StorageTek Virtual Library Extension

Planning Guide

Release 1.5

E57765-09

February 2019

ORACLE®

StorageTek Virtual Library Extension Planning Guide, Release 1.5

E57765-09

Contents

3 VLE Planning

List of Figures

List of Tables

Preface

This preface introduces the planning guide for Oracle's StorageTek Virtual Library Extension (VLE).

Audience

This publication is intended for Oracle or customer personnel responsible for doing site planning for Oracle's StorageTek Virtual Library Extension (VLE).

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit
`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Supplementary VLE Documents

You are entitled to the following supplementary documents:

- *VLE SLA and Standard Firmware Entitlement*
- *Licensing Information User Manual*
- *Written Offer to Provide Certain Source Code*
- *VLE Safety Guide*

1 Introduction

This chapter introduces Oracle's StorageTek Virtual Library Extension (VLE) software and describes the components included in a typical VLE configuration. VLE is back-end disk storage for VTSS. The VLE solution consists of:

- Virtual Tape Storage Subsystem (VTSS) hardware and microcode
- Virtual Tape Control Subsystem (VTCS) software and Storage Management Component (SMC)
- VLE hardware and software
- On-demand capacity, scales-to-petabytes
- Multiple redundant copies of data for the highest availability
- All data can be encrypted at rest for security
- Automatic data integrity checks for durability
- Industry standard APIs at REST
- Support for Migrating and Recalling Virtual Tape Volumes (VTVs) to, and from Oracle Archive Cloud

To VTCS, a VLE looks like a tape library except that the VTVs are stored in Virtual Multi-Volume Cartridges (VMVCs) on disk. With VLE, you can configure either a VLE and tape or a VLE only (for example, with Tapeless VSM configurations) back-end VTV storage solution. A VTSS can migrate VTVs to and recall them from a VLE, just as is done with a real tape library.

Caution:

- If you have a VLE system, HSC/VTCS uses SMC communication services to communicate with the VLE. To ensure that these services are available during VTCS startup, Oracle recommends that you first issue the start command for HSC, then immediately issue the start command for SMC, while HSC is initializing.
- Stopping SMC stops VTCS from sending messages to the VLE, which effectively stops data transfer. Therefore, you should ensure that VTCS activity is quiesced or VTCS is terminated before stopping SMC.
- You cannot use AT-TLS with the SMC HTTP server if you are using VLE.
- Tapeless VSM configurations, if you have only a single-node VLE attached to a specific VTSS and that VLE goes offline.Loss of access to any VTVs migrated to the VLE (not resident in the VTSS) until the VLE comes back online.

See the following sections for further information:

- "What's New for VLE 1.5.3"
- "Supported Platforms"
- "VLE Hardware and Software"
- "Single Node VLE Configuration"
- "Multi-Node VLE Systems"
- "VLE-to-VLE Data Transfer"
- "VTV Encryption"
- "VTV Deduplication"
- "Frame Size Control"
- "Oracle Cloud Extended Storage"

What's New for VLE 1.5.3

VLE 1.5.3 provides:

- Support for 400 MB, 800 MB, 2 GB, 4 GB, and 32 GB VTV
- An additional storage tier in the VSM solution. VTVs can now migrate from VTSS to VLE to provide fast access to recent data. Additionally, VTVs can transition from VLE storage to tape media (MVCs) for long term archive. You can control how VTVs are migrated and archived through the existing HSC Management and Storage Classes, providing full backward compatibility with previous configurations
- Back-end disk storage shared between multiple VTSS systems, ensuring high-availability access to data
- Oracle Cloud Encryption

Note: For VLE 1.1 and higher, a "VLE" is a collection of nodes interconnected with a private network.

Refer to http://docs.oracle.com/cloud/latest/storagecs_common/index.html for further information on setting up a Cloud account, or "Network Requirements for Cloud Extended Storage."

Supported Platforms

VLE 1.5.3 has been tested with a very specific configuration. Using anything other than the approved configuration is not supported.

Note: VLE 1.5.3 software works on both the old and new versions of the hardware stack. Within a single VLE cabinet, there can be no mixing of components.

Stacks may be combined together, such as a VLE with the J4410 JBODS, then by a VLE with the DE2-24C JBODs, thereby, making a multi-node VLE.

VLE Hardware and Software

The VLE, which is a factory-assembled unit in a Sun Rack II Model 1242, includes the following hardware:

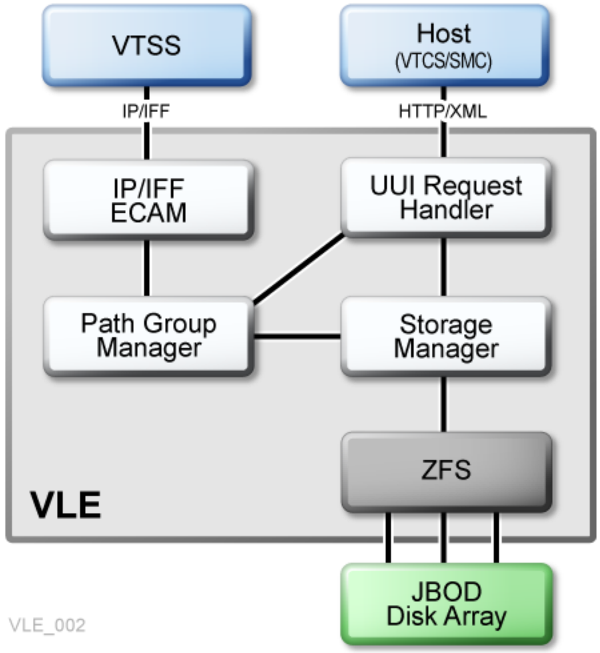
- A server built on a Sun Server X4-4 platform
- Four motherboard 10 Gb ports, two of which can be used for data transfer and other purposes. Two are dedicated for management, service, and support
- A service (ILOM) port
- Four dual port 10 Gb Fibre Optic network cards (six ports available) plus two 10 Gb Copper ports
- One or more Oracle Storage Drive Enclosure DE2-24Cs (DE2-24C) that contain disk (HDDs) in a ZFS RAID array, scalable in effective capacities starting at 200 TB for a single JBOD VLE (assuming a 4 to 1 compression ratio when the data is migrated to the VLE)
- A DVD drive

The VLE software consists of:

- Oracle Solaris 11 Operating System
- ZFS file system and MySQL database
- The VLE application software

Figure 1–1 shows the VLE subsystem architecture

Figure 1–1 VLE Subsystem Architecture



As Figure 1–1 shows, the VLE application software consists of:

- HTTP/XML is the data protocol for host-to-VLE communications.
- The Universal User Interface (UUI) Request Handler, which processes UUI requests from, and produces responses to Storage Management Component (SMC) and Virtual Tape Control Software (VTCS). The UUI Request Handler determines which VLE components are used to service a request.

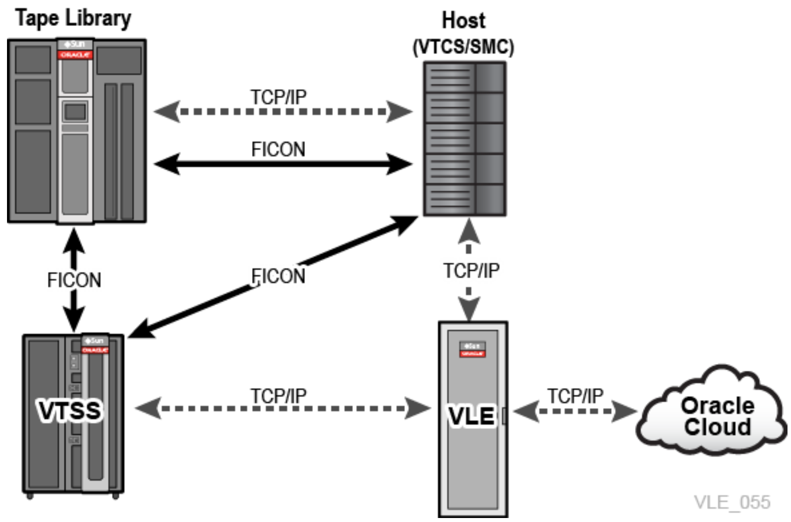
  UUI Request Handler calls:

  – The PathGroup Manager to schedule VTV migrates and recalls. The PathGroup Manager manages all Path Groups, where each Path Group manages a single VTV data transfer between the VTSS and the VLE.
  – The Storage Manager to schedule all report generation.
- The VLE Storage Manager component manages the VMVC/VTV data and meta data on the VLE. The VLE Storage Manager stores VTV data on and retrieves it from the ZFS on the JBOD array.
- TCP/IP/IFF is the data protocol for host to VLE communications, where the IP/IFF/ECAM component handles communications between the VTSS and the VLE.

Single Node VLE Configuration

Figure 1–2 shows a single node VLE configuration.

Figure 1–2 Single Node VLE in a VSM System



As Figure 1–2 shows (where 1 is the MVS host and 2 is the library):

- Multiple TCP/IP connections (between the VTSSs' IP ports and the VLEs' IP ports) are supported, as follows:
  - A single VLE can connect up to 8 VTSSs, so VTSSs can share VLEs.
  - A single VTSS can connect to up to 4 VLEs to increase buffer space for heavy workloads.
- A single VTSS can be attached to:
  - Only RTDs
  - Only other VTSSs (clustered)
  - Only VLEs
  - Any combination of the above
- TCP/IP is the only supported protocol for connections between the VLE and the VTSS and for connections between the VLE and hosts running SMC and VTCS.

Multi-Node VLE Systems

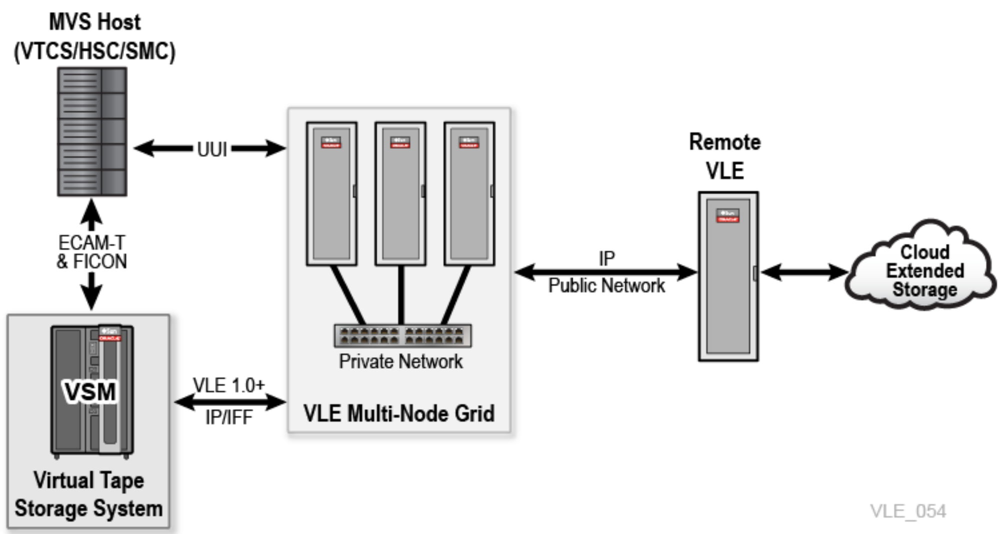
Multi-node VLE systems enable massive scaling of the VLE storage system. You can construct multi-node systems that consist of one to 64 nodes, with multiple nodes interconnected by a private network. A multi-node VLE appears to SMC/VTCS as a single VLE. The VLE ships with 4 TB JBODs, so a single VLE can scale between 200 TB (for a one JBOD system) and 100 PB (for a fully populated 64-node VLE).

> **Note:** These are effective capacities, assuming 4:1 compression.VLE is **architected** for up to 64 nodes, but has only been **validated** for up to 16 nodes.

Figure 1–3 shows a VLE multi-node complex, where the nodes are cross-connected into a dedicated 10 GE switch so that each node can access any other node in the complex, as described in the figure below.

Note: A multi-node VLE can be any combination of 1.5.0, 1.5.1, 1.5.1.A1, 1.5.2, 1.5.2.A1 or 1.5.3 application code levels, but all nodes should be upgraded to 1.5.3 as soon as possible.

Figure 1–3 VLE Multi-Node Complex



Caution: It is recommended that all nodes be running at VLE 1.5.3 and not mixed between 1.5.0, 1.5.1, 1.5.1.A1, 1.5.2 or 1.5.2.A1 with 1.5.3, except during the time frame needed for upgrades.

VLE-to-VLE Data Transfer

The VLE storage system can manage data transfers independently of the VTSS, which frees VTSS resources for front-end (host) workload, which improves the overall VTSS throughput.

Example:

- If your migration policies specify that there should be two VLE copies of a VTV (either in the same or separate VLEs), then the first migration to a VLE will cause data to be transferred from the VTSS. All subsequent VLE migrations for the VTV may be achieved through a VLE to a VLE copy. This reduces the VTSS cycle times required to migrate all copies of a VTV.
- If your environment runs:
  - VLE 1.2 or higher
  - VTCS 7.1 (with the supporting PTFs) or VTCS 7.2 and higher

    You can use VTCS to define more VLE devices than there are VTSS-to-VLE paths through the `CONFIG STORMNGR VLEDEV` parameter. If you use this addressing scheme, then the VTSS resources used to migrate all of the VTV copies to VLE are reduced even further. This is because the path from the VTSS to the target VLE is only reserved when the data transfer is direct from the VTSS to the VLE. For all VLE VRTD actions, a path from the VTSS is only reserved when VTSS data transfer is required. This feature is referred to as Autonomous Device Support (ADS).

VTV Encryption

The encryption feature enables encryption of VMVCs written to the VLE system. Encryption is enabled on a *per node basis*, through an *encryption key* stored on the node, backed up on a USB device. Encryption is entirely managed through the VLE GUI; the host software has no knowledge of encryption, as the VLE de-encrypts VTVs that are recalled to the VTSS.

> **Note:** Encryption can only be enabled on an empty VLE, with no VMVC(s) defined. Enabling encryption on a VLE that already contains customer data cannot be done. Consequently, the decision whether to encrypt must be made during the planning stage of the VLE install.

When you first define new encrypted VMVCs, a USB stick must be present. The keys are backed up onto that USB stick. Before you define additional VMVCs, ensure that the original USB stick has been inserted, so that the old and new keys are synchronized and backed-up.

It is the responsibility of the customer to manage the USB stick as backup when creating encrypted VMVCs. Though you can create encrypted VMVCs without the USB stick being present, you will not be able to mount or read any of the VMVCs without the correct encryption key.

> **Note:** The USB stick should be formatted in FAT or FAT32 on a Windows workstation/server, prior to inserting it into a USB slot of a VLE so that the VLE will recognize it. NTFS and exFAT formatted USB sticks are not supported by VLE.

VTV Deduplication

Deduplication eliminates redundant data in a VLE complex. Deduplication, which is controlled by the `STORCLAS` statement `DEDUP` parameter, increases the effective VLE capacity, and is performed by the VLE before the VTV is written to a VMVC.

To assess deduplication results, enable deduplication, monitor the results with the `SCRPT` report, and fine tune deduplication as necessary. The `SCRPT` report provides the approximate “reduction ratio” for the deduplicated data, which is uncompressed GB divided by used GB. The Reduction Ratio, therefore, includes *both* VTSS compression *and* VLE deduplication. A larger reduction ratio indicates more effective compression and deduplication.

For example, the VTSS receives 16 MB of data, compresses it to 4 MB, and writes the compressed data to a VTV. VLE subsequently deduplicates the VTV to 2 MB and writes it to a VMVC. Thus, the reduction ratio is 16 MB divided by 2 MB, or 8.0:1.

Frame Size Control

Frame Size Control specifies the use of Jumbo Frames on each copy link:

> **Note:** The infrastructure between the VSM and VLE, or between VLEs, must support Jumbo Frames before this will work. If any portion of the infrastructure between these connections does not support Jumbo Frames, it will not work.

- If your TCP/IP network supports Jumbo Frames, enabling this option can improve network performance.
- You enable Jumbo Frames by selecting the `Jumbo Frames` check-box on the `Port Card Configuration Tab`. Selecting this check-box sets the MTU (Maximum Transmission Unit) value to 9000 for the port.
- It is recommended that Jumbo Frames be enabled on links that are set for VLE-to-VLE transfer.

Oracle Cloud Extended Storage

VLE 1.5.2 and higher offers connection from the VLE to the Oracle Cloud. VLE can be configured to optionally migrate and recall customer data directly to and from the Oracle Cloud. VLE configuration options support any combination of data storage in the local VLE disk pool and/or the Oracle Cloud. VLE supports three Oracle Cloud options: Oracle Cloud, Oracle Cloud (Archive), and Encryption within Oracle Cloud. See below for further explanation of the supported Oracle Cloud options.

Oracle's Cloud Extended Storage is an option that allows the customer additional storage capacity. Refer to `http://docs.oracle.com/cloud/latest/storagecs_common/index.html` for further information on setting up a Cloud account, or "Network Requirements for Cloud Extended Storage."

For information regarding metered and non-metered accounts, see:

- `http://docs.oracle.com/cloud/latest/trial_paid_subscriptions/CSGSG/toc.htm`
- For up-to-date Cloud information, see:

  `http://docs.oracle.com/cloud/latest/`
- For further assistance, see:

  `http://docs.oracle.com/cloud/latest/storagecs_common/index.html`

Oracle Storage Cloud Service – Object Storage

With support for VLE 1.5.2 and higher, storing data in the Oracle Storage Cloud - Object Storage is much like storing data in the VLE local disk pool. The following steps outline what is needed to configure a VLE for storing VTV in the Storage Cloud.

The information needed, is:

> **Note:** The Oracle CSE will need to retrieve the customer's Oracle Cloud account information to create the initial connection between the VLE and the Oracle Storage Cloud Service - Object Storage.

- Account Name
- User Name
- User Password
- Authorization URL

> **Note:** MVC ranges are determined by the customer. They are used to configure VTCS host software and given to the Oracle support team for configuration of the VLE.

If the VLE will store VTV data on its local disk pool as well as the Storage Cloud, there will be two VMVC pool ranges defined and configured in the VLE:

- A vMVC range for VLE local disk pool storage
- A vMVC range for the VLE Oracle Cloud storage

Once VMVC definitions are configured in the VLE, VTV Migrate, Recall, and VLE Copy operations can be expected to behave much the same as all VLE operations that use the VLE local storage pool.

> **Note:** The performance of VLE-to-Cloud data transfer performance is subject to IP bandwidth and delay, as well as the Storage Cloud performance capabilities.

Oracle Storage Cloud Service – Archive Storage

With support for VLE 1.5.3 and higher, storing data in the Cloud Archive is much like storing data in the VLE local disk pool, but there are some exceptions regarding a recall of data stored in the Oracle Storage Cloud Service – Archive Storage.

The steps for setting up a VLE for using the Oracle Storage Cloud Service – Archive Storage are similar to the steps for the Oracle Storage Cloud for Object Storage.

The information needed, is:

> **Note:** The Oracle CSE will need to retrieve the customer's Oracle Cloud account information to create the initial connection between the VLE and Oracle Cloud Archive. Cloud Archive account information is the same as Storage Cloud

- Account Name
- User Name
- User Password
- Authorization URL

MVC ranges are determined by the customer. They are used to configure VTCS host software and given to the Oracle support team for configuration of the VLE. The customer will need to provide up to three vMVC ranges when using Cloud Archive:

- A vMVC range for VLE local disk pool storage
- A vMVC range for the VLE Oracle Cloud storage
- A vMVC range for the VLE Oracle Cloud (Archive) storage

When creating vMVCs on the VLE the Oracle support person selects an 'archive' flag for vMVCs that will use Cloud Archive. This is what triggers the 'archive' functionality within the Oracle Cloud.

Once VMVC definitions are configured in the VLE, VTV Migrate, Recall, and VLE Copy operations are possible for all three vMVC ranges but there some exceptions for the Cloud Archive range of vMVCs.

Note: For a more in-depth discussion of Migrate, Restore and Recall, refer to the *Host Software Configuration Guide for Virtual Library Extension (VLE) 1.5.*

Migrate

VTV migrate operations perform the same as for VTVs migrated to VLE local disk pool or Oracle Storage Cloud Service – Object Storage. Once the VTV migrate to the Storage Cloud is complete, the VTV will immediately move to the Cloud Archive.

Note: With VTVs immediately moved to Archived status, users will be unable to immediately recall or use the VTV(s) as a source, for a VLE-to-VLE copy operation.

Recall

Once a VTV is moved to Cloud Archive after a migrate, it cannot be recalled until it has been restored (moved from the Cloud Archive to the Storage Cloud).

Restore

VTVs that are to be restored are identified by the customer and are manually (or host job) restored using a restore command via the SMC UUI interface.

Note: Oracle service level agreement (SLA) to restore a VTV is 4 hours. Multiple restore VTV commands can be initiated at the same time.

Query Restore can be issued to the VTVs that are in the restore process to get current progress (Complete, In progress). Restore operations within the Cloud Archive can be expected to behave much the same as all VLE operations that use the VLE local storage pool.

The performance of VLE-to-Cloud data transfer performance is subject to IP bandwidth and delay, as well as the Oracle Cloud performance capabilities.

Oracle Cloud Encryption (Support for VLE 1.5.3 and Higher)

The Oracle Storage Cloud Service – Object Storage and the Oracle Storage Cloud Service – Archive Storage support Encryption. Controlling Encryption in either of the Oracle Cloud offerings is controlled at the vMVC boundary, That is, if a vMVC is created with the Encryption flag set, all of the VTVs in that vMVC will be encrypted. Migrate and recall operations for encrypted VTVs behave exactly the same for each of the respective Clouds (Archive and non-archive), as described previously.

The only behavior difference is a performance decrease of 10% for encrypted VTVs. The steps for setting up the VLE for using the Oracle Cloud Encryption are very similar to steps described in "Oracle Storage Cloud Service – Object Storage" and "Oracle Storage Cloud Service – Archive Storage".

> **Note:** The Oracle CSE will need to customer Oracle Cloud account information to create the initial connection between the VLE and Oracle Cloud.

Archive Cloud account information is the same as Storage Cloud account information.

The information needed, is:

- Account Name
- User Name
- User Password
- Authorization URL

MVC ranges are determined by the customer. They are used to configure VTCS host software and given to the Oracle support team for configuration of the VLE. The customer will need to provide up to three vMVC ranges when using Oracle Cloud with Encryption :

- A vMVC range for VLE local disk pool storage
- A vMVC range for the VLE Oracle Cloud storage (with or without Encryption)
- A vMVC range for the VLE Oracle Cloud (Archive) storage (with or without Encryption)

> **Note:** When creating vMVCs on a VLE, an Oracle support person sets an encryption flag for any vMVCs that will contain encrypted VTVs.

Once VMVC definitions are configured in the VLE, VTV Migrate, Recall, and VLE Copy operations for Encrypted vMVCs behave exactly as described in "Oracle Storage Cloud Service – Object Storage" and "Oracle Storage Cloud Service – Archive Storage". The Oracle Cloud website can be reviewed for information pertaining to the Encryption feature as it is handled within the Oracle Cloud.

Customer Checklist: Setting Up VLE for Oracle Cloud Storage

Retrieve the following parameters at least one week prior, for the Oracle Field Engineer to be ready to setup VLE 1.5 to connect to Oracle Cloud Storage.

> **Note:** If these values are not readily available, setting up Cloud connectivity will be delayed until the values are available.

Table 1–1 Parameters for Cloud Connectivity

Value	Description	Comment
Oracle Cloud Storage Account	A valid Cloud Storage account, provided by Oracle. Customers should have received an email with account information	The Service Engineer will need the following details when setting up the VLE for Oracle Cloud: URL, Account Name, User Name and Password.

Table 1–1 (Cont.) Parameters for Cloud Connectivity

Value	Description	Comment
Dedicated Ethernet port on VLE	It is strongly recommended that one or more Ethernet ports on the VLE be dedicated to Cloud traffic.	The dedicated Ethernet ports should have connectivity to this subnet.
Dedicated Cloud subnet	A dedicated subnet, provisioned by customer's Information Technology (IT) Department, so Cloud data traffic can be routed through it.	The dedicated Ethernet ports should have connectivity to this subnet.
Static IP Address(es)	One or more valid IP address(es) provided by the Information Technology (IT) Department.	The IP addresses will be assigned to the Ethernet ports. If multiple Ethernet ports and a single IP address is desired, then the Ethernet ports will be aggregated.
Gateway, Network Number and Network Mask	Values to be used when setting the IP address, provided by the Information Technology (IT) Department.	These values should be readily available from the Information Technology (IT) Department.

2

Physical Site Planning

This chapter provides information about activities designed to ensure that the site is equipped to accommodate the power, safety, environmental, HVAC, and data handling requirements of VLE system equipment.

Key site readiness planning considerations include, but are not limited to:

- Site surveys to evaluate and eliminate or mitigate factors which could negatively affect delivery, installation, and operation of VLE system equipment.
- A plan for the layout and location of VLE system equipment and cabling that allows for efficient use and easy maintenance, plus adequate space and facilities for Oracle support personnel and their equipment.
- Facilities construction that provides an optimum operating environment for VLE system equipment and personnel, as well as safe flooring and protection from fire, flooding, contamination, and other potential hazards.
- Scheduling of key events and task completion dates for facilities upgrades, personnel training, and delivery, implementation, installation, testing, and certification activities.

Customers ultimately are responsible for ensuring that their site is physically prepared to receive and operate VLE system equipment, and that the site meets the minimum specifications for equipment operation as detailed in this guide.

Site Evaluation – External Considerations

Before delivery of VLE system equipment, a readiness planning team should identify and evaluate all external site factors that present existing or potential hazards, or which could adversely affect delivery, installation, or operation of the system. External factors that should be evaluated include:

- Reliability and quality of electrical power provided by the local utility, backup power generators, and uninterruptible power supplies (UPSs), and so on.
- Proximity of high-frequency electromagnetic radiation sources (for example, high-voltage power lines; television, radio, and radar transmitters).
- Proximity of natural or man-made floodplains and the resultant potential for flooding in the data center.
- Potential effects of pollutants from nearby sources (for example, industrial plants). For more information, see Appendix B, "Controlling Contaminants".

If any existing or potential negative factors are discovered, the site readiness planning team should take appropriate steps to eliminate or mitigate those factors before VLE system equipment is delivered. Oracle Global Services offers consultation services and other assistance to identify and resolve such issues. Contact your Oracle account representative for more information.

Site Evaluation – Internal Considerations

Before delivery of VLE system equipment, a readiness planning team should identify and evaluate all internal site factors that present existing or potential hazards, or which could adversely affect delivery, installation, or operation of the system. Internal factors that should be evaluated include:

- Structural dimensions, elevator capacities, floor-load ratings, ramp inclines, and other considerations when transferring equipment point-to-point between the delivery dock, staging area, and data center installation site, as described in:
  - "VLE Environmental Specifications"
  - "Requirements for Transferring the VLE Point-to-Point"
- "Requirements for Installing the VLE", which describes floor construction and loading requirements.
- Data center safety system design features and capabilities as described in "Data Center Safety".
- Site power system(s) design and capacity as described in "Site Power Distribution Systems"
- Data center HVAC design features and capabilities as described in "HVAC Requirements"
- Environmental requirements as described in:
  - "Environmental Requirements and Hazards"
  - Appendix B, "Controlling Contaminants"

If any existing or potential negative factors are discovered, the site readiness planning team should take appropriate steps to eliminate or mitigate those factors before VLE system equipment is delivered. Oracle Global Services offers consultation services and other assistance to identify and resolve such issues. Contact your Oracle account representative for more information.

VLE Environmental Specifications

The following sections discuss VLE environmental specifications.

> **Note:** Statistics for power and cooling data are approximate due to variations in data rates and the number of operations occurring.

Base Configuration

The base configuration consists of a Sun Server X4-4, with two 1.2 TB internal SAS drives, four dual port 10 Gb Fibre NICs and one dual port 10Gb Copper NIC, plus two available 10Gb ports on the motherboard, one DE2-24C populated with 24 4TB SAS HDD, and the SunRack II 1242 Cabinet with dual 10KVA PDUs. The only option is additional capacity, in increments of one JBOD, up to a maximum total of 8.

Capacity

- Base Capacity - Native 50 TB, Effective 200 TB

- Max Capacity - Native 400 TB, Effective 1.6 PB

VLE Overall Dimensions - SunRack II 1242 Cabinet (inches)

- Height - 78.7
- Width - 23.6
- Depth - 47.2

Service Clearance (inches)

- Top - 36

> **Note:** 36 inches is the generic Sun Rack II specification. VLE only requires access through the top if the power cables are routed through the top of the rack. Power cables may be routed top or bottom, depending on how the data center is set up.

- Front - 42
- Rear - 36

Weight (Pounds, Fully Populated with 8 JBODs)

Breakdown:

- Server - 85
- Cabinet - 332
- Each JBOD - 110.25
- 8 JBODs - 882

> **Note:** Each JBOD - 110.25

- Total Weight - 1299
- Total Weight plus shipping material - 1570

Power and HVAC

Table 2–1 VLE Server Power and HVAC Requirements (Estimated)

Requirement	Active Idle	Sample
Server Power (Watts)	759	1287
HVAC (BTU/Hr)	2590	4391

The power per JBOD for the DE2-24C is 201.2 Watts at Idle power and 503 Watts at Typical power.

Table 2–2 VLE Configuration Power and HVAC Requirements

JBOD Size	Watts	BTU/Hr
200 TB	1603	5470
400 B	2106	7186

Table 2–2 (Cont.) VLE Configuration Power and HVAC Requirements

JBOD Size	Watts	BTU/Hr
600 TB	2609	8902
800 TB	3112	10619
1 PB	3615	12335
1.2 PB	4118	14051
1.4 PB	4621	15768
1.6 B	5124	17484

Requirements for Transferring the VLE Point-to-Point

Site conditions must be verified to ensure all VLE system equipment can be safely transported between the delivery dock, staging area, and data center without encountering dimensional restrictions, obstructions, safety hazards, or exceeding rated capacities of lifting and loading equipment, flooring, or other infrastructure. *Conditions that must be verified are described below.*

Structural Dimensions and Obstructions

Dimensions of elevators, doors, hallways, and so on, must be sufficient to allow unimpeded transit of VLE cabinets (in shipping containers, where appropriate) from the delivery dock to the data center installation location. See "VLE Overall Dimensions - SunRack II 1242 Cabinet (inches)" for VLE cabinet-dimension details.

Elevator Lifting Capacities

Any elevators that will be used to transfer VLE cabinets must have a certified load rating of at least 1000 kg (2200 lbs.). This provides adequate capacity to lift the heaviest packaged, fully-populated VLE cabinet, a pallet jack (allow 100 kg/220 lbs.), and two persons (allow 200 kg/440 lbs.). See "Weight (Pounds, Fully Populated with 8 JBODs)" for additional cabinet-weight details.

Ramp Inclines

To prevent VLE cabinets from tipping on ramps while being moved from point-to-point, the site engineer or facilities manager must verify the incline angle of all ramps in the transfer path. Inclines cannot exceed 10 degrees (176 mm/m; 2.12 in./ft.).

Requirements for Installing the VLE

The following sections describe requirements for installing the VLE.

Floor Construction Requirements

VLE system equipment is designed for use on either raised or solid floors. Carpeted surfaces are not recommended since these retain dust and contribute to the buildup of potentially damaging electrostatic charges. A raised floor is preferable to a solid floor since it permits power and data cables to be located safely away from floor traffic and other potential floor-level hazards.

Floor-Load Ratings

Solid floors, raised floors, and ramps located along the transfer path for VLE cabinets must be able to withstand concentrated and rolling loads generated by the weight of a populated cabinet, equipment used to lift a cabinet (for example, a pallet jack), and personnel who are moving the cabinet from point-to-point.

Raised floor panels located along a transfer path must be able to resist a concentrated load of 620 kg (1365 lbs.) and a rolling load of 181 kg (400 lbs.) anywhere on the panel, with a maximum deflection of 2 mm (0.08 in.). Raised floor pedestals must be able to resist an axial load of 2268 kg (5000 lbs.). See "Floor Loading Requirements" for additional floor-loading details.

When being moved from one location to another, a VLE cabinet generates roughly twice the floor load as in a static state. Using 19 mm (0.75 in.) plywood along a transfer path reduces the rolling load produced by a cabinet.

Floor Loading Requirements

Note: Exceeding recommended raised-floor loads can cause a floor collapse, which could result in severe injury or death, equipment damage, and/or infrastructure damage. It is advisable to have a structural engineer perform a floor-load analysis before beginning installation of VLE system equipment.

Caution: When being moved, a VLE cabinet creates almost twice the floor load as when static. To reduce floor load and stress, and the potential for damage or injury when moving a VLE (for example, during installation), consider using 19 mm/0.75 in. plywood on the floor along the path where the cabinet will be moved.

Flooring with an overall (superimposed) load rating of 490 kg per square meter (100 lbs per square foot) is recommended. If floors do not meet this rating, a site engineer or facilities manager must consult the floor manufacturer or a structural engineer to calculate actual loads and determine if the weight of a particular VLE system configuration can be safely supported.

Specific information on floor construction requirements is available from the VLE Backline Support group.

Floor Loading Specifications and References A *basic floor load** comprised of 695 kg per square meter (142 lbs. per square foot) to a *maximum, superimposed floor load* # of 462 kg per square meter (94 lbs. per square foot).

Note: * Load over footprint surface area (7093.7 square centimeter/1099.5 square inch) of an unpackaged VLE cabinet, with a maximum weight of 590 kg/1299 lbs., that is, a VLE with 192 array disk drives.

Assumes minimum Z+Z axis dimension of 185.3 cm/73.0 in. (that is, cabinet depth 77.1 cm/30.4 in. + front service clearance of 54.1 cm/21.3 in. + rear service clearance of 54.1 cm/21.3 in.), minimum X+X axis dimension of 104.9 cm/41.2 in. (that is, cabinet width 92.1 cm/36.3 in. + left clearance of 6.4 cm/2.5 in. + right clearance of 6.4 cm/2.5 in.).

Raised-Floor Lateral Stability Ratings In areas of high earthquake activity, the lateral stability of raised floors must be considered. Raised floors where VLE system equipment is installed must be able to resist the horizontal-stress levels, shown in the listing of horizontal force, below.

Seismic Risk Zone: Horizontal Force (V) Applied at Top of Pedestal

- 1: 13.5 kg/29.7 lbs
- 2A: 20.2 kg/44.6 lbs
- 2B: 26.9 kg/59.4 lbs
- 3: 10.4 kg/89.1 lbs
- 4: 53.9 kg/118.8 lbs

> **Note:** Horizontal forces are based on the 1991 Uniform Building Code (UBC) Sections 2336 and 2337, and assume minimum operating clearances for multiple VLE cabinets. Installations in areas not covered by the UBC should be engineered to meet seismic code provisions of the local jurisdiction.

Raised-Floor Panel Ratings Raised floor panels must be able to resist a concentrated load of 590 kg (1299 lbs.) and a rolling load of 181 kg (400 lbs.) anywhere on the panel with a maximum deflection of 2 mm (0.08 in.). Perforated floor panels are not required for VLE system equipment, but if used, must comply with the same ratings.

Raised-Floor Pedestal Ratings Raised floor pedestals must be able to resist an axial load of 2268 kg (5,000 lbs.). Where floor panels are cut to provide service access, additional pedestals may be required to maintain the loading capacity of the floor panel.

Data Center Safety

Safety must be a primary consideration in planning installation of VLE system equipment, and is reflected in such choices as where equipment will be located, the rating and capability of electrical, HVAC, fire-prevention systems that support the operating environment, and the level of personnel training. Requirements of local authorities and insurance carriers will drive decisions regarding what constitutes appropriate safety levels in a given environment.

Occupancy levels, property values, business interruption potential, as well as fire-protection system operating and maintenance costs should also be evaluated. The *Standard for the Protection of Electronic Computer / Data Processing Equipment (NFPA 75)*, the *National Electrical Code (NFPA 70)*, and local and national codes and regulations can be referenced to address these issues.

Emergency Power Control

The data center should be equipped with readily-accessible emergency power-off switches to allow immediate disconnection of electrical power from VLE system equipment. One switch should be installed near each principal exit door so that the power-off system can be quickly activated in an emergency. Consult local and national codes to determine requirements for power disconnection systems.

Fire Prevention

The following fire-prevention guidelines should be considered in the construction, maintenance, and use of a data center:

- Store gases and other explosives away from the data center environment.
- Ensure data center walls, floors, and ceilings are fireproof and waterproof.
- Install smoke alarms and fire suppression systems as required by local or national codes, and perform all scheduled maintenance on the systems.

> **Note:** Halon 1301 is the extinguishing agent most commonly used for data center fire suppression systems. The agent is stored as a liquid and is discharged as a colorless, odorless, electrically nonconductive vapor. It can be safely discharged in occupied areas without harm to personnel. Additionally, it leaves no residue, and has not been found to cause damage to computer storage media.

- Install only shatterproof windows, in code-compliant walls and doors.
- Install carbon dioxide fire extinguishers for electrical fires and pressurized water extinguishers for ordinary combustible materials.
- Provide flame-suppressant trash containers, and train personnel to discard combustible waste only into approved containers.
- Observe good housekeeping practices to prevent potential fire hazards.

Site Power Distribution Systems

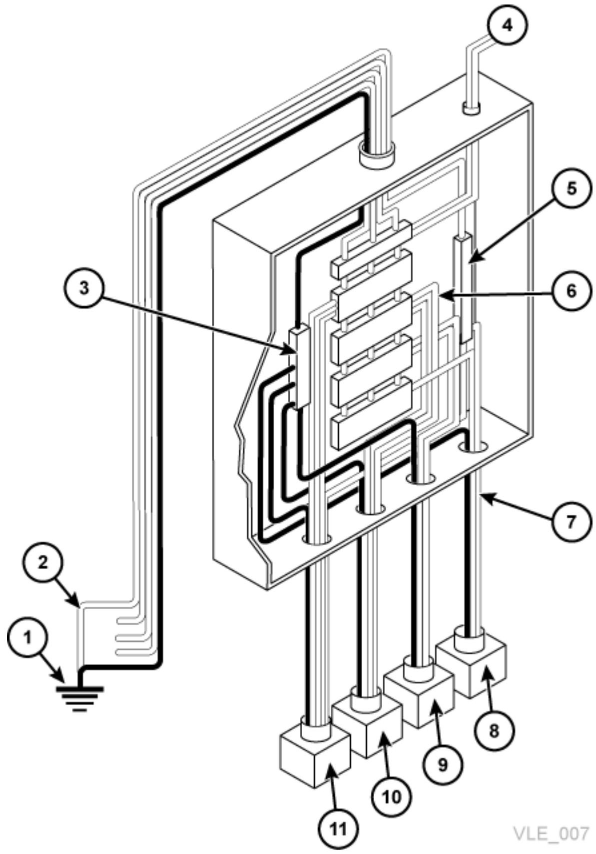
The following elements of the site power distribution system should be evaluated when planning an installation of VLE system equipment.

System Design

A properly installed power distribution system is required to ensure safe operation of VLE system equipment. Power should be supplied from a feeder separate from one used for lighting, air conditioning and other electrical systems.

A typical input power configuration, shown in Figure 2–1, is either a five-wire, high-voltage or a four-wire, low-voltage type, with three-phase service coming from a service entrance or separately derived source, with overcurrent protection and suitable grounding. A three-phase, five-wire distribution system provides the greatest configuration flexibility, allowing power to be provided to both three-phase and single-phase equipment.

Figure 2–1 Site Electrical Power Distribution System



Legend:

1. Service entrance ground or suitable building ground
2. Only valid at service entrance or separately derived system (transformer)
3. Ground Terminal Bar (bound to enclosure) same size as neutral
4. Remotely Operated Power Service Disconnect
5. Neutral Bus
6. Circuit Breakers of Appropriate Size
7. Branch Circuits
8. 120V Single phase
9. 208/240V Single Phase
10. 208/240V 3-Phase (4 wire)
11. 208/240V 3-Phase (5 wire)

Equipment Grounding

For safety and ESD protection, VLE system equipment must be properly grounded. VLE cabinet power cables contain an insulated green/yellow grounding wire that connects the frame to the ground terminal at the AC source power outlet. A similar insulated green or green/yellow wire ground, of at least the same diameter as the phase wire, is required between the branch circuit panel and the power receptacle that attaches to each cabinet.

Source Power Input

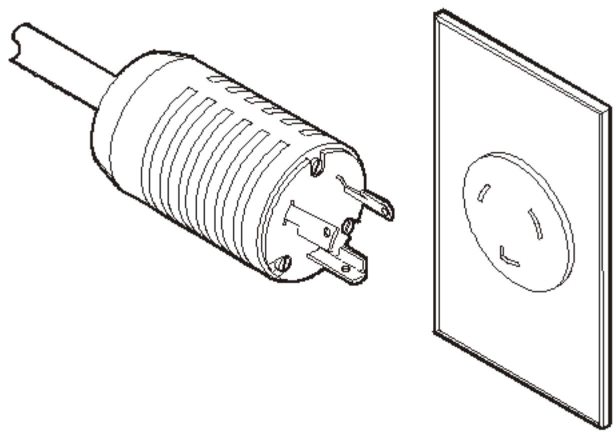
Voltage and frequency ranges at the AC source power receptacle(s) that will supply power to VLE system equipment must be measured and verified to meet the specifications shown in Table 2–3.

Table 2–3 Source Power Requirements for VLE Equipment

Source Power	Voltage Range	Frequency Range (Hz)
AC, single-phase, 3-wire	170-240	47-63

If you are installing the VLE in North America, South America, Japan and/or Taiwan, ensure that the designated power sources are NEMA L6-30R receptacles, and that the cabinet power cords are terminated with the required NEMA L6-30P plugs. The factory ships power cords with NEMA L6-30P plugs to North and South America, Japan and Taiwan. Shipments to EMEA and APAC will ship with IEC309 32A 3 PIN 250VAC IP44 plugs.

The figure below shows a NEMA L6-30P plug and L6-30R receptacle.



If you are installing the VLE outside North America, South America, Japan and/or Taiwan, ensure that the designated source-power receptacles meet all applicable local and national electrical code requirements. Then, attach the required connectors to the three-wire ends of the cabinet power cords.

Dual Independent Source Power Supplies

VLE cabinets have a redundant power distribution architecture designed to prevent disruption of system operations from single-source power failures. Four 30 Amp power plugs are required.

To ensure continuous operation, all power cables must be connected to separate, independent power sources that are unlikely to fail simultaneously (for example, one to local utility power, the others to an uninterruptible power supply (UPS) system). Connecting multiple power cables to the same power source will not enable this redundant power capability.

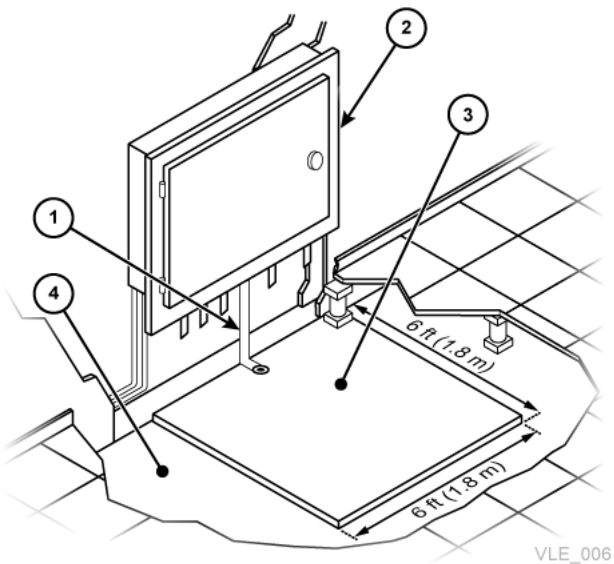
Transient Electrical Noise and Power Line Disturbances

Reliable AC source power free from interference or disturbance is required for optimum performance of VLE system equipment. Most utility companies provide power that can properly operate system equipment. However, equipment errors or failures can be caused when outside (radiated or conducted) transient electrical noise signals are superimposed on power provided to equipment.

Additionally, while VLE system equipment is designed to withstand most common types of power line disturbances with little or no effect on operations, extreme power disturbances (such as lightning strikes) can cause equipment power failures or errors if steps are not taken to mitigate such disturbances.

To mitigate the effects of outside electrical noise signals and power disturbances, data center source power panels should be equipped with a transient grounding plate similar to that shown in Figure 2–2.

Figure 2–2 Transient Electrical Grounding Plate



Legend:

1. Flat Braided/Strained Wire
2. Power Panel
3. Plate
4. Concrete Floor

Electrostatic Discharge

Electrostatic discharge (ESD; static electricity) is caused by movement of people, furniture, and equipment. ESD can damage circuit card components, alter information on magnetic media, and cause other equipment problems. The following steps are recommended to minimize ESD potential in the data center:

- Provide a conductive path from raised floors to ground.
- Use floor panels with nonconducting cores.
- Maintain humidity levels within recommended control parameters.
- Use grounded anti-static work mats and wrist straps to work on equipment.

HVAC Requirements

Cooling and air-handling systems must have sufficient capacity to remove heat generated by equipment and data center personnel. Raised-floor areas should have positive underfloor air pressure to facilitate airflow. If conditions change within a data center (for example, when new equipment is added, or existing equipment is rearranged), airflow checks should be done to verify sufficient airflow.

Environmental Requirements and Hazards

VLE system components are sensitive to corrosion, vibration, and electrical interference in enclosed environments such as data centers. Because of this sensitivity, equipment should not be located near areas where hazardous and/or corrosive materials are manufactured, used, stored, or are in areas with above-average electrical interference or vibration levels.

For best performance, equipment should be operated at nominal environmental conditions. If VLE system equipment must be located in or near adverse environments, additional environmental controls should be considered (and implemented where practicable) to mitigate those factors before installation of the equipment.

3

VLE Planning

This chapter provides information about VLE planning and information, with emphasis on the Oracle Cloud. For Cloud Extended Storage, make sure that the Cloud Storage account is in place before setting up VLE for Cloud access. See "Preparing for Cloud Extended Storage" and "Network Requirements for Cloud Extended Storage"for further details on setting up an account, or "Oracle Storage Cloud Service – Archive Storage" for Archive information.

Software and Hardware Requirements for Virtual Library Extension (VLE)

The following sections will review requirements that must be adhered to for successful implementation of the Oracle's Virtual Library Extension (VLE) features.

Satisfying Mainframe Host Software Requirements

- For ELS 7.2 and higher, support for VLE 1.5 is included in the base level.
- For ELS 7.1 and higher, get the latest `SMP/E` receive `HOLDDATA` and PTFs L1H16J6 and L1H1674 and `SMP/E APPLY` with `GROUPEXTEND`.

Satisfying Network Infrastructure Requirements

If possible, do any configuration of IP addresses, network switch(es) for VLANs or other setup (running cables, and so forth) before the VLE arrives to minimize the installation time. Ensure that the network is ready for connection to the VLE, as follows:

- Valid Cloud Storage Account from Oracle (which will include account name, user name, password and a URL)
- Gigabit Ethernet protocol is required on all network switches and routers that are directly attached to VSM 5 IFF cards. The network interfaces are all 10 Gb. The copper interfaces can and will negotiate down to 1 Gb (or slower) but optimally all traffic will take place over 10 Gb connections
- Name of the Ethernet port (1 Gig or 10 Gig), the subnet the cloud traffic will be routed through, and with the following details:

Name	Values	Comment
Port Host Name		May or may not be in DNS - check with the Network Administrator

Name	Values	Comment
Static IP Address		Should be a valid value - check with the Network Administrator
Net Mask		Check with the Network Administrator
Prefix Length		Example: 24/23/... - check with the Network Administrator
Gateway Address		Should be a valid value - check with the Network Administrator
jumbo		Enabled or not - check with the Network Administrator

- Switches and routers should support Jumbo(mtu=9000) packets for best performance. If the network is not capable of handling Jumbo Frames, turn off this capability at the VTSS and VLE

  If *network redundancy* is required, then each IP connection (between VSM 5 or 6 and VLE, VLE-to-VLE, and VLE-to SMC) must be configured on separate subnets.

  If Jumbo Frames are enabled, then all switches, hubs, or patch panels (including the VLAN and the port channel) between the VLE and its target component must also have Jumbo Frames enabled.

  Note: When a number of static IP address connections are set in the same subnet, the connections will work properly. If one of the cables is pulled or otherwise disrupted, the other connections in that subnet will be lost.

- Check that you are using the proper (customer-supplied) 1 GigE Ethernet cables:
  - CAT5 cables and below are not acceptable for GigE transmission.
  - CAT5E cable: 90 meters is acceptable if run through a patch panel, 100 meters if straight cable.
  - CAT6 cable: 100 meters is acceptable regardless of patch panel configuration.
- Oracle recommends that if a switch or router is used in the configuration, at least two switches or routers be part of the configuration at each location so that the loss of one unit will not bring down the entire configuration.
- Only one TCP/IP connection is required between a VTSS and a VLE. However, for redundancy, Oracle strongly recommends that you have at least two connections between the VTSS and VLE, where the VTSS connections are separate IP addresses. Each TCP/IP connection from a specific VTSS to a specific VLE should be to separate VLE interfaces. If you connect all of the VTSS connections to the same VLE interface, you have a single point of failure at the VLE interface.

In a VLE multi-node system, the VTSS connections should be spread evenly across all nodes. For example, in a two-node VLE, the VTSS connections should be two on node 1, and the other two on node 2. On a four-node VLE, 1 VTSS connection to each node is recommended. If a switch is involved between the VTSS and VLE, then it is possible to have all four connections to each node of a four-node VLE. Due to each VTSS connection representing four drives total, there would be one drive from each connection to each node, for a total of four drives for each node on a four-node VLE.

IP addresses, however, must **never** be duplicated on separate nodes in the VLE for UUI or VTSS. For example, if you have a UUI connection of `192.168.1.1` going to node 1, then do not make a UUI connection on another node using `192.168.1.1` as the IP address. Additionally, if possible, you should never have two interfaces on the same node within the same subnet when configuring IP addresses.

- Similarly, only one UUI connection is required between a VLE and the host, but two are recommended for redundancy, preferably using two independent network paths.

> **Note:** These network paths are separate from the connections to the VTSS. For VLE multi-node configurations, if there are multiple UUI connections, make them from separate nodes in the VLE.

Satisfying Oracle Switch Hardware Requirements

An Oracle ES2-72 Oracle switch is required for three node or greater VLEs.

- A two node VLE does not require a switch but one can be added if further expansion of the two node VLE is planned in the future.
- The Oracle Switch is required for communication and data transfer between nodes (a private network between the VLE nodes); it does not connect to the customer Ethernet infrastructure and is not part of external VLE data transfer operations
- The Oracle Service team will have detailed instructions for installing and configuring the ES2-72 switch.
- The Oracle sales team will also have access to additional documentation to confirm the necessary switch and components for the planned configuration.

The following equipment will be needed for a multi-node VLE installation. When connecting three or four VLE nodes together, you'll need:

- One 7110593 – ES2-72 switch
- One 7110595 – Rear to Front fan unit
- Two SR-JUMP-2MC13 – Power cables
- Two 2124A – Transceivers
- Two X2127 A-10M – QSFP break-out cables
- Sixteen 10800160N – Couplers for connecting QSFP to VLE Optical cables

When connecting five to eight VLE nodes together, you'll need:

- One 7110593 – ES2-72 switch
- One 7110595 – Rear to Front fan unit
- Two SR-JUMP-2MC13 – Power cables

- Four 2124A – Transceivers
- Four X2127 A-10M – QSFP break-out cables
- Thirty-two 10800160N – Couplers for connecting QSFP to VLE Optical cables

When connecting nine to twelve VLE nodes together, you'll need:

- One 7110593 – ES2-72 switch
- One 7110595 – Rear to Front fan unit
- Two SR-JUMP-2MC13 – Power cables
- Six 2124A – Transceivers
- Six X2127 A-10M – QSFP break-out cables
- Forty-eight 10800160N – Couplers for connecting QSFP to VLE Optical cables

When connecting thirteen to sixteen VLE nodes together, you'll need:

- One 7110593 – ES2-72 switch
- One 7110595 – Rear to Front fan unit
- Two SR-JUMP-2MC13 – Power cables
- Eight 2124A – Transceivers
- Eight X2127 A-10M – QSFP break-out cables
- Sixty-four 10800160N – Couplers for connecting QSFP to VLE Optical cables

The appropriate length of LC/LC optic fiber is needed, but it isn't something ordered here. Two cables that are 25m long are shipped with each VLE appliance. If they have been misplaced, they are available from a variety of sources – the customer may have some available, but they should be a maximum length, including patch panels, of 25M. The fiber cable needs to be OM3, 850nm, multi-mode with LC/LC connectors. You need two cables per VLE node to connect to the switch.

Satisfying Serviceability Requirements

The VLE product uses a standard Oracle service strategy common with other Oracle products. Automated Service Response (ASR) is used by the VLE as the outgoing event notification interface to notify Oracle Support that an event has occurred on the VLE and the system may require service. Additionally, in combination with ASR, an outgoing e-mail containing details about an ASR event and a Support File Bundle containing VLE log information necessary to investigate any ASR event will also be sent.

The advantages of ASR functionality are well documented in the ASR FAQ available on the My Oracle Support site (`https://support.oracle.com/CSP/ui/flash.html`) in Knowledge Article Doc ID 1285574.1.

Oracle's expectation is that the VLE will be configured to allow outgoing ASR and e-mail communication with Oracle Support. To support VLE outgoing ASR notifications, the customer will need to supply the information in Table 3–1 to the installing Oracle Field Engineer.

Oracle's expectation is that the VLE will be configured to allow outgoing ASR and e-mail communication with Oracle Support. To support VLE outgoing ASR notifications, the customer will need to supply the information in Table 3–1 to the installing Oracle Field Engineer.

Table 3–1 VTASR Configuration Information

Configuration Value	Example
General Configuration - Site Information	
Company Name	Company Inc
Site Name	Site A
City	AnyTown
General Configuration - Contact Information	
First Name	Joe
Last Name	Companyperson
Contact email	joecompanyperson@company.com
Auto Service Request (ASR) Setup - Oracle Online Account Information	
Customer Oracle CSI Login Name	joecompanyperson@company.com
Customer Oracle CSI Login Password	********
Auto Service Request (ASR) Setup - Internet Connection Settings (Optional)	
Proxy Host Name	web-proxy.company.com
Proxy Port	8080
Proxy Authentication - User Name	
Proxy Authentication - Password	

Note: In Table 3–1, some fields are not required if a proxy server is not being used or if it does not require an ID and password. If the customer will not provide the CSI e-mail ID and password, then the customer can enter it directly during the install process. During this part of the install, the VLE will register itself on the Oracle servers as an ASR qualified product.

The customer is then required to log in to My Oracle Support (MOS) and approve the registration of the VLE. Until this approval is completed by the customer, the VLE is not capable of auto-generating cases through MOS.

For e-mail notification of event and log information, the customer must also supply the information in Table 3–2. If the e-mail server does not require a user name and password, these fields can remain blank.

Table 3–2 Notification Setup - E-mail Configuration Options / ConfCollectStatus

Configuration Value	Example
E-mail Configuration - SMTP Server Name	SMTP.company.com
E-mail Configuration - SMTP Server User Name	

Table 3–2 (Cont.) Notification Setup - E-mail Configuration Options / ConfCollectStatus

Configuration Value	Example
E-mail Configuration - SMTP Server User Password	
E-mail Recipients	vle@invisiblestorage.com *and others as needed*

In cases where outgoing communication steps are not completed at the time of installation or not allowed at all, Oracle's options for timely response to events that require support from the Oracle Service team are greatly reduced. The VLE can be configured to send e-mail containing event and log information directly to a designated customer internal e-mail address. A recipient of this e-mail can then initiate a service request directly with Oracle and forward any e-mails received from the VLE to Oracle Support. In this case, the customer must supply the e-mail address where VLE e-mails are sent, where this e-mail address can accept e-mails of up to 5 MB.

Automated Service Request (ASR) Configuration

By default, the VLE will send ASRs through the ixgbe0 port. The site's mail server will be used to send the ASR alerts and the VLE support file bundles.

Determining VLE Configuration Values

The following sections describe how to determine configuration values for the VLE.

> **Note:** As noted in the following sections, several software configuration values must match values initially set during configuration of the VLE. Use the worksheet to record these values so you can pass them on to the personnel who will configure the VLE and the host software.

Determining Values for the Configuration Scripts

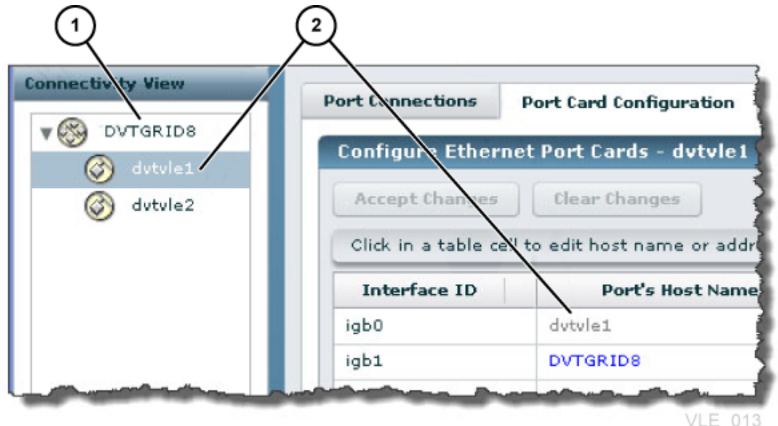
To configure the network for VLE, you run the `configure_vle` script on each node in a multi-node system (or the only node in a single-node system).

Node name is the name of the individual node, commonly referred to as **hostname**. This is the name that identifies this node in the IP environment with a unique DNS entry, with a fully qualified name and a unique IP address. During the initial setup, each VLE node is configured to bind the ixgbe0 interface to the fully qualified hostname and IP address.

ASR registration and generated data uniquely identify the hostname of each node. Once set, it is very difficult to change the name and IP address (you may need to stop all of your services and reboot the node).

It is highly recommended that name, DNS entry, and IP address are generated and validated with the corporate IT department for accessibility through firewalls, gateways, and routers well before the VLEs are installed. This will make the process of setting up, configuring, and bringing up VLE much smoother and faster.

Figure 3–1 VLE Name, VLE Number and Node Name



Legend:

1. **VLE name** from `configure_vle` installation script run on each node
2. **Node name** entered as "hostname" for this node in the `configure_vle` installation script

VLE Name and VLE Number

Each VLE node (connected through the same internal network) has a common VLE name and VLE number (1). The VLE name and number **must be the same** on each node in a multi-node VLE, where the node name is 2.

The VLE Name must be unique and should **not** be the hostname of any of the servers. The default VLE Name is `VLE-NAME`. You can reset the VLE Name when you run the `setup_vle_node` script. The value must be 1 to 8 characters in length, alphanumeric, uppercase. The name can contain a - (dash) but not at the beginning or the end.

Valid values for the VLE number are 1-9

In Figure 3–1, the VLE Name and VLE Number combination is `DVTGRID8`.

To the host software, the VLE Name and VLE Number combination is known as the *subsystem name*, and is specified, as follows:

- The `STORMNGR` parameter value on the VTCS `CONFIG TAPEPLEX` statement for the TapePlex that connects to the VLE or the `NAME` parameter on the `CONFIG STORMNGR` statement (ELS 7.1 and higher).
- The `STORMNGR` parameter value on the VTCS `CONFIG RTD` statement for the VLE.
- The `NAME` parameter value on the SMC `STORMNGR` command that defines the VLE to SMC.
- The `STORMNGR` parameter value on the SMC `SERVER` command for the VLE.
- The `STORMNGR` parameter value on the HSC `STORCLAS` statement.

Host Name for the Node

As shown in Figure 3–1, the Host Name for the Node, which is entered on the `configure_vle` script, appears as:

- The `Port's Host Name` for the `ixgbe0` interface ID for the node.
- The Host Name for the node selected in the node navigation tree.

In Figure 3–1, the Host Name for the node is `dvtvle1`.

Characters can be alphanumeric (A-Z, a-z, 0-9) or "." or "-". The first and last characters of the string cannot be "." or "-". The name cannot be all numeric. The name can be up to 512 characters long, though Internet standards require that the host portion (not including the domain component) be limited to a maximum of 24 characters.

Determining Values for configure_vle

Required values for the `configure_vle` script include the following:

- Hostname for the node; see "Host Name for the Node"
- VLE static IP address for port `ixgbe0`
- Network number, which is the base address of the customer subnet
- Netmask
- The default router IP address (Gateway address)
- The network domain name
- The Name Server IP addresses
- Network search names
- NTP server/client setup (server or client, IP addresses of servers) and date/time values

Determining Values for setup_vle_node

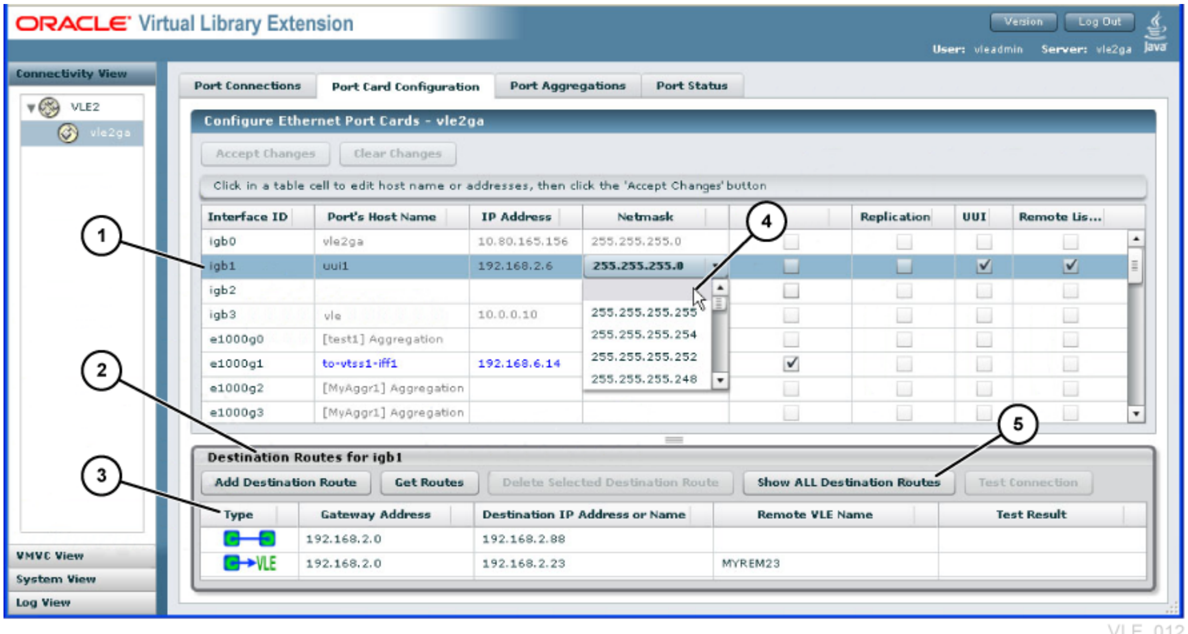
Required values for the `setup_vle_node` script include the following:

- VLE number and name; see "VLE Name and VLE Number."
- Serve Node number (SSN). For multi-node VLEs, each node requires a unique SSN. Valid values for SSN are 1 to 64.
- Server time and date values.

Determining Values for Port Card Configuration

To configure the VLE Ethernet ports, you use the **Connectivity View, Port Card Configuration** tab shown in Figure 3–2. The following sections describe how to determine port card configuration values.

Figure 3–2 VLE GUI Port Card Configuration Tab

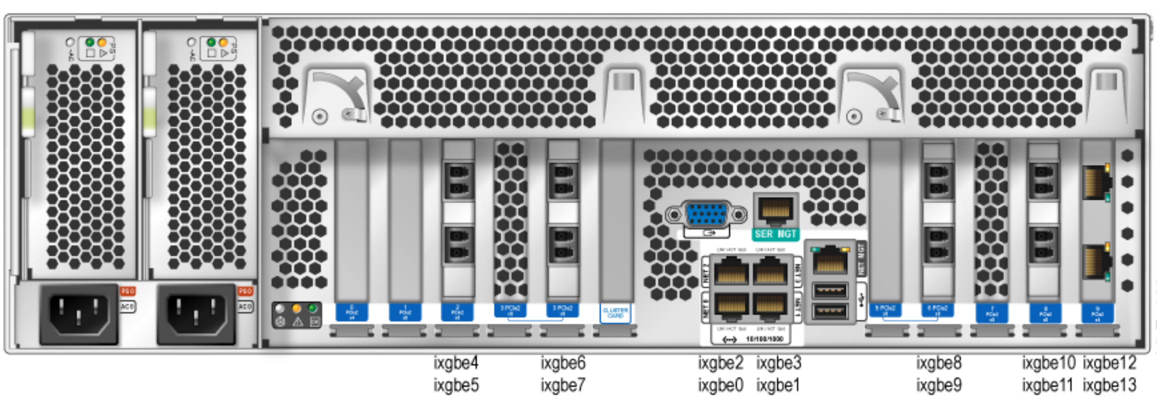


Legend:

1. Selected interface
2. Destination Routes panel to define remote VLE connections and static routes
3. Type of route shown by icons
4. Clear Netmask field by selecting blank item at the top of the drop-down list
5. Content of bottom pane, filtered by the interface selected in the top pane. Click to show all routes for the node

Figure 3–3 shows the 10 GigE Ethernet ports on the rear of the server.

Figure 3–3 VLE 10GigE Ethernet Ports



Work with the customers' network engineer to make sure any VLANs are properly cabled and configured. Oracle recommends that the customers' network connections spread the Ethernet traffic to two or more Ethernet switches to ensure that losing one switch does not end all data traffic.

Ethernet Management Ports

Connect Ethernet cables to those ports that you want to configure as follows:

ixgbe0 (NET0) - Connection to the customer network for ASR traffic and managing the VLE software. During setup, this interface is bound to the fully qualified hostname and IP address unique to each node. It is highly recommended that you do not change them after the initial setup.

- `ixgbe1` (NET1)- Connection to the customer network for UUI (control path) traffic.
- `ixgbe2` (NET2) - Spare, available for redundant UUI connection, or if the customer wants separate ports for separate network segments for the host network and for the sending of ASR alerts.
- `ixgbe3` (NET3)- Dedicated port for service (CSE PC connection for ILOM). Do not connect this port to the network. `ixgbe3` must remain available as an Ethernet port with known access configuration so that it is always be available for service. The pre-configured default IP address for `ixgbe3` is `10.0.0.10`.

Multi-Node Connections

To connect 2 nodes, do one of the following:

Directly connect `ixgbe4` on one node to `ixgbe4` on the second node, and `ixgbe6` on one node to `ixgbe6` on the second node.

> **Note:** the Oracle switch with available ports for 3-node or greater VLEs is required. Connect the nodes (using `ixgbe4` and `ixgbe6`) using the Oracle switch.
>
> When making multi-node connections, you should connect Node 1 to the switch (or the second node, for 2-node VLEs) and run `configure_vle` on Node 1. Then connect Node 2 and run `configure_vle` on Node 2, and so on. After all nodes are connected and `configure_vle` (which calls `configure_vle`) is complete, then proceed with the rest of the configuration.

This procedure is required because the default Internal network address is the same on all nodes when shipped from manufacturing which causes duplicate addresses until all nodes are configured with `configure_vle`.

> **Caution:** When making configuration changes to a multi-node VLE, stop VLE services on all nodes together before starting VLE services on a specific node. That is, you cannot do rolling stop and start(s) of `VLE_services` on a per node basis after a configuration update.

Data Transfer Connections

To make data transfer connections:

- `ixgbe1`, `ixgbe2`, and `ixgbe4` through `ixgbe13` are available for data transfer either from VLE-to-VLE or from VLE-to-VTSS.

> **Note:** Some of these ports may be reserved for other uses, if desired: `ixgbe0` through `ixgbe3`, `ixgbe12` and ixgbe13, when directly connected to a 1 GB link, will operate in 1 GB mode.

Ports' Host Name

The value is the machine (host) name for each IP address to be connected to a VTSS or another VLE. Characters can be alphanumeric (A-Z, a-z, 0-9) or "." or "-". The first and last characters of the string cannot be "." or "-". The name cannot be all numeric. The name can be up to 512 characters long, though Internet standards require that the host portion (not including the domain component) be limited to a maximum of 24 characters.

> **Note:** The Ports' Host Name for `ixgbe0` and `ixgbe3` are established during installation, and cannot be changed at the GUI.

IP Address

The IP address assigned to the port, which must be a valid IP v4 address, in the form of "192.68.122.0." Each byte must be 0-255, there must be 4 bytes, numeric only, except for the decimal points.

Netmask

The network mask for the port must be a valid IP v4 address in the form of "255.255.255.0." Each byte must be 0-255. There **must** be 4 bytes, numeric only, except for the decimal points.

Replication

Select the check-box for each port that will be used for VLE-to-VTSS data exchange.

UUI

Select the check-box for each port that will be used for UUI activity. This port is usually the one used for product configuration and monitoring (including the port used by the GUI browser connection).

> **Note:** Each VLE must have **at least on**e UUI connection, and two or more are recommended for redundancy. If you have two or more in a multi-node VLE, spread the UUI connections out over different nodes.

Remote

This check-box identifies the port as a "Listener" destination for a VLE-to-VLE data exchange. For VLE-to-VLE data transfers, any unused connection can be used from any node in a VLE. If each VLE has two or more nodes, Oracle recommends a **minimum** of one connection from each node to the other VLE. You can run more than one connection from a VLE node to another VLEs' node, but you should **never** run multiple connections from a VLE node to a single port on the other VLE. If both VLEs have more than one node, Oracle recommends spreading the VLE-to-VLE connections across all nodes in each VLE.

Example: VLE1 node 1 has a connection from `192.168.1.1` to VLE2 node 1 at `192.168.1.2`. If a second connection is made from VLE node 1, then the connection should **not** go to VLE2 at `192.168.1.2`.

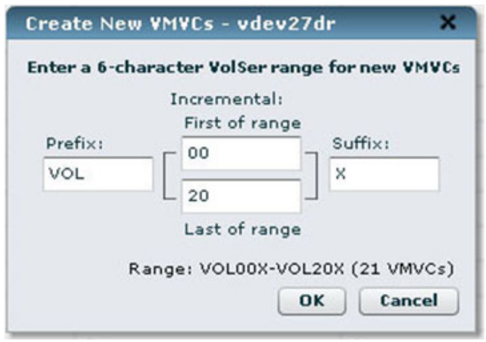
For VLE-to-VLE data transfers, each VLE requires a UUI connection and a VTSS connection. This will ensure VTCS can migrate and recall VTVs from either VLE.

Determining VMVC Range Configuration Values

Ensure that you assign VMVC names and ranges to fit within the site naming scheme. VMVC names and ranges are set by the CSE during configuration, so it is best to have them assigned before configuration.

As shown in Figure 3–4, you use the VLE GUI's **Create New VMVC** dialog box (from the **VMVC View** with a specific node selected in the navigation tree) to specify volser ranges of new VMVCs.

Figure 3–4 VLE GUI Create New VMVC dialog box



Determine values for each of the fields in Figure 3–4, as follows.

Each of the fields allow 0-6 alphanumeric characters, with "assembly" limitations:

- Alphabetic characters are automatically converted to upper case; leading and trailing spaces in all fields are automatically removed.
- Any of the fields can be empty, allowing the incremental value to be first, last, or in the middle of the `volser` range name.
- Any of the fields can be either alphabetic or numeric, with field validations to restrict their usage where necessary. For instance, embedded spaces and special characters are not allowed. Invalid field entries are shown with a red box around the field, and selecting the **OK** button will display an error warning.
- The "Incremental" range fields (prefix and suffix) can be either alphabetic or numeric. Field validations ensure that alphabetic and numeric characters are not mixed in either field, the first value must be less than the last value, and `max` range limits are checked.
- The length of the entire `volser` name range is constructed by assembly of each field – the length of the prefix + length of ranges + length of the suffix.

  Example: Enter a prefix of `AB`, a first of range of `001`, a last of range of `500` and a suffix of `X` to build the `volser` name range of `AB001X - AB500X`. Similar combinations can be built, but the length of the entire assembly must add up to exactly six characters.
- If the built-up name exceeded the valid 6-character `volser` name length (like `AB0001XY - AB1500XY`), clicking the **OK** button displays a warning dialog and does not allow the entry.
- As the range is being built by editing fields, the resulting range is displayed on a line of the dialog just above the **OK** and **Cancel** buttons. The count of VMVCs in the range being built is also displayed in parentheses with the range. If the count exceeds the maximum allowed for the Wildcat box (shown in the "VMVC Counts" fields as `Max`), the text is displayed in bold orange. At the time the **OK** button is

pressed, the current `Available` count is checked, and if the range exceeds this amount, an error dialog is displayed.

- The suffix string must begin with a different character type (alphabetic, not numeric) than the incremental range strings. This is for compatibility with VTCS `volser` name range entry capability. If the range contains the same character type as the beginning of the suffix, the beginning characters of the suffix would be incremented in a range before those in the range fields; that is, VTCS volser name processing is based on character type, not by field-entry of ranges.

  Example: A GUI entry of 1000 for the First of range, 1094 for the Last of range, and a suffix of 55 would make a range of 100055-109455. On VTCS, this would expand to 100055, 100056, 100057…109455 rather than 100055, 100155, 100255…109455. Because it would be difficult for you to match the latter expansion in VTCS `volser` name range entry, this construction is prohibited in the GUI.

- If attempting to define overlapping ranges, only new VMVCs in the range will be added to any already-existing VMVCs (existing VMVCs will not be overwritten or cleared).
- VMVCs have a nominal size of 250 GB (to the host software) and an effective size on the VLE of 1 TB (assuming 4:1 compression). Table 3–3 shows the maximum VMVCs defined for each VLE node capacity.

Table 3–3 VLE Effective Capacities - Maximum VMVCs Per Node

VLE Effective Capacity	Maximum VMVCs
200 TB	200
400 TB	400
800 TB	800
1600 TB	1600

- The VMVC volser ranges that are specified in the VLE GUI must match the volser ranges defined to VTCS.

Planning for Encryption

VLE 1.1 and higher provides encryption of VMVCs written to the VLE system. If a VTV is recalled to the VTSS, it is de-encrypted at the VLE before recall; therefore, the MVS host software has no knowledge of encryption.

> **Note:** Adhere to the following:
>
> - The encryption algorithm used is AES-256-CCM. The access key is a 256 bit file.
> - FIPS 140-2 certification request has been filed with NIST and is in progress.

Encryption is enabled, disabled, and managed at the VLE GUI by an Oracle CSE or other QSP. Encryption is enabled on a per node basis through an encryption key stored on the node, and backed up on a USB device. You can mix encryption and non-encryption nodes in a multi-node VLE because VLE decrypts VTVs, if required, regardless of where they reside on a multi-node VLE.

If, however, you want to encrypt all VTVs on a multi-node VLE, then encryption must be enabled for all nodes.

Some implementation notes:

- *Before* encryption is enabled, there must be **no** VMVCs on the node. Additionally, the USB key backup must be inserted in the node's USB port, and must be writeable and mounted by the operating system.
- Similarly, *before* encryption is disabled, recall VTVs that you want to keep to the VTSS, then delete all VMVCs from the node.
- Encryption keys do not expire, so do **not** generate a new key unless you must (for example, to meet security audit requirements). *Before* you assign a new key:
  - The USB key backup must be inserted in the nodes' USB port, and must be available to write and be mounted by the operating system.
  - If you are certain you want to generate a new key, ignore the warning and overwrite the old key.

Planning for Deduplication

Deduplication eliminates redundant data in a VLE complex. As the deduplication percentage increases, migration performance can correspondingly improve and network use is reduced.

VLE deduplication is performed at the VLE, so the host job and the VTSS are not affected. When a deduplicated VTV is recalled, the VTV is "rehydrated" (reconstituted) at the VLE before it is recalled to the VTSS. Deduplication occurs on a tape block-level within each node, and small blocks (less than 4 K after compression) are not deduplicated.

Deduplication, which is controlled by the `STORCLAS DEDUP` parameter, increases the effective VLE capacity, and is performed by the VLE before the VTV is written to a VMVC. For example, Example 3–1 shows deduplication enabled for two Storage Classes.

Example 3–1 Deduplication Enabled for Local and Remote Storage Classes

```
STOR NAME(VLOCAL) STORMNGR(VLESERV1) DEDUP(YES)
STOR NAME(VREMOTE) STORMNGR(VLESERV2) DEDUP(YES)
```

The `STORCLAS` statements in Example 3–1 specify deduplication for a "local" Storage Class (`VLOCAL`) on the VLE `VLESERV1` and "remote" Storage Class (`VREMOTE`) on the on the VLE `VLESERV2`.

Example 3–2 shows a Management Class that performs deduplication on the Storage Classes in Example 3–1. Any jobs that specify the `DEDUP2` Management Class enable deduplication for the referenced Storage Classes.

Example 3–2 Management Class for Deduplication

```
MGMT NAME(DEDUP2) MIGPOL(VLOCAL,VREMOTE)
```

Note: Deduplication occurs *only after* the `DEDUP(YES)` policy is set.

Deduplication Guidelines

Many sources of mainframe data do **not** benefit from deduplication, such as `syslogs`. Generally data streams that contain timestamps (where every record is different) will not benefit from deduplication. Backup data streams (where the same records may be written multiple times) will typically benefit from deduplication.

Using the SCRPT Report

You can monitor the results with the SCRPT report, as shown in the example below.

```
Storage STORMNGR Node Total Capacity Used Compressed Uncompressed
Reduction

Class          MVCs   (GB)   (GB)    (GB)        (GB)   Ratio

PROD1  VLELIB1  0    4    1000    200     800      3200        16.0:1
```

1 3 750 200 400 1600 8.0:1

2 5 1250 200 400 1600 8.0:1

3 4 1000 0 0 0 1.0:1

VLELIB1 16 4000 600 1600 6400 10.7:1

Total- 16 4000 600 1600 6400 10.7:1

(A11} VLELIB1 0 4 1000 200 800 3200 16.0:1

1 3 750 200 400 1600 8.0:1

2 5 1250 200 400 1600 8.0:1

3 4 1000 0 0 0 1.0:1

VLELIB1 16 4000 600 1600 6400 10.7:1

Total= 16 4000 600 1600 6400 10.7:1

In the above example, the approximate reduction ratio for the data is Uncompressed GB divided by Used GB. The Reduction Ratio, therefore, includes both VTSS compression and VLE deduplication. A larger reduction ratio indicates more effective compression and deduplication.

For example, the VTSS receives 16 MB of data, compresses it to 4 MB, and writes the compressed data to a VTV. VLE, subsequently, deduplicates the VTV to 2 MB, and writes it to a VMVC. Thus, the reduction ratio is 16 MB divided by 2 MB, or 8.0:1.

Because the calculation is done using MB, it is possible to see 0 GB in the Used or Uncompressed fields, yet see a reduction ratio other than 1.0:1.

Using the MEDVERIFY Utility

You can run the `MEDVERify` utility to verify that VTV data can be read on VMVCs (ELS 7.1 and VLE 1.2 and higher, only). For VLE, `MEDVERify` ensures that deduplicated VMVCs can be “rehydrated” (reconstituted) when recalled to the VTSS. `MEDVERify` reports on VMVCs that pass or fail verification and also produces XML output.

For example, to verify VTVs on the VMVCs defined in Example 3–1, enter:

```
MEDVER STOR(VLOCAL)
MEDVER STOR(VREMOTE)
```

In this example:

- `MEDVERify` selects VMVCs in Storage Classes `VLOCAL` and `VREMOTE`.
- `MAXMVC` defaults to 99.
- `CONMVC` defaults to 1 so only a single VMVC is processed at a time.
- No timeout is specified.

Reduced Replication

VLE 1.3 and higher offers *Reduced Replication*, which, through VLE-to-VLE replication, allows VTVs to be copied in deduplicated format. The only data copied is data that did not reside on the destination VLE when the copy began. Reduced replication, therefore, reduces the amount of data copied, which lowers network use and copy times. To optimize Reduced Replication, ensure that deduplication is enabled for **both** the source and target Storage Class. Otherwise:

- If deduplication is enabled for the source but not the destination Storage Class, then VTVs are "hydrated" (reconstituted) before being copied.
- If deduplication is enabled for the destination but not the source Storage Class, then VTVs are deduplicated when received at the destination.

For example, Example 3–3 shows a Management Class that performs Reduced Replication using the Storage Classes in Example 3–1.

Example 3–3 Management Class for Reduced Replication

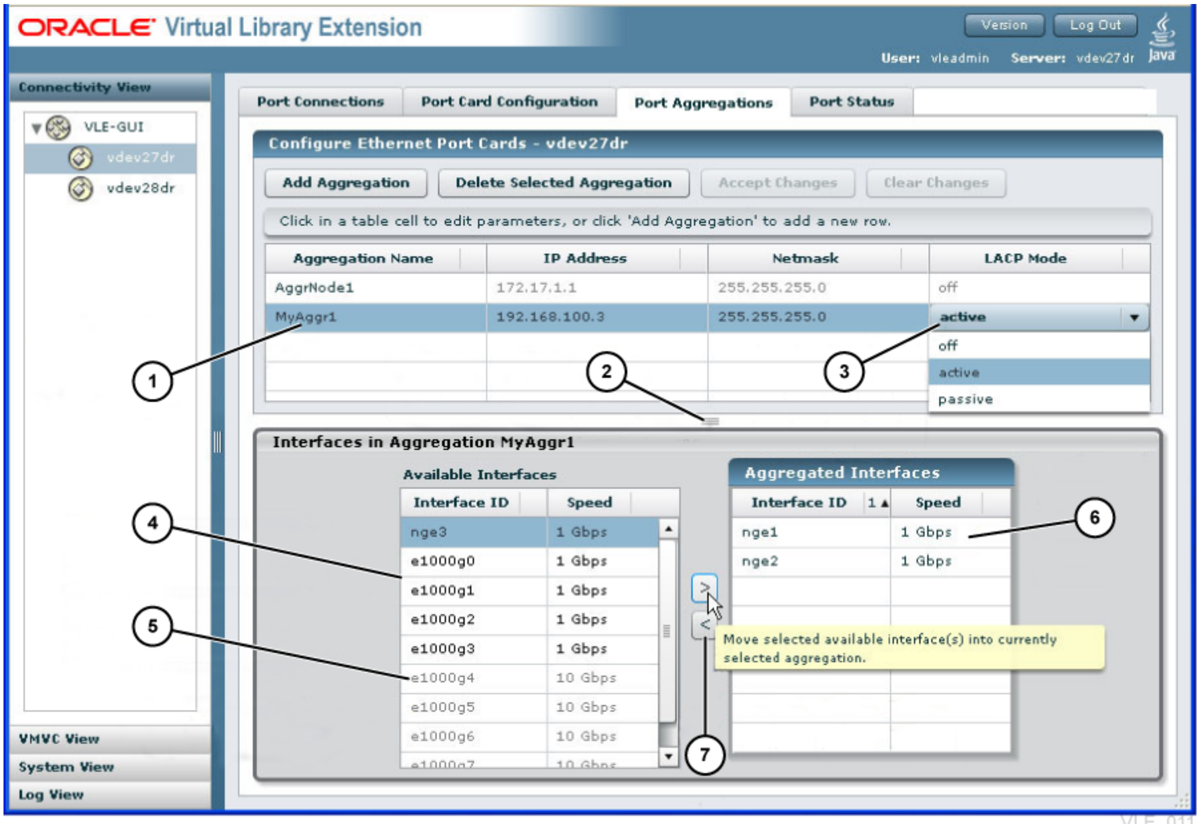
```
MGMT NAME(REDREP) MIGPOL(VLOCAL,VREMOTE)
```

In Example 3–3 both Storage Classes are enabled for deduplication. Because the corresponding VLEs are connected and configured for VLE-to-VLE replication, any jobs that specify the `REDREP` Management Class produce Reduced Replication.

Planning for Link Aggregation

Link aggregation is available for IP configuration in VLE 1.5. A link aggregation consists of multiple interfaces on a VLE node that are configured together as a single, logical unit and share a common IP address. Figure 3–5 shows the **Connectivity View, Port Aggregations** tab, which you use view the predefined "internal" aggregation port (such as `AggrNode1`) and its associated interfaces. You can also define and modify new custom aggregations using this tab.

Figure 3–5 VLE GUI Connectivity View, Port Aggregations Tab



Legend:

1. Currently selected aggregation
2. Drag-up or down to resize panes
3. Drop-down selection of options
4. Pool of port interfaces available for aggregations
5. Interfaces in currently selected aggregation
6. Ports greyed out if wrong speed for aggregation
7. Move interfaces into and out of aggregations with arrow buttons

Benefits of Link Aggregation

Link aggregation provides the following benefits:

- **Less complexity, simpler administration**. Aggregations can simplify VLE configurations by reducing the number of IP addresses required to configure a VLE node, which also prevents drain on the customer address pool. Without link aggregation, more than twenty IP addresses can be required for a fully populated VLE node. Link aggregation can reduce the number of IP addresses to 2, 3, or 4 depending on whether the node has unique Replication, UUI, and/or remote VLE IP requirements.
- **Fault tolerance.** With link aggregation, a link can fail and the traffic will switch to the remaining links, thus preventing an outage or job failure.

- **Load balancing and Bandwidth optimization**. The load is balanced by distributing the load of both inbound and outbound traffic across all links in the aggregation. Using all links as one effectively increases bandwidth because traffic is spread evenly across the aggregated links. You can also increase effective bandwidth by increasing the number of links in the aggregation.

Link Aggregation Requirements

Proceed with the following:

- All links in an aggregation must be the same speed. That is, you cannot configure a 1 GigE and a 10 GigE port in the same aggregation (the VLE GUI does not allow different port speeds in an aggregation).
- The MTU (Maximum Transmission Unit) is configured for the entire aggregation by the Jumbo Frames check-box of the **Port Card Configuration** tab (checking this box sets the MTU (Maximum Transmission Unit) value to 9000 for the aggregation. The switch must support and have the MTU size enabled for all ports within the channel group of the switch.
- An aggregation can consist of a maximum of eight links, which is enforced by the VLE GUI.
- In a switched environment, the first switch from the VLE must support Link Aggregation Control Protocol (LACP) IEEE `802.3ad` and be configured for the aggregation mode. The switch is probably a switch in the customer network, and is typically administered by a customer network administrator, who will administer the VLE configuration. Ensure that you provide the details of the configuration to the administrator.

Switch Configuration

The terms in the following sections vary between switch venders. The terms and discussion below are based on CISCO Ethernet switches. Oracle switch terminology is very similar, and can be found at:

http://docs.oracle.com/cd/E19934-01/html/E21709/z40016b9165586.html#scrolltoc

Channel Groups

A channel group is formed in the first switch that is directly connected to the VLE aggregation ports. Other switches or hops in the IPs' path need not be aware of the existence of the aggregation. The first switch is responsible for handling the traffic flow to and from the aggregation links. Each channel group is the logical grouping of an aggregation. A channel group is created for each aggregation and contains only the ports of the aggregation. The channel group ties the ports of an aggregation together so the switch can direct traffic to and from the aggregation. Because all ports connected to a channel group are known to be a part of the aggregation, **do not** connect ports to a channel group that are not a part of the aggregation. Each channel group has parameters defined for the type of LACP and so forth, and contains the rules for the aggregation.

VLANs

A typical switch configuration can consist of several VLANs (Virtual LANs) that connect the VLE to the system components, such as at VTSS or another VLE. A VLAN is a logical grouping of ports in the switch that appear externally as its own isolated switch. The VLAN is typically comprised of one or more channel groups which were created for an aggregation, along with the ports of the destination or target components such as the VTSS or another switch in a multi-hop environment.

Jumbo Frames

The MTU (Maximum Transmission Unit) is configured for the entire aggregation by the Jumbo Frames check-box of the **Port Card Configuration** tab (checking this box sets the MTU (Maximum Transmission Unit) value to 9000 for the aggregation. If Jumbo Frames are enabled, then all switches between the VLE and its target components must have Jumbo Frames enabled, as well as for all the ports of the VLAN.

LACP Mode

You can select one of the following LACP modes in the **Aggregation Table** of the **Port Aggregations** tab:

- `Off` - Sometimes referred to as manual mode, *off* indicates LACP datagrams (LACPDUs) are not sent. `Off` is the **only** valid mode without a switch. The non-switched configuration is only valid for VLE-to-VLE configurations. When using a switch with `Off` mode, LACP is not enabled in the channel group. The switch must be configured to support the aggregation.
- `Passive` – In Passive mode, datagrams are only sent when the switch requests one.
- `Active` – Datagrams are sent to the switch at regular intervals. The timer default of short is used with VLE and is not adjustable with the VLE GUI or CLI.

Policies

`P3` is the default VLE policy and is not adjustable through the VLE GUI or CLI.

10 GigE Port Aggregations

The 10 GigE links can be aggregated for VLE-to-VTSS, UUI, or VLE-to-VLE connections. Because UUI traffic is minimal, 10 GigE aggregations for UUI only have minimal benefit. 10 GigE aggregations that include all three types of connections, however, can prove beneficial. For VLE-to-VTSS configurations, the switch environment typically has both 10 GigE and 1 GigE connections. In these configurations, the 1 GigE VLE ports connect to the switch's 1 GigE ports and the VLE 10 GigE ports connect to the switch's 10 GigE ports. The 10 GBE ports would be in a channel group, and a part of a VLAN that contains both the 1 GBE and 10 GBE ports.

Note: For VLE-to-VTSS configurations, the switch environment typically has both 10 GigE and 1 GigE connections. In these configurations, the 1 GigE VLE ports connect to the switch's 1 GigE ports and the VLE 10 GigE ports connect to the switch's 10 GigE ports. The 10 GBE ports would be in a channel group and part of a VLAN that contains both the 1 GBE and 10 GBE ports.

Monitoring Aggregations

Regularly monitor aggregations. If an aggregated link fails, VLE does not generate an ASR because the other links in the aggregation still function, so VLE does not detect the failed link. You cannot monitor the status of the individual links of the aggregation. To display the status of an aggregation, go to the **Connectivity View - Port Status** tab panel of a VLE node.

If a link goes down, an entry is logged in /var/adm/messages. The message file is a part of the nightly bundle so that the log can be scanned regularly for failed links. The message in the logs look like the following example:

```
Sep 4 08:30:16 dvtvle3 mac: [ID 486395 kern.infor] NOTICE: ixgbe12 link
down
```

Types of VLE Aggregations

VLE supports three types of connections, each of which can be aggregated, as described in the following sections:

- "VLE-to-VTSS Aggregations"
- "VLE-to-VLE Aggregations"
- "VLE UUI Aggregations"

VLE-to-VTSS Aggregations

This section will describe the best practices for VLE-to-VTSS aggregations.

Best Practices

- Configure a *minimum* of two aggregations for each VTSS to prevent a total outage if an aggregation fails.
- You can connect multiple VTSS(s) to the same aggregations. For example, for a VSM5, you can connect `IFF0` from each VTSS to one aggregation, and connect `IFF2` from each VTSS to a second aggregation and so forth. If you are using only two aggregations, then you can connect `IFF0` and `IFF1` from each VTSS to the first aggregation, and so forth.
- Configure links to an aggregation horizontally across the VLE (`ixgbe4, ixgbe6, ixgbe8, ixgbe10`) to prevent an outage to an aggregation if a network adapter fails.

VLE-to-VLE Aggregations

You can aggregate VLE-to-VLE connections, as follows:

- **Non-switched** - In a non-switched configuration, the same interfaces from two VLEs form the connection. The non-switched environment works the same as the internal network of a two-node VLE without a switch. Non-switched environments are limited to point-to-point configurations only.
- **Switched** - A switched configuration is similar to the configuration described in "VLE-to-VTSS Aggregations."A channel group is formed in the switch for each aggregation, and both channel groups reside in the same VLAN.

  With multi-node VLE, a single aggregation from one node can be connected to multiple nodes of another VLE, or multiple VLEs in a switched environment.

VLE UUI Aggregations

Typically, ports `ixgbe1` and `ixgbe2` are used to make UUI connections. In this configuration, aggregate `ixgbe1` and `ixgbe2` to create a *fault-tolerant configuration*: if one of the links fail, the remaining link still provides the UUI connection. For additional redundancy on multi-node VLEs, aggregate two UUI connections on a second node.

Preparing for Cloud Extended Storage

In order to successfully install VLE 1.5.3, the following requirement must be administered:

> **Note:** Consult with a field engineer before installing VLE 1.5.3.

- A valid Cloud Storage account from Oracle which will include the account name, user name, password and URL

> **Note:** Make sure that the Cloud Storage account is in place before setting up VLE for Cloud access.

Network Requirements for Cloud Extended Storage

VLE specific Oracle Cloud User and Account Credentials need to be known before configuring the VLE Cloud. These will be different from accounts on the VLE and will need to be made with the Oracle Cloud team before they can be set up and used on a VLE.

VLE 1.5.3 must be installed to use the VLE CLI and to support Cloud specific VMVCs.

> **Note:** In order to setup a Cloud account, refer to `http://docs.oracle.com/cloud/latest/storagecs_common/index.html` for further information.

When a number of static IP address connections are set in the same subnet, the connections will work properly. If one of the cables is pulled or otherwise disrupted, however, the other connections in that subnet will be lost.

If network redundancy is required, each IP connection (between VSM 5 or 6 and VLE, VLE-to-VLE and VLE-to-SMC) must be configured on separate subnets.

A

VLE 1.5 Network Configuration

This appendix describes the VLE network starting with VLE 1.5. Configuration examples illustrate common network scenarios, including:

- "Example 1: Multiple VTSS-to-VLE Layout without Network Infrastructure"
- "Example 2: Multiple VTSS-to-VLE Layout with Network Infrastructure"
- "Example 3: Multi-node VLE Traffic"
- "Example 4: VLE-to-VLE Remote Copy Traffic"

Network Changes for VLE 1.5

With the introduction of VLE 1.5 and the X4-4 server, quad-port 1 Gb NIC connections are replaced with dual-port 10 Gb NIC connections. The potential network bandwidth for IFF/Replication connections has increased from 16 Gb (=16 x 1 Gb) to at least 40 Gb of optical bandwidth.

Additional 10 Gb copper/RJ-45 ports are also available. This additional bandwidth can simplify network setup. However, additional network infrastructure must be provided by the customer to accommodate this additional bandwidth.

In general, functions are isolated to specific networks on specific ports. This ensures bandwidth for a given function is theoretically available.

Additionally, separate subnets for all interfaces/aggregations is considered a best practice since a link failure could down other VLE ports on the same subnet.

Table A–1 shows the position and function for each of the VLE 1.5 ports in the X4-4 server.

For comparison, Table A–2 shows the same information for versions prior to VLE 1.5.

In Table A–1 and Table A–2:

- "Cu" indicates Copper/RJ45.
- "O" indicates Optical.
- "O or Cu" indicates either; Optical is the default and Cu is 1 Gb only.
- For fields with an apostrophe (*), note that customers have exploited open 10 Gb connections for VSM5/VSM6 IFF/Replication.

Table A–1 VLE X4-4 VLE Network Configuration (introduced with VLE 1.5)

Position	Port	IFF/REP	Function
MB(Cu)	0	0	ASR
	1		UUI
	2		UUI
	3		Service Access
PCIE3 (O or Cu)	0	1	IFF/Replication
	1	2	IFF/Replication
PCIE5 (O or Cu)	0		Node-to-Node Grid Traffic ((VLE Private)
	1	*	Remote Copy Traffic (VLE to VLE)
PCIE8 (O or Cu)	0		Node-to-Node Grid TRaffic (VLE Private)
	1	*	Remote Copy Traffic (VLE to VLE)
PCIE10 (O or Cu)	0	3	IFF/Replication Traffic
	1	4	IFF/Replication Traffic
PCIE11 (Cu)	0	5	IFF/Replication Traffic
	1	6	IFF/Replication Traffic

For comparison, Table A–2 shows the same information for versions prior to VLE 1.5.

Table A–2 VLE X4470/X4470M2/X2-4 Network Configuration (before VLE 1.5)

Position	Port	IFF/REP	Function
MB (cu)	0	0	ASR
	1		UUI
	2		UUI
	3		Service Access
PCIE0	0	1	IFF/Replication
	1	2	IFF/Replication
	2	3	IFF/Replication
	3	4	IFF/Replication
PCIE3 (10Gb)	0		Node-to-Node Grid Traffic ((VLE Private)
	1	*	Remote Copy Traffic (VLE to VLE)
PCIE4	0	5	IFF/Replication
	1	6	IFF/Replication
	2	7	IFF/Replication
	3	8	IFF/Replication
PCIE5	0	9	IFF/Replication Traffic
	1	10	IFF/Replication Traffic
	2	11	IFF/Replication Traffic
	3	12	IFF/Replication Traffic
PCIE8 (10Gb)	0		Node-to-Node Grid Traffic (VLE Private)
	1	*	Remote Copy Traffic (VLE-to-VLE)

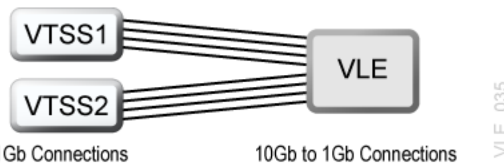
Table A–2 (Cont.) VLE X4470/X4470M2/X2-4 Network Configuration (before VLE 1.5)

Position	Port	IFF/REP	Function
PCIE9	0	13	IFF/Replication Traffic
	1	14	IFF/Replication Traffic
	2	15	IFF/Replication Traffic
	3	16	IFF/Replication Traffic

Example 1: Multiple VTSS-to-VLE Layout without Network Infrastructure

This example illustrates a multiple VTSS-to-VLE network layout (Replication/IFF/Replication) without network infrastructure, as shown in Figure A–1.

Figure A–1 Multiple VTSS-to-VLE without Network Infrastructure



If an environment lacks additional network infrastructure to utilize the full 10 Gb bandwidth, and remote copy capability is *not* a requirement, up to eight (8) IFF/Replication ports can be directly connected to VTSS ports.

These ports will need to be converted to copper, and will only run at 1 Gb link speed (for potential total bandwidth of 8 Gb).

As noted earlier, separate subnets for all interfaces is considered a best practice since a link failure could down other VLE ports on the same subnet.

Table A–3 shows the ports that can be used for IFF/Replication traffic in this example.

Table A–3 VLE IFF/Replication Links

Link	Device	Location	
ixgbe0	ixgbe0	/SYS/MB	
ixgbe1	ixgbe1	/SYS/MB	
ixgbe2	ixgbe2	/SYS/MB	
ixgbe3	ixgbe3	/SYS/MB	
ixgbe4	ixgbe4	/SYS/MB/PCI3	IFF/Replication Traffic
ixgbe5	ixgbe5	/SYS/MB/PCI3	IFF/Replication Traffic
ixgbe6	ixgbe6	/SYS/MB/PCI5	
ixgbe7	ixgbe7	/SYS/MB/PCI5	IFF/Replication Traffic
ixgbe8	ixgbe8	/SYS/MB/PCI8	
ixgbe9	ixgbe9	/SYS/MB/PCI8	IFF/Replication Traffic
ixgbe10	ixgbe10	/SYS/MB/PCI10	IFF/Replication Traffic
ixgbe11	ixgbe11	/SYS/MB/PCI10	IFF/Replication Traffic
ixgbe12	ixgbe12	/SYS/MB/PCI11	IFF/Replication Traffic

Table A–3 (Cont.) VLE IFF/Replication Links

Link	Device	Location	
ixgbe13	ixgbe13	/SYS/MB/PCI11	IFF/Replication Traffic

VTSS and VLE connections for this scenario:

VTSS1	IFF/REP1	192.168.1.11/24
	IFF/REP2	192.168.2.11/24
	IFF/REP3	192.168.3.11/24
	IFF/REP4	192.168.4.11/24

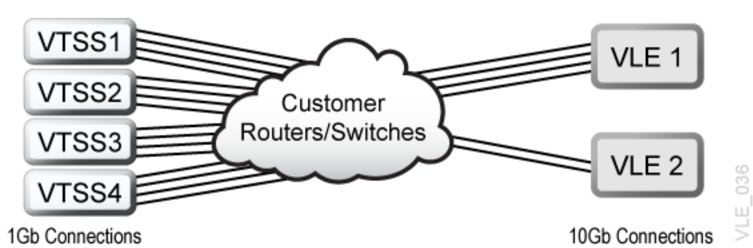
VTSS2	IFF/REP1	192.168.5.11/24
	IFF/REP2	192.168.6.11/24
	IFF/REP3	192.168.7.11/24
	IFF/REP4	192.168.8.11/24

VLE	ixgbe4	192.168.1.10/24
	ixgbe5	192.168.2.10/24
	ixgbe7	192.168.3.10/24
	ixgbe9	192.168.4.10/24
	ixgbe10	192.168.5.10/24
	ixgbe11	192.168.6.10/24
	ixgbe12	192.168.7.10/24
	ixgbe13	192.168.8.10/24

Example 2: Multiple VTSS-to-VLE Layout with Network Infrastructure

This example illustrates a multiple VTSS-to-VLE network layout (Replication/IFF/Replication) with network infrastructure, as shown in Figure A–2.

Figure A–2 Multiple VTSS-to-VLE Layout with Network Infrastructure



While direct connections were technically feasible with the quad-port NICs, that is no longer an option with dual-port 10 Gb NICs. However, the two 10 Gb ports can satisfy the bandwidth needs of the 16, 1 Gb connections. To do this, the customer must provide network infrastructure for the VLE ports to support 10 Gb link speeds and

LACP aggregation, as well as proper routing if VTSS connections and the VLE ports are on different subnets.

VTSS connections for this scenario:

VTSS1	IFF/REP1	192.168.1.11/24
	IFF/REP2	192.168.2.11/24
	IFF/REP3	192.168.3.11/24
	IFF/REP4	192.168.4.11/24

VTSS2	IFF/REP1	192.168.1.12/24
	IFF/REP2	192.168.2.12/24
	IFF/REP3	192.168.3.12/24
	IFF/REP4	192.168.4.12/24

VTSS3	IFF/REP1	192.168.1.13/24
	IFF/REP2	192.168.2.13/24
	IFF/REP3	192.168.3.13/24
	IFF/REP4	192.168.4.13/24

VTSS4	IFF/REP1	192.168.1.14/24
	IFF/REP2	192.168.2.14/24
	IFF/REP3	192.168.3.14/24
	IFF/REP4	192.168.4.14/24

Caution: The customer must ensure that routing is possible between all IFF/Replication connections and the VLE IP addresses.

VLE connections for this scenario:

Link	Device	Location
ixgbe4	ixgbe4	/SYS/MB/PCI3
ixgbe5	ixgbe5	/SYS/MB/PCI3
ixgbe10	ixgbe10	/SYS/MB/PCI10
ixgbe11	ixgbe11	/SYS/MB/PCI10

Configure the IP addresses for the four IFF/Replication subnets on each VTSS.

VLE1	ixgbe4	192.168.1.10/24
	ixgbe5	192.168.2.10/24
	ixgbe10	192.168.3.10/24

	ixgbe11	192.168.4.10/24

Create an aggregation using ixgbe4 and ixgbe10 and assign a single IP address. This provides 20 Gb of bandwidth and redundancy.

Note: Link failure will reduce bandwidth to 10 Gb.

VLE2		ixgbe4	
	aggr2		192.168.1.10/24
		ixgbe10	

Example 3: Multi-node VLE Traffic

This example illustrates a network layout for a multi-node VLE.

Up to 16 VLE nodes may be configured in a multi-node VLE system that operates within a VLE private network (172.17.1.0/24).

Systems with one or two nodes use direct connect ports, while systems with three or more nodes require the Oracle 72 Switch.

Table A–4 shows the ports that can be used for multi-node traffic in this example.

Table A–4 VLE Multi-Node Links

Link	Device	Location	
ixgbe0	ixgbe0	/SYS/MB	
ixgbe1	ixgbe1	/SYS/MB	
ixgbe2	ixgbe2	/SYS/MB	
ixgbe3	ixgbe3	/SYS/MB	
ixgbe4	ixgbe4	/SYS/MB/PCI3	
ixgbe5	ixgbe5	/SYS/MB/PCI3	
ixgbe6	ixgbe6	/SYS/MB/PCI5	Multi-node traffic
ixgbe7	ixgbe7	/SYS/MB/PCI5	
ixgbe8	ixgbe8	/SYS/MB/PCI8	Multi-node traffic
ixgbe9	ixgbe9	/SYS/MB/PCI8	
ixgbe10	ixgbe10	/SYS/MB/PCI10	
ixgbe11	ixgbe11	/SYS/MB/PCI10	
ixgbe12	ixgbe12	/SYS/MB/PCI11	
ixgbe13	ixgbe13	/SYS/MB/PCI11	

Ports are pre-configured in an aggregate and are configured with an IP address based on the number of nodes in the multi-node VLE system:

1	172.17.1.1/24
2	172.17.1.2/24

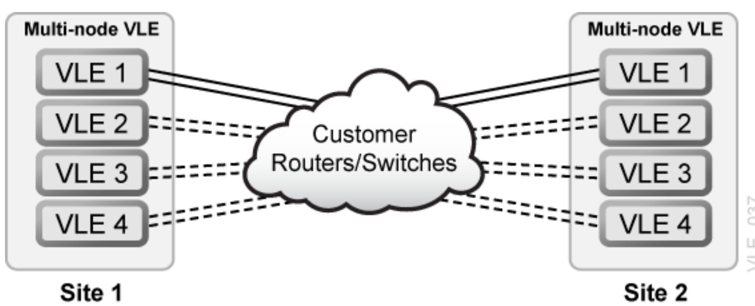
3	172.17.1.3/24
4	172.17.1.4/24
5	172.17.1.5/24
6	172.17.1.6/24
7	172.17.1.7/24
8	172.17.1.8/24
9	172.17.1.9/24
10	172.17.1.10/24
11	172.17.1.11/24
12	172.17.1.12/24
13	172.17.1.13/24
14	172.17.1.14/24
15	172.17.1.15/24
16	172.17.1.16/24

Refer to the separate document *Installing an Oracle 72 port 10Gb Ethernet TOR Switch in a VLE System* for more information.

Example 4: VLE-to-VLE Remote Copy Traffic

This example illustrates a network layout for VLE-to-VLE remote copy traffic., as shown in Figure A–3.

Figure A–3 VLE-to-VLE Remote Copy Traffic



The bottom ports in slot 5 and slot 8 are generally set aside for remote copy traffic to other VLE subsystems at remote sites. As with IFF/Replication traffic, these ports can be aggregated as one link or operated independently on unique subnets.

Table A–5 shows the ports that can be used for remote copy traffic in this example.

Table A–5 VLE Remote Copy Links

Link	Device	Location
ixgbe0	ixgbe0	/SYS/MB
ixgbe1	ixgbe1	/SYS/MB
ixgbe2	ixgbe2	/SYS/MB

Table A–5 (Cont.) VLE Remote Copy Links

Link	Device	Location	
ixgbe3	ixgbe3	/SYS/MB	
ixgbe4	ixgbe4	/SYS/MB/PCI3	
ixgbe5	ixgbe5	/SYS/MB/PCI3	
ixgbe6	ixgbe6	/SYS/MB/PCI5	
ixgbe7	ixgbe7	/SYS/MB/PCI5	Remote Copy traffic
ixgbe8	ixgbe8	/SYS/MB/PCI8	
ixgbe9	ixgbe9	/SYS/MB/PCI8	Remote Copy traffic
ixgbe10	ixgbe10	/SYS/MB/PCI10	
ixgbe11	ixgbe11	/SYS/MB/PCI10	
ixgbe12	ixgbe12	/SYS/MB/PCI11	
ixgbe13	ixgbe13	/SYS/MB/PCI11	

Caution: Customers must ensure that routing is possible between all remote copy networks and ports.

VLE connections for this scenario:

Site #1	VLE1	192.168.10.101/24
	VLE2	192.168.10.102/24
	VLE3	192.168.10.103/24
	VLE4	192.168.10.104/24

Site #2	VLE1	172.27.10.101/24
	VLE2	172.27.10.102/24
	VLE3	172.27.10.103/24
	VLE4	172.27.10.104/24

At least one pair of 10 Gb links are recommended between a VLE node at each site. However, additional links for other nodes may be optionally added if network bandwidth is available.

B

Controlling Contaminants

Appendix B explains the requirements for controlling contaminants.

Environmental Contaminants

Control over contaminant levels in a computer room is extremely important because tape libraries, tape drives, and tape media are subject to damage from airborne particulates. Most particles smaller than ten microns are not visible to the naked eye under most conditions, but these particles can be the most damaging. As a result, the operating environment must adhere to the following requirements:

- ISO 14644-1 Class 8 Environment.
- The total mass of airborne particulates must be less than or equal to 200 micrograms per cubic meter.
- Severity level G1 per ANSI/ISA 71.04-1985.

Oracle currently requires the ISO 14644-1 standard approved in 1999, but will require any updated standards for ISO 14644-1 as they are approved by the ISO governing body. The ISO 14644-1 standard primarily focuses on the quantity and size of particulates and the proper measurement methodology, but does not address the overall mass of the particulates. As a result, the requirement for total mass limitations is also necessary as a computer room or data center could meet the ISO 14644-1 specification, but still damage equipment because of the specific type of particulates in the room. In addition, the ANSI/ISA 71.04-1985 specification addresses gaseous contaminations as some airborne chemicals are more hazardous. All three requirements are consistent with the requirements set by other major tape storage vendors.

Required Air Quality Levels

Particles, gasses and other contaminants may impact the sustained operations of computer hardware. Effects can range from intermittent interference to actual component failures. The computer room must be designed to achieve a high level of cleanliness. Airborne dusts, gasses and vapors must be maintained within defined limits to help minimize their potential impact on the hardware.

Airborne particulate levels must be maintained within the limits of *ISO 14644-1 Class 8 Environment*. This standard defines air quality classes for clean zones based on airborne particulate concentrations. This standard has an order of magnitude less particles than standard air in an office environment. Particles ten microns or smaller are harmful to most data processing hardware because they tend to exist in large numbers, and can easily circumvent many sensitive components' internal air filtration systems. When computer hardware is exposed to these submicron particles in great numbers they endanger system reliability by posing a threat to moving parts, sensitive contacts and component corrosion.

Excessive concentrations of certain gasses can also accelerate corrosion and cause failure in electronic components. Gaseous contaminants are a particular concern in a computer room both because of the sensitivity of the hardware, and because a proper computer room environment is almost entirely recirculating. Any contaminant threat in the room is compounded by the cyclical nature of the airflow patterns. Levels of exposure that might not be concerning in a well ventilated site repeatedly attack the hardware in a room with recirculating air. The isolation that prevents exposure of the computer room environment to outside influences can also multiply any detrimental influences left unaddressed in the room.

Gasses that are particularly dangerous to electronic components include chlorine compounds, ammonia and its derivatives, oxides of sulfur and petrol hydrocarbons. In the absence of appropriate hardware exposure limits, health exposure limits must be used.

While the following sections will describe some best practices for maintaining an ISO 14644-1 Class 8 Environment in detail, there are some basic precautions that must be adhered to:

- Do not allow food or drink into the area.
- Cardboard, wood, or packing materials must not be stored in the data center clean area.
- Identify a separate area for unpacking new equipment from crates and boxes.
- Do not allow construction or drilling in the data center without first isolating sensitive equipment and any air targeted specifically for the equipment. Construction generates a high level of particulates that exceed ISO 14644-1 Class 8 criteria in a localized area. Dry wall and gypsum are especially damaging to storage equipment.

Contaminant Properties and Sources

Contaminants in the room can take many forms, and can come from numerous sources. Any mechanical process in the room can produce dangerous contaminants or agitate settled contaminants. A particle must meet two basic criteria to be considered a contaminant:

- It must have the physical properties that could potentially cause damage to the hardware.
- It must be able to migrate to areas where it can cause the physical damage.

The only differences between a potential contaminant and an actual contaminant are time and location. Particulate matter is most likely to migrate to areas where it can do damage if it is airborne. For this reason, airborne particulate concentration is a useful measurement in determining the quality of the computer room environment. Depending on local conditions, particles as big as 1,000 microns can become airborne, but their active life is very short, and they are arrested by most filtration devices. Submicron particulates are much more dangerous to sensitive computer hardware, because they remain airborne for a much longer period of time and are more apt to bypass filters.

Operator Activity

Human movement within the computer space is probably the single greatest source of contamination in an otherwise clean computer room. Normal movement can dislodge tissue fragments, such as dander or hair, or fabric fibers from clothing. The opening and closing of drawers or hardware panels, or any metal-on-metal activity, can produce metal filings. Simply walking across the floor can agitate settled contamination, making it airborne and potentially dangerous.

Hardware Movement

Hardware installation or reconfiguration involves a great deal of subfloor activity, and settled contaminants can very easily be disturbed, forcing them to become airborne in the supply air stream to the rooms' hardware. This is particularly dangerous if the subfloor deck is unsealed. Unsealed concrete sheds fine dust particles into the airstream, and is susceptible to efflorescence -- mineral salts brought to the surface of the deck through evaporation or hydrostatic pressure.

Outside Air

Inadequately filtered air from outside of the controlled environment can introduce innumerable contaminants. Post-filtration contamination in duct work can be dislodged by air flow, and introduced into the hardware environment. This is particularly important in a downward-flow air conditioning system in which the sub-floor void is used as a supply air duct. If the structural deck is contaminated, or if the concrete slab is not sealed, fine particulate matter (such as concrete dust or efflorescence) can be carried directly to the rooms' hardware.

Stored Items

Storage and handling of unused hardware or supplies can also be a source of contamination. Corrugated cardboard boxes or wooden skids shed fibers when moved or handled. Stored items are not only contamination sources; their handling in the computer room controlled areas can agitate settled contamination already in the room.

Outside Influences

A negatively pressurized environment can allow contaminants from adjoining office areas or the exterior of the building to infiltrate the computer room environment through gaps in the doors or penetrations in the walls. Ammonia and phosphates are often associated with agricultural processes, and numerous chemical agents can be produced in manufacturing areas. If such industries are present near the data center facility, chemical filtration may be necessary. Potential impact from automobile emissions, dusts from local quarries or masonry fabrication facilities or sea mists should also be assessed, if relevant.

Cleaning Activity

Inappropriate cleaning practices can also degrade the environment. Many chemicals used in normal or "office" cleaning applications can damage sensitive computer equipment. Potentially hazardous chemicals outlined in the "Cleaning Procedures and Equipment" section should be avoided. Out-gassing from these products or direct contact with hardware components can cause failure. Certain biocide treatments used in building air handlers are also inappropriate for use in computer rooms, either because they contain chemicals that can degrade components, or because they are not designed to be used in the airstream of a re-circulating air system. The use of push mops or inadequately filtered vacuums can also stimulate contamination.

It is essential that steps be taken to prevent air contaminants, such as metal particles, atmospheric dust, solvent vapors, corrosive gasses, soot, airborne fibers or salts from entering or being generated within the computer room environment. In the absence of hardware exposure limits, use applicable human exposure limits from OSHA, NIOSH or the ACGIH.

Contaminant Effects

Destructive interactions between airborne particulate and electronic instrumentation can occur in numerous ways. The means of interference depends on the time and location of the critical incident, the physical properties of the contaminant and the environment in which the component is placed.

Physical Interference

Hard particles with a tensile strength at least 10% greater than that of the component material can remove material from the surface of the component by grinding action or embedding. Soft particles will not damage the surface of the component, but can collect in patches that can interfere with proper functioning. If these particles are tacky they can collect other particulate matter. Even very small particles can have an impact if they collect on a tacky surface, or agglomerate as the result of electrostatic charge build-up.

Corrosive Failure

Corrosive failure or contact intermittence due to the intrinsic composition of the particles or due to absorption of water vapor and gaseous contaminants by the particles can also cause failures. The chemical composition of the contaminant can be very important. Salts, for instance, can grow by absorbing water vapor from the air (nucleating). If a mineral salts deposit exists in a sensitive location, and the environment is sufficiently moist, it can grow to a size where it can physically interfere with a mechanism, or can cause damage by forming salt solutions.

Shorts

Conductive pathways can arise through the accumulation of particles on circuit boards or other components. Many types of particulate are not inherently conductive, but can absorb significant quantities of water in high-moisture environments. Problems caused by electrically conductive particles can range from intermittent malfunctioning, to actual damage to components and operational failures.

Thermal Failure

Premature clogging of filtered devices will cause a restriction in air flow that could induce internal overheating and head crashes. Heavy layers of accumulated dust on hardware components can also form an insulated layer that can lead to heat-related failures.

Room Conditions

All surfaces within the controlled zone of the data center should be maintained at a high level of cleanliness. All surfaces should be periodically cleaned by trained professionals on a regular basis, as outlined in the "Cleaning Procedures and Equipment" section. Particular attention should be paid to the areas beneath the hardware, and the access floor grid. Contaminants near the air intakes of the hardware can more easily be transferred to areas where they can do damage. Particulate accumulations on the access floor grid can be forced airborne when floor tiles are lifted to gain access to the sub-floor.

The subfloor void in a downward-flow air conditioning system acts as the supply air plenum. This area is pressurized by the air conditioners, and the conditioned air is then introduced into the hardware spaces through perforated floor panels. Thus, all air traveling from the air conditioners to the hardware must first pass through the subfloor void. Inappropriate conditions in the supply air plenum can have a dramatic effect on conditions in the hardware areas.

The subfloor void in a data center is often viewed solely as a convenient place to run cables and pipes. It is important to remember that this is also a duct, and that conditions below the false floor must be maintained at a high level of cleanliness. Contaminant sources can include degrading building materials, operator activity or infiltration from outside the controlled zone. Often, particulate deposits are formed where cables or other subfloor items form air dams that allow particulate to settle and accumulate. When these items are moved, the particulate is re-introduced into the supply airstream, where it can be carried directly to hardware.

Damaged or inappropriately protected building materials are often sources of subfloor contamination. Unprotected concrete, masonry block, plaster or gypsum wall-board will deteriorate over time, shedding fine particulate into the air. Corrosion on post-filtration air conditioner surfaces or subfloor items can also be a concern. The subfloor void must be thoroughly and appropriately decontaminated on a regular basis to address these contaminants. Use only vacuums equipped with High Efficiency Particulate Air (HEPA) filtration in any decontamination procedure. Inadequately filtered vacuums will not arrest fine particles, passing them through the unit at high speeds, and forcing them airborne.

Unsealed concrete, masonry or other similar materials are subject to continued degradation. The sealants and hardeners normally used during construction are often designed to protect the deck against heavy traffic, or to prepare the deck for the application of flooring materials, and are not meant for the interior surfaces of a supply air plenum. While regular decontaminations will help address loose particulate, the surfaces will still be subject to deterioration over time, or as subfloor activity causes wear. Ideally, all subfloor surfaces will be appropriately sealed at the time of construction. If this is not the case, special precautions will be necessary to address the surfaces in an on-line room.

It is extremely important that only appropriate materials and methodology are used in the encapsulation process. Inappropriate sealants or procedures can actually degrade the conditions they are meant to improve, impacting hardware operations and reliability. The following precautions should be taken when encapsulating the supply air plenum in an on-line room:

- Manually apply the encapsulant. Spray applications are inappropriate in an on-line data center. The spraying process forces the sealant airborne in the supply airstream, and is more likely to encapsulate cables to the deck.
- Use a pigmented encapsulant. The pigmentation makes the encapsulant visible in application, ensuring thorough coverage, and helps in identifying areas that are damaged or exposed over time.

- The encapsulant must have a high flexibility and low porosity to effectively cover the irregular textures of the subject area, and to minimize moisture migration and water damage.
- The encapsulant must not out-gas any harmful contaminants. Many encapsulants commonly used in the industry are highly ammoniated, or contain other chemicals that can be harmful to hardware. It is unlikely that this out-gassing could cause immediate, catastrophic failure, but these chemicals will often contribute to corrosion of contacts, heads or other components.

Effectively encapsulating a subfloor deck in an on-line computer room is a very sensitive and difficult task, but it can be conducted safely if appropriate procedures and materials are used.

Avoid using the ceiling void as an open supply or return for the building air system. This area is typically very dirty and difficult to clean. Often, the structural surfaces are coated with fibrous fire-proofing, and the ceiling tiles and insulation are also subject to shedding. Before filtration, this is an unnecessary exposure that can adversely affect environmental conditions in the room. It is important that the ceiling void does not become pressurized, as this will force dirty air into the computer room. Columns or cable chases with penetrations in both the subfloor and ceiling void can lead to ceiling void pressurization.

Exposure Points

All potential exposure points in the data center should be addressed to minimize potential influences from outside the controlled zone. Positive pressurization of the computer rooms will help limit contaminant infiltration, but it is also important to minimize any breaches in the room perimeter. To ensure that the environment is maintained correctly, the following should be considered:

- All doors should fit snugly in their frames.
- Use gaskets and sweeps or address any gaps.
- Avoid automatic doors in areas where they can be accidentally triggered. An alternate means of control would be to remotely locate a door trigger so that personnel pushing carts can open the doors easily. In highly sensitive areas, or where the data center is exposed to undesirable conditions, it may be advisable to design and install personnel traps. Double sets of doors with a buffer between can help limit direct exposure to outside conditions.
- Seal all penetrations between the data center and adjacent areas.
- Avoid sharing a computer room ceiling or subfloor plenum with loosely controlled, adjacent areas.

Filtration

Filtration is an effective means of addressing airborne particulate in a controlled environment. It is important that all air handlers serving the data center are adequately filtered to ensure that appropriate conditions are maintained within the room. In-room process cooling is the recommended method of controlling the room environment. The in-room process coolers re-circulate room air. Air from the hardware areas is passed through the units where it is filtered and cooled, and then introduced into the subfloor plenum. The plenum is pressurized, and the conditioned air is forced into the room, through perforated tiles, which then travels back to the air conditioner for reconditioning. The airflow patterns and design associated with a typical computer room air handler have a much higher rate of air change than typical comfort cooling air conditioners, so air is filtered more often than in an office environment. Proper filtration can capture a great deal of particulates. The filters installed in the in-room, re-circulating air conditioners should have a minimum efficiency of 40% (Atmospheric Dust-Spot Efficiency, ASHRAE Standard 52.1). Low-grade pre-filters should be installed to help prolong the life of the more expensive primary filters.

Any air being introduced into the computer room controlled zone, for ventilation or positive pressurization, should first pass through high efficiency filtration. Ideally, air from sources outside of the building should be filtered using High Efficiency Particulate Air (HEPA) filtration rated at 99.97% efficiency (DOP Efficiency MILSTD-282) or greater. The expensive high efficiency filters should be protected by multiple layers of pre-filters that are changed on a more frequent basis. Low-grade pre-filters, 20% ASHRAE atmospheric dust-spot efficiency, should be the primary line of defense. The next filter bank should consist of pleated or bag type filters with efficiencies between 60% and 80% ASHRAE atmospheric dust-spot efficiency.

ASHRAE 52-76 Dust spot efficiency %	Fractional Efficiencies %		
	3.0 micron	**1.0 micron**	**0.3 micron**
25-30	80	20	<5
60-65	93	50	20
80-85	99	90	50
90	>99	92	60
DOP 95	--	>99	95

Low efficiency filters are almost totally ineffective at removing sub-micron particulates from the air. It is also important that the filters used are properly sized for the air handlers. Gaps around the filter panels can allow air to bypass the filter as it passes through the air conditioner. Any gaps or openings should be filled using appropriate materials, such as stainless steel panels or custom filter assemblies.

Positive Pressurization and Ventilation

A designed introduction of air from outside of the computer room system will be necessary to accommodate positive pressurization and ventilation requirements. The data center should be designed to achieve positive pressurization in relation to more loosely controlled surrounding areas. Positive pressurization of the more sensitive areas is an effective means of controlling contaminant infiltration through any minor breaches in the room perimeter. Positive pressure systems are designed to apply outward air forces to doorways and other access points within the data processing center, in order to minimize contaminant infiltration of the computer room. Only a minimal amount of air should be introduced into the controlled environment. In data centers with multiple rooms, the most sensitive areas should be the most highly pressurized. It is, however, extremely important that the air being used to positively pressurize the room does not adversely affect the environmental conditions in the room. It is essential that any air introduction from outside the computer room is adequately filtered and conditioned to ensure that it is within acceptable parameters. These parameters can be looser than the goal conditions for the room since the air introduction should be minimal. A precise determination of acceptable limits should be based on the amount of air being introduced and the potential impact on the environment of the data center.

Because a closed-loop, re-circulating air conditioning system is used in most data centers, it will be necessary to introduce a minimal amount of air to meet the ventilation requirements of the room occupants. Data center areas normally have a very low human population density; thus, the air required for ventilation will be minimal. In most cases, the air needed to achieve positive pressurization will likely exceed that needed to accommodate the room occupants. Normally, outside air quantities of less than 5% make-up air should be sufficient (ASHRAE Handbook: Applications, Chapter 17). A volume of 15 CFM outside air per occupant or workstation should sufficiently accommodate the ventilation needs of the room.

Cleaning Procedures and Equipment

Even a perfectly designed data center requires continued maintenance. Data centers containing design flaws or compromises may require extensive efforts to maintain conditions within desired limits. Hardware performance is an important factor contributing to the need for a high level of cleanliness in the data center.

Operator awareness is another consideration. Maintaining a fairly high level of cleanliness will raise the level of occupant awareness, with respect to special requirements and restrictions while in the data center. Occupants or visitors to the data center will hold the controlled environment in high regard, and are more likely to act appropriately. Any environment that is maintained to a fairly high level of cleanliness and is kept in a neat and well organized fashion will also command respect from the rooms' inhabitants and visitors.

When potential clients visit the room, they will interpret the overall appearance of the room as a reflection of an overall commitment to excellence and quality. An effective cleaning schedule must consist of specially designed short-term and long-term actions. These can be summarized, as follows:

Frequency	Task
Daily Actions	Rubbish removal
Weekly Actions	Access floor maintenance (vacuum and damp mop)
Quarterly Actions	Hardware decontamination Room surface decontamination
Biennial Actions	Subfloor void decontamination Air conditioner decontamination (as necessary)

Daily Tasks

This statement of work focuses on the removal of each day's discarded trash and rubbish from the room. In addition, daily floor vacuuming may be required in Print Rooms or rooms with a considerable amount of operator activity.

Weekly Tasks

This statement of work focuses on the maintenance of the access floor system. During the week, the access floor becomes soiled with dust accumulations and blemishes. The entire access floor should be vacuumed and damp mopped. All vacuums used in the data center, for any purpose, should be equipped with High Efficiency Particulate Air (HEPA) filtration. Inadequately filtered equipment cannot arrest smaller particles, but rather simply agitates them, degrading the environment they were meant to improve. It is also important that mop-heads and dust wipes are of appropriate non-shedding designs.

Cleaning solutions used within the data center must not pose a threat to the hardware. Solutions that could potentially damage hardware include products that are:

- Ammoniated
- Chlorine-based
- Phosphate-based
- Bleach enriched
- Petro-chemical based
- Floor strippers or re-conditioners

It is important that the recommended concentrations are used, as even an appropriate agent, in an inappropriate concentration can be potentially damaging. The solution should be maintained in good condition throughout the project, and excessive applications should be avoided.

Quarterly Tasks

The quarterly statement of work involves a much more detailed and comprehensive decontamination schedule, and should only be conducted by experienced computer room contamination-control professionals. These actions should be performed three to four times per year, based on the levels of activity and contamination present. All room surfaces should be thoroughly decontaminated, including: cupboards, ledges, racks, shelves and support equipment. High ledges and light fixtures and generally accessible areas should be treated or vacuumed, as appropriate. Vertical surfaces including windows, glass partitions, doors, and so on should be thoroughly treated. Special dust cloths that are impregnated with a particle absorbent material are to be used in the surface decontamination process. Do not use generic dust rags or fabric cloths to perform these activities. Do not use any chemicals, waxes or solvents during these activities.

Settled contamination should be removed from all exterior hardware surfaces, including: horizontal and vertical surfaces. The unit air inlet and outlet grilles should be treated, as well. Do not wipe the unit control surfaces as these areas can be decontaminated by the use of lightly compressed air. Special care should also be taken when cleaning keyboards and life-safety controls. Use specially treated dust wipes to treat all hardware surfaces. Monitors should be treated with optical cleansers and static-free cloths. Do not use Electro-Static Discharge (ESD) dissipative chemicals on the computer hardware, since these agents are caustic and harmful to most sensitive hardware. The computer hardware is sufficiently designed to permit electrostatic dissipation thus no further treatments are required. After all of the hardware and room surfaces have been thoroughly decontaminated, the access floor should be HEPA vacuumed and damp mopped as detailed in the Weekly Actions.

Biennial Tasks

The subfloor void should be decontaminated every 18 months to 24 months based on the conditions of the plenum surfaces and the degree of contaminant accumulation. Over the course of the year, the subfloor void undergoes a considerable amount of activity that creates new contamination accumulations. Although the weekly above floor cleaning activities will greatly reduce the subfloor dust accumulations, a certain amount of surface dirt will migrate into the subfloor void. It is important to maintain the subfloor to a high degree of cleanliness since this area acts as the hardware's supply air plenum. It is best to perform the subfloor decontamination treatment in a short time frame to reduce cross contamination. The personnel performing this operation should be fully trained to assess cable connectivity and priority. Each exposed area of the subfloor void should be individually inspected and assessed for possible cable handling and movement. All twist-in and plug-in connections should be checked and fully engaged before cable movement. All subfloor activities must be conducted with proper consideration for air distribution and floor loading. In an effort to maintain access floor integrity and proper psychrometric conditions, the number of floor tiles removed from the floor system should be carefully managed. In most cases, each work crew should have no more than 24 square feet (six tiles) of open access flooring at any one time. The access floor's supporting grid system should also be thoroughly decontaminated, first by vacuuming the loose debris, followed by damp-sponging the accumulated residue. Rubber gaskets, if present, as the metal framework that makes up the grid system should be removed from the grid work and cleaned with a damp sponge, as well. Any unusual conditions, such as damaged floor suspension, floor tiles, cables, and surfaces within the floor void, should be noted and reported.

Activity and Processes

Isolation of the data center is an integral factor in maintaining appropriate conditions. All unnecessary activity should be avoided in the data center, and access should be limited to necessary personnel only. Periodic activity, such as tours, should be limited, and traffic should be restricted away from the hardware to avoid accidental contact. All personnel working in the room, including temporary employees and janitorial personnel, should be trained in the most basic sensitivities of the hardware to avoid unnecessary exposure. The controlled areas of the data center should be thoroughly isolated from contaminant producing activities.

Ideally, print rooms, check-sorting rooms, command centers, or other areas with high levels of mechanical or human activity should have no direct exposure to the data center. Paths to and from these areas should not necessitate traffic through the main data center areas.

Index