11 Fire Protection

11.1 Introduction

Because fire protection regulations differ between countries and jurisdictions, the designer must use the appropriate local codes and standards. The following section describes the best practices in the United States and can be used for guidance in other locations as although the codes and standards may differ, the safety philosophy and best practices employed will be similar.

11.2 Basic Design Elements

The basic design elements of fire protection are:

- Fire detection—smoke, heat, and early warning detectors connected to an alarm and monitoring panel.
- Fire suppression—extinguishing systems to protect ITE.
- Fire alarm system—a system, including the fire detection systems, with a means to automatically send alarm, supervisory and trouble signals to a central station, security center, fire department, or other approved, constantly attended location, and warn occupants of the presence of smoke, heat, or fire through the use of audible or visual alarms.

11.3 General Requirements and Recommendations

11.3.1 Requirements

The computer room shall be separated from other areas or occupancies within the building by fire-resistance-rated construction. Refer to Section 7.5.7 for minimum fire rating of spaces.

The computer room shall have a fire protection system. If the computer room is located in a sprinklered building, the computer room shall be likewise protected with a sprinkler system. If the data center is a standalone facility (not part of a larger building) or is located in a nonsprinklered building, the computer room shall be protected with a sprinkler system, a gaseous clean agent system, or both a sprinkler system and a gaseous clean agent system.

The basic fire suppression system in a computer room shall be a fire sprinkler pre-action system. The sprinkler system for a computer room shall be valved separately from other sprinkler systems. Valves controlling water to the computer room sprinkler system shall be labeled and easily identified as separate from valves controlling sprinkler water to the rest of the building.

Sprinkler heads shall be flush-mount pendant type if there is a suspended ceiling. The sprinklers shall be installed per applicable local codes, standards, and regulations. If there is no suspended ceiling, sprinkler heads shall be covered with a wire cage to prevent accidental impact and discharge.

Halocarbon clean agent systems, including Halon 1301, shall not be used to protect under an access floor unless the space above the access floor is likewise protected by the same halocarbon clean agent system.

Any furniture in the computer room shall be constructed of metal or nonflammable materials. However, chairs may have seat cushions made of flame-retardant material.

Tapes and records shall be in a separate room with a fire suppression system and with fire-rated construction separating these rooms from the rest of the computer room and from any adjacent occupancies that are not part of the computer room. See Table 7-1 in Section 7.5.7 for further information regarding fire-resistant construction.

Automated tape libraries or other types of automated information storage system (AISS) units shall have a gaseous agent fire suppression system installed within each unit if there are more than 0.76 m^3 (27 ft^3) of tapes or other combustible media.

Combustible materials shall not be stored in the computer room.

The design and installation of systems related to fire protection (e.g., detection, suppression) shall be performed by applicable certified professional as designated by the AHJ.

NOTE: In the context of fire protection, companies providing insurance during the construction or operation of a completed data center may be considered an AHJ.

11.3.2 Recommendations

The fire detection system should include an early warning smoke detection system and a water leak protection system.

When practical, the sprinkler system should have an alternate water source to prevent a single point of failure and to allow maintenance.

Local codes may sometimes require that the suppression agent used below the access floor must be identical to the method used above the floor for the rest of the space or building.

Where it is critical to protect electronic equipment in the computer room, a gaseous, clean agent system dedicated exclusively to the computer room should be considered in addition to any required fire sprinkler system and, when used, it should be configured as the system that is activated first. While overhead water sprinklers provide excellent protection for the building structure, water from sprinklers will not reach fire located within ITE cabinets. Gaseous agent extinguishing systems provide "three dimensional" protection of spaces within equipment enclosures and are capable of suppressing fire in circuit boards and internal components.

If the entire facility is not protected with a gaseous clean agent system, it is a best practice to protect space under access floors with a dedicated inert gas clean agent system or a carbon dioxide total flooding system when the under-floor space contains combustible material (such as non-plenum rated cable). Carbon dioxide should normally not be used above the access floor in computer rooms.

Computer rooms should not have any trash receptacles. All unpacking should occur outside the computer room, and any trash in the computer room should be promptly removed.

Data center personnel should be trained on the use and function of the fire detection and extinguishing systems of the computer room.

Paper should be stored outside the computer room with a fire suppression system separate from the one used by the computer room.

Where not otherwise required by the AHJ, the design and installation of systems related to fire protection (e.g., detection, suppression) should utilize professional fire engineers, designers, and installers with applicable experience.

Lithium-ion (Li-ion) batteries are increasingly being used within centralized UPS systems and as local battery backup within cabinet and racks (See Section 9.5.5.4.3). Some types of lithium ion batteries have volatile chemistry and in the event of an internal short circuit or thermal runaway the resulting fire is difficult to extinguish, as the application of water can produce dangerous gases. If Li-ion batteries are NCA, NMC, a combination LMO/NMC, or other type of volatile chemistry are used, the fire extinguishing system may need to be a different option than sprinklers or augmented by a non-water system to mitigate the risk of a fire. Centralized UPS lithium-ion UPS batteries should be located in a separate room to the ITE.

11.4 Walls, Floors, and Ceilings

11.4.1 Requirements

NFPA 75 provides minimum requirements for the construction of the walls, floors and ceilings of the computer room.

Penetrations through the walls and floor of the room shall be sealed with a fire-resistant material that provides a fire rating at least equal to the rating of the wall and floor. Air ducts shall be provided with automatic fire and smoke dampers where the ducts pass through fire-rated structure. If pass-throughs or windows are provided in the fire-rated walls of a computer room, then such openings shall be provided with a fire-rated shutter or fire-rated window of rating equal to the wall.

Some clean agents such as the inert gas agents will require vents in the enclosure that open during the discharge of clean agent to prevent excessive pressure build up as a result of the influx of gas in the room. Consult NFPA 2001, ISO 14520, and the system manufacturer for guidance.

11.5 Aisle Containment

11.5.1 Introduction

Aisle containment is rapidly becoming a standard feature in data centers in order to minimize air exchanges between hot and cold aisles and to maximize cooling efficiency (See Section 6.6.4.6). Additional volume spaces may be created by hot aisle containment or cold aisle containment structures and barriers such as ceilings above the aisles, doors and door swings at the ends of aisles, and barriers strategically placed to manage the direction of air flow. Aisle containment introduces challenges for fire prevention, detection, and suppression, especially in existing buildings.

11.5.2 Aisle Containment Construction and Materials

11.5.2.1 Requirements

The objective of fire prevention in data centers is to minimize or eliminate the use of combustible materials. Containment aisles or "hot collars" (e.g., equipment cabinet chimneys, vertical exhaust ducts) shall not be considered to be plenums. Materials used to construct containment structures or barriers shall meet the requirements of the AHJ. For locations where the AHJ does not have requirements, materials used shall have a maximum flame spread index of 50 and a maximum smoke development index of 450 as measured by UL 723 (See Section 6.6.4.6).

NOTE: Standards for combustibility include ASTM E84, *Standard Test Method for Surface Burning Characteristics of Building Materials* and UL 723, *Standard for Test for Surface Burning Characteristics of Building Materials*.

Hinged doors used in hot aisles shall open in the direction of egress. Sliding doors and hinged doors shall meet the requirements of the AHJ and be operable from the inside without the use of hands (e.g., "panic hardware") as allowed by the AHJ.

Doors shall meet one of the following criteria:

- Not lockable from the outside
- Designed for lock-out/tag-out (LOTO) to prevent locking a worker inside the space
- Designed to lock from the outside but open from the inside without a key

Releasing devices, if used to remove ceiling panels or other obstructions, shall be listed for the application.

11.5.3 Detection Systems in Contained Spaces

Containment systems, by their very nature, modify and obstruct the natural air flow in a data center, creating challenges for detection systems. The objective of data center detection systems is to identify the precise source of incipient fire conditions (i.e., smoke and rising heat) before a condition turns into actual fire. Contained spaces can increase air temperature, contain high air velocity, increase air turbulence, and redirect air flow away from room smoke detectors, thereby making such precision more difficult. For example, temperatures in a hot aisle or hot collar can be as high as 60 °C (140 °F). The typical air exchange rate in a building is a maximum of 60 air changes per hour (ACH), but in data centers—and especially in contained aisles—the exchange rate can be as high as 500 to 1000 ACH, and air velocities can range from 15 m/min (50 ft/min) to as high as 1500 m/min (5000 ft/min).

11.5.3.1 Requirements

Detectors shall be required within the contained space and shall comply with local regulations.

Detectors shall be listed for use in high volume air flow.

When installed in contained hot aisles or hot collars, detectors that respond to high temperatures shall be able to compensate for the high temperatures normally present in such spaces. Typical temperatures in a contained hot aisle frequently range from over 38 °C (100 °F) to as high as 60 °C (140 °F).

11.5.3.2 Recommendations

Spacing of detectors within a confined aisle or hot collar should be based on best engineering judgment to meet site-specific conditions. Sensor spacing will depend upon the type of smoke detectors being used and manufacturer's recommendations for the conditions of use.

If smoke detectors are used to trigger automatic actions, such as closing dampers or activating power shutdown, multiple sensors should be required to verify a condition. Very early warning fire detector (VEWFD) systems can be sensitive to conditions that could lead to false alarms in the turbulent conditions of a contained space. Cross-zone smoke detection might require two types of detection.

11.5.4 Suppression Systems in Contained Spaces

11.5.4.1 Requirements

Suppression systems used within a contained aisle shall meet or exceed the minimum requirements for suppression systems used in the surrounding space and shall comply with local regulations.

Where containment is introduced into existing data centers, fire suppression systems shall be modified when necessary to meet prevailing codes and standards. For example, sprinkler head placement shall meet local code requirement for clearances to walls or other obstructions to dispersal. The system may have to be retested to verify compliance.

Sprinkler or clean agent system dispersal modification requirements may be waived if:

1) Obstructions are removable prior to an emergency dispersal event,
2) Obstruction can be removed without compromising means of egress, and
3) Removal is initiated by an automatic means of smoke detection.

Fusible links, shrinking panels or other heat-responsive triggers shall not be used as a means for triggering removal of barriers to code-required clearances for suppression systems.

Automatic barrier removal, if used, shall remove all obstructions for the entire suppression zone.

For gaseous fire suppression systems:

- Any additional volumetric space constructed for contained closed loop return air shall be added to the calculated total volume requirement for gaseous agent.
- The concentration of gaseous agent, when released, shall not be less inside a contained space than it is in the area outside the contained space.

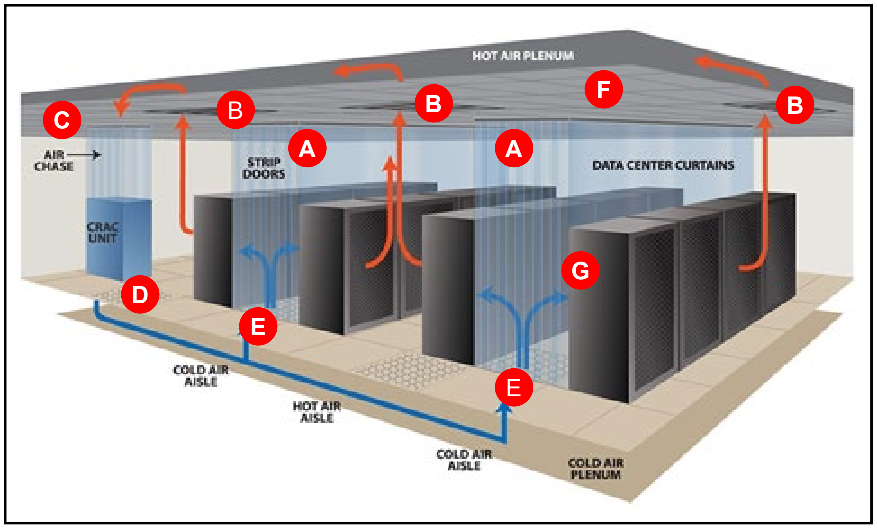
11.5.4.2 Recommendations

Sprinkler piping should be centered at ceiling level within the contained aisle (not above cabinets). Sprinkler heads should be high enough that spray can reach the top of the cabinets on either side of the aisle.

Clean agent nozzles that are too close to a wall or other obstruction can result in “frosting”, thereby reducing the effectiveness of the agent, before the agent has a chance to atomize. Placement of 1.2 − 1.8 m (4 − 6 ft) from the nearest obstruction is recommended.

11.5.5 Additional Information

Figure 11-1 illustrates variations in air flow in contained spaces. Note that Figure 11-1 illustrates cold-aisle containment; it is not meant to illustrate all of the many different variations of aisle containment.



(Illustration courtesy of Tiesche Engineered systems)

Figure 11-1
Variations of Air Flow in a Data Center with Aisle Containment

The following notations in Figure 11-1 indicate the different places where fire detection might be installed:

A. Area monitoring within containment
B. Monitoring at transfer grilles to plenum
C. Monitoring in plenum at return air collection point and prior to entry into HVAC system
D. Monitoring at HVAC supply
E. Monitoring at supply plenum exit points into containment
F. Area monitoring at ceiling
G. In-cabinet monitoring

In a new construction, fire suppression sprinkler pipes on 2.4 m (8 ft) centers grids can be arrayed to meet clearance requirements of most local codes for hot aisle containment and cabinet hot collar containment. Rows will fall on an eight-tile pitch from the center of cold aisle to the center of the adjacent cold aisle. (See Figure 6-5)

Most fires in data centers are presumed to be electrical in nature. Smoke, not heat, is the main cause of damage or injury. Therefore, devices that require heat for activation (e.g., fusible links in sprinkler heads or in drop-down curtains, shrink-activated drop-down ceilings, etc.) are ineffective. If drop-down ceilings and partitions are used, they should be mechanically activated from a smoke detector or other means.

Containment systems can reduce the amount of smoke dilution in a computer room but, at the same time, can increase the smoke dilution within a contained aisle, thereby making it difficult to isolate the specific source of the smoke. Reduction in spacing of detectors based on air change rates within a contained space is typically necessary.

11.6 Handheld Fire Extinguishers

11.6.1 Requirements

Fire extinguishers shall be clearly visible. Each fire extinguisher shall be labeled to describe clearly the type of fire on which it should be used.

11.6.2 Recommendations

Hand-held, clean agent fire extinguishers are recommended and may be required by the AHJ

Extinguishers that use dry chemical agents are not recommended because they can damage electronic equipment.

Switchboard rooms should have clean agent handheld fire extinguishers similar to those used in the computer room.

Handheld fire extinguishers may not be accepted by the AHJ in some jurisdictions as an acceptable alternative to sprinklers.

11.7 Fire Detection

11.7.1 Area Requirements

Table 11-1 lists recommended detection systems for differing data center spaces.

Table 11-1 Recommended Detection Systems for Data Center Spaces

Area	*Detection System*
Computer room	Incipient or early warning intelligent
Network operations center	Incipient or early warning intelligent
Entrance room	Incipient or early warning intelligent
Office	Ionization/photoelectric
Access floors	Photoelectric (where allowed by code)
Electrical distribution rooms	Ionization/photoelectric
Battery and UPS rooms	Ionization/photoelectric
Generator rooms	Thermal or flame detectors
Chiller room	Ionization/photoelectric
Other spaces not listed above	Ionization/photoelectric

NOTE: AHJ requirements may supersede these recommendations.

11.7.2 Detector Technology

11.7.2.1 Addressable Systems

11.7.2.1.1 Recommendations

Provide an addressable, multiplexed, microprocessor-based, electrically supervised fire alarm system for the facility. Design the system to comply with regulatory and code requirements.

11.7.2.2 Design Considerations

11.7.2.2.1 Requirements

The smoke detection system shall be designed to automatically control air supply and exhaust systems and shall be interfaced with the building automation system. Where required, duct-type smoke detectors shall be provided in all ventilation systems.

Smoke detector spacing shall comply with regulatory and code requirements and NFPA 72 or ISO 7420.

11.7.2.2.2 Additional Information

The air velocity of the HVAC system should to be considered as high velocity or turbulent air may require a reduction in smoke detector spacing below normal requirements.

Ionization type detectors are designed to be installed in areas of low air velocity and are not recommended for computer rooms.

Photoelectric type detectors are designed to be installed in areas of higher air velocity. Smoke detectors located in ducts and air plenums should be rated and clearly labeled for use in high air velocity applications.

Incipient air sampling systems are not normally affected by the air velocities found in a typical computer room. Incipient stage fire detection located at the CRAC return air grills provides the most reliable detection. Sample points can be provided in the exhaust air stream from critical pieces of equipment to provide very early warning of equipment overheat.

In many cases, the CRAC can be provided with supplemental built-in smoke detectors intended strictly for internal CRAC system controls. These can be connected to the fire alarm system or BAS.

11.7.2.3 Addressable System, Non-Data Floor Conditions

11.7.2.3.1 Requirements

The system shall provide:

- Smoke detectors in all unoccupied spaces
- Audiovisual notification appliances to meet local code requirements
- Manual pull stations at all exit doors
- Connections from flow/tamper switches to the fire alarm system
- Required interface(s) with the security system. Upon activation, the fire alarm system shall release all security doors
- Monitoring of the fire pump and generators, if provided.

Smoke detectors can sometimes give false alarms. Also, deactivation of HVAC may result in greater hazard than continued air flow, depending upon the design. Where operations are critical and when acceptable to the AHJ, a procedure to control the cessation of air circulation within a room or zone upon activation of smoke detectors shall be permitted.

Fixed temperature heat detectors or flame detectors shall be provided in generator rooms. Temperature set points shall be coordinated with the sprinkler system operation parameters so that the heat detectors will actuate first.

Smoke detectors shall be provided in conjunction with magnetic door holders, where applicable.

Firefighters' control panel, graphic smoke control panel (if required), printer, and annunciator shall be located at the main security office.

Photoelectric and ionization-type smoke detectors shall be provided in UPS equipment and battery rooms.

11.7.2.4 Addressable System Data Floor Conditions

11.7.2.4.1 Requirements

Cross-zoned smoke detectors shall work in conjunction with the pre-action sprinkler system and the clean-agent fire suppression system.

11.7.2.4.2 Additional Information

When an access floor is present in the computer room, photoelectric type detectors may be installed below the floor where permitted by the AHJ.

11.7.3 Early Warning Detection Systems

11.7.3.1 Incipient (Air Sampling) Systems

11.7.3.1.1 Recommendations

In areas where maximum fire protection is required, early warning or incipient type systems should be installed at selected computer room and entrance room locations.

11.7.3.1.2 Additional Information

Early warning or incipient-type systems can be up to 2000 times more sensitive than conventional spot-type detectors.

Consideration needs to be given regarding the level at which incipient systems are used with these systems as premature activation should be avoided.

Incipient control panels may be installed at several locations and connected to the fire alarm control panel.

The air sampling pipe network is a system of copper or PVC pipes installed above or below the access floor with strategically placed air sampling ports. When mounted under an access floor, the pipes are mounted with nonconductive supports to the floor support pedestals midway between data and power raceways.

If added protection is desired, sampling pipes may be run above the ceiling or surface mounted to structures where no ceiling is provided.

A good location for air sampling detection is the return air to the cooling equipment, since all of the air in the room will tend to travel to this location.

11.7.3.2 Early Warning Intelligent Detectors (Alternative to Incipient)

11.7.3.2.1 Additional Information

A class of (spot) detectors provided by several manufacturers is able to detect conditions at the early stages of a fire. The early warning detectors use a combination of laser, infrared, or thermal technology.

The detectors are addressable, which allows for multiple detector protection for pre-action sprinkler and gaseous suppression systems.

The detectors use a processing capability to both learn and automatically compensate for actual conditions.

The detectors should be installed according to codes and manufacturer's recommendations for air velocity and other conditions.

11.8 Fire Suppression

11.8.1 Water Sprinkler Systems

11.8.1.1 Wet System

11.8.1.1.1 Introduction

The wet sprinkler system is a method of fixed fire protection using piping filled with pressurized water, supplied from a dependable source. Closed heat sensitive automatic sprinklers spaced and located in accordance with recognized installation standards are used to detect a fire. Upon operation, the sprinklers distribute the water over a specific area to control or extinguish the fire. Wet systems are applied to the noncritical areas of the data center (see Table 11-2). This system is usually required as a minimum to protect people and property.

As with pre-action sprinkler systems, the wet system may require additional water supplies or fire pumps if there is not enough water pressure available from the utility serving the site (e.g., from the city).

Table 11-2 Recommended Sprinkler Systems for Data Center Spaces

Area	*Sprinkler System*
Computer room	Pre-action sprinkler system
Network operations center	Pre-action sprinkler system
Entrance room	Pre-action sprinkler system
Office	Wet sprinkler system
Electrical distribution rooms	Pre-action sprinkler system
Battery and UPS rooms	Pre-action sprinkler system
Generator rooms	Pre-action sprinkler system
Chiller room	Wet sprinkler system
Other spaces that are not heated and may be exposed to temperatures below freezing (e.g., covered loading dock)	Dry-pipe system
Other spaces not listed above	Wet sprinkler system

NOTE: AHJ requirements may supersede these recommendations.

11.8.1.2 Pre-action Sprinkler System

11.8.1.2.1 Recommendations

The best practice for critical areas is to install a pre-action sprinkler system. This type of sprinkler system provides some safeguard against water damage to the ITE because of an accidental discharge.

11.8.1.2.2 Additional Information

The pre-action sprinkler piping system is similar to the wet system except the piping in the critical areas does not contain water until there is a fire event.

Two events are required before the deluge valve will open and allow water to flow into the sprinkler piping. A single interlock system requires a detection system to operate a valve to flood the fire sprinkler system piping with water. A double interlock system admits water (by opening the deluge valve) in the sprinkler piping upon operation of both detection and a loss of pressure in the sprinkler piping. Both systems have sprinkler heads, requiring a heat rise to open the sprinkler head allowing the water to flow. The interlock system’s designs are intended to prevent accidental water flow in sensitive areas caused by events such as the accidental operation of a sprinkler head or leaks that may develop in the sprinkler piping. Applicable codes and standards require review prior to the application of either of the interlock systems. Types of detection systems include smoke, heat, or other automatic fire detectors such as air sampling detectors or flame detectors.

It is important to note that pendant systems will typically have a column of water in the sprinkler pipe drop from the branch main. The sprinklers should be removed and the pipes drained after system trip testing.

11.8.1.3 Dry Sprinkler Systems

11.8.1.3.1 Introduction

Dry sprinkler systems are similar to pre-action systems in that no water is in the piping until there is a fire event, but their activation system is simpler. The primary difference is that the piping is filled with nitrogen or dehydrated air below the water supply pressure. To prevent the water supply pressure from forcing water into the piping, the design of the dry pipe valve creates a greater force on top of the check valve, where the air is, than under the valve, where the water is. When one or more of the sprinklers heads opens, the air in the piping vents from that sprinkler head(s), reducing the pressure above the valve.

Dry pipe systems are installed in spaces in which the ambient temperature may be cold enough to freeze the water in a wet pipe system. Dry pipe systems are typically not used unless the range of ambient temperatures reaches below 4 °C (40 °F).

11.8.1.3.2 Requirements

Dry sprinkler systems shall not be used in computer room or generator areas of a data center.

11.8.1.3.3 Recommendations

Dry sprinkler systems should be used only in spaces that do not have HVAC and are exposed to ambient temperatures. Dry sprinkler systems are recommended for areas such as outdoor loading docks, parking garages, and unheated storage sheds.

11.8.1.4 Fire Protection Interfaces

11.8.1.4.1 Additional Information

Interfaces to the fire protection system include:

- Fire detection/control/alarm (Section11.8)
- Building automation system (BAS) (Section 13.5)
- Security/guard station (Section 12)
- Electrical power control and monitor system (Section 9.7)
- EPO (emergency power off) system (Section 9.3.16)

11.8.2 Gaseous Fire Suppression

11.8.2.1 Clean Agent Gaseous System

11.8.2.1.1 Introduction

Because of the expense involved with replacing the data center equipment and the difficulty of water from overhead sprinklers to reach fire within ITE cabinets, building owners may consider a gaseous fire suppression system. Fire suppression is achieved by developing an extinguishing concentration of a “clean agent” in the fire zone. Clean agents are stored in pressurized cylinders in or near the computer room to keep pipe lengths short, and most systems are designed to fully discharge within 10 to 60 seconds from initiation.

Gaseous fire suppression systems generally fall into 4 categories:

- CO_2 gas and similar gas fire suppression systems that suppress the fire but also make the room atmosphere unsafe to breathe. These are not recommended for data centers.
- Flooding systems that increasing the concentration of inert gas such as Nitrogen sufficient to suppress the fire but not hazardous to health.
- Clean agent gas discharge systems that chemically suppress the fire and are not hazardous to health. These have a low ozone depletion content but are not allowed in some jurisdictions.
- Non-conductive misting systems that chemically suppress the fire.

EN 15004 provides further information on the different types of gaseous suppression system available

11.8.2.1.2 Requirements

Where clean agent gaseous fire suppression systems are used, the extinguishing concentration shall be maintained long enough for the materials that have been heated by the fire to cool sufficiently so that the fire will not reignite. Standards, such as NFPA 2001, require that 85% of the design concentration be maintained at the highest level of combustibles in the protected space for at least 10 minutes or for a time period long enough to allow for response by trained personnel.

Protection shall extend to all areas of the computer room within the fire-rated envelope. If a separate gaseous agent system is provided for protection of the space under an access floor, it shall be arranged to discharge simultaneously with the gaseous agent system protecting above the access floor.

Subject to the approval of the AHJ, gaseous agent systems may be provided to discharge gas within specific ITE enclosures. Such protection is typically used for automated information storage systems such as automated tape libraries.

Halon 1301 systems shall not be installed in new data centers and not introduced or expanded within existing data centers.

NOTE: Existing Halon 1301 systems may continue in usage unless prohibited by local laws.

Gaseous suppression systems shall not be used within data centers that utilize a direct outside air supply for the cooling systems.

Sufficient air pressure venting for flooding gas systems shall be provided above the protected zone to prevent a gas discharge from causing structural damage.

11.8.2.1.3 Recommendations

The discharge from nozzles on some fire suppression systems can cause noise in excess of 120db, which can cause disk drives to fail. Consider the location of discharge heads and possibility of noise suppressed discharge nozzles.

Preventing the gas leaking from the room or area prior to the fire being extinguished is crucial, as most gaseous suppression systems are heavier than air and are designed to protect a zone some way below the structural ceiling of the room.

Refer to BSRIA AG 17/2002 and other applicable documents for integrating gaseous extinguishing with other systems.

11.8.2.1.4 Additional Information

The air sampling pipe network is a system of pipes installed above or below the access floor with strategically placed air sampling ports. Sample piping material must be approved for use in air plenums when installed in return air ceilings or under raised floors in accordance with the requirements of the AHJ.

11.8.2.2 System Controls

11.8.2.2.1 Introduction

In a gaseous fire suppression system, an automatic fire detection system activates the release of the gas. Two-detector actuations are used to minimize false discharges.

11.8.2.2.2 Requirements

Upon initiation of a stage 2 alarm, system controls shall activate an adjustable time delay prior to activation of the actual release of the suppression gas to allow personnel time to evacuate the area. An abort station for the system shall be located within the computer room and provide the ability to temporarily halt the release of the suppression gas. Halting of the release of the system shall require a continuing manual action (e.g., holding a button/switch). At least one manual release control station and abort control station shall be present in a computer room and located at the exit doors.

11.8.2.2.3 Recommendations

Actuation of one detector should initiate a stage 1 alarm, consisting of audible alarms and automatic notification to the central station or fire/security monitoring system.

Actuation of a second detector should initiate a stage 2 alarm, consisting of an audible alarm that is distinct from the first stage alarm. Discharge commences after a time delay of no greater than 30 seconds, subject to approval by the AHJ.

The abort station should not restart the discharge delay sequence.

A land-line telephone and fire extinguisher should also be located at each exit and emergency station. A land line is an analog line served directly by the service provider and that bypasses the owner’s PBX, voice gateways, or other voice systems.

11.8.3 Oxygen Depletion Systems

11.8.3.1 Introduction

There are systems available which continuously monitor the oxygen content in the air and reduce this to a point where fire will not burn but it is not hazardous to health individuals for up to 6 hours per day. The oxygen content in the air is equivalent to that found at an altitude of approximately 2000m (6500 ft).

The integrity of the room is crucial to allow the system to maintain the lower oxygen content. Consequently, the systems will not work in data centers that utilize a direct outside air supply for the cooling systems.

The energy use of the system is not large but may increase the PUE by a few tenths.

The system will not work quickly enough to extinguish a fire that has already ignited but can be controlled to be active only when the data center is unmanned.

11.9 Fire Alarm Systems

11.9.1 Introduction

The elements of a fire alarm system include:

- Primary power source
- Secondary power source
- Control panel
- Detection and initiation devices
- Notification devices

Figure 11-2 provides an example of a basic fire alarm system. Fire alarm systems are scalable by the addition of additional panels and devices.

Classes of fire alarm systems; whether wired, wireless, or IP-based, generally fall into one of three types:

- Protected Premises – This system is a closed protected system, meaning the entire system is contained to the entire campus or single building. This is protected by a single fire and detection alarm system and is under common ownership and use.
- Supervised – This system embellishes on a protected premises system and is continuously monitored by a central monitoring entity for any abnormal events. The central monitoring entity is responsible for dispatching, reporting, or similar functions in response to alarm initiation.
- Household – This system is typically for private residences with sleeping occupancies.

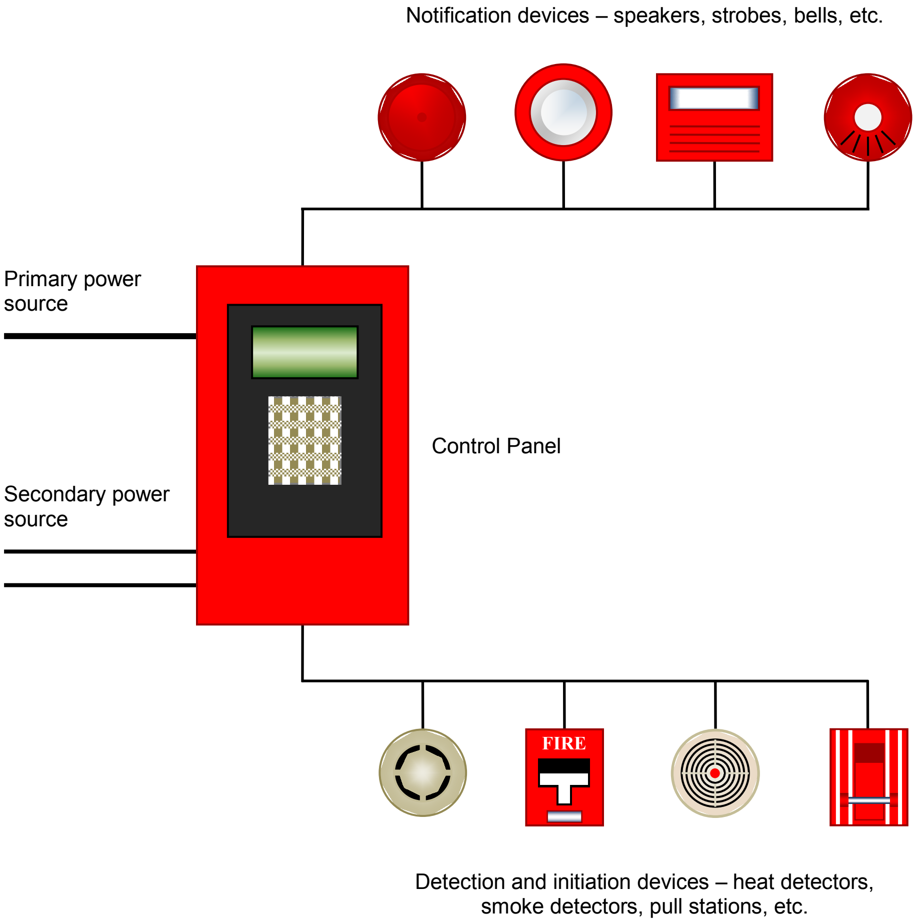

Notification devices – speakers, strobes, bells, etc.
Primary power source
Control Panel
Secondary power source
FIRE
Detection and initiation devices – heat detectors, smoke detectors, pull stations, etc.

Figure 11-2
Basic Fire Alarm System

11.9.2 Requirements

Where not otherwise required by codes and the AHJ, fire alarm systems and their related elements shall be tested and listed by a nationally recognized testing laboratory (NRTL) for the purpose for which it is intended.

As applicable, communication cabling and related ICT infrastructure for fire alarm systems shall meet the requirements of ANSI/BICSI 005.

11.9.3 Additional Information

Some fire alarm systems may utilize network cabling to connect fire alarm or mass notification devices and appliances, provided requirements of the AHJ are met. Use of network cabled fire alarm systems may provide advantages, such as a decrease in overall wiring utilized in the premise, lower time required to locate and correct faults and a decrease in overall equipment required.

11.10 Labeling and Signage

11.10.1 Requirements

All devices shall be labeled with the fire alarm circuit, zone, or address.

Junction boxes shall be painted red or as required by AHJ.

11.10.2 Recommendations

Labeling and signage practices for the fire protection system should include the following:

- Emergency procedures should be posted on all fire alarm control panels and annunciator panels.
- Fire alarm manual stations should be clearly labeled to avoid any confusion. Where permitted, install a cover over these manual stations to avoid accidental triggering.

11.11 Testing and Quality Assurance

11.11.1 Requirements

Startup and commissioning for the fire protection system shall follow those required by applicable standards, regulations, and the AHJ.

11.11.2 Recommendations

Pre-action sprinkler systems should be trip tested at least once every three years.

11.12 Ongoing Operations

11.12.1 Requirements

Site operations and maintenance procedures for the fire protection system shall follow as a minimum those required by applicable standards, regulations, and the AHJ.

11.12.2 Recommendations

Clean agent systems should be maintained in accordance with manufacturer’s instructions and either NFPA 2001 or ISO 14520.

12 Security

12.1 Introduction

Applicable to any data center, in part or in whole, regardless if it is being proposed, built, in current operation, or undergoing renovation or expansion, this section provides requirements, recommendations and additional information about physical security practices and countermeasures necessary to protect the confidentiality, integrity, and availability of a data center. Operational security requirements or recommended practices that may affect a data center's design is also presented.

NOTE: Additional data center operating information may be found in BICSI 009.

There is no guarantee of security implied; however, compliance with the requirements listed in this section should provide an acceptable level of security.

No single countermeasure provides effective security. All architectural, operational, and physical security measures (see Figure 12-1) are intended to do one or more of the following individually and collectively:

- Delay
- Deter
- Detect
- Decide
- Act

Modern data centers are composed of layers of technical, administrative support, and end user space supporting a single or multiple computer room(s) with various amounts of data processing and storage capabilities. Depending on the number and types of potential threats, providing physical security for the data center can encompass the full range of security needs for the site, zones, buildings, rooms, and areas, including:

- Access control devices
- Architectural design
- Barriers
- Detection and alarms
- Guard services
- Surveillance

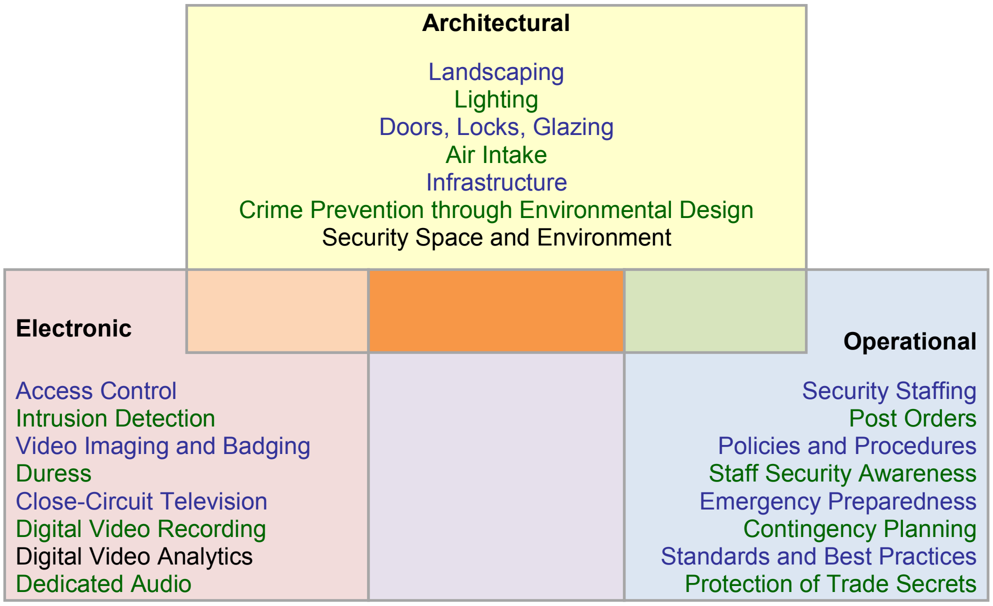


Figure 12-1
Security Measures

12.2 Definitions

Definitions that apply specifically to the security section of this standard:

- *asset*—an employee, contractor, or any physical, technological or intellectual possession.
- *barrier*—a fabricated or natural obstacle used to control access to something or the movement of people, animals, vehicles, or any material in motion.
- *clear zone*—an area separating an outdoor barrier from buildings or any form of natural or manufactured concealment.
- *compartmentalization*—the isolation or segregation of assets from threats using architectural design or countermeasures, including physical barriers.
- *countermeasures*—the procedures, technologies, devices or organisms (dogs, humans) put into place to deter, delay or detect damage from a threat.
- *layering*—the use of many layers of barriers, other countermeasures, or a mixture of both used to provide the maximum level of deterrence and delay (see Figure 12-2).
- *natural barrier*—any object of nature that impedes or prevents access, including mountains, bodies of water, deserts, and swamps.
- *psychological barrier*—a device, obstacle, or lack of obstacle that, by its presence alone, discourages unauthorized access or penetration.
- *risk*—the likelihood that a threat agent will exploit a vulnerability creating physical or technological damage.
- *secured environment*—an area defined within the data center or within the site facilities that has security measures to control physical access to in-scope systems.
- *structural barrier*—something that physically deters or prevents unauthorized access, movement, destruction, or removal of data center assets.
- *threats*—the agents by which damage, injury, loss or death can occur; threats are commonly classified as originating from temperature extremes, liquids, gases, projectiles, organisms, movement or energy anomalies.
- *vulnerability*—a physical, procedural or technical weakness that creates opportunity for injury, death or loss of an asset.

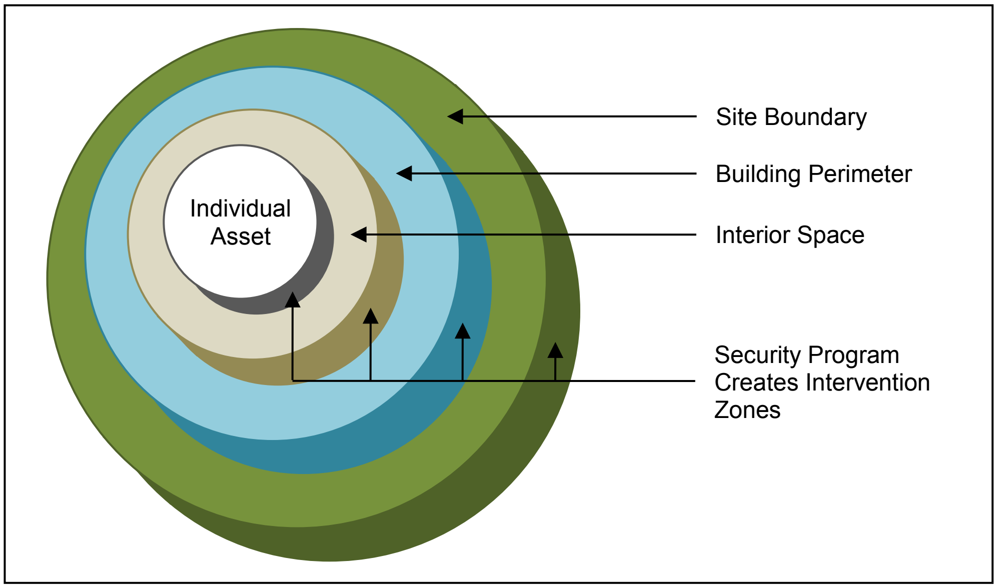


Figure 12-2
Security Layers

12.3 Data Center Security Plan

12.3.1 Introduction

A data center security plan is a document or set of documents providing the framework, policies, and procedures to establish security for data center staff, contractors, and visitors along with the ITE, network technology, telecommunications assets, and the sites and buildings that house them. The data center security plan typically includes the following elements:

- Physical security plan
- IT/cyber security plan
- Disaster recovery plan
- Emergency operation and other required action plans (e.g., regulatory, insurance) specific for the site

12.3.2 Recommendations

The data center security plan should be comprehensive, but easy to read and understand.

Prior to creation of a data center security plan, the data center operator, security architect, or designer should conduct a thorough risk assessment of the existing or future site, buildings and demographics of the data center. A security assessment for the data center should performed during the preplanning and planning stages of construction, and data center security plan should address all areas of potential risk identified. The security assessment should be performed by the security consultant, architect, and engineer team, and contain the following actions and items:

- Manage threat assessment (e.g., identification, frequency, impact)
  - Evaluate potential environmental threats to property
  - Identify potential threats to physical access to the data center
  - Evaluate potential threats to data integrity and information assurance
  - Identify potential threats to human life or safety
  - Evaluate frequency of potential threats
  - Quantify impact if a security breach were to occur
- Coordinate security audit (e.g., building inspections, security surveys, security analysis)
  - Conduct a survey of the facility to evaluate current environmental conditions and security controls
  - Conduct a survey of the facility for controlled access to restricted areas
  - Conduct a survey to determine current security surveillance measures
  - Conduct an audit of current network security controls
  - Conduct an attempt to gain access to the data center network
  - Analyze and interpret regulations affecting data center operations
- Verify against objectives (ascertain security status, current state, protection levels)
  - Determine threat history
  - Interview data center personnel to ascertain criticality of assets
  - Analyze threat history and current security countermeasures
  - Develop framework for security Plan
- Identify countermeasures (e.g., physical, electronic, organizational)
  - Determine layers of security plan
  - Identify environmental security countermeasures
  - Identify manned security countermeasures
  - Identify personal identification requirements
  - Identify level of entrance security
  - Identify access security
  - Identify surveillance countermeasures
  - Identify network security methods and hardware
  - Identify physical security methods and hardware
  - Identify security alert method

List continues on the next page

- Coordinate cost benefit/feasibility/present value studies
  - Evaluate value of assets
  - Determine cost of countermeasures
  - Perform a cost analysis of countermeasures vs. value of assets
  - Determine countermeasures to be applied to facility
- Translate client's disaster recovery plan (DRP) requirements into recovery design recommendations
  - Identify types of potential disasters and the impact to facility
  - Determine short-term and long-term impact of security breach
  - Identify personnel required to carry out disaster recovery plan
  - Develop a disaster recovery plan
  - Implement systems in overall data center design

12.3.3 Physical Security Plan

12.3.3.1 Requirements

A physical security plan shall be created and followed for the data center and the entire building or campus where it is located.

12.3.3.2 Recommendations

During construction on any existing data center, enhanced temporary security measures should be put in place.

12.3.3.3 Additional Information

Historically, the policies, design, practices, technology, and personnel utilized to protect physical assets have been separate from those used to protect ITE and its data. The increasing use and importance of devices that create data, when combined with the increasing sophistication of the attacks and frequency of attempts to capture or compromise that data, requires a move toward a more holistic type of security. Such security will require the data center operator to consider both physical and IT countermeasures.

12.3.4 IT/Cyber Security Plan

The cyber security plan provides security for data at rest and data in motion and protects it from attempts to defeat its confidentiality, integrity or availability through electronic means. Various entities require the protection of sensitive data and the ITE in which such data is stored or by which it is processed or transported. Depending on the size of company and IT dependence, compliance with government, finance, and insurance entities' regulations should have a positive impact on document management, storage management, and the establishment of record retention schedules. Further information may be found in BICSI 009.

Cyber security plans are beyond the scope of this section.

12.3.5 Disaster Recovery Plan

Definitions as defined by NFPA 1600, the standard on disaster/emergency management and business continuity programs:

- Natural events, including drought, fire, avalanche, snow/ice/hail, tsunami, windstorm/tropical storm, hurricane/typhoon/cyclone, biological, extreme heat/cold, flood/wind-driven water, earthquake/land shift, volcanic eruption, tornado, landslide/mudslide, dust/sand storm, and lightning storm.
- Technological events, including hazardous material release, explosion/fire, transportation accident, building/structural collapse, power/utility failure, extreme air pollution, radiological accident, dam/levee failure, fuel/resource shortage, strike, business interruption, financial collapse, and communication failure.
- Human events, including economic, general strike, terrorism (ecological, cyber, nuclear, biological, chemical), sabotage, hostage situation, civil unrest, enemy attack, arson, mass hysteria, and special events.

Additional information on disaster recovery plans may be found in Section 12.9.

12.3.6 Emergency and Other Required Plans

Information concerning emergency operation planning may be found in BICSI 009. The regulatory, financial, insurance, and other legal requirements affecting the operation of a data center will vary widely between countries, regions, localities, and business sectors inhabiting the facility. The data center owner and operator should be familiar with all legal and regulatory requirements concerning privacy, purposeful or accidental disclosure of financial, medical, or personal data, and national security.

Some examples of regulatory and legal documents affecting the operation of the data center include:

- Sarbanes-Oxley
- Industry-specific standards
- US Patriot Act
- Federal Information Processing Standards (FIPS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Blilley (GLB)
- National Association of Security Dealers Conduct Rules 3010, 3013, and 3110
- European Privacy Standards
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
- Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization*

The primary purpose of these rules and regulations are to protect investors, shareholders, employees, and the public from a variety of violations, ranging from accidental disclosure of personal information through the pending collapse of the corporation.

Data center operators, security architects, and designers should avoid viewing these laws and regulations mechanistically, or as a checklist. They should be viewed and approached as a top-down risk assessment.

12.4 Design and the Data Center Security Plan

12.4.1 Introduction

The following items are typically affected by the details found within the data center security plan. This list is not exhaustive, as each data center site and operator may have specific requirements that need to be addressed.

12.4.2 General

The data center should, at a minimum, employ the following protective measures:

- Access control with retention of at least thirty days of access control logs
- Video surveillance system (VSS) with at least thirty days retention of archived footage
- Intrusion detection systems with at least thirty days retention of alarm logs
- Implementing visitor entry control procedures with at least one-year retention of visitor records
- Securing offices, rooms, and facilities
- Protecting against external and environmental threats
- Controlling all access points, including delivery and loading areas

The data center security plan should detail the roles and responsibilities that IT operations and network security can play in supporting the physical security procedures.

12.4.3 Access Control

The control of access to the data center should be addressed in detail by the security plan. Questions answered by the security plan include:

- Who has access to the data center, during what hours and for what reasons.
- If the data center occupies the entire building, how is the security for public areas, loading docks, utility areas, offices, vendor/visitor areas and meeting areas addressed.
- If the data center occupies only a part of the building, how is security to be addressed for common areas with other tenants, elevators, storage areas, risers, normal/emergency pathways, and common telecommunications areas.
- How is access granted, controlled, reviewed and removed.
- How are visitors and contractors managed.
- How are breaches in security policy dealt with.
- Is there a space programming standard that specifies recommendations or a template for each type of space.
- Do some areas, such as the computer room, prohibit sole occupancy by an employee or contractor.
- What levels of authentication are required for access to computer and critical facility rooms.

List continues on the next page

- How are service providers monitored when working in the facility.
- If access control procedures change during non-business hours.
- What types of doors and locks are used for each type of area:
  - Public
  - Semipublic
  - Semiprivate
  - Private
  - Critical facilities, including the computer room floor
- How are keys and badges managed.
- What are the emergency (e.g., fire alarm) event access procedures.

Access restrictions and organizational measures should be taken to ensure that printed or other materials containing confidential information cannot be viewed or removed by unauthorized individuals.

12.4.4 Signage and Display Policy and Procedures

The security plan should identify the wording, readability, and location of signage and displays intended to control pedestrian and vehicular traffic from straying into unauthorized areas.

The plan should address methods of signage and other methods of announcement or reminders to all regarding the observation of non-permanent individuals for compliance with the plan's policies and procedures.

12.4.5 Fire Prevention, Detection, and Suppression

The security plan should contain policy about:

- The type and location of fire suppression equipment.
- The type of protective containers should be used for sensitive material. This may include the reference to or specification of fire-resistance standards.
- The storage of combustible chemicals and materials.
- The fire rating of any containers found in sensitive areas such as trash receptacles.

12.4.6 Monitoring and Alarms Policy and Procedures

The data center should have written guidelines for evaluating emergency responses to all alarms.

The security plan should specify what types of alarms or monitoring systems are used for controlling access to certain areas or devices. Areas of particular concern should be:

- Common cross-connect spaces
- Common riser closets
- Computer room
- Critical facilities rooms/areas
- Elevators and stairwells
- Entrance facilities
- Administrative, HR, and finance departments
- Offices
- Plenum and ceiling spaces
- Telecommunications spaces
- Utility rooms and closets
- Vehicular and pedestrian gates

The security plan should coordinate with the cyber/IT plan how live data and telephone jacks in public or semipublic areas are monitored and secured against unauthorized access. This would include common building areas such as riser closets, common cross-connect areas, entrance facilities and service provider areas.

When applicable, the security plan should coordinate with the cyber/IT security plan, the policy for alarming, and monitoring of computers cases, server cases, and cabinets against the unauthorized access to or removal of discreet components or equipment.

12.4.7 Material Control and Loss Prevention

The security plan should address:

- All aspects of material control and loss prevention for both entry and exit of the data center site, campus, buildings, parking garages, and office areas
- Which materials, including ITE, employees are authorized to bring into and take out of the data center and inspection procedures
- Which materials, including ITE, visitors and contractors are authorized to bring into and take out of the data center and inspection procedures
- Description and control of use for all bring your own device (BYOD) equipment to include electromagnetic emissions and connection to hard and wireless networking
- The inspection and receiving procedures for all deliveries, including authorized points of unloading and personnel authorized to receive deliveries
- Approved methods for disposal of printed materials and magnetic or other media

•

The security plan should specify when property tags, electronic tags, and other identification systems should be affixed to data center equipment and assets.

12.4.8 Surveillance Policy and Procedure

The data center should have written guidelines for evaluating emergency responses to all VSS alarms or incidents.

The security plan should detail:

- Policy for the location and placement of surveillance equipment, including special circumstances noted during the risk/threat assessment.
- Policy and procedure for the protection and secure placement of surveillance devices within offices, work areas, elevators, loading docks, lobbies, parking garages, and exterior areas of the data center.
- Personnel able to authorize special surveillance, covert surveillance, or placement of new VSS equipment.
- The secure placement, storage, and disposal of surveillance tapes and recorded media (servers, storage, and DVR).
- Locations that work may occur outside the range of the VSS with any supervision requirements by or of data center personnel for these locations.

12.5 Building Site Considerations

12.5.1 Introduction

The purpose of building site security is to prevent unauthorized entry or exit by employees and others to determine likely human, man-made, and natural threats and implement countermeasures. Site security also involves the control of pedestrian and vehicular traffic and should ensure that employees, visitors, contractors, and other pedestrians and vehicles can be monitored and inspected as needed.

12.5.2 General Recommendations

All exterior building openings larger than 62,000 mm^2 (96 in^2) should be covered with a security grill using an approved wire fabric and tool resistant 13 mm (0.5 in) steel bars spaced no less than 200 mm (8 in) on center.

All security devices should be installed using security fasteners. Security fasteners eliminate the risk of easy removal and include:

- One-way screws
- Bolts
- Non-removable pins
- Setscrews
- Spot welds

Door hinges that mount to the exterior of the door should have non-removable pins, fixed pins, or center pivots.

Burglar-resistant window/door glazing shall meet the following minimum requirements:

- Total thickness of glass laminate shall be 6 mm (0.25 in) plus 60 mil vinyl film “sandwiched” between the glass.
- Glass shall be tempered, tested, and certified to ASTM Class III of F1233 or UL 972.
- If the window is insulated, the laminated assembly shall be on the exterior of the window.
- Bullet-resistant or blast-resistant glazing is recommended in high crime areas or for buildings near parking areas and roadways.

Bullet-resistant material should at a minimum meet UL super small arms (SSA) threat level using UL 972 test methods.

All exterior doors should have a lock with a deadbolt or equal locking capability.

Mortise locks used for security must adhere to BHMA A156.13 standards and must have a deadbolt throw of 25 mm (1 in) minimum.

12.5.3 Lighting

Lighting is one of the primary considerations for providing the security of occupants and assets in the data center. The following types of lighting should be considered for security use based upon their respective properties, life cycle, environmental conditions, and impact on other security systems (e.g., VSS):

- Incandescent
- Gaseous discharge (mercury/sodium vapor)
- Quartz
- Light emitting diode (LED)

Security or protective lighting should consider of one of the four following types:

- Continuous
- Emergency
- Movable
- Standby

Basic security lighting should be provided to protect the safety of pedestrians, vehicles, and assets, as well as preventing concealment for unauthorized access to the data center site or buildings. Lighting should be provided at the following areas (at a minimum):

- Perimeter fencing
- Building perimeter
- All entrance gates—pedestrian and vehicular
- All building entrances and exits
- Vestibules and lobbies
- Gatehouses/guardhouses
- Windows and exterior openings when the risk of unauthorized access through them is determined
- All pedestrian walkways and public areas
- Stairwells

Lighting should meet the minimum levels of intensity, measured in foot-candles, as listed in Table 12-1.

Table 12-1 Minimum Lighting Levels

Area	*Minimum Lighting lx (fc)*
Outer perimeter	1.5 lx (0.15 fc)
Inner perimeter	4 lx (0.4 fc)
Base of perimeter fence	10 lx (1.0 fc)
Vehicular entrances	10 lx (1.0 fc)
Pedestrian entrances	20 lx (2.0 fc)
Restricted structures	20 lx (2.0 fc)
Clear zones	2 lx (0.2 fc)
Parking areas	10 lx (1.0 fc)

12.5.4 Perimeter Fencing and Barriers

Perimeter fencing, because of threats from local crime, breaking and entering, workplace violence, or other concerns, should include the following design guidelines:

- Fencing should be placed along property lines.
- When employee parking is separate from general parking, fencing or barriers should be used.
- Fencing should be placed along street frontage in high crime areas.
- Fencing should be placed along abutting buildings because of local crime concerns.

Perimeter fencing and gates for the data center should be constructed using the following minimum design requirements:

- Constructed of a 2.9 mm (9-gauge) steel wire with 50 mm (2 in) mesh chain link (minimum)
- For aesthetic purposes, vinyl cladding is acceptable
- 2.4 m (8 ft) high with no top guard
- 2.1 m (7 ft) high with top guard (fence height only)
- Installed in a straight line at ground level, no more than 50 mm (2 in) from the pavement, hard ground or concrete
- Ties fastening the fence fabric to the posts and rails should be 2.3 mm (11-gauge) steel or screw type fasteners

The top guard should face outward and upward and be constructed at a 45° angle. The top guard should only increase the height of the fence by 300 mm (12 in) but should have three strands of double-twisted, four-point barbed wire mounted 150 mm (6 in) equidistant apart.

When fencing is adjacent to vehicular traffic lanes or parking areas, it should be protected by wheel stops, curbs, bollards, or guardrails as required.

When possible, clear zones should be established on either side of the fencing. The planting of even low shrubbery or plantings should be avoided if possible, but at a minimum should be placed no closer to the fence than 0.6 to 0.9 m (2 or 3 ft). Trees or other plantings should never provide points of concealment or assist in unauthorized access to the facility or site.

Signage should be placed on the fence warning of restricted or limited access. All security signage should be placed at 30 m (100 ft) intervals and 1.5 m (5 ft) above the ground.

The following special areas are known to cause breaches of the perimeter and will increase the risk of unauthorized entry:

- Sidewalk elevators
- Utility tunnels
- Storm sewers
- Piers, docks, and wharves

12.5.5 Automotive Threats and Concerns

Because of concerns over vehicle bombs, the following recommendations should be followed when designing parking areas and site traffic control:

- Maintain a minimum perimeter of 30 m (100 ft) from the building.
- Utilize concrete barriers at the curb.
- When possible, have all cars park at a distance from the building.
- Reduce or eliminate underground parking immediately under the data center building.

If possible, data centers should not be located in buildings adjacent to mid or high-rise parking garages.

If possible, elevators should never go directly from the parking garage to office space. Elevators should open and discharge into the lobby.

Parking garages should contain emergency phones or intercoms spaced no less than every 18 m (60 ft). Each telephone or intercom should be clearly marked as such and should be illuminated with blue or some other locally accepted color associated with police or security.

Any onsite parking facility should address the security of pedestrian and vehicular traffic. Surveillance is crucial for security in parking garages and is capable of providing adequate coverage. Key considerations in protecting property and safety include the placement of cameras in the following locations:

- Entrance and all exits
- Guard and cashier booths
- Elevator lobbies and elevators
- Ramps, driveways, and emergency call stations

The following is a list of potential threats that should be considered when assessing the risk of parking areas within or adjacent to data center buildings:

- Assault
- Carbon monoxide
- Chemical, biological, radiological, nuclear, or explosive incidents
- Explosion
- Fire
- Medical emergencies
- Robbery
- Terrorism
- Theft

12.5.6 Threat History

Historical information should be gathered during the planning for any security system design whether new or retrofitted into an existing data center. Typical information gathered during this investigation would include:

- Within the past 5 years, has anyone been successful at this location in damaging any part of the site or data center facility?
- What is the frequency of natural disasters for the data center site? What types of natural disasters have occurred and how often?
- Have any natural, technological, or human disasters rendered the data center or any business at the site inoperable within the last 5 years? Ever?
- What is the frequency of the following within a 1.6 km (1 mi) radius of the data center facility:
  - Assault?
  - Armed robbery?
  - Auto theft?
  - Burglary?
  - Drug trafficking?
  - Fires?
  - Floods?
  - Hurricane/tornado/cyclone?
  - Kidnapping?
  - Murder?
  - Terrorism?
  - Riot?
  - Vandalism?
  - Workplace violence?

The most common threats to all personnel should be identified, and training should be conducted to address these risks.

Employees should be trained to ensure that they act appropriately in high-risk situations such as workplace violence, sabotage, kidnapping, natural disasters, and robbery.

12.5.7 Natural Threats and Concerns

See Section 5 for factors regarding the location and site selection of the data center.

12.5.8 Chemical, Biological, Radiological, Nuclear, and Explosives

Preparation for potential CBRNE threats should be conducted by security and operations personnel for each data center. Each data center should:

- Include CBRNE threat response in the security plan
- Classify threats and the appropriate response
- Include coordination with local EMS and law enforcement
- Include the CBRNE response in the disaster recovery/business continuity planning process

Explosions, whether accidental or because of sabotage, workplace violence, or terrorism should be considered as a threat to the data center building and computer room. The risks associated with explosions or bombs include:

- Injury or death of occupants
- Structural damage to the building
- Damage to the equipment and contents of the building
- Interruption of operations (downtime)

12.5.9 Medical Disasters and Epidemics

The data center should have personnel trained in first aid and cardiopulmonary resuscitation on duty anytime the data center site or buildings are occupied.

First aid supplies should be located in places and marked for easy identification and quick access in the event of an emergency.

First aid supplies should include automatic defibrillator(s) in a quantity recommended by the manufacturer to serve the number of occupants and buildings.

12.5.10 Crime Prevention Through Environment Design

12.5.10.1 Recommendations

The crime reducing concepts and strategies of Crime Prevention through Environmental Design (CPTED) should be followed during the planning process of the design or retrofit of a data center. There are three underlying principles of CPTED. They are:

- Natural access control
- Natural surveillance
- Territorial enforcement

12.5.10.2 Natural Access Control

The data center security architect or designer should utilize natural access control (e.g., placement of doors, fences, lighting, landscaping, other natural or architectural features) to guide pedestrian traffic as it enters and leaves the site, campus, building, or a room or space inside the building.

Each data center room and area should be classified by the level of protection required based upon the sensitivity of the equipment or activity occurring therein. Each area of a data center, including all support areas, closets, critical facility areas, utility and service provider areas, loading docks, lobbies, equipment yards, and offices should be classified into one of five basic CPTED space types:

- Public, used to designate areas that are available for all pedestrian traffic. Public areas could include lobbies, dining areas of restaurants or cafeterias, parking garages, and hallways or sidewalks outside of the controlled access areas.
- Semipublic, which is a term describing areas that are usually accessed from public areas, but not available to everyone. These areas might include conference rooms, restrooms, or break areas which may be outside the controlled access area or may have limited control.
- Semiprivate, a term used to classify space where natural, physical, or electronic access control is used to control pedestrian traffic. Semiprivate areas would include general office space, walled offices not used for sensitive work, private floors in a multitenant building, and non-critical utility rooms.
- Private, spaces that are restricted from most pedestrians, including unauthorized employees. Typical private areas might include the print rooms, call centers, private manager offices, a bank vault, a surgery suite, and the executive floor of an office tower.
- Critical areas that are restricted and controlled from all pedestrians, except for individuals specifically enumerated in the security plan, corporate policy, and procedure documents. Typical critical areas might include computer room of the data center, utility rooms, power and machine yards, telecommunications rooms (TRs) that contain corporate cabling or services, network operations centers (NOCs), tape rooms and ITE staging rooms.

The concept of natural access control can be found in the following practices, which should be considered during any data center design:

- Place lights and attractive landscaping along the main sidewalk leading to the front door of the business.
- Place vegetation so that there is a clear line of sight only to the desired entrance of a building.
- Use lakes, rocks, hills, and vegetation to reduce the number of potential entrances onto a data center site, campus, or building.
- Develop architectural features to obscure the distinctive features of a data center site and to reduce or eliminate vehicular access to the facility.

12.5.10.3 Natural Surveillance

The concept of natural surveillance relies on the use and placement of physical environmental features, walkways, open spaces, pedestrian traffic patterns, and work areas to maximize visibility of the activity within an area by those outside of it and outside the area by those inside it.

Data center security designers should design the rooms, areas, spaces, walkways, and site so that there are many ways for observers to see unauthorized traffic, activity, or criminal behavior. As much as possible, all areas of the data center buildings and site should make the occupants feel safe and comfortable.

Designers should seek to allow maximum use of technology in the future by not obscuring critical or risk-prone areas during the design of natural surveillance or natural access control. Redesign should allow for continued review of the adjacency of a lower CPTED classified space to a higher classified space and assure proper level of security features and methods between them.

12.5.10.4 Territorial Reinforcement

The concept of territorial reinforcement is to create a sense of community or belonging so that if an unauthorized person strays or intentionally enters an area normally restricted to them, they both feel out of place and at risk of being easily identified as such.

The data center security designer should ensure that the atmosphere contributes to a sense of territoriality. The secure space should produce the feeling or sense of proprietorship or territorial influence so that potential offenders perceive this and are discouraged from entering or offending. One way to accomplish territorial reinforcement is to create clear borders between controlled and public spaces so that potential offenders must cross into an unauthorized area in full view of authorized occupants.

12.6 Data Center Elements

12.6.1 Barriers

12.6.1.1 Introduction

Barriers can be classified into three major groups:

- Building exteriors
- Fences
- Masonry structures

Structural barriers are not impenetrable, but they are primarily used to delay entry so that another system(s) can detect and notify employees, guards, monitoring stations, or law enforcement. At a minimum, good use of barriers will force the intruder to leave evidence of penetration and simultaneously trigger an electronic or human countermeasure.

Structural barriers should be put in place to protect against accidental and intentional explosions. The architect and security designer for the data center should consider the relative resistance to explosion that the various barriers offer. The following list of barriers is organized from the most blast resistance to the least:

- Thick, reinforced concrete walls
- Thick brick or concrete walls without reinforcement
- Reinforced concrete walls
- Thick earthen barricades
- Building walls with steel frames
- Sturdy wooden frame walls
- Common brick walls
- Wire-reinforced glass
- Common glass

Table 12-2 demonstrates the thickness of a concrete wall needed to protect from the secondary damage caused by projectiles launched by an explosion at varying distances:

Barriers should be designed in layers so that the asset(s) that need to be protected lie behind or inside multiple levels with the objective of each barrier to create as much delay as possible.

Barriers should also be used to prevent or delay the unauthorized movement or removal of objects by employees, visitors, contractors, or other occupants.

Barriers should be used to delay or prevent access to or damage to the site, buildings, or areas of the data center.

Table 12-2 Thickness of Concrete Wall for Projectile Protection

Distance from Explosion *m (ft)*	*Projective Velocity* *m/s (ft/s)*	*Concrete Wall Thickness* *mm (in)*
30.5 m (100 ft)	610 m/s (2,000 f/s)	305 mm (12 in)
69 m (225 ft)	610 m/s (2,000 f/s)	254 mm (10 in)
152 m (500 ft)	457 m/s (1,500 f/s)	178 mm (7 in)
274 m (900 ft)	305 m/s (1,000 f/s)	127 mm (5 in)
716 m (2,350 ft)	152 m/s (500 f/s)	64 mm (2.5 in)

Source: *Protection of Assets Manual*, ASIS International

A barrier can also be utilized to prevent visual access to a building or asset. Preventing visual access will prevent the potential offender from knowing the location of the asset or that it even exists. An example of a visual barrier would be locating a data center inside an old warehouse or inside of a dense forest with no visual clues of its existence.

Barriers should be utilized to delay or prevent three types of penetration:

- By force
- By deception or stealth
- By accident

When barriers are used outdoors, a clear zone free of anything that could offer concealment, such as trees, weeds, rubbish, small buildings or vehicles, should be maintained.

Guidelines for clear zones around barriers used at data center site perimeters include:

- Clear zones should be maintained on both sides.
- The outside of the barrier should be at least 6 m (20 ft) away from all potential visual obstructions, including buildings, roads, parking lots, and natural objects like trees, rocks, and hills.
- The inside of barriers used for a perimeter should maintain a clear zone that is at least 15 m (50 ft) away from any building or other asset.

12.6.1.2 Vehicle Barriers

The data center architect and security designer should take into consideration the escalating use of vehicles to both inflict primary damage to buildings and persons (intentional and accidental), as well as a delivery mechanism for explosive devices.

Barriers that should be considered when designing protective barriers for the entrances and other vulnerable areas of the data center site and buildings include the following:

- Fences
- Metal highway guard rails
- Concrete vehicle bollards and barriers
- Concrete Jersey barriers
- Metal beams or posts
- Combinations of material such as tires, railroad ties, and earth

Table 12-3 illustrates the vulnerability of various barriers to penetration by vehicles.

Table 12-3 Vehicle Barrier Comparison

Barrier Tested	*Vehicle*	*Barrier Damage*	*Vehicle Damage*	*Occupant Injury*
Chain link fence	3/4 ton pickup truck	Full penetration	Paint scratched	No injury
Double swing gate	3/4 ton pickup truck	Full penetration	Slight dents	No injury
Chain link fence with 19 mm (0.75 in) cable	3/4 ton pickup truck	Full penetration, vehicle stopped, cable held	Extensive front end damage	Risk of injury
Concrete media barrier	3/4 ton pickup truck	No penetration	Major damage	Risk of injury
Tires	3/4 ton pickup truck	No penetration	Major damage	Risk of injury

Source: *Barrier Technology Handbook*, Sandia Laboratories

12.6.1.3 Building Exteriors

Building exteriors should be evaluated for their ability to delay potential attacks on the data center.

During data center planning, the ability of all building surfaces should be evaluated for their performance as security barriers. Existing structures being retrofitted as a data center should include both a physical survey of the structure and a review of available architectural drawings created during initial design and construction.

Evaluation of the architectural drawings and physical inspection of an existing building for the effectiveness of any wall, ceiling, or floor should consider the following metrics at a minimum:

- Amount of space existing between walls, ceiling, and floors
- Risk introduced by the existing or updated HVAC air handling spaces
- Modification of the original walls, ceiling, or floors
- Weaknesses revealed during the physical inspection
- Rooftop accessibility from adjacent structures
- Underfloor accessibility through tunneling
- Underfloor accessibility through drainage tunnels, subways, and other subterranean passageways

The six walls (floor, ceiling, and vertical walls) of any structure housing a data center should be composed of reinforced concrete or other masonry components because of the increase in penetration time over other commonly used materials.

12.6.1.4 Concrete Walls

Concrete walls make excellent barriers and offer excellent psychological deterrence and physical delay. Success in using concrete walls as barriers will depend on the thickness of the concrete and materials used for reinforcement. General guidelines for concrete walls can be found in the following sections.

Concrete or block walls that are used to support structural loads are not necessarily designed to provide enough delay to be an effective barrier. Unreinforced concrete walls offer little protection from penetration. For the security of a data center, all concrete walls should include steel reinforcing bars or rebar. Table 12-4 demonstrates the speed at which a 300 mm (12 in) thick reinforced concrete wall can be penetrated.

Concrete block walls that do not include a reinforcing material offer almost no resistance to penetration using small hand tools. When used for data center construction, concrete block walls should include some type of reinforcing methodology, typically filling the hollow core with concrete or mortar, installation of rebar, or both:

- 100 mm (4 in) thick reinforced concrete walls are typically used for curtain walls and provide little resistance to penetration with hand tools.
- 150 mm (6 in) thick reinforced concrete walls offer more delay, but they are still vulnerable to hand tools and small explosions.
- 200 mm (8 in) thick reinforced concrete walls are common as load-bearing structural support walls and can also be penetrated using hand tools.
- Concrete walls of greater than 200 mm (8 in) are usually found only in the construction of vaults or blast-resistant bunkers.

NOTE: Studies have shown that it can take under a minute to create a person-sized hole in a 200 mm (8 in), mortar-filled block wall with a common sledgehammer and only a few more seconds if 13 mm (0.50 in) steel rebar is added.

Table 12-4 Speed Of Concrete Wall Penetration

300 mm (12 in) thick concrete with #5(16 mm) rebar on 150 mm (6 in) centers

People Needed	*Equipment Needed*	*Equipment Weight kg (lb)*	*Minimum Time min*	*Maximum Time min*
2	Explosives, tamper plate, hand hydraulic bolt cutters	22 kg (48 lb)	2.8	8.4
2	Explosives, hand hydraulic bolt cutters	18 kg (39 lb)	2.8	8.4
1	Explosives, platter	102 kg (225 lb)	1.95	5.85
2	Roto hammer, sledge, punch, handheld power hydraulic bolt cutters, generator	73 kg (161 lb)	15.0	45.0
2	Explosives, tamper plate, handheld hydraulic bolt cutters	69 kg (153 lb)	1.4	4.2

Source: *Barrier Technology Handbook*, Sandia Laboratories

12.6.1.5 Building Openings

Building openings generally are utilized for one of the following purposes:

- Entrance (pedestrians and vehicles)
- Exit (pedestrians and vehicles)
- Natural illumination
- Ventilation
- Material movement (loading docks)
- Utility access
- Drainage

Any building opening less than 5.5 m (18 ft) above ground and larger than 62,000 mm^2 (96 in^2) should be protected by a barrier, alarmed or monitored, for use as an unauthorized access point.

Building openings should be at least as difficult to penetrate as the walls, ceilings, or floor of a data center. Table 12-5 illustrates the amount of time needed to penetrate the standard industrial pedestrian door.

Doors are typically built from one or more of the following materials or a combination of them:

- Wood
- Glass
- Metal

The following should be considered when considering the design and construction of doors for the data center:

- If wooden doors are used, ensure that no gap exists between the doorstop and the doorjamb, which would allow shims or levers to be inserted.
- Hinge pins and mounting screws should always be mounted toward the protected side of the door.
- Hinge pins should always be welded or flanged to prevent unauthorized removal.
- When possible, hinges should be fastened through the doorframe, into the wall stud, or other structural member.
- Doorframes should be securely fastened to the wall studs or other structural member.

Windows mounted on the exterior of a data center building shell are designed for provide natural light, natural ventilation, and visual access, none of which are necessary or advisable for the computer room and many of the secured areas of the data center.

Table 12-5 Time to Penetrate Industrial Pedestrian Doors

Penetration Method	*Noise dB*	*Attack Area*	*Time Needed (minutes)*
Explosives	–	Door face	0.5–1.5
Thermal (Oxy-Lance)	70–76	Door face	1.5–2.5
Thermal (cutting torch)	60–64	Door face	2.0–6.0
Power drill	–	Panic bar	0.5
Axe through metal	72–110	Panic bar	1.5–5.0
Axe through glass	76–100	Panic bar	0.5
Lock pick	–	Lock	0.25–5.0
Wrench	–	Lock	0.5
Pry bar	74–76	Lock frame	0.5
Thermal (cutting torch)	60–73	Hinge pins	0.5–1.5
Hammer and punch	72–75	Hinge pins	1.0–3.0
Explosives	–	Hinge pins	1.0–2.5
Crowbar	60–100	Mesh/window	0.5–2.0

Source: *Barrier Technology Handbook*, Sandia Laboratories

The types of windows used in modern construction include:

- Awning
- Casement
- Horizontal sliding
- Jalousie
- Picture
- Projected

Only picture windows should be installed in any exterior walls of the data center shell.

Exterior windows should be included in the security risk assessment and the appropriate mesh or glazing material consistent with the desired delay or blast resistance desired.

If one or more of the walls of a computer room are exterior walls, there should be no windows of any type on the exterior computer room walls.

Exterior windows should never use putty or molding to secure the panes of glass or plastic in the frame. Only frame mounted (grooved) type of window mounting should be permitted for the data center shell.

Table 12-6 should be used as a guide when determining the amount of delay desired for a window.

12.6.1.6 Glazing

12.6.1.6.1 Overview

Glazing is the installation of glass, plastic, or glass/plastic laminates to increase building surface (especially windows and doors) resistance to explosion, impact, fire, or other threats.

When glass is utilized to fill building openings on the exterior of the data center building shell or interior wall openings, consideration should be given to the danger to occupants and equipment should an explosion occur. If interior or exterior glass is broken, the following undesirable events could occur:

- Unauthorized entry
- Physical injury because of sharp glass fragments, especially when they become airborne as the result of an explosion.
- Property damage to data center assets because of airborne sharp glass fragments following an explosion.
- Physical or property damage because of fragments of glass falling.

Table 12-6 Time to Penetrate Windows

Type of Window	*Tool*	*Penetration Time (minutes)*
Glass		
6 mm (1/4 in) tempered	Fire axe	0.05–0.15
6 mm (1/4 in) wire	Fire axe	0.15–0.45
6 mm (1/4 in) laminated	Fire axe	0.30–0.90
14 mm (9/16 in) security	Sledgehammer, Fire axe	0.75–2.25
Plastic		
6 mm (1/4 in) Lexan®, Lucite™, or Plexiglas®	Fire axe Demolition saw	0.05–0.15 0.15–0.45
13 mm (0.5 in) Lucite™ or Plexiglas®	Fire axe Demolition saw	0.05–0.15 0.35–1.05
13 mm (0.5 in) Lexan®	Fire axe Sledgehammer	2.0–6.0 2.0–6.0
25 mm (1 in) Lucite™ or Plexiglas®	Sledgehammer Fire axe	0.05–0.15 0.10–0.30
Glass with enhancements		
Glass with 2.9 mm (9–gauge) mesh	Fire axe, Bolt cutters	0.25–1.35
Glass with 19 mm (3/4 in) quarry screen	Demolition saw Cutting torch	0.75–2.25 1.35–4.05
Glass with 13 mm (0.5 in) diagonal bars	Bolt cutters Hacksaw	0.5–1.5 1.3–3.9

Source: *Barrier Technology Handbook*, Sandia Laboratories

In conjunction and compliance with local codes and safety regulations, tempered glass should always be used in data center windows and doors. It is 3 to 5 times stronger than ordinary glass, and because of the effects of the tempering process, there is a decreased risk of injury and reduced fragment size of glass fragments following an explosion or penetration.

Plastic or polyester film should also be considered as a method to reduce the risk of injury, damage, and penetration from explosion or forced entry. Film reinforced windows reduce the fragment hazards by retaining glass fragments following an explosion or shattering incident.

Wired glass should also be considered for use in both interior and exterior installations. Many fire and safety codes require the use of glass with wire mesh embedded. It is important to note that while wired glass offers resistance to penetration from large objects, it offers little or no protection from shattered glass fragments or smaller projectiles.

Laminated glass, consisting of alternate layers of glass and plastic, should be considered for any window or door where impact resistance is essential. Tempered, wired and film reinforced glass all resist the initial impact, but they frequently fall away allowing unauthorized entry. Conversely, laminated glass remains in place and retains the ability to deter and further delay entry.

Some laminated glass has electrical properties that permit its use as an alarm. During the attempted penetration of the glass, an alarm is triggered allowing a) the sounding of audible burglar alarms or b) security or law enforcement personnel to gain valuable response time.

Because of their overall strength and resistance to breakage, designers should consider the use of acrylic and polycarbonate-based windows and door glass. These materials are approved for safety and have up to 17 times more resistance to breakage than glass of comparable thickness.

12.6.1.6.2 Bullet Resistant Glass or Glazing

If the threat of gunfire or other projectiles is present, the data center should consider the use of bullet-resisting glass. It is important to fully evaluate the nature and type of attacks being protected against since bullet-resisting glass is available in a variety of thicknesses (19 mm [3/4 in] to 119 mm [4.7 in]) and construction. Attacks can range from individuals with rocks or hammers to high-powered rifles, machine guns, or missiles. It is important to properly assess the risk and threat before selecting bullet-resisting glass.

Security designers should consider the eight levels of resistivity defined in UL 752, which quantifies resistivity based upon the ammunition used and shot pattern or placement:

- Level 1—4.8 mm (3/16 in) thick, solid, open-hearth steel with a tensile strength of 344,738 kPa (50,000 psi) or 9 mm full copper jacket with lead core, 124 grain at 358 m/s (1,175 ft/s) – 3 shots
- Level 2—0.357 Magnum lead soft point, 158 grain at 381 m/s (1,250 ft/s) – 3 shots
- Level 3—0.44 Magnum lead, semiwadcutter gas checked, 240 grain at 411 m/s (1,350 ft/s) – 3 shots
- Level 4—0.30 caliber rifle lead core soft point, 180 grain at 774 m/s (2,540 ft/s) – 1 shot
- Level 5—7.62 mm rifle lead core full copper jacket, 150 grain, 838 m/s (2,750 ft/s) – 1 shot
- Level 6—9 mm full copper jacket lead core, 124 grain, 427 m/s (1,400 ft/s) – 5 shots
- Level 7—5.56 mm rifle lead core full copper jacket, 55 grain, 939 m/s (3,080 ft/s) – 5 shots
- Level 8—7.62 mm rifle lead core full copper jacket, 150 grain, 838 m/s (2,750 ft/s) – 5 shots

Supplemental—All tests have a supplemental shotgun test using a 12-gauge shotgun with 1 rifled lead slug, 437 grain, 483 m/s (1,585 ft/s) and the other 00 lead buckshot with 12 pellets, 650 grain, 366 m/s (1,200 ft/s).

12.6.1.6.3 Burglary-Resistant Glass or Glazing

The data center may be at a high risk for burglary because of quantity and value of the ITE located there. Any window or door containing glass should be evaluated for its resistance to burglary. Some of the criteria used to evaluate the resistance of glass to burglary include:

- Single blow impact testing (smash and grab)
- Multiple impact testing
- High-energy impact testing
- Performance

Data center security designers should also be aware of the five classes of protection defined by ASTM F1233, which evaluate and compare security-glazing methods against three metrics:

- Ballistic attack
- Forced entry
- A combination of both

Forced entry testing involves attacking security glazing using a predefined sequence of tools and weapons. The list below each class is in order of occurrence during classification:

- Class I—ball peen hammer
- Class II—ball peen hammer, 38 mm (1.5 in) pipe/sledge, fire extinguisher, sledgehammer, propane torch, ripping bar
- Class III—ram, 100 mm (4 in) pipe/sledge, sledgehammer, propane torch, ripping bar, chisel/hammer, gasoline, angle iron/sledge, sledgehammer
- Class IV—ram, 100 mm (4 in) pipe/sledge, sledgehammer, propane torch, fire axe, sledgehammer, wood splitting maul, chisel/hammer, sledge/hammer, methylene chloride, fire axe, sledgehammer, chisel/hammer, wood splitting maul
- Class V—ram, 100 mm (4 in) pipe/sledge, sledgehammer, propane torch, fire axe, sledgehammer, wood splitting maul, chisel/hammer, sledge/hammer, methylene chloride, fire axe, sledgehammer, chisel/hammer, wood splitting maul

12.6.1.7 Fences and Metal Barriers

12.6.1.7.1 General

Fences should not be considered as a permanent barrier to forced entry. They introduce delay but not prevention and should be layered with other countermeasures like alarms, surveillance, and guards.

Security designers should consider that even 2.4 m (8 ft) tall fencing with three strands of barbed wire could be compromised in less than 10 seconds.

Fencing should be considered useful as a barrier for:

- Psychological deterrent
- Mark property boundaries
- Limited vehicle barrier
- Most small animals
- Casual intruders
- Opportunistic offenders

Fence design must take into consideration the type of risk and threat. Many fences designed to prevent pedestrian entry have little or no delay factor for vehicles. Guard railing along a highway is one type of vehicular fence, which has almost no impact on the delay of pedestrians or animals.

12.6.1.7.2 Chain Link Fencing

The most widely used fencing for security purposes is the chain link fence.

The Chain Link Fence Manufacturers Institute (CLFMI) and ASTM International maintain the specifications intended as the recognized standards for quality of manufacturing and installation.

Recommended design and installation guidelines for chain link fencing include:

- Line posts should not exceed 3 m (10 ft) spans on average.
- Post hole depths should be at a minimum of 600 mm (24 in) plus an additional 75 mm (3 in) for each 300 mm (12 in) increase in fence height over 1.2 m (4 ft).
- Terminal posts should be braced diagonally to the closest line post, if no top rail is present, and with no more than a 50° angle between the brace and the ground.
- If no top rail is used, then top tension wire must be installed.

  NOTE: Top rails can be used as handholds for climbing the fence.
- The fencing fabric should be 2.9 mm (9 gauge) or greater, and the mesh openings should not be larger than 50 mm (2 in).
- Fencing fabric should reach within 50 mm (2 in) of firm ground, paving, or concrete.
- On soft ground, the fencing fabric should extend below ground and can be set into a concrete apron.
- Any bolts or nuts that are used to fasten any hardware to a fence should be spot welded.
- Any opening for drainage larger than 62,000 mm^2 (96 in^2) should have additional grates, fencing, mesh, grills, or other barriers installed to discourage unauthorized access; drainage should not be impaired.
- For additional delay, a top guard, consisting of three strands of barbed wire, spaced 150 mm (6 in) apart and mounted on the top of the fence at a 45-degree angle outward, inward, or both directions should be considered; since the primary purpose of this fencing is to discourage or delay human entry, the fencing should be at least 2.1 m (7 ft) high, not including the top guard.
- In addition to barbed wire, other barrier protection obstacles can be added to the fencing such as spikes and barbed top guards.
- Gates should be the same height as adjacent fencing (including top guards).
- When privacy is required to conceal activity or remove visual identification of high-value or sensitive assets, strips of material can be woven into the chain link fence; plastic, wood, and fabric are all commonly used for privacy applications.
- Chain link fencing should also be considered for service provider areas, storage, and other areas for temporary security or when hard-walled construction is not an option.

A clear zone should be established for at least 6 m (20 ft) on both sides of the fence with anything that could be used as an aid to climb the fence removed. This includes the trimming of overhanging tree limbs. Other items that might be used to go over the fence include:

- Vehicles
- Boxes
- Ladders
- Construction material (e.g., wood, poles, concrete blocks)
- Skids
- Containers
- Equipment

12.6.1.8 Metal and Welded Wire Barriers

12.6.1.8.1 General

Expanded metal fabric consists of sheets of metal (carbon, galvanized, stainless steel, aluminum, and others) that have been cut or shaped and somewhat flattened or thinned for barrier material that:

- Is resistant to cutting
- Will not unravel or uncoil
- Is easy to fabricate and install
- Permits environmental conditioning, lighting, and inspection of secure spaces like storage areas, service provider cages, cabinets, and other data center areas
- Provides enhanced psychological deterrence

Expanded metal barrier material comes in four styles that should be designed for the anticipated risks and threats in the area installed. The four types of generally accepted expanded metal are:

- Standard
- Grate or diamond plate
- Flattened
- Architectural

Welded wire fabric is created by welding a series of wires at right angles forming a wire fabric where at each intersection the wires are welded together.

Welded wire fabric should be used when a less demanding barrier is needed than expanded wire. Other security applications where welded wire is used include:

- Tool rooms
- Utility areas
- Building automation control rooms
- Computer facilities and rooms
- Window guards
- Lockers
- Animal cages (laboratory environment)

Woven wire fabric is considered a barrier, but it is used for less demanding applications, and is not generally acceptable as a security countermeasure.

12.6.1.8.2 Barbed Wire

For the purposes of this section, barbed wire will also include barbed tape.

Although its original purpose was as an animal barrier, barbed wire is an important auxiliary security enhancement for many barriers, including fencing. Primary uses of barbed wire include:

- Fence fabric
- Top guard for chain link or other fencing
- Concertina coils
- Other barriers

The key benefit of barbed wire is that it is a psychological deterrent and should not be designed as a primary countermeasure to induce delay.

Recommended considerations when using barbed wired in a security design include:

- Number of barbs
- Design of barbs
- Location of barbs

To discourage potential intruders from gripping the barbed wire, designs for data center perimeters and other barbed wire installations should specify four-pointed barbs located on 75 mm (3 in) centers.

Barbed wire strands should be attached to posts that are less than 1.8 m (6 ft) apart with distance between the strands never exceeding 150 mm (6 in).

If soft soils, erosion, or small animals create vulnerabilities, then a single strand of barbed wire should be at ground level. This will also discourage tunneling.

For additional delay, barbed wire strands should be formed into concertina coils. Concertina coils are used in the following ways:

- Top guards on fences and other barriers
- Temporary barriers
- Tactical barriers

12.6.1.9 Gates

Data center perimeters should include no more gates than are necessary. Each gate provides more opportunity for operational failures (left unlocked or open) and vulnerability.

Gates can be manual or motor operated and are available in the following styles:

- Single-swing
- Double-swing
- Multifold
- Overhead single slide
- Overhead double slide
- Cantilever slide single
- Cantilever slide double
- Aircraft sliding gates

12.6.2 Lighting

Effective lighting is a key component to an overall security program; it is a powerful psychological deterrent to criminal activities, and it enables security personnel to perform their work more efficiently. A good lighting design will include the following design parameters:

- Higher brightness levels improve the ability to detect objects and recognize people.
- Horizontal illumination levels assist in identifying objects that are horizontally oriented such as streets, sidewalks, steps, and horizontal obstacles; vertical illumination levels assist in identifying vertically oriented surfaces and assist in visual recognition of other personnel from a safe distance.
- Uniformity in the lighting system eliminates harsh shadows around buildings and surrounding areas; this makes the environment safer for pedestrians and drivers.
- Glare is excessive brightness coming from poorly designed or misapplied lighting fixtures or is reflected from glossy surfaces; glare should be minimized to maintain visibility of the area by personnel and video surveillance equipment.
- Horizontal and vertical lighting levels in parking lots and parking garages should be within limits recommended for visual identification. Lighting levels should be uniform with no dark areas around corners or vehicle parking slots where personnel may hide.
- Entrances to buildings should be illuminated at a higher level than the surrounding areas to increase safety and guide visitors into the facility.

12.6.3 Access Control

12.6.3.1 Introduction

Access control is a broad term that is applicable for digital and physical environments. Access control design should provide the following:

- Permit or deny access
- Log activity and create alerts
- Alter the rate of traffic
- Protect occupants, materials, and information against accidental or malicious disclosure
- Prevent injury for people
- Prevent damage for physical systems

Physical access control systems (PACS) are covered in NIST SP800-116 for personal identity verification (PIV) systems but principles are equally valid for general PACS use.

Figure 12-3 shows the levels of access control, and these levels can be applied to data centers as follows:

- Level 0-Public: These are the spaces where there is no need for authentication such as parking lots, cafeterias etc.
- Level 1-Semi Public: These spaces may contain sensitive information and some form of authentication is necessary to control access such as employee or vendor offices.
- Level 2-Semi Private: Entry to these spaces should be limited to specific groups of people such as storage areas or equipment rooms.
- Level 3-Private: These spaces are the most restricted areas and are critical to the mission of the spaces such as computer rooms. Entry is allowed for specific individuals only.

For physical access, historically types of authentication have been identified as follows:

- Type 1: What a person has (e.g., keys, cards)
- Type 2: What a person knows (e.g., passwords)
- Type 3: What a person is (e.g., fingerprint or iris recognition)

Multi factor authentication only applies when more than one type is used by the access control system. However, processing identity information using digital automated systems blur the differences between these types. For example, a password can be used as Type 2 authenticator but is not considered a secret when it is passed over the wire from the keypad to the controller. Further measures are needed to secure authentication.

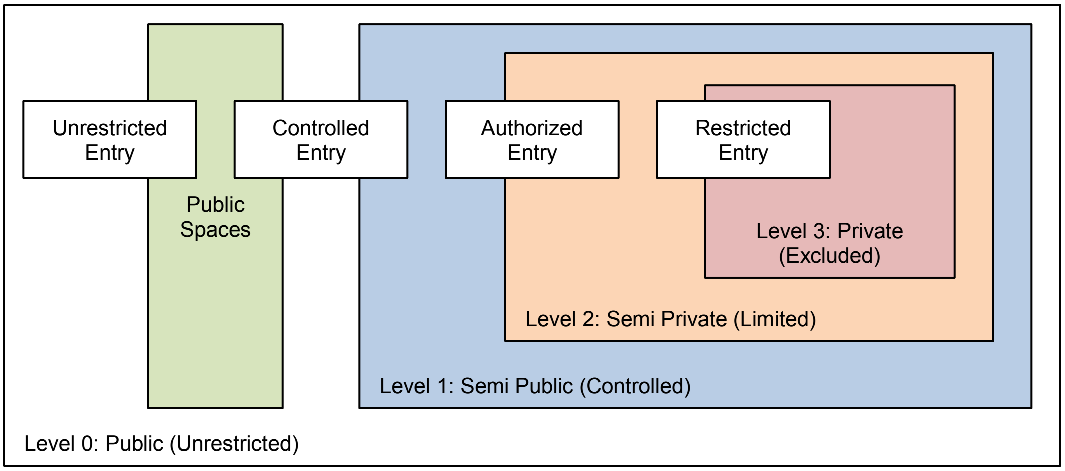

Unrestricted Entry
Controlled Entry
Authorized Entry
Restricted Entry
Public Spaces
Level 3: Private (Excluded)
Level 2: Semi Private (Limited)
Level 1: Semi Public (Controlled)
Level 0: Public (Unrestricted)

Figure 12-3
Levels of Access Control

12.6.3.2 Identity Assurance

Every form of access control must first identify the access requester which is called Identity proofing. This process is explained in great detail in NIST Special Publication 800-63. For the purpose of data centers there are two dimensions for identity assurance, and each has 3 levels to describe the strength of the process.

- Strength of Identity Proofing (IAL1-3)
  - IAL1: No formal identity proofing is required. Any information provided by the requested is accepted as proof.
  - IAL2: At this level, requester should have possession of an authenticator bound to a credential. This can be a form of identity card or physical key.
  - IAL3: At this level, requester should be physically present, and properties should be examined by security provider representative.
- Strength of Authentication Process (AAL1-3)
  - AAL1: Single-factor authentication is used with various secure authentication methods.
  - AAL2: Two-factor authentication is used with secure authentication methods
  - AAL3: On top of two-factor authentication hardware-based authentication (a key through a cryptographic protocol) and impersonation resistance is used.

It is important to make a risk assessment before determining the required IAL and AAL levels.

12.6.3.3 Risk Analysis

It is important to identify different zones in the data center and categorize them according to access levels considering multiple routes of access. Once zones have been identified, a risk assessment should be made to determine strength of identity proofing and authentication process should be selected which will drive the selection of access control technologies such as mechanical locks or electronic access control systems.

Following points should be considered when making the assessment:

- Weight security of personal information to be collected from people that will be using the system with access of personal information.
- Balance ease of use with security. Note that 3-factor authentication is not required on any level and should be used for high risk areas where necessary.
- Cost of acquisition and maintenance for access control systems will increase with strength of authentication. While AAL3 seems necessary for accessing a data center facility, it might not be required if facility is part of a campus.

12.6.3.4 Requirements

All access control systems must be designed according to the following criteria:

- System should provide adequate level of assurance for access control corresponding to the risk of unauthorized access to a designated space.
- System should allow flexibility to change the assurance level over the lifetime of the system. This will provide ease of management where the use of certain space is changed.
- All access control systems must allow emergency egress of the facility in compliance with applicable building codes. The facility designer shall review the applicable life safety code requirements with the AHJ and comply with all AHJ requirements, which can vary from one location to another. The designs, although compliant during the design/redesign period, should not inhibit future changes empowered by changes in AHJ, policy, or procedure requirements to provide the data center with higher levels of security.

All building access points, including maintenance entrances, equipment doors, and emergency exits, shall be assigned a level of access control and utilize appropriate methods of access control for that level.

12.6.3.5 Recommendations

A list should be maintained of the employees and contractors that have been issued keys, access cards, codes, tokens, and badges so that the devices can be confiscated upon termination, confiscated upon change of responsibilities, or to permit the access control codes to be changed.

The access control card system should be configured for multiple levels and multiple areas of access to include temporal changes in access to the more critical areas. Individuals authorized to critical areas, such as the data center floor or critical power and cooling equipment, should be strictly limited as to quantity of staff, need-for access, and permanency of access.

It is important that HR or the department for which an employee or contractor worked immediately notify the "owner" of all access control systems (IT, facilities, or security) when an employee or contractor is terminated or no longer requires access to all areas for which they were/are authorized.

Access control should be coordinated with emergency services personnel with each local agency, including police, fire, and EMS.

When possible, alarms from access control events should transmit to a local or remote location where timely responses or other actions can be initiated. Typical locations include the following:

- Remote contract monitoring company
- Main guard station off-site
- Guard station in another building
- Guard station in the same building

The access control system should be interfaced to the VSS for automated presentation of data to the guard(s) and permanent records.

Where union labor is utilized in the building by the data center corporate enterprise or by another company located in the same building or campus, planning for a labor strike should be included in the security plan, disaster recovery plan, and access control systems.

In the event of a strike, the existing hardware or software authentication should be backed up, and the hardware or software authentication (e.g., locks, access control programming) for striking workers should be temporarily disabled or changed.

12.6.3.6 Locking Mechanisms

12.6.3.6.1 General

Locking mechanisms are grouped into two general categories with a variety of available types and security levels with each one:

Mechanical:

- Warded
- Lever
- Pin tumbler
- Wafer tumbler
- Dial type combination
- Electronic dial type combination
- Mechanical block out devices for equipment ports and cords

Hybrid—electrical and mechanical operation:

- Electric deadbolt
- Electric latch
- Electric strike
- Stair tower
- Electric lockset
- Exit device
- Electromagnetic lock
- Shear lock

The data center security design should include input from the risk, threat, and vulnerability assessment before selecting the appropriate locks for each area.

Planning and analysis should occur during the determination of the types of locking systems to be utilized in the data center. Planning criteria include:

- AHJ restrictions and allowances
- Total number of locks
- Classification of space
- Employee and contractor demographics and turnover
- Type of facility
- Local crime statistics
- Risk/benefit analysis
- Availability and use of other countermeasures

Both the level of skill needed to attack a locking mechanism as well as the psychological deterrence should be considered when selecting a locking mechanism. Among the vulnerabilities of mechanical locks that must be considered when selecting a locking device are:

- Force
  - Separation of the door jamb from the door—door jamb and surround wall materials should be strong enough to meet the delay requirements needed
  - Length of the bolt—a 25 mm (1 in) minimum should be used for all secure areas where risk of attack by force exists
  - Inclusion of an astragal or metal plate covering the gap over the location where the latch enters the keeper
  - Requiring a hardened plate to cover the exposed lock housing and cylinder
  - High-quality pins in pin tumbler cylinders to prevent snapping of the pins and manual rotation of the plug
- Picking
- Taking impressions of keys
- Stealing or unauthorized inheriting keys

12.6.3.6.2 Mechanical Locks

All locks should be meet the highest security grade or criteria for the data center site (e.g., ANSI/BHMA 156, EN 12209, "CP" mark from the Japan Crime Prevention Association). All lock tumblers should be periodically rotated to maintain security as employee and contractor terminations occur. This can be accomplished through rotation of just the tumbler or core or can involve the removal and rotation of the entire lockset.

Locks and keys should never be used as a primary method of access control for computer room doors or other high-value or sensitive areas.

Key control using a single great grand master process is not recommended. This is especially true with larger facilities.

All keys should be coded, included within a comprehensive key control procedure, and have the following words molded or engraved into the key body: *DO NOT DUPLICATE*. When possible, keys should be made on special blanks that are not available to others.

All new installations of door locks should comply with regulatory requirements for disabled occupants. One example of this type of requirements is the ADA, which requires the use lever handles instead of doorknobs.

The security designer for the data center facility should consider the function of the lockset as part of the security, ingress, and egress traffic patterns. Functions of locksets are classified as follows:

- Office, where the handle on either side will operate the latch bolt; locking is accomplished using the thumb turn inside the room or a key on the outside of the room.
- Classroom, where the latch bolt is only operated by the handle inside, or a key outside.
- Institutional, where only a key will operate the latch bolt from either side.
- Corridor, where the same functionality exists as in the office scenario, but the key and thumb turn throw a deadbolt; for safe egress, the inside lever also opens both the deadbolt and the latch bolt.

12.6.3.6.3 Electrified Locksets

Electrified locksets should be a key central design element of any data center security plan. These locksets are locked and unlocked remotely and are commonly layered and integrated with other systems in the electronic access control system.

It is important for the data center security designer to consider the operation of the facility during normal and emergency conditions. The ability to utilize either a "fail safe" or "fail secure" condition for each door must take into consideration the location and emergency egress routes for all occupants as well as the location and risk to high-value equipment and other assets. Failure to design the appropriate lock can create a significant risk of injury or death to occupants because of entrapment or unauthorized entry because of inadvertent opening of doors to storage areas.

A fail-safe lock is one in which the locking mechanism unlocks under any failure condition.

A fail secure condition is where the locking mechanism remains locked under any failure condition.

It is important that fire codes be consulted for requirements for door locking mechanisms and functions. One example of this is the stair tower lock, which releases a dead-locking mechanism if power is removed, allowing the use of door handles.

The electromagnetic lock is an important locking mechanism and secures the door by means of a power electromagnet, which is rated by the force required to open the door when it is energized; typically 2200 N (500 lbf) to 8900 N (2000 lbf).

Combinations of more than one lock type are an important design strategy and should be utilized when attempting to maintain security during normal operation, loss of power, and emergency conditions.

12.6.3.6.4 Cipher and Combination Locks

Cipher locks do not have the ability for multiple codes. The use of cipher locks for computer rooms doors and other high-value or sensitive areas is not recommended because of the high probability of compromise because of "shoulder surfing" and the lack of ability to track entry/exit data.

If cipher locks are used on any door, security, or other data center personnel should verify that the default setting has been changed.

Cipher lock combinations should be changed at least every 30 days; however, 90 days is the maximum time recommended without changing the combination.

12.6.3.7 Doors

NOTE In The US, the following provisions are applicable except as modified by AHJ. However, other countries may have different principles around fail-secure/safe, automatic unlock, and delayed egress.

All doors and other openings associated with the data center (e.g., data center floor, critical facilities rooms and areas, network facilities, etc.) should be provided with status devices (contacts, hinges, etc.) that annunciate and record all events to the access control and permanent documentation system(s).

All normally locked egress doors located within the data center should comply with the required provisions for egress as follows:

- A sensor on the egress side must unlock the door upon detection of an occupant approaching the door
- The locking system is fail-safe
- All doors must utilize listed panic or fire exit hardware that, when operated, unlock the door
- A request-to-exit (REX) manual release device is provided adjacent to the door unlocks the door that meets the following requirements:
  - Has appropriate signage ("PUSH TO EXIT")
  - Directly interrupts power to the door lock (e.g., is hardwired into the door lock control circuit)
  - When activated, unlocks the door for at least 30 seconds
- Initiation of an alarm condition in the facility fire alarm system or activation of the facility sprinkler system automatically unlocks the door, and the door remains unlocked until the fire alarm system is manually reset.

When enhanced security is required in the data center or computer room, exit doors should be equipped with delayed egress locking systems that do not allow egress for a typical period of 15 to 30 seconds after pressing of the exit device for no more than 3 seconds with the following provisions:

- Initiation of an alarm condition in the facility fire alarm system or activation of the facility sprinkler system automatically unlocks the door, and the door remains unlocked until the fire alarm system is manually reset.
- Initiation of the release process activates an audible alarm and visual signal in the vicinity of the door.
- After release, locking shall be by manual means only.
- Signage on egress side of door is provided ("PUSH UNTIL ALARM SOUNDS. DOOR CAN BE OPENED IN 15 SECONDS").

Emergency exits should be monitored and alarmed if the door is opened for any reason without release from the access control system. The delay period should be determined by the amount of time needed for guard response, surveillance activation, or other method activated to monitor the location and reason for the emergency exit alarm.

An interface with the VSS should be provided to permanently archive the buffered video for the period before, during, and after a door alarm condition to allow security personnel to respond to the incident and investigate the incident.

12.6.3.8 Electronic Access Control (EAC) Systems

12.6.3.8.1 Introduction

Also known as *physical access control systems* (*PACS*), these systems are used to authenticate people and grant or deny them access based on certain properties. A good Access Control System should have the following capabilities:

- Should provide a unified secure mechanism to identify and grant or deny access for the facility or campus as a whole.
- Should provide centralized secure logging and searching of all events from all points of entry, including access granted, unauthorized, tampering and device malfunction.
- Should provide access control and logging services even if system components are unable to communicate with any central server.

12.6.3.8.2 General Recommendations

EAC systems should be selected based on facility or campus needs. Automated EAC systems should record all of the following:

- Entry and exit time
- Identification of the entrant
- Authorization mechanism
- Location (and direction if applicable) of access

12.6.3.8.3 Access Cards

Card systems for access control provide a unique access/identification card for every individual with access authorization. Card readers are provided at all designated access entrances to the facility, which interface with the security system and door controls to unlock or open doors when a valid card is presented to the reader.

Access cards have been in use for decades. Due to the advance of computing power, older security features used within the cards have become insecure and provided only for backward compatibility. Especially magnetic stripe cards that do not utilize Integrated Circuits (IC) should be avoided for security reasons. Following features should be considered when looking for new access card implementations:

- *Electromagnetic Properties* – Due to ease of use and sanitary reasons, usage of contactless operations should be preferred. Cards can be used with readers in close distance typically less than 75 mm (3 in). ISO/IEC 14443 family of standards should be selected when selecting access cards. These Cards are also known as proximity cards, use 13.56 Mhz frequency to communicate with the readers and provide more bandwidth between the card and he reader. If usage of cards through contacts are needed, ISO 7816 family standards should also be required.
- *Cryptographic Properties* – Not all cards that have an IC provide enough security. It is recommended that IC is capable of generating public-private key pairs (PKI), validating signatures and storing information encrypted. IC's require card operating systems to function at this level. It is recommended to have a minimum rating of Evaluation Assurance Level (EAL) 4+ for the software and card vendors should be required to upgrade their software for software vulnerabilities found after the release of software.
- *Application Protocols* – Different vendors use different protocols in their implementations with varying degrees of security. Popular implementations have been provided below:
  - *MIFARE* – There are different family of products under this brand, however some do not provide enough security for data center environments. MIFARE Plus SL3 or MIFARE DESFIRE EV1 or higher should be used.
  - *iClass SEOS* – Provided by HIDGlobal, is part of iClass family but is a completely different technology and should be considered for implementation where high authentication levels are required.

12.6.3.8.4 Reader Systems

Figure 12-4 shows an example of a system topology for a reader.

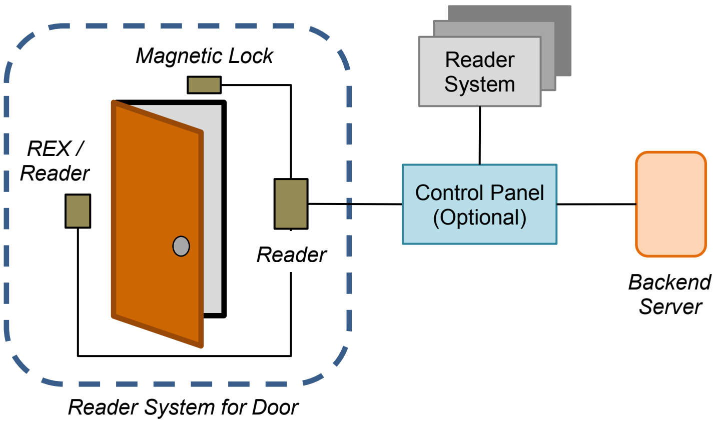


Figure 12-4
Example of an Access Control System Topology

There are 3 types of readers:

- *Basic readers* – These systems pass the information to Control panels through serial protocols and do not make access control decisions. Communications between basic readers and their controllers should be encrypted.
- *Semi-intelligent readers* – These type of reader systems similar to basic reader systems with control panel and control panel acts as credential cache and increase resiliency in case backend server is unavailable.
- *Intelligent readers* – These reader systems, act as the credential cache, make the access decisions and directly communicate to the backend systems over TCP/IP.

In data center environments, the use of combined reader that can read card information, biometric and PIN entry is recommended. When selecting a reader system in general, following should be considered:

- Reader should support various authentication protocols and mechanisms to provide flexibility during implementation.
- Signaling between all components should be secured physically and at protocol level between all components. Especially communications between readers/control panels and backend servers where TCP/IP is used, encrypted communication should be preferred.
- Reader should provide security for the stored keys, password, biometric data on the device.
- Readers using biometric authentication on outdoor settings should be protected from external contaminants such as dirt to facilitate proper operation.
- Vendor should provide software updates for the product in case security vulnerabilities are identified.

For fingerprint scanning:

- A minimum of 250 DPI (dots per inch) rating is required. Specific applications mandated by standards may require higher resolutions such as 500 DPI.
- Live finger detection should be preferred to prevent spoofing.

For face recognition:

- The device should be able to function under all indoor lightning conditions as well as complete darkness.
- Live face detection should be preferred to prevent spoofing by printed images.

12.6.3.9 Special Access Control Applications

12.6.3.9.1 General Recommendations

All electronic card access systems for the data center should incorporate and have active the ability to detect more than one individual going through a controlled doorway with only one card or biometric authentication. Ultrasonic scanning of the mantrap compartment can verify that there is only one individual entering the facility and eliminates the ability of unauthorized individuals to piggyback behind an authorized employee, contractor, or visitor.

All electronic card access systems for the data center should incorporate and have active the anti-passback feature. This feature should only permit one entry without an accompanying exit. When activated, this feature should not interfere with normal and authorized movement within the data center or computer room but limit the ability of more than one employee, contractor, or visitor to use the card for the same ingress or egress.

In high-value or sensitive areas with restricted access, security designers should consider the use of the “two man rule.” This feature of electronic access control systems requires that at least two authorized persons be in any specified area at the same time. When a restricted room or area is empty, two authorized persons must use their access cards within a specific period, typically 45 seconds, or entry is denied and a log entry or some sort of notification is made.

12.6.3.9.2 Mantraps

Mantraps should be designed to provide secure access control, with or without the presence of security personnel, through the use of two interlocked doors on opposite sides of a controlled access compartment. Mantraps can utilize card readers, biometric scanners, and ultrasonic scanning of the mantrap compartment to limit the area to a designated number of authorized personnel able to pass into the secured area. Mantraps can be utilized to control both entry and exit.

In addition to the access control and intrusion sensors, each mantrap should also have the ability to sense chemical, biological, radiological, and nuclear threats within the controlled access compartment.

12.6.3.9.3 Sally Ports

Sally ports consist of a controlled pedestrian or vehicular interior or exterior space secured with two controlled and interlocked doors or gates. Sally ports operate by allowing personnel or vehicles entering the facility to enter the sally port space, and then close the first door before authentication occurs, with the second door being opened only after authentication is completed. Security options that should be considered when designing sally ports for the data center include:

- Designed to facilitate identity verification and authentication while the vehicle and pedestrian is still secured in the sally port space.
- When installed inside a building, sally ports should be able to withstand predetermined levels of explosions.
- Provide safe and isolated location for identification, authentication, and inspection.
- Should have fixed and mobile surveillance to facilitate inspection of vehicles.
- Should have normal and emergency communication equipment installed.
- Should have a secure room with access to the sally port for interviews without the need to leave the sally port area.
- Sally ports can be constructed of a variety of materials, ranging from barriers, such as a chain link fence for outdoor applications to explosion resistant glazed material for the in-building designs.

Sally ports should also be designed to restrict entry to one vehicle at a time to prevent unauthorized entry into the secured space via “piggybacking” or “tailgating”.

12.6.3.10 Turnstiles

If turnstiles are utilized to control pedestrian access to secure data centers, the turnstile should be full height and either integrated with the electronic access control system or monitored and controlled by guards. Half-height turnstiles are easily overcome and provide little security if not augmented by guards or other countermeasures.

12.6.3.11 Gatehouses

Considerations when designing and building gatehouses/guardhouses should include:

- Must provide unobstructed observation in all directions.
- Located in the center of the roadway, providing the ability to stop and inspect vehicles entering and exiting.
- Sufficient access for the volume of vehicles during shift changes and other busy times.
- Traffic arms, pop-up bollards, or other mechanisms to effectively control vehicular traffic.
- Access control for after-hours ingress and egress.
- A turnstile for pedestrian traffic if no inadequate pedestrian traffic control or sidewalks exist or cannot be sufficiently controlled by security staff.
- Buffer areas for those without prior authorization or for handling of employees, contractors, or others who have lost or have problematic identification badges.
- VSS surveillance using multiple cameras to monitor and record images of the driver/passengers, front and rear license plate locations, and a general view of the gatehouse and gate area.
- At least one concrete-filled bollard at each corner of the guardhouse at least 1 m (3.5 ft) high. Metal highway barriers are an acceptable alternate.
- Bullet resistance in high crime areas.

A remote gatehouse/checkpoint can reduce the number of guards or employees needed to secure a perimeter. If a remote gatehouse/checkpoint is used it should have the following features:

- VSS providing images of approaching vehicles, drivers, and optionally, the gate
- Lighting for after dark operation
- Intercom system
- A motor-operated gate
- One or more access control systems (e.g., cards, biometrics, keypads)
- Loop detectors

12.6.3.12 Badging and Identification

The designed badging and identification policy for the site shall be followed. For further information and badging and identification policies, see BICSI 009.

12.6.4 Alarms

12.6.4.1 Introduction

Alarms utilize one or more sensor technologies to detect a variety of conditions relevant to the security of the data center. Sensor technology includes:

- Audio
- Capacitance
- Electro-mechanical
- Glass break sensors
- Passive infrared (PIR), which detects thermal or infrared images
- Light (e.g., photoelectric, laser)
- Ultrasonic and microwave
- Vibration

12.6.4.2 General Recommendations

Audio sensors should be used in the data center perimeter to detect and record any sound in a protected area or filter sounds traveling along fencing or telecommunications conduit to eliminate sounds from traffic or weather and trigger an alarm if impact, cutting, or digging is detected.

Capacitance sensors should be used in the data center to detect changes in electronic fields and are primarily limited to monitoring the electronic field around protected objects.

Electro-mechanical sensors include things like foil, wire and screen detectors, pressure mats, and mechanical and magnetic contacts. When used as sensors in the data center, they should be installed so that the activity of the intruder causes some movement or pressure triggering an alarm and can be mounted on or in a wide variety of locations.

Glass break sensors can be installed on a wall or ceiling surface, but to directly receive the sound waves needed to trigger the sensor, they should be mounted directly across from the window being monitored. Some glass break sensors are subject to false alarms from RFI. Glass break sensors used in data center applications should contain technology immune from RFI induced false alarms.

Passive infrared (PIR) sensors in the data center should be installed so that an intruder must pass across its field of view. PIR devices can be used to protect perimeters, areas, or objects. This includes areas where barriers or mechanical detectors were historically the only countermeasure available, including skylights and maintenance holes.

Known conditions that create false alarms are:

- Rapid changes in temperature
- Bright windows or direct sunlight
- Insects
- Drafts
- RFI

Photoelectric sensors installed in the data center or campus should be used indoors or outdoors in any location where an invisible beam of light is monitored at the receiving end for interruption. False alarms can be triggered by some atmospheric conditions like snow and heavy rain or in an outdoor environment by animals.

Ultrasonic and microwave sensors operate much like PIR sensors, but they substitute sound waves for infrared detection as a trigger. These sensors should be used indoors where the types of movement are limited to protected area such as offices, storage areas, TRs, loading docks, and areas of the data center.

Vibration sensors should be placed in locations where there is a possibility of an attempt to penetrate a wall or floor of a safe, vault, storage area, or other secure area of the data center. Purpose-built data centers or highly secure sites should use sensors within or upon the exterior boundary fencing.

NOTE: Sensors should be hidden or not easily accessible, which may be accomplished through specific fencing materials, construction, or aesthetic elements.

Other sensors that should be considered for use in and around the secure areas of a data center include the following, which are commonly referred to as CBRNE sensors:

- Chemical
- Biological
- Radiological
- Nuclear
- Explosive

12.6.4.3 Intrusion

Intrusion alarms should be used to detect the presence and movement of unauthorized persons at a point of entry, room or general area, or in the proximity of an object.

Intrusion alarms should utilize one or more of the basic alarm triggers as follows:

- Break in an electrical circuit
- Interrupt a light beam
- Detect a sound
- Detect a vibration
- Detect a change in capacitance

12.6.4.4 Other Alarm Systems

Fire detection and prevention is covered in detail in Section 11.

Water detection is covered under leak detection in Section 10.

12.6.4.5 Integration

All alarm outputs should be terminated in one of three methods/locations:

- Local
- Central station
- Proprietary connection (security command center)

Direct connections of selected alarm outputs to EMS, fire, or law enforcement may be implemented if desired or implemented as required by the AHJ.

Local alarms should not be used as the only termination in a data center facility as there is no guarantee that the alarm will be detected and acted upon. Local alarms do have advantages when layered with other termination methods. Those advantages include:

- Psychological deterrent
- Low cost
- May interrupt criminal or unauthorized activity

If central station termination is utilized, the data center operator should periodically test and evaluate the training and response of the monitoring company. If the monitoring service also includes first responder alarm investigation, the background and training of the central station alarm investigators should be periodically evaluated.

Alarm and access control systems must be integrated to allow coordination of programming of desired security operational parameters and a coordinated response to alarm conditions. For example, in many facilities, initiation of a fire alarm signal will be programmed to automatically unlock emergency egress doors in the facility to allow quick evacuation of the facility by personnel. Initiation of a security alarm by motion detectors can be programmed to initiate automatic display of video of the location on the security system computers.

12.6.5 Surveillance

12.6.5.1 Introduction

Security employs two types of surveillance: physical and technical. Physical surveillance techniques are primarily done by humans and are outside the scope of this standard. Technical surveillance is accomplished by electronic equipment, typically cameras and other elements of a VSS.

The VSS serves several purposes in the security of the data center:

- Enable security and monitoring personnel to centrally view many locations simultaneously.
- Provide a visual record of monitored area during alarms and access control events.
- Record crimes, civil, and operational offenses for use as evidence in prosecution and human resources processes.
- Record monitored areas and employee activity for use as a defense in civil and criminal prosecution against the data center.
- Function as part of the video analytics system, which analyzes video content, apply system rules, and produce alarms when conditions are met (e.g., movement within an area that is scheduled to be unoccupied).

12.6.5.2 Recommendations

Placement of cameras, frames per second, resolution, lighting, and other criteria should all be determined as a result of a risk/threat and vulnerability assessment. A qualified security consultant should identify the vulnerable areas and evaluate the operational, technical, and environmental parameters before the VSS design is approved.

Camera placement should be coordinated with lighting designers to provide adequate image resolution to recognize faces, vehicles, types of activity, and other significant facts. This is especially important in outdoor situations where the type of image sensing technology, lens characteristics, and lighting can affect the usability of view or recorded video.

VSS equipment should provide views of both the front and rear of all in-scope systems, clearly identify individuals within the secured environments, and be time stamped.

Cameras should be protected against theft, vandalism or neutralization. Protection for cameras should include:

- Mounting the camera out of reach of pedestrian and vehicular traffic.
- Protecting the camera in a secure enclosure or dome.
- Environmental protection in extreme heat or cold conditions or when the camera's operation requires a controlled environment.
- Securely mounted and fastened to a stationary object.
- In high-risk situations, the camera may have an alarm sensor or switch attached.
- IP cameras can utilize simple network management protocol (SNMP) and trigger an alarm if the camera drops off the network.

When selecting a camera for any overt or covert monitoring scenario, the designer should consider the following performance criteria before selecting any elements of a VSS:

- Video analytics
- Backlight compensation
- Environmental operating limits
- Image sensing device
- Internet protocol (IP) capabilities
- Light compensation
- Method of synchronization
- Power over Ethernet capabilities
- Resolution
- Sensitivity
- Signal-to-noise ratio (SNR)
- Size—dimensions and weight
- Telemetry
- Video output level

Fixed cameras are designed to monitor a defined area and come with adjustable aiming provisions and lenses to allow field setting of the coverage zone and focal length. Once set in the field for the focal length and coverage area, they remain fixed.

Pan-tilt-zoom (PTZ) cameras have an integral motorized mechanism that allow remote control from a special joystick/keyboard controller to move the field of coverage and change image magnification within the limits of the camera. PTZ cameras can be programmed to automatically sweep designated areas within their field of view and can be manually controlled to cover areas or zoom in to an area where suspicious activity is detected.

Cameras mounted outdoors should be environmentally resistant and to have integral heaters and blowers to maintain the housing interior temperature within the camera's operating limits.

When low-light conditions are anticipated, the VSS should utilize cameras designed for this condition as follows:

- Day/night cameras are often used to provide color video during daytime conditions, which switch to monochrome video during nighttime conditions with lower lighting levels.
- Infrared (IR) illuminators generate infrared light that is nearly invisible to the human eye but will enable IR-sensitive cameras to produce high-quality images under nighttime conditions without requiring visible light illumination.

List continues on the next page

- Cameras should be installed to maximize the amount of lighting coming from behind the camera or directed in the same direction as the camera; avoid light sources that provide direct illumination on the camera lens. Current camera technology utilizes charge coupled device (CCD) chips, which are more sensitive to low light and the IR spectrum.
- Lighting sources for areas having video surveillance should have good color rendition such as fluorescent or HID metal halide. Avoid use of low-pressure sodium, high-pressure sodium, and mercury vapor lamp sources, which have poor color rendition and do not adequately support video surveillance equipment performance.

Some video surveillance systems have "video analytics" capability that allows distinguishing of movements detected by the cameras and triggering programmed response such as alarms, recording, or log entries. Cameras utilizing video analytics should be used to monitor high-value or sensitive equipment or areas of the data center where a specific asset is at risk or where it does not make sense to record the surveillance 24/7 such as very sporadic offenses.

Nonfunctioning, decoy or "dummy" cameras should not be used for any area of a data center. Decoys may be easily detectable and, if discovered, can lead to additional liability for the management of the data center facility.

IP cameras should be considered when selecting the VSS for the data center. They have the following performance advantages described below, but they require coordinating with network engineers to operate properly without degrading network performance:

- Cameras can use power over Ethernet (PoE), eliminating the need for separate power supplies, reducing labor and cable costs.
- Additionally, PoE can increase the resiliency of the cameras/security and reduce installation costs because PoE network devices are normally on redundant UPS and generators.
- Surveillance distribution is available to authorized users directly off the network.
- Existing structured cabling system (SCS) infrastructure is used in an open architecture.
- Camera system is scalable and easily expanded.
- Routine permanent archiving of video to capture authorized occupant entries and exits from the facility or controlled spaces may be done utilizing a network storage system rather than physical media.
- Archived video is often employed to maintain a record in case an incident occurs that requires an investigation.

If the VSS is monitored locally by guards or other personnel, the method(s) by which the cameras are monitored should be determined by the threat/risk and vulnerability of person(s) or assets in the area being monitored. The four methods of monitoring surveillance cameras include:

- Dedicated monitors
- Split screens
- Sequential switching
- Alarm switching

Integration of the VSS with alarms or access control applications should be part of the data center security plan. Examples of this would include automatic switching to a fixed camera when the two-man rule is violated for the computer room, or in the same scenario, having a PTZ camera automatically move to the data center access control point when the same alarm occurs.

The use of SNMP also should be used for events and alarms triggered by unauthorized access to or removal of physical layer infrastructure in the data center. An example of this would include the integration of fixed VSS cameras, intelligent patching and integrated alarms in a remote telecommunications room, where the attempted insertion into a data switch activates the surveillance system and notifies the network operations center of the possible unauthorized access.

12.6.6 Time Synchronization

12.6.6.1 Requirements

For security purposes, all critical devices that use time and are connected to the network should synchronize time from a central source of accurate time that is highly available.

12.6.6.2 Recommendations

Most of the systems in a data center require accurate time when communicating internally or externally with outside world. Also, data logging and monitoring systems require synchronized time to correlate events from different systems. It is not recommended to use CMOS clock available in PC hardware since it can drift considerably over time and is not considered accurate for most of the applications inside a data Centre.

Mission-critical facilities may consider installing an atomic clock (generally Stratum 2) that could be used as a master time server for all the network connected devices that doesn't need any Internet connectivity. Another option would be to have a highly available group of servers inside the data center that will be used as master time servers. In Windows domain environments domain controllers are used as a time server for all domain joined clients and can be used as a time source for all other connected devices. For distributed environments with multiple sites connected with low latency reliable networks, all equipment (servers, clients, network equipment and others) is recommended to use a highly available internal master time server.

Master time servers would need to synchronize time from outside reliable time sources. Mostly used methods are Internet Time servers and GPS time synchronization where connectivity is restricted to master time servers only.

12.6.6.3 Network Time Protocol (NTP)

Time synchronization generally uses NTP (network time protocol) or a variant SNTP (simple network time protocol) to provide UTC time. Both use UDP Port 123 and can synchronize time in tens of milliseconds over the Internet. It does not carry local time zone information and can be used between any system providing UTC time. However, care should be taken to make sure time servers and time clients are working properly as there are known problems between NTP using clients and SNTP time servers.

12.6.6.4 Internet Time Servers

There are groups of NTP servers on the Internet that provide time free of charge and are highly available. When selecting following points should be considered:

- It is recommended to look for publicly available NTP servers that are closest to the Data Centre in your country.
- Select a pool of NTP servers that can provide resilience such as pool.ntp.org.
- Do not point all your equipment through the firewall to NTP servers, use an internal master time server to consolidate time synchronization requests.

12.6.6.5 GPS Time Synchronization

The global positioning system (GPS) is a satellite-based system that provides positioning and timing services. GPS timing signals can be received by a relatively low-cost antenna and receiver systems that can provide microsecond level accuracy. When selecting a GPS Time Synchronization appliance, following points should be considered:

- Antennas dedicated to only GPS signals have a coax connector such as BNC, TNC or N-type on 50-ohm coax cable. The antenna should be high gain for longer cable runs and powered by a GPS receiver.
- Combined GPS antenna/receivers generally have RS232 connection and should be avoided because of shorter cable distance and power requirements.
- It is recommended to put GPS antennas on roof tops with 360-degree clear view to provide more than one satellite in view for resilience. If this is not a concern, window mounted indoor antennas can be considered.
- If an outdoor antenna is utilized, usage of surge suppressors fitted in-line on antenna cable is recommended since, any strike in local vicinity of antenna can cause surge causing damage to the NTP server.
- If it is a concern to have a military organization (US military) maintaining the satellites, support for Europe's Galileo Global Navigation Satellite System (GGNS) to be operational by 2019 should be discussed by the vendor.
- It is recommended to have a GPS based NTP appliance connected to antenna to provide time instead of using an add-on module to any other equipment for ease of maintenance and troubleshooting.
- It is recommended to have a single appliance provide time to a highly available group of master time servers, instead of all equipment being connected to the appliance directly.

12.7 Building Shell

12.7.1 General Recommendations

The data center should have an evacuation plan, including procedures on notifying all building occupants and posted evacuation routes.

Public tours should not be conducted in areas where sensitive computer operations are active, personal or sensitive data is visible, or high-value items are stored. If public tours of the data center and computer room are conducted, cameras and camera phones should be prohibited.

All areas through which data passes (e.g., entrance rooms, TRs, media storage rooms, computer rooms) should have some level of access control installed.

High-value computer, satellite, network equipment, and other hardware/software should be stored in rooms with EAC to ensure that only authorized personnel enter and to provide a tracking log in the event of loss.

Media storage, waste disposal, and chemical storage should be separated from computer, network, and telecommunications equipment.

All service personnel, including janitorial, technical, and construction contractors, should be prescreened by security. Unscreened substitutes should be denied access to the site/building/data center.

12.7.2 Doorways and Windows

Skylights, light monitors, atriums, open courts, light courts, windows, or any other openings that penetrate the security of the roof should be approved by the security designer, including appropriate countermeasures to provide security appropriate with the area or room.

All heating, ventilation, and air conditioning openings larger than 62,000 mm^2 (96 in^2) should have some form of barrier installed to prevent unauthorized entry into the building. This recommendation also applies to any other utility openings that penetrate the roof or walls.

Doors located in lobby areas must have glazing that conforms to local building codes. View panes and glass doors must consist of burglar-resistant glass.

All exterior doors should be at least 1.3 mm (16 gauge) steel-reinforced solid core.

Roof hatches should be manufactured from a minimum of 1.3 mm (16 gauge) steel and should lock from the inside only.

When ladders for the rooftop are mounted on the building exterior, a security ladder cover should protect the first 3 m (10 ft) of the ladder.

All permanent roof access should be from the interior of the building.

Doors leading to the roof should meet the security requirements for exterior doors, including double-cylinder deadbolt locks.

Windows should not be placed in the computer room, storage areas, equipment rooms, restrooms, locker, or utility rooms. If windows are necessary or preexisting, the windowsill must be at least 2.4 m (8 ft) above finished floor or any other surface that might provide access.

Window frames should be constructed with rigid sash material that is anchored on the inside and is resistant to being pried open.

The doors to all utility rooms, entrance rooms, TRs, and computer rooms should be locked at all times when not in use. Doors to these rooms should be equipped with door position sensors that trigger an alert if the door is propped or held open for more than 30 seconds.

12.7.3 Signage and Displays

All closed, limited-access, restricted, and secure areas should be designated by the use of prominent signage.

Computer rooms, secure areas, and sensitive areas should not be located on all publicly accessible directories, signs, and maps.

12.7.4 Construction

When the data center is being planned for an existing structure, the security survey should include a structural analysis of the floors, ceilings, and walls to determine the estimated time needed to penetrate them.

Added intrusion alarm and surveillance systems should be designed when the resistance to penetration of any exterior or interior ceiling, wall, or floor is identified as a risk. This includes open plenum areas above dropped ceilings that extend over controlled areas or are separated only by drywall.

Exterior building doors should be constructed of solid metal, wood, mesh-reinforced glass, or covered with a rated metal screen.

When possible, there should be no external windows or doors leading into the computer room.

12.7.5 Elevators

Elevators opening to secure areas should have one or more electronic access control systems to ensure proper identification and authentication of passengers that visit the selected floor.

If possible, separate elevators should be designed to serve secured or sensitive areas.

12.7.6 Emergency Exits

Emergency exits should be configured so that they are only capable of being operated from the inside.

Planners should consider installing automatic door closers and removing door handles from the outside of the emergency exit doors, discouraging use of the door to reenter the facility.

12.7.7 Utilities

All utility feeds should be located underground. If utilities must enter the data center above ground, they must do so at the highest possible distance above ground and must be enclosed in a conduit until safely inside the building shell.

12.7.8 Hazardous Material Storage

Caustic or flammable clean fluids should always be stored in closets or rooms designated for that purpose. They should never be stored in entrance rooms, computer rooms, media storage rooms, TRs, or other locations where telecommunications, network, or ITE is installed or stored.

Cleaning fluids and all other caustic or flammable liquids should always be stored in approved containers and in as small of quantities as possible.

•

12.8 Computer Room and Critical Facility Areas Special Considerations

12.8.1 General

The security plan should contain special considerations for computer rooms and critical facility areas.

All computer rooms and other areas deemed mission critical, inside and outside the building itself, to the operation of the data center should be considered restricted areas.

All security personnel should be made aware of the location of these areas.

All sides of a computer room, including ceiling and underfloor when those areas represent possible points of entry, should be protected by intrusion alarms and surveillance.

Electronic access control (EAC) shall be installed to track and control all ingress and egress to computer rooms and all critical areas.

The use of access control, surveillance, and alarms should be deployed as detailed in the policies and procedures outlined of the security plan to protect all computer rooms and critical facilities. Typical countermeasures deployed to protect these areas include:

- Access control devices, including locks and barriers
- CBRNE detection and protection
- Guard patrols
- Intrusion alarms
- Man traps
- Sensor driven alarms, including fire, smoke, water, and temperature
- Signage
- Surveillance

In a “lights out” data center or when employees and security personnel are not on site 24/7, the intrusion alarms should be monitored by at least one central station such as the corporate NOC or security centers.

Access to the computer room shall be controlled at all times.

All data center and computer room main and backup power supplies, entrance rooms, TRs, and other mission-critical utilities should be located in secure areas with periodic inspections for sabotage.

Badging policy should be strictly enforced in the computer room. If an employee loses or forgets a badge, he or she should be required to wear a visitor badge, complying with any visitor escort policy(s) until such time that the badge is replaced or found.

The ability to authorize access into the computer room should be limited to as few personnel as possible.

Computer room doors should remain closed and locked at all times. When possible, the door(s) should be alarmed to prevent propping open the computer room door.

All visitors and contractors should be required to sign an entry/exit log prior to entering the computer room, even when they are escorted.

Employees should be trained and encouraged to challenge unknown individuals found in the computer room.

Data centers should consider implementing the two-man rule for the computer room and other areas containing high value or sensitive contents.

All after-hour entry/exit into the computer room should be tracked and reviewed by data center security or management personnel.

All removable recording media should be secured when not in use to reduce the likelihood of theft or damage.

Critical information storage areas, such as tape vaults, should be prohibited for use as a work area.

It is a good practice to inspect all containers (including lunch boxes and briefcases) that leave the computer room, high-value, and sensitive areas. This helps prevent the unauthorized removal of proprietary information and storage media.

Authorized data center personnel should be required to remain with all hardware, software, and integration vendors while installation, maintenance, or upgrades are being performed.

Unless job functions require it, programming or coding personnel should not automatically be granted access to the computer room.

12.8.2 Construction

When possible, computer rooms should be physically separated from less secure areas. These areas should be marked as "restricted" or "controlled areas" consistent with signage policy.

Data centers located within multi-storied buildings that have multiple tenants should have structural and security studies performed with the resulting recommendations implemented to reduce the risk of damage to data center equipment from portable explosives detonated above or below the data center ITE or critical facilities systems.

Computer rooms should always contain a drainage system with a capacity large enough to handle potential leakage from sprinklers, chilled water pipes, and any potable water pipes that pass through or adjacent to the computer room.

Computer room floor drains should always be fitted with back-flow valves.

The computer area roof should be constructed to drain or guide water away from the computer room.

The data center should have a supply of waterproof sheets or covers available to adequately cover all hardware, equipment, and supplies.

An industrial wet/dry vacuum cleaner should be kept close to the computer room in the event of a water leak. Vacuum cleaners used in the computer room should be micro filtered with a minimum 99.8% HEPA filter to prevent particles from being released back into the data center. Allowed particulate size may be predetermined thus the vacuum cleaner used should correspond to this determination.

12.8.3 Eavesdropping

Computer rooms handling highly sensitive or valuable data should consider the installation of electronic field emanation reduction features (Tempest) to prevent electronic eavesdropping of data processing activities.

When highly sensitive or valuable data is present, the computer room and any data center area processing this data should be periodically checked for electronic eavesdropping devices.

12.8.4 Media

The computer room should contain a certified fireproof magnetic media cabinet/safe for the storage of critical documents and removable media.

The marking, handling, storing, destroying, or using of storage media should be limited to specific authorized employees or contractors.

12.8.5 Fire Prevention

Computer rooms should not have any trash receptacles. All unpacking should occur outside the computer room, and any trash in the computer room should be promptly removed.

Caustic or flammable cleaning fluids shall not be stored in the computer room.

12.8.6 Dust

Paper shredding, paper bursting, and report separation equipment should always be located outside of the computer room.

Paper products and supplies should always be stored outside of the computer room.

If paper products are required to be stored in the computer room, then the supply should be limited to no more than one day's worth.

12.9 Disaster Recovery Plan

12.9.1 Introduction

All data centers should have a detailed disaster recovery plan. The physical disaster recovery plan should be complimentary or integrated within the IT disaster recovery plan and the organization's business continuity plan (BCP).

12.9.2 Requirements

The data center disaster recovery plan shall deal with all phases of an emergency including:

- Planning
- Predisaster/incident activities
- The disaster/incident
- Response
- Recovery from the disaster/incident

The primary content, procedures, and all emergency lists shall be printed and posted as hard copies, with such postings being strictly maintained and current.

12.9.3 Recommendations

The data center should identify a disaster recovery manager (DRM) who is responsible for the coordination and implementation of the disaster recovery plan.

A detailed analysis of the impact of both long and short-term business interruptions should be conducted. The data center should evaluate the impact of total shutdown for up to 30 days.

Specific employees and contractors should participate in the creation and regular updating of the disaster recovery plan.

The planning for and classification of disasters should follow the guidelines outlined in NFPA 1600.

The disaster recovery plan should take into account the following types of major disasters:

- Aircraft crashes
- Chemical accidents
- Dust
- Earthquakes
- Epidemics
- Falling objects
- Fire
- Electrical hazards
- Hurricanes
- Landslides
- Loss of utility services, including water, electric, and telecommunications
- Other natural disasters
- Weather extremes

The disaster recovery plan should take into account the following types of criminal activity, which can have disastrous impact on the data center:

- Arson
- Blackmail
- Breaking and entering/burglary
- Bribery
- Collusion
- Conspiracy
- Disorderly conduct
- Embezzlement
- Extortion
- Fraud
- Kidnapping
- Looting

List continues on the next page

- Rape
- Riot
- Terrorism
- Theft
- Trespassing
- Vandalism
- White-collar crime

Data centers should regularly and routinely conduct disaster recovery tests.

The test should be evaluated, and modifications made in the disaster recovery plan to address any issues.

Disaster recovery planning should include the creation of mutual aid agreements with other businesses or organizations.

Disaster recovery planning should include the identification of key employees or contractors necessary to restore operation to the data center during a disaster.

Backups should be identified in the event that the primary personnel identified are unable to respond.

Data center and security personnel should meet with appropriate federal, state, and local authorities that have control of surface roads and disaster zones and determine the forms of identification and authorization that will be required during a natural, technological, or human disaster.

Each employee or contractor designated as critical to restoring operation of the data center during a disaster should have some preapproved method of identification and authorization to enter disaster zones should the data center facility be classified as part of such.

Disaster plans should include the identification and listing of likely emergency routes.

Disaster plans should identify primary and secondary methods of communications between key personnel needed to restore operations to the data center.

Identified employees and contractors should have easy access to a contact list containing the names, addresses, telephone numbers, and other contact information for each primary and backup responder.

Because of the variable nature of the availability of communications during a disaster, multiple methods of communication should be available, including:

- Telephones
- Cellular phones
- Personal communication devices with electronic messaging capabilities (e.g., text, email)
- IP phones
- Pagers
- Land mobile radios
- Citizens band (CB) radios

Disaster recovery plans should include detailed plans for all aspects of emergency operation of the data center, including:

- Access/egress badges, keys, cards for all areas, including those normally off limits
- Access control plans for nonemergency personnel
- Operational checklists with detailed documentation and instructions on operation of equipment with which the emergency responder may not be familiar
- Facility shutdown procedures
- Emergency security procedures
- The location of all emergency equipment
- The use of fire and emergency equipment

12.9.4 Security Plan and Disaster Recovery

The security plan should include the development of detailed plans for the notification, response, and emergency operation of the data center following a natural, technological, or human disaster.

The data center operator, security architect, and designer should work with other departments and plans to identify, assess, and mitigate any foreseeable natural or other disasters. The security plan should whenever possible focus on prevention and mitigation to threats.

The security plan should consider and document the various data center or corporate assets and prioritize protection and recovery policies and procedures.

The security plan should put into place systems, processes and procedures prior to a disaster that will enable the data center to:

- Prepare for natural, technological or man-made events.
- Respond to disasters.
- Recover from disasters.
- Work with civilian or military authorities during a disaster.

The security plan should provide detailed measures to protect the following:

- Health and safety of data center or campus occupants at the time of the disaster
- Health and safety of emergency services and disaster aid personnel responding to the incident
- Ability for the data center to continue operations
- Security and recovery of corporate intellectual property assets
- Condition and usability of the site, campus, building(s), critical, and telecommunications infrastructure
- Utilities and telecommunications services
- The environment
- Economic and financial condition of the company
- Regulatory and contractual obligations
- Company's reputation

The security plan should identify the approved and contractual civilian and governmental resources for mutual aid in the event of a disaster.

13 Facility, Ancillary and IP-enabled Systems

13.1 Introduction

While a data center's primary mission to provide proper space (e.g., computer room) and all related services to support the uptime requirements of the network and ITE equipment, a data center may utilize additional facility, infrastructure and ancillary systems to support other functions to assist in data center operations. Systems that may be present include:

- Phone and VoIP systems
- LAN supporting business operations
- Wireless LAN
- Data center infrastructure management (DCIM)
- Building automation and management
- DAS supporting cellular and other systems
- Sound masking and privacy
- Lighting and environmental controls

13.2 General Requirements

13.2.1 Spaces

Non-computer room systems shall be supported by a telecommunication room or other commonly defined telecommunications space that is separate from spaces supporting the data center 's computer room(s).

NOTE: Figure 14-5 shows an example of the cabling topology

13.2.2 Cabling and Cabling Infrastructure

Cabling and related cabling infrastructure for non-computer room systems shall meet applicable standards (e.g., ANSI/TIA 568.0-D, ISO/IEC 118001-1). Systems may have additional requirements as defined in Sections 13.4 – 13.7.

13.2.3 Enclosures

Enclosures are classified as either wall mountable or cabinet or rack mountable. Cabinet or rack mountable enclosures shall meet applicable ISO/IEC or ANSI requirements and allow for mounting within 480 mm (19 in) or 580 mm (23 in) racks.

External enclosures shall:

- Provide enough securing points for a safe attachment to a wall
- Provide protection from the environment at least to the level required by the equipment installed inside
- Be lockable

Internal enclosures shall:

- Have dimensions allowing for fitting in wall spaces and provide enough space to terminate and properly protect incoming and outgoing wiring
- Be lockable, if required
- Meet local fire codes to ensure equipment survivability and reliability during a fire

13.3 General Recommendations

A zone-based cabling topology is recommended for large data centers.

13.4 Data Center Infrastructure Management

13.4.1 Introduction

NOTE: Additional information about DCIM can be found in BICSI 009.

Data center infrastructure management (DCIM) is a software application or a suite of software applications that are configured to gather, monitor, and aggregate data from multiple sub systems within a facility. DCIM is not an actual management tool because it does not directly control data center devices and components; it is used as a data collection and reporting tool. The result of the aggregated data is utilized for automated or manual adjustments to physical infrastructure in order to increase efficiency, provide fault tolerance, provide workflow management, and implement changes resulting from expansion or consolidation of the facility.

DCIM can source data from directly connected components such as electrical components (e.g., UPS, PDUs, RPPs) or environmental (e.g., CRACs CRAHs, temperature probes, humidity probes, wireless environmental reporting devices). Automated adjustments are performed by subsystems, such as a building automation system (BAS) or building management system (BMS), and are initiated by those systems.

DCIM can also source and share data with other facility systems such as BAS, BMS, and EPMS. Each of the human machine interfaces (HMIs) within the other facility systems can also utilize the aggregated data collected by DCIM in order to determine facility based adjustments to be made by the BAS and BMS.

13.4.2 Recommendations

Figure 13-1 shows an example of DCIM architecture. DCIM should consist of an open communication architecture. This architecture exhibits the distinct ability to interface with any third-party software or device over standard IP and industrial communication protocols. Alerts are required for critical threshold breaches as well as trending in order to forecast potential risk. Finally, DCIM should be scalable, enabling the user to monitor conditions on directly connected devices within a small data center or indirectly connected devices through subsystems within an enterprise environment. DCIM should have the ability to perform calculations based upon aggregated data from a proportionate number of devices and meters but exhibiting the ability to make assumptions based upon whether the number of devices and meters are lesser or greater.

DCIM can use collected data in many ways to make more informed decisions, to reduce downtime and cost of operations, to improve performance and key indicators, to optimize asset usage, to implement more informed actions and strategies, and to develop predictive behavior models. Data center professionals must think critically to determine what data is needed for each particular case, also considering future scenarios. This practice prevents missing important measurements and helps to avoid collecting unnecessary data.

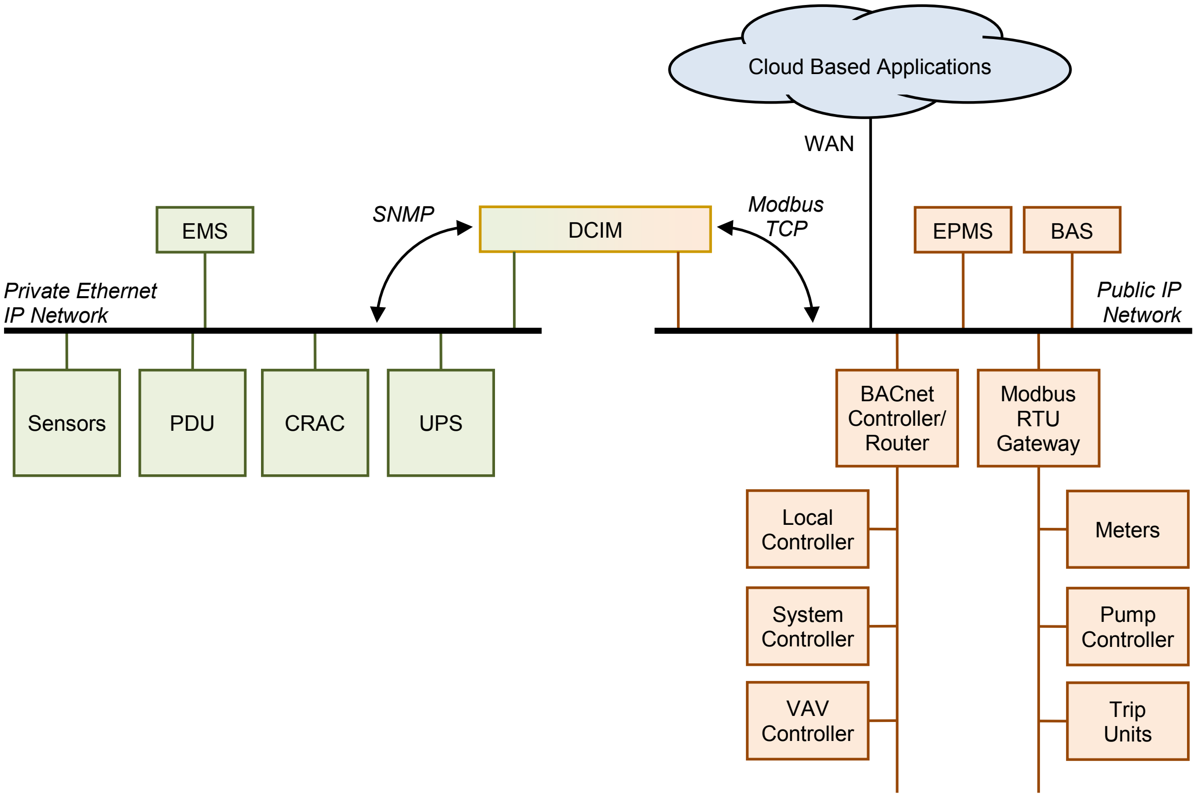


Figure 13-1
Example DCIM Architecture

The DCIM architecture should also permit managing devices on either the company/organization network or a separate dedicated network. The DCIM should also allow management devices that can reside on both the public LAN and the private LAN. Management and monitoring functions may be implemented as either firmware or software configuration within the appliances. Other more complex functions such as workflow management, change management, and analytics, may be performed either by servers within the data center or in the cloud on a server in a service provider's data center. The application requirements should include end user scalability, allowing for future expansion and enhancements.

Data center monitoring and management systems should include end-to-end resource management, covering both the ITE and supporting infrastructure. Resource management is iterative, enabling data center stakeholders to plan and make adjustments. Some tasks include physical space and capacity planning; optimization of power and cooling systems; detection of unused or idle ITE; optimization of ITE resource; workload allocation to control power and environmental parameters; workload balance among ICT equipment; and virtualization. Comprehensive control strategies allow performance optimization, which should include all assets.

13.5 Facility Systems

13.5.1 Introduction

Facility systems typically include lighting, heating/ventilation/air conditioning (HVAC) systems, and power and utility monitoring. These systems are commonly placed under one or more building automation systems (BASs), where a BAS can be defined as an assemblage of products designed for the control, monitoring, and optimization of various functions and services provided for the operation of a building. Depending on the structure of the facility management, fire-life-safety system, security, and other systems related to the specific building may be termed a building system.

13.5.2 General Requirements

Unless strictly specified otherwise by the system manufacturer, communication and network cabling; and related cabling infrastructure and pathways shall meet the specifications of applicable standards (e.g., ANSI/BICSI 007, ANSI/TIA-862-B, ISO/IEC 11801-6)

13.5.3 Building Automation and Management Systems

13.5.3.1 Introduction

A standards-compliant structured cabling system provides a generic cabling system that can transport a wide range of protocols used for BAS, including Ethernet, ARCnet, and TIA/EIA-485-A, allowing the BAS to evolve without changing cabling. A structured cabling system also allows new services to be deployed without running new cable and is easier to administer and troubleshoot than an unstructured cabling system. However, some proprietary or legacy BAS equipment may not function properly on standard-compliant structured cabling, thus requiring the installation of two parallel networks, which should be segregated to minimize maintenance errors causing inadvertent system outages.

13.5.3.2 Requirements

All hardware shall be fault tolerant, that is failing to a condition that maintains the systems in a stable operating condition. This may be in the open, closed, on, or off position depending on the specific system configuration. The amount of hardware redundancy of equipment shall be determined by the Class of the system that the BAS is supporting.

BMS/BAS systems shall conform to an open architecture specification for interfaces to the equipment and systems to be monitored and support SNMP to report status to other management systems.

Networks supporting a mission-critical data center's BAS must be highly reliable and available. To ensure security systems availability, the design and construction shall take into account the potential for network survivability. Specifically:

- Dual (or multiple) network cabling may be considered to interconnect vital equipment and platforms; the dual network cables should be laid along different paths to minimize the chances of being damaged at the same time.

  NOTE: Separate TRs may be allocated to host the redundant equipment and be placed with sufficient physical separation to reduce the chances of all the equipment being damaged at once because of fire or some other localized catastrophic event.

- Active components and equipment shall only be installed at the ends of the link and never within.
- PoE midspan devices shall be installed in the TR, HDA, MDA, or where the link end resides.

The BAS cabling and communications systems cabling shall use separate pathways whenever there is likely to be electromagnetic interference between them. Pathways and spaces used exclusively for BAS cabling shall be clearly marked as such.

Some equipment, such as sensors, may require a topology other than a hierarchical star topology for the portion of the system that does not use structured cabling. In that case, follow manufacturer's instructions and local codes.

Monitoring of BMS/BAS alarms shall be available in the data center's operations center or a similar location wherever the network is being monitored.

13.5.3.3 Recommendations

Use standard structured cabling to support BAS as it provides the greatest flexibility in choice of a BAS system protocol.

Each cabinet and rack line-up (or pod) may have its own zone management enclosure or patch panel. However, uninterrupted links for alarms and control systems monitoring from a central location should be provided.

The BAS should be designed to provide the maximum operational time without interruption in compliance with safety codes guidelines.

Dedicated pathways for mission-critical BAS systems should be provided

Data center BAS cabling should terminate upon separate dedicated IDC blocks and patch panels and not share IDC blocks and patch panels terminating communications links. Data center BAS IDC blocks and patch panels should be clearly marked as such.

The building automation should interface with the data center central power and environmental monitoring and control system (PEMCS). The PEMCS should include a remote engineering console and manual overrides for all automatic controls and set points.

BMS/BAS systems should use open communication standards that are reliable and secure between equipment, controllers and other management systems. BMS/BAS systems themselves should be secure by design and provide remote management capabilities, remote updating and real time event monitoring capabilities.

For new data centers, systems should be selected that use modern and secure protocols such as REST based web services running on HTTPS and SNMP v3. BMS/BAS systems may need to communicate with central management systems such as data center central power and environmental monitoring and control system (PEMCS) and mentioned protocols will provide more flexibility and future proofing for years to come.

There have been many proposed open standards including but not limited to BACNet, Modbus, LONTalk and OPC that are widely adapted. However, usage of protocols that do not work well on Internet protocols (TCP/IP) have been diminishing both because of performance and security concerns. Older protocols that were updated to run on TCP/IP (e.g., ISO 16484-5) but that have security vulnerabilities which cannot be easily fixed should be avoided.

For older equipment that need to work with protocols such as BACNet and Modbus, gateway devices should be used to isolate the protocol between the equipment and gateway on a separate and isolated network (e.g., VLAN, physical links) even if these protocols are running on TCP/IP. Gateways should use modern protocols such as HTTPS and SNMP v3 for the rest of the network to connect to other management systems.

13.5.3.4 Additional Information

Typically, BAS and BMS systems will require dedicated interconnect wiring between the mechanical systems of a building, such as boilers, chillers, chiller control systems, plumbing systems, water treatment, expansion tanks, and unit heaters and the peripheral devices that provide the most immediate level of system monitoring and control. In most modern systems, this level of cabling is the most likely to require proprietary or nonstandard communications cabling. Because of the inherent limitations this type of cabling may have, these peripheral devices should be located within close physical proximity to the mechanical systems to which they are connected.

Media conversion is employed whenever two different media must interface to create a communications link. For example, a balanced twisted-pair to fiber media conversion unit may be used at the ends of an optical fiber link to allow for equipment with balanced twisted-pair ports to communicate with each other through longer distances or an environment with a higher EMI potential, depending on its pathway environment. Some devices may require cable types not typically used in structured cabling. However, this may prevent future upgrades or vendor replacement.

13.5.4 Lighting

13.5.4.1 Introduction

IP-enabled lighting systems and low-voltage lighting may decrease energy usage as compared to a traditional lighting system.

13.5.4.2 Requirements

Where IP-enabled and low voltage lighting systems are used within the computer room, they shall meet the applicable requirements of Section 9.8 and Section 14 of this standard, and ANSI/BICSI 007.

13.6 Electronic Safety and Security Systems

13.6.1 Introduction

To support the safety and security plans of a data center, traditional safety and security systems are increasingly using network concepts and infrastructure to support and provide their intended functionality. Termed “convergence”, network capability and communication is now seen in all manner of systems, including safety (e.g., fire detection and notification, access control, video surveillance and intrusion detection systems). Additionally, these systems are also being integrated with other building systems such as lighting and temperature control.

13.6.2 Cabling Infrastructure

13.6.2.1 Requirements

All systems shall meet applicable codes and AHJ requirements. Additionally, cabling infrastructure for ESS systems shall meet ANSI/BICSI 005.

13.6.2.2 Recommendations

The cabling infrastructure for life safety and critical security systems, should meet, at a minimum, the requirements of Class C2 (see Section 14.2).

Pathways used to support ESS systems should remain separate from communication and other system pathways.

13.7 Wireless Systems

13.7.1.1 Introduction

Wireless communication and data systems (e.g., WLAN, DAS) may be required to support non-critical spaces (e.g., administration) or cellular or radio applications.

13.7.1.2 Requirements

Wireless LAN systems shall meet the requirements of ANSI/BICSI 008.

Any DAS implemented shall applicable codes and AHJ requirements for the services being supported. Cabling and related infrastructure used within a DAS shall meet the requirement of ANSI/BICSI 006.

13.7.1.3 Recommendations

The cabling infrastructure for wireless systems supporting life safety and critical security systems, should meet, at a minimum, the requirements of Class C2 (see Section 14.2).

This page is intentionally left blank

14 Telecommunications Cabling, Infrastructure, Pathways and Spaces

14.1 Introduction

This section is intended to provide design standards for the telecommunications cabling requirements relating to:

- New data centers
- Additions to existing data centers
- Modifications and renovations to existing data centers

NOTE: See ANSI/TIA-942-B, CENELEC EN 50173-5, ISO/IEC 11801-5, or other applicable data center telecommunications cabling standards regarding data center telecommunications cabling topologies and distributors.

Telecommunications distribution consists of two basic elements—the distribution pathways and related spaces and the distribution cabling system.

Telecommunications cabling is, therefore, one subset of telecommunications distribution and may be described as a specific system of balanced twisted-pair, unbalanced cabling (e.g., coaxial) and optical fiber cabling, equipment/patch cords, connecting hardware, and other components supplied as a single entity.

The following partial listing of common services and systems should be considered when the cabling is designed:

- Voice, modem, and facsimile telecommunications service
- Switching and server equipment
- Computer and telecommunications management connections
- Keyboard/video/mouse (KVM) connections
- Intelligent infrastructure management (IIM)
- Wide area networks (WAN)
- Local area networks (LAN)
- Storage area networks (SAN)
- Wireless systems utilized in the data center including wireless LANs
- Other building signaling systems (building automation systems such as fire, security, power, HVAC, and EMS)

In addition to satisfying today's telecommunications requirements, the cabling should be planned to reduce ongoing maintenance and relocation. It should also accommodate future equipment and service changes. Consideration should be given to accommodating a diversity of user applications in order to reduce or eliminate the probability of requiring changes to the cabling as equipment needs evolve. Cabling should be accessible for reconfiguration when under the access floor or overhead on cable raceway systems, however within a properly planned facility, disturbance of the cabling will only occur during the addition of new cabling.

14.2 Telecommunications Cabling Infrastructure Classes

14.2.1 Introduction

A properly designed, installed, and implemented telecommunications cabling infrastructure will support the network architecture. When implemented correctly, redundancy, scalability, and flexibility will not only meet the initial network architecture needs, but also enable adaptation to future network architecture requirements where possible.

To some, it may seem unusual to extract the telecommunications cabling infrastructure, a sub-set of the entire network architecture and infrastructure, as a separate data center services layer. The telecommunications cabling infrastructure has been extracted as a separate data center services layer because there is a clear delineation between the standards bodies that oversee the physical characteristics of the telecommunications cabling infrastructure components (e.g., ISO/IEC, TIA) and the higher layers of the network protocols (e.g., IEEE).

It is important to maintain that separation within the BICSI data center services end-to-end reliability classification so that appropriate implementation and best practices guidance can be provided to align with the standards independently developed by these standard bodies. Although the design of a data center needs to start with a thorough understanding of each service layer starting from the top down, the physical build-out of data centers begins from the bottom-up. The physical network cabling infrastructure must be designed and built often before the complete details of the network architecture are clearly defined. However, if the targeted reliability Class has been identified, the appropriate physical network cabling infrastructure can be designed and implemented.

The telecommunications cabling infrastructure service layer consists of:

- Entrance Pathways: The entrance pathways supporting the service provider's, leased, or customer-owned outside plant cabling from the property line to the data center building.
- Entrance Rooms (ER): The room or area that supports the network service provider's edge equipment, terminating outside plant cable and provisions for their optical switches. ER sometimes also provide Meet-me Room (MMR) functionality.
- Meet-me Room (MMR): See Section 14.6.3.
- Main Distribution Area (MDA): The room or area that supports customer-owned core equipment, including routers, core switches, firewall, load balancers, DNS, and possibly core SAN fabric switches.
- Horizontal Distribution Area (HDA): The area that supports intermediate switching and the horizontal cross-connect field between the EDA and MDA.
- Equipment Distribution Area (EDA): The equipment cabinets and racks that house processing or storage systems hardware. Equipment areas that support large frame processing or storage systems are also considered an EDA.

For the telecommunications cabling infrastructure reliability classes, the corresponding class designation is prefaced with a "C" to identify it represents the "cabling infrastructure" reliability criteria.

14.2.2 Class C0 and C1 Telecommunications Infrastructure

A Class C0 or C1 telecommunications cabling infrastructure is a single path cabling infrastructure. The cross-connect fields throughout the data center support a single path, non-redundant network architecture.

Table 14-1 Class C0 and C1 Overview

Entrance Pathways:	Single path, multiple conduits (as specified in Section 14.5.1) from property line to ER
Entrance Room:	One ER accommodates service provider
Main Distribution Area:	One MDA supports all core equipment
Intermediate Distribution Area	Each HDA supported by a single MDA or IDA
Horizontal Distribution Area:	Non-redundant HDA to support any intermediary switching equipment and horizontal cross-connect fields, multiple HDAs may be required to support port counts and distance limitations within large computer rooms.

14.2.3 Class C2 Telecommunications Infrastructure

A Class C2 telecommunications cabling infrastructure is a single path cabling infrastructure. The cross-connect fields throughout the data center support a single path, non-redundant network architecture. It contains redundant entrance pathways to support, at a minimum, a single link from two providers or ringed topology from one provider.

Table 14-2 Class C2 Overview

Entrance Pathways:	Redundant and diverse multi-path, each path with multiple conduits (as specified in Section 14.5.1) from property line to ER
Entrance Room:	One ER accommodates service provider(s)
Main Distribution Area:	One MDA supports all core equipment
Intermediate Distribution Area	Each HDA supported by a single MDA or IDA
Horizontal Distribution Area:	Non-redundant HDA to support any intermediary switching equipment and horizontal cross-connect fields, multiple HDAs may be required to support port counts and distance limitations within large computer rooms.

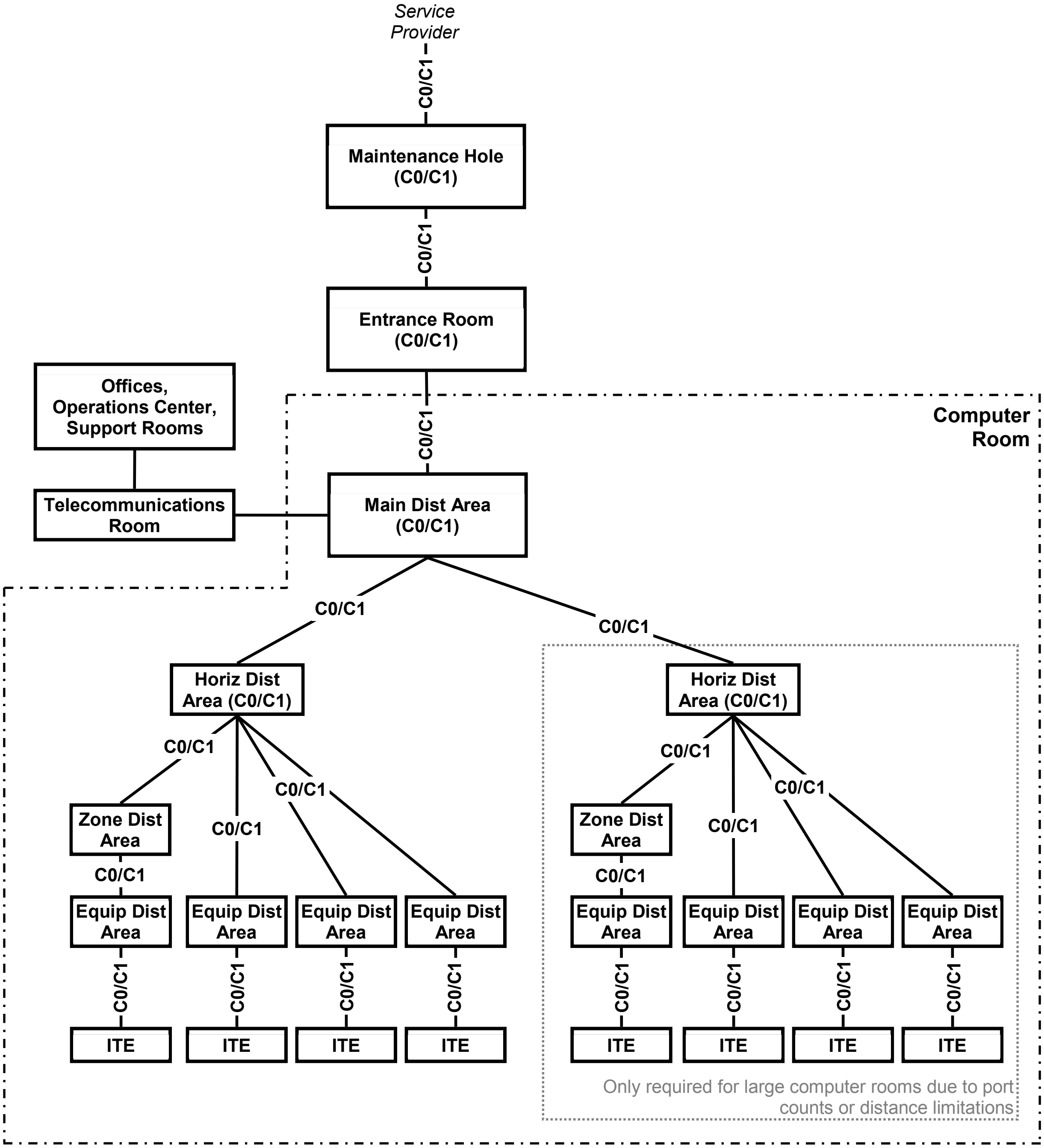


Figure 14-1
Class C0 and C1 Concept Diagram

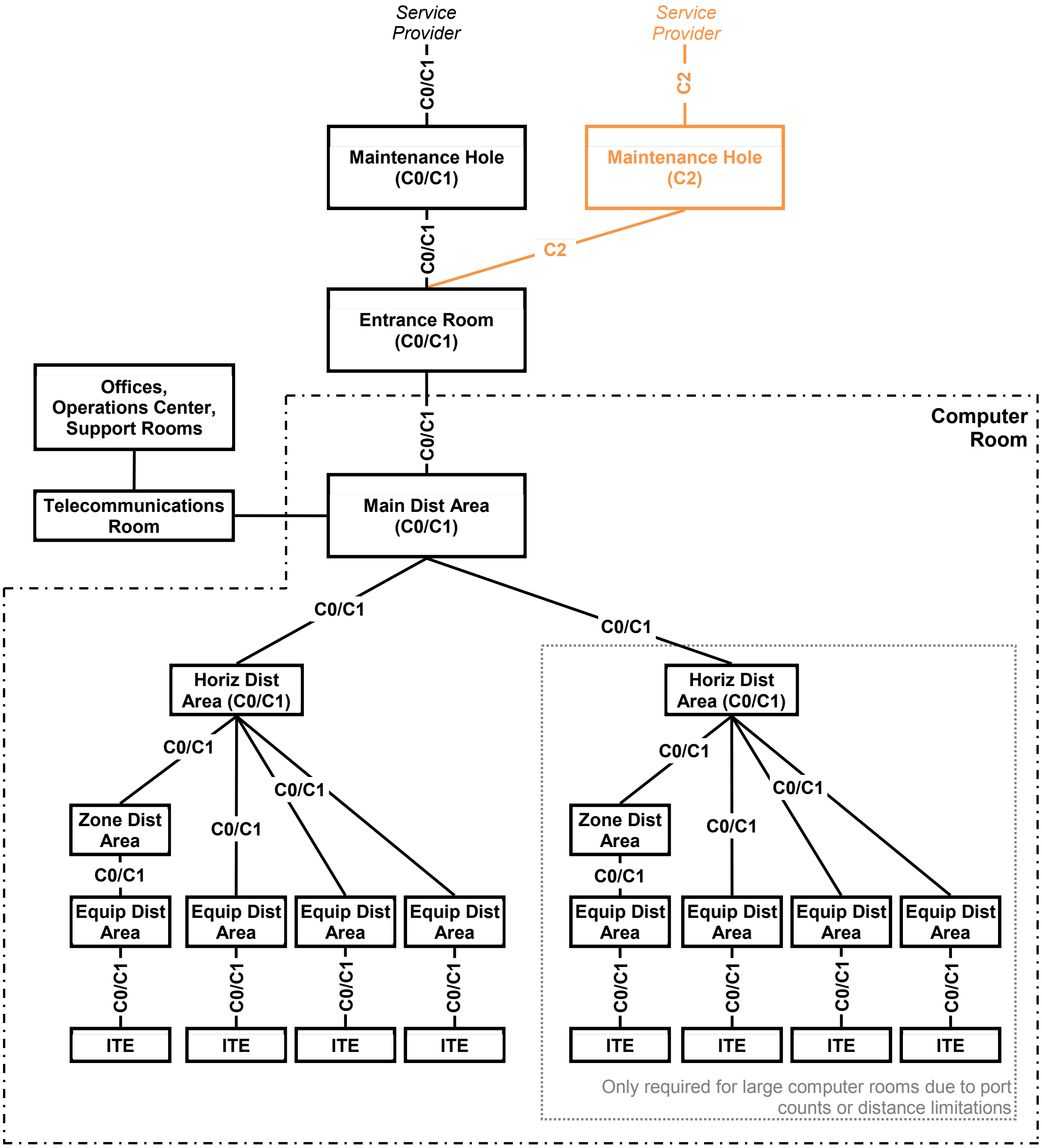


Figure 14-2
Class C2 Concept Diagram

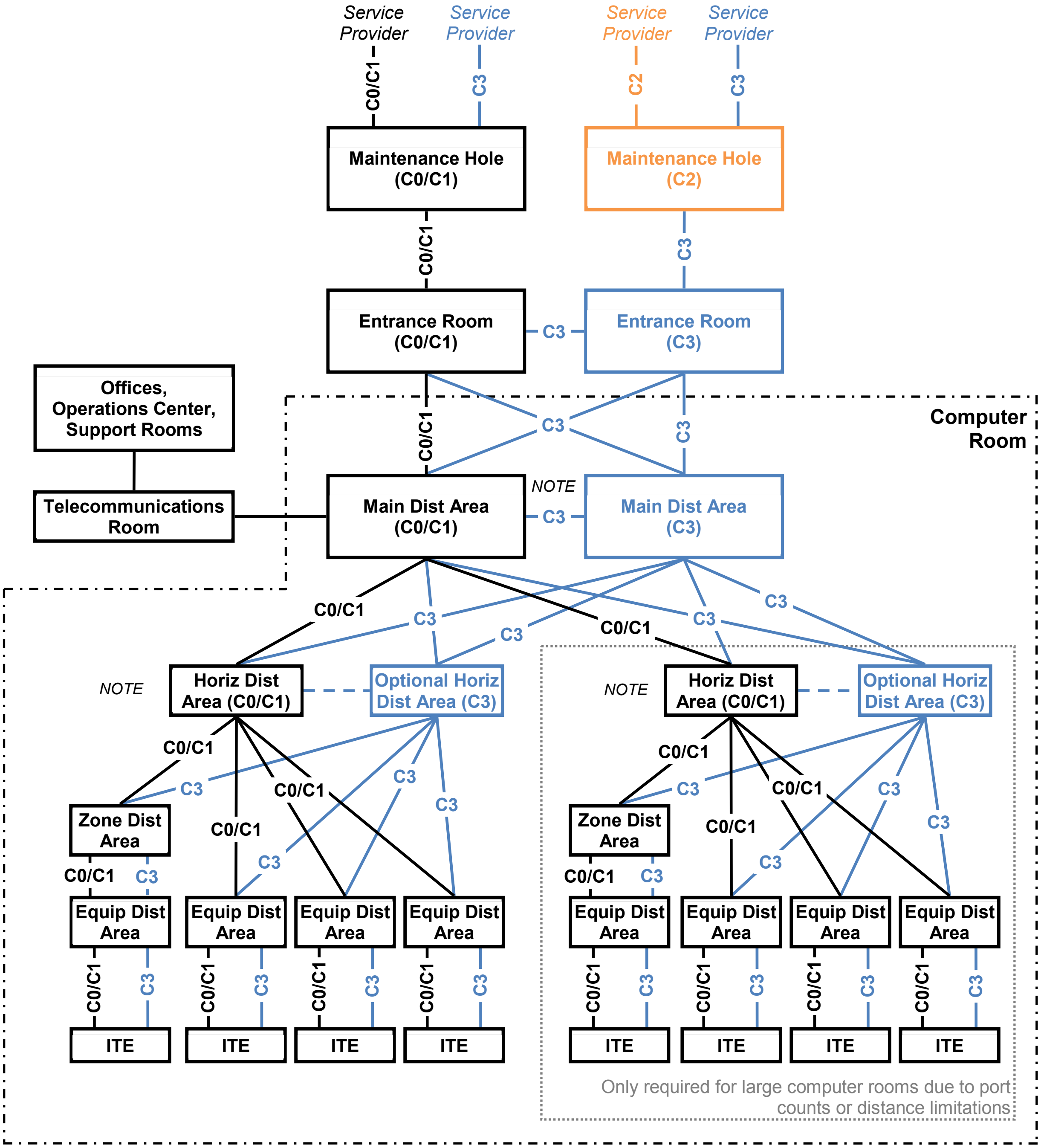
14.2.4 Class C3 Telecommunications Infrastructure

A Class C3 telecommunications cabling infrastructure is a redundant path cabling infrastructure that has redundant cross-connect fields for all backbone network cabling. The redundant backbone cabling is intended to support a redundant network topology (e.g., redundant switches, routers. See class N3 network topology in Section 15.1.

Physically separated redundant horizontal cross-connects and redundant horizontal cabling to equipment cabinets (EDAs) is also recommended. Physical separation between redundant MDAs, IDAs, or HDAs may minimize the risk presented by common modes of failure that may be present within the supporting critical infrastructure (e.g., failure of sprinkler system, raised floor system, cabling pathway system, grounding system). Physical separation may also reduce the impact of any failure because of any event caused by human error or component failure, which is not contained within a MDA or HDA cabinet, thereby exposing adjacent cabinets to risk of failure. Having redundant distributors and cabling may increase operational complexity.

Table 14-3 Class C3 Overview

Entrance Pathways:	Redundant and diverse multi-path, each path with multiple conduits (as specified in Section 14.5.1) from property line to each ER
Entrance Room:	Two ERs to support multiple service providers, providing physical separation between redundant providers edge equipment
Main Distribution Area:	MDAs support the main cross-connect (MC) and backbone network equipment. Redundant MDAs should be physically separated.
Intermediate Distribution Area	IDAs support the intermediate cross-connect (IC) and possibly backbone network equipment. Redundant IDAs should be physically separated.
Horizontal Distribution Area:	HDAs support horizontal cross-connects and may support access layer switches. Equipment cabinets (EDAs) should (but are not required to) have horizontal cabling to two different, physically separated HDAs.



NOTE: Physical separation between redundant MDA and HDA is required to minimize common modes of failure.

Figure 14-3
Class C3 Concept Diagram

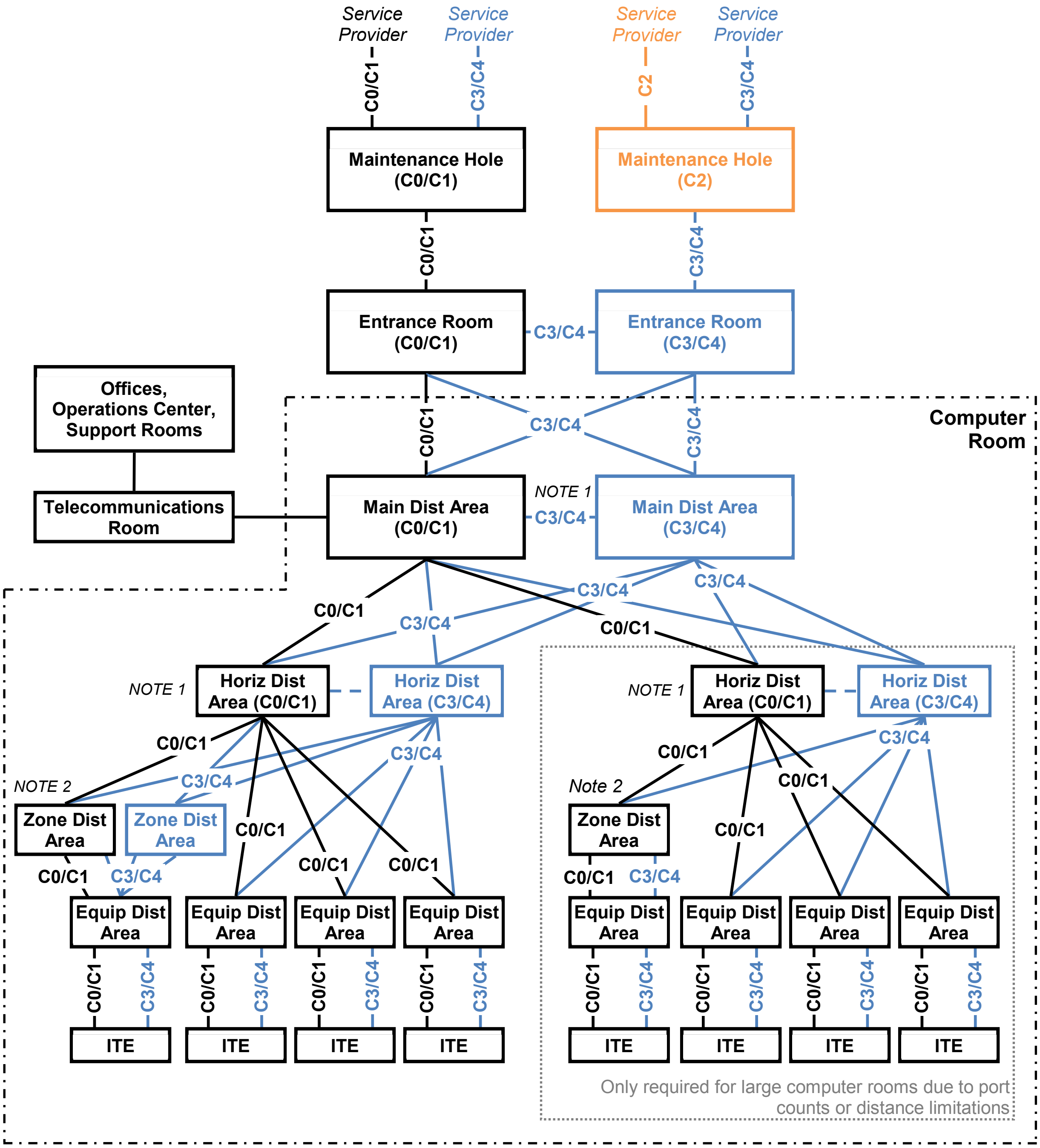
14.2.5 Class C4 Telecommunications Infrastructure

A Class C4 telecommunications infrastructure is a redundant path cabling infrastructure that has redundant cross-connect fields throughout data center network to support redundant network architecture. It contains redundant entrance facilities to support multiple network service provider topologies.

Physical separation between redundant MDAs or HDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure (e.g., failure of; sprinkler system, raised floor system, cabling infrastructure pathway system, grounding system, electrical distribution system) or any event caused by human error or component failure, which is not contained within one MDA or HDA cabinet, thereby exposing adjacent cabinets to risk of failure as well.

Table 14-4 Class C4 Overview

Entrance Pathways:	Redundant and diverse multi-path, each path with multiple conduits (as specified in Section 14.5.1) from property line to each ER
Entrance Room:	Two ERs to support multiple service providers, providing physical separation between redundant providers edge equipment
Main Distribution Area:	Two MDAs to support redundant core equipment. Physical separation between redundant MDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure.
Intermediate Distribution Area	Redundant physically separated IDAs. If an HDA has backbone cabling to IDAs, it must be supported by diversely routed backbone cabling to two physically separated IDAs.
Horizontal Distribution Area:	Redundant HDAs to support any intermediary redundant switching equipment and horizontal cross-connect fields, additional HDAs may be required on both the “A” and “B” network fabric to support increased port counts and distance limitations within large computer rooms. Physical separation between redundant HDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure.



NOTE 1: Physical separation between redundant MDA and HDA is required to minimize common modes of failure.

NOTE 2: Redundant ZDA's are an option, but not a requirement for C4.

Figure 14-4
Class C4 Concept Diagram

14.3 Cabling Topology

14.3.1 Introduction

The basic cabling elements of the data center star topology include:

- Horizontal cabling
- Backbone cabling
- Equipment cabling
- TIA main cross-connect (MC) or ISO/CENELEC main distributor (MD) in the main distribution area (MDA)
- TIA intermediate cross-connect (IC) or ISO/CENELEC intermediate distributor (ID) in the intermediate distribution area (IDA)
- TIA horizontal cross-connect (HC) or ISO/CENELEC zone distributor (ZD) in the horizontal distribution area (HDA), intermediate distribution area (IDA), or main distribution area (MDA)
- TIA zone outlet, TIA consolidation point (CP) or ISO/CENELEC local distribution point (LDP) in the zone distribution area
- Equipment outlets (EO) in the equipment distribution area (EDA)

14.3.2 Horizontal Cabling Topology

14.3.2.1 Requirements

The horizontal cabling shall be installed in a star topology. Each EDA shall be connected to a TIA HC or an ISO/CENELEC ZD in a HDA, IDA, or MDA via horizontal cabling.

14.3.3 Backbone Cabling Topology

14.3.3.1 Requirements

The backbone cabling shall use the hierarchical star topology, as illustrated by Figure 14-5, wherein each HC in the HDA is cabled directly to an MC in the MDA or an IC in an IDA. There shall be no more than two hierarchical levels of cross-connects in the backbone cabling.

Direct backbone cabling to the HC shall be allowed when distance limitations are encountered.

14.3.3.2 Recommendations

The presence of an HDA or IDA is not mandatory. Cabling extending from the TIA HC or ISO/CENELEC ZD in the HDA, IDA, or MDA to the mechanical termination in the EDA is considered horizontal cabling. Sufficient horizontal cable slack should be considered to allow migration to a cross-connect in the HDA, IDA, or MDA.

Backbone cabling cross-connects may be located in TRs, computer rooms, MDAs, IDAs, HDAs, or at entrance rooms.

14.3.4 Accommodation of Non-Star Configurations

14.3.4.1 Introduction

The topology, as shown in Figure 14-5, with the appropriate interconnections, electronics, or adapters in data center distribution areas, accommodates systems that are designed for non-star configurations such as ring, bus, or tree.

14.3.4.2 Recommendations

Cabling is permitted between entrance rooms, MDAs, IDAs, and HDAs to provide redundancy and to avoid exceeding application cabling distance restrictions for connections that route through two HDAs.

14.3.5 Redundant Cabling Topologies

14.3.5.1 Introduction

Redundant topologies can include a parallel hierarchy with redundant distribution areas. These topologies are in addition to the star topology specified in this standard.

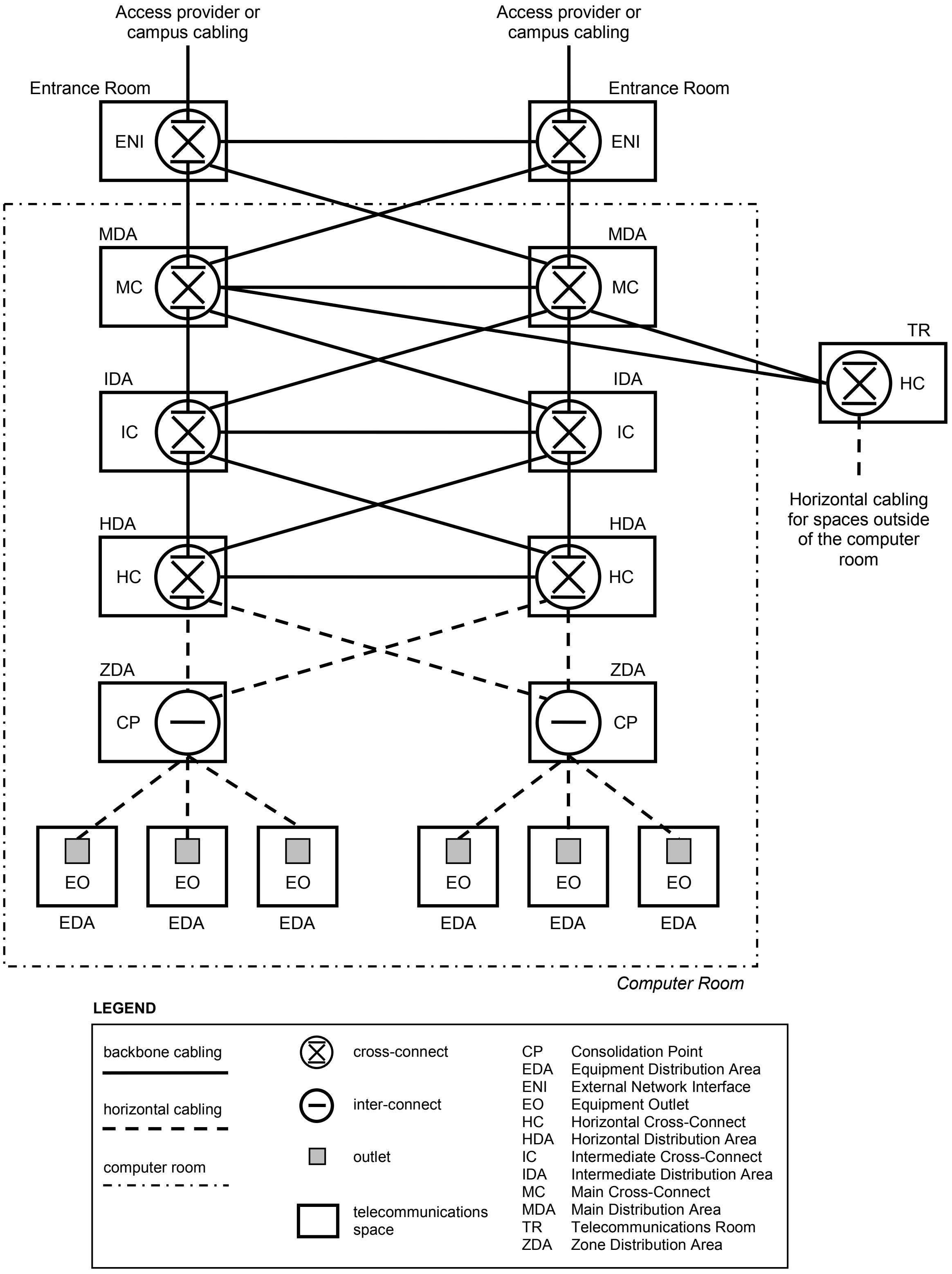

Access provider or campus cabling
Access provider or campus cabling
Entrance Room
Entrance Room
ENI
ENI
MDA
MDA
MC
MC
TR
HC
IDA
IDA
IC
IC
Horizontal cabling for spaces outside of the computer room
HDA
HDA
HC
HC
ZDA
ZDA
CP
CP
EO
EO
EO
EO
EO
EO
EDA
EDA
EDA
EDA
EDA
EDA
Computer Room
LEGEND
backbone cabling
horizontal cabling
computer room
cross-connect
inter-connect
outlet
telecommunications space
CP Consolidation Point
EDA Equipment Distribution Area
ENI External Network Interface
EO Equipment Outlet
HC Horizontal Cross-Connect
HDA Horizontal Distribution Area
IC Intermediate Cross-Connect
IDA Intermediate Distribution Area
MC Main Cross-Connect
MDA Main Distribution Area
TR Telecommunications Room
ZDA Zone Distribution Area

Figure 14-5
Data Center Cabling Topology Example

14.3.6 Low Latency Topology

While the traditional datacenter architecture was based on North-South communication, some recent applications demand increased East-West communication, creating bottlenecks in the MD and IC, therefore increasing latency.

To improve the latency, the fabric architecture can be built into the topology. The method is to connect all access switches to the interconnection switches. It does not replace the star topology but is a version of start with added connections.

Figure 14-6 shows an example of a fabric architecture with redundancy, based on cross-connect in the EDA and only one level of backbone. Additional information on network architectures can be found in Section 15.

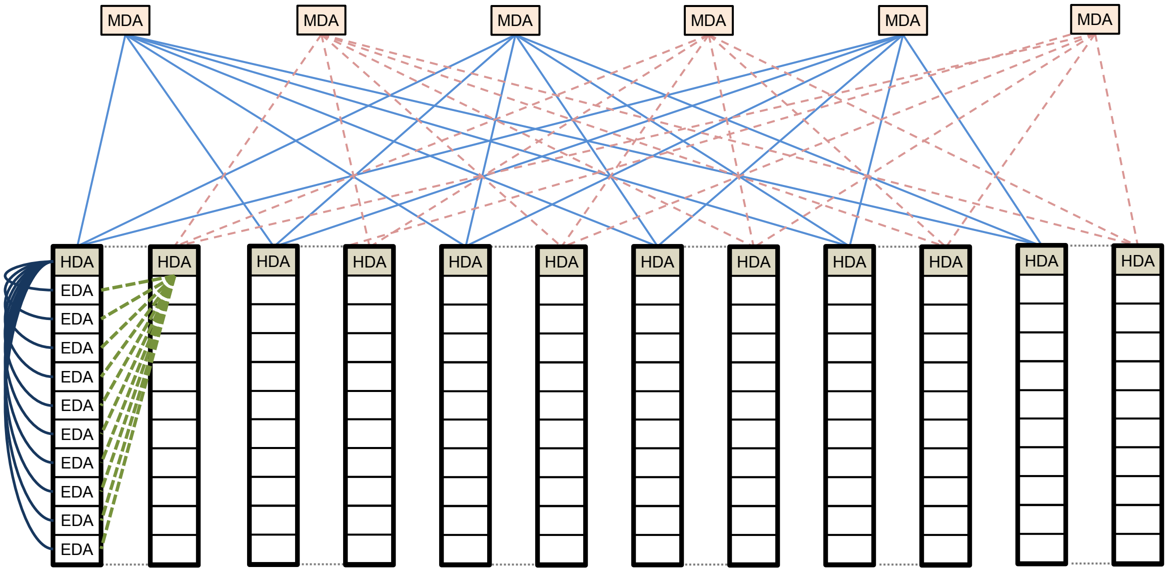


Figure 14-6
Example of a Fabric Architecture with Redundancy

14.4 Data Center Spaces for Telecommunications

14.4.1 Introduction

Data center spaces dedicated to supporting the telecommunications cabling system and related equipment are listed below. These spaces include:

- Entrance room
- Main distribution area (MDA)
- Intermediate distribution area (IDA)
- Horizontal distribution area (HDA)
- Zone distribution area (ZDA)
- Equipment distribution area (EDA)

These spaces may be physically separated or may exist within different areas of the same room through the use of partitions or location.

14.4.2 Design and Structural Requirements

Data center telecommunications spaces such as the MDA and entrance room(s), shall be sized for full data center occupancy, including all anticipated expansions and planned applications.

All data center spaces for telecommunications shall have the same mechanical and electrical redundancy as the computer room(s).

The computer room shall provide an operational environment in line with the limits and requirements set out in the applicable telecommunications cabling and data center standards for an $M_1I_1C_1E_1$ environment (see ISO/IEC TR 29106 or TIA TSB-185).

See Section 7 regarding architectural requirements and recommendations for telecommunications spaces, including door sizes and ceiling heights.

14.4.3 Entrance Rooms

14.4.3.1 Introduction

The entrance room may include both access provider and customer-owned cabling. This space may include the access provider demarcation hardware and access provider equipment and the location where conversion takes place between cabling that is suitable for outside plant applications and cabling that is suitable for premises (i.e., inside plant) applications.

The entrance room interfaces with the data center through the MDA. However, direct connections from intermediate distribution areas (IDAs) or horizontal distribution areas (HDAs) to the entrance rooms are permitted to avoid exceeding circuit distance limitations. The entrance room may be adjacent to or combined with the MDA.

14.4.3.2 Requirements

Access providers that serve the building shall be contacted to ascertain the point(s) of entry to the property and the requirements for their telecommunications cabling, terminations, and equipment.

Class C2 and higher data centers shall have diverse entrance facilities, preferably with route diversity from the data center to different access providers. For example, a Class C2 data center may be served from multiple central offices and multiple service provider point-of-presences that enter the property at different locations.

The location of each building entrance facility shall be coordinated with routing of access provider pathways as well as internal pathways and shall not conflict with the location of other building facilities such as power, gas, and water.

14.4.3.3 Recommendations

Each building point-of-entry supporting an access provider’s outside plant facilities should be located on different (or even opposite) sides of the building. Conduit duct banks and their associated maintenance holes and other pathways from the access provider central offices and service provider point-of-presences to the building’s entrance facilities should be separated by at least 20 m (66 ft) along their entire routes.

A conduit duct bank with appropriately placed maintenance holes that surrounds a data center and incorporates multiple building entrance facilities should be considered for the data center. At least one conduit for replacement cables should be set aside for each internal and entrance pathway to facilitate rapid replacement of cables. The use of innerduct, either conventional or fabric, is recommended to aid in cable management and increased utilization of available conduit space.

When using multiple entrance rooms, entrance rooms should be at least 20 m (66 ft) apart and be in separate fire protection zones. The two entrance rooms should not share power distribution units or air conditioning equipment.

Telecommunications entrance cabling for data centers should not be routed through a common equipment room unless cabling is segregated from common access via conduit or other means.

Entrance rooms should be outside the computer room proper to improve security. However, they may be placed in the computer room or consolidated with the main distribution area if cabling distances for circuits is an issue, security is not an issue, or other security measures are used to ensure security (such as escorting and monitoring the activities of all technicians in the computer room).

Fiber density inside optical fiber cables are increasing rapidly to keep up with greater data bandwidth. This has impact on splice/patching volume in ER, which should be considered when designing an ER. This may go all the way up to providing greater floor space for ER.

The following should be considered when designing the entrance room:

- Cable quantities, dimensions, and weights
- Required number and sizes of conduits
- Conduit, tray, optical fiber duct and other pathway weight and fill capacities
- Physically clear and simple demarcation point between the access provider and customers

14.4.3.4 Additional Information

Where used for the purpose of demarcation, the entrance room typically has separate areas for access provider demarcation:

- Demarcation for balanced twisted-pair circuits (e.g., DS-0, ISDN BRI, telephone lines, DS-1 [T-1 or fractional T-1], ISDN Primary Rate, E-1 [CEPT-1])
- Demarcation for coaxial cabling circuits, (e.g., DS-3 [T-3] and E-3 [CEPT-3])
- Demarcation for optical fiber circuits (e.g., SONET/SDH, Fast Ethernet, 1/10/40/100 Gigabit Ethernet)

Each of these functions may be provided on customer-provided meet-me racks, cabinets, or frames where all service providers hand-off their circuits (see Section 14.6.3).

If an access provider demarks its services into cabinets or racks, the customer typically installs cabling from that access provider's demarcation point to the desired patching location or user equipment.

14.4.4 Main Distribution Area (MDA)

14.4.4.1 Introduction

The MDA includes the main cross-connect (MC), which is the central point of distribution for the data center structured cabling system. The main cross-connect is called the main distributor (MD) in CENELEC EN 50173-5 and in ISO/IEC 24764.

Equipment typically located in the MDA includes:

- Core routers
- Core, spine, or interconnection layer LAN and SAN switches
- High-performance computing switches
- PBX or voice gateways
- T-3 (M13) multiplexers

The MDA may serve one or more IDAs, HDAs, and EDAs within the data center and one or more telecommunications rooms (TRs) located outside the computer room space to support office spaces, operations center, and other external support rooms.

The MDA may include a horizontal cross-connect (TIA) or zone distributor (ISO/CENELEC) when equipment areas are served directly from the MDA. This space is inside the computer room; it may be located in a dedicated room for improved security.

14.4.4.2 Requirements

Every data center shall have at least one MDA. A second MDA shall be provided to meet the availability requirements of the telecommunications infrastructure (e.g., Class C4). If two MDAs are present, both shall meet all requirements of the MDA as specified in the applicable data center standard.

Access provider provisioning equipment (e.g., M13 multiplexers) may be located in the MDA rather than in the entrance room to avoid the need for a second entrance room because of circuit distance restrictions.

14.4.4.3 Recommendations

A second MDA is recommended in Class C3 data centers. Each MDA should have fully diverse cable routes to access multiple entry points so that no single point of failure exists within the site.

When utilizing two MDAs, the MDAs should:

- Have core routers and switches distributed between the MDAs
- Distribute circuits between the two spaces
- Be located in different fire protection zones
- Be served by different power distribution units and air conditioning equipment

14.4.5 Intermediate Distribution Area (IDA)

14.4.5.1 Introduction

The intermediate distribution area (IDA) is the space that supports the intermediate cross-connect. The intermediate cross-connect is called the intermediate distributor (ID) in CENELEC EN 50173-5 and in ISO/IEC 24764.

It may be used to provide a second level cabling subsystem in data centers too large to be accommodated with only MDAs and HDAs. The IDA is optional and may include active equipment such as LAN and SAN switches.

The IDA may include the horizontal cross-connect (TIA) or zone distributor (ISO/CENELEC) for equipment areas served directly from the IDA.

14.4.5.2 Recommendations

The IDA may be inside the computer room but can be located in a dedicated room or a secure cage within the computer room for additional security.

14.4.6 Horizontal Distribution Area (HDA)

14.4.6.1 Introduction

The HDA is used to serve equipment not supported by a horizontal cross-connect (HC) or zone distributor (ZD) in an IDA or MDA. The HDA is the distribution point for cabling to the EDAs.

Equipment typically located in the HDA includes:

- LAN switches
- SAN switches
- Keyboard/video/mouse (KVM) switches

This equipment is used to provide network connectivity to the equipment located in the EDAs. A small data center may not require any HDAs as the entire data center may be able to be supported from the MDA. A typical data center will have several HDAs.

14.4.6.2 Recommendations

The HDA is typically inside the computer room, but it can be located in a dedicated room or a secure cage within the computer room for additional security.

14.4.7 Zone Distribution Area (ZDA)

14.4.7.1 Introduction

The ZDA is an optional interconnection point within the horizontal cabling located between the HDA and the EDA to allow frequent reconfiguration and added flexibility.

The consolidation point in the ZDA is called the local distribution point or LDP in CENELEC EN 50173-5 and in ISO/IEC 24764.

14.4.7.2 Requirements

Horizontal cabling shall contain no more than one ZDA between the HC in the HDA and the mechanical termination in the EDA.

14.4.7.3 Recommendations

The zone distribution area may also serve as a zone outlet for nearby equipment in the computer room.

14.4.8 Equipment Distribution Area (EDA)

14.4.8.1 Introduction

The EDA is the space allocated for IT compute processing and IT storage equipment, including all forms of telecommunications equipment (e.g., computer equipment, telephony equipment).

The telecommunications outlet (TO) in the EDA is called the equipment outlet (EO) in ISO/IEC 24764, CENELEC EN 50173-5, and ANSI/TIA-942-B.

14.4.8.2 Requirements

EDA areas shall not serve the purposes of an entrance room, MDA, IDA, or HDA.

14.5 Outside Plant Cabling Infrastructure

14.5.1 Underground Service Pathways

14.5.1.1 Requirements

The upper surface of underground cable pathways shall be no less than 600 mm (24 in) below the surface.

Non-metallic conduits shall be encased in concrete with a minimum 17.24 MPa (2500 lbf/in^2) compressible strength where there is vehicular traffic above or a bend in the conduits.

Telecommunications entrance pathways shall terminate in a secure area within the data center.

The telecommunications entrance pathways shall be coordinated with other electrical underground pathways (e.g., conduits) and mechanical underground piping systems (e.g., water, waste) while maintaining appropriate pathway separation from physical and operational perspectives.

14.5.1.2 Recommendations

The data center site should include multiple duct banks with customer owned maintenance holes from the property line to the data center.

Duct banks should consist of a minimum of four 100 mm (trade size 4) or equivalent conduits or raceways. If initial plans include more than three access providers providing service to the facility, one additional 100 mm (trade size 4) or equivalent conduit or raceway should be provided for every additional access provider. Each carrier's cabling should be in separate, dedicated conduits or raceways. Carriers should not share pathways.

The number of conduits should consider expected carrier and campus cabling requirements, growth, and conduit fill capacities.

Where not defined by the AHJ, duct banks and conduits should be located at a sufficient depth, typically 600 mm (24 in) to 750 mm (30 in) below surface grade, so both live or dynamic and dead (static) or earth loads can be sustained by the conduit structure. Conduits should be a depth greater than the depth of anticipated future digging.

In regions susceptible to frost, the top of the conduit(s) should be below the frost line. Where this is not practical, adequate protection should be provided to ensure that conduits do not become damaged as a result of ground shifting, particularly at the point of entry into the building.

Maintenance holes and hand holes on the data center property should have locks or other means of deterring access such as nonstandard bolts. The maintenance holes and hand holes should have intrusion detection devices connected to the building security system and monitoring of the maintenance holes and hand holes by video surveillance or other means.

Redundant duct banks should have a 20 m (66 ft) separation minimum along the entire route from the property line to the facility. Where possible, redundant maintenance holes should be connected with at least one 100 mm (trade size 4) or equivalent conduit or raceway.

Conduits for cable replacement should be designated and marked separately from those for additional cables.

When multiple access providers are providing service to the facility, coordination of security requirements of each individual access provider should be within the secure space.

The secure area that houses the telecommunications entrance facility (pathway termination) should preferably be in a telecommunications entrance room that is separate from the computer room.

Any pull boxes or splice boxes for data center cabling (entrance cabling or cabling between portions of the data center) that are located in public spaces or shared tenant spaces should be lockable. They should also be monitored by the data center security system using either a camera or remote alarm.

Entrance to utility tunnels used for telecommunications entrance rooms and other data center cabling should be lockable. If the tunnels are used by multiple tenants or cannot be locked, they should be monitored by the data center security system using either a camera or remote alarm.

14.5.2 Aerial Service Pathways

14.5.2.1 Requirements

Routes for aerial access pathways shall follow same provisioning guidelines from an availability and security perspective as underground data pathways. All aerial pathways shall be properly bonded and grounded as per AHJ requirements.

14.5.2.2 Recommendations

The use of aerial cabling pathways should generally be avoided because of vulnerability to outages. Aerial cabling route selection should take into consideration a number of factors, including, but not limited to, terrain, soil conditions, aesthetics, proximity to direct-buried and underground utilities, access, and weather conditions.

Customer-owned satellite dish farms or aerial towers should be located within the secure perimeter of the facility.

14.6 Access Providers

14.6.1 Access Provider Coordination

14.6.1.1 Requirements

Data center designers shall coordinate with all access providers to determine the access providers' requirements and to ensure that the data center's circuit, demarcation, and entrance facility requirements are provided to satisfy the access providers' specifications.

14.6.1.2 Additional Information

Access providers typically require the following information when planning entrance facilities:

- Address of the building
- General information concerning other uses of the building, including other tenants
- Plans with detailed drawings of telecommunications entrance conduits from the property line to the entrance rooms, including location of maintenance holes, hand holes, and pull boxes
- Assignment of conduits and innerducts to the access provider
- Floor plans for the entrance rooms
- Assigned location of the access providers' protectors, racks, and cabinets
- Routing of cabling within entrance room (e.g., under access floor, over cabinets and racks, other)
- Expected quantity and type of circuits to be provisioned by the access provider, including any planned or foreseen additions or upgrades
- Media types and approximate distances of circuits to be provisioned by the carrier
- Service-level agreements
- Detailed schedules for the project, including date that the access provider will be able to install entrance cabling and equipment in the entrance room and required service activation date
- Requested location and interface for demarcation of each type of circuit to be provided by the access provider
- Carrier office diversity desired, preferably at least two separate access provider offices and service provider point-of-presences
- Carrier route diversity desired, preferably a minimum distance between any two routes of at least 20 m (66 ft) along their entire routes
- Specification of pathways to be used for access provider cabling (e.g., aerial cabling allowed or all underground)
- Type and rating of firestopping measures used at the site
- Requested service date
- Name, telephone number, and e-mail address of primary customer contact and local site contact
- Security requirements for lockable containment and cabinets
- Colocation providers may be required to provide customer name and contact details, if requesting on behalf of their customers

The access providers typically provide the following information:

- Space and mounting requirements for protectors and terminations of balanced twisted-pair cabling
- Quantity and dimensions of access provider's cabinets and racks or space requirements if they are to be provisioned in client cabinets and racks
- Power requirements for equipment, including receptacle types
- Access provider equipment service clearances
- Location of serving access provider central offices
- Route of access provider cabling and minimum separation between routes
- Specification on pathways used (e.g., all underground or portions of routes that are served by aerial cabling)
- Installation and service schedule

14.6.2 Redundancy

14.6.2.1 Introduction

Having multiple access providers protects against total loss of service in the event of a service outage affecting one of the access providers but not the others. However, it is necessary to ensure that the access providers are not sharing facilities that would result in one or more single points of failure that would cause a total service outage despite having multiple access providers.

14.6.2.2 Recommendations

Continuity of telecommunications access provider services to the data center can be improved by using multiple access providers, multiple access provider central offices, and multiple diverse pathways from the access provider central offices to the data center.

The customer should ensure that its services are provisioned from different access provider offices, and the pathways to these access provider cabling centers and central offices are diversely routed. These diversely routed pathways should be physically separated by at least 20 m (66 ft) at all points along their routes.

Access providers should install circuit-provisioning equipment in both entrance rooms so that circuits of all required types can be provisioned from either room. The access provider provisioning equipment in one entrance room should not be subsidiary to the equipment in the other entrance room. The access provider equipment in each entrance room should be able to operate in the event of a failure in another entrance room.

14.6.3 Access Provider Demarcation

14.6.3.1 Introduction

The centralized location for demarcation to all access providers is a single-tenant data center is typically in the telecommunications entrance rooms. In a colocation data center, the meet me room (MMR) is the place where telecommunications service providers (e.g., access providers, content providers, internet service providers) connect to customers and each other. This room may be the same or different room as the telecommunications entrance rooms. The telecommunications service providers or data center owner may opt to locate telecommunications service provider equipment either in the telecommunications entrance rooms or MMRs.

14.6.3.2 General Requirements

In buildings where base isolation is used, access providers shall provide sufficient cable slack to accommodate displacement of the base isolation units.

14.6.3.3 General Recommendations

Access providers should provide demarcation for their circuits in a common owner specified cabinet or rack rather than in their own cabinets or racks as this simplifies cross-connects and management of circuits. Separate demarcation cabinets or racks for each type of circuit may be desirable (e.g., low speed, E-1/T-1, E-3/T-3, optical fiber for STM-x/OC-x services and Ethernet delivery). Cabling from the computer room to the entrance room should terminate in the demarcation areas.

14.6.3.4 Demarcation of Low-speed Circuits

14.6.3.4.1 Recommendations

Access providers should be asked to provide demarcation of low-speed circuits on insulation displacement connection (IDC) connecting hardware. While service providers may prefer a specific type of IDC connecting hardware (e.g., 66-block), they may be willing to hand off circuits on another type of IDC connecting hardware upon request. Access provider should coordinate the type of connectors used with those used by the data center.

Cabling from the low-speed circuit demarcation area to the main distribution area should be terminated on IDC connecting hardware near the access provider IDC connecting hardware.

Circuits from access providers are terminated using one or two pairs on the access provider IDC connecting hardware. Different circuits have different termination sequences as illustrated in Figure 14-7 and Figure 14-8.

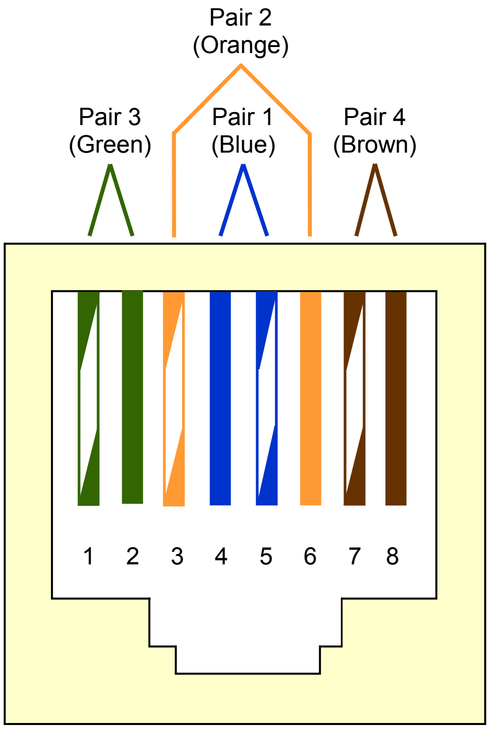


Figure 14-7
Cross-Connection Circuits to IDC Connecting Hardware Cabled to Modular Jacks in the T568A 8-Pin Sequence

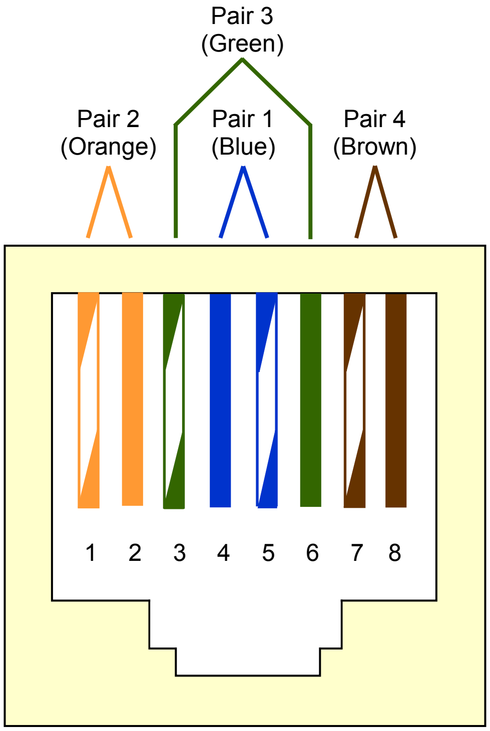


Figure 14-8
Cross-Connection Circuits to IDC Connecting Hardware Cabled to Modular Jacks in the T568B 8-Pin Sequence

Each 4-pair cable from the entrance room to the other spaces in the data center should be terminated in an IDC connector or an eight-position modular jack of compatible performance where the cable terminates outside the entrance room. The IDC connector or eight-position modular jack telecommunications outlet/connector should meet the modular interface requirements specified in standards such as the IEC 60603-7 series of standards.

Pin/pair assignments should be as shown in the T568A sequence, or optionally per the T568B sequence to accommodate certain 8-pin cabling systems as necessary. The colors shown are associated with the horizontal distribution cable. Figure 14-7 and Figure 14-8 depict the front view of a female telecommunications outlet/connector and provide the list of the pair positions for various circuit types.

14.6.3.4.2 Additional Information

The conversion from access provider 1-pair and 2-pair cabling to 4-pair cabling used by the data center structured cabling system can occur either in the low-speed circuit demarcation area or in the main distribution area (MDA).

The access provider and customer IDC connecting hardware can be mounted on a plywood backboard, frame, rack, or cabinet. Dual-sided frames should be used for mounting large numbers of IDC connecting hardware (3000+ pairs).

14.6.3.5 Demarcation of E-1 and T-1 Circuits

14.6.3.5.1 Introduction

Coordinate with the local access providers that will install DS-1/E-1 DSX panels in the DS-1/E-1 demarcation area. Their equipment will preferably fit in 480 mm (19-inch) racks/cabinets. However, 580 mm (23-inch) racks/cabinets may be required by some local access providers, particularly in North America.

14.6.3.5.2 Recommendations

The DSX-1 patch panels may require power for indicator lights. Thus, cabinets or racks supporting access provider DSX-1 patch panels should have at least one electrical circuit or power strip to power DSX-1 panels. As most DSX-1 facilities use -48 V_{DC} or +24 V_{DC} to power their indicators, provisions for DC power sources and fuse panels should be included in any DSX facility.

Cabinet or rack space should be allocated for access provider and customer patch panels, including growth. Access providers may require cabinet or rack space for rectifiers to power DSX-1 patch panels.

A single 4-pair cable can accommodate one T-1 transmit and receive pair. When multiple T-1 circuits are carried on a multipair cable arrangement, multiple cables should be provided; transmit signals should be carried on one multipair cable and the receive signals driven through a separate multipair cable.

If support staff has the test equipment and knowledge to troubleshoot T-1 circuits, the DS-1 demarcation area can use DSX-1 panels to terminate T-1 cabling to the main distribution area. These DSX-1 panels should have either modular jacks or IDC terminations at the rear although wirewrap terminations are acceptable and may still be used.

DSX-1 panels for the main distribution area can be located on the same racks, frames, or cabinets as the ones used for distribution cabling. If DSX panels are separate, they should be located in a space adjacent to the cabinets or racks used for distribution cabling.

The owner or the owner's agent may decide to provide multiplexers (e.g., M13 or similar multiplexer) to demultiplex access provider E-3/T-3 circuits to individual E-1/T-1 circuits. Multiplexers may be placed in the computer room, extending the distance from the entrance rooms that E-1/T-1 circuits can be provisioned. E-1/T-1 circuits from a customer-provided multiplexer should not be terminated in the entrance room E-1/T-1 demarcation area.

The coaxial or optical fiber connecting hardware can be located on the same or separate racks, frames, or cabinets as the ones used for other access provider patch panels. If they are separate, they should be adjacent to the racks/cabinets assigned to the access provider's equipment.

As with other services, the access provider should be consulted to determine and agree to the format of the services from an E-1/T-1 carrier. The normal practice is to have these services provided via telecommunications outlet/connectors.

Access providers should be asked to hand-off E-1/T-1 circuits on RJ48X jacks (individual 8-position modular jacks with loop back), preferably on a DSX-1 patch panel mounted on a customer-owned rack installed in the DS-1 demarcation area. Patch panels from multiple access providers and the customer may occupy the same cabinet or rack.

14.6.3.5.3 Additional Information

Access providers can alternatively hand off DS-1 circuits on IDC connecting hardware. These IDC connecting hardware can be placed on the same frame, backboard, rack, or cabinet as the IDC connecting hardware for low-speed circuits.

The customer may request that the demarcation for E-1 or T-1 circuits be provisioned in the MDA rather than in the entrance room to ensure that circuit distance restrictions are not exceeded. See ANSI/TIA-942-B for distances for T-1 and E-1 circuits in data centers. As described in ANSI/TIA-942-B, note that customer side-DSX panels provide test access for circuits, but they reduce maximum circuit distances.

14.6.3.6 Demarcation of T-3 and E-3 Coaxial Cabling Circuits

14.6.3.6.1 Recommendations

Access providers should be asked to hand-off E-3 or T-3 coaxial circuits on pairs of female BNC connectors, preferably on a DSX-3 patch panel on a customer-owned cabinet or rack installed in the E-3/T-3 demarcation area. Patch panels from multiple access providers and the customer may occupy the same cabinet or rack.

Coordination with the local access providers should involve the installation of DS-3 DSX panels in the DS-3 demarcation area. This equipment should be mounted in 480 mm (19-inch) cabinets or racks in order to maintain consistency with other racks/cabinets. However, 580 mm (23-inch) cabinets or racks may be required by some local access providers, particularly in North America.

If support staff has the test equipment and knowledge to troubleshoot E-3 or T-3 circuits, the E-3/T-3 demarcation area can use DSX-3 panels to terminate 734-type coaxial cabling to the main distribution area. These DSX-3 panels should have BNC connectors at the rear.

The DSX-3 patch panels may require power for indicator lights. Thus, racks/cabinets supporting access provider DSX-3 patch panels should have at least one electrical circuit and a power strip. As most DSX-3 facilities use -48 V_{DC} or +24 V_{DC} to power their indicators, provisions for DC power sources and fuse panels should be included in any DSX facility.

Allocate cabinet and rack space for access provider and customer patch panels, including growth. Access providers may require cabinet and rack space for rectifiers to power DSX-3 patch panels.

Cabling from the E-3/T-3 demarcation area to the main distribution area should be 734-type coaxial cable. Cables in the E-3/T-3 demarcation area can be terminated on a customer patch panel with 75-ohm BNC connectors or directly on an access provider DSX-3 patch panel. Access provider DSX-3 patch panels typically have the BNC connectors on the rear of the panels. Thus, BNC patch panels for cabling to the main distribution area should be oriented with the front of the patch panels on the same side of the cabinet or rack as the rear of the access provider DSX-3 panels.

All connectors and patch panels for E-3 and T-3 cabling should use 75-ohm BNC connectors.

14.6.3.6.2 Additional Information

The customer may request that the demarcation for E-3 or T-3 circuits be provisioned in the MDA rather than in the entrance room to ensure that circuit distance restrictions are not exceeded. See the applicable cabling standard (e.g., ANSI/TIA-942-B) for maximum distances of T-3 and E-3 circuits over coaxial cabling in data centers. As described in ANSI/TIA-942-B, note that customer side-DSX panels provide test access for circuits, but they reduce maximum circuit distances.

14.6.3.7 Demarcation of Optical Fiber Circuits

14.6.3.7.1 Recommendations

Access providers should terminate optical fiber circuits on optical fiber patch panels installed on cabinets or racks in the fiber demarcation area. Optical fiber patch panels from multiple access providers and the customer may occupy the same cabinet or rack. The optical fiber interface should comply with requirements defined in the cabling standards being followed (e.g., IEC 61754-20 [duplex LC-APC]). If requested, access providers may be able to provide a different format connector that is compatible with existing connector formats being used to simplify equipment cord and patch cord requirements.

Coordination with the local access providers should involve the installation of optical fiber patch panels in the optical fiber demarcation area. This equipment should be mounted in 480 mm (19-inch) cabinets or racks in order to maintain consistency with other racks/cabinets. However, 580 mm (23-inch) cabinets or racks may be required by some local access providers, particularly in North America.

Cabling from the optical fiber demarcation area to the main cross-connect in the main distribution area should be coordinated to ensure that the correct quantity, circuit type, media type and interface type are provided.

14.6.3.7.2 Additional Information

The customer may request that the demarcation of optical fiber circuits be provisioned in the MDA rather than in the entrance room to ensure that service provision performance requirements and onward circuit distance restrictions are not exceeded.

In a high-density fiber environment, access providers should consider installing free-standing frames such as two-post frames.

Dark fiber circuits (optical fiber circuits that include optical fiber cable and connectors, but no equipment) should also be terminated in the fiber demarcation area. Dark fiber circuits may either be provided and maintained by the data center owner or by a third-party, such as an access provider. They may be terminated in the patch panels provided by the access provider or by the data center owner.

14.7 Telecommunications Cabling Pathways

14.7.1 General

14.7.1.1 Requirements

Except where otherwise specified, data center cabling pathways shall adhere to the specifications of relevant cabling and containment specifications such as ANSI/TIA-569-D, CENELEC EN 50174-2, or ISO/IEC 14763-2.

Pathways shall be sized for full data center occupancy, including all anticipated expansions and planned applications.

The maximum depth of telecommunications cabling within a solid bottomed cabling pathway (e.g., cable tray, duct) shall not exceed 150 mm (6 in), regardless of the depth of the cable pathway.

For cabling pathway systems that do not contain a solid bottom, the maximum depth of installed cabling is determined by the spot loading and pressure it exerts on the support points of the pathway system. The height of the cable can be determined by using Equation 14-1 or 14-2, where L is the largest distance between support points in the specific cable pathway system and H is the resultant calculated allowed height of the cables.

For values of L as measure in millimeters (mm):

$$H\ (mm) = \frac{150}{1 + (L \times 0.0007)} \tag{14-1}$$

For values of L as measured in inches (in):

$$H\ (in) = \frac{152.4}{25.4 + (L \times 0.4516)} \tag{14-2}$$

Cable heights in these pathways shall not exceed this calculated value. For convenience, Table 14-5 summarizes the calculated results for common interval distances between supports.

Table 14-5 Maximum Cable Stacking Height in Cabling Pathways

L *Distance between points of support (mm)*	*H* *Maximum stacking height in cable pathways (mm)*
0 mm	150.0 mm
100 mm	140.2 mm
150 mm	135.7 mm
250 mm	127.7 mm
500 mm	111.1 mm
750 mm	98.4 mm
1000 mm	88.2 mm
1500 mm	73.2 mm

L *Distance between points of support (in)*	*H* *Maximum stacking height in cable pathways (in)*
0 in	6.00 in
4 in	5.60 in
6 in	5.42 in
12 in	4.94 in
24 in	4.21 in
36 in	3.66 in
48 in	3.24 in
60 in	2.90 in

Pathway systems shall be secured in accordance with AHJ, seismic requirements for the location, and the planned long-term loading. When access floor systems are used, any one of the following methods shall be permitted:

- If approved by pathway and floor system vendors, attachment to metal struts that are captured below the floor by two or more access floor stringers may be acceptable.
- Attachment to metal struts below the access floor that are suitably attached to the permanent floor
- Attachment via threaded rod directly to the permanent floor
- Attachment to channel bases bolted to floor slab

Structured cabling shall not share space within a dedicated optical fiber raceway with optical fiber equipment cords and patch cords. Cables shall not be placed on the bare concrete in contact with earth to avoid moisture. Plan cable tray capacities for the data center at full occupancy. Pay particular attention to cable tray capacities at the distributors and at intersections of cable trays.

14.7.1.2 Recommendations

Where it is not possible to adequately size pathways for full data center occupancy, including future expansions and applications, consider other media (such as optical fiber) or different network architectures (such as distributed LAN and SAN switching) to reduce cabling requirements.

In locations where seismic activity could create a potential risk, telecommunications pathways should be braced per AHJ and applicable standards (see Section 8).

There should be separate raceways or a divider in the raceway to separate balanced twisted-pair and optical fiber cabling. Where it is not practical to separate optical fiber and balanced twisted-pair cabling, optical fiber cabling should be on top of, rather than underneath, balanced twisted-pair cabling.

Optical fiber equipment cords and patch cords should be installed in a dedicated optical fiber pathway that ensures that proper bend radius control is maintained throughout the installation.

Optical fiber cabling should not touch the slab or lay on top of the access floor when it exits a cable tray.

Cabling and cabling pathways should be installed overhead if ceiling heights permit.

All telecommunications cabling under the access floor should be installed in a cabling pathway that is listed or classified by a nationally recognized testing laboratory (NRTL). In the equipment cabinet aisles, allocate separate aisles for power and telecommunications cabling. Telecommunications cabling should be in the hot aisles (the aisles at the rear of the cabinets) and the power cabling should be in the cold aisles (the aisles at the front of the cabinets). Placing the telecommunications cabling in the cold aisles is not recommended as the telecommunications raceways may block airflow to perforated tiles, which should be located in the cold aisles.

14.7.2 Security

14.7.2.1 Requirements

Telecommunications cabling for data centers shall not be routed through spaces accessible by the public or by other tenants of the building unless the cables are in enclosed conduit or other secure pathways.

14.7.2.2 Recommendations

Physical access to cabling infrastructure should be limited strictly to data center cabling engineers and access provider personnel (under data center supervision) on a strictly need-to-access basis.

Any maintenance holes or hand holes on the data center property should have a lock or other means to prevent unauthorized access.

14.7.3 Separation of Power and Telecommunications Cabling

14.7.3.1 Requirements

To minimize coupling between power cabling and balanced twisted-pair cabling, the separation and segregation between power cabling and balanced twisted-pair cabling shall follow the requirements specified by the AHJ and defined in the cabling and pathways standards being followed.

AHJ may require a barrier or greater separation than specified in the cabling and pathways standards.

Where they are used, metallic cabling pathways shall be properly bonded and grounded as per AHJ requirements and applicable standards (e.g., ANSI/NECA/BICSI-607, ANSI/TIA-607-C, ISO/IEC 30129).

14.7.3.2 Recommendations

For computer rooms that use the space under access floor systems for the routing of power and balanced twisted-pair cabling, allocate separate aisles for power and telecommunications cabling whenever possible. Where it is not possible to allocate separate aisles for power cabling and telecommunications cabling in the main aisles, then provide both horizontal and vertical separation of power cabling and telecommunications cabling in the same aisles. Provide horizontal separation by allocating different rows of tiles in the main aisles for power cabling and telecommunications cabling with the power cabling and telecommunications cabling as far apart from each other as possible. Additionally, vertical separation should be provided by placing the telecommunications cabling in cable trays (e.g., wire basket tray) as far above the power cables as possible with the top of the cable tray no less than 50 mm (2 in) below the bottom of the access floor tile. Cables should not impede airflow to equipment in cabinets.

14.7.3.3 Additional Information

There are no requirements for separation of power and telecommunications cabling crossing at right angles, except the separation requirements mandated by applicable electrical codes.

Refer to applicable cabling standards (e.g., ISO/IEC 14763-2, CENELEC 50174-2, ANSI/TIA-942-B) regarding requirements for separation of power and telecommunications cabling.

The performance of a cabling pathway system is dependent on its proper installation, including supports and cabling. Neglecting installation and maintenance guidelines could lead to personal injury as well as damage to property.

14.7.4 Cable Tray Support Systems

14.7.4.1 General Requirements

When routing telecommunications cabling from a cabling pathway to entry into cabinets or frames or when changing between levels of cabling pathways, the cabling shall be managed to maintain their minimum bend radius requirements and be protected from damage or compression when crossing any edge of the cabling pathway system.

Cable ladders and cable tray shall be installed per manufacturers' recommendations.

Supports for the cable ladders and cable tray shall be independent from non-telecommunications utilities (e.g., ducts, conduits, plumbing, luminaries).

Exposed threads and sharp ends of threaded rods shall be covered where they are located where cables may be in contact with them (for example, within cable trays or adjacent to cable ladders.

WARNING: Cable tray shall not be used as a walkway, ladder, or support for people unless the tray is specifically designed for such use.

Non-armored, small diameter optical fiber cables (less than 4 mm in diameter) and optical fiber patch cords should not be placed in wire basket trays without solid bottoms or non-continuous pathways without radiused supports.

14.7.4.2 Overhead Cable Trays

14.7.4.2.1 Requirements

In data centers that use overhead pathways, 200 mm (8 in) minimum access headroom shall be provided from the top of the pathway to the obstruction located above such as another pathway or the ceiling. This clearance requirement does not apply where cable trays cross each other or cross beams, pipes or other building structures.

Typical cable tray types for overhead cable installation include wire basket cable tray, ladder type, or center spine cable tray. Adjacent sections of metallic cable tray shall be bonded together and grounded per manufacturers' guidelines, ANSI/NECA/BICSI 607, other applicable standards (e.g., ANSI/TIA-607-C, ISO/IEC 30129), and AHJ requirements (e.g., NFPA 70), and shall be listed or classified by a NRTL for this purpose. The metallic cable tray system shall be bonded to the data center common bonding network.

When they are supported from above, overhead cable ladders or trays (if used) shall be suspended from the structure above utilizing M12 (0.5 in) or greater threaded rods as required for structural support. Alternatively, the cable trays or ladders may be supported by an overhead support structure using support pillars or a suspended frame designed to support the load of the cable tray and cables.

If used for seismic bracing, ladder racks and cable tray shall be continuous wall to wall to form a brace for the equipment.

Cable tray shall not be routed directly below fire suppression or sprinkler systems.

14.7.4.2.2 Recommendations

In data centers that use overhead pathways, 300 mm (12 in) minimum access headroom should be provided from the top of the pathway to the obstruction located above such as another pathway or the ceiling.

Overhead cabling improves cooling efficiency and is a best practice where ceiling heights permit because it can substantially reduce losses because of supply airflow obstruction and turbulence caused by underfloor cabling and cabling pathways. Other potential advantages of overhead cable tray systems include elimination of access floor, separation of telecommunications cabling from power cabling and plumbing, flood survival, and improved access to cabling. Methods can include ladder racks or cable trays. Care must be taken in the placement of overhead cabling to ensure that return air flow is not obstructed. (See also Section 10.5).

Overhead cable trays may be installed in several layers to provide additional capacity. An installation may include two or three layers of cable trays, one for power cabling and one or two for telecommunications cabling. These overhead cable trays may be supplemented by a duct or tray system for optical fiber equipment cords or patch cords and if there is no access floor system, by brackets for the computer room bonding network.

In aisles and other common spaces in colocation facilities and other shared tenant data centers, overhead cable trays should be protected by one of the following means:

- Solid bottoms and covers
- Height at least 2.7 m (9 ft) above the finished floor to limit accessibility
- Protected through alternate means from accidental and intentional damage

When choosing between supporting cable trays from overhead or from below, overhead suspension is preferred as suspended cable trays provide more flexibility when adding or removing cabinets and racks of varying heights. However, suspended cable trays may require a dedicated support infrastructure and additional planning to preserve the structural integrity of the ceiling. Mechanically fastening cable trays directly to cabinets or racks offers a more compact design that does not affect the structural integrity of the ceiling. However, this method is only suitable if cabinets and racks to which these cable trays are attached will remain throughout the life of the computer room and it is certain that no equipment, cabinets, or racks taller than those to which the cable trays are attached will be needed.

14.7.4.3 Underfloor Cable Trays

14.7.4.3.1 Requirements

When telecommunications cabling is installed under the access floor, it shall be installed in cabling pathways that have no sharp edges that can potentially damage cables.

If the underfloor cable tray attaches to the access floor pedestals or stringers, the loading and attachment method shall comply with the floor manufacturer’s specifications.

Clearance from the bottom of the access floor tile to the top of the cable tray or other raceway shall be at least 50 mm (2 in) to permit cable bundles and innerduct to exit out the top of the tray without incurring damage.

Metallic cable trays utilized in underfloor applications shall be listed or classified by an applicable NRTL. Adjacent sections of metallic cable tray shall be mechanically bonded together and provide electrical continuity and conductivity. Metallic cable trays shall be bonded to the data center’s common bonding network.

The maximum depth of telecommunications cabling in the cable tray shall not exceed 150 mm (6 in) regardless of the depth of the cable tray.

14.7.4.3.2 Recommendations

The underfloor cable trays may be installed in multiple layers to provide additional capacity. Typical installations include two or three layers of cable trays, one for power cabling, and one or two for telecommunications cabling. These underfloor cable trays may be supplemented by a duct or tray system to manage optical fiber jumpers, patch cords, and equipment cords. There should be 300 mm (12 in) and no less than 200 mm (8 in) clearance between layers of underfloor cable trays run in parallel and stacked directly above each other.

Under access floors, upper cable trays should be narrower than lower trays to allow access or have a full tile with no cable trays to provide access for installation and removal of cables.

14.7.4.4 Coordination of Cable Tray Routes

14.7.4.4.1 Recommendations

Planning of overhead cable trays for telecommunications cabling should be coordinated with architects, mechanical engineers, electrical engineers, and plumbing and structural engineers that are designing luminaries, plumbing, HVAC, power, and fire protection systems. Coordination should consider routing, clearances, and accessibility; consider use of three-dimensional drawings to simplify coordination.

Lighting fixtures (luminaires) and sprinkler heads should be placed between cable trays, not directly above cable trays.

Underfloor cable tray routing should be coordinated with other underfloor systems during the planning stages of the building.

14.7.4.5 Underfloor Foam Mats

14.7.4.5.1 Requirements

Where foam matting is used as an underfloor pathway or containment, the foam matting shall be secured to prevent lifting where low or no cables are present and to prevent disturbance of the underfloor airflow.

Foam matting shall also comply with the fire performance requirements for the space it occupies.

14.7.4.5.2 Recommendations

Where foam matting is used as an underfloor pathway or containment, it should be a minimum of 13 mm (0.5 in) thick and fill the aisle between the floor pedestals.

14.8 Backbone Cabling

14.8.1 Introduction

The function of the backbone cabling is to provide connections between the MDA, IDA, HDA, and entrance rooms in the data center cabling system.

Backbone cabling consists of the backbone cables, MC/MD, IC/ID, mechanical terminations, equipment cords, and patch cords or jumpers used for backbone-to-backbone cross-connection.

The backbone cabling is expected to serve the needs of the data center occupants for one or several planning phases, each phase spanning a time scale that may span days, months, or years. During each planning period, the backbone cabling design should accommodate growth and changes in service requirements without the installation of additional cabling. The length of the planning period is ultimately dependent on the design logistics, including material procurement, transportation, and installation and specification control.

14.8.2 General Requirements

The backbone cabling shall allow network reconfiguration and future growth without disturbance of the backbone cabling.

14.8.3 General Recommendations

The backbone cabling should support different connectivity requirements, including both the network and physical console connectivity such as local area networks, wide area networks, storage area networks, computer channels, and equipment console connections.

14.8.4 Cabling Types

14.8.4.1 Introduction

Cabling specified by this standard is applicable to different application requirements within the data center environment. Depending upon the characteristics of the individual application, choices with respect to transmission media should be made. In making this choice, factors to be considered include:

- Flexibility with respect to supported services
- Required useful life of cabling
- Computer room size
- Type and quantity of systems supported
- Channel capacity (transmission performance characteristics) within the cabling system
- Equipment vendor recommendations or specifications

14.8.4.2 Requirements

Each recognized cable has individual characteristics that make it suitable for a range of applications defined against each category or cabling type in the applicable cabling standards. A single cable may not satisfy all end user requirements. It may be necessary to use more than one medium in the backbone cabling. In those instances, the different media shall use the same facility architecture with the same location for cross-connects, mechanical terminations, and interbuilding entrance facilities.

As a result of the wide range of services and site sizes where backbone cabling will be used, more than one transmission medium is recognized. This standard specifies the transmission media that shall be used individually or in combination in the backbone cabling.

Recognized cables, associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet all applicable requirements specified in applicable standards and related addenda (e.g., ISO/IEC 11801-1, ANSI/TIA 568.2-D, ANSI/TIA-568.3-D).

Backbone cabling shall consist of one or more of the following media types:

- 100-ohm balanced twisted-pair Category 5e/Class D minimum, (Category 6/Class E or higher recommended)
- OM3 multimode optical fiber cable minimum, (OM4 or OM5 multimode optical fiber cable recommended)
- OS1 or OS2, single-mode optical fiber cable
- 75-ohm coaxial cabling (Telcordia GR-139-CORE 734-type and 735-type)

NOTES:

1. 734-type and 735-type 75-ohm coaxial cables as specified in Telcordia GR-139-CORE are permitted for E-1, E-3, and T-3 circuits.
2. If specific applications require other types of cabling (e.g., Infiniband cabling, ANSI/TIA-232, V.35, SCSI), the other types may be installed in addition to the cabling listed above. Transmission performance compliance with applicable standards shall apply to local requirements.
3. To determine the suitability of the cabling types listed above for specific applications, systems suppliers, equipment manufacturers, and systems integrators should be consulted.

14.8.5 Redundant Backbone Cabling

14.8.5.1 Introduction

Redundant backbone cabling protects against an outage caused by damage to the primary backbone cabling. Redundant backbone cabling may be provided in several ways, depending on the degree of protection desired.

14.8.5.2 Recommendations

Backbone cabling between two spaces (e.g., a horizontal distribution area and a main distribution area) can be provided by running two cabling channels between these spaces, preferably along different routes. If the computer room has two main distribution areas, redundant backbone cabling to the horizontal distribution area may not be necessary although the routing of cabling to the two main distribution areas should follow different routes.

Some degree of redundancy can also be provided by installing backbone cabling between horizontal distribution areas. If the backbone cabling from the main distribution area to the horizontal distribution area is damaged, connections can be patched through another horizontal distribution area.

14.8.6 Backbone Cabling Length Limitations

14.8.6.1 Introduction

The supportable backbone cabling topologies for the media types recognized in this standard are application and media dependent. Refer to applicable standards for additional information regarding optical fiber and balanced twisted-pair cabling design considerations, including recommended distances and allowable maximum channel insertion loss based on the application's requirements.

Applications with data rates equal to or greater than 1 Gbps should be reviewed in detail to assess support over existing cabling as well as the design for new cabling. For optical fiber, when designing individual optical fiber links or assessing existing cabling, the maximum allowable channel insertion loss for each application must be considered. For balanced twisted-pair cabling, application distances can be constrained by the cabling category.

The compilation of application information detailed in applicable standards (e.g., ANSI/TIA-568.0-D, EN 50173-5, ISO/IEC 11801-5) provide the basic information to make informed decisions about optical fiber and balanced twisted-pair cabling usage and system design.

Interconnections between the individual areas, which are outside the scope of this standard, may be accomplished by employing equipment and technologies normally used for wide area applications.

14.8.6.2 Requirements

In data centers that use longer balanced twisted-pair equipment cords and patch cords, the backbone cabling distances shall be designed to accommodate the maximum cordage length so that when configuring channels for use with applications the combination of equipment cord, permanent link and patch cords never exceeds the channel loss limits.

14.8.6.3 Recommendations

Users of this standard are advised to consult the specific standards associated with the planned service or equipment manufacturers and systems integrators to determine the suitability of the cabling described herein for specific applications.

For balanced twisted-pair cabling, to reduce the effect of multiple connections in close proximity on NEXT loss and return loss, cabling system manufacturers' guidance should be sought on their recommendations for the minimum distance between connection points in a channel. Without that guidance, the backbone cabling lengths should be at least 15 m (50 ft).

14.8.7 Centralized Optical Fiber Cabling

14.8.7.1 Introduction

Many users of data networks implement their network architecture with centralized electronics versus distributed electronics in the computer room.

Centralized cabling provides connections from EDAs to centralized cross-connects by allowing the use of pull-through cabling, interconnection, or splices in the HDA and IDA.

Centralized optical fiber topologies permit the intermediate distribution areas and horizontal distribution areas to have no switches.

An example of centralized optical fiber cabling is shown in Figure 14-9.

14.8.7.2 General Requirements

The administration of moves, adds, and changes for centralized optical fiber cabling shall be performed at the centralized cross-connect. Centralized cabling design shall allow for migration (in part or in total) of the pull-through, interconnect, or splice implementation to a cross-connection implementation.

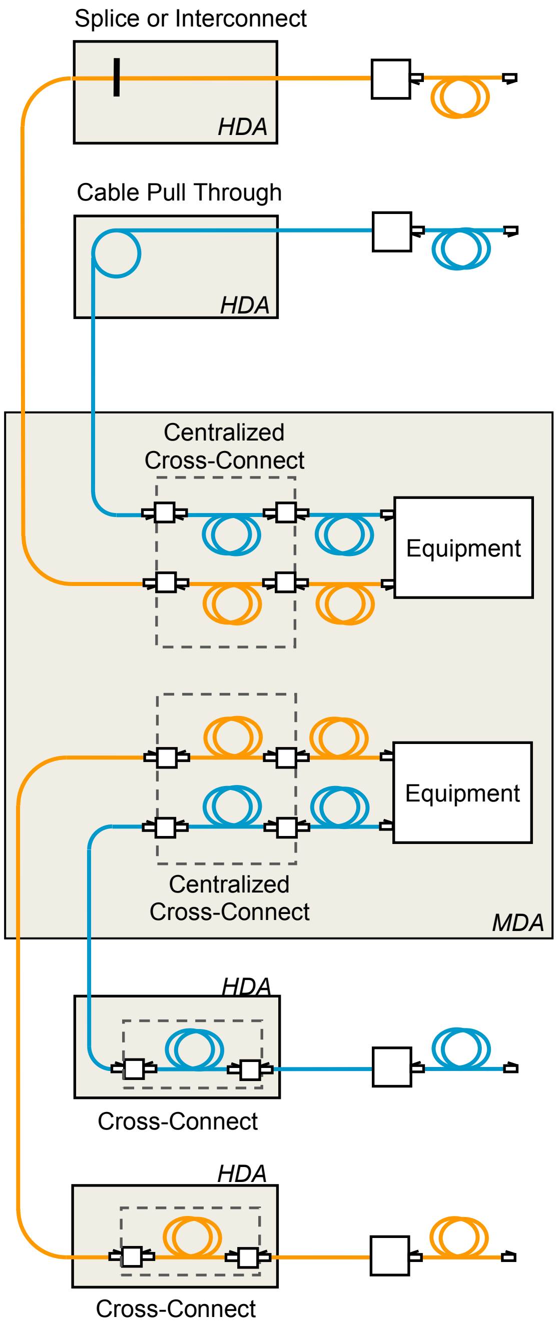


Figure 14-9
Centralized Optical Fiber Cabling Example

Centralized cabling design shall allow for the addition and removal of horizontal and backbone optical fiber cabling. Sufficient space shall be left in the HDA and IDA to allow for the addition of patch panels needed for the migration of the pull-through, interconnect, or splice to a cross-connection.

Sufficient cable slack shall exist in the HDA and IDA to allow movement of the cables when migrating to a cross-connection. Cable slack storage shall provide cable bend radius control so that optical fiber cable bend radius limitations are not violated. Optical fiber cable slack shall be stored in protective enclosures.

14.8.7.3 General Recommendations

Cable slack may be stored as jacketed cable or unjacketed optical fiber (buffered or coated). The layout of the termination hardware should accommodate modular growth in an orderly manner.

14.8.7.4 Centralized Optical Fiber Length Limitations

Centralized cabling implementations shall consider the length limitations of current and expected future protocols, particularly for multimode optical fiber.

> NOTE: Future applications may increase demands on the bandwidth performance from the optical fiber and reduce the operational channel distance.

14.8.7.5 Centralized Cabling Implementation

14.8.7.5.1 Requirements

Centralized cabling design shall allow for migration (in part or in total) of the pull-through (continuous sheath cables), interconnect, or splice implementation to a cross-connection implementation or configuration utilizing equipment (e.g., switches) in the distributors. Centralized cabling shall support the administration and labeling requirements of the cabling standards being followed. Administration of moves and changes shall be performed at the centralized cross-connect. In addition, computer room splice and interconnect hardware shall be labeled with unique identifiers on each termination position. Polarity shall adhere to the requirements of the cabling standards being followed. Service loop storage shall provide bend radius control so that optical fiber bend radius limitations are not violated.

14.8.7.5.2 Recommendations

The computer room backbone subsystem should be designed with sufficient spare circuit capacity to service network equipment needs from the centralized cross-connect without the need to pull additional computer room backbone cables. The computer room backbone optical fiber strand count should be sized to deliver present and future loading to the maximum expected equipment density within the area served by the computer room. Generally, a minimum of two optical fiber strands are required for each network connection device served by the optical fiber cabling system. Service loops for migration to cross-connect or distributed equipment configurations may be stored as jacketed cable or unjacketed fiber (buffered or coated).

14.9 Horizontal Cabling

14.9.1 Introduction

The horizontal cabling is the portion of the telecommunications cabling system that extends from the equipment outlet (EO) in the EDA to the TIA HC or ISO/CENELEC ZD in an HDA, IDA, or MDA.

The horizontal cabling includes:

- Horizontal cables
- Mechanical terminations
- Equipment cords, patch cords, or jumpers;

•

14.9.2 Zone Outlets, Consolidation Points, and Local Distribution Points

14.9.2.1 Requirements

Because of the wide range of services and site sizes where horizontal cabling will be used, more than one transmission medium is recognized. This standard specifies transmission media, which shall be used individually or in combination in the horizontal cabling.

Recognized cabling, associated connecting hardware, jumpers, patch cords, and equipment cords shall meet all applicable requirements specified in applicable standards and related addenda (e.g., ISO/IEC 11801-1, ANSI/TIA-568.2-D, ANSI/TIA-568.3-D).

Horizontal cabling shall consist of one or more of the following media types:

- 4-pair 100-ohm balanced twisted-pair Category 6/Class E minimum (Category 6A/Class E_A or higher recommended)
- OM3 multimode optical fiber cable minimum (OM4 or OM5 multimode optical fiber cable recommended where horizontal fiber cabling lengths exceed 70 m [230 ft])
- OS1 or OS2, single-mode optical fiber cable

NOTE:

1. Category 5e/Class D cabling may be used in an existing data center that already utilizes Category 5e/Class D cabling
2. 734-type and 735-type 75-ohm coaxial cables as specified in Telcordia GR-139-CORE are permitted for E-1, E-3, and T-3 circuits.
3. If specific applications require other types of cabling (e.g., Infiniband cabling, ANSI/TIA-232, V.35, SCSI), the other types may be installed in addition to the cabling listed above. Transmission performance compliance with applicable standards shall apply to local requirements.
4. To determine the suitability of the cabling types listed above for specific applications, systems suppliers, equipment manufacturers, and systems integrators should be consulted.

14.9.3 Redundant Horizontal Cabling

14.9.3.1 Recommendations

Horizontal cabling to critical systems should be diversely routed to improve resilience. Care should be taken not to exceed maximum horizontal cabling lengths when selecting cabling pathways. Critical systems can be supported by two different horizontal distribution areas as long as maximum cabling length limitations are not exceeded. This degree of redundancy may not provide much more resilience than diversely routing the horizontal cabling if the two horizontal distribution areas are in the same fire protection zone.

14.9.4 Balanced Twisted-Pair Cabling

14.9.4.1 Introduction

Balanced twisted-pair cabling performance is described using a scale based on classes or categories, as defined by ISO/IEC and TIA, respectively. While Category 3/Class C is the minimum acceptable performance for backbone cabling, Category 6/Class E is the minimum requirement in ANSI/TIA-942-B and CENELEC EN 50173-5 for horizontal cabling, and Category 6A/Class EA is the minimum requirement as listed in ISO/IEC 24764.

Table 14-6 is based on the minimum cabling channel performance requirements of specific balanced twisted-pair cabling.

14.9.4.2 Recommendations

Category 6A/Class E_A is the minimum performance level recommended for balanced twisted-pair cabling in a data center with the exception of network access cabling to the external network interface (ENI) located in telecommunications entrance rooms.

14.9.4.3 Balanced Twisted-Pair Cabling Supportable Distances

Maximum supportable distances for applications using balanced twisted-pair cabling can be found in the cabling standards being followed (e.g., ISO/IEC 11801-5, CENELEC EN 50173-5, ANSI/TIA-568.0-D).

14.9.5 Optical Fiber Cabling

14.9.5.1 Introduction

There are five classes of multimode optical fiber cabling (OM1, OM2, OM3, OM4, and OM5) and two classes of single-mode optical fiber cabling (OS1 and OS2). Table 14-7 shows the minimum bandwidth or optical performance for each optical fiber cable by type.

14.9.5.2 Requirements

OS1 single-mode and OM3 multimode cable are the minimum performance optical fiber types specified in this standard.

14.9.5.3 Recommendations

OM4 multimode optical fiber is recommended to support 100 Gbps Ethernet, particularly the 4-lane implementation. Multimode optical fiber should be terminated with MPO connectors where 40G and 100G Ethernet is expected to be supported initially or in the future (e.g., backbone cabling between distributors, top of rack switches, and high-15performance servers). OM5 has similar properties to that of OM4 but is capable over supporting higher than 100 Gbps Ethernet.

Table 14-6 Balanced Twisted-Pair Cabling Channel Performance

CENELEC and ISO classes/categories[1]	*TIA categories*	*Frequency characterization*
Class D/Category 5	Category 5e	100 MHz
Class E/Category 6	Category 6	250 MHz
Class E$_A$/Category 6A	Augmented Category 6	500 MHz
Class F/Category 7	n/a[2]	600 MHz
Class F$_A$/Category 7$_A$	n/a[2]	1000 MHz
Class I/Category 8.1	Category 8	2000 MHz
Class II/Category 8.2	Category 8	2000 MHz

NOTE 1: Component performance is indicated by the term “Category”, with system performance indicated by the term “Class”.
NOTE 2: TIA does not define an equivalent.

Table 14-7 Optical Fiber Cable Performance by Type

Classification	*Optical Fiber Type*	*Performance*
OM1[1]	62.5/125 µm multimode	Minimum overfilled launch bandwidth of 200 and 500 MHz•km at 850 and 1300 nm, respectively
OM2[1]	50/125 µm multimode 62.5/125 µm multimode	Minimum overfilled launch bandwidth of 500 and 500 MHz•km at 850 and 1300 nm, respectively
OM3	50/125 µm 850 nm laser-optimized	Minimum overfilled launch bandwidth of 1500 and 500 MHz•km at 850 and 1300 nm, respectively and an effective modal bandwidth of 2000 MHz•km at 850 nm using a restricted mode launch (e.g., vertical cavity surface emitting laser [VCSEL])
OM4	50/125 µm 850 nm laser-optimized	Minimum overfilled launch bandwidth of 3500 and 500 MHz•km at 850 and 1300 nm, respectively and an effective modal bandwidth of 4700 MHz•km at 850 nm using a restricted mode launch (e.g., VCSEL)
OM5	50/125 µm 850 nm laser-optimized	Minimum overfilled launch bandwidth of 3500 and 500 MHz•km at 850 and 1300 nm, respectively and an effective modal bandwidth of 4700 MHz•km at 850 nm using a restricted mode launch (e.g., VCSEL)
OS1	Single-mode	Minimum bandwidth of single-mode optical fiber cable is not characterized in the same manner as multimode. Loss characterization is 1.0 dB per km at 1310 nm and 1550 nm for indoor and 0.5 dB per km at 1310 nm and 1550 nm for outdoor.
OS2	Single-mode	Minimum bandwidth of single-mode optical fiber cable is not characterized in the same manner as multimode. Loss characterization is 0.4 dB per km at 1310 nm, 1383 nm, and 1550 nm for both indoor and outdoor. OS2 fiber is optimized for performance at the 1383 nm window (and is defined in ITU-G652.D).

NOTE: OM1 and OM 2 are not recognized for use in data centers and are only included for completeness.

14.9.5.4 Component Channel Method Versus Application Based Method

There are two methods used for the design and implementation of optical fiber cabling solutions: component channel method and application-based method.

14.9.5.4.1 Component Channel Method

Traditionally, the component method has been used to design and assemble optical fiber cabling solutions without detailed consideration for the applications that eventually will run over the optical fiber cabling channel. This lack of coordination can result in many discussions and disagreements between designers, installers, and operations staff over who is responsible for what when the network equipment is discovered to be inoperable.

Knowledge of the applications to be supported is critical to the effective delivery and future proofing of the optical fiber cabling infrastructure. The designer should first determine what applications are required, the type of connectors, the bandwidth performance, and optical fiber cabling type. The designer should then relate this to the optical performance charts and tables in the cabling standards being followed. The designer can then obtain the maximum permitted loss per optical fiber type and maximum distance over which the application can be supported. Selection and assembly of components is concluded on an accumulated loss basis; the resulting performance is measured against the whole channel and does not identify or acknowledge a worst individual event or component loss figure.

This approach can be used to the designer’s and operator’s advantage when considering the use of more than two connectors or connectors that experience greater signal losses over a shorter channel distance. It effectively converts bandwidth gains into connector loss. Most manufacturers will not recommend or support more than six connectors (three mated pairs of connectors, not including the connectors at the equipment and not including splices) in a multimode or single-mode optical fiber cabling channel because of the resulting cumulative system attenuation.

The demands from the latest and next generation high-speed applications have considerable distance limiting aspects. The applications can only be expected to operate effectively when the balance of media choice, distance, bandwidth, and component loss are all within the prescribed parameters for each application to be supported.

14.9.5.4.2 Application-Based Method

If the applications to be deployed are known, the data center cabling designer can get detailed information about channel losses and maximum channel distance supported for each optical fiber media type from the cabling standards being followed. Dedicated home run optical fiber cabling solutions can be configured from approved component sets.

14.9.5.5 Optical Fiber Cabling Supportable Distances

Maximum supportable distances and maximum channel attenuation for applications using optical fiber cabling can be found in applicable standards (e.g., ANSI/TIA-568.0-D, ISO/IEC 11801-5, CENELEC EN 50173-1). Application tables in these standards are based on the minimum performance requirements for OM1−OM5 classifications of multi-mode fiber and OS1−OS2 single -mode fiber.

14.9.5.6 Single-Mode and Multimode Connector Color Recommendations

The single-mode connector or a visible portion of it should be blue in color, referring to a flat-polished optical fiber endface; the color green should signify a connector featuring an angle polished optical fiber endface. Where a mixture of OS1 and OS2 exist in a single data center space or room, additional identification should be applied to clearly identify the fiber type used.

The multimode connector or a visible portion of it should be:

- Beige for an OM1, 62.5 µm connector (not recognized in standard)
- Black for an OM2, 50 µm connector (not recognized in standard)
- Aqua for an OM3 or OM4, 50 µm laser-optimized connector
- Lime for an OM5, 50 µm laser-optimized connector

Where a mixture of OM3 and OM4 exist in a single data center space or room, additional identification should be applied to clearly identify the fiber type used.

Adapter housing color should represent the cabling performance of the installed permanent fiber using the connector color scheme above.

14.9.6 Horizontal Cabling Length Limitations

14.9.6.1 Introduction

The horizontal cabling length limitations are the cable lengths from the mechanical termination of the cabling at the TIA HC or ISO/IEC ZD in the HDA, IDA, or the MDA to the mechanical termination of the cabling on the EO in the EDA.

14.9.6.2 Requirements

For maximum and minimum cabling lengths, refer to the applicable cabling standards.

14.9.6.3 Recommendations

Horizontal cabling distances in a computer room may need to be reduced to compensate for longer equipment cords in the data center distribution areas. Therefore, careful considerations to the horizontal cabling distance should be made to ensure that cabling distances and transmission requirements are not exceeded when the equipment cords are attached.

NOTE: For balanced twisted-pair cabling, to reduce the effect of multiple connections in close proximity on NEXT loss and return loss and without further guidance from manufacturers, the zone distribution area termination should be located at least 15 m (50 ft) from the horizontal distribution area termination. Consult with the cabling system manufacturer about the minimum distances supported by the chosen product set. Their recommendations may reduce space needed to collect excess cable.

14.9.6.4 Balanced Twisted-Pair Cord Length Limitations

14.9.6.4.1 Introduction

Balanced twisted-pair equipment cords and patch cord assemblies may be constructed with either solid or stranded conductors. The insertion loss (attenuation) performance of stranded cables used in the assembly of these cords is greater than the attenuation of solid conductor cables. While a generic cabling system has a physical channel distance limitation of 100 m (328 ft), there is an assumption made that the combined length of equipment cords and patch cords at both ends of the cabling channel will not exceed 10 m (33 ft). If stranded conductor equipment cords and stranded conductor patch cords with a combined length of more than 10 m (33 ft) are used, refer to the applicable cabling standards for maximum cord lengths.

14.9.6.4.2 Requirements

Manufacturers shall be consulted to confirm the attenuation characteristics of their stranded cables, equipment cords, and patch cords to help ensure that the installed cabling channels will perform to the applicable cabling standards.

Balanced twisted-pair equipment cords used in the context of zone outlets in the ZDA shall meet the minimum performance requirements provided in the cabling standard being followed.

The zone outlet shall be marked with the maximum allowable zone area cable length. One method to accomplish this is to evaluate cable length markings.

14.9.6.5 Horizontal Cabling Applications

14.9.6.5.1 Requirements

For optical fiber, when designing individual optical fiber links or assessing existing cabling, the maximum allowable channel insertion loss for each application shall be considered.

14.9.6.5.2 Recommendations

For optical fiber and balanced twisted-pair cabling, application distances can be constrained by the cabling category or type. The compilation of application information detailed in applicable standards (e.g., ANSI/TIA-568.0-D, CENELEC EN 50173-5, ISO/IEC 11801-5) provide the basic information to make informed decisions about optical fiber and balanced twisted-pair cabling usage and system design.

14.9.7 Shared Sheath Guidelines

14.9.7.1 Introduction

Shared sheath guidelines described in this section are not intended to cover all system designs and installations. It is recommended that the user consult with equipment manufacturers, applications standards, and system providers for additional information.

In general, applications using no common frequencies tend not to interfere with each another. A good example of this is mixing analog voice and digital data signals within the same cable sheath. In a single balanced twisted-pair cable, multiple applications of the same type may operate on different twisted pairs simultaneously without any problems.

14.9.7.2 Recommendations

The designer and installer should follow the recommendations for shared sheath implementation described in the cabling standards being followed.

14.9.7.3 Hybrid and Bundled Cable Assembly Applications

14.9.7.3.1 Introduction

Hybrid and bundled cable assemblies are used to group multiple individual cables together to form a single cable unit routed along a common path. These individual cables may be of the same or different types (e.g., optical fiber cabling and balanced twisted-pair cabling) or of the same or different categories (e.g., Category 6A/Class E_A cabling with Category 6/Class E cabling).

Hybrid cable assemblies are manufactured in a factory whereas bundled cable assemblies may be assembled either in a factory, at a third-party facility, or on site by the installer.

NOTE: Bundled cables are sometimes referred to as loomed, speed-wrap, or whip cable assemblies.

14.9.7.3.2 Requirements

When bundled and hybrid cables are used for horizontal cabling, each cable type shall be recognized and meet the transmission (e.g., recognized categories/classes) and color-code specifications (e.g., 4-pair color-code groupings) for that cable type. Additionally, hybrid or bundled cable assemblies shall meet the hybrid or bundled cable assembly requirements of applicable standards (e.g., ISO/IEC 11801-1, ANSI/TIA-568.2-D, ANSI/TIA-568.3-D, CENELEC EN 50173-1). These requirements apply to hybrid cables and bundled cables assembled prior to installation.

Hybrid and bundled cable assemblies may be installed either as cable or as preconnectorized assemblies. These assemblies, known as trunk cable assemblies, may be pre-connectorized on one or both ends. When used, these hybrid and bundled trunk assemblies are required to meet the hybrid and bundled transmission performance requirements of applicable standards (e.g., ISO/IEC 11801-1, ANSI/TIA 568.2-D, ANSI/TIA-568.3-D, CENELEC EN 50173-1).

14.9.7.3.3 Recommendations

There are a number of other types of horizontal cabling that have not been defined in this standard, yet they may be effective for specific applications. Although these other types of horizontal cabling are not part of the requirements of this standard, they may be used in addition to the best practices offered by this standard.

14.9.7.4 Trunk Cabling Assemblies

14.9.7.4.1 Introduction

Trunk cabling assemblies consist of two or more preconnectorized cabling links of the same or different types or categories that may either be covered by one overall sheath or a collection of individual cable units, which are bound together to form a single trunk unit. The utilization of one sheath provides for fewer individual cables in a pathway, aiding in cable management, though larger pathway bend radii may be required.

As trunk cabling assemblies are provided by the manufacturer, factory terminated connectors may provide improved performance as compared to field terminated connectors. Additionally, the reduction in the number of cables and field termination may reduce time required for cabling installation.

Trunk cabling assemblies require accurate calculation of each cabling link to be included prior to manufacturing and if a trunk cable assembly is damages, multiple cabling links within the assembly may be affected.

14.10 Cabling Installation

14.10.1 General Requirements

Cabling shall be installed and dressed neatly, taking care to adhere to minimum cable bend radii for cables. Take particular care not to leave excess optical fiber loops on the floor or in places where they can be damaged.

14.10.2 Cable Management

14.10.2.1 Introduction

Performance of cable and connecting hardware may become degraded if initial installation and ongoing cable management recommendations are not followed. Installation and maintenance practices for the pulling and placing of horizontal and backbone cabling differs greatly from that of the associated interconnections and cross-connections.

14.10.2.2 Requirements

While all transmission parameters are sensitive to transmission discontinuities caused by connector terminations, return loss, and all forms of crosstalk (e.g., near-end crosstalk [NEXT], attenuation-to-crosstalk ratio–far end [ACR–F], previously known as ELFEXT), performance of balanced twisted-pair systems are particularly sensitive to conductor untwisting and other installation practices that disturb pair balance and cause impedance variations. To prevent these problems, the installer shall adhere to the following practices:

- Remove only as much cable jacket as is required for termination and trimming.
- Follow the manufacturer's instructions for mounting, termination, and cable management.
- Minimize the amount of untwisting in a pair as a result of termination to connecting hardware. For untwisting cabling, maintain pair twists as close as possible to the termination point; the amount of untwisting must not exceed 13 mm (0.5 in) for Category 5e and higher cables.

NOTE: This requirement is intended to minimize untwisting of cable pairs and the separation of conductors within a pair. It is not intended as a twist specification for cable or jumper construction.

For termination fields that require frequent access (e.g., cross-connects used for configuring a network), one way to control termination consistency is by using factory-assembled equipment cords, patch cords, and patch panels that meet the appropriate performance requirements. Jumpers can provide comparable performance, but typically require a higher skill level to implement changes.

Cables shall be dressed into cable management and cabling pathways so that cables and cords do not lie on the floor where they can be stepped on.

14.10.2.3 Recommendations

Telecommunications cabling should be placed in cabling pathways (containment) that provide sufficient space for placement of the media. Consider the following methods of containment for telecommunications cabling installed in dedicated routes:

- Enclosed raceway distribution (e.g., conduit systems)
- Zone distribution (e.g., enclosures)
- Cable trays (e.g., open top systems)

CAUTION: Refer to appropriate codes, standards, and regulations for compliance with flame spread and smoke index properties of cabling used in cabling pathway systems.

Connecting hardware should only be installed in the access floor space when the connecting hardware is one of the following:

- A TIA CP, ISO/CELENEC LDP, or TIA zone outlet in a zone distribution area (ZDA)
- EO in equipment distribution area (EDA) or workstation
- Building automation systems (BAS) horizontal connection point (HCP)

Cross-connections are designed for flexibility to allow for moves, adds, and changes. The structured cabling system user is typically responsible for altering cross-connections to implement network changes. Skill levels among users vary and should be taken into consideration when designing, providing training on, and performing ongoing management of the cross-connection facility. The following guidelines should be followed for appropriate management practices.

In cabling pathways and telecommunications spaces, use appropriate cable routing and dressing fixtures to organize and effectively manage the different cable types. The cable management precautions that should be followed include:

- For suspended cabling, limit the span between supports to 1.5 m (5 ft) or less.
- Cables ties should be installed so as not to deform cables beyond manufacturers' tolerances. Cable ties should be loose and easily rotated so as to not pinch or otherwise deform the cable. Consider hook-and-loop cable ties instead of plastic or metal cable ties. Cable ties should not be used as non-continuous cable supports in lieu of proper supports such as J-hooks. These non-continuous supports should have rounded edges to avoid deforming cords and cables.
- Avoid twisting the cable jacket during installation as this may affect transmission performance.
- For balanced twisted pair cable, use of random spacing between cable ties to avoid return loss resonances.

  NOTE: Uniformly placing cable ties has been shown to produce return loss resonance. However, a recommended minimum variation in the distances between cable ties necessary to avoid this effect has not been published.

WARNING: Never use staples or staple fastening tools to fasten telecommunications cabling in a data center.

The following are cross-connect facility management precautions that should be observed:

- Eliminate or minimize equipment cord, patch cord, and jumper slack in the management field after each cross-connection is completed.
- In cross-connections utilizing balanced twisted-pair or optical fiber equipment cords or patch cords, bend radius can become difficult to control; it is important to achieve desired manageability without loss of performance in a cabling channel by controlling the equipment cord and patch cord bend radii.
- Horizontal cables should be terminated on connecting hardware that is the same performance (Category) or higher. The installed transmission performance of cabling where components of different performance category requirements are used shall be classified by the least-performing component.
- Because horizontal and backbone cables are always terminated on separate connectors, use patch cords or jumpers to make connections between horizontal cables and backbone cables.
- Consider arranging switches and patch panels in distributors to minimize patch cord lengths.

14.10.3 Bend Radius and Pulling Tension Guidelines

14.10.3.1 Introduction

Pay strict attention to the manufacturer's guidelines on bend radii and maximum pulling tension during installation. Notice that the recommended minimum bend radius for a cable during installation may be greater than the recommended bend radius after the cable is installed. This is to minimize tension and deformation as the cables pass around corners during installation.

Cable bend radius requirements minimize the effects of bends on the transmission performance of installed cabling links. These requirements are distinct from the bend radius specifications for conduits.

14.10.3.2 General Recommendations

If multiple cable types are used in any route, use the largest bend radius specified among the cable types used.

Consult the manufacturer's specifications for the minimum bend radius during installation. The minimum bend radius utilized should be the greater of the manufacturers' specifications and the specifications provided in this standard.

14.10.3.3 Balanced Twisted-Pair Cabling Bend Radius and Pulling Tension Requirements

The maximum pull force best practices for balanced twisted-pair cabling shall be established by the cabling products manufacturer. Consult with the applicable cabling products manufacturer for such best practices. See Table 14-8.

14.10.3.4 Optical Fiber Cable Bend Radius and Pulling Tension Requirements

The maximum pull force best practices for optical fiber cabling shall be established by the cabling products manufacturer. Consult with the applicable cabling products manufacturer for such best practices. See Table 14-9.

Table 14-8 Balanced Twisted-Pair Cable Bend Radius and Pulling Tension

Cabling/Cord Types	*Required Minimum Inside Bend Radius Under No Load (No Stress)*	*Required Minimum Bend Radius Under Load (Stress)*	*Recommended Maximum Tensile Load Under Load (Stress)*
4-pair, balanced twisted-pair patch/equip cord	Four times the cord cable's outside diameter	Four times the cord cable's outside diameter	Follow manufacturer specifications
4-pair, balanced twisted-pair cables	Four times the cable's outside diameter	Four times the cable's outside diameter	110 N (25 lbf)
Multipair balanced twisted-pair cables	Follow manufacturer specifications	Follow manufacturer specifications	Follow manufacturer specifications

Table 14-9 Optical Fiber Cable Bend Radius and Pulling Tension

Cable Type and Installation Details	*Maximum Tensile Load During Installation*	*Minimum Bend Radii While Subjected to:*	
		Maximum Tensile Load (During Installation)	*No Tensile Load (After Installation)*
Inside plant horizontal cable with 2 or 4 fibers	220 N (50 lbf)	50 mm (2 in)	25 mm (1 in)
Inside plant cable with more than 4 fibers	Per manufacturer	20-times the cable outside diameter	10-times the cable outside diameter
Indoor/outdoor cable with up to 12 fibers	1335 N (300 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Indoor/outdoor cable with more than 12 fibers	2670 N (600 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Outside plant cable	2670 N (600 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Drop cable installed by pulling	1335 N (300 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Drop cable installed by directly buried, trenched, or blown into ducts	440 N (100 lbf)	20-times the cable outside diameter	10-times the cable outside diameter

NOTE: Non-circular cable bend diameter requirements are to be determined using the minor axis as the cable diameter and bending in the direction of the preferential bend.

14.10.4 Abandoned Cable

14.10.4.1 Introduction

For the purpose of this standard, abandoned cable is described as installed telecommunications cabling that is not terminated at both ends at a connector or other equipment and not identified for future use with some form of labeling.

14.10.4.2 Requirements

Remove abandoned cable as required by the AHJ.

14.10.4.3 Recommendations

It is considered a best practice to remove abandoned cable in the data center.

14.10.5 Cleaning of Optical Fiber Connectors

14.10.5.1 Overview

Contamination of optical fiber connector end-faces is one of the major causes of network malfunctions. Even in the newest critical long-distance fiber path with huge bandwidth, a single dirty connector along the path will reduce the optical signal strength below the design tolerance and may result in large-scale disruptions and/or troubleshooting. In case of optical fibers within or between data centers, such fiber path spans multiple organizations so demarcation and coordination become additional issues that may prolong the troubleshooting process. The minimum size of contaminants that may cause disruption could be less than 2 micrometers (2μm), which means the quality of cleaning required is very high.

This section describes the selection and usage of appropriate cleaning tools and testing equipment for optical fiber connectors, taking into account the most recent trends, and also includes examples of what to avoid during connector cleaning.

NOTE: Additional information on connector end-face cleaning may also be found in ISO/IEC 14763-3, IEC TR 62627-01, and IEC TR 62627-05.

14.10.5.2 Requirements

End-face cleaning shall be performed each time an optical fiber connector (male) is plugged into an adapter (female). End-face cleaning shall be performed on both male and female (which is usually joined with the connector of the other fiber) ends. After the cleaning is performed, the result of cleaning must be checked using an optical power meter (OLTS), or end-face inspection device (scope).

If using dry method cleaning tools, always use a fresh surface for each new connector to be cleaned.

Obey the instructions shown in the manufacturer's official instructions if available.

14.10.5.3 Recommendations

Usually, optical fiber connections need to be tested end-to-end (i.e., between the far ends of the connection on both sides) to verify the integrity of the fiber connection. However, such long-span verification or retroactive remedy of the connection may not always be possible due to site constraints such as access or time limitations, and work schedule or order.

In such cases, both optical power meter and end-face inspection device optical power meter, or end-face inspection device (scope) should be used to verify the quality of the cleaning at the connection point.

The cleaning procedure documents should include sections to record test results of each end-face that is cleaned.

14.10.5.3.1 Cautions on Using Legacy Cleaning Tools

In the past, alcohols such as ethanol, methanol, and IPA (Isopropyl Alcohol), were applied to gauze or swab for cleaning. However, this is no longer recommended practice due to their effect on human body and risks of residual smearing after drying. Similarly, technicians must be aware of the risks inherent in the use of air dusters such as raising dust and causing them to either attach to the cleaned end-face or even scraping dust against it and cause damage.

14.10.5.3.2 Designation of Cleaning Method and Exclusion of Inferior Cleaning Tools

Owner and/or project manager should designate the connector cleaning method to the technicians. In addition, it is useful to designate a list of pre-approved cleaning products to be used on site, in order to forestall troubles associated with ad-hoc use of counterfeit or inappropriate products by on-site technicians.

14.10.5.3.3 Contamination of Newly Delivered Patch Cords

As there exist risks of contamination between shipping out and unpackaging on site, even for freshly delivered patch cords, all patch cord connectors should be cleaned and inspected before connection even when using newly delivered products.

14.10.5.3.4 Prevention of Contamination Through Caps

Caps are supposed to prevent contamination of connectors or adapters. However, contamination of caps themselves cannot be visually checked, and instruments or scopes cannot be used to check for contamination of caps on site. Since connector cleanliness can be checked or inspected using instruments or scopes, technicians should verify cleanliness of end-faces on site after removing the caps from connectors and adaptors without overly relying on the caps themselves.

Technicians should avoid capping the connectors or adaptors after cleaning, instead perform all connections immediately after cleaning.

14.10.5.3.5 Scorching of End-Faces

In cases where contaminated connector end-faces are put into operation, and the amplitude of the optical signal going through the connection is high, high-intensity light will be shone upon the contaminant, resulting in scorched contaminant getting fused onto the end-faces over time. This may not only affect the transmission quality of the operational circuit, but also may degrade the end-surface so much that the port cannot be cleaned sufficiently to permit its re-use when the circuit is released for re-connection.

14.10.5.3.6 Cleaning Inside Network Equipment Ports

Cleaning of optical adapters built into network equipment such as optical transceivers requires intimate knowledge of the equipment in question. Internal structure of these adaptors may use completely different structure compared with physical contact using ferrules that are used in optical connectors, instead using lenses or plates to achieve optical connection. It is very difficult to tell these apart visually from the exterior without intimate knowledge. In addition, as these adaptors often uses very sensitive components, technicians need to follow the manufacturer recommended steps and methodologies for handling them properly.

14.10.5.4 Additional Information

14.10.5.4.1 Types of Cleaners Available

Dry type: uses cloth to wipe off the contaminants

These are commonly used in routine cleaning work, and have several sub-types shown below:

- Pen type—This is a type of cleaning tape/ribbon that uses built-in fibrous string exposed at the tip of a pen to sweep the contaminants from the end-face. The string is mechanically reeled in from the fresh reel into the used reel each time it is used. While this is relatively simple to use, the ease of use may induce lack of care and attention during the cleaning work, resulting in poor cleaning quality.
  When cleaning, the pen tip must be pushed against the adaptor or connector "in straight line" (as in billiard cues). While this is relatively straightforward when working at a reasonable position (ex. eye-level), but becomes much harder when working in awkward posture or position such at high (above head) or low (squatting) levels, often resulting in improper cleaning. This can be remedied by training the technician to push straight by using rulers or other tools to measure the deviation from horizontal and vertical, and have multiple co-workers verify the motion. This type can clean both connectors and adaptors by adding/removing the pen adapter at the tip.
- Stick type—The stick type has a cleaning cloth at the tip of a swab-shaped stick.
  As the force and rotation applied differs between individual technician, it is vital that the technician obey the force and rotation stated in the instructions. Also, care must be taken not to expose the cloth tip during storage to avoid risking contamination. This type can only clean the adaptor-type end-surface.
- Reel type—This type uses built-in cloth strip exposed at a slit or a window in the palm-sized body where the connector end-face is rubbed against to clean the contaminants. The cloth is reeled in manually from the fresh reel into the used reel after each cleaning action.
  Each cleaning action consists of rubbing a connector end-surface against the exposed fresh cloth once in one direction. Details of the actions differ among the products, so always read the instructions and follow its commands. As the section of fresh cloth has to be manually reeled in, make sure that the technician reels a fresh section of the cloth before each cleaning action to ensure that the cleaning is performed on a fresh cloth. This type can only clean the connector end-surface, and not the adaptor end-surface.

Wet type: Uses liquids to remove contaminants from the end-face

This type is used to remove contaminants that cannot be removed using dry type cleaners. This type applies a highly volatile liquid on a purpose-made swab or tissue to wet the connector end-face to remove the contaminants, and then wipe with the dry swab or tissue to dry the surface (Wet to Dry). The cleaning liquid is stored either in a spray bottle or within a pen-shaped vessel. Some liquids are flammable and may be prohibited in some environments. In such case, select a non-flammable liquid. Some liquids are also harmful to humans and require particular care when handling. Technicians using this type need to be fully aware of the details of application, since incomplete knowledge may result in incomplete cleaning, which commonly takes forms of either too much liquid applied, or insufficient dry swipe afterwards.

Tissues used for swiping come in different packaging such as boxes, cylinders, or individual packaging, according to the working environment. Individually packaged tissues were originally intended for outdoor use but may also be used in data centers where there are high awareness of connector cleanliness, low frequency of cleaning, and/or harsh storage environment for the tissues.

Regarding the swabs, usage instructions need to be read carefully, as some types are designed to unfold the tip by pushing the swab into the adaptor with just enough force to bend the axis in order to attain the required cleaning performance.

This type can be used to clean both connectors and adaptors by using the tissues for connectors and swabs for adaptors.

14.10.5.4.2 Examples of Inappropriate Actions on Site

Listed below are some examples of inappropriate cleaning actions caused by deficiencies in knowledge and attention that actually happened on site. These are shared to emphasize the need for proper attitudes towards connector cleaning.

- Connector contaminated by spittles from conversation and sneezing immediately after cleaning work.
- Skipping cleaning of connectors that was unpatched only for a few seconds resulted in a contaminated connection that caused losses above tolerance.
- Performing cleaning and connection of multiple ports in batches instead of individually resulted in cleaning of several connectors being skipped.
- Pointing the cleaned connector upwards resulted in dust falling onto the end-surface and re-contamination.
- Repeated re-runs of cleaning resulted in the frustrated technician applying too much force on the cleaning tool, damaging the connector.
- When handing over a connector between a pair of technicians performing cleaning and patching separately, the connector came into contact with the technician's sleeve and got contaminated.
- Dropped alcohol bottles resulted in spillage inside the computer room.
- Supply of cleaning tools ran out during the work due to insufficient stock being brought over.

14.10.5.4.3 Methods for verifying connector cleanliness.

There are generally 3 methods for verifying cleanliness of optical fiber connectors.

- Visual inspection using scopes (measures amount of contaminants)
- Measurement using OLTS (measures connection losses)
- Measurement using OTDR (measures return losses)

These methods can be used to verify the integrity of connector contact and cleaning. However, there are instances where verification using one method does not guarantee problem-free connection, such as:

- Normal loss value using OLTS may still show contamination upon visual inspection using a scope.
- OLTS may show excess loss although visual inspection using a scope shows no apparent contamination.
- Return loss within tolerances do not guarantee connection loss within tolerance.
- Using auto-test of scopes by different manufacturer may return differing verdict on visual cleanliness.

Contaminants may attach to connector end-surfaces within seconds after cleaning. Therefore, cleaning defects may inevitably occur even after performing all cleaning properly. Therefore, data center owners and managers should document the proper cleaning procedures and methodologies and manage all cleaning activities performed.

Connector cleaning may appear to be an operation issue for data centers, but due to the risk of connector scorching, all cleaning must be performed properly even during initial implementation.

14.11 Field Testing Data Center Telecommunications Cabling

14.11.1 Introduction

Field testing is an effective method of evaluating the transmission performance of installed telecommunications cabling. The field test measurement results of installed balanced twisted-pair or optical fiber telecommunications cabling depend on several factors, including the:

- Transmission performance of cable
- Transmission performance of connecting hardware
- Transmission performance of equipment cords, patch cords, and cross-connect cabling
- Total number of connections
- Installation practices and expertise of the installers
- Maintenance techniques that are used

Field testing conducted on balanced twisted-pair and optical fiber cabling shall be conducted in accordance with specified standards.

NOTE: Refer to the list of standards provided in Section 3 and Appendix I of this standard.

This section provides requirements and recommendations regarding channel and permanent link field-testing, including:

- Installation conformance
- Specifications for field test instruments
- Field test measurement methods
- Interpretation of test results

14.11.2 Installation Conformance

14.11.2.1 Introduction

Installation conformance ensures that field test measurements have been completed in accordance with the terms and conditions of a contract.

14.11.2.2 Requirements

The installation contract shall include field test measurement requirements of the installed cabling to specific industry standards as well as to visually inspect the cabling. Performance field test measurement documentation of the installed cabling shall be provided to the building tenant, building owner or agent per contract requirements, or, in lieu of contract requirements, in the format delivered by the certification test instrument.

Visual inspection of installed cabling is performed by observing the following:

- The condition, workmanship, and finish are satisfactory, including no obvious damage to the cable (e.g., bend radius, tearing, and separation from sources of EMI).
- The marking (labeling) is legible and placed according to specification.
- Mechanical damage is absent, and there is no undesired movement or displacement of parts.
- Flaking of materials or finishes is absent.

Installation conformance to visual inspection requires that a form be submitted, indicating that a visual inspection has been conducted and the form shall document the results of the visual inspection.

14.11.3 100-ohm Balanced Twisted-Pair Cabling Field Testing

14.11.3.1 Introduction

Certification of the balanced twisted-pair cabling determines whether the cabling meets expected performance requirements such as those specified in one or more of the following Categories/Classes of cabling:

- TIA Category 3 cabling
- ISO Class C cabling
- TIA Category 5e cabling
- ISO Class D cabling using ISO Category 5 components
- TIA Category 6 cabling
- ISO Class E cabling using ISO Category 6 components
- TIA Category 6A cabling
- ISO Class E_A cabling using ISO Category 6_A components
- ISO Class F cabling using ISO Category 7 components
- ISO Class F_A cabling using ISO Category 7_A components
- TIA Category 8 cabling
- ISO Class I cabling using ISO Category 8.1 components
- ISO Class II cabling using ISO Category 8.2 components

NOTE: Existing ISO Class E and TIA Category 6 cabling may support IEEE 10GBASE-T at limited distances but will require additional testing and mitigation strategies to ascertain what is achievable. For additional details, see TIA TSB-155-A and ISO/IEC TR 24750.

14.11.3.2 Balanced Twisted-Pair Cabling Field Test Configuration

14.11.3.2.1 Permanent Link Requirements

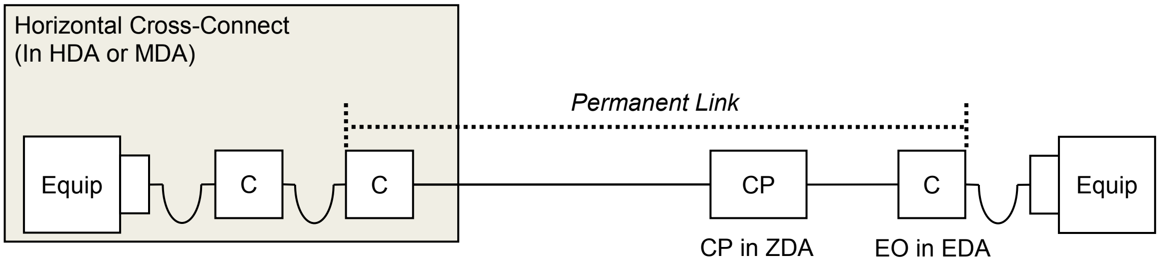
The permanent link test configuration shall be used to certify the performance of the permanently installed balanced twisted-pair cabling.

NOTE: A passing permanent link associated with compliant patch cords always guarantees a compliant channel.

The permanent link shall include:

- Up to 90 m (295 ft) of horizontal cable
- A connection at each end of the horizontal cabling
- Optionally, a consolidation point (CP) or local distribution point (ISO/IEC and CENELEC equivalent of CP in ZDA)

The permanent link configuration excludes the cable portion of the field test instrument cord and the connection to the field test instrument. See Figure 14-10 for an example of a permanent link.



Legend

C	connection	HDA	horizontal distribution area
CP	consolidation point	MDA	main distribution area
EDA	equipment distribution area	ZDA	zone distribution area
EO	equipment outlet		

Figure 14-10
Permanent Link Example

14.11.3.2.2 Channel Requirements

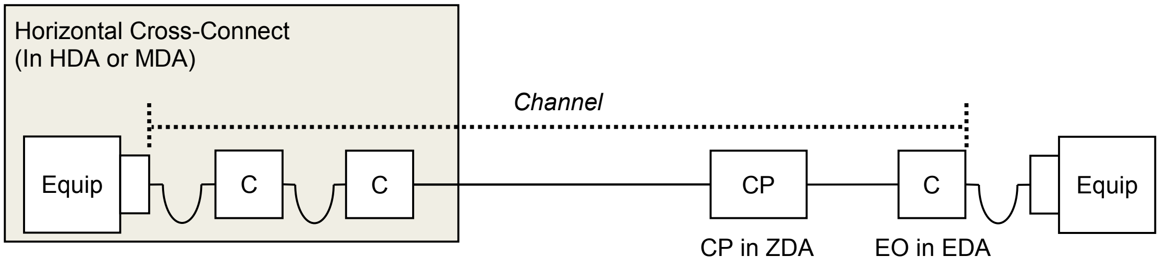
If channel testing is performed, the channel test configuration shall be used to verify end-to-end channel performance of installed balanced twisted-pair cabling.

NOTE: This is generally used prior to connection of active equipment.

The channel includes:

- Horizontal cable
- Patch cords and equipment cords
- A telecommunications outlet/connector
- Optionally, a consolidation point (CP) or local distribution point (ISO/IEC and CENELEC equivalent of CP in ZDA)
- Up to two connections at the horizontal cross-connect

The channel configuration description does not apply to those cases where horizontal cabling is cross-connected to backbone cabling. See Figure 14-11 for an example of a channel.



Legend

C	connection	HDA	horizontal distribution area
CP	consolidation point	MDA	main distribution area
EDA	equipment distribution area	ZDA	zone distribution area
EO	equipment outlet		

Figure 14-11
Channel Model Example

14.11.3.3 Balanced Twisted-Pair Cabling Field Test Parameters

14.11.3.3.1 Requirements

The field test parameters to be measured shall meet the requirements of the cabling standard being followed (e.g., ANSI/TIA-1152, EN 50346). The field test instrument shall support all field test parameters specified by cabling standards.

A pass or fail result for each parameter shall be determined by the allowable limits for that parameter. The test result of a parameter shall be marked with an asterisk (*) when the result is closer to the test limit than the measurement accuracy.

Field test measurements shall be conducted at the temperature the cabling is intended to operate.

14.11.3.4 Balanced Twisted-Pair Cabling Field Test Instrument

14.11.3.4.1 Requirements

Field test instruments shall meet the accuracy requirements for the cabling Category or Class as defined in applicable standards (e.g., ANSI/TIA-1152 or IEC 61935-1). Field test instruments shall:

- Be maintained following the equipment manufacturers guidelines.
- Have a valid calibration certificate, preferably from the equipment manufacturer.
- Be loaded with the latest revision of firmware and test limits.

Accuracy Level IIIe or higher (e.g., Level IV) field test instruments are required to measure the appropriate Category/Class of cabling to ensure accurate field test measurements. Table 14-10 provides information on the field testing configuration, frequency range, and minimum accuracy level of the test instrument for testing ISO Class E_A, ANSI/TIA Category 6A, and higher Classes/Categories of cabling systems.

Field test results that are outside the uncertainty band of the field test instruments are reported as either “pass” or “fail.” Field test results that are inside the uncertainty band of the field test instruments are reported as either “*pass” or “*fail” as appropriate. Measurement results having an asterisk (*) shall be evaluated by the relevant cabling standard or as agreed upon in the contractual specification.

14.11.3.5 Balanced Twisted-Pair Field Test Connectors and Cords

14.11.3.5.1 Field Test Equipment Interfaces, Adapters, and Cords Requirements

Test equipment interfaces, adapters, and cords used as connecting hardware have a limited life cycle and shall be inspected periodically for wear. The field test equipment manufacturer shall provide information on the life cycle of these connectors. Test adapters, interfaces, and measurement quality test cords shall be replaced per manufacturer recommendations. Test adapters, interfaces, and cords shall meet the component requirements of the standards being followed.

14.11.3.5.2 User Cords Requirements

User cords are equipment cords, patch cords, or jumpers that are included as part of the channel. User cords shall be tested in place within a channel. A user cord may be verified by inserting the cord in the channel under test. If the channel conforms to the transmission requirements, the user cord may be approved for use in that channel only. The orientation of the user cords shall not be reversed.

Table 14-10 Balanced Twisted-Pair Field Testing

Field Test Configurations	*Frequency Range*	*Minimum Accuracy Level*
10GBASE-T Class E_A/Category 6A Permanent Link	1–500 MHz	IIIe
10GBASE-T Class E_A/Category 6A Channel	1–500 MHz	IIIe
Class F/Category 7 Permanent Link and Channel	1–600 MHz	IV
Class F_A/Category 7_A Permanent Link and Channel	1–1000 MHz	IV
Class I/Category 8 Permanent Link and Channel	1–2000 MHz	V
Class II/Category 8 Permanent Link and Channel	1–2000 MHz	V

14.11.3.6 Balanced Twisted-Pair Field Test Measurement Results

14.11.3.6.1 Requirements

Field test results shall be stored in the native format of the field test instrument. The measured results of all pairs shall be reported in graphical and table format with the specification limits shown on the graphs or in the table at the same frequencies as specified in the relevant cabling specifications. The reports shall explicitly note whether the measured results exceed the test limits. Additionally, the test results shall be carefully reviewed to ensure compliance to specified standards.

Any reconfiguration of cabling components after testing may change the performance, thereby invalidating previous test results. Such cabling shall require retesting to confirm conformance.

14.11.4 Optical Fiber Cabling Field Testing

14.11.4.1 General

14.11.4.1.1 Introduction

An optical fiber cabling link may consist of a fiber or concatenated fibers (spliced, cross-connected, or interconnected) with a connector or adapter on each end.

There are two approaches for establishing the limits against which to validate an optical fiber channel:

- Against the generic requirements set out in the cabling standard being followed for losses based on a predefined channel of a given distance
- Against the loss requirements for a specific optical fiber application

Factors that affect the attenuation measurements of installed and field tested optical fiber cabling include:

- Optical fiber type
- Link length
- Number and quality of terminations and splices
- Cable stresses
- Transmission wavelength

Link attenuation can be adversely influenced by:

- Severe cable bends
- Poorly installed connectors
- The presence of particulate matter (e.g., dirt or dust) on the endface of connectors

14.11.4.1.2 Requirements

Field testing optical fiber cabling shall be performed on length, optical attenuation, and polarity. An optical loss test set (OLTS), also referred to as a power meter and light source, shall be used to measure optical attenuation and length, if capable, and may be used to ensure correct polarity. An optical time domain reflectometer (OTDR) shall be used to characterize anomalies or damaged areas along the installed fiber and to evaluate uniformity of connections (connectors and splices). Optical fiber cabling field testing shall be conducted in accordance with the published standards for the cabling solution being used.

NOTE: A visible light source is a visible incandescent, LED or laser source used to trace fibers and may be used to verify polarity.

Measurement quality test cords and their connectors used for testing shall meet requirements for reference test cords (e.g., ISO/IEC 14763-3), which will provide accuracy and repeatability of the results obtained.

WARNING: All tests performed on optical fiber cabling that use a laser or light emitting diode (LED) in a test set are to be carried out with safety precautions in accordance with applicable standards (e.g., ANSI Z136.2).

14.11.4.1.3 Recommendations

An OTDR should be used to measure fiber length, reflectance, and optical return loss (ORL).

14.11.4.2 Optical Fiber Cabling Field Test Configuration

14.11.4.2.1 Introduction

There are three test configurations available for use with an OLTS (see IEC 61280-4-1 and IEC 61280-4-2). These are:

- 1 jumper reference method
- 2 jumper reference method
- 3 jumper reference method

Used in conjunction with an OLTS, an optical fiber link may also be tested with an OTDR. This can be accomplished from one end of the fiber. However, a tail cord shall be placed at the far end of the link that is at least 100 m in length so that the far-end connector can be characterized.

14.11.4.2.2 Requirements

For multimode and single-mode cabling, the test jumper connectors and the connector ports under test shall be clean and free of damage in accordance with IEC-61300-3-35.

At the time of assembly or testing of optical fiber, the installer shall view the endfaces of the fiber with a microscope. Viewing the endface may indicate that the endface is damaged or that it is contaminated (e.g., dirt, oil from fingers). When needed, the connector shall be cleaned, repolished, or replaced before making connections.

Channel links shall be tested with an OLTS using a three jumper reference method. The set up and methods for using these are set out in the relevant cabling standards.

Permanent links shall be tested with an OLTS using a one jumper reference method. The set up and methods for using these are set out in the relevant cabling standards.

14.11.4.3 Optical Fiber Test Parameters

14.11.4.3.1 Requirements

The field test parameters to be measured shall meet the requirements of the cabling standards being followed (e.g., ANSI/TIA-568.0-D, EN 50346). Testing installed optical fiber cabling for attenuation with an optical loss test set (OLTS) as described in cabling standards verifying the cabling length and polarity constitutes the minimum degree of testing.

Each optical fiber link shall be measured for its attenuation with an OLTS in each direction and bi-directionally. Fiber length verification may be obtained from cable sheath markings or by use of the OLTS (if the OLTS has length measurement capability). Polarity can be verified with the OLTS while performing attenuation tests. A visible light source, such as a visual fault locator, can also be used to verify polarity.

The link attenuation allowance shall be calculated as follows:

$$\textit{Link Attenuation Allowance (dB)} \;=\; \begin{array}{c} \textit{Cable Attenuation Allowance (dB) +} \\ \textit{Connector Insertion Loss Allowance (dB) +} \\ \textit{Splice Insertion Loss Allowance (dB) +} \\ \textit{Reference jumper Repeatability Allowance (dB)} \end{array} \qquad \text{(14-3)}$$

where:

Cable Attenuation Allowance (dB) = Maximum Cable Attenuation Coefficient (dB/km) * Length (km)

Connector Insertion Loss Allowance (dB) = Number of Connector Pairs * Connector Loss Allowance (dB)

Splice Insertion Loss Allowance (dB) = Number of Splices * Splice Loss Allowance (dB)

Reference jumper Repeatability Allowance (dB) = see Table 14-11

Table 14-11 Reference Jumper Repeatability Allowance

Attenuation with reference cords	*Multimode*	*Singlemode*
Reference Cord to Reference Cord	0.10 dB	0.20 dB
Reference Cord to non-Reference Cord	0.60 dB	0.65 dB
Non-Reference Cord to non-Reference Cord	0.75 dB	0.75 dB

An OTDR trace characterizes the installed fiber link, resulting in an indication of fiber segment length, attenuation uniformity and attenuation rate, connector location and insertion loss, splice location and splice loss, and other power loss events such as a sharp bend that may have been incurred during cable installation.

NOTE: The optical lengths of certain cables (e.g., stranded loose tube) may be longer than the cable sheath because of the fiber lay within the cable sheath. However, the recorded length measurement is assumed to be the physical jacketed cable length.

An acceptable attenuation for optical fiber cabling shall be based on an attenuation allowance equation and then compared to the measured installed loss. The loss allowance equation is based on the component losses for each of the components in the permanent link or channel and includes optical fiber type, cable type, wavelength, link distance, number of connections (e.g., mated pairs), and number of splices. The mean insertion loss of each component shall be obtained from the manufacturer and used in the link attenuation allowance calculation.

14.11.4.3.2 Recommendations

Because the validity of the test depends on a proper reference setting, it is critical to follow step by step the proper procedures described in the standards for each OLTS test.

An OTDR may be used to measure reflectance and ORL.

NOTE: Reflectance is the return loss for individual events (i.e., the reflection above the fiber backscatter level, relative to the source pulse). ORL is the return loss for the entire fiber under test, including fiber backscatter and reflections and relative to the source pulse.

Measured reflectance and ORL values should not exceed the expected values listed in the design or testing documentation.

14.11.4.4 Optical Fiber Cabling Field Test Instrument

14.11.4.4.1 Requirements

Optical fiber field test instruments for multimode cabling shall meet the requirements of applicable standards (e.g., IEC 61280-4-1) and be encircled flux compliant.

Optical fiber field test instruments for single-mode cabling shall meet the requirements of applicable standards (e.g., IEC 61280-4-2).

Field test instruments shall:

- Be maintained following the equipment manufacturer’s guidelines
- Have a valid calibration certificate, preferably from the equipment manufacturer
- Be loaded with the latest revision of firmware and test limits

14.11.4.4.2 Recommendations

Encircled flux limits do not account for enabling existing field test instruments that may meet outdated standards. The use of an external modal conditioner with existing field test instruments adds additional uncertainty. These cumulative uncertainties may cause variations outside the encircled flux limits, more so at one wavelength over another.

14.11.4.5 Additional Information

Common IEEE and Fibre Channel applications in the data center are listed in Table 14-12, Table 14-13 and Table 14-14.

Table 14-12 Common IEEE Applications Using Multimode Optical Fiber Cabling

Name	*Data Rate (Gbps)*	*Maximum Distance*			*Fiber Pairs*	*Connector Type*
		OM3	*OM4*	*OM5*		
1000BASE-SX	1	550 m	550 m	550 m	1	LC Duplex
10GBASE-LX4	10	300 m	300 m	300 m	1	LC Duplex
10GBASE-SR	10	300 m	400 m	400 m	1	LC Duplex
25GBASE-SR	25	70 m	100 m	100 m	1	LC Duplex
50GBASE-SR	*50*	*70 m*	*100 m*	*100 m*	*1*	*LC Duplex*
40GBASE-SR4	40	100 m	150 m	150 m	4	MPO
100GBASE-SR10	100	100 m	150 m	150 m	10	MPO
100GBASE-SR4	100	70 m	100 m	100 m	4	MPO
100GBASE-SR2	*100*	*70 m*	*100 m*	*150 m*	*1*	*LC Duplex*
200GBASE-SR4	*100*	*70 m*	*100 m*	*150 m*	*4*	*MPO*
400GBASE-SR16	400	70 m	100 m	100 m	16	MPO

NOTE: *Gray, italicized* text indicates application was in development at the time of publication of this standard

Table 14-13 Common IEEE Applications Using Singlemode Optical Fiber Cabling

Name	*Data Rate (Gbps)*	*Maximum Distance (OS2)*	*Fiber Pairs*	*Connector Type*
1000BASE-LX	1	5 km	1	LC Duplex
10GBASE-LX4	10	10 km	1	LC Duplex
10GBASE-LR	10	10 km	1	LC Duplex
10GBASE-ER	10	22 km	1	LC Duplex
25GBASE-LR	25	10 km	1	LC Duplex
25GBASE-ER	25	40 km	1	LC Duplex
40GBASE-LR4	40	10 km	1	LC Duplex
40GBASE-ER4	40	40 km	1	LC Duplex
50GBASE-FR	*50*	*2 km*	*1*	*LC Duplex*
50GBASE-LR	*50*	*10 km*	*1*	*LC Duplex*
100GBASE-LR4	100	10 km	1	LC Duplex
100GBASE-ER4	100	40 km	1	LC Duplex
100GBASE-DR2	*100*	*500 m*	*2*	*MPO*
100GBASE-FR2	*100*	*2 km*	*1*	*LC Duplex*
200GBASE-DR4	200	500 m	4	MPO
200GBASE-FR4	200	2 km	1	LC Duplex
200GBASE-LR4	200	10 km	1	LC Duplex
400GBASE-DR4	400	500 m	4	MPO
400GBASE-FR8	400	2 km	1	LC Duplex
400GBASE-LR8	400	10 km	1	LC Duplex

NOTE: *Gray, italicized* text indicates application was in development at the time of publication of this standard

Table 14-14 Common Fibre Channel Applications Using Optical Fiber Cabling

Name	*Fiber Type*	*Data Rate (Gbps)*	*Maximum Distance*				*Fiber Pairs*	*Connector Type*
			OM3	*OM4*	*OM5*	*OS2*		
3200-M5x-SN-S	Multimode	32	70 m	100 m	100 m	–	1	LC Duplex
3200-SN-LC-L	Singlemode	32	–	–	–	10 km	1	LC Duplex
128GFC-SW4	Multimode	128	70 m	100 m	100 m	–	4	MPO
128GFC-PSM4	Singlemode	128	–	–	–	500 m	4	MPO
128GFC-CWDM4	Singlemode	128	–	–	–	2 km	1	LC Duplex
64GFC	*Multimode*	*64*	*70 m*	*100 m*	*100 m*	*–*	*1*	*LC Duplex*
64GFC	*Singlemode*	*64*	*–*	*–*	*–*	*10 km*	*1*	*LC Duplex*
256GFC	*Multimode*	*256*	*70 m*	*100 m*	*100 m*	*–*	*4*	*MPO*
256GFC	*Singlemode*	*256*	*–*	*–*	*–*	*2 km*	*1*	*LC Duplex*

NOTE: *Gray, italicized* text indicates application was in development at the time of publication of this standard

14.11.4.6 Optical Fiber Cabling Field Test Interfaces, Adapters, Connectors, and Cords

14.11.4.6.1 Requirements

Test equipment interfaces, adapters, connectors, and cords used as connecting hardware have a limited life cycle and shall be inspected periodically for wear. The field test equipment manufacturer shall provide information on the life cycle of these components. Test adapters, interfaces, connectors, and cords shall be replaced per manufacturer recommendations.

User cords are equipment cords, patch cords, or jumpers that are included as part of the channel. User cords shall be tested in place within a channel. A user cord may be verified by inserting the cord in the channel under test. If the channel conforms to the transmission requirements, the user cord may be approved for use in that channel only. The orientation of the user cords shall not be reversed.

Connector endfaces shall be inspected with a suitable microscope (minimum 100x magnification) and when necessary cleaned in accordance with manufacturer's instructions prior to mating.

14.11.4.6.2 Recommendations

Test equipment interfaces, adapters, connectors, and cords should be either colored or labeled differently from in-service counterparts (preferably a single color dedicated for 'test equipment') to easily distinguish them from in-service equipment.

The use of temporary index matching materials (gels and fluids) in mated connectors under test is not recommended where the introduction of such materials may invalidate any measurement or test result.

14.11.4.7 Optical Fiber Cabling Field Test Documentation

14.11.4.7.1 Requirements

Documenting the test results provides the information that demonstrates the acceptability of the cabling system or support of specific networking technologies. A permanent record of all tests should be retained together with:

- Details of the measurement procedure
- Details of the measurement type
- Serial number of field test instruments used
- Proof of up to date calibration of the field test equipment
- Details of the measurement quality test cords used

14.12 Telecommunications and Computer Cabinets and Racks

14.12.1 Introduction

As with all other systems of the data center—power, HVAC, and flooring—cabinets and racking systems provide the vital services of proper structural and secure housing for data center equipment. Active and passive equipment have different requirements for mounting, power, ventilation, and cable management.

The vast majority of manufactured ITE cabinets and racks are compliant with EIA/ECA-310-E. Depending on the expected operational environment for a data center, the use of cabinets and racks designed to address or mitigate issues arising from operational decisions may be required. Table 14-15 provides an overview of some of these alternative configurations.

Table 14-15 Alternative Rack Specifications

Attribute\ Rack Type	*Open Rack v2.0*	*CG-Open Rack-19*	*Project Olympus*
Outside Width	Variable 600 mm (24 in) typical	600 mm (24 in)	EIA/ECA-310-E Compliant
Depth	Standard: 1048mm (41.25 in) Shallow: 62 mm (30 in)	1200 mm (47.25 in)	EIA/ECA-310-E Compliant
Height	Variable 2210 mm in use	Variable	EIA/ECA-310-E Compliant
Weight (Loaded)	Variable typically 500 – 1400 kg (1100 – 3085 lb)	Variable typically 500 – 1400 kg (1100 – 3085 lb)	Variable
Mounting Rail Spacing	2533 mm (21·in)	19 in (480 mm) EIA/ECA-310-E Compliant	19 in (480 mm) EIA/ECA-310-E Compliant
Rack Unit (RU) Spacing	48 mm (1.89 in) OpenU (OU)	44.45 mm (1.75 in) EIA/ECA-310-E Compliant	44.45 mm (1.75 in) EIA/ECA-310-E Compliant
Required Access	Primarily Front Only	Primarily Front Only	Primarily Front Only
PSU Architecture	3 phase AC rack PSU to 12V or 48 V_{DC} busbar distribution	3 phase AC rack PSU to $12V_{DC}$ busbar distribution	3 phase PSU internal to server
Battery Backup	Optional typically In-rack Li-ion	Optional typically In-rack Li-ion	Optional typically In-rack Li-ion
Power Feed to Rack	Typically 3 phase AC 230/ 400 V_{AC}	3 phase AC 90 - $264V_{AC}$	3 phase AC 230/ 400 V_{AC}
Airflow	Front to Back	Front to Back	Front to Back

14.12.2 Requirements and Recommendations

14.12.2.1 General Requirements

Two post racks, four post racks, and cabinets shall be secured in accordance with AHJ, seismic requirements for the location, and the planned long-term loading. When access floor systems are used, any one of the following methods shall be permitted:

- Attachment to metal struts that are captured below the floor by two or more access floor stringers
- Attachment to metal struts below the access floor that are suitably attached to the permanent floor
- Attachment via threaded rod directly to the permanent floor
- Attachment to channel bases bolted to floor slab

Cabinets and racks shall be constructed of noncombustible materials.

Performance specifications and overall physical dimensions of cabinets and racks shall conform to applicable codes, standards, and regulations (e.g., ATIS 0600336, EIA/ECA-310-E, IEC 60917).

14.12.2.2 General Recommendations

If not already required by the AHJ in locations where seismic activity could create a potential risk, cabinets and four-post racks in the computer room should be anchored at their base to the permanent floor and preferably braced at the top (the raceway or overhead auxiliary framing can be used for this).

14.12.2.3 Rack Requirements

The following criteria of racks shall conform to applicable codes, standards and regulations (e.g., EIA/ECA-310-E, IEC 60917):

- Channel dimensions and spacing
- Channel hole dimensions and thread systems
- Channel equipment mounting hole vertical spacing (U or RU)
- Panel opening and usable aperture opening

14.12.2.3.1 Rack Recommendations

Maximum height should not exceed 2.4 m (8 ft).

When in a row, multiple racks and their associated vertical cable managers should be bolted together.

14.12.2.4 Cabinet Requirements

The following criteria shall conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917):

- Equipment mounting rail dimensions and spacing
- Equipment mounting rail hole vertical spacing (U or RU)

Options for cable access into the cabinet shall be available from both the top and bottom.

Access floor openings beneath cabinets for cable entry shall offer:

- Protection against damage to the cables
- Restrictions against intrusion of dirt and debris
- Restriction of air passage

Cabinets shall be constructed of noncombustible materials.

14.12.2.5 Cabinet Recommendations

Maximum height should not exceed 2.4 m (8 ft). Width should conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917), allowing for the exceptions noted therein.

Top access ports should provide a means to be closed when not in use.

In seismically active areas, multiple cabinets in a row should be bolted together at the top to provide additional stability.

14.12.3 Cabinet and Rack Configurations

14.12.3.1 General Recommendations

The cabinets and racks are generally installed in a method that segregates the hot and cold areas, so the products themselves should be selected for their capacity to integrate into the general air segregation method.

They should:

- Ensure that the equipment inside always employs the same hot aisle / cold aisle orientation
- If the equipment cannot allow this, such as networking equipment with side-to-side cooling, then the cabinet or rack should provide channeling of the air to reorient it in the right direction.
- Provide cable support in a location that does not impede the airflow and does not risk their damage when moving or adding equipment.
- Manage the cords so that they do not impede the air intake or air exhaust of the ITE.

Cabinets and racks must be selected according to their use.

The EDA holds high densities of ITE. Patch panels should also be placed so that the ports are facing the same direction as the ITE, generally in the rear, to facilitate patching. If cords must cross from front to back, then specific channels should be provided to organize and protect them.

The IDA and MDA generally hold a mix of networking equipment and patch panels. Extra caution should be used to manage the high quantities of patch cords as well as allowing cooling of the networking equipment, often side-to-side. Some specific solutions:

- The use of extra wide cabinets, up to 1 m (39 in) wide, allowing easier management of the cords.
- Using internal compartments in cabinets for air segregation
- Using special networking equipment with front to rear cooling.
- Separating equipment from patching. This can be done by converting the interconnect into a cross connect. In this case, dedicated patching racks can be used outside of the rows.

Finishes should conform to applicable codes, standards, and regulations (e.g., ANSI/TIA-942-B, ATIS 0600336); conductive finishes are recommended to ensure a good bond between equipment and cabinet or rack ground and to prevent oxidation of the base metal. For painted racks, a supplementary bonding/grounding busbar system may be used to ensure a good bond between equipment and cabinet or rack ground. Cabinet and rack bonding and grounding should comply with applicable codes, standards, and regulations (e.g., ANSI/NECA/BICSI-607, ANSI/TIA-607-C, ISO/IEC 30129).

Racks in entrance rooms, main distribution areas and horizontal distribution areas should have dimensions and cable management capacities in accordance with applicable codes, standards, and regulations (e.g., ANSI/TIA-942-B).

The management of the patch cords is critical to allow proper visibility and easy changes. Otherwise there is an increased risk of error during MACs.

There are two main types of patch cord management:

- Horizontal. The typical is a 1U (or more) plate with rings, designed to be placed below each patch panel or active equipment. The general rule is that each 24 ports on a panel or switch is supported by 1U of horizontal manager. For example, a 48port switch could require a 2U manager. Some patch panels have integrated management and do not require extra horizontal managers, allowing to save space.
- Vertical: In cabinets these are generally limited in size by the width of the cabinet. With open racks, more options are available. Some vertical managers also include “finger” type support for every unit of space. These may negate the requirement for horizontal management depending on design.

The density of ports in a rack or cabinet should never be calculated based on the rack-unit space available, but primarily on the space available for patch cords in the management. For example, a 600mm wide cabinet might have 42 RU of space for panels, but it can never support bundles of 100 cords vertically.

Cords should always be selected with shortest possible length that allows the connections according to the design. Extra lengths of cords always create more difficulties in management.

Consider the requirements for future cabling and equipment when determining the number and sizes of cabinets required. Space should be provided in cabinets and racks for technology refresh to preferably allow old equipment to be replaced with new equipment with both the old and new equipment in operation concurrently during the refresh.

14.12.3.2 Rack Configuration Recommendations

Rack depth should meet the mounting and protection needs of the equipment they are to host and, as a minimum, conform to the criteria established in applicable standards (e.g., EIA/ECA-310-E, IEC 60917).

Each rack should have vertical cable managers sized for maximum rack capacity attached on both sides. Vertical cable managers between two racks should be sized to serve both racks simultaneously.

14.12.3.3 Cabinet Configuration Recommendations

Equipment mounting rails should be adjustable front-to-rear and should have rack unit number indications (with numbers starting at the bottom).

Equipment mounting rail dimensions should conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917).

Doors should be removable without tools. Door hinge orientation should be reversible or dual hinged.

Side panels should be removable and lockable without requiring intrusion into the equipment mounting area within the cabinet.

In applications where active equipment, patch panels, and horizontal cable distribution are mixed, floor-tile-width (e.g., 600 mm [24 in] width) cabinets may lack adequate vertical cable management space.

Blanking panels should be installed in unused rack positions to maintain separation between hot aisles and cold aisles and prevent hot exhaust air from recirculating and mixing with chilled air at equipment in-takes. Blanking panels also improve rigidity of cabinets. (see Figure 14-12)

Where cabinets are not secured to the floor, cabinets should utilize an anti-tip rail or other method to prevent a cabinet's movement from temporary forces or loading (e.g., equipment changes, maintenance activities, use of equipment "sliders") shifting the cabinets center of mass.

14.12.4 Cabinet Airflow and Cabling Capacity

14.12.4.1 Airflow

To ensure adequate airflow and to provide adequate space for power strips, telecommunications cabling, and safe access for work, the cabinet depth should be at least 150 mm (6 in) deeper than the deepest equipment to be housed if the cabinet is 700 mm (27.5 in) wide or larger. If the cabinet is less than 700 mm (27.5 in) wide, 11.5 mm (0.45 in) depth should be added for every 10 mm (0.4 in) reduction from 700 mm (27.6 in) width. (See Table 14-16)

Where mesh doors are used for ventilation, the doors should be a minimum 63% open to airflow for allowing chilled air entrance or evacuating heated exhaust air from the cabinet.

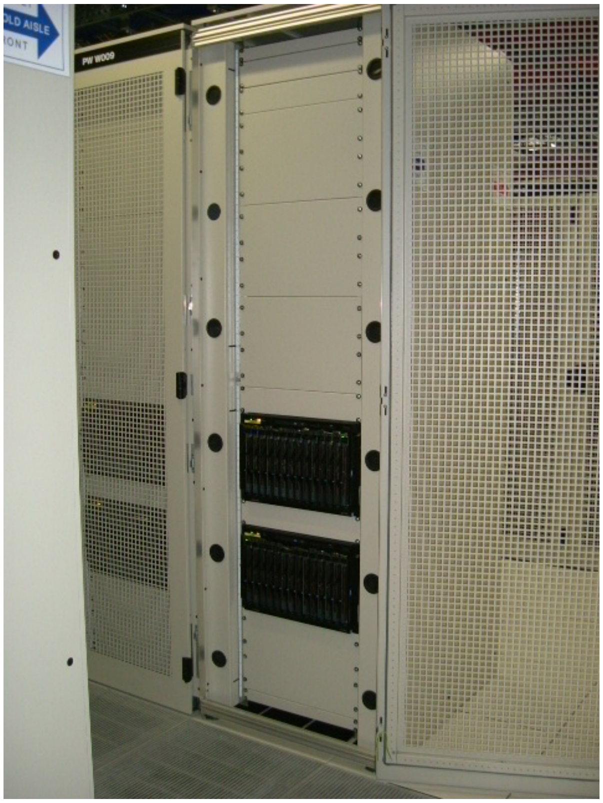


Figure 14-12
Blanking Panels Installed in Empty RUs

Table 14-16 Example of Cabinet Depth Guidelines

Cabinet Width	*Deeper than the Deepest Equipment Housed in the Cabinet*	*Additional Depth for Narrow Cabinets*
600 mm (24 in)	150 mm (6 in)	115 mm (4.5 in)
700 mm (27.5 in)	150 mm (6 in)	N/A
750 mm (29.5 in)	150 mm (6 in)	N/A
800 mm (31.5 in)	150 mm (6 in)	N/A

14.12.4.2 Calculating Cabinet Airflow Capacity

It is recommended that the following formulae be used to calculate door airflow capacity:

Airflow capacity (*AFC*) calculations:

$$AFC_D = \frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}} \qquad (14\text{-}4)$$

Where:

AFC_D is airflow capacity for cabinets with doors

S_D is total surface area of the door panel inside the outer extreme boundaries of airflow openings (mesh, perforations, slots, etc.), in mm^2 (in^2)

F_{EA} is effective (open) area factor of the door mesh material (e.g., 0.65 [65%], 1 if mesh or screen is not used)

A_C is useable cabinet aperture opening at the door plane, in mm (in) (See Figure 14-13)

H_{RMU} is height of one rack unit (44.5 mm [1.75 in])

N_{RMU} is quantity of rack units in the cabinet.

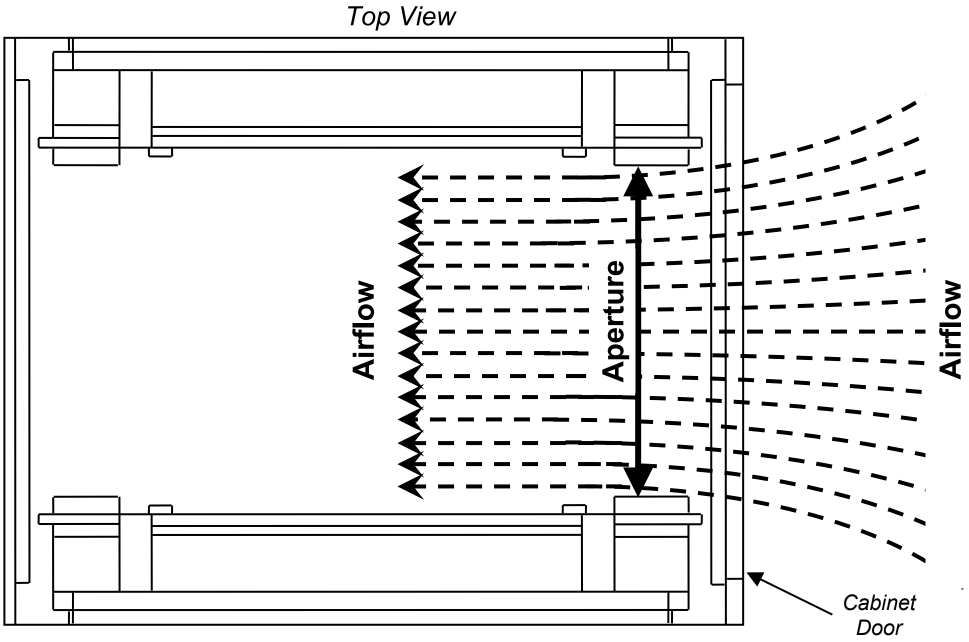


Figure 14-13
Cabinet Aperture Opening

Example: Network cabinet or server cabinet design with mesh doors

NOTE: The following parameters are for demonstration purposes and may not reflect actual properties of a specific cabinet or design requirements.

Given:

- 19-in equipment cabinet
- Height: 42 RMU
- Mesh door with F_{EA} = 0.65, 1,930 mm x 635 mm (76 in x 25 in)
- 1 RMU = 44.5 mm (1.75 in)
- Cabinet open aperture: 450.85 mm (17.75 in)

NOTE: Input data and criteria used in the examples above are provided as samples only. For actual parameters, please refer to the particular network cabinet or server cabinet design requirements.

Airflow capacity:

$$AFC_D = \left(\frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}}\right) = \left(\frac{1{,}930\ mm \times 635\ mm \times 0.65}{450.85\ mm \times 44.5\ mm \times 42}\right)$$

$$AFC_D = \frac{1{,}225{,}550\ mm^2 \times 0.65}{842{,}639\ mm^2} = 0.9454$$

$$AFC_D = \left(\frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}}\right) = \left(\frac{76\ in \times 25\ in \times 0.65}{17.75\ in \times 1.75\ in \times 42}\right)$$

$$AFC_D = \frac{1{,}900\ in^2 \times 0.65}{1{,}304.63\ in^2} = 0.9467$$

Conclusion: the cabinet mesh door open airflow capacity (ACF_D) falls within the recommended limits (e.g., 0.63-1.00 [63%-100%]).

When using Equation 14-4, any area within SD occupied by airflow impervious structures (e.g., such as door latches, door locks, access control panels), must be subtracted from the initial SD to establish the final SD for above calculations.

14.12.4.3 Cabinet Cable Capacity

14.12.4.3.1 Calculating Number of Cables

In order to estimate the number of cables the cabinet can accommodate, the following formulae can be used:

$$N = \frac{S_U}{S_{cable}} \times f_{fill} = \frac{S_I - S_E - S_O}{S_{cable}} \times f_{fill} \qquad (14\text{-}5)$$

where:

N is the number of cables the cabinet can accommodate

S_U is the useful cabinet area, where cables can be installed, mm^2 (in^2)

S_{cable} is the cable cross-sectional area, mm^2 (in^2) (see Section 14.12.4.3.2)

f_{fill} is required or recommended cable pathway fill factor (e.g., 0.4 [i.e., 40 %])

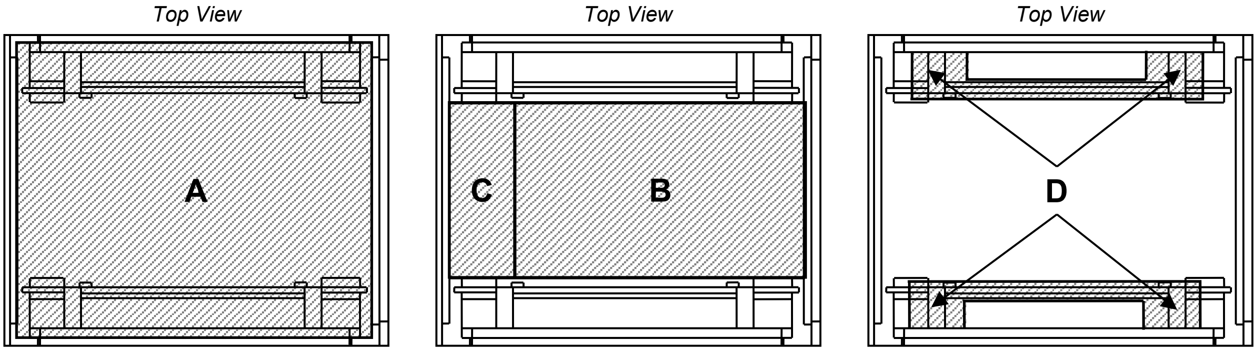
S_I is the cabinet internal area, mm^2 (in^2) (see Section 14.12.4.3.4)

S_E is the area allocated for active equipment and connecting hardware, mm^2 (in^2) (see Section 14.12.4.3.5)

S_O is the area occupied by various obstructing elements, such as rails, power strips, mm^2 (in^2) (see Section 14.12.4.3.6)

Illustrations of S_I, S_E, and S_O components are provided in Figure 14-14.

NOTE: Boundaries of areas shown in Figure 14-14 are for illustration purposes only; actual boundaries may vary depending on the cabinet design and layout.



Area A: S_I —cabinet internal area

Area B: S_E—area allocated for active equipment and connecting hardware including area C

Area C: "dead zone", spare space behind active equipment and connecting hardware

Area D: S_O—area occupied by various obstructing elements, such as rails, power strips, etc.

Figure 14-14
Illustration of Components for Cable Capacity Formulae

14.12.4.3.2 Equation for Cable Cross Section Area (S_{cable})

The following equation for S_{cable} is used when the cables within the cabinet have a consistent diameter.

$$S_{cable} = \pi \times \frac{(d_{cable})^2}{4} = 3.14 \times \frac{(d_{cable})^2}{4} = 0.79 \times (d_{cable})^2 \qquad (14\text{-}6)$$

where:

d_{cable} is the cable diameter, mm (in)

NOTE: See Section 14.12.4.3.3 for information on the calculation of d_{cable} when multiple cable diameters are expected or present.

14.12.4.3.3 Equation for Cable Diameter (d_{cable}) for Multiple Cable Diameters

When cables of differing diameters are to be deployed in a cabinet, because of differing media or performance characteristics (e.g., Category 5e and Category 6A), the cross-sectional area can be approximated. This approximation is based on the diameters of the cables to be installed and the percentage of each cable type expected to be installed (e.g., 40% of the cable will be Category 5e and 60% will be Category 6A).

$$d_{cable} = \sqrt{\sum_{i=1}^{n} P_i \times D_i^2} \qquad (14\text{-}7)$$

where:

d_{cable} is the cable diameter, mm (in)

n is the total number of different cable diameters

P_i is the percentage of the specific (indexed) cable

D_i is the diameter of the specific (indexed) cable

Example

Cable A has a diameter of 4.8 mm (0.19 in) and constitutes 8% of the total, Cable B has a diameter of 7.7 mm (0.30 in) and constitutes 32% of the total and a third cable has a diameter of 5.6 mm (0.22 in) and constitutes 60% of the total

$d_{cable} = \sqrt{}[(0.08 \times 4.8 \text{ mm} \times 4.8 \text{ mm}) + (0.32 \times 7.7 \text{ mm} \times 7.7 \text{ mm}) + (0.6 \times 5.6 \text{ mm} \times 5.6 \text{ mm})]$

$d_{cable} = \sqrt{}(1.843 \text{ mm}^2 + 18.973 \text{ mm}^2 + 18.816 \text{ mm}^2)$

$d_{cable} = \sqrt{}39.632 \text{ mm}^2$

$d_{cable} = 6.30 \text{ mm}$

or

$d_{cable} = \sqrt{}[\ (0.08 \times 0.19 \text{ in} \times 0.19 \text{ in}) + (0.32 \times 0.30 \text{ in} \times 0.30 \text{ in}) + (0.6 \times 0.22 \text{ in} \times 0.22 \text{ in})]$

$d_{cable} = \sqrt{}(0.003 \text{ in}^2 + 0.029 \text{ in}^2 + 0.029 \text{ in}^2)$

$d_{cable} = \sqrt{}0.061 \text{ in}^2$

$d_{cable} = 0.247 \text{ in}$

Once N, the number of cables for a specific cabinet, has been calculated (see Eq. 14-5), the specific number of each cable can be determined by multiplying N by the specific cable percentage.

14.12.4.3.4 Equation for Cabinet Internal Area ($S_{I)}$)

$$S_I = (W_C \times f_D) \times (D_C \times f_D) = W_C \times D_C \times f_D^2 \qquad (14\text{-}8)$$

where:

W_C is cabinet width, mm (in)

D_C is cabinet depth, mm (in)

f_D is dimensional de-rating factor for internal space (e.g., 0.95)

14.12.4.3.5 Equation for Area Allocated for Active Equipment and Connecting Hardware ($S_{E)}$

$$S_E = A_C \times (D_C \times f_D) \qquad (14\text{-}9)$$

where:

A_C is useable cabinet aperture opening, mm (e.g., 450.85 mm [17.75 in])

D_C is cabinet depth, mm (in)

f_D is dimensional de-rating factor for internal space (e.g., 0.95)

14.12.4.3.6 Equation for Area Occupied by Obstructing Elements (S_O)

$$S_O = (S_I - S_E) \times f_O \qquad (14\text{-}10)$$

where:

f_O is de-rating factor taking into account the obstructing elements (e.g., 0.3)

S_I is the cabinet internal area, mm^2 (in^2) (see Section 14.12.4.3.4

S_E is the area allocated for active equipment and connecting hardware, mm^2 (in^2) (see Section 14.12.4.3.5)

14.12.4.3.7 Alternative Equation for Calculating Cabinet Cabling Capacity

As an alternative to separate calculations of each component provided above (which may be required for detailed design analysis), the following reduced formula (14-11) may be used:

$$N = \frac{\{[(D_C - D_E) \times f_D] \times [(W_C - A_C) \times f_D \times (1 - f_O)]\} \times f_{fill}}{0.79 \times (d_{cable})^2} \qquad (14\text{-}11)$$

where:

D_C = cabinet depth, mm (in)

D_E = maximum equipment depth, mm (in)

f_D = dimensional de-rating factor for internal space (e.g., 0.95)

f_{fill} = required or recommended cable pathway fill factor (e.g., 0.4 [i.e., 40 %])

W_C = cabinet width, mm (in)

A_C = useable cabinet aperture opening, mm (e.g., 450.85 mm [17.75 in])

f_O = de-rating factor taking into account the obstructing elements (e.g., 0.3)

d_{cable} = cable diameter, mm (in)

Where available, vendor cable manager calculators should be used to specify a correctly sized cabinet. Where such calculators are not available, Table 14-17 provides cable capacity estimates based on total available space outside of the equipment mounting area and between the rear equipment mounting rail (located at 762 mm [30 in] behind the front frame piece) and the rear frame and allowing 152 mm^2 (0.24 in^2) for vertical power strips, regardless of the presence or lack of vertical cable management accessories.

Cabinets should have adequate width and depth to avoid routing of cabling behind equipment exhausts where they may obstruct proper airflow.

Cable management capacity requirements should be calculated prior to either specifying a cabinet or even specifying a cabinet footprint.

Vertical cable management should be available and should be deployable in either the zero U space or, in deeper, more cabling intensive applications, in the equipment mounting space behind the mounted equipment.

Cabinets should include integral features for attaching any sort of external bracing structures.

Front and rear clearances around cabinets should conform to applicable codes, standards and regulations (e.g., NFPA 70; see also Section 6.6). Minimum clearances should be optimized with either 150° or larger door swing, or split doors with hinges on both sides and latching in the center.

NOTE: Use the cross sectional values from Table 14-17 to calculate the cable capacity of a cabinet per the following procedure:

$$N = round\_down\ (A_{cable\ management\ space} \div A_{cable}) \times f \qquad (14\text{-}12)$$

Where:

N = Number of cables
$A_{cable\ management\ space}$ = cross sectional space from Table 14-17 in mm^2 (in^2)
A_{cable} = cross sectional area of cable, mm^2 (in^2)
f = fill rate

For example, a 1050 mm (41.3 in) deep and 700 mm (27.5 in) wide cabinet with one power strip and 8 mm (0.31 in) diameter cable would be calculated as follows for a 40% fill rate:

$A_{cable\ management\ space}$ = 89600 mm^2
A_{cable} = $\pi \times 4^2$ = 50.24 mm^2
N = (89600/50.24) × 0.4 = 713.3758 = 713

Table 14-17 assumes cables are managed outside the space used for ventilation of equipment. The rows with "a" following the cabinet depth are for one vertically mounted power strip. The rows for "b" following the cabinet depth are for two vertically mounted power strips.

14.12.5 Cabinet and Rack Installations

14.12.5.1 General Requirements

Where the cabinets and racks are on an access floor, they shall be placed so that there are liftable tiles in front and behind each cabinet and rack. This typically means placing the rows of cabinets and racks parallel (rather than at an angle) to the rows of floor tiles and placing the front edge of the cabinets along the edge of the floor tiles to lock down the minimum number of tiles under the cabinets.

Additionally, if the computer room uses the access floor for cooling, cabinets should be placed to ensure that at least two rows of ventilated tiles can be placed in the cold aisles

All overhead cable management (e.g., ladder racks, cable tray) shall remain free of obstructions such as sprinklers, lighting, and electrical outlets.

The designer shall anticipate the weight of the equipment in the cabinets and racks; ensure that the cabinets, racks and floors (both access floors and slabs) are rated to handle the expected weight.

Adequate power shall be available to all cabinets and racks that will hold active equipment and must be installed in accordance with applicable codes and the AHJ.

Each cabinet and rack shall be labeled on the front and back with its identifier. All patch panels, cables, equipment cords, and patch cords shall be properly labeled per applicable standards (e.g., ANSI/TIA-606-C, ISO 14763-2-1). (See Figure 14-15 and Figure 14-16).

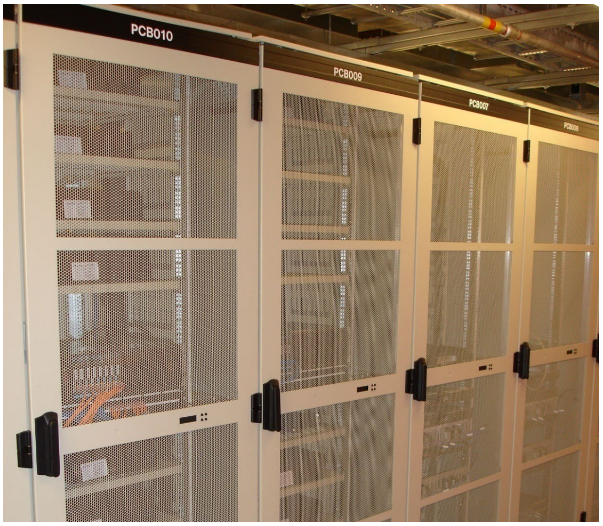


Figure 14-15
Cabinets Are Identified and Labeled

Table 14-17 Available Space for Calculating Cabinet Vertical Cable Capacity

Cross-sectional values in mm^2 (in^2) for noted cabinet depths and widths

Cabinet Frame Depth (mm)	*Cabinet Width (mm)*			
	600 mm	*700 mm*	*750 mm*	*800 mm*
900	15700 (24)	45300 (70)	58400 (90)	71400 (111)
900a[3]	10500 (16)	40100 (62)	53200 (82)	66300 (103)
900b[4]	5400 (8)	35000 (54)	48000(74)	61100 (95)
950	21500 (33)	62100 (96)	80000 (124)	97900 (152)
950a[3]	16300 (25)	56900 (88)	74800 (116)	92700 (144)
950b[4]	11200 (17)	51700 (80)	69600 (108)	87500 (136)
1000	27300 (42)	78800 (122)	124300 (157)	124300 (193)
1000a[3]	22100 (34)	73700 (114)	119200 (149)	119200 (185)
1000b[4]	17000 (26)	68500 (106)	91300 (141)	114000 (177)
1050	32800 (51)	94800 (147)	122100 (189	149500 (232)
1050a[3]	27600 (43)	89600 (139)	117000 (181)	144300 (224)
1050b[4]	22500 (35)	84500 (131)	111800 (173)	139100 (216)
1100	38600 (60)	111500 (173)	143700 (223)	175900 (273)
1100a[3]	33500 (52)	106400 (165)	138600 (215)	170700 (265)
1100b[4]	28300 (44)	101200 (157)	133400 (207)	165600 (257)
1150	44400 (69)	128300 (199)	165300 (256)	202400 (314)
1150a[3]	39300 (61)	123200 (191)	160200 (248)	197200 (306)
1150b[4]	34100 (53)	118000 (183)	155000 (232)	192000 (298)
1200	49900 (77)	144300 (224)	185900 (288)	227500 (353)
1200a[3]	44800 (69)	139100 (216)	180700 (280)	222300 (344)
1200b[4]	39600 (61)	133900 (208)	175500 (272)	217200 (337)

NOTE 1: Standard front-to-rear mounting rail spacing = 750 mm (29.5 in)
NOTE 2: Front rail is set back 25 mm (1 in) from cabinet frame
NOTE 3: Capacity de-rated for one vertically mounted power strip
NOTE 4: Capacity de-rated for two vertically mounted power strips
NOTE 5: IMPORTANT: Capacities are calculated on available space. Vendor specifications need to be referenced to determine actual cable management capacity

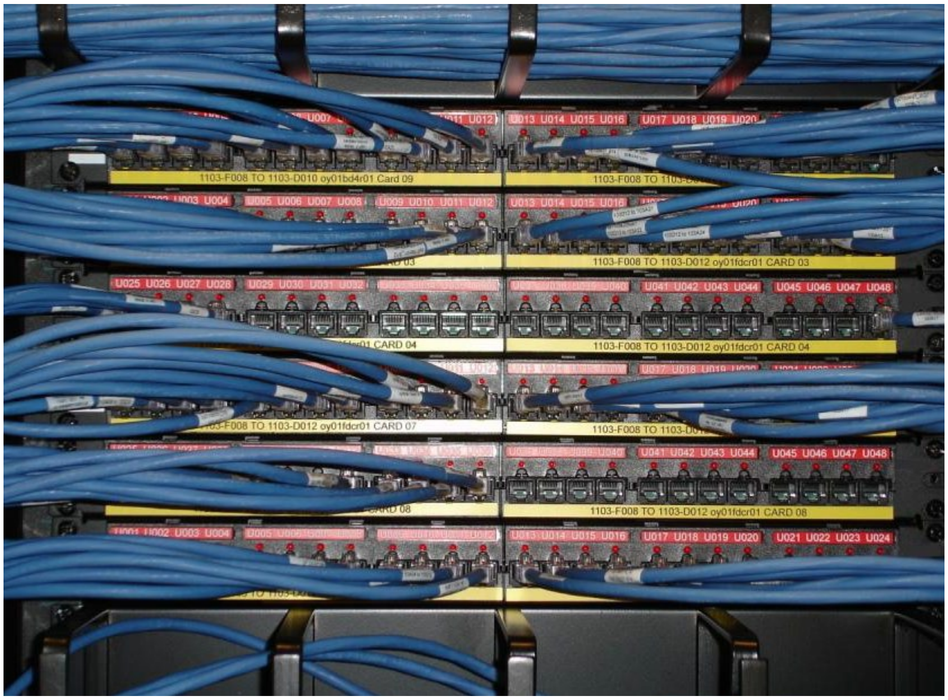


Figure 14-16
Example of Labeled Termination Ports and Equipment Cords

Front rails of cabinets shall be set back from the front of the cabinet to provide adequate room for patch cords, angled patch panels, and equipment that protrude from the front rail. The rail placement should permit the front door to close completely without exceeding the bend radii of cords and cables attached to patch panels and equipment.

Cabinets and racks shall provide adequate ventilation for equipment with airflow that does not use front-to-back cooling (e.g., by providing ducts for equipment with side-to-side). This may require wider cabinets or removing side panels between cabinets.

14.12.5.2 General Recommendations

Cabinet and rack layout designs should be harmonized with lighting (luminaire) delivery layout designs.

Anticipate growth and leave room for expansion when/if possible.

Power strips should be labeled with power distribution unit or electrical panelboard identifier and circuit breaker number.

Power cords should not be installed under equipment, mats, or covering other than access floor tiles. The mounting surface for cabinet and racks should be prepared for the specific anchors required for the application. Refer to manufacturer's recommended practice and verify those practices are acceptable to the local AHJ. Cabinets in a line-up where they are properly attached together may require fewer anchors per cabinet than those installed as standalone units. When drilling into the mounting surface use proper technique to ensure that dust or particles do not get airborne. Using a drill with attached vacuum is an effective way to prevent dust or particles while drilling in floors or walls.

14.12.5.3 Rack Installation Recommendations

Equipment in the computer room should be mounted to cabinet or rack rails rather than placed on shelves as equipment on shelves provides a return path for air between the rear and front of the cabinet or rack.

Floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings.

Consider using openings with gaskets or brush grommets to satisfy requirements to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency. See Figure 14-17 and Figure 14-18 for examples of air recirculation and Figure 14-19 and Figure 14-20 for gaskets and brush grommets.

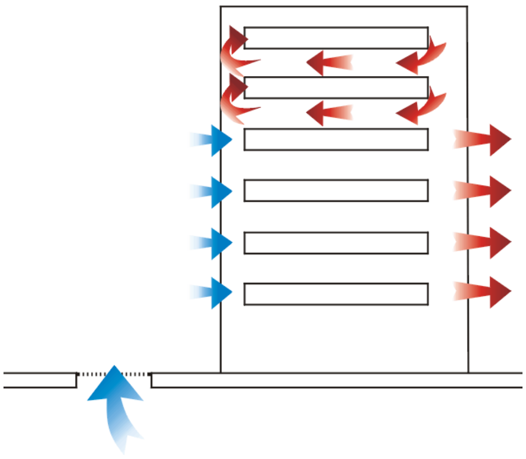


Figure 14-17
Effect Of Internal Hot Air Recirculation

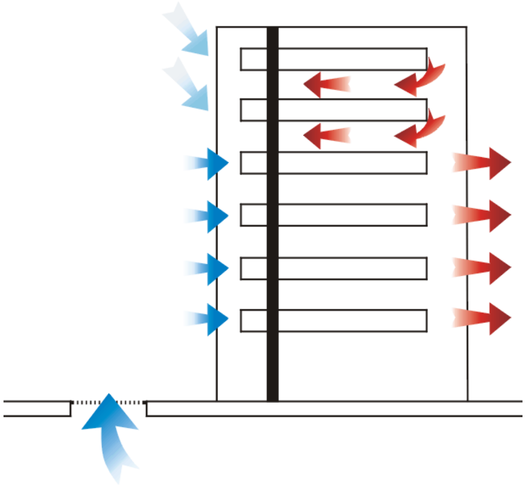


Figure 14-18
How Reducing Internal Hot Air Recirculation Reduces Input Air Temperature

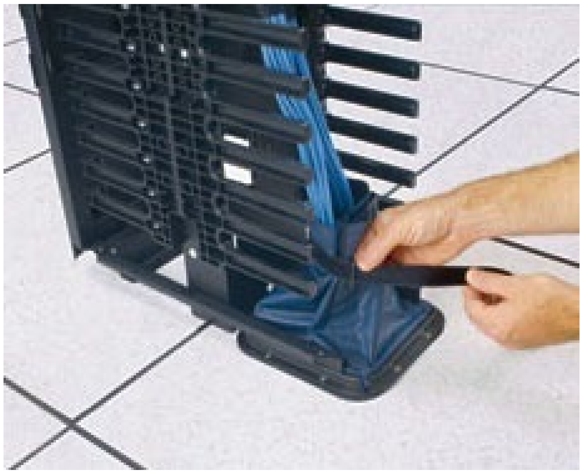


Figure 14-19
Gasket Seals Off Access Floor Tile Cutout In Vertical Cable Manager

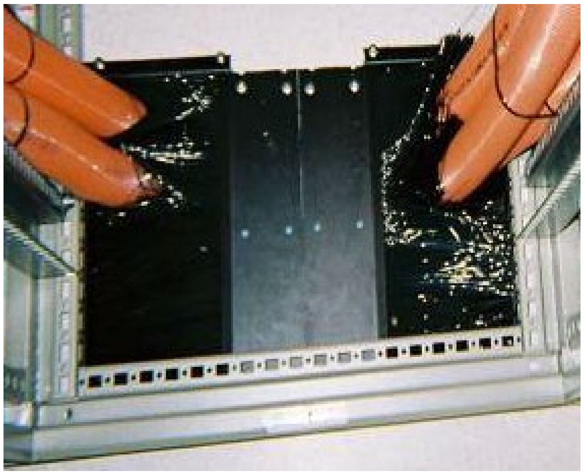


Figure 14-20
Brush Grommet Seals Access Floor Tile Cutout

A dedicated pathway should be provided for equipment cords or patch cords within an MDA, IDA, or HDA that is separate from those used for horizontal and backbone cabling.

Ensure all active devices are properly supported and securely mounted to the rack to prevent equipment damage from improper installation.

In seismically active areas, it is recommended that the design of the attachment methods and the installation be reviewed by a licensed structural engineer. Many jurisdictions will require a seismic certification report signed by a professional engineer.

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means). The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable.

Racks should be set in place and leveled throughout the line-up. Shimming of any anchoring point should not exceed 13 mm (0.5 in) unless specified by the project engineer. If racks require more than 13 mm (0.5 in) of shimming, an engineered solution should be used to ensure rack line-ups are properly supported. Adjacent racks in the line-up should be ganged together before anchors are installed. Install anchors per manufacturer specification, making sure all shims are properly located.

Some line-ups require additional bracing to meet customer specifications or local codes. Required bracing may be based on rack style, equipment, and location. Bracing should be installed as a system to ensure proper fit and support. Install all parts hand tight and then tighten fasteners in a series to prevent stress on rack lineup. All bracing should be installed before racks are populated.

14.12.5.4 Cabinet Installation Recommendations

Avoid empty cabinet or rack positions in rows. Replace removed cabinets or frames and fill any gaps in a row of cabinets with a substitute blanking panel of the same height as the cabinet or frames to either side to avoid recirculation of air between hot and cold aisles. For the same reason, cabinets and racks should be installed with no blank spaces between them. In the case of vacant cabinets and racks and where blank spaces exist in populated cabinets and racks, install blanking panels. Vertical cable managers can provide cable management and block recirculation of air between racks. Cabinets should be butted up against each other. Where possible, bayed cabinets should still share a side panel or include other means to seal the rear-to-front airflow path along the side of rack-mounted equipment.

Given a choice, where placing one edge of the cabinet creates unequal aisle sizes, the front aisle should be the larger one as it provides more working space for installation of equipment into cabinets and a greater area for providing cool air to cabinets.

In order to meet the requirement to restrict air passage through all openings outside the cold aisle on access floors, floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings taking into account anticipated growth.

Furthermore, consider using openings with gaskets or brush grommets to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency. See Figure 14-17 through Figure 14-20 for examples.

Ensure that all active devices are properly supported and securely mounted to the cabinet to prevent equipment damage from improper installation.

Plan equipment, power strip, cable manager, and cabling layouts in cabinets before making a major purchase. Either create detailed drawings or preferably create a mock-up to ensure that:

- All equipment and cable managers fit properly
- There is adequate space and access to power strips
- There is adequate access to cabinet floor and top openings
- There is adequate space for cable management
- Equipment can properly slide in and out as required
- Equipment intakes and exhausts are not blocked by cabling, cable management, or cabinet structure so that air can flow freely within the rack and to exit out the hot side
- Cabinets, racks, and vertical management do not have large openings for recirculation of air from hot to cold aisles

Temporarily remove any doors and panels that may interfere with the cabinet installation.

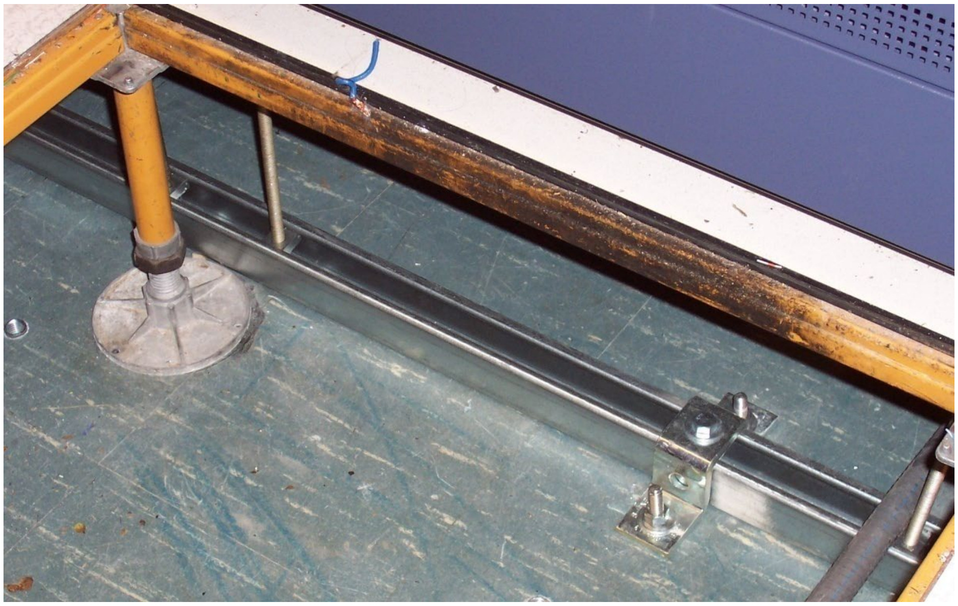
On solid or slab floors, cabinets should be set in place and leveled throughout the line-up. Most cabinets are equipped with leveling feet. If leveling feet are not provided, consult manufacturer for proper shimming hardware.

On access floors, cabinets and racks should be secured to the concrete subfloor. If cabinets in the line-up are to be ganged, attachment hardware should be installed before anchors are installed. Install anchors per manufacturer's specification, making sure all shimming hardware is properly located. (See Figure 14-21).

In seismically active areas, it is recommended that the design of the cabinets and their installation be reviewed by a licensed structural engineer as many jurisdictions require a seismic certification report signed by a professional engineer.

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means). The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable.

Floor tile panels should have correctly sized and placed cutouts for the cabinet or equipment placed over them. The cutout should be under the cabinet/equipment cord opening and properly sized for the quantity and type of cables to be routed through the opening.



NOTE: Threaded rods are uncovered for illustration purposes; exposed threads should be covered.

Figure 14-21
Illustration of Securing Cabinets and Racks on an Access Floor to a Concrete Slab Using Threaded Rod and Steel Channel

14.12.6 Thermal Management in Cabinets

14.12.6.1 Recommendations

There is no one thermal management configuration that works best in every instance. Each may be optimal, depending upon different factors unique to the customer, application, and environment. Serious consideration should be given to understanding the upfront installed costs as well as ongoing operation cost from an energy efficiency and maintenance perspective. At a minimum, equipment should be installed in cabinets with the air intake oriented toward the front of the cabinet or rack and the air exhaust oriented toward the rear of the cabinet or rack, when possible, with the cabinet rows oriented in a "hot aisle/cold aisle" configuration—rears of cabinets facing each other and fronts of cabinets facing each other (See Figure 14-22).

Use of any supplementary cooling mechanisms on a cabinet must take into consideration its effect on the overall fluid dynamics of the air space and how other equipment will be affected.

Considerations of supplemental cooling systems need to include criticality and required levels of redundant backup (see Section 10.7.4. for details).

Cabinets with good passive air management systems in well-designed rooms remove concerns about single points of failure and can support heat loads of twenty kW and higher.

Cabinet fans for cabinets specially designed to handle high heat loads should be on UPS power and have redundant power cords or be on transfer switches to ensure continuous operation.

Cabinet fans should be on separate circuits from the equipment in the cabinet as fans are susceptible to ground faults.

The perimeter of the equipment mounting area is also a path for cold air bypass or hot air recirculation and should be blocked accordingly.

Careful planning is needed for capacities, heat loads, and redundancies required for desired availability and reliability. See Appendix B for further information on availability and reliability.

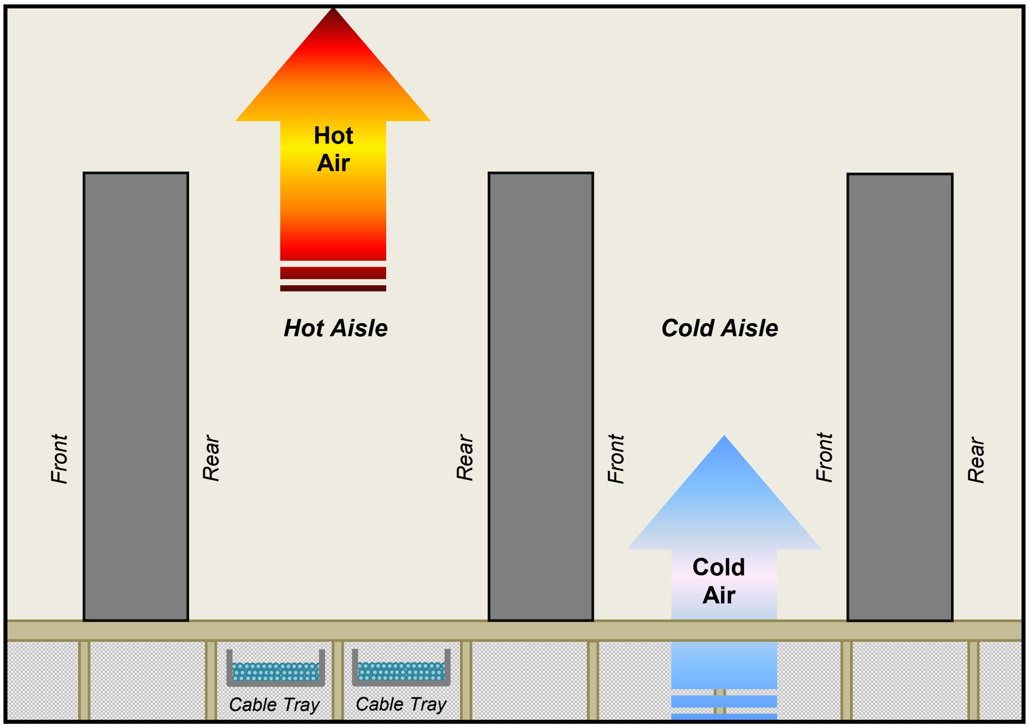


Figure 14-22
Hot Aisle/Cold Aisle Cabinet Layout

14.12.6.2 Additional Information

Specify/purchase the highest quality racks and rack components the budget will allow. They hold up better in the long run through numerous changes.

Over tightening mounting screws will strip out threads in the racks (especially the poorer quality racks). Minimum torque setting on drill/driver is usually sufficient to secure anything in the rack. Refer to manufacturer's specifications for recommended hardware. Specify toolless construction wherever possible.

Cabinets produced by ITE OEMs may provide insufficient space to meet operational cable management requirements or cabling architecture when used for equipment other than originally intended or specified.

Current generation servers will operate with, and high availability environments require, multiple network connections. For example, a single server might typically have two production LAN connections, one or two clustering or virtualization LAN connections, an out-of-band software management LAN connection, a hardware lights out management (LOM) LAN connection, and two (primary and secondary) SAN network connections. Additionally, there may be redundant power supplies requiring two or more power cords per server. Therefore, in a server cabinet that houses twelve servers, the application could potentially encounter seventy-two (72) balanced twisted-pair equipment cords, twenty-four (24) duplex optical fiber equipment cords, and twenty-four (24) power cords for a total of one hundred twenty (120) individual cords, plus any KVM cabling.

Some line-ups require additional bracing to meet customer specifications or local codes. All bracing should be installed before cabinet doors or panels are installed and before the cabinet is populated. Required bracing may be based on cabinet style, equipment, and location. Bracing should be installed as a system to ensure proper fit and support. Install all parts hand tight and then tighten fasteners in a series to prevent stress on cabinet line-up.

Changes in floor tile cuts can be disruptive and time-consuming. To mitigate the change of reworks, floor tile panel cuts should be carefully planned, taking into account current and anticipated power and data cabling requirements as well as all necessary route diversity considerations.

Cabinet roof fans and fan trays generally offer little benefit and can actually be counterproductive, creating hot spots within a cabinet, particularly when used in conjunction with high airflow mesh front doors. Additionally, these fans may disrupt the proper function of hot and cold aisles. Caution should be applied to any use of cabinet fans to assure they will enhance rather than disrupt the proper functioning of hot and cold aisle separation. Rear door fans can be used as long as the actual delivered fan capacity is not less than the cumulative throughput of the equipment fans in the cabinet.

In suboptimized spaces, hot aisle containment or cold aisle containment may compensate for otherwise inadequate cooling by isolating source air from return air.

NOTE: As an installation tip, make a floor cut template on cardboard or directly on the floor tile from the access opening in the cabinet being placed.

14.13 Telecommunications Cabling, Pathways, and Spaces Administration

14.13.1 General

14.13.1.1 Introduction

Documentation, labeling, and administration of data center components are critical to proper operation and maintenance of a data center. Administration systems may be manually operated or utilize an automated system. However, physical labeling of all items should be undertaken irrespective of the system being implemented. The following guidelines and recommendations contained in this section are for the administration of a data center.

14.13.1.2 Requirements

Data centers shall be provided with an identification/administration system following the hierarchical requirements of an approved standard (e.g., ANSI/TIA-606-C, ISO/IEC TR 14763-2-1). The administration system must include identification and labeling requirements for:

- Campus or site
- Building
- Indoor telecommunications space
- Outdoor telecommunications spaces such as maintenances holes, handholes, joining chambers, pedestals, or outdoor cabinets
- Cabinet, frame, or wall segment
- Closure
- Port or termination on closure
- Backbone cable or cable between cabinets, frames, or wall sections
- Pair/port within backbone cable or cable within distributor, telecommunications room, equipment room, or computer room
- Splice - pair in splice on backbone cable or horizontal cable to outlets mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- CP port in ZDA or LDP
- Horizontal cable to telecommunications outlet not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- Telecommunications outlets not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- Splice - pair in splice on horizontal link to telecommunications outlets not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- Patch cord or jumper
- Outdoor pathway system
- Campus or building entrance pathway system
- Pathway system within a building
- Firestop in building pathway system
- Data center pathway system
- Bonding conductor for cabinet or frame
- Cabinets, racks, and frames
- Patch panels
- Patch panel and equipment outlet ports
- Cables, patch cords and equipment cords

14.13.1.3 Recommendations

Supplies for labeling and administration should be part of an inventory system. Cable label makers, labels, markers, spare batteries, and other supplies are often overlooked and should be readily available. This will help ensure proper marking. Consider color-coding of balanced twisted pair patch cords either on the jacket label based on function. Optical fiber cord jacket, optical fiber connectors, and optical fiber adapters colors should follow the recommendations of ANSI/TIA-568.3-D. Optical fiber cords may be color-coded by function by color using the label or font color.

14.13.2 Identification Conventions for Data Center Components

14.13.2.1 Spaces

14.13.2.1.1 Introduction

Spaces in the data center need to be identified and recorded to ensure operational efficiencies. Space identification is traditionally user specified. Additionally, architectural concerns could determine the labeling methods for spaces. Data center spaces are also defined in the various cabling standards.

14.13.2.1.2 Requirements

All spaces shall have a unique identifier and be labeled.

14.13.2.1.3 Recommendations

A space summary report should be available listing all spaces, including their types and locations.

A space with access floor should track the computer room grid. Most computer rooms will use at least two letters and two numeric digits to identify every 600 mm × 600 mm (24 in × 24 in) floor tile. In such computer rooms, the letters will be AA, AB, AC, …, AZ, BA, BB, BC, and so on (See Figure 14-23). For example, a floor tile located in the seventh row (AG) in the twelfth (12) column should be called AG12.

If the computer room is comprised of multiple spaces, the space identifier should be incorporated at the beginning of the floor space identifiers. Therefore, the cabinet at AG05 in room 4DC should be named 4DC-AG05.

In general, space identifiers should be formatted as fs-XXYY, where:

- fs is the optional space identifier.
- XX is floor tile grid row.
- YY is floor tile grid column.

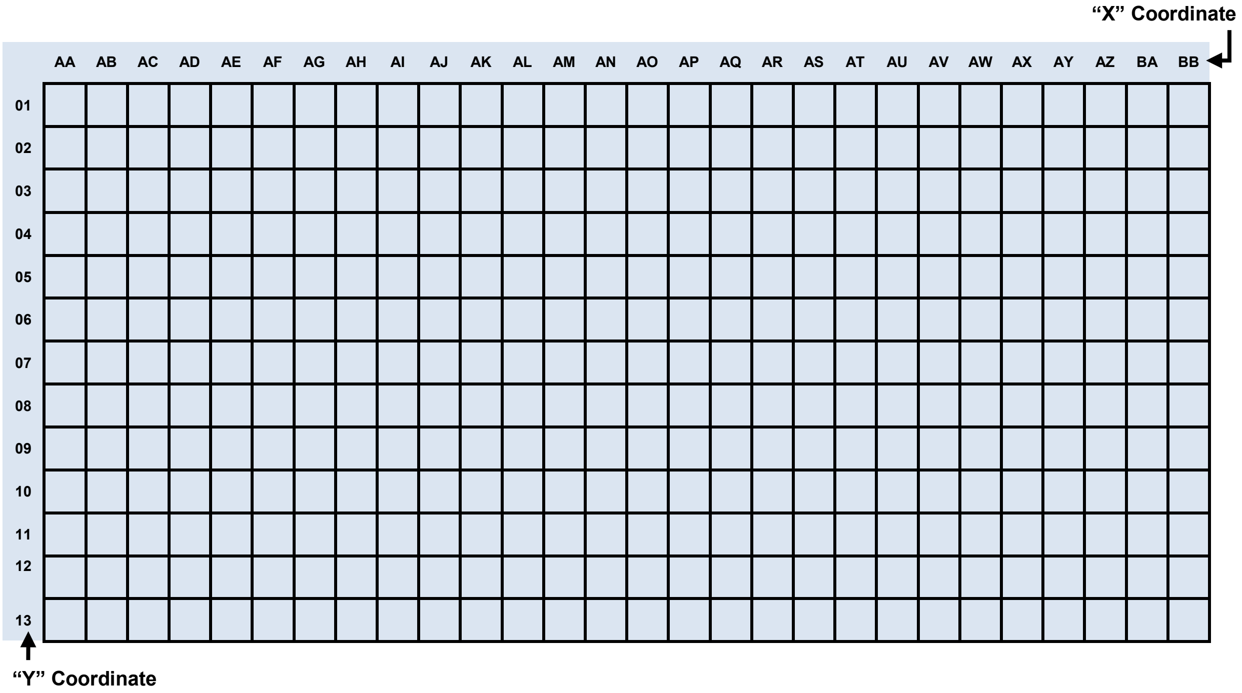

"X" Coordinate
AA AB AC AD AE AF AG AH AI AJ AK AL AM AN AO AP AQ AR AS AT AU AV AW AX AY AZ BA BB
01
02
03
04
05
06
07
08
09
10
11
12
13
"Y" Coordinate

Figure 14-23
Room Grid Coordinate System Example

If the grid coordinate system is used for cabinet identifiers, consider installing signs on the walls corresponding to the grid coordinate system to simply locating cabinets in the computer room.
If the row/cabinet sequence numbers are used for cabinet identifiers, then consider labeling the side panels at the end of the rows with the row IDs.

14.13.2.2 Cabinets and Racks

14.13.2.2.1 Requirements

In facilities with 600 mm × 600 mm (24 in × 24 in) floor tiles, many cabinets and racks will extend over more than one floor tile. In these facilities, each cabinet and rack shall be identified with a tile identifier, using the same location on every cabinet or rack to determine the grid location. This location shall be some point on the front of the cabinet or rack. The location may be the left front corner, right front corner, or front center as long as the same location is used for all cabinets and racks in the facility.

In rooms without a grid identifier, cabinets and racks may be identified by their row number and location within the row. The quantity of characters used for each identifier shall be the same throughout the facility. The numbering shall begin at the same end of each row in the facility, selecting an end that is not at risk of future cabinet or rack growth, such as adjacent to a wall.

The location identifier shall be labeled in plain view on the front and rear of each cabinet and rack. Preferred locations for labels are the top and bottom on a permanent part of the cabinet or rack. Text on the labels shall be upper case and large enough to be easily read from a standing eye-level vantage point near the cabinet or rack. The label text shall be machine printed, and the label color shall contrast with the surface upon which it is affixed (e.g., white on a dark surface, black on a light surface).

14.13.2.3 Pathways

14.13.2.3.1 Introduction

Pathways may include conduit, cable tray systems, or other elements in the data center used to support and convey telecommunications cabling.

14.13.2.3.2 Requirements

All entrance pathways and pathways between rooms shall have a unique identifier per applicable standards (e.g., ANSI/TIA-606-C, ISO/IEC TR 14763-2-1).

All entrance pathways and pathways between rooms shall be labeled at all endpoints.

14.13.2.3.3 Recommendations

Additional labeling should be provided at:

- Intermediate points such as pull boxes and joined cable tray segments
- Regularly spaced intervals in closed loop pathways such as cable tray rings
- Partitioned pathways such as partition duct or innerduct. Unique identifiers shall be provided for each segment

A pathways summary report should be available listing all pathways, including their types, origins, destinations, total capacities, and present fill conditions.

14.13.2.4 Active Equipment

14.13.2.4.1 Introduction

Active equipment includes switches, routers, hubs, firewalls, multiplexers, servers, external storage devices, and other equipment designed to support data center LANs, WANs, SANs, and computing infrastructure.

14.13.2.4.2 Requirements

All pieces of installed equipment shall have a unique identifier.

All active equipment shall be labeled on the front and back with their identifiers. These labels shall be machine generated and legible.

14.13.2.4.3 Recommendations

An active equipment summary report should be available listing all pieces of equipment, including their types, uses, location, connected backbone and horizontal cabling port/pair/strand assignments on termination hardware and other connected equipment.

14.13.2.4.4 Additional Information

A two-digit counter or rack unit location can delineate the active equipment in each cabinet, rack, or frame. The equipment is typically designated by the RU at the top of the active equipment. Rack unit numbering should start from the bottom of the usable space in the cabinet or rack.

14.13.2.5 Bonding and Grounding System

14.13.2.5.1 Requirements

The bonding and grounding system and all components of the bonding and grounding system shall be labeled and identified on all "as-built" documentation in accordance with applicable cabling standards being followed and, if applicable, with manufacturer-recommended labeling systems.

14.13.2.5.2 Recommendations

Bonding and grounding system records should:

- Include next scheduled maintenance information. At a minimum, maintenance should include an inspection and test all bonding and ground connections.
- All bonding and grounding system records should be retained and available for review. This should include the maintenance schedule.

14.13.2.6 Firestopping

14.13.2.6.1 Recommendations

A firestopping system should be labeled and should include digital pictures. Firestop submittals, including manufacturer cutsheets and installation instructions, should be retained and available for review.

Fire detection and suppression systems should be identified on all as-built documents.

14.13.2.7 Alternate Power Systems

14.13.2.7.1 Recommendations

The data center may contain various emergency power systems necessary for redundancy. These should be identified and be labeled.

All components of the alternate power system shall be labeled and identified on all as-built documentation.

All alternate power system records should be retained and available for review. This should include the maintenance schedule.

14.13.3 Records

14.13.3.1 General Recommendations

A cabinet, rack and frame summary report should be available listing all racks, cabinets, and frames, including their types, locations, sizes, capacities, and current usage status.

A cabling summary report should be available listing all cabling, including their types, uses, pair/strand/port counts, sources, destinations, current pair/strand/port usage, backbone and horizontal cabling port/pair/strand assignments on termination hardware, patching/cross-connection assignments, connected equipment, and unterminated or damaged pairs/strands.

It is also recommended that the database source for the cabling reports be able to provide end-to-end circuit trace connectivity reports from either end or from any intermediate point along the circuit.

A cross-connect summary report should be available listing all cross-connects, including their types, uses, pair/strand/port counts, sources, destinations, current pair/strand/port usage, backbone and horizontal cabling port/pair/strand assignments on termination hardware, and connected equipment.

14.13.3.2 Electronic Documents

14.13.3.2.1 Recommendations

Specifications for electronic documentation for the data center should be defined during the design phase and may be contingent on the size and type of the data center.

- Base building—Provide drawings in AutoCAD or similar electronic format.
- Data center—Provide drawings in AutoCAD or similar electronic format.
- Data center utilities – Provide all test results for the data center utilities, including, but not limited to, power, HVAC, and fire detection and suppression systems, in electronic format. These files should be retained.

List continues on the next page

- Balanced twisted-pair and optical fiber cabling—Provide all balanced twisted-pair and optical fiber cabling schedules and test results in electronic format. The cabling schedule should include the “to-from” information that identifies the connection to each piece of equipment or corresponding connecting hardware. These files should be retained.
- Power cabling—Provide all power cabling schedules in electronic format. The power cabling schedule should include the “to-from” information that identifies the connection to each piece of equipment or corresponding connecting hardware. These files should be retained.
- Cabinet and rack elevations—Provide drawings identifying rack layout and equipment placement in AutoCAD or similar electronic format.
- Active equipment inventory—Provide inventory list of all active equipment in spreadsheets, database(s), drawings, or other approved electronic format.

14.13.3.3 Change Control

14.13.3.3.1 Introduction

Access and change control policies and procedures are important elements to consider during the design.

Administration of the data center components is integral to the access and change control policies.

14.13.3.3.2 Requirements

Change control procedures shall be posted and be part of the access requirements. Work shall only be performed after proper approvals.

Change control process shall identify the proper work in progress practices.

Change control process shall include trouble ticket procedures and identify the proper site access as part of the resolution.

Change control procedures shall identify and include all required safety practices.

14.13.4 Automated Infrastructure Management

14.13.4.1 Introduction

Automated infrastructure management features cabling records updating automatically upon changes of equipment cord or patch cord positions in a given Automated patching field. The system may be implemented with the addition of an analyzer or scanner able to monitor all the cabling connections within a given distributor or patching field and update the system database.

The automated infrastructure management system is composed of patch panels, patch cords, analyzers or scanners, additional cables for connections between analyzers or scanners and the patch panels, and management software usually installed in a dedicated server. Monitored patch panel ports are connected to the analyzer or scanner so that when an equipment cord or patch cord is removed or inserted, the system will detect it and update the software database. Therefore, the network administrator will have access to the up-to-date information about the cabling system at any time.

Automated infrastructure management systems may be implemented using two configurations:

- Interconnection
- Cross-connection

Interconnection configuration is implemented by using sensor strips installed on the Ethernet switch ports to provide them with a means for detection of equipment cord or patch cord connections. Figure 14-24 depicts the interconnection configuration.

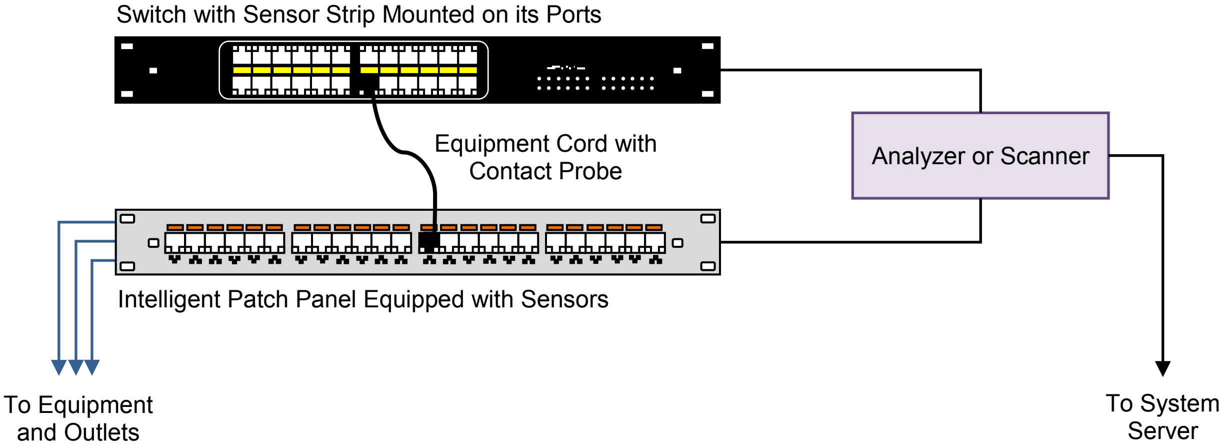

Switch with Sensor Strip Mounted on its Ports
Equipment Cord with Contact Probe
Analyzer or Scanner
Intelligent Patch Panel Equipped with Sensors
To Equipment and Outlets
To System Server

Figure 14-24
Automated Infrastructure Management Interconnection Configuration Example

Cross-connection configuration is implemented through a "mirror" patch panel between the Ethernet switch and the horizontal distribution. Switch ports are mirrored in the automated patch panel, so connections will be made between patch panel ports only and not between switch ports and patch panel ports. This configuration is especially suitable for systems that operate with sensors or micro-switches for detection of equipment cord or patch cord connections. Figure 14-25 depicts the cross-connection configuration.

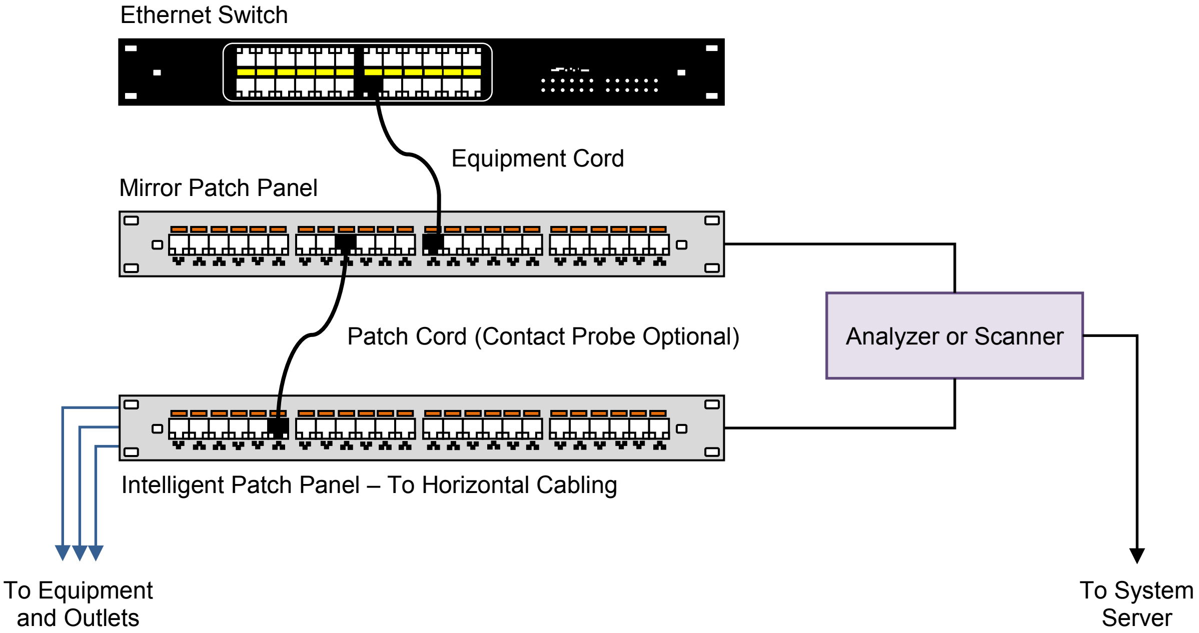


Figure 14-25
Automated Infrastructure Management Cross-Connection Configuration Example

14.13.4.2 Requirements

All automated infrastructure management (AIM) systems shall comply with applicable standards (e.g., ANSI/TIA-5048, ISO/IEC 18598, EN 50174-1).

14.13.4.3 Additional Information

The current existing technologies for the hardware of automated infrastructure are:

- Micro switches imbedded in the ports of the patch panels. They detect the connection of an equipment cord or patch cord.
- Physical contact between a sensor on the patch panel and an extra contact on the equipment cord or patch cord.
- RFID detection between a sensor on the patch panel and a tag fixed on the equipment cord or patch cord.

Some benefits of automated infrastructure management:

- Physical connections between switch ports and patch panel ports can be monitored in real-time.
- Equipment cord and patch cord connections are stored in a software database.
- Communication with network devices can be implemented through SNMP (Simple Network Management Protocol).

  If SNMP is implemented, several network management features can be implemented in the automated patching system, such as alarm configurations, messages through e-mail, in case of unauthorized access to the network and other actions according to prior configuration.
- Permits planning of work orders (moves, additions, and changes).

Some potential disadvantages of automated infrastructure management:

- Difficult or impossible to retrofit into an existing infrastructure
- Higher cost than an equivalent non-automated infrastructure
- May consume additional rack units at locations wherever patching is managed
- Depending on the product selected, manufacturer specific equipment cords or patch cords may be required

15 Information Technology

15.1 Network Infrastructure Reliability

15.1.1 Overview

The network architecture service layer is a critical system supporting the critical business applications. The network architecture must not only be designed to support all the applications and anticipated bandwidth requirements in a scalable manner to accommodate future growth in applications, hosts, and data storage, but also accommodate all these requirements with the level of redundancy that is in alignment with the business objectives. The level of redundancy must be maintained from the initial day-one requirements to the ultimate port counts and bandwidth requirements in a scalable manner.

The level of redundancy must also be aligned across the enterprise. Data centers implemented with single path networks on non-redundant chassis within the data center LAN (representing multiple single point of failure), while connecting to multiple redundant WAN service providers with redundant access circuits. This misalignment either results in excessive WAN service provider recurring costs not required for lower performance objectives or a higher than acceptable risk associated with single points of failure within a data center LAN with higher performance objectives, depending on the targeted overall data center class objective.

The network architecture service layer consists of:

- Internet: The internet network services layer ranges from single link internet access from one service provider to redundant internet access across two or more service providers.
- Wide Area Network (WAN): The WAN network services layer provides network connectivity from the data center to secondary data center(s), other corporate office locations, and possibly key remote partner or customer locations. Services range from a single link from a service provider to redundant circuits/networks from multiple service providers.
- Metropolitan Area Network (MAN): The MAN network services layer provides network connectivity from the data center to secondary data center(s), other corporate office locations, and possibly key remote partner or customer locations, all within a common metropolitan area. MAN services can be implemented using a service provider's network services, leasing dark fiber from vendors or customer-owned fiber optic outside plant distributed throughout the MAN. Services range from a single link to redundant circuits/networks from multiple service providers, leased dark fiber vendors, or customer-owned fiber optic outside plant.
- Local Area Network (LAN): The LAN network services layer consists of the network connectivity within the data center interconnecting the processing systems to the Internet, WAN, and MAN network services. LAN services range from single link connectivity throughout the LAN to redundant connections from the processing systems to the Internet, WAN, and MAN.
- Storage Area Network (SAN): The SAN network services layer consists of the network connectivity within the data center interconnecting the data storage systems to the processing systems and WAN and MAN network services for off-site replication. SAN services range from single link connectivity throughout the SAN to redundant connections from the data storage systems to the processing systems and to the WAN and MAN. For converged SAN/LAN systems, the level of redundancy must meet the minimum requirements of either the LAN or SAN network services.

NOTE: All redundant internet, WAN or MAN network services provisioned over a collapsed ring, common sheath, common pathway, or any other implementation resulting in common modes of failure between the redundant network services are considered "single link". An example is a ringed topology network implemented with full or partial collapsed rings.

For the network architecture reliability classes, the corresponding class designation is prefaced with an "N" to identify it represents the "Network" reliability criteria.

15.1.2 Network Infrastructure Availability Classes

15.1.2.1 Introduction

The following network architecture examples merely represent one example. Any network architecture that meets the intent of, and can validate the performance characteristics of, any network reliability Class would achieve that particular Class rating. While there are generally a few industry accepted, commonly applied redundant LAN/SAN network topologies that meet the higher levels of reliability Class, there are many WAN/MAN network topologies that can meet the higher levels of reliability Class.

Options exist such as redundant services across multiple access provider vendors or provisioned across redundant services from one access provider vendor. It is important that the data center designer validate that the redundant systems or services meet the performance characteristics defined by the network reliability Class. This would include validating logical and physical diversity from the data center throughout the WAN/MAN or to the Internet backbone, not simply to the nearest Central Office (CO).

15.1.2.2 Availability Class N0 and N1

Downtime will result from planned and unplanned events. Downtime of several days has minimum impact on the enterprise. Network services are single link from one service provider.

Table 15-1 provides tactics for Class N0 and N1, and Figure 15-1 shows an example of a Class N0 and N1 infrastructure.

Table 15-1 Tactics for Class N0 and N1

Internet:	Internet access from one service provider via single link.
WAN/MAN:	Single link connection from one service provider.
LAN/SAN:	Single link connections throughout network.

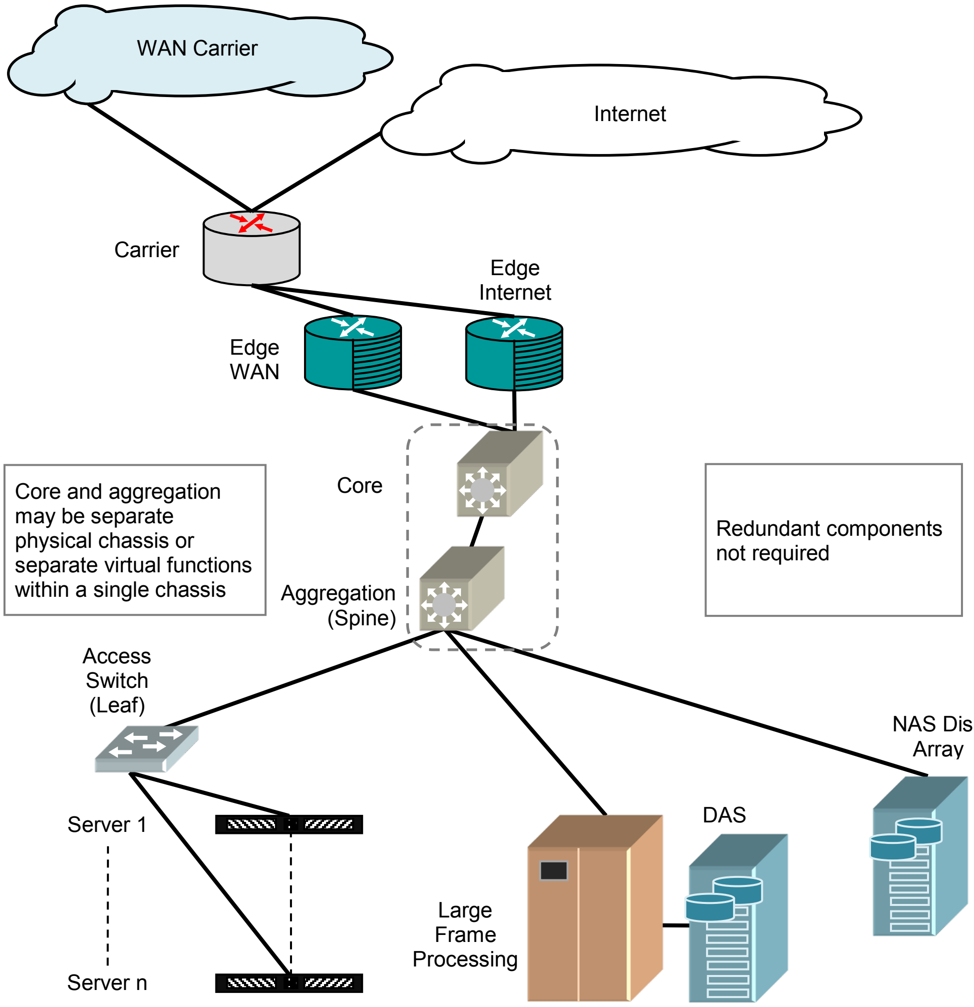


Figure 15-1
Class N0 and N1 Network Infrastructure

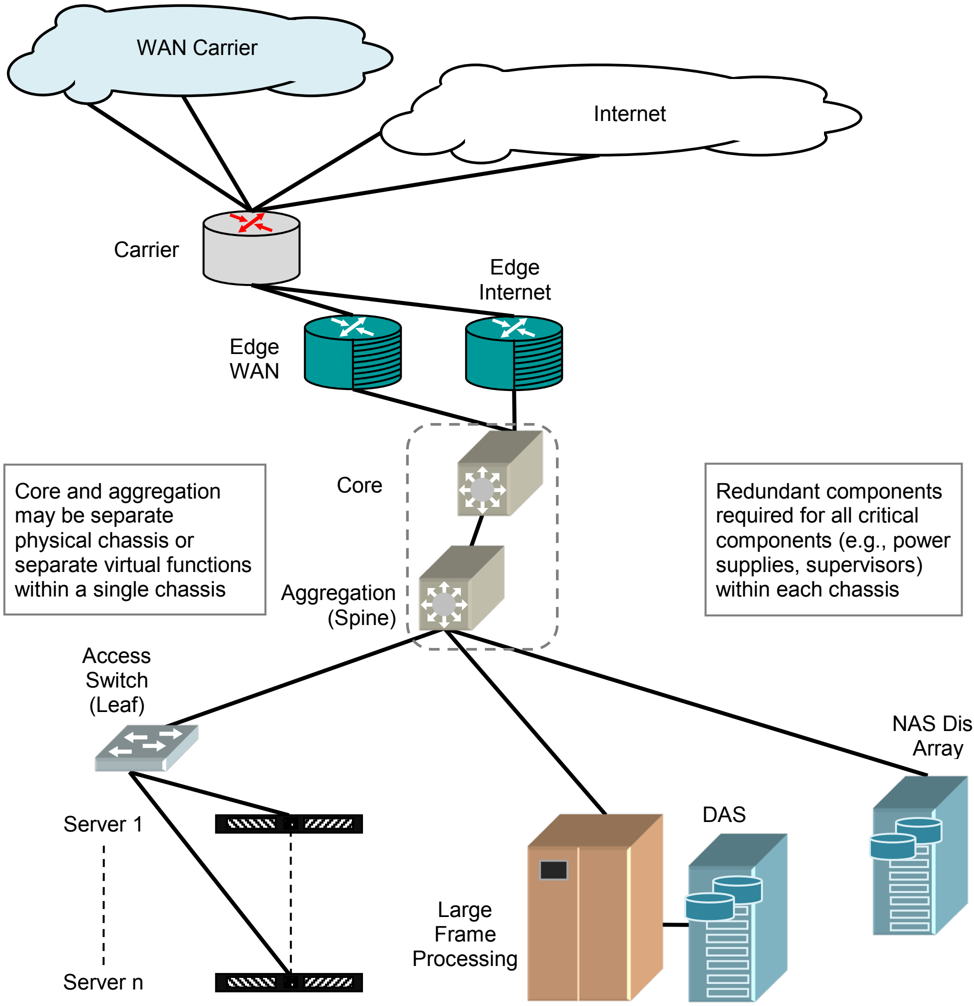
15.1.2.3 Availability Class N2

Class N2 provides a higher level of redundancy to reduce risk of downtime because of failure of critical components with low MTBF. Downtime may result from planned and unplanned events. Downtime of several hours or a couple of days has minimum impact on the enterprise. Network services are single link throughout the LAN/SAN but multi-path from core network to the WAN/MAN.

Table 15-2 provides tactics for Class N2, and Figure 15-2 shows an example of a Class N2 infrastructure.

Table 15-2 Tactics for Class N2

Internet:	Two Internet service providers each with a single local access circuit or a single Internet service provider with either a protected or redundant local access circuits.
WAN/MAN:	Non-redundant circuits from two service providers or a redundant or protected circuit from one service provider.
LAN/SAN:	Single link connections throughout network with redundant critical components such as power supplies, supervisors, or NIC teaming for failover.



Core and aggregation may be separate physical chassis or separate virtual functions within a single chassis

Redundant components required for all critical components (e.g., power supplies, supervisors) within each chassis

Figure 15-2
Class N2 Network Infrastructure

15.1.2.4 Availability Class N3

Additional redundancy is provided to reduce the risk of downtime due to human-error, natural disasters, planned maintenance, and repair activities. Network services are provided with redundant links throughout the network from the processing systems to all upstream network devices and network services.

Table 15-3 provides tactics for Class N3, and Figure 15-3 shows an example of a Class N3 infrastructure.

Table 15-3 Tactics for Class N3

Internet:	Two Internet service providers each with a single local access circuit or a single Internet service provider with either a protected or redundant local access circuits.
WAN/MAN:	Non-redundant circuits from more than two service providers or redundant or protected circuits from two service providers. Leased fiber or customer owned fiber optic outside plant can be implemented in lieu of network services from service provider.
LAN/SAN:	Redundant links and chassis in network from access switches to all upstream network devices; redundant components not required for links and chassis with redundant systems.

15.1.2.5 Availability Class N4

Redundancy is provided throughout the data center network and external network services to reduce the risk of downtime as a result of human-error, natural disasters, planned maintenance, and repair activities. Network services are provided with redundant links throughout the network from the processing systems to all upstream network devices and network services. Redundant critical components provided within critical links and systems.

Table 15-4 provides tactics for Class N4, and Figure 15-4 shows an example of a Class N4 infrastructure.

Table 15-4 Tactics for Class N4

Internet:	Two Internet service providers both with redundant or protected local access circuits.
WAN/MAN:	Multiple circuits from multiple service providers each utilizing redundant or protected local loops. Leased fiber or customer-owned fiber optic outside plant can be implemented in lieu of network services from service provider.
LAN/SAN:	Redundant links, components, and chassis in network from access switches to all upstream network devices.

In reality, there may be very little difference in cost between Class 3 and Class 4 Network architectures. Adding redundant components such as power supplies, supervisors, etc. to implement a Class 4 solution does not normally represent a significant cost increase. However, we are presenting an example of the minimum requirements to meet the performance characteristics of each given Class.

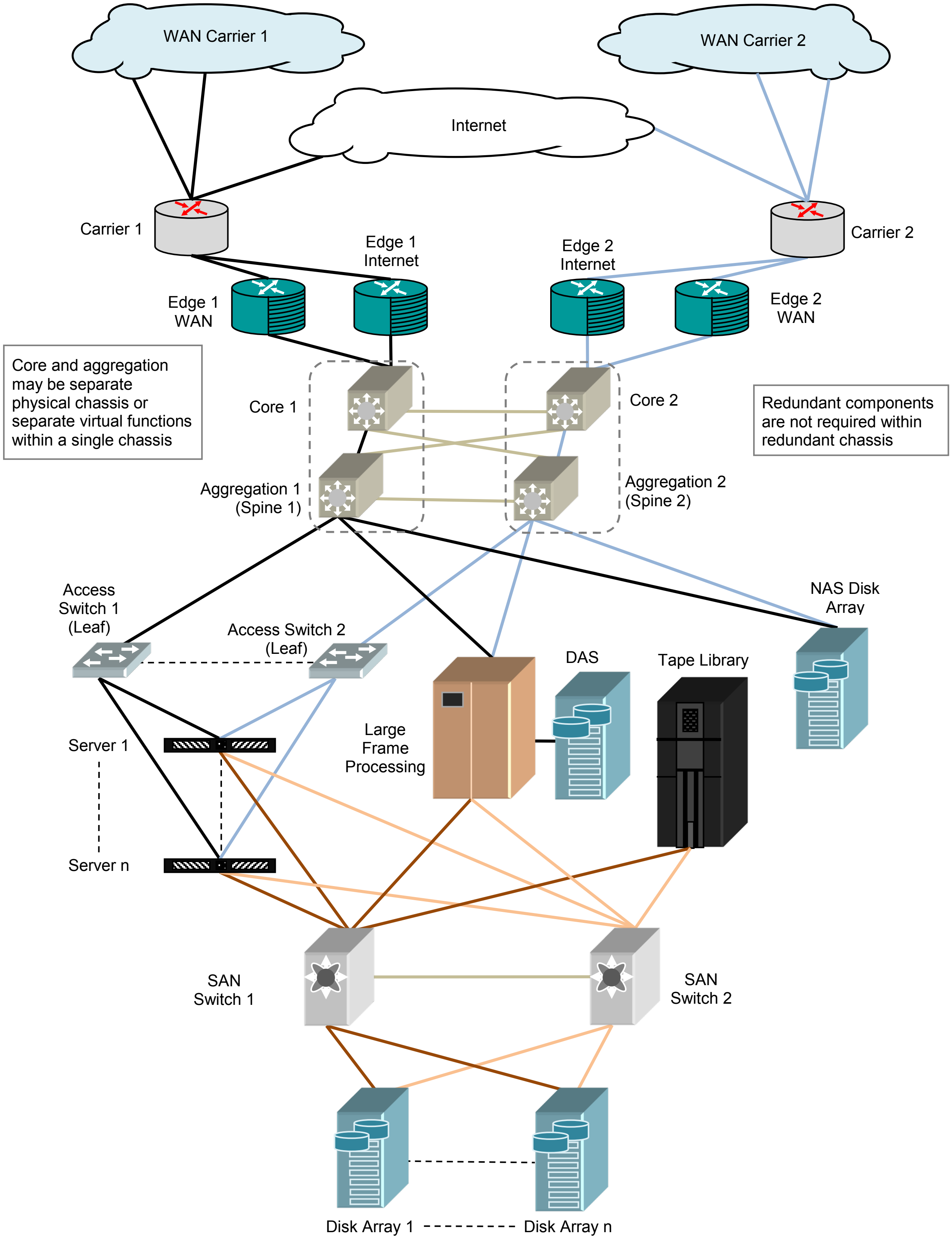


Figure 15-3
Class N3 Network Infrastructure

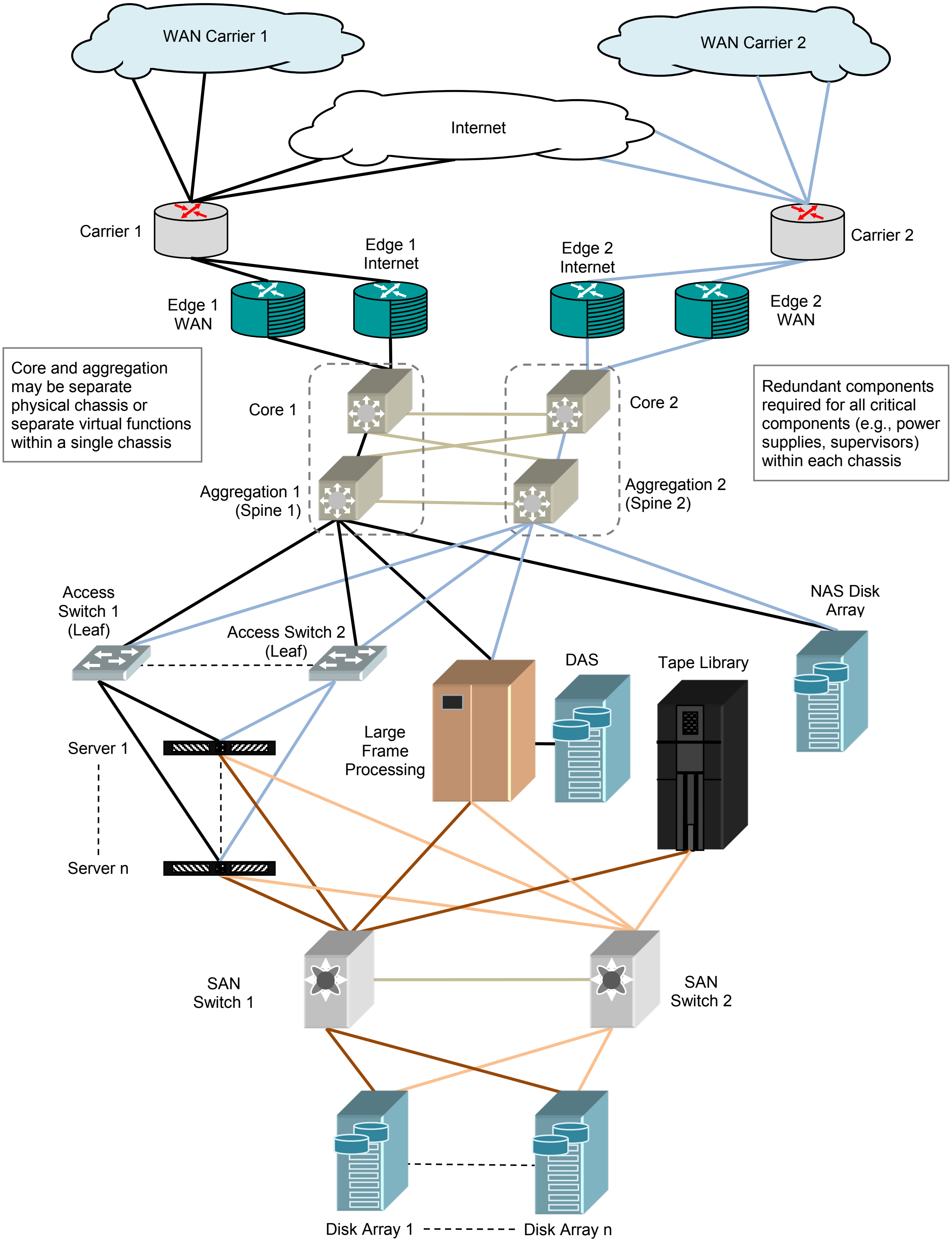


Figure 15-4
Class N4 Network Infrastructure

15.2 Computer Room Layout

15.2.1 Introduction

Computer room layout is affected by cable length restrictions for channel cabling, console cabling, LAN, SAN, and WAN cabling.

15.2.2 Equipment Configuration for Efficiency

The placement of specific ITE may affect initial computer room design decisions and data center design decision may affect final equipment placement. Factors that affect ITE placement in regards to computer room design include:

- Hot and cold aisles:
  - Minimize the reintroduction of hot air into rack and equipment cold air intake vents by using blanking panels.
  - Minimize the loss of the necessary static pressure under the access floor by means of dampers, brushes, or other means to seal cable cutouts and other openings in access floor tiles.
- Dedicated application rows
- Dedicated equipment type areas:
  - The concept of rows containing the same type equipment is a best practice method for both connectivity and airflow. From a connectivity perspective, some equipment is inherently fiber-connected, some copper connected, and some equipment uses proprietary cabling and share proprietary peripherals. By aligning same type equipment, the designer may be able to limit the use of proprietary cabling in cable pathways.
  - From an airflow perspective, having the same type of equipment cabinets or racks in rows helps keep a consistent airflow around equipment, allows for ease of hot/cold aisle design, and better prepares the computer room for portable cooling if necessary.
  - Consider separate areas of the computer room for rack-mounted and floor-standing systems to simplify cabling and the management of cabinets and racks.
  - Develop a small number of standard cabinet and rack cabling configurations for the computer room to simplify cable installation and administration.
- Aisles and walkways sizing
- Cabinet portability
- HVAC maintenance
- Accessibility and emergency egress—refer to Section 7

15.2.3 Connectivity Panel Distribution

15.2.3.1 Introduction

Refer to the most recent version of the relevant standards and reference manuals (e.g., ANSI/TIA-942-B, ISO/IEC 11801-5) for information on standards-based cabling distance limitations:

- Copper and fiber panel distribution
- Dedicated network connectivity rack area
- Distributed connectivity racks:
  - Standards-based rack
  - Standards-based cabinet
  - Underfloor
- Dedicated panels for each equipment cabinet or storage device

15.2.3.2 Recommendations

Figure 15-5 is a representation of simple connection topography for a data center. The connections shown can be copper or optical fiber so long as standards are not violated. Points to remember:

- Stay within recommended lengths.
- Check the AHJ on plenum issues for computer rooms.
- If running above the floor, watch for distance limitations from fire suppression elements (check with AHJ).
- If running under the floor, stay under aisle ways and do not run media under static equipment.
- Keep all runs at 90° turns (not violating bend radius); do not run media on an angle across the room.
- Map out all pathways and provide updated copies to computer room managers.
- If using underfloor cable tray, check with the floor and cable tray manufacturer for best practices regarding stanchion attachment.

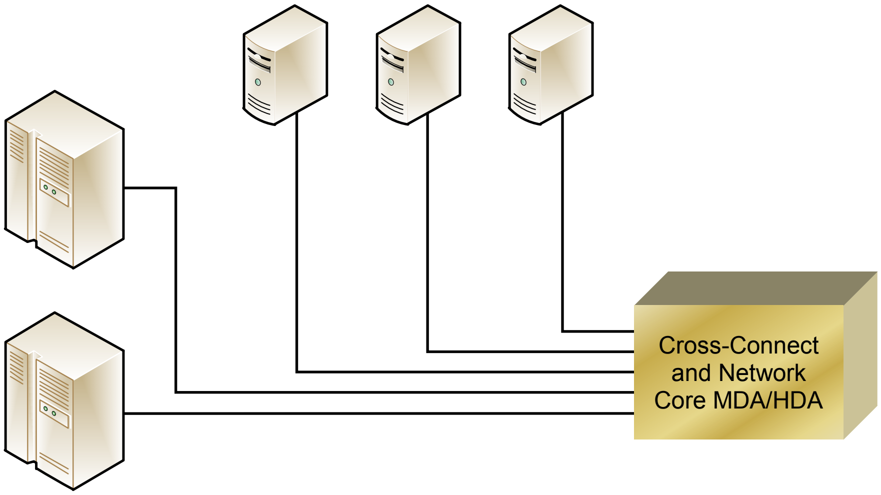


Figure 15-5
Simple Connection Topology

Figure 15-6 shows the basic representation of zone distribution. A zone distribution area can be housed above the floor in an equipment rack or below the floor in an access box. Each method has both advantages and disadvantages. When housed above floor, the connections are easier to access for connection and maintenance. However, the above floor methods use floor space that would otherwise be available for equipment. Below floor methods provide better security and maximize above floor space. However, installing zone boxes under the floor requires proper planning. The network team and the data center management need to agree on long-term commitments regarding placement of the remote distribution units as moving them is difficult in terms of the organization allowing for the necessary downtime. In addition, data center space planners need to understand that equipment cannot be placed on top of underfloor zone distribution areas.

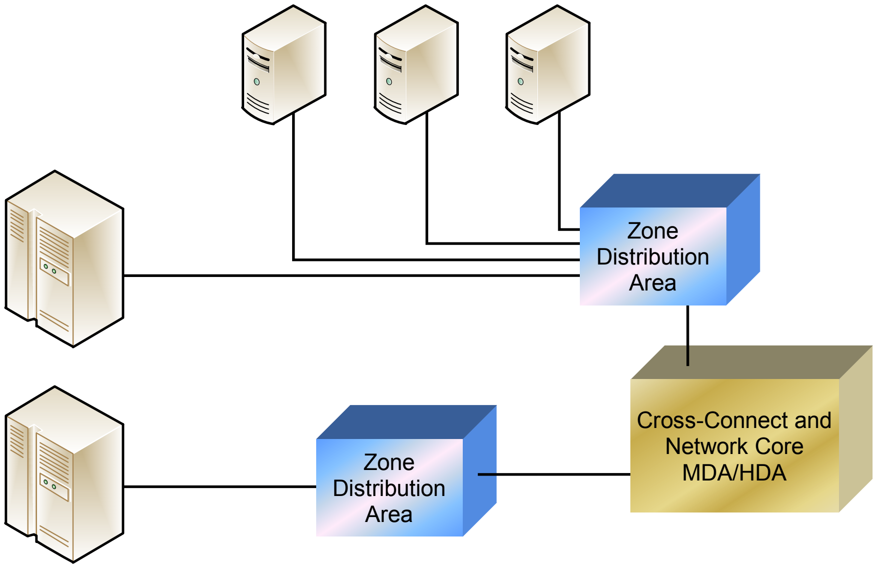


Figure 15-6
Sample Zone Distribution Topology

Figure 15-7 represents a redundant topology using redundant zone distribution areas. Notice that two totally separate pathways are used to keep maximum separation of the cabling from each ZDA.

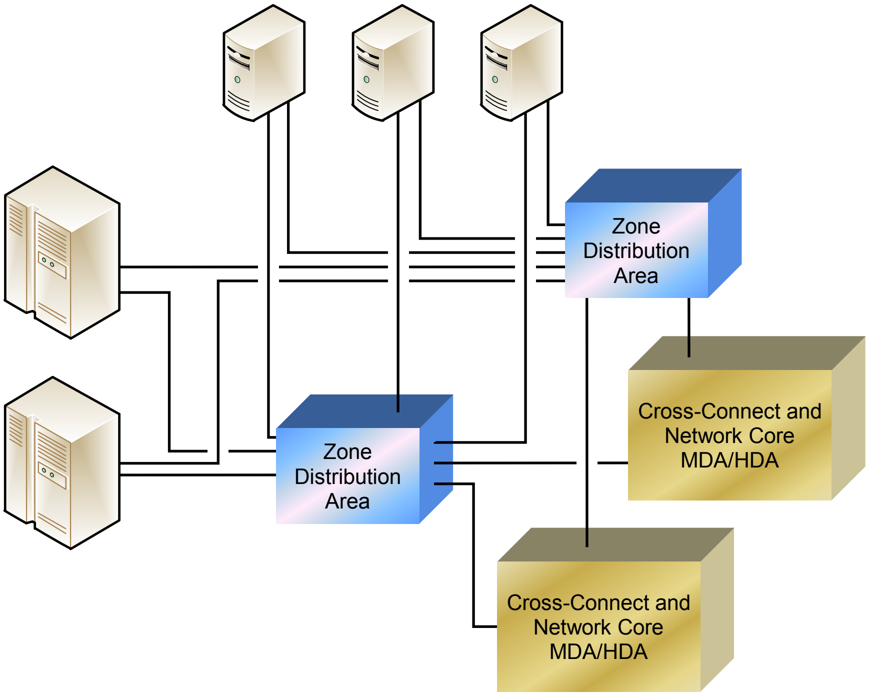


Figure 15-7
Sample Redundant Topology

15.2.4 Switch Placement

15.2.4.1 Locations

The topologies within Section 15.2.3.2 support a variety of strategies for the placement of switches to support network architecture. The desired physical placement of switches may affect decisions concerning a chosen topology and the required cabling and supporting infrastructure. Three common physical location strategies for switches are:

- Centralized
- End-of-row (also referred to as row-based or in-row)
- Top-of-rack

15.2.4.1.1 Centralized

A centralized strategy (see Figure 15-8) places all of the switches into a defined area of the computer room. The cabling infrastructure links all server and storage equipment to the centralized switches. A centralized topology typically requires the most cabling but provides a central location for all switch connections and typically requires fewer switches than other topologies.

15.2.4.1.2 End-of-Row

An end-of-row strategy utilizes two levels of switches as shown in Figure 15-9. The server and storage devices in each row are linked to one or more switches that are placed in a rack or cabinet at the end of the row. All of these end-row switches are then connected to one or more centralized switches to enable communications between all devices in the CR. With this strategy, the rack of cabinet in the row containing the switches can be placed anywhere in the row, providing flexibility in determining cable lengths, cable management and cable routing for both cabling in the cabinet row and to the location of other switches.

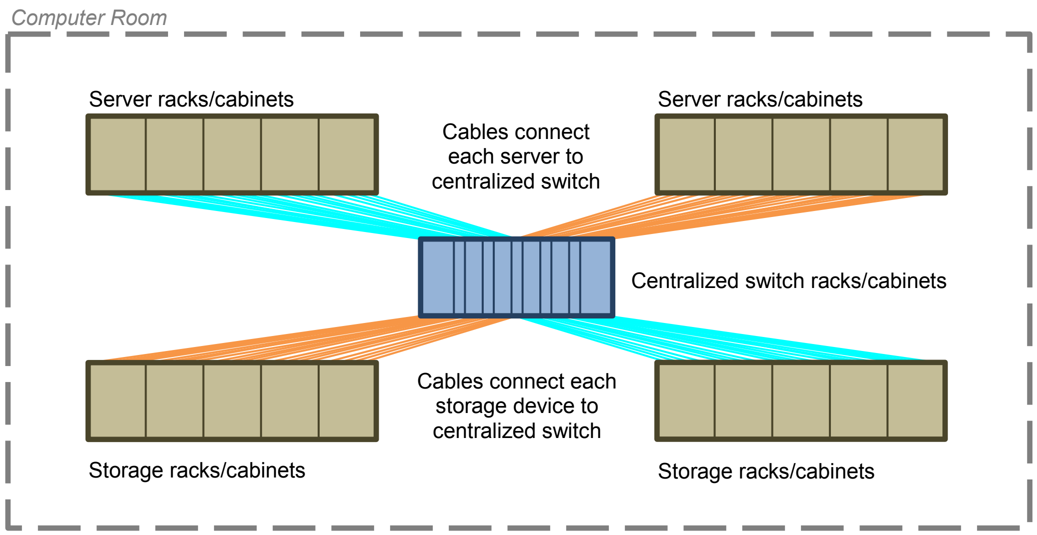

Computer Room
Server racks/cabinets
Cables connect each server to centralized switch
Server racks/cabinets
Centralized switch racks/cabinets
Storage racks/cabinets
Cables connect each storage device to centralized switch
Storage racks/cabinets

Figure 15-8
Centralized Switch Schematic

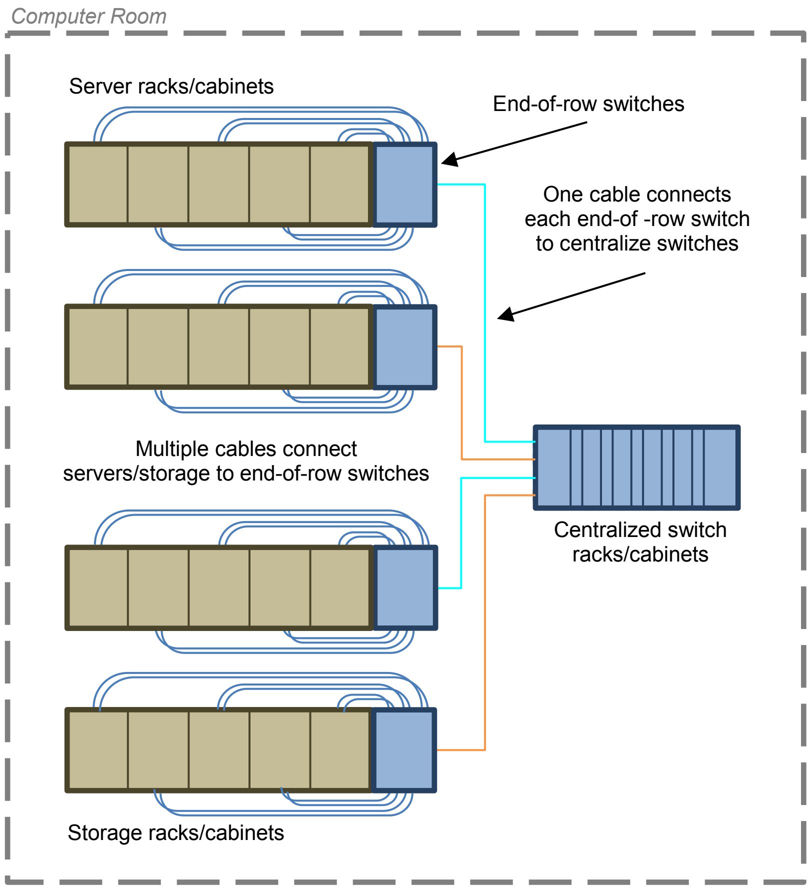

Computer Room
Server racks/cabinets
End-of-row switches
One cable connects each end-of -row switch to centralize switches
Multiple cables connect servers/storage to end-of-row switches
Centralized switch racks/cabinets
Storage racks/cabinets

Figure 15-9
End-of-Row Switch Schematic

An end-of-row strategy uses less overall cabling than the centralized strategy since server and storage devices are located closer to the connecting switch, and only a few cables are required to connect the "end-of-row" switch to a switch in a centralized location. However, the number of switches required increases and the management of switches is no longer possible from one defined area.

15.2.4.1.3 Top-of-Rack

A top-of-rack strategy provides a switch within every rack or cabinet containing servers and storage devices. Each of these switches is then connected to one or more centralized switches to enable communications between all devices in the computer room, as shown in Figure 15-10.

A top-of-rack strategy typically the least amount of cabling as cabling for servers and storage devices to the switch is limited to the vertical distance of the cabinet or rack, with only a few cables routing between the cabinet to the centralized areas. However, switches must be installed and managed in every rack or cabinet in the computer room.

15.2.4.2 Fabrics

How a data center owner or operator plans to manage the total number of connections, how the traffic is flowing, and the most efficient way to connect and utilize computing, networking, and application may affect the location strategy of switches. Layouts of how connections are made in a matrix of switches and servers are commonly referred to as "fabrics", examples of which include:

- Fat-tree / leaf and spine
- Full mesh
- Interconnected mesh
- Virtual switch

Some fabrics, such as fat-tree, may allow the use of all physical location strategies for switches. Others may utilize a limited set to optimize connection, equipment, and other considerations.

15.2.5 Material Storage

The planner should account for enough storage for emergency parts and equipment to minimally maintain the data center in an event. Items, such as tape drives, hot swappable devices, patch cords and test equipment, could be stored in the following areas:

- Network operations center
- Computer room
- In row
- Off-site or out of room staging area

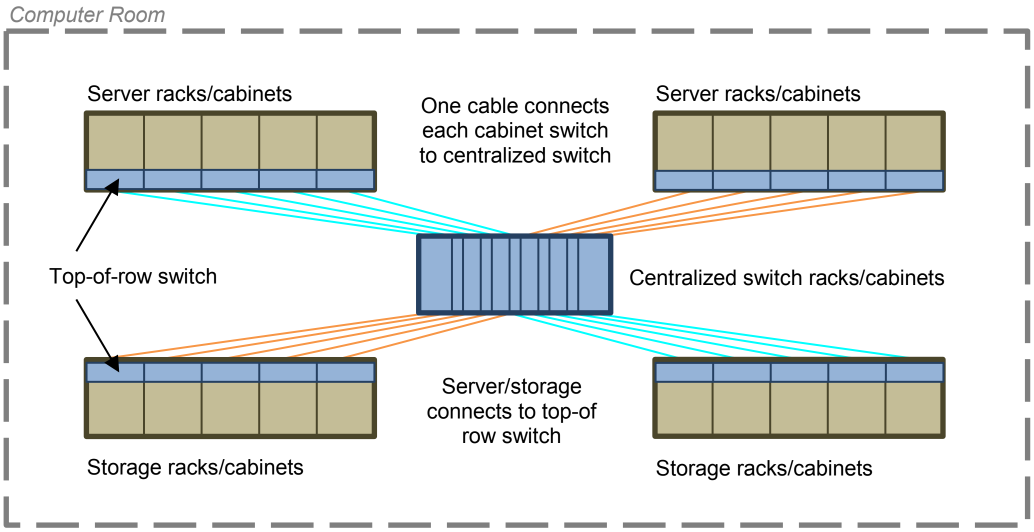

Computer Room
Server racks/cabinets
One cable connects each cabinet switch to centralized switch
Server racks/cabinets
Top-of-row switch
Centralized switch racks/cabinets
Server/storage connects to top-of row switch
Storage racks/cabinets
Storage racks/cabinets

Figure 15-10
Top-of-Rack Switch Schematic

15.3 Operations Center

15.3.1 Monitoring of Building Systems

15.3.1.1 Introduction

Refer to Section 10 and Section 13 for coordination. In general, monitoring systems should be available within the operations center. For more information about the monitoring of security cameras and access control devices, refer to Section 12.

15.3.2 Location

15.3.2.1 Recommendations

System consoles should be networked over private IP address space and accessible from the operations center, so operations personnel do not have to be in the computer room except in cases when human intervention is necessary.

The operations center should be located adjacent to the computer room with a viewing window if possible to provide visual communications.

The center should be equipped with large screen displays for system/network tools (e.g., power consumption, computer room humidity, temperature).

15.3.3 Channel and Console Cabling

15.3.3.1 Introduction

System consoles should be networked over private IP address space and accessible from the operations center. Providing this type of architecture enables a ‘lights-out’ operation in that personnel do not need to be in the computer room, except when human intervention is necessary.

15.3.3.2 Mainframe Channel Cabling

15.3.3.2.1 FICON

Fiber Connection (FICON) is a high-performance protocol. FICON channels enable 100 megabits per second of bidirectional link rates at distances up to 20 km over optical fiber cables. In addition, an I/O interface for mainframes supports the characteristics of existing and evolving higher speed access and storage devices.

In summary, FICON products—from IBM—use a mapping layer that is based on the existing ANSI standard, Fibre Channel-Physical and Signaling Interface (FC-PH). FC-PH specifies the physical signaling, cabling, and transmission speeds for Fibre Channel.

Each FICON channel is capable of supporting more than 4,000 I/O operations per second, which allows each channel to support the same capacity as up to eight Enterprise Systems Connection (ESCON) channels.

Disaster recovery functions, such as tape vaulting, remote disk copy and geographically dispersed parallel Sysplex (which are multiple mainframes strapped together as a single unit) benefit from the large distance supported by FICON channels. Although direct links between FICON devices of 10 kilometers are supported, 20-kilometer links are possible under certain conditions. The FICON protocol also permits additional end-to-end error checking above that provided by the FC-PH transport.

FICON is also designed to support a mixed workload. Small data transfers, typical for transactions, do not have to wait for large data transfers to complete.

Instead, they are multiplexed on the link with the long running operations. This helps to simplify configurations and removes one of the inhibitors to having a single database for transaction processing and business intelligence workloads.

15.3.3.2.2 ESCON

Enterprise System Connection (ESCON) is an IBM optical fiber channel connection technology that provides 17 megabytes per second of throughput. ESCON provides direct channel-to-channel connections between mainframe systems and peripherals over optical fiber links at distances up to 60 kilometers (36 miles). It also provides a way for communication controllers and other devices to share a single channel to a mainframe.

Compared to the copper-based parallel bus and tag channels, ESCON provides greater speeds and uses a serial interface. An ESCON Director is a hub-and-spoke coupling device that provides 8-16 ports (Model 1) or 28-60 ports (Model 2).

15.3.3.2.3 Small Computer System Interface (SCSI) Channel Cabling

The term "SCSI cable" usually refers to a complete cable, including the wire, connectors, and possibly a terminator as well. A number of different types of cables are available with various connector types to create specific cable implementations.

SCSI cables come in two distinct varieties: external and internal. External cables are used to connect SCSI devices that do not reside inside the PC; rather, they have their own enclosures and power supplies. Internal cables connect SCSI devices installed within the system enclosure. These cables are different in construction, primarily because the external environment represents much more of a risk to data corruption. This means external cables must be designed to protect the data traveling on the cable. Internal cables do not have this problem because the metal case of the cabinet shields the components inside from most of the electromagnetic and radio frequency noise and interference from the "outside world." Thus, internal cables can be made more simply and cheaply than external ones.

External cables are commonly called shielded cables because they are made specifically to protect the data they carry from outside interference. They have a very specific design in order to ensure that data traveling on the cable is secured, including the following properties:

- Twisted-pair wiring—All the wires in the cable are formed into pairs, consisting of a data signal paired with its complement. For single-ended signaling each signal is paired with a signal return or ground wire. For differential signaling each "positive" signal is paired with its corresponding negative signal. The two wires in each pair are twisted together. The twisting improves signal integrity compared to running all the wires in parallel to each other. A cable with 50 wires actually contains 25 pairs, and a 68-wire cable contains 34 pairs. This type of wiring is also commonly used in other applications, such as network cabling, for the same reason.
- Shielding—The entire cable is wrapped with a metallic shield, such as aluminum or copper foil or braid, to block out noise and interference.
- Layered structure—The pairs of wires are arranged in layers. The core layer of the cable contains the pairs carrying the most important control signals, REQ and ACK (request and acknowledge). Around the core pairs, other control signals are arranged in a middle layer. The outer layer of the cable contains the data and other signals. The purpose of this three-layer structure is to further insulate the most important signals to improve data integrity.

External cables have a round cross-section, reflecting the circular layers mentioned just above. These cables are not simple to manufacture, and external SCSI cables are generally quite expensive. For internal cables, special steps are not required to protect the data in the wires from external interference. Therefore, instead of special shielded multiple-layer construction, internal devices use unshielded cables. The internal device unshielded cables are flat ribbon cables similar to those used for floppy drives and IDE/ATA devices. These are much cheaper than external cables to make.

Even with internal cables, there are differences in construction (beyond the width issue, 50 wires for narrow SCSI or 68 wires for wide SCSI). One issue is the thickness of the wires used; another is the insulation that goes over the wires. Better cables generally use Teflon as a wire insulation material, while cheaper ones may use PVC. Regular flat cables are typically used for single-ended SCSI applications.

For Ultra2 or faster internal cables using LVD signaling, the poor electrical characteristics of flat ribbon cables begin to become an issue in terms of signal integrity, even within the PC. Therefore, a new type of internal ribbon cable was created that combines some of the characteristics of regular internal and external cables. Pairs are twisted between the connectors on the cable as with external cables, but the ribbon remains flat near the connectors for easier attachment. Ultra2 pair twisting improves performance for high-speed SCSI applications. While pair twisting increases cost, Ultra2 cables are not as expensive as external cables. This technology is sometimes called “twist-n-flat cable” since it is a partially flat and partially twisted pair.

There are several variations of the SCSI cable, each with its own limitations:

- Single-ended (SE) SCSI—Most SCSI devices use SE SCSI signaling. In SE SCSI, each signal is carried by a single wire. SE SCSI is very susceptible to noise and has a rather short distance limitation, a maximum of 6 m (20 ft).
- Differential SCSI (also called high-voltage differential [HVD] SCSI) —Differential SCSI is incompatible with SE SCSI above because it uses differential signaling rather than single-ended signaling. The benefit of using differential SCSI is that it works well in noisy areas and can reach up to 25 m (82 ft) in distance.
- Low-voltage differential (LVD) SCSI—LVD is the newest type of SCSI cabling. LVD SCSI specifications offer distances up to 12 m (39 ft) and legacy support of LVD/SE which offer LVD mode or SE mode. Most LVD SCSI devices are LVD/SE. However, the link can only run in SE mode or LVD mode. If one device on the SCSI bus is SE, all devices will be limited to SE limitations. All devices must be set to LVD to achieve LVD distance and speed capabilities. Note that LVD SCSI cabling requires twist and flat ribbon cable and a LVD/SE terminator or a twist and flat ribbon cable with built-in LVD termination.

15.3.3.3 Serial Console Cabling in the Computer Room and Operations Center

15.3.3.3.1 Recommendations

The recommended maximum distances for EIA/TIA-232-F and EIA/TIA-561/562 console connections up to 20 kb/s are approximately:

- 23 m (75 ft) over Category 3/Class C balanced twisted-pair cabling.
- 27 m (90 ft) over category 5e/class D or category 6/class E balanced twisted-pair cabling.

The recommended maximum distances for EIA/TIA-232-F and EIA/TIA-561/562 console connections up to 64 kb/s are:

- 8 m (25 ft) over Category 3/Class C balanced twisted-pair cabling.
- 10 m (30 ft) over category 5e/class D, category 6/class E or higher balanced twisted-pair cabling.

15.3.4 KVM Switches

15.3.4.1 Introduction

A keyboard, video, mouse (KVM) switch allows a single keyboard, video display monitor, and mouse to be switched to any of a number of computers, typically when a single person interacts with all the computers but only one at a time. The switch provides more table space in addition to saving the cost of multiple keyboards and monitors. KVM switches are commonly used at Web and other server locations with multiple computers but usually by a single administrator or webmaster.

IP protocols are also advancing into KVM switching systems that are used to access server consoles remotely. IP KVMs allow users to remotely control server screens via Web browsers. Wireless KVM solutions are also available. The systems encapsulate KVM signals into Ethernet packets for wireless transmission over the 802.11 wireless LANs. For large data centers, this means saving on KVM cabling and cable management as well as more flexible server control. Security is provided through wireless LAN encryption or by using proprietary protocols.

15.3.4.2 Recommendations

Consider using integrated KVM or console consolidation systems to avoid the need for keyboards, monitors, and mice for every system or rack. IP-based systems allow servers to be managed over the network, allowing support staff to be located away from the data center. However, these systems should incorporate security to ensure that only authorized personnel have console access to the servers.

15.4 Communications for Network Personnel

15.4.1 Wired/Wireless/Hands-Free Voice Communications

15.4.1.1 Introduction

Data center employees spend a lot of time during the day working on multiple systems within multiple cabinets or locations in the data center or adjoining facility. Efficient voice communications is a critical consideration when designing the data center. During critical down times, employees working to repair the system should not need to worry about where the nearest telephone is.

The communications industry provides several methods of technology to consider for this situation, including:

- Wired:
  - Desktop
  - Wall mounted
  - Rack mounted
  - Intercom devices
- Wireless:
  - Analog
  - Cellular
  - VoIP
  - Hands free

Advancements in wireless data technology and digital voice systems permit voice and data systems to share the same wireless system.

An intercom device can be designed in conjunction with overhead speakers and ceiling mounted microphones to provide hands-free communication between the data center staff and support space. The intercom system can also be a very effective form of access control and can be integrated with video and the appropriate door release hardware.

Wireless equipment may not work well in a shielded computer room.

15.4.1.2 Recommendations

When using a wireless VoIP system, one of the more important tasks to perform prior to designing a wireless deployment is to conduct a wireless site survey. This survey will verify that wireless antenna coverage is adequate to provide appropriate Quality of Service (QoS) for voice and data applications.

One note of caution when considering 2-way radios within the data center; some fire suppression systems contain blasting caps that are used to "fire" the release pin on the suppression media tank in the event of a fire. Construction sites use similar explosive caps. Signs are often posted when approaching road construction, which provides warning to turn off two-way radios and cell phones. These caps can be triggered by certain frequencies. Therefore, it is advised that prior to using two-way radio communications in the data center that the fire suppression provider be contacted. The manufacturer or installation contractor will be able to specify if two-way radios can be used in or near the data center. It is further recommended that a NO RADIO ZONE be established of a size as determined by the manufacturer if the data center is using a blasting cap type system (see Figure 15-11).

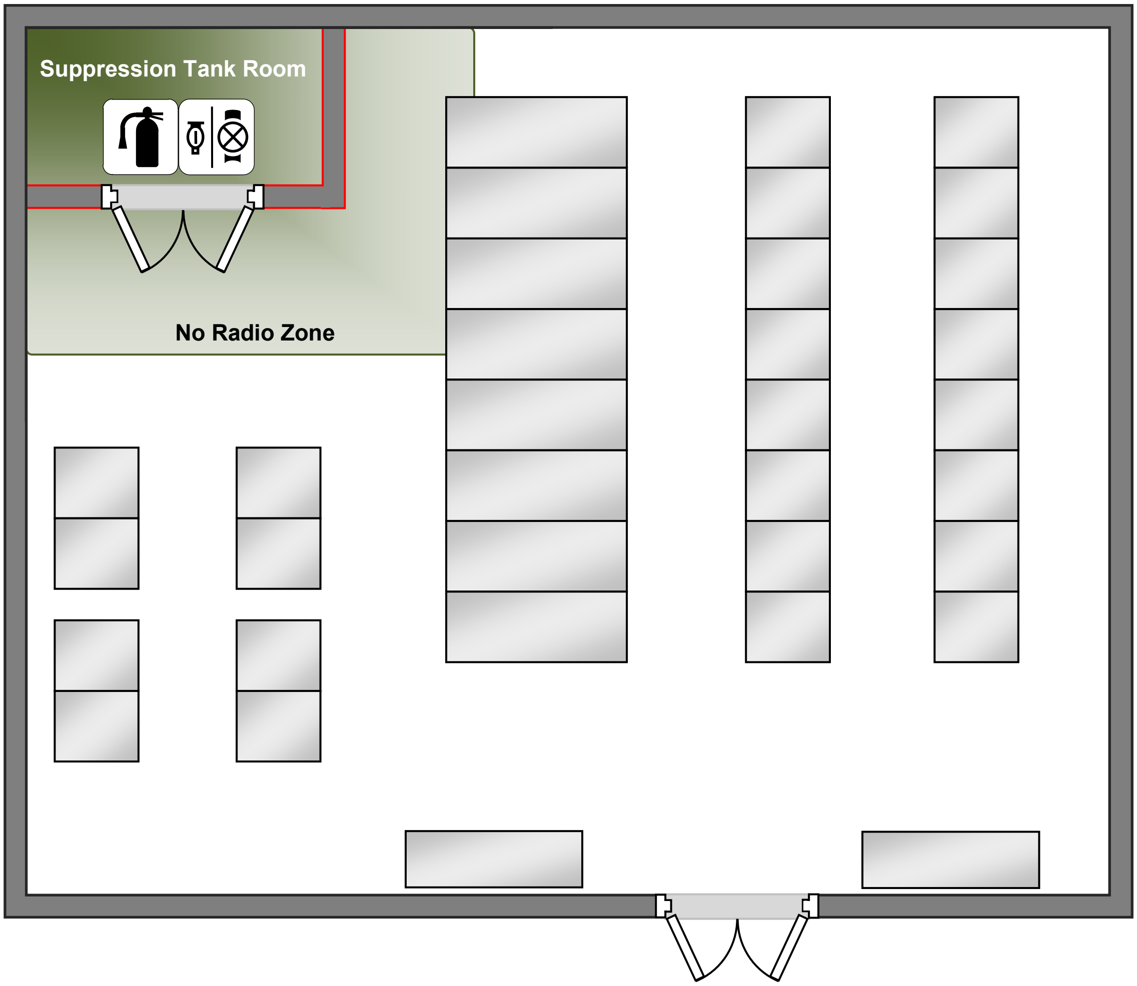


Figure 15-11
No Radio Zone Around Suppression Tank Room

15.4.2 Wireless Network for Portable Maintenance Equipment

With the growing size and complexities of today's data centers, the designer should take advantage of the advancements in wireless technology to potentially provide a redundant maintenance network:

- Personal digital assistant (PDA)
- Tablets
- Scanners—asset tracking

15.4.3 Zone Paging

While overhead paging can be one of the more primitive forms of communication, it can still be very effective for regionalized voice contact in such areas as:

- Network operations center
- Support space
- Computer room

15.5 Network Security for Facility and IT Networks

15.5.1 Overview

There are several networks within the data center beyond the core computer room Ethernet local area or Fiber Channel storage area network. Networks within the data center are made up of discrete IT and facility system networks. Often, the implementation of these networks are planned, designed, installed, and managed by individual departments with little or no communication between the groups, resulting in a lack of coordination and a common set of guidelines or standards.

The networks can be categorized into three main systems:

- Computer Room Networks:
  - Server and NAS Ethernet LAN
  - Storage Fiber Channel SAN
- Building Desktop Networks:
  - Desktop PCs
  - VoIP Telephones
- Facility Building Automation System (BAS) Networks:
  - HVAC Controls
  - Fire Alarm
  - Physical Security
  - Computer Room Power Monitoring
  - Electrical Distribution Control
  - Lighting

Figure 15-12 shows an example of a facility & IT network topology with these types of systems.

Although these network categories are discrete in their topology, they do interface through BMS or DCIM tools to provide key management functionality for data center facility managers, computer operators, and network administrators. It is important that these networks are planned and designed in a coordinated effort to ensure:

- It is clearly understood which staffing roles require access to each network
- Who is responsible to manage each network
- Who is responsible to manage the interfaces between the networks and what levels of security are required at each network interface
- Who is responsible to manage each network, hardware platforms, and operating systems
- Who is responsible to install each network cabling infrastructure pathways

Once these questions have been answered the data center designer can begin to identify where the hardware and core network components should be located, how they are interconnected (if required), and how logical security will be provided.

NOTE: See Section 13 for further information on DCIM and building systems.

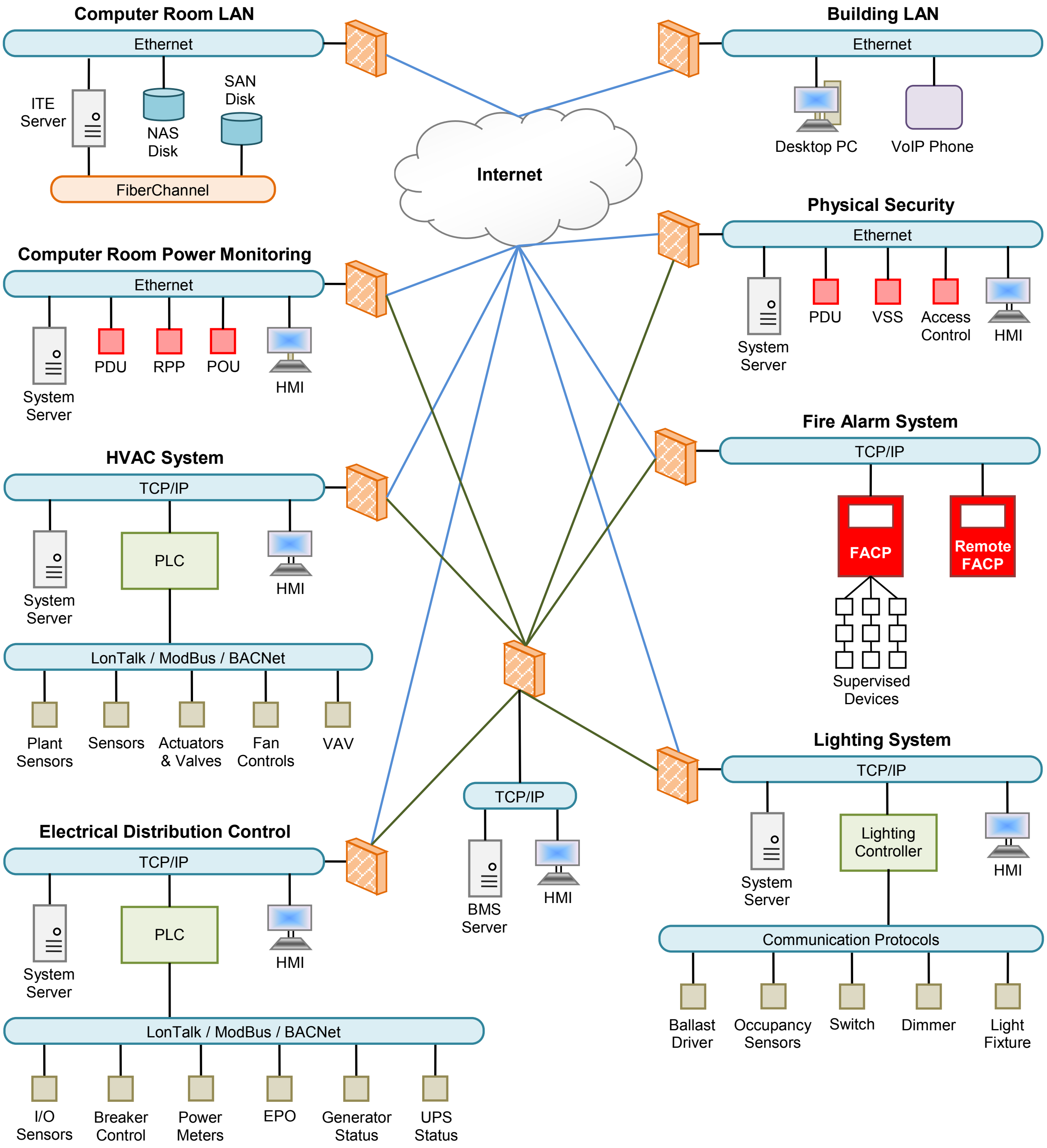


Figure 15-12
Example of Facility & IT Network Topology

15.5.2 Requirements

The configuration of the non-computer room networks shall have logical security that isolates each of these non-computer room networks from each other and from the critical and data sensitive computer room network.

15.5.3 Recommendations

Each of the discrete systems may have server-based control logic which raises the question, “Where should non-IT servers be physically located?” If the non-IT servers are not managed by the IT department, it is not recommended that they be located within the computer room. A separate secure room, or area, within the data center should be provided for non-IT servers. It is recommended that these non-IT servers be supported by a dedicated facility UPS, separate from the UPS that supports the computer room, which meets the Class redundancy of the data center.

The IT network team should be engaged early in the facility design process so that each of these non-computer room networks are clearly understood by the IT network administrators enabling them to plan a suitable firewall design to isolate and protect each of the networks.

15.6 Disaster Recovery

15.6.1 Introduction

In conjunction with disaster recovery planning listed in Section 12.9, there are several considerations specific to the network, ITE, and the data and applications being supported. Some of these considerations include:

- Onsite data storage
- Offsite data storage
- Colocation facility
- Mirroring and latency
- Data center system failures

15.6.2 Onsite Data Center Redundancy

Redundant pathways are typically designed to eliminate or reduce single points of failure in the cabling infrastructure.

Network equipment redundancy includes redundant routers, core, distribution, service appliances, service modules, access layer LAN/SAN switches, hot-swappable port cards, spare wireless antennas, and power supplies.

15.6.2.1 Requirements

Backup equipment cabinets, racks, and associated hardware are required for recovery of campus area networks and metropolitan area networks; long-haul fiber optic emergency facilities are provisioned for high-bandwidth connectivity to critical sites during disasters.

15.6.2.2 Recommendations

Equipment should be in cabinets supported by branch circuits from different electrical panels or power distribution units. Equipment with multiple power supplies and power cords should be plugged into different branch circuits for power redundancy. For equipment with one power cord, consider plugging the equipment into a rack-mount switch or power strip that is fed from two different branch circuits.

15.6.3 Offsite Data Storage

15.6.3.1 Cold Site (Recovery Ranging From 24 Hours to 5 Days)

A cold site is typically a leased or company owned disaster recovery facility providing only the physical space for recovery operations. Clients provide their own hardware, software, and network. Depending on the level of services contracted, equipment is either “cold” (stored at the site) or “cool” (powered up but not in service). Clients transfer data on physical media like tape and optical media. The clients can also transfer data over point-to-point communication lines or via secure VPN tunnels directly to the site. Backup data may be transferred to a second off-site facility as well for remote storage of critical data. The “cold” or “cool” site method provides the replication machines, operating systems, and applications required for disaster recovery at significantly less cost than having a full backup data center. However, recovery time may be unacceptable. The cool disaster recovery site should be tested regularly.

15.6.3.2 Warm Site (Recovery Ranging From 30 Minutes to 8 Hours)

A warm site is a backup site having some, but not all, of the components necessary to immediately restore all business functions. During a disaster, obtaining additional hardware and software will delay recovery to some degree. A warm site can function as a second production data center until needed for disaster recovery. Because the warm site must be able to assume the primary site workload, data must be replicated and transferred to the warm site periodically. Generally, the data replication routine can occur anywhere from once every 24 hours to once a week. The data transfer often takes place through a high-speed data connection. In the event of a disaster, the warm site would run on one day or older data unless real-time mirroring of production data occurs. Real-time mirroring is expensive and requires data synchronization management.

15.6.3.3 Hot Site (Recovery Ranging From 1 Minute to 20 Minutes)

A hot site is a fully operational offsite data center equipped with both the hardware and software systems that can very quickly assume the disaster recovery workload. A hot standby site can be used as an active/active data center for certain applications. This can be achieved by replicating the data in a synchronized fashion between the data centers in real time.

A hot standby site can also be used as an active/standby data center for certain applications. To achieve that, the data should be saved in a synchronized fashion but not necessarily in real time.

15.6.4 Colocation Facility

A colocation facility is a data center in which multiple clients lease small portions of the computer room for their computer and network equipment. Companies typically lease anywhere from one cabinet or rack to several cabinets or racks enclosed in a secured fence or by walls. The equipment may be for backup recovery, for remote storage, or even the primary data center for that client. The advantage to the client is having a secured and controlled computer room environment without having to build and maintain a data center. The colocation owner is typically responsible for moving equipment into the spaces (often called cages or suites), setting up customer-provided cabinets or racks, configuring communications equipment, and creating physical security access lists.

The colocation facility owner provides power as required by the client, circuit delivery facilities, and various levels of support. Colocation facilities generally offer high security, including cameras, fire detection and extinguishing systems, multiple connection feeds, filtered power, backup power generators, and other items to ensure high availability, which is mandatory for all web-based, virtual businesses.

15.6.5 Mirroring and Latency

15.6.5.1 Mirroring

Mirroring is the copying of data from the host system to a second system in real time. Because the data is copied in real time, the information stored on the second system is the same as the information on the host system. Data mirroring is critical for the speedy recovery of critical data after a disaster. Data mirroring can be implemented locally or offsite at a remote data center or colocation facility. When copying data offsite, it is important to consider the form of transmission used, as bandwidth and delay affect the performance and capacity of the mirroring or replication. Transmission methods such as ISDN PRI, T-1, T-3, E-1, E-3, ATM, Gigabit Ethernet, SONET, SDH, and DWDM are commonly employed.

15.6.5.2 Latency

The synchronous replication of data and accessing of that data by applications between two or more systems or data centers is dependent on the distance between the all of the elements involved. As latency increases as the distance increases, latency should be limited so that application or the data replication write functions can show acceptable performance.

15.6.5.3 Physical Connectivity Methods and Devices

Physical connectivity can take many forms (e.g., conventional copper, optical, satellite). Conventional methods include copper connections between devices within the same cabinet, rack, row, or room. While this is the most economical, equipment must be located within a limited distance not to exceed constraints that may limit bandwidth. Other methods can increase the distance and speed of replication; however, there is an inherent increase in costs associated with these methods, which include, but are not limited to, long-haul Ethernet, carrier MPLS networks, ATM, SONET, and DWDM.

15.6.5.4 Location of Real-Time Redundant Storage Device

The location of the redundant storage devices is critical. Possible locations include housing the equipment in the same room, the same building, on campus, or off-site. Considerations include the need to have quick access to the backup equipment for maintenance, disaster recovery timelines and policies, and security levels of protection of the stored information. Other considerations include the financial and criticality aspects of maintaining real time, redundant databases.

It is generally desirable for redundant storage to be located off-site in a location far away enough to avoid losing both copies during a single disaster. It should be noted, however, that many data replication methods have distance limitations.

15.6.5.5 RAID

Short for redundant array of independent (or inexpensive) disks, a category of disk drives that employs two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but are not generally necessary for personal computers.

There are number of different RAID levels:

- Level 0: striped disk array without fault tolerance—provides data striping (spreading out blocks of each file across multiple disk drives) but no redundancy; this improves performance but does not deliver fault tolerance. If one drive fails, then all data in the array is lost.
- Level 1: mirroring and duplexing—provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.
- Level 2: error-correcting coding—not a typical implementation and rarely used, Level 2 stripes data at the bit level rather than the block level.
- Level 3: bit-interleaved parity—provides byte-level striping with a dedicated parity disk. Level 3, which cannot service simultaneous multiple requests, also is rarely used.
- Level 4: dedicated parity drive—a commonly used implementation of RAID, Level 4 provides block-level striping (like Level 0) with a parity disk; if a data disk fails, the parity data is used to create a replacement disk. A disadvantage to Level 4 is that the parity disk can create write bottlenecks.
- Level 5: block interleaved distributed parity—provides data striping at the byte level and stripe error correction information; this results in excellent performance and good f fault tolerance. Level 5 is one of the most popular implementations of RAID.
- Level 6: independent data disks with double parity—provides block-level striping with parity data distributed across all disks.
- Level 7: A trademark of Storage Computer Corporation that adds caching to Levels 3 or 4.
- Level 0 + 1: a mirror of stripes—not one of the original RAID levels, two RAID 0 stripes are created, and a RAID 1 mirror is created over them; used for both replicating and sharing data among disks.
- Level 10: a stripe of mirrors—not one of the original RAID levels, multiple RAID 1 mirrors are created, and a RAID 0 stripe is created over these.

15.6.6 Data Center System Failures

15.6.6.1 Power Failure

In general, the power disaster recovery efforts should include a consideration for redundant external power sources, alternate power supply methods, and dedicated UPS units per equipment, equipment rack, or cabinet (see Section 9).

Power strips within the equipment cabinets or racks should be IP capable to allow for SNMP monitoring and reactive reporting of power consumption, spikes, dips, and preaction alerts.

Communications devices should support multiple power supplies and be capable of continuous operation in the event that one supply fails, loses power, or requires hot swap.

Ensure that equipment that has dual power supplies is plugged into the upstream electrical distribution. (See Section 9.3.15)

15.6.6.2 HVAC Failure

Every facility should have a portable HVAC unit and an adequate number of large fans in storage to provide temporary service to critical equipment. Special considerations must be made in advance to ensure that power is available with the correct type of power receptacle. Additional advanced consideration is required for hot air exhaust from portable HVAC units and properly sized exhaust tubes, including correct lengths. Exhaust tubes and ceiling grid connectors are not necessarily included with portable unit purchases but may be purchased separately.

16 Commissioning

16.1 General

16.1.1 Introduction

Commissioning is the process of ensuring systems are designed, installed, functionally tested, and capable of being operated and maintained according to the owner's design intent and operational needs. Commissioning also provides testing of failure modes and operational procedures that cannot be performed once the data center is in production.

Commissioning is often one of the most neglected aspects of system installation. A system that is properly tested and commissioned will provide the designer, installer, and client with a system that functions correctly, meets the client's requirements, and can help foster a continuing professional business relationship between the designer and client for future work.

Commissioning a building system should clearly identify real and potential issues with the building system and the affiliated subsystems during all phases of the project. Because of its unique facilities requirements and systems, a data center should be commissioned according to industry guidelines and requirements.

16.2 Terminology

Definitions and acronyms that apply specifically to commissioning follow below and only apply to the commissioning section of this standard:

BoD	basis of design
BOM	building´s operational manual
CxA	commissioning agent
CxP	commissioning plan
CxT	commissioning team
DT	design team
O&M	operation and maintenance
OPR	owner´s project requirements
MAC	moves, adds and changes
PM	project manager
RFI	request for information

basis of design (BoD) Documents that are generated by the design team, where it is given specific response to meeting the owner's project requirements in each of the fields of application. They must comply with the laws, codes, regulations, rules and standards.

commissioning (Cx) A quality assurance process that confirms that building´s systems have been designed, constructed or installed correctly, tested and consistently started, documented and operated in strict accordance with the requirements stated by the owner for a contracted execution building project.

commissioning agent (CxA) Agent may consist of one or more individuals with proven experience in accordance with the provisions of the basis of design and is jointly liable with the owner to monitor the technical processes of each of the work areas involved.

Note: Some municipalities / regions / states/countries accept the commissioning agent as a legal AHJ

commissioning plan (CxP) Document prepared by the commissioning agent and approved by the owner, that provides a structure, schedule and coordination plan for the commissioning process from the design phase to the warranty period. The commissioning plan must satisfy the owner's project requirements and establish the roles and responsibilities of commissioning´s team members.

commissioning team (CxT)
Composed of representatives of the owner, project manager, operation and maintenance, design team (architecture and engineering), general contractor and subcontractor, testing, tuning and balancing personnel, manufacturers, commissioning agent, civil protection and all others involved with the commissioning plan.

compliance data sheets
Documents issued by the manufacturer with the technical details and specifications of systems or components, which must be approved by the design team for releasing purchase by the contractor.

construction documents / executive project
Set of documents issued by the design team based on the owner's project requirements, used for contractors to carry out their economic proposal and run the installation or systems.

continuous commissioning
A systematic commissioning process that continues throughout the building´s life cycle.

commissioning team (CxT)
Composed of representatives of the owner, project manager, operation and maintenance, design team (architecture and engineering), general contractor and subcontractor, testing, tuning and balancing personnel, manufacturers, commissioning agent, civil protection and all others involved with the commissioning plan.

compliance data sheets
Documents issued by the manufacturer with the technical details and specifications of systems or components, which must be approved by the design team for releasing purchase by the contractor.

construction documents / executive project
Set of documents issued by the design team based on the owner's project requirements, used for contractors to carry out their economic proposal and run the installation or systems.

continuous commissioning
A systematic commissioning process that continues throughout the building´s life cycle.

contractor and subcontractors
The company or group of companies responsible for the Building Construction with all its facilities, components and systems.

deficiency
Condition of a component, piece of equipment or system that is not in conformity with the owner's project requirements.

design team (DT)
All technical consultants who bring their intellect in the conceptual development of the building, such as architects, engineers, etc. in all disciplines and other technical involved areas.

factory tests
Tests that are made to the equipment at the factory by the manufacturer's personnel. Testing may be done in the presence of owner's representative, as deemed necessary.

functional test
Tests that assess the operation of the equipment and systems installed by the contractor, and may assess: startup and commissioning, compliance values, tolerances, manufacturer's specifications, codes, and rules and standards. The testing performed is typically defined in the owner's project requirements, basis of design as well as the construction documents.

incident log
The collection of any addition, modification or change in the status of the project in stages until the formal start of its operation, and must include the cause, responsible and resolution.

integral system testing
Performance testing and operation of systems to ensure they work in a coordinated manner and properly according to manufacturers' specifications, codes, rules and standards. The testing performed is typically defined in the owner's project requirements, basis of design as well as the construction documents.

operational building manual (OBM)
Documentation that includes all system operating processes and includes all building information from the owner's project requirements up to its implementation.

owner Refers to but is not limited to the person, company or government entity that legally owns a property without limitation.

pre functional tests Verification procedures for ensuring that equipment, components and accessories of a system were installed according to the manufacturers' specifications, codes, rules and standards.

pre functional verification check list A list of visual inspection and component material, and testing to ensure proper installation of the equipment (e.g., belt tension, oil levels, set tags, calibrated sensors). Pre functional word refers to pre-functional tests. These should include checklists by the manufacturer.

seasonal commissioning A systematic commissioning process that is performed in different seasons (e.g., summer, winter) depending on building´s latitude, longitude, altitude.

seasonal / periodic tests Those tests that assess the performance and operation of systems to ensure they work in a coordinated manner and properly according to manufacturers' specifications, codes, rules and standards. They confirm the status of its components prior to the expiration of their guarantees.

submittals Technical documents to be approved by the design team and commissioning agent. They must comply with owner's project requirements.

testing requirements Documents with system specifications, modes, functions, conditions, etc., to be tested. These are not detailed testing procedures.

16.3 Types of Commissioning

16.3.1 New Building

Four types of new building commissioning can be employed, depending on the project scope, client budgets and the design intent as well as existing building commissioning activities.

16.3.1.1 Continuous Commissioning

- Commissioning authority is engaged at the start of project.
- Performance information is gathered and reviewed throughout the life of the facilities.
- Ensures the design intent is maintained through project.

16.3.1.2 Milestone Commissioning

- Defines design milestones procedures.
- Performs testing, component validation, and verification of design intent at agreed upon intervals.

16.3.1.3 Acceptance Phase Commissioning

- Conducts required test on the integrated systems only.
- Reviews all test and maintenance criteria prior to turnover.
- Validates operational performance and correct deficiencies.

16.3.1.4 Network Operability Commissioning

- Performs validation of IT systems before turnover.
- Utilizes documented observed performance to establish baseline criteria.

16.3.2 Existing Building

16.3.2.1 Overview

There is considerable reported value in performing commissioning activities to existing buildings or systems. For existing buildings, this may take one of two forms:

- Retrocommissioning—the application of the commissioning process to a building that has not undergone commissioning and is initiated at some point after operations have already commenced.
- Recommissioning—the performance of the commissioning process to existing installations that had at least an initial commissioning performed, typically to reassess performance because of to modifications in operations, system changes or other concerns.

The goal of either commissioning form is to ensure system operation and performance is in alignment with the operation's current use or needs.

16.3.2.2 Recommendations

A plan for recommissioning should be established as part of a new building's original commissioning process or during an existing building's retrocommissioning process.

16.4 Personnel and Responsibilities

The following commissioning process responsibilities scheme may change depending on applicable law, codes, and standards for the site.

16.4.1 Project Owner

Is responsible for:

- Hiring and paying commissioning agent (CxA) and design team.
- Promptly informing all participants involved in the design, construction and operation to start a commissioning process at once.
- Working together with the CxA and the design team to issue requirements for the OPRs and documents in the process, e.g., building´s classification programs –LEED, UTI, ECoC, BREEAM
- Establishing a representative in the CxT with authority for decision-making.
- Authorizing moves, additions and changes (MACs) in the OPRs based on the results of the commissioning process.
- Receiving and accepting reports of periodic visits and registration of incidents during the work. Participating in the training process.
- Receiving and authorizing the building once the final report of the commissioning process is completed.

NOTE: Because of the size of some projects, the owner hires the services of a project manager (PM) to act as the owner's representative. The PM must notify the design team and the CxA of any MACs that affect or change the OPRs

16.4.2 Design Team (DT)

Is responsible for:

- Developing and delivering the BoD according to the OPRs.
- Developing and providing documentation of each system design included in the design contract according to the OPRs and the corresponding executive project/construction documents.
- Developing and delivering coordination drawings of the facility´s systems.
- Developing and delivering the moves, additions and changes (MACs) in the design/construction documents based on the results of the commissioning process and the scope of the contract.
- Establishing a representative in the CxT.
- Working together with the CxA and Owner to issue requirements for OPRs. Shall participate in Cx meetings, including those held during functional testing process.
- Reviewing and approving the submittals and responding to RFIs concerning the technical specifications and manufacturers' manuals for the construction stage of each system to be designed.
- Working with the CxA to set parameters, ranges, tolerances and performance measurement systems.
- Informing and notifying the owner and CxA of the results of the evaluation (technical and resources) of any MACs that affect or change the OPRs.
- Plan shall follow the commissioning best practices and requirements for the completion on time and Budget.
- Shall attend to all Cx team meetings.

16.4.3 Commissioning Agent

The commissioning agent is the person who has the knowledge, skills and experience to plan, perform and execute a plan of commissioning in one or more of the systems susceptible commissioning in a building. The commissioning agent is responsible for:

- Working together with the owner and DT team to issue requirements for OPRs and the MACs that shall be approved by the owner.
- Working with the design team to develop the feasibility studies and the project schedule.
- Developing the commissioning plan (CxP) and attached documents.
- BoD review to ensure compliance with the OPR. Reviewing the plans and specifications for the planning and design phases.

List continues on the next page

- Planning, organizing and ensuring the Cx processes, attends and coordinates Cx team meetings.
- Ensuring Cx process activities are clearly specified throughout all processes.
- Identifying and integrating the commissioning process activities within the project schedule.
- Reviewing, in conjunction with the design team, contractor and subcontractors manuals and manufacturers' compliance with the BoD to integrate the BOM.
- Documenting and tracking all deviations from the OPRs and keeping track of incidents with the resolutions-incident log.
- Preparing the Cx process progress reports and the closing report of the commissioning process of each stage with recommended actions as well as the final report of commissioning to the Owner.
- Ensuring the final design executive project/construction documents of each specialty can be commissioned.
- Coordinating the review and approval by the design team of the technical specifications and compliance of each system.
- Conducting periodic visits to the work site to ensure quality by issuing the corresponding report, which can be supplemented with documents to ensure compliance with the design. The visit reports should include a checklist and track incidents arising during the work, with the solutions to them and the allocation of those responsible for carrying them out.
- Issuing formats for pre-functional and functional tests described in this document, which shall be approved and used by the commissioning team.
- Validating the information in the pre-functional tests once the contractor and subcontractors have completed them.
- Organizing, coordinating and witnessing the functional tests and performance final tests of systems.
- Checking that required technical training for operation and maintenance personnel is conducted by contractors, subcontractors and equipment manufacturers.
- Checking that required user training on the operation of the systems is carried out.
- Integrating the operations manual of the building (OEM) gathering information by the contractors and with the commissioning team, coordinating the operation and maintenance of all systems.
- Issuing the final report of the commissioning process for acceptance by the owner.
- Preparing the plan of continuous commissioning at the request of the owner.
- The plan shall follow the commissioning best practices and requirements for completion on time and within budget.
- Shall attend to all Cx team meetings.

NOTE: The commissioning agent (CxA) is not responsible or liable for the concept design, design criteria, compliance with codes or national and international standards, the general program of work, the cost estimation and management / administration the work.

The following ae recommendation for the commissioning agent.

- The CxA shall have a management structure that allows it to maintain the capability to perform the functions with technical quality.
- The CxA shall be legally constituted.
- The CxA shall have a quality management system and updated documentation.
- The CxA shall have a code of ethics or conduct and enforce it with the appropriate staff.
- The CxA shall avoid conflicts of interest with persons or organizations with which they have direct business relations in the work for which it has been contracted.
- The CxA shall ensure that personnel assigned to provide temporary or eventual commissioning services has the academic standards for the class and category of interest; staff shall possess professional license and / or certificate based on competency standards, as appropriate.
- The CxA shall comply with the job description for each class or category, including the requirements for education, training, skills, expertise and experience.
- The CxA shall comply with health and safety regulations.

16.4.4 Contractor and Subcontractor

Is responsible for:

- Installing systems based on the final design and scope of its contract.
- Proposing, performing and recording all moves, additions and changes (MACs) in the installation of the systems of their responsibility in coordination with the design team and the scope of its contract.
- Submitting to review and approval by the design team, the technical specifications of compliance, diagram detail and shop drawings of each building system (submittals).
- Updating equipment according to the approved technical specifications.
- Addressing the report's findings of incidents and regular visits to work based on the conditions set out in the commissioning plan (CxP).
- Conducting tests with qualified personnel according to the formats established in the CxP; it shall provide necessary equipment or instruments with current calibration according to the CxP´s specifications.
- Carrying out the training plan for the owner´s operation and maintenance (O&M) staff and system´s users installed under the scope of its contract. (e.g., voice, data, video systems).
- Updating the building operational manual (BOM) in coordination with the CxA and O&M personnel.
- Preparing the O&M plan of installed equipment in coordination with the CxA and O&M personnel.
- Witnessing, in conjunction with the CxA, seasonal Cx to conform to the O&M plan.
- The plan shall follow the commissioning best practices and requirements for completion on time and within budget.
- Shall attend to all Cx team meetings.

16.4.5 Operation and Maintenance Staff (O&M)

Is responsible for:

- Setting the O&M needs of each system under their responsibility so they will be included in OPRs.
- Witnessing testing procedures based on the formats established in the CxP.
- Assisting and providing an acceptance document of the training received by the contractor(s).
- Receiving and revising the building operations manual (BOM).
- Revising, supplementing and approving the operation and maintenance plan for all installed equipment in coordination with CxA.
- Performing the systems´ seasonal recommended testing to all systems. Where appropriate, carrying out the continuous commissioning plan.
- Supervising, monitoring and executing the operation and maintenance of the systems according to plans received. Monitoring and evaluating the performance of systems delivered by contractor(s).
- Its plan shall follow the commissioning best practices and requirements for the completion on time and within budget.
- Shall attend to all Cx team meetings.

16.5 Phases of the Commissioning Process

16.5.1 Overview

The commissioning process is not isolated to one discrete phase of a data center's construction. Rather, the commissioning process has elements in all of a data center’s construction phases. As shown in Figure 16-1, these phases include:

- Pre-Design (Program) Phase
- Design Phase
- Construction & Acceptance Phase
- Occupancy & Operations

Elements of commissioning for each phase are described in the following sections.

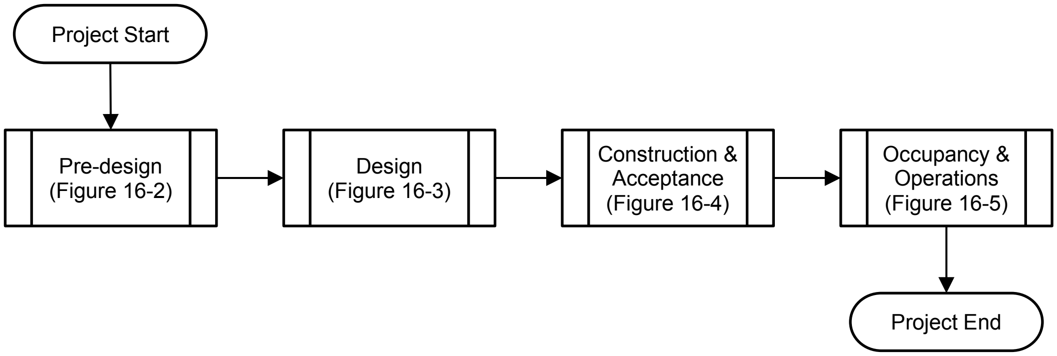

Project Start
Pre-design (Figure 16-2)
Design (Figure 16-3)
Construction & Acceptance (Figure 16-4)
Occupancy & Operations (Figure 16-5)
Project End

Figure 16-1
General Commissioning Phases Flow Chart

16.5.2 Program Phase

The program phase establishes the foundation for the other phases and determines the scope of work and systems to be commissioned. Objectives in the program phase include:

- Establishing the:
  - Design's intent
  - Project owner’s requirements
  - Necessary funding and budgets
- Identifying the:
  - Team
  - Systems to be commissioned
  - Performance reliability requirements or BICSI 002 availability Class rating
  - Required approvals for all phases and receiving those required for the program phase
  - Requirements for training
- Developing the:
  - Commissioning plan
  - Commissioning issues log procedures

Decisions made in the program phase are crucial to the overall success of the commissioning of a data center.

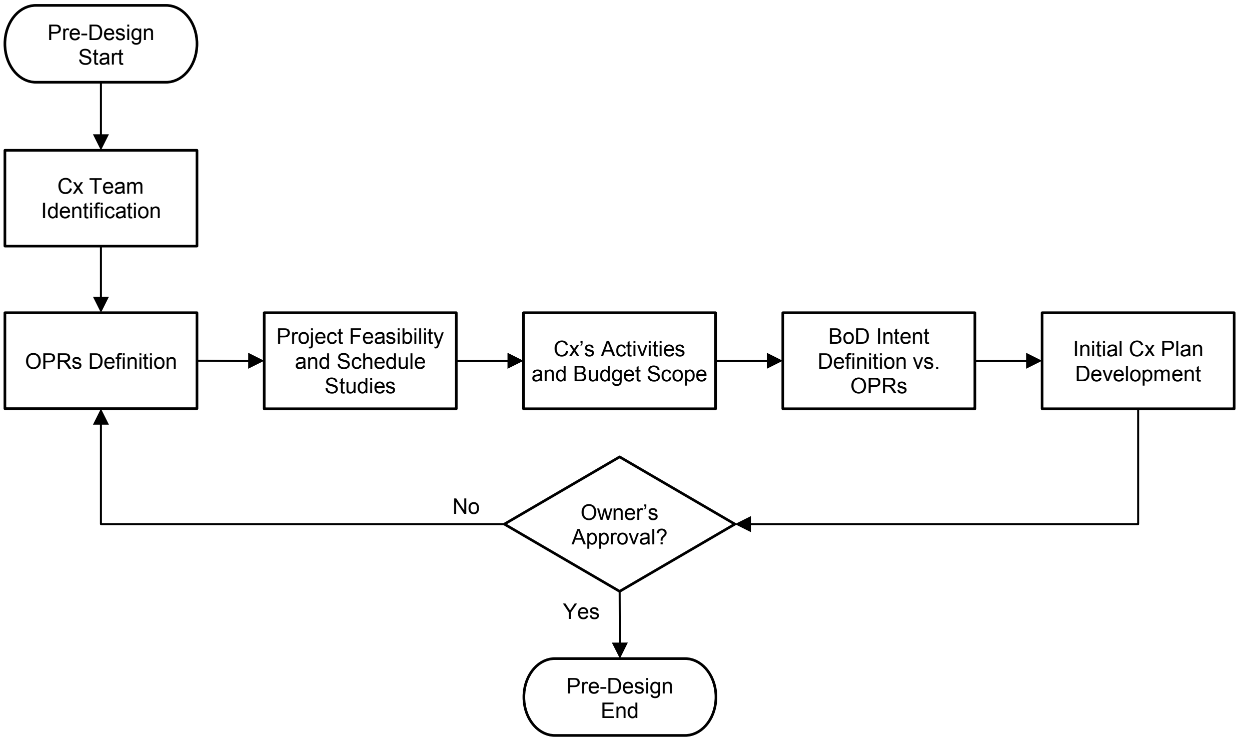

Pre-Design Start
Cx Team Identification
OPRs Definition
Project Feasibility and Schedule Studies
Cx's Activities and Budget Scope
BoD Intent Definition vs. OPRs
Initial Cx Plan Development
Owner's Approval?
No
Yes
Pre-Design End

Figure 16-2
Pre-Design Commissioning Phase Flow Chart

16.5.3 Design Phase

During the design phase, the design of the data center components and systems is completed. Contract documents, specification documents, and system documents are completed. The commissioning agent should review all documents to ensure compliance with the design intent. Objectives in the design phase include:

- Architectural review of the room or building
- Review of the IT and facilities systems
- Execution of a needs assessment and inventorying of IT requirements
- Submission of design intent documentation
- Review of scope of work for all participants, including contractors and vendors
- Review of systems for maintainability in critical environments

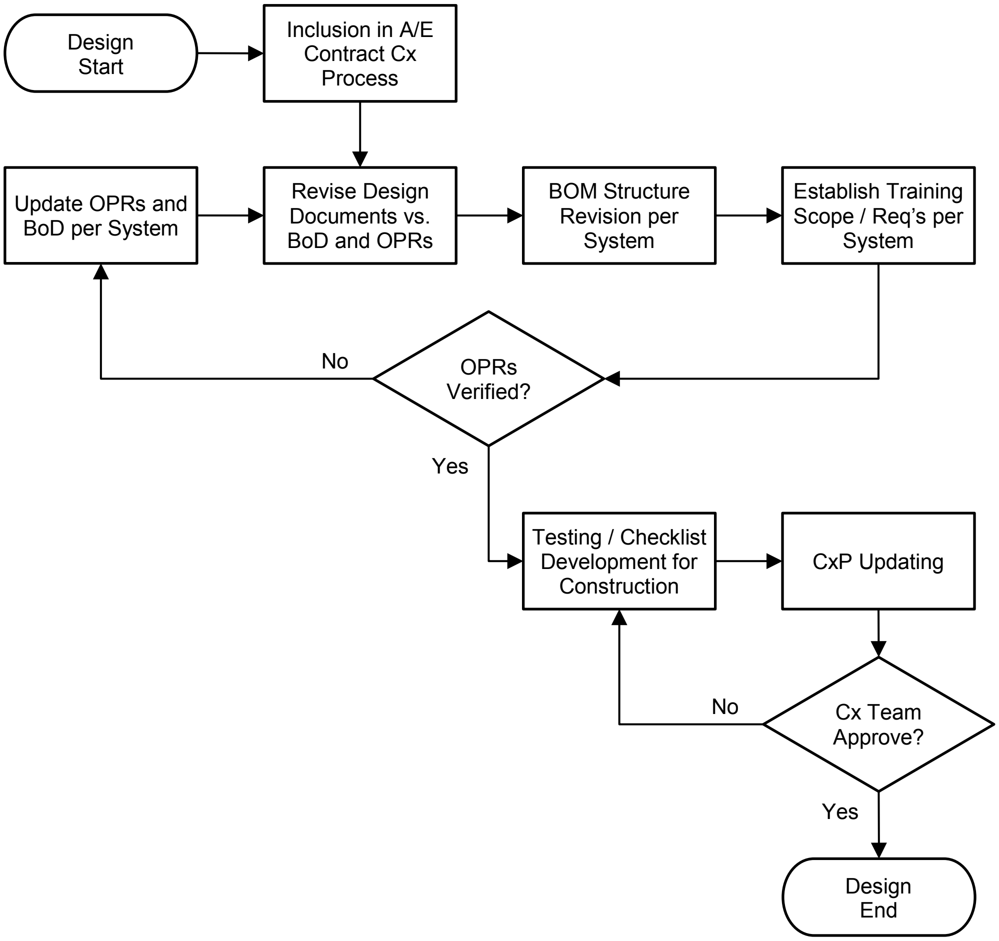

Design Start
Inclusion in A/E Contract Cx Process
Update OPRs and BoD per System
Revise Design Documents vs. BoD and OPRs
BOM Structure Revision per System
Establish Training Scope / Req's per System
No
OPRs Verified?
Yes
Testing / Checklist Development for Construction
CxP Updating
No
Cx Team Approve?
Yes
Design End

Figure 16-3
Design Commissioning Phase Flow Chart

16.5.4 Construction & Acceptance Phase

This phase contains the majority of tasks that can be divided in construction activities and activities. As the building or data center is constructed, the commissioning authority monitors the progress to ensure the design intent is being followed. Objectives in the construction phase include:

- Performance of milestone monitoring
- Completion of prefunctional testing as required
- Submission of field inspections and progress reports
- Monitoring of the change order process and approval authority
- Documentation and approval of any modification of the design intent

As construction and systems are completed, functional performance testing is performed on all the integrated systems. System calibration, manufacturers testing guidelines, and other requirements established during the design intent are completed and documented. Nonperforming systems are identified and corrected prior to startup. Objectives in the acceptance phase include:

- Base line performance documentation
- Functional performance testing
- Site audit
- Warranty audit
- Submission of the final documentation and all test reports

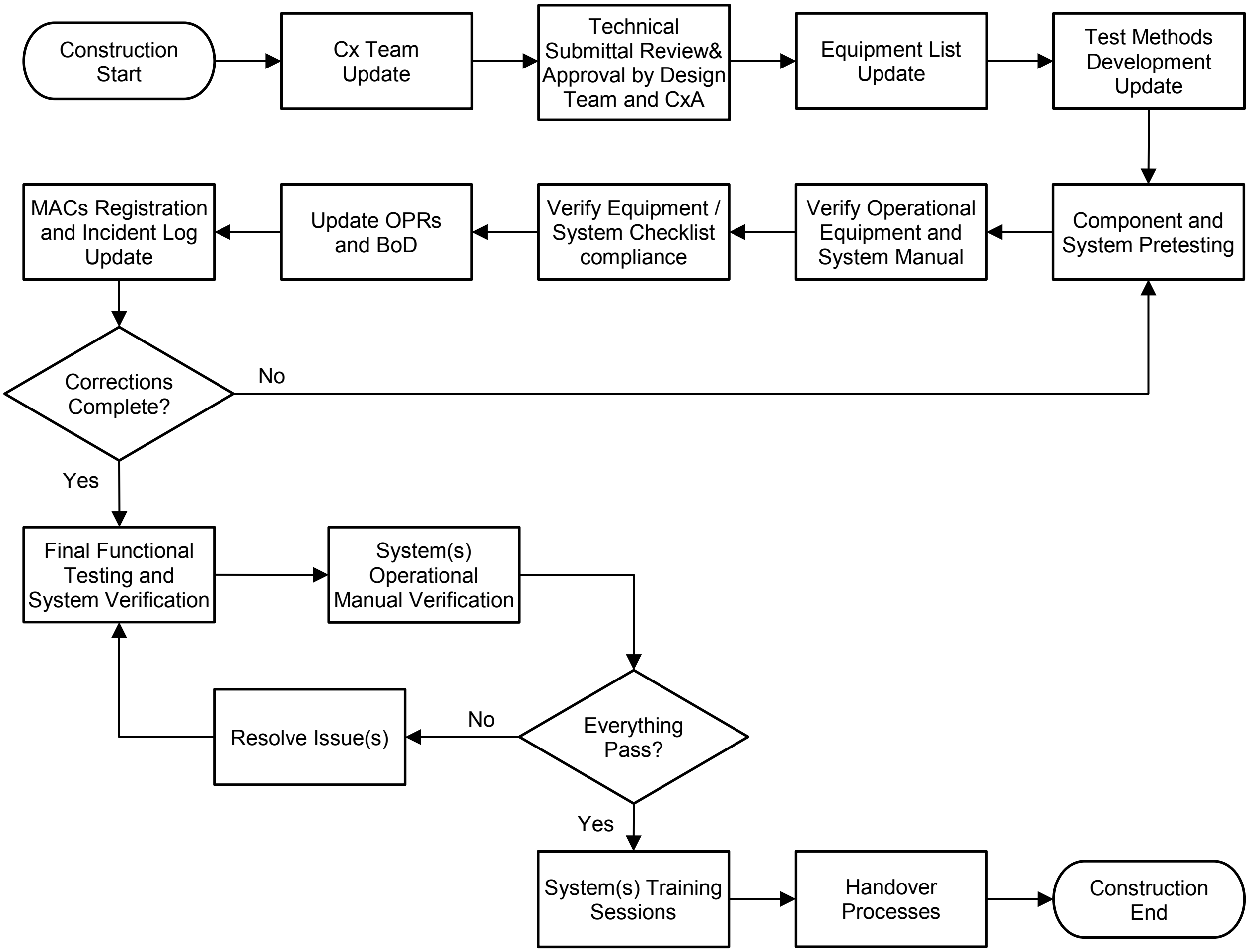

Construction Start
Cx Team Update
Technical Submittal Review& Approval by Design Team and CxA
Equipment List Update
Test Methods Development Update
Component and System Pretesting
Verify Operational Equipment and System Manual
Verify Equipment / System Checklist compliance
Update OPRs and BoD
MACs Registration and Incident Log Update
Corrections Complete?
No
Yes
Final Functional Testing and System Verification
System(s) Operational Manual Verification
Everything Pass?
No
Resolve Issue(s)
Yes
System(s) Training Sessions
Handover Processes
Construction End

Figure 16-4
Construction Commissioning Phase Flow Chart

16.5.5 Occupancy and Operations Phase

Also known as the post-acceptance phase, operations and maintenance procedures are defined and monitored. As an extension of the acceptance phase, the documentation of new systems, changes in the facility, and a process for verification that the design intent is still being met should be clearly documented. Objectives in the post-acceptance phase include:

- Establishment of operations and maintenance (O&M) procedures
- Documents storage and modifications to documents defined
- Training the personnel
- Establishment of moves, adds, and changes (MAC) procedures
- Implementation of change control procedures and policies

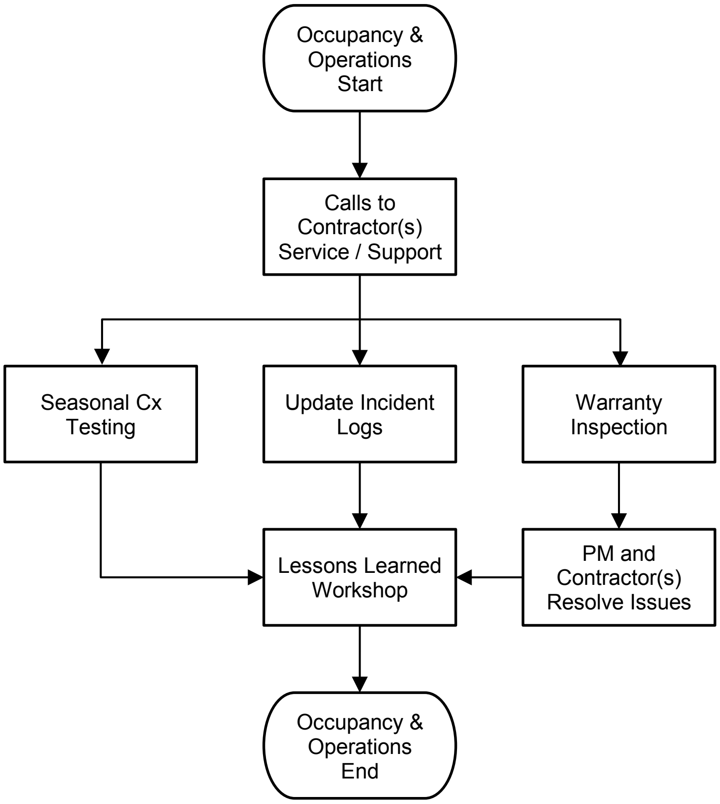

Occupancy & Operations Start
Calls to Contractor(s) Service / Support
Seasonal Cx Testing
Update Incident Logs
Warranty Inspection
Lessons Learned Workshop
PM and Contractor(s) Resolve Issues
Occupancy & Operations End

Figure 16-5
Occupancy and Operations Commissioning Phase Flow Chart

16.6 Commissioning Documents

16.6.1 Introduction

Documentation is one of the primary differentiating aspects for implementing a commissioning process. Thorough documentation prevents random quality control and assurance that often leads to system inefficiencies. Documentation also provides uniform testing protocols for on-going testing procedures and performance analysis. Table 16-1 provides a matrix of commissioning documentation.

Table 16-1 Commissioning Documentation Matrix

Stage	*Document*	*Required by*	*Issued by*	*Revised / Approved*	*Used by*
Pre- Design	Owner´s Project Requirements (OPRs)	Users, O&M, Owner, CxA	Owner, CxA	Owner	CxA, CxT
	Cx Feasibility Study	Owner, CxA	CxA	Owner	CxA, CxT
	Commissioning Plan (CxP)	Owner, DT, CxA	CxA	Owner, DT	Owner, CxA, CxT
	Incidents Registration(log)	CxA	CxA	N/A	CxA, CxT
	Cx Pre-design Stage Process Report	CxA	CxA	Owner	Owner
Design	OPRs update	Users, O&M, Owner, DT	CxA or DT	Owner	CxA, CxT
	Bases of Design (BoD)	DT	DT	CxA	CxA, CxT
	Design Revision and Observations	CxA	CxA	Owner	DT
	Cx´s for Construction specs	Owner, DT, CxA	CxA, System(s) Designer	Owner, CxA	Contractor(s), CxA, DT
	Building Operational Manual (BOM) Index revision	DT, CxA, O&M Contractor(s)	CxA, System(s) Designer	Owner, CxA	DT, Contractor
	Training Needs Alignment / O&M	O&M, User, CxA, DT	Owner or CxA	Owner	DT
	Construction Pre- Functional Tests scheme and checklist	DT, CxA	CxA	CxA, DT	Contractor(s)
	Incidents Registration(log)	CxA	CxA	N/A	CxA, DT
	Cx Plan Update	Owner, DT, CxA, Contractor(s)	CxA	Owner, DT, CxA, Contractor	Owner, DT, CxA, Contractor
	Design Cx Report Stage	CxA	CxA	Owner	Owner, DT
Construction	OPRs Update	Owner, User, DT, CxA, Contractor(s)	Owner, CxA	Owner	CxA, DT, Contractor(s)
	BoD Update	DT	DT	CxA	CxA, Contractor
	Cx Plan update	Owner, DT, CxA Contractor	CxA	Owner, DT, CxA, Contractor(s)	Owner, DT, CxA, Contractor(s)
	Technical Components, Equipment, Systems (Submittals) Revision and Approval Process	Contractor(s)	Contractor(s)	DT, CxA	Contractor(s)
	Equipment list(s) Update	Contractor(s)	Contractor(s)	DT, CxA	Contractor(s)
	Systems Cross Coordination Drawings	DT, Contractor(s)	Contractor(s)	DT, CxA	CxA, Contractor(s)
	Construction Cx Checklist(s)	DT, CxA, Contractors	CxA	DT, CxA	Contractor(s)
	Supervision Reports	Contractor(s)	CxA	Owner, CxA	CxA, Contractors
	Cx Testing Process	DT, CxA, Manufacturer(s)	CxA	DT, CxA	Contractors

Table continues on the next page

Stage	*Document*	*Required by*	*Issued by*	*Revised / Approved*	*Used by*
Construction	Pre-functional Testing Reports	Contractors	CxA	Owner, CxA	Contractor(s)
	Cx Meeting and Documentation	CxA	CxA	All	All
	Training Plan	CxA, O&M Contractor(s)	Contractor(s) Manufacturer(s)	Owner, CxA	O&M, User(s) Contractor(s)
	BOM As-Built	CxA, O&M, Contractor(s), Manufacturer(s)	Contractor(s)	Owner, CxA	O&M, User(s)
	Maintenance Plan	O&M, CxA Contractor(s)	Contractor(s)	Owner, CxA	O&M, User(s)
	Incident Registration (log)	CxA	CxA	N/ A	CxA, DT, Contractor(s)
	Cx report Construction stage	CxA	CxA	Owner	Owner
Occupancy / Operations	OPRs update	Owner, O&M, Users, CxA	DT	Owner, CxA	CxA, DT, Contractor(s)
	Building Operations Manual (BOM) Update	CxA, O&M, Contractor(s)	Contractor(s)	Owner, CxA, O&M	O&M
	O&M Program Update	O&M, CxA, Contractor(s),	O&M	Owner, CxA	O&M, End Users
	Seasonal Testing Process	O&M, CxA, Contractor(s),	Contractor(s)	CxA, O&M	Contractor(s)
	Final Test Reports	O&M, CxA	Contractor(s)	CxA, O&M	O&M, Contractor(s)
	Incidents Registration (Log)	CxA	CxA		Owner, CxA, DT, Contractor(s)
	Cx Process Reports	Owner	CxA	Owner	Owner
	Continuous Cx Plan	CxA, O&M, User(s)	CxA	Owner	Owner, O&M

16.6.2 Owner Project Requirements (OPRs)

This document details the functional requirements of a project and the expectation of how it will be used and operated. It is the base from which all decisions of design, construction, acceptance and operation should be made. It is a living document and can change throughout the entire process of commissioning and shall include at least:

- Owner´s directives
- User´s requirements
- Occupation schedules
- Quality of materials and construction
- Indoor environment quality
- Automation control systems
- Performance criteria
- Environmental and sustainability goals
- Energy efficiency goals
- Comparison of performance requirements
- Adaptability to change
- Health and hygiene
- Acoustics and vibration
- Security

List continues on the next page

- Risk analysis (natural disaster/delinquency /terrorism)
- Estheticians
- Classification program (e.g., LEED, BREEAM, Uptime, EU CoC,)
- Standards, codes and regulations
- Operation and maintenance criteria
- Environmental conditions

16.6.3 Feasibility Commissioning Study

This document should analyze the scope, benefits and costs for commissioning all systems, including verification that all the activities described in this document, are assigned an amount and should define its deliverables.

16.6.4 Project Schedule

This document is developed by the owner and his advisers, provides execution times and shall integrate the concepts of commissioning in it.

16.6.5 Commissioning Plan

This document identifies the processes and procedures for successful commissioning and individual responsibilities of the participants, the program of activities, documentation requirements, communication protocols and reporting assessment procedures. The plan shall contain, but is not limited to, the following:

- Description of activities during the phases of this document
- Formats for process documentation
- Document verification procedures for design
- Procedures to follow when the verification results in non-compliance with OPR
- Schedule of activities according to the project schedule
- Roles and responsibilities
- Commissioning team.
- Reports and testing procedures described in this document
- Procedure required for training
- Proposed schedule of seasonal tests

NOTE: If the above points are properly completed, the plan will be the core of the final commissioning report.

The following systems should be considered for inclusion in the commissioning plan for a data center:

- Electrical systems
- HVAC systems
- Control systems (e.g., BAS)
- Monitoring systems (e.g., BMS)
- Fire protection and suppression systems
- Security systems
- IT infrastructure components and cabling, including LAN, SAN, WAN, management, and BAS/BMS networks
- Grounding systems
- Fuel oil pumping systems
- Inventory monitoring systems
- Leak detection systems
- Systems required by codes or local ordinance to be commissioned
- Critical exhaust and ventilation
- Life safety system

16.6.6 Incident Registration Log

The purpose of this registry is to document all the events that generate a deviation from the OPRs in order to prevent further mistakes in the project.

This format should establish a procedure for documenting design or installation issues that do not comply with the OPRs, maintain control of the unresolved issues, and generate a report of the important issues to be addressed in commissioning team meetings. It shall contain at least:

- Incident identification
- Brief description of the incident
- Identification date
- Name of the team member to solve
- Expected settlement date
- Solution
- Incident and involvement in system performance, time, and cost. Incident classification:
  - Minor incident: It only affects the system where the incident originated without changing operating conditions and performance.
  - Greater incident: Affects the operating conditions and system performance where the incident originated or other systems.
- Actions to prevent recurrence of incidents.

16.6.7 Basis of Design (BoD)

Generated by the design team, the BoD are the documents that specify each of the systems and installations, as well as meeting the OPRs. It is a narrative with initial project data, the considerations that were taken from the OPRs, the basic criteria and evaluated technologies to meet the same OPRs, and shall include at least:

- Owner guidelines
- Systems applicable options
- Criteria for system selection
- Performance criteria for building and systems
- Estimated calculation / dimensioning
- Environmental conditions
- Make and model references
- Assumed operation criteria
- Regulations, codes, standards and reference guides
- System descriptions
- Shall show how each criteria in the OPR is implemented in the design
- Should be developed in simple language for people not trained in engineering
- Modes (normal, emergency, fail and maintenance) and sequences of operation of the systems

16.6.8 Comments on Design Reviews

The purpose of these reviews is:

- To ensure compliance with quality criteria established in the OPR.
- To give feedback in a positive, proactive and concise manner, avoiding value judgments.
- To ensure the design basis is consistent with the RPD.
- To find areas of opportunities to optimize the design.
- To ensure the review is carried out for the coordination of all trades to avoid obstructions, collisions between paths and service spaces.
- To include random review calculation reports, specifications and drawings of each system.

The random check shall be made to 20 percent of the documents of each system. If significant differences are found, another 20 percent should be reviewed. Continuing divergence should require that 100 percent of the documentation of each system be checked, and a full correction of the documentation for each system should be requested.

These documents shall translate comments into the designs for each of the systems and installations. They shall be made at strategic moments in the design stage and should be performed at least twice; at 50 percent and 95 percent of completion.

It is the obligation of the design team to respond to these comment reviews before finishing the design stage.

16.6.9 Construction Specifications for Commissioning

Construction specifications for commissioning establish minimum activities during the Cx construction phase that shall be performed for each system, the purpose of which are included in the scope for contractors. They shall contain:

- Expected runtimes
- Responsibilities
- Lists of measurement instrumentation; properly calibrated
- Documentation requested
- Contractors minimum equipment and material for inspection, testing, startup, operation and maintenance of systems

16.6.10 Building Operations Manual (BOM)

The design stage BOM should be generated to form the structure and minimum requirements of what will be the full BOM. In subsequent stages (construction and occupation), it will be supplemented according to the MAC during the project.

It shall contain at least:

- OPRs
- BoD
- Commissioning plan
- Executives projects and construction documents by system
- Incident registration:
  - Major incidents
  - MAC
- Operation and maintenance manuals generated by contractors
- Training
- Final commissioning report

16.6.11 Guidelines for O&M Training According to Specifications

This document should be integrated based on the requirements set by the designer and manufacturers' manuals. The O&M staff shall revise it and propose any MACs.

16.6.12 List of Test Equipment and Functional Checklist

The design team shall generate a checklist which becomes a guide for the installer that contains specific information for equipment and assemblies required by the OPRs and should include the following:

- Equipment Verification
- Pre-installation Review
- Installation Review

The contractor(s) generates the lists, and the commissioning agent verifies them. This activity it is also known as "pre-functional tests". Verification by the CxA should be performed at 20 percent of the listed equipment and assemblies. If significant differences are found, review another 20 percent. Continuing divergence should require a 100 percent review.

16.6.13 Compliance Technical Data Sheets (Submittals)

Before purchasing equipment and accessories a technical submittal for all equipment shall be issued by the contractor, including the details of what you plan to buy, for review. If approved by the design team, under the supervising commissioning agent, the purchase will be authorized. This review should obtain one of the following results:

- Approved (Ap) – The contractor may purchase them
- Approved with comments (AC) – You can order, but shall respond to comments
- Review and redeliver (RE) – Cannot make the purchase and shall correct the data sheet or the specification that was submitted in the design.

16.6.14 O&M Manual Operation and Maintenance of Systems

As part of the Cx process the submission of detailed documentation for the Operation and Maintenance (O&M) of each of the systems in the building is required, so each contractor shall deliver O&M manuals of the systems installed, containing at least:

- Contractor
- Table of Contents
- Basis of design
- Calculation spreadsheet per system AS BUILT
- Construction documents AS BUILT
- Materials specifications
- Approved Submittals
- Incident registration
- O&M Procedures, both normal operations as planned and unplanned interruption
- Maintenance schedule
- O&M manufacturer´s manual for installed equipment
- Equipment and systems warranties
- Test templates issued and signed by CxA
- Manufacturer and suppliers contact data
- Installation drawings AS BUILT
- Equipment list AS BUILT
- Diagrams and shop drawings AS BUILT
- Operational sequences (normal, fail, emergency and maintenance)
- Digital record of all documentation

16.6.15 List of Equipment

The design team shall deliver the package of project/construction documents, including drawing(s), pictures and tables as necessary, listing the equipment to at least the specificity as described below:

- Identification
- Location in building
- Characteristics
- Physical dimensions
- Brand
- Model
- Technical operational features

NOTE: Once the technical specifications mentioned are approved, if there are changes in some part of the specification, the contractor must update those equipment drawings according to how it was built or installed.

16.6.16 Coordination of Systems Building Plans

Plans should be carried out by level of coordination of the different facilities/systems in which they can identify potential path or location conflicts or interference between them. Each of the systems/facilities shall be indicated in a different color. Once potential conflicts are determined, the design team provides cutouts or sections to determine the heights of each of the possible solutions. Such plans shall be made in a computer-aided design (CAD) program or in a building information modeling (BIM) suite and printed for use as required. It shall be carried out by the design team and confirmed by on-site construction management or the project management team.

16.6.17 Test Procedures

Test procedures should be documented procedures for both pre-functional and functional tests of equipment and systems to ensure that all requirements are met.

NOTE: Testing is a quality assurance process and is a tool to ensure the work is properly done by the contractor.

The CxA shall generate templates for pre-functional and functional tests for recording data in a clear and simple language, sorted by specialty, and specific for each type of equipment. These shall be completed by the contractor performing the work mentioned therein. The will be reviewed by the CxA, following a sampling of 20 percent. If inconsistencies are found, another 20 percent should be reviewed. If the inconsistency persists, the CxA shall review 100 percent of the documentation. The decision of repetition is the responsibility of the owner.

NOTE: It is important that templates and tests aid in detecting the source issue causing the errors rather than provide methods to decrease the incident of errors to an acceptable level for the system.

Test templates shall contain at least:

- Project name, test number, date and time of testing
- Indication whether an original or a repeat of the first test
- Equipment identification of the proven system
- Identification of the measuring equipment and calibration status
- Conditions under which the test is performed
- System performance, equipment or assembly
  - Indicate whether the result meets expectations of the design
  - Signature of the person who developed the test and the team members who supported and witnessed the test along with the date.

16.6.18 Agendas and Minutes of Commissioning Meetings

Agendas shall be filed at the beginning of each meeting of the CxT. The agenda shall include all topics to review. The minutes shall be written and signed, and include agreements reached along with the list of attendees and the date thereof.

16.6.19 Training Plan

A training plan for operation and maintenance of systems and equipment shall be developed and coordinated by CxA with the contractor(s) and the O&M owner's representative that meets the needs and expectations of the owner. Training requirements should be established from the construction documents issued between the design team and the contractor, supported by the vendor or manufacturer, giving a schedule of training sessions. Upon successful completion of the training sessions, the project manager and owner representative will deliver to the contractor a document of training acceptance.

16.6.20 Maintenance Plan

The contractor shall provide at the end of training a maintenance plan which contains for each system recommendations and good practices to be carried out during the lifetime of the systems. This should include a list of parts and recommended spare parts and a schedule for the predictive maintenance and the tendency of systems and equipment that compose it to fail.

16.6.21 Seasonal Testing Procedures

Seasonal testing procedures for each system shall be developed. These procedures shall be carried out under various seasonal conditions over a maximum period of 10 months, or before the expiration of the warranty, whichever comes first. The procedures developed shall include the actual expected performance, along with possible solutions to potential problems that may arise. These should be made using functional tests.

16.6.22 Commissioning Process Report

The commissioning process report shall be drafted by the CxA and include activities and the aforementioned documents and closing reports of each stage. This document terminates the process of commissioning and is to be delivered to the owner.

The following is an outline of the information that should be included in the commissioning report:

- Project name
- Name, address, firm, and telephone number of commissioning authority
- Description of the building:
  - Size
  - Location
  - Use
  - Construction
- HVAC and other installed systems
- List and description of commissioning tasks
- Commissioning plan
- Complete documents
- Completed design intent document

List continues on the next page

- Completed prefunctional test checklists
- Completed functional performance testing reports
- Any outstanding seasonal testing needs
- All noncompliance forms
- Summary of commissioning findings
- Recommendations for system recommissioning
- Recommendations for monitoring the ongoing performance of the system
- Recommendations for system improvements
- Recommendations for establishing trending settings and monitoring activities for ongoing system performance management

16.6.23 Continuous Commissioning Plan

The continuous commissioning plan is a separate document and optional CxP document. It includes everything done in the process of commissioning and described in this document, setting times, responsible and requirements for development; along with activities to follow up on. Basically, it follows the same process, with all activities and documents mentioned and shall be approved by the owner.

16.7 Testing

16.7.1 Introduction

As a quality assurance process, commissioning requires testing at various intervals and in conjunction with the design intent of the project. Functional performance testing is the basis for the commissioning process. The main objective of functional performance tests is to ensure that all systems and equipment are operating efficiently and in accordance with the design intent.

16.7.2 Functional Testing Components

- Equipment description
- Purpose of the test
- Required personnel, tools, and instruments needed to perform the tests
- Design information pertinent to the equipment or system under test
- Detailed sequence of operation, including any operating set points
- Scheduling requirements
- Special instructions or warnings
- Description of expected results
- Sampling strategies

16.7.3 Functional Testing Procedures

- Inspection of equipment for manufacturing and installation defects
- Conditions of test
- Integrated systems test
- What was done to the system to cause a response
- Verification of response
- Comparison of actual response to acceptance criteria

16.7.4 Testing Equipment

16.7.4.1 Requirements

Equipment shall be calibrated according to the manufacturer’s recommendations and whenever suspected of being damaged. Calibration certification shall be kept on record, and copies for each tester provided in turnover documents.

16.7.4.2 Recommendations

Test equipment should be of an accuracy required to test system performance within the tolerances specified by the construction and manufacturer’s documents. Generally, the accuracy of any sensor should be at least twice that of the device being tested.

16.7.5 System Testing

16.7.5.1 Preinstallation Testing

Some subsystems may have components that have been pretested prior to installation. Some components (e.g., video cameras) should have quick functional test performed prior to installation.

Preinstallation tests may:

- Reveal components that have been damaged in shipment and need to be replaced
- Provide the option to calibrate or adjust systems in the shop

16.7.5.2 Preliminary Testing and Calibration

Systems and subsystems should be thoroughly tested and all adjustments and calibrations completed prior to the start of final acceptance testing. This includes the testing of each individual device or component for proper operation and system response.

For example, preliminary testing and calibration of a data center's ESS systems may include testing:

- Each access control device for door prop alarms, forced door alarms, and valid and invalid card reads
- Each alarm point for intrusion detection and video camera call-up and recording
- Video cameras for resolution, light sensitivity, focus, and where applicable, PTZ control
- The functionality and response of the systems' graphical user interface (GUI) system
- Intercom and notification systems for proper operation, sound quality, and intelligibility

16.7.5.3 Burn-in Period

Prior to scheduling the final acceptance test, the commissioning technician should power up and operate each of the systems during a burn-in period. During this burn-in period, each system should be powered and operated for an entire day. A burn-in period could be 2-14 consecutive days or based on client requirements.

Any faults, errors, and noncompliance issues should be corrected prior to beginning the final acceptance testing. Any components or systems that are replaced should also be subject to a burn-in period.

16.7.6 Acceptance Testing

16.7.6.1 Overview

Acceptance testing should be performed after the completion of a successful and complete system burn-in period. As with preliminary testing, acceptance testing should include testing individual devices for proper operation and proper system responses. Acceptance testing is to be complete and test documentation approved by the client prior to the project completion.

16.7.6.2 Plan

Clear acceptance testing guidelines should be provided in the construction specification documents. Those guidelines provided shall define the performance requirements for the system as the acceptance testing plan will be used by the client during the final acceptance test as part of the turnover documentation. The plan should include checklists and procedures with specific areas for recording and documenting all tests and inspections and a summary statement and signature block at the end of the plan.

16.7.6.3 Documentation

16.7.6.3.1 Requirements

Testing documentation shall include full details of all commissioning tests as well as factory testing reports provided by the manufacturer with the equipment.

16.7.6.3.2 Recommendations

The test plan forms and checklists should list any deficiencies and fully document the test results of each acceptance test performed. The client should also document all observed tests and create a punch list of deficiencies that need to be corrected and retested.

16.7.6.4 Retesting Equipment and Systems

16.7.6.4.1 Requirements

The commissioning technician shall correct any deficiencies identified by the client. Upon completion of all corrections, the equipment shall be retested to demonstrate proper operation, integration, and performance.

16.7.6.4.2 Recommendations

Verification of proper system operation and performance should be completed during the preliminary testing stage to avoid retesting. The construction documents should identify who is responsible for labor, materials, and other required support for the supervision and observation of any retesting of failed components or systems.

16.7.7 Electrical System Testing Example

NOTE: See Appendix F for specific examples of PDU, UPS, and generator testing.

For electrical systems, testing typically occurs during the construction and acceptance phases. The following is a typical sequence of testing, though each phase may have a time interval between the completion of one phase prior to the start of the next.

- Level 1—Equipment subject to in-factory testing and certification prior to delivery to the project location.
- Level 2—Equipment installation has been completed and start-up activities are satisfactorily completed by the factory technicians.
- Level 3—Component-level testing.

  Individual electrical system components, like a single generator or UPS power modules are tested. This commissioning step would precede the assembled parallel or complete electrical system testing.
- Level 4
  - Electrical System Functional Testing

    This system-level testing where paralleled or cooperating systems like multiple generators or UPS power modules are tested together as a single unit. This commissioning step would be for electrical systems under a single control system or activity and would precede the complete electrical system testing.
  - Electrical System Operational Testing

    The completed electrical system is tested as a complete and interconnected utility. Unlike electrical system functional testing, this phase of testing examines the entire electrical system to verify the interaction of the various electrical subsystems and to ensure that the electrical system works as a single, coordinated entity. This commissioning step would precede the complete building system testing in Level 5.

  Level 4 should include training and participation of all personnel who will be responsible for any activities during any change of state in the facility power and mechanical systems.
- Level 5—Whole Building Testing.

  Subsequent to the successful functional and operational testing of both the individual or complete electrical and mechanical systems, the entire building's utility infrastructure is examined as a complete system. The goal of this is to validate that the all building utility systems are operating as intended and to verify the proper and expected interactions of those systems (e.g., how the mechanical system responds to a change of state in the electrical system) and to ensure that they work as a single, coordinated entity.

  The building is subjected to the design maximum loads for electrical supply and mechanical cooling/heating. Like previous steps, normal, failure, and maintenance modes of operations are demonstrated. Load response and profiles are typically developed during this phase of the work.

16.8 System Training for Client Staff

16.8.1 Overview

An individual system is a valuable part of the overall solution being provided, with all other integrated systems dependent on proper utilization and operation of each individual system. Therefore, the users should know how to use the entire system properly.

Most system software packages are currently designed around the different roles and job requirements of end users. For instance, some workstation software is written exclusively for the occasional operator who may have the responsibility to occasionally add a user and monitor the alarms that come into the system.

In some cases, software is written exclusively for the administrator who owns the system and is responsible for its operation and all of the integrated systems. A group of users is responsible for maintaining the system. Their work with the software is limited, but they need to be familiar with the hardware. Each group would receive the most value from training that is focused on their everyday tasks.

Manufacturers offer many choices for user training. Because each software application is unique, each training course should be customized to the user's unique needs. This customization should go beyond the content to include class location options. The classes may be held either on the installed system at the end user's location or on test or demonstration equipment at the manufacturer's location.

If the end user has 50 or more users for training, a train-the-trainer program may be more cost effective. This person would get the training, the certificate, and the handout materials from the manufacturer to conduct classes on location. A designer should check with the manufacturer to learn if a train-the-trainer program is offered.

16.8.2 Training Schedules

Scheduling the training is almost as important as the training content. If the training is scheduled too far in advance, the attendees may forget the content because they would not have the opportunity to practice on the system and reinforce the knowledge gained during the class. Last-minute training also should be avoided.

The preferred point in the timeline to do system training is one to two weeks before the system is commissioned and turned over to the customer. The training should be performed on a working system. The training equipment or the installed system can be used in the training.

There is an advantage to training on a live system. Many decisions pertaining to the names and descriptions of door/readers could be determined during training to ensure they make sense to the customer. Simultaneously implemented programming and training reduces the number of hours needed for initial programming and may reduce the number of labor hours charged to the customer. This works best with smaller systems (e.g., 32 readers or less).

Too many control panels and readers may not allow a sufficient time to complete all of the programming during a training session.

If the training courses focus on role-based training, the order of the courses should be carefully considered. The administrator screens should be programmed before the operator screens to facilitate the programming flow. Cross training between the various roles is recommended.

At least two separate instruction sessions should be provided for training the client's operating staff.

The first session is conducted during acceptance testing to provide the initial training needed to operate and maintain the system. The first training session should include:

- General familiarization and operating instructions for each specialty system
- Routine maintenance procedures
- User level programming of software and systems

Instruction on complicated systems and components should be provided by factory-trained technicians.

The second training session should be conducted after the final acceptance to fill in gaps and answer questions that develop once the staff has become familiar with the system.

Each training session should provide all the necessary training materials, including:

- An overview of the implementation and commissioning program
- A description of how the training is to be conducted
- The date, time, and location of the training
- The names and company affiliations of instructors
- A summary of the content
- Recommended reference material

The training sessions should be recorded and archived for repeat training and reference for additional staff. Requirements for system training, training materials, and recordings should be included within the construction documents.

16.8.3 Position or Task Training

The system users may be divided by different roles or job requirements, such as:

- System administrators
- System operators
- Managers
- IT staff
- Maintenance personnel

16.8.3.1 System Administrators

This training generally focuses on the personnel responsible for the system's initial setup and programming. This class teaches the system administrators how to use all the system functions.

These functions may include:

- System parameter programming
- Operator permissions
- Naming conventions for controllers and doors
- Credential holder profile
- Access level assignment
- Identification badge design and production
- Alarm implementation
- Report retrieval
- System backup
- Database archiving

16.8.3.2 System Operators

This training course generally focuses on the occasional users or the personnel responsible for day-to-day operations. This class teaches the system operator to monitor the various functions, including:

- Credential holder profile
- Access level assignment
- Identification badge design and production
- Events—alarm notifications or credential transactions
- Valid or invalid access monitoring
- Alarm response
- Alarm clearance
- Reports
- Manual door opening and closing

16.8.3.3 Managers

This training course generally focuses on personnel who are overseers of the system administrators. The manager would need to know how to delete a user or change the operator or password. This class also teaches:

- Login basics
- System parameter programming
- Operator permissions
- Credential holder profile
- Access level assignment
- Reports

16.8.3.4 Information Technology (IT) Staff

This training course generally focuses on IT department personnel who need to know how systems connect to the LAN or wide area network. The bandwidth and other items, including data requirements, are discussed as well as:

- Network topologies
- Communication to each control panel
- Encryption strategies and capabilities

16.8.3.5 Maintenance Personnel

This training course generally focuses on how the system works and covers:

- Hardware troubleshooting
- System topology
- Networking basics
- Diagnostics
- Simple programming
- Device configurations
- Software troubleshooting

This page intentialloy left blank

17 Data Center Maintenance

17.1 Introduction

Given that the desired availability of a data center or data center systems is typically no less than 99%, insufficient maintenance and maintenance spaces within the data center can contribute to extended unplanned downtime. Additionally, while reducing scheduled downtime for maintenance can aid in obtaining a desired availability level, is not the same as eliminating the time required for the performance of maintenance to reduce the risk of premature equipment or system failure or replacement. Therefore, maintenance requirements should be utilized within the design and planning stages of the data center to assist in meeting performance expectations once the data center is operational.

17.2 Maintenance Plans

17.2.1 Introduction

While maintenance plans are predominantly used during data center operations, the initial maintenance plan should be developed and refined during the design, construction and commissioning phases of a data center to reflect the initial design and any changes that occurred prior to the start of operation.

17.2.2 Maintenance Philosophies

While maintenance is intended to preserve and extend the operational time of equipment or system, there are several maintenance philosophies which provide guidance on scheduling, activities to be performed, and other considerations in meeting maintenance objective. Three common maintenance philosophies are *preventative maintenance*, *predictive maintenance*, and *reliability-centered maintenance*. Depending on the maintenance philosophy chosen, there may be a significantly effect on both the data center's design and the ability to meet its intended operational availability targets.

17.2.2.1 Preventative Maintenance

Preventative maintenance is the most common philosophy of maintenance in use. Through the use of scheduled maintenance activities and additional maintenance based on visual or other defined conditions during a schedule activity, equipment and systems are serviced to preserve reliability prior to the expected failure data.

The following is an example of preventative maintenance schedule and activities for valve-regulated lead-acid (VRLA) batteries.

- Monthly:
  - Visually inspect for evidence of corrosion, container distortion, and dirt
  - Check overall battery float voltages at regular intervals (at least monthly if performed manually; continuous monitoring is recommended)
- Quarterly:
  - Measure and record cell/unit internal ohmic value, temperature, and voltage
- Annually:
  - Measure and record cell-to-cell and terminal connection resistance and measure AC ripple current
  - Compare measurements to base line data, monitor trends, and identify units that fall outside of predicted range (per manufacturer's recommendation)
  - Replace battery units or strings as necessary
  - If UPS is designed with continuously monitored modular battery cartridges, replace when notified by alarm

Preventative maintenance plans can be adjusted for known considerations, such as weather, expected use, and availability of resources, and have varying levels of detail depending on the complexity of the system or equipment being maintained. See BICSI 009 for additional information on preventative maintenance.

17.2.2.2 Predictive Maintenance

Also known as *just-in-time maintenance*, predictive maintenance monitors the conditions of the equipment or system condition to project when maintenance will be required. Predictive maintenance relies on data collection and analysis, which can find systems or equipment in need of adjustment or service from deviations from expected operations or similar equipment in place.

As the status of equipment is often provided by the equipment or the connected system, the collection of data typically does not require operational interruption. system be done while the equipment is in use. Predictive maintenance also improves the ability to plan and prioritize required maintenance activities and materials required, which may minimize delays in completing the maintenance.

17.2.2.3 Reliability-Centered Maintenance

Defined by SAE JA1011, reliability-centered maintenance (RCM) provides a safe minimum level of maintenance by managing the failure modes within a given operating context. RCM incorporates risks to safety, operations, and the maintenance budget within its framework of using maintenance to mitigate risk. For maintenance, RCM recognized five options for the mitigation of risk, which are:

- Preventative maintenance
- Predictive maintenance
- Testing (detective) maintenance
- Operate to failure
- One-time modification

Through risk and criticality of failure analysis, RCM provides a maintenance strategy that address dominant causes of equipment and system and provide guidance on other maintenance activities through criteria such as resource management or cost-effectiveness.

17.2.3 Recommendations

When developing the initial maintenance plan, standards such as BICSI 009 should be used to fully define all aspects of the plan in addition to the information presented here.

The following should be addressed in the creation of a system maintenance plan:

- Identify the maintenance requirements of each system, and ensure that they are conducted as required
- Develop a detailed checklist that tracks maintenance activities as they occur as well as the results of these ongoing checks
- Develop a preventative maintenance program for sensitive systems, devices, or certain restricted areas that may contain sensitive or valuable assets
- Develop effective maintenance contracts that serve both the security contractor and the client
- Develop an ROI that outlines how a nonperforming system may impact the viability of the organization as well as an ROI that details cost savings that occur when the system is able to operate at optimal efficiency
- Utilize intelligence data to justify maintenance and sustainment efforts to management, demonstrating any correlation that might exist that links the available statistics and intelligence data
- Perform a risk analysis that focuses on the organization’s potential exposure and how best to mitigate these exposures with the existing systems

Additional items that may be addressed in a maintenance plan include, but are not limited to:

- Personnel availability and skill set requirements
- Product training, including hands-on familiarization with new products
- Codes, standards, and safety training to maintain skill levels to minimize substandard or unsafe work habits
- Current documentation with detailed records of circuits, optical fibers, and cables
- Cable records maintained for staff to identify potential issues that affect service
- Up-to-date pathway segment records
- Installed equipment baseline—This includes the current version of installed equipment, documented option settings, port configurations, and other information needed for the repair or restoration of individual circuits
- Storage and availability of repair materials—This includes the procedures and process necessary for replenishing materials as they are used. Some quantity of materials must be available to the restoration teams on a 24/7 basis. The maintenance plan must address how this material is to be obtained by the restoration team outside the normal working hours of the support center.
- Initial and sustaining training—The maintenance plan must establish guidelines for training of the initial skill sets necessary for normal operations as well as provide a method for ensuring continued development of the workforce needed. Backup personnel must be available for long-term support and operations.

List continues on the next page

- Restoration procedures—The maintenance plan must establish policies and practices for the routine maintenance and support of the system and demand maintenance response to requirements driven by public demand or natural events. In the event of unplanned system outages along with the policies and practices for routine and demand maintenance, special procedures and policies must be established for emergency or quick system recovery.
- Maintenance schedule for all equipment, including periodic testing and calibration.
- Management escalation procedures with contact information for emergency call out of the workforce.

All maintenance activities should be carefully planned and performed by personnel familiar with the entire system to be maintained as well as with all its interdependencies. As part of the operational maintenance strategy, a plan should be drafted determining the order and sequence of all annual maintenance and testing procedures.

For data centers designed with redundant components or systems (Class 2 or higher), it is especially important not to plan work on primary and secondary components of the same system or mirrored components simultaneously.

17.2.4 Additional Information

Sources of information for maintaining data center systems will vary from codes and standards applicable to telecommunication and electrical systems to manufacturer requirements for specific equipment and specialized systems (e.g., CRAC, access flooring, lock hardware).

17.3 System Maintenance

This section provides general guidelines for the maintenance of systems which may affect the final design of the data center or its systems and does not cover all applicable requirements related to specific system maintenance. Some maintenance issues (e.g., taking systems offline) may be mitigated by designing the system to meet the applicable requirements of Class 3 or higher.

17.3.1 General Requirements and Recommendations

17.3.1.1 Requirements

At a minimum, applicable AHJ requirements and manufacturer's specifications for the system shall be followed for applicable maintenance. Where applicable, system (e.g., electrical, HVAC) maintenance shall be performed by qualified, licensed/bonded/insured technicians who have been trained (and certified when such certification is available) on the specific type of equipment.

17.3.1.2 Recommendations

To minimize the need for unscheduled maintenance, all components of a system should be designed for high reliability. Where possible, components should provide a minimal requirement of downtime for service, whether it is preventive or remedial.

System maintenance should include periodic testing of the systems to ensure that they are operating properly. Backup system testing should be scheduled during off hours, even if the electrical systems are designed to keep all critical loads running when one or more electrical service feeds are shut down as the testing may uncover a defect that causes a system outage.

17.3.2 Electrical Systems Maintenance

17.3.2.1 Introduction

Many electrical systems are required to support a working data center. Some of these systems will require more maintenance than others. Generators, batteries, and UPS systems will require periodic maintenance at manufacturer-specified or industry standard intervals.

NOTE: Appendix I contains a listing of many commonly encountered standards from NFPA, IEEE, and other standards organization for electrical system maintenance.

17.3.2.2 Requirements

All electrical work shall be accomplished in accordance with all applicable codes and safety regulations as mandated by the AHJ.

Certain maintenance functions, such as replacement of hot swappable elements, shall be permitted to be performed by trained operators when the equipment has been so designed and procedures have been specified.

Perform inspections as required by the AHJ, and may include:

- UPS and power generation systems periodic maintenance inspections performed in accordance with manufacturer's specifications and the AHJ

  NOTE: Standards such as NFPA 70B illustrate the importance of Effective Electrical Preventive Maintenance (EPM) and recommend routine maintenance on a semiannual basis for UPS systems, and additional suggestions on what should be inspected, measured, and possibly tested.

- Emergency lighting operational check as required by AHJ
- BAS and fire alarm systems operational check as required by AHJ

Generators shall undergo regular testing to meet AHJ requirements and be maintained per the generator manufacturers' instructions. Testing under a load bank will prevent the potential of jeopardizing the critical load. However, local code may require testing under live load.

NOTE: Standards such as NFPA 110 contain further recommendations for maintenance and testing of generators.

17.3.2.3 Recommendations

Safe performance of electrical maintenance and testing should conform to the manufacturers' procedures. Additionally, perform inspections as specified by the equipment manufacturers.

Inspections and recommendations that are in addition to those that may be required by the AHJ include:

- All power connections secure
- IR thermography scanning is recommended once per year to identify loose or poor connections and unbalanced electrical loads, all characterized by increased resistance or temperature rise
- All receptacles and power strips properly labeled with circuit ID (e.g., PDU ID, RPP ID, breaker position)
- All safety features in place and operational
- Doors and cover plates on panelboards and power distribution units in place and operating properly
- Consider battery monitoring in UPS systems
- Lighting systems checked, and bulbs replaced as required
- Check fuel quality for generators annually
- Inspections should be performed on batteries as recommended by IEEE standards

All electrical equipment should be initially tested after installation and then periodically throughout the life of the equipment. Testing should be performed on the equipment individually and as an integrated system to ensure compatibility and proper interaction between equipment in accordance with the design intent. Frequency of testing shall conform to manufacturer's recommendation as a minimum. Equipment or devices susceptible to significant wear resulting from testing, such as (but not limited to) batteries, should not be subjected to more testing than is recommended by the manufacturer. Testing of equipment or devices performed at high risk should be limited to the recommendation of the manufacturer.

17.3.3 HVAC and Mechanical Systems Maintenance

17.3.3.1 Requirements

HVAC systems shall be maintained according to manufacturer's specifications.

17.3.3.2 Recommendations

Numerous commercially available environmental monitoring tools run on LANs and provide computer room environment reporting to the operations center. Operations personnel can then take preventative measures if computer room conditions begin to approach threshold levels.

All mechanical equipment should be initially tested after installation and then periodically throughout the life of the equipment. Testing should be performed on the equipment individually and as an integrated system to ensure compatibility and proper interaction between equipment in accordance with the design intent. Frequency of testing shall conform to manufacturer's recommendation as a minimum. Equipment or devices susceptible to significant wear resulting from testing, such as (but not limited to) batteries, should not be subjected to more testing than is recommended by the manufacturer. Testing of equipment or devices performed at high risk should be limited to the recommendation of the manufacturer.

17.3.4 Telecommunication Cabling and Infrastructure Maintenance

17.3.4.1 Introduction

Cabling systems, once installed, will normally require very little maintenance, provided the structured cabling system is designed and installed to comply with appropriate codes and standards of the data center location. Properly built cabling systems do not generally break under normal usage without some external force causing breakage.

17.3.4.2 Recommendations

Cable access and having the requisite space to perform maintenance activities are the most important factors to maintenance of structured cabling systems in the data center. Cable pathways and spaces should be designed and built in compliance with applicable standards and follow the recommended cable fill ratios. There should be sufficient space for moves, adds, and changes that will normally occur as changes and reconfigurations take place in the data center.

Cabling systems should be inspected periodically for cable degradation, cracks, abrasions, heat, deformation, brittleness, movement, corrosion, or other indications of abuse and age. In addition to scheduled inspections, when moves, adds, and changes are performed, visual inspection and necessary repair or replacement of cabling and infrastructure should occur.

Sufficient means for cabling management should be provided to minimize patch cable congestion. Patch cable congestion can impede the ability to perform maintenance activities on the structure (e.g., cabinet, rack) or the cabling and equipment contained within.

As some ITE requires front access for maintenance and others require rear access, front and rear access should be provided where equipment may be mounted. for maintenance. Some specialty peripheral equipment, such as robotic tape storage systems, may require front, rear and side maintenance access because of the complexity and size of the internal subsystems and components. Where not otherwise specified, a minimum of 1 m (3 ft) of access space in front and rear is should be provided for maintenance.

Removing front and rear cabinet doors during maintenance is not recommended for:

- Cabinets that rely on ventilation fans installed in the doors
- Cabinets that require the presence of these doors for proper air circulation
- Data centers that rely on lockable/locked cabinet doors to prevent untrained/unauthorized personnel from accessing cabinet contents
- Data centers that require a high aesthetic (e.g., client tours, data center "showcase")

Liquid-cooled cabinets require special procedures for access and maintenance because of high heat loads being generated in these cabinets. Any door open time will need careful planning to reduce the impact of cooling loss on the equipment contained in them.

Where used, access floors should be maintained to prevent floor instability and safety hazards from occurring. Space(s) contained underneath an access floor should be maintained to minimize 1) particulate (e.g., sand, dust) accumulation, 2) the occurrence of contamination (e.g., rust, mold, mildew) and 3) adverse effects on the rooms environmental (e.g., temperature, humidity) levels.

17.3.5 IT Equipment and Systems Maintenance

17.3.5.1 Introduction

IT systems for data centers come in many configurations from small servers that fit in a single rack unit or blade server chassis module to very large multiple processor systems that consume several cabinets and can require a footprint of 1.7 m^2 (18 ft^2) or more.

Maintenance on a small switch usually consists of whole unit removal and replacement when failure is detected. In contrast, a large enterprise class switch will consist of a chassis with multiple "blades" and redundant power supplies. Maintenance on a large switch like this requires removal and replacement of the individual defective "blade" or power supply. Some systems can be ordered with redundant "hot swappable" components that make it possible to run virtually forever without taking a system offline for hardware maintenance.

17.3.5.2 Requirements

All equipment and systems proposed for installation in the data center will have manufacturer-recommended installation specifications that shall be reviewed in advance by planners, configuration managers and facilities managers to help determine the maintenance space required for each respective system installed in the data center. Most equipment and systems will also have maintenance documentation, web-based technical support, or maintenance programs ranging from defective component mail-in replacement to providing on-site maintenance technicians.

Sufficient space to access ITE and for the performance of required maintenance actions shall be provided.

After maintenance actions, cable location and routing shall be restored to minimize patch cable congestion and to a state equal to or better than prior to IUT equipment maintenance.

17.3.5.3 Recommendations

The space provided for the performance of ITE maintenance tasks may be in areas other than where the equipment was mounted, such as a designated location with the computer room or a dedicated space outside of the computer room.

Whether maintenance activities are performed by factory-authorized technicians or trained competent on-site personnel, maintenance plans should adhere to the manufacturer's recommended maintenance plan for proper operation of IT equipment and systems.

17.3.6 Data Center and Building System Maintenance

17.3.6.1 Fire Protection and Fire Suppression Systems

All fire suppression systems should only be maintained by properly trained, certified, and authorized persons.

Standards such as NFPA 2001 and ISO 14520 outlines inspection, maintenance, testing, and training for fire suppression systems and should be adhered to as a guide for maintenance of fire suppression systems unless the local AHJ specifies otherwise.

17.3.6.2 Security Systems

Maintenance policies and procedures listed within the security plan should be included within the maintenance plan. Depending on the established security policy and the complexity of the security systems in use, maintenance of these systems should be performed by on-site security personnel or local security systems contractors.

All maintenance is dependent upon the type of security systems in place and due to the variety of systems available and criticality of the security systems maintenance should only be performed by the appropriate system specialists.

NOTE: Very little preventive maintenance is necessary with most modern systems and is often performed in conjunction with remedial maintenance.

17.3.6.3 Monitoring and Management Systems

Maintenance requirements for monitoring and management systems may be affected by the systems to which they are connected. Maintenance of monitoring and management systems should be performed by trained or authorized personnel for the specific system.

Specific maintenance procedures for integrated systems may be required and should be documented within the maintenance plan.

17.4 Maintenance Recordkeeping

17.4.1 Recommendations

Although maintenance recordkeeping is not mandatory, it is a valuable tool to establish maintenance histories, baselines, and data trending.

Recordkeeping can be a simple as maintaining a paper maintenance log for each device/system under maintenance. However, a maintenance database is a much more efficient way of tracking maintenance information.

Some commercial industrial maintenance software products can be tailored for specific applications such as maintenance tracking or facilities management in the data center.

By using software to track maintenance actions, histories, baselines, and data trending can be established to determine the life cycle of components/systems under maintenance. Histories, baselines, and data trending can help to determine if a particular component(s) or systems are prone to premature failure. Histories, baselines, and data trending aid maintenance personnel in being proactive in maintaining failure prone systems and knowing which parts/components should be on hand and when they can anticipate needing them.

17.5 Service Contracts

17.5.1 Recommendations

A service contract should clearly define the terms and conditions between the organization and the contractor. Using written agreements that specify the scope of work (SoW) eliminates misunderstandings and miscommunications.

The service contract should include the:

- Work to be performed and the frequency of said performance (e.g., weekly, monthly, quarterly)
- Price of the contract for the standard service and cost for additional services that are not part of the standard contract (e.g., after-hours or weekend response)
- Terms on which the contract can be terminated by either party

Although different contractors may be servicing different components of the systems at the same facility, the following information should be included as an integral part of all service contracts:

- Facilities to be covered
- Normal working hours and days on which service work can be performed without impacting the organization's business
- Labor rate per hour and associated materials and parts required for normal serving of the systems to be serviced
- Type of response expected (e.g., callback, physical presence on-site) and time frame required once a service call is placed to the contractor's business
- Method of communicating with the contractor, including calls occurring outside the contractor's normal hours of operation
- Categories of system or device failure matched to an emergency condition
- Detailed list of all the systems and related devices to be serviced under the proposed contract

17.5.2 Example ESS Service Contract Provisions

For example, an ESS contract may include:

- Power supplies.
- Detection devices and their specific location within the facility (e.g., motion detectors, glass break detectors, pull stations, smoke detectors).
- Field and data-gathering panels.
- Servers, workstations, printers, network devices, and related peripheral devices.
- Surveillance cameras, listing types (fixed or pan, tilt, and zoom [PTZ]; Internet protocol [IP] or analog), housings, domes, recording devices, camera controllers, and display monitors.
- Uninterruptible power supply (UPS) and related power conditioning and surge protection devices.
- Electronic door locking devices, listing types (e.g., strike, magnetic lock, electrified mortise handset, shear lock).
- Communication devices (e.g., emergency telephones, two-way intercoms, one-way paging systems).
- Audible and other emergency display devices.

This page intentionally left blank

Appendix A Design Process (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

A.1 Introduction

Communication and documentation are critical in the planning of space, power, and cooling requirements of data centers. Gaps commonly occur due to incomplete communication between disciplines. For example, “watts/m^2 or watts/ft^2” specifications may not be adequate. More specific planning and communication of kW per cabinets of various types, along with the anticipated “end-state” deployment, may lead to higher level of success.

A.1.1 Traditional A/E Design Process

The architectural/engineering (A/E) design process for traditional commercial buildings involves space programming that identifies the various functional areas required. This task is typically performed by the architect or interior designer by interviewing the end users of each of the functional area and surveying the existing spaces occupied by the end user.

Once the “people” space and “people” flow have been identified, the architect or interior designer will work with the various engineering disciplines to determine the appropriate space for the supporting infrastructure (e.g., electrical and mechanical equipment spaces).

When all of the space programming has been completed, the process will then move into the design phases: planning, schematic design, design development, and construction documents.

All of these design efforts are often done without input from IT. However, doing so may result in inadequate telecommunications spaces and pathways to accommodate the desired telecommunications cabling system.

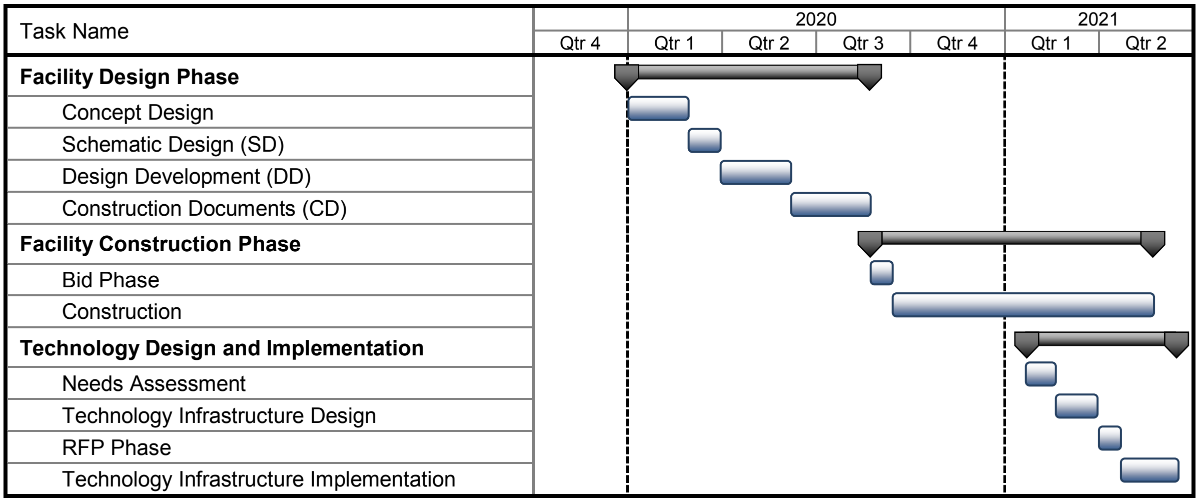


Figure A-1
Traditional A/E Design Process

A.1.2 Traditional Technology Design Process

The technology design process for traditional commercial space often starts after the physical design of the facility has been completed, often weeks afterward.

The technology process includes a needs assessment that identifies the specific technology requirements of each stakeholder.

When the needs assessment has been completed, the technology design moves into the detailed design and RFP development.

Technology design efforts are sometimes done with little or no coordination with the architectural and engineering design teams. However, doing so may result in inadequate telecommunications spaces and pathways to accommodate the desired telecommunications cabling system.

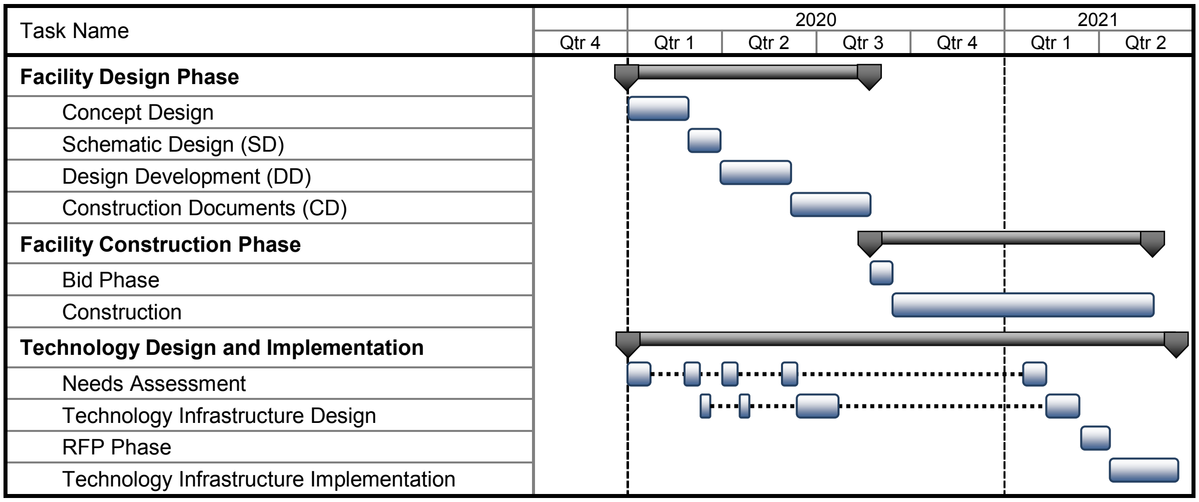


Figure A-2
Data Center A/E Design Process

A.1.3 Data Center Design Process Requirements

A data center is an engineering and technologically complex facility that cannot be approached in a similar manner as traditional commercial space.

The design process must start with a thorough understanding of the technology (network, servers, connectivity) requirements and engineering requirements (power and cooling). The design process for a data center is not focused so much on the "people" space and flow but on the network and computer equipment space and flow. This drives the process to start with the engineering effort before the architectural design effort.

User or application requirements: both user and application requirements tend to drive the reliability of the data center. The design process must gather data regarding the availability and operational requirements of the people and applications supported by the data center and design the space accordingly (see Appendix B for guidance in calculating availability).

A.2 Project Delivery Methods

A.2.1 Design-Bid-Build

The design-bid-build process is a method of project delivery that separates the architectural and engineering design services from construction services.

The end user or owner may hold separate contracts for the design and construction services. The A/E design services and the construction services can both be negotiated or competitively bid in an open or selected market with the responses evaluated with respect to cost, experience, schedule, and any other end user requirement.

The design-bid-build process consists of the entire facility design being completed by the architect/engineering team with the deliverables consisting of a set of construction documents and specifications.

These construction documents (CDs) are then issued to contractors for negotiated or competitive pricing. In a bid environment, the contractors that are allowed to bid are either:

- Invited by the end user
- Selected through a qualification process prior to the issuance of bid documents

The bid documents, prepared based on the user's needs and budget as previously defined, are issued to all contractors interested in bidding.

The architectural/engineering design team will usually be involved in construction administration, which includes periodic site surveys to assess the work progress and compliance with bid documents and specifications.

A.2.2 Design-Build

The design-build process is a method of project delivery in which one entity, the design-builder, provides the architectural, engineering, and construction services all under one contract.

The design-build process starts with a consultant developing the program for the facility to develop the general scope of the project. The general contractor is then selected through either negotiation or competitive bid to complete the design and construction services.

The single entity in the design-build process can be a general contractor, construction management firm, or consulting firm. Each project will result in varying amounts of the scope of work being performed by the single entity. It will be the single entity's responsibility to bring together a team that has the experience to complete the project as required by the end user.

The design-build project delivery method has often been used when the schedule is a primary driver for a successful project. It is also acceptable when schedule is not an issue.

Further information can be obtained from the Design-Build Institute of America website (www.dbia.org).

A.2.3 Construction Management

The construction management (CM) project delivery model can be a fee-based service or an at-risk based service. The construction manager is responsible to, and under contract exclusively with, the owner. The construction manager represents the owners' interests throughout the various phases of the project.

The CM model is similar to the design-bid-build model in that there is a separation of the architectural and engineering design services from the construction services. It is also similar to the design build model in that the CM represents the constructor's perspective throughout the design process, but the CM is solely responsible to the owner and does not have any financial incentive through value engineering during the construction phase.

To obtain the greatest advantage of the CM delivery model, the owner should engage the CM very early in the project at the concept development design phase.

The CM delivery model provides flexibility to the owner in procuring the construction services:

- The owner can procure the construction services, managed by the CM, with a single contract where the general contractor and subtrades are all under contract through one prime contractor.
- The owner can also procure the construction services with multiple contracts where the general contractor and significant subtrades (electrical and mechanical) are under separate contracts directly with the owner; the multiple contracts with the owner would be managed by the CM.

The fee-based CM model is where the CM is under contract to the owner for a fixed fee and all construction contracts are negotiated between the owner and the contractors.

The “at-risk” based CM model is where the CM commits to the owner the delivery of the construction project with a guaranteed maximum price or GMP. This model is similar to the CM acting as a construction consultant to the owner during the design phase and as a prime general contractor during the construction phase.

NOTE: Further information can be obtained from the Construction Management Association of America (http://cmaanet.org).

A.3 Facility Design Phases

A.3.1 Planning and Concept Development

The following tasks are commonly included within the planning phase:

- Data center IT and telecommunications infrastructure requirements documents
- Facility programming
- Space relationships/flow diagrams
- Project development scheduling
- Project budgeting
- Life cycle cost studies
- Economic feasibility studies
- Agency consulting/review/approval
- Site selection/analysis utilization
- Environmental studies as well as city or county requirements and permit requirements
- Power requirements and availability
- Energy studies
- Existing facilities surveys
- Client-supplied data coordination
- Services related to project management
- Presentations
- Marketing studies
- Project financing
- Special studies
- Re-zoning assistance
- Project promotion
- Legal survey
- Geotechnical analysis

A.3.2 Schematic Design (SD)

The following tasks are commonly included within the schematic design phase:

- Client-supplied data coordination
- Program and budget evaluation
- Review of alternative design approaches
- Architectural schematic design
- Schematic design drawings and documents
- Statement of probable construction costs
- Client consultation
- Interior design concepts
- Special studies (e.g., future facilities, environmental impact)
- Special submissions or promotional presentations
- Special models, perspectives, or computer presentations
- Project management
- Agency consultation
- IT and telecommunications infrastructure conceptual design documents
- Structural design concepts
- Mechanical design concepts

List continues on the next page

- Electrical design concepts
- Civil design concepts
- Landscape concepts
- Statements of probable costs

A.3.3 Design Development (DD)

The following tasks are commonly included within the design development phase:

- Client-supplied data coordination
- Design coordination
- Architectural design development
- Design development drawings and documents
- Client consultation
- Interior design development
- Special studies/reports (e.g., planning tenant or rental spaces)
- Promotional presentations
- Models, perspectives, or computer presentations
- Project management
- Agency consultation
- IT and telecommunications infrastructure detailed design documents
- Structural design development
- Mechanical design development
- Electrical design development
- Civil engineering design development
- Landscape development
- Detailed construction cost estimates or quantity surveys
- Cost estimate reconciliation with budget

NOTE: Further information can be obtained from the Design-Build Institute of America (http://www.dbia.org/).

A.3.4 Prepurchase

- Define list of long lead items
- Prepare specifications for prepurchase items
- Bid or procure items ahead of issuance of facility construction documents because of possible long lead material cost increases

A.3.5 Construction Documents (CD)

The following tasks are commonly included within the construction documents phase:

- Client-supplied data coordination
- Project coordination
- Architectural construction documents (working drawings, form of construction contract and specifications)
- Document checking and coordination
- Client consultation
- Interior construction documents
- Alternative bid details and special bid documents
- Project management
- Agency consultation
- Low-voltage/telecommunications cabling system bid documents
- Structural construction documents
- Mechanical construction documents
- Electrical construction documents
- Statements of probable costs
- Civil engineering construction documents

List continues on the next page

- Landscape documents
- Detailed construction cost estimates or quantity surveys
- Cost estimate reconciliation with budget

A.4 Technology Design Phases

A.4.1 Needs Assessment

The following tasks are commonly included within the needs assessment phase:

- Develop a project plan that will outline the tasks, timeframes, and responsibilities for completing the technology project.
- Conduct information gathering sessions identifying and documenting the technology and business needs.
- Review the existing technology systems.
- Interview IT and facilities personnel and determine the group(s) that will be responsible for each portion of the data center infrastructure when the project is complete.
- Review anticipated growth and new technologies.
- Review timeframes, capital, and operational budgets.
- Develop data center IT/Telecommunications infrastructure requirements document.
- Develop a business case for recommendations made during needs assessment analysis.

A.4.2 Design Analysis

The following tasks are included within the design analysis phase:

- Review, evaluate, and prioritize all of the information received and documented during the needs assessments phase
- Validate vendor qualification criteria, technology applications, required infrastructure, industry standards and best practices, budgets and other pertinent information with project stakeholders
- Develop conceptual design for data center IT and telecommunications infrastructure

A.4.3 Acquisition

The following tasks are included within the acquisition phase:

- Develop the detailed IT and telecommunications infrastructure design.
- Draft the RFP for the technology vendor services, including detailed specifications and drawings. The RFP should also include the project organization, expected milestone schedule, current construction schedule, and responsibility matrix.
- Analyze and evaluate all bid responses for accuracy and completeness and financial, technical, and service qualifications.
- Assist in the selection process and final contract review and negotiations.

A.4.4 Implementation

The following tasks are included within the implementation phase:

- Provide project management services to facilitate the implementation of the technology vendor’s service contract.
- Facilitate regularly scheduled status meetings to review procedures and processes, maintenance records, and documentation submitted by vendor to ensure that the end user is receiving the service and support as outlined in the service contract.
- Assist end user in measuring and benchmarking services provided by the technology vendor.

A.5 Commissioning

The following tasks are included within the commissioning phase:

- Request design intent document from A/E of record that is reflective of original basis of design identified in concept documents.
- Request sequence of operation for electrical and mechanical components.
- Validate alignment between sequence of operations and controls methodology; review SCADA and building automation system topology and sensor locations.
- Prepare system readiness checklists to be signed off by contractors prior to startup of individual components.
- Prepare verification test procedures for each component in each system and record anomalies encountered.
- Conclude commissioning testing with integrated system test for normal, failure, and maintenance modes; apply simulated loads, such as server simulator load banks, to fully test the entire data center load carrying components.
- Conclude commissioning phase with a lessons learned report that serves to benchmark the operation of electrical and mechanical systems. The corrective action report would also be prepared during this phase.

A.6 Data Center Documentation

A.6.1 Recommendations

Data center documentation should include:

- Construction and implementation:
  - Contract documents:
    - Request for bid/quote
    - Project schedule
    - Specifications
    - Floor plan drawings
    - Outside plant drawings
    - Telecommunications cabling system drawings
    - Equipment layout drawing and details
    - Cabinet and rack elevations
    - Cable pathway details
    - Construction change orders
  - As-built drawings
  - Construction administration reports
  - Test reports
  - Punch-list reports
  - Operations and maintenance (O&M) manuals
  - Close-out, sign-off, and acceptance certificates
  - Certificate of occupancy
- Ongoing change management documentation, including system inventories and configuration databases. These may also be used as a starting point for relocation planning documentation.
- Relocation planning documentation such as equipment, system, and application inventories, including system and application dependencies.

A.7 Existing Facility Assessments

When existing facilities are planned to be used within a data center design, failure to perform adequate surveys and assessments of the existing facility can cause cost-overruns, project delays and impair the data center from operating at its intended capacity and performance level. When performing assessments on existing facilities, the following items should be assessed, with the findings used to inform design decisions:

- Business continuity
  - Identify current capacity and maximum capacity levels of data center
  - Review current and maximum capacity rating against client's current needs
  - Review disaster recovery plans and resiliency to major outages and disasters against client's current needs
- State of the building and architectural elements
  - Physical security of data center (e.g., electronic systems, architectural security, bollards)
  - Structural and architectural (e.g., access floor, lift) loading limits
  - Sizing and dimensions of equipment delivery paths
- State of the data center's primary systems (e.g., mechanical, electrical, connectivity)
  - Review existing utility services (e.g., availability and cost of power, infrastructure, water, gas)
  - Review current system and component availability against original intended design and client need
  - Review current system efficiency rating against original intended design and client need
  - Review existing equipment for supportability, age, maintainability, and warranty
  - Identify aging technology and items needing a "refresh"
- State of secondary and ancillary systems
  - Review systems against original intended design and client need
  - Review existing equipment for supportability, age, maintainability, and warranty
- Operational performance
  - Assess operational performance against original intended levels and client need
  - Review current state of the data center operational procedures (e.g., personnel, policies, maintenance operations procedures) as applicable to design factors
  - As needed,
    - Review current state of the data center physical security (e.g., incident reports, surveillance systems, access control logs)
    - Review operations documentation
    - Review and assess safety procedures (e.g., lock out/ tag out procedures) and documentation

While these items are part of a data center assessment for design, these items can also be used in documenting a current data center's status and identification of areas that are no longer meeting intended design or client requirements.

Appendix B Reliability and Availability (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

B.1 Introduction

B.1.1 Overview

People have come to expect ready access to information 24 hours a day, every day. The Internet as well as more traditional enterprises—both business and governmental—now operate 7 days a week, 24 hours a day. Typical 24/7 operations include banking systems, credit card companies, 911 emergency centers, telecommunications networks, hospital systems, overnight delivery operations, large multinational concerns, and other international organizations. With the increased reliance on 24/7 availability of information and data processing support, the reliance on mission-critical data centers has also increased.

However, the mission-critical data processing center requires additional thought and planning, because of its differences with a conventional building (e.g., home, store, office building). Consider some data center and mission-critical facility norms:

- Mission-critical power requirements far exceed any conventional building type. The power supplied to a typical office building is about 110 W/m^2 (10 W/ft^2) while mission-critical facilities often require power between 650 W/m^2 (60 W/ft^2) and 2200 W/m^2 (200 W/ft^2), if not more.
- The ratio of combined mechanical and electrical service space to the overall usable space is typically between 1:3 and 1:4 in a conventional building, but it is close to 1:1 for data centers.
- The cost of mission-critical facilities can run up to four times the cost of more conventional building types as power and cooling requirements drive the cost and design.

These numbers are revealing. Mission-critical power, cooling and network systems evolved from a philosophy dubbed "system + system", meaning that for every critical system, a duplicate system is in place to provide service while the other is repaired, maintained, or tested off-line. Additionally, the risk of natural and provoked disasters causing potential IT downtime dictates a hardened building shell as well as sufficient capacity on site.

Continuous operation implies that critical systems need a measured approach to incorporating reliability with redundant systems being the typical method used. After all, a shutdown can cripple the revenue generating continuity of a business, ruin customer confidence, and possibly threaten its existence if the shutdown is extensive. Disruption to the IT systems underpinning today's industrialized societies may cause loss of life and endanger communities, depending upon the nature and location of the service.

Mission-critical services requiring 7 day at 24 hours/day operations need a comprehensive strategy to sustain their vital activities. Many small businesses have at least a 5 day at 12 hour/day high-availability operating requirement—less rigorous standards, yet still substantial. Mission-critical design variations will stem from each user's requirements. Starting with site selection criteria and working forward through each layer of architectural, engineering, network, IT systems, and operational design, reliability and reducing the risk of downtime must be the prime focus that is weighed and coordinated throughout the design process.

Mission-critical data centers have not traditionally been high-profile projects, yet their design issues are increasingly complex and critical. With an emerging design terminology and vocabulary, their rapid evolution calls for an exceptional degree of building and IT systems coordination and integration. These data centers are not merely warehouses for servers; instead, they rival medical operating rooms or semiconductor plants, with their precise environmental controls and power requirements. Intense, sustained work shifts with employees monitoring computer screens mean that workplace design issues must also be addressed.

Important facility design considerations also extend well beyond the context of the mission-critical building itself. Utility deregulation is causing uncertainty. Increasing power demands challenge reliability of the power supply itself. Some utilities even question their own capacity to power mission-critical facilities. Because IT plants can be highly sensitive to temperature and power fluctuations, these concerns are attracting increased attention. It is not an issue that can be addressed simply through the purchase of UPS systems.

To increase the likelihood of success of a mission-critical facility, required performance levels of availability and reliability should be defined, prior to the start or formalization of the design, procurement, and maintenance requirements and processes. Failure to define performance and availability levels prior to the project start often yields higher construction, implementation, and operational costs as well as inconsistent and unpredictable performance.

B.1.2 Goals and Objectives

This appendix presents an overview for planning mission-critical data centers with the following strategic goals:

- Establish a consistent, cost-effective process
- Develop optimum design and implementation solutions
- Develop a common enterprise-wide design vocabulary
- Establish performance criteria used to generate or evaluate mission-critical data center services.

Additionally, this appendix provides a method for determining data center criticality, which aids in the alignment of project objectives and budgets with appropriate performance levels. It should be noted that the recommendations reached by using this method can then be presented to management for determining if the cost of implementation can be justified.

The information and method presented within this appendix does not address business continuity requirements. For example, an enterprise may be better served by multiple data centers of lower Availability Class (See Section B.6) than a single data center of a higher Availability Class.

NOTE: Information on multiple data center architectures can be found in Appendix E.

B.2 Creating Mission-Critical Data Centers Overview

There are four stages in the process of designing a new mission-critical data center or upgrading an existing one. These are represented in Figure B-1 and described afterward.

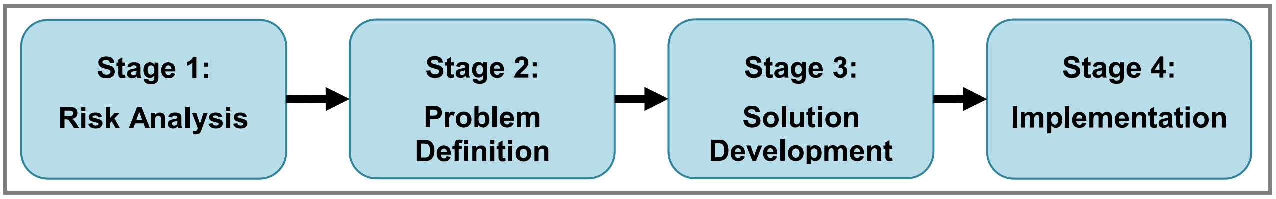


Figure B-1
Planning Process for a Mission-Critical Facility

- Stage 1: Risk Analysis
  Risk analysis is a linear process. Three key characteristics are defined to arrive at an expression of the criticality of a mission-critical data center:
  - Identify operational requirements for the section of the data center under analysis—the opportunity to suspend operations for scheduled maintenance
  - Identify availability requirements—the targeted uptime of the systems or zones during operations and the ability to endure unplanned interruption of operations
  - Define the impact of downtime—the consequences of unplanned disruptions on the mission

  The process of analyzing and mitigating risk is described in Section B.3. Risk analysis also serves as an important reference source for the remaining three stages of creating a mission-critical data center.
- Stage 2: Problem Definition
  After completing risk analysis, characterize the data center in terms of computer room space, power, and cooling capacity required to support IT hardware (which may be used to define ITE density) and anticipated redundancy requirements. This information is usually documented in the data center concept design.
- Stage 3: Solution Development
  Convert the data center conceptual design into one or more design solutions to solve the specific design problem and meet the objectives of the targeted Availability Class.

List continues on the next page

- Stage 4: Implementation
  Construct the chosen solution, incorporating implementation tactics consistent with the targeted Availability Class. This will include appropriate maintenance and operations procedures to ensure a sustainable level of availability.

The remainder of this appendix pertains to risk analysis and the methodology for selecting data center design Availability Classes.

B.3 Risk Analysis

It is impossible to eliminate the risk of downtime, but risk reduction is an important planning element. In an increasingly competitive world, it is imperative to address downtime in business decisions. The design of systems supporting critical IT functions depends on the interaction between the criticality of the function and its operational profile.

Criticality is defined as the relative importance of a function or process as measured by the consequences of its failure or inability to function. The operational profile expresses the time intervals over which the function or process must operate.

To provide optimal design solutions for a mission-critical data center, consider several key factors. NFPA 75 identifies seven considerations for protection of the environment, equipment, function, programming, records, and supplies in a data center. These include:

- What are the life safety aspects of the function? For example, if the system failed unexpectedly, would lives be put at risk? Examples of such applications include automated safety systems, air traffic control, and emergency call centers.
- What is the threat to occupants or exposed property from natural, man-made, or technology-caused catastrophic events? Will the building be:
  - Equipped with fire suppression?
  - Located within a flood zone?
  - Require seismic reinforcement or dampening because of ground stability and vibration transmission?
  - Located within a tornado or hurricane “corridor”?
- What would be the economic loss to the organization from the loss of function or loss of records?
- What would be the economic loss to the organization from damaged or destroyed equipment?
- What would be the regulatory or contractual impact, if any? For example, if unplanned downtime resulted in loss of telephone service or electrical service to the community, would there be penalties from the government?
- What would be the impact of disrupted service to the organization’s reputation? For example, would subscribers switch to a competitors’ service?
- What is the access to redundant off-site processing systems (e.g., “high performance computing”, massively paralleled systems, cloud service provider, disaster recovery site, backup data center)?

The methodology presented in Section B.5 for determining a data center’s facility Availability Class integrates these considerations and defines the appropriate risk management strategy.

B.4 Availability

B.4.1 Introduction

Availability is the probability that a component or system is in a condition to perform its intended function. While similar to *reliability*, availability is affected by more events than a failure requiring repair or replacement of a component or system.

B.4.2 Calculating Availability

While there are different formulae to calculate availability for calculations involving systems, availability, in its simplest form, is the ratio of uptime observed during a specified interval over the total time of that interval (Equation B-1).

$$\text{Availability} = \frac{\text{Uptime within Observation Interval}}{\text{Total Time of Observation Interval}} \qquad \text{(B-1)}$$

While equation B-1 can generate the availability of a system, the result does not provide information which can be used to improve the observed value. By splitting total time into its two primary elements (uptime and downtime), the equation changes to the form shown in equation B-2.

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \quad \text{(B-2)}$$

While equation B-2 proves mathematically what is known through observation or experience (reductions in downtime increases availability), downtime itself can be split into two types: scheduled and unscheduled.

When the two types of downtime are inserted into equation B-2, the resultant equation is shown in equation B-3.

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Scheduled Downtime} + \text{Unscheduled Downtime}} \quad \text{(B-3)}$$

Thus, equation B-3 shows that availability can be increased by reductions in one or both types of downtime.

B.4.3 Types of Downtime

B.4.3.1 Scheduled Downtime

Scheduled downtime contains activities or events such as:

- Preventive maintenance
- System and equipment setup and upgrades
- System testing/optimization
- Scheduled facilities related events
- Remedial maintenance

B.4.3.2 Unscheduled Downtime

Unscheduled downtime events include:

- Repairs due to failure
- Maintenance delay
- Facility-related failures/outages

B.5 Determining the Data Center Availability Class

B.5.1 Overview

While there are innumerable factors that can be evaluated in a mission-critical data center, there are three factors that can quickly be quantified, providing for an easy determination of an Availability Class and the necessary functions and features required for data center services. These factors are:

- Operational requirements
- Operational availability
- Impact of downtime

Paying careful attention to these factors determines an appropriate Availability Class that matches the mission-critical data center cost with the functions it is intended to support.

Figure B-2 shows how these factors interact in determining the data center services Availability Class with these factors and how to determine an Availability Class described in Sections B.5.2−B.5.5.

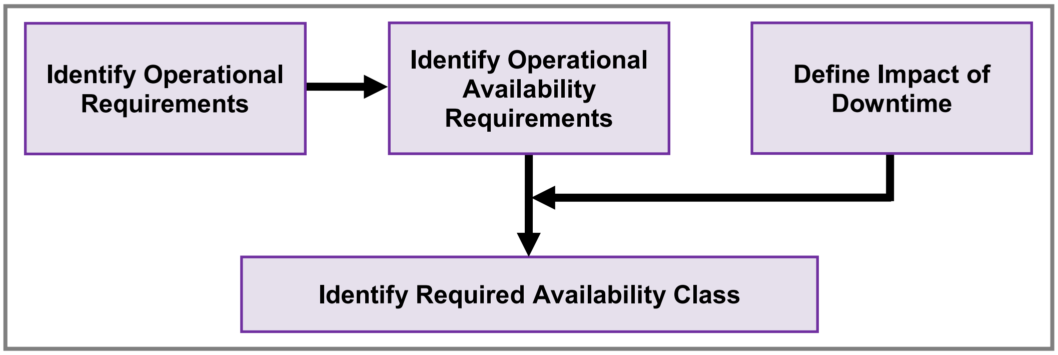

Identify Operational Requirements
Identify Operational Availability Requirements
Define Impact of Downtime
Identify Required Availability Class

Figure B-2
Relationship of Factors in Data Center Services Availability Class

B.5.2 Identify Operational Requirements

The first step in determining the Availability Class associated with mission-critical data center services is to define the data center's intended operational requirements. Sufficient resources must be available to achieve an acceptable level of quality over a given time period. IT functions that have a high-quality expectation over a longer time period are by definition more critical than those requiring less resources, lower quality, and/or are needed over a shorter time period.

While there are many factors in operations, the key factor to be assessed in this step is the amount of time to be provided for testing and maintenance activities that disrupt normal operation. This is often known as *planned maintenance shutdown*. Once the time for planned maintenance shutdowns is known, this value can be used within Table B-1 to determine an Operational Level. The value of time used should not include projections for unplanned repairs or events. The indicated Operational Level is used in the next step (see Section B.5.3).

Table B-1 Identifying Operational Requirements: Time Available for Planned Maintenance Shutdown

Operational Level	*Annual Hours Available for Planned Maintenance Shutdown*	*Description*
0	> 400	Functions are operational less than 24 hours a day and less than 7 days a week. Scheduled maintenance down time is available during working hours and off hours.
1	100-400	Functions are operational less than 24 hours a day and less than 7 days a week. Scheduled maintenance down time is available during working hours and off-hours.
2	50-99	Functions are operational up to 24 hours a day, up to 7 days a week, and up to 50 weeks per year; scheduled maintenance down time is available during working hours and off hours.
3	0-49	Functions are operational 24 hours a day, 7 days a week for 50 weeks or more. No scheduled maintenance down time is available during working hours.
4	0	Functions are operational 24 hours a day, 7 days a week for 52 weeks each year. No scheduled maintenance down time is available.

NOTE: The term *shutdown* means that operation has ceased; the equipment is not able to perform its mission during that time. Shutdown does *not* refer to the loss of system components if they do not disrupt the ability of the system to continue its mission.

B.5.3 Quantify and Rank Operational Availability Requirements

The second step in determining the Availability Class is to identify the data center's operational availability requirements, specifically the total uptime that the data center services must support without disruption. The term *availability* includes that ITE is operational and able to perform its function; it does not solely refer to operation of the supporting infrastructure. Operational availability refers only to scheduled uptime—that is, the time during which the IT functions are actually expected to run.

These operational availability requirements are reflected by the determination of an Operational Availability rating. By using the Operational level determined in the previous step (See Section B.5.2) and indexing that value with the allowed maximum annual downtime within Table B-2, an Operational Availability Rating is indicated.

NOTE: The Operational Availability Rating is used in conjunction with information from the next step (See Section B.5.4) to determine the Data Center Availability Class (shown in Section B.5.5).

Table B-2 Identifying Operational Availability Rating: Maximum Annual Downtime (Availability %)

	Allowable Maximum Annual Downtime (minutes) *Availability as %* *Nines of Availability*				
Operational Level *(from Table B-1)*	*x > 5000* *x < 99%* *2-9's*	*5000 ≥ x > 500* *99% ≤ x < 99.9%* *3-9's*	*500 ≥ x > 50* *99.9% ≤ x < 99.99%* *4-9's*	*50 ≥ x > 5* *99.99% ≤ x < 99.999%* *5-9's*	*5 ≥ x* *99.999% ≤ x* *6-9's*
Level 0	0	0	1	2	2
Level 1	0	1	2	2	2
Level 2	1	2	2	2	3
Level 3	2	2	2	3	4
Level 4	3	3	3	4	4

The cost of downtime must be weighed against the cost of mitigating risks in achieving high availability. Note that less than a second of power interruption or a few minutes of cooling interruption can result in hours of recovery time. Thus, the objective is to identify the intersection between the allowed maximum annual downtime and the intended operational level. A function or process that has a high availability requirement with a low operational profile has less risk associated with it than a similar function with a higher operational profile.

B.5.4 Determine Impact of Downtime

The third step in determining the Availability Class is to identify the impact or consequences of downtime. This is an essential component of risk management because not all downtime has the same impact on mission-critical data center services. Identifying the impact of downtime on mission-critical functions helps determine the tactics that will be deployed to mitigate downtime risk. As shown in Table B-3, there are five impact classifications, each associated with a specific impact scope.

B.5.5 Identify the Data Center Availability Class

The final step in determining the data center Availability Class is to combine the three previously identified factors to arrive at a usable expression of availability. This expression of availability is used as a guide to determine the facility (architectural and engineering) and IT (network, cable plant, computer processing and storage system) features needed to appropriately support critical IT functions. Since operational level is subsumed within the availability ranking, as explained in Section B.5.3, the task is to matrix the availability ranking against the impact of downtime to arrive at an appropriate Availability Class. Table B-4 shows the intersection of these two values, and the resultant Data Center Availability Class.

Table B-3 Classifying the Impact of Downtime on the Mission

Classification	*Description – Impact of Downtime*
Isolated	Local in scope, affecting only a single function or operation, resulting in a minor disruption or delay in achieving non-critical organizational objectives.
Minor	Local in scope, affecting only a single site, or resulting in a minor disruption or delay in achieving key organizational objectives.
Major	Regional in scope, affecting a portion of the enterprise (although not in its entirety) or resulting in a moderate disruption or delay in achieving key organizational objectives.
Severe	Multiregional in scope, affecting a major portion of the enterprise (although not in its entirety) or resulting in a major disruption or delay in achieving key organizational objectives.
Catastrophic	Affecting the quality of service delivery across the entire enterprise or resulting in a significant disruption or delay in achieving key organizational objectives.

Table B-4 Determining Data Center Services Availability Class

Impact of Downtime (from Table B-3)	*Operational Availability Rating (from Table B-2)*				
	0	*1*	*2*	*3*	*4*
Isolated	**Class 0**	**Class 0**	**Class 1**	**Class 3**	**Class 3**
Minor	**Class 0**	**Class 1**	**Class 2**	**Class 3**	**Class 3**
Major	**Class 1**	**Class 2**	**Class 2**	**Class 3**	**Class 3**
Severe	**Class 1**	**Class 2**	**Class 3**	**Class 3**	**Class 4**
Catastrophic	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 4**

B.6 Data Center Availability Classes

To a great degree, design decisions are guided by the identified Availability Class. Therefore, it is essential to fully understand the meaning of each Availability Class. Each Availability Class is defined in terms of four areas of concern:

1) **Component redundancy** increases reliability by providing redundancy for critical high-risk, low-reliability components within systems.
2) **System redundancy** increases reliability even more by providing redundancy at the system level.
3) **Quality** ensures that high quality is designed and implemented in the data center, thereby reducing the risk of downtime due to failure during initial installation and/or premature wear. Since MTBF is a major factor in the determination of system reliability, it stands to reason that higher quality components with lower failure rates will result in systems that are more reliable.
4) **Survivability** refers to reducing the risk of downtime by protecting against external events such as physical forces, security breaches, and natural disasters.

The following subsections provide more detail on how each of these four factors is defined for each of the five Availability Classes. Each Class also includes an example application for facility power.

NOTE: Facility power in the examples below uses the prefix “F”, as listed Section B.7.

B.6.1 Availability Class 0

The objective of Class 0 is to support the basic requirements of the IT functions without supplementary equipment. Capital cost avoidance is the major driver. There is a high risk of downtime because of planned and unplanned events. However, in Class 0 data centers maintenance can be performed during non-scheduled hours, and downtime of several hours or even days has minimum impact on the mission.

Table B-5 Tactics for Class 0

Component redundancy:	None
System redundancy:	None
Quality control:	Standard commercial quality
Survivability:	None
Application:	A critical power distribution system separate from the general use power systems would not exist. There would be no back-up generator system. The system might deploy surge protective devices, power conditioning, or even small or non-redundant uninterruptible power supply (UPS) systems to allow the specific equipment to function adequately. Utility grade power does not meet the basic requirements of critical equipment. No redundancy of any kind would be used for power, air conditioning, or networking for a similar reason. Class F0 has multiple single-points of failure.

B.6.2 Availability Class 1

The objective of Class 1 is to support the basic requirements of the IT functions. There is a high risk of downtime because of planned and unplanned events. However, in Class 1 data centers, remedial maintenance can be performed during nonscheduled hours, and the impact of downtime is relatively low.

Table B-6 Tactics for Class 1

Component redundancy:	None
System redundancy:	None
Quality control:	Standard commercial quality
Survivability:	None
Application:	In Class F1, the critical power distribution system would deploy a stored energy device and a generator to allow the critical equipment to function adequately (utility grade power does not meet the basic requirements of critical equipment). No redundancy of any kind would be used for power or air conditioning for a similar reason.

B.6.3 Availability Class 2

The objective of Class 2 is to provide a level of reliability higher than that defined in Class 1 to reduce the risk of downtime because of component failure. In Class 2 data centers, there is a moderate risk of downtime as a result of planned and unplanned events. Maintenance activities can typically be performed during unscheduled hours.

Table B-7 Tactics for Class 2

Component redundancy:	Redundancy is provided for critical components
System redundancy:	None
Quality control:	Premium quality for critical components
Survivability:	Moderate hardening for physical security and structural integrity
Application:	In Class F2, the critical power, cooling, and network systems would need redundancy in those parts of the system that are most likely to fail. These would include any products that have a high parts count or moving parts, such as UPS, controls, air conditioning, generators, ATS or systems that are outside the control of the data center management such as network access carrier services. In addition, it may be appropriate to specify premium quality devices that provide longer life or better reliability.

B.6.4 Availability Class 3

The objective of Class 3 is to provide additional reliability and maintainability to reduce the risk of downtime because of natural disasters, human-driven disasters, planned maintenance, and repair activities. Maintenance and repair activities will typically need to be performed during full production time with no opportunity for curtailed operations.

Table B-8 Tactics for Class 3

Component redundancy:	Redundancy is required for critical and noncritical components, except where the component is part of a redundant system; redundancy is also provided to increase maintainability.
System redundancy:	System redundancy is required where component redundancy does not exist
Quality control:	Premium quality for all components
Survivability:	Significant hardening for physical security and structural integrity
Application:	In Class F3, the critical power, cooling, and network systems must provide for reliable, continuous operations even when major components (or, where necessary, major subsystems) are out of service for repair or maintenance. To protect against unplanned downtime, the power, cooling, and network systems must be able to sustain operations while a dependent component or subsystem is out of service.

B.6.5 Availability Class 4

The objective of Class 4 is to eliminate downtime through the application of all tactics to provide continuous operation regardless of planned or unplanned activities. All recognizable single points of failure are eliminated. Systems are typically automated to reduce the chances for human error and are staffed 24/7. Rigorous training is provided for the staff to handle any contingency. Compartmentalization and fault tolerance are prime requirements for a Class 4 data center.

Table B-9 Tactics for Class 4

Component redundancy:	Redundancy is provided for all critical components and to increase maintainability; also provided for noncritical components.
System redundancy:	System redundancy is provided with component redundancy so that overall reliability is maintained even during maintenance activities.
Quality control:	Premium quality for all components. Where practical, equipment and components in the primary and redundant systems should come from different manufacturers, be a different model, or from different production lots as to avoid being affected by the same type fault or component recall simultaneously.
Survivability:	All systems are self-supporting in any event and are protected against the highest levels of natural forces.
Application:	The critical power, cooling, and network systems in a Class F4 facility must provide for reliable, continuous operations even when major components (or, where necessary, major subsystems) are out of service for repair or maintenance. To protect against unplanned downtime, systems must be able to sustain operations while a dependent component or subsystem is out of service.

B.7 Availability Class Sub Groups

The data center is not just a facility or building, but it is a collection of services that supports the critical business processes. The data center services Availability Class model can be used to guide design and operational decisions for the following critical services:

- Facility: The facility systems (e.g., power, cooling, controls) can be categorized into one of the sub group Class F0 through Class F4 as indicated in Sections 7, 9, and 10.
- Cable Plant: The network cable plant topology can be categorized into one of the sub group Class C0 through Class C4 as indicated in Section 14.
- Network Infrastructure: The network architecture and topology can be categorized into one of the sub group Class N0 through Class N4 as indicated in Section 15.
- Data Processing and Storage Systems: The computer processing and storage systems can be categorized into one of the sub group Class S0 through Class S4 as indicated in Appendix C.
- Applications: The applications can be categorized into one of the sub group Class A0 through Class A4 as indicated in Appendix C.

B.8 Reliability Aspects of Availability Planning

Achieving an optimum Class of availability for a mission-critical data center requires strategic planning to determine the risks, design features. and potential improvement measures that will lead to fewer critical-systems related failures.

B.8.1 Reliability Engineering Principles and Calculating Reliability

Reliability is the probability that equipment or a system will perform its intended function, within stated conditions, for a specified period of time without failure. It is expressed as a percentage (i.e., a number between 0 and 1), in which a lower percentage indicates a greater likelihood of failure in a given period of time. Reliability is not the same as *availability.* Whereas reliability uses the number (frequency) of failures within a period of time within its calculation, availability utilizes the amount of time equipment or a system is non-operational as a result to planned or unplanned failures, interruptions, or events.

Over the last 30 years, data has been collected and analyzed for a wide variety of mechanical and electrical components and their failure characteristics. This has led to broad-based industry standards for the analysis and design of reliable power and cooling systems (e.g., IEEE 3006 series).

The reliability of a given system can be calculated from the published MTBF (mean time between failures) data for given components of that system. This calculation can then be combined to yield an overall expression of system reliability through the analysis of all series and parallel subsystems. The calculations are as follows:

$$R = e^{(-\lambda T)} \qquad \text{(B-4)}$$

where:

R = reliability (percent probability of success)

e = exponential function

λ = failure rate (the reciprocal of MTBF)

T = time period (same units as failure rate)

Example: A UPS module has a published MTBF of 17,520 hours (one failure every two years). Its failure rate would then be 0.00005708 failures per hour. What is its one-year reliability or the probability of not failing in one year (8,760 hours)?

$R = e^{(-0.00005708 \times 8,760)}$

$R = 0.6065$ or 60.65%

To obtain the reliability of a given system, the individual reliability of each component must be calculated, then the reliability of parallel subsystems, and then the series reliability of all subsystems as follows and as illustrated in Figure B-3.

The reliability of a series system is equal to the product of all component reliabilities. The reliability of a parallel system is equal to the complement of the product of all component complements. Thus, the reliability for the system in Figure B-3 would be calculated as follows:

$R_{A1A2} = R_{A1} \times R_{A2} = 0.5 \times 0.5 = 0.25$

$R_A = 1 - [(1 - R_{A1A2}) \times (1 - R_{A3})] = 1 - [(1 - 0.25) \times (1 - 0.5)] = 0.625$

$R_B = 1 - [(1 - R_{B1}) \times (1 - R_{B2})] = 1 - [(1 - 0.61) \times (1 - 0.61)] = 0.848$

$R_{TOTAL} = R_A \times R_B = 0.625 \times 0.848 = 0.53$ (53%)

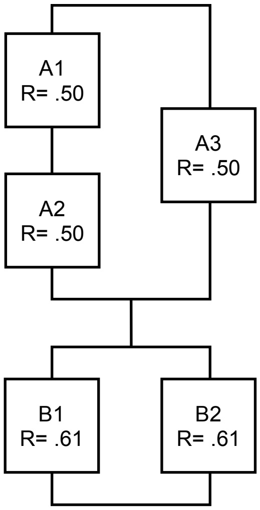


Figure B-3
Sample Reliability Calculation

B.8.2 Trends Affecting Reliability of Critical IT Facilities

As more and more clients require service-level guarantees, service providers and facility managers must determine what data center service performance is required to provide the agreed-to or sufficient end user availability. Table B-10 shows the relationship between availability percentage and allowable downtime.

Availability levels of 99.99% (50 minutes of downtime per year) allow practically no downtime for maintenance or other planned or unplanned events. Therefore, migrating to high-reliability solutions is imperative.

As computers have become more reliable, the overall percentage of downtime events caused by critical system failures has grown. Although the occurrence of such outages remains small, the total availability is dramatically affected because repair times (mean time to repair or MTTR) for certain critical system outages are lengthy (i.e., generator, UPS, chiller).

Where practical, equipment in redundant systems should come from different manufacturers, or different models or different production lots, as to avoid both systems being affected by the same type fault or component recall simultaneously.

Table B-10 Relationship Between Availability Percentage and Allowable Downtime

Targeted Availability (percent)	*Allowable Maximum Annual Downtime (minutes)*
< 99.0	>5000
99 to 99.9	500 – 5000
99.9 to 99.99	50 – 500
99.99 to 99.999	5 – 50
99.999 to 99.9999	0.5 – 5.0

B.8.3 Planning Process

A proactive, strategic planning approach to mission-critical data center design and management requires a five-step process:

1) Analyze the current data center.
2) Identify and prioritize risks and vulnerabilities.
3) Provide solutions to minimize risks.
4) Develop an implementation strategy.
5) Measure performance, and verify improvement.

This process should be performed in a continual cycle over the course of a year (see Figure B-4). By use of this cycle, plans can be refined and modified as objectives are met or new technology is deployed.

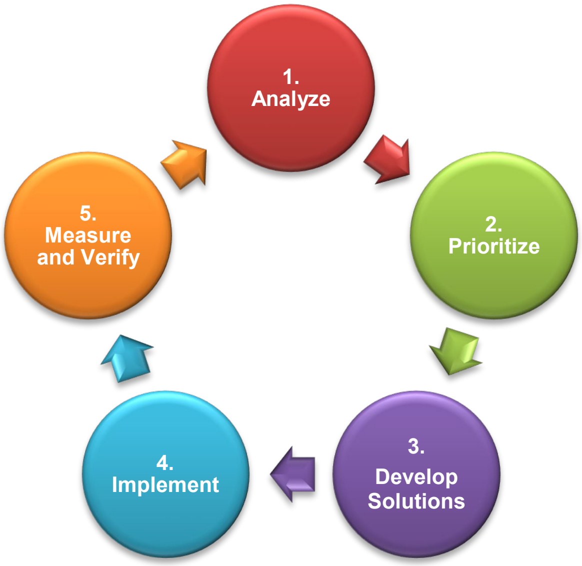


Figure B-4
Continuous Improvement Cycle

B.9 Other Factors

The process by which mission-critical Availability Classes are defined is not a perfect science. As projects are built, there will be unexpected outcomes and learned lessons. The following are just a few factors that may alter the selected Availability Class. Other factors will be added over time.

B.9.1 Intangible Consequences of Downtime

On occasion, a new product rollout, technical initiative, or other major endeavor will be announced. With heightened press exposure or internal performance pressures, there will be an incalculable and unpredictable cost of unplanned downtime. Avoiding these types of circumstances may dictate a higher Availability Class than is otherwise indicated.

B.9.2 Scheduled Deployment

If a critical IT function must be deployed quickly, it may dictate different risk management strategies outside that normally considered.

B.9.3 Unusual Budget Constraints

If the established budget for a critical data center will not support the required Availability Class, then a less reliable data center will need to be implemented unless additional funding is provided.

B.10 Other Reliability Alternatives

B.10.1 Multiple Data Centers

System designs with clustered systems having nodes spread across two or more Class 3 data centers can meet or exceed the uptime of a system in a single Class 4 data center. In such a design, the first failover is to the local node (synchronous), the second failover is to a nearby data center (~16 km [10 miles], and still synchronous), and the third is to a remote data center (but asynchronous). Such a design does increase the facility’s overhead and therefore, the cost. However, it offers a way for designers to avoid many of the costs associated with Class 4 data centers, whether owned, leased or collocated.

B.10.2 Software Orchestration

Within a single data center, container orchestration software can be utilized to provide resilience that will allow for the downtime of servers, racks and pods and not affect the performance of applications. Such a method may provide Class 3 level performance while utilizing Class F2 infrastructure.

B.11 Reliability Planning Worksheet

Use the following planning guide starting on the next page to determine the critical IT requirements.

Project name: ______________________________

Project number: ______________________________

Project description: ______________________________

____

Project location: ______________________________

____

STEP 1: Determine Operational Requirements

1) How many hours of operation must be supported during a production week? _____
2) How many scheduled production weeks are there? (if production occurs every week enter 52.14) _____
3) Multiply line 1 by line 2, and enter here. This is annual production hours: ______
4) Subtract line 3 from 8,760, and enter the result here: _______
5) Are there additional available days or weekends each year for scheduled downtime that have not been accounted for in lines 2 or 3? Enter the total annual available hours: ______
6) Add lines 4 and 5 and enter the result (allowable annual maintenance hours) here: ______
7) If line 6 is greater than 400, the Operational Level is 0; otherwise, proceed to the next line.
8) If line 6 is greater 100, the Operational Level is 1; otherwise, proceed to the next line.
9) If line 6 is between 50 and 99, the Operational Level is 2; otherwise, proceed to the next line.
10) If line 6 is between 1 and 49, the Operational Level is 3; otherwise, the Operational Level is 4.

STEP 2: Determine Operational Availability Rank.

1) Based on the operational level from Step 1 above:
   - Level 0; Proceed to line 2.
   - Level 1: Proceed to line 3.
   - Level 2: Proceed to line 4.
   - Level 3: Proceed to line 5.
   - Level 4: Proceed to line 6.
2) Operational Level 0: If the maximum annual downtime is:
   - 500 minutes or greater, then the availability requirement is Operational Availability Rank 0.
   - Between 50 and 500 minutes, then the availability requirement is Operational Availability Rank 1.
   - Less than 50 minutes, then the availability requirement is Operational Availability Rank 2.

   Proceed to Step 3.
3) Operational Level 1: If the maximum annual downtime is:
   - 5000 minutes or greater, then the availability requirement is Operational Availability Rank 0.
   - Between 500 and 5000 minutes, then the availability requirement is Operational Availability Rank 1.
   - Less than 500 minutes, then the availability requirement is Operational Availability Rank 2.

   Proceed to Step 3.
4) Operational Level 2: If the maximum annual downtime is:
   - 5000 minutes or greater, then the availability requirement is Operational Availability Rank 1.
   - Between 5 and 5000 minutes, then the availability requirement is Operational Availability Rank 2.
   - Less than 5 minutes, then the availability requirement is Operational Availability Rank 3.

   Proceed to Step 3.

Continues on next page

5) Operational Level 3: If the maximum annual downtime is:
    - 50 minutes or greater, then the availability requirement is Operational Availability Rank 2.
    - Between 5 and 50 minutes, then the availability requirement is Operational Availability Rank 3.
    - Less than 5 minutes, then the availability requirement is Operational Availability Rank 4.

    Proceed to Step 3.
6) Operational Level 4: If the maximum annual downtime is:
    - 50 minutes or greater, then the availability requirement is Operational Availability Rank 3.
    - Less than 50 minutes, then the availability requirement is Operational Availability Rank 4.

    Proceed to Step 3.

STEP 3: Define Mission-Critical Risk Level

Downtime will reduce or negatively impact operations (select one):

- Catastrophic (e.g., across the entire enterprise) ______
- Severe (e.g., across a wide portion of the enterprise) ______
- Major (e.g., across a single region or department) ______
- Minor (e.g., at a single location) ______
- Isolated (e.g., a single non-critical function) ______

STEP 4: Determine from the Table below

1) Select the column from the Operational Availability Rank in Step 2.
2) Select the row from the Risk Level in Step 3.
3) Your Availability Class is where the two intersect: _____

Data Center Services Availability Class

Impact of Downtime	*Operational Availability Rank*				
	0	*1*	*2*	*3*	*4*
Isolated	**Class 0**	**Class 0**	**Class 1**	**Class 3**	**Class 3**
Minor	**Class 0**	**Class 1**	**Class 2**	**Class 3**	**Class 3**
Major	**Class 1**	**Class 2**	**Class 2**	**Class 3**	**Class 3**
Severe	**Class 1**	**Class 2**	**Class 3**	**Class 3**	**Class 4**
Catastrophic	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 4**

This page is intentionally left blank

Appendix C Alignment of Data Center Services Reliability with Application and System Architecture (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

C.1 Overview

The BICSI reliability classification framework can be used to guide the data center network, network cable plant, and facility systems. It is important to first understand the constraints or flexibility that is built into the application architecture and the processing and storage systems architecture before defining the reliability requirements of the underlying lower level systems. If the applications support location transparent high availability clusters or cloud services (either private or public cloud based services) that can be implemented across multiple data centers, then the reliability of each data center facility may be able to be reduced as the reliability is built into the technology rather than the facility. This framework is provided to support the analysis of the data center services end-to-end reliability. After all, the "data center" is not just a facility or building, but it is a collection of services that supports critical business processes.

C.2 Application Reliability

The application layer content within this appendix is not meant to drive various methods of application architecture, but rather to identify how application architecture designs can be categorized into the reliability Classes based on how they can meet the defined performance characteristics. With the application architecture design quantified according to the performance requirements of the reliability Classes, it will be possible to correlate the required performance characteristics of the underlying data center service layers, enabling the end-to-end alignment. This framework can assist in:

- Identifying how lower level services can be designed with increased redundancy to overcome the impact of reduced reliability of monolithic application architecture.
- Identify how developing distributed location transparent application architecture with increased redundancy across multiple lower level services can take advantage of reducing the reliability Class of the lower level services.

One of the key elements of any application design is the architecture of the application layers. This architecture defines how the pieces of the application interact with each other and what functionality each piece is responsible for performing. The application layer is divided up to create a series of application layers, each of which is responsible for an individual or atomic element of the application's processing. Applications that meet the higher level performance requirements generally have each layer running on a different system or in a different process space on the same system than the other layers.

The application layers consist of:

- Presentation: The presentation layer contains the components that are required to enable user interaction with the application.
- Business Logic: The business logic layer is where the application-specific processing and business rules are maintained.
- Data: The data layer consists of data access and data store. Data access is responsible for communicating (I/O) and integrating with the data stores that the application needs to be able to function. Data store consist of the data sources accessed by the application. The data sources could be databases, structured, or unstructured file systems.

For the performance characteristics, the application is prefaced with an "A" to identify how it aligns with the reliability Class criteria.

C.2.1 Data Center Application Architecture Availability Classes

The following application architecture examples merely represent one example of many software engineering solutions.

C.2.2 Availability Class A0 and A1

Application layers are implemented without the ability to be distributed or enable diverse user access. Application layers are hardware dependent, non-redundant with no seamless failover or self-healing capabilities from presentation to data layer. All application layers may be implemented on the same process space on the same system.

Table C-1 Tactics for Class A0 and A1

Presentation Layer:	Common user access
Business Logic Layer:	Hardware dependent, monolithic logic
Data Layer:	Non-redundant I/O, hardware dependent non-redundant data sources

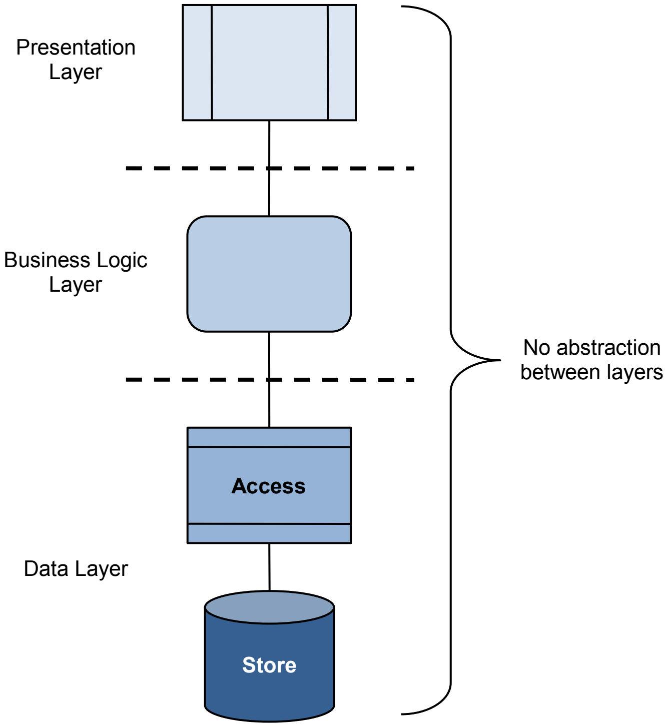


Figure C-1
Class A0 and A1 Application Architecture

C.2.3 Availability Class A2

Business logic layer is designed to support seamless transition between distributed logic. Data layer is designed to support redundant I/O, providing failover or self-healing capabilities. Application layers may be hardware dependent. All application layers may be implemented on the different process spaces on the same system. Active-passive application architecture is an example of application reliability classification A2.

Table C-2 Tactics for Class A2

Presentation Layer:	Common user access
Business Logic Layer:	Hardware dependent, distributed logic
Data Layer:	Support for redundant I/O and redundant hardware dependent data sources

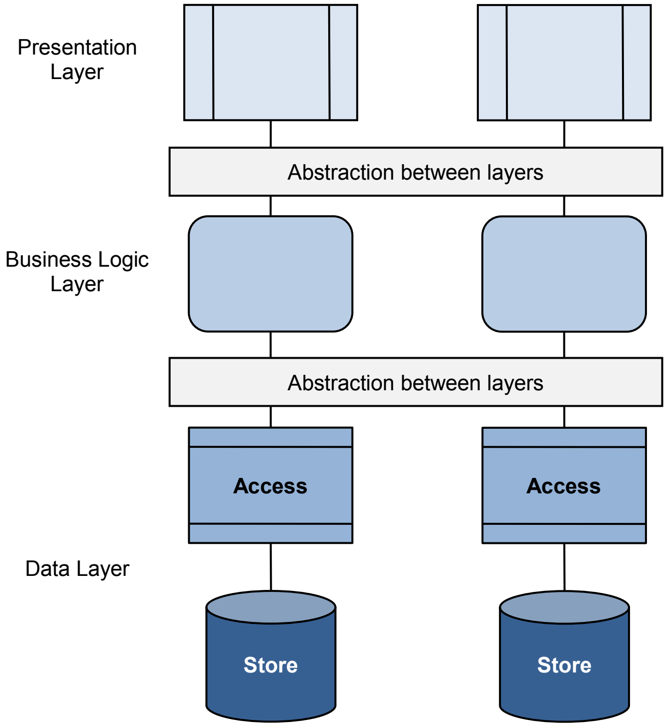


Figure C-2
Class A2 Application Architecture

C.2.4 Availability Class A3 and A4

Business logic layer is designed with seamless transition between redundant distributed logic and hardware platforms. Data layer provides failover or self-healing capabilities on redundant platforms. Application layers will be hardware independent, supporting virtualization and virtual server relocation across the enterprise. The application architecture is capable of expanding horizontally within individual application layers or across all application layers, either within a common data center, across multiple data centers or data center service providers. Each application layer will run on a different system. Active-active architecture supporting virtual server relocation, service orientated architecture (SOA), and location transparent cloud-based application architectures are examples of application reliability classification A3 and A4.

Table C-3 Tactics for Class A3 and A4

Presentation Layer:	Diverse user access
Business Logic Layer:	Hardware abstraction, distributed logic
Data Layer:	Redundant I/O, redundant hardware independent data sources

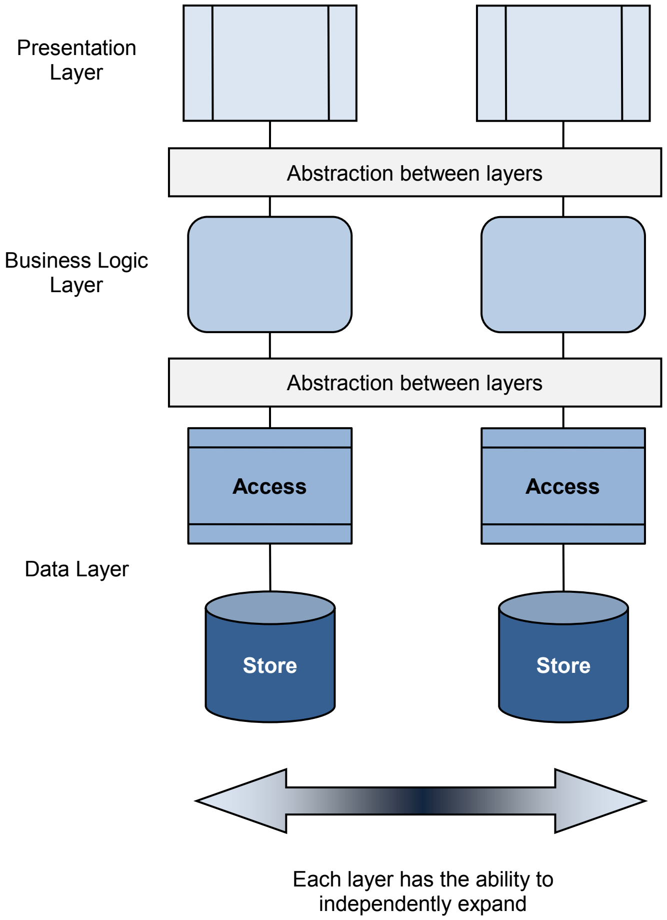

Presentation Layer
Abstraction between layers
Business Logic Layer
Abstraction between layers
Access
Access
Data Layer
Store
Store
Each layer has the ability to independently expand

Figure C-3
Class A3 and A4 Application Architecture

C.2.5 Data Center Systems Architecture Summary

It is uncommon for an enterprise data center to have all applications align within the performance requirements of a single reliability class. Each application is developed according to its own requirements and functionality specifications. However, if the business has identified a baseline performance requirement that meets the overall organization's objectives, the associated reliability class should either be the minimum objective or lower level data center service layers should provide higher than identified reliability to compensate, including disaster recovery/business continuity capabilities.

C.3 Data Processing and Storage Systems Reliability

The data processing and storage systems layer has historically been directly dependent on the higher application architecture layer. However, with the development of virtualization and cloud computing, the data processing and storage services layer can be abstracted from the higher application architecture services layer.

Historically, appliance server applications relying on direct attached storage was the predominant low-cost data storage technology solution. The development of network attached and scalable enterprise cross platform storage systems from various manufacturers have also provided a cost effective alternative to the traditional "big iron" enterprise storage systems. Virtualization has also had a significant impact on the data storage system industry, providing intelligent data management, including automated layer management based on defined performance requirements and retention policies.

Current application architecture, data processing, and storage systems not only provide autonomy between the application and the associated data processing hardware, but also provide autonomy between the data processing hardware and the data storage systems.

The data processing and storage systems consist of:

- Processing: The processing systems range from application-specific appliance servers to virtualized, high performance or grid computing hardware solutions.
- Storage: The storage systems range from platform specific direct attached disks to enterprise platform independent networked storage systems.

For the performance characteristics, the data processing and storage systems are prefaced with an "S" to identify how it aligns with the reliability Class criteria.

C.3.1 Data Center Systems Availability Classes

The following system architecture examples merely represent one example of many system engineering solutions.

C.3.2 Availability Class S0 and S1

Systems are implemented on specific platforms and are hardware dependent with no seamless failover or self-healing capabilities.

Table C-4 Tactics for Class S0 and S1

Processing Systems:	Application specific hardware dependent processing
Storage Systems:	Platform dependent direct attached storage

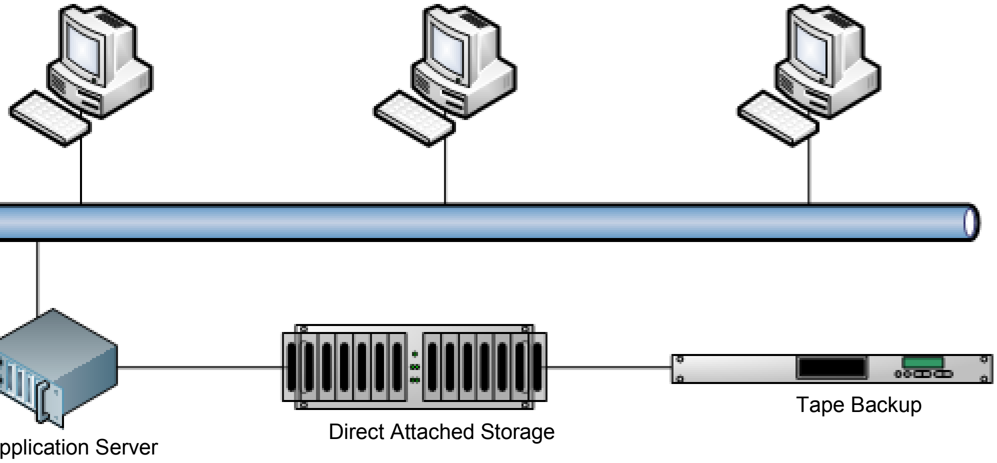


Figure C-4
Class S0 and S1 Systems Architecture

C.3.3 Availability Class S2

Systems are implemented on specific platforms and are hardware dependent with failover capabilities. System failure recovery performed through application and data storage failover to redundant systems.

Table C-5 Tactics for Class S2

Processing Systems:	Application-specific hardware dependent processing with mirrored application on redundant hardware
Storage Systems:	Platform dependent network attached storage with mirrored data on redundant network attached storage system

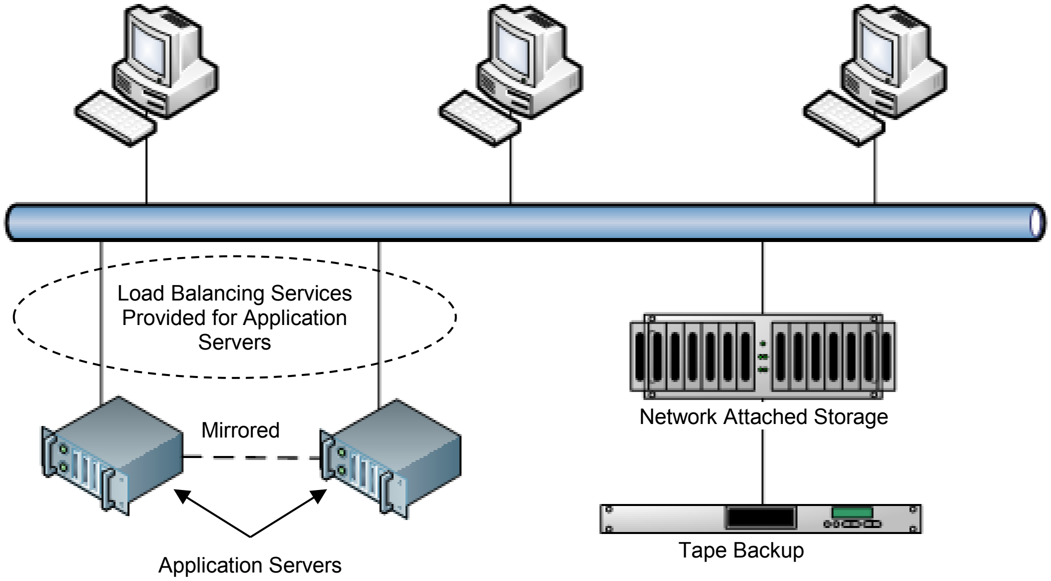


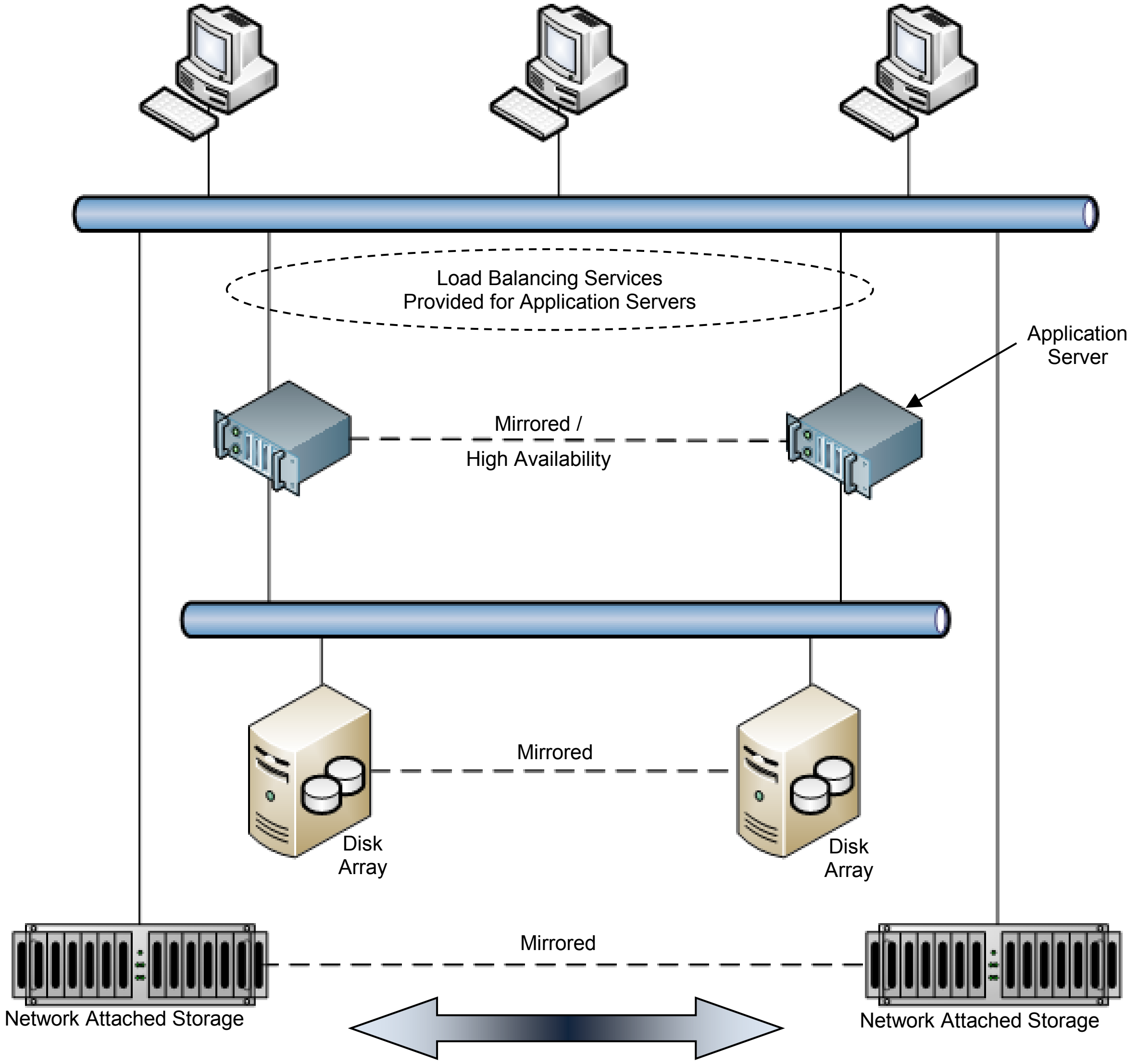
Figure C-5
Class S2 Systems Architecture

C.3.4 Availability Class S3

Processing systems are implemented on specific platforms and are hardware dependent with failover capabilities or on virtualized processing space with location transparency. Storage systems, whether network attached or enterprise cross platform storage systems, are provided with failover capabilities.

Table C-6 Tactics for Class S3

Processing Systems:	Application specific hardware dependent or virtualized processing space with mirrored application on redundant hardware
Storage Systems:	Network attached or enterprise cross-platform storage with mirrored data on redundant storage systems



Mirrored or high-availability systems require that lower level service layers (e.g., network, cabling infrastructure, facilities) supporting redundant processing or storage systems do not have any common mode failures that would impact the systems service layer.

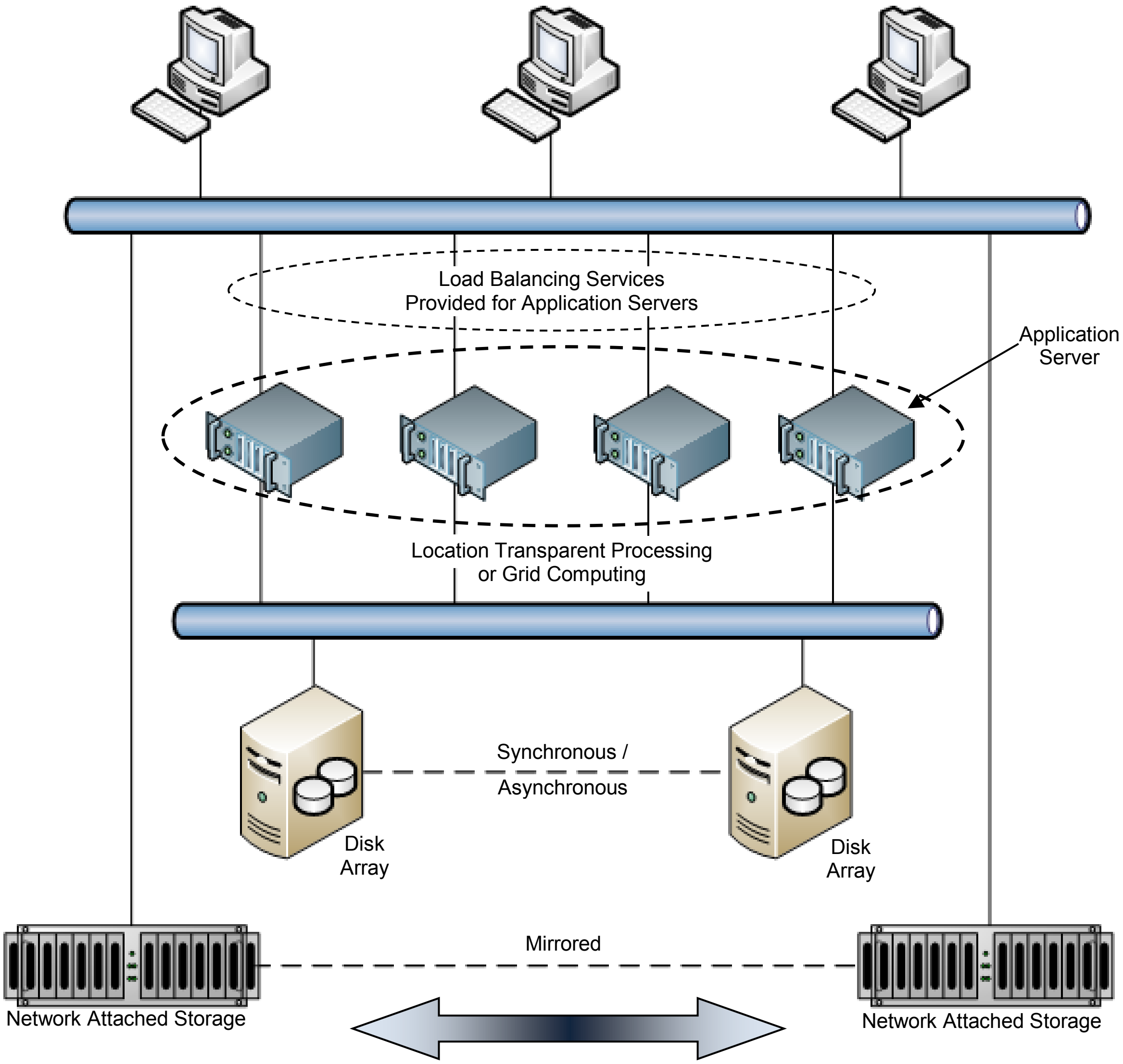
Figure C-6
Class S3 Systems Architecture

C.3.5 Availability Class S4

Systems are provided with system and component redundancy to provide seamless failover in the event of component or chassis failure. No common mode failures exist between processing and storage systems.

Table C-7 Tactics for Class S4

Processing Systems:	Location transparent, virtualized systems or hardware dependent grid computing, processing systems independent from storage systems
Storage Systems:	Network attached or enterprise cross-platform storage with mirrored data on redundant storage systems, automated data management among and between storage layers



Mirrored or high-availability systems require that lower level service layers (e.g., network, cabling infrastructure, facilities) supporting redundant processing or storage systems do not have any common mode failures that would impact the systems service layer.

Figure C-7
Class S4 Systems Architecture

Appendix D Data Center Services Outsourcing Models (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

D.1 Data Center Services Outsourcing Models

There are various data center outsourcing models that are available to organizations that desire to procure the data center services layer as a service from external vendors. The outsourcing models include:

- Managed services
- Colocation
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Cloud services is not defined as an outsourcing model, but rather, as a method of dynamically delivering outsourced services enabling rapid scaling of capacity up or down as the business requirements change. This dynamic capability can be implemented within a private cloud, public cloud, or private-public hybrid cloud architecture. Public cloud services can be provided by any of the XaaS outsourcing models.

D.1.1 Managed Services Model

The managed services model is used when the business has an existing data center with sufficient redundancy, capacity, and security to meet the business and IT objectives. For various reasons, the business may not want to maintain the staff required to operate the data center. The business contracts with an external vendor to operate the facility and possibly the hardware. The facility and hardware are owned and controlled by the business.

The value of managed services is that businesses can reduce or eliminate staff resources that are required to support the data center infrastructure.

D.1.2 Colocation Services Model

The colocation model consists of the business leasing computer room capacity from an external data center vendor. The external vendor provides physical security, floor space, power, cooling, and the ability to connect to one or more network service providers. The business owns and manages all IT hardware, applications, and OS/middleware.

D.1.3 Infrastructure as a Services (IaaS) Model

The IaaS model consists of the business owning and managing the applications and OS/middleware. The external vendor owns and manages the data center facility and hardware.

D.1.4 Platform as a Services (PaaS) Model

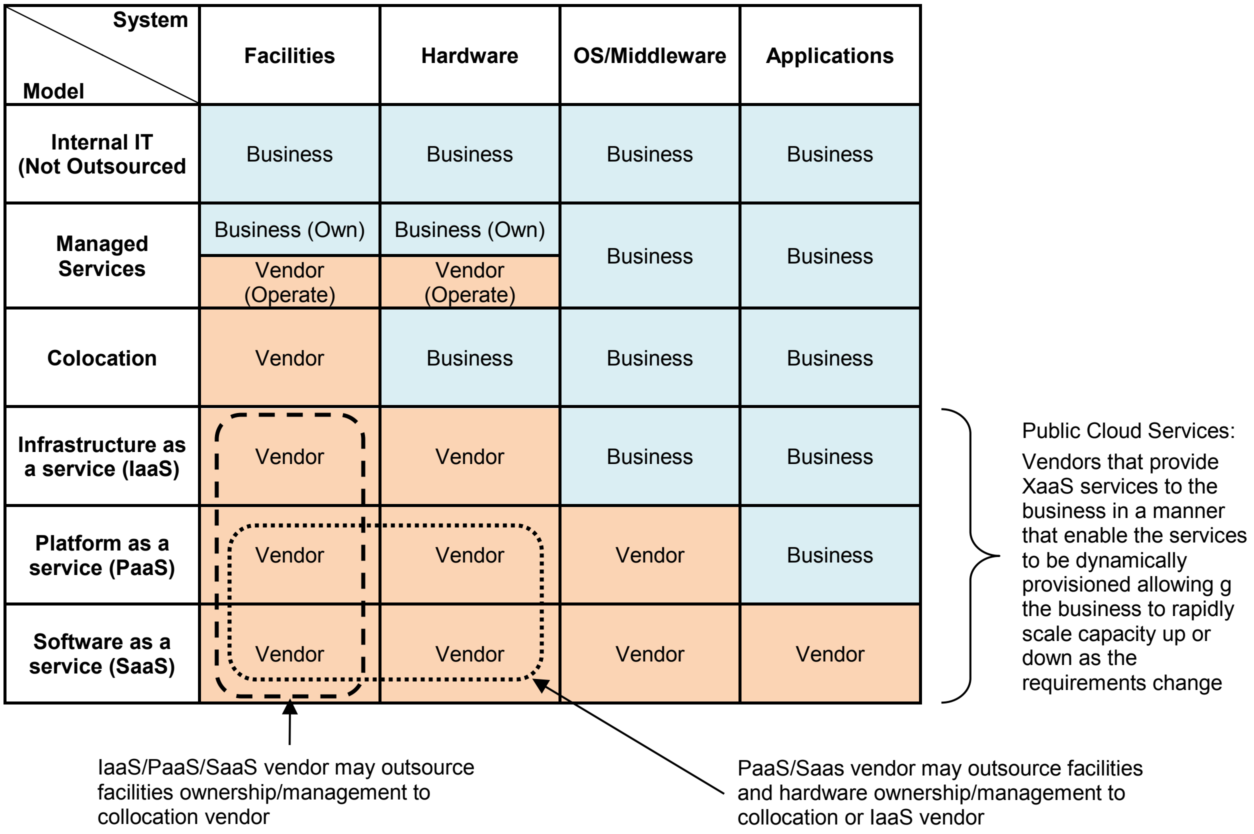
The PaaS model consists of the business owning and managing the applications. The external vendor owns and manages the data center facility, hardware, and OS/middleware.

D.1.5 Software as a Services (SaaS) Model

The SaaS model, also known as "full-service hosting", consists of the vendor owning the entire infrastructure stack: the facility, hardware, applications, and OS/middleware.

D.2 Data Center Services Outsourcing Model Comparison

The amount of control that the business has over the infrastructure, applications, and data is reduced as the model moves from the internal IT model to the SaaS model. It is very common for IaaS, PaaS, and SaaS outsourcing vendors to use a colocation vendor to own and manage the data center facility. Also, the PaaS and SaaS outsourcing vendors may use an IaaS vendor to own and manage the hardware. This is an important consideration when conducting due diligence on outsourcing vendors as the total infrastructure, application and data stack may consist of one or two vendor relationships behind the outsourcing vendor the end user is negotiating with. Understanding the entire stack is critical to ensuring the outsourcing solution will be able to meet the objectives of the business and the commitments that IT is making to the user community.



System / Model	Facilities	Hardware	OS/Middleware	Applications
Internal IT (Not Outsourced	Business	Business	Business	Business
Managed Services	Business (Own) Vendor (Operate)	Business (Own) Vendor (Operate)	Business	Business
Colocation	Vendor	Business	Business	Business
Infrastructure as a service (IaaS)	Vendor	Vendor	Business	Business
Platform as a service (PaaS)	Vendor	Vendor	Vendor	Business
Software as a service (SaaS)	Vendor	Vendor	Vendor	Vendor

Public Cloud Services: Vendors that provide XaaS services to the business in a manner that enable the services to be dynamically provisioned allowing g the business to rapidly scale capacity up or down as the requirements change

IaaS/PaaS/SaaS vendor may outsource facilities ownership/management to collocation vendor

PaaS/Saas vendor may outsource facilities and hardware ownership/management to collocation or IaaS vendor

Figure D-1
Outsourcing Model Matrix

Note that cloud services is not an outsourcing model; rather, it is a method of dynamically delivering outsourced services enabling rapid scaling of capacity up or down as the business requirements change. Public cloud services can be provided by any of the XaaS outsourcing models. One method of taking advantage of public cloud services is to augment internal IT services (private cloud) with public cloud services from a XaaS vendor during periods of peak demands on IT services to meet either processing, storage, or bandwidth capacity. In this case it is required that the internal network infrastructure and application architecture be developed as a private cloud in order to seamlessly integrate with the Public Cloud services offered by the XaaS vendors.

D.3 Public Cloud Services

Public cloud service vendors provide all the data center service layers for the applications they support for the customer. As previously mentioned, a public cloud service vendor may own and manage all data center services layers for their customers, or they may own and manage the application layer and outsource all lower level services layers to other vendors.

Due diligence is required by those considering public cloud services to ensure that the data center services and the public cloud model offered by the vendor provide the level of redundancy and diversity required based on the customer's objectives.

There are generally four levels of redundancy available for the implementation of public cloud services. Each of the levels identified below represent different common modes of failure that may result in outages to the customer.

D.3.1 Virtual Redundancy Level

The virtual redundancy level consists of a public cloud service vendor that provides virtual redundancy within a single physical data center. All shared physical resources represent potential single points or common modes of failure to the customer. It would be critical to validate the level of redundancy provided by all the lower layer data center services if the customer is purchasing cloud services based solely on virtual redundancy to ensure that the overall reliability objectives can be achieved by the sole cloud services vendor.

D.3.2 Redundant Availability Zone Level

The redundant availability zone level consists of a public cloud service vendor that provides redundant availability zones across multiple physical data centers within a common region. All physical resources within each data center do not represent potential single points or common modes of failure to the customer. All external risks, both natural and man-made, that the data centers are exposed to may represent potential common modes of failure to the customer. It would be critical to validate the level of redundancy provided by all the lower layer data center services and the risk of all common modes of failure between the two data centers if the customer is purchasing cloud services based solely on redundant availability zones to ensure that the overall reliability objectives can be achieved by the sole cloud services vendor.

D.3.3 Redundant Cloud Region Level

The redundant cloud region level consists of a public cloud service vendor that has at least two data centers located in separate diverse regions. There are no common modes of failure with any of the data centers internal physical resources or external natural and man-made risks. The customer has the ability to move data center services between the diverse data centers as required. If the reliability of the lower layer data center services cannot be validated, it would be prudent to assume the redundant cloud region level provided by a single cloud services vendor would achieve Class 3 reliability requirements if distributed across two or more physically diverse data centers. As the vendor distributes its redundant cloud region cloud services across more (greater than three) data centers, each located within physically diverse regions, the lower level layers become less significant in ensuring that the cloud services will provide the users access to the applications and data without disruption.

D.3.4 Redundant Cloud Provider Level

The redundant cloud provider level consists of multiple public cloud service vendors, located in separate regions, providing the ability of the customer to move their data center services between providers as required. All physical resources within each vendor's data center do not represent potential single points or common modes of failure to the customer. All external risks, both natural and man-made, that the data centers are exposed to do not represent potential common modes of failure to the customer. The redundant cloud provider model also eliminates the risk of the complete loss of a cloud provider because of external business events or business failure.

D.4 Outsourcing Model Decision Tree

The decision tree shown in Figure D-2 helps guide discussions on the suitability of outsourcing options on an application-by-application basis. It is not intended to identify the specific option that is best suited for the business, but it is primarily intended to identify options for each specific application that are not suited for the business. Once the options that are not suitable have been identified, each of the available options can be evaluated against cost, operational, functional, and security criteria.

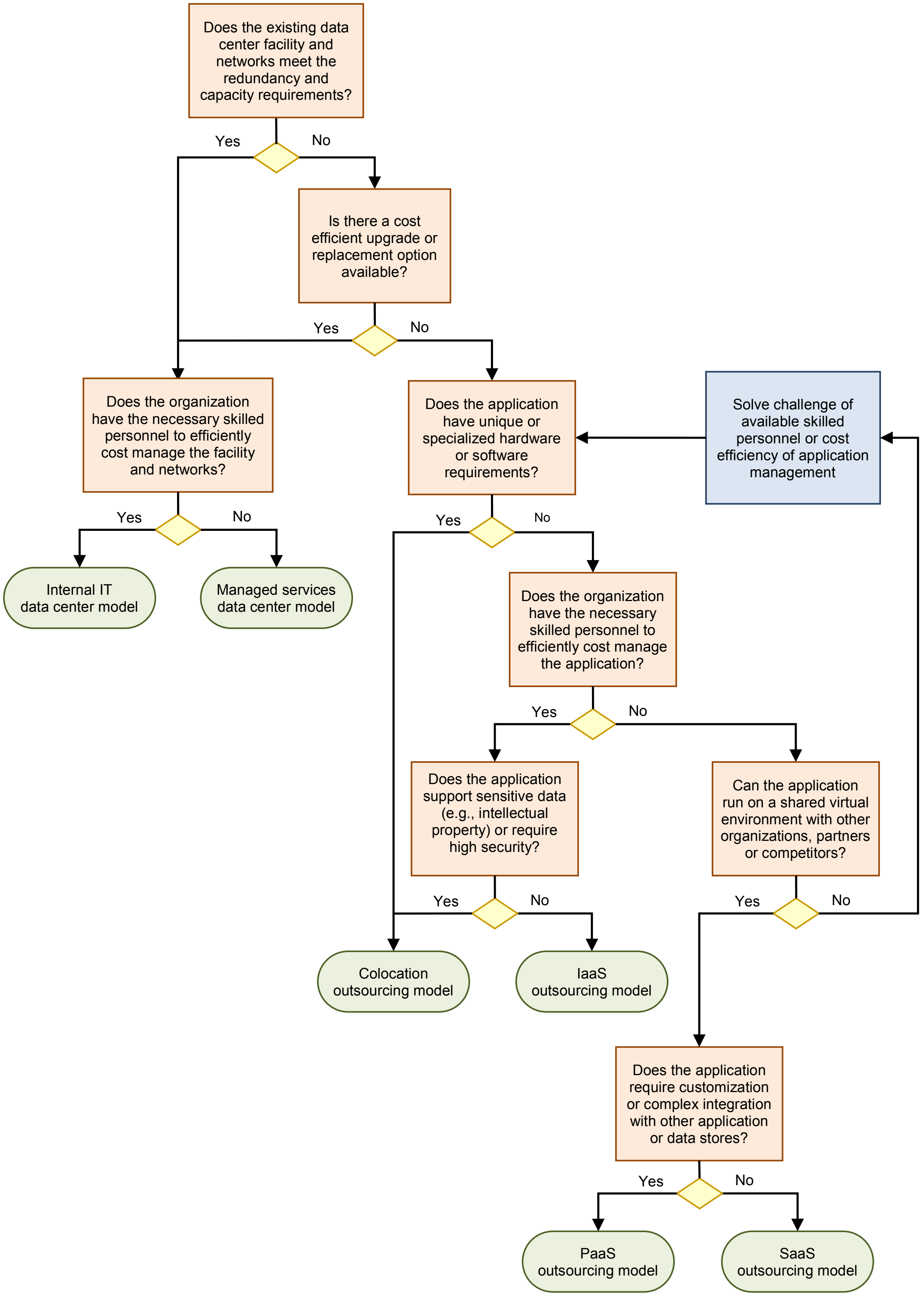

Does the existing data center facility and networks meet the redundancy and capacity requirements?
Yes
No
Is there a cost efficient upgrade or replacement option available?
Yes
No
Does the organization have the necessary skilled personnel to efficiently cost manage the facility and networks?
Yes
No
Internal IT data center model
Managed services data center model
Does the application have unique or specialized hardware or software requirements?
Solve challenge of available skilled personnel or cost efficiency of application management
Yes
No
Does the organization have the necessary skilled personnel to efficiently cost manage the application?
Yes
No
Does the application support sensitive data (e.g., intellectual property) or require high security?
Can the application run on a shared virtual environment with other organizations, partners or competitors?
Yes
No
Yes
No
Colocation outsourcing model
IaaS outsourcing model
Does the application require customization or complex integration with other application or data stores?
Yes
No
PaaS outsourcing model
SaaS outsourcing model

Figure D-2
Outsourcing Decision Tree

Appendix E Multi-Data Center Architecture (Informative)

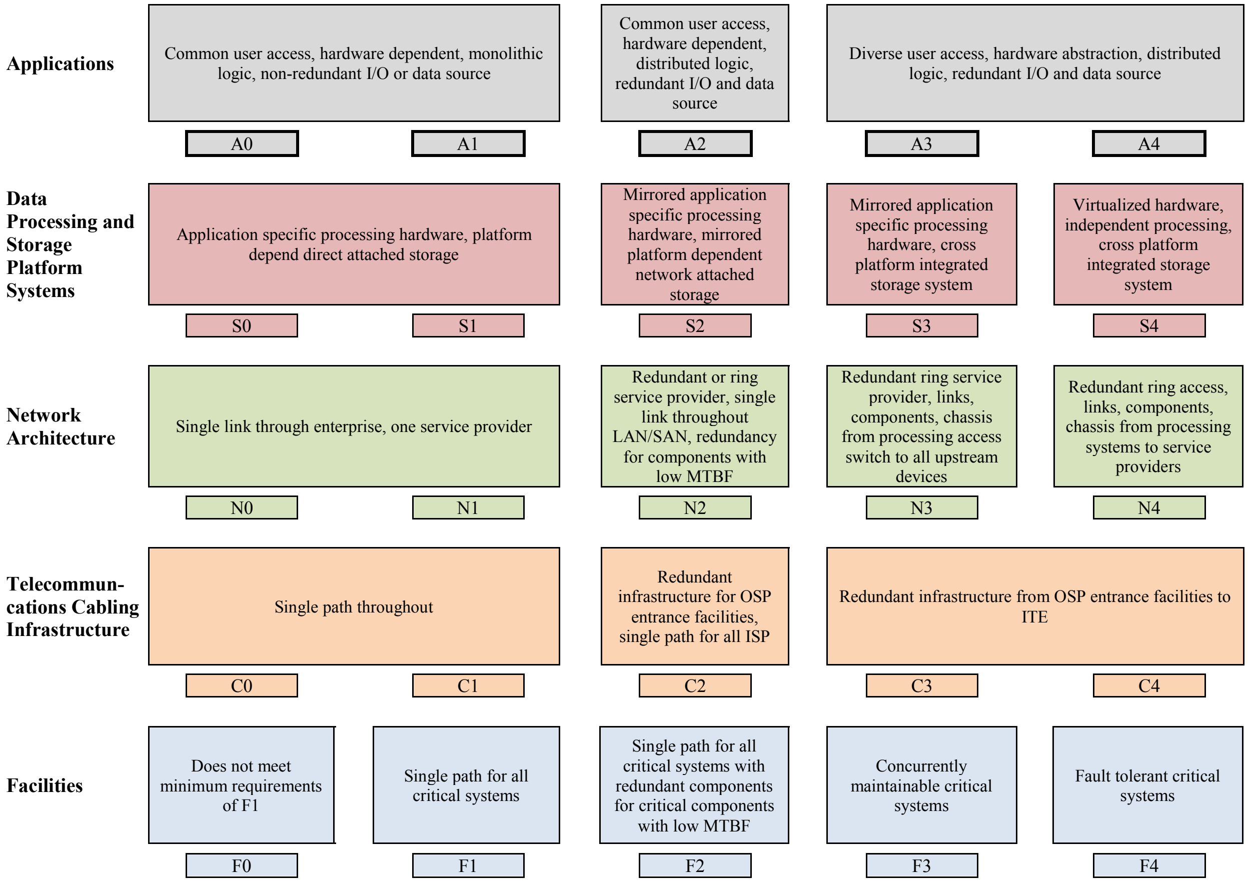
This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

E.1 Overview

Prior to virtualization, location transparent applications and cloud services, the optimal data center services configuration consisted of an alignment of the reliability classes across all the data center service layers. This provided the minimum required level of reliability and redundancy without over building any one of the data center service layers. However, it is unlikely that a single data center would have all the applications, data processing, and storage platform systems aligned within a single reliability classification no matter what the targeted base data center reliability classification is.

One of the values of the BICSI data center services reliability framework model is it can be used to:

- Identify the minimum reliability targets.
- Provide a structured methodical approach to guide decisions on how to adjust lower layer services to compensate for higher layer services reliability inadequacies.
- Guide discussions regarding the possible technical and cost benefits of increasing the reliability of the network architecture and higher layers above the targeted reliability class across multiple data centers so that cost savings can be realized by building each of the data centers facilities to a lower Class than the targeted reliability classification.



Applications	Common user access, hardware dependent, monolithic logic, non-redundant I/O or data source		Common user access, hardware dependent, distributed logic, redundant I/O and data source	Diverse user access, hardware abstraction, distributed logic, redundant I/O and data source	
	A0	A1	A2	A3	A4
Data Processing and Storage Platform Systems	Application specific processing hardware, platform depend direct attached storage		Mirrored application specific processing hardware, mirrored platform dependent network attached storage	Mirrored application specific processing hardware, cross platform integrated storage system	Virtualized hardware, independent processing, cross platform integrated storage system
	S0	S1	S2	S3	S4
Network Architecture	Single link through enterprise, one service provider		Redundant or ring service provider, single link throughout LAN/SAN, redundancy for components with low MTBF	Redundant ring service provider, links, components, chassis from processing access switch to all upstream devices	Redundant ring access, links, components, chassis from processing systems to service providers
	N0	N1	N2	N3	N4
Telecommun-cations Cabling Infrastructure	Single path throughout		Redundant infrastructure for OSP entrance facilities, single path for all ISP	Redundant infrastructure from OSP entrance facilities to ITE	
	C0	C1	C2	C3	C4
Facilities	Does not meet minimum requirements of F1	Single path for all critical systems	Single path for all critical systems with redundant components for critical components with low MTBF	Concurrently maintainable critical systems	Fault tolerant critical systems
	F0	F1	F2	F3	F4

Figure E-1
Reliability Framework Across All Service Layers

E.2 High Availability In-House Multi-Data Center Architecture Example

In this example, a customer has identified Class 3 as the targeted data center services reliability level. The customer has multiple facilities that can support critical data center functions. By provisioning the applications with high-availability configuration across two data center facilities, the customer will be able to achieve the targeted reliability and availability objectives.

It is important that any man-made or natural event common mode risks that may exist within the geographical region that is common between the two data centers be identified and evaluated. The communications between the two data centers can be synchronous or asynchronous, depending on the recovery point objective (RPO) and recovery time objective (RTO) of the disaster recovery/business continuity requirements and the physical distance limitations between the two data centers.

There are times when there are man-made or natural event common mode risks to both data centers that have been deemed an acceptable risk to the organization. An example would be multi-regional events, such as multi-State power outages, that an organization deems acceptable. There would be no loss of data within the data center (running on backup power sources); however, the users would not have access to the applications or data as their networks and systems would be off-line throughout the multi-state region. The organization might determine that the users would not have an expectation of accessing the data in this scenario, and there would be no loss of revenue or business reputation as a result. Therefore, the costs associated with building out multiple data centers across a wider geographical area (possibly outside synchronous communication capabilities) may not be justified.

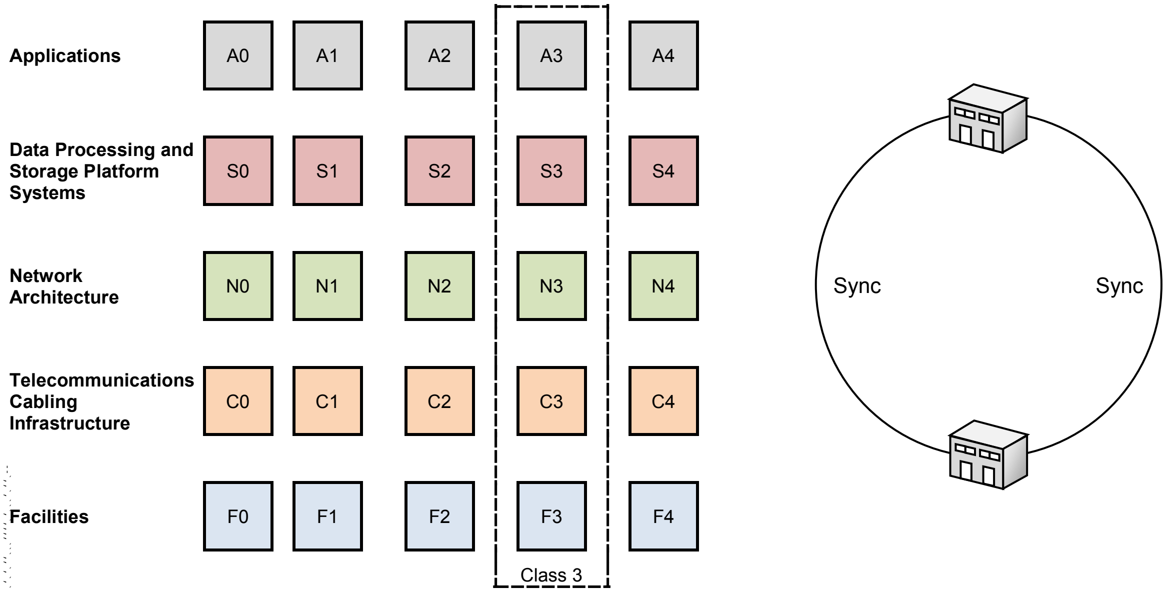


Figure E-2
Multi-Data Center Class 3 Example

E.3 Private Cloud Multi-Data Center Architecture Examples

Private cloud services are implemented in customer-owned data centers. Private cloud applications are developed to improve scalability, speed of deployment, and reliability with the abstraction on the reliance on the lower layer data center services. Private cloud applications may enable the customer to implement highly reliable applications without requiring highly reliable lower layer data center services.

E.3.1 Private Cloud Multi-Data Center Architecture – Class 3 Solution/Three Class 2 Facilities

The first example is a customer that has identified at least two Class 3 data centers as the targeted data center services reliability level. The private cloud applications would be implemented across diverse geographical regions. By provisioning the private cloud applications across three Class 2 data center facilities, the customer may be able to achieve similar reliability and availability objectives. The applications can move around each of the data center facilities with the loss of any one facility having little or no impact on the enterprise.

The two data centers connected via synchronous communications would be located within a common region. The data center that is connected via asynchronous communications would be located outside the region, ensuring no natural or man-made event represents a common mode of failure.

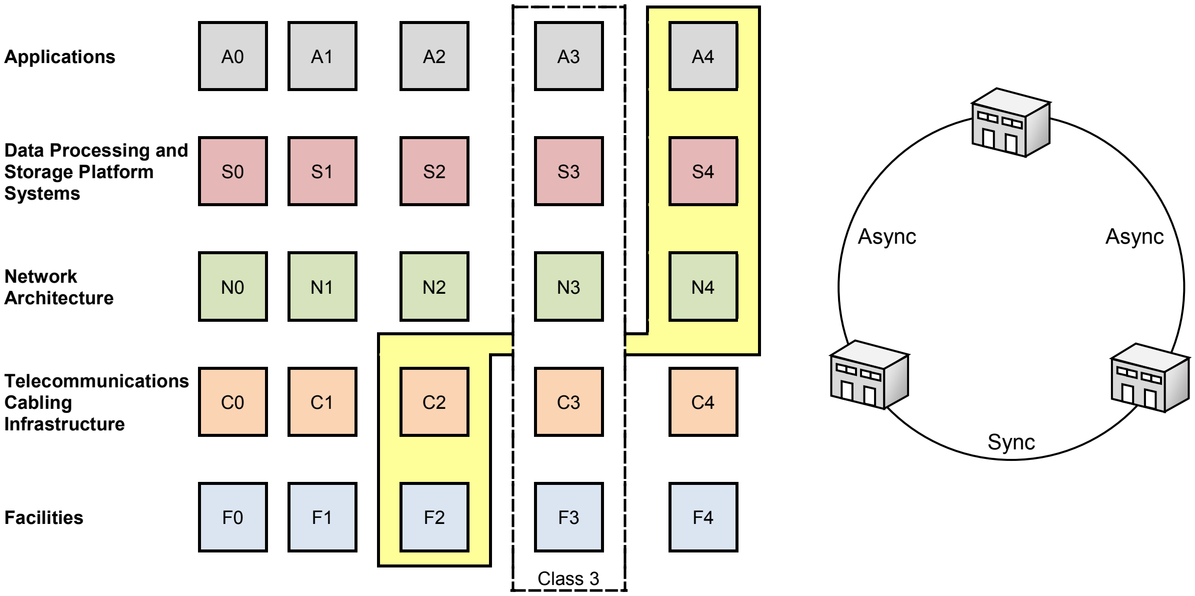


Figure E-3
Multi-Data Center Class 3 Example With Three Class 2 Facilities

This example is not provided as a solution that will always equate to two Class 3 data centers; rather, it is provided to show how the data center services reliability framework can be used to evaluate various options.

E.3.2 Private Cloud Multi-Data Center Architecture – Class 4 Solution/Four Class 2 Facilities

The second example is a customer that has identified two Class 4 data centers as the targeted data center services reliability level. By provisioning the private cloud applications across four Class 2 data center facilities, both within a common region and outside common regions, the customer may be able to achieve similar reliability and availability objectives. The applications can move around each of the data center facilities with the loss of any one facility or facilities within a region having little or no impact on the enterprise.

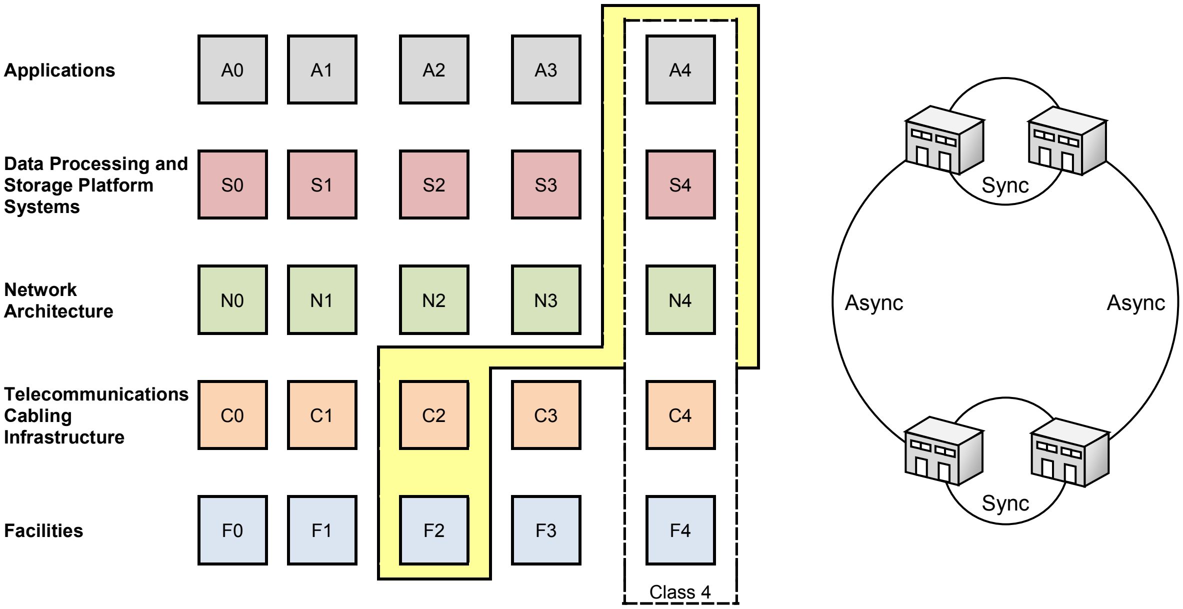


Figure E-4
Multi-Data Center Class 4 Example with Four Class 2 Facilities

Two of the data centers are connected via synchronous communications located within a common region. The pair of data centers located within each common region are connected via asynchronous communications. The pair of data centers would be located outside each other's region, ensuring no natural or man-made event represents a common mode of failure.

This example is not provided as a solution that will always equate to two Class 4 data centers, but it is provided to show how the data center services reliability framework can be used to evaluate various options.

Appendix F Examples of Testing Documentation (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

F.1 Introduction

This appendix provides examples of two different tests that may be performed during commissioning. Section F.2 provides an example of PDU testing and Section F.3 provides an example of UPS and diesel generator testing.

F.2 Example of PDU Testing

F.2.1 Purpose

To establish steps necessary to finish commissioning the PDUs and perform the Integrated Systems Test in customer room #1 while minimizing potential impact to critical customer equipment.

F.2.2 Introduction

- Connect temporary power jumper from M1BB tiebreaker to 1HUPSDP2
- Shift critical load to UPS 2B at the ASTS PDU level.
- Transfer UPS system 1A to internal bypass from UPS mode
- Energize A side PDUs in customer room #1
- Transfer UPS system 1A from internal bypass to UPS mode
- Power up the B side of customer room #1 PDU/ASTSs using temporary power
- Perform ASTS Commissioning Procedure on STS 3B
- Leave A side PDUs in customer room #1 on the 1A UPS
- Shift critical load in Customer Room #3 and Network to UPS 1A at the ASTS PDU level
- Transfer UPS system 2B to internal bypass from UPS mode
- Energize B side PDUs in customer room #1
- Transfer UPS system 2B from internal bypass to UPS mode
- Restore power to normal power paths

F.2.3 Systems Impacted

The following systems may be impacted by this procedure: UPS system 1A, UPS system 2B and all STS PDUs.

F.2.4 Backout Plan

If a problem occurs with a PDU or STS during testing, it will be isolated from the system until it is repaired.

ID	*Time mark*	*Duration*	*Task*	*Resource*	*Control*
			Run temporary power jumpers from M1BB tie breaker to panel 1HUPSDP 2, 4, 6		
		N/A	Site check-in		
			Enable contractor badges for access to proper work areas.		
			Notify monitoring company of impending work. Disable ALC page out function.		
		30 min	Project meeting – introductions, review of project, safety, and tool inventory		
1			At the MSDA, select source 1 (UPS 1A) as the Master Source.		

ID	*Time mark*	*Duration*	*Task*	*Resource*	*Control*
2			Record the load on UPS System 1A at the SCC control panel: kVA _________ kW __________ Phase A amps___________ Phase B amps___________ Phase C amps___________		
3			Record the load on UPS System 2B at the SCC control panel: kVA _________ kW __________ Phase A Amps___________ Phase B Amps___________ Phase C Amps___________		
4			Verify that all STS's are programmed with UPS 2B as Preferred source. If the STS is programmed with UPS 1A as the preferred source, transfer to UPS 2B as the preferred source using the following procedure: 3STS1A Time____________ 3STS2A Time____________ 3STS3A Time____________ 3STS4A Time____________ 3STS5A Time____________ 3STS6A Time____________		

ID	*Time mark*	*Duration*	*Task*	*Resource*	*Control*
4c			3STS7A Time____________ 3STS8A Time____________ 3STS9A Time____________ STSNETA Time____________ 1) At the STS, select **Monitor Mimic** screen and verify that no alarms are present. 2) Select **Source Transfer** screen and verify: a. Source 2 voltage available b. ON Source 1 c. Source 1 Preferred d. OK to transfer e. synchronization within 15°. 3) Simultaneously press **Alarm Reset** and **Down** buttons. 4) Verify transfer by checking **ON Source Message**: a. ON Source 2 b. Source 2 Preferred.		
5			Verify load increase on UPS 2B. It should be approximately the same as recorded in step 1.		
6			Verify that UPS 1A and UPS 2B are operating normally and that transfer to bypass is not inhibited.		
7			1) Transfer UPS 1A from UPS mode to **Internal Bypass** by: a. Verifying at UPS User Interface Panel: b. OK to transfer c. Static Switch connected d. no alarms present. 2) Review **Load Transfer Procedures** on the UPS User Interface Panel. 3) Using the **Push to Turn Voltage Adjust Pot**, set UPS output voltage 2 to 4 V above bypass voltage. 4) Verify UPS leads by 1° to 3° (Synchronization graphic is in upper right corner of display).		
7c			1) If OK to Transfer is highlighted, simultaneously press **Control/Enable** and **Bypass** buttons. 2) Press **Horn Off** to silence alarm. 3) At the UPS SCC Monitor Mimic verify: a. System Bypass Breaker closed b. UPS Output Breaker open.		

ID	*Time mark*	*Duration*	*Task*	*Resource*	*Control*
8			Energize A PDUs on normal UPS Source: 1) In CR1 at Panel 1HUPSDP 1, 3, 5 open and lock out breaker being fed by temporary power from M1BB. 2) At UPS 1A SCC distribution in room XXX, close Feeder to 1HUPSDP 1, 3, 5 3) In CR1 at Panel 1HUPSDP 1, 3, 5 close Breaker Main – DP (Fed From UPS1A) 4) Close the Main Input breaker then the Subfeed 1 and Subfeed 2 breakers at: a. 1PDU1A b. 1PDU2A c. 1PDU3A d. 1PDU4A		
9			Transfer UPS 1A from internal bypass to UPS mode by: 1) Verify at UPS SCC **Monitor Mimic** Panel. a. UPS on Internal Bypass b. UPS Modules are on line 2) Review **Load Transfer Procedures** on the UPS User Interface Panel. 3) Using the **Push to Turn Voltage Adjust Pot**, set UPS output voltage 2 to 4 V above bypass voltage. 4) Verify UPS leads by 1° to 3° (Synchronization graphic is in upper right corner of display). 5) If OK to Transfer is highlighted, simultaneously press **Control/Enable** and **UPS** buttons.		
9c			1) At the UPS SCC Monitor Mimic verify: a. System Bypass Breaker open b. UPS Output Breaker closed 2) Reset the UPS system output voltage to 488 V.		
10			Verify that UPS 1A and UPS 2B are operating normally and that transfer to bypass in not inhibited.		
11			In customer room #1 open and lock out feed from UPS 2B to panel 1HUPSDP2, 4, 6.		
12			Close tie breaker in M1BB		
13			In customer room #1: 1) Close breaker 1HUPSDP2, 4, 6 2) Close tie breakers among 1HUPSDP2, 1HUPSDP4, and 1HUPSDP6 3) Energize B side PDUs		
15			Perform ASTS Commissioning Procedure on STS 3B: 1) Ensure that the ASTS is in normal operating mode, and that no alarms are present. NOTE: During the performance of the tests, verify proper normal and alarm indications are present. Verify remote alarm indications.		

ID	*Time mark*	*Duration*	*Task*	*Resource*	*Control*
15c			1) Apply 100% load to the output of the ASTS. 2) Perform calibration checks for source 1 and record in the appropriate table. 3) Infrared scan the source 1 side and output of the ASTS after 100% load has been applied for at least one hour. Infrared scan the source 1 PDU. 4) Perform a maintenance isolation to source 1 maintenance bypass. 5) Infrared scan the source 1 maintenance bypass of the ASTS after 100% load has been applied for at least one hour. 6) Perform a restoration to normal operation. 7) Perform a manual transfer to source 2. 8) Perform calibration checks for source 2 and record in the appropriate table. 9) Infrared scan the source 2 side and output of the ASTS after 100% load has been applied for at least one hour. Infrared scan the source 2 PDU. 10) Perform a maintenance isolation to source 2 maintenance bypass. 11) Infrared scan the source 2 maintenance bypass of the ASTS after 100% load has been applied for at least one hour. 12) Infrared scan the output breaker distribution section. 13) Perform a restoration to normal operations. 14) Perform a manual transfer to source 1.		

F.3 Example of UPS and Diesel Generator Testing

NOTES:

1. Checkboxes (☑) have been incorporated into the following procedure to ensure full compliance to all steps contained herein.

2. Other types of backup power can be used; this example test plan uses a diesel generator.

F.3.1 Purpose

- To demonstrate that the new UPS module and diesel generator associated with the data center client facility will function in accordance with the manufacturer's specifications
- To ensure that these new critical power components will function accordingly in their parallel configuration

F.3.2 Scope

Testing to be performed as part of this procedure will be done as follows:

1) UPS 4 (600 kW required):
   - Input and output THD measurements
   - Voltage regulation measurements
   - Step load transient response
   - Bypass transfer transient tests
   - Transfer to battery transient response
   - Rectifier ramp in measurement.
2) Parallel UPS (1800 kW required):
   - Voltage regulation measurements
   - Module output load sharing measurements
   - Step load transient response
   - Bypass transfer transient tests
   - Module fault off and restore transient response.

3) DG 3 (2000 kW required):
   - 4 hour burn in
   - Output THD measurements
   - Voltage regulation measurements
   - Step load transient response
   - 100 % block load transient response
4) Parallel DG system (2000 kW required):
   - Load sharing measurements
   - Voltage regulation measurements
   - DG fault off and restore transient response.

F.3.3 Vendor's Responsibility

The technicians from each vendor have the responsibility of operating their equipment, and guiding all attending personnel through this procedure.

Vendors are also responsible to provide copies of all startup paperwork, and all equipment specifications for review and inclusion into the final commissioning report.

A copy of all vendor paperwork must be available at the beginning of the commissioning to ensure that applicable equipment startup checks have been performed.

F.3.4 General Contractor's Responsibility

They are responsible for ensuring that the following are available as needed during the performance of this procedure:

□ Technician(s) from the UPS vendor

□ Technician(s) from the diesel engine vendor

□ A minimum of two site familiar electricians to assist as necessary in the performance of this test procedure (e.g., to operate electrical distribution breakers, and or assist with load banks as needed); Additional electricians may be required in the event that the commissioning process will otherwise be delayed.

□ An infrared camera and operator (must be an infrared camera with the ability to take sample thermograms to establish a baseline recording of all major electrical equipment)

□ To provide the necessary air-cooled load banks and cables (please be sure that the cables provided are sufficient in length and ampacity for the amount of load); load bank positioning should be determined before cables are ordered; resistive load equal to the full load rating of each system to be tested shall be available.

1) For UPS module load testing, the load banks should be connected directly to the output switchgear of each UPS module (this will require 480 V load banks with external fan power capability):
2) For UPS module testing 1200 kW required. The external fan power for the load banks must be connected to a source, which will not be interrupted during the commissioning process.
3) For diesel generator testing, the load banks should be connected directly to the output of the paralleling cabinet. (This will require 480 V load banks with external fan power capability).
   - For diesel generator testing, a minimum of twelve, ideal of twenty-four 200 kW resistive load bank must be available.
   - The necessary diesel fuel oil.

□ To ensure that all parties are aware of their individual responsibilities as they pertain to this procedure

□ To ensure that all testing prerequisites are met before the commencement of the commissioning procedure (this includes the load bank hookup and placement for each day of commissioning)

□ To inform all applicable subcontractors that there will be no other work permitted in the spaces where commissioning is being performed. Failure to adhere to this requirement can result in personnel injury and equipment damage.

F.3.5 Testing Agent's Responsibility

The testing agent shall provide the necessary engineering personnel to complete the proposed testing, and will furnish the following test equipment or its equivalent:

- 2 each power analysis recorder (power meter)
- 1 each chart recorder
- 2 each digital multimeters
- 1 each 600A clamp on current probe for multimeter

F.3.6 Requirements

- The diesel generator system shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to it.
- Each diesel generator (single unit) shall be capable of accepting a 100% block load, and fully recovering (voltage and frequency) within 15 seconds.
- The diesel generator switchgear shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to it.
- The diesel generators shall be capable of paralleling, and load sharing to within 5% of each other from 25% to 100% system load.
- The UPS system shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to this equipment.
- Resistive load equal to the full load rating of each system to be tested shall be available.
- During the performance of this procedure, no other work will be permitted in the spaces in which equipment is being tested (e.g., while UPS module testing is being performed, no other work will be permitted in the UPS room, or in the area through which load bank cables are run). No other work will be permitted on equipment feeding the equipment, directly or indirectly controlling power to devices being commissioned.

  Note that this precaution must be adhered to since the proposed work will require testing on exposed and energized electrical equipment – other work in the area jeopardizes the safety of the testing engineers, and the individuals doing the work.

F.3.7 Emergency Generator System Testing

The purpose of this test is to record the operating parameters and compare them to the manufactures specifications. The results of this testing will also be used as a baseline for future testing.

Note that if at any time during the diesel generator testing should a call for emergency occur from any ATS the load bank shall be turned off, the load bank breaker shall be opened and the DG system returned to automatic operation.

F.3.7.1 Diesel Generator

F.3.7.1.1 Diesel Heat Run

This step shall be performed by the diesel vendor and paperwork should be presented to the testing agent's engineer:

□ Place this diesel generator on line and load to 2000 kW

□ Heat run at full load for four (4) hours

□ Take readings of voltage, current, frequency, revolutions per minute and all engine data available from the DG display panel (e.g., exhaust temperature, battery voltage, oil pressure, coolant temperature) every 15 minutes. Take a note of any revolutions per minute instability.

F.3.7.1.2 Infrared Scan

□ Infrared scan the engines once full load has been applied for a minimum of 1 hour.

□ Infrared scan each cylinder head. Values shall be at the same aim point for each head and within 2.5 °C (4.5 °F) of each other.

□ Infrared scan the four turbos and ensure uniform temperatures for all four.

□ Conduct an infrared scan of all power terminal connections, circuit breakers, between the generator and load bank, and record temperature following a minimum of 15 minutes operation at 100% load. Terminal temperature shall not exceed 75 °C (167 °F) Maximum.

□ Conduct an infrared scan of the generator bearing housing and record the generator bearing housing temperature. Bearing housing temperature shall not exceed 50 °C (122 °F) maximum.

□ Repeat the steps in this section after 3 hours of full load operation for each diesel generator being tested. Any abnormalities should be brought to the engineer's attention.

F.3.7.1.3 Steady State Tests

□ Start the engine. Apply 100% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at 100% load. Record data from the power meter and engine generator panel on the attached data sheet.

□ Apply 50% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the powermeter at 50% load. Record data from the powermeter and engine generator panel on the attached data sheet.

□ Remove all of the load. Take a snapshot of output voltage, current, frequency and harmonic content with the powermeter at no load. Record data from the powermeter and engine generator panel on the attached data sheet.

F.3.7.1.4 Transient Response Tests

□ With generator output at no-load (just load bank fans running), apply 50% rated kW load in one step (0 to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as “0 to 50% Transient”.

□ With generator output loaded to 50%, apply another 50% rated kW load in one step (50% to 100% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as “50% to 100% Transient”.

□ With generator output loaded to 100%, remove 50% rated kW load in one step (100% to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as “100% to 50% Transient”.

□ With generator output loaded to 50%, remove all load in one step. Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as “50% to 0% Transient”.

F.3.7.1.5 Block Load Test

The purpose of this test is to establish the load that this engine generator combination can accept and recover to rated voltage and frequency within 15 seconds.

With generator output at no-load, apply 100% rated kW load in one step. Make sure that the load does not exceed 100% capacity. For instance, if the generator is rated for 2000 kW, applying 2050 kW will cause the generator to respond out of specification. In this case, lowering the load by 100 kW is still acceptable as 100% block load. Record output voltage, current, and frequency with the power meter in **Monitor** mode. Annotate the event recording as “0% to 100% Transient.”

Note that if the engine is unable to recover to rated voltage and frequency within 15 seconds, reduce the block load amount to 75% and repeat the test. Annotate the testing record accordingly.

F.3.7.2 Diesel Generator Parallel Testing

Note that for parallel diesel generator testing, full system load for these tests is 2000 kW.

F.3.7.2.1 Steady State Tests

□ Place all engine generators on line. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at no load. Annotate the power meter recording as “0% Load”. Record data from the power meter and engine generator parallel panel meter on the attached data sheet.

□ With no load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.

□ Apply 50% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at 50% load. Annotate the power meter recording as “50% Load”. Record data from the power meter and Engine Generator Parallel Panel meter on the attached Data Sheet.

□ With 50% load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.

□ Apply 100% load to the system. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at 100% load. Annotate the power meter recording as “100% Load”. Record data from the power meter and Engine Generator Parallel Panel meter on attached Data Sheet.

□ With 100% load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.

F.3.7.2.2 Transient Response Tests

□ With system output at no-load, (just load bank fans running), apply 50% rated kW load in one step (0 to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “0 to 50% Transient”.

□ With system output loaded to 50%, apply another 50% rated kW load in one step (50% to 100% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “50% to 100% Transient”.

□ With system output loaded to 100%, remove 50% rated kW load in one step (100% to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “100% to 50% Transient”.

□ With system output loaded to 50%, remove all load in one step. Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “50% to 0% Transient”.

□ With system output at no-load, apply 100% rated kW load in one step. Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “0% to 100% Transient.”

F.3.7.2.3 Generator Fault Testing

□ Connect the power recorder to monitor three phase output voltage and current on the diesel generator parallel bus. Setup the power recorder for 15 minute monitoring period. Create the new power recorder **Site Information** directory and annotate it as “DG Fault Offs”. Create new **Location Information** directories for each DG and annotate them accordingly.

□ Place all diesel generators in parallel.

□ Apply 100% load to the system.

□ Link to the power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory as “Fault off and Restore DG 1”, and start recording.

□ Open the output breaker for DG 1 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.

□ Restore DG 1 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.

□ Stop the recording and download the data.

□ Link to the power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory **Fault off and Restore DG 2**, and start recording.

□ Open the output breaker for DG 2 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.

□ Restore DG 2 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.

□ Stop the recording and download the data.

□ Link to the power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory **Fault off and Restore DG 3**, and start recording.

□ Open the output breaker for DG 3 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.

□ Restore DG 3 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.

□ Stop the recording and download the data.

F.3.8 UPS Testing

F.3.8.1 Critical Load Isolation

□ Start the diesel generators using the test online position on the parallel switchgear.

□ Ensure that the three circuit breakers (UPS-Input SWGR, UPS-Maint. Bypass A, and UPS-Maint. Bypass B) on the DG parallel switchgear are all closed.

□ Transfer Switchboard UPS-Input to emergency.

□ Transfer the UPS system to bypass.

□ Transfer the Maintenance Bypass Switch A to Generator bypass.

□ Transfer the Maintenance Bypass Switch B to Generator bypass.

□ Open the output breakers on the UPS Parallel Switchgear.

□ Shutdown the UPS system and connect the load banks.

F.3.8.2 UPS Module # 1

UPS Data

Make:________________________ Model: ______________________

Serial #: ________________________ kVA: ________ kW: __________

Battery Data

Make: ______________________ Model: __________________________

# of Strings: ____ Jars/string: _____ Cells/Jar: _____ Float/Cell: ______

F.3.8.2.1 Steady-State Load Tests

☐ Connect the power meter to the input of the UPS module to be tested.

☐ Record three phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) at the following load levels:

1) 100% load
2) 50% load
3) No load (0% load).

☐ Connect the power meter to the output of the UPS module to be tested.

☐ Record three phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) at the following load levels:

1) 100% load
2) 50% load
3) No load (0% load).

☐ While 100% load is applied to the unit record the following on the attached data pages:

1) 3-phase current into the input filter
2) 3-phase current into the output filter
3) 3-phase current into the rectifier(s).

F.3.8.2.2 Transient Load Tests

☐ Connect the waveform recorder to the output of the UPS module to measure three phases of output voltage, and one phase of output current.

☐ Record the following load step transients with the waveform recorder:

1) 0%–50%–0%
2) 50%–100%–50%
3) 25%–75%–25%.

☐ Connect the Waveform recorder to measure three phases of system output voltage.

☐ Place the CT on one phase of the system SS bypass and record the following transfer transients with the waveform recorder:

1) Normal transfer to bypass with 100% load applied
2) Module failure to bypass with 100% load applied.

☐ Place the CT on one phase of the UPS module’s output and record the following transfer transient with the waveform recorder:

- Transfer from bypass to UPS with 100% load applied.

F.3.8.2.3 Infrared Scan

☐ Infrared scan the entire UPS module after 100% load has been applied for a minimum of 15 minutes.

☐ Infrared scan the upstream and downstream breakers of the UPS module after 100% load has been applied for a minimum of 15 minutes.

F.3.8.2.4 Battery Discharge Transient Test

☐ Verify that the waveform recorder is set to measure three phases of output voltage and one phase of input current.

☐ Verify that 100% load is applied to the UPS module.

☐ Send the UPS module to battery. Record the following:

- The initial transfer to battery with the waveform recorder.

☐ Restore the UPS input.

- Record the utility restoration and rectifier ramp with the waveform recorder.

F.3.8.3 Parallel UPS System Testing

Parallel System Control Cabinet Data:

Model #: ______________________Serial #:______________________

SCC Rating: ____________SCC Breaker Rating:_____________Amps.

F.3.8.3.1 Steady-State Load Tests

□ Connect the power meter to the output of the parallel system cabinet.

□ Apply 100% load to the UPS system.

1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the power meter.
2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.

□ Apply 50% load to the UPS system.

1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the power meter.
2) Record system output voltage, system output current, and bypass voltage on the System **Cabinet Load Test Data** table.
3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.

□ Remove the entire load from the UPS system.

1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the power meter.
2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.

F.3.8.3.2 Transient Load Tests

□ Connect the waveform recorder to the output of the parallel system cabinet to measure three phases of output voltage, and one phase of output current.

□ Record the following load step transients with the waveform recorder:

1) 0%–50%–0%
2) 50%–100%–50%
3) 25%–75%–25%.

□ Connect the waveform recorder to measure three phases of output voltage, and one phase of the bypass current.

□ Place four UPS modules on line, apply 100% system level load, and record the following transfer transients with the waveform recorder:

1) Normal transfer to bypass
2) Transfer from bypass to UPS.

F.3.8.3.3 Infrared Scan

□ Place all UPS modules in parallel.

□ Place full system level load on the UPS system.

□ Infrared scan the UPS side of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.

□ Transfer the UPS system to static bypass and increase the load to full static bypass current.

□ Infrared scan the static switch bypass side of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.

□ Transfer the UPS system to maintenance bypass and infrared scan the maintenance bypass side and distribution of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.

F.3.8.4 Parallel UPS Module Fault Testing

□ Connect the waveform recorder to monitor three phases of output voltage on the UPS parallel bus.

□ Place all UPS modules in parallel.

□ Apply 100% load to the system.

□ Place a waveform recorder CT on the output of UPS Module 1, and connect to the waveform recorder.

□ Open the output breaker for UPS 1 to remove it from the bus. Record the transient with the waveform recorder.

□ Restore UPS 1 to the parallel bus. Record the transient with the waveform recorder.

☐ Place a waveform recorder CT on the output of UPS Module 2, and connect to the waveform recorder.
☐ Open the output breaker for UPS 2 to remove it from the bus. Record the transient with the waveform recorder.
☐ Restore UPS 2 to the parallel bus. Record the transient with the waveform recorder.
☐ Place a waveform recorder CT on the output of UPS Module 3, and connect to the waveform recorder.
☐ Open the output breaker for UPS 3 to remove it from the bus. Record the transient with the waveform recorder.
☐ Restore UPS 3 to the parallel bus. Record the transient with the waveform recorder.
☐ Place a waveform recorder CT on the output of UPS Module 4, and connect to the waveform recorder.
☐ Open the output breaker for UPS 4 to remove it from the bus. Record the transient with the waveform recorder.
☐ Restore UPS 4 to the parallel bus. Record the transient with the waveform recorder.

F.3.8.5 Critical Load Restoration

☐ Shut down the UPS system and disconnect the load banks.
☐ Close the output breakers on the UPS parallel switchgear.
☐ Transfer the UPS system to bypass.
☐ Transfer the maintenance bypass switch B to UPS.
☐ Transfer the maintenance bypass switch A to UPS.
☐ Start the UPS system and transfer from bypass to UPS.
☐ Transfer switchboard UPS-Input to normal.
☐ Shutdown the diesel generators by returning the DG parallel switchgear to **Automatic**.

F.3.9 Data Tables

DIESEL HEAT RUN TEST DATA SHEET UNIT #: __________
DATA COLLECTED BY: ______________ TEST DATE:______________
DIESEL MANUFACTURER: ______________ RATING: ____________
MODEL NO. ______________ SERIAL NO___________________

	Time	0:00	0:15	0:30	0:45	1:00	1:15	1:30	1:45	2:00	2:15	2:30	2:45	3:00	3:15	3:30	3:45	4:00
Engine Data	Exhaust temp left (°F)																	
	Exhaust temp right (°F)																	
	Battery voltage (V_{DC})																	
	Engine revolutions																	
	Oil pressure (psi)																	
	Fuel pressure (psi)																	
	Coolant temp (°F)																	
Output	Phase A-B V_{AC}																	
	Phase B-C V_{AC}																	
	Phase C-A V_{AC}																	
	Phase A current																	
	Phase B current																	
	Phase C current																	
	Frequency (Hz)																	
	kW																	

DIESEL GENERATOR TEST DATA SHEET

UNIT NO: ______________________________ TEST DATE: ___________

MANUFACTURER: _____________________

GENERATOR MODEL NO: _______________ SERIAL NO. ___________

ENGINE _______________________________ SERIAL NO. ___________

Engine Data

	No load	50% load	100% load
Exhaust temp left (°F)			
Exhaust temp right (°F)			
Battery voltage (V_{DC})			
Engine revolutions per minute			
Oil pressure (psi)			
Coolant temp (°F)			

Generator Data

	No load		50% load		100% load	
	Panel mtr	Test inst.	Panel mtr	Test inst.	Panel mtr	Test inst.
Phase A–B voltage						
Phase B–C voltage						
Phase C–A voltage						
Phase A current						
Phase B current						
Phase C current						
Frequency (Hz)						
L–L THD (%)						

Paralleling Switchgear, 3 Generators in Parallel

		System output voltage			*System output current*			*System additional readings*		
		A - B	*B - C*	*C - A*	*A*	*B*	*C*			
No load	*Panel meter*									
No load	*Test instr*									
50% load	*Panel meter*									
50% load	*Test instr*									
100% load	*Panel meter*									
100% load	*Test instr*									

Parallel Load Sharing, All 3 Generators

	GEN 1			*GEN 2*			*GEN 3*		
Mtrs:	*θA*	*θB*	*θC*	*θA*	*θB*	*θC*	*θA*	*θB*	*θC*
0% GEN									
0% Swgr									
50% GEN									
50% Swgr									
100% GEN									
100% Swgr									

UPS MODULE #_____

Load Test and Meter Calibration Data

		Input voltage			*Input current*			*Output voltage*			*Output current*		
		A–B	*B–C*	*C–A*	*A*	*B*	*C*	*A–B*	*B–C*	*C–A*	*A*	*B*	*C*
0%	*Panel meter*												
	Test inst												
	THD												
50%	*Panel meter*												
	Test inst												
	THD												
100%	*Panel meter*												
	Test inst												
	THD												

Input Harmonic Filter Current Balance

	A∅	*B∅*	*C∅*	*A∅ - N*	*B∅ - N*	*C∅ - N*
AMPS						

Output Harmonic Filter Current Balance

	A∅	*B∅*	*C∅*	*A∅ - N*	*B∅ - N*	*C∅ - N*
AMPS						

Rectifier Current Balance

	△A	*△B*	*△C*	*YA*	*YB*	*YC*
AMPS						

UPS System Cabinet Readings

		System output voltage			*System output current*			*Bypass voltage*		
		A–B	*B–C*	*C–A*	*A*	*B*	*C*	*A–B*	*B–C*	*C–A*
0%	*Panel meter*									
	Test instr									
	THD									
50%	*Panel meter*									
	Test instr									
	THD									
100%	*Panel meter*									
	Test instr									
	THD									

Parallel Load Sharing, UPS Modules 1, 2, 3, and 4

	UPS 1			*UPS 2*			*UPS 3*			*UPS 4*		
Mtrs:	*θA*	*θB*	*θC*	*θA*	*θB*	*θC*	*θA*	*θB*	*θC*	*θA*	*θB*	*θC*
0% UPS meter												
0% parallel meter												
50% UPS meter												
50% parallel meter												
100% UPS meter												
100% parallel meter												

Attendees

Telecommunications Contractor: ______________________________

Owner: ______________________________

____

____

General Contractor: ______________________________

____

Electricians: ______________________________

____

____

____

UPS Vendor: ______________________________

____

____

Infrared: ______________________________

____

Diesel Vendor: ______________________________

____

____

Diesel Switchgear: ______________________________

____

____

Appendix G Design for Energy Efficiency (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

G.1 Introduction

Opinions about where power is being consumed in a data center will vary from one data center to another and is a topic of debate, but there is general consensus within the IT community that more than half of the power is consumed by the infrastructure that supports the ITE. Most calculations estimate that 50-55% of the power goes into supporting infrastructure. Figure G-1 shows where energy can be lost. The Green Grid suggests that as little as 30% of the power might actually go into useful work, depending upon how many infrastructure elements (e.g., chillers, transformers, CRACs, etc.) are present. The amount of power actually used by the ITE could be even smaller if ITE is deployed and utilized effectively. Numerous studies have found that most data centers have lots of stranded capacity with the typical server running at only 20% of its capacity; frequently, legacy servers remain connected even though they are no longer being used.

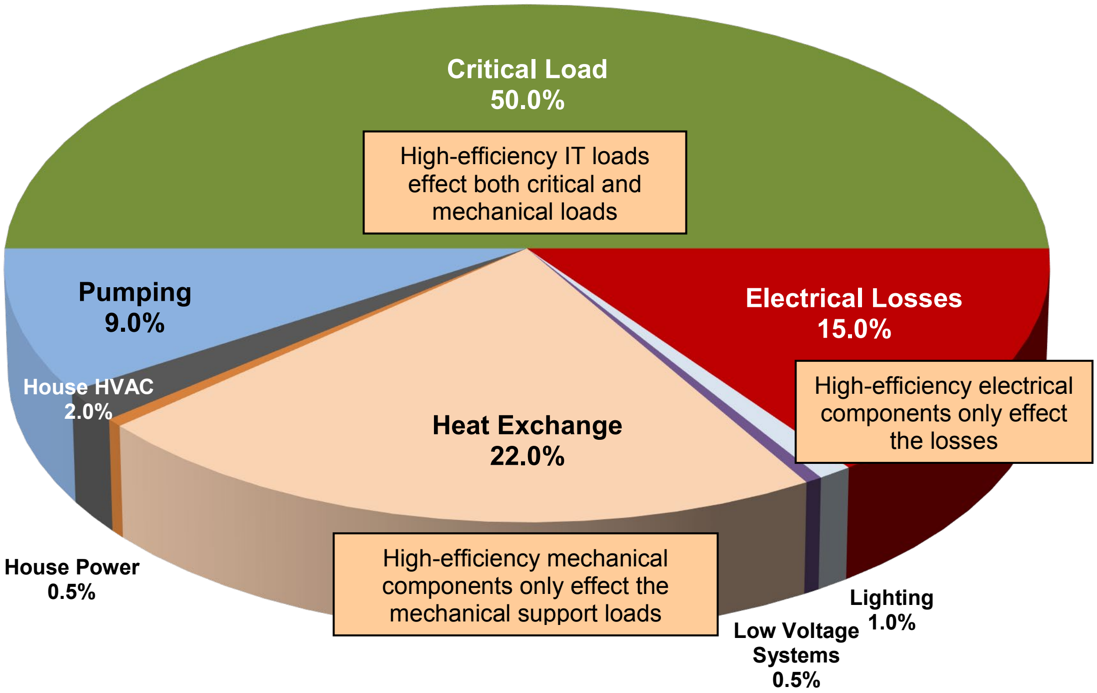


Figure G-1
Example of Data Center Electricity Utilization

Some progress is being made on data center efficiency thanks to higher awareness of the operating costs, better instrumentation, and better metrics such as power utilization effectiveness (PUE). Better software solutions, such as virtualization, are being developed that allow for server consolidation, resulting in higher efficiency and lower total cost of ownership (TCO).

Data center efficiency cannot be managed if it is not accurately measured. Effective measurement relies on the number, location, and accuracy of meters as well as the frequency of measurements. For example, PUE reporting guidelines identify three different sampling levels that factor in where the samples are taken (e.g., UPS, PDU output, or server input), where the facility input power is measured, and how often the measurements are taken (e.g., monthly/weekly, daily, or continuously).

The PUE reporting metric does not factor in the characteristics of the meters themselves. For example, data center switchboard meters are typically "utility grade" with > 99.5% accuracy, whereas meters in rack-mounted power strips frequently have accuracy as low as 96-98%. Because ITE power supplies can create harmonic currents, even when provided with power factor correction filters (e.g., when ITE is operated well below its rated capacity), meters that do not provide true RMS measurements can give misleading data. Higher precision usually means higher capital cost.

G.2 Design for Efficiency

"Design for efficiency" cannot be a separate function. The objective is to create a data center that consumes the least amount of energy possible for any given operation or activity within the data center, but to do so without compromising safety, security, or availability of the IT operation. Efficiency considerations affect almost every aspect of a data center's design. So-called "holistic" design considerations include:

- Site selection (e.g., climate, proximity to water, air quality, power source[s], etc.)
- Building construction and layout:
  - Construction materials
  - Multi use/multi-tenant vs. purpose-built
  - "Modular" (e.g., containerized) and scalable versus "traditional" network architecture
  - Human-machine interface
  - Layout of operational and support spaces
  - Placement of IT and non-ITE
  - Use of alternative energy (e.g., wind, solar, thermal storage, etc.)
  - High performance building methods, metrics, and certifications (e.g., USGBC LEED, ASHRAE bEQ, ENERGY STAR for buildings/data centers, The Green Grid PUE, STEP Foundation, *EU Code of Conduct for Data Centres*)
- Selection of energy-efficient ITE (e.g., servers, storage devices, etc.)
- Selection of energy-efficient devices within the direct power path (e.g., transformers, UPS systems, power distribution units, power strips, etc.)
- Design of critical path power flow to ensure that the data center, area or zone meets the performance requirements of the desired Availability Class (e.g., levels of redundancy) with minimum power consumption
- Decisions on deployment of open racks versus ITE cabinets
- Selection and placement of energy-efficient essential support equipment (e.g., air conditioning systems) including such things as:
  - Perimeter versus row-integrated versus ceiling-mount air handling systems
  - Minimizing the distance that air, water, or power must travel between source and use
- Design of mechanical systems to optimize the operating environment of ITE (e.g., operating temperature, humidity), including such things as:
  - Raised floors versus slab
  - Equipment layout (hot-aisle/cold-aisle)
  - Aisle containment systems
  - Air or water side economizer operation
  - Cogeneration/combined heat and power (CHP)
- Integration of building information management systems
  - Metering, reporting, and controls

Certain principles apply to any design such as:

- Design for the entire system rather than for individual components. Two data centers with identical ITE can have very different electric bills and different PUE because of the system design and the activities of the data center
- Optimize equipment cooling infrastructure:
  - At some point, liquid cooling may be a better option than air cooling, but also consider flexibility, capital costs, operating costs, and reliability of pumps.
  - Lay out equipment in a manner to minimize the mixing of ITE input and exhaust air.
  - Use blanking panels.
  - Utilize ITE designed to operate reliably at high ambient temperatures.
  - Consider cabinets versus open rack systems.
  - Consider aisle containment systems.
  - Use water or air-side economizers where feasible.
- Configure and utilize software such as data center infrastructure management (DCIM) software. Minimize the number of task-specific or proprietary software protocols that are used. A common language that can interface with a building information management (BIM) system is best.
- Avoid running power and signal cabling in spaces meant for movement of air (such as under a raised floor) as this practice can create obstructions and alter air patterns.
- Minimize the distances that air, power, and/or water must travel to reach the ITE. Consider using point of use (close-coupled) power systems, air conditioning systems, and/or chilled water distribution systems.
- Use modular equipment (power, cooling, and IT) in order to match the infrastructure components to the needs of the ITE (i.e., “right-size”).
- Use best-in-class power equipment that can deliver high efficiency over a broad range of loads (e.g., percent efficiency in the high 90s when running at 20% to 100% of load). Consider multi-mode equipment that can operate in higher efficiency modes when conditions are favorable (e.g., UPS with eco-mode option or air conditioning with economizer mode).
- Install energy-efficient lighting (e.g., LED) and controls to illuminate only when and where needed.
- Plumb for efficiency. Close couple wherever possible. Insulate plumbing and make it easily accessible without interrupting other datacenter infrastructure.
- Run plumbing (e.g., chilled water) in directions parallel to the equipment and to air flow.

G.3 Efficiency Content of BICSI 002-2019

Within BICSI 002, sections that include information related to improving efficiency are identified in the following list:

• Design for Efficiency and Metrics	Section 6.7
• Site Selection	Section 5
• Building Construction and Configuration	
– Alternative Energy Considerations	Section 5.7.6.4
– Cooling Capacity	Section 6.3
– Critical Path Power Space Planning	Section 6.2
– Environmental Design	Section 6.4.11
– Functional Adjacencies	Section 6.4
– General Considerations	Section 7.2
– Modularity	Section 6.1.2
• Power	
– Capacity versus Utilization	Section 9.1.5
– Critical Path Power Space Planning	Section 6.2
– Direct Current (DC)	Section 9.3.13
– Distribution with Access Floor	Section 6.5.2
– Lighting	Section 9.8
– Mechanical Equipment Support	Section 9.4
– Monitoring	Section 9.7

List continues on the next page

• Mechanical/Cooling Systems	
– Access floors	Section 6.5.1
– Aisles (e.g., hot/cold aisle, containment)	Sections 6.6.4, 14.12.5
– Ceilings	Section 7.5.11
– Space Planning	Section 6.3
– Air Flow (Thermal) Management	Sections 10.5, 14.12.6
• Information Technology Equipment	
– Aisles	Section 6.6.4
– Computer Room Configuration	Section 15.2
– Racks, Cabinets and Frames	Sections 6.6.3, 14.12
– With use of access floors	Section 6.5
• Data Center Infrastructure Management (DCIM)	Section 13.4

Note that this list is not inclusive of all efficiency content within BICSI 002 as other recommendations outside of the sections listed above may provide additional efficiency benefit.

Appendix H Colocation Technical Planning (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

H.1 Introduction

Deploying systems in colocation facilities (colos) outsources many data center functions, permitting faster deployment, reducing initial capital costs, and allowing information technology (IT) to concentrate on IT rather than facility issues.

Careful planning and investigation are needed before committing to move into a colo:

- To ensure that the colocation facility meets the requirements
- To ensure that the colocation service provider clearly understands the requirements
- Possibly to detail these requirements in the contract documents.

Ensure that the colo can meet the design requirements before finalizing selection. The colocation providers will need to provide a great deal of detailed information for the designer to plan the cage/suite properly. The designer may need to work with several colocation providers concurrently, not only to ensure competitive pricing, but also to ensure that there is a viable alternative if there is a major shortcoming with the primary site that arises during discovery or a major issue that arises during contract negotiations.

H.2 Administrative

When working with the colocation site provider, it is useful to have the following information:

- Site code name (helps when communicating with the colo to use the same name for the site that they do).
- Primary contact for addressing technical questions and issues.
- Site address, floor, room name, and cage number/code for deliveries and work requests.

H.3 Floor Plan

1) Obtain floor plan of data center showing proposed suite/cage.
2) Determine if the equipment fits in the space with desired cabinets and adjacencies including doors, ramps, man traps, aisles, columns, and other support equipment required in the space (electrical, cooling, fire suppression)
3) Is there room for expansion? If so, where? Is it possible to arrange right of first refusal for the expansion space?
4) Are there any adjacent rooms that could be of concern (electrical rooms or elevators that could create EMI), competitors, potentially hazardous spaces such as kitchens?
5) Is space needed on the computer room or nearby for other functions such as staging, operations staff, security staff, storage, media destruction and secure storage?

H.4 Ceiling Height

1) What height is required for the cabinets (with and without casters), racks, and frames.
2) What height is required for any overhead cable tray, optical fiber duct, and power busway/tray?
3) What is the structural ceiling height?
4) What is the false ceiling height (if present)? Can the false ceiling be removed if required to provide adequate clear ceiling height?
5) What are the heights of other obstructions that cannot be raised such as beams and fire suppression pipes? If the obstructions are lower than the desired clear ceiling height, ask the colocation provider to provide the location of the obstructions with their heights on the floor plan.
6) What is the height of obstructions that can be moved (such as lights, electrical ducts, and fire suppression heads? If the obstructions are lower than the desired clear ceiling height, ask the colocation provider to provide the location of the obstructions with their heights on the floor plan. If they need to be moved, determine the relocation cost.
7) What clearance do local codes require around the sprinklers? For example, in the US and many other countries, it is a 450 mm (18 in) dome around the sprinkler head.
8) Where are the light fixtures? They should be above the aisles and not above the cabinets/trays to meet 500 lux requirements in aisles.

H.5 Movement of Equipment

1) What are the dimensions and weights of the cabinets and equipment packaged for shipment?
2) Can the cabinets/equipment be tilted? If so, what is the maximum tilt?
3) How much height is added by the pallet jack used to transport the cabinet/equipment from the loading duct to the cage/suite?
4) Can the loading dock, elevator, hallways and all doors along the entire delivery route accommodate the delivery of the cabinets and equipment?
   - A. Door heights
   - B. Man trap sizes
   - C. Elevator sizes
   - D. Floor loading
   - E. Elevator weight capacity
   - F. Maximum tilt of ramps
5) The ADA recommends a maximum ramp slope of 1:12 for wheel chairs, which is a gradient of 8.3%, or a 4.76-degree slope. This is the desired maximum slope if a ramp must be used for personnel to enter the cage/suite.
6) The British Industrial Truck Association (BITA) specifies a maximum slope of 12.5% for forklift trucks, which is a gradient of 1:8 or 7.13 degrees. This is the desired maximum slope for ramps to be used for movement of equipment.

H.6 Floor Loading

1) What are the weight and dimensions of the heaviest cabinets fully loaded with equipment and media?
2) What are the static, dynamic, and concentrated load specifications of the raised floor?
3) Does the slab need to be reinforced to support the heaviest cabinets?
4) What are the seismic risks and requirements for this site? Should we use seismic cabinets?
5) If the suite/cage will include racks or seismic cabinets, what is the construction of the floor slab? Will the colo permit cabinets and racks to be bolted to the slab? If not, what measures does the colo propose/permit for adequately securing the cabinets and racks?

H.7 Cabinets

1) If colocation facility provides cabinets what are
   - A. Cabinet manufacturer and model number(s)
   - B. Dimensions (height, width, length). Note:
     - o 600 mm cabinet are adequate for servers
     - o Distributors and network equipment should be in 800 mm wide cabinets or in open racks
   - C. Usable rack units (RUs)
   - D. Maximum load rating(s)
   - E. Accessories installed (e.g., for cable management, cooling) – is more cable management required?
   - F. Default rail locations – can we specify them to be moved?
     - o Need rails set back for network and distributor cabinets (~250 mm)
     - o Front to rear rail spacing of 736 mm works for most equipment
2) What type of cabinets and racks are permitted? For example, some colos specify that only cabinets with vertical exhaust ducts are allowed, no racks.
3) What type of containment is required?
   - A. No containment required
   - B. Hot-aisle containment
   - C. Cold-aisle containment with roof
   - D. Cold-aisle containment, but with no roof required
4) If containment with roof is required determine requirements for fire protection (commonly, the roof panels must drop if there is a fire)

H.8 Meet-Me Rooms (MMRs) / Point-of-Presence Rooms (POPs)

1) What are the number and location of Meet-Me Rooms (MMRs) or Point-of-Presence (POP) Rooms that will serve the cage/suite (should be at least 20 meters apart)
2) What is the identification information for the carriers to order circuits to each MMR/POP? (Customer will need different information for each room to manage where each circuit terminates)
3) Is the customer permitted to install their own patch panels or cabinets in the MMR/POP rooms? (Some customers such as carriers, ISPs, or owners of large suites, want responsibility for the circuits from the carrier demarcation point in the MMR/POP to the suite/cage)
4) If the customer desires and is permitted to install cabinets in the MMR/POP rooms, request floor plans and proposed locations for cabinets in these rooms
5) If the customer desires and is permitted to install patch panels (but use the colo cabinets/racks), then request the floor plan, cabinet ID, and RU locations for the patch panels
6) Cabinets and patch panels in colo MMR/POP rooms may have locks for additional security
7) Which carriers/service providers can provision circuits to each MMR/POP?
8) What type of circuits can each carrier provide in each MMR/POP. Many colos can only provision telephone lines from one room.
9) Is there are need to install cabling and antennas for satellite, network timing, microwave radio, or other services? If so, specify antenna location, mounting, and cabling requirements to colo.
10) Specify any requirements for conduits for antenna cabling, security cabling (badge readers, cameras, cabinet locks) and DCIM (PDU and air conditioning controls/monitoring)

H.9 Cabling to MMR/POP Rooms

1) What are the routes for cabling from these rooms to the cage/suite (should be diversely routed and not overlap)
2) What degree of protection does the customer require for this cabling and can the colo provide the required protection
   A. Open cable trays (most common)
   B. Shared conduit
   C. Dedicated conduit from MMR/POP to cage/suite with no shared pull boxes) – all pull boxes with locks unique to customer. If dedicated conduit is needed specify size and type of conduit and number and type of innerduct. Review location and specification of pull boxes.
3) Who is responsible for installing cabling from MMR/POP rooms to customer cage/suite?
4) How is the customer charged for the cabling (one-time cost only, one-time cost + monthly recurring, monthly recurring only)?
5) If carrier installs cabling, specify exactly the cabling required from the cage/suite to each MMR/POP room (type, quantity, connectors):
   A. Single-mode optical fiber (for carrier and campus connections) – typically LC/UPC, but may be LC/APC (angled) for broadcast video, wave division multiplexing, other
   B. Multimode optical fiber (used by some carriers for Ethernet connections) – typically LC
   C. Balanced twisted pair (for telephone lines, fractional-E1/T1, E1/T1, some Ethernet connections from carriers) – typically on 8-pin modular jack (RJ45)
6) Assign size, cabinet location and RU location of patch panels to MMR/POP in cage/suite. Some colos may allow customer to specify model # of panel.
7) Colo to specify cabinet ID, patch panel, and ports for terminations in MMR/POP (used to specify cross-connects of circuits to cage)

H.10 Cabling within Cage/Suite

1) Customer typically responsible for cabling within the cage, but this may be outsourced to colo
   - Customer will need to specify exactly the cabling required including type, quantity, termination hardware, cabinet ID and RU location of patch panels
2) Cabinets may need to be secured to the slab (or raised floor system) – who performs this work?
   - Customer will need to specify exactly where cabinets are to be located, exact locations typically required for containment systems to work
3) Cabinets may need floor tile cuts for bonding conductor, power cables, and telecommunications cabling
   - Customer will need to specify type and location of tile cuts
   - Determine manufacturer and model # of grommet used by colo
4) Determine who is responsible for bonding each cabinet (using 6 AWG / 16 mm^2) stranded bonding conductor for each cabinet. Many colos do not allow customers to perform work under the raised floor,
5) If customer is responsible for bonding conductors, designer will need to know size of conductors (for sizing taps) and location of mesh-BN (height and horizontal distance) relative to the cabinets (for lengths of bonding conductors),
6) Determine if the customer has the option of installing cable trays under the access floor (if overhead clearances are not adequate or if more cable tray capacity is desired. Some colos do not permit telecommunications cabling under the access floor. Other colos may desire that telecommunications cabling be under the access floor.

H.11 Power

1) Where and how is power distributed (e.g., power whips under the floor, overhead in cable trays, overhead using electrical bus, other) – obtain elevation showing location of power – ensure adequate separation from copper cabling per applicable standard (e.g., ISO/IEC 14763-2, ANSI/TIA-569-D, CENELEC EN 50174-2),
2) Determine if the color or the customer is responsible for providing cabinet PDUs/power strips.
3) If the colo provides the power strips – what is the model #, # of phases, number of receptacle, and type of receptacles
   - Confirm that the # and type of receptacles matches equipment
4) Who is allowed to plug power strips into the receptacles under the floor? Be certain that power strips are labeled with the PDU/RPP and breaker of the electrical receptacle
5) Customer should provide electrical requirements (kW load for each cabinet). Load may require replacement of single-phase circuits with 3-phase circuits or additional circuits.
6) If customer provides power strips, provide colo with number, type, and location of receptacles
7) Some customers are responsible for Remote Power Panels (RPPs) and/or breakers
   - Need to determine responsibilities for purchase, acquisition, and monitoring
8) Some colos provide monitoring (e.g., circuit level monitoring, temperature) – determine what colo monitors and how reports can be provided to the customer

H.12 Physical Security

1) Building security: what type of security does the building have at all entrances?
2) Room security – what type of security is used within the building to critical rooms (computer room, electrical, mechanical, MMR/POP) card reader, biometric, cameras, audit trail, anti-tailgating, anti-passback?
3) What type of locks are used for access to the customer cage - physical lock, badge reader, audit trail?
4) Access to badge reader logs – if badge reader is controlled by colo, how long are access logs kept and how can customer request logs to cage/suite?
5) Security cameras - specify locations, who monitors video?
6) Video storage duration – if colo owns and monitors camera, how long is security video stored and how can the customer request video?
7) Type of cage or wall material for the customer cage/suite?
8) What can other customers see or access (maybe with a stick or tool) through the cage?
9) What is the height of the cage – does it reach to the false ceiling, permanent ceiling, or below it?
10) Does the wall or cage reach below the raised floor? If not, what prevents someone from entering the cage or suite from below (e.g., bolted tiles) or from unplugging receptacles below cage?

H.13 Storage and Staging

1) How much temporary storage space is available?
2) What is the procedure for access to the storage room?
3) Where can the customer stage equipment for unboxing, building, and configuring gear?
4) What are the procedures and rules for the staging area and storage room?

H.14 Loading Dock

1) What is the size of the loading dock what is the maximum size vehicle that it can accommodate?
2) Are lift gates needed/not needed?
3) What are the scheduling procedures for deliveries, loading dock, and/or elevators - are there limited hours?
4) Does the building require certificate of insurance from the company performing the deliveries for deliveries of equipment inside the computer room?
5) Note the maximum ramp slope if the delivery requires a ramp. For example, the British Industrial Truck Association (BITA) specifies a maximum slope of 12.5% for forklift trucks, which is a gradient of 1:8 or 7.13 degrees.

H.15 Work Rules and Procedures

1) What are the access procedures for customer employees, contractors, and vendors
2) Working under access floor - procedures regarding alarms, notification, tools
3) Types of work not permitted by the customer or customer contractors
4) Other work rules / procedures
5) How to request work orders by the colo
6) Expected turnaround time for quotes and turnaround time for completing work once quote is approved

This page is intentionally left blank

Appendix I Related Documents (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

The following standards and documents are related to or have been referenced within recommendations of this standard and provide additional information that may be of use to the reader.

American Society for Testing and Materials (ASTM International)

- ASTM B539, *Measuring Contact Resistance of Electrical Connections (Static Contacts)*
- ASTM E136, *Standard Test Method for Behavior of Materials in a Vertical Tube Furnace at 750°C*
- ASTM E814, *Standard Test Method for Fire Tests of Penetration Firestop Systems*
- ASTM F1233, *Standard Test Method for Security Glazing Materials and Systems*

American Society of Civil Engineers (ASCE)

- ASCE/SEI 59, *Blast Protection of Buildings*

American Society of Heating, Refrigerating, and Air-Conditioning Engineer (ASHRAE)

- ANSI/ASHRAE 52.2, *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*
- ANSI/ASHRAE/IESNA 90.1, *Energy Standard for Buildings Except Low-Rise Residential Buildings*
- ANSI/ASHRAE 90.4*, Energy Standard for Data Centers*
- AG05, *ASHRAE Guideline 0 Commissioning Process*
- *ASHRAE Handbook – Fundamentals*
- *ASHRAE Handbook – HVAC Applications*
- *ASHRAE Handbook – HVAC Systems and Equipment*

BICSI

- ANSI/BICSI 003, *Building Information Modeling (BIM) Practices for Information Technology Systems*
- BICSI 009, *Data Center Operations and Maintenance Best Practices*
- ANSI/BICSI N1, *Installation Practices for Telecommunications and ICT Cabling and Related Cabling Infrastructure*
- ANSI/BICSI N2, *Practices for the Installation of Telecommunications and ICT Cabling Intended to Support Remote Power Applications*

British Standards Institute (BSI)

- BS 5839, *Fire detection and fire alarm systems for buildings*
- BS 6266, *Fire protection for electronic equipment installations – Code of practice*
- BS 9999, *2017 Fire safety in the design, management and use of buildings – Code of practice*

Builders Hardware Manufacturers Association (BHMA)

- ANSI/BHMA A156.13, *Mortise Locks & Latches*

Building Services Research and Information Association (BSRIA)

- AG 17/2002, *Fire Extinguishing Systems: A guide to their integration with other building services*
- BG 5/2003, *Cooling solutions for IT - A guide to planning, design and operation*

Chartered Institute of Building Services Engineers

- *Guide A: Environmental Design*
- *Guide B2: Ventilation and Ductwork*
- *Guide B3: Air conditioning and Refrigeration*
- *Guide C: Reference Data*
- *Guide E: Fire Safety Engineering*
- *CIBSE Commissioning Code A: Air Distribution Systems*
- *CIBSE Commissioning Code C: Automatic Controls*
- *CIBSE Commissioning Code R: Refrigeration*
- *CIBSE Commissioning Code W: Water Distribution Systems*

European Committee for Electrotechnical Standardization (CENELEC)

- EN 54, *Fire detection and fire alarm systems parts 1-32*
- EN 78, *Refrigerating systems and heat pumps‒Safety and environmental requirements parts 1-4*
- EN 5004, *Fixed firefighting systems–Gas extinguishing systems Parts 1-9*
- EN 12845, *Fixed firefighting systems–Automatic sprinkler systems–Design, installation and maintenance*
- EN 16750, *Fixed firefighting systems–Oxygen reduction systems–Design, installation, planning and maintenance*
- EN 50541-1, *Three phase dry-type distribution transformers 50 Hz, from 100 kVA to 3 150 kVA, with highest voltage for equipment not exceeding 36 kV‒Part 1: General requirements*
- EN 50600, *Information technology‒Data centre facilities and infrastructures part 1 and parts 2.1 to 2.5*

EMerge Alliance

- *Data/Telecom Center Standard*

European Telecommunications Standards Institute (ETSI)

- ETSI EN 300 132-3, *Environmental Engineering (EE); Power supply interface at the input to telecommunications and datacom (ICT) equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400 V*

Factory Mutual

- *FM Global Property Loss Prevention Data Sheets 1-28*

The Green Grid

- *WP#46 - Updated Air-Side Free Cooling Maps: The Impact of ASHRAE 2011 Allowable Ranges*
- *WP#73 - Fluid Connector Best Practices for Liquid-cooled Data Centers*
- *WP#75 - Server Energy Efficiency in Data Centers and Offices*

Illuminating Engineering Society (IES)

- *IESNA Lighting Handbook*
- ANSI/IESNA RP-1-04, *American National Standard Practice for Office Lighting*

Institute of Electrical and Electronics Engineers (IEEE)

- ANSI/IEEE C2, *National Electrical Safety Code (NESC)*
- IEEE C62.72, *IEEE Guide for the Application of Surge-Protective Devices for Low-Voltage (1000 Volts or Less) AC Power Circuits*
- IEEE 485, *IEEE Recommended Practice for Sizing Lead-Acid Batteries for Stationary Applications*
- IEEE 902 (The IEEE Yellow Book), *IEEE Guide for Maintenance, Operation and Safety of Industrial and Commercial Power Systems*
- IEEE 946, *IEEE Recommended Practice for the Design of DC Auxiliary Power Systems for Generating Systems*
- IEEE 1013, *IEEE Recommended Practice for Sizing Lead-Acid Batteries for Stand-Alone Photovoltaic (PV) Systems*
- IEEE 1375, *IEEE Guide for the Protection of Stationary Battery Systems*
- IEEE 1635, *IEEE/ASHRAE Guide for the Ventilation and Thermal Management of Batteries for Stationary Applications*
- IEEE 1692, *Guide for the Protection of Communications Installations from Lightning Effects*
- IEEE 3005 series, *IEEE Energy & Standby Power Systems, previously published as IEEE 446 (The IEEE Orange Book), IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*
- IEEE 3006 series, *IEEE Power Systems Reliability* standards, *previously published as IEEE 493 (The IEEE Gold Book), IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*

Institution of Engineering and Technology (IET)

- *Code of Practice for Cyber Security in the Built Environment*
- *Code of Practice for Electromagnetic Resilience*
- *Requirements for Electrical Installations BS 7671:2018 (IET Wiring Regulations 18th Edition)*

Insulated Cable Engineers Association

- ICEA S-83-596, *Indoor Optical Fiber Cables*
- ICEA S-87-640, *Optical Fiber Outside Plant Communications Cable*
- ICEA S-104-696, *Standard for Indoor-Outdoor Optical Fiber Cable*
- ICEA S-110-717, *Optical Drop Cables*

International Electrotechnical Commission (IEC)

- IEC 60603-7, *Connectors for electronic equipment (multiple document series)*
- IEC 61300-3-6, *Basic Fibre Optic Test Procedures – Part 3: Examination and measurement (multiple document series)*
- IEC 61754, *Fibre Optic Connector Interface (multiple document series)*
- IEC 62040, *Uninterruptible power systems (UPS) (multiple document series)*
- IEC 62305-1, *Protection against lightning. General principles*
- IEC 62305-4, *Protection against lightning. Electrical and electronic systems within structures*

International Organization for Standardization (ISO)

- ISO/IEC 14908-1, *Information technology – Control network protocol*
- ISO 16484, *Building automation and control systems*
- ISO 27000 Series, *Information technology – Security techniques – Information security management systems*
- ISO 27001, *Information security management*
- ISO/IEC TR 29106:2007, *Information technology – Generic cabling – Introduction to the MICE environmental classification*
- ISO/IEC 30134-1, *Information technology – Data centres – Key performance indicators – Part 1: Overview and general requirements*
- ISO/IEC 30134-2, *Information technology – Data centres – Key performance indicators – Part 2: Power usage effectiveness (PUE)*
- ISO/IEC 30134-3, *Information technology – Data centres – Key performance indicators – Part 3: Renewable energy factor (REF)*
- ISO/IEC 31000, *Risk management – Guidelines*

Laser Institute of America (ASC Z136)

- ANSI Z136.2, *American National Standard for Safe Use of Optical Fiber Communications Systems Utilizing Laser Diode and LED Sources*

National Electrical Contractors Association (NECA)

- ANSI/NECA 339, *Standard for Building and Service Entrance Grounding and Bonding*

National Electrical Manufacturers Association

- ANSI C80.3, *American National Standard For Steel Electrical Metallic Tubing (EMT)*
- NEMA VE 1, *Cable Tray Systems*
- NEMA VE 2, *Metal Cable Tray Installation Guidelines*

National Fire Protection Association (NFPA)

- NFPA 70B, *Recommended Practice for Electrical Equipment Maintenance*
- NFPA 90A, *Standard for the Installation of Air-conditioning and Ventilating Systems*
- NFPA 101, *Life Safety Code*
- NFPA 110, *Standard for Emergency and Standby Power Systems*
- NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems*
- NFPA 258, *Recommended Practice for Determining Smoke Generation of Solid Materials*
- NFPA 5000, *Building Construction and Safety Code*
- *NFPA Fire Protection System for Special Hazards*

National Institute of Science and Technology (NIST)

- NIST SP 800-30, *Guide for Conducting Risk Assessments*

Open Compute Project

- *Colocation Facility Guidelines for Deployment of Open Compute Racks*

SAE International

- SAE JA1011, *Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes*

Telecommunications Industry Association (TIA)

- TIA-232-F, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*
- ANSI/TIA-455-57-B, FOTP-57, *Preparation and Examination of Optical Fiber Endface for Testing Purposes*
- ANSI/TIA-455-95-A, FOTP-95, *Absolute Optical Power Test for Optical Fibers and Cables*
- ANSI/TIA-455-133-A, FOTP-133-IEC-60793-1-22, *Optical Fibres-Part 1-22: Measurement Methods and Test Procedures-Length Measurement*
- TIA-4720000-A, *Generic Specification for Optical Waveguide Fibers*
- ANSI/TIA-485-A, *Electrical Characteristics of Generators and Receivers For Use In Balanced Digital Multipoint Systems*
- ANSI/TIA-526-7-A, *Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant, Adoption of IEC 61280-4-2 edition 2: Fibre-Optic Communications Subsystem Test Procedures – Part 4-2: Installed Cable Plant – Single-Mode Attenuation and Optical Return Loss Measurement*
- ANSI/TIA-526-14-C, *Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant; IEC 61280-4-1 Edition 2, Fibre-Optic Communications Subsystem Test Procedure – Part 4-1: Installed Cable Plant – Multimode Attenuation Measurement*
- ANSI/TIA-568.1-D, *Commercial Building Telecommunications Cabling Standard*
- ANSI/TIA-758-B, *Customer Owned Outside Plant Telecommunications Infrastructure Standard*
- TIA-TSB-185, *Environmental Classification (Mice) Tutorial*

Underwriters Laboratories (UL)

- ANSI/UL 797, *Standard for Electrical Metallic Tubing – Steel*
- ANSI/UL 972, *Burglary-Resisting Glazing Material*
- ANSI/UL 1479, *Standard for Fire Tests of Through-Penetration Firestops*

United States Department of Defense

- UFC 3-301-01, *Structural Engineering*
- UFC 3-310-04, *Seismic Design of Buildings*

Other Standards and Documents

- *2019 Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency: Version 10.1.0*
- *Americans with Disabilities Act* (United States)
- *Disability Discrimination Act* (Australia)
- Federal Communications Commission (FCC) Part 15 and Part 68 (United States)
- *International Fire Code (IFC)*, 2009
- Rural Utilities Services (RUS), Bulletin 345-63, *RUS Specifications for Acceptance Tests and Measurements of Telephone Plant (1995)*

This page intentionally left blank