Virtual Library Extension

Planning Guide

Version 1.0

E23002-05

Revision 05

Submit comments about this document to STP_FEEDBACK_US@ORACLE.COM

Virtual Library Extension Planning Guide

Table of Contents

Preface

Audience

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

1

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), etc.
- Proximity of high-frequency electromagnetic radiation sources (e.g., 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 (e.g., industrial plants).

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
- Site power system(s) design and capacity
- VLE system equipment power system design and capacity
- Data center safety system design features and capabilities
- Data center environmental (HVAC) design features and capabilities
- Potential effects of corrosive materials, electrical interference, or excessive vibration from sources in close proximity to system equipment.

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.

Transferring Equipment 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 to be verified are described below.

Structural Dimensions and Obstructions

Dimensions of elevators, doors, hallways, etc. 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 "Appliance Overall Dimensions - SunRack II 1242 Cabinet (inches)" on page 18 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 (roughly 620 kg (1365 lbs.) with 192 array drives), a pallet jack (allow 100 kg/220 lbs.), and two persons (allow 200 kg/440 lbs.). See "Weight (Base pounds - 638, Max pounds - 1299)" on page 18 for additional cabinet-weight details.

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 (e.g., 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 16 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.

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.).

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 as to 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 1-1 on page 12, 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.

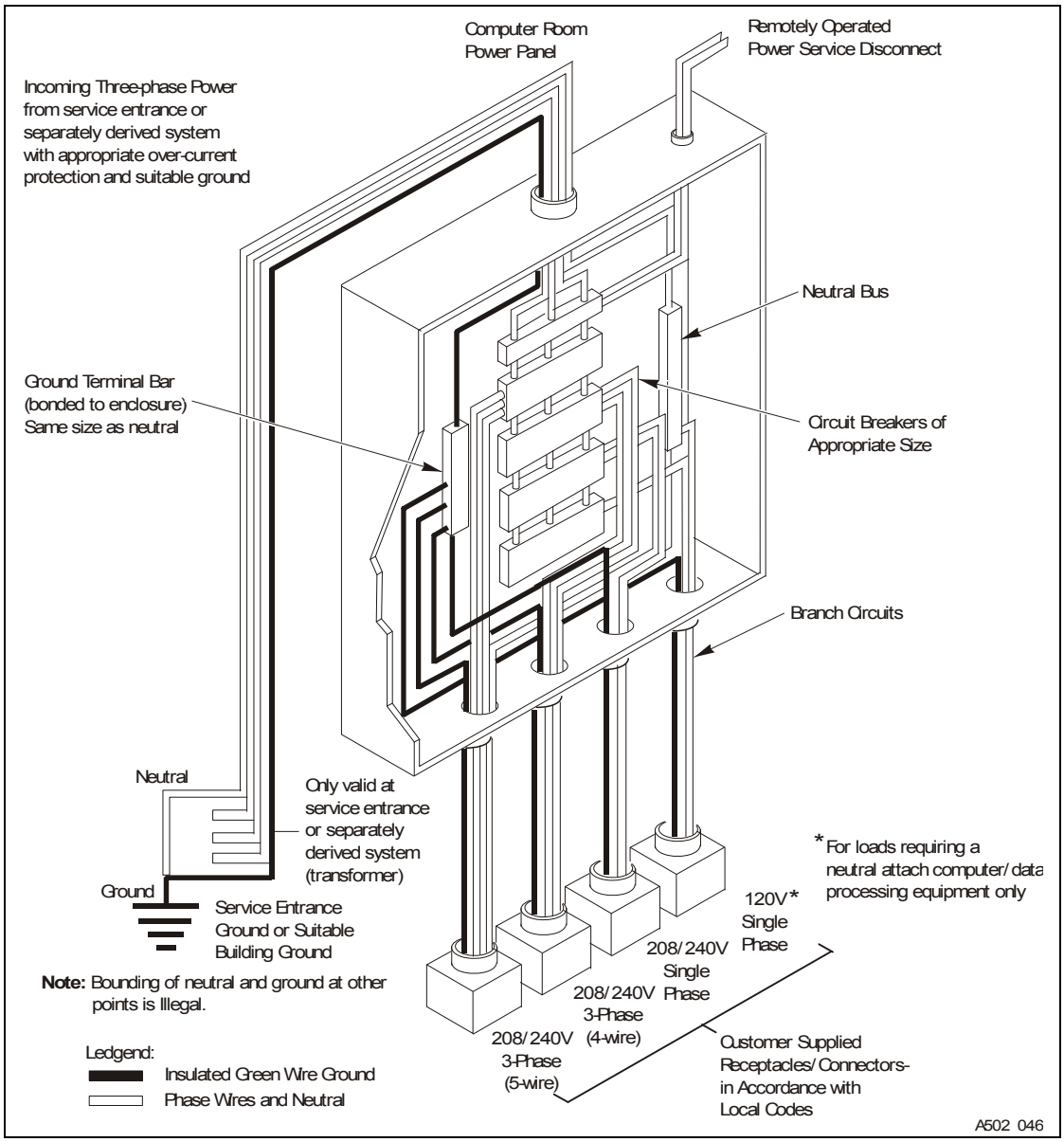


FIGURE 1-1 Site Electrical Power Distribution System

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

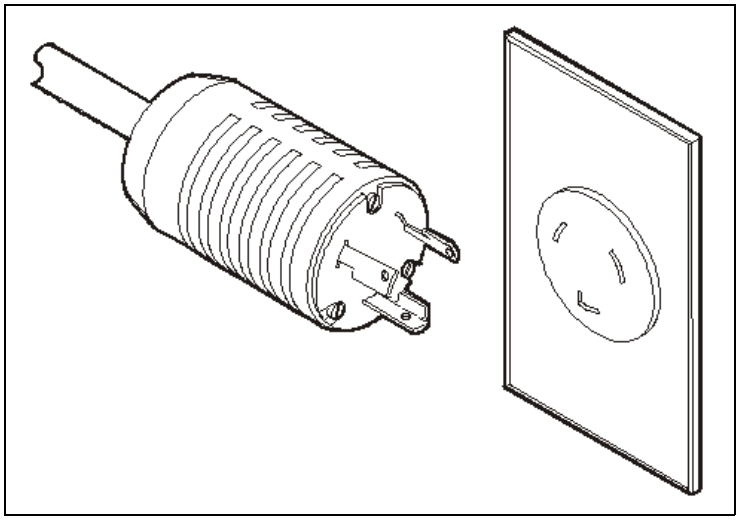
Voltage and frequency ranges at the AC source power receptacle(s) that will supply power to VLE system equipment must be measured and verified to meet the specifications shown in TABLE 1-1.

TABLE 1-1 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, make sure that the designated power sources are NEMA L6-30R receptacles, and make sure 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, make sure 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 (e.g., one to local utility power, the other 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 1-2.

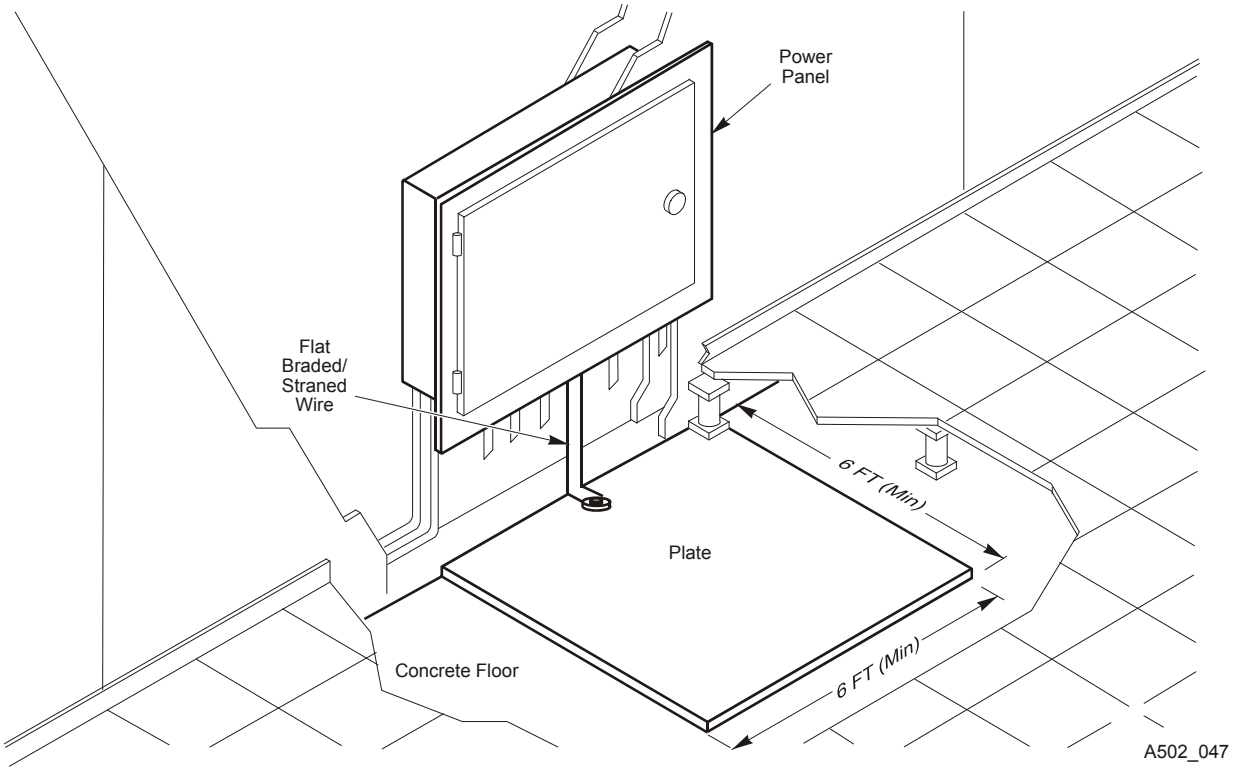


FIGURE 1-2 Transient Electrical Grounding Plate

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 (e.g., 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 prior to installation of the equipment.

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 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 (e.g., 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 1-2 VLE Floor Loading Specifications

Basic Floor Load*	Maximum Superimposed Floor Load #
730 kg/m2 (149 lbs./ft2)	485 kg/m2 (99 lbs./ft2)

Note –

- * Load over footprint surface area (7093.7 cm2/1099.5 in2) of an unpackaged VLE cabinet, with a maximum weight of 620 kg/1365 lbs., i.e., a VLE with 192 array disk drives.
- # Assumes minimum Z+Z axis dimension of 185.3 cm/73.0 in. (i.e., 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. (i.e., 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 1-3.

TABLE 1-3 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 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.). 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.

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 an x4470 Server, with two 500GB Internal SATA drives, four quad port Gigabit Ethernet NICs, two dual port 10Gb Ethernet cards, two Thebe dual port SAS HBAs; two J4410 JBODs, each populated with 24 2TB SAS HDD; and the SunRack II 1242 Cabinet with dual 10KVA PDUs. The only option is additional capacity, in increments of two JBODs, up to a maximum total of 8.

Capacity

- Base Capacity - Native 55 TB, Effective 220 TB
- Max Capacity - Native 220 TB, Effective 880 TB

Appliance Overall Dimensions - SunRack II 1242 Cabinet (inches)

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

Service Clearance (inches)

- Top - 36
- Front - 36
- Rear - 36

Weight (Base pounds - 638, Max pounds - 1299)

Breakdown:

- Server - 85
- Cabinet - 332
- Each JBOD - 110.25
- 8 JBODs - 882
- Total Weight - 1299
- Total Weight plus shipping material - 1570

Power ((Base Watts – 2232, Max Watts – 5436)

Breakdown:

- Server - 1164 (peak) 722 (Idle)
- Each JBOD- 534 (peak) 389 (Idle)
- 8 JBODs- 4272 (peak) 3112 (Idle)
- Total Power- 5436 (peak) 3834 (Idle)

HVAC ((Base BTU/HR – 7618, Max BTU/Hr – 18556)

Breakdown:

- Server - 3972 (peak) 2464 (Idle)
- Each JBOD - 1823 (peak) 1328 (Idle)
- 8 JBODs - 14584 (peak) 10624 (Idle)
- Maximum Heat - 18556 (peak) 13088 (Idle)

Remote Connections

Server Ethernet Ports:

- Sixteen Ethernet ports on four quad-port Gigabit Ethernet cards for data backup and recall.
- Four (two used) 10Gb Ethernet ports on two dual-port cards for VLE interconnectivity on private network
- Four on-board Gigabit Ethernet ports for software level interaction – At most two are used for remote connections and management. One is for service connections direct to the server node.
- Network Management Ethernet port for remote server management below OS level - ssh or GUI.

Other Ethernet ports: Two PDU management/monitoring ports for power.

2

VLE Planning

This chapter provides information about VLE planning topics.

Satisfying MVS Host Software Requirements

VTCS and SMC 6.2 and above supports VLE. See My Oracle Support for the VTCS and SMC PTFs that are additionally required for VLE support.

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.
- 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 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 4 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 2-node VLE, the VTSS connections should be two on node1 and the other two on node 2. On a 4-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 4-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 4-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 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 2-4 to the installing Oracle Field Engineer.

TABLE 2-4 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
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 2-4 on page 23, 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 2-5. If the email server does not require a user name and password, these fields can remain blank.

TABLE 2-5 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 (available through your StorageTek representative) to record these values so you can pass them on to the personnel who will configure the VLE and the host software.

Determining the Subsystem Name

You must specify the VLE subsystem name on the following:

- The `STORMNGR` parameter value on the VTCS `CONFIG TAPEPLEX` statement for the TapePlex that connects to the VLE.
- 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 SMC `SERVER` command for the VLE.

The default subsystem name as the VLE comes from Manufacturing is `VLETEST`. Typically, you reset this name with the `General Configuration` Tab of the `VLE` GUI.

If you reset the subsystem name, the value must be1 to 8 characters in length, alphanumeric, uppercase.

For example, `VLE1`

Determining the VLE Host Name

The default subsystem name as the comes from Manufacturing is v-*serial_number*, where *serial_numbe*r is the unique serial number of the VLE. You can reset the VLE Host Name when you run the `setup_network` script during VLE configuration. The VLE Host Name must be:

- All upper case with no spaces.
- The valid host name character set is A-Z, a-z, 0-9, . and a dash (-), where the dash cannot be at the end of the string.
- You must use two or more numbers or at least one letter for the field. A single digit is invalid.
- The host name can be up to 24 characters.

Best practices is to provide a meaningful Host Name. For example, `vle-dp-15` for `e1000g15`. For more information, see "4470 Server Ethernet Port Layout" on page 26.

Determining VLE Ethernet Port Card Configuration Values

4470 Server Ethernet Port Layout

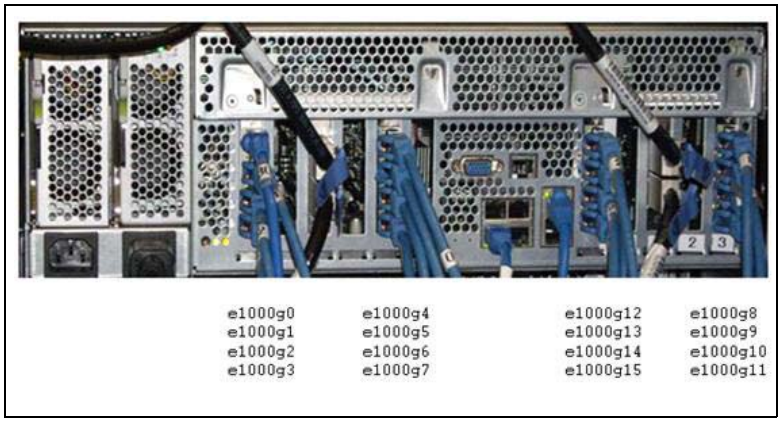


FIGURE 2-3 4470 Ethernet Ports

As shown in FIGURE 2-3:

- The figure shows the port number on the back of the server. See "VLE Preconfigured Default Values" on page 39 for the preconfigured default values for these ports.
- The management ports (igb0 through igb3), can be on a network segment that is private or public. igb0, igb1(optional: igb2) and igb3 are dedicated for use by the VLE and should **not** be used for to connecting to a VTSS for data transfer:
  - igb0 - This interface is bound to the VLE hostname and a dedicated static IP address. VLE hostname is the name of the VLE. It should be no longer than 24 characters and should not start with a number. The hostname should be registered with the customer's domain name server (DNS) prior to the installation and should have a valid static IP address.

    Note –

    - Once you set the hostname the first time fin the configuration script for igb0, **do not** change it using the VLE GUI. There is a special procedure for changing that hostname because many resources use that initial information. If you ever have to change that hostname, work with VLE Buckling Support – do not change it without their procedures. It will also involve significant downtime for the VLE; make sure the customer gets the name right the first time.
    - Whenever you have a dedicated VLE hostname igb0, you should be able to ping from a laptop or desktop across the network and get a response from it.

- For example, if the VLE hostname is tikka1, the domain is 'customer-net.com' and the customer has a proper DNS entry with the IP address of 25.80.146.30, you can verify that the setup is correct by opening a terminal window on your laptop or any computer connected to the network and then issuing a 'ping' command to the fully qualified VLE name.

  ```
  $ ping tikka1.customer-net.com
  ```

  The response should be:

  ```
  PING tikka1.customer-net.com (25.80.146.30): 56 data bytes
  64 bytes from 25.80.146.30: icmp_seq=0 ttl=250 time=1.050 ms
  64 bytes from 25.80.146.30: icmp_seq=1 ttl=250 time=0.598 ms
  64 bytes from 25.80.146.30: icmp_seq=2 ttl=250 time=0.719 ms
  ```

  You should **not** get the following message:

  ```
  ping: cannot resolve tikka1.customer-net.com: Unknown host
  ```

  If you get the 'Unknown host' message, then the VLE hostname is not registered with DNS. You should make sure that the customer makes the proper DNS entry and you have verified it, before proceeding to execute the setup_network.

- igb1 - This interface is bound to the VLE system and should have a dedicated static IP address. The system name is how the mainframe hosts (SMC and VTCS) communicate with the VLE and adheres to the naming convention of the mainframe environment.
- igb2 - This interface is bound to the alternate path to VLE and should have a dedicated static IP address. This will be the failover path used by the mainframe hosts (SMC and VTCS) to communicate with VLE.
- igb3 - It is used by the Oracle trained VLE service engineer only.

- The data ports (e1000g0 to e1000g15) - are typically dedicated data transfer from the VTSS, but can be designated as UUI connections if desired.
- In addition, there are two Ethernet ports available for monitoring the PDUs if desired. They can be configured to send out alerts and can be put on the same or different network segments from the management ports. If you want to monitor the PDUs, two IP addresses (DHCP or Static) are required for that purpose. These are wholly independent of the VLE software, so they can be on the same or different networks.

VLE GUI Connectivity View - Port Card Configuration Tab

As shown in FIGURE 2-4, you use the Connectivity View to configure the Ethernet ports that connect:

- The VLE to the VTSS.
- The VLE to the host (SMC/VTCS).

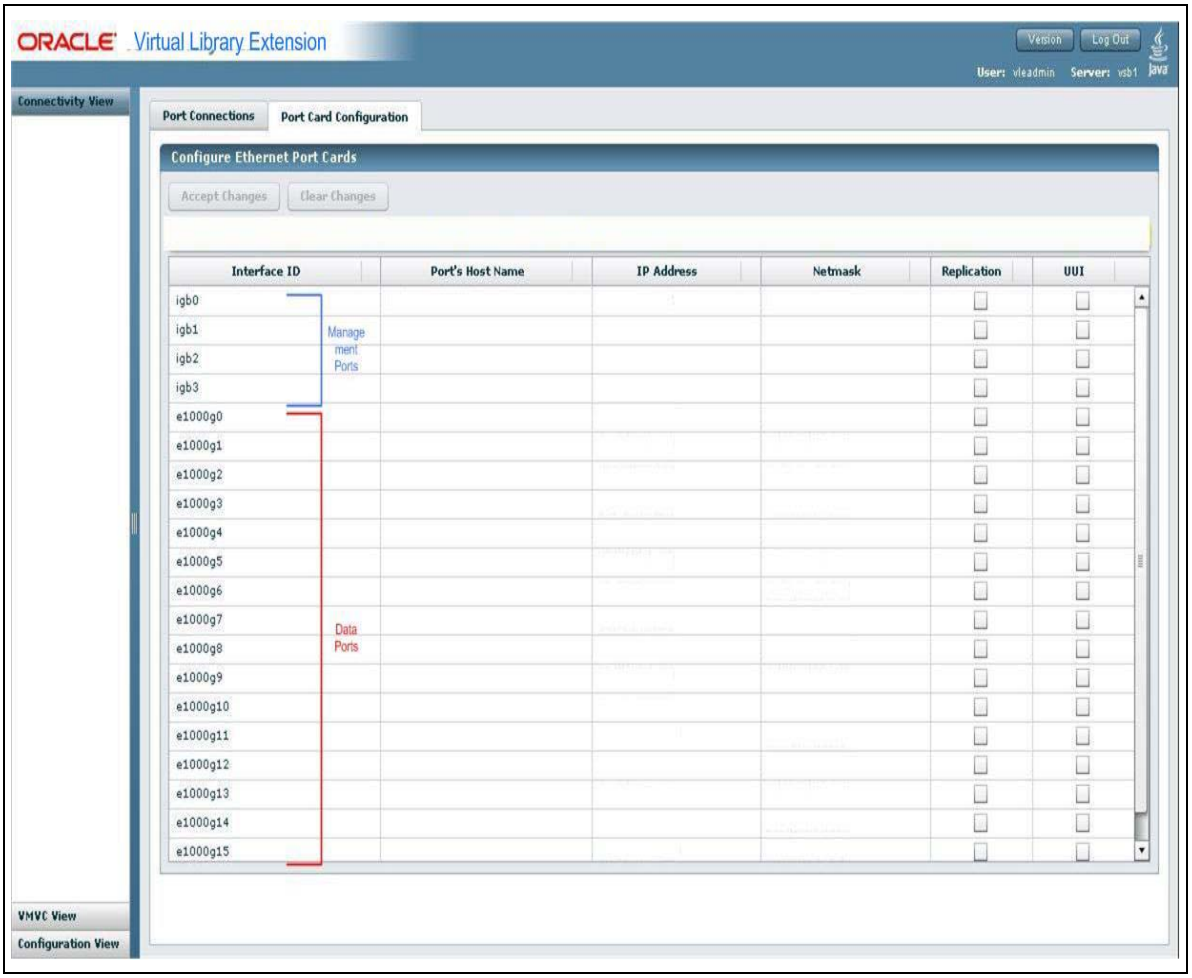


FIGURE 2-4 VLE GUI Connectivity View - Port Card Configuration Tab

See *Installing, Configuring, and Servicing the VLE Appliance* for more information on the VLE GUI.

FIGURE 2-4 on page 28 shows the Port Card Configuration Tab where you determine values for each of the fields as follows:

Interface ID

The Ethernet interface identifier, which is preset. In a Solaris terminal window, you can enter the `ifconfig -a` command to display the Interface ID for each port.

Port's Host Name

See "Determining the VLE Host Name" on page 25. You set this value when you run the configuration script. **Do not** change this value using this tab, which can render the VLE inoperable!

IP Address

A valid customer-provided IPV4 address for the port.

Assign the IP addresses as follows:

Note –

- The VLE Ethernet ports are pre-configured, which provides the files required for the ports to function and makes the configuration easier. Typically, the data port IP addresses are reconfigured for the network. TABLE B-9 on page 39 lists the default values.
- `igb3` is preconfigured with the static IP address shown in TABLE B-9 on page 39. Do not change the preconfigured address and 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 is always be available for service.
- All of the VLE ports that you use (except `igb3`, which has a fixed, static IP address) should be assigned unique network addresses (that is, not just unique host addresses).
- The VLE data transfer ports must be assigned unique network addresses to fully use available bandwidth. Similarly, each VSM5 IFF3 card must be on its own subnet. Additionally, StorageTek recommends that each pair of VTSS and VLE port addresses are the only addresses on their individual subnet.
- StorageTek recommends that you assign the data transfer ports to official private addresses, which may be less likely to collide with existing addresses on the LAN.
- The IP Address, Netmask, and Gateway values must be a valid IPv4 address in the form and in the range of 0.0.0.0 to 255.255.255.255.

Netmask

The customer-provided Network Mask. Typically, you use the VLE default for this value.

Replication

Is this IP address used for VLE-to-VTSS connections for VTV replication (yes or no)?

UUI

Is this IP address used for VLE-to-host (VTCS/SMC) connections (yes or no)?

Note – In general, a port is used either for VTV replication or UUI connection, but not both. Mainframe host connections (SMC/ VTCS), therefore, are specified as a UUI connections, whereas the VLE data ports are specified as Replication ports.

Determining VMVC Range Configuration Values

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

As shown in FIGURE 2-5, you use the `Create New VMVC Dialog Box` to specify volser ranges of new VMVCs.

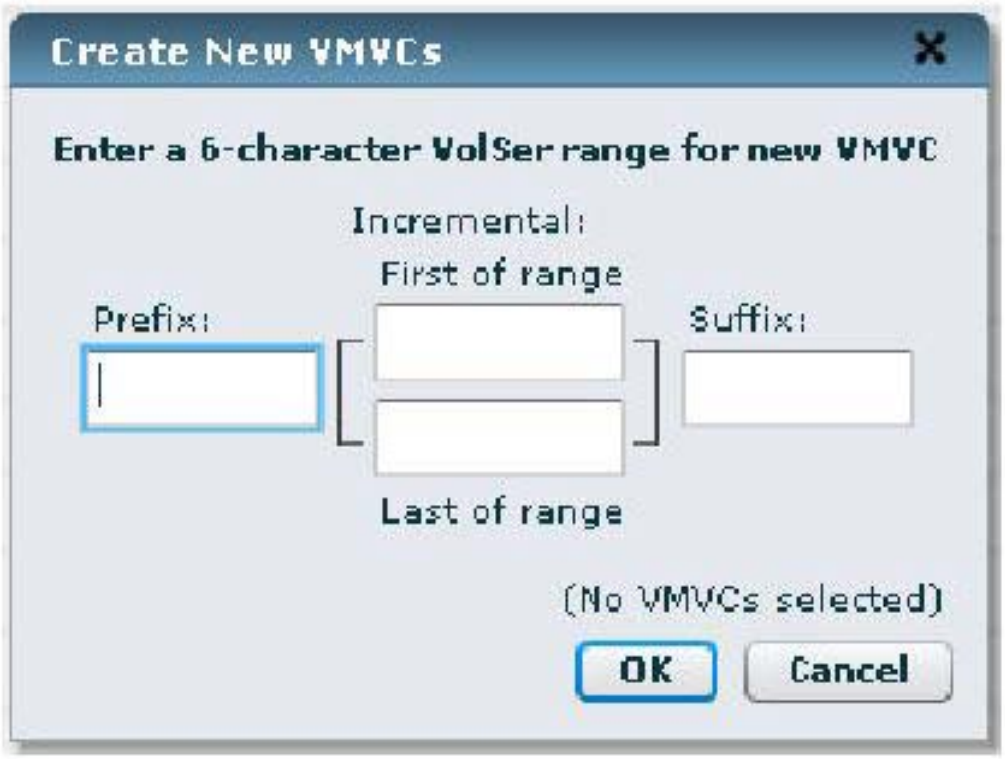


FIGURE 2-5 VLE GUI Create New VMVC Dialog Box

As FIGURE 2-5 shows, VMVC volsers must be 6 characters. You determine values for each of the fields as follows:

Prefix String

A Prefix is optional. If specified, alphanumeric characters that comprise the volser range prefix. The GUI converts lower or mixed case into upper case. For example, if you enter “ty”, the GUI converts this to “TY”.

First Range Value

The first alphanumeric value in a VMVC range.

Last Range Value

The last alphanumeric value in a VMVC range.

Suffix String

A suffix is optional. If specified, alphanumeric characters that comprise the volser range Suffix. The GUI converts lower or mixed case into upper case. For example, if you enter “ty”, the GUI converts this to “TY”.

Note –

- 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 2-6 shows the maximum VMVCs you can define for each VLE capacity.

TABLE 2-6 VLE Capacities - Maximum VMVCs

VLE Effective Capacity	Maximum VMVCs
220 TB	220
440 TB	440
660 TB	660
880 TB	880

- If you attempt to define overlapping ranges, they will display as separate rows during editing, but are collapsed after submitting the changes with the Commit New Groups button – the updated display will show a single group for any overlapping ranges.
- The VMVC volser ranges you specify in the VLE GUI must match the volser ranges defined to VTCS!

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

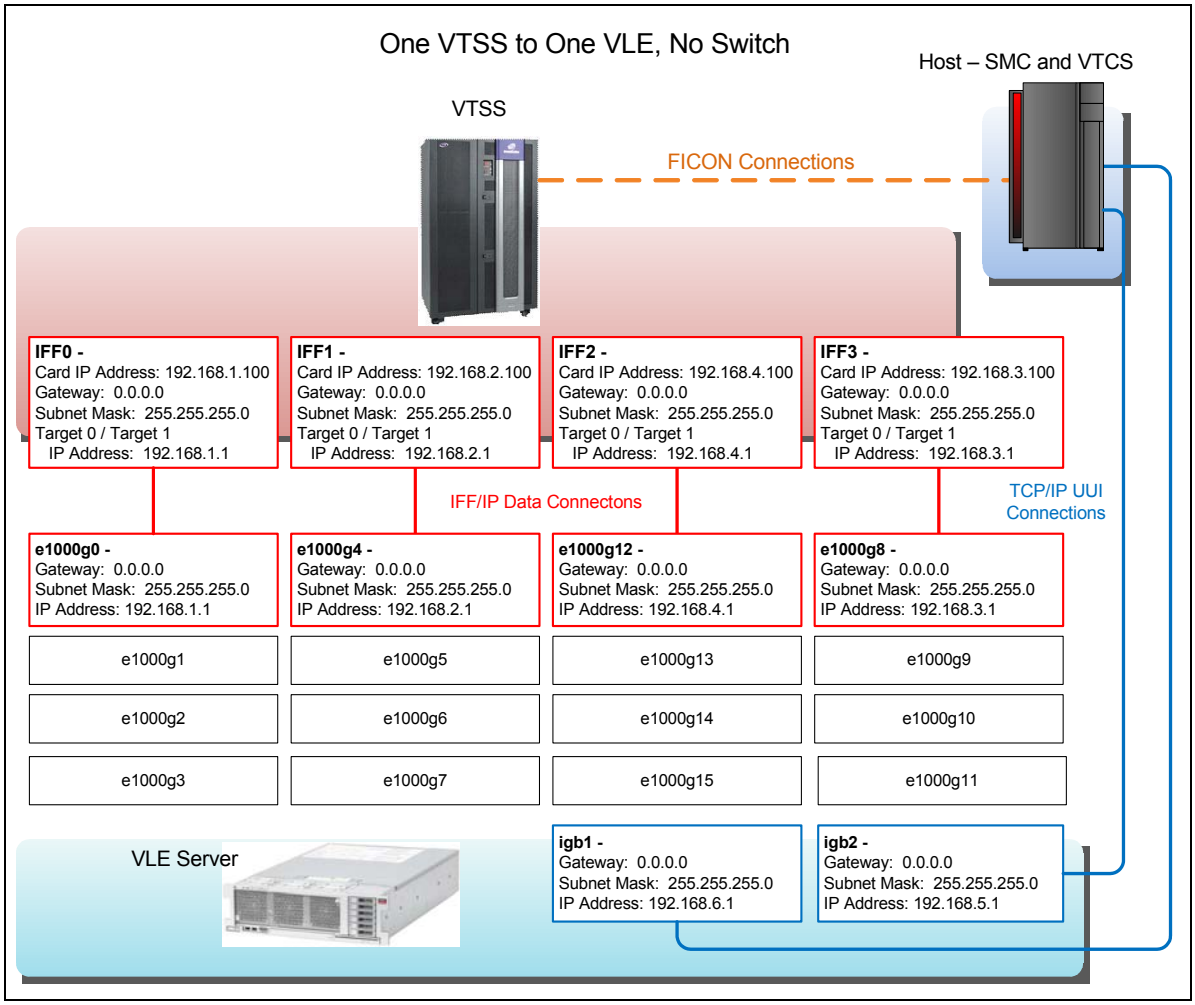


FIGURE A-6 Example 1: One VTSS Connected to One VLE

As FIGURE A-6 on page 34 and TABLE A-7 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-7 Example 1 Configuration Values

IFF Card and Target	IPIF Value	Interface ID	IP Address	Check Box
Data Connections				
IFF0 Target 0	0A:0	e1000g0	192.168.1.1	Replication
IFF0 Target 1	0A:1			
IFF1 Target 0	0I:0	e1000g4	192.168.2.1	
IFF1 Target 1	0I:1			
IFF2 Target 0	1A:0	e1000g12	192.168.4.1	
IFF2 Target 1	1A:1			
IFF3 Target 0	1I:0	e1000g8	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

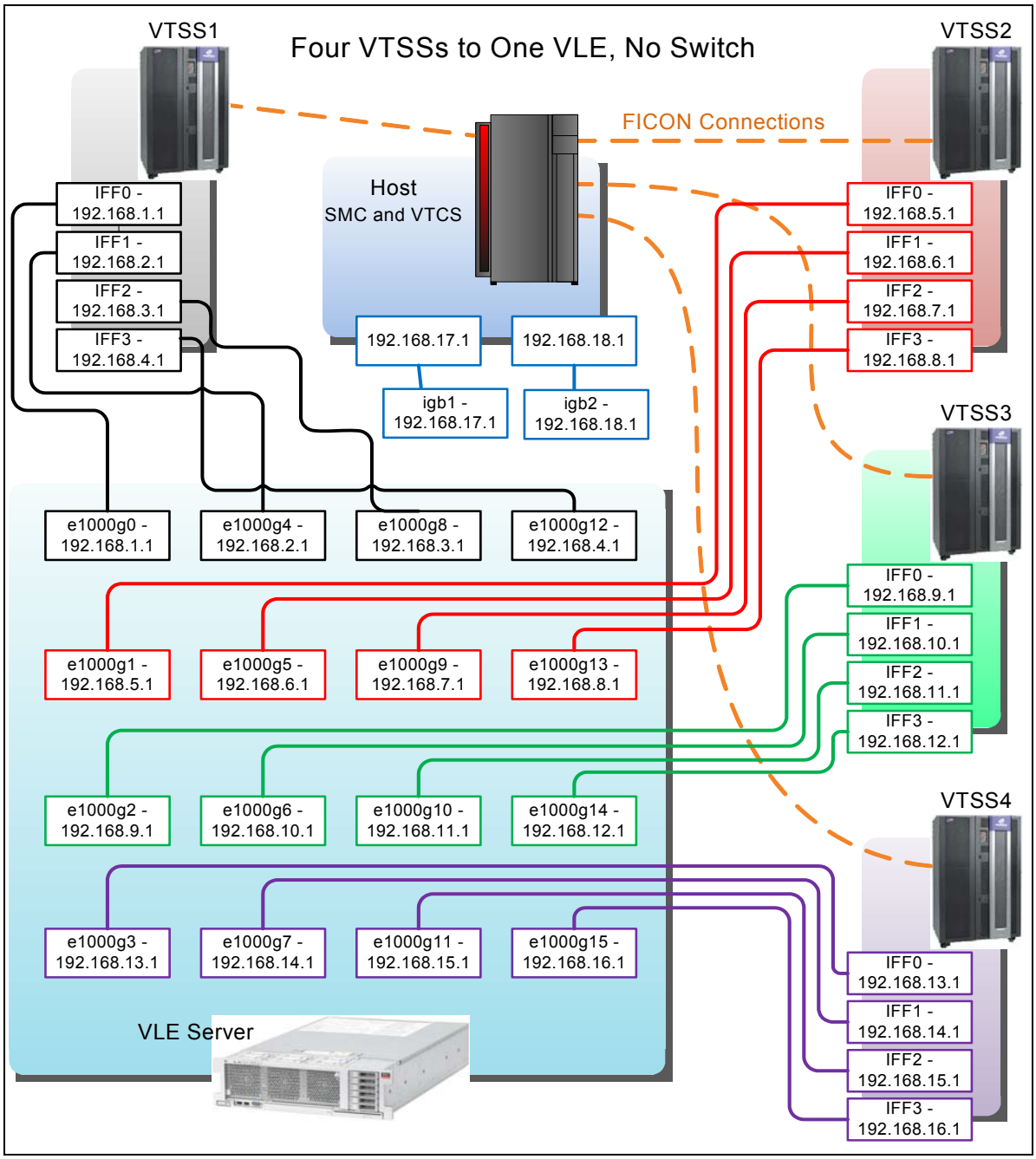


FIGURE A-7 Example 2: Four VTSSs Connected to One VLE

As FIGURE A-7 on page 36 and TABLE A-8 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-8 Example 2 Configuration Values

VSM5	IFF Card and Target	IPIF Value	Interface ID	IP Address	Check Box
		Data Connections			
	IFF0 Target 0	0A:0	e1000g0	192.168.1.1	Replication
	IFF1 Target 0	0I:0	e10004	192.168.2.1	
	IFF2 Target 0	1A:0	e1000g8	192.168.3.1	
VTSS1	IFF3 Target 0	1I:0	e1000g12	192.168.4.1	
	IFF0 Target 0	0A:0	e1000g1	192.168.5.1	
	IFF1 Target 0	0I:0	e1000g5	192.168.6.1	
	IFF2 Target 0	1A:0	e1000g9	192.168.7.1	
VTSS2	IFF3 Target 0	1I:0	e1000g13	192.168.8.1	
	IFF0 Target 0	0A:0	e1000g2	192.168.9.1	
	IFF1 Target 0	0I:0	e1000g6	192.168.10.1	
	IFF2 Target 0	1A:0	e1000g10	192.168.11.1	
VTSS3	IFF3 Target 0	1I:0	e1000g14	192.168.12.1	
	IFF0 Target 0	0A:0	e1000g3	192.168.13.1	
	IFF1 Target 0	0I:0	e1000g7	192.168.14.1	
	IFF2 Target 0	1A:0	e1000g11	192.168.15.1	
VTSS4	IFF3 Target 0	1I:0	e1000g15	192.168.16.1	

TABLE A-8 Example 2 Configuration Values

UUI Connections					
			igb1	192.168.17.1	UUI
			igb2	192.168.18.1	

B

VLE Preconfigured Default Values

The VLE Ethernet ports are pre-configured, which provides the files required for the ports to function and makes the configuration easier. Typically, the IP addresses for the data ports, `e1000g0-e1000g15`, are reconfigured for the network, as are management ports `igb0` and `igb1` (and possibly `igb2`). TABLE B-9 shows the VLE ethernet port default values.

TABLE B-9 VLE Port Configuration Default Values

Interface ID	Port Host Name	IP Address	Netmask
igb0	`v-`*serial_number*	10.0.1.1	255.255.255.0
igb1		10.0.2.1	255.255.255.0
igb2		10.0.3.1	255.255.255.0
igb3	`Service`	10.0.0.10	255.255.255.0
e1000g0		192.168.0.1	255.255.255.0
e1000g1		192.168.1.1	255.255.255.0
e1000g2		192.168.2.1	255.255.255.0
e1000g3		192.168.3.1	255.255.255.0
e1000g4		192.168.4.1	255.255.255.0
e1000g5		192.168.5.1	255.255.255.0
e1000g6		192.168.6.1	255.255.255.0
e1000g7		192.168.7.1	255.255.255.0
e1000g8		192.168.8.1	255.255.255.0
e1000g9		192.168.9.1	255.255.255.0
e1000g10		192.168.10.1	255.255.255.0
e1000g11		192.168.11.1	255.255.255.0
e1000g12		192.168.12.1	255.255.255.0
e1000g13		192.168.13.1	255.255.255.0
e1000g14		192.168.14.1	255.255.255.0
e1000g15		192.168.15.1	255.255.255.0

C

Controlling Contaminants

Environmental Contaminants

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

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

Oracle currently requires the ISO 14644-1 standard approved in 1999, but will require any updated standards for ISO 14644-1 as they are approved by the ISO governing body. The ISO 14644-1 standard primarily focuses on the quantity and size of particulates as well as 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 in the vicinity of 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, applicable human exposure limits from OSHA, NIOSH or the ACGIH should be used.

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 in size 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. Only vacuums equipped with High Efficiency Particulate Air (HEPA) filtration should be used 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 in order 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 prior to 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.
- Gaskets and sweeps can be used to address any gaps.
- Automatic doors should be avoided 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, and 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	**Fractional Efficiencies %**		
Dust spot efficiency %	**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 in order to accommodate positive pressurization and ventilation requirements. The data center should be designed to achieve positive pressurization in relation to more loosely controlled surrounding areas. Positive pressurization of the more sensitive areas is an effective means of controlling contaminant infiltration through any minor breaches in the room perimeter. Positive pressure systems are designed to apply outward air forces to doorways and other access points within the data processing center in order to minimize contaminant infiltration of the computer room. Only a minimal amount of air should be introduced into the controlled environment. In data centers with multiple rooms, the most sensitive areas should be the most highly pressurized. It is, however, extremely important that the air being used to positively pressurize the room does not adversely affect the environmental conditions in the room. It is essential that any air introduction from outside the computer room is adequately filtered and conditioned to ensure that it is within acceptable parameters. These parameters can be looser than the goal conditions for the room since the air introduction should be minimal. A precise determination of acceptable limits should be based on the amount of air being introduced and the potential impact on the environment of the data center.

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

Cleaning Procedures and Equipment

Even a perfectly designed data center will require 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
Bi-Annual 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, etc. 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. Specially treated dust wipes should be used to treat all hardware surfaces. Monitors should be treated with optical cleansers and static-free cloths. No Electro-Static Discharge (ESD) dissipative chemicals should be used 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.

Bi-Annual 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 so as 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 so as 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.