StorageTek Virtual Library Extension

Planning Guide

E41530-04

April 2014

StorageTek Virtual Library Extension Planning Guide

E41530-04

Contents

A VLE Configuration Examples

B VLE Link Aggregation Examples

C Controlling Contaminants

Index

List of Figures

List of Tables

Preface

This preface introduces this guide.

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 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*
- *VLE Documentation Third Party Licenses and Notices*
- *Written Offer to Provide Certain Source Code*
- VLE Safety Guide

1

What is Virtual Library Extension?

Oracle's StorageTek Virtual Library Extension (VLE) is back-end disk storage for VTSS. VLE provides:

- 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.

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

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:

- **Note that** 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.
- **Also note that** 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.
- **Note that** in Tapeless VSM configurations, if you have only a single-node VLE attached to a specific VTSS and that VLE goes offline, you lose access to any VTVs migrated to the VLE that are not resident in the VTSS until the VLE comes back online.

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

VLE Hardware and Software

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

- A server built on a Sun Server X2-4 platform.
- Four 1GigE ports for a combination of SMC UUI connections and service connections.
- A service (ILOM) port.
- Four Quad-port 1GigE cards, which provide 16 Ethernet ports for data transfer.
- 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 200TB for a single JBOD VLE (assuming a 4 to 1 compression ratio when the data is migrated to the VLE).
- Two dual-port 10GigE Network Adapter (NIC) cards per server, which are required for the internal network connections for VLEs with 2 or more nodes (or, with the Oracle switch, for 3 or more nodes).
- A DVD drive.

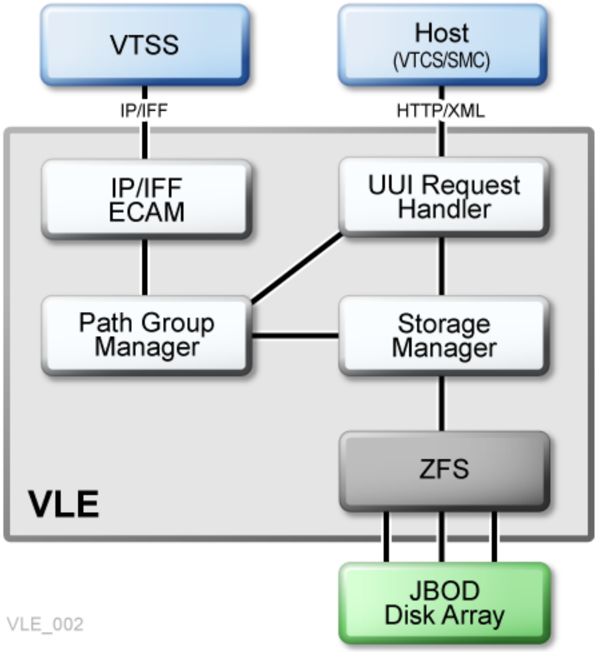
The VLE software consists of:

- 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.

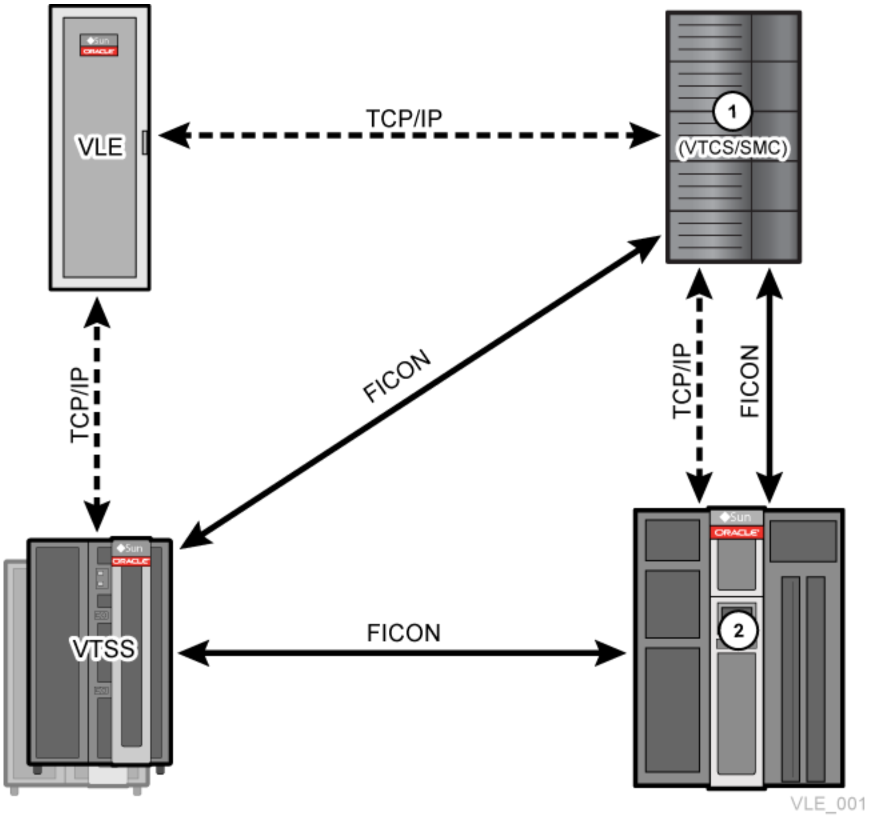
  UUI Request Handler calls:

  - 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 VTSS's IP ports and the VLE's 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 can 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. **For Version 1.4**, the VLE now ships with 4Tb JBODs. A single VLE, therefore**, 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. **Also note** that VLE is **architected** for up to 64 nodes, but has only been **validated** for up to 7 nodes.

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

1 - MVS Host

2 - Remote VLE

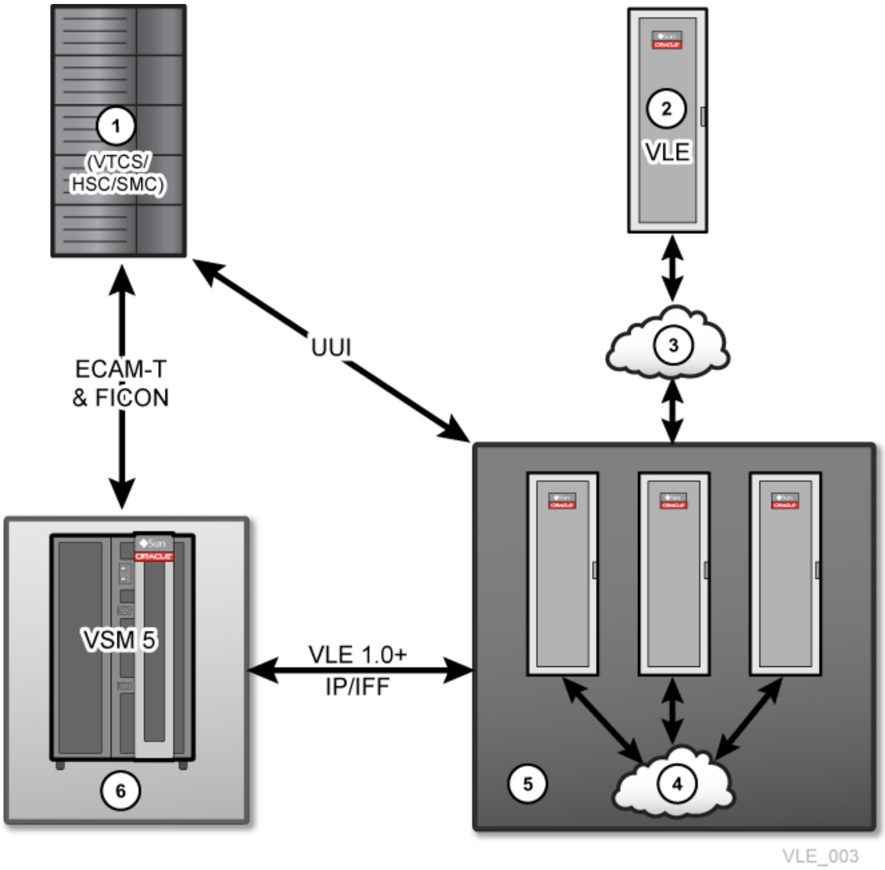
3 - Public Network

4 - Private Network

5 - VLE Multi-Node Grid

6 - Virtual Tape Storage System

Figure 1–3 VLE Multi-Node Complex



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 through-put. For 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 migrate to a VLE will cause data to be transferred from the VTSS and all subsequent VLE migrates 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 above, and
  - VTCS 7.1 (with the supporting PTFs) or VTCS 7.2

  Then 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 the VTV copies to VLE are reduced even further 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.

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 deencrypts VTVs that are recalled to the VTSS.

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 4Mb, and writes the compressed data to a VTV. VLE subsequently deduplicates the VTV to 2Mb and writes it to a VMVC. Thus, the reduction ratio is 16Mb divided by 2Mb or 8.0:1.

Early Time To First Byte (ETTFB)

Early Time To First Byte (ETTFB), also known as the concurrent tape recall/mount feature, allows the VTSS to use a VTD to read data as it being recalled from VLE:

- ETTFB is set globally through `CONFIG GLOBAL FASTRECL`.
- If `CONFIG GLOBAL FASTRECL=YES`, you can disable ETTFB on per VTSS basis through `CONFIG VTSS NOERLYMNT`.

`CONFIG GLOBAL` **and** `CONFIG VTSS` apply to **both** ETTFB for RTDs and ETTFB for VLE.

Frame Size Control

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

- **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 box sets the MTU (Maximum Transmission Unit) value to 9000 for the port.

2

Physical Site Planning

This chapter provides information about activities designed to ensure 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 C, "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" on page 2-2
  - "Requirements for Transferring the VLE Point to Point" on page 2-4
- "Requirements for Installing the VLE" on page 2-4, which describes floor construction and loading requirements.
- Data center safety system design features and capabilities as described in "Data Center Safety" on page 2-6.
- Site power system(s) design and capacity as described in "Site Power Distribution Systems" on page 2-7
- Data center HVAC design features and capabilities as described in "HVAC Requirements" on page 2-10
- Environmental requirements as described in:
  - "Environmental Requirements and Hazards" on page 2-10
  - Appendix C, "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

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 X2-4, with two 900GB Internal SAS drives, four quad port Gigabit Ethernet NICs, two dual port 10Gb Ethernet cards, one Erie dual port SAS HBA, 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 does not require access through the top except for power cables.

- Front - 36
- 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	1100
HVAC (BTU/Hr)	2590	3753

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 TB	3206	7186
600 TB	2609	8902
800 TB	3112	10619
1 PB	3615	12335

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

JBOD Size	Watts	BTU/Hr
1.2 PB	4118	14051
1.4 PB	4621	15768
1.6 PB	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, or 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)" on page 2-3 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)" on page 2-3 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" on page 2-5 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

WARNING: Exceeding recommended raised-floor loads can cause a floor collapse, which could result in severe injury or death, equipment damage, and 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/m2 (100 lbs./ft2) 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

Table 2–3 VLE Floor Loading Specifications

Basic Floor Load*	Maximum Superimposed Floor Load #
695 kg/m^2 (142 lbs./ft^2)	462 kg/m^2 (94lbs./ft^2))

Note:

* Load over footprint surface area (7093.7 cm2/1099.5 in^2) 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 Table 2–4 on page 2-6.

Table 2–4 Raised Flooring Horizontal Force Chart

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	40.4 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 of590 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 (5000 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, and 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, and 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 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 on page 2-8, 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, and with overcurrent protection and suitable grounding. A three-phase, five-wire distribution system provides the greatest configuration flexibility, since it allows power to be provided to both three-phase and single-phase equipment.

In Figure 2–1:

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

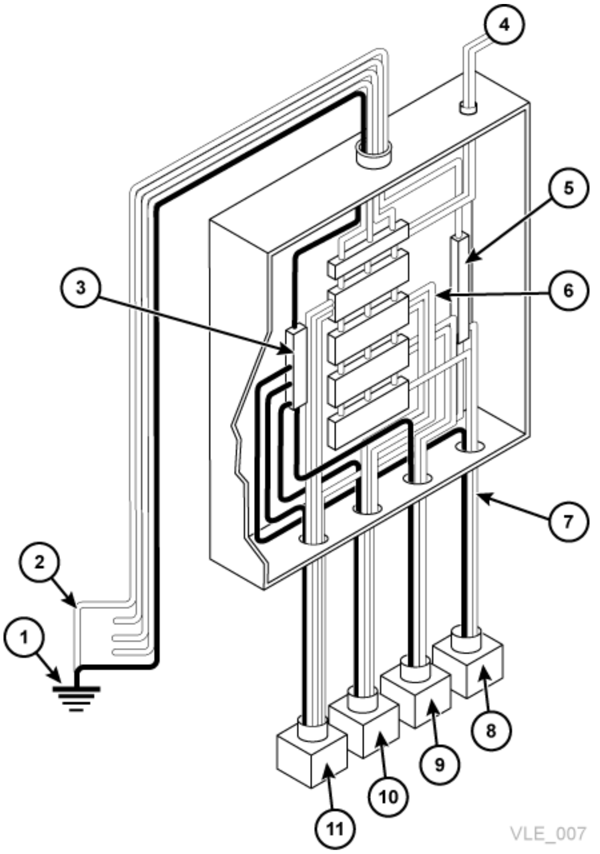
8 - 120V Single Phase

9 - 208/240V Single Phase

10 - 208/240V 3-Phase (4 wire)

11 - 208/240V 3-Phase (5 wire)

Figure 2–1 Site Electrical Power Distribution System



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

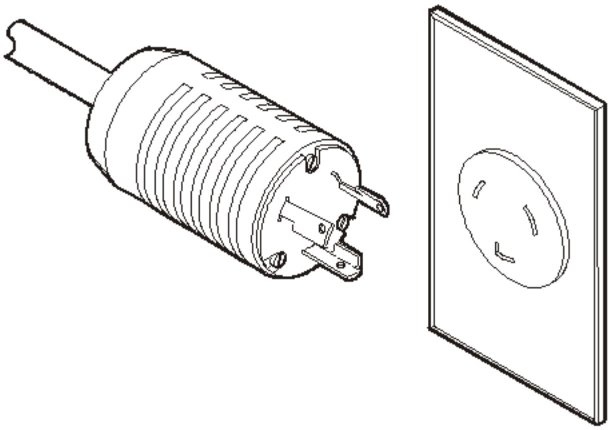
Voltage and frequency ranges at the AC source power receptacle(s) that will supply power to VLE system equipment must be measured and verified to meet the specifications shown in Table 2–5.

Table 2–5 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 the North and South America, Japan and Taiwan, ensure that the designated power sources are NEMA L6-30R receptacles, and ensure 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 the North and South America, Japan and Taiwan, ensure that 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 where:

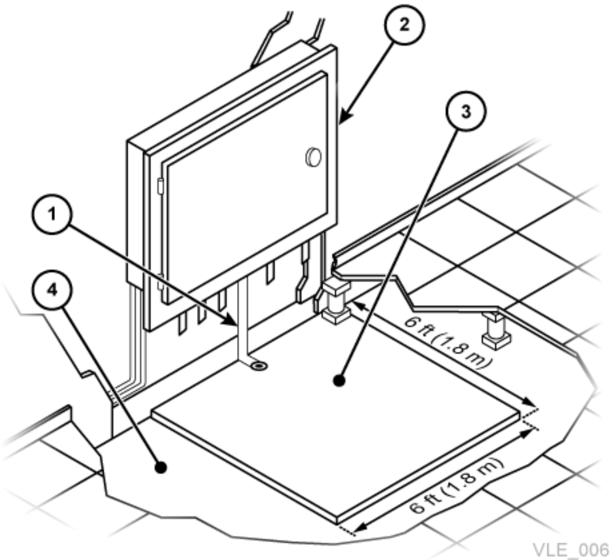
1 - Flat Braided/Strained Wire

2 - Power Panel

3 - Plate

4 - Concrete Floor

Figure 2–2 Transient Electrical Grounding Plate



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, or stored, or 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 topics.

Satisfying Mainframe Host Software Requirements

For ELS 7.2, support for VLE 1.4 is included in the base level. For ELS 7.0 and 7.1, get the latest SMP/E receive HOLDDATA and PTFs described in Table 3–1 and SMP/E APPLY with GROUPEXTEND.

Table 3–1 ELS Supporting PTFs for VLE

ELS 7.0	ELS 7.1
L1H16C1	L1H16J6
L1H1672	L1H1674

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:

- Gigabit Ethernet protocol is required on all network switches and routers that are directly attached to VSM5 IFF cards. The IFF card will only do speed negotiation to the 1 Gb speed.
- 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.

> **Note:** 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.

- Check that you are using the proper (customer-supplied) 1GigE 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.

- StorageTek 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 whole configuration.
- Only one TCP/IP connection is required between a VTSS and a VLE. However, for redundancy, StorageTek strongly recommends that you have a total of four 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 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. Because each VTSS connection represents four drives total, then 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 that 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

The Oracle switch is required for three node or greater VLEs, and can be used for two-node VLEs.

Note: Your VLE is shipped with the following components:

- The dual-port 10GigE NIC cards shown in Figure 3–4. These cards have installed the pluggable fiber transceivers.
- VLEs are shipped with a 1M fiber optic cable connecting ixgb0 to ixgb2. For single node systems, leave the cable connected. VLEs are also shipped with two 25M fiber optic cables that are connected to ixgbe1 and ixgbe3 (the free ends are affixed to the rack). For single-node systems, leave the free ends of the 25M fiber optic cables affixed to the rack. If you are going to use ixgbe1 and ixgbe3 for VLE-to-VLE connections, remove the 25M cables from ixgbe1 and ixgbe3 to make these ports available. If you are making multi-node connections, remove the 1M cable from ixgb0 to ixgb2 and the 25M cables from ixgbe1 and ixgbe3 to make these ports available. You can then use the 25M cables for node-to-node connections.

Order the switch, part X2074A-R to install the switch in a Sun Rack II cabinet.

For each of the first four VLE Nodes that connect through the switch, order two each of the following:

- SFP #X2129A-N
- The appropriate length of LC/LC optic fibre cable, which must be OM3, 850nm, multi-mode, maximum length, including patch panels, of 35M. Two cables per VLE are required to connect to the switch.

For VLE nodes 5 through 7 in the network, **in addition** to the above, order two total (**not** two per node) of the following:

- X2124A-N QSFP parallel fiber optics short wave transceivers.
- X2127A-10M QSFP optical cable splitters. These cable splitters are a single 10M long cable which splits after 9M into four cables for the final one meter in length. Each of these four cable lengths has an LC connector on the end and for the fifth VLE node, you will be able to plug one of the cable ends directly into the VLE node. The overall length of the cable is 10M so that VLE will need to be closer to the switch than VLEs connected by a 35M (or shorter) cable.

For **each** of 6-7 (or if you need more cable for node 5), ensure that you have two of the following:

- LC/LC couplers 10800160-N Spare: LC DUPLEX COUPLING RECEPTACLES.
- LC/LC fibre optic cables no more than 25 meters in length, OM3, 850nm, multimode. The limit is 25 meters because the cables must connect to the QSFP cable, which is 10M, using the couplers.

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 email 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 email communication with Oracle Support. To support VLE outgoing ASR notifications, the customer will need to supply the information in Table 3–2 to the installing Oracle Field Engineer.

Table 3–2 CAM 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

Table 3–2 (Cont.) CAM Configuration Information

Configuration Value	Example
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 3–2, 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 email ID and password, then the customer can enter it directly during the install process. ASR registration takes place during the CAM configuration portion of the VLE install. 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 into 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 email notification of event and log information, the customer must also supply the information in Table 3–3. If the email server does not require a user name and password, these fields can remain blank.

Table 3–3 Notification Setup - Email Configuration Options / ConfCollectStatus

Configuration Value	Example
Email Configuration - SMTP Server Name	SMTP.company.com
Email Configuration - SMTP Server User Name	
Email Configuration - SMTP Server User Password	
Email 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 email containing event and log information directly to a designated customer internal email address. A recipient of this email can then initiate a service request directly with Oracle and forward any emails received from the VLE to Oracle

Support. In this case, the customer must supply the email address where VLE emails are sent, where this email address can accept emails of up to 5M.

ASR Configuration

By default the VLE will send ASRs through the igb0 port. The site's mail server will be used to send the ASR alerts and the VLE support file bundles. When configuring CAM to send ASRs, it is necessary to input the customer SunSolve email ID and password. When configuring CAM, the customer provides the Oracle CSI email address and password or inputs this information directly into the CAM GUI at the time the CAM Configuration Procedure is performed.

Determining VLE Configuration Values

The following sections tell 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 `IP_and VMVC_Configuration.xls` 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

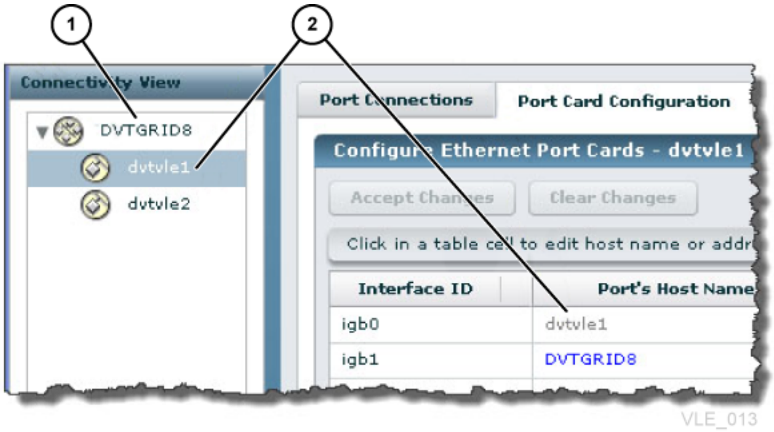
To configure the network for VLE, you run the `configure_vle` script on each node in a multi-node system (or the only node in a single-node system).

In Figure 3–1:

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

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



Click in a table cell to edit host name or addr

Interface ID	Port's Host Name
igb0	dvtvle1
igb1	DVTGRID8

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 in the following:

- 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 above).
- 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 igb0 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 alpha-numeric (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 and CAM limitations 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" on page 3-6
- VLE static IP address for port igb0
- 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" on page 3-5.
- 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 tell how to determine port card configuration values.

In Figure 3–2:

1 - Selected interface.

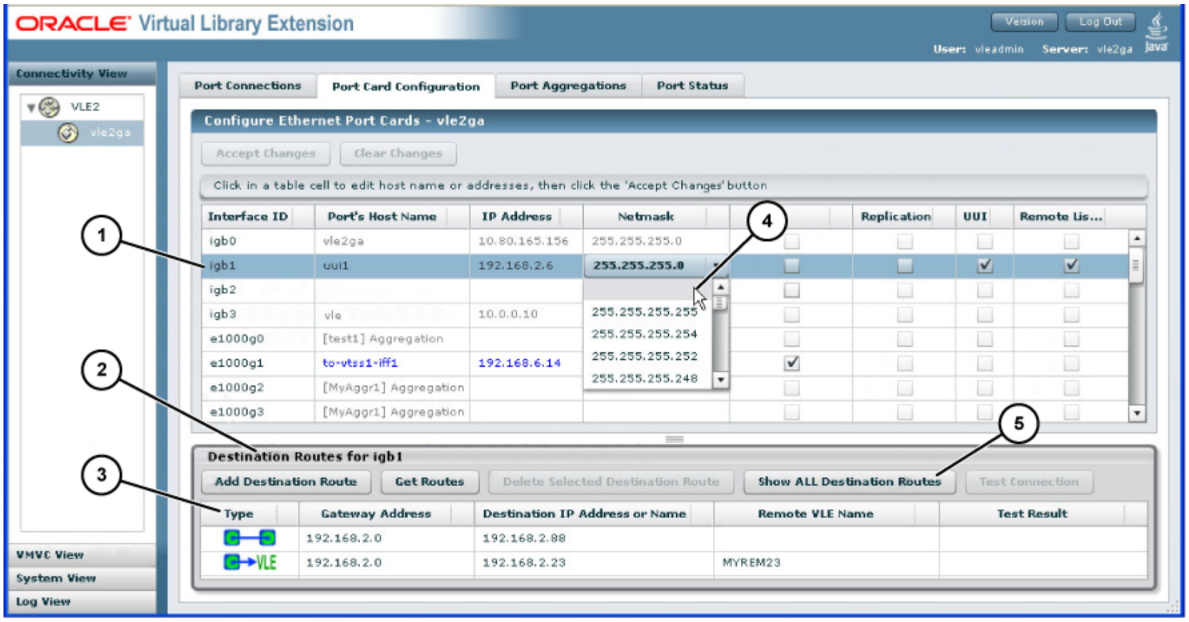
2 - Destination Routes panel to define remote VLE connections and static routes.

3 - Type of route shown by icons.

4 - Clear Netmask field by selecting blank item at top of drop down list.

5 - Content of bottom pane is filtered by interface selected in top pane. Click this button to show all routes for node.

Figure 3–2 VLE GUI Port Card Configuration Tab



Configure Ethernet Port Cards - vle2ga

Click in a table cell to edit host name or addresses, then click the 'Accept Changes' button

Interface ID	Port's Host Name	IP Address	Netmask		Replication	UUI	Remote Lis...
igb0	vle2ga	10.80.165.156	255.255.255.0	□	□	□	□
igb1	uui1	192.168.2.6	255.255.255.0	□	□	☑	☑
igb2				□	□	□	□
igb3	vle	10.0.0.10		□	□	□	□
e1000g0	[test1] Aggregation			□	□	□	□
e1000g1	to-vtss1-iff1	192.168.6.14		☑	□	□	□
e1000g2	[MyAggr1] Aggregation			□	□	□	□
e1000g3	[MyAggr1] Aggregation			□	□	□	□

Destination Routes for igb1

Type	Gateway Address	Destination IP Address or Name	Remote VLE Name	Test Result
●—●	192.168.2.0	192.168.2.88		
●→VLE	192.168.2.0	192.168.2.23	MYREM23	

Interface IDs

The Interface IDs identify the port. You can correlate this ID to ports using the Solaris command `status_vle_ips`. These identifiers are established before the VLE hardware is delivered, and cannot be modified.

Figure 3–3 shows the 1GigE Ethernet ports (igb4 to igb19) on the rear of the server.

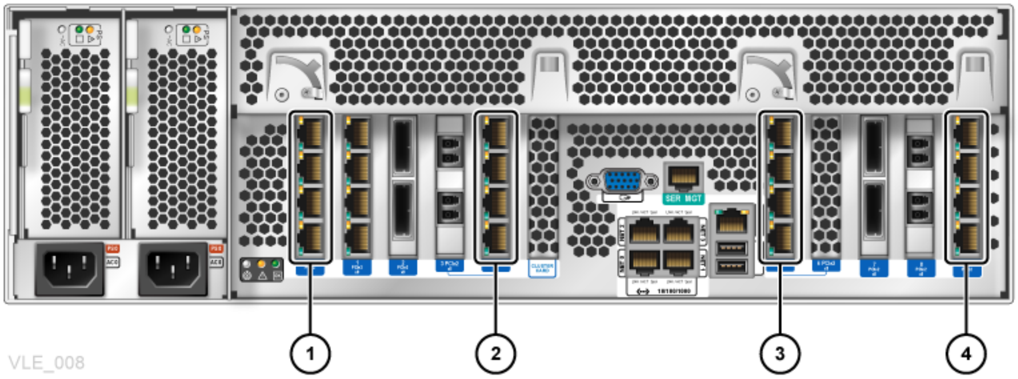
1 - igb4, igb5, igb6, igb7 (from top to bottom)

2 - igb8, igb9, igb10, igb11 (from top to bottom)

3 - igb16, igb17, igb18, igb19 (from top to bottom)

4 - igb12, igb13, igb14, igb15 (from top to bottom)

Figure 3–3 VLE 1GigE Ethernet Data Ports



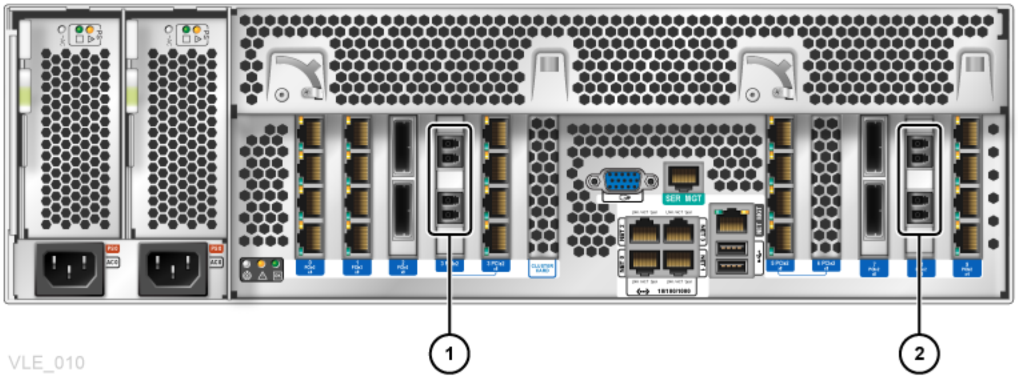
The 1GigE Ethernet ports are general purpose ports that can be used for UUI connection, Replication (VLE to VTSS data exchange), Remote Listener (VLE to VLE data exchange) or any combination of all three types.

VLE servers include two dual-port 10GigE NIC cards per server as shown in Figure 3–4.

1 - ixebe0, ixebe1 (from top to bottom)

2 - ixebe2, ixebe3 (from top to bottom)

Figure 3–4 VLE Dual-port 10GigE NIC cards



As Figure 3–4 shows, the 10GigE ports (in the red boxes) have interface IDs of `ixgbe0-ixgbe3`.

Note: VLEs are shipped with a 1M fiber optic cable connecting `ixgb0` to `ixgb2`. For single node systems, leave the cable connected. VLEs are also shipped with two 25M fiber optic cables, which you can use to connect multi-node system.

Ports ixgbe0 and ixgbe2 are **reserved** for:

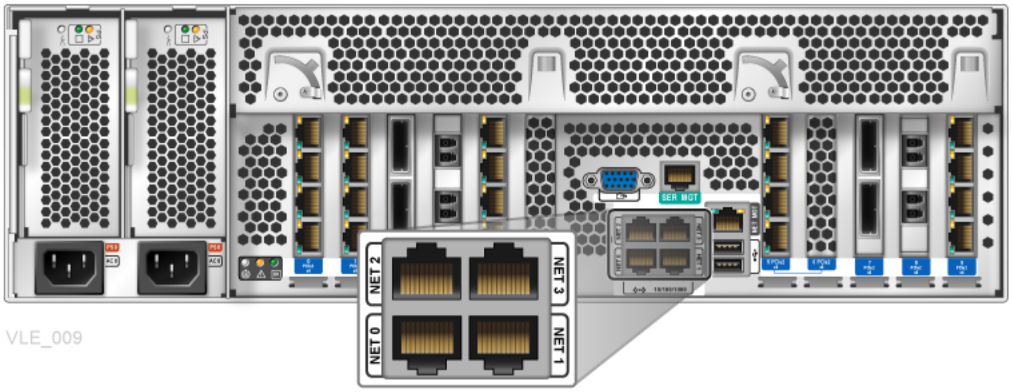
- Connections to the Oracle switch for three-node or greater configurations.
- Direct connections to another node in two-node configurations. To connect two nodes, you can do one of the following:
  - Directly connect `ixgbe0` on one node to `ixgbe0` on the second node, and `ixgbe2` on one node to `ixgbe2` on the second node.
  - Connect the nodes through the Oracle switch.

Ports `ixgbe1` and `ixgbe3` are general purpose ports that can be used for UUI connection, Replication (VLE to VTSS data exchange), Remote Listener (VLE to VLE data exchange) or any combination of all three types.

VLE Ethernet Management Ports

The management ports are marked on the back of the case `NET0-NET3` as shown in Figure 3–5.

Figure 3–5 VLE Ethernet Management Ports



As shown in Figure 3–5:

- The management ports (igb0 through igb3) can be on a network segment that is private or public and are typically used as follows:
  - `igb0` (`NET0`) - **Reserved** for connection to the network for ASR traffic and managing the VLE software.
  - `igb1` (`NET1`) - General purpose port, typically used for connection to the network for UUI (control path) traffic.
  - `igb2` (`NET2`) - General purpose port, typically used for redundant UUI connection, or if you want separate ports for separate network segments for the host network and for the sending of ASR alerts.
  - `igb3` (`NET3`) - **Reserved** as dedicated port for service. **Note that** this port can use a single cable and function as **both** the service port and the ILOM port. Do not connect this port to the network. `igb3` must remain free and open as an Ethernet port with known access configuration so that it will always be available for service. The preconfigured default IP address for igb3 are:
    - 10.0.0.10 for use as a service port. You use `igb3` as a service port to access the VLE CLI.
    - 10.0.0.1 for use as an ILOM port.

Port’s 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 alpha-numeric (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 and CAM limitations require that the host portion (not including the domain component) be limited to a maximum 24 characters. **Note that** the Port’s Host Name for igb0 and igb3 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, which 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, the two unused 10GigE connections (`ixgbe1` and `ixgbe3`) or any unused 1GigE connection can be used from any node in a VLE. If each VLE has two or more nodes, StorageTek 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 VLE's node but you should **never** run multiple connections from a VLE node to a single port on the other VLE. If both VLE's have more than one node, StorageTek recommends spreading the VLE to VLE connections across all nodes in each VLE.

For 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.

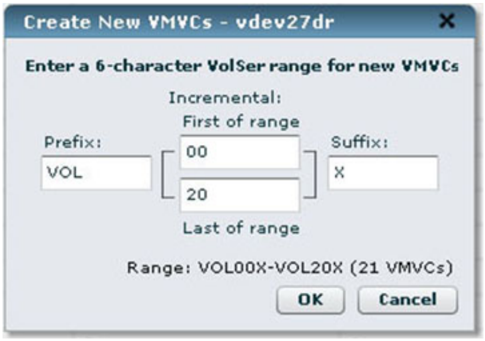
For VLE to VLE data transfers, each VLE requires a UUI connection and an VTSS connection. This will ensure VTCS can migrate and recall VTVs from either VLE.

Determining VMVC Range Configuration Values

Ensure that you assign VMVC names and ranges to fit within the site's 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 3–6, you use theVLE 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 3–6 VLE GUI Create New VMVC dialog box



Create New VMVCs - vdev27dr

Enter a 6-character VolSer range for new VMVCs

Incremental:

Prefix: VOL

First of range: 00

Last of range: 20

Suffix: X

Range: VOL00X-VOL20X (21 VMVCs)

You determine values for each of the fields in Figure 3–6 as follows:

- Each of the fields allows 0-6 alpha-numeric characters, with the "assembly" limitations below.
- 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.

  For example, you could 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. For 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 you attempt 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 1TB (assuming 4:1 compression). Table 3–4 shows the maximum VMVCs you can define for each VLE node capacity.

Table 3–4 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 you specify in the VLE GUI must match the volser ranges defined to VTCS!

Planning for Encryption

VLE 1.1 and above 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:

- 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.

Note that encryption is enabled, disabled, and managed at the VLE GUI by a StorageTek 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 de encrypts 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 node's USB port, and must be writeable and 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 4K 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; that is, there is no retroactive deduplication.

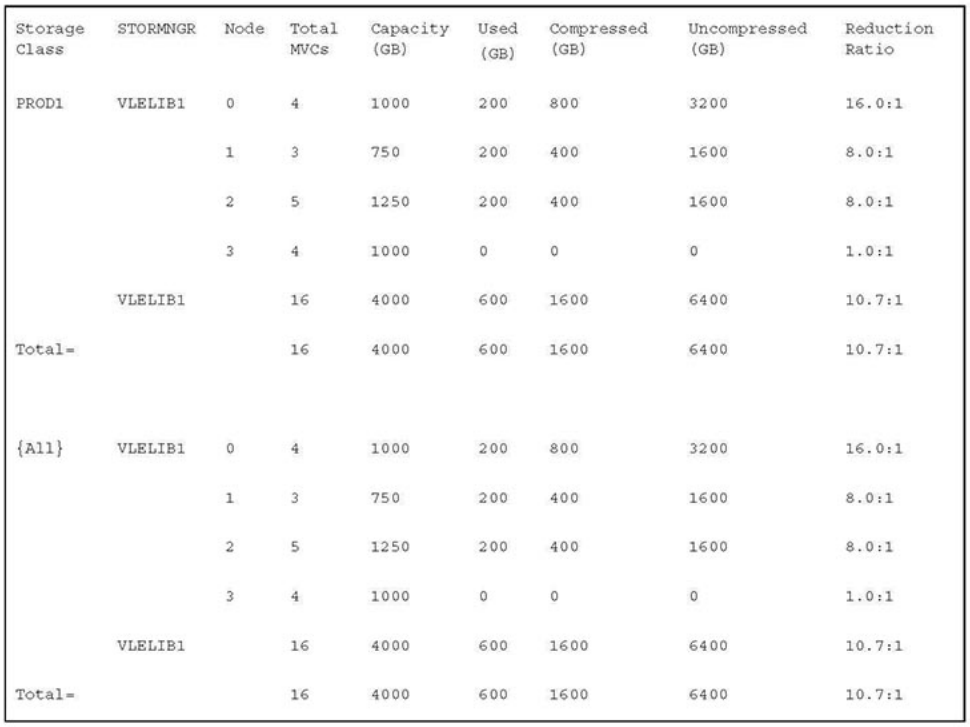
Deduplication Guidelines

That's a quick "how to" for deduplication, now what are the guidelines for what data should and should not be deduplicated? 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

After deduplication is enabled, how do you know how well it is working? You can monitor the results with the SCRPT report, as shown in the example in Figure 3–7

Figure 3–7 SCRPT Report



```
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


{All}     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 Figure 3–7, the approximate reduction ratio for the 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 4Mb, and writes the compressed data to a VTV. VLE subsequently deduplicates the VTV to 2Mb and writes it to a VMVC. Thus, the reduction ratio is 16Mb divided by 2Mb or 8.0:1.

Because the calculation is done using Mb, it is possible to see 0Gb 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 above 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 on page 3-13, 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 time out is specified.

Reduced Replication

VLE 1.3 and above 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 on page 3-13.

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 for VLE 1.4. 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 3–8 shows the **Connectivity View, Port Aggregations** tab, which you use view the pre-defined "internal" aggregation port (such as `AggrNode1`) and its associated interfaces. You can also define and modify new custom aggregations using this tab.

In Figure 3–8:

1 - Currently selected aggregation.

2 - Drag up or down to resize panes.

3 - Drop down selection list of options.

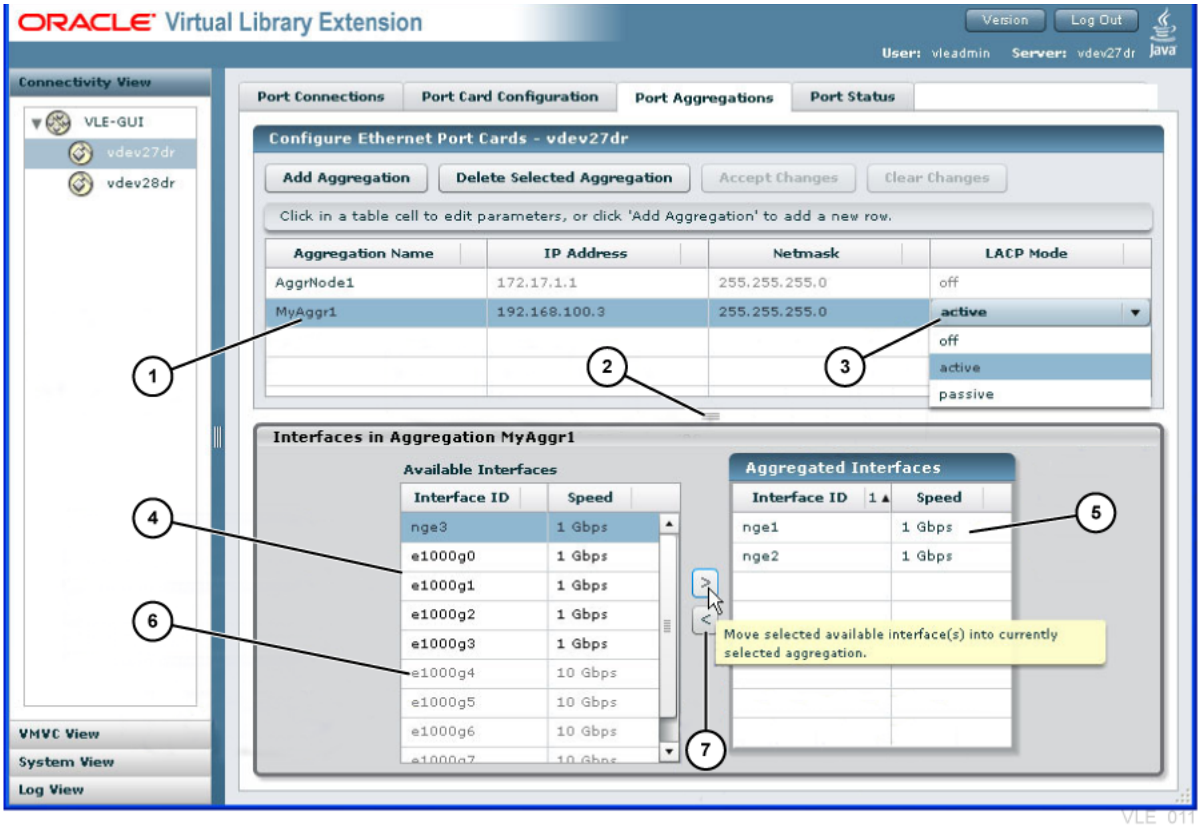
4 - Pool of port interfaces available for aggregations

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.

Figure 3–8 VLE GUI Connectivity View, Port Aggregations Tab



Click in a table cell to edit parameters, or click 'Add Aggregation' to add a new row.

Aggregation Name	IP Address	Netmask	LACP Mode
AggrNode1	172.17.1.1	255.255.255.0	off
MyAggr1	192.168.100.3	255.255.255.0	active

Available Interfaces

Interface ID	Speed
nge3	1 Gbps
e1000g0	1 Gbps
e1000g1	1 Gbps
e1000g2	1 Gbps
e1000g3	1 Gbps
e1000g4	10 Gbps
e1000g5	10 Gbps
e1000g6	10 Gbps
e1000g7	10 Gbps

Aggregated Interfaces

Interface ID	Speed
nge1	1 Gbps
nge2	1 Gbps

Move selected available interface(s) into currently selected aggregation.

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.

For examples of link aggregation, see Appendix B, "VLE Link Aggregation Examples".

Link Aggregation Requirements

- All links in an aggregation must be the same speed. That is, you cannot configure a 1GigE and a 10GigE 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

Note that 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 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 IP's 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 part of the aggregation **do not** connect ports to a channel group that are not 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 and 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.

10GigE Port Aggregations

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

Monitoring Aggregations

Ensure that you 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.

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

```
Sep 4 08:30:16 dvtvle3 mac: [ID 486395 kern.info] NOTICE: igb12 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" on page 3-19
- "VLE to VLE Aggregations" on page 3-19
- "VLE UUI Aggregations" on page 3-19.

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 VTSSs 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 (igb4, igb8, igb12, igb16) to prevent an outage to a aggregation if a network adapter fails.

For examples of VLE to VTSS link aggregation, see Appendix B, "VLE Link Aggregation Examples".

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" on page 3-19. 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, you use ports `igb1` and `igb2` to make UUI connections. In this configuration, aggregate `igb1` and `igb2` to create a *fault-tolerant configuration*: if one of the links fails, the remaining link still provides the UUI connection. For additional redundancy on multi-node VLEs, aggregate two UUI connections on a second node.

A

VLE Configuration Examples

This appendix contains the following configuration examples (all examples are direct connect, no switch):

- "Example 1: One VTSS Connected to One VLE" on page A-3
- "Example 2: Four VTSSs Connected to One VLE" on page A-5
- "Example 3: VLE to VLE Copy" on page A-7
- "Example 4: One VTSS Connected to a 3-Node VLE" on page A-9

"VLE Configuration Examples" on page A-1 shows the VLE GUI screens used for these examples.

VLE GUI Configuration Screens

The following sections describe the VLE GUI configuration screens used to configure the examples in this appendix. For more information on the VLE GUI, see *VLE Installation, Configuration, and Service Guide*.

Port Card Configuration Tab

Figure A–1 shows the **Port Card Configuration** tab, which is used in all examples. Assume the default **Netmask** value and use whatever value you want for the **Port's Host Name** field. The table for each example provides the **IP Address** and **Check Box** (Replication, UUI, Remote) values that correspond to the **Interface ID** field value.

In Figure A–1:

1 - Currently selected aggregation.

2 - Drag up or down to resize panes.

3 - Drop down selection list of options.

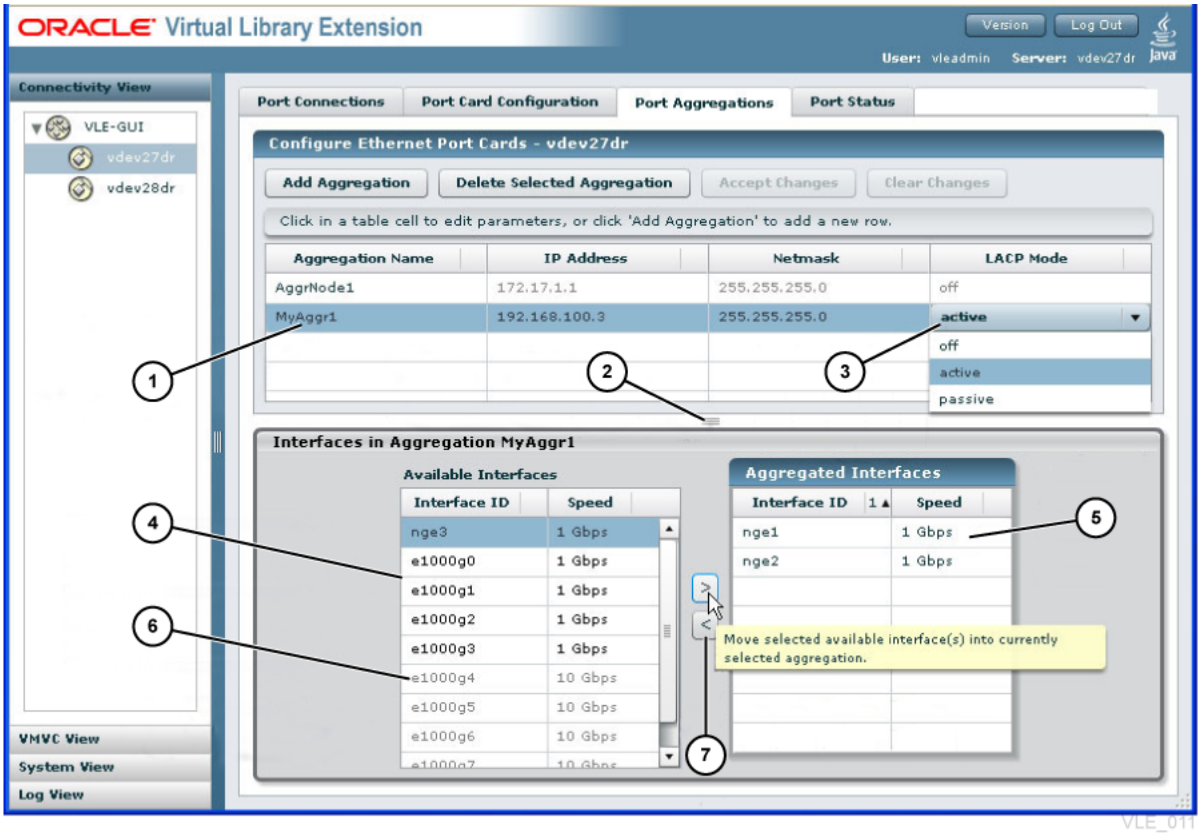
4 - Pool of port interfaces available for aggregations

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.

Figure A–1 Port Card Configuration Tab



Configure Ethernet Port Cards - vdev27dr

Click in a table cell to edit parameters, or click 'Add Aggregation' to add a new row.

Aggregation Name	IP Address	Netmask	LACP Mode
AggrNode1	172.17.1.1	255.255.255.0	off
MyAggr1	192.168.100.3	255.255.255.0	active

LACP Mode options: off, active, passive

Interfaces in Aggregation MyAggr1

Available Interfaces

Interface ID	Speed
nge3	1 Gbps
e1000g0	1 Gbps
e1000g1	1 Gbps
e1000g2	1 Gbps
e1000g3	1 Gbps
e1000g4	10 Gbps
e1000g5	10 Gbps
e1000g6	10 Gbps
e1000g7	10 Gbps

Aggregated Interfaces

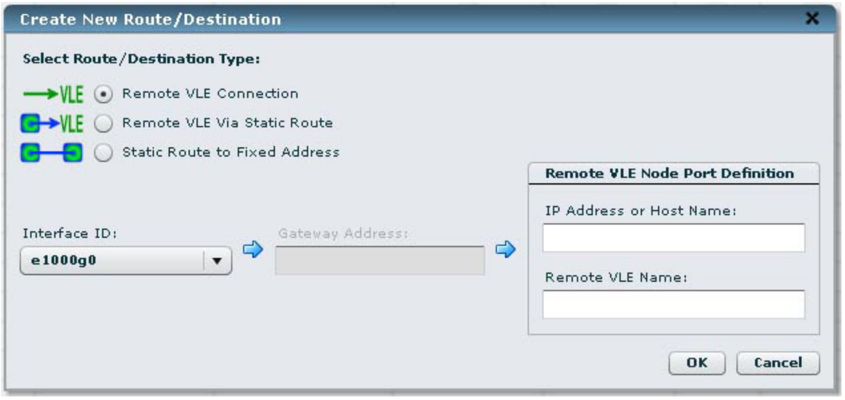
Interface ID	Speed
nge1	1 Gbps
nge2	1 Gbps

Move selected available interface(s) into currently selected aggregation.

Create New Route/Destination dialog boxes

Figure A–2 and Figure A–3. You use one of these dialog boxes in "Example 3: VLE to VLE Copy" on page A-7.

Figure A–2 Create New Route/Destination dialog box - Remote VLE



Create New Route/Destination

Select Route/Destination Type:

● Remote VLE Connection
○ Remote VLE Via Static Route
○ Static Route to Fixed Address

Interface ID: e1000g0

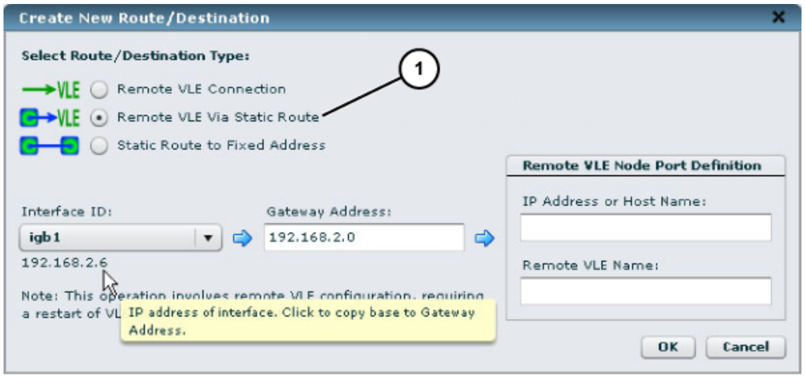
Gateway Address:

Remote VLE Node Port Definition

IP Address or Host Name:

Remote VLE Name:

Figure A–3 Create New Route/Destination dialog box - Remote VLE, Static Route



Create New Route/Destination ✕

Select Route/Destination Type:

○ Remote VLE Connection
● Remote VLE Via Static Route
○ Static Route to Fixed Address

Interface ID: igb1 ▼ ⇨

192.168.2.6

Gateway Address: 192.168.2.0 ⇨

Remote VLE Node Port Definition

IP Address or Host Name:

Remote VLE Name:

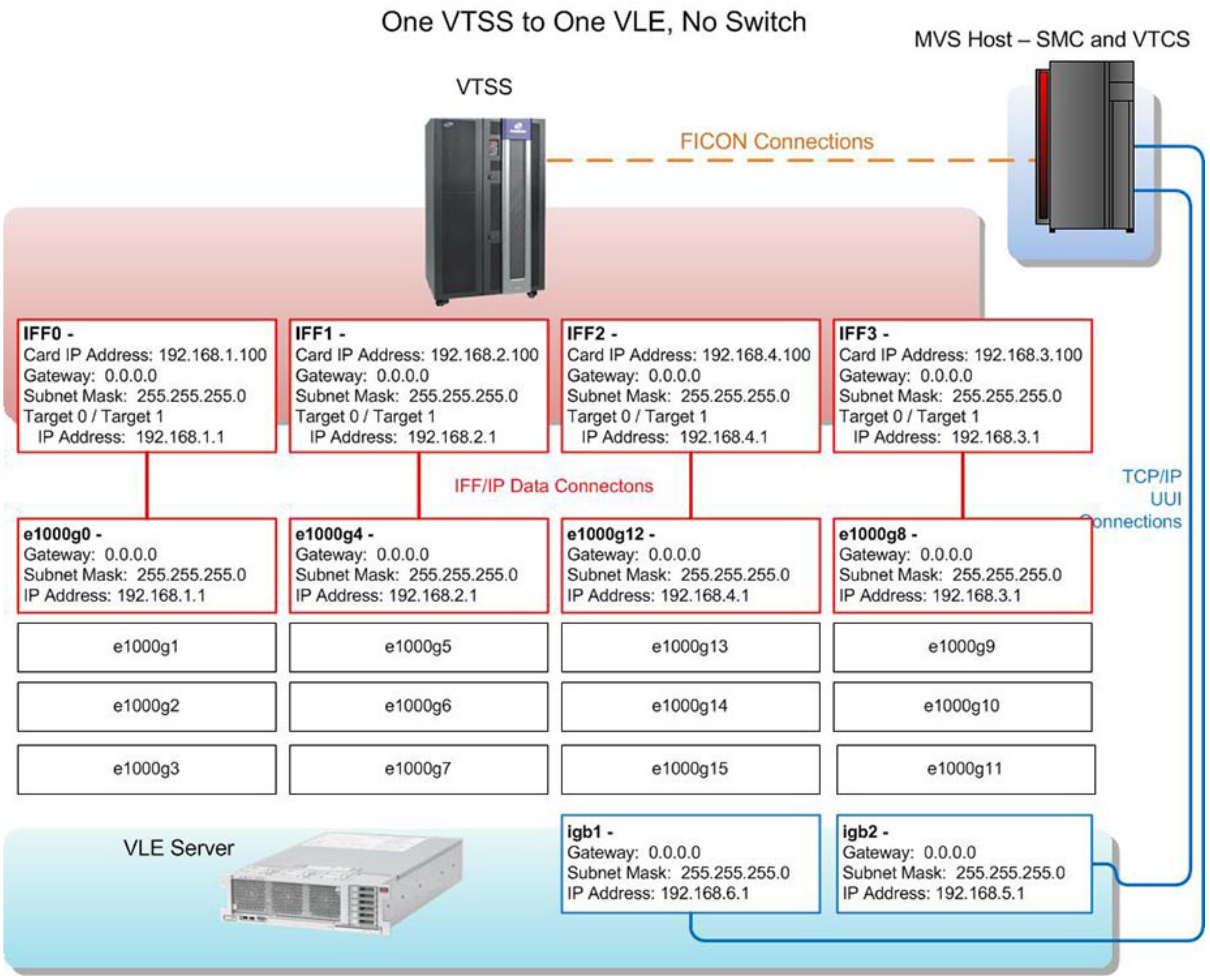
Note: This operation involves remote VLE configuration, requiring a restart of VL

IP address of interface. Click to copy base to Gateway Address.

1 - Selection modifies available entry fields

Example 1: One VTSS Connected to One VLE

Figure A–4 Example 1: One VTSS Connected to One VLE



IFF0 -
Card IP Address: 192.168.1.100
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
Target 0 / Target 1
IP Address: 192.168.1.1

IFF1 -
Card IP Address: 192.168.2.100
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
Target 0 / Target 1
IP Address: 192.168.2.1

IFF2 -
Card IP Address: 192.168.4.100
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
Target 0 / Target 1
IP Address: 192.168.4.1

IFF3 -
Card IP Address: 192.168.3.100
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
Target 0 / Target 1
IP Address: 192.168.3.1

e1000g0 -
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
IP Address: 192.168.1.1

e1000g4 -
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
IP Address: 192.168.2.1

e1000g12 -
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
IP Address: 192.168.4.1

e1000g8 -
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
IP Address: 192.168.3.1

igb1 -
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
IP Address: 192.168.6.1

igb2 -
Gateway: 0.0.0.0
Subnet Mask: 255.255.255.0
IP Address: 192.168.5.1

As Figure A–4 on page A-3 and Table A–1 show, in this one VTSS to one VLE example, two targets on each IFF card connect to a single port on the VLE, where the IP addresses must match. Note that the third octet of the IP addresses is unique to each IFF card to VLE port connection, so these connections share a unique subnet.

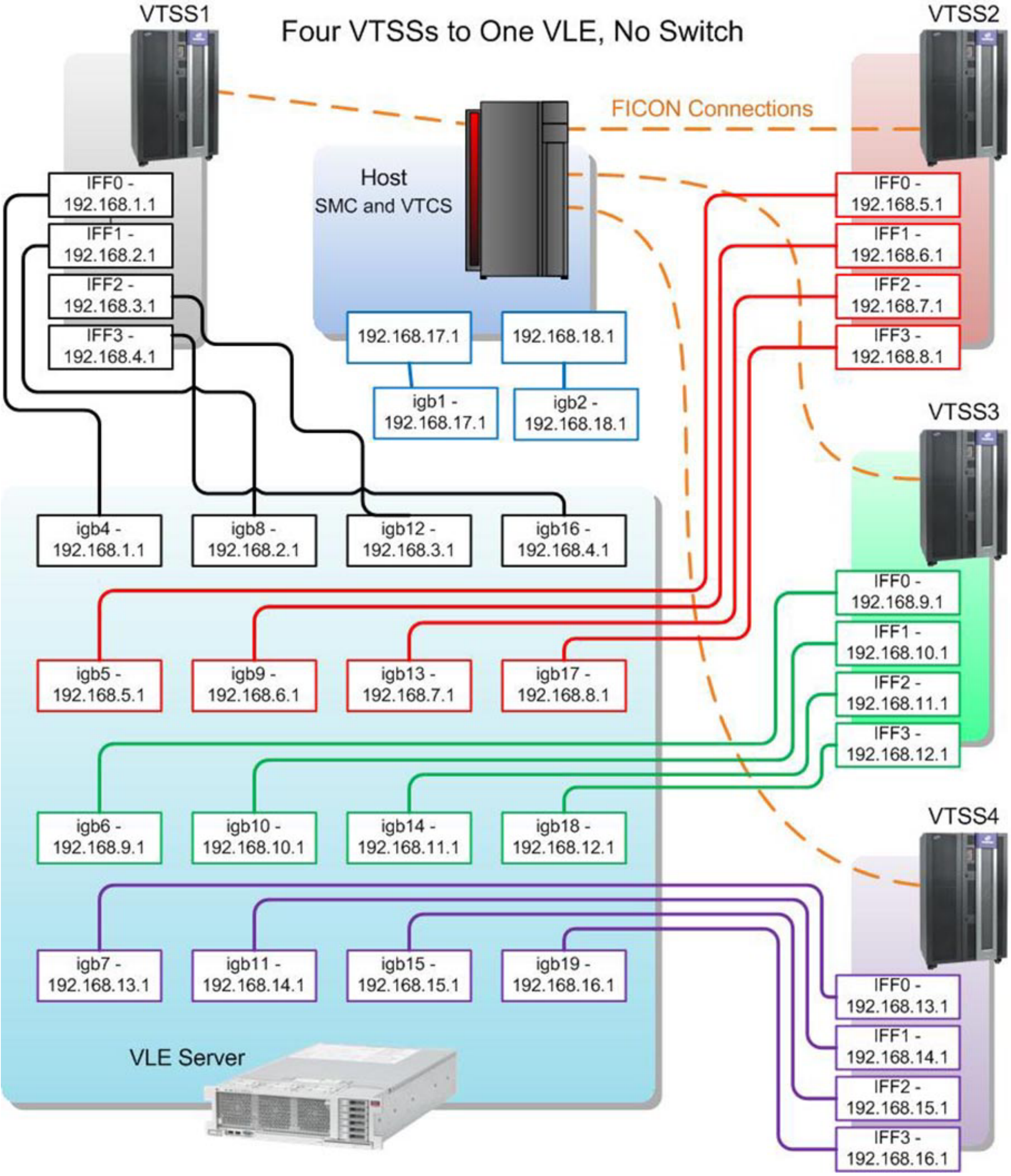
Using two targets on each IFF card optimizes performance, because each target represents a socket, which enables a migrate and a recall to occur simultaneously on the same IFF card. Two targets optimizes performance, there is no performance benefit to assigning more than two targets per IFF card to the same VLE port.

Table A–1 Example 1 Configuration Values

IFF Card and Target	IPIF Value	Interface ID	IP Address	Check Box
Data Connections				
IFF0 Target 0	0A:0	igb4	192.168.1.1	Replication
IFF0 Target 1	0A:1			
IFF1 Target 0	0I:0	igb8	192.168.2.1	
IFF1 Target 1	0I:1			
IFF2 Target 0	1A:0	igb16	192.168.4.1	
IFF2 Target 1	1A:1			
IFF3 Target 0	1I:0	igb12	192.168.3.1	
IFF3 Target 1	1I:1			
UUI Connections				
		igb1	192.168.6.1	UUI
		igb2	192.168.5.1	

Example 2: Four VTSSs Connected to One VLE

Figure A–5 Example 2: Four VTSSs Connected to One VLE



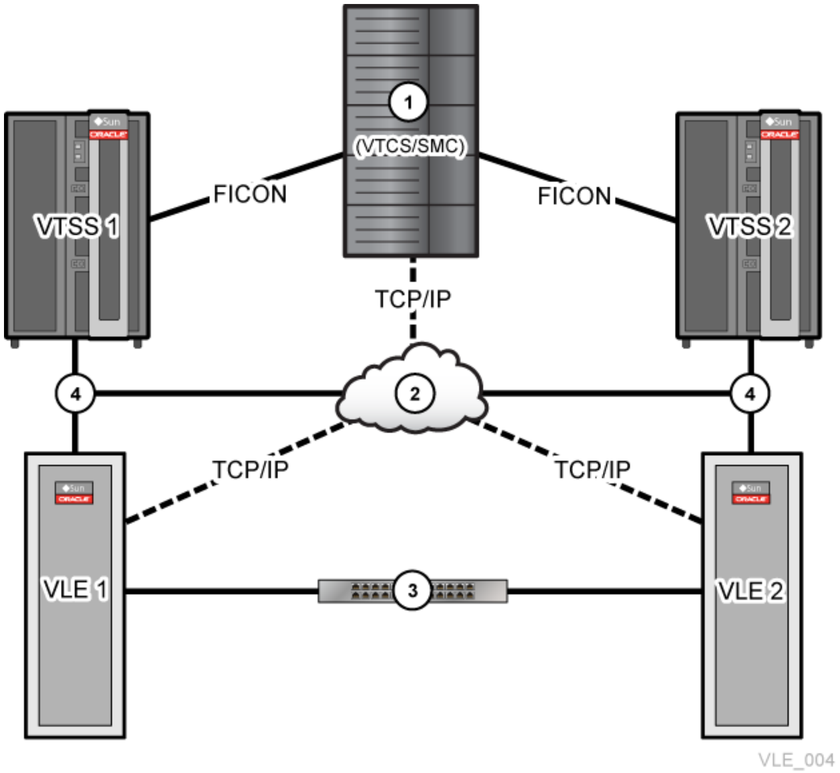
As Figure A–5 and Table A–2 show, in this four VTSS to one VLE example, each IFF target to VLE port connection (where the IP addresses must match) is on its own unique subnet, as shown by the different colors for each subnet (UUI connections are shown in blue).

Table A–2 Example 2 Configuration Values

VSM5	IFF Card and Target	IPIF Value	Interface ID	IP Address	Check Box
Data Connections					
VTSS1	IFF0 Target 0	0A:0	igb4	192.168.1.1	Replication
	IFF1 Target 0	0I:0	igb8	192.168.2.1	
	IFF2 Target 0	1A:0	igb12	192.168.3.1	
	IFF3 Target 0	1I:0	igb16	192.168.4.1	
VTSS2	IFF0 Target 0	0A:0	igb5	192.168.5.1	
	IFF1 Target 0	0I:0	igb9	192.168.6.1	
	IFF2 Target 0	1A:0	igb13	192.168.7.1	
	IFF3 Target 0	1I:0	igb17	192.168.8.1	
VTSS3	IFF0 Target 0	0A:0	igb6	192.168.9.1	
	IFF1 Target 0	0I:0	igb10	192.168.10.1	
	IFF2 Target 0	1A:0	igb14	192.168.11.1	
	IFF3 Target 0	1I:0	igb18	192.168.12.1	
VTSS4	IFF0 Target 0	0A:0	igb7	192.168.13.1	
	IFF1 Target 0	0I:0	igb11	192.168.14.1	
	IFF2 Target 0	1A:0	igb15	192.168.15.1	
	IFF3 Target 0	1I:0	igb19	192.168.16.1	
UUI Connections					
			igb1	192.168.17.1	UUI
			igb2	192.168.18.1	

Example 3: VLE to VLE Copy

Figure A–6 Example 3: VLE to VLE Copy



As Figure A–6 and the example values in Table A–3 show, in this two VTSSs to two VLEs, VLE to VLE copy example:

- Each VTSS is connected to the MVS Host (1) and is cross-connected to each VLE for VTSS to VLE copy (4 are the VTSS to VLE TCP/IP connections and 2 is the 1GigE TCP/IP network).
- The VLEs are connected to each other through a network that includes the 10 GigE switch (3).

Each VTSS, therefore, can migrate a separate VTV copy to each VLE, which provides a redundancy/high availability solution similar to that provided by Clustered VTSS. The default behavior can be that the second copy is made through VLE to VLE connections. To enforce VTSS to VLE migration for the second copy, use the STORCLAS FROMLST parameter. For more information, see *Configuring the Host Software for VLE*.

Table A–3 Example 3 Configuration Values

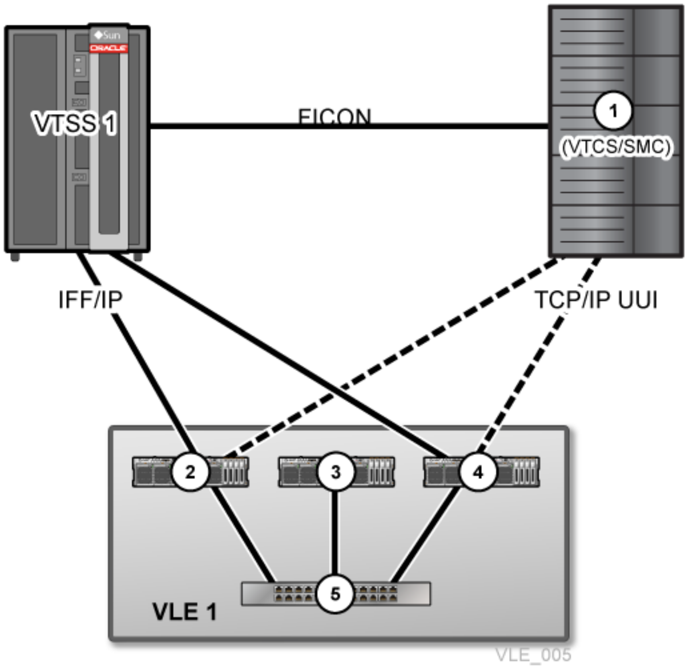
VSM5	IFF Card and Target	IPIF Value	VLE, Interface ID	IP Address	Check Box

Table A–3 (Cont.) Example 3 Configuration Values

VLE to VTSS Data Connections					Replication
VTSS1	IFF0 Target 0	0A:0	VLE1, igb4	192.168.1.1	
	IFF1 Target 0	0I:0	VLE1, igb8	192.168.2.1	
	IFF2 Target 0	1A:0	VLE1, igb12	192.168.3.1	
	IFF3 Target 0	1I:0	VLE1, igb16	192.168.4.1	
	IFF0 Target 1	0A:1	VLE2, igb4	192.168.5.1	
	IFF1 Target 1	0I:1	VLE2, igb8	192.168.6.1	
	IFF2 Target 1	1A:1	VLE2, igb12	192.168.7.1	
	IFF3 Target 1	1I:1	VLE2, igb16	192.168.8.1	
VSM5	IFF Card and Target	IPIF Value	VLE, Interface ID	IP Address	Check Box
VLE to VTSS Data Connections					
VTSS2	IFF0 Target 0	0A:0	VLE1, igb5	192.168.9.1	Replication
	IFF1 Target 0	0I:0	VLE1, igb9	192.168.10.1	
	IFF2 Target 0	1A:0	VLE1, igb13	192.168.11.1	
	IFF3 Target 0	1I:0	VLE1, igb17	192.168.12.1	
	IFF0 Target 1	0A:1	VLE2, igb5	192.168.13.1	
	IFF1 Target 1	0I:1	VLE2, igb9	192.168.14.1	
	IFF2 Target 1	1A:1	VLE2, igb13	192.168.15.1	
	IFF3 Target 1	1I:1	VLE2, igb17	192.168.16.1	
VLE to VLE Data Connections					
			VLE1, ixgbe1	192.168.17.1	Remote
			VLE1, ixgbe3	192.168.18.1	
			VLE2, ixgbe1	192.168.17.2	
			VLE2, ixgbe3	192.168.18.2	
UUI Connections					
			VLE1, igb1	192.168.19.1	UUI
			VLE1, igb2	192.168.20.1	
			VLE2, igb1	192.168.21.1	
			VLE2, igb2	192.168.22.1	

Example 4: One VTSS Connected to a 3-Node VLE

Figure A–7 Example 4: One VTSS Connected to a Three-Node VLE



As the example values in Table A–4 show, in this one VTSS to a 3-Node VLE example:

- The 10 GigE switch (5) provides an internal network for data exchange between the nodes that make up `VLE1` where 2 - Node 1, 3 - Node 2, and 4 - Node 3.
- To provide redundancy, nodes `1` and `3` both have IFF/IP connections for data exchange with the VTSS and TCP/IP UUI connections to the Mainframe host.
- Node 3 is a data repository and has no Mainframe host (1) or VTSS connections.

Table A–4 Example 4 Configuration Values

IFF Card and Target	IPIF Value	VLE Node, Interface ID	IP Address	Check Box

Table A–4 (Cont.) Example 4 Configuration Values

Data Connections				Replication
IFF0 Target 0	0A:0	Node 1, igb4	192.168.1.1	
IFF0 Target 1	0A:1			
IFF1 Target 0	0I:0	Node 1, igb8	192.168.2.1	
IFF1 Target 1	0I:1			
IFF2 Target 0	1A:0	Node 3, igb4	192.168.3.1	
IFF2 Target 1	1A:1			
IFF3 Target 0	1I:0	Node 3, igb8	192.168.4.1	
IFF3 Target 1	1I:1			
UUI Connections				
		Node 1, igb1	192.168.5.1	UUI
		Node 3, igb2	192.168.6.1	

B

VLE Link Aggregation Examples

This appendix contains the following link aggregation examples:

- "Example 1: Single-Node VLE Connected to Two VSM5s" on page B-3
- "Example 2: Two-Node VLE Connected to Two VTSSs" on page B-4

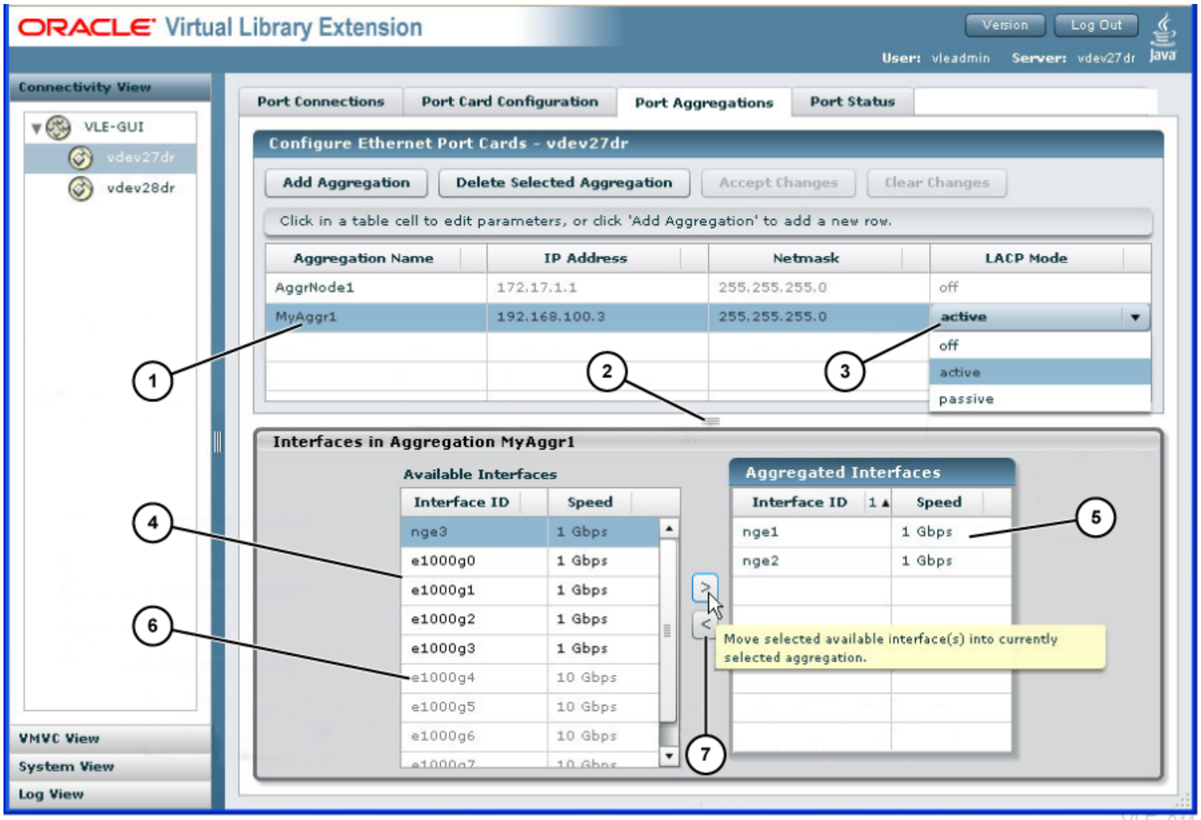
"VLE GUI Configuration Screens" on page B-1 shows the VLE GUI screens used for these examples.

VLE GUI Configuration Screens

The following section shows the VLE GUI Configuration Screen used to configure the examples in this appendix. For more information on the VLE GUI, see *VLE Installation, Configuration, and Service Guide*.

Port Aggregations tab

Figure B–1 Port Aggregations tab



Configure Ethernet Port Cards - vdev27dr

Click in a table cell to edit parameters, or click 'Add Aggregation' to add a new row.

Aggregation Name	IP Address	Netmask	LACP Mode
AggrNode1	172.17.1.1	255.255.255.0	off
MyAggr1	192.168.100.3	255.255.255.0	active

off
active
passive

Interfaces in Aggregation MyAggr1

Available Interfaces

Interface ID	Speed
nge3	1 Gbps
e1000g0	1 Gbps
e1000g1	1 Gbps
e1000g2	1 Gbps
e1000g3	1 Gbps
e1000g4	10 Gbps
e1000g5	10 Gbps
e1000g6	10 Gbps
e1000g7	10 Gbps

Aggregated Interfaces

Interface ID 1 ▲	Speed
nge1	1 Gbps
nge2	1 Gbps

Move selected available interface(s) into currently selected aggregation.

Figure B–1 shows the **Port Aggregations** tab, which is used in all examples.

1 - Currently selected aggregation.

2 - Drag up or down to resize panes.

3 - Drop down selection list 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.

Example 1: Single-Node VLE Connected to Two VSM5s

Figure B–2 Example 1: Single-Node VLE Connected to Two VTSSs

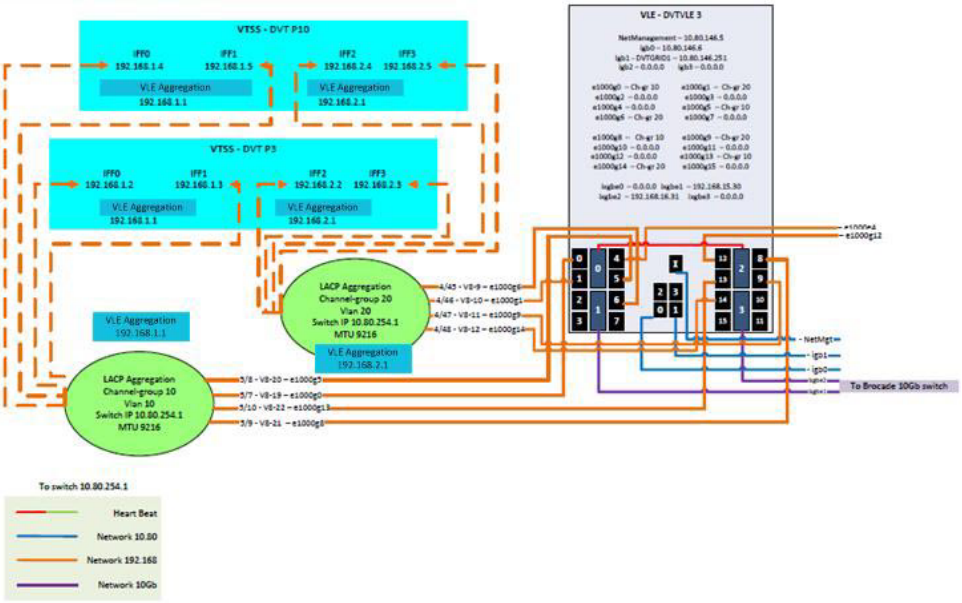


Figure B–2 shows a single-node VLE connected to two VSM5s as follows:

- Ports igb4, igb9, igb12, and g1000g13 are aggregated to the switch's Channel group 10 with an IP address of 192.168.1.1 and the aggregation is connected each VSM5's IFF0 and IFF1 cards.
- Ports igb4, igb8, igb13, and igb18 are aggregated to the switch's Channel group 20 with an IP address of 192.168.2.1 and the aggregation is connected each VSM5's IFF2 and IFF3 cards.

Note the following benefits versus a non-aggregated configuration:

- **Simplify the configuration**: Just two IP addresses were required at the VLE (192.168.1.1 and 192.168.2.1).
- **Provide fault tolerance**: The links to each aggregation are configured evenly and horizontally across the VLE to prevent an outage to a aggregation if a network adapter fails. Additionally, both aggregations serve each VSM5, so if an aggregation fails, the other aggregation can continue the connection to the VSM5.
- **Load balancing and bandwidth optimization**: Each aggregation consists of four separate links to distribute the traffic load and optimize bandwidth.

Example 2: Two-Node VLE Connected to Two VTSSs

Figure B–3 Two-Node VLE Connected to Two VTSSs

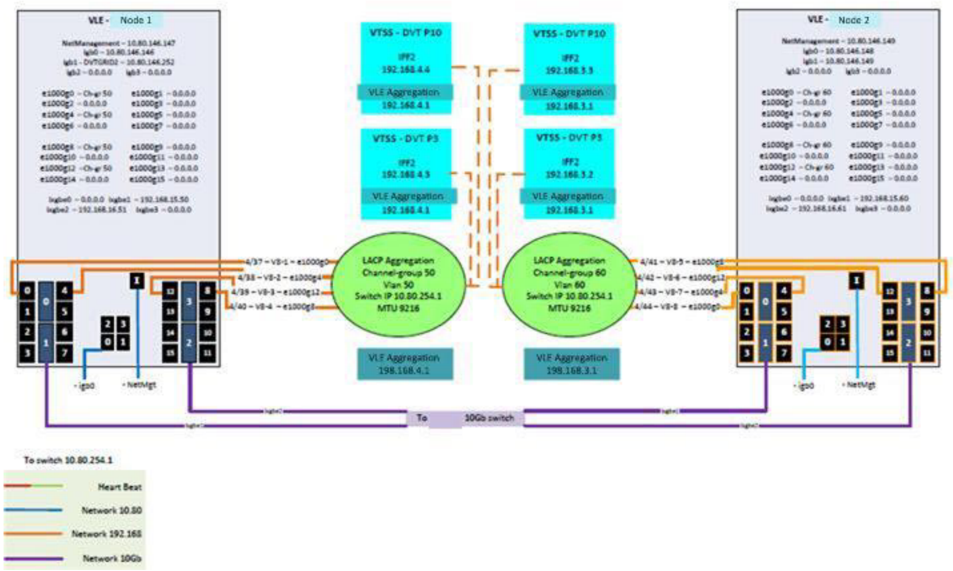

VLE - Node 1
NetManagement - 10.80.146.147
igb0 - 10.80.146.146
igb1 - DVTGRID2 - 10.80.146.252
igb2 - 0.0.0.0 igb3 - 0.0.0.0
e1000g0 - Ch-gr 50 e1000g1 - 0.0.0.0
e1000g2 - 0.0.0.0 e1000g3 - 0.0.0.0
e1000g4 - Ch-gr 50 e1000g5 - 0.0.0.0
e1000g6 - 0.0.0.0 e1000g7 - 0.0.0.0
e1000g8 - Ch-gr 50 e1000g9 - 0.0.0.0
e1000g10 - 0.0.0.0 e1000g11 - 0.0.0.0
e1000g12 - Ch-gr 50 e1000g13 - 0.0.0.0
e1000g14 - 0.0.0.0 e1000g15 - 0.0.0.0
ixgbe0 - 0.0.0.0 ixgbe1 - 192.168.15.50
ixgbe2 - 192.168.16.51 ixgbe3 - 0.0.0.0
VTSS - DVT P10
IFF2
192.168.4.4
VLE Aggregation
192.168.4.1
VTSS - DVT P3
IFF2
192.168.4.5
VLE Aggregation
192.168.4.1
VTSS - DVT P10
IFF2
192.168.3.3
VLE Aggregation
192.168.3.1
VTSS - DVT P3
IFF2
192.168.3.2
VLE Aggregation
192.168.3.1
4/37 - V8-1 - e1000g0
4/38 - V8-2 - e1000g4
4/39 - V8-3 - e1000g12
4/40 - V8-4 - e1000g8
LACP Aggregation
Channel-group 50
Vlan 50
Switch IP 10.80.254.1
MTU 9216
LACP Aggregation
Channel-group 60
Vlan 60
Switch IP 10.80.254.1
MTU 9216
4/41 - V8-5 - e1000g8
4/42 - V8-6 - e1000g12
4/43 - V8-7 - e1000g4
4/44 - V8-8 - e1000g0
VLE Aggregation
198.168.4.1
VLE Aggregation
198.168.3.1
VLE - Node 2
NetManagement - 10.80.146.149
igb0 - 10.80.146.148
igb1 - 10.80.146.149
igb2 - 0.0.0.0 igb3 - 0.0.0.0
e1000g0 - Ch-gr 60 e1000g1 - 0.0.0.0
e1000g2 - 0.0.0.0 e1000g3 - 0.0.0.0
e1000g4 - Ch-gr 60 e1000g5 - 0.0.0.0
e1000g6 - 0.0.0.0 e1000g7 - 0.0.0.0
e1000g8 - Ch-gr 60 e1000g9 - 0.0.0.0
e1000g10 - 0.0.0.0 e1000g11 - 0.0.0.0
e1000g12 - Ch-gr 60 e1000g13 - 0.0.0.0
e1000g14 - 0.0.0.0 e1000g15 - 0.0.0.0
ixgbe0 - 0.0.0.0 ixgbe1 - 192.168.15.60
ixgbe2 - 192.168.16.61 ixgbe3 - 0.0.0.0
- igb0
- NetMgt
- igb0
- NetMgt
To 10Gb switch
To switch 10.80.254.1
Heart Beat
Network 10.80
Network 192.168
Network 10Gb

Figure B–3 shows a two-node VLE connected to two VSM5s as follows:

- Ports igb4, igb8, igb12, and g1000g12 of Node 1 are aggregated to the switch's Channel group 50 with an IP address of 192.168.4.1 and the aggregation is connected each VSM5.
- Ports igb4, igb8, igb12, and g1000g12 of Node 2 are aggregated to the switch's Channel 60 with an IP address of 192.168.3.1 and the aggregation is connected each VSM5.

Note the following benefits versus a non-aggregated configuration:

- **Simplify the configuration**: Just two IP addresses were required at the VLE (192.168.4.1 and 192.168.3.1).
- **Provide fault tolerance**: The links to each aggregation are configured evenly and horizontally across each node to prevent an outage to a aggregation if a network adapter fails. Additionally, both aggregations serve each VSM5, so if an aggregation fails, the other aggregation can continue the connection to the VSM5. Finally, each node services each VSM5, providing additional redundancy.

Load balancing and b**andwidth optimization**: Each aggregation consists of four separate links to distribute the traffic load and optimize bandwidth.

C

Controlling Contaminants

This appendix tells how to control 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 they 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 room's 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 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 room's 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 insulative 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 of the 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 totally 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.

- It 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 industry are highly ammoniated or contain other chemicals that can be harmful to hardware. It is very 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. Even before filtration, this is an unnecessary exposure that can adversely affect environmental conditions in the room. It is also 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 the environment is maintained correctly, the following should be considered:

- All doors should fit snugly in their frames.
- Use gaskets and sweeps o 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 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 much 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 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 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 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 room's 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 also 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’s air inlet and outlet grilles should be treated as well. Do not wipe the unit’s 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 and then 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 to 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