80.1
!
wccp router-list 1 10.0.81.2 10.0.81.3
!
wccp tcp-promiscuous router-list-num 1 l2-redirect mask-assign assign-method-strict
!
wccp version 2
!
policy-engine application
 name SQL
  classifier Oracle
   match dst port eq 1521
  exit
  map basic
   name SQL classifier Oracle action optimize full
  exit
exit
!
```

The **ip default-gateway** statement references the IP address of the Hot Standby Routing Protocol (HSRP) address shared by the WAN edge routers. The **wccp router-list** statement references the IP addresses of both local WAN edge routers. Together, the WCCPv2 configurations on the routers and WAEs allow the devices to negotiate the appropriate interception and redirection parameters. The policy map for SQL is configured to port 1521, by default, however this can be customized to a customer-specific configuration

Figure 4 shows the Cisco WAAS Central Manager GUI and the three WAE devices in the test topology. The WAE-7341 devices are called "dca-wae-7341-1" and "dcb-wae-7341-1." The Central Manager is called "dca-wae-512-cm."

Figure 4 Cisco WAAS Central Manager GUI



As soon as a Data Guard starts shipping archive logs, run the following CLI command on one of the WAEs to verify that it is optimizing the traffic.

```
dca-wae-7341-1# show tfo connection summary
Optimized Connection List
Policy summary order: Our's, Peer's, Negotiated, Applied
F: Full optimization, D: DRE only, L: LZ Compression, T: TCP Optimization
Local-IP:Port     Remote-IP:Port    ConId  PeerId       Policy
101.1.33.17: 60244  201.1.33.17:1521   127119  00:1a:64:26:e4:a0  F,F,F,F
101.1.33.17: 60243  201.1.33.17:1521   127118    00:1a:64:26:e4:a0  F,F,F,F
101.1.33.17: 60242  201.1.33.17:1521   127117  00:1a:64:26:e4:a0  F,F,F,F
```

This **show** command displays all of the connections that are optimized by the WAE. A table displays the tuple information, internal connection ID, peer WAE ID and policy. The "F,F,F,F" means the WAE is fully optimizing Data Guard traffic at ports 1521 from IP addresses 101.1.33.17 (Primary Database host) and 201.1.33.17 (Standby Database host).

Test Methodology

Each test consisted of replicating Oracle archive log files using Data Guard with and without Cisco WAAS, and then comparing the time taken for shipping the log files from primary database to standby database, which was the key metric.

Tests were conducted for T3 (45Mbps) and OC12 (622Mbps) bandwidths using latencies of 4ms, 68ms and 380ms. Latencies were simulated using Linux Netem. Application data changes are generated using a custom program such that the redo log generation rate was maintained at a rate of 28MB/sec. Each of the tests was run for a 30-minute interval which resulted in about 50GB worth of archive log files. The standby database was shutdown while the logs on the primary database were generated. At the end of each 30-minute interval, the standby database was restored for archive log shipping.

Test Results

In all tests, WAAS dramatically increased throughput and reduced the number of packets and amount of data that had to be sent over the network. Redo log generation was maintained at a rate of 28MB/sec. Table 3 summarizes the results of all the tests.

Table 3 Test Result Summary

Latency	Bandwidth	Log Shipping Native (Minutes)	Log Shipping With WAAS (Minutes)	%Improvement with log shipping	Throughput Improvement
4ms	T3 (45Mbps)	140	45	67.8%	82%
68ms	T3 (45 Mbps)	180	58	67%	83%
380ms	T3 (45Mbps)	230	115	50%	84%
68ms	OC12(622Mbps)	40	29	27.5%	83%
380ms	OC12(622Mbps)	180	140	50%	83%

The following charts illustrate the findings graphically.

Figure 5 and Figure 6 show comparisons of log shipping improvements for Data Guard traffic when WAAS was enabled.

Figure 5 Data Guard traffic with T3 (45Mbps) for Varying Latencies

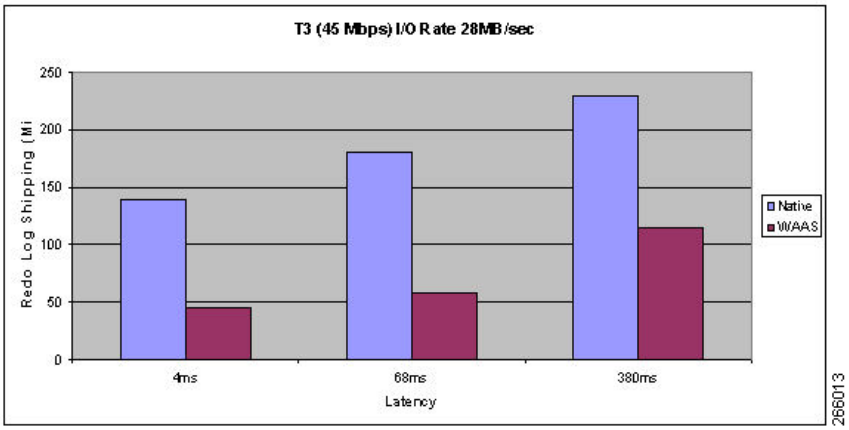
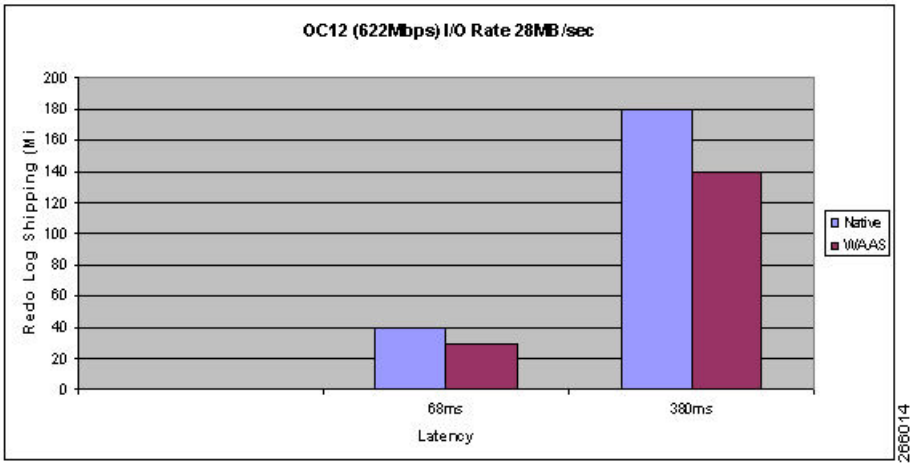
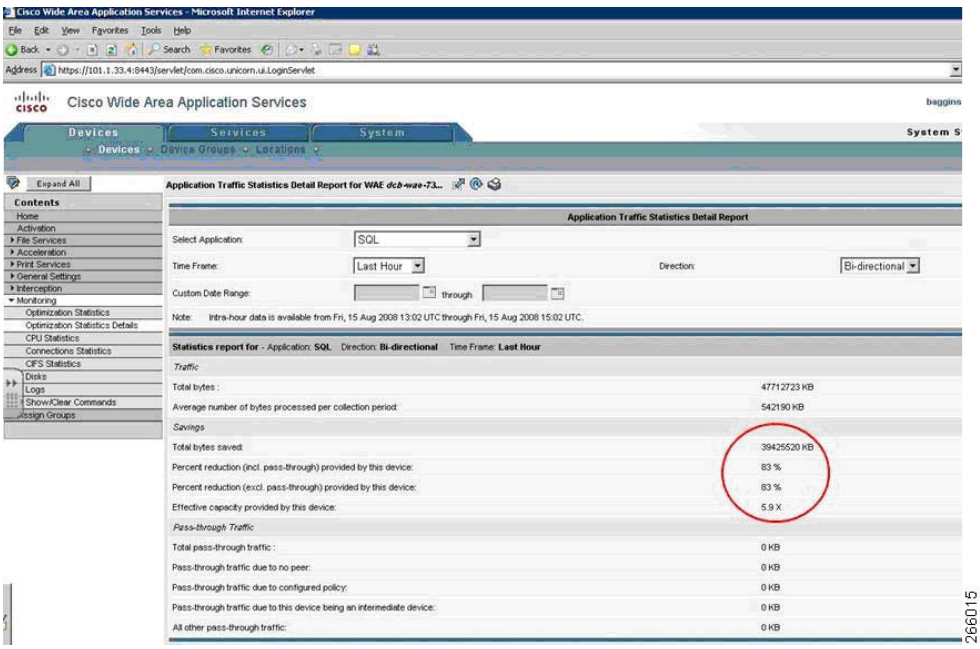


Figure 6 Data guard Traffic with OC12 (622Mbps)



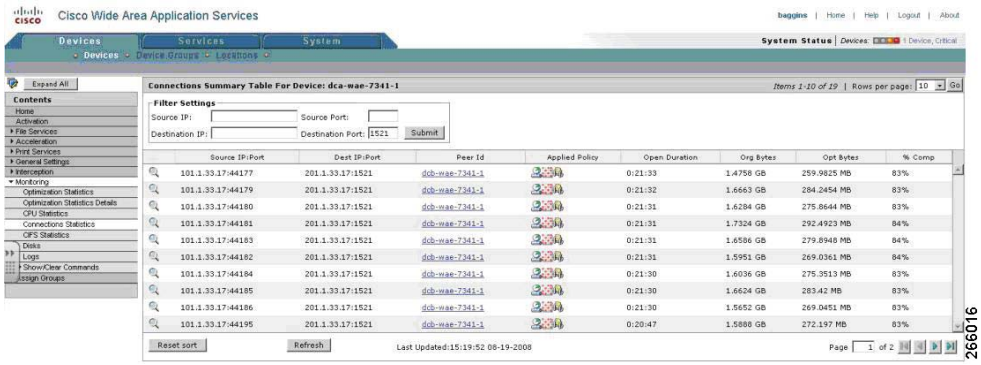
From a WAAS point of view, many statistics are available for the Network Administrator to track the statistics. The following highlights the various statistics captured from the CM GUI and WAE CLI. For example, Figure 7 shows a portion of the CM GUI showing the Optimization Statistics screen.

Figure 7 Cisco WAAS CM Optimization Statistics



In Figure 8, the WAAS Central Manager shows that Cisco WAAS reduced the SQL traffic by 83%. Note that none of the SQL traffic passed through the device natively; it was all optimized.

Figure 8 Cisco WAAS TFO optimization statistics



The WAAS Central Manager shows each SQL TCP connection being reduced by WAAS by 83% to 84%.

Summary

The test results reported in this white paper demonstrate how well Oracle Data Guard and Cisco WAAS in Application Accelerator mode can work together to improve replication performance and reduce network resource requirements. Once configured, Cisco WAAS is completely transparent to Data Guard traffic. Together, Oracle Data Guard and Cisco WAAS ensure customers' objectives of maintaining Recovery Point and Recovery Time Objectives across a wide range of network environments.

References

The following Oracle and Cisco reference material is available online.

Oracle Reference Documents

1. Creating a 10g Data Guard Physical Standby on Linux (Metalink Noteid : 248382.1)
2. Oracle Data Guard Failover and Switchover best practices (Metalink Noteid: 271448.1)
3. MAA Data Guard Redo Transport and Network Best Practices 10gR2. (Metalink Noteid: 387174.1)
4. Oracle Data Guard Overview

   http://www.oracle.com/technology/deploy/availability/htdocs/Data GuardOverview.html

Cisco Reference Documents

1. Enterprise Data Center Wide Area Application Services (WAAS) Design Guide

   http://www.cisco.com/application/pdf/en/us/guest/netsol/ns377/c649/ccmigration_09186a008081c7da.pdf
2. Cisco Wide Area Application Services Configuration Guide (Software Version 4.0.19)

   http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/configuration/guide/waas4cfg.html
3. Release Note for Cisco Wide Area Application Services (Software Version 4.0.19)

   http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/release/notes/ws4019rn.html

4. Cisco WAAS Optimizations for Data Protection Applications

   http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6870/prod_white_paper0900aecd8051c0a6.pdf

5. Cisco Wide Area Application Services (WAAS) V4.0 Technical Overview

   http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6870/prod_white_paper0900aecd8051d5b2.html