Guidelines and Best Practices for the Installation and Maintenance of Data Networking Equipment

Version 1.0

May, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: OL-28696-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Guidelines and Best Practices for the Installation and Maintenance of Data Networking Equipment

CONTENTS

CHAPTER 1

Introduction

This chapter describes the purpose, audience, and organization of this document. It also describes the importance of installation, maintenance, outlines types of maintenance programs, and lists relevant industry standards.

Purpose

This document provides general guidelines and best practices to follow during the installation and maintenance of Cisco's data networking equipment. These guidelines and best practices are based on empirical data and years of experience conducting field assessments and applying industry standards. They should be referred to in conjunction with the requirements that are outlined in the respective installation guides of Cisco data networking equipment. This document also describes requirements that are frequently missed by customers and partners in the installation sites.

Refer to the product documentation of the Cisco products that are mentioned in this document for more information on the relevant safety warnings for each.

Audience

This document is meant for customers or Cisco qualified personnel who are responsible for the installation and maintenance of data networking equipment in an installation site.

Document Organization

Title	Description
Chapter 1, "Introduction"	Describes the importance of installation and maintenance; outlines types of maintenance programs; and lists the relevant industry standards.
Chapter 2, "Installation"	Outlines the installation guidelines and best practices to follow for data networking equipment. It also outlines some installation requirements that are frequently missed by customers and partners.
Chapter 3, "Maintenance"	Outlines the guidelines and best practices to follow during the maintenance of data networking equipment. It also outlines some maintenance requirements that are frequently missed by customers and partners.

Information Classification

Information in the subsequent chapters is classified as outlined in Table 1-1.

Table 1-1 Information Classification

Classification	Description
Frequently Missed Requirements	Requirements that are already outlined in the installation guides of Cisco data networking equipment, but are often missed during installation. These requirements are supported by images of correct and/or incorrect implementation practices.
Guidelines	Recommended methods of implementing requirements that are already outlined in the existing installation guides of Cisco data networking equipment. While these guidelines are not mandatory, they support the successful implementation of requirements in the field especially when multiple methods are possible.
Best Practices	Refer to tasks, processes, methods, or techniques that are not required, but if implemented, provide benefits to customers and partners to better operate their equipment. They originate from lessons learned in the field by Cisco personnel, industry standards, and so on.

Document Conventions

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Importance of Installation

A faulty or incomplete installation of Cisco data networking equipment can lead to improper functioning or premature failure, and may even limit the possibility of performing effective maintenance. Even though the installation procedures are outlined in the Cisco installation guides, additional installation recommendations are included in Chapter 2, "Installation".

Importance of Maintenance

Regular equipment maintenance ensures that each device runs efficiently during its intended life span. Maintenance refers to all the actions that are performed to prevent a piece of equipment from failing, or to repair a failed or damaged piece of equipment. Therefore, maintenance is essentially a *time-based* or *equipment-based* function, which can be categorized based on when it is performed.

The benefits of conducting maintenance activities are as follows:

- An increase in the life span of the equipment, which results in an increase in the operational uptime of the network.
- A reduction in hardware failure, which saves operational costs in maintaining the network.
- An increase in the productivity of the operational resources.

For more information on the different types of maintenance programs, see the "Types of Maintenance Programs" section on page 1-3.

Types of Maintenance Programs

The following types of maintenance programs are performed on most types of equipment:

- Reactive Maintenance, page 1-4
- Preventive Maintenance, page 1-4
- Predictive Maintenance, page 1-5
- Reliability-Centered Maintenance, page 1-5

Note This document covers only preventive maintenance programs in detail in the subsequent chapters.

Based on the type of environment in a customer's network, the customer or partner can choose the maintenance program that aligns to their business requirement.

Reactive Maintenance

Reactive maintenance, also known as *breakdown* maintenance, is one of the most commonly adopted approaches and refers to the actions that are performed to restore a failed piece of equipment to bring it back to a workable condition. It is typically performed when the equipment needs to be replaced.

The advantages of a reactive maintenance program may include the following:

- It is cost-effective as the maintenance activity is performed only when the equipment breaks down. Therefore, there is no cost incurred till such time.
- It is not labor-intensive as manpower is not utilized to perform periodic maintenance activities.

The disadvantages of a reactive maintenance program may include the following:

- It leads to increased long-term equipment costs due to failures that can be severe or catastrophic during operational hours. Unplanned failures may also result in significant financial impact to the business.
- It leads to an increased labor cost if an overtime is required to compensate for the equipment downtime.
- The cost of replacing the failed or damaged piece of equipment.
- The probable damage to secondary equipment (assuming that it is kept in the same environment as the primary equipment) due to the failure in the primary equipment.

Preventive Maintenance

Preventive maintenance refers to the maintenance of equipment on a *time-based* schedule. It is based on the premise that many instances of equipment failure or malfunction can be prevented if a comprehensive maintenance schedule is followed.

The advantages of a preventive maintenance program may include the following:

- It is predictable and therefore makes budgeting and planning easier.
- It leads to reduced energy usage thereby increasing energy savings. For example, if the air filters are periodically cleaned, they are more efficient and consume less power to effectively operate the fans.
- It provides flexibility and periodicity of maintenance schedules.
- It increases the life cycle of the individual components of a piece of equipment.
- It provides a sense of assurance that the equipment is properly maintained and functioning as designed.
- It reduces the frequency and severity of equipment failure and malfunction, which helps to increase the operational uptime of the network.

The disadvantages of a preventive maintenance program may include the following:

- It is time-consuming and labor-intensive.
- It does not consider the current state of the equipment before the maintenance activity is performed.

Predictive Maintenance

Predictive maintenance, also known as *condition-based* maintenance, refers to the actions that are performed on a piece of equipment when one or more conditions are met. These conditions indicate when a piece of equipment is about to fail or deteriorate in performance based on the data that is gathered after observing the state of the equipment. Technological advancement in equipment monitoring has lead to the development of tools that help maintenance personnel gather and analyze condition data, and then perform maintenance on a piece of equipment at the appropriate time.

The advantages of a predictive maintenance program may include the following:

- It enables pre-emptive corrective actions to be taken.
- It leads to lower downtime of the equipment.
- It leads to lower maintenance cost because the maintenance activity is performed only when certain system conditions are met.
- It reduces labor cost and the man-hours that are spend on unnecessary maintenance activities.
- It reduces problems that may arise due to the unnecessary interference by the maintenance personnel.
- It leads to an improvement in the overall safety and reliability of the system.

The disadvantages of a predictive maintenance program may include the following:

- It typically leads to higher personnel training costs.
- It may overlook devices that require maintenance.

Reliability-Centered Maintenance

Reliability-centered maintenance refers to a methodology that is developed to address certain key issues that cannot be addressed by the other maintenance programs. It is based on the premise that all equipment is not of equal importance for the smooth functioning and safety of a facility. It considers the difference in the design and operation of different types of equipment, which leads to a differential in the probability of failure and damage to the equipment. It also considers an important factor of not having unlimited access to finance and personnel, and therefore, seeks to prioritize and optimize the use of the same.

An optimally structured reliability-centered maintenance program can be broken down as follows:

- Less than 10% Reactive
- 25% to 35% Preventive
- 45% to 55% Predictive

Industry Standards

In addition to the standards that are already mentioned in the installation guides of Cisco data networking equipment, refer to the following standards for the operational and maintenance requirements:

- Telcordia GR-63 “NEBS Requirements: Physical Protection”
- “iNEMI Position Statement on the Limits of Temperature, Humidity and Gaseous Contamination in Data Centers and Telecommunication Rooms to Avoid Creep Corrosion on Printed Circuit Boards”

- ISA-S71.04-1985 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants
- ASHRAE TC 9.9 “2011 Thermal Guidelines for Data Processing Environments - Expanded Data Center Classes and Usage Guidance”
- National Electrical Manufacturers Association (NEMA) Type 1
- International Electrotechnical Commission (IEC) IP-20
- National Electrical Code (NEC) National Fire Protection Association (NFPA) 70, Article 800.133 (2005 NEC)

CHAPTER 2

Installation

This chapter outlines the guidelines and best practices for the installation of data networking equipment. The information is mainly based on the experience gathered from environmental assessments that are performed by Cisco personnel at customer sites around the world. It also covers a few installation requirements, which are already included in the respective installation guides, but are often missed.

The implementation of the installation requirements is mandatory for the proper functioning of Cisco data networking equipment. The guidelines and best practices that are explained in this module help improve operations by minimizing the risk of failure, increasing the mean time between failures (MTBF), reducing the installation time, and planning the maintenance costs.

This chapter includes the following sections:

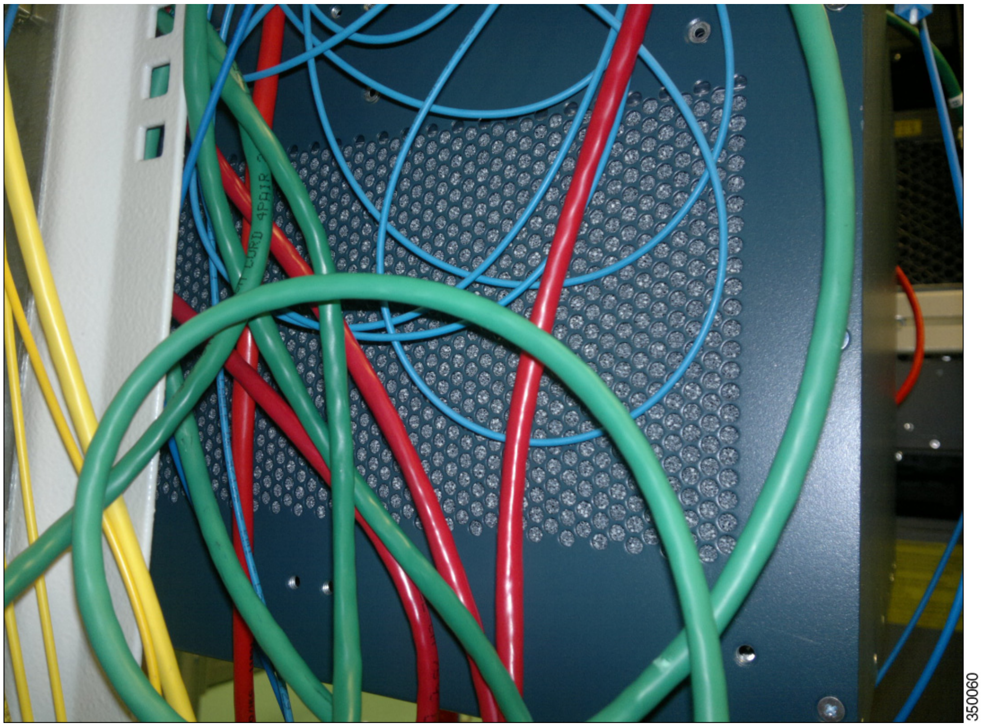
Cabling

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

- Ensure that the cables are not installed in front of the air ventilation grids (as shown in Figure 2-1) as it leads to improper ventilation, overheating of the equipment, and dust accumulation.

Figure 2-1 Cables Obstructing the Air Grid on the side of a Cisco Data Networking equipment

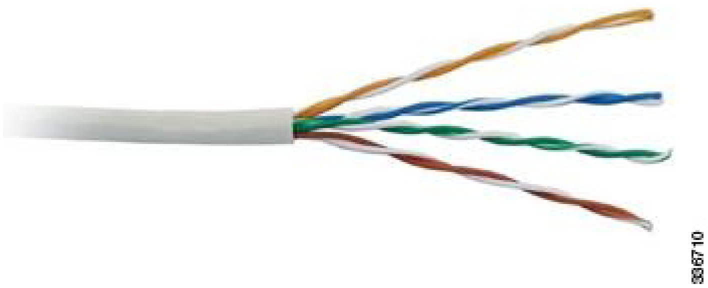


Guidelines

The following guidelines are recommended during the installation of cables:

- Avoid placing multiple cable bundles over each other, or over bundling the cables, as it leads to performance degradation of the cables below.
- Ensure that the cables twisted (as shown in Figure 2-2) together for canceling out Electromagnetic Interference (EMI) from the external sources are not exposed even partially, as it results in EMI issues.

Figure 2-2 Twisted Cable



- Separate the copper and fiber cables in the runs (or have separate runs) because the weight of the copper cables can crush the fiber cables that are placed below it.

- Use cables that are resistive to bend loss if excessive bending of cables cannot be prevented due to installation constraints.
- Avoid mounting the cabling components in places that block accessibility to other equipment (such as a power strip or fans) in and out of the racks.
- Maintain extra cables for contingency needs as spares for the backbone and horizontal runs.
- Avoid the following actions that can stress the cable:
  - Applying extra twists.
  - Pulling or stretching beyond the specified pulling load rate.
  - Bending it beyond the specified bend radius, and not beyond 90º.
  - Creating tension in the suspension runs.
  - Stapling or applying pressure with the cable ties.
- Avoid routing the cables through holes and pipes, as this can limit the addition of cable runs in the future.
- Label the cables with their destination at each and every termination point (to ensure that both the ends of the cable are labeled for identification and traceability).
- Test every cable during installation and termination. If a problem occurs, tag the malfunctioning cables and separate them out.
- If applicable, locate the main cabling distribution area close to the central region of the installation site to minimize the cable distances.
- Preserve the same density of twists in the cable pairs till its termination for horizontal and backbone twisted-pair cabling as applicable.
- Dedicate outlets for terminating horizontal cables, that is, assign a port in the patch panel for each horizontal run.
- Include sufficient vertical and horizontal runs when designing the cables. Otherwise, even a slight change, such as the removal of a cable can cause downtime.
- Use the angled patch panels in high-density areas, such as the cable distribution area. Use the straight patch panels in the distribution racks.
- Avoid exposing cables to areas of condensation and direct sunlight.
- Remove the abandoned cables, as they restrict the airflow, and contribute to the possible increase in the operational temperatures, which can affect the durability of the system.
- Avoid routing the cables over equipment and other patch panel ports (as shown in Figure 2-3). Instead, route the cables below or above, and into the horizontal cable manager (if it is in place) (as shown in Figure 2-4 and Figure 2-5).
- The NEC (NFPA 70), Article 800.133 (2005 NEC) indicates the separation requirements. This section of the NEC specifies the following:
  Communication wires and cables shall be separated at least 50 mm (2 inches) from conductors of any electric, power, Class 1, non-power limited fire alarm, or medium-power network-powered broadband communication circuits.
  However, there are multiple exceptions to this generic rule, so refer to the *NEC (NPFA 70)* standard for more information.

Figure 2-3 Improper Cabling Causing Ineffective Operations and Maintenance

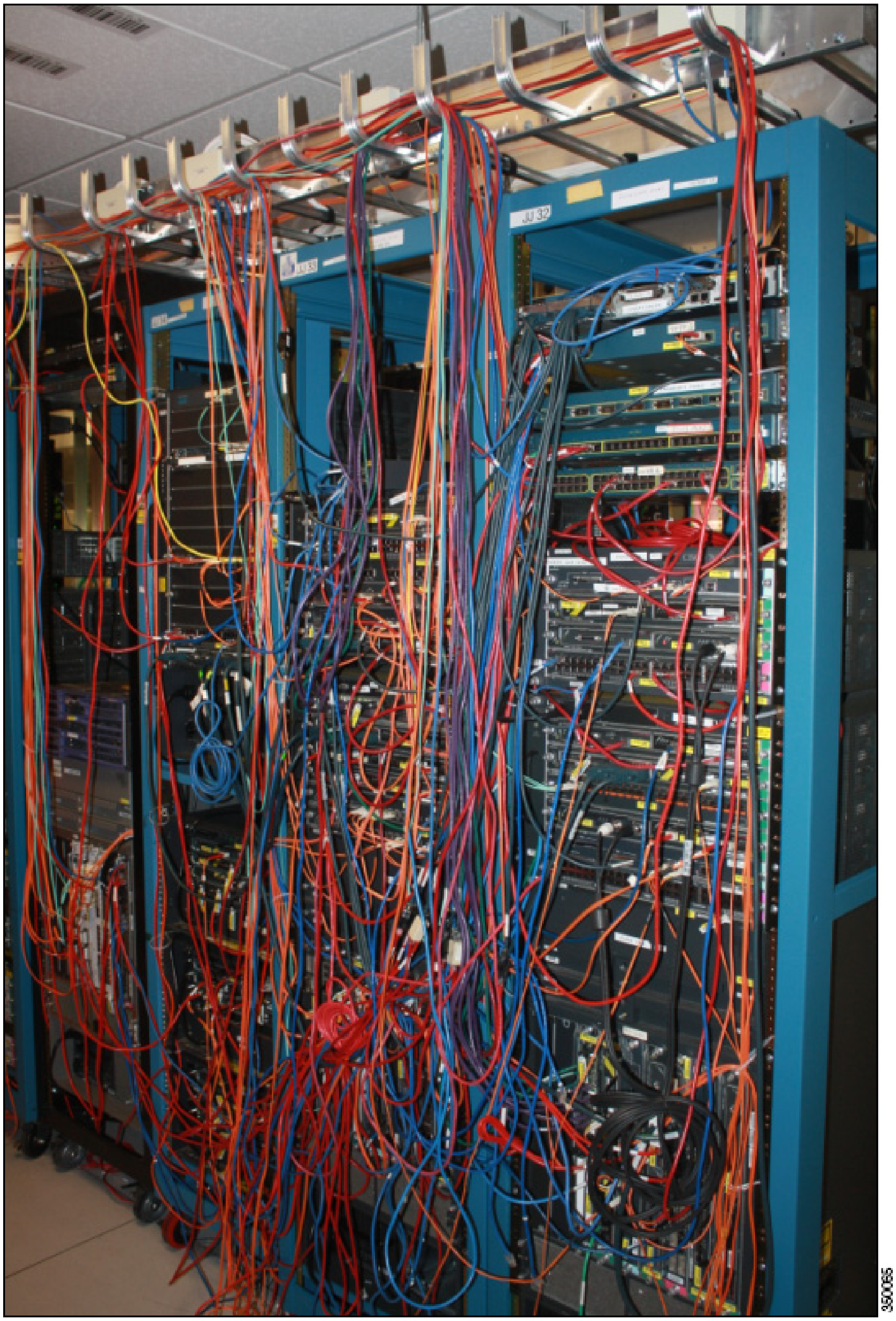


Figure 2-4 *Proper Cabling*

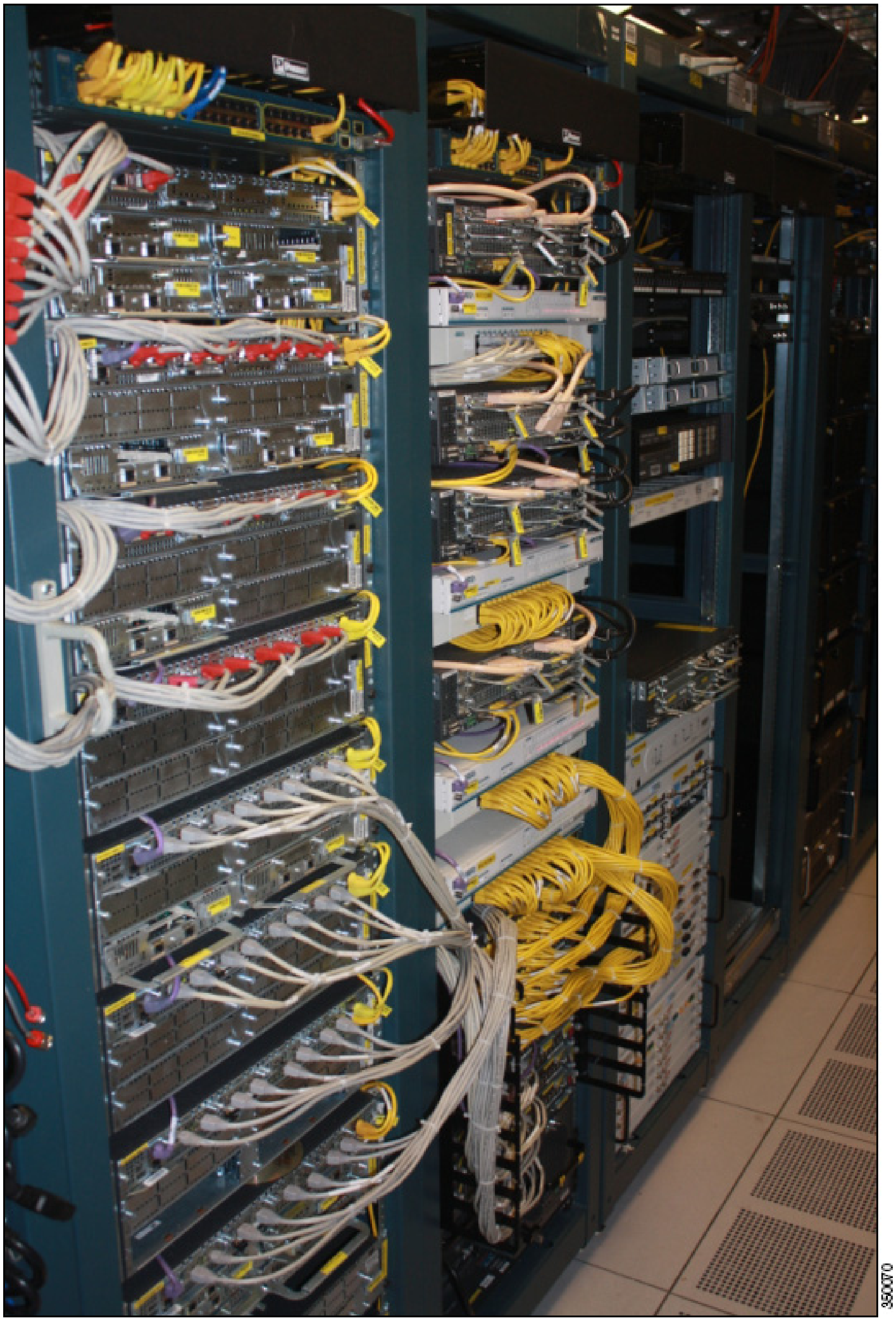


Figure 2-5 Efficient Cabling

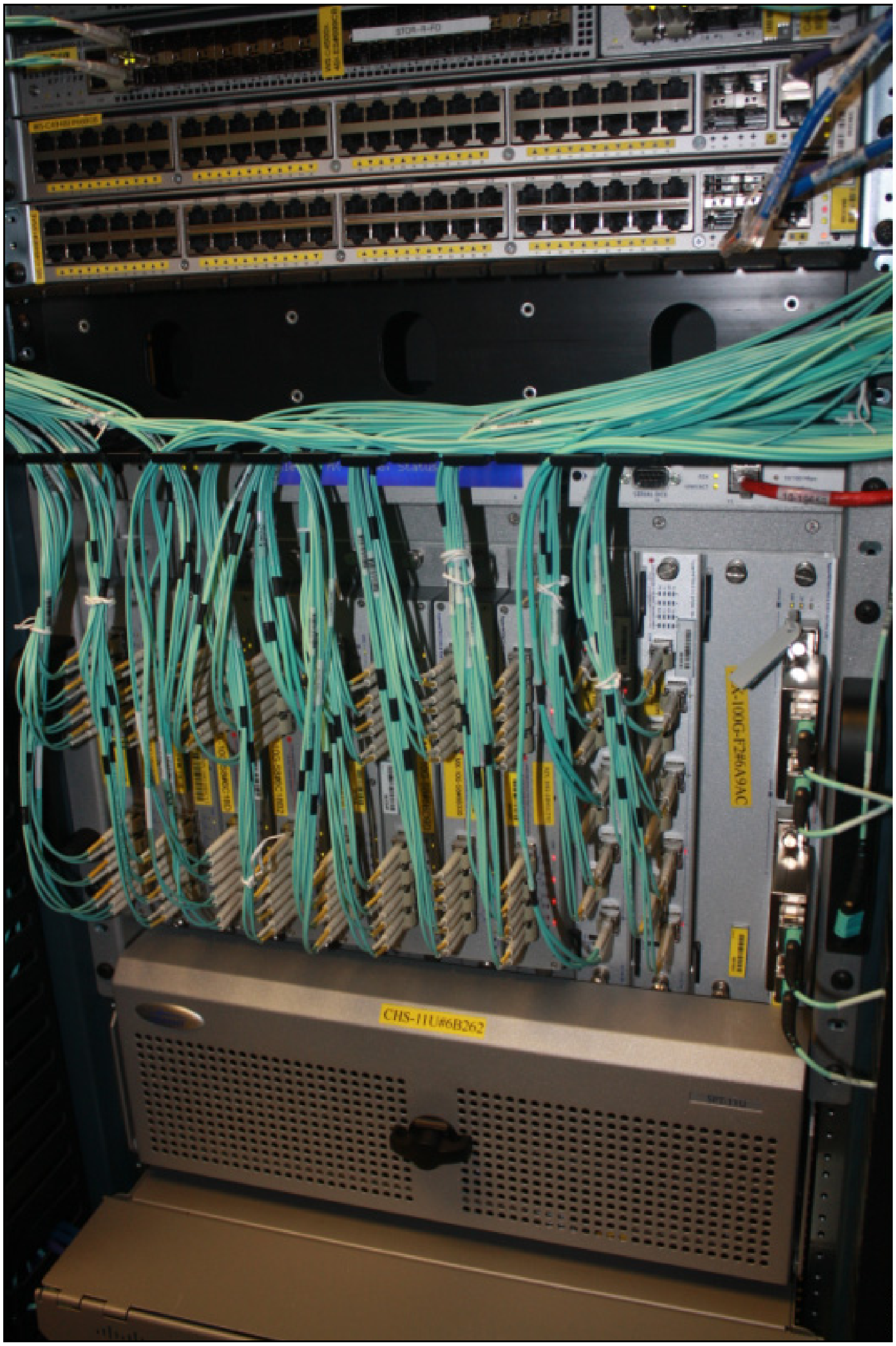
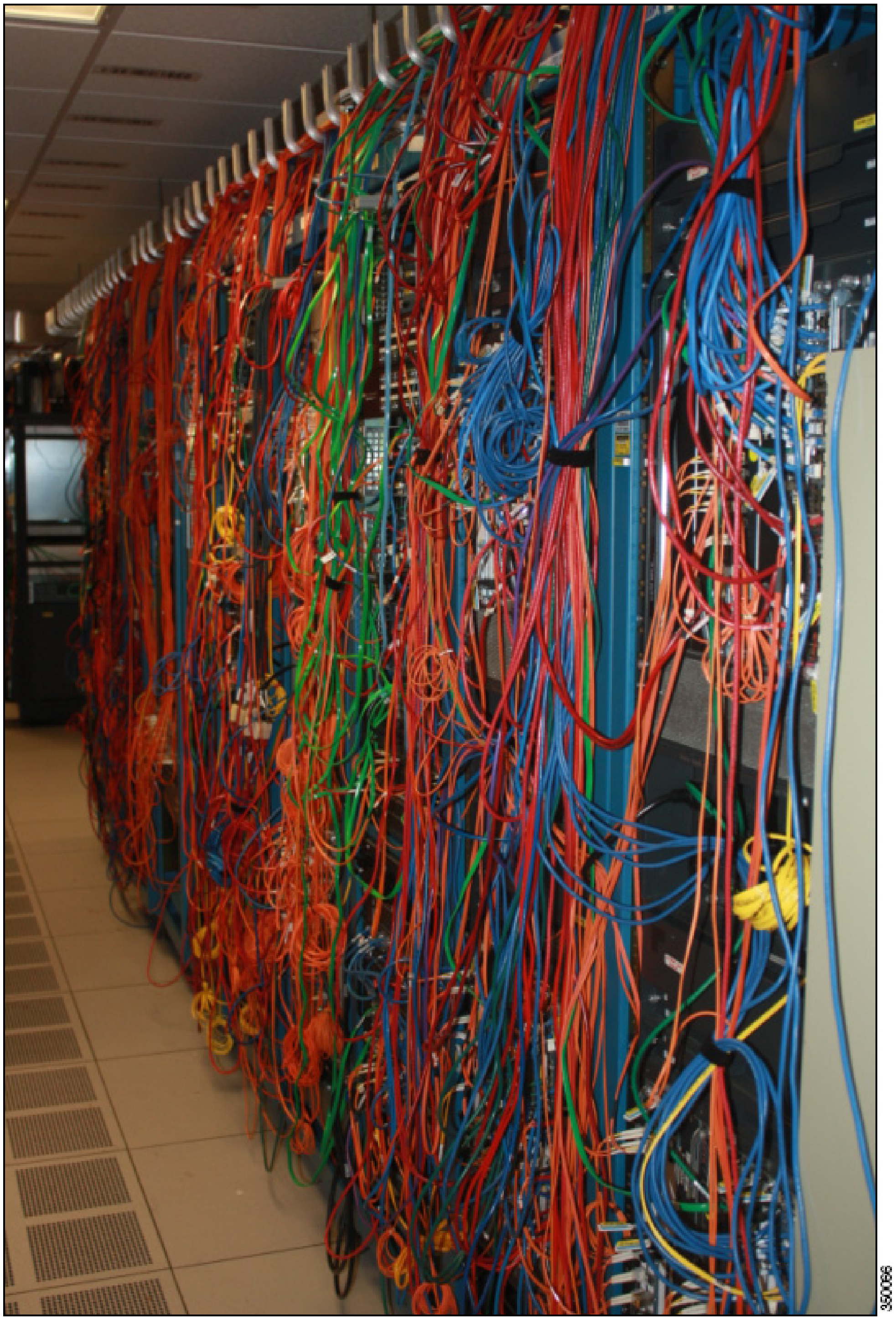
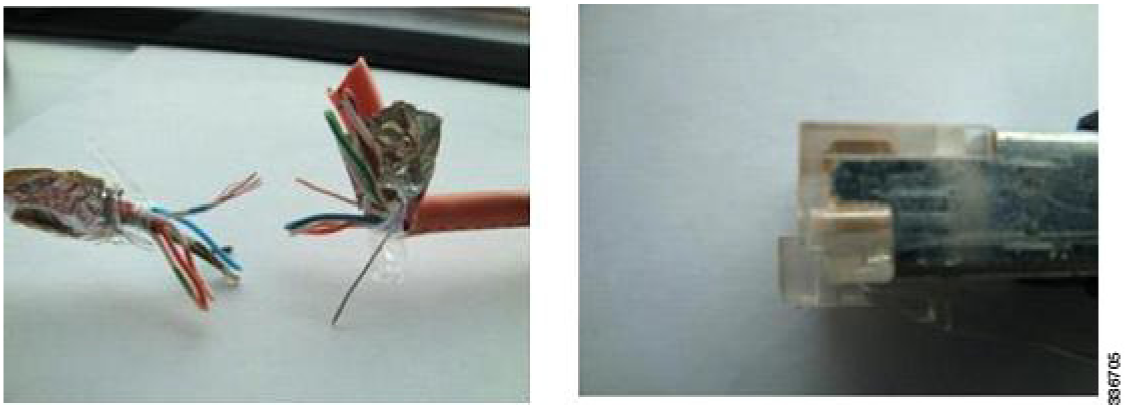


Figure 2-6 Inefficient Cabling



- Avoid using patch cables, which are used to connect data networking equipment to patch panels that are constructed using a solid core STP cable with stranded core RJ-45 connectors (as shown in Figure 2-7), because this can cause failure of the individual cables over a period of time due to connector differences and core size. Also, the risk of failure increases due to the movement or flexing of cables and/or stress between the cable and connectors.

Figure 2-7 Patch Cables with Solid Core STP Cable and Stranded Core RJ-45 Connectors

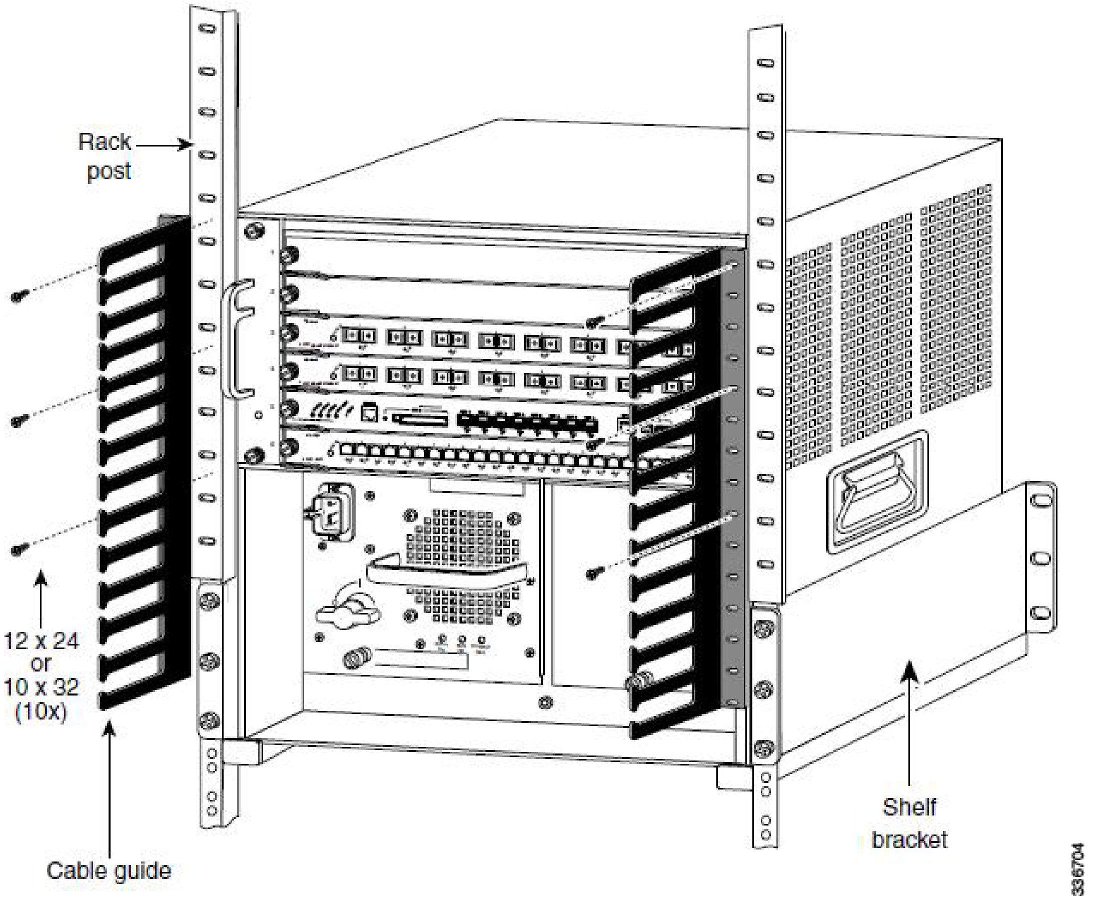


Best Practices

The following best practices are recommended during the installation of cables:

- Install higher cable categories to meet the application requirements that may arise in the future.
- Use thin and high-density cables as necessary to enable more cable runs in tight spaces.
- Use modular cabling systems to map the ports from equipment with high density port counts.
- Avoid leaving loose cables on the floor, as this could constitute as a major safety hazard. Instead, use the vertical, horizontal, or overhead cable managers.
- Store a few spare patch cables. The type and quantity of the patch cables can be determined from the installation and projected growth. Ensure to store all the unused cables in a bagged and capped condition when not in use.
- Use the patch cable of exact length, and leave some slack at each end for end device movements.
- Use vertical and horizontal cable guides for routing cables within and between the racks.
- Use cable spool devices in the cable managers to prevent kinks and sharp bends in the cable.
- Bundle the related cables together in groups (for example, bundle the ISL cables and uplinks to their core devices), as this eases management and troubleshooting.
- Use the Velcro-based ties every 1 to 2 meters for bundling or securing the cables, and avoid using the zip ties as they apply pressure on the cables.
- Regularly maintain the cabling documentation, labeling, and physical or logical cabling diagrams.
- Document and regularly update all the cabling components and their mapping.
- For new installations or re-cabling of the existing equipment, install the cable guides to reduce mechanical stress and bending of the data cables, and to enhance the maintainability. Figure 2-8 shows an example of the recommended cable guides for the Cisco Catalyst 6500 chassis. The installation and usage of cable guides should be independent of the number of cables that are installed. However, there are products that do use cable guides, or where the cable guides cannot be installed. For more information on the cable guides, see the installation guides that support specific Cisco data networking equipment.

Figure 2-8 Examples of Recommended Cable Guides for the Cisco Catalyst 6500 Chassis



- Cable guides are particularly useful because excessive bending of the interface cables damages them. Figure 2-9 shows an example of an efficient way of cabling using the cable guides. The minimum long-term, low-stress bend radius (as shown in Figure 2-10) of the fiber optic cable should be less than 15 times the cable diameter. A smaller bend radius can change the characteristics of the fiber cable, which could cause signal errors.

Figure 2-9 Efficient Cabling using Cable Guides

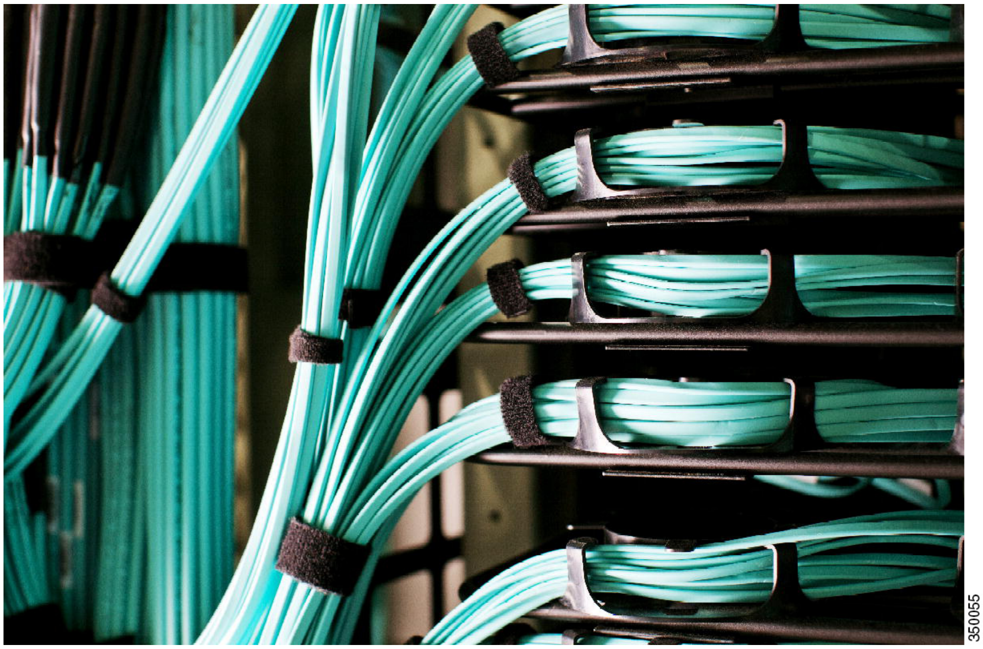
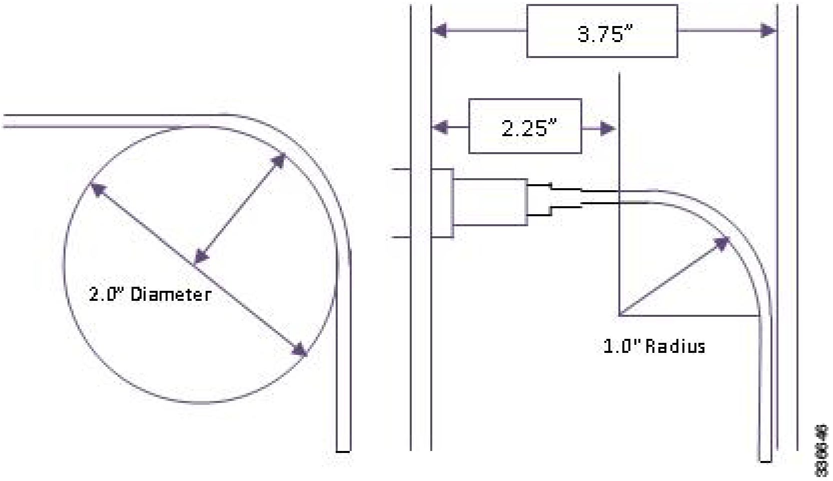


Figure 2-10 Bend Radius



Grounding

- Introduction, page 2-11
- Frequently Missed Requirements, page 2-11
- Guidelines, page 2-17
- Best Practices, page 2-18

Introduction

Ground (earth) refers to the reference point in an electrical circuit from which other voltages are measured, or a common return path for an electric current, or a direct physical connection to the Earth.

Electrical circuits are connected to the ground (earth) for several reasons. For example, in equipment that is powered by the mains, the exposed metal parts are connected to the ground to prevent the user contact with dangerous voltage if the electrical insulation fails. Connections to the ground limit the build up of static electricity when handling electrostatic-sensitive devices.

Frequently Missed Requirements

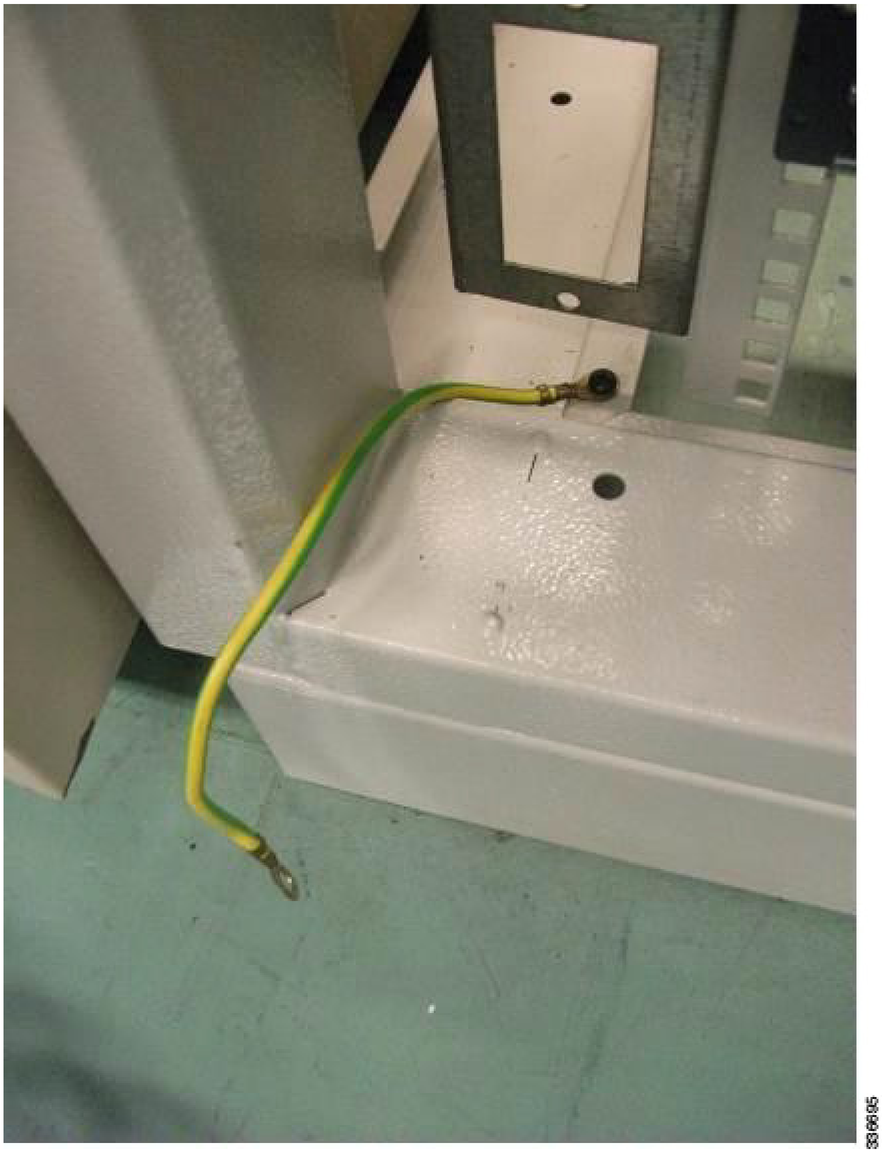
The following are examples of requirements that are frequently missed in the field:

- Equipment racks are often not connected to the installation site or building ground. So, the equipment managers should ensure that all the equipment racks are grounded to the building. If not done, it can pose a serious safety risk to the personnel. Additionally, an electrical current can cause operational deficiencies or expose the data networking equipment to the risk of permanent failure due to ESD risk.

Note One of the initial instructions in Cisco installation guides is to ground the rack. Because there are different laws and legislations in different countries, this activity is usually performed by qualified electricians that have the proper instrumentation to help them test the effectiveness of the rack grounding.

Figure 2-11 depicts the grounding cable that is not connected to the grounding bar of the installation site.

Figure 2-11 Rack Grounding Cable not Connected to the Grounding Bar



- In addition to rack grounding, many Cisco data networking devices require the installation of an NEBS (Network Electrical Building System) compliant ground, and they have dedicated grounding points for that. This is because a system that uses only an AC third prong ground is not sufficient to fully ground the device. Electrical damage can lead to the following failures:
  - Damage to the component due to Electrostatic Discharge (ESD)
  - Data corruption
  - System lockup
  - Frequent system reboots

- Some customers claim that they do not need NEBS grounding as they rely on metal-to-metal connections between the Cisco device and rack. However, this connectivity can become weak over time (for example, due to vibrations) and make the grounding ineffective. Instead, use a multimeter to verify the effectiveness of the metal-to-metal connectivity. For example, the use of plastic screws and washers to minimize vibrations avoids effective metal-to-metal connections.

  Even though the multimeter confirms good connectivity, you still need NEBS as the metal-to-metal connections can get disconnected from the rack and power supply during the maintenance of the equipment and it is only the NEBS grounding that ensures that the grounding is still in place.

Figure 2-12 Missed System (NEBS) Grounding on a Cisco Nexus 7000

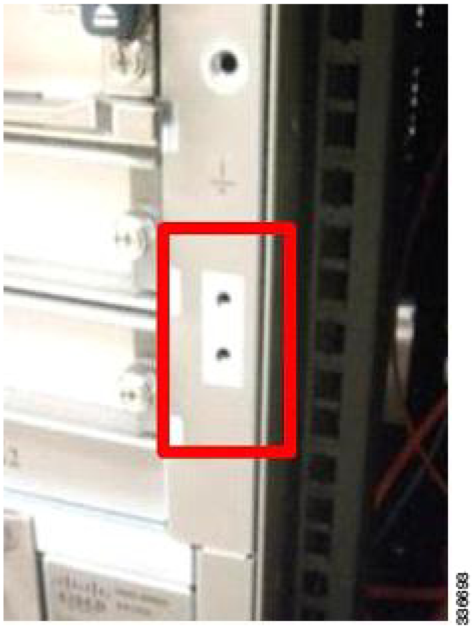


Figure 2-13 Missed System (NEBS) Grounding on a Cisco ONS 15454

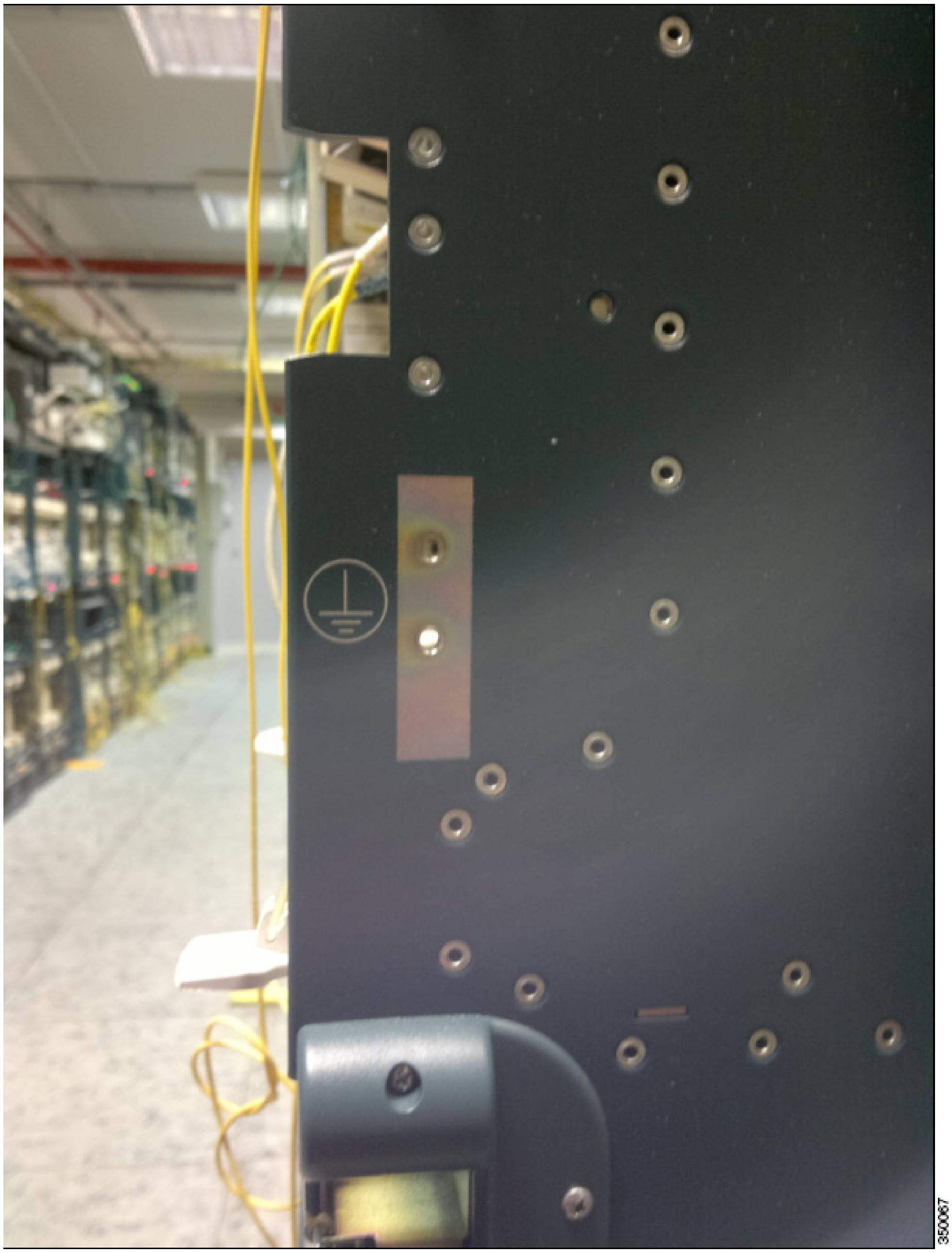


Figure 2-14 Missed System (NEBS) grounding on a Cisco Catalyst 6500

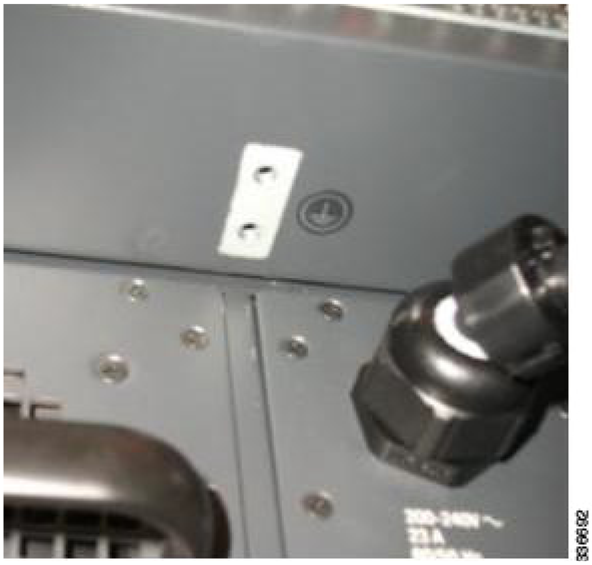
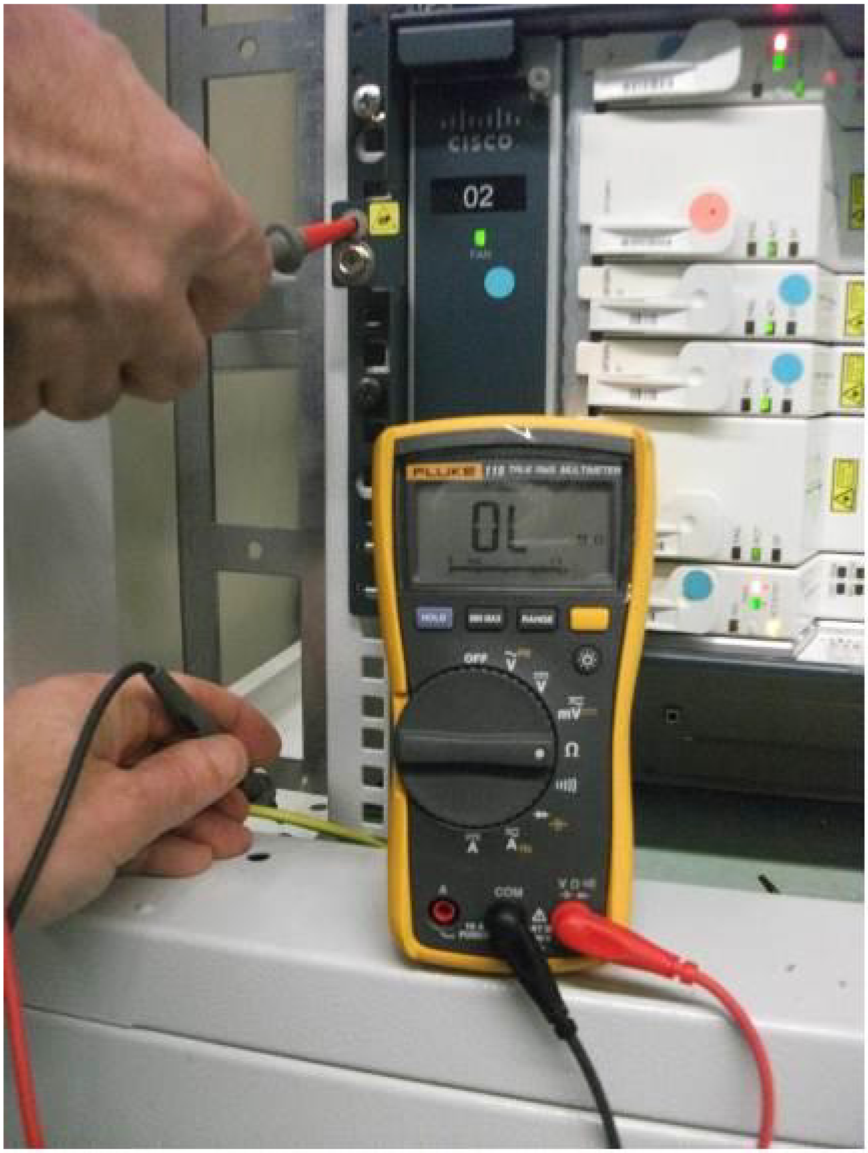
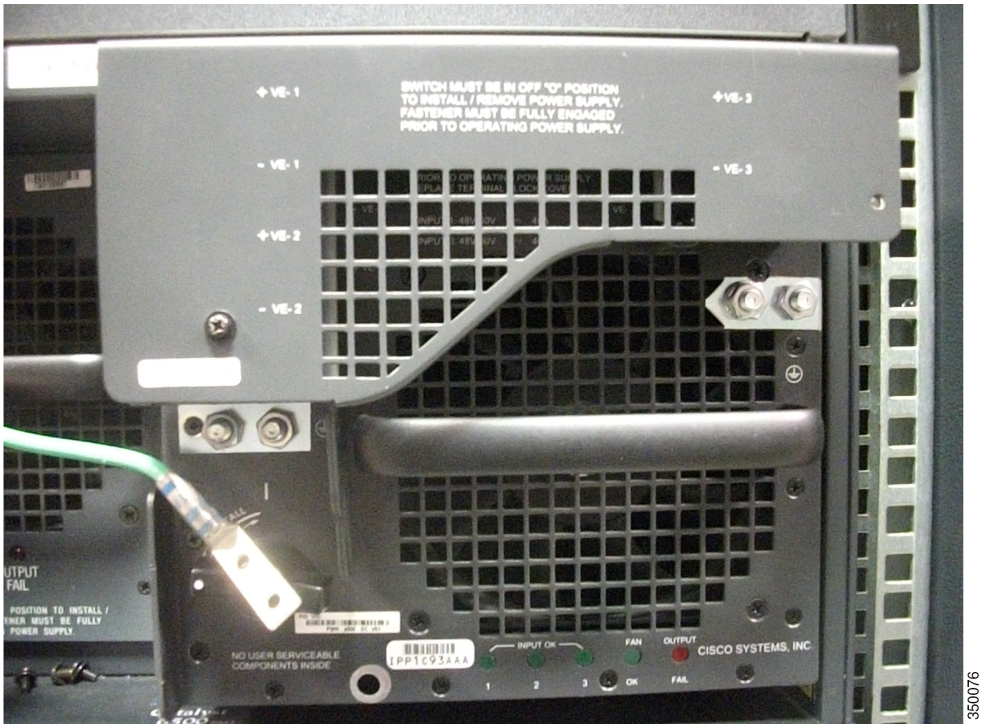


Figure 2-15 Ineffective Metal-to-Metal Contact between Cisco Chassis and Installation Rack



- A few of the Cisco power supplies require dedicated and independent grounding. But, during the field survey, it was observed that most customers do not provide Cisco power supplies with dedicated and independent grounding as it should be, under the false assumption that the metal-to-metal contact with the device is sufficient.

Figure 2-16 8700 W Power Supply not Grounded - Installed in a Cisco Catalyst 6513


+VE-1
-VE-1
+VE-2
-VE-2
+VE-3
-VE-3
SWITCH MUST BE IN OFF "O" POSITION TO INSTALL / REMOVE POWER SUPPLY. FASTENER MUST BE FULLY ENGAGED PRIOR TO OPERATING POWER SUPPLY.
NO USER SERVICEABLE COMPONENTS INSIDE
INPUT OK
1
2
3
OK
FAN
OUTPUT
FAIL
CISCO SYSTEMS, INC.
350076

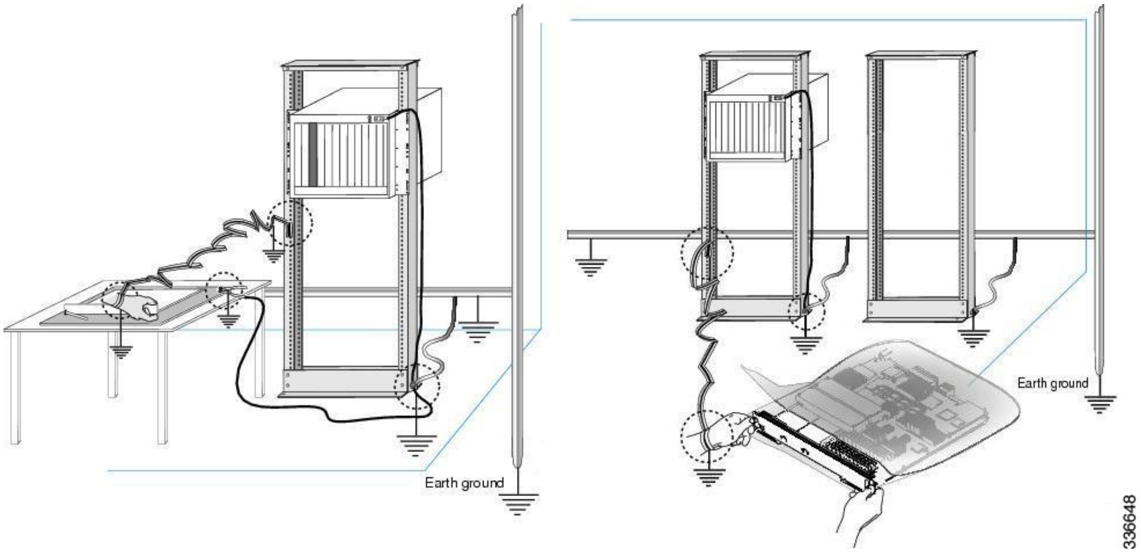
- Pay special attention to the racks and other Cisco equipment that are painted with non-conductive paint, as the connection of ground wiring to the painted surfaces may be unreliable. Ground wiring should always have metal-to-metal contact unless you are sure that the paint is conductive.

Guidelines

The following guidelines are recommended for the effective implementation of the grounding requirements for data networking equipment:

- Perform an initial test (using a calibrated multimeter) to check the effectiveness of the earth or system grounding from the rack to the pit and maintain the test records.
- Ensure that proper grounding practices are in place (as shown in Figure 2-17), so that the buildings and the equipment installed in them have low-impedance connections and a low-voltage differential between the chassis. For more information on how to prevent ESD damage during installation and perform proper grounding, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms* (http://www.cisco.com/en/US/docs/optical/esd_grounding/guide/esd_grounding.html). Though these guidelines are specifically designed for optical products, they are generic enough to apply to the vast majority of Cisco products.

Figure 2-17 Guidelines for Grounding During Installation, Operation, and Maintenance



Best Practices

Use a multimeter or an equivalent device to check the effectiveness of the connectivity between different parts of the installed equipment (such as, cards, chassis, and racks) to the building ground. The multimeter readings should be less than 1 Ohm for good point-to-point resistivity.

Electrostatic Discharge (ESD)

Introduction

Electrostatic Discharge (ESD) refers to the transfer of electrostatic charge between bodies at varied voltages that is caused by direct contact or induced by an electrostatic field. When you walk across a carpet and touch a metal door knob, you experience a slight shock on your fingers. If the same ESD occurs in data networking equipment, the equipment can be damaged or destroyed.

ESD damage occurs most often when printed circuit boards are improperly handled while being transported in metal carriers. Electromagnetic interference (EMI) shielders and connectors are integral components of the metal carrier, and help to protect the board from ESD. However, it is best to use the ESD protection devices when handling circuit boards.

In summary, ESD damage occurs due to the following:

- Direct electrostatic discharge to the device.
- Electrostatic discharge from the device.

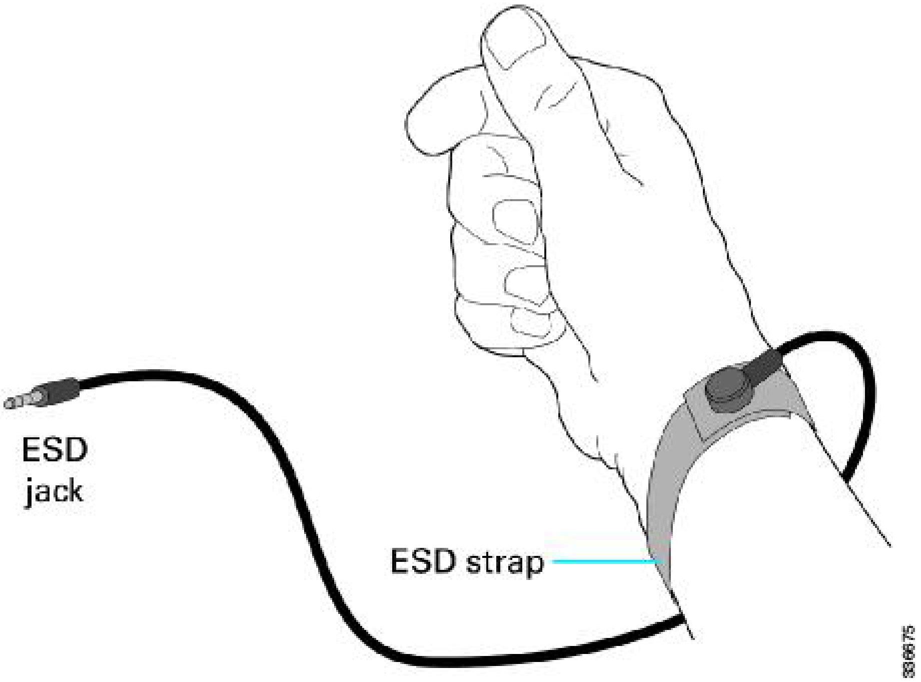
- Field-induced discharges.

ESD damage is also unknowingly caused when inspecting, sorting, or installing the ESD-sensitive devices.

The following are the most common devices used during the installation of data networking equipment to prevent ESD damage:

- Antistatic wrist strap—Also called an ESD strap is made of an insulated material with a wire attached to specifically drain the electrical charges away. Attach one end of the wrist strap to an earth ground, that is, the ground pin on an extension cord, and wrap the other end around your wrist as shown in Figure 2-18. The wrist strap uses a 1 Mohm resistor to drain away the charge if the wire touches a charged object. Instead of using this safety device if you wrap a simple wire around your wrist, you might get electrocuted. An ESD strap protects against low voltage. However, if you wear an antistatic wrist strap when there is a chance of encountering high voltage, the strap allows the voltage to channel through your body.

Figure 2-18 ESD Wrist Strap



- Antistatic bags—Collect static charges on their outer side. Use these bags when storing or shipping equipment because they keep the stray dust charges away from the equipment. The antistatic bags use the Faraday cage effect to keep the charges only on the external part of the bag, which help to protect the electronic equipment that is stored inside.
- ESD static mats—Consists of an insulated material and two wires with clips on each end of the wire. Spread the mat on a flat surface near the ground, and attach one of the clips to the ground. This transfers the charge from the electronic equipment placed on the mat to the ground.

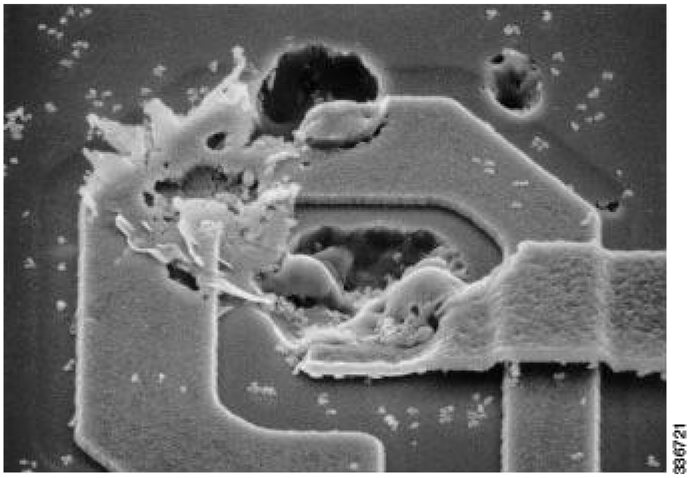
Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

- Always use an ESD wrist strap to prevent the damage from ESD between your body and sensitive electronic components during the installation of electronic devices.

Note Most Cisco data networking equipment are shipped with a disposable wrist strap that is included in the package. Unfortunately, many people think that the static charges that are accumulated on their bodies get discharged when they physically come in contact with any of the electronic components. However, this is incorrect, because air is conductive due to the presence of ions. Therefore, ESD damage can occur when you come in contact with electronic components that are located less than 12 inches (about 30 cm) away from the body. So, it is important to wear a wrist strap during the initial preparation and installation of the equipment.

Figure 2-19 Failed Component due to ESD Damage



- Ensure that the wrist strap is properly connected to the equipment. Most Cisco equipment has an appropriate hole to plug the wrist strap into and ensure good connectivity to the device and ultimately the ground. In case of limitations such as the length of the wrist strap preventing the connection to the proper connecting point on the device, ensure that the wrist strap is connected to an unpainted surface or a ground wiring that mounts on the device or rack. Avoid connecting the wrist strap to painted surfaces.

Figure 2-20 Permanent (metallic) Wrist Strap Connected to the Bond Point of Cisco Equipment

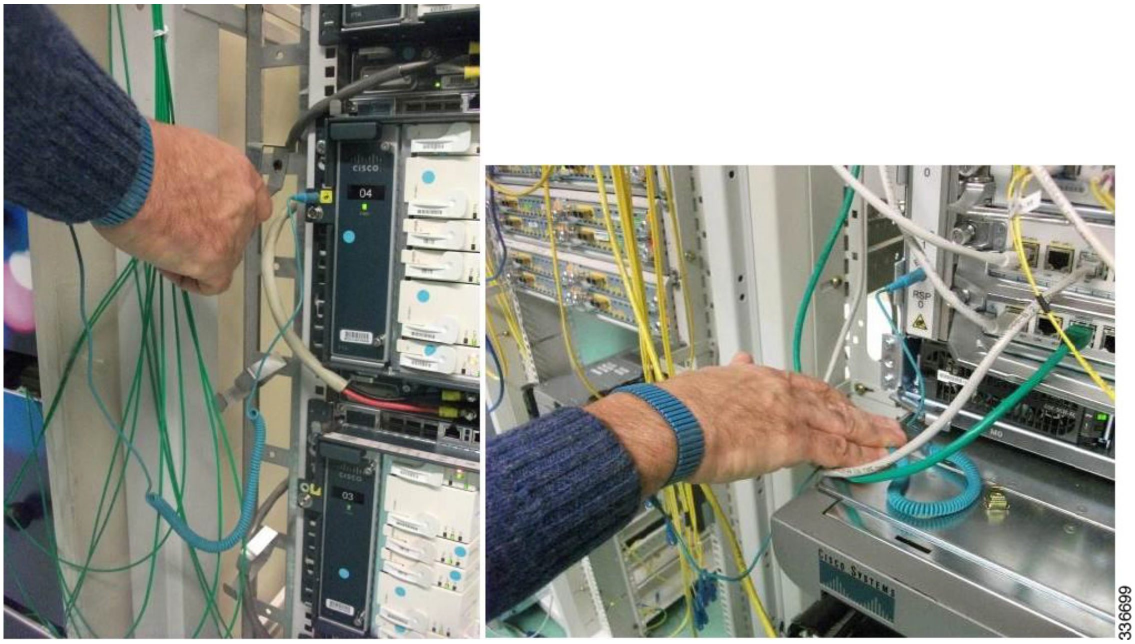


Figure 2-21 Temporary Wrist Strap Connected to a Non-conductive Part of the Rack

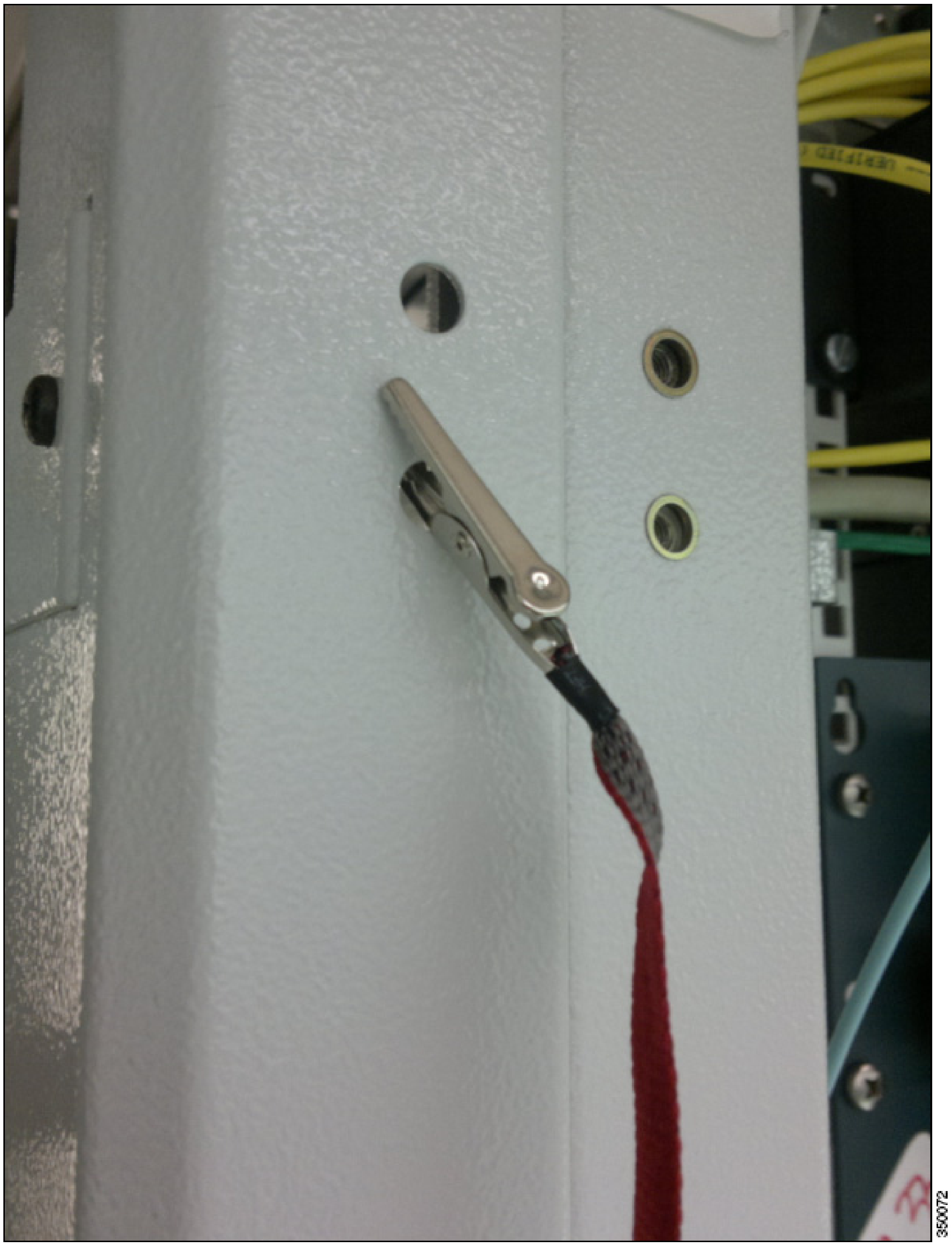
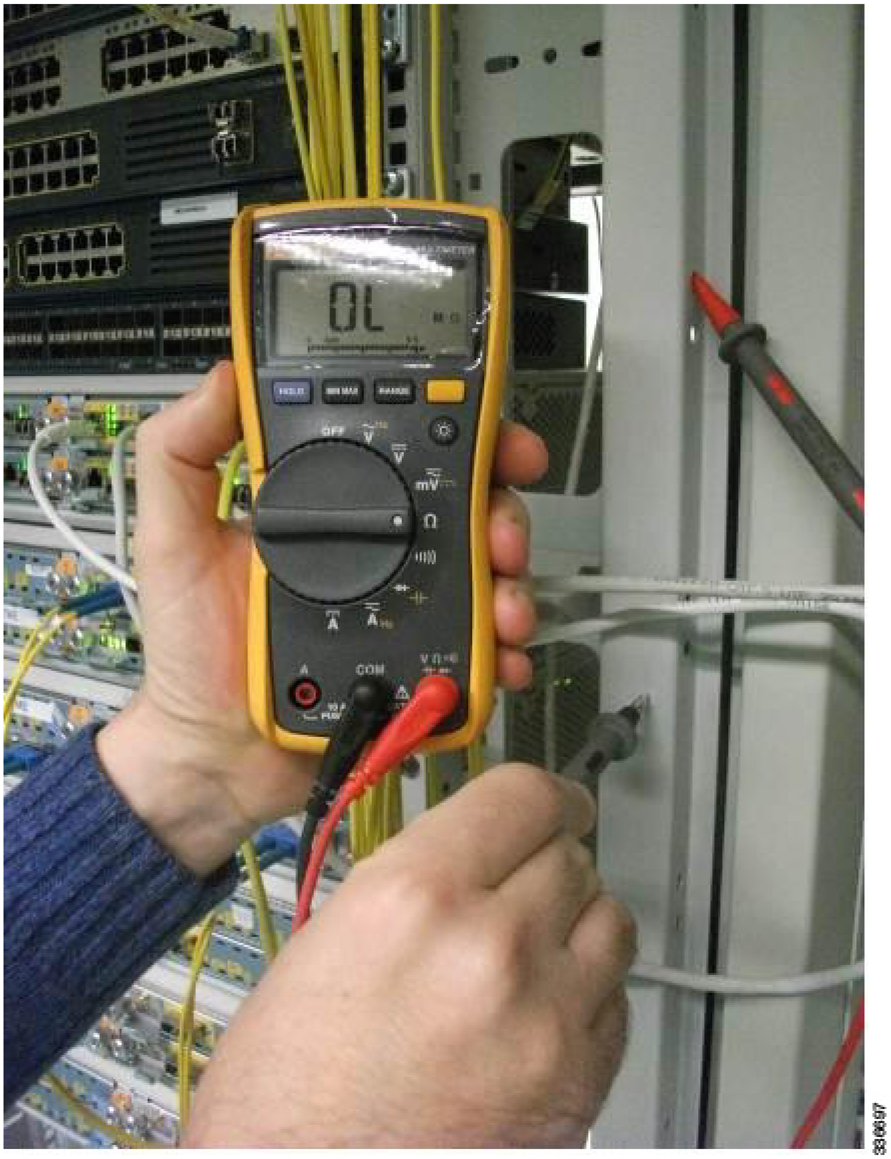
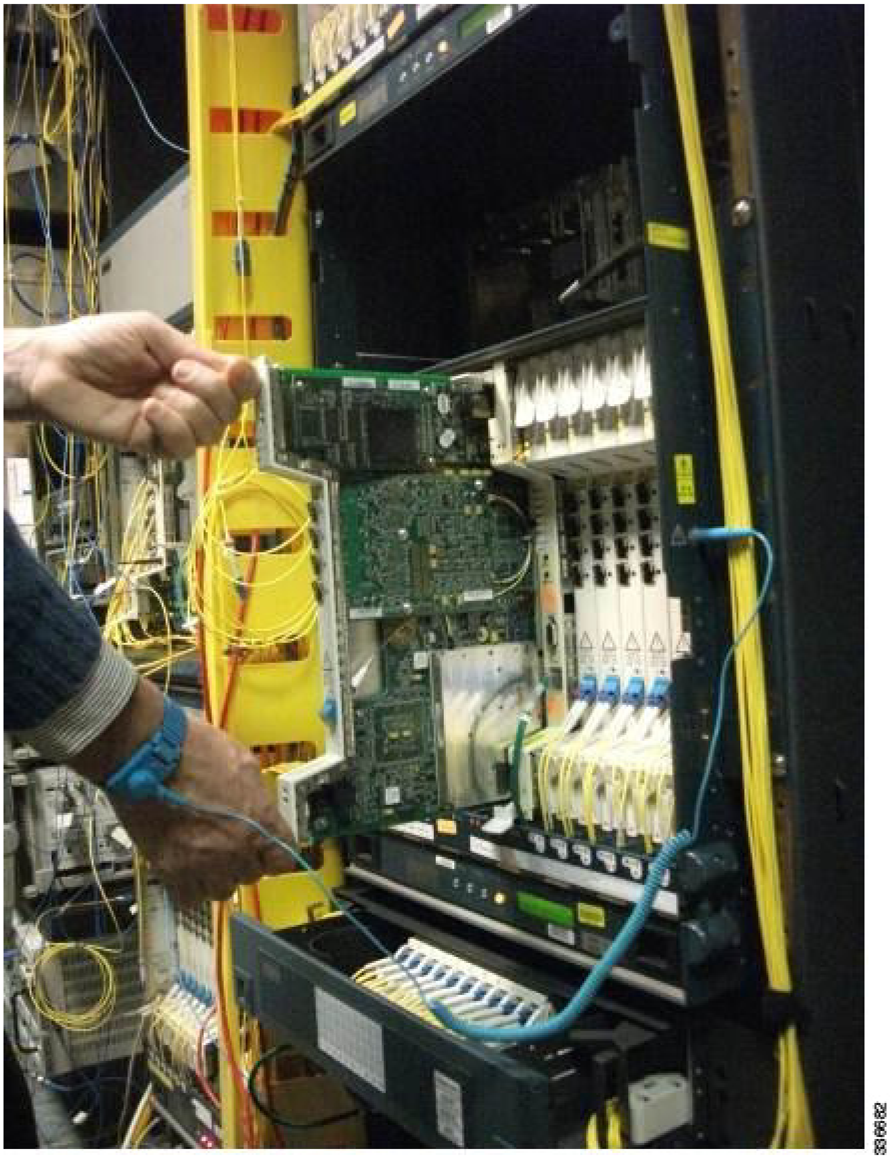


Figure 2-22 Non-conductive Paint on a Rack



- During the installation or removal, handle the electronic equipment, particularly the boards only, using the available handles or edges. Even if you are using an ESD wrist strap, it is important to avoid touching the electronic components to prevent mechanical damage or depositing oil that is present on your hands.

Figure 2-23 How to Handle Cards during Installation

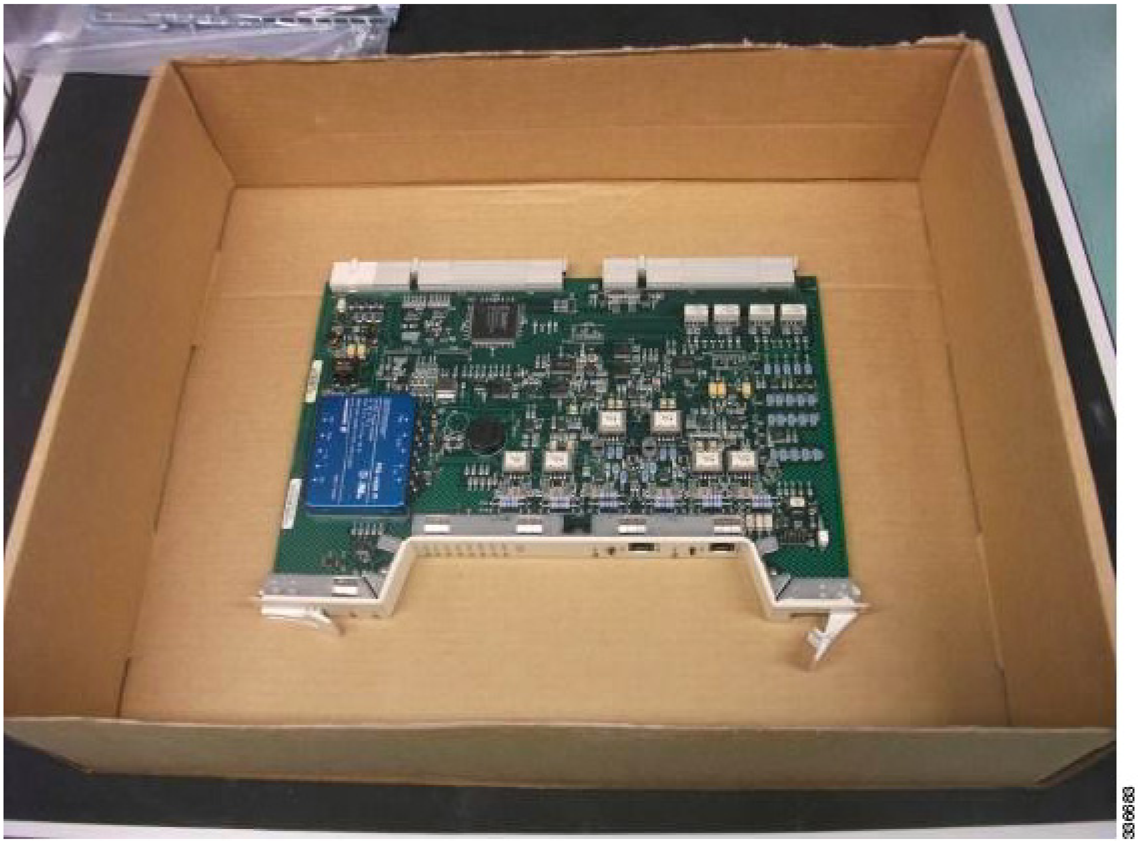


- When replacing a failed card, place it side up on an antistatic surface (ESD mat) or in a static-shielding bag.

Note Based on a customer or partner request, Cisco may perform a failure analysis of the returned equipment from the field. If the equipment becomes further damaged during transportation because of inappropriate or missing packaging, the results of the failure analysis can be misleading.

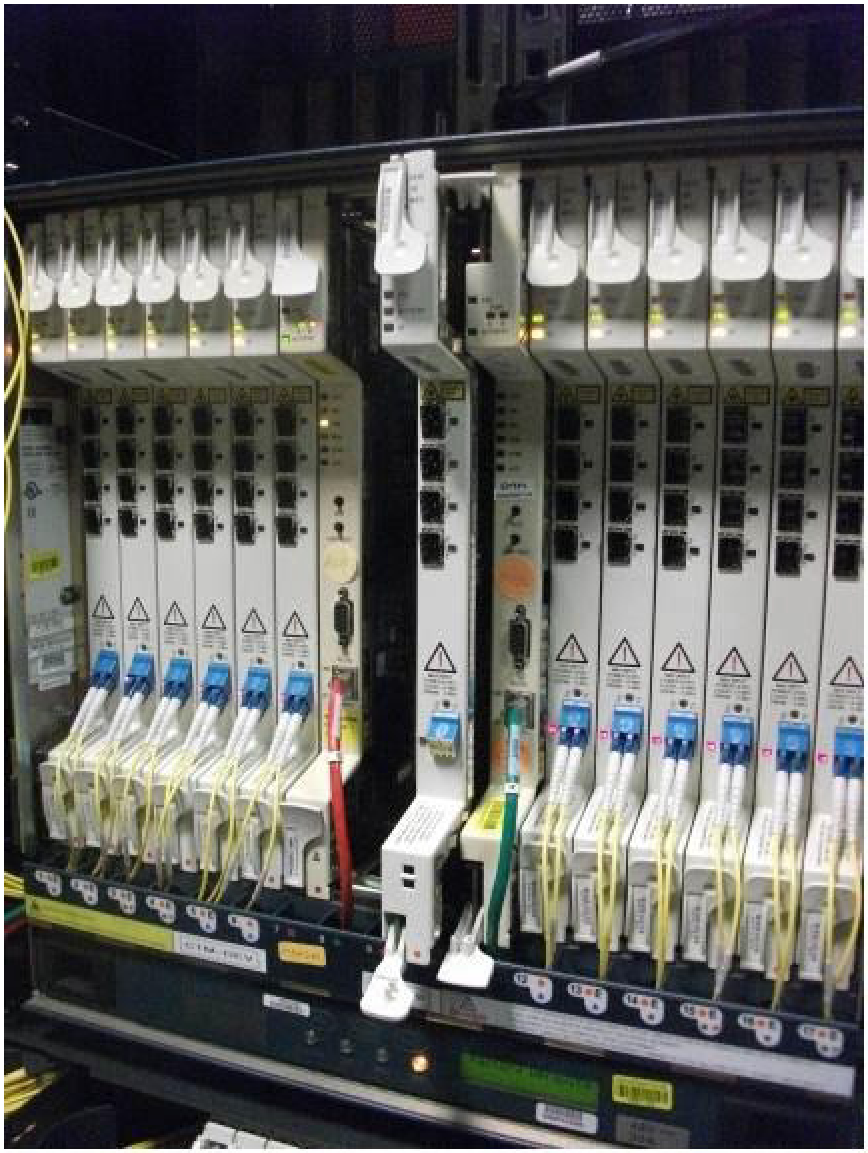
Note Cisco tries to repair most of the failed equipment that is returned from the field, so inappropriate handling or transportation can make the equipment unrepairable.

Figure 2-24 Failed Card Returned to Cisco in Inappropriate Packaging (without ESD-protective bag or foam to prevent mechanical damage during transportation)



- Insert the card into the chassis completely until you can tighten the captive screws and/or levers to ensure a good connection between the backplane of the chassis and card. This is necessary for proper grounding and ESD protection of the cards.

Figure 2-25 Card not Properly Inserted in the Chassis



Guidelines

The following guidelines are recommended to prevent ESD damage:

- Test the following to ensure that the equipment is ESD protected during installation:
  - Powered tools—Provide a conductive path to the ground from the working part of AC-powered tools. For powered hand tools, such as soldering irons, ensure that the tip-to-ground resistance is less than 1 ohm.

Note Ground resistance increases with use; however, maintain its value to less than 20 ohms.

  - Automated Handlers—Ensure the following when using the automated handlers:

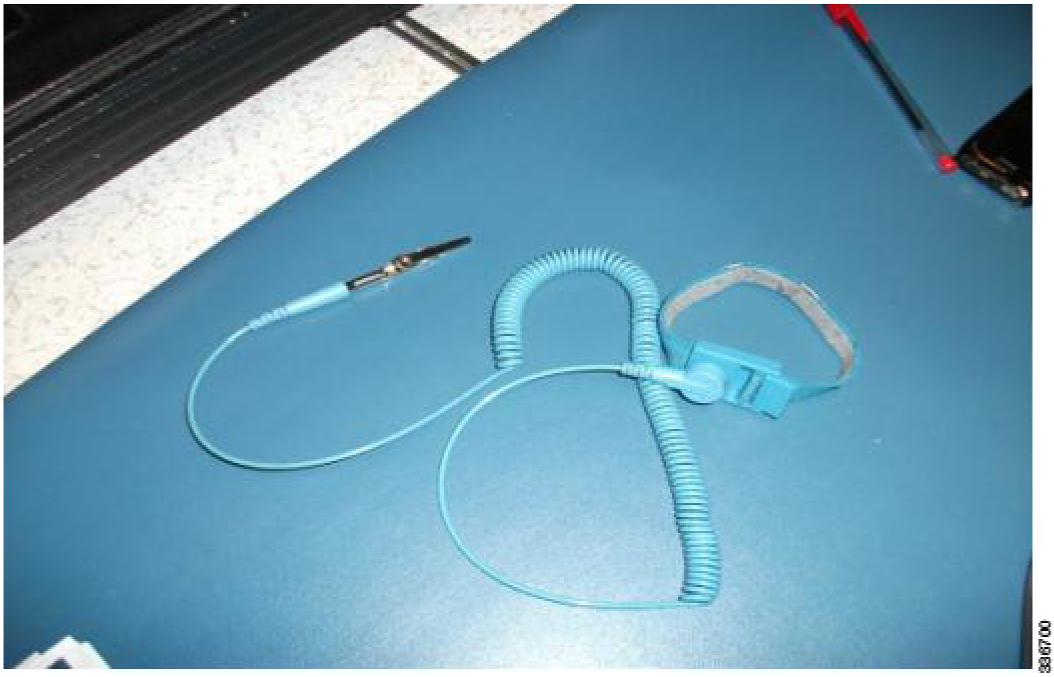
- Establish a continuous and conductive path to the ground in all the conductive or static dissipative components of automated handling equipment whether they are static or in motion.
- Ensure that the automated handling equipment minimizes the charge generation of the ESD items.

Best Practices

The following best practices are recommended to prevent ESD damage:

- Use permanent or metallic wrist straps instead of the disposable ones as metallic wrist straps have better connectivity to the skin of the operator, and are less prone to failure when compared to the disposable wrist straps, which are made of inexpensive and not very resistant material.

Figure 2-26 Permanent (not disposable) Wrist Strap



- In all the installation sites that have conductive floors (tested according to the ANSI 20.20 standard), encourage wearing ESD shoes that have metallic elements, so that the static electricity gets discharged when the shoes come in contact with the ESD flooring. However, we recommend that with ESD shoes, users should also wear a wrist strap when handling sensitive components. This is essential for users working at a bench where they can rest their feet on a table bar and loose contact with the floor. Facilities with ESD flooring should test the flooring periodically to ensure that it maintains conductivity. However, be cautious during floor maintenance as the floor waxes can reduce conductivity and create a level of insulation that prevents the effective dissipation of electrostatic current. When implementing ESD flooring and ESD shoes, the facility should also have an ESD testing station to permit users to test their shoes to ensure that they maintain good conductivity throughout the lifetime of the shoes.
- Avoid wearing synthetic clothes because they conduct an electrical charge.
- Avoid wearing jewelry because metals are good conductors of electricity.

- Use an ESD mat (see Figure 2-27) that is grounded to the rack when performing a card swap. In fact, if it is not possible to immediately store the replaced or damaged cards in an anti-static bag, the ESD mat offers a surface to temporarily keep the electronic equipment and prevent ESD damage. Figure 2-28 outlines how to ground the mat to the same potential as the chassis and the rack.

Figure 2-27 ESD Mat

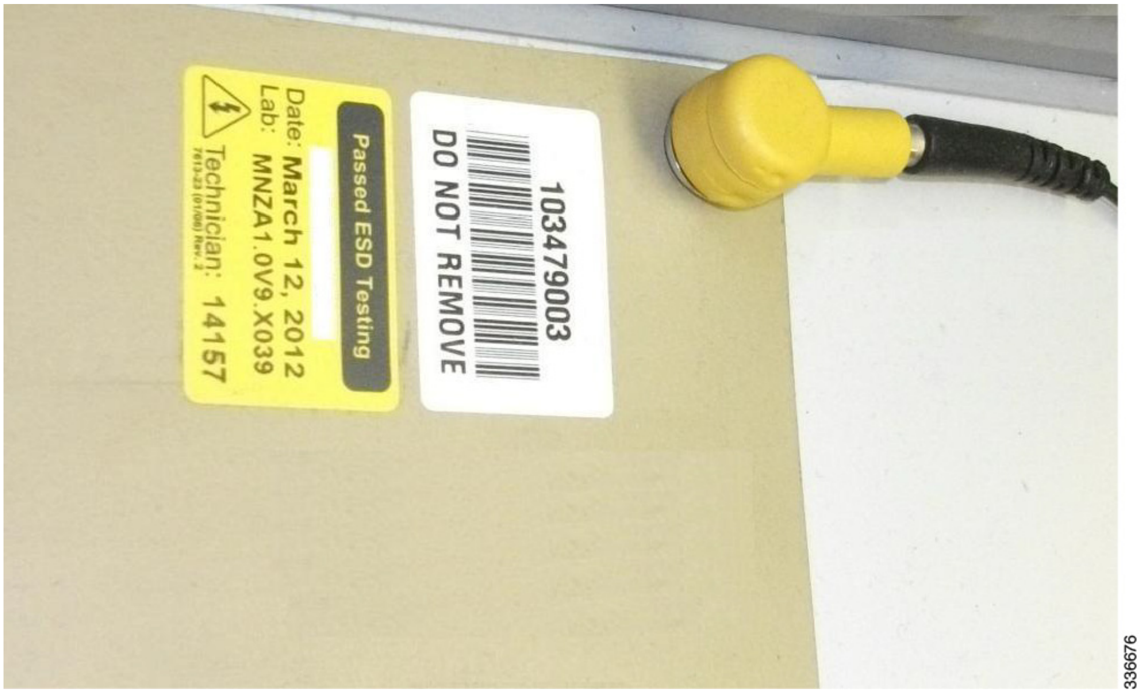
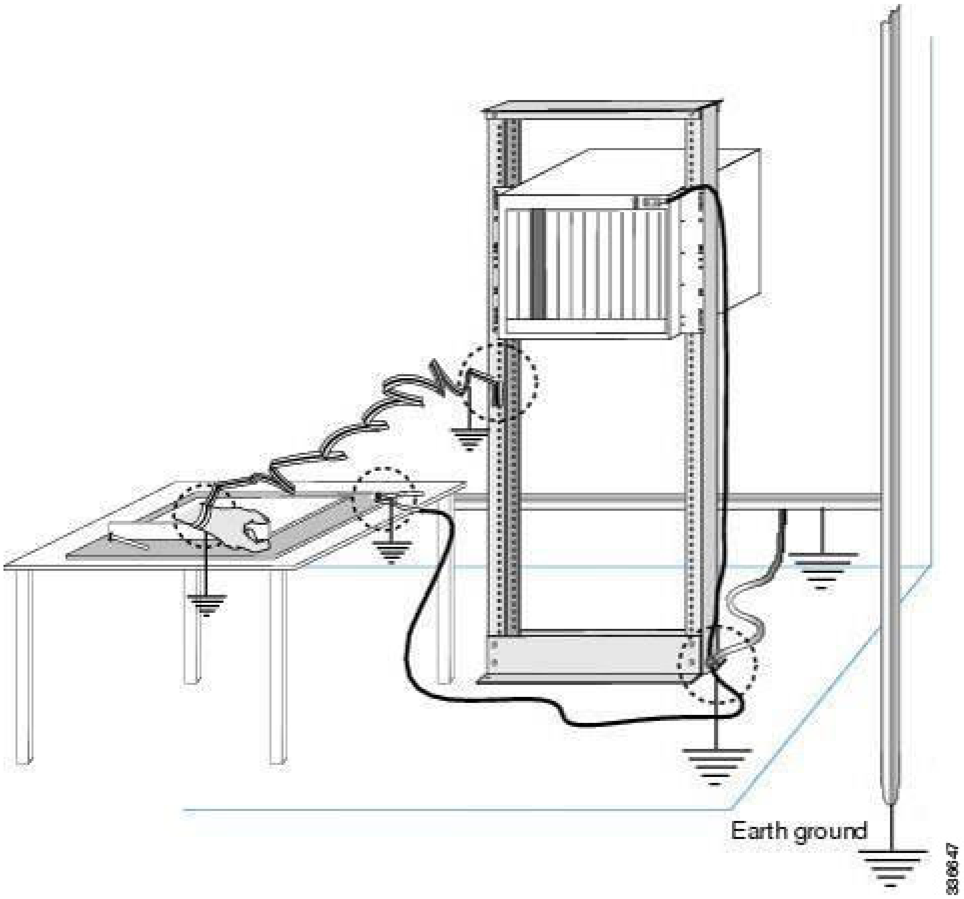


Figure 2-28 Preventing ESD Damage during Card Installation and Replacement



- Each time before using the wrist strap (permanent or disposable), test it using a multimeter to ensure that the resistance is less than 1 Mohm. This should be performed in addition to the periodic test of the ESD protective devices in accordance to the maintenance program of the customer or partner.
- If the installation site has ESD-protected areas, perform the following:
  - Post appropriate signage indicating the ESD-protected area, so that it is clearly visible to people entering the area.
  - Allow only those who have completed the appropriate ESD training into the protected areas. The content of the training material should follow the ANSI 20.20 certification standard.
  - Ionize or use other charge-mitigating techniques in the workstations to neutralize the electrostatic field if it is a threat.

Figure 2-29 Typical ESD Protected Area

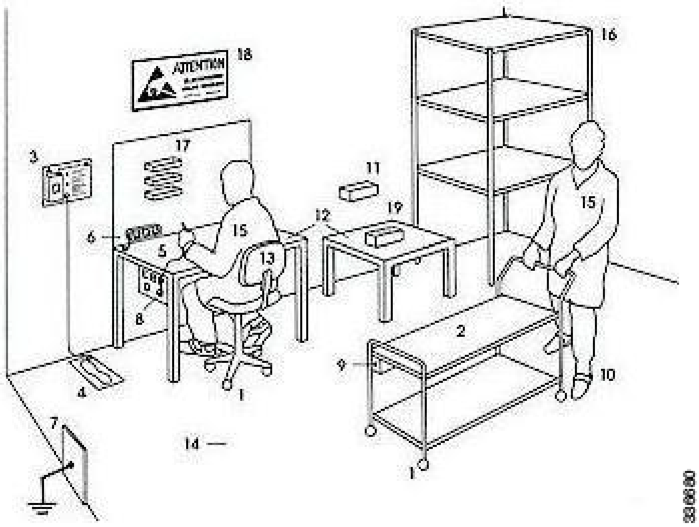


Table 2-1 describes each of the points in Figure 2-29.

Table 2-1 Numbers and Descriptions

Number	Description
1	Groundable wheels
2	Groundable surface
3	Wrist band and footwear tester
4	Footwear footplate
5	Wrist band and grounding cord
6	Grounding cord
7	Ground
8	Earth Bounding Point (EBP)
9	Groundable point of trolley
10	Toe and heel strap (footwear)
11	Ionizer
12	Dissipative surfaces
13	Seating with groundable feet and pads
14	Floor
15	Garments
16	Shelving with grounded surfaces
17	Groundable racking
18	ESD Protective Area (EPA) sign
19	Machine

Airflow

Introduction

Proper airflow through the data networking equipment helps maintain effective operating temperatures and prevents the premature end of life of the equipment. Improper airflow due to no or limited space between the chassis air vents and the adjacent walls leads to equipment overheating. The usage of incorrect cabinets prevents proper airflow and ventilation. Telecom racks are a good choice in applications that require maximum cooling, or immediate access to the front, back, and sides of the equipment as no doors or side covers are used. However, the telecom racks are not recommended in environments, such as banks or installation sites that are shared with other entities, where security issues or concerns need to be considered.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

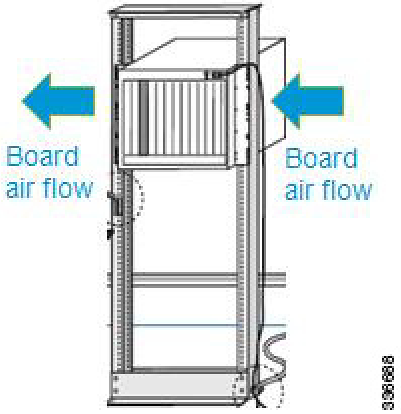
- Maintain a minimum air space of 6 inches between the chassis air vents and the adjacent walls. (Figure 2-1 depicts an example of how cabling can obstruct the air grids.)
- Maintain a minimum horizontal separation of 12 inches (about 30 cm) between the two chassis.

Best Practices

Figure 2-30 depicts the air flow in and out of a chassis. The air flow can be from front to back or right to left or vice versa, or up to down or vice versa, depending on the model of the Cisco data networking equipment. Apart from this, Figure 2-30 also shows the benefits of the usage of a telecom rack for better airflow. Specifically, to reduce the operating temperature and humidity, consider removing the closed cabinet, unless it is required for security reasons, such as if third-party properties are also present.

The use of a fully closed cabinet (no perforations in the doors) is a good idea only when pumping fresh air directly into the cabinet, and not in the room as a whole. These cabinets typically have vents at the top to facilitate the exhaust. For these closed cabinets, pay special attention to maintain the minimum clearance (usually 6 inches) between the equipment and side or back walls.

Figure 2-30 Airflow In and Out of a Cisco Catalyst 6500 Chassis



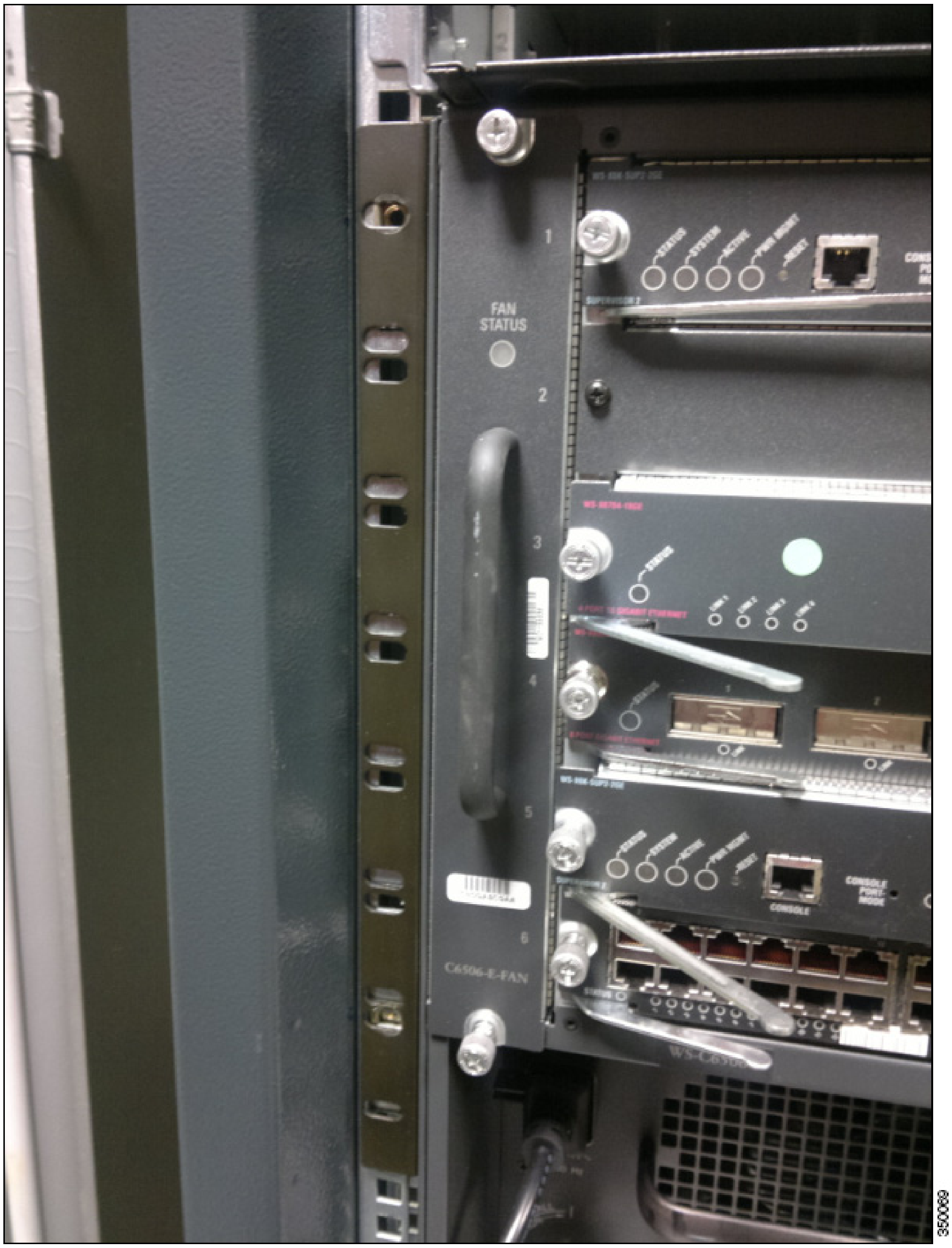
Mechanical Assembly

- Frequently Missed Requirements, page 2-32
- Best Practices, page 2-33

Frequently Missed Requirements

Missing or loose screws during the installation of data networking equipment (as shown in Figure 2-31) can lead to safety issues (for example, accidentally dropping the card on the floor and hitting the operator) or the malfunctioning of the card due to bad connectivity with the chassis.

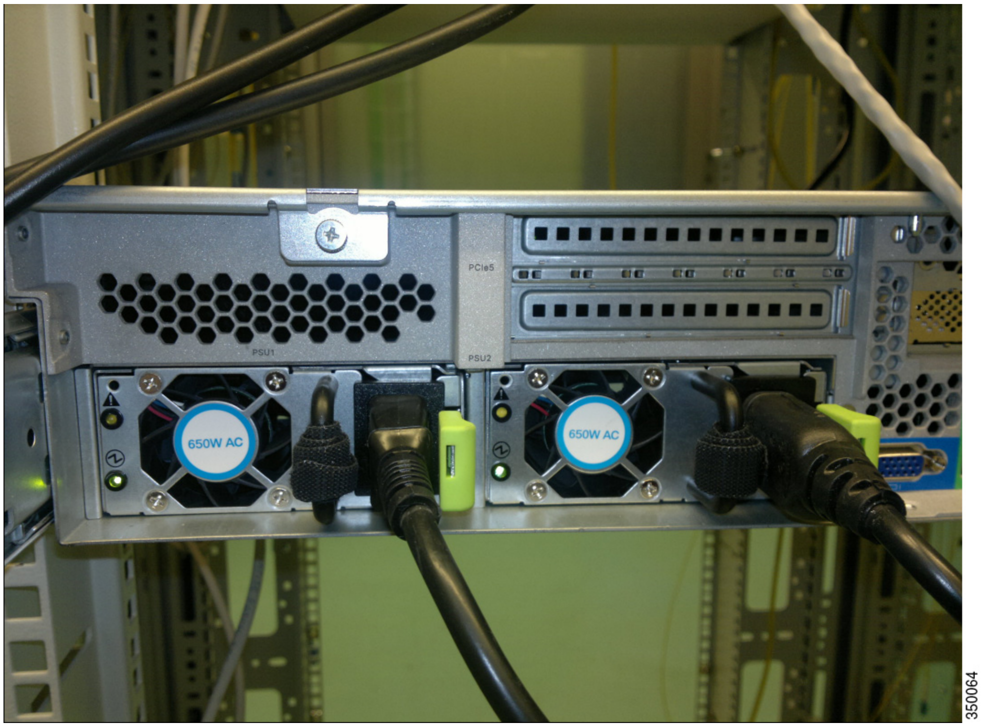
Figure 2-31 Missing Screws when Connecting Cisco Data Networking Equipment to the Rack



Best Practices

When the Cisco data networking equipment uses two or more power supplies (as shown in Figure 2-32), the equipment managers should connect them to two different power circuits, so that if one of them fails, the device continues to operate properly.

Figure 2-32 Equipment Powered by Two Separate Power Supplies (one redundant)



Faceplates

Introduction

To ensure the proper functioning of the data networking equipment, it is essential to protect unused slots using blank faceplates. They prevent the following:

- Entry of dust into the chassis.
- Abnormal board temperature.
- Electro-magnetic interferences (EMI) phenomena.

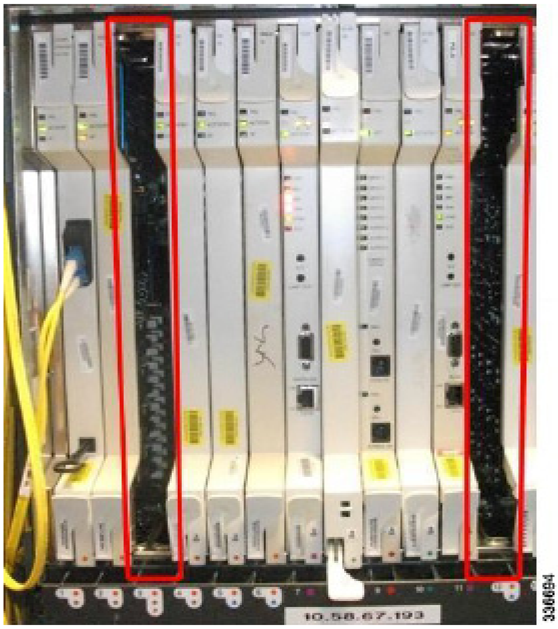
Frequently Missed Requirements

Typically, blank faceplates are provided with a new chassis. So, it is important to ensure that they are properly stored, so that they can be used when changing an installation configuration or making an installed card redundant.

If blank faceplates are not available, you can order them as spare parts. For more information, see the installation guides that support the specific Cisco data networking equipment.

Figure 2-33 outlines an example of an installation with missing blank faceplates. Noncompliance with this requirement can have a major impact on the reliability of electronic equipment.

Figure 2-33 Missing Blank Faceplates



Optical Connectors and Ports

Introduction

When optical connectors and ports are not protected using the appropriate protective caps, it leads to the following:

- Improper functioning of the ports.
- Board failures due to the presence of dust on the boards.
- Poor cable connectivity due to dust in the port.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

- Figure 2-34 shows unused optical connectors without protective caps. This leads to accumulation of dust on the optical fibres that can result in transmission errors and damage to the connectors. Additionally, the optical connectors shown in Figure 2-34 are seen lying on the floor, which can cause them to get accidentally trampled by operators.

- Use protective caps on unplugged optical ports to prevent dust from contaminating them. Missing this can cause them to get accidentally damaged. Figure 2-35 shows an example of unused optical ports without protective caps.

Figure 2-34 Unused Optical Connectors Without Protective Caps

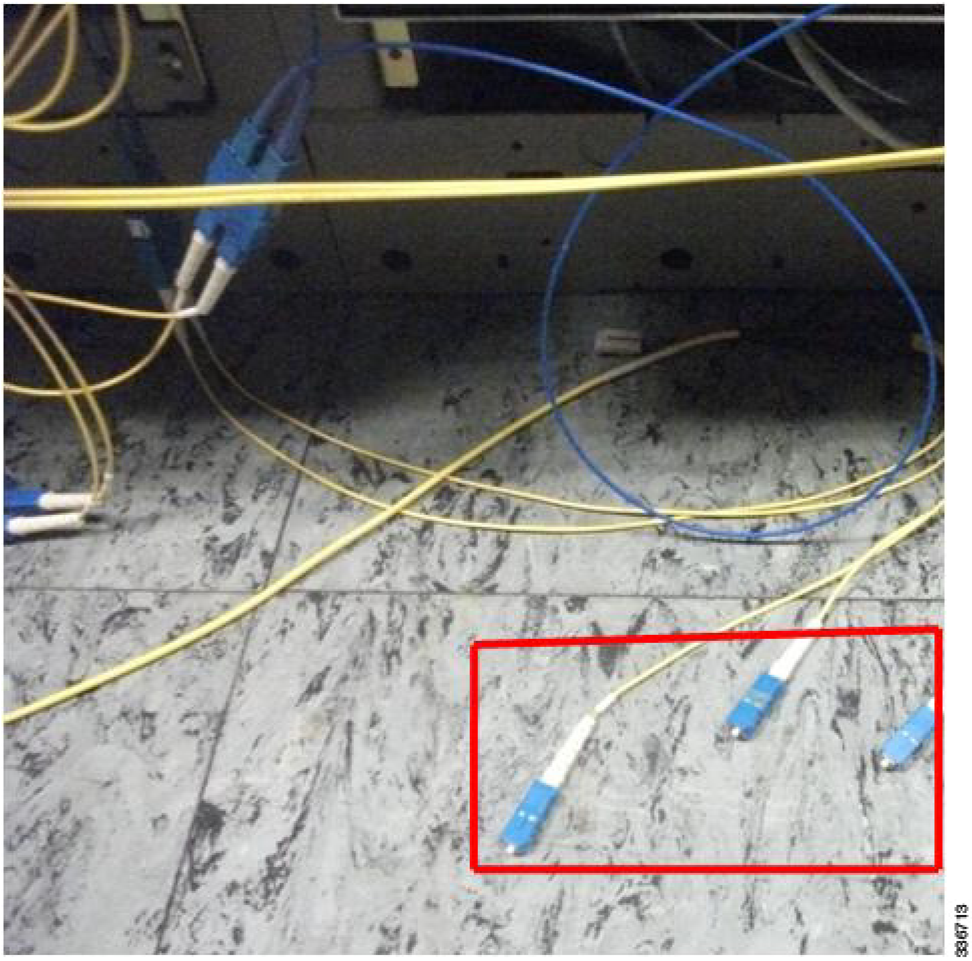


Figure 2-35 Unused Optical Ports Without Protective Caps

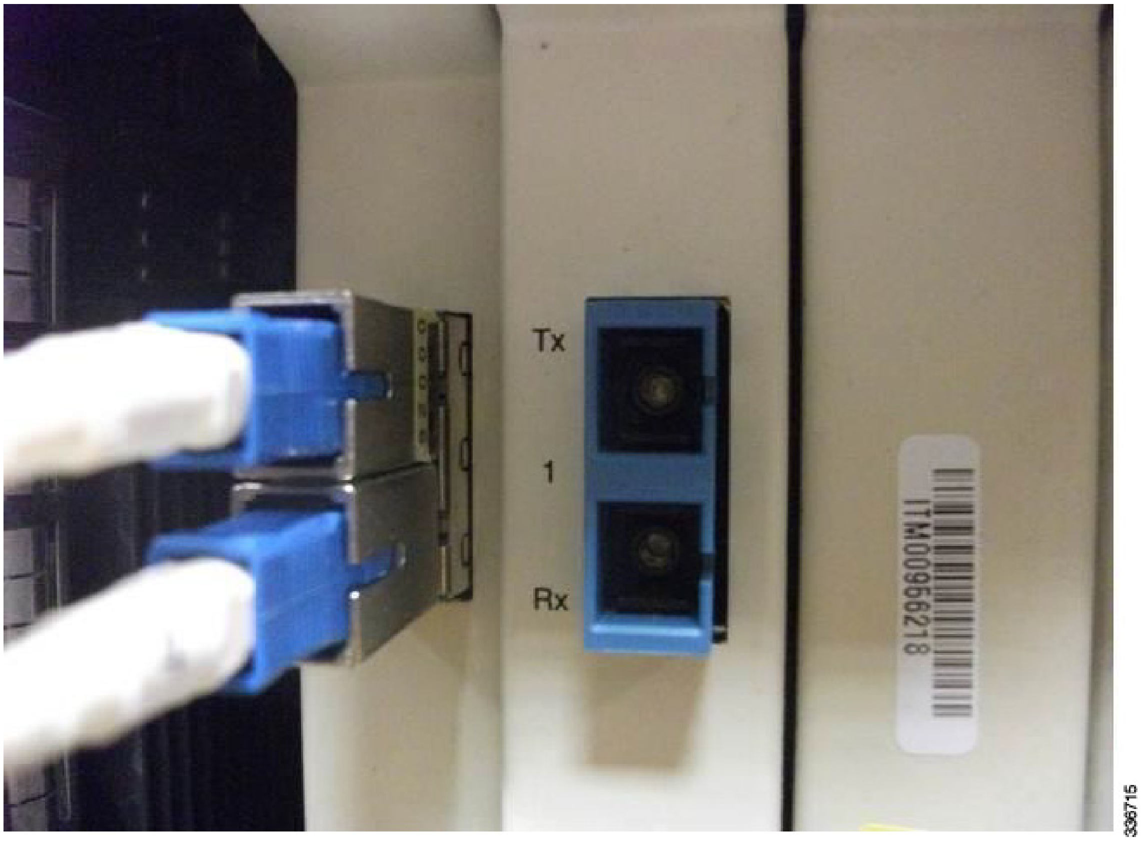
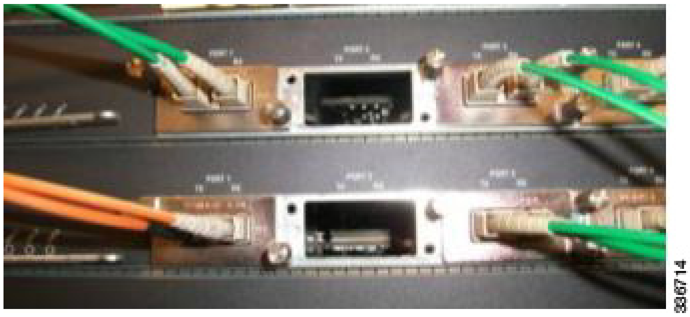


Figure 2-36 Another Example of Unused Optical Ports Without Protective Caps



Surge Protection

Introduction

Power problems can be traced to various sources. The most dramatic ones are natural disasters as they completely knock out the power supply by severing the utility lines. The less dramatic sources include overburdened circuits, the introduction of unseen threats, such as surges, brownouts, and line noise. Therefore, every unprotected line that enters the equipment, whether it carries data or power, represents a potential conduit for power problems.

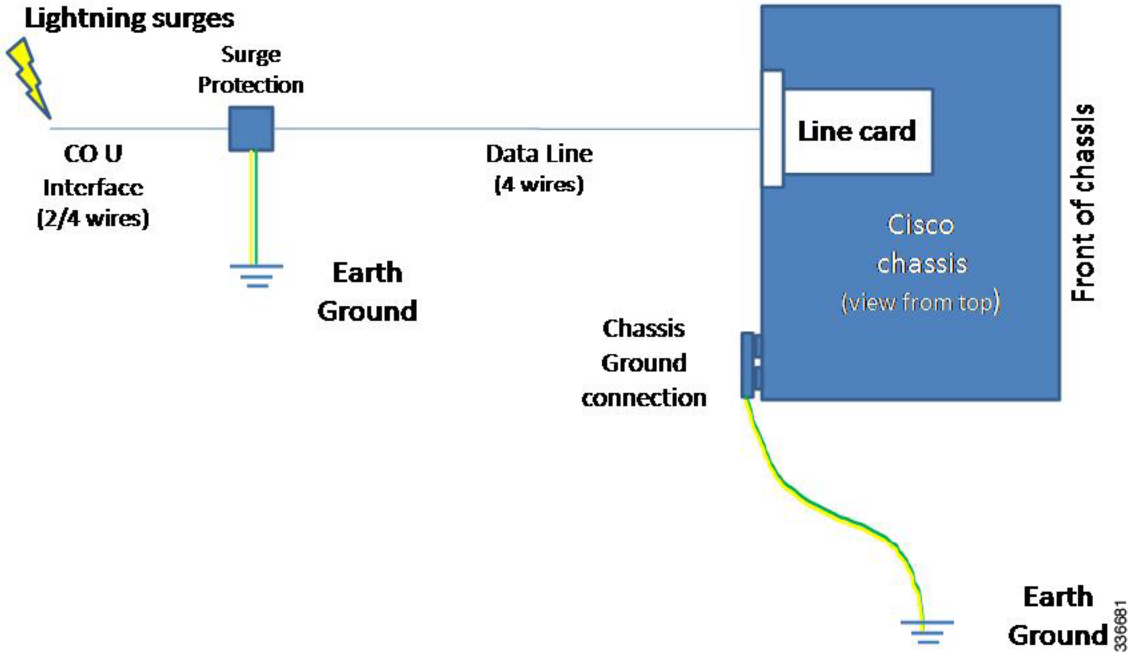
Surges and spikes refer to the short-term voltage increases. They cause data corruption, catastrophic equipment damage, and incremental damage that degrade the performance of the equipment. Surges and spikes occur mostly due to lightning strikes, thunderstorms, ground faults, and sudden power restoration after an outage.

Surge protectors trap the voltage that exceeds certain limits. When spikes occur for a certain duration of time, a trapping device known as a Metal Oxide Varistor (MOV) that is present in the surge protector gets activated. Every surge protector has an MOV, which helps in diverting the surge current. The lifespan of an MOV shortens with use as more surge currents are diverted. They do not display any indication of wear and tear, nor do they provide any forewarning of failure. So, when they suddenly fail, their temperatures increase rapidly and cause fires.

Most surge protectors function as a power strip even after their surge trap mechanism is degraded by power spikes. This can cause the following dangers:

- If another power surge occurs, it damages the equipment that is plugged into this surge protector.
- If sufficient voltage passes through the surge protector during a second power spike, a resistant short is formed that produces heat and can lead to fire.

Figure 2-37 Surge Protection on an ISDN Line Card Installed in a Cisco Chassis



Best Practices

The following best practices are recommended to ensure surge protection of the data networking equipment:

- Use only the surge protectors or power strips that have an internal circuit breaker. These units trip the breaker as soon as the power strip is overloaded to prevent overheating and fire.
- Ensure that all the surge protectors or power strips are UL-approved. Also ensure that the surge protector is listed as a TRANSIENT VOLTAGE SURGE SUPPRESSOR as per the UL 1449 performance standard for surge suppressors.
- Energy absorption or dissipation rating in joules indicates the amount of energy the surge protector can absorb before it fails. A higher number indicates greater protection.
- Surge protectors are not immediately activated; therefore, there is a slight delay in response to the power surge. A longer response time signifies a longer duration of time that the equipment is exposed to the power surge. So, a surge protector that responds in less than one nanosecond is ideal.
- Unplug the cord from the power source when the surge protector or power strip is not in use.

Temperature and Humidity

Introduction

The optimal temperature and RH levels are best controlled by installing air conditioners in the installation site.

It is important to maintain the RH level in an installation site because when humidity is too low, it can contribute to ESD failures; and when it is too high, it can cause water to condense inside the Cisco data networking equipment, which causes electrical short circuits that trip circuit breakers and damages the equipment. High humidity and condensation also cause rust and corrosion in the equipment, which ultimately leads to their failure.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

- Ensure that thermometers and hygrometers are present in the installation site, so that optimal temperature and humidity levels are maintained for the proper functioning of Cisco data networking equipment. In some installation sites, even though these instruments are present, they allow for only manual readings, and in such scenarios, if the sites are remotely located without any personnel permanently present, the readings are not frequently recorded. Therefore, it is not possible to ensure that the optimal parameters are maintained.

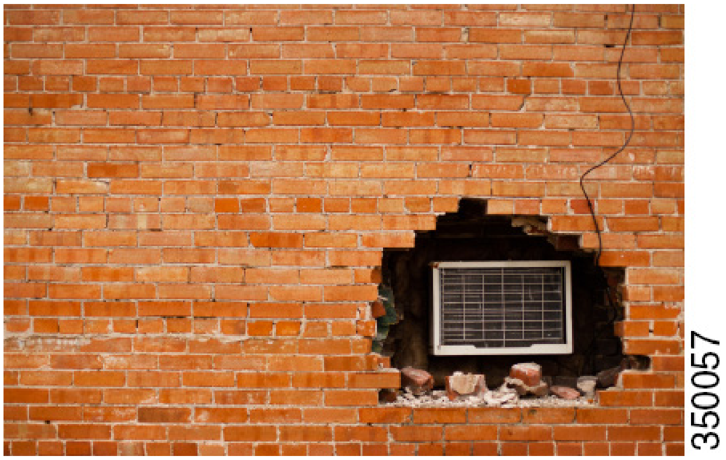
- Ensure that the optimal temperature and humidity levels are also maintained in the storage areas of the installation sites. In addition, see the installation guides that support specific Cisco data networking equipment for the minimum and maximum allowed values for temperature and humidity.

Guidelines

The following guidelines are recommended to monitor the temperature and humidity at optimal levels:

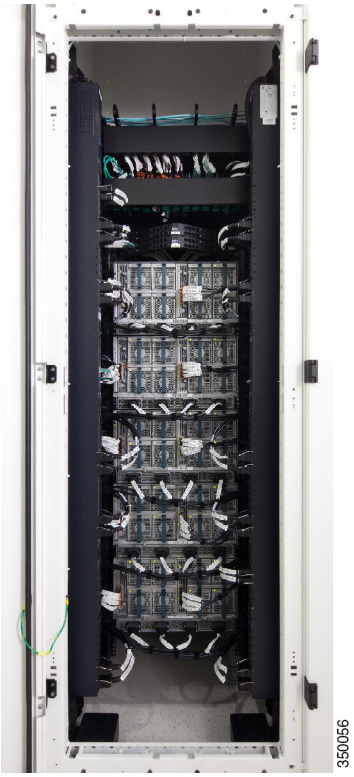
- In installation sites that have an AC system in place, ensure that they do not have openings in the side walls or the main door because these enable the entry of external air, dust, and airborne contaminants, thereby making devices, such as air scrubbers ineffective.

Figure 2-38 Opening on the Side Wall of an Installation Site



- Avoid installing the air conditioning systems in front of or close to the data networking equipment. In case of malfunction or heavy rain and humidity, there is a risk that the device can blow moisture (including airborne contaminants, if present) into the equipment. If this is not feasible, consider diverting the airflow with a deflector or an equivalent device.
- When using closed cabinets, even if the minimum clearance between the equipment and side walls is met, the airflow may not be optimal, which can cause the temperature and humidity to exceed the maximum allowable limits. In such a scenario, remove the cabinet doors and side walls to improve ventilation, assuming that there are no security threats posed because of this.

Figure 2-39 Main Door of a Closed Cabinet Removed to Improve Airflow



- Align all the AC units with hot aisles. By doing so, their cooling efficiency increases as the hot exhaust air directly flows to the return ducts and minimizes the mixing with the cold air streams.
- Ensure that the AC units in occupied areas have appropriate and consistent temperature and relative humidity settings to avoid units working against each other.

Best Practices

The following best practices are recommended to monitor the temperature and humidity at optimal levels:

- Install a device for continuously monitoring environmental factors, such as temperature, humidity, the presence of water on the floor, and so on. Even though these devices are installed in remote installation sites that are not connected in real-time with the headquarters of the customer or partner, they detect if an abnormal condition, such as a thunderstorm increasing the humidity level above the dew condensation point, occurs in the installation site, and investigate if there is a correlation with equipment failure. These devices are extremely useful in sites that are not air conditioned. If the device is connected to the Facility Operation Center of the customer or partner, an alarm is generated when a threshold limit is crossed, and immediate corrective action is taken. Additionally, sensors that are installed on the boards of many types of Cisco data networking equipment measure the temperature and can be remotely monitored through appropriate software applications.
- Maintain a temperature difference of not more than 10ºC between the intake and exhaust air in a product.

- Most Cisco installation guides for data networking equipment specify the minimum distance between two adjacent chassis as 12 inches. However, even when this distance is maintained, a chain effect on the ambient temperature is observed when the air intake of one chassis is supplied by the exhaust air of the adjacent chassis, and so on. Therefore, avoid installing the chassis in a sequential manner to prevent an adverse impact on the ambient temperature and humidity levels.

Figure 2-40 'Chain Effect' leading to the Chassis in Rack 1 Exceeding the Maximum Allowed Temperature

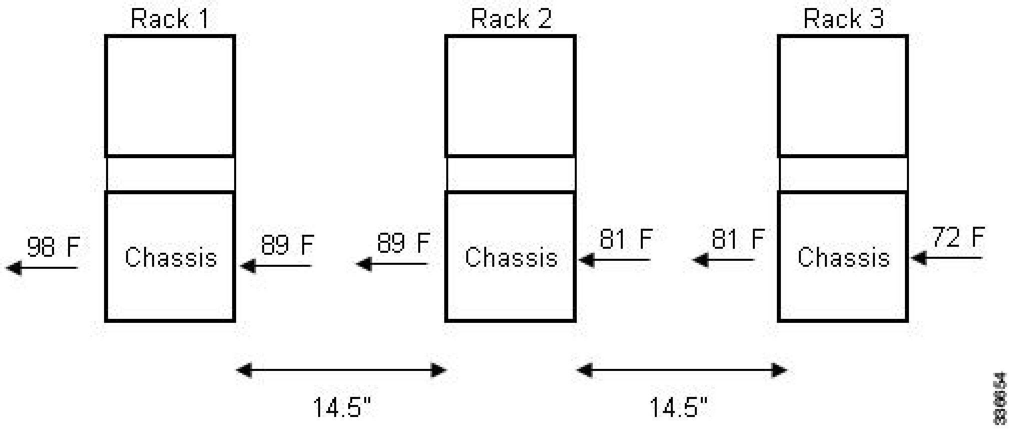
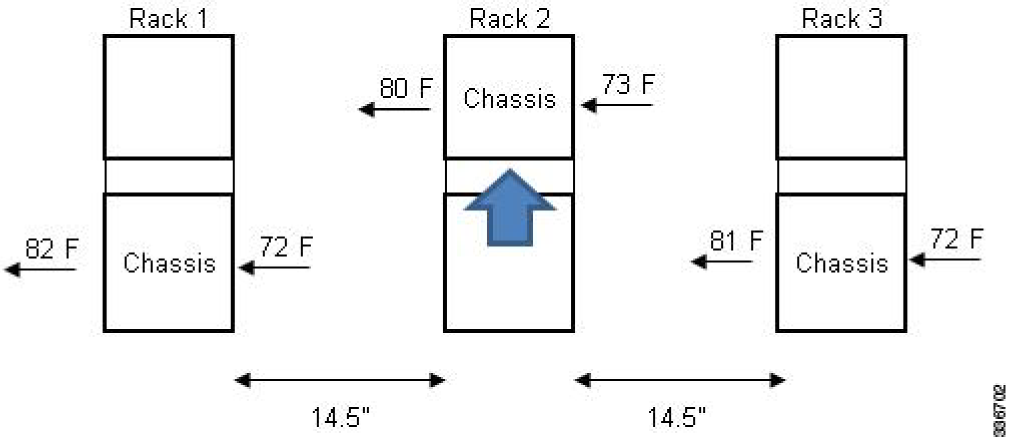


Figure 2-41 Preventing the 'Chain Effect' on Temperature through Correct Installation Practices



CHAPTER 3

Maintenance

This chapter outlines the frequently missed requirements, guidelines, and best practices to follow during the maintenance of data networking equipment and installation sites.

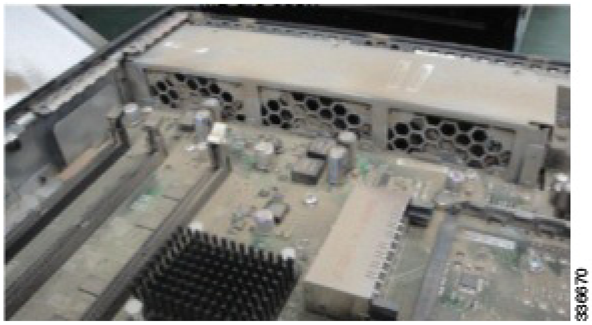
Dust and Particulates

Introduction

Dust is everywhere, but is often invisible to the naked eye. It consists of fine particles in the air that originate from various sources, such as soil dust lifted by weather, volcanic eruptions, and pollution. Dust in an installation site may contain small amounts of textile, paper fibres, and minerals from outdoor soil. It may also include natural contaminants, such as chlorine from the marine environment and industrial contaminants such as sulfur.

Dust may also originate from air conditioning systems, cartons and paper-based materials, clothing and shoes, carpets (if present), and even drop ceiling tiles. Smaller dust particles that have a diameter of one micrometer or less can remain suspended in the air for very long periods of time. Dust and debris are particularly dangerous when ionized and attracted to electronic equipment as shown in Figure 3-1.

Figure 3-1 Dusty Motherboard



The accumulation of dust and debris on electronic equipment has the following adverse effects:

- It increases the working temperature of the equipment that reduces the reliability and working life of the equipment in accordance to the Arrhenius effect, and therefore, the reliability of equipment decreases with an increase in the operating temperature.
- The moisture and corrosive elements that are present in the dust can cause premature board failure due to the corrosion of the electronic or mechanical components.

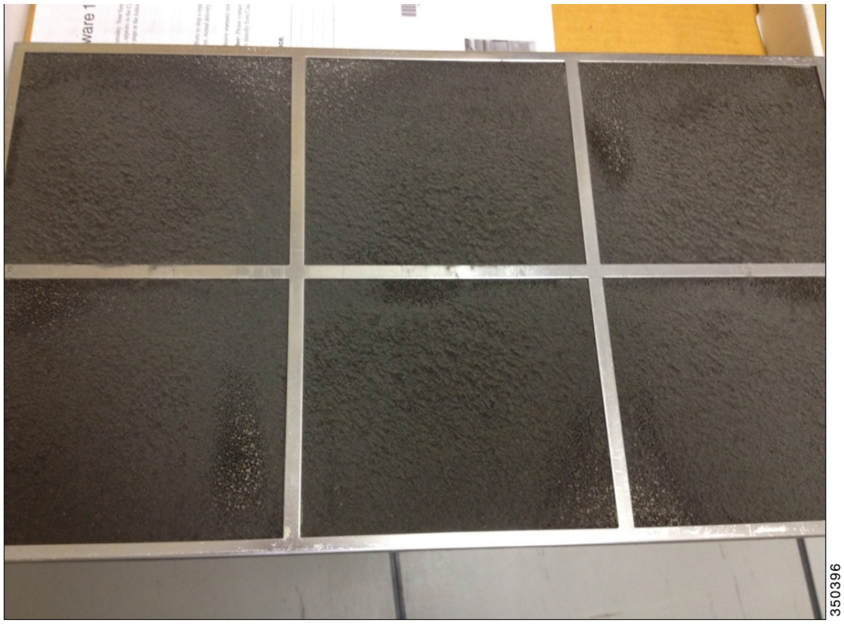
These adverse effects can be accelerated by the presence of fans in the data networking equipment that ingest dust and other particles into the equipment, which causes an accelerated accumulation of contaminants in the equipment. Usually, the higher the volume of air that is generated by the fans for cooling, the higher the quantity of dust and particulates that deposit inside the equipment. So, the best way to prevent this problem is to remove or minimize the presence of dust and particulates in the installation site.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

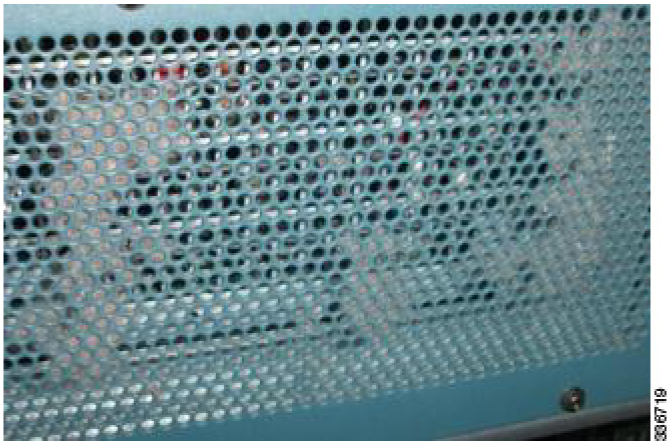
- Periodically check the air filters. If they are dirty or clogged with dust, replace them, because cleaning and reusing them is not permissible as per the requirement for all products that are compliant to the *Network Equipment Building Systems (NEBS) GR-63-CORE* standard.

Figure 3-2 Clogged Filter



- Periodically clean the inlet air grids in low-end platform products, which usually do not have separate air filters.

Figure 3-3 Air Grid of a Data networking Device Clogged with Dust and Particulates



- Apply dust caps on all empty optical ports that are not in use. Cap the optical cable terminations as well. Noncompliance to this requirement can lead to adverse effects such as transmission errors.

Figure 3-4 Unprotected Optical Connectors

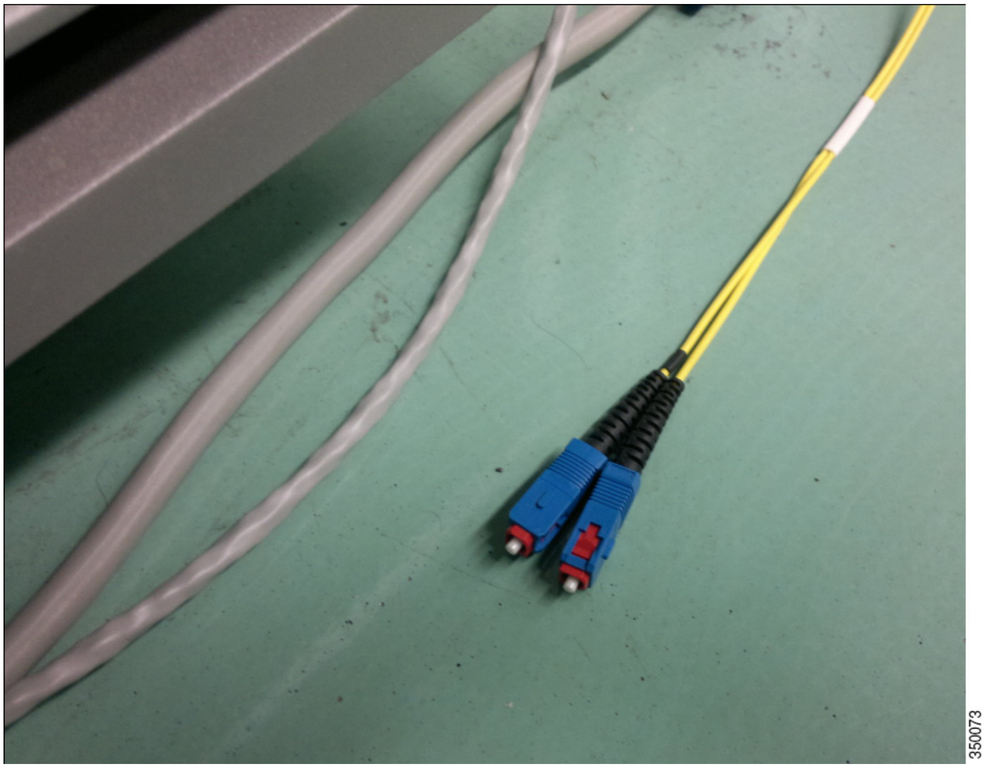
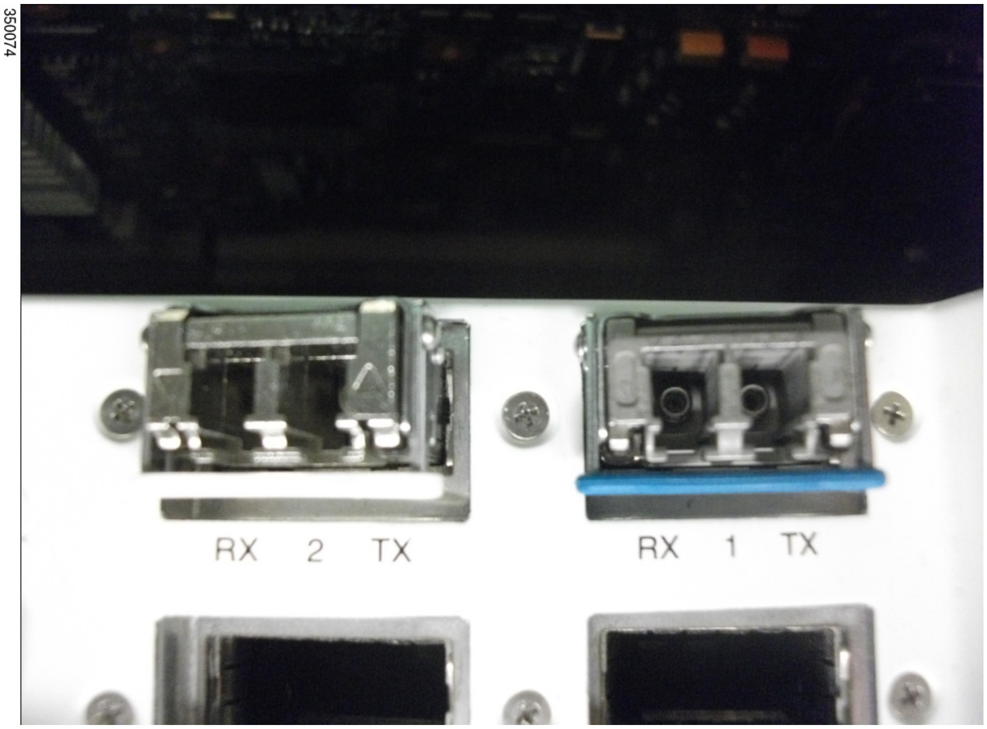


Figure 3-5 Unprotected Optical Ports

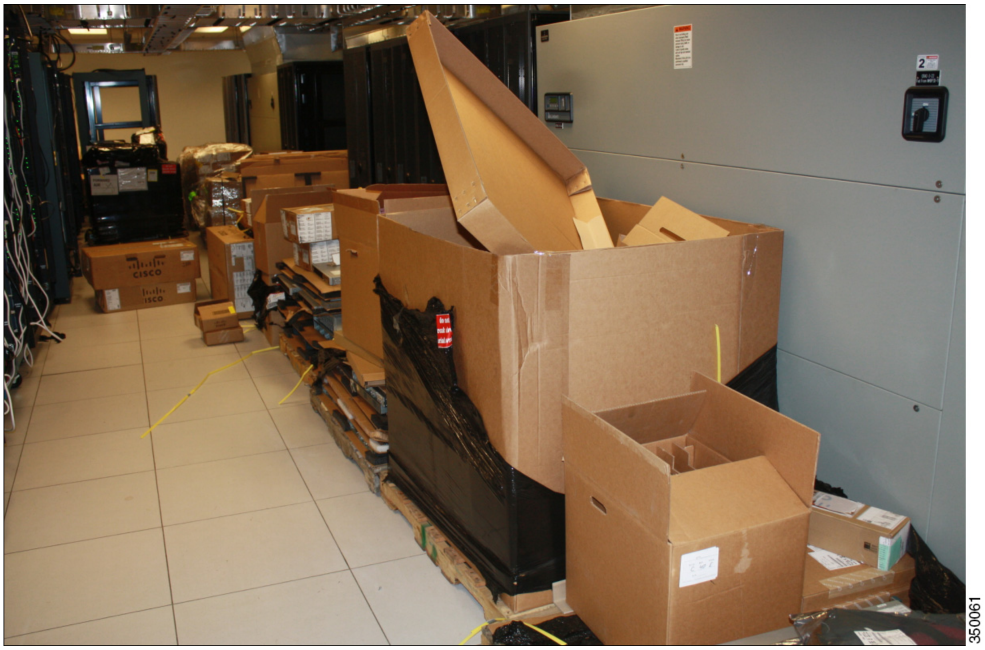


Guidelines

The following guidelines are recommended to prevent dust particulates from accumulating in or around data networking equipment:

- Install an air filtration system to prevent or minimize the presence of dust and particulates in the installation site and in the data networking equipment. There are two main types of mechanisms as follows:
  - At the site level—Proper filtering of the air intake by using air filters. For example, on the air conditioning system.
  - At the card or device level—Installation of filters as recommended by the specific equipment installation guides.
- Periodically check the filters to verify that they are efficiently working as per the instructions included in the operating manuals of the equipment. Also, ensure the following:
  - Do not vacuum an air filter while it is being installed. Before you clean it, completely remove the air filter to prevent contaminants from being drawn into the equipment, and then clean it outside the data center.
  - Never wash a filter and then install it in the system. Moisture can get drawn into the system and attract more dust that can accelerate the effects of corrosion.
- Cartons and packaging material, such as wooden pellets, fiberboard, and so on should not be permitted in the installation site because they present a dust hazard as shown in Figure 3-6, and can become airborne and get carried into the network equipment air intake vents. Dust is especially damaging when impregnated with moisture in damp conditions.

Figure 3-6 Cartons inside an Installation Site



- The Cisco installation guides for optical fibre equipment specify guidelines for cleaning the optical connectors. We recommend cleaning the optical connectors using a CLETOP cassette cleaner (type A for SC connectors or type B for MT-RJ connectors), and follow the product directions. If a CLETOP cassette cleaner is not available, perform the following steps:
  1. Use a lint-free tissue that is soaked in 99 percent pure isopropyl alcohol to gently wipe the faceplate.
  2. Wait for five seconds for the surfaces to dry and repeat, if necessary.
  3. Remove any residual dust from the faceplate with clean, dry, oil-free compressed air.
  4. Use a magnifying glass or an inspection microscope to inspect the ferrule at an angle. Do not look directly into the aperture. Repeat the process if any contamination is detected.
- Establish a program that includes the following for regular cleaning:
  - Clean the spaces under the raised or access floor periodically. Dirt, dust, and debris, which collect in and are blown through raised-floor cavities, will eventually make their way into the air filters. Under-floor dirt can cause unexpected electrical shorts, data transmission problems, and even fires.
  - Minimize dust dispersion during housekeeping by placing dust bins outside the installation site to avoid further dust displacement.
  - Clean the equipment at regular intervals as the dust can cause the equipment to retain heat and potentially cause unwanted downtime.
- Adopt good housekeeping procedures.
- Ensure that the cleaning frequency is consistent with the rate at which contaminants are introduced. For example, in a very dusty environment, increase the cleaning frequency to ensure that the filters efficiently operate.
- Use approved vacuum cleaners in environments that are prone to combustible dust. For example, in a polypropylene factory, an aluminum mine, and so on.

Figure 3-7 Dust-Free Chassis in an Installation Site where Regular Cleaning is Performed

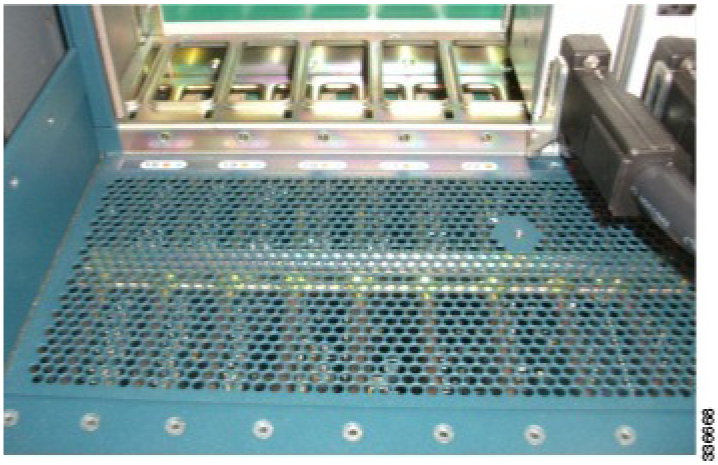
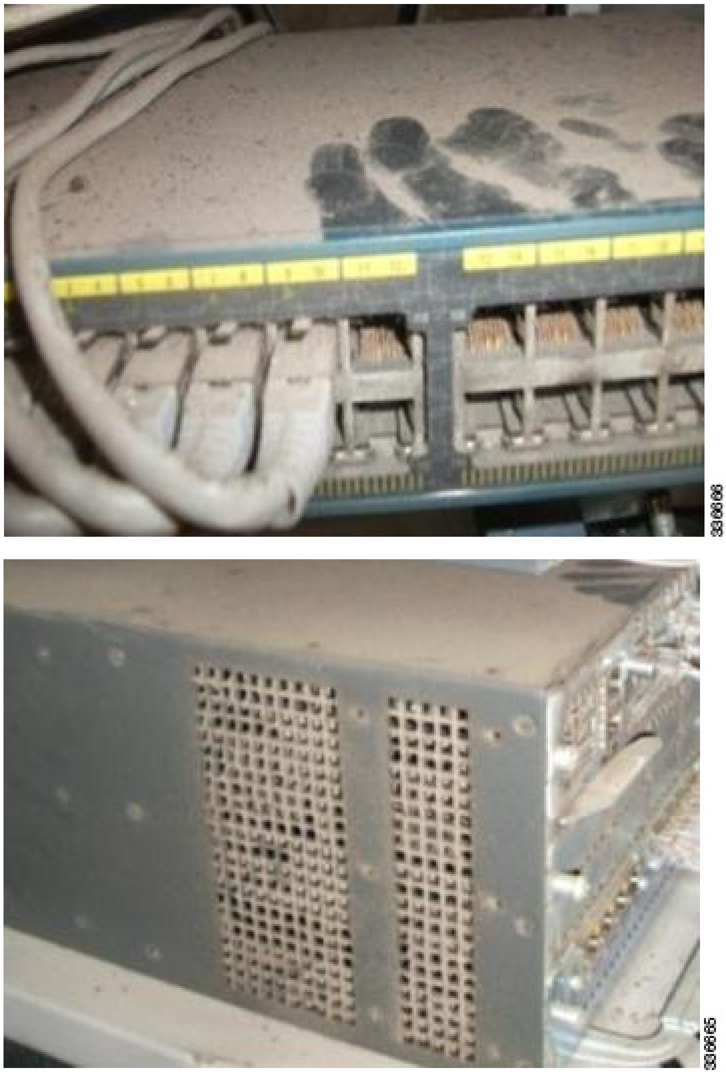


Figure 3-8 Data Networking Equipment on which Regular Cleaning is NOT Performed



- The following standards provide guidelines for the acceptable working environments and acceptable levels of suspended particulate matter:
  - Network Equipment Building Systems (NEBS) GR-63-CORE
  - National Electrical Manufacturers Association (NEMA) Type 1
  - International Electrotechnical Commission (IEC) IP-20

Best Practices

The following best practices are recommended to minimize dust and particulates:

- If the measures taken to prevent the entry of dust and particulates into the installation site are not effective, consider performing periodic cleaning of the inner part of the data networking equipment. To uninstall and get access to the inner part of the equipment, follow the instructions that are outlined in the installation guides for the specific data networking equipment, paying special attention to the safety requirements. On getting access, clean the dusty equipment as follows:

- Do not touch or brush the equipment. Instead use an air duster or air blower, keeping it at a minimum distance of 12 inches (about 30 cm) to prevent potential ESD damage.
- When blowing the equipment with air, pay attention not to push the dust under the electronic components (resistors and capacitors), because this could worsen the problem. Additionally, ensure that the air pressure is not so high that it damages the electronic components.
- Perform air blowing outside the installation site, possibly in the open air or in a place where the dust that is blown away does not create any harm or re-enter the facility.

Figure 3-9 Dusty Board

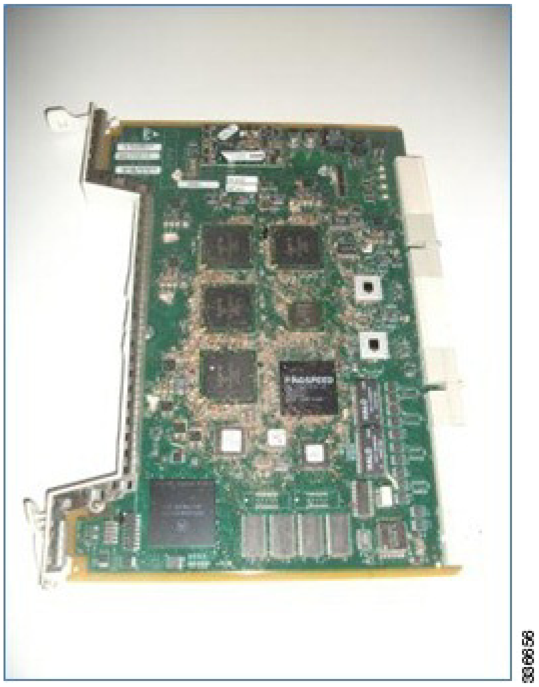


Figure 3-10 Cleaned Board

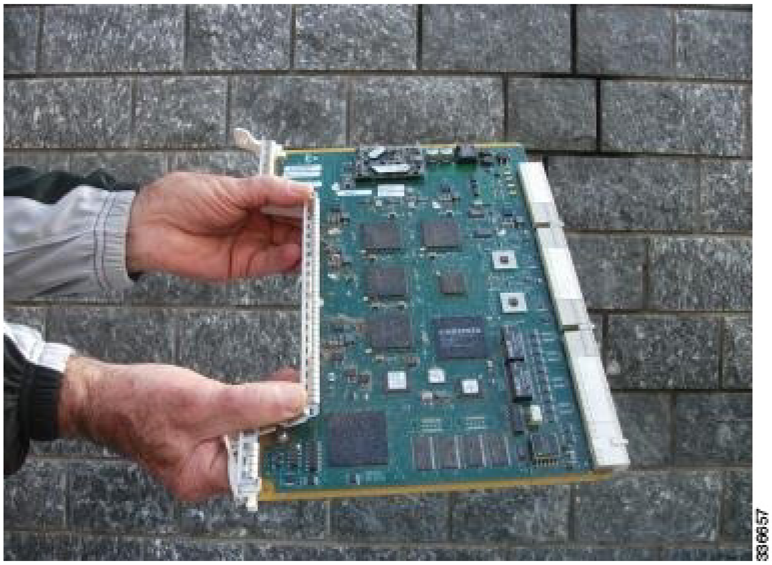


Figure 3-11 Cleaning the Dusty Board with an Air Duster or Air Blower

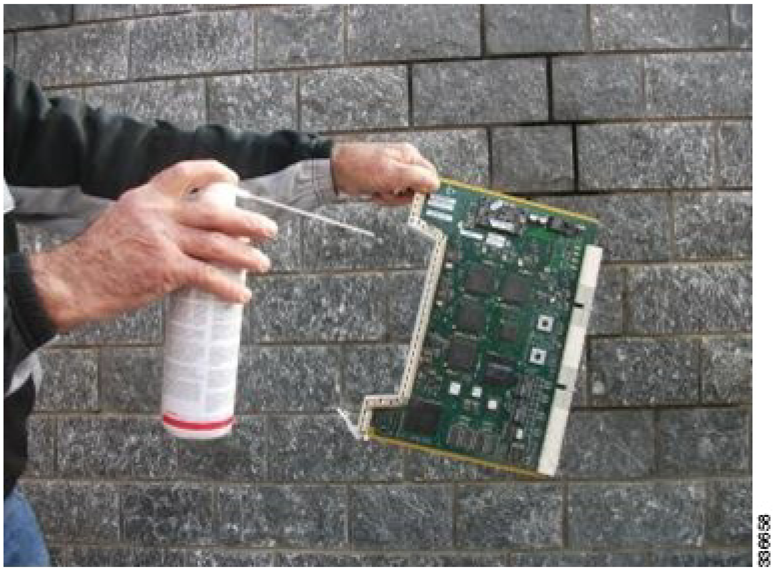
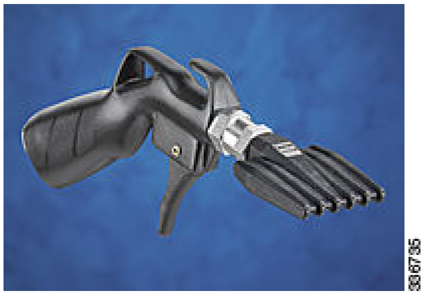
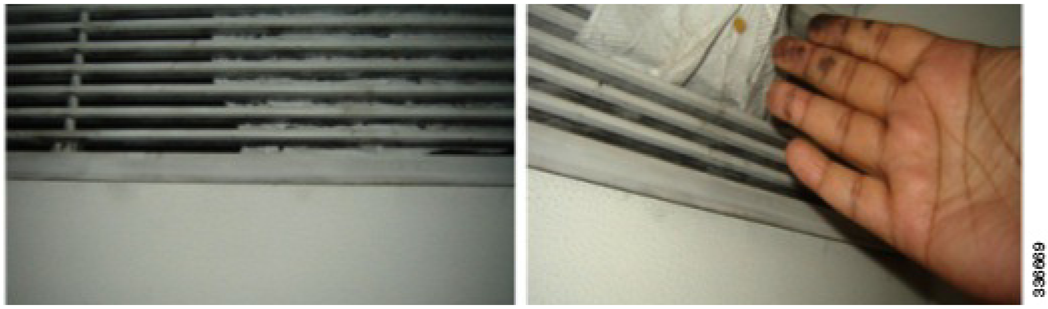


Figure 3-12 Air Blower



- Perform periodic cleaning of the AC ducts in the installation site. Dust and particulates can clog the air intake and reduce the operational efficiency of the AC system as a whole. See Figure 3-13.

Figure 3-13 Clogged Air Conditioner Duct



- Remove shoes before accessing the installation site. The dust that is deposited on the shoes can be released inside the installation site. An alternative is to install a tack (sticky) mat at the entrance door.
- Keep the door closed during maintenance operations to prevent the dust from entering inside the installation site.

- Only skilled operators should clean the equipment.
- Provide access to all the hidden areas including ducts, beam, and the area above suspended ceilings to access the dust buildup levels.
- Prohibit smoking in and around the installation site, because smoking is not only a fire hazard, but it also generates dust and particulates.
- Prohibit food and drink inside the installation site, because they are potential generators of dust and particulates.
- Provide training for all the operators working in the installation site to recognize and prevent dust hazards.

Corrosion

Introduction

Corrosion can be defined as a chemical reaction that occurs between electronic components and gases that cause metal deterioration and commonly attack edge connectors, pin connectors, IC plug-in sockets, wire wraps, and other metal components. Depending on the type and concentration level of the corrosive gases, performance degradation of the components can occur rapidly or over a period of time. It also leads to blocked currents, brittle connection points, and overheated electrical systems. As the chemical reactions continue, the corrosion by-products form insulating layers on circuits and usually cause electronic failure, short circuits, pitting, and metal loss.

These corrosive pollutants are invisible to the human eye and are ten times smaller than the smallest particulate matter. Gas concentrations are usually measured in parts per billion (ppb). At a concentration of only 3 ppb, hydrogen sulfide can corrode copper to the extent that electronic components can fail within five years. At 50 ppb, failure can occur within 6 months.

The following types of corrosion can occur:

- *Whisker growth*—Microscopic metal crystals that grow on the surface of the conductive metals. This is caused due to the presence of sulfide molecules, such as silver sulfide on a silver surface, which freely migrates over the metallic surface and collects at the dendrite boundaries where nucleation takes place, and the sulfide crystals grow on the surface of the metal. These *whiskers* can have diameters of around 20 im and can grow up to 20 mm in length. The severity of the environment, that is, the type and level of gases, humidity, and temperature determine the speed with which these whiskers are created, and the level of disruption of the flow of electrical current.
- Attack by gaseous contaminants—This is the more conventional corrosive attack primarily caused by the attack of gaseous contaminants and accelerated by heat and moisture. Rapid shifts in temperature or humidity cause small parts of the circuits to fall below the dew point temperature, which facilitates the condensation of the contaminants. RH that is above 50% accelerates corrosion by forming conductive solutions on a small scale on the electronic components. Microscopic pools

of condensation then absorb the contaminant gases to become electrolytes where crystal growth and electroplating occur. RH that is above 80% causes electronic corrosive damage to occur regardless of the levels of contamination.

A certain type of corrosion known as *creep corrosion*, which is typically a PCBA (Printed Circuit Board Assembly) level defect, occurs when a product is subjected to a harsh, sulfur-rich (hydrogen sulfide) end-use environment for a prolonged period of time. The corrosion initiates at the site of certain exposed metals, such as copper and silver, and then creeps along the surface creating shorts, or corrodes deep into the metal creating openings. Creep corrosion occurs on resistors, PCBs, and other components. No electrical bias is required to create the creep corrosion by-product. The time to failure varies depending on the contaminate levels and surface finish type. In general, it is between six months to five years.

The most common gases that can cause the corrosion of electronic components are as follows:

- Active sulfur compounds—This group includes hydrogen sulfide, elemental sulfur, and organic sulfur compounds, such as the mercaptans. When they are present at low ppb levels, they rapidly attack copper, silver, aluminum, and iron alloys. The presence of moisture and small amounts of inorganic chlorine compounds and/or nitrogen oxides greatly accelerate the sulfide corrosion. However, the attack can still occur in low relative humidity environments as well. Active sulfurs rank with inorganic chlorides as the predominant cause of atmospheric corrosion in the process industries.
- Sulfur oxides—Oxidized forms of sulfur, such as sulfur dioxide and trioxide are generated as the combustive byproducts of sulfur-bearing fossil fuels. Low ppb levels of sulfur oxides can passivate reactive metals and retard corrosion. However, at higher levels, they attack certain types of metals. The reaction with metals normally occurs when these gases dissolve in water to form sulfurous and sulfuric acid.
- Nitrogen oxide compounds—NOX compounds, such as nitrous oxide and nitric oxide are generated as the combustive byproducts of fossil fuels, and have a critical role in the formation of ozone in the atmosphere. They are also believed to have a catalytic effect on the corrosion of base metals by chlorides and sulfides. In the presence of moisture, some of these gases form nitric acid that attacks most common metals.
- Inorganic chlorine compounds—This group includes chlorine, chlorine dioxide, hydrogen chloride, and so on. Their reactivity depends on the specific composition of the gas. In the presence of moisture, these gases generate chloride ions that readily react with copper, tin, silver, and iron alloys. These reactions are significant even when the gases are present at low ppb levels. At higher concentrations, many materials are oxidized by exposure to chlorinated gases. Therefore, particular care must be given to equipment that is exposed to air that contains chlorinated contaminants. Sources of chloride ions, such as bleaching operations, sea water, cooling tower vapors, and cleaning compounds, and so on should be considered when classifying industrial environments. They are seldom absent in major installations.
- Hydrogen fluoride—This compound is a member of the halogen family, and reacts in the same manner as the inorganic chloride compounds.
- Ammonia and its derivatives—Reduced forms of nitrogen, such as ammonia, amines, ammonium ions are mainly present in fertilizer plants, agricultural applications, and chemical plants. Copper and copper alloys are particularly susceptible to corrosion in ammonia environments.

The following electronic components are particularly sensitive to corrosion attack:

- Edge Connectors—The contacts can be primarily made of copper or gold that is plated over a nickel-plated copper substrate. However, both are susceptible to corrosion. In the latter, the conducting surface of the printed circuit board (PCB) is covered with a thin layer of gold plating that is provided to ensure that the electrical contact between the board and the connector is maintained with the highest integrity over a long period of time. Because gold is a noble metal, it is

usually not attacked by ambient levels of corrosive gases. However, the gold layer is typically only between 4 and 8 Fm thick and the plating thickness is fairly porous. This permits the passage of adsorbed corrosive gases through the layer of gold, which then attacks the underlying layers of nickel and/or copper. The salts from the corrosive reaction form a higher volume than the pure metal and *lift off* the gold plating, or are forced back through the pores to the surface of the gold plating. In both the cases, the contact arm no longer rests on the conductive metal, but instead rests on a high resistance coating.
In earlier generations of electronic equipment, with operating voltages in the region of 24V and 48V DC, equipment failures occurred only after many years of operation, because the voltage was sufficient to break down the thin high-resistance layers caused due to salt formation. However, the modern generation of electronics are more sensitive to this type of corrosion, because the voltage is not sufficiently high to break down these high-resistance layers. Therefore, failure due to corrosion occurs earlier in the lifetime of the equipment.

- Pin Connectors—The problems experienced on pin connectors and IC plug-in sockets are similar to those experienced in edge connectors. However, edge connectors appear more susceptible to corrosive attack and failures can occur earlier than pin connectors and IC sockets.
- Wire-wrap Connection Pins—These are particularly sensitive to corrosive attack because the wire forms a *smear* contact between the pin and the wire with up to four different metallic alloys being exposed.
- Electrical Systems—In heavy current systems, the build-up of corrosive byproducts can cause overheating that results in a reduction in the equipment life, or even explosions inside the circuit breakers, contactors, motor starters, and so on. It is also observed that corrosion of springs and thermal overload elements leads to malfunction of the protection circuits. Traditionally, substations and motor control centers contained only heavy current equipment. However, these rooms now contain increasing numbers of electronic interlocking, protection, and signaling equipment. As such, the air purity required in these rooms is equivalent to that required in electronics rooms.

Pay particular attention to the European Union directive 2002/95/EC on the Restriction of the use of certain Hazardous Substances in electrical and electronic equipment (RoHS), which was implemented in July 2006. This was the first of many regulations with the aim of eliminating lead in electronic products. However, ongoing research has shown that PCBs that are made using lead-free materials are more susceptible to corrosion, and that lead-free products with an immersion silver surface finish are particularly susceptible to corrosion in high sulfur environments. So, corrosive environments exist in locations that would otherwise be considered benign if not for the changes in electronic equipment mandated by the RoHS legislation.

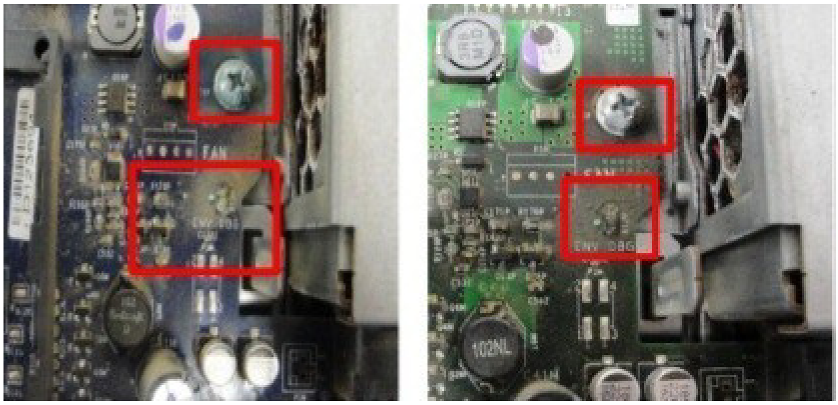
Numerous equipment manufacturers are working together to provide more guidance on methodologies that are aimed to control air quality in installation sites. An example of this effort is the *International Electronics Manufacturing Initiative (iNEMI) Position Statement on the Limits of Temperature, Humidity and Gaseous Contamination in Data Centers and Telecommunication Rooms to Avoid Creep Corrosion on Printed Circuit Boards*. This position statement defines the temperature, humidity, and copper and silver corrosion rate limits within which PCBs reliably perform in the field with respect to creep corrosion. It is important to note that this document defines the recommended range for temperature and humidity in an installation; any choice outside the recommended range (for temperature and humidity) is a balance between the additional energy savings of the cooling system versus the possible resulting degradation of reliability, acoustics, and electrical performance.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

- All Cisco data networking equipment are qualified in accordance with the *NEBS-GR63-CORE “Physical Protection”* standard, which states the maximum concentration of contaminants for indoor installations, that is, hydrogen sulfide levels should not be more than 50 ppb. There are different methods to verify if the detected values are exceeding the threshold, define the appropriate corrective actions to fix the problem, and prevent the recurrence of corrosion.

Figure 3-14 Corroded Components



- Avoid touching contacts on modules and protect the equipment from extreme temperatures and moist, salty environments.

Guidelines

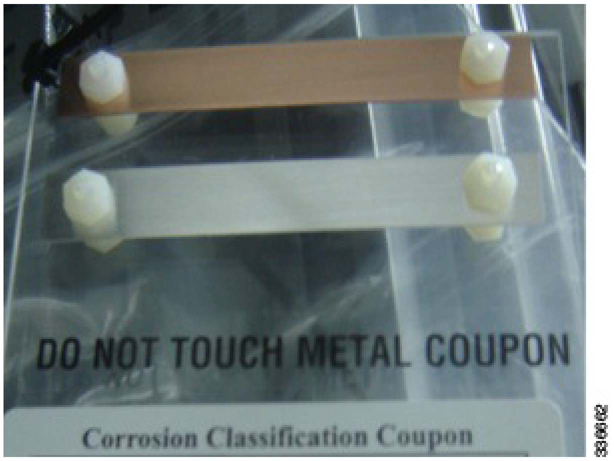
The following guidelines are recommended to prevent corrosion:

- If you suspect that corrosion may be contributing to equipment failure, for example, in case the reliability is much lower than predicted or visual signs of potential corrosion, perform the following methods to investigate and confirm the presence and severity of the corrosion:
  - Direct Gas Monitoring—Electronic devices that are designed for real-time gas monitoring accurately measure air quality to assess compliance with standards or control criteria. These devices quickly respond to changes in the measured variable, and are capable of detecting levels of a wide range of pollutants in the low ppb ranges as well. Individually, chemical pollutants can also be monitored using analytical techniques that provide both the sensitivities and selectivity, which are required to perform accurate low-level real-time monitoring. The major disadvantage of the use of real-time gas monitoring devices is their relatively higher cost when compared to other techniques.
  - Reactivity Monitoring—This method employs the use of a Corrosion Classification Coupon (CCC), which is a less expensive technique due to no capital investment and a monthly cost of less than one-tenth the gas monitoring technique. The coupons are placed close to the equipment that is subject to failure, so that it is exposed to the same environmental conditions for a period of 30-90 days, and then analyzed for the amount and type of corrosion that has occurred. This provides cumulative reactivity rates, an assessment of the average environmental conditions over a period of time, and an indication of the types and relative levels of corrosive gaseous pollutants.

    Originally, copper CCCs were used to indicate the presence of corrosive gases to test the reactivity of copper to establish environmental classifications. However, it was observed that copper was not sufficiently sensitive to most of the primary pollutants, such as sulfur dioxide, nitrogen oxides, ozone, and chlorine, which are of concern in industrial environments. Also, copper coupons cannot detect the presence of environmental chlorine, which is relevant for installation sites that are located close to a marine environment. Therefore, silver coupons are also used because silver is more sensitive to low levels of corrosive gases and chlorine than copper is.

Silver can detect changes (as small as 1 ppb) in the levels of gaseous pollutants in the ambient environment, and differentiate the classes of the contaminants. Additionally, silver is predominantly used in electronic equipment due to the RoHS initiative. Silver corrosion forms at a rate that is independent of the ambient humidity, and therefore provides a more accurate picture of the total reactivity levels of the ambient environment. The corrosion that is reported from reactivity monitoring with CCCs is actually the sum of the individual corrosion films that are formed on the coupons. For copper coupons, sulfide and oxide films are most commonly formed and reported as copper sulfide. For silver coupons, sulfide, chloride, and oxide films are formed and reported as silver sulfide, silver chloride, and silver oxide respectively. After the coupon has been exposed for the 30-90 day window period, it is analyzed by a specialized company to determine the type and amount of corrosive chemicals present in the facility, and its relative contribution to the total corrosion that is caused.

Figure 3-15 Copper and Silver Coupons used for Reactivity Monitoring of Corrosion



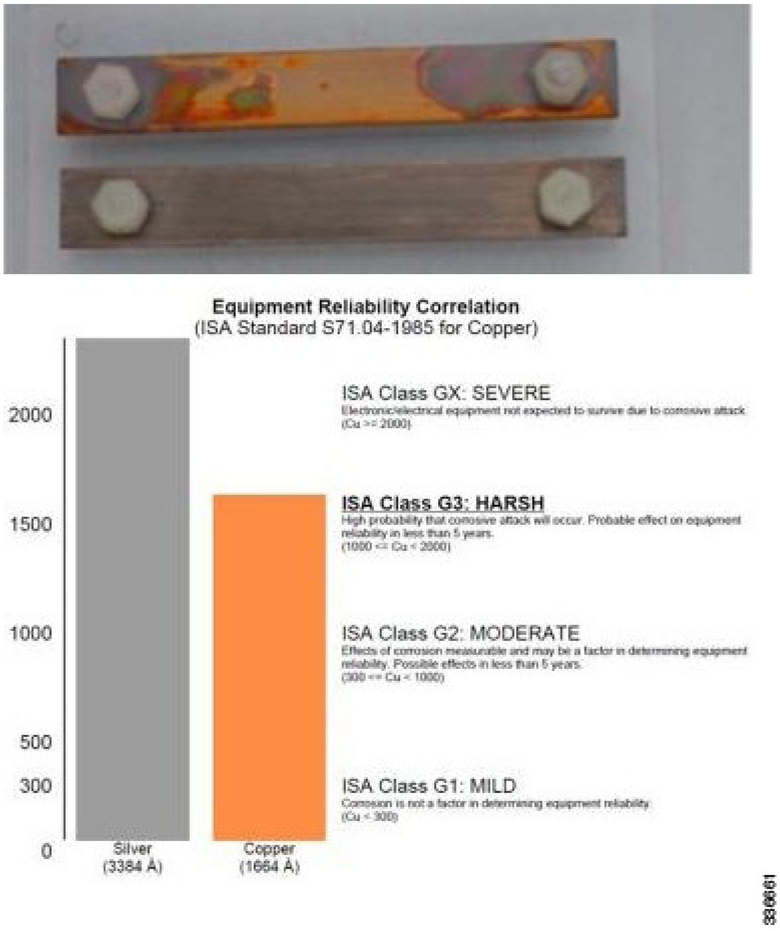
Note Reactivity monitoring is the recommended method because it provides a better representation of the environmental conditions that the data networking equipment is exposed to in the medium to long term range.

Based on the analysis of the chemical elements that constitute the films that are deposited on the coupons, the environment is classified (in accordance with the *ISA-S71.04-1985 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants* standard) into the following severity levels:

- G1 Mild (<300Å)—An environment that is sufficiently well controlled, so that corrosion is not a factor in determining equipment reliability.
- G2 Moderate (<1000Å)—An environment in which the effects of corrosion are measurable and corrosion may be a factor in determining equipment reliability.
- G3 Harsh (<2000Å)—An environment in which there is a high probability of corrosive attack. This level should prompt further evaluation and lead to environmental controls or specially design and packaged equipment.

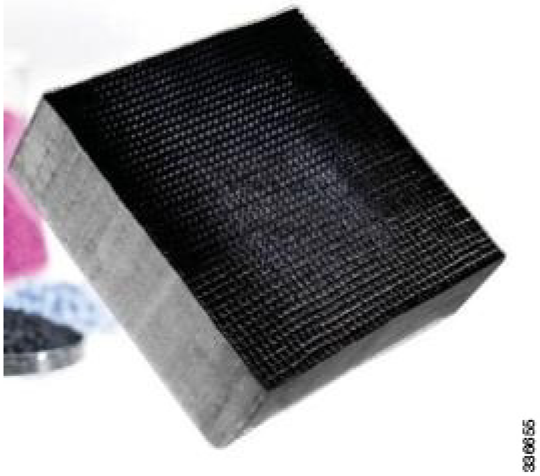
- GX Severe (>2000Å)—An environment in which only specially designed and packaged equipment would be expected to survive. The specifications for equipment in this class are a matter of negotiation between the user and supplier.

Figure 3-16 Copper and Silver Coupons Exposed to a G3 Classified Environment for 30 days



For severity levels of G2 and G3, specialized vendors can provide and install equipment, such as air scrubbers to chemically filter the air before pumping it into the installation site.

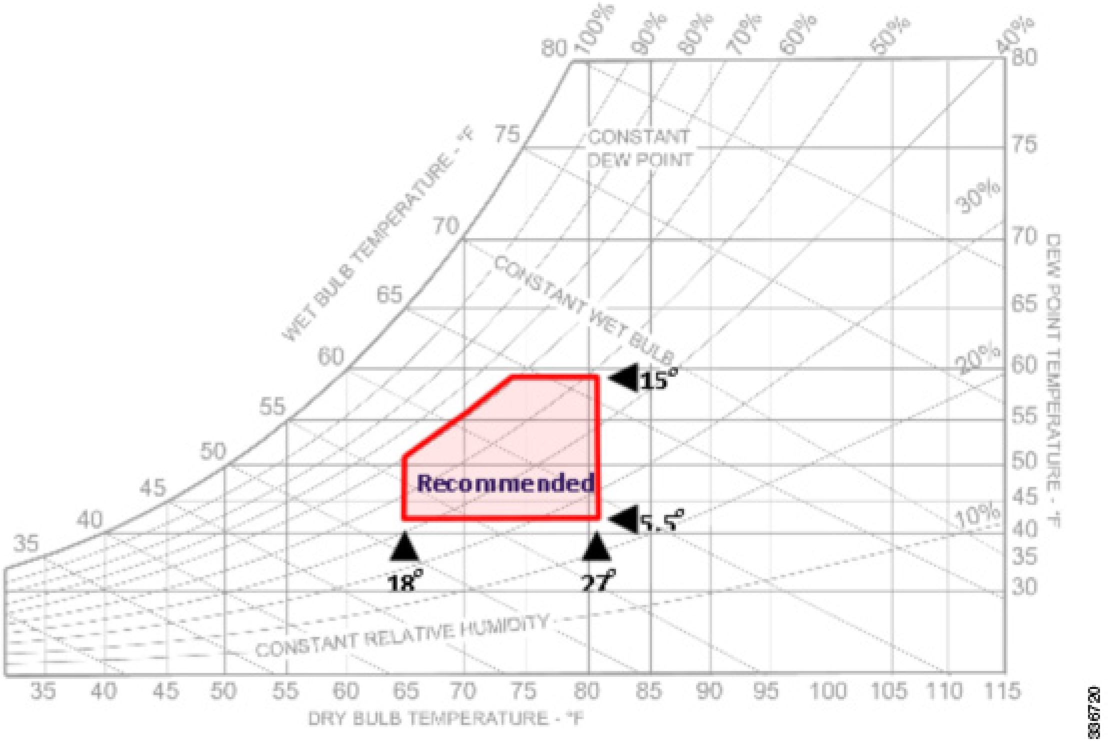
Figure 3-17 ***Media for Chemical Air Filtration (Installed in an Air Purification System)***



- Because ambient pressure, humidity, and temperature have a relevant impact on the corrosion rate, perform the following:
  - Constantly monitor these parameters.
  - Avoid using direct air cooling on active data networking equipment.
  - Avoid the presence of water trap areas inside the installation site.
  - Whenever possible, ensure that the installation site is fully air conditioned to ensure that the environmental factors are controlled.
  - Reduce the heating load per unit volume because it needs more airflow to maintain the data networking equipment within acceptable temperature limits. The increased airflow increases the exposure of the equipment to the detrimental effects of accumulated dust and to the increased intake of gaseous contaminants.
- The iNEMI recommends the following temperature and humidity ranges to prevent corrosion (see the *International Electronics Manufacturing Initiative (iNEMI) Position Statement on the Limits of Temperature, Humidity and Gaseous Contamination in Data Centers and Telecommunication Rooms to Avoid Creep Corrosion on Printed Circuit Boards*):
  - Temperature within 18°C to 27°C (64.4° F to 80.6°F)
  - Relative humidity less than 60%
  - Dew point within the range of 5.5° C to 15°C (41.9° F to 59.0°F)

  The recommended range is also shown in the psychrometric chart shown in Figure 3-18. Adherence to these values maximizes the hardware reliability and minimizes the risk of creep corrosion, which is a leading cause of hardware failure. If you decide to operate the equipment outside the recommended range, network managers will have to weigh the cost of additional energy savings, that is, the use of a cooling system, versus the possible degradation of reliability, acoustics, and electrical performance. Operating within the range supports the highest degree of equipment reliability and minimizes corrosion, even though the equipment data sheets may state wider ranges of minimum and maximum temperature and humidity (for example, 0° C to 40° C and 5% to 95% RH). Continuous equipment operation at the minimum and maximum limits is not recommended. As an example, Cisco quality engineers have observed equipment having an MTBF of 100,000 hours at 25°C deteriorating to a MTBF of 58,800 hours if operated at 35°C, which is a reduction of 41% in reliability.

Figure 3-18 Recommended Operating Range of Equipment to Minimize the Risk of Corrosion



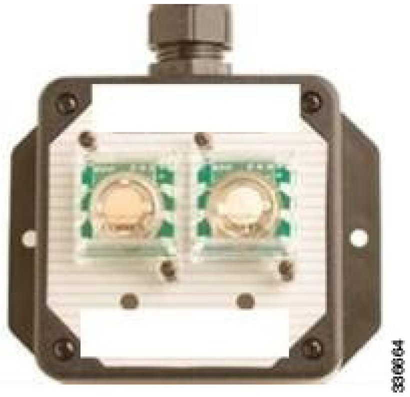
Best Practices

Consider installing real-time corrosion measurement systems when investigations have confirmed the presence of corrosive gases in the installation site and there are concerns about the effectiveness of the preventive measures that are currently implemented.

Corrosion monitors are microprocessor-controlled devices that are able to measure the total environmental corrosion attributed to gaseous pollutants. They typically detect and record changes of 1 ppb in the concentration of corrosive gases. It is this ability that is regarded as one of the main requirements for any real-time monitoring protocol to be used in such environments. Corrosion monitors employ copper and silver-plated Quartz Crystal Microbalances (QCMs), which provide real-time information on the amount of corrosion that occurs due to the presence of gaseous pollutants.

Corrosion monitors enable you to take preventive action before serious damage can occur. The appropriate reactivity and alarm levels for a particular application can be adjusted. They can be independently operated and directly wired to a central computer system or networked to relay information from multiple units to a central location. The data that is monitored can be uploaded to a PC for viewing and trending. Therefore, the most current information on the levels of corrosive contaminants can be obtained, and environmental classification databases can be established and maintained to provide historical data.

Figure 3-19 Real-time Corrosion Measurement System



Temperature and Humidity

- Introduction, page 3-18
- Frequently Missed Requirements, page 3-18
- Guidelines, page 3-20
- Best Practices, page 3-21

Introduction

Air conditioners and their associated subsystems, such as chillers, cooling towers, condensers, duct work, pump packages, and so on are used to maintain the temperature and humidity within the allowed range. For more information, see the minimum and maximum allowed values that are specifically outlined in the respective Cisco equipment installation guides.

The number and power of AC units depend on the changes in the facility thermal load, so proper dimensioning should be performed during installation. Also, it is important that these devices are periodically checked to verify that they operate efficiently and in accordance with the requirements of the installation site.

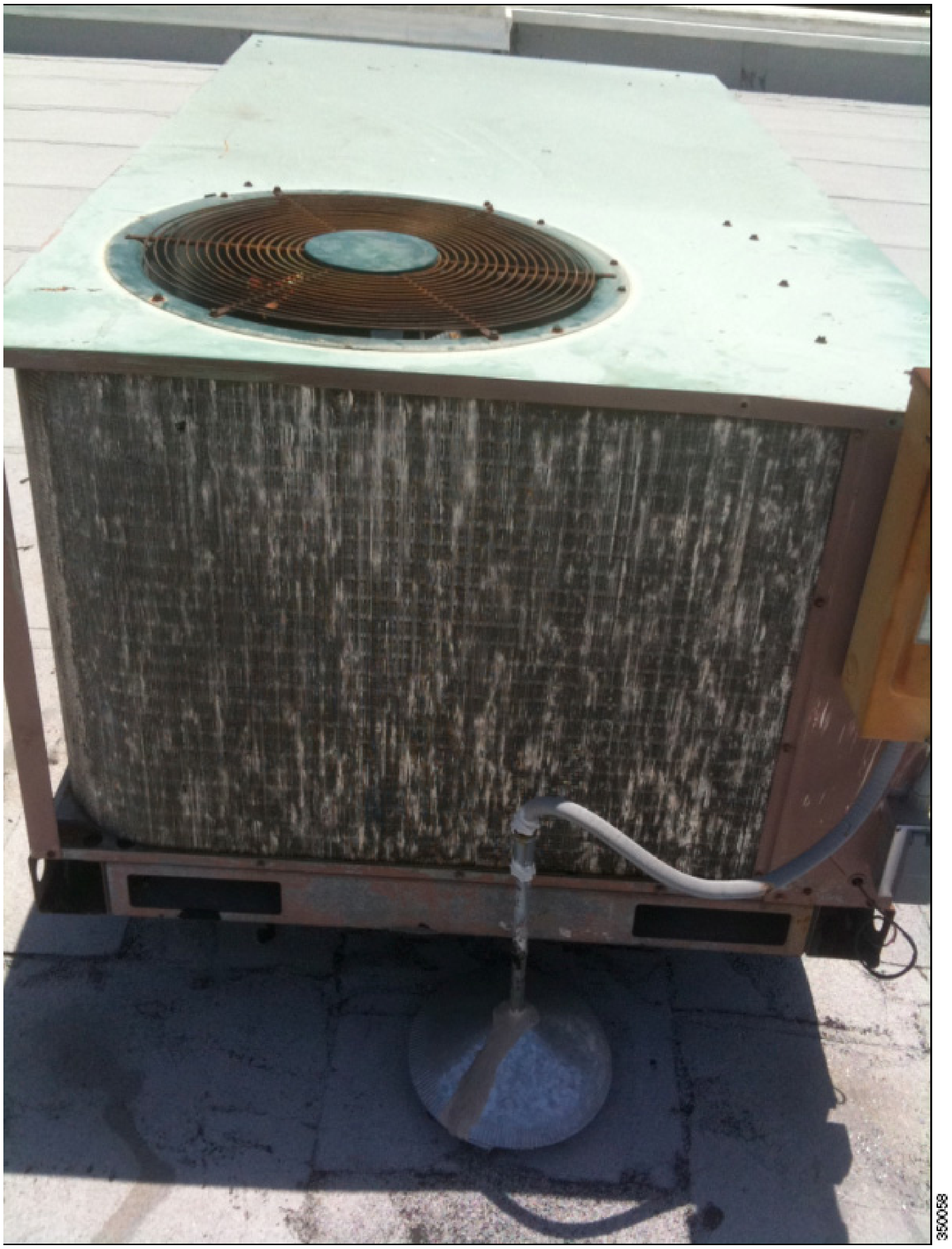
For sites that are not air conditioned, it is important that the temperature and humidity are periodically monitored and recorded to verify if they are within the allowed range.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

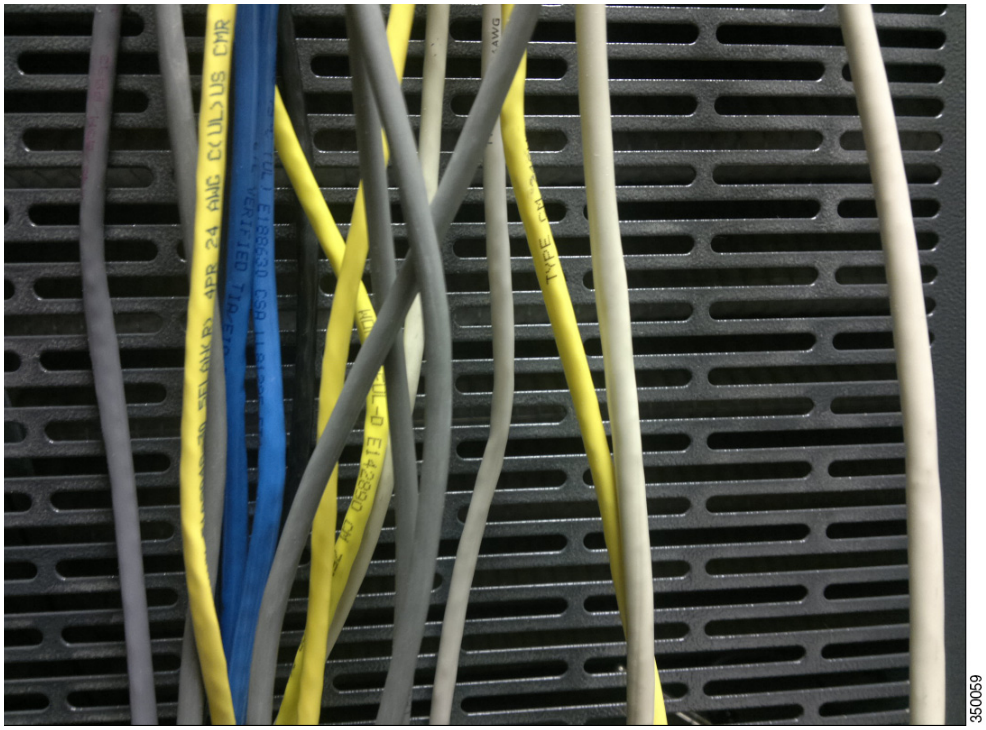
- It was observed that the air conditioners were not working or were operating under incorrect conditions. If you rely on the air conditioning system to maintain the temperature and humidity within appropriate limits in the installation site, it is important that the air conditioners are serviced as per the manufacturing specifications, and that maintenance records are properly stored.

Figure 3-20 Air Conditioner not Working at an Installation Site (No Periodic Maintenance)



- Clear the cables and other items that are placed in front of the AC as they create an obstruction to the air flow as shown in Figure 3-21.

Figure 3-21 Cables Blocking the Air Conditioner Grid



- Maintain regular records of the periodic temperature and humidity readings as proof that the data networking equipment is operated within the proper limits. Even though the instrumentation is properly installed in most installation sites, regular records of the readings are not always available.

Guidelines

The following guidelines are recommended to properly maintain the temperature and humidity in the installation site:

- American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) recommends operating network equipment within the following ranges of temperature and relative humidity (see the *ASHRAE TC 9.9 "2011 Thermal Guidelines for Data Processing Environments - Expanded Data Center Classes and Usage Guidance"*):
  - Temperature within 18° C to 27° C (64.4° F to 80.6° F)
  - Relative humidity less than 60%
  - Dew point within the range of 5.5° C to 15° C (41.9° F to 59.0° F)

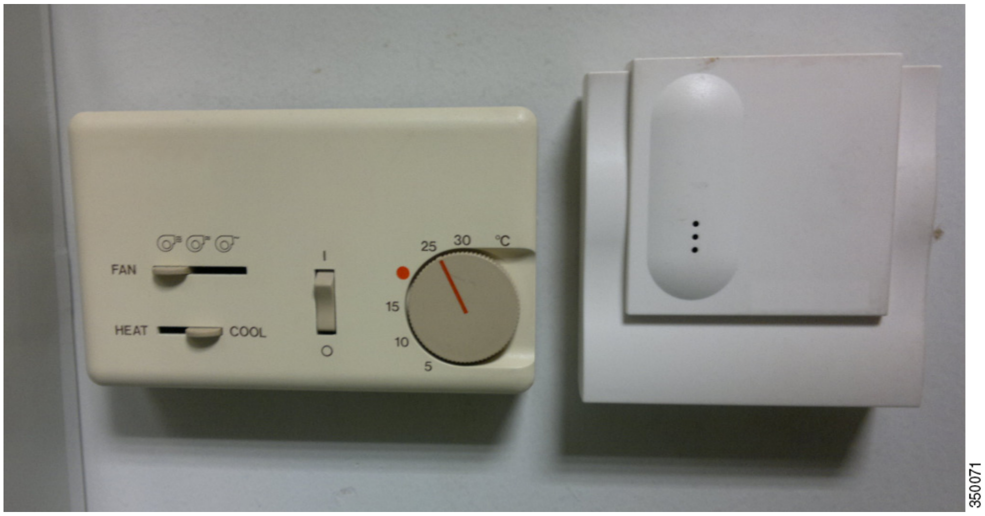
  Operating within this range supports the highest degree of equipment reliability, even though the equipment data sheets may state wider ranges of minimum and maximum temperature and humidity (for example, 0° C to 40° C and 5% to 95% RH). Continuous equipment operation at the minimum and maximum limits is not recommended. As an example, Cisco quality engineers have observed equipment having an MTBF of 100,000 hours at 25°C deteriorating to a MTBF of 58,800 hours if operated at 35°C, which is a reduction of 41% in reliability.

  Please note that these recommended values have also been included in the iNEMI Position Statement (see the "Guidelines" section on page 3-13).

- Ensure that the temperature and humidity instrumentation is calibrated, so that their readings are accurate and correct.
- Regularly service the cooling equipment, and if necessary, replace the system.
- Check the overall cooling capacity to ensure that it is not exceeded by the Cisco data networking equipment.

- Install a sufficient number of temperature and humidity sensors in the installation site to reflect the real operating conditions of the equipment as shown in Figure 3-22. Because most installation sites are rather large, a single sensor that is placed close to the entrance does not accurately reflect the operating conditions of the data networking equipment on the other end of the installation site.

Figure 3-22 Temperature Monitoring Devices



- Periodically review the data networking equipment and cooling deployment against strategy. For example, if new or additional equipment is installed, the air conditioning system may not be sufficient anymore to properly cool down the installation site.
- Shut down the data networking equipment when it is not in use based on your business needs. Consider using smart PDUs for this purpose.

Best Practices

The following best practices are recommended to properly maintain the temperature and humidity in the installation site:

- Record air intake temperatures at the bottom, middle, and top of each installation rack, and compare with the manufacturer's recommendations.
- Check for gaps within racks (unused rack space without blanking panels, empty blade slots without blanking blades, unsealed cable openings) or excess cabling that may affect the cooling performance.
- Install blanking panels and implement cable management regime because the unused vertical space in rack enclosures allows hot exhaust from equipment to take a shortcut back to the intake and causes the equipment to heat up unnecessarily.

- For installation sites that are not air conditioned, install fan-assisted devices that can improve the airflow to high-density racks and can increase the cooling capacity between each rack, because high-density racks create hot spots.
- For installation sites that are air conditioned, connect the air conditioning equipment to a backup system, so that it is operational during power outages. Ensure that the backup power generator is dimensioned in such a way that it can provide backup power for the expected duration of the outage, that is, in some countries, power outages are frequent and average a certain duration of time. Therefore, the customer or partner has to find a balance between the cost of the generator and the number of hours of backup power to provide. As part of the maintenance schedule, periodically test the efficiency of the backup power generator as per the manufacturer's specifications and local laws and legislation.
- Maintain and analyze records for the trending patterns.

Grounding

- Guidelines, page 3-22
- Best Practices, page 3-22

Guidelines

Periodically check that the grounding of all the installed data networking equipment is still in place and effective. The minimum recommended frequency is once a year. You can verify this according to following guidelines:

- Visually verify that a proper grounding wire is present and connected to the installation site grounding bar and the device. If the wire is not present, contact the facility personnel or electricians to put it in place. If the floor is grounded, the rack can be connected to the site grounding bar through the floor and a grounding chain.
- Perform a connectivity test between the device and the installation site grounding bar using a multimeter. The recommended values for the resistance are between 1 and 5 Ohm. However, refer to the local laws and legislation for the exact values.
- Create and archive a record for the test that is performed. A sticker can be attached to the device with the following information:
  - Name of the operator.
  - Date when the test was performed.
  - The ID of the rack.
  - The ID of the instrumentation used.
  - The value measured.

Best Practices

Periodically test the effectiveness of the building or the facility grounding and ensure that the testing equipment is operated by the facility personnel.

Surge Protection

- Guidelines, page 3-23
- Best Practices, page 3-23

Guidelines

Replace or supplement the surge protection circuitry periodically where the protection status is not indicated as repeated surges can degrade the protection over a period of time.

Best Practices

Visually inspect all the surge protectors or power strips on a regular basis to ensure that they are not damaged or have any signs of wear and tear. During visual inspection, ensure that the plug is plugged into their respective outlets. The surge protectors or power strips always have either a three-prong grounded plug or a polarized plug with one of the blades being larger than the other. Do not use a two or three prong adapter to power the unit. The surge protectors or power strips must have a cord of 6 feet in length.

ESD Protection

- Introduction, page 3-23
- Frequently Missed Requirements, page 3-23
- Guidelines, page 3-25
- Best Practices, page 3-25

Introduction

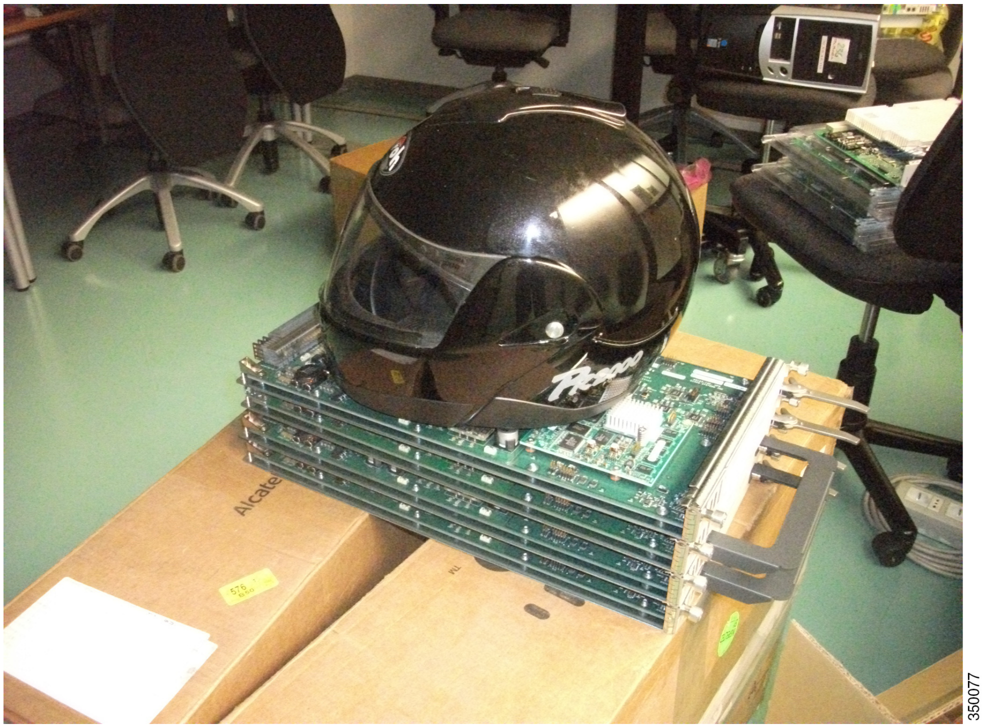
ESD protection is important not only during the installation of data networking equipment, but also during its life stages from inception, production, testing, installation, and use.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

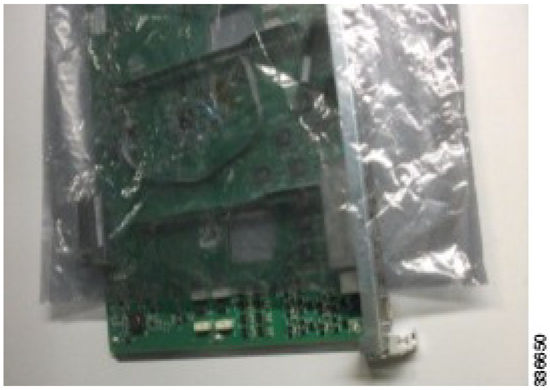
- Cards should be stored in ways to prevent the risk of ESD damage. Cards that are currently not in production or failed should be stored in the ESD-protective bags or on ESD workbenches. They should not be stacked on top of each other, which increase the risk of mechanical damage to the electronic components. They should also be kept away from ESD generators, such as a helmet as shown in Figure 3-23.

Figure 3-23 Electronic Boards Exposed to the Risk of ESD



- The missing or incorrect use of an ESD wrist wrap when installing or uninstalling the data networking equipment.
- Incorrect storage and transportation of ESD-sensitive items in an unsealed ESD-approved bag or container. Figure 3-24 shows a board stored in an unsealed antistatic bag, so that there is no Faraday cage effect to protect it from the risk of ESD damage.

Figure 3-24 Board Stored in an Unsealed Antistatic Bag



- No record that the ESD wrist straps and other devices used for preventing ESD damages is tested for effectiveness, that is, the resistance value of the antistatic strap should be between 1 and 10 MOhm.

Guidelines

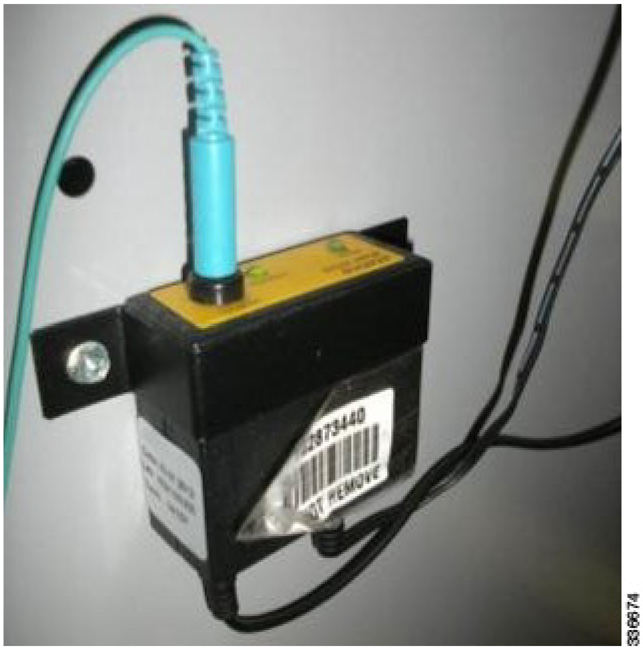
Implement maintenance practices that are mentioned in the *ANSI 20.20 Standard* to ensure the effectiveness of all the devices that are installed and used to prevent ESD damage.

Best Practices

The following best practices are recommended to ensure proper ESD protection:

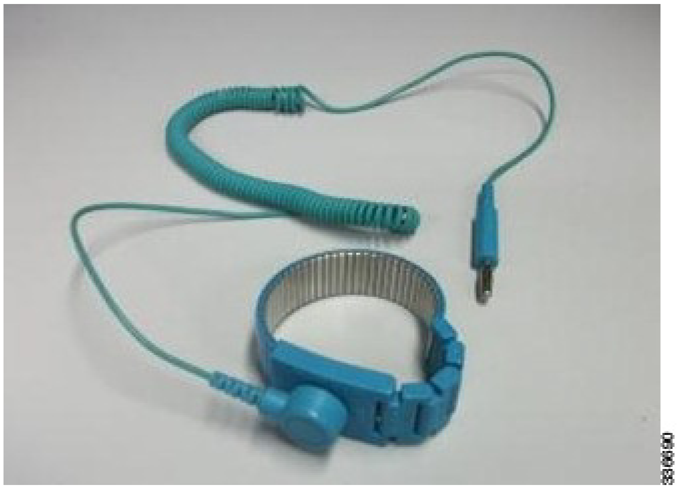
- Use devices that continuously monitor ESD. They can be installed at workbenches, racks and storage areas, and prevent the need to periodically monitor that the wrist straps are effectively working. On the device, when the light is green, it means that the wrist straps are properly connected and worn by the operator, and are effectively discharging (see Figure 3-25). Due to their low cost for purchase and installing them, they are strongly recommended.

Figure 3-25 ESD Continuous-monitoring Device



- Use a permanent or metallic wrist strap instead of a disposable one.

Figure 3-26 Metallic Wrist Strap



- Prohibit food and drink inside the installation site, because they are potential generators of static charges.
- If the installation site has an ESD-certified floor, wear ESD shoes when handling the ESD-sensitive equipment.

Fire Suppression

- Introduction, page 3-26
- Best Practices, page 3-27

Introduction

Fires in installation sites can occur due to the following:

- Power problems
- Raised floors and other concealed areas
- Electrical events such as lightning and power surges
- System discharge
- Hazardous materials
- Electronic equipment or branch circuit failures, and so on.

Fire protection should be redundant and fault tolerant. In an installation site, the primary goal of the fire protection system is to get the fire under control without disrupting the flow of business and threatening the safety of the personnel. Typically, a fire protection solution identifies the presence of a fire, communicates its existence to the occupants and relevant personnel, and finally contains and extinguishes it, if possible.

The following are few examples for fire detection or the suppression elements:

- Linear heat detection (heat-sensing cable)—Placed along wire trays and electrical pathways above and below the raised floor.

- Intelligent spot-type detection—Placed at every air conditioning unit intake and exhaust.
- Air sampling smoke detection—Placed above and below a raised floor.
- Portable fire extinguishers.
- Pull stations, signaling devices, and a control system.

Note All the detection systems should enter an alarm state before the total flooding suppression system discharges.

Typically, the control system is programmable and capable of monitoring all the devices. It coordinates the sequence of events after the initial alarm as follows:

1. Sounds a separate evacuation alarm prior to discharge.
2. Closes the ventilation dampers to prevent air from escaping.
3. Discharges the fire suppressing agent.
4. Notifies the local authorities.

Note Every installation site should refer to the recommended local laws and regulations for fire suppression techniques. The following best practices are in addition to the recommended local laws and regulations.

Best Practices

The following best practices are recommended to prevent fire:

- Ensure that the fire detection system is properly designed and periodically monitored.
- Ensure that the installation site is built far from other buildings that may pose a fire threat.
- Clearly post a list of emergency phone numbers and procedures near the exit of each installation site.
- Use advanced detectors that can detect fire in its incipient stage and notifies a central control center which in turn notifies the personnel and suppression systems.
- Use an approved fireproof sealant to seal openings in the installation site walls.
- Ensure that the fire dampers are installed in all the air ducts inside the installation site.
- Ensure that pull stations are placed at every exit in the protected space, and once pulled, it notifies the fire department.
- Install an emergency power off switch (to switch off power in all or some parts of the installation site) and use it in case of fire emergencies.
- Use suppression agents that do not destroy the data networking equipment. For example, water sprinklers are not recommended in sites that have electronic equipment installed, because they can get more damaged by water than smoke and fire.
- Ensure that the portable fire extinguishers are placed in all the critical locations.
- Free all of the electrical panels of any obstructions.
- Enforce a strict no-smoking policy in the installation site.
- Avoid using combustible materials, such as paper, cloth, and some plastics inside the installation site.
- Keep the installation site free of any trash receptacles and combustible dust particulates.

- Avoid using wooden or plastic furniture (unless they are fire-proof certified) in the installation site.
- Avoid running power cords under equipment, mats, or other covering. For example, in case of a short circuit, cables can overheat and result in catching fire if close to combustible material.
- Train all the personnel on how to behave in case of a fire, specifically the individuals that are supposed to operate the fire protection systems and extinguishers.

Access Control

- Introduction, page 3-28
- Best Practices, page 3-28

Introduction

Physical security refers to the process where the personnel are provided controlled access to the facilities in an installation site. As new technologies, such as biometric identification and remote management of securing data are widely used, the traditional card-and-guard security is replaced using the security systems that can provide positive tracking and identification of human activity in and around the site installation. Therefore, before investing in security equipment, evaluate the specific security requirements and determine the most cost-effective and appropriate security measures for your facility.

Best Practices

Table 3-1 outlines the types of safety measures for access control in a site installation.

Table 3-1 Safety Measures for Access Control in a site installation

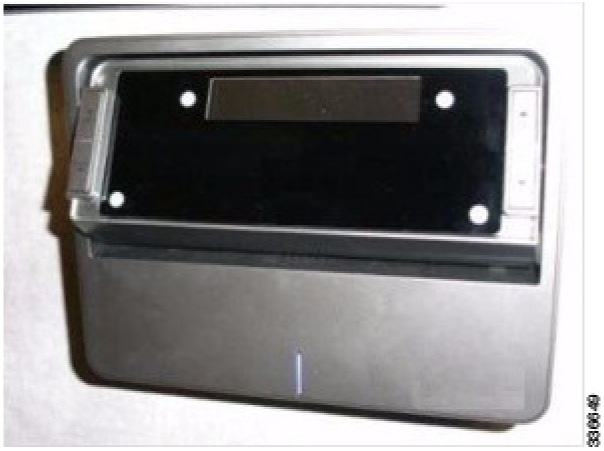
General Security	Physical Security	Logical Security
- Appoint a security guard to implement, monitor, and enforce the security rules that the management has established and authorized.	- Restrict access to the data network and other critical devices, such as data networking equipment, and so on to authorized personnel and staff members whose job functions require the use of these equipment. - Limit or remove the signage on doors to sensitive areas to reduce the chances of unauthorized staff or an intruder from locating the equipment and damaging it.	- Assign unique user IDs to each user. - Periodically review the user accounts to ensure that accessibility is appropriate, and adjust access rights when users change their jobs. - Remove access rights when users move out.

Perform the following to ensure secured access control:

- Map the security plan—Draw a map of the installation site and identify areas of entry points that require different levels of access. These areas have concentric boundaries. For example, depict the installation site as a square within a larger area, such as the building perimeter, and the concentric areas, such as the utility rooms, offices, and visitor areas. The concentric areas have different access methods that provide added protection known as the depth of security. With the depth of security, an inner area is protected by its own access options and those of the areas within it.

- Create the access criteria—A person is allowed access to a secured area on the basis of their identity, purpose, and the need to know. The following are used to identify people who fall under the three general categories:
  - What you have—Refers to what you wear or carry, such as a key, token, or a card attached to a key ring. However, this is the least reliable method of identification as there is no guarantee that the item is used by the correct person, because it can be shared, lost, stolen, or found.
  - What you know—Refers to a password, procedure, or code for things, such as opening a coded lock, verifying a card reader, and so on. However, a code or password poses a threat because if the password is easy to remember, it can be easy to guess, and if it is tough to remember, you are likely to write it down elsewhere, which reduces its security.
  - What you are—Refers to identifying unique physical characteristics. Biometric scanning techniques are developed to detect human features, such as fingerprints, hand, iris, and face. The biometric devices are the most reliable access methods.
- Select the optimal security scheme—A typical security scheme includes the following:
  - Provide access to the installation site only to the authorized and trained personnel to prevent any issues.
  - Instruct security guards, if any, about their duties.
  - Ensure that personnel who have access to the secured areas have proper identification and authorization to enter it.
  - Ensure that all visitors sign the register and wear proper IDs, so that they can be easily identified.
  - Install an appropriate device to prevent unauthorized entrance. This device could include a locked door, badge reader, biometric reader, security personnel, and so on. Figure 3-27 shows a biometric reader that is used for biometric identification.

Figure 3-27 Biometric Reader



- Create a Code of Conduct document that outlines all the Dos and Donts that should be observed in the installation site. This document can be displayed on the entrance door, and should be signed off and recorded by all the operators before entering the installation site.

Maintenance Schedules

Introduction

The primary goal of maintenance is to avoid the potential failure of the data networking equipment. A Planned Preventive Maintenance (PPM) schedule is adopted to maintain the data networking equipment and facilities in the satisfactory operating conditions through systematic inspection, detection, and correction of the incipient failures in the equipment. The PPM increases the equipment life expectancy, minimizes malfunction risks during transit, and reduces emergency repairs.

There are several resources for identifying the proper planned preventive maintenance (PPM) routines. The resources that should be considered when building the PPM frequencies and associated tasking for the critical assets are as follows:

- User and installation guides for the data networking equipment.
- Identify all the critical and non-critical data networking equipment.
- Review all local or countrywide statutory, and regulatory requirements for the critical equipment. For example:
  - Life Safety System Testing frequencies
  - Environmental limitations on generator run-times
- Verify the physical boundaries encompassing the identified critical equipment or system.
- Determine and analyze the factors that support the critical equipment. For example:
  - Power supply
  - Grounding system
  - Lightning protection
  - Cooling, heating and ventilation systems
  - Water supply
  - Supporting structure
  - All ancillary equipment
- Determine all the potential single points of failure, and the likelihood of a failure in an adjacent area that may cause undesirable conditions in the defined critical areas during the execution of the PPM.
- Perform a thorough pre-check inspection before a new equipment is loaded.
- Review Original Equipment Manufacturer (OEM) recommended PPM frequencies and tasking.
- Consider maintenance approach (reactive, preventive, reactive, predictive, and reliability centered maintenance).
- Develop job plans that are specific to the site conditions and critical assets.
- As appropriate, review the PPM tasking and frequencies to ensure statutory compliance.

Frequently Missed Requirements

The following are examples of requirements that are frequently missed in the field:

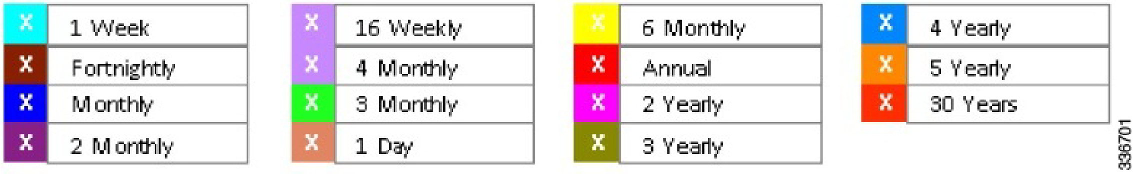
- No maintenance program is established or executed as planned.
- Personnel in charge of maintenance have not completed the required trainings and/or do not demonstrate the right skills for servicing the equipment.

Guidelines

The following guidelines are recommended for the maintenance activity:

- Consolidate all the scheduled maintenance activities for the installation site.
- Perform a PPM regime based on the minimum frequencies that are established for each device present in the installation site. An example of the frequencies for the PPM activity is as shown in Figure 3-28.

Figure 3-28 PPM Activity Frequency



X	1 Week	X	16 Weekly	X	6 Monthly	X	4 Yearly
X	Fortnightly	X	4 Monthly	X	Annual	X	5 Yearly
X	Monthly	X	3 Monthly	X	2 Yearly	X	30 Years
X	2 Monthly	X	1 Day	X	3 Yearly		

- Regularly review the PPM schedule with the stakeholders.
- Ensure that the eventual shut down dates of the installation site are pre-fixed and approved.
- Plan and mobilize the manpower or materials required for smooth execution of work.
- Communicate about the shutdown activity with all the stakeholders.
- Ensure that gradual shut-down or load shedding of the UPS power or main utilities power. Switch ON the main utilities power or UPS and observe for any abnormalities.
- Inform all the stakeholders to start up with their routine activities upon the completion of the shutdown activity.

Best Practices

The following guidelines are recommended to ensure proper maintenance activity:

- Maintain Asset Lists—An asset profile should be maintained for each asset in the site installation that encapsulates the specific parameters of an asset type and knowledge of its behaviors. For example, a data equipment model's profile would contain information about power redundancy, internal wiring, the relationship of power consumption to utilization, and various other properties to correctly interpret the information from the asset. It will be referenced when reviewing the service reports. The asset database may be referenced from a computerized maintenance and management system (CMMS) or manually.
- Create a maintenance checklist for the installation site.

GLOSSARY

A

AC	Alternating Current
ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigerating, and Air Conditioning Engineers

B

BICSI	Building Industry Consulting Service International

C

CENELEC	European Committee for Electrotechnical Standardization
CHW system	Chilled Water system
CMMS	Computerized Maintenance and Management System
CRAC	Computer Room Air Conditioner

D

DC control	Delta Current control
DLRO test	Digital Low Resistance Ohmmeter test
DX HVAC	Direct Expansion Heating, Ventilation, and Air Conditioning

E

EIA	Energy Information Administration
EMI	Electromagnetic Interference

EPO station	Emergency Power Off station
ESD	Electrostatic Discharge

H

HDD	Hard Disk Drive
HPL	High Pressure Laminate
HV feeder	High Voltage feeder
HX tube	Heat Expansion tube

I

IEC	International Electrotechnical Commission
iNEMI	International Electronics Manufacturing Initiative
ISA	International Society of Automation
ISO	International Organization for Standardization
ISL	Inter-switch Link

L

LV power circuit breaker	Low Voltage power circuit breaker

M

MOV	Metal Oxide Varistor
MTBF	Mean Time Between Failures

N

NEBS	Network Equipment Building System
NEC	National Electrical Code

NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association

O

OEM	Original Equipment Manufacturer

P

PCBA	Printed Circuit Board Assembly
PDU	Power Distribution Unit
PPM	Planned Preventive Maintenance

Q

QCM	Quartz Crystal Microbalance

R

RH	Relative Humidity

S

STP cable	Shielded Twisted Pair cable

T

TIA	Telecommunications Industry Association
TTR test	Transformer Turns Ratio test

U

UL	Underwriters Laboratories
UPS	Uninterruptible Power Supply

V

VAC	Volts Alternating Current
VDC	Volts Direct Current

INDEX