This whitepaper 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 were performed by Cisco personnel at customer sites around the world. It also covers a few installation requirements, which are already included in the product’s hardware installation guides, but are often missed.

The implementation of the installation requirements specified in the product’s manuals 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.
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

• For Fiber Cables, page 5
• For Copper and Fiber Cables, page 6

For Copper Cables

The following guidelines are recommended during the installation of copper 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 copper cables are twisted (as shown in Figure 2-2) together for canceling out Electromagnetic Interference (EMI) from the external sources that are not exposed even partially, as it results in EMI issues.

![Figure 2-2 Twisted Cable](image)

• Avoid the following actions that can stress the cable:
  - Applying extra twists.
  - Pulling or stretching beyond the specified pulling load rate.
  - Creating tension in the suspension runs.
  - Stapling or applying pressure with the cable ties.

• Preserve the same density of twists in the cable pairs till its termination for horizontal and backbone twisted-pair cabling as applicable.
• 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 2-3), because this can cause failure of the individual cables over a period of time due to connector differences and core size (with no metal to metal connection between the blades of the connector and the core of the cable). Even though connectivity is initially established, the risk of failure increases due to the movement or flexing of cables and/or stress between the cable and connectors.
For Fiber Cables

The following guidelines are recommended during the installation of fiber cables:

• Avoid the following actions that can stress the cable:

  – Pulling or stretching beyond the specified pulling load rate.
  – Bending it beyond the specified bend radius.
  – Creating tension in the suspension runs.
For Copper and Fiber Cables

The following guidelines are recommended during the installation of both copper and fiber cables:

- 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.
- Unless you are running the cables in an outdoor environment, ensure that appropriately sized conduits, cable raceways and/or ladders are used for future expansion.
- 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.
- 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 2-4). Instead, route the cables below or above, and into the horizontal cable manager (if it is in place) (as shown in Figure 2-5 and Figure 2-6).
For Copper and Fiber Cables, Cont.

- If running cables in/out of a sealed outdoor cabinet, ensure that all the cable glands are sealed to prevent dust and moisture from entering the box.
- For separation requirements of communications wires and electric power cables, refer to the NEC (NFPA 70) standard. As an example, see what is stated in Article 800.133 (2005 NEC):

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, please check the national and local electrical codes and regulations, since they may overrule the requirements mentioned in this standard.

Figure 2-4, Figure 2-5, Figure 2-6, and Figure 2-7 are examples of good and bad cabling practices.
Network Cabling Design
Best Practices: 2017

Guidelines, Cont.

Figure 2-6 Efficient Cabling

Figure 2-7 Inefficient Cabling
For Copper Cables

The following best practices are recommended during the installation of copper 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 the Velcro-based ties every 1 to 2 meters for bundling or securing the cables, and avoid using zip ties as they apply pressure on the cables.

For Fiber Cables

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

• Do not touch the fiber tips of fiber cables.
• Use single mode and multi-mode optical fiber cables as per the optical transceiver requirement.

For Copper and Fiber Cables

The following best practices are recommended during the installation of both copper and fiber cables:

• Do not use copper and fiber cables whose connector retention tabs are broken.
• While inserting copper and fiber cables, check that the connector retention tab locks into the connector or the optical transceiver properly.
• 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 that all the unused cables are stored 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.
• 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 not 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.

Figure 2-9 Efficient Cabling using Cable Guides

Figure 2-10 Bend Radius - Example
Grounding

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 from coming into contact with dangerous voltage if an internal fault, such as an insulation failure occurs. Furthermore, connections to the ground also prevent the buildup of static electricity.

Frequently Missed Requirements

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

• Equipment racks are not connected to the installation site or the building ground. Equipment managers should ensure that all the equipment racks are grounded to the building. If this is not done, there can be a serious safety risk to the personnel, since they could assume that the equipment is properly grounded when it is actually not. Additionally, an electrical discharge 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.
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 this purpose.

This is because a system that uses only an AC third prong ground is not sufficient to fully ground the device. Electrostatic discharge (ESD) can lead to the following failures:

- Damage to electronic components
- Data corruption
- System lockup
- Frequent system reboots

Some service technicians claim that they do not need NEBS grounding as they rely on metal-to-metal connections between the Cisco device and rack. First of all, even if the metal-to-metal connectivity seems properly in place, you need to use a multi-meter to verify the effectiveness of the connectivity. For example, the use of plastic screws and washers to minimize vibrations avoids effective metal-to-metal connections. You need to 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.

In addition, even though the multimeter confirms good connectivity, you cannot trust the metal-to-metal connection between the equipment and the rack over the time, since the connection may not work properly anymore. For example, the connection can become loose because of vibrations. So, it is only the NEBS grounding lug that ensures that the grounding is always 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
A few Cisco power supplies require dedicated and independent grounding.

However, during the field survey, it was observed that most service technicians 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.
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 earth 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 and the ground.

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.
Use a multimeter or an equivalent device to check the effectiveness of the connectivity between the different parts of the installed equipment (such as cards, chassis, and racks) to the building ground. Using IEEE Std 142-2007 “Recommended Practice for Grounding” and IEEE Std 1100-2005 “Recommended Practice for Powering and Grounding Electronic Equipment”, the ideal grounding value would be less than 1 ohm from the equipment into the Earth.

However, achieving this would be costly and burdensome for most of the installations, so, our recommendation for grounding is not to exceed 5 ohms at Earth into the grounding rod and not to exceed 1 ohm from the grounding rod to the equipment. Please note that the 25 ohms noted in NEC grounding methods should not be interpreted to mean that 25 ohms is a reasonable resistance for a grounding system. Using the maximum 5+1 ohm approach covers realistic soil conditions for the ground rod(s), and reasonable length/sizing of the wiring used in the ground infrastructure. Finally, remember that if there are local laws and legislation setting grounding values, you should refer to them.
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.

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 can be 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 is usually worn on the nondominant hand (the left wrist for a right-handed person). It is connected to the ground through a coiled retractable cable and 1 megohm resistor, which allows high-voltage charges to leak through but prevents a shock hazard when working with low-voltage parts.
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. The mats can be placed on the floor or on workbenches (where available).

ESD damage occurs most often when printed circuit boards are improperly handled while being transported. Even when a PCB is inserted in a metal frame (for example, like in a SFP transceiver), you should not assume it is protected from ESD, because the metal frame acts as a Faraday cage: connectors or EMI shields on the board can still be a path for electrostatic discharges, if directly exposed to external contact. So, adopt appropriate ESD protection devices (such as antistatic bags) when handling such device.
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.

![Failed Component due to ESD Damage](image)

**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 in the wrist strap and ensure good connectivity to the device and ultimately the ground (Figure 2-20). 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 a rack. Avoid connecting the wrist strap to painted surfaces (see Figure 2-22 and Figure 2-23).
Figure 2-20 Permanent (Metallic) Wrist Strap Connected to the Bond Point of Cisco Equipment
During installation or removal, handle electronic equipment 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.
When replacing a failed card, place it component 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. The repaired equipment is used as a replacement for eventual additional failures in the field but is never sold as “brand new.”

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.
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, the ideal value is less than 1 ohm and it should not exceed 5 ohm. Please refer to the “Best Practices” section on page 2-15 in “Grounding” for more details.

- **Automated Handlers** (devices that are used to move electronic parts from one working station to another in a production environment) – 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 disposable ones as metallic wrist straps have better connectivity to the skin of the operator, and are less prone to failure when compared to disposable wrist straps, which are made of inexpensive and not very resistant material. Because of this, the grounding cable or strip in disposable wrist straps can easily break, making the wrist strap totally ineffective. Since permanent (metallic) wrist straps are very reasonably priced (usually a few US dollars), the usage of disposable wrist straps is not worth the risk.
• 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 lose 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 floor waxes can reduce conductivity and create a level of insulation that prevents the effective dissipation of electrostatic charge. 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.

• Use an ESD mat (see Figure 2-28) 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 2-29 outlines how to ground the mat to the same potential as the chassis and the rack.
Best Practices, Cont.

Figure 2-29 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 with 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 the 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.
  - Deionize or use other discharge-mitigating techniques in the workstations to neutralize eventual electrostatic charges.
Figure 2-30 Typical ESD Protected Area

1. Groundable Wheels
2. Groundable Surface
3. Wristband and Footwear Tester
4. Footwear Footplate
5. Wristband and Grounding Cord
6. Grounding Cord
7. Ground
8. Earth Bounding Point
9. Groundable Pointe of Trolley
10. Toe and Heel Strap (Footwear)
11. Deionizer
12. Dissipative Surfaces
13. Seating With Grounding Feet and Pads
14. Floor
15. Garments
16. Shelving With Grounded Surfaces
17. Groundable Racking
18. ESD Protective Area (EPA) Sign
19. Machine
Introduction

Proper airflow through the data networking equipment helps maintain effective operating temperatures and prevents the premature end of the equipment life. Improper airflow due to no or limited space between the chassis air vents and the adjacent walls leads to equipment overheating. The use of incorrect cabinets prevents proper airflow and ventilation. The selection of the type of rack for an installation site depends on the air-flow of the installed equipment (front to back, side to side, and so on), security requirements (for example, equipment shared by different companies) and many other factors. Based on these considerations, fully open and/or closed racks, with perforated or no doors can be chosen for the installation site.

Frequently Missed Requirements

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

- Maintain a minimum air space clearance (Refer to product manuals for the actual value. For example, 6 inches for Cisco 6500 switch) in front of the chassis air vents. Figure 2-1 depicts an example of how cabling can obstruct the air grids).
- For equipment that has side-to-side airflow, maintain a minimum horizontal separation of 12 inches (about 30 cm) between the two chassis.

Best Practices

Figure 2-31 depicts the air flow in and out of a Catalyst 6509 chassis. The air flow of a Cisco router 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. In addition, some operators may have their own installation requirements that have to be considered in addition to the ones explicitly mentioned in the installation manuals of Cisco data networking equipment. Whatever the requirements, it is recommended to install equipment that facilitates the air flow to ensure cooling. For example, if access to the equipment needs to be restricted due to security reasons, a fully-enclosed cabinet may be used. In that case, perforated doors facilitate the air flow.
Airflow

Figure 2-31 Airflow In and Out of a Cisco Catalyst 6509 Chassis
Missing or loose screws during the installation of data networking equipment (as shown in Figure 2-32) can lead to major safety issues (for example, a heavy chassis may drop, hit the operators and create serious injuries or the malfunctioning of the card due to bad connectivity with the chassis.

**Guidelines**

- Check the backplane connectors on the board and the chassis prior to insertion.
- In the early 1990’s, uninterrupted power service into a building was not always a given. Major power outages caused many issues such as downed communications, stuck elevators, and airport shutdowns. Even at the system level, power supply mean time between failures was a low hour number. In the last 20 years, many changes have been made to power delivery, spanning entry into the building all the way to the equipment. Installations today include multiple back-up generators and multiple UPS systems providing solid facility power to all sensitive or necessary equipment. Power supply systems have gone from 100’s of hours MTBF to 1000’s of hours MTBF. Equipment power includes N+N or N+X system power redundancy, providing a very stable equipment power system. The combined implementation from the facility input to the equipment input means that power interruptions have been eliminated as a contributor to system wide outages.

- Cisco continues to provide equipment power redundancy at the power shelf and power supply level in one of two formats. The most widely accepted format is the N+N dual power source redundancy. This implementation provides two completely divided power systems supplying power to the internal electronics. Any power fault on one side is isolated and the equipment continues to operate on the power from the other side, the other “N”. This provides very high reliability to the system, providing maximum fault free operation form power related events.
• Another accepted format is the N+X power source redundancy inside equipment. This type of solution has “X” number more power supplies in the event of a power supply failure, but does not always provide power shelf redundancy or power shelf fault redundancy. Though not as fault tolerant or as reliable as the N+N redundant power system, the N+X implementation does meet minimal customer requirements and can be implemented with a cost advantage.

• Low down time equipment requiring minimal to zero power outages is best suited for N+N power systems providing the highest reliability advantages, while equipment that can tolerate low levels of power faults is best suited for the N+X power system providing good reliability and improved cost.
Faceplates

Introduction

To ensure the proper airflow and heat dissipation of the data networking equipment, it is essential to protect unused slots using blank faceplates. The blank faceplates provide the following benefits:

- Prevent entry of dust into the chassis
- Prevent abnormal board temperature
- Prevent Electro-magnetic interferences (EMI) phenomena
- Prevent access to energy hazards or hazardous voltage (for example, operators touching high voltage components on exposed boards)
- Provide a complete fire enclosure for the chassis

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 2-34 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 2-34 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 2-35** shows unused optical connectors without protective caps. This leads to accumulation of dust on the optical fibers that can result in transmission errors and damage to the connectors. Additionally, the optical connectors shown in **Figure 2-35** 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 2-36** shows an example of unused optical ports without protective caps, while **Figure 2-37** an example of unused optical ports with protective caps.
Introduction

What are Electrical Surges? Importance of Surge Protectors

An electrical surge happens when high voltage electrical current travels through your cable lines, telephone lines, AC power and Data Transmission lines. This can cause tangible damage to Data Networking equipment, installed in the data centre/installation sites resulting in burning out of electronics.

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

Types of Electrical Surges

Different situations can lead to an electrical surge. Often, the causes cannot be foreseen or prevented, which is why it is necessary to seek out the best possible proper protection for Equipment installation sites. There are two main kinds of power surges.

1. External Power Surges – These are damaging power surges caused by external, usually weather-related factors like thunderstorms. These surges can easily damage the data networking equipment installed for business purposes. One of the most common causes of surges in many parts of globe is lightning. Some geography has frequent lightning storms, which can deliver large currents that cause destructive electrical surges.

2. Internal Power Surges – These are the kind of electrical surges that service technician should be mindful while planning surge protection. They are practically undetectable and, like external power surges, can definitely cause damage to data networking equipment. Here are two of the possible causes of internal power surges:

- Utility disturbances – This is often due to an overload in power outlets that can happen when too many appliances are plugged in. This is why it is dangerous to plug too many individual electronic devices into a single electrical socket.
- Blackouts – When power is restored following a blackout, the electrical wiring and lines can be subject to a rush of current. This often unpredictable surge can cause real harm to Data Networking equipment.
How do Electrical Surges Cause Damage?

Power surges can run dangerous amounts of electric current to Data Networking equipment. This current will generate heat and can severely damage components, or even lead to fire. Surges tend to damage data equipment in a slow, discreet manner often called EOS (Electrical Overstress). Damage often accumulates until the equipment stops working completely.

Equipment Protection

AC Input line protection, for this discussion, can be broken down into 4 basic categories:

- **In-line UPS** – Using an in-line UPS system that converts the input power into DC and then back into AC again, isolates the equipment from line noise, harmonic distortion, low voltage, high voltage, and almost every type of power quality concern. This type of system uses batteries and a transformer to completely isolate the AC output from the AC input and any power related problems introduced at the input. This type of AC line protection can be the best defense against line disturbances effecting the equipment.

- **Control Voltage Transformer (CVT) or Constant Voltage Transformer** – The standard transformer is a simple ratio device where the ration of the output voltage to input voltage does not change. This type of transformer passes through any line voltage variations. The CVT uses gap magnetics to ride through short term durations (<200msec) in input voltage variation, or a variable ration adjuster to compensate for the short term voltage changes. The result is an output voltage fairly stable and consistent with load changes.

- **Surge Suppression** – Surges and spikes refer to short-term voltage changes. 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 certain duration of time, a trapping device known as a Metal Oxide Varistor (MOV) that is present in the surge protector gets activated. The MOV diverts the surge current away from the output load. The lifespan of MOVs shortens as surge currents are diverted. They do not display any indication of wear and tear, nor do they provide any forewarning of failure. When they suddenly fail, their temperatures increase rapidly and may cause fires. Most surge protectors function as a power strip even after their surge trap mechanism is degraded by power spikes, causing 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.
Introduction, Cont.

• **Lightening Suppression** – Lightening suppression is dealt with in two basic ways:
  - A diversion grid of rods placed at key locations at the highest points around a facility connected by copper wire to the ground helps to keep stray surges from entering the inside of a facility. Lightening, once inside a building, is notoriously hard to mitigate and often leads to severe equipment damage. The best prevention is to keep the lightening outside the facility.
  - Solid grounding of all copper data cabling coming into a facility via grounding blocks will prevent lightening from entering a facility on the broadband or SDN copper data lines by diverting any current flowing on the shield or inner conductors into earth ground. DC Input line protection is typically not required, though ground quality is still equally important as it is in AC Input Line protection.
• DC Rectifiers should be providing some level of protection in the AC to DC isolation circuit. The DC is not only isolated from the AC input line, but also very well filtered. Most DC Rectifiers provide equal or almost equal power line quality seen from the in-line UPS.
• Battery strings absorb a certain amount of surges and transients within the DC power distribution. Think of it as having huge number of capacitors filtering the DC line.

**How do Electrical Surges Cause Damage?**

When used properly, data line protection allows the use of copper cabling rather than fiber optics to interconnect internet communications and technology gear from one building to another, basically originating from inside a building, through the outside elements, and into another building for termination. When implemented with surge and transient suppression techniques, this type of cabling solution can offer a reliable, long term, low cost interconnect solution in those locations better suited for copper then fiber.

• **Copper cabling** – Use high quality copper cabling with a combination wire and foil shield. Bonding of the shield wire must be done in accordance with the connector company and the internet communications and technology gear provider to provide the best protection.
• **Transient suppression and lightening protection** – A combination data line filter and grounding block is the most effective way to divert energy/current flow on the data line to earth ground, allowing only the data to continue towards the internet communications and technology gear. This type of protection prevents transients from reaching the network equipment and damaging the interface.
Introduction, Cont.

Figure 2-38 Surge Protection on an ISDN Line Card Installed in a Cisco19xx Chassis

**Best Practices**

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

- Using an inline UPS or DC rectifier adds a substantial amount of equipment power protection. Consult your provider’s manual for proper installation and maintenance for continues maximum protection.
- Install data line protection and lightening protection in areas known to have transient voltage problems or high to severe lightning strike rates.
- 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.
- 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.
**Introduction**

The optimal temperature and RH levels are best controlled by installing air conditioners at 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. At 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.
- Many times, it is observed that there is no control of the temperature difference between the intake and the outtake (exhaust) air of data networking equipment. If the delta exceeds what is specified in the respective product manuals, it can be a sign of overheating of components that could lead to a premature failure of the device.

**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.
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.

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.
The following best practices are recommended to control the temperature and humidity. They sense particularly for small installation sites that usually do not have sophisticated environmental control systems:

- Install a device for continuously monitoring environmental factors, such as temperature, humidity, the presence of water on the floor, and so on. If the site is an unstaffed installation, ensure that the device can be remotely accessed. Information that is received from the devices can be valuable in assessing whether the environmental conditions at the site could be contributing to performance issues or equipment failures. These devices are especially useful at sites that are not air conditioned. If the device is connected to the Facility Operation Center of the customer or partner, an alarm can be generated when a pre-set threshold limit is crossed, and corrective action can be initiated. Additionally, the sensors installed in many Cisco data networking equipment measure the inlet air temperature and can be remotely monitored through appropriate software applications.

- For equipment that have the cooling airflow side-to-side (right to left of vice-versa), most of the Cisco installation guides for data networking equipment already specify the minimum distance between two adjacent chassis, usually 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.